Group Policy Preferences

By Archiveddocs

Archived: 2026-04-05 12:41:19 UTC

Group Policy Preferences is a collection of Group Policy client-side extensions that deliver preference settings to domain-joined computers running Microsoft Windows desktop and server operating systems. Preference settings are administrative configuration choices deployed to desktops and servers. Preference settings differ from policy settings because users have a choice to alter the administrative configuration. Policy settings administratively enforce setting, which restricts user choice.

Group Policy Preferences are distributed to domain-joined computers using the Group Policy. The flexibility of Group Policy enables it to deliver opaque configuration data to a domain-joined computer running Windows. The opaque data is then transferred to a Group Policy client side extension at which point the opaque data becomes relevant because the client-side extension understands the data.

This document describes how the Group Policy Drive Maps and Printers client-side extensions process their configuration data. With this knowledge, administrators can more effective design and deploy Group Policy Drive Map and Printer items in their environment. And, the information presented in this technical reference enables IT Professionals to troubleshoot Group Policy Drive Map and Printer processing.

Prerequisite Fundamentals

Group Policy

Group Policy is a management technology included in Windows Server that enables you to secure computer and user settings. Securing these settings ensures a common computing environment for users and lowers the total cost of ownership by restricting accidental or deliberate configurations that adversely affect the operating system.

A Group Policy object (GPO) is a logical object composed of two components, a Group Policy container and a Group Policy template. Windows stores both of these objects on domain controllers in the domain. The Group Policy container object is stored in the domain partition of Active Directory. The Group Policy template is a collection of files and folders stored on the system volume (SYSVOL) of each domain controller in the domain. Windows copies the container and template to all domain controllers in a domain. Active Directory replication copies the Group Policy container while the File Replication Service (FRS) or the Distributed File System Replication (DFSR) service copies the data on SYSVOL.

The Group Policy container and template together; make the logical object called a Group Policy object. Each Group Policy object contains two classes of configuration: user and computer. Computer configuration settings affect the computer as whole, regardless of the logged on user. User configuration settings affect the currently logged on user, and may vary with each user. Some examples of computers settings are power management, user

rights, and firewall settings. Examples of user settings include Internet Explorer, display settings, and Folder Redirection.

Group Policy objects and their settings apply to computers and user to which they are linked. You can link GPOs to an Active Directory site, domain, organizational unit, or nested organizational unit. Group Policy objects separate from the containers to which they are linked. This separation enables you to link a single GPO to multiple containers. Linking GPOs to many containers enables a single GPO to apply to users or computer within multiple container. This defines the scope of the GPO. Computer configurations apply to computers within the container or nested containers. User configurations apply to users in the same fashion.

Policy settings apply to computers at computer startup and to users during user logon. Windows Server 2012 and Windows 8 includes a Group Policy service. During computer startup, the Group Policy service queries Active Directory for the list of GPOs that are within scope (linked) of the computer object. Again, this includes:

- The site in which the computer resides
- The domain in which the computer is a member
- The parent organizational unit to which the computer is a direct member and any other organizational units above the parent OU.

The Group Policy service decides which GPOs apply to computers (there are many ways to filer GPOs from applying, which is beyond the scope of this introduction) and applies those policy settings. Client-side extensions (CSEs) are responsible for applying policy settings contained in the GPOs. A Group Policy client-side extension is a separate component from the Group Policy service that is responsible for reading specific policy setting data from the GPO and applying it to the computer or user. For example, the Group Policy registry client-side extension reads registry policy setting data from each GPO and then applies that information into the registry. The security CSE reads and applies security policy settings. The Folder Redirection CSE reads and applies Folder Redirection policy settings.

Group Policy processing repeats when the user logs on the computer. The Group Policy service decides the GPOs that apply to the user and then applies user policy settings.

It’s important that you have a firm understanding of how to create, modify, and link Group Policy objects to containers in Active Directory. Group Policy Preferences use the same concepts as Group Policy. In fact, you manage Group Policy Preferences the same way that you manage Group Policy. This is a review of Group Policy; it’s not complete. If you are unfamiliar with how to manage Group Policy or you need a thorough refresher, then you can read the Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista (Microsoft Press 2008).

Client-side Extensions

A Group Policy client-side extensions is an isolated component that is responsible for processing specific policy settings delivered by the Group Policy infrastructure. The format in which each Group Policy client-side extension saves data can be unique to each extension. And, the Group Policy infrastructure is unaware of this format, nor

does it care. Group Policy's purpose is to deliver settings to the computer where each client-side extension applies their portion of the policy settings from multiple Group Policy objects.

To help understand the relationship between the Group Policy infrastructure and the Group Policy client-side extensions-- consider a postal carrier. The postal carrier collects information from various sources and delivers that information to you. The postal carrier has no idea what information they are delivering. The information could be a letter, a DVD, or a CD with photos. The postal carrier only knows they are to deliver the information to a specific address.

In this analogy, the Group Policy service is the postal carrier-- it delivers the information without out any knowledge about the information. The information delivered by the postal carrier represents the different policy settings. The Group Policy client-side extension represents the person receiving the information. Addresses can have many recipients. Each recipient receives their own mail in an expected format. The Group Policy client side extension reads its respective policy setting information and performs actions based on information contains in the policy settings.

Group Policy Processing

Group Policy application is the process of deciding which Group Policy objects that Windows applies to a user or computer and then applying those settings. Understanding Group Policy processing is key to planning and deploying Group Policy settings. Misunderstanding Group Policy processing is the most common cause of unwanted and unexplainable policy settings.

The key to understanding Group Policy processing is Scope. **Scope** is simply a collection of all Group Policy objects that should apply to a user or computer based on their object's location in Active Directory. You create scope by **linking** Group Policy objects to specific locations within Active Directory.

The key to understanding Group Policy processing is Scope. **Scope** is simply a collection of all Group Policy objects that should apply to a user or computer based on their object's location in Active Directory. You create scope by **linking** Group Policy objects to specific locations within Active Directory.

Group Policy provides options that can change the scope of Group Policy object. Changing the scope of Group Policy objects affects which policy settings apply and those that do not. You change the scope of Group Policy using **processing order**, **filtering**, and **link options**.

Scope

Group Policy processing must identity the scope to which it is applying policy settings. Scope is simply states as where the user or computer object resides within the Active Directory hierarchy. The easiest way to discover the scope of a user or computer object is to lookup the respective user or computer's distinguished name in Active Directory. An object's distinguished name in a directory provides the objects identity and the objects location within the directory. Consider the following distinguished name.

```
CN=Kim Akers,OU=Human Resources, DC=corp,DC=contoso,DC=com
```

From this, the Group Policy service determines the name of the user object, the organizational unit that contains the user object, and the domain in which the user object resides.

```
CN=Jeff Low,OU=Managers,OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
```

Linking

Understanding Group Policy scope requires knowing where to link Group Policy objects so they apply to users or computer. To enable a Group Policy object to apply to a user or computer, you associate it with a specific location within Active Directory. Associating a Group Policy object with an object in Active Directory is called linking.

