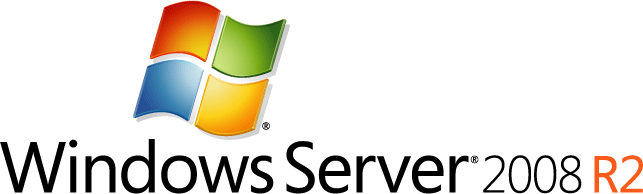
****

****  
  
**大量啟用技術參考指南**

**Windows 7 與 Windows Server 2008 R2**

Microsoft Corporation

發佈日期：2009 年 7 月

摘要

本參考指南適用於其組織正在規劃部署 Windows® 7 與 Windows Server® 2008 R2 作業系統大量啟用版本的資訊技術 (IT) 實作人員。本書為 *Volume Activation Planning Guide*（大量啟用規劃指南）、*Volume Activation Deployment Guide*（大量啟用部署指南）及 *Volume Activation Operations Guide*（大量啟用操作指南）的伴讀手冊。

本文件與其中任何參照文件僅供參考之用，Microsoft 不針對本文件進行明示或暗示保證。本文件的資訊（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本文件或使用本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、Hyper-V、Windows、Windows Server 和 Windows Vista 為 Microsoft 公司集團的商標。

本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**

[簡介 1](#_Toc534493623)

[使用者體驗 2](#_Toc534493624)

[Slmgr.vbs 選項 5](#_Toc534493625)

[登錄設定 12](#_Toc534493626)

[群組原則物件設定 15](#_Toc534493627)

[KMS 啟用時機 17](#_Toc534493628)

[KMS 探索搜尋順序 18](#_Toc534493629)

[啟用實例 19](#_Toc534493630)

[KMS 案例 19](#_Toc534493631)

[單一網站網路的預設 KMS 實作 20](#_Toc534493632)

[複雜、全域網路中的 KMS 實作 22](#_Toc534493633)

[MAK 案例 25](#_Toc534493634)

[MAK 獨立啟用 27](#_Toc534493635)

[MAK 代理啟用 32](#_Toc534493636)

[VAMT 對於 KMS 啟用的支援 39](#_Toc534493637)

[將 KMS 轉換為 MAK 啟用 40](#_Toc534493638)

[KMS 主機金鑰與產品的對照 41](#_Toc534493639)

[啟用原則值 43](#_Toc534493640)

[KMS 用戶端安裝金鑰 44](#_Toc534493641)

[啟用錯誤碼 46](#_Toc534493642)

[Windows 事件記錄檔 56](#_Toc534493643)

[WMI 屬性和方法 60](#_Toc534493644)

[詞彙 69](#_Toc534493645)

[資源連結 70](#_Toc534493646)

# 簡介

本指南提供[Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（大量啟用規劃指南）、[Volume Activation Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=150083)（大量啟用部署指南）及[Volume Activation Operations Guide](http://go.microsoft.com/fwlink/?LinkId=150084)（大量啟用操作指南）的技術參考資訊。如需 Microsoft® Volume Activation 及其元件的概觀，請參閱[Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（大量啟用規劃指南）。本參考指南包含：

* 使用者體驗
* Slmgr.vbs 選項
* 登錄設定
* 群組原則物件 (GPO) 設定
* 金鑰管理服務 (KMS) 啟用時機
* KMS 探索搜尋順序
* 啟用實例
* KMS 主機金鑰與產品的對照
* 啟用原則值
* KMS 用戶端安裝金鑰
* 啟用錯誤碼
* Windows® 事件記錄檔
* Windows Management Instrumentation (WMI) 屬性和方法
* 詞彙
* 資源

**注：**關於其他使用大量啟用的軟體，如需相關支援，請參閱特別針對這些應用程式所撰寫的文件。

本指南採用下列慣例：

* 命令列和命令列選項以粗體顯示。
* 命令列選項中的保留位置以角括弧 (<>) 括住。
* 選用命令列選項以方括弧 ([]) 括住。
* 登錄子機碼和值名稱以粗體顯示。

