KAK - Event ID 1004 — Terminal Services Client Access License (TS CAL) Availability

Applies To: Windows Server 2008

A terminal server must be able to contact (discover) a Terminal Services license server in order to request Terminal Services client access licenses (TS CALs) for users or computing devices that are connecting to the terminal server. In addition, the Terminal Services licensing mode configured on a terminal server must match the type of TS CALs available on the license server.

Note: A terminal server running Windows Server 2008 can only communicate with a license server running Windows Server 2008.

Event Details

Product:	Windows Operating System
ID:	1004
Source:	Microsoft-Windows-TerminalServices-RemoteConnectionManager
Version:	6.0
Symbolic Name:	EVENT_CANNOT_ISSUE_LICENSE
Message:	The terminal server cannot issue a client license. It was unable to issue the license due to a changed (mismatched) client license, insufficient memory, or an internal error. Further details for this problem may have been reported at the client's computer.

Diagnose

This error might be caused by one of the following conditions:

- The licensing mode for the terminal server does not match the type of TS CALs installed on the license server.
- The RDP encryption levels on the terminal server and the client are not compatible.
- The certificate on the terminal server is corrupted.

The licensing mode for the terminal server does not match the type of TS CALs installed on the license server

To perform this procedure, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To determine the licensing mode for the terminal server:

1. On the terminal server, open Terminal Services Configuration. To open Terminal Services Configuration, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. In the left pane, click **Licensing Diagnosis**.
4. Review the following information in Licensing Diagnosis:
    - Under **Terminal Server Configuration Details**, note the licensing mode for the terminal server.
    - Under **Terminal Services License Server Information**, note the type of TS CALs installed on any license server that is listed as discovered. Information about the type of TS CALs installed on a license server is listed under **License Server Configuration Details**, which is displayed when you click a license server listed as discovered under **Terminal Services License Server Information**.
5. If the licensing mode for the terminal server does not match the type of TS CALs installed on the license server, see the section titled "Specify the licensing mode for the terminal server."

The RDP encryption levels on the terminal server and the client are not compatible

To perform this procedure, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To determine the RDP encryption level compatibility:

1. On the terminal server, open Terminal Services Configuration. To open Terminal Services Configuration, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Under **Connections**, right-click the connection (for example, **RDP-Tcp**), and then click **Properties**.
4. On the **General** tab, note the value of **Encyption level**. For more information about encryption levels, see "Configure Server Authentication and Encryption Levels" in the Terminal Services Configuration Help in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?LinkId=101637).
5. On the client computer, start Remote Desktop Connection. To start Remote Desktop Connection, click **Start**, click **Run**, type **mstsc.exe**, and then press ENTER.
6. Click the icon in the upper-left corner of the **Remote Desktop Connection** dialog box, and then click **About**. Look for the phrase "Maximum encryption strength" in the **About Remote Desktop Connection** dialog box. This value is the maximum encryption strength supported by the version of Remote Desktop Connection running on the computer.
7. If the maximum encryption strength supported by the version of Remote Desktop Connection running on the client computer is not supported by the encryption level configured on the terminal server, see the section titled "Change the RDP encryption level on the terminal server."

The certificate on the terminal server is corrupted

If the licensing mode for the terminal server matches the type of TS CALs installed on the license server and the RDP settings on the terminal server and the client are compatible, the certificate on the terminal server might be corrupted. To resolve this issue, see the section titled "Delete the appropriate registry subkey."

Resolve

To resolve this issue, use the resolution that corresponds to the cause you identified in the Diagnose section. After performing the resolution, see the Verify section to confirm that the feature is operating properly

Cause	Resolution
The licensing mode for the terminal server does not match the type of TS CALs installed on the license server	Specify the licensing mode for the terminal server
The RDP encryption levels on the terminal server and the client are not compatible	Change the RDP encryption level on the terminal server
The certificate on the terminal server is corrupted	Delete the appropriate registry subkey

Specify the licensing mode for the terminal server

To resolve this issue, specify the Terminal Services licensing mode on the terminal server.

The Terminal Services licensing mode determines the type of Terminal Services client access licenses (TS CALs) that a terminal server will request from a license server on behalf of a client connecting to the terminal server. Although there is a licensing grace period during which no license server is required, after the grace period ends, clients must receive a valid TS CAL issued by a license server before they can log on to a terminal server.

Important: The Terminal Services licensing mode configured on a terminal server must match the type of TS CALs available on the license server.

To perform this procedure, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To specify the Terminal Services licensing mode:

1. On the terminal server, open Terminal Services Configuration. To open Terminal Services Confiiguration, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Under **Licensing**, double-click **Terminal Services licensing mode**.
4. Select either **Per Device** or **Per User**, depending on your environment. For more information about the two options, see "Specify the Terminal Services Licensing Mode" in the Terminal Services Configuration Help in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?LinkId=101638).
5. Click **OK**, and then click **OK**.

Note: You can also specify the Terminal Services licensing mode for a terminal server by using Group Policy.

