

PolicyAnalyzer.exe v4.0

Group Policy Analyzer Utility

Overview

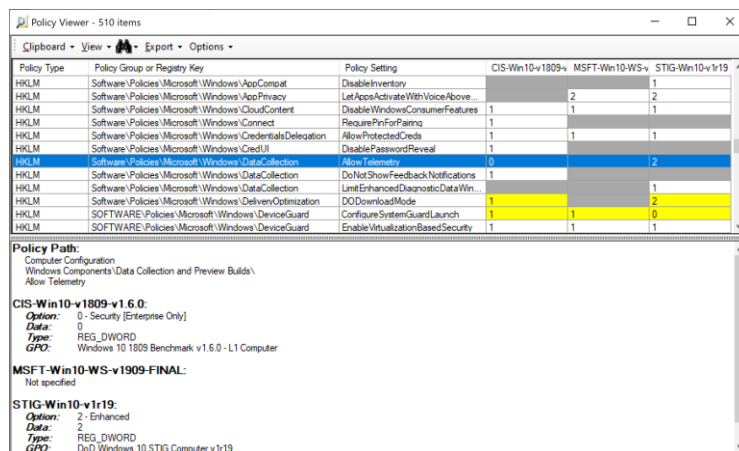
Policy Analyzer is a lightweight utility for analyzing and comparing sets of Group Policy Objects (GPOs). It can highlight when a set of Group Policies has redundant settings or internal inconsistencies and can highlight the differences between versions or sets of Group Policies. It can also compare one or more GPOs against local effective state. You can export all its findings to a Microsoft Excel spreadsheet.

Policy Analyzer lets you treat a set of GPOs as a single unit, and represents all settings in one or more GPOs in a single “.PolicyRules” XML file. You can also use .PolicyRules files with LGPO.exe v3.0 to apply those GPOs to a computer’s local policy, instead of having to copy GPO backups around.

Treating a set of GPOs as a single unit also makes it easy to determine whether particular settings are duplicated across the GPOs or are set to conflicting values. You can capture an initial set and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.

For example, the Microsoft-recommended baseline for Windows 10 version 1909 includes eight separate GPOs. Policy Analyzer can treat them as a single set, show all the differences between that set and the Microsoft-recommended baselines for Windows Server version 1909 with a single comparison. You can also use it to verify changes that were made to your production GPOs.

The following screenshot shows three baselines compared with one another. 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, and to display the setting’s help text in the lower pane.



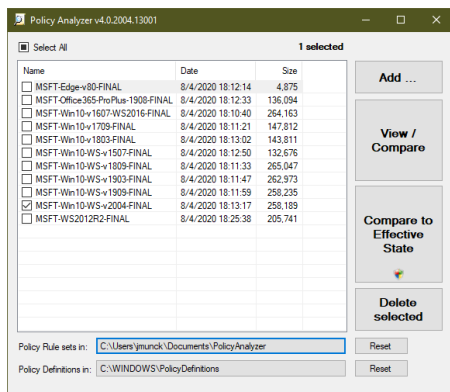
The following screenshot shows Policy Analyzer’s Excel output. Policy Analyzer sorts results primarily by the Group Policy path and setting name columns, which are the leftmost columns.

