**Volume Activation Planning Guide**

**Windows 7 and Windows Server 2008 R2**

Microsoft Corporation

Published: June 2009

Abstract

Volume Activation helps Volume Licensing customers automate and manage the activation process of Volume Licensing media. Volume Licensing customers and special program subscribers such as the Microsoft Partner Program, MSDN®, and Microsoft® TechNet—are eligible for Volume Licensing software and media. This guide is for information technology (IT) professionals whose organizations are planning to deploy Volume Activation versions of the Windows® 7 and Windows Server® 2008 R2 operating systems.

This document and any document referenced herein is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. 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.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Hyper-V, MSDN, Windows, the Windows logo, Windows Server, Windows Vista, and Windows Web Server are trademarks of the Microsoft group of companies.

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

**Contents**

[Introduction 5](#_Toc230000209)

[Learn About Product Activation 6](#_Toc230000210)

[Activation Options 6](#_Toc230000211)

[Retail 6](#_Toc230000212)

[Original Equipment Manufacturer 7](#_Toc230000213)

[Volume Licensing 7](#_Toc230000214)

[Volume Activation Models 8](#_Toc230000215)

[Key Management Service 8](#_Toc230000216)

[Multiple Activation Key 8](#_Toc230000217)

[What If Systems Are Not Activated? 9](#_Toc230000218)

[Grace Period 9](#_Toc230000219)

[Grace Period Expiration 9](#_Toc230000220)

[Product Keys 10](#_Toc230000221)

[Review Available Activation Models 11](#_Toc230000222)

[Key Management Service 11](#_Toc230000223)

[Minimum Computer Requirements 11](#_Toc230000224)

[How KMS Works 13](#_Toc230000225)

[Planning a KMS Deployment 15](#_Toc230000226)

[Multiple Activation Key 18](#_Toc230000227)

[Volume Activation Management Tool 19](#_Toc230000228)

[MAK Architecture 19](#_Toc230000229)

[Evaluate Client Connectivity 20](#_Toc230000230)

[Core Network 22](#_Toc230000231)

[Isolated Networks 23](#_Toc230000232)

[High-Security Zone 23](#_Toc230000233)

[Branch Office Locations 25](#_Toc230000234)

[Individual Disconnected Computers 26](#_Toc230000235)

[Test/Development Labs 26](#_Toc230000236)

[Map Computers to an Activation Method 28](#_Toc230000237)

[Determine Product Key Needs 29](#_Toc230000238)

[Choosing the MAK Key 30](#_Toc230000239)

[Choosing the KMS Key 31](#_Toc230000240)

[Choosing the KMS Host 33](#_Toc230000241)

[Determine Monitoring and Reporting Needs 35](#_Toc230000242)

[Windows Management Instrumentation 35](#_Toc230000243)

[System Center Configuration Manager 35](#_Toc230000244)

[Event Logs 36](#_Toc230000245)

[KMS Management Pack 36](#_Toc230000246)

[Volume Activation Management Tool 36](#_Toc230000247)

[Appendix A: Information Sent to Microsoft 37](#_Toc230000248)

[Appendix B: Licensing Conditions 38](#_Toc230000249)

[Activated 39](#_Toc230000250)

[Grace 39](#_Toc230000251)

[Genuine 39](#_Toc230000252)

[Notifications 40](#_Toc230000253)

# Introduction

Volume Activation is a configurable solution that helps IT pros automate and manage the product-activation process on computers that are running the Windows Vista®, Windows® 7, Windows Server® 2008, and Windows Server 2008 R2 operating systems licensed under a Microsoft® Volume Licensing program and other programs that provide Volume License editions of Windows. This guide provides planning steps and scenarios to assist in planning a Volume Activation deployment specifically for the Windows 7 and Windows Server 2008 R2 operating systems.

**Note**   This document provides Volume Activation planning guidance for the Windows 7 and Windows Server 2008 R2 operating systems. However, this guide does address interoperability between both generations of products. For more information about planning Volume Activation for Windows Vista and Windows Server 2008, see Volume Activation 2.0 Technical Guidance on the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkID=75674>).

A Volume Activation deployment includes the following steps:

1. Learn about product activation.
2. Review available activation models.
3. Evaluate client connectivity.
4. Map the physical computer or virtual machine to an activation method.
5. Determine product key needs.
6. Determine monitoring and reporting needs.

# Learn About Product Activation

Product activation is the process of validating software with the manufacturer. Activation confirms the genuine status of a product and that the product key is not compromised. It is analogous to the activation of credit cards or new mobile phones. Activation establishes a relationship between the software’s product key and a particular installation of that software on a device.

All activation methods that are used by Microsoft are designed to help protect user privacy. Data that is sent during activation is not traceable to the computer or user. The data that is gathered is used to confirm that the software is a legally licensed copy. It is then aggregated for statistical analysis. Microsoft does not use this information to identify or contact the user or organization.

For example, during online activations, information such as the software version, language, the product key, the Internet Protocol (IP) address, and information about the hardware of the device are sent to Microsoft. The IP address is used only to verify the location of the request because some editions of Windows such as Windows 7 Starter can be activated only within certain target market geographies.

## Activation Options

Licenses for Windows 7 and Windows Server 2008 R2 can be obtained through one of three basic channels: retail, original equipment manufacturer (OEM), or Volume Licensing. Each channel has its own unique methods of activation. Because organizations can obtain their operating systems through any of the three available channels, they can choose a combination of activation methods.

### Retail

Windows 7 and Windows Server 2008 R2 products that are acquired through a retail store are individually licensed and are activated in the same way as retail versions of the Windows Vista and Windows Server 2008 operating systems. Each purchased copy comes with one unique product key (printed on the product packaging), which the user enters during the product installation. The computer uses this product key to complete the activation after the installation of the operating system is complete. This final activation step can be accomplished online or by telephone.

### Original Equipment Manufacturer

Most OEMs sell systems that include a standard build of the Windows 7 or Windows Server 2008 R2 operating system. Hardware vendors perform OEM activation by associating the operating system to the firmware (basic input/output system, or BIOS) of the computer. This process occurs before the computer is sent to the customer so that no additional actions are required by the user. This method of activation is known as OEM activation.

OEM activation is valid as long as the customer uses the OEM-provided image on a system. To create a customized image, customers can use the image provided by the OEM as the basis for creating the custom image. Otherwise, a different activation method must be used. For further details on customizing Windows and activation impacts refer to the following [whitepaper](http://go.microsoft.com/fwlink/?LinkID=137292&clcid=0x409).

**Note**OEM activation is applicable to computers with Windows installed that are purchased through OEM channels.

### Volume Licensing

Microsoft Volume Licensing offers customized programs that are tailored to the size and purchasing preference of the organization. These programs provide simple, flexible, and affordable solutions that enable organizations to easily manage their licenses. To become a Volume Licensing customer, the organization needs to set up a Volume License agreement with Microsoft.