# 使用者體驗

Windows® 7 和 Windows Server® 2008 R2 會針對特定的啟用問題而顯示適合的通知和對話  
方塊。表 1 描述這些通知和對話方塊與每一個問題的對應關係。

**注**：Windows Server 2008 核心版本不提供通知使用者體驗。

表 1. 通知狀態的球形文字說明和對話方塊

| **問題** | **通知球形文字說明** | **對應的對話方塊** |
| --- | --- | --- |
| 最近安裝的 Windows 版本在啟用寬限期結束時尚未啟用。 |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |

|  |  |  |
| --- | --- | --- |
| 先前已啟用的 Windows 版本偵測到電腦硬體或基本輸入/輸出系統 (BIOS) 發生變更，這些變更需要重新啟用 Windows。另外，已啟用的 KMS 用戶端未在 180 天內自行重新啟用。 |  | 37-HW OOT.jpg |
| Windows 已透過 KMS 啟用，但在 180 天加 30 天寬限期內尚未更新其啟用。 |  | 37-KMS OOT.jpg |

|  |  |  |
| --- | --- | --- |
| 線上驗證失敗，或偵測到有惡意的啟用探索允許未經授權的 Windows 版本通過產品啟用。 |  | 37-NG.jpg |
| Windows 偵測到 Windows 授權元件已 變更。 |  | 37 - No Key.jpg |
| Windows 偵測到其授權檔案已變更。 |  | 37 - Reinstall.jpg |

# Slmgr.vbs 選項

由於 Windows 7 和 Windows Server 2008 R2 中的 WMI 有所變動，Slmgr.vbs 指令碼已不適合跨平台執行。不支援從 Windows Vista® 作業系統使用 Slmgr.vbs 來管理 Windows 7 或 Windows Server 2008 R2 系統。嘗試從 Windows 7 或 Windows Server 2008 R2 管理舊版系統會產生明確的版本不符錯誤。例如，執行 **cscript slmgr.vbs <Vista 電腦名稱> /dlv** 會產生下列輸出：

Microsoft (R) Windows Script Host 5.8 版   
Copyright (C) Microsoft Corporation. All rights reserved.

遠端電腦不支援此版本的 SLMgr.vbs

若要管理遠端用戶端，請使用大量啟用管理工具 (VAMT) 1.2 版或更高版本，或是建立可辨別平台差異的自訂 WMI 指令碼。如需大量啟用的 WMI 屬性和方法的詳細資訊，請參閱本參考指南後面的「」一節。

以下描述 Slmgr.vbs 指令碼的語法，表 2 描述每一個命令列選項：

slmgr.vbs [電腦名稱 [使用者] [密碼]] [<選項>]

