

Re: Big Security Permission Mistake – Please Help if You Can

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.configuration_manage/2004-03/1068.html

From: Adm C (*admchrissnospam_at_nospamhotmail.com*)

Date: 03/30/04

Date: Tue, 30 Mar 2004 16:37:40 -0500

Try this (not sure what you did – more details of what you did might help.

C

HOW TO: Reset Security Settings Back to the Defaults

Applies To

This article was previously published under Q313222

IN THIS TASK

a.. SUMMARY

b..

a.. Sample Command to Reset Security Settings

b.. Secedit Parameters

SUMMARY

This step-by-step article describes how to set the security settings back to the default settings.

back to the top

Sample Command to Reset Security Settings

NOTE: After security settings are applied, you cannot undo the changes without restoring from a backup. If you are uncertain about resetting your security settings back to the default security settings, you must make a complete backup that includes the "System State" (the registry files). Items that are reset include NTFS file system files and folders, the registry, policies, services, privilege rights, and group membership.

To reset your operating system back to original installation default security settings:

1.. Click Start, click Run, type cmd, and then press ENTER.

2.. Type secdit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose, and then press ENTER. You receive a "Task is completed" message, and a warning message that something could not be done. You can safely ignore this message. For more information about this message, view the %windir%\Security\Logs\Scesrv.log file.

back to the top

Secedit Parameters

a.. /configure – Specifies that Secedit.exe should set system security settings.

b.. /DB filename – Provides the path to a database that contains the security template to be applied. This is a required argument, but the database file does not have to exist if you use the /CFG switch to specify a security template.

c.. /CFG filename – This argument is only valid when you use it with the /DB parameter. It is the path to the security template that will be imported into the database and applied to the system. If you do not specify this argument, the template that is already stored in the database will be applied.

d.. /overwrite – This argument is only valid when the /CFG argument is also used. This specifies whether the security template in the /CFG argument overwrites any template or composite template that is stored in the database instead of appending the results to the stored template. If this is not specified, the template in the /CFG argument will be appended to the stored template.

e.. /areas AreaName1AreaName2... Specifies the security areas to be applied to the system. The default is "all areas." Each area must be separated by a space.

AreaNameX – Description

SECURITYPOLICY – Local policy and domain policy for the system, including account policies, audit policies, and other policies.

GROUP_MGMT – Restricted group settings for any groups that are specified in the security template.

USER_RIGHTS – User logon rights and granting of privileges.

REGKEYS – Security on local registry keys.

FILESTORE – Security on local file storage.

SERVICES – Security for all defined services.

NOTE: Each of these areas coincide with similar names in the Security Template.

f.. /log logpath – You can use this switch to configure the location of the log file that tracks the changes.

g.. /verbose – Specifies more detailed progress information.

h.. /quiet – Minimize the amount of feedback that is provided during the update on the screen and in the log file.

For online help about Secedit, click Start, click Run, type %windir%\help\secedit.chm, and then press ENTER.

back to the top

The information in this article applies to:

a.. Microsoft Windows XP Professional

Last Reviewed: 4/1/2003 (2.0)

Keywords: kbenv kbhowto kbHOWTOMaster KB313222 kbAuditPro

"stevens@stevens.com" <user@domain.invalid> wrote in message
news:O%23mwewcFEHA.3080@tk2msftngp13.phx.gbl...

I recently changed security permissions on the C: drive of my server and now a number of applications don't work – or can't be uninstalled. Performing a System Restore back to a previous date does not solve the problem – and trying to manually restore the setting has proven unsuccessful in getting things to work again.

Questions:

1. Is there anyway to revert just the C: drive's security settings back to the default setting that existed before I screwed it up?
2. Would Windows Repair successfully revert the C: drive's security settings? If so, would it also affect the settings of my two RAID arrays in this server that are set as "Read Only" so clients cannot delete files?
3. Is there anyway for me to copy a specific file or folder from one of my many previous Drive Image archives that I have made or my C: drive using Powerquest Drive Image software in order to revert the system back to its former settings? If so, which file would I want to copy from the Drive Image Archive?

Thanks in advance for the help. I'm desperate.