User Guide

Release 5.3
Revision/Update Information: August 17, 2012
Software Version: PowerBroker Desktops 5.3
Revision Number: 0

COPYRIGHT NOTICE
Copyright © 2005–2012 BeyondTrust Software, Inc. All rights reserved. Use of this software and/or document, as and when applicable, is also subject to the terms and conditions of the license between the licensee and BeyondTrust Software, Inc. ("BeyondTrust") or BeyondTrust's authorized remarketer, if and when applicable.

TRADE SECRET NOTICE
This software and/or documentation, as and when applicable, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of BeyondTrust and/or of the respective manufacturer or author, and may not be disclosed to others without the prior written permission of BeyondTrust. This software and/or documentation, as and when applicable, have been provided pursuant to an agreement that contains prohibitions against and/or restrictions on copying, modification and use.

DISCLAIMER
BeyondTrust makes no representations or warranties with respect to the contents hereof. Other than, any limited warranties expressly provided pursuant to a license agreement, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE.

LIMITED RIGHTS FARS NOTICE (If Applicable)
If provided pursuant to FARS, this software and/or documentation, as and when applicable, are submitted with limited rights. This software and/or documentation, as and when applicable, may be reproduced and used by the Government with the express limitation that it will not, without the permission of BeyondTrust, be used outside the Government for the following purposes: manufacture, duplication, distribution or disclosure. (FAR 52.227-14(g)(2)(Alternate II))

LIMITED RIGHTS DFARS NOTICE (If Applicable)
If provided pursuant to DFARS, use, duplication, or disclosure of this software and/or documentation by the Government is subject to limited rights and other restrictions, as set forth in the Rights in Technical Data – Noncommercial Items clause at DFARS 252.227-7013.

TRADEMARK NOTICES
PowerBroker, Password, and PowerKeeper are registered trademarks of BeyondTrust. PowerSeries, PowerADvantage, PowerBroker Password Safe, PowerBroker Directory Integrator, PowerBroker Management Console, PowerBroker for Desktops, PowerBroker for Virtualization, and PowerBroker Express are trademarks of BeyondTrust. SafeNet and SafeNet logo are registered trademarks of SafeNet, Inc. Copyright 2009, by SafeNet, Inc. All rights reserved. Product names of any third party remain the trademarks of such third party manufacturers and/or distributors, respectively.

FICTITIOUS USE OF NAMES
All names of persons mentioned in this document are used fictitiously. Any resemblance to actual persons, living or dead is entirely coincidental.

OTHER NOTICES
If and when applicable the following additional provisions are so noted:
BeyondTrust is a registered trademark of BeyondTrust Software, Inc. This document is for informational purposes only. BeyondTrust offers no warranties, express or implied, in this document. Microsoft, Internet Explorer, Outlook, Windows, Windows Server, and Windows Vista are trademarks or registered trademarks of Microsoft Corporation. Other names mentioned herein may be trademarks of their respective owners.

LIBRARY NOTICES

crypto.lib Library
Permission to use, copy, and modify this software without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software. NOTE: Some of the algorithms in cryptolib may be covered by patents. It is the responsibility of the user to ensure that any required licenses are obtained.

SOME PARTS OF CRYPTOLIB MAY BE RESTRICTED UNDER UNITED STATES EXPORT REGULATIONS.
THIS SOFTWARE IS BEING PROVIDED “AS IS”, WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR AT&T MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

detours.lib Library
Microsoft Research Detours Package, Professional Version 2.1 Build_216.

DISCLAIMER AND LICENSE:
==================================
The entire Detours package is covered by copyright law.
Copyright © Microsoft Corporation. All rights reserved.
Portions may be covered by patents owned by Microsoft Corporation.

libtomcrypt.lib Library
Tom St Denis, tomsdenis@iahu.ca, http://libtomcrypt.org.

ziputil.lib Library
Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

xmlparse.lib Library
Other names mentioned herein may be trademarks of their respective owners.

 IPAddressControlLib
Copyright © 2007 Michael Chapman
# Contents

**Introduction**................................................................. 9

**What's New in Version 5.3.**.................................................. 10

**Additional Information**..................................................... 13
  - Documentation for PowerBroker Desktops.................................. 13
  - Support for PowerBroker Desktops......................................... 13
  - Available Resources......................................................... 13
  - Before Contacting Technical Support.................................... 14
  - Contacting Support.......................................................... 14

**Product Overview**.......................................................... 16
  - How PowerBroker Desktops Works.......................................... 16
  - PowerBroker Desktops Terminology...................................... 18
  - PowerBroker Desktops Architecture..................................... 19
  - What You Can Do with PowerBroker Desktops............................. 19
    - Use the Management Dashboard to Get Started....................... 20
    - Manage Application and Process Security with Rules............... 22
      - Target Applications and Processes.................................. 22
      - Perform Application Control........................................ 22
      - Modify Permissions.................................................... 23
      - Modify Privileges..................................................... 23
      - Modify Integrity Level................................................. 23
      - Fine-Tune the Targeting of a Rule.................................. 23
    - Customize and Manage User Messages.................................. 25
    - Back Up Group Policy Objects........................................... 26
    - View and Manage Reports................................................ 26

**Getting Started with PowerBroker Desktops**.......................... 28
  - Creating or Editing a GPO................................................ 28
  - Viewing the Management Dashboard...................................... 30
  - Planning a Rule.............................................................. 32
    - Determining the Type of Rule Needed.................................. 32
    - Determining an Application Control Approach......................... 34
      - Blacklisting............................................................... 34
      - Whitelisting.............................................................. 35
    - Using Wildcards in Rule Properties.................................... 37
      - Wildcard Cautions and Examples...................................... 38
      - Wildcards and Subfolders.............................................. 38
    - Choosing a Rule Creation Method....................................... 39
  - Creating a Rule with the Wizard......................................... 40
  - Generating Rules with the Reporting Console.......................... 43
  - Generating Rules and Creating Reports.................................. 44
Generating Multiple Rules for a Type of Application ........................................... 45
Creating or Editing a Rule with the Properties Dialog ........................................... 47
Changing the Name of a Rule ................................................................................. 50
Viewing a Settings Report ...................................................................................... 50
Disabling or Enabling a Rule ................................................................................. 52
Working Offline ...................................................................................................... 52
Effects of Disabling Rules or Extensions ............................................................... 53

Targeting Applications or Processes ...................................................................... 54
Targeting by Location (Path Rule) .......................................................................... 54
  Example: Elevate IE for a Website .................................................................... 57
  Example: Elevate a Visual Basic Script .............................................................. 58
  Example: Elevate a Registry Merge ................................................................. 59
  Example: Elevate a Batch File .......................................................................... 60
Targeting by Signature (Publisher Rule) ................................................................ 61
  Target by Publisher Only .................................................................................. 62
  Target by Any Digital Signature Element ......................................................... 63
Targeting Regardless of Location (Hash Rule) ......................................................... 64
Targeting by Folder Location (Folder Rule) .............................................................. 67
Targeting an Installation File by Location (MSI Path Rule) ...................................... 70
Targeting Installation Files by Folder Location (MSI Folder Rule) .......................... 72
Targeting through Internet Explorer (ActiveX Rule) ............................................... 75
Targeting Applications on Demand (Shell Rule) ..................................................... 79
Targeting a CD/DVD (CD/DVD Rule) ................................................................... 81
Targeting Applications That Trigger UAC (UAC Rule) ........................................... 82

Selecting an Action for Application Control .......................................................... 84

Configuring Common Options .............................................................................. 86

Configuring Token Security ................................................................................. 88
  Modifying Permissions ....................................................................................... 89
  Modifying Privileges .......................................................................................... 91
  Modifying Process Security .............................................................................. 93
  Modifying Integrity Level .................................................................................. 94

Configuring Execution Options ............................................................................. 96

Targeting Users or Computers with Item-Level Targeting .................................... 98
  Grouping Targeting Items into a Collection ...................................................... 101

Arranging the Order of Rules ................................................................................. 104

Advanced Techniques ............................................................................................ 106
  Copying a Rule .................................................................................................. 106
Managing Multiple Rules with a Collection .............................................................. 107
 Rule Processing When Collections Are Present .................................................... 109
Using Variables in Rule Properties ............................................................................. 111
 Environment Variables ............................................................................................ 111
 Process and Volatile Variables ................................................................................. 112
 Select a Variable Dialog .......................................................................................... 114
Managing User Messages ........................................................................................... 116
 Creating Application Launch Dialogs (Application Launch) .................................. 117
  Example: Passcode Access When UAC Is Triggered .............................................. 120
 Creating Blocked Application Dialogs (Blocked Application) ............................ 121
 Customizing the Appearance of Internet Explorer When Elevated ....................... 122
  (IE Elevation) ........................................................................................................ 123
 Customizing the Internet Explorer Component Failure Dialog (IE Failure) ......... 124
 Customizing the Right-Click Menu Options (On-Demand Elevation) ................. 126
 Customizing the UAC Information Dialog (UAC Prompt Detected) .................. 127
 Customizing the Internet Explorer Download Dialog ......................................... 130
Generating a Passcode to Respond to a Message ...................................................... 132
 Generating a Passcode ............................................................................................ 132
 Changing the Key Pair and Keys Path ..................................................................... 133
Viewing and Managing Reports ................................................................................. 135
 Types of Reporting Services Reports ..................................................................... 135
 Viewing a Reporting Services Report ..................................................................... 136
 Auditing and Reporting Dashboard ........................................................................ 136
 ActiveX Details Report ........................................................................................... 138
 Applications by Path Report .................................................................................... 139
 Applications by Hash Report .................................................................................... 141
 Applications by Computer Report ........................................................................... 142
 Application Hash Details Report ............................................................................. 144
 Application Path Details Report .............................................................................. 145
 Shell Executions Report ............................................................................................ 147
Configuring Logging for Data Collection ................................................................. 149
 Backing Up a GPO ................................................................................................. 152
 Editing the XML Source Code of a Rule ................................................................. 153
Troubleshooting ......................................................................................................... 154
 Rules Have No Effect ............................................................................................... 154
 Compatibility Issues with Some Applications ....................................................... 156
 Problems Requiring Process-Specific Access Rights .............................................. 156
 Other Problems ........................................................................................................ 159
Troubleshooting Mechanisms .................................................................................... 160
 Event Logging ........................................................................................................... 160
 Using the Event Viewer ............................................................................................ 162
 System Log Events .................................................................................................... 163
 Application Log Events ............................................................................................. 164
 Tracing with Policy Monitor ..................................................................................... 165
 Policy Monitor ........................................................................................................... 165
Introduction

PowerBroker Desktops is a Group Policy extension that provides a least privilege security model for Windows. Using PowerBroker Desktops, you can provide standard users with elevated permissions for selected tasks and applications. You can also reduce permissions of applications such as Internet Explorer and Outlook when launched by administrators.

This guide provides instructions for using PowerBroker Desktops and information about product features, benefits, functions, unique concepts, and basic procedures.

Where to Begin

- If you have not yet installed PowerBroker Desktops or need information about licensing, see the PowerBroker Desktops Installation Guide.
- If you are upgrading to a new version, see the PowerBroker Desktops Upgrade Guide.
- If you are already familiar with PowerBroker Desktops, see “What’s New in Version 5.3,” page 10, to learn about the new features and functions available in this version.
- If you are new to PowerBroker Desktops, see “Getting Started with PowerBroker Desktops,” page 28, to learn how to create rules to perform application control and manage application and process security.
- For an introduction to Group Policy, see “Appendix A: Group Policy Primer,” page 170.
- For support and additional documentation, see “Additional Information,” page 13.
What's New in Version 5.3

Version 5.3 of PowerBroker Desktops brings new features and functions that make creating and managing rules and Group Policy easier. Highlights of this version include:

- **Adding or Removing Administrator Rights** – You can make all of the permissions, privileges, and integrity level changes necessary to add or remove Administrator rights by selecting a single action.

- **One-Time Access by Passcode** – 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. For example, you could provide access to an application for a support professional who does not have an end-user's credentials available. A list of the applications most frequently launched by using Authorization Code is included on the Auditing and Reporting Dashboard.

- **Message Improvements** – The PowerBroker Desktops Messages window provides more realistic approximations of dialogs produced by messages so that you can see the impact of your configuration before deploying it. Optional Passcode access functionality has been incorporated into Application Launch and Blocked Application messages. More properties of messages can be configured, and the readability of the available options has been improved.

- **Internet Explorer Elevation Improvements** – When a rule is used to elevate Internet Explorer, the user experience is improved. Visual indicators of the elevated state of Internet Explorer appear in the title tab and status bar, and the text can be customized.

- **Shell Rule Improvements** – You can use Shell rules to allow users to elevate files with any of the following extensions on demand:
  - EXE (Executable file)
  - 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)
Streamlined Interface – In the Properties dialogs for rules and collections, related functionality has been gathered onto fewer tabs so that fewer clicks are needed and so that it is easier to review properties quickly. In the Create a Rule Wizard, the Security page has been reorganized to better align with the typical workflow.

Streamlined Documentation – The Help has been reorganized to require fewer clicks, to better support the typical workflow, and to make information easier to find.

The following features were included in PowerBroker Desktops beginning in previous 5.x versions:

• **Actions for Application Control** – For most rule types, you now have a choice of actions available, and you can use actions to achieve a blacklisting or whitelisting approach to application control.

• **Auditing and Reporting** – PowerBroker Desktops Auditing and Reporting lets you collect privilege-related event log data from client computers into a database, and then sort and filter this data into reports about applications used, privileges required, how applications are launched, and which users have administrator privileges. Using the Reporting Console, you can generate rules for applications based on user needs for privilege elevation. Using Reporting Services, you can view graphical reports.

• **Auditing and Reporting Improvements** – The layout of Reporting Services reports has been improved and the installation process for Auditing and Reporting has been simplified.

• **Messages** – You can use messages to customize prompts and elements of the user interface for end-users. You can display customized messages to prompt end-users to enter their user name and password or a justification. You can display a message when a particular application is launched, when a UAC prompt is detected, or when the installation of an ActiveX control fails in Internet Explorer. You can also customize the appearance of Internet Explorer when it is elevated, and customize the text displayed in context menus when end-users right-click executable files (EXE) or Windows Installer packages (MSI).

• **Blocked Application Dialogs** – You can display a dialog box when an end-user attempts to start a prohibited application. You can provide a contact email address from which end-users can request authorization.
• **Management Dashboard** – The PowerBroker Desktops dashboard provides a high-level entry point into the product. The dashboard is available by selecting the BeyondTrust node in the Group Policy Management Editor. From the Management Dashboard, you can access information, open tools and wizards, and view reports that document rule settings and XML. The Management Dashboard provides a convenient and easy-to-use way of interacting with PowerBroker Desktops.

• **Rule Wizard** – The rule wizard further simplifies the task of building rules. This wizard guides you step-by-step through all the phases of rule creation. Helpful prompts and information are always available to clarify each step of the process. The wizard can build any type of rule and can also be disabled when you want direct access to the rule properties dialog.

• **Publisher Rule** – This type of rule uses an application's digital signature elements as a target. One or more signature elements can be specified to build very specific rules. For example, a Publisher rule can be targeted at a specific version of a signed application by using the version parameter available in the rule. This rule type replaced the less powerful Certificate rule.

• **Rule Collections** – You can now group rules into collections to enhance rule management and organization. A rule collection is treated as a single entity, and a filter applied to a collection is recognized and used by every rule in the collection. A collection simplifies the organization and management of large rule sets.

• **Expanded Wildcard Use** – You can substitute wildcard characters in Path and Argument fields in more types of rules. Wildcards can now be used in the following rule types: Shell, MSI Path, MSI Folder, and UAC (user account control).

• **Refined Look and Feel** – Many areas of the PowerBroker Desktops user interface have been redesigned to be more intuitive and familiar, and leveraging your experience with other software. For example, the Item-level targeting interface mimics similar functions in Group Policy tools, and the rule wizard and Publisher rule will be familiar to users of Microsoft AppLocker for Windows 7.
Additional Information

For more information about PowerBroker Desktops, see the documentation and resources listed in the following sections.

Documentation for PowerBroker Desktops

For information about installing and licensing PowerBroker Desktops, see the PowerBroker Desktops Installation Guide.

The PowerBroker Desktops documentation includes:

- PowerBroker Desktops Installation Guide
- PowerBroker Desktops User Guide
- PowerBroker Desktops Upgrade Guide V4.x to V5.3
- PowerBroker Desktops Upgrade Guide V5.x to V5.3

Support for PowerBroker Desktops

BeyondTrust provides an online knowledge base, as well as telephone and web-based support. In addition, when working with any PowerBroker Desktops item, you can click the Help button to view detailed information about available options.

Available Resources

The PowerBroker Desktops Knowledge Base provides information and solutions to many known problems and issues. Registered users can access the Knowledge Base by logging onto the BeyondTrust Customer/Partner Portal on our website.

To download a comprehensive set of over 120 pre-configured rules, log onto the BeyondTrust website (www.beyondtrust.com), navigate to the documentation area for PowerBroker Desktops, and click the Rules Library link for this version of PowerBroker Desktops.
Before Contacting Technical Support

Tip: Is the PowerBroker Desktops client software running?

A computer must have the PowerBroker Desktops client software installed and running to recognize rules. If a computer does not respond to a rule or a policy setting, make sure that the client software is installed and activated on the computer. Run the Policy Monitor (polmon.exe) utility on the computer to check for client software activation and functionality. For more information, see “Tracing with Policy Monitor,” page 165.

Obtain as much information about the problem as possible using PowerBroker Desktops troubleshooting tools. For more information, see “Troubleshooting Mechanisms,” page 160.

To expedite support, collect the following information:

- Image or the full text of any error messages
- Context of the problem, including affected platforms
- How to reproduce the problem
- For client problems: A copy of the XML configuration data that produces the problem, trace output, event log messages, and RSoP reporting data if available

Contacting Support

If you encounter problems that are not covered in the documentation, contact BeyondTrust technical support.

When contacting technical support, provide the following information:

- Your company name
- Telephone and email address where you can be contacted
- Description of the problem and the steps you have taken to resolve it

You can contact BeyondTrust technical support by email, through the BeyondTrust website, or by telephone. Support is staffed 24 hours per day, seven days per week.

**Telephone** - In the United States, +1 800-234-9072. Outside the United States, +1 818-575-4040.

**Email** - pbd-support@beyondtrust.com

**Web** - To submit a support request:
2. Click Login and log into the BeyondTrust website using the password provided to you by BeyondTrust.
3. After reading the Welcome message, scroll to the top of the BeyondTrust Customer/Partner Portal pane and click Customer Support Center.
4. Scroll down to the Add/View Incidents section and click the + icon.
5. In the View Your Incidents pane, click Add Incident, enter the details requested, and click Submit Incident to file your request for technical support.
Product Overview

In many organizations, higher levels of privileges are often given to ordinary users so that they can run an application or perform mundane system tasks such as mounting a printer or setting the system clock. However, granting such privileges creates significant vulnerability to network security. When credentials are elevated, common users can perform a wide variety of tasks beyond the scope their responsibility and authority.

In a truly secure environment, users are given rights to only the resources they need, and only when they need the resource. Ideally, all users are assigned Least Privileged User Accounts (LUA). This means that they have minimal rights in the overall network context.

Unfortunately, in the Windows® environment, many applications and processes require elevated rights in order to be launched and run.

How PowerBroker Desktops Works

PowerBroker Desktops enables you to create rules (Group Policy items) that define and govern how individual processes and applications are assigned rights. By creating a rule, you determine the specific permissions and privileges assigned to an application. When a user launches the application, the rule is communicated to the client computer as a matter of policy.

The following illustration depicts the role of PowerBroker Desktops within the enterprise as it monitors launch events and adjusts privileges.
In addition to application rules, you can create rules that apply to system tasks and process, as well as to individual users. Using these rules, you might provide access to system clock functions for all users. You might also limit the ability to launch and run a spreadsheet application to users or computers in the Finance organizational unit (OU).

By customizing access in this way, you match security restrictions to the needs of your organization. At the same time, you provide protection to the network while maintaining user productivity.

PowerBroker Desktops communicates privilege configuration within the Windows Group Policy framework. When Group Policy is refreshed, PowerBroker Desktops rules take effect. They are enforced any time the related application or process launches.

The PowerBroker Desktops user interface, running within the Group Policy Management Editor in Windows Server or Windows, displays as shown in the following example:

In this example, the **PowerBroker Desktops** node is selected under **Computer Configuration, Policies, BeyondTrust**. A second **PowerBroker Desktops** node is displayed under **User Configuration, Policies, BeyondTrust**.

Because the **PowerBroker Desktops** node under **Computer Configuration** is selected, the right pane lists rules that were created by the administrator to apply to specific computers. These rules determine how a process or an application is accessed and run on a computer.
PowerBroker Desktops Terminology

PowerBroker Desktops uses terminology specific to its features and functions. It is important to understand some key terms before you start using the product.

These terms include the following:

- **Elevation** - The act of assigning administrator rights to a process or a procedure, such as the launching of an application. Elevation is usually accomplished invisibly (from a user's point of view) and on an as-needed basis. Rules are used to perform elevation. Various parameters assigned to rules determine the scope and limitations of elevation.

- **Process Token** - A process token (sometimes called an access token) is an object that describes the security context of a process or a thread. The information in the token includes the identity and privileges of the user account associated with the process or thread.

  During login, the operating system verifies the user’s password by comparing it to information stored in a security database. If the password is authenticated, the operating system produces a process token. Every process executed on behalf of this user includes a copy of this token.

- **Permissions** - Standard permissions are those that control a broad range of detailed permissions. The most popular permission is Full Control. Full Control enables the user that is granted this set of permissions to do almost anything to the object with which the permissions are associated.

  Other standard permissions include the following: Modify, Read and Execute, Read and Write. Folders have the same standard permissions as files with one additional standard permission called List Folder Contents.

- **Privileges** - These control the access to system-wide resources on a computer, and they can override the permissions that are set on particular objects. Privileges such as adjusting the time, loading and unloading of device drivers, and shutting down the computer are examples of user privileges.

- **Rule Set** - Rules are created in the PowerBroker Desktops snap-in. Multiple rules comprise a rule set. Rules enable you to implement specific configurations for users and for computers.

  Rules are contained in Group Policy Objects (GPOs), which are linked to Active Directory containers such as sites, domains, or organizational units (OUs). Rules enable you to manage user and computer objects.
PowerBroker Desktops Architecture

PowerBroker Desktops provides a kernel-mode security driver that resides on the client computer. This security driver is deployed and installed in a single Windows installer package (.MSI) that also contains the Group Policy client-side extension (CSE) and the Windows Management Instrumentation (WMI) namespace for reporting the Resultant Set of Policy (RSoP), and computer state model data.

Most organizations deploy this MSI by using Group Policy or their preferred software distribution technology.

The security driver monitors process launches on the client computer and checks each launch against the rules communicated to the client through Group Policy. When a rule exists, the security driver intercepts the launch event and modifies the security token for that process according to the instructions contained in the rule.

The benefits of this approach include:

- No secondary accounts are required (unlike “Run As” style solutions).
- Security exposure is not increased.

Applications that need to write to HKEY_CURRENT_USER do not fail because the process still launches under the authenticated user. This enables a common user to perform specific tasks and operations that normally require administrator-level privileges.

For more information about PowerBroker Desktops rules, see the product FAQ in the Knowledge Base. You can access the Knowledge Base by logging into the BeyondTrust website using the password provided to you by BeyondTrust, clicking Customer Support Center, and then clicking the PowerBroker Desktops logo in the Knowledge Base pane.