Active Directory has rules that govern where you can link Group Policy objects. Active Directory objects to which you can link Group Policy objects include:

- Site objects
- Domain objects
- Organizational Unit objects

Linking Group Policy objects to these Active Directory objects is strategic in deploying Group Policy. These are container objects. Container objects, as the name implies, means they can include other objects within them-- they representing hierarchical grouping of objects in a directory. Site objects can contain computer objects from multiple domains. Domain objects can contain multiple Organizational Units, computers and user objects. Organizational Unit objects can contain other Organizational Unit objects, computers, and users. Let's look at the distinguished name again.

```
CN=Jeff Low,OU=Managers,OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
```

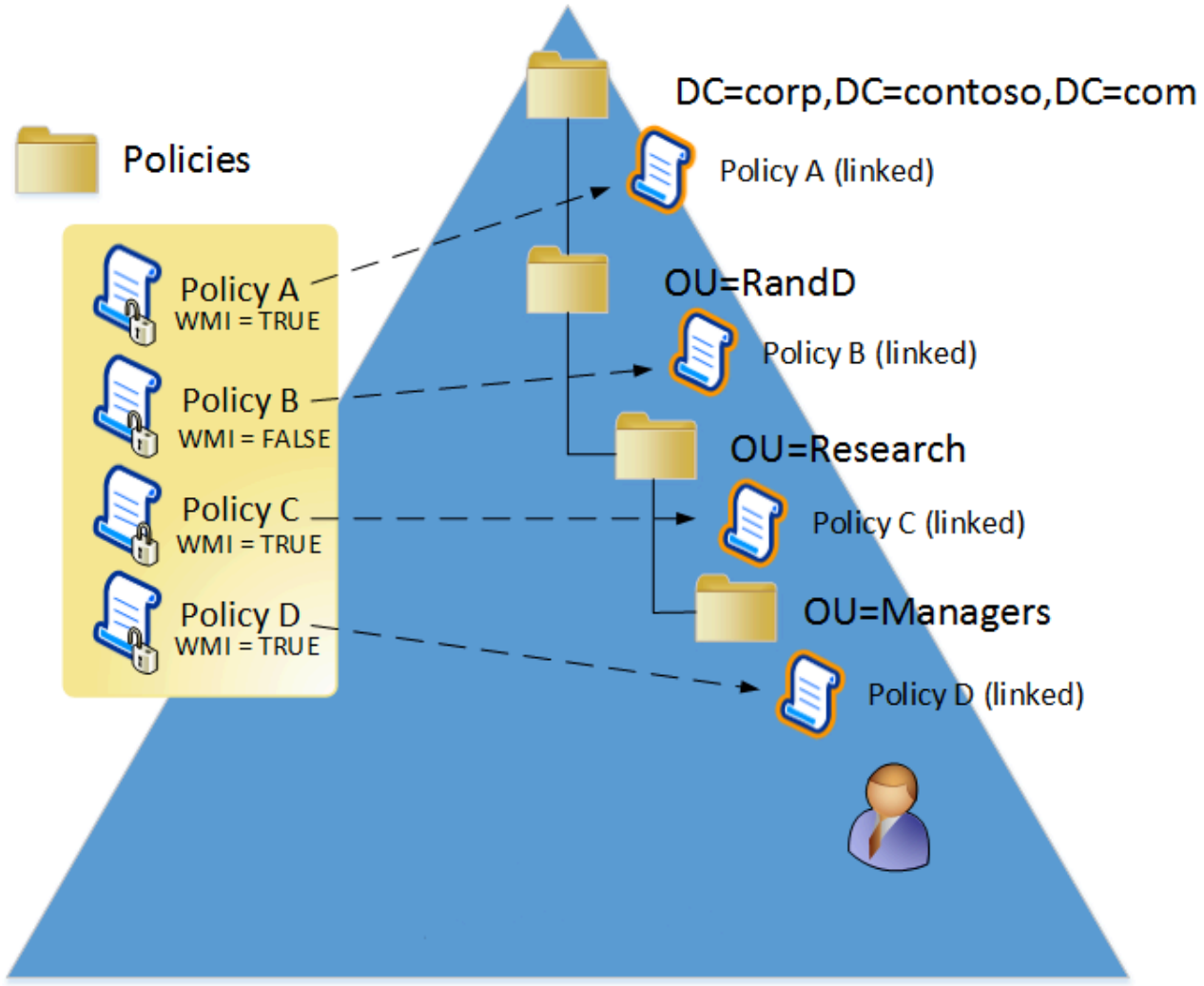
Close examination of the distinguished name reveals each container object that could potentially apply Group Policy settings to the user. The CN=Jeff Low is the user object name. You cannot link Group Policy directly to a user object. However, the remaining portion of the name shows the object’s location. Working left to right, you can discover each container object that is capable of apply Group Policy to the user.

```
 OU=Managers,OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
OU=RandD,DC=corp,DC=contoso,DC=com
DC=corp,DC=contoso,DC=com
```

Each of these locations represent the scope of Group Policy. The Group Policy service collects linked Group Policy objects from each of these locations in the directory. This represents the scope of Group Policy for the user or computer.

Notice the order in which Windows collects the list of Group Policy objects? It begins with the OU closest to the user and traverses up the directory to the object furthest away from the user, which is typically the domain object.

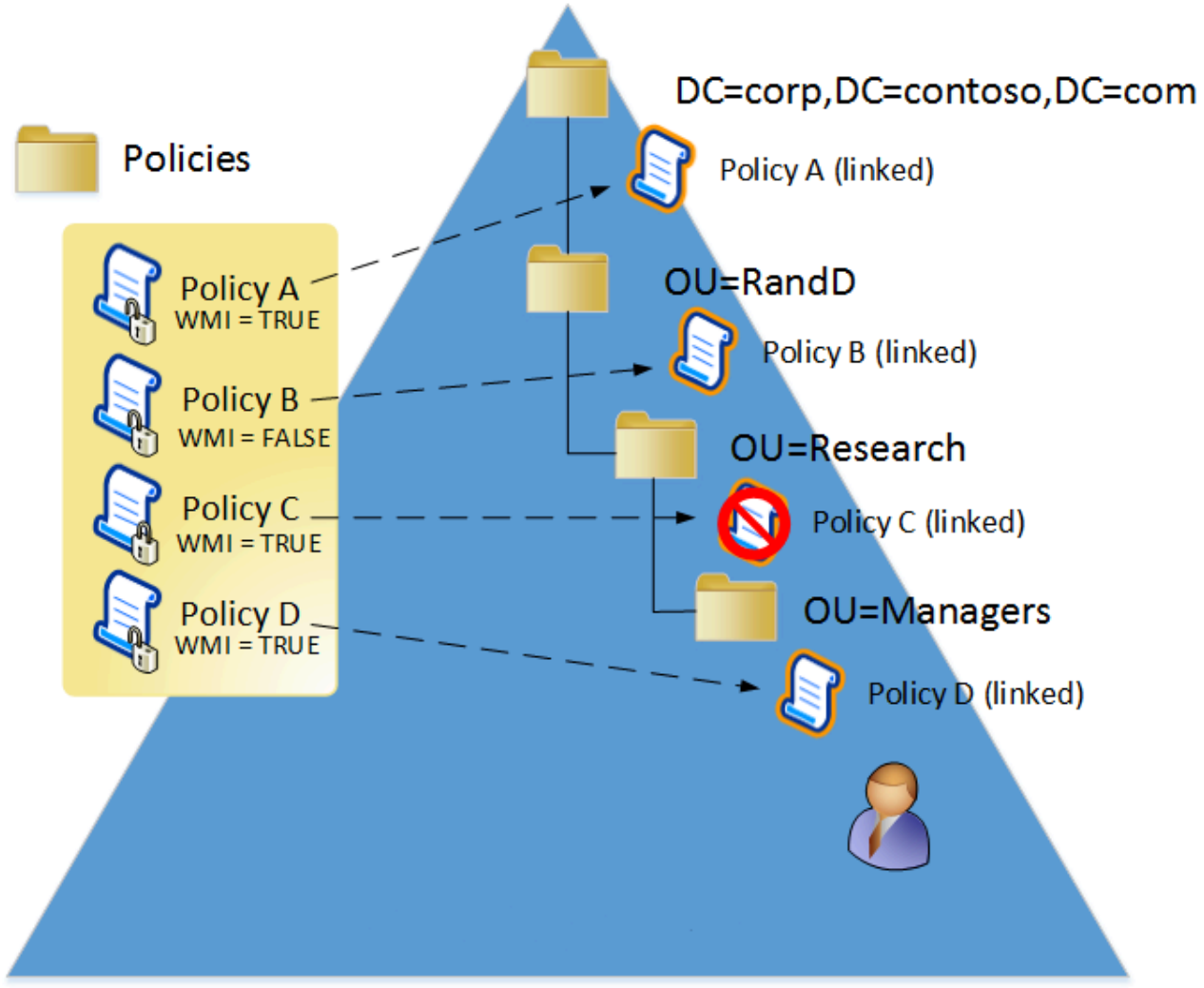
Through linking, you have a list of Group Policy objects that are in scope with the user or computer. However, not every GPO in the list should apply to the user or computer.



