Privilege Authority 2.0

Administrator's Guide

SCRIPTLOGIC

ScriptLogic Corporation

6000 Broken Sound Parkway NW

Boca Raton, Florida 33487-2742

1.561.886.2400

www.scriptlogic.com

Trademark Acknowledgements

Privilege Authority, ScriptLogic and the ScriptLogic logo are either registered trademarks or trademarks of ScriptLogic Corporation in the United States and/or other countries. The names of other companies and products mentioned herein may be the trademarks of their respective owners.

Documentation Conventions

Typeface Conventions

Bold	Indicates a button, menu selection, tab, dialog box title, text to type, selections from drop-down lists, or prompts on a dialog box.

Contacting ScriptLogic

ScriptLogic may be contacted about any questions, problems or concerns you might have at:

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

561.886.2400 Sales and General Inquiries

561.886.2450 Technical Support

561.886.2499 Fax

www.scriptlogic.com

ScriptLogic on the Web

ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search Frequently Asked Questions, for the answers to the most common non-technical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

Contents

Overview

It is an accepted principle by network administrators that users in the domain be configured with a minimum permission set and not be added to any local groups such as the Local Administrators or Power Users group on the workstation. Using this least privilege configuration will enhance security and data protection while also reducing faults and support.

However, System Administrators, for a long time, have been running into situations where users require administrative rights to run an application. At times it is to support legacy applications that only work when run by someone with administrative rights; other times it is because a user works remotely, or is travelling and needs greater control of their system; or it might be that Administrators want to give their users rights to install commonly used software that often and automatically needs to be updated.

A common but misguided solution to this is to give these users administrator rights which solves the problem at hand but often leads to many more.

Privilege Authority (PA) solves this issue by raising the privilege level for specific processes, allowing those that require elevated rights to run, while maintaining the least restrictive privilege set for the user.

What's new in Privilege Authority 2.0:

- The Community Rules Exchange server is integrated into Privilege Authority and is used to download/share elevation rules;
- Privilege Authority is now available in a Professional version that can be purchased from ScriptLogic. In Privilege Authority Professional, Group Policy Object (GPO) rules can be based on the following data:
    - digital certificates;
    - the computer operating system version or operating system class, i.e. server or workstation;
    - the computer name;
    - the computer group or organizational unit;
    - the computer IP address range (IPv4/IPv6);
    - certain registry key;
    - certain file
- User Interface has been improved for look and feel

How Does Privilege Authority Work?

There are two software components included with Privilege Authority:

- Privilege Authority Server is a management application. It is installed on a server in the domain and used to create and manage rules within Group Policy.
- Privilege Authority Client is a service that runs on the client machine. It applies the rules created in the Privilege Authority Server application by monitoring processes as they are launched on the client and raises or reduces the privileges of the processes that it is configured to monitor.

Microsoft Active Directory and Group Policy are used to distribute the Privilege Authority rules to client machines.

Licensing

Privilege Authority is available in 2 editions: *Privilege Authority Community Edition* and *Privilege Authority Professional*.

Privilege Authority Community Edition is absolutely free, but in comparison with Privilege Authority Professional, it lacks the following features:

- Group Policy Object (GPO) rules can be based on digital certificates;
- GPO rules can be based on the computer operating system version or operating system class – server or workstation;
- GPO rules can be based on a computer name, computer group or organizational unit, computer IP address range (IPv4/IPv6), or certain registry key or file;
- full technical support.

Privilege Authority Professional must be purchased but has a 30-day trial period.

Following the common PA 2.0 setup, the customer has access to the Community Edition only. To start trying Privilege Authority Professional, please register (see Figure 1):

Note:

Internet connection is required to perform registration.

If you fail registering due to any connection problems, you can download the package on your own from the ScriptLogic website.

1. On the PA Server, go **Start** > **All Programs** > **ScriptLogic Corporation** > **Privilege Authority** > **Privilege Authority** (or, use the **Privilege Authority** shortcut icon of the **Start** menu).
2. Click the **Try PA Pro!** button in the left-hand tree pane.
   Or, click **Help** > **Begin Evaluation of Pro**.

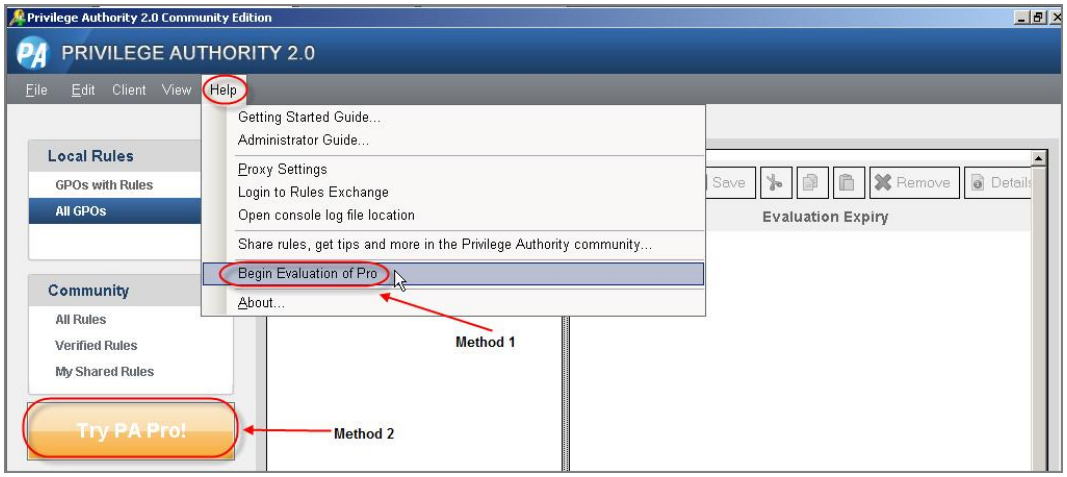

Figure 1. Choosing to use PA Professional in trial mode.

3. On the two-tabbed screen that will show, click the **Try PA Pro!** button, or switch to the **Register** tab.

4. Provide some information about yourself by filling in the form that will be presented. (The obligatory fields as shown in Figure 2.) Click **Register**.

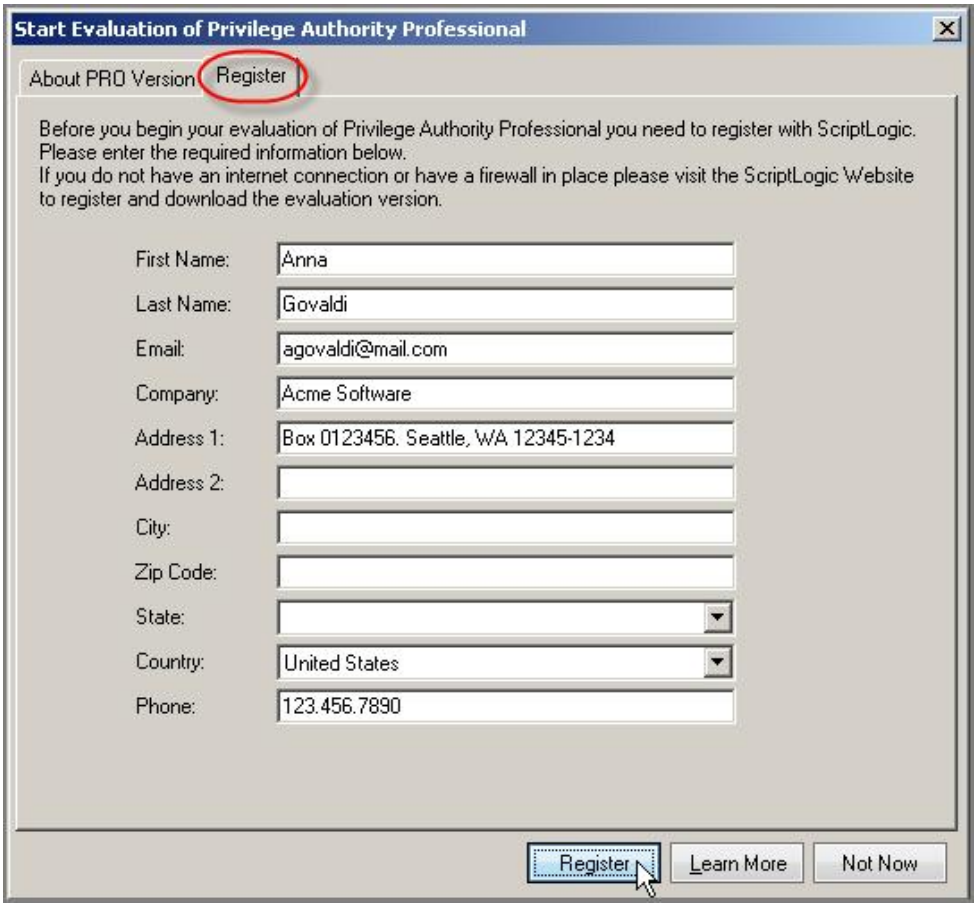

Figure 2. Registering for Privilege Authority Professional.

5. The notification will show to inform you that the rules containing features of Privilege Authority 2.0 Professional will stop working on the client machine(s) in 30 days after starting the evaluation.

6. Click **OK** within the notification window and the Privilege Authority Console name will change to **Privilege Authority 2.0 Professional Evaluation**.

Now you have access to all Privilege Authority Professional features for the 30-day trial period. (See Figure 3.)

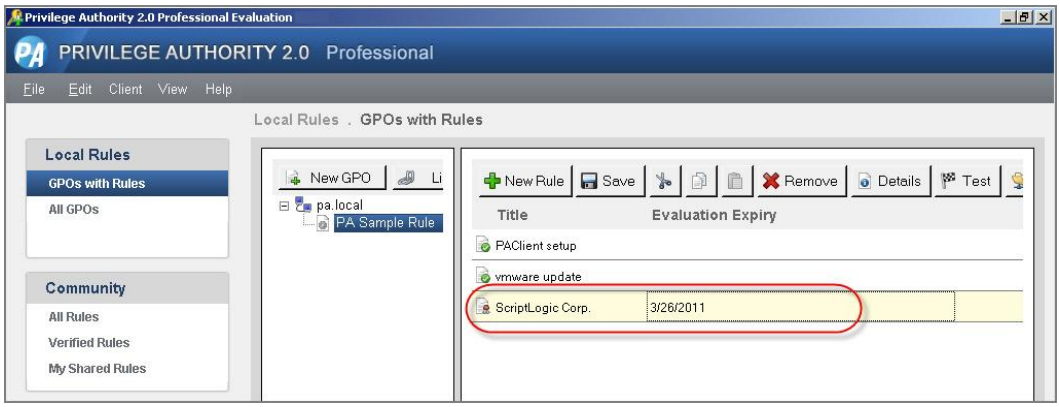

Figure 3. This rule is based on a digital certificate - the Privilege Authority Professional Evaluation feature – and it will be applied until the day specified.