**注：**關於其他使用大量啟用的軟體，如需相關支援，請參閱特別針對這些應用程式所撰寫的文件。

表 2. Slmgr.vbs 命令列選項

| **選項** | **描述** |
| --- | --- |
| **[電腦名稱]** | 遠端電腦的名稱（預設值為本機電腦） |
| **[使用者]** | 在遠端電腦上具有必要權限的帳戶 |
| **[密碼]** | 在遠端電腦上具有必要權限之帳戶的密碼 |
| **全域選項** | |
| **/ipk 產品金鑰** | 嘗試安裝 5×5 產品金鑰。由此參數提供的產品金鑰已確認有效，且適用於已安裝的作業系統。如果無效，則傳回錯誤。  如果金鑰有效且適用，則安裝金鑰。如果已安裝金鑰，則自動取代它。  為了避免授權服務不穩定，應該重新啟動系統，或重新啟動軟體保護服務。  必須在升級的命令提示字元下執行此操作，不然就必須設定**標準使用者操作**登錄值，以允許不具權限的使用者可額外存取軟體保護服務。 |
| **/ato [啟用識別碼]** | 對於已安裝 KMS 主機金鑰或多重啟用金鑰 (MAK) 的零售版本和大量授權系統，**/ato** 會提示 Windows 嘗試進行線上啟用。  對於已安裝一般大量授權金鑰 (GVLK) 的系統，此參數會提示嘗試進行 KMS 啟用。執行 **/ato** 時，已設定為暫停自動嘗試 KMS 啟用 (**/stao**) 的系統仍然會嘗試 KMS 啟用。  參數 **[啟用識別碼]** 會擴充 **/ato** 支援來識別電腦上安裝的 Windows 版本。指定 **[啟用識別碼]** 參數會將此選項的執行結果限定於該啟用識別碼相關聯的版本。執行 **Slmgr.vbs /dlv all** 可取得已安裝的 Windows 版本的啟用識別碼。如果您需要支援其他應用程式，請參閱該應用程式所提供的指南，以取得進一步的指示。  KMS 啟用不需要較高的權限。但是，線上啟用需要提高權限，不然就必須設定**標準使用者操作**登錄值，以允許不具權限的使用者可額外存取軟體保護服務。 |
| **/dli [啟用識別碼 | All]** | 顯示授權資訊。  依預設，**/dli** 會顯示已安裝的使用中 Windows 版本的授權資訊。指定 **[啟用識別碼]** 參數會顯示該啟用識別碼相關聯之指定版本的授權資訊。指定 **[All]** 作為參數會顯示所有適用之已安裝產品的授權資訊。  此操作不需要較高的權限。 |
| **/dlv [啟用識別碼 | All]** | 顯示詳細的授權資訊。  依預設，**/dlv** 會顯示已安裝之作業系統的授權資訊。指定 **[啟用識別碼]** 參數會顯示該啟用識別碼相關聯之指定版本的授權資訊。指定 **[All]** 參數會顯示所有適用之已安裝產品的授權資訊。  此操作不需要較高的權限。 |
| **/xpr [啟用識別碼]** | 顯示產品的啟用到期日。依預設，這是指目前的 Windows 版本，且主要適用於 KMS 用戶端，因為 MAK 和零售啟用永久有效。  指定 **[啟用識別碼]** 參數會顯示該啟用識別碼相關聯之指定版本的 啟用到期日。  此操作不需要較高的權限。 |
| **進階選項** | |
| **/cpky** | 在「全新體驗」(OOBE) 操作期間，某些服務操作需要登錄中已存在產品金鑰。**/cpky** 選項會從登錄中移除產品金鑰，以防止惡意程式碼竊取此金鑰。  對於部署金鑰的零售安裝，最佳做法是執行此選項。MAK 和 KMS 主機金鑰不需要此選項，因為這是這些金鑰的預設行為。對於其他類型的金鑰，如果預設行為不會從登錄中清除金鑰，此時才需要此選項。  必須在升級的命令提示字元下執行此操作。 |
| **/ilc <授權檔案>** | 此選項會安裝由必要參數所指定的授權檔案。這些授權可能安裝做為疑難排解工具、為了支援權杖型啟用而安裝，或手動安裝整合式應用程式的過程中安裝。  在此程序執行期間不會驗證授權：授權驗證超出 Slmgr 的責任範圍。驗證是由軟體保護服務在執行階段負責進行。  必須在升級的命令提示字元下執行此操作，不然就必須設定**標準使用者操作**登錄值，以允許不具權限的使用者可額外存取軟體保護服務。 |
| **/rilc** | 此選項會重新安裝 %SystemRoot%\system32\oem 和 %SystemRoot%\System32\spp\tokens 中儲存的所有授權。這些是安裝期間所儲存的「已知正確」複本。  將會取代信任存放區中任何相符的授權。其他任何授權不受影響，例如，受信任認證單位 (TA) 發行授權 (IL)、應用程式的授權。  必須在升級的命令提示字元下執行此操作，不然就必須設定**標準使用者操作**登錄值，以允許不具權限的使用者可額外存取軟體保護服務。 |
