

Privilege Authority[®]

© 2012 ScriptLogic Corporation
ALL RIGHTS RESERVED.

ScriptLogic, the ScriptLogic logo and Point,Click,Done! are trademarks and registered trademarks of ScriptLogic Corporation in the United States of America and other countries. All other trademarks and registered trademarks are property of their respective owners.

Privilege Authority

Organizations that give their end users local administrator rights on their computers face severe internal and external security risks. Users with unlimited power to change settings and install and run software on their computers are highly vulnerable to attack by virus and malware. In addition they can disable security settings on their machines and prevent protective processes from running giving them access to critical information for potential misuse and security breaches. (For example, users with administrator rights can read wireless network access key on Windows 7 computers, meaning they can add other devices to the network without administrator permission).

Privilege Authority allows administrators to enforce a secure Least Privilege environment to counter these threats and reduce help desk support costs without adversely impacting user productivity. Once the IT administrator has locked down the environment by taking away the local admin rights of end users, he or she can use Privilege Authority to granularly delegate administrator privileges to users for selective tasks like installing and updating approved applications and ActiveX controls, accessing selected Windows features and running business applications so end users can meet their functional responsibilities.

New Feature Highlights for Version 2.7

Summary

Privilege Authority 2.7 addresses real life management challenges faced by administrators. It allows Domain Administrators to delegate privilege management responsibilities to Organizational Unit (OU) administrators so they can deploy privilege policies easily and with minimal disruption to their Group Policy infrastructure. The following new features are available in version 2.7:

- Deploy Privilege Policies without Domain Administrator Rights
- Support for User- and now Computer-Type Privilege Policies
- Enhanced Privilege Authority Console for Easier Policy Deployment
- Assisted Creation of Policies Based on Running Processes
- Support for Installing ActiveX Controls in the Latest Internet Explorer Version 9

Deploy Privilege Policies without requiring Domain Administrator Rights

Privilege Authority no longer requires an administrator to have domain privileges or access to central domain resources like SYSVOL to deploy privilege policies. It restricts policy deployment to only those GPOs where the administrator has Read/Write permissions, so that Domain Administrator can now delegate privilege management responsibilities to OU administrators for their respective OUs by just granting them permissions on selected GPOs. This allows OU administrators to fully use Privilege Authority for their respective OUs without requiring any additional privileges for the rest of the domain.

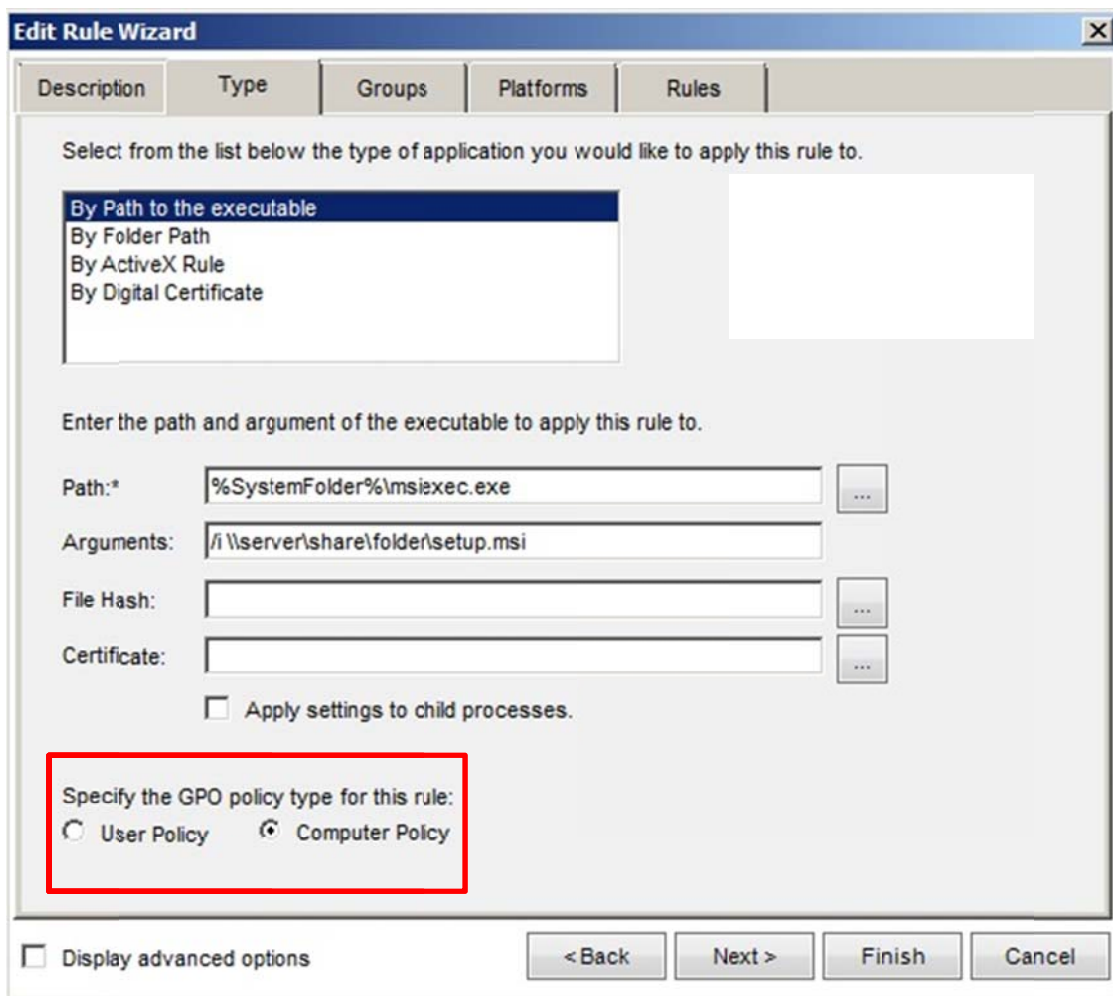
The Privilege Authority Reporting capability can be deployed either by a Domain Administrator to use for the entire domain, or by OU administrators for their respective OUs.

