

KMS activation: known issues

Article • 08/22/2022

Try our Virtual Agent

- It can help you quickly identify and fix common issues related to KMS and MAK activation

This article describes common questions and issues that can arise during Key Management Service (KMS) activations, and provides guidance for addressing the issues.

ⓘ Note

If you suspect that your issue is related to DNS, see [Common troubleshooting procedures for KMS and DNS issues](#).

Should I back up KMS host information?

Backup is not required for KMS hosts. However, if you use a tool to routinely clean up event logs, the activation history stored in the logs can be lost. If you use the event log to track or document KMS activations, periodically export the Key Management Service event log from the Applications and Services Logs folder of Event Viewer.

If you use System Center Operations Manager, the System Center Data Warehouse database stores event log data for reporting, therefore you do not have to back up the event logs separately.

Is the KMS client computer activated?

On the KMS client computer, open the **System** control panel, and look for the **Windows is activated** message. Alternatively, run `Slmgr.vbs` and use the `/dli` command-line option.

The KMS client computer does not activate

Verify that the KMS activation threshold is met. On the KMS host computer, run `Slmgr.vbs` and use the `/dli` command-line option to determine the host's current count. Until the KMS host has a count of 25, Windows 7 client computers cannot be activated.

Windows Server 2008 R2 KMS clients require a KMS count of 5 for activation. For more information about KMS requirements, see the [Volume Activation Planning Guide](#).

On the KMS client computer, look in the Application event log for event ID 12289. Check this event for the following information:

- Is the result code 0? Anything else is an error.
- Is the KMS host name in the event correct?
- Is the KMS port correct?
- Is the KMS host accessible?
- If the client is running a non-Microsoft firewall, does the outbound port have to be configured?

On the KMS host computer, look in the KMS event log for event ID 12290. Check this event for the following information:

- Did the KMS host log a request from the client computer? Verify that the name of the KMS client computer is listed. Verify that the client and KMS host can communicate. Did the client receive the response?
- If no event is logged from the KMS client, the request did not reach the KMS host or the KMS host was unable to process it. Make sure that routers do not block traffic using TCP port 1688 (if the default port is used) and that stateful traffic to the KMS client is allowed.

What does this error code mean?

Except for KMS events that have event ID 12290, Windows logs all activation events to the Application event log under the event provider name Microsoft-Windows-Security-SPP. Windows logs KMS events to the Key Management Service log in the Applications and Services folder. IT pros can run Slui.exe to display a description of most activation-related error codes. The general syntax for this command is as follows:

Windows Command Prompt

```
slui.exe 0x2a ErrorCode
```

For example, if event ID 12293 contains error code 0x8007267C, you can display a description of that error by running the following command:

Windows Command Prompt

```
slui.exe 0x2a 0x8007267C
```

For more information about specific error codes and how to address them, see [Resolving common activation error codes](#).

Clients are not adding to the KMS count

To reset the client computer ID (CMID) and other product-activation information, run **sysprep /generalize** or **slmgr /rearm**. Otherwise, each client computer looks identical, and the KMS host does not count them as separate KMS clients.

KMS hosts are unable to create SRV records

Domain Name System (DNS) may restrict Write access or may not support dynamic DNS (DDNS). In this case, give the KMS host Write access to the DNS database, or create the service (SRV) resource record (RR) manually. For more information about KMS and DNS issues, see [Common troubleshooting procedures for KMS and DNS issues](#).

Only the first KMS host is able to create SRV records

If the organization has more than one KMS host, the other hosts might not be able to update the SRV RR unless the SRV default permissions are changed. For more information about KMS and DNS issues, see [Common troubleshooting procedures for KMS and DNS issues](#).

I installed a KMS key on the KMS client

KMS keys should be installed only on KMS hosts, not on KMS clients. Run **slmgr.vbs -ipk <SetupKey>**. For tables of keys that you can use to configure the computer as a KMS client, see [KMS client setup keys](#). These keys are publicly known and are edition-specific. Remember to delete any unnecessary SRV RRs from DNS, and then restart the computers.

A KMS host failed

If a KMS host fails, you must install a KMS host key on a new host and then activate the host. Make sure that the new KMS host has an SRV RR in the DNS database. If you install the new KMS host using the same computer name and IP address as the failed KMS host, the new KMS host can use the DNS SRV record of the failed host. If the new host

has a different computer name, you can manually remove the DNS SRV RR of the failed host or (if scavenging is enabled in DNS) let DNS automatically remove it. If the network is using DDNS, the new KMS host automatically creates a new SRV RR on the DNS server. The new KMS host then starts collecting client renewal requests and begins activating clients as soon as the KMS activation threshold is met.

If your KMS clients use auto-discovery, they automatically select another KMS host if the original KMS host does not respond to renewal requests. If the clients do not use auto-discovery, you must manually update the KMS client computers that were assigned to the failed KMS host by running **slmgr.vbs /skms**. To avoid this scenario, configure the KMS clients to use auto-discovery. For more information, see the [Volume Activation Deployment Guide](#).