PowerBroker® for Windows® Release Notes

This document provides an overview of the new features and enhancements implemented in this release of PowerBroker® for Windows®. For detailed information on new functionality, see the documentation.

PowerBroker® for Windows® 7.8.0.21 - 14 December 2018

INFORMATION

Microsoft Windows 10 Update 1809

PowerBroker for Windows 7.8.0.21 is compatible with the Microsoft Windows 10 Update Version 1809 Build 17763. There are no changes to the 7.8.0.21 release.

PowerBroker® for Windows® 7.8.0.21 - Released 30 November 2018

NEW FEATURES

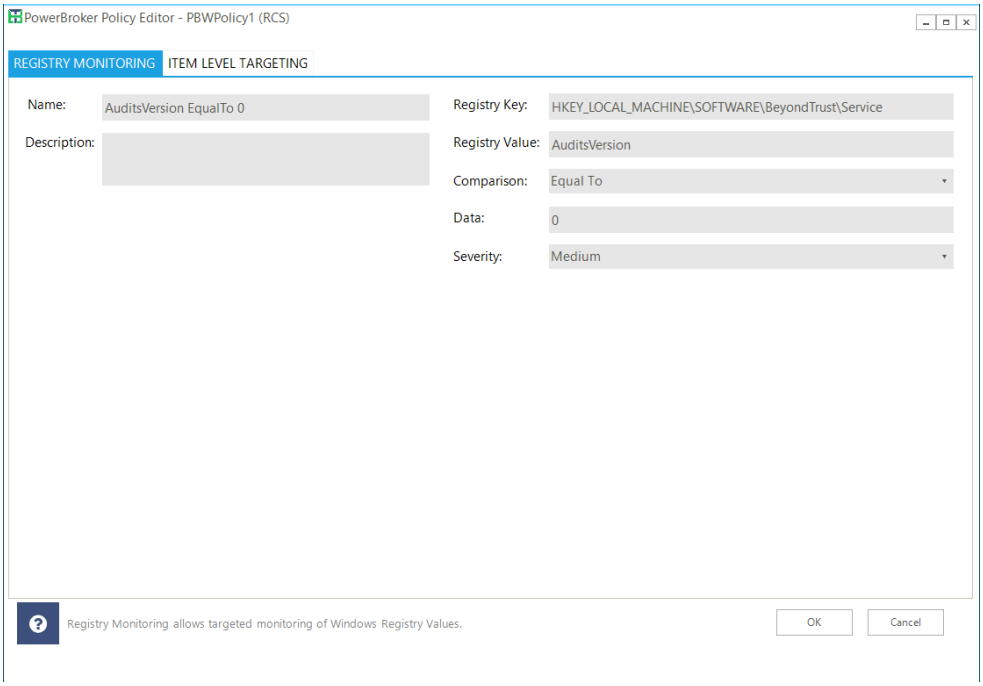
Registry Monitoring (#157394)

A new rule type has been added that enables you to monitor specific registry keys for changes to the expected values. Registry Monitoring rules are processed according to the Discovery Scan interval, and requires those components to be installed and enabled on the client machines. A Registry Monitoring rule activates when the data matches the parameters configured in the PowerBroker Policy Editor. An audit event is then forwarded to BeyondInsight.

The following registry hives are supported:
HKEY_LOCAL_MACHINE (HKLM)
HKEY_USERS (HKU)

The following registry hives are NOT supported, since they are shortcuts to other keys:
HKEY_CLASSES_ROOT: Use HKEY_LOCAL_MACHINE\SOFTWARE\Classes
HKEY_CURRENT_CONFIG: Use HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current
HKEY_CURRENT_USER: Use HKEY_USERS\[CURRENT_USER-SID]

IMPORTANT: BeyondInsight 6.8 or higher is required for reporting on events generated by this feature. Additional documentation is included in the PowerBroker for Windows User Guide.



NOTE: Drag and drop importing of rules only works for .xml files - .reg files need to be imported using the right click menu. No more than 50 Registry Monitoring rules may be created.

ENHANCEMENTS

Policyupdate /force (#139148)

Policyupdate.exe now supports a /force flag. This will require the policy to be sent down from BeyondInsight and the client to apply the policy, regardless of whether or not a change was made to the policy.

UVM Appliance Support (#140453)

PowerBroker for Windows now provides protection for BeyondTrust UVM Appliances.

Local User Policy (#142640)

Local Users are now supported for BeyondInsight policy deployment.

Export Option (#111424)

A button was added in Central Policy Mode to export all rules and settings with a single click.

FIXES

Right-Click Menu Performance (#155935)

A performance improvement was made to the speed with which the right-click menu option is displayed. Rule precedence for Hash and Publisher Rules is now applied when the "Run Elevated" option is selected. If a higher priority Deny rule is in place, the user will see the following message after selecting the Run Elevated option: "You have no permissions to launch [appname] elevated".

Microsoft Outlook: ost file in use (#158319)

A fix was implemented to prevent an error that the ost file is in use when whitelisting rules are in place.

Certificate Name (#162645)

A fix was implemented for when the certificate subject or issuer values contained an "=" character.

User Message Justifications (#164939)
User messages now allow the administrator to delete all preset justifications.

File Integrity Events - User Name (#16511)
File Integrity events now send the user name to BeyondInsight.

PBPS User Name (#155518)
The name of the logged in user (not the RunAs user) is now displayed in PowerBroker Password Safe events.

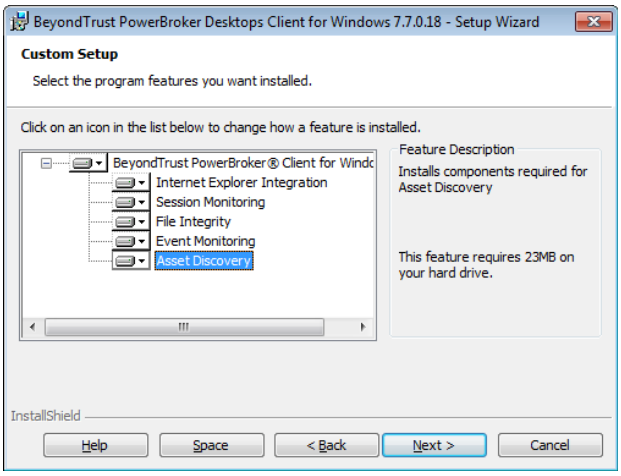
Password Safe Progress Bar (#143883)
The Password Safe progress bar window is no longer the forced active window on top of the credentials window.

PowerBroker® for Windows® 7.7.0.18 - Released 28 September 2018

NEW FEATURES

Asset Discovery (#154382)

This feature provides you with the ability to run a scan detailing out the Hardware, Ports, Processes, Scheduled Tasks, Services, Shares, Software and Users on the local machine. The client installer has a new option to install the Asset Discovery feature:



To install this option via the command line, use "RetinaDiscovery_x64" or "RetinaDiscovery_x86" as the feature name. For example, to install all features on a 64-bit OS, the following command line would be used:
PowerBroker for Windows Client (64 Bit) 7.7.msi /qn
ADDLOCAL=PBWClient,CPIntegration,Client_x64,EventMonitor_x64,FileIntegrity_x64,IEIntegration_x64,RetinaDiscovery_x64,Runtime_x64,SessionMonitor_x64 SERVER=[SERVERNAME]
CERTIFICATE=eEyeEmsClient WORKGROUP="BeyondTrust Workgroup"

The scan can be started manually by running the following executable: c:\Program Files\Beyondtrust\PowerBroker for Windows Client\Tools\discovery.exe. The scan data will then be forwarded to the configured BeyondInsight server upon completion of the scan.

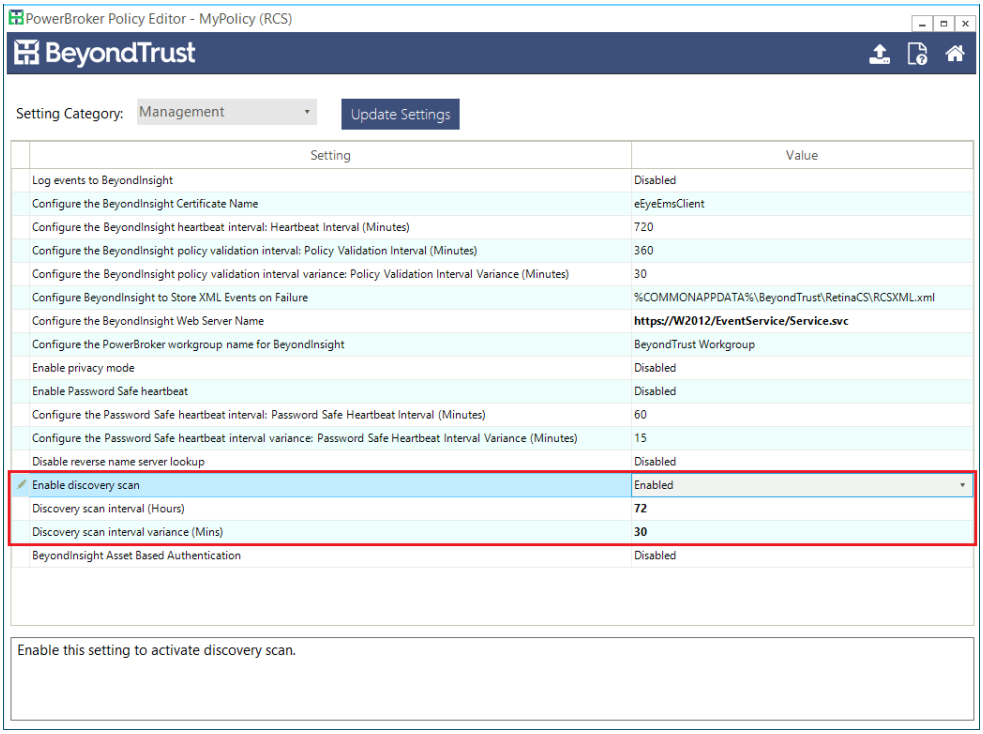
A scan can also be set to run on a schedule via the following settings:

Enable discovery scan: Run discovery either according to a specified interval or manually.

Discovery scan interval (Hours): Enter the number of hours between scans.

Discovery scan interval variance (Minutes): Set the scan interval variance in minutes. This is a range for a random offset value to be added to the scan interval.

NOTE: All three settings must be configured in order for scheduled scans to run.



FIXES

UAC Prompt Logging (#149206)
UAC Prompts are now logged correctly.

Quarantined Files (#156204)
Files are now moved to the Quarantine folder when a rule is applied.

Modification of Installed Features (#159569)
Reconfiguration of the agent to include features or change central policy requires an uninstallation and reinstallation of the product to prevent unauthorized tampering.

PowerBroker® for Windows® 7.6.0.18 - Released 10 August 2018

INFORMATION

Quarantine Rules (#156204)

When a Quarantine rule is applied the targeted application is blocked, but not moved to Quarantine in PowerBroker for Windows 7.5.1/7.6. This will be addressed in a future release.

NEW FEATURES

PowerBroker Password Safe Events (#140524)

Added the ability to test current passwords and log events containing the results. Also added new events for password change requests and any resulting errors. The following events are logged in PowerBroker for Windows 7.6:

28709 - PowerBroker for Windows processed the following password changes from Password Safe.
This event displays the user names for any passwords that were changed, along with the status result of the change.

28710 - PowerBroker for Windows failed to process the following password changes from Password Safe.
This event will display any errors from password change results.

28711 - PowerBroker for Windows processed the following password tests from Password Safe
This event displays the user names for any passwords that were tested, along with the status result of the test.

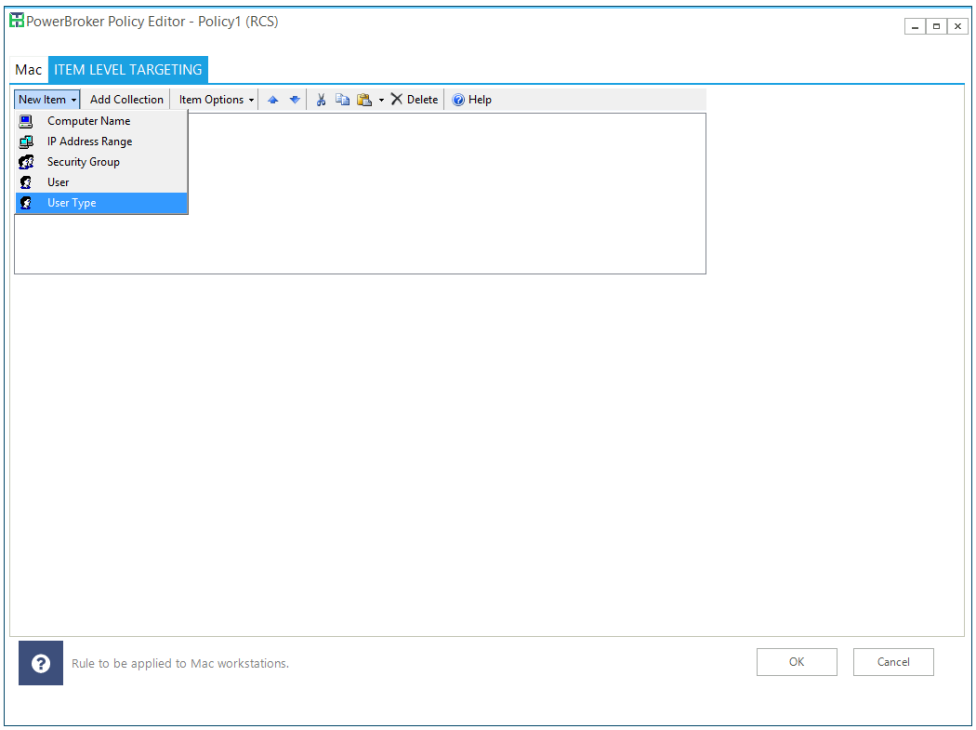
28712 - PowerBroker for Windows encountered failures while performing the following password tests from Password Safe.
This event will display any errors that happened from password test results.

NOTE: These events are logged to the System Event Log as well as BeyondInsight.

Item Level Targeting for Mac (#133086)

Item Level Targeting for Mac is now supported. Computer targeting options include Computer Name and IP Address Range. User targeting options include Computer Name, IP Address Range, Security Group, User, and User Type.

NOTE: PowerBroker for Mac 1.5 is required for this feature.



FIXES

Policy Editor Login (#147749)

The Policy Editor now allows multiple login attempts on invalid user name or password.

Central Policy: Item-Level Targeting (#148550)

Item-Level Targeting now works correctly when targeting registry keys within HKEY_CURRENT_USER for user policies deployed via central policy.

Editing VBS/BAT Files on DFS Shares (#150802)

Resolved an issue with users being unable to edit .VBS and .BAT files stored on DFS Shares when PowerBroker for Windows was installed.

Item-Level Targeting (#147742)

A display issue with Operating System Item-Level Targeting was resolved.

PowerBroker® for Windows® 7.5.1.8 - Released 8 June 2018

FIXES

High CPU Usage (#143033, #144946)
A performance enhancement was made to address high CPU usage under certain scenarios.

Performance Enhancement (#144328)
A performance enhancement was made when publisher or hash rules are in use.

Issue Stopping Driver (#145304)
A system crash issue while stopping the privman driver has been fixed.

Right-Click Options (#146796)
Performance has been improved when right-clicking on a large file with Hash or Publisher rules in place.

NOTE: When a Shell rule is in place, there may still be a delay in the menu appearing the first time a file is right-clicked. Subsequent right-clicks should be faster.

Diagnostics Application (#148823)
The Diagnostics Application now works correctly when Session Monitoring components are not installed.

PowerBroker® for Windows® 7.5.0.18 - Released 17 May 2018

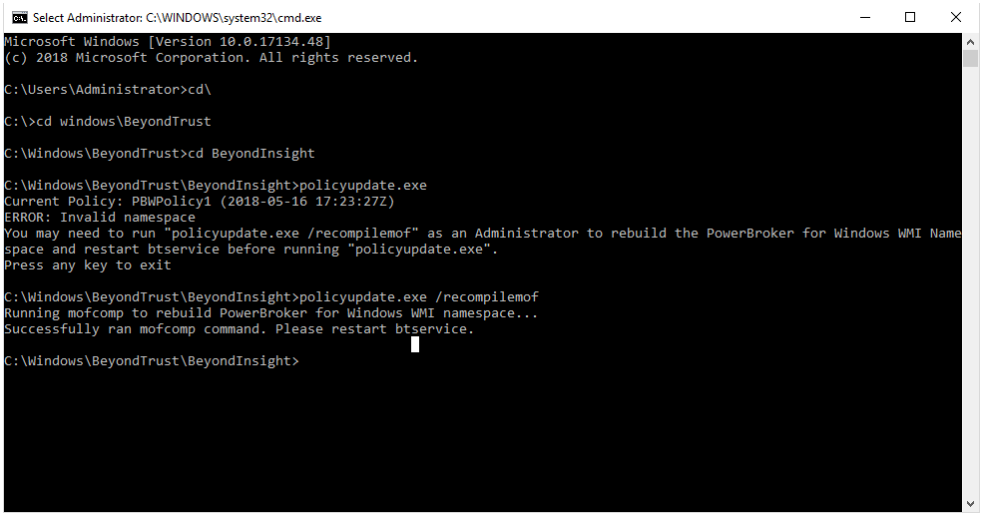
INFORMATION

Windows 10 April 2018 Update (1803) Support

The Windows 10 April 2018 Update, Version 1803 Build 17134 is now supported.

NOTE: The Microsoft Windows 10 1803 update deletes the PowerBroker for Windows WMI data. If you are using Central Policy Mode, regular policy validate events will still occur after the Windows 1803 update completes. However, if you are manually updating policy using the policyupdate tool, you may see an error: "Invalid namespace."

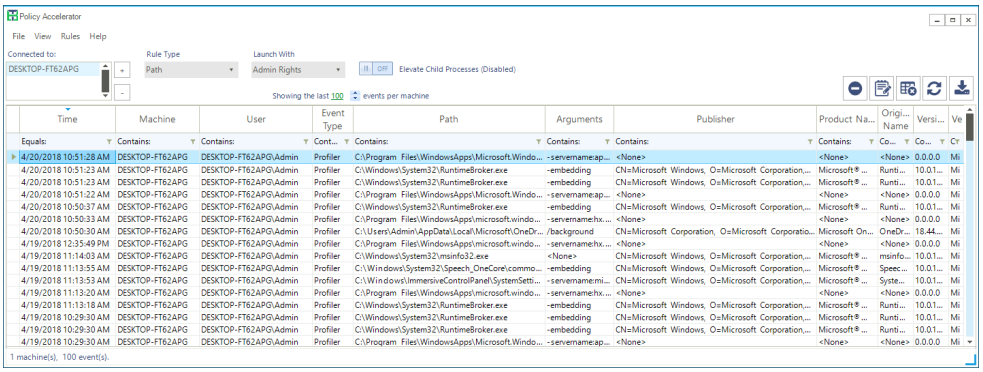
If this error occurs:
1. Open an elevated command prompt and run "policyupdate /recompilemof"
2. Run "sc stop btservice"
3. Run "sc start btservice"



This will re-add the PowerBroker for Windows data to WMI. This command will only need to be run once after the 1803 upgrade, and only if you are using the policyupdate tool to manually update policy.

NEW FEATURES

Policy Accelerator (#133091)



Policy Accelerator is a tool now included in the Policy Editor installer. This utility is designed to connect to a local and/or network machine's System Event Logs in order to collect data on PowerBroker for Windows Events. Using these events, rulesets can be generated based on the applications that have been executed on the local or remote machine.

ENHANCEMENTS

Diagnostics Tool (#133094)

The Diagnostics Tool user interface has been updated. New options for troubleshooting data collection have been added.

Item-Level Targeting: Cross-Domain Support (#81473)

Item-level targeting has been improved to support targeting objects from different domains.

NOTE: The user creating the rule must have rights to view the objects in the other domain.

Publisher Rule: Signed PowerShell Scripts (#128409)

You can now create Publisher Rules on signed PowerShell scripts.

NOTE: This option only works when you right-click the script and choose Run with Powershell, or run the command "PowerShell [path].ps1". This does not work if you are running the script from a PowerShell window that is already open.

Privman Exclusions (#135142)

The privman exclusion (ExcludedApps) has been enhanced to improve compatibility with third party software such as VirtualBox.

NOTE: For the low-level exclusion to take place, environment variables must NOT be in use. If environment variables are in use privman will still be loaded into the process but will be inactive. Wildcards may be used.

Uninstall Applications (#139235)

Creating rules to target uninstalling specified applications using the ProductCode GUID is now supported. To uninstall an application from Programs and Features, create a path rule with the path set to "c:\windows\system32\msiexec.exe" and the arguments set to "/x {GUID}", where {GUID} is the ProductCode for the install package . Polmon now displays the guid during uninstall to assist with rule creation.

APPLICATION: C:\Windows\system32\msiexec.exe
ARGUMENTS: /x {GUID}

UAC Prompt Logging (#141064)

UAC Prompt logging was improved to include more events.

NOTE: There may still be certain cases where the UAC prompt does not log events. This will be investigated for further improvement in a future release.

FIXES

Process Security Options - Add Admin Rule (#99542)

The Add Admin rule was updated to include the following two options by default on rule creation:

PROCESS_SET_QUOTA - regulates how much memory is reserved for process
PROCESS_SUSPEND_RESUME - allows to suspend/resume process

When an existing rule is in place that does not contain these options, right-click Run As Administrator may fail with the error: "Error: Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."

NOTE: If you have existing Add Admin token rules for the applications you are trying to right-click and Run as Administrator, you will need to enable the above Process Security Options manually in those rules by either changing to a custom token rule or re-creating the rule.

Shell Rule: Shortcut Links (#120202)

A fix was implemented for certain scenarios where a Shell rule was not applied correctly to applications launched via a shortcut.

Session Monitoring (#135749)

Session Monitoring data is now sent to BeyondInsight correctly when the .NET Framework 4.5 is installed and TLS 1.2 is in use.

Crash on Upgrade (#135567)

An intermittent crash on upgrade was resolved.

Trace Logging (#131762)

An improvement was made to pmsd trace logging.

LSA Protection (#131780)

An issue was resolved when LSA Protection was enabled with secure boot on: "Rule --NOT-- Applied" was shown in polmon.

Windows 10: Rule --NOT-- Applied (#142352)

An issue was resolved on certain Windows 10 machines that would cause "Rule --NOT-- Applied" to be displayed in polmon.

File Integrity: User Policy Rules (#132004)

File Integrity rules deployed via user policy are now applied.

Dynamic Rules (#132352)

Dynamic Rules now work when files are copied using Windows Explorer on Windows 7.

Asset Policy Removal (#132997)

Asset-based rules distributed via Central Policy are now removed when the policy is no longer assigned to the machine.

Heartbeat Interval and Variance (#133565)

The heartbeat and interval variances now have a minimum value of 1.

Default Heartbeat Interval (#131768)

The default Heartbeat interval has been changed to 12 hours from 6.

Rule Wizard (#133708)

The Rule Wizard now captures the "CN=" data for Publisher rules.

ADMX files (#136845)

The version number has been updated in the ADMX file.

McAfee ePO Client version (#144278)

The PowerBroker for Windows client now reports the correct version number to McAfee ePO.

Asynchronous Event Logging (#121003)

Asynchronous event logging was updated to match the response with the proper event.

PowerBroker® for Windows® 7.4.0.15 - Released 23 February 2018

INFORMATION

Windows 10 Fall Creator's Update (#134068)
Windows 10 Fall Creator's Update (RTM 1709 Build 16299) is now supported.

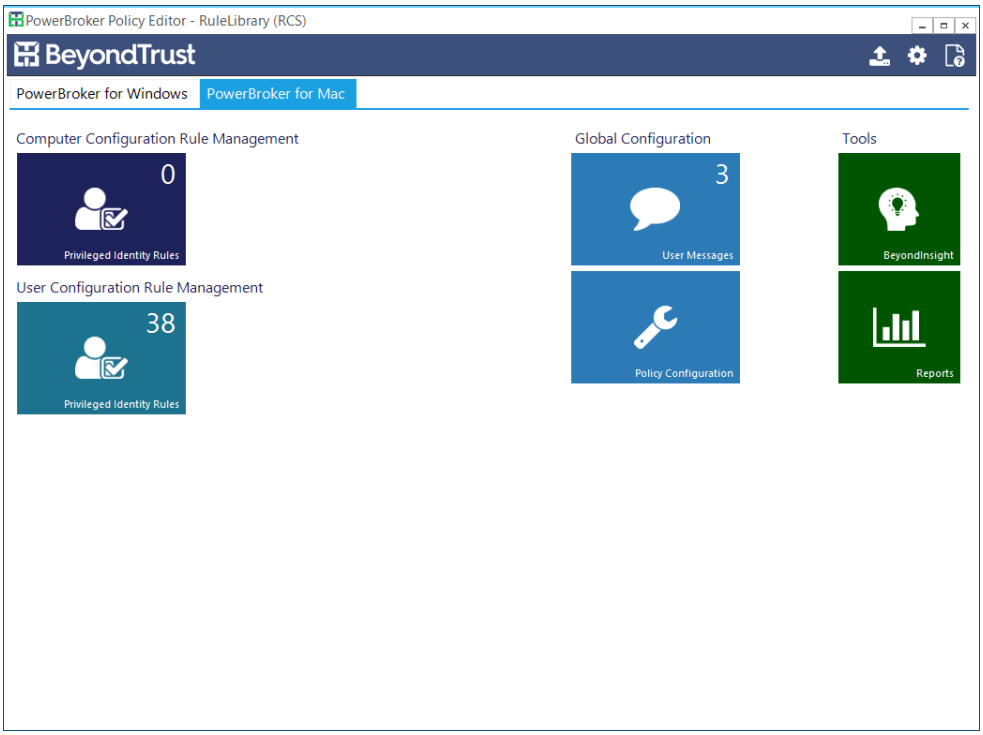
Heartbeat Variance Settings (#133511)
The variance settings for heartbeat intervals should not be set to 0. The user interface will prevent setting these values to 0 in a future release.

Command Line Install (#131299)
To install in ePO mode via the command line, the following string must be added to the ADDLOCAL option:

ADDLOCAL=EpoIntegration,EpoIntegration_x64
or
ADDLOCAL=EpoIntegration,EpoIntegration_x86

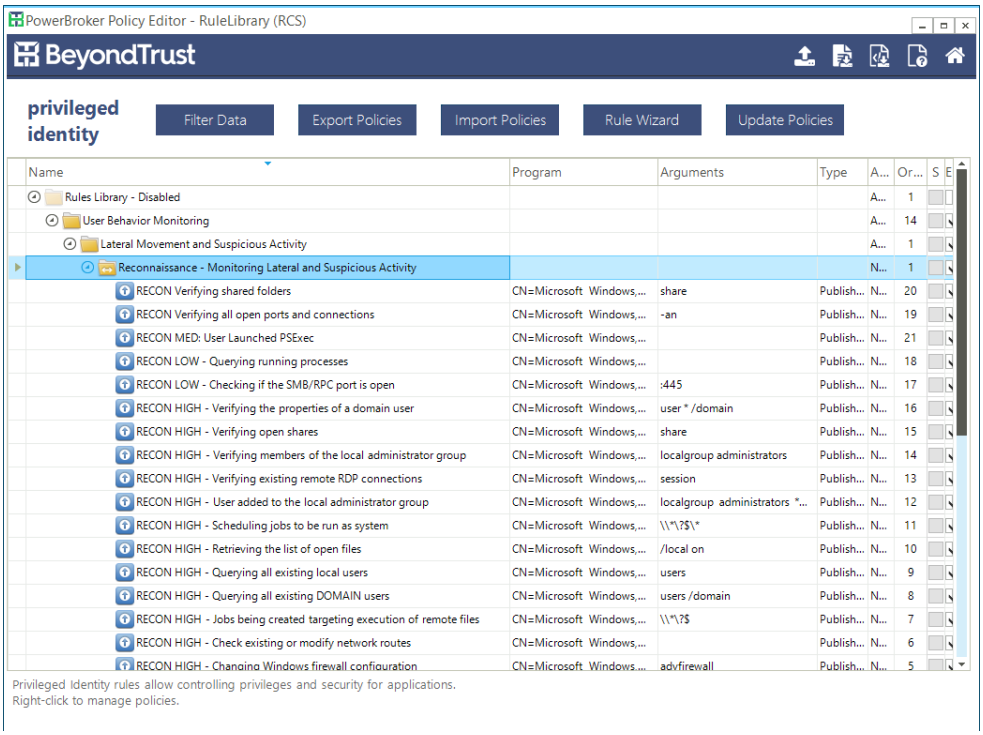
NEW FEATURES

PowerBroker for Mac User Policy (#120452)
The Policy Editor now supports creating user-based PowerBroker for Mac policies.



Lateral Movement Rules (#116985)

The Rule Library now includes a set of Lateral Movement and Suspicious Activity rules. These rules can be used to track methods used by threat actors to gain deeper access and a higher set of privileges in a network, suspicious behavior and potential threats.



ENHANCEMENTS

Password Safe Event Logging (#122695)

Password Safe Event Logging was expanded. Event logs now include password changes (28709) and failures (28710). Heartbeats (28706) and password changes (28709) are logged to the PBWriteToFile log.

Rule Library Updates (#109342)

The Rule Library has been updated. The Publisher Rules now contain CN= data and the Java rules have been updated.

Security Software Compatibility (#117242)

Compatibility has been improved with third party security software, including TrendMicro, AVG, and Cylance.

FIXES

TestConnection (#109699)

TestConnection now errors gracefully when run as a limited user.

Deny Rules (#109291)

Deny Rules are now applied consistently when "Run As Administrator" is selected.

Passive Rules (#118969/#112716)

An issue with Passive Rules was resolved.

Publisher Rules (#11481)

Matching was improved for Publisher rules.

Credential Guard (#116548)

High CPU usage no longer occurs when Credential Guard is enabled.

Publisher Rules (#121654)

Publisher rules now match correctly when there is a comma in the data.

McAfee ePO Mode (#122314)

Memory usage has been improved when McAfee ePO is used for policy distribution.

Multifactor Authentication (#124010)

An issue was resolved with authentication when using MSCHAPv2.

McAfee ePO (#124439)

PowerBroker for Windows now handles upgrades correctly when the client is deployed via McAfee ePO.

Passcode Generator (#127453)

Key Pairs are now generated successfully from within the Policy Editor.

User Policy (#120123)

User Policies are now applied correctly regardless of whether or not an asset based policy is applied.

Trace Logging (#120123)

Improvements were made to RetinaEvents trace logging.

TestConnection (#120851)
TestConnection now checks the updated registry location for the installerID.

Memory usage (#121171)
Memory usage was improved when the RCSXML file increases in size.

Initial heartbeat (#122134)
On install, the initial heartbeat no longer sends an empty InstallIdentifier string.

File Integrity (#123820)
The Publisher drop-down in File Integrity rules now works correctly.

Compatibility Mode (#124740)
Improvements were made to compatibility mode.

PowerBroker for Mac Policy Export (#124944)
PowerBroker for Mac policies now export correctly.

Special Character encoding (#125505)
Improvements were made to handle special character encoding for rules, specifically ampersands.

Uninstall (#130696)
The authentication folder is now removed on uninstall.

Btservice (#132161)
Changes to improve btservice stability were made.

PowerBroker® for Windows® 7.3.1 - Released 30 October 2017

INFORMATION

McAfee Endpoint Security (ENS)

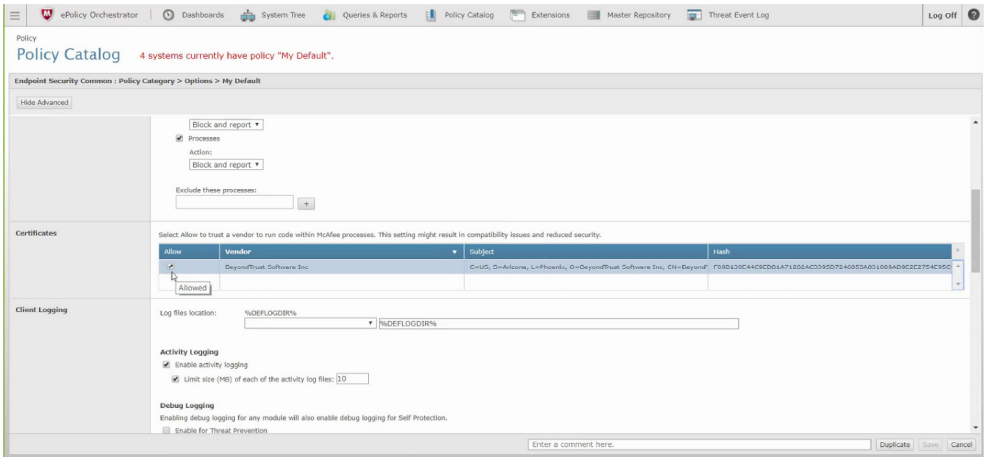
If McAfee Endpoint Security is installed prior to the BeyondTrust PowerBroker for Windows Client, an event with Event ID 34865 – "Malware Detected" will be generated. This occurs due to the fact that the PowerBroker for Windows Client installer copies privman64.dll to the Windows\System32 folder. This action is detected as a malicious activity by ENS if the BeyondTrust certificate has not been added to the trust store.

To prevent this issue, prior to deploying PowerBroker for Windows, the BeyondTrust certificate should be configured as as a trusted certificate in the ENS policy. ENS will then consider the BeyondTrust certificate as trusted and will allow BeyondTrust code to run within McAfee processes.

NOTE: If this policy is not configured, a large number of events may be generated.

To add certificate to the trust store:

Endpoint Security Common: Policy Category > Options > My Default > Certificates > Check "Allow" for BeyondTrust and save the policy. Enforce the policy on clients and once policy is enforced, send the deployment tasks.



NEW FEATURES

McAfee ePolicy Orchestrator 5.9

PowerBroker for Windows now supports McAfee ePolicy Orchestration 5.9. There is a separate ePO 5.9 PowerBroker for Windows extension that must be installed in order to use ePO 5.9 with PowerBroker for Windows.

ENHANCEMENTS

Risk and Compliance Rules (#107836)

Risk and Compliance Rules are now supported for policy distribution in ePO Mode.

NOTE: BeyondInsight is still required in order for the clients to download audit data.

Enforce BeyondInsight Connection Settings (#113611)

A new setting was added to the Troubleshooting section. When enabled, this will force the clients to update the BeyondInsight Connection settings from the policy. With this setting enabled, the client-side settings will be overwritten with the settings from the policy, regardless of if the policy settings are the defaults.

User Interface Controls (#108428)

The Telerik controls were upgraded.

FIXES

Privmanfi events (#113202)

Privmanfi will no longer attempt to self-heal when the driver is not present. This was generating many events with the following path: "C:\WINDOWS\System32\RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultInstall 128 C:\WINDOWS\System32\BeyondTrust\driverFI\privmanfi.inf".

McAfee ePO: Policy Editor Time Out (#111555)

An issue was resolved with a licensing timeout when retrieving policies from ePO.

Cylance PROTECT (#109341)

A fix was implemented to improve compatibility with Cylance PROTECT.

Parsing Issue (#107725)

A path parsing issue was resolved when applying rules to a script.

Collections: UI Issue (#106977)

An issue with the "Enforce Action" checkbox was resolved. The Cancel button now works correctly when editing a collection.

Blocked Messages (#107349)

Blocked user messages now appear correctly for applications that are launched from the immersive control panel and match Deny rules.

PowerShell: Command Line Windows (#109261)
Command line applications no longer launch in a new console window when executed from PowerShell and a rule is applied.

Licensing issue (#108720)
A fix was implemented to resolve an intermittent license processing issue.

Renaming a policy (#109083)
Renaming a policy now works correctly in Central Policy Mode.

Compatibility Mode (#114172)
Compatibility Mode is functional again in PowerBroker for Windows 7.3.1. This option may not be used when Secure Boot is enabled.

