Volume Activation 2.0 Operations Guide

for

Windows Vista® and Windows Server® 2008

Microsoft Corporation

Published: March, 2008

Abstract

Volume Activation 2.0 is designed to automate and manage the activation process for volume licensing customers. This document provides operational guidance for Microsoft Volume Licensing customers who have deployed Volume Activation 2.0 in their organization's environment.

Volume Activation 2.0 Operations Guide

Introduction

This guide contains information to assist you in managing the activations of volume editions of Windows Vista® and Windows Server® 2008 in your environment. Topics covered include available management tools, troubleshooting, recovery from unlicensed states, and resolving Non-Genuine issues, as well as specific information on managing each method of volume activation.

Management Tools for Volume Activation

There are several tools available to monitor and manage the activation status of volume license editions of Windows Vista and Windows Server 2008.

Volume Activation Management Tool (VAMT)

VAMT enables you to manage MAK-activated systems in your environment. VAMT collects data on both MAK Proxy and MAK Independent activation clients, including information about product keys and current license states. VAMT stores MAKs in a computer information list (CIL) file. This allows administrators to query the online Microsoft® Activation servers to determine the number of activations remaining on an organization's MAKs. The CIL is an XML file and is readable using any text editor, such as Notepad.

For more information about VAMT, see the **VAMT Step by Step Guide** that is included with the VAMT installation files. You can download VAMT at http://go.microsoft.com/fwlink/?LinkID=77533.

Systems Management Server (SMS) 2003 SP3

Systems Management Server (SMS) 2003 Service Pack 3 (SP3) contains built-in asset intelligence reporting, which utilizes Windows® Management Interface (WMI) to generate detailed activation reports for MAK- and KMS-activated Windows Vista and Windows Server 2008 computers.

Group Policy Support

There are no specific settings for volume activation in Group Policy. However, all configuration and property data for VA 2.0 is accessible though WMI and the Windows registry, and can therefore be managed with Group Policy.

Volume Activation Troubleshooting

All activation events are logged. The event provider name for all activation events is Microsoft-Windows-Security-Licensing-SLC. These events are saved to the Windows Application event log, except the KMS activity events that have the event number 12290. These events are saved to the Key Management Service log that is located in the **Applications and Services** folder.

You can use Slui.exe to display a description of most activation-related error codes. The following is the general syntax for this command:

```
Slui.exe 0x2a ErrorCode
```

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

```
Slui.exe 0x2a 0x8007267C
```

KMS Activation Troubleshooting Steps

The following table presents common issues that can occur during KMS activations and steps you can take to resolve these issues.

Table 1: Troubleshooting Steps for Common KMS Activation Issues

Issue	Resolution
Is the computer activated?	Look for **Windows is activated** in the Welcome Center or in the **System** application in Control Panel. You can also run **Slmgr.vbs** with the **/dli** parameter.
The computer will not activate.	Verify that the KMS activation threshold is met. Run **Slmgr.vbs** with the **/dli** parameter on the KMS host to determine the host's current count. Until the KMS host has a count of 25, Windows Vista clients do not activate. Windows Server 2008 KMS clients require a KMS count of 5 to activate. On the KMS client, look in the Application event log for event

Issue	Resolution
	12289. Check this event for the following: • Is the result code 0? Anything else is an error. • Is the KMS host name in the event correct? • Is the KMS port correct? • Is the KMS host accessible? • If the client is running a third-party firewall, do you need to configure the outbound port? On the KMS host, look in the KMS event log for event 12290. Check this event for the following: • Did the KMS host log a request from the client computer? Verify that the name of the KMS client is listed. Verify that the client and KMS host can communicate. Did the client receive the response? Ensure that routers do not block traffic using TCP port 1688, if you are using the default port, and that stateful traffic to the KMS client is allowed. • If no event is logged from the KMS client, the request did not reach the KMS host or the KMS host was unable to process it.
What does this error code mean?	If Slmgr.vbs returns a hexadecimal error code, or event 12288 contains a result code other than 0, determine the corresponding error message by running the following command: `Slui.exe 0x2a ErrorCode`
Clients are not adding to the KMS count.	You need to run `sysprep /generalize` or `slmgr /rearm` to reset the client computer ID (CMID) and other product activation information. Otherwise, each client computer looks identical and the KMS host does not count them as separate KMS clients.
KMS hosts are unable to create SRV records on a non-Microsoft DNS server.	Your DNS may restrict write access, or may not support dynamic DNS (DDNS). In this case, you need to give the KMS host write access to the DNS database or create the SRV record manually. For more information about this, see the *Volume Activation 2.0 Deployment Guide*.
Only the first KMS host is able to create SRV records on a Microsoft DNS server.	If you have more than one KMS host, the other hosts are not able to update the SRV record unless the SRV default permissions are changed. See. For more information about this, see the *Volume Activation 2.0 Deployment Guide*.
I installed a KMS key on the KMS	KMS keys should only be installed on KMS hosts and should not be installed on KMS clients. Run `slmgr.vbs -ipk <SetupKey>.`

Issue	Resolution
client.	The *Volume Activation 2.0 Deployment Guide* contains a table of setup keys that you can use to revert the computer back to a KMS client. These keys are publicly known and are edition-specific. Remember to delete any unnecessary SRV resource records from DNS and restart the computers.

MAK Activation Troubleshooting Steps

The following table presents common issues that can occur during MAK activations and steps you can take to resolve these issues.

Table 2: Troubleshooting Steps for Common MAK Activation Issues

Issue	Resolution
How can I tell if my computer is activated?	Look for **Windows is activated** in the Welcome Center or in the **System** application in Control Panel. You can also run **Slmgr.vbs** with the **/dli** parameter.
The computer will not activate over the Internet.	Ensure that the computer can access the Internet. Confirm and configure any necessary proxy settings, using either the Internet browser or Control Panel. If the computer is not able to connect to the Internet, use telephone activation.
Internet and telephone activation fail.	Contact your local activation center. For phone numbers of activation centers worldwide, go to http://go.microsoft.com/fwlink/?LinkID=107418. You need to provide your Volume License agreement information and proof of purchase when you call.
Slmgr.vbs /ato returns an error code.	If Slmgr.vbs returns a hexadecimal error code, determine the corresponding error message by running the following script: `Slui.exe 0x2a 0x ErrorCode`

Volume Activation Operations

KMS Health Monitoring

You can monitor KMS activations using the Key Management Service (KMS) Management Pack for System Center Operations Manager (Ops Mgr) 2005. The KMS Management Pack monitors the health of KMS hosts by checking for error conditions and availability. It alerts administrators about potential problems such as

KMS initialization failures, DNS SRV publishing issues, when KMS counts drop below activation thresholds, and when no KMS activity occurs for more than 8 hours.

