Basic - Day 1, Day 2

Tuesday, June 16, 2020 12:08 PM

Retail and OEM activation - Day 1

Wednesday, June 10, 2020 9:40 AM

Retail activations

The retail activation method has not changed in several versions of Windows and Windows Server. Each purchased copy comes with one unique product key (often referred to as a retail key). The user enters this key during product installation. The computer uses this retail key to complete the activati on after the installation is complete. Most activations are performed online, but telephone activation is also available. Recently, retail keys have been expanded into new distribution scenarios. Product key cards are available to activate products that have been preinstalled or downloaded. Programs such as Windows Anytime Upgrade and Get Genuine allow users to a cquire legal keys separately from the software. These electronically distributed keys may come with media that contains software, they can come as a software shipment, or th ey may be provided on a printed card or electronic copy. Products are activated the same way with any of these retail keys.

Original Equipment Manufacturer （OEM)

Most original equipment manufacturers (OEMs) sell systems that include a standard build of the Windows operating system. The hardware vendor activates Windows by associating the operating system with the firmware (BIOS) of the computer. This occurs before the computer is sent to the customer, and no ad ditional actions are required. OEM activation is valid as long as the customer uses the OEM-provided image on the system. OEM activation is available only for computers that are purchased through OEM channels and have the Windows operating system preinstalled.

Windows Product Key embedded by the OEM in BIOS
Command to get the OEM key **C:\windows\system32\wmic path SoftwareLicensingService get OA3xOriginalProductKey**

Bug: the kms client switch from enterprise to pro version automatically:
Install enterprise GVLK on a system with no KMS available. Have a Professional OEM:DM key in the MSDM table. After the proactive troubleshooter runs, it will change to pro edition. It affects the users machine who use GVLK but do not have a KMS server available immediately and the user's machines which are d isconnected from their corporate network for too long. The issue was observed in 1809, but not in previous OS. There's something changed in the binary clipsvc.dll.

The workaround is to use the command "SLMGR /ipk <product key>" to reinstall the enterprise KMS client key, and then run "slm gr /ato" to reactivate the machine to enterprise version.

Additionally, Microsoft has release the fix: https://support.microsoft.com/en-us/help/4490481/windows-10-update-kb4490481

Reference: https://docs.microsoft.com/en-us/windows/deployment/volume-activation/plan-for-volume-activation-client>

Volume Activation - Day 1, Day 2

Wednesday, June 10, 2020 9:39 AM

MAK

Monday, June 15, 2020 3:05 PM

Multiple Activation Key

A Multiple Activation Key (MAK) is commonly used in small- or mid-sized organizations that have a volume licensing agreement, but they do not meet the requirements to operate a KMS or they prefer a simpler approach. A MAK also allows permanent activation of computers that are isolated from the KMS or are part of an isolated network that does not have enough computers to use the KMS.
To use a MAK, the computers to be activated must have a MAK installed. The MAK is used for one-time activation with the Microsoft online hosted activation services, by telephone, or by using VAMT proxy activation. In the simplest terms, a MAK acts like a retail key, except that a MAK is valid for activating multiple computers. Each MAK can be used a specific number of times. The VAMT can assist in tracking the number of activations that have been performed with each key and how many remain.
Organizations can download MAK and KMS keys from the Volume Licensing Service Center website. Each MAK has a preset number of activations, which are based on a percentage of the count of licenses the organization purchases; however, you can increase the number of activations that are available with your MAK by calling Microsoft.

Multiple Activation Key Activation

MAKs are installed on each volume-licensed computer that will activate with a Microsoft server, either over the Internet or by contacting a Microsoft call center. They can be installed on individual computers or can be included in an image that can be bulk-duplicated or provided for download using Windows Deployment Services (WDS).
Batch activation is supported for one-time MAK activation of a large number of computers. Activations for computers that activate with Microsoft do not expire (unlike KMS Activation).
MAKs should be used for computers that are rarely or never able to connect to the organization's network. A MAK can be installed on a computer that was set up to use KMS, but risks expiration of its grace period. Pop-up notifications are presented to the user with increasing frequency as the computer nears the end of its grace period.

Steps for Configuring and Deploying MAK Activation

To configure and deploy MAK activation, complete one of the following tasks:

- Optional: Enable Standard User MAK Activation
- Configure a volume-licensed edition to use MAK Activation

To activate a computer manually using MAK activation, complete one of the following tasks:

- Manual MAK Activation over the Internet
- Manual MAK Activation by Telephone with Script

To activate if interactive logon has been disabled (end of grace period), complete the following task:

- MAK Activation if Interactive Logon is Disabled

Optional: Enable Standard User MAK Activation

An optional registry key can be created by an administrator to allow a standard user to apply MAK keys and activate computers. This should be carefully considered, because it does loosen security by allowing standard users the ability to change licensing status of the computer. Apply this change only with the understanding of this risk.

Once this change has been made, ignore all comments in the MAK activation section regarding administrator privileges, unless they explicitly state that the standard user mode does not allow access to the function.

To enable standard user MAK activation:

1. On the client computer, create the following registry key using RegEdit.exe:

   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL
2. Within this new subkey, add the following:

   Value Name: **UserOperations**

   Type: **DWORD**

   Value Data: **1**

   This allows standard users to:

- Assign a MAK to a KMS client
- Replace another MAK
- Manually activate the computer

Note:	When a standard user changes a VLK 2.0 product key, the ProductID registry values are not updated. This primarily affects pro duct support, but there could be other unanticipated side effects. Microsoft support personnel should be aware of this and should use another method to determine the activation method.

Configure Volume-licensed Edition for MAK Activation

Configure a volume-licensed edition to use MAK Activation with the following procedures:

- Using the Windows interface
- Using a script

These procedures also apply to systems previously configured for KMS Activation, which are at risk of reaching the end of their activation expiration or initial grace period.

Note:	When a MAK is installed for the first time, it begins a new 30-day grace period for activation. However, in cases where systems configured to use KMS are changed to use MAK, no new 30-day grace period is given.

To configure a volume-licensed edition for MAK Activation, using the Windows interface:

1. Install Windows Vista with the desired volume licensed media.
2. Do not supply a product key during setup.
3. Boot and log on as a user with administrative privileges.
4. Load the System Properties control-panel applet:

   Click **Start**, right-click **Computer**, and then select **Properties**.
5. In the **Activation** section, click **Change product key**.
6. User Access Control (UAC) prompts for permission; click **Continue**.
7. In the **Change your product key for activation** window, enter the MAK.
8. The computer attempts to activate over the Internet; the next screen indicates success or failure (usually due to network connectivity).
9. If activation fails, the computer automatically retries (the user does not need to be an administrator for automatic activations).

10. Optional: To disable automatic activation attempts:
    - Use RegEdit.exe to edit the following registry subkey:

      HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual
    - Change the value of this subkey to **1**

To configure a volume-licensed edition for MAK Activation, using a script:

1. Install Windows Vista with the desired volume licensed media.
2. Do not supply a product key during setup.
3. Boot and log on as a user with administrative privileges.
4. Open a Command Prompt window (with elevated privileges if not running as an administrator).
5. Run the following script, using the MAK:

   cscript \windows\system32\slmgr.vbs -ipk <Multiple Activation Key>
6. The computer attempts to activate over the Internet per the next scheduled interval.
7. Optional: To activate immediately, follow the **To activate manually over the Internet, using MAK and a script** procedure.
8. If activation fails, the computer automatically retries (user does not need to be an administrator for automatic activations).
9. Optional: To disable automatic activation attempts:
   a. Use RegEdit.exe to edit the following registry subkey:

      HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual
   b. Change the value of this subkey to **1**.

Manual MAK Activation Over the Internet

A computer using MAK Activation can be activated with the following procedures:

- Using the Windows interface
- Using a script

To activate manually over the Internet, using MAK and the Windows interface:

1. Start the System Properties applet from the Welcome Center or from the Control Panel; if UAC prompts for permission, click **Allow**.
2. Select **Click here to activate Windows now** to start the Activation wizard; if UAC prompts for permission, click **Allow**.
3. If the computer has access to the Internet and is able to activate, Windows reports **Activation was successful**.
4. If activation fails, the wizard reports the failure, and presents additional options, including the option to activate by telephone.

To activate manually over the Internet, using MAK and a script:

1. Open a Command Prompt window (with elevated privileges if not running as an administrator).
2. Run this script to activate; it reports success or failure with a result code:

   cscript \windows\system32\slmgr.vbs –ato

Manual MAK Activation by Telephone with Remote Script

Administrators can use this procedure to activate computers connected to their organization's network but not connected to the Internet, or whose users do not have administrative privileges.

If this procedure will be used frequently or for multiple target computers, it may be useful to adapt the built-in script Slmgr.vbs to automate the process.

To activate manually over the telephone, with MAK and a remote script:

1. Open a Command Prompt window (with elevated privileges if not running as Administrator).
2. To enable copying from the Command Prompt window using mouse selection and the ENTER key, ensure that the QuickEdit Mode edit option is set.
3. Obtain the Installation ID from the target system using the following script:

   cscript \windows\system32\slmgr.vbs *<Computer> <User> <Password>* **–dli**
4. The script displays several sections of license information, grouped by Product ID; the section that lists the last five characters of the MAK in **Partial Product Key** includes the Product ID and Installation ID required for phone activation.
5. Save the Product ID and Installation ID values.
6. Use the SET command to retrieve the %COMPUTERNAME% value.
7. Save the %COMPUTERNAME% value.
8. Call the automated phone system for the region; telephone numbers can be obtained through the **Find available phone numbers for activation** wizard, in the Software Licensing User Interface (Slui.exe); to access, run the following command:

   slui.exe 4
9. Use the Interactive Voice Response system to obtain the Confirmation ID for the target computer.
10. Provide the corresponding Installation ID from the activating computer when prompted.
11. Activate the target computer (%computername%) by installing the Confirmation ID with this script:

    cscript \windows\system32\slmgr.vbs *<Computer> <User> <Password>* **–atp** *<Product ID> <Confirmation ID>*

MAK Activation If Interactive Logon Is Disabled

Install a MAK and activate a computer if interactive logon has been disabled using the following procedures:

- Using the Windows interface
- Using a script

If a computer has reached the end of its 30-day grace period without activating, interactive logons are disabled. All other computer functions are available, and limitedfunctionality is provided through the Slui.exe, to support recovery by an Administrator.

Procedures in this section apply in the following situations; installation of a MAK in this state may be required, depending on circumstances:

- The initial grace period has expired.
- The computer's hardware was changed significantly and the subsequent 30-day grace period has expired.
- The computer was configured for KMS, but is unable to connect with a KMS computer and has reached the end of its grace period.
- The computer was configured for MAK, but the MAK is no longer valid (the allowed number of activations might have been exceeded, or the key might have been stolen and blocked from further activations).

To activate if interactive logon is disabled, using MAK and the Windows interface:

1. If the activation period has expired, the Activate Windows Now wizard provides options to support changing product keys and activate the computer.
2. Select the appropriate option in order to install a MAK; options include:
   a. **Activate Windows online now**
   b. **Activate using the automated telephone system**

c. **Buy a new product key online** (after entering a new MAK if there is an existing Internet connection) - Although this option is not intended for volume licensing customers, it can be used to set a proxy in the browser if activation is failing due to a network configuration problem:

   i. In Microsoft Internet Explorer®, on the **Tools** menu, click **Internet Options**, and then click **Connections**.

   ii. Choose the appropriate connection method.

   iii. Select the **Settings** button to set the Proxy server.

d. **Retype the product key** - Use this option to enter a new MAK, and then choose the Activate Windows Online option

e. **Show me other ways to activate** - Use this option after entering new MAK to activate with a modem, or to use the automated telephone system

To activate if interactive logon is disabled, using MAK and a script:

1. This method can only be run remotely by an administrator and assumes that necessary services are operational and ports are open.
2. Use the procedure **Manual MAK activation by Telephone with Remote Script**.

MAK Activation Using Batch

Batch MAK activation is intended to provide a cost-effective, batched, Internet-based activation alternative to telephone activation. This enables customers to activate large numbers of connected client computers, and support scenarios where client computers are disconnected, and only another centrally located computer has access to the Internet for activation through Microsoft.

(Batch activation procedures will be added to this lesson when they become available.)

KMS

Monday, June 15, 2020 3:05 PM

How Key Management Service works

KMS uses a client–server topology. KMS client computers can loca
te KMS host computers by using DNS or a static configuration. KMS clients contact the KMS host by using RPCs carried over TCP/IP. A single KMS host can support an unlimited number of KMS clients.

Key Management Service activation thresholds

KMS clients will be activated only after this threshold has been met.

KMS client operating system versions(Win10, Win8.1, Win7), must receive an activation count of 25 or more.
KMS server operating system versions(Win Server 2019, 2016, 2012 R2, 2012 etc.), receives an activation count that is 5 or more.

Key Management Service activation renewal

KMS activations are valid for 180 days (the *activation validity interval*). To remain activated, KMS client computers must renew their activation by connecting to the KMS host at least once every 180 days. By default, KMS client computers attempt to renew their activation every 7 days. If KMS activation fails, the client computer retries every two hours. After a client computer's activation is renewed, the activation validity interval begins again.

Key Management Service connectivity

KMS activation requires TCP/IP connectivity. By default, KMS hosts and clients use DNS to publish and find the KMS. By default, client computers connect to the KMS host for activation by using RPCs through TCP port 1688. (You can change the default port.)

Activating subsequent Key Management Service hosts

Each KMS key can be installed on up to six KMS hosts. These hosts can be physical computers or virtual machines. After activating a KMS host, the same host can be reactivated up to nine times with the same key. If the organization needs more than six KMS hosts, you can request additional activations for your organization's KMS key by calling a Microsoft Volume Licensing Activation Center to request an exception.