	A	B	C	D	E	F	G	H	I	J	K
	Policy Path	Policy Setting Name	Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	Local registry Option	Local registry Type			
1	Policy Config	Policy Path	Policy Setting Name	Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	Local registry Option	Local registry Type		
17	Advanced Audit Policy Config	Audit Policy/Privilege Use	Sensitive Privilege Use	Audit Policy	Privilege Use	Sensitive Privilege Use				STS0-Win10-2015-10-M	STS0-Win10-2015-10-M
18	Advanced Audit Policy Config	Audit Policy/System	Object Access	Audit Policy	System	Object Access				Success and Failure	Success and Failure
19	Advanced Audit Policy Config	Audit Policy/System	Other System Events	Audit Policy	System	Other System Events				Success and Failure	Success and Failure
20	Advanced Audit Policy Config	Audit Policy/System	Security State Change	Audit Policy	System	Security State Change				Success	Success
21	Advanced Audit Policy Config	Audit Policy/System	Security System Extension	Audit Policy	System	Security System Extension				Success and Failure	Success and Failure
22	Advanced Audit Policy Config	Audit Policy/System	System Integrity	Audit Policy	System	System Integrity				Success and Failure	Success and Failure
23	User Configuration	Windows Components/Attachment Manager	Do not preserve zone information in file attachments	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Do not preserve zone information in file attachments				Disabled	Disabled
24	User Configuration	Windows Components/Attachment Manager	Notify antivirus programs when opening attachments	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Notify antivirus programs when opening attachments				Enabled	Enabled
25	User Configuration	Windows Components/Network Sharing	Prevent users from sharing files within the network	HKCU	Software\Microsoft\Windows\CurrentVersion\Network Sharing\Sharing	Prevent users from sharing files within the network				Enabled	Enabled
26	User Configuration	Windows Components/Internet Explorer	Disable changing certificate settings	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Disable changing certificate settings				Multiple possible	Multiple possible
27	User Configuration	Windows Components/Internet Explorer	Disable AutoComplete for forms	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Disable AutoComplete for forms				Disabled	Disabled
28	User Configuration	Windows Components/Internet Explorer	Turn on the auto-complete feature for user	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Turn on the auto-complete feature for user				Multiple possible	Multiple possible
29	User Configuration	Windows Components/Internet Explorer	Turn on the auto-complete feature for user	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Turn on the auto-complete feature for user				Disabled	Disabled
30	User Configuration	Windows Components/Internet Explorer	Turn on the auto-complete feature for user	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Turn on the auto-complete feature for user				False	False
31	User Configuration	Windows Components/Internet Explorer	Disable AutoComplete for forms	HKCU	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Feeds	Disable AutoComplete for forms				Enabled	Enabled
32	User Configuration	Control Panel/Personalization	Enable screen saver	HKCU	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Enable screen saver				Enabled	Enabled
33	User Configuration	Control Panel/Personalization	Password protect the screen saver	HKCU	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Password protect the screen saver				Enabled	Enabled
34	User Configuration	Control Panel/Personalization	Screen saver timeout	HKCU	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Screen saver timeout				Enabled	Enabled
35	User Configuration	Control Panel/Personalization	Force specific screen saver	HKCU	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Force specific screen saver				Enabled	Enabled
36	User Configuration	Start Menu and Taskbar/Notifications	Turn off toast notifications on the lock screen	HKCU	Software\Microsoft\Windows\CurrentVersion\Start Menu and Taskbar\Notifications	Turn off toast notifications on the lock screen				Enabled	Enabled
37	Computer Configuration	Local Policies/Security Options	Secure Windows Firewall	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Secure Windows Firewall				Enabled	Enabled
38	Security Settings	Local Policies/Security Options	Recovery console: Allow automatic admin	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Recovery console: Allow automatic admin				REG_DWORD	REG_DWORD
39	Security Settings	Local Policies/Security Options	Interactive logon: Number of previous logons	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Interactive logon: Number of previous logons				REG_DWORD	REG_DWORD
40	Security Settings	Local Policies/Security Options	Interactive logon: Smart card and removable media	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Interactive logon: Smart card and removable media				REG_DWORD	REG_DWORD
41	Computer Configuration	Windows Components/Credential User	Enumerate administrator accounts on elev	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Enumerate administrator accounts on elev				Disabled	Disabled
42	Computer Configuration	Windows Components/Credential User	Enumerate administrator accounts on elev	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Enumerate administrator accounts on elev				Do not include any	Do not include any
43	Computer Configuration	Windows Components/AutoPlay Policies	Turn off AutoPlay	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Turn off AutoPlay				All drives	All drives
44	Computer Configuration	System/Internet Communication	Restrict Internet communication	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Restrict Internet communication				Enabled	Enabled
45	Security Settings	Local Policies/Security Options	Turn off Internet download for Web	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Turn off Internet download for Web				Enabled	Enabled
46	Security Settings	Local Policies/Security Options	User Account Control: Behavior of the elevated	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Behavior of the elevated				REG_DWORD	REG_DWORD
47	Computer Configuration	Windows Components/Windows Defender	Turn on Windows Defender	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	Turn on Windows Defender				REG_DWORD	REG_DWORD
48	Security Settings	Local Policies/Security Options	User Account Control: Detect application	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Detect application				REG_DWORD	REG_DWORD
49	Security Settings	Local Policies/Security Options	User Account Control: Run all administrative	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Run all administrative				REG_DWORD	REG_DWORD
50	Security Settings	Local Policies/Security Options	User Account Control: Only elevate UIAccess	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Only elevate UIAccess				REG_DWORD	REG_DWORD
51	Security Settings	Local Policies/Security Options	User Account Control: Allow UIAccess app	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Allow UIAccess app				REG_DWORD	REG_DWORD
52	Security Settings	Local Policies/Security Options	User Account Control: Virtualize file and re	HKLM	Software\Microsoft\Windows\CurrentVersion\Control Panel\Personalization	User Account Control: Virtualize file and re				REG_DWORD	REG_DWORD

