

Windows GPO

Deep Dive

Daniel L. Benway

Systems & Network Administrator / Engineer

BS/CS, MCSE (NT4, 2000), MCTS (SCCM 2012), CCNA (2.0), Network+, CLP (AD R4)



<http://www.linkedin.com/in/DanielLBenway>



<http://www.DanielLBenway.net>



@Daniel_L_Benway

General Information on Group Policy Objects:

- The term “Group Policy Object” refers to the Group Policy, not the AD Object (Site, Domain, Organizational Unit) against which the policy is applied.
- Containers cannot have GPOs, only Local Computers, Sites, Domains, and OUs can have GPOs.
- OUs are used to apply Group Policies, delegate administrative control, provide for application functionality and access, and group similar objects for ease of administration.
- NT4 used System Policies instead of GPOs.

Windows 20XX GPOs vs. NT4 System Policies:

- In Windows 20XX, Group Policy Objects are applied against Local Computers, Sites, Domains, and Organizational Units, whereas in Windows NT4 System Policies are applied against security groups.
- Windows 20XX Group Policies are only applied against Windows 20XX-like computers (20XX Servers, 2000 Professional, XP, Vista, 7, 8). If you want to use System Policies for NT4 or 9x clients, you have to create them with their respective policy editor, put them in the NETLOGON shares of all authenticating Domain Controllers (NT4 and W20XX) and have them applied against security groups.
- The NETLOGON share for Windows 20XX is systemroot\ sysvol\ “domain_name” \scripts (where “domain_name” is the actual DNS FQDN of the Windows 20XX domain).
- The Windows 20XX REPL\$ share is systemroot\ system32\ repl\ export, but it isn’t very important seeing how directory replication is handled by the AD replication schemes. Chapter 8 of the Domain Migration Cookbook in MS TechNet 1/2001 explains how to deal with directory replication of the NETLOGON share in a mixed mode environment.

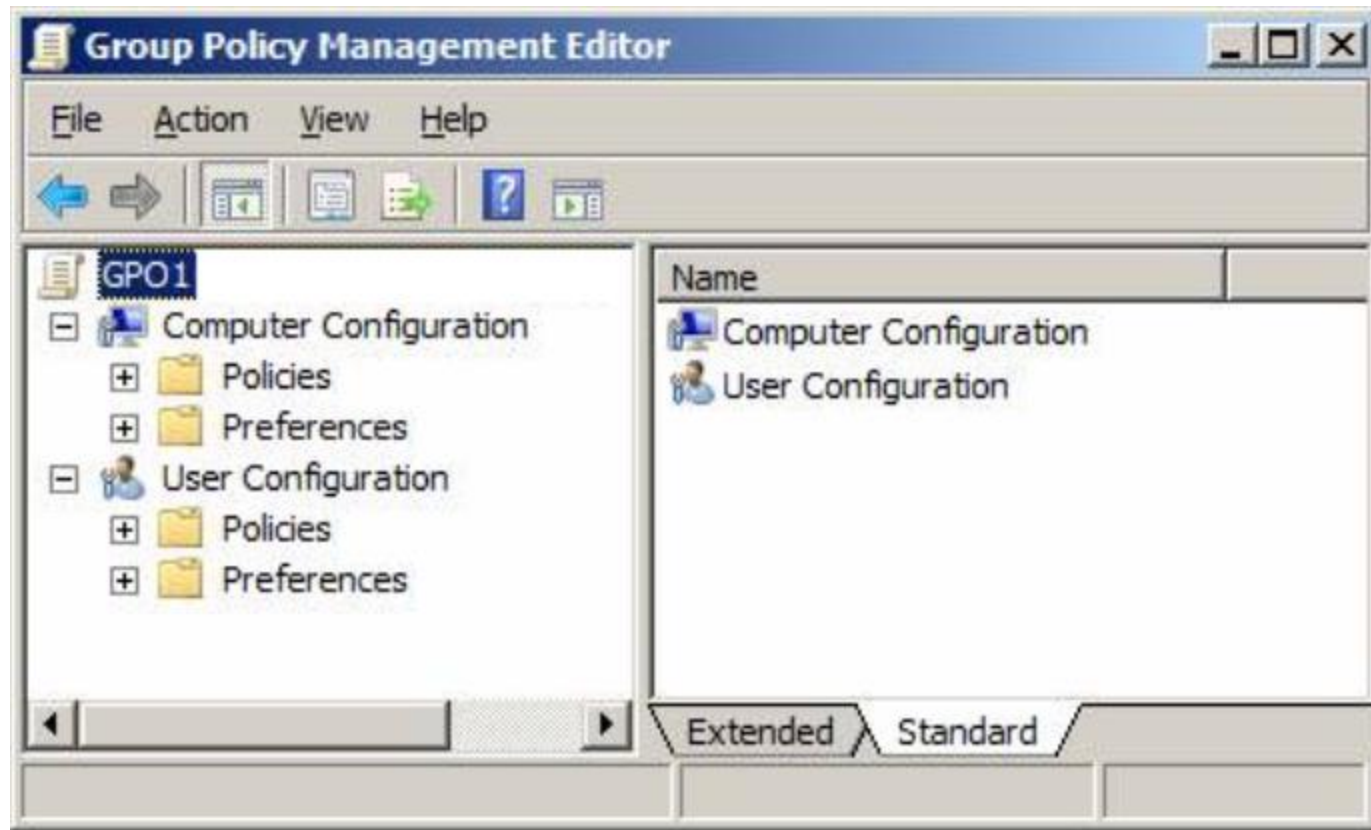
GPO Structure:

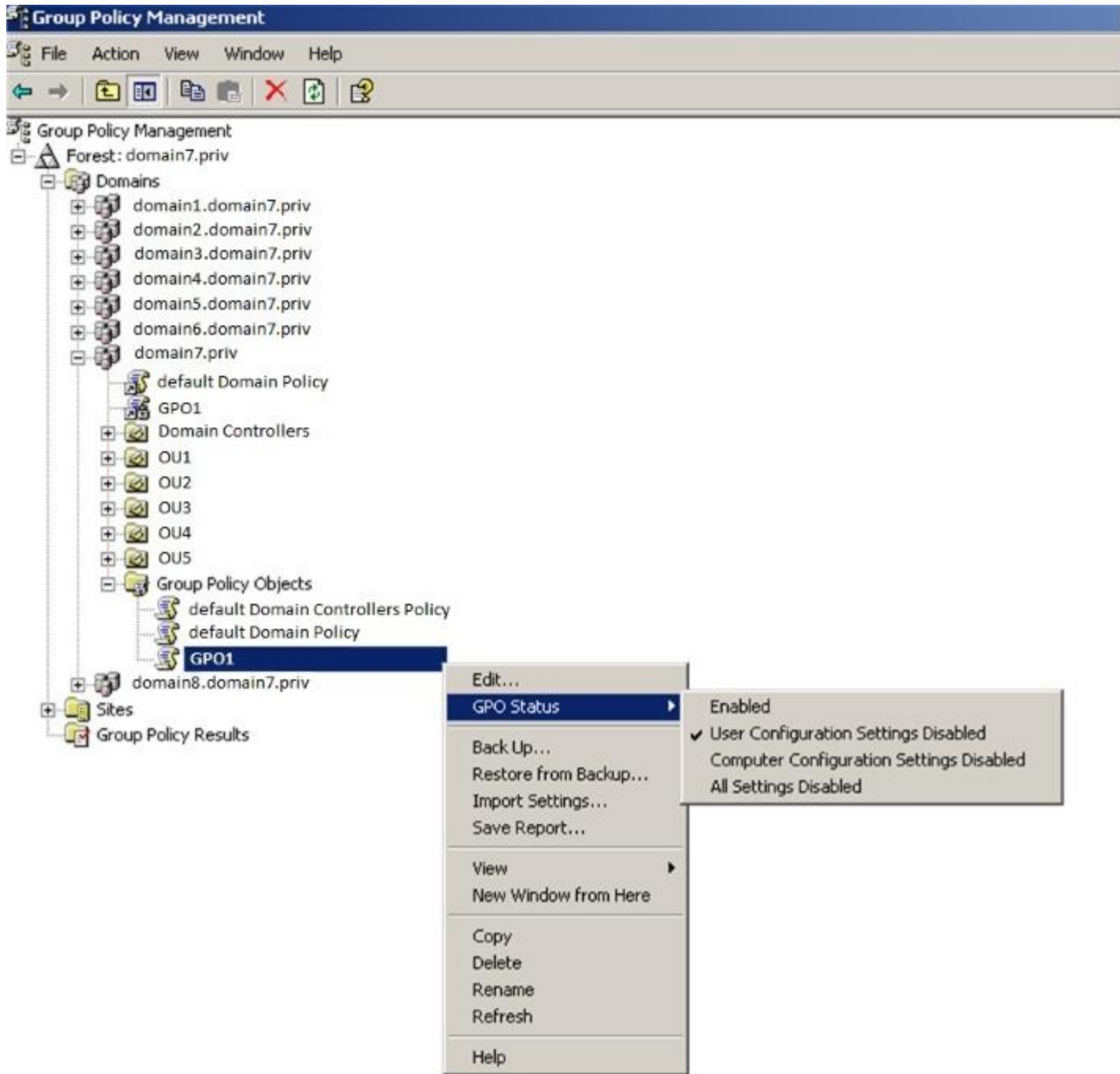
- GPOs have two parts: Computer Configuration, and User Configuration.
- The division between these two parts is not absolute, because many settings in the Computer Configuration can be viewed as 'user related', and many settings in the User Configuration can be viewed as 'computer related'.
- For example, user password policies are in the 'Computer Configuration' portion of GPOs.
- The division between Computer Configuration and User Configuration is more about when and how the settings are applied than the difference between the user and the computer.



Group Policy Preferences:

- Group Policy preferences, new for the Windows Server 2008 operating system, expand the range of configurable settings within a Group Policy object (GPO).
- Group Policy preferences enable you to deploy settings to client computers without restricting the users from changing the settings. This capability provides you with the flexibility to decide which settings to enforce (Policies) and which settings to not enforce (Preferences).





GPO Status:

- You can enable or disable the computer configuration settings, the user configuration settings, or the entire GPO. This will effect the GPO itself, and thus any links to it.
- You can enable or disable any of the links that connect a GPO to an AD object, but doing so will effect only that particular link and will not change any other link, or the GPO itself.
- It is important to disable the computer settings, the user settings, or the entire GPO when they are not being used in order to speed up processing on the client side, and reduce overhead on the DC side.

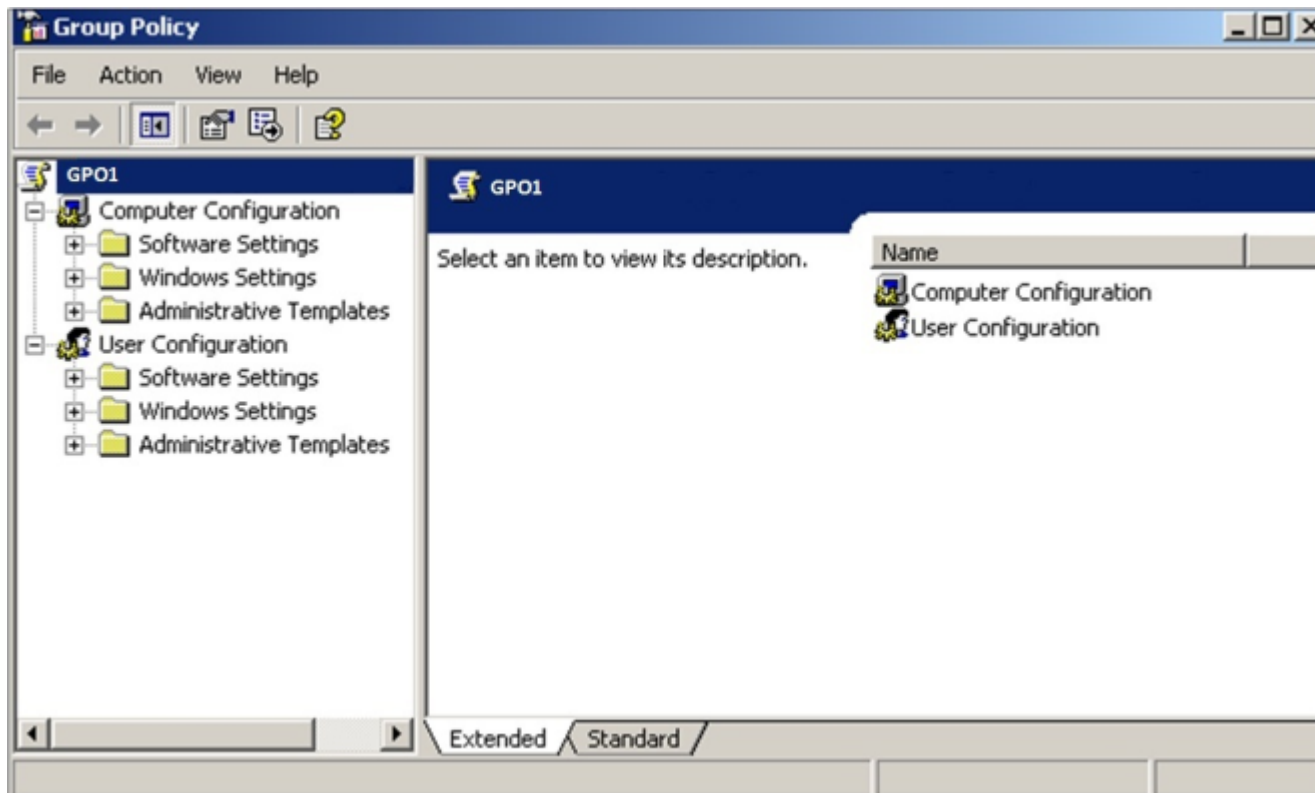
Group Policy Processing Sequence:

Don't confuse processing sequence with Link Order, Inheritance, or RSOP.