Rules Display Issue (#111182)
The correct rules are now displayed when clicking on tiles and both computer and user rules are in place.

File Integrity and Publisher Info (#113208)
File Integrity rules that contain Publisher Info no longer cause issues at logon or with launching applications.

User Message Fields (#113026)
User Message fields for user name and password now display the correct values on the client.

McAfee ePO: Error handling (#104683)
When attempting to connect to ePO with invalid credentials, an unauthorized error message is now displayed.

Shell and Path rule (#105188)
A duplicate user message is no longer displayed when both Shell and Path rules are applied. When a Path rule supercedes a Shell rule the Run Elevated option is no longer displayed.

Collections: Imported rules (#107534)
When rules are imported under a collection, the Rule Action enforcement is now correctly applied.

ePO and Policy Editor (#110532)
Closing the policy editor prior to saving a modified policy no longer results in an unhandled exception.

PasswordSafe and Multifactor Authentication (#115714)
Multifactor Authentication now works correctly when used with a PasswordSafe user message.

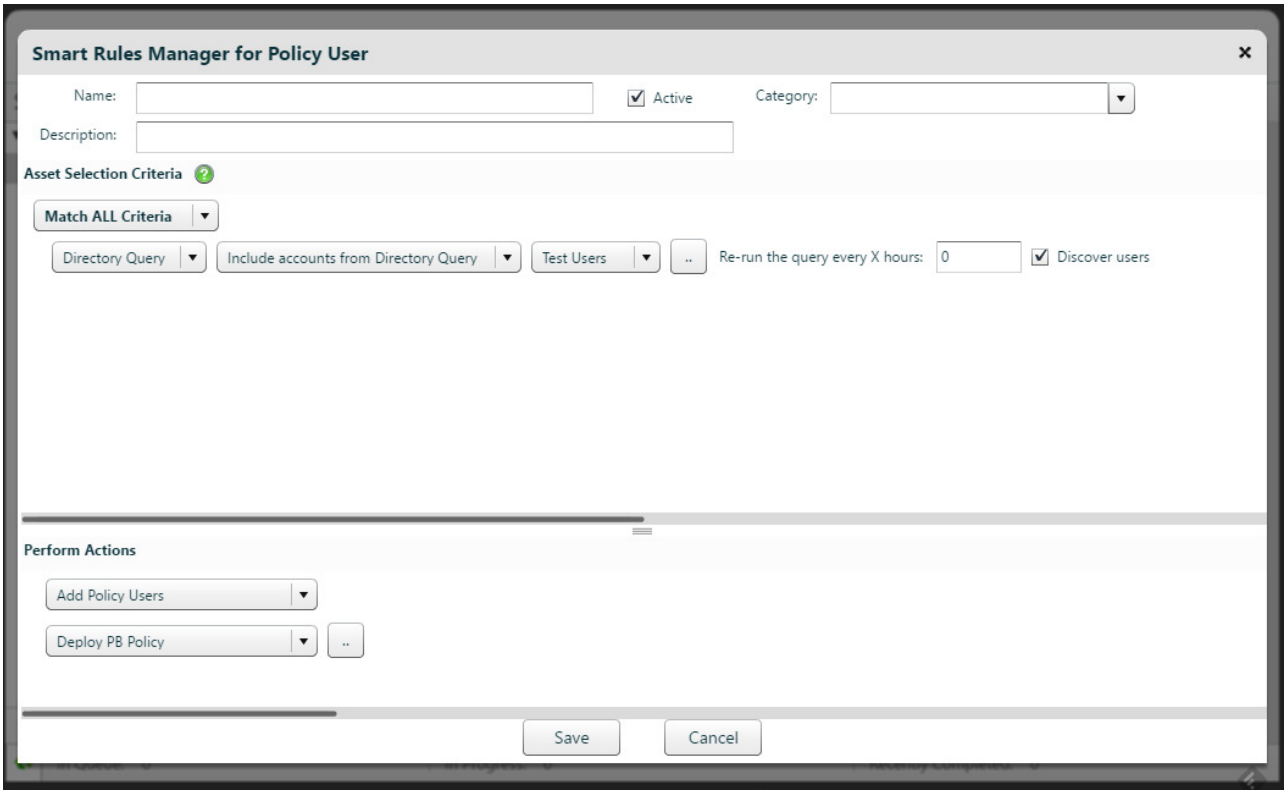
Rule Library (#112639)
A rule for the Directory Utility was added to the Mac default rules.

PowerBroker® for Windows® 7.3 - Released 28 June 2017

NEW FEATURES

User Based Policy in Central Policy Mode (#80896)

Central Policy mode now is able to assign user based policies. In order to create a smart group that targets policy users, the user account must be available via a BeyondInsight Directory Query.



Publisher Rules: Support for "CN=" (#80917)

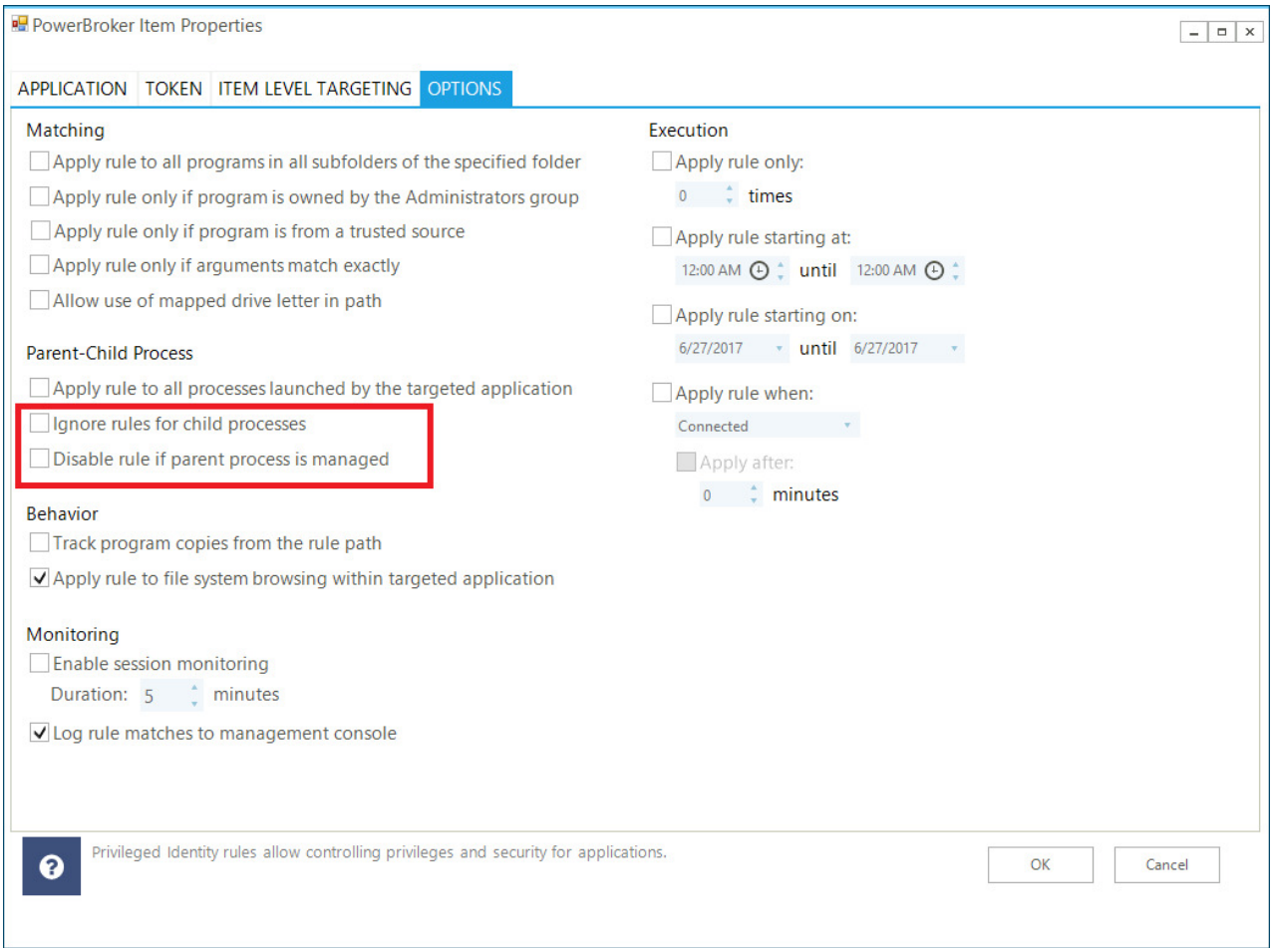
Added support for "CN" information in the publisher details.

Publisher Rules and Wildcards (#80918)

Added support for wildcards in the publisher details.

Parent/Child Process Options (#82488, #80899)

Added the ability to bypass rule matching if the parent process is managed by PowerBroker for Windows. On the Options tab, there are now the options to "Ignore rules for child processes" and "Disable rule if parent process is managed":



Ignore rules for child processes
Child processes of the targeted application will not have any further rules applied if "Apply rule to all processes launched by the targeted application" setting is checked. This checkbox is compatible with all actions: Add Admin, Custom Token, No Change (Passive), PowerBroker Password Safe, and Deny rules.

Disable rule if parent process is managed
Do not apply the rule if the parent process has a rule applied. This checkbox is compatible with all actions: Add Admin, Custom Token, No Change (Passive), PowerBroker Password Safe, and Deny rules.

Shell Rules and Rule Order (#94867, #94287)

Shell Rules (SHELL_RULE_V2) now process in order with other rule types. The Shell rule now lists the path name instead of btes.exe with arguments. The Shell rule will be applied according to precedence with other rules.

NOTE: "Ignore rules for child processes" is always checked on the Shell rule. Once a Shell rule is applied, no further rules will apply. Rules created in older versions of PowerBroker for Windows will continue to work the same as in the past (i.e. the old Shell rules will continue to ignore precedence with other rule types).

The Shell rule may accept for elevation files which are not technically executable. For example, if you create a link (.lnk), a low priority SHELL rule will be applied, as a DENY rule would not match for mspaint.exe.lnk.

Trusted Sources (#83924)

There is a new option to "Apply rule only if program is from a trusted source." When this option is enabled, the rule will not apply to applications downloaded from the internet by Internet Explorer, Edge, Chrome, Firefox, or files copied from or located at external drives, such as USB, CD/DVD. The rule will apply when the application is executed from a local or network drive.

Track Program Copies From the Rule Path (#99531)

Path rules only. If an executable is copied from the location specified in the rule, PowerBroker for Windows will still apply the rule when the application is run from the new file location. Dynamic hash rules are created for targeted applications that are copied to a new location.

User Messages: Default Image Size (#80047)

Added the default image size for banner images in user messages.

ENHANCEMENTS

Support Package Tool (#89364)

The PMIE log and network adapter information is now included in the support package details.

Compatibility with Antivirus Programs (#103514/#97531)

Improved compatibility with Trend Micro OfficeScan and Kaspersky Antivirus.

Item Level Targeting (#96489/#104524)

The user SID now refreshes correctly in Item Level Targeting.

PBPS Rules and Variables (#65695)

Variables are now supported for PowerBroker Password Safe rules. The %username% variable should be used in conjunction with user-based rules.

FIXES

User Interface Error (#103099)
An unhandled exception no longer occurs when adding custom permissions on Windows 10 Creator's Update.

MOF recompile (#104423, #102563)
The polsecc.mof and polsecu.mof files are now automatically recompiled on gpupdate.

NOTE: This does not replace all WMI data deleted by the Microsoft Windows 10 upgrade, but it does eliminate the errors on gpupdate.

Maximize Button (#97228)
The maximize button on the policy editor now works correctly.

Multifactor Authentication Error (#98794)
Resolved an issue with Multifactor Authentication failing with Microsoft .NET 4.0 or higher on the client machine.

Illegal characters (#105585)
The "<" and ">" symbols in a path no longer cause an unhandled exception in the policy editor.

PowerBroker® for Windows® 7.2.2 - Released 5 May 2017

INFORMATION

Multifactor Authentication

If PowerBroker for Windows user messages are configured to use Multifactor Authentication, currently the Microsoft .NET Framework 3.5 must be installed on the clients.

ENHANCEMENTS

Windows Server 2016 (#85718)

PowerBroker for Windows now supports Microsoft Windows Server 2016. Windows Server 2016 has also been added to Item Level Targeting.

Windows 10 Creator's Update (#91452)

Windows 10 Creator's Update (RTM 1703 Build 15063) is now supported.

NOTE: If you have installed a prior version of PowerBroker for Windows on Windows 10 Creator's Update, you must stop btservice and privman, uninstall, and then reboot before installing 7.2.2.

Windows 10 Upgrades (#96170)

A registry key location was moved due to it being deleted by Windows 10 upgrades. HKLM\Software\Microsoft\Windows\CurrentVersion\BeyondTrust was moved to HKLM\SOFTWARE\BeyondTrust\PBW.

TLS 1.2 Support (#91044, #81154)

TLS 1.2 is now supported by PowerBroker for Windows. SSL3, TLS1.0, TLS1.1, and TLS1.2 are compatible with PowerBroker for Windows on multiple versions of the Microsoft .NET Framework (3.5, 4.0, 4.5, 4.6 and 4.7).

NOTE: TLS 1.1 requires .NET 4.0 or higher. TLS 1.2 requires .NET 4.5 or higher.

IMPORTANT: Upgrading from Microsoft .NET Framework 3.5 to 4.0 when PowerBroker for Windows is currently installed will *not* re-register pbwrcsclient.dll, since the 4.0 version of the framework which is required for TLS 1.1 and 1.2 must be installed first. PowerBroker for Windows must be removed and reinstalled in order to re-register pbwrcsclient.dll. Repairing PowerBroker for Windows using the client installer does *not* re-register pbwrcsclient.dll. Removal and re-install is required.

User Messages on Secure Desktop (#91988, #94848)

A new option was added to configure whether or not User Messages are displayed on the secure desktop. There is also a new option to minimize user messages when a hyperlink in the message is selected (instead of the default behavior of closing the user message).

FIXES

BTService (#81052)

A crash was resolved with btservice when PowerBroker Password Safe rules were in use.

Cryptsvc Dependency (#86556, #92289)

The installer now adds a dependency on cryptsvc to btservice. This resolves conflicts at logon time that occurred under certain scenarios (i.e. Citrix Virtual Delivery Agent).

Risk and Compliance Rules (#89026)

Older versions of Java are now detected correctly by Risk and Compliance rules.

User Messages (#89605)

An issue was resolved with user messages being deleted from the registry when there were both user and computer policies. User Messages are now only cleared when computer policy is processed.

Diagnostics Package (#81444)

The diagnostics support package now includes the pmsd backup trace log.

Command Line Applications (#85549, #81206, #84548, #80072)

A fix was added to allow command line applications to run correctly when elevated by a rule.

Session Monitoring (#83534, #66476)

An option to suppress WMI quota errors in Session Monitoring was added to the Settings. This setting may be needed when large numbers of session monitoring instances are in use on a single machine.

Passcode Generator (#88864)

A fix was added to improve support for multiple users generating passcodes on the same machine.

Policy Editor (#88300)

Using the arrow keys to navigate within the policy editor list view now works correctly.

Multiple Monitors (#52770)

Improved support for user messages being displayed on systems that have multiple monitors.

Cancel button (#80626)

The Cancel button now works correctly when changing the rule action in the Policy Editor.

User Messages and Quotes (#80663)

User Messages now support double quotes in the message body text.

User Messages: Support URL (#85184)

The Support URL link now works correctly on Blocked User Messages.

Group Policy Caching (#83825)

Support has been improved for environments where group policy caching is in use. This resolves issues with the license file not being found in a local group policy cache.

Session Monitoring (#86373)

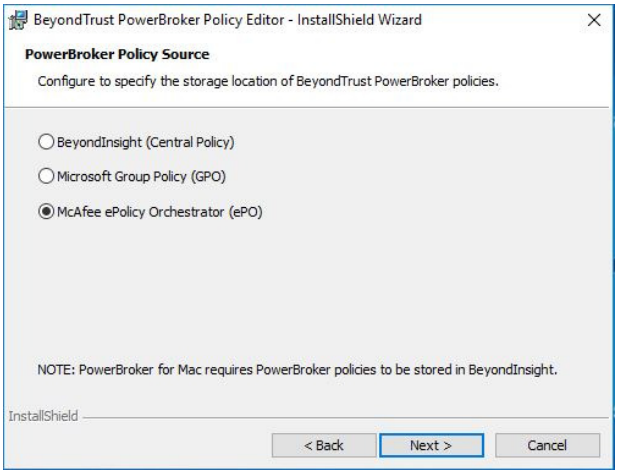
Improved support for session monitoring with different screen resolutions.

PowerBroker® for Windows® 7.2.1 - Released 16 January 2017

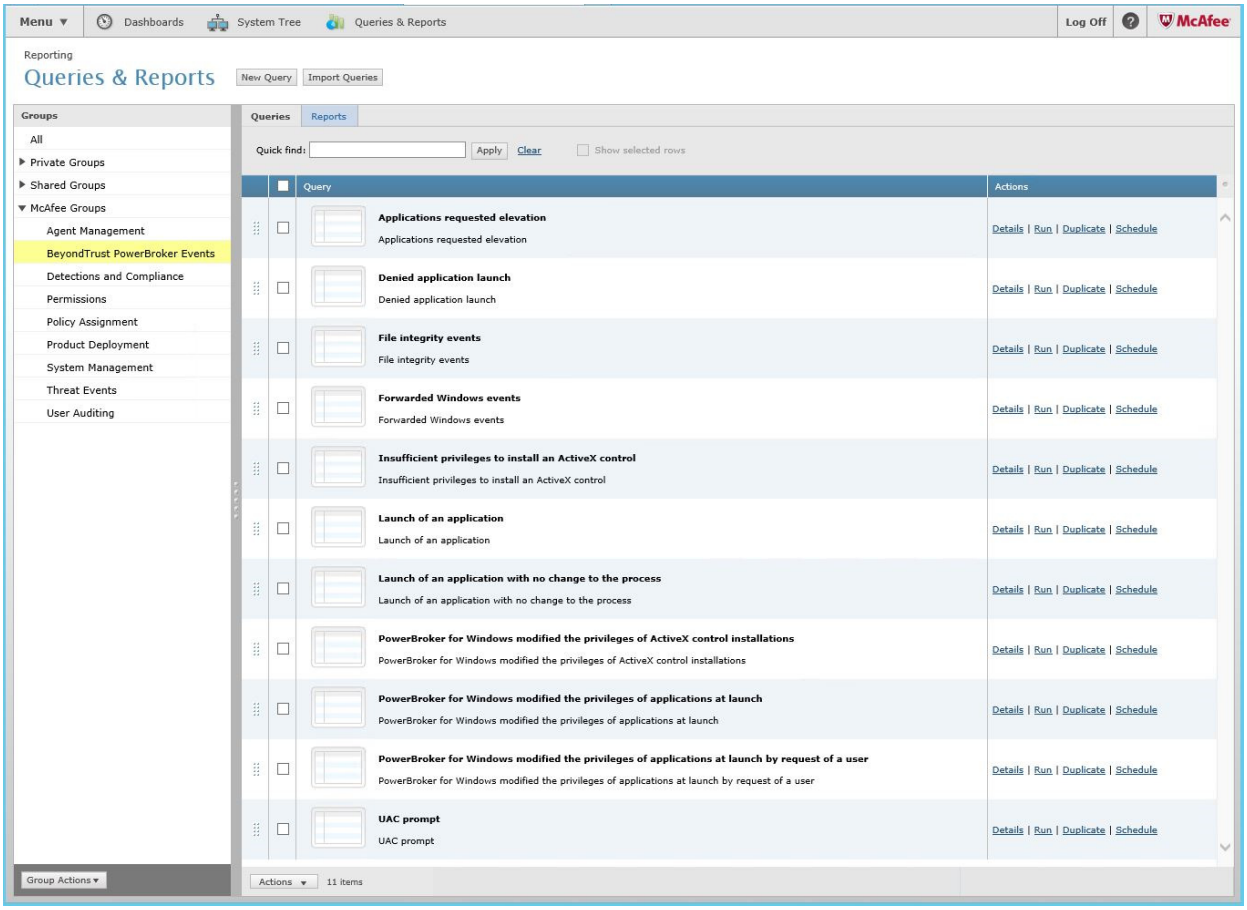
NEW FEATURES

McAfee ePolicy Orchestrator

PowerBroker for Windows is now integrated with McAfee ePolicy Orchestrator for policy distribution and logging. There is a new option in the installer to select McAfee ePO for policy distribution:



Event Logging for PowerBroker for Windows is also included within McAfee ePolicy Orchestrator:

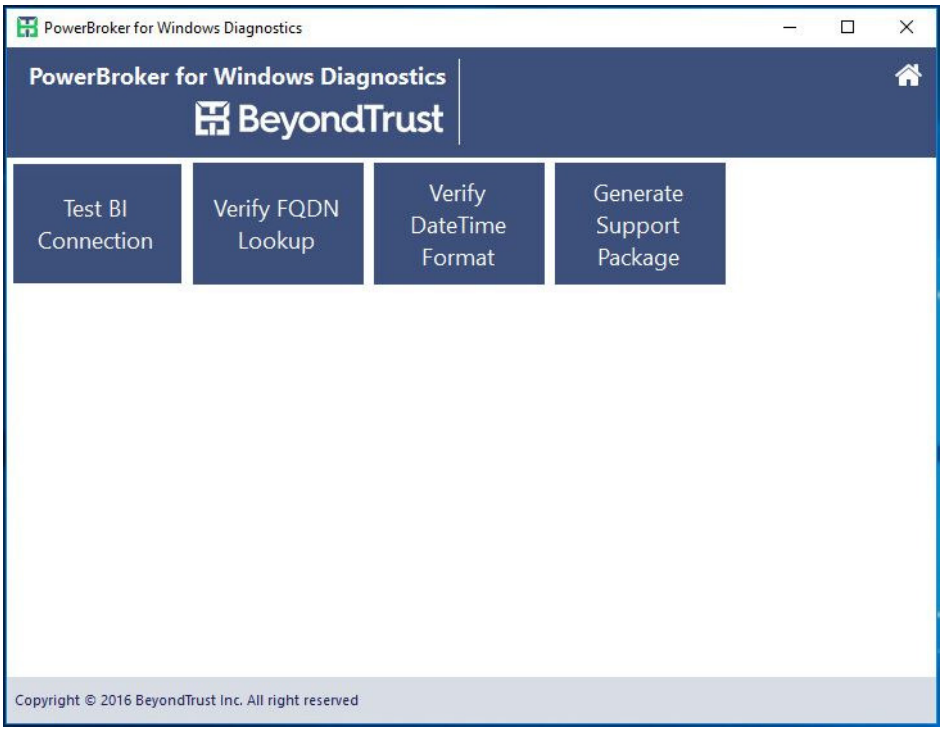


For more information, see the BeyondTrust PowerBroker for Windows - McAfee ePolicy Orchestrator Guide.

NOTE: Custom user message images are not currently supported when using McAfee ePO for policy distribution.

Support Diagnostic Application (#48068)

A new support diagnostic tool has been added to the client installer. This tool automatically generates and gathers logs for troubleshooting purposes.



FIXES

File Integrity Rules (#79870)
GPUpdate now succeeds when a file integrity deny rule is in place for the C:\Windows directory.

Password Safe User Messages (#78351)
Cancelling a Password Safe message during the credential check no longer causes a CPU spike.

File Path Parsing (#80138)
An issue was resolved with parsing the path and arguments in certain scenarios.

MMC Crash (#82555)
An issue was resolved when closing out of the Privileged Identity rules window.

Multiple Monitors and User Messages (#52770)
Improved support was added for User Messages on multiple monitors.

NOTE: Windows 10 will currently display a white background instead of the dimmed background.

BTService Crash (#77403)
An issue with BTService crashing was resolved.

Resource Monitor (#77484)
A fix was added to allow resource monitor to elevate correctly.

MOF Files (#81024)
An issue with the MOF file compilation was resolved.

Compatibility Mode Setting (#80383)
When using BeyondInsight for policy distribution, when Compatibility Mode is disabled the registry key is now written correctly.

Test Connection (#74327)
The Test Connection application will no longer display the error "Unable to retrieve the user's SID".

PowerBroker® for Windows® 7.2.0 - Released 18 November 2016

NEW FEATURES

Secure Boot (#76765)

PowerBroker for Windows now supports Secure Boot on Microsoft Windows 10 Anniversary Edition (Build 1607).

NOTE: The privman and privmanfi drivers are now signed by Microsoft, in addition to the BeyondTrust signing certificates.

ENHANCEMENTS

Microsoft EMET (#74914)

Support for Microsoft EMET has been improved. Privilege Elevation (compatibility) mode is no longer required when Microsoft EMET is installed.

Windows 10 upgrades (#77263)

Support has been improved for Windows 10 in-place upgrades.

NOTE: In order to improve support for Windows 10 upgrades, PowerBroker for Windows now installs certain files to the "%Program Files%\BeyondTrust\PowerBroker for Windows Client" directory.

Self-Healing Drivers (#59698)

The privman and privmanfi.sys drivers will be reinstalled automatically if needed when btservice starts.

Invalid Characters (#40920)

Event Reporting has been improved when applications contain invalid characters in the path and arguments fields.

Error Reporting (#44001)

Error reporting on the client has been improved when there is no policy assigned in BeyondInsight.

FIXES

Email Address (#44259)

User Messages no longer contain a link when no email address is present.

Heartbeats (#64602)

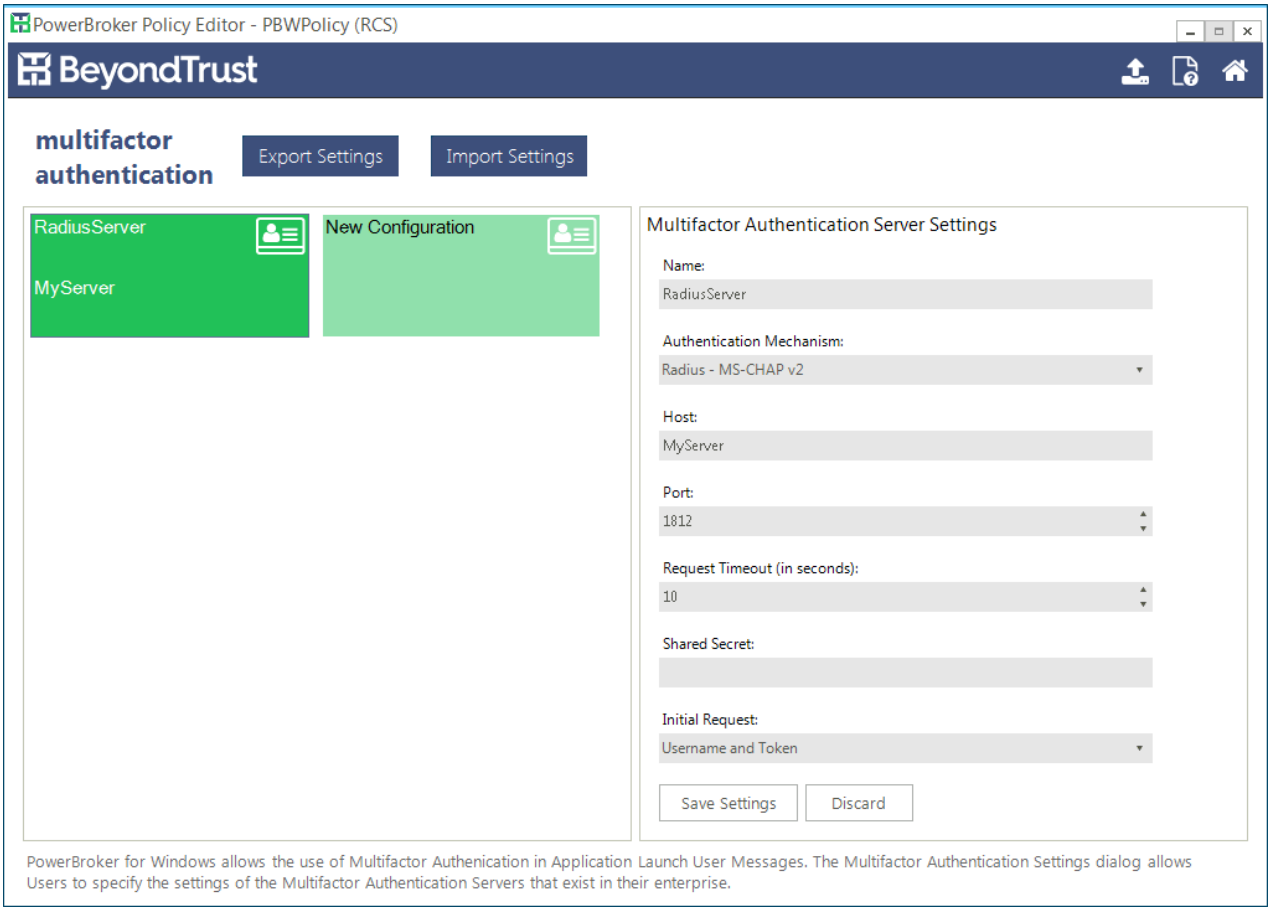
Trailing periods in the DNS name are now removed from the heartbeat event sent to BeyondInsight.

PowerBroker® for Windows® 7.1.0 - Released 2 September 2016

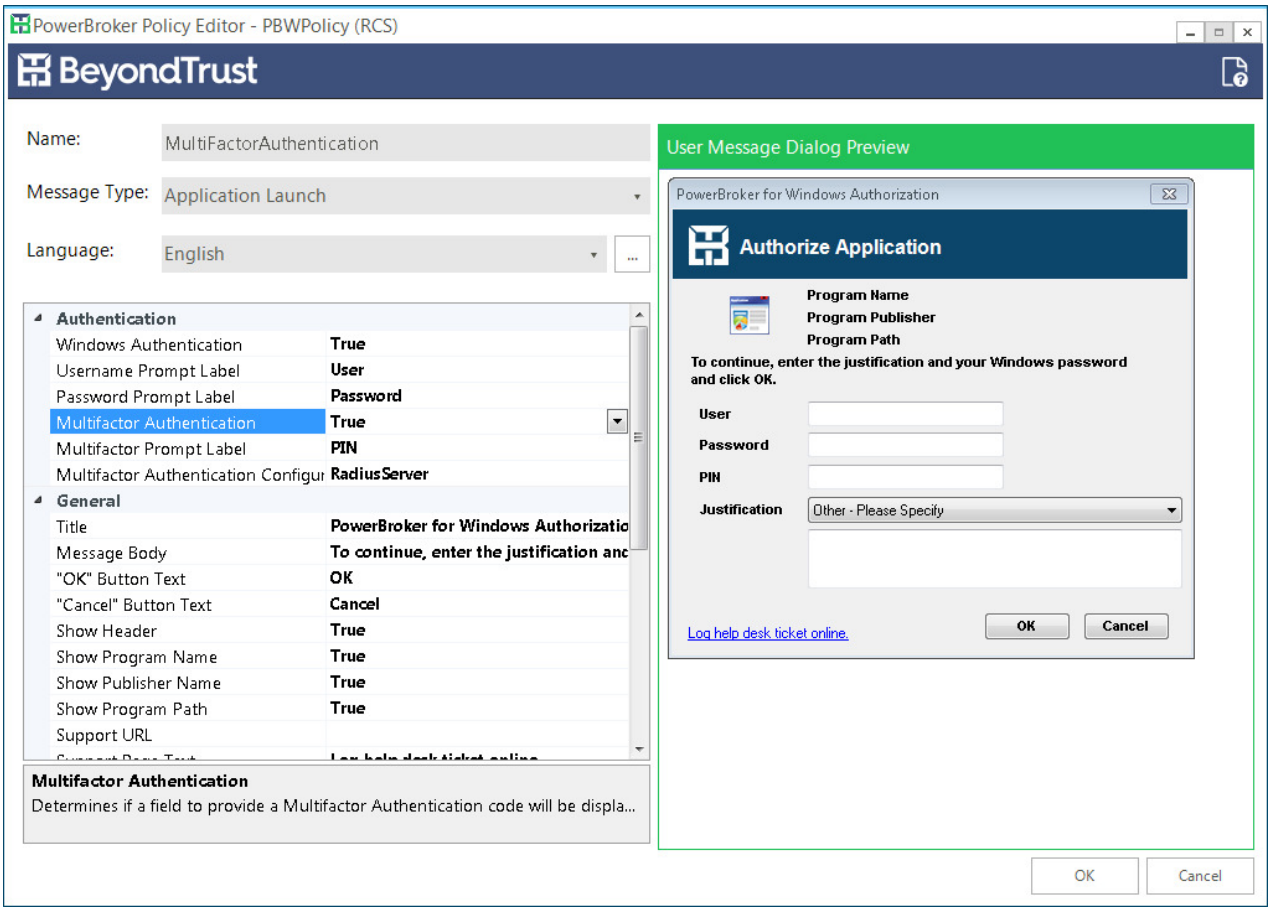
NEW FEATURES

Multifactor Authentication (#58517)

PowerBroker for Windows user messages now support Radius PIN-based authentication.



Application Launch user messages are supported, including on PowerBroker Password Safe rules. PIN-based authentication may be used with or without Windows authentication.



NOTE: Authentication via SMS push requests is not currently supported. (#67094)

FIXES

Ampersand in Publisher Rule (#64023)
An ampersand in a publisher rule no longer causes the rule to not apply.

Event Monitoring Collections (#68465)
An issue was resolved with editing event monitoring rule collections.

App-V Compatibility (#68283)
A compatibility issue with App-V was resolved.

PowerBroker® for Windows® 7.0.3 - Released 15 July 2016

ENHANCEMENTS

BeyondInsight Asset Based Authentication (#55558)

In the Management Settings there is a new option to enable BeyondInsight Asset Based Authentication. Enabling this setting alows BeyondInsight to handle authentication of assets for PowerBroker PasswordSafe requests. If this setting is enabled the user will not be required to enter a password when a PowerBroker Password Safe rule is applied.

NOTE: BeyondInsight 6.0 is required. Prior versions of BeyondInsight do not support this feature.

PowerBroker PasswordSafe Rules (#59058)

Improvement made to running applications with a PowerBroker PasswordSafe rule. Applications are first attempted to be run as BATCH, then as INTERACTIVE.

FIXES

User Messages: Support URL (#59456)

The support URL now launches correctly from links in User Messages.

Importing Publisher Rules (#59464)

The custom values checkbox and the slider now work correctly when XML rules are copied from BeyondInsight into PowerBroker for Windows with incomplete publisher info.

TestConnection (#59943)

TestConnection.exe no longer processes the StoreOnFailure file.

Bypass BeyondInsight Certificate Usage (#64255)

Session Monitoring logs are now sent to BeyondInsight when Bypass BeyondInsight Certificate Usage is enabled.

Svchost.exe (#52960)

An intermittent compatibility issue with svchost.exe was resolved.
NOTE: The result of a UAC prompt event (Yes/No) will no longer be reported in the Response data.

Updates to Rule Library (#54001)

The Rule Library was updated with changes to the cpalaunch ruleset.

User Interface improvement (#54718)

The ruleset is now checked for duplicate rule GUIDs.

Touch Screens (#54783, #43767)

The virtual keyboard is now displayed on touch screen devices.

Client Installer (#54909)

The client installer no longer prompts to reinstall when session monitoring is not selected.

PowerBroker® for Windows® 7.0.2 - Released 18 April 2016

NEW FEATURES

Signing Certificate

PowerBroker for Windows is now signed with a SHA 256 certificate. Contact support to obtain a client installer for operating systems that do not support SHA 256 (Microsoft Windows 2008). Windows 7 and Windows 2008 R2 must have Microsoft patch KB3033929 installed prior to install.

