Network security: Configure encryption types allowed for Kerberos

learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos

- Article
- 04/19/2017

In this article

1. Reference
2. Security considerations
3. Related articles

Applies to

- Windows 11
- Windows 10
- Windows Server

Describes the best practices, location, values, and security considerations for the **Network security: Configure encryption types allowed for Kerberos** security policy setting.

Reference

This policy setting allows you to set the encryption types that the Kerberos protocol is allowed to use. If it isn't selected, the encryption type won't be allowed. This setting might affect compatibility with client computers or services and applications. Multiple selections are permitted.

For more information, see KDC event ID 16 or 27 is logged if DES for Kerberos is disabled.

The following table lists and explains the allowed encryption types.

Encryption type	Description and version support
DES_CBC_CRC	Data Encryption Standard with Cipher Block Chaining using the Cyclic Redundancy Check function Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. The Windows 7, Windows 10, Windows 11, Windows Server 2008 R2, and later operating systems don't support DES by default.

Encryption type	Description and version support
DES_CBC_MD5	Data Encryption Standard with Cipher Block Chaining using the Message-Digest algorithm 5 checksum function Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. The Windows 7, Windows 10, Windows 11, Windows Server 2008 R2, and later operating systems don't support DES by default.
RC4_HMAC_MD5	Rivest Cipher 4 with Hashed Message Authentication Code using the Message-Digest algorithm 5 checksum function Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.
AES128_HMAC_SHA1	Advanced Encryption Standard in 128-bit cipher block with Hashed Message Authentication Code using the Secure Hash Algorithm (1). Not supported in Windows 2000 Server, Windows XP, or Windows Server 2003. Supported in Windows Vista, Windows Server 2008, Windows 7, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.
AES256_HMAC_SHA1	Advanced Encryption Standard in 256-bit cipher block with Hashed Message Authentication Code using the Secure Hash Algorithm (1). Not supported in Windows 2000 Server, Windows XP, or Windows Server 2003. Supported in Windows Vista, Windows Server 2008, Windows 7, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.
Future encryption types	Reserved by Microsoft for other encryption types that might be implemented.

Possible values

The encryption type options include:

- DES_CBC_CRC
- DES_CBC_MD5
- RC4_HMAC_MD5
- AES128_HMAC_SHA1
- AES256_HMAC_SHA1

- Future encryption types

  As of the release of Windows 7 and Windows Server 2008 R2, these options are reserved by Microsoft for other encryption types that might be implemented.

Best practices

Analyze your environment to determine which encryption types will be supported and then select the types that meet that evaluation.

Location

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Default values

Server type or Group Policy Object (GPO)	Default value
Default domain policy	Not defined
Default domain controller policy	Not defined
Stand-alone server default settings	Not defined
Domain controller effective default settings	The default OS setting applies, DES suites aren't supported by default.
Member server effective default settings	The default OS setting applies, DES suites aren't supported by default.
Effective GPO default settings on client computers	The default OS setting applies, DES suites aren't supported by default.

Security considerations

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Vulnerability

Windows Server 2008 R2, Windows 7, and Windows 10, don't support the DES cryptographic suites because stronger ones are available. To enable Kerberos interoperability with non-Windows versions of the Kerberos protocol, these suites can be enabled. However, doing so might open attack vectors on computers running Windows Server 2008 R2, Windows 7 and Windows 10. You can also disable DES for your computers running Windows Vista and Windows Server 2008.

Countermeasure

Don't configure this policy. This disablement will force the computers running Windows Server 2008 R2, Windows 7, and Windows 10 to use the AES or RC4 cryptographic suites.

Potential impact

If you don't select any of the encryption types, computers running Windows Server 2008 R2, Windows 7 and Windows 10, might have Kerberos authentication failures when connecting with computers running non-Windows versions of the Kerberos protocol.

If you do select any encryption type, you'll lower the effectiveness of encryption for Kerberos authentication but you'll improve interoperability with computers running older versions of Windows. Contemporary non-Windows implementations of the Kerberos protocol support RC4 and AES 128-bit and AES 256-bit encryption. Most implementations, including the MIT Kerberos protocol and the Windows Kerberos protocol, are deprecating DES encryption.

Related articles

- Security Options