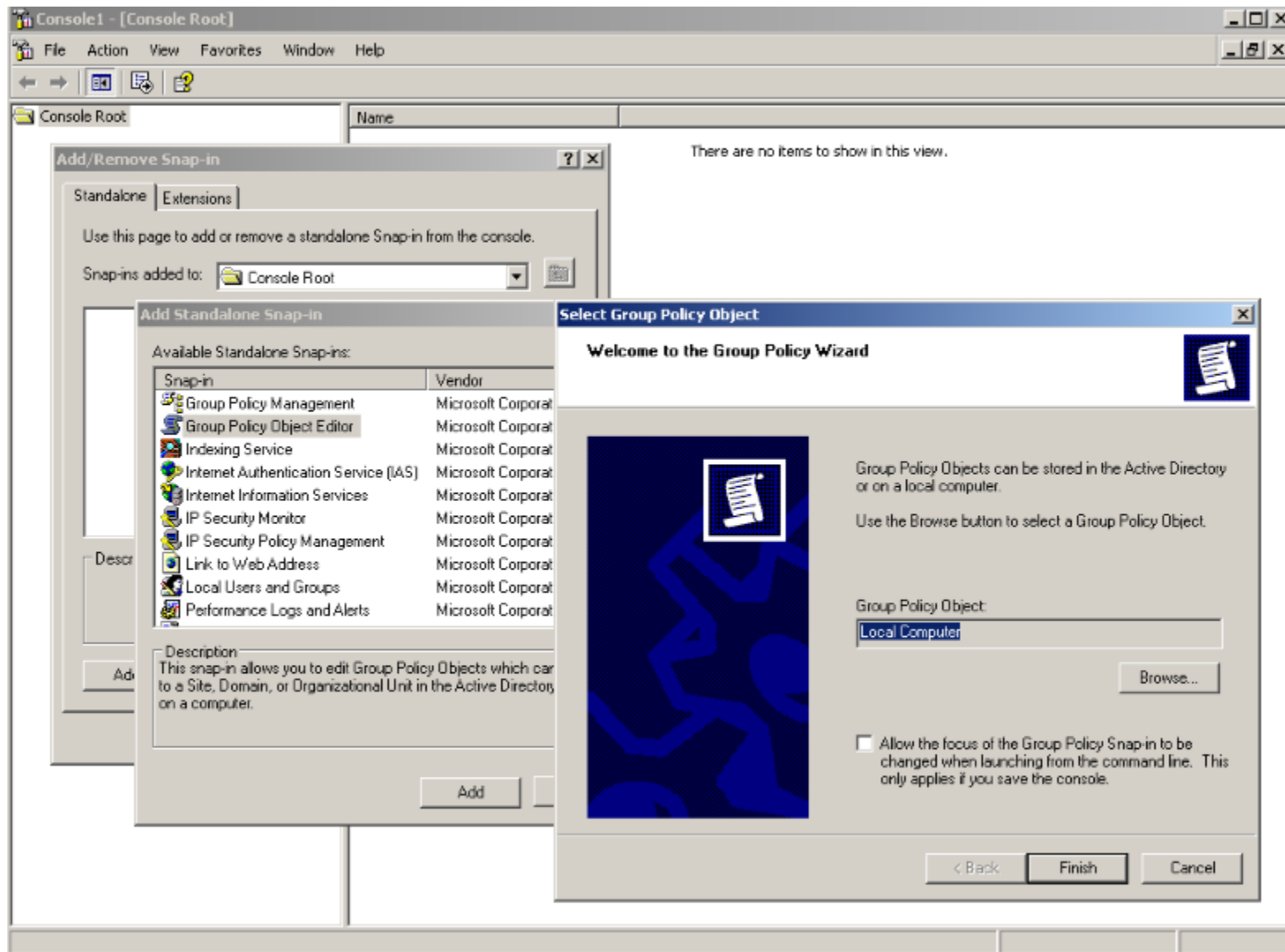
The Group Policy settings are processed in the following sequence by default:

1. The computer starts:
 - 1.1. Computer Configuration is applied
 - 1.2. Startup scripts are run (sequentially by default - each one must complete or time out before the next will start)
2. The user logs on:
 - 2.1. User Configuration is applied
 - 2.2. Logon scripts applied through the user portion of Group Policy are run
 - 2.3. Logon scripts associated with the user account run

These defaults can be changed with Loopback functionality.

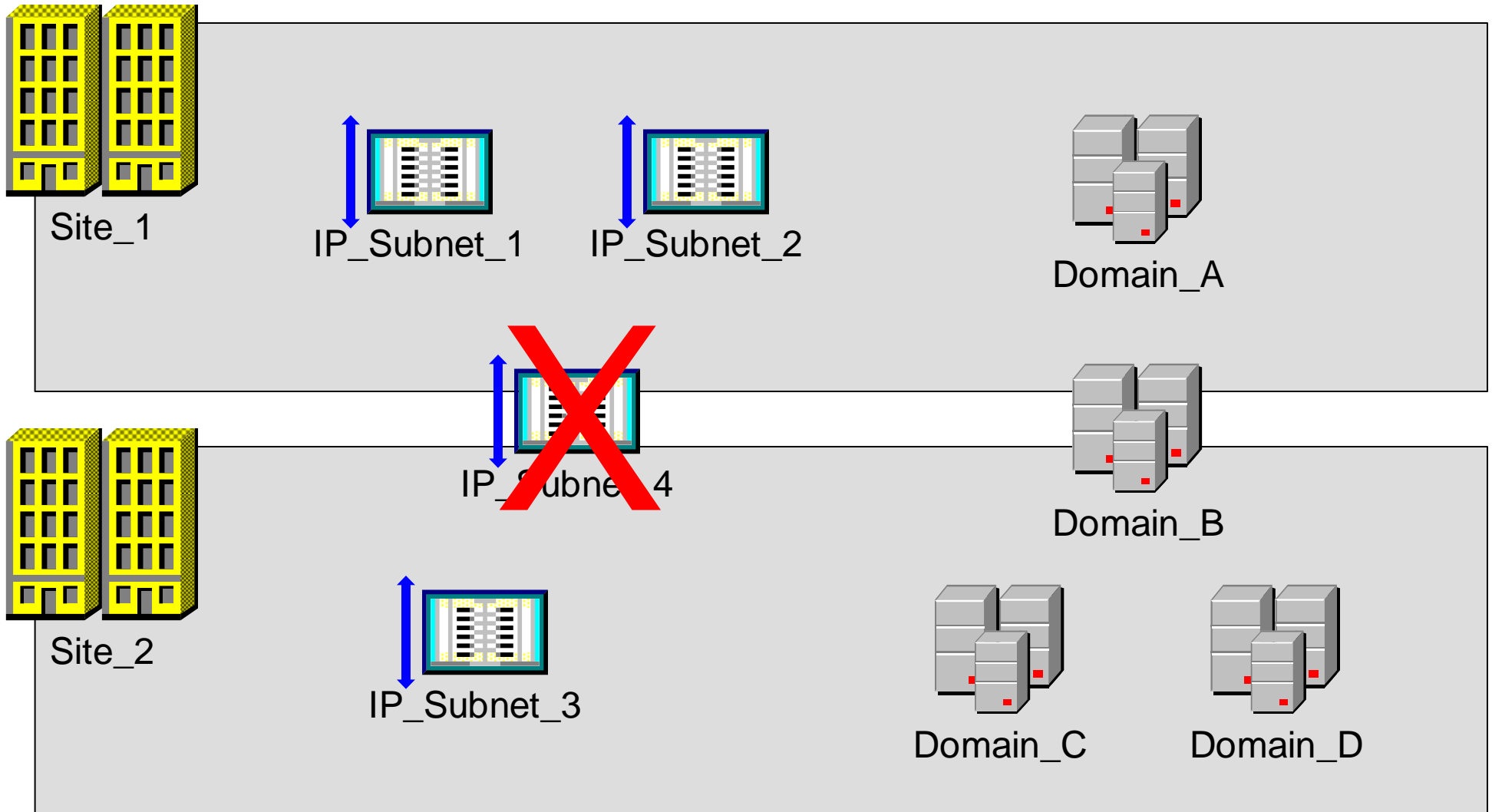


Local GPO / Local Computer Policy / Local Policy:



Note that the Local GPO doesn't have an 'Enforced' (previously known as 'No Override') option, thus one cannot locally set options that can never be overridden by GPOs that reside at a higher level in the Active Directory.

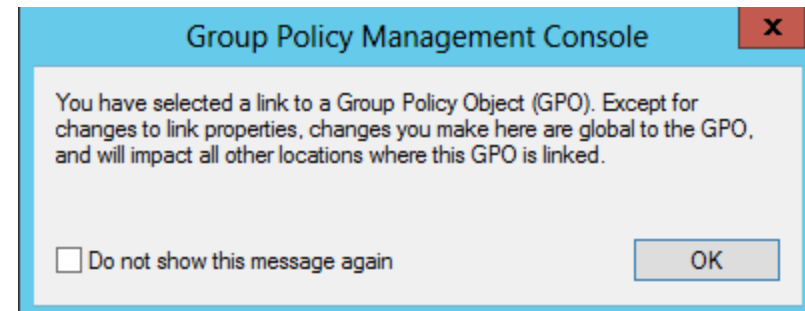
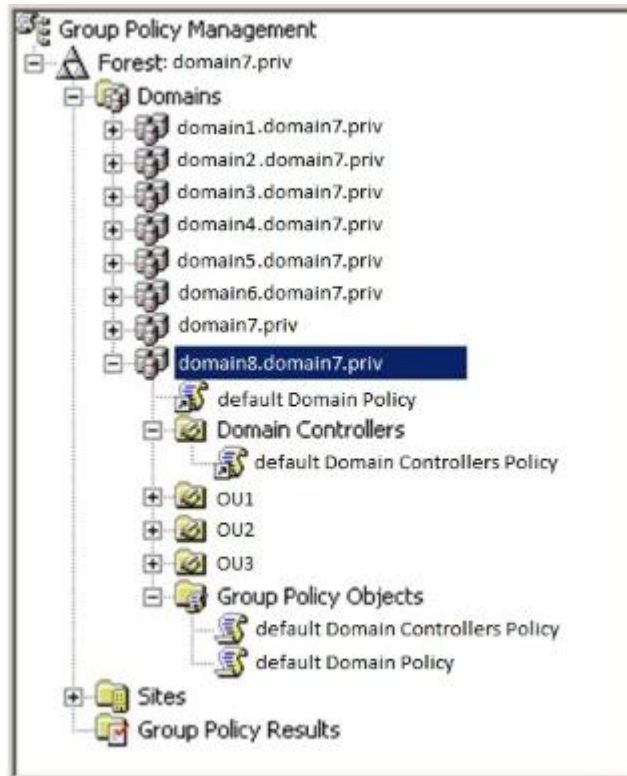
Sites, Subnets, and Domains:



- A site may contain multiple subnets
- A site may contain multiple domains
- A subnet may NOT span multiple sites
- A domain may span multiple sites

Linking a GPO to an AD Object:

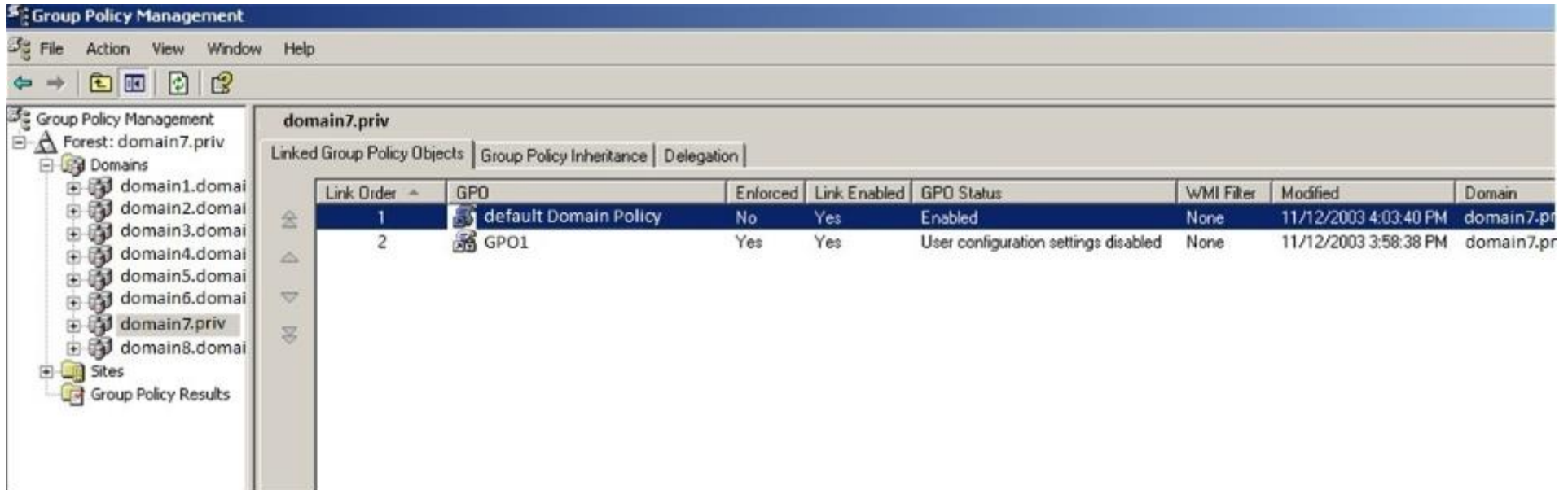
- AD based GPOs (vs. local computer policies) are linked to sites, domains, or OUs, but they don't actually belong to those AD objects. Site, Domain, and OU GPOs are actually stored in the Domain Partition for the domain in which they were created (this is a bit strange for Site GPOs because a site can contain many Domains, and a Domain can span sites).
- You can create new GPOs, add links to existing GPOs, delete links to existing GPOs, or delete the actual GPOs themselves as well as all links that refer to them.
- You can link to GPOs from non-local domains, but this is almost always poor practice due to latency.