To apply the Privilege Authority Professional license file:

1. Click **Help -> About -> Apply License File** and then use the **Browse** button to locate the license file.

2. Click the **Apply License File** button that will get activated soon after the file is located.

Installation

SYSTEM REQUIREMENTS

The Privilege Authority setup file comprises both the server and client applications. Once both applications are installed, Privilege Authority will use Microsoft Group Policy to distribute rules between the client and server.

The server application requires Microsoft .NET Framework 3.5 for its installation and Microsoft Group Policy Management Console (GPMC) to run. The client can be installed on a Windows workstation or server.

The following is necessary for proper installation and operation of Privilege Authority.

PA Server System Requirements

- .NET Framework 3.5 Service Pack 1 or later
- Microsoft Group Policy Management Console (required to run Privilege Authority)
- Adobe Reader to open the Privilege Authority Guides.

PA Server Operating System Requirements

- Windows XP SP2 or higher
- Windows Server 2003 SP1 or higher
- Windows Vista
- Windows Server 2008/2008 R2
- Windows 7 Enterprise, Professional, or Ultimate Editions

PA Client System Requirements

- No special requirements

PA Client Operating System Requirements

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

Network Requirements

Both PA Server and Clients should be deployed as a part of the Active Directory infrastructure.

INSTALLATION AND UPGRADE

This section details the Privilege Authority installation, removal and upgrade processes:

- Privilege Authority Server Installation
- Privilege Authority Client Installation
- Privilege Authority Upgrade
- Privilege Authority Uninstallation

Installation Process

Privilege Authority uses a client-server model. The main installation will setup the server side (which is comprised of the Privilege Authority Console) and extract the Privilege Authority Client MSI file. Deploy the Privilege Authority Client to each client using Group Policy Management Console or any other software tools, e.g. ScriptLogic Desktop Authority.

Prior to the installation, refer to the System Requirements to make sure your system meets the necessary requirements and prerequisites.

Privilege Authority should be deployed as a part of the Active Directory infrastructure on a computer residing within the internal LAN network.

The following series of steps walk through the installation of Privilege Authority:

- Privilege Authority Server Installation
- Privilege Authority Client Installation

Privilege Authority Server Installation

Privilege Authority Server must be installed on a domain member and run under the context of an account that has rights to change Group Policy. The installation wizard guides you through a series of dialog boxes. Click **Next** on each dialog box to advance to the next option.

1. Run the Privilege Authority setup executable.
2. **Welcome** is the initial dialog box. Click **Next** to continue.
3. The **License Agreement** dialog box appears. If you agree with the license agreement, select the *I accept the terms in the License Agreement* option and click **Next** to continue.

4. On the **Destination Directory** dialog box, select a path and destination folder. The installation path depends on the system architecture and defaults to: `%PROGRAMFILES%\ScriptLogic Corporation\Privilege Authority` or `%ProgramFiles(x86)%\ScriptLogic Corporation\Privilege Authority`. Click the **Browse** button to select a different installation path. Click **Next** to continue.

5. Click **Install** on the final installation dialog to proceed with the installation. Once the file copying portion of the install is complete, click **Finish**.

Following the completion of the Privilege Authority Server installation, perform the Privilege Authority Client installation.

Privilege Authority Client Installation

Once Privilege Authority Server is installed, deploy the Privilege Authority client(s) to the computers on the domain. For these purposes, you may use login scripts or software deployment tools.

Administrative privileges are required to run the PA Client setup locally.

PA Server must be running the PA Client software to make use of the PA rule testing functionality.

To install PA Client on the PA server computer:

- Click **Client** > **Install Client** within the Privilege Authority Console toolbar. The client installation will start. On completing the process, the computer will automatically reboot.

To install PA Clients on your domain via Microsoft Group Policy Management Console:

1. Click **Client** > **Open file location** within the Privilege Authority Console toolbar to locate the PA Client file.

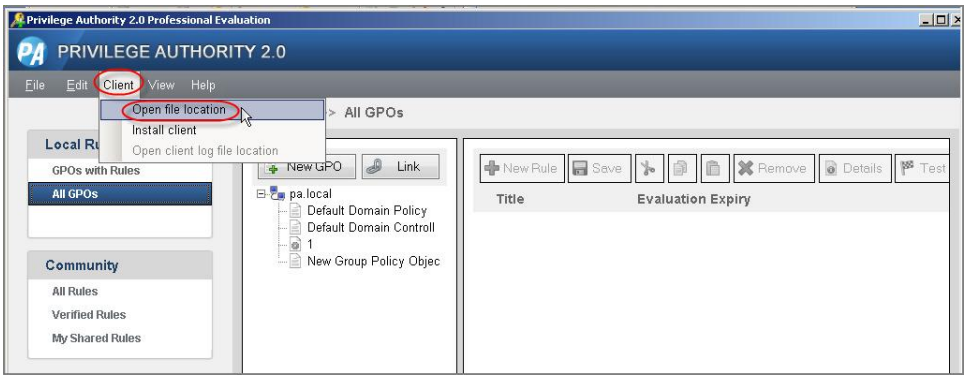

Figure 4. Locating the Privilege Authority Client setup file.

2. Copy the `PAClient.msi` file to a network share that can be read by all users. Or, just share the file folder.

3. Open the Group Policy Management Console on the server and select to create a new Group Policy Object by right-clicking on **Group Policy Objects** and selecting **New** from the popup menu.

4. Enter a name for the new GPO and click **OK**. (See Figure 5.)

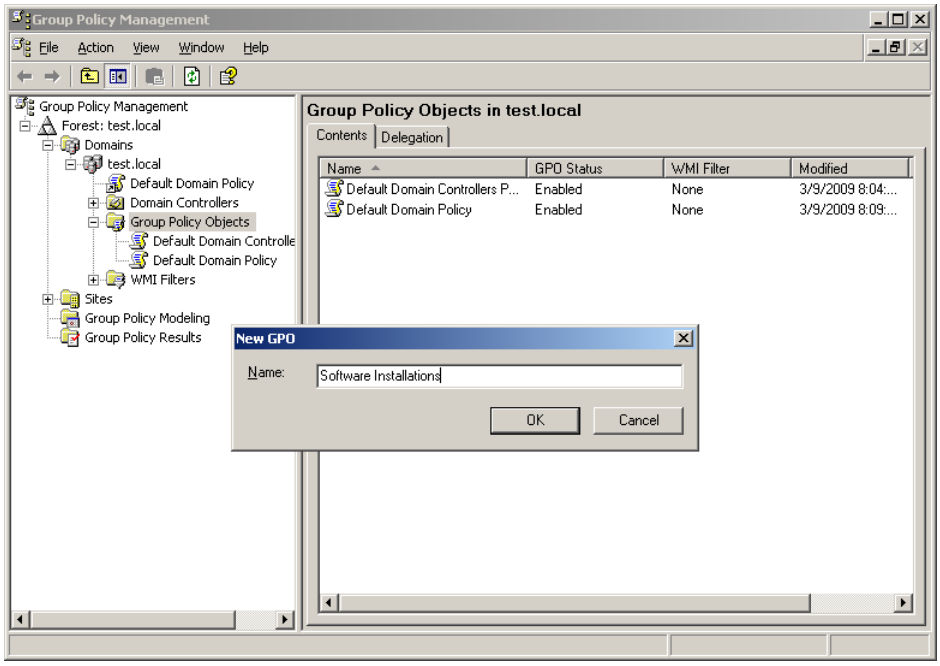

Figure 5 Creating a new Group Policy Object via GPMC

5. Open the newly created GPO by selecting it, right-clicking, and selecting **Edit**.

6. In the Group Policy Object Editor, select **Computer Configuration >** (*within Windows Server 2008*) **Policies > Software Settings > Software installation**. In the right hand pane, right-click on the newly created GPO, and select **New > Package**.

Note

If the PA Client distribution GPO is computer based (defined under the Computer Configuration), enable the "Always wait for the network at computer startup and logon" policy (located in Computer Configuration > (*for Windows Server 2008*) Policies >Policies>Administrative Templates>System>Logon). Otherwise, PA Client installs after the 2nd reboot of the client computer.

If the PA Client distribution GPO is user based (defined under the User Configuration), then PA Client installs after 1st logon.

7. In the dialog box that will open, browse to the `PAClient.msi` file on the network share where it was copied to in step 1.
(We recommend that you use the **File name** field to specify the Client location in the UNC (Universal Naming Convention) format, e.g. `\\computername\sharename\filename.msi`).
Click **Open**. (See Figure 6.)

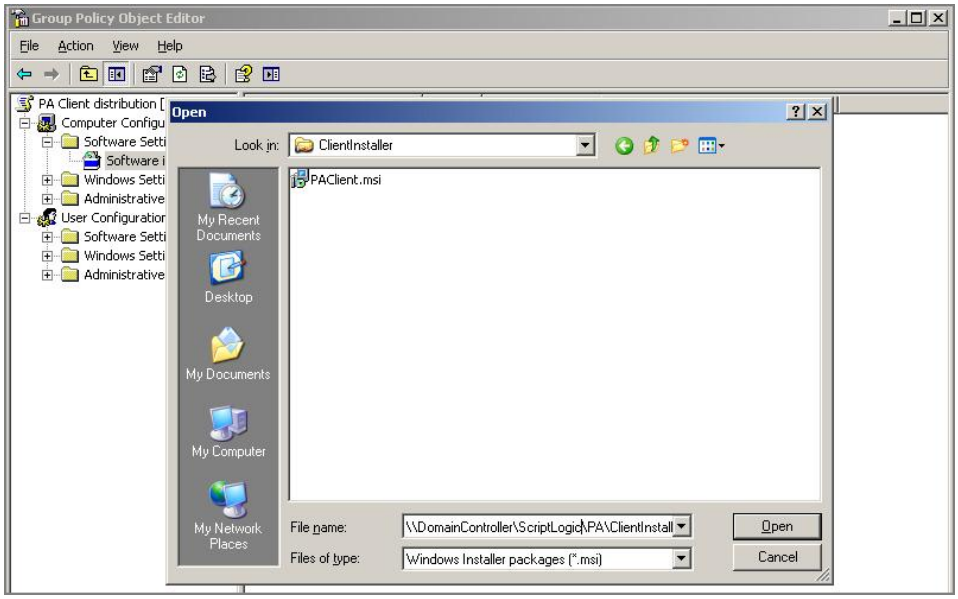

Figure 6. Opening the Privilege Authority Client from a network share.