| **/rearm** | 此選項會重設啟用計時器。**sysprep /generalize** 也會 呼叫 **/rearm** 程序。  如果 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SoftwareProtectionPlatform\SkipRearm 登錄子機碼等於 **1**，此操作不會執行任何動作。如需此登錄子機碼的詳細資訊，請參閱本指南後面的「」一節。  必須在升級的命令提示字元下執行此操作，不然就必須設定**標準使用者操作**登錄值，以允許不具權限的使用者可額外存取軟體保護服務。 |
| **/upk [啟用識別碼]** | 此選項會解除安裝目前的 Windows 版本的產品金鑰。重新啟動系統之後，除非安裝新的產品金鑰，否則系統會處於「未授權」狀態。  您可以選擇性地使用 **[啟用識別碼]** 參數來指定另一個已安裝的產品。  必須在升級的命令提示字元下執行此操作。 |
| **大量授權：KMS 用戶端選項** | |
| **/skms 名稱[:連接埠] |：連接埠 [啟用識別碼] [啟用識別碼]** | 此選項指定要聯繫的 KMS 主機電腦的名稱及（選用的）連接埠。設定此值會停用 KMS 主機的自動偵測。  如果 KMS 主機僅使用網際網路通訊協定第 6 版 (IPv6)，必須以 [主機名稱]:連接埠 格式指定位址。IPv6 位址包含冒號 (:)，但 Slmgr.vbs 指令碼無法正確剖析冒號。  必須在升級的命令提示字元下執行此操作。 |
| **/ckms [啟用識別碼]** | 此選項會從登錄中移除指定的 KMS 主機名稱、位址和連接埠資訊，並還原 KMS 自動探索行為。  必須在升級的命令提示字元下執行此操作。 |
| **/skhc** | 此選項會啟用 KMS 主機快取（預設值），這樣會在初次探索工作中 KMS 主機之後禁止使用網域名稱系統 (DNS) **優先順序**和**權數**。如果系統已無法再聯繫工作中 KMS 主機，則會重新嘗試探索。  必須在升級的命令提示字元下執行此操作。 |
| **/ckhc** | 此選項會停用 KMS 主機快取。此設定會指示用戶端在每次嘗試 KMS 啟用時使用 DNS 自動探索（使用**優先順序**和**權數**時，建議使用此選項）。  必須在升級的命令提示字元下執行此操作。 |
| **KMS 主機設定** | |
| **/sai <間隔>** | 此選項會設定未啟用的用戶端嘗試 KMS 連線的間隔，以分鐘為單位。建議採用預設值（2 小時），但啟用間隔必須介於 15 分鐘和 30 天之間。  KMS 用戶端一開始會從登錄中挑選此間隔，但會在接收到第一個 KMS 回應後切換至 KMS 設定。  必須在升級的命令提示字元下執行此操作。 |
| **/sri <間隔>** | 此選項會設定已啟用的用戶端嘗試 KMS 連線的更新間隔，以分鐘為單位。更新間隔必須介於 15 分鐘和 30 天之間。KMS 伺服器和用戶端最初都會設定此選項。預設值為 10080 分鐘（7 天）。  KMS 用戶端一開始會從登錄中挑選此間隔，但會在接收到第一個 KMS 回應後切換至 KMS 設定。  必須在升級的命令提示字元下執行此操作。 |
| **/sprt <連接埠>** | 此選項會設定連接埠，供 KMS 主機用來接聽用戶端啟用要求。預設 TCP 連接埠為 1688。  必須在升級的命令提示字元下執行此操作。 |
| **/sdns** | 啟用 KMS 主機的 DNS 發佈（預設值）。  必須在升級的命令提示字元下執行此操作。 |
| **/cdns** | 停用 KMS 主機的 DNS 發佈。  必須在升級的命令提示字元下執行此操作。 |
| **/spri** | 將 KMS 優先順序設定為一般（預設值）。  必須在升級的命令提示字元下執行此操作。 |
| **/cpri** | 將 KMS 優先順序設定為低。  使用此選項可在共同裝載環境下將爭用 KMS 的情況降到最低。請注意，此值可能會因為使用的應用程式及伺服器角色類型不同而導致 KMS 耗盡。請小心使用。  必須在升級的命令提示字元下執行此操作。 |
| **權杖型啟用設定** | |
| **/lil** | 列出已安裝的權杖型啟用發行授權。 |
| **/ril <ILID> <ILvID>** | 移除已安裝的權杖型啟用發行授權。  必須在升級的命令提示字元下執行此操作。 |
| **/stao** | 設定**僅權杖型啟用**旗標，停用自動 KMS 啟用。  必須在升級的命令提示字元下執行此操作。 |
| **/ctao** | 清除**僅權杖型啟用**旗標（預設值），啟用自動 KMS 啟用。  必須在升級的命令提示字元下執行此操作。 |
| **/ltc** | 列出可啟用已安裝之軟體的有效權杖型啟用憑證。 |
| **/fta <憑證指紋> [PIN]** | 強制使用已識別的憑證來執行權杖型啟用。使用受硬體（例如智慧卡）保護的憑證時，提供的選擇性個人識別碼 (PIN) 可以解除鎖定私密金鑰，而不會出現 PIN 提示。 |