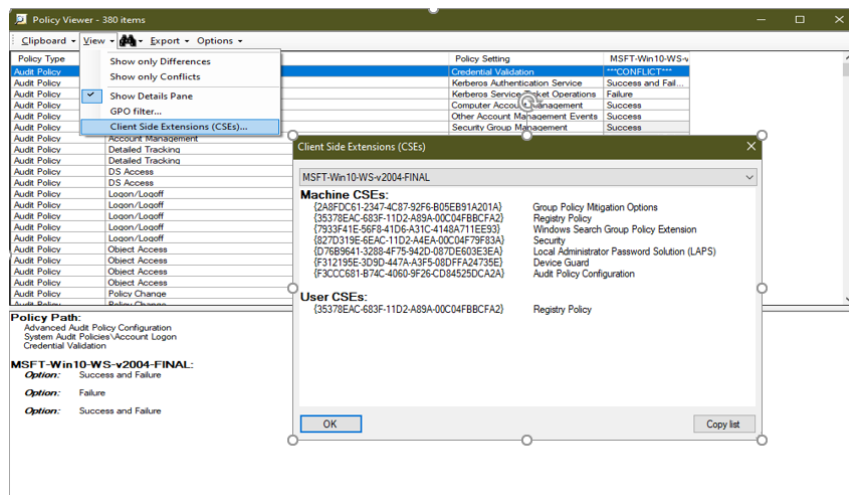
Policy Analyzer is a lightweight standalone application that doesn’t require installation, and doesn’t require administrative rights (except for the “Compare to Effective State” feature, described later).

What’s New in Version 4.0

The “Compare to Effective State” button has replaced the “Compare local registry” and “Local Policy” checkboxes that used to be in the Policy Analyzer main window. Press it to compare the selected baseline(s) to the current system state. If the selected baseline(s) contain any user configuration settings, they are compared against the current user’s settings. “Compare to Effective State” requires administrative rights if the selected baseline(s) include any security template settings or Advanced Auditing settings. The effective state corresponding to the selected baseline(s) settings are saved to a new policy rule set.



Policy Analyzer now captures information about Group Policy Client-Side Extensions (CSEs) when you import GPO backups. From a Policy Viewer window, choose View \ Client Side Extensions (CSEs) to view the Machine and User CSEs for each baseline in the Viewer. (Note that LGPO.exe’s improved support for CSEs includes the ability to apply CSE configurations from Policy Analyzer’s .PolicyRules files.)



Policy Analyzer now maps settings and sub-settings to display names more completely and more accurately, including mapping the GUIDs for Attack Surface Reduction (ASR) rules to their display names, and improved localization.

GPO2PolicyRules

You can now automate the conversion of GPO backups to Policy Analyzer .PolicyRules files and skip the GUI. GPO2PolicyRules is a new command-line tool that is included with the Policy Analyzer download. It takes two command-line parameters: the root directory of the GPO backup that you want to create a .PolicyRules file from, and the path to the new .PolicyRules file that you want to create. For example:

```
GPO2PolicyRules.exe C:\BaselinePkg\GPOs C:\Users\Analyst\Documents\PolicyAnalyzer\baseline.PolicyRules
```

Terms of Use

Terms of Use have been included in the download.

