**大量啟用部署指南**

**Windows 7 與 Windows Server 2008 R2**

Microsoft Corporation

發佈日期：2009 年 6 月

摘要

大量啟用可以協助大量授權客戶將啟用程序自動化，並加以管理。此文件適用於之前已經完成大量啟用部署的規劃，現在已準備就緒來檢視並執行部署所需程序的資訊技術 (IT) 執行者。

此文件與其中任何參照文件僅供參考之用，Microsoft 不針對此文件進行明示或暗示保證。此文件的資訊（包含 URL 及其他網際網路網站的參考）如有變更，怒不另行通知。使用者必須擔負使用此文件或使用此文件後所導致任何結果的全部風險。除非另有特別說明，否則在此案例中描述的公司、組織、產品、網域名稱、電子郵件位址、標誌、人員、處所及事件皆為虛構。其中未影射任何真實的公司、組織、產品、網域名稱、電子郵件位址、標誌、人員、處所或事件。使用者必須負責遵守所有適用的著作權法。未經 Microsoft Corporation 明確的書面許可，不得針對任何目的或以任何方式或形式（電子、機械、影印、記錄或其他方式）將本文件任何部分予以重製、儲存或放入檢索系統或予以傳送，此規定未限制著作權許可之權利。

Microsoft 可能擁有本文件所提及內容中所含之專利權、專利申請權、商標、著作權或其他智慧財產權。除非 Microsoft 書面授權合約明確規定者外，提供本文件並未授予貴用戶上述專利權、商標、著作權或其他智慧財產權。

© 2009 Microsoft Corporation。

Microsoft、Active Directory、Windows、Windows Server 和 Windows Vista 為 Microsoft 公司集團的商標。

此文件提及的實際公司及產品的名稱為個別擁有者的商標。

內容

[內容 3](#_Toc234133410)

[簡介 5](#_Toc234133411)

[KMS 啟用 6](#_Toc234133412)

[設定 KMS 主機 6](#_Toc234133413)

[遠端執行 Slmgr.vbs 8](#_Toc234133414)

[為遠端軟體授權管理員作業設定 Windows 防火牆 9](#_Toc234133415)

[以工作群組電腦為目標的遠端作業 10](#_Toc234133416)

[設定 DNS 10](#_Toc234133417)

[變更 SRV 記錄的預設 DNS 權限 11](#_Toc234133418)

[發佈到多個 DNS 網域 12](#_Toc234133419)

[手動在 DNS 中建立 SRV 記錄 13](#_Toc234133420)

[手動在 BIND 8.2 或更高的 DNS 伺服器中建立 SRV 記錄 14](#_Toc234133421)

[停用將 KMS SRV 記錄發佈到 DNS 15](#_Toc234133422)

[安裝 KMS 主機 16](#_Toc234133423)

[設定 KMS 用戶端 17](#_Toc234133424)

[手動指定 KMS 主機 18](#_Toc234133425)

[啟用 KMS 用戶端的自動探索 19](#_Toc234133426)

[將尾碼項目新增到 KMS 用戶端 20](#_Toc234133427)

[部署 KMS 用戶端 21](#_Toc234133428)

[手動啟用 KMS 用戶端 22](#_Toc234133429)

[將 MAK 用戶端轉換為 KMS，將 KMS 用戶端轉換為 MAK 23](#_Toc234133430)

[將零售版本轉換為大量啟用 24](#_Toc234133431)

[MAK 啟用 25](#_Toc234133432)

[將 KMS 用戶端轉換為 MAK 啟用 25](#_Toc234133433)

[在安裝作業系統期間安裝 MAK 26](#_Toc234133434)

[在安裝作業系統後安裝 MAK 27](#_Toc234133435)

[停用自動啟用 28](#_Toc234133436)

[啟用 MAK 用戶端 28](#_Toc234133437)

[透過網際網路啟用 MAK 用戶端 29](#_Toc234133438)

[透過代理伺服器啟用 MAK 用戶端 30](#_Toc234133439)

[使用電話啟用 MAK 用戶端 31](#_Toc234133440)

[使用 VAMT 啟用 MAK 用戶端 32](#_Toc234133441)

[停用自動啟用 33](#_Toc234133442)

[整合 MAK 與 Deployment Workbench 33](#_Toc234133443)

[重新啟用電腦 34](#_Toc234133444)

[附錄 A：選用設定 35](#_Toc234133445)

[啟用標準使用者啟用 35](#_Toc234133446)

[停用啟用通知 35](#_Toc234133447)

[啟用功能的登錄金鑰變更 36](#_Toc234133448)

[附錄 B：自動安裝檔案範例 37](#_Toc234133449)

