Guidelines for troubleshooting the Key Management Service (KMS)

Article • 09/19/2023

Enterprise customers set up Key Management Service (KMS) as part of their deployment process because it lets them use a simple, straightforward process to activate Windows in their environments. Usually, once you set up the KMS host, the KMS clients connect to the host automatically and activate on their own. However, sometimes the process doesn't work as expected. This article walks you through how to troubleshoot any issues you may encounter.

For more information about event log entries and the `slmgr.vbs` script, see Volume Activation Technical Reference.

Where to begin troubleshooting KMS

Let's start with a quick refresher on how KMS activation works. KMS is a client-server model that has some similarities to Dynamic Host Configuration Protocol (DHCP). However, instead of handing out IP addresses to clients on their request, KMS enables product activation. KMS is also a renewal model, in which the clients try to reactivate on a regular interval. There are two roles: the *KMS host* and the *KMS client*.

- The KMS host runs the activation service and enables activation in the environment. To configure a KMS host, you must install KMS key from the Volume License Service Center (VLSC) and then activate the service.
- The KMS client is the Windows operating system that you deploy in the environment and need to activate. KMS clients can run any edition of Windows that uses volume activation. The KMS clients come with a preinstalled key, called the *Generic Volume License Key (GVLK)* or *KMS Client Setup Key*. The presence of the GVLK is what makes a system a KMS client. The KMS clients use DNS SRV records (`_vlmcs._tcp`) to identify the KMS host. Next, the clients automatically try to discover and use this service to activate themselves. During the 30-day out-of-the-box grace period, they try to activate every two hours. After you activate the KMS clients, they try to renew their activation every seven days.

From a troubleshooting perspective, you may have to look at both the host and client sides to figure out why an issue is happening.

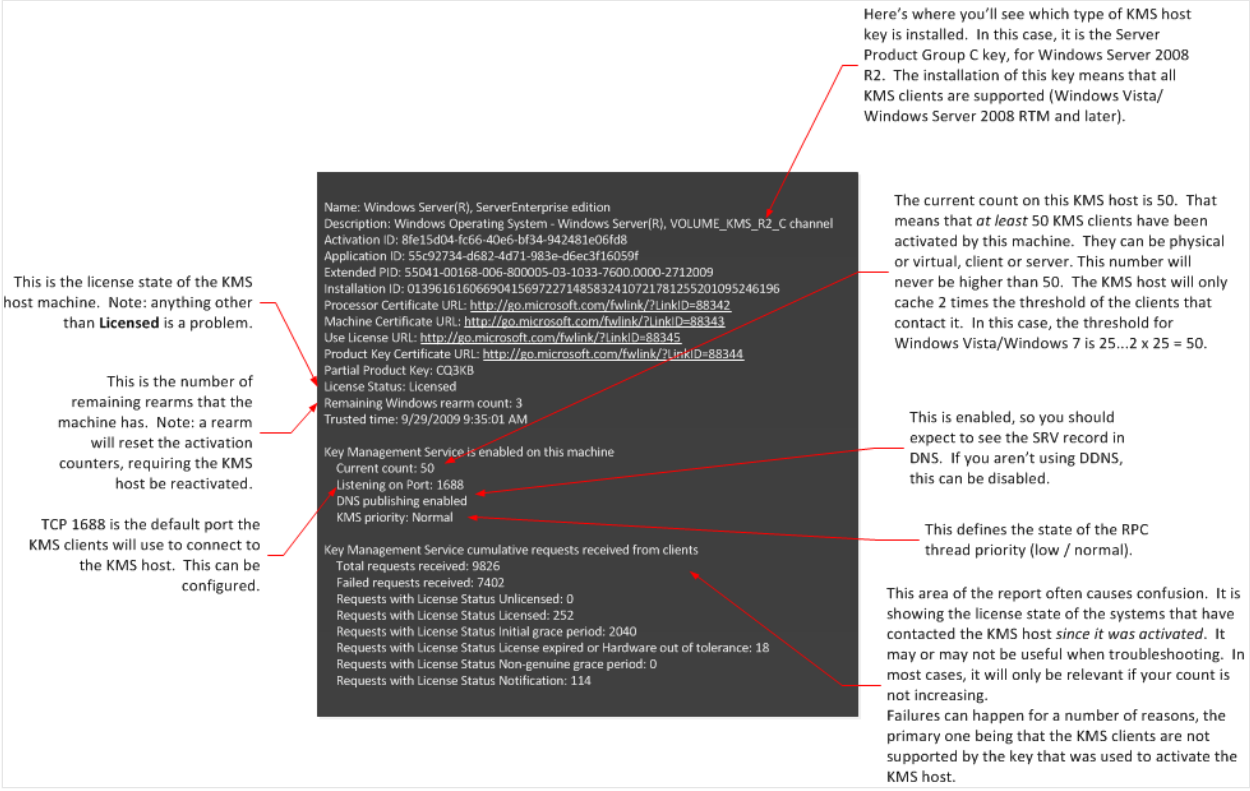
Troubleshooting on the KMS host

When you're examining the KMS host during troubleshooting, there are two areas you should look at:

- Check the status of the host software license service using the `slmgr.vbs` command in a command-line prompt.
- Check the Event Viewer for events related to licensing or activation.

Check the Software Licensing service using the slmgr.vbs command

To see verbose output from the Software Licensing service, open an elevated command prompt window and enter `slmgr.vbs /dlv`. The following screenshot shows the results of running this command on one of our KMS hosts within Microsoft.



Here are some variables you should pay attention to in the output while troubleshooting:

- The *Version Information* is at the top of the `slmgr.vbs /dlv` output. The version information is useful for determining whether the service is up-to-date. Making sure everything's up to date is important because the KMS service supports different KMS host keys. You can use this data to evaluate whether or not the version you're currently using supports the KMS host key you're trying to install. For more information about updates, see An update is available for Windows Vista and for Windows Server 2008 to extend KMS activation support for Windows 7 and for Windows Server 2008 R2.

- The *Name* indicates which edition of Windows is running on the KMS host system. You can use this information to troubleshoot issues that involve adding or changing the KMS host key. For example, you can use this information to verify if the OS edition supports the key you're trying to use.
- The *Description* shows you which key is currently installed. Use this field to verify whether the key that first activated the service was the correct one for the KMS clients you've deployed.
- The *License Status* shows the status of the KMS host system. The value should be **Licensed**. Any other value means you should reactivate the host.
- The *Current Count* displays a count between **0** and **50**. The count is cumulative between operating systems and indicates the number of valid systems that have tried to activate within a 30-day period.

  If the count is **0**, either the service was recently activated or no valid clients have connected to the KMS host.

  The count doesn't increase above **50**, no matter how many valid systems exist in the environment. The count is set to cache only twice the maximum license policy returned by a KMS client. The maximum policy set by the Windows client OS requires a count of **25** or higher from the KMS host to activate itself. Therefore, the highest count the KMS host can have is 2 x 25, or 50. In environments that contain only Windows Server KMS clients, the maximum count on the KMS host is **10**. This limit is because the threshold for Windows Server editions is **5** (2 x 5, or 10).

  A common issue related to the count happens when the environment has an activated KMS host and enough clients, but the count doesn't increase beyond one. When this issue happens, it means the deployed client image wasn't configured correctly, so the systems don't have unique Client Machine IDs (CMIDs). For more information, see KMS client and The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network. One of our Support Escalation Engineers has also blogged about this issue at KMS Host Client Count not Increasing Due to Duplicate CMIDs.

  Another reason why the count may not be increasing is that there are too many KMS hosts in the environment and the count is distributed over all of them.
- **Listening on Port**. Communication with KMS uses anonymous RPC. By default, the clients use the 1688 TCP port to connect to the KMS host. Make sure that this port is open between your KMS clients and the KMS host. You can change or configure the port on the KMS host. During their communication, the KMS host sends the

port designation to the KMS clients. If you change the port on a KMS client, the port designation is overwritten when that client contacts the host.

We often get asked about the *cumulative requests* section of the `slmgr.vbs /dlv` output. Generally, this data isn't helpful for troubleshooting. The KMS host keeps an ongoing record of the state of each KMS client that tries to activate or reactivate. Failed requests indicate the KMS host doesn't support certain KMS clients. For example, if a Windows 7 KMS client tries to activate against a KMS host that was activated by using a Windows Vista KMS key, the activation fails.