KMS cli*ent setup k*eys

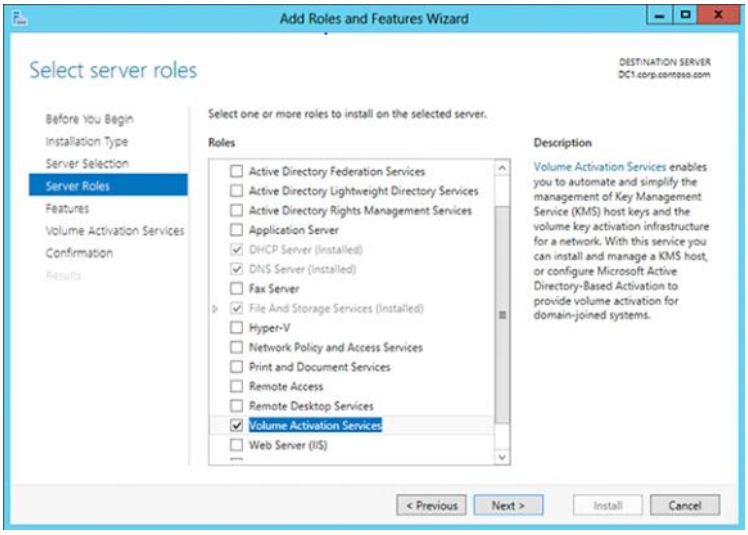
https://docs.microsoft.com/en-us/windows-server/get-started/kmsclientkeys

KMS host key is backwards compatible. Depending on which operating system your KMS server is running and which operating systems we want to activate, we might need to install prerequisite updates.
https://docs.microsoft.com/en-us/windows-server/get-started-19/activation-19

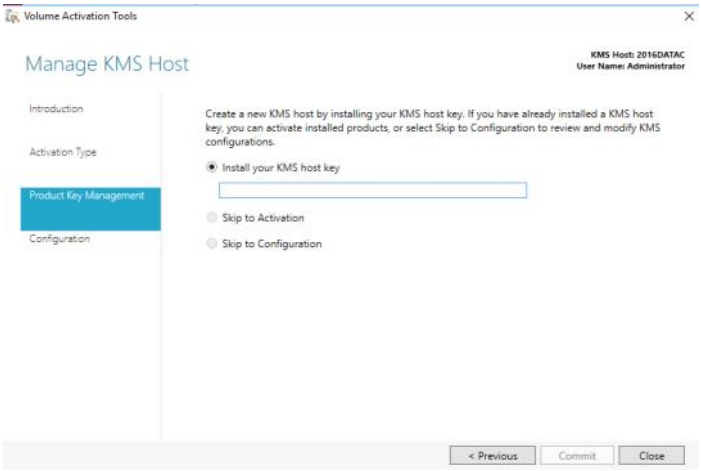
How to setup a KMS host

It would look like the steps in the article below:

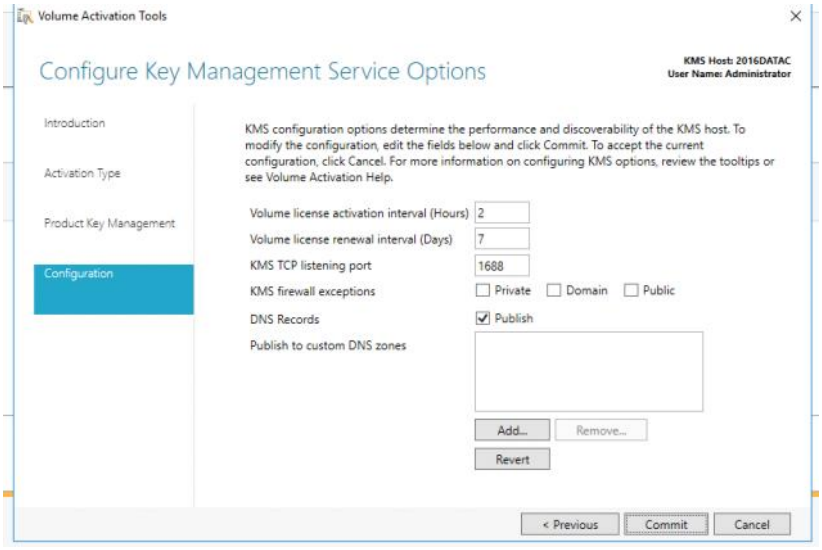
Configuring KMS hosts in Windows Server 2012 R2:
https://docs.microsoft.com/en-us/windows/deployment/volume-activation/activate-using-key-management-service-vamt#key-management-service-in-windows-server2012r2
Deploy KMS Activation | Microsoft Docs



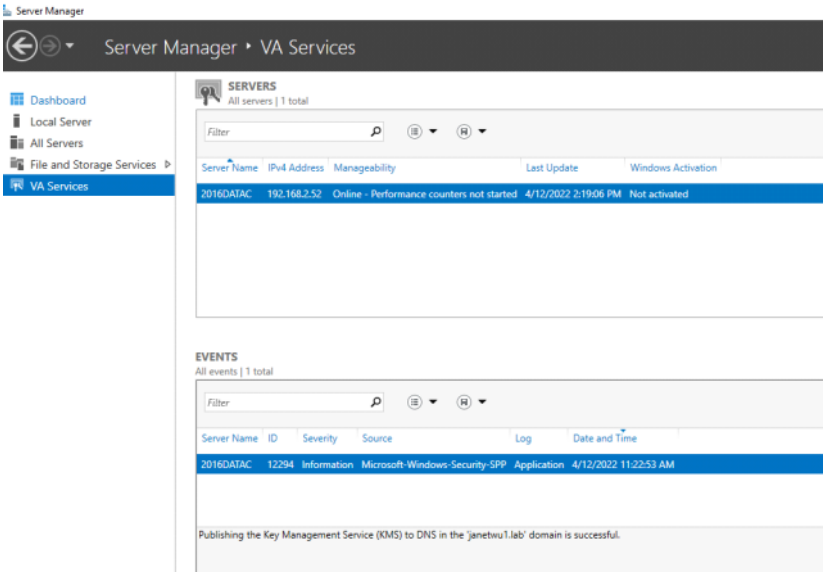
After the role installed successfully, we can open Volume Activation Tools from Server Manager or vmw.exe command



Regarding KMS SRV record: We will have KMS SRV records publish option when setup KMS. It is currently by design that the KMS server will **only publish the SRV RR when it is first installed** and not each time the SPPSVC service or the computer starts up.

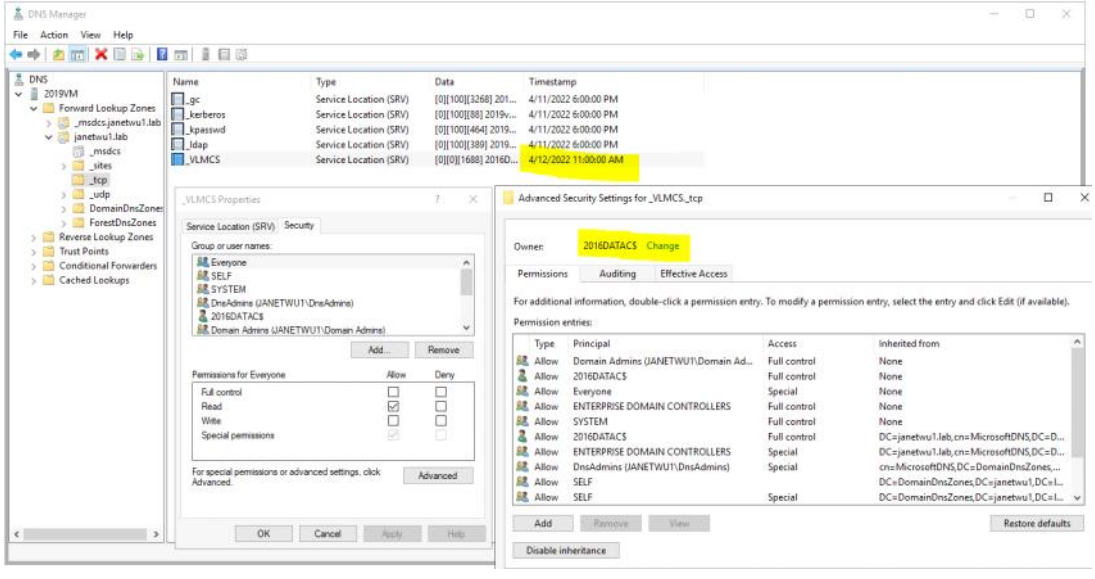


Event ID 12294 indicates that the KMS host successfully created the SRV RRs. Event ID 12293 indicates that the attempt to create the SRV RRs was unsuccessful. it is currently by design that the KMS server will only publish the SRV RR when it is first installed and not each time the SPPSVC service or the computer starts up.

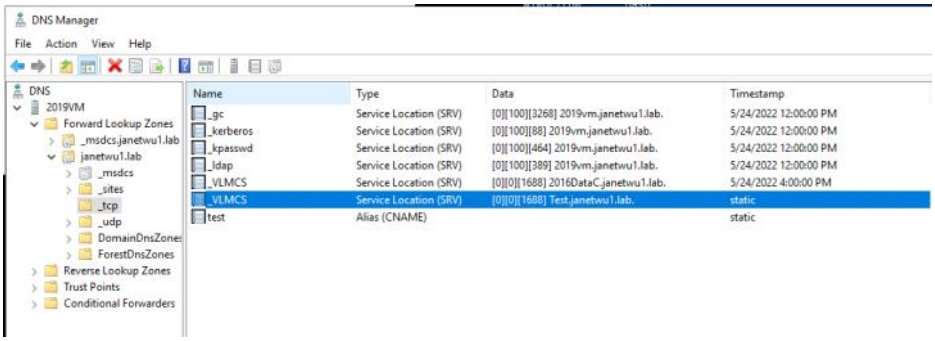


On DNS Server, open DNS Manger console, we will see the SRV record as below. The owner of the SRV record is the KMS host machine name. We can see the of the SRV if this is published from KMS host automatically. If we manually create a SRV, we will see Static in Timestamp column.

Automatic KMS SRV:

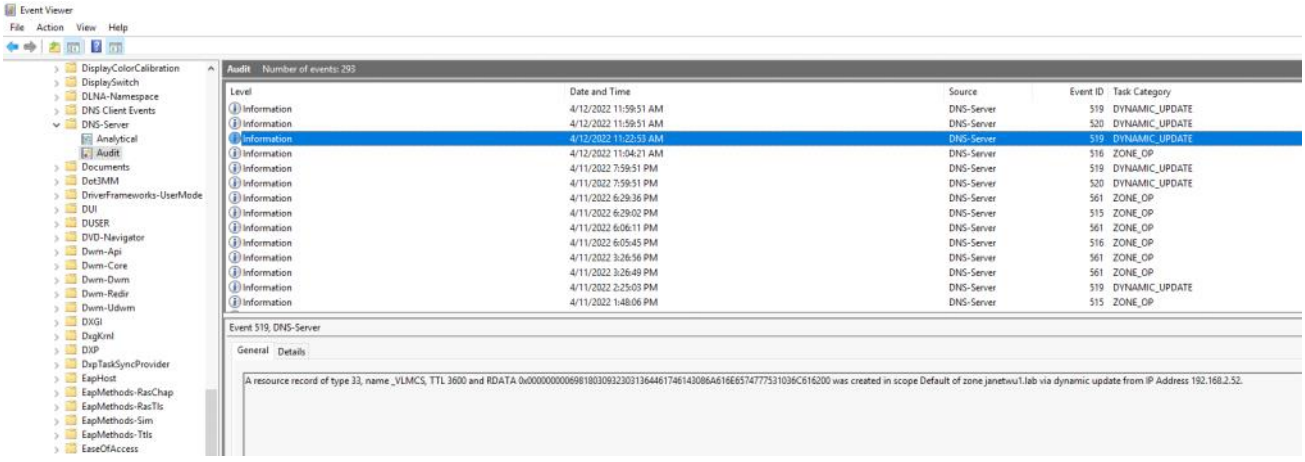


Manually KMS SRV:

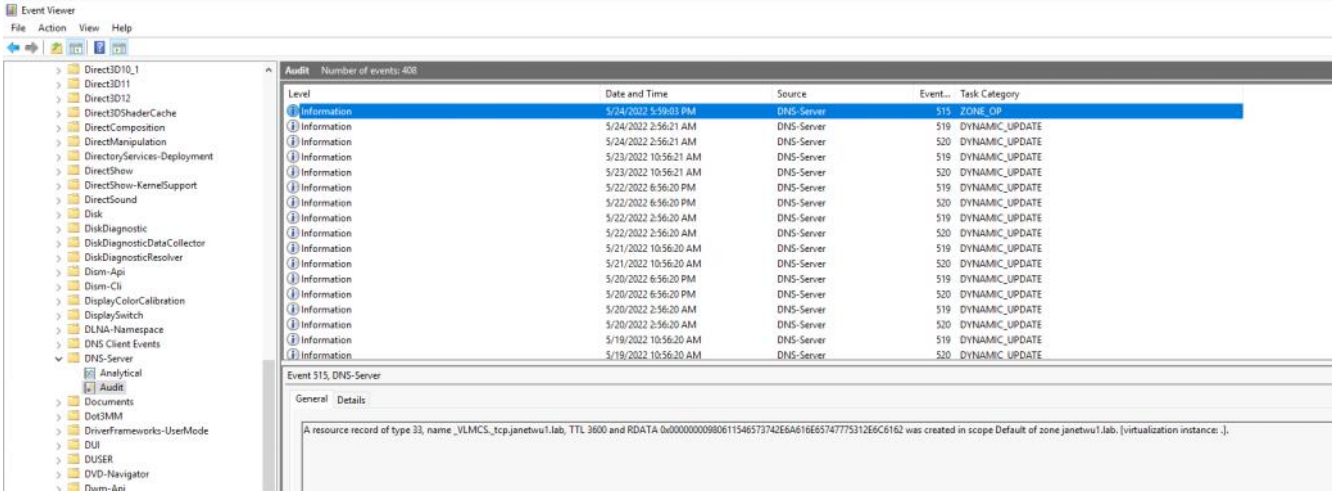


On DNS server event log(Event Viewer\Applications and Services Logs\Microsoft\Windows\DNS-Server):

Automatic KMS SRV:



Manually KMS SRV



On KMS client:

- Verify if the correct KMS server can be resolved correctly:
  nslookup -type=srv _vlmcs._tcp
- Verify if the KMS can be contacted:
  telnet <KMS FQDN or IP> 1688

Guidelines for troubleshooting the Key Management Service (KMS)
https://docs.microsoft.com/en-us/windows-server/get-started/activation-troubleshoot-kms-general

Logs:

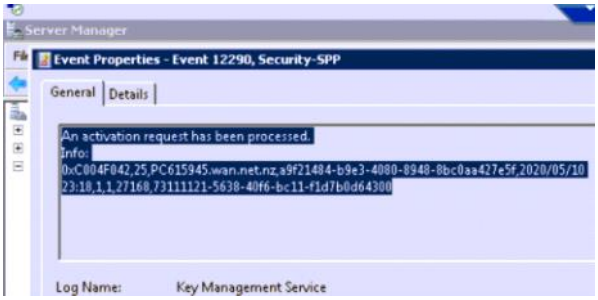
Most licensing actions and events are recorded in the Event log (ex: Application Log events 12288-12290).
The client establishes a TCP session with the KMS, and sends a single request packet. The KMS responds and the session is closed. The same type of request-response is used for activation requests and renewal requests.
Both requests and responses are logged by the client in the Application Event Log, as Microsoft-Windows-Security-SPP events 12288 and 12289, respectively. For example:

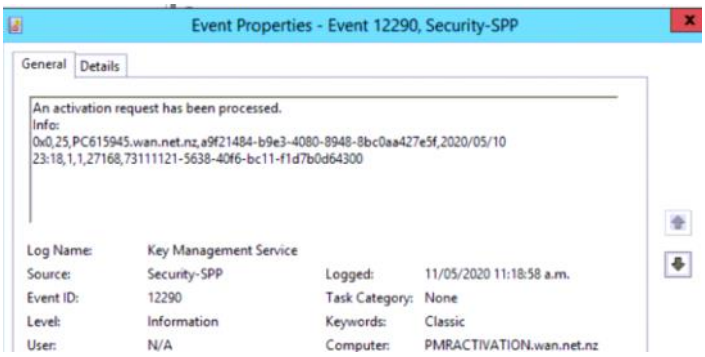
Log Name: Application
Source: Microsoft-Windows-Security-SPP
Date: 7/6/2018 1:42:32 AM
Event ID: 12288
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: WIN-1K3KQ62QL7P
Description:
The client has sent an activation request to the key management service machine.

