August 17, 2012

powerbroker® desktops

Installation Guide

Release 5.3

beyondtrust®
securing the perimeter within

www.beyondtrust.com
Corporate Headquarters
2173 Salk Avenue
Carlsbad, CA 92008

Phone: +1 818.575.4000

Revision/Update Information: August 17, 2012
Software Version: 5.3
Document Revision: 1

detours.lib Library
Microsoft Research Detours Package, Professional Version 2.1 Build_216.
DISCLAIMER AND LICENSE:
=======================

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

Contents

Introduction

This guide provides the installation instructions and software requirements for PowerBroker Desktops. For information about its features, benefits, functionality, and basic procedures, see the *PowerBroker Desktops User Guide*.

If you are upgrading from an earlier version of PowerBroker Desktops, follow the instructions in the *PowerBroker Desktops Upgrade Guide*.

The following sections include the document conventions, list of documentation for the product, and where to get additional product information and technical assistance.

Conventions Used in This Guide

Specific font and linespacing conventions are used in this book to ensure readability and to highlight important information such as commands, syntax, and examples.

Font Conventions

The font conventions used for this document are:

- `Courier New Font` is used for program names, commands, command arguments, directory paths, variable names, text input, text output, configuration file listings, and source code. For example:
  `C:\Documents and Settings\All Users`
- **`Courier New Bold Font`** is used for information that should be entered into the system exactly as shown. For example:
  `pbdeploy.exe`
- *`Courier New Italics Font`* is used for input variables that need to be replaced by actual values. In the following example, the variable *`MyServer`*, must be replaced by an actual environment server name and the variable *`MyFolder`* must be replaced by an actual folder name:
  `\\`*`MyServer`*`\`*`MyFolder`*`\pbdcl32.msi`
- **Bold** is used for Windows buttons. For example:
  Click **OK**.

Linespacing Conventions

The linespacing of commands, syntax, examples, and computer code in this manual may vary from actual Windows and Unix/Linux usage because of space limitations. For example, if the number of characters required for a single line does not fit within the text margins for this book, the text is displayed on two lines with the second line indented as shown in the following sample:

```
C:\Windows\SYSVOL\domain\Policies\<GUID>\<MACHINE or USER>
   \PBDesktops
```

Where to Go Next?

For licensing information and installation instructions for PowerBroker Desktops, see the *PowerBroker Desktops Installation Guide.*

For information about what you can do with PowerBroker Desktops and how to get started using PowerBroker Desktops, see the *PowerBroker Desktops User Guide.*

Documentation Set for PowerBroker Desktops

The complete PowerBroker Desktops documentation set includes the following:

- *PowerBroker Desktops Installation Guide*
- *PowerBroker Desktops User Guide*
- *PowerBroker Desktops Upgrade Guide: Upgrading from V5.x to V5.3*
- *PowerBroker Desktops Upgrade Guide: Upgrading from V4.x to V5.3*
- *PowerBroker Desktops* online help

Obtaining Support

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 Partner Portal on the BeyondTrust 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

Be sure to read this section 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.

Obtain as much information about the problem as possible using troubleshooting tools such as Policy Monitor, trace logging, event logging, and Resultant Set of Policy (RSoP) logging. For more information, see "Troubleshooting Mechanisms" in the *PowerBroker Desktops User Guide*.

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 or through the BeyondTrust website. If you are located in the United States, you can also contact technical support by telephone. Technical Support is staffed 24 hours per day, seven days per week.

Telephone: +1 800-234-9072

Email: `pbd-support@beyondtrust.com`

Web: To submit a support request online, do the following:

1. Browse to http://www.beyondtrust.com.
2. Click **Login** and log into the BeyondTrust Support website using the password provided to you by BeyondTrust.

3. After reading the Welcome message, scroll to the top of the **BeyondTrust Partner Portal** pane and click **Customer Support Center.**
4. Scroll down the page 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.

Installing PowerBroker Desktops Components

You must install two PowerBroker Desktops components. An optional reporting component can also be installed:

- **Snap-in** - This component must be installed on computers, usually domain controllers, used to edit Group Policy Objects (GPOs). This snap-in provides the ability to change the permissions and privileges of Windows applications using rules, thereby implementing a least privilege security model for Windows.

  You use the PowerBroker Desktops snap-in installer to install this component.
- **Client** - This component must be installed on each computer on which PowerBroker Desktops rules are enforced. This client software enables computers to recognize PowerBroker rules in GPOs.

  You can deploy this component to computers by using standard Windows functionality.
- **Reporting** - These components can be installed to provide auditing and reporting for application and process elevation. PowerBroker Desktops Reporting uses SQL Services Reporting Services.

For snap-in installation instructions, see "Installing the Snap-in," page 14. For client installation instructions, see "Installing PowerBroker Desktops Client Software," page 18. For Auditing and Reporting installation instructions, see "Installing and Configuring Auditing and Reporting (PBReports)," page 21.

Installation MSI Packages

The following table identifies installation MSI packages and the components installed by each. Note that separate installer files are provided for 32-bit and for 64-bit systems.

Table 1. PowerBroker Desktops Installation Components

Installer .MSI File	Contains and Installs

Snap-in installers:
`pbdsnap32.msi`
`pbdsnap64.msi`
	PowerBroker Desktops Snap-in
	Extensions to the Group Policy Management Editor and Resultant Set of Policy (RSoP) snap-ins. These extensions provide the ability to change permissions and privileges of Windows applications using rules. This component must be installed on computers used to edit GPOs.

	GPMC Integration Group Policy client-side extensions for planning and processing policy, including support for GPMC operations. These extensions are recommended for computers used to edit GPOs. They are not required for basic GPMC support.

Client installers:
`pbdcl32.msi`
`pbdcl64.msi`
	PowerBroker Desktops Client
	The client software contains a security driver that monitors process launch, checks for applicable rules, and modifies security token when a rule exists.
	The client software also provides client-side extensions used for creating and processing policy, enabling computers to recognize PowerBroker Desktops items in GPOs.
	The client software is normally distributed to computers using a distribution tool, such as Group Policy.

`pbdreporting.msi`	**PowerBroker Desktops Reporting** Installs the database for Auditing and Reporting and the RSS and RDL files required to generate reports for Reporting Services.

Software Requirements

PowerBroker Desktops can be used with a variety of Windows and Windows Server operating systems. The following sections detail the operating systems supported by each PowerBroker Desktops component.

Snap-in Requirements

The PowerBroker Desktops snap-in must be installed on computers that are used to edit GPOs. The snap-in can be installed on computers running any of the following operating systems:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 SP1 or later
- Windows 7
- Windows Vista
- Windows XP SP2 or later

Note: The .NET Framework V4.0 and .NET Framework V3.5 Features must be installed prior to installing PowerBroker Desktops. If .NET Framework V3.5 Features are installed, they may be listed under Features or Windows features rather than in the list of installed programs.

Client Software Requirements

PowerBroker Desktops client software can be installed on computers running any of the following operating systems:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 SP1 or later
- Windows 7
- Windows Vista
- Windows XP SP2 or later

Auditing and Reporting Software Requirements

PowerBroker Desktops Auditing and Reporting includes both a Reporting Console and Reporting Services reports. Although the Reporting Console is installed automatically with the PowerBroker Desktops snap-in, Reporting Services requires installation of PowerBroker Desktops Reporting. You can use PowerBroker Desktops without installing Reporting Services.