What You Can Do with PowerBroker Desktops

When you use PowerBroker Desktops to manage application and process security with rules, you can perform application control and modify security associated with the application or process such as permission levels, privileges, and integrity level. You can also configure user messages to require end users to provide credentials or to submit a justification for a request for elevation, and you can customize the messages displayed to end users. You can fine-tune the targeting of a rule to relevant users and computers by using item-level targeting like that available for Group Policy Preferences. You can view and manage audit data and reports about administrator and user rights, rules applied, and application usage.
By using PowerBroker Desktops rules, you can increase or decrease security restrictions for users when they are performing specific Windows tasks or running specific applications. For example, you can:

- Elevate the permission level for restricted users performing a common Windows task or running an application requiring higher privileges.
- Elevate the permission level for restricted users running any applications in a specific folder.
- Reduce the permissions for administrators when using applications such as Internet Explorer and Outlook.
- Elevate all applications from a specific company.
- Elevate a specific version of an application.
- Provide a self-service software installation point for restricted users.
- Enable restricted users to use the Add Hardware wizard or prevent users from using the wizard.
- Enable restricted users to add or remove plug and play hardware or prevent users from adding plug and play hardware.
- Enable restricted users to shut down their computers.
- Enable users to elevate applications on demand.
- Enable users to elevate all applications on a certain CD or DVD.
- Enable certain users to use credentials in UAC dialogs to initiate application launch.

**Use the Management Dashboard to Get Started**

The PowerBroker Desktops management dashboard serves as a friendly starting point from which you can create rules to manage application and process security, manage user messages, generate reports, and perform other PowerBroker Desktops tasks.

The management dashboard has the following sections:

- **Getting Started** - Provides links to online help and other useful information sources.
- **Tools and Wizard** - Provides access to features for auditing and reporting, creating rules and collections, managing user messages, and generating passcodes that an administrator can use to provide authorized users with access to an application.
- **Rule Summary** - Provides summary-level information about the number of rules in use by type. It also provides access to individual rule settings reports and XML reports. Settings reports provide the details of a rule's attributes and permissions. XML reports display the XML coding that represents a rule in the PowerBroker Desktops environment.
For more information, see “Viewing the Management Dashboard,” page 30.
Manage Application and Process Security with Rules

When you use PowerBroker Desktops to manage application and process security with rules, you can target applications and processes; perform application control; modify permissions, privileges, and integrity level for an application; and fine-tune the targeting of a rules.

Target Applications and Processes

PowerBroker Desktops enables you to target applications so that a rule applies only to specific applications. When you create a rule, you select the type of rule to create based on how you want the rule to target applications or processes. You can target:

- Applications or Windows Installer (MSI) packages based on their file path or folder location, or you can target an application regardless of its location.
- A specific version of an application.
- Any application that triggers a UAC prompt.
- Any application that specified by a user.
- All installations initiated through Internet Explorer, specific installations initiated through Internet Explorer, or the installation of ActiveX controls.
- All applications on a specific CD or DVD.

For more information, see “Determining the Type of Rule Needed,” page 32.

Perform Application Control

Prior to version 5.2 of PowerBroker Desktops, the action performed by all rules was to run the targeted application with a custom token for which you specified permissions, privileges, and integrity level in each rule. In version 5.2 and later, most rule types include a choice of actions, and you can use actions to perform application control. You can use either a blacklisting or whitelisting approach to managing the execution of applications and processes. You can also use actions to add or remove Administrator rights when an application is run.

For more information, see “Selecting an Action for Application Control,” page 84.
**Modify Permissions**
You can use a rule to make changes to the permissions of an application or a process when it is run. Permissions are defined by the security groups listed in the process token. With each rule, you can add security groups to or remove security groups from the application’s process token.

The effect is the same as making changes to the end-user’s group memberships, but only for the specified applications.

For more information, see “Modifying Permissions,” page 89.

**Modify Privileges**
You can use a rule to change the privileges of an application or a process. With each rule, you can grant or deny privileges to the application.

The effect is the same as if the privileges were granted or denied to the end-user but only for the specified applications.

This feature is especially useful because Windows grants as standard privileges the ability to **Shut down the system** and **Take ownership of files or other objects**. On some computers, these are not tasks that administrators want users to be able to perform.

For more information, see “Modifying Privileges,” page 91.

**Modify Integrity Level**
You can use a rule to change the integrity level of an application or a process when it is run.

The effect is the same as making changes to the end-user’s integrity level, but only for the specified applications.

For more information, see “Modifying Integrity Level,” page 94.

**Fine-Tune the Targeting of a Rule**
Item-level targeting enables you to restrict an individual rule so that it is applied only to selected users and computers. By using item-level targeting with rules, you can manage a wider variety of users and computers with a smaller number of GPOs.

For example, within a single GPO you can include similar rules customized for selected users and computers, with each targeted rule to apply its settings only to the relevant users or computers.
The New Item menu of the Item-Level Targeting Editor looks like the following:

PowerBroker Desktops provides more than 25 types of targeting items that you can use to fine tune and enhance the application of security configurations to users and computers.

When multiple targeting items are specified, the Item Options menu provides access to boolean operators such as AND/OR and IS/NOT. Using these operators you can conjoin multiple items in a logical expression.

In addition, collections of items can be named and saved. This is helpful when frequently used constraints must be applied repeatedly.

Using item-level targeting, you can accomplish selective rule application such as:
Elevate the security of application X, but only for members of the Finance security group.

You can configure more complex targeting expressions so that a rule is applied only to users or computers with a specific combination of characteristics. For example:

Modify the security of version 3.0.135 of application X, but only for members of the Finance security group when they launch the application on a specific computer.

For more information, see “Targeting Users or Computers with Item-Level Targeting,” page 98.

**Customize and Manage User Messages**

You can use PowerBroker Desktops to require end users to provide credentials or to submit a justification for a request for elevation and to customize the messages displayed to end users.

Alternatively, 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. For example, you could provide access to an application for a support professional who does not have an end-user's credentials available. Using an authorization dialog, the user can send an Authorization Code generated using a public key to a specified email address and gain one-time access to the application by entering a Passcode received from an administrator in response. For information about generating a Passcode, see “Generating a Passcode to Respond to a Message,” page 132.

Using PowerBroker Desktops, you can configure the following types of messages:

- **Application Launch** - A customized message is displayed in a dialog box to end users when they attempt to launch applications for which they lack sufficient privileges. User name, password, and justification can be requested, or one-time access can be authorized by Passcode.

- **Blocked Application** - A customized message is displayed in a dialog box to end users when they attempt to launch a prohibited application. One-time access to the application can be authorized by Passcode.

- **IE Elevation** - Text in the Internet Explorer user interface is customized to indicate when Internet Explorer has been elevated.

- **IE Failure** - A customized message is displayed in a dialog box when an end user with insufficient privileges attempts to install an ActiveX component.

- **On-Demand Elevation** - Customized context menu options are displayed when an end user right-clicks an executable file (EXE) or a Windows Installer package (MSI).
**UAC Prompt Detected** - A customized message precedes the standard User Account Control (UAC) prompt, and the standard UAC prompt can be suppressed.

For more information, see “Managing User Messages,” page 116.

**Back Up Group Policy Objects**

PowerBroker Desktops can create up to three Group Policy Object (GPO) backup files using standard GPO backup procedures. These files contain the rule XML code that defines each rule you have created. You could create a backup file to store in a source control system for version control or to import into a PowerBroker Desktops utility such as PBDeploy.

For more information, see “Backing Up a GPO,” page 152.

**View and Manage Reports**

Using Auditing and Reporting (PBReports) for PowerBroker Desktops, you can view and manage audit data and reports about administrator and user rights, rules applied, and application usage. Usage data is gathered from client computers by using Microsoft Event Forwarding, and SQL Server Reporting Services (SSRS) is used to generate detailed, filterable reports.

The following Reporting Services reports are provided:

- **Auditing and Reporting Dashboard** - Graphical charts of data about the applications most frequently launched, requiring elevation, triggering User Account Control (UAC), launched by Shell rule. Also, charts about ActiveX controls, rules applied, local administrators, and the ratio of administrator users to standard users.
- **ActiveX Details** - Information about installation events for ActiveX controls in Internet Explorer
- **Applications by Path** - Information about all applications under management tracked by launch path
- **Application Path Details** - Increased details about all applications under management tracked by launch path
- **Applications by Hash** - Information about all applications under management tracked by hash code
- **Application Hash Details** - Increased details about all applications under management tracked by hash code
- **Applications by Computer** - Information about application usage on a particular client
- **Shell Rule Executions** - Information about every Shell rule-based application launch
For more information, see “Viewing and Managing Reports,” page 135.
Getting Started with PowerBroker Desktops

PowerBroker Desktops enables you to create rules in the Group Policy Management Editor, part of the Group Policy Management Console (GPMC). Each PowerBroker Desktops rule elevates or reduces the permissions and privileges of a Windows application or process at runtime. A rule can also elevate or reduce the permissions and privileges of an MSI package or an ActiveX control when they launch.

You can create rules by using the Create a Rule Wizard or by using the Properties dialog for a rule. You can also generate rules automatically by using Auditing and Reporting. Rule generation is a practical way to assemble a basic rule set for your organization based on existing application usage. You can then refine this set of rules to meet your specific needs.

For increased targeting granularity, you can use item-level targeting to apply some rules only to selected computers or specific users.

The following sections can help you get started creating and configuring rules to manage security for applications and processes.

Creating or Editing a GPO

You can create a Group Policy Object (GPO) using the Group Policy Management Console (GPMC). You can then use the Group Policy Management Editor to edit the GPO. Within the Group Policy Management Editor, you use the PowerBroker Desktops node to create and edit rules.

Note: For an introduction to Group Policy concepts and terminology, see “Appendix A: Group Policy Primer,” page 170, and the “Glossary,” page 183.

To create or edit a GPO, do the following:

1. Click Start, Control Panel, Administrative Tools, Group Policy Management to open the Group Policy Management Console (GPMC).

   Tip: If the GPMC Is Not Installed

   If you have not installed the GPMC, you can download it for free from http://microsoft.com/downloads. If you are running an older version of Windows Server, you can open the Group Policy Object Editor from Active Directory Users and Computers or from a custom Microsoft Management Console.

2. In the GPMC, click a Forest, expand the list of Domains, and click the domain in which you want to configure PowerBroker Desktops rules.
3. To create a new GPO in which to configure PowerBroker Desktops rules:
   a. Right-click Group Policy Objects and select New.

   ![Image of Group Policy Management window with New option highlighted]

   b. Specify a name for the GPO and click OK.

   ![Image of New GPO dialog box]

4. To add PowerBroker Desktops rules to an existing GPO or to change rules in an existing GPO, click Group Policy Objects to display the list of GPOs.

5. Right-click the GPO in which you want to configure PowerBroker Desktops rules and click Edit to launch the Group Policy Management Editor.
Note: To configure a local GPO on your computer rather than a domain GPO, from a Windows command prompt run `gpedit.msc` to open the Local Group Policy Editor. If you want to use Group Policy to manage software installation, you must use a domain GPO rather than the local GPO.

To display the PowerBroker Desktops management dashboard, see “Viewing the Management Dashboard,” page 30. If you are creating new PowerBroker Desktops rules, see “Planning a Rule,” page 32. If you are modifying an existing rule, see “Creating or Editing a Rule with the Properties Dialog,” page 47.

**Viewing the Management Dashboard**

The PowerBroker Desktops management dashboard serves as a starting point from which you can create rules to manage application and process security, manage user messages, generate reports, and perform other tasks.

To use the management dashboard:

1. In the Group Policy Management Editor, click either **BeyondTrust** node. The management dashboard is displayed in the details pane of the Group Policy Management Editor.
2. The management dashboard is organized into the following sections. Click a link in the dashboard to access a resource.
   - **Getting Started** - Provides links to online help and other useful information sources.
   - **Tools and Wizard** - Provides access to features for auditing and reporting, creating rules and collections, managing user messages, and generating passcodes that an administrator can use to provide authorized users with access to an application.
For more information, see the following:

- “Viewing and Managing Reports,” page 135
- “Creating a Rule with the Wizard,” page 40
- “Managing Multiple Rules with a Collection,” page 107
- “Managing User Messages,” page 116
- “Generating a Passcode to Respond to a Message,” page 132

For information about modifying an existing rule, see “Creating or Editing a Rule with the Properties Dialog,” page 47.

- **Rule Summary** - Provides summary-level information about the number of rules in use by type. It also provides access to individual rule settings reports and XML reports. Settings reports provide the details of a rule’s attributes and permissions. XML reports display the XML coding that represents a rule in the PowerBroker Desktops environment. For more information, see “Viewing a Settings Report,” page 50.

The following is an excerpt from the management dashboard.
Planning a Rule

Before you create a new rule, you should determine the type of rule needed, determine the appropriate action for the rule to support your approach to application control, and choose a rule creation method appropriate to your circumstances.

Determining the Type of Rule Needed

PowerBroker Desktops enables you to create rules that target applications by using various methods. The following tables provide guidance about selecting the type of rule applicable to a particular situation.

Table 1. Selecting a Rule Type for a Security Need

<table>
<thead>
<tr>
<th>To modify permissions and privileges of…</th>
<th>Use a…</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Windows process</td>
<td>Path rule</td>
</tr>
<tr>
<td>A program in a specific location</td>
<td>Path rule</td>
</tr>
<tr>
<td>A specific program regardless of location</td>
<td>Hash rule</td>
</tr>
<tr>
<td>All applications published by a specific company</td>
<td>Publisher rule</td>
</tr>
<tr>
<td>All programs in a specific folder</td>
<td>Folder rule</td>
</tr>
<tr>
<td>A specific version of an application</td>
<td>Publisher rule</td>
</tr>
<tr>
<td>An MSI package in a specific location</td>
<td>MSI Path rule</td>
</tr>
<tr>
<td>All MSI packages in a specific folder</td>
<td>MSI Folder rule</td>
</tr>
<tr>
<td>All installations initiated by Internet Explorer</td>
<td>ActiveX rule</td>
</tr>
<tr>
<td>Specific installations initiated by Internet Explorer</td>
<td>ActiveX rule</td>
</tr>
<tr>
<td>Installation of all ActiveX controls</td>
<td>ActiveX rule</td>
</tr>
<tr>
<td>Installation of specific ActiveX controls</td>
<td>ActiveX rule</td>
</tr>
<tr>
<td>All applications on a certain CD or DVD</td>
<td>CD/DVD rule</td>
</tr>
<tr>
<td>Any application that a user specifies</td>
<td>Shell rule</td>
</tr>
<tr>
<td>An application that triggers a UAC prompt</td>
<td>UAC rule</td>
</tr>
</tbody>
</table>
The following table provides guidance about the type of rule to select to address various user management scenarios.

**Table 2. Selecting a Rule Type for a Management Scenario**

<table>
<thead>
<tr>
<th>I want to…</th>
<th>Use a…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elevate the permission level for restricted users performing a common Windows task or running an application requiring higher privileges</td>
<td>Path rule or Hash rule</td>
</tr>
<tr>
<td>Elevate the permission level for restricted users running any applications in a specific folder</td>
<td>Folder rule</td>
</tr>
<tr>
<td>Reduce the permissions for administrators when using applications such as Internet Explorer and Outlook</td>
<td>Path rule or Hash rule</td>
</tr>
<tr>
<td>Elevate all applications from a specific company</td>
<td>Publisher rule</td>
</tr>
<tr>
<td>Elevate a specific version of an application</td>
<td>Publisher rule</td>
</tr>
<tr>
<td>Provide a self-service software installation point for restricted users</td>
<td>Folder rule for executable and MSI Folder rule for MSI packages</td>
</tr>
<tr>
<td>Enable restricted users to use the Add Hardware wizard or prevent users from using the wizard</td>
<td>Path rule</td>
</tr>
<tr>
<td>Enable restricted users to add or remove plug and play hardware or prevent users from adding plug and play hardware</td>
<td>Path rule</td>
</tr>
<tr>
<td>Enable restricted users to shut down their computers</td>
<td>Path rule</td>
</tr>
<tr>
<td>Enable users to elevate applications on demand</td>
<td>Shell rule</td>
</tr>
<tr>
<td>Enable users to elevate all applications on a certain CD or DVD</td>
<td>CD/DVD rule</td>
</tr>
<tr>
<td>Enable certain users to use credentials in UAC dialogs to initiate application launch</td>
<td>UAC rule</td>
</tr>
</tbody>
</table>
**Determining an Application Control Approach**

Prior to version 5.2 of PowerBroker Desktops, the action performed by all rules was to run the targeted application with a custom token for which you specified permissions, privileges, and integrity level in each rule. In version 5.2 and later, most types of rules have a choice of actions available, and you can use actions to perform application control.

You can use actions in concert to achieve a whitelisting or blacklisting approach to application control. You can see a demonstration of application control using PowerBroker Desktops. For more information about specific actions, see “Selecting an Action for Application Control,” page 84.

**Note:** Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. You must arrange rules according to the intended order of processing so that rules with an action of Run application(s) with custom token, Add Admin rights to application(s), or Remove Admin rights from application(s), can take precedence over rules with other actions, and so that rules with an action of Run application(s) with no change can take precedence over rules with an action of Deny execution of application(s). For more information, see “Arranging the Order of Rules,” page 104.

**Note:** If you are using PowerBroker Desktops rules in multiple GPOs and those rules have the potential to impact the same application, you must also arrange the GPOs according to the intended order of processing. GPOs are processed sequentially from highest precedence number to lowest. If two GPOs each contain a PowerBroker Desktops rule that configures security for the same application, both rules take effect in sequence. The rule in the GPO with the lowest precedence number wins because it is the last to be applied.

**Blacklisting**

When using a blacklisting approach for application control, all applications are permitted unless you block them. You run most applications with a custom token or with no associated rule, and you create rules to deny the execution of applications that you specify.

To implement a blacklisting approach to application control:

- For applications and processes that you want to permit, you do not have to create rules. If you want to permit an application or process but also want to configure its security by using a rule, select one of the following
actions for the rule:

- **Run application(s) with custom token**
- **Add Admin rights to application(s)**
- **Remove Admin rights from application(s)**

- For applications and processes that you want to prohibit, create a rule and select an action of **Deny execution of application(s)**.

---

**Whitelisting**

When using a whitelisting approach for application control, all applications are blocked from running except those that you permit.

⚠️ **Warning: Do not block the operating system**

If you create a rule to block all applications without first creating a rule that allows the operating system to run, computers to which the rule applies may not boot properly. It is recommended that you first create a passive rule for C:\Windows or %systemroot% before you create your blocking rule.

After you create your blocking rule, you must position it so that it will only be executed if no other rule is applicable. Move it to the lowest order number within the GPO. If you are using multiple GPOs, ensure that the GPO containing your blocking rule has the highest precedence.

To implement a whitelisting approach to application control:

- **Required initial configuration** - Before you create a rule to block all applications from running, you must create rules that permit the operating system and other critical software to run. After those rules are in place, you create a rule to block all other applications from running except those permitted by rules. For details, see "Initial Configuration
for Whitelisting" following this section.

- For applications and processes that you want to prohibit, you do not have to create additional rules.
- For applications and processes that you want to permit, create a rule and select one of the following actions:
  - Run application(s) with custom token
  - Add Admin rights to application(s)
  - Remove Admin rights from application(s)
  - Run application(s) with no change (passive)
    Note: For rules with an action of Run application(s) with no change (passive), the Apply rule to all processes launched by the targeted application check box has no effect. You must specify child processes separately for whitelisting.

**Initial Configuration for Whitelisting**

You must perform the following initial configuration to implement a whitelisting approach to application control:

1. To ensure that the operating system can run, create a Path rule that includes the following:
   - Path: C:\Windows or %systemroot%
   - Action: Run application(s) with no change (passive)
   - Select the following option: Apply rule to all programs in all subfolders of the specified folder

2. Optional. To ensure that applications installed in the C:\Program Files* folder can run, create a Path rule that includes the following:
   - Path: C:\Program Files*
   - Action: Run application(s) with no change (passive)
   - Select the following option: Apply rule to all programs in all subfolders of the specified folder

3. To prevent unapproved applications from running, create a Path rule that includes the following:
   - Path: *
   - Action: Deny execution of application(s)
   - Select the following options:
     - Apply rule to all programs in all subfolders of the specified folder
     - Apply rule to all processes launched by the targeted application
Position this blocking rule so that it has the lowest order number in the GPO. If you are using multiple GPOs, ensure that the GPO containing this rule has the highest precedence. It should be executed only if no other rule is applicable.

Using Wildcards in Rule Properties

Wildcard characters are supported in some text input fields in the rule Properties dialog and Create a Rule Wizard. The asterisk (*) wildcard can replace one or more characters in a string. The question mark (?) wildcard can replace a single character in a string.

For example, MyComputer? matches MyComputer9 and MyComputerW, but not MyComputer09 or MyComputer. When using the multi-character wildcard, MyC*mputer matches MyComputer, MyCxmputer, and MyCxxxmputer.

The following types of rules support wildcards:

- **Publisher** - In the Product name, File name, or Product version fields
- **Shell** - In the Arguments field
- **Path** - In the Path and Arguments fields
- **Hash** - In the Arguments field
- **Folder** - In the Folder field
- **MSI Path** - In the Package field
- **MSI Folder** - In the Folder field
- **UAC** - In the Path field

For more information about these fields, see the section for the type of rule under “Targeting Applications or Processes,” page 54.

Variables can also be used in some rule properties. For information, see “Using Variables in Rule Properties,” page 111.
**Wildcard Cautions and Examples**

The net effect of a wildcard is to make a rule more generic. However, this might not always be in the best interest of the rule. For example, when using wildcards for path rules, it is wise to make the rule as specific possible to keep the rule secure. Consider the wildcard placement in the following example:

```
http://*example.com/*
```

The * placement makes this URL very broad and thus potentially subject to abuse.

If the site is not a trusted site, a better use of the wildcard is exemplified by the following:

```
http://example.com/printers/downloads/*
```

This placement narrows the scope of the rule. In this example, hard-coding as much as possible of the actual path or URL prevents the standard user from downloading unapproved files from unforeseen locations.

Another typical use for a wildcard is in a setting in which a naming convention is used to represent hardware such as servers or computers. In this case, a wildcard can be substituted for certain elements of the name. For example:

```
\example_accounting1
\example_accounting2
\example_sales
\example_engineering
\example_marketing
```

All these servers can be addressed by the following:

```
\example*
```

As these examples illustrate, wildcards must be used with caution, and only after evaluating the all their potential effects on the rule.

**Wildcards and Subfolders**

A check box setting available in many rule types can change rule behavior when a wildcard is used. This setting allows a rule to traverse a directory structure. The setting is:

**Apply rule to all programs in all subfolders of the specified folder.**

When this setting is enabled, and a wildcard is used, a rule will behave as described in the following table.

For this example, the following statement is used as the rule path statement or argument: `c:\Folder1\*\my.exe`. This statement uses a wildcard to represent a folder.
Table 3. Rule Behavior for the wildcard statement: C:\Folder1\*\my.exe

<table>
<thead>
<tr>
<th>Subfolder Setting is Enabled</th>
<th>Executable Path</th>
<th>Executable File is Elevated</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>c:\Folder1\my.exe</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>C:\Folder1\my.exe</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>C:\Folder1\Folder2\my.exe</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>C:\Folder1\Folder2\my.exe</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>C:\Folder1\Folder2\Folder3\my.exe</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>C:\Folder1\Folder2\Folder3\my.exe</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The table illustrates that when the subfolder setting is enabled, the rule will traverse the subdirectory structure looking for a match until it finds one.

In addition, if the * wildcard is substituted for the executable name (*.exe), all executable files in the directory structure will have the rule applied. This technique is often used to apply a rule to multiple applications stored in a hierarchical directory structure.

Choosing a Rule Creation Method

After you have created a GPO, you must edit the GPO to create and apply PowerBroker Desktops rules.

You can create rules in the following ways:

- **Using the Wizard** - The Create a Rule Wizard can guide you step-by-step through the creation and configuration of a new rule. The wizard is a good choice if you are new to the concepts of rule creation and application elevation. For more information, see “Creating a Rule with the Wizard,” page 40.