Privilege Elevation Mode (#47122, #44318)

A new option to configure the privilege elevation mode was added. Enabling this setting uses the Application Initialization (Compatibility) method to load PowerBroker for Windows dynamic link libraries (DLLs). Setting this to Not Configured (default) or Disabled will cause PowerBroker for Windows to use the default (Kernel) method of loading DLLs.

NOTE: Enabling this setting may be necessary when other security software packages are installed for compatibility. This includes endpoint security tools like Microsoft EMET, Cylance, and Bromium.

Parent Process (#46686)

The parent process is now set to the launching application when a rule is applied.

NOTE: If Integrity Level on the rule is set to Low, the parent process will remain pmlauncher.exe.

ENHANCEMENTS

Run as Different User: gpmc.msc fails (#29648)

GPMC.msc will now load when launched via "Run as different user" and a rule is applied.

Bypass File Integrity Level (#44429)

A new option has been added to bypass file integrity level settings. With this setting enabled process integrity level will be set to match the rule. This is useful when elevating an application from a Low integrity level folder.

Publisher Rules (#32380)

Publisher rules will now match when wildcards are specified for blank fields.

User Messages and Help Desk Link (#32437)

The "Log a help desk ticket" link in user messages now launches Internet Explorer as the user.

Item Level Targeting: Operating System (#40536)

Windows 8.1 and Windows 2012 R2 were added to the operating system item-level targeting options.

Password Safe Rule (#44362)

When creating a rule to use PowerBroker Password Safe credentials, "Run As User" is now a mandatory field.

Item Level Targeting: Local Security Groups (#44474)

Added the ability to specify a local security group in Item-Level Targeting.

Future Upgrades with Client Protection (#45231, #47101)

Upgrading with Client Protection enabled will be possible for future releases. This enhancement only takes effect when upgrading from 7.0.2 and higher. It does not apply when upgrading from versions prior to 7.0.2.

Security Enhancement (#44509)

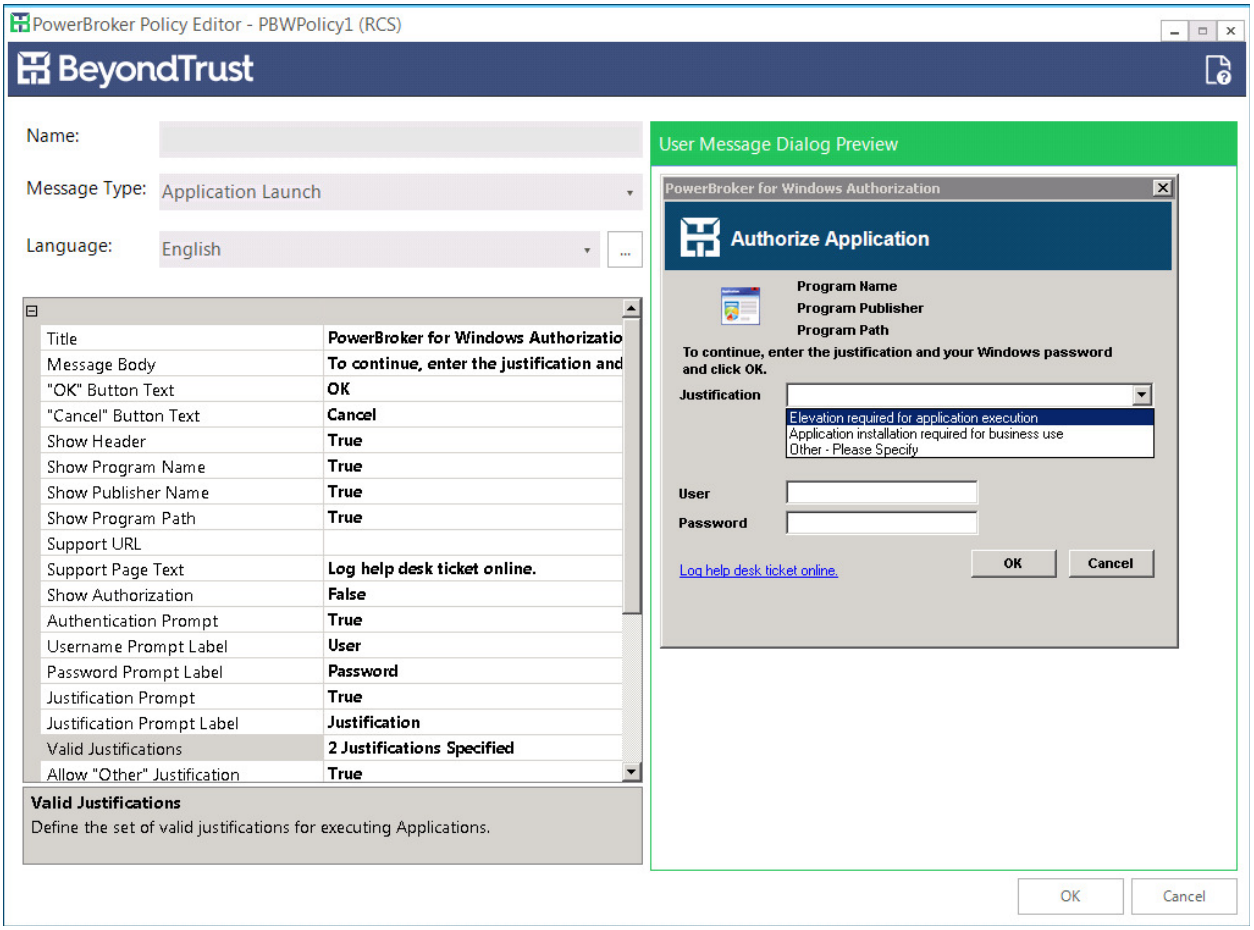
The Capture folder was added to the list of protected folders.

UAC Prompt(#44436)

Added the ability to configure whether or not the UAC prompt appears when the user clicks "Cancel" on an application launch user message.

User Messages: Justifications (#44506)

There is now a drop-down for justifications on user messages:



Importing Rules (#44566)

The ability to import rules directly into a collection was added.

Rebranding (#46362)

Colors and images were updated to the new BeyondTrust logo.

Performance Optimization (#46441)

The number of settings that trigger the hash/publisher calculation was reduced. Now only these settings cause hash/publisher evaluation:

ApplicationLaunch
ApplicationModifiedPrivileges
UserRequestedModifiedPrivileges
DeniedAppLaunch
PassiveAppLaunch
QuarantineEvents
Hash or Publisher rule

Client Certificate (#46542)

The option to not require a client certificate for BeyondInsight communication was added.

Item Level Targeting: LDAP Query (#48019)

Added the ability to specify a server name in an LDAP query in Item Level Targeting.

Session Monitoring on UAC Rules (#49775)

UAC rules now support session monitoring.

Disable Reverse Name Server Lookup (#50311)

A new option to disable reverse name server lookup for retrieving of fully qualified domain name has been added to the Management settings.

PowerBroker PasswordSafe Timeout (#51165)

The timeout on PowerBroker PasswordSafe updates was increased to allow for bulk password updates.

Oracle 11g Client Install (#47749)

A PowerBroker PasswordSafe rule will now work to install the Oracle 11g client installer.

Security enhancements (#44412)

Security enhancements were made to the ProgramData\BeyondTrust\RetinaCS folder.

FIXES

Caps Lock (#29673)
A Justification can now be entered when Caps Lock is enabled.

User Message Localization (#40357)
A localization issue was resolved with the justification text on user messages.

Installer: Upgrade improvements (#40792, #41004)
Improvements were added to the installer to mitigate issues with upgrades.

Item Level Targeting: LDAP (#43914)
Filtering based on LDAP://<SID =%reversedusersid%> now works correctly.

Double Quote MSI Names (#44532)
A setting was added to surround msi filenames in double quotes when the installer is elevated and the msi filename contains spaces.

Publisher Rule (#44557)
Trailing spaces are now ignored in matching on Publisher Rules.

Invalid Characters (#44577)
A check was added for invalid characters in the rule name (", <,> and & characters).

DateTime Reporting (#48970, #50311, #47205)
Improvements were made to date and time reporting across locales.

Intermittent Crash (#52322)
An intermittent crash was resolved.

PowerBroker® for Windows® 7.0.1 - Released 2 December 2015

NEW FEATURES

PowerBroker for Mac User Messages and Deny Action (#16767)
Support for PowerBroker for Mac User Messages and a new Deny Action have been added to the Policy Editor.

ENHANCEMENTS

Windows 10 Item-Level Targeting (#16835)
The option to target rules based on the Windows 10 operating system has been added.

FIXES

Windows 10: Integrity Level (#16883)
The Integrity Level is now changed correctly on Windows 10 when a rule is applied.

Session Monitoring with FIPS Enabled (#16821)
Session Monitoring now works correctly when FIPS is enabled.

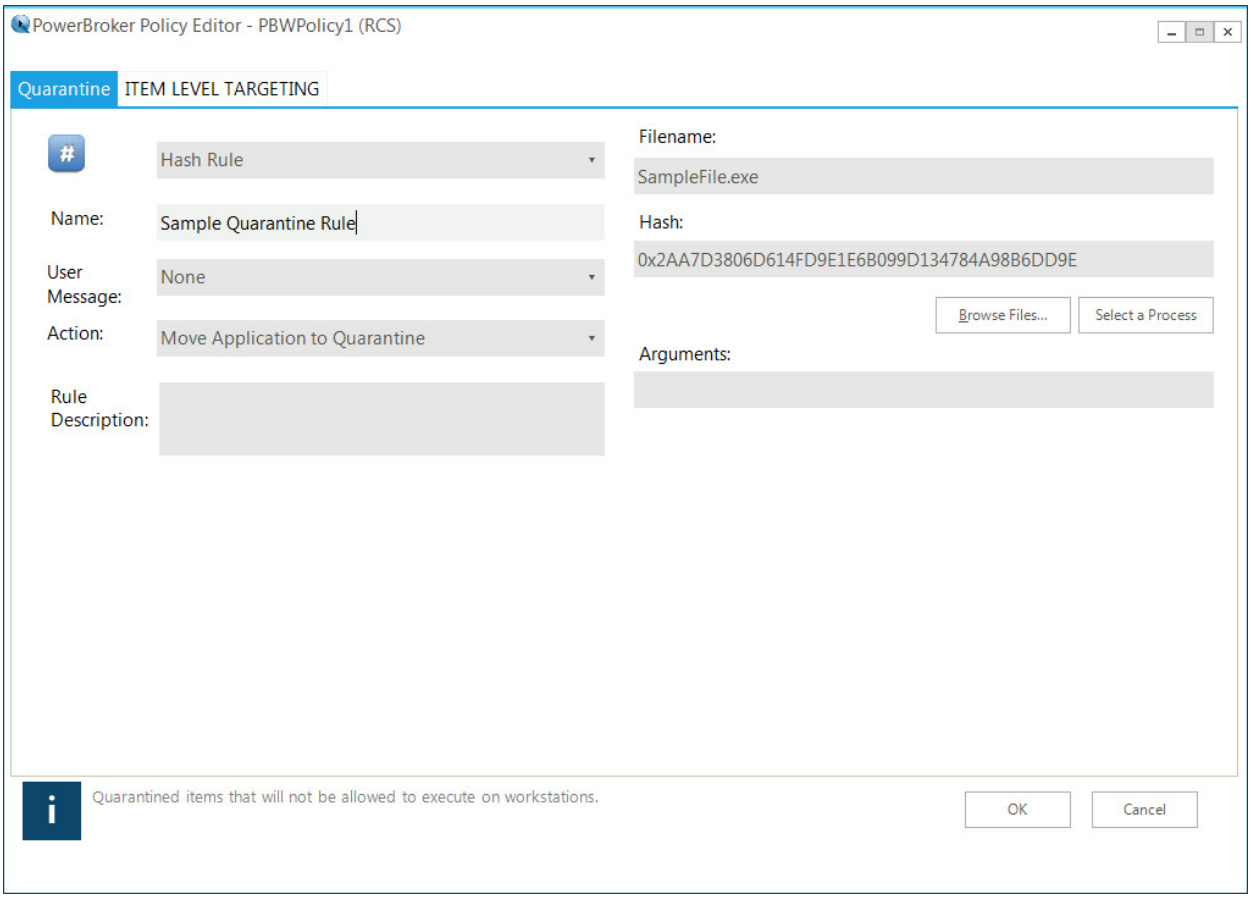
Windows 10: Risk and Compliance Rules (#16822)
Operating System version on Windows 10 is now reported correctly to BeyondInsight.

PowerBroker® for Windows® 7.0 - Released 30 October 2015

NEW FEATURES

Support for Windows 10 (#16736)
Windows 10 Enterprise, Long Term Service Branch, and Professional are now supported.

Quarantine Rules (#16738)
The ability to Quarantine and Restore executables has been added:



Rules are created based on a hash of the file. On execution, PowerBroker for Windows now checks for Quarantine rules. If a rule matches, the file is quarantined. If the action is changed to Restore, the restore is completed on policy update.

NOTE: Executables run from zip files will be blocked, but not quarantined.

Support for Multiple Policies (#16758)
Multiple policies are now supported when using BeyondInsight for policy distribution.

NOTE: Older versions of the PowerBroker for Windows client do not support multiple policies. If multiple policies are used prior to upgrading the client to 7.0 or higher, only the lowest priority policy will be distributed.

PasswordSafe: Windows Service Account Credentials Change (#16619)
Passwords will now be updated for any services running under a local account.

NOTE: The service will not be restarted.

ENHANCEMENTS

Heartbeat and Stored Events (#16817)
Stored Events are now sent on a successful heartbeat.

BeyondInsight: Computer Item Level Targeting (#16740)
When using BeyondInsight for policy distribution, computer-based item level targeting is now supported.

PasswordSafe: User Name field (#16741)
The User Name field in the Password Safe user message is now read-write.

User Interface Resizing (#16576)
The User Interface now automatically resizes.

FIXES

Bloomberg Installer (#16790)
A compatibility issue with the Bloomberg installer was resolved.

Session Monitoring and Multiple Rule Matches (#16747)
Session Monitoring no longer stops recording when there are multiple rule matches.

Corrupted History File (#16667)
When the PowerBroker for Windows history file gets corrupted, the following group policy update will now work.

Memory Issues (#16772)
A memory leak with btservice was resolved.

Client Installer (#16752)
Communication with BeyondInsight now works after the client is repaired.

Snapin Installer (#16808)
Modifying the snapin installer will now show the correct features in the policy editor after install.

BeyondInsight: OS Information (#16309)
Operating System information is now sent to BeyondInsight.

PowerBroker® for Windows® 6.8.3 - Released 1 October 2015

FIXES

Working Directory (#16771)
When an application is executed from a mapped drive, the application's working directory is now maintained when a rule is applied.

PowerBroker® for Windows® 6.8.2 - Released 3 September 2015

ENHANCEMENTS

Client Protection Enhancements (#16744)
The Client Protection feature has been enhanced to further harden the PowerBroker for Windows Client.

Client Protection Exclusions (#16745, 16762)
The Client Protection feature has been enhanced to exclude specified Users and/or Groups from Client Protection.

BeyondInsight Client Certificate Setting (#16746)
The BeyondInsight Client Certificate Name setting has been enhanced to allow Users to optionally match the SSL Certificate based on the Subject and Issuer fields of the certificate.

BeyondInsight Client Certificate Name (#16761)
The BeyondInsight Client Certificate Name setting has been enhanced to allow Users to specify System Environment Variables in the setting value.

GenerateNewInstallerID Quiet Mode (#16722, #16766)
The GenerateNewInstallerID application has been updated to include a "/quiet" switch to enable a quiet execution mode.

PowerBroker® for Windows® 6.8.1 - Released 30 July 2015

ENHANCEMENTS

Unified Installers (#16635)
The 32 bit and 64 bit Installers for the PowerBroker for Windows Client and PowerBroker Policy Editor have been combined to provide a single EXE for each product that will install the appropriate files for the CPU Architecture of the Target Operation System.

Session Monitoring Settings (#16724)
New settings to control Session Monitoring Queue Sizes have been added.

FIXES

Rule Collection Enforce Action (#16734)
An issue with the Enforce Action feature in Rule Collections was resolved.

Client Installation Error (#16710)
An issue with the Client Installation on some workstations was resolved.

Item Level Targeting Issue (#16743)
An issue with Item Level Targeting persistence was resolved.

PowerBroker® for Windows® 6.8.0 - Released 16 July 2015

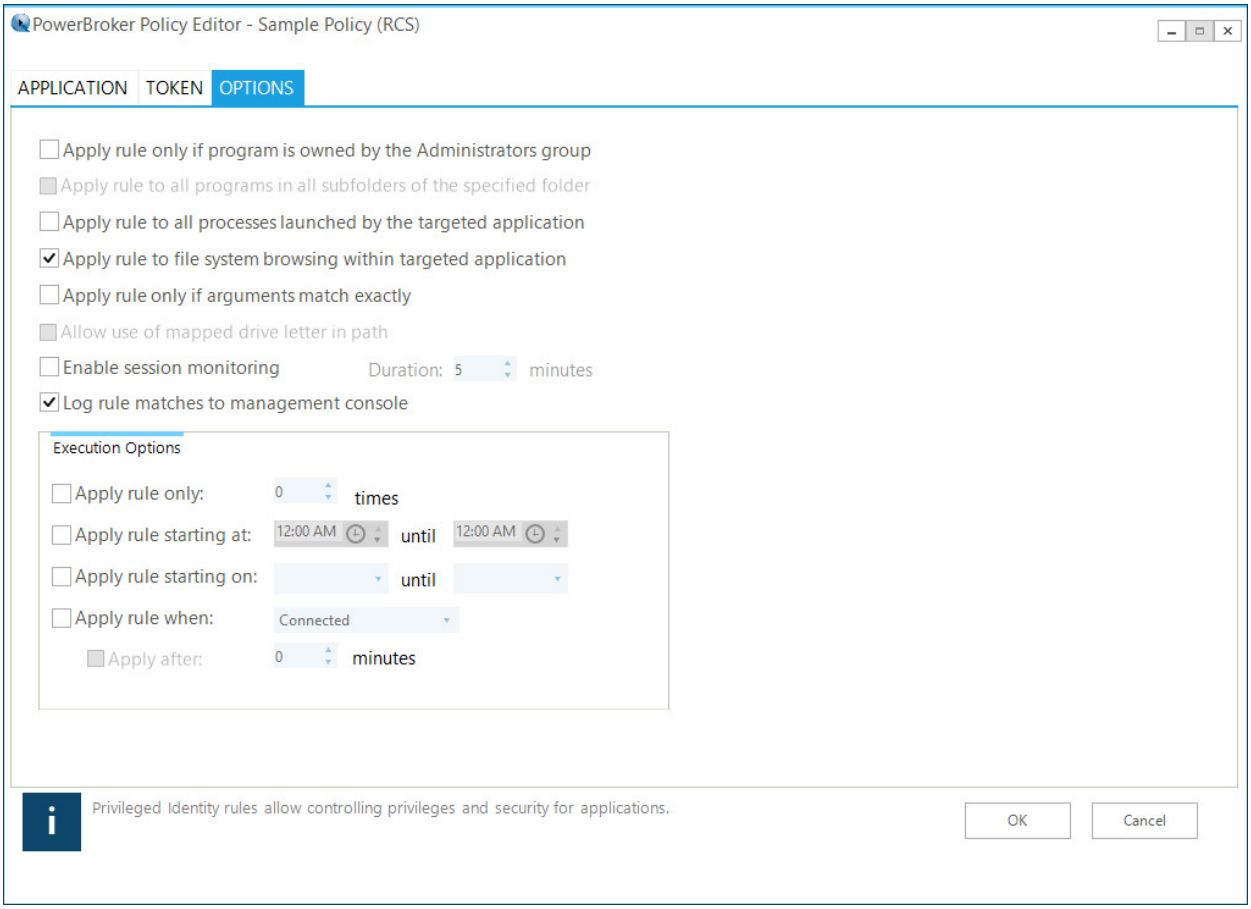
INFORMATION

Windows Vista and Windows Server 2003 (#16680)
Windows Vista and Windows Server 2003 are no longer supported.

PowerBroker Policy Editor
The PowerBroker for Windows Snapin is now known as the PowerBroker Policy Editor to encompass the inclusion of PowerBroker for Mac Policy Management.

ENHANCEMENTS

Enable/Disable Rule Logging on a Per Rule Basis (#16409)
Privilege Identity and Risk rules have a new option to enable/disable the logging of rule matches to the management console.



PowerBroker Policy Editor Windows Resizing (#16634)
All Windows in the PowerBroker Policy Editor can now be resized.

Session Monitoring Enhancements (#16551, #16676, #16685)
Session Monitoring data integrity and security has been enhanced.

Passcode Generator Directory (#16593)
The Passcode Generator Directory is now created during the PowerBroker for Windows Client installation.

FIXES

Rule Wizard Execution Time Frame (#16566)
An issue with differences in Execution time frame between the standard rule editor and the rule creation wizard were resolved.

Rules Library Updates (#16652, #16700, #16721)
The Rules Library provided with the PowerBroker Policy Editor has been updated to resolve issues with some rules. A set of rules for PowerBroker for Mac was also included.

Item Level Targeting in the Rule Wizard (#16660)
An issue that caused the User item to be unavailable on some Item Level Targeting controls was resolved.

File Integrity Rule Loading (#16695)
An issue around the loading of File Integrity rules was resolved.

UAC Prompt User Message (#16713)
An issue with the UAC Prompt User Message on non-English Windows Operating Systems was resolved.

Username Event Field (#16577)
An issue with the Username field on some events was resolved.

PowerBroker® for Windows® 6.7.3 - Released 8 May 2015

FIXES

Rule Not Triggering (#16663)
An issue with case sensitivity with rules was resolved.

Move To operation in Snapin with Collections (#16693)
Moving a Rule within a Collection was sometimes resetting the Rule's Action.

Microsoft Visual Studio Debugger Error (#16584)
An issue was resolved involving some 32 bit processes running on 64 bit systems.

PowerBroker® for Windows® 6.7.2 - Released 6 April 2015

FIXES

Session Monitoring Notification (#16672)
Enhanced security on session monitoring notification so it can not be terminated.

PowerBroker® for Windows® 6.7.1 - Released 10 March 2015

ENHANCEMENTS

Shell Rule (#16434)
The Shell rule now works with the .msu file extension.

FIXES

Remove Admin Rights (#16662)
An issue was resolved with the Remove Admin Rights option.

"Apply rule to file system browsing" (#16657)
An issue was resolved with "Apply rule to file system browsing".

Snapin Installer (#16631)
The Snapin may now be installed to a custom location.

File Versioning (#16630)
A improvement was implemented to file versioning.

Cisco AnyConnect (#16629)
A compatibility issue was resolved with Cisco AnyConnect.

UAC Prompt Message (#16623)
The UAC Prompt message now appears correctly when an application is launched from a network share.

NTPrint.exe (#16609)
NTPrint.exe can now be successfuly elevated.

Justification Prompt (#16563)
The Justification prompt will no longer accept only spaces.

DNS Name reporting (#16444)
An improvement was made to DNS name reporting with BeyondInsight.

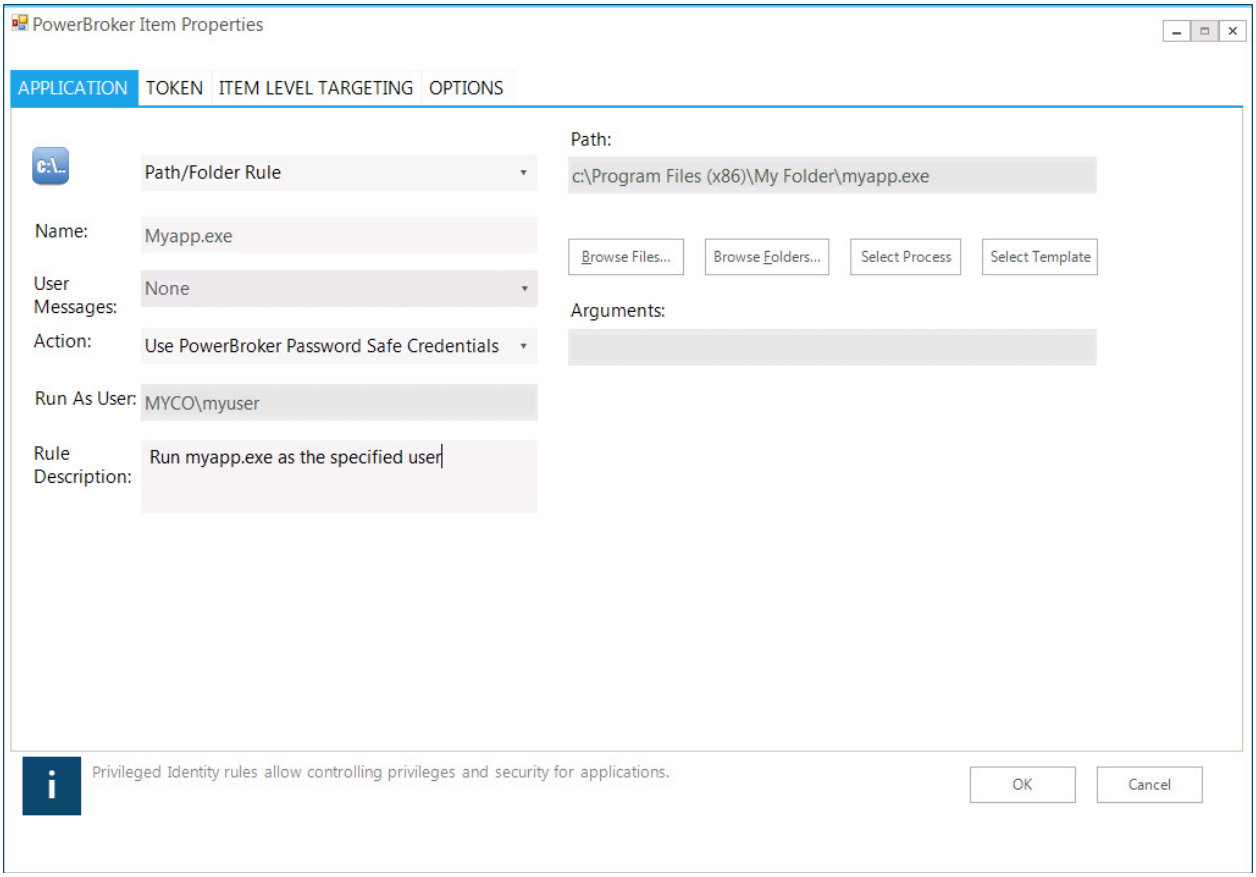
PowerBroker® for Windows® 6.7 - Released 16 January 2015

INFORMATION

Windows XP (#16595)
Windows XP is no longer supported.

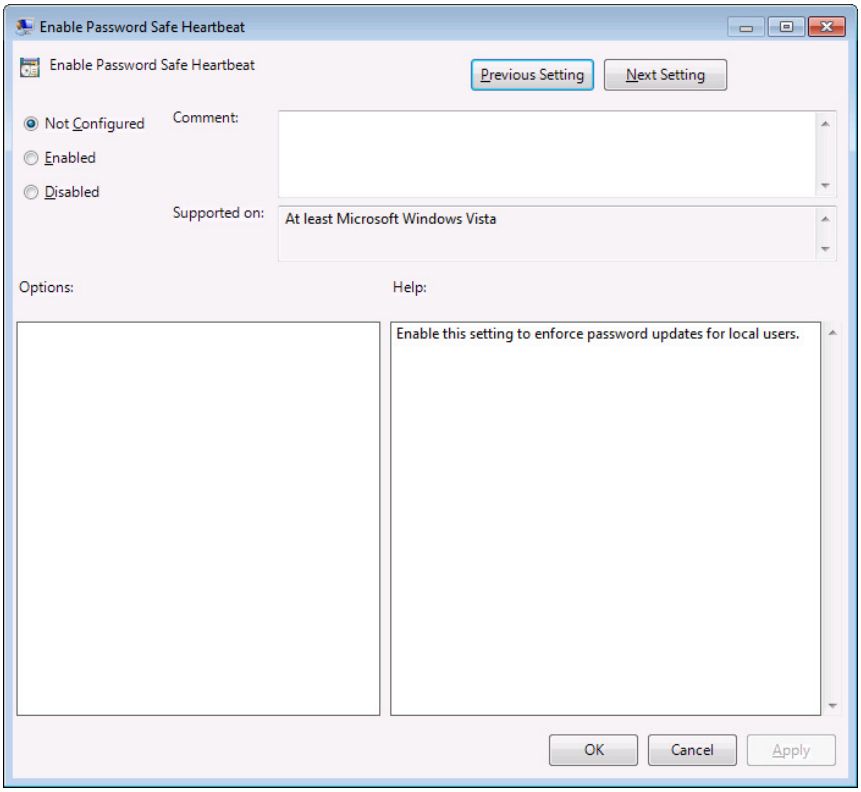
NEW FEATURES

Password Safe Integration: RunAs User (#16536)
There is a new option to run applications as a different user. This feature requires BeyondInsight and a PowerBroker Password Safe license.



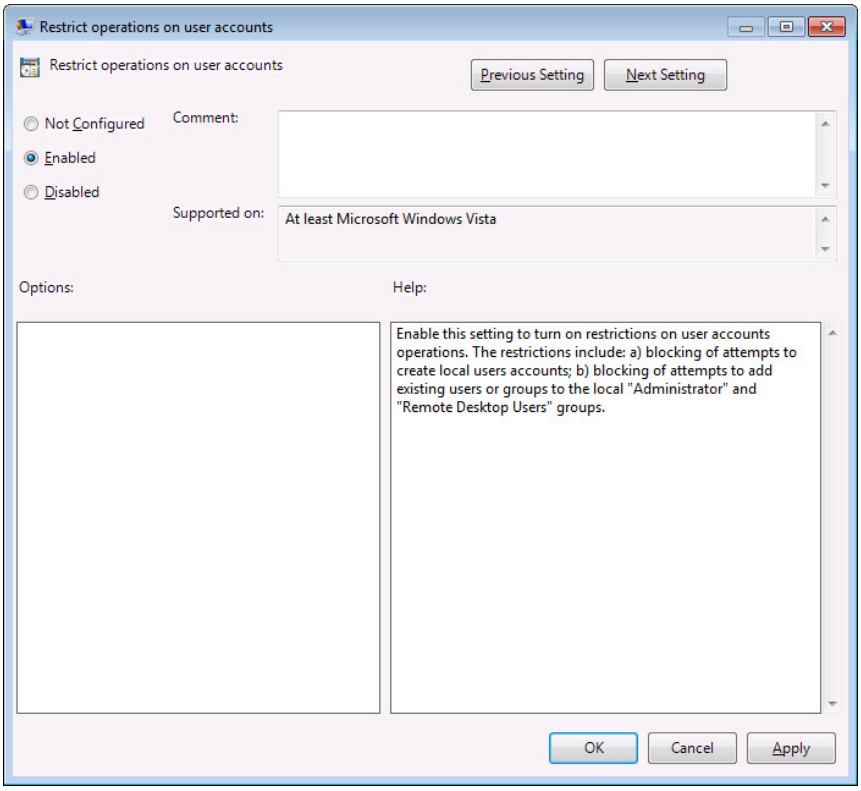
Password Safe Integration: Password Change (#16536)

PowerBroker for Windows now supports changing passwords for local user accounts.



Prevent admin from adding users (#16537)

There is now an option to prevent admins from adding local users. This option also blocks attempts to add users to the local Administrator and Remote Desktop Users groups.

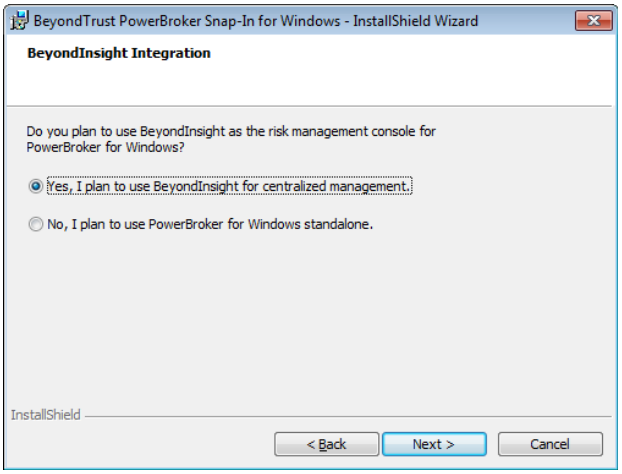


VBAM rule support for alerts on registry/dll use (#16538)

Risk and Compliance (VBAM) rules now support evaluating dlls as well as exes. In addition, a global setting is available to monitor the registry.

Simplified Snapin Installer (#16554)

The Snapin installer has been simplified for non-BeyondInsight environments. Features that require BeyondInsight are only displayed in the UI if this option is selected on install.



ENHANCEMENTS

Remember Justification (#16395)

There is now an option to remember justifications and pre-populate the justification field.

FIXES

ActiveX failure message (#16550)

The Email link now appears correction on the ActiveX Failure message.

Vulnerability issue was resolved (#16571)

A privilege escalation vulnerability with btservice was resolved.

Fix to Trace Logging (#16574)

Trace logging no longer logs sensitive data.

UAC Logging (#16583)

Windows UAC prompts are now logged.

"URL is Null or Empty" (#16597)

The error "URL is null or Empty" was removed when BI logging is not enabled.

Uninstalls and Client Protection (#16540)

Uninstalls are now prevented when Client Protection is enabled.

User Message GUIDs (#16552)

User Message GUIDS are no longer changed on import.

PowerBroker® for Windows® 6.6.1 - Released 2 September 2014

INFORMATION

Microsoft .NET Framework (#16553)
The PowerBroker for Windows Client now supports either the Microsoft .NET Framework 3.5 or 4.0. The Snap-In still requires the Microsoft .NET Framework 4.0.

FIXES

BeyondInsight Events (#16543)
An issue was resolved with StoreOnFailure and BeyondInsight events.

Windows Encrypting File System (#16411)
An ADM(X) setting was added to disable the use of Windows Encrypting File System (EFS).

DLL Registration on Install (#16533)
The method of dll registration on install has been changed. McAfee no longer blocks the installer from registering files.

Java Applications (#16534)
An issue running Java-based applications with PBW has been resolved.

User Messages: Upgrade Issue (#16529)
An issue upgrading user messages from older versions (branded PowerBroker Desktops) has been resolved.

Global User Messages (#16525)
"Used in Rules" has been removed for global user messages.

