

 PolicyMaker™ Standard Edition

---

Welcome to PolicyMaker Standard Edition. For a quick start with PolicyMaker, please review the following topics:

1. [Installation](#)
  2. [Group Policy Concepts](#)
  3. [PolicyMaker Concepts](#)
  4. [Troubleshooting](#)
  5. [Licensing](#)
  6. [Support](#)
- 

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Support

---

Hours: 8:00 am to 8:00 pm ET (GMT -5) weekdays

Phone: 1.603.433.5885

Web/Email: <http://www.desktopstandard.com/support>

### ◆ Before Contacting Support

Before contacting support, please obtain as much information as possible using existing PolicyMaker troubleshooting aids, including [trace options](#), [event logging](#), and [RSoP logging](#). The [online knowledge base](#) and [support forums](#) are also valuable support resources.

In order to expedite support for troubleshooting problems, please have available an image or the full text of any error messages, the context of a given problem, including affected platform(s) and how to reproduce the problem. For client problems, it is generally helpful to provide a copy of the [XML configuration data](#) that produces the problem, trace output, event log messages, and RSoP reporting data as available.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Licensing

---

### Purchasing

Contact DesktopStandard sales at <http://www.desktopstandard.com/sales> or 1.603.433.5885, or an authorized DesktopStandard Value Added Reseller, to obtain a free Evaluation license keyset or to purchase software licenses and obtain a Registered license keyset.

### Operating Modes

PolicyMaker usage is controlled by two types of license keys - Registered and Evaluation. Without a key, PolicyMaker runs in Demonstration mode. Each mode is subject to the limitations described in the "PolicyMaker End User License Agreement" (EULA). In Demonstration mode, PolicyMaker Client Side Extension(s) (CSE) are limited to performing configurations from a Local GPO only. With a Registered or Evaluation license key, PolicyMaker is subject to the functional limitations specified by the key.

#### Tip

A license file is not required for Group Policy Object Editor or RSoP snap-in extension operation - or for promotional extensions such as the Registry extension.

### Requesting a License Key

A license key request file may be generated within PolicyMaker from the [License Request](#) property page on the licensing property sheet that is launched from the PolicyMaker -> Licensing... menu bar option. This sheet provides a domain and OU browser as well as an Active Directory object counter, which together allow you to determine the licenses required and to format the request appropriately. Generally a license request file is saved to the desktop, using the export button, and sent to DesktopStandard or a reseller via email. Requests are saved to the following location for future use.

[%AllUsersProfile%\Application Data\DesktopStandard\PolicyMaker\request.xml](#)

### Importing a License Key

Generally a license key file is provided via email, and imported into PolicyMaker using the [Local License](#) property page on the licensing property sheet that is launched from the PolicyMaker -> Licensing... menu bar option. This option is available whenever any PolicyMaker item is selected within the GPO editor. The Local License property page always reflects the state of the locally saved license file, not the license file in use by a GPO. Once the license file is imported via the licensing property sheet, it will be saved to the local computer in the following location upon selection of Apply/OK from the property sheet:

[%AllUsersProfile%\Application Data\DesktopStandard\PolicyMaker\license.xml](#)

#### Applying a key to a GPO

Upon every save event, the license key is automatically merged from the above location into the GPO location listed below. Note that each non-Local GPO must have a current license key in order to process policy. After you import a new or upgraded license key, a save event must occur in every GPO where PolicyMaker settings (for the product(s) in question) are applied. To force a save event, open any PolicyMaker item's property sheet and hit OK.

This is generally only an issue following a license key upgrade or change. The changed key is not automatically applied to all GPOs, and there is currently no automated process to distribute it to all GPOs. If the resulting key file is the same for all GPOs, the file may be simply copied into the GPOs in the SYSVOL path, as shown below - in which case it is not required to force a change in each GPO.

### Viewing a GPO's License Key

Each PolicyMaker save to a non-Local GPO will copy the license file to the following location within the GPT:

[{GPO ID}\PolicyMaker\license.xml](#)

As long as the non-Local GPO contains a valid license file, the CSE will process policy according to that license. If a GPO does not contain a license file, its policy will not be processed by the CSE and an event log error will result. To view any GPO's license file, use the [GPO License](#) property page on the licensing property sheet that is launched from the PolicyMaker -> Licensing... menu bar option.

#### Tip

The license file can be added to the GPO from one location, by one administrator, and others may edit the GPO. Alternatively, the license file may be distributed to administrators using Group Policy.

### Viewing a GPO's Current License Key

The license key that resides within any GPO may be viewed within PolicyMaker from the [GPO License](#) property page on the licensing property sheet that is launched from the PolicyMaker -> Licensing... menu bar option. Note that this license key is dynamically updated from the contents of the local license file following any change to PolicyMaker

settings in the GPO.

### Licensing Restrictions

The license key may restrict usage by date, location, and quantity of managed directory objects. Functionally, Registered and Evaluation license keys are identical. Before processing policy for a list of GPOs, each PolicyMaker CSE validates the license key in each non-Local GPO and processes each of the keys' restrictions. Restrictions are calculated as follows.

#### Date

If the date (in local time) of the computer on which a PolicyMaker CSE is processing is greater than the date specified in the license.xml for a given GPO, the CSE will not process policy for that GPO.

#### Location

Locations may be licensed by domains and/or organizational units. A CSE will not process policy for a given GPO unless the user (for user policy) or computer (for computer policy) is in or under a licensed location.

#### Quantity

Quantity is calculated by the "PolicyMaker License" CSE during background refresh. Each CSE uses this information to determine if the number of non-disabled user (for user policy) or computer (for computer policy) objects contained under the relevant Location (see above) exceeds the licensed quantity for that location. A CSE will not process policy for that GPO if the licensed quantity is exceeded. Note that PolicyMaker does not keep a list of license usage and therefore relies on a current Active Directory object count.

#### Note

If a CSE prohibits policy processing for any licensing reasons, a license error is written to the computer's system event log and previous execution RSoP data for the CSE is left unchanged, so as to reflect the current state of policy.

#### Grace Period

A fourteen (14) day grace period is implemented for license quantity excess. If quantity is exceeded, CSEs will report a warning to the [event log](#) while operating within 14 days of the last successful license check. If the grace period is exceeded the CSEs will not process policy for the GPO and an error will be written to the event log.

#### Reducing Active Directory Object Counts

If the current count of objects in an Active Directory container exceeds the licensed count, policy is processed for that container on clients (producing a license warning or error), and the number of objects in that container is then reduced within compliance with the licensed quantity, client-side processing will take up to 24 hours to recognize the correction due to quantity caching.

## Installation

### Components

PolicyMaker consists of three main components, Group Policy Object Editor (GPOE) snap-in extensions, Resultant Set of Policy (RSoP) snap-in extensions, and Client Side Extensions (CSE). All components are installed by the main product installation (polmkr.msi), however CSEs should be distributed to other computers using the much smaller polmkrcl.msi.

Although PolicyMaker components comply fully with Microsoft's documented interface specifications for extending Group Policy, they do not come pre-installed with Windows. Software installation policy provides an ideal mechanism for distributing both the snap-in and client side extensions. Administrative Templates policy is used to configure and restrict access to both snap-in and client side extensions.

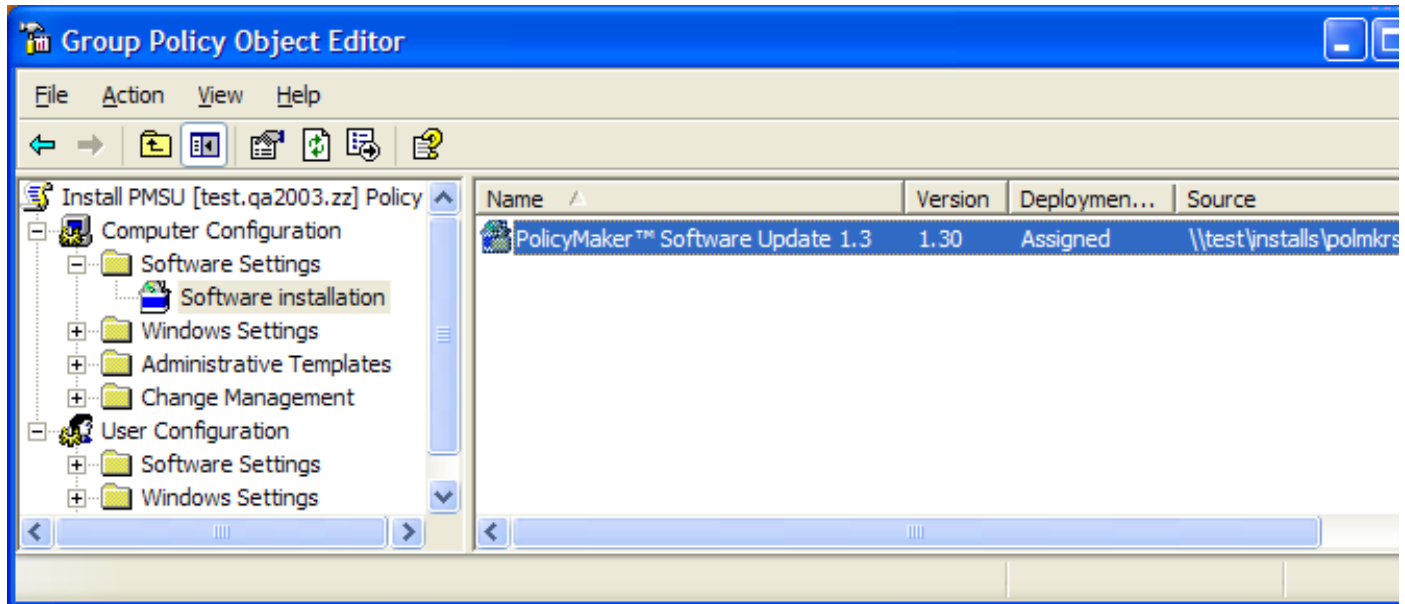
### Snap-in Extensions

The PolicyMaker snap-in extensions are installed by running the polmkr.msi package (the main installation that is downloaded from the DesktopStandard Internet web site). There are eleven unique extensions, to both the GPOE and RSoP snap-ins, corresponding to Client Side Extensions (CSE). Several of these extend both user and computer policy. Additionally, in italics, there are four placeholder snap-in extensions to both the GPOE and RSoP snap-ins. These placeholders provide no client-side functionality or reporting respectively.

Extension	User	Computer	GPOE CLSID	RSoP CLSID
Applications	x		{0DA274B5-EB93-47A7-AAFB-65BA532D3FE6}	{0E2CF4C8-5BB5-419F-9895-96228B5}
Data Sources	x	x	{1612b55c-243c-48dd-a449-ffc097b19776}	{12922C44-556C-43A7-9095-5759C95}
Devices	x	x	{1b767e9a-7be4-4d35-85c1-2e174a7ba951}	{1391E5EF-1D22-428F-9450-E6DF363}
Display Options	x		{20807589-ec7-497a-ac8f-97c7aa1cfc28}	{1B5CE5CC-D1DE-47E6-9AA9-5909D9E}
Drive Maps	x		{2EA1A81B-48E5-45E9-8BB7-A6E3AC170006}	{2EA2B67A-ABAA-4D19-A6CB-0C646F2}
Environment Variables	x	x	{35141B6B-498A-4cc7-AD59-CE93D89B2CE}	{3046E3CB-FA17-48e1-B09E-AC9868E}
Files	x	x	{3BAE7E51-E3F4-41D0-853D-9BB9FD47605F}	{35431322-5EBA-4A37-B19A-751CFDC}
Folder Options	x	x	{3BFAE46A-7F3A-467B-8CEA-6AA34DC71F53}	{37D29921-6EAB-4F04-BAD7-2EAD7E1}
Folders	x	x	{3EC4E9D3-714D-471F-88DC-4DD4471AAB47}	{39B46312-7BE1-488A-B003-CBB3081}
Ini Files	x	x	{516FC620-5D34-4B08-8165-6A06B623EDEB}	{58E1F15D-8DAC-4CB7-B5B5-CB2597E}
Internet Settings	x		{5C935941-A954-4F7C-B507-885941ECE5C4}	{50C8721B-21B7-4DD0-A214-23B8536}
Local Users and Groups	x	x	{79F92669-4224-43CC-9C5C-6EFB4D87DF4A}	{62A5ACA2-C447-45F8-9A02-89567B1}
Mail Profiles	x		{8B20DDF0-9FF2-484E-A68B-2927421B7022}	{89A63B6D-E099-4E3E-BFEA-84EA9E7}
Network Options	x	x	{949FB894-E883-42C6-88C1-29169720E8CA}	{902713DE-1112-4174-BE22-53A75C1}
Power Options	x	x	{9AD2BAFE-63B4-4883-A08C-C3C6196BCAFD}	{9DAABB1C-6E81-41B0-93E3-02C2E1E}
Printers	x	x	{A8C42CEA-CDB8-4388-97F4-5831F933DA84}	{A1234588-3F91-404C-AE23-95A81EA}
Regional Options	x		{B9CCA4DE-E2B9-4CBD-BF7D-11B6EBFBDD7}	{AAE5F40F-606C-4C03-8860-C726CA7}
Registry	x	x	{BEE07A6A-EC9F-4659-B8C9-0B1937907C83}	{BD1D253A-2487-4B0E-AA01-3A7EB8C}
Scheduled Tasks	x	x	{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}	{C0876FA6-FAE9-4750-9339-DC0D251}
Services		x	{CC5746A9-9B74-4be5-AE2E-64379C86E0E4}	{C67355EA-6E7B-45a3-BC36-7B15F67}
Shortcuts	x	x	{CEFFA6E2-E3BD-421B-852C-6F6A79A59BC1}	{C88AB69A-B272-4FF9-80A7-43D916E}
Start Menu	x		{CF848D48-888D-4F45-B530-6A201E62A65F}	{D1D2BAD7-4061-4DBB-B856-0FCE791}
System	x		{DAE1786B-4A9B-4A9B-83D2-6CA72045EDB2}	{E1B7013C-20DE-40CE-80BD-0D1913E}
<i>Computer Settings</i>		x	{54294B1F-8888-4592-B382-8C4F5C109CB1}	{C7FB0933-D44B-4788-BDDA-E366E35}
<i>User Settings</i>	x		{5B99D9E8-DE05-459a-A20C-195D83766ACE}	{BC5CDBD1-166A-43c7-91F8-0C458F1}
<i>Control Panel</i>		x	{17C6249E-BA57-4F69-AE93-4FB3D25CD9D7}	{1D147B84-E99F-40CB-8D5D-A267194}
<i>Control Panel</i>	x		{F63F9611-3227-4f94-BFCD-5E48F9C9AD82}	{1B1B4514-83FB-4EE5-988B-5D602E2}

The polmkr.msi package may be installed manually or distributed to administrators via a GPO using Microsoft's

software installation policy. The minimum installation requirement for the extensions is Windows 2000. No Active Directory schema extensions are implemented and no services are installed by PolicyMaker. The CSEs are automatically installed during snap-in component installation in order to ensure that Local GPO processing is functional on the editing computer, and that RSoP planning mode is available even if PolicyMaker settings are not to be applied on the editing computer.



#### Note

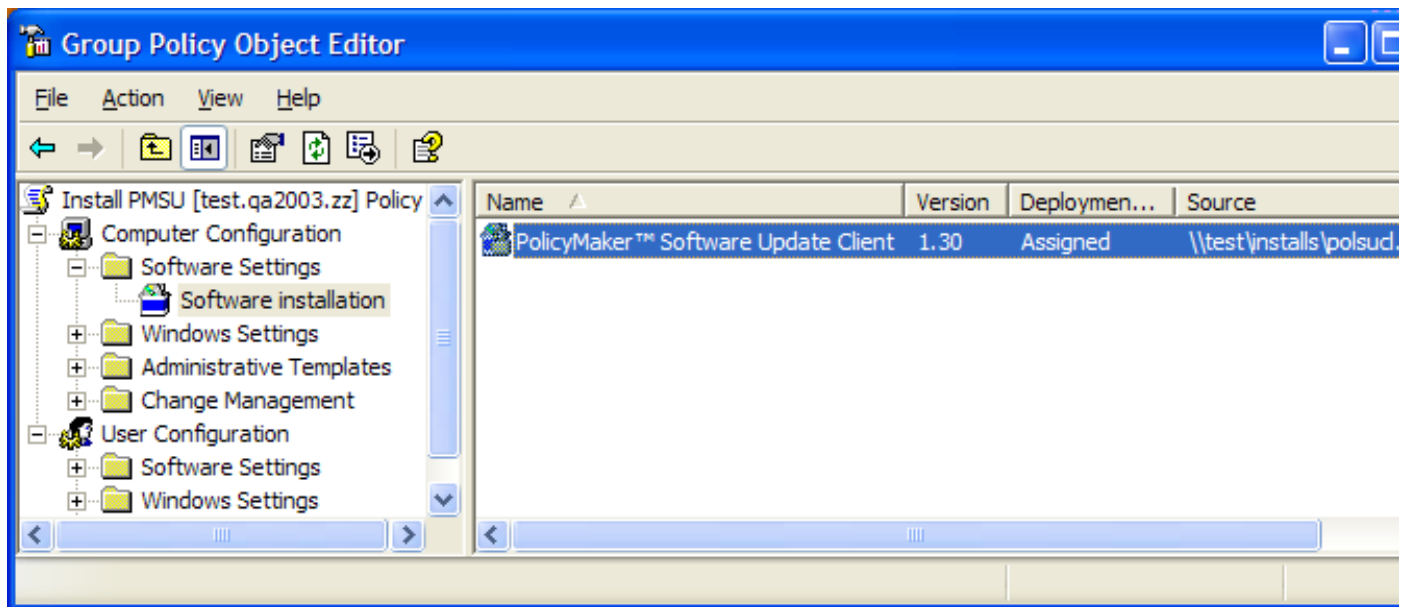
PolicyMaker snap-in extensions may be restricted using Microsoft's Administrative Templates policy. Installation of the polmkr.msi installs the [desktopstandard.adm](#) to the standard template location. The desktopstandard.adm includes user policies for restricting access to each GPOE and/or RSoP snap-in extension.

#### Client Side Extensions

In addition to installing the snap-in extensions, the polmkr.msi installs the PolicyMaker CSEs and places a copy of the CSE distribution package (polmkrcl.msi) on the local computer in the following location.

[DesktopStandard\PolicyMaker\Client\polmkrcl.msi](#)

To distribute the polmkrcl.msi (~950kb), publish it via a GPO using Microsoft's software installation policy.



The polmkrcl.msi must be distributed to all computers that are expected to execute PolicyMaker settings. If the CSE package is not installed, PolicyMaker GPO settings will have no effect on a given computer. If a CSE is not of a version compatible with PolicyMaker snap-in data, the CSE will not process policy, and an error will be written to the computer's system event log. The following CSEs are installed by polmkrcl.msi. Note that the "PolicyMaker License" CSE performs required PolicyMaker background refresh [licensing calculations](#) and is not configurable.

CSE Name	CSE GUID
PolicyMaker License	{00000040-789B-494F-BF51-216A4110581C}
PolicyMaker Environment Variables	{08E9566B-1390-4bfb-B19F-EA465BAD922D}
PolicyMaker Local Users and Groups	{08F5166F-E66B-4F15-80BF-DE94F083472A}
PolicyMaker Devices	{0947EA96-E4DE-48C5-99AD-FCC1829FFE86}
PolicyMaker Network Options	{15D30905-443F-4097-8FA8-0A2E35B475DC}
PolicyMaker Drive Maps	{1EA5E892-2292-438f-8D05-40E7B0007585}
PolicyMaker Folders	{F0DB2806-FD46-45b7-81BD-AA3744B32765}
PolicyMaker Files	{F17E8B5B-78F2-49a6-8933-7B767EDA5B41}
PolicyMaker Data Sources	{F27A6DA8-D22B-4179-A042-3D715F9E75B5}
PolicyMaker Ini Files	{F55DA052-16E1-434b-803F-F6A9F6945957}
PolicyMaker Services	{F581DAE7-8064-444A-AEB3-1875662A61CE}
PolicyMaker Folder Options	{F5BFF32F-D563-460D-8764-890933FB03C0}
PolicyMaker Scheduled Tasks	{F648C781-42C9-4ED4-BB24-AEB8853701D0}
PolicyMaker Registry	{F6E72D5A-6ED3-43d9-9710-4440455F6934}
PolicyMaker Application	{F9C77450-3A41-477e-9310-9ACD617BD9E3}
PolicyMaker Printers	{FD023FFE-C165-40d5-A201-439FC65AC8A5}
PolicyMaker Shortcuts	{FD2D917B-6519-4BF7-8403-456C0C64312F}
PolicyMaker Mail Profiles	{FD44098A-CA65-4054-8A70-EBAFAB263C70}
PolicyMaker Internet Settings	{FEF373ED-6CBE-4294-83EC-008D502B394A}
PolicyMaker Start Menu	{FF87F78A-E3A2-4AAE-B049-7E6BB1670D7B}
PolicyMaker System	{FF9F4E10-88EA-4B3B-BE8F-298A2AA76EB5}
PolicyMaker Display Options	{FFA88417-A483-49EF-BFED-35B3F1847EB0}
PolicyMaker Regional Options	{FFAA00BB-0D9B-401B-E71B-EF5ED1D88E6D}
PolicyMaker Power Options	{FFC64763-70D2-45BC-8DEE-7ACAF1BA7F89}

## Files Installed

All PolicyMaker Standard Edition feature CSEs are all implemented in a single DLL which is installed into the following location on each client computer:

[%SystemRoot%\System32\polprocl.dll](#)

Additionally, all PolicyMaker products share a single common DLL, which implements the License CSE.

[%SystemRoot%\System32\polcmncl.dll](#)

## Registration Performed

No COM objects are registered by the CSEs. The CSE installation performs minimal registration in the following registry location:

[HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions](#)

## WMI Changes

CSE installation extends the local computer [WMI namespace](#) in order to support [RSOP planning and logging](#) modes. This is management data local to each computer and has no impact on Active Directory schema.

## Note

CSEs may be configured using Microsoft's Administrative Templates policy. Installation of the polmkr.msi installs the [desktopstandard.adm](#) to the standard template location. The desktopstandard.adm includes computer policies for configuring the standard CSE options, as well as PolicyMaker features.

See the [uninstallation](#) topic detailed information on removing PolicyMaker.

## Troubleshooting

---

PolicyMaker provides several mechanisms for troubleshooting CSE operation. These include configurable tracing, configurable event logging, and Resultant Set of Policy (RSoP) reporting. For detailed information on troubleshooting specialized extensions, such as Software Update, see that extension's troubleshooting guide.

### Client Side Tracing

CSE tracing is disabled by default, and may be enabled by utilizing the [desktopstandard.adm](#) within Microsoft's Administrative Templates policy extension. When the PolicyMaker snap-in extensions are installed, the desktopstandard.adm is installed into the default location for administrative templates. Import this template into Administrative Templates policy within a computer configuration. This template includes policy settings for control of standard CSE behaviors, the size and location of each CSE's trace file, and the quantity of event logging. Tracing provides detailed output on each CSE's operation in a simple text format.

### Event Logging

CSE event logging of errors is always enabled. Using the desktopstandard.adm additional categories of event log messages may be enabled. This includes warnings and informational messages. An example of a typical event log warning is a policy that does not get applied due to a filter that returns false. An example of a typical informational message is the success of an individual policy setting.

### Resultant Set of Policy (RSoP)

Windows XP and later computers support RSoP logging by CSEs. Windows 2003 Server also supports RSoP planning mode. RSoP logging and planning mode data may be viewed in the RSoP snapin, as presented by each snap-in extension.

#### Logging Mode

All PolicyMaker extensions support logging mode. RSoP logging consists of writing data to the computer's WMI repository so that the data may later be collected by an administrator to determine what actions the CSE performed. All PolicyMaker CSEs support logging mode.

Typical RSoP snap-in extensions provide RSoP reporting data within a read-only user interface similar to that implemented by the corresponding GPOE snap-in extensions. This means that each property page for each item must be viewed to see the configuration results. PolicyMaker RSoP extensions each implement a single node. Clicking on this node presents a detailed HTML report in the MMC result view. This report shows the results of all settings applied by that particular extension.



#### Tip

Selecting the XML toolbar button presents the XML associated with the displayed RSoP report, and contains more detailed information.

#### Planning Mode

All PolicyMaker extensions support planning mode. RSoP planning is a simulation process that uses the WMI repository similarly to RSoP logging. However, in contrast to logging mode, CSEs are launched by the server and are directed to not perform actual configuration – but report to WMI as if they had. This allows the administrator to view the same type of data as in logging mode, without actually performing configurations. In planning mode, PolicyMaker assumes all [filters](#) pass and all action modes (PolicyMaker Standard Edition and Registry Extension) are effectively "Update". It is important to note that this behavior does include filter items such as security group and computer, regardless of administrator choices in the planning mode wizard.

#### User Environment Log (userenv.log)

The User Environment Log is a text log file written to the following location by winlogon. This file contains general information about the user environment and about the execution of individual Group Policy CSEs. Because the information that is logged is generic to all CSEs and the policy environment, this log fully supports and reports properly on PolicyMaker policy processing. The log is created in the following location.

`%SystemRoot%\Debug\UserMode\userenv.log`

The level of logging can be controlled using the following registry settings.

```
Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value: UserEnvDebugLevel
Value Type: REG_DWORD
Value Data: 0x00010002 (65538)
```

UserEnvDebugLevel can have the following values:

```
None: 0x00000000
Normal: 0x00000001
```



Verbose: 0x00000002  
Logfile: 0x00010000  
Debugger: 0x00020000

The default value is "Normal | Logfile" (0x00010001). Set this to 0x00010002 to "Verbose | Logfile" (0x00010002) to enable verbose tracing to the userenv.log file.

#### Status Messages

During foreground processing of Group Policy, Windows will write various messages to the status window. Foreground policy is defined by the presence of the status window, which is presented during computer startup (computer policy) logon and during user logon (user policy).

PolicyMaker extensions may write status messages, providing additional useful information. The status window accepts both normal and verbose levels of messaging. By default the level is set to normal. Verbose status messages can be enabled using the following registry value.

Key: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon  
Value: VerboseStatus  
Value Type: REG\_DWORD  
Value Data: 0x00000001 (1)

## Version History

---

This document outlines changes in PolicyMaker Standard Edition since its initial release on November 24, 2003.

[New Features](#)  
[Enhancements](#)  
[Bug Fixes](#)

### PolicyMaker Standard Edition 2.5.1

*Released 11/23/05*

7533 Internet Settings: Trusted Zone > Custom Level > Download Signed ActiveX Controls Enabled was always set to Prompt  
7387 MSI Wizard may launch for Office 2000 when the client runs  
7229 Power Options: "Prompt for password..." option does not take effect  
7099 Error determining license usage in some cases  
7075 Scheduled tasks would not run if they were set to begin or end on the first of the month  
7025 Power Options: error 0x8007051a - two revision levels are incompatible  
6110 Legacy user browser may show up instead of native AD browser  
6033 Outlook: Desktop Alert Settings button doesn't take effect  
6005 MSI Query Filter: product/component browsers implemented  
6003 Shortcuts are truncated to 8 character filenames when the path is not accessible during creation  
5536 Internet Settings: Advanced > Security: "Use SSL 2.0", "Use SSL 3.0", and "Use TLS 1.0" cannot be enabled/disabled separately  
5512 Snap-in view extension may collapse view  
5412 Power Options: "When I close the lid of my portable computer" incorrectly sets "When I press the power button on my computer"  
3590 Environment Variable policy should automatically use REG\_EXPAND\_SZ when unexpanded variables found in value  
3428 New Group Policy processing mode filter

### PolicyMaker Standard Edition 2.5.0

*Released 7/7/05*

5374 Unknown error during licensing processing  
5371 Add Local Printer policy  
5347 Exchange Server: Lookup Mailbox defaults to "ProfileMaker"  
5324 Add a folder browser to the archive location selector  
5289 Add Outlook 2003 signature settings  
5219 MessageBox timeout not working (never times out)  
5215 Desktopstandard.adm should allow for background refresh disable on more CSEs  
5210 Intermittent drag and drop to explorer error "cannot read from source file or disk"  
5203 PolicyMaker 2 licensing GUI doesn't indicate that a version 1 license is outdated, etc.  
5201 Add apply button on the license property sheet  
5200 License property sheet text for demonstration mode is misleading  
5194 Display a "New Mail Desktop Alert" property not working in Outlook 2003  
5187 Don't write a policy applied event if the filter did not pass (no event)  
5175 WMI Query with empty results may cause CSE failure  
5167 Computers with the PolicyMaker client imaged with Ghost may not process policies  
5166 File policy should make source file optional for update mode  
5164 Scheduled Tasks - Advanced: Date control shows current date and not selected date  
5163 Multiple IP printers with the same driver name not possible  
5159 Power scheme can't be set if all schemes are deleted  
5143 Add "When I press the sleep button on my computer" option to power options  
5138 Scheduled Tasks: invalid characters cause policy to not be applied, prevent UI entry  
5136 Scheduled Tasks: Changing drop-down incorrectly changes time  
5127 Registry Tab - typo in "Value type" field  
5123 Add support for multivalue Registry properties  
5118 Name change from "Policy Maker" to "PolicyMaker"  
5113 Add "Location" field to IP Printer tab  
5096 Implement Unicode Personal Folders support  
5045 Devices policy does not disable subclass items individually  
5021 Internet Settings: Custom Security Settings: "Administrator" should be "Administrator approved"  
5018 Internet Settings: Custom Security settings should open with .NET FX-reliant components at top  
5004 Power Scheme may not set as the default in some situations  
4827 New MSI Filter control  
4800 New options for WMI Filter  
4260 Improve license quantity error message, currently returns no grace key message  
4194 Add RPC over HTTP to Exchange GUI  
3386 Error "0x8007000e Not enough storage is available to complete this operation."

## 3044 New LDAP Filter control

### PolicyMaker Professional 2.0.2

*Released 12/21/04*

4813 [Selecting "GPMC Integration" during install causes interruption when GPMC not present](#)

### PolicyMaker Professional 2.0.1

*Released 12/17/04*

4811 [Add hibernate option to "When I close the lid on my portable..."](#)

4809 [Changing a power scheme name resets other combo box values](#)

4801 [Add GPMC backup, restore, import and copy support](#)

4799 [Additional policy removal options for Local Group policy](#)

4797 [Device policy removal option incorrectly sets action to 'Enable'](#)

### PolicyMaker Professional 2.0.0.188

*Released 12/06/04*

4798 [Error in license key validation](#)

4795 [View extension 'Filtered by ancestor' is always 'No'](#)

### PolicyMaker Professional 2.0.0

*Released 12/02/04*

4625 [Ten new control panel extensions](#)

### PolicyMaker Professional 1.0.4

*Released 6/4/04*

4390 [Some Automatic Updates scheduled install times may not present properly](#)

4214 [Not using native Windows browsers when not on a domain](#)

4177 [User and security group browsers return SID unresolvable error](#)

4163 [Error message "Catastrophic fail" on copy of unexpanded scope item](#)

4160 [Toolbars not refreshed after property sheet opens](#)

4143 [Outlook "Reset the Outlook Bar to defaults ..." option fails with path not found error](#)

4142 [New MOM Management Pack for monitoring policy application](#)

4135 [Filter browser windows are centered below selecting control](#)

4114 [Browsers should default to logged-on domain, not local computer](#)

4037 [Creation of additional mailboxes in Exchange service returns error 0x8004010f](#)

3658 [Memory leak in snap-in resolved](#)

3208 [Multiselect cut/copy causes a save for each item on paste](#)

### PolicyMaker Professional 1.0.3

*Released 4/28/04*

4012 ["Cached Exchange Mode" settings are not retained in the UI](#)

3963 [Some error codes incorrectly or not translated to text](#)

3962 [Standardize event log messages](#)

3941 [Remove hidden filters from HTML settings reports](#)

3927 [Remove license checks for registry extension \(now free\)](#)

3911 [Support for new Windows XP SP2 languages](#)

3907 [New registry filter features \(substring and version string matching\)](#)

3908 [Allow version number segments greater than 255 in file version filter](#)

3906 [New filter naming and documentation capability](#)

3859 [Drive hide/show options processed incorrectly](#)

3850 [Shared driver path should be required for TCP/IP printer configuration](#)

3843 [Make CSE policies default to default CSE registered behavior](#)

3840 [Disable all user context filters and filter options in computer policy](#)

3804 [Write extension names into CSE policies for ease of troubleshooting](#)

3679 [Language filter Native option returns true only for English platforms](#)

3670 [New Operating System filter category for service packs](#)

3649 [PolicyMaker default installation location should show full path](#)

3647 [PolicyMaker non-default installation location causes snapin error](#)

3634 [Enforced GPOs are enforced but may not show highest precedence in RSoP](#)

3632 [Only one IMAP service gets configured when there are several in the configuration](#)

3631 [Apostrophe character not properly entitized by XML parser, could cause invalid RSoP data](#)

3626 ["Logon network security" property in the Exchange service UI may not save correctly](#)

3620 [Add domain/OU validator to key request UI](#)

3604 [Settings on Internet E-mail tab don't appear to stay disabled](#)

3599 [Default Outlook 2003 Send/Receive option should match Outlook default](#)

3594 [User policy should access the GPO in user context to prevent inappropriate access error](#)

3593 [Trace data written in user context not recorded if user did not have access to trace file](#)

3586 [Exchange Settings do not stay red after disabling](#)

3481 [Send/Receive settings may be reset by Exchange service in update mode](#)

3477 [Legacy user browser displays duplicate list of users](#)

3471 [Add License CSE policy to DesktopStandard.adm template](#)

3474 User profile variables (i.e. %DesktopDir%) do not set correctly in computer policy (system vs. all users)  
3469 Outlook Layout tab settings not presenting saved values correctly  
3468 Don't write unused Exchange properties to XML  
3467 Computer in OU filter should not throw error if computer not in forest  
3465 Hidden filters should be exclusive (ANDed vs. ORed with visible filters)  
3454 Wildcard '?' acts like '\*' at the end of a string  
3287 New support for wildcards in Terminal Session filters  
3285 Drive mappings may cause popup or tray error if reconnect at logon set  
3284 Drive maps may not match properly if previously remembered  
3269 New Client TCP/IP Address range option in Terminal Session filter  
3203 New native Active Directory browsers for all AD objects  
3202 New hierarchical registry policy settings and multiselect registry browser  
3136 Filter control shows filters after an apply with filter option deselected  
2651 Message box variable name field should be gray when disabled  
2260 Registry "get value" variable information field goes blank if value is too long

#### PolicyMaker Professional 1.0.2

*Released 12/9/03*

3464 Office 2003 application extension browser buttons do not launch browser  
3463 Registry browser may not present all values  
3460 New feature for wildcard text matching on user filters  
3457 Browser shows default icon when not running on Windows XP  
3450 OU browser doesn't initially show all OUs  
3449 Refresh of a leaf item in the network browsers may return wrong icon  
3448 Text match on user and domain filters not functional  
3447 Filters do not get saved on apply  
3438 AD browser may obtain wrong NetBIOS domain name if domain renamed

#### PolicyMaker Professional 1.0.1

*Released 11/26/03*

3425 Outlook plugin layout tab disabled settings show as enabled  
3422 Root RSoP nodes should have default view extension (MMC 2.0 only)  
3421 Settings report second level (setting level) should match RSoP  
3418 Licensing user and computer counts may not exactly match number of Active Directory objects  
3415 Licensing menu bar may be disabled (MMC 1.2 only)  
3413 If settings xml files and history files are manually deleted, CSE(s) may hang up  
3404 Include an image of the settings report in the help topic  
3403 License Request help topic missing image

#### PolicyMaker Professional 1.0.0

*Released 11/24/03*

## Release Notes

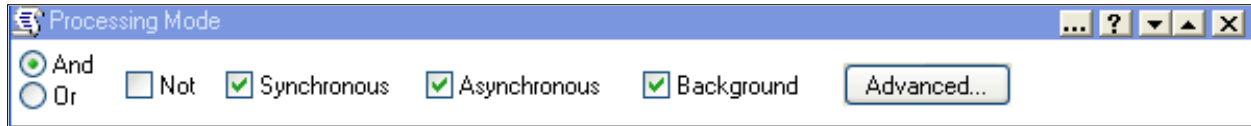
---

This document is meant to give you an overview of the new features, enhancements, and bug fixes implemented in this release of PolicyMaker Standard Edition. For detailed information on new functionality, please see the Help file. For a complete listing of changes, see the [Version History](#).

PolicyMaker Standard Edition 2.5.1 - Released November 23, 2005

### NEW FEATURES

New Processing Mode Filter (#3428)



The Processing Mode Filter allows you to filter based on the processing mode in which the CSE is currently executing. See [Processing Mode Filter](#) in the help file.

### OTHER ENHANCEMENTS

MSI Filter Browsers (#6005)

The MSI filter now provides browsers for MSI components and MSI patches.

### FIXES

Error determining license usage (#7099)

In some situations, the client may fail to determine license usage which would cause a failure of the client to apply policy.

Power Options: error 0x8007051a - two revision levels are incompatible (#7025)

In some situations, the above error code may have occurred when setting Power Options policy.

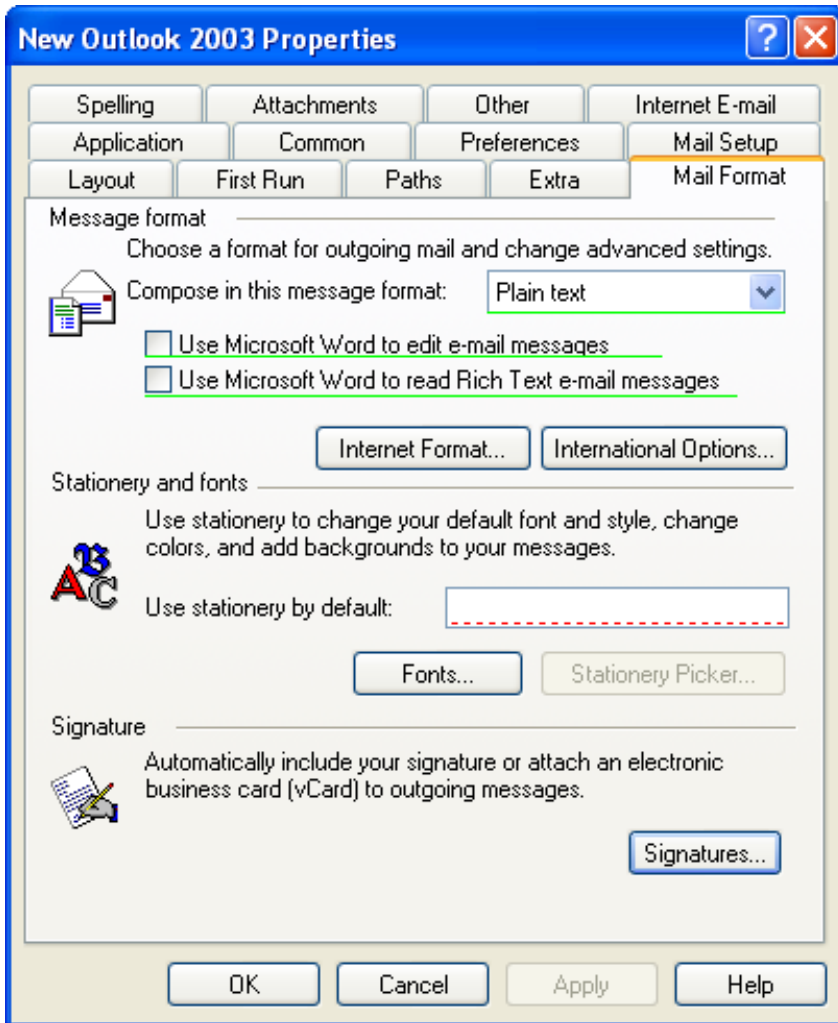
Shortcuts are truncated to 8 character filenames when the path is not accessible during creation (#6003)

When creating a shortcut, if the shortcut target path didn't exist at the time, the shortcut would be successfully created with an invalid truncated path. This is caused by the normal behavior of the shortcut API. The fix will prevent the creation of a shortcut to a file system target that is not accessible and produce an appropriate error and trace information.

PolicyMaker Standard Edition 2.5.0 - Released July 7, 2005

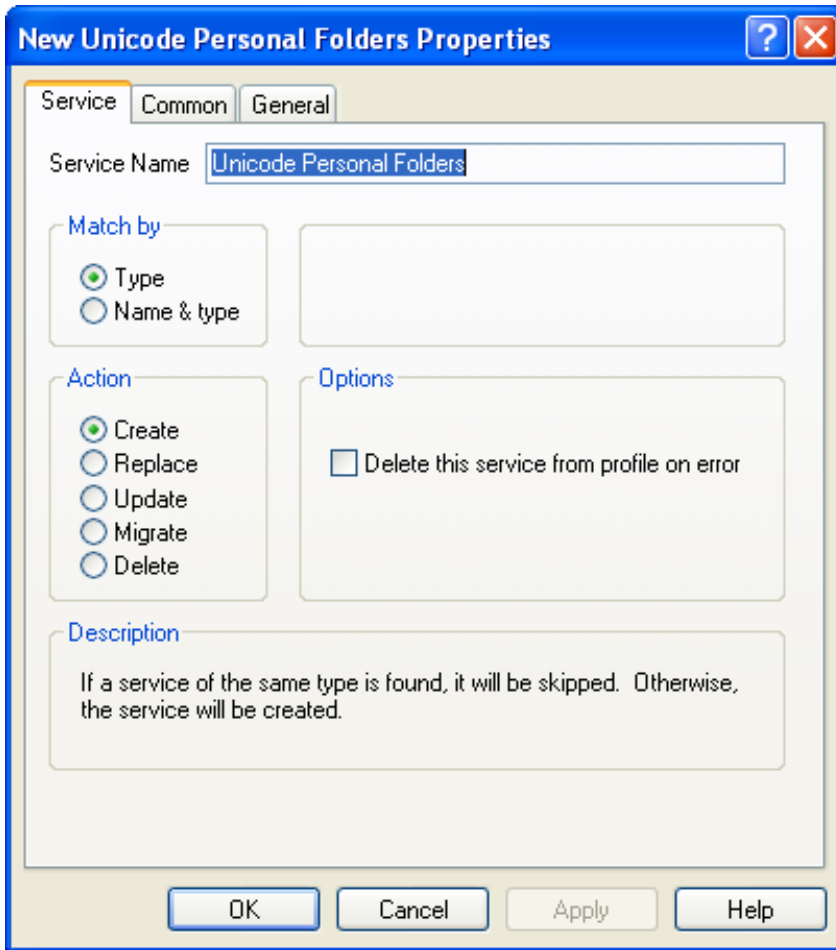
### NEW FEATURES

Outlook Signatures (#5289)



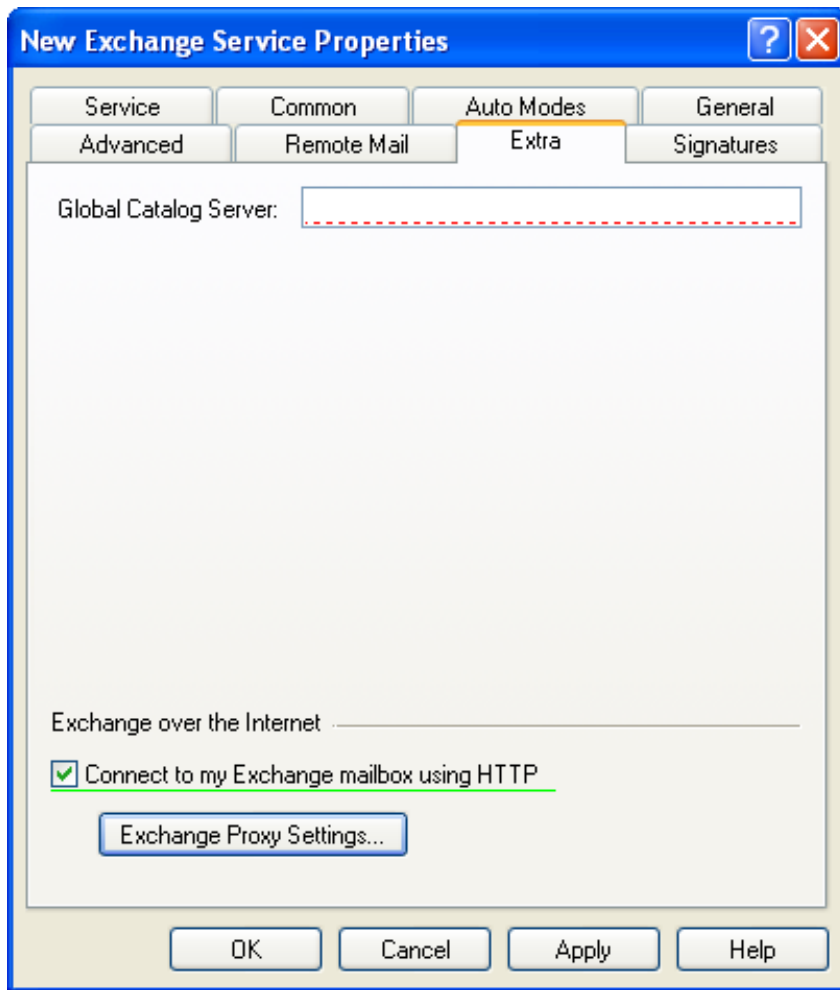
A "Signatures" tab was added to the Exchange GUI that allows the setting of the Outlook 2003 Signatures used in the context of the Exchange Service. Under "User Settings/Applications/Outlook (2000, 2002, 2003)", on the Mail Format tab, there is now an option that allows editing of rich-text signatures (with embedded variables) that will be applied to an Outlook Profile.

Unicode Personal Folder (#5096)



In MAPI Profiles, you now have the option to add a Unicode Personal Folder.

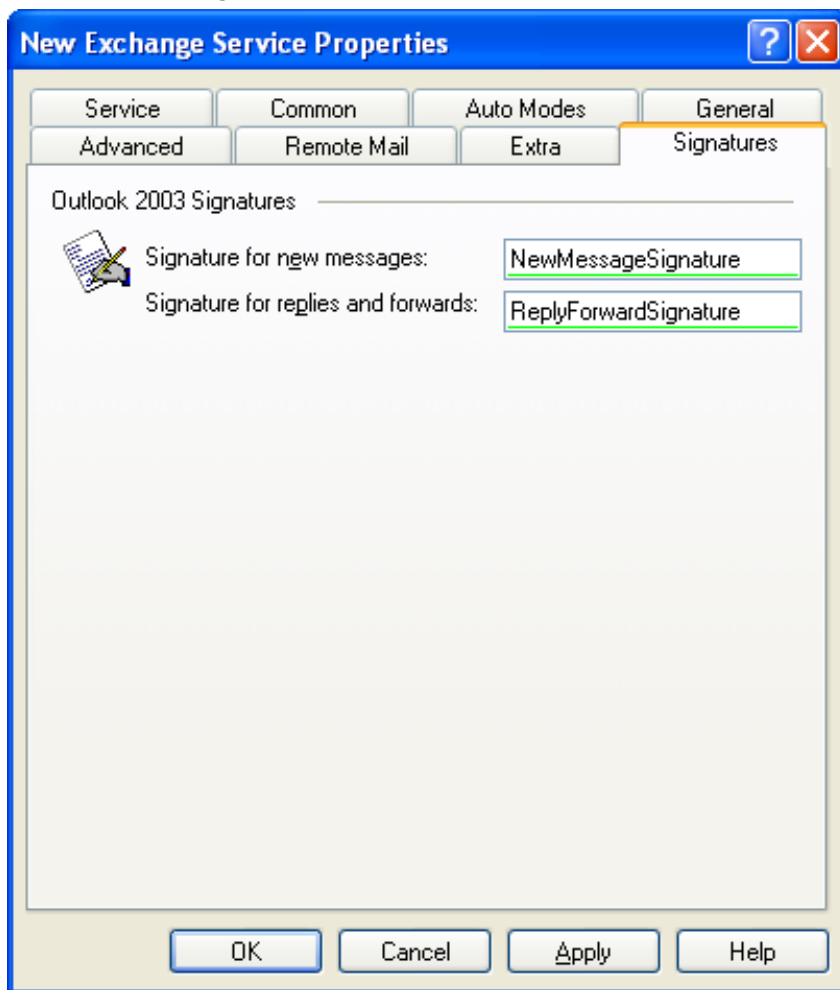
RPC over HTTP (#4194)



In the Exchange Service, there is a new option on the "Extra" tab to connect to an Exchange mailbox using RPC over HTTP.

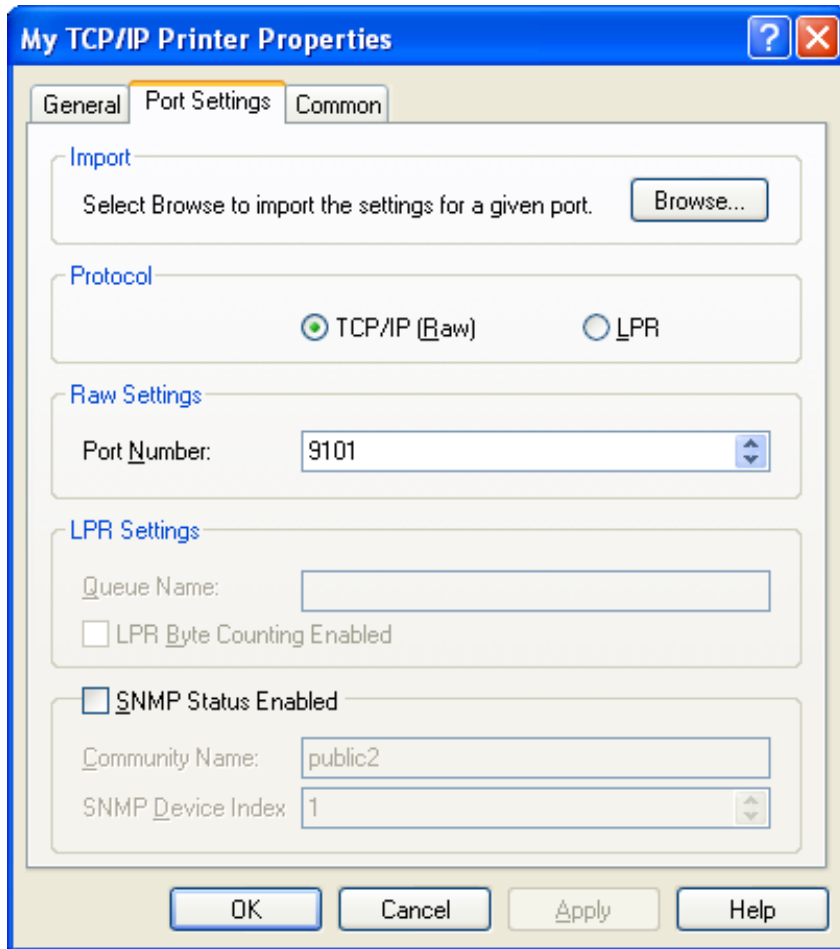


## Outlook 2003 Signatures (#5289)



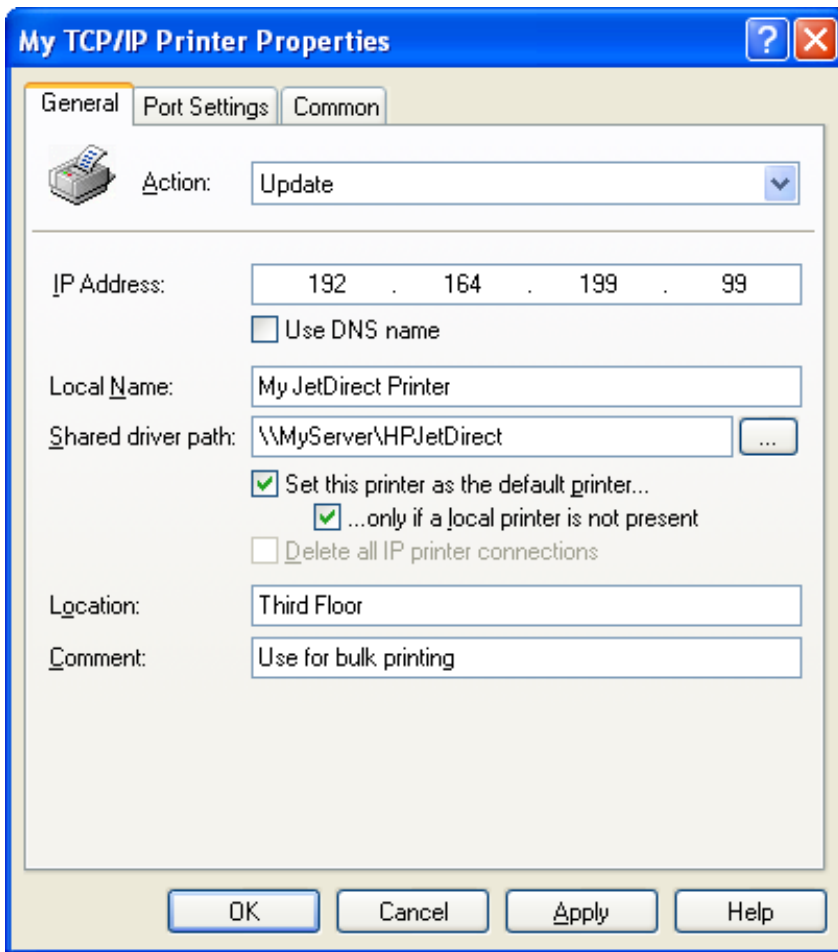
In the Exchange Service, there is a new option on the "Signatures" tab to specify the signatures to use when using an Exchange service account with Outlook 2003.