Info:
0xC004F06C, 0x00000000, 84.25.14.16:1688, de29b964-6219-4114-88c6-49942d8c9607, 2018/07/05 17:42, 1, 2, 37680, 620e2b3d-09e7-42fd-802a-17a13652fe7a, 5

KMS logs requests it has received from all clients as Microsoft-Windows-Security-SPP event 12290. Note that this KMS event is located in the Applications and Services Logs\Key Management Service event log. For example:

信息	7/5/2018 10:42	Microsoft-Windows-Security-SPP	12290	无	已处理了激活请求。 信息: 0xC004F06C,5,WIN-1K3KQ62QL7P,de29b964-6219-4114-88c6-49942d8c9607,2018/07/05 17:42,1,2,37680,620e2b3d-09e7-42fd-802a-17a13652fe7a





ADBA

Monday, June 15, 2020 3:07 PM

ADBA provides a way to activate these products if the computers can join the company's domain. When the user joins their computer to the domain, the ADBA object automatically activates Windows installed on their computer, as long as the computer has a Generic Volume License Key (GVLK) installed. No single physical computer is required to act as the activation object, because it is distributed throughout the domain.

Active Directory-Based Activation Overview
https://docs.microsoft.com/en-us/windows/deployment/volume-activation/active-directory-based-activation-overview

Step-by-step configuration: Active Directory-based activation
https://docs.microsoft.com/en-us/windows/deployment/volume-activation/activate-using-active-directory-based-activation-client#step-by-step-configuration-active-directory-based-activation

The difference between ADBA and KMS as below:

KMS:

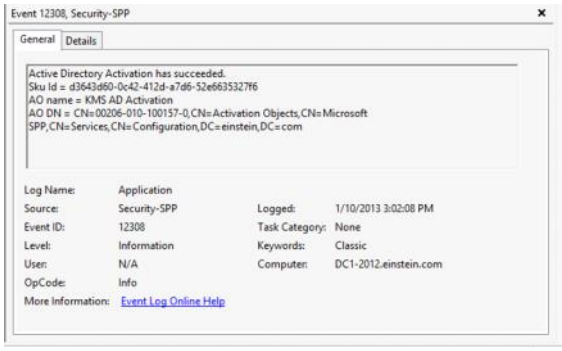
- A minimum number of qualifying computers (activation threshold)
- Support Windows 7, Windows Server 2008 R2 and later OS activation
- KMS clients contact the KMS host by using RPCs carried over TCP/IP, RPC 1688 TCP port used with KMS.

ADBA

- No thresholds, any domain-joined computers running a supported operating system with a Generic Volume License Key (GVLK) will be activated automatically and transparently
- It only works with Windows 8, Windows Server 2012, and later and it is forest wide, can activate domain-joined computers only
- No TCP 1688 (KMS) is used, but default LDAP instead

Active Directory-Based Activation vs. Key Management Services
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/active-directory-based-activation-vs-key-management-services/ba-p/256016

Troubleshooting Active Directory Based Activation (ADBA) clients that do not activate
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/troubleshooting-active-directory-based-activation-adba-clients/ba-p/259504



Basic - Day 3, Day 4

Tuesday, June 16, 2020 12:09 PM

ESU License and Activation - Day 3

Wednesday, June 10, 2020 10:04 AM

Obtaining Extended Security Updates for eligible Windows devices - Microsoft Tech Community

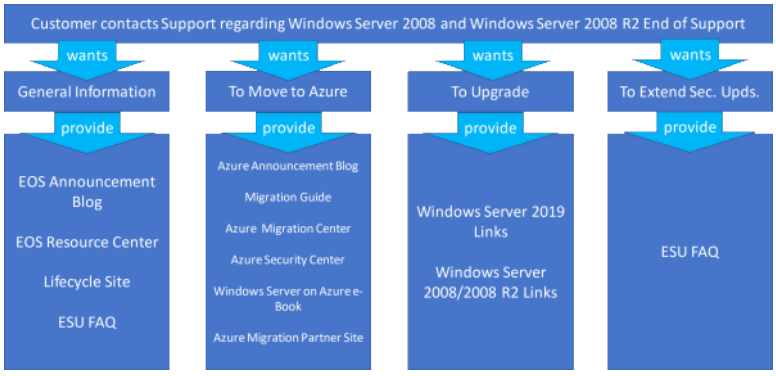
Background:

Windows server 2008 SP2/ Windows Server 2008 R2 /Windows 7 reach the end of support on 1/14/2020.

In this case, we have three options can provide for customer. Please see attached file to get more details.

- Move to Azure
- To Upgrade
- To Extend Security Updates

New Options for Windo...



ESU Activation:

To get ESU, we need to perform ESU activation for windows 7/windows server 2008r2.

Below is the detailed steps for you to activate ESU MAK key.

Purchasing Extended Security Updates through Volume Licensing

Now, Is walket' through where to purchase Windows 7 ESUs, and how to find the appropriate key on the Volume Licensing Service Center.

Extended Security Updates are available through specific Microsoft Volume Licensing programs. Coverage is available in three consecutive 12-month increments beginning January 14, 2020. Extended Security updates are available for purchase in 12-month increments only. You cannot buy partial periods (e.g. 6 months of updates).

1. Visit the Volume Licensing Service Center and sign in using your company's credentials.
2. Select **Licenses** > **Relationship Summary** > **Licensing ID** > **Product Keys**.

Purchasing Windows 7 ESUs through a Cloud Solution Provider (CSP)

Windows 7 ESUs are also available via the Cloud Solution Partner (CSP) program. To purchase Windows 7 ESUs through a CSP, contact one of the CSP partners listed in the Microsoft solution provider database. If you are a partner and need details on procuring Windows 7 ESUs through the Partner Center, see Purchasing Windows 7 ESUs as a Cloud Solution Provider.

Installation prerequisites

Note: The prerequisites listed in this section will be updated as needed.

The following steps must be completed before installing and activating ESU keys:

1. Install the following SHA-2 code signing support update and the following servicing stack update (SSU):

   Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1:
   Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1: March 12, 2019 (KB4490628)
   and
   SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019 (KB4474419)

Windows Server 2008 Service Pack 2 (SP2):
Servicing stack update for Windows Server 2008 SP2: April 9, 2019 (KB4493730)
and
SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019 (KB4474419)

2. Install the SSU listed below (or a later SSU) and the ESU licensing preparation package:

Windows 7 SP1 and Windows Server 2008 R2 SP1
Servicing stack update for Windows 7 SP1 and Server 2008 R2 SP1: May 12, 2020 (KB4555449) ***or later***
and
Extended Security Updates (ESU) Licensing Preparation Package (KB4538483)

Windows Server 2008 SP2:
Servicing stack update for Windows Server 2008 SP2: May 12, 2020 (KB4555448) ***or later***
and
Extended Security Updates (ESU) Licensing Preparation Package (KB4538484)

Note: Once a servicing stack update is installed, it cannot be removed or uninstalled from the machine. For more information, see Servicing stack updates.

Note: Classified as a Security-only package, the ESU licensing preparation package is available via Windows Server Update Services (WSUS) or the Microsoft Update Catalog. The ESU licensing preparation package is not currently available via Windows Update.

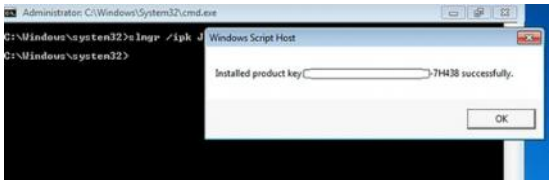
Installation and activation

Once you have installed the prerequisites listed above, you're ready to install and activate the ESU license key.

Note: Installing the ESU product key will not replace the existing Windows OS product key on the device.

First, install the ESU product key using the Windows Software Licensing Management Tool (slmgr). Then:

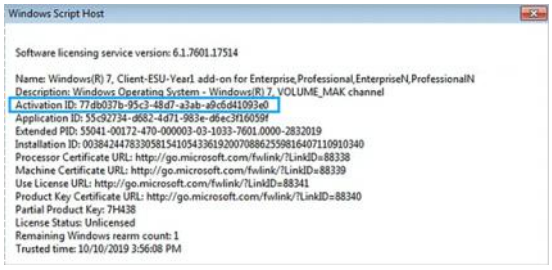
1. Open an elevated Command Prompt.
2. Type **slmgr /ipk *<ESU key>*** and select **Enter**.
3. If the product key is installed successfully, you will see a message similar to the following:



Note: If you see the Error:0xC004F050 while trying to install the product key on Windows Server 2008 SP2, your device may require an additional reboot.

Next, find the ESU Activation ID:

1. In the elevated Command Prompt, type **slmgr /dlv** and select **Enter**.
2. Note the **Activation ID** as you will need it in the next step.



Once the ESU key is activated, continue to use your current update and servicing strategy to deploy ESUs through Windows Update, WSUS, the Microsoft Update Catalog, or whichever patch management solution you prefer. Extended Security Updates will have the Security-only update classification.

Note: Windows Update offline scan files (WSUSScn2.cab) will continue to be available for Windows 7 SP1, Windows Server 2008 R2 SP1, and Windows Server 2008 SP2. If you have devices running one of these operating systems, but don't have ESUs, those devices will show up as non-compliant in your patch management and compliance toolsets.

Configure firewall whitelists for activation

If you are using a proxy firewall, you may need to whitelist the activation endpoints for ESU key activation to succeed.

For online activation (i.e. local key deployment), you will need to whitelist all the following URLs:

Windows 7 SP1 and Windows Server 2008 R2 SP1
https://go.microsoft.com/fwlink/?linkid=88338
https://activation.sls.microsoft.com/slspc/SLActivate.asmx
https://go.microsoft.com/fwlink/?linkid=88339
https://activation.sls.microsoft.com/slrac/SLCertify.asmx
https://go.microsoft.com/fwlink/?linkid=88340
https://activation.sls.microsoft.com/slpkc/SLCertifyProduct.asmx
https://go.microsoft.com/fwlink/?linkid=88341
https://activation.sls.microsoft.com/sllicensing/SLLicense.asmx

Windows Server 2008 SP2
https://go.microsoft.com/fwlink/?linkid=48189
https://activation.sls.microsoft.com/slspc/SLActivate.asmx
https://go.microsoft.com/fwlink/?linkid=48190
https://activation.sls.microsoft.com/slrac/SLCertify.asmx
https://go.microsoft.com/fwlink/?linkid=48191
https://activation.sls.microsoft.com/slpkc/SLCertifyProduct.asmx
https://go.microsoft.com/fwlink/?linkid=48192
https://activation.sls.microsoft.com/sllicensing/SLLicense.asmx

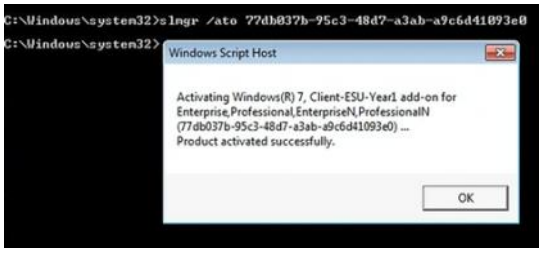
For proxy activation using the Volume Activation Management Tool (VAMT), whitelist the following URLs:

- https://activation.sls.microsoft.com/BatchActivation/BatchActivation.asmx
- http://go.microsoft.com/fwlink/?LinkId=82160 (This FWLink redirects to the above URL.)

Once you have completed your whitelists, you are ready to activate the ESU product key:

1. Open an elevated Command Prompt.
2. Type **slmgr /ato *<ESU Activation Id>*** and select **Enter**.

You should now see a message stating that you have activated the key successfully:



The following table outlines possible values for **<ESU Activation Id>**. The activation IDs are the same across all eligible Windows ESU editions and all devices enrolled for that program

ESU program	ESU SKU (or Activation) ID
Windows 7 SP1 (Client)	
Year 1	77db037b-95c3-48d7-a3ab-a9c6d41093e0
Year 2	0e00c25d-8795-4fb7-9572-3803d91b6880
Year 3	4220f546-f522-46df-8202-4d07afd26454
Windows Server 2008 R2 SP1 and Windows Server 2008 (Server)	
Year 1	553673ed-6ddf-419c-a153-b760283472fd
Year 2	04fa0286-fa74-401e-bbe9-fbfbb158010d
Year 3	16c08c85-0c8b-4009-9b2b-f1f7319e45f9

Important: Activation via **Control Panel** > **System and Security** > **System** > **Activate Windows** cannot be used to activate ESU keys. It activates the Windows operating system only.

Once you have activated the ESU product key, you can verify the status at any time by following these steps:

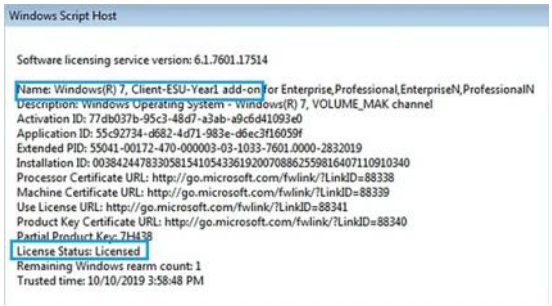
Windows 7 SP1 and Windows Server 2008 R2 SP1:

1. Open an elevated Command Prompt.
2. Type **slmgr /dlv** and select **Enter**.

Windows Server 2008 SP2:

1. Open an elevated Command Prompt.
2. Type **slmgr /dlv <Activation ID>** or **slmgr /dlv all** and select **Enter**.

The **License Status** will show as **Licensed** for the corresponding ESU program, as shown below:



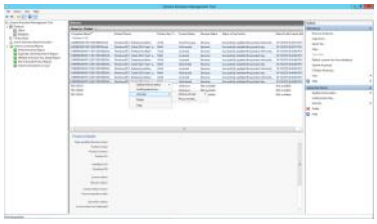
Note: We recommend using a management tool, such as System Center Configuration Manager, to send the slmgr scripts to your enterprise devices.

To install and activate ESU for devices that are *not* connected to the Internet, you can use the VAMT or phone activation.

Volume Activation Management Tool configuration

You can use the VAMT for online and/or proxy activation. To install and activate ESU keys using the VAMT, follow these steps:

1. Download and install the Volume Activation Management Tool.
2. Download the VAMT- ESU configuration file and update your VAMT configuration file.
3. Configure the client device's firewall for the VAMT.
4. Add the ESU product key to the VAMT.
5. Select the product, right-click, select **Activate**, then select your activation method, as shown below:



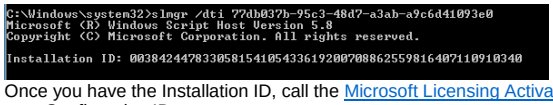
Note: For systems that cannot connect to the Internet for activation, you can use the VAMT to perform proxy activation.

For additional guidance on how to install and activate Windows 7 ESU keys on multiple devices using a multiple activation key (MAK), see this post.