To download the KMS Management Pack, go to the System Center Operations Manager product catalog at http://go.microsoft.com/fwlink/?LinkID=110332. This download includes a Management Pack guide that covers installation, configuration, and included rules. Several sample reports are also included, as well as data grooming and indexing processes.

KMS Activity Reporting

If an OpsMgr 2005 agent is installed on KMS hosts, the event log data generated on the KMS host is collected and forwarded to the Operations data warehouse. The data is then aggregated in the Operations data warehouse, so it is available for reports. Table 3 describes the reports that are included in the KMS Management Pack.

Table 3: Reports Included in the KMS Management Pack

Report Name	Description
Activation Count Summary	Displays the number of KMS activations for each Windows edition across a number of historical time ranges.
Virtual Machine Summary	Displays, by Windows edition, the number of virtual and physical KMS client computers that have activated in the past 14 days.
KMS Activity Summary	Displays new KMS activations for each Windows edition within the past day. You can display data from all KMS hosts or you can add a filter to display data from a subset of KMS hosts.
Licensing Status Summary	Displays the number of days left until a KMS client needs to renew its activation, as well as the license state for each KMS client that has connected to a KMS host.
Machine Expiration Chart	Displays the number of computers that are in an Initial/Out of Box (OOB), Out of time (OOT)/Expired, or Non-Genuine grace periods, and which could go to an unlicensed condition in the next 30 days.
Machine Expiration Detail	Lists the computers that are in Initial/Out of Box (OOB), Out of time (OOT)/Expired, or Non-Genuine grace periods and which could go to an RFM condition in the next 7 days.

Working with 64-Bit Windows Vista KMS Hosts

The OpsMgr 2005 agent is available only as a 32-bit application. As a result, 64-bit versions of Windows Vista RTM are not automatically added to the KMS computer group defined by the KMS Management Pack. KMS hosts running Windows Vista SP1 or Windows Server 2008 are not affected by this issue. Computers that are not a member of this group do not send data to Operations data warehouse. Since reports are generated from this data warehouse, computers with 64-bit versions of Windows Vista are not automatically included in KMS management pack reports.

To resolve this issue, you can create a custom Computer Group on the OpsMgr 2005 console and add the 64-bit Windows Vista RTM KMS hosts to it.

KMS Host Failover

If a KMS host fails, you must install a KMS key on a new host and activate it. You then need to ensure that the new KMS host has an SRV resource record in the DNS database. If you install the new KMS host with the same computer name and IP address as the failed KMS host, the new KMS host can use the DNS SRV record of the failed host. If the new host has a different computer name, you need to manually remove the DNS SRV record of the failed host. If your network is using DDNS, the new KMS host automatically creates a new SRV record in the DNS server. The new KMS host then starts collecting client renewal requests and begins activating clients as soon as the KMS activation threshold is met.

If your KMS clients are using auto-discovery, they automatically choose another KMS host if their original KMS host does not respond to renewal requests. If you are not using auto-discovery, you need to update the KMS client computers that were assigned to the failed KMS host.

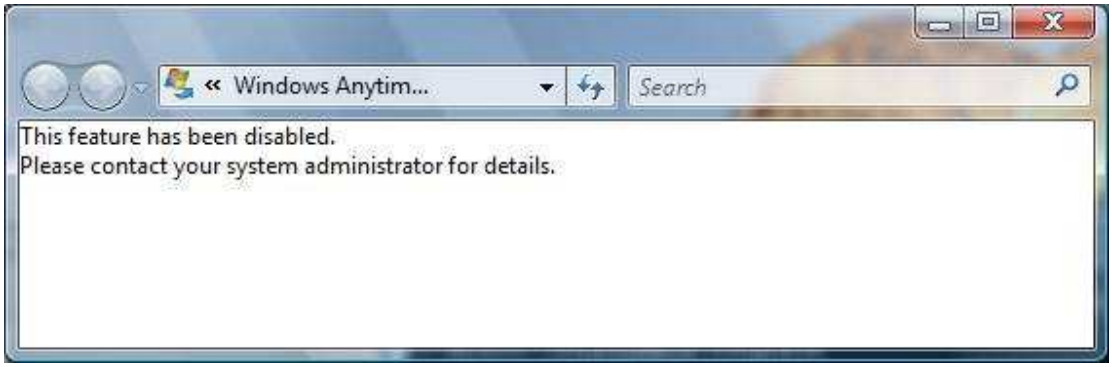
Disabling Windows Anytime Upgrade for Windows Vista

The Windows Anytime Upgrade (WAU) program allows Windows Vista Business users to purchase an upgrade directly from Microsoft by clicking the **Windows Anytime Upgrade** link in the **Extras and Upgrades** subfolder of the **All**

Programs menu. This link and the program are only in Windows Vista Business editions available through volume-licensed and retail channels.

System administrators can choose to disable WAU for users by adding a registry value to the reference image before deploying Windows. When WAU is disabled and the user clicks the WAU link, the error message, shown in Figure 1, appears. This prevents the user from obtaining an upgrade license using Control Panel.

Figure 1: Disabled WAU



Warning Some procedures in this section contain registry changes. Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To disable the WAU link

1. Log on to the client computer.
2. Open an elevated command prompt. To do this, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
3. At the command prompt, type **regedit.exe** and then press **Enter**.
4. Navigate to **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\WAU**. If needed, create the **Explorer** and **WAU** keys. To create the Explorer key, right-click the **Policies** key, point to **New**, and then click **Key**. Type **Explorer** as the name of the new key, and then press **Enter**. To create the Explorer key, right-click the new **Explorer** key, point to **New**, and then click **Key**. Type **WAU** as the name of the new key, and then press **Enter**.

To disable the WAU link

5. In the tree pane, click the **WAU** key. Right-click in the details pane, point to **New**, and then click **DWORD (32 bit) Value**.
6. Type **Disabled** as the name of the new value, and then press **Enter**.
7. Right-click the new **Disabled** value, and then click **Modify**.
8. In the **Value data box**, type **1** and then click **OK**.
9. Exit the registry editor.
10. Complete the reference image and deploy it using standard techniques.