- To specify the Terminal Services licensing mode for a terminal server by using Group Policy, enable the **Set Terminal Services licensing mode** Group Policy setting. This Group Policy setting is located in **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Licensing**. Note that the Group Policy setting will take precedence over the setting configured in Terminal Services Configuration.
- To configure the Group Policy setting in Active Directory Domain Services (AD DS), use the Group Policy Management Console (GPMC). To configure the Group Policy setting locally on a terminal server, use the Local Group Policy Editor. For more information about configuring Group Policy settings, see either the Local Group Policy Editor Help (http://go.microsoft.com/fwlink/?LinkId=101633) or the GPMC Help (http://go.microsoft.com/fwlink/?LinkId=101634) in the Windows Server 2008 Technical Library.

Change the RDP encryption level on the terminal server

To resolve this issue, change the RDP encryption level on the terminal server to a level that is supported by the version of Remote Desktop Connection that is running on the client computer.

By default, Terminal Services connections are encrypted at the highest level of security available (128-bit). However, some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such legacy clients, you can set the encryption level of the connection to send and receive data at the highest encryption level supported by the client.

To perform this procedure, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To change the RDP encryption level:

1. On the terminal server, open Terminal Services Configuration. To open Terminal Services Configuration, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Under **Connections**, right-click the connection (for example, **RDP-Tcp**), and then click **Properties**.
4. On the **General** tab, change the value of **Encyption level** to a level that is appropriate for the version of Remote Desktop Connection that is running on the client computer. For more information about encryption levels, see "Configure Server Authentication and Encryption Levels" in the Terminal Services Configuration Help in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?LinkId=101637).

When you change the encryption level, the new encryption level takes effect the next time a user logs on. If you require multiple levels of encryption on one terminal server, install multiple network adapters and configure each adapter separately.

Note: You can also change the RDP encryption level on the terminal server by using Group Policy.

- To set the RDP encryption level for the terminal server by using Group Policy, enable the **Set client connection encryption level** Group Policy setting. This Group Policy setting is located in **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Security**. Note that the Group Policy setting will take precedence over the setting configured in Terminal Services Configuration.
- To configure the terminal server to use FIPS as the encryption level by using Group Policy, enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing** Group Policy setting. This Group Policy setting is located in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**. Note that this Group Policy setting will take precedence over the setting configured in Terminal Services Configuration and takes precedence over the **Set client connection encryption level** policy setting.
- To configure the Group Policy setting in Active Directory Domain Services (AD DS), use the Group Policy Management Console (GPMC). To configure the Group Policy setting locally on a terminal server, use the Local Group Policy Editor. For more information about configuring Group Policy settings, see either the Local Group Policy Editor Help (http://go.microsoft.com/fwlink/?LinkId=101633) or the GPMC Help (http://go.microsoft.com/fwlink/?LinkId=101634) in the Windows Server 2008 Technical Library.

Delete the appropriate registry subkey

To resolve this issue, delete the **MSLicensing** registry subkey on the client computer, restart the client computer, and then try again to connect remotely to the terminal server from the client computer. If the issue persists, delete the **Certificate**, **X509 Certificate**, **X509 Certificate2**, and **X509 Certificate ID** registry entries on the terminal server, restart the terminal server, and then try again to connect to the terminal server from the client computer.

Delete the MSLicensing registry subkey

To perform this procedure on the client computer, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To delete the **MSLicensing** registry subkey:

Caution: Incorrectly editing the registry might severely damage your system. Before making changes to the registry, you should back up any valued data.

1. On the client computer, open Registry Editor. To open Registry Editor, click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Locate the **HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing** registry subkey.
4. Click **MSLicensing**.
5. Before deleting the **MSLicensing** subkey, back up the subkey. To back up the subkey, do the following:
    1. On the **Registry** menu, click **Export Registry File**.
    2. In the **File name** box, type **mslicensingbackup**, and then click **Save**. If you need to restore this registry subkey, double-click **mslicensingbackup.reg**.
6. To delete the **MSLicensing** subkey, on the **Edit** menu, click **Delete**, and then click **Yes**.
7. Close **Registry Editor**, and then restart the client.
8. After the client computer is restarted, try again to connect remotely to the terminal server from the client computer.

Delete the appropriate registry entries on the terminal server

If the issue persists, delete the **Certificate**, **X509 Certificate**, **X509 Certificate2**, and **X509 Certificate ID** registry entries on the terminal server.

To perform this procedure on the terminal server, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To delete the appropriate registry entries:

Caution: Incorrectly editing the registry can severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

1. On the terminal server, open Registry Editor. To open Registry Editor, click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Locate the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Terminal Server\RCM** registry subkey.
4. Click **RCM**.
5. Before deleting the subkeys, back up the **RCM** subkey. To back up the subkey, do the following:
    1. On the **Registry** menu, click **Export Registry File**.
    2. In the **File name** box, type **tsrcm**, and then click **Save**. If you need to restore this registry subkey, double-click **tsrcm.reg**.
6. To delete the **Certificate**, **X509 Certificate**, **X509 Certificate2**, and **X509 Certificate ID** registry entries, right-click each entry, click **Delete**, and then click **Yes**.
7. Close **Registry Editor**, and then restart the terminal server.
8. After the terminal server is restarted, try again to connect remotely to the terminal server from the client computer.