Security Filtering

Group Policy scope is the list of all Group Policy objects that may be applicable to the user or computer because of their object's location within Active Directory. Security Filtering determines if the respective user or computer has the proper permissions to apply the Group Policy object. A user or computer must have the **Read** and **Apply Group Policy** permissions for the Group Policy service to consider the Group Policy object applicable to the user.

The Group Policy services iterates through the entire list of Group Policy objects determining if the user or computer has the proper permissions to the GPO. If the user or computer has the permissions to apply the GPO, then the Group Policy service moves that GPO into a filtered list of GPOs. It continues to filter each Group Policy object based on permissions until it reaches the end of the list. The filtered list of Group Policy objects contains all GPOs within scope of the user or computer and are applicable to the user or computer based on permissions.



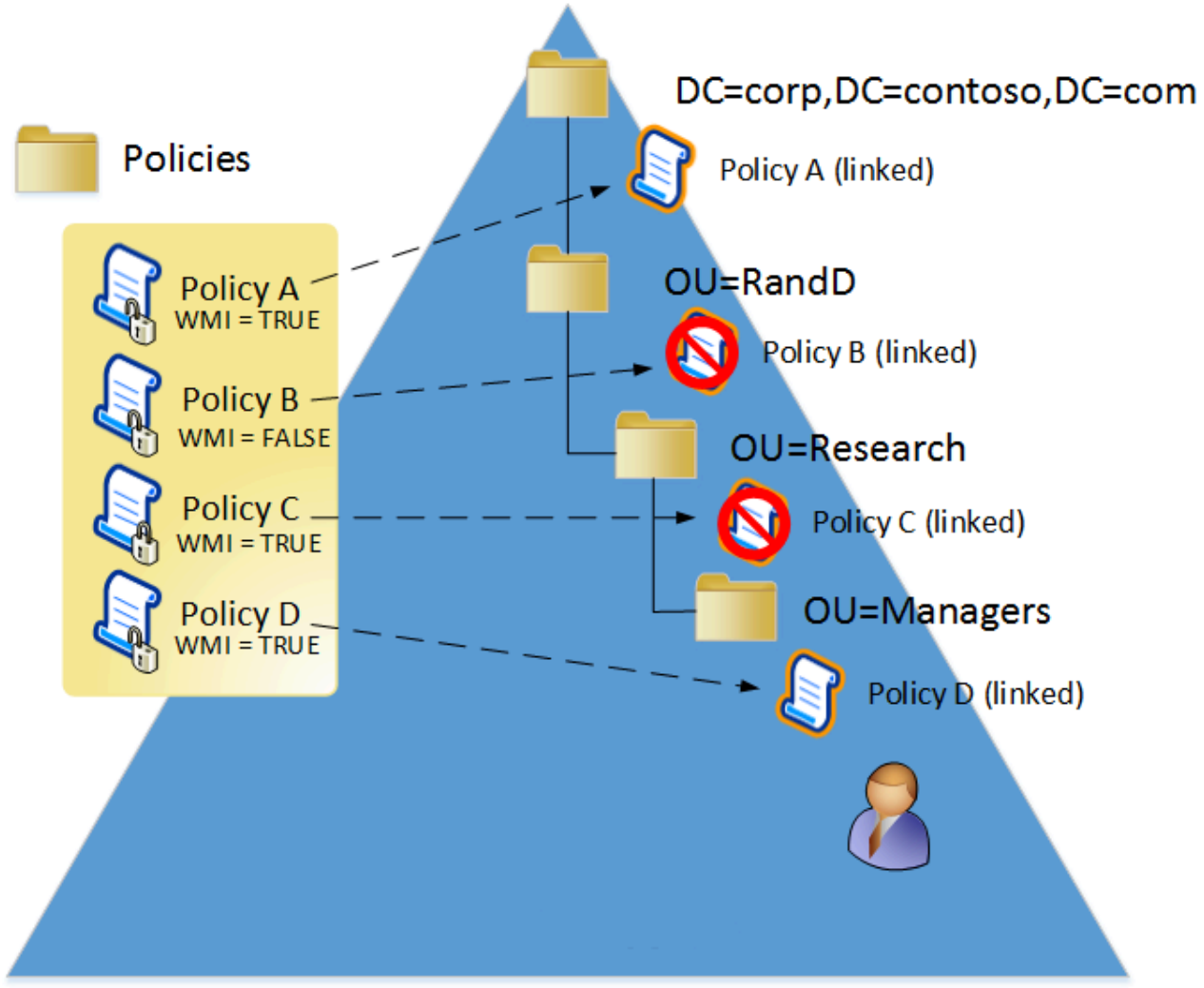
WMI Filtering

WMI filtering is the final phase of determining the scope of Group Policy objects that apply to a user or computer.

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM). WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

Group Policy provides more filters to control the scope of applicable Group Policy objects. WMI enables you to create queries to interrogate specific features of the computer, operating system, and other managed components. In the form of queries, you create criteria that behave like logical expressions-- where the result equates to true or false. You associated, or link these criteria to a Group Policy object. If the criteria evaluates to true, the Group Policy object remains applicable to the user and is kept in the filtered list. If the criteria evaluates to false, the Group Policy service removes the Group Policy object from the filtered list.

Once WMI filtering completes, the Group Policy service has a list of filter Group Policy objects. This final list represents all applicable Group Policy objects for the user or computer. Internally, Security and WMI filtering occur in one cycle.