## IP Printer Port Settings (#5388)

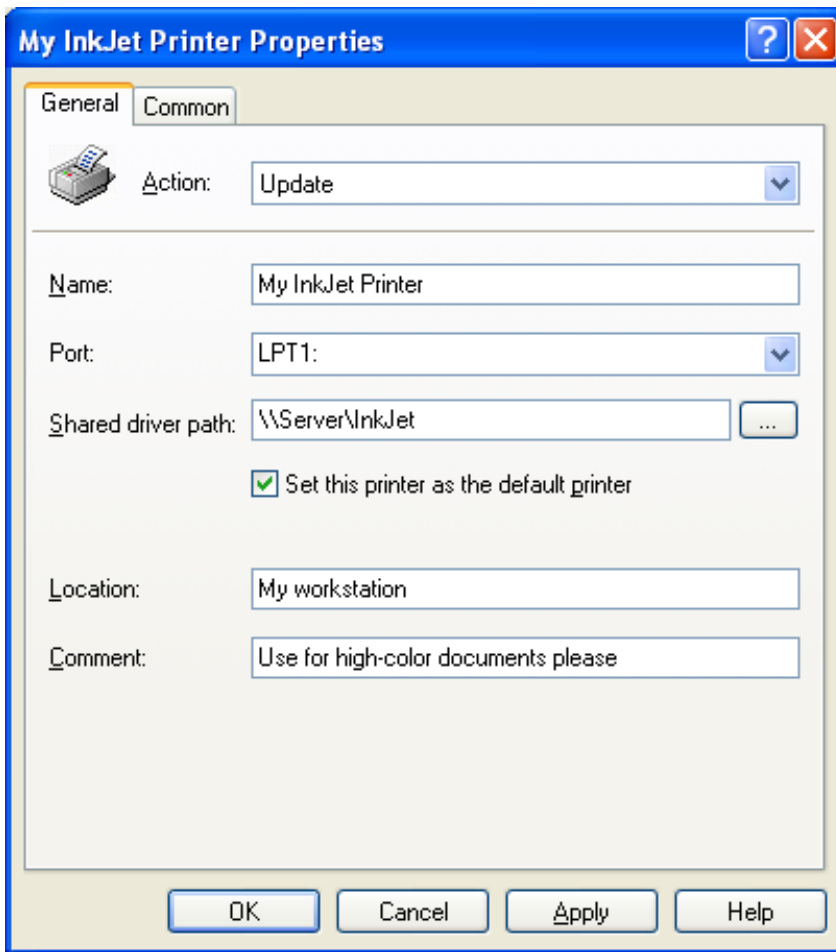


There is a new "Port Settings" tab from which it is possible to specify the port number and other configuration options for network printers. The browser lists all of the IP ports supported by Windows and will configure the appropriate default settings for each. LPR and multi-port IP printers are also now supported.

Named IP Printers (#5163)

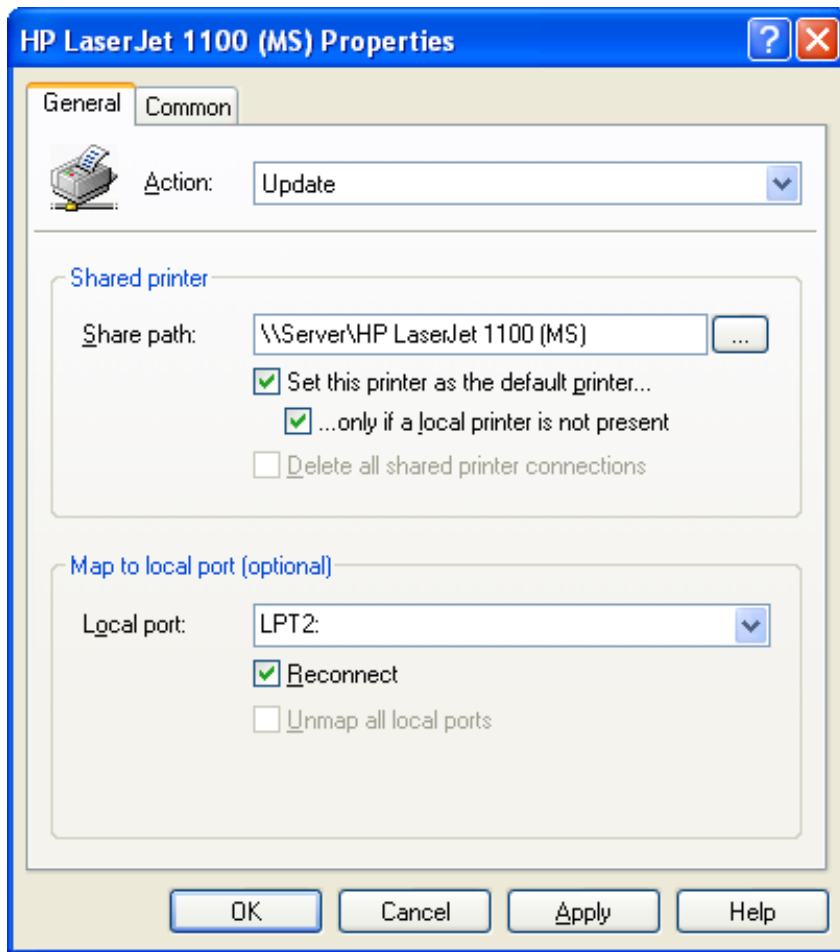


In previous versions of PolicyMaker Standard Edition, it was not possible to connect multiple IP printer items to multiple IP printers of the same model, as the name of the printer item was derived from the "driver name" used by the shared (driver source) printer. A new (optional) field was added, "Local Name," that allows you to specify the name that the printer is given when it is created. If this optional field is filled in, all actions will apply to the printer item by the local name rather than the port name. If left blank, the printer name will be automatically generated as in previous versions.



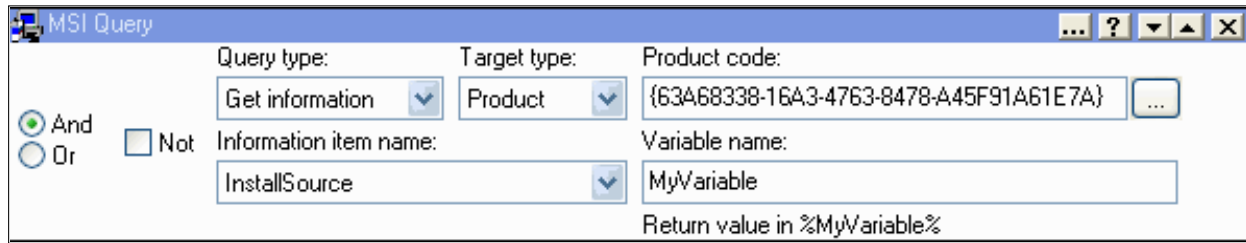
PMSE now supports configuration of a local printer on a COM, LPT, or USB port. Drivers are installed from a shared printer of the same model on the network.

Map Shared Printer to Local Port (#5211)



This allows a shared network printer to be mapped to a legacy LPT port.

### New MSI Filter (#4827)



The screenshot shows the 'MSI Query' dialog box. It has a title bar with a question mark and a close button. The dialog is divided into several sections. On the left, there are radio buttons for 'And' (selected) and 'Or', and a checkbox for 'Not'. The main area contains three columns: 'Query type:' with a dropdown menu set to 'Get information'; 'Target type:' with a dropdown menu set to 'Product'; and 'Product code:' with a text box containing '{63A68338-16A3-4763-8478-A45F91A61E7A}' and a browse button. Below these, there is an 'Information item name:' dropdown set to 'InstallSource' and a 'Variable name:' text box containing 'MyVariable'. At the bottom, it says 'Return value in %MyVariable%'.

The MSI Query Filter allows you to filter based on version or product code information from any MSI-installed Product, Patch or Component. For more information, see [MSI Query](#) in the help file.

### New LDAP Filter (#3044)



The screenshot shows the 'LDAP Query' dialog box. It has a title bar with a question mark and a close button. On the left, there are radio buttons for 'And' (selected) and 'Or', and a checkbox for 'Not'. The main area has a table-like structure with columns: 'Filter', 'Binding', 'Attribute', and 'Variable name'. The 'Filter' column has an empty text box. The 'Binding' column has a text box containing 'LDAP:'. The 'Attribute' and 'Variable name' columns have empty text boxes.

The LDAP Query Filter allows you to filter based on whether or not an LDAP search returns results. For more information, see [LDAP Query](#) in the help file.

### WMI Filter - New Options (#4800)



The screenshot shows the 'WMI Query' dialog box. It has a title bar with a question mark and a close button. On the left, there are radio buttons for 'And' (selected) and 'Or', and a checkbox for 'Not'. The main area has a table-like structure with columns: 'Query', 'Namespace', 'Property', and 'Variable name'. The 'Query' column has an empty text box. The 'Namespace' column has a text box containing 'Root\cimv2'. The 'Property' and 'Variable name' columns have empty text boxes.

The WMI Query filter now allows you to change the WMI namespace for a WMI Query. The WMI Query result can also now be saved to an environment variable for use in other PolicyMaker items. For more information, see [WMI Query](#) in the help file.

## OTHER ENHANCEMENTS

### Licensing Enhancements (#4260)

License processing has been updated to improve usability and error reporting.

### Name Change (#5032)

PolicyMaker Standard Edition was rebranded as a DesktopStandard product and the product name was changed from "Policy Maker Professional".

### MAPI Profiles (#5128)

Each checkbox, radio button group, or combobox can now be enabled or disabled independently from all other controls.

### Devices (#5045)

In previous versions, all devices of a class were enabled or disabled as a group. You can now enable or disable each device model independently.

## FIXES

### Subdomains may not apply policy due to licensing failure (#5191)

When PolicyMaker Standard Edition was installed on a subdomain of a parent domain, policies were not always applied to the clients due to a failure in licensing calculation.

### Power Options (#5159)

Power options will no longer fail if the user and computer power options have the same name.

### Message Box Filter (#5219)

The "Message Box" filter no longer fails to automatically "timeout" after the specified time.

### MultiValue Registry String (#5129)

Changes were made to both the Registry Extension and Registry Wizard to handle multivalue strings.

## Group Policy Concepts

---

Group Policy is a framework for user and computer configuration on Windows 2000 and later computers that are members of the Active Directory. Group Policy makes some fundamental assumptions about how users and computers should be configured in an enterprise environment. The primary assumption is that desired configurations are often common across multiple users and across multiple computers, and these groupings often reflect organizational structure.

### Organization

Active Directory organizational units (OU) exist to facilitate this grouping, and to allow such units to be members of other units. This organization is distinct from security group and domain organization, which are both fundamentally oriented around security priorities and do not generally reflect an organization's hierarchy. Group Policy settings can be applied to OUs, Domains, and Sites.

### Group Policy Objects and Storage

A Group Policy Object (GPO) is a collection of configuration settings that can be applied to certain users and/or computers based on their membership in a site, domain, or organizational unit. Each GPO has a name and a globally unique identifier (GUID). A GPO consists primarily of data that is stored in two distinct locations on a network, the Group Policy Container (GPC) and the Group Policy Template (GPT).

The GPC is system data that is stored in the Active Directory, associated with the GPO by its GUID. The GPT stores the actual configuration settings. This data resides in the following directory for a given GPO, and is synchronized to all domain controllers on a given domain:

`SYSVOL\{Domain}\Policies\{GPO GUID}`

### Editing Group Policy

The Group Policy Object Editor (GPOE) is the primary means for administrators to configure settings within a GPO. The GPOE is implemented as a Microsoft Management Console (MMC) snap-in that integrates various plugins known as Group Policy snap-in extensions. Configuration settings in the GPO are manipulated by a network administrator using the various graphical extensions that are integrated into the single GPOE application.

### Applying Group Policy

Policy settings are applied by Client Side Extensions (CSEs). Processing of GPO settings by CSEs is periodically initiated by the winlogon operating system process. Settings are organized into user and computer configurations. Winlogon will initiate processing of user settings during user logon, and computer settings during computer boot. This is known as foreground processing. Additionally, both user and computer configuration will be initiated periodically, which is known as background processing. By default, background processing occurs every 90 minutes (with a random offset of 0 to 30 minutes), or every 5 minutes on domain controllers, although the parameters are subject to change by an administrator. Some extensions support only user or computer configuration, and some support only foreground processing.

CSEs are extensions to client computer policy processing capability and generally correspond to a snap-in extension counterpart. CSEs implement the settings that exist in one or more GPOs. Winlogon calculates which GPOs are to be applied, based on various criteria, and launches each CSE as necessary. Winlogon provides the CSE with the path to each GPT and the CSE processes the settings in the GPT accordingly.

### Group Policy Reporting

The architecture for Group Policy reporting is called Resultant Set of Policy (RSoP). RSoP consist of two distinct modes: planning and logging. Logging mode is Group Policy's reporting system. RSoP reports utilize data generated by CSEs that implement the RSoP reporting interface on Windows XP and later computers. The RSoP MMC snap-in is the primary tool for viewing Group Policy results. Like the GPOE, the RSoP snap-in integrates various plugins known as RSoP snap-in extensions. Each extension reports on the configuration results from the last execution of its corresponding CSE for a particular computer or user.

### Group Policy Troubleshooting

There are a number of tools available for Group Policy [troubleshooting](#).

---





## Group Policy Tools

---

Microsoft provides several additional Group Policy tools in addition to the Group Policy Object Editor (GPOE) and Resultant Set of Policy (RSOP) snap-ins. Unlike the GPOE and RSOP tool and Group Policy Client Side Extension (CSE) execution, these tools are not part of the Group Policy specification, and are not all fully compliant with third party extensibility. PolicyMaker supports these tools inasmuch as they are currently supportable.

- [Security Editing Utility \(secedit.exe\)](#)
  - [Group Policy Update Utility \(gpupdate.exe\)](#)
  - [Group Policy Results Tool \(gpresult.exe\)](#)
  - [Group Policy Inventory \(gpinventory.exe\)](#)
  - [Windows Help and Support](#)
  - [Group Policy Management Console \(GPMC\)](#)
-

## Security Editing Utility (secedit.exe)

---

secedit.exe /refreshpolicy is a Windows 2000 command that serves the same purpose as the newer [gpupdate](#). PolicyMaker fully supports use of this tool.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Group Policy Update Utility (gpupdate.exe)

---

The Group Policy Update Utility is a command line tool that is available from Microsoft for both Windows 2000 and Windows XP. The tool accepts various command line parameters and forces local execution of group policy for user and/or computer processing. Because all policy extensions will be executed during each application of Group Policy, PolicyMaker fully supports use of this tool.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Group Policy Results Tool (gpresult.exe)

---

The Group Policy Results Tool is a command line tool that is available from Microsoft for both Windows 2000 and Windows XP. The tool accepts various command line parameters and outputs to the console detailed information on Group Policy settings. This tool only supports a fixed list of Microsoft GPEs and will not report on individual PolicyMaker settings, however the other more generalized features do support PolicyMaker extensions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Group Policy Inventory (gpinventory.exe)

---

Group Policy Inventory allows administrators to collect Group Policy and other information from any number of computers in their network. [PolicyMaker fully supports use of this tool.](#)

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Windows Help and Support

---

"Help and Support" is available on the Windows XP Start menu. RSoP reporting for the local computer and user is available by selecting:

[Start/Help and Support Center/Computer Information/Tools/Advanced System Information/View Group Policy Settings Applied](#)

This HTML document reports on RSoP data, but currently only supports a fixed list of Microsoft GPEs and will not report on PolicyMaker settings.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Group Policy Management Console (GPMC)

The Group Policy Management Console is a Microsoft downloadable tool (MMC snap-in), that Microsoft describes as follows:

*"In conjunction with Windows Server 2003, Microsoft has released a new Group Policy management solution that unifies management of Group Policy. The Microsoft Group Policy Management Console (GPMC) provides a single solution for managing all Group Policy-related tasks.*

*The GPMC lets administrators manage Group Policy for multiple domains and sites within one or more forests, all in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management. Together these advantages make Group Policy much easier to use and help you manage your enterprise more cost-effectively."*

GPMC is currently provided only as a downloadable add-on, and runs on 32-bit versions of Windows XP SP1 and later and Windows 2003 Server. It can also be used remotely to manage GPOs on Windows 2000 SP2 and later domain controllers. Another benefit of GPMC is an update to gpedit.dll, which improves both the Group Policy Object Editor and the Resultant Set of Policy snap-ins.

<http://www.microsoft.com/windowsserver2003/gpmc/default.aspx>

The tool is a welcome and exciting addition to the task of Group Policy administration. However, it's important to note that GPMC is an administration console, and does not add any additional computer configuration capabilities to Group Policy.

### Compatibility

The GPMC includes many areas of functionality, most of which are fully compatible with Microsoft's Group Policy Extension specification and therefore PolicyMaker. There are several areas of functionality which are based on the specific implementations of individual Group Policy Extensions. In these areas the support for PolicyMaker may be limited, or accessible from a component external to the GPMC. The following table summarizes the GPMC support of third party extensibility.

Feature	Supported	Comments
<b>Root/Forest/Domains/Sites</b>		
Contents tab	yes	fully supported
<b>Domain/OU</b>		
Linked Group Policy Objects tab	yes	fully supported
Group Policy Inheritance tab	yes	fully supported
Delegation tab	yes	fully supported
<b>GPO</b>		
Scope tab	yes	fully supported
Details tab	yes	fully supported
Settings	external	fully supported in GPO Editor
Delegation	yes	fully supported
<b>Group Policy Modeling</b>		
Group Policy Modeling Wizard	yes	fully supported

Contents tab	yes	fully supported
Summary tab	yes	fully supported
Settings tab	external	fully supported in RSoP snap-in
Query tab	yes	fully supported
<b>Group Policy Results</b>		
Group Policy Results Wizard	yes	fully supported
Contents tab	yes	fully supported
Summary tab	yes	fully supported
Settings tab	external	fully supported in RSoP snap-in
Policy Events tab	no	third party event ids ignored
<b>GPO Operations</b>		
Create/Delete:	yes	fully supported
Linking:	yes	fully supported
Editing:	yes	fully supported
Searching:	yes	fully supported
<b>GPO Processing</b>		
Enable/Disable	yes	fully supported
WMI Filtering	yes	fully supported
Security Filtering	yes	fully supported
Enforcement	yes	fully supported
Inheritance Blocking	yes	fully supported
Loopback Processing	yes	fully supported
<b>GPO Operations</b>		
Backup/Restore:	yes	fully supported
Copy/Paste	partial	migration table settings not used
Import	partial	migration table settings not used
<b>GPO Scripting</b>		
GPMC Scripting:	partial	depends upon scripted object
GPMC Sample Scripts		
BackupAllGPOs.wsf	yes	fully supported



BackupGPO.wsf	yes	fully supported
CopyGPO.wsf	partial	migration table settings not used
CreateEnvironmentFromXML.wsf	yes	fully supported
CreateGPO.wsf	yes	fully supported
CreateMigrationTable.wsf	yes	fully supported
CreateXMLFromEnvironment.wsf	yes	fully supported
DeleteGPO.wsf	yes	fully supported
DumpGPOInfo.wsf	yes	fully supported
DumpSOMInfo.wsf	yes	fully supported
FindDisabledGPOs.wsf	yes	fully supported
FindDuplicateNamedGPOs.wsf	yes	fully supported
FindGPOsByPolicyExtension.wsf	yes	fully supported
FindGPOsBySecurityGroup.wsf	yes	fully supported
FindGPOsWithNoSecurityFiltering.wsf	yes	fully supported
FindOrphanedGPOsInSYSVOL.wsf	yes	fully supported
FindSOMsWithExternalGPOLinks.wsf	yes	fully supported
FindUnlinkedGPOs.wsf	yes	fully supported
GetReportsForAllGPOs.wsf	yes	fully supported
GetReportsForGPO.wsf	yes	fully supported
GrantPermissionOnAllGPOs.wsf	yes	fully supported
ImportAllGPOs.wsf	partial	migration table settings not used
ImportGPO.wsf	partial	migration table settings not used
ListAllGPOs.wsf	yes	fully supported
ListSOMPolicyTree.wsf	yes	fully supported
QueryBackupLocation.wsf	yes	fully supported
RestoreAllGPOs.wsf	yes	fully supported
RestoreGPO.wsf	yes	fully supported
SetGPOCreationPermissions.wsf	yes	fully supported
SetGPOPermissions.wsf	yes	fully supported
SetGPOPermissionsBySOM.wsf	yes	fully supported
SetSOMPermissions.wsf	yes	fully supported

There are three areas where GPMC features do not currently support PolicyMaker extensions - operations, settings reporting and events.

### Operations

PolicyMaker fully supports the GPMC implementation of Backup, Restore, Copy and Paste of GPOs. This support requires that the PolicyMaker snap-in be installed on the same computer that is running the GPMC and that 'GPMC

Integration' not be deselected during installation.

Import is also supported, however migration of settings (across domains) includes porting them through a migration table, so that location-dependant values, such as server names, file paths, etc. can be altered to suit the new location. The GPMC migration table does not currently support PolicyMaker settings. However, since PolicyMaker uses a common XML schema for all of its settings, this is a fairly simple task to automate, and can even be done using a simple text search and replace tool.

Import/Export of configuration data in PolicyMaker can be also performed using drag and drop between GPOs in the MMC, or to and from XML files.

### Settings Reports

Since each Group Policy extension implements its own settings persistence format, it is not a simple task for GPMC to report on each extension, even on just Microsoft extensions. This currently requires the GPMC implement proprietary parsing and presentation of various file formats, including .adm, .pol, .aas, etc. The GPMC doesn't implement parsing for third party extension data, nor does it provide a settings reporting extension mechanism.

However, each Policy extension includes a reporting capability that looks nearly identical to the GPMC settings report, including both XML and HTML formats. These reports are available within the GPOE on each PolicyMaker extension.

The only difference is that the reports are not integrated with the GPMC reports.

Modeling and Results reporting has a similar issue, in that each extension is required to write proprietary RSoP data to the WMI repository for both planning mode and logging mode executions. This data is used by the Modeling and Results settings reports respectively. Although the common data is accessible to the GPMC, there is no mechanism to extend the reports.

Each PolicyMaker extension, in accordance with the Group Policy interface standard, implements a corresponding RSoP snap-in extension. In a manner similar to PolicyMaker GPOE settings reporting, each of these extensions includes a reporting capability that looks nearly identical to the GPMC Modeling and Results settings reports, in both XML and HTML formats. The only difference is that the reports are not integrated with the GPMC reports.

### Policy Events

Policy Events are simply event log messages with well-known event numbers. The GPMC keys off of certain events and duplicates them in a view similar to the Event Viewer snap-in. GPMC hard-codes event identification, and thereby excludes third party extension events. However, these same events alongside PolicyMaker events, can easily be viewed in the Event Viewer snap-in.

## PolicyMaker Concepts

---

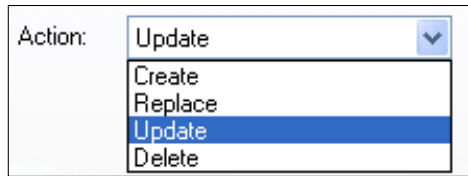
PolicyMaker implements a number of standardized conventions that fall outside of the scope of the Group Policy specification. These and other useful topics relating to applying policy are listed here.

- [Action Modes](#)
- [DesktopStandard ADM Template](#)
- [Browsers](#)
- [Common Tab](#)
- [Disabling Items](#)
- [Plugins](#)
- [Policy Processing](#)
- [Root Mapping](#)
- [RSOP Reports](#)
- [Security Contexts](#)
- [Settings Reports](#)
- [User Interface Conventions](#)
- [Variables](#)
- [WMI Namespace \(RSOP\)](#)
- [XML Integration](#)

## Action Modes

---

PolicyMaker implements standardized "Action" modes with the following basic behaviors. Although these behaviors are consistent within PolicyMaker, each item type interprets the selected Action mode in its own context.



- Create - Create the object only if it does not already exist.
- Replace - Delete the object first, then create it.
- Update - Create the object if it does not exist, otherwise modify it.
- Delete - Delete the object.
- Migrate - Modify an item if it exists, otherwise do nothing (not shown above).

### Icon Masking

PolicyMaker implements icon masking to visually reflect the action mode of a given item. Icons are typically masked as follows:



### Matching

All items that implement Action modes must have matching criteria for determining whether an object exists. For example, [Profiles](#) may be matched by their default status or the profile name. [MAPI Services](#) may be matched by service type or type with display name. Note the following:


- The match criteria may not always be obvious, such as with [Mapped Drive](#) and [Shared Printer](#) items. The match criteria for a Drive item is the drive letter, but with a Network Printer it is the share path of the printer. The help for each item that implements action modes includes documentation of the item's match criteria.
- The match criteria is always applied at the most detailed level specified in the item. For example, if a [Registry](#) item is set to delete and a "Value name" is specified, it is the value name that will be deleted, not the "Key" that contains it. However, if only a key is specified for delete, the last key in the "Key Path" will be deleted.
- In some cases, an item can support matching multiple objects. This includes a [MAPI Service](#) item in delete mode, a [Profile](#) item set to match all profiles, delete all [Shared Printers](#), and delete all [Mapped Drives](#). Other item types can only match a single object.
- Matching is never text case-sensitive.

### Standard Action Items

Each of the following item types implements a standardized Action option.

- [Data Sources](#)
- [DUN Connection](#)
- [Environment Variable](#)
- [File](#)
- [File Type](#)
- [Folder](#)
- [Ini File](#)
- [Local Group](#)
- [Local User](#)

- [Mapped Drive](#)
  - [Open With](#)
  - [Power Scheme](#)
  - [Profile](#)
  - [Registry](#)
  - [Service](#)
  - [Shared Printer](#)
  - [Shortcut](#)
  - [TCP/IP Printer](#)
  - [VPN Connection](#)
- 

 Note

Only Profile and Service items implement the Migrate Action. Profile and Service items implement Action choices as a radio button option group. All other items implement Action choices in a drop-down list (as shown above) at the top of the item's first property sheet tab.

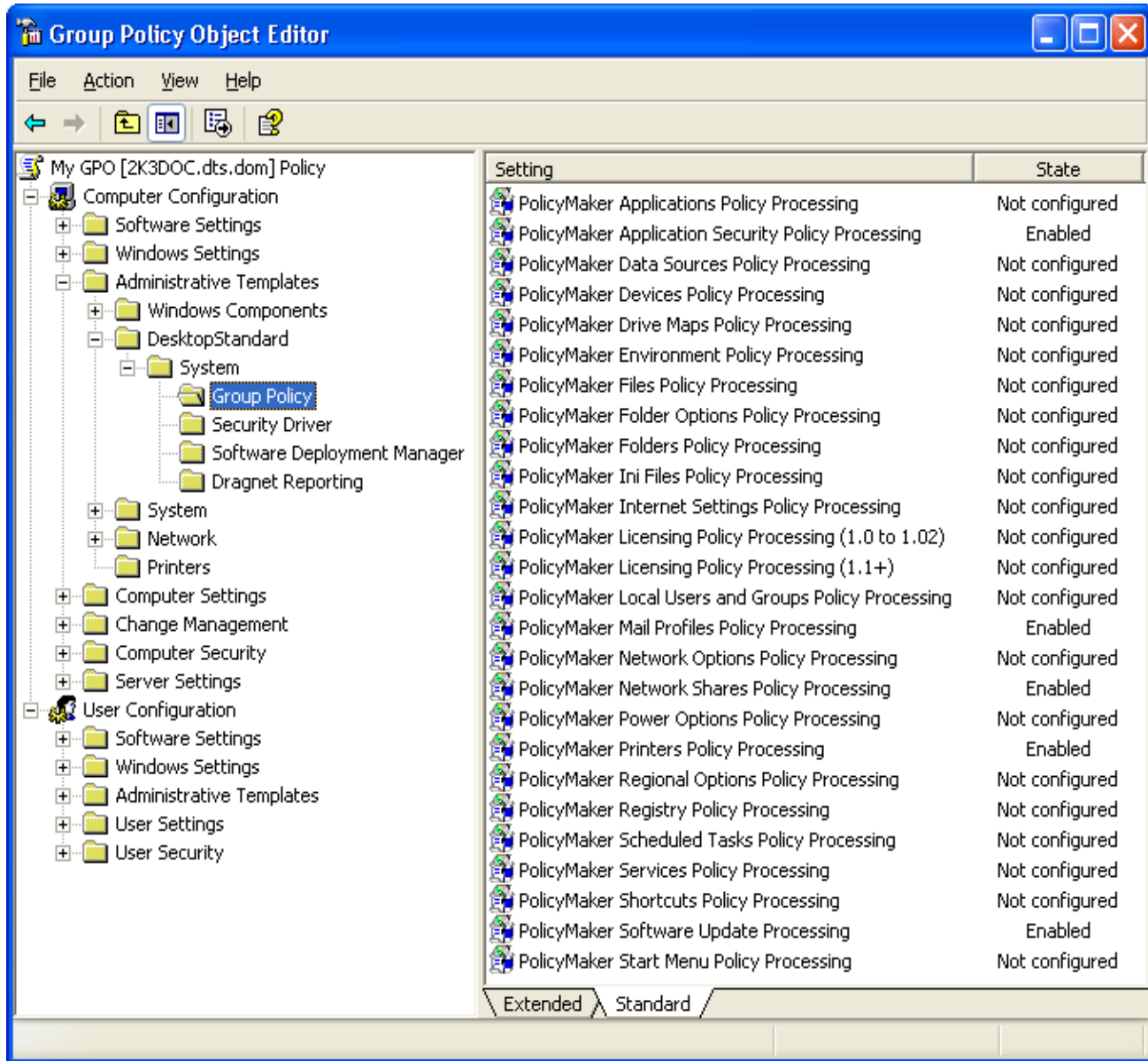
---

## DesktopStandard.ADM

The desktopstandard.adm file includes policy settings for configuring CSEs (computer policy) and restricting administrator access to GPOE and RSoP snap-in extensions (user policy). This file is placed into the standard location by the main PolicyMaker installation. In order to utilize these policies, add the DesktopStandard.adm to a GPO using Microsoft's "Administrative Templates" policy, for user and/or computer policy as desired.

### Client Side Extension Policies

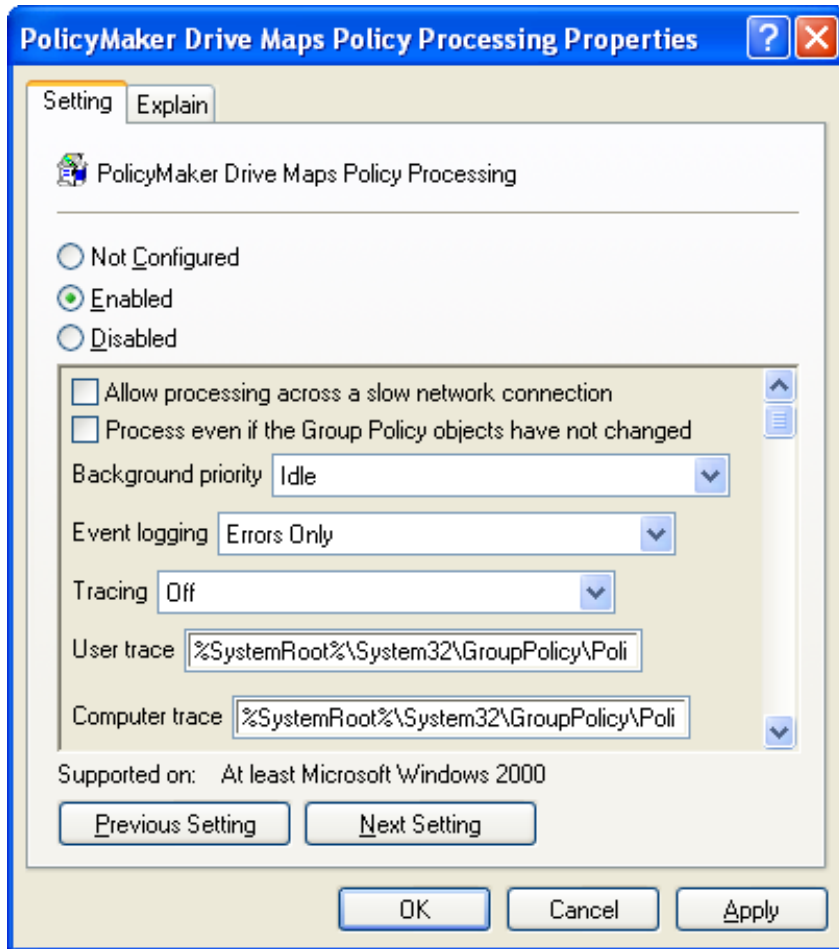
CSE policies control the behavior of each PolicyMaker CSE independently and for all use on a given computer. Note that the default values for these policies match the behavior of the CSE if no policy is set. This is not the case with many of the corresponding Microsoft CSE policies.



The screenshot shows the Group Policy Object Editor window. The left pane displays a tree view of the GPO structure, with the 'DesktopStandard' folder under 'Administrative Templates' selected. The right pane shows a list of 25 settings with their current states. The settings are as follows:

Setting	State
PolicyMaker Applications Policy Processing	Not configured
PolicyMaker Application Security Policy Processing	Enabled
PolicyMaker Data Sources Policy Processing	Not configured
PolicyMaker Devices Policy Processing	Not configured
PolicyMaker Drive Maps Policy Processing	Not configured
PolicyMaker Environment Policy Processing	Not configured
PolicyMaker Files Policy Processing	Not configured
PolicyMaker Folder Options Policy Processing	Not configured
PolicyMaker Folders Policy Processing	Not configured
PolicyMaker Ini Files Policy Processing	Not configured
PolicyMaker Internet Settings Policy Processing	Not configured
PolicyMaker Licensing Policy Processing (1.0 to 1.02)	Not configured
PolicyMaker Licensing Policy Processing (1.1+)	Not configured
PolicyMaker Local Users and Groups Policy Processing	Not configured
PolicyMaker Mail Profiles Policy Processing	Enabled
PolicyMaker Network Options Policy Processing	Not configured
PolicyMaker Network Shares Policy Processing	Enabled
PolicyMaker Power Options Policy Processing	Not configured
PolicyMaker Printers Policy Processing	Enabled
PolicyMaker Regional Options Policy Processing	Not configured
PolicyMaker Registry Policy Processing	Not configured
PolicyMaker Scheduled Tasks Policy Processing	Not configured
PolicyMaker Services Policy Processing	Not configured
PolicyMaker Shortcuts Policy Processing	Not configured
PolicyMaker Software Update Processing	Enabled
PolicyMaker Start Menu Policy Processing	Not configured

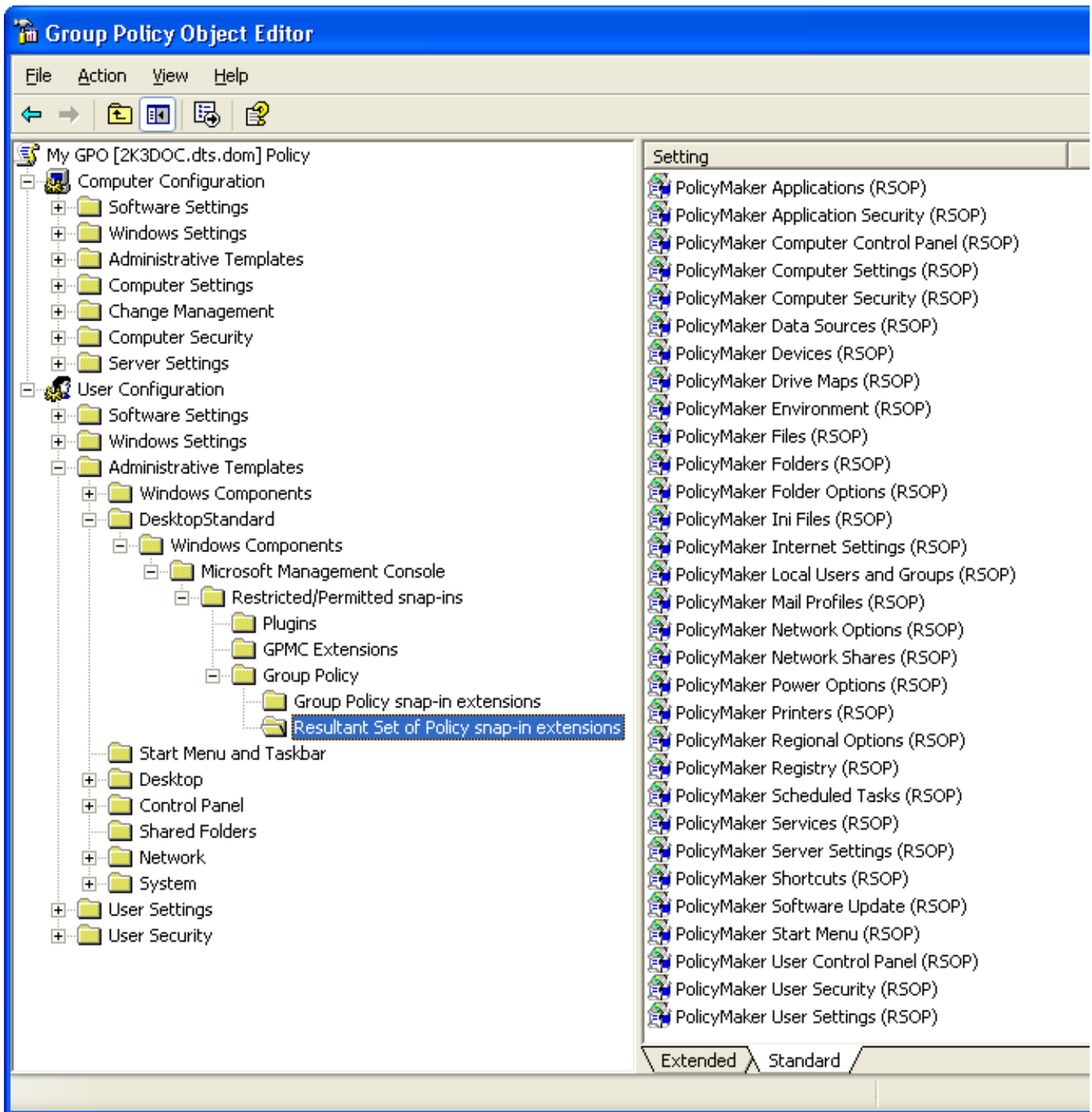
The first two (or three) checkboxes affect Winlogon processing of the CSE. The remaining items are implemented by the particular CSE when it runs. These include the following options:



- Background priority may be specified, so that you may elevate the processing priority of the CSE's thread.
- Event logging can be elevated to include warnings, or warnings and informational messages.
- Tracing can be turned on.
- User, Computer, and Planning Mode alternate trace file paths may be specified.
- Max Trace File Size can be set.

#### Snap-in/RSoP Extension Policies

Snap-in policies exist in the user configuration portion of the desktopstandard.adm. These policies are simple enable/disable settings that allow an administrator to restrict access to PolicyMaker snap-in extensions. A disabled extension will not appear in the GPOE and cannot therefore be utilized by the user (i.e. lower-level administrator) to whom the policy has been applied.





## Browsers

---

PolicyMaker includes a common system of network and other object browsers. Browsers make data entry simpler and more accurate for administrators. The types of browsers are listed below.

---

### Active Directory Browsers

Native Active Directory browsers are used to browse all types of directory objects, as well as local computer objects.

---

### Command Line Browser

Used to browse a list of running processes and sample command lines.

---

### File Browser

Select any file, various masks may be applied. Can also create and/or delete files and/or folders from within this browser.

#### Selecting Network Paths

When selecting a path to an object for use in a configuration, the path to the object must be addressable by the end-user (or SYSTEM) context. For this reason local paths are not generally advisable.

---

### Folder Browser

This browser is based on the Shell Object Browser. Can also create folders from this browser.

#### Selecting Network Paths

When selecting a path to an object for use in a configuration, the path to the object must be addressable by the end-user (or SYSTEM) context. For this reason local paths are not generally advisable.

---

### Icon Browser

Used to browse files and icons within a selected file.

---

### Data Source Browser

Used to import ODBC data source names (DSNs), ODBC driver names, and connection attributes into a Data Source policy setting.

---

### Device Browser

Modeled after the Windows Device Manager and used to locate devices for a Device policy setting.

---

### Printer Port Browser

Browse to any locally installed port monitor to select a LPR or TCP/IP printer port.

---

### ProgId Browser

Implemented in a drop-down on File Types policy.

---

### Registry Browser/Wizard

The Registry Browser appears similar to Regedit and can browse any key or value on the local computer. The Registry Wizard is similar to the Registry Browser, but supports multiple selection of keys and/or values. Selection of a key does not automatically select child keys and values.

---

### Service Browser

Select any system service from the local computer for use in Services policy.

---

### Shell Object Browser

Select any shell object anywhere on the network. These objects are not addressed using standard path syntax, however the "paths" to these objects are generally relative and can be therefore applied from one computer to another.

---

### VPN/DUN Browser

Used to copy information from an existing remote access connection into a policy.

---

#### Variable Selector

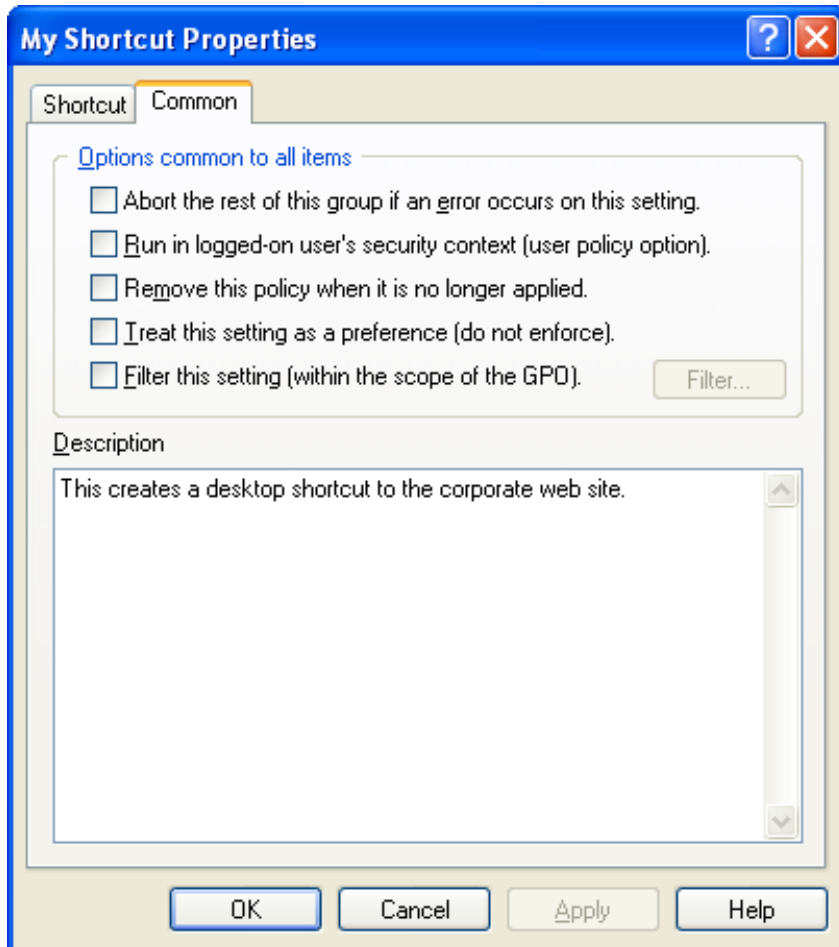
Select [variables](#) from a list of names and descriptions. Used to automatically insert variables into configuration data in resolved or unresolved syntax. Content is controlled by an [XML document](#) installed with the snapin.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Common Tab

The "Common" tab is appended to the property sheet of all configuration items. This item controls features that are common to all items.



Abort the rest of this group if an error occurs on this setting.

This option refers to any configuration or other error that may occur while processing this particular item, and does not apply to policy system failures. If an error is unsuppressed, then processing of subsequent settings in the particular extension, for the one affected GPO, will cease and a failure event will be recorded for the failed item. The extension will restart processing on settings in subsequent GPOs. Note that in a hierarchy such as Mail Profiles policy, a parent item will suppress any child errors.

The default for most item types is to not abort (error suppression on). In this case an error will be logged as an [informational event](#) and processing will continue with the next item. If no errors occur, or if all errors are suppressed, the extension will record an overall success event. If an error is not suppressed, the even log will record it as an error. Mail Profiles policy service items do not suppress errors by default.

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

**This user policy option is disabled in computer configurations.** All PolicyMaker user configuration items have the option to utilize either the logged-on user security context, or the SYSTEM security context. Computer configurations may run when no user is logged on and therefore have access only to the SYSTEM security context.

The default for most items is to run in the SYSTEM security context. However, Mail Profile policy runs in user security context by default. Some items always set user security context when making a particular API call that may always require user context, while other parts of that item will honor the specified context. This is the case with Shared Printer policy, which always uses user context to map the printer share, but by default uses SYSTEM context to install drivers. All context switching can be monitored in the [trace output](#).

This setting may be useful when accessing the logged-on user's network resources. In SYSTEM context the extension has access to everything on the local computer, and can be given access to network resources by adding the target computer to the resource ACL. In the logged-in user's context, the extension will have permissions to only the local and network resources to which the user has access.

 Important

This option is not transitive (does not affect the security context of child items).

Remove this policy when it is no longer applied.

This powerful setting, also known as "purge mode" requires a good deal of understanding.

If enabled, this item causes an individual policy to be removed every time it is processed. For some items that may only be in foreground processing, but for background processing this may happen at each refresh interval. PolicyMaker retains a history of each policy configured until the next processing occurs. Each policy in the history that has this option set, and previously passed filtering, will be run in its own "delete mode" prior to processing the GPO's current policy settings.

This option is disabled if the policy is performing a delete action, since the policy leaves nothing to remove.

This item is only available on items that constitute a single "policy setting". Service items, for example, are part of Mail Profile policy and do not constitute individual policy settings.

#### Note

For most PolicyMaker items, the result item defines the policy setting. However more complex policies, such as Mail Profiles, define the policy on an intermediate level. In Mail Profiles policy, the policy is determined solely by the profile name on the profile item, and service items are merely part of that policy. Since only whole policies may be removed using this option, it is disabled on items (such as service) that are not themselves policies.

#### Optimization

Placing settings into purge mode will cause more processing than if settings are not in purge mode. If you limit the use of this mode, you can reduce the amount of processing that takes place. Regardless, every time a change is made to an extension's settings for a given GPO, the previously applied purge mode settings from that GPO for that extension will be deleted and the new ones applied.

The result of using this option is to cause any setting that is no longer applied, for any reason, to be removed. This includes settings that are no longer set because of PolicyMaker options (filtered out, deleted, disabled or "redlined"), but also to any GPO level action, such as GPO security restrictions, WMI filters, full/partial disabling, de-linking, deletion or removal of the user/computer from the GPO's scope of management (SOM).

#### Effect of Action Modes

Many policies implement action modes that may result in the policy not performing any actual configuration. For example, Registry policy has the option to Create, Replace, Update, or Delete a registry key. Create, Replace and Update all allow purge mode, because they are non-delete actions. In Create mode, if the target key already exists, the key is not configured by PolicyMaker. Nonetheless, if this policy is in purge mode, the key (and all of its sub-keys and values) will be deleted on the next refresh interval. The rule is that any policy configured with a non-delete action mode will be removed by purge mode. Item types that do not have action mode options (such as Applications) are considered to be configured with non-delete action modes.

Treat this setting as a preference (do not enforce).

This option configures a special filter, known as a "run once". At client side processing of the item, this option places a unique value it into HKEY\_LOCAL\_MACHINE for a computer configuration item and in HKEY\_CURRENT\_USER for a user configuration item in the following location:

`\Software\DesktopStandard\PolicyMaker\Client\RunOnce\{unique id}`

If the registry value is found the next time the item is evaluated, the item is skipped. This changes the setting into a preference in that it will only be applied one time. In "purge mode" this setting is disabled, since removal of the policy at each pass cancels the desired effect of the option. If this option is not specified, then the item will be configured each time policy is refreshed. Note that this option is processed regardless of the results of the true filter settings for a given item.

Filter this setting (within the scope of the GPO).

Select this option to enable the "Filter..." button. If the option is already selected, the item already has a filter.

Deselecting the option erases all of the items filters upon apply. Filters are edited using the filtering window, which is presented when the "Filters..." button is clicked. Filters are applied to individual items before they are processed. See [filtering](#) for more information on configuring individual and combined filters.

#### Description

This field is provided for you to document your individual settings. The contents of this field can be seen in the MMC 2.0 "Extended" view (left side of the result pane) when the item is selected, and is also visible in the MMC description bar (which is off by default), and in both GPOE and RSoP settings reports.

#### PolicyMaker View Extension

All Common tab settings are presented in the MMC 2.0 view extension in the "Processing" and "Description" windows for convenience. Note that changes to values are not reflected until an item is reselected.

## Disabling Items

---

Any item may be disabled in order to remove it from client side processing without removing its configuration data from the GPO. To disable any item, select the item in the GPOE and press the disable toggle button on the item's toolbar. To reenable a disabled item, press the same toggle button again. If the button is red (click to disable) the item is enabled, if the button is green (click to enable), the item is disabled. All disabled items are ignored by CSEs.

### Working Offline

An easy way to disable all settings in an extension is to disable the extension's root item (i.e. the "Printers" node). This allows for changes to be made to any settings within that extension without causing any client side configuration of those settings. When the configuration is complete, simply reenable the root extension. Note that if settings are in [purge mode](#), disabling them will cause them to be removed if they are still disabled when policy is next applied.

### Performance

If all settings in a particular extension are disabled in a given GPO, either for user or computer settings, the corresponding CSE will still be run for that GPO in the user or computer context as appropriate. In order to prevent CSE execution for a given extension, you must either disable the extension's root item, or delete all settings in that extension. If no GPOs contain settings for a given CSE, it will not be run on the client computer.

If an extension has no children and is disabled, its settings file will be deleted from the GPO. Note that the next time the GPO is opened, the extension icon will not be dimmed, since there is no settings file to store that state. This is the expected behavior, as the extension is reset to the same state it would be in if the GPO was first created and there were no changes to the extension. Removing the settings file removes it from SYSVOL replication.

### Note

PolicyMaker HTML [settings reports](#) do not reflect disabled items, however XML settings reports show all items.

---

## Event Log

---

### Event Viewer Interpretation

The Event Viewer snapin will present messages from PolicyMaker CSEs. All PolicyMaker events are written the Application log. The "Source" will be the name of the particular CSE (e.g. "DesktopStandard Drive Maps").

### Microsoft Operations Manager (MOM)

See the [PolicyMaker Management Pack](#) (PMMP) topic for monitoring PolicyMaker events on critical computers using MOM.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Microsoft Operations Manager (MOM) Management Pack

---

The PolicyMaker Management Pack (PMMP), for monitoring PolicyMaker events on critical computers, is installed to the following location as part of the main product installation.

[DesktopStandard\Management Packs\pmmp.akm](#)

This can be used in conjunction with the Microsoft [Group Policy Management Pack](#) (GPMP) to monitor all relevant Group Policy events.

PolicyMaker Registry Extension includes the MOM 2005 MOM Pack. Previous versions shipped with the MOM 2000 MOM Pack. The MOM 2000 MOM Pack is available from DesktopStandard support.

See the [Event Log](#) topic for more information.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Writing a Plugin

---

PolicyMaker implements a robust and standards-based plugin system. The plugin architecture allows anyone to write a fully-integrated graphical extension to PolicyMaker, giving that extension the ability to utilize and control the capabilities of the PolicyMaker system - which also includes automatic support for ProfileMaker.

### Built-In Plugins

PolicyMaker supports extending two configuration item types using plugins. These are [Applications](#) and [MAPI Services](#). PolicyMaker application plugins are designed for more general use than service plugins, however they are implemented in exactly the same manner. PolicyMaker ships with 9 application plugins and 15 service plugins. These are grouped so that one DLL implements all application plugins (appext.dll) and one DLL implements all service plugins (svcext.dll).

### Microsoft Specifications

The plugin model is based entirely on the MMC property sheet extension model from Microsoft. [Platform SDK documentation](#) includes sample code for extending an existing snap-in property sheet. Although writing a robust MMC snap-in is a complex task, implementation of a single property sheet extension is relatively simple for an experienced software developer. A snap-in extension is implemented as a single COM object and can be built and shipped as a single self-registering DLL.

### DesktopStandard Specifications

PolicyMaker plugins are based on the principle that the plugin vendor will supply a set of property pages that extend the primary page, which is supplied by PolicyMaker. There is a common primary page used by all application plugins, and a common primary page used by all service plugins. This page is always implemented as "tab zero" in the property sheet. Note that PolicyMaker also implements the [common tab](#) on all property sheets, and this tab will generally display as "tab 1".

#### Step 1

Write a property sheet extension according to Microsoft specifications.

#### Step 2

Extend the appropriate PolicyMaker node. Extending one of the two node GUIDs is a matter of following instructions in the Microsoft Platform SDK documentation referenced above.

In order to extend PolicyMaker's application property sheet, a plugin must register its property sheet extension to extend the following node GUID: [{C8535E2E-148D-494d-8E9A-71FC46649B5E}](#)

In order to extend PolicyMaker's service property sheet, a plugin must register its property sheet extension to extend the following node GUID: [{E8FA1F11-2562-4fc1-ADD4-DBF9161B98FC}](#)

#### Note

Once a node is extended by a functional property page extension, [all instances](#) of that node will have the new property page(s) incorporated. Restricting the presentation of the extension pages to the appropriate content is the responsibility of each plugin. That process is outlined in the steps below.