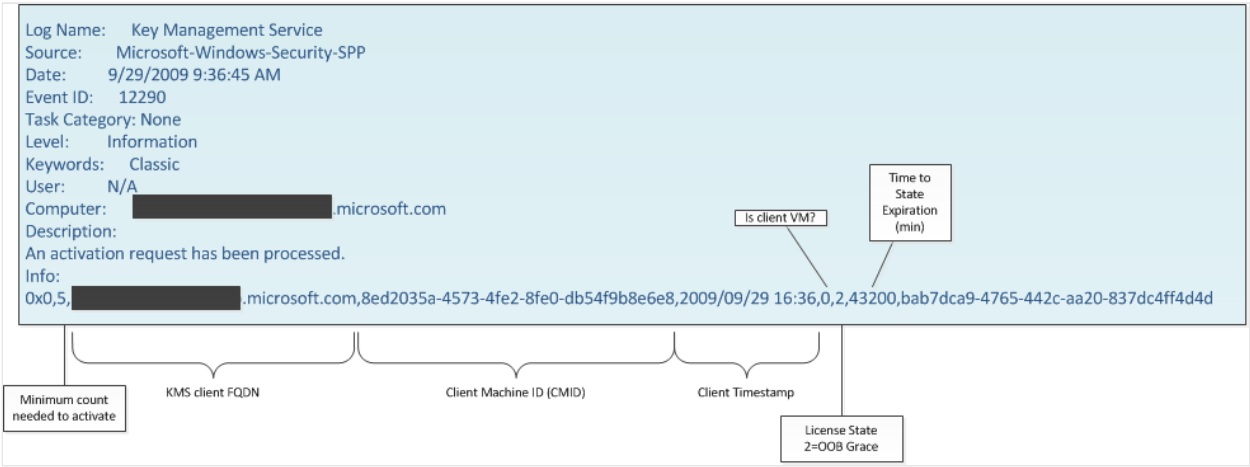
The *Requests with License Status* lines describe all possible license states, past and present. From a troubleshooting perspective, this data is relevant only if the count isn't increasing as expected. In that case, you should see the number of failed requests increasing. To resolve this issue, you should check the product key that was used to first activate the KMS host system. Also, notice that the cumulative request values reset only if you reinstall the KMS host system.

Useful KMS host events

The event IDs described in the following sections are ones you should become familiar with to make troubleshooting host-related issues more efficient.

Event ID 12290

The KMS host creates a log labeled *Event ID 12290* when a KMS client contacts the host when it's trying to activate. Event ID 12290 contains information you can use to figure out what kind of client contacted the host and why a failure occurred. The following segment of an event ID 12290 entry comes from the Key Management Service event log of our KMS host.



The event details include the following information:

- The *Minimum count needed to activate*, which reports that the count from the KMS host must be **5** in order for the client to activate. That means that this OS is a Windows Server OS, although this variable alone doesn't indicate which edition the client is using. If your clients aren't activating, make sure that the host's count allows the client to activate.
- The *Client Machine ID (CMID)*, which is a unique value on each system. If this value isn't unique, it's because the image wasn't correctly configured for distribution using sysprep. To learn more about generalizing your computers, see Sysprep (Generalize) a Windows installation. When you encounter this issue, the KMS host count doesn't increase even though there are enough clients in the environment. For more information, see The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network.
- The *License State and Time to State Expiration*, which is the current license state of the client. This variable can help you tell whether a client is trying to activate for the first time or if it's trying to reactivate. The time entry can also tell you how long the client remains in that state if nothing else changes.

If you're troubleshooting a client and can't find a corresponding event ID 12290 on the KMS host, then the client isn't connecting to the KMS host. Reasons why the event ID 12290 entry is missing can include:

- There's been a network outage.
- The host isn't resolving or isn't registered in DNS.
- The firewall is blocking TCP 1688.
  - The port could also be blocked in other places within the environment, including on the KMS host system itself. By default, the KMS host has a firewall exception for KMS, but this exception isn't automatically enabled. You have to enable the exception manually.
- The event log is full.

KMS clients log two corresponding events: event ID 12288 and event ID 12289. For information about these events, see the KMS client section.