PowerBroker Desktops Auditing and Reporting has the following requirements:

- SQL Server 2008 R2 or SQL Server 2008 R2 Express Advanced Edition must be installed in your environment.
- SQL Management Tools, an optional feature of SQL Server or SQL Server Express, must be installed.
- SQL Server Reporting Services (SSRS) must be installed and running on SQL Server or SQL Server Express. (If SSRS is not installed, you can still use the Reporting Console to provide basic reporting and to generate rules, but you cannot use the Reporting Services.)
- Windows Event Forwarding must be permitted.
- Windows Remote Management (WinRM) V2.0 must be installed. WinRM V2.0 is included in Windows 7 and Window Server 2008 R2. If you have a version of Windows or Windows Server that does not include WinRM V2.0, you can download it from http://support.microsoft.com/kb/968930.
- On the computer that will serve as the event collector, you must install the PowerBroker Desktops snap-in. To ensure accurate reporting, the Reporting Console must be run only from this computer. Reporting Services can be run from any computer.
- The PowerBroker Desktops client software must be deployed to all client computers from which you want to obtain data for rule generation. Firewall ports 5985 and 80 must be configured as exceptions on these computers.

Installing the Snap-in

The snap-in must be installed on a computer used to manage Group Policy Objects (GPOs) and domains. This type of computer is usually a domain controller. PowerBroker Desktops rules are distributed from the domain controller's `SYSVOL` folder. However, this location might not be where they were created or edited.

Tip: Where to find the snap-in installer

You must download the PowerBroker Desktops snap-in installer file from the BeyondTrust website. You can then install it on any computer from which you can edit domain policy.

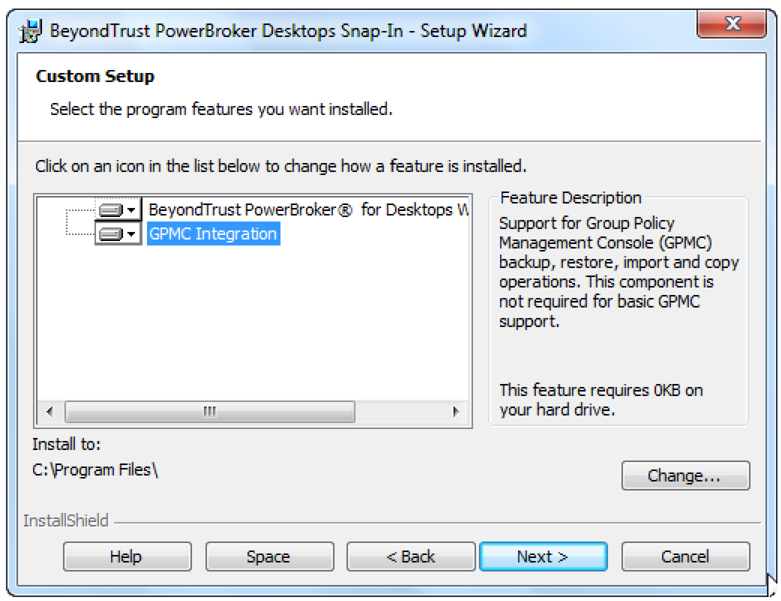
Access the snap-in installer from the BeyondTrust Evaluations and Download webpage. After you log into the website, choose one of the following versions of the snap-in installer to download:

`pbdsnap32.msi` for the 32-bit snap-in installer
`pbdsnap64.msi` for the 64-bit snap-in installer

To install the snap-in, do the following:

1. Download an installer .MSI file from the BeyondTrust website.
2. Double-click on the `pbdsnap32.msi` or `pbdnap64.msi` file name.
   For 32-bit computers, use `pbdsnap32.msi`.
   For 64-bit computers, use `pbdsnap64.msi`.
3. In the Welcome dialog of the Setup Wizard, click **Next**.
4. In the License Agreement dialog, accept the license terms and click **Next**.
5. In the Custom Setup dialog, choose an installation location. Either accept the default root installation folder, or click **Change** and select a different location. Click **Next**.

   Note: If you are installing in an environment that includes the Microsoft Group Policy Management Console (GPMC), the installation wizard displays a GPMC Integration feature. Installing this feature is required for full GPMC functionality.



6. Click **Install** to continue the installation using the path you specified.
7. When prompted, click **Finish** to complete the installation.

Verifying Snap-in Installation

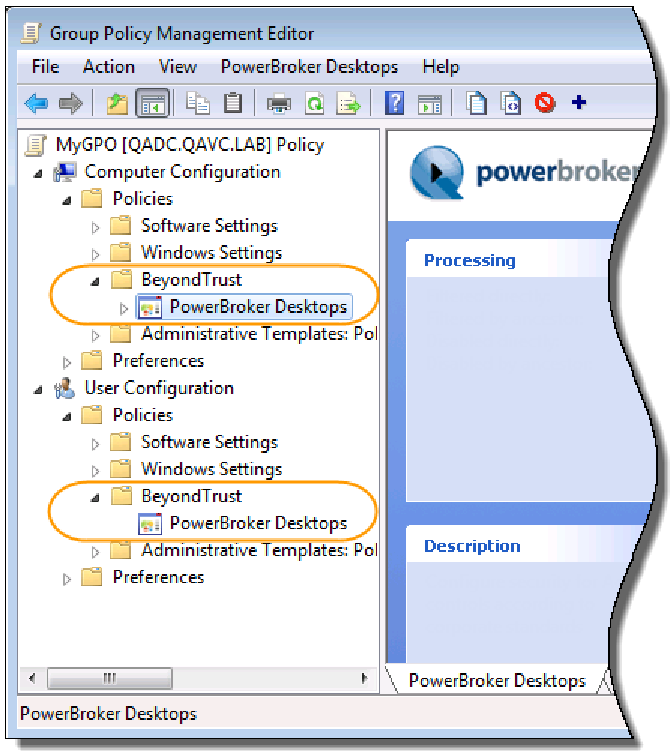
To verify that the snap-in was successfully installed, do the following:

1. Start the Group Policy Management Console (GPMC) by clicking **Start**, **Run** and entering **`gpmc.msc`**.
2. Right-click a GPO and select **Edit**.

   Note that the items are added to the Group Policy Management Editor and are displayed under the following nodes:

   – **Computer Configuration**, **Policies**, **BeyondTrust**.

   – **User Configuration**, **Policies**, **BeyondTrust**.



Configuring the Passcode Generator

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. For more information about the Passcode Generator, see the *PowerBroker Desktops User Guide*.

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 "Verifying Snap-in Installation," page 16.
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.
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.

Installing PowerBroker Desktops Client Software

The client software must be installed on all computers that are to be managed by PowerBroker rules.

Note: Rules embedded in GPOs have no effect on computers that do not have the client software installed and running.

Tip: Where to find the client software installer

You must download the PowerBroker Desktops client software installer file from the BeyondTrust website. You can then deploy the `.msi` file to the organization's desktops.

Access the client software installer from the BeyondTrust Evaluations and Download webpage. After you log into the site, choose one of the following versions of the client software installer to download:

`pbdcl32.msi` for the 32-bit client installer
`pbdcl64.msi` for the 64-bit client installer

Deploying Client MSI Packages

The recommended installation method for client computers is to use the Group Policy Management Editor in the Microsoft Group Policy Management Console (GPMC) to deploy the client software installation MSI package to all client computers in a domain.