Backup Requirements

Backup is not required for KMS hosts. However, if the event log is used to track or document KMS activations, periodically export the **Key Management Service** event log from the **Applications and Services Logs** folder. If you use a tool to perform routine cleanup of event logs, you can lose the activation history stored in the logs. If you use System Center Operations Manager 2005, the event log data is collected and stored in the Operations data warehouse for reporting, so no backups of the event log are necessary.

Managing License States

The display license information (**/dli**) parameter of Slmgr.vbs displays the current license state of Windows Vista and Windows Server 2008 computers. The output of this parameter also includes general information about the current license, time remaining before expiration, and time remaining in the grace period.

The following is an example of the information displayed when Slmgr.vbs /dli runs on a KMS client.

```
Name: Windows(TM) Vista, Enterprise edition
Description: Windows Operating System - Vista, ENVIRONMENT channel
Partial Product Key: RHXCM
License Status: Licensed
Volume activation expiration: 43162 minutes (29 days)
Evaluation End Date: 11/29/2007 4:59:59 PM
```

```
Key Management Service client information
    Client Machine ID (CMID): 45d450a8-2bef-4f04-9271-6104516a1b60
    DNS auto-discovery: KMS name not available from DNS
    KMS machine extended PID: 11111-00140-008-805425-03-1033-5384.0000-
1752006
    Activation interval: 120 minute(s)
    Renewal interval: 10080 minute(s)
```

The following is an example of the information displayed when Slmgr.vbs /dli runs on a KMS host.

```
Name: Windows(TM) Vista, Enterprise edition
Description: Windows Operating System - Vista, ENVIRONMENT channel
Partial Product Key: RHXCM
License Status: Licensed
Volume activation expiration: 43162 minutes (29 days)
Evaluation End Date: 11/29/2007 4:59:59 PM

Key Management Service is enabled on this machine
    Current count: 7
    Listening on Port: 1688
    DNS Publishing: Enabled
    KMS priority: Normal
```

More detailed licensing information is available using the **/dlv** parameter. The following is an example of the information displayed when Slmgr.vbs /dlv runs on a KMS host.

```
Software licensing service version: 6.0.5384.4
ActivationID: 14478aca-ea15-4958-ac34-359281101c99
ApplicationID: 55c92734-d682-4d71-983e-d6ec3f16059f
Extended PID: 11111-00140-009-000002-03-1033-5384.0000-1942006
Installation ID: 000963843315259493598506854253663081409973656140419231
```

Note Both the /dli and /dlv commands work when run on retail and OEM activated computers as well. For more information about available activation methods and possible license states, see the *Volume Activation 2.0 Deployment Guide*.

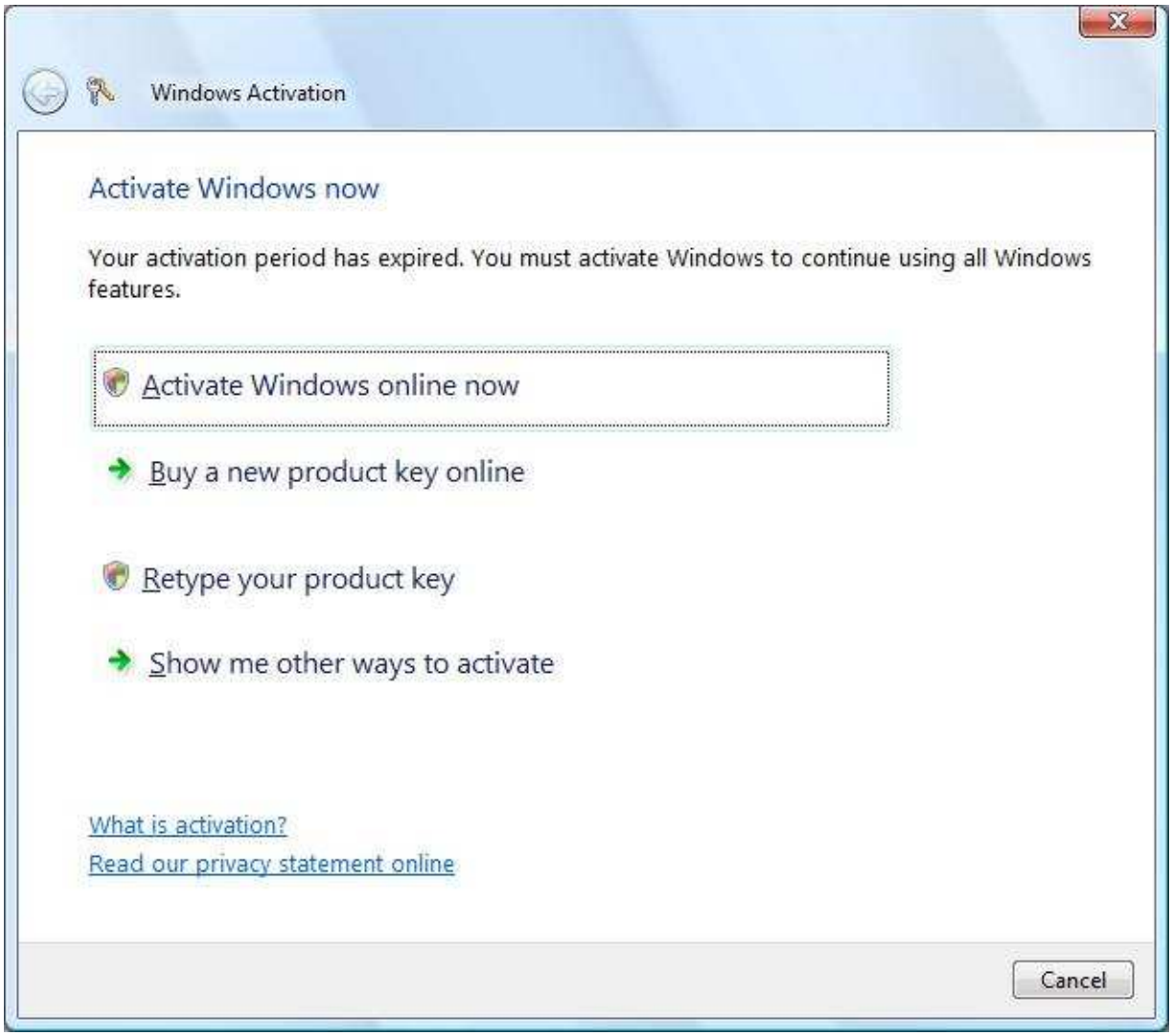
Recovery from an Unlicensed State

This section provides a description of the user experience when a Windows Vista or Windows Server 2008 computer falls into an unlicensed or notification state, and a description of the options to return the computer to a licensed state.