There are two legal ways to acquire a full license for a new computer with a Windows client operating system.The first and most economical way is to have the license preinstalled through the original equipment manufacturer.The other option is to purchase a fully packaged retail product.

Microsoft Volume Licensing programs such as Open License, Select License, and Enterprise Agreements coveronly upgrades to Windows client operating systems. A qualifying OS licensing is needed for each computer before upgrade rights obtained through Volume Licensing can be exercised on these computers.

For more information on Volume Licensing including list of qualifying OS, go to <http://go.microsoft.com/fwlink/?LinkId=73076>.

**Note:**   Some editions of Windows, such as Windows 7 Enterprise, are available only through the Volume Licensing channel.

## Volume Activation Models

Volume Activation allows volume license customers to automate the activation process so that it is transparent to users. Volume Activation applies to computers that are covered under a Volume Licensing program. It is used strictly as a tool for activation, and it is not tied to license invoicing or billing.

Volume Activation provides two models for completing volume activations: Key Management Service (KMS) and Multiple Activation Key (MAK). KMS allows organizations to activate systems within their network, and MAK activates systems on a one-time basis by using the hosted activation services provided by Microsoft. Customers can use either or both key types to activate systems in their environments.

### Key Management Service

With KMS, IT pros can complete activations on their local network, eliminating the need for individual computers to connect to Microsoft for product activation. KMS is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. By default, volume editions of Windows 7 and Windows Server 2008 R2 connect to a system that hosts the KMS service to request activation. No action is required from the user.

KMS requires a minimum number of computers (physical or virtual machines) in a network environment. The organization must have at least five computers to activate Windows Server 2008 R2 and at least 25 computers to activate clients that are running Windows 7. These minimums are referred to as activation thresholds.

To use KMS activation with Windows 7, the computer must have the qualifying OS license (often obtained through OEMs as part of the new PC purchase) and contain a Windows Marker in BIOS.

### Multiple Activation Key

MAK is used for one-time activation with Microsoft’s hosted activation services. There are two ways to activate computers using MAK. The first method is MAK Independent activation, which requires that each computer independently connect and be activated with Microsoft either over the Internet or by telephone. The second method is MAK Proxy activation. With this method, a computer acting as a MAK proxy gathers activation information from multiple computers on the network, and then sends a centralized activation request on their behalf. MAK Proxy activation is configured using the Volume Activation Management Tool (VAMT).

**Note**   KMS is the default key for Volume Activation clients. Using MAK activation requires installing a MAK key. For more information about converting KMS clients to MAK, see the [*Volume Activation Deployment Guide*](http://go.microsoft.com/fwlink/?LinkId=150083).

## What If Systems Are Not Activated?

Activation is designed to provide a transparent activation experience for users. If activation does not occur immediately after the operating system is installed, Windows 7 and Windows Server 2008 R2 still provide the full functionality of the operating system for a limited amount of time, or grace period. The length of a grace period is 30 days for Windows 7 and Windows Server 2008 R2. After the grace period expires, both operating systems remind the user through notifications to activate the computer.

### Grace Period

During the initial grace period, there are periodic notifications that the computer requires activation. Once per day, during the logon process, a notification appears to remind the user to activate the operating system. This continues until there are three days remaining in the grace period. For the first two of the final three days of the grace period, the notification appears every four hours. During the final day of the grace period, the notification appears every hour, on the hour.

### Grace Period Expiration

After the initial grace period expires or activation fails, Windows 7 and Windows Server 2008 R2 continue to notify users that the operating system requires activation. Until the operating system is activated, reminders that the computer must be activated appear in several places throughout the product:

* Notification dialogs appear during logon after user credentials entry.
* Notifications appear at the bottom of the screen above the notification area.
* A persistent desktop notification remains with a black desktop background.
* A reminder might appear when users open certain Windows applications.

## Product Keys

Volume Activation does not change how Volume Licensing customers obtain their product keys. They can obtain MAK and KMS keys at the Volume Licensing Service Center (VLSC) Web site at <http://go.microsoft.com/fwlink/?LinkId=107544> or by calling an Activation Call Center. Service Provider License Agreement (SPLA) partners can only obtain keys by calling an Activation Call Center. Customers in the United States can call 1-888-352-7140. International customers should contact their local support center. For the telephone numbers of Activation Call Centers worldwide, go to <http://go.microsoft.com/fwlink/?LinkId=107418>. When calling a support center, customers must have the Volume License agreement.

Volume Licensing customers can log on to the VLSC Web site at any time to view their KMS key information. The VLSC Web site also contains information on how to request and use MAKs. For more information about MAK and KMS keys, including information about increasing the number of allowed activations, see the **Existing Customers** page at <http://go.microsoft.com/fwlink/?LinkId=74008>.

# Review Available Activation Models

Volume Activation provides the following activation models:

* Key Management Service (KMS)
* Multiple Activation Key (MAK)

The model chosen depends on the size, network infrastructure, connectivity, and security requirements of the organization. IT pros can choose to use only one or a combination of these activation models.

**Note**Token-based Activation is a specialized activation option available for approved Microsoft Volume Licensing customers. It is designed for use in specific scenarios, where the end systems are completely disconnected from the network or phone. This option enables customers to use public key infrastructure (PKI) and digital certificates (or *tokens*, typically stored on smart cards) to activate Windows 7 Enterprise and Windows Server 2008 R2 locally without contacting either customer-hosted KMS or the Microsoft-hosted activation service using MAK. For more information about Token-based Activation, contact a Microsoft Account Team or Services Representative.

## Key Management Service

KMS activates computers on a local network, eliminating the need for individual computers to connect to Microsoft. To do this, KMS uses a client–server topology. KMS client computers can locate KMS host computers by using Domain Name System (DNS) or a static configuration. KMS clients contact the KMS host by using remote procedure call (RPC). KMS can be hosted on computers that are running the Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

### Minimum Computer Requirements

When planning for KMS activation, the network must meet or exceed the activation threshold, or the minimum number of qualifying computers that KMS requires. IT pros must also understand how the KMS host tracks the number of computers on the network.

#### KMS Activation Thresholds

KMS can activate both physical computers and virtual machines. To qualify for KMS activation, a network must have a minimum number of qualifying computers, called the activation threshold. KMS hosts activate clients only after meeting this threshold. To ensure that the activation threshold is met, a KMS host counts the number of computers that are requesting activation on the network.

The KMS client computers are activated after meeting the activation threshold. The computers running Windows server 2008 or Windows Server 2008 R2 the activation threshold is five. For computers running Windows Vista or Windows 7 the activation threshold is 25. The thresholds include clients and servers that are running on physical computers or virtual machines.