#### Step 3

Obtain the [IXMLDOMDocument](#)\* from the primary snapin's [IDataObject](#)\*. This process is described in general Microsoft [Platform SDK documentation](#) as well. The required parameterization follows:

```
#define CCF_AUTOPROF_XMLDOM L"CCF_AUTOPROF_XMLDOM"

IXMLDOMDocument* pXmlDom = NULL;

CLIPFORMAT cfApmXMLDOM = ::RegisterClipboardFormatW( CCF_AUTOPROF_XMLDOM );

FORMATETC formatetc = { cfApmXMLDOM, NULL, DVASPECT_CONTENT, -1, TYMED_HGLOBAL };

STGMEDIUM stgmedium = { TYMED_HGLOBAL, NULL };

stgmedium.hGlobal = GlobalAlloc( GMEM_SHARE, sizeof( pXmlDom ) );

HRESULT hr = lpIDataObject->GetDataHere( &formatetc, &stgmedium );

if ( SUCCEEDED( hr ) )
```



```

{
    LPBYTE pbNewData =
    reinterpret_cast<LPBYTE>( ::GlobalLock( stgmedium.hGlobal ) );

    if ( pbNewData == NULL )
    {
        hr = E_UNEXPECTED;
    }
    else
    {
        ::CopyMemory( &pXmlDom, pbNewData, sizeof( pXmlDom ) );

        if ( !::GlobalUnlock( stgmedium.hGlobal ) )
        {
            hr = HRESULT_FROM_WIN32( GetLastError() );
        }
    }
}

if ( stgmedium.hGlobal != NULL )
{
    if ( ::GlobalFree( stgmedium.hGlobal ) != NULL )
    {
        hr = HRESULT_FROM_WIN32( GetLastError() );
    }
}
}

```

The call to `IDataObject::GetDataHere( &formatetc, &stgmedium )` returns a 32 bit interface pointer to an `IXMLDomDocument` object. This object is the XML document for the item which launched the property sheet with the PolicyMaker snap-in. If the item is being added to the snapin for the first time, this document will be assigned to the item that is created upon first Apply/OK of the property sheet. This document is kept in scope for the life of the property sheet (at a minimum). The interface is reference-counted as the result of the `GetDataObject()` query and as such must be released when the property sheet extension is destroyed. Note that the life of a property sheet extension completely ends when the property sheet is closed. At that point it is released by the MMC (which initiated its creation).

The XML document is the key to PolicyMaker integration. This document contains several key pieces of information:

- the GUID of the item that was extended (root element's "clsid" attribute)
- the GUID registered by the plugin, see below (root element's "extid" attribute)
- all of the display information for the snap-in item (root element)
- all of the configuration information for the CSE ("Properties" element)
- all of the filter information for the CSE ("Filters" element)
- all of the [common tab](#) parameterization (root element)

The plugin has the ability to modify, delete, and/or add to any of these parameters at will. Note however that the document must follow PolicyMaker schema, which is not formally specified at this point. To ensure compliance with the schema, generate data using the PolicyMaker GUI for a built-in item, and then mimic this format within the plugin.

#### Note

By properly configuring the XML document, a plugin can actually create new items below the object that it is extending, and after a first apply, these items will expand within the snap-in extension. These items must be limited to items that are supported in that context.

#### Important

The root element's "clsid" and "extid" attributes should not be changed or removed. This could lead to unexpected behavior and is not supported.

#### Step 4

Implement support for PolicyMaker menu integration. This will cause the extension to appear in the list of supported extensions in the context menu (for either application or service as appropriate). This also provides PolicyMaker display information and the extension GUID which is provided back to the extension in the "extid" XML attribute (see above). The following example lists the required registry settings for an application plugin and a service plugin. All values are REG\_SZ type. "(Default)" refers to the default (i.e. unnamed) value, and presents in the snapin's status bar as a menu item is highlighted.

##### Application Plugin

```
HKEY_LOCAL_MACHINE\SOFTWARE\DesktopStandard\Plugins\Applications\Outlook 2002
(Default) = Outlook 2002 Application Properties
ExtId = {534C025C-CA82-4C32-A4B9-A3FC4A35D48F}
Snapin = {6A712058-33C6-4046-BCF9-0EA3A8808EDC}
```

##### Service Plugin

```
HKEY_LOCAL_MACHINE\SOFTWARE\DesktopStandard\Plugins\Services\Exchange Service
(Default) = Exchange Service Properties
ExtId = {252E3DD2-6767-4FFC-9213-AC018E0DAB72}
Snapin = {61B613EC-ACF7-45F5-8916-A366C9F255E1}
```

##### Note

PolicyMaker bundles all extensions of a type in the same DLL. This results in a common Snapin CLSID for each extension by type. This complicates extension integration and is not a requirement, nor is it recommended for inexperienced snapin developers.

##### Important

Do not use the GUIDs or CLSIDs listed above. These are registered to the "Outlook 2002" application plugin and the "Exchange Service" plugin respectively. Generate a new CLSID for each extension snapin and a new GUID for each extension.

#### Step 5

Exclude plugin integration unless the XML document's root element includes the "extid" attribute of the extension. Simply don't add any property pages, and return S\_FALSE if "extid" does not match the registered ExtId for your extension (see step 4). This prevents extension of incorrect item types.

```
// NOTE: 'pXmlDom' is from the code example in step 3.

#define STRING_MATCH 0

const WCHAR g_szwExtId[] = L"{5F6A652F-1FA2-4A5C-B4DB-48D5D8095F47}";

bool bAddPage = false;

IXMLDOMNode* pAttExtId = NULL;

// get the "extid" attribute:
hr = pXmlDom->selectSingleNode( L"/Application/@extid", &pAttExtId );

if ( hr == S_OK )
{
    BSTR bstrExtId;

    hr = pAttExtId->get_text( &bstrExtId );

    if ( SUCCEEDED( hr ) )
    {
        // use case insensitive comparison:
        int nResult = _wcsicmp( bstrExtId, g_szwExtId );

        if ( nResult == STRING_MATCH )
        {
            // this is the correct extid, create property page:
            bAddPage = true;
        }
    }
}
```

```

    }
    else
    {
        // this is some other extid, skip property page creation:
        bAddPage = false;
    }

    SysFreeString( bstrExtId );
}

pAttExtId->Release();
}
else
{
    // "extid" attribute was not present:
    hr = E_UNEXPECTED;
}
}

```

#### Step 6

Implement an apply handler on each page.

PolicyMaker intercepts the apply notification (PSN\_APPLY) on tab zero. This is the only tab that is guaranteed to have been visited. Unvisited tabs do not get an apply notification, however all visited tabs will get the notification from the property sheet. **This event should be ignored by the plugin's property pages.**

Instead of handling the apply message, implement an apply handler that traps the OnQuerySiblings( 0xFF00, 0 message, which PolicyMaker sends from tab zero. This message is passed by tab zero to each tab sequentially during an apply event. Any tab can suspend the apply (due to data validation failure or otherwise) by returning a non-zero value.

#### Note

The above process is necessary to ensure that a visited tab handles the apply notification and that each tab has completed its apply before the XML document is released. Tab zero issues the apply event to its snap-in item immediately after it completes the custom apply handler. The snap-in item at that point may destroy document, and will do so in certain circumstances (i.e. new item creation).

#### Important

Do not write to the XML document unless an apply has occurred. PolicyMaker will consider the document as unchanged unless it receives an apply event, and this event cannot be initiated by the plugin.

#### Step 7

Implement user interface. Read XML into controls in each property page's OnInitDialog(). Update the XML document in each page's apply handler.

#### Note

Any element that contains the attribute/value `disabled="1"` is ignored by Policy client-side processing and i ProfileMaker is stripped from the deployed configuration.

#### Step 8

Implement help support (optional). Help is implemented using the integrated MMC HTML help system, according Microsoft Platform SDK documentation. If properly implemented, the extension's help file should be merged into main help file for the PolicyMaker snapin, just as are the DesktopStandard application and service extensions.



#### ProfileMaker Support

ProfileMaker and PolicyMaker share a common extensibility model. The plugins that ship with PolicyMaker also support ProfileMaker, and as such install into a common folder. **Any plugin written to specifications will support both ProfileMaker and PolicyMaker.** ProfileMaker is a product with similar capabilities as PolicyMaker, however it supports Windows 9x and NT4 platforms in addition to Windows 2000+.

#### Licensing

PolicyMaker Standard Edition includes full support for DesktopStandard plugins. Any party may write a plugin to specifications and utilize it within PolicyMaker Standard Edition without additional PolicyMaker licensing considerations. Third party plugin licensing considerations are outside the scope of PolicyMaker licensing.



## Policy Processing

Client Side Extension (CSE) processing order is calculated by the operating system, which initiates each CSE. During each policy refresh interval, the operating system determines which CSEs should be launched based on several criteria, including the following:

- Computer/user processing
- Settings changes/policy
- Slow link detection/policy
- Background/foreground/policy
- Registry policy success/failure
- Access restrictions
- Enabled/disabled
- WMI filters
- Enforcement
- Inheritance blocking
- Loopback processing

It should be clear from the list above that determining why a CSE is not being launched by Windows is often a complex troubleshooting task. This process is the subject of much published information, and as such is not within the scope of this document.

### Processing Order

The CSEs that are to be launched are launched in the order listed below. This ordering is the same for user and for computer policy, although these two modes operate entirely independently.

CSE Name	CSE GUID
PolicyMaker Environment Variables	{08E9566B-1390-4bfb-B19F-EA465BAD922D}
PolicyMaker Local Users and Groups	{08F5166F-E66B-4F15-80BF-DE94F083472A}
PolicyMaker Application Security	{090CB18E-9CCD-42BA-BD10-53F5F7A3F9F4}
PolicyMaker Devices	{0947EA96-E4DE-48C5-99AD-FCC1829FFE86}
Wireless	{0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63}
PolicyMaker Network Options	{15D30905-443F-4097-8FA8-0A2E35B475DC}
PolicyMaker Drive Maps	{1EA5E892-2292-438f-8D05-40E7B0007585}
Folder Redirection	{25537BA6-77A8-11D2-9B6C-0000F8080861}
Registry (ADM Templates)	{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Microsoft Disk Quota	{3610EDA5-77EF-11D2-8DC5-00C04FA31A66}
QoS Packet Scheduler	{426031c0-0b47-4852-b0ca-ac3d37bfc39}
Scripts	{42B5FAAE-6536-11d2-AE5A-0000F87571E3}
Security	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Internet Explorer Branding	{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
EFS recovery	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
Software Installation	{C6DC5466-785A-11d2-84d0-00c04fb169f7}
PolicyMaker Software Update	{D58ABC6E-E15E-4AC2-B446-EEC37B6B45FB}
IP Security	{E437BC1C-AA7D-11D2-A382-00C04F991E27}
PolicyMaker Folders	{F0DB2806-FD46-45b7-81BD-AA3744B32765}
PolicyMaker Files	{F17E8B5B-78F2-49a6-8933-7B767EDA5B41}
PolicyMaker Data Sources	{F27A6DA8-D22B-4179-A042-3D715F9E75B5}
PolicyMaker Ini Files	{F55DA052-16E1-434b-803F-F6A9F6945957}
PolicyMaker Services	{F581DAE7-8064-444A-AEB3-1875662A61CE}
PolicyMaker Folder Options	{F5BFF32F-D563-460D-8764-890933FB03C0}
PolicyMaker Scheduled Tasks	{F648C781-42C9-4ED4-BB24-AEB8853701D0}
PolicyMaker Registry	{F6E72D5A-6ED3-43d9-9710-4440455F6934}
PolicyMaker Applications	{F9C77450-3A41-477e-9310-9ACD617BD9E3}

PolicyMaker Printers	{FD023FFE-C165-40d5-A201-439FC65AC8A5}
PolicyMaker Shortcuts	{FD2D917B-6519-4BF7-8403-456C0C64312F}
PolicyMaker Mail Profiles	{FD44098A-CA65-4054-8A70-EBAFAB263C70}
PolicyMaker Network Shares	{F0EA65FA-3D73-472D-99E5-7E577FD0984B}
PolicyMaker Internet Settings	{FEF373ED-6CBE-4294-83EC-008D502B394A}
PolicyMaker Start Menu	{FF87F78A-E3A2-4AAE-B049-7E6BB1670D7B}
PolicyMaker Regional Options	{FFAA00BB-0D9B-401B-B71B-EF5ED1D88E6D}
PolicyMaker Power Options	{FFC64763-70D2-45BC-8DEE-7ACAF1BA7F89}

## Processing is always Sequential

CSEs always process policy in order and one after the other, i.e. sequentially, for user or computer configuration.

### Note

Given that these two types of configuration operate independently, it is also possible and not uncommon for user and computer processing to occur simultaneously.

As a result policy can be "chained" in order to leverage the results of one in another. For example, a PolicyMaker Drive Maps policy may set a drive map to the end-user's home directory. This drive map can be referenced in Microsoft's Folder Redirection policy. Later the PolicyMaker Folders policy can create nested folders within the drive, PolicyMaker Files policy can copy a file to the new folder, and PolicyMaker Mail Profiles policy can configure a Personal Folders service to point to that file. Extensions are ordered to optimize the potential for policy chaining.

## Foreground, Background and Asynchronous Processing

This is possibly the most misunderstood aspect of Group Policy processing. Asynchronous processing does not mean that CSEs are processed out of order or processed concurrently, that GPOs are processed out of order, or that "cached" GPOs are applied. These are never the case (with the exception that user and computer policy may process simultaneously, as noted above). Processing is always ordered and sequential. Asynchronous processing is simply a reference to the asynchronous foreground mode of policy processing. Policy is processed in two basic modes, foreground and background. However, foreground mode is split into synchronous foreground and asynchronous foreground. The mode in which the computer processes policy in the foreground is subject to several factors, but the change in processing is relatively simple.

Asynchronous processing is nothing more than background refresh that starts during the logon or startup process. The essential difference with asynchronous processing is that it does not hold up the logon or startup process, thereby giving the end-user the impression that the process is faster. However, there are important things to consider when allowing Group Policy to process in the foreground asynchronously.

1. The most important consideration is that settings that would otherwise be applied before the user has access to their environment, are not applied until later. This may have negative security or end-user experience implications.
2. Some individual policy settings will only take effect if set before the computer or user logon process completes. For example, when the explorer loads it may look for the policy that sets the wallpaper, and load the default wallpaper if the policy is not set. Of course it must do this or the wallpaper would be changing right before the end-users' eyes. As a result, these policies have no effect if not run in synchronous foreground. As we will see, this produces some unpredictable results.
3. Some policy types will only be effective when run in synchronous foreground. For example Microsoft's Disk Quota CSE disallows background processing (which also prevents asynchronous foreground processing). One might think that this would result in Disk Quota policy never being applied unless the computer had asynchronous processing disabled, which would be the case if it were not for something call ForceRefreshFG, which also produces some unpredictable results.
4. It's also important to note that while some CSEs are generally documented to only apply policy in one mode or another, they may in fact be registered to run in both modes. For example, Microsoft's Software Installation policy processes in all three modes, but performs different actions in synchronous foreground vs. background/asynchronous foreground. While this policy type is not registered to require foreground processing, the features that only run in foreground do require it. However, because the extension allows background and asynchronous processing, the system is never forced into synchronous processing because of this policy type alone. This too can lead to unpredictable results.

### Tip

From the above four situations, it should be clear that it might be best to avoid asynchronous foreground processing altogether.

## What's in a Name?

The name asynchronous is meant to indicate that the logon process executes concurrently with Group Policy processing, not that the Group Policy extensions process concurrently with each other. Interestingly, the name foreground is a reference to the fact that during such processing the startup/logon splash window is presented and the Group Policy extensions have the opportunity to write status messages to this window. The window is in the

"foreground". Some people have taken the fact that there is also a shutdown/logoff window, and that fact that there are shutdown/logoff scripts, to mean that "foreground" is also a reference to shutdown/logoff. Although these windows may actually state that Windows is processing policy, this is in fact not technically accurate. No Group Policy processing occurs at shutdown or logoff (what would be the point?). Logoff and shutdown scripts are executed at this time, however such scripts are not Group Policy. Microsoft's Scripts policy only configures the registry to run scripts, but does not run them itself. This also explains why this extension runs in background refresh.

#### Forced into Foreground

A CSE that registers a requirement for foreground processing forces the entire computer into foreground processing, on the next foreground event. In other words, if any one CSE is to be launched, but requires foreground processing, Winlogon will not launch that CSE, and will set the value ForceRefreshFG=1 into that CSE's section of the registry. If during the next startup/logon event, Winlogon sees this value for any CSE, it will initiate policy processing synchronously and thereby be able to launch the extension that requires it. Interestingly, this setting applies to both user and computer processing (as does the configuration option below). Therefore it is likely that user processing would force the computer into synchronous logon and vice versa. This automatic mode switching leads to the generally undesirable effect of some CSEs applying policy only after a second logon or startup, or even at every other logon or startup.

As mentioned in the list above, some individual policies may be processed in background, but may not take effect unless set before logon/startup. As a result these settings may never take effect if some other extension doesn't coincidentally force the system into foreground mode.

#### Configuring Synchronous Processing

Windows 2000 and Windows 2003 Server computers process foreground policy synchronously by default. Windows XP processes foreground policy asynchronously by default. In order to enable synchronous processing (at startup/logon) on Windows XP, you must ensure that the following policy is enabled (and disabled/not configured on Windows 2000/2003):

[Computer Configuration\Administrative Templates\System\Logon\  
"Always wait for the network at computer startup and logon"](#)

This setting ensures that policy completes before the startup/logon is completed. The change to the default setting on Windows XP was designed to speed up startup and logon processing. However, when performing configurations that must take effect before the end-user has access to their desktop, synchronous processing must be enabled.

#### Ordering of GPOs

When a CSE processes its policy, it always processes all GPOs that have settings applied. Winlogon gives each CSE a list of GPOs that have policy settings that may apply to the user or computer, depending on the context (i.e. the changed list). A list of GPOs that formerly had, but no longer have, policy settings is also provided (i.e. the deleted list). Technically, it's up to each CSE to decide exactly what to do with these lists. However, standard processing rules dictate that if the CSE is to execute any policy, it must execute all of its policies from each GPO in the order provided to it by Winlogon. This preserves GPO enforcement and other processing issues related to precedence. If only changed GPOs were ever processed independently, then merely changing one GPO would allow a low-level administrator to override higher precedence policy.

#### Policy Caching

Group Policy objects (GPO) neither download nor cache to network computers. A GPO is a combination of all of the settings in the Group Policy Template (GPT) and the Group Policy Container (GPC). The GPT is file system storage in SYSVOL, and the GPC is Active Directory data. The GPC information is read by Winlogon as it launches CSEs, and the GPT information is read by each individual CSE as necessary. However, given that often one CSE will run, and others will not - even though all may have settings in a particular GPO - it should be obvious that downloading the entire GPO to workstations would cause serious and unnecessary performance problems.

Since GPOs are never downloaded, they cannot be cached. This confusion around this subject is based on several issues. The first issue is the fact that there are aspects of GPO processing that create cached data. For example, Winlogon records a historical list of all GPOs that have been processed for all users, including all extensions that processed policy. This list contains no information about individual policy settings. Therefore it could be said that the GPO is cached, except for the fact that the implications are substantially different than GPO caching.

Some individual extensions also record historical data in order to perform policy removal. Microsoft's Folder Redirection is an example of this. Without this information it would not be possible to remove settings that were previously applied, since the removal often corresponds to an event such as the deletion of the entire GPO by an administrator, and revertible actions taken by CSEs will vary by each computer and/or user.

#### Offline Behavior

When a computer disconnects from the network, and the domain is no longer accessible, policy is no longer processed. GPOs are stored in domains and without access to those domains, policy cannot be processed. If the user logs on with cached domain credentials, it's the same as if they had merely unplugged the computer while on the domain - policy does not process. However, if the user switches to a local account, the computer/user account will then be subject to Local GPO processing. When on the domain, Local GPO processes first (at the lowest priority). When on a local computer account, Local GPO is the only GPO to process. If the computer is then accessible to a different domain, policy from that new domain is now processed - again following the processing of the same Local GPO.





## Root Mapping

---

PolicyMaker supports mapping of a network share to a drive letter, on all operating systems. In some cases it may be desirable to map a subfolder of a network share to a drive letter. This is often referred to as a "root map", owing to its NetWare origins. Windows 2000+ clients connecting to Windows 2000+ servers natively support root mapping.

### Common Use

Root Mapping is useful in creating home directory drive maps for each end-user. By default, Windows servers create home directories as subfolders of a share, and do not share each directory. Root mapping the home directory prevents the need to share each and every user's home directory, and it prevents the end-user from having to browse a long list of user directories in order to locate their home directory on the network.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## RSoP Reports

PolicyMaker includes built-in reporting on Resultant Set of Policy for both logging and planning modes. There are two methods for generating a settings report for any PolicyMaker extension in the RSoP snap-in - XML and HTML.

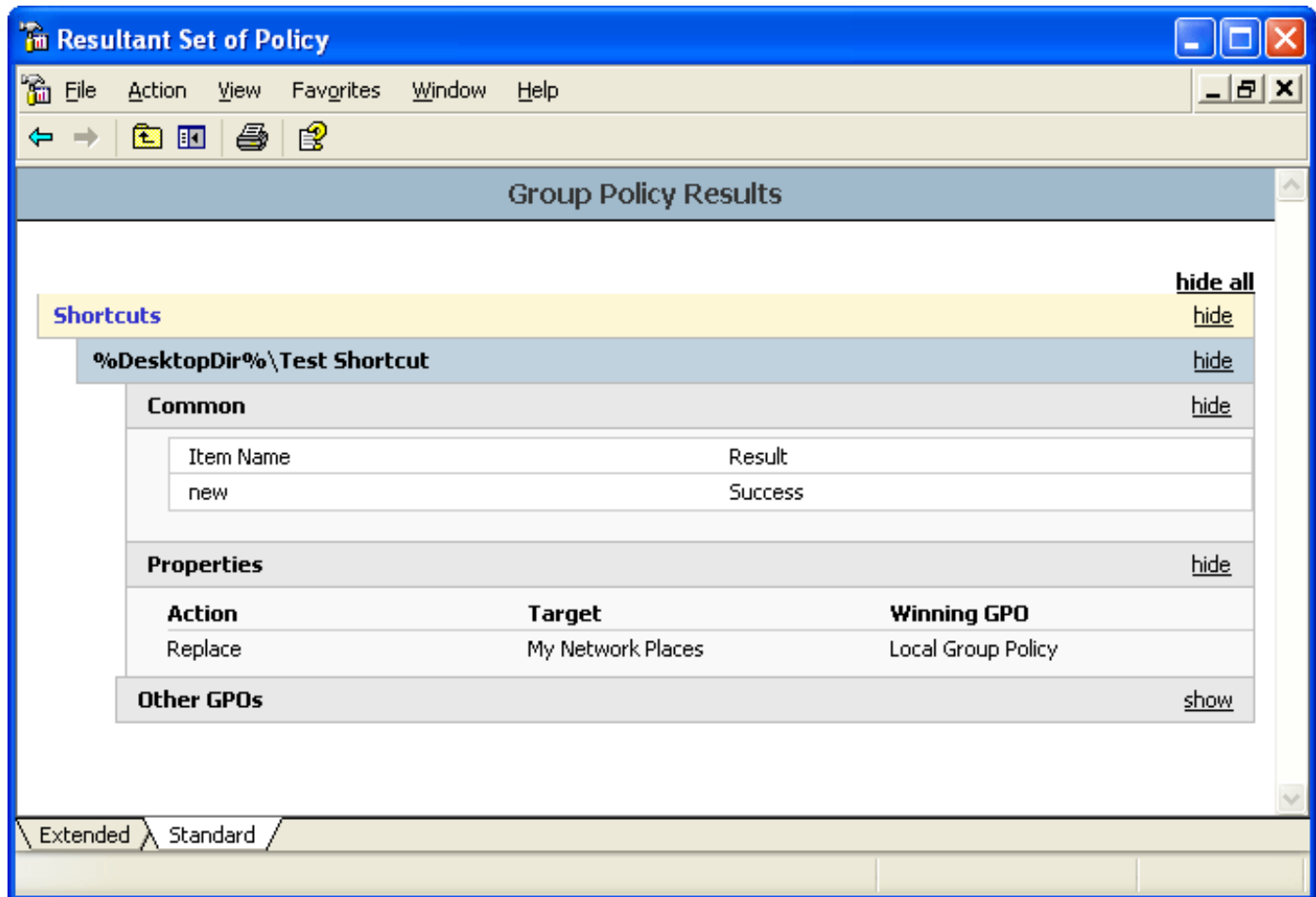
### XML

Each PolicyMaker RSoP item is based on XML data drawn from the RSoP query's result set. All PolicyMaker RSoP extensions expose XML reporting via the MMC print option. Selecting the print toolbar button or context menu option launches Internet Explorer with a copy of the item's XML data. This can then be printed or saved as desired. See the topic [XML Integration](#) for more options relating to XML reporting.

### HTML

The HTML RSoP report is generated by selecting any PolicyMaker extension within the RSoP snap-in. If the extension item does not appear, then there is no data for that extension in the RSoP query's result set. Selecting the item presents an HTML document in the MMC result pane for that item.

This document closely resembles the RSoP settings report from the [GPMC](#). The document is generated by XSLT transformation of the XML data behind the selected item. See [Understanding RSoP Reports](#) for more information.



The screenshot shows the 'Resultant Set of Policy' MMC console. The title bar reads 'Resultant Set of Policy'. The menu bar includes 'File', 'Action', 'View', 'Favorites', 'Window', and 'Help'. The toolbar contains navigation and action icons. The main pane is titled 'Group Policy Results' and displays a tree view for 'Shortcuts'. The selected item is '%DesktopDir%\Test Shortcut'. Below it, the 'Common' section shows a table with 'Item Name' (new) and 'Result' (Success). The 'Properties' section shows a table with 'Action' (Replace), 'Target' (My Network Places), and 'Winning GPO' (Local Group Policy). The 'Other GPOs' section is visible at the bottom. The console has tabs for 'Extended' and 'Standard'.

### Understanding RSoP Reports

PolicyMaker RSoP reports are based on the data written to the WMI repository by the CSE corresponding to the selected RSoP snap-in extension. The data is queried from WMI in XML format, and translated into a single dynamic HTML document in the MMC result view.

If no RSoP data exists for a particular extension, then the RSoP extension will not be present in the RSoP snap-in. If there is an error generating data for a particular extension, the icon of the computer or user configuration item will reflect a warning state, and the property page for the same items will provide summary error information.

RSoP reports include the name of each policy, its particular properties, and data showing what values were set for the policy each time it was applied, and the order in which these settings were applied. This ordering is known as policy precedence. The policy listed first has the highest precedence and therefore was applied last, and is the policy that has lasting effect.

### Notes

Some policies may optionally set multiple settings, and if two instances of the same policy do not set all of the same

settings, some settings from a lower precedence policy may also take effect. Some policies may be marked as preferences, and as such are not removed when the policy is no longer to be applied. These settings may be in effect after the policy is no longer being applied, but at this point these settings are no longer reported in RSoP.

Actions that may affect more than one setting, such as configuring/deleting "all profiles", deleting "all printers", deleting "all drive maps", and deleting "all files/folders" may not give the full picture in RSoP. These options can impact other individual settings but this will not be reflected as such in the precedence reporting.

Setting a "computer" value (such as an HKEY\_LOCAL\_MACHINE registry value) in user policy is allowed but is not considered a best-practice. Since precedence, as reported in RSoP, is limited to the user or computer context, the same actual value set in both will not compete for precedence in the report. Note that this is not generally the case with a "user" value set in a computer config. For example, a HKEY\_CURRENT\_USER registry value set in computer policy will configure the Default User (HKEY\_USERS/.Default), and therefore reflects accurately.

---

## Security Contexts

---

### What is a Security Context?

A user establishes a security context by presenting credentials for authentication (i.e. logon). If the credentials are authenticated, the operating system produces an access token that identifies the group memberships and privileges associated with the user's account. The operating system checks your access token whenever you try to access a resource (i.e. a file, registry setting, network share, etc.). It compares the information in your access token to the accounts and groups allowed or denied access by the object's security descriptor.

### Security Contexts Used by Group Policy

Group Policy provides two security contexts that may be used when executing user policy, and one for computer policy. SYSTEM is not an "administrator", however it does have the permissions of the "SYSTEM" group, which by default is everything on a computer.

### Security Contexts in PolicyMaker

By default, most PolicyMaker items run in SYSTEM context.

#### Exceptions

The exceptions to the above rule are as follows:

1. A user policy item can be run in user security context by selecting the security context option on the [common tab](#) for the item.
  - The common tab security context setting is not transitive. Security context changes are not passed to child items.
  - Filters are not affected by the common tab security context setting.
2. Components of certain user policy items do not function properly in the SYSTEM security context, and are therefore always run in user context. These include:
  - [Security Group](#) filter.
  - [Language](#) filter (User Locale option).
  - [File Match](#) filter (attempts SYSTEM context if user doesn't have permissions).
  - [Drive Mapping](#) APIs.
  - [Network Printer](#) mapping APIs.
  - Default printer setting (for both [Network Printer](#) and [TCP/IP Printer](#) in user context).

### Providing Network Access to the SYSTEM Context

SYSTEM does not have the network permissions of the logged-on user, although it can be given network access. SYSTEM is essentially the computer's "user" account. With Windows 2000/XP/2003 computers that are members of an Active Directory domain, you may add the computers into a security group. This security group may then be given permissions to any network resource on an Active Directory computer. This will give all SYSTEM accounts for the client machines that are members of the security group, access to the network resource.

### Using Drive Maps in SYSTEM context

Drive maps are part of the end-user's user profile. When running in system context, PolicyMaker items will not "see" paths that are provided as end-user drive maps. Use UNC paths instead.

#### Note

The [File Match](#) filter makes an exception in this case and attempts to convert drive maps to UNC paths automatically when running user policy.

## Settings Reports

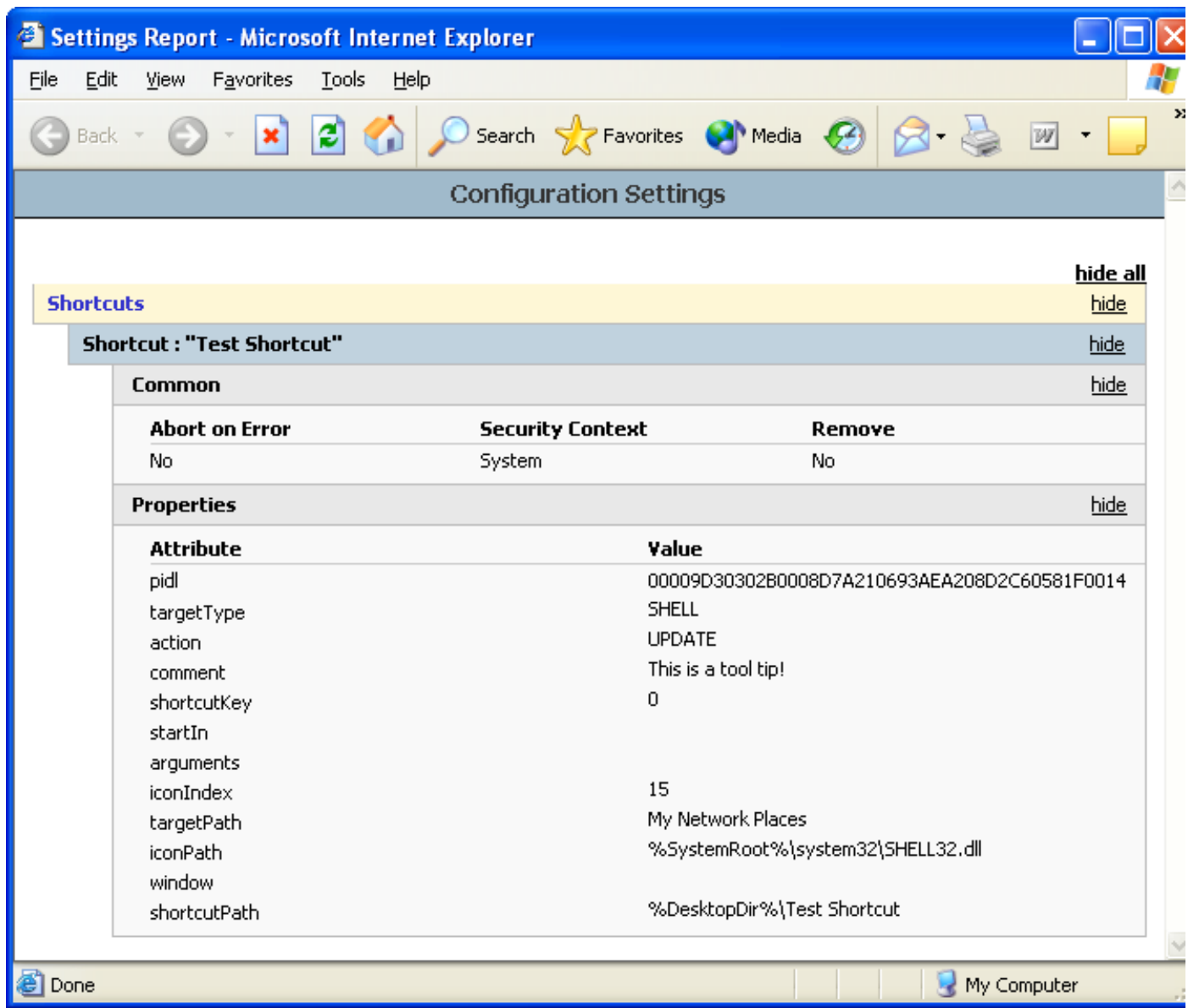
PolicyMaker includes built-in reporting on settings within a configuration. There are two methods for generating a settings report, XML and HTML.

### XML

Each PolicyMaker item, in both the GPOE and RSOP snap-ins, is based on XML data. All items expose XML reporting via the MMC print option. Selecting the print toolbar button or context menu option launches Internet Explorer with a copy of the item's XML data. This can then be printed or saved as desired. See the topic [XML Integration](#) for more options relating to XML reporting.

### HTML

The HTML settings report is generated by clicking the pencil toolbar button or "Settings Report" context menu option on any configuration item. This action will launch Internet Explorer and display the formatted document, reporting on all settings at or below the selected item. This document is generated by XSLT transformation of the XML data behind the selected item and its children. The document is designed for printing, with page breaks after each item. [Common tab](#) descriptions appear in the header of each item. This allows you to document each individual item as you see fit.



**Settings Report - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

**Configuration Settings**

**Shortcuts** [hide all](#)

**Shortcut : "Test Shortcut"** [hide](#)

**Common** [hide](#)

Abort on Error	Security Context	Remove
No	System	No

**Properties** [hide](#)

Attribute	Value
pidl	00009D30302B0008D7A210693AEA208D2C60581F0014
targetType	SHELL
action	UPDATE
comment	This is a tool tip!
shortcutKey	0
startIn	
arguments	
iconIndex	15
targetPath	My Network Places
iconPath	%SystemRoot%\system32\SHELL32.dll
window	
shortcutPath	%DesktopDir%\Test Shortcut

Done My Computer

## Uninstallation

---

### Uninstallation

Both polmkr.msi and polmkrcl.msi may be removed using control panel "Add or Remove Programs". Removal of client side extensions does not remove the WMI namespace expansion or associated RSoP data. Removal of snap-in extensions does not impact data that may have been saved to any GPOs, including the Local GPO.

#### Important

Note that the snap-in extension install also installs the CSEs on that computer, and as such will remove the CSEs upon uninstallation. To remove the snap-in extensions and leave the CSEs, install the polmkrcl.msi and then uninstall the snap-in extensions.

---

## User Interface Conventions

---

### Configuring Policies

Configuring PolicyMaker policy settings is nearly identical to Microsoft policy settings. The main difference is the set of standardized options that are common to each policy. These are listed below.

### Adding New Items

Policy items are added to an extension using the MMC's "New" context/action menu option. The "+" toolbar button serves as a way to easily select the first item in the "New" menu.

### Disabling Items and Extensions

Disable/enable is a PolicyMaker toolbar toggle button option that is available for extensions and all child items. This option is described in greater detail in the [Disabling Items](#) topic.

### XML Reports

An XML report can be generated from any item by selecting the "Print" option from the MMC toolbar or context menus.

### Settings Reports

An HTML report can be generated from any item by selecting the pencil button from the PolicyMaker toolbar. This option is described in greater detail in the [Settings Reports](#) topic.

### View Extensions

MMC 2.0 includes result view extensions that provide details on a selected item. All PolicyMaker items and desktopstandard.adm template settings support view extension data. The description value that can be entered on the [common tab](#) is presented in the view extension by default.

### Refresh

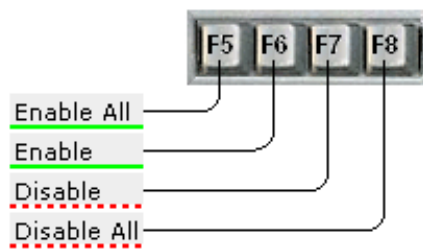
Reloads from XML file settings within the GPO and refreshes all presentation values. This allows an administrator to refresh the presentation if changes were made by another administrator to the same configuration data.

#### Note

PolicyMaker does not currently implement the reload from file feature.

### Property Underlining

Red properties are "disabled" and green properties are "enabled". A disabled property will not be applied during the configuration process. Generally properties are enabled by default unless they require a specific value that, if missing, might cause the application to have problems.



In order to change the underlined state of a property, select the desired property with the mouse (or by tabbing to it) and press F6 to enable or F7 to disable. With any property on a page selected, F5 may be used to enable all properties on the page, and F8 may be used to disable all properties on a page.

Some controls, such as Internet Explorer lists, utilize red/green diamonds for the same purpose as underlining described above. This difference is entirely cosmetic. Red underlines are dashed in order to create greater contrast. For more information see KB article [10017](#).

### Drag and Drop/Cut and Move/Copy and Paste

PolicyMaker includes robust clipboard functionality, including import/export using XML as a native format. Items can be dragged to/from the desktop or other applications.

Additionally, all child items of a root extension can be cut/copied/pasted to any acceptable location. This differs from XML transfer in that items transfer as objects and can be moved and duplicated easily. In MMC 2.0 this includes transfer between two different instances of the MMC, whereas with MMC 1.2 this is only supported in a single instance of the MMC.

#### Tip

You can move or copy settings between GPOs using this feature, and XML transfer makes settings [backup](#) easy.

ProfileMaker includes the same capabilities. Settings can be transferred between ProfileMaker and PolicyMaker, making migration from (or coexistence with) a legacy network a simple task.

#### Move Up/Down

Move up/move down are a pair of PolicyMaker toolbar button options that are available for all children of extension items. This includes scope items, such as the registry collection, and all result items. The processing order executed by the CSE is not always important, however when there is a concern for ordering, this feature allows you to change the processing order easily in the user interface. Scope items reflect their processing order in the hierarchy (top-to-bottom). Result item processing order can be seen in the order column.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.



## Variables

---

PolicyMaker supports Windows environment variables and generates a number of additional process environment variables. Any variable may be used in a configuration parameter value, such as a profile name or path to a PST file. Each help document states whether variables are supported in a specific field.

 **Tip** By using PolicyMaker's [Registry Matching filter](#) and/or [Message Box](#) filter, you can define variables at client run-time, and have these control behavior using the [Environment Variable](#) filter or as values in a policy setting.

### About Environment Variables

The Windows "environment" is a list of variables saved as name/value pairs. To see the current list of variables, type "SET" at the command prompt. Each process, including the desktop (explorer.exe) has a list of variables unique to the process. When one process launches another, normally a copy of the environment of the launching process is passed to the launched process.

### Where does the environment come from?

Environment variables are generated in several ways. The operating system process loads variables from the registry at computer startup (system variables), for users as they log on (user variables), and in certain cases from the "volatile" environment (volatile variables). These are located in the following locations respectively:

- [HKEY\\_LOCAL\\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment](#)
- [HKEY\\_CURRENT\\_USER\Environment](#)
- [HKEY\\_CURRENT\\_USER\Volatile Environment](#)

Variables are also generated from dynamic data by the user's explorer.exe process (i.e. %UserName% and %LogonServer%). Any process may generate additional variables and add them to its own environment. The PolicyMaker CSEs set a number of variables for your use in policy settings. The values for several of these are written to the [trace](#).

### Process and Volatile Variables

Variables set directly into the environment of a process that are not saved to the system or user variable registry keys, are called process variables. These variables go "out of scope" as the process terminates. In other words, they cease to exist. Some applications use the volatile environment registry key to pass process variables from one application to another.

### PolicyMaker Process Variables

PolicyMaker CSEs implement the process variables listed below. All of the variables are supported on all client platforms. In order to test the value of a given variable, place the variable into the contents of a [Message Box](#) filter. When the CSE displays the message box it will contain the run-time value. Unless these variables also happen to be Windows persistent environment variables, they only have definition when used in PolicyMaker settings.

#### Note

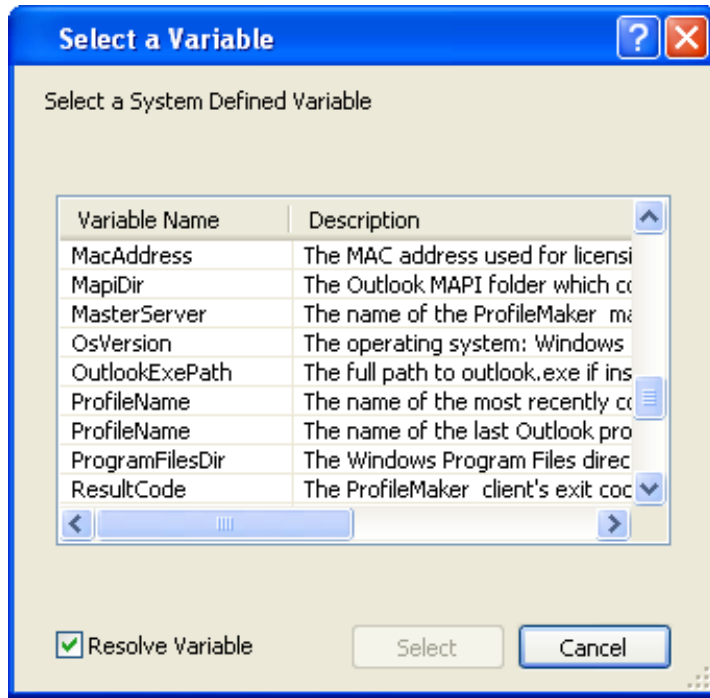
Variables are not text case sensitive.

- [%ComputerName%](#) - The NetBIOS name of the computer.
- [%DomainName%](#) - The domain name or workgroup of the computer.
- [%LogonServer%](#) - The domain controller that authenticated the current user.
- [%DateTime%](#) - The current time (UTC).
- [%DateTimeEx%](#) - The current time (UTC) with milliseconds.
- [%LocalTime%](#) - The current local time.
- [%LocalTimeEx%](#) - The current local time with milliseconds.
- [%OsVersion%](#) - The operating system: Windows 2000 | Windows XP | Windows 2003 | Unknown.
- [%MacAddress%](#) - The first detected MAC address on the computer.
- [%TraceFile%](#) - The path/name of the trace file.
- [%LastError%](#) - The last error code encountered during configuration.
- [%LastErrorText%](#) - The last error code text description.
- [%LogonUser%](#) - The user name of the current user.
- [%LogonUserSid%](#) - The SID of the logon user.
- [%LogonDomain%](#) - The domain of the current user.
- [%LdapUserSid%](#) - The SID of the logon user in LDAP escaped binary format.

- [%LdapComputerSid%](#) - The SID of the computer in LDAP escaped binary format.
- [%BinaryComputerSid%](#) - The SID of the computer in hexadecimal format.
- [%BinaryUserSid%](#) - The SID of the logon user in hexadecimal format.
- [%ReversedComputerSid%](#) - The SID of the computer in reversed byte order hexadecimal format.
- [%ReversedUserSid%](#) - The SID of the logon user in reversed byte order hexadecimal format.
- [%ExchangeUser%](#) - The Windows user name of the owner of the last configured Exchange mailbox.
- [%ExchangeUserSid%](#) - The SID of the owner of the last configured Exchange mailbox.
- [%ExchangeDomain%](#) - The domain membership the owner of the last configured Exchange mailbox.
- [%ExchangeLdapSid%](#) - The SID of the owner of the last configured Exchange mailbox in LDAP escaped binary format.
- [%ExchangeDisplayName%](#) - The display name of the most recently configured Exchange mailbox (not including standard or migration modes).
- [%ProfileName%](#) - The name of the last Outlook profile configured.
- [%TimeStamp%](#) - The time stamp of the configurations being executed.
- [%ResultCode%](#) - The client's exit code.
- [%ResultText%](#) - The client's exit code text description.
- [%ProfileName%](#) - The name of the most recently configured MAPI profile.
- [%MapiDir%](#) - The Outlook MAPI folder which contains the MAPISVC.INF.
- [%TempDir%](#) - The current user's temp directory as determined by Windows API.
- [%WindowsDir%](#) - The Windows directory.
- [%SystemDir%](#) - The Windows system directory.
- [%SystemDrive%](#) - The name of the drive from which the operation system is running.
- [%ProgramFilesDir%](#) - The Windows Program Files directory.
- [%OutlookExePath%](#) - The full path to outlook.exe if installed.
- [%AppDataDir%](#) - The current user's application data directory.
- [%DesktopDir%](#) - The current user's desktop directory.
- [%StartMenuDir%](#) - The current user's start menu directory.
- [%ProgramsDir%](#) - The current user's programs directory.
- [%StartUpDir%](#) - The current user's startup directory.
- [%FavoritesDir%](#) - The current user's Explorer favorites directory.
- [%SendToDir%](#) - The current user's send to directory.
- [%RecentDocumentsDir%](#) - The current user's recent documents directory.
- [%NetPlacesDir%](#) - The current user's my network places directory.
- [%CommonAppdataDir%](#) - The 'all users' application data directory.
- [%CommonDesktopDir%](#) - The 'all users' desktop directory.
- [%CommonStartMenuDir%](#) - The 'all users' start menu directory.
- [%CommonProgramsDir%](#) - The 'all users' programs directory.
- [%CommonStartUpDir%](#) - The 'all users' startup directory.
- [%CommonFavoritesDir%](#) - The 'all users' Explorer favorites directory.
- [%CurrentProcessId%](#) - The numeric identity of the main client thread.
- [%CurrentThreadId%](#) - The numeric identity of the main client process.
- [%PolicyMakerVersion%](#) - The version of the running PolicyMaker CSE.

#### Variable Selector

The variable selector is a special [browser](#) designed for selecting known variables from a descriptive list.



The selector can be launched from any text edit control that meets the following criteria:

- Not disabled
- Not read-only
- Not restricted to a numeric value

To launch the selector, place the cursor in an edit control and hit the **F3 function key**. When a variable is selected, the variable will be inserted in the location of the cursor. When the client runs, this variable will be resolved to its then-current value.

#### ◆ Variable Non-Resolution

To prevent this resolution, uncheck the "Resolve Variable" option in the selector. This will place "<>" characters between the "%%" variable delimiters and the variable name (i.e. "%<ProgramFiles>%"). These will be removed by the PolicyMaker client, and the variable will remain unresolved.

#### 🔧 Customizing the Selector

The selector variable names and descriptions are generated from an [XML document](#). By altering this document, you can add, remove, and/or change names and descriptions at will. Note that changes to this document have no effect on the availability, or lack thereof, of variables during client execution.

## WMI Namespace

---

In order to support RSoP, each Client Side Extensions (CSE) must write data to a local computer's Windows Management Instrumentation (WMI) repository. This data is made available to the administrator via the RSoP planning and logging mode interfaces. WMI data is collected from a computer using the RSoP snap-in wizard. Each Group Policy extension is accompanied by an RSoP snap-in extension to display its data.

PolicyMaker provides client side functionality and RSoP snap-in extensions to support both logging and planning mode. In order to write RSoP data to WMI, the WMI namespace of a computer is extended when a PolicyMaker CSE is installed. Note that PolicyMaker does not extend the Active Directory schema.

The following table describes the namespace extension implemented by PolicyMaker. Each PolicyMaker CSE adds a single WMI class to the RSOP\_PolmkrProSetting namespace, and all classes are based on the single class RSOP\_PolmkrSetting (bold below), which is in turn based on Microsoft's RSOP\_PolicySetting.

```
class RSOP_PolmkrSetting : RSOP_PolicySetting
{
    string polmkrBaseGpoDisplayName;
    string polmkrBaseCseGuid;
    string polmkrBaseGpeGuid;
    string polmkrBaseHash;
    string polmkrBaseKeyValues[];
    string polmkrBaseInstanceXml;
};
class RSOP_PolmkrProSetting : RSOP_PolmkrSetting
{
};
class RSOP_PolmkrIniFileSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrRegistrySetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrDriveSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrPrinterSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrShortcutSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrInternetSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrProfileSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrFileSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrFolderSetting : RSOP_PolmkrProSetting
{
    string id;
```

```
    uint32 precedence;
};
class RSOP_PolmkrApplicationSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrEnvironmentSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrDeviceSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrRegionalSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrFolderOptionSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrStartSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrNetworkSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrPowerSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrLocalGroupSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
class RSOP_PolmkrDataSourceSetting : RSOP_PolmkrProSetting
{
    string id;
    uint32 precedence;
};
};
```

## XML Integration

---

PolicyMaker includes extensive support for XML and opportunities to integrate and extend capabilities using XML. XML is the primary data format for PolicyMaker persistence and data transfer. Each PolicyMaker snap-in item, supports [XML display of its settings](#) . Each of these items obtains all of its persisted settings from an XML document.

In addition to XML display, PolicyMaker configuration items support XML drag and drop, as well as copy and paste. Any configuration item may be copied into a Unicode, text, XML, or other file, or any number of other clipboard receptacles, including the Windows Explorer and desktop, Notepad, Microsoft Word, Microsoft Excel, and many other. These documents may also be copied back into the appropriate PolicyMaker extension, dynamically populating any number of items from raw XML. This makes it a very easy task to archive, transfer, backup, restore, and report on configuration settings.

### Tip

Office 2003 XML integration makes this XML integration an even more valuable prospect for administrators. XML configuration data can be seamlessly transferred between PolicyMaker and Microsoft Word, Access, and/or Excel 2003. Office documents can easily be directed at live configuration data in order to produce always up-to-date settings reports.

The following XML files are part of this system.

---

### Files Related to Licensing:

```
{ GPO ID } \PolicyMaker\license.xml
%AllUsersProfile%\Application Data\DesktopStandard\PolicyMaker\license.xml
%AllUsersProfile%\Application Data\DesktopStandard\PolicyMaker\request.xml
```

---

### Configuration Settings:

```
{ GPO ID } \User\PolicyMaker\<extension>\<extension>.xml
{ GPO ID } \Machine\PolicyMaker\<extension>\<extension>.xml
```

Note that by default PolicyMaker Professional 1.x extensions utilize the following legacy paths, even in later PolicyMaker Standard Edition versions. However, if the extension subfolder above is manually created, that location will be used instead.

```
{ GPO ID } \User\PolicyMaker\<extension>.xml
{ GPO ID } \Machine\PolicyMaker\<extension>.xml
```

---

Values used by the [variable selector](#) are generated from an XML file in the following location:

### Variable Selector:

```
%AllUsersProfile%\Application Data\DesktopStandard\PolicyMaker\variables.xml
```

---

## Applications

---

Group Policy extension for configuration of [Applications](#).

Application items are generated from the list of application [plugins](#) installed on the same computer as the PolicyMaker snap-in extensions. The following application plugins are installed with PolicyMaker by default:

- Office 2003
- Office XP
- Office 2000
- Office 97
- Office 95
- Outlook 2003
- Outlook 2002
- Outlook 2000
- Outlook 97

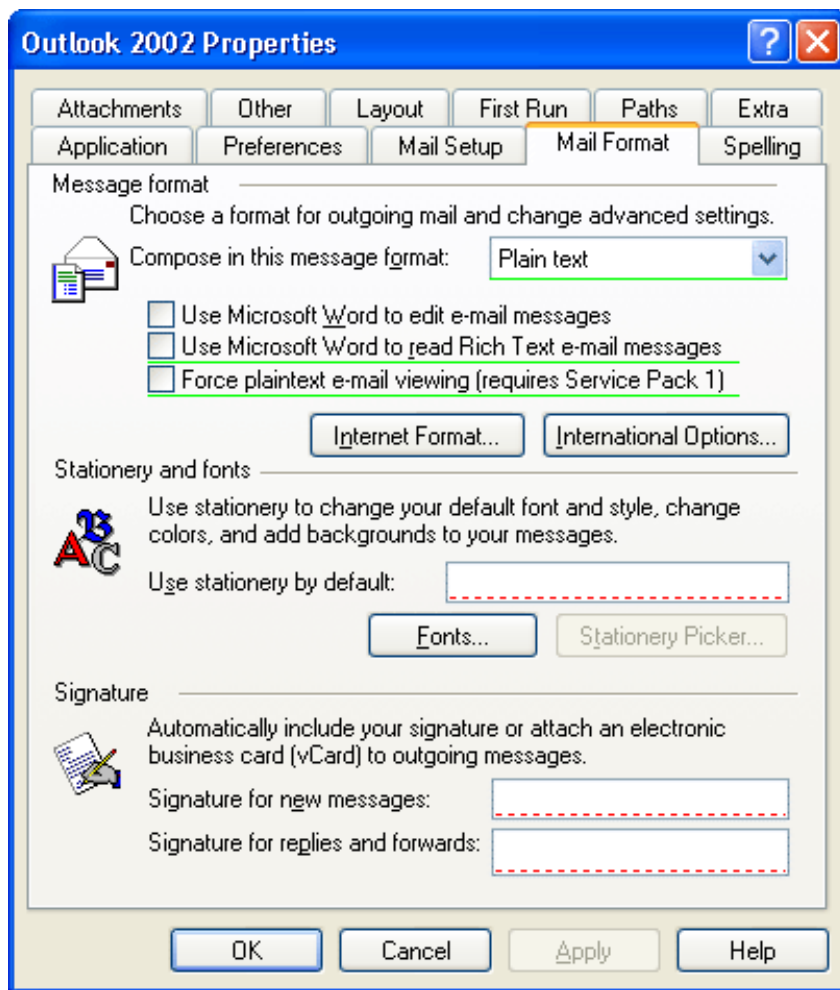
Application items offer several distinct benefits over individual registry and other settings:

- Application items look similar to the actual application that they are designed to support. This makes it very easy to find and understand each desired property.
- Application settings are applied as a group. This provides a high level of organization, especially when applying different application settings to different users.
- Application items implement application "discovery" - thus preventing the configuration items from being implemented on the target platform unless the applicable version of the application is installed.
- Application items implement property underlining, which allows properties to be selectively enabled or disabled while keeping the settings visible for context.