# 登錄設定

表 3 描述大量啟用所支援的登錄設定。

表 3. 登錄設定

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **登錄子機碼：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **值** | **類型** | | **描述** | | **範圍** |
| **Activation\AlternateURL** | **REG\_SZ** | | 選擇性地包含系統管理員提供的 URL。如果填入此機碼，某些啟用對話方塊會包含一個可在預設瀏覽器中開啟的新連結：**瞭解線上啟用**。 | | 所有 |
| **DisableDnsPublishing** | **REG\_DWORD** | | 將此值設定為非零值，可禁止 KMS  主機自動發佈至 DNS。 | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **格式：**網域名稱, <優先順序>,  <權數>  選擇性地包含一份由 KMS 用來自動發佈其 DNS 服務 (SRV) 記錄的完整網域清單。這通常會使用 KMS 主網域，因此不需在此包含該網域。這取決於  **DisableDnsPublishing** 值。  **優先順序**和**權數**為選用參數。如果未提供這些參數，則在 SRV 記錄中 會設為 **0**。 | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | 將此值設定為非零值，以便將在共同裝載環境中的 KMS 爭用降到最低。請注意，在忙碌的系統上，這樣可以避免 KMS 主機必須保持足夠的數量。 | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | 在 KMS 主機上設定此值可強制 KMS 在指定的 TCP 連接埠上接聽。如果未指定此值，主機會使用 TCP 連接埠 1688。 | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | 設定此值以強制 KMS 用戶端使用特定 KMS 主機。無預設值。  如果指定 App-ID 或 SKU-ID，這會在儲存此值的子機碼下建立：  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName | | KMS 用戶端 |
| **KeyManagementServicePort** | **REG\_SZ** | | 設定此值以強制 KMS 用戶端與 KMS 進行通訊時，由 KMS 用戶端使用特定 TCP 連接埠。如果未指定此值，用戶端會使用連接埠 1688。  如果指定 App-ID 或 SKU-ID，這會在儲存此值的子機碼下建立：  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort | | KMS 用戶端 |
| **KeyManagementServiceVersion** | **REG\_SZ** | | 設定此值可讓 Microsoft Operations Manager (MOM) 2005 自動探索 KMS。如果 KMS 在電腦上不再有任何作用，請刪除此值。 | | KMS |
| **UserOperations** | **REG\_DWORD** | | 依預設不存在此值，預設值為 **0**，但這需要提高權限。建立此值並設定為 **1**，可讓標準使用者安裝產品金鑰並啟用和重新授權電腦，而不需要提高授權。  此設定也可由儲存在 **\policies** 登錄子機碼下的 GPO 來設定。 | | 所有 (不限於 KMS) |
| **VLActivationInterval** | **REG\_DWORD** | | KMS 伺服器和用戶端最初都會設定此值。預設值為 120 分鐘（2 小時）。KMS 用戶端一開始會從登錄中挑選此間隔，但會在接收到第一個 KMS 回應後切換至 KMS 設定。最小值為 15 分鐘，最大值為 43,200 分鐘（30 天）。 | | KMS 用戶端與伺服器 |
| **VLRenewalInterval** | **REG\_DWORD** | | KMS 伺服器和用戶端最初都會設定此值。預設值為 10,080 分鐘（7 天）。KMS 用戶端一開始會從登錄中挑選此間隔，但會在接收到第一個 KMS 回應後切換至 KMS 設定。因此，永遠不會使用用戶端設定。最小值為 15 分鐘，最大值為 43,200 分鐘（30 天）。 | | KMS 用戶端與伺服器 |
| **登錄子機碼：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **值** | **類型** | **描述** | | **範圍** | |
| **Manual** | **REG\_DWORD** | **0** = 允許自動線上啟用（預設值）  **1** = 停用自動啟用 | | MAK 和 KMS 主機，但不是 KMS 用戶端 | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = 顯示啟用通知及球形文字說明（預設值）  **1** = 如果 Windows 不是處於「通知」或「未授權」狀態，則隱藏啟用相關的所有通知。不建議使用。 | | 所有 (不限於 KMS) | |