A KMS host responds to each valid activation request from a KMS client with the count of how many computers have contacted the KMS host for activation. Clients that receive a count below their activation threshold are not activated. For example, if the first two computers that contact the KMS host are running Windows 7, the first receives an activation count of 1, and the second receives an activation count of 2. If the next computer is a Windows 7 virtual machine, it receives an activation count of 3, and so on. None of these computers is activated, because computers running Windows 7 must receive an activation count ≥25 to be activated. KMS clients in the grace state that are not activated because the activation count is too low connect to the KMS host every two hours to get the current activation count and will be activated when the threshold is met.

If the next computer that contacts the KMS host is running Windows Server 2008 R2, it receives an activation count of 4, because activation counts are a combination of computers running Windows Server 2008 R2 and Windows 7. If a computer running Windows Server 2008 or Windows Server 2008 R2 receives an activation count that is ≥5, it is activated. If a computer running Windows 7 receives an activation count ≥25, it is activated.

#### Activation Count Cache

To track the activation threshold, the KMS host keeps a record of the KMS clients that request activation. The KMS host gives each KMS client a client machine identification (CMID) designation, and the KMS host saves each CMID in a table. Each activation request remains in the table for 30 days. When a client renews its activation, the cached CMID is removed from the table, a new record is created, and the 30-day period begins again. If a KMS client does not renew its activation within 30 days, the KMS host removes the corresponding CMID from the table and reduces the activation count by one.

The KMS host caches twice the number of CMIDs that KMS clients require to help ensure that the CMID count does not drop below the activation threshold. For example, on a network with clients that are running Windows 7, the KMS activation threshold is 25. The KMS host caches the CMIDs of the most recent 50 activations. The KMS activation threshold for Windows Server 2008 R2 is five. A KMS host that is contacted only by KMS clients that are running Windows Server 2008 R2 would cache the 10 most recent CMIDs. If a client that is running Windows 7 later contacts that KMS host, KMS increases the cache size to 50 to accommodate the higher threshold. KMS never reduces the cache size.

### How KMS Works

KMS activation requires TCP/IP connectivity. By default, KMS hosts and clients use DNS to publish and find the KMS service. The default settings can be used, which require little to no administrative action, or KMS hosts and clients can be manually configured based on network configuration and security requirements.

#### KMS Activation Renewal

KMS activations are valid for 180 days. This is called the activation validity interval. To remain activated, KMS clients must renew their activation by connecting to the KMS host at least once every 180 days. By default, KMS client computers attempt to renew their activation every seven days. IF KMS activation fails, the client will retry every two hours. After a client’s activation is renewed, the activation validity interval begins again.

#### Publication of the KMS Service

The KMS service uses service (SRV) resource records (RR) in DNS to store and communicate the locations of KMS hosts. KMS hosts use DNS dynamic update protocol, if available, to publish the KMS SRV RRs. If dynamic update is not available or the KMS host does not have rights to publish the RRs, the DNS records must be published manually, or IT pros must configure client computers to connect to specific KMS hosts.

**Note**DNS changes may take time to propagate to all DNS hosts, depending on the complexity and topology of the network.

#### Client Discovery of the KMS Service

By default, KMS clients query DNS for KMS service information. The first time a KMS client queries DNS for KMS service information, it randomly chooses a KMS host from the list of SRV RRs that DNS returns.

The address of a DNS server containing the SRV RRs can be listed as a suffixed entry on KMS clients, which allows advertisement of SRV RRs for KMS in one DNS server and KMS clients with other primary DNS servers to find it.

Priority and weight parameters can be added to the **DnsDomainPublishList** registry value for KMS. Establishing KMS host priority groupings and weighting within each group allows IT pros to specify which KMS host the clients should try first and balances traffic among multiple KMS hosts. Only Windows 7 and Windows Server 2008 R2 provide the priority and weight parameters.

If the KMS host that a client selects does not respond, the KMS client removes that KMS host from its list of SRV RRs and randomly selects another KMS host from the list. When a KMS host responds, the KMS client caches the name of the KMS host and uses it for subsequent activation and renewal attempts. If the cached KMS host does not respond on a subsequent renewal, the KMS client discovers a new KMS host by querying DNS for KMS SRV RRs.

By default, client computers connect to the KMS host for activation by using anonymous RPCs through TCP port 1688. (IT pros can change the default port.) After establishing a TCP session with the KMS host, the client sends a single request packet. The KMS host responds with the activation count. If the count meets or exceeds the activation threshold for that operating system, the client is activated and the session is closed. The KMS client uses this same process for renewal requests. The communication each way is 250 bytes.

### Planning a KMS Deployment

The KMS service does not require a dedicated server. The KMS service can be co-hosted with other services, such as Active Directory® Domain Services (AD DS) domain controllers and read-only domain controllers (RODCs). KMS hosts can also run on physical computers or virtual machines that are running any supported Windows operating system, including Windows Server 2003. Although a KMS host that is running Windows Server 2008 R2 can activate any Windows operating system that supports Volume Activation, a KMS host that is running Windows 7 can activate only computers running Windows 7 and Windows Vista clients. A single KMS host can support unlimited numbers of KMS clients; however, Microsoft recommends deploying a minimum of two KMS hosts for failover. Most organizations can use as few as two KMS hosts for their entire infrastructure.

**Note**KMS is not automatically included in Windows Server 2003. To host KMS on computers that are running Windows Server 2003, download and install KMS from one of the following sites:

* For x86-based computers: Key Management Service 1.1 (x86) for Windows Server 2003 SP1 and Later (<http://go.microsoft.com/fwlink/?LinkID=82964>)
* For x64-based computers: Key Management Service 1.1 (x64) for Windows Server 2003 SP1 and Later (<http://go.microsoft.com/fwlink/?LinkId=83041>).

#### Planning DNS Server Configuration

The default KMS auto-publishing feature requires SRV RR and DNS dynamic update protocol support. KMS client default behavior and KMS SRV RR publishing are supported on a DNS server that is running Microsoft software or any other DNS server that supports SRV RRs (per Internet Engineering Task Force [IETF] Request for Comments [RFC] 2782) and dynamic updates (per RFC 2136) . For example, Berkeley Internet Domain Name (BIND) versions 8.x and 9.x support both SRV records and dynamic update.

The KMS host must be configured so that it has the credentials needed to create and update SRV, A (Internet Protocol version 4, or IPv4), and AAAA (Internet Protocol version 6, or IPv6) RRs on the DNS servers, or the records need to be created manually. The recommended solution for giving the KMS host the needed credentials is to create a security group in AD DS, and then add all KMS hosts to that group. In a DNS server that is running Microsoft software, ensure that this security group is given full control over the \_VLMCS.\_TCP record on each DNS domain that will contain the KMS SRV RRs.

#### Activating the First KMS Host

KMS hosts on the network need to install a KMS key, and then be activated with Microsoft. Installation of a KMS key enables the Key Management Service on the KMS host. After installing the KMS key, complete the activation of the KMS host by telephone or online. Beyond this initial activation, a KMS host does not communicate any information to Microsoft.