## Application

### Configuring Application Properties

To configure the application's properties, select the new item's "properties" from the toolbar, menu bar or context menu. This will present a dialog that closely resembles the selected application's user interface. This extension uses [property underlining](#) to control which settings you want applied.



### Outlook Properties

Note that Outlook application properties are not tied to Outlook MAPI profiles since PolicyMaker application properties are global to all MAPI profiles. However there is a PolicyMaker "Outlook MAPI" service for each version of Outlook. This service contains supported Outlook properties that are contained within a MAPI profile. If a property is grayed in one interface, it may be supported in the other. If it is grayed in both locations, it is not supported by PolicyMaker. This distinction is entirely the result of Outlook implementation by Microsoft. For more information see KB article [10168](#).

### Unsaved Properties

When an application item is added to a configuration, no properties are actually set into the configuration. Only after a tab has been visited and applied will enabled properties be made part of a configuration. All previously visited tabs are applied when you click OK or Apply on any single tab. For more information see KB article [10168](#).

### Filter

Any [filter](#) applied to any item can prevent that item from executing under specified conditions. Unless a filter is applied to an application item, the item will configure each time the it is run. This has the practical effect of "enforcing" the item configuration, especially if run regularly such as at logon. To apply application properties one time only, use a the "RunOnce" Filter.

### Hidden Filters

Application items implement hidden filters. These filters are identical to those that can be creted using the filters view. However, these filters contain the "hidden" XML attribute, which prevents them from appearing in the filters



view. Trace output will show these filters, and their source can be viewed by inspecting the application item's [raw XML](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Data Sources

---

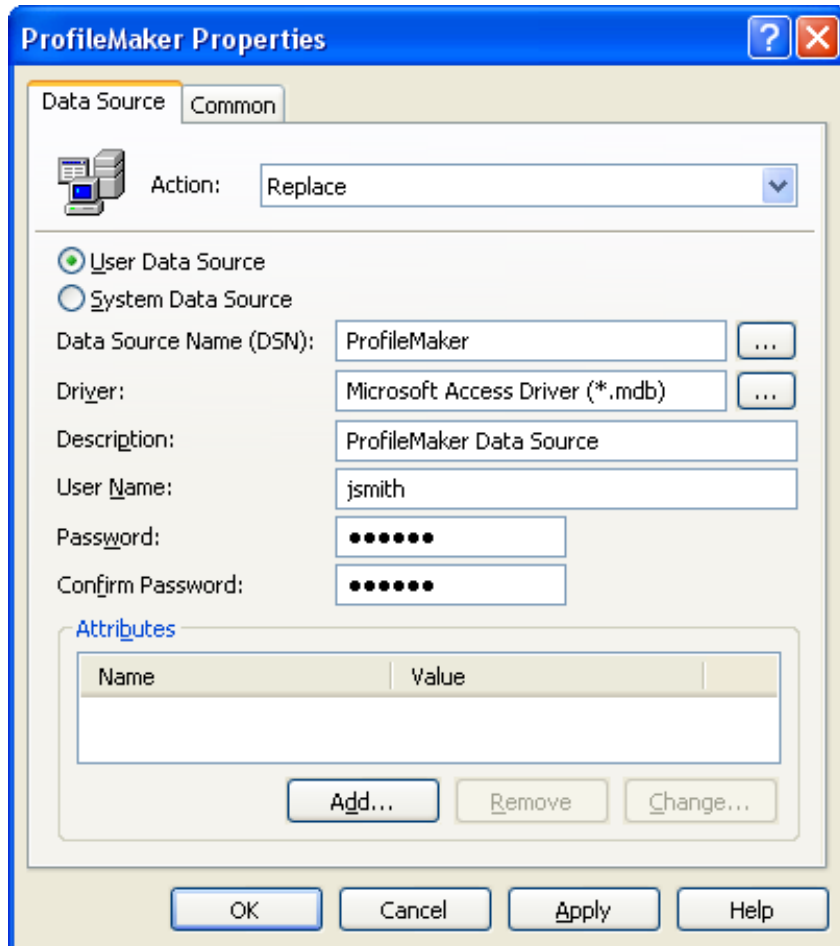
Group Policy extension for configuration of [Data Sources](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Data Source

"Data Source" is a configuration item that is used to configure an ODBC system or user data source.



### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by a combination of Data Source Name (DSN) and the User vs. System Data Source property.

- Create - creates the data source, if it does not already exist.
- Replace - delete the data source and then create it.
- Update - if the data source does not exist, it will be created. Specified properties are then set.
- Delete - deletes the data source if it exists.

### User Data Source:

A User data source is one that is only visible to the user for whom it is created.

### System Data Source:

A System data source is visible to all users on the machine, including system services.

### Data Source Name (DSN):

**Required setting.** The name of the data source, also known as a DSN. The browse button launches the [Data Source Browser](#), which populates all attributes from an existing DSN. [Variables](#) may be used in this setting.

### Driver:

**Required setting.** The ODBC driver used by this data source to connect to a database. Although this field is required, it is not used in targeting the data source. This field is currently required for the delete action. The browse button launches the [Data Source Browser](#), which in this context populates only the selected Driver. [Variables](#) may be

used in this setting.

Description:

An optional description for the data source. [Variables](#) may be used in this setting.

Password:

An optional password that is used by the data source to connect to the database.

 Password Security

The password is encrypted before being saved into the configuration XML. The password is decrypted by the Data Sources client side extension so that it may be applied to the data source configuration. It is important to note that it is technically possible, although difficult, to recover the password from the settings file.

Attributes:

Data source attributes define all aspects of the data source configuration. In update mode, attributes may be added or overwritten if the data source already exists. Attributes cannot be deleted from an existing data source without replacing the data source. [Variables](#) may be used in any of these settings.

---

 Tip

The best method for setting up a data source is to use the Data Source browser to select an existing data source, which will in turn populate all of the attributes of that data source.

---

 Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Devices

---

Group Policy extension for enabling and disabling hardware [Devices](#).

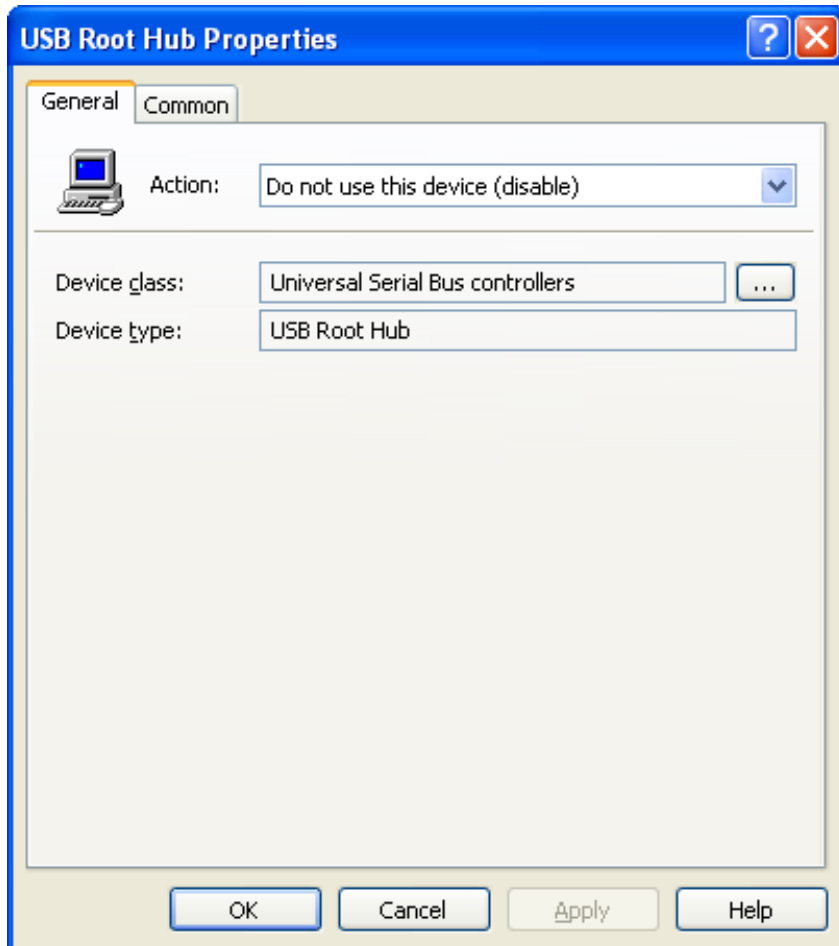
---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Device

---

"Device" is a configuration item used to enable or disable a class or subtype of hardware device.



---

This policy can be used to implement restrictions against the availability of USB devices, optical, floppy and other types of removable drives, parallel and serial ports, sounds devices and more. If a class of device is selected, all devices of that class will be disabled. If a device type is selected, all devices of that class subtype will be disabled.

Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by device class.

- Use this device (enable) - enables the device type or device class as specified.
- Do not use this device (disable) - disables the device type or device class as specified.

Device class:

**Required setting.** This setting allows you to choose from a list of device classes. The browse button launches the [Device Browser](#).

Device type:

An optional device type (sub-class). This field is filled in automatically by the device browser when a type is selected.


---

### Notes

This policy works in the same manner for user and computer policy, since devices are global to the computer. User policy is recommended when there are per-user differences in the desired application of the device restrictions. Note that some devices which appear in the device manager cannot be disabled. While disabling takes effect immediately, the Windows Device Manager may not show the "red x" on the device immediately. The device property

sheet will show the current device status however.

Because this policy is primarily used for disabling devices, the [common tab](#) option to "Remove this policy when it is no longer applied" is only available when the policy is set to disable the device and the removal of the policy re-enables the device.

 Warning

Use caution when disabling devices as you may effectively render a computer unusable.

---

 Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Drive Maps

---

Group Policy extension for configuration of [Mapped Drives](#).

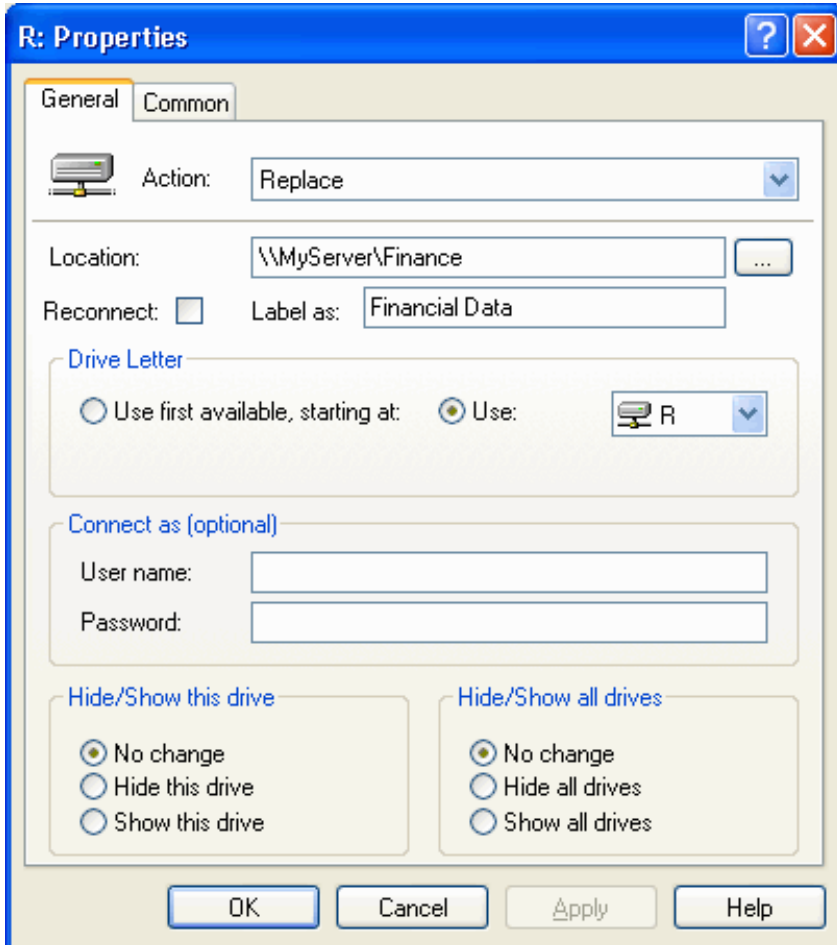
---

© 2005 DesktopStandard Corporation. All Rights Reserved.



## Mapped Drive

"Mapped Drive" is a configuration item that is used to set up drive mappings to network shares for individual users. This policy is only processed in Group Policy's [foreground processing](#) mode.



### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Drive Letter. When using the "Use first available, starting at" option, matching is performed by Location.

- Create - creates the drive map, if it does not already exist. The Hide/Show status and Label is then set.
- Replace - deletes the drive map, if found. The drive map is then created and the Hide/Show status and Label is set.
- Update - creates the drive map, if not found. The Hide/Show status and Label is then set.
- Delete - deletes the drive map(s) if found.

### Location:

**Required setting in Create or Replace modes.** The fully qualified UNC path of the network share that will be mapped to the specified drive letter. [Hidden shares](#) can be mapped using standard Windows terminology (e.g. "\\ server\c\$ " to map the hidden root share of the "c:" drive on "\\server"). [Folders within shares](#) can also be mapped (e.g. "\\ server\share\folder "). The browse button launches the [Share Browser](#), which supports subfolder browsing. [Variables](#) may be used in this setting.

### Note

In update mode this path may be left empty, however if the drive letter does not already exist, an error will occur attempting to create the drive map. An empty path in update mode is intended to allow the administrator to update the Hide/Show status of a [physical drive letter](#), or all drives, without the need to map a drive. In delete mode this setting is disabled.

Reconnect :

Forces Windows to map this drive at every logon for this end-user, even if PolicyMaker does not run. In delete mode, or with an empty Location (in update mode) this setting is disabled. This option is useful if the Drives CSE is set to not "Process even if the Group Policy objects have not changed" (see [desktopstandard.adm](#)), or if it is desired to have maps automatically reconnect even if the user is logging on with cached domain credentials (in which case Group Policy does not run). **If this option is set, it is not possible to use this drive letter in subsequent CSEs, such as folder redirection.**

Label as :

**Windows 2000+ only.** Sets the label of the specified/configured drive letter.

Drive Letter:

#### Not in Delete Mode

- Use first available, starting at:
  - Maps the first unused drive letter to the Location, in alphabetical order, starting at the specified letter (inclusive).
  - If this option encounters an existing drive mapped to the same share path as specified in Location, it will match that drive. This allows the option to be used to map the first available drive letter but to prevent repeatedly remapping the same path to multiple drive letters.
- Use: (or Existing:)
  - Maps the specified drive letter to the Location.
  - Label changes to "Existing" when in update mode with an empty Location.

#### Delete Mode Only

- Delete all, starting at:
  - Deletes all drive letters for this end-user, starting at the specified letter (inclusive).
- Delete:
  - Deletes the specified drive letter.

#### Note

"Delete all" skips physical drives without error. However, an error will occur if a drive letter is specified to be replaced or deleted, and that drive letter is a physical drive.

Connect as (optional):

If the logged-on user does not have at least read access to the share, you can provide credentials using this setting. Windows caches these credentials until the user logs off.

User name:

A user name of a user with at least read permissions to the Location. This setting is disabled in delete mode. [Variables](#) may be used in this setting.

Password:

The password for the user account associated with "user name". Note that this value is not encrypted in the configuration data file. This setting is disabled in delete mode. [Variables](#) may be used in this setting, even though the text is hidden.

#### Note

This will cause Windows to prompt the end-user for credentials to connect to the drive as the end-user logs on, if: the end-user does not have permissions to the share, the drive map is persistent (i.e. "Reconnect at logon " is set), and PolicyMaker is not remapping the drive.

Hide/Show this drive:

Hides (or unhides) the specified drive letter from within the Windows Explorer. This supports both mapped and physical drives.

Hide/Show all drives:

Hides all (or unhides all) drive letters from within the Windows Explorer. This supports both mapped and physical drives.

 Hint

By selecting "Hide all drives" and "Show this drive" you cause the specified drive letter to be the only visible drive. Conversely, by selecting "Show all drives" and "Hide this drive" you ensure that the specified drive letter is the only hidden drive.

---

 Note

By default, this item will have access to all objects with the SYSTEM Access Control Entry (ACE). This item will always use the end-user's security context to locate and map/delete drive(s), and will only have access to network shares accessible to that user. To change this item to run with end-user permissions (in a user configuration), change the security context on the [common tab](#). Since mapping is always done in the user's context, this only affects the ability to set drive hide/show policy.

 Hide/Show

Hide/Show options utilize a system policy to hide or unhide a drive letter. This is a single policy for all drive letters. Any change to this policy will affect the presentation of drive letters. It is not recommended to use Administrative Templates policy to set this policy if you are setting it using PolicyMaker. Within PolicyMaker the last drive map item to execute will control this policy. Also note that when hiding or unhiding a single drive letter using PolicyMaker, the hidden status of other drive letters will not be impacted.

---

 Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---

## Environment Variables

---

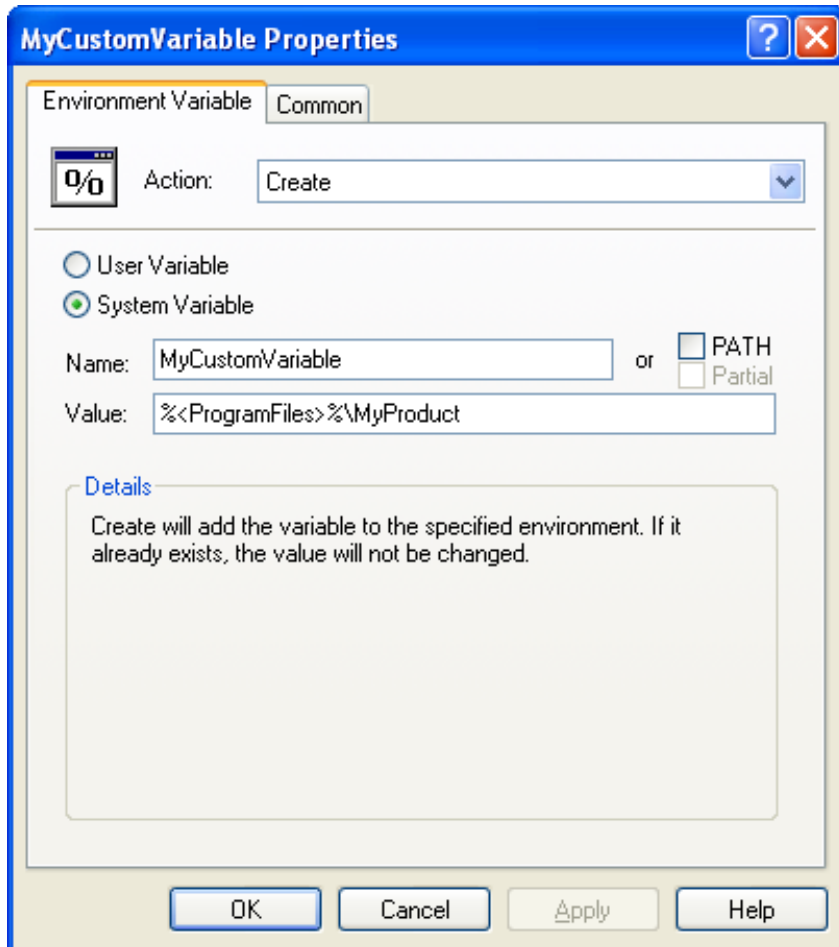
Group Policy extension for configuration of [Environment Variables](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Environment Variable

"Environment Variable" is used to set persistent user or system environment variables. The current environment is immediately refreshed.



### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by variable name.

When targeting the %PATH% variable, matching is by name (i.e. PATH) and if "Partial" is specified the partial value is matched within the existing PATH value. A partial PATH match is case insensitive.

- Create - creates the variable only if it does not exist.
- Replace - replaces the variable if found, otherwise creates it.
- Update - **same as Replace.**
- Delete - deletes the variable if found.

### User Variable:

User variables are persisted in the HKEY\_CURRENT\_USER registry hive and affect each user independently. If this option is selected for a computer policy, the variable will be set for the "Default User" and will not have an immediate effect in the operating system.

### System Variable:

System variables are persisted in the HKEY\_LOCAL\_MACHINE registry hive and affect all users of the computer.

### PATH:

This option is available only with System Variable selected. This is functionally the same as entering "PATH" into the name field, however it will also immediately enable the "Partial" option.

Partial:

This option specifies that the Action should affect a single PATH segment, not the entire PATH value. This allows you to make modifications to an existing PATH string.

#### Variables in PATH

The PATH environment variable normally contains unresolved system environment variables (such as "%windir%"). [Variable Non-Resolution](#) syntax can be used in PATH segments to prevent environment variables from being pre-resolved by PolicyMaker. PolicyMaker will match PATH segments in both their resolved and unresolved form and automatically replace segments that contain resolved environment variables with the unresolved equivalent. For example, "C:\Windows\MyFolder" will be replaced with "%windir%\MyFolder" if the Value field contains "%<windir>%\MyFolder".

Name:

**Required setting.** The name of the environment variable. Names are not case sensitive, but will be persisted as provided.

Value:

The desired value of the specified environment variable. For a partial PATH this can include only one token. Since the PATH is delimited by the semicolon (";") character, this means that the semicolon should not be included in this value. [Variables](#) may be used in this setting.

#### Variable Expansion

If the Value contains an unresolved environment variable, it will be stored as REG\_EXPAND\_SZ instead of the default, which is REG\_SZ. See the [Variable Non-Resolution](#) topic for information.

Details:

A dynamic description of the intended results of the setting.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Files

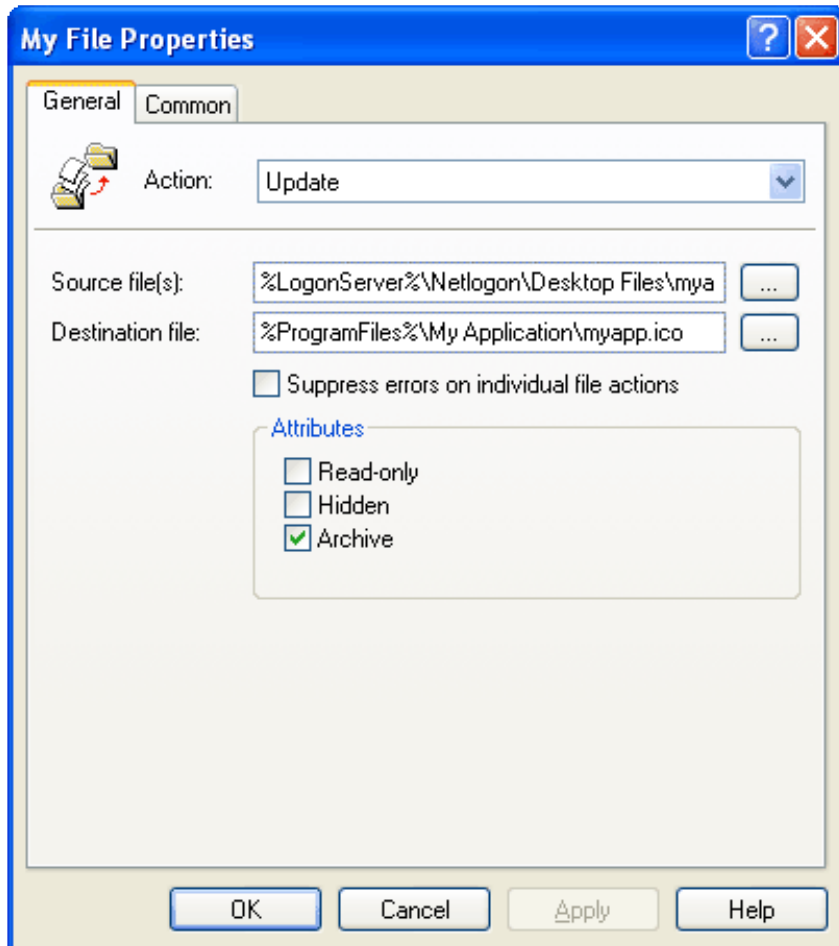
---

Group Policy extension for management of individual [Files](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

"File" is a configuration item that is used to copy or delete files.



This policy supports single and multiple file transfer and delete operations. When one or more wildcard characters (\* or ?) are placed into the Source path, the 'Destination file' path transitions to 'Destination folder'. For a single file transfer, a source file name that differs from a destination file name is acceptable. For multiple file (wildcard) transfers, each destination file name matches the source file name.

**Action:**

One of the standard PolicyMaker [action modes](#). Matching is performed on a per-file basis by comparing Source file with Destination file.

- Create - copies each file, and sets specified attributes, skipping files that already exist.
- Replace - same as Create except that each file is deleted first if it exists.
- Update - if a file does not exist, it will be created. File attributes will be set on each of the target file(s).
- Delete - delete each file if it exists. Folders are never deleted.

**Source file(s):**

**Required setting (except in delete mode).** The fully qualified UNC path of the file to be copied, from the perspective of PolicyMaker client side extension on the desktop. The path should not be quoted. The wildcards \* and ? are accepted and if specified cause the Destination field to be interpreted as a folder. This parameter is disabled in Delete mode. The browse button launches the [File Browser](#). [Variables](#) may be used in this setting.

**Destination file/folder:**

**Required setting.** The fully qualified UNC path of the location to copy the file, from the perspective of PolicyMaker client side extension on the desktop. Parent folders will be created as necessary. The path must not be quoted. The



file name must be included, and does not have to match the Source file name. If the [common tab](#) option to 'remove this policy when it is no longer applied' is set, the destination file will be deleted. This does not apply to a multiple file operation, in which case no files will be deleted. The browse button launches the [File Browser](#) (or the [Folder Browser](#) if wildcards are specified in the path). [Variables](#) may be used in this setting.

Delete file(s):

Required setting (delete mode only). The wildcards \* and ? are accepted. Folders, subfolders and files in subfolders are not affected. To configure folders use [Folder policy](#).

Suppress errors if target not deletable

This affects only errors that result from an attempt to copy a file in replace mode, delete a file, or set attributes on a file, not other types of processing errors. This option is distinct from the default policy error suppression which can be overridden on the [common tab](#). Create and Update modes disable this option.

#### Important

It's important to note that the error in could have resulted from any number of circumstances, such as target file in use, access denied, or the source file not found. Using this setting allows a large number of files to be transferred even if one or more fail - however the [trace file](#) would be the only way to detect such failures if this option is used.

Attributes:

Standard file system attributes to set on a file after it is Created, Replaced, or Updated. Many incremental backup systems utilize the archive attribute to determine that a file system object has been created or changed, and to back up this object on the next increment. For this reason the PolicyMaker default is set to set the archive attribute on any modified folder. Unchecked settings cause the attribute to be removed from the target file. Delete mode disables these options.

---

#### Notes

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#).

This item will reset the "Read Only" attribute of any target file in order to accomplish the specified task, although the attribute may be specified.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---

## Folder Options

---

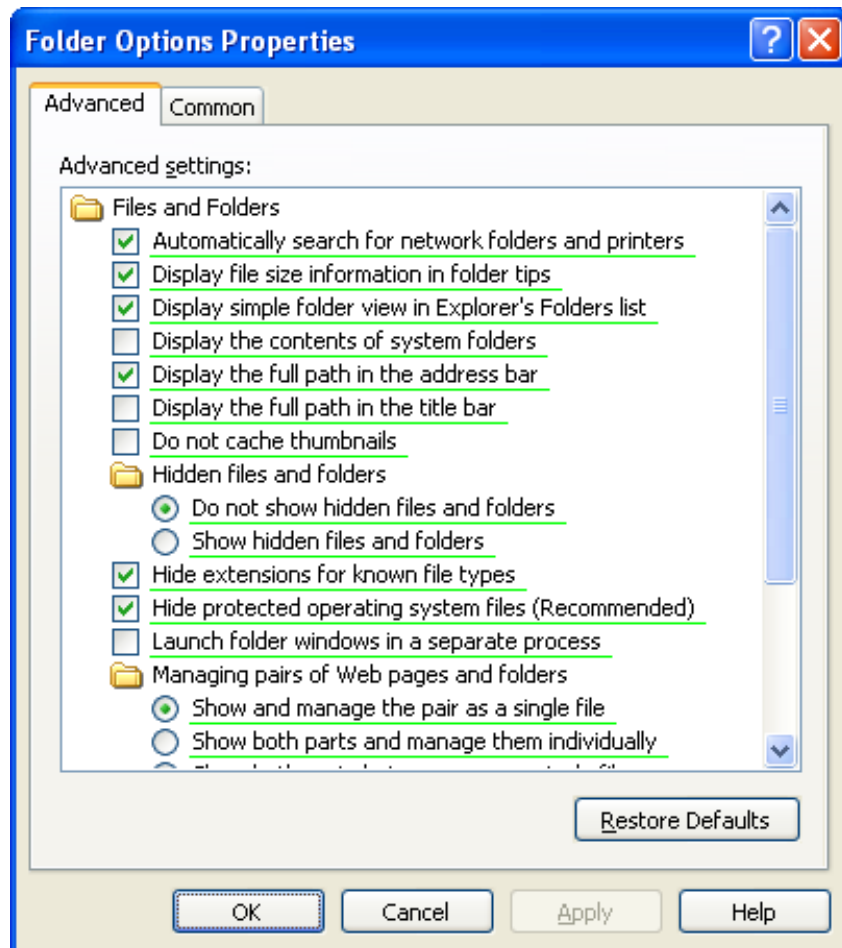
Group Policy extension for configuration of [Folder Options](#), [File Types](#), and [Open With](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Folder Options

"Folder Options" controls various Explorer settings that pertain to an individual end-user.



This extension uses [property underlining](#) to control which options are applied. For an explanation of each particular setting, see the control panel Folder Options applet.

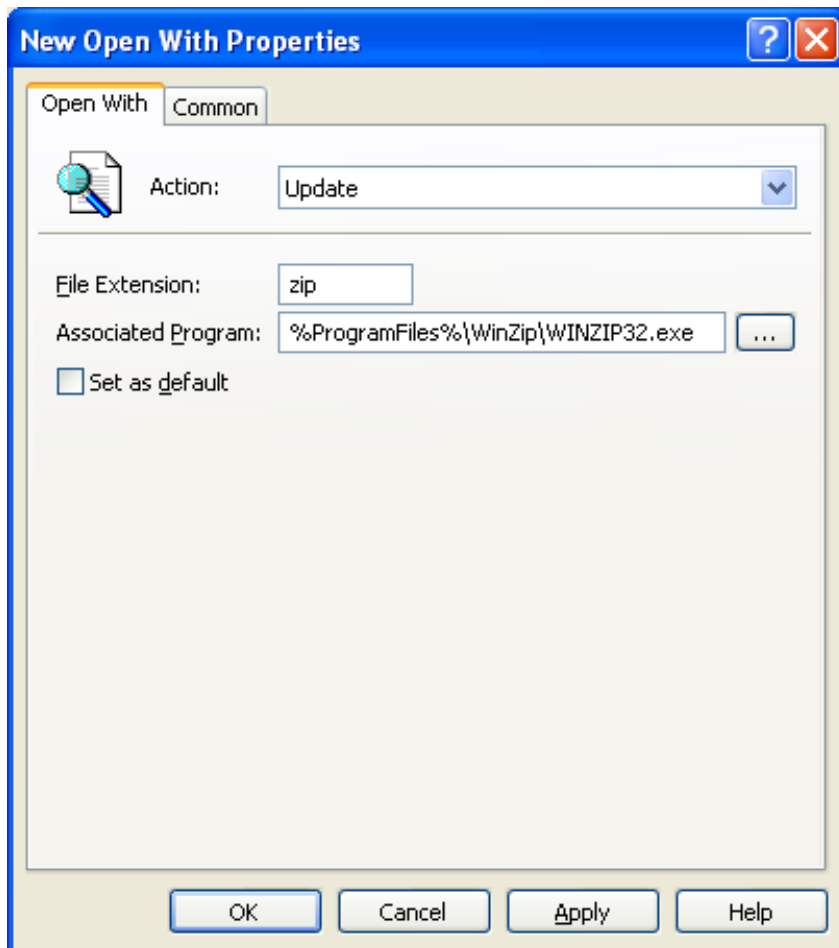
### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Open With

---

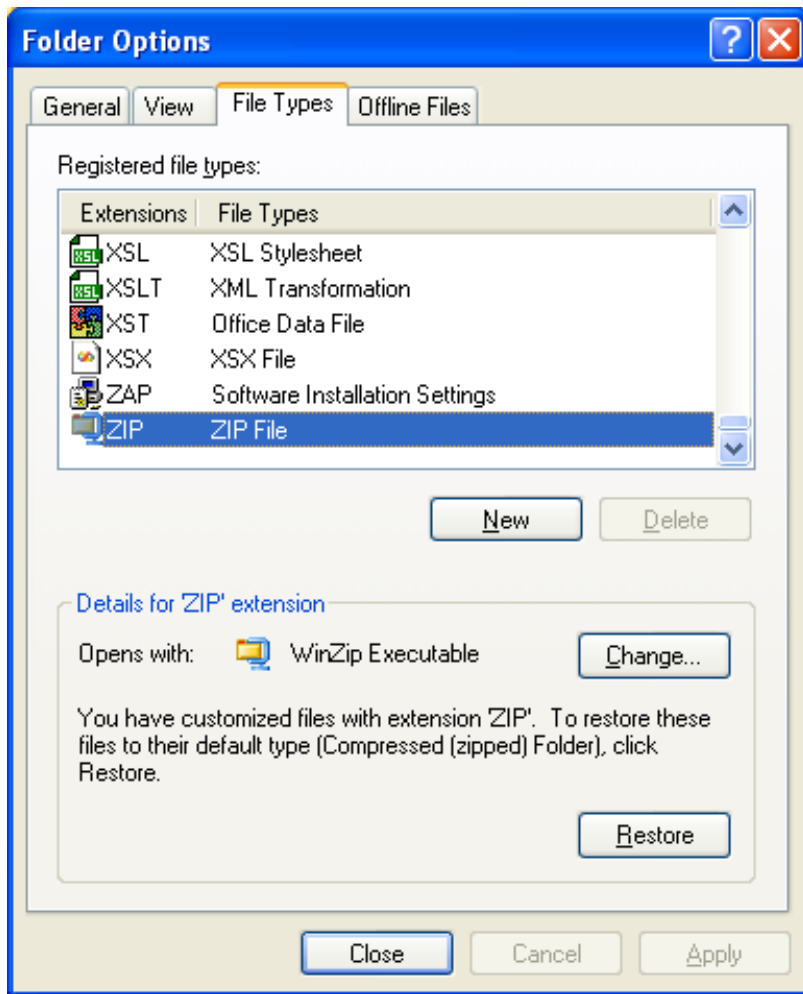
"Open With" is a configuration item that is used to configure user-specific program associations with file extensions.



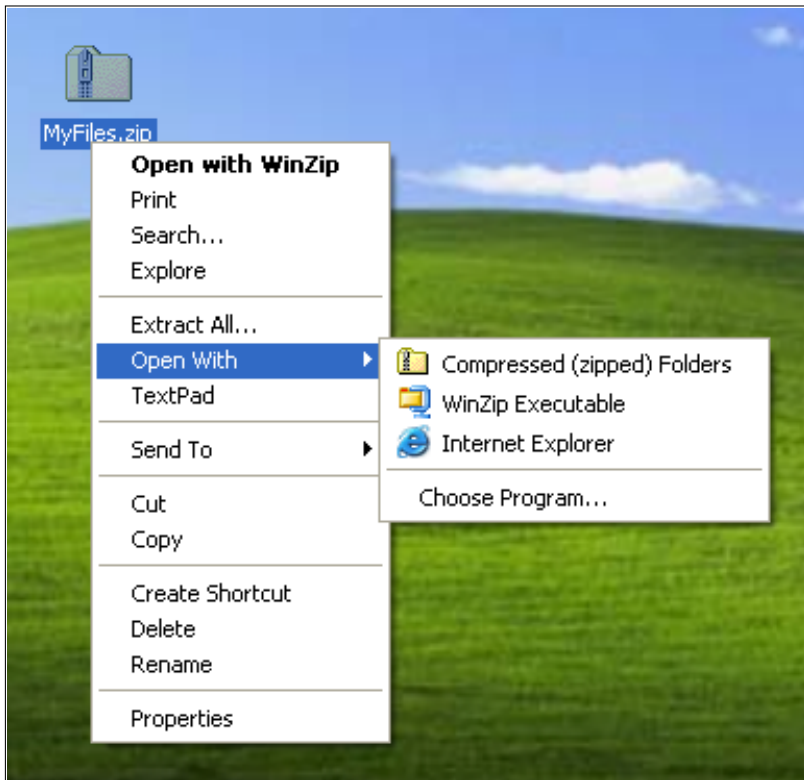
---

This policy allows you to manage file associations for users without modifying the registered extensions for the whole computer. Open With associations take precedence over [File Type](#) associations, but only for the user(s) to whom they are applied.

The Folder Options control panel applet shows a combination of Open With settings and File Types settings on the single File Types property page (see below):



The presence of the "Restore" button on this tab indicates that the File Type association has been overridden by an Open With association. It is possible to set more than one Open With association per file extension. If more than one is set, the default Open With is used to open a document with the extension by default. The list of associations may be accessed from the Explorer's Open With context menu item (see below):



**Action:**

One of the standard PolicyMaker [action modes](#). Matching is performed by file extension within the user profile.

- Create - creates the file association, if it does not already exist.
- Replace - delete the file association and then create it.
- Update - if the association does not exist, it will be created. If it exists, settings will be updated.
- Delete - delete the file association if it exists.

**File Extension:**

**Required setting.** Specifies the extension to associate with the Associated Program. [Variables](#) may be used in this setting.

**Associated Program:**

**Required setting (except in delete mode).** This setting allows you to associate a program, either by manually entering a path or by browsing the computer. The browse button launches the [File Browser](#). [Variables](#) may be used in this setting.

**Set as default:**

Set the specified Associated Program as the default to open the File Extension.

 **Note**

The Explorer's Open With context submenu is presented only if there is more than one Open With association.

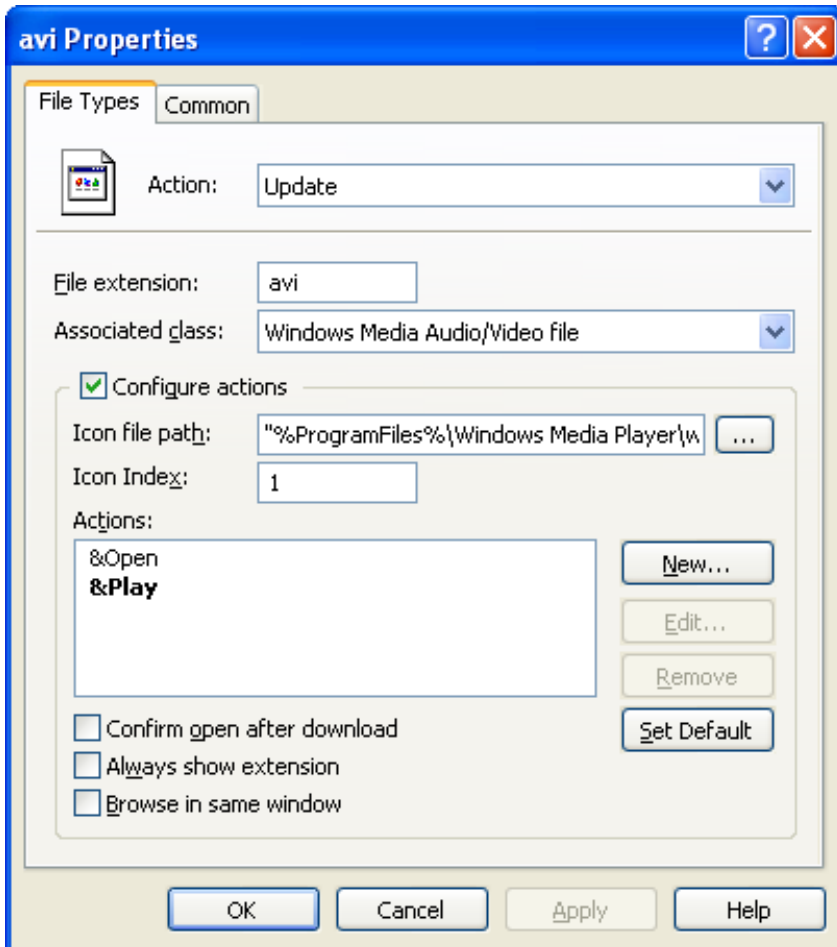
---

 **Filter**

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## File Types

"File Types" is a configuration item that is used to configure computer-global program (progid/class) associations with file extensions.



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by computer file extension registration.

- Create - creates the class association, if it does not already exist.
- Replace - delete the class association and then create it.
- Update - if the association does not exist, it will be created. If it exists, actions will be updated.
- Delete - delete the file association if it exists. This does not delete the class registration itself.

File extension:

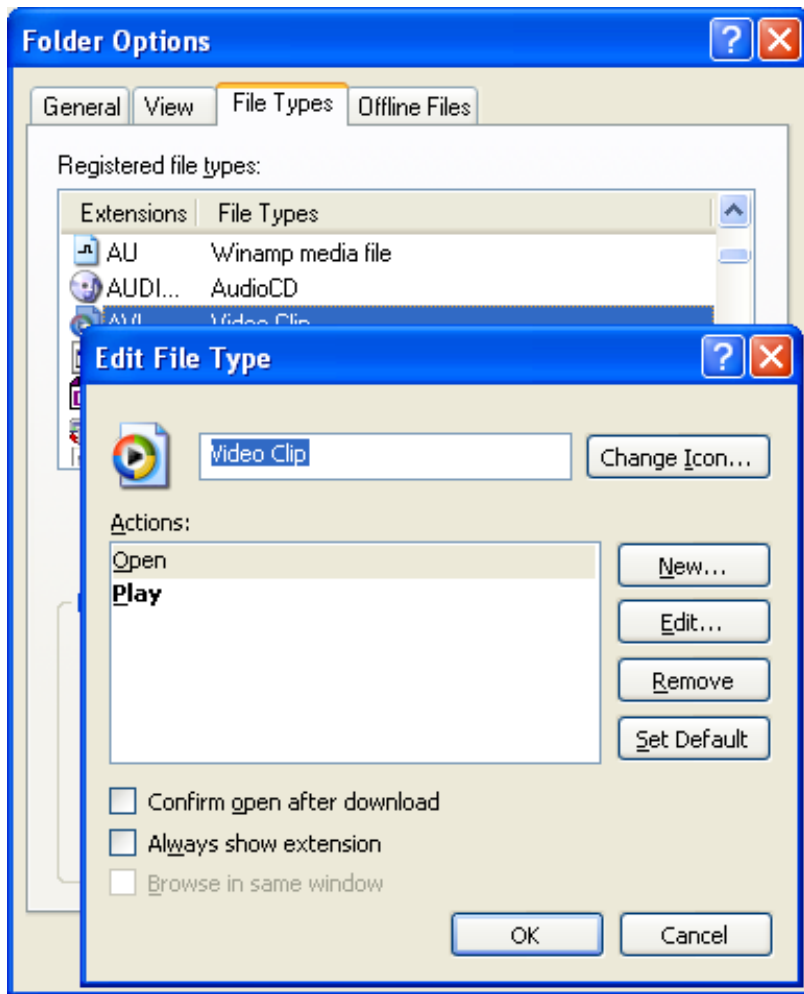
**Required setting.** Specifies the extension to associate with the Associated Program. [Variables](#) may be used in this setting.

Associated class:

**Required setting (except in delete mode).** This setting allows you to associate a registered program, by selecting it from the drop-down [ProgId Browser](#). The selected class must be previously registered on target computers in order for configuration to succeed. [Variables](#) may be used in this setting.

Configure actions:

These are advanced settings that should only be modified with a good understanding of their effect. The behavior of these settings is based on the behavior of the similar interface in the control panel's Folder Options applet on the File Types property page - under the "Advanced" button (see below):



#### Action updates

Each Action configured will replace in full any action of the same name that was previously registered under the Associated class. Apart from overwriting an Action, this policy does not support removal of Actions, or other items in the Configure actions section.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---



## Folders

---

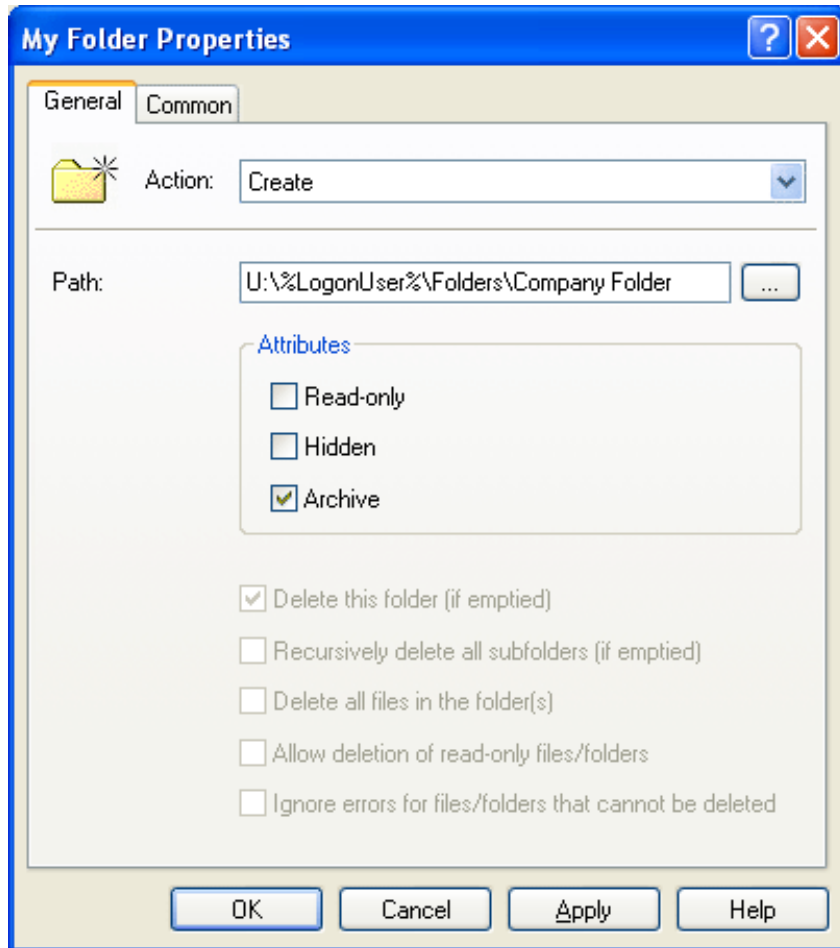
Group Policy extension for management of individual [Folders](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Folder

"Folder" is a configuration item that is used to create and/or delete Explorer folders/contents.



### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by folder Path.

- Create - creates the folder, with specified attributes, if it does not already exist.
- Replace - same as Delete except the folder will subsequently be created, with the specified attributes.
- Update - if the folder does not exist, it will be created. Folder attributes will be set.
- Delete - delete the folder and/or its contents, if it exists, with options to recurse.

### Path:

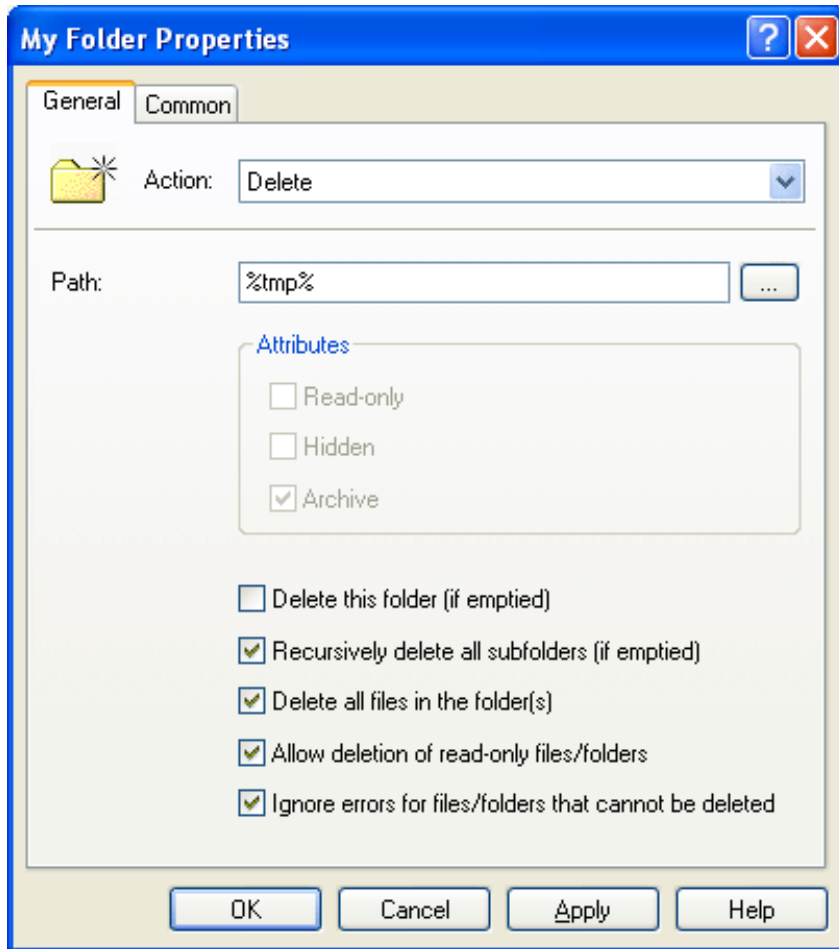
**Required setting.** The fully qualified UNC path of the target folder, from the perspective of PolicyMaker client side extension on the desktop. The path should not be quoted or contain a trailing slash. The browse button launches the [Folder Browser](#). [Variables](#) may be used in this setting.

### Attributes:

Standard file system attributes to set on a folder after it is Created, Replaced, or Updated. Many incremental backup systems utilize the archive attribute to determine that a file system object has been created or changed, and to back up this object on the next increment. For this reason the PolicyMaker default is set to set the archive attribute on any modified folder. Delete mode removes these options.

### Delete/Replace Options:

The last five options on the Folder property sheet are enabled only in Delete and Replace modes. The following example demonstrates clearing the "temp" directory.



- Delete this folder (if emptied)
    - Delete this folder will be made after all other delete processing has completed.
    - The folder delete cannot succeed if the folder is not empty.
    - To prevent an error on this delete attempt (i.e. if the folder was not emptied), set the "Ignore errors..." option.
  - Recursively delete all subfolders (if emptied)
    - Recurse to lowest child folder(s) and delete all of their parent folders up to (but not including) the specified folder.
    - Folder deletions cannot succeed if the folders are not empty.
    - To prevent an error on these delete attempts (i.e. if the folder was not emptied), set the "Ignore errors..." option.
  - Delete all files in the folder(s)
    - Delete all files in the specified folder (and subfolders if "Recursively delete..." option is set).
  - Allow deletion of read-only files/folders
    - Attempt to delete files that have the read-only attribute set, by first resetting the attribute.
    - Ignore errors for files/folders that cannot be deleted
    - If a file is "in process", permissions to the file are denied, or if for some other reason the files is undeletable, PolicyMaker will normally return the error code. However, with this option set, PolicyMaker will continue processing and not return an error.
    - This option may be useful when clearing the "temp" directory (as shown in the example above).
-

#### Notes

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#).

In order to create a specified folder, PolicyMaker will create all parent folders. If the parent folders already exist, they will be ignored. No changes are ever made to parent folders, nor are they ever created in an attempt to delete a child folder. To modify a parent folder (such as "U:\% LogonUser%\Folders " in the example above), create a separate item to specifically target that folder.

#### Important

Deleting or replacing a folder [recursively with file delete](#) can be extremely damaging if the wrong folder value is provided or if the behavior of this feature is not understood. When a folder is deleted (or replaced) recursively with files, all of its children, including all subfolders (and their subfolders etc.) as well as all of the files in all such folders, will be deleted.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---

## Ini Files

---

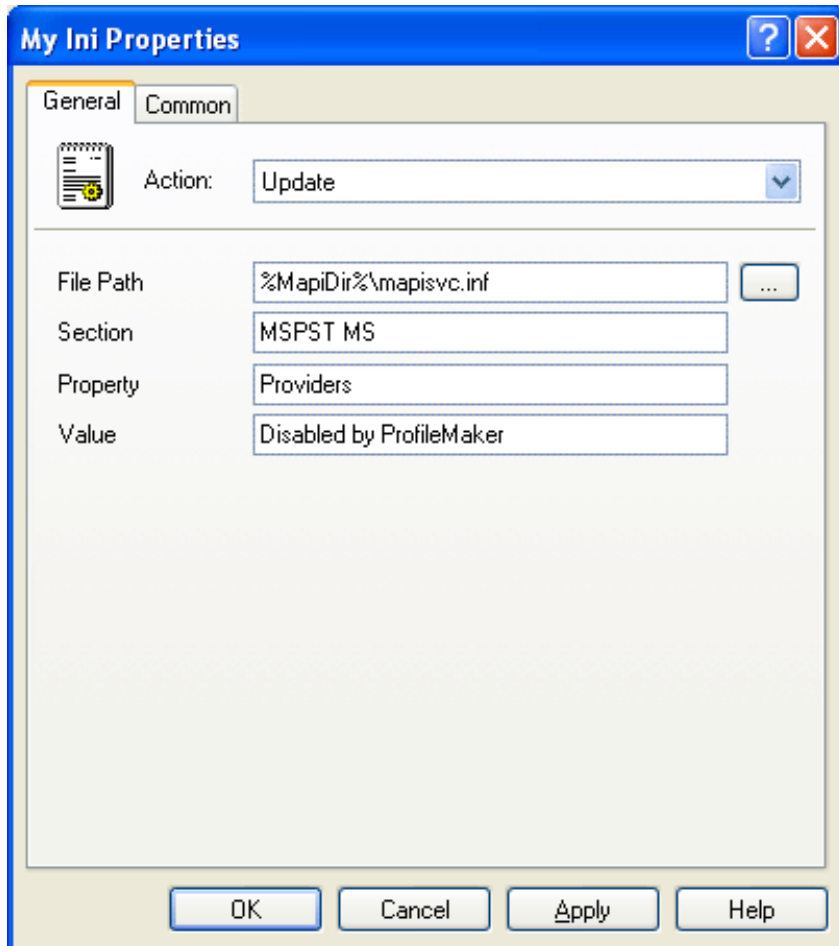
Group Policy extension for configuration of [Ini Files](#).