To deploy the client software:

1. Download the client installer package (MSI file) from the BeyondTrust website.

2. Save the installer package.

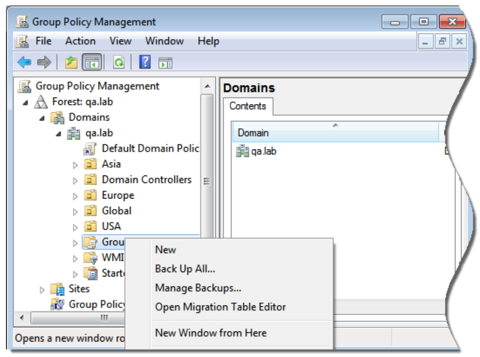
Tip: Save the installer package in an accessible location

The installer package must be hosted in a location (such as a network share) that is accessible to the SYSTEM account of each computer where the software should be installed. The path provided must use the following format:

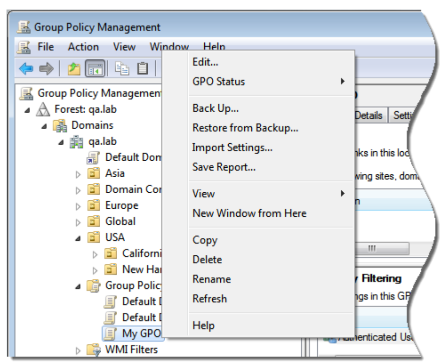
`\\`*`MyServer`*`\`*`MyFolder`*`\pbdcl32.msi`

3. Click **Start**, **Control Panel**, **Administrative Tools**, **Group Policy Management** to open the Group Policy Management Console (GPMC). If the GPMC is not already installed, it can be downloaded from http://microsoft.com/downloads. In older versions of Windows Server or Windows, you can open the Group Policy Object Editor from Active Directory Users and Computers or from a custom Microsoft Management Console.

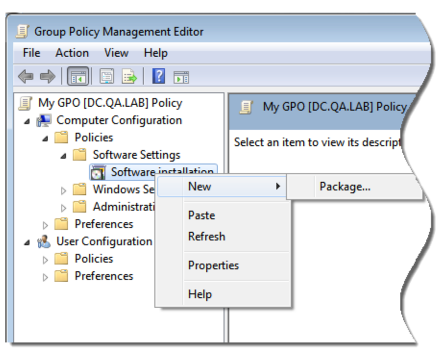
4. In the GPMC, click **Forest**, **Domains**, **<*MyDomain*>**, **Group Policy Objects**.
5. To create a new GPO, right-click **Group Policy Objects** and click **New**. Enter a name for the GPO and click **OK**. Alternatively, you can add configurations to an existing GPO.



6. Right-click the GPO and click **Edit** to launch the Group Policy Management Editor so that you can configure settings for the GPO.

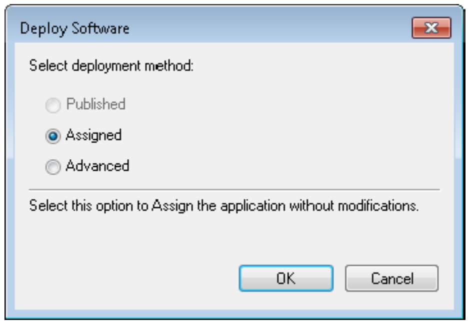


7. In the Group Policy Management Editor, click **Computer Configuration**, **Policies**, **Software Settings**. Right-click **Software Installation** and click **New**, **Package**.

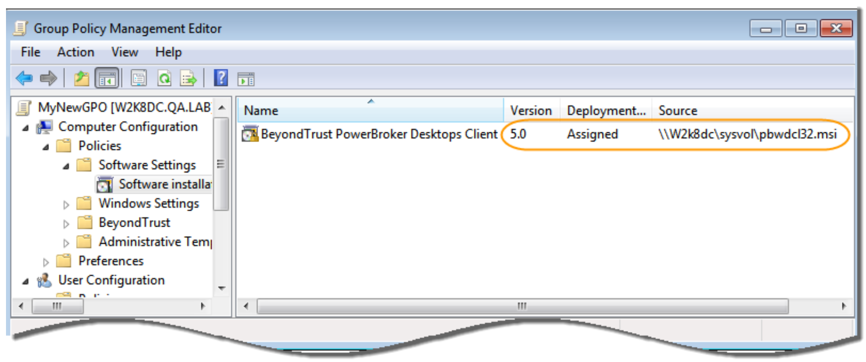


8. Select the client installer package and click **Open**.

9. Select **Assigned** and click **OK**.



10. After a brief delay, the name of the software to be installed is displayed in the details pane of the Group Policy Management Editor as shown in the following figure:



If the name does not appear, right-click **Software Installation** and select **Refresh** until it does. To modify installation settings, double-click the item name in the display pane. To remove an item, right-click the item name and select **All Tasks, Remove**.

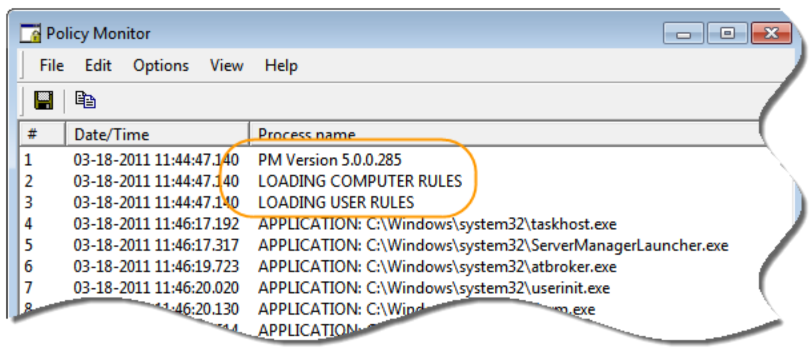
11. Reboot each client computer to initiate client installation. This can be done manually or by using Group Policy mechanisms.

    After the client is installed, the computer can recognize and enforce PowerBroker Desktops V5.3 rules.

Verifying the Client Software Installation

Use the policy monitor program to verify the client has been successfully installed on a computer. To verify client software installation, make sure the computer has been re-booted and then do the following:

1. On a computer on which the client was installed, start Policy Monitor by selecting **Start, Run** and entering: **`polmon.exe`**
2. In the resulting Policy Monitor window, ensure that no connection errors are reported and that computer and user rules have been successfully loaded. A sample Policy Monitor output is shown in the following figure:



Installing and Configuring Auditing and Reporting (PBReports)

PowerBroker Desktops Auditing and Reporting 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.

Prior to using PowerBroker Desktops Auditing and Reporting, you must ensure that the requirements for it are met. For details, see "Auditing and Reporting Software Requirements," page 13.

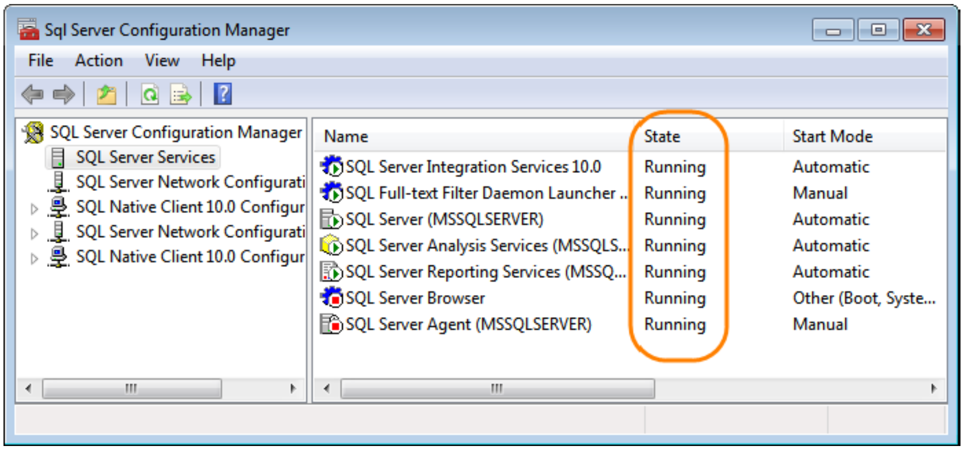
For full Auditing and Reporting functionality, you must run the `pbdreporting.msi` file to install PowerBroker Desktops Auditing and Reporting components. Also, you must perform initial configuration for the event collector computer, PowerBroker Desktops client computers, and the PowerBroker Desktops snap-in to support Auditing and Reporting.