KMS keys are only installed on KMS hosts, never on individual KMS clients. Windows 7 and Windows Server 2008 R2 have safeguards to help prevent inadvertently installing KMS keys on KMS client computers. Any time users try to install a KMS key, they see the warning shown in Figure 1.



Figure 1   Installing a KMS key

#### Activating Subsequent KMS Hosts

Each KMS key can be installed on up to six KMS hosts, which can be physical computers or virtual machines. After activating a KMS host, the same host can be reactivated up to nine more times with the same key.

If the organization needs more than six KMS hosts, IT pros can request additional activations for the organization’s KMS key by calling the Activation Call Center to request an exception. For more information, see the Volume Licensing Web site at <http://go.microsoft.com/fwlink/?LinkID=73076>.

#### Upgrading Existing KMS Hosts

KMS hosts that are running Windows Server 2003, Windows Vista, or Windows Server 2008 can be configured to support KMS clients that are running Windows 7 and Windows Server 2008 R2. For Windows Vista and Windows Server 2008, it is necessary to update the KMS host with a package with files that support the expanded KMS client. This package is available through the Microsoft Download Center at <http://www.microsoft.com/downloads> or through Windows Update and Windows Server Update Services (WSUS). Once the package is installed on the KMS host, a KMS key that is designed to support Windows 7 and Windows Server 2008 R2 can be installed and activated as described earlier in this guide. The KMS key that supports the new versions of the Windows operating systems also provides support for the previous Volume License editions of Windows that are acting as KMS clients.

In the case of updating a Windows Server 2003 KMS host, all necessary files are contained within the KMS 1.2 downloadable package, which is available through the Microsoft Download Center at <http://www.microsoft.com/downloads>.

#### Planning KMS Clients

By default, computers that are running Volume License editions of Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 are KMS clients, and no additional configuration is needed. KMS clients can locate a KMS host automatically by querying DNS for SRV RRs that publish the KMS service. If the network environment does not use SRV RRs, a KMS client can be manually configured to use a specific KMS host.

To manually configure KMS clients, follow the steps in the [Volume Activation Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=150083).

#### Activating as a Standard User

Windows 7 and Windows Server 2008 R2 do not require administrator privileges for activation. However, this change does not allow standard user accounts to remove Windows 7 or Windows Server 2008 R2 from the activated state. An administrator account is still required for other activation- or license-related tasks, such as “rearm.”

## Multiple Activation Key

A MAK is used for one-time activation with Microsoft’s hosted activation services. Each MAK has a predetermined number of allowed activations; this number is based on Volume Licensing agreements and does not match the organization’s exact license count. Each activation using a MAK with Microsoft’s hosted activation service counts toward the activation limit.

There are two ways to activate computers by using a MAK:

* MAK Independent activation. Each computer independently connect and be activated with Microsoft, over the Internet or by telephone. MAK Independent activation is best suited for computers within an organization that do not maintain a connection to the corporate network.
* MAK Proxy activation. MAK Proxy activation enables a centralized activation request on behalf of multiple computers with one connection to Microsoft. MAK Proxy activation is configured using the Volume Activation Management Tool (VAMT). MAK Proxy activation is appropriate for environments in which security concerns may restrict direct access to the Internet or the corporate network. It is also suited for development and test labs that lack this connectivity.

MAK is recommended for computers that rarely or never connect to the corporate network and for environments in which the number of computers needing activation does not meet the KMS activation threshold. MAK can be used for individual computers or with an image that can be duplicated or installed by using Microsoft deployment solutions. MAK can also be used on a computer that was originally configured to use KMS activation. This is useful for moving a computer off the core network to a disconnected environment.

### Volume Activation Management Tool

Included in the Windows Automated Installation Kit (Windows AIK), VAMT is a stand-alone application that collects activation requests from several computers, and then sends them to Microsoft in bulk. VAMT allows IT pros to specify a group of computers to activate using AD DS, workgroup names, IP addresses, or computer names. After receiving the activation confirmation codes, VAMT distributes them to the computers that requested activation. Because VAMT also stores these confirmation codes locally, it can reactivate a previously activated computer after it is reimaged without contacting Microsoft. Additionally, VAMT can be used to easily transition computers between MAK and KMS activation methods.

Download the Windows Automated Installation Kit (AIK) for Windows 7 RC (<http://go.microsoft.com/fwlink/?LinkId=136976>) from the Microsoft Download Center.

### MAK Architecture

MAK Independent activation installs a MAK product key on a client computer. The key instructs that computer to activate with Microsoft servers over the Internet. In MAK Proxy activation, VAMT installs a MAK product key on a client computer, obtains the installation ID (IID) from the target computer, sends the IID to Microsoft on behalf of the client, and obtains a confirmation ID (CID). The tool then activates the client by installing the CID.

# Evaluate Client Connectivity

Each Volume Activation method is best suited to a particular network configuration. To select the best activation method or methods for the organization, assess the network environment to identify how different groups of computers connect to the network. Connectivity to the corporate network, Internet access, and the number of computers that regularly connect to the corporate network are some of the important configuration characteristics to identify. Most medium- to large-sized organizations use a combination of activation methods because of the varied ways their client computers connect to the networks.

KMS is the recommended activation method for computers that are well connected to the organization’s core network or that have periodic connectivity, such as computers that are offsite. MAK is the recommended activation method for computers that are offsite with limited connectivity or that cannot connect to the core network because of security restrictions. These include computers in lab and development environments that are isolated from the core network.

Table 1 lists common network configurations and the best practice recommendations for each configuration. Each solution factors in the number computers and network connectivity of the activation clients.

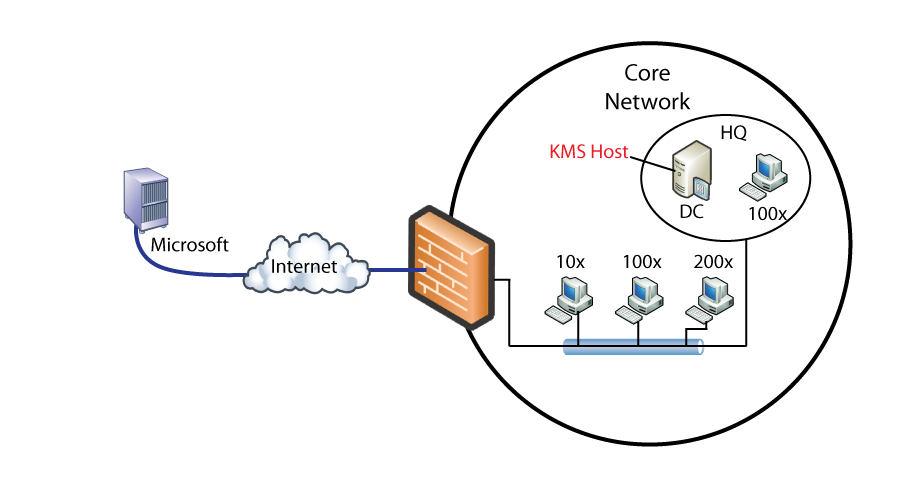
Table 1   Planning Considerations by Network Infrastructure