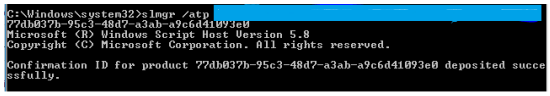
Activating ESU keys via phone

To activate ESU keys via phone, use the slmgr command options **- /dti** and **/atp**. To activate ESU keys via phone, follow these steps:

1. Open an elevated Command Prompt.
2. Type **slmgr.vbs /ipk <ESU MAK Key>** and select Enter. to install the product key.
3. Get the Installation ID for the ESU Key using the corresponding ESU Activation ID (see the table of ESU Activation IDs for each program listed earlier in the blog post). For example:



4. Once you have the Installation ID, call the Microsoft Licensing Activation Center for your region; they will walk you through the steps to get the Confirmation ID. Make a note of your Confirmation ID.
5. Type **slmgr /atp <Confirmation ID> <ESU Activation ID>** to activate the ESU SKU using the Confirmation Id obtained in the above step.



6. Type **slmgr /dlv <Activation ID>** or **slmgr /dlv all** and select **Enter** to verify that the **License Status** shows as **Licensed**.

Azure virtual machines

You do not need to deploy an additional ESU key for Azure virtual machines (VMs), Windows 7 ESU with Windows Virtual Desktop, or for bring-your-own images on Azure for Windows 7, Windows Server 2008, and Windows Server 2008 R2. Like on-premises devices, you will need to install the appropriate SSUs as outlined in the **Installation prerequisites** section above on your VMs. After installing the SSUs noted above, VMs will be enabled to download the ESU updates.

But for the

A pre-patched Windows 7 image and a pre-patched Windows Server 2008 R2 SP1 image are available from the Azure Marketplace. Azure Stack VMs or Azure VMware solutions should follow the same process as on-premises devices

For answers to commonly asked questions about ESU for Windows Server 2008 and 2008 R2 SP1, see Extended Security Updates frequently asked questions.

Next steps

If your organization still has devices running Windows 7 SP1, Windows Server 2008, or Windows Server 2008 R2 SP1, we recommend that you take the steps outlined above today and take advantage of Extended Security Updates to help ensure that your devices continue to receive necessary security updates

If you are interested in learning more about Extended Security Updates, please see the following resources:

- Announcement: Availability of ESU for purchase
- Prepare for Windows Server 2008 end of support
- Extended Security Updates FAQ
- Windows 7 end of support information for enterprises
- Windows 7 end of support FAQ

Reference:
Obtaining Extended Security Updates for eligible Windows devices

VAMT tool - Day 4

Wednesday, June 10, 2020 9:40 AM

Volume Activation Management Tool (VAMT) Technical Reference

The Volume Activation Management Tool (VAMT) enables network administrators and other IT professionals to automate and centrally manage the Windows®, Microsoft® Office, and select other Microsoft products volume and retail-activation process. VAMT can manage volume activation using Multiple Activation Keys (MAKs) or the Windows Key Management Service (KMS). VAMT is a standard Microsoft Management Console (MMC) snap-in that requires the Microsoft Management Console (MMC) 3.0. VAMT can be installed on any computer that has one of the following Windows operating systems:

- Windows® 7 or above
- Windows Server 2008 R2 or above

Important

VAMT is designed to manage volume activation for: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 (or later), Microsoft Office 2010 (or above).

VAMT is only available in an EN-US (x86) package.

1. Introduction to VAMT
2. Install and Configure VAMT
   - VAMT Requirements
   - Install VAMT
   - Configure Client Computers
3. VAMT Step-by-Step Scenarios
   - Scenario 1,: Online Activation
   - Scenario 2: Proxy Activation
   - Scenario 3: KMS Client Activation

Below is the ESU activation with VAMT:

ESU with VAMT

Assignment

Tuesday, August 4, 2020 4:37 PM

Install a VAMT tool in lab, installing a product key and checking license status for a remote machine via VAMT tool

Advance - Day 5

Tuesday, June 16, 2020 12:09 PM

Subscription Activation - Day 5

Wednesday, June 10, 2020 9:40 AM

Two important parts about Subscription Activation:
Overview of subscription activation: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
How to deploy subscription activation: https://docs.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses

Videos about Subscription Activation:
Subscription Based Activation and Troubleshooting
https://msit.microsoftstream.com/video/fe24a1ff-0400-aa78-5f43-f1ea6dbc1a39?channelId=519d6d40-dc47-4317-92fc-184352c82852

Useful info during case handling:

Frequently-used scoping questions for subscription activation:

1. What are you trying to achieve (Desired Result)?/ May I know your main concern? e.g. OS was auto convert from Ent to Pro, need change convert back to Ent; Or cannot convert to Ent for the 1st time.
2. How/ Where did you find this issue?
3. How did this machine activate before? KMS, MAK or retail, etc.
4. How many impacted computers?
5. Did this issue happen before?
6. Alternatively, what operation did you performing when the problem started to occur? e.g. run slgmr /dlv and slmgr /ato to activate KMS Ent key again.
7. May I know the exact error messages or error page?

Data collection

1. Check current key: cscript *slmgr.vbs /dlv > dlv.txt* to save output to txt file (on client & server, if applicable)
2. Check current subscription activation status:
   screenshot of **Settings > Update & Security > Activation**
3. Check the OS build: **Settings > System > About** or run the **winver** command
4. Check if the device having a firmware-embedded activation key, type the commands at an elevated Windows PowerShell prompt:
   *(Get-WmiObject -query 'select * from SoftwareLicensingService').OA3xOriginalProductKey*
5. Check the logged user account info:
   Screenshot of **Settings > Accounts > Other people > Work or school user section** or run the **whoami** command.
   What is the UPN (user principal name) of the logged user account like 123@contoso.com?
6. Did you change any local user account or other users without licenses to sign in this computer? If yes, may I have that user account name?
7. What licenses assigned to the current signed-in user? Did you have any screenshot of the user license assignment including win10 Enterprise for this user in Office 365 portal or Azure portal?
8. Run the **LicensingDiag**.exe and upload the logs in the workspace. **Note:** the log will be named as "Machinename_Date_diag.cab" under C:\Users\alias \AppData\Local\Temp

LicensingDiag

A PowerApp Bot for subscription activation

https://powerva.microsoft.com/canvas?cci_bot_id=ae5ba020-262e-4ee0-8fdd-c63717997665&cci_tenant_id=72f988bf-86f1-41af-91ab-2d7cd011db47

A PowerApp Bot to help...

Optional

Wednesday, November 25, 2020 10:03 AM

Narrow down slmgr script issues via WMI

Wednesday, November 25, 2020 10:03 AM

As you may know the slmgr.vbs script gathers Windows license information and performs Windows activation via WMI queries. If you found any error returns from slmgr script, I will recommend you continue narrowing down more to the specific WMI calling.

Basically, slmgr script uses the InstallProductKey method in **SoftwareLicensingService** class for key installation, other actions such as Windows activation and querying license information are from **SoftwareLicensingProduct** class. (slmgr.vbs also queries **SoftwareLicensingTokenActivationLicense** class for token-based activation, we may add this in further if needed).

We can use Powershell commands or WMI tester (wbemtest) to simulate the same actions.

Note

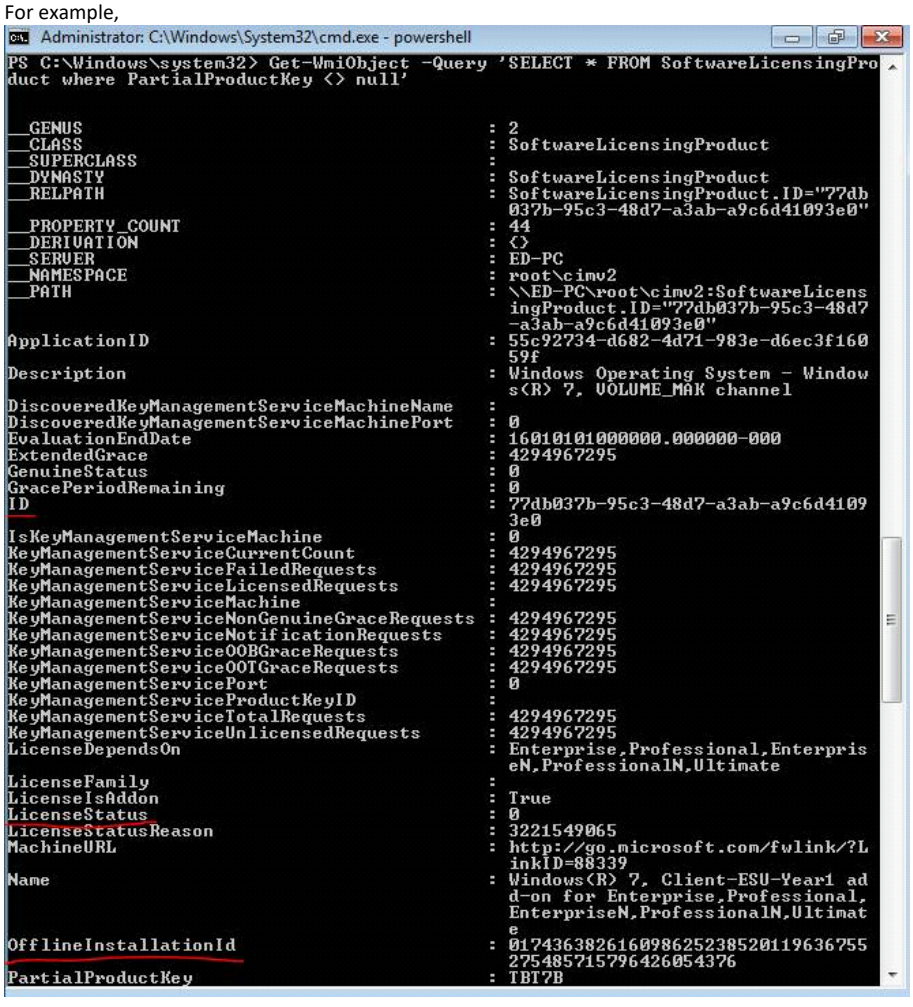
1. For Server 2008 R2 and 2008 SP2, PowerShell is not built-in that we need to add this feature in Server Manager.
2. Slmgr.vbs varnished some data from WMI queries with more readable names, here are the differences.

Slmgr.vbs	WMI
ActivationID	**ID**
InstallationID	**OfflineInstallationID**
LicenseStatus	**0** - Unlicensed **1** - Licensed **2** - Initial grace period **3** - Additional grace period (KMS license expired or hardware out of tolerance **4** - Non-genuine grace period **5** - Notification **6** - Unknown

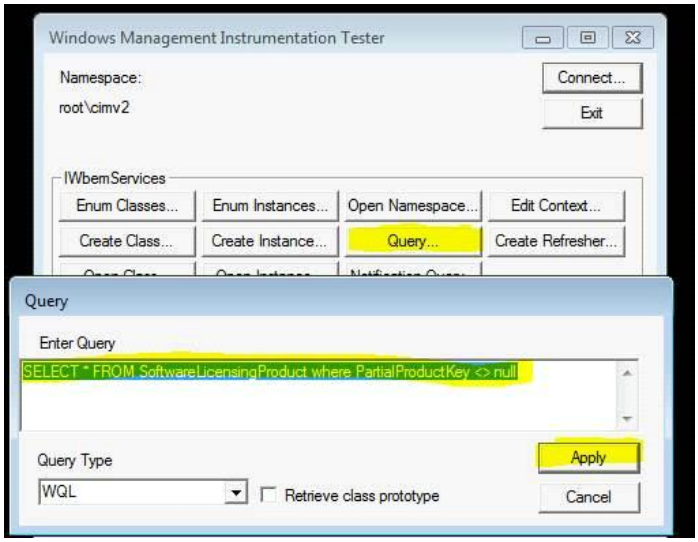
Display Current License (DLV)

```
Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingProduct where PartialProductKey <> null'
```

For example,



Same action via WMI tester,



Display Current License (DLV with ALL)

```
Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingProduct'
```

Install Product Key

```
$SoftwareLicensingService = Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingService'
$SoftwareLicensingService.InstallProductKey('<Product Key>')
```

For example,

```
PS C:\Windows\system32> $SoftwareLicensingService = Get-WmiObject -Query 'SELECT
 * FROM SoftwareLicensingService'
PS C:\Windows\system32> $SoftwareLicensingService.InstallProductKey('XD6Y3-VV37K
-J3R62-KTG4T-TBT7B')


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ReturnValue      :
```

Note: Methods of SoftwareLicensingService class are not able to invoked via WMI tester, I will suggest to you test this action via PowerShell commands.

Uninstall Product Key

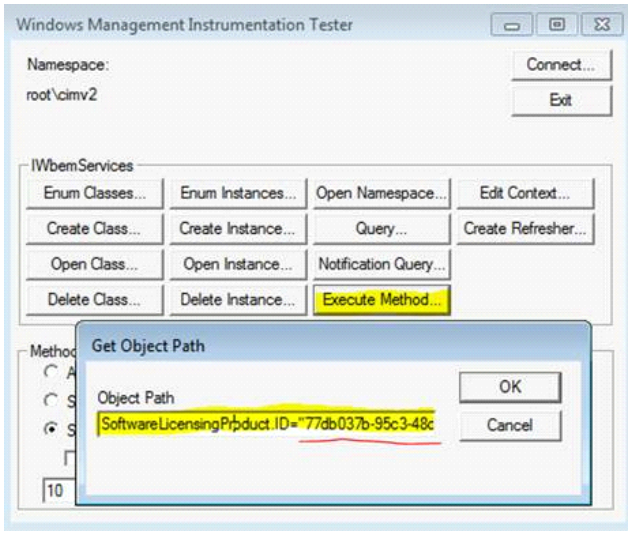
```
$License = Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingProduct where ID = "<Activation ID>"'
$License.UninstallProductKey()
```

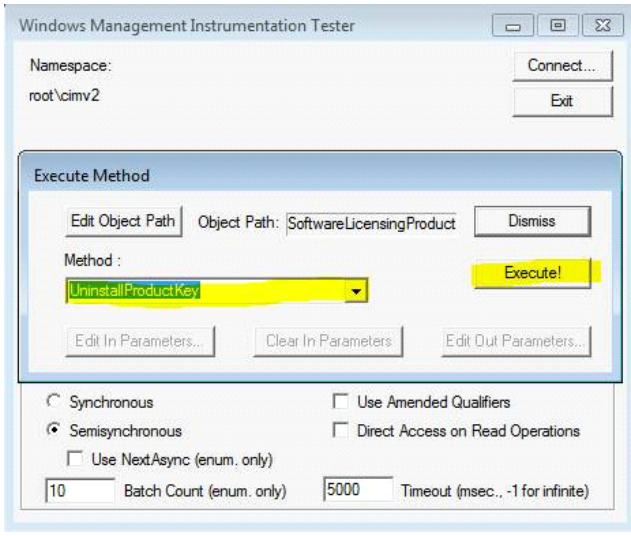
For example,

```
PS C:\Windows\system32> $CurrentActiveLicense = Get-WmiObject -Query 'SELECT * F
ROM SoftwareLicensingProduct where ID = "77db037b-95c3-48d7-a3ab-a9c6d41093e0"'
PS C:\Windows\system32> $CurrentActiveLicense.UninstallProductKey()


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ReturnValue      :
```

