

Windows Vista

Volume Activation 2.0 Step-By-Step Guide

Microsoft® Corporation

Published: October, 2006 (last updated 11/29/06)

Purpose

This guide provides planning, deployment, and operational guidance for activating volume editions of the Windows Vista™ operating system.

Who Should Use the Volume Activation 2.0 Step-by-Step Guide?

This guide is targeted at IT professionals who are responsible for deploying and managing Windows Vista deployment.

Information in this document, including URL and other Internet Web site references, is subject to change without notice.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveX, Windows, Windows 2000, Windows Server, Windows Vista, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
Problem.....	1
Volume Activation 2.0 Solution	1
Volume Activation 2.0 Overview.....	2
Planning Guidance	3
Prepare	3
Product Activation Types.....	3
Target Environment Considerations	5
User Connectivity Considerations.....	7
Map Computers to Activation Solutions	8
Plan Monitoring and Reporting	9
Plan Support	10
Deployment Example.....	10
Deployment Example for MAK Independent Activation and KMS Activation	10
Deployment Example for MAK Proxy Activation.....	12
Media Considerations.....	13
Product Key Deployment Considerations.....	14
Obtaining Volume License Keys.....	15
Deployment Guidance.....	16
General Considerations for Windows Vista	16
Tools under Development.....	16
Administrative Credentials.....	16
MAK Activation	17
Prerequisites for MAK Activation.....	17
Known Issues for MAK Activation.....	17
Steps for Installing and Activating MAK Clients.....	17
KMS Activation	23
Prerequisites for KMS Activation.....	24
Known Issues for KMS Activation.....	24
Steps for Installing, Configuring, and Deploying KMS Activation.....	24
Operational Guidance	32
Built-in Scripting Support	32
Remote Scripting Support	32
Microsoft Key Management Service MOM Pack.....	33
Known Issues with the MOM Pack.....	34
KMS Health Monitoring.....	34
KMS Activity Reporting	34
Backup Requirements	34

Group Policy Support	35
Disabling Windows Anytime Upgrade	35
Display Volume license Information	36
Software Asset Management.....	37
Troubleshooting.....	38
MAK Activation Troubleshooting Steps.....	38
KMS Activation Troubleshooting Steps.....	38
KMS Activation of OEM Computers.....	40
Mapping Error Codes to Text Messages	40
Reviewing Activation Events	40
WMI Providers	Error! Bookmark not defined.
Resolving Reduced Functionality Mode	41
Appendix 1: Resolving Non-Genuine Issues on Computers	44
Recovering Non-Genuine Windows Vista Computers	44
Recovery from Non-Genuine State Due to Tampered Files.....	45
Recovery from Non-Genuine State for Invalid or Blocked Product Key.....	45
Appendix 2: Recovery from RFM using Standard User Product Activation Web Page	47
Appendix 3: Resolving MOM 2003 Installation Issue.....	50
Appendix 4: Guidance Worksheet Job-Aid.....	51
Appendix 5: Understanding License States	52
Additional Resources	54

Introduction

Problem

Software piracy is a problem that is increasing every year, despite a range of efforts to combat it. In May 2006, the Business Software Alliance, a leading software industry forum, reported that 35 percent of all software installed worldwide during 2005 was pirated or unlicensed. Piracy on this scale continues to create great challenges for Microsoft[®] Corporation, and affects consumers, partners, and the industry.

While the financial impact on the software industry and the consumers who are defrauded by counterfeit software are serious, there are also impacts that go beyond dollars. Many consumers who end up with a counterfeit copy of Microsoft software are unwitting victims of a crime. They believe that they purchased a properly licensed copy, often have documents to back up the purchase, and yet their copy of Microsoft Windows[®], Microsoft Office, or Windows Server[®] is not properly licensed. In addition, counterfeit software is increasingly becoming a vehicle for the distribution of viruses and malicious software (also called malware) that can target unsuspecting users, potentially exposing them to corruption or loss of personal or business data and identity theft.

For these reasons, Microsoft continually invests in technologies and programs to help protect consumers and businesses from the risks and hidden costs of counterfeit and unlicensed software.

Volume Activation 2.0 Solution

Volume Activation 2.0 is a new requirement in the Windows Vista™ operating system and Windows Server® Code Name "Longhorn," which requires activation of each Windows Vista license acquired under a Volume License agreement. When designing and building the new volume activation technologies, Microsoft focused on two goals:

- Close significant piracy loopholes (Volume License keys represent majority of the keys that are involved in Windows piracy.)
- Improve the volume customer experience.

Volume Activation 2.0 is designed to help increase protection and to help better manage the Volume License keys in managed and non-managed environments as well as provide flexible deployment options for customers. The process is transparent for end users, and the Volume Activation 2.0 solution works in a variety of customer environments.

Benefits of Volume Activation 2.0

Volume Activation 2.0 supports centrally managed Volume License keys. The Key Management Service (KMS) key used for KMS activation is only installed on the KMS host and never on individual computers. The Multiple Activation Key (MAK), although resident on the individual computer, is encrypted and kept in a trusted store so that users are not exposed to the key and are not able to obtain the key once it has been installed on the computer.

Volume Activation 2.0 supports a simplified setup and is generally invisible to the customers. By default, Volume editions do not require a product key to be entered during setup. The computer must be activated during an automatic 30-day grace period.

System Administrators can count KMS activations using standard system management software, for example, Microsoft Operations Manager (MOM) and others in the future. Windows Management Infrastructure (WMI), extensive event logging, and built-in Application Programming Interfaces (APIs) may provide a wealth of detail about installed licenses and about the license state and current grace or expiration period of MAK and KMS-activated computers.

Volume Activation 2.0 also may provide enhanced security through frequent background validations for Genuine modules. This is currently limited to critical software, but may be expanded greatly over time.

Volume Activation 2.0 Overview

Volume Activation 2.0 provides a simple and security-enhanced activation experience for enterprise customers, while addressing issues associated with Volume License keys in the previous versions of Windows and may reduce risks of leakage to both Microsoft and its customers. Volume Activation 2.0 provides system administrators the ability to centrally manage and protect product keys, in addition to several flexible deployment options to activate the computers in the environment regardless of the size of the environment. In the future, Volume Activation 2.0 will also provide the basis for an easy-to-use, comprehensive, integrated activation process that will support both Microsoft and third-party applications. Volume Activation 2.0 is also the starting point for a strong software asset management system that will deliver immediate and future benefits.

Volume Activation 2.0 provides customers with two types of keys and three methods of activation. Customers are free to use any or all of the options, constrained only by their organization's needs and network infrastructure.

- Multiple Activation Key (MAK)
 - MAK Proxy Activation
 - MAK Independent Activation
- Key Management Service (KMS) Key
 - KMS Activation

Planning Guidance

This section of the *Volume Activation 2.0 Step-by-Step Guide* provides guidance on planning and determining the appropriate Volume Activation 2.0 options for their environment. The process consists of the following four steps:

1. Prepare
2. Map Computers to Activation Solutions
3. Plan monitoring and reporting
4. Plan Support



Prepare

This first step of selecting an appropriate Volume Activation 2.0 option involves considering the following:

- Product activation types
- Target environment considerations
- User connectivity considerations

Product Activation Types

There are three basic types of activation for Windows Vista:

- Volume
- OEM
- Retail

The following sections provide details on each of these types of activation.

More details about activation for Windows Server “Longhorn” will be released in the coming months and for other products in the coming years.

Volume Activation 2.0

As discussed earlier, Volume Activation 2.0 provides customers with the following two types of keys and three methods of activation.

- Multiple Activation Key (MAK)
 - MAK Proxy Activation
 - MAK Independent Activation
- Key Management Service (KMS) Key
 - KMS Activation

Customers are free to use any or all of the options, constrained only by the needs of their organization and its network infrastructure.

Multiple Activation Key

MAK activation uses a technology similar to that in use with MSDN® Universal and Microsoft Action Pack subscriptions. Each product key can activate a specific number of computers. If the use of volume-licensed media is not controlled, excessive activations result in depletion of the activation pool. MAKs are activation keys. They are not used to install Windows but rather to activate it after installation. You can use them to activate any volume edition of Windows Vista.

A MAK is used to activate each system under MAK management. Activation can be performed over the Internet or by telephone. As each computer contacts Microsoft's activation servers, the activation pool is reduced. You can check the number of remaining activations from the Microsoft Licensing Web sites and request additional activations by contacting the Microsoft Activation Call Center.

There are two ways to activate computers using MAK:

- **MAK Proxy Activation¹**: Is a solution that enables a centralized activation request on behalf of multiple desktops with one connection to Microsoft.
- **MAK Independent Activation**: Requires that each desktop independently connects and activates against Microsoft.

Advantages of MAK activation include the ability to automate key assignment and activation and no requirement to periodically renew activation. Additional requirements include the need to request more activations when the number of activations passes the predetermined limit, the need to manage the installation of MAKs (automated by Business Desktop Deployment (BDD) 2007), the requirement for reactivation when significant hardware changes occur, and the potential need to manually activate systems using a telephone when no Internet connection is available.

Key Management Service (KMS) Key

Key Management Service (KMS) enables organizations to perform local activations for computers in a managed environment without connecting to Microsoft individually. A KMS Key is used to enable the Key Management Service on a machine controlled by an organization's system administrator. KMS usage is targeted for managed environments where more than 25 computers are consistently connected to the organization's network. Computers running Windows Vista activate by connecting to a central Windows Vista computer running the KMS service.

After initializing KMS, the KMS activation infrastructure is self-maintaining. Users can install a KMS key and enable the KMS service on Windows Vista systems. The KMS service can easily be co-hosted with other services, and it does not require any additional software for downloading or installing. Windows Server 2003 KMS service for Volume Activation 2.0 is currently under development with expected availability in 2007. A single KMS host can support hundreds of thousands of KMS clients. It is expected that most organizations will be able to operate with just two KMS hosts for their entire infrastructure (one main KMS host and one backup host for redundancy).

¹ MAK Proxy Activation will be available in the solution code name Volume Activation Management Tool (VAMT) which is currently under development with expected availability in 2007.

A KMS host must have at least 25 physical Windows Vista clients connected to it before any of them will activate. Systems operating in virtual machine (VM) environments can also be activated using KMS, but they do not contribute to the system count.

Clients must renew their activation by connecting to the KMS Host at least once every 180 days. Clients not yet activated will attempt to connect with the KMS host every two hours (value configurable). Once activated, they will attempt to connect to the KMS host every seven days (value configurable) and if successful will renew their 180-day activation life span. Clients locate the KMS host using one of the two methods:

- **Auto-Discovery**, in which a KMS client uses domain name service records to automatically locate a local KMS host.
- **Direct connection**, where a system administrator specifies the KMS host location and communication port.

Clients have a 30-day grace period to complete activation. Clients not activated within this time period will go into Reduced Functionality Mode (RFM).

As mentioned above, KMS clients activated with KMS periodically try to renew their activation. If they are unable to connect to a KMS host for more than 180 days, they enter a 30-day grace period, after which they enter RFM until a connection can be made with a KMS host, or until a MAK is installed and the system is activated online or via telephone. This feature prevents computers that have been removed from the organization from functioning indefinitely without adequate license coverage.

OEM Activation 2.0

OEM Activation 2.0 can be a valuable component in your overall activation strategy. Advantages of using OEM SKUs and OEM Activation 2.0 include permanent out of the box activation and the ability for customers to request custom media images from their OEM manufacturer. Volume license media can be preinstalled but must be activated by either MAK or KMS.

Retail Activation

Like MAK activation, a computer installed with retail versions of Windows Vista must be activated online or over telephone with Microsoft. Each installation of Windows Vista requires a separate product key. Retail versions of Windows Vista cannot use a KMS for activation purposes.

Target Environment Considerations

For each target environment where Windows Vista will be deployed, determine the current infrastructure capabilities. Some common questions to answer are:

Questions	Considerations
How many computers will be deployed in the target network?	KMS requires a minimum of 25 computers connected to the KMS host before Windows Vista client computers can be activated.

Questions	Considerations
Does the network support TCP/IP connectivity?	KMS activation requires TCP/IP connectivity (port TCP/1688 default). A KMS activation request and response takes approximately 450 bytes. Consider the impact of periodic activation for slow and/or high-latency links.
Do computers in the target environment have Internet connectivity?	For automatic MAK Independent Activation, each computer requires connectivity to the Internet.
Does the current Domain Name System (DNS) service support SRV records and DDNS?	Dynamic DNS and SRV record support are required for the default auto-publishing and auto-discovery functionality used by KMS. Both Microsoft Windows® 2000 or later DNS and BIND 8.x or newer fully support these features. Manual configuration of DNS for KMS support is detailed later in this guide.

Table 1: Infrastructure Analysis Questions

For a target environment that has TCP/IP connectivity to a hub location and can support the KMS bandwidth requirements, a centralized KMS is a recommended option. If the same location does not have TCP/IP connectivity to a hub location but can support the necessary computer count (n-count), a local KMS is a viable solution. MAK activation is a preferred option for laptops and other target environments that cannot meet the n-count. Prior to choosing an activation option, it is important to have a clear understanding of user connectivity requirements and infrastructure capabilities, along with any business requirements.

