

Policy Analyzer

Version 3.2

Aaron Margosis
Microsoft Corporation
1 June 2016

Overview

Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). It can highlight when a set of Group Policies has redundant settings or internal inconsistencies, and can highlight the differences between versions or sets of Group Policies. It can also compare GPOs against current local policy settings and against local registry settings. And you can export its findings to a Microsoft Excel spreadsheet.

Policy Analyzer lets you treat a set of GPOs as a single unit. This makes it easy to determine whether particular settings are duplicated across the GPOs or are set to conflicting values. It also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.

For example, the US Government Configuration Baseline (USGCB) for Windows 7 includes seven different GPOs. Policy Analyzer can treat them as a single set, and show all the differences between them and the Microsoft recommended baselines for Windows 10 and Internet Explorer 11 with a single comparison. You can also use it to verify changes that were made to your production GPOs.

The following screenshot shows two baselines compared with each other and to corresponding registry values on the local system. The lower pane displays the Group Policy setting, location, and other information associated with the selected row. Conflicting settings are highlighted in yellow; absent settings are shown as a grey cell. Policy Analyzer also offers options to display only rows containing conflicts or other differences.

Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	STIG-Win10-2015-10-30	Win10-IE11-Baselin
HKCU	Software\Policies\Microsoft\Window...	No Toast Application Notification...		1	1
HKLM	Software\Microsoft\WcmSvc\wfinet...	AutoConnectAllowedOEM		0	0
HKLM	Software\Microsoft\Windows NT\Cu...	SecurityLevel	0	0	0
HKLM	Software\Microsoft\Windows NT\Cu...	CachedLogonsCount	10	10	4
HKLM	Software\Microsoft\Windows NT\Cu...	ScRemoveOption	0	1	1
HKLM	Software\Microsoft\Windows\Curren...	EnumerateAdministrators		0	0
HKLM	Software\Microsoft\Windows\Curren...	NoAutorun		1	1
HKLM	Software\Microsoft\Windows\Curren...	NoDriveTypeAutoRun		255	255
HKLM	Software\Microsoft\Windows\Curren...	NoWebServices		1	1
HKLM	Software\Microsoft\Windows\Curren...	ConsentPromptBehaviorAdmin	5	2	2
HKLM	Software\Microsoft\Windows\Curren...	ConsentPromptBehaviorUser	3	0	0
HKLM	Software\Microsoft\Windows\Curren...	DisableAutomaticRestartSignOn		1	1
HKLM	Software\Microsoft\Windows\Curren...	EnableInstallerDetection	1	1	1
HKLM	Software\Microsoft\Windows\Curren...	EnableLUA	1	1	1

Policy Path:
User Configuration
Start Menu and Taskbar\Notifications\
Turn off toast notifications on the lock screen

Local registry:
Not specified

STIG-Win10-2015-10-30:
Option: Enabled
Data: 1
Type: REG_DWORD

Win10-IE11-Baselines-DRAFT:
Option: Enabled
Data: 1
Type: REG_DWORD

The following screenshot shows Policy Analyzer's Excel output. Policy Analyzer sorts results primarily by the Group Policy path and setting name columns, which are the leftmost columns.

