How to use the SysKey utility to secure the Windows Security Accounts Manager database

Archived: 2026-04-05 21:10:45 UTC

For a Microsoft Windows NT version of this article, see 143475.

Summary

The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows 2003 Security Accounts Management Database (SAM) stores hashed copies of user passwords. This database is encrypted with a locally stored system key. To keep the SAM database secure, Windows requires that the password hashes are encrypted. Windows prevents the use of stored, unencrypted password hashes.

You can use the SysKey utility to additionally secure the SAM database by moving the SAM database encryption key off the Windows-based computer. The SysKey utility can also be used to configure a start-up password that must be entered to decrypt the system key so that Windows can access the SAM database. This article describes how to use the SysKey utility to secure the Windows SAM database.

More Information

Configure Windows System Key Protection

To Configure Windows System Key Protection, follow these steps:

1. At a command prompt, type syskey, and then press ENTER.
2. In the **Securing the Windows Account Database** dialog box, note that the **Encryption Enabled** option is selected and is the only option available. When this option is selected, Windows will always encrypt the SAM database.
3. Click **Update**.
4. Click **Password Startup** if you want to require a password to start Windows. Use a complex password that contains a combination of upper case and lower case letters, numbers, and symbols. The startup password must be at least 12 characters long and can be up to 128 characters long.

   Note If you must remotely restart a computer that requires a password (if you use the **Password Startup** option), a person must be at the local console during the restart. Use this option only if a trusted security administrator will be available to type the Startup password.
5. Click **System Generated Password** if you do not want to require a startup password.

   Select either of the following options:

- Click **Store Startup Key on Floppy Disk** to store the system startup password on a floppy disk. This requires that someone insert the floppy disk to start the operating system.
- Click **Store Startup Key Locally** to store the encryption key on the hard disk of the local computer. This is the default option.

Click **OK** two times to complete the procedure.

Remove the SAM encryption key from the local hard disk by using the **Store Startup Key on Floppy Disk** option for optimum security. This provides the highest level of protection for the SAM database.

Always create a back-up floppy disk if you use the **Store Startup Key on Floppy Disk** option. You can restart the system remotely if someone is available to insert the floppy disk into the computer when it restarts.

Note The Microsoft Windows NT 4.0 SAM database was not encrypted by default. You can encrypt the Windows NT 4.0 SAM database by using the SysKey utility.

Need more help?

Want more options?

Explore subscription benefits, browse training courses, learn how to secure your device, and more.
