**Volume Activation Deployment 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. This document is for information technology (IT) implementers who have planned a Volume Activation deployment and are now ready to review and perform the procedures needed for that deployment.

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.

Microsoft, Active Directory, Windows, Windows Server, and Windows Vista 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

[Contents 3](#_Toc230000254)

[Introduction 5](#_Toc230000255)

[KMS Activation 6](#_Toc230000256)

[Configuring DNS 6](#_Toc230000257)

[Change the Default DNS Permissions for SRV Records 7](#_Toc230000258)

[Publish to Multiple DNS Domains 7](#_Toc230000259)

[Manually Create SRV Records in DNS 8](#_Toc230000260)

[Manually Create SRV Records in a BIND 8.2 or higher DNS Server 9](#_Toc230000261)

[Disable Publishing of KMS SRV Records to DNS 9](#_Toc230000262)

[Installing KMS Hosts 10](#_Toc230000263)

[Configuring KMS 11](#_Toc230000264)

[Running Slmgr.vbs Remotely 12](#_Toc230000265)

[Configuring Windows Firewall for Remote Software License Manager Operations 12](#_Toc230000266)

[Remote Operations Targeting Workgroup Computers 13](#_Toc230000267)

[Configuring KMS Clients 13](#_Toc230000268)

[Manually Caching a KMS Host 14](#_Toc230000269)

[Disable Automatic Activation 14](#_Toc230000270)

[Enable Auto-discovery for a KMS Client 14](#_Toc230000271)

[Adding Suffixed Entries to KMS Clients 15](#_Toc230000272)

[Deploy KMS Clients 15](#_Toc230000273)

[Manually Activate a KMS Client 15](#_Toc230000274)

[Converting MAK Clients to KMS and KMS Clients to MAK 16](#_Toc230000275)

[Converting Retail Editions to Volume Activation 16](#_Toc230000276)

[MAK Activation 18](#_Toc230000277)

[Converting KMS Clients to MAK Activation 18](#_Toc230000278)

[Installing a MAK During Operating System Installation 18](#_Toc230000279)

[Installing a MAK After Operating System Installation 18](#_Toc230000280)

[Disabling Automatic Activation 19](#_Toc230000281)

[Activating MAK Clients 19](#_Toc230000282)

[Activating MAK Clients over the Internet 19](#_Toc230000283)

[Activating MAK Clients Through a Proxy Server 20](#_Toc230000284)

[Activating MAK Clients Using the Telephone 20](#_Toc230000285)

[Activating MAK Clients Using VAMT 21](#_Toc230000286)

[Integrating MAKs with Deployment Workbench 21](#_Toc230000287)

[Reactivating Computers 23](#_Toc230000288)

[Appendix A: Optional Configurations 24](#_Toc230000289)

[Enabling Standard User Activation 24](#_Toc230000290)

[Disabling Activation Notifications 24](#_Toc230000291)

[Registry Key Changes for Activation Features 24](#_Toc230000292)

[Appendix B: Sample Unattended Installation File 27](#_Toc230000293)

# Introduction

This guide describes Microsoft® Volume Activation deployment concepts. Volume Activation consists of two technologies—Key Management Service (KMS) and Multiple Activation Key (MAK)—that allow Volume Licensing customers to activate Volume License editions of the Windows® 7 and Windows Server® 2008 R2 operating systems. The Volume Licensing Service Center at <https://www.microsoft.com/licensing/servicecenter/> provides more information about Volume Licensing.

When planning to use Volume Activation, an organization must choose KMS, MAK, or any combination of the two. The activation methods chosen depend on the needs of the organization and the network infrastructure. For more information about planning a Volume Activation deployment, see the [Volume Activation Planning Guide.](http://go.microsoft.com/fwlink/?LinkId=155926)

**Note**   This document provides Volume Activation deployment guidance for the Windows 7 and Windows Server 2008 R2 operating systems. This guide does address interoperability between both generations of products, however. For more information about deploying Volume Activation for Windows Vista® and Windows Server 2008, see <http://go.microsoft.com/fwlink/?LinkID=75674>.

**Note**   This guide describes procedures that run scripts and make changes to the registry. These rights can be delegated to selected information technology (IT) implementers, and the rights to change product keys and perform activations can even be assigned to users, although Microsoft does not recommend this practice.

If activation fails, see the [Volume Activation Operations Guide](http://go.microsoft.com/fwlink/?LinkId=150084) for troubleshooting help. The guide includes an error code reference with steps for resolving common issues.

# KMS Activation

KMS activation works with minimal administrative intervention. If the network environment has Dynamic Domain Name System (DDNS) and allows computers to publish services automatically, deploying a KMS host can require very little effort. If the organization has more than one KMS host or the network does not support DDNS, additional configuration tasks may be necessary.

Warning   Some procedures in this section require changing the registry. Problems can occur if the registry is modified incorrectly by using Registry Editor or another method, and these problems might require reinstalling the operating system. Microsoft cannot guarantee that these problems can be resolved. IT pros modify the registry at their own risk.

The remainder of this section describes the following key tasks:

1. Configuring KMS hosts
2. Configuring DNS
3. Installing KMS hosts
4. Configuring KMS clients

## Configuring KMS Hosts

Software License Manager, sometimes referred to as SL Manager (Slmgr.vbs), is a script used to configure and retrieve Volume Activation information. The script can be run locally on the target computer or remotely from another computer, but it should be run from an elevated command prompt. If a standard user runs Slmgr.vbs, some license data may be missing or incorrect, and many operations are prohibited.

Slmgr.vbs can use Wscript.exe or Cscript.exe, and administrators can specify which script engine to use. If no script engine is specified, Slmgr.vbs runs using the default script engine, wscript.exe.

**Note**KMS requires a firewall exception on the KMS host. If using the default TCP port, enable the KMS Traffic exception in Windows Firewall. If using a different firewall, open TCP port 1688. If using a non-default port, open the custom TCP port in the firewall.

The Software Licensing Service must be restarted for any changes to take effect. To restart the Software Licensing Service, use the Microsoft Management Console (MMC) Services snap-in or can run the following command at an elevated command prompt:

net stop sppsvc && net start sppsvc

Slmgr.vbs requires at least one parameter. If the script is run with no parameters, it displays help information. Table 1 lists Slmgr.vbs command-line options along with a description of each. Most of the parameters in Table 1 configure the KMS host. However, the parameters /sai and /sri are passed to KMS clients after they make contact with the host. The general syntax of Slmgr.vbs is as follows:

slmgr.vbs /parameter

Table 1   Slmgr.vbs Parameters

| Parameter | Description |
| --- | --- |
| /sprt PortNumber | Sets the TCP communications port on a KMS host. Replace PortNumber with the TCP port number to use. The default setting is **1688**. |
| /cdns | Disables automatic DNS publishing by a KMS host. |
| /sdns | Enables automatic DNS publishing by the KMS host. |
| /cpri | Lowers the priority of KMS host processes. |
| /spri | Sets the priority of KMS host processes to **Normal**. |
| /sai ActivationInterval | Changes how often a KMS client attempts to activate itself when it cannot find a KMS host. Replace ActivationInterval with a number of minutes. The default setting is **120**. |
| /sri RenewalInterval | Changes how often a KMS client attempts to renew its activation by contacting a KMS host. Replace RenewalInterval with a number of minutes. The default setting is **10080** (7 days). This setting overrides the local KMS client settings. |
| /dli | Retrieves the current KMS activation count from the KMS host. |

### Running Slmgr.vbs Remotely

To run Slmgr.vbs remotely, administrators must supply additional parameters. They must include the computer name of the target computer as well as a user name and password of a user account that has local administrator rights on the target computer. If run remotely without a specified user name and password, the script uses the credentials of the user running the script.

The following syntax shows the additional parameters needed to run Slmgr.vbs remotely:

slmgr.vbs TargetComputerName [username] [password] /parameter [options]

### Configuring Windows Firewall for Remote Software License Manager Operations

Slmgr.vbs uses Windows Management Instrumentation (WMI), so administrators must configure the Windows Firewall to allow WMI traffic:

* For a single subnet, allow the **Windows Management Instrumentation (WMI)** exception in Windows Firewall.
* To allow WMI traffic across multiple subnets, allow the connection for **Windows Management Instrumentation (ASync-In)**, **Windows Management Instrumentation (DCOM-In)**, and **Windows Management Instrumentation (WMI-In)**. Additionally, allow remote access in the scope. Configure these settings by using Windows Firewall with Advanced Security, which is the Administrative Tools folder.

Note   By default, Windows Firewall Exceptions in the Private and Public profiles only apply exceptions to traffic originating on the local subnet. To expand the exception so that it applies to multiple subnets, change the exception settings in Windows Firewall with Advanced Security or, if joined to an AD DS domain, choose the Domain Profile.

### Remote Operations Targeting Workgroup Computers

Administrators can allow Slmgr.vbs to run remotely against computers that belong to a workgroup. To do so, create the **DWORD** value **LocalAccountTokenFilterPolicy** in the registry subkey **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** on KMS clients. Set this value to **0x01**.

## Configuring DNS

The following sections describe concepts for configuring DNS to work with Volume Activation:

* If more than one KMS host is used, see the section “Change the Default DNS Permissions for SRV Records.”
* To enable KMS clients using different DNS servers to find KMS hosts, see the section “Publish to Multiple DNS Domains.”
* To manually add SRV resource records for KMS hosts, see the sections “Manually Create SRV Records in DNS,” “Manually Create SRV Records in a BIND 8.2 or Higher DNS Server,” and “Disable Publishing of KMS SRV Records to DNS.”

Note   DNS changes may not be reflected until all DNS servers have been replicated.

### Change the Default DNS Permissions for SRV Records

If you are using only one KMS host, you might not need to configure permissions in DNS. The default behavior is to allow a computer to create an SRV resource record and then update it. However, if you have more than one KMS host (the usual case), the other hosts will be unable to update the SRV resource record unless SRV default permissions are changed.

The following high-level procedure is an example from Microsoft’s own environment. It does not give detailed steps, which might be different from one organization to another, and it is not the only way to achieve the desired result:

1. Create a global security group in Active Directory® that will be used for your KMS hosts. An example is *Key Management Service Group*.
2. Add each of your KMS hosts to this group. They must all be joined to the same domain.
3. Once the first KMS host is created, it will create the original SRV record. If the first KMS host is unable to create the SRV resource record, it may be because your organization has changed the default permissions. In this case, manually create the SRV resource record as the section “Manually Create SRV Records in DNS” describes.
4. Set the permissions for the SRV group to allow updates by members of the global security group.

**Note** A domain administrator can delegate the ability to carry out the preceding steps to administrators in the organization. To do so, create a security group in Active Directory, give that group permission to change the SRV records, and then add the delegates.

### Publish to Multiple DNS Domains

By default, the KMS host is registered only in the DNS domain to which the host belongs. If the network environment has only one DNS domain, no further action is required.

If there is more than one DNS domain name, a list of DNS domains can be created for a KMS host to use when publishing its SRV RR. Setting this registry value suspends the KMS host’s default behavior of publishing only in the domain specified as the Primary DNS Suffix.

Optionally, add priority and weight parameters to the **DnsDomainPublishList** registry value for KMS. This feature enables an administrator to establish KMS host priority groupings and weighting within each group to define which KMS host to try first and balance traffic among multiple KMS hosts.

Note   DNS changes might not be reflected until all DNS servers have been replicated. Changes made too frequently (time < replication time) can leave older records if the change is performed on a server that has not been replicated.

To automatically publish KMS in multiple DNS domains, add each DNS domain suffix to whichever KMS should publish to the multi-string registry value **DnsDomainPublishList in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**. After changing the value, restart the Software Licensing Service to create the SRV RRs.

Note   This key has changed from the Windows Vista® location of **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.

After configuring a KMS host to publish to multiple domains, export the registry key, and then import it in to the registry on additional KMS hosts. To verify that this procedure was successful, check the Application event log on each KMS host. Event ID 12294 indicates that the KMS host successfully created the SRV RRs. Event ID 12293 indicates that the attempt to create the SRV RRs was unsuccessful. For a complete list of error codes, see the [Volume Activation Operations Guide](http://go.microsoft.com/fwlink/?LinkId=150084).

### Manually Create SRV Records in DNS

If the environment does not support DDNS, the SRV RRs must be manually created to publish the KMS host. Environments that do not support DDNS should disable publishing on all KMS hosts to prevent event logs from collecting failed DNS publishing events. To disable auto-publishing, use the Slmgr.vbs script with the **/cdns** command-line option. See the “Configuring KMS” section for more information about the Slmgr.vbs script.

Note   Manually created SRV RRs can coexist with SRV RRs that KMS hosts automatically publish in other domains as long as all records are maintained to prevent conflicts.

Using DNS Manager, in the appropriate forwarding lookup zone, create a new SRV RR using the appropriate information for the location. By default, KMS listens on TCP port 1688, and the service is \_VLMCS. Table 2 contains example settings for a SRV RR.

Table 2   SRV Resource Record

| Name | Setting |
| --- | --- |
| Service | \_VLMCS |
| Protocol | \_TCP |
| Port number | 1688 |
| Host offering the service | FQDN of KMS Host |

### Manually Create SRV Records in a BIND 8.2 or higher DNS Server

If the organization uses a non-Microsoft DNS server, the needed SRV RRs can be created as long as the DNS server is compliant with Berkeley Internet Name Domain (BIND) 8.2 or higher. When creating the record, include the information shown in Table 3. The **Priority** and **Weight** settings shown in Table 3 are only used by Windows 7 and Windows Server 2008 R2.

Table 3   SRV RR Information

|  |  |
| --- | --- |
| Name | Setting |
| Name | \_vlmcs.\_tcp |
| Type | SRV |
| Priority | 0 |
| Weight | 0 |
| Port | 1688 |
| Hostname | FQDN of KMS Host |

To configure a BIND 8.2 or higher DNS server to support KMS auto-publishing, configure the BIND server to enable RR updates from KMS hosts. For example, add the following line to the zone definition in named.conf:

allow-update { any; };

Note   An allow-update statement can also be added in named.conf.options to allow DDNS for all zones hosted on this server.

### Disable Publishing of KMS SRV Records to DNS

KMS hosts automatically publish their existence by creating SRV RRs in DNS. To disable automatic DNS publishing by a KMS host, use the Slmgr.vbs script with the **/cdns** command-line option.

Using the Slmgr.vbs script to disable automatic DNS publishing is preferred, but you can also perform this task by creating a new **DWORD** value called **DisableDnsPublishing** in the registry, and set its value to **1**. This value is at **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** in the registry. To re-enable the default behavior for publishing of KMS SRV records to DNS, set the value to **0**.

## Installing KMS Hosts

To enable KMS functionality, a KMS key is installed on a KMS host; then, the host is activated over the Internet or by phone using Microsoft’s activation services. Computers running Windows 7 or Windows Server 2008 R2 can both serve as KMS hosts.

Windows Vista, Windows Server 2003, and Windows Server 2008 can also serve as KMS hosts. The KMS clients that a KMS host can activate are dependent on the host key used to activate the KMS host. For more information about KMS host keys, see the [*Volume Activation Planning Guide*](http://go.microsoft.com/fwlink/?LinkId=155926).

Install and activate a KMS key on a Windows 7 or Windows Server 2008 R2 computer by using an elevated command prompt:

* To install a KMS key, type **slmgr.vbs /ipk <KmsKey>** at a command prompt.
* To active online, type **slmgr.vbs /ato** at a command prompt.
* To activate by using the telephone, type **slui.exe 4** at a command prompt.

After activating the KMS key, restart the Software Protection Service.

Windows 7 and Windows Server 2008 R2 display the warning shown in Figure 1 any time administrators install a KMS host key by using the UI (Users will not see this warning if they install a KMS host key by using the Slmgr.vbs script). This message prevents accidentally installing a KMS key on computers that administrators do not intend to be KMS hosts.



Figure 1   The KMS key warning

To verify that the KMS host is configured correctly, check the KMS count to see whether it is increasing. In the Command Prompt window on the KMS host, type **slmgr.vbs /dli** to display the current KMS count. Administrators can also check the Key Management Service log in the Applications and Services Logs folder for event ID 12290. The Key Management Service log records activation requests from KMS clients. Each event displays the name of the computer and the time stamp of each activation request.

## Configuring KMS Clients

This section describes concepts for installing and configuring computers as KMS clients. By default, Volume License editions of Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 are KMS clients. If the computers the organization wants to activate by using KMS are using either of these operating systems and the network allows DNS auto-discovery, no further configuration is needed.

If a KMS client is configured to search for a KMS host using DNS but does not receive SRV records from DNS, Windows 7 and Windows Server 2008 R2 log the error in the event log.

### Manually Specifying a KMS Host

Administrators can manually assign a KMS host to KMS clients by using KMS host caching. Manually assigning a KMS host disables auto-discovery of KMS on the KMS client. A KMS host is manually assigned to a KMS client by running:

slmgr.vbs /skms <value>:<port>

where value is either the KMS\_FQDN, IPv4Address, or NetbiosName of the KMS host and port is TCP port on the KMS host.

### Enable Auto-discovery for a KMS Client

By default, KMS clients automatically attempt to discover KMS hosts. Auto-discovery can be disabled by manually assigning a KMS host to a KMS client. This action also clears the KMS host name from the KMS client’s cache. If auto-discovery is disabled, it can be re-enable by running **slmgr.vbs /ckms** at a command prompt.

### Adding Suffixed Entries to KMS Clients

By adding the address of a DNS server containing the SRV RR as a suffixed entry on KMS clients, administrators can advertise KMS hosts on one DNS server and allow KMS clients with other primary DNS servers to find it. For more information about configuring a domain suffix search list on KMS clients, see the Microsoft Help and Support article, “How to configure a domain suffix search list on the Domain Name System clients,” at <http://support.microsoft.com/kb/275553>.

### Deploy KMS Clients

The information in this section is for Volume Licensing customers using the Windows Automated Installation Kit (Windows AIK) to deploy and activate a Windows operating system. Prepare KMS clients for deployment by using the System Preparation Tool (Sysprep) or the Slmgr.vbs script:

* **Sysprep.** Before capturing an image, run Sysprep with the **/generalize** command-line option to reset the activation timer, security identifier (SID), and other important settings. Resetting the activation timer prevents the image’s grace period from expiring before the image is deployed. Running Sysprep.exe does not remove the installed product key, and administrators are not prompted for a new key during mini-setup. If no rearms are left, the Sysprep operation completes but the activation timers are not changed and an error is returned that explains the situation.
* **Slmgr.vbs.** When building demo virtual machines (VMs) for internal use (e.g., building VMs for the organization’s sales department or to set up a temporary training environment), running the Slmgr.vbs script with the **/rearm** command-line option extends the grace period another 30 days, which in turn resets the activation timer but makes no other changes to the computer. The activation timer can be reset three times for computers running Windows 7 or Windows Server 2008 R2.

### Manually Activate a KMS Client

By default, KMS clients automatically attempt to activate themselves at preset intervals. To manually activate KMS clients (for example, disconnected clients) before distributing them to users, use the Control Panel System item, or run **slmgr.vbs /ato** at an elevated command prompt. The Slmgr.vbs script reports activation success or failure and provides a result code. To perform activation, the KMS client must have access to a KMS host on the organization’s network.

### Converting MAK Clients to KMS and KMS Clients to MAK

By default, Windows 7 and Windows Server 2008 R2 operating systems use KMS for activation. To change existing KMS clients to MAK clients, simply install a MAK key. Similarly, to change MAK clients to KMS clients, run:

slmgr.vbs /ipk <KmsSetupKey>

where KmsSetupKey is one of the setup keys shown in Table 4. After installing the KMS setup key, activate the KMS client by running **cscript slmgr.vbs /ato**.

Table 4   KMS Client Setup Keys

| Operating System Edition | Product Key |
| --- | --- |
| Windows 7 | |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| Windows Server 2008 R2 | |
| Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Windows Server 2008 R2 for Itanium-Based Systems | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Windows Web Server 2008 R2 | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |

### Converting Retail Editions to Volume Activation

Retail editions of Windows 7 Professional and Windows Server 2008 R2 can be converted to KMS clients, provided that the organization has acquired the appropriate volume licenses and conforms to the Product Use Rights. To convert Windows 7 Professional and all editions of Windows Server 2008 R2 from retail to a KMS client, skip the **Product Key** page during operating system installation. When installation is complete, open an elevated Command Prompt window and type:

Slmgr.vbs /ipk <SetupKey>

where SetupKey is the KMS client setup key from Table 4 that corresponds to the edition of Windows 7 or Windows Server 2008 R2.

# MAK Activation

MAK activation is used for one-time activation through Microsoft’s hosted activation services, with no renewals required. For background information about MAK activation, see the [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926).

## Converting KMS Clients to MAK Activation

Windows 7 and Windows Server 2008 R2 install automatically as KMS clients. To convert a KMS client to MAK activation, install a MAK. A MAK can be installed during or any time after operating system installation.

A MAK key can be installed on a reference image of Windows 7 and Windows Server 2008 R2 to make all installations from that image use MAK activation instead of the default KMS activation. Doing so alleviates the need to specify a MAK in an unattended installation file.

### Installing a MAK During Operating System Installation

Administrators can convert a KMS client to a MAK client during the initial installation of Windows 7 or Windows Server 2008 R2 by including a MAK in an unattended setup (Unattend.xml) file. The Unattend.xml file can be used with Setup.exe or Windows Deployment Services. For more information, see the Unattended Windows Setup Reference help file in the Windows AIK at <http://go.microsoft.com/fwlink/?LinkId=136976>. For a sample unattended installation file, see “Appendix B: Sample Unattended Installation File.”

Note   The MAK is stored in clear text in the Unattend.xml file. During an unattended installation, the file Unattend.xml or AutoUnattend.xml is copied to the %SystemRoot%\Panther folder of the target computer. However, at the end of the Setup process, the Setup program replaces it with “SENSITIVE\*DATA\*DELETED.”

### Installing a MAK After Operating System Installation

A volume edition of Windows 7 and Windows Server 2008 R2 can be configured to use MAK activation by using the Control Panel System item or by running the Slmgr.vbs script:

* To install a MAK by using the System application, click the **Change your product key** link, and then type the MAK in the **Change your product key for activation** dialog box.
* To install a MAK by using Slmgr.vbs, run the following command at a command prompt:

slmgr.vbs /ipk <MultipleActivationKey>

where MultipleActivationKey is the MAK.

If users install a MAK by using the UI, the MAK client attempts to activate itself over the Internet one time. If the users install a MAK key by using the Slmgr.vbs script, the MAK client does not try to activate automatically.

### Disabling Automatic Activation

To disable automatic activation on any MAK client, set the **DWORD** registry value **Manual** to **1**. This value is in the registry subkey **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Activating MAK Clients

The MAK client attempts to activate over the Internet at the next scheduled interval. Administrators can force immediate activation over the Internet, by telephone, or by using the Volume Activation Management Tool (VAMT).

To confirm activation, check the system tray for a notification that says, “Windows is activated.” Alternatively, type **slmgr.vbs /dli** at a command prompt to view the activation status of a computer.

### Activating MAK Clients over the Internet

A MAK client can be activated over the Internet in either of two ways:

* Click the **Click here to activate Windows now link** in the Control Panel System item. Windows reports whether the activation was successful. If activation was unsuccessful, a wizard presents additional options.
* Run **slmgr.vbs /ato** at a command prompt. Additional options are not presented when using slmgr.vbs.

### Activating MAK Clients Through a Proxy Server

Activation over the Internet may be blocked if the proxy server requires user authentication. In Microsoft Internet Security and Acceleration (ISA) Server, this setting is called Basic Authentication. Because activation requests do not present the user's credentials to the proxy server, Microsoft recommends not using Basic Authentication with ISA Server or other proxy servers. However, if Basic Authentication or a comparable mechanism must be used on the proxy server, add the following URLs to the **Proxy Authentication exclusion** list:

http://go.microsoft.com/\*

https://sls.microsoft.com/\*

https://sls.microsoft.com:443

http://crl.microsoft.com/pki/crl/products/MicrosoftRootAuthority.crl

http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl

http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl

http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl

http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl

### Activating MAK Clients Using the Telephone

To activate computers that are connected to the organization’s network but do not have Internet connectivity by using Slmgr.vbs. In the Command Prompt window, type:

slmgr.vbs TargetComputerName <Username> <Password> /dti

to display the information required to complete telephone activation. To obtain the telephone number for an Activation Call Center in your local region, run **slui.exe 4**. Use the Interactive Voice Response system to obtain the confirmation ID (CID); then, run:

slmgr.vbs TargetComputerName <UserName> <Password> /atp <CID>

to install the CID. If activation is performed frequently or multiple computers are activated, it may be more useful to automate the process using the Slmgr.vbs script.

### Activating MAK Clients Using VAMT

VAMT allows automation of MAK deployment and activation over the network by distributing MAKs from a centralized console, as Figure 2 shows. VAMT queries Microsoft activation servers to get the number of remaining activations for a given MAK, then lists the activation status of all MAK-activated systems in the environment. This count is a snapshot in time, not a real-time count. VAMT version 1.2 is included in the Windows AIK, which is available from the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkId=136976>.



Figure 2   The VAMT user interface

### Disable Automatic Activation

Automatic activation can be disabled on any KMS client by setting the existing **DWORD** value **Manual** to **1**. This value is in the registry subkey **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Integrating MAKs with Deployment Workbench

Microsoft Deployment Toolkit (MDT) also provides a solution for deploying MAKs. In Deployment Workbench, administrators configure the MAK in task sequences, which add the MAK to the Unattend.xml file used during installation. Administrators can prepare the reference image for KMS activation, then, during deployment, MDT activates the installation by using a MAK as long as it does not detect a KMS infrastructure. MDT applies the MAK after installing the image. For more information about MDT, see **Deployment TechCenter** at <http://technet.microsoft.com/en-us/deployment/default.aspx>.

# Reactivating Computers

Periodically, Windows 7 and Windows Server 2008 R2 check the hardware configuration of the computer on which the operating system is installed. If the operating system detects that the hardware is substantially different, reactivation is required. The actual weighting factors and threshold values vary, because these values must keep pace with the constantly evolving computer hardware market. In general, computers that use MAK activation use the same reactivation rules as retail activation. KMS clients focus more on hard disk changes to determine the need for reactivation.

Client activations are valid for 180 days. This period 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. After a client’s activation is renewed, the activation validity interval begins again.

# Appendix A: Optional Configurations

Volume Activation supports optional configurations that may work in some environments but are not recommended for most. The procedures in this appendix require a Software Protection Service restart before they take effect.

## Enabling Standard User Activation

To enable standard user activation on a KMS client, add a new **DWORD** registry value named **UserOperations** and set its value to **1**. Create this value in the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** registry subkey.

When complete, administrative rights are no longer required for some operations, such as installing a product key (**slmgr.vbs /ipk**), installing a license (**slmgr.vbs /ilc**), or rearming (**slmgr.vbs /rearm**). This means that a standard user can switch a KMS client to MAK activation, manually activate a computer, and—if necessary—replace an existing MAK with a new MAK. Doing so is not recommended, however, because it lowers security on the computer.

Note   If a standard user installs a MAK or KMS key, the **ProductID** registry values are not updated. This behavior primarily affects product support, and Microsoft Customer Support Services (CSS) is aware of this situation.

## Disabling Activation Notifications

Although not recommended, software licensing notifications can be turned off by adding a new **DWORD** value named **NotificationDisabled** with a value of **1** to the registry. Create it in the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** registry subkey. This value disables all software licensing notifications, including balloons, wizards, and task dialog boxes.

## Registry Key Changes for Activation Features

Windows 7 and Windows Server 2008 R2 include a new Software Protection Platform (SPP) key in the registry. For product activation in managed environments, configure the **Activate Windows now** dialog box to display an optional **Learn About Activation Online** link, as shown in Figure 3.

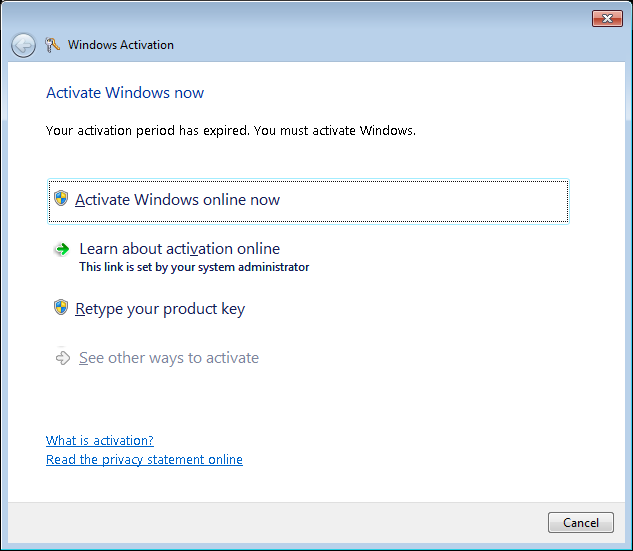


Figure 3   Learn about activation online

Clicking this custom link loads an administrator-defined URL in the user’s default browser. This URL can point to a custom Web page or other file stored on the local computer or on a network share. A Volume Licensing customer can use this link to provide customer-specific information about activation. Displaying the link requires setting the **REG\_SZ** value **ActivationAlternateURL** to the URL of the Web page to display when the user clicks it. The value **ActivationAlternateURL** is in the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** registry subkey.

# Appendix B: Sample Unattended Installation File

<?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>

<cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-com:cpi" />

</unattend>