Verifying SQL Server Services

Verify that SQL Server Services are running.

1. In SQL Server or SQL Server Express, open **SQL Server Configuration Manager**.
2. In the left plane, click **SQL Server Services**.

3. In the right pane, ensure that the state shown for **SQL Server** and **SQL Server Reporting Services** is **Running**.

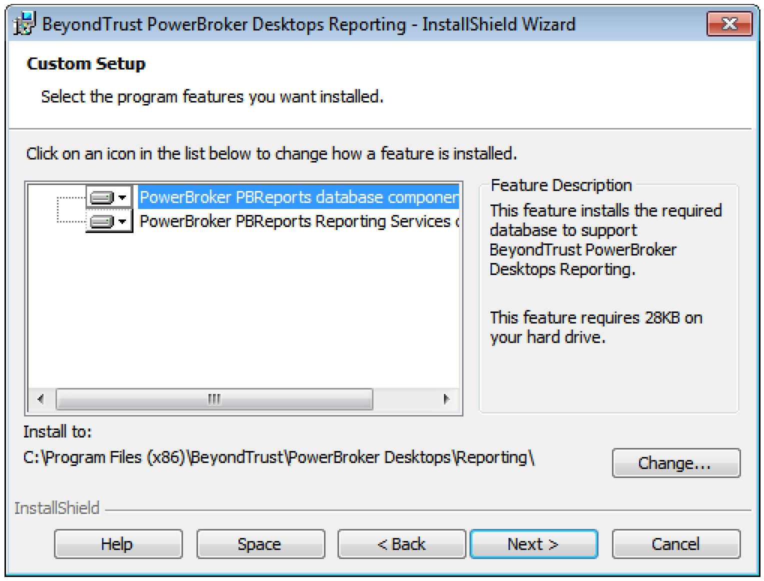


Installing Auditing and Reporting Components

Download the installer for PowerBroker Desktops Reporting, and install the database and Reporting Services components on a computer that hosts or can connect to a SQL Server or SQL Server Express instance.

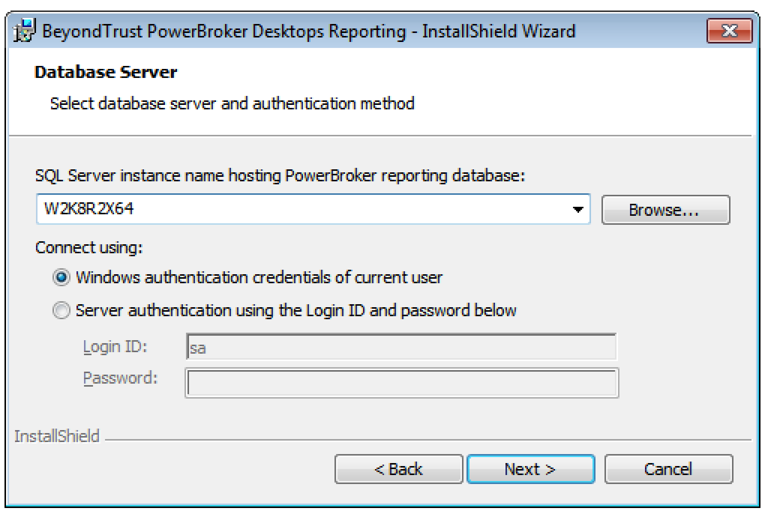
1. Browse to http://www.beyondtrust.com.
2. Click **Login** and log using the password provided to you by BeyondTrust.
3. After reading the Welcome message, scroll to the top of the **BeyondTrust Partner Portal** pane and click **Customer Support Center.**
4. In the **Software/Documentation** section, click **PowerBroker Desktops**.
5. Click **I Accept** to accept the Software License Agreement.
6. On the PowerBroker Desktops page, download the `pbdreporting.msi` file and save it to a folder that is accessible to your instance of SQL Server or SQL Server Express.
7. Run `pbdreporting.msi` and follow the instructions on screen.
8. In the Welcome dialog of the Setup Wizard, click **Next**.
9. In the License Agreement dialog, accept the license terms and click **Next**.

10. In the Custom Setup dialog, either click **Next** to accept the default installation locations, or else select alternative locations for the components before clicking **Next**.

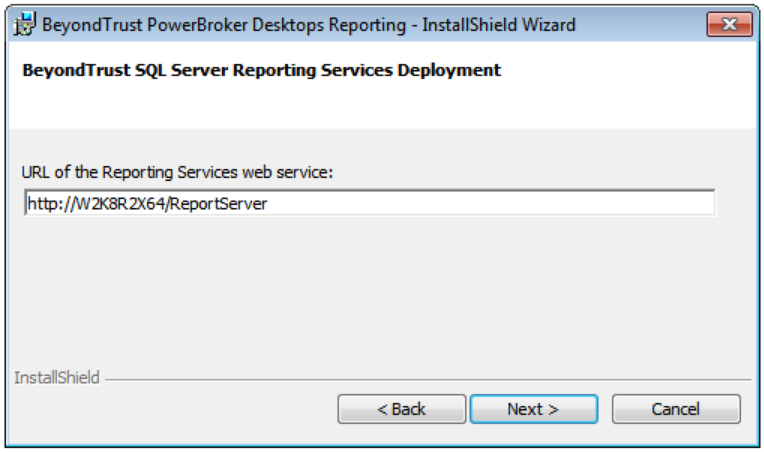


11. In the Database Server dialog, browse to or type a SQL Server or SQL Server Express instance, specify either Windows Authentication or Server Authentication, enter credentials if needed, and click **Next**.

Note: If your server instance is not displayed in the browser, type it instead. If you are installing PowerBroker Desktops Reporting on a computer that has the default instance of SQL Server installed, you can enter **.** as the name.



12. In the BeyondTrust SQL Server Reporting Services Deployment dialog, enter the **URL of the Reporting Services web service** for SQL Server Reporting Services.



13. Wait while the installer runs. Installation progress may be affected by network traffic and by how busy the computer hosting SQL Server or SQL Server Express is. Progress may appear to pause and then resume. When installation is complete, click **Finish**.

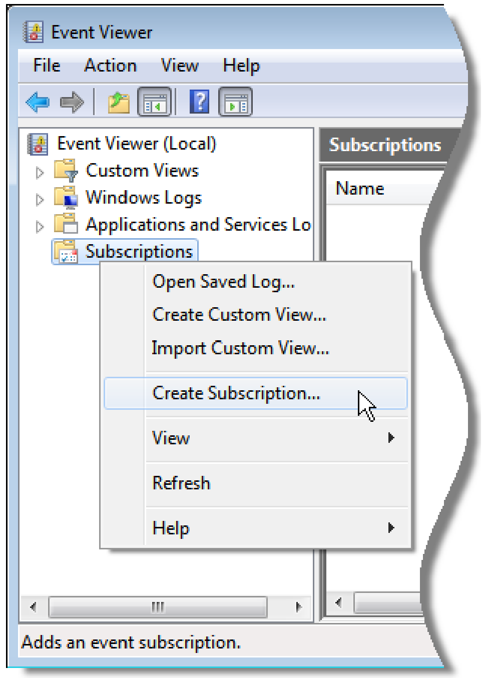
Note: Nothing is added to the Start menu by this installation. You can verify installation by confirming that **BeyondTrust PowerBroker Desktops Reporting** appears under **Programs and Features** in the **Control Panel**. You must configure the event collector and client computers before you can generate useful reports.

