Privilege Authority 2.0

Quick Start 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.

Privilege Authority Editions

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:

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** (see Figure 1).

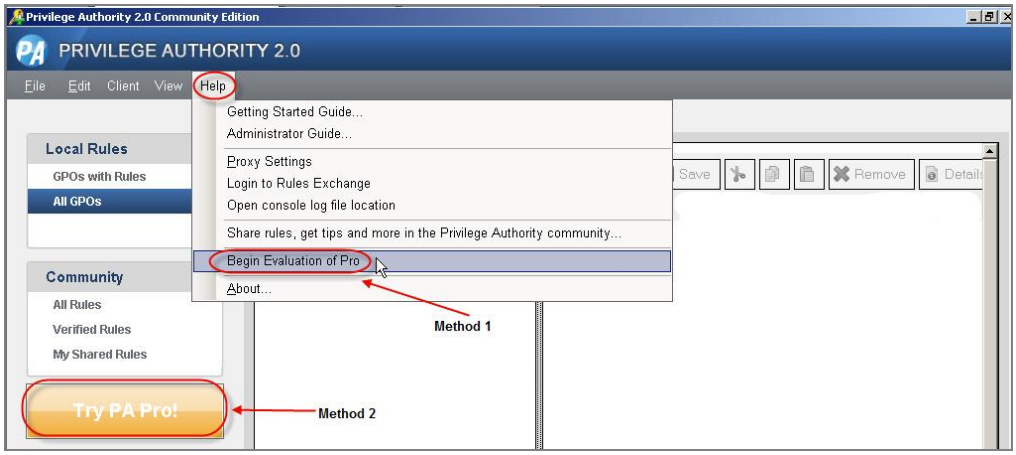

Figure 1. Choosing to use PA Professional in trial mode.

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**.

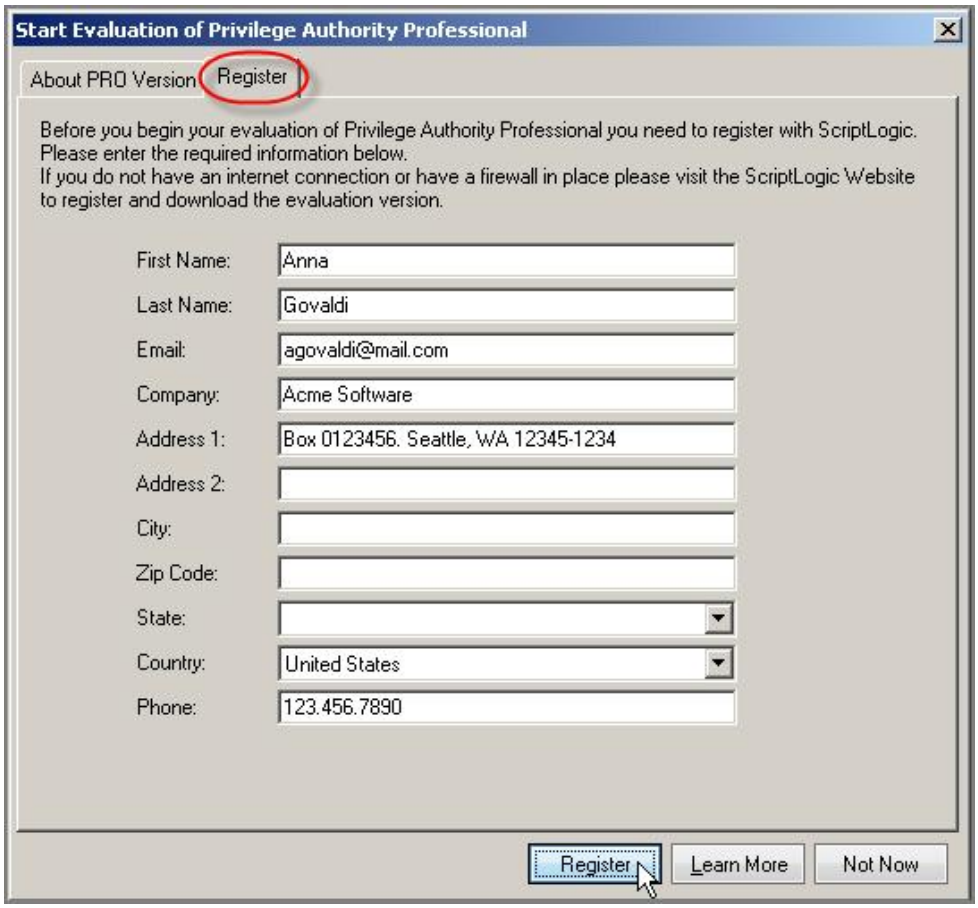

Figure 2. Registering for Privilege Authority Professional.

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**. (See Figure 3.)

Now you have access to all Privilege Authority Professional features for the 30-day trial period.