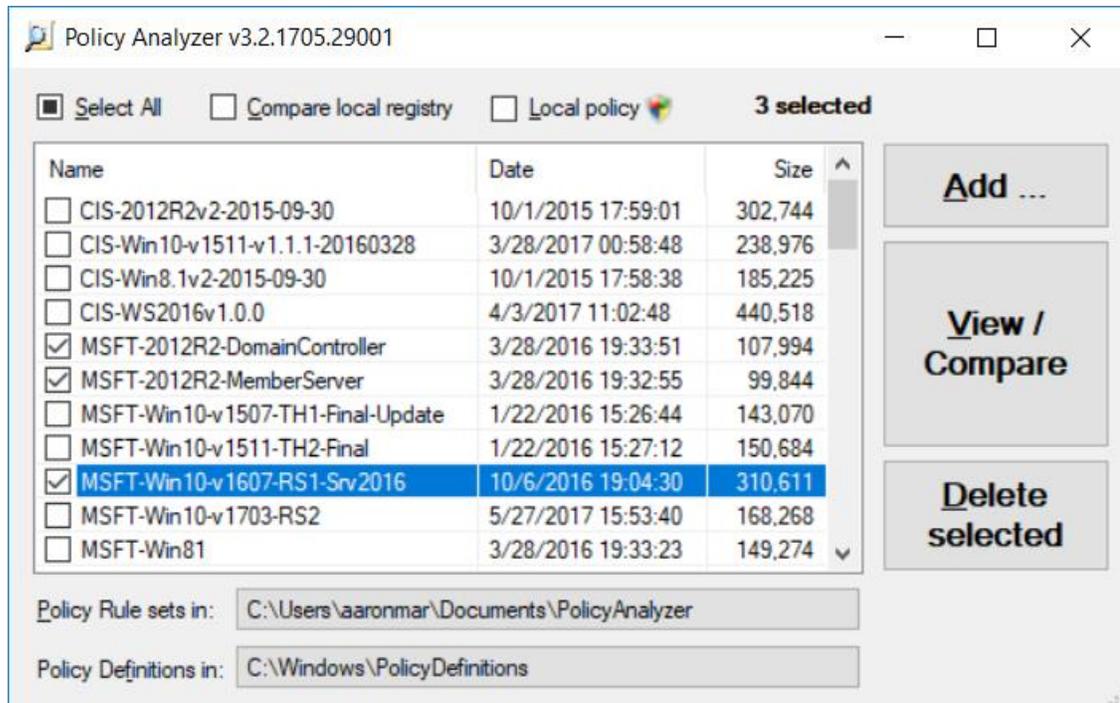
Policy Path	Policy Setting Name	Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	STIG-Win10-2015-10-30 Option
Advanced Audit Policy Conf\Audit Policy\Privilege Use	Sensitive Privilege Use	Audit Policy	Privilege Use	Sensitive Privilege Use		Success and Failure
Advanced Audit Policy Conf\Audit Policy\System	IPsec Driver	Audit Policy	System	IPsec Driver		Success and Failure
Advanced Audit Policy Conf\Audit Policy\System	Other System Events	Audit Policy	System	Other System Events		Success
Advanced Audit Policy Conf\Audit Policy\System	Security State Change	Audit Policy	System	Security State Change		Success and Failure
Advanced Audit Policy Conf\Audit Policy\System	Security System Extension	Audit Policy	System	Security System Extension		Success and Failure
Advanced Audit Policy Conf\Audit Policy\System	System Integrity	Audit Policy	System	System Integrity		Success and Failure
User Configuration\Windows Components\Attachment Manager	Do not preserve zone information in file attachments	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\DoNotPreserveZoneInformation	Do not preserve zone information in file attachments		Disabled
User Configuration\Windows Components\Attachment Manager	Notify antivirus programs when opening files	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\NotifyAntivirus	Notify antivirus programs when opening files		Enabled
User Configuration\Windows Components\Network Sharing	Prevent users from sharing files within the network	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\PreventSharing	Prevent users from sharing files within the network		Enabled
User Configuration\Windows Components\Internet Explorer	Disable changing certificate settings	HKCU	Software\Policies\Microsoft\Internet Explorer\Feeds\DisableChangingCertificateSettings	Disable changing certificate settings		[Multiple possible]
User Configuration\Windows Components\Internet Explorer	Disable AutoComplete for forms	HKCU	Software\Policies\Microsoft\Internet Explorer\Feeds\DisableAutoCompleteForForms	Disable AutoComplete for forms		[Multiple possible]
User Configuration\Windows Components\Internet Explorer	Turn on the auto-complete feature for user names and passwords	HKCU	Software\Policies\Microsoft\Internet Explorer\Feeds\TurnOnAutoCompleteForUserNamesAndPasswords	Turn on the auto-complete feature for user names and passwords		Disabled
User Configuration\Windows Components\Internet Explorer	Turn on the auto-complete feature for user names and passwords	HKCU	Software\Policies\Microsoft\Internet Explorer\Feeds\TurnOnAutoCompleteForUserNamesAndPasswords	Turn on the auto-complete feature for user names and passwords		False
User Configuration\Windows Components\Internet Explorer	Turn on the auto-complete feature for user names and passwords	HKCU	Software\Policies\Microsoft\Internet Explorer\Feeds\TurnOnAutoCompleteForUserNamesAndPasswords	Turn on the auto-complete feature for user names and passwords		Enabled
User Configuration\Control Panel\Personalization	Enable screen saver	HKCU	Software\Policies\Microsoft\Windows\ScreenSaver\ScreenSaverActive	Enable screen saver		Enabled
User Configuration\Control Panel\Personalization	Password protect the screen saver	HKCU	Software\Policies\Microsoft\Windows\ScreenSaver\ScreenSaverSecure	Password protect the screen saver		Enabled
User Configuration\Control Panel\Personalization	Screen saver timeout	HKCU	Software\Policies\Microsoft\Windows\ScreenSaver\ScreenSaverTimeout	Screen saver timeout		Enabled
User Configuration\Control Panel\Personalization	Force specific screen saver	HKCU	Software\Policies\Microsoft\Windows\ScreenSaver\ScreenSaverEexe	Force specific screen saver		Enabled