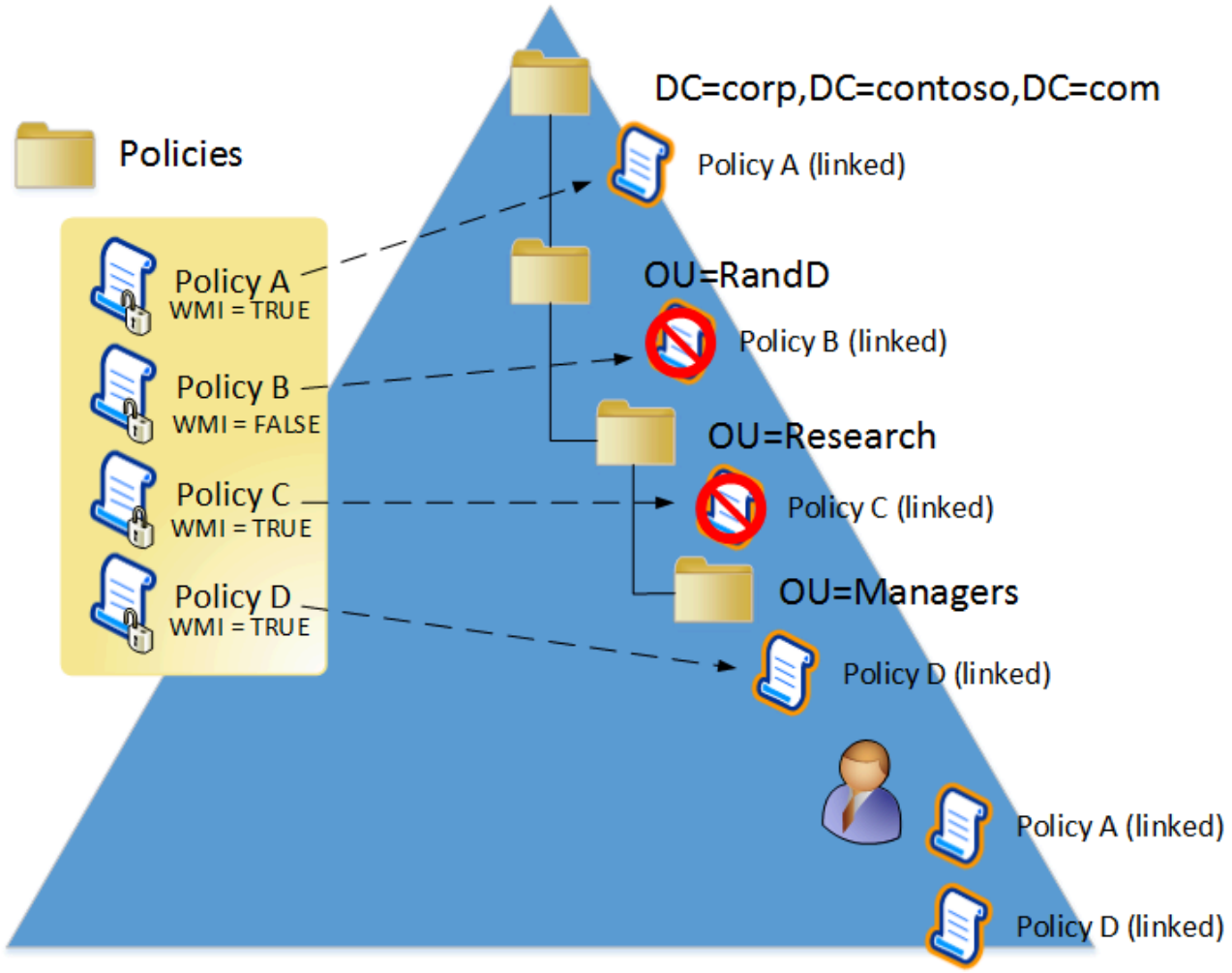
Processing Order

Group Policy has a specific order in which it applies Group Policy objects. Understanding the order in which Group Policy objects apply is important because Group Policy uses the order of application to resolve conflicting policy settings among different Group Policy objects linked to different locations within Active Directory.

Local, Site, Domain, and OU

The Group Policy service applies the Local Group Policy first, then Group Policy objects from the Site, followed by Group Policy objects from the domain, and Group Policy objects from organization units. If the targeted user or computer to receive Group Policy settings, then the Group Policy service applies Group Policy objects from OUs furthest in lineage from the user to closest in lineage to the user. Consider the filtered list of applicable Group Policy objects.

```
 DC=corp,DC=contoso,DC=com
OU=RandD,DC=corp,DC=contoso,DC=com
OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
OU=Managers,OU=Research,OU=RandD,DC=corp,DC=contoso,DC=com
```



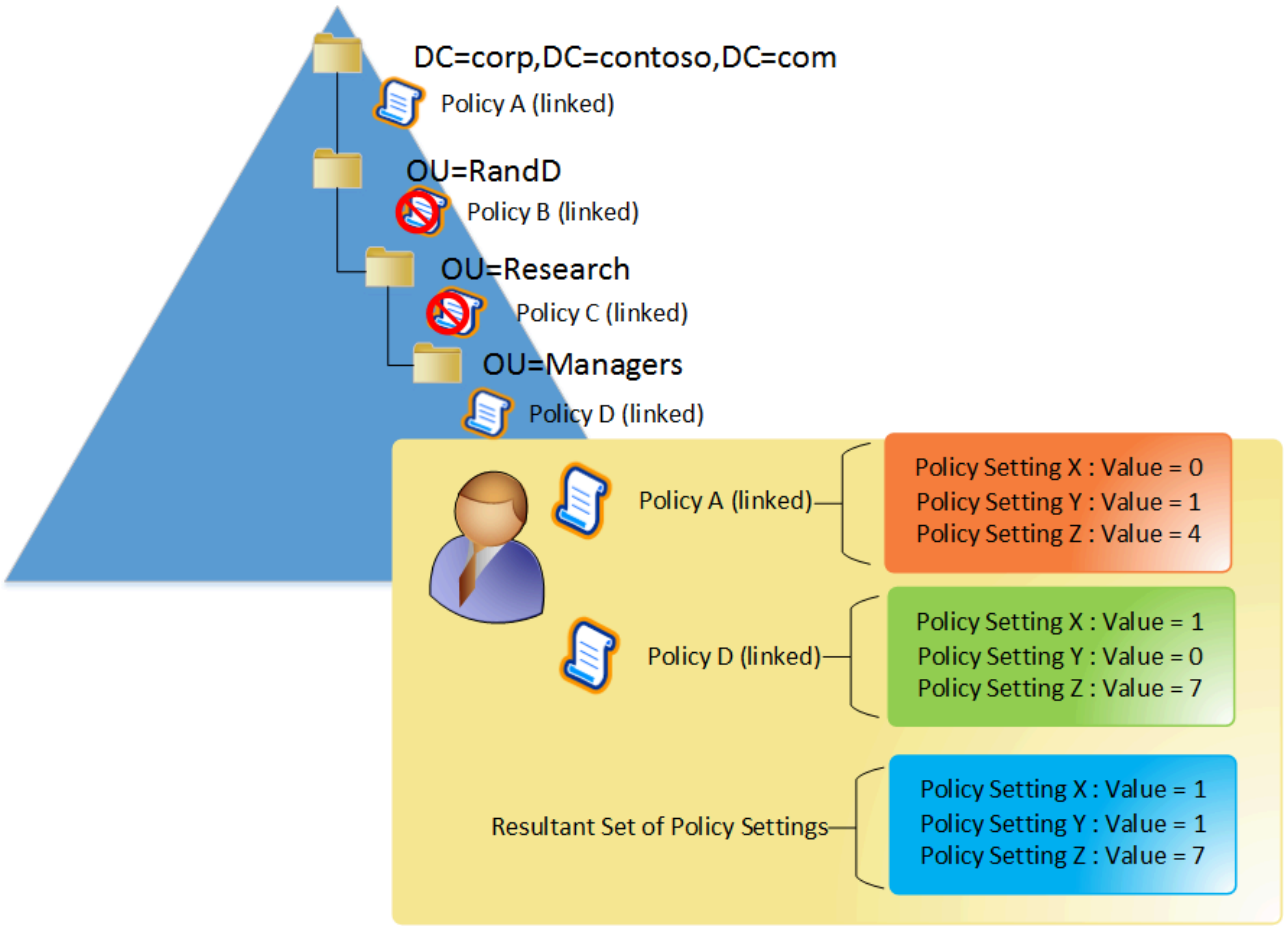
Notice the order of Group Policy objects has changed from the first list. This reordering of Group Policy occurs during the Security and WMI filter processing. The Group Policy service builds the first list of GPOs by finding the user or computer object and then collecting all linked GPOs as it walks up the directory tree. The GPOs are listed backwards from the order they apply because as the Group Policy service adds the newly discovered link location to the bottom of the list. This explains why the domain location is at the bottom of the list.

However, when filtering the list for security and WMI filters, the Group Policy service starts at the top of the list, which is the OU closest in lineage to the user or computer object. The service builds a new list (the filtered list) by placing the GPOs that pass through the filter into the filtered list. The service inverts the order of the original list, making the domain location at the top of the list. The location closest to the user is at the bottom of the list —the order Group Policy applies GPOs to users and computers.