- Default Domain Policy and default Domain Controllers Policy GPOs cannot be deleted. This is as designed. Those GPOs always have the following GUIDs respectively:
 - {31B2F340-016D-11D2-945F-00C04FB984F9} – default Domain Policy
 - {6AC1786C-016F-11D2-945F-00C04FB984F9} – default Domain Controllers Policy
- Best practice, don't edit the Default Domain Policy GPO, or the Domain Controllers GPO. Keep these unaltered and clean. If you need different settings, create new GPOs with lower link orders.

Link Order:

In the event that a single AD object (a Site, Domain, or OU) has multiple GPOs linked to it, (n+1) is applied first, then (n) is applied, then (n-1) is applied. E.g., 3 is applied first, then 2 is applied, then 1 is applied (which means 1 is the strongest and most patient).



The screenshot shows the Group Policy Management console for the domain7.priv. The left pane shows a tree view of domains from domain1.domai to domain8.domai. The right pane shows the 'Linked Group Policy Objects' tab for domain7.priv. A table lists the linked GPOs with their link order, names, enforcement status, link status, GPO status, WMI filters, modification dates, and domains.

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	default Domain Policy	No	Yes	Enabled	None	11/12/2003 4:03:40 PM	domain7.pr
2	GPO1	Yes	Yes	User configuration settings disabled	None	11/12/2003 3:58:38 PM	domain7.pr

GPO Tattooing:

GPO settings that modify the following four registry keys will revert back to defaults when the GPO falls out of the scope of management:

HKEY_LOCAL_MACHINE\Software\Policies

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

HKEY_CURRENT_USER\Software\Policies

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Changes outside of the above four registry keys will likely get 'tattooed' onto the target systems, and can only be put back at default settings by deploying a counter-GPO, or otherwise re-configuring the target systems.

Best approach? Test your GPO settings and their removals before production deployment! Also, third-party products like 'PolicyPak' can help.

For more info:

Google 'GPO tattoo'

Understanding Policy "Tattooing"

<http://gpoguy.com/whitepapers/understanding-policy-tattooing>

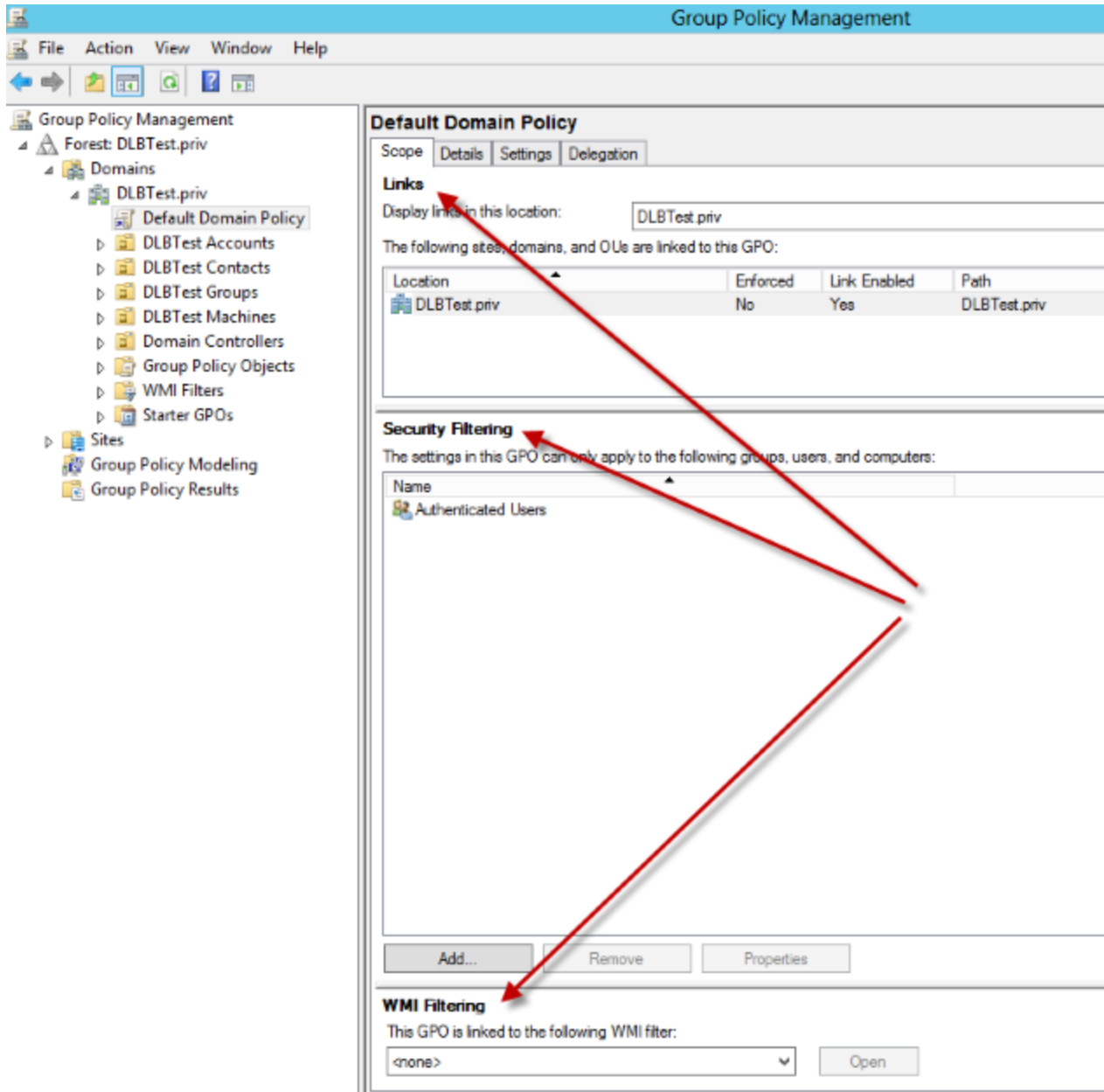
Jeremy Moskowitz, Group Policy MVP

Group Policy: Understanding ADM-ADMX files Tattooing (and what to do about it)

http://www.youtube.com/watch?v=bJHx_4A3AHo

GPO Scope:

Scope settings belong to a GPO, not just its link. I.e., modifying the scope of a GPO or a link to it will modify the scope of the GPO as well as all links to it.



A GPO's scope is set by three things:

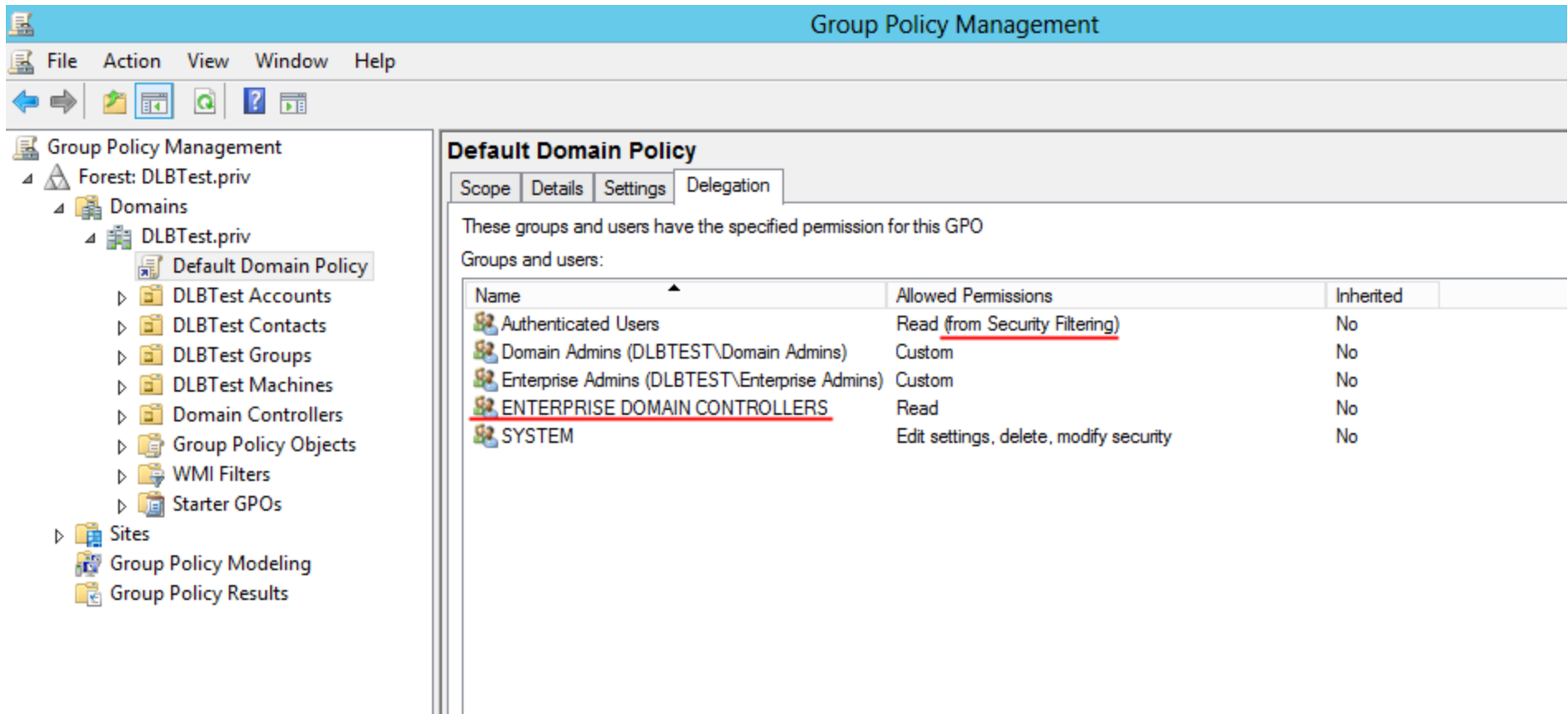
1. Links – To what OUs is the GPO linked?

2. Security Filtering – A GPO affects only those computer and/or user accounts that are within the Security Filter. 'Authenticated Users' is a misnomer because it really means 'Authenticated Users and Computers', or even 'Authenticated Objects.'

3. WMI Filtering - A GPO affects only those computer and/or user accounts that are within the WMI Filter.

GPO Delegation:

Who has rights to read and apply the GPO? Who has rights to edit the GPO?



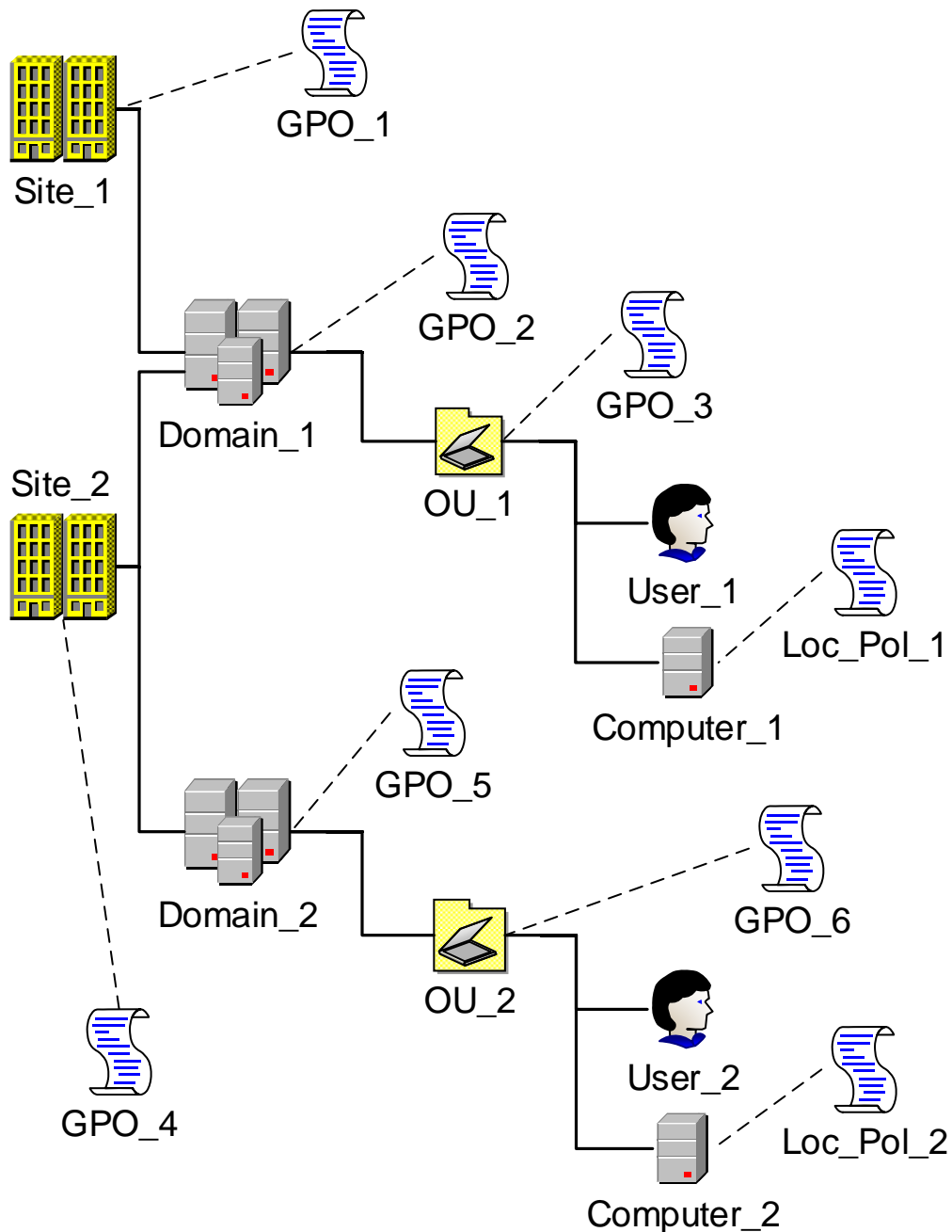
The screenshot shows the Group Policy Management console. The left pane displays the tree structure: Group Policy Management > Forest: DLBTest.priv > Domains > DLBTest.priv > Default Domain Policy. The right pane shows the 'Delegation' tab for the 'Default Domain Policy'. It lists groups and users with their allowed permissions and whether they are inherited.