8. In the **Deploy Software** dialog that shows, select **Assigned**.

9. Assign the new GPO to the domain or OU. To assign it to the domain, right-click on the domain in GPMC and select **Link an Existing GPO...**. Select the GPO in the resulting dialog box and click **OK**. (See Figure 7.)

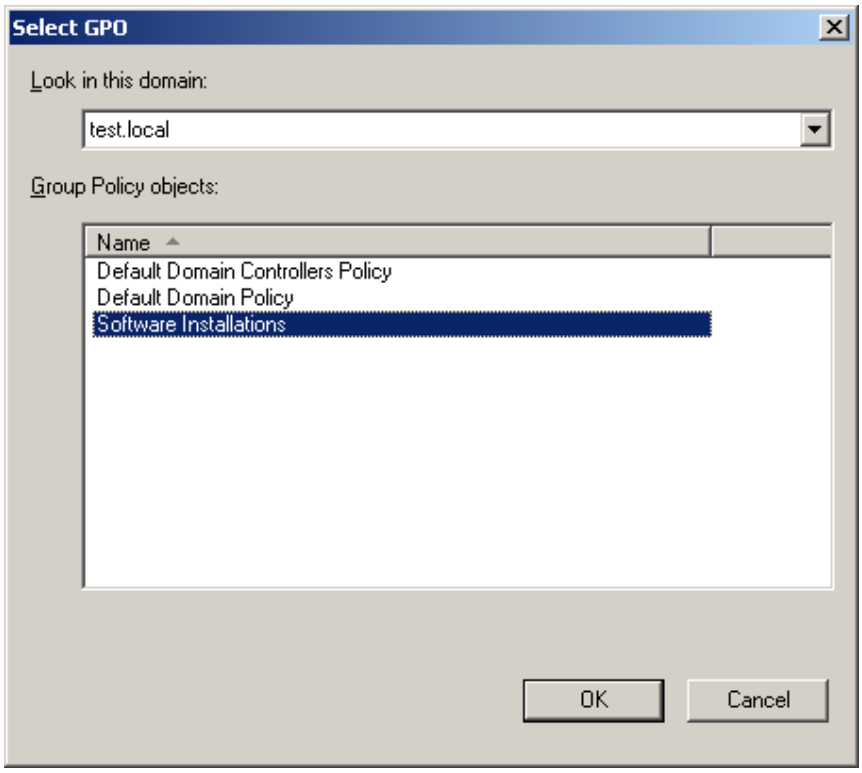

Figure 7. Assigning the new GPO to a domain.

Once the client is deployed to a computer (the `CSEHost.exe` process is running and the **Privilege Authority Client** record shows in Add/Remove Programs), the new GPO rules created via Privilege Authority are applied to running processes.

Privilege Authority Upgrade

Use the Privilege Authority 2.0 setup file to upgrade the PA Server component installed with the previous PA releases (Privilege Authority 1.1, Privilege Authority 1.2, Privilege Authority 2.0 Beta and RC) on the local computer. The upgrade also ensures that all your GPO rules created with the older version of PA will be available in Privilege Authority 2.0.

To upgrade PA Clients installed with a previous Privilege Authority release (Privilege Authority 1.1, Privilege Authority 1.2, or Privilege Authority 2.0 Beta and RC):

- Install the newer version over the older one the same way you initially installed the PA Clients.

See Privilege Authority Uninstallation and Privilege Authority Client Installation sections for more information.

Privilege Authority Uninstallation

To uninstall any of the Privilege Authority components from a local computer, use the Windows Control Panel tool. The uninstaller completely removes all the PA-specific data. Once PA is removed, the rules created with PA will continue working as they will still be present in the GPOs.

To run PA Server/Client removal on a local machine, administrative privileges are required.

If the PA Client has been installed using a network share - for example if deployed via a mass deployment tool, this network share must be available during PA Client removal (See Figure 8).

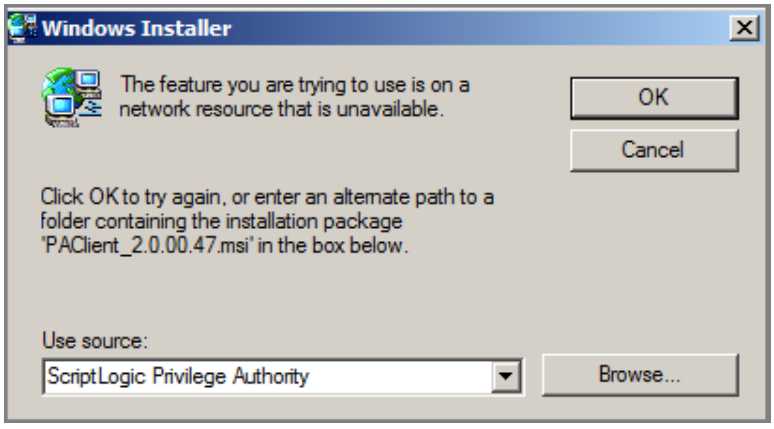

Figure 8. The PA Client removal fails as the network share is currently unavailable.

Getting Started with Privilege Authority

Once the PA Server and Client are installed on your domain, you can start using Privilege Authority to work with GPO rules in your environment.

Privilege Authority Console provides a user interface to create/manage/apply the rules. To start the Privilege Authority Console:

- On the PA Server, go **Start** > **All Programs** > **ScriptLogic Corporation** > **Privilege Authority** > **Privilege Authority**. Or, you can use the **Privilege Authority** shortcut icon of the **Start** menu.

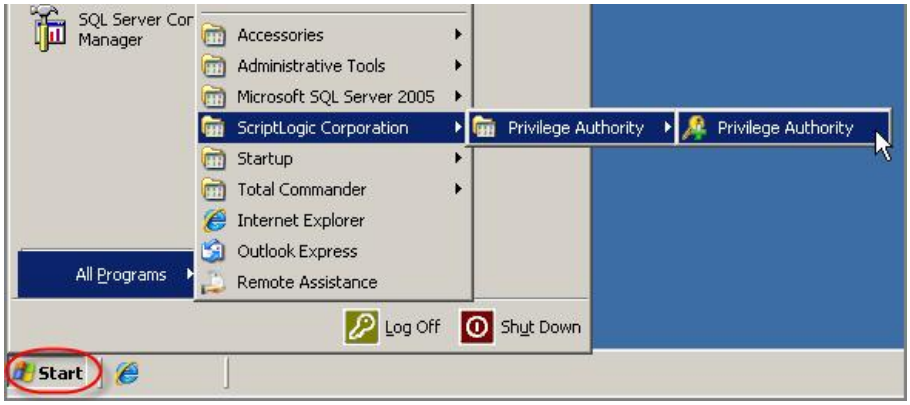

Figure 9. Opening the PA Console.

The Privilege Authority Console workspace is comprised of:

- The left-hand sidebar allows you to view the Local Rules and Community Rules that are currently available to you:
    - The **Local Rules** node displays the GPOs available within your domain within two sub-sections:
        - **GPOs with Rules** shows the GPOs with rules created via Privilege Authority;
        - **All GPOs** shows all the GPOs available in your domain. The GPOs with rules created via Privilege Authority are marked with special icons.
    - The **Community** node displays the rules available on the Community Rules Exchange server in the three sub-sections:
        - **All Rules** shows all the rules available on the Community Rules Exchange server;
        - **Verified Rules** contains the rules that have been tested by ScriptLogic to confirm they function as intended in a default Windows environment.

        - **My Shared Rules** shows the rules you have uploaded to the Community Rules Exchange server.

- The right-hand pane for the **Local Rules** node consists of:
    - The **GPO Section** to create/manage group policy objects;
    - The **Rules Section** to create and manage GPO rules.
- The right-hand pane for the **Community** node provides for the possibility to work with the rules from the Community Rules Exchange server.

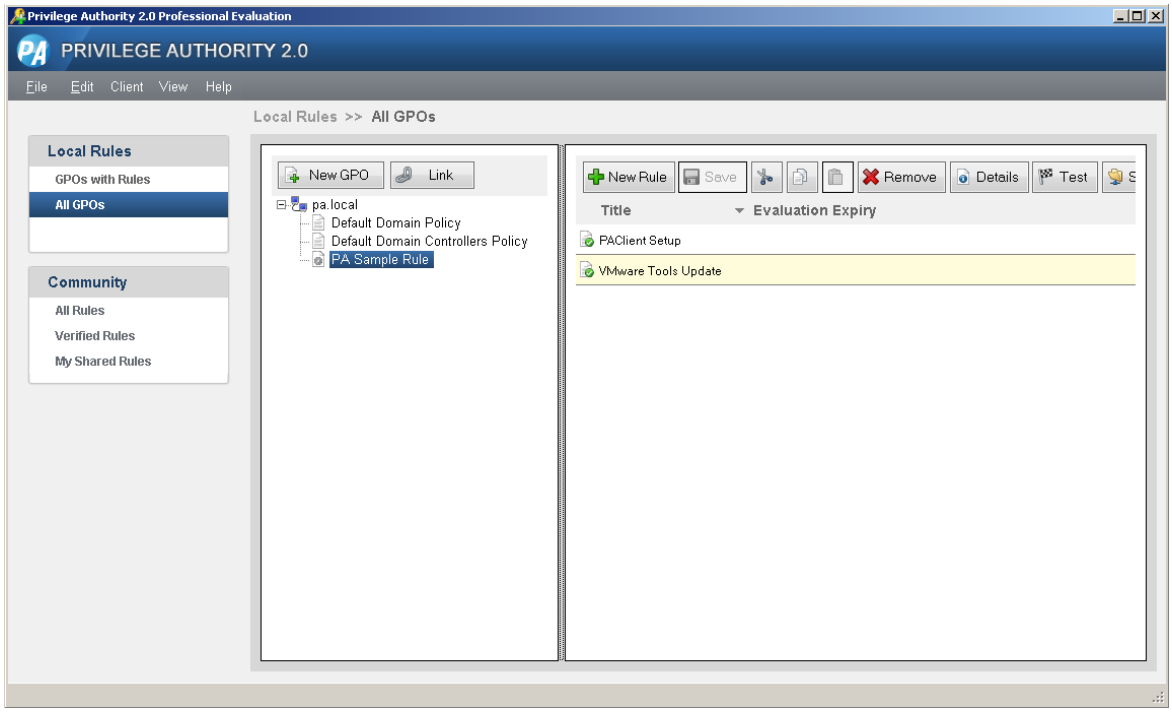

Figure 10. Privilege Authority user interface main view.

