

Group Policy Settings Storage

Understanding Group Policy Settings Storage

Group Policy leverages a complex and sometimes inconsistent model when it comes to storing the settings that you specify within a Group Policy Object (GPO). This is probably owing to the fact that, while there was a central group at Microsoft is responsible for the Group Policy infrastructure, each product area that has policy settings (e.g. Security, IE, desktop) was responsible for implementing its own policy tools to leverage that infrastructure. As a result, policy settings for a given policy area may be scattered between file system storage and AD-based storage. To better understand this, let's take a quick look at how Group Policy Objects are structured.

Group Policy Structure

A GPO is composed of two pieces. When you create a new GPO, an AD object of class group Policy Container gets created under the System\Policies container within your AD domain, as Figure 1 shows.

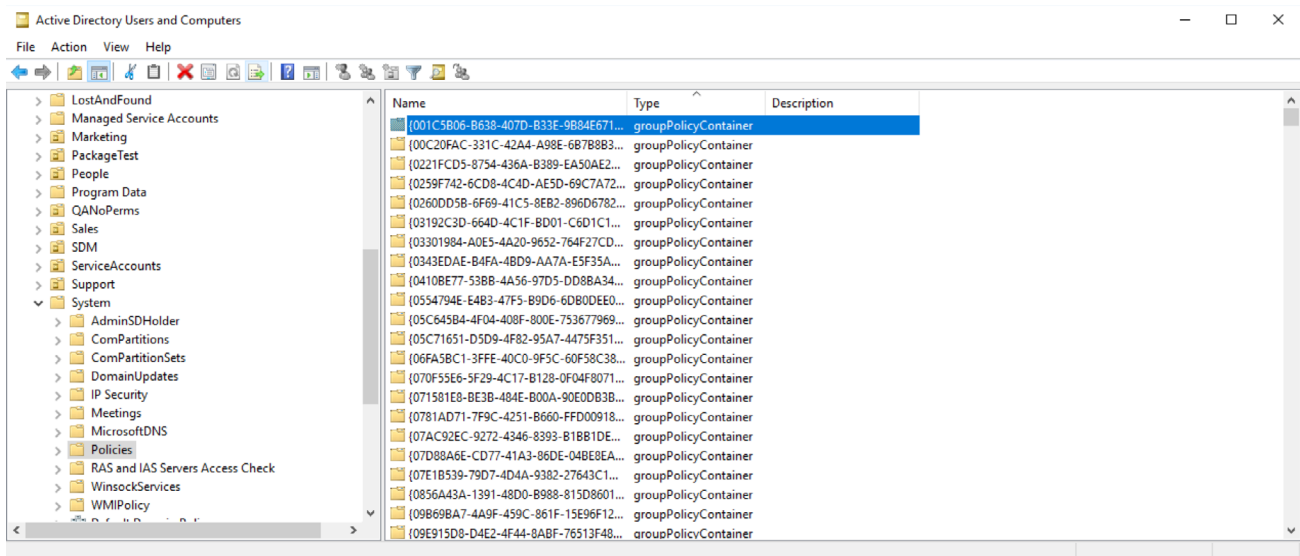


Figure 1: Viewing the AD portion of a GPO using AD Users & Computers

This AD portion of a GPO is called the **Group Policy Container**, or GPC. As you can see in Figure 1, Windows refers to GPOs by a unique GUID (i.e. the 128-bit identifier shown in braces) rather than by its “friendly” name, which is the name you assign to it when you first create the GPO. The implication here is that you can have many GPOs within a domain that are named with the same friendly name, but they will always be unique because their GUIDs are unique (except for the built-in Default Domain Policy and Default Domain Controller Policy GPOs, which have the same well-known GUIDs in every AD installation). In addition to the GPC, a new GPO creates a set of file folders and files within the SYSVOL share of the DC you’re focused during the creation process (by default this is usually the PDC role-holder DC within your domain). These folders and files are created under the Policies folder within SYSVOL. Similar to the GPC, when you create a new GPO, a GUID-named folder is created under the Policies folder within SYSVOL, as shown in Figure 2.