---

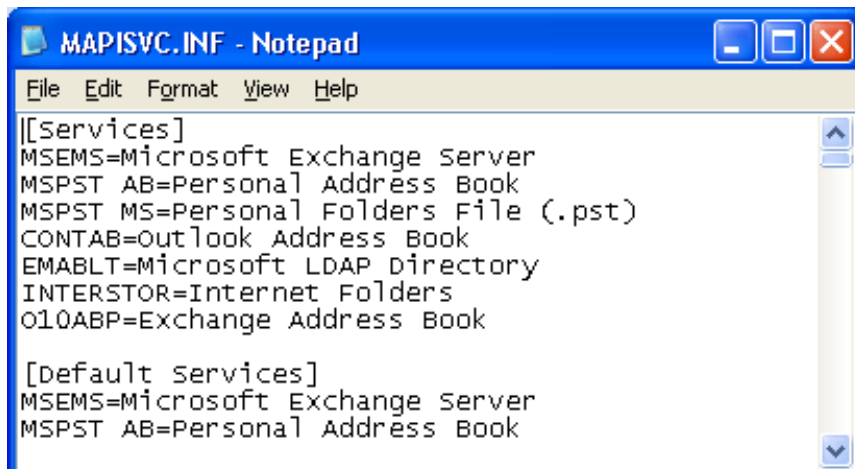
© 2005 DesktopStandard Corporation. All Rights Reserved.

## Ini File

"Ini File" is a configuration item that is used to change ini file values.



The following example shows a typical ini file (in this case with the file extension ".inf"). A "section" refers to all values below the header contained in square brackets, up to the end of the file or the next section header. In the example, "[Services]" and "[Default Services]" are section headers. A "property" is named by the value on the left of an equal sign ("="). In the example "MSEMS" is a property name. A "value" refers the data on the right side of the equal sign, attached to a property.



#### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Section name if no Property is specified, otherwise matching is performed by Property name. An empty property value in an actual ini file is interpreted in the same manner as a property that does not exist.

- Create
  - File Path only - **not allowed**.
  - Section only - **not allowed**.
  - Property - creates the Property/Value pair in the Section, if the Property does not already exist. If the Property exists, the item is skipped.
  
- Replace
  - File Path only - **not allowed**.
  - Section only - **not allowed**.
  - Property - deletes the Property/Value from the Section, if the Property exists. The Property/Value pair are then created in the Section.
  
- Update
  - File Path only - **not allowed**.
  - Section only - **not allowed**.
  - Property - **same as Replace**.
  
- Delete
  - File Path only - deletes the File, if it exists.
  - Section only - deletes the Section and all of its values, if it exists.
  - Property - deletes the Property/Value pair from the Section, if the Property exists.

#### File Path:

**Required setting.** The fully qualified UNC path of the target ini file, from the perspective of PolicyMaker client side extension on the desktop. The path should not be quoted. The file is only created if necessary to create a property. Parent folders will be created as necessary as well. The browse button launches the [File Browser](#), which enters the selected file path into this setting. [Variables](#) may be used in this setting.

#### Section:

The name of the target section in the specified file, not including the brackets. The section is only created if necessary to create a property. If this setting is empty, the item will target a file only. [Variables](#) may be used in this setting.

#### Property:

The name of the desired property. If this is not specified, the item will target a file or section as appropriate. [Variables](#) may be used in this setting.

#### Value:

The value of a property. If this is empty, and a property name is specified, the item will configure the property with an empty value. Values may be quoted as necessary. Typically quotes are removed from values as they are read by an application or the operating system. All values are manipulated as text. This setting is disabled in delete mode. [Variables](#) may be used in this setting.

---

#### Notes

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#). This item will reset the "Read Only" attribute of any file that it needs to alter.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

# Internet Settings

---

Group Policy extension for configuration of [Internet Settings](#).

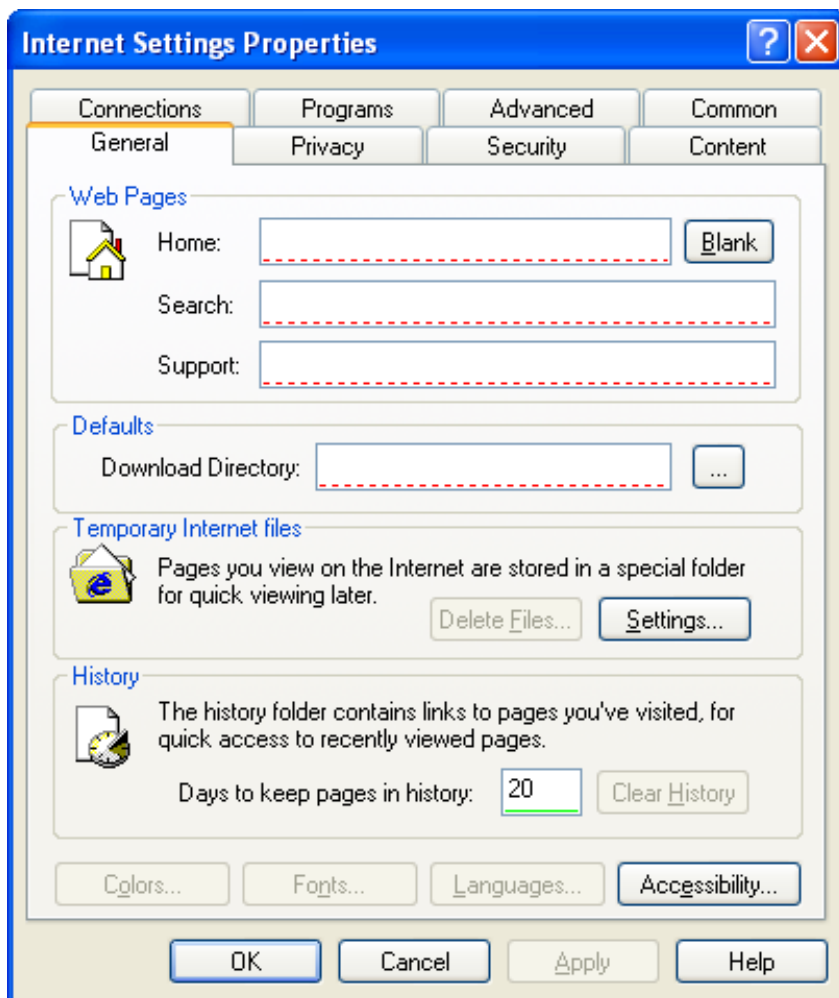
---

© 2005 DesktopStandard Corporation. All Rights Reserved.



## Internet Settings

"Internet Settings" policy is used for customization of user-configurable Internet Settings. This policy is similar to [Application](#) policy, especially in its use of [property underlining](#). This policy is not version-specific, but can be made so using a [filter](#) if desired.



### Note

Green and red diamonds are used on list views in place of underlining.

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

## Licensing

---

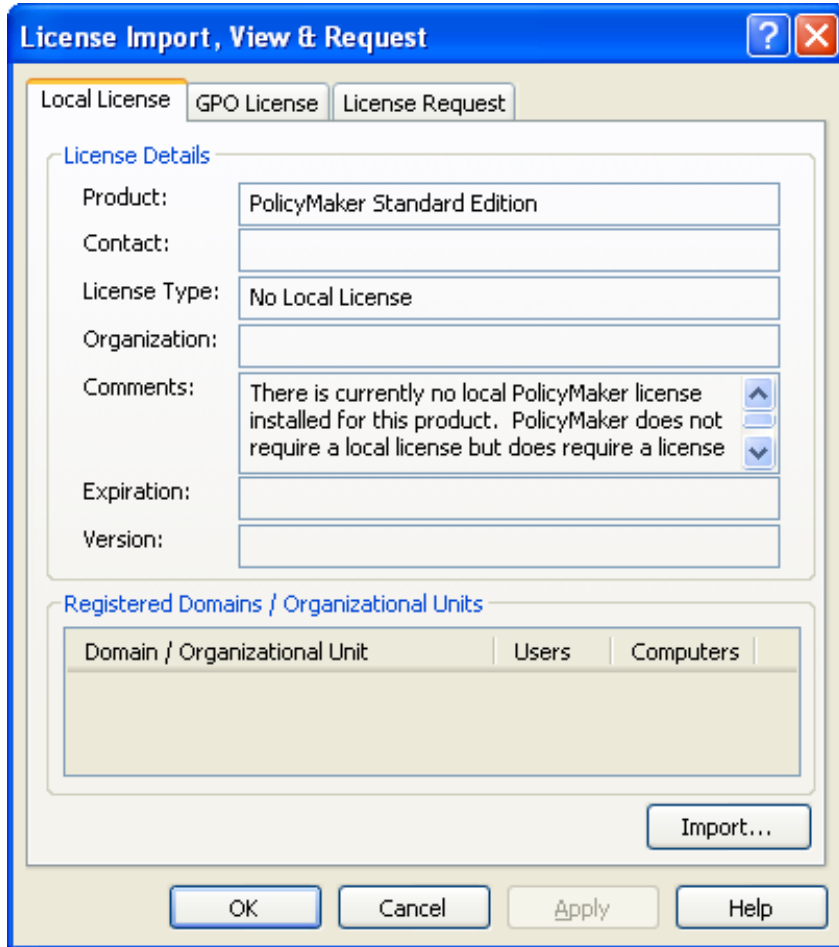
For more details on licensing issues, see the following topics:

1. [Licensing](#)
  2. [Local License](#)
  3. [GPO License](#)
  4. [License Request](#)
- 

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Local License

The Local License tab of the [licensing](#) property sheet allows you to import a license key file (i.e. license.xml) to the local computer (if it is valid and you hit OK/Apply after importing it). This tab also shows the status of the local license key. The local license key is automatically deployed into any non-Local GPO when any PolicyMaker setting is edited in that GPO from that computer. This deployment can also be accomplished using the Deploy button on the [GPO License tab](#).



**License Import, View & Request**

Local License | GPO License | License Request

**License Details**

Product: PolicyMaker Standard Edition

Contact:

License Type: No Local License

Organization:

Comments: There is currently no local PolicyMaker license installed for this product. PolicyMaker does not require a local license but does require a license

Expiration:

Version:

**Registered Domains / Organizational Units**

Domain / Organizational Unit	Users	Computers
------------------------------	-------	-----------

Import...

OK Cancel Apply Help

### Import...

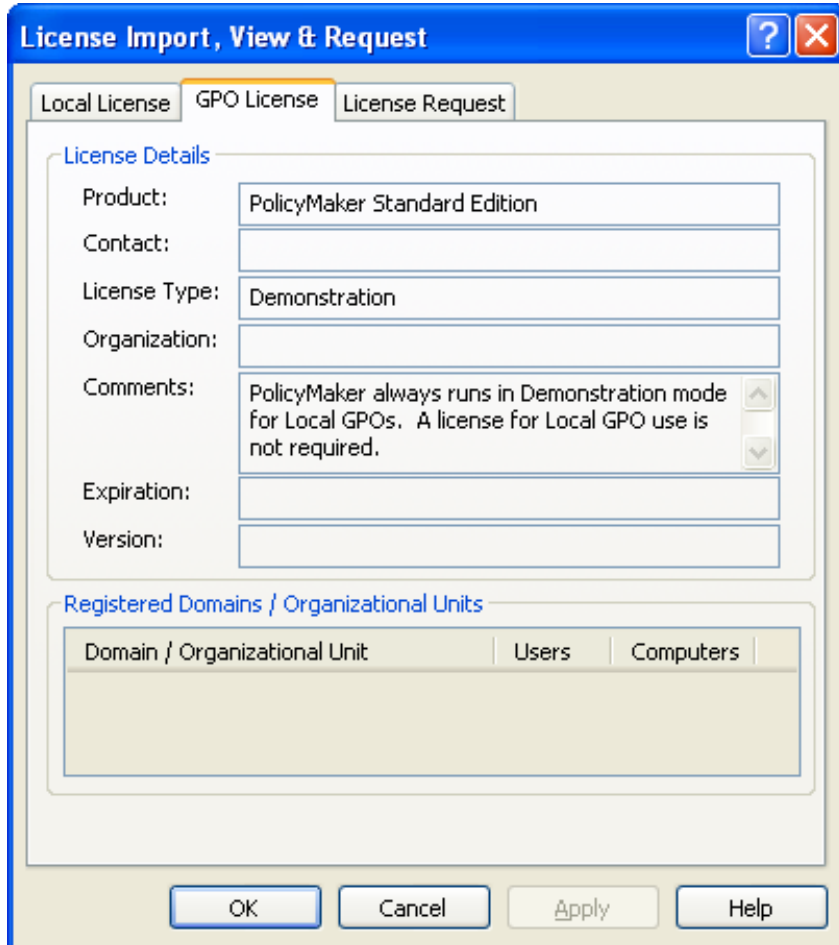
Present a file browse dialog which allows you to select and import a license key file. This file is generally emailed to you after purchasing a registered key or after requesting an evaluation key.

### See also

[GPO License](#) and [License Request](#).

## GPO License

The GPO License tab of the [licensing](#) property sheet allows you view the status of the license key in the selected GPO.



**License Import, View & Request**

Local License | **GPO License** | License Request

**License Details**

Product: PolicyMaker Standard Edition

Contact:

License Type: Demonstration

Organization:

Comments: PolicyMaker always runs in Demonstration mode for Local GPOs. A license for Local GPO use is not required.

Expiration:

Version:

**Registered Domains / Organizational Units**

Domain / Organizational Unit	Users	Computers
------------------------------	-------	-----------

OK Cancel Apply Help

License Type:

A Local GPO will always reflect "Demonstration". A non-Local GPO with no license key will reflect "Unlicensed" and non-promotional Client Side Extensions (CSEs) for the unlicensed product will not process policy for that GPO.

### Deploying a License

To deploy the [local license](#) key to a non-Local GPO, select Deploy. The Deploy button is hidden if there is no valid local license. Alternatively, If you edit policy for this product in this GPO, the license will be automatically deployed to the GPO. Finally, you may manually copy the license.xml to the following folder within any non-Local GPO:

{GPO ID}\PolicyMaker\license.xml

### Tip

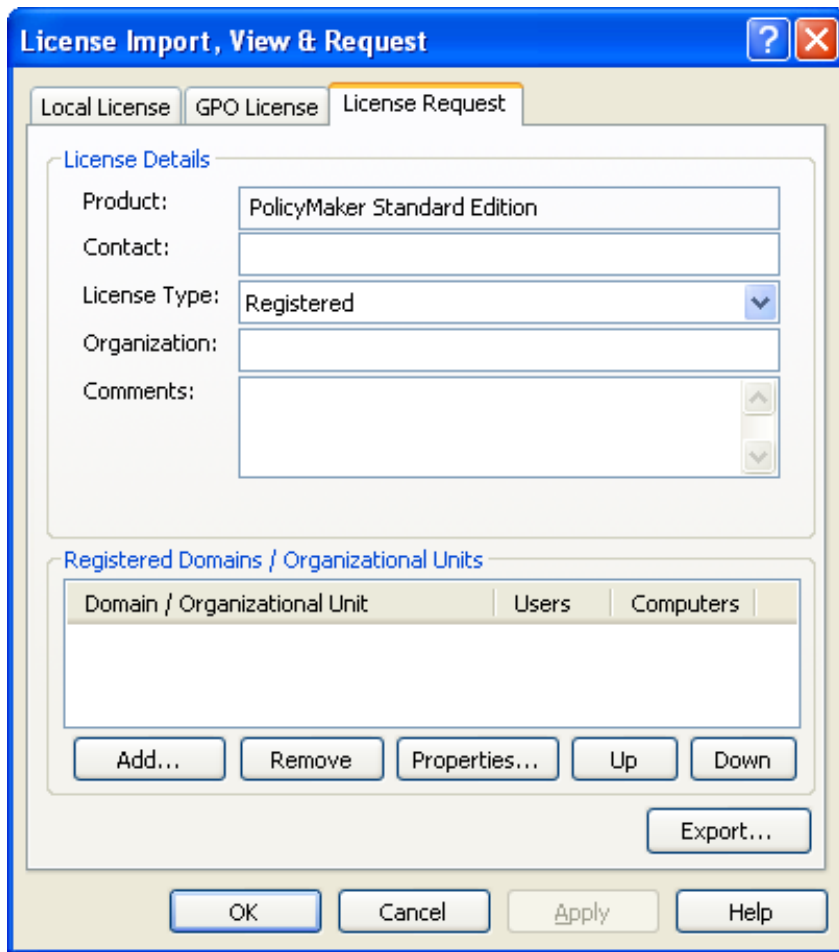
One administrator may deploy the license file to any and all non-Local GPOs and then other administrators may then edit these GPOs without needing the license file locally, and without receiving a warning. This prevents the need to widely distribute the license file.

### See also

[Local License](#) and [License Request](#).

## License Request

The License Request tab of the [licensing](#) property sheet allows you to create and export a license request file (i.e. request.xml), and view the status of that key. The request will be saved (if you hit OK/Apply after changing it) to the local computer for future use, although it has no effect on software product functions.



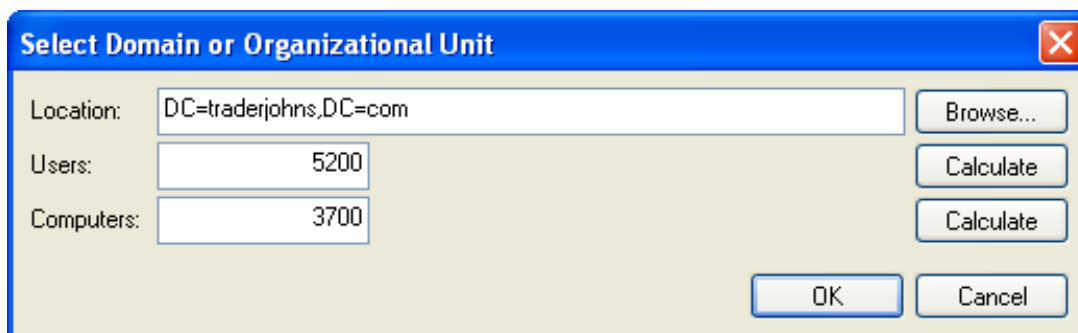
Domain / Organizational Unit	Users	Computers
------------------------------	-------	-----------

Export...

Present a file browse dialog which allows you to save the current license request as a file. This file is typically emailed to a DesktopStandard account representative or authorized reseller, as part of a request for a registered or evaluation key.

Add.../Properties:

Select this option to specify the domain(s) and/or organizational units under which you desire to apply GPOs containing PolicyMaker settings. Any number of domain/ou items may be listed.



Location:	DC=traderjohns,DC=com	Browse...
Users:	5200	Calculate
Computers:	3700	Calculate

Location:

The fully-qualified Active Directory path to the desired domain or organizational unit.

#### Important

It is not recommended to license organizational units within the same hierarchy, as this will result in unnecessary licensing cost and processing overhead.

#### Sites

The location must be a domain or organizational unit. Site-linked GPOs are licensed to domain(s).

Browse...:

Launch a [browser](#) to help you select the Location.

Users:

The number of non-disabled users in the specified location (including all child organizational units). This must be equal to (or greater than) the number of non-disabled users in this location at the time when PolicyMaker CSEs execute. If this number is exceeded, the PolicyMaker CSEs will enter the [license grace period](#) and at the end of this period will cease performing user configurations.

#### Loopback Policy

Loopback policy is a Group Policy CSE processing mode which causes user configuration settings within a GPO(s) to be applied as the result of a computer (not the user) being within the GPO's scope of management (SOM). License quantity for user policy applied in loopback mode is checked against the number of users in the licensed OU to which the logged-on user belongs.

Computers:

The number of non-disabled computers in the specified location (including all child organizational units). This must be equal to (or greater than) the number of non-disabled computers in this location at the time when PolicyMaker CSEs execute. If this number is exceeded, the PolicyMaker CSEs will enter the [license grace period](#) and at the end of this period will cease performing computer configurations.

 See also

[Local License](#) and [GPO License](#) .

## Local Users and Groups

---

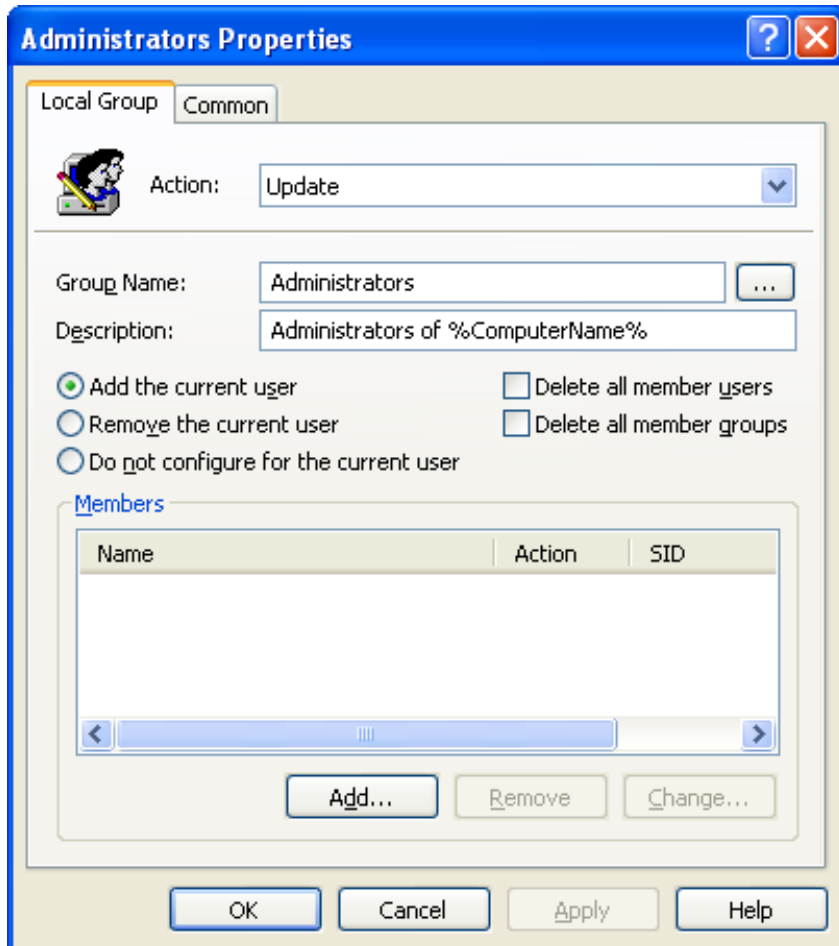
Group Policy extension for configuration of [Local Users](#) and [Local Groups](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Local Group

"Local Group" is a configuration item that is used to configure local security groups.



This policy allows you to managed standardized local groups in several ways. You can create restricted groups by replacing either the group or all of its members (in Update mode) each time the policy is processed. You can also add specific users to groups in order to grant such user accounts certain access. Additionally, in user policy, you can add or remove the logged-on user to/from specific groups - such as the administrators group. The only configurable parameters of a group are its membership and its description, both of which can be modified in Update mode. Members may be added to and/or removed from a group.

Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by group text name.

- Create - creates the group, if it does not already exist. Updates are not applied to a pre-existing group.
- Replace - same as Create except the group is deleted first if it exists. This results in a SID change for the group.
- Update - if the group does not exist, it will be created. Specified actions are then performed on the group.
- Delete - delete the group if it exists.

Group Name:

**Required setting.** The name of the group. The browse button launches the [Group Browser](#). [Variables](#) may be used in this setting.

Description:

An optional description to be applied to the group. [Variables](#) may be used in this setting.



Add the current user:

**User policy only.** Adds to the group the user for whom the policy is being applied. Note that the user is already logged on and as such will not obtain the effect of group membership until the following logon.

Remove the current user:

**User policy only.** Removes from the group the user for whom the policy is being applied. Note that the user is already logged on and as such will effectively retain membership in the group until the following logon.

Do not configure for the current user:

**User policy only.** Does not perform an action with respect to the user for whom the policy is being applied.

Delete all member users:

Removes all user members from the group. This is processed before any member additions are attempted.

Delete all member groups:

Removes all group members from the group. This is processed before any member additions are attempted.

Members:

Add/remove user/computer members to/from the group. Members are specified by SID if the [Group Browser](#) is used. Otherwise members are specified by their text name and are resolved at run-time. Members may be specified using standard conventions. For example, the following formats are valid:

MyGroup  
MyDomain\MyUsername  
MyComputer\MyGroup  
BUILTIN\Administrators  
.\Administrator

A member specified with no prefix will be resolved at run-time using standard resolution logic (by first searching the local host and then the network domain accounts for a match). To specify a local user (member of the builtin domain), use the ".\" notation.

 Note

For an add operation, if a user/group is not resolvable a client-side error occurs. For a remove operation, no such error occurs if the member is unresolvable.

---

 Tip

When set to "Remove this policy when it is no longer applied" on the [common tab](#), this policy provides the option to remove the entire group or only the members last added to the group.

---

 Filter

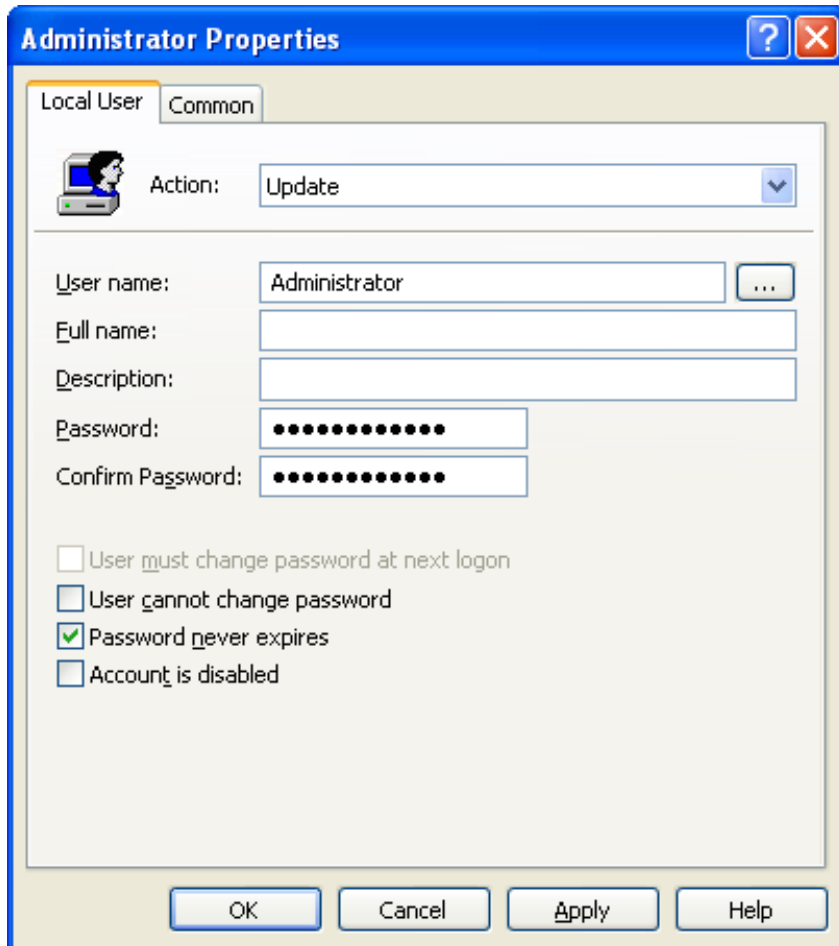
Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Local User

---

"Local User" is a configuration item that is used to configure local computer user accounts.



This policy allows you to managed standardized local user accounts in several ways. You may use this policy to change the password for an existing user account, such as the Administrator account, on multiple computers. You may also use this to create new local accounts, such as for use with a [Windows service](#), custom application, or off-domain end-user logon. User accounts can also be automatically added to new or existing groups using [Local Group](#) policy. All of the settings of this policy may be applied to an existing user account in Update mode.

### Action:

One of the standard PolicyMaker [action modes](#). Matching is by user name.

- Create - creates the user, if it does not already exist. Updates are not applied to a pre-existing account.
- Replace - same as Create except the user is deleted first if it exists. This results in a SID change for the user account.
- Update - if the user does not exist, it will be created. Settings are then applied to the user account.
- Delete - delete the user if it exists.

### User Name:

**Required setting.** The text name of the local user account. The browse button launches the [User Browser](#). [Variables](#) may be used in this setting.

### Full Name:

An optional display name to be set for the user. [Variables](#) may be used in this setting.

### Description:

An optional description to be set for the user. [Variables](#) may be used in this setting.

#### Password:

When the policy creates or replaces an account, this will be the new password for the account and is required to match password policy on the computer. On a Windows 2003 domain the default is a 4 character minimum.

If updating an existing account, this field may be left empty to indicate no change to the existing password. If a password is specified in an update scenario, the password will be applied to the existing account.



Tip

The password must comply with the computer's password policy, or an error will be generated by the client when configuration is attempted. User accounts cannot be created without supplying a password that conforms to the password policy.

#### ◆ Password Security

The password is encrypted before being saved into the configuration XML. The password is decrypted by the Local Users and Groups client side extension so that it may be applied to configuring the user. It is important to note that it is technically possible, although difficult, to recover the password from the settings file.

#### Additional attributes:

The remaining attributes are applied to the configured account.

---



#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Mail Profiles

---

Group Policy extension for configuration of [Mail Profile](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Mail Profile

---

"Mail Profile" is a configuration item that is used to configure mail profiles for Outlook and other MAPI applications. This policy is only processed in Group Policy's [foreground processing](#) mode.

### Match by

Specifies the method for finding preexisting MAPI profiles.

- Name  
The profile with a matching name will be modified according to the selected *Action*.
- Default  
The default profile will be modified according to the selected *Action*.
- All  
All existing profiles will be modified according to the selected *Action*.
- Temporary  
A temporary profile will be created and then removed from the profile list after configuration.

### Action

Specifies the action to be performed on a nonexistent or preexisting MAPI profile that meets the above criteria. The expected outcome of each possible combination of the *Match by* and *Action* options is displayed in the *Description* field at the bottom of the tab.

- Create  
The profile will be created if a matching profile is not found.
- Replace  
The profile will be replaced if a matching profile is found. A new profile will be created if a matching profile is not found.
- Update  
The profile will be updated if a matching profile is found. A new profile will be created if a matching profile is not found.
- Migrate  
The profile will be updated only if a matching profile is found.
- Delete  
The profile that meets the *Match by* criteria will be deleted.

### Options

- Make this the default profile  
Sets this profile as the default MAPI profile.
- Delete profile if a configuration error occurs  
The profile will be deleted if an error occurs that prevents any aspect of the configuration from succeeding.

### Windows Messaging profile prompt

These options allow you to show or suppress the profile select dialog box that appears when a MAPI application is started

- Don't change existing setting  
The current profile prompt setting will remain unchanged.
  - Disable  
The profile prompt will be disabled.
  - Enable  
The profile prompt will be enabled.
  - Smart (when more than one profile exists)  
The profile prompt will be enabled, but only in the case where more than one profile exists in the profile list.
-



## Addressing

---

### Show this address list first

This item can contain any valid address list. This includes read-only address lists, such as the "Global Address List" for Exchange Server, address books that cannot contain recipients, such as the "Outlook Address Book" root container, and address books that can be updated, such as the "Personal Address Book".

- Address Book Type  
This select box allows you to specify the first address list shown in your messaging application.
- Address Book Name  
This box allows you to specify a display name for the first address list.
- SubContainer  
This box specifies the location of the address list.

**Note:** The Microsoft Exchange Directory contains two address lists by default so you must specify the name of the address list in the "Name" field ( ie . "Global Address List").

### Keep personal addresses in

This item can only contain address books that can be updated, such as the "Personal Address Book". The "Outlook Address Book" can be used but you must specify the folder that contains the writable address list ("Contacts" is the Outlook default folder).

- Address Book Type  
This select box allows you to specify the type of address book where your personal addresses will be stored.
- Address Book Name  
This box allows you to specify a display name for the personal address list.
- SubContainer  
This box specifies the location of the personal address list.

### Erase existing search order list before configuring

This option removes all address books from the existing address book search order list before making changes to it.

### Address book search order

Enter the address books in the desired order. Any address books not listed here will neither be automatically added nor used for name lookup by a messaging client. If no address books are listed PolicyMaker will not set the order, as a result, the default address book for each of the services in the profile will be used instead.

Selecting the Add, Remove, Properties, Up, or Down buttons will allow you to manipulate the following items:

- Address Book Type  
This select box allows you to specify the type of address list.
- Address Book Name  
Allows you to specify a display name for the address book.
- SubContainer  
Allows you to set the path where the address book is located.
- Action  
Allows you to specify an action to take when modifying the address book search order list.  
*Insert* - Places the address book at the top of the search order list.  
*Append* - Places the address book at the end of the search order list.  
*Remove* - Deletes the address book from the search order list.



#### Note

Addressing options will be bypassed if there is an error creating the MAPI profile.

## Contacts

---

Erase existing contact folder list before configuring

This option removes all contacts folders from the list before making changes to it.

Configure these contact folders as address books

To set up a contacts folder, a corresponding folder should be created (on the *Folders* tab) as type "Contact" so that the contacts folder will be created prior to being added to the contacts folder list.

Selecting the Add, Remove, Properties, Up, or Down buttons will allow you to manipulate the following items:

- **Store Type**  
The type of the store in which the contact folder will be configured.
- **Store Name**  
The display name of the store in which the contact folder will be configured.
- **SubFolder**  
The location of the contact folder within the store.
- **Address Book Name**  
The name of the contact folder to be configured. If this optional property is omitted, the *SubFolder* property will be used.
- **Action**  
Allows you to specify an action to take when adding contact folder to the list.  
*Insert* - Places the contact folder at the top of the list.  
*Append* - Places the contact folder at the end of the list.  
*Remove* - Deletes the contact folder.



## Delivery

---

### Default Store

Sets the default delivery location for incoming messages.

- **Store Type**  
Allows you to select from a list of possible default store locations.
- **Store Name**  
Allows you to specify a display name for the default store.

### Transport Order

Enter the display names of transport providers as they appear in the Windows Messaging "Delivery" tab, in the desired order. Any providers not listed here, but present in the profile, are automatically added to the end of the list in the previously existing order. This option is necessary only if you have more than one information service that supports the same address type. For example, you might have Microsoft Exchange Server followed by Internet Mail. Any message you send to an Internet recipient could be processed and sent via Microsoft Exchange Server, because this service also supports Internet addresses. If you want all messages addressed to Internet recipients to be processed by the Internet Mail service, move this service to the top of the list.

Selecting the Add, Remove, Properties, Up, or Down buttons will allow you to manipulate the following items:

- **Transport Type**  
Allows you to select from a list of possible transport items.
- **Transport Name**  
Allows you to specify a display name for the transport item.

### Notes

Delivery options will be bypassed if there is an error creating the MAPI profile.

Delivery options do not require PolicyMaker to log on to the message stores and as such can be configured for password protected stores without a password prompt (unlike "Addressing" and "Folders" options).

Outlook XP and above implement their own non-MAPI transport ordering systems. These options will not affect transport ordering for these applications.

## Folders

---

Configure these MAPI folders

Items in this list represent folders that will be created if they do not already exist in the specified store.

Selecting the Add, Remove, Properties, Up, or Down buttons will allow you to manipulate the following items:

- **Store Type**  
The type of the store in which the folder(s) will be configured.
  - **Store Name**  
The display name of the store in which the folder(s) will be configured.
  - **Folder Path/Name**  
The location/name of the folder within the store.
  - **Folder Type**  
The class of folder to be configured. Technically this translates into the MAPI "IPF" (Interpersonal Message Folder) type.
-

## Mail Service

---

"Mail Service" is a subcomponent of [Mail Profile](#) policy and is not a policy by itself.

### Match by

Specifies the method for finding preexisting MAPI services.

- Type  
The service of the same type will be modified according to the selected *Action*.
- Name & Type  
The service of the same type and name will be modified according to the selected *Action*.

### Action

Specifies the action to be performed on a nonexistent or preexisting MAPI service that meets the above criteria. The expected outcome of each possible combination of the *Match by* and *Action* options is displayed in the *Description* field at the bottom of the tab.

- Create  
The service will be created if a matching service is not found.
- Replace  
The service will be replaced if a matching service is found. A new service will be created if a matching service is not found.
- Update  
The service will be updated if a matching service is found. A new service will be created if a matching service is not found.
- Migrate  
The service will be updated only if a matching service is found.
- Delete  
All services that meet the *Match by* criteria will be deleted.

### Options

- Present service configuration property sheet  
The service will display its property sheet during configuration to collect information from the end user (such as a password).
- Delete this service from profile on error  
The service will be deleted from the profile if an error occurs during configuration.

## Network Options

---

Group Policy extension for configuration of [VPN Connections](#) and [Dial-Up Networking](#).

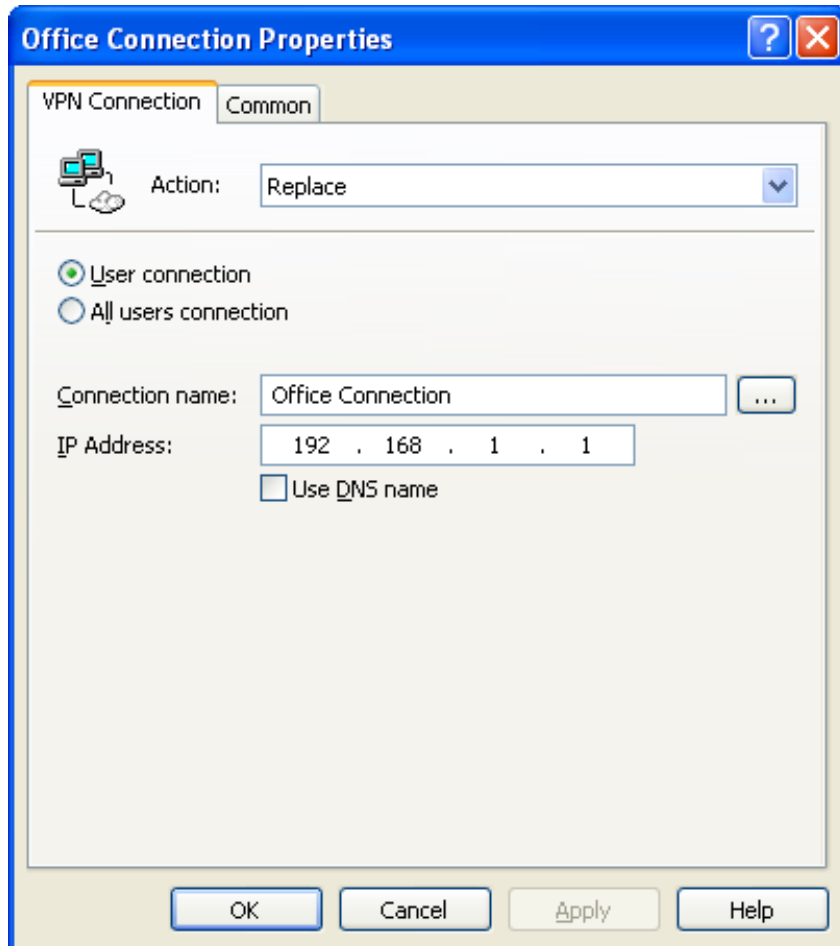
---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## VPN Connection

---

"VPN Connection" is a configuration item that is used to manage VPN connections users and computers.



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Connection name and User connection vs. All user connection.

- Create - creates the VPN connection, if it does not already exist.
- Replace - same as Create except the VPN connection is deleted first if it exists.
- Update - if the VPN connection does not exist, it will be created.
- Delete - delete the VPN connection if it exists.

User connection:

A User connection is visible only to the user for whom it is configured.

All users connection:

An all users connection is visible to all users of the machine.

Connection name:

**Required setting.** The name you want to use when referencing this connection. The browse button launches the [VPN Browser](#). [Variables](#) may be used in this setting.

IP Address/DNS Name:

**Required setting.** The IP address or DNS name (as specified by Use DNS name) of the VPN to which the connection will be made. [Variables](#) may be used in the DNS Name field.

Use DNS name:

Specify that the IP Address field should switch to DNS Name.

---



Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

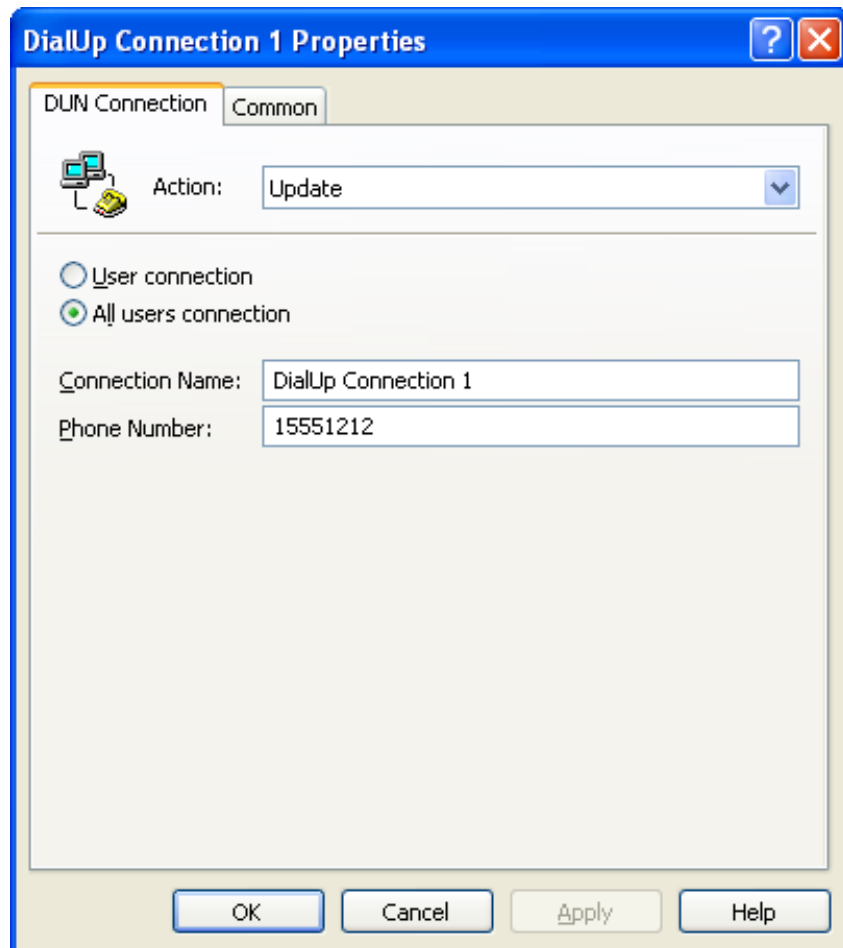
---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Dial-Up Networking Connection

---

"DUN Connection" is a configuration item that is used to manage DUN connections for users and computers.



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Connection name and User connection vs. All user connection.

- Create - creates the DUN connection, if it does not already exist.
- Replace - same as Create except the DUN connection is deleted first if it exists.
- Update - if the DUN connection does not exist, it will be created.
- Delete - delete the DUN connection if it exists.

User connection:

A User connection is visible only to the user for whom it is configured.

All users connection:

An all users connection is visible to all users of the machine.

Connection name:

**Required setting.** The name you want to use when referencing this connection. The browse button launches the [DUN Browser](#). [Variables](#) may be used in this setting.

Phone Number:

**Required setting.** The phone number to which the connection will be made. [Variables](#) may be used in this setting.

---

 Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.



## User/Computer Control Panel

---

This extension holds policy extensions that configure settings that are manually configured via the control panel for a user or computer. User settings are grouped in user policy, and computer settings are grouped in computer policy.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## User/Computer Settings

---

This extension holds general policy extensions that affect a user or computer. User settings are grouped in user policy, and computer settings are grouped in computer policy.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Power Options

---

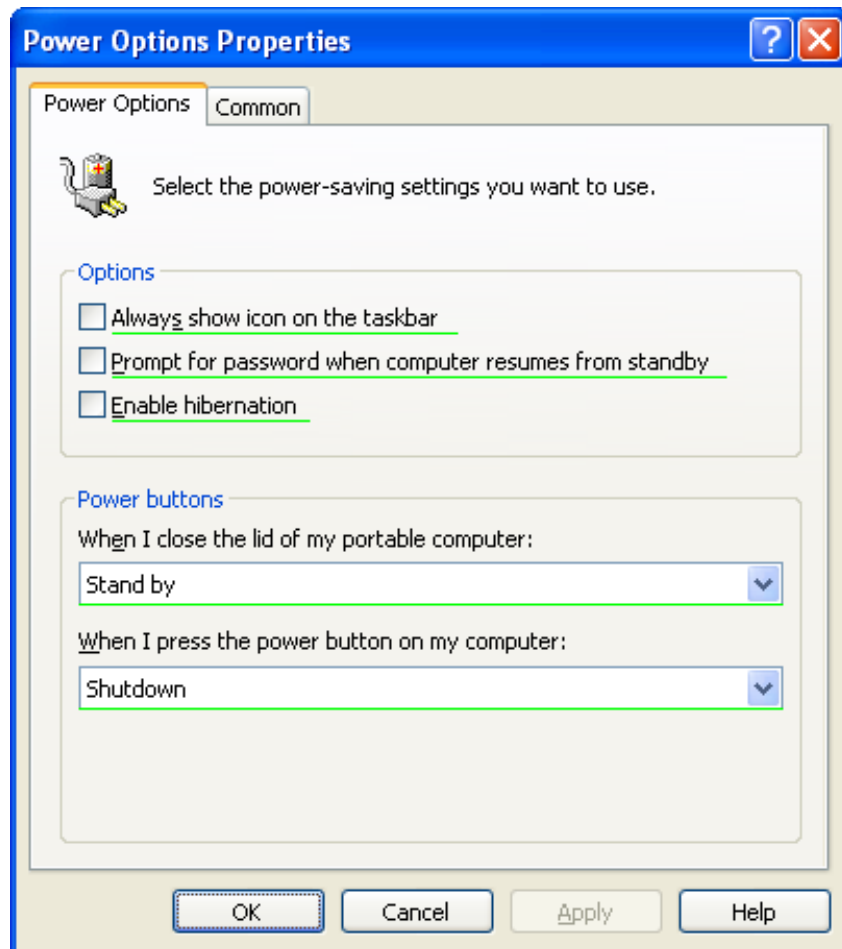
Group Policy extension for configuration of [Power Options](#) and [Power Schemes](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Power Options

"Power Options" is a configuration item that is used to manage the operating system's handling of various power conditions.



Power options are settings that exist for a user or a computer. In computer policy, these settings are applied to the computer environment and in user policy they are applied to the user's environment. The settings are stored separately in these environments. However, in order to affect the current state of the computer, they are also applied to the currently active computer settings. The currently active settings exist in one place, globally for the computer - as the computer can only execute one set of power settings at a time.

When computer or user policy is applied these settings are stored for the computer or user respectively, and also immediately made active. Therefore if user policy runs after computer policy, the user settings will replace the active settings that may have been made active previously by a computer or user.

Although a local administrator or power user can manually change their power settings using the control panel, other users cannot. Regardless, the settings that are configured for users become active when they log on and remain so even after they log off.

As a result settings applied to the computer environment become active when the computer is started and no user has logged on. However, using Power Options policy, which supports computer background refresh, active power settings can be reset when computer policy is applied and no users are logged on.

**Always show icon on the taskbar:**

This option enables or disables a power icon in the task tray. This is disabled in computer policy.

**Prompt for password when computer resumes from standby:**

This option will cause the computer to be password protected when it comes out of hibernation.

**Enable hibernation:**

This option will allow the computer to enter hibernation mode. To configure idle time before automatic hibernation, use the [Power Scheme](#) policy.

#### Power buttons:

These options tell the operating system what to do when computer power buttons are pressed. Note that not all options are available in all operating systems. If an option is provided for a platform that does not support the option, the value will be set to the default value for that system.

---

#### Notes

This page uses [property underlining](#) to control which settings are applied.

---

#### Filter

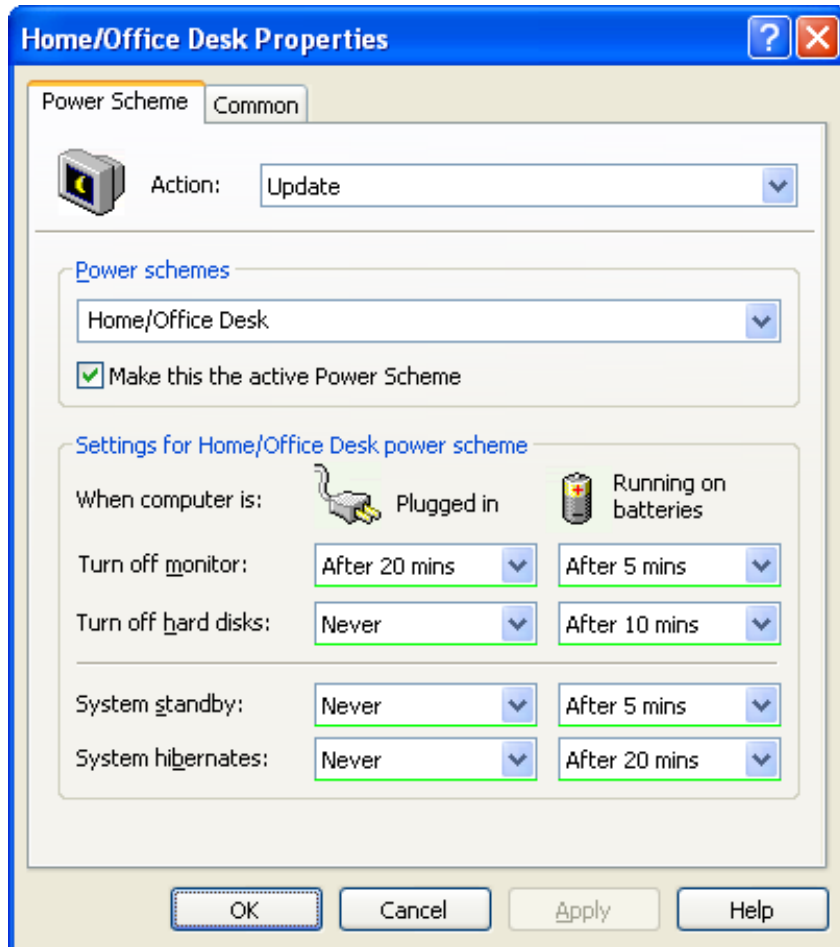
Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Power Scheme

"Power Scheme" is a configuration item to configure how a computer manages hardware power consumption following various periods of inactivity.



Power schemes are groups of settings that are combined under a name. Schemes exist independently for users and computers. In computer policy, these schemes are applied to the computer environment and in user policy they are applied to the user's environment. The settings are stored separately in these environments. However, in order to affect the current state of the computer, they are also applied to the currently active computer settings (if 'Make this the active Power Scheme' is set). The currently active settings exist in one place, globally for the computer - as the computer can only execute one set of power settings at a time.

When computer or user policy is applied these settings are stored for the computer or user respectively, and also immediately made active (if set active). Therefore if the user policy runs after the computer policy, the user settings will replace the active settings that may have been made active previously by a computer or user. Although a local administrator or power user can manually change their active power scheme settings using the control panel, other users cannot. Regardless, the scheme that is configured for users becomes active when they log on and remains so even after they log off.

As a result the active scheme applied to the computer environment becomes the default, and therefore active when the computer is started and no user has logged on. However, using Power Scheme policy, which supports computer background refresh, active power scheme settings can be reset when computer policy is applied and no users are logged on.

Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Power Scheme name within in the applicable user/computer context. Note that Windows XP Gold

- Create - creates and configures the Power Scheme, if it does not already exist.
- Replace - same as Create except the Power Scheme is deleted first if it exists.
- Update - if the Power Scheme does not exist, it will be created. If it exists it may be made active.

- Delete - delete the Power Scheme if it exists.

Power schemes:

**Required setting.** The name of the power scheme. [Variables](#) may be used in this setting.

 Windows 2000

Windows 2000 computers display only the default schemes provided for Windows 2000. Also note that names are language-specific display values and must be targeted accordingly.

Settings for:

These settings control what values are to be contained within the specified power scheme. For the creation of a new scheme, any disabled values are pulled from the default power scheme for the computer/user. The property sheet selects the standard settings for any power scheme selected in the Power Schemes menu.

---

 Notes

This page uses [property underlining](#) to control which settings are applied.

---

 Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Printers

---

Group Policy extension for configuration of [TCP/IP Printers](#) , [Shared Printers](#) and [Local Printers](#).

