Understanding Windows Security Templates

Date Launched: Oct 06, 2004
Last Updated: Oct 06, 2004
Section: Articles :: Misc Network Security

Author: Derek Melber

Printable Version

Rating: 3.9 / 5 - 22 Votes

1 2 3 4 5

A security template contains hundreds of possible settings that can control a single or multiple computers. The security templates can control areas such as user rights, permissions, and password policies. Security templates can be deployed centrally using Group Policy objects (GPOs). Finally, security templates can be customized to include almost any security setting on a target computer.

Contents of a Security Template

All security templates are created equal. This means that each one contains potentially hundreds of settings that can control security on a target computer. For all of the new security templates that are created, every setting is "Not configured" by default. This means that the security template does not change the settings on the target computer. However, with just a couple of clicks, you can easily configure many security settings that can change many computers at one time.

As we analyze what a security template is, we need to understand that it is really a portion of a GPO. If you look at Figure 1, it shows a typical Local GPO security settings.

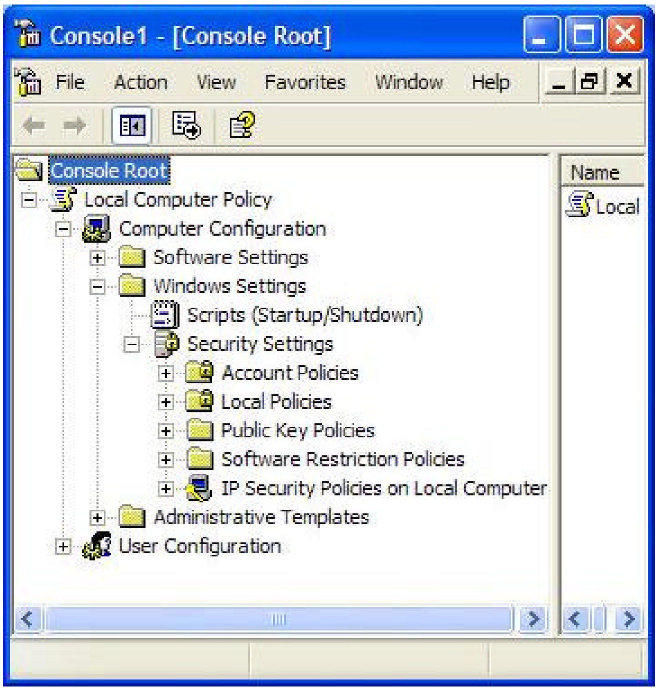
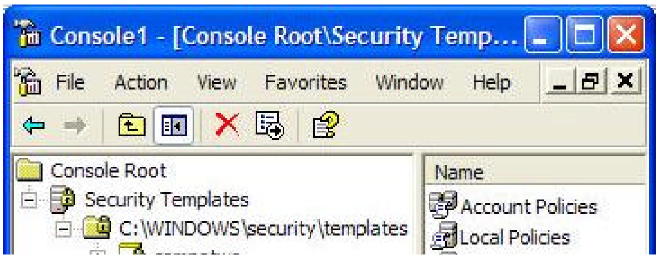


Figure 1. Typical Local GPO showing the security settings for a computer.

Now, look at Figure 2, which is a full list of the security template.



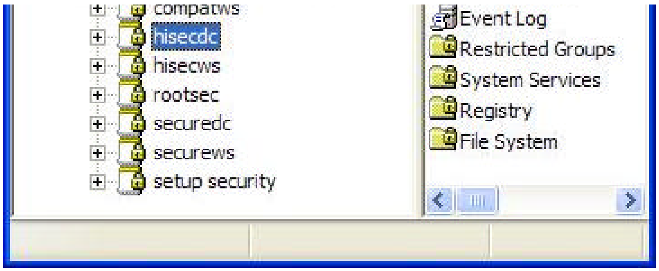


Figure 2. Typical security template structure.

As you can see, there is a direct correlation between the two. The reason for this is that a security template is nothing more than a text based file that can update all of these security settings in a GPO. There are some other subfolders and details under each section of the security, which we take a look at here.

Account Policy

The account policy section is really three groups of settings in one. The account policies control user passwords and when the user forgets their password at logon.

- Password Policy – This configures the password itself, with regard to validity period, length of password, and complexity of the password.
- Account Lockout policy – This configures how the password will react when the user fails to input their correct password multiple times.
- Kerberos Policy – This controls the Kerberos ticketing for the domain communication. This is ONLY available for GPOs that are linked to the domain level.