# 群組原則物件設定

表 4 描述群組原則設定，可供組織用來防止作業系統在「通知」狀態下將桌面變更為黑色。

表 4. 群組原則物件設定

| **原則名稱** | **描述** |
| --- | --- |
| **使用者設定 -> 系統管理範本 -> 控制台 -> 個人化 ->  防止變更桌面背景** | 防止使用者新增或變更桌面的背景設計。  依預設，使用者可以使用「個人化」或「顯示控制台」項目 中的**桌面背景**頁面，將背景設計（底色圖案）新增至他們的 桌面。  如果您啟用此設定，使用者就無法變更桌面背景的任何設定。  若要指定群組的底色圖案，請使用**桌面底色圖案**設定。  **注**：您也必須啟用**桌面底色圖案**設定，才能防止使用者變更桌面底色圖案。如需詳細資訊，請參閱 Microsoft 說明及支援文章「系統管理員在群組原則選取「防止變更桌面底色圖案」選項後，您仍可以變更桌面底色圖案設定值」，網址為 <http://support.microsoft.com/kb/Q327998>。  另請參閱**只允許點陣圖底色圖案**設定。 |
| **使用者設定 -> 系統管理範本 -> 桌面 -> 桌面 -> 桌面底色圖案** | 指定在所有使用者的桌面上顯示的桌面背景（底色圖案）。  此設定可讓您指定使用者桌面上的底色圖案，同時防止使用者變更影像或其呈現方式。您指定的底色圖案可以儲存為點陣圖 (\*.bmp) 或 JPEG (\*.jpg) 檔案。  若要使用此設定，您輸入儲存底色圖案影像之檔案的完整路徑和名稱。您可以輸入本機路徑，例如 C:\Windows\web\wallpaper\home.jpg,，也可以輸入通用命名慣例 (UNC) 路徑，例如 \\Server\Share\Corp.jpg。當使用者登入時，如果指定的檔案無法使用，則不會顯示底色圖案。使用者無法指定替代的底色圖案。您也可以使用此設定來指定底色圖案影像要置中、並列或延展顯示。使用者無法變更這項指定。  如果您停用此設定或未設定它，則不會顯示任何底色圖案。不過，使用者仍然可以自行選取底色圖案。  另請參閱相同位置中的**只允許點陣圖底色圖案**設定，以及「使用者設定\系統管理範本\控制台」中的**防止變更底色圖案** 設定。  **注**：此設定不會套用至遠端桌面伺服器工作階段。 |
| **使用者設定 -> 系統管理範本 -> 控制台 -> 個人化 -> 防止變更桌面圖示** | 防止使用者變更桌面圖示。  依預設，使用者可以使用「個人化」或「顯示控制台」項目中的**桌面圖示設定**對話方塊，以顯示、隱藏或變更桌面圖示。  如果您啟用此設定，使用者就無法變更任何桌面圖示。  在 Windows Vista 以前的作業系統中，此設定也會隱藏「顯示控制台」項目中的**桌面**索引標籤。 |