Conflict Resolution

Each Group Policy object contains the same number of potential policy settings. Therefore, it is possible to have the same policy setting defined in multiple Group Policy objects. Conflicts occurs when the same policy setting is configured in multiple Group Policy objects. Like two cars competing for the same space on the road—one wins and the other loses. Group Policy handles conflicts by using a method known as last-writer-wins. Last-writer-wins resolves conflicts by declaring the prevailing setting as the setting that Group Policy writes last. Therefore, the

Group Policy object containing the conflicting policy setting that applies last is the setting that wins over all other settings.



The Processing Order section of this document describes that Group Policy objects apply in Local, Site, Domain, and Organizational Unit order. Based on this processing hierarchy:

- Policy settings in Group Policy objects linked to the Active Directory site resolve policy setting conflicts between the Local Group Policy object and Group Policy objects linked to the Active Directory site.
- Policy settings in GPOs linked to the domain resolve policy setting conflicts between Group Policy objects linked to the Active Directory site and GPOs linked to the Active Directory domain.
- Policy settings in GPOs linked to an organizational unit resolve policy setting conflicts between Group Policy objects linked to the Active Directory domain and GPOs linked to an organizational Unit.
- Policy settings in GPOs linked to a child organizational unit resolve policy settings conflicts between Group Policy objects linked to the child organizational unit and GPOs linked to the parent organizational unit.

Conflict Resolution among GPOs linked at the same Location

Group Policy enables you to link multiple Group Policy objects at each site, domain, and organization unit locations in the directory. Until now, conflict resolution only identified resolutions between conflicting policy

settings linked at two different locations in Active Directory. What about conflicting policy settings in Group Policy objects that are linked at the same location?

Group Policy continues to use the last-writer-wins method for resolving policy setting conflicts among Group Policy objects linked as the same location in Active Directory. Understanding how the Group Policy Management Console (GPMC) links Group Policy objects to locations in Active Directory explains the processing order of Group Policy objects link at the same location in Active Directory.

GPLink Attribute

The locations that support Group Policy linking, Active Directory sites, domains, and organizational units, do so because each of these objects have a GPLink attribute. The GPLink attribute is a single-valued attribute that accepts a value of a string data type. While the Active Directory Schema enforces the single-valued nature of the GPLink attribute, Group Policy uses the attribute as a multivalued attribute. The GPMC writes the value of the GPLink attribute using the following format.

```
[distinguishedNameOfGroupPolicyContainer;linkOPtions][…][…]
```

The distingushedNameOfGroupPolicyContainer token represents the distinguished name of the Group Policy Container. A Group Policy object is a single logical object composed of two components of information. The component of information stored on the file system is the Group Policy template. The remaining component, the Group Policy Container is an object in Active Directory object that lives in the domain partition of Active Directory. As previously covered, the distinguished name of a directory object provides the object’s name and location in the directory.

The linkOptions token is an integer value that defines the link options associated with the Group Policy object. Currently, you can enable or disable linked of Group Policy objects. Also, you can configure the link as enforced. The linkOptions value is a bit value where combining values varies the configurations.

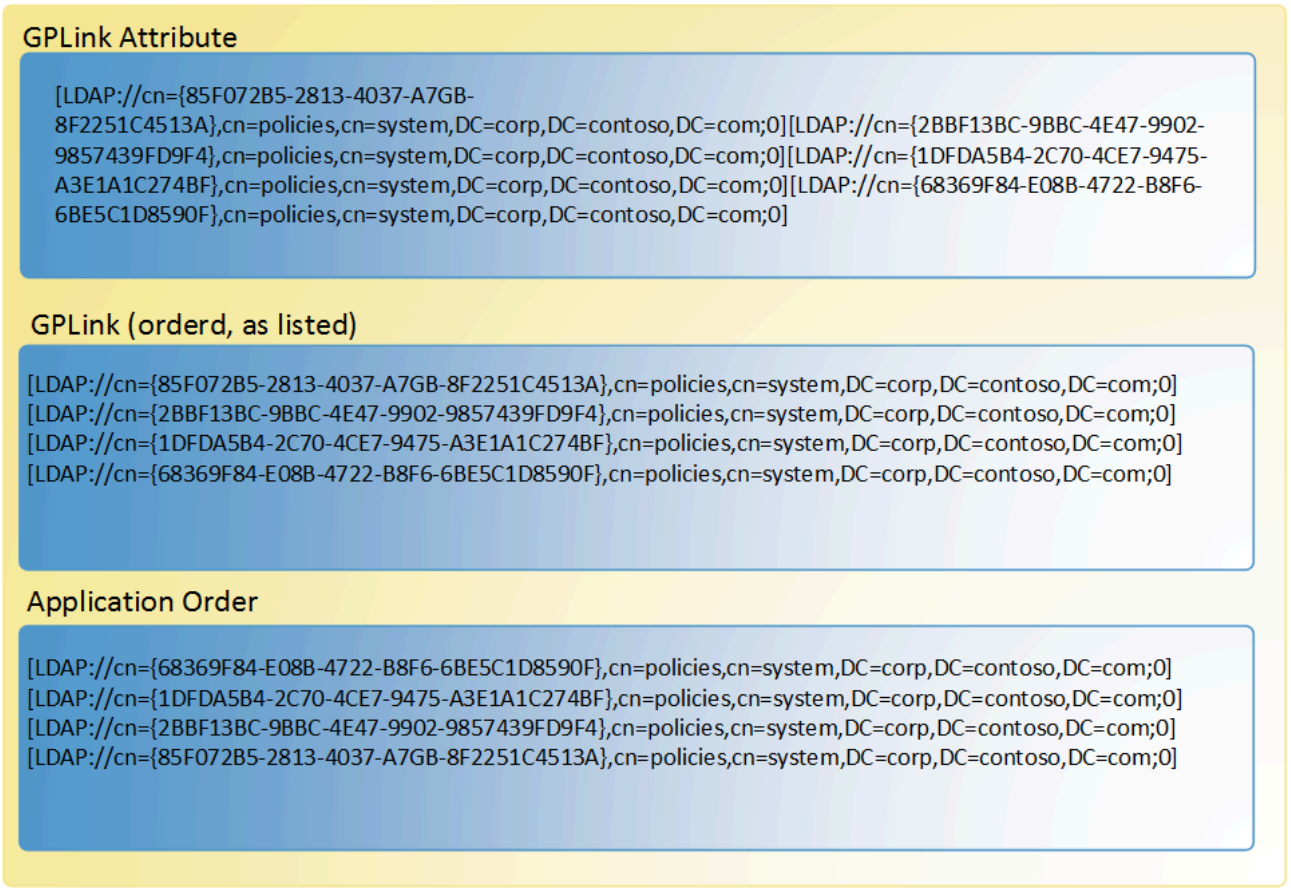
```
 Enabled0x0
Disabled 0x1
Enforced0x2
```

Disabling the link of a Group Policy objects prevents the Group Policy service from including that GPO in the list of GPOs within scope of the targeted user or computer. The distinguishedNameOfGroupPolicyContainer and the linkOptions token are enclosed in square brackets ([ ]) and separated by a semicolon (;). This represents a singly linked Group Policy object. Linking another Group Policy object to the location inserts a new distingushedNameOfGroupPolicyContainer and linkOptions combination before the existing combination; it does not add the new combination to the end. The linking pattern continues to insert newly linked GPOs at the beginning of the value; by moving existing values to the right.

The Group Policy service reads this long string as a list of values from left to right. The first GPO link entry in the value is the first to apply at this location. The next entry in the value applies afterwards. The process continues until the last GPO in the value applies.