- **Using the Reporting Console** - You can use the PowerBroker Desktops Reporting Console, which analyzes client computer application usage, to generate rules based on that analysis. The Reporting Console is ideal if you are familiar with rules and elevation and want a way to generate rules based on application usage by end-users. Auditing and Reporting can inventory the applications in use on targeted client computers and analyze the permissions required by each. You can generate rules based on end-user needs for specific applications. For more information, see “Generating Rules with the Reporting Console,” page 43.
Using the Properties dialog - If you have disabled the wizard and are creating a new rule or if you are editing an existing rule, you can use the Properties tabbed dialog to configure a rule. To create a rule using the rule properties dialog, you must disable the Create a Rule Wizard using the button on the management dashboard. Creating a rule by using the Properties dialog allows you to configure every rule property. For more information, see “Creating or Editing a Rule with the Properties Dialog,” page 47.

Creating a Rule with the Wizard

If you have a basic knowledge of rule types, the rule wizard provides an easy way to build a rule. The wizard guides you through all the steps that are required to configure and name a rule. Each wizard page corresponds to a tab in the rule property sheet. Helpful text prompts assist you in making configuration choices and selections.

The wizard can be enabled or disabled on the management dashboard using a button. When enabled, the wizard starts any time Create New Rule is selected. When the wizard is disabled, clicking Create New Rule opens a rule properties dialog.

Note: Before you create a rule, it is recommended that you consider which type of rule is appropriate to the situation and what approach you want to use for application control. For more information, see “Planning a Rule,” page 32.

To create a rule using the rule wizard, do the following:
1. Open the PowerBroker Desktops dashboard by clicking a BeyondTrust node in the Group Policy Management Editor.
2. In the Tools and Wizard section of the dashboard, click Create a New Rule.
Note: If the wizard is turned off, a Properties dialog opens. Close the Properties dialog, click the Enable Wizard button to the right of the Create a New Rule link on the management dashboard, and then click Create a New Rule again.

3. In the wizard, if the Before you begin page is displayed, review its content and click Next to display the Rule type page.

4. On the Rule type page, select the type of rule you want to use to target an application or process. For more information about rule types, see “Determining the Type of Rule Needed,” page 32.

5. Follow the prompts on the subsequent pages to configure the rule. For more information about the concepts, see the following topics about configuring properties of a rule using the Properties dialog:
   - “Targeting Applications or Processes,” page 54
   - “Selecting an Action for Application Control,” page 84
   - “Configuring Common Options,” page 86
   - To specify a previously-configured message to be displayed to users to whom this rule is applied, select a Message. You can use a message to require users to provide credentials or to enter a justification for an elevation request. You can configure messages by right-clicking the PowerBroker Desktops node in the Group Policy Management Editor and then clicking Manage User Messages. For more information, see “Managing User Messages,” page 116.
   - “Configuring Token Security,” page 88
   - “Configuring Execution Options,” page 96
   - “Targeting Users or Computers with Item-Level Targeting,” page 98
6. On the last page of the wizard, provide a name for the rule, provide a description (optional), and click **Create**.
   
The new rule is added to the bottom of the rule list and you are prompted to create another rule or to exit the wizard.

7. In the Group Policy Management Editor, change the order of this rule as needed to support application control. Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. Rules with an action of **Custom Token**, **Add Admin Token**, or **Remove Admin Token** should have the highest order numbers and rules with an action of **Deny Execution** should have the lowest order numbers. For more information, see “Arranging the Order of Rules,” page 104.

After you have created a rule, you can edit it by clicking the **PowerBroker Desktops** node in the Group Policy Management Editor, right-clicking the rule, and clicking **Properties**. For more information, see “Creating or Editing a Rule with the Properties Dialog,” page 47.
Generating Rules with the Reporting Console

Manually creating rules to control application access in a large organization is a daunting task. The PowerBroker Desktops Reporting Console uses Microsoft Event Forwarding to collect privilege-related event log data from computers running the PowerBroker Desktops client software into a SQL Server or SQL Server Express database. This data includes information about the applications being used, the privileges they require, and how they are launched, as well as information about which users have administrator privileges.

Using the Reporting Console, you can sort and filter this data into useful reports and generate PowerBroker Desktops rules for applications based on user needs for privilege elevation.

Tip: Configuring auditing and reporting

Before you can use the Reporting Console, you must have a SQL Server or SQL Server Express database installed in your environment, and you must configure auditing and reporting for PowerBroker Desktops. See the PowerBroker Desktops Installation Guide for more information.
You can use the Reporting Console to individually generate rules, or you can generate multiple rules for specific types of applications. You can also flag applications for inclusion in reports.

**Generating Rules and Creating Reports**

To generate rules for applications by using the Reporting Console:

1. In the Group Policy Management Console (GPMC), edit a Group Policy Object (GPO).
2. In the Group Policy Management Editor, open the PowerBroker Desktops management dashboard by clicking either of the BeyondTrust nodes.
3. In the Tools & Wizard section of the dashboard, click Reporting Console.
4. On first use: In the PowerBroker Desktops Reporting Console, click Options. If the PBDatabase Connection field does not already contain the path to the SQL Server or SQL Server Express database that you configured to collect event data, then specify the path, select an Authentication type, specify credentials if needed, and click OK.

   Tip: Troubleshooting the Configuration of Reporting

   If no events are listed in the Reporting Console, see the PowerBroker Desktops Installation Guide for information about how to configure auditing and reporting.

5. For initial, individual generation of rules, either of the following options is recommended as a starting point. However, you can also filter the list of events by user, computer, group, publisher, application, event, rule type, or date and time as appropriate to help you identify relevant events for your organization.

   - To find applications that require privileges, in the Application Filtering Options box, select Show Applications Requiring Privileges. If that option is not listed, then no such events have been detected.

   - To find applications that require elevated privileges, in the Filter Options box, under Event, select Apps Requiring Elevation. If that option is not listed, then no such events have been detected.

6. Click an event and view the details pane below the table for more information about the event.
7. If you want to flag specific applications to be included in a filtered report of flagged applications:
   a. Right-click an application event and select Flag Application. (This option is not available for some event types.)
   b. Repeat for each event that you want to include in the report.
c. In the **Application Filter Options** box, select **Show only Flagged Applications**.

d. Click **Create Report**.

8. When you find an event for an application for which you would like to generate a rule to provide elevated privileges, right-click the event and click one of the following options. Some options are not available for some event types or file types.

   – **Generate Publisher Rule** - Generate a rule to provide elevated privileges for the selected application identified by its digital signature (EXE, MSI, and MSP files only).

   – **Generate Path Rule** - Generate a rule to provide elevated privileges for the selected application identified by its path.

   – **Generate Hash Rule** - Generate a rule to provide elevated privileges for the selected application identified by its hash code.

9. In the Generate Rule window, select the entire text of the rule and click **Copy To Clipboard**.

10. In the Group Policy Management Editor under either **Computer Configuration** or **User Configuration**, expand the **BeyondTrust** node.

11. Right-click the **PowerBroker Desktops** node and click **Paste**. The rule is displayed in the details pane.

   For information about making changes to a rule, see “Creating or Editing a Rule with the Properties Dialog,” page 47.

**Generating Multiple Rules for a Type of Application**

To generate multiple rules for applications of a particular type by using the Reporting Console:

1. In the Group Policy Management Console (GPMC), edit a Group Policy Object (GPO).

2. In the Group Policy Management Editor, open the PowerBroker Desktops management dashboard by clicking either of the **BeyondTrust** nodes.

3. In the Tools & Wizard section of the dashboard, click **Reporting Console**.

4. On first use: In the PowerBroker Desktops Reporting Console, click **Options**. If the **PBDatabase Connection** field does not already contain the path to the SQL Server or SQL Server Express database that you configured to collect event data, then specify the path, select an **Authentication** type, specify credentials if needed, and click **OK**.
Tip: Troubleshooting the Configuration of Reporting

If no events are listed in the Reporting Console, see the PowerBroker Desktops Installation Guide for information about how to configure auditing and reporting.

5. In the Application Filtering Options box, select Filter Applications for Multiple Rule Creation.
6. Select a category of applications by which to filter the event data:
   - ActiveX Controls
   - Denied Applications - Applications denied execution by rules
   - MsiExec.exe - Windows Installer packages
   - MMC.exe - Microsoft Management Console items
   - Rundll32.exe - Control Panel items
   - All Other Applications - All applications except ActiveX controls, applications denied execution by rules, Windows Installer packages, Microsoft Management Console items, and Control Panel items.

7. Review the events. You can click an individual event to display more information about it in the details pane below the table.
8. For the application category that you selected, select all of the applications for which you want to create rules. You can use the Shift key or the Ctrl key to select multiple applications.
9. Right-click the selected applications and click one of the following options. Some options are not available for some application types.
   - Generate Publisher Rule - For each application, generate a rule to provide elevated privileges for the selected application identified by its digital signature (EXE, MSI, and MSP files only).
   - Generate Path Rule - For each application, generate a rule to provide elevated privileges for the selected application identified by its path.
   - Generate Hash Rule - For each application, generate a rule to provide elevated privileges for the selected application identified by its hash code.

10. In the Generate Rule window, select the entire text and click Copy To Clipboard.
11. In the Group Policy Management Editor under either Computer Configuration or User Configuration, expand the BeyondTrust node.
12. Right-click the PowerBroker Desktops node and click Paste. The rules are displayed in the details pane.
For information about making changes to a rule, see “Creating or Editing a Rule with the Properties Dialog,” page 47.

Creating or Editing a Rule with the Properties Dialog

If you have disabled the Create a Rule Wizard and are creating a new rule or if you are editing an existing rule, you can use the Properties tabbed dialog to configure the rule. Creating a rule in this way allows you to configure every rule property.

Tip: Before You Begin

Before you begin, see the following:

- “Creating or Editing a GPO,” page 28
- “Viewing the Management Dashboard,” page 30
- “Planning a Rule,” page 32

To create or modify a rule, do the following:

1. If creating a new rule, on the management dashboard if the **Disable Wizard** button is displayed to the right of the **Create a New Rule** link, click the button to disable the wizard.

2. In the Group Policy Management Editor, do one of the following:
   - If applying this rule to selected computers, click **Computer Configuration, Policies, BeyondTrust, PowerBroker Desktops**.
   - If applying this rule to selected users, click **User Configuration, Policies, BeyondTrust, PowerBroker Desktops**.

3. If creating a new rule, right-click the **PowerBroker Desktops** node and select **Create New Rule**.
**Note:** When the wizard is disabled, clicking **Create a New Rule** on the management dashboard also opens a **Properties** dialog box for a new rule.

4. If modifying an existing rule, right-click the rule to be edited and select **Properties**.

5. On the **Application** tab, select a rule type for the rule and configure options specific to the rule type to target applications or processes. For more information, see “**Targeting Applications or Processes,**” page 54.

6. Select an **Action** for application control or to add or remove Administrator rights. For more information, see “**Selecting an Action for Application Control,**” page 84.

7. Optional. On the **Application** and **Options** tabs, select any appropriate check boxes for restricting or extending the circumstances under which the rule is applied. For more information, see “**Configuring Common Options,**” page 86.
8. Optional. To specify a previously-configured message to be displayed to users to whom this rule is applied, select a Message. You can use a message to require users to provide credentials or to enter a justification for an elevation request. You can configure messages by right-clicking the PowerBroker Desktops node in the Group Policy Management Editor and then clicking Manage User Messages. For more information, see “Managing User Messages,” page 116.

9. Optional. To alter the permissions, privileges, process security, or integrity level with which the application or process is run, click the Token tab and configure options. These options are available only if the action selected is Run application(s) with custom token. Otherwise, the token is pre-configured. For more information, see the following:
   – “Modifying Permissions,” page 89
   – “Modifying Privileges,” page 91
   – “Modifying Process Security,” page 93
   – “Modifying Integrity Level,” page 94

10. Optional. To apply the rule only a limited number of times, only during a specified timeframe, or only under specific network conditions, click the Options tab and configure Execution options. For more information, see “Configuring Execution Options,” page 96.

11. Optional. To fine-tune the targeting of the rule, select the Item-Level Targeting check box on the Application tab and click Targeting. Configure targeting items so that the rule is applied only to appropriate users, computers, or groups. For more information, see “Targeting Users or Computers with Item-Level Targeting,” page 98.

12. Optional. In the Rule Description field on the Application tab, enter an explanation of the purpose of the rule and any details that would be helpful to administrators updating the rule or configuring related rules.

13. Click OK to save and close the rule.

14. In the Group Policy Management Editor, change the order of this rule as needed to support application control. Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. Rules with an action of Custom Token, Add Admin Token, or Remove Admin Token should have the highest order numbers and rules with an action of Deny Execution should have the lowest order numbers. For more information, see “Arranging the Order of Rules,” page 104.

Tip: Copying and Pasting a Rule
You can copy and paste (or drag and drop) a rule in the Group Policy Management Editor to create a duplicate rule that you can modify.
Changing the Name of a Rule

You can change the name of a rule without affecting the policy settings within it. To change the name, right-click the rule, select Rename, and enter a new name.

Viewing a Settings Report

PowerBroker Desktops includes built-in reporting about rules within a Group Policy Object (GPO).

The following types of reports are available:

- **Settings Report** - A Settings report is an easy-to-read, HTML-based report that documents all the configuration parameters of the selected rules or all rules. Rules are presented by type (Path, Hash, and so forth) and are listed in the order in which they appear in the application security file. You can use a Settings report to gain an overview of how a rule is configured and the effect the rule has on its target application or process.

- **XML Report** - An XML report provides the actual XML notation that represents the selected rules or all rules. This notation specifies all the configuration parameters of a rule. Rules are presented by type (Path, Hash, and so forth) and are listed in the order in which they appear in the application security file. You can use the XML report to view the internal operation of a rule and to understand how it interacts with its target application.

Note: HTML-based settings reports do not include disabled items. XML settings reports include all items.
The following is an example of an HTML-based settings report:

![Settings Report](image)

There are several points in PowerBroker Desktops from which you can display a settings report.

To display a settings report for a rule by using the Management Dashboard:

1. In the Group Policy Management Editor, click either **BeyondTrust** node to display the Management Dashboard.
2. In the **Rule Summary** section of the Management Dashboard, click the **Settings Report** or **XML Report** icon in the row for the rule for which you want to view a report.

To display a settings report for one or more rules by using the Group Policy Management Editor toolbar:

1. In the Group Policy Management Editor, expand either **BeyondTrust** node and click the **PowerBroker Desktops** node.
2. Optional. In the PowerBroker Desktops pane, you can select specific rules to limit the report to those rules.
3. In the Group Policy Management Editor toolbar, click the **Display a settings report** icon or the **Display the XML data** icon to display a report.
To display a settings report for all rules and policy settings in a GPO:

1. In the Group Policy Management Console (GPMC), within a domain in a forest, expand the Group Policy Objects collection and click the GPO for which you want to display a report.
2. In the details pane, click the Settings tab to display an HTML-based settings report for the GPO.

To view and manage audit data and reports about administrator and user rights, rules applied, and application usage, use Auditing and Reporting (PBReports) for PowerBroker Desktops. For information, see “Viewing and Managing Reports,” page 135.

**Disabling or Enabling a Rule**

You can disable a rule to remove it from client-side processing without removing its configuration data from the Group Policy Object (GPO). A disabled rule is ignored by the client computer. You can enable a rule later to reactivate it on client computers.

The revised state of the rule takes effect during the next Group Policy update.

To disable or enable a rule, do the following:

- To disable a rule, select the rule in the Group Policy Management Editor and click the Disable button on the toolbar.
- To enable a rule, select the rule in the Group Policy Management Editor and click the Enable button on the toolbar.

**Working Offline**

If you want to make changes to rules without allowing client-side processing of rules until your changes are complete, you can temporarily disable the PowerBroker Desktops node under either Computer Configuration or User Configuration. This will prevent client-side processing of rules in that extension in a particular GPO. When your changes are complete, re-enable the node.
Effects of Disabling Rules or Extensions

If all PowerBroker Desktops rules for either for user or computer policy are disabled in a given GPO, the corresponding client-side extension (CSE) is still run for that GPO in the user or computer context as appropriate. To prevent PowerBroker Desktops from executing, you must either disable the extension's root node or delete all rules in that extension. If no GPOs contain rules for a given CSE, it will not be run on client computers.

If the PowerBroker Desktops extension contains no rules and is disabled, its settings file is deleted from the GPO. The next time the GPO is opened, the extension icon will not be dimmed because there is no settings file to store that state. The extension is reset to the state that it was in when first created. Removing the settings file removes it from the SYSVOL replication.

Note: PowerBroker Desktops HTML-based settings reports do not include disabled items. XML settings reports include all items.
Targeting Applications or Processes

PowerBroker Desktops enables you to target applications or processes so that a rule applies only to specific applications or processes. When you create a rule, you select the type of rule to create based on how you want the rule to target applications or processes.

Tip: Choosing the Type of Rule
For information about how to choose the appropriate type of rule, see “Determining the Type of Rule Needed,” page 32.

Targeting by Location (Path Rule)

To target an application or process based on its location so that you can modify its permissions or privileges when it is run, do the following:

Note: Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the Application tab in the Properties dialog, select Path rule.
2. Enter a path or click to select a process or file. You can browse to operating system specific templates for a variety of Windows processes, such as Internet Options or Add Hardware.

3. Select one of the following:
   - A process running on your computer
   - A standard Windows process, such as Add or Remove Programs or Display; select the specific Windows version (and in some cases the service pack) and whether to target the Control Panel, Desktop, or Task Bar process.
   - An application
   - An executable file; click Select a file to navigate to an executable file, either a local file or a file on a network share path

   It is recommended that you create rules based on network share paths using the fully qualified UNC paths, such as \\MyServer\MyFolder\MyApp.msi. If necessary, mapped drives may be used. When you create a rule based on a mapped drive, select Allow use of mapped drive letter in path on the Options tab.

   Note: Because a limited user has the ability to change a mapped drive, selecting this option presents a security risk because it can enable the user to elevate an unintended application.
Tip: Default Security Settings

If the Default Security Settings dialog opens, you can click Yes to automatically populate the permissions and privileges needed for the task. This is recommended to simplify identification of these permissions and privileges even if your intention is to restrict them. You can modify these security settings when you configure options on the Permissions and Privileges tabs.

4. Optional. If you are planning to select Run application(s) with custom token as the action for the rule, you can restrict the targeting of the application by specifying Arguments:
   - To target this application only if specific command line arguments are used when the application is launched, enter the Arguments. This field is not case-sensitive. Depending on your Path selection, the field may be automatically populated.
   - To target this application regardless of any command line arguments specified when the application is launched, leave the Arguments field blank.

Tip: Using Variables, Wildcards, and Partial Commands

You can use variables and wildcards in the Path and Arguments fields, and you can use a partial command in the Arguments field.

A partial command is considered a match as long as each character from left to right matches the beginning of the actual process command.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press F3.

For more information, see the following:
   - “Using Variables in Rule Properties,” page 111
   - “Using Wildcards in Rule Properties,” page 37

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.

Path rules can be used in creative ways to target a variety of objects other than applications. For examples that demonstrate how the Path rule can be applied to scripts, batch files, and registry operations, see the sections that follow.
Example: Elevate IE for a Website

You can use a Path rule to elevate Internet Explorer (IE) when the users browse to a specific website. This functionality is available only for the 32-bit versions of IE 7, 8, and 9.

To elevate IE for a specific website, create a Path rule with the following properties:

- **Path** - Full path to the iexplore.exe file
- **Arguments** - URL of website to be elevated
- **Action** - Add Admin rights to application(s)

When the user browses to the specified website, a second instance of IE opens in a new window with elevated permissions, and the user is presented with the option to close the first instance. To indicate that IE is running in an elevated state, the title bar in the new window includes the text **BT ELEVATED** and the status bar includes the text **BeyondTrust PowerBroker Desktops Rule Applied - Internet Explorer Elevated.** For information about how you can customize this text by using a message, see “Customizing the Appearance of Internet Explorer When Elevated (IE Elevation),” page 123.

If the user browses from one website to another, the rule is not reapplied. Another rule that includes the second URL is required for any additional websites.

If multiple IE elevation Path rules are required, make sure that permissions, privileges, and integrity level are consistent for all rules. You can do so by selecting the action **Add Admin rights to the application(s)**, which configures these settings automatically.
The following figure shows a typical IE elevation Path rule Properties dialog:

![Elevate IE for Corp Website Rule Properties](image)

**Note:** Elevation of Internet Explorer 9 - Elevation is not as obvious in IE 9 as elevation in other versions. In a default IE 9 installation, the status bar is hidden and the only elevation indicator is **BT ELEVATED** on the page tab. To enable the status bar, a user can right-click in a blank area to the right of the new tab button and then select **Status Bar**. You can configure many features of IE by using Administrative Template settings or preference items.

**Example: Elevate a Visual Basic Script**

To elevate a script, create a rule to point to the scripting host. In the arguments field, target the specific script you would like to elevate to prevent the user from elevating any script.
The following figure shows a Path rule that elevates a script:

![Path rule diagram]

Taking another approach, you can enter `WindowsServer\Netlogon` in the Path field without a file specified, or you can use a Folder rule. This approach elevates all scripts in the folder.

**Example: Elevate a Registry Merge**

To elevate a registry merge, add the path to `regedit.exe`. In the arguments field, scroll down to the registry file you wish to elevate as shown in the following example:

![Registry merge rule diagram]
The elevation of the *.reg and script files are targeted to the item in the arguments field, the user cannot self elevate any script or *.reg file on their own when an argument is present.

**Example: Elevate a Batch File**

A batch file is actually an application and can be treated as one with regard to elevation. As a result, you can elevate a batch file by specifying the path to (or hash of) the batch file as shown in the following example:

![Image of MyBatchFileRule Properties](image)

**Warning: Protect Elevated Batch Files**

If you elevate a batch file, it is strongly recommended that you take measures to protect the batch file from being edited so that it cannot be used to compromise your organization’s security.
Targeting by Signature (Publisher Rule)

Use the Publisher rule to target a digitally signed file by any element of its digital signature.

Note: Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

Note: As of V5.0, the Publisher rule replaced the Certificate rule. Existing Certificate rules are brought forward during an upgrade. However, to update these Certificate rules to Publisher rules, you must open one Certificate rule in version 5.x and then save it. After you do this, any additional version 4.x Certificate rules are updated to Publisher rules.

Signed files can include executable files, MSI files, and MSP files. Signature elements can include the name of publisher (company), the application name, the file version number, the date of release, and more.
After you have selected a signed file to target, the Publisher rule configuration dialog looks similar to the following:

Use the slider control to add items to the rule or enable Use custom values and enter items directly in the input fields.

**Target by Publisher Only**

Targeting the Publisher element of a signed file has several advantages. The file can move to any location and the rule will still apply. In addition, the file can be updated to a newer version and still be managed by the same rule.

To target a file by the Publisher element of its digital signature, do the following:

1. On the Application tab in the Properties dialog, select Publisher rule.
2. Select a signed file to target. You can select either of the following:
   - A process running on your computer (providing it is signed)
   - A file. (Use the Browse button to locate the file.)
3. Select the file. The name of the publisher is displayed in the Publisher text box.

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Target by Any Digital Signature Element

You can make a rule that targets a very specific instances of a signed file. This enables you to build granular Publisher rules that are based on individual characteristics of a signed file.

To target a file by an element of its digital signature, do the following:

1. In the New Rule Wizard or, on the Application tab in the Properties dialog box, select Publisher rule.
2. Select a signed file to target by using the Publisher .
3. In the signature dialog box, use the slider control to select one or more signature elements. You can select the following:
   - Publisher - Name of specific software publisher
   - Product name - Name of software product
   - File name - Name of signed file (EXE, MSI, or MSP file)
   - Product version - Version number of a specific product.

   Tip: Broaden the Rule’s Scope by Using a Wildcard
   You can broaden the scope of a Publisher rule by using the (*) wildcard character. This character can be used in the following Publisher rule input fields: Product name, File name, and Product version. The wildcard must be used to replace an entire string. Partial strings incorporating the wildcard along with static characters are not supported.