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (DLBTEST\Domain Admins)	Custom	No
Enterprise Admins (DLBTEST\Enterprise Admins)	Custom	No
<u>ENTERPRISE DOMAIN CONTROLLERS</u>	Read	No
SYSTEM	Edit settings, delete, modify security	No

- Modifying the delegation settings of a GPO or a link to it will modify the delegation settings of the GPO as well as all links to it.
- Note how the 'Read' right is given to 'Authenticated Users' from the Security Filter.
- Note that 'Enterprise Domain Controllers' has the 'Read' right... If you create a new GPO that has this configuration item, it means that 'ADPrep.exe /DomainPrep /GPPrep' was run during an upgrade to 2008 R1 or higher.

Inheritance:

- Inheritance is the combining of GPOs to determine what GPO settings are available at a particular level of the Active Directory.
- Do not confuse Inheritance with Link Order, Processing Sequence, or Resultant Set Of Policy (RSOP).



4LSDOU

NT4 System Policy
 Local Policy
 Site GPO
 Domain GPO
 Organizational Unit GPO

1. If you have a Windows NT 4.0 client in a workgroup or a domain, the only policies that can apply are downlevel Windows NT 4.0 policy (POL) file policies.
2. If you have a standalone Windows 20XX client or server, policies are evaluated in the following order:
 - 2.1. downlevel Windows NT 4.0 policy (POL) file
 - 2.2. windows 20XX local GPO
3. If you have a Windows 20XX client or member server in a mixed-mode domain, policies are evaluated in the following order:
 - 3.1. downlevel Windows NT 4.0 policy (POL) file
 - 3.2. windows 20XX local GPO
 - 3.3. site GPO
 - 3.4. domain GPO
 - 3.5. organizational Unit GPOs in priority order, applied in a hierarchical fashion down the tree ending with the Organizational Unit that the computer or user resides in
4. If you have a Windows 20XX client or member server in a native-mode domain, policies are evaluated in LSDOU order.

Modifying Inheritance:



No Override / Enforce

The 'No Override' / 'Enforce' option can be set on a given **GPO link**.

- 'No Override' was the old term, 'Enforce' is the new term.
- The 'No Override' / 'Enforce' option is a function of a GPO link, not the GPO itself.
- The 'No Override' / 'Enforce' option prevents a lower level GPO from overriding conflicting settings from a higher level GPO.
- The 'No Override' / 'Enforce' option applies only to the Group Policy Object for which it is specifically set (i.e. the 'No Override' / 'Enforce' option is never passed to or from Group Policy Objects; it has to be hard set; it is not transitive).
- The Local GPO doesn't have a 'No Override' / 'Enforce' option, thus one cannot locally set options that can never be overridden by GPOs that reside at a higher level in the Active Directory.
- The 'No Override' / 'Enforce' option is stronger than the 'Block Policy Inheritance' option, thus 'No Override' / 'Enforce' beats 'Block Inheritance.'
- If two GPOs are in conflict, and both have 'No Override' / 'Enforce' set, then the GPO that was applied first will win (e.g. a Site 'No Override' / 'Enforce' GPO will win over a Domain 'No Override' / 'Enforce' GPO).

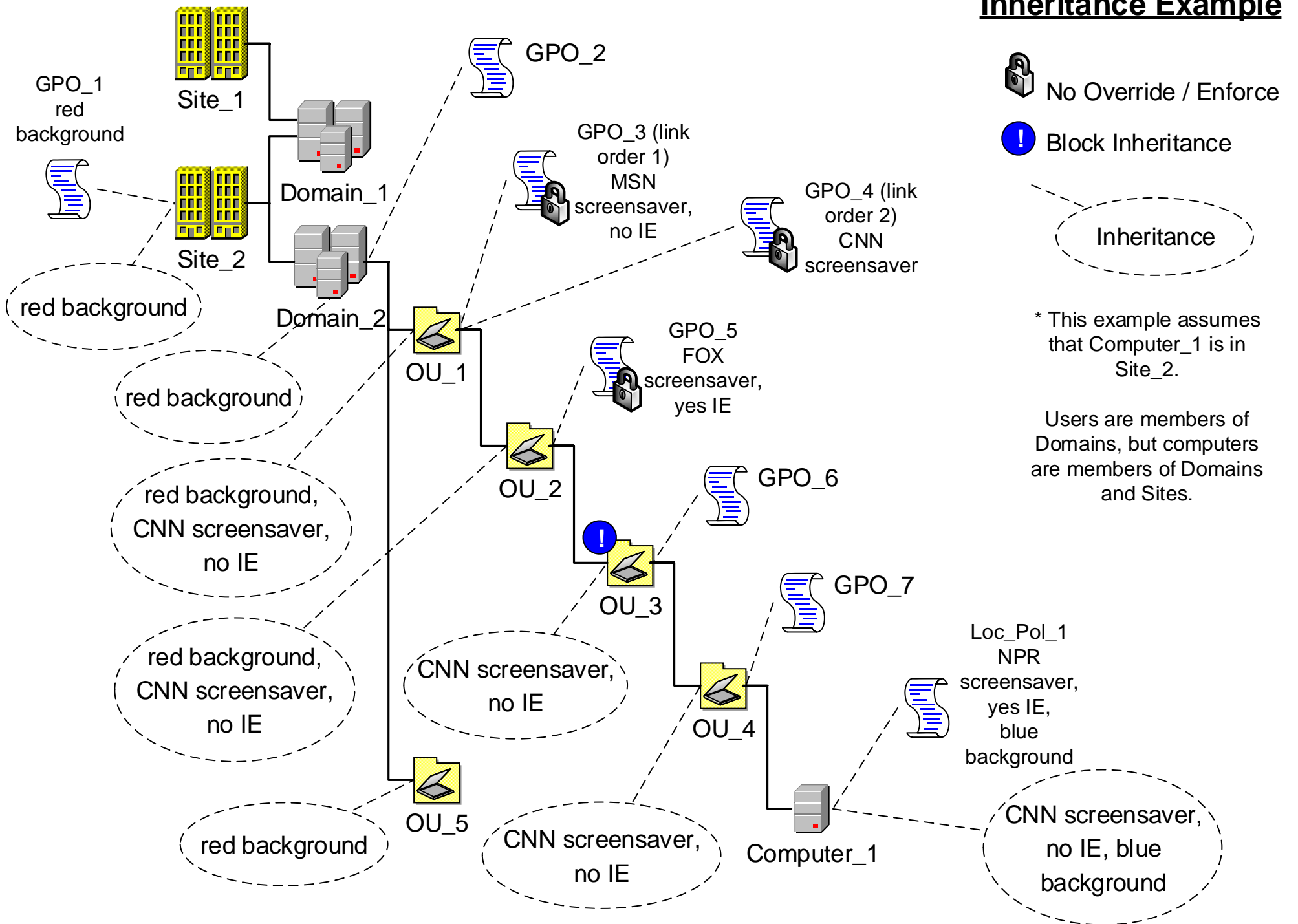


Block Inheritance

The 'Block Inheritance' option can be set on a given **OU**.

- The 'Block Policy Inheritance' option forces an OU to block policy inheritance from all parent AD objects.
- The 'Block Policy Inheritance' option applies only to the Group Policy Object for which it is specifically set (i.e. the 'Block Policy Inheritance' option is never passed to or from Group Policy Objects; it has to be hard set; it is not transitive).
- An OU will not inherit settings from a GPO linked to a grandparent (or great grandparent, etc.) if the OU's parent is blocking inheritance (i.e. a single 'Block Policy Inheritance' will break the inheritance chain).

Inheritance Example

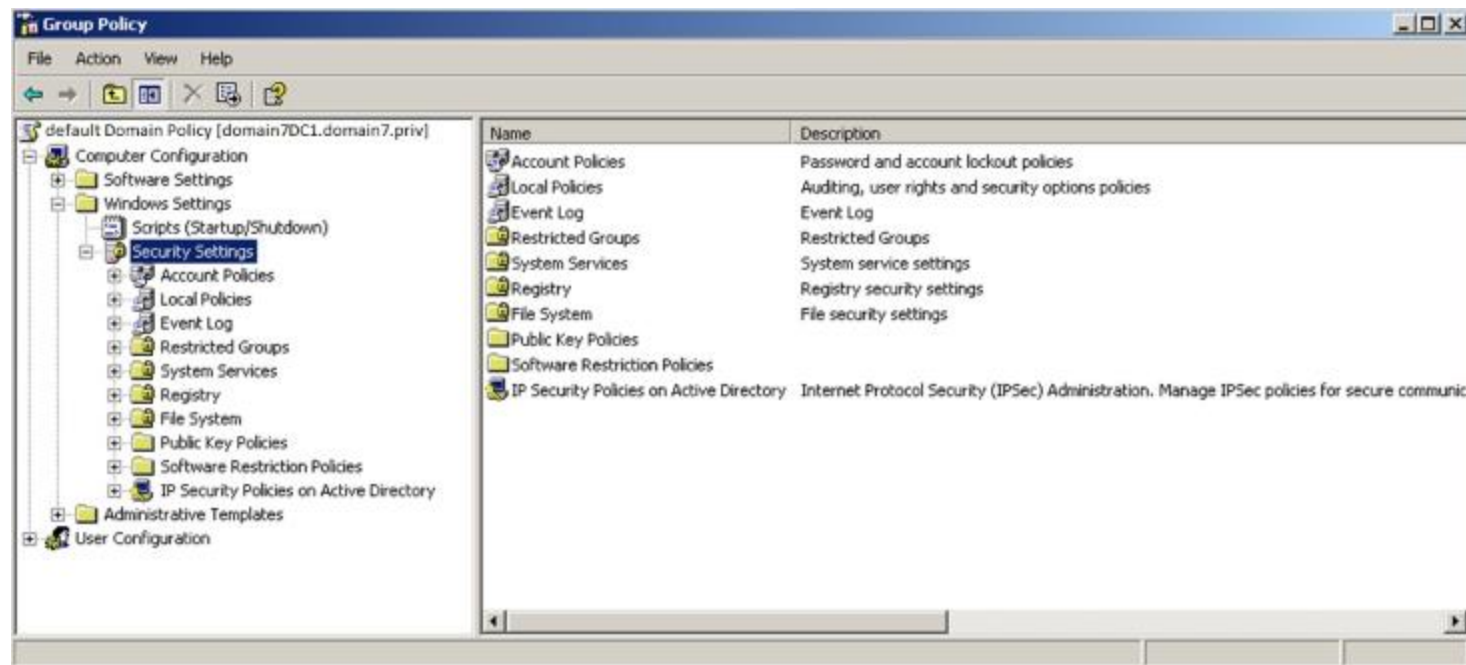


Domain-Wide Scope:

Of the security settings in a GPO, Account Policies and Public Key Policies have domain-wide scope. This means that Account Policies and Public Key Policies are determined by what is specified in the Domain-level GPOs regardless of any 'Enforced' / 'No Override' or 'Block Inheritance' settings that are set at the Site or OU levels. The reason is that the Domain is the basic security unit for a Microsoft based infrastructure, and the domain-wide scope of Account Policies and Public Key Policies ensures that these security settings are controlled at the Domain level, and not at any other level.

The exception is that Account Policy settings determined by inheritance at an OU level (not Domain-wide scope) are applied when users use computer-local accounts to log into the local computer.

([http://technet.microsoft.com/en-us/library/cc748850\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc748850(v=ws.10).aspx)).



I once saw an environment (2003 Rx Domain around 2010 or 2011) where a GPO set a password policy at the Domain level, and a second GPO set it on an OU that MS ADAM was configured to use, and that contained the MS ADAM servers. The OU was shielded by a 'Block Inheritance' somewhere in the OU path. When the password policy at the Domain level was set to 'enforced'/'no override', MS ADAM used the Domain policy, but when the Domain level GPO was not set to 'enforced'/'no override' MS ADAM used the policy set at the OU level. I didn't test this completely, but my preliminary analysis indicated that MS ADAM was looking at Account Policy settings determined by inheritance at the OU level, not Account Policies as determined by Domain-wide scope.

RSOP (Resultant Set Of Policy) Definition:

- Resultant Set Of Policy is the environment that is actually experienced when a particular user logs into a particular computer.
- Do not confuse RSOP with Link Order, Processing Sequence, or Inheritance.

RSOP.msc

Resultant Set of Policy is being processed...