---

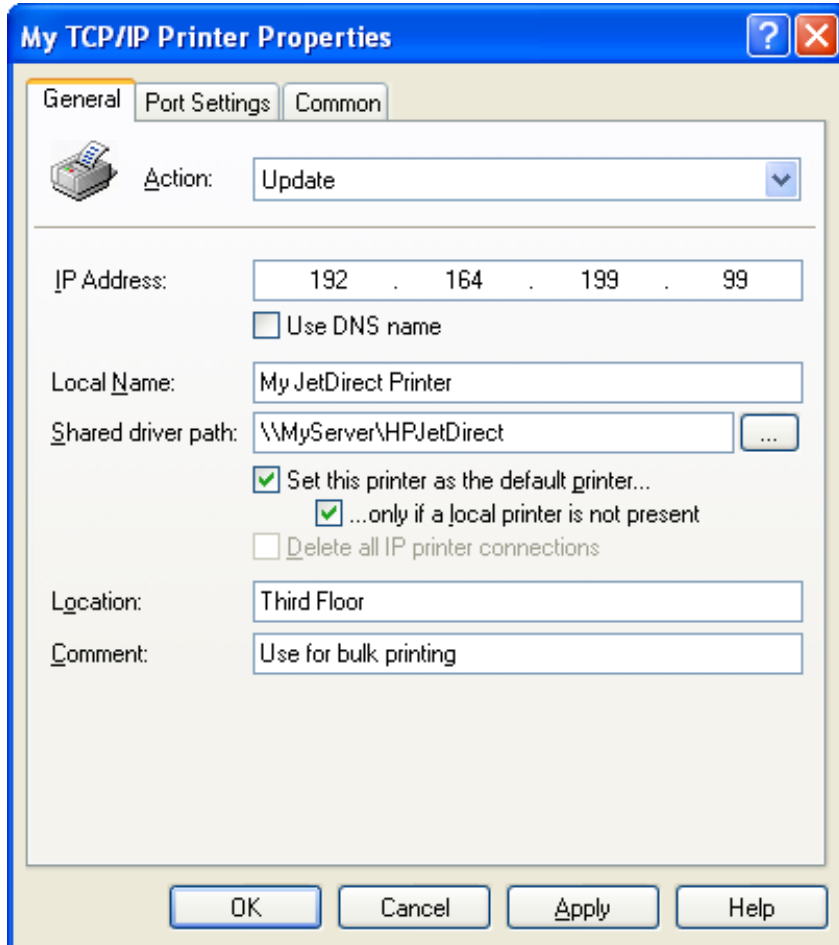
© 2005 DesktopStandard Corporation. All Rights Reserved.



## TCP/IP Printer

"TCP/IP Printer" is a configuration item that is used to set up TCP/IP and LPR printer connections on Windows 2000 and later computers. This option cannot be used to configure a shared printer connection. To configure a shared printer use the [Network Printer](#) item (in a user configuration). Note that while this item may be configured in user policy, it affects all users of the computer.

General Tab:



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by printer IP address.

- Create - creates the printer connection, if it does not already exist. The default status is then set.
- Replace - deletes the printer connection, if found. The connection is then created and default status set.
- Update - creates the printer connection, if not found. The default status is then set.
- Delete - deletes the printer connection, if found. Drivers are not deleted.

IP Address:

**Required setting.** The Internet Protocol (IP) address of the printer.

Use DNS Name

Changes the IP Address field to "DNS Name", allowing entry of a resolvable name for the printer address. [Variables](#) may be used in the DNS Name field.

Local Name (optional):

The name to give the printer item in the "Printers and Faxes" shell folder. If a Local Name is specified, the configuration will match using the Local Name of the printer instead of the IP Address (or DNS Name) of the

port.

Shared driver path:

**Required setting (except in Delete mode).** The fully qualified UNC path of a shared connection to the TCP/IP printer. This setting is disabled in delete mode. Configuration will not transfer drivers if the required and current drivers are already present on the workstation. The browse button launches the [Printer Browser](#). [Variables](#) may be used in this setting.

#### Driver Distribution

Installing a printer on a Windows server only installs the drivers for the operating system currently running on the server. If a printer is going to be configured on computers running a different operating systems, you must install printer drivers for these other operating systems, to the shared driver path. To share printer drivers, follow these steps:

Shared from a Windows NT Server

Right-click on the printer's icon, select "Properties" and switch to the "Sharing" tab. At the bottom of the tab, find a list box entitled "Alternate Drivers". Highlight the items in the list that represent the operating systems on your network and select "OK". The installation disk that came with the printer might be needed to complete this operation.

Shared from a Windows 2000 Server

Right-click on the printer's icon, select "Properties" and switch to the "Sharing" tab. On the lower right, find a button entitled "Additional Drivers" that launches a dialog box. Check off the items in the list that represent the operating systems on your network and select "OK". The installation disk that came with the printer might be needed to complete this operation.

#### Note

This path is only used by PolicyMaker for driver installation. The actual printer connection will be direct from the workstation to the TCP/IP printer. Once the driver installations have been completed, this printer share may be removed from the network if desired.

#### Note

The shared printer's Online/Offline state may be applied to the printer being configured. It is suggested that you leave the shared printer Online to prevent this from happening.

Set this printer as the default printer...:

Makes the printer the default Windows printer for the logged-on user. This setting is disabled in delete mode and when this item is configured in computer policy.

...only if a local printer is not present:

Bypasses changing the default printer if there is another "local" printer configured on the computer. This setting is disabled in delete mode and if "Set this printer as the default printer" is not selected.

#### Note

A "local" printer is any printer that is *physically connected* to a Parallel (LPT) Port, Serial (COM) Port or Universal Serial Bus (USB) port. There are also "virtual" printers that masquerade as local printers, such as the Adobe PDF writer and others. These do not qualify as a "local" printer for the purposes of this option.

Delete all IP printer connections:

Deletes all IP printers from the computer. This option does not affect printer shares. The setting is enabled only in delete mode.

Location:

Arbitrary text that will be displayed in the printer's "Location" field. [Variables](#) may be used in this setting.

Comment:

Arbitrary text that will be displayed in the printer's "Comment" field. [Variables](#) may be used in this setting.

---

#### Notes

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). PolicyMaker can configure the printer even if the end-user has no ability to copy drivers or configure printers due to security or policy restrictions. To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#).

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

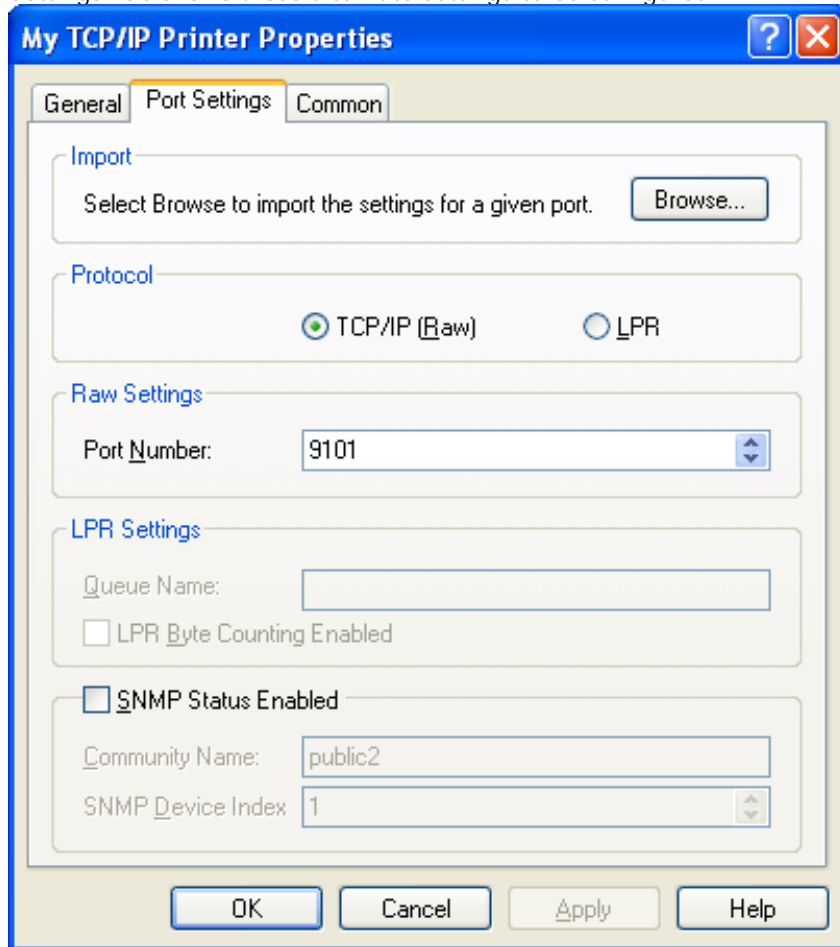


## TCP/IP Printer - Port Settings

"TCP/IP Printer" is a configuration item that is used to set up TCP/IP printer connections on Windows 2000+ computers. This option cannot be used to configure a shared printer connection. To configure a shared printer use the [Network Printer](#) item (in a user configuration). Note that while this item may be configured in user policy, it affects all users of the computer.

Port Settings Tab:

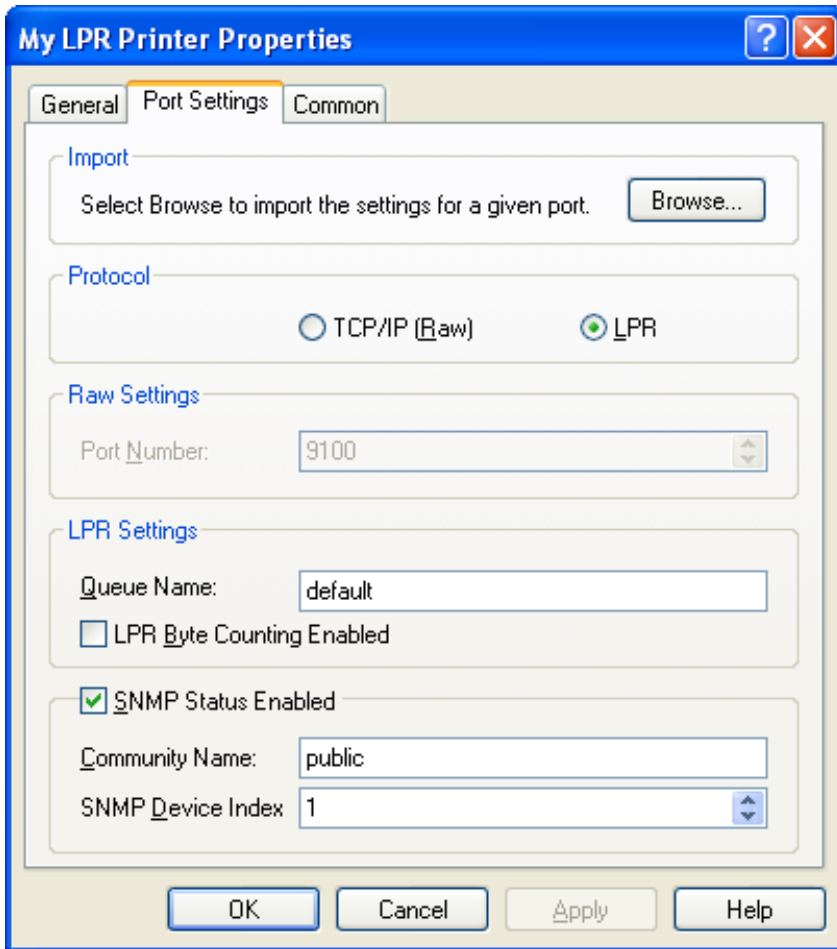
Some single- or multiple-port TCP/IP and LPR printers use different port settings than the standard defaults. The Port Settings Tab allows these alternate settings to be configured.



The screenshot shows the 'My TCP/IP Printer Properties' dialog box with the 'Port Settings' tab selected. The dialog has three tabs: 'General', 'Port Settings', and 'Common'. The 'Port Settings' tab contains the following sections:

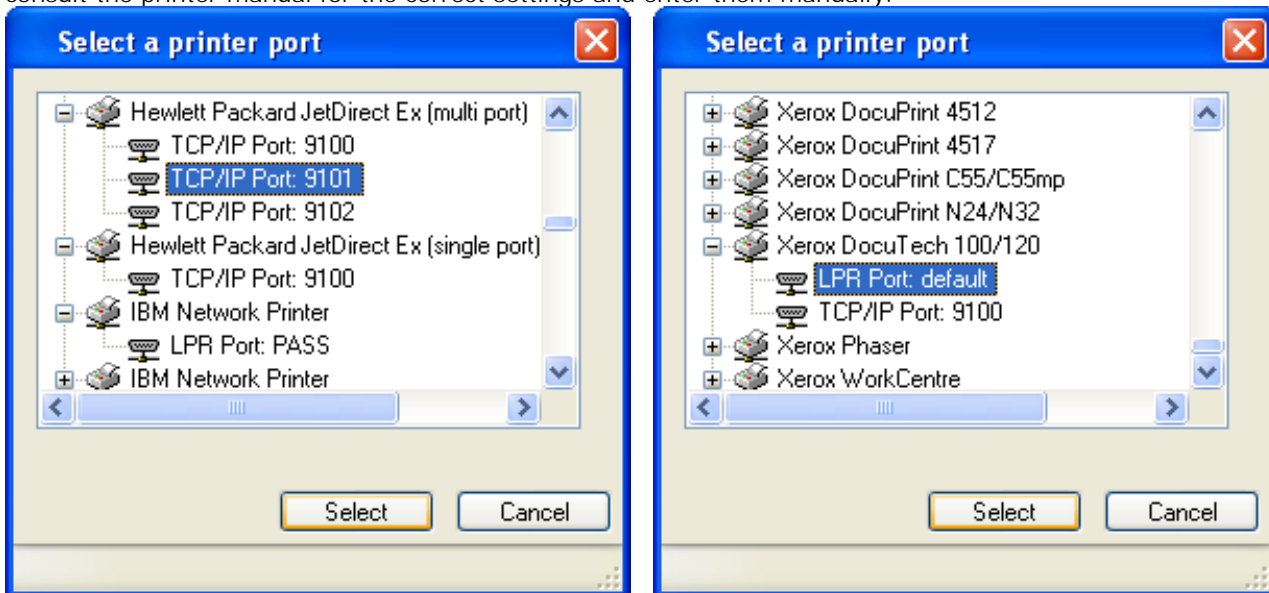
- Import:** A text box with the instruction 'Select Browse to import the settings for a given port.' and a 'Browse...' button.
- Protocol:** Two radio buttons: 'TCP/IP (Raw)' (selected) and 'LPR'.
- Raw Settings:** A 'Port Number' field with a dropdown menu showing '9101'.
- LPR Settings:** A 'Queue Name' text box, an unchecked checkbox for 'LPR Byte Counting Enabled', and an unchecked checkbox for 'SNMP Status Enabled'.
- SNMP Settings:** A 'Community Name' text box containing 'public2' and an 'SNMP Device Index' dropdown menu showing '1'.

At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.



### Import

The Browse feature brings up a list of TCP/IP and LPR printer models. Selecting a port from this list will automatically fill in the Protocol, Raw, LPR and SNMP settings with appropriate values. If your model of printer is not in the list, consult the printer manual for the correct settings and enter them manually.



### Protocol

Specifies the type of printer to which the connection will be made:

- TCP/IP (Raw) - The printer is a TCP/IP (or "Port 9100") printer.
- LPR - The printer is an RFC1179-compliant LPR printer.

## Raw Settings

These settings apply only to TCP/IP (Raw) printers:

Port Number - The TCP/IP Port to use when communicating with the printer. The default is 9100.

## LPR Settings

These settings apply only to LPR printers:

Queue Name - The name of the LPR Queue to use when communicating with the printer. The default is "LPR".

LPR Byte Counting Enabled - If this box is checked, document sizes are calculated locally prior to being sent to the printer. Some LPR ports require this setting to be enabled to prevent data loss.

### Note

If this box is automatically *checked* by the Import feature, the selected LPR port requires this setting to be enabled.

## SNMP Status Enabled

Specifies whether or not the printer port will support RFC1759. By default, this box is unchecked.

### Note

When this box is automatically set by the Import feature, it can be set to one of these states:

- Checked - The selected port supports RFC1759.
- Unchecked - The selected port does not support RFC1759.
- Indeterminate (shown below) - The selected port may support RFC1759.



The screenshot shows a checkbox labeled "SNMP Status Enabled" which is checked. Below it are two input fields: "Community Name" with the value "public" and "SNMP Device Index" with the value "1".

### Note

If this box is left set to the indeterminate state (shown above), it is functionally the same as leaving it unchecked.

### Community Name

Specifies the SNMP community name used by the printer. The default is "public".

### SNMP Device Index

Specifies the SNMP device index used by the printer. The default is 1.

---

## Notes

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). PolicyMaker can configure the printer even if the end-user has no ability to copy drivers or configure printers due to security or policy restrictions. To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#).

---

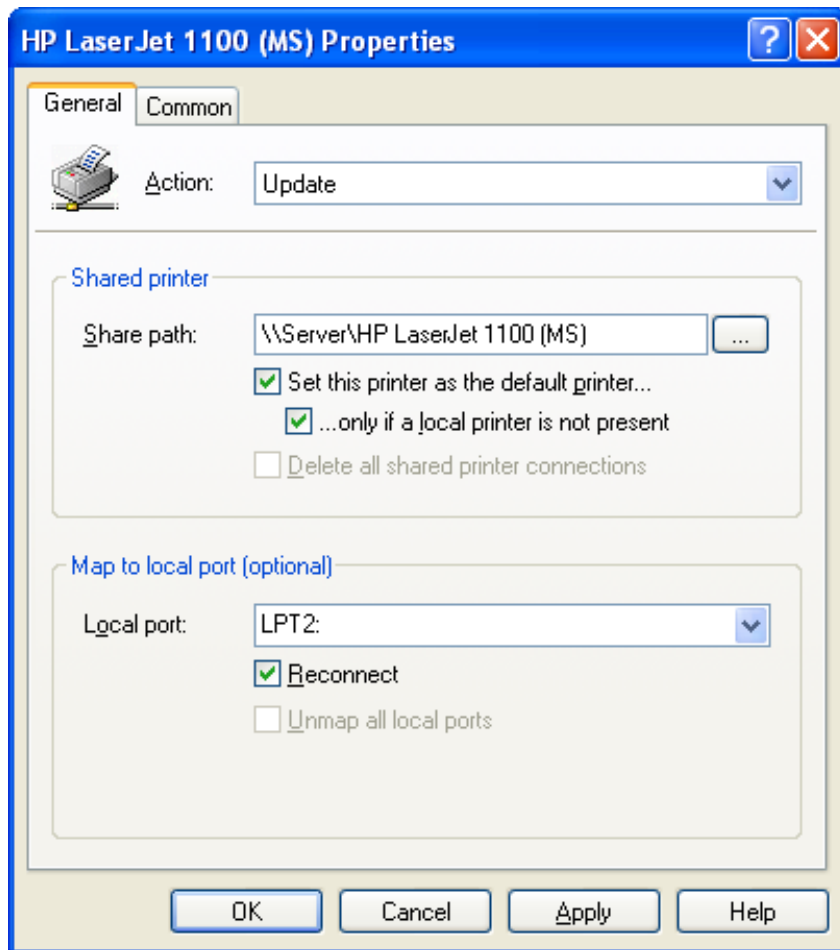
## Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Shared Printer

"Shared Printer" is a configuration item that is used to set up printer connections to shared network printers. This option cannot be used to configure a TCP/IP printer connection. To configure a TCP/IP printer use the [TCP/IP Printer](#) item.



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Share path.

- Create - creates the printer connection, if it does not already exist. The default status is then set.
- Replace - deletes the printer connection, if found. The connection is then created and default status set.
- Update - creates the printer connection, if not found. The default status is then set.
- Delete - deletes the printer connection(s) if found. Drivers are not deleted.

Share path:

**Required setting (except with "Delete all shared printer connections" selected).** The fully qualified UNC path of a shared printer. This setting is disabled with "Delete all network printers" selected. The browse button launches the [Printer Browser](#). [Variables](#) may be used in this setting.

### Driver Distribution

Installing a printer on a Windows server only installs the drivers for the operating system currently running on the server. If a printer is going to be configured on computers running a different operating systems, you must install printer drivers for these other operating systems, to the shared driver path. PolicyMaker supports versioned driver distribution on all platforms. To share printer drivers, follow these steps:

#### Shared from a Windows NT Server

Right-click on the printer's icon, select "Properties" and switch to the "Sharing" tab. At the bottom of the tab,

find a list box entitled "Alternate Drivers". Highlight the items in the list that represent the operating systems on your network and select "OK". The installation disk that came with the printer might be needed to complete this operation.

#### Shared from a Windows 2000 Server

Right-click on the printer's icon, select "Properties" and switch to the "Sharing" tab. On the lower right, find a button entitled "Additional Drivers" that launches a dialog box. Check off the items in the list that represent the operating systems on your network and select "OK". The installation disk that came with the printer might be needed to complete this operation.

Set this printer as the default printer...:

Makes the printer the default Windows printer for the logged-on user. This setting is disabled in delete mode.

...only if a local printer is not present:

Bypasses changing the default printer if there is any "physical" printer configured on the machine. This setting is disabled in delete mode and if "Set this printer as the default printer" is not selected.

#### Note

A local printer is any printer that is not a connection to a shared network printer. There are several types of such printers, including Parallel Port (LPT) printers, Universal Serial Bus (USB), Serial, Infrared, Fax (via modem), TCP/IP, etc. There are also "virtual" printers that masquerade as local printers, such as the Adobe PDF writer and others. Any of these may qualify as a local printer for the purposes of this option.

Delete all shared printer connections:

Specifies deletion of all shared printer connections for the logged-on user. Enabled only in delete mode.

Map to local port (optional)

These settings allow a shared printer connection to be mapped to a local printer port so that it can be used by legacy applications that do not support shared printers.

Local port

The local printer port's name (Example: "LPT2:"). In delete mode, this field specifies the port mapping to be removed.

Reconnect

If this is checked, the connection persists across logon sessions.

Unmap all local ports

Removes all local port mappings for the logged-on user. Enabled only in delete mode.

---

#### Note

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). PolicyMaker can therefore configure a printer connection even if the end-user has no ability to copy drivers or configure printers due to security or policy restrictions. The driver installation is always performed in the security context specified on the common tab. This item will always use the end-user's security context to map the printer connection and set the default printer status. To change this item to run fully within end-user permissions, change the security context on the [common tab](#).

#### Driver Distribution

Installing a printer on a Windows server only installs the drivers for the operating system currently running on the server. If a printer is going to be shared with other computers on a network that are running different operating systems, you must install printer drivers (on the printer share) for these other operating systems.

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---



## Regional Options

---

Group Policy extension for configuration of [Regional Options](#).

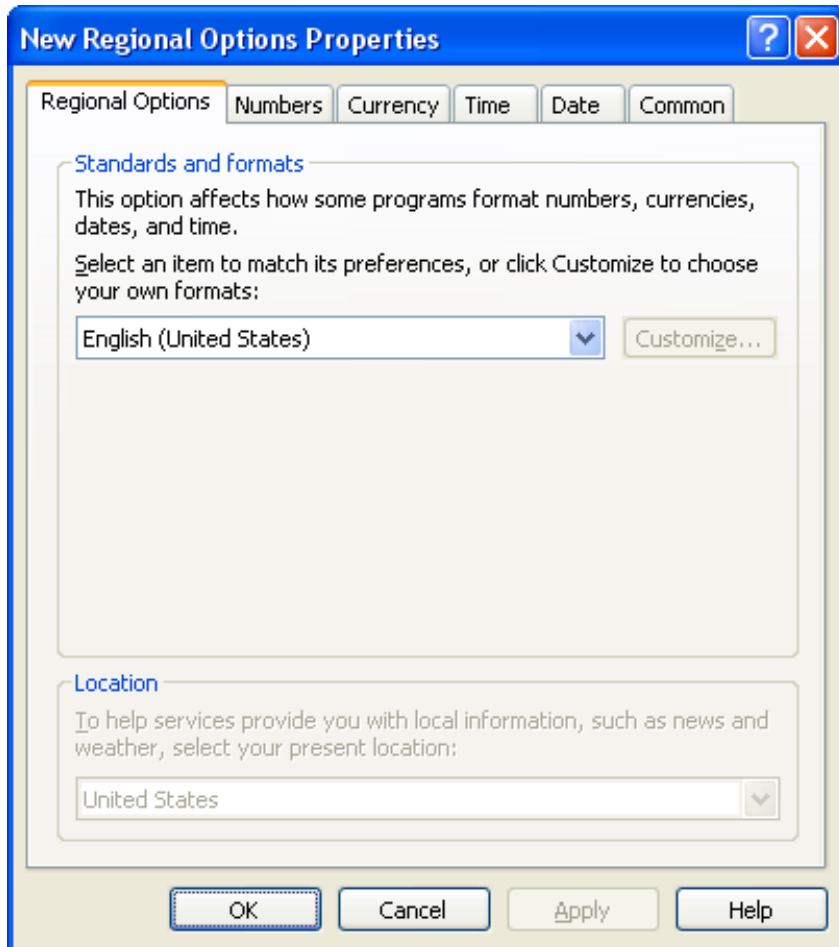
---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Regional Options

---

"Regional Options" is a configuration item that manages how numbers, currency, dates, and time values are displayed for users.



---

### Note

Selecting a locale resets all of the values on the other tabs. When applied this policy will change the default locale for the end-user and optionally apply changes to that locale as specified in other tabs.

---

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Regional Options - Currency

"Regional Options - Currency" affects how the locale specified on the "[Regional Options](#)" tab will display various currency value types.

The screenshot shows the 'English (United States) Properties' dialog box with the 'Currency' tab selected. The 'Sample' section displays 'Positive: \$123,456,789.00' and 'Negative: (\$123,456,789.00)'. The settings are as follows:

Setting	Value
Currency symbol:	\$
Positive currency format:	\$1.1
Negative currency format:	(\$1.1)
Decimal symbol:	.
No. of digits after decimal:	2
Digit grouping symbol:	,
Digit grouping:	123,456,789

Buttons at the bottom: OK, Cancel, Apply, Help.

### Note

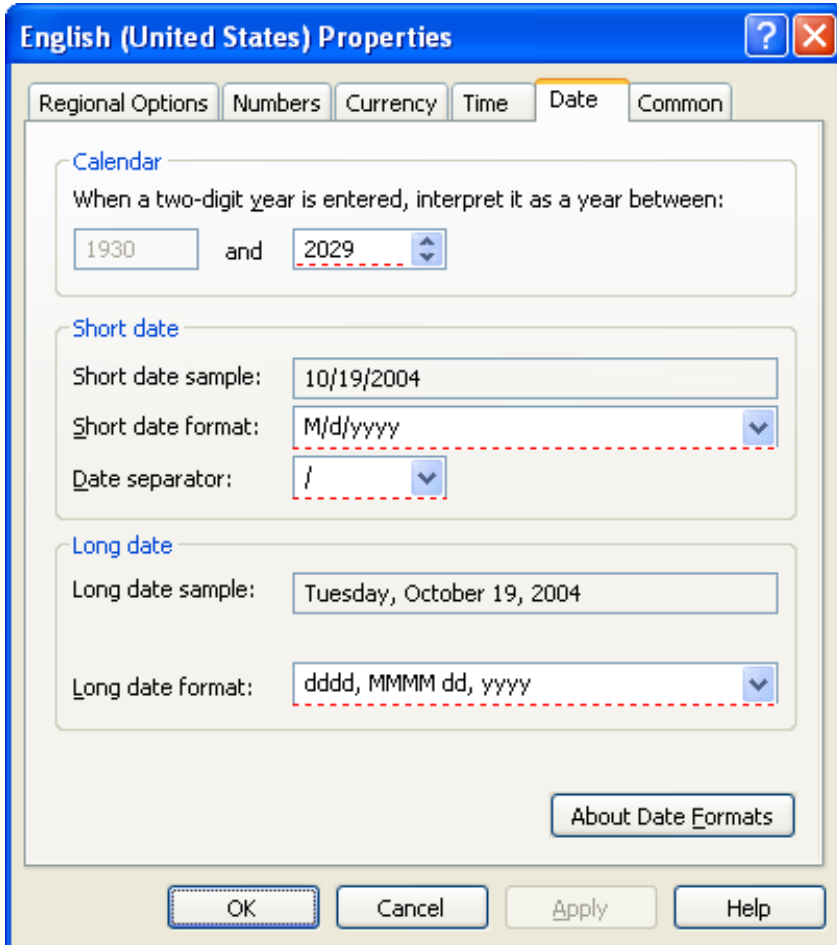
This page uses [property underlining](#) to control which settings are applied. By default all settings are disabled (red).

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Regional Options - Date

"Regional Options - Date" affects how the locale specified on the "[Regional Options](#)" tab will display various date/time value types.



**English (United States) Properties**

Regional Options Numbers Currency Time **Date** Common

**Calendar**

When a two-digit year is entered, interpret it as a year between:

1930 and 2029

**Short date**

Short date sample: 10/19/2004

Short date format: M/d/yyyy

Date separator: /

**Long date**

Long date sample: Tuesday, October 19, 2004

Long date format: dddd, MMMM dd, yyyy

About Date Formats

OK Cancel Apply Help

### Note

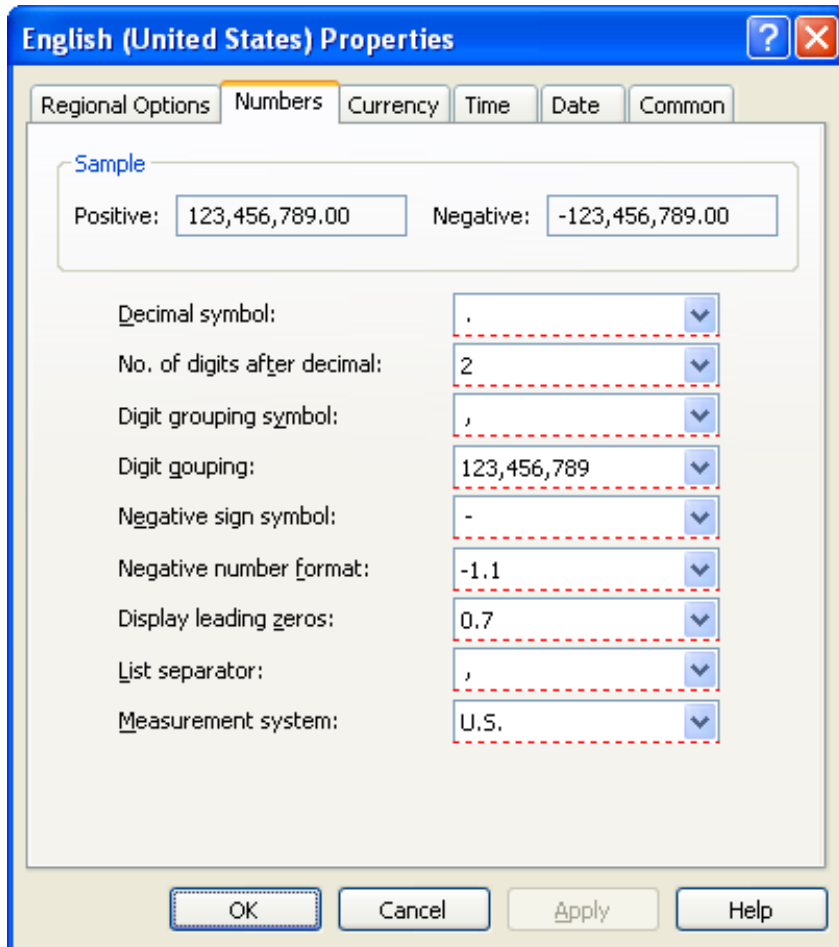
This page uses [property underlining](#) to control which settings are applied. By default all settings are disabled (red).

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Regional Options - Numbers

"Regional Options - Numbers" affects how the locale specified on the "[Regional Options](#)" tab will display various numeric value types.



### Note

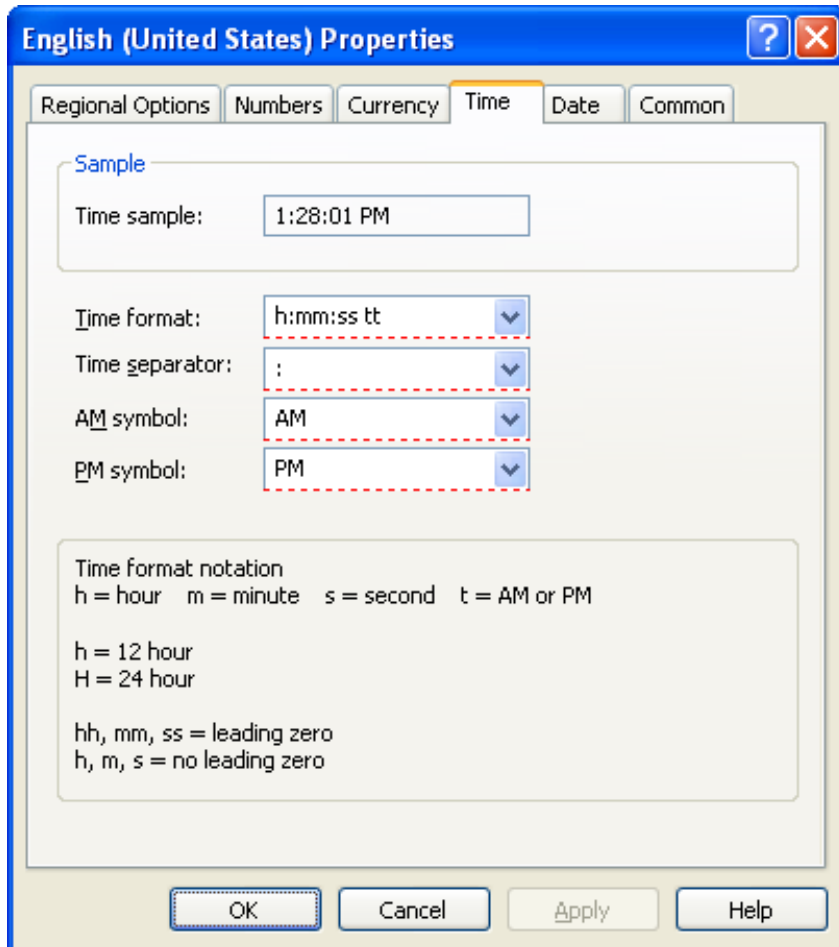
This page uses [property underlining](#) to control which settings are applied. By default all settings are disabled (red).

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Regional Options - Time

"Regional Options - Time " affects how the locale specified on the "[Regional Options](#)" tab will display various time value types.



### Note

This page uses [property underlining](#) to control which settings are applied. By default all settings are disabled (red).

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Registry

---

Group Policy extension for configuration of [Registry](#) settings.

### Note

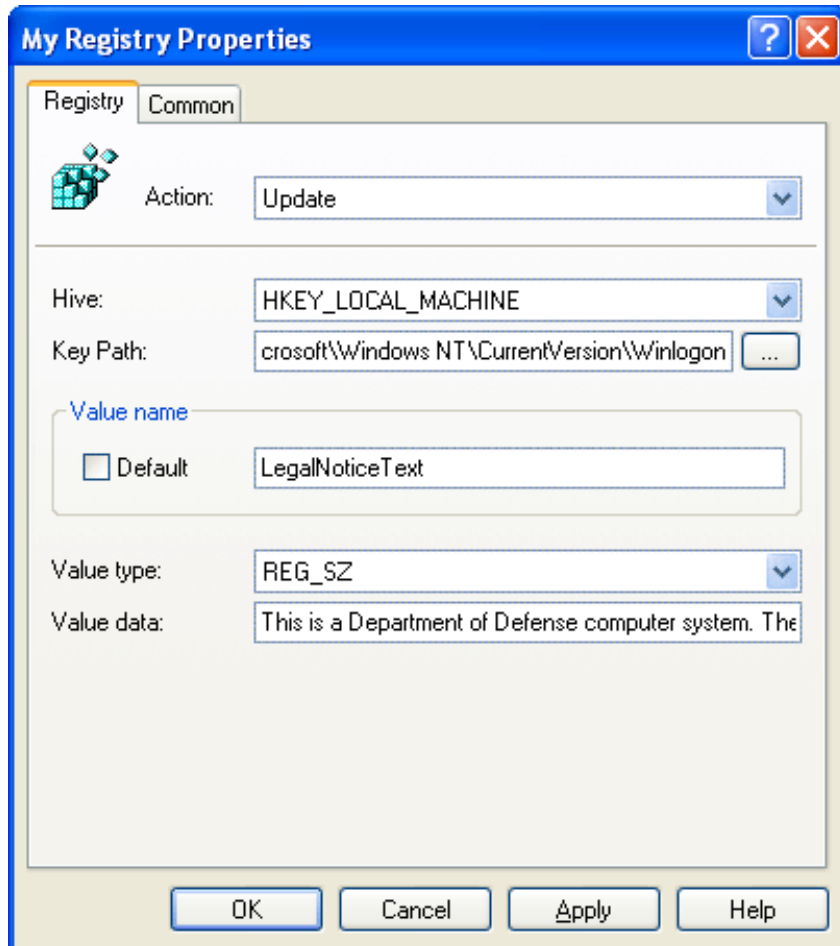
The Registry extension is a [promotional component](#) of PolicyMaker, and as such does not require a license key.

---

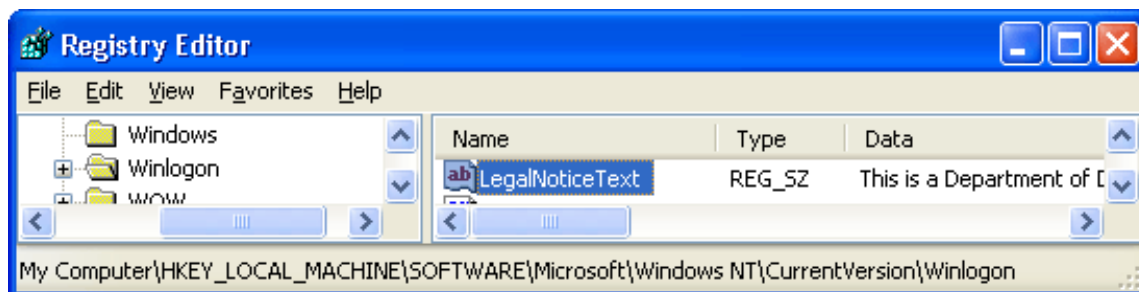
© 2005 DesktopStandard Corporation. All Rights Reserved.

## Registry

"Registry" is a configuration item that is used to change Windows Registry settings.



The following example shows a typical registry entry as shown in "regedit.exe". A "hive" refers to the main part of the registry (i.e. HKEY\_LOCAL\_MACHINE). A "key" refers to a "folder", contained within a hive. The path to the selected key (shown with an open folder in the left pane) is shown in the status bar, starting after the hive. A registry "value" consists of a "value name", "value type", and "value data" which correspond to the columns "Name", "Type", and "Data" in the right pane below. Each registry key can have a "default" value. This value is simply an unnamed value that is represented in regedit.exe with the name "(default)".



Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by Key name if no Value is specified (i.e. "Value name" empty and "Default" not selected ), otherwise matching is performed by Value name.

- Create



- Key Path only - creates the Key, if it does not already exist.
- Value - creates the Value (name/type/data) in the Key Path, if the Value does not already exist. If the Value exists, the item is skipped.
- Replace
  - Key Path only - deletes the Key, and all of its values and subkeys, if the Key already exists. The Key is then created.
  - Value - deletes the Value if it already exists. The Value is then created in the Key.
- Update
  - Key Path only - same as Create.
  - Value - same as Replace.
- Delete
  - Key Path only - deletes the Key, and all of its values and subkeys, if the Key already exists.
  - Value - deletes the Value if it already exists.

#### Hive:

The root location of the desired setting. In computer policy, the default option is HKEY\_LOCAL\_MACHINE (which includes HKEY\_CLASSES\_ROOT). In user policy, the default option is HKEY\_CURRENT\_USER.

- HKEY\_CLASSES\_ROOT - alias into HKEY\_LOCAL\_MACHINE\Software\Classes
- HKEY\_CURRENT\_USER - alias into HKEY\_USERS\{logged-on user's specific hive}
- HKEY\_LOCAL\_MACHINE - generally settings that affect all users of the machine
- HKEY\_USERS - generally settings that affect individual users
- HKEY\_CURRENT\_CONFIG - alias into HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Hardware Profiles\Current

#### Key Path:

**Required setting.** The path to the desired registry key. This required value should not contain a trailing slash and should not be quoted. Key paths are not text case sensitive. The browse button launches the [Registry Browser](#). [Variables](#) may be used in this setting.

#### Value name:

The name of the desired registry value. If this is empty (and "Default" is not selected) the registry item targets a key and not a value. Value names are not text case sensitive. [Variables](#) may be used in this setting.

#### Default:

Select this option to specify the default (i.e. unnamed) value for the specified registry key.

#### Value type:

This setting is required when a value name is specified, and is disabled in delete mode.

#### Value data:

This setting is disabled in delete mode. Possible formats include the following:

- REG\_SZ
  - text data in any format is allowed
  - empty values are valid
  - [Variables](#) may be used in this setting.
- REG\_EXPAND\_SZ
  - text data in any format is allowed
  - empty values are valid

- [Variables](#) may be used in this setting.
- Use the unresolved variable syntax to set an unresolved value
  - example: to set a value that contains "%ProgramFiles%\DesktopStandard", use "%<ProgramFiles>%\DesktopStandard". This syntax prevents resolution of the %ProgramFiles% environment variable - and PolicyMaker replaces the %<...>% with %...% before comparison.

- REG\_MULTI\_SZ

- this data type is a list of strings with NULL separators.
- text data in any format is allowed.
- an empty value is valid; leave the entire field empty to denote an empty value.
- [Variables](#) may be used in this setting.
- setting multiple values is supported; use returns ("Enter" key) to separate values.
- PolicyMaker replaces all of the values with the contents of the "Value data" field.

 Note

The registry editor (regedit.exe) shows NULL separators as spaces in the "Data" column and as returns in the "Value data" field on the "Edit Multi-String" dialog. Similarly, PolicyMaker shows NULL separators as spaces in the "Value Data" column and as returns in the "Value data" field.

 Note

The registry editor (regedit.exe) does not support empty strings embedded in a multi-value string list. Therefore, PolicyMaker will automatically disregard all empty lines (returns) entered into the "Value data" field. Only the valid (non-empty) values will be shown on subsequent visits to the property page.

- REG\_DWORD

- a single 32-bit numeric value
- an empty value is interpreted as a zero (0)
- entered as hexadecimal (00000000 - FFFFFFFF) or decimal (0 - 4294967295)

- REG\_BINARY

- a stream of hexadecimal bytes
- an empty value is valid and will result in a zero length buffer
- bytes entered Least Significant Byte (LSB) to the left
- a value with an odd number of characters will be padded on the right with a "0"
  - example: 30d692f4eb1 becomes 30d692f4eb10 when processed
- only valid hexadecimal characters may be typed
- values may be pasted from ".reg" (regedit.exe) files, including commas:
  - example: 30,d6,92,f4,eb,10 becomes 30d692f4eb10 when applied

---

 Note

By default this item will have access to all objects with the SYSTEM Access Control Entry (ACE). To change this item to run with end-user permissions (in user policy), change the security context on the [common tab](#).

 Important

Deleting or replacing a registry [key](#) can be extremely damaging if the wrong key value is provided or if the behavior of this feature is not understood. When a key is deleted (or replaced), all of its children, including all subkeys (and their subkeys etc.) as well as all of the values of all such keys, will be deleted. It is not possible to delete a registry key otherwise.

---



Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Scheduled Tasks

---

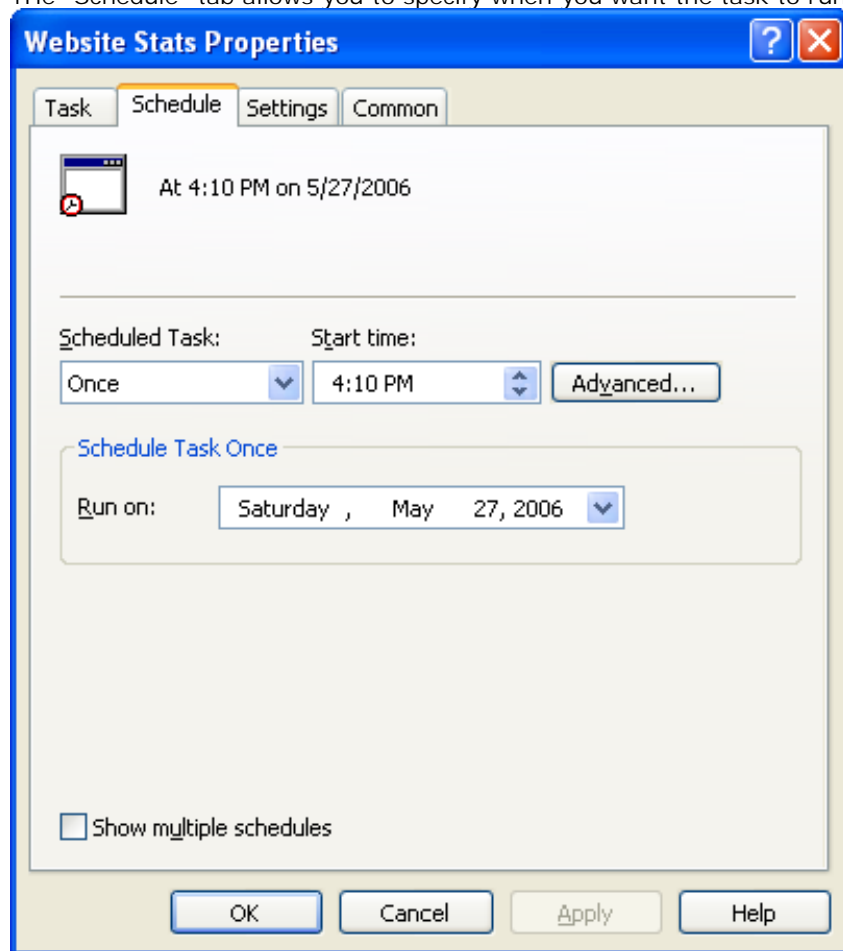
Group Policy extension for configuration of [Scheduled Tasks](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Scheduled Tasks - Schedule

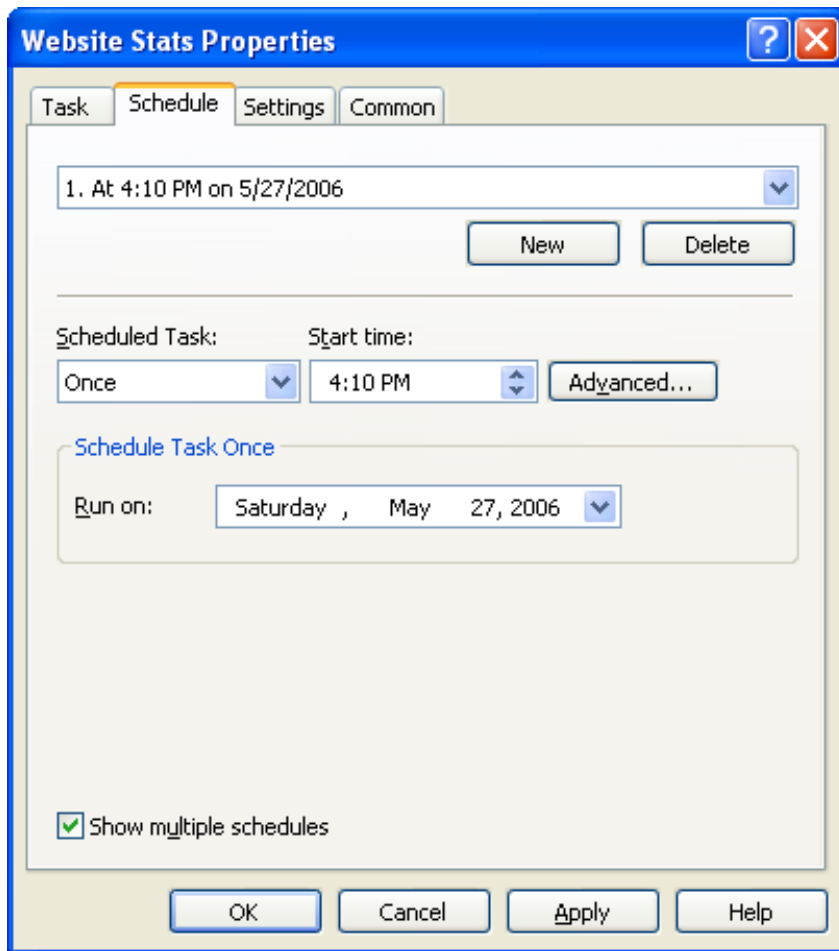
The "Schedule" tab allows you to specify when you want the task to run.



This page controls the scheduled triggers under which the task will run and supports all options available in the control panel's Scheduled Tasks applet.

Show multiple schedules

Select this option to enable multiple schedule trigger capability (shown below).



#### New

Adds a new schedule trigger to the task.

#### Delete

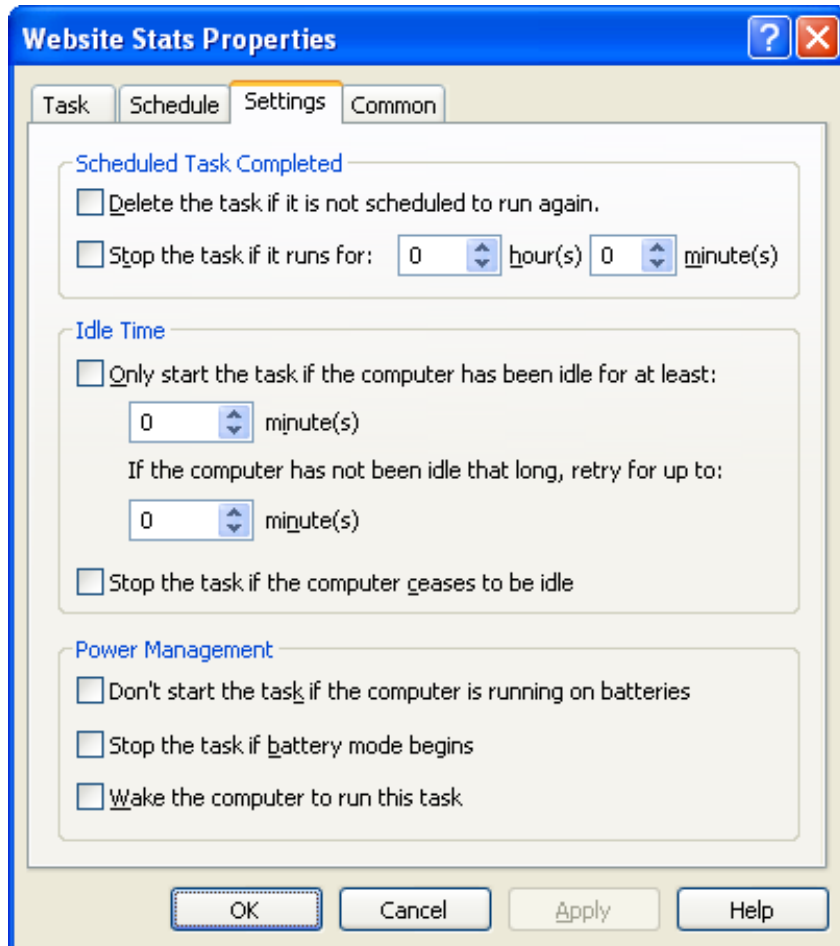
Removes the selected schedule trigger from the task.

#### Scheduled Task

The properties of each selected schedule trigger can be specified below this heading.

## Scheduled Tasks - Settings

"Scheduled Tasks - Settings" allows you to set parameters for a given task.



### Scheduled Task Completed:

Allows you to control the behavior of the task upon completion.

Delete the task if it is not scheduled to run again  
If the task is set to run a single time, it will delete itself upon completion.

Stop the task if it runs for: # hour(s) # minute(s)  
Specify an amount of time to allow a given task to run before execution is stopped. This can prevent a task from running in an infinite loop.

### Idle Time:

This group of settings controls how a task will run if the computer is being used.

Only start the task if the computer has been idle for at least  
If the computer has been idle for a specified time, run the task.

If the computer has not been idle that long, retry for up to  
Keep checking the computer's period of inactivity until it reaches a maximum time limit.

Stop the task if the computer ceases to be idle  
If the computer becomes active, stop running the specified task.

### Power Management:

Allows you to control how a task will be treated under different power conditions.

Don't start the task if the computer is running on batteries  
If the computer is using an external power source, run the task.

Stop the task if battery mode begins

When a computer's power source switches to battery mode, for instance when a power surge or failure occurs, this task will stop executing.

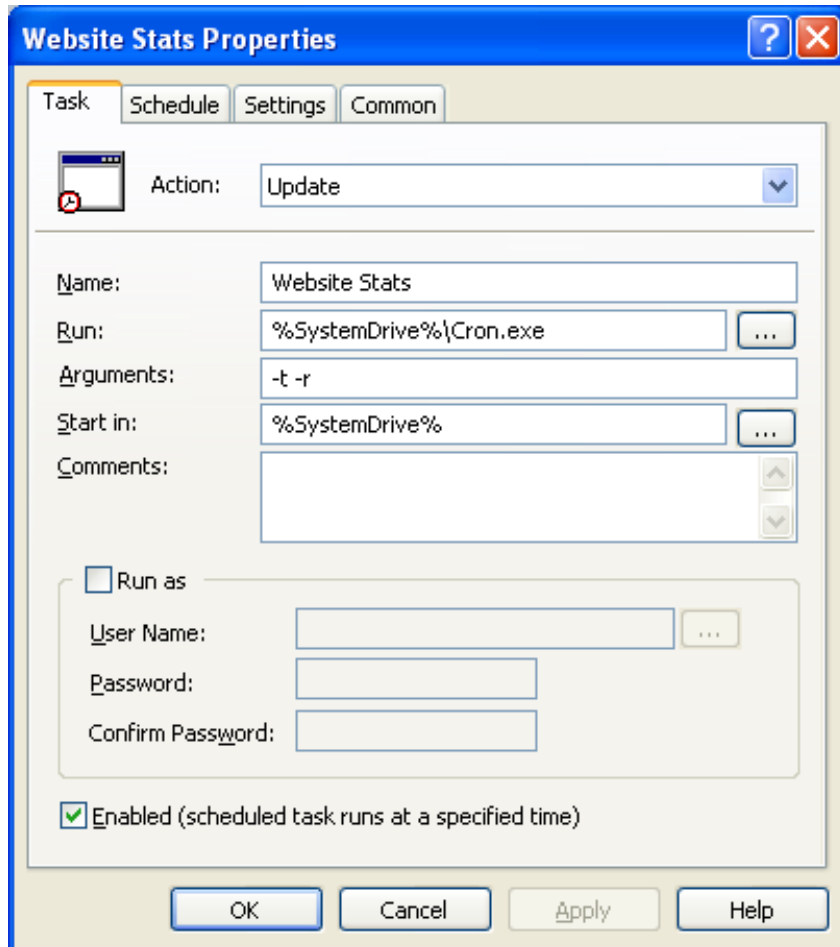
Wake the computer to run this task

If a power-saving feature is active on the computer when the task is set to run, return to full power mode and execute the task.