Same action via WMI tester,



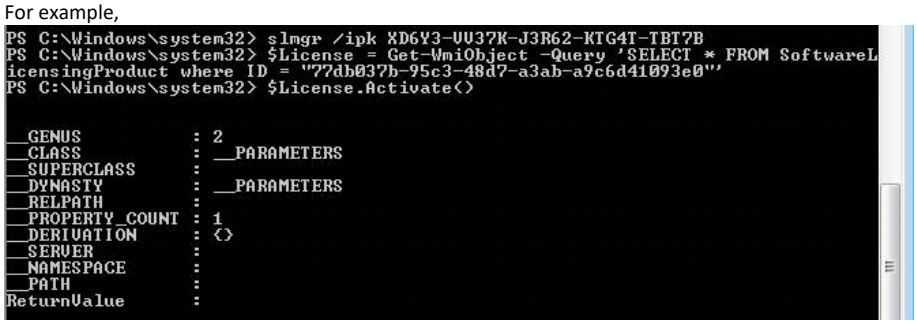


Activation

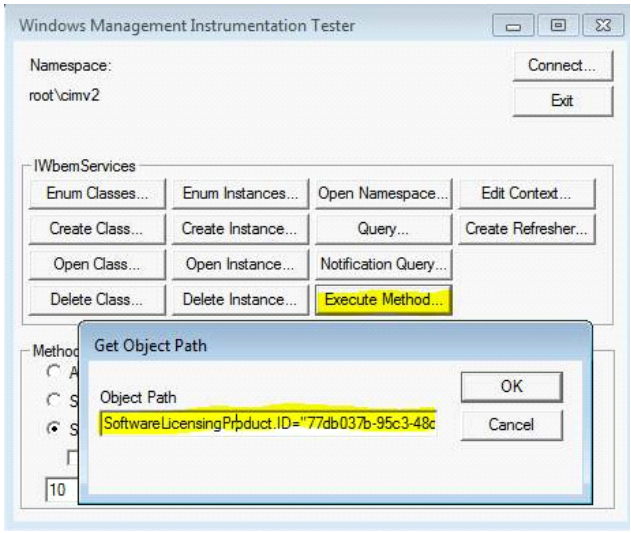
- Online Activation

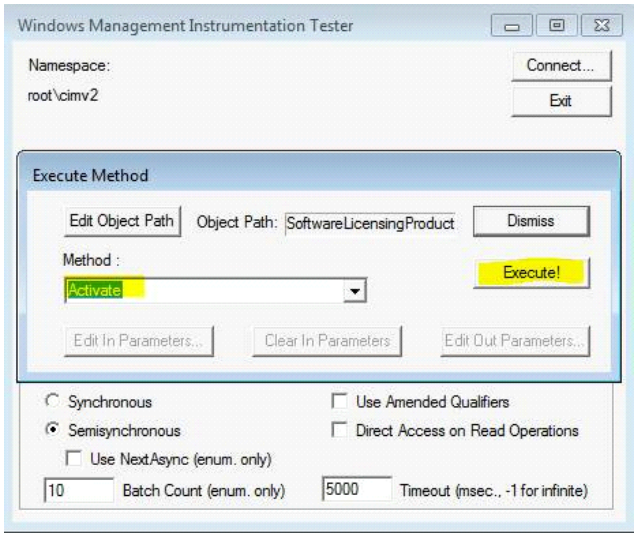
```
$License = Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingProduct where ID = "<Activation ID>"'
$License.Activate()
```

For example,



Same action via WMI tester,

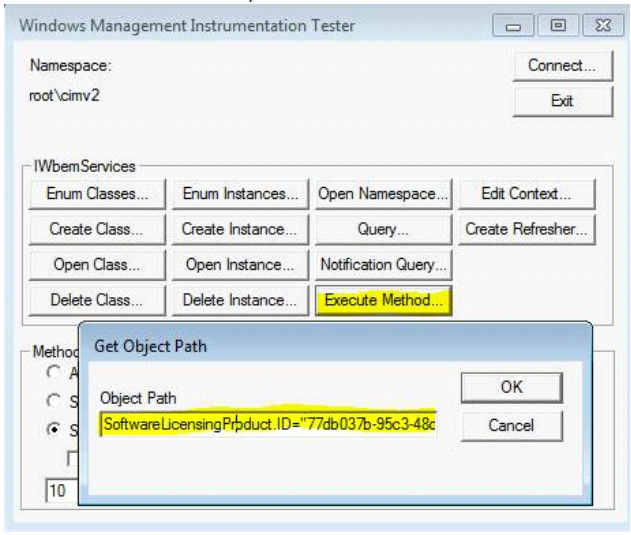


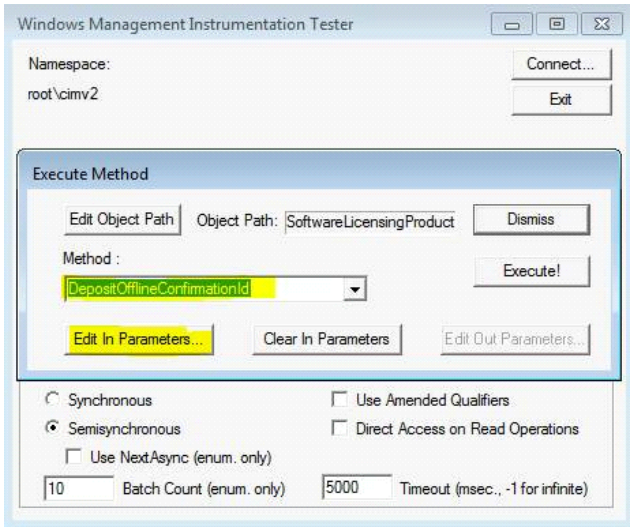


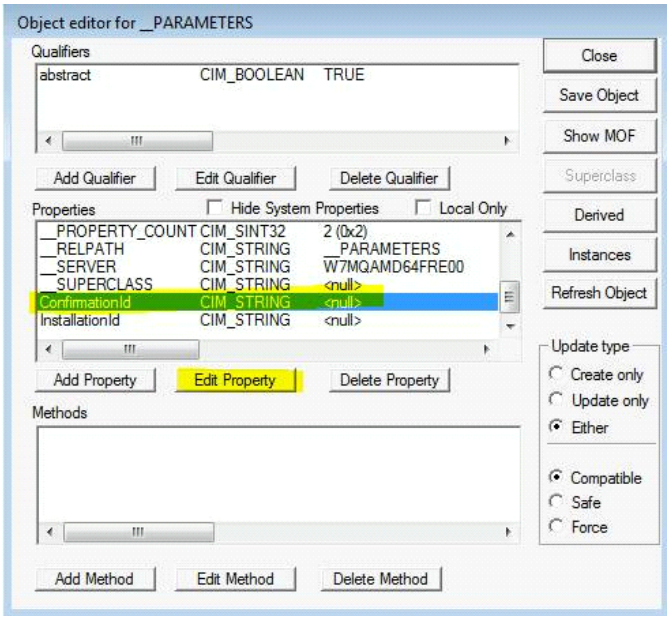
- Phone Activation

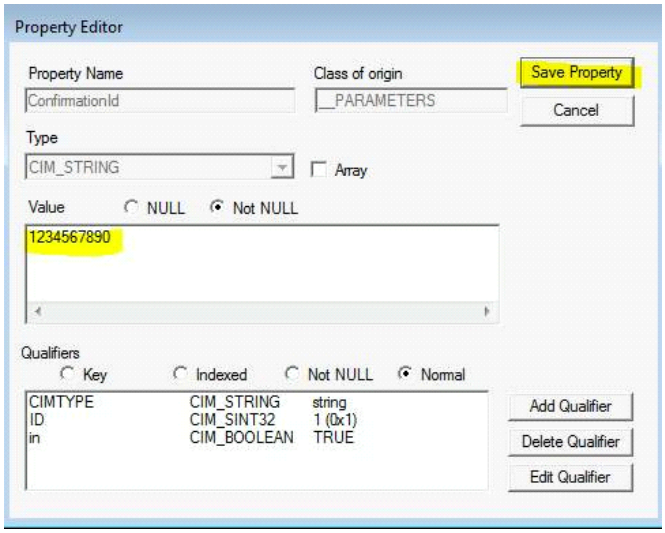
```
$License = Get-WmiObject -Query 'SELECT * FROM SoftwareLicensingProduct where ID = "<Activation ID>"'
$License.DepositOfflineConfirmationId('<InstallationID>','<ConfirmationID>')
```

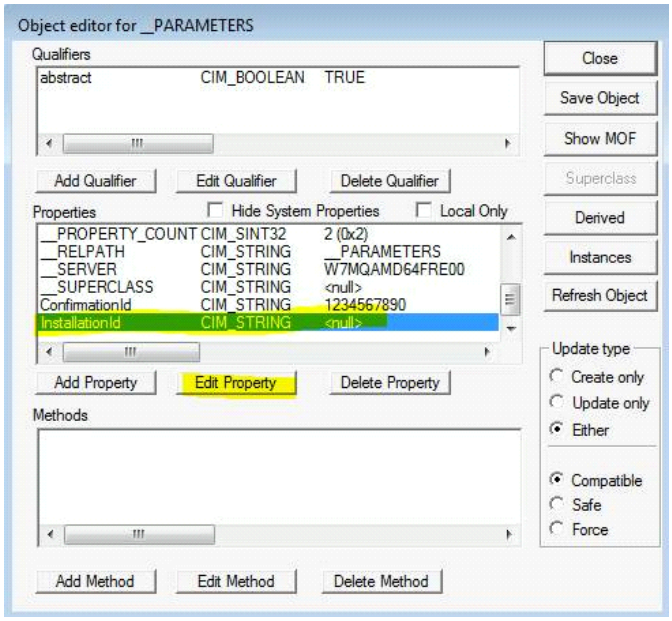
Same action via WMI tester,

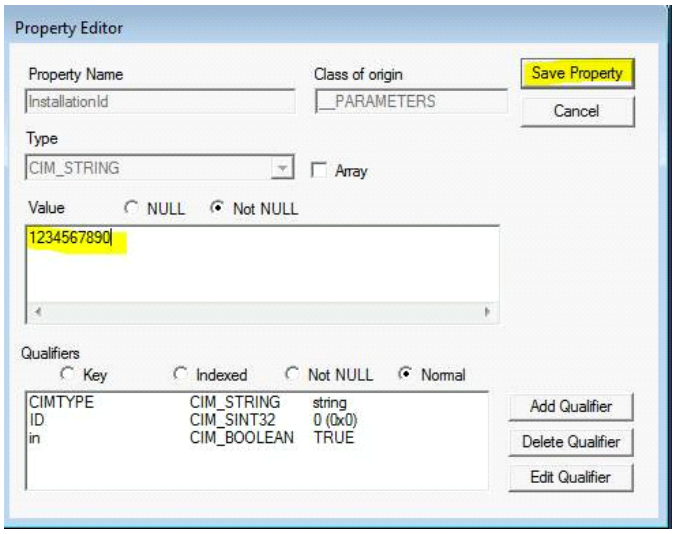


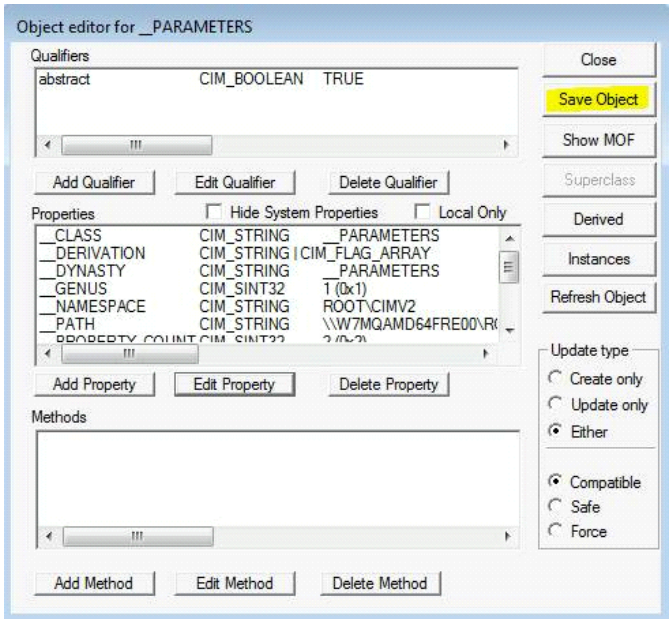

Windows Management Instrumentation Tester
Namespace:
root\cimv2
Connect...
Exit
Execute Method
Edit Object Path
Object Path: SoftwareLicensingProduct
Dismiss
Method :
DepositOfflineConfirmationId
Execute!
Edit In Parameters...
Clear In Parameters
Edit Out Parameters...
Synchronous
Semisynchronous
Use NextAsync (enum. only)
Use Amended Qualifiers
Direct Access on Read Operations
10
Batch Count (enum. only)
5000
Timeout (msec., -1 for infinite)

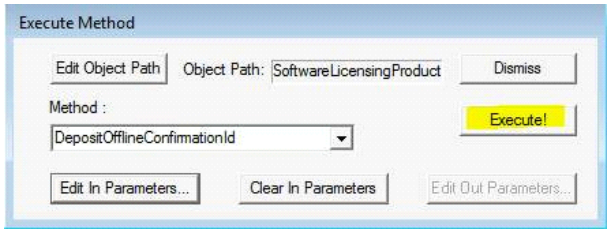

Object editor for __PARAMETERS
Qualifiers
abstract CIM_BOOLEAN TRUE
Add Qualifier
Edit Qualifier
Delete Qualifier
Properties
Hide System Properties
Local Only
__PROPERTY_COUNT CIM_SINT32 2 (0x2)
__RELPATH CIM_STRING __PARAMETERS
__SERVER CIM_STRING W7MQAMD64FRE00
__SUPERCLASS CIM_STRING <null>
ConfirmationId CIM_STRING <null>
InstallationId CIM_STRING <null>
Add Property
Edit Property
Delete Property
Methods
Add Method
Edit Method
Delete Method
Close
Save Object
Show MOF
Superclass
Derived
Instances
Refresh Object
Update type
Create only
Update only
Either
Compatible
Safe
Force


Property Editor
Property Name
ConfirmationId
Class of origin
__PARAMETERS
Save Property
Cancel
Type
CIM_STRING
Array
Value
NULL
Not NULL
1234567890
Qualifiers
Key
Indexed
Not NULL
Normal
CIMTYPE CIM_STRING string
ID CIM_SINT32 1 (0x1)
in CIM_BOOLEAN TRUE
Add Qualifier
Delete Qualifier
Edit Qualifier