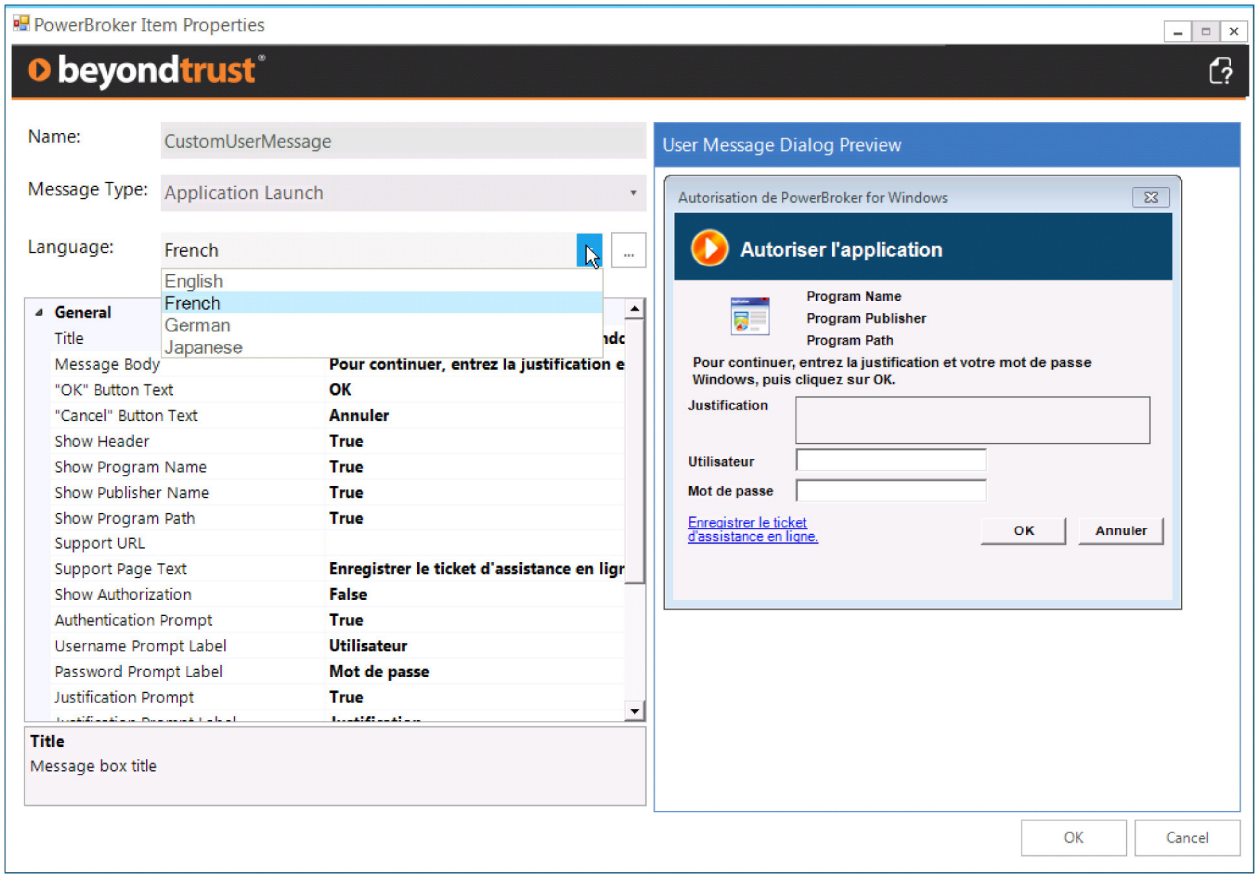
UI Hang (#16527)
When there is a large number of rules, selecting the tile "Rules with Session Monitoring" will no longer cause MMC to hang.

PowerBroker® for Windows® 6.6 - Released 11 July 2014

NEW FEATURES

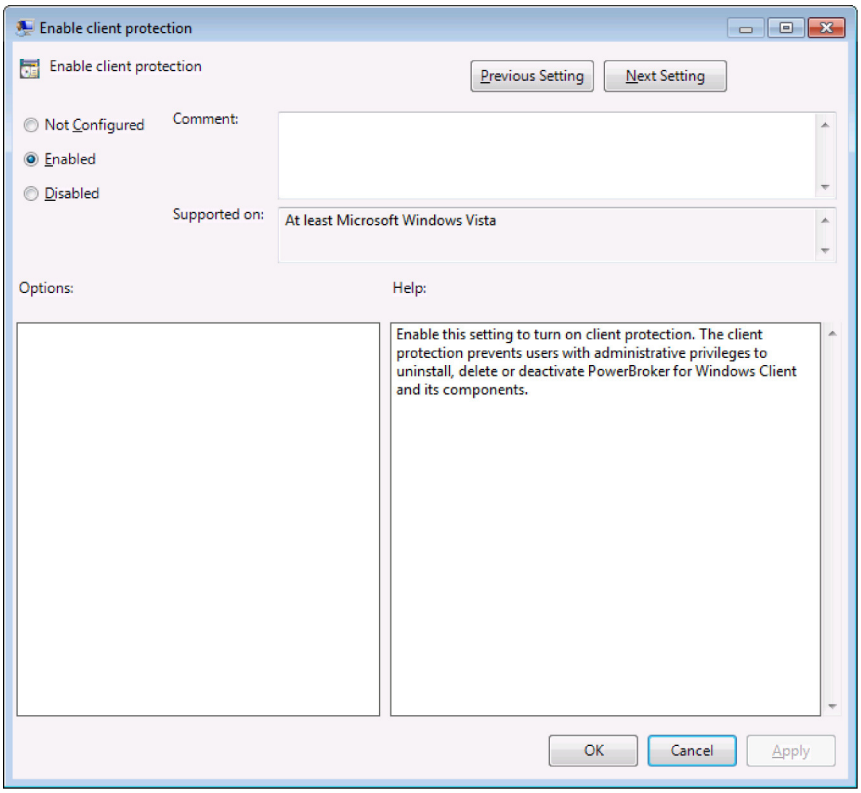
Localized User Messages (#16386, #16496)
User messages may now be localized and displayed according to the user's Windows display language. In addition, translations are provided for the default messages and default text in the following languages: Spanish (Spain), French, Italian, German, Simplified Chinese, Japanese.

To facilitate the translation of custom user messages, user message text may be exported to a Microsoft Excel file, translated, and re-imported into PowerBroker for Windows.



Tamper Protection (#16401)

A new option has been added to prevent admins from stopping PowerBroker for Windows services, or from modifying or deleting PowerBroker for Windows files. To make use of this feature, enable "Enable Client Protection" in the Security Driver settings.



Rule Library (#16452)

Examples of how to prevent the uninstall of commonly used applications have been added to the rule library.

Internet Explorer 11 Enhanced Protected Mode (#16388)

Internet Explorer 11 Enhanced Protected Mode is now supported.

ENHANCEMENTS

System Environment Variables (#16388)

System Environment Variables are now supported in user messages.

NOTE: User environment variables are not currently supported.

User Messages: OK button (#16500)

The OK button is no longer displayed when authentication and justification are disabled, but authorization is enabled. In this scenario, Passcode and Cancel are now the only buttons.

BeyondInsight settings (#16275)

Client settings related to BeyondInsight are now loaded immediately on update.

Update Button (#16334)

An update button was added to the home page in BeyondInsight mode.

FIXES

Double Justification Prompt (#16414)

A second Justification prompt is no longer displayed when the Windows Desktop theme is set to Classic.

Version Number (#16345)

The Version Number is now displayed in Help->About.

NOTE: This does not include the build number. The build number is displayed in Programs and Features.

Xenapp Virtual Delivery Agent (#16472)

An issue was resolved when the Xenapp Virtual Delivery Agent and the PowerBroker for Windows client were installed.

Trial Director (#16421)

A compatibility issue with Trial Director was resolved.

Passcode and UNC shares (#16416)

An issue was resolved with passcodes when launching applications from certain UNC shares.

BeyondInsight Tracing (#16352,16293)

Improvements were made in configuring BeyondInsight-related trace logging.

PowerBroker® for Windows® 6.5.2 - Released 18 April 2014

INFORMATION

Microsoft Encrypting File System (EFS) (#16411)

Microsoft Encrypting File System is required to be enabled and the service running in order for Session Monitoring to work.

Security Driver Trace Logging (#16408)

Security Driver trace logging should not be enabled in a production environment due to impact on performance. This setting is for troubleshooting purposes only. A warning has been added to the setting.

ENHANCEMENTS

Security Enhancements (#16403)

A number of minor compiler changes were made to ensure the product is delivered in a secure manner.

Microsoft Detours(#16397)

Vulnerability in Microsoft Detours software used in PowerBroker for Windows.

FIXES

Intermittent: Rules do not Apply (#16385)

An intermittent issue was resolved with rules not applying. This would occur only with the latest (fastest) CPUs.

F3 in Filters (#16399)

F3 now works correctly in Filters.

Rule Library (#16400)

Privileged Identity rules from the rule library are now disabled on import.

Microsoft Detours (#16397)

A vulnerability in Microsoft Detours software used in PowerBroker for Windows has been addressed.

PowerBroker® for Windows® 6.5.1 - Released 28 February 2014

INFORMATION

Windows 2012 R2 Support (#16376)

Windows 2012 R2 is now supported for both the snapin and client.

Session Monitoring and Windows 8/2012 R2 (#16356)

The Session Monitoring notification will not be displayed on the Windows 8 App Store ("Metro-style") desktop. However, the Windows 8 desktop will still be captured if session monitoring is in progress. The notification will be displayed on the Classic desktop.

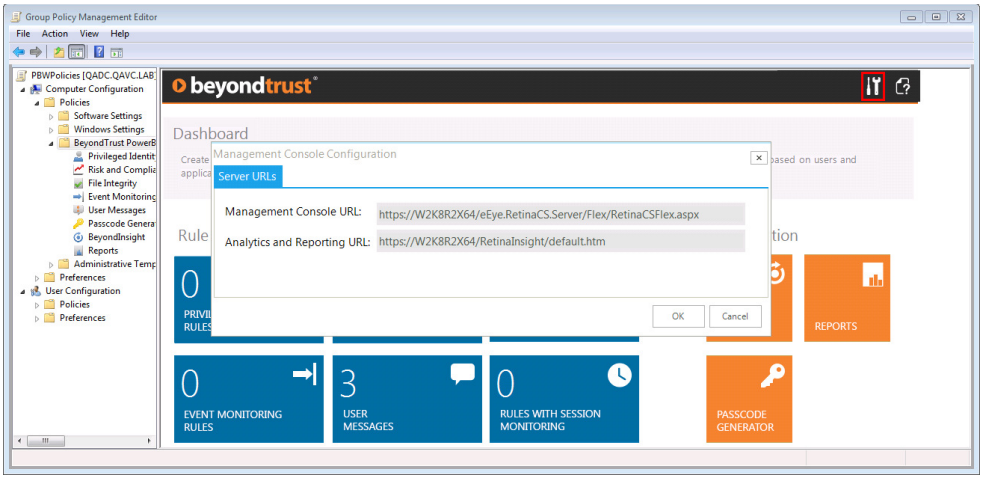
Session Monitoring and Windows 8/2012 R2 (#16370)

If session monitoring is enabled and capturing screens, all keystrokes for "Metro" applications will be captured and stored. Keystroke filtering may be used for these applications.

ENHANCEMENTS

BeyondInsight and Reports Custom URLs (#16271)

Custom URLs for BeyondInsight and Reporting can now be configured via the toolbar icon in the Dashboard. HTTP and HTTPS are both supported.



Installer ID (#16330)

A unique Install ID is generated on install. If the PowerBroker for Windows client is installed on a base image, and BeyondInsight is being used, the Install ID will need to be regenerated after deploying the image. This utility is located at: c:\Windows\BeyondTrust\BeyondInsight\generatenewinstallerid.exe.

File System Browsing and Microsoft Office (#16311)

The "Apply rule to file system browsing within targeted application" is now supported for Microsoft Office 2007, 2010, and 2013.

NOTE: This feature is NOT supported for Microsoft Office 2003.

FIXES

Privacy Mode and Session Monitoring (#16357)

When Privacy Mode is enabled, the user name is now hashed in session monitoring data.

Deleting Collections (#16361)

An issue was resolved with deleting multiple collections.

Duplicate Names (#16365)

The check for duplicate rule names was removed.

Profiling and SEP 12.1 RU4 (#16382)

An issue was resolved when profiling was enabled and Symantec Endpoint Protection 12.1 RU4 was installed.

Scrollbar Location After Editing Rule (#16374)

After editing a rule, the focus now remains in the correct position on the vertical scrollbar.

PowerBroker® for Windows® 6.5 - Released 20 December 2013

INFORMATION

File Integrity Rule Order (#15969)

File Integrity rule order has been reversed to match Privileged Identity rules.

IMPORTANT: If you have existing File Integrity rules that depend on rule order, they should be tested and adjusted as needed before upgrading production machines.

Internet Explorer (#15425)

For Internet Explorer 10, if an IE rule is in place and the Integrity Level is set to Medium, the rule should be set to c:\program files*\internet explorer\iexplore.exe.

BeyondInsight Central Policy Mode (#15890)

Only one smart rule configured to deploy PBW Policy should be applied to each machine.

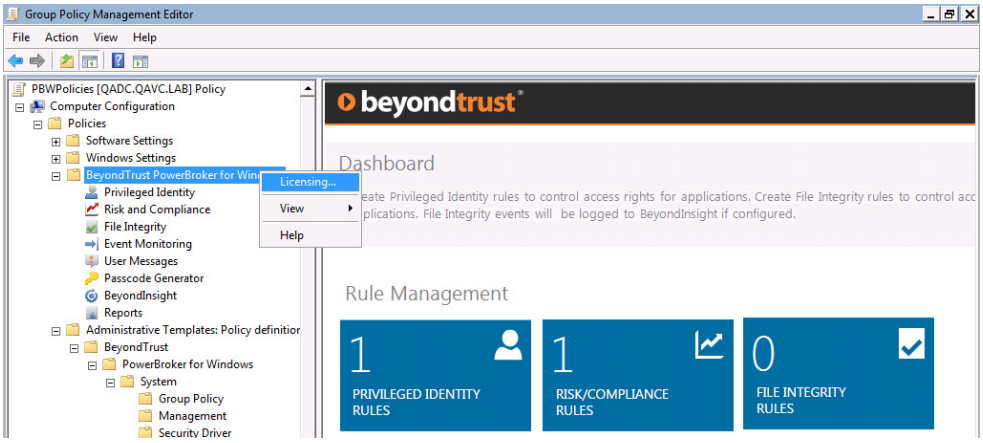
.NET Framework versions (#16097)

The Snap-In requires the .NET Framework 4.0. The client requires the .NET Framework 3.5 for BeyondInsight integration and Session Monitoring.

For Windows 8/8.1, the .NET Framework 3.5 is not installed by default and will need to be added in Programs and Features->Windows Features. This must be done **prior** to deploying the client.

Licensing (#16174)

The Licensing Menu is now available via a right-click option on the BeyondTrust PowerBroker for Windows node. It is no longer available on the top Menu bar.



Windows 8.1 (#16242)

Windows 8.1 is supported with PowerBroker for Windows 6.5. Internet Explorer Enhanced Protected Mode is not supported (see below).

Internet Explorer: Enhanced Protected Mode (#16204)

ActiveX Rules and IE rules are not supported on Windows 8/8.1 when Enhanced Protected Mode is enabled. These rules will function on Windows 8/8.1 when Enhanced Protected Mode is disabled.

URL is null or empty (#16247)

The error "URL is null or empty" may occur if the BeyondInsight URL is being rewritten while data is attempting to be sent (i.e. on gpupdate /force). The data should send successfully once the URL has been written to the registry.

Troubleshooting (#16273)

Relevant settings have been moved to a "Troubleshooting" section in the ADM(X)/Settings. The settings in this section should be used for troubleshooting with BeyondTrust support. The logging settings in the Troubleshooting section should NOT be enabled in a production environment. Enabling the logging settings may result in a significant performance decrease.

Central Policy Tracing (#16293)

To enable tracing in Central Policy mode, a change must be made to the default path for the trace file.

Central Policy Settings (#16275)

Central Policy Mode settings are loaded on restart of btservice, or the current heartbeat interval on the client. The recommended method is to configure all settings before deploying the policy via BeyondInsight. To force a reload of the settings, restart btservice (or reboot).

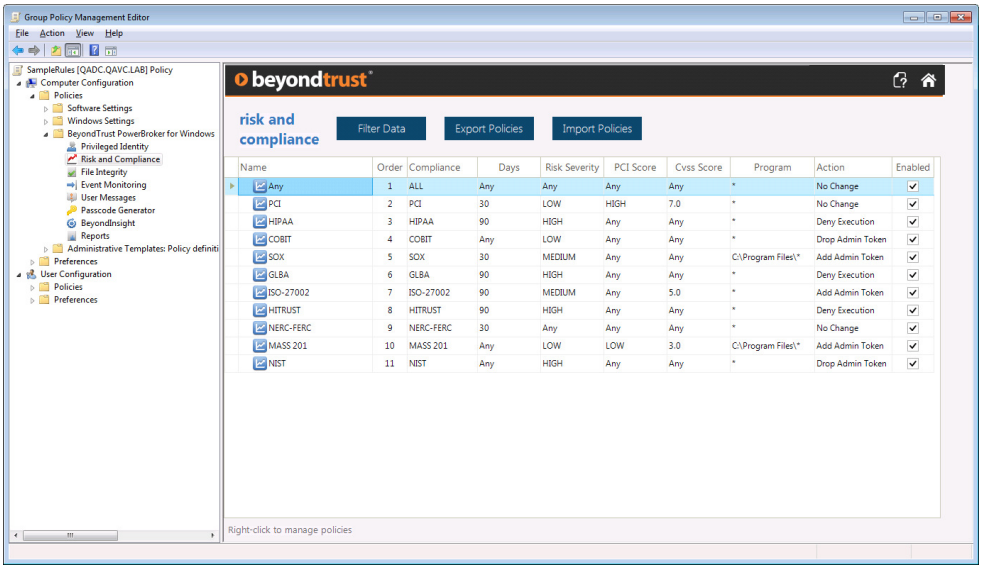
NEW FEATURES

Full GPME Integration (#15965)

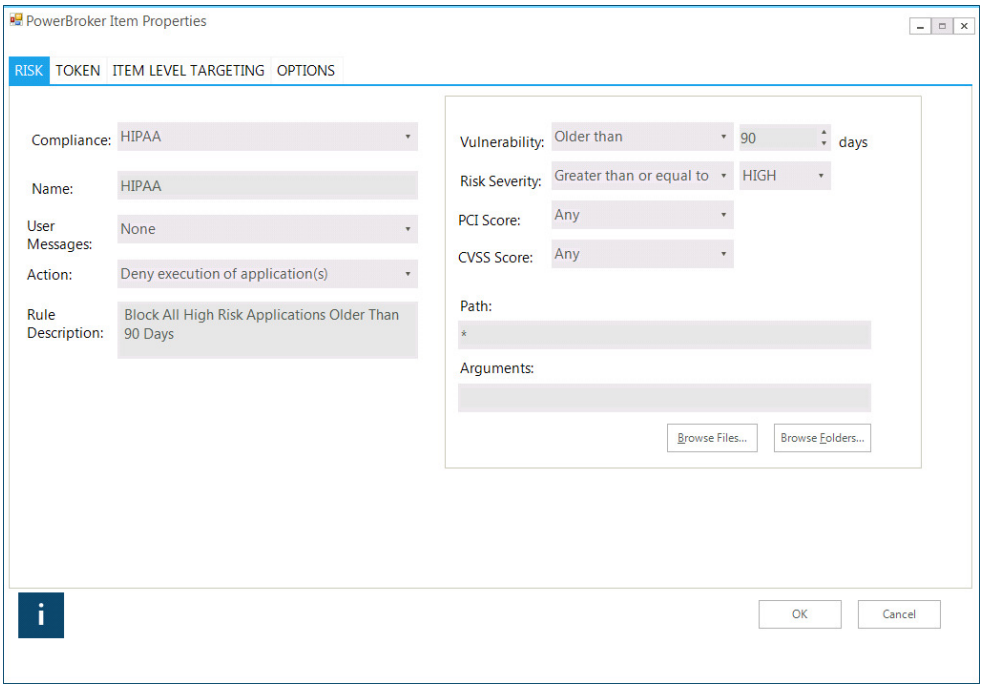
The PowerBroker for Windows User Interface is now fully integrated with the Group Policy Management Editor. In addition to the rules, User Messages and Passcode Generator can be accessed directly from the MMC tree view. Various UI components, including Passcode Generator, have also been updated to match the integration work.

Risk and Compliance (#16060)

A new rule type, Risk and Compliance, has been added to PowerBroker for Windows:



This rule type can be used to elevate, block, or allow applications based on vulnerability data. Applications can be targeted based on age of the audit information, risk severity, PCI Score, CVSS Score, and Path/Arguments. In addition, User Messages and Item Level targeting may also be used with this rule type.



IMPORTANT: BeyondInsight is required in order to use this feature.

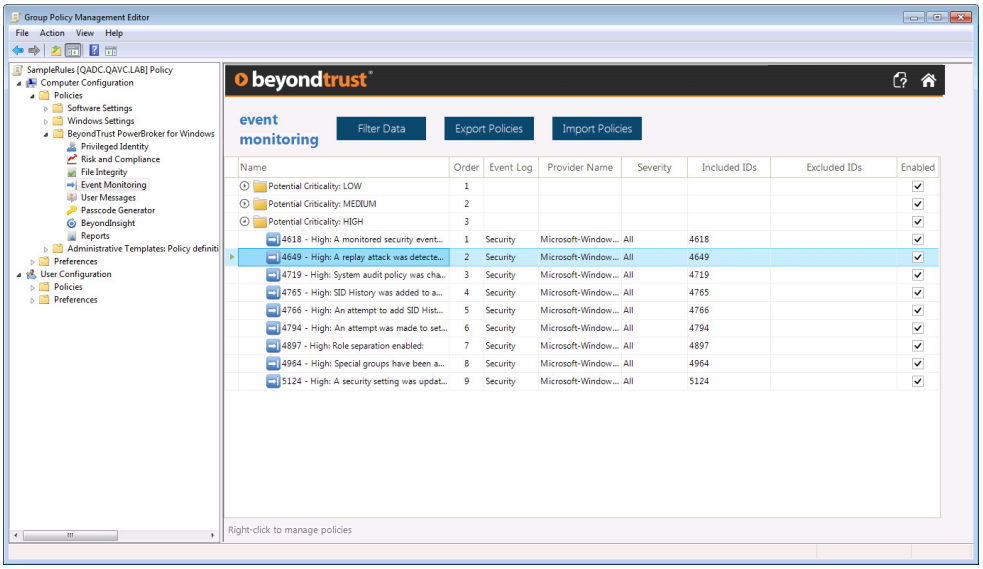
Audit Version (#16235)

The audit information is transferred to the client from BeyondInsight. This is saved to the registry in the following location: HKEY_LOCAL_MACHINE\SOFTWARE\BeyondTrust\Service\AuditsVersion.

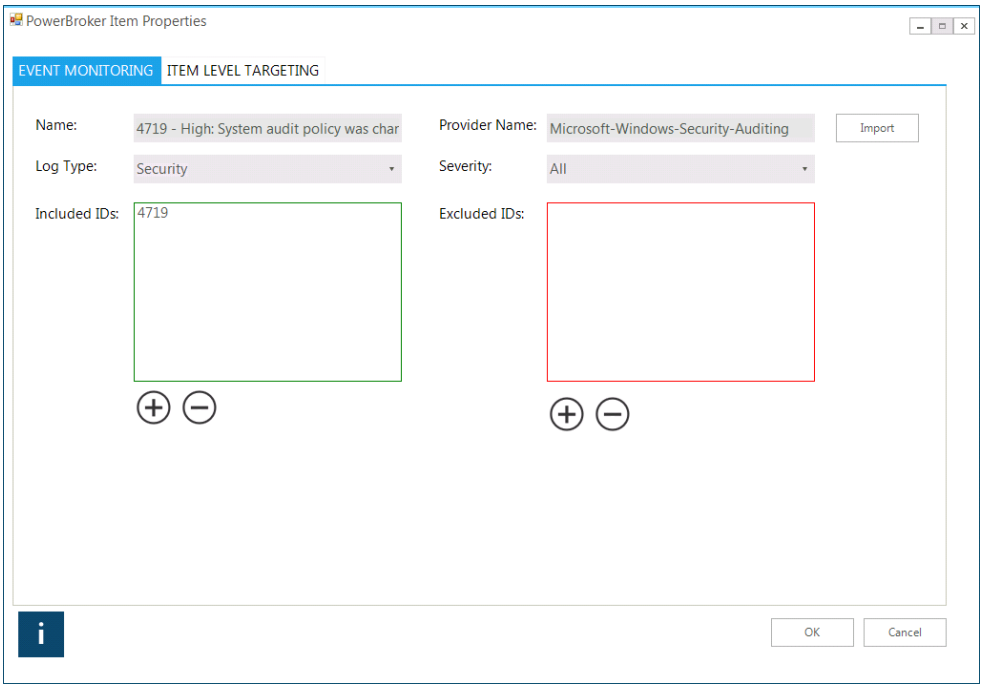
NOTE: The audits data is saved on the client to C:\Windows\BeyondTrust\pbd\config\rcs\Audits.transformed.xml. This file does not contain the version number.

Windows Event Monitoring (#16103)

A new rule type, Event Monitoring, has been added to PowerBroker for Windows:



This feature enables Windows Event Logs to be forwarded to BeyondInsight based on Log Type, Provider Name, Severity, and ID. Item Level Targeting may also be used with this rule type in Group Policy mode.



On initial install it will scan past events for anything that matches rules that are in place. It saves the last time of scan and record numbers to avoid reporting of duplicate events in the registry under HKEY_LOCAL_MACHINE\SOFTWARE\BeyondTrust\WinEvtFwd.

NOTE: Log Type, Provider name, and Severity are required fields. The name is based on data in the XML and may vary according to the event format. If "EventSourceName" is present then it is treated as a source name, otherwise "Name" is used. To easily import the data, copy an event from the Windows event log and click the "Import" button. The fields will automatically be populated based on the data in the event.

If Windows Event Monitoring is configured to forward PRIVMAN events, it is recommended to enable the "Turn off Windows Event Logging of Application Launch Data" setting to avoid duplicate data being sent to BeyondInsight.

Windows Event Monitoring is not supported on Windows XP.

Rules Library (#16109)

The Rules Library has been added to the Snap-In Installer as an optional component.

Event Monitoring/Risk and Compliance Sample Rules (#16259)

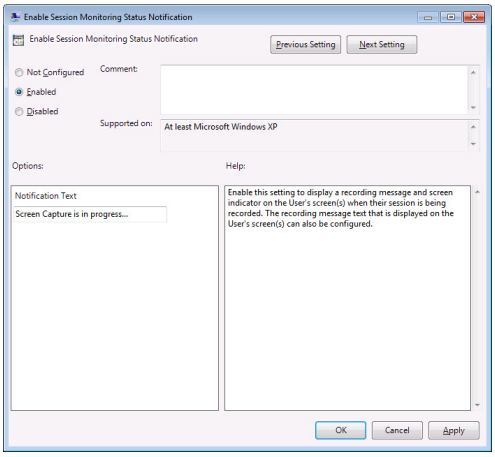
Sample Event Monitoring and Risk and Compliance rules have been added to the Rules Library. The sample Event Monitoring rules are based on the Microsoft Best Practices for monitoring events.

BeyondInsight Integration and Reports (#16123)

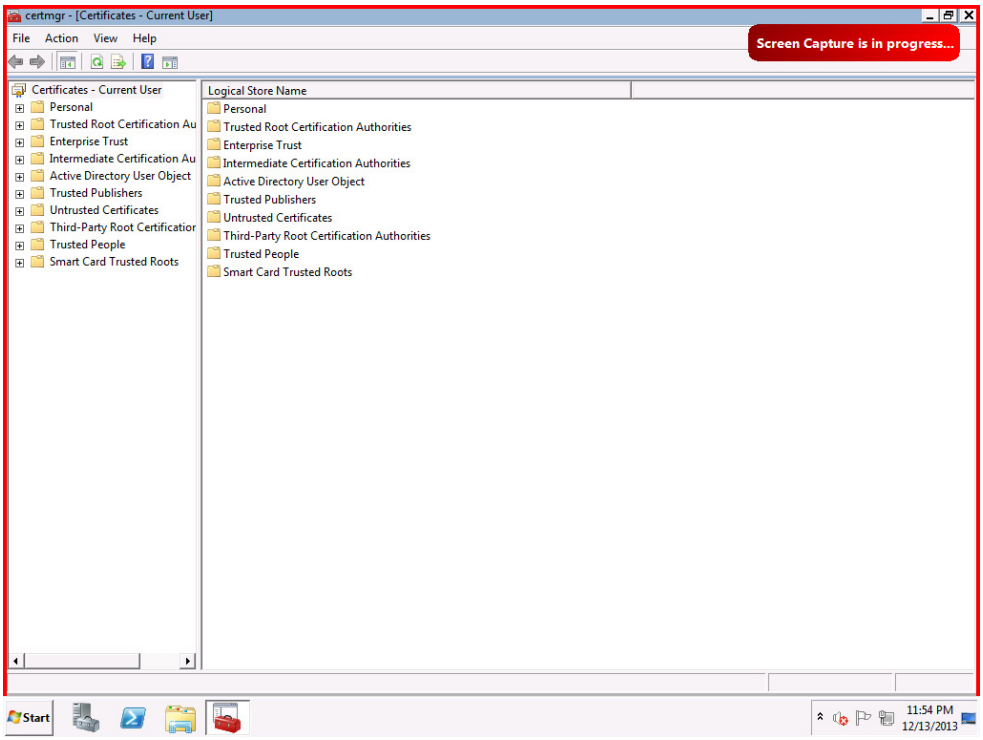
BeyondInsight and Reports can now be access directly from within the PowerBroker for Windows UI. The BeyondInsight URL must first be configured either on install or via ADM(X) setting.

Session Monitoring Notification (#16170)

There is now an option to notifiy the user that their session is being recorded. This is a global setting configurable in the Session Monitoring section of the ADM(X)\Settings.



When this setting is enabled, when a user's session is being recorded they will be notified by a red border around all monitors as well as the text "Screen Capture is in progress..." This text is configurable in the ADM(X) template\Central Policy Settings.



Privacy Mode (#16248)

A global setting to "Enable Privacy Mode" has been added under Management. When enabled, this setting will replace user names with a unique hash for data sent to BeyondInsight.

NOTE: The user hash may not be decrypted by BeyondInsight.

IMPORTANT: Hashing on user names for data privacy during session monitoring is not supported at this time.

ENHANCEMENTS

Session Monitoring: Passwords (#16277)

Passwords are no longer captured for Windows applications that have the field masked.

IMPORTANT: This will not work for passwords entered in web browsers. To exclude web browsers and other applications from keystroke logging, enable "Configure keyboard logging excluded apps" in the Session Monitoring Settings.

Process Security (#14916)

The following options were added to Process Security: Set Session ID, Suspend/Resume, Change Permissions, Change Owner.

Authorization User Message (#15832)

The option to minimize the authorization user message has been added.

Passcode Message Email Content (#15833)

Default text may now be configured for emails requesting passcode authorization. The Email Introduction property has been implemented in the Authorization section of App Launch and Blocked App user messages. Text configured in this field will appear at the top of passcode authorization request emails.

Turn off Windows Event Logging of Application Launch Data (#16065)

A new setting was added to prevent data from being logged to the Windows Event log for the application launch events. This setting, "Disable Windows Event Logging of Application Launch Data" appears in the Security Driver section of the ADM(X)/BeyondInsight Settings.

NOTE: All other events should still be logged when this setting is Enabled. Only 28691-28699 should not be logged to the Windows Event log.

Arguments in Publisher Rules (#16101)

Publisher Rules now support targeting based on arguments.

PolicyUpdate.exe (#16139)

RCSUpdate.vbs has been converted to a command line tool that is now installed to the following location on the client: c:\windows\beyondtrust\BeyondInsight\policyupdate.exe. When running in Central Policy mode, running this tool will update the PowerBroker for Windows policies with the latest from BeyondInsight.

Client: Command Line Install (#16190)

The command-line install of the client has been simplified. To install via the command line, use the following syntax:

pbwcl64.msi /qn ADDLOCAL=[FEATURELIST] SERVER=[SERVERNAME] CERTIFICATE=eEyeEmsClient WORKGROUP="BeyondTrust Workgroup"

Replace [FEATURELIST] with comma-delimited list of features. PBWClient,Client_XX, Runtime_XX are required.

For example, to install all components except session monitoring and Central Policy Integration:
pbwcl32.msi /qn ADDLOCAL=PBWClient,Client_x86,Runtime_x86,EventMonitor_x86,FileIntegrity_x86,IEIntegration_x86
pbwcl64.msi /qn ADDLOCAL=PBWClient,Client_x64,Runtime_x64,EventMonitor_x64,FileIntegrity_x64,IEIntegration_x64

To install all components except file integrity and event monitoring, and run policy in BeyondInsight Central Policy mode:
pbwcl32.msi /qn ADDLOCAL=PBWClient,Client_x86,Runtime_x86,SessionMonitor_x86,IEIntegration_x86,CPIntegration SERVER=[SERVERNAME] CERTIFICATE=eEyeEmsClient WORKGROUP="BeyondTrust Workgroup"
pbwcl64.msi /qn ADDLOCAL=PBWClient,Client_x64,Runtime_x64,SessionMonitor_x64,IEIntegration_x64,CPIntegration SERVER=[SERVERNAME] CERTIFICATE=eEyeEmsClient WORKGROUP="BeyondTrust Workgroup"

x64 [FEATURELIST]:
REQUIRED:PBWClient,Client_x64,Runtime_x64,
CENTRAL POLICY INTEGRATION: CPIntegration
EVENT MONITORING: EventMonitor_x64
FILE INTEGRITY: FileIntegrity_x64
ACTIVE X\IE Rules: IEIntegration_x64
SESSION MONITORING: SessionMonitor_x64

x86 [FEATURELIST]:
REQUIRED: PBWClient,Client_x86,Runtime_x86,
CENTRAL POLICY INTEGRATION: CPIntegration
EVENT MONITORING: EventMonitor_x86
FILE INTEGRITY: FileIntegrity_x86
ACTIVE X\IE Rules: IEIntegration_x86
SESSION MONITORING: SessionMonitor_x86

Snapin Folders (#16071)

The "Shared" folder is no longer created by the Snap-In installer. These files are now installed to the PowerBroker for Windows folder.

FIXES

Prevent Privman from being loaded into specified processes (#16058)

The exclusion list setting "Prevent Privman from being loaded into specified processes" (ExcludedApps) has been re-added to the ADM(X) and BeyondInsight Settings.

IMPORTANT: Privman will still appear to be loaded in excluded processes, but will not have any effect. This was done to prevent potential issues with unloading, but still allow the dll to effectively be excluded.

Item-Level Targeting (#16173)

Hitting the delete key in a text field in item-level targeting will no longer delete the filter.

Installer: Modify Option (#16301)

pmbho.dll is now registered correctly when IE Integration is added via the "Modify" option in the installer.

Issue with LDAP binds (#16281)

An intermittent issue was resolved that could cause a crash in wscript.exe with LDAP binds.

PowerBroker® for Windows® 6.1 - Released 16 September 2013

INFORMATION

Upgrading from 6.0.1 (#16132)
If you are manually upgrading the client from 6.0.1, an uninstall and reboot before installing 6.1 is recommended.

IE Rules and User Messages (#15421)
User Messages are not supported with rules on Internet Explorer.

RCS Policy Intervals (#15981)
In a production environment, the intervals for the heartbeat, policy validation and variance should never be set to 0.

ENHANCEMENTS

Custom Certificates (#16093)
Custom certificates are now supported for Retina CS communication.

Citrix XenApp 6.5 (#15083)
A fix has been implemented to improve support for Citrix XenApp 6.5.

AppInit_DLLs (#16166)
The full path to btpload32.dll/btpload64.dll is now written to the AppInit_DLLs registry key.

RCSUpdate.vbs (#15971)
RCSUpdate.vbs now has improved error reporting.

File Integrity Logging (#15476)
Policy Monitor (polmon) now supports File Integrity logging.

ADM(X) Settings (#16058)
"Prevent Privman from being loaded into specified processes" has been removed from ADM(X) and RCS mode settings, as it is no longer required or supported.

"KeepBtploadLoadedForApps" is no longer effective and has been replaced by "UnloadBtploadLoadedForApps". This setting only applies when Profiling is NOT enabled for the application and is for troubleshooting purposes only.

Session Monitoring (#16049)
When a session monitoring enabled rule is applied, data is now captured immediately upon application launch.

Multi-Select Privileges (#15485)
The ability to select all or multiselect to enable/disable privileges has been added.

Trace Logging (#15999)
The User Interface now has trace logging. Set the following registry key to enable logging:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BeyondTrust\UI
REG_SZ: LogFilePath
Value: Set to folder name

File Integrity and Wildcards (#15952)
Wildcards (*,?) are now supported for File Integrity rules in the application path and arguments fields.