Event ID 12293

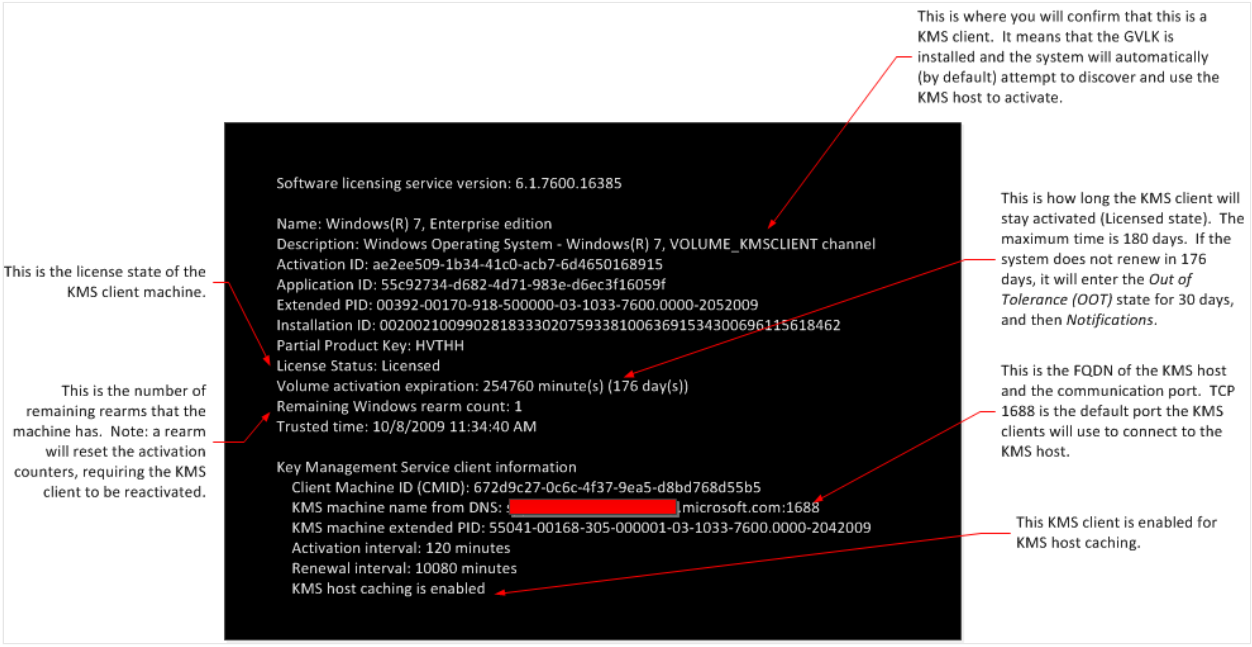
Another relevant event to look for on your KMS host is *Event ID 12293*. This event indicates that the host didn't publish the required records in DNS. This scenario can potentially cause failures, and you should make sure the event isn't there after you set up your host and before you deploy clients. For more information about DNS issues, see Common troubleshooting procedures for KMS and DNS issues.

KMS client

You can also use the `slmgr.vbs` command and Event Viewer to troubleshoot activation on the KMS clients.

Slmgr.vbs and the Software Licensing service

To see verbose output from the Software Licensing service, open an elevated Command Prompt window and enter `slmgr.vbs /dlv` at the command prompt. The following screenshot shows the results of this command on one of our KMS hosts within Microsoft.



Here are some variables you should pay attention to in the output while troubleshooting:

- *Name*, which tells you which edition of Windows the KMS client system is using. You can use this variable to verify that the version of Windows you're trying to activate is compatible with KMS.
- *Description*, which shows you which key was installed. For example, `VOLUME_KMSCLIENT` indicates that the system has installed the KMS Client Setup Key, or GVLK, which is the default configuration for volume license media. A system with a GVLK automatically tries to activate by using a KMS host. If you see a different value here, such as MAK, you must reinstall the GVLK to configure this system as a KMS client. You can manually install the key by following the instructions to run `slmgr.vbs /ipk <GVLK>` in KMS client setup keys, or follow the directions in Volume Activation Management Tool (VAMT) Technical Reference to use the VAMT instead.