Recovering from RFM

RFM applies only to systems running instances of Windows Vista RTM. When a system is in RFM, upon logon the user is presented with a dialog box, shown in Figure 2. It is recommended that the system is either activated or transitioned to a grace period before applying Windows Vista Service Pack 1 (SP1).

Figure 2: RFM Dialog box (applicable only to Windows Vista RTM)



The option the user selects depends on the activation method desired.

- Clicking **Activate Windows online now** results in the system attempting to connect to either a KMS host or Microsoft hosted activation services, depending on whether the system is configured as a KMS client or has a MAK installed.
- Users who need to purchase a product key should click **Buy a new product key online**.
- Users who have another product key, such as a MAK, should click **Retype your product key**.
- Users who have no Internet connection should click **Show me other ways to activate** to use telephone activation. This option is not available if an Internet connection is detected on the system.

In Windows Vista SP1 and Windows Server 2008, RFM is removed from the product and replaced with a notifications-based experience.

You can return a client to its initial activation state for the current license by using the Slmgr.vbs script with the */rearm* option. This option resets the computer's activation timer and reinitializes some activation parameters, including a KMS client's client computer ID (CMID).

The number of times you can reset the activation timers is limited and depends on how many times **sysprep /generalize** is run to create the distribution media. The maximum number of possible resets for Windows Vista Business and Windows Server 2008 is three. You can reset Windows Vista SP1 Enterprise edition five times.

Recovering from a Non-Genuine State

If a KMS or MAK key is lost or misused, the product key can be marked Non-Genuine and invalid for activation. In this case, the product key checked during validation is considered invalid and the system fails validation. A watermark is added to the desktop and periodic notifications appear to remind the user to validate the license status of the system. In addition, the computer can be placed in a 30-day Non-Genuine state grace period. This allows for the time needed to obtain a new product key.

When evidence of system tampering is detected, the system goes into a Non-Genuine or tampered state depending on the tamper. If the computer has tampered files, the best way to recover is to reinstall the operating system and then reactivate. If a KMS host or KMS client is marked Non-Genuine due to a compromised product key, you should replace the KMS key on all KMS hosts configured with that key. You can then force an immediate reactivation of the KMS clients, using Slmgr.vbs /ato, or allow the clients to reactivate according to the activation renewal schedule. If the original key is compromised on a MAK-activated computer, you need to install a new MAK.

Before you can recover from a validation failure, you need to first determine why the computer failed validation, then you can take appropriate recovery steps. You

should first begin by examining the Application event log for Event ID 8209. The reason for the validation failure is listed in this event.

After a computer is reactivated, it must visit the Genuine Microsoft Software Web site at http://go.microsoft.com/fwlink/?LinkId=64187 for a validation to change the Non-Genuine state to Genuine.

Activation of Windows OEM Computers

Windows Vista and Windows Server 2008 have different usage rights based on the channel you use to purchase them. Generally, the product usage rights for Original Equipment Manufacturer (OEM) licensed products prohibit you from converting an OEM installation of an operating system to a volume licensed installation. However, there are exceptions. If one of the exceptions applies, you can change an OEM version of Window Vista or Windows Server 2008 to a volume licensed version.

One exception that allows you to change an OEM installation to a volume licensed installation is if you purchase Software Assurance within 90 days of purchasing the OEM product. This exception applies only to Windows Vista or Windows Server 2008. Another exception is if the OEM product is the same product for which you have a volume licensing agreement. Volume licensing customers have reimaging rights and may be eligible to upgrade an OEM installation using volume licensing media. For more information about imaging rights, see http://go.microsoft.com/fwlink/?LinkId=110334.

Computers obtained through OEM channels that have an ACPI_SLIC table in the system BIOS are required to have a valid Windows marker in the same ACPI_SLIC table. The appearance of the Windows marker is important for Volume License customers who are planning to use Windows Vista Volume License media to re-image or upgrade an OEM system through the re-imaging rights they have in their volume license agreement. Computers that have an ACPI_SLIC table without a valid Windows marker generate an error when a volume edition of Windows Vista is installed.

You cannot activate these systems with KMS, but you can activate them using a MAK or a retail key. You can also contact the OEM for a replacement motherboard

that contains a valid Windows marker in the ACPI_SLIC table or purchase new computers that have an operating system and a valid BIOS installed.

Appendix 1: WMI Software Licensing Classes and Properties

VA 2.0 uses Slmgr.vbs to make configuration changes. Slmgr.vbs uses WMI to access WMI classes and properties.

WMI Properties

Required Privilege: Standard User

Class	Name	Type	Description	Scope	Examples	Slmgr
SoftwareLicensingProduct	ApplicationID	string	The ID of current product's Application.	All	55c92734-d682-4d71-983e-d6ec3f16059f	
SoftwareLicensingProduct	Description	string	Product Description	All	Windows Operating System - Vista, VOLUME_KMSCLIENT channel	did
SoftwareLicensingProduct	EvaluationEndDate	datetime	The expiration date of this product's application. After this date, the LicenseStatus changes to Unlicensed, and the product cannot activate.	All	8/29/2007 4:59:59 PM [formatted]	dli
SoftwareLicensingProduct	GracePeriodRemaining	uint32	Remaining time in minutes before the parent application becomes unlicensed. For Volume clients, this is the remaining time before re-activation is required.	All	43193	dli
SoftwareLicensingProduct	ID	string	Product Identifier	All	14478aca-ea15-4958-ac34-359281101c9	did, ato
SoftwareLicensingProduct	LicenseDependsOn	string	The dependency identifier for the family of SKUs used to determine license relationships for add-ons.	All	14478aca-ea15-4958-ac34-359281101c8	
SoftwareLicensingProduct	LicenseFamily	string	The family identifier for the SKU used to determine license relationships for add-ons.	All	14478aca-ea15-4958-ac34-35928110112	
SoftwareLicensingProduct	LicenseIsAddon	boolean	Indicates true if the product is identified as an add-on license.	All	TRUE	

