**Руководство по развертыванию
Volume Activation**

**ОС Windows 7 и Windows Server 2008 R2**

Корпорация Майкрософт (Microsoft Corp.)

Опубликовано: июнь 2009 г.

Аннотация

Служба Volume Activation позволяет пользователям корпоративного лицензирования автоматизировать и управлять процессом активации. Данный документ предназначен для ИТ-разработчиков, планировавших развертывание Volume Activation и готовых изучить, а затем выполнить процедуры, необходимые для данного развертывания.

Данный документ, как и любой другой документ, ссылки на который содержатся в этом документе, предоставляется исключительно в информационных целях, и корпорация Майкрософт не предоставляет никаких гарантий, явных или подразумеваемых, в данном документе. Содержащиеся в данном документе сведения, в том числе URL-адреса и другие ссылки на веб-сайты, могут быть изменены без предварительного уведомления. Полную ответственность за использование или результаты использования данного документа несет пользователь. Компании, организации, продукты, имена доменов, адреса электронной почты, эмблемы, люди, места и события, упоминающиеся в примерах, являются вымышленными (если не указано другое). Никаких ассоциаций с существующими компаниями, организациями, продуктами, именами доменов, адресами электронной почты, эмблемами, людьми, местами или событиями не подразумевается. Пользователь несет ответственность за соблюдение всех применимых законов об авторских правах. Согласно законам об авторских правах, никакие части данного документа не могут быть воспроизведены, сохранены или использованы в поисковых системах, переданы в любой форме или любыми способами (электронным, механическим, в виде фотокопий, записей или другими способами) или использованы в любых других целях без письменного разрешения корпорации Майкрософт.

Корпорации Майкрософт могут принадлежать патенты, заявки на патенты, товарные знаки, авторские права и другие права интеллектуальной собственности, имеющие отношение к данному документу. Предоставление данного документа не гарантирует прав на эти патенты, товарные знаки, авторские права и другую интеллектуальную собственность за исключением случаев, когда это явно указано в письменном лицензионном соглашении корпорации Майкрософт.

© Корпорация Майкрософт (Microsoft Corp.), 2009 г.

Microsoft, Active Directory, Windows, Windows Server и Windows Vista являются товарными знаками группы компаний Майкрософт.

Названия других продуктов или предприятий, указанные здесь, могут быть товарными знаками соответствующих владельцев.

Содержание

[Содержание 3](#_Toc234207062)

[Введение 5](#_Toc234207063)

[Активация KMS 6](#_Toc234207064)

[Настройка узлов KMS 6](#_Toc234207065)

[Удаленный запуск сценария Slmgr.vbs 8](#_Toc234207066)

[Настройка брандмауэра Windows для работы диспетчера удаленного лицензирования ПО 9](#_Toc234207067)

[Удаленная работа для конечных компьютеров рабочей группы 10](#_Toc234207068)

[Настройка DNS 10](#_Toc234207069)

[Измените разрешения DNS по умолчанию для записей SRV 11](#_Toc234207070)

[Публикация нескольких DNS-доменов 12](#_Toc234207071)

[Создание записей SRV в DNS вручную 13](#_Toc234207072)

[Создание записей SRV вручную на совместимом BIND 8.2 или на более позднем DNS-сервере. 14](#_Toc234207073)

[Отключение публикации записей SRV KMS на DNS 15](#_Toc234207074)

[Установка узлов KMS 16](#_Toc234207075)

[Настройка клиентов KMS 17](#_Toc234207076)

[Указание узла KMS вручную 18](#_Toc234207077)

[Включение автообнаружения для клиента KMS 19](#_Toc234207078)

[Добавление дополнительных записей к клиентам KMS 20](#_Toc234207079)

[Развертывание клиентов KMS 21](#_Toc234207080)

[Активация клиента KMS вручную 22](#_Toc234207081)

[Преобразование клиентов MAK в клиентов KMS и клиентов KMS в MAK 23](#_Toc234207082)

[Преобразование розничных версий в активацию корпоративного лицензирования Volume Activation 24](#_Toc234207083)

[Активация MAK 25](#_Toc234207084)

[Преобразование клиентов KMS в активацию MAK 25](#_Toc234207085)

[Установка MAK во время установки операционной системы 26](#_Toc234207086)

[Установка ключа MAK после установки операционной системы 27](#_Toc234207087)

[Отключение автоматической активации 28](#_Toc234207088)

[Активация клиентов MAK 28](#_Toc234207089)

[Активация клиентов MAK через Интернет 29](#_Toc234207090)

[Активация клиентов MAK через прокси-сервер 30](#_Toc234207091)

[Активация клиентов MAK по телефону 31](#_Toc234207092)

[Активация клиентов MAK с помощью VAMT 32](#_Toc234207093)

[Отключение автоматической активации 33](#_Toc234207094)

[Интеграция MAK со средством Deployment Workbench 33](#_Toc234207095)

[Повторная активация компьютеров 34](#_Toc234207096)

[Приложение 1. Дополнительные конфигурации 35](#_Toc234207097)

[Включение стандартной пользовательской активации 35](#_Toc234207098)

[Отключение уведомлений об активации 35](#_Toc234207099)

[Изменение ключа реестра для функций активации 36](#_Toc234207100)

[Приложение 2. Образец файла автоматической установки 38](#_Toc234207101)

# Введение

В данном руководстве описываются концепции развертывания
Microsoft® Volume Activation. Volume Activation состоит из двух технологий — службы управления ключами (KMS) и ключа многократной активации (MAK), которые позволяют пользователям Volume Licensing активировать выпуски
Volume License ОС Windows® 7 и Windows Server® 2008 R2. Volume Licensing Service Center по адресу <https://www.microsoft.com/licensing/servicecenter/> содержит дополнительные сведения о службе Volume Licensing.

При планировании использования Volume Activation организация должна выбрать KMS, MAK или сочетание двух этих способов. Выбранный способ активации зависит от потребностей организации и инфраструктуры сети. Дополнительные сведения о планировании развертывания Volume Activation см. в
документе [Руководство по планированию Volume Activation.](http://go.microsoft.com/fwlink/?LinkId=155926)

**Примечание.**В данном документе содержится руководство по развертыванию Volume Activation для операционных систем Windows 7 и Windows Server 2008 R2. Тем не менее, в данном руководстве рассматривается вопрос взаимодействия между двумя поколениями продуктов. Для получения дополнительных сведений о развертывании Volume Activation для Windows Vista® и
Windows Server 2008 см. <http://go.microsoft.com/fwlink/?LinkID=75674>.

**Примечание.**В данном руководстве описываются процедуры, с помощью которых запускаются сценарии и выполняются изменения в реестре. Данные права могут предоставляться избранным ИТ-разработчикам, а права изменять ключи продукта и выполнять активации могут быть предоставлены пользователям, хотя это не рекомендуется корпорацией Майкрософт.

При ошибке активации см. [Руководство по эксплуатации Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084) для получения инструкций по устранению неполадок. В этом руководстве содержится код ошибки, а также шаги по устранению наиболее распространенных неполадок.

# Активация KMS

Активация KMS выполняется с минимальными административными действиями. Если сетевая среда имеет динамический DDNS и разрешает компьютерам автоматически публиковать службы, для развертывания узла KMS могут потребоваться незначительные усилия. Если организация имеет несколько узлов KMS или сеть не поддерживает DDNS, может потребоваться выполнение дополнительных задач по настройке.

Предупреждение  Для выполнения некоторых процедур, приведенных в данном разделе, требуется изменение реестра. Неправильное изменение реестра с помощью редактора реестра или другим способом может привести к неполадкам, в результате которых может потребоваться переустановка операционной системы. Корпорация Майкрософт не может гарантировать решение данных проблем. Изменение реестра выполняется ИТ-специалистами под их ответственность.

В основной части данного раздела описываются следующие ключевые задачи.

1. Настройка узлов KMS
2. Настройка DNS
3. Установка узлов KMS
4. Настройка клиентов KMS

## Настройка узлов KMS

Software License Manager, иногда обозначаемый какSL Manager (Slmgr.vbs), является сценарием, который используется для настройки и получения сведений о Volume Activation. Данный сценарий может быть запущен локально на конечном компьютере или удаленно с другого компьютера, но он должен быть запущен из командной строки с повышенными правами. При запуске сценария Slmgr.vbs стандартным пользователем некоторые данные лицензии могут быть неверными или отсутствовать, а выполнение многих действий запрещено.

Slmgr.vbs может использовать Wscript.exe или Cscript.exe, а администраторы могут указать, какой обработчик сценариев необходимо использовать. Если обработчик сценариев не указан, Slmgr.vbs запускается с помощью обработчика сценариев по умолчанию wscript.exe.

**Примечание.**KMS требует исключения брандмауэра на узле KMS. Если используется порт TCP по умолчанию, включите исключение трафика KMS в брандмауэре Windows. При использовании другого брандмауэра откройте порт TCP 1688. При использовании порта, который не является портом по умолчанию, откройте пользовательский порт TCP в брандмауэре.

Служба лицензирования ПО должна быть перезапущена, чтобы изменения вступили в силу. Чтобы запустить Службу лицензирования ПО, используйте оснастку Службы на консоли управления (MMC) или запустите следующие команду из командной строки с повышенными правами:

net stop sppsvc && net start sppsvc

Для Slmgr.vbs необходим по меньшей мере один параметр. Если сценарий запускается без параметров, отобразится справочная информация. В таблице 1 приведены параметры командной строки Slmgr.vbs наряду с описанием каждого параметра. Большинство параметров в таблице 1 используются для настройки узла KMS. Тем не менее, параметры /sai и /sri передаются клиентам KMS после установления связи с узлом. Общий синтаксис Slmgr.vbs является следующим:

slmgr.vbs /parameter

Таблица 1  параметры Slmgr.vbs

| Параметр | Описание |
| --- | --- |
| /sprt PortNumber | Определяет порт коммуникаций TCP на узле KMS. Замените PortNumber номером используемого порта TCP. Параметр по умолчанию равен **1688**. |
| /cdns | Отключает автоматическую публикацию DNS узлом KMS. |
| /sdns | Включает автоматическую публикацию DNS узлом KMS. |
| /cpri | Снижает приоритет процессов узла KMS. |
| /spri | Устанавливает приоритет процессов узла KMS на уровень **Обычный**. |
| /sai ActivationInterval | Изменяет частоту попыток клиента KMS выполнить активацию при невозможности найти узел KMS. Замените ActivationInterval количеством минут. Параметр по умолчанию равен **120**. |
| /sri RenewalInterval | Изменяет частоту попыток клиента KMS обновить активацию путем установления связи с узлом KMS. Замените RenewalInterval количеством минут. Параметр по умолчанию равен **10080** (7 дней). Данный параметр переопределяет параметры локального клиента KMS. |
| /dli | Получает текущее значение счетчика активаций KMS с узла KMS. |

### Удаленный запуск сценария Slmgr.vbs

Чтобы выполнить удаленный запуск Slmgr.vbs, необходимо предоставить дополнительные параметры. Эти параметры должны включать в себя имя конечного компьютера, а также имя пользователя и пароль учетной записи пользователя, которые имеет права локального администратора на конечном компьютере. При удаленном запуске без указания имени пользователя и пароля сценарий отображает учетные данные пользователя, который выполняет сценарий.

В следующем синтаксисе показаны дополнительные параметры, которые требуются для удаленного запуска Slmgr.vbs:

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

### Настройка брандмауэра Windows для работы диспетчера удаленного лицензирования ПО

Сценарий Slmgr.vbs использует инструментарий управления Windows (WMI), следовательно, администраторы должны настроить брандмауэр Windows для разрешения трафика WMI.

* Для единой подсети разрешите разрешение **Инструментария управления Windows (WMI)** в брандмауэре Windows.
* Чтобы разрешить прохождение трафика WMI через несколько подсетей, разрешите соединение для **Инструментария управления Windows (ASync-In)**, **Инструментария управления Windows (DCOM-In)** и **Инструментария управления Windows (WMI-In)**. Дополнительно разрешите удаленный доступ в области. Настройте эти параметры с помощью брандмауэра Windows с расширенными параметрами безопасности, который находится в папке Администрирование.

Примечание  По умолчанию исключения брандмауэра Windows в общих и частных профилях применяют исключения только к трафику, создаваемому на локальной подсети по умолчанию. Чтобы расширить исключение для его применения к нескольким подсетям, измените параметры исключения в брандмауэре Windows с расширенными параметрами безопасности или, при подключении к домену AD DS, выберите профиль домена.

### Удаленная работа для конечных компьютеров рабочей группы

Администраторы могут разрешить Slmgr.vbs выполнять запуск удаленно по отношению к компьютерам, принадлежащим к рабочей группе. Для этого создайте значение **DWORD** **LocalAccountTokenFilterPolicy** в подключе реестра**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Policies\System** на клиентах KMS. Настройте это значение на **0x01**.

## Настройка DNS

В следующих разделах описываются основные понятия настройки DNS для работы с Volume Activation.

* При использовании нескольких узлов KMS см. раздел «Изменение разрешений DNS по умолчанию для записей SRV».
* Чтобы включить нахождение клиентами KMS узлов KMS с помощью различных DNS-серверов, см. раздел «Публикация на несколько DNS-доменов».
* Чтобы добавить вручную записи ресурсов SRV для узлов KMS, см. разделы «Создание записей SRV в DNS вручную», «Создание вручную записей SRV
в BIND 8.2 или более позднем DNS-сервере», а также «Отключение публикации записей SRV KMS в DNS».

Примечание.  Изменения DNS могут не отобразиться, пока все DNS-серверы не будут дублированы.

### Измените разрешения DNS по умолчанию для записей SRV

Если используется только один узел KMS, настройка разрешений в DNS может не требоваться. Поведением по умолчанию является разрешение компьютеру создать запись ресурса SRV, а затем обновить ее. Однако при наличии нескольких узлов KMS (наиболее распространенная ситуация) другие узлы не смогут обновить запись ресурса SRV, если не будут изменены разрешения SRV по умолчанию.

Приведенная ниже высокоуровеневая процедура — пример из собственной среды корпорации Майкрософт. Данная процедура не содержит подробно описанных действий, которые могут различаться в каждой организации, и не является единственным способом добиться результата.

1. Создайте глобальную группу безопасности в Active Directory®, которая будет использоваться узлами KMS. Примером может служить *Группа службы управления ключами*.
2. Добавьте каждый из узлов KMS в данную группу. Все эти узлы должны быть подключены к одному и тому же домену.
3. После того как будет создан первый узел KMS, он создаст изначальную запись SRV. Если первому узлу KMS не удается создать запись ресурса SRV, это может быть связано с изменением вашей организацией полномочий по умолчанию. В этом случае необходимо вручную создать запись ресурса SRV в соответствии с положениями раздела «Создание записей SRV в DNS вручную».
4. Настройте разрешения для группы SRV таким образом, чтобы разрешать обновления, выполненные членами глобальной группы безопасности.

**Примечание.**Администратор домена может передать полномочия на выполнение предыдущих шагов администраторам организации. Для этого создайте группу безопасности в Active Directory, предоставьте этой группе разрешение изменять записи SRV, а затем добавьте делегатов.

### Публикация нескольких DNS-доменов

По умолчанию узел KMS регистрируется только в DNS-домене, к которому узел относится. При наличии одного DNS-домена в сетевой среде выполнение дальнейших действий не требуется.

При наличии нескольких имен DNS-доменов необходимо создать список
DNS-доменов для узла KMS для использования при публикации записи ресурса SRV. Настройка данного значения реестра приостанавливает поведение по умолчанию узла KMS, который выполняет публикацию только в домене, указанном как Основной DNS-суффикс.

Дополнительно добавьте параметры приоритет и вес к значению реестра **DnsDomainPublishList** для KMS. Данная функция позволяет администратору устанавливать приоритетные группы узлов KMS и их вес в пределах каждой группы для определения узла KMS, который необходимо использовать первым, и уравновешивания трафика между несколькими узлами KMS.

Примечание.  Изменения DNS могут не отобразиться, пока все DNS-серверы не будут дублированы. При слишком частых изменениях (время < время дублирования) могут остаться более ранние записи, если изменения выполняются на сервере, который не был дублирован.

Каждый суффикс DNS-домена, на который должен выполнить публикацию KMS,
к многостроковому значению реестра **DnsDomainPublishList
в HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**. После изменения значения перезапустите службу лицензирования ПО для создания записи ресурса SRV.

Примечание.  Данный ключ изменил свое местоположение на Windows Vista® **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.

После настройки узла KMS для публикации на нескольких доменах выполните экспорт ключа реестра, а затем импортируйте его в реестр на дополнительных узлах KMS. Чтобы убедиться в успешном выполнении данной процедуры, проверьте журнал приложений на каждом узле KMS. Событие ID 12294 указывает, что узел KMS успешно создал записи ресурса SRV. Событие ID 12293 указывает, что попытка создать записи ресурса SRV была неуспешной. Полный список кодов ошибок см. в документе [Руководство по эксплуатации Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084).

### Создание записей SRV в DNS вручную

Если среда не поддерживает DDNS, записи ресурса SRV должны быть созданы вручную для публикации на узле KMS. Среды, которые не поддерживают DDNS, должны отключить публикацию на всех узлах KMS для предотвращения сбора журналами событий неуспешных событий публикации DNS. Чтобы отключить автопубликацию, используйте сценарий Slmgr.vbs с параметром командной строки **/cdns**. См. раздел «Настройка KMS» данного документа для получения дополнительных сведений о сценарии Slmgr.vbs.

Примечание.  Созданные вручную записи ресурса SRV могут сосуществовать с записями ресурса SRV, автоматически публикуемыми узлами KMS в других доменах, пока все записи сохраняются для предотвращения конфликтов.

С помощью диспетчера DNS в соответствующей зоне прямого просмотра создайте новую запись ресурса SRV с помощью соответствующих сведений для местоположения. По умолчанию KMS собирает данные на порте TCP 1688, а служба является \_VLMCS. В таблице 2 содержатся примеры параметров для записи ресурса SRV.

Таблица 2  Запись ресурса SRV

| Имя | Параметр |
| --- | --- |
| Служба | \_VLMCS |
| Протокол | \_TCP |
| Номер порта | 1688 |
| Узел, предоставляющий службу | FQDN узла KMS |

### Создание записей SRV вручную на совместимом BIND 8.2 или на более позднем DNS-сервере.

Если организация использует DNS-сервер, не изготовленный корпорацией Майкрософт, можно создавать необходимые записи ресурса SRV, пока DNS-сервер совместим с Berkeley Internet Name Domain (BIND) 8.2 или выше. При создании записи укажите сведения, приведенные в Таблице 3. Параметры **Приоритет** и**Вес**, приведенные в Таблице 3, используются только в Windows 7 и Windows Server 2008 R2.

Таблица 3  Запись ресурса SRV

|  |  |
| --- | --- |
| Имя | Параметр |
| Имя | \_vlmcs.\_tcp |
| Тип | SRV |
| Приоритет | 0 |
| Вес | 0 |
| Порт | 1688 |
| Имя узла | FQDN узла KMS |

Чтобы настроить BIND 8.2 или более позднюю версию DNS-сервера на поддержку автопубликации KMS, настройте сервер BIND на включение обновлений записи ресурса с узлов KMS. Например, добавьте следующую строку в определение зоны в named.conf:

allow-update { any; };

Примечание.  Отчет allow-update также может добавлен в named.conf.options для разрешения DDNS для всех зон, размещенных на данном сервере.

### Отключение публикации записей SRV KMS на DNS

Узлы KMS автоматически публикуют свое существование путем создания записей SRV в DNS. Чтобы отключить автопубликацию DNS узлом KMS, используйте сценарий Slmgr.vbs с параметром командной строки **/cdns**.

Предпочтительно использовать сценарий Slmgr.vbs для отключения автопубликации DNS, но также можно выполнить эту задачу путем создания нового значения **DWORD**, именуемого **DisableDnsPublishing** в реестре, и установки значения на **1**. Это значение находится в **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** в реестре. Чтобы повторно включить поведение по умолчанию для публикации записей SRV KMS на DNS, установите значение на **0**.

## Установка узлов KMS

Чтобы обеспечить функционирование службы KMS, ключ KMS устанавливается на узел KMS, затем узел активируется по телефону или с помощью служб активации корпорации Майкрософт. Компьютеры под управлением Windows 7 или Windows Server 2008 R2 могут выполнять роль узлов KMS.

Windows Vista, Windows Server 2003, и Windows Server 2008 также могут выполнять роль узлов KMS. Клиенты KMS, которые могут быть активированы узлом KMS, зависят от ключа узла, используемого для активации узла KMS. Дополнительные сведения о ключах узла KMS см. в документе *[Руководство по планированию Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926)*.

Установите и активируйте ключ KMS на компьютере под управлением Windows 7 или Windows Server 2008 R2 с помощью командной строки с повышенными правами.

* Чтобы установить ключ KMS, введите **slmgr.vbs /ipk <KmsKey>** в командной строке.
* Чтобы выполнить активацию в Интернете, введите **slmgr.vbs /ato** в командной строке.
* Чтобы выполнить активацию по телефону, введите **slui.exe 4** в командной строке.

После активации ключа KMS перезапустите службу защиты программного обеспечения.

В Windows 7 и Windows Server 2008 R2 отображается предупреждение, показанное на Рисунке 1, каждый раз, когда администраторы устанавливают ключ узла KMS с помощью пользовательского интерфейса (пользователи не увидят это предупреждение при установке ключа узла KMS с помощью сценария Slmgr.vbs). Данное сообщение предотвращает случайную установку ключа KMS на компьютеры, которые не предназначаются администраторами для выполнения роли узлов KMS.



Рисунок 1  Предупреждение ключа KMS

Чтобы проверить правильность настройки узла KMS, проверьте счетчик KMS на предмет возрастания значений. В окне командной строки на узле KMS введите **slmgr.vbs /dli** для отображения текущего счетчика KMS. Администраторы также могут проверить журнал службы управления ключами в папке «Приложения» и службы на предмет наличия события ID 12290. В журнале службы управления ключами регистрируются запросы активации, поступающие от клиентов KMS. В каждом событии отображается имя компьютера, а также отметка времени отдельного запроса на активацию.

## Настройка клиентов KMS

В данном разделе описаны основные понятия по установке и настройке
компьютеров в качестве клиентов KMS. По умолчанию выпуски корпоративных лицензий Windows Vista, Windows 7, Windows Server 2008 и Windows Server 2008 R2 являются клиентами KMS. Если компьютеры, которые организации необходимо активировать с помощью KMS, работают под управлением одной из этих операционных систем, а сеть позволяет автообнаружение DNS, дальнейшая настройка не требуется.

Если клиент KMS настроен на выполнение поиска узла KMS с помощью DNS, но не получает записи SRV от DNS, Windows 7 и Windows Server 2008 R2 зарегистрируют ошибку в журнале событий.

### Указание узла KMS вручную

Администраторы могут вручную назначить узел KMS клиентам KMS с помощью кэша узла KMS. Назначение узла KMS вручную отключает автообнаружение KMS на клиенте KMS. Узел KMS назначается вручную клиенту KMS путем запуска следующей команды:

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

где value является KMS\_FQDN, IPv4Address или NetbiosName узла KMS, а port — порт TCP на узле KMS.

### Включение автообнаружения для клиента KMS

По умолчанию клиенты KMS автоматически предпринимают попытки обнаружить узлы KMS. Отключить автообнаружение можно путем назначения узла KMS клиенту KMS вручную. При выполнении данного действия также удаляется имя узла KMS из кэша клиента KMS. Если функция автообнаружения отключена, она может быть повторно включена путем запуска **slmgr.vbs /ckms** в командной строке.

### Добавление дополнительных записей к клиентам KMS

Путем добавления адреса DNS-сервера, содержащего запись SRV, в качестве дополнительной записи на клиенты KMS, администраторы могут оповестить узлы KMS на одном DNS-сервере, чтобы позволить клиентам KMS с другими первичными DNS-серверами найти указанный DNS-сервер. Дополнительные сведения о настройке списка поиска суффикса домена на клиентах KMS см. в статье справки и поддержки Майкрософт «Настройка списка поиска суффикса домена
в клиентах службы доменных имен» по адресу <http://support.microsoft.com/kb/275553>.

### Развертывание клиентов KMS

Сведения, содержащиеся в данном разделе, предназначены для пользователей корпоративного лицензирования, развертывающих и активирующих операционную систему Windows с помощью пакета автоматической установки Windows. Подготовка клиентов KMS к развертыванию выполняется с помощью программы подготовки системы (Sysprep) или сценария Slmgr.vbs.

* **Sysprep.** Перед захватом образа запустите Sysprep с параметром командной строки **/generalize** чтобы сбросить таймер активации, идентификатор безопасности (SID) и другие важные параметры. Сброс таймера активации предотвращает истечение льготного периода образа до развертывания образа. При выполнении Sysprep.exe не происходит удаления установленного ключа продукта, и не отображается запрос на создание нового ключа во время мини-установки. Если возвращений к исходному состоянию активации не осталось, операция Sysprep завершается, но таймеры активации не меняются
и отображается ошибка с объяснением ситуации.
* **Slmgr.vbs.** При создании демонстрационных виртуальных компьютеров для внутреннего использования (например, создание виртуальных компьютеров для отделов продаж организации или для создания временной обучающей среды) запуск сценария Slmgr.vbs с помощью параметры командной строки **/rearm** продлевает льготный период на 30 дней, что в свою очередь сбрасывает таймер активации, но не вызывает никаких изменений на компьютере. Можно сбрасывать таймер активации три раза для компьютеров под управлением Windows 7 or Windows Server 2008 R2.

### Активация клиента KMS вручную

По умолчанию клиенты KMS автоматически предпринимают попытки выполнить активацию через предварительно заданные промежутки времени. Для активации клиентов KMS вручную (например, отключенных клиентов) до их распределения пользователям используйте элемент системы панели управления или запустите **slmgr.vbs /ato** в командной строке с повышенными правами. Сценарий Slmgr.vbs сообщает об ошибке или успешном выполнении активации с предоставлением кода результата. Для выполнения активации клиент KMS должен иметь доступ к узлу KMS в сети организации.

### Преобразование клиентов MAK в клиентов KMS и клиентов KMS в MAK

По умолчанию операционные системы Windows 7 и Windows Server 2008 R2 используют KMS для выполнения активации. Для преобразования существующих клиентов KMS в клиентов MAK достаточно установить ключ MAK. Аналогичным образом, для преобразования клиентов MAK в клиентов KMS запустите следующую команду:

slmgr.vbs /ipk <KmsSetupKey>

где KmsSetupKey — один из ключей установки, приведенных в Таблице 4.
После установки ключа установки KMS выполните активацию клиента KMS путем запуска **cscript slmgr.vbs /ato**.

Таблица 4  Ключи установки клиента KMS

| Выпуск операционной системы | Ключ продукта |
| --- | --- |
| Windows 7 |
| Windows 7 Профессиональная | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Профессиональная N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Корпоративная | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Корпоративная N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows 7 Корпоративная 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 для компьютеров на базе процессоров Itanium | 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 |

### Преобразование розничных версий в активацию корпоративноголицензирования Volume Activation

Можно преобразовать розничные версии Windows 7 Профессиональная
и Windows Server 2008 R2 в клиентов KMS при условии, что организация приобрела соответствующие корпоративные лицензии и имеет права использования продукта. Чтобы преобразовать Windows 7 Профессиональная и все выпуски Windows Server 2008 R2 из розничных версий в клиент KMS, пропустите страницу**Ключ продукта** во время установки операционной системы. Когда установка завершена, откройте окно командной строки с повышенными правами и введите следующие данные:

Slmgr.vbs /ipk <SetupKey>

где SetupKey — ключ установки клиента KMS, приведенный в Таблице 4,
который соответствует выпуску Windows 7 или Windows Server 2008 R2.

# Активация MAK

Активация MAK используется для однократной активации с помощью размещенных служб активации Майкрософт. Обновлений не требуется. Для получения базовых сведений об активации MAK см. [Руководство по планированию Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926).

## Преобразование клиентов KMS в активацию MAK

Windows 7 и Windows Server 2008 R2 устанавливаются автоматически в качестве клиентов KMS. Для преобразования клиента KMS в активацию MAK необходимо установить ключ MAK. Ключ MAK можно установить во время установки операционной системы или в любое время после ее установки.

Ключ MAK можно установить на эталонный образ Windows 7 и Windows Server 2008 R2, чтобы для всех установок с этого образа вместо активации KMS использовалась активация MAK. Это устраняет необходимость указывать ключ MAK в файле автоматической установки.

### Установка MAK во время установки операционной системы

Администраторы могут выполнять преобразование клиента KMS в клиента MAK во время первоначальной установки Windows 7 или Windows Server 2008 R2 путем включения ключа MAK в файл автоматической установки (Unattend.xml). Файл Unattend.xml можно использовать вместе с Setup.exe или службами развертывания Windows® (WDS). Дополнительные сведения см. в файле справки Справочник по автоматической установке Windows в Windows AIK по адресу: <http://go.microsoft.com/fwlink/?LinkId=136976>. Образец файла автоматической установки см. раздел «Образец файла автоматической установки» в Приложении 2.

Примечание.  Ключ MAK хранится в открытом тексте в файле Unattend.xml. Во время
автоматической установки файл Unattend.xml или AutoUnattend.xml копируется в папку
%SystemRoot%\Panther на конечном компьютере. Тем не менее, на заключительной стадии процесса установки программа установки заменяет его файлом «SENSITIVE\*DATA\*DELETED».

### Установка ключа MAK после установки операционной системы

В корпоративном выпуске ОС Windows 7 и Windows Server 2008 R2 активацию MAK можно настроить с помощью элемента Система панели управления, или запустив сценарий Slmgr.vbs.

* Чтобы установить ключ MAK с помощью системного приложения, щелкните ссылку **Изменить ключ продукта** и введите ключ MAK в диалоговом окне **Изменение ключа продукта для активации**.
* Чтобы установить ключ MAK с помощью сценария Slmgr.vbs, выполните следующую команду в командной строке:

slmgr.vbs /ipk <MultipleActivationKey>

где MultipleActivationKey — ключ MAK.

При установке ключа MAK с помощью пользовательского интерфейса клиент MAK попытается выполнить активацию через Интернет. При установке ключа MAK с помощью сценария Slmgr.vbs клиент MAK не будет пытаться выполнить автоматическую активацию.

### Отключение автоматической активации

Чтобы отключить автоматическую активацию клиента MAK, установите значение **Manual** для значения реестра **DWORD** на **1**. Это значение находится
в подразделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Активация клиентов MAK

Клиент MAK попытается выполнить активацию через Интернет во время следующего запланированного промежутка времени. Администраторы могут выполнять немедленную активацию через Интернет, по телефону или с помощью средства управления активацией корпоративных лицензий (VAMT).

После завершения активации на панели задач отобразится уведомление «Активация Windows выполнена». В противном случае введите **slmgr.vbs /dli** в командной строке, чтобы просмотреть состояние активации компьютера.

### Активация клиентов MAK через Интернет

Выполнить активацию клиента MAK через Интернет можно двумя способами.

* В элементе «Система» панели управления щелкните ссылку **Щелкните здесь, чтобы активировать Windows**. Система Windows уведомит, выполнена ли активация успешно. Если активацию не удалось выполнить, мастер предоставит дополнительные варианты действий.
* В командной строке выполните команду **slmgr.vbs /ato**. При использовании сценария slmgr.vbs дополнительные варианты действий будут недоступны.

### Активация клиентов MAK через прокси-сервер

Активация через Интернет может быть заблокирована, если прокси-сервер требует проверки подлинности пользователя. В системе Microsoft Internet Security and Acceleration Server (ISA-сервер) данный параметр называется Обычная проверка подлинности. Поскольку запросы на выполнение активации не предоставляют прокси-серверу учетные данные пользователя, корпорация Майкрософт не рекомендуется использовать обычную проверку подлинности с помощью ISA Server или других прокси-серверов. Тем не менее, если необходимо использовать обычную проверку подлинности или аналогичный механизм на прокси-сервере, добавьте следующие URL-адреса в список **Исключения
проверки подлинности прокси-сервера**:

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

### Активация клиентов MAK по телефону

Активировать компьютеры, подключенные к корпоративной сети, но не имеющие выхода в Интернет, можно с помощью сценария Slmgr.vbs. В окне командной строки введите:

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

чтобы отобразить сведения, необходимые для выполнения активации по телефону. Чтобы узнать номер телефона центра активации для вашего региона, введите **slui.exe 4**. С помощью интерактивной системы автоответчика получите идентификатор CID, а затем введите:

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

чтобы установить CID. При частом выполнении активации или активации нескольких компьютеров, представляется целесообразным автоматизировать данный процесс с помощью сценария Slmgr.vbs.

### Активация клиентов MAK с помощью VAMT

Средство VAMT позволяет автоматизировать развертывание и активацию MAK по сети путем распространения ключей MAK с централизованной консоли (как показано на рисунке 2). Средство VAMT отправляет запросы на серверы активации Майкрософт для получения количества оставшихся активаций для указанного ключа MAK, а затем отображает состояние активации всех систем
в среде, активированных с помощью ключа MAK. Данное количество — это моментальный снимок, сделанный в определенный момент времени, и не отображает данные в режиме реального времени. Средство VAMT версии 1.2 входит
в состав системы Windows AIK, которая доступна в центре загрузки Майкрософт по адресу: <http://go.microsoft.com/fwlink/?LinkId=136976>.



Рисунок 2. Пользовательский интерфейс VAMT

### Отключение автоматической активации

Чтобы отключить автоматическую активацию клиента KMS, установите значение **Manual** для значения реестра **DWORD** на **1**. Это значение находится
в подразделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Интеграция MAK со средством Deployment Workbench

Набор средств Microsoft Deployment Toolkit (MDT) также предоставляет решение для развертывания ключей MAK. В средстве Deployment Workbench администраторы могут настроить ключ MAK в последовательности задач, которая добавляет ключ MAK в файл Unattend.xml, используемый при установке. Администраторами подготавливается эталонный образ для активации KMS, а затем во время развертывания набор средств MDT запускает установку с помощью ключа MAK, поскольку не удается обнаружить инфраструктуру KMS. Ключ MAK применяется набором средств MDT после установки образа. Дополнительные сведения о наборе средств MDT см. на веб-сайте **Deployment TechCenter** по
адресу: <http://technet.microsoft.com/en-us/deployment/default.aspx>.

# Повторная активация компьютеров

ОС Windows 7 и Windows Server 2008 R2 периодически проверяют конфигурацию оборудования компьютера, на котором установлена операционная система. Если операционная система обнаружит, что оборудование значительно отличается, потребуется реактивация. Весовые коэффициенты и пороговые значения могут варьироваться, так как данные значения должны соответствовать постоянно меняющемуся рынку оборудования. Как правило, в компьютерах, активированных с помощью ключа MAK, используются те же правила повторной активации, что и при розничной активации. Клиенты KMS больше сосредоточиваются на изменениях жесткого диска, чтобы установить потребность реактивации.

Активации клиента действительны в течение 180 дней. Этот период называется сроком действия активации. Чтобы оставаться активированными, клиенты KMS должны обновлять активацию, выполняя подключение к узлу KMS как минимум каждые 180 дней. По умолчанию клиентские компьютеры KMS выполняют обновление активации каждые семь (7) дней, После обновления клиентской активации отсчет срока действия активации начнется заново.

# Приложение 1. Дополнительные конфигурации

Volume Activation поддерживает дополнительные конфигурации, которые могут работать в некоторых средах, но в основном не рекомендуются. Чтобы описываемые в данном приложении процедуры вступили в силу, необходимо перезапустить службу защиты программного обеспечения.

## Включение стандартной пользовательской активации

Чтобы включить стандартную пользовательскую активацию клиента MAK, добавьте новое значение реестра **DWORD** с именем **UserOperations** и установите для него значение **1**. Это значение создается в подразделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**.

После этого для выполнения некоторых операций, таких как установка ключа продукта (**slmgr.vbs /ipk**), установка лицензии (**slmgr.vbs /ilc**) или возвращение к исходному состоянию активации (**slmgr.vbs /rearm**) больше не требуются права администратора. Это означает, что стандартный пользователь может перейти с клиента KMS на активацию MAK, выполнить активацию компьютера вручную и, если необходимо, заменить существующий MAK новым MAK. Однако выполнение данной процедуры не рекомендуется, так как это снижает уровень безопасности компьютера.

Примечание.  При установке стандартным пользователем ключа MAK или KMS значения реестра **ProductID** не обновляются. Это воздействует в первую очередь на поддержку продукта. Службам поддержки Microsoft известно о данной ситуации.

## Отключение уведомлений об активации

Хотя данное действие не рекомендуется, отключить уведомления об активации можно, добавив новое значение реестра **DWORD** с именем **NotificationDisabled** и установив для него значение **1**. Это значение создается в подразделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**. Это значение отключает все уведомления о лицензировании, включая выноски, мастеры,
а также диалоговые окна задач.

## Изменение ключа реестра для функций активации

В реестре операционных систем Windows 7 и Windows Server 2008 R2 содержится новый ключ платформы защиты программного обеспечения (SPP). Для активации продукта в управляемых средах необходимо настроить диалоговое окно**Активация Windows**, чтобы в нем отображалась дополнительная ссылка **Дополнительные сведения об активации через Интернет**, как показано на рисунке 3.



Рис 3  Дополнительные сведения об активации через Интернет

При нажатии этой ссылки в веб-браузере по умолчанию загрузится настроенный администратором URL-адрес. Этот URL-адрес может быть связан с пользовательской веб-страницей или другим файлом, который хранится на локальном компьютере или в сетевой папке. Эта ссылка может использоваться пользователем корпоративного лицензирования для предоставления личных данных об активации. Для отображения ссылки необходимо установить значение
**ActivationAlternateURL** для **REG\_SZ** в URL-адресе отображаемой веб-страницы. Значение **ActivationAlternateURL** находится в подразделе реестра **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**.

# Приложение 2. Образец файла автоматической установки

<?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>