

1999050308324125?Open&src=&docid=2000081610075225&nsf=ghost.nsf

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-09/0102.html>

From: -|Tree=Bonz|- (nospam_at_hotmail.com)

Date: 09/13/05

Date: Tue, 13 Sep 2005 00:47:08 GMT

<http://service1.symantec.com/SUPPORT/ghost.nsf/docid/1999050308324125?Open&src=&docid=2000081610075225>

How to change the SID on a Windows XP, Windows 2000, or Windows NT computer

Situation:

You are copying a Windows XP, Windows 2000, or Windows NT computer to another computer, and you want to know how to change the Security Identifier (SID) afterward.

Solution:

Need to change the SID

When you clone a Windows NT/2000/XP installation to many computers, the destination computers have the same SID and computer name as the source Windows installation. Because Windows NT/2000/XP networks use each computer's SID and computer name to uniquely identify the computer on the network, you must change the SID and computer name on each destination (client) computer after cloning.

Overview of ways to change the SID after cloning

* Ghost Walker

Ghost Walker is a Ghost utility included in the corporate Ghost versions and Norton Ghost 2003. Ghost Walker is a DOS program that allows you to change the SID and computer name at each client computer after cloning, that is, before restarting the computer into Windows.

* Ghost Console

The option SID Change is available on the Task you create in Ghost Console. When you use this option, Ghost remotely runs Ghost Walker at each client computer. That is, Ghost does not require that you visit each client computer to change the SID.

* Microsoft's System Preparation Tool (SysPrep)

Microsoft provides the SysPrep utility for preparing a source computer before creating an image of that computer. SysPrep allows you to change the SID, computer name, and other configuration information. When used on a Windows 2000/XP installation, SysPrep also prompts the client computers to rebuild their Plug and Play driver database.

* Third party utilities

Problems with changing SIDs

When the SID changer cannot locate and change all of the files that it needs to change, some applications or Windows features may not work on the destination computer.

Example of need to remove features before creating an image file

For instance, Windows 2000 NTFS File Encryption and Windows NT and Windows 2000 Protected Storage

<http://service1.symantec.com/SUPPORT/ghost.nsf/docid/1999050308324125?Open&src=&docid=2000081610075225>

use a SID as a unique token. When you change the SID, Windows can no longer access encrypted files or Protected Storage media. To prevent the problem, these features must be removed before creating the image file.

Test the image file before rolling it out

For these reasons we advise that you prepare for mass rollouts or upgrades by first testing the image file on the various computer environments that you will rollout the image to, including testing the applications after cloning to a new computer.

Which SID changer to use

Each method for changing the SID has its own advantages and disadvantages. Use the SID changer recommended for the operating system being cloned.:

Note: Because Microsoft support varies depending upon the operating system, method of cloning, and method of changing the SID, refer to the Microsoft document Do Not Disk Duplicate Installed Versions of Windows (Article ID 162001) for more detailed information.

* Windows 2000 or Windows XP installation: Use Microsoft's System Preparation (SysPrep) tool.

Although Ghost Walker successfully changes the SID on Windows 2000/XP computers, Microsoft's System Preparation (SysPrep) tool changes the SID and prompts Windows 2000/XP to rebuild its Plug-and-Play driver database.

Alternatively, instead of using SysPrep for all configuration changes, you can use SysPrep to rebuild the driver database and use Ghost to change the SID and computer name. Here are the general steps:

1. Disable the SysPrep feature that changes the SID.
2. Run SysPrep at the source Windows 2000 computer immediately before cloning.
3. Use Ghost to create an image file of the source computer.
4. Check the SID Change option on the Task that you create in Ghost Console.
5. Run the Task to rollout the image.

* Windows NT installation: Use Ghost Walker or the SID Change option in Ghost Console.

Because Ghost Walker is more thorough than SysPrep at changing all instances of the SID, and Windows NT does not have a Plug and Play driver database for the Windows NT SysPrep utility to rebuild, Ghost Walker is a better choice for changing the SID and computer name on Windows NT installations.