What' next:

- Creating GPO Rules with Privilege Authority
- Using GPO Rules Configured by Other Users (Community Rules Exchange)

Using Privilege Authority

This section demonstrates how to implement typical tasks within Privilege Authority and includes the following topics:

- **Creating GPO Rules with** Privilege Authority**.**
  The section will detail the types of rules PA can create and how to create them.
- Using GPO Rules Configured by Other Users (Community Rules Exchange)**.**
  This section will show how to take advantage of the integration with the Community Rules Exchange server - a new feature of Privilege Authority 2.0. With this feature, you can access the Community Rules Exchange server that stores rules created by other system administrators. You can either download these rules or upload ones you have created yourself.

CREATING GPO RULES WITH PRIVILEGE AUTHORITY

The following section will detail how to create a GPO rule within Privilege Authority.

There are four types of rules that you can create with PA:

- a file rule, where the path of the executable is specified (**By Path to the executable**);
- a folder path rule, in which case, the rule will be applied to all processes run from the path (**By Folder Path**);
- an ActiveX rule, where a URL is specified (**By ActiveX Rule**);
- (*available only within the Professional edition*) a digital certificate to specify the name of the publisher (**By Digital Certificate**).

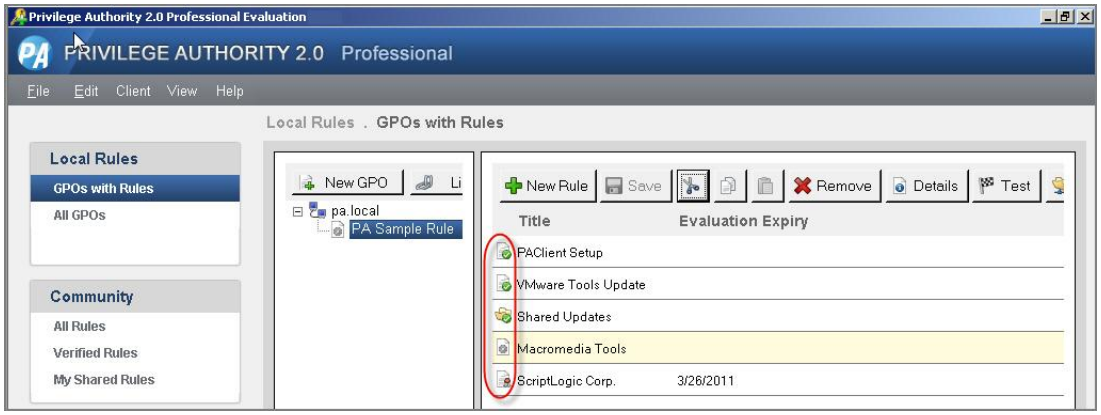

Figure 11. Different types of rules marked with special icons.

A special wizard will help you define the necessary settings for the rule.

The *Privilege Authority 2.0 Getting Started Guide* references sample GPO rule creation – the *Allowing ITunes to Install* rule.

Note

Make sure you have logged into the Privilege Authority server under the account of the domain administrator and the account is provided with the "WRITE" permissions to the SYSVOL share (\\domainName\sysvol<file:///\\domainName\sysvol>).

Step 1. Choose/Create the GPO to assign a rule to.

Within the Privilege Authority Console, navigate to the **All GPOs** node in the left-hand pane of the PA Console, select the domain and choose an existing GPO rule below it or create a new GPO to assign a rule to.

To create a new group policy object, click the **New GPO** button, name the new GPO and click **OK**. The newly created GPO will be added to the **All GPOs** list. (See Figure 12.)

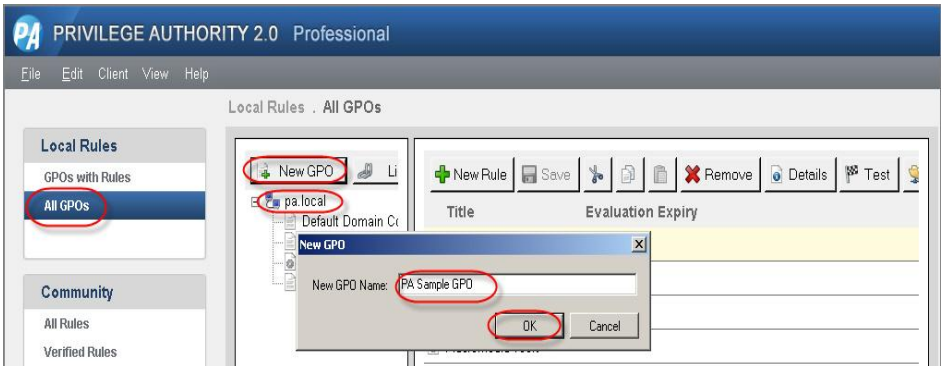

Figure 12. Creating a new GPO in the Privilege Authority Console.

Step 2. Link the GPO with an OU or the domain.

By default, the GPO is linked to the domain under which it is located. To link the GPO to a specific OU or another domain, with the GPO highlighted in the left-hand panel, click the **Link** button above it. A dialog will be displayed allowing you to browse for an OU or to select to add the GPO to the domain. (See Figure 13.)

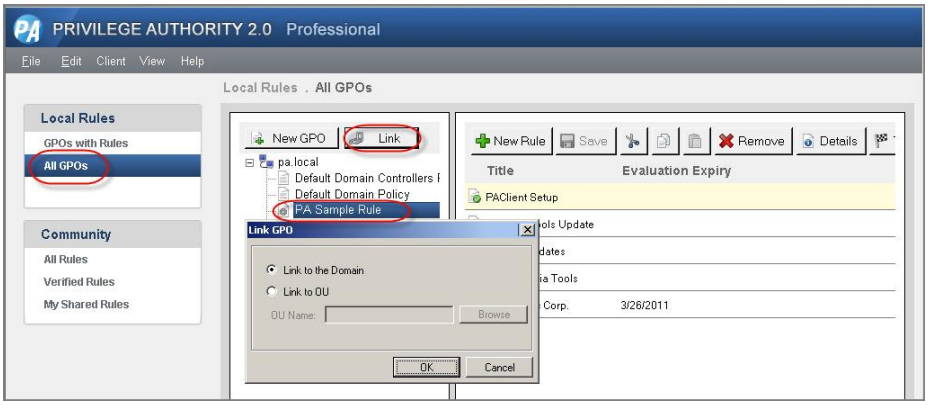

Figure 13. Add the GPO to the domain.

Note

You can link the GPO to an OU that contains users. The GPO rule linked to an OU will apply only in case the user stored within this OU is currently logged in to the client machine.

Step 3. Configure the rule within a GPO.

Within the **All GPOs** node, select the GPO from the list under the domain that your local computer is a part of. Click the  **New Rule** button and a wizard will be displayed (see Figure 14 and Figure 15). Walk through the wizard by clicking **Next** to specify all the necessary data to configure the rule.

The wizard's steps are referenced in the *Using the Wizard* section.

Or, use the GPO rules other system administrators have configured and uploaded to the Community Rules Exchange server.

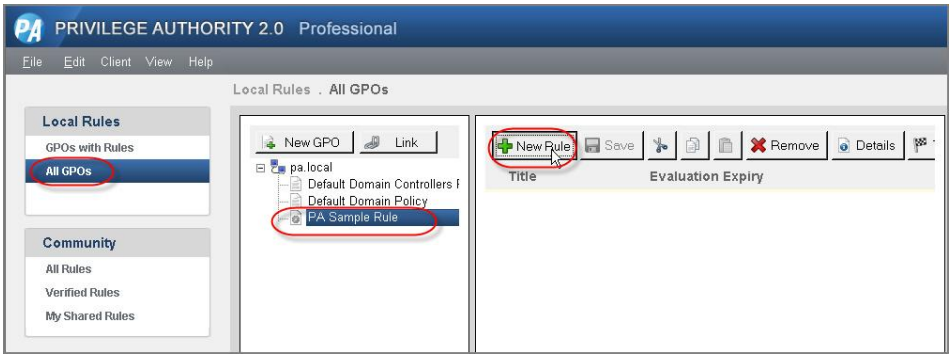

Figure 14. Selecting to add a rule to existing GPO.

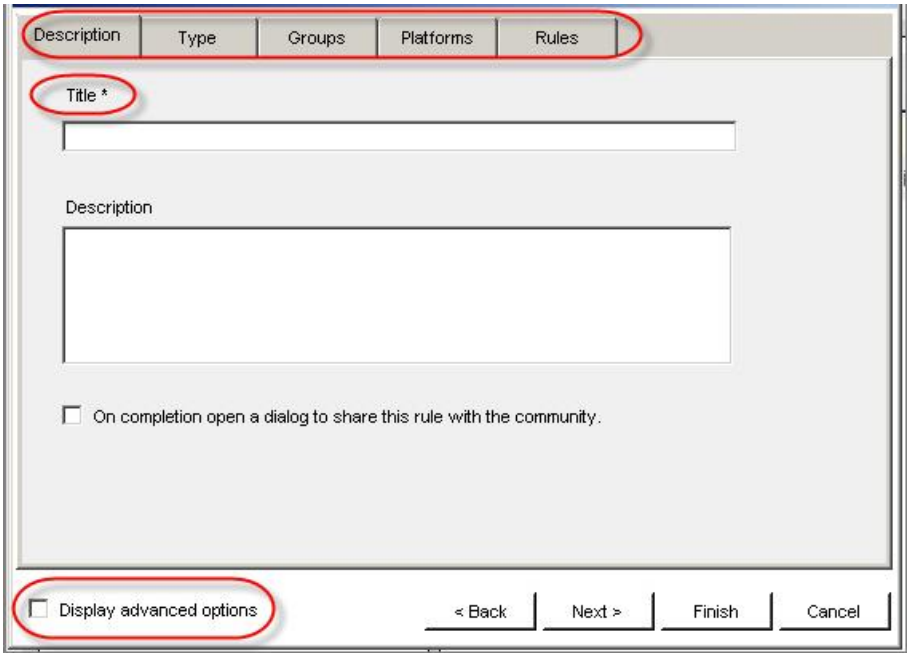

Figure 15. The Privilege Authority wizard's main window.