# 簡介

本指南描述 Microsoft® 大量啟用部署的概念。大量啟用包括兩種技術：金鑰管理服務 (KMS) 和多重啟用金鑰 (MAK)，這兩種技術可以讓大量授權客戶啟用 Windows® 7 和 Windows Server®2008 R2 作業系統的大量授權版本。大量授權服務中心
<https://www.microsoft.com/licensing/servicecenter/> 提供大量授權的詳細資訊。

如果貴組織規劃使用大量授權，則必須選擇 KMS、MAK 或者兩者的任意組合。啟用方法的選擇取決於組織與網路基礎結構的需求。如需規劃大量啟用部署的詳細資訊，請參閱 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（大量啟用規劃指南）。

**注：**此文件提供 Windows 7 與 Windows Server 2008 R2 作業系統的大量啟用部署指南。然而本指南亦說明兩世代產品之間的互通性。如需部署 Windows Vista® 與 Windows Server 2008 的大量啟用的詳細資訊，請參閱 <http://go.microsoft.com/fwlink/?LinkID=75674>。

**注：**本指南描述執行指令碼以及對登錄進行變更的程序。這些權利可以委派給選定的資訊技術 (IT) 執行者，而變更產品金鑰以及執行啟用的權利甚至可以指派給使用者，但 Microsoft 不建議此做法。

如果啟用失敗，請參閱[大量啟用操作指南](http://go.microsoft.com/fwlink/?LinkId=150084)獲取疑難排解說明。本指南包括錯誤代碼參照與解決常見問題的步驟。

# KMS 啟用

KMS 啟用只需少量的管理介入便可以執行。如果網路環境具有動態網域名稱系統 (DDNS)，並且允許電腦自動發佈服務，則部署 KMS 主機的任務相當輕鬆。如果組織有多部 KMS 主機或者網路不支援 DDNS，則可能需要其他設定工作。

警告   此節中的某些程序要求變更登錄。如果使用登錄編輯程式或其他方法錯誤地修改了登錄，可能會發生問題，並且這些問題可能需要重新安裝作業系統才能解決。Micorosft 無法保證這些問題是否能夠順利解決。IT 專業人員擔負修改登錄的可能風險。

此節的其餘部分描述下列重要工作：

1. 設定 KMS 主機
2. 設定 DNS
3. 安裝 KMS 主機
4. 設定 KMS 用戶端

## 設定 KMS 主機

軟體授權管理員（有時稱為 SL 管理員 ）(Slmgr.vbs) 是用於設定與擷取大量啟用資訊的指令碼。此指令碼可以在目標電腦本機執行或者從其他電腦遠端執行，但是其應該從升級的命令提示字元下執行。如果標準使用者執行 Slmgr.vbs，則部分授權資料可能遺失或者不正確，並且會禁止許多作業。

Slmgr.vbs 可以使用 Wscript.exe 或 Cscript.exe，管理員可以指定要使用的指令碼引擎。如果沒有指定指令碼引擎，Slmgr.vbs 會使用預設的指令碼引擎 wscript.exe 執行。

**注：**KMS 要求在 KMS 主機上套用一個防火牆例外狀況。如果使用預設的 TCP 連接埠，請在 Windows 防火牆中啟用 KMS 流量例外狀況。如果使用不同的防火牆，請開啟 TCP 連接埠 1688。如果使用非預設的連接埠，請開啟防火牆中的自訂 TCP 連接埠。

必須重新啟動軟體授權服務，任何變更才能生效。若要重新啟動軟體授權服務，請使用 Microsoft 管理主控台 (MMC) 服務嵌入式管理單元，或者在升級的命令提示字元下執行下列命令：

net stop sppsvc && net start sppsvc

Slmgr.vbs 要求最少有一個參數。如果此指令碼在沒有參數的情況下執行，則會顯示說明資訊。表 1 列出 Slmgr.vbs 命令列選項以及每個選項的描述。表 1 中的大多數參數都用於設定 KMS 主機。但是，在 KMS 用戶端與主機聯繫後，參數 /sai 與 /sri 會傳送到 KMS 用戶端。以下為 Slmgr.vbs 的一般語法：

