Top 5 security settings in Group Policy of Windows Server 2008

With over 5000 settings in the new Group Policy of Windows Server 2008, you may be overwhelmed by choosing which settings are most important to yourself and your network. Implementing the security settings for the desktop to comprehensively enhance security is by reducing the available attack surface. How to reduce the attack surface on

Derek Melber

How to reduce the attack surface on desltop computers by using 5 security settings in Group Policy.

With over 5000 settings in the new Group Policy of Windows Server 2008, you may be overwhelmed by choosing which settings are most important to yourself and your network. Implementing the security settings for the desktop to comprehensively enhance security is by reducing the available attack surface. In security settings, there are some that only support Windows Vista, while others may be compatible with Windows XP SP2.

Control the internal Administrator group membership

One of the most insecure settings you can give users is internal administrative access. By adding a user account to the internal Administrators group, users will be granted almost ultimate control on their desktop. They can perform most actions, even if the network is configured to deny this access. Actions that the user can perform, thanks to internal administration rights, include:

1. Remove their computer from the domain
2. Change the Registry settings
3. Change permissions on folders and files
4. Change system settings, such as settings in files located in the system directory.
5. Install apps
6. Remove installed applications, security patches and service packs.
7. Access to the website allowed by the firewall
8. Download and install ActiveX controls, Web applications or other malicious applications downloaded from the Internet.

Although requiring users to have administrator rights to allow certain applications to work, this type of access is often very dangerous and easy to place the desktop and the entire network on security attacks.

With Windows Server 2008 Group Policy, users can now be removed from the internal Administrators group by using only a simple policy. This setting controls Windows XP SP2 and higher operating systems. They are Group Policy's new Preferences settings. To access this setting, you need to open the Group Policy Object and

go to:

User ConfigurationPreferencesControl Panel

Then right-click **Local Users and Groups** . From the menu, click **New - Local Group** . Then the following dialog box will appear, see Figure 1.

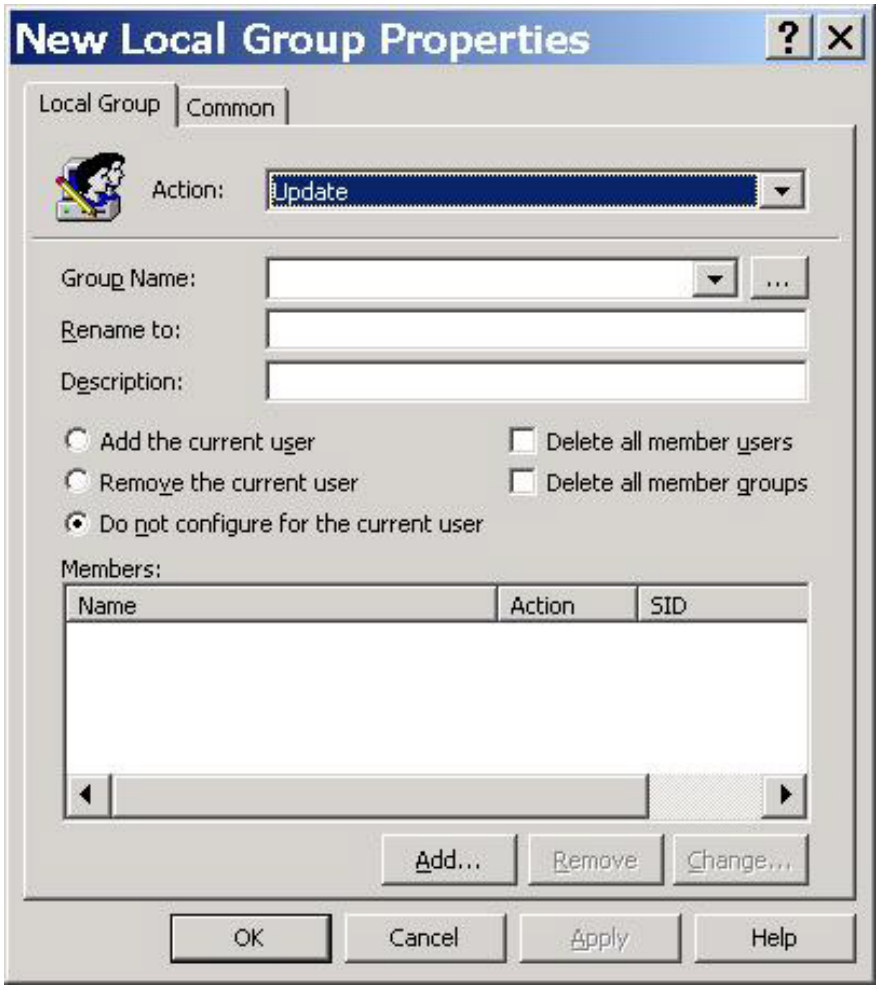

Figure 1: Group Policy Preference for Local Group

To configure the policy, type Administrators in the Group text box, then check the ' **Remove the current User** ' checkbox. While the Group Policy next background refreshes all user accounts that are within the scope of management of the GPO, where this setting is configured, the accounts will be removed from the Administrators group on the computer they log on .