Object editor for __PARAMETERS
Qualifiers
abstract CIM_BOOLEAN TRUE
Close
Save Object
Show MOF
Add Qualifier
Edit Qualifier
Delete Qualifier
Superclass
Properties
Hide System Properties
Local Only
Derived
__PROPERTY_COUNT CIM_SINT32 2 (0x2)
__RELPATH CIM_STRING __PARAMETERS
__SERVER CIM_STRING W7MQAMD64FRE00
__SUPERCLASS CIM_STRING <null>
ConfirmationId CIM_STRING 1234567890
InstallationId CIM_STRING <null>
Instances
Refresh Object
Update type
Add Property
Edit Property
Delete Property
Create only
Update only
Either
Methods
Compatible
Safe
Force
Add Method
Edit Method
Delete Method


Property Editor
Property Name
Class of origin
Save Property
InstallationId
__PARAMETERS
Cancel
Type
CIM_STRING
Array
Value
NULL
Not NULL
1234567890
Qualifiers
Key
Indexed
Not NULL
Normal
CIMTYPE CIM_STRING string
ID CIM_SINT32 0 (0x0)
in CIM_BOOLEAN TRUE
Add Qualifier
Delete Qualifier
Edit Qualifier


Object editor for __PARAMETERS
Qualifiers
abstract CIM_BOOLEAN TRUE
Close
Save Object
Show MOF
Add Qualifier
Edit Qualifier
Delete Qualifier
Superclass
Properties
Hide System Properties
Local Only
Derived
__CLASS CIM_STRING __PARAMETERS
__DERIVATION CIM_STRING CIM_FLAG_ARRAY
__DYNASTY CIM_STRING __PARAMETERS
__GENUS CIM_SINT32 1 (0x1)
__NAMESPACE CIM_STRING ROOT\CIMV2
__PATH CIM_STRING \\W7MQAMD64FRE00\R
Instances
Refresh Object
Update type
Add Property
Edit Property
Delete Property
Create only
Update only
Either
Methods
Compatible
Safe
Force
Add Method
Edit Method
Delete Method



Get ActivationID of installed licenses

```
Get-WmiObject -Query 'SELECT ID,Description,Name FROM SoftwareLicensingProduct where PartialProductKey <> null'
```

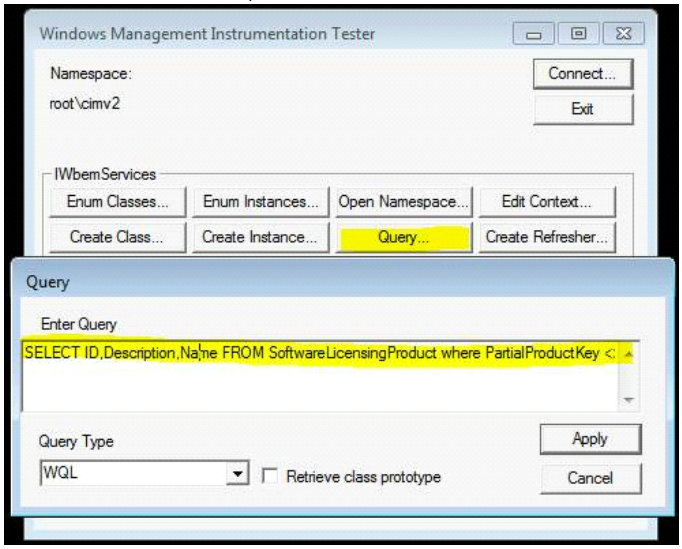
For example,

```
PS C:\Windows\system32> Get-WmiObject -Query 'SELECT ID,Description,Name FROM So
ftwareLicensingProduct where PartialProductKey <> null'


__GENUS          : 2
__CLASS          : SoftwareLicensingProduct
__SUPERCLASS     :
__DYNASTY        :
__RELPATH        : SoftwareLicensingProduct.ID="77db037b-95c3-48d7-a3ab-a9c6d41
                   093e0"
__PROPERTY_COUNT : 3
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
Description      : Windows Operating System - Windows(R) 7, VOLUME_MAK channel
ID               : 77db037b-95c3-48d7-a3ab-a9c6d41093e0
Name             : Windows(R) 7, Client-ESU-Year1 add-on for Enterprise,Profess
                   ional,EnterpriseN,ProfessionalN,Ultimate

__GENUS          : 2
__CLASS          : SoftwareLicensingProduct
__SUPERCLASS     :
__DYNASTY        :
__RELPATH        : SoftwareLicensingProduct.ID="ae2ee509-1b34-41c0-acb7-6d46501
                   68915"
__PROPERTY_COUNT : 3
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
Description      : Windows Operating System - Windows(R) 7, VOLUME_KMSCLIENT ch
                   annel
ID               : ae2ee509-1b34-41c0-acb7-6d4650168915
Name             : Windows(R) 7, Enterprise edition
```

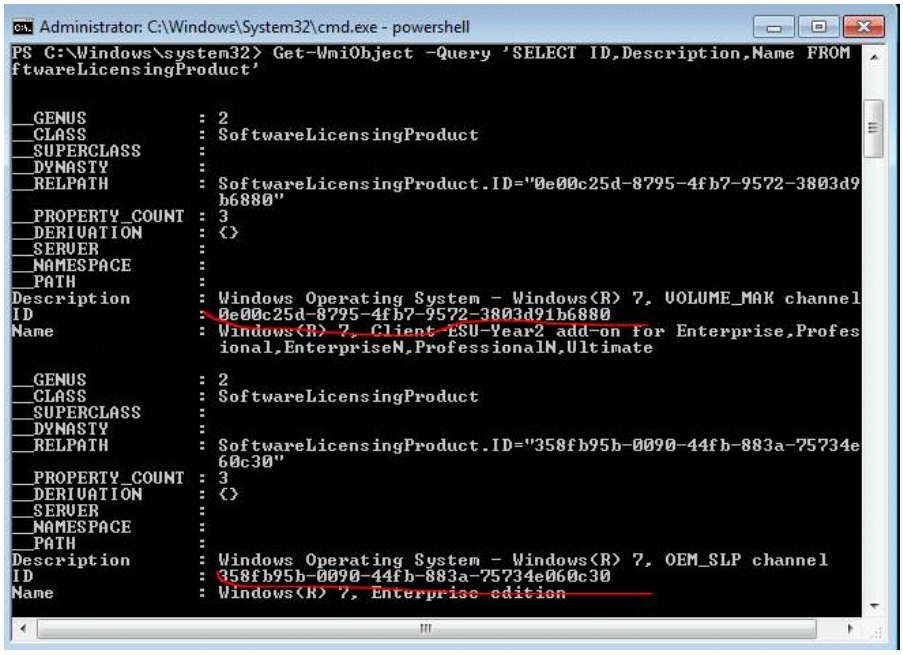
Same action via WMI tester,



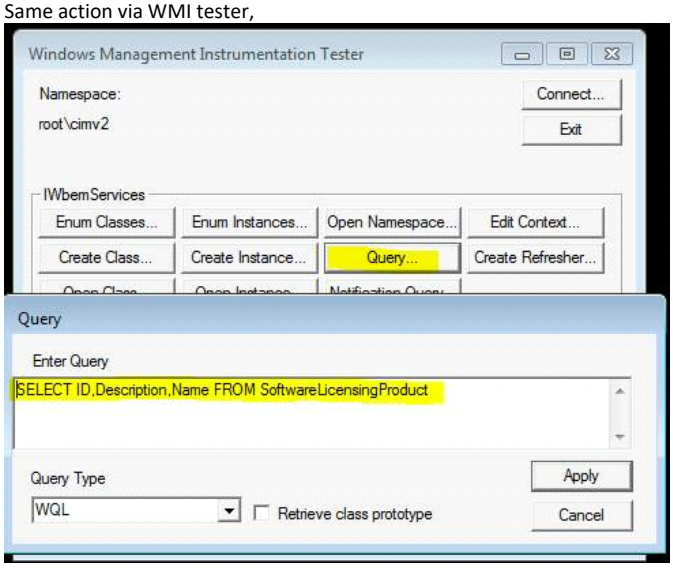
Get ActivationID of all Licenses

```
Get-WmiObject -Query 'SELECT ID,Description,Name FROM SoftwareLicensingProduct'
```

For example,



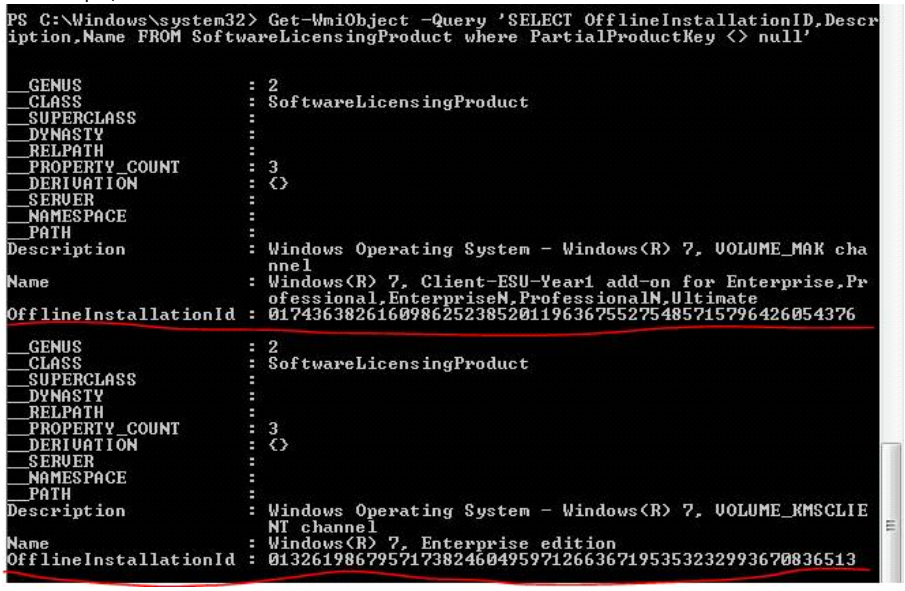
Same action via WMI tester,



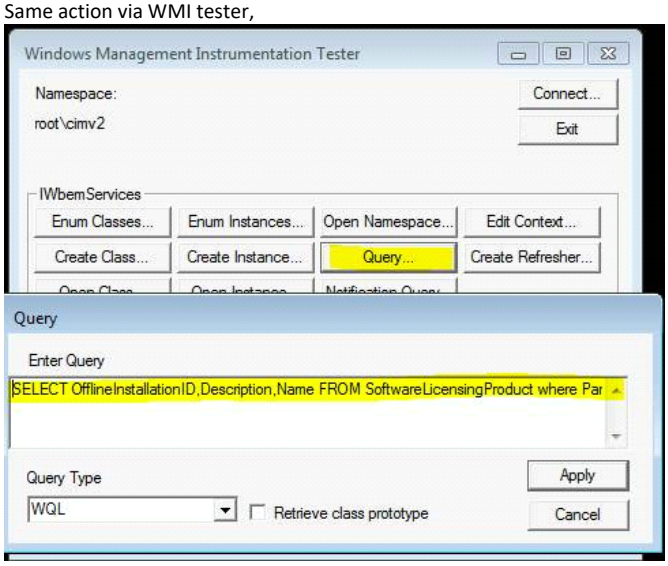
GET InstallationID of installed licenses

```
Get-WmiObject -Query 'SELECT OfflineInstallationID,Description,Name FROM SoftwareLicensingProduct where PartialProductKey <> null'
```

For example,



Same action via WMI tester,



Case Card

Wednesday, September 23, 2020 10:18 AM

Activation

Case Sharing: Win10 1809 Subscription Activation did not work when AzureAdPrt is Yes

Wednesday, July 29, 2020 8:49 AM

Symptom

Hybrid AAD Joined device windows 10 1809 cannot convert OS from Pro to Ent with M365 E5 licenses assigned.

Logon UPN: seven.xie@joyson.cn
Store cannot get user ticket for current logon UPN while AAD logs showed getting AzureAdPrt successfully in device registration.

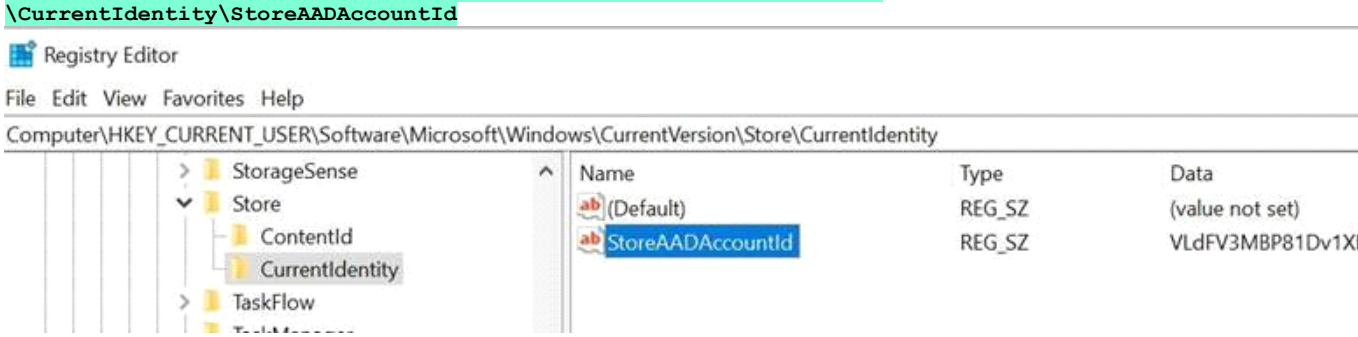
Error page:

Cause

Store requires the user ticket for PerUser account (the primary account).

Resolution

1. Sign out with the current user from Microsoft Store, delete the key **StoreAADAccountId** if any existing value on the registry key:
   `RegQueryValue` **`HKCU\Software\Microsoft\Windows\CurrentVersion\Store\CurrentIdentity\StoreAADAccountId`**



2. Sign in computer with the synced account again and the subscription activation successfully changed the OS to Ent.

Troubleshoot

1. The dsregcmd output and "Add Work or School account" showed device connected to **HQ.joysoncorp.com(HQ)**:

Note:
Usually, the logon UPN suffix will be same as the custom domain name that verified on AAD, e.g. the custom domain verified is **fareast.corp.microsoft.com** and our logon UPN is alias@microsoft.com.
However, customer can also use different UPN suffix from the domain verified on AAD, like in this case, logon UPN is seven.xie@**joyson.cn** not seven.xie@joysoncorp.com while the verified domain is **HQ.joysoncorp.com**.

1. Dsregcmd output showed the user succeed to get AADPRT and device is hybrid joined:

++++++++++
AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : YES
DomainName : HQ

TenantName : Joyson Group
TenantId : b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad
Idp : login.windows.net
AuthCodeUrl : https://login.microsoftonline.com/b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad/oauth2/authorize
AccessTokenUrl : https://login.microsoftonline.com/b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad/oauth2/token

NgcSet : NO
WorkplaceJoined : NO
WamDefaultSet : YES
WamDefaultAuthority : organizations
WamDefaultId : https://login.microsoft.com
WamDefaultGUID : {B16898C6-A148-4967-9171-64D755DA8520} (AzureAd)

AzureAdPrt : YES
AzureAdPrtUpdateTime : 2020-05-22 05:09:40.000 UTC
AzureAdPrtExpiryTime : 2020-06-05 08:54:38.000 UTC
AzureAdPrtAuthority : https://login.microsoftonline.com/b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad
EnterprisePrt : NO
EnterprisePrtAuthority :

IsDeviceJoined : YES
IsUserAzureAD : YES
++++++++++

3. Store logs suspected licensing services cannot get the AAD user ticket for current user logon session while the AAD states the user token has been successfully acquired as the PRT is

AzureAdPrt is Yes.