Step 4. Save the rule.

Upon completing the wizard, click the **Save** button on the menu bar of the **Rule** section. Or, if asked, confirm the saving of the rule. (See Figure 16.)

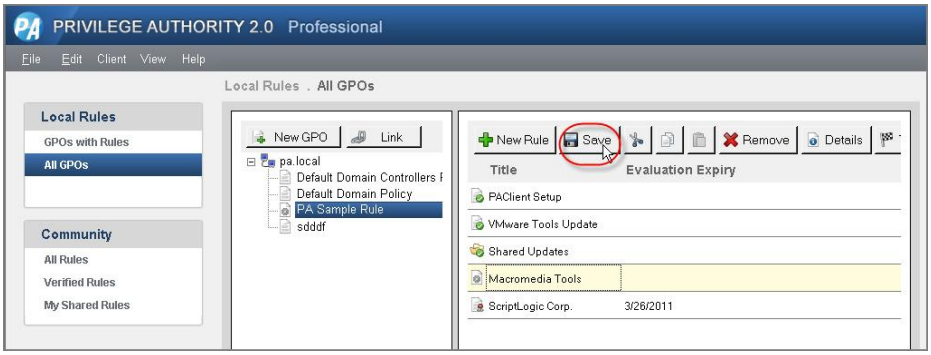

Figure 16. Save the rule.

Once the rule is created, the GPO's icon will get marked with the icon to notify that the GPO contains a rule and will be listed within the **GPOs with Rules** node. (See Figure 17.)

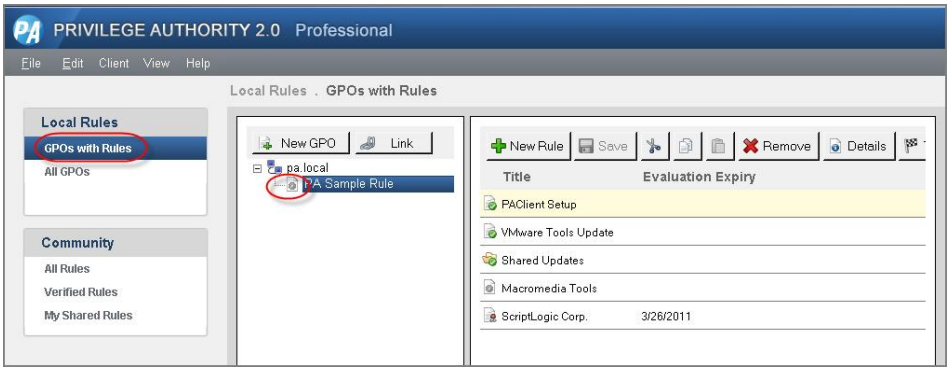

Figure 17. The marked-in icon indicates that GPO is assigned with a rule.

The rule will be applied to the processes started on the client machine right after the group policy update occurs on the client machine.

Once the rule is created, you can:

- Test its settings and the way it will apply (see the *Testing and Applying the Rule* section).
- Share your rule on the Community Rules Exchange server (see the *Sharing your Rules with the Community* section).
- Edit or delete the rule (see the *Managing the Rules* section).

Using the Wizard

A special wizard will help you define the necessary settings for the rule.

To run the wizard:

1. Within the **All GPOs** node, select the GPO from the list under the domain that your local computer is a part of. You may also click the  **New GPO** button to create the GPO, if necessary.
2. Click the  **New Rule** button and a wizard will be displayed (see Figure 18).

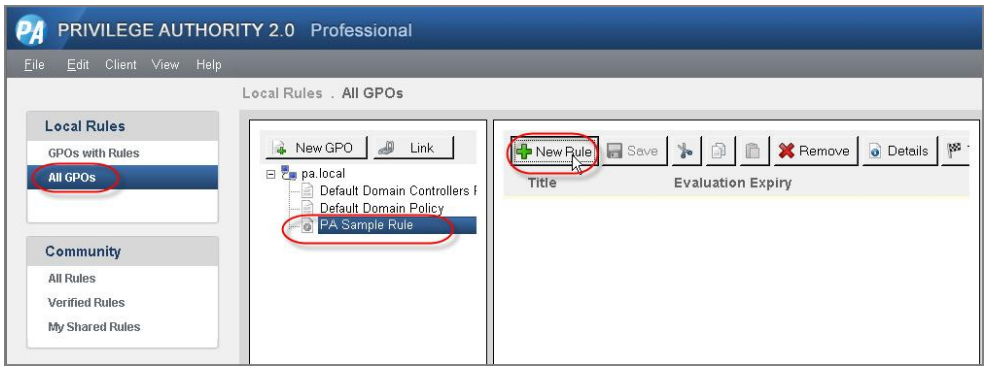

Figure 18. Selecting to add a rule to existing GPO.

3. Walk through the wizard by clicking **Next** to specify all the necessary data to configure the rule.

   The list of steps defaults to **Description**, **Type**, **Groups**, **Platforms**, and **Rules** (with **Platforms** and **Rules** available only in PA Professional). The **Privileges** and **Integrity** steps show as advanced options.

   Only the fields marked ***** on the **Description** and **Type** tabs of the wizard are mandatory, all the others are optional. If you happen to miss specifying any of the required data, the wizard will warn you on this right after you click **Finish**.

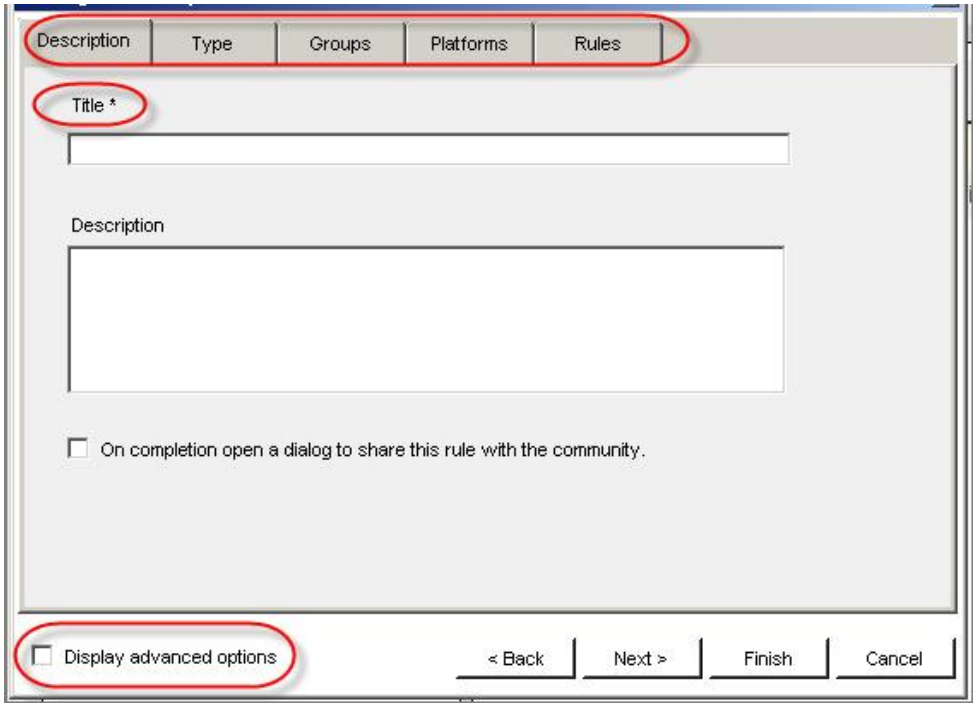

Figure 19. The wizard main window.

   All the steps of the wizard are detailed in the following corresponding sections:

   - Using the Type tab
   - Using the Description tab
   - Using the Groups tab
   - Using the Platforms tab
   - Using the Rules tab
   - Using the Privileges tab
   - Using the Integrity tab

4. Click **Finish** to save and apply the rule.

(*If applicable*) If, on the Description step of the wizard, you have chosen to share the rule with the community, confirm or edit in the dialog that will open on the final step of the wizard.

Figure 20. Setting the details to share the rule.

Using the Description tab

On the first screen of the wizard:

- Enter a name and an optional description for the rule so you can identify it.
- You may also choose to share your rule with the community by selecting the **On completion open a dialog to share this rule with the community** box. You may also choose to share the rule at any time later, when you have tested the rule.

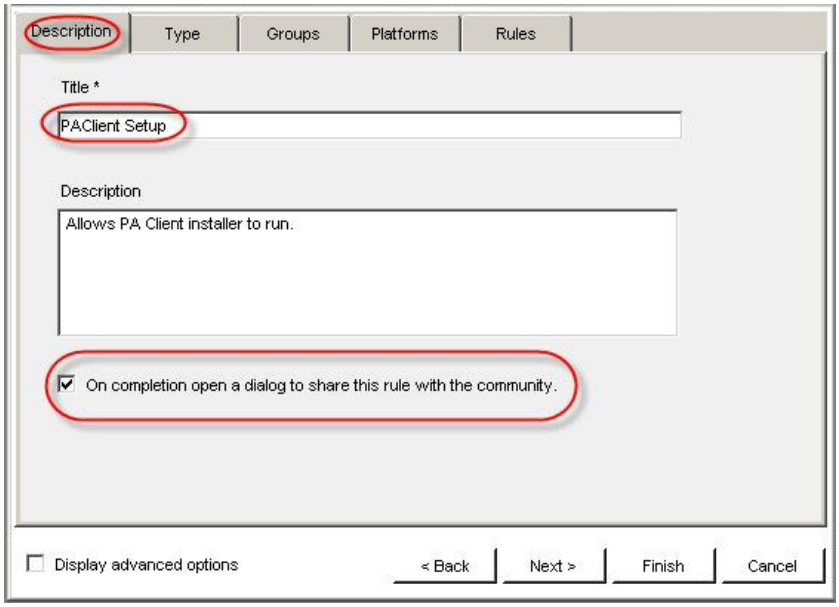

Figure 21. Specify a title and share the rule with the community.