Computer Configuration\Start Menu and Taskbar\Notifications	Turn off toast notifications on the lock screen	HKCU	Software\Policies\Microsoft\Windows\CurrentVersion\TaskbarAndStartMenu\TurnOffToastNotificationsOnLockScreen	Turn off toast notifications on the lock screen		Enabled
Computer Configuration\System\Internet Communication Management	Turn off Internet download for Web	HKLM	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\TurnOffInternetDownloadForWeb	Turn off Internet download for Web		Enabled
Security Settings\Local Policies\Security Options	User Account Control: Behavior of the elevation prompt for administrators (standalone)	HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System\UACBehaviorOfTheElevationPromptForAdministrators	User Account Control: Behavior of the elevation prompt for administrators (standalone)	5	2
Security Settings\Local Policies\Security Options	User Account Control: Behavior of the elevation prompt for standard users	HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System\UACBehaviorOfTheElevationPromptForStandardUsers	User Account Control: Behavior of the elevation prompt for standard users	5	2
Security Settings\Local Policies\Security Options	Interactive logon: Number of previous logons that can be cached	HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	Interactive logon: Number of previous logons that can be cached	0	10
Security Settings\Local Policies\Security Options	Interactive logon: Smart card removal behavior	HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SmartCardRemovalBehavior	Interactive logon: Smart card removal behavior	0	6
Computer Configuration\Windows Components\Credential Management	Enumerate administrator accounts on elevation	HKLM	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\EnumerateAdministrators	Enumerate administrator accounts on elevation	0	Disabled
Computer Configuration\Windows Components\AutoPlay Policies	Set the default behavior for AutoRun	HKLM	Software\Microsoft\Windows\CurrentVersion\AutoPlay\NoAutorun	Set the default behavior for AutoRun	1	Do not execute any commands
Computer Configuration\System\Internet Communication Management	Restrict Internet communication	HKLM	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds\RestrictInternetCommunication	Restrict Internet communication	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Detect application installations from trusted sources	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Detect application installations from trusted sources	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Detect application installations from trusted sources	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Detect application installations from trusted sources	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Run all administrators in Admin Approval Mode	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Run all administrators in Admin Approval Mode	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Only elevate UIAccess applications that are installed in protected areas	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Only elevate UIAccess applications that are installed in protected areas	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Allow UIAccess applications to be installed in protected areas	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Allow UIAccess applications to be installed in protected areas	1	Enabled
Security Settings\Local Policies\Security Options	User Account Control: Virtualize file and registry settings for applications that do not request elevation	HKLM	Software\Microsoft\Windows\CurrentVersion\UAC\UACBehaviorOfTheElevationPromptForTrustedSources	User Account Control: Virtualize file and registry settings for applications that do not request elevation	1	Enabled