* Other Windows installations, such as Windows 95/98/Me: Use Ghost Walker or the SID Change option in Ghost Console. Use the SID Change option when running a Task in Ghost Enterprise Console and use Ghost Walker when cloning with Ghost Multicast Server.

If you use a third party SID changer, make sure that the SID changer changes all instances of the old SID where the SID is used to control access to files, registry settings, and so on. If the SID changer does not update old instances of the SID, some application programs may not work. In addition, Windows will no longer recognize the security settings, resulting in either no access to selected system resources or global access to system resources, increasing security risks on the system.

Ghost Walker

Run Ghstwalk.exe at the target computer after you write the disk or partition image to the computer. Ghost Walker changes the SID for all user profiles on the computer to a statistically-unique, randomly-generated value. Because both Ghost.exe and Ghost Walker run in DOS, changing the SID with Ghost Walker does not require an additional restart.

Number of characters in the new name

The new name must contain the same number of characters as the computer name of the source computer. Ghost Walker can change the computer name on all supported Windows operating systems.

Available in these Ghost versions

- * Symantec Ghost 7.0
- * Symantec Ghost 7.5
- * Symantec Ghost 8.x
- * Norton Ghost 2003

SID Change option on Ghost Console

This option is available in all Ghost versions that include the feature Ghost Console.

Use this option

* For cloning Windows NT installations when you want Ghost to remotely change the SID on the client computers. To change the SID automatically, check the "SID Change" option on the Clone tab in the Task. To change other configuration items, check the Configuration option on the General tab in the Task, and then choose an option in the Configuration tab.

* If you decide to use the SID Change option for cloning a Windows 2000/XP installation, use either the SysPrep option that changes the SID or the Ghost Console SID Change option, but not both options.

SysPrep

Although Ghost successfully changes the SID on Windows 2000/XP computers, Microsoft's System Preparation (SysPrep) tool changes the SID and prompts Windows 2000/XP to rebuild its Plug-and-Play driver database.

Advantages to using SysPrep

* Rebuilding the driver database is a significant advantage because the rebuild decreases the amount of user intervention required at the client computers when the source computer and client computers do not have exactly the same hardware.

* It invokes the Windows 2000/XP Setup Wizard, which is normally only seen during installation. The Wizard enables you to enter details regarding new users, licensing information, and other identification information.

* It allows you to install different drivers for the hard disk controller on the first startup after cloning. When the client computer requires different hard drive controller drivers than the source computer, the new drivers are loaded before the Plug and Play detection begins.

* It can be configured to have Windows 2000/XP to rebuild its Plug-and-Play driver database on the first startup after cloning. The rebuild process removes drivers for devices that are not on the client computer and adds Windows drivers for devices that are on the client computer but were not on the source computer.

* It supports most of the unattended installation parameters, including computer name, domain, and network settings. These parameters are command-line arguments for the Windows installation command.

* It can be configured to run automatically, without having to visit the client computers.

No Symantec technical support for SysPrep

Symantec does not provide technical support for SysPrep. SysPrep is written, maintained, and supported by Microsoft.

To use SysPrep

See the document How to use SysPrep with Ghost. Note that SysPrep requires an additional restart after

cloning.

Technical Information:

SIDs, workgroups, and domains

For more information on why you must change the SID for workgroups and domains, see the section "Security identifier (SID) for workstations participating in a domain" in the document Introduction to cloning a Windows NT, Windows 2000, or Windows XP computer.

SIDs and security

Many programs, including Windows itself, base security features on the SID and the computer name.

The parts the SID changer needs to change

When the SID changer cannot locate and change all instances of the SID and computer name, or locate and change proprietary calculated values that are based on the SID and computer name, some applications or Windows features may not work on the destination computer after changing the SID.

References:

GhostWalker

Introduction to Ghost Walker

How to run Ghost Walker from a command line.

Cloning Windows servers

Cloning a Windows NT or Windows 2000/2003 Server

Separator

Translations of this Document:

Given the time needed to translate documents into other languages, the translated versions of this document may vary in content if the English document was updated with new information during the translation process.

The English document always contains the most up-to-date information.