Group Policy inherently assigns each GPO precedence based on the order it reads the list—left to right. Therefore, the first GPO in the value has the lowest precedence in the list of linked Group Policy objects. The next GPO in the value has a higher precedence than the previous GPO because it applies its policy settings after the previous GPO; by winning any policy setting conflicts between the two GPOs. Each GPO that follows has a higher precedence than the Group Policy object before it in the link order. The last GPO in the value has the highest precedence because it is the last Group Policy object the Group Policy service applies.

The best way to understand this is to think of the long string as a list of GPOs. Take the first GPO (the left most GPO) in the value and place it the list. Take the next links GPO listed and place on top of the list (causing all others to move down in the list by one). Continue this process until the last GPO is on top of the list. This final GPO linked entries list is in precedence order, which means the list is processed from the bottom to the top.



When viewed in a list in precedence order, it's easy to discover that GPOs higher in the list have more precedence than GPOs lower in the list. As a result, GPOs lower in the list lose policy setting conflicts and GPOs higher in the list win policy setting conflicts.

Link Options

As previously stated, a Group Policy linked as options of enabled, disabled, and enforced. The enabled and disabled options are intuitive to understand. When an enabled link is considered in the scope of Group Policy for the targeted user or computer. A disabled linked behaves as if the Group Policy object was never linked.

Enforced

The Enforced link option is the exception to all rules. The Enforced option ensures the settings from the linked GPO always win conflicts regardless of any other Group Policy object that contains policy settings that may conflict with those of the linked GPO. The GPMC visually represents an enforced Group Policy link by adding a padlock to the existing linked policy icon. Group Policy settings from an enforced link always apply, even if the organizational unit has block policy inheritance enabled

Block Policy Inheritance

The last item about Group Policy processing order is Block Policy Inheritance, or simply known as Block Inheritance in the Group Policy Management Console. Each domain and organizational unit in Active Directory object contains a **GPOptions** attribute. This setting enables you to block Group Policy settings linked higher in the processing order from applying to users and computers that are typically in containers lower in the processing order.

For example, policy settings linked to the domain apply to computers and users within the entire domain, regardless of their parent organizational unit. However, you can use GPMC to block inheritance on the domain or an organizational unit to prevent normal Group Policy setting from applying to users and computers within that container. Blocking policy inheritance on the domain prevents Group Policy settings from GPOs linked to the Active Directory site from applying to the domain. Blocking policy inheritance on organizational units prevents normal Group Policy settings from GPOs linked to sites and domains from applying to the organizational units.

Block policy inheritance does not prevent Group Policy settings from enforced linked Group Policy objects from applying to users and computers. Group Policy settings from enforced links apply regardless of the block policy inheritance status on domain and organizational unit objects.

Group Policy Preferences

Group Policy Preferences extends Group Policy. Preferences are not Group Policy settings. Windows stores both settings in the registry; however; policy settings have an advantage over preferences—they typically override a preference.

You can configure Windows using the user interface. The user interface presents you with choices; you choose the options you like; and click OK or close the dialog box. Windows then saves your choices to the registry so it can recall those settings later. Settings configurable by the user are known as preferences (notice the lowercase “p”). Mapping a shared folder or choosing a default home page is an example of preferences. When you set the home page using Internet Explorer, you can close the web browser and open it up again and it remembers your home page. Policy settings differ from preferences because policy settings are enforced on the user or computer. Policy prevents the user from changing their settings. Typically, users configure preferences.

Group Policy Preferences enables you to deploy desired configurations to computers and users without limiting the user from choosing a different configuration. It is important to remember that while the user can change the configuration, Group Policy Preferences are Group Policy client-side extensions. Group Policy Preferences refresh with Group Policy; therefore, Group Policy overwrites any preference settings altered by the user with the value configured in a Group Policy Preference. Replacing a user configured preference setting with one configured using Group Policy Preferences is not the same as Group Policy. A true Group Policy setting enforces

the setting and restricts the user from changing the setting. Users can easily change preference values enabled by Group Policy Preferences until the next refresh of Group Policy (which returns the preference settings back to the value configured in the Group Policy Preference item).

Client-side Extensions

Group Policy Preferences are Group Policy client-side extensions. There are 20 extensions that makes up Group Policy Preferences. These extensions include

Client Side Extension	Description
Group Policy Environment	Create, modify, or delete environment variables.
Group Policy Local Users and Groups	Create, modify, or delete local users and groups.
Group Policy Device Settings	Enable or disable hardware devices or classes of devices.
Group Policy Network Options	Create, modify, or delete virtual private networking (VPN) or dial-up networking (DUN) connections.
Group Policy Drive Maps	Create, modify, or delete mapped drives, and configure the visibility of all drives.
Group Policy Folders	Create, modify, or delete folders.
Group Policy Network Shares	Create, modify, or delete network shares
Group Policy Files	Copy, modify the attributes of, replace, or delete files.
Group Policy Data Sources	Create, modify, or delete Open Database Connectivity (ODBC) data source names.

Group Policy INI Files	Add, replace, or delete sections or properties in configuration settings (.ini) or setup information (.inf) files.
Group Policy Folder Options	Create, modify, or delete folders.
Group Policy Schedule Tasks	Create, modify, or delete scheduled or immediate tasks.
Group Policy Registry	Copy registry settings and apply them to other computers. Create, replace, or delete registry settings.
Group Policy Printers	Create, modify, or delete TCP/IP, shared, and local printer connections.
Group Policy Shortcuts	Create, modify, or delete shortcuts.
Group Policy Internet Settings	Modify user-configurable Internet settings
Group Policy Start Menu Settings	Modify Start menu options.(Not applicable for Windows 8 and Windows Server 2012)
Group Policy Regional Options	Modify regional options.
Group Policy Power Options	Modify power options and create, modify, or delete power schemes.
Group Policy Applications	Configure settings for applications.

Common Configurations

Most Group Policy Preference items share a common configuration that enable you to control the scope of Group Policy Preference processing for each configured preference item.

Stop processing items in this extension if an error occurs on this item

Each preference extension can contain one or more preference items. By default, a failing preference item does not prevent other preference items in the same extension from processing.

If the **Stop processing items in this extension if an error occurs on this item** option is selected, a failing preference item prevents remaining preference items within the extension from processing. This change in behavior is limited to the hosting Group Policy object (GPO) and client-side extension. It does not extend to other GPOs.

It’s important to understand that Group Policy Preference extensions process preference items from the top of the list and work their way to the bottom. The preference extension only stops processing preference items that follow the failing preference item (items appearing below the failing preference items as they appear in the list).

Run in logged-on user's security context (user policy option)

There are two security contexts in which Group Policy applies user preferences: the SYSTEM account and the logged-on user.

By default, Group Policy processes user preference items using the security context of the SYSTEM account. In this security context, the preference extension is limited to environment variables and system resources available only to the computer.

If the **Run in logged-on user's security context** option is selected, it changes the security context under which the preference item is processed. The preference extension processes preference items in the security context of the logged-on user. This allows the preference extension to access resources as the user rather than the computer. This can be important when using drive maps or other preferences in which the computer may not have permissions to resources or when using environment variables. The value of many environment variables differ when evaluated in a security context other than the logged-on user.

Group Policy Preference extensions that need to process in the user’s security context, such as Drive Maps and Printers **automatically** switch to the user’s context and do not need you to adjust this setting.

Remove this item when it is no longer applied

Group Policy applies policy settings and preference items to users and computers. You decide which users and computers receive these items by linking one or more Group Policy objects (GPOs) to Active Directory sites, domains, or organizational units. User and computer objects in these containers receive policy settings and preference items defined in the linked GPOs because they are within the scope of the GPO.

Unlike policy settings, the Group Policy service does not remove preference settings when the hosting GPO becomes out of scope for the user or computer.

