

Group Policy Security Templates

For the free video please see
<http://itfreetraining.com70-640/security-templates>

This video will look at the Security Settings that can be configured in Windows using Group Policy. The video also looks at how these settings can be imported and exported using Security Templates.

History Of Security Templates



- Security Templates
 - Improve compatibility
 - Increase security



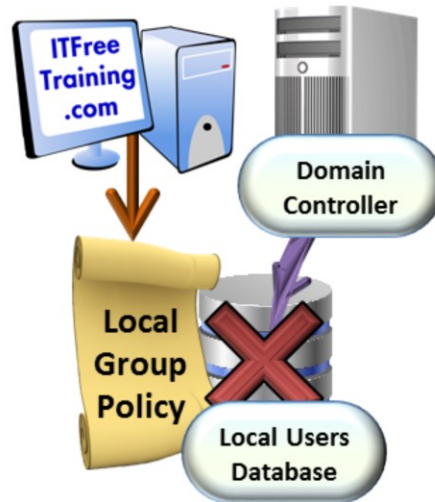
- No security templates available for download

History of Security Templates

With the release of Windows XP, Microsoft tightened up the security in the operating system. These security changes prevented software from writing to areas of the system. These changes made the system more secure and also helped make the operating system support multi users. The changes also prevented some software from running. Microsoft released some security templates to change the default security. One particular security template when applied changed the security of Windows XP to make it run more like Windows 2000. There was also another security template which tightened up the security for high risk environments. With operating systems after Windows XP, Microsoft did not release security templates for these operating systems as security is performed using other tools like Security Configuration Wizard.

Local Security Policy

- Found on every computer



Local Security Policy

Every Windows computer has local group policy settings. These settings will have the same effect as those that are applied from the domain level assuming the domain level group policy settings do not overwrite these settings. When a server is prompted to a Domain Controller, the security settings part of the local group policy for that Domain Controller is no longer used. This is why in Group Policy Management there is a Default Domain Controller Group Policy created. This Group Policy is designed to replace the settings that would have been applied using the local group policy. The Security Settings are found under Computer Configuration\Windows Settings\Security Settings. If you open Local Security Policy from the start menu, this will show only these settings from the local group policy.

Demonstration

Demonstration

If you want to import or export the security settings from a computer, you can do this by right clicking Security Settings and selecting Import Policy or Export Policy. This can be done by opening local group policy or running Local Security Policy from the start menu.

Security Configuration and Analysis can be run to compare the settings applied locally and the settings that you are importing. There is no shortcut for this tool so in order to use it you need to run MMC and then add the Security Configuration and Analysis snap-in.

Before you can use Security Configuration and Analysis to compare settings, you first need to create a database. This can be done by using the open option. The open option will open an existing database or create a new database if a database is not found. Once you have a database created, you can import an existing security template. Once imported you can see the settings currently applied on the computer and compare them with the settings in the security template. These settings can then be reviewed and changed before they are applied to the computer.

SecEdit

SecEdit /Validate filename

Checks security template

SecEdit /Import /db DBFilename /cfg TemplateFilename /OverWrite
Import Template into Database. Overwrite switch erases database first.

SecEdit /Analysis /db Filename

Compares database to computer settings. Results viewed in GUI.

SecEdit /Configure /db Filename

Applies the settings in the database to the local computer.

SecEdit

Security Configuration and Analysis can also be run from the command line using the command

SecEdit. Examples are given below.

SecEdit /Validate filename

Checks security template

SecEdit /Import /db DBFilename /cfg TemplateFilename /OverWrite

Import Template into Database. Overwrite switch erases database first.

SecEdit /Analysis /db Filename

Compares database to computer settings. Results viewed in GUI.

SecEdit /Configure /db Filename

Applies the settings in the database to the local computer.

Summary

- Every Windows computer has local group policy
- All Group Policy contains a security settings
 - Contains password settings
 - Defines user account rights
- Domain Controllers local accounts are disabled
 - Default Domain Controllers Policy configures DC's security settings
- Settings can be export/imported to an INF file

Summary

Every Windows computer has a local group policy. This defines the default settings for the computer like what rights each user has. On a Domain Controller, the local user database is disabled so in effect the security settings defined on a Domain Controller have no effect. In order to configure security settings on Domain Controllers, a Group Policy called Default Domain Controllers Policy is created.

References

"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 330-339