Group Policy Preferences Overview

Requirements and Features

By Darren Mar-Elia, SDM Software

Overview

The Group Policy Preferences (GPP) feature was first made available at the release of Windows Server 2008. GPP is technology that Microsoft acquired when they purchased DesktopStandard and was referred to as PolicyMaker. Essentially, GPP is a set of client-side extensions and a management interface that adds to the policy capabilities that were previously available from Windows. The name "Preferences" underscores the fact that all of these new policy capabilities added by GPP are just that—preferences rather than policies that cannot be undone by an end-user. That being said, they do allow for a wide variety of additional configuration capability through Group Policy that previously had required complex logon scripts to automate.

Requirements

Despite its coincident release with Server 2008, you do **not** need to have Server 2008 deployed in your environment in order to deploy and use GPP. In fact, the new policy features in GPP support XP, Server 2003, Vista and Server 2008 "clients". In order for clients to process GPP policy settings, they must install the GPP Client Side Extension (CSE) package, which is available from Microsoft's download site (download.microsoft.com). There is a version for each platform so ensure that you install the correct version. The CSE package does not ship as a .MSI file, so unfortunately (and ironically) it can not be deployed using the GP Software Installation feature. Note that SP1 for Vista installs the CSEs by default. All other platforms currently require a separate installation. Its also important to note that some platforms require a pre-requisite package called XMLLite before you can deploy the GPP CSEs. More information about XMLLite can be found on any of the GPP CSE download pages. It is worth noting that if any of the following conditions are true on your client systems, they do not need the XMLLite package pre-installed:

- Windows Server 2003, **SP2** and Windows XP **SP3** already include XMLLite, and thus it's not required as a separate install before you install Group Policy Preferences on those versions of the OS
- Windows Server 2003, **SP1** and Windows XP, **SP2** with **Internet Explorer 7** installed also do not need XMLLite, as it is included with IE 7.

In addition to installing the GPP CSE on all client systems that you want to deploy GPP settings too, you need to be able to manage those settings. That means having a version of the Group Policy

Management Console (GPMC) and Group Policy Editor MMC snap-in that recognizes those settings. In order to manage GPP settings, you must be running either a Vista, SP1 system or a Server 2008 system. With those pre-requisites, you then need GPMC installed. On Server 2008, this can be installed as a separate feature called “Group Policy Management”. On Vista, SP1, you must install the separate Remote Server Administration Tools (RSAT) package and then install the Group Policy Management feature that is part of RSAT. Once that is installed, you can both report on and manage GPP settings just as you would the normal GP settings, using both GPMC and the “new” GP Management Editor (GPME). Note that GPP settings are not supported on the local GPO, so if you expecting to start gpedit.msc and see GPP settings, you will not.

Features

GPP comes with a large number of new capabilities for policy-based configuration management. It’s a fair statement to make that once you are leveraging GPP, there are probably very few scenarios that require you to still use logon scripts to configure aspects of your environment. Before we get into specific features, its worthwhile to point out one significant capability that GPP brings that is not available in any of the “native” Group Policy settings. This is a feature called “item-level targeting”. Item-level targeting, as the name implies, allows you to set very granular filters on individual policy items within a GPO. This is significantly different from previous Group Policy filtering capabilities in that previously your only control over which computers and users received a GPO were by using security group filtering, linking of the GPO and/or WMI filters. Item-level targeting allows you to have different filtering criteria for each setting within a given GPO. So, in addition to targeting say, the “Marketing” OU using the native GPO linking, you can also use item-level targeting on GPP settings within that GPO to target only the market computers in that OU that are on laptops, or are on a specific IP address range, or only during a specific period of the day. Indeed, there are no less than 27 filter criteria that you can use to control individual settings within a GPO. Obviously, this much granularity can be both a blessing and a curse, if over-used!

Now let’s look at each main feature within GPP and describe how it can add value to your Windows configuration management tasks. GP Preferences are found within the GPME snap-in under Computer or User Configuration\Preferences, within either a Windows Settings or Control Panel Settings subfolder.

