Security usage is available in Windows Server 2003

This is one of the easy-to-understand step-by-step tutorials of the Microsoft help provided to users. This article describes how to apply pre-defined security templates in Windows Server 2003. Microsoft Windows Server 20

This is one of the easy-to-understand step-by-step tutorials of the Microsoft help provided to users. This article describes how to apply pre-defined security templates in Windows Server 2003. Microsoft Windows Server 2003 provides a number of security templates that help you increase the security of your network. You can edit them to suit your specific requirements by using the Security Templates component in Microsoft Management Console (MMC).

Security templates are pre-defined in Windows Server 2003

1. **Default *security* (*Setup security.inf*)**

   Setup security.inf is created during the installation process and is separate for each computer. Each computer has a different type of *Setup security.inf* depending on whether the installation program is completely new from the beginning or an upgrade. It shows the default security settings applied by the operating system during the installation process, including file permissions for the root of the system drive. This security template can be used for both servers and clients but cannot be applied to domain controllers. You can also use parts of this model for recovery if a risk situation appears.

   Do not apply the *Setup security.inf* using Group Policy because this can reduce the speed of system execution.

   Note : In Microsoft Windows 2000, two mixed security templates exist: ocfiless (for file servers) and ocfilesw (for workstations). In Windows Server 2003, both files are replaced by the *Setup* file *security.inf* .
2. **Default security for domain controllers (*DC security.inf*)**

   This template is created when the server is upgraded to a domain controller. It maps file, register, and system service default security settings. If you reapply this model, the settings will be set to the default value. However, this type of template can override privilege on new files, registry keys and system services created by other programs.
3. **Compatible (*Compatws.inf*)**

   This template changes file and register permissions that are allocated to members of the Users group, consistent with the requirements of most programs that are not included in the Windows Logo Program for Software. The *Compatible* model also removes all members of the Power Users group.

   For more information on the Windows Logo Program for Software, you can refer to the Microsoft website:

http://www.microsoft.com/winlogo/default.mspx

Note : Compatible models cannot be applied to domain controllers.

4. **Security (*Secure * .inf*)**

   Secure templates define advanced security settings that at least affect program compatibility. Examples include password definition, lockout mode and stronger auditing settings. In addition, these templates limit the use of LAN Manager and NTLM authentication protocols by configuring the client to only send NTLMv2 replies and configure the server to refuse to answer the LAN. Manager.

   There are two built-in security models in Windows Server 2003: *Securews.inf* for workstations and *Securedc.inf* domain controllers. For more information on how to use these models and some other security templates, you can search the Microsoft **Help and Support Center for** help with the " *predefined security templates* " keyword (the *security templates)* . available meaning).

5. **High security (*hisec * .inf*)**

   Highly Secure describes in detail the additional limitations not yet defined in *Secure* , such as the level of encryption and symbols needed for authentication and data exchange through secure channels, between the client and server Server Message Block (SMB).

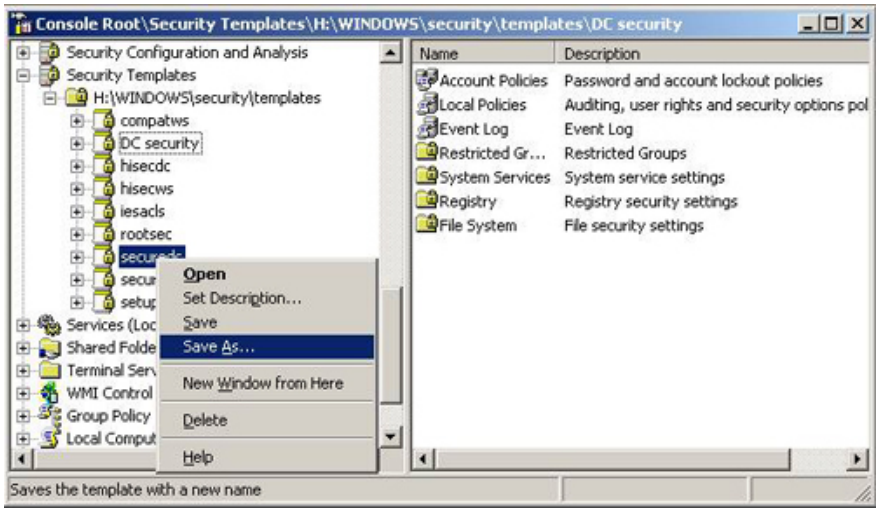
6. **Secure system root directory (*Rootsec.inf*)**

   This template specifies the permissions of the root directory. By default, *Rootsec.inf* defines the permissions for the root file of the system drive. You can use this model to re-apply root directory privileges if they are randomly changed. Or you can edit this sample model to apply the same root permissions to many other departments. This pattern does not override explicit permissions defined in child objects; it only copies the inherited rights in those child objects.

7. **The template does not have a SID for Terminal Server users (*Notssid.inf*)**

   You can apply this template to remove the Windows Terminal Server security identifier (SID) from the file system and registry locations when the Terminal Services (Terminal Services) does not run. After you do this, system security will not be fully improved.

For more detailed information about all the pre-defined model models in Windows Server 2003, you can search in Microsoft's **Help and Support Center** help with the " *predefined security templates* " keyword.



Important : Execute a security model model on the domain controller can change the Default Domain Controller Policy or Default Domain Policy settings. The sample model used can override permissions on new files, registry keys and system services created by other programs. After using the security model, you may have to restore the old "policy". Before performing some of the following steps on the domain controller, create a backup of the SYSVOL share file.

Use a security template

1. **Go** to **Start** , select **Run** , type ***mmc*** on the command box and click **OK** .
2. On the **File** menu, click on the **Snap-in Add / Remove button** .
3. Select **Add** .
4. In the **Available Stand Alone Snap-ins list** , select **Security Configuration and Analysis** , click **Add** > **Close** and finally **OK** .
5. In the left pane, click on **Security Configuration and Analysis** and see the instructions in the right pane.
6. Right-click on **Security Configuration and Analysis** , select **Open Database** .
7. In the **File** name box, type the name of the confused data file and click **Open** .
8. Click on the security template you want to use, then click **Open** to enter the information in the form into the database.
9. Right-click on **Security Configuration and Analysis** in the left pane and select **Configure Computer Now** .

You finished reading the article "**Security usage is available in Windows Server 2003**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.