Configuring the Event Collector (Windows Event Forwarding)

On the computer that will serve as the event collector, perform the following steps to create a subscription to support Auditing and Reporting:

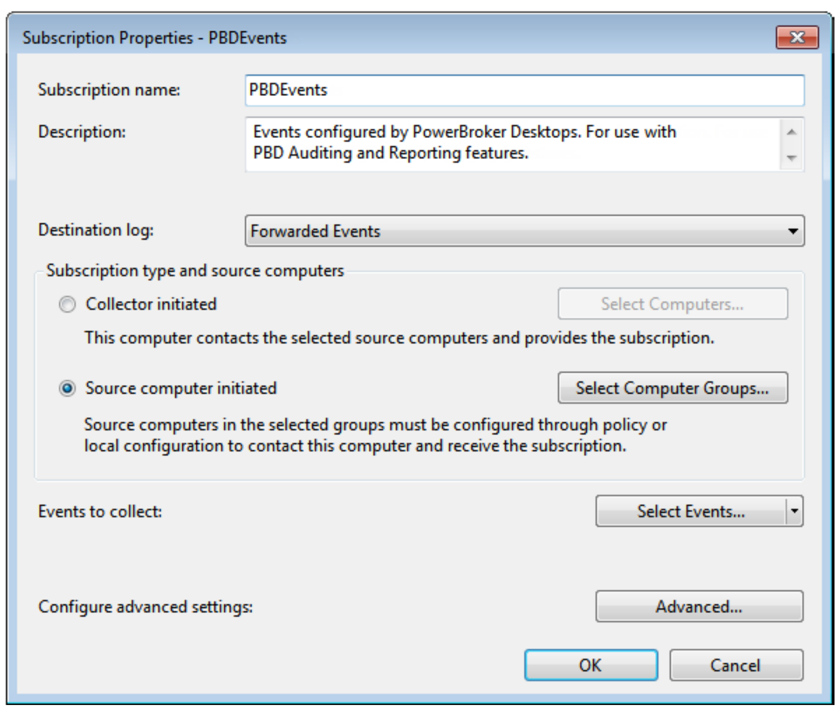
1. In Administrative Tools in Windows, open **Event Viewer**.
2. In Event Viewer, click **Subscriptions**. If a dialog asks if you want to start the Windows Event Collector Service, click **Yes**.

3. Right-click **Subscriptions** and click **Create Subscription**.



4. In the **Subscription Properties** dialog, enter a name for the subscription, such as `PBDEvents`.

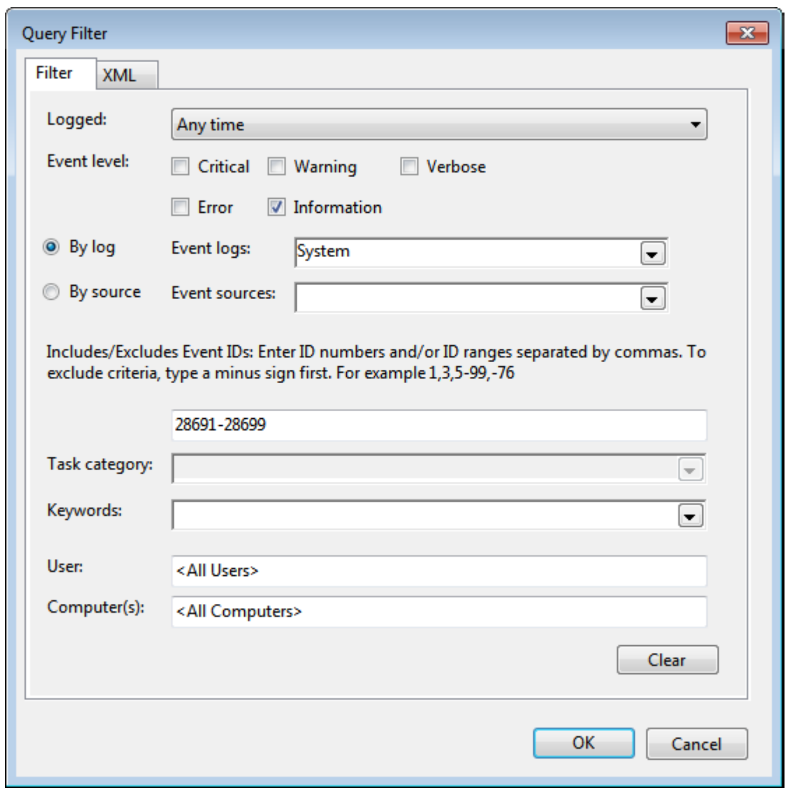
5. In the **Subscription type and source computers** box, click **Source computer initiated**.



6. Click **Select Computer Groups**.
   a. In the **Computer Groups** dialog, click **Add Domain Computers** and select the computers for which you want to be able to generate reports or from which you want to gather application usage data for generating rules.

      Note: If the PowerBroker Desktops client software is installed on the computer serving as the event collector, do not include that computer in the computer groups selected.

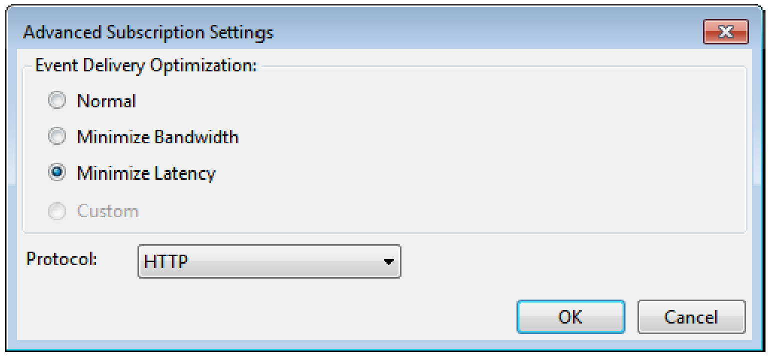
   b. Click **OK** to close the Computer Groups dialog.
7. Click **Select Events.**
   a. In the Query Filter dialog, for **Event Level** select **Information**.
   b. Select **By log** and then for **Event logs** select **System**.
   c. In the **Includes/Excludes Event IDs** field, type `28691-28699` to specify PowerBroker Desktops events.



   d. Click **OK** to close the Query Filter dialog.
8. Click **Advanced**.
   a. In the Advanced Subscription Settings dialog, specify how frequently you want to forward events. To forward events every 15 minutes, click

Normal. To forward events as quickly as possible, click **Minimize Latency**.

b. For **Protocol**, select **HTTP**.



c. Click **OK** to close the Advanced Subscription Settings dialog.

9. Click **OK** to close the Subscription Properties dialog.

10. To configure Auditing and Reporting to function on an event collector that is using a locale other than en-US, you must install the English language pack.

    Note: You do not need to change the locale of the event collector or to install the English language pack on client computers.

    a. View the Windows Server 2008 R2 Service Pack 1 Multilingual User Interface Language Packs page on the Microsoft Download Center. http://www.microsoft.com/download/en/details.aspx?id=2634

    b. Select the English (US) language and download the English language pack (Windows6.1-KB2483139-x64-en-US.exe).

    c. Install the English (US) language pack from the Windows Server 2008 R2 Service Pack 1 Multilingual User Interface Language Pack on the computer serving as the event collector.

    d. Open a command prompt and run the following command, substituting the name of the subscription that you created in step 4 for *`SubscriptionName`*:

    ```
    wecutil ss SubscriptionName -l:en-US
    ```

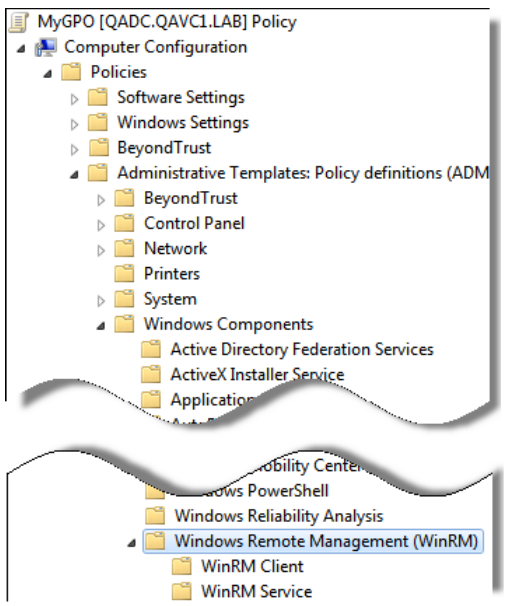
    Ensure that the subscription is initialized by the event collector, not the source computer.