slmgr.vbs /parameter

表 1   Slmgr.vbs 參數

| 參數 | 描述 |
| --- | --- |
| /sprt PortNumber | 設定 KMS 主機上的 TCP 通訊連接埠。以要使用的 TCP 連接埠號碼取代 PortNumber。預設設定為 **1688**。 |
| /cdns | 停用 KMS 主機的自動 DNS 發佈。 |
| /sdns | 啟用 KMS 主機的自動 DNS 發佈。 |
| /cpri | 降低 KMS 主機程序的優先順序。 |
| /spri | 將 KMS 主機程序的優先順序設定為 **Normal（一般）**。 |
| /sai ActivationInterval | 變更 KMS 用戶端在找不到 KMS 主機時嘗試自行啟用的頻率。以分鐘數取代 ActivationInterval。預設設定為 **120**。 |
| /sri RenewalInterval | 變更 KMS 用戶端嘗試透過聯繫 KMS 主機以更新其啟用的頻率。以分鐘數取代 RenewalInterval。預設設定為 **10080**（7 天）。此設定會覆寫本機 KMS 用戶端設定。 |
| /dli | 從 KMS 主機擷取目前的 KMS 啟用計數。 |

### 遠端執行 Slmgr.vbs

若要遠端執行 Slmgr.vbs，管理員必須提供其他參數。這些參數必須包括目標電腦的電腦名稱，以及對目標電腦具有本機管理員權限的使用者帳戶的使用者名稱與密碼。如果在沒有指定的使用者名稱與密碼的情況下遠端執行，則指令碼會使用執行此指令碼的使用者的認證。

以下語法顯示遠端執行 Slmgr.vbs 所需的其他參數：

slmgr.vbs TargetComputerName [使用者名稱] [密碼] /parameter [選用]

### 為遠端軟體授權管理員作業設定 Windows 防火牆

Slmgr.vbs 使用 Windows Management Instrumentation (WMI)，所以管理員必須將 Windows 防火牆設定為允許 WMI 流量：

* 對於單一子網路，請允許 Windows 防火牆中的 **Windows Management Instrumentation (WMI)** 例外狀況。
* 若要允許 WMI 流量通過多個子網路，請允許 **Windows Management Instrumentation (ASync-In)**、**Windows Management Instrumentation (DCOM-In)** 以及 **Windows Management Instrumentation (WMI-In)** 連線。此外，請允許此範圍內的遠端存取。透過使用具有進階安全性的 Windows 防火牆（即「系統管理工具」資料夾）設定這些設定。

注**：**依預設，私人設定檔與公用設定檔中的 Windows 防火牆例外狀況僅會將例外狀況套用至來自本機子網路的流量。若要擴展例外狀況以使其套用到多個子網路，請變更具有進階安全性的 Windows 防火牆中的例外狀況設定，或者如果已加入到 AD DS 網域，請選擇網域設定檔。

### 以工作群組電腦為目標的遠端作業

管理員可以允許 Slmgr.vbs 針對屬於某工作群組的電腦遠端執行。若要這麼做，請在 KMS 用戶端的登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Policies\System** 中建立 **DWORD** 值 **LocalAccountTokenFilterPolicy**。將此值設定為 **0x01**。

## 設定 DNS

以下各節描述設定 DNS 以用於大量啟用的概念：

* 如果使用多部 KMS 主機，請參閱「變更 SRV 記錄的預設 DNS 權限」一節。
* 若要讓使用不同 DNS 伺服器的 KMS 用戶端尋找 KMS 主機，請參閱「發佈到多個 DNS 網域」一節。
* 若要手動新增 KMS 主機的 SRV 資源記錄，請參閱以下各節：「手動在 DNS 中建立 SRV 記錄」、「手動在 BIND 8.2 或更高的 DNS 伺服器中建立 SRV 記錄」和「停用將 KMS SRV 記錄發佈到 DNS」。

注**：**直到所有 DNS 伺服器被複寫後，才能反映出 DNS 變更。

### 變更 SRV 記錄的預設 DNS 權限

如果您僅使用一部 KMS 主機，則無需設定 DNS 中的權限。預設行為是允許電腦建立 SRV 資源記錄，然後對其進行更新。但是，如果您有多部 KMS 主機（通常情況），則只有變更 SRV 預設權限，其他主機才能更新 SRV 資源記錄。

以下高階程序是來自 Microsoft 環境的範例。它沒有提供詳細的步驟（每個組織的步驟可能不同），而且也不是達到想要結果的唯一方法：

1. 在 Active Directory® 中建立用於您的 KMS 主機的全域安全性群組。範例是 *Key Management Service Group*。
2. 將您的每部 KMS 主機新增到此群組。它們必須加入到同一個網域。
3. 建立第一部 KMS 主機後，它將建立原始的 SRV 記錄。如果第一部 KMS 主機無法建立 SRV 資源記錄，則可能是因為貴組織變更了預設權限。在此情況下，按照「手動在 DNS 中建立 SRV 記錄」一節中的描述，手動建立 SRV 資源記錄。
4. 設定 SRV 群組的權限，以允許全域安全性群組的成員進行更新。