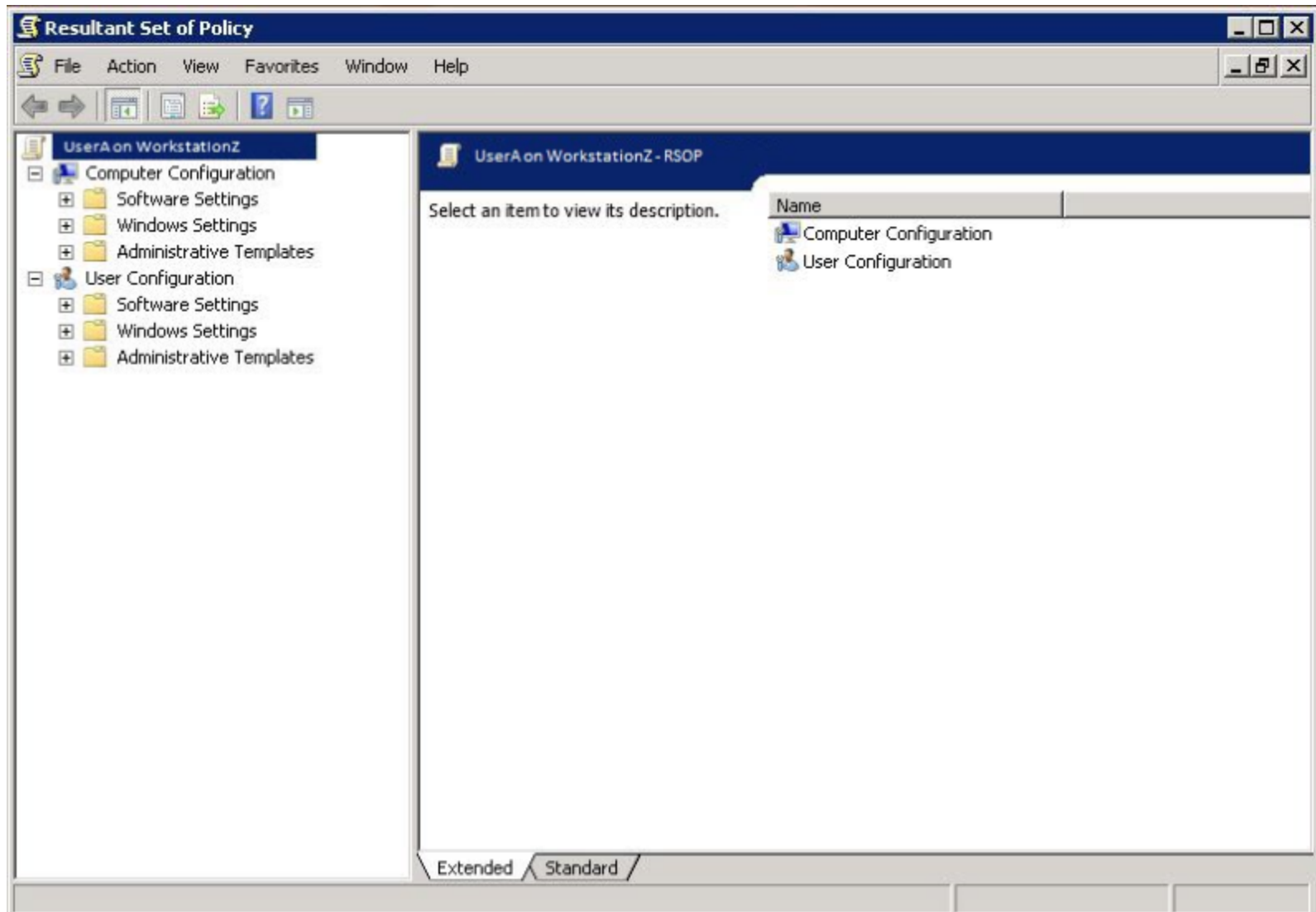
This Microsoft Management Console contains the RSoP snap-in defined below.



Starting with Microsoft Windows Vista Service Pack 1 (SP1), the Resultant Set of Policies (RSoP) report does not show all Microsoft Group Policy settings. To see the full set of Microsoft Group Policy settings applied for a computer or user, use the command-line tool gpresult.

Please wait while it is processed.

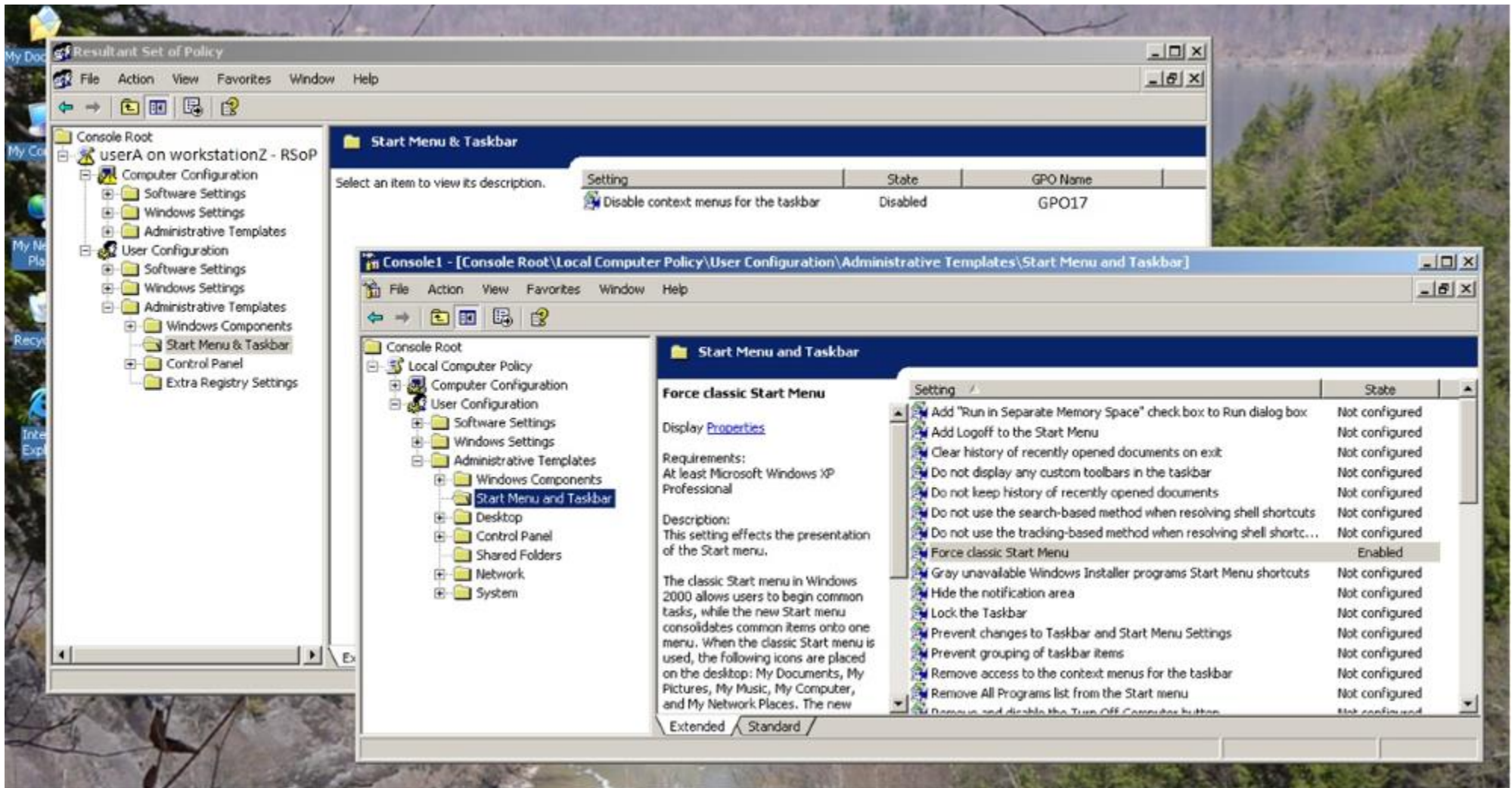
- RSOP.msc displays the Resultant Set Of Policy, but often shows incomplete information.
- GPRresult.exe, GP Modeling in GPMC.msc, and GP Result in GPMC.msc are better tools.



RSOP.msc, cont'd:

This slide shows what RSOP tells us (the background window) and what the Local Computer Policy is (foreground window, from GPEdit.msc).

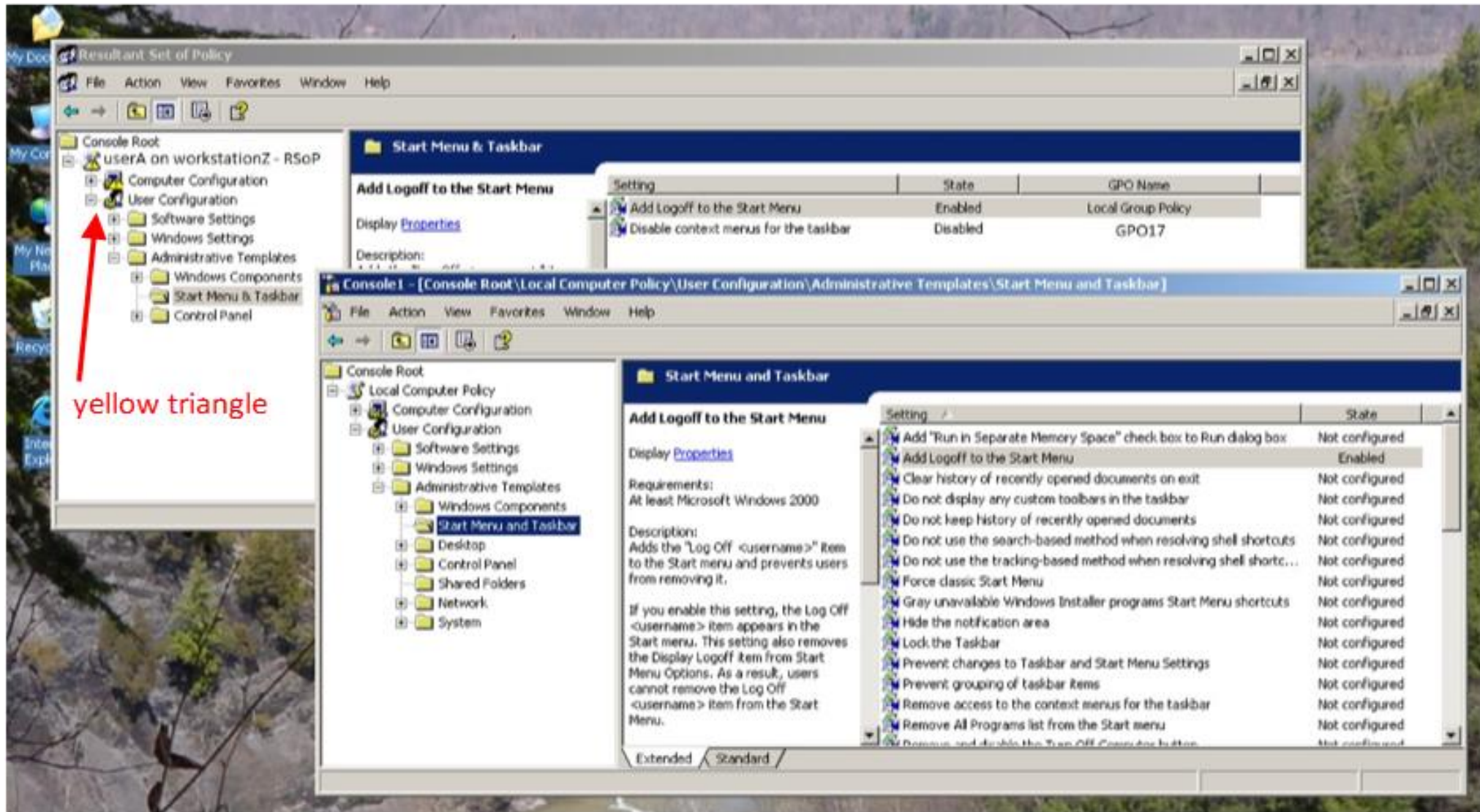
- RSOP.msc sometimes doesn't display all settings from the Local Computer Policy. For example, in this slide, in the foreground window, we see that 'Force classic Start Menu' is enabled by the Local Computer Policy, but that setting doesn't show up at all in RSOP, the background window, as being set by any Policy anywhere.
- RSOP gathers policies data from a Common Information Model Object Management (CIMOM) database on the local computer. Local Group Policy is not stored in this database and cannot be queried by RSOP. Gpedit.msc and secpol.msc just edits system settings directly. (<http://social.technet.microsoft.com/Forums/windowsserver/en-US/67c8d598-f61d-449a-a12b-a89a42251192/local-security-policies-do-no-show-up-in-rsop>)



RSOP.msc, cont'd:

This slide shows what RSOP tells us (the background window) and what the Local Computer Policy is (foreground window, from GPEdit.msc).

- If you see a yellow warning triangle or a red error X icon in RSOP.msc, right click on the computer configuration or user configuration and select properties. There should be an error tab that will show you what errors or warnings were encountered when applying group policy. Also look in the System and Application event logs.



