

# KMS activation deployment for Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016

If your network environment supports the dynamic DNS update protocol and allows computers to automatically export services, deploying KMS hosts will probably require very little effort.

If the organization has more than one KMS host or the network does not support dynamic updates, additional configuration tasks may be needed.

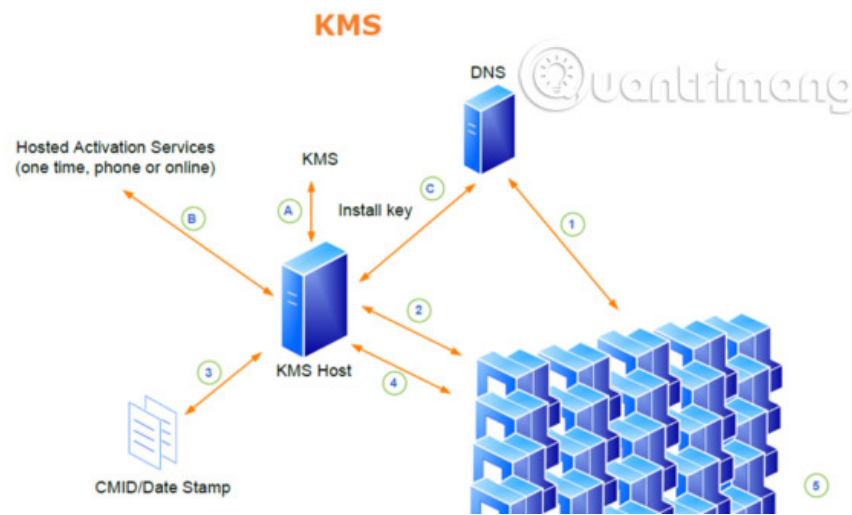
## KMS activation deployment for Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016

1. KMS activation deployment for Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016
2. Configure KMS host
  1. Run Slmgr.vbs remotely
  2. Configure Windows Firewall for remote operations of Software License Manager
  3. Remotely control the operation of the destination computers
3. Configure DNS
4. Change the default DNS permissions for SRV records
5. Export to multiple DNS domains
6. Manually create SRV records in DNS
  1. Manually create the SRV record in BIND DNS Server 8.2 or later
  2. Disable export of KMS SRV recording to DNS
7. Install KMS host
8. Configure KMS client
  1. Manually specify a KMS host
  2. Turn on Auto-discovery feature for KMS client
  3. Add suffix entry to KMS Client
  4. Deploy KMS client
  5. Manually activate KMS Client

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 to resolve these problems, you may be required to reinstall the operating system. Microsoft cannot guarantee that these problems can be resolved because the registry modification has potential risks.

The rest of this section describes the following main tasks:

1. Configure KMS host
2. Configure DNS
3. Install KMS host
4. Configure KMS client



## Configure KMS host

Software License Manager, sometimes called SL Manager (**Slmgr.vbs**), is a script used to configure and retrieve Volume Activation information. This script can be run locally on the destination computer or run remotely with another computer, but it will be run from a command prompt. If a basic 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**, so administrators can specify which script tools to use. If no scripting tool is specified, Slmgr.vbs will run with the default script tool, **wscript.exe**.

**Note** : KMS requires removal of the firewall on the KMS server. If using the default TCP port, activate KMS Traffic Exception in Windows Firewall. If using another firewall, open TCP port 1688. If you don't use the default port, open the custom TCP port in the firewall.

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

```
net stop sppsvc && net start sppsvc
```

Slmgr.vbs requires at least one parameter. If the script is run without parameters, the script will display help information. Table 1 lists the Slmgr.vbs command line options along with a description of each option. Most of the parameters in Table 1 will help configure the KMS host. However, the parameters **/ errors** and **/ sri** are passed to the KMS clients after they come into contact with the server. The general syntax of Slmgr.vbs is as follows:

```
slmgr.vbs / parameter
```

### Table 1 - Slmgr.vbs parameters

## Parameters

### Describe

#### / sprt PortNumber

Set TCP communication port on KMS host. Replace PortNumber with the TCP port number to use. The default setting is **1688**.

#### / cdns

Disable the DNS export feature automatically by KMS host.

