



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

EFS ENCRYPTION ALGORITHMS IN WINDOWS XP SP1

Products: Windows XP Professional with Service Pack 1; Windows Server 2003

Overview

EFS (Encrypting File System) was first introduced in Windows 2000 as a means of providing file- and folder-level encryption capabilities for mobile users. EFS transparently encrypts and decrypts files as they are written to or read from the disk, respectively, and typically does not provide any encryption while traveling on the network (that functionality is left to SSL, VPNs, and IPSec in transport mode). Since its introduction, EFS has been refined in Windows XP Professional (Windows XP Home does not support EFS) to allow multi-user access to EFS-encrypted files. With the introduction of Service Pack 1 (SP1) for Windows XP Professional, EFS now supports three different encryption algorithms: Expanded DES (DESX), with a cipher strength of 56 bits or 128 bits (if high encryption support is installed); Triple DES (3DES), with a cipher strength of 168 bits; and the Advanced Encryption Standard (AES), with a cipher strength of 256 bits. Windows Server 2003 also shares the same functionality.

Unfortunately, these encryption algorithms are not interoperable. This technical note discusses how to specify which EFS encryption algorithm a Windows XP Professional-based system (with Service Pack 1) should use when encrypting files.

More Information

Specifying the EFS encryption algorithm that should be used involves editing the Registry. (As always, use extreme caution when editing the Registry to avoid irreparable damage to the operating system.)

To specify the encryption algorithm, use Registry Editor (regedit.exe) to navigate to the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS

At this location, create a value named AlgorithmID (of type REG_DWORD) and specify the following data for this value (be sure to select the Hexadecimal radix when entering this data):

- For DESX (expanded DES), specify a value of 0x6604.
- For 3DES (Triple DES), specify a value of 0x6603.
- For 256-bit AES (Advanced Encryption Standard), specify a value of 0x6610. This is the default value for Windows XP Professional systems with Service Pack 1.

DESX is fully compatible with Windows 2000, Windows XP Professional (both pre- and post-SP1), and Windows Server 2003. 3DES is only compatible with Windows XP Professional (before and after the installation of SP1), and AES is compatible with only SP1 or later of Windows XP Professional.

To maximize security (but minimize compatibility with earlier versions of Windows that support EFS), specify AES as the EFS encryption provider.

To maximize compatibility with earlier versions of Windows that support EFS, on the other hand, specify DESX as the EFS encryption algorithm.

Keep in mind that all EFS-encrypted files should be decrypted before changing the EFS encryption algorithm, or the data contained within those files will be lost. After the encryption algorithm is specified in the Registry and the system is restarted, the files may be encrypted again.

Other Notes

None

Related Articles/Resources

The following Microsoft Knowledge Base article provides additional information on how to specify the encryption algorithm used by Windows XP's version of EFS:

329741: EFS Files Appear Corrupted When You Open These Files Using Windows 2000 or Windows XP Pre-SP1

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.