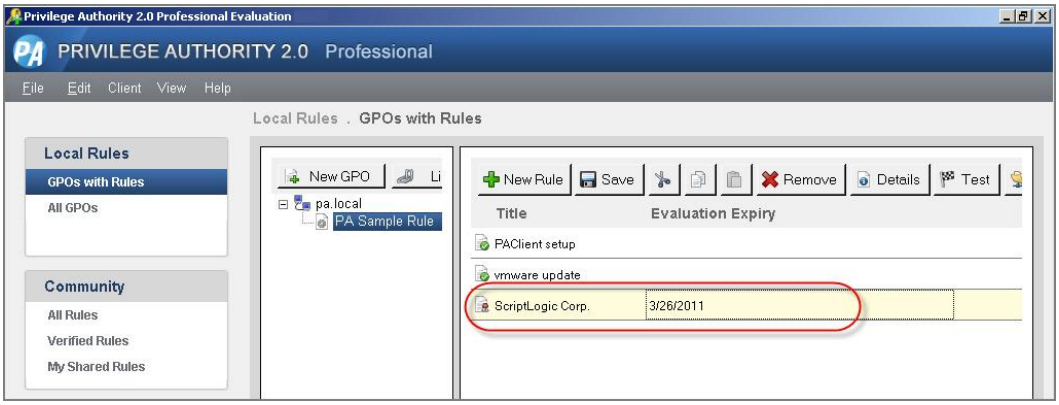

Figure 3. This rule is based on a digital certificate - the Privilege Authority Professional Evaluation feature – and it will be applied until the day specified.

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 applications are necessary for proper installation and operation.

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

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.

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.

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 locate the PA Client file:

- Click **Client** > **Open file location** within the Privilege Authority Console toolbar

Refer to *Privilege Authority Administrator's Guide* to know how install the PA Clients on your domain via Microsoft Group Policy Management Console

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.

Getting Started

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

- Creating GPO Rules to Apply Privileges in your Environment
- Using GPO Rules Configured by Other Users (Community Rules Exchange)

CREATING GPO RULES TO APPLY PRIVILEGES IN YOUR ENVIRONMENT

There are 4 types of rules that you can create with Privilege Authority:

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

Creating rules with Privilege Authority is easy. To create a rule:

1. Select the domain and GPO to which assign a rule. (Create a special GPO first if necessary.)
2. Assign the GPO to an Active Directory OU or domain.
3. Use the wizard to define a new Privilege Authority rule within a selected GPO.

   Or, use GPO rules other system administrators have configured and shared in their environments.
4. Save the rule.
5. (*Optional*) Upload your rule to the Community Rules Exchange server.
6. The next time Group Policy is refreshed on the client, the rules are applied to processes when they are launched.

The following section will detail the common way to create a GPO rule within Privilege Authority.

Allowing ITunes to Install

In this section we will create a rule that will allow users to install an application that is downloaded from the internet, in this case the `ITunesSetup.exe` file. This application requires administrative privileges to be installed. (See Figure 4.)

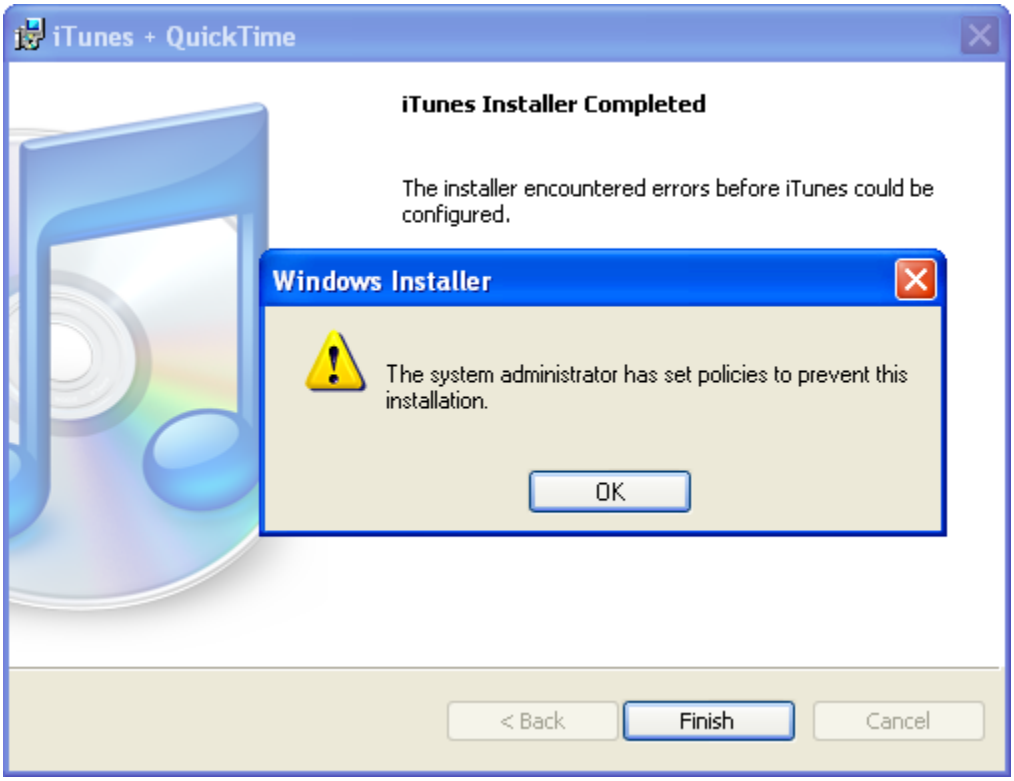

Figure 4. Error shows when installing an application without proper permissions.