4. Optional. Enable the Use Custom Values check box to change displayed signature information. For example, you can do any of the following:
   - Use the version widget to specify an earlier or later product version than the version displayed in the File version box.
   - Change any value in the text input fields.

5. Click OK to return to the Properties dialog.

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting Regardless of Location (Hash Rule)

To target a specific version of an application regardless of its location so that you can modify its permissions or privileges when it is run, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the **Application** tab in the **Properties** dialog, select **Hash rule**.

2. Click ![select application icon] to select an application. A SHA1 hash code is generated from the selected application file or process. You can select any of the following:
• A process running on your computer.

• An executable file. Click **Select a file** to navigate to an executable file, either a local file or a file on a network share path or mapped drive.

It is recommended that you create rules based on network share paths using the fully qualified UNC paths, such as `\MyServer\MyFolder\MyApp.msi`. If necessary, mapped drives may be used. When you create a rule based on a mapped drive, select **Allow use of mapped drive letter in path** on the **Options** tab.

**Note:** Because a limited user has the ability to change a mapped drive, selecting this option presents a security risk because it can allow the user to elevate an unintended application.

An SHA1 hash code is calculated from the selected executable or process.

3. Optional. If you are planning to select **Run application(s) with custom token** as the action for the rule, you can restrict the targeting of the application by specifying **Arguments**:

• To target this application only if specific command line arguments are used when the application is launched, enter the **Arguments**. This field is not case-sensitive.
• To target this application regardless of any command line arguments specified when the application is launched, leave the **Arguments** field blank.

---

**Tip: Using Variables, Wildcards, and Partial Commands**

You can use variables, wildcards, and a partial command in the **Arguments** field.

A partial command is considered a match as long as each character from left to right matches the beginning of the actual process command.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press **F3**.

For more information, see the following:

- “Using Variables in Rule Properties,” page 111
- “Using Wildcards in Rule Properties,” page 37

---

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
**Targeting by Folder Location (Folder Rule)**

To target all applications in a specific folder so that you can modify their permissions or privileges when they are run, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the **Application** tab in the **Properties** dialog, select **Folder rule**.

![Image of Folder Rule in Properties Dialog]
2. Specify a path or click to select a folder, which can be either a local folder or a folder on a network share path. Wildcards are supported in this field.

It is recommended that you create rules based on network share paths using the fully qualified UNC paths, such as `\MyServer\MyFolder\`. If necessary, mapped drives may be used. When you create a rule based on a mapped drive, select **Allow use of mapped drive letter in path** on the **Options** tab.

**Note:** Because a limited user has the ability to change a mapped drive, selecting this option presents a security risk because it could enable the user to elevate an unintended application.

**Tip: Using Variables and Wildcards**

You can use variables and wildcards in the **Path** field.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press **F3**.

For more information, see the following:

- “Using Variables in Rule Properties,” page 111
- “Using Wildcards in Rule Properties,” page 37
Caution: Folder Rules and the system32 Folder

A problem can occur if a Folder rule is applied to the \system32 folder in some versions of Windows. For example, using Windows XP and Windows Server 2003 (x86 and x64) if a Folder rule is applied to \windows\system32 and the user logs off, the user cannot log in again. The system attempts the login operation but cannot complete it. To escape this condition, the computer must be rebooted.

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting an Installation File by Location (MSI Path Rule)

The MSI Path rule modifies msiexec.exe permissions and privileges, yet enables you to target by individual Windows Installer package (MSI file). To target a Windows Installer package based on its location so that you can modify its permissions or privileges when it is installed, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the Application tab in the Properties dialog, select **MSI Path rule**.

2. Specify a path or click ![folder_icon] to select a Windows Installer package, either a local file or a file on a network share path. This field also supports wildcard use.

It is recommended that you create rules based on network share paths using the fully qualified UNC paths, such as `\\MyServer\MyFolder\MyApp.msi`. If necessary, mapped drives may be used. When you create a rule based on a mapped drive, select **Allow use of mapped drive letter in path** on the Options tab.

**Note:** Because a limited user has the ability to change a mapped drive, checking this option presents a security risk because it could enable the user to elevate an unintended application.
**Tip: Using Variables and Wildcards**

You can use variables and wildcards in the **Package** field.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press **F3**.

For more information, see the following:

- “Using Variables in Rule Properties,” page 111
- “Using Wildcards in Rule Properties,” page 37

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting Installation Files by Folder Location (MSI Folder Rule)

The MSI Folder rule modifies msiexec.exe permissions and privileges, and enables you to target Windows Installer packages (MSI files) by folder.

To target all Windows Installer packages in a specific folder so that you can modify their permissions or privileges when they are installed, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the Application tab in the Properties dialog, select MSI Folder rule.

![Image of Properties dialog with MSI Folder Rule selected.](image)
2. Enter a path or click \ to select a folder, which can be either a local folder or a folder on a network share path.

It is recommended that you create rules based on network share paths using the fully qualified UNC paths, such as `\MyServer\MyFolder\`. If necessary, mapped drives may be used. When you create a rule based on a mapped drive, select **Allow use of mapped drive letter in path** on the **Options** tab.

**Note:** Because a limited user has the ability to change a mapped drive, checking this option presents a security risk because it could enable the user to elevate an unintended application.

**Tip: Using Variables and Wildcards**

You can use variables and wildcards in the **Folder** field.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press **F3**.

For more information, see the following:

- “Using Variables in Rule Properties,” page 111
- “Using Wildcards in Rule Properties,” page 37
To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting through Internet Explorer (ActiveX Rule)

ActiveX rules are not limited to ActiveX controls but apply in general to component installations initiated by Internet Explorer (IE). With IE running as a restricted user, control installations normally fail (often without proper feedback) because the installations occur within the IE process and therefore within the same restricted security context.

An ActiveX rule causes a targeted control to install in a separate context that can have permissions and privileges individually modified by the rule.

Tip: Elevate IE for Complete Security

For more advanced ActiveX controls and web-based applications that install components beyond the standard Internet Explorer add-on, elevation of Internet Explorer is highly recommended. See “Example: Elevate IE for a Website,” page 57, for information about how IE can be secured.

To target the installation of a specific ActiveX control, the installation of all ActiveX controls, or installations initiated by Internet Explorer so that you can modify their permissions or privileges, do the following:

Note: Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the Application tab in the Properties dialog, select ActiveX rule.

![Application tab in Properties dialog]

- The "New PowerBroker Desktops Properties" dialog shows the Application tab with the ActiveX rule selected.
- This rule targets an ActiveX control installation and is one of several options available, including Publisher rules, Path rules, and others.
- The "Run application(s) with" option is visible, indicating that tasks can be performed after the application is executed.
2. Target all component installations or a specific component installation
   - To target all component installations, select **Apply rule to all ActiveX control installations**.

**Caution:** This option allows all ActiveX controls

Selecting **Apply rule to all ActiveX control installations** allows all ActiveX controls to be installed, regardless of whether they are desirable. It is recommended that you carefully consider your users and your environment when deciding whether to select this option.
To target a specific component installation, clear the **Apply rule to all ActiveX control installations** check box and specify any desired limitations. You can restrict the targeting of this rule to components with the following specific items:

- **Source URL**: Such as [http://www.microsoft.com](http://www.microsoft.com).
- **Archive file name**: Such as `mycontrol.cab`. Enter the file name in the `Control` field.
- **CLSID**: Such as `{AD787F30-34D1-43EB-BC61-968DDD60E1A8}`.
- **MIME type**: Such as `application/pdf`.
- **Version of a control** (A specific control must first be entered in the `Control` field): The version range may be open-ended (such as `<1.00`) or closed (such as `>=1.00` and `<2.00`).

**Tip: Customizing Internet Explorer Dialogs**

After completing this rule, see “Managing User Messages,” page 116, for information about how you can customize the text in dialogs that are related to installation and downloads performed through Internet Explorer.
Tip: Securing ActiveX Rules

To make an ActiveX rule secure, target a specific component and specify a source URL. Source URL is considered secure because to spoof a control’s source URL, a malicious website would first have to compromise other network (or local computer) components, such as DNS. Other parameters used with a source URL provide configuration granularity. However, without a trusted source URL specified, use of any other ActiveX targeting parameter is not considered secure, as a site can easily host a control with any of these parameters.

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting Applications on Demand (Shell Rule)

A Shell rule enables users to elevate a specified executable file, installer package, script, shortcut, or Control Panel item by using a right-click option. When a Shell rule is applied to a computer, a user can elevate a file that is one of the supported file types by right-clicking it and selecting Run Elevated for an executable file or Install Elevated for a Windows Installer (MSI) package. The text that is displayed in the right-click menu for this option is configurable. For more information, see “Managing User Messages,” page 116.

Files with the following file extensions can be targeted by using a Shell rule:

- EXE (Executable file)
- 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)

To enable users to elevate applications on demand, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.
1. On the **Application** tab in the **Properties** dialog, select **Shell rule**.

2. In the **Arguments** field, enter the path to the executable file, installer package, script, shortcut, Control Panel item, or other application that you want users to have the option to elevate. You can use variables, wildcards, or partial commands to specify multiple applications.

   To allow users to elevate any application that they choose, leave this field blank. This approach may not be desirable because it provides users with the ability to elevate all applications and executables.

   **Tip: Using Variables, Wildcards, and Partial Commands**

   You can use variables, wildcards, and a partial command in the **Arguments** field.

   A partial command is considered a match as long as each character from left to right matches the beginning of the actual process command.

   For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press **F3**.

   For more information, see the following:
   - “Using Variables in Rule Properties,” page 111
   - “Using Wildcards in Rule Properties,” page 37

   To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting a CD/DVD (CD/DVD Rule)

The CD/DVD rule enables you to elevate all executables on a specific CD or DVD, based on the serial number of the CD or DVD.

To target all applications on a specific CD or DVD so that you can modify their permissions or privileges when run, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the **Application** tab in the **Properties** dialog, select **CD/DVD rule**.

   ![PowerBroker Desktops Properties](image)

   **CD/DVD**:
   - **Arguments**: MSI PATH RULE - Target installations by MSI file path
   - **Message**: CD/DVD RULE - Target a CD-ROM or DVD
   - **Action**: UAC RULE - Target any application started via UAC

2. Click ![Folder icon] to select a CD or DVD. You must insert the CD or DVD in your local computer to select it. PowerBroker Desktops detects the serial number of the CD or DVD.

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting Applications That Trigger UAC (UAC Rule)

User Account Control (UAC) is a security component in Windows 7 and Windows Vista that enables users to perform common tasks that normally require administrative privileges.

You can use a UAC rule to grant full Administrator rights to any application that presents a UAC prompt.

Tip: One-Time Elevated Access by Passcode

If you want to provide users with an opportunity to enter a Passcode to gain one-time elevated access to any application for which a UAC prompt is triggered, you can configure a UAC rule with an Application Launch message selected. For more information, see “Creating Application Launch Dialogs (Application Launch),” page 117.

To target an application that triggers a UAC prompt so that you can modify its permissions or privileges:

Note: Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. On the Application tab in the Properties dialog, select UAC Rule.

2. Specify a Path for the application or applications to target. You can browse to an application that you want to target or type in a path. If arguments are needed, specify them in the Arguments field.
Tip: Using Variables, Wildcards, and Partial Commands

You can use variables and wildcards in the Path and Arguments fields, and you can use a partial command in the Arguments field.

A partial command is considered a match as long as each character from left to right matches the beginning of the actual process command.

For the list of PowerBroker Desktops variables, click the field to which you want to add a variable and press F3.

For more information, see the following:

- “Using Variables in Rule Properties,” page 111
- “Using Wildcards in Rule Properties,” page 37

Note: By default, a UAC information dialog is not displayed when an application launch that normally triggers a UAC prompt is elevated by PowerBroker Desktops. You can configure whether a UAC dialog is displayed and configure a customized dialog by .

To finish configuring this rule, continue at step 6 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Selecting an Action for Application Control

Rules provide you with a choice of actions that you can use to perform application control or to add or remove Administrator rights. You can use either a blacklisting or whitelisting approach to managing the execution of applications and processes.

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

You can run an application with a custom token, run an application with Administrator rights added or removed, run an application with no change to its token, or deny execution of an application. The action that you select should be appropriate to the approach to application control that you have chosen. For more information, see “Determining an Application Control Approach,” page 34.

- **Run application(s) with custom token** - The application is run with the permissions, privileges, and integrity level that you configure in this rule.
- **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.)

- **Run application(s) with no change (passive)** - The application is run with no change to the process token. 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:** For rules with an action of Run application(s) with no change, the Apply rule to all processes launched by the targeted application check box has no effect. You must specify child processes separately.

- **Deny execution of application(s)** - The application process is terminated immediately after any associated message box is closed or immediately if there is no associated message box, effectively preventing the application from being used. Any changes to the permissions, privileges, and integrity level specified in the rule are irrelevant because the application is terminated. (This action is not available for ActiveX rules, Shell rules, or UAC rules.)

To finish configuring this rule, including arranging the order of rules so that the action selected can have the intended effect for application control, continue at step 7 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Configuring Common Options

If the action specified for a rule is **Run application(s) with custom token**, common options are available that you can use to restrict or extend the circumstances under which the rule is applied.

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

The options displayed depend on the type of rule selected. Also, some options may be dimmed but selected because they are required or dimmed but cleared because they are not permitted.

Depending on the type of rule and the action selected, the following options may be configurable:

- **Apply rule only if program is owned by the Administrators group** - To target the application only if it is a local file owned by the Administrators group, select this option. (If available, this option appears on the Application tab in the rule Properties dialog.)

- **Apply rule to all programs in all subfolders of the specified folder** - To target all applications in subfolders of the folder specified by the rule, select this option. (If available, this option appears on the Application tab in the rule Properties dialog.)

- **Apply rule to all packages in all subfolders of the specified folder** - To target all installation files in subfolders of the folder specified by the rule, select this option. (If available, this option appears on the Application tab in the rule Properties dialog.)

- **Apply rule to all processes launched by the targeted application (or control)** - To cause processes launched by the application or process to inherit the permission or privilege changes specified in the rule, select this option. (If available, this option appears on the Application tab in the rule Properties dialog.)

- **Apply rule to file system browsing within targeted application** - To elevate any File Open/Save dialogs launched from within the application or process targeted by the rule, select this option. By default, this option is enabled. Disabling this option for an elevated application or process causes administrator rights to be omitted from File Open/Save dialogs. (If available, this option appears on the Options tab in the rule Properties dialog.)
If the rule removes administrator rights from an application or process, this option has no effect. Administrator rights will not be re-added to the File Open/Save dialog after they have been removed from a targeted application or process.

- **Apply rule only if arguments match exactly** - To target an application only if the arguments specified in the rule exactly match those with which the application is run, select this option. Otherwise, arguments are matched with a multiple character wildcard (*) on the end of the string. (If available, this option appears on the **Options** tab in the rule Properties dialog.)

- **Allow use of mapped drive letter in path** - To apply the rule based on a mapped drive instead of a UNC path, select this option. Otherwise, the rule is based on a UNC path, regardless whether the application is run from a mapped drive. (If available, this option appears on the **Options** tab in the rule Properties dialog.)

In general, it is recommended that you create Path rules and Folder rules based on the UNC path and leave this option cleared. If you must create a rule based on a mapped drive, select this option to make PowerBroker Desktops apply the rule based on the mapped drive, not the UNC path.

**Note:** Because a standard user has the ability to change a mapped drive, selecting this option could allow them to elevate an unintended application.

To finish configuring this rule, continue at step 8 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Configuring Token Security

By using PowerBroker Desktops, you can modify the token associated with an application or process. You can alter the permissions, privileges, process security, or integrity level for users or computers targeted by a rule when using applications or processes targeted by the rule. For example, you can grant Administrator permissions to users for use only while using a particular application, or you can deny specific privileges when an application is launched from a particular group of computers.

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.

You can perform the following tasks to alter the token:

- “Modifying Permissions,” page 89
- “Modifying Privileges,” page 91
- “Modifying Process Security,” page 93
- “Modifying Integrity Level,” page 94
Modifying Permissions

After you have targeted an application or process, you can make modifications to the permissions of that application or process when it is run. Permissions are defined by the security groups listed in the process token. By default, this list includes all security groups to which the end-user (who launched the process) belongs.

With each rule, you can add security groups to and/or remove security groups from the application’s process token. The effect is the same as making changes to the end-user’s group memberships but only for the specified application.

**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.

To modify the permissions for an application or process that you have targeted, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. In the Properties dialog box, click the **Token** tab.

2. In the Permissions box, click **Add** to configure modifications to permissions for a new security group, whether adding a group to or removing a group from the permissions for the application.

3. In the **Group** dialog box, specify a group name or click to browse to a group.
4. When specifying a group name, use one of the naming conventions shown in the following examples:
   – **MyGroup** (This will be resolved during Group Policy processing using standard resolution logic, first searching the local host and then the network domain accounts for a match.)
   – **MyDomain\MyDomainGroup**
   – **MyComputer\MyGroup**
   – **BUILTIN\MyGroup**
   – **.\MyGroup** (indicates a group on the local computer)

   **Tip: SID Resolution**

   If browsing to select a group, the SID is resolved automatically when you make your selection and the name (although displayed) is ignored when permissions are determined. If entering a group name manually, the SID is resolved during Group Policy processing on client computers.

5. Select an **Action** for the group.
   – To enable this group to use the application if the group does not have permission to do so, select **Add this group to the security token**.
   – To prevent this group from using the application if the group already has permission to do so, select **Remove this group from the security token**.

6. Click **OK** to close the **Group** dialog box.
7. Repeat to configure modifications for additional security groups.
Tip: Removing or Changing Modifications to Permissions

To delete a modification to permissions for a security group (whether adding a group to or removing a group from the permissions for the application), select the group and click **Remove** on the **Permissions** tab. To change the security group name or the action for a modification to permissions for a security group, select the group and click **Change** on the **Permissions** tab.

To finish configuring this rule, continue at step 9 in “Creating or Editing a Rule with the Properties Dialog,” page 47, if you want to further configure token security. Otherwise, continue at step 10.

For information about issues unique to members of the Administrators group, see “Rules Have No Effect,” page 154.

**Modifying Privileges**

After you have targeted an application or process, you can select modifications to be made to the privileges of that application or process when it is run. With each rule, you can grant or deny privileges to the application. The effect is the same as if the privileges were granted or denied to the end-user but this applies only for the specified application.

**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.

To modify the privileges for an application or process that you have targeted, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.
1. In the **Properties** dialog, click the **Token** tab.

2. You can either make changes to the privileges associated with an application or you can limit the privileges for an application to those that you specify. In the **Privileges** box, specify an approach:
   - To make changes to the privileges associated with an application's token, leave the **Remove all privileges before applying** check box cleared. This approach is recommended unless you fully understand the privileges required by the application.
   - To limit the privileges for a process to those that you configure, select the **Remove all privileges before applying** check box.

3. To improve security, by default PowerBroker Desktops configures privileges as disabled. The targeted application must enable them. If an application requires that privileges already be enabled for the application to function correctly, select the **Enable all granted privileges** check box.

4. In the **Privileges** box, click **Change**.

5. In the **Privileges** dialog, select a privilege and specify an **Action** for it. Move the mouse pointer over a privilege to display a description. You can use the **Shift** or **Ctrl** keys to select multiple privileges and configure them simultaneously:
– To grant the selected privileges to the application if it does not have them, click **Grant**.

– To deny the selected privileges to the application if it does have them, click **Deny**.

– To remove an existing modification the privileges, click **Deselect**.

6. Repeat these steps to configure modifications for other privileges, and then click **OK** to close the **Privileges** dialog.

To finish configuring this rule, continue at step 9 in “Creating or Editing a Rule with the Properties Dialog,” page 47, if you want to further configure token security. Otherwise, continue at step 10.

**Modifying Process Security**

In most cases, it is not necessary to grant process-specific access rights to elevate an application. However, if attempts to elevate a particular application have failed or caused problems, granting process-specific access rights may be necessary.

For more information, see “Problems Requiring Process-Specific Access Rights,” page 156.
To finish configuring this rule, continue at step 9 in “Creating or Editing a Rule with the Properties Dialog,” page 47, if you want to further configure token security. Otherwise, continue at step 10.

Modifying Integrity Level

Windows and Windows Server operating systems have a security setting that PowerBroker Desktops enables you to adjust for applications. PowerBroker Desktops enables you to elevate or lower the Integrity Level under which an application runs. By default, most applications run under Medium Integrity Level.

Note: The Integrity Level setting has no effect on computers running Windows XP or Windows Server 2003.

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.
To modify the integrity level for an application or process that you have targeted, do the following:

**Note:** Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.

1. In the Properties dialog box, click the **Token** tab.

![Token tab in Properties dialog](image1)

2. In the **Integrity Level** box, use the slider to specify the integrity level to be used when running the process.

   ![Integrity Level slider](image2)

To finish configuring this rule, continue at step 9 in “Creating or Editing a Rule with the Properties Dialog,” page 47, if you want to further configure token security. Otherwise, continue at step 10.
Configuring Execution Options

Using execution options, you can restrict how many times a rule is applied, the time span during which the rule is applied, and the network connection when the rule is applied. Execution options are applied at run time.

In the rule Properties dialog, execution options are specified on the Options tab. For information about other options on this tab, see “Configuring Common Options,” page 86.

Note: Before you begin, see “Creating or Editing a Rule with the Properties Dialog,” page 47. Alternatively, for information about using a wizard to create a rule, see “Creating a Rule with the Wizard,” page 40.
To configure execution options, on the **Options** tab in Properties dialog of a rule, select the check box for any execution options desired and specify any values needed for the options selected:

- **Apply rule only**: Allows the rule to be applied only a specified number of times.
- **Apply rule starting at**: Allows the rule to be applied only during specified hours.

**Tip: Time Zones**

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.

- **Apply rule starting on**: Allows the rule to be applied only during a specified date range.
- **Apply rule when**: Allows the rule to be applied only under certain network conditions.
  - **Connected**: Rule is applied only when the computer is connected to a network via wireless, network cable, or VPN connection.
  - **Connected Locally**: Rule is applied only when the computer is connected to a network either via wireless or network cable connection.
  - **Connected via VPN/dialup**: Rule is applied only when the computer is connected to a VPN/dialup connection.
  - **Disconnected**: Rule is applied only when the computer is disconnected from all networks.
  - **Disconnected - Apply after**: Rule is applied only when computer has been disconnected from a network for the specified amount of time.

The rule must be applied before the client computer is disconnected from the network.

To finish configuring this rule, continue at step 11 in “Creating or Editing a Rule with the Properties Dialog,” page 47.
Targeting Users or Computers with Item-Level Targeting

After you have targeted an application or process with a rule and configured modifications to be made to the permissions and privileges of that application or process when it is run, you can limit the application of these security modifications to selected users and computers.

Using item-level targeting, you can manage a wider variety of users and computers with a smaller number of Group Policy Objects (GPOs). Within a single GPO, you can configure a rule to apply its settings only to specific users and computers.

Each targeting item results in a value of either TRUE or FALSE. When using multiple targeting items, you can select the logical operation (AND or OR) by which to combine each targeting item with the preceding one. You can also create parenthetical groupings of targeting items by using collections. If the combined value of all targeting items for a rule is FALSE, settings in the rule are not applied to the user or computer.

Many types of targeting items are available. The following image shows the Targeting Editor and the menu of available item types:
By applying targeting items to a rule collection, you can apply the same targeting items to multiple rules to save time and effort. For information about applying targeting items to a collection of rules, see “Managing Multiple Rules with a Collection,” page 107.

To limit the security modifications of a rule or collection to users, groups, or computers that meet filtering requirements imposed by item-level targeting, do the following to configure targeting items:

1. On the Application tab in the Properties dialog for a rule or the Collection tab in Properties dialog for a collection, select the Item-Level Targeting check box.