GPRResult.exe:

```
C:\Windows\System32\cmd.exe

C:\>GPRResult /?

GPRESULT [/S system [/U username [/P [password]]] [/SCOPE scope]
[/USER targetusername] [/U | /Z]

Description:
  This command line tool displays the Resultant Set of Policy (RSOP)
  for a target user and computer.

Parameter List:
  /S      system          Specifies the remote system to connect
                        to.
  /U      Idomain\user    Specifies the user context under which
                        the command should execute.
  /P      [password]     Specifies the password for the given
                        user context. Prompts for input if omitted.
  /USER   Idomain\user    Specifies the user name for which the
                        RSOP data is to be displayed.
  /SCOPE  scope          Specifies whether the user or the
                        computer settings needs to be
                        displayed.
                        Valid values: "USER", "COMPUTER".
  /U      /U             Specifies that the verbose information
                        is to be displayed. Verbose information
                        details specific settings that have
                        been applied with a precedence of 1.
  /Z      /Z             Specifies that the super-verbose
                        information is to be displayed. Super-
                        verbose information details specific
                        settings that have been applied with a
                        precedence of 1 and higher. This allows
                        you to see if a setting was set in
                        multiple places. See the Group Policy
                        online help for more information.
  /?      /?             Displays this help/usage.

NOTE: If you run GPRESULT without parameters, it returns the RSOP data
      for the current logged-on user on the computer it was run on.

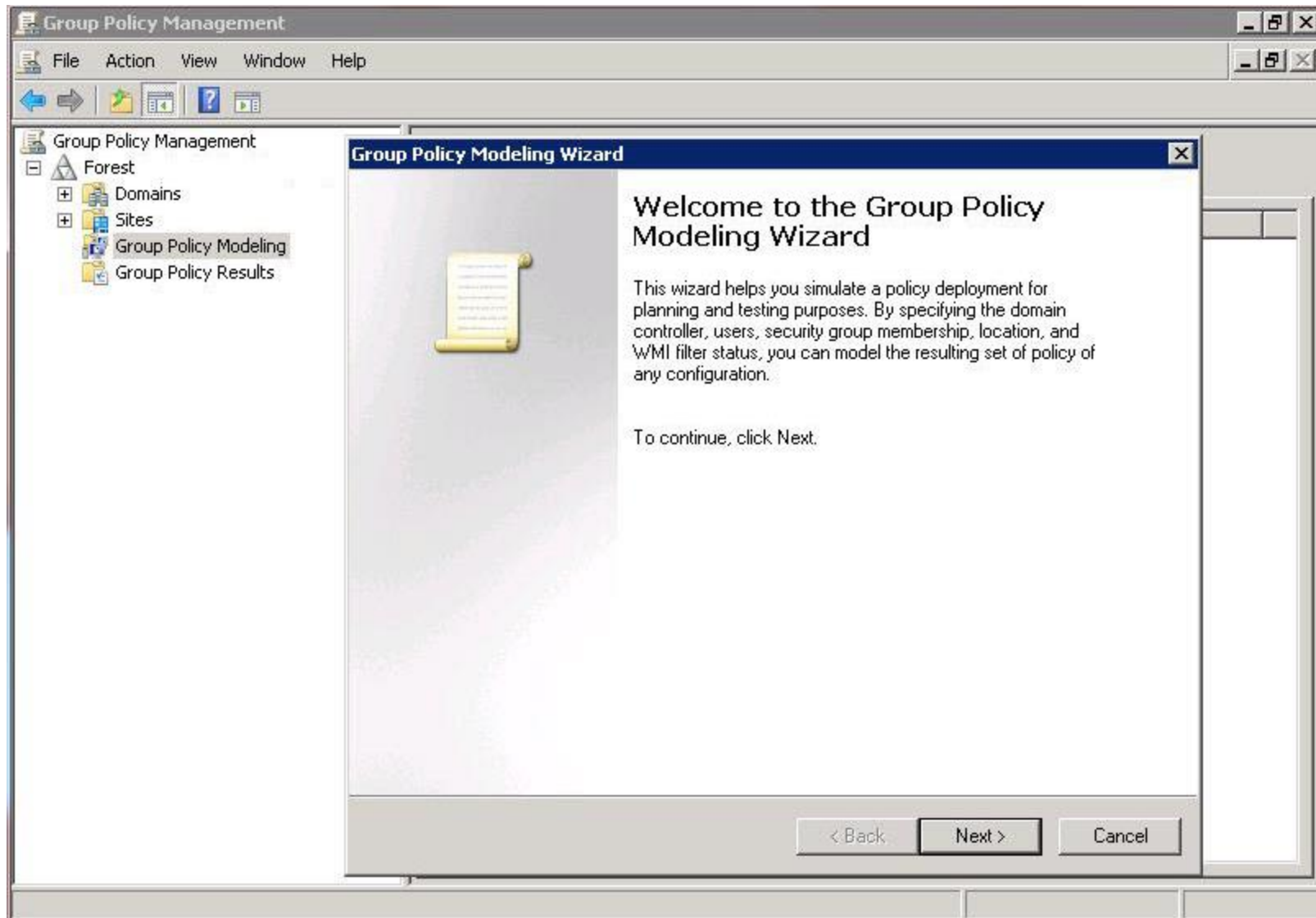
Examples:
  GPRESULT
  GPRESULT /USER targetusername /U
  GPRESULT /S system /USER targetusername /SCOPE COMPUTER /Z
  GPRESULT /S system /U username /P password /SCOPE USER /U

C:\>_
```

- GPRResult.exe is a command-line tool for troubleshooting the application of GPOs.
- GP Modeling in GPMC.msc, and GP Result in GPMC.msc are GUI tools for that same purpose.

GP Modeling (in GPMC.msc):

- This is a simulation done on the server (so it can be run when the target machine is offline).
- In contrast to Group Policy Modeling, Group Policy Results reveals the actual Group Policy settings that were applied to the destination computer. The target must be running Windows XP Professional or later.
- GPMC.msc can be loaded onto non-DC servers and workstations through RSAT (Remote Server Administration Tools).

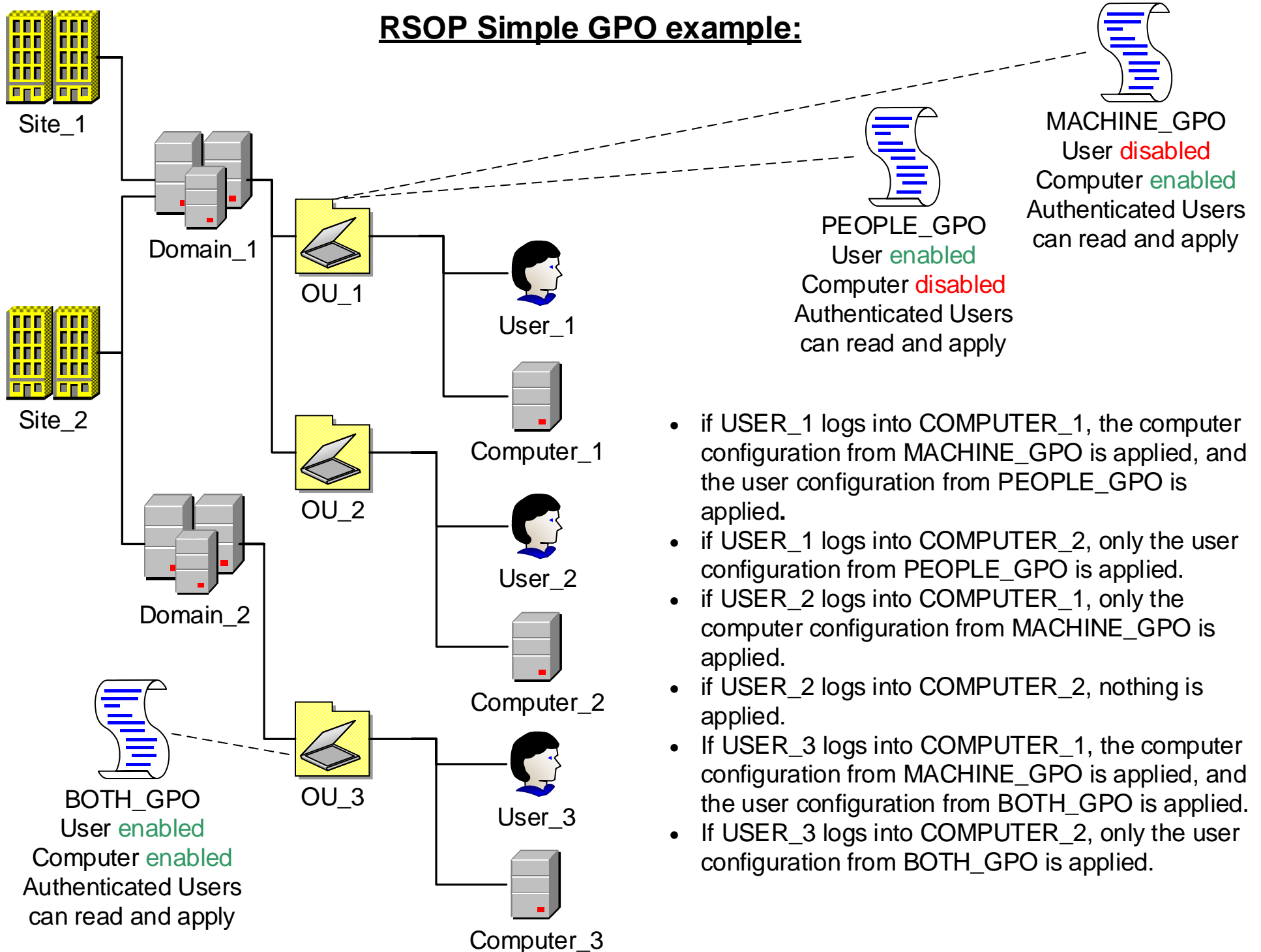


GP Results (in GPMC.msc):

- This is actual data from the target computer, not a simulation done on the server (so the target machine must be online).
- In contrast to Group Policy Modeling, Group Policy Results reveals the actual Group Policy settings that were applied to the destination computer. The target must be running Windows XP Professional or later.
- GPMC.msc can be loaded onto non-DC servers and workstations through RSAT (Remote Server Administration Tools).



RSOP Simple GPO example:



- if USER_1 logs into COMPUTER_1, the computer configuration from MACHINE_GPO is applied, and the user configuration from PEOPLE_GPO is applied.
- if USER_1 logs into COMPUTER_2, only the user configuration from PEOPLE_GPO is applied.
- if USER_2 logs into COMPUTER_1, only the computer configuration from MACHINE_GPO is applied.
- if USER_2 logs into COMPUTER_2, nothing is applied.
- If USER_3 logs into COMPUTER_1, the computer configuration from MACHINE_GPO is applied, and the user configuration from BOTH_GPO is applied.
- If USER_3 logs into COMPUTER_2, only the user configuration from BOTH_GPO is applied.

Loopback Settings:

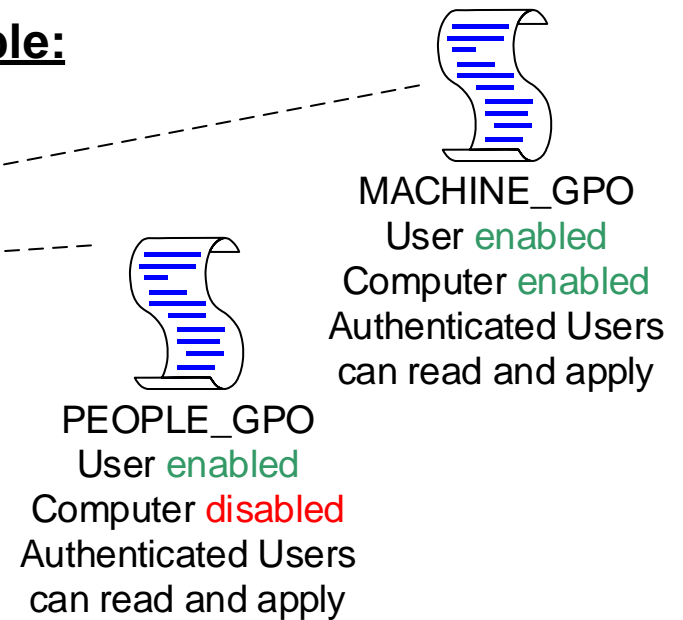
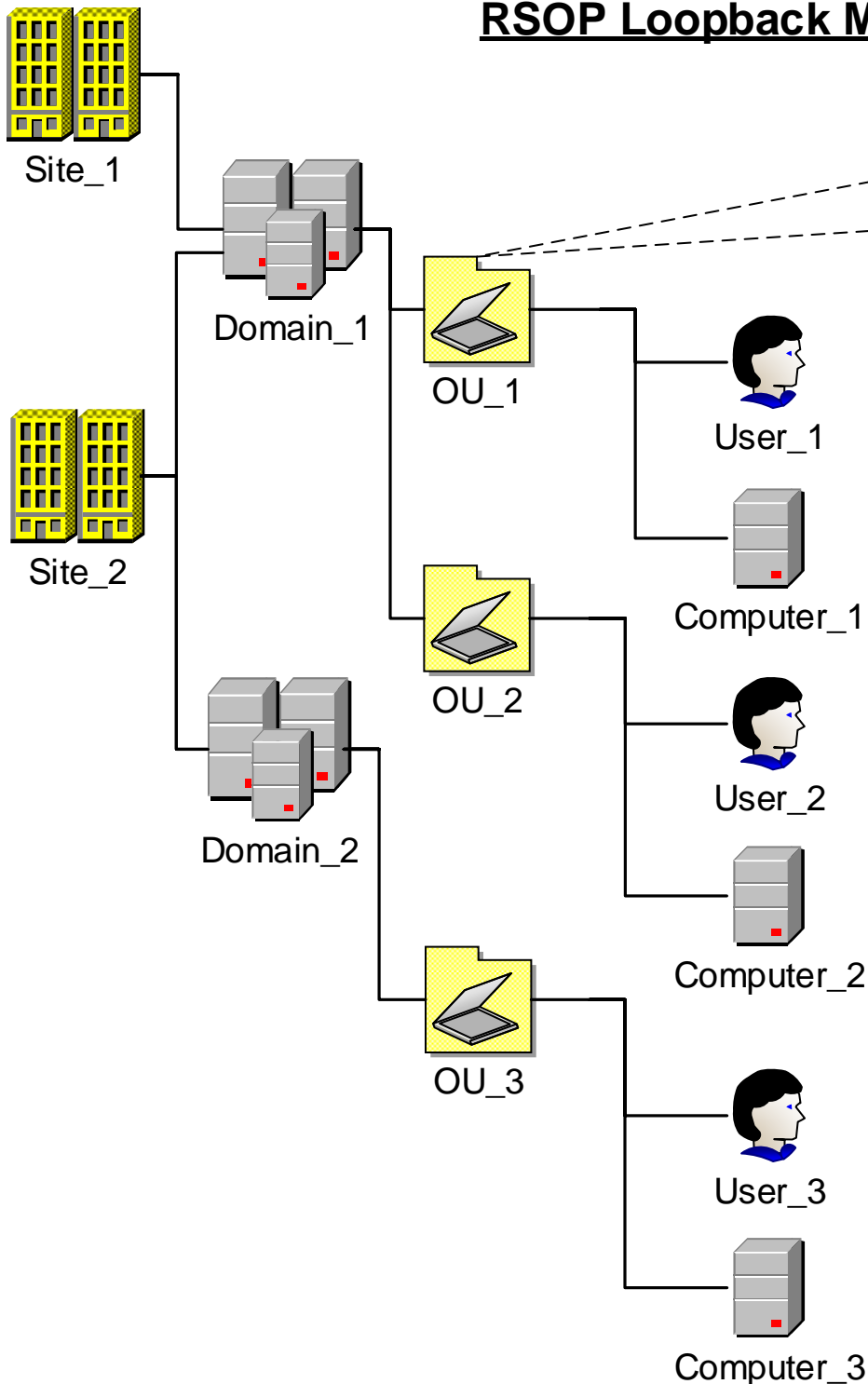
The screenshot displays the Group Policy console for a Group Policy Object (GPO) named 'GPO1'. The left pane shows the tree structure under 'Computer Configuration' > 'Administrative Templates' > 'System' > 'Group Policy'. The main pane shows the 'User Group Policy loopback processing mode' policy, which is currently set to 'Not configured'. A list of other policies is visible on the right, including 'Disable background refresh of Group Policy', 'Apply Group Policy for computers asynchronously during startup', 'Apply Group Policy for users asynchronously during logon', 'Group Policy refresh interval for computers', 'Group Policy refresh interval for domain controllers', 'Allow Cross-Forest User Policy and Roaming User Profiles', 'Group Policy slow link detection', 'Registry policy processing', 'Internet Explorer Maintenance policy processing', 'Software Installation policy processing', 'Folder Redirection policy processing', 'Scripts policy processing', 'Security policy processing', 'IP Security policy processing', 'EPS recovery policy processing', and 'Disk Quota policy processing'.