If you choose to share the rule, you will be presented with the Privilege Authority Community Forum registration dialog referenced in the *Registering with the Community Rules Exchange Server* section.

Using the Type tab

Within the **Type** tab, you will specify the most essential parameters of the processes for which the current rule will apply to. Here you are given a choice of several rule types (the number of types varies depending on the Privilege Authority edition):

- By Path to the executable
- By Folder Path
- By ActiveX Rule
- (*available only within the Professional edition*) By Digital Certificate

Select the type and specify the corresponding options that depend on the selected type. The options are detailed below.

By Path to the executable

When building the **By Path to the executable** rule type, specify the following fields (see Figure 22):

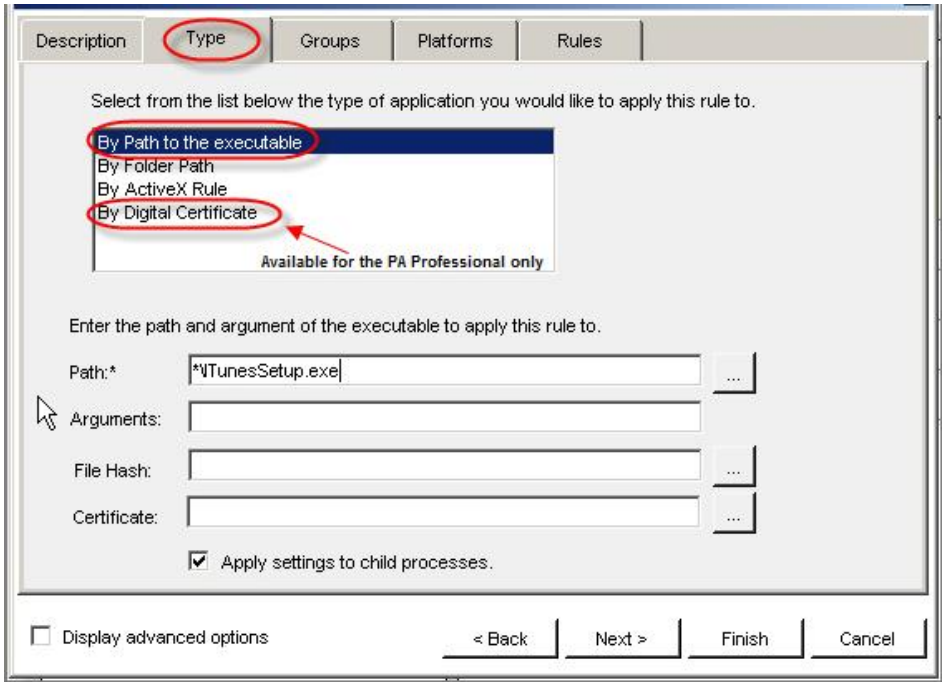

Figure 22. Specify the GPO rule type and fill in the required field.

- **Path** – requires that you specify the path to an executable that will run the processes on the client machine. This may be a path on the client local machine or a network share. Use the common variables % or * to identify the path, e.g. `*\filename.exe`.

  Use the following formats: `\\ComputerName\SharedFolder\Resource` or `DriveLetter:\Filename.exe`.

Note

When saving the "By path to an executable" rule, consider that PA converts the specified path into existing environment variables.

If you use the **Browse** button to locate the executable, a dialog will show and offer to create a unique cryptographic hash for the file to secure the file's identification (see Figure 23). Click **Yes** if you want to apply the rule to only this exact file. Click **No** if you are creating the rule for the file for which data is likely to be updated, or for any file with this name within the specified folder.

Figure 23. Choose if you need to create the file hash.

- (*Optional*) In the **Arguments** field, specify the common or user-defined arguments with which the executable will be run. With this field defined, the rule will apply only if the executable is run with the argument specified.
- (*Optional*) If creating the rule for an exact file, the **File Hash** field will help you prevent security issues. Click the **Browse** button to locate the executable and to create a unique cryptographic hash for the file so that the rule will not apply to dangerous content that is similarly named.

Note

The rule with the File Hash field specified will not apply to a file that has modified content (e.g. modified in the course of program updates). Thus do not add the file hash to the rule for a file which data is likely to be updated, or for any file with this name in the specified location.

- (*Optional*) (*Available for PA Professional*) For the sake of security, specify the publisher of the digital certificate for the specified file. Enter the exact publisher name either manually or use the **Browse** button to locate the file signed with the necessary digital certificate.
- The **Apply settings to child processes** check box is enabled by default to ensure that all operations the executable will trigger will run successfully and will not fail due to lack of privileges.

By Folder Path

Use the **By Folder Path** rule type if you have to elevate/decrease the privileges for the applications/processes that will start from within a specific folder on the client local machine or a network share.

- Use the **Browse** button to locate the folder or specify its location manually. Use the common variables % or * if necessary, e.g. `*\filename.exe`.
- (*Optional*) The **Apply settings to subfolders** setting will apply the rule to the processes started from any of the subfolders.
- The **Apply settings to child processes** check box is enabled by default to ensure that all the operations the executables trigger will run successfully and will not fail due to lack of privileges.

By ActiveX Rule

Use the **By ActiveX Rule** type to allow installation of ActiveX controls from the Internet.

- In the **Source URL** field, specify the ActiveX control URL, e.g.

  `http://*.macromedia.com*`

By Digital Certificate

(*Available only within the Professional edition*)

The **By Digital Certificate** rule provides for the possibility to apply certain privileges to any processes signed with a digital certificate of a specified publisher.

- Specify the publisher of the digital certificate of the processes for which you need to set the rights. Enter the exact publisher name either manually or use the **Browse** button to locate a file signed with the necessary digital certificate and insert the publisher automatically.
- The **Apply settings to child processes** check box is enabled by default to ensure that the rule settings will be applied to the child processes as well.

Using the Groups tab

(*Optional*)

The next tab is where you select an Active Directory user group whose rights are to be applied to the process. A group can be added or removed from a process. By removing a group from a process you can decrease the privileges with which the process will run.

- Click the button to add the Administrators group (this is the group stored within the BUILTIN\Administrators Active Directory OU) to the list (see Figure 24) We recommend using this group of users with complete and unrestricted access to a local computer instead of domain administrators.

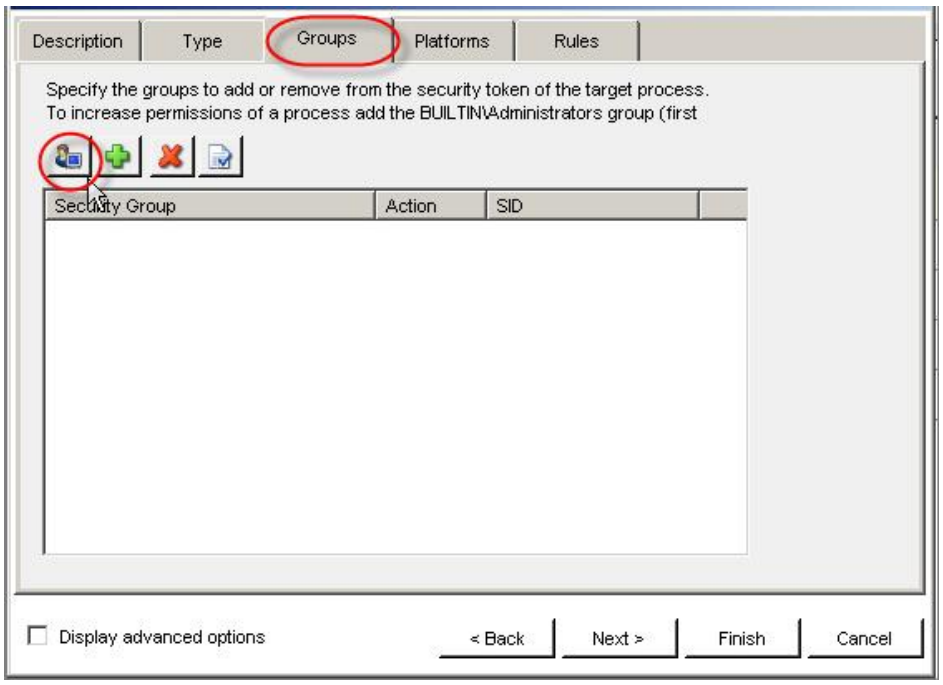

Figure 24. Add the Administrators group to the security token of the process.

- To add/remove any other Active Directory group privileges to the process(es), use the button. In the window that will open, specify the action, add or remove, you need to perform with the group.
- To delete/modify the record within the **Security Group** list, use the or buttons.

Using the Platforms tab

(*Optional*)

(*Available only for Privilege Authority Professional*)

Within this tab, you can define on which computer type, server or workstation, or with which operating system(s), the rule will apply. (See Figure 25.)

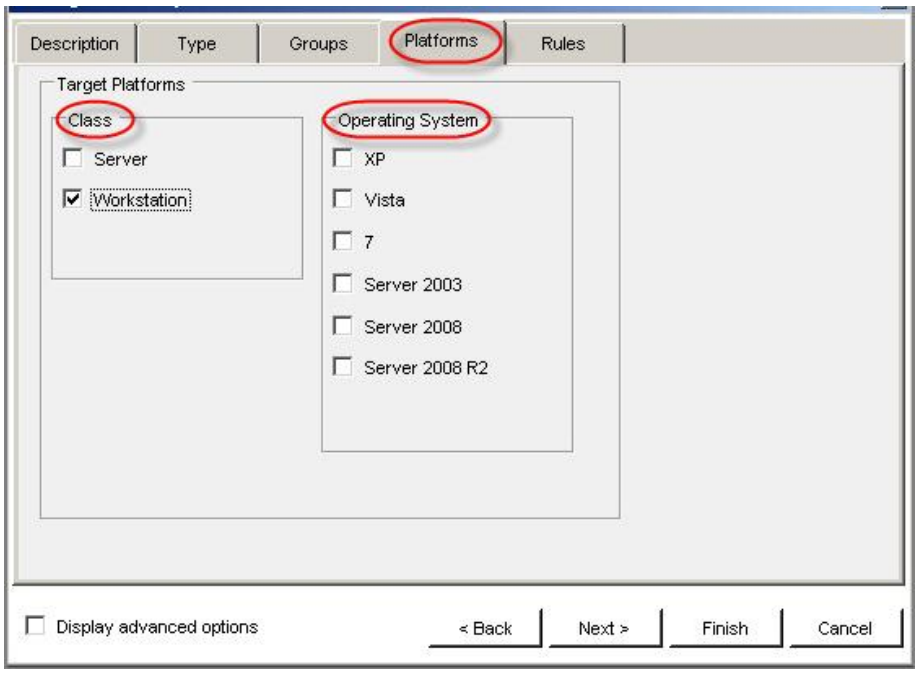

Figure 25. Specify the platforms to apply the new rule on.