Policy Analyzer is a lightweight standalone application that doesn't require installation, and doesn't require administrative rights (except for the "local policy" feature, described later).

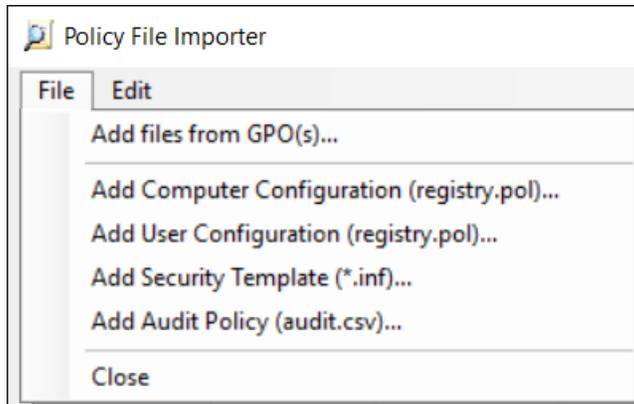
Adding Policy Rule sets

A Policy Analyzer *Policy Rule set* is a single XML file with a *.PolicyRules file extension, and containing data collected from GPO files that you identify. A single Policy Rule set can contain data from any number of GPO files from any number of GPOs.

Run PolicyAnalyzer.exe. The list box shows Policy Rule sets in the directory named by the “Policy Rule sets in” label (see screenshot). Initially this directory will be empty. (You can prepopulate it with the sample PolicyRules files included in the zip file.) On startup, this will be a PolicyAnalyzer subdirectory of your Documents directory. Click on the directory name to change to a different directory.



To add a Policy Rule set to the Policy Analyzer collection, click the *Add...* button in the main window to open the Policy File Importer dialog box. Add files to include in the rule set using the Importer’s File menu, shown in the screenshot below. The quickest way to add files to the set is to choose *Add files from GPO(s)...* and select a directory which contains one or more GPO backups. Policy Analyzer identifies the backups and adds files to the set, with policy names also taken from the backup. You can also add policy files one at a time using the other “Add” options.