The following table lists some general target environment considerations for selecting a product activation option.

Policy	Impact on Activation
High security network (no external data transfer allowed)	Data of any kind may not be transferred across network boundary. OEM activation may be the best solution in these scenarios.
Restricted Internet access	Locations from which access to the Internet is restricted. KMS or MAK Activation can be used for activation.
Periodic connectivity	Computers are required to connect to the organization's network periodically so that administrators can proactively manage them for updates. Because KMS-based activation is valid for 180 days, these computers need to reconnect or they will fall into Reduced Functionality Mode (RFM).

Table 2: Security Policy Considerations

In addition to the listed considerations, it is equally important to consider any organizational policies, for example regarding KMS host sizing or co-hosting.

KMS Host Sizing

KMS host processing capacity should not be a limiting factor for virtually any size organization. A single KMS host is capable of supporting hundreds of thousands of KMS clients, and KMS requests are only a few hundred bytes each. In addition, when attempting to activate, the client computers make a KMS request every two hours (default) and only once every seven days when activated. Normally, a client computer activates with the initial request.

Following are some considerations for planning a KMS host:

- KMS is compute-cycle intensive while actively processing requests. CPU usage can momentarily reach 100 percent on a single-processor computer during request processing.
- KMS memory usage can vary from approximately 10 MB to around 25 MB, depending on the number of incoming requests.
- Network overhead is minimal.
Less than 250 bytes are sent in each direction for a complete client-KMS exchange, plus TCP session setup and teardown. The only additional network traffic is for auto-discovery, which usually occurs only once per client computer, as long as the same KMS continues to be available for subsequent renewals.
- Large organizations may want multiple KMS hosts for load-balancing and redundancy purposes.

Co-Hosting KMS

To minimize cost, most organizations prefer to co-host KMS along with other functions. KMS is designed to support co-hosting. KMS can easily coexist with common server roles, including domain controllers. It has a small resource footprint during normal operation, although it can become compute-bound as noted in the previous section. This is most likely to occur after a large deployment of KMS clients or if most users start their computers in a short period. If CPU consumption is an issue, KMS supports a low priority option.

User Connectivity Considerations

Assess your environment and identify how your computers are connected to the network. Connectivity to the network, Internet access, number of computers that regularly connect to the network are some of the important characteristics to identify. Some organizations may have a combination of environments where some are connected to the corporate network while others are not. In this case, more than one activation option is used. These factors are important considerations in selecting an activation method.

The following table lists the common types of user connectivity along with the characteristics.

Connectivity Type	Characteristics
Connected	Computers that are typically connected to the network
Remote w/Periodic Connectivity	Computers that are located "in the field" and have on-demand organizational network connectivity usually through Virtual Private Network (VPN) or by visiting a local office.
Remote w/Limited Connectivity	Computers that are located "in the field" and have no direct access to the network, but may have web-based access to organizational resources.
Disconnected	Computers that may never connect to the network or that may connect very infrequently (that is, less than twice a year).

Table 3: Connectivity Types

While KMS activation is a more attractive option for computers with connectivity type 'Connected' or 'Remote w/Periodic Connectivity', MAK activation is a more logical choice for computers with connectivity type 'Remote w/Limited Connectivity' or 'Disconnected'. Choosing an activation option is not as black or white as determining types of user connectivity.



Map Computers to Activation Solutions

The second step to selecting appropriate activation options is to map computers to activation solutions. The goal is to ensure that all computers are associated with an activation option. Look at the sample Guidance Worksheet shown in Table 4 to see how to map your computers to activation solutions. To complete the worksheet, you need to determine the following:

- The total number of computers that need to be activated using a Volume Activation 2.0 method
- The number of computers that will not connect at least once every 180 days (Use MAK activation option.)
- The number of computers in environments where there are less than 25 computers (Use MAK activation option.)
- The number of computers that will regularly connect to the network (Use KMS activation option.)

- The number of computers in disconnected environments where there are more than 25 computers and there is no Internet connectivity (Use KMS activation option.)
- The number of computers in disconnected environments where there are less than 25 computers and there is no Internet connectivity (Use MAK activation option.)

Criteria	Type of Activation	Number of Computers
Total number of computers to be activated	N/A	100,000
Number of computers that will not connect at least once every 180 days	MAK	-3,000
Number of computers in environments where there are less than 25 computers	MAK	-1,000
Number of computers that will regularly connect to the network	KMS	-95,000
Number of computers in disconnected environments where there are more than 25 computers and no Internet connectivity	KMS	-250
Number of computers in disconnected environments where there are less than 25 computers and there is no Internet connectivity	MAK	-750
Remaining computer count should be zero		0

Table 4: Sample Activation Mapping Worksheet

A blank worksheet is available as a job-aid in [Appendix 4](#).



Plan Monitoring and Reporting

It is critical to establish monitoring and reporting for KMS and MAK. For MAKs, be sure to include monitoring the number of MAK activations used by viewing the Microsoft licensing websites. If your environment can support the requirements for KMS (25 computers for Windows Vista activation) then it's recommended to deploy a KMS so that computers will not run in Reduced Functionality Mode.

Refer to the following sections to set up reporting in the environment for Volume Activation 2.0:

- KMS MOM Pack (This may be available in Q1 2007) – provides KMS Management and sample reports for KMS activation. See [KMS Activity Reporting](#) for descriptions.
- Activation reporting through various system management tools will be available soon.
- The file "Volume Activation 2.0 Technical Attributes.xls" lists all of the WMI methods, properties, registry keys, and event IDs for product activation.



Plan Support

Create support scripts for the following scenarios to address common Volume Activation 2.0 issues:

- [Steps to convert from KMS to MAK](#)
- [Steps to convert from MAK to KMS](#)
- [Troubleshooting Activation issues](#)
- [Recovery from RFM](#)
- [Recovery from non-Genuine](#)

Information located in the "[Deployment Guidance](#)" section later in this guide may assist in developing the script. Additional items to consider are:

- Training to bring support staff up to date on Volume Activation 2.0
- Escalation management to ensure issues are raised to trained personnel

Deployment Example

Deployment Example for MAK Independent Activation and KMS Activation

Many enterprises have networks that are separated into multiple security zones. This can present a problem to a system administrator when activating Windows Vista. Fortunately, there are several options when deploying Windows Vista in a heterogeneous environment.

The following figure shows the example of a potential network configuration using MAK Independent activation and KMS activation. Note that this example is intended for illustration purposes only to show key scenarios.

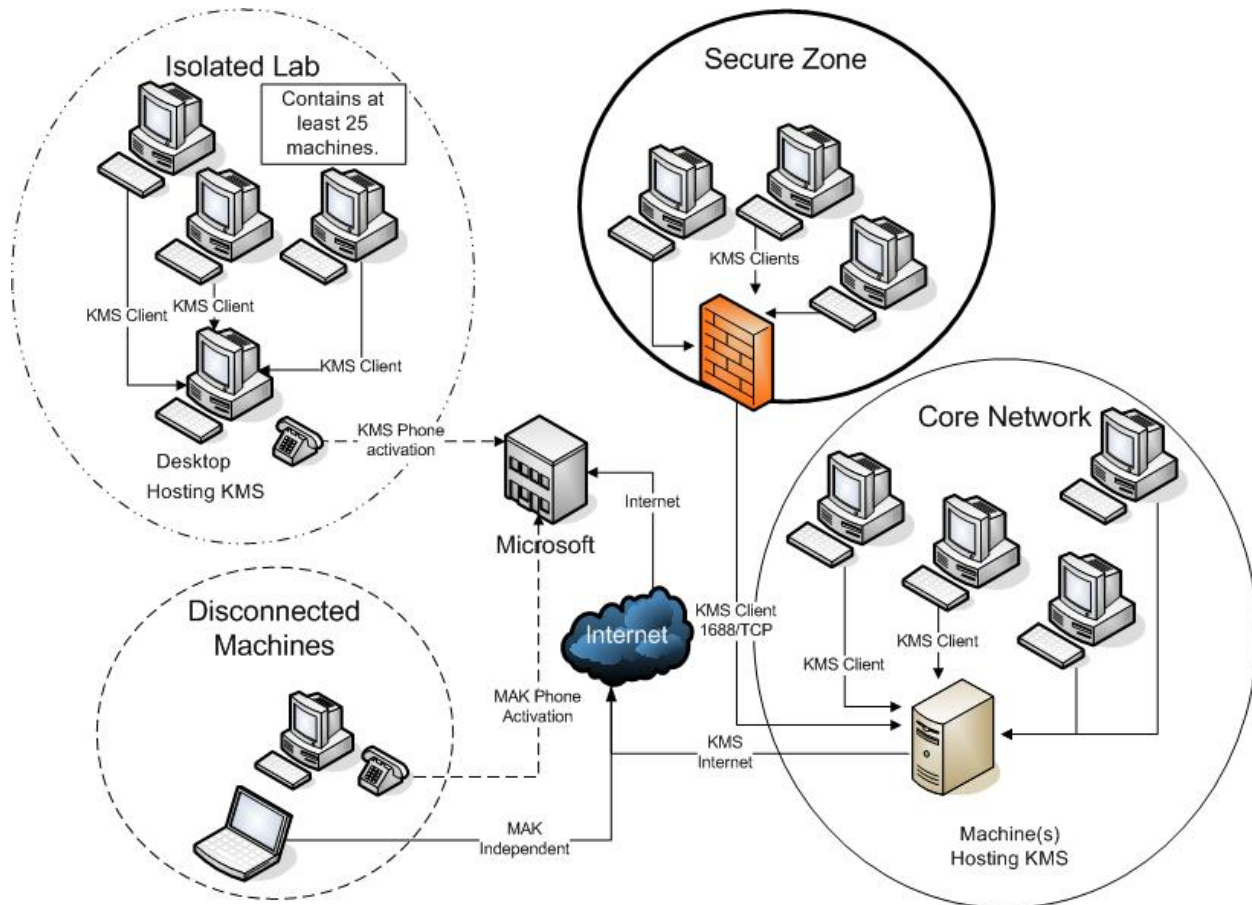


Figure 1: Network configuration using MAK and KMS

In this example, the enterprise has computers in the following different scenarios:

- Core network:** The core network has redundant KMS hosts. All computers in the main corporate network query DNS for the KMS SRV record and activate themselves after contacting the KMS service running on one of these computers. The KMS hosts were activated directly through the Internet.
- Secure zone:** Many enterprises have secure zones that are carved out of the corporate network by installing a firewall to block all traffic between the secure zone and the rest of the network. To allow these computers to activate using the corporate KMS using RPC over TCP/IP, the network administrator has to allow 1688/TCP outbound from the secure zone and allow RPC reply back in.
- Isolated lab:** In the isolated lab scenario, corporate security policy does not allow any traffic between computers in the isolated lab and the rest of the corporate network. This could be through a firewall that blocks all, but a very limited number of ports or where there is no network connectivity at all. Because the lab has more than 25 computers, users can deploy a KMS service to one Windows Vista computer in the lab. All computers in the lab will then simply activate using the local KMS host. The KMS host itself is activated by calling Microsoft and getting the confirmation ID (CID).
- Disconnected computers:** Computers that are not on the corporate network and/or are in a lab that has less than 25 computers must activate using MAK. If a computer requires occasional connectivity to the Internet (for example, the laptop of a traveling salesperson), it can activate against Microsoft directly. The computer needs connectivity

to the Internet only once (to activate) and will not need to be reactivated unless there is a major change in the hardware. If a computer is in a lab and has no network connectivity at all, it can activate against Microsoft over a telephone the same way the KMS host is activated in the isolated lab scenario.

Deployment Example for MAK Proxy Activation

There are some customers who may not want to use KMS. This section covers the example of an enterprise using a MAK proxy activation tool code named "Volume Activation Management Tool (VAMT)" to perform all activations for Windows Vista volume editions.

The following figure shows the example of a potential network configuration using MAK and VAMT. Note that this example is intended for illustration purposes only to show all key scenarios.