## Scheduled Tasks - Task

"Scheduled Tasks" is a configuration item that is used to managed tasks that appear within the Scheduled Tasks control panel applet.



This policy not only provides complete control over the options available to an administrator within the control panel, but also provides options that are not exposed within the control panel applet. It is important to note that Scheduled Tasks are not related to the "AT" task scheduler, which does not produce tasks that are manageable within the Scheduled Tasks applet.

Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by task Name.

- Create - creates the task, if it does not already exist.
- Replace - same as Create except the task is deleted first if it exists.
- Update - if the task does not exist, it will be created. Settings are then applied to the task and schedules are replaced in full.
- Delete - delete the task if it exists.

Name:

**Required setting.** The name of the task. [Variables](#) may be used in this setting.

Run:

**Required setting (except in delete mode).** The command line that the task scheduler will execute. [Variables](#) may be used in this setting.

Arguments:

Command-line arguments to be passed to the task. [Variables](#) may be used in this setting.

**Start in:**

The working directory for the task when it is launched. The path should not be quoted or have a trailing slash. The browse button launches the [Folder Browser](#). [Variables](#) may be used in this setting.

**Comments:**

A description of the task. [Variables](#) may be used in this setting.

**Run as:**

This setting is interpreted differently for user policy and computer policy. Specifying a "Run as" account indicates that the task will be run under the security context of the specified account, and will have the ability to run according to its schedule whether or not the user is logged on to the computer.

If "Run as" is not selected, the following rules apply:

Computer policy

The task is executed in the security context of the Task Scheduler service, normally SYSTEM.



**Tip**

This policy can be used to wake computers that are in standby mode at a specified time. To do this schedule any task at the desired wake time and ensure that computer policy has an opportunity to be processed before the wake time and before the machine goes into standby.

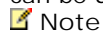
User policy

The task is executed in the security context of the logged-on user, and the task will be launched only if the user is logged on to the computer. A running task may continue to run once the user logs off.



**Tip**

Processes initiated from a logon script are terminated by Windows once the logon script completes. This policy can be used to launch a process upon user logon without having to run the process from a logon script.



**Note**

The Task Scheduler service does not support running tasks in this mode for Windows 2000 or Windows XP Gold. Windows XP Service Pack 1 and later, and Windows 2003 and later support this mode.

**Username:**

The username of the account under which the task will be executed. [Variables](#) may be used in this setting. The following formats are acceptable:

[MyUsername](#)  
[MyDomain\MyUsername](#)  
[MyComputer\MyUsername](#)

**Password:**

The password for the specified Username.

**Password Security**

The password is encrypted before being saved into the configuration XML. The password is decrypted by the Scheduled Tasks client side extension so that it may be applied to configuring the user. It is important to note that it is technically possible, although difficult, to recover the password from the settings file.

**Enabled:**

Configures the task as an enabled task. If not checked the task will still be configured but will not execute.

---



**Note**

The Task Scheduler service must be running for tasks to execute. [Services](#) policy may be used to ensure that the service is running. Scheduled tasks are not visible to restricted users.

---



**Filter**

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Services

---

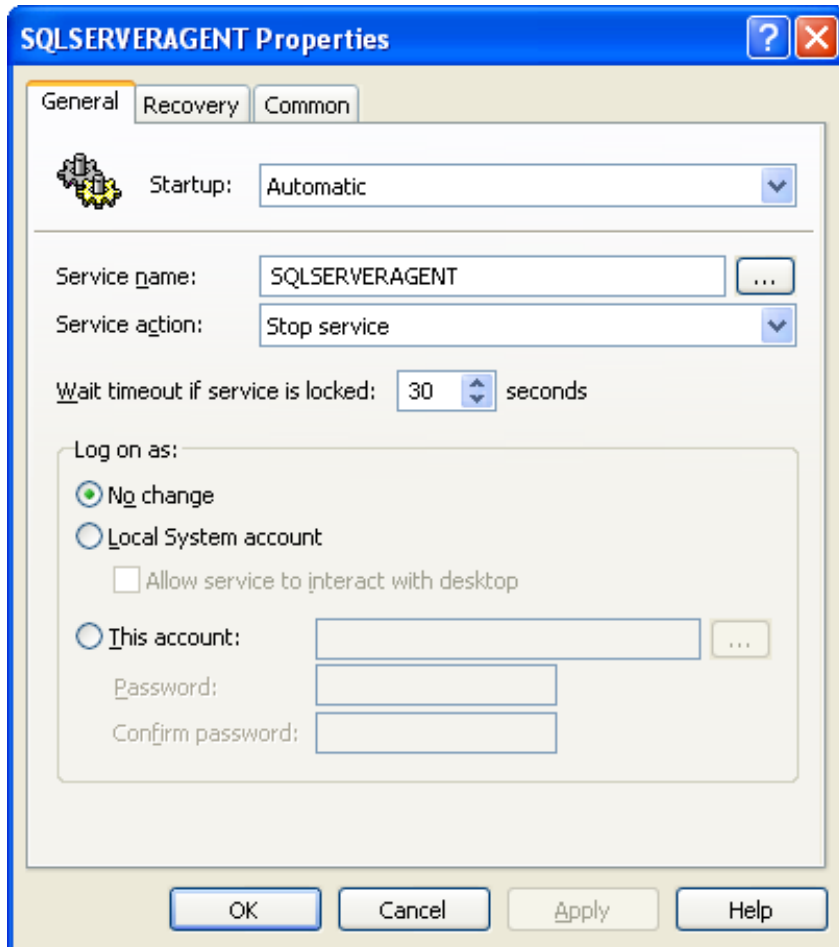
Group Policy extension for configuration of [Services](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Service

"Service" is a configuration item that is used to manage operating system services, providing the ability to configure all options available in the Services administrative tools applet.



Service policy does not implement standard PolicyMaker [action modes](#), as services must already exist. Matching is performed by the Service name. In general, each specified setting is applied to the service if the service does not already have that setting enabled. This minimizes interaction with the service.

### Startup:

If other than 'No change' is applied, the service startup mode is updated if required. This setting does not require a service restart to take effect.

### Service name:

**Required setting.** The unique name of the service. The browse button launches the [Service Browser](#). [Variables](#) may be used in this setting.

### Service action:

If other than 'No change' is applied, the final service state will be set to started or stopped as specified.

- No change - do not change the service running status.
- Start service - if not already started, start the service.
- Stop service - if not already stopped, stop the service.
- Restart service - stop the service if running, and then start it.
- Restart service if required - if a configuration action requires a restart, the service will be started or restarted.

### Notes

Service start/stop occurs after all other configuration for the policy, and as such a service cannot be started or

restarted if the Startup mode is set to disabled.

Wait timeout if service is locked:

There are two situations that require the use of a wait timeout. Both may occur in the same policy depending on the situation. If the timeout value is exceeded, and error is returned by the policy.

#### Database Locking

If the service database is locked and the policy must perform configuration of the service, the policy will wait for access up to the timeout period specified. The configuration that requires this access includes 'Log on as' and 'Startup' mode changes only. Startup, stop and [Recovery tab](#) options do not require the policy to wait on a lock.

#### Service Locking

A service that is in transition will be waited on for the 'Wait timeout...' specified, both for a stop transition and a start transition - whether initiated by the policy or externally. The total timeout may therefore be twice the specified time in a restart situation.

Logon as:

The account under which the service will run. If 'No change' is specified, the service account will not be configured.

Most services run as 'Local System'. Local System services may interact with the desktop.

Other accounts, including 'NT AUTHORITY\NetworkService' and 'NT AUTHORITY\LocalService' may be selected using the [User Browser](#) or entered directly. Generally an account name that is local to multiple computers should be entered as ".\Username" - which indicates that the account must be resolved from the local computer's domain. If an account name other than an 'NT AUTHORITY' is specified, the password for the account is required.

#### Password Security

The password is encrypted before being saved into the configuration XML. The password is decrypted by the Services client side extension so that it may be applied to configuring the service. It is important to note that it is technically possible, although difficult, to recover the password from the settings file.

---

 Filter

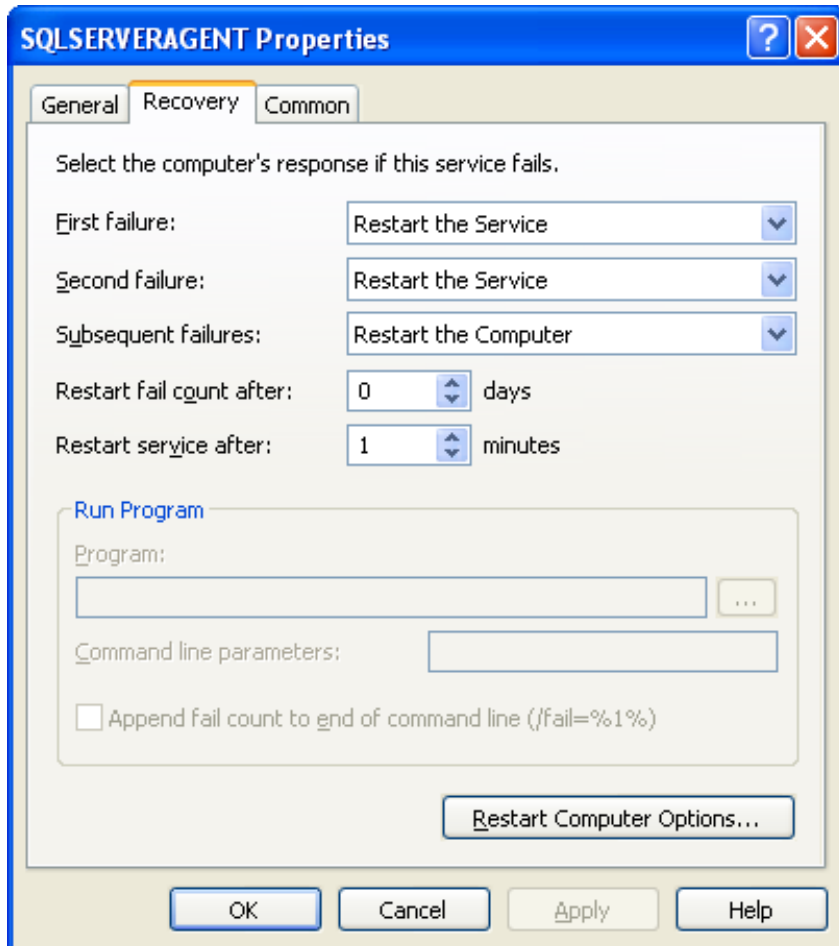
Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Services - Recovery

"Services - Recovery" controls the various failover modes and settings available for a service.



The screenshot shows the "SQLSERVERAGENT Properties" dialog box with the "Recovery" tab selected. The dialog has three tabs: "General", "Recovery", and "Common". The "Recovery" tab contains the following settings:

- Select the computer's response if this service fails.**
- First failure:** Restart the Service
- Second failure:** Restart the Service
- Subsequent failures:** Restart the Computer
- Restart fail count after:** 0 days
- Restart service after:** 1 minutes

Below these settings is a section titled "Run Program" with the following options:

- Program:** (Empty text box with a browse button "...")
- Command line parameters:** (Empty text box)
- Append fail count to end of command line (/fail=%1%)

At the bottom of the "Run Program" section is a button labeled "Restart Computer Options...". At the very bottom of the dialog are the standard "OK", "Cancel", "Apply", and "Help" buttons.

These settings operate in the same manner the corresponding settings in the Services administrative tools applet.

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

## Shortcuts

---

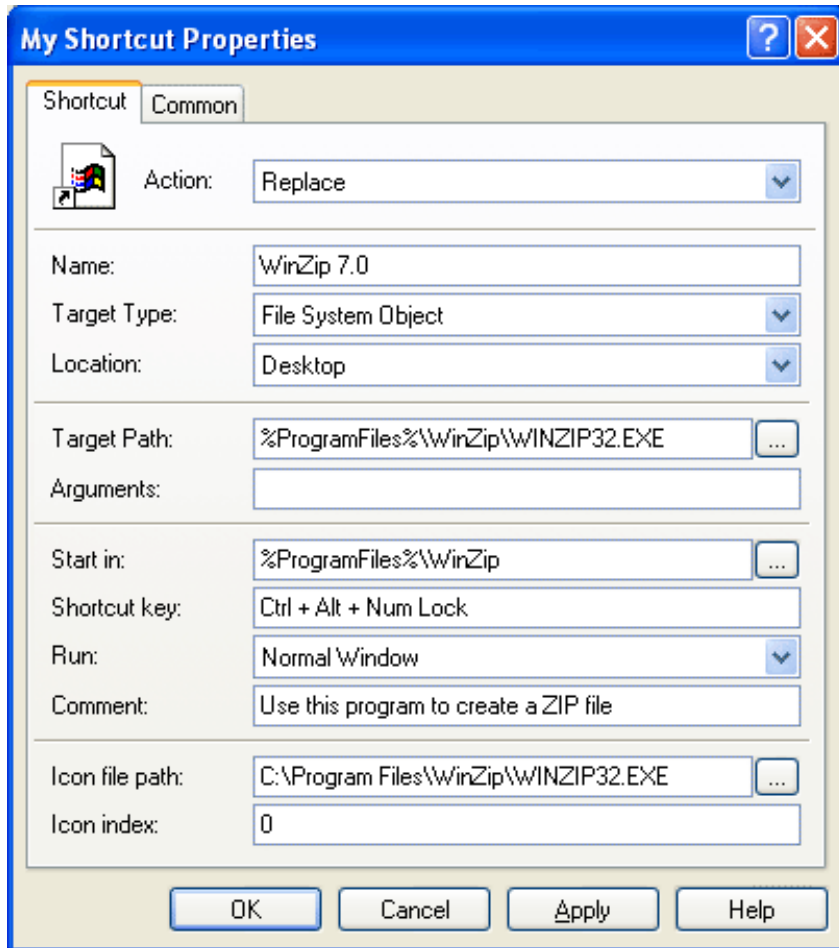
Group Policy extension for configuration of [Shortcuts](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Shortcut

"Shortcut" is a configuration item that is used to configure a shortcut to a file system object, shell object or URL.



### ◆ Important Note on Mapped Drives

When configuring a shortcut that uses a mapped drive letter in any parameter, ensure that (1) the item is in user policy, (2) the drive letter exists prior to shortcut policy execution, and (3) that the policy is set to run in the logged-on user's security context (on the [Common Tab](#)). SYSTEM context does not have access to drive maps, which exist only for users. If this is set incorrectly the shortcut may configure successfully but may have a truncated or otherwise altered path.

#### Action:

One of the standard PolicyMaker [action modes](#). Matching is performed by a combination of Name, Type (extension) and Location.

- Create - creates the shortcut, if it does not already exist.
- Replace - delete the shortcut, if it exists, and create it regardless.
- Update - if the shortcut does not exist, it will be created. If it exists, all parameters will be updated.
- Delete - delete the shortcut, if it exists.

#### Name:

**Required setting.** The display name of the shortcut. The value should not be quoted. If a specified folder does not exist, it will be created. [Variables](#) may be used in this setting.

<Specify full path>

If "<Specify full path>" is chosen in the "Location" field, this setting must contain the full path to the folder that will contain the shortcut, as well as the shortcut name. For example, the following creates a shortcut named



"My DesktopStandard Shortcut" in the folder "%ProgramFilesDir%\DesktopStandard":

<Specify full path>  
[%ProgramFilesDir%\DesktopStandard\My DesktopStandard Shortcut](#)

If the path specified is not fully qualified, the shortcut will be placed into the current directory of the CSE, which would normally be the system directory.

#### Sub-locations

If a subfolder of a standard location is desired, the subfolder may be prefixed to this setting as well. For example, the following creates a shortcut named "My DesktopStandard Shortcut" in the "DesktopStandard" subfolder of the "Explorer Favorites" location:

[Explorer Favorites]  
[DesktopStandard\My DesktopStandard Shortcut](#)

#### Target Type:

This setting controls what browse options are available for the "Target Path" setting. There are three basic types of shortcuts supported by Windows.

- File System Object

An object that can be addressed using a traditional Windows path. This includes a file, folder, drive, share, document, computers, etc. With this type selected, the "Target Path" browse button enables a file system browse window and paths can optionally be entered manually.

- URL

An Internet-style URL that could be provided directly to Internet Explorer, including HTTP, HTTPS, FTP, etc. With this type selected, the "Target Path" browse button is disabled. The URL must be typed or pasted into the path.

- Shell Object

Any object addressable within the Windows shell, including printers, desktop items, control panel items, special folders, as well as files, folders, shares, computers, network resources, etc. With this item selected, the "Target Path" browse button enables a shell object browser and the field itself is disabled for manual entry.

#### Location:

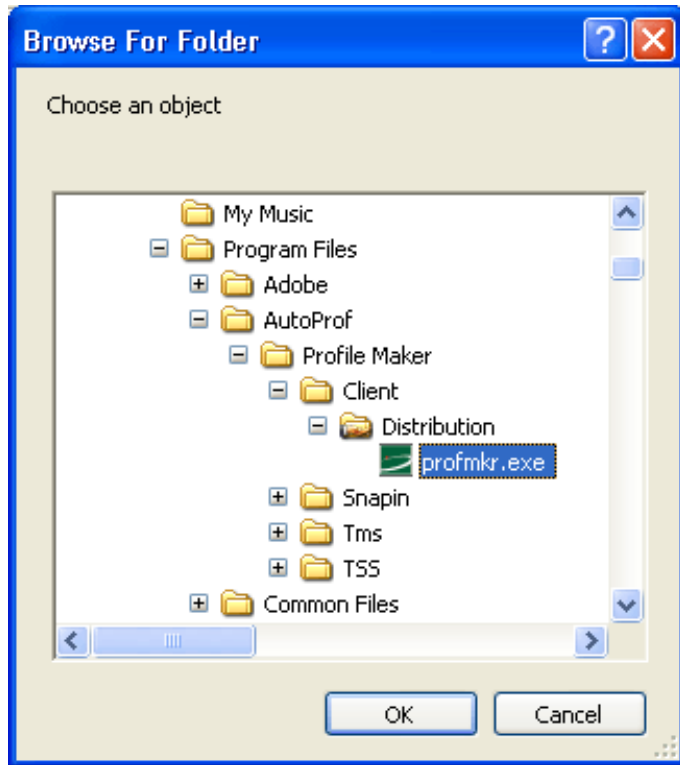
One of a list of standard locations for a shortcut to be placed. "All Users" locations are relative to the "All Users" directory, others are relative to the logged-on user.

#### Target path:

The setting is the path to the item to which the shortcut refers. The following are examples of different types of target items. The path should not be quoted. The browse button launches the [Shell Object Browser](#). [Variables](#) may be used in this setting when not using the "Shell Objects" Target Type.

#### File System Objects

These types of objects can be browsed by selecting the "..." button to the right of this field, or entered manually. Some selectable objects are not file system objects and will return an error if selected. If a shortcut is selected from the browser, the target object is returned, not the shortcut itself.



Examples include:

- Path to a local folder

`%<ProgramFiles>%\DesktopStandard\ProfileMaker`

- Path to a local executable file

`%<ProgramFiles>%\DesktopStandard\ProfileMaker\Client\Distribution\profmkr.exe`

- Path to a local help document

`%<ProgramFiles>%\DesktopStandard\ProfileMaker\Snapin\profmkr.chm`

- UNC path to a network share

`\\MyServer\Netlogon`

- Name of a network or local computer

`\\MyServer`

- Shared printer on remote machine

`\\Server\HP LaserJet 4050 Series PS`

- Drive Letter

`H:`

#### ◆ Variables in Target Path

Note that variables may be placed into the target path. Any variable in resolved syntax, such as `%ProgramFiles%`, will be resolved by PolicyMaker before the shortcut is created. If you desire to place an unresolved variable into the target (or other) path, you must use the [unresolved variable](#) syntax, specifically `%<ProgramFiles>%` using the previous example. However, unresolved variables must be variables that are

known to the user's environment (such as %ProgramFiles%). This is not the case with many PolicyMaker variables which are generated for internal use but not set as persistent environment variables by default.

#### URL

These types of objects must be entered manually, as the address would appear in the Internet Explorer address field. Examples include:

- URL to a web page (defaults to IE web page icon, or website icon)

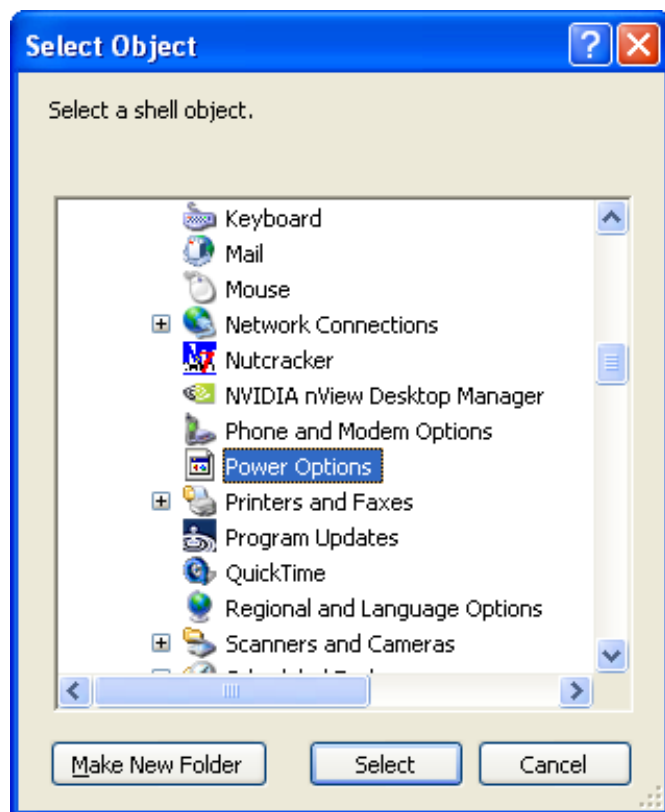
<http://www.desktopstandard.com>

- URL to an FTP site (defaults to IE FTP icon)

<ftp://ftp.desktopstandard.com>

#### Shell Objects

These types of objects may only be browsed by selecting the "..." button to the right of this field. If a shortcut is selected from the browser, the target object is returned, not the shortcut itself.



#### Note

When an object is selected, the display name of the object is presented and the field is disabled. Examples include:

- Shell path to the Control Panel

[Desktop/My Computer/Control Panel](#)

- Shell path to a specific printer

[Desktop/My Computer/Control Panel/Printers/HP LaserJet 4050 Series PS](#)

#### Arguments:

Optional setting. Argument(s) for the command line specified by the "Target file path". [Variables](#) may be used in

this setting.

Start in:

Optional setting. Working directory, where files required by the Target item exist. The path should not be quoted or have a trailing slash. The browse button launches the [Folder Browser](#). [Variables](#) may be used in this setting.

Shortcut key:

Creates a keyboard method to launch the shortcut. Function keys, including <F1>...<F12>, <CTRL>+<ALT>+<key>, <NUM key> and more, can be programmed to launch the shortcut on the target desktop.

Run:

Specifies how the window should display when opened using the shortcut. Choices are: Minimized, Maximized or Normal Window.

Comment:

The tool tip text that appears when the mouse is hovered over a shortcut. [Variables](#) may be used in this setting.

Icon file path:

The fully qualified path to an icon file. If this value is not set, the "Icon index" setting is ignored and Windows chooses the default icon for the item based on its type (as if the icon had been made by using the mouse to drag a shortcut to the "Target" object). The path should not be quoted. The browse button launches the [Icon Browser](#). [Variables](#) may be used in this setting.



Icon index:

The zero-based index of the desired icon in the file specified by "Icon file path". If no icon file path is specified, this value is ignored. An icon can be specified for any type of shortcut. This setting is also filled in by the Icon Browser.

---

#### Notes

This item will reset the "Read Only" attribute of any shortcut that it needs to alter.

If a shortcut is selected in the browser, its target item will be selected. In other words, it is not possible to specify a shortcut to a shortcut using the browser.

By default this item will run with end-user permissions (in user policy), to give the item access to all objects with the SYSTEM Access Control Entry (ACE), change the security context on the [common tab](#).

---

#### Filter

Apply a [filter](#) to this item to prevent it from executing for specified users, computers or other conditions.

## Start Menu

---

Group Policy extension for configuration of [Start Menu](#) settings.

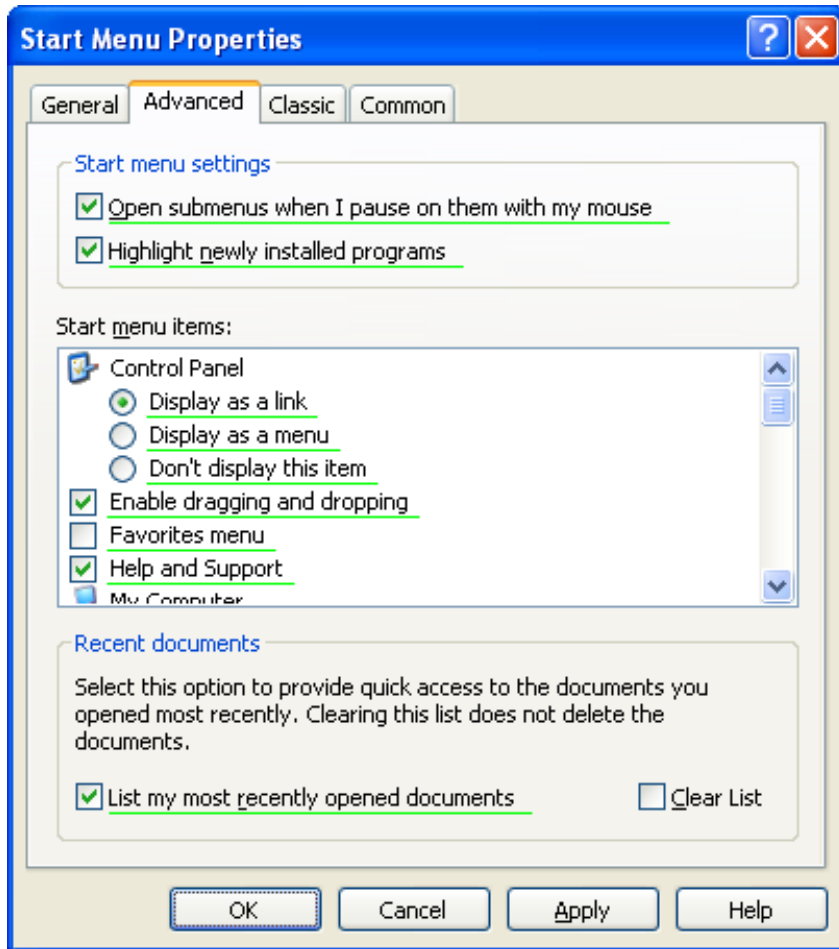
---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Start Menu - Advanced

---

"Start Menu - Advanced" is a group of settings that control the Start Menu and Programs menu.



---

### Note

This page uses [property underlining](#) to control which settings are applied. By default all settings are enabled (green).

---

### Filter

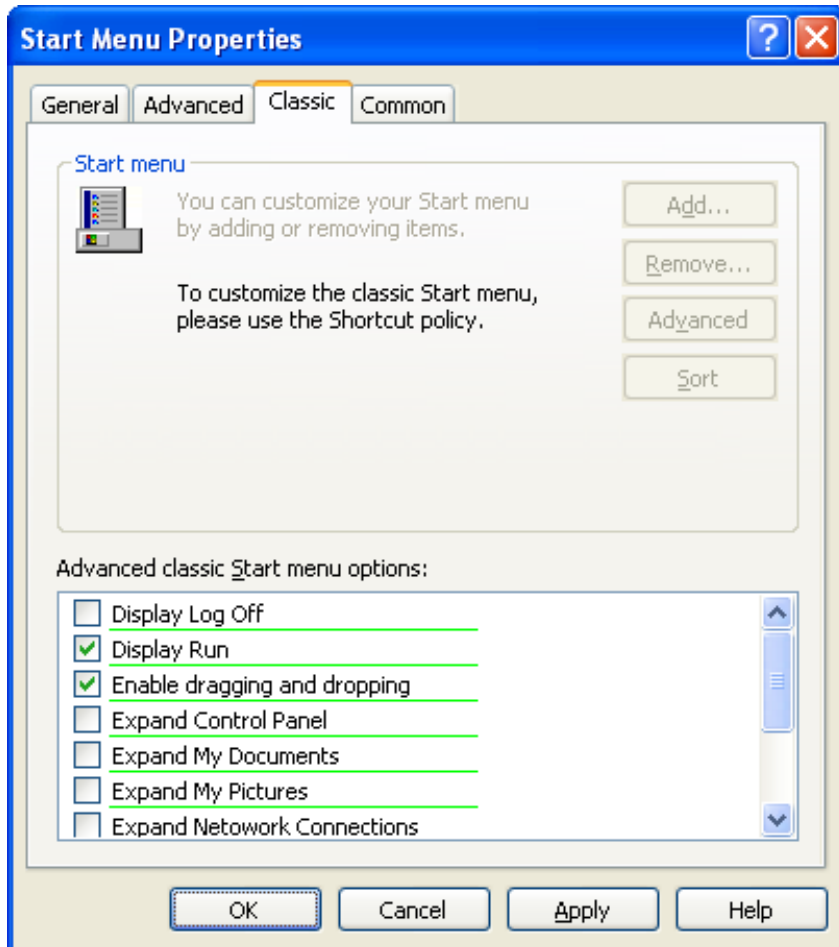
Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Start Menu - Classic

---

"Start Menu - Classic" settings control how the Start Menu looks when the Classic Start Menu is presented (which is always the case on Windows 2000).



---

### Note

This page uses [property underlining](#) to control which settings are applied. By default all settings are enabled (green).

---

### Filter

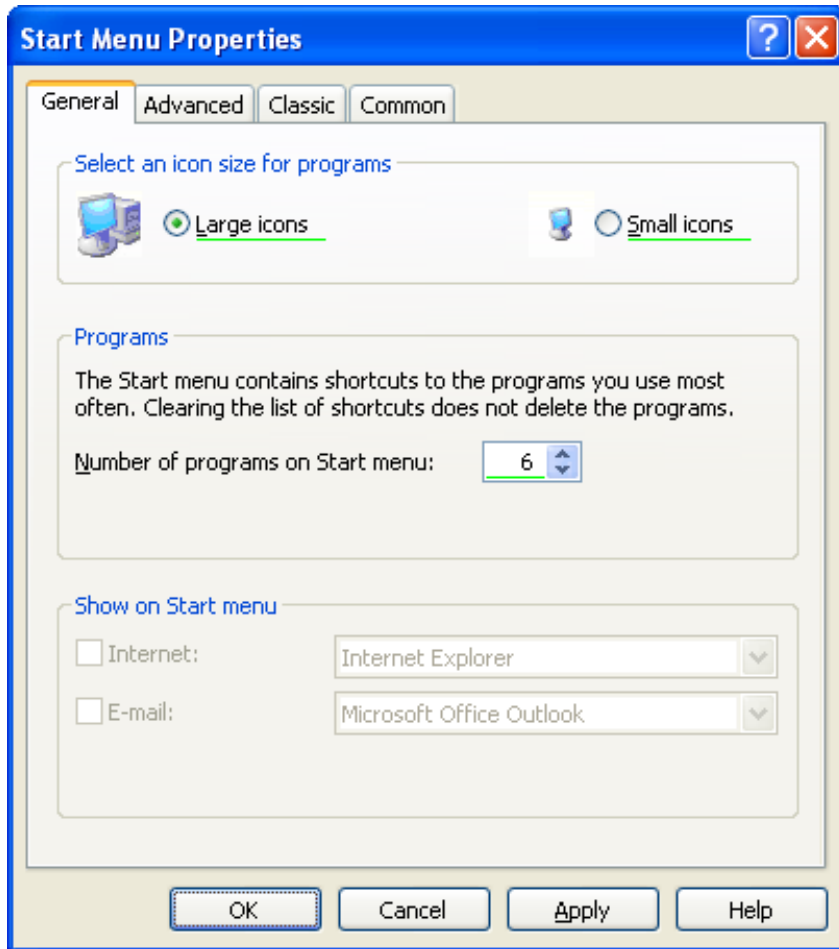
Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

## Start Menu

---

"Start Menu" is a configuration item for managing settings that control the look and feel of the Start Menu.



---

### Note

This page uses [property underlining](#) to control which settings are applied. By default all settings are enabled (green).

---

### Filter

Apply a [filter](#) to this item to prevent it from executing for specified computers or other conditions.

---

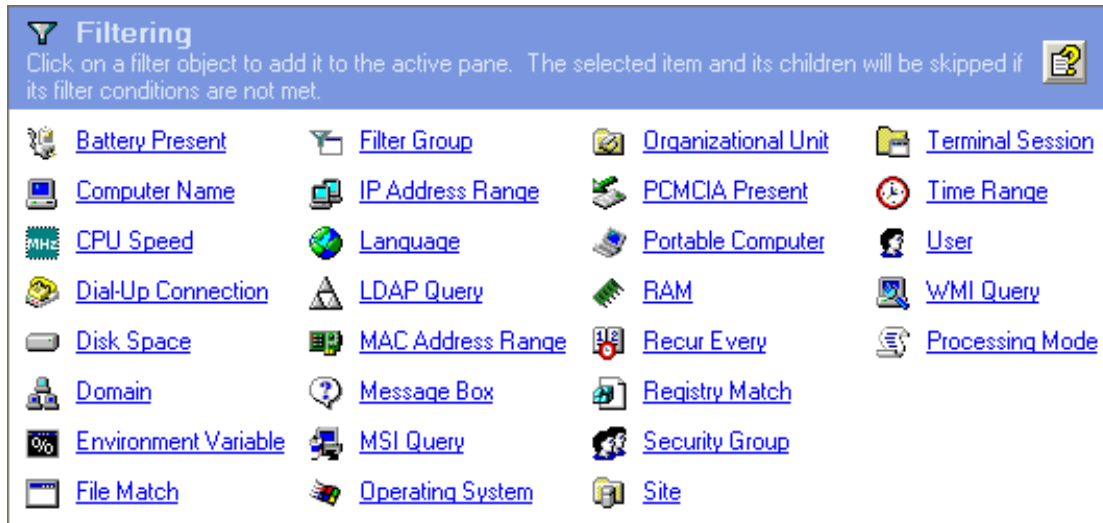


## Filters

Filters allow an administrator to selectively exclude a policy setting during processing by the client side extension. Filters are always evaluated prior to action modes. As with a disabled item, if a filter excludes an item none of its children will be processed.

### Filter Header

Click on an item below to see a full description of its functionality.



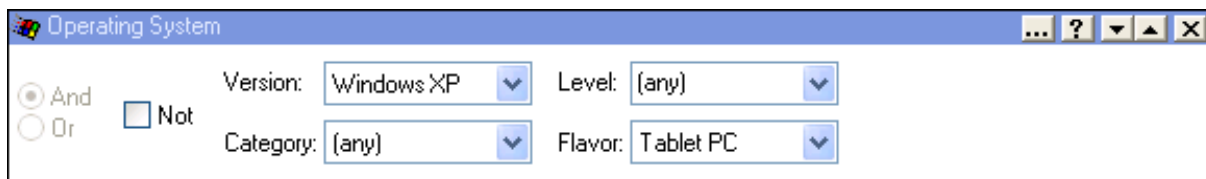
### How to Apply a Filter

To add a filter, click on a filter type in the header. For this example, Operating System has been selected. Once selected, the filter appears in the Active Filters view below the header, as shown below:

### Active Filters Frame

The frame below the filter header shows all of the filters in effect for the selected item.

By selecting {Windows XP, (any), Tablet PC} (below) we have ensured that the selected item will only execute on Tablet PC computers.



### How to Document Filters

Each filter can be named and given a description. These values are used in [trace output](#), [settings reports](#) and [RSOP reports](#). To set these values, click the "..." in the upper right corner. A filter's name is shown in the filter's title bar following the filter type.

### How to Obtain the Filter Result in a Variable

Each filter returns a true/false value. That value is captured in a variable that is automatically generated from the filter's name. If the filter is unnamed then no variable is generated.

### How to Obtain Help on a Filter

To obtain help on a filter, click the "?" in the upper right corner of the filter.

### How to Move a Filter

Filters are automatically moved with a configuration item. Filters can also be moved individually, both within a single item and from one item to another.

Filters can be ordered within the Active Filters frame by drag and drop (grab the title bar) or by moving filters up/down via the arrows in the upper right corner of the filters. Filters may also be moved or copied to the Active Filters frame of another open filters window.

### How to Delete a Filter

To remove a filter from the view, click the "x" in the upper right corner, or double-click the icon in the upper left

corner of the filter.

#### Disabled Filters

Filter selections will be disabled if they are not applicable to the current user/computer policy context.

#### Filter Inheritance

If filters applied to a parent item evaluates to "false", then the collection and all of its children will be skipped. If the item's filter evaluates to "true", the item will perform its configuration and then the item's children will be evaluated in the same manner.

#### The "Not" Option

Each individual filter has a "Not" checkbox. This option negates the result of the calculation performed by the particular filter. With this option set, a filter that would otherwise evaluate to "true" will evaluate to "false".

#### Multiple Filters

Filters may be combined without limitation on a single item. There is no limit to the number of filters allowed.

#### And, Or and () Options

When multiple filters are applied, you have the option to choose the logical relationship between the filters. The default relationship between filter items is "And". Using the Boolean operators "And" and "Or" you can generate complex logical conditions that the item must satisfy before being executed. Using [filter groups](#) you can create parenthetical expressions, with any level of nesting.

#### ◆ Processing

All filters under an item will be evaluated before a decision is made to execute or bypass that item. Order of execution is sequential from top to bottom. All filters in an item are always processed, unless a failure occurs in one of them. The [security context](#) for most filters is SYSTEM. See individual filter documentation for exceptions. Filter processing is not affected by the security context setting on the item's common tab (PolicyMaker Standard Edition and PolicyMaker Registry Extension).

## Battery Present

---



This filter returns true if there is at least one battery in the computer.

---

### Not:

Reverses the results of this filter. With this option selected this filter returns true only if there is no battery in the computer.

---

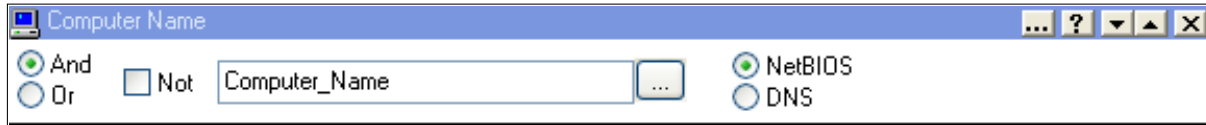
### Portable Detection

This filter can be useful for portable computer detection, as can the [PCMCIA Present](#) and/or [Portable Computer Filter](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Computer Name



This filter returns true if the computer's name matches the specified NetBIOS or DNS host name.

### Not:

Reverses the results of this filter. With this option selected this filter returns true only if the computer name does not match the specified name.

### Name:

The computer name against which the name of machine will be compared. Matching is not text case sensitive. [Variables](#) may be used in this setting. The browse option launches the [Computer Browser](#).

### NetBIOS:

Instructs PolicyMaker to compare the specified name to the NetBIOS name of the computer. Uses the %ComputerName% variable for comparison.

### DNS:

Instructs PolicyMaker to resolve the specified name and compare the result to the IP address(es) of the computer. The specified host name is first resolved into one or more IP address(es) using the Windows name resolution behavior in effect on the computer. There is no required format for the specified name except that it must be resolvable to an IP address. The list of IP addresses obtained is compared to all of the IP addresses bound to all network adapters on the computer. If a single match exists, the filter returns true.

### Wildcards

If "NetBIOS" is selected, the computer name field accepts any combination of the standard wildcards \* (multiple character) and ? (single character). For example:

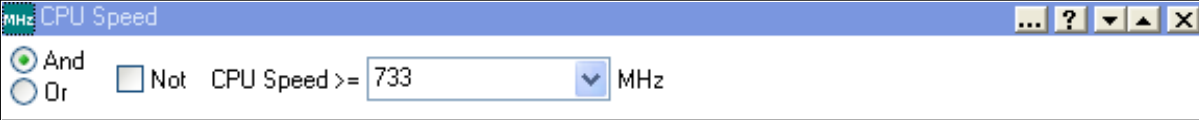
"Desktop?" will match Desktop0, Desktop9, DesktopW, but not Desktop01 or Desktop

"Desk\*top" will match Desktop, Desk1top, Desk123top

Because of the advanced resolution method used for matching multiple addresses against multiple bindings, wildcards are not supported with the "DNS" option selected.

## CPU Speed

---



MHz CPU Speed

And  
 Or

Not CPU Speed >= 733 MHz

This filter returns true if the speed of the computer's CPU is greater than or equal to the speed specified.

---

### Not:

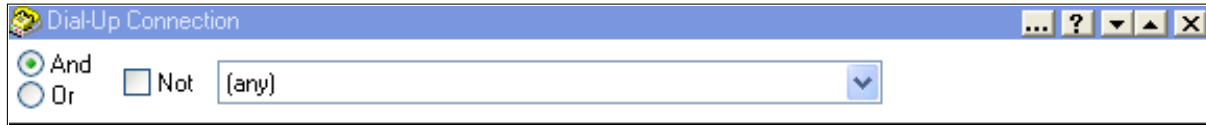
Reverses the results of this filter. This is logically the equivalent of the filter reading "CPU Speed < [xxx] MHz".

### MHz:

The speed against which the CPU of the computer will be compared. [Variables](#) may be used in this setting.

---

## Dial-Up Networking



**Dial-Up Network filtering is not available in computer policy.** This filter returns true if there is an active Windows "Dial-Up Networking" (DUN) connection of the type specified.

### Not:

Reverses the results of this filter. With this option selected this filter returns true only if a DUN connection of the type specified is not active on the computer.

### Connection Type:

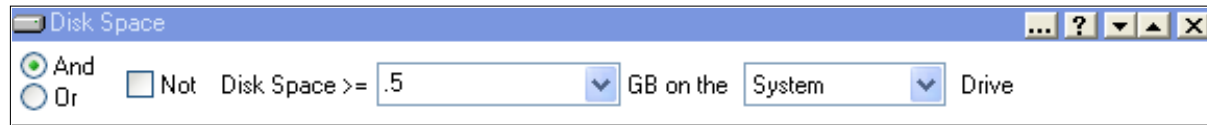
These types are defined by Windows Dial-Up Networking. The "(any)" option will match any type of connection in the list below.

- (any)
- Telephone modem accessed through a COM port
- ISDN card with corresponding NDISWAN driver installed
- X.25 card with corresponding NDISWAN driver installed
- Virtual Private Network (VPN)
- Asynchronous Transfer Mode (ATM)
- Frame Relay
- Sonet
- Switched 56K access
- Infrared Data Association (IrDA) device
- Serial Port direct connection
- Parallel Port direct connection
- Generic
- Packet Assembler/Disassembler
- PPP over Ethernet (PPPoE) [not supported on Windows 2000]

### Note

There is no requirement that the user be logged on to the network over the connection, just that the connection be active on the computer.

## Disk Space



This filter returns true if the free space remaining on the specified drive is greater than or equal to the amount specified.

### Not:

Reverses the results of this filter. This is logically the equivalent of the filter reading "Disk Space < [xxx] GB on the [x] Drive".

### GB:

The amount of space (in gigabytes) against which the free space of the specified drive will be compared. Decimal values (e.g. .5) are allowed. [Variables](#) may be used in this setting.

### Space Measurement

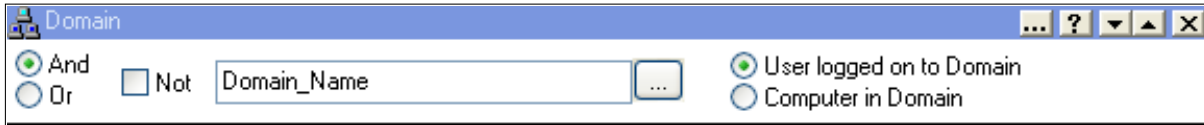
Some drive manufacturers advertise a gigabyte as 1,000 MB ( $10^3 + 2^{20}$  bytes) or even 1,000,000 KB ( $10^6 + 2^{10}$  bytes). PolicyMaker uses true gigabytes ( $2^{30}$  bytes), as does Windows.

### Drive:

Either the "System" drive, or a specific drive letter. The System drive option directs PolicyMaker to use the %systemdrive% variable for determining the comparison drive letter. The specified drive letter may be a mapped network drive.

## Domain Name

---



This filter returns true if the current end-user is logged on to the specified domain/workgroup (or the computer is a member of the specified domain, depending on the option selected).

---

### Not:

Reverses the results of this filter. Returns true if the end-user is not logged on to the specified domain (or the computer is not a member of the specified domain, depending on the option selected).

### Name:

The NetBIOS domain name with which to compare domain membership. Matching is not text case sensitive. [Variables](#) may be used in this setting. The browse option launches the [Domain Browser](#).

### User logged on to Domain:

**This option is disabled in computer policy.** Compare the specified domain name with the domain to which the end-user is logged on. This is also the domain of which the end-user is a member. This is the default option in user policy. Uses the %LogonDomain% variable for comparison.

### Computer in Domain:

Compare the specified domain name with the domain (or workgroup) to which the computer belongs. This is the only option in computer policy. Uses the %DomainName% variable for comparison.

---

### Wildcards

The domain name field accepts any combination of the standard wildcards \* (multiple character) and ? (single character). For example:

"Domain?" will match Domain0, Domain9, DomainW, but not Domain01 or Domain

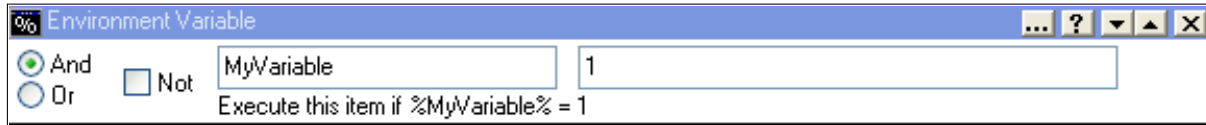
"Dom\*ain" will match Domain, Dom1ain, Dom123ain

---



## Environment Variable

---



This filter returns true if the specified variable matches the value specified. All PolicyMaker variables are implemented internally as environment variables. There are four basic types of environment variables; process, system, user and volatile. PolicyMaker implements its own internal variables as process variables. PolicyMaker also integrates all system and user variables that are set at the time the CSE is launched.


---

### Not:

Reverses the results of this filter. Returns true if the specified variable does not exist or does not match the specified value.

### Variable:

The name of the variable. Matching of variables is not text case sensitive. [Variables](#) are not supported in this setting.

 PolicyMaker incorporates persistent environment variables and variables set during the client side extension execution. Non-persistent variables that are set by one client side extension are not available in others.

### Match Value:

The value to match against the value of the specified variable. Matching is text case independent. [Variables](#) can be used in this setting.

---

### Use with the [Message Box](#) Filter

In user policy, the Message Box filter allows for a specified environment variable to be set to "1" if the end-user selects Yes (or OK) from the message box. This variable can be used in subsequent variable filters without again presenting a message box.

---

## File Match

The top screenshot shows the 'File Match' dialog box with the following settings:

- Logic:  And,  Or,  Not
- Match Type: File/Folder Exists
- Path: [Empty text box]

The bottom screenshot shows the 'File Match' dialog box with the following settings:

- Logic:  And,  Or,  Not
- Match Type: Match File Version
- Path: [Empty text box]
- Comparison Operators:  >,  <,  >=,  <=
- Version Fields: [0] [.] [0] [.] [0] [.] [0]

This filter returns true if the file or folder parameters are matched. The filter expands when a Match Type other than "File/Folder exists" is selected.

### Not:

Reverses the results of this filter. This is logically the equivalent of the filter reading "File/folder does not exist" or "File does not exist in the version range specified".

### Match Type:

- File/Folder Exists - returns true if the file or folder specified by the Path parameter exists.
- Match File Version - returns true if the file specified by the Path parameter exists, has a version resource, and the version falls within the range specified.

### Path:

The path to the file or folder. [Variables](#) can be used in this setting. The browse button launches the [File Browser](#).

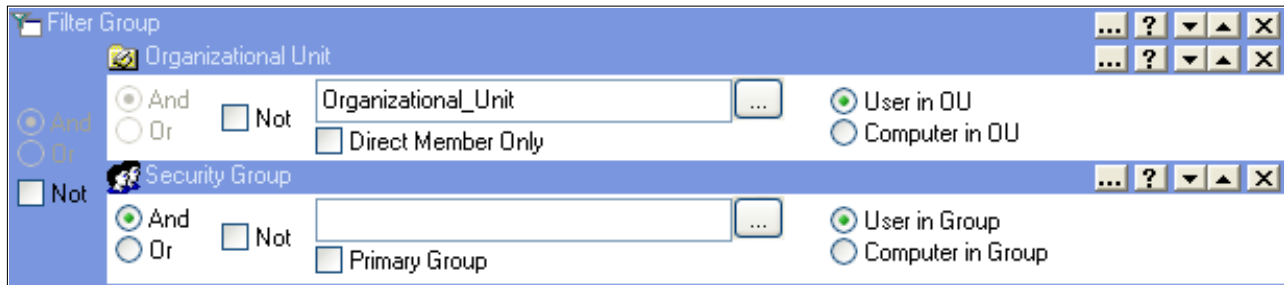
### Versions

Versions are specified for the "Match File Version" option only. The lower bound for the file version is on the left control, the upper bound on the right. Version values are consistent with Windows file versions, and each segment has a lower bound of 0 and an upper bound of 65535.

### ◆ Security Context

File/folder detection is always first performed in the SYSTEM [security context](#). If this fails for permissions, the detection is performed in the security context of the logged-on user (in a user policy), regardless of common tab settings (PolicyMaker Standard Edition and PolicyMaker Registry Extension). This allows the filter to match files and folders on the network, to which the SYSTEM context may not have permissions. In SYSTEM context PolicyMaker converts any end-user drive map to a UNC path so that it may be "seen" in system context.

## Filter Group



Using filter groups you can create parenthetical filter expressions, with any level of nesting.

Not:

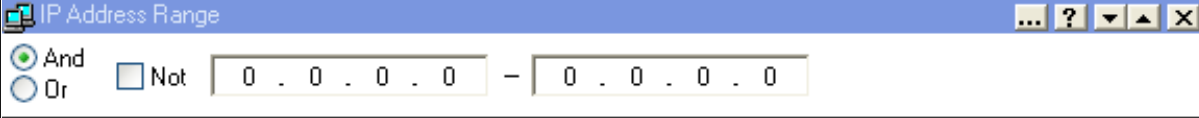
Reverses the results of the filter group.

Adding filters to a filter group

To add a filter to a group, add the filter to the [Active Frame](#) by selecting it from the list of filter types in the header. Next drag and drop the filter to the body area of the filter group. To add additional filter items, use the same technique, positioning the filter by dragging the filter until the red line highlights the desired position. Filter groups can be added to filter groups using the same technique.

## IP Address Range

---




This filter returns true if one of the computer's IP addresses falls within the specified range.

---

Not:

Reverses the results of this policy. Returns true if the none of the computer's IP addresses falls within the specified range.

---

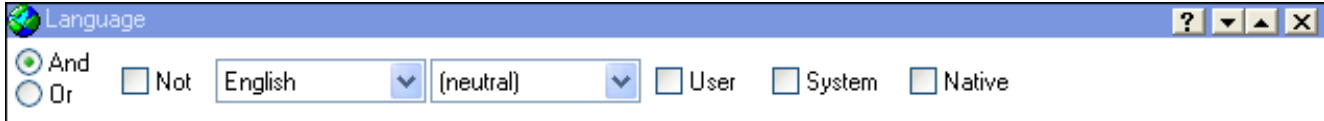
 Specifying a single address

The range is inclusive of the endpoints. Specifying the same value in each field results in a single address check.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Language



The screenshot shows a dialog box titled "Language" with a blue title bar. It contains two radio buttons: "And" (selected) and "Or". To the right of "And" is a checkbox labeled "Not". There are two dropdown menus: the first is set to "English" and the second is set to "(neutral)". To the right of these are three checkboxes: "User", "System", and "Native", all of which are currently unchecked.

This filter returns true if the specified locale (language/sub-language) is installed on the computer. Additional options allow this filter to be narrowed to return true only if the specified locale is the user's locale and/or the operating system locale.

Not:

Reverses the results of this filter.

