Deploying security templates

Once you have the perfect security template -- either a default security template or a custom one that you designed -- you can apply it to the computer or computers it was designed for. Keep in mind that the overall design of the OUs, including the placement of computer accounts, plays a key role in how and where you can deploy these security templates.

You have four options at your disposal for deploying security templates. Only one option is related to GPOs, and it is the most popular option. The other options are valid but are not related to GPOs.

- Importing security templates into GPOs
- Using the Security Configuration and Analysis tool
- Using the Secedit.exe command-line tool
- Using the Security Configuration Wizard and the *scwcmd* command

A best practice for deploying security templates is to import them into a GPO, which will then push out the security settings that you initially configured in the security template. This method relies on the Active Directory and OU design accommodating this rollout.

Before you can implement this method, you must complete the following steps. First, create OUs for the different types of computers that will receive a different security template. Second, move the computer accounts for these computers into the appropriate OU. Third, create and link a GPO for each of the computer OUs that you created in the first step. Now, you are ready to include the security templates into the GPOs.

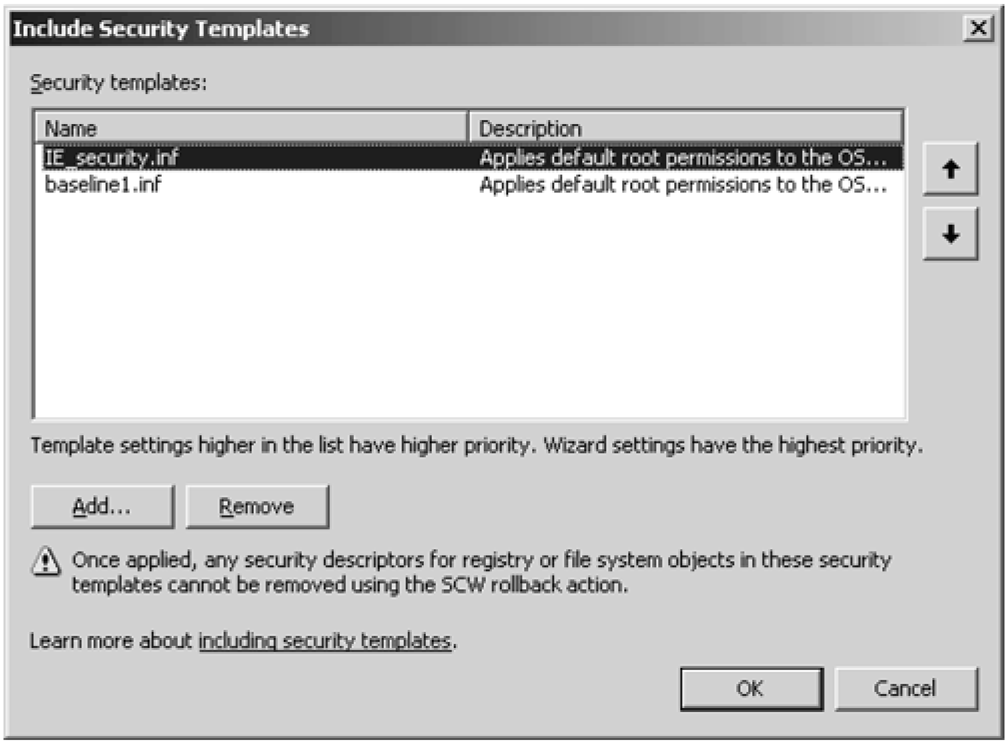
To import a security template into a GPO, complete these steps:

1. Open the target GPO using the Group Policy Object Editor.
2. Expand the GPO to the following node: Computer Configuration\Windows Settings\Security Settings.
3. Right-click Security Settings and select the Import Policy from the shortcut menu.
4. Browse and select the security template (.inf file) that you want to include and click Open.
5. Verify that some of the configurations from the security template are correct in the GPO, and then close the Group Policy Object Editor.
6. Repeat these steps for each security template that you create. The settings that have been imported into the GPO will take approximately 90 minutes to reach the target computer, not considering any intersite replication considerations.

The Security Configuration and Analysis tool performs two tasks: configuring and analyzing security. The tool works with security templates only to perform these duties. Therefore, once you have a security template, you can use this tool to deploy the settings. The drawback of the tool is that it is not capable of configuring multiple computers at once -- it can configure only the computer on which it is running. You must therefore visit each computer that should receive the security template settings. Of course, this is not feasible in most environments, even those with only a few dozen computers. Therefore, this method is best suited to hardening standalone servers that are not part of an Active Directory domain.

The Secedit.exe tool can perform the same functions as the Security Configuration and Analysis tool. Because the Secedit.exe tool can be scripted, it can be used in a logon or startup script. This allows for multiple computers to be configured with a single script. The Secedit.exe tool was also used in Windows 2000 to refresh GPOs. However, Windows Server 2003 and Windows XP don't use Secedit.exe to refresh GPOs, so the tool is now used almost solely for deploying security templates.

A new option for deploying security templates is to use the Security Configuration Wizard together with the *scwcmd* command. The wizard produces security policies, which can include security templates as discussed earlier. The wizard can accept a single security template or multiple templates. When you include the security templates, you can prioritize them to ensure that the correct settings take precedence because the settings within each security template update the security policy. This wizard page can be seen in Figure 5-6.



Include Security Templates

Security templates:

Name	Description
IE_security.inf	Applies default root permissions to the OS...
baseline1.inf	Applies default root permissions to the OS...

Template settings higher in the list have higher priority. Wizard settings have the highest priority.

Once applied, any security descriptors for registry or file system objects in these security templates cannot be removed using the SCW rollback action.

Learn more about including security templates.

Figure 5-6: Prioritizing security templates that are imported into the Security Configuration Wizard

NOTE To configure multiple servers with a security policy, you can use the Security Configuration Wizard command-line suite of tools. The *scwcmd configure* command allows you to specify the security policy and create a list of servers that the policy will affect. For more information on this option, type **scwcmd configure** at the command prompt.

After you create your security policy using the Security Configuration Wizard, you need to deploy them efficiently to the appropriate servers on the network. By using Group Policy to deploy security policies created using the Security Configuration Wizard you can optimize the deployment of the security settings. Use the *scwcmd transform* command to create a Group Policy object that includes the settings that you configured within the security policy. Use the following syntax to convert a security policy to a GPO:

Scwcmd transform /p:*PathAndPolicyFileName* /g:*GPODisplayName*

In this example, *PathAndPolicyFileName* is the security policy that you created earlier using the Security Configuration Wizard. This must include the .xml filename extension. *GPODisplayName* is the name that the GPO will show when you view it in the Group Policy Object Editor or in the Group Policy Management Console (GPMC).

IMPORTANT The GPO that you create based on the security policy is immediately available in Active Directory. However, the GPO will not apply to any server until it is linked to a site, the domain, or an OU containing server accounts.