| **Network Infrastructure** | **Recommendations** | **Considerations** |
| --- | --- | --- |
| **Core network**  Well-connected local area network (LAN)  Most common scenario | If total computers > KMS activation threshold:   * Small (<100 machines): KMS host = 1 * Medium (>100 machines): KMS host ≥ 1 * Enterprise: KMS host > 1   If total computers ≤ KMS activation threshold:   * MAK (by telephone or Internet) * MAK Proxy | * Minimize the number of KMS hosts * Each KMS host must consistently maintain a count of total machines > KMS activation threshold * KMS hosts are autonomous * KMS host is activated by telephone or Internet |
| **Isolated network**  Branch office, high-security network segments, perimeter networks  Well-connected zoned LAN | If ports on firewalls can be opened between KMS clients and hosts:   * Use KMS hosts in core network   If policy prevents firewall modification:   * Use local KMS hosts in an isolated network * MAK (by telephone or Internet) * MAK Proxy | * Firewall configuration   + RPC over TCP (TCP port 1688)   + Initiated by the client * Change management on firewall rule sets |
| **Test or development lab**  Isolated network | If total computers > KMS activation threshold:   * KMS host = 1 (per isolated network)   If total computers ≤ KMS activation threshold:   * No activation (reset grace period) * MAK (by telephone) * MAK Proxy performed manually | * Variable configuration * Limited number of computers * KMS host and MAK activation through telephone; MAK Proxy performed manually |
| **Individual disconnected computer**  No connectivity to the Internet or core network  Roaming computers that periodically connect to the core network or connect through a virtual private network (VPN)  Roaming computers with Internet access but no connection to the core network | For clients that connect periodically to the core network:   * Use the KMS hosts in the core network   For clients that never connect to the core network or have no Internet access:   * MAK (by telephone)   For networks that cannot connect to the core network:   * If total computers > KMS activation threshold:   + Small: KMS host = 1   + Medium: KMS host ≥ 1   + Enterprise: KMS host > 1 * If total computers ≤ KMS activation threshold, MAK Independent or MAK Proxy performed manually   For clients that never connect to the core network but have Internet access:   * MAK (by Internet) | * Restricted environments or networks that cannot connect to other networks * KMS host can be activated, moved to disconnected network * KMS host and MAK activation by telephone; MAK Proxy performed manually |

The following sections describe examples of Volume Activation solutions in heterogeneous corporate environments that require more than one activation method. Each scenario has a recommended activation solution, but some environments may have infrastructure or policy requirements that are best suited to a different solution.

## Core Network

A centralized KMS solution is recommended for computers on the core network. This solution is for networks that have well-connected computers on multiple network segments that also have a connection to the Internet. Figure 2 shows a core network with a KMS host.

Figure 2   Core network scenario

**Note**A KMS host can be installed on a virtual machine, but select a virtual machine that is unlikely to be moved to a different host computer. If the virtual KMS host is moved to a different host computer, the operating system detects the change in the underlying hardware, and the KMS host must reactivate with Microsoft. KMS hosts can activate with Microsoft up to nine times.

## Isolated Networks

Many organizations have networks that are separated into multiple security zones. Some networks have a high-security zone that is isolated because it has sensitive information, while other networks are separated from the core network because they are in a different physical location (such as branch office locations).

### High-Security Zone

High-security zones are network segments that are separated by a firewall that limits communication to and from other networks segments. If the computers in a high-security zone are allowed access to the core network by allowing TCP port 1688 outbound from the high-security zone and an RPC reply inbound, activate computers in the high-security zone by using KMS hosts located in the core network. This way, the number of client computers in the high-security network does not have to meet any KMS activation threshold.

If these firewall exceptions are not authorized and the number of total computers in the high-security zone is sufficient to meet KMS activation thresholds, add a local KMS host to the high-security zone. Then, activate the KMS host in the high-security zone by telephone.

Figure 3 shows an environment that has a corporate security policy that does not allow traffic between computers in the high-security zone and the core network. Because the high-security zone has enough computers to meet the KMS activation threshold, the high-security zone has its own local KMS host. The KMS host itself is activated by telephone.

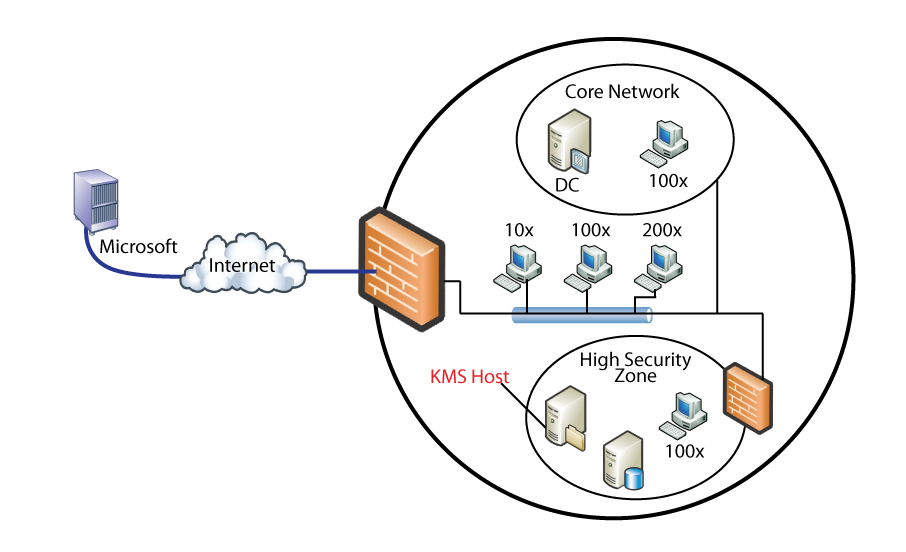


Figure 3   High-security network scenario

If KMS is not appropriate because there are only a few computers in the high-security zone, MAK Independent activation is recommended. Each computer can be activated independently with Microsoft by telephone.

MAK Proxy activation by using VAMT is also possible in this scenario. Because the computers in the high-security zone do not have Internet access, VAMT can discover them by using AD DS, computer name, IP address, or membership in a workgroup. VAMT uses Windows Management Instrumentation (WMI) to install MAK product keys and CIDs and to retrieve status on MAK clients. Because this traffic is not allowed through the firewall, there must be a local VAMT host in the high-security zone.