Configuring the Client Computers

You must configure certain policy settings and apply them to all client computers from which you want gather Auditing and Reporting data. These client computers act as source computers by providing the data.

On a computer from which you can manage Group Policy:

1. In the Group Policy Management Console (GPMC), edit a Group Policy Object (GPO) that is applied to all of the client computers that you want to act as source computers.
2. In the Group Policy Management Editor, expand **Computer Configuration, Policies, Administrative Templates, Windows Components, Windows Remote Management (WinRM)**.

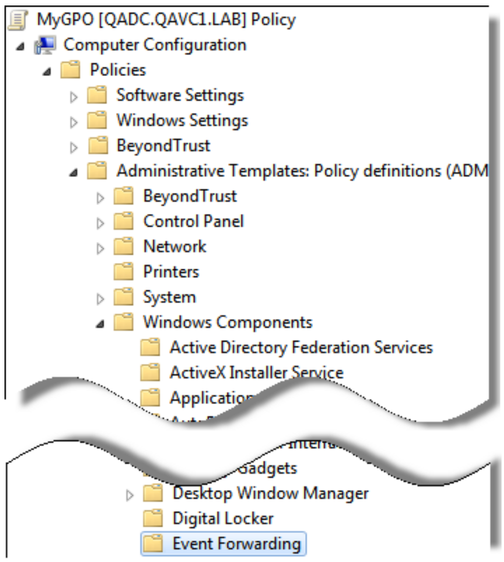


   a. Expand **WinRM Service**.
      For each of the following policy settings, double-click the policy setting to edit it, click **Enabled**, configure any additional options noted, and click **OK** to save and close the policy setting.
      – **Allow automatic configuration of listeners** - If the computers are not in a trusted environment, it is recommended that you specify IP addresses or ranges. Otherwise, enter ***** in the **IPv4 filter** and **IPv6 filter** fields.
      – **Allow CredSSP authentication**
      – **Turn On Compatibility HTTP Listener**
      – **Turn On Compatibility HTTPS Listener**

   b. Expand **WinRM Client**.
      For each of the following policy settings, double-click the policy setting to edit it, click **Enabled**, configure any additional options noted, and click **OK** to save and close the policy setting.

- **Allow CredSSP authentication**
- **Trusted Hosts** - In the **TrustedHostsList** field, enter your domain name, using wildcards if needed. For example, `*.example.com`.

3. In the Group Policy Management Editor, expand **Computer Configuration, Policies, Administrative Templates, Windows Components, Event Forwarding**.



a. Double-click **Configure the server address, refresh interval, and issuer certificate** to open the properties dialog for the policy setting.

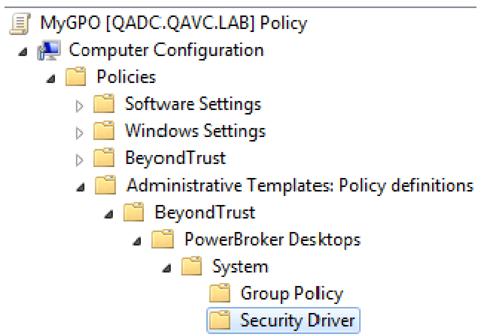
b. Click **Enabled**.

c. Click **Show**. Enter **`Server=`** followed by the fully-qualified domain name of the event collector computer (for example, `Server=myserver.example.com`), and then click **OK** to close the Show Contents dialog.

d. Click **OK** to save and close the policy setting.

4. Configure the events to be forwarded to the event collector.

   In the Group Policy Management Editor, expand **Computer Configuration, Policies, Administrative Templates, BeyondTrust, PowerBroker Desktops, System, Security Driver**.



   For each of the following policy settings, double-click the policy setting to edit it, click **Enabled**, and click **OK** to save and close the policy setting.

   – **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**

5. Either wait for the next Group Policy update to occur or else run `gpupdate /force`.

Configuring the PowerBroker Desktops Snap-in

Configure the PowerBroker Desktops snap-in to point to the database and to SQL Server Reporting Services so that you can view reports.

On a computer from which you can manage Group Policy:

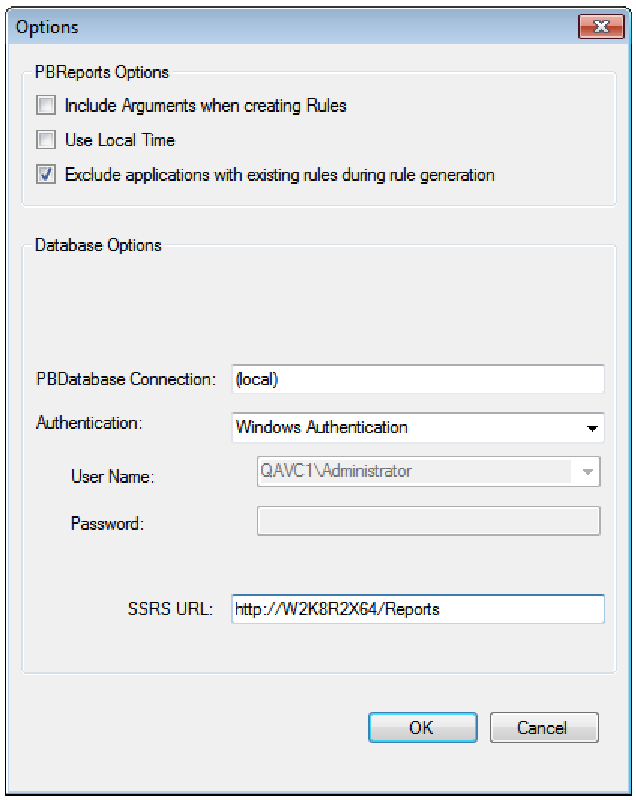
1. In the Group Policy Management Console (GPMC), edit a Group Policy Object (GPO).
2. In the Group Policy Management Editor, open the PowerBroker Desktops management dashboard by clicking either of the BeyondTrust nodes.
3. In the **Tools & Wizard** section of the dashboard, scroll to the **Auditing and Reporting** section and click **Reporting Console**.
4. In the **PowerBroker Desktops Reporting Console**, click **Options**.

5. In the **PBDatabase Connection** field, enter **`(local)`** if the SQL Server or SQL Server Express instance is on the computer where you installed the database components during the PowerBroker Desktops Reporting installation process.

   Otherwise, enter a fully qualified SQL Server or SQL Server Express instance. Examples: `MyServer\MySQLInstance` or `192.168.1.1\MySQLInstance`

6. In the **Authentication** field, select an authentication type and enter credentials if needed.

7. In the **SSRS URL** field, enter the **Report Manager URL** for **SQL Server Reporting Services**. (In SQL Server 2008 R2, you can find the Report Manager URL by clicking **Start, Microsoft SQL Server 2008 R2, Configuration Tools, Reporting Services Configuration**.)