**注：**網域管理員可以將執行之前步驟的能力委派給組織中的管理員。若要這麼做，請在 Active Directory 中建立安全性群組，給予這個群組變更 SRV 記錄的權限，然後新增委派人。

### 發佈到多個 DNS 網域

依預設，KMS 主機僅在主機所屬的 DNS 網域中註冊。如果網路環境僅有一個 DNS 網域，無需執行任何後續動作。

如果有多個 DNS 網域名稱，可以為 KMS 主機建立其發佈 SRV RR 時所使用的 DNS 網域清單。設定此登錄值會暫停 KMS 主機的僅在指定為主要 DNS 尾碼的網域中發佈的預設行為。

可以選擇在 **DnsDomainPublishList** 登錄值中為 KMS 新增 *priority* 和 *weight* 參數。此功能可以讓管理員在每個群組中建立 KMS 主機優先順序群組和權數，以定義哪部 KMS 主機首先嘗試並平衡多部 KMS 主機間的流量。

注：直到所有 DNS 伺服器被複寫後，才能反映出 DNS 變更。如果在未被複寫的伺服器上執行變更，則變更頻率過高（時間少於複寫時間）會留下較舊的記錄。

若要自動將 KMS 發佈到多個 DNS 網域中，請將 KMS 應該發佈到的每個 DNS 網域尾碼
新增至**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
SoftwareProtectionPlatform 中的多字串登錄值 DnsDomainPublishList**。變更此值後，請重新啟動軟體授權服務，以建立 SRV RR。

注：此金鑰變更自 Windows Vista® 位置 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**。

將 KMS 主機設定為發佈到多個網域後，請匯出登錄金鑰，然後將其匯入到其他 KMS 主機上的登錄。若要驗證此程序是否成功，請檢查每部 KMS 主機上的應用程式事件記錄檔。事件識別碼 12294 指出 KMS 主機已成功建立 SRV RR。事件識別碼 12293 指出嘗試建立 SRV RR 失敗。如需錯誤代碼的完整清單，請參閱[大量啟用操作指南](http://go.microsoft.com/fwlink/?LinkId=150084)。

### 手動在 DNS 中建立 SRV 記錄

如果環境不支援 DDNS，則必須手動建立 SRV RR 以發佈 KMS 主機。不支援 DDNS 的環境應該停用所有 KMS 主機上的發佈，以防止事件記錄檔收集失敗的 DNS 發佈事件。若要停用自動發佈，請使用帶有 **/cdns** 命令列選項的 Slmgr.vbs 指令碼。請參閱「設定 KMS」一節取得 Slmgr.vbs 指令碼的詳細資訊。

注：只要維持所有記錄以防止發生衝突，則手動建立的 SRV RR 可與 KMS 主機自動在其他網域中發佈的 SRV RR 並存。

在適當的轉送查閱區域中，透過 DNS 管理員使用此位置的適當資訊新建 SRV RR。依預設，KMS 在 TCP 連接埠 1688 上接聽，並且服務是 \_VLMCS。表 2 包含 SRV RR 的範例設定。

表 2   SRV 資源記錄

| 名稱 | 設定 |
| --- | --- |
| 服務 | \_VLMCS |
| 通訊協定 | \_TCP |
| 連接埠號碼 | 1688 |
| 提供服務的主機 | KMS 主機的 FQDN |

### 手動在 BIND 8.2 或更高的 DNS 伺服器中建立 SRV 記錄

如果組織使用的是非 Microsoft DNS 伺服器，則只要 DNS 伺服器與 Berkeley Internet Name Domain (BIND) 8.2 或更高相容，便可以建立所需的 SRV RR。建立記錄時，請包括表 3 中顯示的資訊。表 3 中顯示的**優先順序**與**權數**設定僅可以由 Windows 7 與 Windows Server 2008 R2 使用。

表 3   SRV RR 資訊

|  |  |
| --- | --- |
| 名稱 | 設定 |
| 名稱 | \_vlmcs.\_tcp |
| 類型 | SRV |
| 優先順序 | 0 |
| 權數 | 0 |
| 連接埠 | 1688 |
| 主機名稱 | KMS 主機的 FQDN |

若要設定 BIND 8.2 或更高的 DNS 伺服器以支援 KMS 自動發佈，請將 BIND 伺服器設定為從 KMS 主機啟用 RR 更新。例如，將下面一行新增到 named.conf 中的區域定義：

allow-update { any; };