==========

5/22/2020 5:26:29 PM Getting user tickets for S-1-5-21-3833889453-1992424714-450002985-2653
Function: SingleUserStoredIdentitySnapshot::CaptureIdentity
Source: onecoreuap\enduser\winstore\licensemanager\lib\identity.cpp (350)
5/22/2020 5:26:30 PM hr: 0x80004005
Function: WinStoreAuth::AuthenticationInternal::FindAccount
Source: \winstoreauth.cpp (1581)
5/22/2020 5:26:30 PM hr: 0x80004005
Function: WinStoreAuth::AuthenticationInternal::GetAllAccountTickets
Source: \winstoreauth.cpp (638)
5/22/2020 5:26:30 PM hr: 0x80070525 //ERROR_NO_SUCH_USER The specified account does not exist.
Function: WaitForOperation
Source: onecoreuap\enduser\winstore\licensemanager\inc\util.h (294)
5/22/2020 5:26:30 PM No authenticated user, no ticket. (0x80070525) //ERROR_NO_SUCH_USER The specified account does not exist.
Function: CaptureLegacyMSATicket
Source: onecoreuap\enduser\winstore\licensemanager\lib\identity.cpp (125)
5/22/2020 5:26:30 PM No user tickets captured for S-1-5-21-3833889453-1992424714-450002985-2653, so this might not end well.
Function: SingleUserStoredIdentitySnapshot::CaptureIdentity
Source: onecoreuap\enduser\winstore\licensemanager\lib\identity.cpp (416)
5/22/2020 5:26:30 PM Requesting license for 8d419748-b6f9-41a8-e3d0-ebd7a8880244 at /v7.0/licenses/content (https://licensing.mp.microsoft.com) (Corr: aVLAtSFuGEWZmVaB.40)
Function: LicenseProxyService::DoRequestLicense
Source: onecoreuap\enduser\winstore\licensemanager\lib\proxy.cpp (1960)
5/22/2020 5:26:30 PM License Response: 0 leases, 0 keys for contentId 8d419748-b6f9-41a8-e3d0-ebd7a8880244 (Corr: aVLAtSFuGEWZmVaB.40, Svr: 00003D1F)
Function: LogRequestLicenseSuccess
Source: onecoreuap\enduser\winstore\licensemanager\lib\telemetry.cpp (195)
5/22/2020 5:26:30 PM Satisfaction error from service: 1: Users do not possess any satisfying entitlements for the content id in question. (Corr: aVLAtSFuGEWZmVaB.40, Svr: 00003D1F)
Function: LogSatisfactionError
Source: onecoreuap\enduser\winstore\licensemanager\lib\telemetry.cpp (135)

==========

4. From **TbDiag.exe GetAccount** output, we can see customer indeed having two PerUser accounts.

==========
[9] AccountId : 52qc9dkg4krst2t8pknpqare
UserName : Seven.XieO365@joyson.onmicrosoft.com
AccountRevisionNumber: 207
AccountScope: PerUser
AccountEnumerableState: AlwaysAllowed
AccountPerUserId:
Properties :
UPN : Seven.XieO365@joyson.onmicrosoft.com
DisplayName : Seven.Xie-O365
IsDefaultPicture : True
TenantId : b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad
PasswordExpiresOn : 13291397679
PasswordChangeUrl : https://portal.microsoftonline.com/ChangePassword.aspx
FirstName : Seven
OID : 1927c8cc-4688-48bd-93ec-3b8dd716de47
Authority : https://login.microsoftonline.com/common
SignInName : Seven.XieO365@joyson.onmicrosoft.com
UserName : Seven.XieO365@joyson.onmicrosoft.com
LastName : Xie

[10] AccountId : g1aub1v99a0g51g4k1u850nb
UserName : seven.xie@joyson.cn

AccountRevisionNumber: 2630

AccountScope: PerUser

AccountEnumerableState: AlwaysAllowed

AccountPerUserId:

Properties :

UPN : seven.xie@joyson.cn

DisplayName : Seven Xie ???

IsDefaultPicture : False

TenantId : b953e8d2-f5f3-4cff-a9b1-e5b91ce608ad

PasswordChangeUrl : https://portal.microsoftonline.com/ChangePassword.aspx

FirstName : ??

OID : 0c29031e-5cad-433e-a523-62f1d3d167fa

Authority : https://login.microsoftonline.com/common

SignInName : seven.xie@joyson.cn

UserName : seven.xie@joyson.cn

LastName : ?

==========

5. Checked the ETL trace, found two user tickets but both are for the PerApplication accounts (**8qdbg3QVvzzPNw6Z_ubMKCOQaViMuH9JUd0SzTfB7RE** and **4ypwhxIasFnHkIs-2UMoE_sGQWuVinmix5_lCyvukp0**) , not the target PerUser account **g1aub1v99a0g51g4k1u850nb**.

```
3140 [0]1EB0.77B0::05/22/20-17:26:30.0105964
[Microsoft.Windows.Security.TokenBroker]
[FindAllSystemAccountsOperationWorkerNumberOfAccountsEvent] AccountCount=2,
PluginPfn=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
3141 [0]1EB0.77B0::05/22/20-17:26:30.0106307
[Microsoft.Windows.Security.TokenBroker] [Reg_GetPluginPFNEvent]
ProviderId=https://login.microsoft.com, Authority=consumers,
RealProviderId=https://login.live.com
3142 [0]1EB0.77B0::05/22/20-17:26:30.0106565
[Microsoft.Windows.Security.TokenBroker] [Reg_GetPluginPFNResultEvent]
ProviderPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3143 [0]1EB0.77B0::05/22/20-17:26:30.0106629
[Microsoft.Windows.Security.TokenBroker]
[FindAllSystemAccountsOperationWorkerNextPluginEvent]
PluginPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3144 [0]1EB0.77B0::05/22/20-17:26:30.0106849
[Microsoft.Windows.Security.TokenBroker]
[GetAllProviderAccountsFromDataStoreEvent]
ProviderPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3145 [0]1EB0.77B0::05/22/20-17:26:30.0106859
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheGetAllObjectIdsForTypeEvent] ObjectType=0,
OwnerPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3146 [3]1EB0.77B0::05/22/20-17:26:30.0123096
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadAllObjectIdsForTypeFromCacheEvent] ObjectType=0,
OwnerPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3147 [3]1EB0.77B0::05/22/20-17:26:30.0127867
[Microsoft.Windows.Security.TokenBroker]
[GetAllProviderAccountsFromDataStoreAccountsCountEvent] NumberOfAccounts=0
3148 [3]1EB0.77B0::05/22/20-17:26:30.0127916
[Microsoft.Windows.Security.TokenBroker]
[FindAllSystemAccountsOperationWorkerNumberOfAccountsEvent] AccountCount=0,
PluginPfn=Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
3149 [3]1EB0.77B0::05/22/20-17:26:30.0128235
[Microsoft.Windows.Security.TokenBroker] [Reg_GetPluginPFNEvent]
ProviderId=https://xsts.auth.xboxlive.com, Authority=NULL,
RealProviderId=https://xsts.auth.xboxlive.com
3150 [3]1EB0.77B0::05/22/20-17:26:30.0128470
[Microsoft.Windows.Security.TokenBroker] [Reg_GetPluginPFNResultEvent]
ProviderPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3151 [3]1EB0.77B0::05/22/20-17:26:30.0128527
[Microsoft.Windows.Security.TokenBroker]
[FindAllSystemAccountsOperationWorkerNextPluginEvent]
PluginPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3152 [3]1EB0.77B0::05/22/20-17:26:30.0128721
[Microsoft.Windows.Security.TokenBroker]
[GetAllProviderAccountsFromDataStoreEvent]
```

ProviderPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3153 [3]1EB0.77B0::05/22/20-17:26:30.0128730
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheGetAllObjectIdsForTypeEvent] ObjectType=0,
OwnerPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3154 [2]1EB0.77B0::05/22/20-17:26:30.0177048
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadAllObjectIdsForTypeFromCacheEvent] ObjectType=0,
OwnerPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3155 [2]1EB0.77B0::05/22/20-17:26:30.0182186
[Microsoft.Windows.Security.TokenBroker]
[GetAllProviderAccountsFromDataStoreAccountsCountEvent] NumberOfAccounts=0
3156 [2]1EB0.77B0::05/22/20-17:26:30.0182241
[Microsoft.Windows.Security.TokenBroker]
[FindAllSystemAccountsOperationWorkerNumberOfAccountsEvent] AccountCount=0,
PluginPfn=Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
3157 [2]1EB0.77B0::05/22/20-17:26:30.0182442
[Microsoft.Windows.Security.TokenBroker] [TokenBrokerInternalFindAllAccounts]
wilActivity=hresult=0 (0x00000000)

3284 [2]1EB0.55CC::05/22/20-17:26:30.1274193
[Microsoft.Windows.Security.TokenBroker] [Reg_CreateProviderFromRegistration]
AliasPluginId=null, AliasAuthority=null, UserContextToken=961202156
3285 [2]1EB0.55CC::05/22/20-17:26:30.1275758
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationMappedEvent]
EffectivePluginId=https://login.microsoft.com,
EffectiveAuthority=organizations
3286 [2]1EB0.55CC::05/22/20-17:26:30.1275787
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationCreateEvent] AccountType=???????,
Purpose=???????
3287 [2]1EB0.55CC::05/22/20-17:26:30.1279338
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationLogoEvent]
Logo=@{Microsoft.AAD.BrokerPlugin_1000.17763.1.0
_neutral_neutral_cw5n1h2txyewy?ms-
resource://Microsoft.AAD.BrokerPlugin/Files/Assets/Logo.png}
3288 [2]1EB0.55CC::05/22/20-17:26:30.1279366
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationAumIdEvent]
AumId=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy!App
3289 [2]1EB0.55CC::05/22/20-17:26:30.1279888
[Microsoft.Windows.Security.TokenBroker] [InitializeAccountFromDataStoreEvent]
AccountId=8qdbg3QVvzzPNw6Z_ubMKCOQaViMuH9JUd0SzTfB7RE, Flags=7,
ProviderPfn=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy, AppPfn=NULL
3290 [2]1EB0.55CC::05/22/20-17:26:30.1280008
[Microsoft.Windows.Security.TokenBroker] [TBStoredObjectCreateEvent]
ObjectType=0, ObjectId=ac961f383e390ee233b31a60095a157ad9a7c81f,
StringObjectId=8qdbg3QVvzzPNw6Z_ubMKCOQaViMuH9JUd0SzTfB7RE,
OwnerPfn=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
3291 [2]1EB0.55CC::05/22/20-17:26:30.1289476
[Microsoft.Windows.Security.TokenBroker] [TBStoredObjectInitializeEvent]
ObjectFolderPath=C:\Users\seven.xie\AppData\Local\Packages
\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\AC\TokenBroker\Accounts,
ObjectFilePath=C:\Users\seven.xie\AppData\Local\Packages
\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\AC\TokenBroker\Accounts
\ac961f383e390ee233b31a60095a157ad9a7c81f.tbacct
3292 [2]1EB0.55CC::05/22/20-17:26:30.1289797
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadBytesEvent] CacheKey=gzd5vuHIcipVPBBwDLa3at8YI6U=
3293 [2]1EB0.55CC::05/22/20-17:26:30.1305493
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadBytesFromCacheEvent]
CacheKey=gzd5vuHIcipVPBBwDLa3at8YI6U=
3294 [3]1EB0.55CC::05/22/20-17:26:30.1329334
[Microsoft.Windows.Security.TokenBroker]
[InitializeAccountFromDataStoreAccessCheckEvent] PropertyViewAllowed=true
3295 [3]1EB0.55CC::05/22/20-17:26:30.1335550
[Microsoft.Windows.Security.TokenBroker] [TokenBrokerInternalFindAccount]
wilActivity=hresult=0 (0x00000000)

3207 [1]1EB0.55CC::05/22/20-17:26:30.0690786
[Microsoft.Windows.Security.TokenBroker] [Reg_CreateProviderFromRegistration]
AliasPluginId=null, AliasAuthority=null, UserContextToken=961202156
3208 [1]1EB0.55CC::05/22/20-17:26:30.0691620
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationMappedEvent]
EffectivePluginId=https://login.microsoft.com,
EffectiveAuthority=organizations
3209 [1]1EB0.55CC::05/22/20-17:26:30.0691634
[Microsoft.Windows.Security.TokenBroker]

```
[Reg_CreateProviderFromRegistrationCreateEvent] AccountType=???????,
Purpose=???????
3210 [1]1EB0.55CC::05/22/20-17:26:30.0694666
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationLogoEvent]
Logo=@{Microsoft.AAD.BrokerPlugin_1000.17763.1.0
_neutral_neutral_cw5n1h2txyewy?ms-
resource://Microsoft.AAD.BrokerPlugin/Files/Assets/Logo.png}
3211 [1]1EB0.55CC::05/22/20-17:26:30.0694682
[Microsoft.Windows.Security.TokenBroker]
[Reg_CreateProviderFromRegistrationAumIdEvent]
AumId=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy!App
3212 [1]1EB0.55CC::05/22/20-17:26:30.0695130
[Microsoft.Windows.Security.TokenBroker] [InitializeAccountFromDataStoreEvent]
AccountId=4ypwhxIasFnHkIs-2UMoE_sGQWuVinmix5_lCyvukp0, Flags=7,
ProviderPfn=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy, AppPfn=NULL
3213 [1]1EB0.55CC::05/22/20-17:26:30.0695244
[Microsoft.Windows.Security.TokenBroker] [TBStoredObjectCreateEvent]
ObjectType=0, ObjectId=75ec28599ef8d03426d05c6d7842fccbdf477125,
StringObjectId=4ypwhxIasFnHkIs-2UMoE_sGQWuVinmix5_lCyvukp0,
OwnerPfn=Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
3214 [1]1EB0.55CC::05/22/20-17:26:30.0703350
[Microsoft.Windows.Security.TokenBroker] [TBStoredObjectInitializeEvent]
ObjectFolderPath=C:\Users\seven.xie\AppData\Local\Packages
\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\AC\TokenBroker\Accounts,
ObjectFilePath=C:\Users\seven.xie\AppData\Local\Packages
\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\AC\TokenBroker\Accounts
\75ec28599ef8d03426d05c6d7842fccbdf477125.tbacct
3215 [1]1EB0.55CC::05/22/20-17:26:30.0703658
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadBytesEvent] CacheKey=o+z7YY9IC+soea3xlWjsTByGsUM=
3216 [1]1EB0.55CC::05/22/20-17:26:30.0720389
[Microsoft.Windows.Security.TokenBroker]
[TBStoredObjectWithCacheReadBytesFromCacheEvent]
CacheKey=o+z7YY9IC+soea3xlWjsTByGsUM=
3217 [1]1EB0.55CC::05/22/20-17:26:30.0730509
[Microsoft.Windows.Security.TokenBroker]
[InitializeAccountFromDataStoreAccessCheckEvent] PropertyViewAllowed=true
3218 [1]1EB0.55CC::05/22/20-17:26:30.0734594
[Microsoft.Windows.Security.TokenBroker] [TokenBrokerInternalFindAccount]
wilActivity=hresult=0 (0x00000000)
```

Searched in the account list, we can see those two user tickets are for **PerApplication** accounts, no for **PerUser** account.

```
[12] AccountId : 8qdbg3QVvzzPNw6Z_ubMKCOQaViMuH9JUd0SzTfB7RE

  UserName : seven.xie@joyson.cn

  AccountRevisionNumber: 3

  AccountScope: PerApplication

  AccountEnumerableState: AlwaysAllowed

  AccountPerUserId: g1aub1v99a0g51g4k1u850nb
```

```
[8] AccountId : 4ypwhxIasFnHkIs-2UMoE_sGQWuVinmix5_lCyvukp0
  UserName : Seven.XieO365@joyson.onmicrosoft.com
  AccountRevisionNumber: 26
  AccountScope: PerApplication
  AccountEnumerableState: AlwaysAllowed
  AccountPerUserId: 52qc9dkg4krst2t8pknpqare
  Properties :
```

Takeaway:

Token can be created for **user** or **application**.