Class	Name	Type	Description	Scope	Examples	Slmgr
SoftwareLicensing Product	LicenseStatus	uint32	License status of this product's application. 0=Unlicensed, 1=Licensed, 2=OOBGrace, 3=OOTGrace, 4=NonGenuineGrace.	All	1	dli
SoftwareLicensing Product	MachineURL	string	Software licensing server URL for the binding certificate.	Retail, MAK, KMS	http://go.microsoft.com/fwlink/?LinkId=51099	dli
SoftwareLicensing Product	Name	string	Product Name	All	Windows(TM) Vista, Enterprise edition	ato, dli
SoftwareLicensing Product	OfflineInstallationId	string	Offline Installation Identifier of this product's application. Used for offline activation. Returns null if a product key is not installed.	Retail, MAK, KMS	000963843315259493598506854253663081409973656140419231	atp, dli
SoftwareLicensing Product	PartialProductKey	string	Last five characters of this product's key. Returns null if a product key is not installed.	All	RHXCM	dli
SoftwareLicensing Product	ProcessorURL	string	Software licensing server URL for the process certificate.	Retail, MAK, KMS	http://go.microsoft.com/fwlink/?LinkId=51098	dli
SoftwareLicensing Product	ProductKeyID	string	Product key ID. Returns null if a product key is not installed.	All	11111-00140-009-000002-03-1033-5378.0000-1262006	dli
SoftwareLicensing Product	ProductKeyURL	string	Software licensing server URL for the product certificate.	Retail, MAK, KMS	http://go.microsoft.com/fwlink/?LinkId=51100	dli
SoftwareLicensing Product	UseLicenseURL	string	Software licensing server URL for the user license.	Retail, MAK, KMS	http://go.microsoft.com/fwlink/?LinkId=51101	dli
SoftwareLicensing Service	ClientMachineID	string	The unique identifier for this KMS client computer. The KMS client generates CMID the first time it attempts to connect to the Key Management Service. CMID = NULL otherwise.	KMS client	387c843f-9cb6-4176-bfcd-82129c770b55	dli
SoftwareLicensing Service	IsKeyManagementServiceMachine	uint32	Indicates whether the computer has the Key Management Service enabled: 1 if true, 0 if false.	KMS	1	dli

Class	Name	Type	Description	Scope	Examples	Slmgr
SoftwareLicensingService	KeyManagementServiceCurrentCount	uint32	The count of currently active volume clients. -1 indicates the computer is not enabled as a Key Management Service or has not received any client licensing requests.	KMS	50	dli
SoftwareLicensingService	KeyManagementServiceFailedRequests	uint32	The total count of failed KMS requests.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceLicensedRequests	uint32	The count of KMS requests from clients with License Status 1=Licensed.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceMachine	string	The registered Key Management Service computer name. Returns null if SetKeyManagementServiceMachine has not been called.	KMS client	kms01.contoso.com	dli
SoftwareLicensingService	KeyManagementServiceNonGenuineRequests	uint32	The count of KMS requests from clients with License Status is 4=NonGenuineGrace.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceOOBGraceRequests	uint32	The count of KMS requests from clients with License Status 2=OOBGrace.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceOOTGraceRequests	uint32	The count of KMS requests from clients with License Status 3=OOTGrace.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceProductKeyID	string	Key Management Service product key ID. Returns null if not applicable.	KMS client	11111-00140-008-800002-03-1033-5358.0000-1102006	
SoftwareLicensingService	KeyManagementServiceTotalRequests	uint32	The total count of valid KMS requests.	KMS	50	dlv
SoftwareLicensingService	KeyManagementServiceUnlicensedRequests	uint32	The count of KMS requests from clients with License Status 0=Unlicensed.	KMS	50	dlv
SoftwareLicensingService	PolicyCacheRefreshRequired	uint32	A flag indicating whether the licensing policy-cache is stale. 1=Refresh required, 0=not required.	All	0	dli

Class	Name	Type	Description	Scope	Examples	Slmgr
SoftwareLicensingService	RequiredClientCount	uint32	The minimum number of clients required to connect to a Key Management Service computer to enable volume licensing.	KMS client	25	
SoftwareLicensingService	Version	string	Version of the Software Licensing service.	All	6.0.5378.0	dlv
SoftwareLicensingService	VLActivationInterval	uint32	The activation frequency, in minutes, of how often the current computer should contact the Key Management Service computer before the client is licensed.	KMS, KMS client	120	dli
SoftwareLicensingService	VLRenewalInterval	uint32	The renewal frequency, in minutes, of how often the current computer should contact the Key Management Service computer after the client is licensed.	KMS, KMS client	10080	dli

New Properties only in Windows Vista SP1 and Windows Server 2008

SoftwareLicensingService	LicenseStatusReason	uint32	The reason HRESULT for the current license status.	All	0xHC004F009	
SoftwareLicensingProduct	LicenseStatus	uint32	License status of this product's application. 0=Unlicensed, 1=Licensed, 2=OOBGrace, 3=OOTGrace, 4=NonGenuineGrace, 5=Notification	All	1	dli
SoftwareLicensingService	KeyManagementServiceNotificationRequests	uint32	The count of KMS requests from clients with License Status 5=Notification.	KMS	50	dlv

WMI Methods

These apply to all licensing, not just volume licensing.

Required Privilege: Administrator

Note: This is enforced by the Software Licensing Service and registry ACLs. A registry override in Windows Vista allows a standard user to call specific methods. These are designated with (*) after the method's name. To do this, an administrator must create and set the following new registry value:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL

Value Name: UserOperations

Type: DWORD

Value Data: 1

Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

Class	Name	Type	Parameters	Description	Scope
SoftwareLicensingService	InstallProductKey*	unit32	[in] string ProductKey	Install a product key.	All
SoftwareLicensingService	InstallLicense*	uint32	[in] string License	Install a license for the current product.	All
SoftwareLicensingService	InstallLicensePackage*	uint32	[in] string LicensePackage	Install a license package for the current product.	All
SoftwareLicensingService	SetKeyManagementServiceMachine	uint32	[in] string MachineName	Sets the name of the Key Management Service computer to use for Volume Activation.	KMS client
SoftwareLicensingService	ClearKeyManagementServiceMachine	uint32		Clear Key Management Service computer name.	KMS client
SoftwareLicensingService	SetVLActivationInterval	uint32	[in] uint32 ActivationInterval	The activation frequency, in minutes, of how often the current computer should contact the Key Management Service computer before the client is licensed. The frequency must be greater than or equal to 15 and less than or equal to 43200. An error is returned if the method is called and the computer is not a Key Management Service.	KMS