注：allow-update 陳述式也可以新增到 named.conf.options，以允許 DDNS 用於此伺服器上裝載的所有
區域。

### 停用將 KMS SRV 記錄發佈到 DNS

KMS 主機會透過在 DNS 中建立 SRV RR 來自動發佈其存在。若要停用 KMS 主機的自動 DNS 發佈，請使用帶有 **/cdns** 命令列選項的 Slmgr.vbs 指令碼。

使用 Slmgr.vbs 指令碼來停用自動 DNS 發佈是偏好的做法，但是您也可以透過在登錄中新建名為 **DisableDnsPublishing** 的 **DWORD** 值來執行此工作，並將其值設定為 **1**。此值位於登錄中的 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
SoftwareProtectionPlatform**。若要重新啟用將 KMS SRV 記錄發佈到 DNS 的預設行為，請將值設定為 **0**。

## 安裝 KMS 主機

若要啟用 KMS 功能，請將 KMS 金鑰安裝在 KMS 主機上，然後透過網際網路或電話使用 Microsoft 啟用服務啟用主機。執行 Windows 7 或 Windows Server 2008 R2 的電腦都可以作為 KMS 主機。

Windows Vista、Windows Server 2003 以及 Windows Server 2008 也可以作為 KMS 主機。KMS 主機可以啟用的 KMS 用戶端取決於用於啟用 KMS 主機的主機金鑰。如需 KMS 主機金鑰的詳細資訊，請參閱 *[Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)*（大量啟用規劃指南）。

透過使用升級的命令提示字元安裝並啟用 Windows 7 或 Windows Server 2008 R2 電腦上的 KMS 金鑰：

* 若要安裝 KMS 金鑰，請在命令提示字元下輸入 **slmgr.vbs /ipk <KMS 金鑰>**。
* 若要線上啟用，請在命令提示字元下輸入 **slmgr.vbs /ato**。
* 若要使用電話啟用，請在命令提示字元下輸入 **slui.exe 4**。

啟用 KMS 金鑰後，請重新啟動軟體保護服務。

任何時間管理員使用 UI 安裝 KMS 主機金鑰，Windows 7 與 Windows Server 2008 R2 都會顯示圖 1 中所示的警告（如果管理員使用 Slmgr.vbs 指令碼安裝 KMS 主機金鑰，使用者將無法看到此警告）。此訊息可以防止在管理員不想將其用作 KMS 主機的電腦上意外安裝 KMS 金鑰。



圖 1   KMS 金鑰警告

若要驗證是否正確設定 KMS 主機，請檢查 KMS 計數是否正在增加。在 KMS 主機上的「命令提示字元」視窗中，輸入 ****slmgr.vbs /dli**** 以顯示目前的 KMS 計數。管理員還可以檢查事件識別碼 12290 的「應用程式及服務記錄檔」資料夾中的「金鑰管理服務」記錄檔。「金鑰管理服務」記錄檔記錄來自 KMS 用戶端的啟用要求。每個事件都會顯示電腦名稱與每個啟用要求的時間戳記。

## 設定 KMS 用戶端

此節描述安裝電腦並將電腦設定為 KMS 用戶端的概念。依預設，Windows Vista、Windows 7、Windows Server 2008 以及 Windows Server 2008 R2 的大量授權版本是 KMS 用戶端。如果組織要使用 KMS 啟用的電腦使用的是這些作業系統中的一種，並且網路允許 DNS 自動探索，則無需後續設定。

如果 KMS 用戶端設定為使用 DNS 搜尋 KMS 主機，但是沒有從 DNS 收到 SRV 記錄，則 Windows 7 與 Windows Server 2008 R2 會在事件記錄檔中記錄該錯誤。

### 手動指定 KMS 主機

管理員可以透過使用 KMS 主機快取，手動將 KMS 主機指派給 KMS 用戶端。手動指派 KMS 主機會停用 KMS 用戶端上的 KMS 自動探索。透過執行下列命令將 KMS 主機手動指派給 KMS 用戶端：

slmgr.vbs /skms <值>:<連接埠>

其中，值 可以是 KMS 主機的 KMS\_FQDN、IPv4Address 或 NetbiosName，連接埠 是 KMS 主機上的 TCP 連接埠。

### 啟用 KMS 用戶端的自動探索

依預設，KMS 用戶端會自動嘗試探索 KMS 主機。可以透過將 KMS 主機手動指派給 KMS 用戶端來停用自動探索。此動作還可以從 KMS 用戶端的快取清除 KMS 主機名稱。如果已停用自動探索，則可以透過在命令提示字元下執行 **slmgr.vbs /ckms** 來重新啟用。