### Branch Office Locations

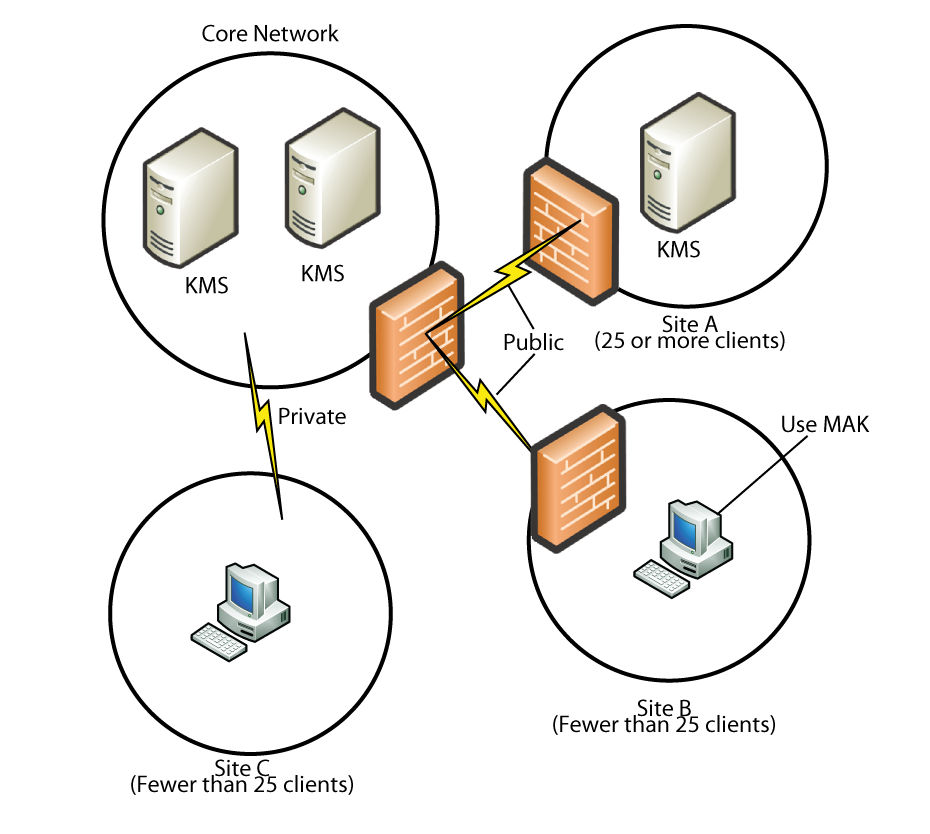
Figure 4 shows an enterprise network that supports client computers in three branch offices. Site A uses a local KMS host, because it has more than 25 client computers, and it does not have secure TCP/IP connectivity to the core network. Site B uses MAK activation, because KMS does not support sites with fewer than 25 KMS client computers, and the site is not connected by a secure link to the core network. Site C uses KMS, because it is connected to the core network by a secure connection over a private wide area network (WAN), and activation thresholds are met by using core network KMS clients.

Figure 4   Branch office scenario

## Disconnected Individual Computers

Some users in an organization may be in remote locations or may travel to many locations. This scenario is common for roaming clients, such as the computers of salespeople or other users who are offsite but not at branch locations. This scenario can also apply to remote branch office locations that have no connection or an intermittent connection to the core network.

Disconnected computers can use KMS or MAK depending on how often the computers connect to the core network. Use KMS activation for computers that connect to the core network—directly or through a VPN—at least once every 180 days and where the core network is using KMS activation. Use MAK Independent activation—by telephone or the Internet—for computers that rarely or never connect to the core network. Figure 5 shows disconnected clients that are using MAK Independent activation through the Internet and the telephone.

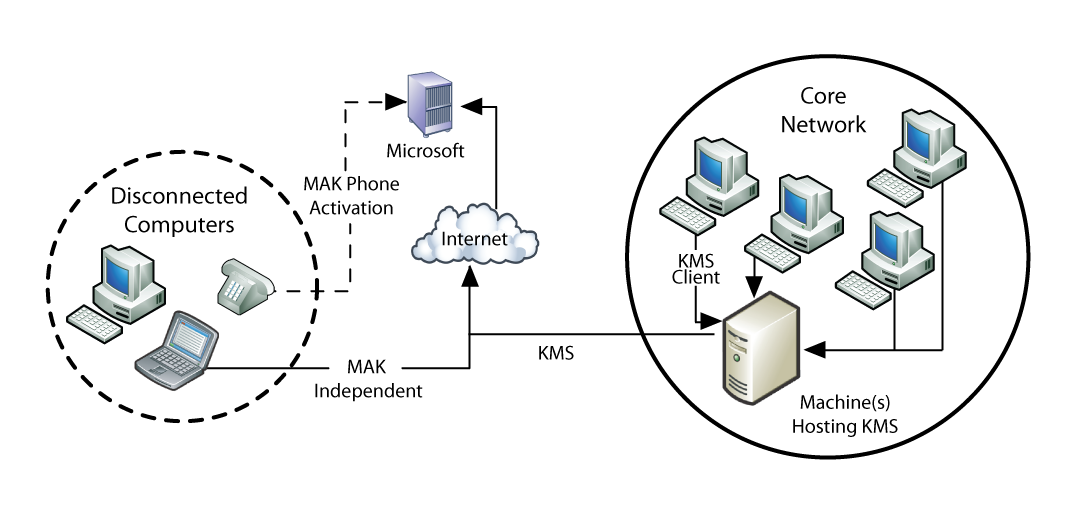


Figure 5   Disconnected computers scenario

## Test and Development Labs

Lab environments usually have large numbers of virtual machines, and computers in labs are reconfigured frequently. Determine whether the computers in test and development labs need activation. The initial 30-day grace period of a computer that is running Windows 7 or Windows Server 2008 R2 can be reset three times without activating it. Therefore, if you are rebuilding lab computers within 120 days, these computers need not be activated.

If lab computers do require activation, use KMS or MAK activation. Use KMS activation if the computers have connectivity to a core network that is using KMS. If the number of computers in the lab meets the KMS activation threshold, deploy a local KMS host.

In labs that have a high turnover of computers as well as a small number of KMS clients, it is important to monitor the KMS activation count to maintain a sufficient number of cached CMIDs on the KMS host. A KMS host caches activation requests from computers for 30 days. (See the section “[Minimum Computer Requirements](#_Minimum_Computer_Requirements)” earlier in this guide for more information about how CMIDs affect activations.) If the lab environment needs activation but does not qualify for KMS activation, use MAK activation. MAK clients are activated by telephone or over the Internet, whichever is available to the lab.

MAK Proxy activation with VAMT can also be used in this scenario. Install VAMT in the isolated lab network and also in a network that has access to the Internet. In the isolated lab, VAMT performs discovery, obtains status, installs a MAK product key, and obtains the IID of each computer in the lab. This information can then be exported from VAMT, saved to removable media, and then the file can be imported to a computer that is running VAMT and has access to the Internet. VAMT sends the IIDs to Microsoft and obtains the corresponding CIDs that are needed to complete activation. After exporting this data to removable media, take it to the isolated lab to import the CIDs so that VAMT can complete the activations.