Support for Machine Type Privilege Policies

Until version 2.7 Privilege Authority only supported “user” type privilege policies, so that when they are deployed such policies are enforced for the targeted users on all computers. With version 2.7, Privilege Authority includes support for “computer” type privilege policies. When a computer type policy is deployed it will be enforced for all users on the targeted computer. This will allow administrators to deploy privilege policies using existing GPOs irrespective of whether they are assigned by computer or by user in the domain.

This option is available within Rules Wizard when creating a privilege policy. The following image indicates the precise location of the option. The User Policy is the default option and needs to be changed to Computer Policy for this feature to take effect.

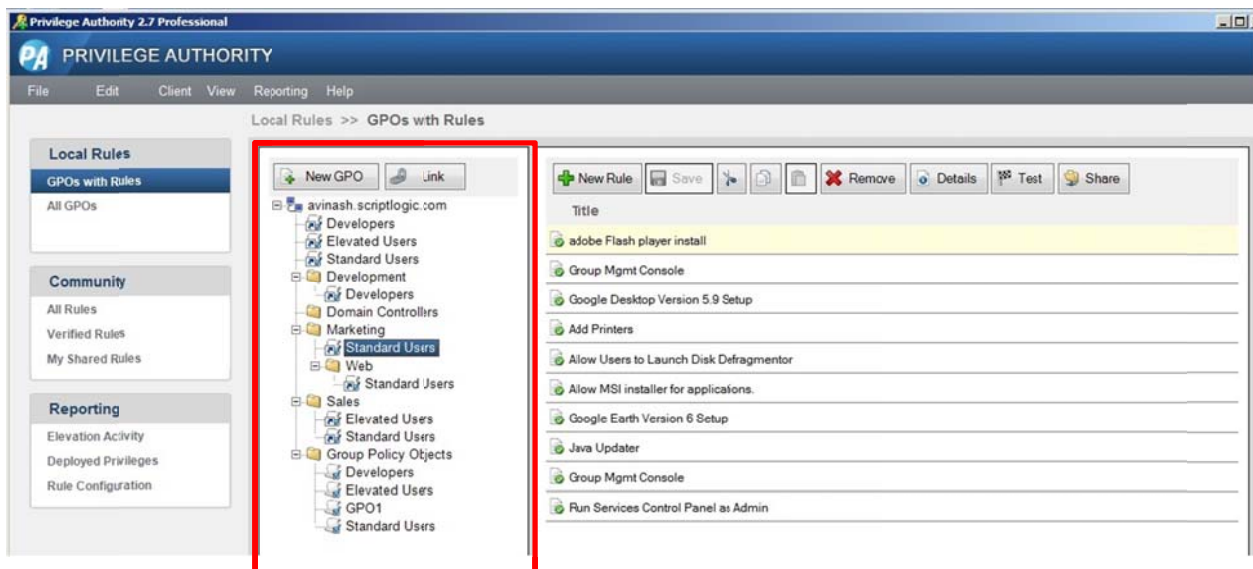
NOTE: This is a premium feature and will be available only in Professional Edition.