Class	Name	Type	Parameters	Description	Scope
SoftwareLicensingService	SetVLRenewalInterval	uint32	[in] uint32 RenewalInterval	The renewal frequency, in minutes, of how often the current computer should contact the Key Management Service computer after the client is licensed. The frequency must be greater than or equal to 15 and less than or equal to 43200. An error is returned if the method is called and the computer is not a Key Management Service.	KMS
SoftwareLicensingService	ClearProductKeyFromRegistry	uint32		Clear product key from the registry.	All
SoftwareLicensingService	ReArmWindows*	uint32		Reset the licensing status of the computer.	All
SoftwareLicensingService	RefreshLicenseStatus*	uint32		Update the licensing status of the computer so that applications have access to current licensing information.	All
SoftwareLicensingService	AcquireGenuineTicket	uint32	[in] string TemplateId, [in] string ServerUrl	Acquire a Genuine ticket online.	All
SoftwareLicensingProduct	UninstallProductKey	unit32		Uninstall this product's key.	All
SoftwareLicensingProduct	Activate*	uint32		Activate this product.	All except OEM_SLP
SoftwareLicensingProduct	DepositOfflineConfirmationId*	uint32	[in] string InstallationId	Activates this product by depositing an Offline Confirmation Identifier for this product when performing a telephone activation.	Retail, MAK, KMS

KMS Registry Keys / Values

Registry path: **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**

Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL			
Value	**Type**	**Description**	**Scope**
DisableDnsPublishing	REG_DWORD	Set this to a non-zero value to block auto-publishing to DNS.	KMS
EnableKmsLowPriority	REG_DWORD	Set this to a non-zero value to minimize contention from KMS in a co-hosted environment. Note that this could lead to KMS starvation, depending on what other applications or server roles are active. Use with care.	KMS
KeyManagementServiceName	REG_SZ	Set this value to force the use of a specific KMS system by the KMS client. No default. (Note: slmgr -skms <KMS> sets this.)	KMS client
KeyManagementServicePort	REG_SZ	Set this to force the use of a specific TCP port by the KMS client when it communicates with a KMS. No default.	KMS client
KeyManagementServiceListeningPort	REG_SZ	Set this on the KMS computer to cause clients using DNS auto-discovery to communicate over this port. No default.	KMS
DnsDomainPublishList	REG_MULTI_SZ	Create a list of fully qualified domains that KMS will use to auto-publish its SRV record. The KMS home domain is always used, so it is not necessary to include it here. This depends on the DisableDnsPublishing setting.	KMS
VLActivationInterval	REG_DWORD	This is set initially on both MSC server and client sides. Default = 120 (in minutes, 2 hours). WMI supports set method, but only works on KMS-enabled computer. KMS client initially picks up this interval from registry, but switches to KMS setting after it receives the first KMS response.	KMS
VLRenewalInterval	REG_DWORD	This is set initially on both MSC server and client sides. Default = 10080 (in minutes, 7 days.). WMI supports set method, but only works on KMS-enabled computer. KMS client initially picks up this interval from registry, but switches to KMS setting after it receives the first KMS response.	KMS

Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL			
Value	**Type**	**Description**	**Scope**
KeyManagementServiceVersion	REG_SZ	Set this for MOM automatic discovery of the Key Management Service (current default is to use the WMI SoftwareLicensingService Version property). Delete this value if the KMS is no longer functional on the computer.	KMS
UserOperations	REG_DWORD	Create and set to 1 to enable standard users to install product keys, activate, and rearm computers. With this registry setting enabled, all product key installation, activation, and rearm requests must be done using the built-in Slmgr.vbs script.	All (not just KMS)

Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation			
Value	**Type**	**Description**	**Scope**
Manual	REG_DWORD	0 = Allow Auto-activation (Default) 1 = Disable Auto-activation	All (not just KMS)
NotificationDisabled	REG_DWORD	0 = Activation notices and balloons will be shown (Default) 1 = All activation related notices will be hidden. Not recommended.	All (not just KMS)

Registry path: HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL This is physically under HKUsers\S-1-5-20\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL (S-1-5-20 is well-known NetworkService SID)			
Value	**Type**	**Description**	**Scope**
KeyManagementServiceRegisteredDomainName	REG_SZ	Cached Domain name when KMS is enabled. This is mainly used when KMS computer domain is changed so it re-publishes DNS RR. No default. This is a KMS-side registry setting.	KMS
KeyManagementServiceRegisteredHostName	REG_SZ	Cached host name when KMS is enabled. This is mainly used when KMS computer name is changed so it re-publishes DNS RR. No default. This is a KMS-side registry setting.	KMS

Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL			
Value	**Type**	**Description**	**Scope**
KeyManagementServiceRegisteredPortNumber	REG_SZ	Cached port number when KMS is enabled. This is mainly used when KMS computer name is changed so it re-publishes DNS RR. No default. This is KMS side registry setting.	KMS
DiscoveredKeyManagementServiceName	REG_SZ	Cached KMS computer name through discovery on KMS client. No default.	KMS client
DiscoveredKeyManagementServicePort	REG_SZ	Cached KMS port number through discovery on KMS client. No default.	KMS client
CustomerPID	REG_SZ	This is CSVLK PIDX, cached after KMS client is activated. This is for use by Customer Support Services. No default.	KMS client

KMS Events Logged in Windows Event Log

Log file name (except 12290): Windows Applications Logs

Log file name 12290): Applications and Services Logs\Key Management Service

Event provider name: Microsoft-Windows-Security-Licensing-SLC

Source name: Software Licensing Service

Event ID	Logged By	Description	Message	Parameters Fields included in comma-delimited string		Examples
				Name	**Description**	
12288	Client	Request generation failure or after RPC submit (client)	The client has sent an activation request to the key management service computer.%nInfo:%n%1	HRESULT	Return code	0x0,
				Status	Flags (note 1)	0x8,