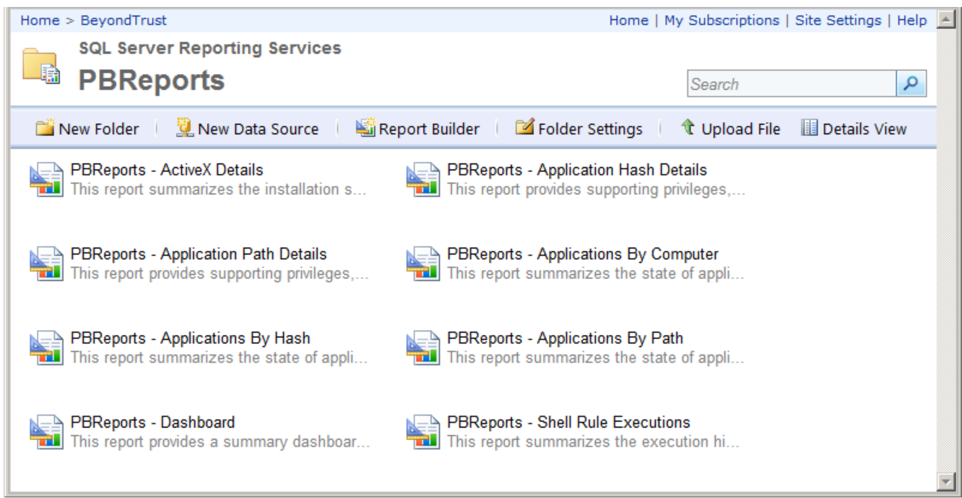
   

8. Click **OK**.

Verifying Reporting Services

After you have allowed a Group Policy update to occur or have run `gpupdate /force`, on a computer on which the PowerBroker Desktops snap-in is installed and from which you can manage Group Policy:

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, scroll to the **Auditing and Reporting** section and click **Reporting Services**.
4. On the PBReports page, click a report title to view a report.



For more information, see “Viewing and Managing Reports” in the *PowerBroker Desktops User Guide*.

Licensing and Operating Modes

There are two types of PowerBroker Desktops licenses:

- **Registered Product** - You have purchased software licenses or obtained free evaluation licenses from BeyondTrust or an authorized reseller and have imported a registered license. The product is fully functional and can be used across multiple domains.
- **Evaluation Product** - You have installed PowerBroker Desktops with a temporary license. The product is fully functional, can be used in multiple domains but has an expiration date encoded in the license.

A 14-day grace period is implemented for license expiration. If the term of the license is exceeded, CSEs will report a warning to the event log while operating within 14 days of the last successful license check. If the grace period is exceeded, the CSEs will not process policy for the GPO and an error will be written to the event log.

Demonstration Mode

When no license is present, PowerBroker Desktops runs in Demonstration mode. In this mode all rules are fully functional within a local GPO, but the product will process (that is, enforce) only the template rules from a network GPO.

Template rules are preconfigured rules specific to an operating system. They are accessible from the **Path** widget on the **Application** tab of the **Properties** dialog.

The advantage of Demonstration mode is that it allows the configuration and deployment of template rules without the requirement of a license. In addition, it supports the creation of most rule types so you can gain familiarity with rules and policy making. However, even though most types of rules can be created, only template rules are functional at the domain level.

When a license is eventually acquired, all rules that have been created (template and non-template rules) in Demonstration mode are functional and can be deployed across the domain without modification. This feature leverages the time invested and experience gained with PowerBroker Desktops.

Note: In Demonstration mode, the following operations are not supported by a template rule: **Add Printers**, **Add Plug and Play Devices**, and configuration of network settings.

Obtaining a License

To request a free temporary license or to purchase a registered license, do one of the following:

- Contact BeyondTrust Sales at http://pm.beyondtrust.com/sales or +1-800-234-9072.
- Contact a BeyondTrust sales representative.

A sales representative will guide you through the submission of a license request file.

Creating a License File Request

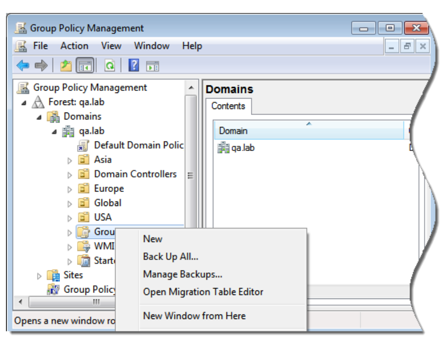
To create a license file request, do the following:

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

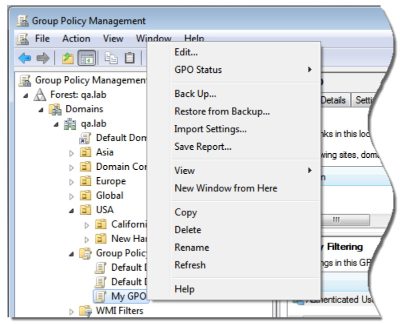
> **Tip: If GPMC is not installed**
>
> If you have not installed the GPMC (a free tool available at http://microsoft.com/downloads), you can open the Group Policy Management Editor from the Active Directory Users and Computers dialog or from a custom Microsoft Management Console.

2. In the GPMC, click **Forest**, **Domains, <*MyDomain*>**, **Group Policy Objects**.

3. To create a new GPO, right-click **Group Policy Objects** and click **New**. Enter a name for the GPO and click **OK**. Alternatively, you can add configurations to an existing GPO instead.

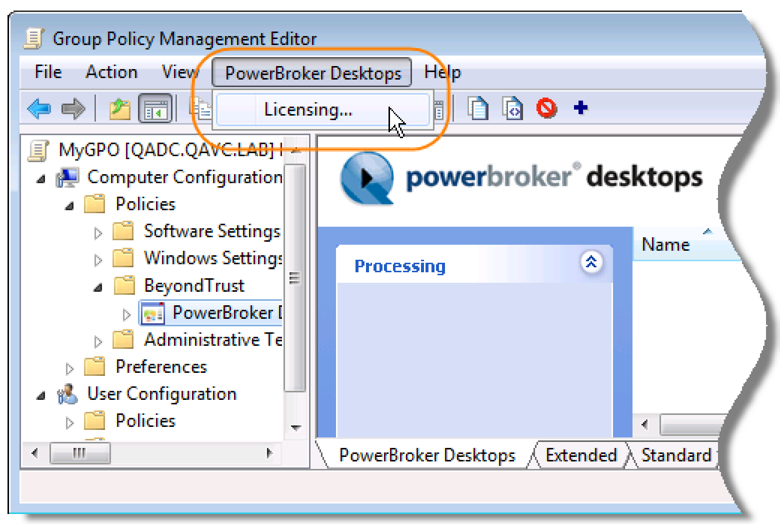


4. Right-click the GPO and click **Edit** to open the Group Policy Management Editor to use for configuring settings for the GPO.

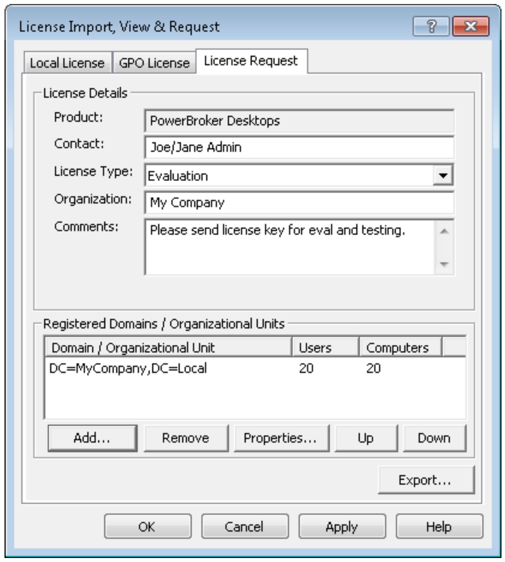


5. In the Group Policy Management Editor, click **User Configuration, Policies, BeyondTrust** and select the **PowerBroker Desktops** node.