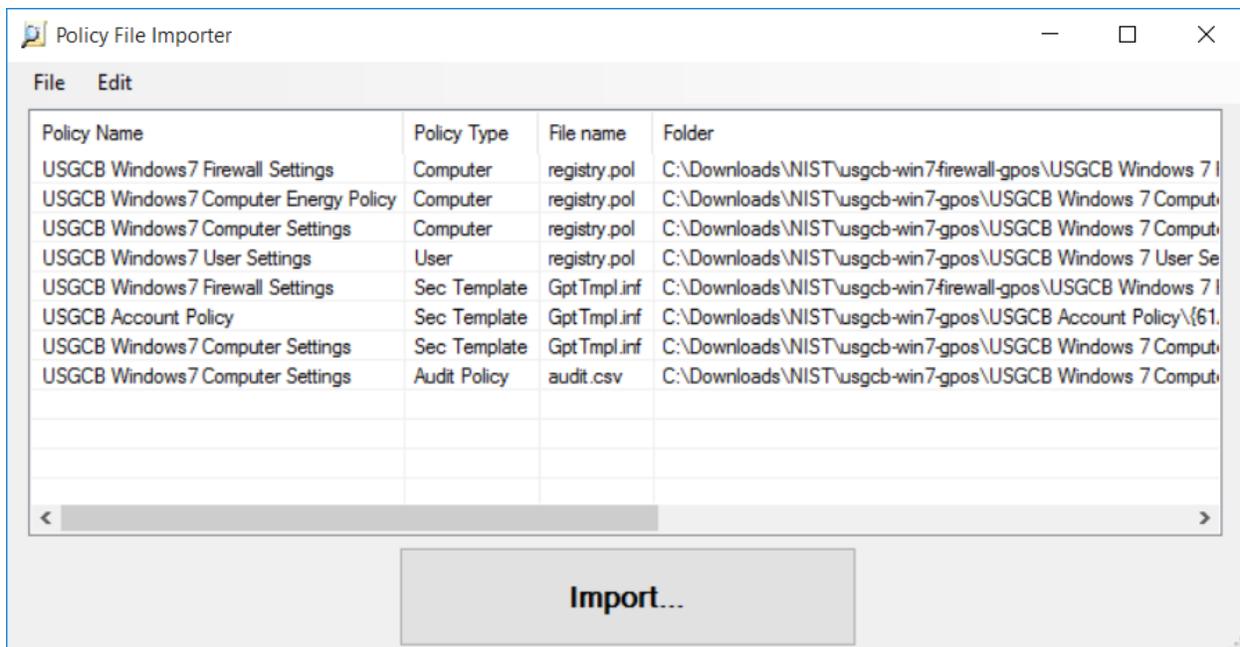


Policy Analyzer can ingest three types of GPO files: registry policy files, security templates, and audit policy backup files. The format of registry policy files (typically “registry.pol”) is a [documented](#), binary file format, normally produced by Group Policy editors such as GpEdit.msc. Registry policy files contain registry commands relative to an unspecified root key, and do not contain information explicitly indicating whether they are targeted for Computer Configuration (HKLM) or User Configuration (HKCU). The target root key is derived by the registry.pol file’s being in a “Machine” or “User” directory. Registry policy files contain settings from several sections of GPO editors, most notably the Computer and User Administrative Templates sections, Windows Firewall with Advanced Security, and Application Control Policies (AppLocker). If you add a registry policy file individually, you must specify whether it should be treated as a Computer or User Configuration file.

Security template files (usually “GptTmpl.inf”) are text files in the old Windows 3.x “.ini” file format. Security template files typically contain settings from the Account Policies and Local Policies sections under Computer Configuration\Windows Settings\Security Settings in the GPO editor. These settings include password policy, account lockout policy, *legacy* audit policy, user rights assignments, and security options.

Audit policy backup files (usually “audit.csv”) are comma-separated values (CSV) text files. They contain data representing the settings in the Advanced Audit Policy Configuration folder under Security Settings.

If you add files using *Add files from GPO(s)...*, Policy Analyzer identifies GPO names from files in the GPO backup or backups. If you pick files using the other options, Policy Analyzer sets the file’s policy name to a placeholder value. You can change the policy name associated with a file by selecting the row and pressing F2 or by double-clicking the name, and then typing in the name of your choice. To remove a file from the set before importing, select the row and press the Del key or choose *Delete* from the Edit menu. After you have selected all the files you want to include and are satisfied with the policy names associated with those files, click the Import button and enter a file name in which to save the set. Policy Analyzer ingests the content of the specified files, canonicalizes it and saves it as an XML file with a .PolicyRules file extension. When you add a file to the collection, Policy Analyzer automatically checks the box next to the file in the list so that you can view it immediately (optionally with other policy rule sets) by clicking the View/Compare button.



You can include as many GPOs in a single GPO set as you want. Typically it can make sense to treat GPOs that are applied together as a single set. Note that if you include multiple GPOs in a GPO set, Policy Analyzer does not attempt to determine precedence order between the GPOs. Policy Analyzer can show when a set of GPOs contains contradictory settings, but it will not predict which setting will “win.”