- Select the **Server** option of the **Class** list to apply the rule to all the Windows Server operating systems: Windows Server 2003/2008/2008 R2.
- Select the **Workstation** option of the **Class** list to apply the rule to all operating systems, Windows XP/Vista/7, other than the Windows Server operating systems.
- Select the exact Windows operating system by marking the corresponding option(s) of the **Operating System** list.

Using the Rules tab

(*Available only for Privilege Authority Professional*) (*Optional*)

The **Rules** tab allows you to specify additional granular settings to apply to the process. It may include whether it should/should not run on a computers with certain prefix in the name, or pertaining to some special group or IP address range, etc. (See Figure 26.)

You can add the following validation logic parameter(s):

- **Computer Name**,
- **Computer Group**,
- **Computer OU**,
- **IP Address Range (IP v4/IP v6)**,
- **File Exists**,
- **Registry Key Exists**.

To set the rule parameters within the **Rules** tab:

1. Click **Add** to open the **Add Validation Logic Rule** window.
2. Within the window, select the type of logic to the rule, and then specify the logic parameters. When specifying the logic parameters:
    - you can use the common * and % variables;
    - select the **Not** operator to exclude the item(s) specified from the rule if necessary.

    When specifying the **Computer Name**, **Computer Group**, and **Computer OU** sections:

    - Enter the name/part of the names of the computers on which to apply the rule. Use the **Browse** button to view the computers on the domain/network.

    In the **File Exists** section, set a certain file that must exist on the client machine or on the network in order for the rule to run. Use the following formats: `\\ComputerName\SharedFolder\Resource` or `DriveLetter:\Filename.exe`.

    In the **Registry Key Exists** section, set the registry key that must exist on the client machine in order for the rule to run.

    Click **Save** when finished specifying the rule logic settings. The logic record will show on the main **Validation Logic Rules** screen.

3. To add another logic rule, specify whether it will be an AND or OR rule, and then repeat steps 1 through 2.

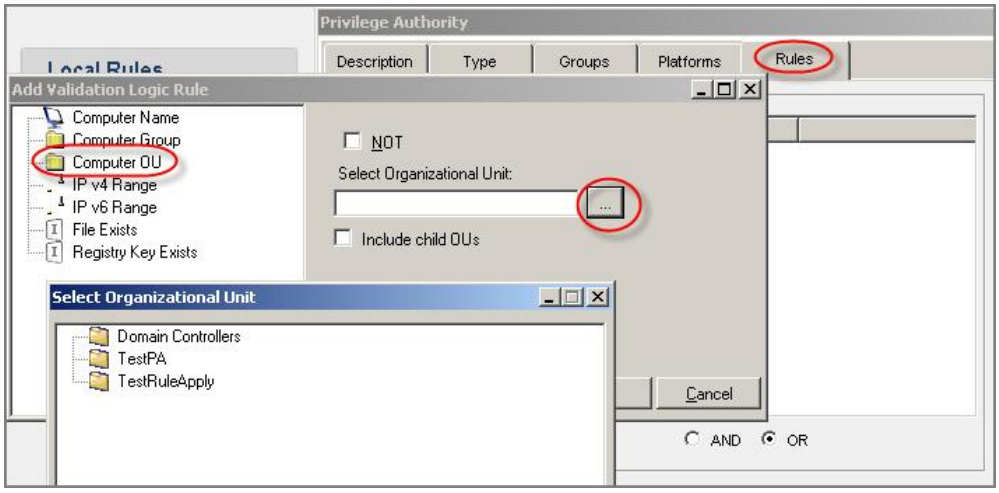

Figure 26. Specify additional parameters to the rule.

Using the Privileges tab

(*Available as advanced option*)

On the **Privileges** tab you can grant or deny certain privileges the process can perform. The privileges are the standard Windows policies listed in the User Rights Assignment list (Local Security Settings \ Local Policies).

- To apply/deny a privilege(s) to the processes (including child processes), select the necessary one(s) and then click **Grant**/**Deny**. Multi-select privileges with the **CTRL+** buttons.
- To discard your choices, select the privilege and click **Not Set**.

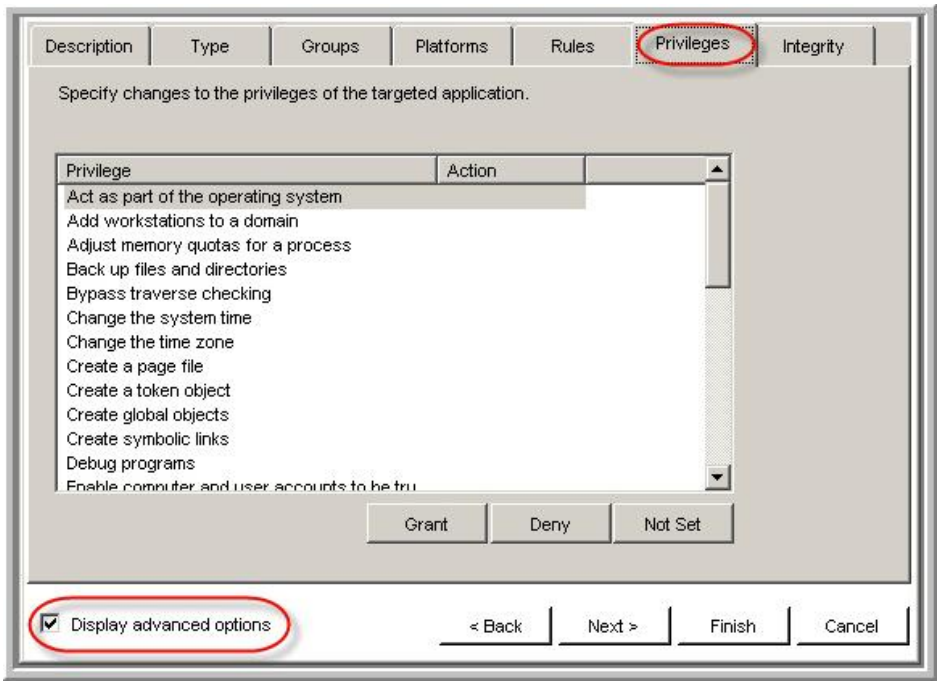

Figure 27. Specify changes to the privileges of the application.

Using the Integrity tab

(For Windows Vista, Server 2008/2008 R2 and Windows 7 OSs)

(*Available as advanced option*)

The integrity level is an inner feature of the Windows operating systems beginning with the Vista operating system. It is used to differentiate the security level with which the process will run.

By default this setting does not apply and is set to the **Untrusted level** option.

TESTING AND APPLYING THE RULE

Note

To test the rule on your local computer, ensure the computer is installed with the PA Client.

Privilege Authority offers the possibility to test the settings of the rule created with Privilege Authority. During the test you can simulate the process to which the rule is to be applied on the PA server machine.

To test the rule:

1. Select the rule, and then click the  **Test** button. The command will start the **Test File Rule** window to test the rule on your local machine. The window shows the steps necessary for the rule to run and present their status in the **Test Progress** section:

   - if the PA Client is installed on your computer (use the link to know how to install the client locally on the PA Server machine);
   - if the Group Policy update has run successfully on your computer;
   - if the specified GPO is present on the domain;
   - if the rule exists on the client side and on the domain.

   If the test fails on any of the steps, resolve the issues before continuing with the rule testing.

2. Once the **Starting Process Monitor** window is presented, manually run the process the rule will apply to. Note that you should run the process with the parameters specified in the **Rule Details** section of the **Test File Rule** window. Click **Continue**.

3. The **Test File Rule** window content will change and show the two tabs: the **Started Processes** tab with the processes started right after you have continued with the **Starting Process Monitor** window and the **All Processes** tab with all the currently running processes. The process that you've started to test the rule will show in the list of the **Started Processes** tab with either the "tick" or "cross" sign. If the process is crossed out, look at the **Process Details** and either check that you started the process with the right parameters or modify the rule settings.

MANAGING THE RULES

Once the rule is created, you can change its settings or delete the rule, or upload the rule to the Community Rules Exchange server.

- To delete, modify or share the selected rule with the community, use the corresponding toolbar buttons (see Figure 28).

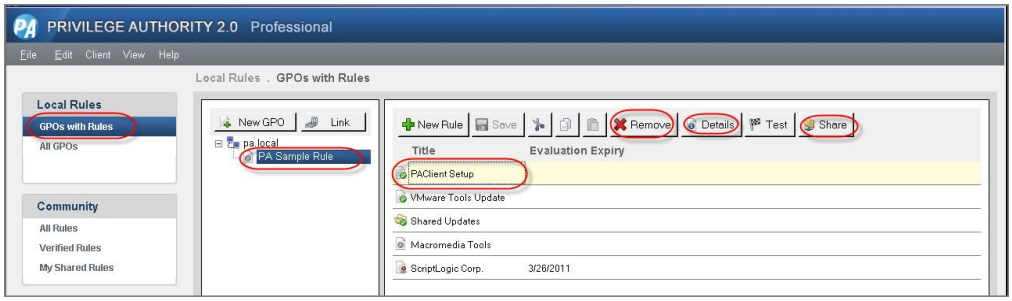

Figure 28. Use the toolbar to manage a GPO rule.

- To delete a GPO created with Privilege Authority, use Microsoft Group Policy Management Console.

If you are using the Privilege Authority Community Edition and try to access a rule with any of the Privilege Authority Professional features, to view or modify its settings, a special notification will show (see Figure 29). By clicking **Yes**, you'll open the **Edit Rule** window that will show all the rule settings except for the Professional ones. Modifying the rule will not discard any of the Professional features.

Figure 29. Accessing a rule with a Pro feature running PA Community Edition.