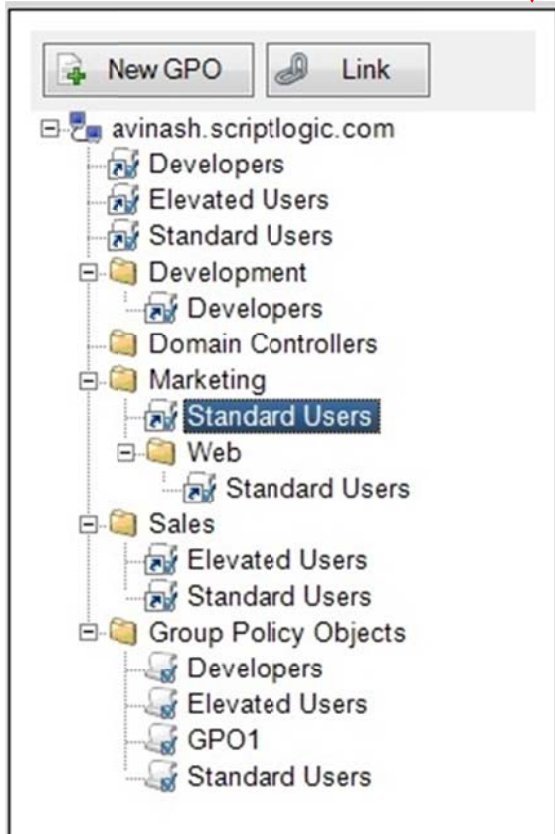


The screenshot shows the 'Edit Rule Wizard' dialog box with the 'Rules' tab selected. The 'Type' section is highlighted with a red box, showing two radio buttons: 'User Policy' and 'Computer Policy'. The 'Computer Policy' option is selected. The 'Path' field contains '%SystemFolder%\msiexec.exe' and the 'Arguments' field contains '/i \\server\share\folder\setup.msi'. The 'Apply settings to child processes' checkbox is unchecked. The 'Display advanced options' checkbox is also unchecked. The 'Back', 'Next', 'Finish', and 'Cancel' buttons are visible at the bottom.

Enhanced Console for Easier Policy Deployment

Finding the right GPO for deploying privilege policies can be very challenging when Active Directory contains a large number of OUs and GPOs. Version 2.7 offers an enhanced Privilege Authority console to make that task easier. The simple listing of GPOs in the Console has now been replaced with the Domain hierarchy showing all the OUs and the GPOs listed in a tree structure. An administrator can now quickly identify the right GPO to be used for deploying a privilege policy by expanding the tree structure to determine the associated OUs, removing the need to switch between the Privilege Authority console and the Group Policy Management Console (GPMC). Note that the Privilege Authority console will display only those GPOs in the tree where the administrator has Read/Write permissions. The administrator can create new GPOs and link them to appropriate OUs if required permissions are in place in Active Directory.