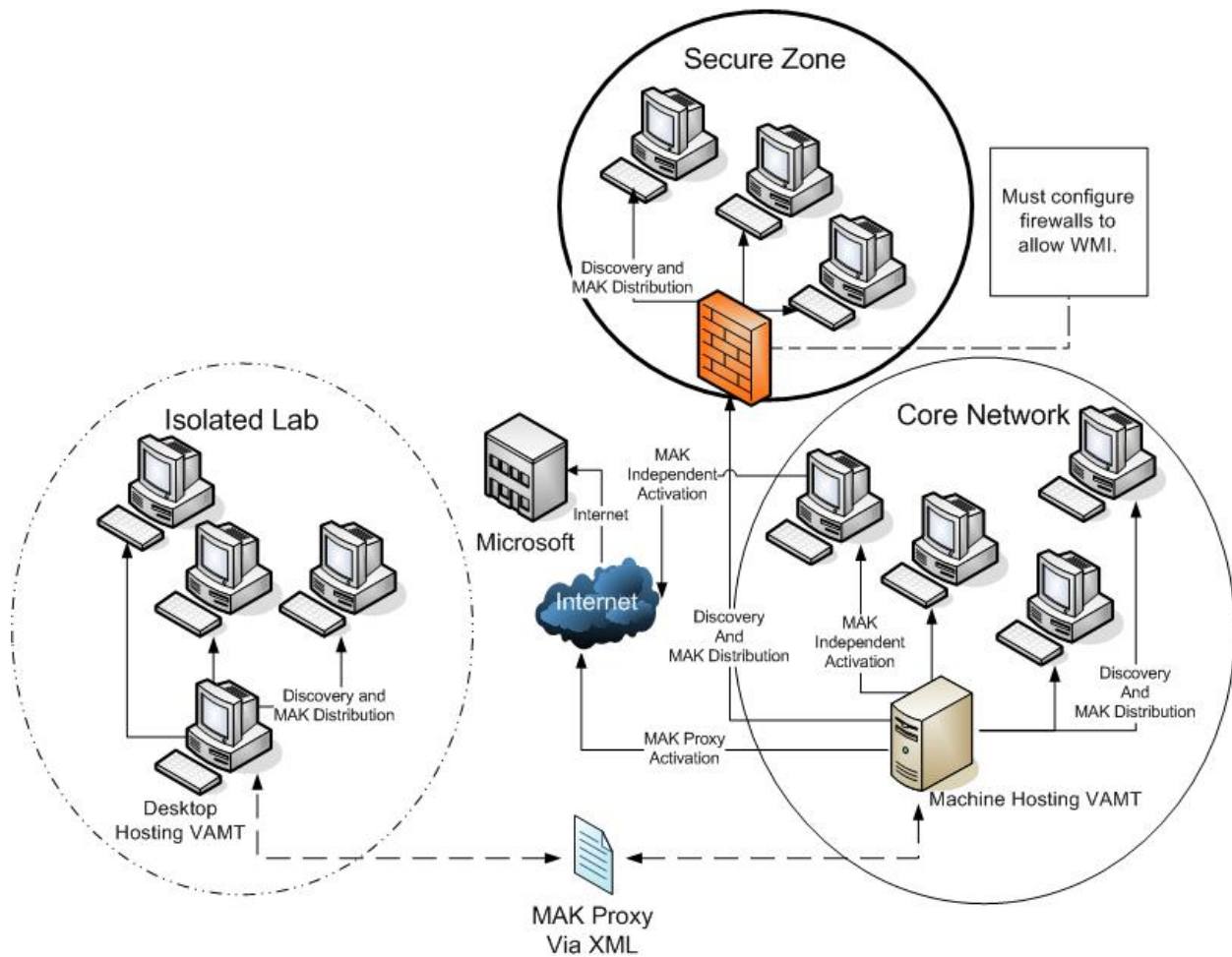


Figure 2: Network configuration using MAK and VAMT

The figure shows computers in the following scenarios:

- Core network:** In the core network scenario, the VAMT is deployed to a computer that can access the Internet. The administrator can perform an "Add Machine" function against the Active Directory domain or workgroups to find computers on the network. After discovering the computers and the returned status, the administrator can perform either MAK independent activation or MAK proxy activation.

A MAK independent activation installs a MAK on a client computer and requests activation against Microsoft servers over the Internet. A MAK proxy activation installs a MAK on a client computer, obtains the installation ID (IID), sends the IID to Microsoft on behalf of the client, and obtains a confirmation ID (CID) that the tool activates the client by installing the corresponding CID.

Note For more information about the Windows Vista Privacy Statement, see <http://go.microsoft.com/fwlink/?LinkId=52526>.

- **Secure zone:** In this scenario, the tool can activate computers using MAK proxy activation. This assumes that the clients in the secure zone do not have Internet access. The following two key issues need to be addressed:
 - The computers must be discoverable (through Active Directory® directory service or Workgroups).
 - The tool has to make a call to the WMI services on the computer to get status and install MAKs and CIDs.

This requires the firewall to be configured to allow DCOM RPC traffic through it. For more details on this, see "How to configure RPC dynamic port allocation to work with firewalls" at the following URL:

<http://support.microsoft.com/?kbid=154596>
- **Isolated lab:** In the isolated lab scenario, the tool is hosted inside the isolated lab. The tool performs discovery, obtains status, installs a MAK, and obtains IID on all computers in the lab. The tool then exports the list of computers to a file on removable media. The administrator imports the machine data onto a computer running the tool in the core network. Once this is done, the tool sends the IIDs to Microsoft and obtains the corresponding CIDs, which the administrator then exports to a file on removable media and takes it back to the isolated lab. Once this data is imported into the tool, the administrator can activate the isolated lab computers by installing the CIDs.

Note For more information about the Windows Vista Privacy Statement, see <http://go.microsoft.com/fwlink/?LinkId=52526>.

Media Considerations

Volume License Product Use Rights require that you have a previous qualifying operating system license for each copy of Windows Vista you deploy. The default 32-bit Volume License media are upgrade-only and are not bootable². You must first boot a previous version of Windows and then run the setup to install Windows Vista. Bootable media is also available on request through your Volume License portal.

² 64-bit Volume License media are not restricted in this way, since there is no supported upgrade path.

Windows Vista Volume License Media

Edition	32-bit	64-bit
Windows Vista Business	Upgrade, Full	Full
Windows Vista Enterprise	Upgrade, Full	Full

Table 5: Windows Vista Volume License Media

Product Key Deployment Considerations

Volume editions of Windows Vista default to KMS-based activation and do not require a product key to be entered during setup. Windows Vista Volume License editions use a specific pre-defined setup key in the sources\pid.txt file. MAKs can be specified with a variety of methods during deployment or post deployment.

How to specify Product Key:	KMS	MAK
During setup	No key required. Volume license editions (by default) use the product key in \sources\pid.txt for KMS activation	No product key can be entered while running manual setup.
With an unattend file ³	No key required. Volume license editions (by default) use the product key in \sources\pid.txt for KMS activation	Specify MAK in the “ specialize ” pass in autounattend.xml (for DVD boot) or unattend.xml (for network share installs) or imageunattend.xml (for WDS installations)
With image-based deployment (ImageX.exe or other tools) ⁴	No key required. The activation method of the reference image is used.	No key required. The activation method of the reference image is used.
Post-operating system installation	No key required. Volume License editions (by default) use the product key in \sources\pid.txt for KMS activation	<ol style="list-style-type: none"> 1. Use the Change Product Key option in Control Panel. 2. After installation, use

³ You will need to ensure that at least one other setting is configured in the “WindowsPE” pass in the autounattend.xml. For more information, see the Unattended Windows Setup Reference help file in the Windows Automated Installation Kit (Windows AIK). The MAK is stored in clear text in the *.XML file as required by the setup process. During the unattended installation process the unattend.xml file is copied to the target machine (%systemroot%\panther folder) but at the end of setup, the actual ProductKey value in this file is deleted and replaced with “SENSITIVE*DATA*DELETED”.

⁴ For more information on using imagex.exe see the Deploy an Image section of the “Getting Started with the Windows Automated Installation Kit (Windows AIK)” guide.

How to specify Product Key:	KMS	MAK
		<p>slmgr.vbs to install and activate the MAK. This process can be scripted, configured for use by Standard Users and is used by the Business Desktop Deployment (BDD) Solution Accelerator.</p> <p>3. The tool code named "Volume Activation and Management Tool (VAMT)" will enable administrators to automate MAK deployment over networks and will be available in 2007.</p>

Table 6: MAK and KMS Product Key Deployment Options

In all deployment scenarios, the product activation timers must be reset by running "%systemroot%\system32\sysprep\sysprep /generalize" on the reference system prior to distributing the image to users.

Obtaining Volume License Keys

Organizations that participate in any Volume License programs can obtain Volume License keys from:

- eOpen (<https://eopen.microsoft.com/EN/default.asp>)
- Microsoft Volume Licensing Services (MVLS) (<https://licensing.microsoft.com/eLicense/L1033/default.asp>)
- Microsoft Activation Call Center - US Customers call 1-888-352-7140.

For international customers, contact your local support center.

For phone numbers of activation centers worldwide, go to the following URL:

<http://www.microsoft.com/licensing/resources/vol/numbers.mspx>

Customers will need to provide their Volume License agreement information and proof of purchase when they call.

By default, KMS keys are limited to 6 computers, each with up to 9 reactivations.

Administrators can obtain an override by calling their local Microsoft Activation Call Center.

MAK has an upper limit on the number of activations based on the type of agreement that exists between the customer and Microsoft. Customers can request the limit to be increased by calling their local Microsoft Activation Call Center.

Important note: You are responsible for both the use of keys assigned to you and the activation of products using your KMS hosts.

- You should not disclose keys to third parties.
- You may not provide unsecured access to your KMS hosts over an uncontrolled network such as the Internet.

Deployment Guidance

The Deployment Guidance section provides step-by-step instructions for activating volume editions of Windows Vista.

For general considerations, read the following section:

- [General Considerations for Windows Vista](#)

For implementing MAK Activation, read the following sections:

- [MAK Activation Overview](#)
- [Prerequisites for MAK Activation](#)
- [Known Issues for MAK Activation](#)
- [Steps for Installing and Activating MAK clients](#)

For implementing KMS Activation, read the following sections:

- [KMS Activation Overview](#)
- [Prerequisites for KMS Activation](#)
- [Known Issues for KMS Activation](#)
- [Steps for Installing, Configuring, and Deploying KMS Activation](#)

General Considerations for Windows Vista

This section provides general considerations on deploying Windows Vista.

Tools under Development

- MAK Proxy Activation will be available in the solution code name Volume Activation Management Tool (VAMT) which is currently under development with expected availability in 2007.
- Windows Server 2003 KMS service for Volume Activation 2.0 is currently under development with expected availability in 2007.

Administrative Credentials

To complete any of the steps, you must be a member of the Administrators group. All script functions must be run from a command prompt using elevated permissions unless activation is enabled for standard users. See [Enable Standard User MAK Activation](#) section to enable this option.

MAK Activation

MAKs are installed on each volume-licensed computer that will activate once with Microsoft over the Internet or telephone. A MAK 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). MAKs are recommended 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 activation, whose activation is at risk of expiring, or that has actually reached the end of its grace period. The 30-day grace period cannot be extended and therefore, you must activate MAK immediately. As a computer nears the end of its activation grace period, pop-up activation notifications are presented to users with increasing frequency, unless pop-up notifications are disabled on the computers.

Prerequisites for MAK Activation

To activate MAK on client computers, you must have appropriate Volume License media and access to the Internet or telephone.

Known Issues for MAK Activation

Prior to MAK activation, it is important to understand the following known issue with MAK activation:

If a standard user changes a Volume License key, the ProductID registry values will not be updated which primarily affects product support. Microsoft's Customer Support Services are aware of this issue and will use another method to determine the activation method.

Steps for Installing and Activating MAK Clients

Steps for installing MAK vary depending on whether you are performing them during or after operating system installation.

- To install MAK after operating system installation, perform the steps provided in [Configure a client to use MAK activation using the Windows interface](#) or [Configure a client to use MAK activation using a script](#).
- To install MAK during operating system installation, perform the steps provided in [Configure MAK using unattended setup files](#).

To activate a client computer using MAK activation, perform the steps provided in any one of the following sections:

- [Activate MAK using Internet activation](#)
- [Activate MAK using Phone activation](#)
- [Activate MAK using the tool code named "Volume Activation Management Tool"](#)

To allow standard users (non-administrator) to change product key, complete the following task:

- [Standard User MAK Activation](#)

Install a Multiple Activation Key after Operating System Installation

Configure a volume-licensed edition to use MAK activation with one of the following procedures:

- [Using the Windows Interface](#)
- [Using a script](#)

Note that these procedures also apply to systems that were previously configured to use KMS activation.

To configure a client computer to use MAK activation using the Windows interface

1. Choose and install the desired volume licensed media. No product key is required during setup.
2. Start the computer and log on with administrator privileges. Open System Properties in Control Panel, by clicking **Start** and then right-clicking **Computer** and clicking **Properties**.
3. In the **Activation** section, click **Change product key**.
You will be prompted for permission. Click **Continue**.
4. In the **Change your product key for activation** dialog box, enter the MAK.

The computer attempts to activate over the Internet. The next screen will indicate whether it activated successfully or was unable to activate for some reason (usually due to network connectivity).

If activation was not successful, the computer attempt to retry automatically (The user does not need to be an administrator for automatic activations). To disable automatic activation attempts, change the registry value

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual to 1.

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](http://support.microsoft.com/kb/256986/) (<http://support.microsoft.com/kb/256986/>) Description of the Microsoft Windows registry.