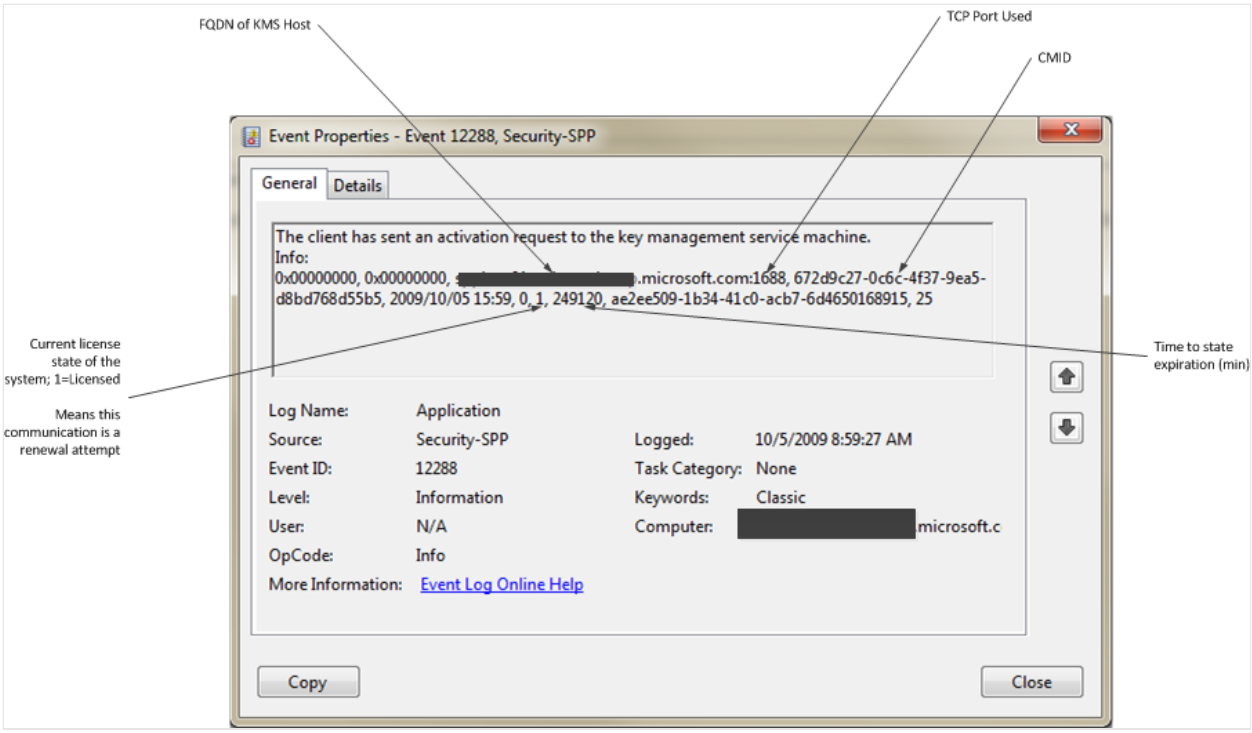
- The *Partial Product Key*, which you can use to determine whether the KMS Client Setup Key matches the operating system the KMS client is using. By default, the correct key is present on systems that are built using media from the Volume License Service Center (VLSC) portal. In some cases, customers may use Multiple Activation Key (MAK) activation until there are enough systems in the environment to support KMS activation. You must install the KMS Client Setup key on these systems to transition them from MAK to KMS. Use VAMT to install this key and make sure you're using the correct key.
- *License Status* shows the status of the KMS client system. For a system activated by KMS, this value should be **Licensed**. Any other value may indicate that there's a problem. For example, if the KMS host is functioning correctly and the KMS client still doesn't activate or is stuck in a **Grace** state, that means something is preventing the client from reaching the host system. This blockage can be a firewall issue, network outage, and so on.
- The *Client Machine ID (CMID)*, which should be unique in every KMS client. As mentioned in Check the Software Licensing service using the slmgr.vbs command, a common issue related to count is if the count doesn't increase beyond one no matter how many KMS hosts or clients you activate in the environment. For more information, see The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network.
- The *KMS Machine Name from DNS*, which shows both the FQDN of the KMS host that the client successfully used for activation and which TCP port it used to communicate.
- *KMS Host Caching*, which shows whether or not caching is enabled. Caching is typically enabled by default. When you enable caching, the KMS client caches the same KMS host that it used for activation and communicates directly with this host instead of querying DNS when it's time to reactivate. If the client can't contact the cached KMS host, it queries DNS to discover a new KMS host.

KMS client events

The following sections describe client events that you should be familiar with to help you troubleshoot potential issues more efficiently.