To create a GPO rule via Privilege Authority:

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. Start the Privilege Authority Console.

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

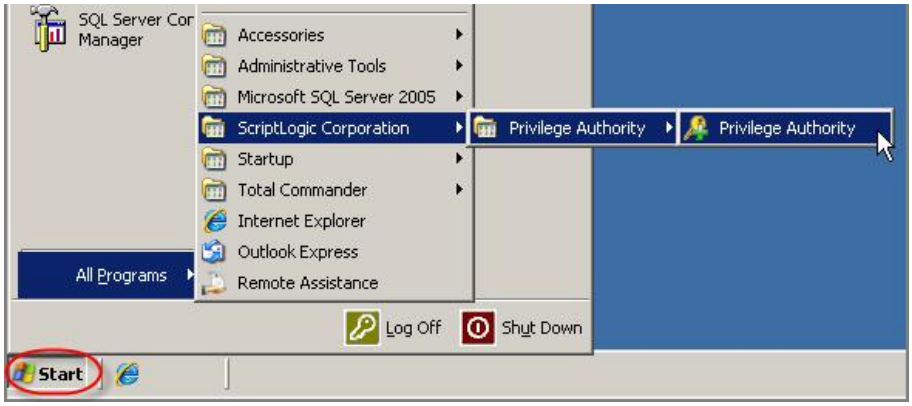

Figure 5. Opening the PA Console.

Step 2. Choose/Create the GPO to assign a rule to.

Navigate to the **All GPOs** node in the left-hand pane of the PA Console, select the domain and then choose/create the 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 6.)

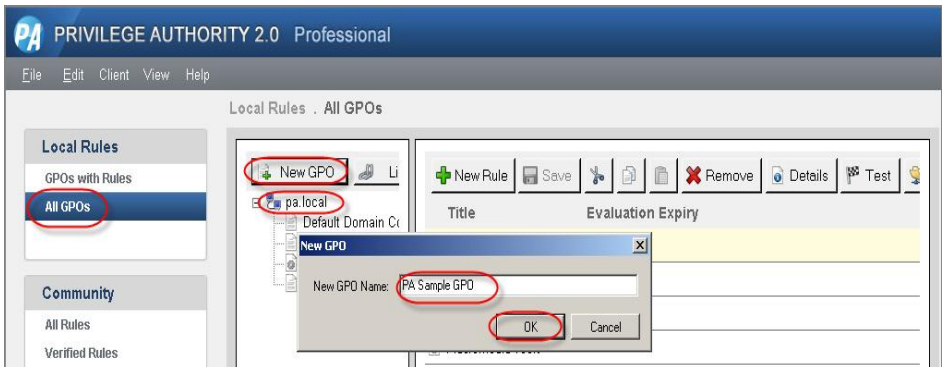

Figure 6. Creating a new GPO in the Privilege Authority Console.

Step 3. 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 7.)

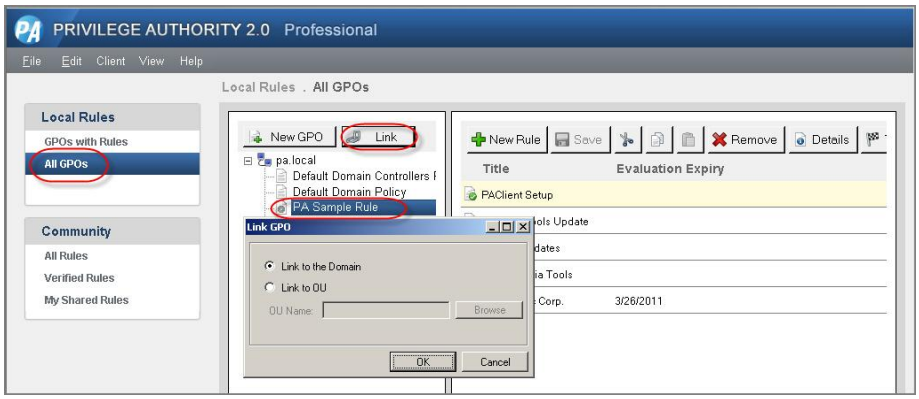

Figure 7. Add the GPO to the domain.

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 4. Configure the rule within a GPO.

Within the **All GPOs** node, select the GPO from the list under the desired domain that your local computer is a part of. Click the  **New Rule** button and a wizard will be displayed (see Figure 8). 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. (See Figure 9.)

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**.