Using Policy Analyzer to view and compare baselines

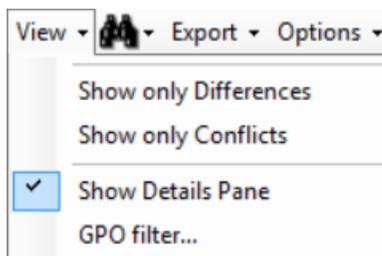
Enable one or more of the Policy Rule sets’ checkboxes and click View/Compare to open the Policy Viewer shown earlier. The Policy Viewer lists all the settings configured by the policy sets and the values configured by each policy set in its own column. The cell background is yellow if any two policy sets configure the value differently. A grey background with no text indicates that the policy set in that column does not configure the setting. A white background indicates that the policy set configures the setting and that no other policy set configures that setting to a different value. A light grey background in a cell indicates that the policy set defines the same setting multiple times, typically in different GPOs. The Details Pane in the lower section of the window identifies the path (or paths) in the Group Policy Object editor that can configure the selected setting, the GPO option or options associated with the selected values, the underlying data type, and any other available information. As an example of “other available information,” if the values represent security descriptors or security identifiers, Policy Analyzer translates them into human-readable form (or nerd-readable form, anyway ☺). Note that if two policies configure the same registry value to “5”, but one sets it as a numeric value and the other as a text string value, Policy Analyzer will flag this difference (REG_DWORD vs. REG_SZ). You can view additional information about the GPOs associated with each setting by enabling *Show GPO names [and files] in Details pane* and *Show explanation text for settings* in the Options menu.

If you enable the *Compare local registry* checkbox option in the Policy Analyzer main window, Policy Analyzer adds a “Local registry” column to the Policy Viewer and populates it with local registry data corresponding to the registry values configured by the other policy sets. A grey-background cell indicates that the registry value does not exist or that Policy Analyzer could not read it.

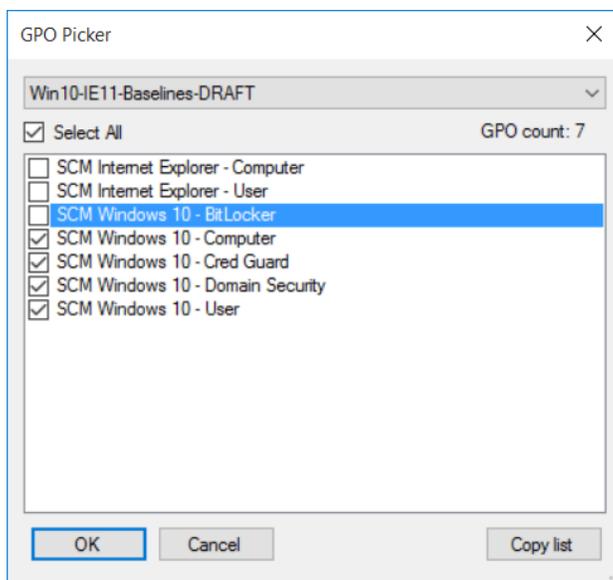
Enable the *Local policy* checkbox option to capture the current local group policy as a new policy set and add it as a column in the Policy Viewer. Capturing local policy requires administrative rights, so Policy Analyzer launches a helper app that requires elevation. The policy snapshot is added to the policy rules list with a name incorporating the computer name with the date and time of the capture. (See the Technical Notes section later in this document for details about what is included in the snapshot.)

All columns in the Policy Analyzer list can be sorted by clicking their headers, and can be reordered by dragging the headers to new positions. You can hide the Details Pane by toggling the *Show Details Pane* option in the View menu.

Because one of the Policy Analyzer's main purposes is to identify differences between sets of policies, the View menu enables you to hide settings that are the same. Enable *Show only Differences* to hide all rows that have the same value across all policy sets. Enable *Show only Conflicts* to show only those rows in which different values are configured. Put another way, *Show only Differences* shows rows that have any grey or yellow cells; *Show only Conflicts* shows only rows that have yellow-background cells.



Select *GPO filter* from the View menu to view a subset of the GPOs in a selected column. In the screenshot below, the "Win10-IE11-Baselines-DRAFT" policy set is selected in the Policy Rule Set dropdown and shows that it consists of 7 GPOs. Select policy rule sets from the dropdown and uncheck any GPOs that you do not want to include in the Policy Viewer list. This enables you to focus on specific GPOs in the comparison. Click *Copy list* to copy the displayed list of GPOs to the clipboard as text.



You can search for entries using the binoculars icon menu, or Ctrl+F and F3, and entering a search term in the Find dialog box. Policy Viewer will begin or resume search from the currently-selected row, and search for the text in the displayed list as well as in group policy paths and names associated with the entries.