The 'User Group Policy loopback processing mode Properties' dialog box is open, showing the 'Setting' tab. It has three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. Below the radio buttons is a 'Mode' dropdown menu with three options: 'Replace' (selected), 'Merge', and 'Replace'. The dialog also includes 'Previous Setting', 'Next Setting', 'OK', 'Cancel', and 'Apply' buttons.

Setting	State
Disable background refresh of Group Policy	Not configured
Apply Group Policy for computers asynchronously during startup	Not configured
Apply Group Policy for users asynchronously during logon	Not configured
Group Policy refresh interval for computers	Enabled
Group Policy refresh interval for domain controllers	Not configured
User Group Policy loopback processing mode	Not configured
Allow Cross-Forest User Policy and Roaming User Profiles	Not configured
Group Policy slow link detection	Not configured
Registry policy processing	Not configured
Internet Explorer Maintenance policy processing	Not configured
Software Installation policy processing	Not configured
Folder Redirection policy processing	Not configured
Scripts policy processing	Not configured
Security policy processing	Not configured
IP Security policy processing	Not configured
EPS recovery policy processing	Not configured
Disk Quota policy processing	Not configured

- Loopback settings are only available in the 'Computer Configuration' portion of a GPO.
- Generally speaking, Loopback settings are for when you want the computer to dictate the RSOP instead of the user (think kiosks). Specifically speaking, loopback settings are for when you want the computer's GPOs to have more (or all) control over the user portion of RSOP than the user's GPOs.

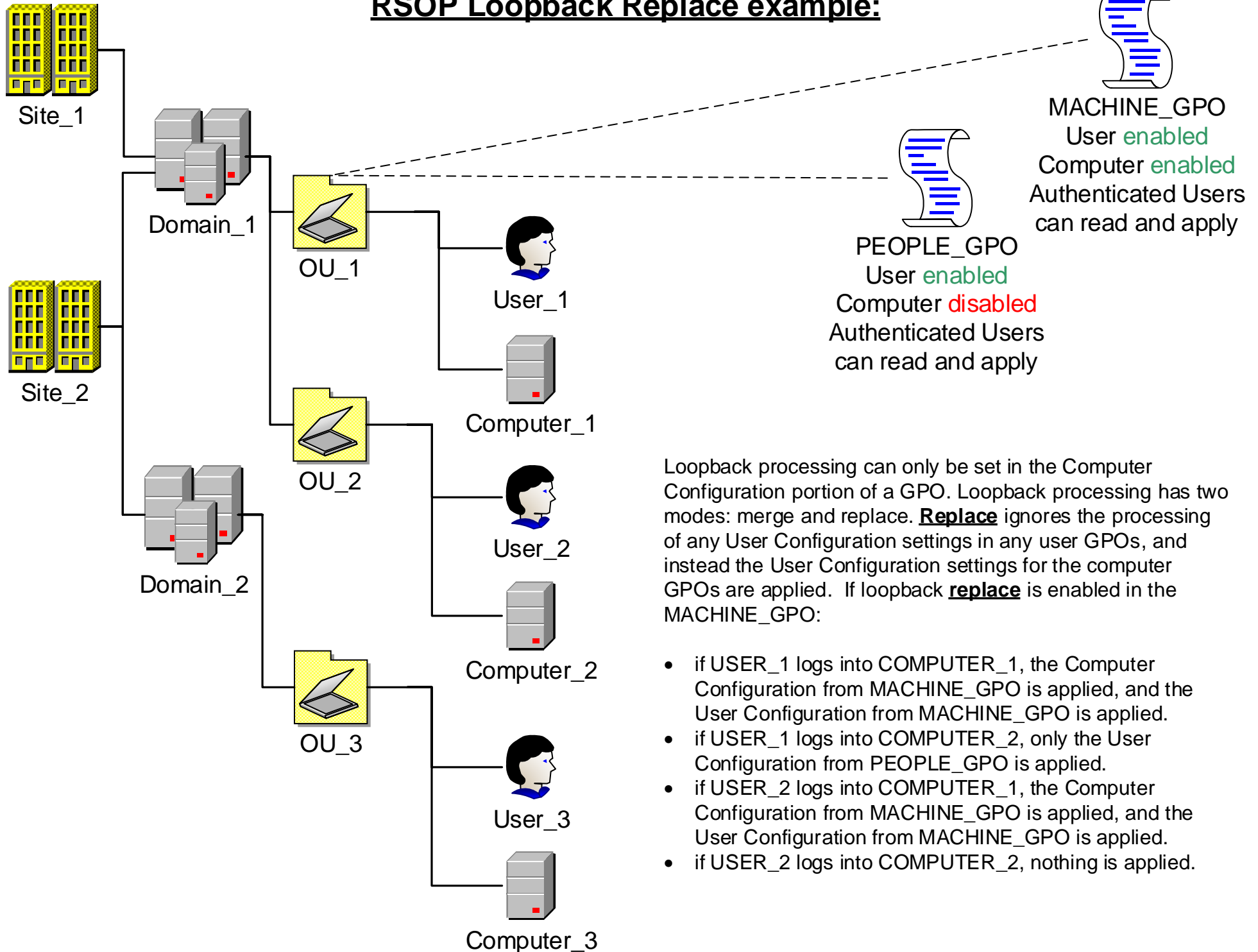
RSOP Loopback Merge example:



Loopback processing can only be set in the Computer Configuration portion of a GPO. Loopback processing has two modes: merge and replace. **Merge** means that the User Configuration portion of the computer's GPOs are applied after the normal application of the User Configuration portion of the user's GPOs. If loopback **merge** is enabled in the MACHINE_GPO:

- if USER_1 logs into COMPUTER_1, the Computer Configuration from MACHINE_GPO is applied, and the User Configuration from PEOPLE_GPO is applied, then the User Configuration from MACHINE_GPO is applied.
- if USER_1 logs into COMPUTER_2, only the User configuration from PEOPLE_GPO is applied.
- if USER_2 logs into COMPUTER_1, the Computer Configuration from MACHINE_GPO is applied, and the User Configuration from MACHINE_GPO is applied.
- if USER_2 logs into COMPUTER_2, nothing is applied.

RSOP Loopback Replace example:



Loopback processing can only be set in the Computer Configuration portion of a GPO. Loopback processing has two modes: merge and replace. **Replace** ignores the processing of any User Configuration settings in any user GPOs, and instead the User Configuration settings for the computer GPOs are applied. If loopback **replace** is enabled in the MACHINE_GPO:

- if USER_1 logs into COMPUTER_1, the Computer Configuration from MACHINE_GPO is applied, and the User Configuration from MACHINE_GPO is applied.
- if USER_1 logs into COMPUTER_2, only the User Configuration from PEOPLE_GPO is applied.
- if USER_2 logs into COMPUTER_1, the Computer Configuration from MACHINE_GPO is applied, and the User Configuration from MACHINE_GPO is applied.
- if USER_2 logs into COMPUTER_2, nothing is applied.

Security Policy Refresh Intervals:

Per KB article 277543:

In Windows 2000, Group Policy updates are dynamic and occur at specific intervals. If there have been no changes to Group Policy, the client computer still refreshes the security policy settings at regular intervals for the Group Policy object (GPO).

If no changes are discovered, GPOs are not processed, but security policies are. For security policies, there is a value that sets a maximum limit of how long a client can function without reapplying non-changed GPOs. By default, this setting is every 16 hours plus the randomized offset of up to 30 minutes. Even when GPOs that contain security policy settings do not change, the policy is reapplied every 16 hours and the following event is logged in the Application event log:

Event Type: Information

Event Source: SceCli

Event Category: None

Event ID: 1704

GPO Refresh Interval, Computer:

The screenshot shows the Group Policy console for GPO1. The left pane shows the tree structure with 'Computer Configuration' > 'Administrative Templates' > 'System' > 'Group Policy' selected. The main pane displays the 'Group Policy refresh interval for computers' setting, which is currently 'Not configured'. A description explains that this policy specifies a background update rate for Group Policies in the Computer Configuration folder. A table on the right lists various other Group Policy settings, all of which are currently 'Not configured'.

Setting	State
Disable background refresh of Group Policy	Not configured
Apply Group Policy for computers asynchronously during startup	Not configured
Apply Group Policy for users asynchronously during logon	Not configured
Group Policy refresh interval for computers	Not configured
Group Policy refresh interval for domain controllers	Not configured
User Group Policy loopback processing mode	Not configured
Allow Cross-Forest User Policy and Roaming User Profiles	Not configured
Group Policy slow link detection	Not configured
Registry policy processing	Not configured
Internet Explorer Maintenance policy processing	Not configured
Software Installation policy processing	Not configured
Folder Redirection policy processing	Not configured
Scripts policy processing	Not configured
Security policy processing	Not configured
IP Security policy processing	Not configured
EFS recovery policy processing	Not configured
Disk Quota policy processing	Not configured

GPO Refresh Interval, User:

The screenshot shows the Group Policy console with the following structure:

- GPO1
 - Computer Configuration
 - Software Settings
 - Windows Settings
 - Administrative Templates
 - Windows Components
 - System
 - Logon
 - Disk Quotas
 - DNS Client
 - Group Policy
 - Windows File Protection
 - Network
 - Printers
- User Configuration
 - Software Settings
 - Windows Settings
 - Administrative Templates
 - Windows Components
 - Start Menu & Taskbar
 - Desktop
 - Control Panel
 - Network
 - System
 - Logon/Logoff
 - Group Policy

The main pane displays the policy details for 'Group Policy refresh interval for users':

Group Policy refresh interval for users

Display [Properties](#)

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

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

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

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

Setting	State
Group Policy refresh interval for users	Not configured
Group Policy slow link detection	Not configured
Group Policy domain controller selection	Not configured
Create new Group Policy Object links disabled by default	Not configured
Enforce Show Policies Only	Not configured
Disable automatic update of ADM files	Not configured

Extended / Standard

GPUUpdate.exe:

```
C:\Windows\System32\cmd.exe

C:\>GPUupdate /?
Microsoft Windows Operating System Group Policy Refresh Utility v5.1
© Microsoft Corporation. All rights reserved.

Description: Refreshes Group Policies settings.

Syntax: GPUupdate [/Target:<Computer | User>] [/Force] [/Wait:<value>]
        [/Logoff] [/Boot] [/Sync]

Parameters:

Value          Description
/Target:<Computer | User> Specifies that only User or only Computer
                        policy settings are refreshed. By default,
                        both User and Computer policy settings are
                        refreshed.

/Force         Reapplies all policy settings. By default,
                only policy settings that have changed are
                applied.

/Wait:<value>  Sets the number of seconds to wait for policy
                processing to finish. The default is 600
                seconds. The value '0' means not to wait.
                The value '-1' means to wait indefinitely.
                When the time limit is exceeded, the command
                prompt returns, but policy processing
                continues.

/Logoff        Causes a logoff after the Group Policy settings
                have been refreshed. This is required for
                those Group Policy client-side extensions
                that do not process policy on a background
                refresh cycle but do process policy when a
                user logs on. Examples include user-targeted
                Software Installation and Folder Redirection.
                This option has no effect if there are no
                extensions called that require a logoff.

/Boot         Causes a reboot after the Group Policy settings
                are refreshed. This is required for those
                Group Policy client-side extensions that do
                not process policy on a background refresh cycle
                but do process policy at computer startup.
                Examples include computer-targeted Software
                Installation. This option has no effect if
                there are no extensions called that require
                a reboot.

/Sync         Causes the next foreground policy application to
                be done synchronously. Foreground policy
                applications occur at computer boot and user
                logon. You can specify this for the user,
                computer or both using the /Target parameter.
                The /Force and /Wait parameters will be ignored
                if specified.

C:\>_
```

SecEdit:

You can use SecEdit.exe with the /REFRESHPOLICY switch to impose group policy object settings upon a target workstation immediately as follows:

- SECEDIT /REFRESHPOLICY MACHINE_POLICY /ENFORCE: Immediately imposes group policy object settings located within the "machine" node of relevant group policy objects.
- SECEDIT /REFRESHPOLICY USER_POLICY /ENFORCE: Immediately imposes group policy object settings located within the "User" node of the relevant group policy objects.

NOTE: secedit /refreshpolicy only updates the Group Policy settings for the secedit client side extension. It will not refresh any other settings.

Terminal Services servers, Software Installation, and GPOs:

This slide shows how GPO-based software installation behaves on Terminal Servers.