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

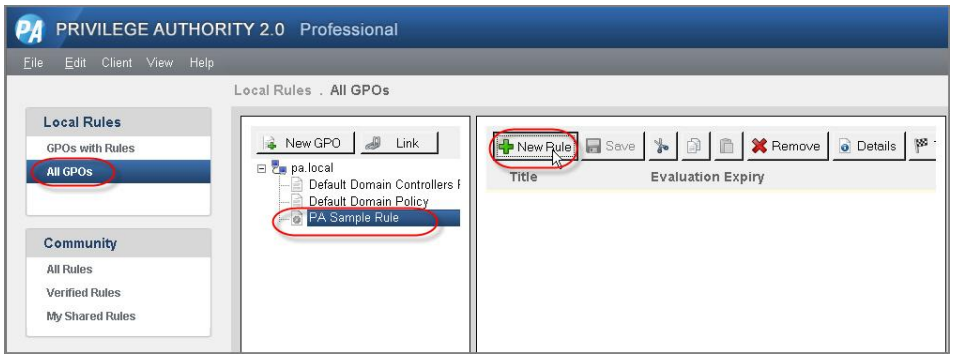

Figure 8. Selecting to add a rule to existing GPO.

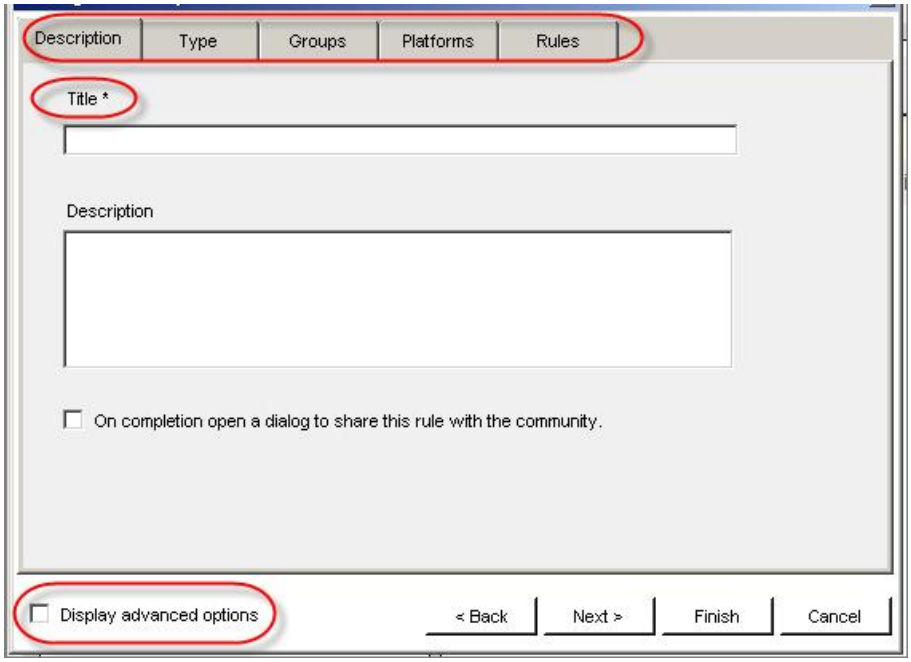

Figure 9. The Privilege Authority wizard's main window.

1. Within the dialog, enter a name for the rule so you can identify it.

   You may also choose to share your rule with the community by marking it in the corresponding box (see Figure 10). You can share the rule at any time later, when you have tested the rule.

   If you choose to share the rule, you will be presented with the Privilege Authority Community Forum registration dialog shown on Figure 11. The dialog is referenced in the *Registering with the Community Rules Exchange Server* section.

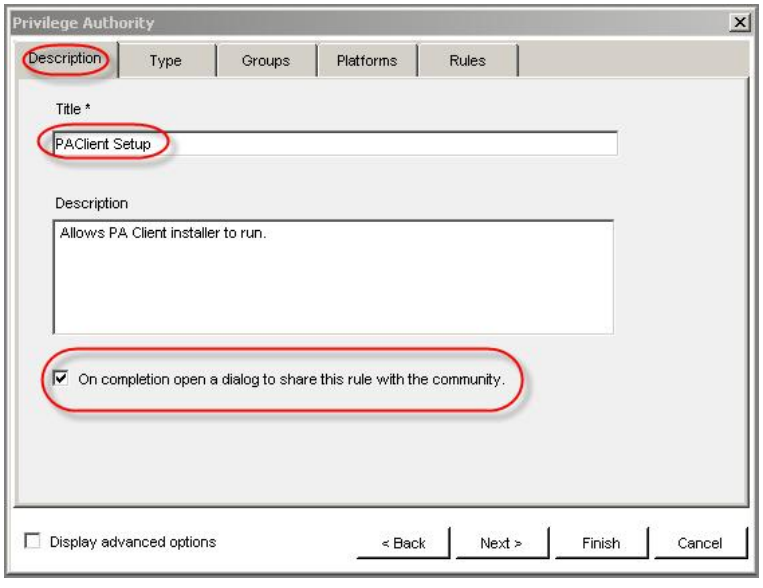

Figure 10. Specify a title and optionally share the rule with the community.

Figure 11. Registering to upload to the Community Exchange server.

2. You are given a choice of several rule types (the number of types varies depending on the Privilege Authority edition). Let's select the first option, **By Path to the executable,** and specify the path to the executable. You can either enter a full or partial path in the form of `*\filename.exe`.

   For this example enter ***\ITunesSetup.exe**.