### 將尾碼項目新增到 KMS 用戶端

透過將包含 SRV RR 的 DNS 伺服器的地址作為尾碼項目新增到 KMS 用戶端，管理員可以在一部 DNS 伺服器上通告 KMS 主機，並允許使用其他主要 DNS 伺服器的 KMS 用戶端來尋找。如需在 KMS 用戶端上設定網域尾碼搜尋清單的詳細資訊，請參閱 Microsoft 說明及支援文章「如何設定網域名稱系統的用戶端的網域尾碼搜尋清單」，網址為

<http://support.microsoft.com/kb/275553>。

### 部署 KMS 用戶端

此節中的資訊適用於使用 Windows 自動安裝套件 (Windows AIK) 部署與啟用 Windows 作業系統的大量授權客戶。透過使用系統準備工具 (Sysprep) 或 Slmgr.vbs 指令碼準備要部署的 KMS 用戶端。

* **Sysprep。**在擷取影像之前，請使用 **/generalize** 命令列選項執行 Sysprep，以重設啟用計時器、安全性識別碼 (SID) 及其他重要設定。重設啟用計時器可以防止在部署影像之前影像的限定期限過期。執行 Sysprep.exe 不會移除已安裝的產品金鑰，並且不會在迷你安裝期間提示管理員輸入新金鑰。如果沒有剩餘的重複安裝，則 Sysprep 作業完成，但是啟用計時器不會變更，而且會傳回解釋此情況的錯誤。
* **Slmgr.vbs。**建立示範虛擬機器 (VM) 以供內部使用（例如，為組織的銷售部門建立 VM，或者設定暫時的訓練環境）時，執行帶有 **/rearm** 命令列選項的 Slmgr.vbs 指令碼可以將限定期限再延長 30 天，這樣會重設啟用計時器，但是不會對電腦進行任何其他變更。執行 Windows 7 或 Windows Server 2008 R2 電腦的啟用計時器可以重設三次。

### 手動啟用 KMS 用戶端

依預設，KMS 用戶端會在預設間隔自動嘗試自行啟用。若要在將 KMS 用戶端散佈給使用者之前手動啟用 KMS 用戶端（例如，未連接的用戶端），請使用「控制台」的「系統」項目，或在升級的命令提示字元下執行 **slmgr.vbs /ato**。Slmgr.vbs 指令碼會報告啟用成功還是失敗，並提供結果代碼。若要執行啟用，KMS 用戶端必須對組織網路上的 KMS 主機具有存取權限。

### 將 MAK 用戶端轉換為 KMS，將 KMS 用戶端轉換為 MAK

依預設，Windows 7 與 Windows Server 2008 R2 作業系統使用 KMS 進行啟用。若要將現有的 KMS 用戶端變更為 MAK 用戶端，只需安裝 MAK 金鑰。同樣地，若要將 MAK 用戶端變更為 KMS 用戶端，請執行：

slmgr.vbs /ipk <KMS 安裝金鑰>

其中，KMS 安裝金鑰 是表 4 中所示的其中一個安裝金鑰。安裝 KMS 安裝金鑰後，透過執行 **cscript slmgr.vbs /ato** 啟用 KMS 用戶端。

表 4   KMS 用戶端安裝金鑰

| 作業系統版本 | 產品金鑰 |
| --- | --- |
| 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 |
| Itanium 型系統適用的 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 |

### 將零售版本轉換為大量啟用

如果組織已取得適當的大量授權且符合「產品使用協議」，則 Windows 7 Professional 和 Windows Server 2008 R2 的零售版本也可以轉換為 KMS 用戶端。若要將 Windows 7 Professional 和所有版本的 Windows Server 2008 R2 從零售版本轉換成 KMS 用戶端，請在作業系統安裝期間跳過**產品金鑰**頁面。安裝完成時，開啟升級的「命令提示字元」視窗並輸入：

Slmgr.vbs /ipk <安裝金鑰>

其中，安裝金鑰 是來自表 4 的 KMS 用戶端安裝金鑰，與 Windows 7 或 Windows Server 2008 R2 版本相對應。

# MAK 啟用

MAK 啟用是透過 Microsoft 裝載的啟用服務進行的單次啟用，無須進行更新。如需 MAK 啟用的背景資訊，請參閱 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（大量啟用規劃指南）。

## 將 KMS 用戶端轉換為 MAK 啟用

Windows 7 和 Windows Server 2008 R2 會自動作為 KMS 用戶端進行安裝。若要將 KMS 用戶端轉換為 MAK 啟用，請安裝 MAK。MAK 可以在安裝作業系統期間安裝，也可以在以後的任何時間安裝。

可以將 MAK 金鑰安裝在 Windows 7 和 Windows Server 2008 R2 的參照映像上，以使從該映像進行的全部安裝使用 MAK 啟用（而非預設的 KMS 啟用）。這樣可以不必在自動安裝檔案中指定 MAK。