Event ID 12288 and Event ID 12289

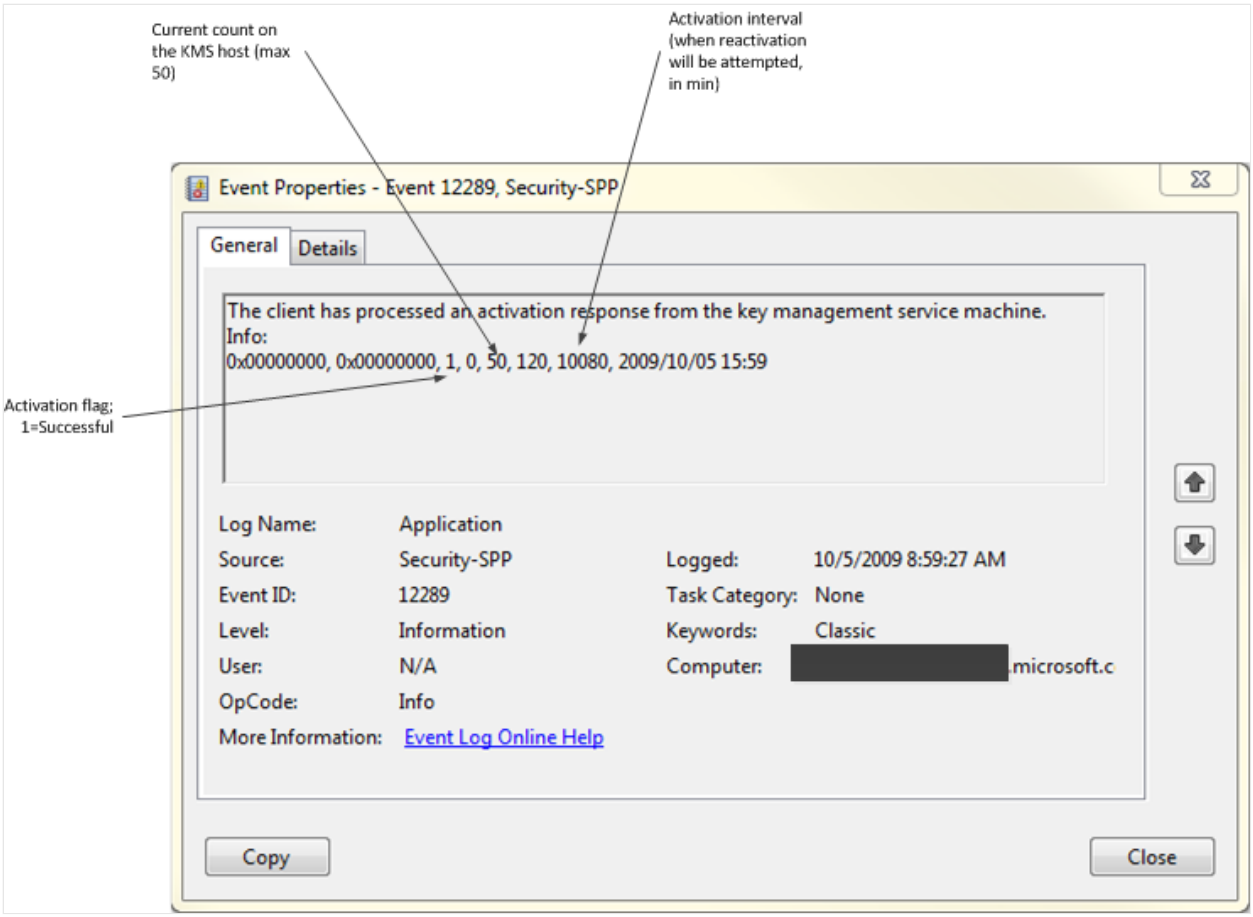
When a KMS client successfully activates or reactivates, the client logs two events: event ID 12288 and event ID 12289. The following screenshot showing a segment of an event ID 12288 entry comes from the Key Management Service event log of our KMS client.



If you see only event ID 12288 without a corresponding event ID 12289, either the KMS client couldn't reach the KMS host, the KMS host didn't respond, or the client didn't receive the host's response. In these cases, you must verify that the KMS host is discoverable and that the KMS clients can contact it.

The most relevant information in event ID 12288 is the data in the *Info* field. For example, Info shows the current state of the client and which FQDN and TCP port the client used when it tried to activate. You can use the FQDN to troubleshoot scenarios where the count on a KMS host doesn't increase. For example, if there are too many KMS hosts available to the clients (either legitimate or unsupported systems), then the count may be distributed over all of them.

An unsuccessful activation doesn't always mean that the client has event ID 12288 and not 12289. A failed activation or reactivation may also have both events. In this case, you have to examine the second event to verify the reason for the failure.



The Info section of event ID 12289 provides the following information:

- *Activation Flag*, which indicates whether the activation succeeded (**1**) or failed (**0**).
- *Current Count on the KMS Host*, which shows the count value on the KMS host when the client tries to activate. If activation fails, it may be because the count is insufficient for this client OS or that there aren't enough systems in the environment to build the count.

What does support ask for?

If your activations aren't working as expected after troubleshooting, you can contact Microsoft Support for technical assistance. The Support Engineer typically asks for the following information:

- `slmgr.vbs /dlv` output from the KMS host and KMS client systems.
- Event logs from both the KMS host (Key Management Service log) and KMS client systems (Application log).

Next steps

- Ask the Core Team: #Activation