2. Click Targeting to open the Targeting Editor window.
3. To create or modify targeting items, in the Targeting Editor window:
   a. To create a new targeting item, click the **New Item** menu and select a type of targeting item to create.
   b. To modify an existing targeting item, click the targeting item to display its properties.
   c. Configure any properties for the targeting item in the lower part of the Targeting Editor window.
   d. If you want to invert the result of the targeting item, in the **Item Options** menu, select **IS NOT**.
   e. Optional. To label the targeting item and include a comment, in the **Item Options** menu, select **Label**. Enter a name and comment, and then click **OK** in the **Label Targeting Item** dialog.
   f. If this targeting item is not the first one listed in the Targeting Editor or in a collection, click the **Item Options** menu and click either **AND** or **OR** to specify the logical operation by which to combine this targeting item with the preceding one.
   g. Repeat to create any additional targeting items needed.

4. To move a targeting item or collection up or down in the list, click the item to move and then click the **Move Up** or **Move Down** arrow button in the menu bar.

5. To move a targeting item into or out of a collection:
   a. Right-click the targeting item and select **Cut**.
   b. Right-click the collection to which you want to add the item or any targeting item that is at the level where you want to add the item and select **Paste**.

6. Click **OK**. The rule or rule collection will be applied to users, groups, or computers only if the logical result of the targeting items when combined is TRUE.

   To finish configuring this rule, continue at step 12 in “Creating or Editing a Rule with the Properties Dialog,” page 47.

**Example: Fast notebook computers with old operating systems**

In this example, targeting items are configured as follows to target fast notebook computers that are running older operating systems. The targeting items are combined using AND operations to produce a logical result of TRUE or FALSE for each computer.

- **Operating System** IS NOT Windows 7 on a Workstation.
- **Battery Present** IS present. (This usually indicates a notebook computer.)
- **CPU Speed** IS greater than or equal to 3000MHz.
This combination of targeting items causes the rule to be applied only to notebook computers not running Windows 7 and that have a 3GHz or faster CPU.

For information about each type of targeting item, see the PowerBroker Desktops Help.

For information about grouping targeting items into collections of targeting items, see “Grouping Targeting Items into a Collection,” page 101.

**Grouping Targeting Items into a Collection**

A collection of targeting items enables you to create a parenthetical grouping of items within a larger targeting expression. You can nest one targeting item collection within another to create more complex logical expressions.

A collection of targeting items allows a rule to be applied to computers or users only if the collection of targeting items specified results in a value of TRUE. If IS NOT is selected for the collection, the rule is applied only if the collection of targeting items specified results in a value of FALSE.
You can build a collection of targeting items by right-clicking a targeting item and selecting from the menu to choose the items, as shown in the following example:

To create or modify a collection of targeting items, do the following:

1. On the Application tab in the Properties dialog for a rule or the Collection tab in Properties dialog for a collection, select the Item-Level Targeting check box.
2. Click Targeting to open the Targeting Editor window.
3. To create a new collection of targeting items, in the Targeting Editor window:
   a. To create a new collection, click Add Collection.
   b. To modify an existing collection, click the collection to select it.
   c. If you want to invert the result of the targeting collection, in the Item Options menu, select IS NOT.
   d. Optional. To label the targeting collection and include a comment, in the Item Options menu, select Label. Enter a name and comment, and then click OK in the Label Targeting Item dialog.
e. If this targeting collection is not the first item listed in the Targeting Editor or in a collection, click the **Item Options** menu and click either **AND** or **OR** to specify the logical operation by which to combine this collection with the preceding item.

4. To add a new targeting item to the collection, right-click the collection and select a type of targeting item to add. Configure the targeting item. For more information, see “Targeting Users or Computers with Item-Level Targeting” on page 98.

5. To add an existing targeting item to the collection,
   a. Right-click the targeting item that you want to add to the collection and click **Cut**.

   a. Right-click the collection and click **Paste**.

6. To move a targeting item or collection up or down in the list, click the item to move and then click the **Move Up** or **Move Down** arrow button in the menu bar.

7. Click **OK**. The rule or rule collection will be applied to users, groups, or computers only if the logical result of the targeting items when combined is TRUE.

**Example: Restricting time window and user language for rule**

The following is an example of an item-level targeting configuration that includes a collection containing time, date, and language items. Because the collection allows the associated rule to be applied only if the combination of the items in the collection produces a result of TRUE, the collection limits the rule it is associated with to being applied on Sunday, between 9 AM and 5 PM to computers on which the user language is traditional French.
Arranging the Order of Rules

Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. If more than one PowerBroker Desktops rule within a GPO would target the same application, the rule with the highest order number wins and no other rules within the GPO take effect on that application. If a rule under User Configuration and a rule under Computer Configuration both target the same application, only the rule under User Configuration takes effect on the application.

**Note:** If you are using PowerBroker Desktops rules in multiple GPOs and those rules have the potential to impact the same application, you must also arrange the GPOs according to the intended order of processing. GPOs are processed sequentially from highest precedence number to lowest. If two GPOs each contain a PowerBroker Desktops rule that configures security for the same application, both rules take effect in sequence. The rule in the GPO with the lowest precedence number wins because it is the last to be applied.

You must arrange rules according to the intended order of processing so that rules with an action of **Custom Token**, **Add Admin Token**, or **Remove Admin Token** can take priority over rules with other actions, and so that rules with an action of **No Change** can take priority over rules with an action of **Deny Execution**.

Configure the order of the rules within a GPO to achieve the following:

- Rules with an action of **Custom Token**, **Add Admin Token**, or **Remove Admin Token** should have the highest order numbers.
- Rules with an action of **No Change** should have order numbers less than those with **Custom Token**, **Add Admin Token**, or **Remove Admin Token**, but greater than those with **Deny Execution**.
- Rules with an action of **Deny Execution** should have the lowest order numbers.

To view and change the order of rules in a GPO:

1. In the Group Policy Management Editor, display the PowerBroker Desktops extension:
   - If applying rules to computers, click **Computer Configuration**, Policies, BeyondTrust, PowerBroker Desktops
   - If applying rules to users, click **User Configuration**, Policies, BeyondTrust, PowerBroker Desktops.
2. Review the values in the **Order** column and the **Action** column.

3. To change the **Order** number for a rule, click the rule and then click the up arrow or down arrow in the toolbar of the Group Policy Management Editor.

4. Repeat with other rules until you have achieved the intended order.

For information about rule order when collections are used, see “Managing Multiple Rules with a Collection,” page 107.

For more information about rule order and application control, see “Determining an Application Control Approach,” page 34.
Advanced Techniques

In addition to the basic technique of configuring rules to manage security for applications and processes, you can use PowerBroker Desktops to accomplish the following:

- “Copying a Rule,” page 106
- “Managing Multiple Rules with a Collection,” page 107
- “Using Variables in Rule Properties,” page 111
- “Managing User Messages,” page 116
- “Generating a Passcode to Respond to a Message,” page 132
- “Viewing and Managing Reports,” page 135
- “Configuring Logging for Data Collection,” page 149
- “Backing Up a GPO,” page 152
- “Editing the XML Source Code of a Rule,” page 153

Copying a Rule

You can copy and paste (or drag and drop) a rule to copy it from one Group Policy Object (GPO) to another. If you want to create two similar rules within a GPO, you can copy and paste a rule within the same GPO to create a duplicate rule that you can edit as a starting point for a new rule.

If you are familiar with XML, you can also drag and drop a rule to your desktop so that you can manually edit the source code of the rule in an XML editor. For more information, see “Editing the XML Source Code of a Rule,” page 153.
Managing Multiple Rules with a Collection

You can organize rules in a group called a collection. A collection enables you to treat multiple rules as a single entity. This feature is useful when you want to apply the same item-level targeting to several rules or when you want to organize rules into physical groupings for ease of maintenance or review.

To create or modify a rule collection, do the following:

1. In the Group Policy Management Editor, do one of the following:
   - If applying this collection to selected computers, click **Computer Configuration, Policies, BeyondTrust, PowerBroker Desktops**.
   - If applying this rule to selected users, click **User Configuration, Policies, BeyondTrust, PowerBroker Desktops**.

2. If creating a new collection, right-click the **PowerBroker Desktops** node and select **Create New Collection**.

3. If modifying an existing collection, right-click the collection and click **Properties**.

4. In the Properties dialog for the collection, enter a name for the collection in the **Collection name** field.

5. Optional. 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.

   For more information, see “Selecting an Action for Application Control,” page 84.

6. Optional. To specify a previously-configured message to be displayed to users to whom rules in this collection are applied, select a message. You can use a message to require users to provide credentials or to enter a justification for an elevation request. You can configure messages by right-clicking the **PowerBroker Desktops** node in the Group Policy Management Editor and then clicking **Manage User Messages**.

   If you configure a message for a collection and a message for a rule in that collection, both messages are displayed if the rule is applied.

   For more information, see “Managing User Messages,” page 116.
7. Optional. To alter the permissions, privileges, process security, or integrity level with which the applications or processes are run for the entire collection, click the **Token** tab and configure options. These options are available only if the action selected is **Run application(s) with custom token**.

If you have not enforced an action for the collection, you can also configure additional permissions, privileges, process security, or integrity level options within each rule.

For more information, see the following:
- “Modifying Permissions,” page 89
- “Modifying Privileges,” page 91
- “Modifying Process Security,” page 93
- “Modifying Integrity Level,” page 94

8. Optional. To configure item-level targeting for entire the collection, select the **Item-Level Targeting** check box and click **Targeting**. Configure targeting items so that the collection is applied only to appropriate users or computers.

You can also configure additional item-level targeting within each rule.

For more information, see “Targeting Users or Computers with Item-Level Targeting ,” page 98.

9. Optional. In the **Collection Description** field on the **Collection** tab, enter an explanation of the purpose of the collection and any details that would be helpful to administrators updating the collection or creating related collections.

10. Click **OK** to save and close the collection.

11. In the Group Policy Management Editor, change the order of this collection as needed to support application control. Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. Rules with an action of **Custom Token, Add Admin Token**, or **Remove Admin Token** should have the highest order numbers and rules with an action of **Deny Execution** should have the lowest order numbers. For more information, see “Arranging the Order of Rules,” page 104.

12. To add rules to the collection, do either of the following:
- To move an existing rule into the collection, click the existing rule in the list of rules and collections and drag it into the collection.
- To create a new rule in the collection, double-click the collection in the list of rules and collections to navigate into the collection and then create rules from that location.
Rule Processing When Collections Are Present

The order number for each rule and collection is displayed in the Order column of the PowerBroker Desktops user interface. However, a collection and a rule can have the same order number, and each collection can contain rules and collections.

Keep the following in mind when trying to determine rule processing order:

• Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. (For more information, see “Arranging the Order of Rules,” page 104.)

• When a rule and a collection have the same order number, the individual rule is processed before the collection.

• When a rule collection contains a sub-collection, rules in the parent collection are processed first, then rules in the sub-collection are processed.

• Rule collections are automatically assigned an order number when they are created. You can change the order number of a collection by selecting the collection in the Group Policy Management Editor and clicking the **Move the selected item up** or **Move the selected item down** arrow buttons in the menu bar.

Example: Rule and Collection Processing

The following rule list contains collections and individual rules, and one of the collections contains a sub-collection. The Order column identifies the overall rule processing flow of this mix of rules and collections. Regardless of whether the rules are sorted in ascending order, descending order, or by using another column header, they will always be processed sequentially from highest order number to lowest.
Because an individual rule always takes precedence over a collection with the same order number, the MyPathRule (Order: 4), MyPublisherRule (Order: 3), and the All ActiveX Installations rule (Order: 2) are processed before any of the rules in Other Collection (Order: 2) are processed. After all the rules in Other Collection are processed, UAC Rule (Order: 1) is processed.

Processing then moves to My Collection (Order: 1). My Collection contains a sub-collection. The rules in the outermost collection are processed first, and then the rules in the inner collection are processed.
Using Variables in Rule Properties

PowerBroker Desktops supports Windows environment variables and generates additional process environment variables. These variables can be incorporated into rule properties, such as a path to an executable. For more information whether a particular field supports variables, see the section for the type of rule under “Targeting Applications or Processes,” page 54.

Wildcards can also be used in some rule properties. For information, see “Using Wildcards in Rule Properties,” page 37.

Tip: Using Item-Level Targeting and Variables

By using a Registry Match targeting item, you can define variables at client run-time to control behavior using an Environment Variable targeting item or as values in a rule. For more information, see “Targeting Users or Computers with Item-Level Targeting,” page 98

Environment Variables

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

Where does the environment come from?

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

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
- HKEY_CURRENT_USER\Environment
- HKEY_CURRENT_USER\Volatile Environment

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

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

PowerBroker Desktops Process Variables

PowerBroker Desktops CSEs implement the process variables listed below. All of the variables are supported on all client platforms. Unless these variables also happen to be Windows persistent environment variables, they only have definition when used in PowerBroker Desktops settings.

Note: Variables are not text case sensitive.

- **AppDataDir** - The current user's application data directory.
- **BinaryComputerSid** - The SID of the computer in hexadecimal format.
- **BinaryUserSid** - The SID of the logon user in hexadecimal format.
- **CommonAppdataDir** - The 'all users' application data directory.
- **CommonDesktopDir** - The 'all users' desktop directory.
- **CommonFavoritesDir** - The 'all users' Explorer favorites directory.
- **CommonProgramsDir** - The 'all users' programs directory.
- **CommonStartMenuDir** - The 'all users' start menu directory.
- **CommonStartUpDir** - The 'all users' startup directory.
- **ComputerName** - The NetBIOS name of the computer.
- **CurrentProcessId** - The numeric identity of the main process.
- **CurrentThreadId** - The numeric identity of the main thread.
- **DateTime** - The current time (UTC).
- **DateTimeEx** - The current time (UTC) with milliseconds.
- **DesktopDir** - The current user's desktop directory.
- **DomainName** - The domain name or workgroup of the computer.
- **FavoritesDir** - The current user's Explorer favorites directory.
- **LastError** - The last error code encountered during configuration.
- **LastErrorText** - The last error code text description.
- **LdapComputerSid** - The SID of the computer in LDAP escaped binary format.
- **LdapUserSid** - The SID of the logon user in LDAP escaped binary format.
- **LocalTime** - The current local time.
- **LocalTimeEx** - The current local time with milliseconds.
- **LogonDomain** - The domain of the current user.
- **LogonServer** - The domain controller that authenticated the current user.
- **LogonUser** - The username of the current user.
- **LogonUserSid** - The SID of the logon user.
- **MacAddress** - The first detected MAC address on the computer.
- **NetPlacesDir** - The current user's my network places directory.
- **PrivilegeManagerVersion** - The version of the running PowerBroker Desktops CSE.
- **ProgramFilesDir** - The Windows Program Files directory.
- **ProgramsDir** - The current user's programs directory.
- **RecentDocumentsDir** - The current user's recent documents directory.
- **ResultCode** - The client's exit code.
- **ResultText** - The client's exit code text description.
- **ReversedComputerSid** - The SID of the computer in reversed byte order hexadecimal format.
- **ReversedUserSid** - The SID of the logon user in reversed byte order hexadecimal format.
- **SendToDir** - The current user's send to directory.
- **StartMenuDir** - The current user's start menu directory.
- **StartUpDir** - The current user's startup directory.
- **SystemDir** - The Windows system directory.
- **SystemDrive** - The name of the drive from which the operating system is running.
- **TempDir** - The current user's temp directory as determined by Windows API.
- **TimeStamp** - The time stamp of the configurations being executed.
- **TraceFile** - The path/name of the trace file.
- **WindowsDir** - The Windows directory.
Select a Variable Dialog

The Select a Variable dialog allows you to select known variables from a list.

To display the Select a Variable dialog, click in a text field in a rule or collection Properties dialog and press the F3 key. When you select a variable, it is inserted at the position of the cursor and is enclosed by % characters to indicate that it is a variable. When the PowerBroker Desktops client software runs, this variable is resolved to its current value on the client computer at that time.

Preventing Variable Resolution

To prevent a variable from being resolved when the client software runs, clear the Resolve Variable check box in the dialog. This inserts <> characters between the %% variable delimiters and the variable name (for example, %<ProgramFiles>%).
Customizing the List of Variables

The variable names and descriptions in the Select a Variable dialog are generated from an XML document, variables.xml. By altering this document, you can add, remove, or change these names and descriptions. Changes to this document have no effect on the availability of variables during client software execution.

The location of the variables.xml file on a computer that is running the PowerBroker Desktops snap-in depends on the operating system.

- For Windows Server 2008, Windows 7, or Windows Vista
  C:\ProgramData\BeyondTrust\PowerBroker Desktops\n
- For Windows Server 2003 or Windows XP
  C:\Documents and Settings\All Users\Application Data\BeyondTrust\PowerBroker Desktops\n
Managing User Messages

You can use PowerBroker Desktops to require end users to provide credentials or to submit a justification for a request for elevation and to customize the messages displayed to end users.

Using PowerBroker Desktops, you can configure the following types of message:

- **Application Launch** - A customized message is displayed in a dialog box to end users when they attempt to launch applications for which they lack sufficient privileges. User name, password, and justification can be requested, or one-time access can be authorized by Passcode.

- **Blocked Application** - A customized message is displayed in a dialog box to end users when they attempt to launch a prohibited application. One-time access to the application can be authorized by Passcode.

- **IE Elevation** - Text in the Internet Explorer user interface is customized to indicate when Internet Explorer has been elevated.

- **IE Failure** - A customized message is displayed in a dialog box when an end user with insufficient privileges attempts to install an ActiveX component.

- **On-Demand Elevation** - Customized context menu options are displayed when an end user right-clicks an executable file (EXE) or a Windows Installer package (MSI).

- **UAC Prompt Detected** - A customized message precedes the standard User Account Control (UAC) prompt, and the standard UAC prompt can be suppressed.

**Tip: Customizing the IE Download Dialog**

You can customize how download progress is displayed in Internet Explorer download dialogs by using the PowerBroker Desktops Administrative Template. For information, see “Customizing the Internet Explorer Download Dialog,” page 130.
Creating Application Launch Dialogs (Application Launch)

You can display a dialog box when an end user attempts to start an application for which they lack sufficient privileges. You can request that the end user provide authentication credentials, type in a justification, or both.

Alternatively, 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. For example, you could provide access to an application for a support professional who does not have an end-user's credentials available. Using an authorization dialog, the user can send an Authorization Code generated using a public key to a specified email address and gain one-time access to the application by entering a Passcode received from an administrator in response. For information about generating a Passcode, see “Generating a Passcode to Respond to a Message,” page 132.

You can create multiple Application Launch messages and select a message in a PowerBroker Desktops rule to control which message is active for a given situation. Several default messages are provided, but you can also create your own. The default messages cannot be modified.

To create an Application Launch dialog box, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click Computer Configuration or User Configuration, BeyondTrust. Right-click PowerBroker Desktops and click Manage User Messages to open the PowerBroker Desktops Messages window.
3. In the Message Name field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.
4. To create a dialog box to be displayed when an end user attempts to start an application without sufficient privileges, for Message Type select Application Launch.
5. In the left column, configure text and settings for the dialog.
   – To display a header, set Show Header to True in the General section. In the Header section, configure an icon, text, and background for the header. For any images, it is recommended that you use a path to a shared location accessible to client computers and computers used to manage Group Policy. The recommended dimensions for a custom image background are 415 pixels wide by 56 pixels high.
– Specify text for the dialog title, **OK** button, and **Cancel** button. If you want to require that end users specify a justification or user name and password, it is recommended that you include guidance in the **Message body** field about what they should enter.

– To display the program name, path, and publisher, set **Show Program Name**, **Show Publisher Name**, and **Show Program Path** to True.

– To prompt the user to enter a justification, set **Justification Prompt** to True. If event logging is turned on, the justification is recorded in the event log.

– To prompt the user to enter a user name and password, set **Authentication Prompt** to True.

– To include a support link, configure the **Support URL** and **Support Page Text** fields.

– To offer a user requiring immediate one-time access to an application an option to enter authorization by Passcode instead of entering credentials, in the **General** section, set **Show Authorization** to True. Scroll up to view the **Authorization** section. Configure options in this section to customize the authorization dialog that the user can open by clicking the **Passcode** button. Authorization Codes and Passcodes are generated using a key pair and are not reusable.
The right column displays an overview of the resulting dialog or dialogs for you to review.

6. Click OK to save the message configuration. For this message to be displayed for users, you must associate it with a PowerBroker Desktops rule. For more information, see “Creating or Editing a Rule with the Properties Dialog,” page 47.
Example: Passcode Access When UAC Is Triggered

If you want to provide users with an opportunity to enter a Passcode to gain one-time elevated access to any application for which a UAC prompt is triggered, you can configure a UAC rule with an Application Launch message selected. If you want to provide a Passcode entry opportunity without including the option to enter credentials, set Show Authorization to True, Authentication Prompt to False, and Justification Prompt to False, as shown in the following example.

For information about configuring a UAC rule, see “Targeting Applications That Trigger UAC (UAC Rule),” page 82.
Creating Blocked Application Dialogs (Blocked Application)

You can display a dialog box when an end user attempts to start a prohibited application. You can provide a contact email address from which end users can request authorization.

Alternatively, 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. For example, you could provide access to an application for a support professional who does not have an end-user's credentials available. Using an authorization dialog, the user can send an Authorization Code generated using a public key to a specified email address and gain one-time access to the application by entering the Passcode received from an administrator in response. For information about generating a Passcode, see “Generating a Passcode to Respond to a Message,” page 132.

You can create multiple Blocked Application messages and select a message in a PowerBroker Desktops rule to control which message is active for a given situation.

To create a Blocked Application dialog box, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click Computer Configuration or User Configuration, BeyondTrust. Right-click PowerBroker Desktops and click Manage User Messages to open the PowerBroker Desktops Messages window.
3. In the Message Name field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.
4. To create a dialog box to be displayed when an end user attempts to start a prohibited application, select Blocked Application for Message Type.
5. In the left column, configure text and settings for the dialog.
   - To display a header, set Show Header to True in the General section. In the Header section, configure an icon, text, and background for the header. For any images, it is recommended that you use a path to a shared location accessible to client computers and computers used to manage Group Policy. The recommended dimensions for a custom image background are 415 pixels wide by 56 pixels high.
   - Specify text for the dialog title and Cancel button. In the message body, include any instructions about what the user should do.
– To display the program name, path, and publisher, set **Show Program Name**, **Show Publisher Name**, and **Show Program Path** to True.

– To display an administrator’s email address for end users to contact to request access, specify the address in the **Email Address** field. You can specify the subject line for the email in the **Email Subject** field. To omit the address, leave the **Email Address** field blank.

– To include a support link, configure the **Support URL** and **Support Page Text** fields.

– To offer a user requiring immediate one-time access to an application an option to enter authorization by Passcode instead of entering credentials, in the **General** section, set **Show Authorization** to True. Scroll up to view the **Authorization** section. Configure options in this section to customize the authorization dialog that the user can open by clicking the **Passcode** button. Authorization Codes and Passcodes are generated using a key pair and are not reusable.

The right column displays an overview of the resulting dialog or dialogs for you to review.

6. Click **OK** to save the message configuration. For this message to be displayed for users, you must associate it with a PowerBroker Desktops rule. For more information, see “Creating or Editing a Rule with the Properties Dialog,” page 47.
Customizing the Appearance of Internet Explorer When Elevated (IE Elevation)

You can customize the appearance of Internet Explorer to indicate when it has been elevated by PowerBroker Desktops. For an example of how you can elevate Internet Explorer, see “Example: Elevate IE for a Website,” page 57.

Tip: Only One IE Elevated Message Can Be Active

Only one IE Elevated message can be active on a given computer and only one IE Elevated message can be configured per GPO. For example, if different IE Elevated messages are configured in two GPOs and both GPOs are applied to a particular computer, only the message for the winning policy setting will be in effect.