Event ID	Logged By	Description	Message	Parameters Fields included in comma-delimited string		Examples
				Server:Port	Name:port	kms01.contoso.com:1688
				CMID	Client Machine ID	08c3bda0-c556-4b61-9e4e-7bf6d4df80be,
				Client Time	Request timestamp	2006/1/14 2:30,
				VM Info	Unused	1,
				Licensing Status	License status 0 - Unlicensed 1 - Licensed (Activated) 2 - OOB grace 3 - OOT grace 4 - NonGenuineGrace	2,
				Time to Expiration	Time remaining (minutes)	40123,
				ActID	Activation ID - identifies the license	cf67834d-db4a-402c-ab1f-2c134f02b700,
				N-Policy	Minimum count client needs to activate	25
12289	Client	After KMS response validation (client)	The client has processed an activation response from the key management service computer.%nInfo:%n%1	HRESULT	Return code	0x0,
				Status	Flags (note 1)	0x4000008,
				fBound	Activated flag	0,
				Unused	Unused - ignore	0,
				Count	KMS current count	4,
				Activation Interval	Request interval when not activated (minutes)	120,
				Renewal	Request interval	10080,

Event ID	Logged By	Description	Message	Parameters Fields included in comma-delimited string		Examples
				Interval	when activated (minutes)	
				Client Time	Request timestamp	1/14/2006 2:30
12290	KMS	KMS server side log for each request	An activation request has been processed.%nInfo:%n%1	HRESULT	Return code	0x0,
				N-Policy	Client product minimum count needed to activate	25,
				Machine	Client computer name	kms03.site5.contoso.com,
				CMID	Client Machine ID	e5c98033-aab6-4d0b-9af9-1d399597dd56,
				Client Time	Request timestamp	2006/1/14 22:36,
				VM Info	Client OS is running in a virtual machine	1,
				Licensing Status	License status 0 - Unlicensed 1 - Licensed (Activated) 2 - OOB grace 3 - OOT grace, 4 - NonGenuineGrace	2,
				Time to Expiration	Time remaining (minutes)	40123,
				ActID	Activation ID - identifies the license	cf67834d-db4a-402c-ab1f-2c134f02b700
12291	KMS	KMS initialization failure	Volume-licensed client was unable to initialize the Key Management Service renewal timer.%nInfo:%n%1	HRESULT	Return code	

Event ID	Logged By	Description	Message	Parameters Fields included in comma-delimited string		Examples
12292	KMS	Renewal timer initialization failure	Key Management Service (KMS) failed to initialize renewal timer.%nInfo:%n%1	HRESULT	Return code	
12293	KMS	DNS RR publishing failure	Publishing the Key Management Service (KMS) to DNS in the '%2' domain failed.%nInfo:%n%1	P1: HRESULT P2: DNS domain	P1: Return code P2: DNS domain name	
12294	KMS	DNS RR publishing success	Publishing the Key Management Service (KMS) to DNS in the '%1' domain is successful.%n	DNS domain	DNS domain name	

Flags:

SL_VL_BINDING_STATUS_OTHER_PC	0x00000008
SL_VL_BINDING_ERROR_NO_BINDING_SERVER_REGISTRATION	0x01000000
SL_VL_BINDING_ERROR_INVALID_REGISTRATION_DATA_TYPE	0x02000000
SL_VL_BINDING_ERROR_NOT_ENOUGH_COUNT	0x04000000
SL_VL_BINDING_ERROR_NOT_WINDOWS_SLP	0x08000000

The first one is just a warning: It's set for E_SLP_MISSING_ACPI_SLIC for OEM check. The others are error code status codes.

KMS RPC Messages

RPC Request

Name	Type	Size [bytes]	Description
Version	DWORD	4	Version control of request
VMInfo	DWORD	4	Virtual machine instance if non-zero

Name	Type	Size [bytes]	Description
LicenseStatus	DWORD	4	Licensing status 0 - Unlicensed 1 - Licensed (Activated) 2 - OOB grace 3 - OOT grace 4 - NonGenuineGrace
BindingExpiration	DWORD	4	Interval until expiration (minutes)
AppID	UUID	16	Application ID
ActID	UUID	16	Activation configuration ID (Product)
KMSID	UUID	16	Key Management Service ID
CMID	UUID	16	Client machine ID
N-Policy	DWORD	4	N count policy
ClientTime	FILETIME	8	Client request timestamp
CMID_prev	UUID	16	Previous client machine ID
MachineName	STRING	128	Client computer's fully qualified domain name
MAC	BLOB	16	MAC blob of all above data
Total		**252**	**Request size**

RPC Response

Name	Type	Size [bytes]	Description
Version	DWORD	4	Version control of request
PID Size	DWORD	4	Size of PID
PID Data	BYTE	Variable	KMS Product Key ID. Unicode string including null terminator (example: "11111-00116-106-000474-00-1033-5231.0000-2782005" size: 98 (0x62))
CMID	UUID	16	Client machine ID
ClientTime	FILETIME	8	Client request timestamp
Count	DWORD	4	Current KMS count
VLActivationInterval	DWORD	4	Activation interval policy

Name	Type	Size [bytes]	Description
VLRenewalInterval	DWORD	4	Renewal interval policy
MAC	BLOB	16	MAC blob of all above data
Total		**60 + PID (70+98=158 for example)**	

Appendix 2: Troubleshooting by Error Code

The following table provides troubleshooting help when using volume editions of Windows Vista and Windows Server 2008 operating systems.

Error Code	Error Message	Activation Type	Possible Cause	Troubleshooting Steps
0xC004C001	The activation server determined the specified product key is invalid	MAK	Invalid MAK entered.	Verify the key is the MAK provided by Microsoft. Contact the Microsoft Activation Call Center to verify the MAK is valid.
0xC004C003	The activation server determined the specified product key is blocked	MAK	The MAK is blocked on the activation server.	Contact the Microsoft Activation Call Center to obtain a new MAK and install/activate the system.
0xC004B100	The activation server determined that the computer could not be activated.	MAK	The key is unsupported.	Verify the key is the MAK provided by Microsoft. Contact the Microsoft Activation Call Center to verify MAK is valid.
0xC004C008	The activation server determined that the specified product key could not be used.	KMS	The KMS key has exceeded the activation limit.	KMS keys will activate up to 10 times, on 6 different computers. If more activations are necessary, contact the Microsoft Activation Call Center.
0xC004C020	The activation server reported that the Multiple Activation Key has exceeded its limit.	MAK	The MAK has exceeded the activation limit.	MAKs by design have a limited number of activations. Contact the Microsoft Activation Call Center to obtain a new MAK or increase the limit on existing MAK.
0xC004C021	The activation server reported that the Multiple Activation Key extension limit has been exceeded.	MAK	The MAK has exceeded the activation limit.	MAKs by design have a limited number of activations. Contact the Microsoft Activation Call Center to obtain a new MAK or increase the limit on the existing MAK.
0xC004F009	The software Licensing Service reported that the grace period expired.	MAK	Grace period expired before system was activated, now system is in RFM mode.	Follow the Reduced Functionality Mode (RFM) recovery guidelines in the *Volume Activation 2.0 Operations Guide*.
0xC004F00F	The Software Licensing Server reported that the	MAK/KMS client/KMS	The hardware has changed or	MAK - Reactivate the system during the Out of Tolerance grace period using either online or phone