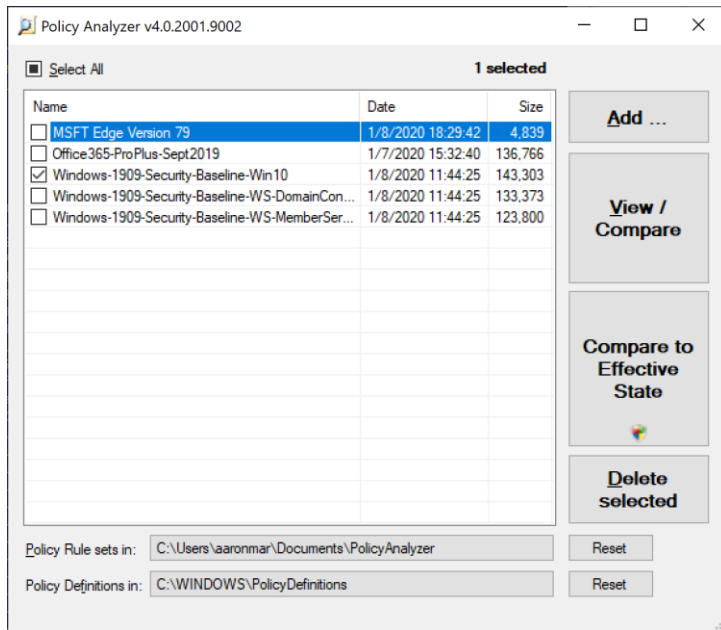
Adding Policy Rule sets

A Policy Analyzer *Policy Rule set* is a single XML file with a *.PolicyRules file extension, 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.

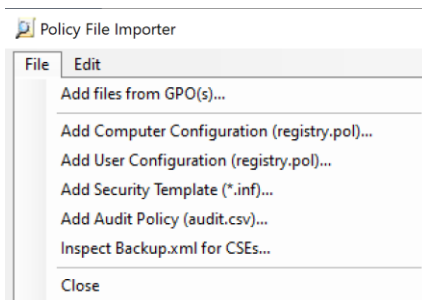
Policy Analyzer provides two ways to create .PolicyRules files. The new GPO2PolicyRules.exe command-line utility is the simpler way. The Policy Analyzer GUI is a little more complex but gives you the most flexibility.

Creating a PolicyRules file with the Policy Analyzer GUI

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. Click the Reset button next to it to set it back to the default 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 four types of GPO files: registry policy files, security templates, audit policy backup files, and backup.xml files that reference Group Policy client side extensions (CSEs) required by settings in the GPO. 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.

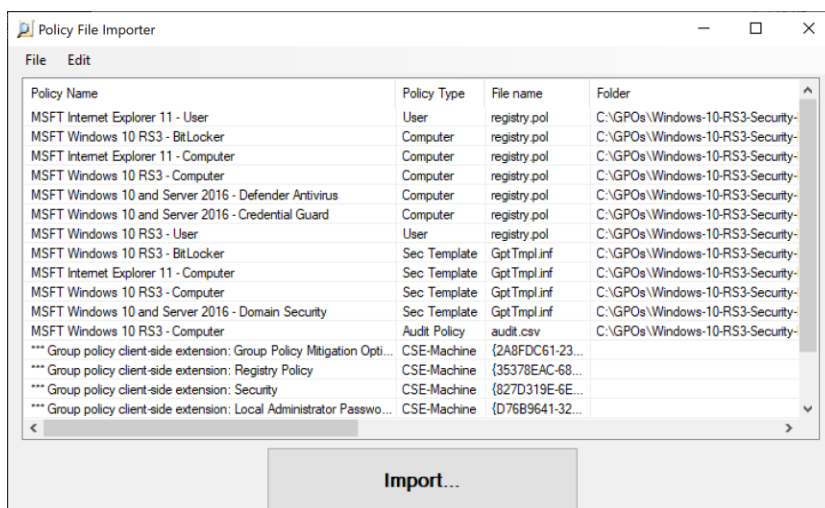
Security template files (usually “GptTmpl.inf”) are text files in the old Windows 3.x “.ini” file format. Security template files typically contain settings from the Account Policies and Local Policies sections under Computer Configuration\Windows Settings\Security Settings in the GPO editor. These settings 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.

