 Filter by title

Event ID 27 KDC error on domain controllers

How to disable the Subject Alternative Name for UPN mapping

How to force Kerberos to use TCP instead of UDP

KDC event 16 or 27 if DES for Kerberos is disabled

KDC service on an RODC can't start and generates error 1450

Kerberos authentication fails when a user belongs to many groups

Kerberos SPN is on wrong account

Kerberos Unsupported etype error

KRB_AP_ERR_MODIFIED error on Kerberos client

Logging on a user account fails

Registry keys about Kerberos protocol and KDC

Resource SID compression causes authorization problems

SSO with pre-logon fails during user logon

TGS requests for krbtgt account fail

The Fingerprint Registration Wizard doesn't run

> Legacy authentication (NTLM)

> Netlogon, secure channel, DC Locator

> Permissions, access control, and auditing

> Secure channel issues


> Security templates

> Windows LAPS

> Windows Servicing, Updates and Features on Demand

> Windows Server End of Support (EoS) FAQ

> Support Tools

 **Download PDF**

KDC event ID 16 or 27 is logged if DES for Kerberos is disabled

Article • 12/26/2023 • [3 contributors](#)

 [Feedback](#)

In this article

- [Summary](#)
- [Symptoms](#)
- [Cause](#)
- [Workaround](#)
- [More information](#)

This article describes how to enable DES encryption for Kerberos authentication in Windows 7 and in Windows Server 2008 R2.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 977321

Summary

Starting with Windows 7, Windows Server 2008 R2, and all later Windows operating systems, Data Encryption Standard (DES) encryption for Kerberos authentication is disabled. This article describes various scenarios in which you may receive the following events in the Application, Security, and System logs because DES encryption is disabled:

- KDCEVENT_UNSUPPORTED_ETYPE_REQUEST_TGS
- KDCEVENT_NO_KEY_INTERSECTION_TGS

Additionally, this article explains how to enable DES encryption for Kerberos authentication in Windows 7 and in Windows Server 2008 R2. For detailed information, see the "Symptoms," "Cause," and "Workaround" sections of this article.



Symptoms

Consider the following scenarios:

- A service uses a user account or a computer account that is configured for only DES encryption on a computer that is running Windows 7 or Windows Server 2008 R2.
- A service uses a user account or a computer account that is configured for only DES encryption and that is in a domain together with Windows Server 2008 R2-based domain controllers.
- A client that is running Windows 7 or Windows Server 2008 R2 connects to a service by using a user account or a computer account that is configured for only DES encryption.
- A trust relationship is configured for only DES encryption and includes domain controllers that are running Windows Server 2008 R2.
- An application or a service is hardcoded to use only DES encryption.

In any of these scenarios, you may receive the following events in the Application, Security, and System logs together with the **Microsoft-Windows-Kerberos-Key-Distribution-Center** source:

 Expand table

ID	Symbolic name	Message
27	KDCEVENT_UNSUPPORTED_ETYPE_REQUEST_TGS	While processing a TGS request for the target server %1, the account %2 did not have a suitable key for generating a Kerberos ticket (the missing key has an ID of %3). The requested etypes were %4. The accounts available etypes were %5. Event ID 27 - KDC Encryption Type Configuration 
16	KDCEVENT_NO_KEY_INTERSECTION_TGS	While processing a TGS request for the target server %1, the account %2 did not have a suitable key for generating a Kerberos ticket (the missing key has an ID of %3). The requested etypes were %4. The accounts available etypes were %5. Changing or resetting the password of %6 will generate a proper key. Event ID 16 - Kerberos Key Integrity 

Cause

By default, the security settings for DES encryption for Kerberos are disabled on the following computers:

- Computers that are running Windows 7
- Computers that are running Windows Server 2008 R2
- Domain controllers that are running Windows Server 2008 R2

Note

Cryptographic support for Kerberos exists in Windows 7 and in Windows Server 2008 R2.By default, Windows 7 uses the following Advance Encryption Standard (AES) or RC4 cipher suites for "encryption types" and for "etypes":

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC


Services that are configured for only DES encryption fail unless the following conditions are true:

- The service is reconfigured to support RC4 encryption or to support AES encryption.
- All client computers, all servers, and all domain controllers for the domain of the service account are configured to support DES encryption.

By default, Windows 7 and Windows Server 2008 R2 support the following cipher suites: The DES-CBC-MD5 cipher suite and the DES-CBC-CRC cipher suite can be enabled in Windows 7 when it's required.

Workaround

We strongly recommend that you check whether DES encryption is still required in the environment or check whether specific services require only DES encryption. Check whether the service can use RC4 encryption or AES encryption, or check whether the vendor has an authentication alternative that has stronger cryptography.

Hotfix [978055](#)  is required for the Windows Server 2008 R2-based domain controllers to correctly handle encryption type information that is replicated from the domain controllers

that are running Windows Server 2003. See more information section below.