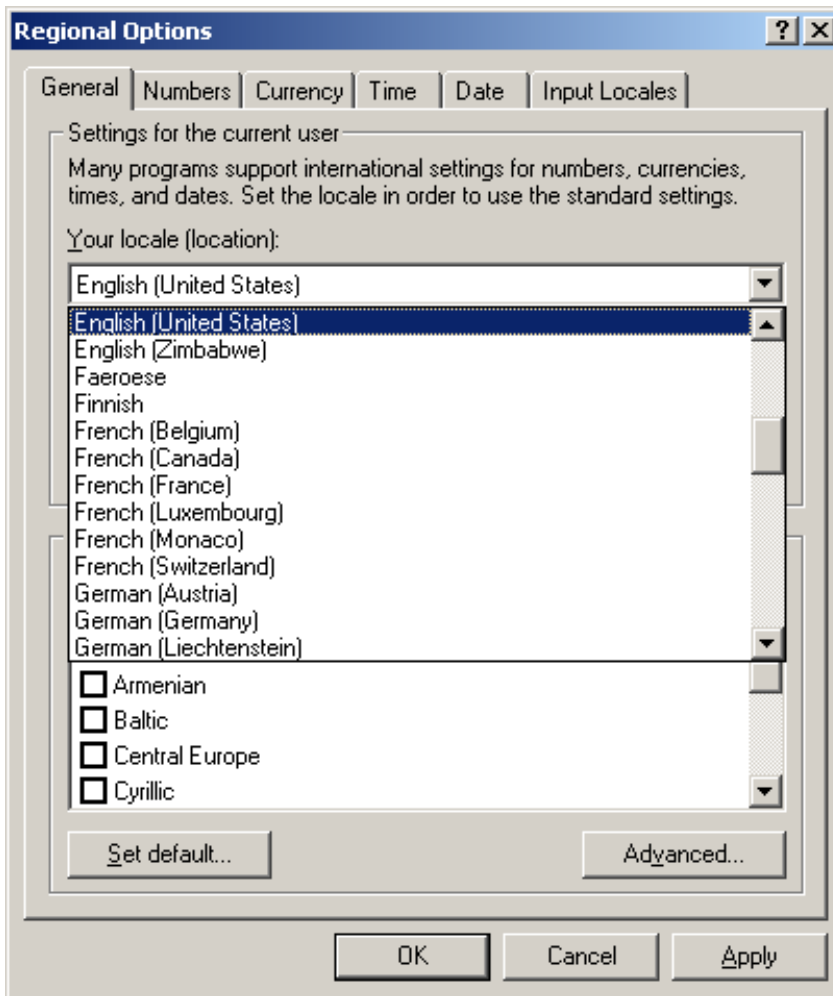
Primary Language (first option):

The major language (i.e. French).

Sub-Language (second option):

Generally the region in which the language is spoken (i.e. Canada (French)). Language and Sub-language are combined to create a locale identifier. If "(neutral)" is specified, the Sub-Language will be ignored and PolicyMaker will match any locale containing the specified primary language.

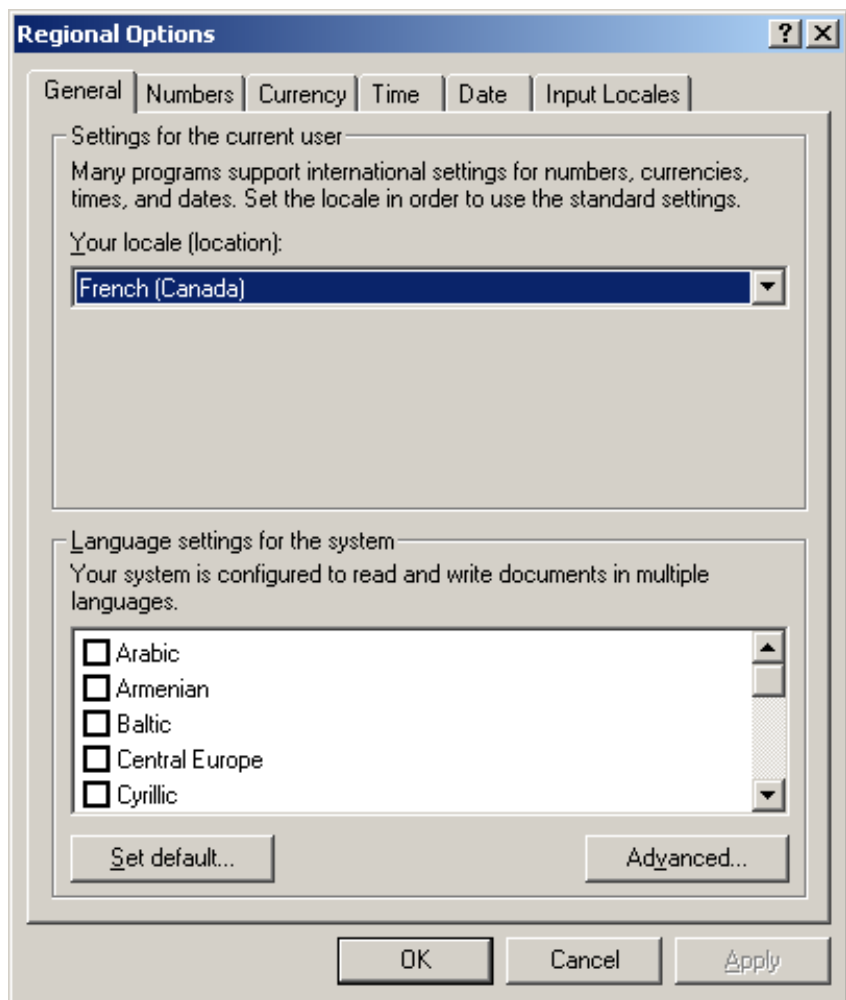
If you do not select either of the "User Locale" or "System Locale" options, this filter will return true if the specified locale is installed on the computer. The following drop-down list in the "Regional Options" control panel applet shows the currently installed locales.



The screenshot shows the "Regional Options" dialog box with the "Input Locales" tab selected. The "Settings for the current user" section contains a text box with the instruction: "Many programs support international settings for numbers, currencies, times, and dates. Set the locale in order to use the standard settings." Below this is a label "Your locale (location):" followed by a list box. The list box contains the following entries: "English (United States)" (highlighted), "English (Zimbabwe)", "Faeroese", "Finnish", "French (Belgium)", "French (Canada)", "French (France)", "French (Luxembourg)", "French (Monaco)", "French (Switzerland)", "German (Austria)", "German (Germany)", "German (Liechtenstein)", "Armenian", "Baltic", "Central Europe", and "Cyrillic". There are checkboxes next to "Armenian", "Baltic", "Central Europe", and "Cyrillic", all of which are unchecked. At the bottom of the list box are two buttons: "Set default..." and "Advanced...". At the very bottom of the dialog box are three buttons: "OK", "Cancel", and "Apply".

User Locale:

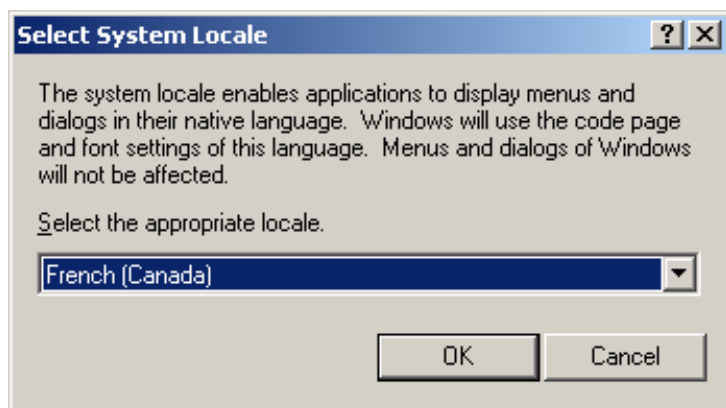
**This option is disabled in computer policy.** The specified locale must be currently selected as the user's locale.



 This option is useful when presenting a [Message Box](#) or other user interface item to an end-user.


System Locale:

The locale must be the locale of the operating system.




Native OS:

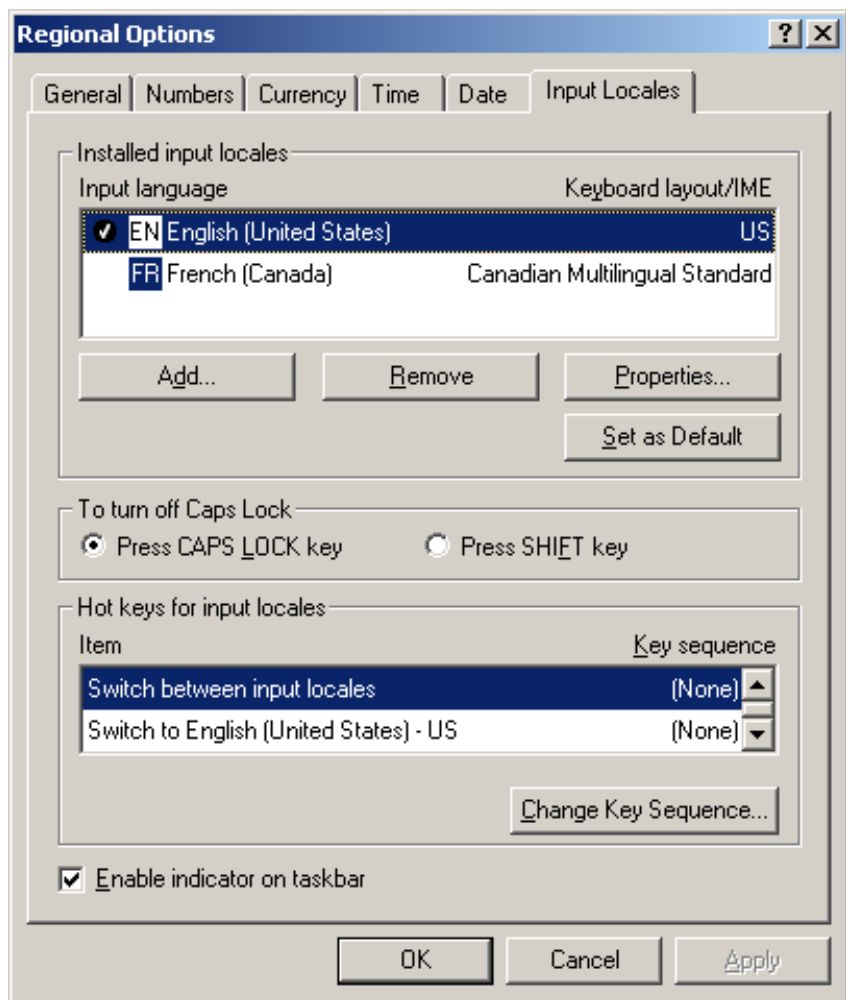
The locale must match the language of NTDLL.DLL.

 As this references the core operating system language, this option is useful when installing a Service Pack or other software.

---

 Input Locales

Input locales (as shown below) are not a feature of this filter.



#### ◆ Security Context

In a user policy, the User Locale test is performed in the security context of the logged-on user, regardless of common tab settings (PolicyMaker Standard Edition and PolicyMaker Registry Extension). This does not have an impact on security, but this knowledge it may be useful in interpreting the client side trace.

## LDAP Query



This filter returns true if the specified Attribute is found in the filtered search of the container specified by the binding.

### Not:

Reverses the result of this filter.

### Filter (optional):

The LDAP search filter to execute within the scope of the container specified in Binding. All subcontainers are searched. If this value is empty, the Binding may specify a non-container object.

#### Example:

This LDAP search filter will find all users with a last name that starts with the letter A.

`(&(objectClass=user)(sn= A*))`

### Binding:

The path to a container in which the search will be conducted. The object must be a container if a Filter is specified, or an error will result. If the Binding cannot be satisfied, an error results. Note that the binding prefix is case sensitive, i.e. "LDAP" must be upper case.

#### Examples (filtered or not filtered):

`LDAP:` - Bind to the root of the namespace.

`GC:` - Bind to the root of the Global Catalog.

`LDAP://servername` - Bind to a specific server.

`LDAP://distinguishedName` - Bind to a specific container by its distinguished name.

#### Examples (not filtered only):

`LDAP://<SID=%reversedusersid%>` - Bind to the user object (or computer object in computer policy).

`LDAP://<SID=%reversedcomputersid%>` - Bind to the computer object.

`LDAP://<GUID=objectGuid>` - Bind to a specific object by its unique identifier.

### Attribute (optional):

Specific Attribute to look for in the first returned row. If the attribute is specified and not found, the filter returns false.

#### Example:

This attribute contains the 'canonical name' of the object:

`cn`

### Variable name (optional):

Environment variable that will be set to the value of the Attribute, if one is found. The following data types are supported for return in variable values. Other types will succeed but return an empty value:

`ADSTYPE_DN_STRING`  
`ADSTYPE_CASE_EXACT_STRING`  
`ADSTYPE_CASE_IGNORE_STRING`  
`ADSTYPE_PRINTABLE_STRING`  
`ADSTYPE_NUMERIC_STRING`  
`ADSTYPE_OBJECT_CLASS`  
`ADSTYPE_BOOLEAN`

### Notes

The query search preferences are set to search subtrees of the container, but not to chase referrals. See ADSI documentation from Microsoft for more information on these subjects.



## MAC Address Range

---



MAC Address Range

And  
 Or

Not

00 - 00 - 00 - 00 - 00 - 00 - 00 - 00

00 - 00 - 00 - 00 - 00 - 00

This filter returns true if one of the computer's MAC addresses falls within the specified range.

---

Not:

Reverses the results of this filter. Returns true if the none of the computer's MAC addresses falls within the specified range.

---

### Specifying a Single Address

The range is inclusive of the endpoints. Specifying the same value in each field results in a single address check.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Message Box



This filter presents a message box prompt to the end-user. The user is given the choice of selecting Yes/No (or OK/Cancel) from the prompt. The filter returns true if the end-user selects Yes (or OK). If a variable is specified and the end-user selects Yes (or OK) the variable is set to "1".

**Message Box filtering is not available in computer policy.** If a message box filter is executed in synchronous foreground processing, the message box will appear on the winlogon desktop (i.e. prior to the user desktop being available). In asynchronous foreground or background processing, the message box will be presented in the end-user's desktop environment.

**Not:**

Reverses the results of this filter. Returns true if the end-user selects No (or Cancel). If a variable is specified, the value is set to "1" if the user selects Yes (or OK) and "0" for No (or Cancel), regardless of this Not option.

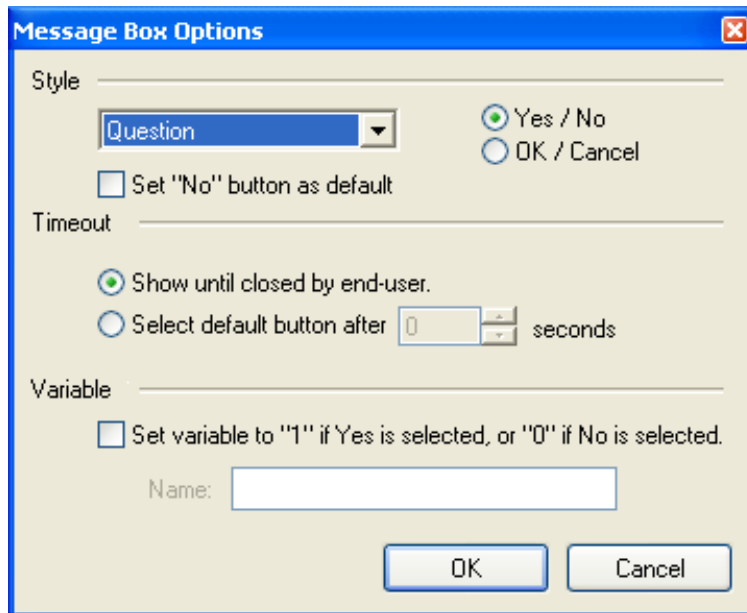
**Title:**

The text that will appear in the title bar of the message box prompt. [Variables](#) may be used in this setting.

**Body:**

The text that will appear in the body of the message box prompt. [Variables](#) may be used in this setting.

**Options...:**



**Style**

Controls the selection of icon and sound. These are dependant upon operating system settings on the end-user's computer. The default style is "Question".

**OK/Cancel or Yes/No:**

Controls the type of buttons presented to the end-user. The text on these buttons is operating system and language dependant. The default is "Yes/No".

**Set "No" (or "Cancel") button as default:**

Sets the No/Cancel button as the default button for the message box. If the end-user hits <enter> with the message box open, the action will be No/Cancel. The default is Yes/OK.

**Timeout**

These options cause the message box to close automatically without end-user input. Message box timeout options prevent PolicyMaker from suspending the logon process with a message box if the end-

user is not present or attentive. The message box closes by selecting the button that you have specified as the default (see above).

- Show until closed by end-user
- Select default button after [] seconds

#### Variable

Set variable to "1" if Yes is selected, or "0" if No":

Sets the specified variable to the value "1" if the end-user selects Yes/OK or sets the variable to "0" if the end-user selects No/Cancel. The variable will not persist after the client side extension terminates. By default, no variable is set.

Variable name:

The name of the variable to set. [Variables](#) are not supported in this setting.

[! - Test Message Box]:

Preview the message box for appearance. [Variables](#) are not resolved at preview time.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Message Box



This filter presents a message box prompt to the end-user. The user is given the choice of selecting Yes/No (or OK/Cancel) from the prompt. The filter returns true if the end-user selects Yes (or OK). If a variable is specified and the end-user selects Yes (or OK) the variable is set to "1".

**Message Box filtering is not available in computer policy.** If a message box filter is executed in synchronous foreground processing, the message box will appear on the winlogon desktop (i.e. prior to the user desktop being available). In asynchronous foreground or background processing, the message box will be presented in the end-user's desktop environment.

**Not:**

Reverses the results of this filter. Returns true if the end-user selects No (or Cancel). If a variable is specified, the value is set to "1" if the user selects Yes (or OK) and "0" for No (or Cancel), regardless of this Not option.

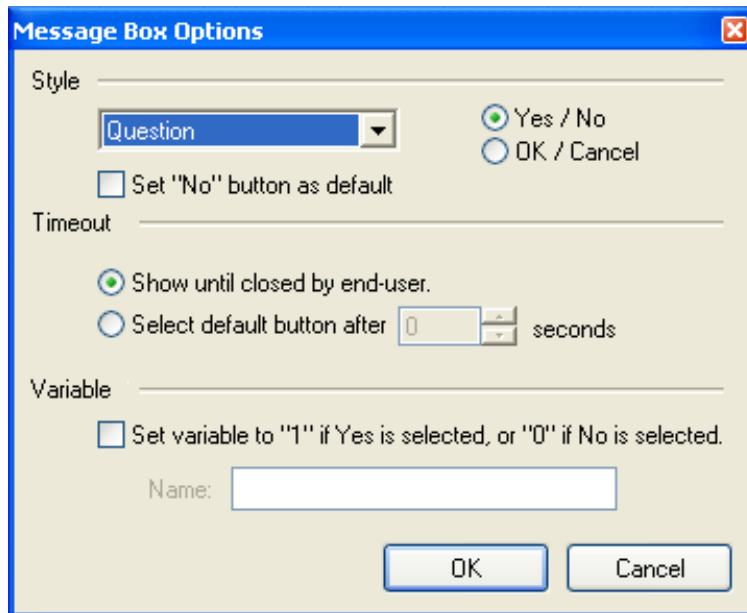
**Title:**

The text that will appear in the title bar of the message box prompt. [Variables](#) may be used in this setting.

**Body:**

The text that will appear in the body of the message box prompt. [Variables](#) may be used in this setting.

**Options...:**



**Style**

Controls the selection of icon and sound. These are dependant upon operating system settings on the end-user's computer. The default style is "Question".

**OK/Cancel or Yes/No:**

Controls the type of buttons presented to the end-user. The text on these buttons is operating system and language dependant. The default is "Yes/No".

**Set "No" (or "Cancel") button as default:**

Sets the No/Cancel button as the default button for the message box. If the end-user hits <enter> with the message box open, the action will be No/Cancel. The default is Yes/OK.

**Timeout**

These options cause the message box to close automatically without end-user input. Message box timeout options prevent PolicyMaker from suspending the logon process with a message box if the end-

user is not present or attentive. The message box closes by selecting the button that you have specified as the default (see above).

- Show until closed by end-user
- Select default button after [] seconds

#### Variable

Set variable to "1" if Yes is selected, or "0" if No":

Sets the specified variable to the value "1" if the end-user selects Yes/OK or sets the variable to "0" if the end-user selects No/Cancel. The variable will not persist after the client side extension terminates. By default, no variable is set.

Variable name:

The name of the variable to set. [Variables](#) are not supported in this setting.

[! - Test Message Box]:

Preview the message box for appearance. [Variables](#) are not resolved at preview time.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## MSI Query

MSI Query

And  Or  Not

Query type: Target exists Target type: Product Product code: {63A68338-16A3-4763-8478-A45F91A61E7A}

MSI Query

And  Or  Not

Query type: Version match Target type: Product Product code: {63A68338-16A3-4763-8478-A45F91A61E7A}

>  >= 2 . 0 . 0 . 0  <  <= 4 . 0 . 0 . 0

MSI Query

And  Or  Not

Query type: Get information Target type: Product Product code: {63A68338-16A3-4763-8478-A45F91A61E7A}

Information item name: InstallSource Variable name: MyVariable

Return value in %MyVariable%

MSI Query

And  Or  Not

Query type: Match property Target type: Product Product code: {63A68338-16A3-4763-8478-A45F91A61E7A}

Property name: Manufacturer Property value: Microsoft Corporation

This filter returns true if certain aspects of an MSI-installed Product, Patch or Component meet the specified criteria.

**Not:**  
Reverses the result of this filter.

**Query type:**

- Target exists - The filter returns true if:
  - Product - The product that has the specified Product code is installed.
  - Patch - The patch that has the specified Patch code has been applied.
  - Component - The keyfile of a component that has the specified Component code is installed.
- Version Match - The filter returns true if:
  - Product - The product that has the specified Product code is within the specified version range.
  - Component - The keyfile of a component that has the specified Component code is within the specified version range.


(For example, the filter in the second graphic will return true if the product's major version is at least 2 and less than 4)

Note: Properties and info items (below) are obtained from the product to which a given component belongs if the Target type is set to "Component".

Note: The filter will return false if the Target does not exist for the following Query types:

- Get property or Get information - The specified property or info item is stored in the provided Variable.
- Match property or Match information - The filter returns true if the specified property or info item is equal

to the provided Value.

 Note: The filter will return false if the specified property or info item is undefined (has no value).

Target type:

- Product - Locates an installed product that has the specified Product code.
  - Patch - Locates an applied patch that has the specified Patch code.
  - Component - Locates the installed keyfile of a component that has the specified Component code.
- 

Example (getting an info item value):

The third filter will return true if the product is installed and the "InstallSource" info item is defined. Additionally, the variable "MyVariable" will be set to the value of the "InstallSource" info item.

Example (matching a property value):

The fourth filter will return true if the product is installed and the value of the "Manufacturer" property is "Microsoft Corporation".

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Operating System

---



Operating System

And  Or  Not

Version: Windows 2000 Level: (any)

Category: (any) Flavor: (any)

This filter returns true if the specified platform matches the client platform.

---

### Not:

Reverses the results of this filter. Returns true if the specified platform does not match the client platform.

### Version (first option):

The major version of Windows.

### Level

The service pack level of the major version of Windows specified. "Gold" is used to specify a match only with no service pack.

### Category (second option):

The category of Windows operating system, i.e. Windows 2000: Member Server, Domain Controller, or Workstation.

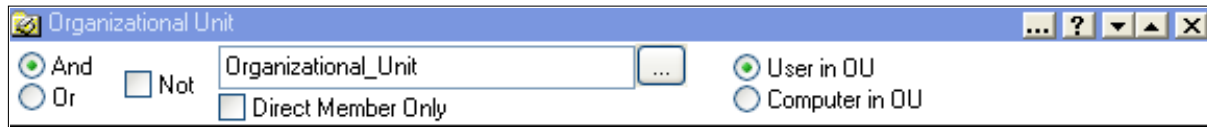
### Flavor (third option)

The flavor of the operating system, i.e Windows XP: Professional, Home Edition, Tablet PC, etc.

---



## Organizational Unit



This filter returns true if the current end-user is a member of the specified Active Directory (AD) Organizational Unit (OU) (or the computer is a member of the specified OU, depending on the option selected). The membership test optionally excludes all inherited OU membership.

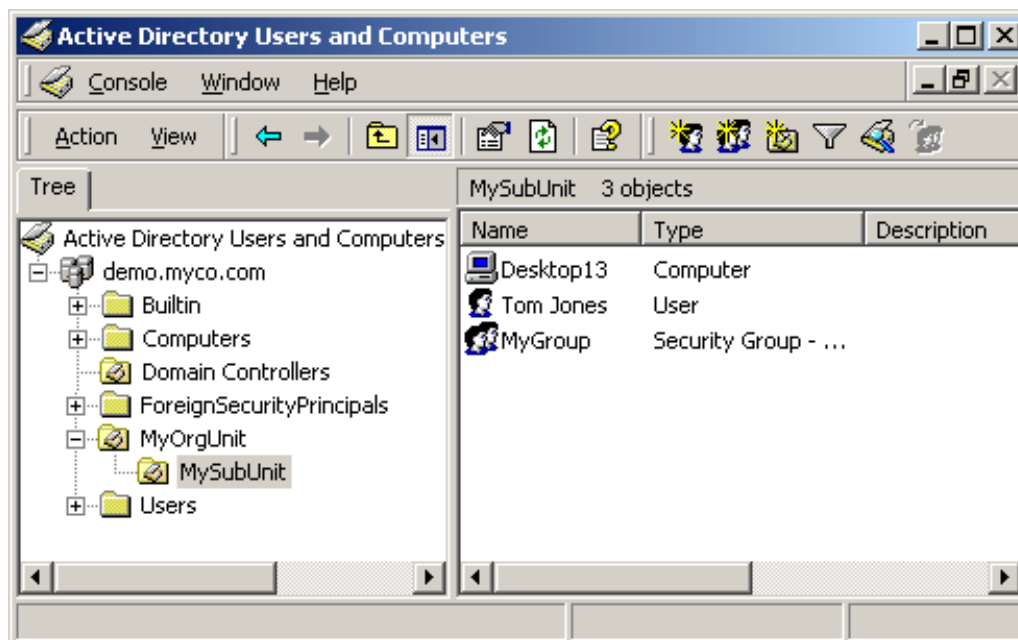
### Not:

Reverses the results of this filter. Returns true if the end-user is not a member of the specified OU (or the computer is not a member of the specified OU, depending on the option selected).

### Name:

The OU name with which to compare OU membership. E.g., "MyOrgUnit" or "MySubUnit" in the example below. Matching is not text case sensitive. [Variables](#) may be used in this setting. The browse button launches the [OU Browser](#). This field supports three formats:

- unqualified: MySubUnit
- partially qualified: OU=MyOrgUnit,OU=MySubUnit
- fully qualified: OU=MyOrgUnit,OU=MySubUnit,DC=Demo,DC=desktopstandard,DC=com



### Direct Member Only:

Return true only if the user (or computer) is a direct member of the specified OU. This eliminates consideration for inheritance. E.g., in the example above, if "Tom Jones" were logged on as the end-user, and the specified OU was "MyOrgUnit", the filter would return false if this option was selected and true otherwise.

### User in OU:

**This option is disabled in computer policy.** Compare the specified OU with the OU to which the end-user belongs. This is the default option in user policy.

### Important

In computer policy there is no user context, and this option is therefore not recommended in computer policy.

### Computer in OU:

Compare the specified OU with the OU to which the computer belongs. This is the only option in computer policy.

### Security Groups as OU Members

In the example above, "MyGroup" is a security group that is a member of "MySubUnit". Users (and computers) that are members of this security group are not members of "MySubUnit" or "MyOrgUnit" unless they are otherwise members of the OU (as is "Tom Jones").

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## PCMCIA Present

---



This filter returns true if there is at least one PCMCIA slot (with drivers installed) in the computer.

---

### Not:

Reverses the results of this filter. With this option selected this filter returns true only if there are no PCMCIA slots in the computer (or none of the physical slots have drivers installed).

---

### Portable Detection

This filter can be useful for portable computer detection, as can the [Battery Present](#) and/or [Portable Computer Filter](#).

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Portable Computer




This filter returns true if the computer is listed as a portable in the current hardware profile. Additionally, this filter can be limited to portable computers with a specified docking state.

### Not:

Reverses the results of this filter.

### Docking State:

The docking state of a portable is always reported to be one of three values. Any combination of these states may be selected.

 If no states are selected, the filter will return true for a portable regardless of its docking state. Selecting all three possible states will have the same result.

- Unknown:

Return true if the computer is portable and the docking state is "unknown".

- Docked:

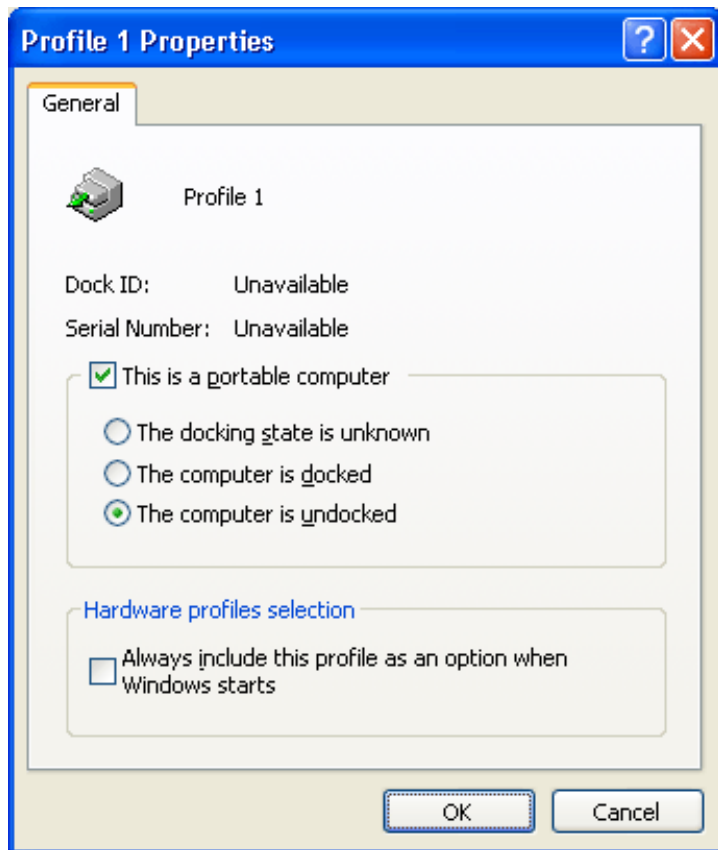
Return true if the computer is portable and the docking state is "docked".

- Undocked:

Return true if the computer is portable and the docking state "undocked".

### How is portable status determined?

The following image shows the docking state as reported by the Windows XP operating system. All supported versions of Windows will report the portable status and docking state, however the accuracy of this setting is dependant upon the BIOS. If the BIOS reports this value to the operating system, the BIOS value will override any manually set value each time the computer boots. As a result, on newer computers, this setting is reasonably reliable. The [Battery Present](#) and/or [PCMCIA Present](#) Filter can also be useful for portable computer detection.



## RAM Total

---



The screenshot shows a dialog box titled "RAM" with a blue header bar. On the left, there are two radio buttons: "And" (selected) and "Or". To the right of these is a checkbox labeled "Not". The main text of the dialog is "Total Ram >=" followed by a text input field containing the number "64" and a dropdown arrow, and then "MB". The dialog box has standard window controls (minimize, maximize, close) in the top right corner.

This filter returns true if the amount of RAM in the computer is greater than or equal to the amount specified.

---

Not:

Reverses the results of this filter. This is logically the equivalent of the filter reading "Total RAM < [xxx] MB".

MB:

The amount of RAM to which the RAM in the computer will be compared. [Variables](#) may be used in this setting.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## Recur Every

---



Recur Every

And  
 Or

Not

Weekly

Sunday

This filter returns true if the current date falls within the date specification.

---


### Not:

Reverses the results of this filter. Returns true if the current date does not falls within the date specification.

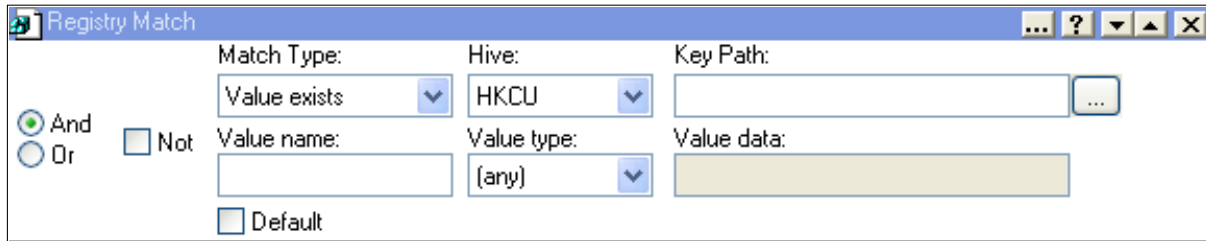
### Options:

- Weekly:
    - Day of Week:  
Returns true if current day of the week matches the one specified (e.g. Monday).
  - Monthly:
    - Day of Every Month:  
Returns true if the current day of the month matches the one specified (e.g. 15th).
  - On Date
    - Date:  
Returns true if the current date matches the date specified (e.g. January 1, 2003).
    - Every Year:  
Check this option to ignore the year. Returns true if the current date matches the day of the year specified (e.g. January 1st - every year).
-

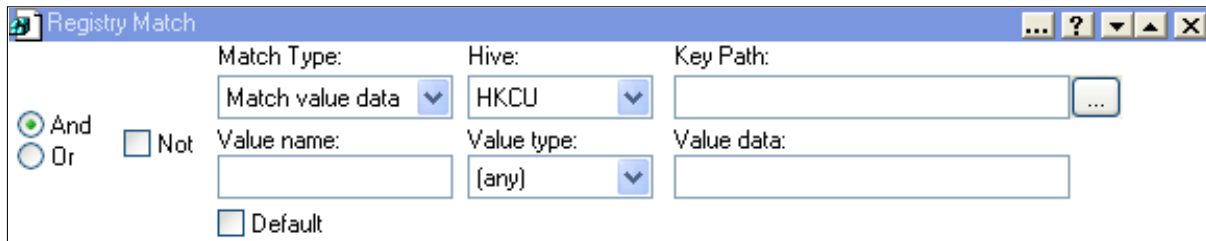
## Registry Match



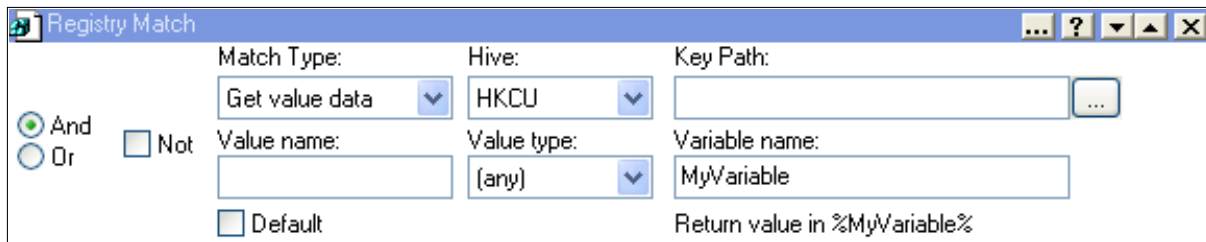
Registry Match dialog box showing the "Key exists" match type. The "And" radio button is selected. The "Match Type" dropdown is set to "Key exists", "Hive" is "HKCU", and "Key Path" is empty.



Registry Match dialog box showing the "Value exists" match type. The "And" radio button is selected. The "Match Type" dropdown is set to "Value exists", "Hive" is "HKCU", and "Key Path" is empty. The "Value name" and "Value data" fields are empty, and "Value type" is set to "(any)".



Registry Match dialog box showing the "Match value data" match type. The "And" radio button is selected. The "Match Type" dropdown is set to "Match value data", "Hive" is "HKCU", and "Key Path" is empty. The "Value name" and "Value data" fields are empty, and "Value type" is set to "(any)".



Registry Match dialog box showing the "Get value data" match type. The "And" radio button is selected. The "Match Type" dropdown is set to "Get value data", "Hive" is "HKCU", and "Key Path" is empty. The "Value name" and "Value data" fields are empty, and "Value type" is set to "(any)". The "Variable name" field is set to "MyVariable".

This filter returns true if the specified registry key or value is found. It may also be used to return the value data under any registry value name in a variable. The filter expands when a Match Type other than "Key exists" is selected.

### Not:

Reverses the results of this filter.

### Match Type:

This setting controls the behavior of the filter. The possible options are:

- Key exists - returns true if the specified registry key exists.
- Value exists - returns true if the specified registry value exists.
- Match value data - returns true if the specified registry value exists and matches the specified value (REG\_DWORD stored in XML as hexadecimal).
  - Decimal format - returns true if the specified registry value exists and matches the specified value (REG\_DWORD values stored in XML as decimal).
  - Substring match - returns true if the specified registry value exists and contains the specified value
  - Version match - returns true if the string version number found in the registry value specified falls within the range specified.
- Get value data - returns true under the same conditions as "Match value data" and returns the value data in the specified variable.

### Hive:

The registry hive. All hives are supported. The list is abbreviated for space considerations. The following values are selectable:



- HKCU = HKEY\_CURRENT\_USER
- HKU = HKEY\_USERS
- HKLM = HKEY\_LOCAL\_MACHINE
- HKCC = HKEY\_CURRENT\_CONFIG
- HKCR = HKEY\_CLASSES\_ROOT

#### Key Path:

The path to registry key. This setting should not contain the hive specification. Key paths are not text case sensitive. The browse button launches the [Registry Browser](#). A key or value may always be selected using the browser, and the appropriate data will be filled into the various fields as appropriate for the specified "Match Type". [Variables](#) can be used in this setting.

#### Value Name:

This setting is not available for the "Key Exists" filter. This is the name of the registry value that should be matched. Value names are not text case sensitive. [Variables](#) can be used in this setting.

#### Default:

Select default to specify the "(Default)" value for a key.

#### Note

The default value is actually just a typical value that has a zero-length name. Regedit shows this value under each key as a REG\_SZ named "(Default)", even if that value doesn't exist. In this case Regedit also shows "(value not set)" in the data column. PolicyMaker will return false when filtering against a default value that doesn't actually exist.

#### Value Type:

This setting is not available for the "Key Exists" filter. This is the registry data type that must match in order for the filter to pass. The "(any)" type will attempt to match regardless of the actual data type of the value. Note that it is technically possible for "default" values to have any data type, although REG\_SZ is most common. All registry data types that are visible in Regedit are supported, specifically:

- REG\_SZ
- REG\_EXPAND\_SZ
- REG\_MULTI\_SZ
- REG\_DWORD
- REG\_BINARY

#### Value Data/Substring:

This setting is not available for the "Key Exists" filter. This is the data that will be matched against the data in the specified registry value. [Variables](#) can be used in this setting.

#### (any)

Attempts to match with the value regardless of its data type. The value data is converted to a string for matching, using the conversion rules below.

#### REG\_SZ

Matches are not text case sensitive.

#### REG\_EXPAND\_SZ

Matches are not text case sensitive and environment data in the value is not expanded. It is common to have to match unresolved environment variables. Use the unresolved variable syntax to match an unresolved value. For example, to match a value that contains "%ProgramFiles%\DesktopStandard", use "%<ProgramFiles>%\DesktopStandard". This syntax prevents resolution of the %ProgramFiles% environment variable - and PolicyMaker replaces the %<...>% with %...% before comparison.

#### REG\_MULTI\_SZ

This data type is a list of strings with NULL separators. PolicyMaker reads the first string in this list and ignores any others when matching. Matches are not text case sensitive.

#### REG\_DWORD

Regardless of the value of the Decimal/Hexadecimal option, PolicyMaker saves REG\_DWORD settings as an eight character hexadecimal strings if "Hex match" is selected, and decimal strings otherwise. The results are the same when the REG\_DWORD data type is specified. For example, to match the dword value (as presented in Regedit) 0x00000001, enter decimal "1" or hexadecimal "00000001", regardless of the matching

mode. Hexadecimal values that are entered with less than 8 characters are prefixed with zeroes by the client.

#### REG\_BINARY

These types are converted to hexadecimal strings for comparison with the data specified in this setting. The data must be entered in the same format and byte order. For example, to match the binary value (as presented in Regedit) "0B 5F 78 03 AC 09 22", enter "0B5F7803AC0922" into this setting. Binary values are always compared as hexadecimal strings, and as such also support the "Substring match" option.

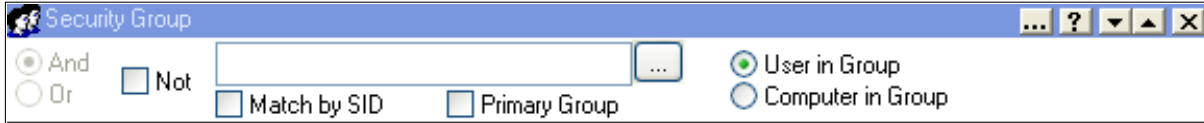
#### Variable Name:

This setting is only available with the "Get value data" filter. This contains the name of the variable into which you want the found value data returned. The data is converted to the appropriate format for the data type, as described in the "Value Data" section above. [Variables](#) are not supported in this setting.

#### Versions

Versions are specified for the "Version match" option only. The lower bound for the version is on the left control, the upper bound on the right. Version values are consistent with Windows file versions, and each segment has a lower bound of 0 and an upper bound of 65535. A registry value with a period (".") or comma (",") delimited version string in four segments can be matched as if it were an actual file version.

## Security Group



This filter returns true only if the user (or computer) is in the specified group, and has the specified group as the primary group (if the "Primary Group" option is selected).

### Not:

Reverses the results of this filter. Returns true only if the user (or computer) is not a member of the specified group, or does not have the specified group as the primary group (if the "Primary Group" option is selected).

### Group Name:

The domain\name of the selected security group. PolicyMaker retains groups by the Security Identifier (SID) of the group. The domain\name text cannot be edited directly, since this filter is based on the group SID (which is not shown).

#### Note

The domain\name of the group is presented for reference purposes, but is not used in membership calculations. If a group name is changed, the original group name will continue to be presented in this filter, however the SID of the group will remain the same and calculations are based on the SID.

### Match by SID:

If this option is selected, the edit control is disabled and groups must be selected using the Browse button. The edit control displays the domain\name of the selected group as it existed at the time of selection. PolicyMaker retains a group by the group's Security Identifier (SID). The domain\name text cannot be edited directly, since this filter is based on the group's SID (which is not shown).

### Primary Group:

If selected, instructs the filter to return true only if the specified group is the user's primary group. This option is disabled when "Computer in Group" is selected.

### Browse...:

The browse button launches the [Group Browser](#).

#### Note

It is possible that a group may appear in the list but still not be resolvable on the network into a SID. If this is the case an error message will be presented when the group is selected from the browser. If the SID of the group is known, it can be manually inserted into the raw XML for the filter, or selected by running the snap-in on the computer where the group resides.

### User in Group:

**This option is disabled in computer policy.** The filter returns true if the user is in the specified group. This is the default option in user policy.

### Computer in Group:

The filter returns true if the computer is in the specified group. This is the only option in computer policy. The "Primary Group" option is disabled with this option selected.

## Types of Groups Supported

PolicyMaker supports two categories of security groups - domain and local.

- Domain groups
  - Global groups are selectable in the user browser under their associated domain.
  - Universal groups are selectable in the user browser under every domain.
- Local groups
  - Local groups are local to a member server or workstation local. These include created and "built-in" groups.
  - Domain Local groups are not supported or selectable using the user browser.

- Well-known groups include local groups such as "Administrators" as well as dynamic local groupings such as "Dialup Users" (i.e. users who are connected via a dial-up connection are automatically members of this group).
- Unsupported groups
  - Distribution groups are not supported or selectable using the user browser.

#### ◆ Membership Determination

The context of group membership determination depends on the type of group, client operating system, and the User Prompt option. Although the license SID can change based on Exchange mailbox configuration, this change does not affect group determination for the purposes of this filter.

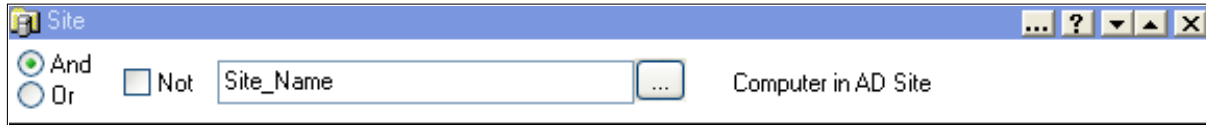
#### ◆ Security Context

All security group membership tests are performed in the security context of the logged-on user, regardless of common tab settings (PolicyMaker Standard Edition and PolicyMaker Registry Extension). This does not have an impact on security, but this knowledge it may be useful in interpreting the client trace.

#### ✍ Nested Groups Supported

PolicyMaker will consider a user who is a member of a group that is a member of the specified group, as being a member of the specified group.

## Site



This filter returns true if the Active Directory (AD) site of the computer matches the site specified.

### Not:

Reverses the results of this filter. Returns true if the computer is not in the site specified.

### Site:

The filter matches the name of the AD site where a computer resides. For a domain controller (DC), the name of the site is the location of the configured DC. For a workstation or member server, the name specifies the workstation site as configured in the domain of the computer. Matching is not text case sensitive. [Variables](#) may be used in this setting. The browse button launches the [Site Browser](#).

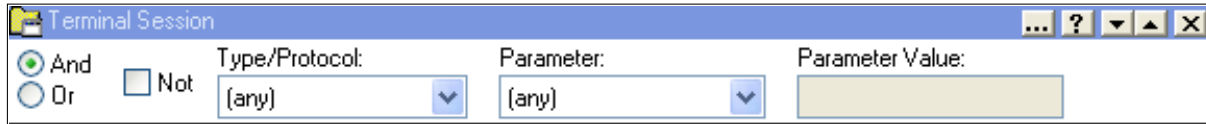
### Wildcards

The domain name field accepts any combination of the standard wildcards \* (multiple character) and ? (single character). For example:

"Site?" will match Site0, Site9, SiteW, but not Site01 or Site

"Si\*te" will match Site, Si1te, Si123te

## Terminal Session



This filter returns true if the end-user is running in a terminal session as specified.

**Not:**  
Reverses the results of this filter.

**Type/Protocol:**  
Terminal session filtering is not available in computer policy, however "Console" may be selected.

- (any) - Any type of terminal session, including a console logon.
- Microsoft Terminal Services - A Terminal Services session (including XP Remote Desktop).
- Citrix MetaFrame (ICA) - A Citrix MetaFrame (ICA) session.
- Console - The computer is running terminal services (not including XP Remote Desktop).



### Remote Desktop

Windows XP remote desktop is included in the "Microsoft Terminal Services" category. Since there is no other type of terminal session supported on Windows XP, this can be combined with an Operating System filter to detect a remote desktop session.

**Parameter:**  
If an option other than "(any)" is selected, you must specify the corresponding value in the "Parameter Value" field.

- Application Name - The published name of the application. Note that for Citrix applications, you must prefix the application name with a "#".
- Client Name - The name of the connecting computer.
- Initial Program - The path and name of the initial program.
- Session Name - Created dynamically and takes the form of RDP\_tcp# or ICA\_tcp# at the most basic level and can also be defined by users, such as LAB\_3RD\_FLOOR#.
- Working Directory - The working directory for the session on the server.
- Client TCP/IP Address - The address range of the client computer

**Parameter Value:**  
The required value corresponding to a selection, other than "(any)", in the "Parameter" setting.

### Wildcards

The parameter field (with the exception of Client TCP/IP Address) accepts any combination of the standard wildcards \* (multiple character) and ? (single character). For example:

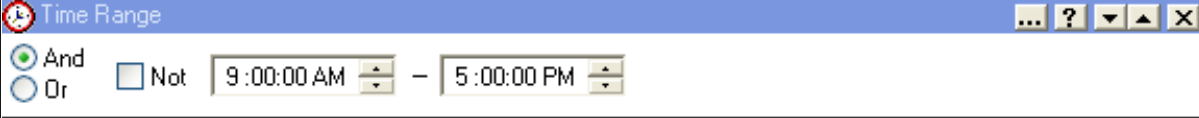
"MyComputer?" will match MyComputer0, MyComputer9, MyComputerW, but not MyComputer01 or MyComputer  
"MyC\*mputer" will match MyComputer, MyCxmpueter, MyCxxxmpueter

### Notes

Terminal Session detection is not supported on Windows NT4 platforms prior to Service Pack 4, and will return false.

## Time Range

---



This filter returns true if the current time on the end-user's computer falls within the specified time range.

---

### Not:

Reverses the result of this filter. Returns true if the current time on the end-user's computer does not fall within the specified time range.

---

### Spanning Two Days

The right box is always greater than the left. If a lesser time code appears to the right, it is considered to be on the next day.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.

## User



The screenshot shows a dialog box titled "User". On the left, there are two radio buttons: "And" (which is selected) and "Or". To the right of these is a "Not" checkbox. Further right is a text input field. At the bottom right, there is a "Match by SID" checkbox. A small "..." button is located to the right of the text input field. The dialog box has a standard Windows-style title bar with a question mark, a dropdown arrow, and a close button.

User filtering is not available in computer policy. This filter returns true if the logged-on user is the user specified.

### Not:

Reverses the results of this filter. Returns true if the logged-on user is not the user specified.

### User:

#### [x] Match by SID:

If this option is selected, the edit control is disabled and users must be selected using the Browse button. The edit control displays the domain\name of the selected user as it existed at the time of selection. PolicyMaker retains a user by the user's Security Identifier (SID). The domain\name text cannot be edited directly, since this filter is based on the user's SID (which is not shown).

#### Note

The domain\name of the user is presented for reference purposes, but is not used in comparisons. If a user name is changed, the original user name will continue to be presented in this filter, however the SID of the user will remain the same and calculations are based on the SID.

#### [ ] Match By SID:

With this option deselected, the edit control is enabled for direct text entry. Users may be selected using the Browse button or typed it. The domain name should not be entered.

#### Note

The match is performed by way of a case insensitive wildcard match against the user name of the logged-on user. This is generally the same as the %username% environment variable.

### Browse...:

The browse button launches the [User Browser](#).

#### Note

It is possible that a user may appear in the list but still not be resolvable on the network into a SID. If this is the case an error message will be presented when the user is selected from the browser. If the SID of the user is known, it can be manually inserted into the raw XML for the filter.

#### Wildcards

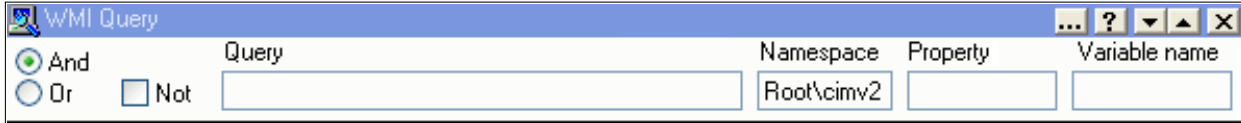
When "Match by SID" is not selected, the user name field supports any combination of the standard wildcards \* (multiple character) and ? (single character). For example:

"User?" will match User0, User9, UserW, but not User01 or User

"Us\*er" will match User, Us1er, Us123er



## WMI Query



<input checked="" type="radio"/> And	Query	Namespace	Property	Variable name
<input type="radio"/> Or <input type="checkbox"/> Not		Root\cimv2		

This filter returns true if one or more class instances are returned by the query.

**Not:**  
Reverses the result of this filter.

**Query:**  
The WMI query text.

**Example:**  
This WMI query will return true if the computer is set to the US Eastern time zone (EST):

`Select * from win32_timezone where bias = -300`

**Namespace:**  
The namespace in which to execute the query. The default value is "Root\cimv2".

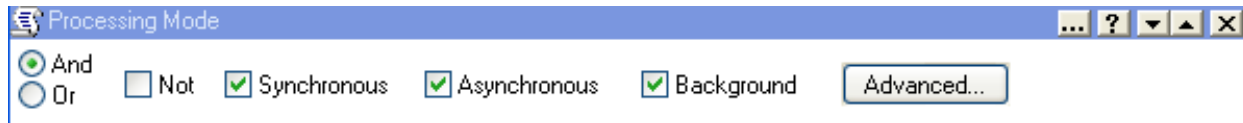
**Property (optional):**  
Specific property to look for in the first returned class instance, for example:

`DaylightName`

**Variable name (optional):**  
Environment variable that will be set to the value of the specified Property in the first returned class instance.

This value of the Property will be "`Eastern Daylight Time`" if the above query example returns true.

## Processing Mode



This filter returns true if any of the Group Policy processing modes selected match the mode currently in effect or if any of the processing flags selected are currently in effect. See the [Policy Processing](#) topic for more information on Group Policy processing modes.

### Not:

Reverses the result of this filter.

### Synchronous:

Group Policy is being processed in synchronous foreground mode. The logon (user policy) or startup (computer policy) process waits for Group Policy to be applied before continuing.



#### Note

Windows 2000 and Windows Server 2003 process Group Policy in this mode by default.

### Asynchronous:

Group Policy is being processed in asynchronous foreground mode. The logon (user policy) or startup (computer policy) process does not wait for Group Policy to be applied before continuing.



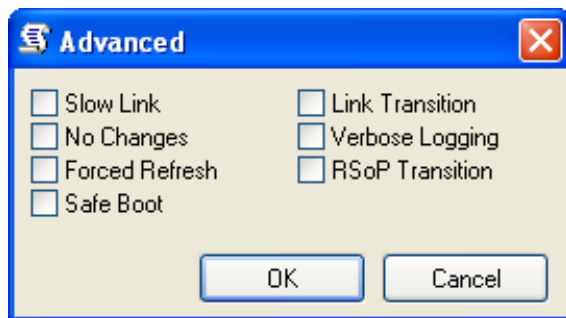
#### Note

Windows XP processes Group Policy in this mode by default.

### Background:

Group Policy is being processed in background refresh mode.

### Processing Flags (Advanced)



### Slow Link:

Group Policy is being applied across a slow link.

### No Changes:

There were no changes to any the Group Policy Objects linked to this user or computer.

### Forced Refresh:

A forced Group Policy refresh is being applied.

### Safe Boot:

Windows is running in safe mode.

### Link Transition:

A change in link speed was detected between the application of the previous policy and the application of the current policy.

### Verbose Logging:

Verbose output to the event log is in effect.

### RSOP Transition:

A change in RSoP logging was detected between the application of the previous policy and the application of the current policy.

---

© 2005 DesktopStandard Corporation. All Rights Reserved.