### 在安裝作業系統期間安裝 MAK

管理員可以在初始安裝 Windows 7 或 Windows Server 2008 R2 時，透過將 MAK 包含在
自動安裝 (Unattend.xml) 檔案中，將 KMS 用戶端轉換為 MAK 用戶端。Unattend.xml 檔案可與 Setup.exe 或 Windows 部署服務一起使用。如需詳細資訊，請參閱 Windows AIK 中
的說明檔 *Unattended Windows Setup Reference*（Windows 安裝程式自動安裝參考）(<http://go.microsoft.com/fwlink/?LinkId=136976>)。如需自動安裝檔案的範例，請參閱「附錄 B：自動安裝檔案範例」。

注：MAK 以純文字的形式儲存於 Unattend.xml 檔案中。在自動安裝期間，Unattend.xml 或 AutoUnattend.xml 檔案複製到目標電腦的 %SystemRoot%\Panther 資料夾下。但是，在安裝程序結束時，安裝程式將使用「SENSITIVE\*DATA\*DELETED」將其取代。

### 在安裝作業系統後安裝 MAK

透過使用「控制台」的「系統」項目或執行 Slmgr.vbs 指令碼，可以設定 Windows 7 和 Windows Server 2008 R2 的大量啟用版本以使用 MAK 啟用：

* 若要透過使用「系統」應用程式安裝 MAK，請按一下**變更產品金鑰**連結，然後在**變更您的啟用產品金鑰**對話方塊中鍵入 MAK。
* 若要使用 Slmgr.vbs 安裝 MAK，請在命令提示字元下執行下列命令：

slmgr.vbs /ipk <多重啟用金鑰>

其中，多重啟用金鑰 為 MAK。

如果使用者使用 UI 安裝 MAK，則 MAK 用戶端會嘗試透過網際網路進行一次啟用。如果使用者使用 Slmgr.vbs 指令碼安裝 MAK 金鑰，則 MAK 用戶端不會嘗試自動啟用。

### 停用自動啟用

若要停用任何 MAK 用戶端上的自動啟用，請將 **DWORD** 登錄值 **Manual** 設定為 **1**。此值位於登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\SoftwareProtectionPlatform\Activation** 內。

## 啟用 MAK 用戶端

MAK 用戶端會嘗試在下一排定的間隔內透過網際網路啟用。管理員可以強制透過網際網路、使用電話或使用大量啟用管理工具 (VAMT) 立即啟用。

若要確認啟用，請檢查系統匣中是否有「Windows 已啟用」的通知。或者，在命令提示字元下，輸入 **slmgr.vbs /dli** 以查看電腦的啟用狀態。

### 透過網際網路啟用 MAK 用戶端

可以下列任一方式透過網際網路啟用 MAK 用戶端：

* 按一下「控制台」的「系統」項目中的**按一下此處，立即啟用 Windows** 連結。Windows 會報告啟用是否成功。如果啟用失敗，精靈將會顯示其他選項。
* 在命令提示字元下執行 **slmgr.vbs /ato**。使用 slmgr.vbs 時不會顯示其他選項。

### 透過代理伺服器啟用 MAK 用戶端

如果代理伺服器需要使用者驗證，則透過網際網路的啟用可能遭到封鎖。在 Microsoft Internet Security and Acceleration (ISA) Server 中，此設定稱為基本驗證。由於啟用要求不會向代理伺服器顯示使用者認證，因此 Microsoft 建議不要針對 ISA Server 或其他代理伺服器使用「基本驗證」。但是，如果必須在代理伺服器上使用「基本驗證」或等效的機制，請將下列 URL 新增到**代理驗證排除**清單中：

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

### 使用電話啟用 MAK 用戶端

若要啟用已連線至組織網路但是無網際網路連線能力的電腦，請在「命令提示字元」視窗中使用 Slmgr.vbs，輸入：

slmgr.vbs TargetComputerName <使用者名稱> <密碼> /dti

以顯示完成電話啟用所需的資訊。若要取得您當地啟用客服中心的電話號碼，請執行 **slui.exe 4**。使用互動語音回應系統取得設定 ID (CID)；然後執行：

slmgr.vbs TargetComputerName <使用者名稱> <密碼> /atp <CID>

以安裝 CID。如果頻繁執行啟用或者啟用多台電腦，使用 Slmgr.vbs 指令碼將啟用程序自動化會更實用。

### 使用 VAMT 啟用 MAK 用戶端

VAMT 透過從集中控制台散佈 MAK，允許 MAK 部署及透過網路的啟用自動化，如圖 2 所示。VAMT 會查詢 Microsoft 啟用伺服器以取得給定 MAK 的剩餘啟用次數，然後列出環境中所有 MAK 啟用之系統的啟用狀態。此計數為及時快照，而非實時計數。VAMT 1.2 版包含在 Windows AIK 中，可以從 Microsoft 下載中心下載 Windows AIK