IMPORTANT: Wildcards are NOT currently supported in the file name or if used after the backslash trailing the directory name. (i.e. c:\myfolder*) (#16072). In addition, if a wildcard is used in the folder name on a Deny rule, the folder name will not be protected (#16112).

Session Monitoring (#15944)
In addition to the Custom Token and Add/Remove Admin Rights actions, session monitoring rules will now take effect when the rule action is set to "No Change" (passive mode).

Retina CS Policies (#15941)
In RCS Mode, the server, workgroup, and certificate names are now pre-populated in the UI based on registry settings for a new policy.

NOTE: Existing policies stored in Retina CS will not be changed.

Modify/Repair Installation (#13198)
The options to Modify or Repair the installation have been added.

FIXES

BTService crash (#16084)
An issue was resolved that would sometimes cause btservice to crash when file integrity rules were in place.

Passcode Generator (#16085)
Issue was resolved that would sometimes cause the following error: "Cannot create a stable subkey under a volatile parent key."

NOTE: Workaround for prior versions: Reboot and run passgen immediately after logon.

Windows 8 x86 install (#16075)
BTservice is now installed correctly on Windows 8 x86.

User Messages (#16028)
The focus is now automatically set to the Justification textbox for user messages containing both authorization and justification fields.

User Messages and SpiderOak (#16016)
User Messages now display when SpiderOak is installed and a .cmd file is launched.

File Integrity Deny rule (#15608)
If a File Integrity Deny rule is in place, the user can no longer modify or remove the targeted directory.

Toolbar buttons (#15543)
Issues with some of the legacy toolbar buttons have been resolved.

Publisher Rules (#16023)
Publisher Rules imported with Custom Values may now be modified after import.

MSI Rules (#15975)
MSI Rules ending in a wildcard are now correctly set to MSI_PATH.

File Integrity - Product Version (#15950)
The Product Version is now detected correctly for Windows files.

Publicpass.xml (#15911)
For ease of upgrade, the client installer no longer removes publicpasss.xml on uninstall.

Session Monitoring and UAC Rules (#15696)
The Session Monitoring option has been greyed out for UAC rules since it is not supported.

PowerBroker® for Windows® 6.0.1 - Released 14 June 2013

FIXES

Slider on Publisher Rule (#15966)
When editing a Publisher Rule, the slider control may now be used.

Publisher Rules (#15980)
The behavior of the Custom Values checkbox has been fixed.

Display of Collections (#15979)
A display issue with collections has been resolved.

Tree View Navigation (#16003)
The location in the tree view is now retained when viewing rules.

NOTE: The legacy tree view will still be refreshed on editing rules.

Legacy UI display (#15992)
Display issues have been resolved in the snap-in list view.

Importing Rules (#15982)
An issue with importing rules has been resolved.

File Integrity Events (#15882)
An issue with duplicate File Integrity events has been resolved.

Rule Wizard (#15959)
If you create a rule in an enforced collection using the Rule Wizard, the correct action will now be shown in the tree view.

Rule Wizard (#15987)
The Rule Wizard now accommodates longer collection names.

BeyondTrust EPP compatibility (#15997)
The 32-bit client installer now writes the correct registry key required for EPP compatibility.

Upgraded Rules (#16000)
Upgraded rules will now work correctly when the Session Monitoring checkbox is selected.

Loading Rules (#16006)
Privileged Identity rules are now loaded when a File Integrity rule is edited.

User Messages (#16032)
The Help URL is now displayed in the UI on a blocked message.

PowerBroker® for Windows® 6.0 - Released 31 May 2013

INFORMATION

Challenge-Response Keys (#15863)

On upgrading PowerBroker for Windows from prior versions, the private and public keys must be regenerated. Public keys must be re-distributed to the clients with the upgrade to 6.0. The new certificate and registry keys must be distributed to any machines that will be generating passcodes.

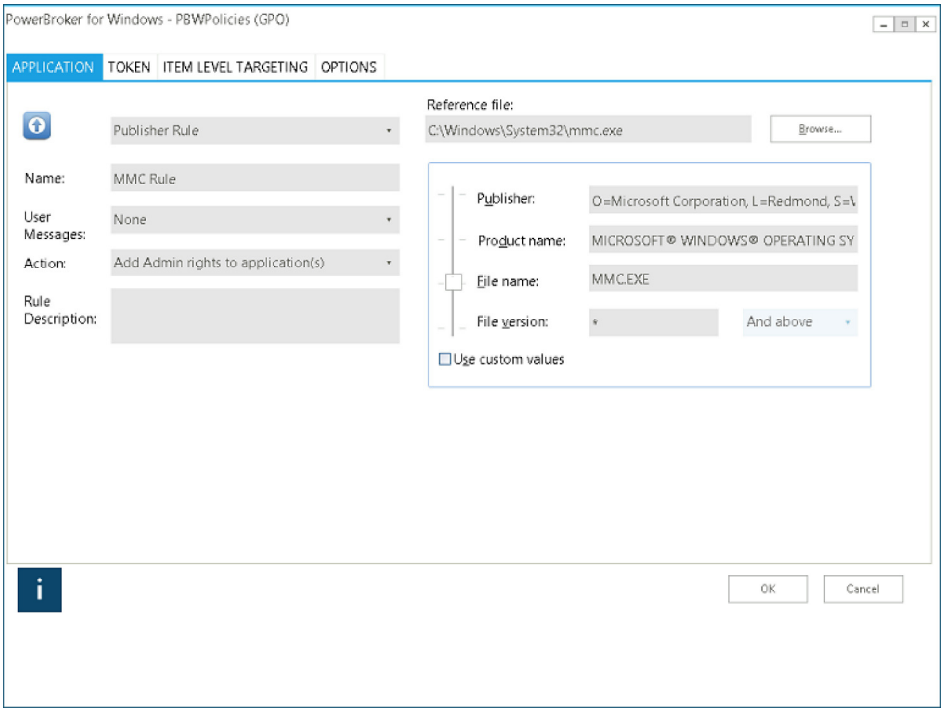
Refresh Issue (#15845)

There is an intermittent display issue when there are more than 3 levels of collections in the legacy snapin. To work around the issue, refresh the screen, or view the collections and rules using the new user interface.

NEW FEATURES

User Interface Refreshed and Redesigned (#15455)

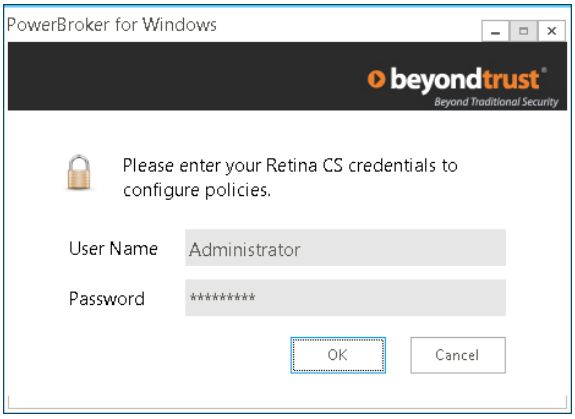
The user interface has been redesigned for a simpler, cleaner, and more intuitive user experience.



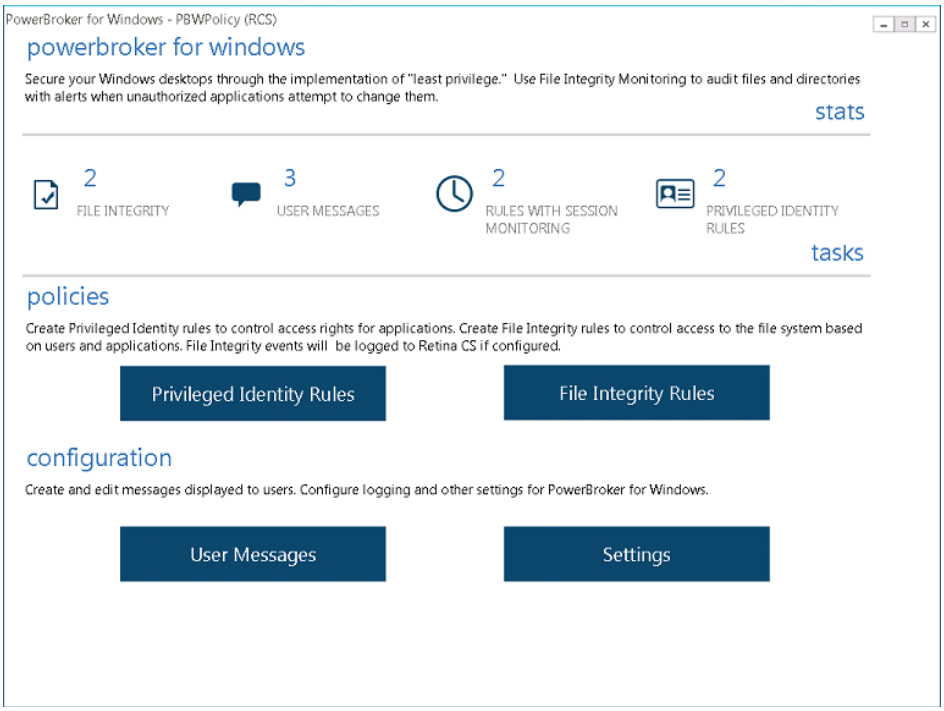
Retina CS Policy Distribution (#15861)

PowerBroker for Windows policies may now be deployed from within Retina CS. Group Policy is no longer required, but may still be used.

When the Central Policy option is selected on the snapin install, a link is added to the Windows Start Menu that will launch the user interface in Retina CS Mode:

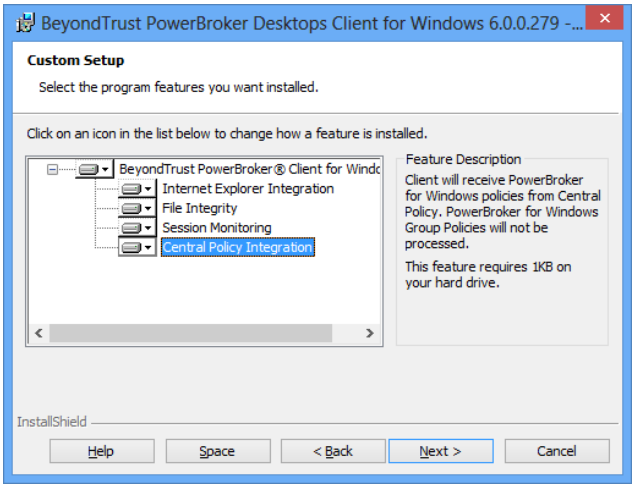


A common user interface is used for either Group Policy or Retina CS policy deployment.

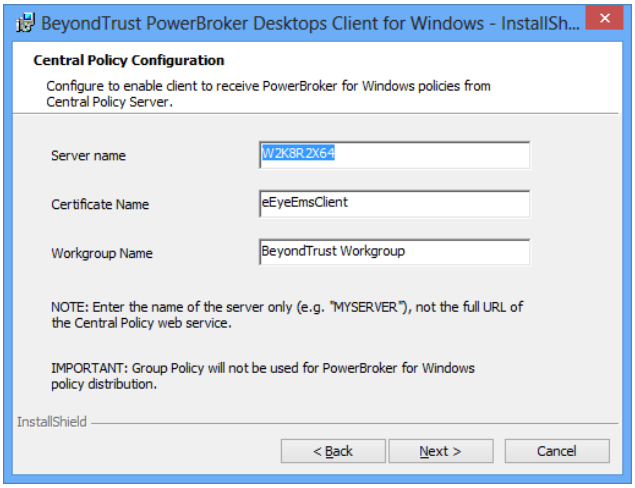


NOTE: Item Level Targeting is only available in GPO Mode.

The client installation also has a new option called "Central Policy Integration".



Selecting this option at install time will enable you to configure PowerBroker for Windows to accept policies from Retina CS.



The Retina CS certificate installer (certinstaller.msi) should be run before installing the client.

In addition, these options may be configured using a command line install. To install all client components, use the following syntax:

pbwcl64.msi /qn ADDLOCAL=ALL SERVER=[SERVERNAME] CERTIFICATE=eEyeEmsClient WORKGROUP="BeyondTrust Workgroup"

RCS Mode: Heartbeat Events (#15886)

In Retina CS Mode, heartbeat events (event ID 28701) are sent synchronously, and are not written to the storeonfailure file.

Settings in RCS Mode (#15870)

For the Retina CS Management Settings, the Server Name, Workgroup, and Certificate name settings will only be distributed to the client in RCS mode if they are modified from the defaults. This is to avoid overwriting any settings populated by ADM\ADMX and to retain connectivity to Retina CS.

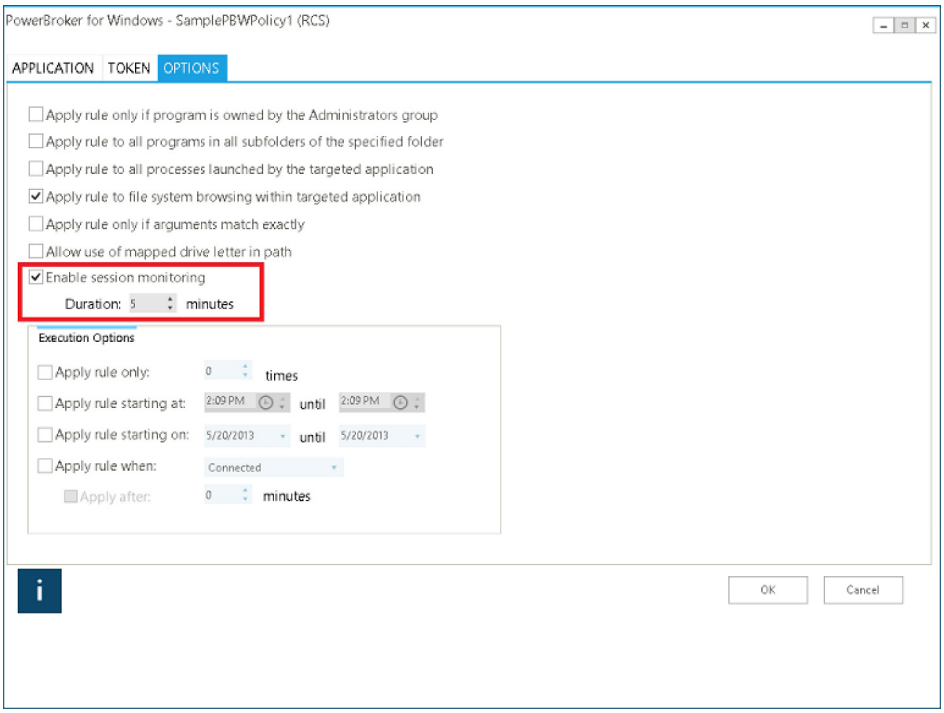
In an environment that is using both Retina CS policy deployment and group policy:

1. Prior to installing the client, ensure that the ADMX settings are not applied to machines receiving Retina CS policy.
--OR--
2. Ensure that the ADMX settings match the Settings in Retina CS.

Session Monitoring (#15696)

A new feature has been added to record screen captures, keystrokes and mouse clicks while a PowerBroker for Windows rule is in effect. This data can then be forwarded to Retina CS for viewing.

NOTE: Not all rule types (e.g. UAC and Passive rules) are compatible with Session Monitoring.



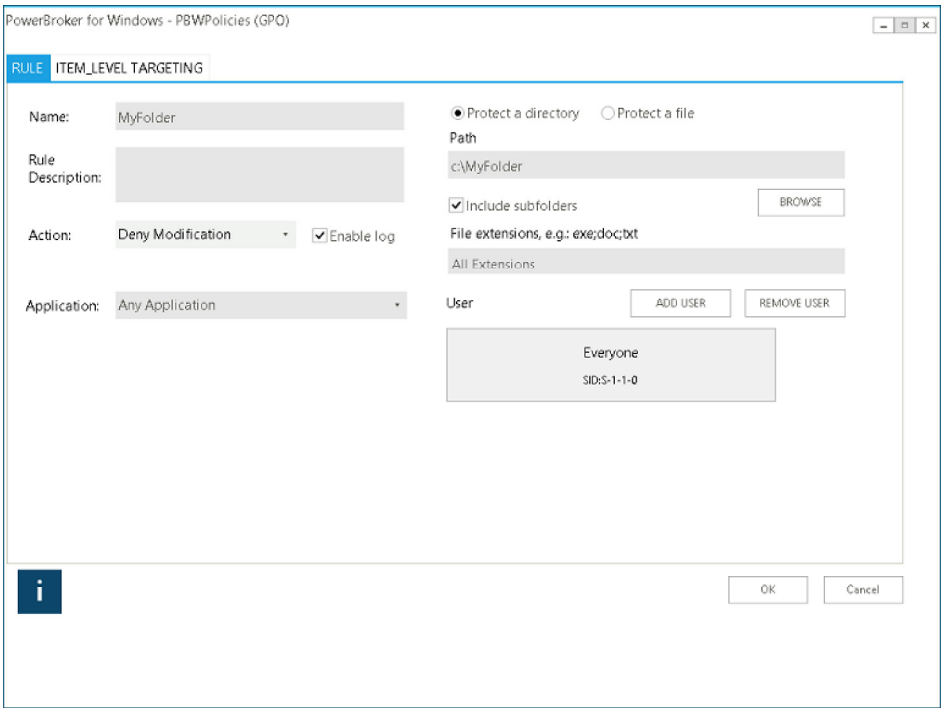
The PowerBroker for Windows client installer will install the Session Monitoring component by default. However, it is an optional component and may be deselected.

IMPORTANT: In order for Session Monitoring logs to be sent to the Retina CS Server, the full URL must be configured in the registry. This will happen automatically on install, but if the URL is changed either via ADM\ADMX or in the Settings, the full URL must be specified. (i.e. https://MYSERVER/EventService/EventService.svc)

File Integrity (#15464)

A new feature has been added to track and/or prevent changes to the file system based on the application or user.

NOTE: File Integrity functionality is only supported on Windows Vista and above.



The PowerBroker for Windows client installer will install the File Integrity component by default. However, it is an optional component and may be deselected.

NOTE: File Integrity functionality is not supported on Windows XP.

File Integrity Driver (#15875)

BTService must be stopped before stopping the file integrity (privmanfi) driver.

File Integrity Messages (#15843)

The operating system is used for relaying "Deny" messages to the user. UAC messages may be displayed under certain circumstances; however, a user who has been denied access rights will be unable to use UAC to modify protected files.

File Integrity Directories (#15608)

To protect the parent directory itself as well as the contents, create two rules on the directory - one with "Protect a directory" selected, and one with "Protect a file" selected.

File Integrity Wildcards/Partial Paths (#15952)

Wildcards/Partial Paths are not currently supported for File Integrity rules.

File Integrity File Versions (#15950)

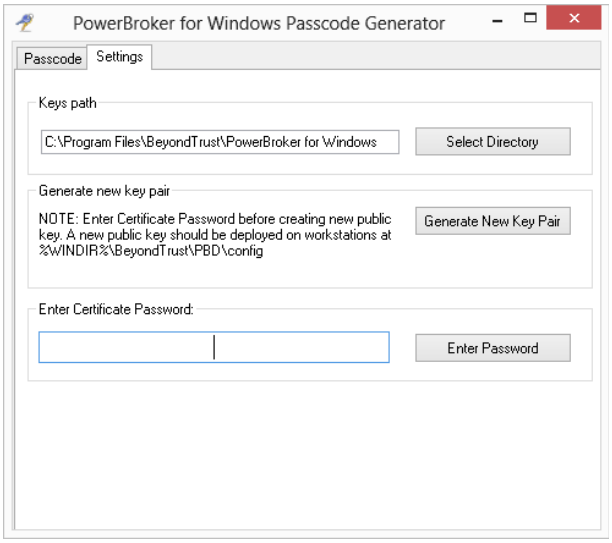
File Integrity rules currently use the version from .MUI files, which may differ from the version displayed in the file properties.

ENHANCEMENTS

Passcode Generation (#15461)

A certificate is now required for Passcode Generation.

IMPORTANT: On upgrading from prior versions, a new certificate and key pair must be generated, and the public key distributed to all clients.



NOTE: The Snapin Installer may now be used to only install the Passgen component.

FIXES

Issue with cvtres.exe (#15626)

Cvtres.exe no longer generates a console window during iPass service startup when cvtres.exe has been elevated.

User Messages and Justification (#15584)

When Justification and Authentication are both enabled on a user message, the Justification is no longer limited to 44 characters.

PowerBroker® for Windows® 5.5.3 - Released 27 March 2013

INFORMATION

Internet Explorer 10

Internet Explorer 10 launches both 64-bit and 32-bit processes. In order to elevate a web site, both executables must be targeted. This can be accomplished either with a wildcard (i.e. C:\Program Files*\Internet Explorer\iexplore.exe) or by using two separate rules. In addition, "Apply rule to all processes launched by the targeted application" must be enabled.

FIXES

Windows 8 - btpload64.dll (#15529)

Btpload64.dll is now installed to the system32 directory on Windows 8.

"+" Button (#15533)

The "+" button will now work to add a rule.

Column Sorting (#15532)

The column sorting in the snapin now works correctly.

File System Browsing and Child Processes (#15458)

When child processes are elevated and the "Apply rule to file system browsing within the application" checkbox is enabled, the file system dialog now drops admin rights.

Symantec Endpoint Protection (#15448)

An issue was resolved with launching installers when SEP was present.

Performance (#15444)

An issue was corrected where, under certain circumstances, there was a performance issue on launching applications.

PowerBroker® for Windows® 5.5.2 - Released 21 February 2013

FIXES

Registration of pbwrcsclient.dll (#15441)

Symantec Endpoint Protection no longer prevents pbwrcsclient.dll from being registered on install.

Compatibility issue with Symantec Endpoint Protection (#15437)

A compatibility issue was resolved with Symantec Endpoint Protection and certain .NET applications.

Group Policy Update (#15436)

An issue was resolved with the licensing check on group policy update.

PowerBroker® for Windows® 5.5.1 - Released 16 January 2013

FIXES

Item-Level Targeting (#15426)

The Item-Level Targeting dialog now launches correctly.

PowerBroker® for Windows® 5.5 - Released 15 January 2013

INFORMATION

Internet Explorer 10 on Windows 8 (#15395)

ActiveX and Internet Explorer rules are supported on the Windows 8 Desktop user interface. They are not supported in the Windows 8 App Store ("Metro-style") user interface.

Internet Explorer Elevation (#15423)

Internet Explorer 10 for Windows 7 is not currently supported. The 64-bit version of Internet Explorer 9 is not supported for Internet Explorer rules and ActiveX rules. For Internet Explorer 8 on Windows XP, navigating between elevated\unelevated sites in the same window is not supported. In addition, the integrity level on Internet Explorer rules must be set to High.

Windows 8 App Store User Interface (#15395)

PowerBroker for Windows rules are not supported in the Windows 8 App Store ("Metro-style") user interface. Applications that are launched from the App Store UI but run on the desktop may be elevated.

Windows 8: Windows Firewall - Advanced Settings

On Windows 8, Windows Firewall - Advanced Settings requires an additional rule on c:\windows\system32\shpafact.dll.

NEW FEATURES

Windows 8 Support (#15416)

PowerBroker for Windows now supports Windows 8 Desktop applications. Internet Explorer 10 64-bit on the Windows 8 Desktop is now supported.

IMPORTANT: The .NET Framework 2.0 must be installed prior to installing PowerBroker for Windows in order for Retina CS logging to work.

ENHANCEMENTS

Item-Level Targeting (#15393)

Windows 8 has now been added to the Item-Level Targeting options.

IE Elevation Message Box (#15403)

There is no longer a message box when navigating between elevated and unelevated sites.

FIXES

System Event Service (#15415)

An error no longer occurs on logon when Retina CS logging is enabled.

Internet Explorer Elevation (#15316)

An issue was resolved with Internet Explorer elevation.

Snap-In Uninstall (#15390)

The Snap-In uninstall no longer removes privatepass.xml.

Client Uninstall (#15391)

The Client uninstall no longer removes publicpass.xml.

Welcome Screen set to Czech Republic (#15388)

Policies now trigger correctly when the Welcome screen is set to Czech Republic.

TestConnection (#15381)

TestConnection now shows the correct return status each time.

Rule Wizard (#15392)

The Rule Wizard Execution Options now default to the current day.

PowerBroker® for Windows® 5.4.1 - Released 19 December 2012

ENHANCEMENTS

Tracing for RCS (#15383)
In the ADMX template there is now an option under Management to Enable Retina CS Trace Logging. This creates a trace log on the client that can be used for troubleshooting purposes.

Heartbeat Events (#15380)
Heartbeats are now logged to system event log.

TestConnection.exe (#15382)
TestConnection now sends a true heartbeat event.

FIXES

Regional Settings (#15394)
Events will now be processed correctly when the client regional settings are set to something other than en-US.

Registry Keys (#15405)
The InstallerID and ClientVersion registry keys are now written correctly when UAC is enabled.

Asynchronous event logging (#15371)
The RCS asynchronous event logging option now works correctly.

Heartbeat interval (#15374)
The heartbeat interval now works correctly when set to "0".

PowerBroker® for Windows® 5.4 - Released 26 November 2012

INFORMATION

Rebranding (#15272)
BeyondTrust PowerBroker Desktops has been rebranded as PowerBroker® for Windows®.

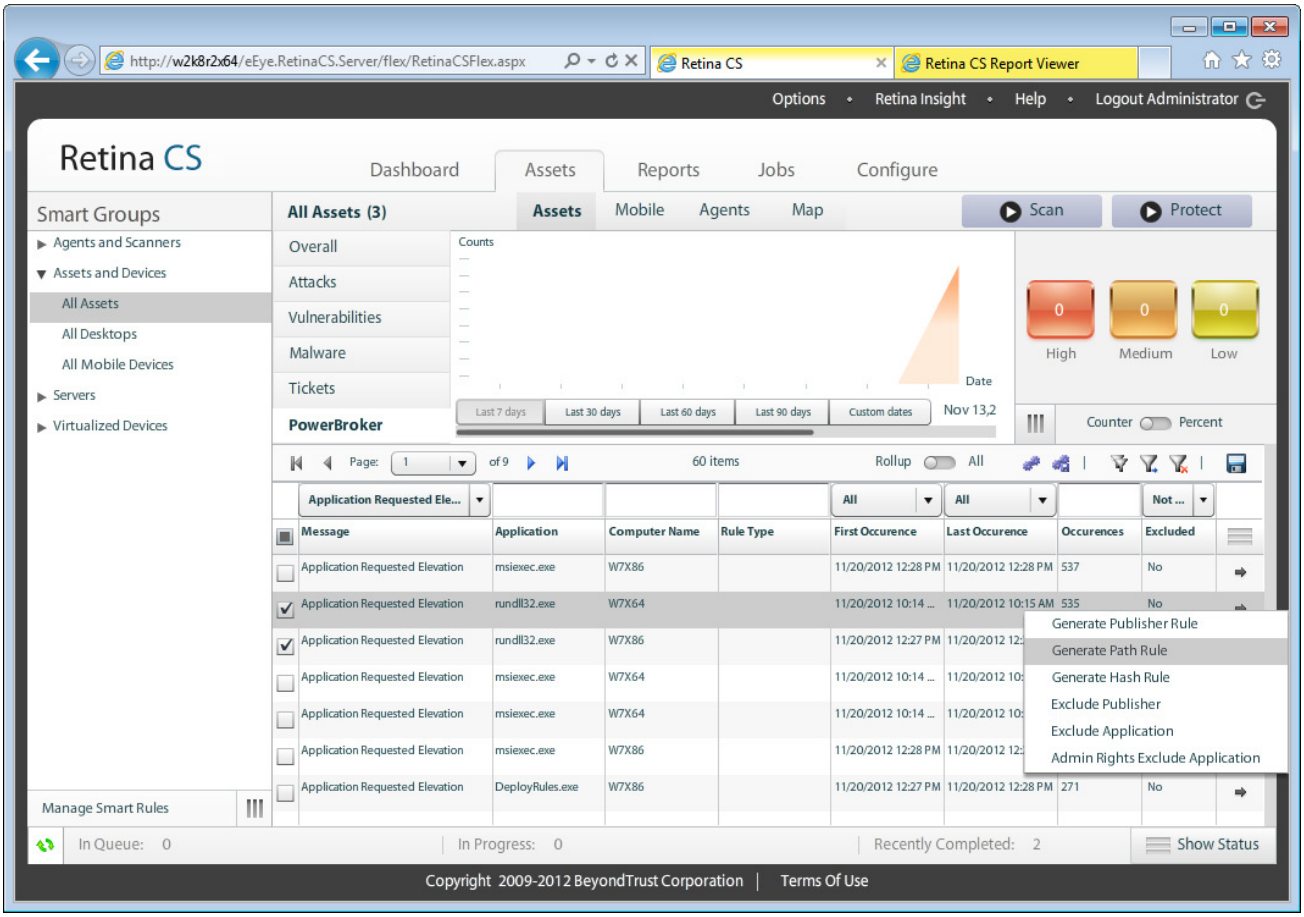
Certificates (#15373)
Event IDs 28680 and/or 36885 may be generated if there are too many trusted certificates installed. To resolve, remove the certificates that are not needed.

PBReports (#15302)
PBReports has been removed from the installer. This functionality has been replaced by Retina CS integration. The local user reports will be implemented in a future release.

NEW FEATURES

Retina CS Integration (#15301)
PowerBroker for Windows now integrates with Retina CS for reporting and rule generation.

IMPORTANT: In order to use the Retina components for reporting, the .NET Framework 2.0 must be installed on the client prior to installing PowerBroker for Windows 5.4.



FIXES

User Messages (#15233)
Some display issues with User Messages in the snap-in have been resolved.

RAM Filter (#15141)
An issue with filtering on RAM on Windows 2008 R2 has been resolved.

User Type (#14809)
The User Type field in the event data has been renamed Process Type.

Backup\Restore rules (#15110)
The Backup\Restore rules in the templates have been updated.

User Messages (#15277)
An issue was resolved with user messages.

Copy and Paste (#15299)
An issue with copying and pasting rules in the snap-in has been resolved.

PowerBroker® Desktops 5.3 - Released 20 August 2012

INFORMATION

Management Pack (#15039)

Beyondtrust.akm has been removed from the installer.

Logo Field (#15052)

The Logo field in User Messages has been replaced by the customizable header.

Custom Images (#15233)

If changing any properties in the Header section of an existing message for which the Background Type is Custom Image, you must re-select the Image file path immediately before making your changes to the header. Otherwise, changes to the header may not take effect.

Message Types and Compatible Rule Actions (#15237)

When selecting a message to apply to a rule or collection, ensure that the message type is compatible with the rule action. This is especially important for Blocked and Passive Rule actions, and with the Passcode functionality.

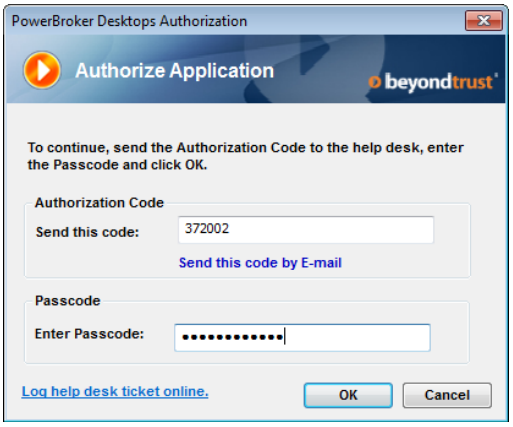
Blocked Application Message and Header Text (#15235)

When configuring a Blocked Application message with the Default BeyondTrust header graphic, shorten the header text to ensure no overlap occurs with the background logo.

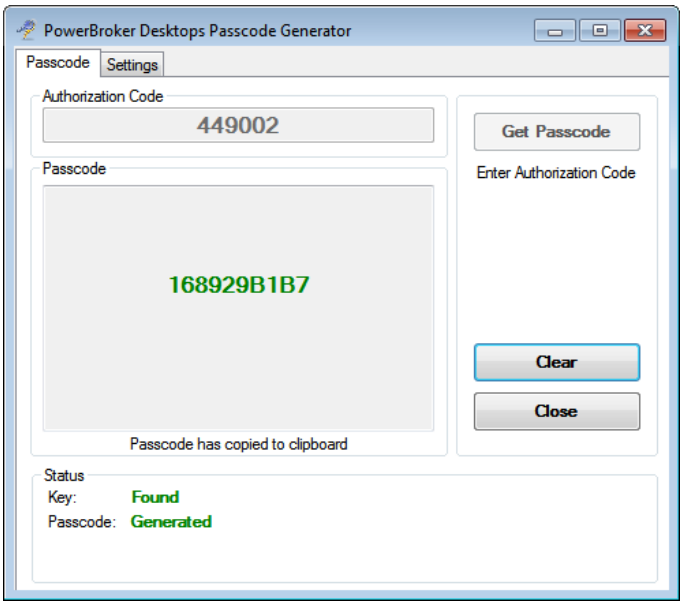
NEW FEATURES

Challenge/Response (#14881)

To provide a user with immediate one-time access to an application requiring authentication, you can provide an option for the user to obtain and enter a Passcode for authorization instead of credentials. Using an authorization dialog, the user can obtain an Authorization Code for the launch attempt (generated using a public key) and send it to a specified email address.



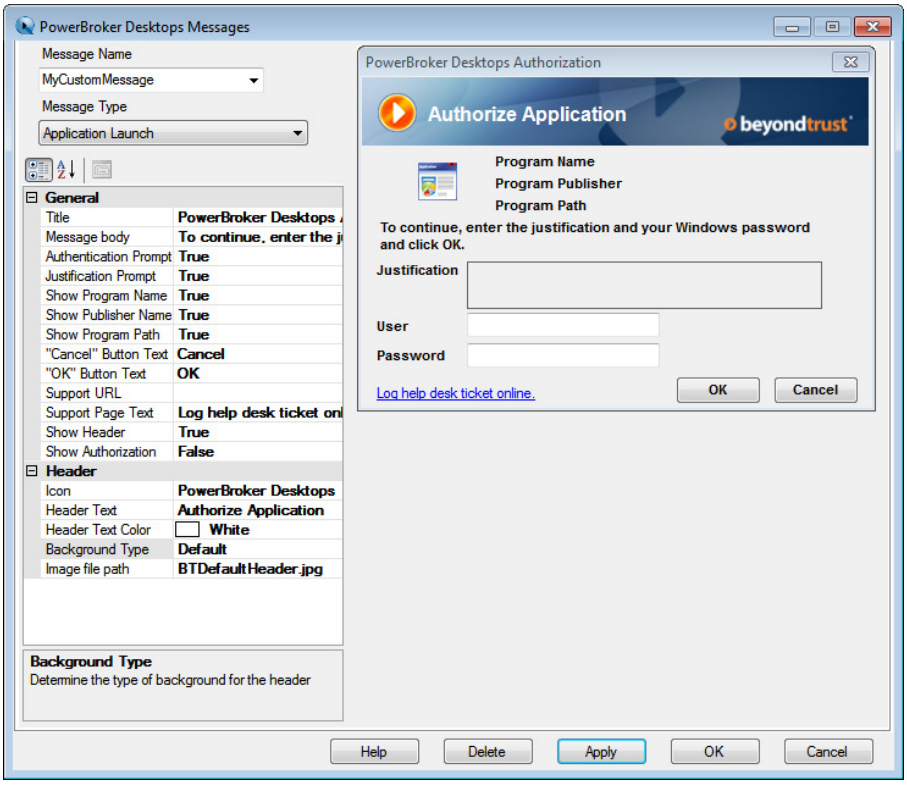
An administrator enters the Authorization Code into the Passcode Generator to produce a Passcode, and then provides it to the user to allow one-time access to the application. This functionality is available by using Application Launch and Blocked Application messages.



User Messages Enhancements (#14882)

User Messages now support customized message headers. This includes the ability to set custom background and text colors. Alternately, instead of setting a background color, there is now the option to display either a Default BeyondTrust graphic or a custom graphic in the header.