Note

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

You may optionally fill in the other fields provided. Switch to the next tab (or click the **Next** button at the bottom of the dialog) and enter the necessary data. (See Figure 12.)

The rule types and their settings configuration are detailed in the Privilege Authority Administrator's Guide.

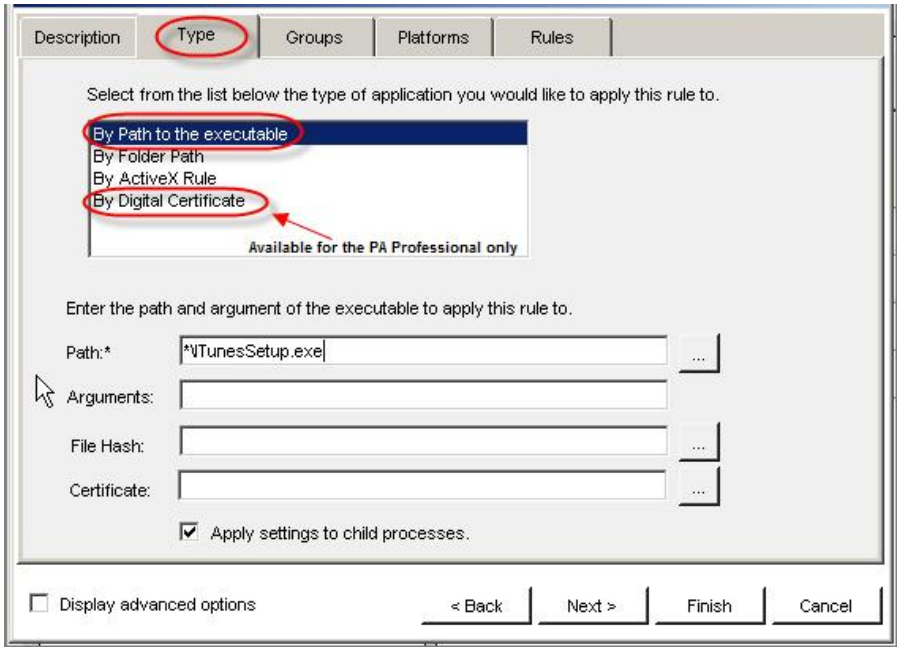

Figure 12. Specify the GPO rule type and fill in the required field.

3. (*Optional*) The next screen is where you select a Group whose rights are to be applied to the process. A Group can be added or removed from a process by using use the button. In this case select the button which will add the Administrators Group to the list (this is the group stored within the BUILTIN\Administrators Active Directory OU). (See Figure 13.)

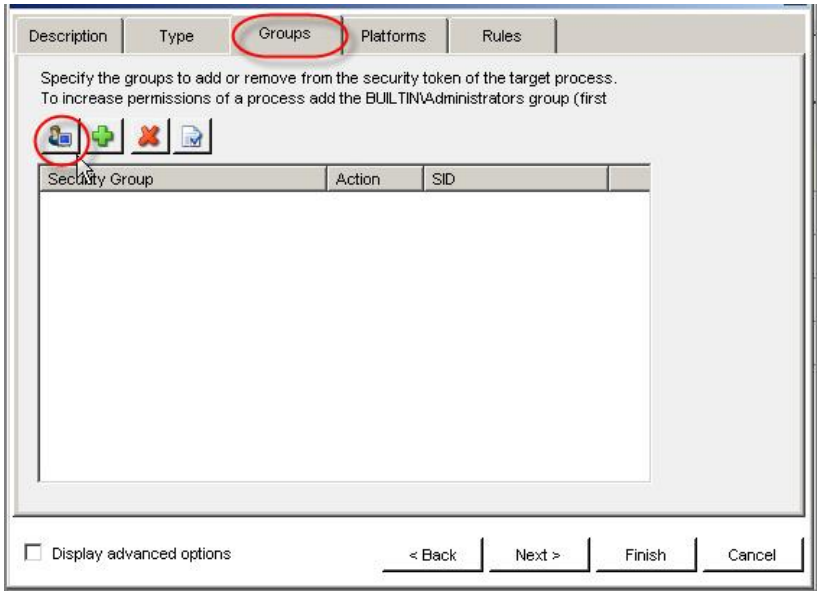

Figure 13. Add the Administrators group to the security token of the process.

4. (*Available only for Privilege Authority Professional*) (*Optional*) Define on which machine type, all servers and/or all workstations, and/or on which operating system(s) the process may start. (See Figure 14.)