(<http://go.microsoft.com/fwlink/?LinkId=136976>)。



圖 2   VAMT 使用者介面

### 停用自動啟用

可以透過將現有的 **DWORD** 值 **Manual** 設定為 **1** 來停用任何 KMS 用戶端上的自動啟用。此值位於登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** 內。

## 整合 MAK 與 Deployment Workbench

Microsoft Deployment Toolkit (MDT) 還提供了部署 MAK 的解決方案。在 Deployment Workbench 中，管理員在工作順序中設定 MAK，工作順序會將 MAK 新增至安裝期間使用的 Unattend.xml 檔案中。管理員可以為 KMS 啟用準備參照映像，然後在部署期間，MDT 只要未偵測到 KMS 基礎結構，就會使用 MAK 啟用安裝。安裝完該映像後，MDT 會套用 MAK。如需 MDT 的詳細資訊，請參閱 **Deployment TechCenter（部署技術中心）**

(<http://technet.microsoft.com/en-us/deployment/default.aspx>)。

# 重新啟用電腦

Windows 7 和 Windows Server 2008 R2 會定期檢查安裝作業系統的電腦的硬體設定。如果作業系統偵測到硬體發生了重要變更，便會要求重新啟用。實際權數因數與閾值視情況而定，因為這些值必須與持續發展的電腦硬體市場保持同步。一般來說，使用 MAK 啟用的電腦與零售啟用使用的重新啟用規則相同。KMS 用戶端更多依賴硬碟變更來確定是否需要重新啟用。

用戶端啟用的有效期是 180 天。此期限稱為啟用有效間隔。為了維持啟用狀態，KMS 用戶端必須至少每 180 天連線至 KMS 主機一次，以更新啟用。依預設，KMS 用戶端電腦每 7 天會嘗試更新其啟用。更新用戶端的啟用後，啟用有效間隔會再次開始。

# 附錄 A：選用設定

大量啟用支援選用設定，它們在某些環境中可以起作用，但是對於大多數環境不建議使用。此附錄中的程序要求重新啟動軟體保護服務才能使設定生效。

## 啟用標準使用者啟用

若要在 KMS 用戶端上啟用標準使用者啟用，請新增 **DWORD** 登錄值 **UserOperations**，並將其值設定為 **1**。在登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\SoftwareProtectionPlatform** 內建立此值。

完成後，某些操作就不再需要管理權限，例如安裝產品金鑰 (**slmgr.vbs /ipk**)、安裝授權 (**slmgr.vbs /ilc**) 或者重複安裝 (**slmgr.vbs /rearm**)。這意味著標準使用者可以將 KMS 用戶端切換成 MAK 啟用、手動啟用電腦，以及在必要時使用新的 MAK 取代現有的 MAK。但是不建議這樣做，因為會降低電腦的安全性。

注：如果標準使用者安裝 MAK 或 KMS 金鑰，則不會更新 **ProductID** 登錄值。此行為主要會影響產品支援，並且 Microsoft 客戶支援服務 (CSS) 知道此情況。

## 停用啟用通知

軟體授權通知可以透過下列方式關閉：在登錄中新增 **DWORD** 值 **NotificationDisabled**，並將該值設為 **1**（但是不建議這麼做）。在登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform
\Activation** 內建立此值。此值會停用所有軟體授權通知，包括球形文字說明、精靈以及工作對話方塊。

## 啟用功能的登錄金鑰變更

Windows 7 與 Windows Server 2008 R2 在登錄中包括新軟體保護平台 (SPP) 金鑰。對於管理環境中的產品啟用，請設定**立即啟用 Windows** 對話方塊，以顯示選用的**瞭解線上啟用**連結，如圖 3 中所示。



圖3   瞭解線上啟用

按一下此自訂連結將管理員定義的 URL 載入使用者的預設瀏覽器。此 URL 可以指向自訂網頁
或其他儲存在本機電腦或網路共用上的檔案。大量授權客戶可以使用此連結提供客戶特定的啟
用資訊。若要顯示此連結，需要將 **REG\_SZ** 值 **ActivationAlternateURL** 設定為在使用者按一下此連結時要顯示的網頁的 URL。值 **ActivationAlternateURL** 在登錄子機碼 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** 內。

# 附錄 B：自動安裝檔案範例

<?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>