NOTE: The recommended size for a custom image in the header is by 415 X 56 pixels.



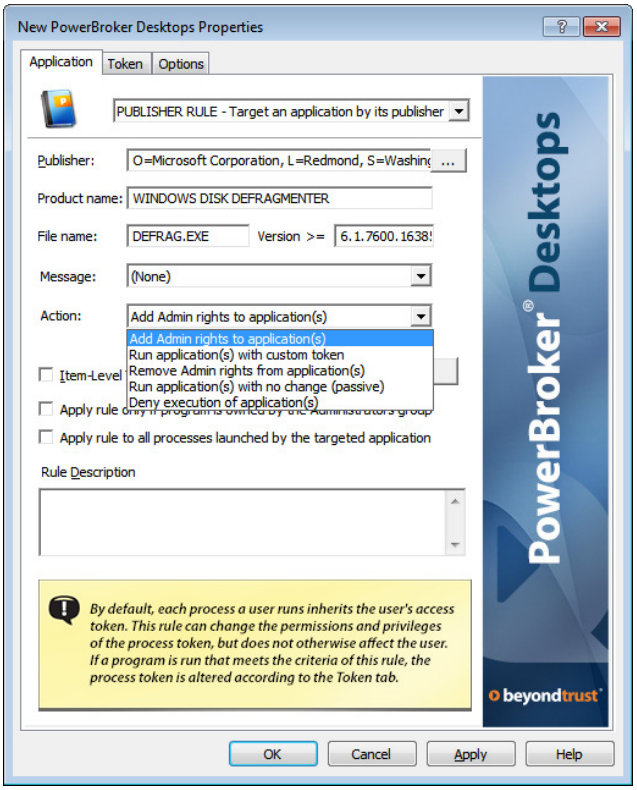
Support for Hyperlinks (#14884)

The ability to specify a hyperlink in a user message has been added.

NOTE: If a hyperlink is added to a message that appears on the secure desktop (i.e., one where credentials may be typed in), the user message will be closed in order to leave the secure desktop and display the URL. At this time, hyperlinks are launched only with Internet Explorer.

Additional Rule Actions (#14885)

Two new rule actions have been added:



Add Admin rights to application(s)
The application is run with local Administrator rights added. Any changes to the permissions, privileges, and integrity level previously configured in the rule are removed and replaced with pre-configured rights.

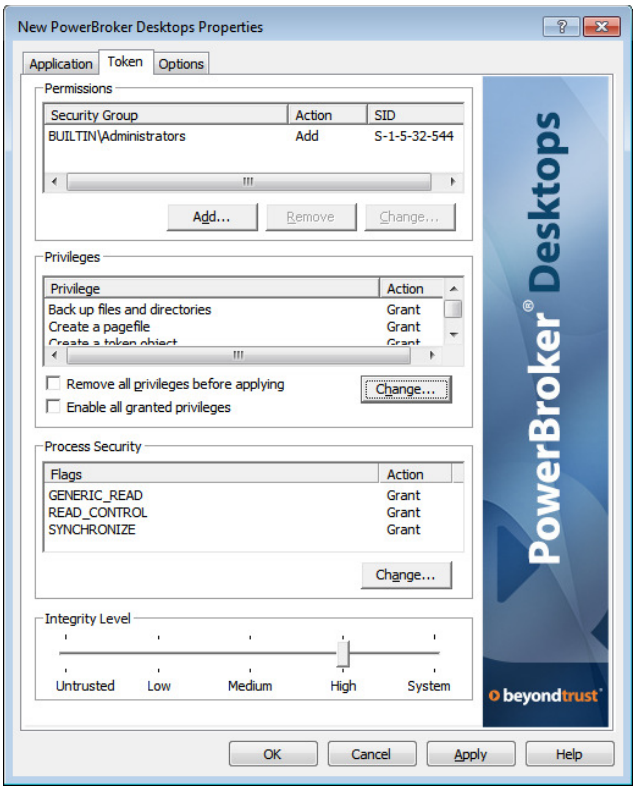
Remove Admin rights from application(s)
The application is run without local Administrator rights. Any changes to the permissions, privileges, and integrity level previously configured in the rule are removed and replaced with pre-configured rights. (This action is not available for ActiveX rules, Shell rules, or UAC rules.)

NOTE: This option supports dropping local administrative rights, not domain administrative rights.

Process Token Tab (#14885)

All changes to the process token have been consolidated to one tab.

NOTE: If an action other than Run application(s) with custom token is selected, then the permissions, privileges, process security, and integrity level are pre-configured and cannot be modified.

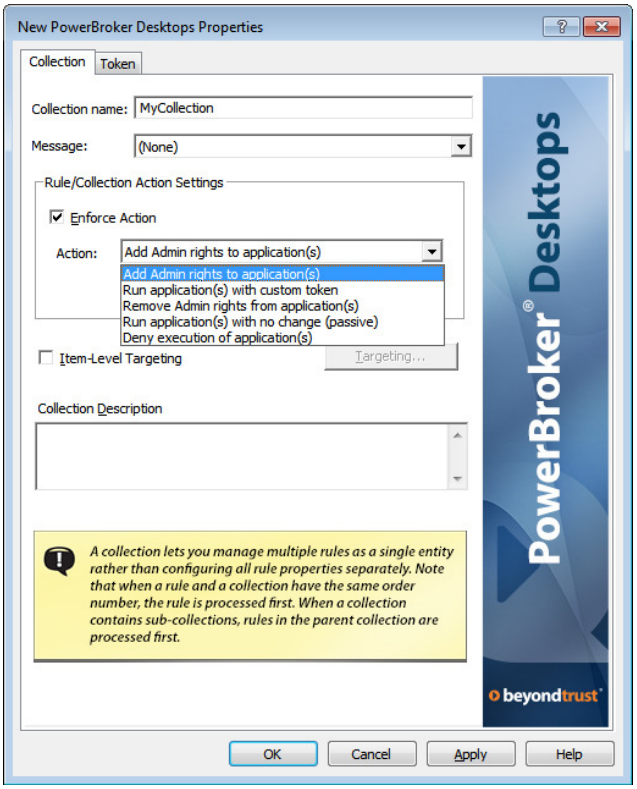


Configure Action on a Collection (#14885)

The Rule Action can now be configured at the collection level. To specify an action and token configuration to be used for all rules in the collection instead of individually configuring an action and token in each rule, select the Enforce Action check box and select an Action.

Selecting Enforce Action causes the action, permissions, privileges, process security, and integrity level configured for the collection to override any previously-configured settings for those options in rules within the collection.

NOTE: Messages set at the rule level will still override those set at the Collection level.



Shell Rule: Expanded List of Supported File Extensions (#13002)

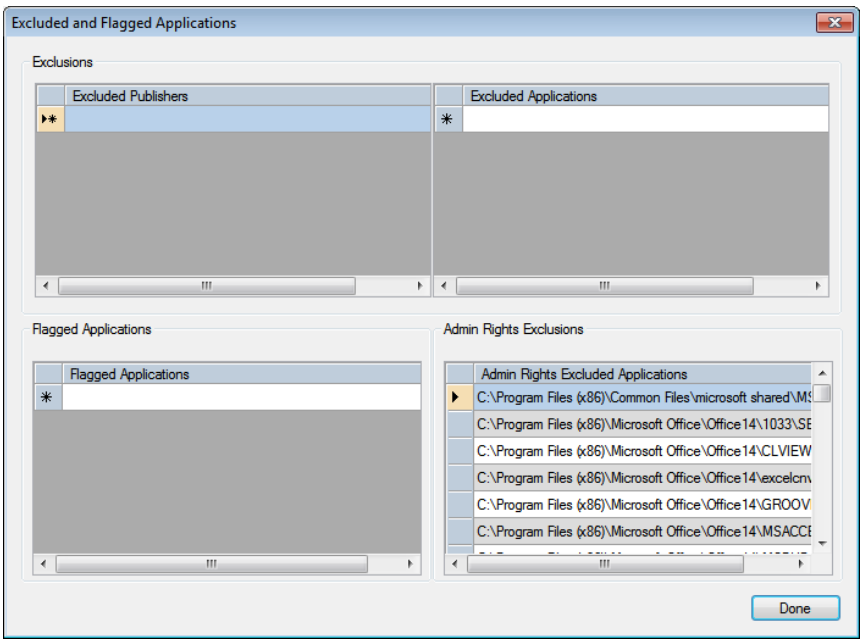
The following extensions are now supported for use with the Shell Rule:

LNK (Shortcut)
MSI (Windows Installer package)
MSP (Windows Installer patch)
MSC (Microsoft Common Console document)
CPL (Control Panel item)
CMD (Windows Command script file)
PS1 (Windows PowerShell script file)
VBS (VBScript script file)
WSF (Windows script file)
BAT (Windows batch file)

Reporting: Admin Rights Exclusion List (#15058)

A new Exclusion List has been added to PBReports to facilitate the building of rulesets based on the Application with Insufficient Privileges event (Event ID 28691). The list is pre-populated on upgrade of the database with applications that are commonly detected as requiring administrative privileges, but do not require them for common usage. This list can be modified as needed.

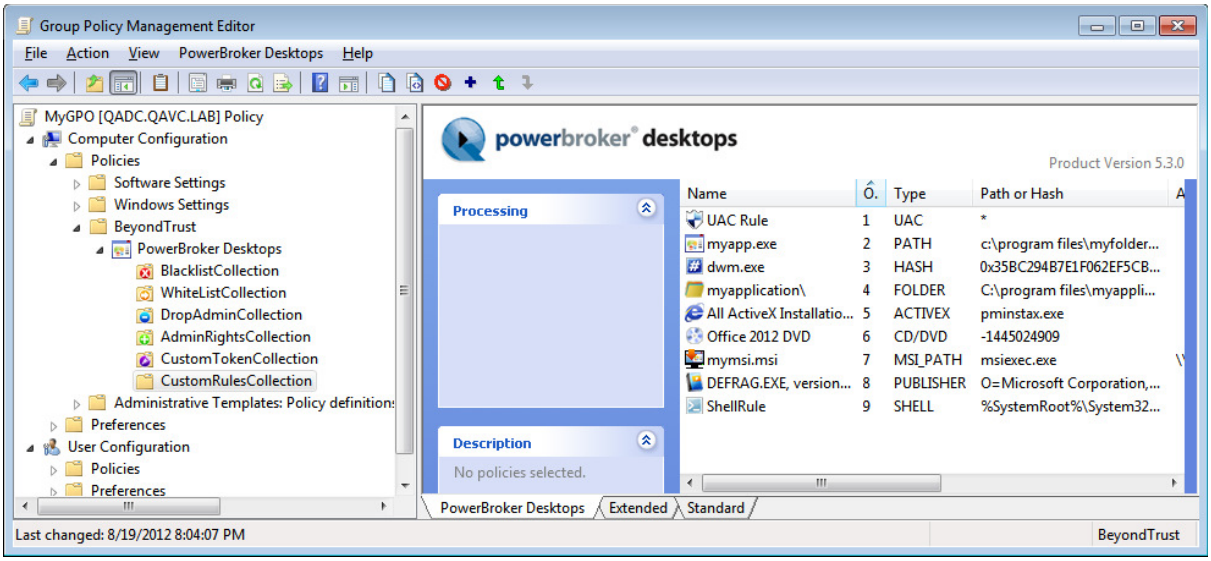
NOTE: Executables in this list will only hide 28691 events in the PBReports Console, and in the SSRS Dashboard Report. Any applications specified using wildcards will not be excluded from the Dashboard Report.



ENHANCEMENTS

User Interface Graphical Enhancements (#14885)

Graphical indicators in the user interface have been added and improved.



Path Rules That Target Internet Explorer: Improved Usability (#14883)

Navigating between non-elevated and elevated websites has been improved.

Reporting: Backup Parsing (#14912)

A backup parsing method has been added to pbreports to support instances when Microsoft Windows does not format forwarded events with RenderingInfo. This specifically occurs when forwarding events from non-English XP machines.

PBReports Logging (#14894)

Logging has been added to pbreports. To enable logging, set the following registry key:

KEY: HKLM\SOFTWARE\BeyondTrust\PBDesktops\PBReports\
VALUE NAME: LoggingDetail
TYPE: REG_SZ
VALUE DATA:
-1 - Logging Off
 0 - Log Tracing Info
 1 - Log Debug Info
 2 - Log Errors
 3 - Log Exceptions

FIXES

PBReports: Local Users (#15138)
Issues with reporting on local user accounts have been addressed.

Installation of Reporting Components (#15101)
The Reporting components now correctly detect when SQL Server Reporting Services is installed.

"Apply Rule Only" now works correctly (#15046)
"Apply Rule Only" now applies the rule the correct number of times.

Citrix Services (#15015)
A compatibility issue with Citrix services has been resolved.

NOTE: Due to a remaining issue on the Citrix side, an exclusion list may still be necessary.

PBReports Data Import (#15014)
An issue importing certain characters in pbreports has been resolved.

Item-level targeting in subdomains (#14900)
An issue has been resolved with item-level targeting in subdomains.

Installation: Detection of .NET Frameworks (#14878)
A snapin installation issue with the detection of the .NET Frameworks has been resolved.

NOTE: Currently both the .NET 3.5 and 4.0 Frameworks are required for the snapin.

Shell Rule combinations (#15162)
A Shell Rule will now allow any other rules in place to be applied to the application.

Publisher Rule: Version Number (#15150)
An issue has been resolved with version number matching on a publisher rule.

PowerBroker® Desktops Windows® Edition 5.2.2 - Released 4 May 2012

FIXES

Auditing and Reporting (PBReports) internationalization (#14893)

Auditing and Reporting (PBReports) now imports data correctly regardless of the operating system language used on the event collector and client computers.

NOTE: The computer serving as the event collector must have the English (US) language pack installed and the subscription locale set to en-US. For more information, see the *PBWD Installation Guide*.

PBReports single quotes (#14889)

Data is now parsed correctly for all fields when a single quote is present.

PowerBroker® Desktops Windows® Edition 5.2.1 - Released 3 April 2012

ENHANCEMENTS

Read Only Domain Controller (#14859)

PowerBroker Desktops is now compatible with 2008 R2 Read Only Domain Controllers (RODCs).

FIXES

Item Level Targeting (#14874)

Computer Security Group Item Level Targeting now works correctly with the "NOT" filter.

Error in Event Log (#14861)

An intermittent error in the event log involving MS Visual C++ and GPScript.exe was resolved.

Symantec Tamper Protection Alert (#14849)

An issue was resolved involving Symantec Tamper Protection Alerts.

NOTE: There are still reported issues with Symantec Tamper Protection that are not related to PowerBroker Desktops.

Symantec Endpoint Protection 12.1 (#14801, #14871)

Issues were resolved with Symantec Endpoint Protection 12.1.

PowerBroker® Desktops Windows® Edition 5.2 - Released 1 February 2012

IMPORTANT

Upgrading Reporting Components

Prior to upgrading the pbreports database, see the PBWD Upgrade Guide for specific instructions on retaining existing data.

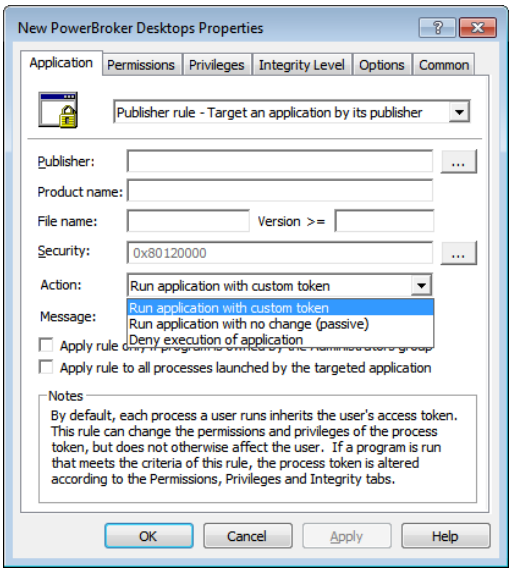
Reporting Installer

In some instances, the SQL database may not show up in the Reporting Installer browser. Manually enter the server and instance name in order to install the database, or type "." for a local default instance.

NEW FEATURES

Application Control (#14755)

A new Action control in the Snap-In adds the ability to control the execution of applications via passive (whitelist) or deny (blacklist) actions.



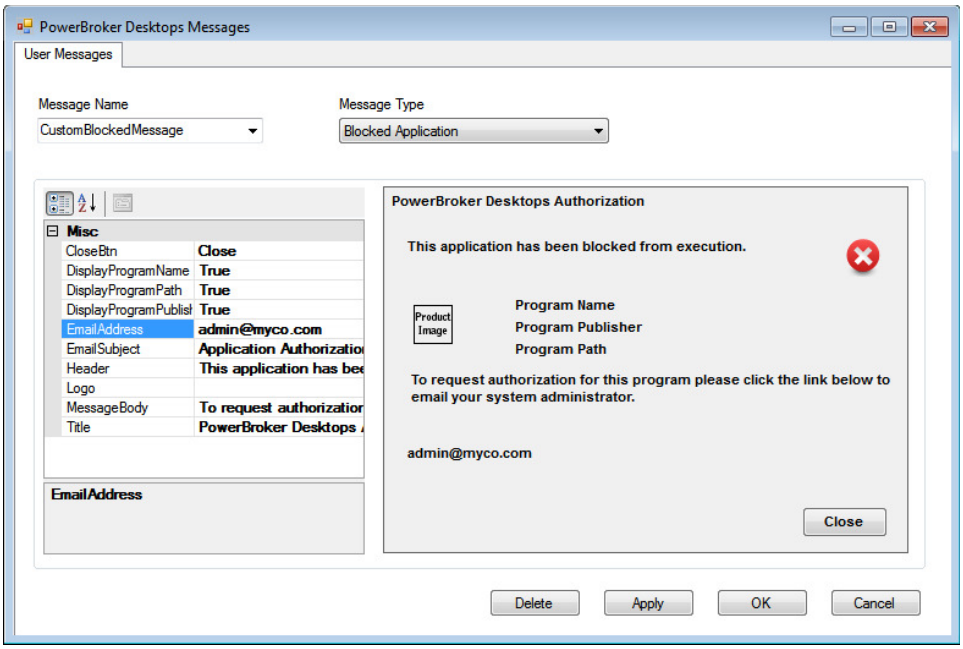
The following options are available:

Run application with custom token
Default. Rules upgraded from prior versions will be automatically set to this option. The token of the targeted application will be adjusted as specified by the rule.

Run application with no change (passive)
Application will be allowed to run, but no change will be made to the process token. To be used in conjunction with Deny rule(s).

Deny execution of application
Block application from executing. Application will exit immediately after any associated message boxes have been closed.

These options may be used with or without an associated message box. A new "Blocked Application" message type is available to associate with blocked applications:



Passive/Denied Application Launch Events (#14806)

The ADMX/ADM templates have two new options:

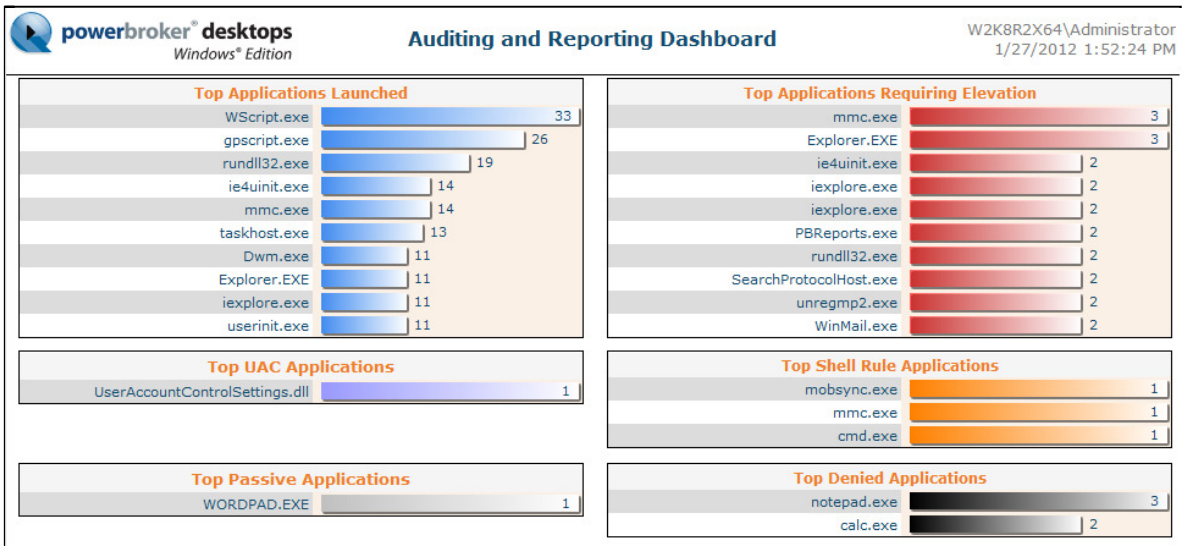
Log application launch with Action: Deny Execution
Logs an event to the System Event Log with ID 28698 each time an application is blocked by a Deny rule.

Log application launch with Action: No Change (passive)
Logs an event to the System Event Log with ID 28699 each time an application is allowed to run by a Passive rule.

If event forwarding is configured and new Application Control (Passive/Deny) rules are created, the Subscription on the Event Collector will need to be updated to include the two new event IDs.

Application Control Reports (#14812)

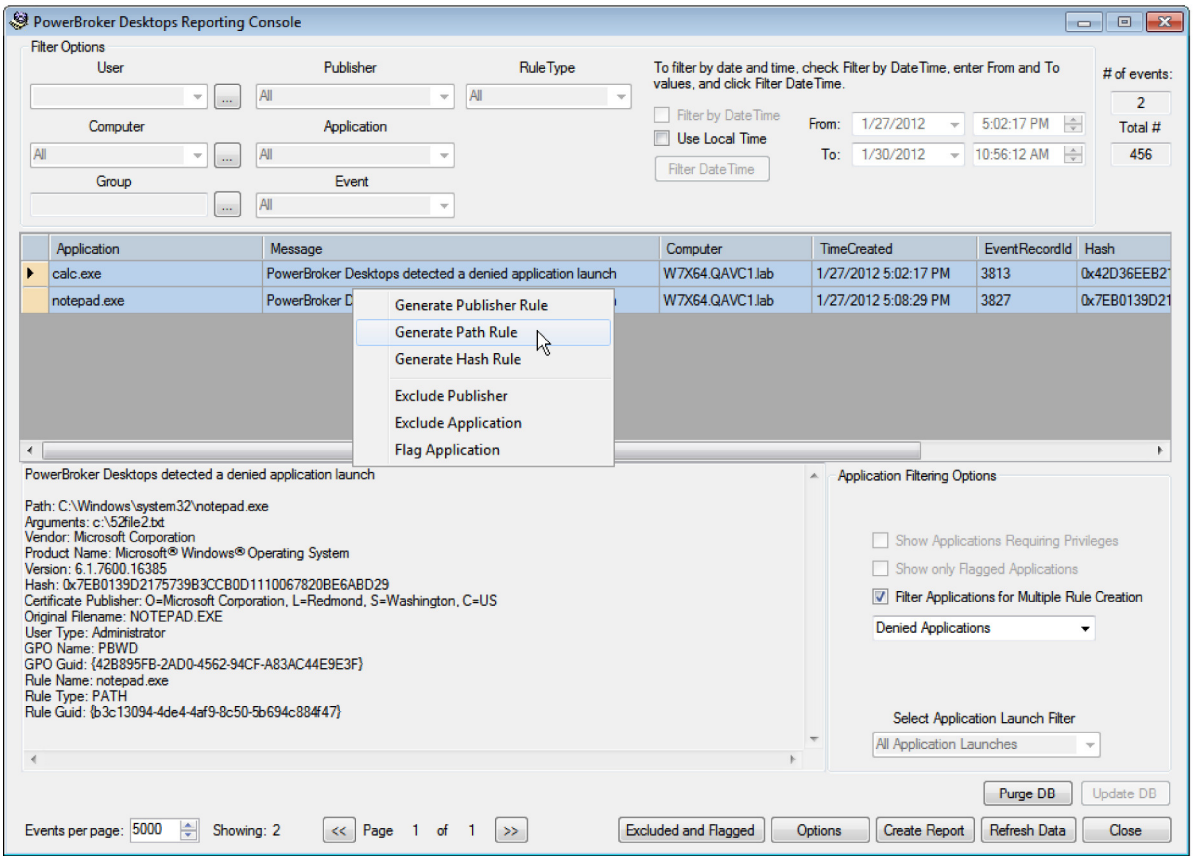
The SSRS Reports now include information on passive and denied applications. In addition, there are two new reports in the Dashboard that show the most frequent passive and denied application executions.



PBReports: Passive Rule Generation (#14823)

Denied or Passive rule applied events may be viewed and filtered in the Reporting Console. A passive rule may be generated from a Denied Rule Applied event via a right-click option. In addition, multiple Passive rules may be generated from Denied events by checking "Filter Applications for multiple rule creation" and selecting "Denied Applications".

NOTE: This functionality may be particularly useful when there is a default deny rule in place.



Reporting Installer (#14803)

An installer (pbwdreporting.msi) is now available for the database and SQL Server Reporting Services reports.

IMPORTANT: To preserve data in an existing pbreports database, do not install the database component. If the database component is selected, any existing pbreports database will be backed up and overwritten when the installer is run.

ENHANCEMENTS

Log application launch with Action: Custom Token (#14818)

The ADM/ADMX template description for "Log application launch with rule applied" option has been changed to "Log application launch with Action: Custom Token" to reflect the new functionality. No changes have been made to the registry key associated with this option.

State Model Data (#14771)

State Model data is no longer stored in the registry when "Log Application State Data" is set to Disabled or Not Configured.

PBDeploy: User Messages (#14711)

A processing issue was resolved with user messages and pbdeploy.

UAC Prompt Detected (#14660)

Longer amounts of text may now be displayed in the UAC Prompt Detected dialog.

PBDeploy: Signing of User Messages (#14649)

Custom user messages are now signed for use with pbdeploy.

FIXES

PBReports Data (#14794)
PBReports now imports events correctly when there is a single quote in the application name.

Wizard: User Messages (#14748)
Configured user messages are now available for selection when you create a new rule on a collection using the wizard.

Reporting Services (#14688)
A message is now displayed in the Snap-In when Reporting Services is not configured.

Authentication with space in username (#14558)
The authentication option on a rule now works when the user name contains a space.

Rule Type in Event Logs (#13378)
The Rule Type is now logged correctly for child processes.

PowerBroker® Desktops Windows® Edition 5.1.2 - Released 29 December 2011

ENHANCEMENTS

PBReports Windows Authentication (#14789)
PBReports now supports connecting to the SQL database using Windows Authentication.

PBReports SQL Login (#14642)
The PBReports SQL login is now configurable.

FIXES

PBReports: Error handling (#14705)
Error handling was improved when an incorrect connection string was specified.

PBReports Regional Settings (#14761)
An issue was resolved that occurred when the regional settings were changed on the collector.

NOTE: In some scenarios the client will need to be installed on the collector in order for the events to appear properly.

Wizard: Apply to subfolders (#14757)
Enabling apply to subfolders on rules created by the rule wizard now works correctly.

Profiling and SQL Express Install (#14754)
A SQL Express installation will no longer fail when profiling is enabled.

Forwarded Event Log Text (#14745)
Formatting issues were resolved when regional settings on the client were set to other than US.

Issue with rule matching (#14744)
An issue was resolved that prevented some applications from matching on a rule. This specifically occurred with Apple Software Update.

NTR Connect (#14742)
An issue was resolved involving NTR remote support software.

PowerBroker® Desktops Windows® Edition 5.1.1 - Released 2 December 2011

FIXES

Rule Wizard (#14743)
The Rule Wizard now launches correctly when the Snap-In is installed to a non-default location.

Symantec PGP Desktop (#14735)
A compatibility issue with Symantec PGP Desktop was resolved.

PowerBroker® Desktops Windows® Edition 5.1 - Released 30 September 2011

INFORMATION

PBDeploy (#14710)

PBDeploy does not support User Messages in the current release.

User Messages (#14702)

User Messages will not propagate to the client until at least one rule has been created in the GPO.

Upgrading: UAC Prompt Detected, IE Elevation, IE Failure Messages (#14701)

After upgrading the PBWD clients to 5.1, the UAC Prompt Detected and Internet Explorer Failure messages will no longer appear. The IE Elevation messages will revert back to the default text. These messages will need to be reconfigured in the User Messages dialog.

Upgrading: On Demand Right-Click Menu (#14707)

Customized Shell Rule right-click context menu items will be displayed as the default text after upgrade ("Run Elevated" and "Install Elevated"). These options will need to be reconfigured in the User Messages dialog.

.NET Framework 4.0 (#14519)

The Snap-In installer now requires the .NET Framework 4.0.

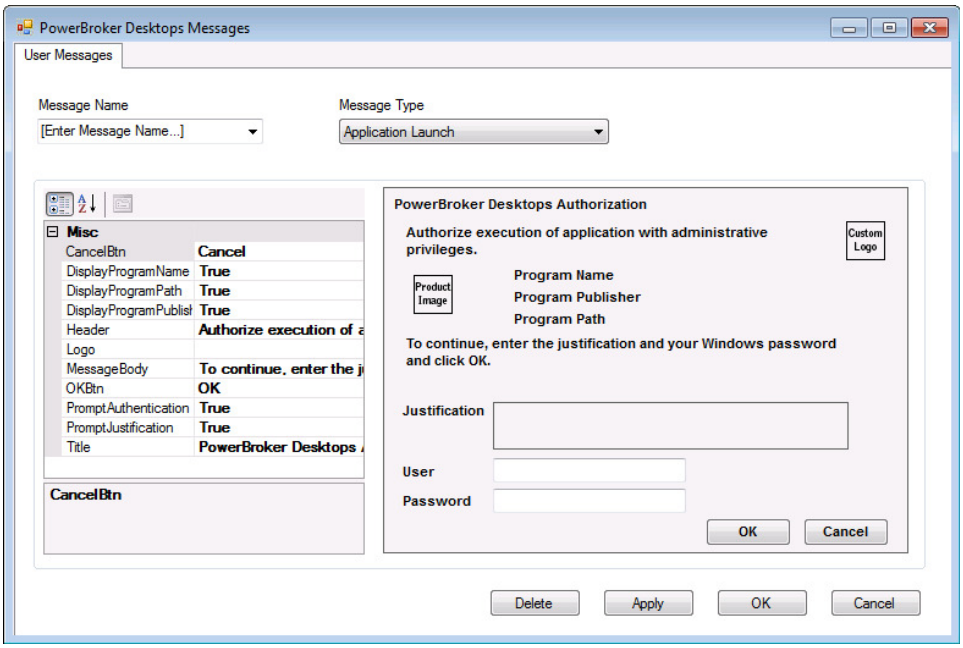
64-bit Internet Explorer (#13204)

Internet Explorer elevation is not supported for the 64-bit version of Internet Explorer.

NEW FEATURES

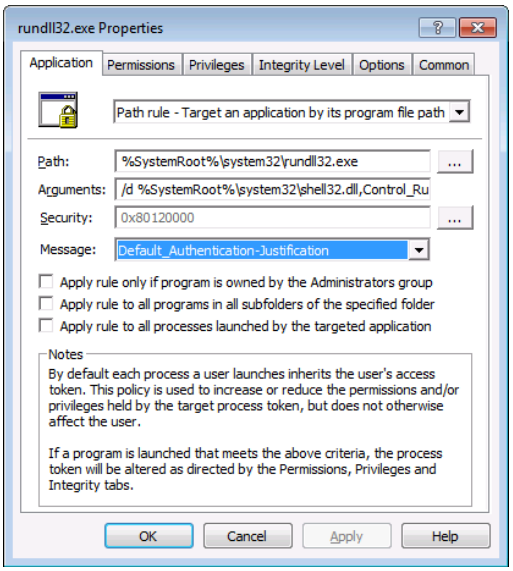
User Messages (#14513)

Authentication\Justification User Messages, UAC Prompt Detected User Messages, Internet Explorer Elevation, Internet Explorer Failure, and the On Demand Elevation right-click menu can be configured in the new User Messages dialog.



The Authentication\Justification messages can then be linked at either the rule or collection level. The UAC Prompt Detected Message and the On Demand Elevation context menu options are global to the GPO and are active once configured.

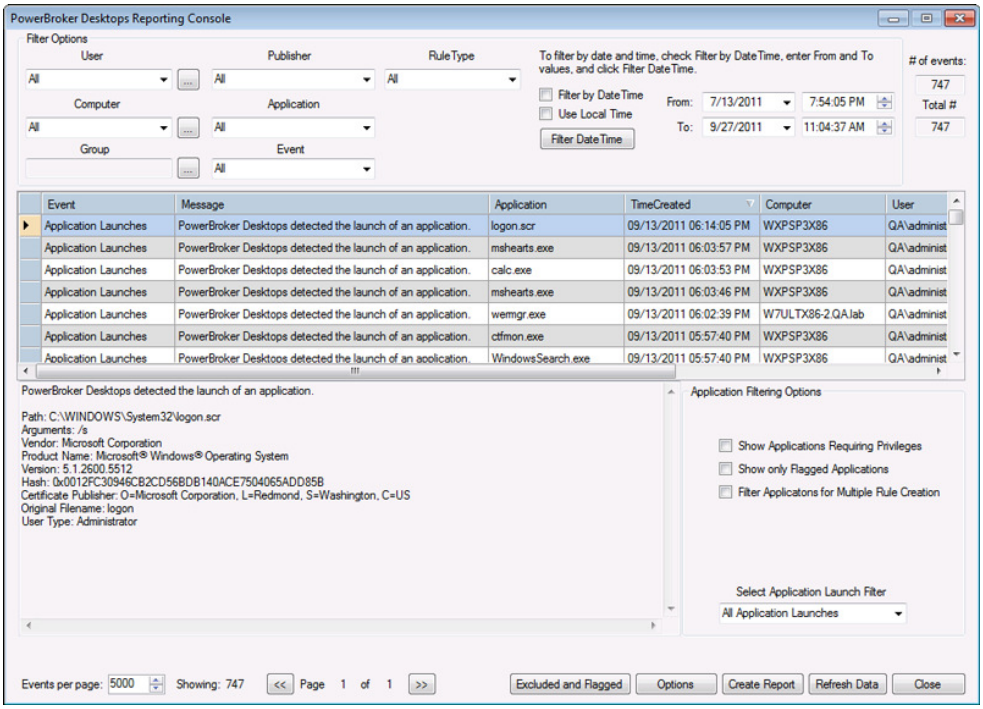
On upgrade from prior versions, any rules with authentication and\or justification checked will automatically be linked to the appropriate default message box. The link to the Authentication\Justification message box replaces the checkboxes present in prior versions.



Reporting Console (#14478)

The Reporting Console is now installed with the Snap-In. When configured with event forwarding and a PBWD database (separate download), the reporting console can be used to build rule sets for applications that require elevation.