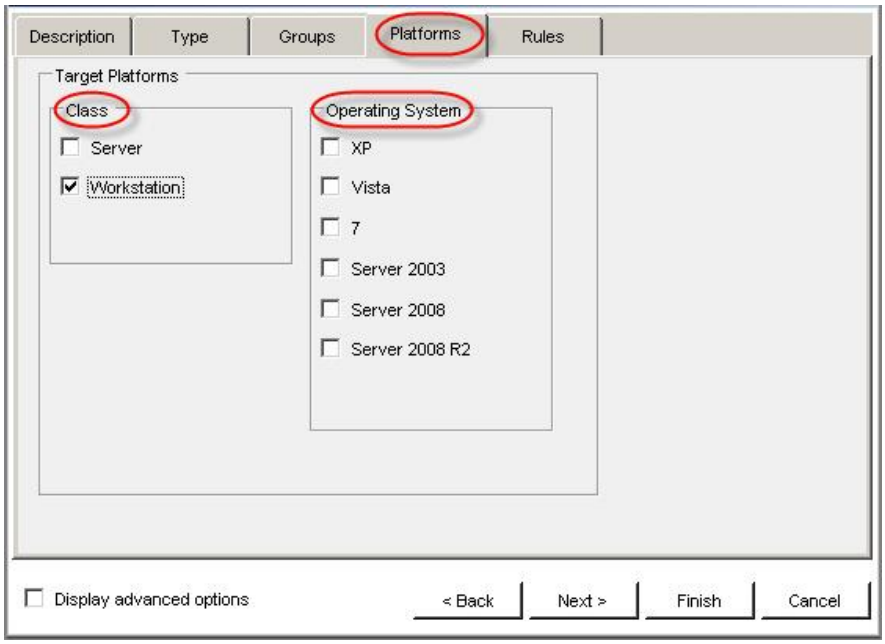

Figure 14. Specify the platforms to apply the new rule on.

5. (*Available only for Privilege Authority Professional*) (*Optional*) The **Rules** tab allows you to specify additional validation logic to apply to the process. It may include whether it should/should not run on computers with certain prefix in the name, or pertaining to some special group or IP address range, etc. (See Figure 15.)

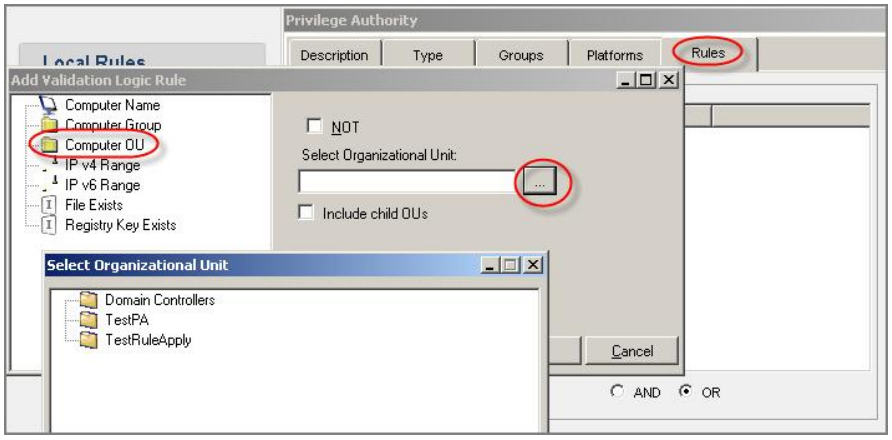

Figure 15. Specify additional parameters to the rule.

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

   (*If applicable*) If you have previously chosen to share the rule with the community confirm or edit in the dialog that will open.

Figure 16. Setting the details to share the rule.

Step 5. Save the rule.

Upon completing the wizard, click the **Save** button on the menu bar of the **Rule** section. If asked, confirm the saving of the rule. (See Figure 17.)

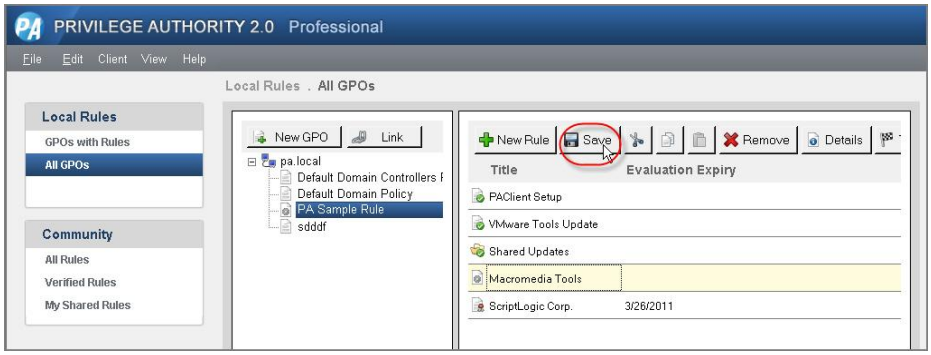

Figure 17. Save the rule.

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 18.)

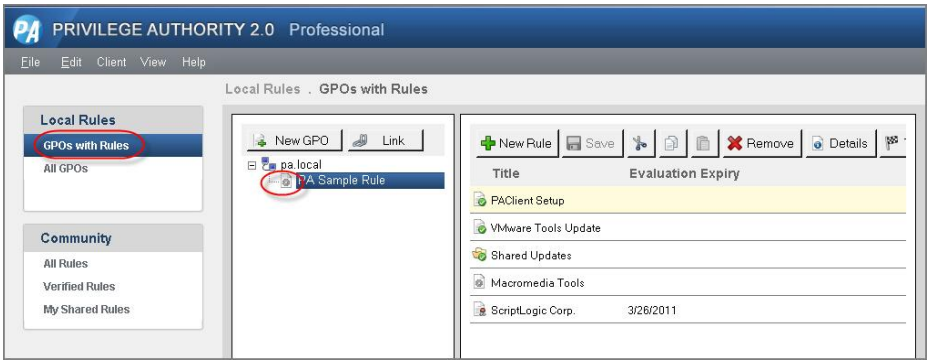

Figure 18. The marked-in icon indicates that GPO is assigned with a rule.