Figure 3: Change your product key for activation dialog box

To configure a client computer to use MAK activation using a script

1. Choose and install the desired volume licensed media. No product key is required during setup.
2. Start the computer and log on with administrator privileges.
3. Launch a command window (with elevated privileges if not running as administrator).
4. Run the following script, using your MAK:
cscript \windows\system32\slmgr.vbs -ipk <Multiple Activation Key>

The computer attempts to activate over the Internet per the next scheduled interval. To activate immediately, follow the procedure in [To activate manually over the Internet using MAK activation using a script](#).

If activation was not successful, the computer attempts to retry automatically. To disable automatic activation attempts, change the registry value **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual** to 1.

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: 256986 (<http://support.microsoft.com/kb/256986/>) Description of the Microsoft Windows registry.

Install Multiple Activation Key during Operating System Installation

Configure a MAK using unattended setup files using this method:

- Use Setup.exe or Windows Deployment Service (WDS) and specify a MAK product key in the "specialize" pass in an *unattend.xml* on a floppy disk for boot from DVD installation or by running `setup /unattend: <path to file>` for network share based installation. For more information, see the Unattended Windows Setup Reference help file and the *Windows Automated Installation Kit (WAIK) User's Guide for Windows Vista*: <http://go.microsoft.com/fwlink/?LinkId=76683>

A sample autounattend.xml file to install a MAK is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-Setup" processorArchitecture="x86"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <UserData>
        <AcceptEula>true</AcceptEula>
      </UserData>
    </component>
  </settings>
  <settings pass="specialize">
    <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <ProductKey>MAK Product Key</ProductKey>
    </component>
  </settings>
</unattend>
```

Note The MAK is in clear text in the *.XML file as required by the setup process using these methods. During unattended installation process, the file `unattend.xml/autounattend.xml` is copied to the target computer (%systemroot%\panther folder) but at the end of setup, the actual ProductKey value is deleted and replaced with "SENSITIVE*DATA*DELETED".

Activate MAK Clients

You can activate MAK clients using any of the following procedures:

- [Activate MAK using Internet Activation](#)
- [Activate MAK using Phone Activation](#)
- [Activate MAK using the tool code named "Volume Activation Management Tool"](#)

Activating MAK Clients using Internet Activation

Activate a computer that uses MAK activation with one of the following procedures:

- [Using the Windows Interface](#)
- [Using a script](#)

To activate MAK manually using the Windows interface

1. Open **System** Properties in Control Panel.
If you are prompted for permission, click **Allow**.
2. Click **Click here to activate Windows now**.
This launches the activation wizard. If you are prompted for permission, click **Allow**.
If your computer has access to the Internet and is able to activate, Windows reports that the activation was successful.
If you are unable to activate, the wizard reports the failure and presents additional options, including the ability to activate using the telephone.

To activate MAK manually over the Internet using a script

1. Launch a command window (with elevated privileges if not running as Administrator).
2. Run the following script to perform activation:

```
cscript \windows\system32\slmgr.vbs -ato
```

The script will report success or failure with a result code.

Activating MAK Clients using Phone Activation

Use this procedure to activate computers that are connected to the organizational network and do not have Internet connectivity.

If you need to perform activation frequently or activate multiple computers, it may be more useful to automate the process by adapting the built-in script (slmgr.vbs).

To activate manually over the telephone with a remote script using MAK activation

1. Launch a command window (with elevated privileges if not running as Administrator). To enable copying from the command window using mouse selection and the ENTER key, ensure that the QuickEdit Mode Edit Option is set.
2. Obtain the IID from the target computer using the following script:

```
cscript \windows\system32\slmgr.vbs <ComputerName> <Username> <Password> -dli
```
3. This will display several sections of license information grouped by Product ID. The section that lists the last five characters of your MAK in Partial Product Key is the one that includes the Product ID and IID required for phone activation. Save both of these values, along with the %COMPUTERNAME%. (Use the set command to find this.)
4. Call the automated phone system for your region.
You can obtain the relevant telephone numbers by using the Find available phone numbers for activation wizard through the software licensing user interface by running *slui.exe 4* at a command prompt.
You can use the Interactive Voice Response system to obtain the CID for the target computer. When prompted, provide the corresponding IID from the computer you are activating.
5. Activate the target computer (%COMPUTERNAME%) by installing the CID using the

To activate manually over the telephone with a remote script using MAK activation

following script:

```
cscript \windows\system32\slmgr.vbs <ComputerName> <UserName> <Password> -  
atp <Confirmation ID>
```

Activating MAK using the tool code named "Volume Activation Management Tool"

Microsoft is currently developing VAMT to provide a cost-effective, batched Internet-based activation alternative to telephone activation. This solution will enable customers to activate a group of connected client computers and will support scenarios where client computers may be disconnected, and only a centrally located computer hosting the tool has access to the Internet or to Microsoft. MAK Proxy Activation will be available in the solution code name Volume Activation Management Tool (VAMT) which is currently under development with expected availability in 2007.

Optional MAK Configuration - Enabling Standard User MAK Activation

You can optionally create a registry key to allow a standard user to apply MAK and activate a computer. However, because this lowers security on the computers, it is critical that you understand the heightened risk in allowing standard users to change the licensing status. Once you make this change, administrator privileges are no longer required for product activation.

To enable optional Standard User MAK activation

1. On the client computer, create the following registry key using regedit.exe.
2. Navigate to **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**
3. Enter the following data:
 - Value Name: UserOperations
 - Type: DWORD
 - Value Data: 1

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](http://support.microsoft.com/kb/256986/) (http://support.microsoft.com/kb/256986/) "Description of the Microsoft Windows registry."

This procedure allows a standard user to switch to a MAK from a KMS client or replace an existing MAK. It also allows a standard user to manually activate the computer.

Note If a standard user changes a volume product key, the ProductID registry values will not be updated this primarily affects product support. The Microsoft Customer Support Services are aware of this issue, and will use another method to determine the activation method.

KMS Activation

Key Management Service (KMS) enables organizations to perform local activations for computers in a managed environment, without the need to connect to Microsoft individually. You can enable KMS functionality on any Windows Vista or Windows Server “Longhorn” computer by installing the KMS key and then activating the computer against Microsoft once, either over the Internet or over the telephone. After initializing KMS, the KMS activation infrastructure is self-maintaining. The KMS service does not require dedicated computers to run it, and can be easily co-hosted with other services. A single KMS host can support hundreds of thousands of KMS clients. It is expected that most organizations will be able to operate with just two KMS hosts for their entire infrastructure (one main KMS host and a backup host for redundancy).. Windows Server 2003 KMS service for Volume Activation 2.0 is currently under development with expected availability in 2007. In case of significant changes to the hardware on the KMS host, reactivation is a must.

By default, Windows Vista Business and Windows Vista Enterprise Edition are designed to activate using KMS, without the need for user interaction. Client computers locate the KMS host dynamically using the SRV records found in the DNS or connection information specified in the registry. The client computers use information obtained from the KMS host to self-activate. A KMS host must have at least 25 physical Windows Vista client computers connected to it before any one of them can activate. This is referred to as n value or n-count. Computers that operate in virtual machine (VM) environments can be activated using KMS, but they do not contribute to the count of activated systems.

Clients that are not activated attempt to connect with the KMS host every two hours (value configurable). This interval can be configured at the KMS host by setting the `ActivationInterval` (see [To Configure KMS hosts for KMS Activation](#)). Clients must renew their activation by connecting to the KMS host at least once every 180 days to stay activated. Once activated, the client computers attempt to renew their activation every seven days. This interval can be configured at the KMS host by changing the `RenewalInterval` (see [To Configure KMS hosts for KMS Activation](#)). This value is sent to a client each time the client connects. After each successful connection, the expiration is extended out to the full 180 days.

When a client computer activates against a KMS host, its client machine ID (CMID) is added to a protected table. On successful renewals, the corresponding cached CMID and date stamp are removed from the table. If the client computer does not renew its activation within 30 days, the corresponding CMID is removed from the table and the count is reduced by one.

Client computers connect to KMS host for activation information using anonymous RPC over TCP using default port 1688. This port information can be configured. The connection is anonymous, enabling workgroup computers to communicate with the KMS host. The firewall and the router network may need to be configured to pass communications for the TCP port that will be used. The client computer establishes a TCP session with the KMS host and then sends a single request packet. The KMS host then responds and the session is closed. The same type of request-response is used for activation requests as well as renewal requests. Both requests and responses are logged by the client in the global application event log (Microsoft Windows Security Licensing SLC events 12288 and 12289, respectively). KMS host logs the requests that it receives from all client computers (Microsoft-Windows-Security-Licensing-SLC event 12290). Note that this KMS event is located in the Applications and Services Logs\Key Management Service event log.

Prerequisites for KMS Activation

- You must provide a KMS host with the appropriate Volume License media. KMS clients must also have the appropriate Volume License media to activate against the KMS host.
- KMS clients must be able to access a KMS host. Consider the following:
- Firewalls and the router network may need to be configured to pass communications for the TCP port that will be used (default 1688).

If the Windows Firewall is used, no configuration is required on the client computer, because bi-directional TCP sessions that originate from the client computer are automatically allowed. You can configure the TCP port on the client computer or KMS host by using the `slmgr.vbs` script or setting registry values. You can also set up Group Policy for this. An exception has been added to the Windows Firewall to facilitate opening the default port 1688.

- If IPSec authentication is used to restrict end-to-end communication between computers in the network, you may need to configure one or more KMS hosts as “boundary machines,” that is, disable IPSec authentication in some situations. For example, some of your clients may be in workgroups or you may have domain-based clients that must access a KMS host across an Active Directory forest. The procedure for configuring this is beyond the scope of this guide.
- You may need to configure the Applications and Services Logs\Key Management Service event log on KMS hosts to ensure that it is large enough to accommodate the volume expected in your organization. Each 12290 event, which occurs every time a KMS client connects to the KMS host, requires approximately 1,000 bytes. You can set the log size in the **Log Properties** dialog box.

Known Issues for KMS Activation

On using KMS activation, you may encounter the following known issues:

- Changing the Renewal Interval will not take effect on a KMS client until after the change is received by the client and the software licensing service (slsvc) is restarted.
- Computers running Windows Vista RTM require an RTM KMS to activate; Beta versions of KMS do not support activation of Windows Vista RTM clients.

Steps for Installing, Configuring, and Deploying KMS Activation

To install and configure KMS hosts, perform the steps provided in the following sections:

- [Install KMS hosts](#)
- [Configure KMS hosts](#)

For information and steps to configure KMS publishing to DNS, see the following sections:

- [KMS publishing to DNS overview](#)
- [Prerequisites for KMS Publishing to DNS](#)
- [Known Issues for KMS Publishing to DNS](#)
- [Steps for Configuring KMS Publishing to DNS](#)

To install, configure, deploy, and activate KMS clients, perform the steps in the following sections:

- [Install KMS clients](#)
- [Configure KMS clients](#)
- [Deploy KMS clients](#)
- [Activate KMS clients manually](#)
- [Convert a client using MAK Activation to use KMS Activation](#)

KMS Hosts

This section includes procedures for installing and configuring computers as KMS hosts.

Installing KMS Hosts

Install and activate a computer as a KMS host using the following procedure.

To install KMS hosts for KMS activation

1. Choose and install the desired volume licensed media. No product key is required during setup.
2. Start the computer, log on, and launch a command window with elevated privileges.
3. Install your KMS key. Do not use the Windows interface for this. Run the following script:

```
cscript C:\windows\system32\slmgr.vbs -ipk <Volume License Key>
```

4. Activate the KMS host with Microsoft, either using online activation or telephone activation:
 - For online activation (You must be able to access the Internet from the computer), run the following script:

```
cscript C:\windows\system32\slmgr.vbs -ato
```

- For telephone activation (if you do not have access to the Internet), run the following command and follow the on-screen instructions:

```
slui.exe 4
```

The KMS host is now ready to be used by KMS clients for activation. Additional configuration is optional and will usually not be required.

Configuring KMS Hosts

All KMS configurations are optional and should only be used if required for the local environment. All configuration options require that you launch an elevated command prompt and use the built-in script.

To configure KMS hosts for KMS activation

1. Optionally configure the TCP communications port that the KMS host will use by running:

```
cscript C:\windows\system32\slmgr.vbs -sprt <port>
```

KMS clients that use direct registration have to be configured accordingly. Clients that use auto-discovery will automatically receive and configure the port when they select a KMS host. Remember to restart the slsvc.exe service or restart the computer if you want this to take effect immediately.
2. Optionally disable automatic DNS publishing by using the following scripts:

To configure KMS hosts for KMS activation

cscript C:\windows\system32\slmgr.vbs -cdns

Re-enable automatic DNS publishing using the following script:

cscript C:\windows\system32\slmgr.vbs -sdns

3. Optionally set the KMS host to process using lowered scheduler priority:

cscript C:\windows\system32\slmgr.vbs -cpri

Revert to normal priority:

cscript C:\windows\system32\slmgr.vbs -spri

4. Optionally set the activation interval that clients will use if not activated (default is 120 minutes). Run the script:

cscript C:\windows\system32\slmgr.vbs -sai <ActivationInterval>

5. Optionally set the renewal interval that the clients will use for periodically extending their activation expiration (in minutes – default is seven days).

6. Run the following script:

cscript C:\windows\system32\slmgr.vbs -sri <RenewalInterval>

Note You must restart the KMS service (or the computer) for changes to take effect. To restart the KMS service, you can use the *Services* snap-in or run these commands in an elevated command window (answer Y when prompted):

net stop slsvc && net start slsvc

KMS Publishing to DNS

KMS publishing allows clients to automatically locate a KMS (called auto-discovery) with zero client configuration. Clients automatically use DNS auto-discovery if they have not been registered to use a specific KMS.

KMS Publishing to DNS Overview

KMS hosts automatically attempt to publish their existence in SRV Resource Records as defined in RFC2782 (<http://www.ietf.org/rfc/rfc2782.txt>). SRV records can contain multiple entries. These include DNS Address records, which provide the fully qualified domain name for their KMS service providers, as well as attributes, namely priority, port, and weight. KMS only supports the port attribute – priority and weight are ignored.

KMS publishes its host name (A record) and port in the SRV record. Clients query DNS and retrieve a list of KMS SRV records. They select a KMS host randomly from this list and then attempt to use this information to connect to the KMS. If the connection is successful, the KMS location is cached for subsequent connections. Otherwise, the process repeats until the client is able to connect to a KMS or until the list is exhausted.

Advantages of using SRV records include:

- Does not require the use of Active Directory
- Is not limited to Active Directory forests
- The KMS host's TCP port number is configurable without having to touch the clients.

Site affinity, DNS priority, DNS weight, or other optimizations are not supported by KMS in the Windows Vista release. One way to control which KMS host will be used by clients that use DNS auto-discovery is to use different SRV records for different DNS domains.

Alternatively, you would need to use direct KMS registration on each client computer.

Publishing is enabled by default as soon as a computer is configured as KMS. It attempts to self-publish its location and port in its own DNS domain. Publishing can be disabled by setting the registry value *DisableDnsPublishing*, as described in [Configure KMS hosts for KMS Activation](#). System administrators can also create a list of DNS domains that a KMS host will use to automatically publish their SRV records, see [Automatically publish KMS in additional DNS domains](#).

For KMS publishing to work, the DNS system must support Dynamic updates (DDNS). It may also be necessary to configure DNS security so that KMS hosts have the required permissions to create or update these records. For more information about DDNS, see <http://www.ietf.org/rfc/rfc2136.txt>. Windows servers support DDNS, starting with Windows 2000, as do versions of BIND8.x and later.

A KMS host will automatically update its SRV entries if the software licensing service (slsvc.exe) detects that the computer name or TCP port has changed during service startup. It will also update them once each day, in order to ensure that they are not automatically removed (scavenged) by the DNS system.

Not all DNS systems support SRV publishing. In these cases, it is necessary to create or copy the SRV record manually. This can readily be accomplished from a command line or by scripting.

Prerequisites for KMS Publishing to DNS

To complete this task, ensure that you meet the following requirements:

- The following procedures assume you are using Active Directory and DNS service. Configuring non-Microsoft DNS services, for example, BIND 9.x, is outside the scope of this guide. However, it should always be possible to configure SRV records manually.
- Clients that will need access to KMS hosts across another domain or forest are able to do so.
- If you are using Active Directory and Microsoft's DNS server, you must be a member of the Domain Administrators group, have delegated privileges, or have arranged for the procedures to be carried out by the authority responsible for DNS in your organization. Equivalent requirements apply for non-Microsoft DNS services.

Known Issues for KMS Publishing to DNS

KMS publishing has been successfully tested with BIND 9.x. Any server that supports DDNS and SRV resource records per the RFCs should support KMS publishing. Any deployment that is using a non-Microsoft DNS should be fully tested before use in production.

Steps for Configuring KMS Publishing to DNS

To configure DNS in Active Directory, complete the following tasks:

- [Configure security for KMS publishing to DNS](#)
- [Automatically publish KMS in additional domains](#)

To configure security for KMS publishing to DNS

1. If you are using only one KMS host, you may not need to configure any permission, because the default behavior is to allow a computer to create an SRV record and then update it. However, if you have more than one KMS hosts (the usual case), the others will be unable to update the SRV record unless SRV default permissions are changed. This procedure is an example that has been implemented in the Microsoft environment. It is not the only way to achieve the desired result. Detailed steps for each of the tasks are not provided, because they may differ from one organization to another.
2. If you are a domain administrator and want to delegate the ability to carry out the following steps to others in your organization, optionally create a security group in Active Directory and add the delegates, for example, create a group called Key Management Service Administrators, and then delegate permissions to manage the DNS SRV privileges to this security group. The remainder of this procedure assumes that either a domain administrator or delegate is performing the steps.
3. Create a global security group in Active Directory that will be used for your KMS hosts, for example, Key Management Service Group.
4. Add each of your KMS hosts to this group. They must all be joined to the same domain.
5. Once the first KMS host is created, it should create the SRV record. Add each KMS host to this security group.
6. If the first computer is unable to create the SRV record, it may be because your organization has changed the default permissions. In this case, you will need to create the SRV record manually with the name `_VLMCS._TCP` (service name and protocol) for the domain. Set the time-to-live (TTL to 60 minutes).
7. Set the permissions for the SRV group to allow updates by members of the global security group.

To automatically publish KMS in additional DNS domains

1. On the KMS host, create the following registry key, using regedit.exe.
2. Navigate to **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**
Value Name: DnsDomainPublishList
Type: REG_MULTI_SZ
Value Data: Enter each DNS Domain that KMS should publish to on separate lines.
Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: 256986 (<http://support.microsoft.com/kb/256986/>)
Description of the Microsoft Windows registry.
It is useful to export the registry key for later use or to import into another KMS host.
3. Restart the Software Licensing Service and the records should be created immediately. The application event log will contain a 12294 event for each successfully published domain and a 12293 event for each unsuccessful domain publishing attempt.

To automatically publish KMS in additional DNS domains

4. For the 12293 event, the failure code can be diagnosed by running the following:
slui.exe 0x2a 0x<error code>
See [Mapping error codes to text messages](#) for example.

KMS Clients

This section includes procedures for installing and configuring computers as KMS clients.

Install KMS clients

Install KMS clients using this procedure.

To install KMS clients for KMS activation

1. Choose and install the desired volume licensed media. No product key is required during setup.
2. If you use DNS auto-discovery, no further configuration is required.
3. For domain-joined computers, the DNS auto-discovery of KMS requires that the DNS zone corresponding to either the primary DNS suffix of the computer or the Active Directory DNS domain contain the SRV resource record for a KMS.
4. For workgroup computers, DNS auto-discovery of KMS requires that the DNS zone corresponding to either the primary DNS suffix of the computer or the DNS domain name assigned by DHCP (option 15 per RFC 2132) contain the SRV resource record for a KMS.

Configuring KMS Clients

Configure KMS clients using this procedure.

To configure KMS clients for KMS activation

1. Configuration is only required for KMS clients that will use direct registration with their KMS host. Direct registration overrides DNS auto-discovery. Configuration can be scripted to run remotely and can use Group Policy or logon scripts, assuming that:
 - The required services are enabled on the computer.
 - The port used for KMS communications is not blocked in firewalls or routers.
 - Access permissions are set correctly. (All methods that are implemented in WMI or through the registry require Administrator privileges unless standard user activation has been enabled).
2. On the KMS client, register the KMS host's fully qualified domain name (FQDN), for example *kms03.site5.contoso.com* and, optionally, the TCP port used to communicate with KMS (if you are not using the default):
`cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>[:<port>]`
3. Optionally, the IP or NetBIOS ID (name of the computer) can be used instead of the FQDN.
`cscript \windows\system32\slmgr.vbs -skms <IPv4 Address><:port>`
`cscript \windows\system32\slmgr.vbs -skms <IPv6 Address><:port>`

To configure KMS clients for KMS activation

```
cscript \windows\system32\slmgr.vbs -skms <MachineName> <:port>
```

4. To re-enable auto-discovery for a client computer that was registered to use a specific KMS, run the following built-in script:

```
cscript \windows\system32\slmgr.vbs -ckms
```

Deploying KMS Clients

Deploy KMS clients using this procedure.

To deploy KMS clients for KMS activation

1. Run `sysprep /generalize` immediately prior to shutting down your deployment reference image. This resets the activation timer, security identifier, and other important parameters. Resetting the activation timer is important to prevent images from requiring activation immediately after starting first boot.
Note that running Sysprep does not remove the installed product key and you will not be prompted for a new key during mini-setup.
2. Use an imaging technology that is compatible with Windows Vista.
3. Deploy using standard techniques such as disk duplication or WDS.

Activating a KMS Client Manually for KMS Activation

You can activate a computer that uses KMS activation with the following procedures. Note that KMS clients attempt to activate automatically at preset intervals. However you may wish to be sure that some clients (mobile clients, for instance) are activated before distributing them.

- [Using the Windows Interface](#)
- [Using a script](#)

To activate a KMS client manually using the Windows interface

1. Open **System** properties in Control Panel.
If you are prompted for permission, click **Allow**.
2. Click **Click here to activate Windows now**.
This launches the activation wizard. If you are prompted for permission, click **Allow**.
If your computer has access to the network and a KMS, Windows reports that activation was successful.
If the activation fails, the wizard reports the failure. For activation to occur, it is necessary for 25 computers to be present. Until that happens, activation will fail with error code 0xC004F038.

To activate a KMS client manually using a script

1. Launch a command window (with elevated privileges if not running as Administrator).
2. Run the following script to activate:

```
cscript \windows\system32\slmgr.vbs -ato
```

To activate a KMS client manually using a script

The script reports activation success or failure, along with a result code.

If you were unable to activate, the wizard will report the failure. For activation to occur, it is necessary for 25 computers to be present. Until that happens, activation will fail with error code 0xC004F038.

Converting a Client Computer using MAK Activation to use KMS Activation

To convert a client computer using MAK activation to use KMS

1. Ensure that the computer is connected to the network and can access a KMS host.
2. Obtain the 5x5 setup key from the file *sources\pid.txt* on the installation media.
3. Launch a command window with elevated privileges.
3. Run the following script to install the setup key (this automatically removes the MAK):

```
cscript \windows\system32\slmgr.vbs -ipk <setup key>
```

4. Run the following script to activate the computer:

```
cscript \windows\system32\slmgr.vbs -ato
```

The script reports success or failure, along with a result code.

Important Note It is important that Windows be activated before the computer is rebooted if more than 30 days have elapsed since initial installation. If it reaches the end of the grace period without activating the computer will be in Reduced Functionality Mode.

Operational Guidance

This section of the Step-by-Step guide provides operational guidance on implementing Volume Activation 2.0.

Built-in Scripting Support

A built-in script is provided to support Volume Activation 2.0. This script can be run locally on the target system or remotely from another computer. Examples provided in this section presume local script use for simplicity. You must supply all the parameters shown in brackets for remote use.

The general syntax is:

```
C:\>cscript C:\windows\system32\slmgr.vbs <ComputerName> <UserName> <Password> <Option>
```

You can also run the script using wscript or use the default script engine by simply running slmgr.vbs. If the script is invoked without specifying an option, usage information will be displayed. If you do not specify user name and password, the script takes the credentials of the user that runs the script.

Important note: Even for the display-only options, all script functions must be run from a command prompt using elevated permissions unless activation is enabled for standard users. When running in default configuration as a standard user, some data may be missing or incorrect for the display-license option (-dli). To accomplish this, right-click the shortcut for the Command Prompt and click Run as administrator.

Remote Scripting Support

To run the script remotely, make sure that you have the name of the target computer as well as the credentials with appropriate privileges. In addition, services and ports that are required to support remote use must be appropriately configured.

To use remote functionality of the slmgr.vbs script, you need to make a few changes to the remote system. An exception must be set in the client firewall. To use slmgr.vbs remotely with computers in a workgroup, set a registry key to modify the User Access Control to allow remote administrative operations. If you plan to use slmgr remote functionality across your organization, consider making these changes in your image before deployment.

To configure Windows Firewall for remote slmgr.vbs functionality within a single subnet

1. In Control Panel, double-click **Security, Windows Firewall** settings.
2. Click the **Exceptions** tab.
3. Select the **Windows Management Instrumentation (WMI)** check box.
4. Click **OK**.

Note Windows Firewall Exceptions only apply exceptions originating on the local subnet by default. To expand the exception to apply to multiple subnets, you need to change the exception settings in the Windows Firewall with Advanced Security.

To configure Windows Firewall for remote slmgr.vbs functionality across multiple subnets

1. In Control Panel, double-click **Administrative Tools**, and then double-click **Windows Firewall with Advanced Security**.
2. Double-click each of the following three WMI items in turn and make the following changes (a-d):
 - a. Windows Management Instrumentation (*ASync-In*)
 - b. Windows Management Instrumentation (*DCOM-In*)
 - c. Windows Management Instrumentation (*WMI-In*)
3. On the **General** tab, select the **Allow the connection** check box.
4. On the **Scope** tab, change the Remote IP Address setting from "Local Subnet" (default) to allow the specific access you need.
5. On the **Advanced** tab, verify selection of all profiles that are applicable to the organizational network.
6. Click **OK**.

To create a registry value for remote slmgr.vbs functionality for computers joined in a workgroup

1. On the client computer, create the following registry key using regedit.exe.
2. Navigate to **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system**
3. Enter the following details:
 - Value Name: LocalAccountTokenFilterPolicy
 - Type: DWORD
 - Value Data: 1

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](#) Description of the Microsoft Windows registry.

Microsoft Key Management Service MOM Pack

You can use the Microsoft Windows Key Management Service MOM pack to manage the KMS environment, to meet the established availability requirements, and to support extensive reporting of KMS activations.

The KMS MOM Pack is shipped separately from Windows Vista. To download the KMS MOM Pack, go to <http://www.microsoft.com/technet/prodtechnol/mom/mom2005/catalog.aspx>

Note This may be available in Q1 2007.

Documentation provided with the MOM pack discusses installation, configuration and how to use KMS rules on your MOM Server as well as the KMS reports on your MOM Data Warehouse.

Known Issues with the MOM Pack

On 64-bit versions of Windows Vista, the MOM 2003 Agent (which is 32 bits) cannot see the version number stored in the registry. This value is used to determine membership in the Computer Group defined by the KMS MOM Pack. Without being joined in the Computer Group, the KMS will not provide data to the MOM server's data warehouse. The registry value is created by `slmgr.vbs` when the KMS is activated and is stored by default in the 64-bit view of the registry. There are two ways to work around this issue; for details, see [Appendix 3: Resolving MOM 2003 Installation Issue](#).

KMS Health Monitoring

The KMS MOM Pack monitors the health of the KMS hosts by checking for error conditions and availability. It alerts administrators when a potential problem is observed. Alerts are generated for the following conditions:

- KMS initialization failures
- DNS SRV publishing failures
- KMS host count is below a specified threshold
- No KMS activity has occurred for designated periods

KMS Activity Reporting

A sample set of SQL reports is provided for use as a basis for extensive reporting on activation. These reports are as follows:

- **Activation Count Summary:** Shows the number of KMS activations for each Windows edition and for several historical time ranges.
- **Virtual Machine Summary:** Breaks the cumulative number of virtual machines and physical machines that are activated using KMS activations for each Windows edition.
- **KMS Activity Summary:** Shows daily new KMS activations for each Windows edition. The Total Requests chart shows daily KMS request activity, which includes both activations and renewals, for each Windows edition.
- **Licensing Status Summary:** Shows the number of days left to expiration for computer that have connected to a KMS for each of the license states.
- **Machine Expiration Chart:** Shows the number of computers that are in OOB, OOT/Exp, or non-Genuine grace, whose users could be locked out (Unlicensed) in the next 30 days.
- **Machine Expiration Detail:** Lists the computers that are in OOB, OOT/Exp or non-Genuine grace whose users could fall into Reduced Functionality Mode (Unlicensed) in the next 7 days.

Backup Requirements

Back up is not required for KMS hosts. However, if you need to track the KMS activations, you can periodically export the Key Management Service Event log data under Applications and Services Logs for activation history.

Group Policy Support

There are no Group-Policy specific additions or changes for Volume Licensing. All configuration and property data is supported by WMI and/or the Windows registry, and can therefore, be managed with Group Policy.

Disabling Windows Anytime Upgrade

The Windows Anytime Upgrade (WAU) program allows a Windows Vista Business user to purchase an upgrade directly from Microsoft by clicking the Windows Anytime Upgrade link in **All Programs** and **Extras and Upgrades**. This link and the program are only provided in Windows Vista Business editions because both volume-licensed and retail versions of this product are available (unlike Windows Vista Enterprise, which is only sold as a Volume License version).

Allowing users to attempt to upgrade their computers is generally undesirable. Fortunately, there is a way for system administrators to disable access to WAU in Windows Vista Business editions by adding a registry value to the reference image prior to deployment. When WAU is disabled, an error message is displayed if the user clicks the WAU link, as shown in the figure that follows. This prevents the user from obtaining an upgrade license using the Control Panel. Note that a determined user can still attempt to upgrade by going directly to the Microsoft Windows Anytime Upgrade Web site.

The following procedure helps disable access to the site.

To disable Windows Anytime Upgrade using Volume Activation media

1. On the reference image for client computer, create the WAU registry value using regedit.exe.
2. Navigate to **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**
 - If necessary, create subkeys and navigate to **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\WAU**
 - Create the following values under **WAU**
Value Name: **Disabled**
Type: DWORD
Value Data: 1

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](#) Description of the Microsoft Windows registry.

3. Complete the reference image and deploy it using standard techniques. The resulting media will display an error message if the user clicks on the WAU link.

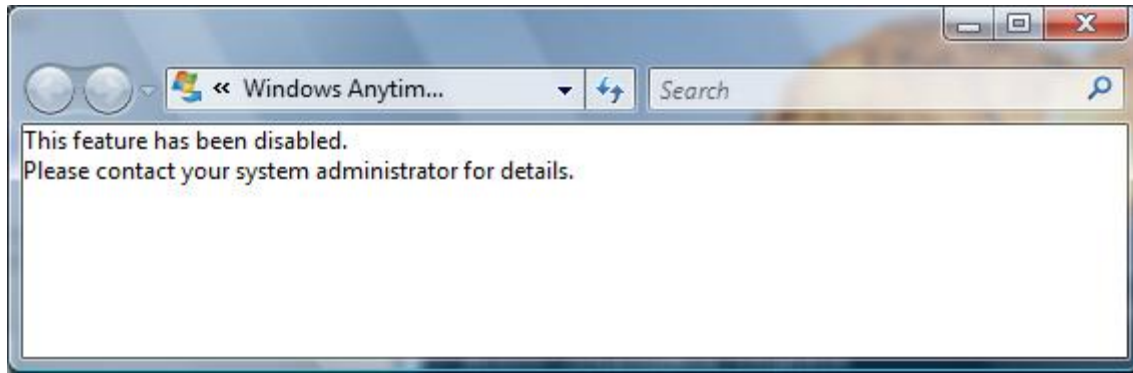


Figure 4: Disabled WAU

Display Volume license Information

You can display information about your Volume License computers using the `slmgr.vbs -dli` script. This provides general information about the current license, including the license state and remaining expiration time or grace period, and information for KMS clients or KMS hosts. In addition to this information, you can view more detailed licensing information using the `slmgr.vbs -dlv`, which may be useful for support purposes.

The following procedure helps display Volume License information.

To display Volume License information

1. Launch the command window. (Administrator privilege is not required here.)
2. Run the following script:


```
cscript \windows\system32\slmgr.vbs -dli
```
3. Information displayed includes the following:
 - **Global information (example)**
 - 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: 8/29/2007 4:59:59 PM
 - **For KMS clients (example)**
 - 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)
 - **For KMS machines (example)**

To display Volume License information

Key Management Service is enabled on this machine

Current count: 7

Listening on Port: 1688

DNS Publishing: Enabled

KMS priority: Normal

4. Run the following script to display more licensing support information that may be useful for support purposes:

```
cscript \windows\system32\slmgr.vbs -dlv
```

For example:

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

5. Run the following script to display more licensing support information for all installed licenses:

```
cscript \windows\system32\slmgr.vbs -dlv all
```

Note Only one license can be in use, namely the one that has a partial product key.

Software Asset Management

Software Asset Management (SAM) is about knowledge of software, its life-cycle, and its use within an organization. Knowledge of exactly what software the business owns, owning only the software each business needs, and being able to actively manage new software purchases help organizations in better management of their software as asset.

Organizations fully in control of their software assets reap the benefits of higher productivity, reduced downtime, increased support from software vendors, and increased ability to stay compliant to the software licensing terms. With the introduction of Software Protection Platform (SPP) in Windows Vista and Windows Server "Longhorn", Microsoft is introducing a licensed store, set of Public APIs (see MSDN for details), and WMI properties (see "Volume Activation 2.0 Technical Attributes.xls" in <http://go.microsoft.com/fwlink/?LinkID=75673>) as part of SPP. This enables remote querying, tracking, and reporting of individual installations and the corresponding license information.

Troubleshooting

This section provides guidance on troubleshooting some commonly faced issues of Volume Activation 2.0.

MAK Activation Troubleshooting Steps

The following table presents issues related to MAK activation.

Issue	Resolution
How can I tell if my computer is activated?	<ol style="list-style-type: none"> 1. Look for "Windows is activated" in the Welcome Center or in System under Control Panel. 2. Run the slmgr.vbs -dli script. "License Status:" shows whether you are activated ("Licensed"), in OOB grace, or OOT grace. If it displays "Unlicensed," you will not be able to log on again until your computer is activated.
Computer does not activate over the Internet.	<p>Ensure that the computer can access Internet sites, for example, http://microsoft.com.</p> <p>You may need to set a proxy. Do this from your browser or Control Panel.</p> <p>If the computer cannot connect to the Internet, use telephone activation.</p>
Internet and telephone activation fail.	<p>Contact the Microsoft Activation Call Center at 1-888-352-7140 (US customers only). For international customers, contact your local support center. For phone numbers of activation centers worldwide, go to the following URL:</p> <p>http://www.microsoft.com/licensing/resources/vol/numbers.mspx</p> <p>Customers will need to provide their Volume License agreement information and proof of purchase when they call.</p>
slmgr.vbs -ato returns an error code.	<p>If slmgr.vbs returns a hexadecimal error code, you can determine the corresponding error message by running the following script:</p> <p><i>Slui.exe 0x2a 0x<error code></i></p>

Table 7: MAK Troubleshooting Steps

KMS Activation Troubleshooting Steps

The following table presents issues related to KMS activation.

Issue	Resolution
How can I tell if my computer is activated?	<ol style="list-style-type: none"> 1. Look for "Windows is activated" in the Welcome Center or in System under Control Panel.

Issue	Resolution
	<p>2. Run the <code>slmgr.vbs -dli</code> script.</p> <p>"License Status:" shows whether you are activated ("Licensed"), in OOB grace, or OOT grace. If it displays "Unlicensed," you will not be able to log on again until your computer is activated.</p>
<p>The computer does not activate.</p>	<p>Verify that the KMS host has been contacted by the minimum number of clients required for activation. Until the KMS host has a count of 25, clients will not be allowed to activate. If a client fails to activate at all within 30 days, it will fall into Reduced Functionality Mode and will be prevented from logging on. Run <code>slmgr.vbs -dli</code> on the KMS host to determine its "current count."</p> <p>On the KMS client, look in the Windows Application event log for event #12289 (KMS response). If you find one at the expected time, report this to Microsoft, because the computer should have activated.</p> <p>Check client event #12288 and consider the following:</p> <ul style="list-style-type: none"> • Is the result code 0? Anything else is an error. • Is the KMS host name shown in the event correct? • Is the KMS port correct? • Is the KMS host accessible? • If you have a third-party firewall, does your outbound port need to be configured? <p>Check KMS event #12290</p> <ul style="list-style-type: none"> • Did the KMS host log an event for the client computer? Check to see if the name of your computer is listed? If so, the response was sent to the client, but got lost in the network or at the client. Verify that the client and KMS host can communicate. Ensure that your routers do not block TCP traffic to TCP port 1688 (default). Check the firewall on the client. • If no event was logged for the client, its request did not reach the KMS or the KMS was unable to process it.
<p><code>slmgr.vbs -ato</code> returns an error code.</p>	<p>If <code>slmgr.vbs</code> returns a hexadecimal error code, or event 12288 contains a result code other than 0, you can determine the corresponding error message by running the following command:</p> <p><i><code>Slui.exe 0x2a 0x<error code></code></i></p>

Table 8: KMS Troubleshooting Steps

KMS Activation of OEM Computers

For KMS activation to work, computers obtained through the Original Equipment Manufacturer (OEM) channels which 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 OEM through the re-imaging rights provided in their Volume License agreement. Computers that have an ACPI_SLIC table without a valid Windows marker will result in the following error(s) on these systems and they will be unable to activate using a KMS:

Error Code: Invalid Volume License Key

In order to activate, you need to change your product key to a valid Multiple Activation Key (MAK) or Retail key.

You must have a qualifying operating system license AND a Volume License Windows Vista upgrade license, or a full license for Windows Vista through an OEM or from a retail source.

ANY OTHER INSTALLATION OF THIS SOFTWARE IS IN VIOLATION OF YOUR AGREEMENT AND APPLICABLE COPYRIGHT LAW.

Error Code: 0xC004F059

Description: The Software Licensing Service reported that a license in the computer BIOS is invalid.

Options to resolve the above errors are:

- Use a Multiple Activation Key (MAK) to activate the computer.
- Contact your OEM for a replacement motherboard that contains a valid Windows marker in the ACPI_SLIC table.
- Purchase new computers with Microsoft Windows preinstalled to ensure that a valid BIOS is installed in the system.

Volume licensed versions of Windows require upgrading from a qualifying operating system as per the terms of your agreement.

Mapping Error Codes to Text Messages

You can use slui.exe to map most activation-related error codes to corresponding text messages. Run the following command on your Windows Vista computer:

```
Slui.exe 0x2a 0x<error code>
```

This will display a dialog box with the error information.

For example, if event 12293 contains an error code 0x8007267C, you can determine the corresponding error message by running the following command:

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

The message will display "No DNS servers configured for local system."

Reviewing Activation Events

The Windows event log provides detailed logging of activation events. The event provider name for all activation events is Microsoft-Windows-Security-Licensing-SLC. All events are found in the Windows Application event log except for the KMS activity event 12290, which

is in its own event log in Applications and Services Logs\Key Management Service. For a detailed list of events, see "Volume Activation 2.0 Technical Attributes.xls."

WMI Software Licensing Classes and Properties

The built-in script, `c:\windows\system32\slmgr.vbs`, uses Windows Management Infrastructure (WMI) to access available WMI classes and properties. Use `slmgr.vbs -dli` to display activation-related information. For a list of software licensing classes and properties, see "[Volume Activation 2.0 Technical Attributes.xls](#)."

Resolving Reduced Functionality Mode

As with Windows XP, after initial installation and the conclusion of the grace period, product activation will be required. Failure to activate will result in the copy of Windows Vista being placed in Reduced Functionality Mode (RFM). There is no start menu, no desktop icons, and the desktop background is changed to black. After one hour, the system will log the user out without warning. It will not shut down the computer, and the user can log back in. This is different from the Windows XP RFM experience, which limited screen resolution, colors, sounds and other features.

It should be noted that in all versions of product activation, the software can be used during the Initial Grace period without entry of a product key. Once a copy of Windows Vista has moved into RFM, the user will be presented the four options listed in the following figure, at their next logon attempt:



Figure 5: Windows Activation Dialog box

- Users who already have a product key but have not activated their computer should click **Activate Windows online now**.
- By clicking **Access your computer with reduced functionality**, the default Web browser is started and the user is presented with an option to purchase a new product key. The Web browser will fully function and Internet connectivity will not be blocked.
- If the user has acquired another product key (either through eligibility for a MAK or by purchasing a key online), they can use the new key to activate by clicking **Retype your product key**.
- If no Internet connection is detected, the user can click **Show me other ways to activate** to use telephone activation. This option will not be active if an Internet connection is present on the system.

A copy of Windows Vista can go into RFM under the following two scenarios:

- **Scenario 1:** If any of the following events occurs for the given license type:
 - **For MAK activated and KMS host computers:** Failure to activate within the grace period (that is, 30 days after installation) or failure to renew activation within 30 days of a major hardware replacement
 - **For KMS activated computers:** Failure to activate with a KMS within 30 days of installation, failure to renew activation with KMS within 210 (180 days plus 30 days grace period) days of previous renewal, or failure to renew activation with KMS within 30 days of hard drive replacement
- **Scenario 2:** A copy of Windows Vista may be required to reactivate for the following reasons, and failure to successfully reactivate during the 30-day grace period will cause the copy of Windows Vista to go into RFM:
 - The activation process has been determined to have been tampered with or worked around, or other tampering of license files is detected.
 - A leaked, stolen, or prohibited product key is detected and blocked by Microsoft Product Activation servers. Product keys may be prohibited for any of the following reasons: The product key is abused, stolen, or pirated; the product key is seized as a result of anti-piracy enforcement efforts; the key is beta or test key and has been disabled; there was a manufacturing error in the key; or the key has been returned. When a copy of Windows enters RFM as a result of this scenario, the user is notified of this status via a message pop-up.

In the event that a system is placed into RFM, the following remedies are available:

- If a client has exceeded the grace period, the **Windows Activation** dialog box appears, as shown in Figure 5. Follow the prescribed activation process and the options already described. These include entering a new product key, obtaining a new product key, or re-entering the original product key.
- Reconnect a KMS-activated client to the network that houses the KMS host. The client automatically contacts the KMS host to renew its activation.
- If a KMS client cannot be returned to its home network but is able to access the Internet, it can be activated using a MAK. In the **RFM** dialog box, click **Change Product Key** to type the MAK. If the client is unable to connect to the Internet, you can also use telephone activation. Changing to a MAK does not provide an additional grace period. The client remains in RFM until the computer is activated—either via the Internet or by telephone. You can also supply the MAK through scripting by using the `slmgr.vbs` script

with the *-ipk* option. (See [Configure a client to use MAK Activation using a script](#) for details.)

Note Alternatively, to automate this process for end users (if the standard user activation option is enabled), the administrator can create a script called by a custom web page. See [Appendix 2: Standard User Activation Webpage](#).

- A client can be returned 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 unique machine ID (also known as *client machine ID*, or CMID). The number of times this can be repeated is limited and depends on how many times *sysprep /generalize* is run to create the distribution media. The maximum number of rearms possible is three. Note that rearm requires administrator privilege. However, an Administrator can enable use by ordinary users by creating the following registry entry:

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SL\UserOperations** (REG_DWORD) to *1*.

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](#) Description of the Microsoft Windows registry.

Appendix 1: Resolving Non-Genuine Issues on Computers

If either a Volume Activation 2.0 customer or Microsoft detects that a KMS key or a MAK has been misused, after discussions between the customer and Microsoft, the product key can be marked as invalid for activation and as non-Genuine. When a volume edition client visits Microsoft Web sites requiring Genuine Validation, it will have to download and run either an ActiveX® control or a small .exe application to access the download. If the computer is configured with an invalid key or tampered files are detected, the computer will fail Genuine Validation. The user will be notified by a watermark on the desktop and periodic notifications to validate the Genuine status of the system by visiting a Microsoft Web site. In addition, the computer may be placed in a 30-day non-Genuine grace period during which it needs to be configured with a new product key or reinstalled if tampered files are detected. For MAK configured systems, a new MAK must be installed and activated on the computer. For computers activated with an invalid KMS key, the KMS host must first be activated with a new KMS key. KMS clients will then reactivate themselves after contacting the reconfigured KMS host. In both scenarios, computers that have downloaded the Genuine Advantage ActiveX control must also visit the Genuine Advantage Web site to change their Genuine status from non-Genuine to Genuine after being activated with a new product key. If a new product key has not been installed and activated, and the status has not changed during the 30-day non-Genuine grace period, the computer will start in non-Genuine RFM. In RFM, a user will only have options to access Web sites using their browser for an hour, before being logged off by the system.

Two different approaches exist to correct the Genuine status of a computer that is running a volume licensed version of Windows Vista: the manual approach using `slmgr.vbs` and the Product Activation Wizard. This guide outlines both these approaches.

Note The script method (available post Windows Vista RTM) will help administrators perform network-based recovery of non-Genuine computers.

Recovering Non-Genuine Windows Vista Computers

This process is comprised of the following two steps:

1. Determine the reason for Genuine Validation failure.
2. Follow appropriate recovery steps for KMS or MAK-configured computers.

On a non-Genuine computer, examine the Application Event Log, for Event ID: 8209

Log Name: Application

Source: Microsoft-Windows-Security-Licensing-SLC

Event ID: 8209

The description field will provide an error code explaining the non-Genuine status of a computer.

Error Code	Reason
0x8004C40B	Tampered files
0x8004C465	Invalid or Blocked Product Key

Table 9: RFM Reason Error Codes

Recovery from Non-Genuine State Due to Tampered Files

It is recommended to re-install the operating system on computers that have non-Genuine status due to tampered files, after ensuring that all required user data has been saved to another location. After installing the operating system, the computer will have to be activated. The user can then validate Genuine status at:

<http://go.microsoft.com/fwlink/?LinkId=64187>.

Recovery from Non-Genuine State for Invalid or Blocked Product Key

If a KMS host or KMS client is marked non-Genuine due to a compromised product key, you need to replace the KMS key on all KMS hosts configured with the compromised product key. Then, you need to activate all KMS clients against the re-keyed KMS hosts.

To recover KMS hosts in non-Genuine Grace

1. Install the new KMS key on each KMS host configured with the invalid KMS key. Run `Slmgr.vbs [computername] [username] [password] -ipk <new_KMS_Key>` in an elevated command prompt.
2. Activate the new KMS key. Run `Slmgr.vbs [computername] [username] [password] -ato` in an elevated command prompt.
3. Verify that the new product key is installed by running: `Slmgr.vbs [computername] [username] [password] -dli` from a command prompt.
4. If the KMS host is installed with the Genuine Advantage ActiveX control, visit the Genuine Advantage Web site (<http://go.microsoft.com/fwlink/?LinkId=64187>) to validate the status.
5. Restart "Software Licensing" service by clicking **Start, Settings, Control Panel, Administrative Tools, and Services**. Select **Software Licensing Service** and click [Restart].
6. Restart the KMS host to remove the non-Genuine watermark from the desktop.

Note It is recommended not to download software from the Internet directly on a computer providing KMS services.

Next, perform the following steps to recover KMS clients:

To recover KMS clients in non-Genuine Grace

1. Reconfigure all KMS hosts as outlined in [To recover KMS Hosts in non-Genuine Grace](#).
2. Administrators can wait for all KMS clients to auto-renew their activations within 7 days (default), or force activation renewal by using the slmgr.vbs script: `slmgr.vbs [computername] [username] [password] -ato`.
3. Verify that clients activate themselves after contacting the reconfigured KMS host and by running `slmgr.vbs [computername] [username] [password] -dli` from a Command Prompt.
4. If the KMS client is installed with the Genuine Advantage ActiveX control, visit the Genuine Advantage Web site (<http://go.microsoft.com/fwlink/?LinkId=64187>) to validate the status.