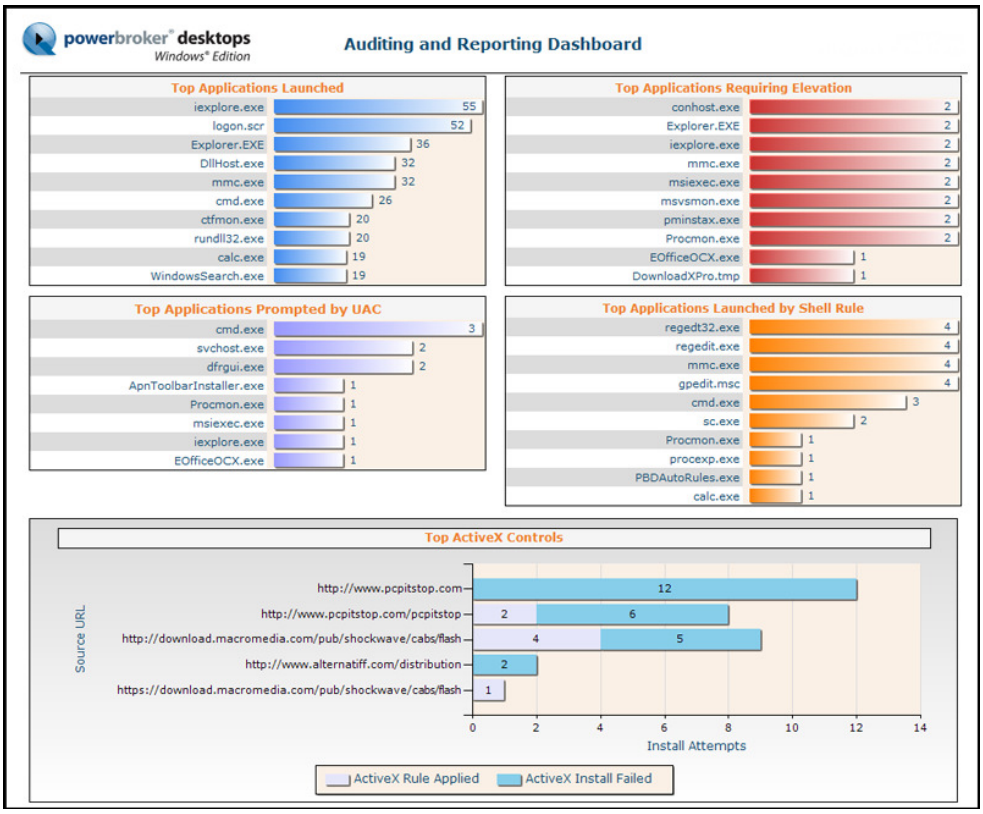
IMPORTANT: A PBWD SQL database, as well as SSRS reports, must be downloaded, manually installed, and configured in order to use this functionality.



SSRS Reports (#14486)

There are now SSRS reports that display information on application execution and rules applied.

IMPORTANT: A PBWD SQL database, as well as SSRS reports, must be downloaded, manually installed, and configured in order to use this functionality.



ENHANCEMENTS

Rule Type in Application Event Log (#14570)
The Rule Type is now displayed correctly in the application event log on child processes.

UAC and COM (#14537)
The UAC Rule now elevates COM objects. In addition, COM objects may now be profiled.

UAC Rule and MSIs (#14535)
MSIs can now be elevated via a UAC Rule.

PBDeploy and Collections (#14078)
PBDeploy now supports collections.

Collection name in HTML report (#14077)
The HTML report now displays the collection name.

User Account Control Info dialog (#14063)
The UAC Information Dialog now has a task bar icon.

State Model Class names (#13866)
The state model data class names now have PB prepended to their names.

Disabling multiple collections (#13724)
Multiple collections may now be disabled with one click.

FIXES

CPALaunch printers (#14654)
An issue was resolved with cpalaunch and printers.

Wildcards and Publisher Rules (#14579)
The Publisher Rule will now match when a wildcard is used in the file name field and the application does not have an original file name.

Wildcards (#14547)
An issue with wildcards at the beginning of a path rule was resolved.

File version (#14525)
The File version is now used to create rules instead of the Product Version.

ADM\ADMX: ActiveX Ignore key (#14524)
The ActiveX Ignore key now works for multiple ActiveX CLSIDs.

BTService (#14517)
An intermittent issue was resolved with BTService.

Automatic Rule Generator (#14514)
The Automatic Rule Generator now continues if connecting to one machine in a list fails.

Privileges on UAC, Shell, and CDROM rules (#13820)
When the Privileges tab is selected, all privileges are now automatically granted on UAC, Shell, and CD-ROM rules.
NOTE: Privileges on these rules can still be customized as needed.

Organization Unit Filter (#13754)
An Organization Unit filter can no longer be saved without an OU name being entered.

Collections display issue (#13690)
A minor refresh issue was resolved in the tree view with collections.

Justification text length (#13133)
The justification text length allowed in the UI now matches the length in the application event log.

PowerBroker® for Desktops Windows® Edition 5.0.1 - Released 17 June 2011

FIXES

Issue with Profiling (#14526)

Under certain conditions, an issue with profiling caused some applications to hang on launch.

PowerBroker® for Desktops Windows® Edition 5.0 - Released 18 April 2011

INFORMATION

Upgrading from prior versions (#13931)

IMPORTANT: Prior to upgrading from previous versions, review the Upgrade Guide for important instructions. In addition to obtaining a new license, other special procedures are required to preserve rules and settings during an upgrade.

Internet Explorer 9 (#13909)

Internet Explorer 9 is now supported for both ActiveX and IE Elevation rules.

.NET Framework 3.5 (#13836)

The Snap-in installer now requires the .NET Framework 3.5.

Excel 2010 (#13818)

When elevating Excel 2010, due to DDE, Integrity Level should be set to Medium. If Sharepoint is being used, PROCESS_SET_QUOTA must be enabled in Process Security.

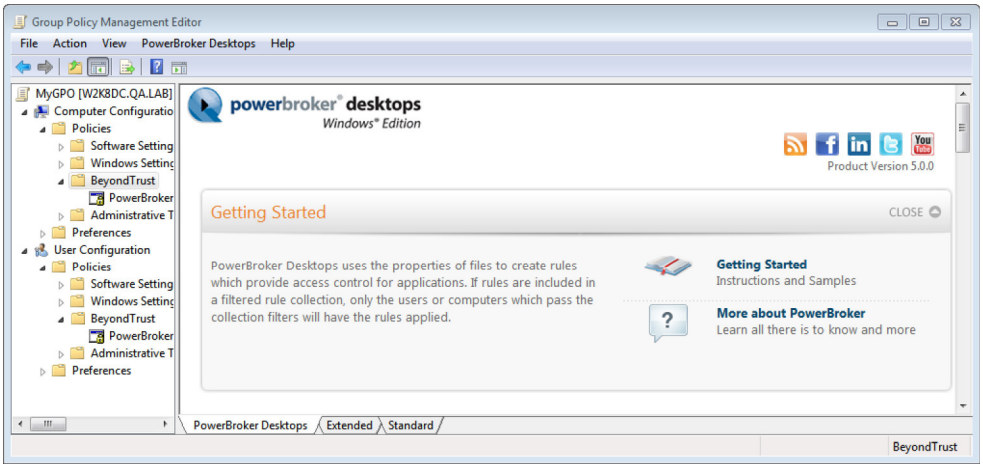
Drag and Drop (#13101)

Dragging and dropping the rules to or from the snap-in fails with UAC enabled. Right-click copy/paste is successful.

NEW FEATURES

Management Dashboard (#13972)

Select the BeyondTrust node to view the new Management Dashboard. The Management Dashboard provides links to a variety of information resources, tools, and reports to assist in creating, managing, and maintaining rule-based security.



The dashboard consists of three sections:

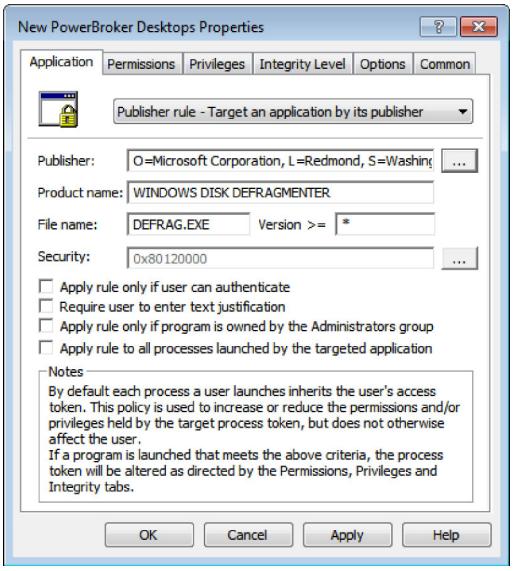
Getting Started:
Provides links to documentation and sample files.

Tools and Wizard:
Provides quick access to rule creation wizard, automatic rule generation wizard, and links to manage your rules.

Rule Summary:
Displays high-level information on rules as well as links to reports.

Publisher Rule (#13772)

The Publisher Rule has replaced the Certificate rule in 5.0. Certificate Rules are converted to Publisher rules when they are edited in the 5.0 snap-in.



Publisher Rules enable targeting elevation based on one or more of the following criteria:

Publisher
Company name in the signing certificate.

Product Name
Name of the software product

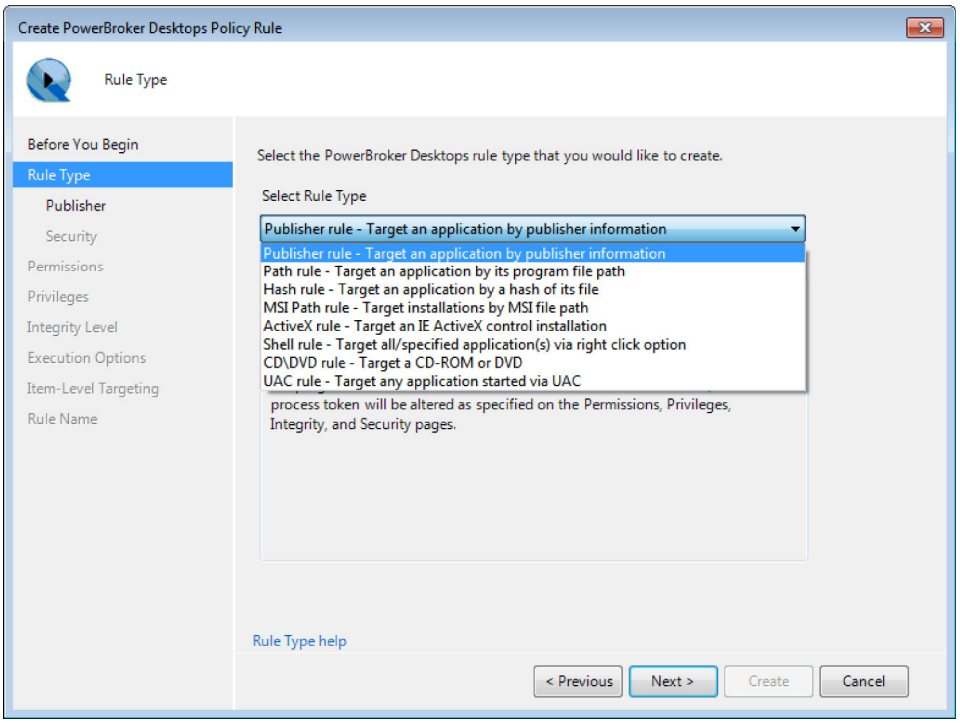
File Name
Full file name. EXE, MSI, and MSP formats are supported.

File Version
Targeting allows for minimum, maximum, or exact file version.

NOTE: Partial wild card matches are not supported in these fields.

Rule Wizard (#13568)

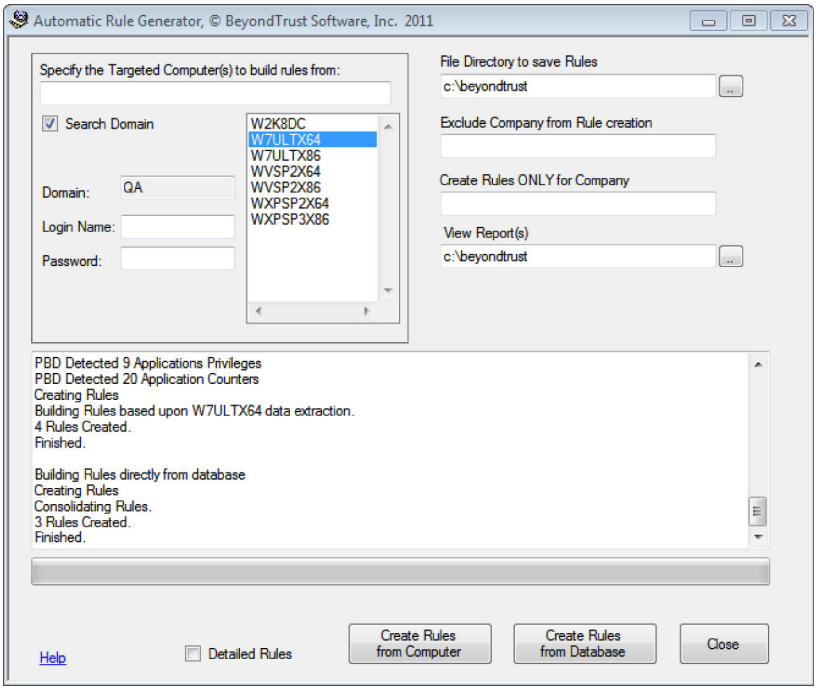
The Rule Wizard guides the user through all steps required to create a rule. Launch the Rule Wizard via the "Create New Rule" option in the snap-in, or the link in the Management Dashboard. All rule types may be created in the Wizard. Folder\MSI Folder rules have been incorporated into Path\MSI Path rules. To create a Folder\MSI Folder rule, use the folder browser in the appropriate Path rule.



NOTE: The Rule Wizard is enabled by default on a new 5.0 snap-in installation. To use the Properties Sheets to create new rules, select "Disable Wizard" on the first page of the wizard and then click Cancel, or select the "Disable Wizard" button in the Dashboard.

Automatic Rule Generation (#13663)

The Automatic Rule Generator, in conjunction with State Model Logging, enables the rapid creation of rules based on applications that have been run on targeted machine(s).



To automatically generate rules for applications that require administrative privileges, enable the following settings in the Administrative Template:

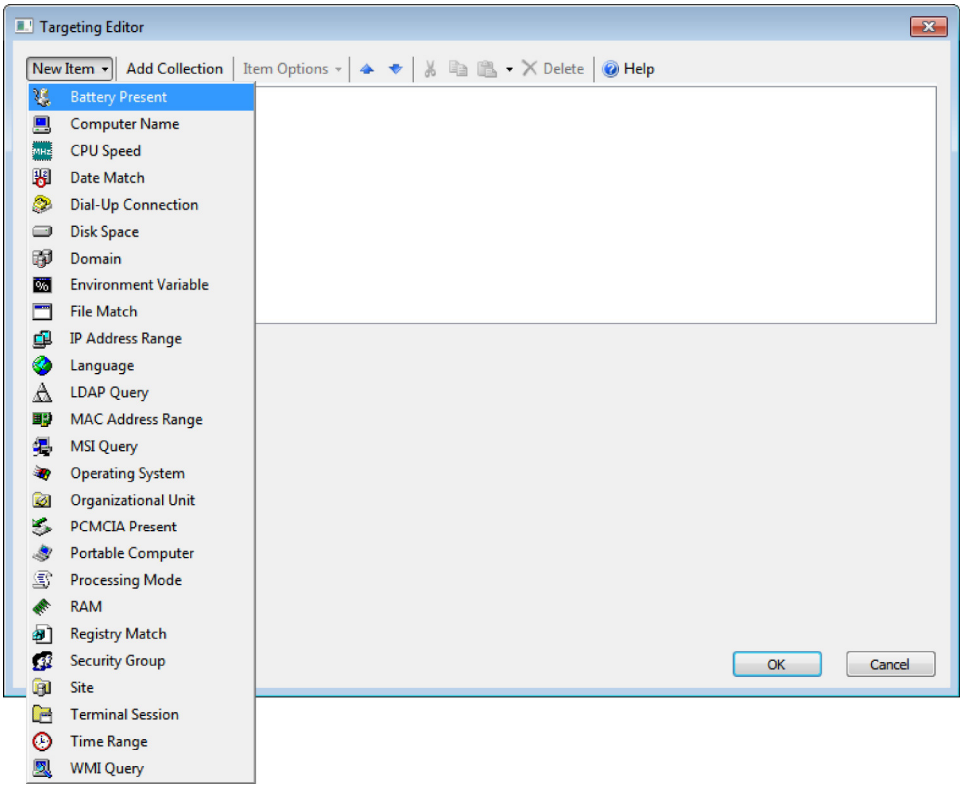
State Model Logging
Log Application Launch requiring elevated privileges

Generate data on the client machine by launching the targeted applications. In the Automatic Rule Generator select the machine(s) and click "Create Rules from Computer". The rules will be saved to the specified directory, and can then be imported into the snap-in via copy/paste.

NOTE: All automatically generated rules should be verified before deployment.

Item Level Targeting (#13503)

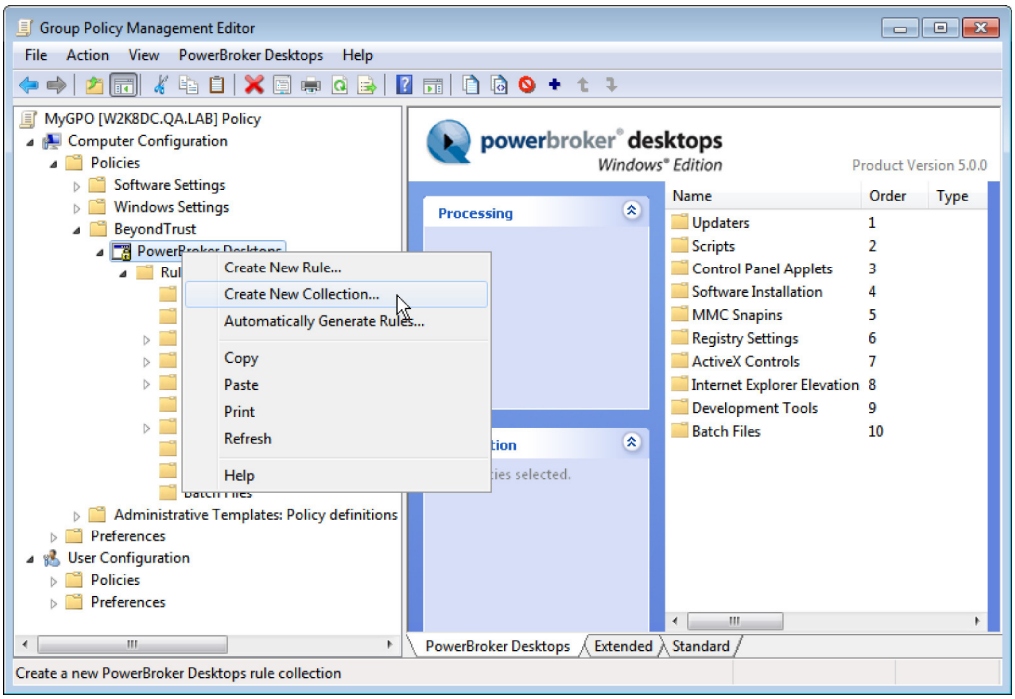
The Filters screen has been replaced with Item-Level Targeting.



NOTE: Existing Filters are compatible with the new Item Level Targeting screen. The Message Box filter has been removed.

Collections (#13106)

Collections enable the grouping of rules in a folder structure. Item Level Targeting can be specified on a collection. This is especially useful if multiple rules require the same filter, as the filter will only need to be configured once for all rules in the collection.



NOTE: Standard Group Policy precedence also applies to collections. Rules not in collections are processed first, followed by rules which are contained in a collection.

IMPORTANT: Collections are not currently supported for use with pbdeploy or the free version (unlicensed domain policy).

State Model Logging (#13352)

The data logged in the state model has been expanded to include logging on UAC success\failure, Shell and other rule launches, application launch times, and justification text, in addition to applications requiring administrative privileges. The data logged is controlled via the Logging settings in the Administative Templates.

CPALaunch Updates (#13868)

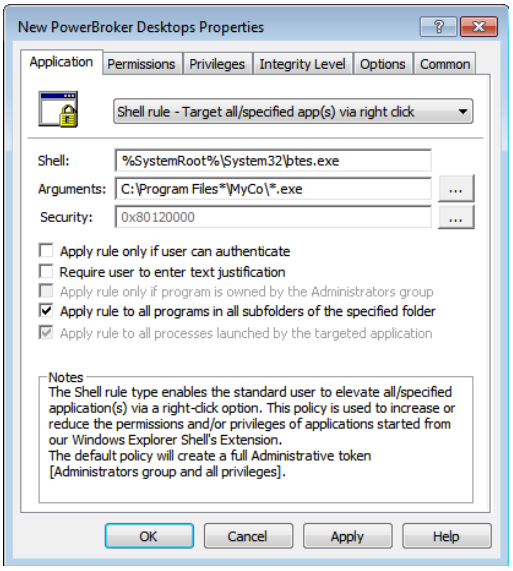
CPALaunch has a new option to enable a standard user to install Windows Updates on Windows 7.

To enable a standard user to perform these operations, create a rule with the following parameters:

Path: c:\windows\system32\cpalaunch.exe
Arguments: updates

Shell Rule (#13507)

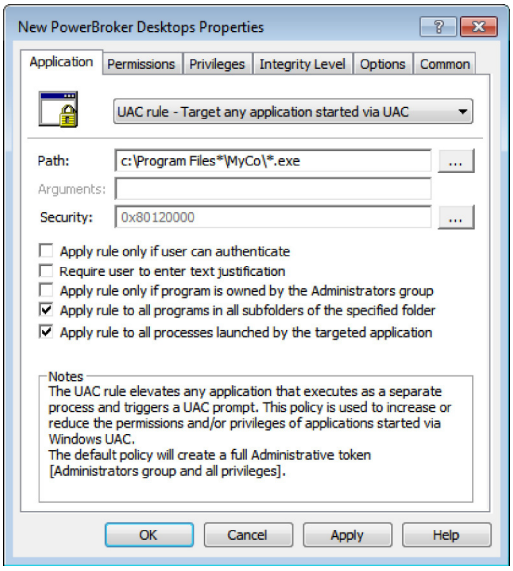
The Shell Rule may now be applied to individual applications or folders. This enables allowing only certain applications to be elevated via a right-click option.



NOTE: Wild cards are supported.

UAC Rule (#13508)

The UAC Rule may now be applied to individual applications or folders. This enables only specified applications or folders to be elevated, eliminating the UAC prompt.



NOTE: Wild cards are supported. The application must be launched as a separate process in order for the UAC Rule to apply.

ENHANCEMENTS

Exclusion Lists (#13960)

Exclusion Lists may now be configured in the administrative template.

NOTE: The registry keys are written as REG_EXPAND_SZ.

Wild Cards and Exclusion Lists (#13471)

With the exception of KeepBtpLoadLoadedforApps, all exclusion lists now support wild cards.

Wild Cards (#13197)

In addition to path rules, wild cards are now supported in Folder, MSI Path, MSI Folder, Shell, and UAC rules.

Wild card behavior has changed in 5.0. If a wild card is used in place of a folder name, it will only match if one folder matches the wild card path.

> **Example Rule:** c:\rootfolder*\childfolder*.exe
>
> c:\rootfolder\folder1\childfolder\myexe.exe: Will match
> c:\rootfolder\folder1\folder2\childfolder\myexe.exe: Will not match

IMPORTANT: Any rules that contain wild cards should be verified prior to deployment.

Default Rule Name (#13891)

When a path rule ends in a wild card, the default rule name now includes the parent folder name

Lock Pages in Memory (#13413)

The Lock Pages in Memory privilege has been added to the available list of Privileges.

NOTE: Enabling this privilege may introduce performance issues and processing delays.

Performance Improvement (#13637)

The performance of Hash and Publisher (Certificate) rules has been improved.

System Variable Name Change (#13922)

The PrivilegeManagerVersion system variable has been updated to PBDesktopsVersion. Any rule using this variable will need to be manually updated to the new variable name.

Administrative Template Change (#13245)

The names of the administrative templates have been changed from beyondtrust.adm(x) to beyondtrust.pbwd.adm(x).

Name Change (#13931)

Names of folders\files have been changed from Privilege Manager to PowerBroker Desktops.

FIXES

UAC Information Dialog (#13563)
Clicking the link on the UAC information dialog now correctly loads the current user's Outlook profile.

Internet Explorer Elevation (#13500)
When creating a rule to elevate Internet Explorer, the path must now include "\Internet Explorer\iexplore.exe".

FiberLink (#13725)
Fiberlink now installs correctly when the user is a member of Network Configuration Operators or Backup Operators.

Command Line Apps (#13581)
Output from command line applications is now displayed correctly when a PowerBroker Desktops rule is applied.

Profiler Exclusion List\Child Processes (#13910)
If a parent process is added to the Profiler Exclusion List, as long as the parent\child relationship is maintained, the child will also be excluded.

NOTE: If a rule is applied, the child process will not be excluded.

PBDeploy and VPN connection (#13683)
PBDeploy now works when connected via a VPN connection.

PowerBroker® for Desktops Windows® Edition 4.9.4 - Released 7 February 2011

NEW FEATURES

CPALaunch (#13761)

A utility has been added that enables a standard user to remove programs, change network card settings, and add local printers. CPALaunch.exe is installed by the client to %systemroot% \system32.

To enable a standard user to perform these operations, create rule(s) with the following parameters:

Path
c:\windows\system32\cpalaunch.exe

Arguments
Change network settings: networks
Add local printers: printers
Remove programs: programs

"Apply rule to all processes launched by the targeted application" must be enabled. A shortcut with the appropriate mandatory arguments may be created and deployed to desktops.

NOTE: If a rule for cpalaunch is added, any existing template rules for "Alter TCP/IP Settings - Windows 7" should be removed or disabled.

Before using this utility, see the CPALaunch Technical Note posted on the Documentation section of the BeyondTrust web site for more information.

FIXES

Launching Visual Studio (#13642)

An issue was resolved launching Visual Studio when profiling was enabled.

Network Drive Mapped as System - IBM Clearcase (#13583)

Polmon will no longer show a lost connection to the privman service when a network drive is mapped from a Local System account. This previously occurred under an IBM ClearCase installation.

Issue with Google Chrome on 64-bit OS (#13519)

Chrome will now load web pages correctly on a 64-bit operating system.

NOTE: A rule cannot be applied to Chrome.

Multiple Paths in Exclusion Lists (#13501)

The BTSuppressHook and ExcludedProfilerApps registry keys now work correctly with multiple paths.

PowerBroker® for Desktops Windows® Edition 4.9.1 - Released 6 October 2010

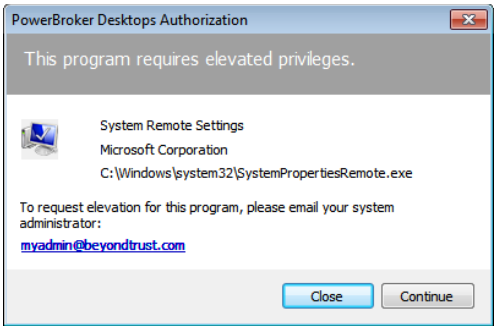
NEW FEATURES

Logging of UAC Prompts (#13317)

There is now an option in the ADM/ADMX template to log all User Account Control (UAC) prompts to the system event log. PowerBroker Desktops also logs whether or not the UAC prompt passed validation. If the UAC prompt passed validation, the account used for elevation is logged.

UAC Information Dialog (#13394)

There is now an option in the ADM/ADMX template to display a customizable dialog when a UAC prompt is detected. This dialog enables the user to email the system administrator with an elevation request.



The information displayed to the end user can be changed via the UAC Information Dialog Customization setting in the ADM/ADMX template. In addition to the text in the dialog, the email address and default subject and body of the email may be customized. A custom logo may be displayed by copying an image with the following specifications to the client machines:

Image Sizes: 32x32, 40x40 or 48x48 pixels
Default Image Name and Location: C:\Windows\BeyondTrust\messagelogo.bmp

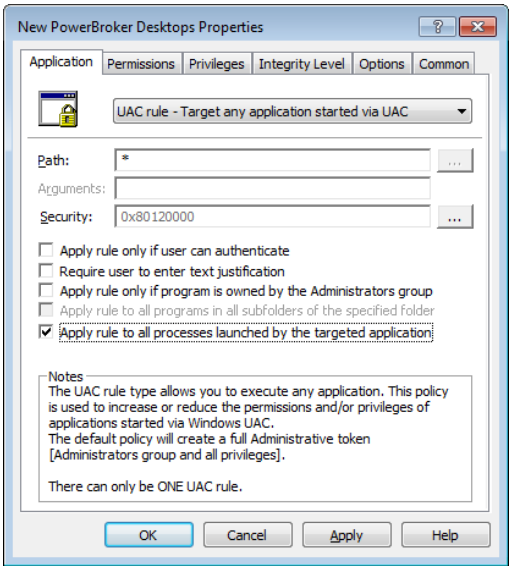
NOTE: The image must be copied to the client machine in order for it to be displayed. The image path and name are customizable via the ADM/ADMX template setting.

The user has the option to Close the dialog after emailing the administrator, or to click Continue to proceed to the Windows UAC prompt.

IMPORTANT: This dialog will only detect UAC prompts launched via a separate process.

UAC Rule (#13259)

There is now an option to create a rule that will elevate executables detected by User Account Control (UAC).



NOTE: MSIs will not be elevated via a UAC rule. A separate process must be launched in order for the UAC rule to apply.

Rule Set Auto-Backups (#13426)

The snap-in now automatically backs up the rule set when a modification to a rule is made. The rule backups are saved to the Application Data directory. The directory path is different depending on the OS. Up to 3 backups per GPO will be created, which may be used to track and\or reverse local changes to the rules.

On 2003 server and XP:
C:\Documents and Settings\All Users\Application Data\BeyondTrust\PowerBroker Desktops\GPOBackupData

On Windows 2008/7/Vista:
C:\ProgramData\BeyondTrust\PowerBroker Desktops\GPOBackupData

Filename format:
AppSecComp_GPOName.xml
AppSecUser_GPOName.xml

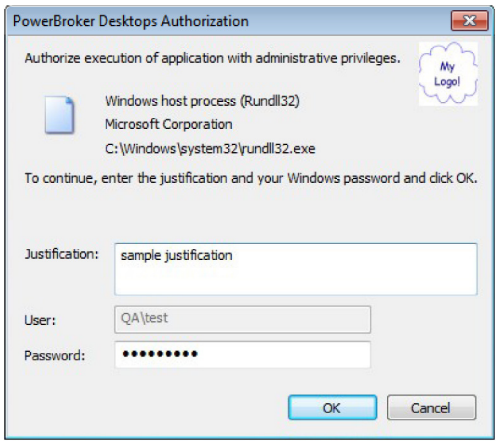
These rule backups may be used to deploy rules to users or computers that are not currently connected to the domain. For more information, see the PBDeploy Guide.

Customized Authentication/Justification Dialog (#12048)

The text in the Authentication/Justification dialog may now be customized via an ADM/ADMX template setting. A custom logo may be displayed by deploying an image with the following specifications to the client machines:

Image Sizes: 32x32, 40x40 or 48x48 pixels
Default Image Name and Location: C:\Windows\BeyondTrust\messagelogo.bmp

NOTE: The image must be copied to the client machine in order for it to be displayed. The image path and name are customizable via an ADM/ADMX template setting.



ENHANCEMENTS

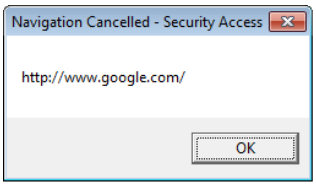
Increased Visibility of Elevated Internet Explorer (#13473)

Changes have been made to improve the visibility of an elevated instance of Internet Explorer. When an instance of Internet Explorer has been elevated via a rule, the title bar now displays "BT: [Page Title]" and the status bar displays:
" ** BeyondTrust PowerBroker Desktops Rule Applied - Internet Explorer Elevated ** ".

This text, as well as the title of the cancellation dialog message, is customizable via a new ADM/ADMX template setting.

Navigation Cancelled Dialog (#13502)

When a user navigates from an elevated Internet Explorer page to a non-elevated page, the URL now appears in the body of the message box instead of the title:



Excluding an Application from a Rule (#13457)

It is now possible to exempt applications from having PowerBroker Desktops rules applied. For example: An application which has compatibility issues with PowerBroker Desktops is located in a folder which has a folder rule applied. To avoid moving the application or changing the rule, the application may be excluded using the following registry key:

KEY: HKLM\SOFTWARE\Policies\BeyondTrust\PrivilegeManager
VALUE NAME: btSuppressHook
TYPE: REG_SZ
VALUE DATA: Set to the path(s) of the executable(s), separated by a semicolon

Additional Information:
Wildcards and UNC Paths are supported.
Application Profiling will still be enabled for any application specified in this key.
Any application specified in this key will not have a rule applied.

Examples:
A single application: C:\Program Files\Java\jre6\bin\java.exe
All applications in a specified folder: C:\Program Files\Java*
Multiple applications: C:\Windows\System32\userinit.exe;C:\Windows\system32\verclsid.exe
Application launched from a UNC path: \\Server\Share\Application.exe

Profiler Exclusion List (#13308)

In the event of compatibility issues, profiler dlls may now be excluded from being loaded into specified processes. To configure, the following registry key must be set:

KEY: HKLM\SOFTWARE\Policies\BeyondTrust\PrivilegeManager
VALUE NAME: ExcludedProfilerApps
TYPE: REG_SZ
VALUE DATA: Set to the path of the executable to be excluded

If an application is specified in the Exclusion List, then btpload.dll and btprof.dll will not be loaded into the process.

To exclude multiple applications, separate the paths with a semicolon. Environment variables (i.e. %SystemRoot% or %ProgramFiles%) are allowed. Wildcards may be used to exclude entire folders. Child processes of any excluded application will also be excluded.

Example: %SystemRoot%\system32\notepad.exe;c:\test.exe;%windir%\system32\cmd.exe;%ProgramFiles%*

FIXES

Sophos and Application Profiling (#13483)

When Sophos was installed and application profiling was enabled, Internet Explorer failed to launch properly when the PowerBroker Desktops browser helper object was enabled.

Driver Verifier (#13274)

An issue reported by verifier.exe on Windows 7 was resolved.

PowerBroker® for Desktops Windows® Edition 4.8 - Released 13 July 2010

INFORMATION

Rebranding (#13229)

BeyondTrust Privilege Manager has been rebranded as PowerBroker® for Desktops Windows® Edition.

NOTE: Due to the name change, when upgrading from previous Privilege Manager versions, if Policy Processing was enabled in the ADM/ADMX it will need to be reconfigured in order to write trace logs to the new location. Event logging keys are unchanged.

Windows 2000 (#13261)

Windows 2000 is no longer supported.

NEW FEATURES

Template Rules and Licensing (#13173)

The built-in template rules will now apply without a license.

NOTE: Add Local Printer, Alter TCP/IP Settings, and Add Plug and Play Device still require a license for domain policy.

FIXES

Defrag Rule (#13202)

The Defrag rule now works correctly when the user is a member of the Network Configuration Operators group.

Stopping PowerBroker Desktop Service (#13142)

When the privman driver is stopped, the PowerBroker Desktop Service now stops immediately.

Restarting privman (#13064)

An improvement was made to the behavior of the driver on restart.

Error in Application Event Log (#13073)

Userenv Error (ID 1085) in Application Event Log is no longer logged on reboot.

VMWare ThinApps (#13129)

VMWare ThinApps now display correctly on the desktop when elevated.

Privilege Manager 4.7 - Released 31 May 2010

INFORMATION

Internet Explorer Enhanced Security (#12620)

By default, Internet Explorer Enhanced Security disables third party browser extensions. To enable ActiveX rules to apply with Enhanced Security enabled, check "Enable third-party browser extensions" and restart Internet Explorer.

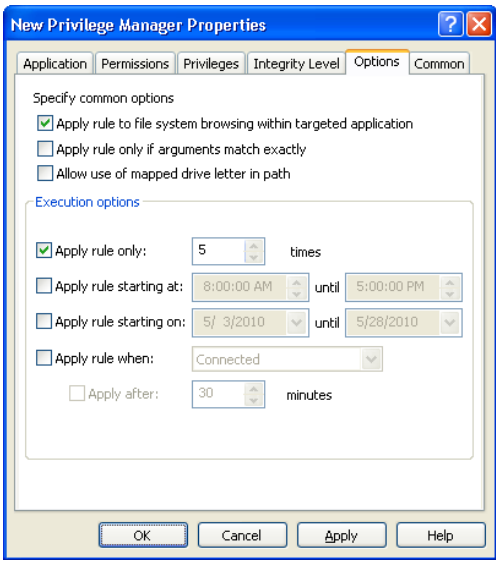
Windows 2000 (#13143)

If you are upgrading from Privilege Manager 4.1.0 or later on Windows 2000, you must uninstall the prior version and reboot before installing Privilege Manager 4.7.