The `ItunesSetup.exe` file installation should be allowed once the Group Policy is updated on the client. (See Figure 19.)

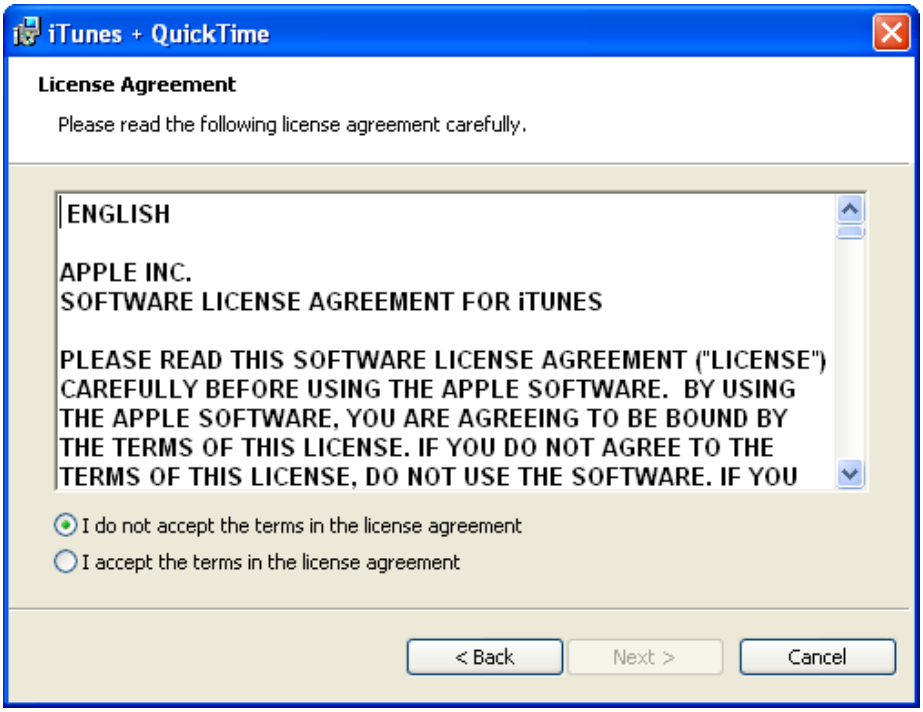

Figure 19. The installation has been allowed via Privilege Authority.

- To delete/modify/test (the latter requires Privilege Authority Client installed on the PA Server host) or share the selected rule with the community, use the corresponding toolbar buttons (see Figure 20).

  The rule testing functionality is detailed in *Privilege Authority Administrator's Guide*.

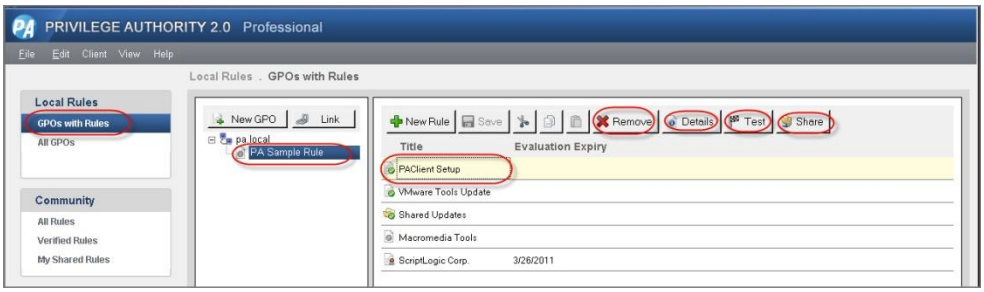

Figure 20. Use the toolbar to manage a GPO rule.

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

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 just 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.

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

- Once you open the Privilege Authority Console and click **All Rules** located under the **Community** node, the list of rules will show (provided that you are connected to the Internet). (See Figure 21.)

Figure 21. The Community Rules list.

Use the Community Rules to:

- apply the Community Rules in your domain
- share your rules with the community (see *the Privilege Authority 2.0 Administrator's Guide*)
- edit, comment and rate the Community rules (see the *Privilege Authority 2.0 Administrator's Guide*).

Applying Community Rules to your Domain

To make use of a certain rule within the **Rules Exchange All Rules** list or just to see how 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 22.)