**Note**In High Security mode, VAMT removes all personally identifiable information (PII) from the file that it exports. This file is a readable Extensible Markup Language (XML) file that can be reviewed in any XML or text editor.

# Map Computers to an Activation Method

After evaluating the recommended activation scenarios, the next step is using Volume Activation to map computers to activation methods. The goal is to ensure that all computers are associated with an activation option. Table 2 provides a simple job aid that ensures that all computers are mapped to an activation method. When completing this job aid, ensure that all computers using KMS are on networks that meet KMS activation thresholds.

Table 2. Activation Method Worksheet

|  |  |  |
| --- | --- | --- |
| Criterion | Activation method | Number of computers |
| Total number of computers to be activated | |  |
| Number of computers that will connect to the network at least once every 180 days (directly or by VPN) and where the KMS activation threshold is met | KMS |  |
| Number of computers that do not connect to network at least once every 180 days | MAK |  |
| Number of computers in isolated networks where the KMS activation threshold is met | KMS |  |
| Number of computers in isolated networks where the KMS activation threshold is not met | MAK |  |
| Number of computers in test/development labs that will not be activated | None |  |
| Remaining computer count should be zero | |  |

# Determine Product Key Needs

The Windows 7 and Windows Server 2008 R2 operating systems come in a variety of editions. To simplify Volume Activation and the number of product keys that an organization needs, Microsoft created *product key groups*. Product keys for KMS and MAK apply to product groups rather than individual editions; however, KMS and MAK use product key groups differently:

* MAK activation uses product key groups as individual groupings. Product keys for MAK activations are directly associated with a single product group and can only activate the Windows editions within that specific product group.
* With KMS, product keys work hierarchically with the product groups. Product keys for KMS activations are associated with a product group and can activate the editions within that specific product group, as well as other editions below in the product hierarchy.

The product groups for Windows 7 and Windows Server 2008 R2 are shown in Table 3.

Table 3. Product Groupings

| Volume License product key group | Windows Operating System Edition |
| --- | --- |
| Client VL | * Windows 7 Professional * Windows 7 Enterprise |
| Server Group A | * Windows Server 2008 R2 HPC Edition * Windows Web Server 2008 R2 |
| Server Group B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise |
| Server Group C | * Windows Server 2008 R2 Datacenter * Windows Server 2008 R2 for Itanium-Based Systems |

## Choosing the MAK product key group

Because MAK product keys are associated with a single group it can only activate OS editions that corresponds to that group, chose the MAK from a group that matches the Windows edition to be installed. For example, if you are installing Windows 7 Enterprise, install the Client VL MAK key in the image or directly on the target systems.

## Choosing the KMS Key

With KMS, product keys are associated with a product group and can activate the Windows editions within that specific product group as well as any editions below it in the product hierarchy. The first and least-inclusive group of the hierarchy is the Client Volume Licensing product group; Server Group C is the most inclusive group in the KMS hierarchy.

This hierarchy extends to Windows Vista and Windows Server 2008 Volume License editions and product key groupings. Separate KMS keys will be issued for each product key grouping, meaning that a customer will have access to a KMS key for Client VL for both Windows 7 and Windows Vista. The KMS key for the newer Windows products will also activate the previous generation, meaning that a customer can have a single KMS key to activate multiple editions and generations of Windows. Table 4 shows the correlation between the product groupings.

Table 4. Product Group Correlation

| Volume License product key group | Windows edition  (Windows 7 and Windows Server 2008 R2) | Windows edition  (Windows Vista and Windows Server 2008) |
| --- | --- | --- |
| Client VL | * Windows 7 Professional * Windows 7 Enterprise | * Windows Vista Business * Windows Vista Enterprise |
| Server Group A | * Windows Web Server 2008 R2 * Windows Server 2008 R2 HPC Edition * Windows HPC Server 2008 R2 | * Windows Web Server 2008 * Windows Compute Cluster Server 2008 |
| Server Group B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise | * Windows Server 2008 Standard * Windows Server 2008 Enterprise * Includes editions without  Hyper-V™ |
| Server Group C | * Windows Server 2008 R2 Datacenter * Windows Server 2008 R2 for Itanium-based Systems | * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems * Includes editions without  Hyper-V |

## Choosing the KMS Host

As previously mentioned in this guide, KMS can be hosted on a client or server operating system on a physical computer or a virtual machine. When choosing the KMS host system, consider the operating system editions that will be activated with KMS. A KMS that is hosted on Windows 7 can only activate client operating systems, but a KMS that is hosted on Windows Server 2008 R2 can activate both client and server computers. See Table 5 for an explanation of this hierarchy.

Table 5   KMS Hierarchy

| Product Key group | KMS can be hosted on (KMS key activates KMS host) | Windows product editions activated by this KMS host |
| --- | --- | --- |
| Client VL for Windows 7 | * Windows Vista * Windows 7 * KMS for Windows Server 2003 v1.2 | * Windows 7 Professional * Windows 7 Enterprise * Windows Vista Business * Windows Vista Enterprise |
| Server Group A for Windows Server 2008 R2 | * KMS for Windows Server 2003 v1.2 * Windows Web Server 2008 * Windows Web Server 2008 R2 * Windows HPC Server 2008 * Windows HPC Server 2008 R2 | Includes previous plus:   * Windows Web Server 2008 R2 * Windows Web Server 2008 * Windows HPC Server 2008 R2 * Windows HPC Server 2008 |
| Server Group B for Windows Server 2008 R2 | Includes previous plus:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise | Includes previous plus:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise |
| Server Group C | Includes previous plus:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems | Includes previous plus:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 for Itanium-Based Systems |

# Determine Monitoring and Reporting Needs

Organizations that use Volume Activation need to track product key usage and the license conditions of activated computers. Customers can view their KMS key information and the number of activations that remain on a MAK key on the Volume Licensing Service Center at <http://go.microsoft.com/fwlink/?LinkId=107544>.

Additionally, several tools are available to help Volume Licensing customers manage activations and product key usage. The following sections describe the available tools and how each tool helps Volume Licensing customers:

## Windows Management Instrumentation

Data gathered during activation is accessible by using WMI. In fact, several of the tools available use WMI to access Volume Activation data. See the [Volume Activation Technical Reference Guide](http://go.microsoft.com/fwlink/?LinkId=152550) for a list all of WMI methods, properties, registry keys, and event IDs for Volume Activation.

## System Center Configuration Manager

Customers can use Microsoft Systems Management Server (SMS) 2003 with SP3 or Microsoft System Center Configuration Manager 2007 to monitor the license conditions of their organization’s computers. For a detailed description of the available license conditions, see Appendix B: [Licensing Conditions](#_Appendix_B:_Licensing) later in this guide.