The *Export* menu enables you to export data from the Policy Viewer to an Excel spreadsheet. *Export table to Excel* exports only the data in the table view. *Export all data to Excel* includes data shown in the Details Pane, including GPO paths, option names, and data types, as well as the information selected by the Options menu.

To translate registry values to Administrative Templates GPO paths and names, Policy Analyzer reads all the ADMX files from the directory identified by the “Policy Definitions in” label at the bottom of Policy Analyzer’s main window, and corresponding language-specific ADML files from its subdirectories. The local %windir%\PolicyDefinitions directory is selected by default. You can choose a different set of ADMX files by clicking the directory name and selecting a different path, which can be a network share such as a central store. Note that this will affect only new View/Compare operations, not already-displayed results.

Policy Analyzer makes every effort to use the ADML files from the user’s preferred UI language. If Policy Analyzer cannot find an ADML file from the user’s language subdirectory, Policy Analyzer looks in the EN-US and finally in the EN subdirectory. Policy Analyzer also tries to use the operating system’s main language when displaying other settings, but some text is hardcoded in English.

Splitting and merging policy files

Policy Analyzer comes with two PowerShell scripts, Split-PolicyRules.ps1 and Merge-PolicyRules.ps1.

Split-PolicyRules.ps1 splits the content of a “PolicyRules” file that represents multiple GPOs into separate files – one for each GPO. The -basename parameter becomes the base name of the new files, with the GPO names appended to that base name.

For example, the sample file MSFT-Win10-v1607-RS1-Srv2016.PolicyRules combines settings from eleven different GPOs, so Split-PolicyRules.ps1 produces eleven files from it, as shown here. Note that the -basename parameter can include an absolute or partial path as well as a name.

```
PS C:\demo> Split-PolicyRules.ps1 .\MSFT-Win10-v1607-RS1-Srv2016.PolicyRules .\targetDir\Win10v1607-WS2016
.\targetDir\Win10v1607-WS2016-SCM Internet Explorer 11 - User.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows Server 2016 - Domain Controller Baseline.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 and Server 2016 - Credential Guard.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 RS1 - User.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows Server 2016 - Member Server Baseline - Computer.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 RS1 - BitLocker.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 RS1 - Computer.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 and Server 2016 - Domain Security.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Internet Explorer 11 - Computer.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows Server 2016 - Member Server Baseline - User.PolicyRules
.\targetDir\Win10v1607-WS2016-SCM Windows 10 and Server 2016 - Defender.PolicyRules
```

Merge-PolicyRules.ps1 combines the content of two PolicyRules files into a one PolicyRules set, which is written to the pipeline. Redirect that output to a file using the > operator or the Out-File cmdlet. For example:

```
.\Merge-PolicyRules.ps1 .\RuleSetOne.PolicyRules .\RuleSetTwo.PolicyRules > .\RuleSetOneTwo.PolicyRules
```

Technical notes

Policy Analyzer consists of a primary executable, PolicyAnalyzer.exe, and two helper program files, PolicyRulesFileBuilder.exe and PolicyAnalyzer_GetLocalPolicy.exe. (Someday hopefully all packaged into a single executable, Sysinternals-style.) All three should be copied into the same directory.

PolicyAnalyzer.exe and PolicyAnalyzer_GetLocalPolicy.exe both require .NET Framework v4.6. Run only PolicyAnalyzer.exe.

Because most multi-valued settings are order-independent, Policy Analyzer canonicalizes multi-valued settings by sorting them alphabetically. This treats settings as identical when only the order is different. For example, if *SeSystemTimePrivilege* is set to “*S-1-5-19, *S-1-5-32-544” in one template and “*S-1-5-32-544, *S-1-5-19” in another, they produce the same end result, but a straight text comparison would show a difference. There are rare cases where multi-valued settings are order-dependent (such as “ECC Curve Order”), and as a result, actual differences can become masked. (I’ll work on this.)