5. Restart the client to remove the non-Genuine desktop watermark.

To recover MAK activated computers in non-Genuine Grace

1. Install a new MAK on each computer configured with the invalid MAK. Run `Slmgr.vbs [computername] [username] [password] -ipk <new_MAK_Key>` in an elevated command prompt.
2. Activate the new MAK. Run `Slmgr.vbs [computername] [username] [password] -ato` in an elevated command prompt.
3. Verify that the new product key is installed by running: `Slmgr.vbs [computername] [username] [password] -dli` from the command prompt.
4. If the MAK computer is installed with the Genuine Advantage ActiveX control, visit the Genuine Advantage Web site (<http://go.microsoft.com/fwlink/?LinkId=64187>) to validate the status.
5. Restart the system to remove the non-Genuine watermark from the desktop.

To recover KMS hosts or clients or MAK activated computers in non-Genuine RFM

1. For MAK configured computers, use the remote operations functionality of slmgr.vbs as detailed in the previous procedure: [To recover MAK activated computers in non-Genuine Grace](#).
2. For KMS hosts, use the remote operations functionality of slmgr.vbs as detailed in the previous procedure: [To recover KMS hosts in non-Genuine Grace](#).
3. For KMS clients, first ensure that the KMS host has been recovered as detailed in the previous procedure: [To recover KMS hosts in non-Genuine Grace](#). Then use the remote operations functionality of slmgr.vbs as detailed in the above section: [To recover KMS clients in non-Genuine Grace](#).
4. For computers in non-Genuine RFM, after completing step 1, 2 or 3, click the link in the non-Genuine RFM window to visit the Genuine Advantage Web site (<http://go.microsoft.com/fwlink/?LinkId=64187>) to validate the status.
5. Restart the computer to remove the desktop watermark.

Appendix 2: Recovery from RFM using Standard User Product Activation Web Page

By default, product activation in Windows Vista requires local administrator privileges. However, system administrators can configure computers for product activation by standard users by creating and setting the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\UserOperations (REG_DWORD) to 1.

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](#) Description of the Microsoft Windows registry.

Even after setting this registry value, the Product Activation Wizard will still be displayed with the User Account Control 'shield' icon. The standard user is left with two options for installing product keys and activating computers:

- **Command Line:** Use the slmgr.vbs script to install product keys, and activate the computer. For the specific syntax, see the "[Deployment Guidance](#)" section earlier in this guide.
- **Standard User Product Activation Web page (ProductActivation.htm):** In the file StandardUserProductActivation.zip, a sample Web page containing a VBScript is provided for administrators for implementing standard user activation. This Web page provides the standard user with several options:
 - **Product Keys:** Enter in a new product key or install an optional administrator configured product key
 - **Activation methods:** Activate using the Internet, activate over telephone, or reset the grace period for activation. The 'reset' option can be run only three times from the first time the operating system is installed. A reset is also performed when running 'sysprep /generalize'.

The StandardUserProductActivation.zip file can be downloaded from the Windows Vista Volume Activation 2.0 Download Center at <http://go.microsoft.com/fwlink/?LinkID=75674>

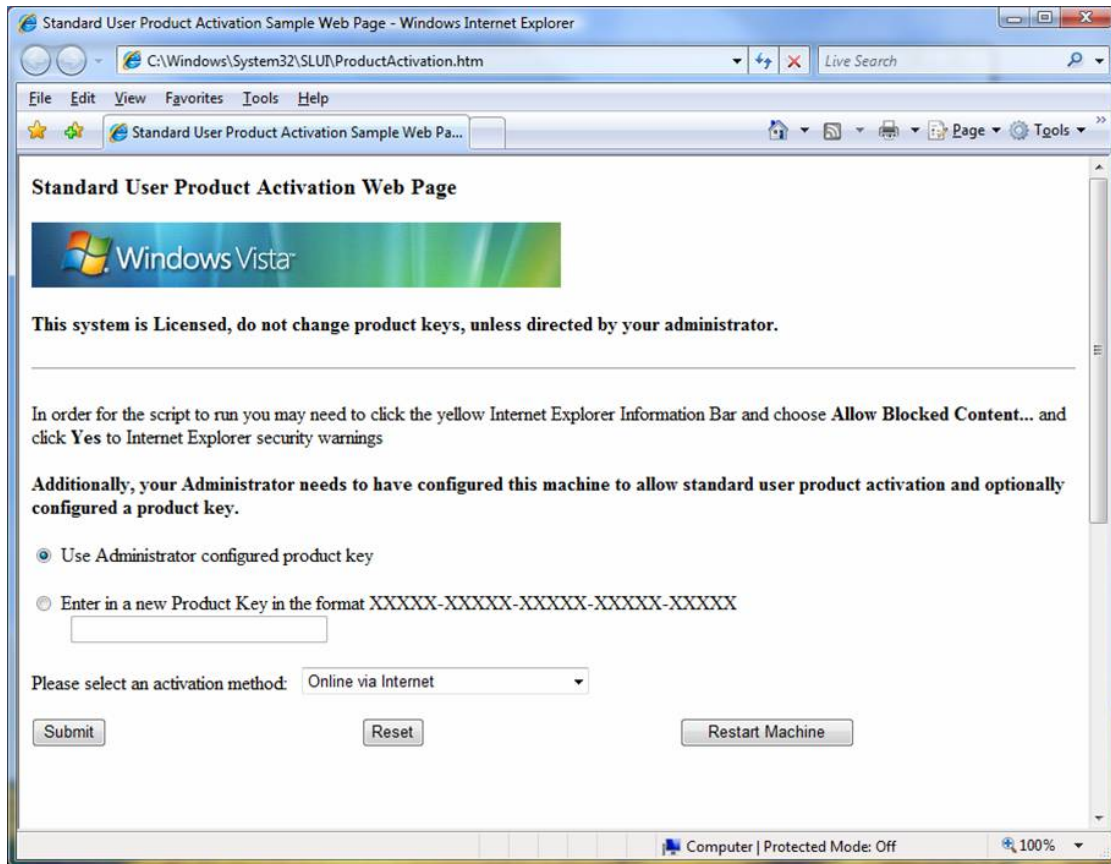


Figure 6: Standard User Product Activation Web page

System administrators can use this Web page to enable easier recovery for standard users whose computers are in RFM. When a user's computer is in RFM, they are provided the four choices shown in the following figure (upon logon):

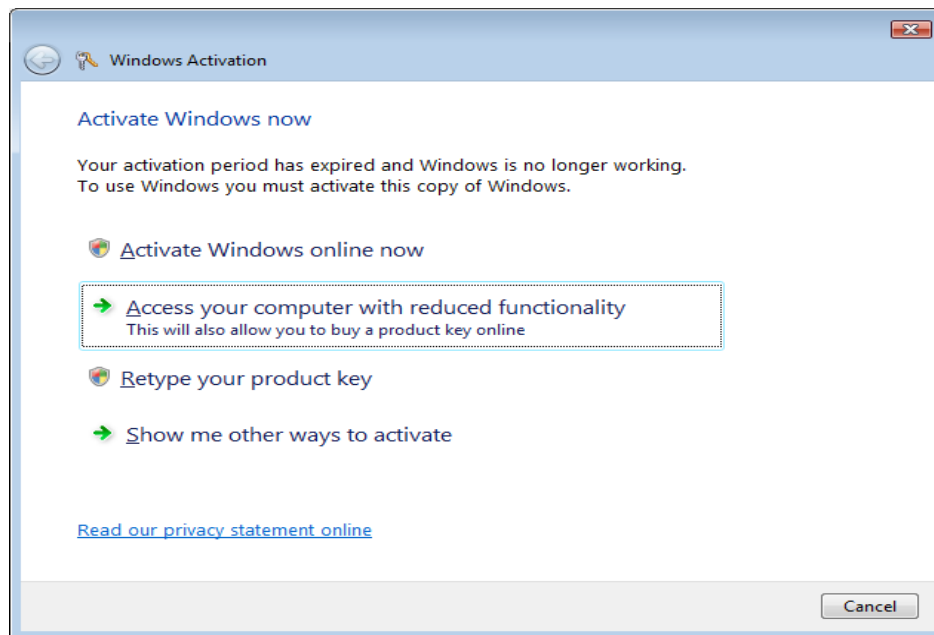


Figure 7: Reduced Functionality Mode screen

In this screen, the only option available to standard users is to choose 'Access your computer with reduced functionality', which will start the default Web browser on the system. After this is started, the standard user will need to access the Standard User Activation Web page, which would be in their Favorites (if previously installed by an administrator) and configure a new product key to return to full functionality mode. The user will have to allow ActiveX scripts to run so that the VBScript can use existing WMI methods to install a product key and activate the computer. Note this Web page requires the VBScript engine to work properly.

To deploy Standard User Product Activation Web page

1. On the reference system, install the Web page (productactivation.htm and windows-vista.png into a folder accessible by standard users, such as %systemroot%\system32\SLUI). It is recommended to customize the Web page for your organization to include support specific information such as telephone numbers and contact information.
2. Optionally, configure an administrator specified product key (5x5) in a file named pid.txt. The Web page (by default) is configured to look for this file in the %systemroot%\system32\SLUI folder.
3. This Web page can then be deployed as an Internet Explorer Favorite to users by a number of methods:
 - Use the Internet Explorer Administration Kit (IEAK).
 - Use Group Policy in Active Directory environments.
4. Configure the FavoritesList option in the component "Microsoft-Windows-IE-InternetExplorer" in an unattend.xml setup file.

To test the Standard User Product Activation Web page

1. On a computer that is not activated and is configured for Standard User activation, force the system to go into RFM mode, by advancing the clock ahead by 31 days and restarting the computer.
2. Log on as a Standard User on the computer. Verify if you see the RFM screen (Figure 7) and can choose **Access my computer with reduced functionality**.
3. Verify that Internet Explorer starts, and that the Standard User Product Activation Web page can be loaded from the Favorites menu.
4. Choose 'Yes' to any ActiveX prompts to allow the VBScript to run successfully.
5. Choose to install a new product key or the administrator configured key (if applicable), and choose the appropriate activation method.
6. Follow the steps in the Web page for manual phone activation (if applicable).
7. Verify the process completed successfully. Close the RFM wizard and restart the system.
8. Verify that logging on as a standard user or local administrator displays the desktop. Verify that the computer has been activated correctly by running 'slmgr -dli'.

Appendix 3: Resolving MOM 2003 Installation Issue

On 64-bit versions of Windows Vista, the MOM 2003 Agent (which is 32 bits) cannot see the version number stored in the registry. This value is used to determine membership in the Computer Group defined by the KMS MOM Pack. Without being joined in the Computer Group, the KMS will not provide data to the MOM server's data warehouse. The registry value is created by `slmgr.vbs` when the KMS is activated, and is stored by default in the 64-bit view of the registry.

There are two ways to workaroud this installation issue:

- This problem can be mitigated by creating a custom Computer Group on the MOM server that explicitly adds all KMS hosts for collection. This can be keyed off of *Machine Name* or any other queryable property.
- From an elevated command prompt, type `REGEDIT.EXE`. This will open the registry editor in an Administrative user context. In Regedit, copy the value of

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SL\KeyManagementServiceVersion

into

HKLM\Software\wow6432node\Microsoft\WindowsNT\CurrentVersion\SL\KeyManagementServiceVersion

Regardless of the workaround chosen, it is critical that all KMS hosts running the 64-bit version of the operating system have the same workaround applied.

Important note: This section contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: [256986](#) Description of the Microsoft Windows registry.

Appendix 4: Guidance Worksheet Job-Aid

Use this Sample Guidance Worksheet to map your computers to activation solution.

Criteria	Type of Activation	Number of Computers
Total number of computers to be activated	N/A	
Number of computers that will not connect at least once every 180 days	MAK	
Number of computers in environments where there are less than 25 computers	MAK	
Number of computers that will regularly connect to the network	KMS	
Number of computers in disconnected environments where there are more than 25 computers and no Internet connectivity	KMS	
Number of computers in disconnected environments where there are less than 25 computers and there no Internet connectivity	MAK	
Remaining computer count should be zero		

Table 10: Guidance Worksheet

Appendix 5: Understanding License States

Windows Vista utilizes five license states to track activation. The five states are Licensed, Initial Grace, non-Genuine Grace, Out of Tolerance Grace, and Unlicensed. The term “grace period” refers to a length of time provided to allow any necessary actions to return the computer to the licensed state. All grace periods last 30 days.

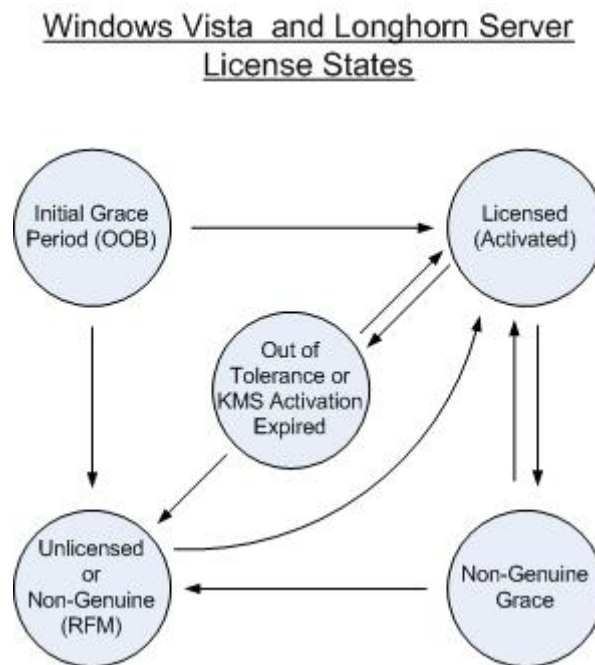


Figure 8: License States

- **Licensed:** Computers have been properly activated. Activation can happen in several ways including Internet and Phone activation. Additionally, KMS clients can activate themselves after contacting an activated KMS host.
- **Initial Grace (or OOB Grace):** Starts the first time you start your computer after you install the operating system. It provides 30 days for the computer to be activated. The initial grace period can only be restarted by running *sysprep /generalize*, or by using *slmgr.vbs -rearm*. These processes reset the Initial Grace timer to 30 days. This will only work three times.
- **Non-Genuine Grace:** Occurs only on a computer that has the Windows Genuine ActiveX control installed, and then fails Genuine Validation. The computer is marked non-Genuine, and the License State may be changed to non-Genuine Grace. If this happens, non-Genuine Grace provides 30 days for the computer to be reactivated and validated Genuine by revisiting the WGA website at <http://www.microsoft.com/genuine>.
- **Out of Tolerance Grace:** Begins when cumulative hardware changes on an activated computer push it beyond a tolerance level, or when a KMS client goes for 180 days without contacting a KMS. OOT Grace provides 30 days for a computer to be reactivated. A computer may be activated and then fall into OOT grace any number of times, and each time the OOT Grace timer will be reset to 30 days.

- **Unlicensed:** When any grace period is allowed to expire, the computer becomes Unlicensed. An Unlicensed computer runs in Reduced Functionality Mode (RFM), which provides users very limited access to the system in one-hour increments and presents a window containing links to properly license and activate the computer. If the computer falls into RFM from non-Genuine Grace, the user is presented with a window containing links and solutions specific to recovery from non-Genuine RFM. Further documentation on recovery from RFM is available in the "[Troubleshooting](#)" section earlier in this guide.

Additional Resources

- For answers to frequently asked questions about Windows Vista Volume Activation 2.0, refer to the "Volume Activation 2.0 FAQ" in <http://go.microsoft.com/fwlink/?LinkId=76702>
- For a list of WMI methods, KMS registry keys, KMS events, KMS error codes, and KMS RPC messages, refer to the "Volume Activation 2.0 Technical Attributes.xls" in <http://go.microsoft.com/fwlink/?LinkId=76703>
- For information about the Microsoft Solution Accelerator for Business Desktop Deployment (BDD): <http://go.microsoft.com/fwlink/?LinkId=76620>
- For a list of Volume License products available, go to: <http://www.microsoft.com/licensing/default.aspx>