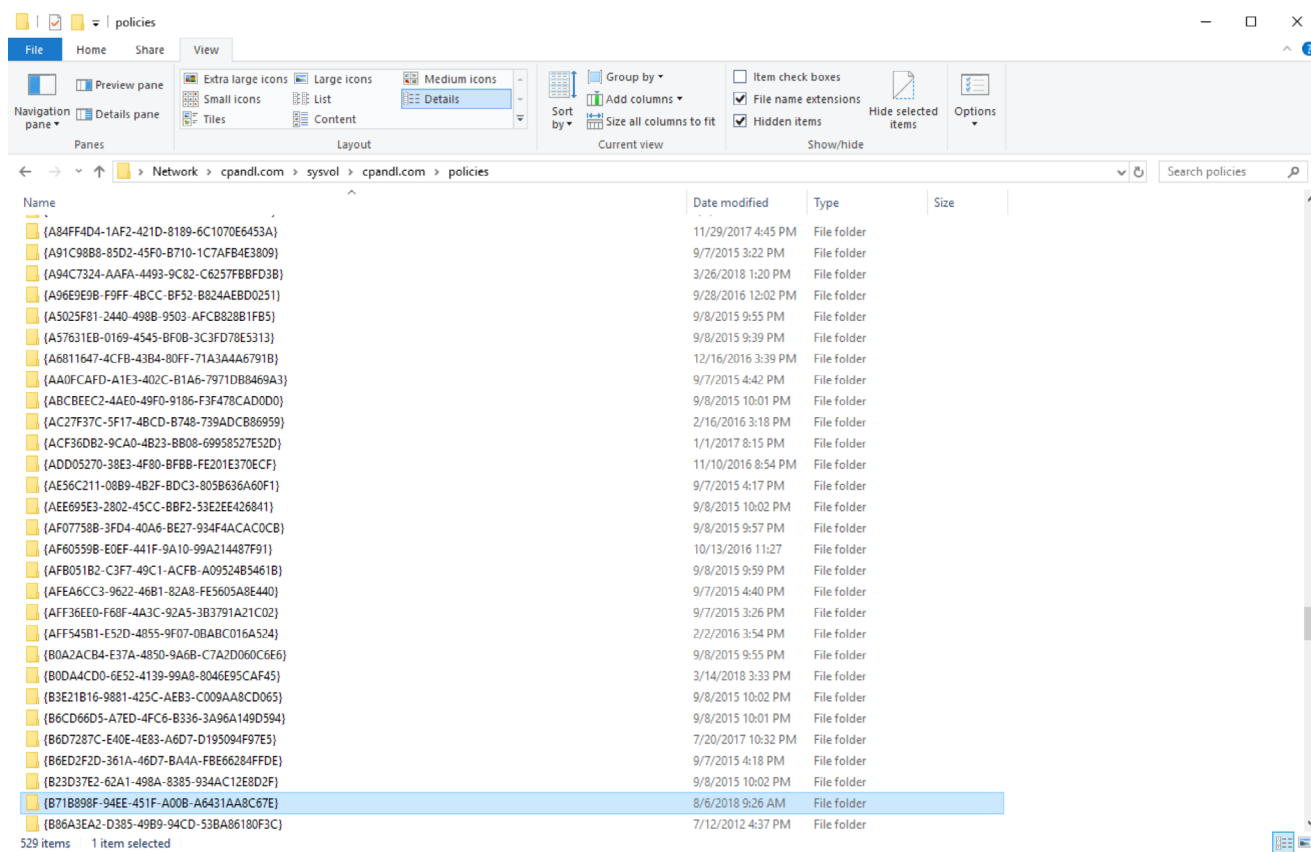


Figure 2: Viewing the SYSVOL portion of a GPO

This portion of a GPO that is stored as folders and files in SYSVOL is referred to as the Group Policy Template, or GPT. The GPT is where the majority of GPO settings are stored when you edit a GPO. That is, there are set of folders and files that get created under each GUID-named folder that store the policies that you enable within a GPO. However, while most policy settings are stored in the GPT, some policy areas store their settings in both the GPC and GPT, while still others use only the GPC and even others that don't use either the GPC or GPT. While this may seem confusing, keep in mind that it is the responsibility of the author of each policy extension (e.g. Administrative Templates, Folder Redirection, Software Installation) to decide on where to store their settings, and there is no standard for either location or format of settings storage. Over the years, Microsoft has coalesced on using the registry.pol file more and more, rather than building new storage models. While the preferred location is the GPT, there may be good reasons an extension author might choose to put their data elsewhere. Let's look at Windows. Table 1 provides a complete list of where settings are stored for each of the standard extensions that ship with current versions of Windows (Windows 10 and Server 2016 as of this writing).