To customize Internet Explorer when elevated, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click Computer Configuration or User Configuration, BeyondTrust. Right-click PowerBroker Desktops and click Manage User Messages to open the PowerBroker Desktops Messages window.
3. In the Message Name field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.
4. To customize the appearance of Internet Explorer when it is elevated, for Message Type select IE Elevation.
5. In the left column, configure the text for the Internet Explorer user interface. The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.
   - Title - Enter text to be added to the title bar before the title of web pages in elevated instances of Internet Explorer.
   - StatusBar - Enter text to be displayed in the status bar at the bottom of elevated instances of the Internet Explorer window.
   - NavigationBar - Enter text to be displayed in the title bar of the dialog that provides the user with the option to close the un-elevated instance of Internet Explorer from which the user attempted to connect to a website for which a rule provides elevation.
The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.

6. Click OK to save the message configuration. You do not associate this type of message with specific rules.

**Customizing the Internet Explorer Component Failure Dialog (IE Failure)**

Using ActiveX rules, you can restrict or enable component installations initiated by Internet Explorer (IE). With IE running as a restricted user, component installations normally fail (often without proper feedback) because the installations occur within the IE process and therefore within the same restricted security context.

Using a message, you can notify end users when a component installation fails and even provide an interactive response through email.

**Tip: Only One IE Failure Message Can Be Active**

Only one IE Failure message can be active on a given computer and only one IE Failure message can be configured per GPO. For example, if different IE Failure messages are configured in two GPOs and both GPOs are applied to a particular computer, only the message for the winning policy setting will be in effect.

To customize or hide the Internet Explorer failure dialog, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click **Computer Configuration** or **User Configuration**, **BeyondTrust**. Right-click **PowerBroker Desktops** and click **Manage User Messages** to open the PowerBroker Desktops Messages window.
3. In the **Message Name** field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.

4. To customize the dialog that is displayed when an ActiveX control fails due to lack of permissions, select **IE Failure** for the **Message Type**.

5. In the left column, configure text and settings for the dialog. The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.
   - To customize the message: Specify a title, message body, and **OK** button text for the dialog box. Set **ShowDialog** to **True**. Optionally, you can specify an administrator’s email address for end users to contact to request access. The administrator’s email address will appear as a link in the dialog.
   - To prevent a message from being displayed: By default, a message is displayed when a user with insufficient privileges attempts to install an ActiveX component. If, instead of customizing the dialog box, you want to prevent the dialog box from opening, then set **ShowDialog** to **False**.

The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.

6. Click **OK** to save the message configuration. You do not associate this type of message with specific rules.
The resulting dialog displayed to the end user looks like the following:

![Component Installation Failure dialog]

Customizing the Right-Click Menu Options (On-Demand Elevation)

Using a Shell rule, you can enable users to elevate an application on demand using a right-click menu option. You can customize or localize the text that is displayed in the menu when an end user right-clicks an executable file (EXE) or a Windows Installer package (MSI).

Tip: Only One On-Demand Elevation Message Can Be Active

Only one On-Demand Elevation message (including text for both EXE and MSI files) can be active on a given computer and only one On-Demand Elevation message can be configured per GPO. For example, if different On-Demand Elevation messages are configured in two GPOs and both GPOs are applied to a particular computer, only the message for the winning policy setting will be in effect.

To customize the right-click menu text for executable files and Windows Installer packages, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click Computer Configuration or User Configuration, BeyondTrust. Right-click PowerBroker Desktops and click Manage User Messages to open the PowerBroker Desktops Messages window.
3. In the **Message Name** field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.

4. To customize the menu that is displayed when an end user right-clicks an EXE file or an MSI file, select **On-Demand Elevation** for **Message Type**.

5. In the left column, configure text for the right-click menu options for executable files and Windows Installer packages. The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.

   The right column displays an overview of the resulting text for you to review, but you cannot enter text in the right column.

6. Click **OK** to save the message configuration. You do not associate this type of message with specific rules.

**Customizing the UAC Information Dialog (UAC Prompt Detected)**

User Account Control (UAC) is a security component in Windows 7 and Windows Vista that enables users to perform common tasks that normally require administrative privileges.

You can provide a customized dialog box instead of the UAC dialog box, or you can display the customized dialog box first and follow it with the standard UAC dialog box. You can use this feature to provide an email link to enable end users to email the system administrator with an elevation request.

**Tip: Only One UAC Prompt Detected Message Can Be Active**

Only one UAC Prompt Detected message can be active on a given computer and only one UAC Prompt Detected message can be configured per GPO. For example, if different UAC Prompt Detected messages are configured in two GPOs and both GPOs are applied to a particular computer, only the message for the winning policy setting will be in effect.
To customize the UAC dialog box, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.

2. In the Group Policy Management Editor, click Computer Configuration or User Configuration, BeyondTrust. Right-click PowerBroker Desktops and click Manage User Messages to open the PowerBroker Desktops Messages window.

3. In the Message Name field, type a name for the message. This name is displayed to Group Policy administrators so that they can select this message when configuring a PowerBroker Desktops rule. The name is not displayed to end-users.

4. To customize the dialog that is displayed when an ActiveX control fails due to lack of permissions, select UAC Prompt Detected for Message Type.

5. In the left column, configure text and settings for the dialog.
   - To display a header, set Show Header to True in the General section. In the Header section, configure an icon, text, and background for the header. For any images, it is recommended that you use a path to a shared location accessible to client computers and computers used to manage Group Policy. The recommended dimensions for a custom image background are 415 pixels wide by 56 pixels high.
   - Specify text for the dialog title, OK button, and Cancel button. To display the default UAC dialog when Cancel is clicked, set Show UAC to True. To prevent the default UAC dialog from being displayed, set Show UAC to False. In the message body, include any instructions about what the user should do.
   - To display the program name, path, and publisher, set Show Program Name, Show Publisher Name, and Show Program Path to True.
   - To display an administrator’s email address for end users to contact to request access, specify the address in the Email Address field. You can specify the subject line for the email in the Email Subject field.
   - To include a support link, configure the Support URL and Support Page Text fields.
The right column displays an overview of the resulting dialog or dialogs for you to review.

![Message Configuration Screen]

6. Click **OK** to save the message configuration. You do not associate this type of message with specific rules.

**Tip: Passcode Access When UAC Is Triggered**

If you want to provide users with an opportunity to enter a Passcode to gain one-time elevated access to any application for which a UAC prompt is triggered, you can configure a UAC rule with an Application Launch message selected. For more information, see “Targeting Applications That Trigger UAC (UAC Rule),” page 82, and “Creating Application Launch Dialogs (Application Launch),” page 117.
Customizing the Internet Explorer Download Dialog

You can customize the download progress dialog that Internet Explorer displays when an end-user attempts to download a file through Internet Explorer or browses to a page containing an ActiveX control.

**Note:** You enable this customization by using a BeyondTrust Administrative Template setting rather than by using the Messages field in a rule.

To customize the Internet Explorer download dialog:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. In the Group Policy Management Editor, click **Computer Configuration or User Configuration, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Security Driver**. If you are using an older operating system such as Windows Server 2003 or Windows XP and this path does not exist, you may need to manually install the Administrative Template. For more information, see “Installing the BeyondTrust Administrative Template,” page 174.
3. To customize the download progress dialog that is displayed when an end-user attempts to download, double-click **Customize IE Download Dialog**.

4. In the Properties window, click **Enabled**.
5. Configure other settings and click **OK**.
The following is an example of the dialog displayed when a user browses in Internet Explorer to a page containing an ActiveX control.

![Control Downloader Dialog](image-url)

Control Downloader

The page you are visiting contains an embedded control. Please be patient while it is downloaded.

Downloading ...

[Cancel]
Generating a Passcode to Respond to a Message

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. For example, you could provide access to an application for a support professional who does not have an end-user's credentials available.

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. You can create rules that target specific applications and associate an Application Launch message or a Blocked Application message with each rule. For information about configuring messages, see “Managing User Messages,” page 116.

If you want to provide users with an opportunity to enter a Passcode to gain one-time elevated access to any application for which a UAC prompt is triggered, you can configure a UAC rule with an Application Launch message selected. For more information, see “Targeting Applications That Trigger UAC (UAC Rule),” page 82, and “Creating Application Launch Dialogs (Application Launch),” page 117.

Generating a Passcode

To generate a Passcode, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. Open the Passcode Generator by using one of the following methods:
   - On the management dashboard, click Generate a Passcode.
   - In the console tree of the Group Policy Management Editor, right-click a PowerBroker Desktops node and select Passcode Generator.
3. In the PowerBroker Desktops Passcode Generator dialog, enter the Authorization Code received from the user who is requesting access. Only numeric characters can be entered.
4. Click **Get Passcode**.

![PowerBroker Desktops Passcode Generator](image)

- If the Authorization Code is valid, a Passcode is displayed. Send this Passcode to the user who requested access. To access the application, the user must enter the Passcode into the same instance of the dialog from which the user copied the Authorization Code.
- If the Authorization Code is not valid or no key is found, an error message is displayed in the **Status** box.

### Changing the Key Pair and Keys Path

A default key pair that includes a public key and a private key is installed along with the PowerBroker Desktops client software and snap-in software. It is recommended that you generate a new key pair before deploying to a production environment.

**Note:** If administrators use more than one computer to generate Passcodes, you must ensure that all of these computers are using the same key pair, and it is recommended that you use a shared folder accessible only to administrators for the keys path.

To replace the key pair used to generate Passcodes, do the following:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.
2. Open the Passcode Generator by using one of the following methods:
   - On the management dashboard, click **Generate a Passcode**.
   - In the console tree of the Group Policy Management Editor, right-click a **PowerBroker Desktops** node and select **Passcode Generator**.

3. Click the **Settings** tab in the PowerBroker Desktops Passcode Generator dialog.
   ![PowerBroker Desktops Passcode Generator](image)

4. To change the path to where the Passcode Generator creates keys and to where it stores the private key, in the **Keys path** box click **Select Directory** and navigate to a folder. If more than one computer is used to generate Passcodes, you must make this change on each of these computers, and it is recommended that you use a shared folder that is accessible only to administrators. Changing the keys path does not change the location for the public key on client computers.

5. To generate a new public and private key pair:
   a. Click **Generate New Key Pair**.
   b. Deploy the new public key to the following folder on each client computer:
      ```
      %WINDIR%\BeyondTrust\PBD\config
      ```
   c. If more than one computer is used by administrators to generate Passcodes and you are not using a shared folder for the keys path, you must copy the new key pair to the keys path for each computer used to generate Passcodes.
Viewing and Managing Reports

Using Auditing and Reporting (PBReports) for PowerBroker Desktops, you can view and manage audit data and reports about administrator and user rights, rules applied, and application usage. Usage data is gathered from client computers by using Microsoft Event Forwarding, and SQL Server Reporting Services (SSRS) is used to generate detailed, filterable reports.

Note: In addition to the reporting capabilities that are available through Reporting Services, you can also view reporting data and produce basic reports using the Reporting Console. For more information, see “Generating Rules and Creating Reports,” page 44

Tip: Configuring Auditing and Reporting
Before you can use Reporting Services, you must have a SQL Server or SQL Server Express database installed in your environment, and you must configure Auditing and Reporting for PowerBroker Desktops. See the PowerBroker Desktops Installation Guide for more information.

Types of Reporting Services Reports

The following are the types of Reporting Services reports and the data they contain. Several of the reports have a feature called cross-linking that allows you to easily move from a high-level report to more detailed information.

The following Reporting Services reports are provided:

- Auditing and Reporting Dashboard - Graphical charts of data about the applications most frequently launched, requiring elevation, triggering User Account Control (UAC), launched by Shell rule. Also, charts about ActiveX controls, rules applied, local administrators, and the ratio of administrator users to standard users.
- ActiveX Details - Information about installation events for ActiveX controls in Internet Explorer
- Applications by Path - Information about all applications under management tracked by launch path
- Application Path Details - Increased details about all applications under management tracked by launch path
- Applications by Hash - Information about all applications under management tracked by hash code
- Application Hash Details - Increased details about all applications under management tracked by hash code
Applications by Computer - Information about application usage on a particular client
Shell Rule Executions - Information about every Shell rule-based application launch

Viewing a Reporting Services Report

To view a Reporting Services report:
1. In the Group Policy Management Console (GPMC), edit a Group Policy Object (GPO).
2. In the Group Policy Management Editor, view the PowerBroker Desktops management dashboard by clicking either BeyondTrust node.
3. In the Tools & Wizard section of the dashboard, scroll to the Auditing and Reporting section and click Reporting Services.
4. On the PBReports page, click a report title to view a report.
5. Provide any search criteria required by the report.
6. Click View Report.
7. In a summary-level report, click a link to view a detailed report for that line item.

Note: If a report does not contain data, ensure that the client computers have the Administrative Template settings with names beginning with Log application launch configured under Computer Configuration, Policies, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Security Driver.

Auditing and Reporting Dashboard

The Auditing and Reporting Dashboard provides charts about application usage, installation of ActiveX controls, rules applied, and types of users.

Note: Data from client computers is included only if those computers are configured for Auditing and Reporting as specified in the PowerBroker Desktops Installation Guide.
The charts on the first part of the Auditing and Reporting Dashboard show the applications most frequently launched, most frequently requiring elevation, most frequently triggering User Account Control (UAC), most frequently launched by using a Shell rule, most frequently launched without a rule (passive), and most frequently denied launch.

![Auditing and Reporting Dashboard](image)

The charts on the second part of the Auditing and Reporting Dashboard show the applications most frequently launched by using Passcode, the ActiveX controls most frequently installed, the ActiveX controls for which ActiveX rules are most frequently applied, and the rules most frequently applied with a modified token (excluding instances of elevation by Shell rules).
The charts on the third part of the Auditing and Reporting Dashboard display the computers with the most local administrator accounts, the ratio of administrator users to standard users, the most active computers, and the most active users.

The chart on the fourth part of the Auditing and Reporting Dashboard displays the number of rules with custom tokens applied to users and computers each day during the previous thirty days, categorized by type of rule.

**ActiveX Details Report**

The ActiveX Details report presents all details associated with the installation of an ActiveX control. For each installation of an ActiveX control, the client computer collects and reports the following information:

- Source URL of the control
- Control name
- Control version
- Number of PowerBroker Desktops (rule-based) attempts to install the control
- Number of failed installations of the control
- User name
- Domain name
- Computer name
- Time of first attempt to install the control
- Whether a particular attempt to install the control was rule-based
- Whether a particular attempt to install the control failed
- Time of the most recent attempt to install the control
Data is grouped into rows by source URL and can be expanded to reveal more specific installation details. The Last Install Attempt in a detail row is for the specified computer and user for the selected control. The Most Recent Install Attempt for the source URL is for all client computers and end-users as filtered by the report parameters.

Parameters
The parameters are cascading (they must be entered in the following order and each parameter after the first is constrained by the one that precedes it). You can specify values for the following parameters in this report:
1. Source URLs of ActiveX controls
2. User names

Report Features
The following features are available in this report:

- **Sorting** - Column headers for each grouping row provide an interactive sort button to arrange items in ascending or descending order.

- **Source URL** - Can be expanded to provide additional detail about the installation.

The following is a typical ActiveX Details report. In this example, the entries for two Source URLs have been expanded to reveal additional information about the installation of each control, including the users who installed it.

### Applications by Path Report

The Applications by Path report presents a table of applications on each client computer. For each launch of an application, the client computer collects and reports the following information:

- Full path
- Application file name
- Product name
- Time of the last detected launch of the application
• Application file hash code
• Launch arguments
• Product version

Data is sorted by path. The full path item provides additional data, including the file hash code of the application, the arguments used when launching the application, and the product version number.

Because it is possible for different paths, product versions, and arguments to appear for a given path, the report may present multiple detail rows for each expanded application full path.

Last Launch Event for a detail row is for the specified hash code, arguments, and product version, for all client computers for the selected path. The Last Launch Event for the application full path is for all hash codes, arguments, product versions, and client computers for the specified path.

**Parameters**
You can specify which of the following types of events to include in the report:
• Applications requiring elevation
• Application launches
• PowerBroker Desktops rule applied
• UAC consent prompted
• Denied application launches
• Passive application launches

**Report features**
The following features are available in this report:
• **Sorting** - Column headers for each grouping row provide an interactive sort button to sort by ascending or descending order.
• **File Hash** - This item provides a dynamic link to the application Hash Details report for the specified hash code.
• **Product Version** - This item provides a dynamic link to the Application Path Details report for the specified product version.

The following is a typical Applications by Path report. In the example below, the white area contains expanded information about the explorer.exe application.
Applications by Hash Report

The Applications by Hash report groups the data by the application hash code rather than by the application path. For each launch of an application, the client computer collects and reports the following information:

- File hash code
- Application file name
- Product name
- Time of last detected launch
- Full path of the application
- Arguments used to launch the application
- Product version

Data is sorted by hash code. You can expand these rows to view more specific launch details. Because it is possible for different paths, product versions, and arguments to appear for a given hash code, the report may present multiple detail rows for each expanded application file hash code.

The Last Launch Event for a detail row is for the specified path, product version, and arguments for all client computers for the selected hash code. The Last Launch Event for the application hash code is for all paths, arguments, product versions, and client computers for the specified hash code.

Parameters

You can specify which of the following types of events to include in the report:

- Applications requiring elevation
- Application launches
- PowerBroker Desktops rule applied
- UAC consent prompted
- Denied application launches
- Passive application launches
Report Features
The following features are available in this report:

- **Sorting** - Column headers for each grouping row provide an interactive sort button to sort by ascending or descending order.

- **Full Path** - This item provides a dynamic link to the Application Path Details report for the specified path.

- **Product Version** - This item provides a dynamic link to the Application Hash Details report for the specified product version.

The following is an Applications by Hash report. In this example, the white row displays expanded information about the hash code of the cmd.exe application in the blue row immediately above it.

### Applications by Computer Report

The Applications by Computer report presents a table of computers that are reporting through the PowerBroker Desktops client computer. For each launch of an application, the client computer collects and reports the following information:

- Domain name
- Computer name
- User name
- User type
- Whether the user is a Local Administrator
- Full path of the launched application
- Arguments used to launch the application
- Product version
- Time of last detected launch for the specific path, product version, and arguments

Data is grouped into rows by domain name, computer name, and user name with specific launch details provided on each row.
The Last Launch Event in a detail row is for the specified path, product version, and arguments for the selected client computer and user.

**Parameters**

You can select multiple values for parameters in this report. They are non-cascading (no parameter constrains the one that follows it) and all values are available for each parameter. The Select All option is available for each parameter.

You can enter the following parameters for this report:
- Computer name
- User name

Additionally, you can specify which of the following types of events to include:
- Applications requiring elevation
- Application launches
- PowerBroker Desktops rule applied
- UAC consent prompted
- Denied application launches
- Passive application launches

**Report Features**

The following features are available in this report:

- **Sorting** - Column headers for each grouping row provide an interactive sort button to arrange items in ascending or descending order (with the exception of Service Pack and Build).
- **Full Path** - This item provides a dynamic link to the Application Hash Details report for the specified path.
- **Product Version** - This item provides a dynamic link to the Application Path Details report for the specified product version.

The following is an Applications by Computer report. In this example, expanded information is displayed for the computer W7X86.QAVC1.lab.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Option</th>
<th>Owner Name</th>
<th>Owner Type</th>
<th>Path Name</th>
<th>Path Hash</th>
<th>Last Launch Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>W7X86.QAVC1.lab</td>
<td>\PowerStreameL\Administrator</td>
<td>\PowerStreameL\Administrator</td>
<td>%\Windows\System32\wevtutil.exe</td>
<td>5.1.3000.0</td>
<td>7/24/2011 1:48 P</td>
</tr>
<tr>
<td>2</td>
<td>W7X86.QAVC1.lab</td>
<td>\PowerStreameL\Administrator</td>
<td>\PowerStreameL\Administrator</td>
<td>\W7X86.QAVC1.lab\PowerStreameL\Desktops\Desktops.exe</td>
<td>5.1.3000.0</td>
<td>7/24/2011 1:48 P</td>
</tr>
<tr>
<td>3</td>
<td>W7X86.QAVC1.lab</td>
<td>\PowerStreameL\Administrator</td>
<td>\PowerStreameL\Administrator</td>
<td>%\Windows\System32\wevtutil.exe</td>
<td>5.1.3000.0</td>
<td>7/24/2011 1:48 P</td>
</tr>
<tr>
<td>4</td>
<td>W7X86.QAVC1.lab</td>
<td>\PowerStreameL\Administrator</td>
<td>\PowerStreameL\Administrator</td>
<td>%\Windows\System32\wevtutil.exe</td>
<td>5.1.3000.0</td>
<td>7/24/2011 1:48 P</td>
</tr>
<tr>
<td>5</td>
<td>W7X86.QAVC1.lab</td>
<td>\PowerStreameL\Administrator</td>
<td>\PowerStreameL\Administrator</td>
<td>%\Windows\System32\wevtutil.exe</td>
<td>5.1.3000.0</td>
<td>7/24/2011 1:48 P</td>
</tr>
</tbody>
</table>

BeyondTrust® August 17, 2012 143
**Application Hash Details Report**

The Application Hash Details report presents all details associated with the launch of an application hash code. For each launch, the client computer collects and reports the following information:

- Hash code of the binary file
- Application file name
- File version of the launched file
- Product name
- Certificate publisher
- Product vendor
- Command line arguments passed
- Full path of the launched application
- Computer name
- User name
- User type
- Number of applications requiring elevation
- Number of application launches
- Number of PowerBroker Desktops rule-based application launches
- Number of Shell rule-based application launches
- Number of UAC consent prompted application launches
- Number of denied application launches
- Number of passive application launches
- Path, privileges, and last launch time

The detail data is grouped into several sections, including:

- **Launch Counters by Argument** - Reports the launch counters per combination of argument and full path, for the selected hash code.

- **Launch Counters by System** - Reports the launch counters per combination of domain, computer, and user for the selected hash code.

- **Privileges Details** - Specifies the required privileges to launch the application.
Parameters
The parameters are cascading (they must be entered in the following order and each parameter after the first is constrained by the one that precedes it). You can enter values for the following parameters:

1. **Hash filter** - Provides a means to filter for hash codes containing a specific sequence. The default value for this parameter is NULL (implying do not filter).
2. **Hash** - A drop-down list of hash codes. The default value for this parameter is all hash codes. Selecting a hash parameter filter constrains the list of hash codes to values containing the specified character sequence.

Report Features
The following features are available in this report:

- **Full path** - A dynamic link to the Application Path Details report for the specified path and product version.
- **System** - A dynamic link to the Application by Computer report for the specified computer.
- **User name** - A dynamic link to the Application by Computer report for the specified user.

The following is an Application Hash Details report:

![Application Hash Details Report](image)

**Application Path Details Report**

The Application path Details report presents details about an application launch from a specified path. For each launch, the client computer collects and reports the following information:

- Full path of the launched application
- Application file name
- Version of the launched file
• Product name
• Certificate publisher
• Product vendor
• Command line arguments passed
• Hash code of the binary file
• Computer name
• User name
• User type
• Number of applications requiring elevation
• Number of application launches
• Number of PowerBroker Desktops rule-based application launches
• Number of Shell rule-based application launches
• Number of UAC consent prompted application launches
• Number of denied application launches
• Number of passive application launches
• Path, privileges, and last launch

The detail data is grouped into the following sections:
• Launch Details by Argument - Reports launch counters per combination of argument and hash code for the selected path
• Launch Counters by System - Reports launch counters per combination of domain, computer, and user for the selected path
• Privileges Details - Specifies the required launch privileges

Parameters
You can select only a single value for each parameter in this report. The parameters are cascading (they must be entered in the following order and each parameter after the first is constrained by the one that precedes it). You can enter values for the following parameters:
1. Filename of the application
2. Full path of the application
3. Version of the application

Report Features
The following features are available in this report:
• Hash - A dynamic link to the Application Hash Details report for the specified path and product version.
The following is an Application Path Details report:

![Application Path Details](image)

**Shell Executions Report**

The Shell Rule Executions report presents a table of applications on each client computer that have been launched by a Shell rule on demand elevation operation. This occurs when a user responds to a launch prompt dialog triggered by a Shell rule. In this dialog, the user enters the justification or authentication information.