6. From the Group Policy Management Editor menu bar, click **PowerBroker Desktops, Licensing** to display the License Import, View & Request dialog.



7. Click the **License Request** tab.

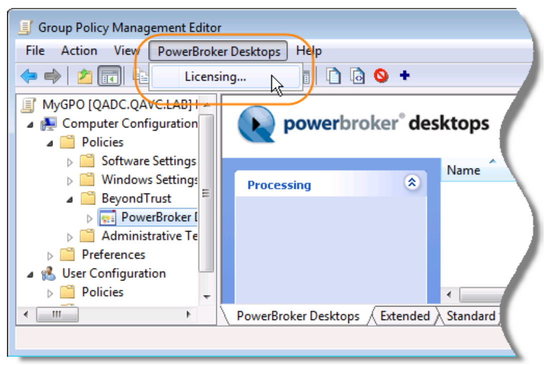


8. Provide a contact name, select the type of license that you are requesting, enter the name of your company or organization, and (optionally) enter comments.
9. Select the domains to be licensed.
10. In the **Registered Domains** field, click **Add**.
11. In the Select Domain dialog, click **Browse**.
12. Select a domain and click **OK**.
13. Click **Calculate** for **Users**, and then click **Calculate** for **Computers** to determine the number of non-disabled users and computers currently in the selected domain.
14. Edit the **Users** and **Computers** fields to set quantities appropriate for your organization.
15. Click **OK**.
16. Repeat these steps for each domain or OU that you want to license.
17. Click **Export** to generate a license request file.
18. Email your license request file to license.request@beyondtrust.com. Your BeyondTrust sales representative (if ordering directly from BeyondTrust) or an authorized reseller will respond to you. After your license request is approved, a license key is sent to the email address you provided.

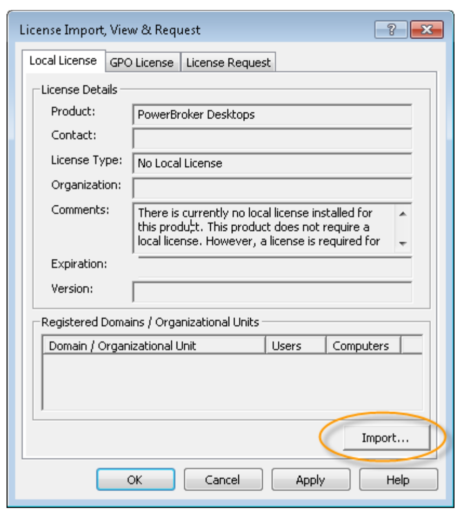
Importing a License File

After you receive a license you must import it into PowerBroker Desktops. To import a license key, do the following:

1. After installing PowerBroker Desktops, edit a GPO.
2. In the Group Policy Management Editor, click **User Configuration, Policies, BeyondTrust**.
3. In the Group Policy Management Editor menu bar, click **PowerBroker Desktops, Licensing**.



4. On the **Local License** tab, click **Import**.



5. Select the PowerBroker Desktops `license.xml` file that you received from your BeyondTrust sales representative or authorized reseller, and click **Open**.
6. Click **OK**.

Note: The license is automatically applied to new GPOs when policy is edited from this computer; however, you must deploy the license to all existing GPOs for it to take effect in those GPOs.

Tip: Manually importing a license

To manually import a license rather than using the previous procedure, copy the `license.xml` file to:
`%AllUsersProfile%\Application Data\BeyondTrust\PowerBroker Desktops`

When using a Windows version prior to Windows Vista, using `%AllUsersProfile%` points to:

`C:\Documents and Settings\All Users`

When using Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows Vista, using `%AllUsersProfile%` points to:

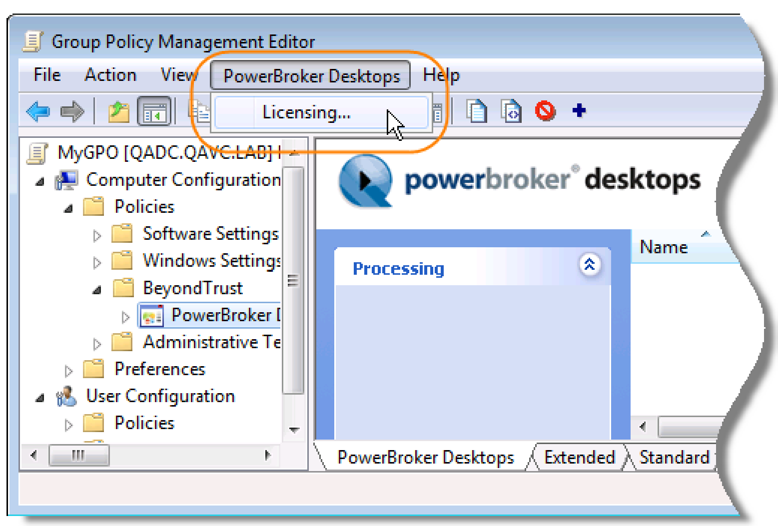
`C:\ProgramData`

Note: The license is automatically applied to new GPOs when edited from this computer. However, you must deploy the license to all existing GPOs for it to take effect in those GPOs.

Deploying a License to Existing GPOs

To apply a new license to existing GPOs, deploy the license to each GPO as follows:

1. In the Group Policy Management Console (GPMC), edit a GPO.
2. In the Group Policy Management Editor, click **User Configuration**, **Policies, BeyondTrust**.
3. In the menu bar, click **PowerBroker Desktops, Licensing**.



4. Click the **GPO License** tab and then the **Deploy** button to deploy the new license to this GPO.

   Note: The **Deploy** button displays only if you have imported a valid license on the local computer.

5. Repeat for each GPO that contains BeyondTrust settings.

Frequently Asked Licensing Questions

This section can help you to determine how many licenses you require.

Do I need a license to process PowerBroker Desktops rules and policy settings?

A license is not required to use basic rules and policy settings provided with PowerBroker Desktops. A license is required to create and use custom rules and policy settings of your own creation.

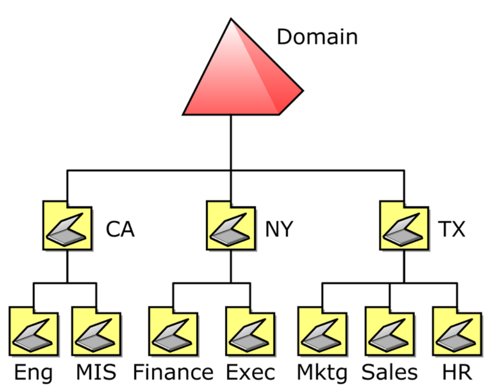
Do I need user or computer licenses?

User licenses are required to configure PowerBroker Desktops items under the `User Configuration` node in the Group Policy Management Editor. A user configuration item is processed when the user logs in and Windows policy is refreshed (but only if the user is logged in).

Computer licenses are required to configure items under the `Computer Configuration` node in the Group Policy Management Editor. A computer configuration item is computer-specific (that is, applies to a computer when any user or no user is logged in) and is processed when the computer boots and Windows policy is refreshed.

Which containers (domains) should I license?

License the domain or container at the highest level in which all objects in the container and all subcontainers can be configured by PowerBroker Desktops. For the network shown in the following example diagram where you want to apply policy rules only to the Eng, MIS, and Finance departments, you must license the CA and Finance organizational units (OUs).



How many licenses do I need?

A license is required for all active computer and/or user objects in the licensed domain. In the network shown in the previous diagram, if a GPO containing PowerBroker Desktops items is to be applied to the TX subdomain, a license is required for all active objects in the TX, Mktg, Sales, and HR subcontainers.

Are objects in subcontainers counted towards licensed totals?

Yes, all active objects in the licensed domain are counted in the license total.

Index