Table 1: Group Policy Storage Locations

Group Policy Extension	Storage Location	Comments
Administrative Template Policy	Stored in SYSVOL, under the GPT container for a given GPO. Admin Template policy is stored in a file called registry.pol , which can be defined per user and per computer. Within a given GPT, if you've defined both user and computer AT policy, you will see a registry.pol file under both the user and machine sub-folders.	As you will see in this table, many policy areas overload registry.pol to store their settings—so it is no longer *just* Admin Templates
Advanced Audit Policy Configuration	Stored in SYSVOL, in the GPT container for a given GPO under Machine\Microsoft\Windows NT\Audit , in a text file called audit.csv	
Application Control Policies (AppLocker)	Uses registry.pol to store settings under the Machine folder in the GPT.	
Deployed Printers	Stored in AD (GPC) under either the Machine or User container. Under each, there is a container called PushedPrinterConnections that contain objects of class msPrint-ConnectionPolicy . There is one of these objects for each published printer in the GPO.	

Group Policy Extension	Storage Location	Comments
Disk Quota	Stored in SYSVOL, under the GPT container for a given GPO. Disk quota policy is also stored in registry.pol , however, you'll only find it in the copy of registry.pol stored under the machine folder, as this is a per-machine policy only.	
Folder Redirection	Stored in SYVOL, under the GPT container for a given GPO. FR policy is stored in one or two files called fdeploy.ini and fdeploy1.ini , in the sub-folder User\Documents & Settings within the GPT.	Fdeploy.ini is only used for backwards compatibility to XP and 2003 systems. All Windows systems starting with Vista will read from fdeploy1.ini.
Group Policy Preferences-Environment	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\EnvironmentVariables or User\Preferences\EnvironmentVariables folders in a file called EnvironmentVariables.xml	
Group Policy Preferences-Files	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Files or User\Preferences\Files folders in a file called Files.xml	
Group Policy Preferences-Folders	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Folders or User\Preferences\Folders folders in a file called Folders.xml	
Group Policy Preferences-Ini Files	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Inifiles or User\Preferences\Inifiles folders in a file called IniFiles.xml	
Group Policy Preferences-Registry	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Registry or User\Preferences\Registry folders in a file called Registry.xml	
Group Policy Preferences-Network Shares	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\NetworkShares folder in a file called NetworkShares.xml	
Group Policy Preferences-Shortcuts	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Shortcuts or User\Preferences\Shortcuts folders in a file called Shortcuts.xml	

Group Policy Extension	Storage Location	Comments
Group Policy Preferences-Data Sources	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\DataSources or User\Preferences\DataSources folders in a file called DataSources.xml	
Group Policy Preferences-Devices	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Devices or User\Preferences\Devices folders in a file called Devices.xml	
Group Policy Preferences-Folder Options	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\FolderOptions or User\Preferences\Options folders in a file called FolderOptions.xml	
Group Policy Preferences-Local Users and Groups	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Groups or User\Preferences\Groups folders in a file called Groups.xml	
Group Policy Preferences-Network Options	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\NetworkOptions or User\Preferences\NetworkOptions folders in a file called NetworkOptions.xml	
Group Policy Preferences-Power Options	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\PowerOptions or User\Preferences\PowerOptions folders in a file called PowerOptions.xml	
Group Policy Preferences - Printers	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Printers or User\Preferences\Printers folders in a file called Printers.xml	
Group Policy Preferences – Scheduled Tasks	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\ScheduledTasks or User\Preferences\ScheduledTasks folders in a file called ScheduledTasks.xml	
Group Policy Preferences - Services	Stored in Sysvol, under the GPT container for a given GPO, within either the Machine\Preferences\Services folder in a file called Services.xml	
Group Policy Preferences – Drive Maps	Stored in Sysvol, under the GPT container for a given GPO, within either the User\Preferences\Drives folder in a file called Drives.xml	

Group Policy Extension	Storage Location	Comments
Group Policy Preferences – Internet Settings	Stored in Sysvol, under the GPT container for a given GPO, within either the User\Preferences\InternetSettings folder in a file called InternetSettings.xml	
Group Policy Preferences-Regional Options	Stored in Sysvol, under the GPT container for a given GPO, within either the User\Preferences\RegionalOptions folder in a file called RegionalOptions.xml	
Group Policy Preferences-Start Menu	Stored in Sysvol, under the GPT container for a given GPO, within either the User\Preferences\StartMenuTaskbar folder in a file called StartMenuTaskbar.xml	
Group Policy Preferences-Devices	IE Maintenance settings were stored in SYSVOL under the GPT container for a given GPO. Specifically IE Maintenance settings were stored in the GPT under the \User\Microsoft\IEAK folder. IE Zonemapping settings, specifically the setting called Site to Zone Assignment under Administrative Templates, are stored in registry.pol in the GPT under the Machine or User folders.	IE Maintenance policy has been deprecated by Microsoft so you may not ever see these files again. IE Zonemapping is it's own Client Side Extension (CSE) and uses what's called an ExtensionGUID tag in the Inetres.admx file. ExtensionGUIDs are used in ADMX files when a policy area wants to use registry.pol to store it's settings, but requires extra logic to apply those registry entries. In the case of IE Zonemapping, zone mapping information is stored in multiple registry keys and the IE Zonemapping CSE fires up and does extra work to process those registry entries and apply them to IE.