#### / sdns

Allow automatic DNS export by KMS host.

#### / cpri

Reduce the priority of the KMS host process.

#### / spri

Set the priority of the KMS host process to Normal.

#### / wrong ActivationInterval

Change the frequency of KMS client activation when it is impossible to find the KMS host. Replace ActivationInterval with the number of minutes. The default setting is **120**.

#### / sri RenewalInterval

Change the frequency of the KMS client trying to renew the activation, by contacting the KMS host. Replace RenewalInterval with the number of minutes. The default setting is **10080** (7 days). This setting overrides the local KMS client settings.

#### / dli

Retrieve the current KMS activation number from KMS host.

## Run Slmgr.vbs remotely

To run Slmgr.vbs remotely, administrators must provide additional parameters. They must include the name of the destination computer, as well as the username and password of the local admin account on the destination computer. If running remotely without the specified username and password, the script will use the login information of the user running the script.

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

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

## Configure Windows Firewall for remote operations of Software License Manager

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

1. For a subnet, allow Windows Management Instrumentation (WMI) Exception in Windows Firewall.
2. To enable WMI traffic on multiple subnets, allow connection to Windows Management Instrumentation (ASync-In), Windows Management Instrumentation (DCOM-In) and Windows Management Instrumentation (WMI-In). Also, allow remote access within range. Configure these settings using Windows Firewall and Advanced Security, in the Administrative Tools folder.

**Note :** By default, **Windows Firewall Exceptions** in **Private and Public profiles** apply exceptions for only traffic originating on the local subnet. To extend the exception and apply it to multiple subnets, change the settings in Windows Firewall and Advanced Security or, if you have joined AD DS domain, select **Domain Profile**.

## Remotely control the operation of the destination computers

Administrators can allow Slmgr.vbs to run remotely with team computers. To do so, create a DWORD value:

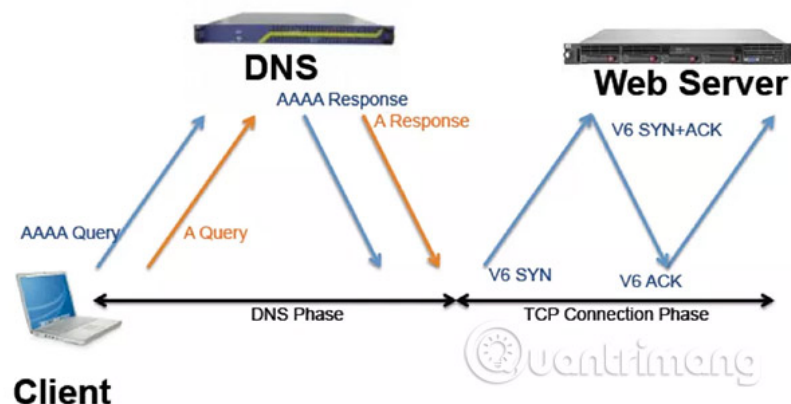
```
LocalAccountTokenFilterPolicy
```

in the registry subkey

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

on KMS client. Set this value to **0x01**.

## Configure DNS



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

If more than one KMS host is used, see the "**Changing the default DNS permissions for SRV records**" section.

To allow the KMS client to use different DNS servers to find KMS hosts, see the section ' **Exporting multiple DNS domains** '.

To manually add SRV resource records to KMS host, see the " **Manual creation of SRV records in DNS** " section, " **Manually create SRV records in BIND DNS Server 8.2 or later** " and " **Disable functions export KMS SRV record to DNS** ".

**Note** : DNS changes may not be reflected until all DNS servers have been copied.

## **Change the default DNS permissions for SRV records**

If you only use one KMS host, you may not need to configure permissions in DNS. The default behavior is to allow the computer to create SRV resource records and then update it. However, if you have more than one KMS host (normal case), other KMS hosts will not be able to update SRV resource records unless the default SRV permissions are changed.

The following advanced process is an example from the Microsoft environment. It does not provide detailed steps, which may differ slightly from different organizations, and it is not the only way to achieve the desired results.

Creating a global security group in **Active Directory**, will be used for your KMS hosts. The example is **Key Management Service Group** . Add your KMS hosts to this group. All of them must have the same domain.

When the first KMS host is created, it will create the original SRV record. If KMS first host cannot create SRV resource records, then your organization may have changed the default permissions. In this case, manually create the SRV resource record as in the section ' **Creating manual SRV records in DNS** '.

Set permissions for the SRV group to allow members of the global security group to update.

**Note** : Domain administrators can authorize the ability to perform the previous steps for an administrator in the organization. To do so, create a security group in **Active Directory**, allowing that group to change the SRV record and then add the members.

## **Export to multiple DNS domains**

By default, KMS host is only registered in the DNS domain containing the host. If the network environment has only one DNS domain, you do not need to take any further action.

If there is more than one DNS domain name, a list of DNS domains can be created for a KMS host to use, when exporting its SRV RR. Setting this registry value will halt the default behavior of the KMS host for exporting in the specified domain as the primary DNS suffix. You can add priority and weight parameters to the **DnsDomainPublishList** registry value for KMS. This feature allows administrators to set priority groups for KMS hosts and weights in each group to determine which KMS hosts first access and balance between multiple KMS hosts.

**Note** : DNS changes may not be reflected until all DNS servers are copied. Changes made too often can leave older records, if changes are made on a server that has not yet been copied.

To automatically export KMS in multiple DNS domains, adding each DNS domain suffix to any KMS will export the multi-string registry value:

```
DnsDomainPublishList in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
```

After changing the value, restart the Software Licensing Service to create the SRV RRs.

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

After configuring the KMS host to export to multiple domains, export the registry key and then import it into the registry on the 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 has successfully created SRV RRs. **Event ID 12293** indicates that the attempt to create SRV RR failed.

## Manually create SRV records in DNS

If the environment does not support dynamic updates, the SRV RRs must be manually created to export the KMS host. Environments that do not support dynamic updates should disable export on all KMS hosts to prevent failure to collect DNS export logs. To turn off automatic export, use the SImgr.vbs script with the command line option / **cdns**. See the ' **Configuring KMS** ' section for more information about the SImgr.vbs script.

**Note** : Manually created SRV RRs can coexist with the SRV RR that KMS hosts automatically export in other domains, as long as all records are maintained to prevent conflicts.

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

Name

Setting

Service

\_VLMCS

Protocol

\_TCP

Port number

1688

Host provides service

FQDN of KMS host

## Manually create the SRV record in BIND DNS Server 8.2 or later

If an organization uses DNS hosts other than Microsoft, the necessary SRV RRs can be created, provided that DNS hosts comply with the Berkeley Internet Name Domain (BIND) 8.2 or higher. When creating a record, include the information shown in Table 3. The priority and critical settings shown in Table 3 are only used by Windows 7 and Windows Server 2008 R2.

Name

Setting

Name

\_vlmcs.\_tcp

Species

SRV

Priority level

0

Critical level

0

Gate

1688

Host Name

FQDN of KMS host

To configure BIND DNS Server 8.2 or later, support KMS automatic export, configure BIND server to allow updating RR from KMS host. For example, add the following line to the zone definition in **named.conf**: **allow-update {any; };**;

**Note:** An update permission command can also be added in **named.conf** options , to enable dynamic updates for all regions stored on this server.

## Disable export of KMS SRV recording to DNS

KMS host automatically exported by creating SRV RR in DNS. To disable automatic DNS export by a KMS host, use the **Slmgr.vbs** script with the command line option / **cdns**.

Using the **Slmgr.vbs** script to turn off the DNS auto export feature takes precedence, but you can also do this by creating a new DWORD value named **DisableDnsPublishing** in the registry and setting its value. into **1** . This value is located in **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** in the registry. To re-enable the default behavior of exporting

KMS SRV to DNS, set the value to **0** .

## Install KMS host

To activate the KMS function, a KMS key is installed on a KMS host; After that, the host is activated via the Internet or by phone using Microsoft activation services. Windows 7 or Windows Server 2008 R2 computers can all function as KMS hosts. Windows Vista, Windows Server 2003, and Windows Server 2008 can also act as KMS hosts. The KMS clients that a KMS host can activate depend on the host key used to activate the KMS host.

Please install and activate KMS key on Windows 7 or Windows Server 2008 R2 computer using the command prompt:

1. To install KMS key, type **slmgr.vbs / ipk** at the command prompt.
2. To activate online, type **slmgr.vbs / ato** at the command prompt with admin rights.
3. To activate using the phone, type **slui.exe 4** at the command prompt.
4. After activating KMS key, restart the Software Protection Service.

Windows 7 and Windows Server 2008 R2 display alerts whenever an administrator installs KMS host key using the user interface (Users will not see this warning if they install KMS host key using use the Slmgr.vbs script). This message helps prevent unintentional installation of a KMS key on a computer that the administrator does not intend to use as a KMS host.

To verify that the KMS host is configured correctly, check the KMS number to see if it is increasing. In the Command Prompt window on KMS host, type **slmgr.vbs / dli** to display the current KMS number. The administrator 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 the activation request from the KMS client. Each event will show the computer's name and the timestamp of each activation request.

## Configure KMS client

This section describes the concepts for installing and configuring computers like KMS clients. By default, Volume License versions of Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2 are KMS clients. If the computers that the organization wants to activate using KMS are using one of these operating systems and the network allows automatic DNS detection, you won't need further configuration.

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

## Manually specify a KMS host

Administrators can manually assign a KMS host to the KMS clients using the KMS host cache. Manually assigning a KMS host will disable automatic KMS detection on the KMS client. A KMS host is manually assigned to a KMS client by running **: / skms name[:port] |="" :="" port="" [Activation ID]** in which **KMS\_FQDN**, **IPv4Address** or **NetbiosName** of host and port is TCP port on KMS host.

If KMS host only uses Internet Protocol version 6 (IPv6), the address must be specified in the format **[hostname]: port** (using square brackets). The IPv6 address contains a colon ( **:** ), which will be parsed

incorrectly by the Slmgr.vbs script.

## Turn on Auto-discovery feature for KMS client

By default, KMS clients automatically detect KMS hosts. The Auto-discovery feature can be turned off by manually assigning a KMS host to a KMS client. This action also deletes the KMS host name from the KMS client cache. If the Auto-discovery feature is disabled, it can be reactivated by running **slmgr.vbs / ckms** at the command prompt.

## Add suffix entry to KMS Client

By adding the address of the DNS server containing the RR SR as the suffix entry on the KMS client, the administrator can notify the KMS host on a DNS server and allow the KMS clients with the other primary DNS servers to find it.

## Deploy KMS client

The information in this section is for Volume Licensing customers to use the Windows Automated Installation Kit (Windows AIK) to deploy and activate a Windows operating system. Prepare the KMS clients to deploy using the System Preparation Tool (**Sysprep.exe**).

Before taking a picture, run Sysprep.exe with the command line option / **generalize** to reset the trigger timer, security identifier (SID) and other important settings. Resetting the activation timer will prevent the extension of the image from expiring before deploying the image. Running Sysprep.exe does not remove the installed software key and the administrator is not prompted to enter a new key during the mini setup process. If there is no / rearm, running Sysprep.exe will still complete but the activation timer does not change and the returned error will explain the situation further.

When building demo virtual machines for internal use (for example, building virtual machines for the organization's sales department or setting up a temporary training environment), run the Slmgr.vbs script with options. Select the command / **rearm** to extend the extension time for another 30 days, in turn reset the trigger timer but without any other changes to the computer. The trigger timer can be reset three times for computers running Windows 7 or Windows Server 2008 R2.

## Manually activate KMS Client

By default, KMS clients automatically try to activate themselves at predefined intervals. To manually activate the KMS clients (for example, the clients have disconnected) before distributing them to users, use the System Control System section, or run **slmgr.vbs / ato** at the command prompt with admin rights. Slmgr.vbs will report success or failure and provide the resulting code. To perform activation, the KMS client must have access to a KMS host on the organization's network.

>> See more: Deploying KMS activation (Part 2)

You finished reading the article "**KMS activation deployment for Windows 10, Windows 8.1, Windows Server 2012 R2, Windows Server 2016**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