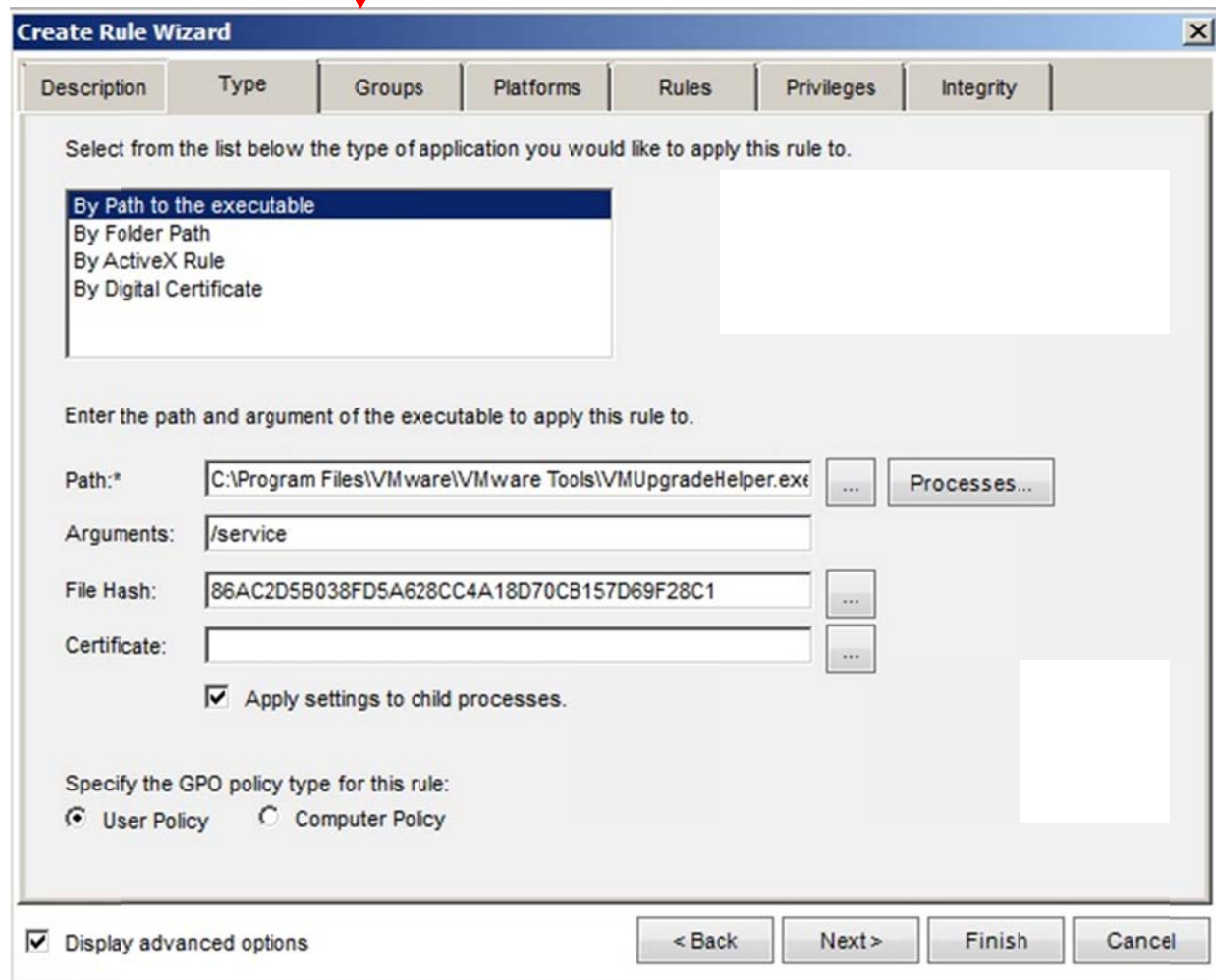
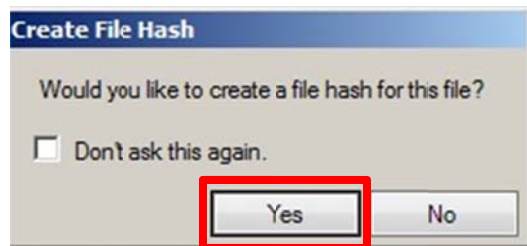




Assisted Creation of Policies Based on Running Processes

Most organizations have a mix of different types of application, some of which are built in-house or customized for their industry. It is hard to find pre-built privilege policies for such applications requiring IT administrators to spend time and energy building custom policies. Privilege Authority offers a new feature in version 2.7 that allows administrators to create process-specific policies quickly and easily. Policy creation activity starts with administrators starting the application on their computer with administrator rights. They can then use the newly added “Processes...” button in the “Type” tab in Privilege Authority’s Rules Wizard to select the process that was spawned by the application. Once the process is selected, the Rules Wizard will capture all the relevant information of that process required by the Wizard’s fields in the tabs “Type”, “Privileges” and “Integrity”. The Rules Wizard also captures the file hash and the digital certificate of the process if available. All that the administrator is required to do to complete the policy definition is to specify the policy’s target criteria and its required privilege level, which are values for the fields in the Rules Wizard tabs “Platforms” “Groups” and “Rules”. Once the rule is created, it can be deployed through the appropriate Group Policy Object (GPO). The images provided below highlight the options to be used to create such a policy.

NOTE: This is a premium feature and will be available only in Professional Edition.



Support for Internet Explorer 9

Privilege Authority 2.7 now supports privilege elevation of ActiveX Control installations in the latest Internet Explorer version 9.