Group Policy Extension	Storage Location	Comments
IP Security	<p>IP Sec policy is a special case—settings are stored as special objects strictly in AD but not within the GPC. Namely IPsec policy settings are stored under the CN=IP Security, CN=System container within a domain. So, IP Security settings are stored domain wide and can be referenced by any GPO in the domain. When you assign a particular IPsec policy to a GPO, an additional object is created within the GPC of the GPO—specifically, an ipsecPolicy object is created under the Machine\Microsoft\Windows container under the GPO. This object stores the association between the available IPsec policies in the domain and that GPO.</p>	
Name Resolution Policy	<p>Uses registry.pol to store settings under the Machine folder in the GPT.</p>	
Policy-based QoS	<p>Uses registry.pol to store settings under the Machine folder in the GPT.</p>	
Public Key Policy	<p>Uses registry.pol to store settings under either the Machine or User folder in the GPT</p>	
QoS Packet Scheduler	<p>Stored in SYSVOL, under the GPT container for a given GPO. QoS policy is also stored in registry.pol, however, you'll only find it in the copy of registry.pol stored under the machine folder, as this is a per-machine policy only.</p>	
Security Settings	<p>Stored in SYSVOL under the GPT container for a given GPO. Security settings are stored in the Machine\Microsoft\Windows NT\SecEdit folder in a file called GptTmpl.inf</p>	<p>The format of this file is identical to those created when you use the MMC security templates editor to create a security template. This policy area encompasses several different parts of the GP Editor namespace, including Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry (permissions) and File System (permissions).</p>

Group Policy Extension	Storage Location	Comments
Software Installation	Stored in both the GPC and GPT. Within the GPT, deployed package information is stored under the container machine (or user)\Applications, within an "Application Advertisement File" or .AAS file. Within the GPC, a special object of class packageRegistration is created for each application deployed. This object can be found in the GPC for a GPO under machine (or user)\Class Store\ Packages	packageRegistration objects found in the GPC contain information such as the path to the MSI file, any transforms (modifications) that have been selected and whether the application is published or assigned.
Software Restriction Policy	Uses registry.pol to store settings under the Machine or User folder in the GPT.	
Startup/Shutdown & Logon/Logoff Scripts	Stored in SYSVOL under the GPT container for a given GPO. Machine-specific scripts are stored in the machine\scripts\startup; machine\scripts\ shutdown folders. User-specific scripts are stored in the user\logon and user\ logoff folders.	Note that script files themselves do not have to be stored in SYSVOL. You can reference scripts located anywhere on your network, as long as they are accessible to the computer or user. The scripts.ini file found in the computer\scripts folder and user\scripts folder in SYSVOL contains the actual references to any scripts that you've defined.
Windows Firewall with Advanced Security	Stored under the Machine folder in SYSVOL, in registry.pol	
Wired (IEEE 802.3) Policies	Stored in AD (GPC) within the path CN=IEEE8023,CN=Windows,CN=Microsoft, CN=Machine	Wired policies are stored under the container specified, as objects of class ms-net-ieee-8023- GroupPolicy, where each one of these objects is created for each policy created.
Wireless (IEEE 802.11 Policies)	Stored in AD (GPC) within the path: CN=wireless,CN=Windows, CN=Microsoft,CN=Machine	Wireless policies are stored in AD (GPC) as objects of class msieee80211-Policy.

About SDM Software

Since 2006, SDM Software has been delivering advanced configuration governance solutions that help organizations secure their Windows environments and maintain business continuity both on premises and in the cloud. Solutions cover the full lifecycle of configuration management on Microsoft platforms, including reporting, migration, automation, auditing, change control, recovery, and compliance reporting. As experts in Group Policy and Intune, SDM Software helps optimize the configuration journey on Microsoft platforms for organizations of all sizes. Learn more at www.sdmsoftware.com