



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

Recommended Version



Event ID 27 — KDC Encryption Type Configuration

Article • 08/26/2009

In this article

[Event Details](#)

[Resolve](#)

[Verify](#)

[Related Management Information](#)

Applies To: Windows Server 2008 R2



Kerberos allows certain encryption types that can be used to encrypt Kerberos tickets. Other encryption types can be configured for Kerberos clients that do not support the default encryption types.

Event Details

 Expand table

Product:	Windows Operating System
ID:	27
Source:	Microsoft-Windows-Kerberos-Key-Distribution-Center
Version:	6.1
Symbolic Name:	KDCEVENT_UNSUPPORTED_ETYPE_REQUEST_TGS
Message:	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.

Resolve

Configure an available encryption type

Kerberos supports several encryption types that are used to encrypt the tickets. If you are using a non-Microsoft Kerberos client to request a ticket from a Windows-based Kerberos server, the Kerberos client must support the same encryption type. Use the event log message to determine the available encryption type and configure the Kerberos client accordingly.

Verify

To verify that the Kerberos client is configured with an available encryption type, you should ensure that a Kerberos ticket was received from the Key Distribution Center (KDC) and cached on the local computer. You can view cached Kerberos tickets on the local computer by using the Klist command-line tool.

Note: Klist.exe is not included with Windows Vista, Windows Server 2003, Windows XP, or Windows 2000. You must download and install the Windows Server Resource Kit before you can use Klist.exe.

To view cached Kerberos tickets by using Klist:




1. Log on to a Kerberos client computer within your domain.
2. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. Type **klist tickets**, and then press ENTER.
4. Verify that a cached Kerberos ticket is available.
 - Ensure that the **Client** field displays the client on which you are running Klist.
 - Ensure that the **Server** field displays the domain in which you are connecting.
5. Close the command prompt.

Related Management Information

[KDC Encryption Type Configuration](#)

[Core Security](#)

 English (United States)  Your Privacy Choices  Theme 

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

© Microsoft 2024