If the **Remove this item when it is no longer applied** option is selected, it changes this behavior. After selecting this option, the preference extension decides if the preference item should not apply to targeted users or computers (out of scope). If the preference extension decides the preference item is out of scope, it removes the settings associated with the preference item.

Selecting this setting changes the preference item's action to **Replace**. During Group Policy application, the preference extension recreates (deletes and creates) the results of the preference item. When the preference item is out of scope for the user or computer, the results of the preference item are deleted, but not created. Preference items can become out of scope by using item-level targeting or by higher-level Group Policy filters such as WMI and security group filters.

The **Remove this item when it is no longer applied** option is not available when you set the preference item action to Delete.

Apply once and do not reapply

Preference items apply when Group Policy refreshes.

By default, the results of preference items are rewritten each time Group Policy refreshes. This ensures the preference item results are consistent with what you configured in the Group Policy object.

If the **Apply once and do not reapply** option is selected, it changes this behavior, so the preference extension applies the results of the preference item to the user or computer only once. This option is useful when you do not want the results of a preference item to reapply.

Item-level Targeting

Group Policy provides filters to control which policy settings and preference items apply to users and computers. Preferences provide an added layers of filtering called targeting. Item-level targeting enables you to control if a preference item applies to a group of users or computers.

Use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items—each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.

Each targeting item results in a value of either true or false. You can apply multiple targeting items to a preference item and select the logical operation (AND or OR) by which to combine each targeting item with the preceding one. If the combined result of all targeting items for a preference item is false, then the settings in the preference item are not applied to the user or computer. Using targeting collections, you can also create parenthetical expressions.

Battery Present

A Battery Present targeting item allows a preference item to be applied to computers or users only if one or more batteries are present in the processing computer. If Is Not is selected, it allows the preference item to be applied only if the processing computer does not have one or more batteries present.

If an uninterruptible power supply (UPS) is connected to the processing computer, a Battery Present targeting item may detect the UPS and identify it as a battery.

Computer Name

A Computer Name targeting item allows a preference item to be applied to computers or users only if the computer's name matches the specified computer name in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the computer's name does not match the specified computer name in the targeting item.

CPU Speed

A CPU Speed targeting item allows a preference item to be applied to computers or users only if the processing computer's CPU speed is greater than or equal to the value specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the processing computer's CPU speed is less than or equal to the value specified in the targeting item.

Date Match

A Date Match targeting item allows a preference item to be applied to computers or users only if the day or date matches that specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the day or date does not match that specified in the targeting item.

Dial-up Connection

A Dial-Up Connection targeting item allows a preference item to be applied to users only if a network connection of the type specified in the targeting item is connected. If Is Not is selected, it allows the preference item to be applied only if no network connection of the type specified in the targeting item is connected.

Dial-Up Connection targeting items detect whether a type of network connection exists, not whether the user is logged on through a connection of that type.

Disk Space

A Disk Space targeting item allows a preference item to be applied to computers or users only if the processing computer's available disk space is greater than or equal to the amount specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the processing computer's available disk space is less than or equal to the amount specified in the targeting item.

Domain

A Domain targeting item allows a preference item to be applied to computers or users only if the user is logged on to or the computer is a member of the domain or workgroup specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the user is not logged on to or the computer is not a member of the domain or workgroup specified in the targeting item.

Environment Variables

An Environment Variable targeting item allows a preference item to be applied to computers or users only if the environment variable and value specified in the targeting item are equal. If Is Not is selected, it allows the preference item to be applied only if the environment variable and value specified in the targeting item are not equal or if the environment variable does not exist.

If you want to restrict the scope of multiple preference items with a complex set of targeting items, you can simplify configuration by using an environment variable. For example, create an Environment Variable preference item that generates a new environment variable with a value of 1, and apply the targeting items to it. To apply the same targeting to other preference items, add an Environment Variable targeting item to those preference items, and configure it to require a value of 1 for the variable that you created using an Environment Variable preference item.

File Match

A File Match targeting item allows a preference item to be applied to computers or users only if the file or folder specified in the targeting item exists, or only if the file exists and is a version within the range specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the file or folder specified in the targeting item does not exist, or only if the version of the file is not within the range specified in the targeting item.

IP Address Match

An IP Address Range targeting item allows a preference item to be applied to computers or users only if the processing computer's IP address is within the range specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the processing computer's IP address is not within the range specified in the targeting item.

Language

A Language targeting item allows a preference item to be applied to computers or users only if the locale specified in the targeting item is installed on the processing computer. Additional options allow you to restrict the targeting to the user's or computer's locale. If Is Not is selected, it allows the preference item to be applied only if the processing computer's locale does not match the specified locale in the targeting item.

A locale is composed of a language and, in some cases, a geographic area in which the language is spoken or the alphabet used. For example, French (Canada) is a locale composed of the language French and the geographic area Canada.

LDAP Query

An LDAP Query targeting item allows a preference item to be applied to computers or users only if the LDAP query returns a value for the attribute specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the LDAP query does not return a value for the attribute specified in the targeting item.

MAC Address Range

A MAC Address Range targeting item allows a preference item to be applied to computers or users only if any of the processing computer's MAC addresses are within the range specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if none of the processing computer's MAC addresses are not within the range specified in the targeting item.

Range starting points and ending points are inclusive. You can specify a single address by typing the same value in both boxes.

MSI Query

An MSI Query targeting item allows a preference item to be applied to computers or users only if certain aspects of an MSI installed product, update, or component on the processing computer match the specified criteria in the targeting item. If Is Not is selected, it allows the preference item to be applied only if certain aspects of an MSI installed product, update, or component on the processing computer do not match the specified the specified criteria in the targeting item.

Operating System

An Operating System targeting item allows a preference item to be applied to computers or users only if the processing computer's operating system's product name, release, edition, or computer role matches those specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the operating system's product name, release, edition, or computer role does not match those specified in the targeting item.

Organizational Unit

An Organizational Unit targeting item allows a preference item to be applied to computers or users only if the user or computer is a member of the organizational unit (OU) specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the user or computer is a not member of the OU specified in the targeting item.

PCMCIA Present

A PCMCIA Present targeting item allows a preference item to be applied to computers or users only if the processing computer has at least one PCMCIA slot present. If Is Not is selected, it allows the preference item to be applied only if the processing computer does not have any PCMCIA slots present.

A PCMCIA slot is considered present when the drivers for the slot are installed and the slot is functioning correctly.

Portable Computer

A Portable Computer targeting item allows a preference item to be applied to computers or users only if the processing computer is identified as a portable computer in the current hardware profile on the processing computer or if the processing computer is identified as a portable computer with the docking state specified in the targeting item. When Is Not is selected, it allows the preference item to be applied only if the processing computer is not identified as a portable computer in the current hardware profile on the processing computer or if the docking state of the processing computer differs from the docking state specified in the targeting item.

Processing Mode

A Processing Mode targeting item allows a preference item to be applied to computers or users only if the Group Policy processing mode or conditions on the processing computer match at least one of those specified in the

targeting item. If Is Not is selected, it allows the preference item to be applied only if the Group Policy processing mode or conditions on the processing computer do not match any of those specified in the targeting item.

RAM

A RAM targeting item allows a preference item to be applied to computers or users only if total amount of physical memory in the processing computer is greater than or equal to the amount specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the total amount of physical memory in the processing computer is less than the amount specified in the targeting item. Provide the total amount of physical memory in megabytes (MB). One gigabyte (GB) of physical memory is entered as 1024. Four gigabytes of physical memory are entered as 4096.