- **Environment:** The environment extension is per-computer and per-user and lets you configure both system and user environment variables (e.g. %temp%) on a given target system. Note that with all GPP settings, you can choose different actions for this extension. You can create a new environment variable, update or replace an existing one, or delete an existing one.
- **Files:** Both a per-computer and per-user extension that lets you distribute files to your end-user computer or user. For example, you might use this to distribute shortcuts to your user’s desktops or data files required for a local desktop application.

- **Folders**: Both a per-computer and per-user extension that lets you create, update and delete folder structures on target systems or users. For example, you might use this setting to delete temporary folders that get created on computers.
- **Ini Files**: Both a per-computer and per-user extension that lets you create, delete or update values within text-based ini files. Ini files are an old Windows configuration method that pre-dates the registry, but that are still used by some applications. You can actually use this extension to update individual key-value pairs within an INI file without having to write a new file down to the computer or user.
- **Registry**: Both a per-computer and per-user extension—this extension is powerful in that you can create, delete and update registry keys and values on target systems. Because this extension provides the ability to easily push registry values to computers and users through a GUI interface, and because it supports all the different value types in the registry, this extension effectively eliminates the need for creating custom ADM files for pushing out registry modifications through Administrative Template policy.
- **Network Shares**: A per-computer extension only—this extension lets you create shares on target computers—be they desktops or servers. You can create, delete and update shares, in fact, on any target system. In addition, the extension lets you set a user limit on the share and even enable the Access-Based Enumeration (ABE) feature on Server 2003, SP1, but in fact does not expose the ability to control share permissions.
- **Shortcuts**: This is both a per-computer and per-user extension that lets you create and distribute shortcuts to computers and users. You can manage shortcuts to file systems, web URLs and Windows shell objects (e.g. My Computer). This extension does not copy .lnk files around, but rather creates shortcuts on the fly, that meet your specifications. You can specify all of the normal parameters of a shortcut, including the "Start in" field, the icon that appears with the shortcut and any arguments for the target that the shortcut executes
- **Drive Maps**: This is a per-user extension that lets you control drive mappings for end users. You can create, delete and update drive mappings to UNC paths and can control which drive letter is mapped (or use next available). You can also choose to hide or show the particular drive letter to the user. Note that using this extension along with item-level targeting by user group; you can effectively replace logon scripts that map drives based on group membership, within a single GPO.
- **Data Sources:** This is a per-computer and per-user extension that lets you manage system or user ODBC data sources used by applications that leverage databases. This extension lets you choose the ODBC driver type, and provide credentials for the connection to the database, which are stored encrypted within the GPO.
- **Devices**: This is a per-computer and per-user extension that lets you allow or deny use of devices based on the device class. So, for example, you could use this extension to deny the use of all thumb drives or all CD burners. Note that this device restriction capability is less granular than that provided in native Group Policy for Vista, but does provide a basic device restriction capability for XP clients that did not exist otherwise.