NEW FEATURES

Execution Options: Number of executions (#12253)

On the Options tab, there is a new checkbox that enables a rule to be applied a specified number of times.

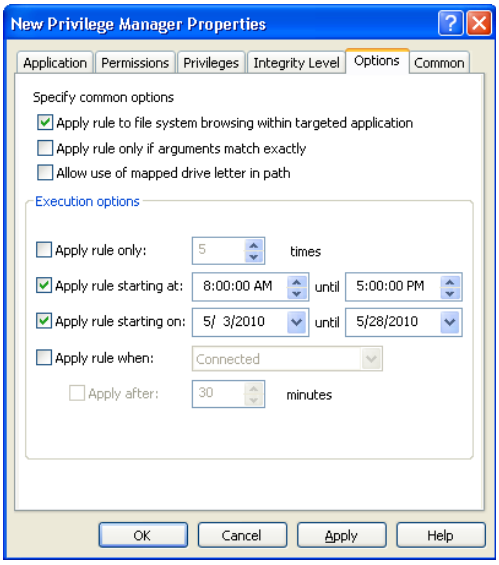


NOTE: If the rule is updated after it has been applied to the client, the rule GUID changes in the registry and the counter is reset.

Execution Options: Date/Time (#13029)

There is now an option to apply rules only during specified dates and/or hours.

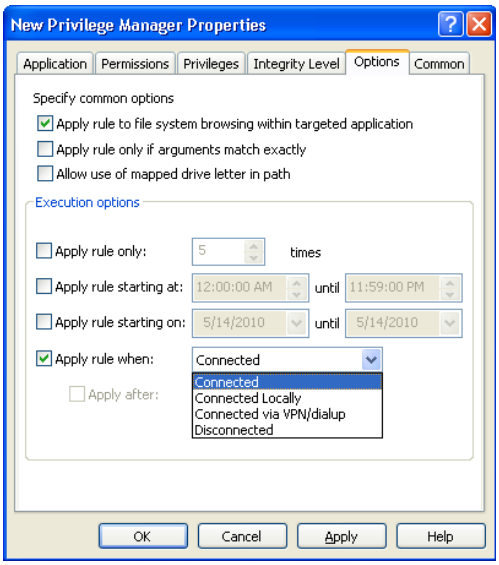
NOTE: The rule is applied on the client according to the client's time zone. For example, if the rule is set to apply between 9 AM and 5 PM, it will apply on the client between 9 AM and 5 PM according to the client's time.



Execution Options: Network Status (#12251)

Rules can now be applied according to whether a machine is on a network, VPN connection, or disconnected from the network.

NOTE: This option is not supported on Windows 2000.



Connected

Rule applies when computer is connected to a network via wireless, a network cable, or VPN connection.

Connected Locally

Rule applies when computer is connected to a network either via wireless or a network cable.

Connected via VPN/dialup

Rule applies when computer is connected to a VPN/dialup connection.

Disconnected

Rule applies when computer is disconnected from any network.

Disconnected - Apply after:

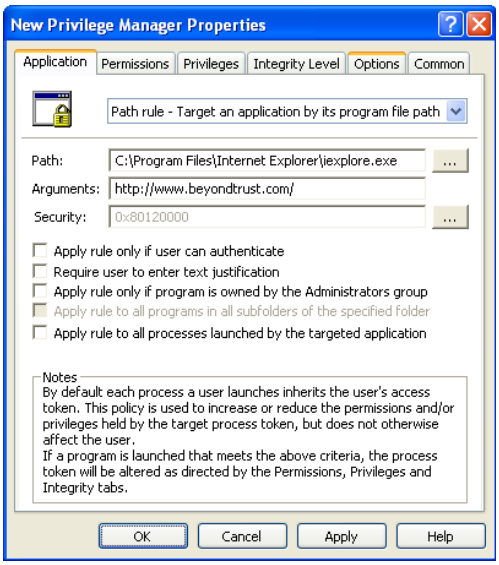
Rule applies when computer has been disconnected from a network for the specified amount of time.

Wild cards in Path Rules (#13059)

Wild cards are now supported in Path rules.

Internet Explorer Elevation (#13203)

Internet Explorer can now be elevated for specified web sites via a path rule. This feature is only supported for Windows Internet Explorer versions 7 and 8. To elevate Internet Explorer for a certain web site, create a path rule with the URL as the arguments:



Path

Enter the full path to iexplore.exe. For 32-bit machines, set the path to "C:\Program Files\Internet Explorer\iexplore.exe". For 64-bit machines use "C:\Program Files (x86)\Internet Explorer\iexplore.exe". Wild cards are also supported.

Arguments

Enter the URL for the web site to be elevated (i.e. http://www.beyondtrust.com). Wild cards are supported in this field as well (i.e. http*://*.beyondtrust.com).

Permissions

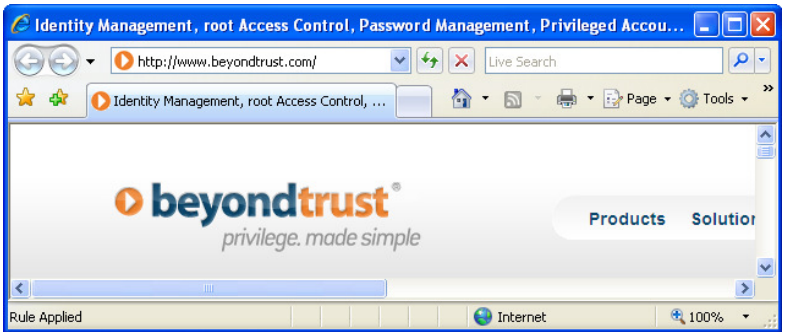
Add BUILTIN\Administrators.

Integrity Level

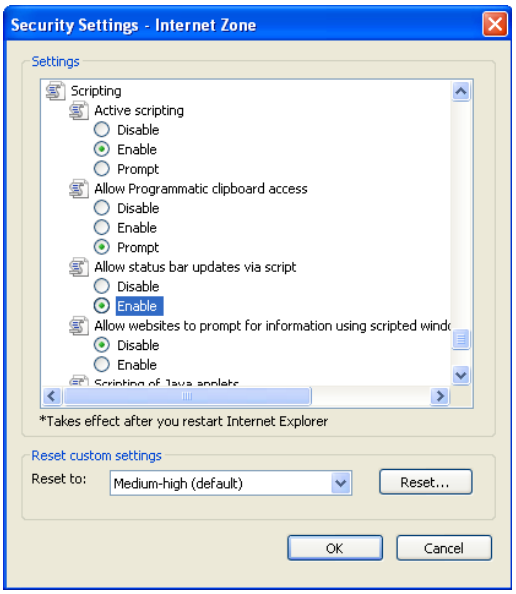
Recommended: Set to Medium.

NOTE: When a user navigates from one elevated web site to another, the rule is not reapplied. For this reason, if there are multiple Internet Explorer rules, keeping the Permissions/Privileges/Integrity level consistent throughout the rules is recommended.

When a rule matches, an elevated version of Internet Explorer will launch in a new window, and the new window will display "Rule Applied" in the lower left-hand corner:



NOTE: "Allow status bar updates via script" must be set to Enable in Internet Explorer Security Settings in order for the elevated window to display "Rule Applied".



If the user navigates to another web page that is not elevated, an error message will appear and the original page will be reloaded.

ENHANCEMENTS

Logging and btpload.dll (#12778)

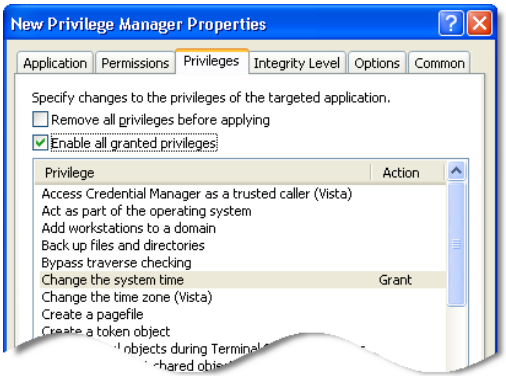
A new registry key was created which prevents btpload32.dll from being unloaded if the process name and path is found in the registry key value.

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BeyondTrust\PrivilegeManager
VALUE: KeepBtploadLoadedForApps
TYPE: REG_SZ

NOTE: Value should be set to the path of the executable, terminated by a semicolon. Any application specified in this key will have the following dlls loaded: btpload32.dll, btprof32.dll, privman32.dll.

Enable Privileges (#12773)

A new checkbox has been added to the snap-in which allows the user to enable all granted privileges by default.



NOTE: For security reasons, by default Privilege Manager sets privileges to Disabled. It is then up to the application to set the flag to Enabled. Certain applications may require the flag to be set to Enabled in order for the application to work correctly. If that is the case, checking the "Enable Privileges" box should resolve the issue.

ActiveX Rules: Ignore key (#12435)

Adding the CLSID of an ActiveX control to the following key will cause Privilege Manager to not install the control, as well as not prompt the user with the failure dialog box:

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BeyondTrust\SD
VALUE: Ignore
TYPE: REG_MULTI_SZ

Shell Rule (#13139)

There is no longer an icon next to the "Run Elevated" right-click menu option.

FIXES

Run As (#13104)
Run as now works correctly when a rule is applied to a process.

Profiling (#13056)
An issue with certain applications running incorrectly with profiling enabled has been fixed.

Event Logs (#12823)
The user name is now displayed in the system event log when "Detected the launch of an application requiring elevated rights" logging is enabled.

Elevating Cmd (#12677)
Child processes of an elevated command prompt are now correctly elevated when "Apply rule to all processes launched by the targeted application" is selected in the rule.

TCP/IP Settings (#12645)
The built-in rules were updated with the new "Alter TCP/IP Settings" shortcut rules.

RSOP Report (#12643)
The RSOP report was updated to match the snap-in user interface.

Date/Time Rule (#12601)
In the built-in rules, the Date/Time arguments for Windows 7 and Windows Vista have been corrected.

Screen set to 120 DPI (#12555)
The snap-in now displays correctly when the screen resolution is set to 120 DPI.

Untrusted Integrity Level (#12554)
An issue with an applied rule using the Untrusted Integrity Level has been resolved.

Security Enhancements (#12090)
Code was moved out of LSASS.exe and into btservice.exe.

Microsoft Office files (#13062)
Double-clicking a Microsoft Office file on a network share now opens the file successfully.
NOTE: The process security permission PROCESS_CREATE_THREAD must be selected in the rule for this to work.

Privilege Manager 4.6 - Released 23 November 2009

INFORMATION

Elevating an Installation Package (#12464)

When an executable is launched by an msi installation package, the process may be elevated even if "Apply rule to all subprocesses" is not checked. This will only occur if the application is launched by the installer. Subsequent launches of that application will only be elevated if there is a separate rule in place targeting the application.

Elevating a Flash Plug-In (#12015)

Certain Flash installations will require both an ActiveX rule and a rule on an external binary that is downloaded and installed. If a rule is required on an additional executable, all permissions in Process Security may be required.

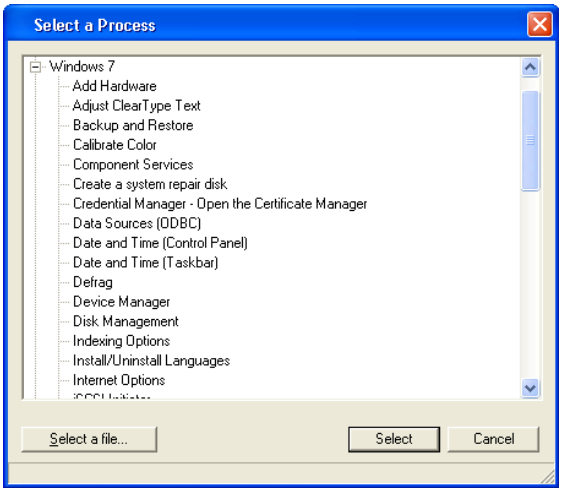
ActiveX rules on Windows 2008 (#12620)

ActiveX rules do not apply on Windows 2008 and Windows 2008 R2 when Internet Explorer Enhanced Security Configuration is Enabled.

NEW FEATURES

Improved Windows 7 Support (#12404)

Privilege Manager now offers improved support for Windows 7 Enterprise, Ultimate, and Professional. Windows 7 control panel rules have been added to the pre-built path rules:

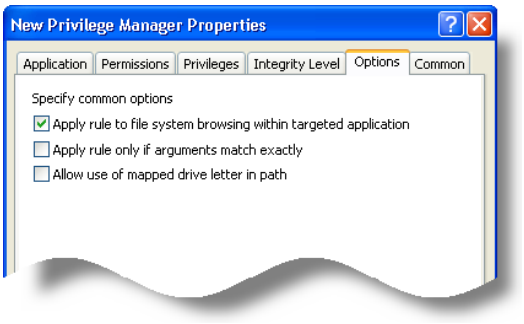


Windows 7 has also been added to the filters.

Apply Rule to File System Browsing (#12397)

There is a new checkbox named "Apply rule to file system browsing within targeted application." Unchecking this box for an elevated application will cause the admin rights to be dropped on the File Open/Save dialog box on compatible applications. By default, this box is checked (i.e. the File Open/Save dialog will be elevated).

NOTE: Unchecking this option will have no effect if the rule removes admin rights. Admin rights will not be re-added to the File Open/Save dialog once they have been removed on a targeted application.



Exclusion List (#12061)

It is now possible to exclude privman.dll from being loaded into specified processes. To configure, the following registry key must be set:

KEY: HKLM\SOFTWARE\Policies\BeyondTrust\PrivilegeManager
VALUE NAME: ExcludedApps
TYPE: REG_SZ

Set the value to the path of the executable you wish to exclude. If an application is specified in the Exclusion List, then privman.dll is not loaded into the process and any child processes will have their permissions/privileges inherited from the excluded application. This is true even if "Apply rule to all processes launched by the targeted application" is unchecked. In addition, no other Privilege Manager rules targeting the child process will be applied. Only applications whose parent process has privman.dll loaded will have Privilege Manager rules applied. An excluded application may still have a rule applied to it, as long as its parent process has privman.dll loaded.

To exclude multiple applications, separate the paths with a semicolon. Environment variables (i.e. %SystemRoot% or %ProgramFiles%) are allowed.

Example: %SystemRoot%\system32\notepad.exe;c:\test.exe;%windir%\system32\cmd.exe

ENHANCEMENTS

Security Enhancement (#12254)

Process owner protection has been updated to match improvements in Windows Vista, 2008, and 7.

Privilege Manager Driver (#12252)

Changes have been made to enhance the performance of the driver.

Permission field (#12045)

When the user clicks the Add button on the Snap-in Permissions tab, the Group dialog is now pre-populated with BUILTIN\Administrators.

FIXES

Microsoft Project Server (#12433)
An issue with authentication on the Microsoft Project EULA web page has been fixed.

Privilege Logging on x64 (#12046)
Polmon now logs privileges on 64-bit machines when Enable Privileges Adjustment Logging is enabled in the ADM/ADMX template.

Compiling in Cygwin (#12230)
An issue that caused an error when compiling in Cygwin has been fixed.

NOTE: PROCESS_DUP_HANDLE must be granted in Process Security.

Printing from Internet Explorer (#12113)
Printing from Internet Explorer with Protected Mode enabled no longer fails.

Launching Task Manager via Ctrl+Shift+Esc (#12103)
Task Manager now elevates correctly when launched from the shortcut keys (Ctrl+Shift+Esc)

Event Logging of Applications Requiring Admin Privileges (#12013)
Applications are now logged to the System Event Log as requiring admin privileges when UAC is enabled for a standard user.

Certificate Rules (#11630)
An issue that caused certificate rules to fail to apply was fixed.

Command Prompt Focus (#11602)
If an application that was launched from a command prompt was elevated, the command prompt did not get focus until the application was closed.

Compatibility with WSFTP (#11533)
A compatibility issue with WSFTP and conflicting versions of psapi.dll has been fixed.

Privilege Manager 4.5 - Released 31 July 2009

NEW FEATURES

Logging to the System Event Log (#12053)

Privilege Manager now supports logging information on application execution to the System Event Log. These options are configurable via the ADM/ADMX template.

The following options are available under Computer Configuration\Administrative Templates\BeyondTrust\System\Security Driver:

Detected the launch of an application

Log each time an application launches. NOTE: Enabling this setting will generate a large volume of log information.

Detected the launch of an application requiring elevated privileges

Log each time Privilege Manager detects an executed application that requires elevated privileges above Standard User.

Modified the privileges of an application at launch

Log each time an application launches that has had its privileges modified by Privilege Manager.

Modified the privileges of an application at launch by request of a user

Log each time a user launches an application using the Shell Rule capability of Privilege Manager.

Modified the privileges of an ActiveX control installation

Log each time an ActiveX control installation has its privileges modified by Privilege Manager.

Detected insufficient privileges to install an ActiveX control

Log each time an ActiveX control fails to install due to insufficient privileges.

ENHANCEMENTS

Event Log standardization (#12052)

All client-side extension logs now have a source of "Privilege Manager" and are logged to the application event log. All other logs have a source of "PRIVMAN" and are logged to the system event log.

FIXES

ARA Logging disabled (#11682)

ARA logging can no longer be enabled in Privilege Manager.

HookMode disabled (#11676)

The HookMode registry key no longer has any effect.

Extra blank line added to registry key (#11614)

The client installer no longer adds an extra blank line to the following registry key: HKLM\System\CurrentControlSet\Control\Lsa\Authentication Packages.

Error launching Microsoft Access (#11606)

With a rule on Microsoft Access, launching it via an mdb file or a shortcut no longer generates an error on Windows Vista in Admin Approval mode.
NOTE: The Integrity level must be set to Medium.

Manual install of Windows Updates (#11572)

Standard users can once again install Windows Updates by using the link in the Start menu. For more information contact technical support.

Snap-in and MSXML (#11449)

The Privilege Manager Snap-in installer no longer overwrites registry keys required by MSXML.

Privilege Manager 4.1.6 - Released 15 April 2009

FIXES

System hang (#11647)
An issue was eliminated that caused machines to stop responding under certain conditions.

Privilege Manager 4.1.4 - Released 11 February 2009

INFORMATION

Certificate Rule
Creating a certificate rule for Microsoft Corporation is not recommended.

FIXES

Scheduled Tasks (#11549)
Applications run as Scheduled Tasks are now elevated correctly.

Integrity Levels (#11527)
Integrity levels are now handled correctly on Windows Vista/2008.

Elevated command line applications (#11570)
Running an elevated command line application no longer generates a separate DOS window.

Privilege Manager 4.1.1 - Released 9 December 2008

INFORMATION

Upgrading from 4.1.0

If you are upgrading from Privilege Manager 4.1.0 and Privileges Adjustment Logging is enabled, you must disable it and reboot before upgrading. This can be disabled via the 4.0.1 ADM template, or by setting the following value in the registry:

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BeyondTrust\SD
VALUE: LogPrivileges = 0
TYPE: REG_DWORD

NOTE: This setting is disabled by default and should only be used for troubleshooting. If this key is not present or is set to 0, you do not need to change anything before upgrading.

If you are upgrading from Privilege Manager 4.1.0 on Windows 2000, you must uninstall 4.1.0 and reboot before installing Privilege Manager 4.1.1.

ENHANCEMENT

Novell ZENworks v4.2 Integration (#11515)

Privilege Manager now elevates applications launched from within Novell ZENworks v4.2.

Privilege Manager 4.1 - Released 24 November 2008

INFORMATION

Process Isolation (ShatterProof)

Process Isolation is not compatible with Windows Vista or Windows Server 2008. This feature will be deprecated in the next major release.

BitDefender 10

BitDefender 10 may intermittently cause slft.exe to crash. This is a known BitDefender bug affecting sockspy.dll.

Upgrading on Vista x64 with Certificate Rule

If you are manually upgrading the client from 4.0.1 on a Vista x64 machine and have a Certificate Rule in place for Microsoft Corporation, the upgrade may fail with an error referencing the Workstation service. To work around this issue, set the Integrity Level to High.

NOTE: If you are upgrading the client via a Software Installation policy this error will not occur.

Upgrading on Vista Gold (Service Pack 0)

If you are upgrading Privilege Manager on Vista Gold, under certain circumstances the upgrade may not complete successfully due to a bug in the Microsoft Visual C++ 2005 SP1 merge module.

SYMPTOM: When launching polmon, you will see the following error: "Cannot access kernel driver."

RESOLUTION: Any one of the following options will resolve the installation issue:

1. Reinstall the Microsoft Visual C++ 2005 SP1 Redistributable Package: **(x86)** **(x64)**
   -OR-
2. Install Windows Vista Service Pack 1, the Microsoft .NET Framework 2.0 Service Pack 1 **(x86)** **(x64)**, or the **Microsoft .NET Framework 3.0 Service Pack 1**
   -OR-
3. Install the Privilege Manager Snap-In, which will reinstall the Microsoft Visual C++ 2005 SP1 runtime.

NEW FEATURES

Support for Windows Vista + RSAT, Server 2008 (#10985)

The Privilege Manager snap-in now supports editing network policies on Windows Vista SP1 + RSAT, as well as Windows Server 2008.

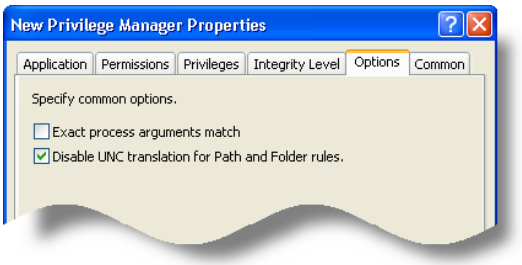
Application Arguments (#11300)

There is now an option to require an exact match of the application arguments in order to elevate an application.

NOTE: This option does not apply to Shell, CD/DVD and Certificate rule types.

Rules based on Mapped Drives (#11407)

The "Disable UNC translation for mapped drives and folder rules" option enables you to create and apply rules based on mapped drives. By default, Privilege Manager applies rules based on the UNC path. As a limited user has the ability to change a mapped drive, checking this option presents a security risk as it could enable them to elevate an unintended application.



ENHANCEMENTS

Policy Monitor Multi-Select (#11376)

Polmon now allows you to select multiple lines.

Integrity Level set to High (#11362)

When adding the Administrators group on the Permissions tab, the Integrity Level must be set to High on Windows Vista and 2008. This is now automatically set when a rule is created in the snap-in.

Operating Systems Filter (#11360)

Unsupported operating systems such as Windows 9.x and NT 4.0 were removed from the operating systems filter.

User Configurable Timeout (#11310)

There is now a registry key that enables the user to set a custom timeout value when connecting to the Application Rights Auditor server to upload data. This value will also be logged to pmslft.log.

KEY: SOFTWARE\Policies\BeyondTrust\SLFT
VALUE: ConnectTimeout, default value: 3000 (milliseconds)
TYPE: REG_DWORD

KEY: SOFTWARE\Policies\BeyondTrust\SLFT
VALUE: SendTimeout, default value: 4500 (milliseconds)
TYPE: REG_DWORD

Event Log on Authentication Failure (#11301)

If a user is prompted to authenticate by Privilege Manager, but the authentication fails when they enter their credentials, an event is logged to the system event log.

Security Enhancement (#11298)

Additional protection has been added against privilege escalation attacks.

Application Execution Logging (#11256)

There is a new ADM/ADMX setting to control the amount of data logged on application execution. This setting enables you to log no executions, log all executions, log only executions with the Administrators token, or log only executions with a Privilege Manager rule match.

NOTE: Application Rights Auditor Logging must be enabled in order for this setting to take effect.

Authentication and Justification unlinked (#11220)

The "Apply rule only if user can authenticate" and "Require user to enter text justification" checkboxes have been unlinked. Each option may now be used independently.

CD/DVD Rule (#11132)

The CD/DVD Rule now elevates MSIs.

Defrag Rule (#10598)

A defrag rule for XP has been added to the built-in path rules.

FIXES

User Filter (#11532)
Editing a policy with a user filter caused an error.

HookMode and Vista (#11442)
Setting HookMode=0 in the registry caused an error with some applications on Vista.

ActiveX Window (#11418)
The ActiveX installation dialog is now always in the foreground.

Unchanged Security Context Prompt (#11398)
User was prompted to change permissions when editing a rule with only a change to the Integrity Level.

Low integrity level and sound (#11366)
Sound will now work for an application set to a low integrity level.

NOTE: You must change the default process security by granting PROCESS_DUP_HANDLE.

Privilege Manager node re-activated (#11356)
The Privilege Manager node in the Snap-In (HTML view) is now visible when Internet Explorer 7 is installed.

Vista Integrity Level (#11353)
A process set to a Low integrity level could still read from a file/folder with a higher integrity level and no-read-up set.

NOTE: Any files/folders that the process requires access to will need to be set to the same integrity level using chml or icacls (i.e. Mozilla Firefox).

Vista Backup (#11351)
The Backup rule (sdlct.exe) now works on Windows Vista Service Pack 1.

NOTE: You must have Service Pack 1 installed - the backup rule will not work on Service Pack 0.

Deleting a printer (#11340)
Using Delete (Elevated) on a network printer deleted the printer from the server if the user had the necessary rights.

Error elevating the remote debugger monitor (#11338)
An invalid handle error occurred when elevating the remote debugger monitor (msvsmon.exe).

User Filter (#11333)
When using the Match by SID in the User filter, the user name was not persisted.

Vista and Protected Administrators (#11324)
Privilege Manager now elevates applications correctly when logged in as an administrator on Vista with User Account Control enabled.

Organization Unit (OU) Filter (#11303)
The OU Filter now closes the opened port in a timely manner.

Vista Filter (#11289)
The Vista Filter now works correctly if you select a flavor (Ultimate, Business, etc.).

ActiveX Rule Security (#11276)
In certain circumstances the ActiveX installer process could be used to elevate an unauthorized application.

Novell Netware Shares (#11250)
Privilege Manager now correctly resolves Novell Netware shares.

Timeout with User Authentication Dialog Box (#11227)
The Authentication Dialog box timed out incorrectly and closed.

Profiler causes some applications to delay (#11224)
In some instances applications would run slowly or hang with profiling enabled.

Fix to Java Web Applications (#11223)
The Privilege Manager Browser Helper Object (pmbho) caused some Java web-based applications to not work.

USB Drive (#11217)
Rules did not apply to certain USB drives unless the drive was in the machine during boot up.

Snap-In Installation (#11149)
Inconsistencies in the Snap-In installation package were removed.

Invalid Signature (#10994)
Some rules produced an invalid DSA signature error.

MSI Rules with Mapped Drives (#10506)
A UNC MSI Path or Folder rule did not apply when the MSI was launched fron a mapped drive.

ActiveX Installation Failure Dialog Box (#10311)
The ActiveX Installation Failure Dialog Box did not appear on Windows Vista.

Privilege Manager 4.0 - Released 5 May 2008

INFORMATION

.NET Framework 2.0
You must install the .NET Framework 2.0 before installing the BeyondTrust Privilege Manager 4.0 Snap-in.

NEW FEATURES

Integrity Levels on Vista (#10104)
Privilege Manager now supports changing the integrity level for a process on Vista machines.

Shell Rule (#11048)
New Shell rule has been added to enable user to elevate applications on demand.

Certificate Rules (#10298)
You can now target an application based on certificate.

UAC with Administrative Privileges (#10309)
Rules are now applied on Vista with UAC enabled when the user has administrative privileges (i.e. is a member of Network Configuration Operators Group).

User Authentication (#11051)
You now have the option to apply a rule only when a user authenticates using their credentials.

CD/DVD Rule (#11070)
You now have the option to elevate all applications on a certain CD or DVD.

User Justification Logging (#11072)
You now have the option to require a user to enter a justification for the application elevation, which will be logged.

ENHANCEMENTS

New OS Filters (#10972)
Windows Vista SP1, Windows XP SP3, and Windows Server 2008 have been added to the OS Filters.

64-bit Snap-in (#11080)
Privilege Manager snap-in is now a true 64-bit snap-in.

Server 2008 Control Panel Rules (#11006)
Added Server 2008 Control Panel rules.

ADM/ADMX have new setting (#11016)
The ADM/ADMX files now enable you to change the LogPrivileges setting.

FIXES

SD Log in ADMX (#11009)
The ADMX now retains the setting for a custom location for the pmsd log file.

Privilege Manager 3.5.1 - Released 28 September 2007

INFORMATION

Compatibility with Microsoft Advanced Group Policy Management

Microsoft Advanced Group Policy Management (AGPM, formerly DesktopStandard's GPOVault) does not currently support third-party extensions. As a result, Privilege Manager rules will not be preserved when the GPO has been edited with AGPM.

FIXES

Outlook data file access error (#8348)

Applying a rule to Outlook caused an error accessing the pst or ost files.

Polmon version information (#8543)

Polmon.exe: Help -> About had the wrong version information.

Snap-in version information (#8540)

SnapIn: Help -> About had the wrong version information.

Shortcuts to Internet Explorer (#8536)

Rules were not applied to Internet Explorer when it was launched from a shortcut.

Plug & Play USB device installations (#8530)

Plug & Play USB device installations weren't elevated in 3.0.1.

NOTE: Plug & Play USB device installations will not elevate on Windows Vista in the current Privilege Manager release. If the driver is already present on the machine, Windows Vista does not require local admin privileges to install the driver. If the driver is not present on the machine, you may use Windows native policy to enable standard users to install drivers.

Printing from an application with rules applied (#8513)

Installed printers did not show up when printing from an application that had a Privilege Manager rule applied.

Vista privileges on XP SP2 (#8389)

Granting/Denying a Vista privilege caused policies to not apply on XP SP2.

Privilege Manager 3.5 - Released 21 August 2007

NEW FEATURES

Support for User Account Control (#8531)

Privilege Manager rules will apply when a standard user logs onto a machine with UAC enabled. Note: Privilege Manager rules will not trigger when UAC is enabled and the user is logged on as a local administrator.

Installation with UAC enabled (#8527)

Privilege Manager will now install with Windows Vista's User Account Control (UAC) enabled.

ENHANCEMENTS

ActiveX controls and authentication (#8523)

ActiveX rules will now work with a proxy server that requires authentication.

Executable Manifests on Vista x86 (#8507)

Privilege Manager no longer requires the requestedExecutionLevel to be defined in the manifest of an elevated executable on Vista 32-bit machines.

NOTE: Stopping and restarting the driver on Vista x86 will require a reboot. This affects both manually using "sc stop" and "sc start" as well as upgrading to a future version. To disable this feature, add a DWORD value named "DisableManifestEx" under HKLM\Software\Policies\beyondtrust\SD and set it to "1". If you set this key, you will need to set the requestedExecutionLevel in the manifest of any elevated applications.

FIXES

ADMX Template (#8526)

The setting to enable/disable the User/Computer Settings nodes was reversed in ADMX template.

Offline triggering of rules (#8524)

Rules now are triggered when a machine is booted without a network connection.

Mapped drives to DFS shares (#8511)

Rules will now trigger when an application is run from a mapped drive to a DFS share.

Wildcards in ActiveX rules (#8508)

A malformed path in an ActiveX rule elevated all ActiveX installs. To elevate all ActiveX controls for a web site, specify "http://*.mywebsite.com". If only "*.mywebsite.com" is entered (without http://), no controls will be elevated.

Privilege Manager 3.0.2 - Released 27 April 2007

ENHANCEMENTS

Improvement to elevating executables on Vista (#8507)
Privilege Manager no longer requires requestedExecutionLevel to be defined in the manifest of an elevated executable on Vista.

FIXES

Error on uninstall (#8476)
An error sometimes occurred while uninstalling Privilege Manager.

Privilege Manager 3.0.1 - Released 10 April 2007

ENHANCEMENTS

Driver Name Change (#8495)
The Privilege Manager driver name was changed from pmsecdrv.sys to privman.sys.

Improvement in Upgrade Process (#8465)
An extra reboot is no longer required when upgrading the client from 2.5.5.

Optimization - Reload Rules (#8492)
Polmon will only "Reload Rules" when tracing is enabled.

FIXES

Fix to command line parser (#8487)
An error occurred parsing certain command lines in a rule.

UAC Warning Message on Vista (#8454)
An error message is displayed when installing on Vista if User Account Control (UAC) is enabled.

Privilege Manager 3.0 - Released 23 March 2007

SUPPORTED PLATFORMS

64-bit Platforms

Windows Vista, Windows XP SP2, Windows 2003 SP1

32-bit Platforms

Windows Vista, Windows XP SP2, Windows 2003 SP1, Windows 2000 SP4 (with Update Rollup Package + Windows Installer 3.1)

INSTALLATION INFORMATION

Upgrade from previous versions

You must uninstall previous versions of Application Security before installing Privilege Manager 3.0. For details on upgrading from previous versions, see the upgrade documentation.

ADM Template

Any Policymaker Application Security settings that were enabled in the DesktopStandard ADM template must now be configured in the BeyondTrust ADM template. Once the BeyondTrust ADM template is configured, the PolicyMaker Application Security settings should be set to "Not Configured" in the DesktopStandard ADM template.

Vista: User Account Control

User Account Control must be turned off on any Vista machines in order to install and use Privilege Manager 3.0.

Windows 2000

Windows Installer 3.1 must be installed on any Windows 2000 machines before installing Privilege Manager 3.0.

OTHER INFORMATION

Upgrading from PolicyMaker Application Security

Version 1.x and 2.x policies will not be automatically transferred into Privilege Manager 3.0. You must either copy and paste the appropriate xml data from the sysvol location or copy/paste from a v1.x or v2.x PolicyMaker Application Security snap-in.

Vista Privileges

If you grant or deny any of the 5 Vista-specific privileges, the policy will not apply on any non-Vista machines. For this reason, if your policy requires changing Vista-specific privileges, you should make a separate rule for non-Vista machines.

Message Box on Vista

Applying a policy with a message box filter will cause Vista machines to hang on boot.

64-bit Machines

The Privilege Manager extension will only appear when MMC is run in 32-bit mode. **More information**

Internet Explorer Enhanced Security on Windows 2003

Windows 2003 SP1: If Internet Explorer Enhanced Security is installed, ActiveX rules will not apply.

NEW FEATURES

Support for Windows Vista (#8358)

Privilege Manager now supports Windows Vista. The rules for Vista Control Panel applications were also added to the Paths.

ADMX Templates on Vista Machines (#8405)

Vista supports a new XML-based format for ADM templates. New ADM templates have an extension of "ADMX" and are loaded automatically from either %systemroot%\PolicyDefinitions [local policy] or %systemroot%\sysvol\domain\policies\PolicyDefinitions [network policy] when the Group Policy Object Editor is opened. Classic ADM templates are still supported in Vista, and when loaded the settings will appear under "Classic Administrative Templates (ADM)\BeyondTrust".

BeyondTrust Privilege Manager supports both the classic ADM as well as the new ADMX template on Vista machines.

Support for 64-bit machines (#8384)

Privilege Manager now supports 64-bit machines.

Registry Key Displays Required Privileges in Polmon (#8397)

There is now a registry key that will display the privileges required to run an application in Policy Monitor (polmon.exe). This setting will only display privileges on 32-bit systems.

ENHANCEMENTS

Rebranding (#8451)

BeyondTrust Privilege Manager has been rebranded from DesktopStandard PolicyMaker Application Security. The Privilege Manager extension now appears in the Group Policy Object Editor under Computer/User Security -> Privilege Manager.

FIXES

OU Filter: Special Characters in OU Crashed MMC (#8364)

If you had an OU with a special character such as "/", and you tried to create an OU filter on a Privilege Manager rule against that OU, MMC would crash.