1. Determine whether the application is hard-coded to use only DES encryption. But it's disabled by the default settings on clients that are running Windows 7 or on Key Distribution Centers (KDCs).

To check whether you're affected by this problem, collect some network traces, and then check for traces that resemble the following sample traces:

```
Frame 1 {TCP:48, IPv4:47} <SRC IP> <DEST IP> KerberosV5 KerberosV5:TGS Request
Realm: CONTOSO.COM Sname: HTTP/<hostname>.<FQDN>

Frame 2 {TCP:48, IPv4:47} <DEST IP> <SRC IP> KerberosV5 KerberosV5:KRB_ERROR
- KDC_ERR_ETYPE_NOSUPP (14)

0.000000 {TCP:48, IPv4:47} <source IP> <destination IP> KerberosV5
KerberosV5:TGS Request Realm: <fqdn> Sname: HTTP/<hostname>.<fqdn>
-Etype:
+SequenceOfHeader:
+EType: aes256-cts-hmac-sha1-96 (18)
+EType: aes128-cts-hmac-sha1-96 (17)
+EType: rc4-hmac (23)
+EType: rc4-hmac-exp (24)
+EType: rc4 hmac old exp (0xff79)
+TagA:
+EncAuthorizationData:
```

2. Determine whether the user account or the computer account is configured for only DES encryption.

In "Active Directory Users and Computers" snap-in, open user account properties, and then check whether the **Use Kerberos DES encryption types for this account** option is set under the **Account** tab.

If you conclude that you're affected by this issue and that you have to turn on the DES encryption type for Kerberos authentication, enable the following Group Policies to apply the DES encryption type to all computers that are running Windows 7 or Windows Server 2008 R2:

1. In the Group Policy Management Console (GPMC), locate the following location:

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

2. Click to select the Network security: Configure encryption types allowed for Kerberos option.
3. Click to select **Define these policy settings** and all the six check boxes for the encryption types.
4. Click **OK**. Close the GPMC.

ⓘ **Note**

The policy sets the `SupportedEncryptionTypes` registry entry to a value of **0x7FFFFFFF**. The `SupportedEncryptionTypes` registry entry is at the following location:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\parameters

Depending on the scenario, you may have to set this policy at the domain level to apply the DES encryption type to all clients that are running Windows 7 or Windows Server 2008 R2. Or,

you may have to set this policy at the organizational unit (OU) of the domain controller for the domain controllers that are running Windows Server 2008 R2.

More information

The DES-only application compatibility issues are encountered in the following two configurations:

- The calling application is hardcoded for only DES encryption.
- The account that runs the service is configured to use only DES encryption.

The following encryption type criteria must be satisfied for Kerberos authentication to work:

1. A common type exists between the client and the domain controller for the authenticator on the client.
2. A common type exists between the domain controller and the resource server to encrypt the ticket.
3. A common type exists between the client and the resource server for the session key.

Consider the following situation:

 Expand table

Role	OS	Supported encryption level for Kerberos
DC	Windows Server 2003	RC4 and DES
Client	Windows 7	AES and RC4
Resource Server	J2EE	DES

In this situation, the criteria 1 is satisfied by RC4 encryption, and the criteria 2 is satisfied by DES encryption. The third criterion fails because the server is DES-only and because client doesn't support DES.


The hotfix 978055 must be installed on each Windows Server 2008 R2-based domain controller if the following conditions are true in the domain:

- There are some DES-enabled user or computer accounts.
- In the same domain, there's one or more domain controllers that are running Windows 2000 Server, Windows Server 2003, or Windows Server 2003 R2.

Note

- Hotfix 978055 is required for the Windows Server 2008 R2-based domain controllers to correctly handle encryption type information that is replicated from the domain controllers that are running Windows Server 2003.
- The Windows Server 2008-based domain controllers do not require this hotfix.
- This hotfix isn't required if the domain has only Windows Server 2008-based domain controllers.

For more information, click the following article number to view the article in the Microsoft Knowledge Base:

[978055](#)  FIX: User accounts that use DES encryption for Kerberos authentication types cannot be authenticated in a Windows Server 2003 domain after a Windows Server 2008 R2 domain controller joins the domain

Feedback

Was this page helpful?

👍 Yes

👎 No

[Provide product feedback](#) 

Additional resources




Training

Module

[Troubleshoot Active Directory - Training](#)

Learn how to troubleshoot AD DS service failures or degraded performance. Learn how to recover deleted security objects and the AD DS database, and how to troubleshoot hybrid authentication issues.

 English (United States)  Your Privacy Choices  Theme 

[Manage cookies](#) [Previous Versions](#) [Blog](#)  [Contribute](#) [Privacy](#)  [Terms of Use](#) [Trademarks](#)  [© Microsoft 2024](#)