Group Policy backups include a backup.xml file that among other things references the Group Policy client-side extensions (CSEs) required by settings in the GPO. A CSE is a DLL registered with the Group Policy engine on a managed computer and that performs additional actions beyond the simple setting of a registry value. Numerous GP settings require that a CSE be invoked to fully implement the policy’s intended effect.

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. (Note that editing the “Policy Name” value CSE entries has no effect on what gets saved.) 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, deleted any entries you don’t want, 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.”

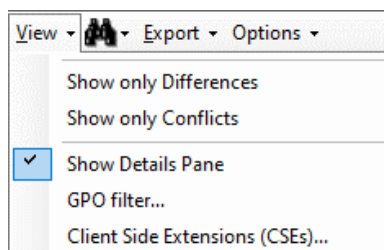
Using Policy Analyzer's Policy Viewer to view and compare baselines

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.

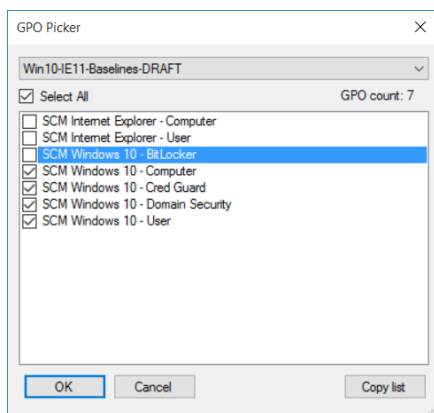
Enable one or more of the Policy Rule sets' checkboxes and click "Compare to Effective State" to compare the selected baselines against the local computer's current configured state. The operation will require UAC elevation if any of the selected baselines include security template or advanced auditing settings that require elevation to retrieve. The Policy Viewer will show the combined settings from all the selected Policy Rule sets in one column under the heading "Baseline(s)," and the corresponding current settings on the local computer and the logged-on user in a separate column under the heading "Effective state." The effective state settings are also saved to a new .PolicyRules file with a name combining "EffectiveState_," the current computer name, and the current date and time in the format "yyyyMMdd- HHmmss." For example, "EffectiveState_WKS51279_20200210-183947.PolicyRules."

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.

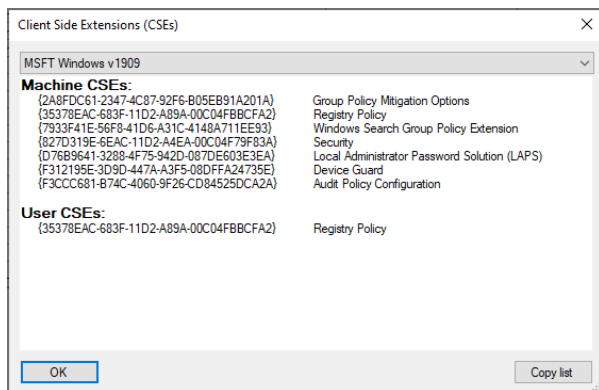
Because one of the Policy Analyzer's main purposes is to identify differences between sets of policies, the View menu enables you to hide settings that are the same. Enable *Show only Differences* to hide all rows that have the same value across all policy sets. Enable *Show only Conflicts* to show only 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.



Select *Client Side Extensions (CSEs)* from the View menu to review a list of the CSEs associated with the GPO backups in each column. Click *Copy list* to copy the displayed list of CSEs to the clipboard as text. (Note that earlier versions of Policy Analyzer did not capture information about CSEs, so the PolicyRules files they created will not report any CSEs.)



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.

Policy Viewer shows *****CONFLICT***** in a cell to indicate that the GPO set has multiple definitions for the setting that are not all the same. It reports `[[delete]]` to indicate that the GPO includes a command to delete the registry value if it exists, and `[[Delete all values]]` to indicate that the GPO includes a command to delete all values within a key. Several GPOs that manage lists of settings will delete all values within a key before setting the values in the list.

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.

The current version of Policy Analyzer covers most areas of Group Policy, but does not yet include support for analysis of Group Policy Preferences, nor of startup, shutdown, logon, or logoff scripts.