Systems Management Server with SP3 and System Center Configuration Manager use built-in Asset Intelligence reporting and WMI to generate detailed activation reports for computers that are running Windows 7 or Windows Server 2008 R2. This information can also serve as the starting point for an organization to track and report software asset management from a licensing perspective. Additionally, System Center Operations Manager 2007 can be used to monitor the health and heartbeat for the Key Management Service.

## Event Logs

The KMS service records every action in the application logs of KMS clients and hosts. A KMS client records activation requests, renewals, and responses in the KMS client’s local application log using Windows Security Licensing (SLC) event IDs 12288 and 12289. The KMS host logs a separate entry for each request it receives from a KMS client as SLC event ID 12290. These entries are saved to the Key Management Service log in the Applications and Services Logs folder. Each KMS host keeps an individual log of activations. There is no replication of logs between KMS hosts, although log forwarding can be used to replicate logs from multiple KMS hosts to a center location for monitoring. For more information about KMS events, see the [*Volume Activation Technical Reference Guide*](http://go.microsoft.com/fwlink/?LinkId=152550).

## KMS Management Pack

KMS event logs can be archived and reviewed manually. Or with Microsoft System Center Operations Manager 2007, IT pros can use the Windows Key Management Service Management Pack for System Center Operations Manager. The KMS Management Pack can monitor the health and heartbeat of the KMS service. To download this Management Pack and guidance, see the **System Center Pack Catalog** at <http://go.microsoft.com/fwlink/?LinkID=110332>.

## Volume Activation Management Tool

Organizations can use VAMT to manage KMS and MAK activations on their networks. Additionally, they can use it to monitor the number of MAK activations remaining. It reports on the license condition of all computers that are using Volume Activation, and it tracks the MAK activation count.

# Appendix A: Information Sent to Microsoft

Microsoft uses the information collected during activation to confirm that the copy of the software is licensed. The information is then aggregated for statistical analysis. Microsoft does not use the information to identify or contact the organization. For more information about the information that is captured during activation and the use of that data by Microsoft, see <http://go.microsoft.com/fwlink/?LinkID=52526>http://go.microsoft.com/fwlink/?LinkId=52526.

During MAK activation and KMS host activation, the following information is sent to Microsoft:

* Product key
* Operating system edition and the channel from which it was obtained
* Current date
* License and activation condition
* Hardware ID hash, which is a non-unique number that cannot be reverse-engineered
* Language settings
* IP address, which is used only for verifying the location of the request

# Appendix B: Licensing Conditions

The software licensing architecture governs the licensing condition of computers that are running Windows operating systems. This architecture has a policy engine built from a number of core Windows security technologies. It is designed to protect the code and the associated licensing condition from tampering or other malicious behavior.

The policy engine gets data from a set of cryptographically signed eXtensible rights Markup Language (XrML) license files. XrML is an industry-standard rights expression language that a number of Windows components use. License files define the rights and conditions of the installed edition of Windows. All licensing files and other data that the policy engine uses are digitally signed or encrypted by using keys that are chained to secure roots of trust with Microsoft.

Windows 7 and Windows Server 2008 R2 may be in one of four software licensing conditions: activated, grace, genuine, or notifications. The following sections describe these conditions, which reflect the status of the computer’s activation and genuine state, which dictates the user experience. Figure 6 illustrates these conditions.

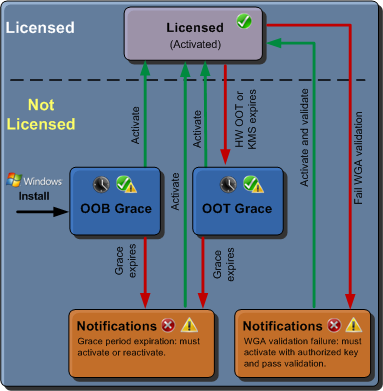


Figure 6   License states

## Activated

When a computer is activated, users can access the full functionality of the operating system. A combination of licensing files and a set of policies (rights) granted as a result of the activation process defines the functionality for a Windows edition. Individual Windows components call software licensing application programming interfaces (APIs) to determine which rights are granted and adjust their functionality according to the response.

## Grace

After installing a Windows 7 or Windows Server 2008 R2 operating system but before activating it, users can access the full functionality of the operating system for a limited time (the grace period). The length of a grace period is 30 days for either the client or server operating system. During this initial grace period, the operating system periodically notifies the user that the computer needs to be activated. Additionally, Windows can fall in to out-of-tolerance grace when the hardware changes significantly. The notifications are minimally intrusive and may not start at the beginning of the grace period, but they increase in frequency toward the end of the grace period.

## Genuine

The genuine state is not associated with the activation process. Instead, it is a condition determined by the online genuine validation service. When a user attempts to download or use a genuine-only feature, the online validation service checks the operating system of the requesting computer.

An operating system can have one of three genuine states:

* **Non-genuine**. The computer has obtained a ticket from the online validation service indicating that it is not genuine.
* **Local genuine**. The computer has not obtained a validation ticket.
* **Genuine**. The computer has a ticket that is signed by Microsoft from the online validation service indicating that it is genuine.

The genuine license condition applies only to client versions of the Windows operating system. Initially, during the grace period, a computer running these Windows versions is always in a local genuine condition. A computer is never marked non-genuine until after it fails validation through the online validation service and receives a non-genuine ticket. Likewise, after a computer has a non-genuine status, it must successfully validate itself through the online validation service to receive a genuine ticket.

Although it is necessary for a computer to be activated to be considered genuine, the process of activation does not reset or clear a previous non-genuine status. As a result, to return a computer to a fully functional activated condition, it must be both activated and validated against the online validation service. For more information, see **Genuine Microsoft Software** <http://go.microsoft.com/fwlink/?LinkId=151993> on the Microsoft Web site.

## Notifications

The purpose of the notifications-based experience is to differentiate between an activated (genuine) from an unlicensed (non-genuine) copy of Windows in a way that maintains computer functionality, such as logon, access to the familiar desktop, and so on. Reduced Functionality Mode (RFM) is not in Windows 7 or Windows Server 2008 R2. Instead, both operating systems have a notifications-based experience. This new notifications user experience means that computers that are not activated during their grace periods (initial activations and those that result from hardware changes) or that fail validation may provide the following user experience:

* After logging on to the computer, users see a dialog box reminding them that Windows must be activated along with options to activate now or later. If users do not interact with this dialog box within two minutes, the logon process continues normally.
* In the notifications state, Windows changes the desktop wallpaper to a solid black background, displays notifications in the notification area indicating the activation state, and displays dialog boxes showing actions that the user must take.
* In the notifications state, users have access to the full functionality of the installed version of Windows, with the following features disabled:
* A computer configured as a KMS host responds to KMS client requests with an error message that KMS has not been activated.
* Windows Update downloads security and critical updates (optional updates are excluded).
* Optional downloads requiring the online validation service—also referred to as genuine-gated downloads—are not available.

The computer must be activated for it to leave the notifications state.