For each detected Shell rule application launch, the client computer collects and reports the following information:

- Full path of the launched application
- Application file name
- Product version
- Product name
- User name
- Computer name
- Arguments used to launch the application
- Justification text entered by user
- Time of last detected launch for the specific path, user, and computer
The data is grouped into rows by path and arguments. Computer, user, and justification data are provided in each row. The Launch Time in a detail row is for the specified computer, user, and path.

**Parameters**

You can select only a single value for each parameter in this report. The parameters are cascading (they must be entered in the following order and each parameter after the first is constrained by the one that precedes it). You can enter values for the following parameters:

1. Full path of the application
2. User names

**Report Features**

The following features are available in this report:

- **Sorting** - Column headers for each grouping row provide an interactive sort button to arrange columns on ascending or descending order.
- **System** - This item provides a dynamic link to the Application by Computer report for the specified computer.
- **User Name** - This item provides a dynamic link to the Application by Computer report for the specified user.

The following is an excerpt from a Shell Rule Executions report, with one entry expanded to show additional details:
Configuring Logging for Data Collection

PowerBroker Desktops includes logging options that are managed through the BeyondTrust Administrative Template. The following are some of the client-side logging options available in the Security Driver collection in the template:

- **Log all application launches** - Enable this setting to log each time an application launches. Note that enabling this option generates a large volume of log information.

- **Log application launch requiring elevated privileges** - Enable this setting to log each time PowerBroker Desktops detects an executed application requiring elevated privileges above Standard User.

- **Log application launch with Action: Deny Execution** - Enable this setting to log each time an application launch is denied due to PowerBroker Desktops.

- **Log application launch with modified token** - Enable this setting to log each time an application launches that has had its privileges modified by PowerBroker Desktops.

- **Log application launch with Action: No Change (passive)** - Enable this setting to log each time a whitelisted application is launched with no changes to permissions, privileges, process security, or integrity level.

- **Log application launch elevated by Shell rule** - Log each time a user launches an application using the Shell rule capability of PowerBroker Desktops.

- **Log ActiveX install with rule applied** - Log each time an ActiveX control installation has its privileges modified by PowerBroker Desktops.

- **Log ActiveX install failure due to insufficient privileges** - Log each time an ActiveX control fails to install due to insufficient privileges.

- **Log UAC prompts** - Log all client UAC prompts. This is useful for determining when user is asking for administrative privileges.

There are many other settings available in the BeyondTrust Administrative Template. For more information about the available settings, see “Appendix B: Administrative Template Settings,” page 173.

Most settings for client-side logging are configured in the Security Driver collection of the Administrative Template. The Security Driver collection is located under the Administrative Templates node of the Group Policy Management Editor.
Note: If you installed and configured Auditing and Reporting (PBReports), then you have already configured the policy settings for logging for data collection. For information about installing and configuring Auditing and Reporting, see the *PowerBroker Desktops Installation Guide*.

To configure logging for data collection:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.

2. In the Group Policy Management Editor, click **Computer Configuration** or **User Configuration**, **Administrative Templates**, **BeyondTrust**, **PowerBroker Desktops**, **System**, **Security Driver**.

   If you are using an older operating system such as Windows Server 2003 or Windows XP and this path does not exist, you may need to manually install the Administrative Template. For more information, see “Installing the BeyondTrust Administrative Template,” page 174.

3. For each of the following policy settings, double-click the setting to open its properties dialog, click **Enabled**, configure any options, and click **OK**.
   - Log ActiveX install with rule applied
   - Log ActiveX install failure due to insufficient privileges
   - Log application launch requiring elevated privileges
   - Log all application launches
   - Log application launch with Action: Deny Execution
   - Log application launch with modified token
• Log application launch with Action: No Change (passive)
• Log application launch elevated by Shell Rule
• Log UAC prompts

Events are logged in the **System** section of the Event Log on client computers. For information about the Event Log or about using logging for troubleshooting, see “Troubleshooting Mechanisms,” page 160.
Backing Up a GPO

PowerBroker Desktops can create up to three GPO backup files using standard GPO backup procedures. These files contain the rule XML code that defines each rule you have created. You could create a backup file to store in a source control system for version control or to import into a PowerBroker Desktops utility such as PBDeploy.

The location of the GPO backup files on a computer running the PowerBroker Desktops snap-in depends on the operating system.

- For Windows Server 2008, Windows 7, or Windows Vista
  C:\ProgramData\BeyondTrust\PowerBroker Desktops\GPOBackupData

- For Windows Server 2003 or Windows XP
  C:\Documents and Settings\All Users\Application Data\BeyondTrust\PowerBroker Desktops\GPOBackupData

The following naming conventions are used for the GPO backup file names:

- AppSecComp_<GPOName>.xml
- AppSecUser_<GPOName>.xml

Backup File Name Examples

The following list shows examples of typical GPO backup file names:

- AppSecUser_<GPOName>.xml
- AppSecUser_<GPOName>.xml.bk1
- AppSecUser_<GPOName>.xml.bk2
- AppSecUser_<GPOName>.xml.bk3

As a result of the Microsoft Application Data Folder Security rules when multiple non-administrator users create Group Policy rules on the same computer, only the snap-in user that created the GPO or snap-in users with administrator permissions are allowed to update the backup files. To avoid permission problems, grant the user the appropriate permissions in the GPOBackupData folder.
Editing the XML Source Code of a Rule

PowerBroker Desktops rules are XML-based. You can make changes to an existing rule in the Properties dialog of the rule. (For more information, see “Creating or Editing a Rule with the Properties Dialog,” page 47.) However, if you are familiar with XML, you can also view and edit the XML source code of a rule.

You can view the XML source code of a rule by viewing an XML settings report. For more information, see “Viewing a Settings Report,” page 50.

To manually edit the XML source code of a rule:

1. Drag and drop (or copy and paste) a rule from the Group Policy Management Editor to your desktop or another folder on your computer.
2. Open the rule source file in an XML editor so that you can manually edit the source code of the rule.
3. Drag and drop the changed rule source file back into the Group Policy Management Editor.

Tip: Using XML Integration

XML integration in other software makes PowerBroker Desktops XML integration an even more valuable prospect for administrators. XML configuration data can be seamlessly transferred between PowerBroker Desktops and other applications such as Microsoft Word, Access, or Excel. Office documents can be directed at live configuration data to produce up-to-date settings reports on an ongoing basis.
Troubleshooting

This section answers common questions about using PowerBroker Desktops and provides information about troubleshooting mechanisms and performing logging and tracing.

For information about troubleshooting specific issues, see the following topics:

- “Rules Have No Effect,” page 154
- “Compatibility Issues with Some Applications,” page 156
- “Problems Requiring Process-Specific Access Rights,” page 156
- “Other Problems,” page 159

For information about logging, tracing, event log messages, and the Policy Monitor utility, see “Troubleshooting Mechanisms,” page 160.

Rules Have No Effect

If you have configured rules but they are having no effect, review the following questions.

**Have you deployed the client software?**
The PowerBroker Desktops client software must be installed on a computer if the computer is to recognize rules and policy settings.

The client software is not installed by the snap-in installer. You must separately download the client software from the BeyondTrust website and install and deploy it.

In addition, if you have not rebooted the computer after installing the client software, rules will not be recognized. You must reboot the client computer to complete the client installation process.

**Have you linked the GPO to an organizational unit and refreshed Group Policy?**
You must link a GPO to an organizational unit (OU) for rules in that GPO to be applied to users or computers in that OU. Also, Group Policy must be refreshed before new rules or changes to rules will take effect.

**Have you placed rules under Computer Configuration or User Configuration as required?**
Rules can be created for either the Computer Configuration or the User Configuration of a GPO. You must select the correct location for a rule.
If the user is a member of Administrators, have you resolved process ownership issues?
When the user launching an executable is a member of the Administrators security group, the process token may be owned by the Administrators group rather than by the user. On Windows XP and Windows Server 2003, this behavior is optional, and the default is to give the user ownership of processes. However, on these newer operating systems, this default may be changed by creating a PowerBroker Desktops policy.

If the process token is owned by Administrators and the Administrators group is removed, BeyondTrust gives ownership of the process to the user who launched the process (if this is not already the case). By default, this does not result in any change on Windows XP or Windows Server 2003. If the Administrators group was the owner and ownership is changed to the user, any object (such as a file or registry setting) that is created by the process is owned by the user.

The newer behavior (implemented by default on Windows XP and Windows 2003 and as modified by BeyondTrust when necessary) provides an improved audit trail of object creation because new objects are associated with the specific user who created them.

Have you ensured that multiple rules do not conflict?
PowerBroker Desktops processes rules according to standard Group Policy processing methodology. Within each Group Policy Object (GPO), rules are processed sequentially from highest order number to lowest, and only the first rule that targets an application takes effect. If user and computer rules are competing for the same process, user policy takes priority over computer policy. For more information, see “Arranging the Order of Rules,” page 104.

Note: If you are using PowerBroker Desktops rules in multiple GPOs and those rules have the potential to impact the same application, you must also arrange the GPOs according to the intended order of processing. GPOs are processed sequentially from highest precedence number to lowest. If two GPOs each contain a PowerBroker Desktops rule that configures security for the same application, both rules take effect in sequence. The rule in the GPO with the lowest precedence number wins because it is the last to be applied.

Have you analyzed the situation using logging and tracing options?
For information about logging and tracing, see “Troubleshooting Mechanisms,” page 160.
Compatibility Issues with Some Applications

When some applications launch, they attempt to unload a PowerBroker Desktops DLL file (btpload32.dll). Unloading this file can cause system instability and other problems and is not recommended.

To prevent this DLL from being unloaded by an application, you can add a key to the Windows registry. This key blocks the unload operation even if the process name and path are found in the registry key value.

To add this key to the registry, do the following:

1. In the Group Policy Management Editor, navigate to the Security Driver section of the BeyondTrust Administrative Template. For more information, see "Appendix B: Administrative Template Settings".
2. In the list of Security Driver options, select Prevent Btpload from being unloaded from the specified process.
3. Enter the path to the executable file that attempts to unload Btpload.
4. Click OK.

The application specified in the path setting will have the following DLLs loaded: btpload32.dll btprof32.dll privman32.dll.

Problems Requiring Process-Specific Access Rights

In most cases, it is not necessary to grant process-specific access rights to elevate an application. However, if attempts to elevate a particular application have failed or caused problems, granting process-specific access rights may be necessary.

The following are examples of situations in which you may need to grant process-specific access rights:

- If printer connections that have been installed on a computer are missing after you have attempted to elevate an application that uses the built-in printer dialog, try granting the PROCESS_DUP_HANDLE access right to see if it resolves the problem.
- If an application returns a duplicate handle error, try granting the PROCESS_DUP_HANDLE access right to see if it resolves the problem.
- If an application uses remote procedure calls and your attempts to elevate the application have been unsuccessful, try granting the PROCESS_DUP_HANDLE access right to see if it resolves the problem.
- If you are unable to stop an application after elevating it, try granting the PROCESSS_TERMINATE access right to see if it resolves the problem.
More generally, if you have attempted to elevate an application and the attempt has failed, then as a troubleshooting measure you can try granting all of the process-specific access rights. If that resolves the problem, then it is recommended that you experiment to determine the minimum process-specific access rights that are needed and grant only those that are required by the application that you are elevating.

---

**Caution: Permitting Writing to Memory**

Because process-specific access rights that permit writing to process memory have the potential to be misused to hijack a process and write malicious code into memory, you should grant only the minimum process-specific access rights required.

---

To grant process-specific access rights in a rule:

1. Open the Group Policy Management Editor and double-click the rule to which you want to add process-specific access rights.

2. In the Properties dialog for the rule, review the **Action** selected on the **Application** tab.

   - If the action is **Run application(s) with custom token**, click the **Token** tab and continue to step 3.

   - Otherwise, the token is automatically configured by the action and you must manually configure the token instead. To make this change:
     a. Click the **Token** tab and record the permissions, privileges, process security, and integrity level currently configured.
     b. Click the **Application** tab and change the action to **Run application(s) with custom token**.
     c. Click the **Token** tab and configure the permissions, privileges, and integrity level to match what you recorded. For more information, see “Configuring Token Security,” page 88.
3. In the **Process Security** box on the **Token** tab, click the **Change** button.

4. In the **Process Security** dialog, select process-specific access rights (flags) beginning with **PROCESS** as necessary, and then click **OK**.

5. In the Properties dialog, click **OK**.

**Note:** The READ_CONTROL, SYNCHRONIZE, and GENERIC_READ rights are required and cannot be deselected. By default, no other rights are selected.

For more information about process security settings, see [Process Security and Access Rights](#) on the MSDN website.
Other Problems

This section provides information about other problems users occasionally have encountered.

**PowerBroker Desktops Components not displayed or installed**
If the prerequisites for a component are not met before installation, that component will not be installed nor will it be displayed under Custom Setup during installation.

For information about snap-in and client software requirements, see the *PowerBroker Desktops Installation Guide*.

**Installing client triggers anti-spyware warning**
Installing the client causes some anti-spyware programs to display warnings or errors because it installs a browser helper object. The BeyondTrust Browser Helper is required for ActiveX rules.

You can configure anti-spyware to allow the BeyondTrust Browser Helper. It is located in the system32 folder and is named pmbho.dll.

You can install the PowerBroker Desktops client without the Browser Helper and therefore without the ActiveX rule functionality. For instructions, see the Knowledge Base. You can access the Knowledge Base by logging into the BeyondTrust website using the password provided to you by BeyondTrust, clicking **Customer Support Center**, and then clicking the **PowerBroker Desktops** logo in the Knowledge Base pane.

**Unable to apply a rule to a 16-bit application**
When elevating 16-bit applications, the rule may not trigger when you run the application or you may see a **RULE--NOT--APPLIED** message in the Policy Monitor.

The reason for this is that some 16-bit applications do not appear as distinct processes, but rather are run in the Windows 16-bit Virtual DOS Machine (**ntvdm.exe**). The 16-bit applications also need to be run in a separate memory space to properly adjust the application’s process token.

If the application is not displaying in Policy Monitor, it is likely that **ntvdm.exe** is controlling the process. When this is the case, it may be necessary to write a rule for **ntvdm.exe**.

If you get a rule match but see a **RULE--NOT--APPLIED** message, configure the process to run in a separate memory space by doing the following:
1. Create a shortcut to the application.
2. Right-click the shortcut and select **Properties**.
3. Click **Advanced**.
4. Select the **Run in separate memory space** check box.
Passcode does not work
Passcodes provide one-time access and cannot be reused to launch an application a second time. If a user needing immediate access sends an Authorization Code to request access, closes the authorization dialog before entering a Passcode, attempts to launch the application a second time, and enters the Passcode received for the first launch attempt, access is denied. The user must request a new Passcode for the new launch attempt.

Authorization Codes and Passcodes are generated using a key pair that includes a public key and a private key. The public key must be installed on client computers, and the private key must be installed on computers used to generate Passcodes. For more information, see “Generating a Passcode to Respond to a Message,” page 132.

Troubleshooting Mechanisms
PowerBroker Desktops supports several mechanisms for troubleshooting client-side extension (CSE) operation. These include:

- “Event Logging,” page 160
- “Tracing with Policy Monitor,” page 165
- “Trace Logging,” page 166
- “Resultant Set of Policy (RSoP) Reporting,” page 167
- “Windows User Environment Log (userenv.log),” page 168
- “Status Messages,” page 169

Note: To configure logging for data collection rather than troubleshooting, see “Configuring Logging for Data Collection,” page 149.

Event Logging
PowerBroker Desktops events are written to the Windows Event Log and can be viewed in the Event Viewer. Events related to PowerBroker Desktops appear in the Event Log under either the System section or the Application section.

Client-side extension (CSE) event logging of errors is always enabled. By using the BeyondTrust Administrative Template, you can enable additional categories of event log messages, such as warnings and informational messages. An example of a typical event log warning is a failed ActiveX control installation attempt. An example of a typical informational message is the success of an individual policy setting.

For information about initial configuration of logging, see “Configuring Logging for Data Collection,” page 149. For information about further configuring logging for troubleshooting, see “Trace Logging,” page 166.
When logging for PowerBroker Desktops is enabled in the Administrative Template, messages and errors are sent from several components. The source of the event and the event ID are included in the log. A privman event source usually indicates a client-side event, while a PowerBroker Desktops event source usually indicates an event related to the snap-in.

In the Event Viewer, a typical Event Log segment looks like the following.

In this example, an information message was sent from the Privman component with an event ID of 28675, indicating that the Security Driver loaded correctly on the client computer.

In the Event Viewer, double-click the row for an event to display additional information about it. Some event messages also include information about application privileges, permissions, and user credentials.
If policy settings do not appear to be reaching client computers, look for the following events in the System section of the Windows Event Log.

**Common PowerBroker Desktops Messages**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message Text</th>
<th>Event Source</th>
<th>Event Log Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>28691</td>
<td>PowerBroker Desktops detected the launch of an application with insufficient privileges when running under a standard user account</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28692</td>
<td>PowerBroker Desktops detected the launch of an application</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28693</td>
<td>PowerBroker Desktops modified the privileges of an application at launch</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28694</td>
<td>PowerBroker Desktops modified the privileges of an application at launch by request of a user</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28695</td>
<td>PowerBroker Desktops modified the privileges of an ActiveX control installation</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28696</td>
<td>PowerBroker Desktops detected insufficient privileges to install an ActiveX control</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28697</td>
<td>PowerBroker Desktops detected a UAC prompt</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28698</td>
<td>PowerBroker Desktops detected a denied application launch.</td>
<td>privman</td>
<td>System</td>
</tr>
<tr>
<td>28699</td>
<td>PowerBroker Desktops detected the launch of an application with no change to the process.</td>
<td>privman</td>
<td>System</td>
</tr>
</tbody>
</table>

**Using the Event Viewer**

To open the Windows Event Viewer:

1. In Windows, click **Start, Administrative Tools, Event Viewer**. Alternatively, you can enter `eventvwr` in a search box or at a command prompt.
2. If prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the Event Viewer, under **Windows Logs** review the **System** and **Application** sections of the log for events and messages described in the preceding table.
System Log Events

System events usually relate to rule implementation and application usage. PowerBroker Desktops events in the System portion of the event log display a source name of privman.

Additional detail about an event is available by double-clicking the event in the Event Viewer. This opens the Event Properties dialog where the event is described in detail. The following is a typical System Event Properties dialog.
Application Log Events

Events written to the Application section of the Windows event log involve policy processing and licensing. These events display their source as PowerBroker Desktops or PowerBroker Desktops License.

The following is a typical application log segment.

Additional detail about an event is available by double-clicking the event in the Event Viewer. This opens the Event Properties dialog where the event is described in detail. The following is a typical Application Event Properties dialog.
Tracing with Policy Monitor

Client-side extension (CSE) tracing is disabled by default and can be enabled by using the BeyondTrust Administrative Template within Microsoft’s Administrative Templates policy extension. This Administrative Template includes policy settings for the control of standard CSE behaviors, the size and location of each CSE trace file, and the quantity of event logging. Tracing provides detailed output on each CSE’s operation in a simple text format.

When the PowerBroker Desktops snap-in extensions are installed, the BeyondTrust Administrative Template is installed into the default location for administrative templates. If you are using an older operating system, you may need to manually import the BeyondTrust Administrative Template.

For information about initial configuration of logging, see “Configuring Logging for Data Collection,” page 149. For information about turning on trace logging for troubleshooting, see “Trace Logging,” page 166.

Policy Monitor

The client-side troubleshooting utility called Policy Monitor (polmon.exe) runs on a client computer. This utility monitors all processes running on the client and displays information about each process, including the full path of the launching process and other details pertinent to rule operation.

This utility is particularly useful for determining the state of the client, and for diagnosing problems when a rule does not function as expected on the client.

The following is an excerpt from a typical Policy Monitor trace:

To perform tracing with Policy Monitor:
1. Navigate to the %windir%\system32 folder.
2. Double-click polmon.exe to launch Policy Monitor. An entry is displayed in Policy Monitor for each process running on the computer.
3. From a command prompt, run `gpupdate /force`. An entry is listed in Policy Monitor for each rule applied, as well as for other processes.

4. Launch an application or process to which a rule has been applied. The full path of the launching process, any matches found, and any rules applied are displayed in the Policy Monitor.

   **Note:** If the path is listed, but there is no mention of a command line match or rule being applied, then the process was not recognized as one to which a rule should have been applied. This result typically occurs if the rule was not configured correctly.

For more information about using Policy Monitor, see Knowledge Base article 10408 on the BeyondTrust website. You can access the Knowledge Base by logging into the BeyondTrust website using the password provided to you by BeyondTrust, clicking Customer Support Center, and then clicking the PowerBroker Desktops logo in the Knowledge Base pane.

### Trace Logging

**Note:** For information about initial configuration of logging, see “Configuring Logging for Data Collection,” page 149.

To turn on trace logging for troubleshooting by using the BeyondTrust Administrative Template:

1. Edit a Group Policy Object (GPO). For detailed instructions, see “Creating or Editing a GPO,” page 28.

2. Click **Computer Configuration, Policies, Administrative Templates, BeyondTrust, PowerBroker Desktops, System**.
   If you are using an older operating system such as Windows Server 2003 or Windows XP and this path does not exist, you may need to manually install the Administrative Template. For more information, see “Installing the BeyondTrust Administrative Template,” page 174.

3. If an application is not launching correctly, you can configure Security Driver logging options to generate a trace log that you can send to BeyondTrust Support for assistance.

   **Note:** This policy setting should be enabled only for troubleshooting and only temporarily. If left enabled, it can degrade performance.

   To generate this trace log, do the following:

   a. In the console tree, click **Security Driver**, then double-click **Log Security Driver events** in the details pane.
   b. Click **Enabled**, then configure logging and tracing options.
   c. Click **OK**.

4. If policy settings are failing to reach client computers, you can configure PowerBroker Desktops policy processing options to generate a trace log.
The log file generated is named pmuser.log if for user policy or pmcomp.log if for computer policy.

**Note:** This policy setting should be enabled only for troubleshooting and only temporarily. If left enabled, it can degrade performance.

To generate this trace log, do the following:

- In the console tree, click **Group Policy**.
- Double-click **PowerBroker Desktops Policy Processing** in the details pane.
- Click **Enabled**, then scroll down and configure logging and tracing options.
- Click **OK**.
- Double-click **PowerBroker Desktops Licensing Policy Processing** in the details pane.
- Click **Enabled**, then scroll down and configure logging and tracing options.
- Click **OK**.

For more information, see the following:

- “Troubleshooting Mechanisms,” page 160
- “Appendix B: Administrative Template Settings,” page 173

### Resultant Set of Policy (RSoP) Reporting

Computers running Windows XP support RSoP logging by client-side extensions (CSEs). Windows Server 2003 also supports RSoP planning mode. RSoP logging and planning mode data may be viewed in the RSoP snap-in, as presented by each snap-in extension.

**Note:** Microsoft has deprecated the RSoP snap-in for Windows Vista or later and Windows Server 2008 or later. For these operating systems, the RSoP snap-in still includes all PowerBroker Desktops policy settings but may not include all Microsoft policy settings. To view all computer policy settings applied or all user policy settings applied, you can use the Group Policy Results or Group Policy Modeling options in the Group Policy Management Console (GPMC) or the GPResult command-line tool. For more information, see Microsoft TechNet.
Logging Mode

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

Typical RSoP snap-in extensions provide RSoP reporting data within a read-only user interface similar to that implemented by the corresponding Group Policy Management Editor snap-in extensions. This means that each properties dialog for each item must be viewed to see the configuration results. PowerBroker Desktops RSoP extensions each implement a single node. Clicking this node displays a detailed HTML report in the MMC result view. This report shows the results of all settings applied by that particular extension.

Tip: Displaying the XML for an RSoP report
Selecting the XML toolbar icon presents the XML associated with the displayed RSoP report and contains more detailed information.