Reset internal Administrator password

In conjunction with the first Group Policy setting, the internal Administrator password also needs to be reset. This is because the user has administrator privileges before removing them from the local admin group.

After the user account has been removed from the local admin group, this group account password needs to be reset. If this setting can be done simultaneously with removing user accounts, they will not be able to know or change the new internal Administrator password.

This setting controls Windows XP SP2 and newer operating systems. It is setting up a new Group Policy Preferences. To access this setting, open the Group Policy Object and go to:

Computer ConfigurationPreferencesControl Panel

Then right-click **Local Users and Groups** . From the menu, click **New - Local User** . The following dialog box will appear.

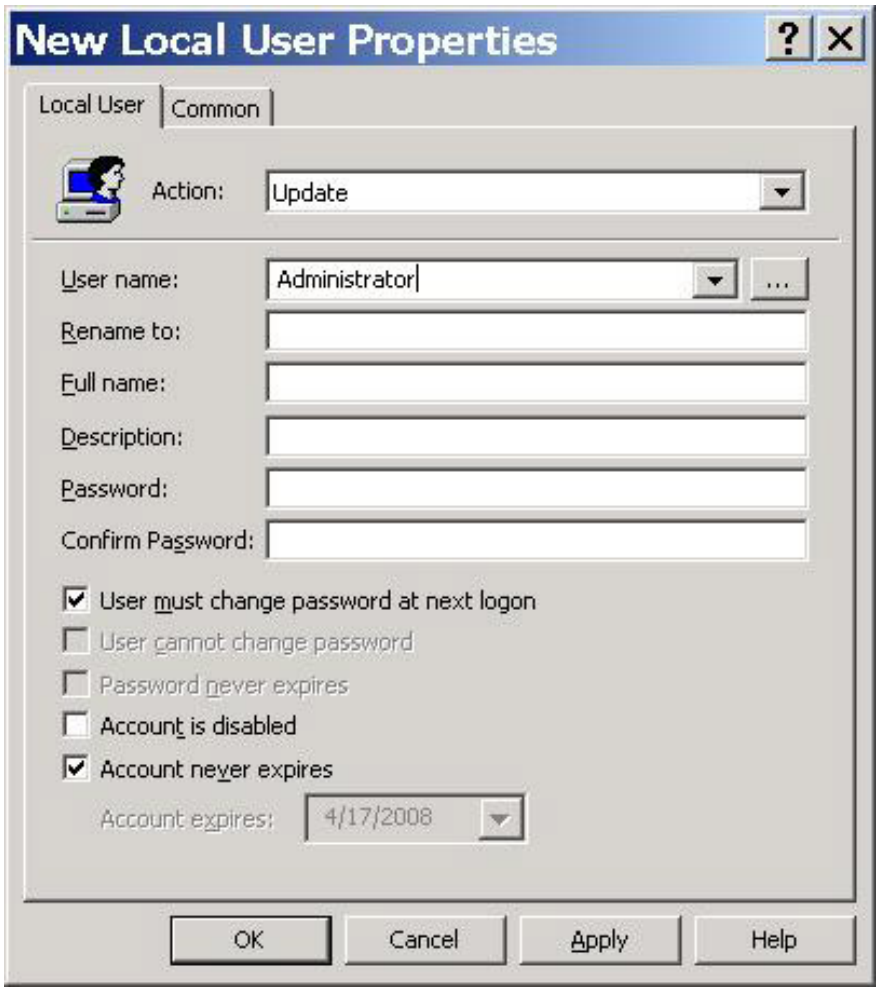

Figure 2: Group Policy Preference for Local User

To configure the policy, type Administrator in the User name text box, then type a new password in the Password text box, confirm the password in the Confirm Password box. While the new Group Policy background refreshes all computer accounts within the scope of management of the GPO, the internal Administrator password will be reset.

Windows Firewall with advanced security

Previously, users and administrators were dreaming about Windows Firewall, due to the limited capabilities of their products. Now, Windows Firewall has a number of advanced security settings that allow them to have a better understanding of the firewall.

Windows Firewall's new advanced security features not only incorporate inbound and outbound filtering, but also IPSec.

These settings can only be controlled with Windows Vista and within the security area of ??Group Policy. To access this setting, open the Group Policy Object and go to:

When you open the policy, you will see the following three buttons:

1. Inbound rules
2. Outbound rules
3. Connection Security Rules

If you right-click these options, you can select the New Rule option, see the inbound rule shown in Figure 3.