Error Code	Error Message	Activation Type	Possible Cause	Troubleshooting Steps
	hardware ID binding is beyond level of tolerance.	host	the drivers were updated on the system.	activation.[1] KMS – Reboot or run *slmgr.vbs /ato*[2]
0xC004F014	The Software Licensing Service reported that the product key is not available	MAK/KMS client	No product keys are installed on the system.	Install MAK product key or install KMS Setup key found in \sources\pid.txt on the installation media.
0xC004F02C	The software Licensing Service reported that the format for the offline activation data is incorrect.	MAK/KMS client	The system has detected that the data entered during phone activation is not valid.	Verify Confirmation ID is correctly entered.
0xC004F035	The software Licensing Service reported that the computer could not be activated with a Volume license product key. Windows Vista Volume licensed systems require upgrading from a qualified operating system. Please contact your system administrator or use a different type of key.	KMS client/KMS host	Windows Vista Volume editions are licensed for upgrade only. Installing a Volume OS on a computer that does not have a qualifying OS installed is not supported.	Install a qualifying version of a Microsoft OS, and then reinstall the Volume OS.
0xC004F038	The software Licensing Service reported that the computer could not be activated. The count reported by your Key Management Service (KMS) is insufficient. Please contact your system administrator.	KMS client	Count on KMS host is not high enough. KMS count must be ≥5 for Windows Server 2008 or ≥25 for Windows Vista.	More physical computers are needed in the KMS pool (minimum of 5 for Windows Server 2008 or 25 for Windows Vista) for KMS clients to activate. Run *Slmgr.vbs /dli* to get current count on the KMS host.
0xC004F039	The software Licensing Service reported that the	KMS client	This error is occurs when a	Troubleshoot the network connection between the KMS and the client. Make sure that TCP-1688

[1] *SLUI 4* displays the list of telephone numbers for telephone activation.

[2] Run S*lmgr.vbs* commands from an elevated command prompt using **Run as administrator**.

Error Code	Error Message	Activation Type	Possible Cause	Troubleshooting Steps
	computer could not be activated. The Key Management Service (KMS) is not enabled.		KMS request is not answered.	(default) is not blocked by a firewall or otherwise filtered.
0xC004F041	The software Licensing Service determined that the Key Management Server (KMS) is not activated. KMS needs to be activated.	KMS client	KMS host is not activated.	Activate the KMS host with either online or phone activation.
0xC004F042	The software Licensing Service determined that the specified Key Management Service (KMS) cannot be used.	KMS client	Mismatch between KMS client and KMS host.	Check that a Beta client is not activating against a Released KMS host, or a Released client against a Beta KMS host.
0xC004F050	The Software Licensing Service reported that the product key is invalid.	KMS, KMS client, MAK	This can be caused by a typo in the KMS key, or by typing in a Beta Key on a Released version of the OS.	Install the appropriate KMS key on the corresponding version of Windows. Check the spelling. If the key is being copied and pasted, make sure that em-dashes have not been substituted for the dashes in the key.
0xC004F051	The software Licensing Service reported that the product key is blocked.	MAK/KMS	The product key on the activation server is blocked by Microsoft.	Obtain a new MAK/KMS key, install it on the system, and activate.
0xC004F064	The software Licensing Service reported that the non-Genuine grace period expired.	MAK	Windows Genuine Advantage has determined the system is not Genuine.	Follow the Non-Genuine RFM recovery guidelines in the *Volume Activation 2.0 Operations Guide*.
0xC004F065	The software Licensing Service reported that the application is running within	MAK/KMS client	Windows Genuine Advantage has	Obtain and install a Genuine product key and activate the system during the grace period. If not, the system will go into Non-Genuine RFM mode at

Error Code	Error Message	Activation Type	Possible Cause	Troubleshooting Steps
	the valid non-genuine period.		determined the system is not Genuine. The system will continue to run during the Non-Genuine grace period.	the end of the grace period.
0xC004F066	The Software Licensing Service reported that the product SKU is not found.	MAK/KMS client	Volume media has been used with a non-Volume key.	Match the product key to the OS edition. Contact the Product Activation Call Center for assistance.
0xC004F069	The Software Licensing Service reported that the computer could not be activated. The Key Management Service (KMS) determined that the request timestamp is invalid.	KMS client	The system time on the client computer is too different from the time on the KMS host.	Time sync is important to system and network security for a variety of reasons. Fix this issue by changing the system time on the client to sync with the KMS. Use of an NTP time source or AD for time synchronization is recommended. This issue uses UTP time, and is independent of Time Zone selection.
0x80070005	Access denied. The requested action requires elevated privileges.	KMS client/MAK /KMS host	UAC (User Access Control) prohibits activation processes from running in a non-elevated command prompt.	Run *slmgr.vbs* from an elevated command prompt. Right-click cmd.exe and choose "Run as Administrator".
0x8007232A	DNS server failure.	KMS host	The system has network or DNS issues.	Troubleshoot network and DNS.
0x8007232B	DNS name does not exist.	KMS client	The KMS client cannot find KMS SRV resource records in DNS.	1. Point the KMS client to KMS host using slmgr.vbs /skms <kmshostname> 2. Install KMS host. 3. Obtain a MAK and change the product key then activate the system. 4. Troubleshoot DNS.

Error Code	Error Message	Activation Type	Possible Cause	Troubleshooting Steps
0x800706BA	The RPC server is unavailable.	KMS client	Firewall settings are not configured on the KMS host or DNS SRV records are stale.	Ensure the KMS port is allowed access through the firewall on the KMS host or ensure SRV records point to a valid KMS host. Troubleshoot network connections.
0x8007251D	No records found for DNS query.	KMS client	The KMS client cannot find KMS SRV resource records in DNS.	Troubleshoot network connections and DNS.