Planning Mode

PowerBroker Desktops extensions support planning mode. RSoP planning is a simulation process that uses the WMI repository similarly to RSoP logging. However, in contrast to logging mode, CSEs are launched by the server and are directed to not perform actual configuration – instead they report to WMI as if they had. This allows the administrator to view the same type of data as in logging mode, without actually performing configurations.

In planning mode, PowerBroker Desktops assumes all item-level targeting items pass. Note that this behavior includes items such as Security Group and Computer, regardless of administrator choices in the planning mode wizard.

For more information about RSoP, see the Microsoft TechNet website.

Windows User Environment Log (userenv.log)

If Group Policy is failing to apply policy settings and using PowerBroker Desktops client-side tracing and event logging has not helped you identify the problem, configuring verbose logging for the Windows User Environment Log may produce helpful troubleshooting information.
The User Environment Log is a text log file written by Winlogon. This file contains general information about the user environment and about the execution of individual Group Policy CSEs. Because the information that is logged is generic to all CSEs and the policy environment, this log fully supports and reports about PowerBroker Desktops policy processing. The log is created in the following location:

%SystemRoot%\Debug\UserMode\userenv.log

You can control the level of logging by creating and configuring the following registry value:

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

You can disable logging or set the level of logging to either normal or verbose logging directed to a log file:

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Value Data (Hexadecimal)</th>
<th>Value Data (Decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No logging</td>
<td>0x00000000</td>
<td>0</td>
</tr>
<tr>
<td>Normal logging to a log file</td>
<td>0x00010001</td>
<td>65537</td>
</tr>
<tr>
<td>Verbose logging to a log file</td>
<td>0x00010002</td>
<td>65538</td>
</tr>
</tbody>
</table>

For more information about the User Environment Log, see Microsoft TechNet.

### Status Messages

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

PowerBroker Desktops extensions can write status messages, providing additional information. The status window accepts both normal and verbose levels of messaging. By default, the level is set to normal.

Verbose status messages can be enabled by creating and configuring the following registry value:

Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name:VerboseStatus
Value Type: REG_DWORD
Value Data: 0x00000001 (1)
Appendix A: Group Policy Primer

If you are new to Group Policy, or are unfamiliar with how to create and edit a GPO, this appendix provides an introduction to Group Policy and instructions for creating and editing a Group Policy Object (GPO).

Basic Group Policy Concepts

Group Policy is a framework for user and computer configuration on Windows computers that are members of Active Directory. Group Policy makes some fundamental assumptions about how users and computers should be configured in an enterprise environment.

The primary assumption is that desired configurations are often common across multiple users and computers. These groupings often reflect organizational structure.

Organization

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

Group Policy Objects and Storage

A Group Policy Object (GPO) is a collection of configuration settings that can be applied to certain users or computers (or both) based on their membership in a site, domain, or organizational unit. Each GPO has a name and a globally unique identifier (GUID).

A GPO consists primarily of data that is stored in two distinct locations on a network:

- **Group Policy Container (GPC)** - Holds system and policy settings data that is stored in the Active Directory and associated with the GPO by its GUID.

- **Group Policy Template (GPT)** - Stores the actual configuration settings.

All GPO data is synchronized to all domain controllers on a given domain.
Editing Group Policy

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

Applying Group Policy

Policy settings are applied by Client Side Extensions (CSEs). Processing of GPO settings by CSEs is periodically initiated by the Winlogon operating system process. Settings are organized into user and computer configurations. Winlogon initiates processing of user settings during user logon, and computer settings during computer boot. This is known as foreground processing.

Additionally, both user and computer configuration are initiated periodically, which is known as background processing. By default, background processing occurs every 90 minutes (with a random offset of 0 to 30 minutes), or every 5 minutes on domain controllers, although the parameters are subject to change by a Group Policy administrator. Some extensions support only user or computer configuration, and some support only foreground processing.

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

Group Policy Reporting

The architecture for Group Policy reporting is called Resultant Set of Policy (RSoP). RSoP consists of two distinct modes:

- **Planning** - Shows what the Group Policy does when it is activated
- **Logging** - Group Policy’s reporting system. RSoP reports use data generated by CSEs that implement the RSoP reporting interface on Windows XP and later computers.
The RSoP MMC snap-in is the primary tool for viewing Group Policy results. Like the GPME, the RSoP snap-in integrates various plug-ins known as RSoP snap-in extensions. Each extension reports on the configuration results from the last execution of its corresponding CSE for a particular computer or user.

**Creating or Editing a GPO**

For information about how to create or edit a GPO, see “Creating or Editing a GPO,” page 28.
Appendix B: Administrative Template Settings

The PowerBroker Desktops Administrative Templates enable you to configure PowerBroker Desktops extensions (including logging and tracing options) and manage administrator access to the Group Policy Management Editor and Resultant Set of Policy (RSoP) snap-ins.

To accommodate different Windows Server and Windows operating systems, two versions of the BeyondTrust Administrative Template are available. If you are using Windows Server 2008, Windows 7, or Windows Vista, the ADMX/ADML version of the BeyondTrust Administrative Template is installed and added to the Group Policy Management Editor automatically when you install the snap-in. It includes the following files:

- **Beyondtrust.pbd.admx** - This template file provides Administrative Template settings.

- **Beyondtrust.pbd.adml** - This template file is a language file and is used to display text in the user interface for the Administrative Template settings. It is also used for internationalization. It is stored under: ...

  \windows\policydefinitions\en-us

If you are using Windows Server 2003 or Windows XP, the ADM version of the BeyondTrust Administrative Template, **Beyondtrust.pbd.adm**, is installed automatically when you install the snap-in, but you must manually add the BeyondTrust Administrative Template to the Group Policy Object Editor. The ADM file provides Administrative Template settings and is used to display text in the user interface for those settings. For more information, see “Installing the BeyondTrust Administrative Template,” page 174.
In the Group Policy Management Editor, the Security Driver collection in the BeyondTrust Administrative Template looks like the following. You can double-click a setting to view its properties and configure it.

For more about using the BeyondTrust Administrative Template, see the following:

- “Configuring Logging for Data Collection,” page 149
- “Troubleshooting Mechanisms,” page 160

**Installing the BeyondTrust Administrative Template**

If you are using an older operating system such as Windows Server 2003 or Windows XP, you may need to manually add the ADM version of the BeyondTrust Administrative Template to the Group Policy Object Editor. Although the Administrative Template is installed along with the PowerBroker Desktops snap-in, you must add the Administrative Template to the Group Policy Object Editor so that you can access the settings.

**Tip: Newer Operating Systems**

If you are using Windows Server 2008, Windows 7, Windows Vista, or later operating systems, the ADMX/ADML version of the BeyondTrust Administrative Template is added for you automatically when you install the PowerBroker Desktops snap-in. The Administrative Template settings are displayed in the Group Policy Management Editor.
If you have a previous version of the BeyondTrust Administrative Template installed, you should remove it and add the V5.3 Administrative Template to incorporate the features of this version.

To add or update the ADM version of the BeyondTrust Administrative Template:

1. Edit a Group Policy Object (GPO) in the Group Policy Object Editor or Group Policy Management Editor. For detailed instructions, see “Creating or Editing a GPO,” page 28.

2. In the Group Policy Object Editor or Group Policy Management Editor, click Computer Configuration, right-click Administrative Templates, and then select Add/Remove Templates. The Add/Remove Templates dialog displays a list of Current Policy Templates.

3. If BeyondTrust is not in the list of Current Policy Templates, click Add and find the template in the C:\windows\inf folder.

4. Double-click BeyondTrust.pbd.adm and then click Close. For this GPO, the following paths are added to the Group Policy Object Editor:
   - Computer Configuration, Policies, Administrative Templates, BeyondTrust
   - User Configuration, Policies, Administrative Templates, BeyondTrust

For more about the BeyondTrust Administrative Template, see the following:

- “Configuring Logging for Data Collection,” page 149
- “Troubleshooting Mechanisms,” page 160

**Group Policy Processing Settings**

The following policy settings for managing PowerBroker Desktops policy processing and license policy processing are available in the BeyondTrust Administrative Template.
Policy Processing Settings

The following table provides the PowerBroker Desktops policy processing settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Path in the Group Policy Management Editor</th>
</tr>
</thead>
</table>
| PowerBroker Desktops Policy Processing | PowerBroker Desktops client-side extension (CSE) policy processing settings and tracing and logging options. Available options include:  
• Allow processing across a slow connection  
• Configure background priority  
• Configure event logging  
• Turn tracing on or off  
• Specify trace file locations and maximum size | Computer Configuration, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Group Policy |
| PowerBroker Desktops (GPME) | If disabled, the PowerBroker Desktops extension is not displayed for administrators targeted by the GPO. Similar options exist for Computer Security, User Security, and the View Extension. | User Configuration, Administrative Templates, BeyondTrust, PowerBroker Desktops, Windows Components, Microsoft Management Console, Restricted/Permitted snap-ins, Group Policy, Group Policy Snap-in Extensions |
| PowerBroker Desktops (RSOP) | If disabled, information related to the PowerBroker Desktops extension is not displayed in the Resultant Set of Policy console. Similar options exist for Computer Security and User Security. | User Configuration, Administrative Templates, BeyondTrust, PowerBroker Desktops, Windows Components, Microsoft Management Console, Restricted/Permitted snap-ins, Group Policy, Resultant Set of Policy Snap-in Extensions |

License Policy Processing Settings

The following table provides the License policy processing settings. You access these settings at **Computer Configuration, Policies, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Group Policy**.

The following setting is available:
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Licensing Policy Processing | PowerBroker Desktops licensing client-side extension (CSE) policy processing settings and tracing and logging options for the range of versions indicated.  
• Available options include:  
• Configure event logging  
• Turn tracing on or off  
• Computer trace  
• Planning trace  
• Specify trace file locations and maximum size |

For information about licensing, see “Licensing” in the *PowerBroker Desktops Installation Guide.*

## Logging and Tracing Settings

The BeyondTrust Administrative Template includes options for configuring logging and tracing, either for troubleshooting or for data collection.

PowerBroker Desktops can be configured to log events to the Windows event log. This information is useful when troubleshooting problems or analyzing the implementation of rules. For more information, see “Troubleshooting Mechanisms,” page 160, and “Configuring Logging for Data Collection,” page 149.

A tracing utility called Policy Monitor (*polmon.exe*) is provided with PowerBroker Desktops. Policy Monitor monitors the operation and activities of the client-side extensions (CSEs) running on a client computer. For more information, see “Tracing with Policy Monitor,” page 165.

PowerBroker Desktops Auditing and Reporting (PBReports) uses log information to generate audit data and reports about administrator and user rights, rules applied, and application usage. For more information, see “Viewing and Managing Reports,” page 135.

## Security Driver Settings

The Security Driver collection includes settings related to logging and other operating features. You can view and configure the properties of an Administrative Template setting by double-clicking it.

You can find the security driver settings under **Computer Configuration, Policies, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Security Driver** in the Group Policy Management Editor.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ActiveX install with rule applied</td>
<td>Logs ActiveX control installation requiring a privilege modification.</td>
</tr>
<tr>
<td>Log ActiveX install failure due to insufficient privileges</td>
<td>Logs failed ActiveX control install due to insufficient privileges.</td>
</tr>
<tr>
<td>Log application launch requiring elevated privileges</td>
<td>Logs every application launch requiring privileges greater than standard user.</td>
</tr>
<tr>
<td>Log all application launches</td>
<td>Logs every application launch.</td>
</tr>
<tr>
<td>Log application launch with Action: Deny Execution</td>
<td>Logs each time an application launch is denied execution by PowerBroker Desktops.</td>
</tr>
<tr>
<td>Log application launch with modified token</td>
<td>Logs each application launch for which the token has been modified by PowerBroker Desktops.</td>
</tr>
<tr>
<td>Log application launch with Action: No Change (passive)</td>
<td>Logs each time a whitelisted application launches with no changes to permissions, privileges, process security, or integrity level.</td>
</tr>
<tr>
<td>Log application launch elevated by Shell rule</td>
<td>Logs each launch performed by a Shell rule.</td>
</tr>
<tr>
<td>Block ActiveX install based on CLSID</td>
<td>Blocks the installation of an ActiveX control based on the control’s COM Class Identifier (CLSID).</td>
</tr>
<tr>
<td>Log application state data</td>
<td>Activates logging on clients to support the Automatic Rule Generator and SCCM reporting. (Not used by Auditing and Reporting.)</td>
</tr>
<tr>
<td>Prevent application from having rules applied</td>
<td>Activates BTSupressHook feature to exempt application from rules</td>
</tr>
<tr>
<td>Prevent Profiler from being loaded into specified process</td>
<td>Used for troubleshooting only.</td>
</tr>
<tr>
<td>Prevent Privman from being loaded from specified process</td>
<td>Used for troubleshooting only.</td>
</tr>
<tr>
<td>Prevent Btpload from being unloaded into specified process</td>
<td>Used for troubleshooting only.</td>
</tr>
<tr>
<td>Customize IE download dialog</td>
<td>Allows customization of download progress dialog that appears when an end-user attempts to download. Available options include:</td>
</tr>
<tr>
<td></td>
<td>- Time after which to show progress dialog if less than a selected percentage complete</td>
</tr>
<tr>
<td></td>
<td>- Cancel button text</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Log Security Driver events</td>
<td>Security Driver logging and tracing options.</td>
</tr>
<tr>
<td></td>
<td>Available options include:</td>
</tr>
<tr>
<td></td>
<td>• Configure event logging</td>
</tr>
<tr>
<td></td>
<td>• Turn tracing on or off</td>
</tr>
<tr>
<td></td>
<td>• Specify trace file location and maximum size</td>
</tr>
<tr>
<td>Log UAC prompts</td>
<td>Logs each UAC prompt presented to user.</td>
</tr>
</tbody>
</table>
Appendix C: Additional Technical Information

This appendix provides additional technical information about the following topics related to PowerBroker Desktops.

- “Security Contexts,” page 180
- “WMI Namespace,” page 181

Security Contexts

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

Security Contexts Used by Group Policy

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

Security Contexts in PowerBroker Desktops

The PowerBroker Desktops CSE runs in SYSTEM context as computer policy and in the user's context as user policy.

Providing Network Access to the SYSTEM Context

SYSTEM does not have the network permissions of the logged-on user, although it can be given network access. SYSTEM is essentially the computer's user account. With Windows and Windows Server computers that are members of an Active Directory domain, you can add the computers into a security group. This security group can then be given permissions to any network resource on an Active Directory computer. This gives all SYSTEM accounts for client computers (that are members of the security group) access to the network resource.
**WMI Namespace**

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

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

ActiveX Control

A software component that provides interactive operation and additional features on a Web page, such as animation and menus.

Automatic Rule Generator

A software utility that gathers state model data from client computers and analyzes application use. Based on this analysis, the utility then constructs a set of rules customized to the applications and permissions required to launch the applications. These rules are reviewed by the administrator and then pasted into the snap-in. Beginning in PowerBroker Desktops V5.1, the Automatic Rule Generator has been functionally replaced by the PowerBroker Desktops Reporting Console.

Client-Side Extension (CSE)

As specified in the Microsoft Platform SDK, a true client-side extension (CSE) to Group Policy is a dynamic-link library that implements Group Policy on clients. Extensions are loaded by client computers only if needed when processing Group Policy.

Extension

Writing a Group Policy extension enables you to use your own data store for policy settings, create a richer user interface (UI) through the Group Policy Editor, or implement your own client-side processing for Group Policy.

Filters

See "item-level targeting."

gpupdate command

The gpupdate command refreshes local and Active Directory-based Group Policy settings, including security settings on the computer from where it is run. You can use gpupdate locally on Windows XP and later computers to refresh policy immediately.

Group Policy

An Active Directory-based system for applying management policy settings to users and computers, as originally specified by Microsoft.

Group Policy Management Console (GPMC)

Microsoft’s Group Policy Management Console, the unified console for managing Group Policy. The GPMC is accessed using Start, Control Panel, Administrative Tools, Group Policy Management. (The GPMC is available for free download from the Microsoft website.)
Group Policy Management Editor
The primary tool for editing policy settings in GPOs is the Group Policy Management Editor. The Group Policy Management Editor can be launched by editing a GPO in the GPMC.

Group Policy Object (GPO)
A collection of configuration settings that may be applied to users and/or computers by the Group Policy system built into Windows networks. A domain GPO consists of data in the SYSVOL and Active Directory, both of which are synchronized across all domain controllers. A GPO can contain multiple rules.

Hash Code
A numerical, hexadecimal value generated from a key (meaningful to the user) by means of a hashing function. When configuring a Hash rule, PowerBroker Desktops generates an SHA1 hash code from the executable selected and places it in the Hash field of the Properties box.

Item-level targeting
Item-level targeting enables you to target an individual rule or rule collection within a GPO to apply (or not apply) under specific conditions of hardware, software, and identity. If item-level targeting is applied to a rule, then the rule will not be processed by a particular computer or user if the targeting conditions are not met.

Microsoft Management Console (MMC)
The primary management console application for Microsoft Windows. The GPMC and RSoP consoles are MMC snap-ins.

MSI
File name extension for Microsoft installer packages.

Privilege Manager

Property
A configuration setting within a rule or other policy item.

Resultant Set of Policy (RSoP)
The Group Policy technology behind logging and planning reports and also a MMC snap-in for viewing planning and logging data.

Rule
A PowerBroker Desktops construct that determines how an application is elevated and launched. A rule is a policy item created using the PowerBroker Desktops snap-in and
applied to PowerBroker Desktops client computers by Group Policy update operation. Each GPO can contain multiple rules.

**Security Driver**
A driver that sits on the client computer, monitors process launches, and checks each against the rules that are communicated to the client through Group Policy. If a PowerBroker Desktops rule exists for the process, the security driver intercepts the process creation event and manipulates the token for that process embedding in it parameters related to the rule.

**SID**
Security identifier. A unique alphanumeric character string used to specify a user or group.

**Token**
A token contains the security information for a login session and identifies the user, the user’s groups, and the user’s privileges.

**Windows Management Instrumentation (WMI)**
Microsoft implementation of Web-Based Enterprise Management (WBEM), supporting the Common Information Model (CIM).

**Windows User Account Control (UAC)**
Microsoft security implementation introduced in Windows Vista. UAC enables common users to perform certain administrative tasks by prompting them for credentials using a dialog.
Index

A
actions 22, 34, 84, 104
Active Directory 170
ActiveX Details Report 138
ActiveX rule 75
Administrative Template
customizing the IE download dialog 130
installing 174
license policy processing settings 176
logging 149
policy processing settings 176
security driver settings 177
settings reference 173
Administrators group 155
application control 22, 34, 84, 104
Application Hash Details Report 144
Application Launch message 117
Application Path Details Report 145
Application tab 47
Applications by Computer Report 142
Applications by Hash Report 141
Applications by Path Report 139
Auditing and Reporting 26, 135
Auditing and Reporting Dashboard 136
Authorization Code 132

B
backup 26, 152
blacklisting 22, 34
Blocked Application message 121

C
CD/DVD rule 81
Certificate rule 61
changing a rule name 50
Client Side Extensions (CSEs) 171
collection rules 107
targeting items 101
creating a Group Policy Object 28
creating rules planning 32
using the Properties dialog 47
using the Reporting Console 43
using the Wizard 40
customizing
Internet Explorer 57, 75, 123-124, 130
right-click menu options 79, 126
UAC information dialog 127

D
dashboard
management See management dashboard
reporting See Auditing and Reporting Dashboard
debugging 154
digital signature 61

E
editing a Group Policy Object 28
Event Log 149, 160

F
Folder rule 67
globally unique identifier (GUID) 170
Group Policy concepts 170
Group Policy Management Console 28, 170
Group Policy Management Editor 28, 171
Group Policy Object (GPO) 28, 170
Group Policy Template 170
Hash rule 64
IE Download dialog 130
IE Elevation message 123
IE Failure message 124
installers, targeting 70, 72, 75
installing
    BeyondTrust Administrative Template 174
integrity level 23, 94
Internet Explorer
    customizing component failure dialog 124
    customizing download dialog 130
    customizing when elevated 123
elevate for specific website 57
item-level targeting 23, 98
knowledge base 13
license policy processing settings 176
location, targeting by 54, 67
logging
    for data collection 149
for troubleshooting 160
management dashboard 20, 30
messages 116
modifying token security
Integrity Level 23, 94
Permissions 23, 89
Privileges 23, 91
Process Security 93, 157
MSI Folder rule 72
MSI Path rule 70
On-Demand Elevation message 126
one-time access 96, 116, 132
Options tab 86, 96
order 104, 108
organizational unit (OU) 170
Passcode 132
Path rule 54
Permissions 23, 89
Policy Monitor 165
polmon.exe 165
PowerBroker Desktops 9
architecture 19
how it works 16
rule See rule
terminology 18
Privileges 23, 91
Process Security 93, 156
process token 18, 88
Publisher rule 61 options 86, 96

R

reporting

Reporting Console 43 rule type 32, 54
Reporting Services 135 token security 88
collection 104, 107 targeting See targeting

Reported Set of Policy (RSoP) 167 troubleshooting 154
services 135 types 32
settings reports 50 ActiVeX 75

reports, Reporting Services

ActiveX Details 138 CD/DVD 81
Application Hash Details 144 Certificate 61
Application Path Details 145 Hash 67
Applications by Computer 142 MSI Folder 72
Applications by Hash 141 MSI Path 70
Applications by Path 139 Path 54
Auditing and Reporting Dashboard 136 Publisher 61
Shell Executions 147 Shell 79
Resultant Set of Policy (RSoP) 167, 171 UAC 82

rule

changing name of 50 variables 111
changing name of 50 wildcards 37
changing name of 50 Wizard 40

confl icts 104, 107

creating security contexts 180
creating

planning security driver settings 177
planning

using the Properties dialog security group 89
using the Properties dialog

using the Reporting Console Security page 40
using the Reporting Console

using the Wizard security, process 93, 156
using the Wizard

modifying Settings Report 50
modifying

order 104, 108 Shell Executions Report 147
order

Properties 47 Shell rule 79
Properties

action 34, 84, 104 standard permissions 18
action

execution options 96 support 13, 154
execution options

item-level targeting 98
item-level targeting

BeyondTrust® August 17, 2012 189
<table>
<thead>
<tr>
<th>T</th>
<th>Windows process</th>
<th>See targeting, application or process</th>
</tr>
</thead>
<tbody>
<tr>
<td>targeting</td>
<td>32, 54, 98</td>
<td>WMI namespace 181</td>
</tr>
<tr>
<td>application or process</td>
<td>32, 54</td>
<td></td>
</tr>
<tr>
<td>by location</td>
<td>54, 67</td>
<td></td>
</tr>
<tr>
<td>regardless of location</td>
<td>37, 61, 64</td>
<td></td>
</tr>
<tr>
<td>computers</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>groups</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>installation files</td>
<td>70, 72, 79</td>
<td></td>
</tr>
<tr>
<td>installations through IE</td>
<td>57, 75</td>
<td></td>
</tr>
<tr>
<td>item-level targeting</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>miscellaneous options</td>
<td>86, 96, 98</td>
<td></td>
</tr>
<tr>
<td>network conditions</td>
<td>97-98</td>
<td></td>
</tr>
<tr>
<td>time frame</td>
<td>96, 98</td>
<td></td>
</tr>
<tr>
<td>users</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>variables</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>wildcards</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>targeting item collection</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>Token tab</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>tracing</td>
<td>165</td>
<td></td>
</tr>
<tr>
<td>troubleshooting</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>types of rules</td>
<td>See rule, types</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UAC Prompt Detected message</td>
<td>127</td>
</tr>
<tr>
<td>UAC Rule</td>
<td>82, 120, 127</td>
</tr>
<tr>
<td>user messages</td>
<td>See messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>variables</td>
<td>111</td>
</tr>
<tr>
<td>viewing reports</td>
<td>See reporting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>W</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>whitelisting</td>
<td>22, 34</td>
</tr>
<tr>
<td>wildcards</td>
<td>37</td>
</tr>
</tbody>
</table>