If the issue persists, do the following:

1. On the client computer, back up and then delete the **MSLicensing** registry key and its subkeys.
2. On the terminal server, back up and then delete the **Certificate**, **X509 Certificate**, **X509 Certificate2**, and **X509 Certificate ID** registry entries.
3. Deactivate and then reactivate the license server. For information about deactivating and reactivating a license server, see the topic "Managing TS Licensing" in the TS Licensing Manager Help in the Windows Server 2008 Technical Library (http://go.microsoft.com/fwlink/?LinkId=101645).
4. Restart the terminal server and the client computer and then try again to connect remotely to the terminal server from the client computer.

Verify

To verify that the terminal server can discover (contact) a Terminal Services license server with the appropriate type of Terminal Services client access licenses (TS CALs), use Licensing Diagnosis in Terminal Services Configuration.

To perform this procedure, you must have membership in the local **Administrators** group, or you must have been delegated the appropriate authority.

To use Licensing Diagnosis in Terminal Services Configuration:

1. On the terminal server, open Terminal Services Configuration. To open Terminal Services Configuration, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. In the left pane, click **Licensing Diagnosis**.
4. Under **Terminal Server Configuration Details**, the value for **Number of TS CALs available for clients** should be greater than 0.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Terminal Server\RCM

Текст взят с почившего в небытие сайта asu.newmail.ru. Автор неизвестен.

Просьба не цитировать этот документ и не давать на него никаких ссылок.

90 дневное ограничение временной лицензии служб терминалов Windows 2003 Server.

Для подключения клиента к серверу приложений под Windows 2003 Server (в том числе, с установленным Citrix Meta Frame 1.8 for Windows 2003 Server, вне зависимости, ICA или RDP используется) необходимо иметь лицензию, которая хран ится локально, у клиентских станций под Windows 9x/NT она находится в реестре по адресу HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing . Выдает эту лицензию сервер с Windows 2003 Server на котором запущена служба "Лицензирование служб терминалов" (C:\WINNT\System32\lserver.exe). Без регистрации (активизации) службы "Лицензирование служб терминалов" клиентам выдаются временные лицензии, с 90 дневным ограничением срока действия. По окончанию срока подключение для этого клиента становится невозможным (Сервера становятся недоступны для данного клиента).

Снятие 90 дневного ограничения:

Пример 1 - временные лицензии.

Дата и время выдачи лицензии и окончания действия временной лицензии (через 90 дней) берется с сервера, на котором установлена эта служба, при этом все выданные лицензии хранятся в базе данных сервера, на котором установлена данная служба только для просмотра администратором. При переустановке службы база данных обнуляется. При подключении клиента к серверу проверяется только наличие и дата окончания лицензии на клиенте относительно сервера, к которому он подключается.

В качестве проверки был произведен следующий опыт: Служба "Лицензирование служб терминалов" была запущена на сервере с Windows 2003 Server с установленным 2020 годом. На клиентах, уже имеющих временную лицензию была удалена веточка реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing . На фирменных тонких клиентах, уже подключавшихся к серверу был обнулен (перезаписан) флеш. На станциях, не подключавшихся до этого, никаких процедур не производилось. На всех клиентских станциях была запущена клиентская программа и произведено соединение с сервером. После этого дата на сервере была возвращена на текущую. Подключения прошли без проблем и после изменения дат на серверах и рабочих станциях в пределах до 2019 года. Возможно, в ближайшем времени Microsoft решит эту проблему.

Пример 2 - активизация сервера.

В качестве эксперимента знакомый автора зашел на https://activate.microsoft.com и заполнил анкету вымышленными сведениями. При этом имя, фамилия, организация были в точности такие же, какие вводились в свойства сервера. После этого был получен код для активизации сервера лицензий. Далее было предложено зарегистрировать лицензии. После заполнения необходимого количества был запрошен номер заявки (Enrollment Agreement Number). В зарубежной поисковой системе на запрос Enrollment Agreement Number нашлись пять номеров:

6565792
5296992
3325596
4965437
4526017

То есть, для активации сервера нужно знать:

1. 25 символьный (5x5 цифробукв) серийный номер, на основании которого генерируется код продукта маски xxxxx-xxx-xxxxxxx-xxxxx (где x - цифробуква)
2. На основании кода продукта генерируется 35 символьный (7x5 цифробукв) код сервера лицензий.
3. На основании кода сервера лицензий, имени, фамилии, организации и 7 значного номера соглашения Enrollment Agreement Number генерируется 35 символьный (7x5 цифробукв) код ключевого пакета лицензий. Если эта цепочка принадлежит не одному серверу, возможно работать не будет.

Пример 3 - Установка обманного "hotfix".

Для снятия ограничения можно попробовать установить на сервер Windows 2003 хакерский "hotfix" TS_CRACK.ZIP (57K).
Внимание! Данный метод не проверялся!