- **Folder Options:** This is a per-computer and per-user extension that lets you set file extension associations. For example, you can use this extension to associate all .pdf files with a particular PDF Writer, such as Adobe Acrobat. You can of course, also use this extension to update or remove existing associations.
- **Local Users and Groups**: This is both a per-computer and per-user extension that provides a variety of control around local user and group accounts. For example, you can use this extension to create a new local user on all of your desktop or server machines. But, more interestingly, you can also use this extension to update the passwords on existing accounts, like the local administrator, thereby giving you the ability to make periodic mass password changes to the local administrator account on all your machines. The passwords themselves are stored as 256-bit AES encrypted strings within the GPO's setting storage in SYSVOL. This is true for all passwords that are supported in GPP, in fact. As for group management, think of this feature as a more flexible version of Restricted Groups policy. Within this GPP feature, you can create, delete and update existing groups and their members. You can rename groups, you can delete all members from groups and you can add/remove members from groups.
- **Network Options**: This per-computer and per-user extension lets you manage VPN and Dial-up Networking (DUN) connections on your systems. This means you can, for example, centrally create a VPN client configuration for all of your corporate users that require VPN-based remote access, and if something changes in your VPN configuration, you can easily update those connections using this feature.
- **Power Options:** This per-computer and per-user extension lets you configure power management settings on XP/2003 systems (note that Vista/2008 comes with GP-based power management options already). You can configure power options, which include things like enabling hibernation and setting the behavior, for example, on laptops when you close their lid or press the power button. You can also configure power schemes, including creating your own custom schemes. These schemes define, for example, how long before the monitor shuts off when the system is plugged in vs. on battery, how the hard drive and CPU behave, etc.
- **Printers:** This per-computer and per-user extension lets you manage printer mappings. You can use it to install Shared, TCP/IP or Local printers. Shared printers are per-user only, and probably the most common way of connecting up a user with a printer. And, like the Drive Maps extension, you can use this extension along with item-level targeting to map printers based on criteria such as user groups or IP address ranges.
- **Scheduled Tasks**: This per-computer and per-user extension lets you create scheduled tasks to execute applications at particular times. Basically this provides a Group Policy interface into the Windows Task Scheduler on target systems. It also supports something called an immediate task, which means that you can set an immediate task to execute as soon as Group Policy processes this setting.
- **Services**: This is a per-computer extension that lets you control service configuration. While this extension is somewhat redundant to the existing Group Policy security setting

that lets you configure service startup type and security, the GPP version of this feature gives you more control. While you can't configure service security using this extension, you can configure elements of a service such as the account that it uses to logon to the system (along with password changes to those service accounts) as well as the recovery behavior of the service (e.g. restart after failure or run an external program when the service fails). In addition, this extension supports the ability to perform actions on the service (like stopping and starting it) when the policy is processed.

- **Internet Settings**: This per-user extension provides additional control over IE 5, 6 and 7 configurations. Although GP already provides both IE Maintenance policy and Administrative Templates settings for controlling IE security and behavior, this GPP extension provides some additional control that these two earlier policy areas do not, such as the ability to configure all of the options on IE's Tools, Internet Options, Advanced tab as well as more common aspects such as the Connections tab, home page and the size of Temporary Internet Files and browser history.
- **Regional Options:** This per-user extension provides the ability to control the options available in the Control Panel, Regional Settings applet, such as default user locale, how numbers, currency, data and time are displayed, and the user's default country location.
- **Start Menu**: This per-user extension lets you control the configuration of the Start Menu and its various options. From here you can enable or disable items that should appear on the Start Menu, set the size of Start Menu icons and how many programs appear, as well as customizing "Classic Start Menu" behavior. Note that this extension supports both XP and Vista.

General Behaviors

In addition to the features listed above, each policy item in GPP supports some general behaviors to help future control how the settings are applied to users and computers. These are:

- **Stop Processing items in this extension if an error occurs:** prevents further GP processing for a given extension if an error is encountered.
- **Run in logged-on user's security context (user policy option)**: per-user GPP settings will normally run in the context of the system account unless this option is specified.
- **Remove this item when it is no longer applied:** Let's you forcibly remove the policy setting when the policy falls out of scope of the user or computer (otherwise the policy setting is left in place).
- **Apply once and do not reapply**: Normally, preferences apply based on the action you choose (e.g. Create, Delete, Update, Replace) or in the case of a change to the underlying setting (e.g. the user un-does a setting that has been delivered by GPP. If this option is checked, then the setting is applied once but then never again. This option is useful for making one-time "suggestions" for a given setting that the user can override.
- **Item-level targeting**: Provides the granular targeting that we have already discussed.

Summary

As you can see, GP Preferences provides a wealth of additional policy configuration capabilities, as well as very granular targeting of policy. And while you do need at least Vista, SP1 or Server 2008 to manage these new settings, they can be processed by any systems running XP and above with the CSE package installed. Care need be taken to ensure that you don't go overboard with item-level targeting, but the fact that it is there, in addition to all of the added configuration capabilities within GPP, means that there are few configuration tasks on Windows that can't be performed centrally using Group Policy.