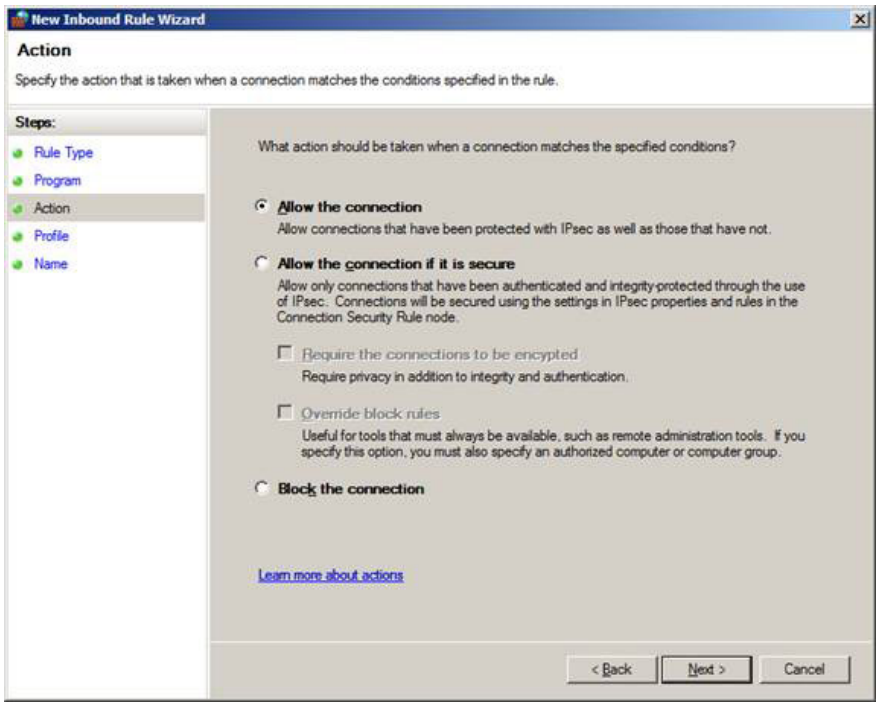

Figure 3: One of the screens in the Inbound rule wizard.

UAC

User Account Control (UAC) gives you an option to help protect the computer where users and administrators log on. UAC is currently a great idea for all administrators and can be a good solution for standard users. Since UAC requires all users to be standard users for all tasks, it helps protect against any application or virus that

wants to write to protected areas on the computer by prompting The user uses a dialog box whenever the protected area of ??the computer is accessed. It is possible to access an application, install an application, change the registry, write to the file system, .

This is great for all administrators, because they can use a certain user account for daily tasks, both for IT and for personal use. For standard users, only the UAC will work well in case all applications running on the workstation can run without requiring administrator credentials. In this situation, users can perform all operations and run all applications as a standard user. Then if a task needs to be done with higher access (administrator level) then they may need help from the support team or system administrator.

UAC control settings can be found at **Computer ConfigurationPoliciesWindows SettingsSecurity SettingsLocal PoliciesSecurity Options** , see Figure 4 below.

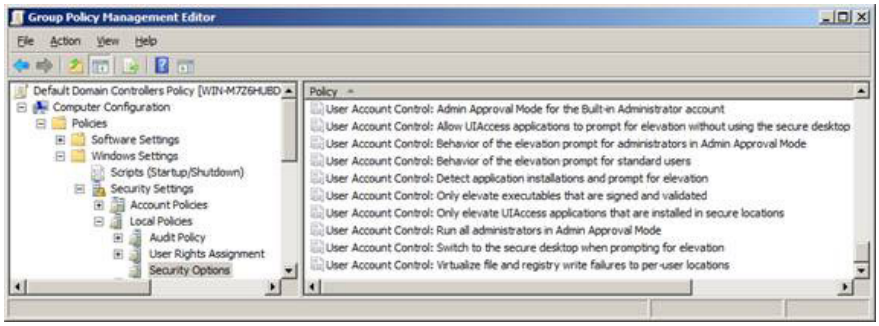

Figure 4: Group Policy options to control UAC

Password policy

Although passwords are not really as attractive as a security setting, the ability to control passwords using Group Policy should not be ignored in this top 5 list. Windows Server 2008 still uses Group Policy to determine the initial account policy settings, which haven't changed since Windows 2000. The settings are initially configured in the Default Domain Policy, but they can be created in any Which GPO period is associated with the domain. One thing you should keep in mind is that the GPO includes account policy settings that must have the highest priority compared to all GPOs associated with the domain.

The settings that you can configure are shown in Figure 5 and the settings shown in Table 1.

Figure 5: Password policy settings in Default Domain Policy
Here are some guidelines for these policy settings:

Policy setting Minimum value Safety value Minimum password life11 Maximum password life18045 Password minimum length814 + Complexity of passwordEnabled Enabled

Table 1

Conclude

The Windows Server 2008 Group Policy options are really impressive. With over 5000 settings, you will be completely comfortable in controlling computers in your environment. 5000+ settings to ensure security for all environments and users are essential. If you take advantage of the settings introduced in this article, you will make sure your desktop environment becomes much more secure.