When user accessing to certain apps like outlook or Facebook, it requires an application token to access the resources, usually called access token. The application token means no interactions required from user and the **PerApplication** account is used for creating those app token during the authentication and authorization.

For the windows logon on the hybrid devices, it will not authenticate the **PerApplication** account when user asking for AD/AAD resources at each request but instead, it will create a primary account, it should be a **PerUser** account type that used to generate user ticket later. Once granted, user will be able to access to the AD or AAD resources in a period. When we checking the **Store event logs** to see if any user ticket, the user ticket here we saw should be generated by a **PerUser** account. Hence, **you need to first ensure there are PerUser accounts listed in the output of TbDiag.exe GetAccount /provider https://login.windows.net**.

Meanwhile, the **AzureAdPrt** we usually saw in the dsregcmd output is the **primary refresh token**, which is used for **SSO and obtained during Windows Logon / user signin or unlock** (hence it is a user token as it is generated with user credential). For windows 10 AAD joined machine or hybrid joined machine, if you want to use the SSO supported services like O365, SaaS apps or Windows Integrated authentication apps or AD FS, the PRT is needed. The PRT can be used to exchange the access token to allow user can access to the resources like O365, outlook and etc. Without it, the user will be prompted for credentials when accessing applications every time.

In brief, if you see **AzureAdPrt is Yes**, this is **not** meaning our Store getting the user ticket. Regarding to Store requesting for licenses, it will first check if any previous user signing Microsoft Store and generate a registry key here: If yes, Store will check it whether it is generated by PerUser or PerApplication. If PerApplication, Store may report no user ticket found. What you can do is to delete this registry and sign out and sign in computer again as a quick workaround, the new logon session will check tokencache or generate a new user ticket.

【Additional links for activation】

Thursday, August 18, 2022 2:20 PM

>>KMS host key backwards compatible:

CSVLK group	CSVLK can be hosted on	Windows editions activated by this KMS host
Volume License for Windows Server 2022	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Windows Server 2022 (all editions) • Windows Server Semi-Annual Channel • Windows Server 2019 (all editions) • Windows Server 2016 (all editions) • Windows 11 Enterprise/Enterprise N • Windows 11 Professional/Professional N • Windows 11 Professional for Workstations/Professional N for Workstations • Windows 11 for Education/Education N • Windows 10 Enterprise LTSC/LTSC N/LTSB • Windows 10 Enterprise/Enterprise N • Windows 10 Professional/Professional N • Windows 10 Professional for Workstations/Professional N for Workstations • Windows 10 for Education/Education N • Windows Server 2012 R2 (all editions) • Windows 8.1 Professional • Windows 8.1 Enterprise • Windows Server 2012 (all editions) • Windows Server 2008 R2 (all editions) • Windows Server 2008 (all editions) • Windows 7 Professional • Windows 7 Enterprise
Volume License for Windows Server 2019	• Windows Server 2019 • Windows Server 2016 • Windows Server	• Windows Server Semi-Annual Channel • Windows Server 2019 (all editions) • Windows Server 2016 (all editions) • Windows 10 Enterprise LTSC/LTSC N/LTSB • Windows 10 Enterprise/Enterprise N

Details please check the link below:
Key Management Services (KMS) activation planning for Windows Server | Microsoft Docs

>>KMS activation thresholds:

Key Management Service activation thresholds

You can activate physical computers and virtual machines by contacting a KMS host. To qualify for KMS activation, there must be a minimum number of qualifying computers (called the activation threshold). KMS clients will be activated only after this threshold has been met. Each KMS host counts the number of computers that have requested activation until the threshold is met.

A KMS host responds to each valid activation request from a KMS client with the count of how many computers have already contacted the KMS host for activation. Client computers that receive a count below the activation threshold are not activated. For example, if the first two computers that contact the KMS host are running Windows 10, the first receives an activation count of 1, and the second receives an activation count of 2. If the next computer is a virtual machine on a computer running Windows 10, it receives an activation count of 3, and so on. None of these computers will be activated, because computers running Windows 10, like other client operating system versions, must receive an activation count of 25 or more. When KMS clients are waiting for the KMS to reach the activation threshold, they will connect to the KMS host every two hours to get the current activation count. They will be activated when the threshold is met.

In our example, if the next computer that contacts the KMS host is running Windows Server 2012 R2, it receives an activation count of 4, because activation counts are cumulative. If a computer running Windows Server 2012 R2 receives an activation count that is 5 or more, it is activated. If a computer running Windows 10 receives an activation count of 25 or more, it is activated.

Activation count cache

To track the activation threshold, the KMS host keeps a record of the KMS clients that request activation. The KMS host gives each KMS client a client ID designation, and the KMS host saves each client ID in a table. By default, each activation request remains in the table for up to 30 days. When a client renews its activation, the cached client ID is removed from the table, a new record is created, and the 30day period begins again. If a KMS client computer does not renew its activation within 30 days, the KMS host removes the corresponding client ID from the table and reduces the activation count by one. However, the KMS host only caches twice the number of client IDs that are required to meet the activation threshold. Therefore, only the 50 most recent client IDs are kept in the table, and a client ID could be removed much sooner than 30 days. The total size of the cache is set by the type of client computer that is attempting to activate. If a KMS host receives activation requests only from servers, the cache will hold only 10 client IDs (twice the required 5). If a client computer running Windows 10 contacts that KMS host, KMS increases the cache size to 50 to accommodate the higher threshold. KMS never reduces the cache size.

Details please check the link below:
[Activate clients running Windows 10 (Windows 10) - Windows Deployment | Microsoft Docs]

>>Key Management Services (KMS) client Setup Key(Generic Volume License Key (GVLK)):

Install a product key

If you are converting a computer from a KMS host, MAK, or retail edition of Windows to a KMS client, install the applicable product key (GVLK) from the list below. To install a client product key, open an administrative command prompt on the client, and run the following command and then press `Enter`:

Copy

```
slmgr /ipk <product key>
```

For example, to install the product key for Windows Server 2022 Datacenter edition, run the following command and then press `Enter`:

Copy

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

Generic Volume License Keys (GVLK)

In the tables that follow, you will find the GVLKs for each version and edition of Windows. LTSC is *Long-Term Servicing Channel*, while LTSB is *Long-Term Servicing Branch*.

Windows Server (LTSC versions)

Windows Server 2022

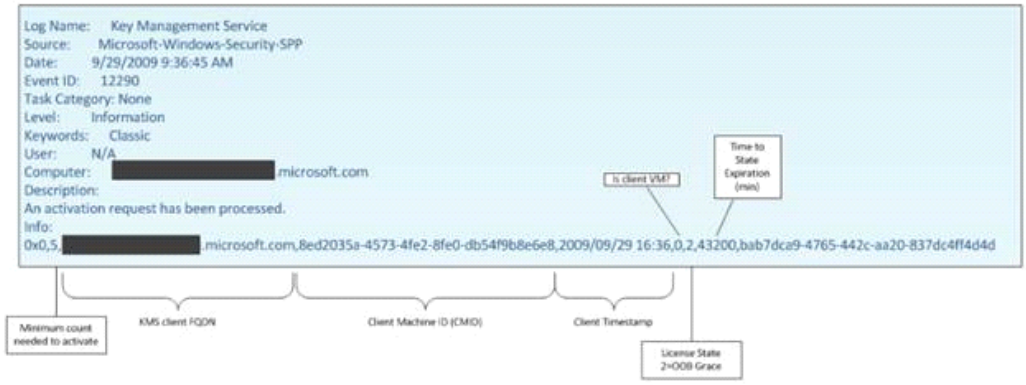
Operating system edition	KMS Client Product Key
Windows Server 2022 Datacenter	WX4NM-KYWYW-QJJR4-XV3QB-6VM33
Windows Server 2022 Standard	VDYBN-27WPP-V4HQT-9VMD4-VMK7H

Details please check the link below:
[Key Management Services (KMS) client activation and product keys for Windows Server and Windows | Microsoft Docs]

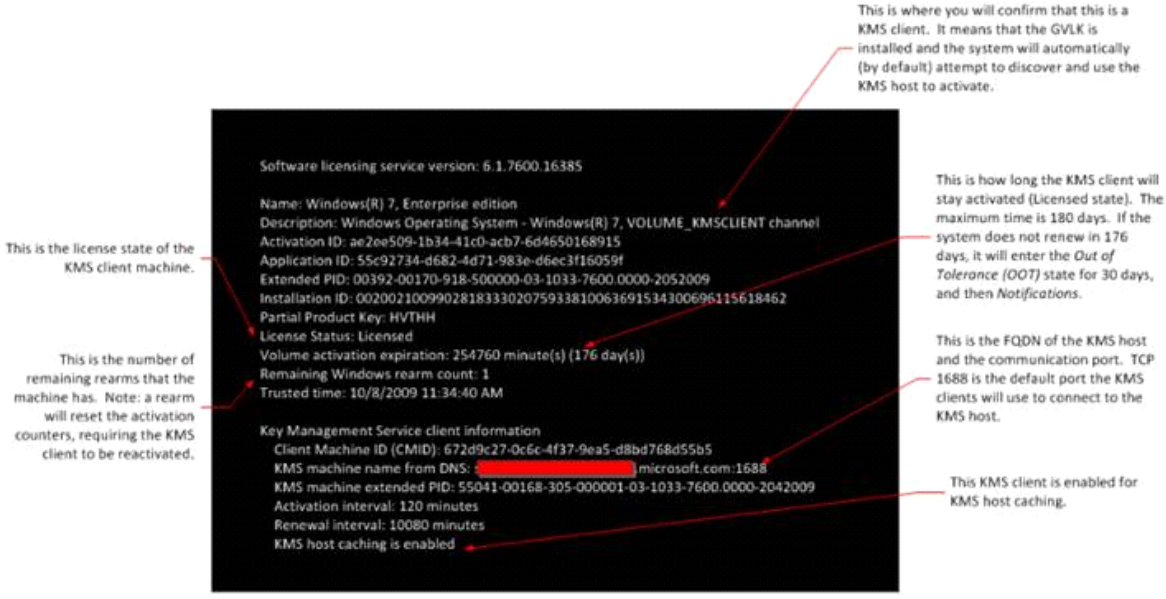
>>KMS host & client log checking:
The following screenshot shows the results of slmgr.vbs /dlv on one of our KMS hosts within Microsoft:

The KMS host logs Event ID 12290 when a KMS client contacts the host in order to activate. Event ID 12290 provides a significant amount of information that you can use

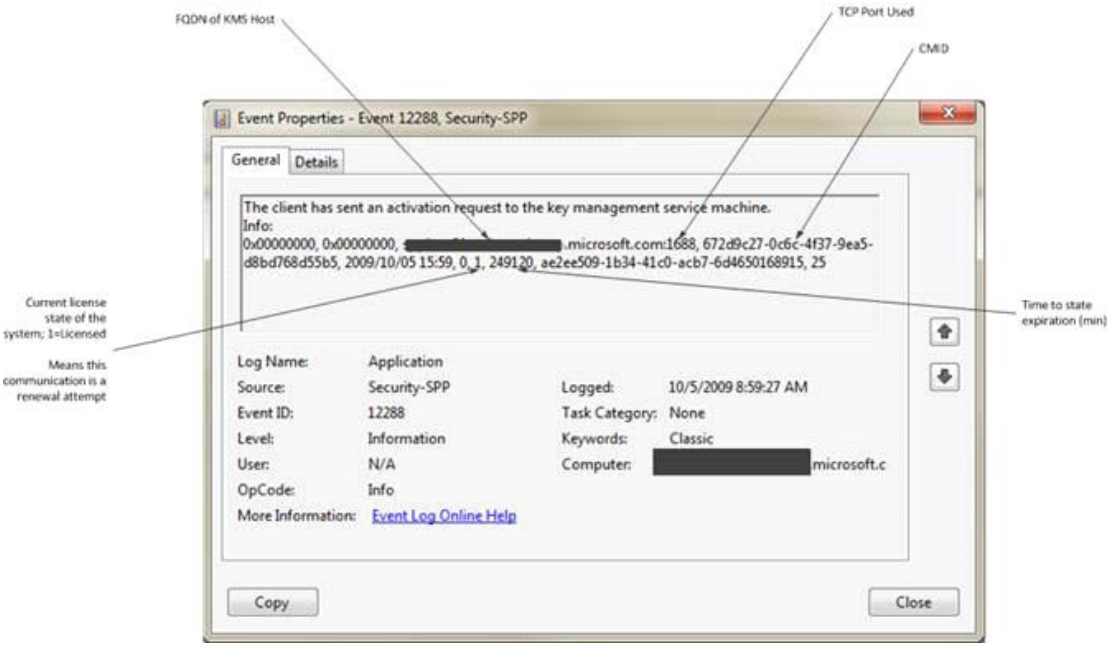
to figure out what kind of client contacted the host and why a failure occurred. The following segment of an event ID 12290 entry comes from the Key Management Service event log of our KMS host.



The following screenshot shows the results of slmgr.vbs /dlv on one of our KMS client machines:



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



Details please check the link below:
Guidelines for troubleshooting KMS | Microsoft Docs

>>Slmgr command:
Slmgr.vbs Options for Volume Activation | Microsoft Docs

>>How to configure the ADBA:
Active Directory-Based Activation vs. Key Management Services - Microsoft Tech Community

Activate using Active Directory-based activation (Windows 10) - Windows Deployment | Microsoft Docs

>>ESU Activation
Obtaining Extended Security Updates for eligible Windows devices - Microsoft Tech Community

【Additional documents for activation】

Thursday, August 18, 2022 2:20 PM

>>Activation Video links:
Xiaoyu Zhuang - Monday, August 28, 2017 3.05.58 PM.mp4
Xiaoyu Zhuang - Tuesday, August 29, 2017 1.39.34 PM.mp4

>>Activation All Documents for your reference:
Whampoa Military Academy - Activation - All Documents (sharepoint.com)

>>Activation Architecture: