**批量激活部署指南**

**Windows 7 和 Windows Server 2008 R2**

Microsoft Corporation

发布日期：2009 年 6 月

摘要

批量激活可以帮助批量许可用户将激活过程自动化并加以管理。本文档是为已计划部署批量激活而且现在准备了解并执行该部署所需过程的信息技术 (IT) 执行人员编写的。

本文档以及其中引用的任何文档仅供参考，Microsoft 在本文档中未做任何明示或隐含的担保。本文档中的信息（包括 URL 和其他 Internet 网站参考）如有更改，恕不另行通知。使用本文档的全部风险或后果均由用户承担。除非另有说明，否则本文档举例所言公司、组织、产品、域名、电子邮件地址、徽标、人物、地点和事件均为虚构。Microsoft 无意将他们与任何真实的公司、组织、产品、域名、电子邮件地址、徽标、人物、地点或事件相关联，也不应推定为存在任何此类关联。使用者必须遵守所有适用的版权法律。在适用法律不限制版权权利的前提下，未经 Microsoft Corporation 明确书面许可，不得出于任何目的、以任何形式或借助任何手段（电子、机械、影印、录制或其他手段）对本文档任何部分进行复制、存储、引入检索系统或进行传播。

Microsoft 可能拥有本文档所涉及的专利权、专利申请权、商标权、版权或其他知识产权。除非 Microsoft 在任何书面许可协议中明确规定，否则提供本文档并不表示授予您上述专利权、商标权、版权或其他知识产权。

© 2009 Microsoft Corporation。

Microsoft、Active Directory、Windows、Windows Server 和 Windows Vista 是 Microsoft 集团公司的商标。

此处提及的实际公司和产品的名称可能是其各自所有者的商标。

目录

[目录 3](#_Toc107906784)

[简介 5](#_Toc107906785)

[KMS 激活 6](#_Toc107906786)

[配置 KMS 主机 6](#_Toc107906787)

[远程运行 Slmgr.vbs 8](#_Toc107906788)

[为远程软件许可证管理器操作配置 Windows 防火墙 9](#_Toc107906789)

[针对工作组计算机的远程操作 10](#_Toc107906790)

[配置 DNS 10](#_Toc107906791)

[针对 SRV 记录更改默认 DNS 权限 11](#_Toc107906792)

[发布到多个 DNS 域 12](#_Toc107906793)

[在 DNS 中手动创建 SRV 记录 13](#_Toc107906794)

[在 BIND 8.2 或更高版本的 DNS 服务器中手动创建 SRV 记录 14](#_Toc107906795)

[禁止将 KMS SRV 记录发布到 DNS 15](#_Toc107906796)

[安装 KMS 主机 16](#_Toc107906797)

[配置 KMS 客户端 17](#_Toc107906798)

[手动指定 KMS 主机 18](#_Toc107906799)

[启用 KMS 客户端的自动发现 19](#_Toc107906800)

[向 KMS 客户端添加带后缀的条目 20](#_Toc107906801)

[部署 KMS 客户端 21](#_Toc107906802)

[手动激活 KMS 客户端 22](#_Toc107906803)

[MAK 客户端与 KMS 客户端的相互转换 23](#_Toc107906804)

[将零售版本转换为批量激活版本 24](#_Toc107906805)

[MAK 激活 25](#_Toc107906806)

[将 KMS 客户端转换为使用 MAK 激活 25](#_Toc107906807)

[在安装操作系统过程中安装 MAK 26](#_Toc107906808)

[在安装操作系统之后安装 MAK 27](#_Toc107906809)

[禁用自动激活 28](#_Toc107906810)

[激活 MAK 客户端 28](#_Toc107906811)

[通过 Internet 激活 MAK 客户端 29](#_Toc107906812)

[通过代理服务器激活 MAK 客户端 30](#_Toc107906813)

[使用电话激活 MAK 客户端 31](#_Toc107906814)

[使用 VAMT 激活 MAK 客户端 32](#_Toc107906815)

[禁用自动激活 33](#_Toc107906816)

[将 MAK 与 Deployment Workbench 集成 33](#_Toc107906817)

[重新激活计算机 34](#_Toc107906818)

[附录 A：可选配置 35](#_Toc107906819)

[启用标准用户激活 35](#_Toc107906820)

[禁用激活通知 35](#_Toc107906821)

[激活功能的注册表项更改 35](#_Toc107906822)

[附录 B：无人参与安装文件示例 37](#_Toc107906823)

# 简介

本指南对 Microsoft® 批量激活部署概念进行了说明。批量激活包含两种技术（密钥管理服务 (KMS) 和多次激活密钥 (MAK)），允许批量许可用户激活 Windows® 7 和 Windows Server® 2008 R2 操作系统的批量许可版本。批量许可服务中心（网址为   
<https://www.microsoft.com/licensing/servicecenter/>）提供了有关批量许可的详细信息。

在计划使用批量激活时，组织必须选择 KMS、MAK 或两者的任意组合。选择哪种激活方法取决于组织的需求和网络基础结构。有关规划批量激活部署的详细信息，请参阅 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（批量激活规划指南）。

**注：**本文档提供针对 Windows 7 和 Windows Server 2008 R2 操作系统的批量激活部署指南。不过，本指南可解决两代产品之间的互操作性问题。有关针对 Windows Vista® 和 Windows Server 2008 部署批量激活的详细信息，请参阅 <http://go.microsoft.com/fwlink/?LinkID=75674>。

**注：**本指南介绍了运行脚本和修改注册表的过程。这些权限可以委派给选定的信息技术 (IT) 执行人员，而更改产品密钥和执行激活的权限甚至可以分配给用户，但 Microsoft 不推荐这样做。

如果激活失败，请参阅[批量激活操作指南](http://go.microsoft.com/fwlink/?LinkId=150084)，获取疑难解答方面的帮助。本指南包含错误代码参考，并提供常见问题的解决步骤。

# KMS 激活

KMS 激活需要的管理干预极少。如果网络环境包含动态域名系统 (DDNS) 并且允许计算机自动发布服务，则部署 KMS 主机是非常容易的事情。如果组织具有多台 KMS 主机，或者网络不支持 DDNS，则可能需要执行额外的配置任务。

警告：本节中的一些过程需要更改注册表。如果使用注册表编辑器或使用其他方法错误地修改了注册表，则可能会发生问题。一旦发生这些问题，则可能需要重新安装操作系统。Microsoft 不保证这些问题能够得以解决。IT 专业人员修改注册表需自行承担风险。

本节的剩余部分将描述下列关键任务：

1. 配置 KMS 主机
2. 配置 DNS
3. 安装 KMS 主机
4. 配置 KMS 客户端

## 配置 KMS 主机

软件许可证管理器，有时称为 SL 管理器 (Slmgr.vbs)，是一种用于配置和检索批量激活信息的脚本。此脚本可以在目标计算机本地运行，也可以从另一台计算机远程运行，但它应在升级的命令提示符下运行。如果标准用户运行 Slmgr.vbs，则某些许可证数据可能会缺失或不正确，许多操作也将被禁止。

Slmgr.vbs 可以使用 Wscript.exe 或 Cscript.exe，而管理员可以指定要使用哪个脚本引擎。如果没有指定脚本引擎，Slmgr.vbs 将使用默认脚本引擎 wscript.exe 运行。

**注：**KMS 要求在 KMS 主机上应用一项防火墙例外。如果使用的是默认 TCP 端口，请在 Windows 防火墙中启用 KMS 通信例外。如果使用的是其他防火墙，请打开 TCP 端口 1688。如果使用非默认端口，请在防火墙中打开自定义的 TCP 端口。

必须重新启动软件授权服务才能使更改生效。要重新启动软件授权服务，请使用 Microsoft 管理控制台 (MMC) 服务管理单元，也可以在升级的命令提示符下运行以下命令：

net stop sppsvc && net start sppsvc

Slmgr.vbs 至少需要一个参数。如果此脚本不带参数运行，则会显示此脚本的帮助信息。表 1 列出了 slmgr.vbs 的命令行选项，并提供了每个选项的说明。表 1 中的大多数参数都用于配置 KMS 主机。不过，当 KMS 客户端与主机联系之后，参数 /sai 和 /sri 将传递到这些客户端。Slmgr.vbs 的一般语法如下所示：

slmgr.vbs /parameter

表 1 Slmgr.vbs 参数

| 参数 | 说明 |
| --- | --- |
| /sprt PortNumber | 设置 KMS 主机上的 TCP 通信端口。用您要使用的 TCP 端口号替换 PortNumber。默认设置为 **1688**。 |
| /cdns | 禁用 KMS 主机的自动 DNS 发布。 |
| /sdns | 启用 KMS 主机的自动 DNS 发布。 |
| /cpri | 降低 KMS 主机进程的优先级。 |
| /spri | 将 KMS 主机进程的优先级设置为**标准**。 |
| /sai ActivationInterval | 更改 KMS 客户端在找不到 KMS 主机的情况下尝试自行激活的频率。用分钟数替换 ActivationInterval。默认设置为 **120**。 |
| /sri RenewalInterval | 更改 KMS 客户端尝试通过联系 KMS 主机续订其激活的频率。用分钟数替换 RenewalInterval。默认设置为 **10080**（7 天）。该设置将覆盖本地的 KMS 客户端设置。 |
| /dli | 从 KMS 主机检索当前 KMS 激活计数。 |

### 远程运行 Slmgr.vbs

要远程运行 Slmgr.vbs，管理员必须提供附加参数。其中必须包括目标计算机的计算机名，以及在目标计算机上拥有本地管理员权限的用户帐户的用户名和密码。如果在没有指定用户名和密码的情况下远程运行 Slmgr.vbs，则该脚本将使用运行该脚本的用户的凭据。

下面的语法显示远程运行 Slmgr.vbs 所需的附加参数：

slmgr.vbs TargetComputerName [用户名] [密码] /parameter [可选]

### 为远程软件许可证管理器操作配置 Windows 防火墙

Slmgr.vbs 使用 Windows Management Instrumentation (WMI)，因此管理员必须配置 Windows 防火墙，以允许 WMI 通信：

* 对于单一子网，在 Windows 防火墙中允许 **Windows Management Instrumentation (WMI)** 例外。
* 要允许跨多个子网进行 WMI 通信，应允许连接 **Windows Management**

**Instrumentation (ASync-In)**、**Windows Management Instrumentation (DCOM-In)** 和 **Windows Management Instrumentation (WMI-In)**。另外，还应允许在此范围内进行远程访问。配置这些设置时，请使用高级安全 Windows 防火墙，即“管理工具”文件夹。

注：默认情况下，专用和公用配置文件中的 Windows 防火墙例外仅应用于源自本地子网的通信。要扩展例外以将其应用到多个子网，请在高级安全 Windows 防火墙中更改例外设置；如果加入了 AD DS 域，请选择域配置文件。

### 针对工作组计算机的远程操作

管理员可以允许 Slmgr.vbs 针对属于某个工作组的计算机远程运行。为此，请在 KMS 客户端的注册表子项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\  
CurrentVersion\Policies\System** 中创建 **DWORD** 值 **LocalAccountTokenFilterPolicy**。  
请将该值设置为 **0x01**。

## 配置 DNS

以下各节介绍了配置 DNS 以用于批量激活的相关概念：

* 如果使用多台 KMS 主机，请参阅“针对 SRV 记录更改默认 DNS 权限”一节。
* 要允许 KMS 客户端使用不同的 DNS 服务器来查找 KMS 主机，请参阅“发布到多个 DNS 域”一节。
* 要为 KMS 主机手动添加 SRV 资源记录，请参阅以下各节：“在 DNS 中手动创建 SRV 记录”、“在 BIND 8.2 或更高版本的 DNS 服务器中手动创建 SRV 记录”和“禁止将 KMS SRV 记录发布到 DNS”。

注：在所有 DNS 服务器均复制完之前，DNS 更改可能不会反映出来。

### 针对 SRV 记录更改默认 DNS 权限

如果仅使用一台 KMS 主机，则可能无需在 DNS 中配置权限。默认行为是允许某台计算机创建一个 SRV 资源记录，然后对其进行更新。不过，如果使用多台 KMS 主机（通常情况），除非更改 SRV 默认权限，否则其他主机将无法更新 SRV 资源记录。

下面的概要过程是 Microsoft 自身环境中的一个示例。它未提供详细的步骤，因为不同组织所采取的具体步骤可能会有所不同，并且它不是实现预期结果的唯一途径：

1. 在 Active Directory® 中创建一个将用于 KMS 主机的全局安全组。例如，*Key Management Service Group*。
2. 将每台 KMS 主机添加到该组。所有主机均必须加入同一域中。
3. 一旦创建了第一台 KMS 主机，就会为其创建原始 SRV 记录。如果第一台 KMS 主机无法创建 SRV 资源记录，这可能是由于贵组织更改了默认权限。在这种情况下，请按照“在 DNS 中手动创建 SRV 记录”一节中所述，手动创建 SRV 资源记录。
4. 设置 SRV 组的权限，以允许全局安全组成员执行更新。

**注：**域管理员可以将执行上述步骤的权限委派给组织中的管理员。为此，请在 Active Directory 中创建一个安全组，将更改 SRV 记录的权限授予该组，然后在该组中添加代理人。

### 发布到多个 DNS 域

默认情况下，KMS 主机仅在其所属的 DNS 域中注册。如果网络环境中仅包含一个 DNS 域，则无需进一步操作。

如果存在多个 DNS 域名，则可以创建一个 DNS 域列表，供 KMS 主机发布其 SRV RR 时使用。设置此注册表值将只在指定为“主 DNS 后缀”的域中暂停 KMS 主机的默认发布行为。

将 priority 和 weight 参数添加到 KMS 的 **DnsDomainPublishList** 注册表值中（可选）。通过此功能，管理员可以在每个组中创建 KMS 主机优先级组和权重，以指定首先尝试连接哪台 KMS 主机，并平衡多台 KMS 主机之间的通信。

注：在所有 DNS 服务器均复制完之前，DNS 更改可能不会反映出来。如果在尚未复制的服务器上过于频繁地执行更改（时间 < 复制时间），则将保留较旧的记录。

要在多个 DNS 域中自动发布 KMS，请将 KMS 应发布到的每个 DNS 域的后缀添加到   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
SoftwareProtectionPlatform** 中的多字符串注册表值 **DnsDomainPublishList**。更改该值后，重新启动软件授权服务，以创建 SRV RR。

注：此项已从 Windows Vista® 中的 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL** 位置进行更改。

将 KMS 主机配置为发布到多个域之后，导出注册表项，然后将其导入到其他 KMS 主机的注册表中。要验证此过程是否成功，请检查每台 KMS 主机上的应用程序事件日志。事件 ID 12294 表明 KMS 主机已成功创建 SRV RR。事件 ID 12293 表明创建 SRV RR 的尝试失败。有关错误代码的完整列表，请参阅[批量激活操作指南](http://go.microsoft.com/fwlink/?LinkId=150084)。

### 在 DNS 中手动创建 SRV 记录

如果环境不支持 DDNS，则必须手动创建 SRV RR，以发布 KMS 主机。不支持 DDNS 的环境应禁止发布到所有 KMS 主机，以防事件日志收集失败的 DNS 发布事件。要禁用自动发布，请将 Slmgr.vbs 脚本与 **/cdns** 命令行选项一起使用。有关 Slmgr.vbs 脚本的详细信息，请参阅“配置 KMS”一节。

注：只要保持所有记录不互相冲突，手动创建的 SRV RR 就可以与其他域中 KMS 主机自动发布的 SRV RR 共存。

在适当的正向查找区域中，通过 DNS 管理器使用该位置的相应信息创建一个新的 SRV RR。默认情况下，KMS 侦听 TCP 端口 1688，服务为 \_VLMCS。表 2 列出了 SRV RR 的示例设置。

表 2 SRV 资源记录

| 名称 | 设置 |
| --- | --- |
| 服务 | \_VLMCS |
| 协议 | \_TCP |
| 端口号 | 1688 |
| 提供服务的主机 | KMS 主机的 FQDN |

### 在 BIND 8.2 或更高版本的 DNS 服务器中手动创建 SRV 记录

如果组织使用非 Microsoft DNS 服务器，那么，只要该 DNS 服务器符合 Berkeley Internet Name Domain (BIND) 8.2 或更高版本的规范，就可以创建所需的 SRV RR。创建记录时，请包含表 3 中显示的信息。表 3 中显示的**优先级**和**权重**设置仅用于 Windows 7 和 Windows Server 2008 R2。

表 3 SRV RR 信息

|  |  |
| --- | --- |
| 名称 | 设置 |
| 名称 | \_vlmcs.\_tcp |
| 类型 | SRV |
| 优先级 | 0 |
| 权重 | 0 |
| 端口 | 1688 |
| 主机名 | KMS 主机的 FQDN |

要将 BIND 8.2 或更高版本的 DNS 服务器配置为支持 KMS 自动发布，请将 BIND 服务器配置为允许来自 KMS 主机的 RR 更新。例如，将下面一行添加到 named.conf 中的区域定义中：

allow-update { any; };

注：也可以将 allow-update 语句添加到 named.conf.options 中，以允许此服务器上托管的所有区域使用 DDNS。

### 禁止将 KMS SRV 记录发布到 DNS

KMS 主机通过在 DNS 中创建 SRV RR 来自动发布其是否存在。要禁止 KMS 主机自动发布 DNS，请将 Slmgr.vbs 脚本与 **/cdns** 命令行选项一起使用。

首选操作是使用 Slmgr.vbs 脚本来禁用自动 DNS 发布，但您也可以通过以下方法来执行此  
任务：在注册表中创建一个名为 **DisableDnsPublishing** 的新 **DWORD** 值，然后将其值  
设置为 **1**。该值在注册表中的位置为 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows NT\CurrentVersion\SoftwareProtectionPlatform**。要重新启用将 KMS SRV 记录发布到 DNS 的默认行为，请将该值设置为 **0**。

## 安装 KMS 主机

要启用 KMS 功能，应将 KMS 密钥安装在某台 KMS 主机上，然后通过 Internet 或电话，使用 Microsoft 的激活服务激活主机。运行 Windows 7 或 Windows Server 2008 R2 的计算机都可以用作 KMS 主机。

运行 Windows Vista、Windows Server 2003 和 Windows Server 2008 的计算机也可以用作 KMS 主机。KMS 主机可以激活的 KMS 客户端取决于用于激活该 KMS 主机的主机密钥。有关 KMS 主机密钥的详细信息，请参阅 [*Volume Activation Planning Guide*](http://go.microsoft.com/fwlink/?LinkId=155926)（批量激活规划指南）。

通过使用升级的命令提示符，在 Windows 7 或 Windows Server 2008 R2 计算机上安装并激活 KMS 密钥：

* 要安装 KMS 密钥，请在命令提示符下键入 **slmgr.vbs /ipk <KMS 密钥>**。
* 要联机激活，请在命令提示符下键入 **slmgr.vbs /ato**。
* 要使用电话激活，请在命令提示符下键入 **slui.exe 4**。

激活 KMS 密钥后，请重新启动软件保护服务。

每当管理员使用 UI 安装 KMS 主机密钥时，Windows 7 和 Windows Server 2008 R2 都会显示如图 1 中所示的警告（如果使用 Slmgr.vbs 脚本安装 KMS 主机密钥，则用户将看不到此警告）。此消息可以防止无意间将 KMS 密钥安装在管理员不打算用作 KMS 主机的计算机上。

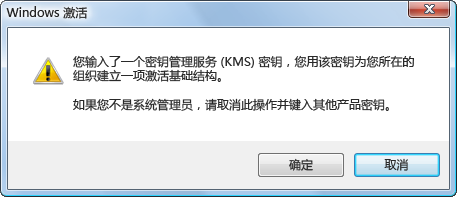


图 1 KMS 密钥警告

要验证 KMS 主机配置是否正确，请检查 KMS 计数，确定它是否增加了。在 KMS 主机的“命令提示符”窗口中，键入 **slmgr.vbs /dli** 可显示当前的 KMS 计数。管理员也可以检查“应用程序和服务日志”文件夹中的“密钥管理服务”日志，查看 ID 为 12290 的事件。“密钥管理服务”日志记录来自 KMS 客户端的激活请求。每个事件显示一个激活请求所源自的计算机的名称，以及该请求的时间戳。

## 配置 KMS 客户端

本节介绍安装和配置用作 KMS 客户端的计算机的相关概念。默认情况下，Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 的批量许可版本均可用作 KMS 客户端。如果组织要使用 KMS 激活的计算机运行的是上述操作系统之一，且网络允许 DNS 自动发现，则不需要进行进一步配置。

如果 KMS 客户端配置为使用 DNS 来搜索 KMS 主机，但未收到来自 DNS 的 SRV 记录，则 Windows 7 和 Windows Server 2008 R2 将在事件日志中记录该错误。

### 手动指定 KMS 主机

管理员可以使用 KMS 主机缓存将 KMS 主机手动分配给 KMS 客户端。手动分配 KMS 主机将禁用 KMS 客户端上的 KMS 自动发现。通过运行以下命令，可将 KMS 主机手动分配给 KMS 客户端：

slmgr.vbs /skms <值>:<端口>

其中，值 是 KMS 主机的 KMS\_FQDN、IPv4Address 或 NetbiosName，端口 是 KMS 主机上的 TCP 端口。

### 启用 KMS 客户端的自动发现

默认情况下，KMS 客户端会自动尝试搜索 KMS 主机。可以通过为 KMS 客户端手动分配 KMS 主机来禁用自动发现。此操作还会将 KMS 主机名从 KMS 客户端缓存中清除。如果禁用了自动发现，可以通过在命令提示符下运行 **slmgr.vbs /ckms** 来重新启用它。

### 向 KMS 客户端添加带后缀的条目

通过将包含 SRV RR 的 DNS 服务器的地址以带后缀条目的形式添加到 KMS 客户端上，管理员可以在一台 DNS 服务器中播发 KMS 主机，并允许使用其他主 DNS 服务器的 KMS 客户端查找该条目。有关在 KMS 客户端上配置域后缀搜索列表的详细信息，请参阅 Microsoft 帮助和支持文章“如何在域名系统客户端上配置域后缀搜索列表”，网址为   
<http://support.microsoft.com/kb/275553>。

### 部署 KMS 客户端

本节中的信息适用于使用 Windows 自动安装工具包 (Windows AIK) 部署和激活 Windows 操作系统的批量许可用户。使用系统准备工具 (Sysprep) 或下面的 Slmgr.vbs 脚本准备部署 KMS 客户端：

* **Sysprep。**在捕获映像之前，请将 Sysprep 与 **/generalize** 命令行选项一起运行，以重置激活计时器、安全标识符 (SID) 和其他重要设置。重置激活计时器可防止映像的宽限期在部署映像之前过期。运行 Sysprep.exe 不会删除已安装的产品密钥，在最小化安装期间不会提示管理员提供新密钥。如果未进行重置，则 Sysprep 操作能够完成，但激活计时器并未更改，而且将返回一个错误来说明此情况。
* **Slmgr.vbs。**在构建供内部使用的演示虚拟机 (VM)（如为组织的销售部门构建虚拟机或搭建临时培训环境）时，将 Slmgr.vbs 脚本与 **/rearm** 命令行选项一起运行可将宽限期再延长 30 天。此操作将重置激活计时器，但不会对计算机作其他更改。对于运行 Windows 7 或 Windows Server 2008 R2 的计算机，激活计时器可以重置三次。

### 手动激活 KMS 客户端

默认情况下，KMS 客户端会尝试以预设的间隔自行激活。要在向用户分发 KMS 客户端（如断开连接的客户端）之前手动激活这些客户端，请使用控制面板中的“系统”项，或在升级的命令提示符下运行 **slmgr.vbs /ato**。Slmgr.vbs 脚本将报告激活是否成功，并提供一个结果代码。要执行激活，KMS 客户端必须对组织网络中的 KMS 主机具有访问权限。

### MAK 客户端与 KMS 客户端的相互转换

默认情况下，Windows 7 和 Windows Server 2008 R2 操作系统使用 KMS 进行激活。要将现有的 KMS 客户端更改为 MAK 客户端，只需安装一个 MAK 密钥。同样，要将 MAK 客户端更改为 KMS 客户端，请运行：

slmgr.vbs /ipk <KMS 安装密钥>

其中，KMS 安装密钥 是表 4 中显示的安装密钥之一。安装完 KMS 安装密钥之后，可通过运行 **cscript slmgr.vbs /ato** 来激活 KMS 客户端。

表 4 KMS 客户端安装密钥

| 操作系统版本 | 产品密钥 |
| --- | --- |
| 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 |
| 用于基于 Itanium 的系统的 Windows Server 2008 R2 | 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 |

### 将零售版本转换为批量激活版本

可以将 Windows 7 Professional 和 Windows Server 2008 R2 的零售版本转换为 KMS 客户端，但前提是组织已获得相应的批量许可证且遵循“产品使用协议”。要将 Windows 7 Professional 和所有版本的 Windows Server 2008 R2 从零售版本转换为 KMS 客户端，请在操作系统安装的过程中跳过**产品密钥**页面。安装完成后，打开升级的“命令提示符”窗口并键入：

Slmgr.vbs /ipk <安装密钥>

其中，安装密钥 是表 4 中与 Windows 7 或 Windows Server 2008 R2 的版本相对应的 KMS 客户端安装密钥。

# MAK 激活

使用 MAK 激活，可以通过 Microsoft 托管的激活服务进行一次性激活，激活后无需续订。有关 MAK 激活的背景信息，请参阅 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（批量激活规划指南）。

## 将 KMS 客户端转换为使用 MAK 激活

Windows 7 和 Windows Server 2008 R2 自动安装为 KMS 客户端。要将 KMS 客户端转换为使用 MAK 激活，需要安装 MAK。您可以在安装操作系统期间或之后的任何时间安装 MAK。

可以将 MAK 密钥安装到 Windows 7 和 Windows Server 2008 R2 的参考映像中，以使所有从该映像进行的安装都使用 MAK 激活，而不使用默认的 KMS 激活。这样便可以减少在无人参与安装文件中指定 MAK 的需要。

### 在安装操作系统过程中安装 MAK

通过将 MAK 包含到无人参与安装文件 (Unattend.xml) 中，管理员可以在 Windows 7 或 Windows Server 2008 R2 的初始安装过程中，将 KMS 客户端转换为 MAK 客户端。Unattend.xml 文件可与 Setup.exe 或 Windows 部署服务一起使用。有关详细信息，请参阅 Windows AIK 中的帮助文件 Unattended Windows Setup Reference（无人参与 Windows 安装程序参考），网址为 <http://go.microsoft.com/fwlink/?LinkId=136976>。要查看无人参与安装文件的示例，请参阅“附录 B：无人参与安装文件示例”。

注：MAK 以明文格式存储在 Unattend.xml 文件中。在无人参与安装过程中，文件 Unattend.xml 或 AutoUnattend.xml 会复制到目标计算机的 %SystemRoot%\Panther 文件夹中。不过，在安装过程结束时，安装程序会将其替换为“SENSITIVE\*DATA\*DELETED”。

### 在安装操作系统之后安装 MAK

可以通过使用控制面板中的系统项或运行 Slmgr.vbs 脚本，将 Windows 7 和 Windows Server 2008 R2 的批量版本配置为使用 MAK 激活。

* 要使用“系统”应用程序安装 MAK，请单击**更改您的产品密钥**链接，然后在**更改您的产品密钥以便激活**对话框中键入 MAK。
* 要使用 Slmgr.vbs 安装 MAK，请在命令提示符下运行以下命令：

slmgr.vbs /ipk <多次激活密钥>

其中，多次激活密钥 为 MAK。

如果用户使用 UI 安装 MAK，则 MAK 客户端会尝试通过 Internet 一次性自行激活。如果用户使用 Slmgr.vbs 脚本安装 MAK 密钥，则 MAK 客户端不会尝试自动激活。

### 禁用自动激活

要在任意 MAK 客户端上禁用自动激活，请将 **DWORD** 注册表值 **Manual** 设置为 **1**。该值位于注册表子项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** 中。

## 激活 MAK 客户端

MAK 客户端会在下一个计划间隔尝试通过 Internet 激活。管理员可以通过 Internet、电话或使用批量激活管理工具 (VAMT) 强制进行立即激活。

要确认是否已激活，请检查系统任务栏中是否有通知显示“Windows 已激活”。或者，也可以在命令提示符下键入 **slmgr.vbs /dli**，以查看计算机的激活状态。

### 通过 Internet 激活 MAK 客户端

MAK 客户端可以通过 Internet 按下列任一方式激活：

* 单击控制面板上“系统”项中的**单击此处立即激活 Windows** 链接。Windows 会报告激活是否成功。如果激活失败，则会有一个向导列出一些其他选项。
* 在命令提示符下运行 **slmgr.vbs /ato**。使用 slmgr.vbs 时，不会显示其他选项。

### 通过代理服务器激活 MAK 客户端

如果代理服务器要求进行用户身份验证，则通过 Internet 的激活可能会受阻。在 Microsoft Internet Security and Acceleration (ISA) Server 中，此设置称为基本身份验证。由于激活请求不向代理服务器显示用户凭据，因此 Microsoft 建议您不要对 ISA 服务器或其他代理服务器使用基本身份验证。但如果必须在代理服务器上使用基本身份验证或类似机制，则请将以下 URL 添加到**代理身份验证排除**列表中：

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

### 使用电话激活 MAK 客户端

要激活已连接到组织网络的但不具有 Internet 连接的计算机，请使用 Slmgr.vbs，即在“命令提示符”窗口中，键入：

slmgr.vbs TargetComputerName <用户名> <密码> /dti

以显示完成电话激活所需的信息。要获取您所在地区的激活呼叫中心的电话号码，请运行 **slui.exe 4**。可以使用交互式语音响应系统获取确认 ID (CID)，然后运行：

slmgr.vbs TargetComputerName <用户名> <密码> /atp <CID>

以安装 CID。如果需要频繁执行激活或需要激活多台计算机，则使用 Slmgr.vbs 脚本自动执行激活过程可能会帮助更大。

### 使用 VAMT 激活 MAK 客户端

VAMT 通过从一个集中控制台分发 MAK 来实现 MAK 网络部署和激活的自动化，如图 2 所示。VAMT 会通过查询 Microsoft 激活服务器来获取给定 MAK 的剩余激活次数，然后列出环境中所有使用 MAK 激活的系统的激活状态。此计数是一个即时快照，不是实时计数。VAMT 版本 1.2 包含在 Windows AIK 中，您可以从 Microsoft 下载中心获取 Windows AIK，网址为   
<http://go.microsoft.com/fwlink/?LinkId=136976>。



图 2 VAMT 用户界面

### 禁用自动激活

任何 KMS 客户端上的自动激活均可禁用，方法是将现有的 **DWORD** 值 **Manual** 设置为 **1**。该值位于注册表子项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** 中。

## 将 MAK 与 Deployment Workbench 集成

Microsoft 部署工具包 (MDT) 还提供部署 MAK 的解决方案。在 Deployment Workbench 中，管理员可以在任务序列中配置 MAK，这些任务序列会将 MAK 添加到安装期间使用的 Unattend.xml 文件中。管理员可以准备好用于激活 KMS 的参考映像。这样，在部署期间，只要 MDT 检测不到 KMS 基础结构，它就会使用 MAK 来激活安装。MDT 会在安装映像之后应用 MAK。有关 MDT 的详细信息，请访问 **Deployment TechCenter**（部署技术中心），网址为 <http://technet.microsoft.com/en-us/deployment/default.aspx>。

# 重新激活计算机

Windows 7 和 Windows Server 2008 R2 操作系统会定期检查其所在计算机的硬件配置。如果操作系统检测到硬件有重大变化，则需要重新激活。实际权重系数和阈值会不断变化，因为这些值必须与不断发展变化的计算机硬件市场保持同步。一般而言，使用 MAK 激活的计算机与使用零售激活的计算机遵循相同的重新激活规则。KMS 客户端会更关注硬盘变化，以确定是否需要重新激活。

客户端激活有效期为 180 天。这段时间称为激活有效间隔。若要保持激活状态，KMS 客户端必须通过至少每 180 天连接一次 KMS 主机来续订激活。默认情况下，KMS 客户端计算机每 7 天进行一次激活续订尝试。在续订客户端激活之后，激活有效间隔重新开始。

# 附录 A：可选配置

批量激活支持的可选配置可在某些环境中使用，但对于大多数环境不推荐使用。本附录所述过程要求重新启动软件保护服务才能使配置生效。

## 启用标准用户激活

要在 KMS 客户端上启用标准用户激活，请添加一个名为 **UserOperations** 的新 **DWORD** 注册表值，并将其值设置为 **1**。请在注册表子项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows NT\CurrentVersion\SoftwareProtectionPlatform** 中创建该值。

完成后，某些操作（例如安装产品密钥 (**slmgr.vbs /ipk**)、安装许可证 (**slmgr.vbs /ilc**) 或重置 (**slmgr.vbs /rearm**) 将不再需要管理权限。这意味着标准用户可以将 KMS 客户端转换为使用 MAK 激活，手动激活计算机，并在必要时用新的 MAK 替换现有 MAK。然而，不推荐使用此过程，因为它会降低计算机的安全性。

注：如果标准用户安装 MAK 或 KMS 密钥，则 **ProductID** 注册表值不会进行更新。此行为主要会影响产品支持，Microsoft 客户支持服务部门 (CSS) 知道这种情况。

## 禁用激活通知

虽然不建议这样做，但可通过以下方法关闭软件授权通知：将一个名为 **NotificationDisabled** 的新 **DWORD** 值添加到注册表，并将其值设置为 **1**。请在注册表子项 **HKEY\_LOCAL\_MACHINE\  
SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\  
Activation** 中创建该值。此值会禁用所有软件授权通知，包括气球、向导和任务对话框。

## 激活功能的注册表项更改

Windows 7 和 Windows Server 2008 R2 在注册表中包含一个新的软件保护平台 (SPP) 项。要在托管环境中进行产品激活，请将**立即激活 Windows** 对话框配置为显示一个名为**了解联机激活**的可选链接，如图 3 中所示。

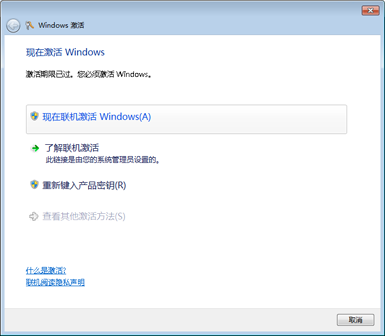


图 3 了解联机激活

单击这个自定义链接可在用户的默认浏览器中加载一个由管理员定义的 URL。此 URL 可以指向某个自定义网页，也可以指向存储在本地计算机或网络共享上的其他文件。批量许可用户可以使用此链接提供特定于用户的激活信息。要显示此链接，需要将 **REG\_SZ** 值 **ActivationAlternateURL** 设置为网页的 URL，以便在用户单击链接时显示此网页。值 **ActivationAlternateURL** 位于注册表子项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
SoftwareProtectionPlatform** 中。

# 附录 B：无人参与安装文件示例

<?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>