User Rights

User rights control access to what a user and/or group can do on a computer. The user rights control the entire computer that it is configuring, not just a portion of it. User rights control administrative privileges such as logging on locally, backing up files, and changing the system time. The ability to control user rights in a security template breaks the old model where each computer needed to be configured individually to control user rights.

Event Log

The inclusion of event log settings in a security template adds a new dimension to the ability to control all computers' centrally. In the past, the only way to ensure that the three default logs (application, system, and security) were configured properly was to configure each server separately. These settings that can be made to control the size of the log file, the retention method of the log file, and the number of days to retain the log, and whether or not the guests group can access the security log.

Restricted Groups

Restricted groups are designed to control the members of a group, either at the domain level or in the local SAM of domain members. Restricted groups can be confusing and have strange results. Therefore, it is suggested that you thoroughly test your desired results before your roll them out into production.

The Restricted groups setting should be combined with the "Process even if the Group Policy objects have not changed" setting. This will keep the membership of the groups consistent, even if a local administrator decides to add more members to the group without approval.

One more thing to keep in mind with regard to restricted groups is that you can't combine different group settings from multiple security templates. This occurs when you import different security templates into GPOs linked to different levels in Active Directory. The result is that the last GPO and restricted group will be configured, removing all other group modifications in previously applied GPOs.

System Services

Before Active Directory and GPOs, you had to configure system services on each computer individually. Then, with the advent of GPOs, you could configure system services within the GPO to apply to multiple computers in a consistent manner. With security templates, you can configure the system services offline, test them, then roll them out with a GPO.

You can control many aspects of System Services by using security templates. Here are the options that you can configure for Services from a GPO:

- Startup mode – You can configure Automatic, Manual, or Disabled.
- ACL – Each service has an ACL, even though you can't see this from the Service itself. The GPO opens up this option. You can configure users or groups to have access to Start, Stop, Manage, etc each service.

The configuration of the security template with regard to system services is unique.

The configuration of the security template with regard to system services is unique. Depending on which computer you use to configure the security template will dictate which system services are available in the interface to configure. For example, if you configure the security template from a Windows XP Professional computer that has a default installation, you won’t be able to configure certain services in the security template such as IIS and File Replication Service. The solution to this problem is to create and manage security templates from computers that have all of the necessary services that you need to configure on the target computers.

File and Registry permissions

You can configure both the ACL and SACL for both files and Registry keys through the security templates. This gives you ultimate control over every file and Registry key, since the interface allows for you to browse for the file and key you want to control. You also control how the permissions act with the other subfolders and files and subkeys in the hierarchical structure of the file system or Registry. These settings include:

- Propagate inheritable permissions to all subfolders and files
- Replace existing permission on all subfolders and files with inheritable permissions
- Do not allow permissions on this file or folder to be replaced

The target that you configure in these settings does need to exist or the target computer, or the setting might cause other settings to fail.

Built-in security templates

There are plenty of built-in security templates that you can choose from. These templates are categorized for domain controllers, servers, and workstations. These security templates have default settings which have been designed by Microsoft. You can find all of these security templates in the C:\Windows\Security\Templates folder. Here is a list of the security templates that you will find in this folder.

- Compatws.inf – This is required by older applications that need to have weaker security to access the Registry and the file system.
- DC security.inf – This is used to configure security of the Registry and File system of a computer that was upgraded from Windows NT to Windows 2000/2003.
- Hisecdc.inf – This is used to increase the security and communications with the domain controllers.
- Hisecws.inf – This is used to increase security and communications for the client computers and member servers.
- Notssid.inf – This is used to weaken security to allow older applications to run on Windows Terminal Services.
- Ocfiless.inf – This is for optional components that are installed after the main operating system is installed. This will support services such as Terminal Services and Certificate Services.
- Securedc.inf – This is used to increase the security and communications with the domain controllers, but not to the level of the High Security DC security template.
- Securews.inf – This is used to increase security and communications for the client computers and member servers.
- Setup security.inf – This is used to reapply the default security settings of a freshly installed computer.

Summary

As you can see by this basic overview of security templates, they are used to centralize security on many computers at one time. The breadth that a security template covers is rather large, providing control over some of the most important security settings on any computer. With Microsoft providing you with a default set of security templates that can be used immediately or as a starting place, you can begin to centralize the security configurations immediately.

About Derek Melber

Derek Melber runs and operates www.auditingwindows.com, the first dedicated Web site for Windows Auditing and Security, and home to the only books on auditing Windows. He has also written an e-book series on Group Policy, available at http://www.mcpmag.com/resources. Derek also provides custom training. You can reach Derek at derekm@braincore.net.