Registry Match

A Registry Match targeting item allows a preference item to be applied to computers or users only if the registry key or value specified in the targeting item exists, if the registry value contains the data specified in the targeting item, or if the version number in the registry value is within the range specified in the targeting item. If the targeting item allows the preference item and if Get value data is selected in the targeting item, then the targeting item saves the value data of the specified registry value to the environment variable specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the registry key or value specified in the targeting item does not exist, if the registry value does not contains the data specified in the targeting item, or if the version number in the registry value is not within the range specified in the targeting item.

Security Group

A Security Group targeting item allows a preference item to be applied to computers or users only if the processing computer or user is a member of the group specified in the targeting item and optionally only if the specified group is the primary group for the processing computer or user. If Is Not is selected, it allows the preference item to be applied only if the processing computer or user is not a member of the group specified in the targeting item and optionally only if the specified group is not the primary group for the processing computer or user.

Security Group

- Domain groups
    - Domain local
    - Global groups
    - Universal groups
- Local groups
    - Local groups (including built-in groups)
    - Well-known

Site

A Site targeting item allows a preference item to be applied to computers or users only if the processing computer is in the site in Active Directory specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the processing computer is not in the site in Active Directory specified in the targeting item.

Targeting Collection

The targeting items applied to a preference item are evaluated as a logical expression. A targeting collection allows you create a parenthetical grouping within that expression. You can nest one targeting collection within another to create more complex logical expressions.

A targeting collection allows a preference item to be applied to computers or users only if the collection of targeting items specified results in a value of true. If Is Not is selected, it allows the preference item to be applied only if the collection of targeting items specified results in a value of false.

Terminal Session

A Terminal Session targeting item allows a preference item to be applied to users only if the processing user is logged on to a terminal services session with the settings specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the user is not logged on to a terminal services session or the user is logged on to a terminal services session without the settings specified in the targeting item.

Time Range

A Time Range targeting item allows a preference item to be applied to computers or users only if the current time on the end user's computer is within the time range specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the current time on the end user's computer is not within the range specified in the targeting item.

User

A User targeting item allows a preference item to be applied to users only if the processing user is the user specified in the targeting item. If Is Not is selected, it allows the preference item to be applied only if the processing user is not the user specified in the targeting item.

WMI Query

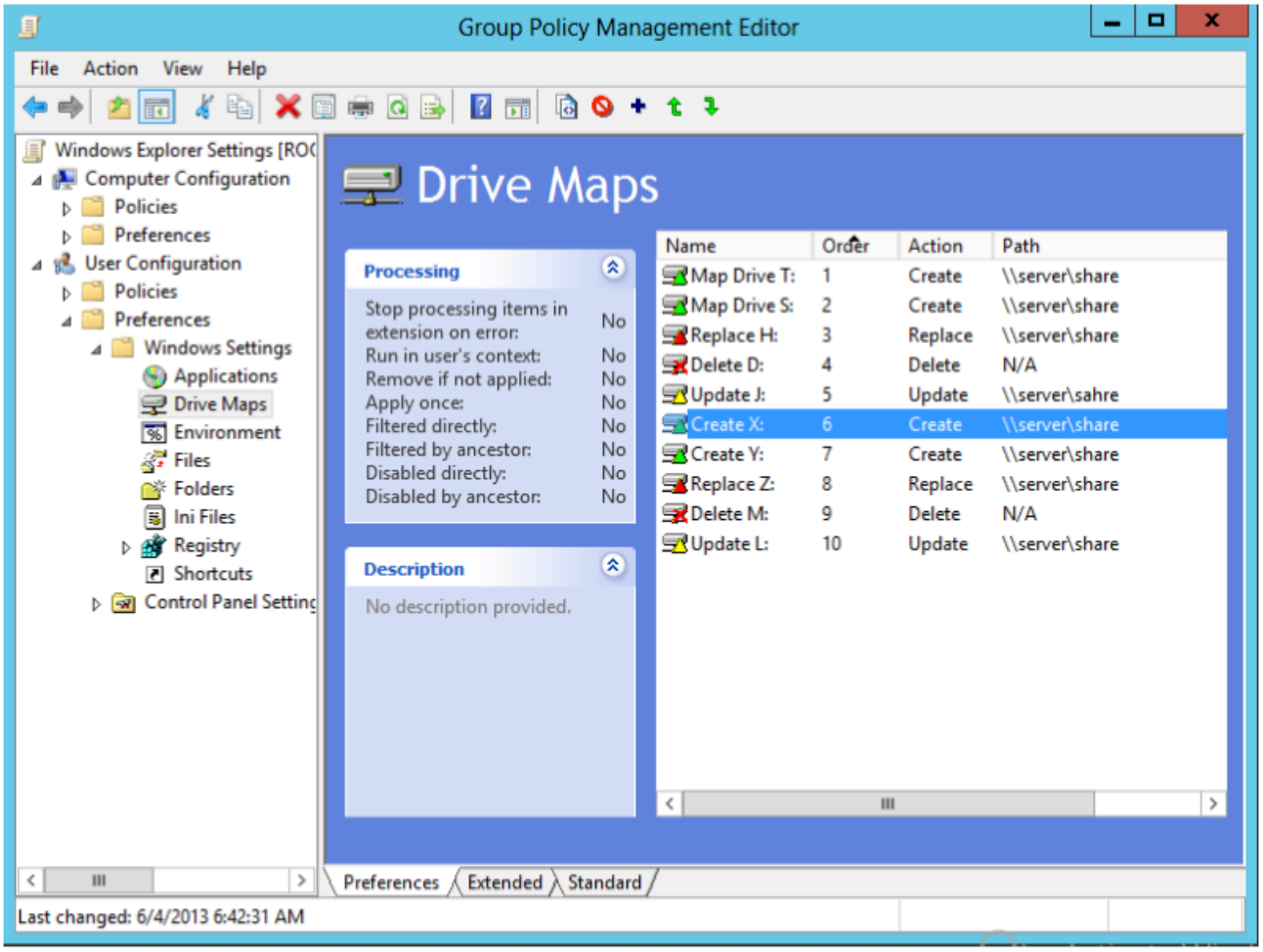
A WMI Query targeting item allows a preference item to be applied to computers or users only if the processing computer evaluates the WMI query as true. If Is Not is selected, it allows the preference item to be applied only if the processing computer evaluates the WMI query as false.

Processing

Earlier, this document explained Group Policy processing. Group Policy Preference client-side extensions adhere to these same rules. Therefore, linked hierarchy, security and WMI filtering can change the scope of Group Policy

object configured with Group Policy Preferences. By changing the scope, users and computers may or may not receive settings or preference items configured in these Group Policy objects.

However, Group Policy Preference client-side extensions have their own internal processing. You can configure one or more preference items for a single Group Policy Preference extension to process within a single Group Policy object. For example, you can configure a single GPO to contain 10 Drive Map Preference items within a single GPO.



During Group Policy processing, the Group Policy infrastructure cycles through a list of Group Policy extensions. As it moves to each extension, it shares information relevant for the extension to process its portion of Group Policy. Critical components of the information shared with the extensions include a list of Group Policy objects that included changes, a list of Group Policy objects that are no longer in scope with the user or computer. Also, the Group Policy infrastructure provides information specific to this instance of Group Policy processing such as if the network connection is considered a slow link.

The Group Policy Preference extension uses the information about the changed and out-of-scope Group Policy objects to process its policy settings. Group Policy Preference client-side extensions process preference items in order from the top of the list to the bottom of the list.

The results of processing each preference item vary depending on the action configured in the preference item. Also, item-level targeting can prevent the preference item from applying to the user or computer. The Group

Policy Preference client-side extension applies each item in the list until it reaches the end of the list, or exits because of a common configuration settings such as **Stop processing items in this extension if an error occurs on this item or Apply once and do not reapply**. Once the preference extensions applies all preference items in the list, it returns control to the Group Policy service.

Source: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v%3Dws.11)