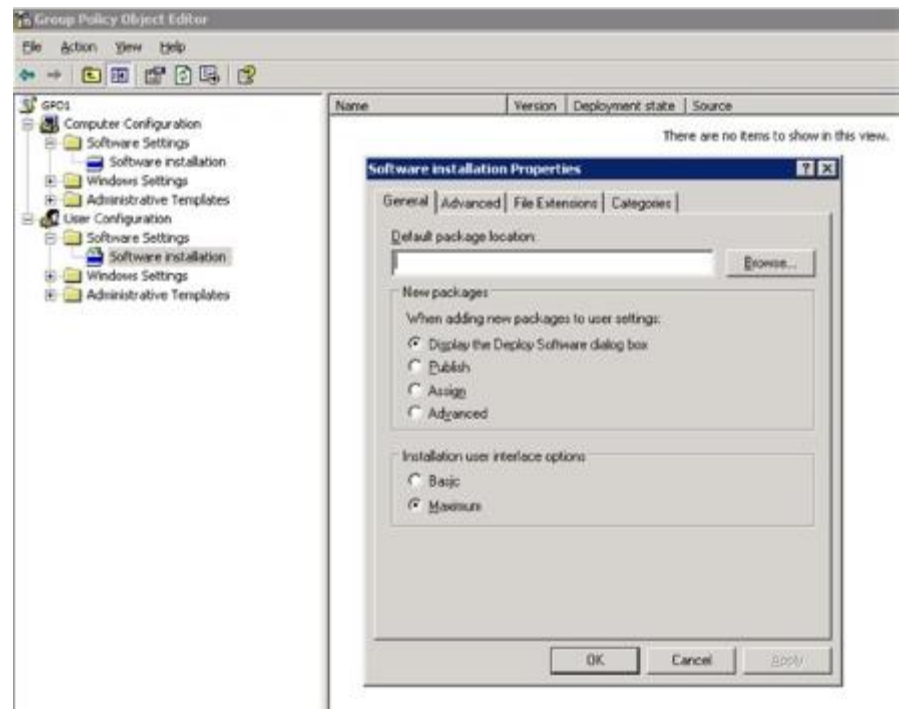
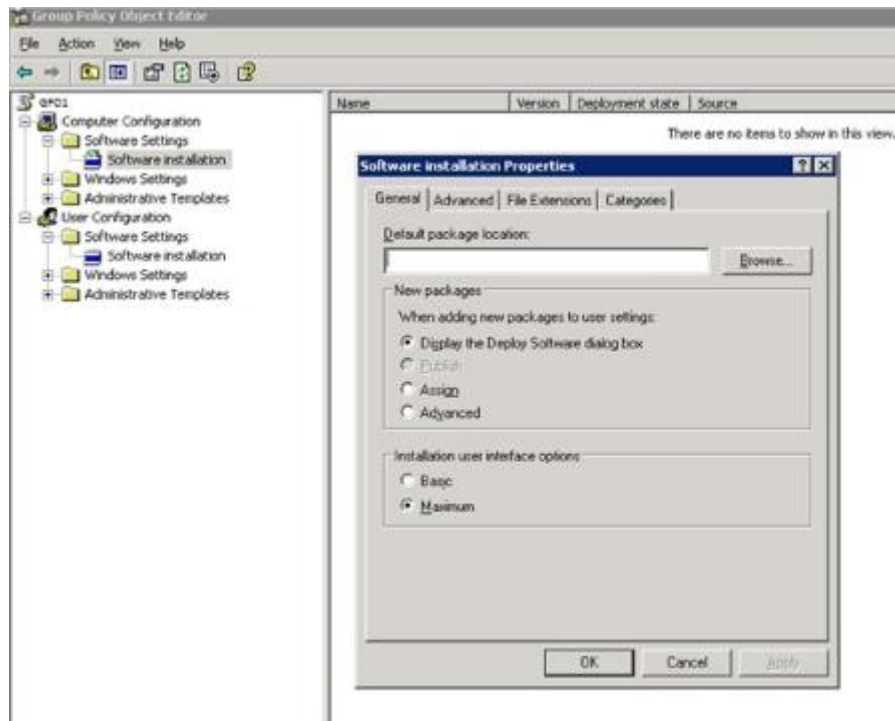
Windows 2000 Server

Chapter 23 - Software Installation and Maintenance

Table 23.12 shows when assigned and published software is supported on remote administration and application Terminal Services servers.

Table 23.12 Support for Managed Software on Terminal Services

Software Installation	Remote Administration	Application Server
User Assigned	Supported: Supported means that software installation and maintenance works in the same manner as it would on Windows 2000 Professional	Not applied, software is not installed.
Publish	Supported: Supported for both Windows Installer packages and existing setup programs defined in .zap files for publishing.	Not applied, software is not installed.
Computer Assigned	Supported	Supported: A domain user, with a roaming user profile might roam to an application server. Their application shortcuts follow them to the application server. If the server has the same application either installed (per computer) or assigned, and the user activates the shortcut, the shortcut works (either activating or installing the application). If the application is neither installed nor assigned, the shortcut does nothing.



GPO = GPC + GPT:

Group Policy Object

Group Policy Container (GPC)	Group Policy Template (GPT)
in Active Directory (<u>NTDS.dit</u>) transported by RPC	in sysVol transported by FRS / DFSR
The GPC contains referential meta-data. The GPC is responsible for keeping references to Client Side Extensions (CSEs are what actually apply the GPO settings on the target computer), the path to the GPT, paths to software installation packages, and other referential aspects of the GPO.	The GPT contains: <ul style="list-style-type: none">○ the <u>Administrative Templates</u> (.ADM, .ADMX, .ADML) for that <u>particular</u> GPO, which are the metadata / schema which delineate the available configuration changes that the GPO can perform○ the actual <u>values</u> for the configuration changes that the GPO actually enforces onto the target computers (including startup, logon, logoff, shutdown scripts)
Where is the GPC? in AD Users & Computers (must enable Advanced Features under the View PDM): Domain > System > Policies > GUID in <u>ADSIEdit.msc</u> : Domain partition > System > Policies > GUID	Where is the GPT? by the miracle of shortcutting: C:\Windows\SYSTEMVOLUME31\policies = C:\Windows\SYSTEMVOLUME31\sysvol\FQ name of Domain\policies = \\ServerName\sysvol\FQ name of Domain\policies = \\FQ name of Domain\sysvol\FQ name of Domain\policies

Note: An orphaned GPT is when a GPO gets deleted from AD but not sysVol.

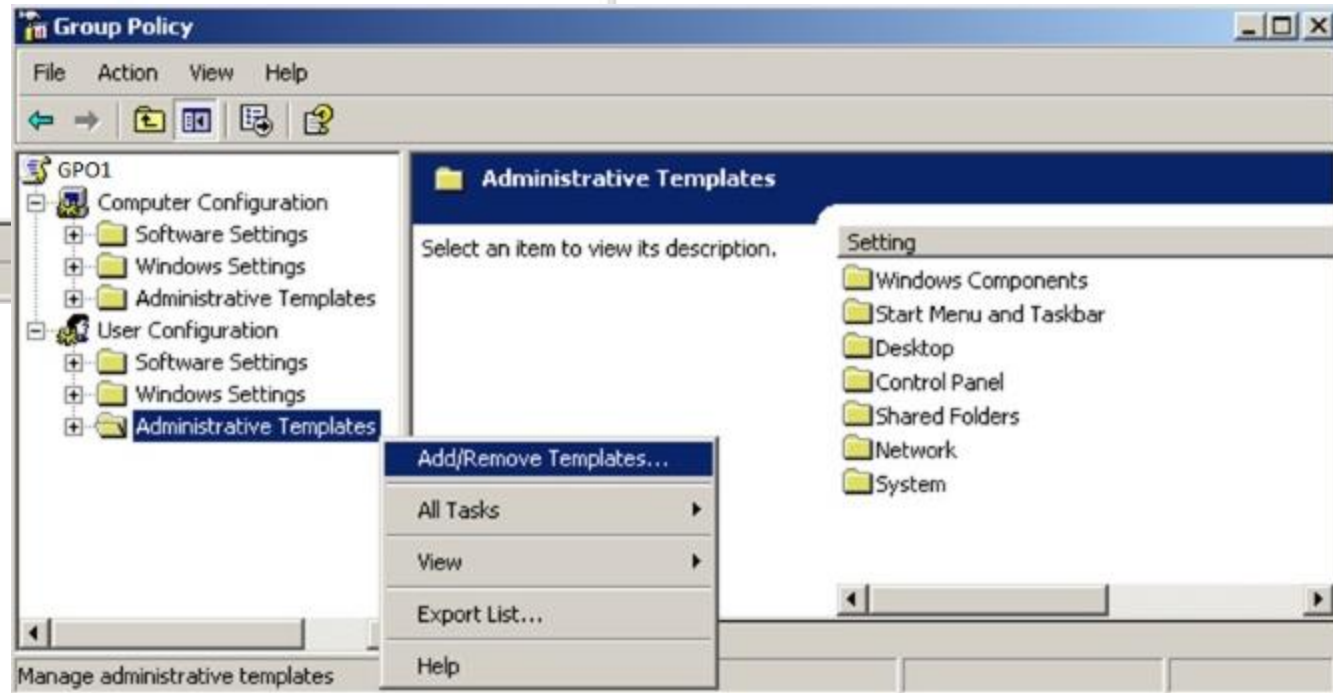
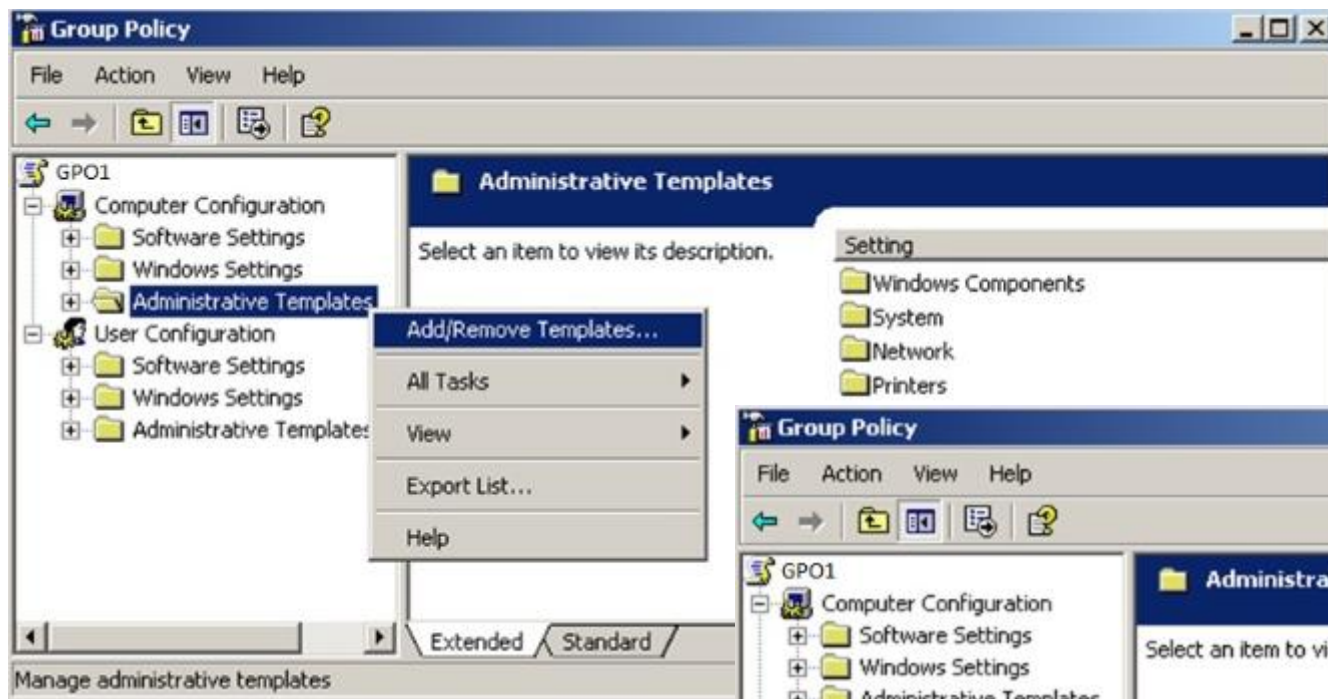
Subfolders of the Group Policy Template:

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

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

Administrative Templates:

- Administrative Templates are utilized when editing a GPO, not when applying it to target computers.
- To see all of the Administrative Templates that were used to edit a particular GPO, open both of the 'Administrative Templates' folders of that particular GPO.
- The screen-shots below show how to add/remove a new template to/from the Computer or User portion of a GPO (typically a template is added to one or the other, but not both). The new GPO options will then be available when editing the GPO.



Administrative Template Storage:

- Administrative Templates are .ADM, .ADMX, and .ADML files.
- Windows 2000 versions of Group Policy editors did some level of version control / currency updating of Administrative Templates. GPMC.msc does none of this.
- Prior to Windows Vista and 2008 the Administrative Templates used by a particular GPO were stored in that GPO's GPT (in its ADM folder), because they were copied there automatically when the GPO was created, or when templates were added through GPMC's 'Add/Remove Templates'.
- Windows Vista, 2008, and later can use a Central Store for .ADMX and .ADML files. To create a Central Store for .ADMX and .ADML files, create a folder that is named PolicyDefinitions in the following location: \\FQDN\SYSTEM\vol\FQDN\policies. The Group Policy tools of these newer OSs will use this folder.

Misc:

- To avoid edit/replication conflicts in sysVol (_NTFRS a.k.a. morphed folders) always point GPMC.msc to the PDC Emulator (open GPMC.msc, RC the domain, LC Change Domain Controller)
- It's best to store GPO controlled scripts (startup, logon, logoff, shutdown) on a central file server because it'll save space if more than one GPO uses each script, and the centralized location will be easier to manage and change-control.
- Create the Central Store for Administrative Templates (the 'PolicyDefinitions' folder).
- I've yet to find an authoritative source which describes how to best organize GPOs for speed, so I recommend that you make them as clean and simple as possible to facilitate their management, and thus reduce the likelihood of redundant, conflicting, and confusing settings. Computers and networks are so fast these days, just create your GPOs such that they're easy to administer and let the hardware bear the load. Also bear in mind that things like drive mapping and folder redirection will likely be slower to process (because of authentication) than local things like simple desktop settings.