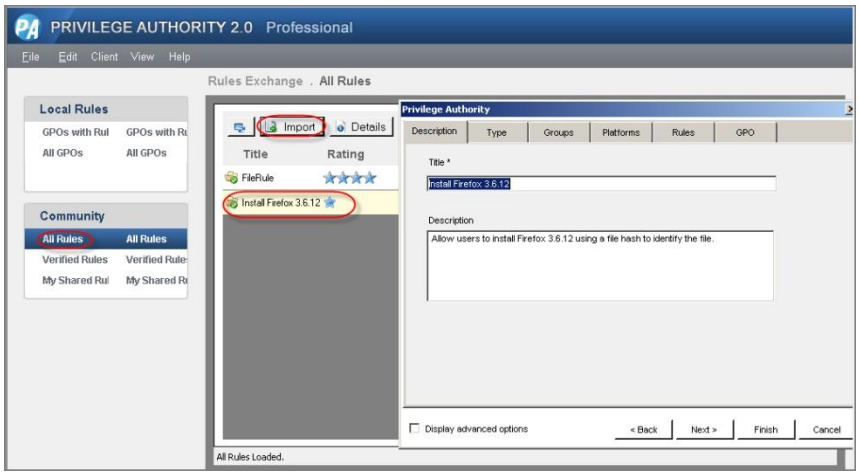

Figure 22. Opening the community rule dialog.

Note

If the list of rules does not populate automatically, try the following: click Help -> Proxy Settings, and specify the proxy server data in the window that will open. (See Figure 23.)

Figure 23. Specifying the proxy server settings.

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 a certain 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 24.)

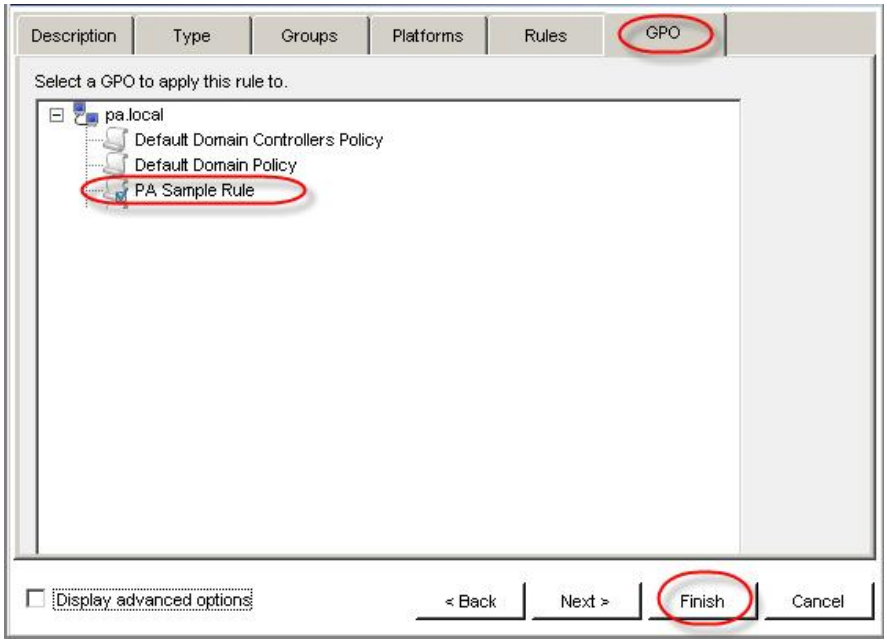

Figure 24. Selecting a GPO to apply the rule to.

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

The rule will now display in the list of rules of the corresponding GPO under the **Local Rules** node. (See Figure 25.)

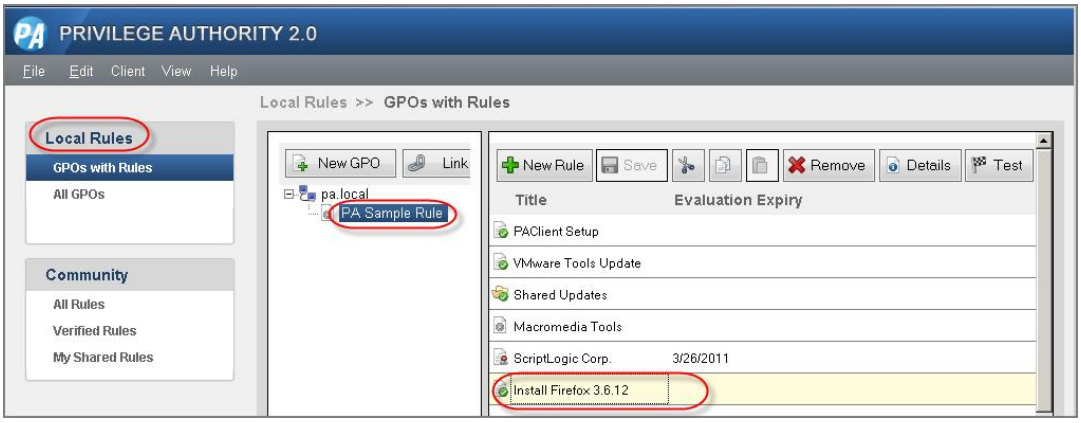

Figure 25. A community rule has been set to apply to a GPO in your domain.

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

Refer to Privilege Authority Administrator's Guide for other operations with the Community rules.

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 26):

- If you are already registered with 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 the following 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 26. 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 log in at the server as a different user:

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