USING GPO RULES CONFIGURED BY OTHER USERS (COMMUNITY RULES EXCHANGE)

The ScriptLogic team has created and supports a special GPO rules database stored on the Community Rules Exchange server. By using the Community Rules Exchange feature, you can make use of the GPO rules other system administrators have shared on the server as well as upload your own rules.

You can also access the database to get a sample list of GPO settings that may be used in an environment and know how they can be defined with Privilege Authority.

This feature is available within any of the Privilege Authority editions.

- Once you open the Privilege Authority Console, click **All Rules** located under the **Community** node. The list of rules will show (provided that you are connected to the Internet). (See Figure 30.)

Figure 30. The Community Rules list.

Use the **Community** rules to:

- apply the Community rules in your domain
- share your rules with the community
- comment and rate the Community rules.

Applying Community Rules to your Domain

To make use of a certain rule within the **Community** list or just to see how the GPO settings can be configured with Privilege Authority:

1. Within the **All Rules** section of the **Community** node of the Privilege Authority Console, select the rule, and then click the **Import** icon. A dialog containing the rule settings will open. (See Figure 31.)

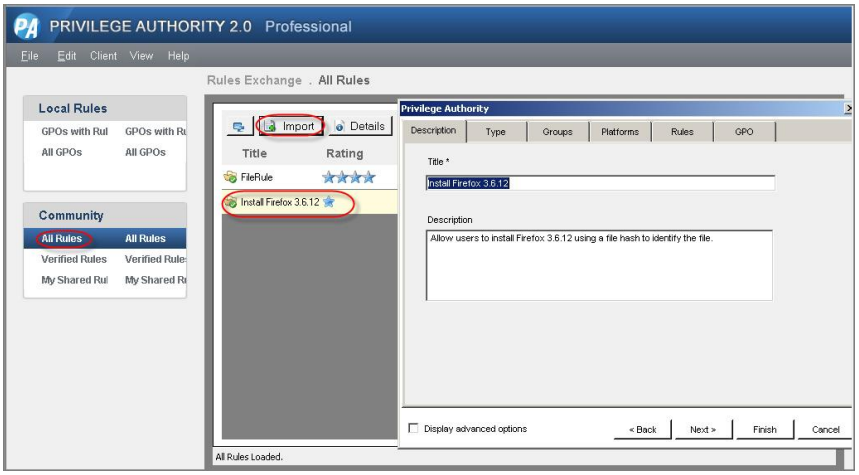

Figure 31. Opening the community rule dialog.

If you are using the Privilege Authority Community Edition and try to import a rule with any of the Privilege Authority Professional features, a special notification will show (see Figure 32). By clicking **Yes**, you'll open the **Import Rule Wizard** window that will show all the rule settings except for the Professional ones.

Figure 32. Importing a rule with a Pro feature running PA Community Edition.

2. (*Optional*) You may switch between the available tabs of the dialog to view its settings or adjust the GPO rule to your needs.

3. Click the **GPO** tab to assign the rule to an already existing GPO in your environment. (Follow the link if you'd like to create a custom GPO to link the rule to.) (See Figure 33.)

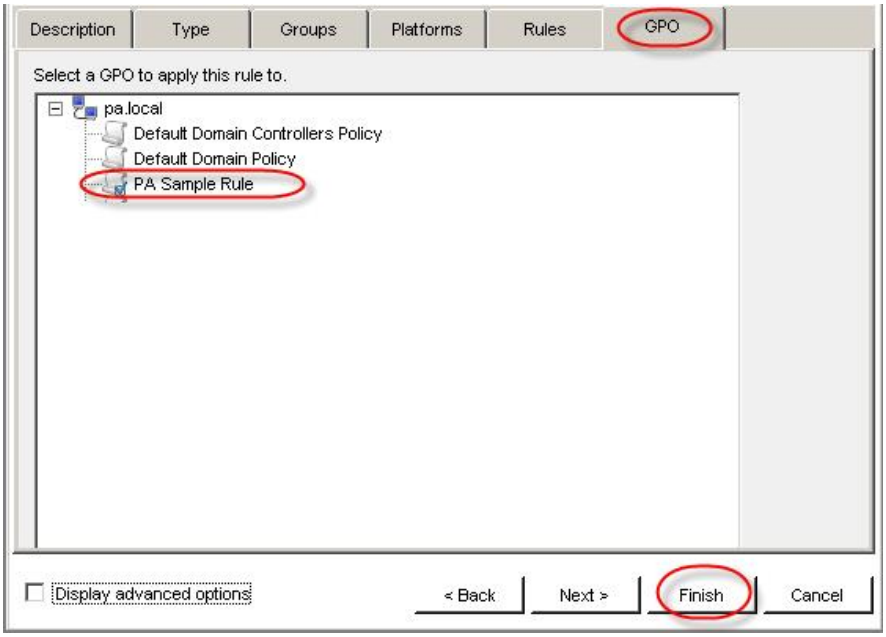

Figure 33. Selecting a GPO to apply the rule to.

4. Click **Finish** to add the rule to your domain's GPO settings.

The rule will now display in the list of rules of the corresponding GPO under the **Local Rules** node. (See Figure 34.)

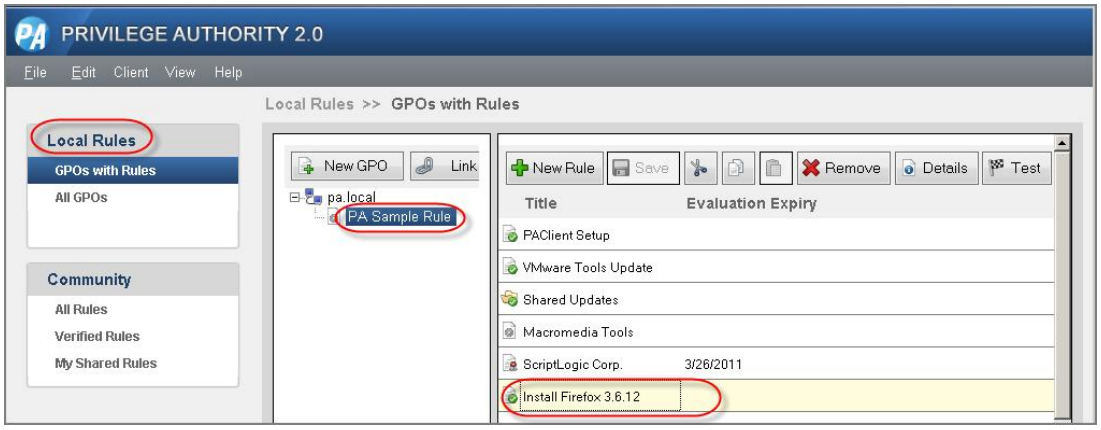

Figure 34. A community rule has been set to apply to a GPO in your domain.

The rule will apply once the Group Policy is updated on the client machine.

When the rule displays within the **Local Rules** node, you can administer it as any ordinary PA rule.

Sharing your Rules with the Community

To share your rules that you think other system administrators might find useful:

1. Within the **Local Rules** node, right-click the desired rule to share, and then select **Share with Rules Exchange** within the shortcut menu. (See Figure 35.)

Figure 35. Selecting a rule to share.

2. Within the window that opens, make any necessary changes to the GPO rule settings, and click **OK**. (See Figure 36.)

Figure 36. Modifying and confirming to share the rule.

3. (*If applicable*) If you have not registered at the Privilege Authority Community Forum, you will be presented with the registration/login dialog. The dialog is detailed in the *Registering with the Community Rules Exchange Server* section.

Once the registration is complete, the rule will be displayed under the **Community** node in the **All Rules** section as well as within the **My Shared Rules** list. (Figure 37.)

Figure 37. The rule has been successfully uploaded to the Community Rules Exchange.

Managing the Community Rules

To delete the rule that you've shared from the **Rules Exchange All Rules** list:

- From within the **My Shared Rules** section, select the rule, and then click the **Delete** toolbar button. The rule will be deleted after the operation is confirmed.

To modify the settings of the rule that you've shared:

1. Use the Local Rules node, to make the necessary changes.
2. Upload the rule with changes to the Community Rules Exchange site. The rule's info will be updated automatically.

Within the **Community** node, you can modify the title or description of the rule that you've shared:

- From within the **My Shared Rules** section, select the rule, and then use the icon to set the rule's title and description info as necessary.

To rate any rules uploaded to the Community Exchange Server:

1. From within any section of the **Community** node, right-click the desired rule, and then choose between the **Not set**, **Poor**, **Fair**, **Good**, **Very Good**, or **Excellent** option of the **My Rating** sub menu.
2. Your rating will be saved and the average total will show in the **Rating** column of the grid.

To comment the rules uploaded to the Community Exchange Server:

- From within any section of the **Community** node, double-click the desired rule, and then use Add Comment button to place your comment. Registration at Community Rules Exchange is required.

REGISTERING WITH THE COMMUNITY RULES EXCHANGE SERVER

When you upload your rules to the the Community Rules Exchange Server, view the **My Shared Rules** node content, or want to place a comment on a Community rule, you first have to be authorized by the server. To do this, fill in the **Register or Sign-In** form (see Figure 38):

- If you are already registered on the forum, enter your email and password in the corresponding fields of the **Login** section and click **Login**.
- If you are not yet registered with the community, click on the **Register on the web** link. You will be directed to the Privilege Authority Community Forum registration page. Fill in every field of the form that will be shown. Click **Register**.

  You may also use the **Register** tab of the dialog, to fill in the registration form.

When registering/logging into the community server, please note that the password restriction policy must compile with the current password policy of the Rules Exchange Server, e.g. currently it must consist of at least 7 characters.

Figure 38. Registering to upload to the Privilege Authority Community Exchange server.

Tip

To prevent connection problems when registering over the internet, consider specifying your proxy server settings in the PA Console before you proceed with registration.

To switch to a different user account:

- Click **Help** -> **Logout of Rules Exchange**. Now, when required, you'll be asked to provide your new login details.

TROUBLESHOOTING CONNECTION PROBLEMS

If the **Rules Exchange All Rules** list does not populate automatically or you fail registering with the Rules Exchange forum, try specifying your proxy settings within the Privilege Authority Console to solve the issue.

- To open the **Proxy Server Settings** window, click **Help** -> **Proxy Settings**, and specify the proxy server data in the window that will open.

Figure 39. Specifying the proxy server settings.

Index