# KMS 啟用時機

KMS 啟用時機由兩項設定所控制：啟用計時器和更新計時器：

* KMS 啟用間隔 決定 KMS 用戶端在啟用之前和在寬限期與通知期間，每隔多久嘗試啟用一次。此值是在用戶端上執行 **slmgr.vbs /sai *間隔*** 而設定。間隔以分鐘為單位，預設值為 120 分鐘。如需詳細資訊，請參閱「」和「」。當系統聯繫到 KMS 主機之後，KMS 主機設定會覆寫本機用戶端設定。
* KMS 更新間隔 決定 KMS 用戶端在啟用之後，每隔多久嘗試向 KMS 重新啟用一次。可以使用 **slmgr /sri *間隔*** 來設定此值。間隔以分鐘為單位來設定。預設值為 10,080 分鐘（7 天）。此值可以在用戶端設定，但會被 KMS 主機提供的值所覆寫。

在操作中，KMS 用戶端會在啟動時嘗試聯繫 KMS 主機，而在失敗時會每隔「啟用間隔」分鐘就重新嘗試聯繫一次。依預設，這會每隔兩小時發生一次。當 KMS 啟用成功時，用戶端會接收並儲存 KMS 主機的更新間隔，而 Windows 會啟用 180 天。啟用更新的運作如同滑動視窗一樣，類似動態主機設定通訊協定 (DHCP) 租用。用戶端會啟用 180 天，但仍然會每隔「更新間隔」分鐘（預設值為 7 天）就嘗試重新啟用一次。如果成功，180 天的週期會重設。如果失敗，系統會等待網路變更或其他合格事件，以觸發另一次嘗試。經過 15 分鐘，系統就會停止監控合格事件，但仍然會每隔「啟用間隔」分鐘就嘗試一次。

如果經過 180 天都沒有成功重新啟用，用戶端會轉換到容許寬限期外 (OOT)。如果在轉換到 OOT 的 30 天內未啟用，則會進入通知模式。

# KMS 探索搜尋順序

當 KMS 自動探索已啟用（預設值）且 KMS 主機快取未停用時，KMS 用戶端會依照下列順序來決定要使用的 KMS（它們會嘗試每一步，直到具有正確金鑰的已啟用 KMS 主機有所回應為止）：

* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ 登錄值中的 SKU 特定值
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ 登錄值中的 AppID 特定值
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ 登錄值中的全域值
* SKU 特定快取的 KMS 主機（這是上次 KMS 成功啟用時所使用的主機的快取身分識別）。
* DNS 自動探索（採用**權數**和**優先順序**）

如果快取的 KMS 沒有回應，則執行探索。

# 啟用實例

以下各節描述 KMS 和 MAK 啟用的主要案例。

## KMS 案例

KMS 可以支援簡單、單一網站的網路及全域網路。下列案例顯示：

* KMS 的預設實作。
* 此實作擴充來支援全域網路。

### 單一網站網路的預設 KMS 實作

Contoso 具有 100 個 Windows 7 企業版用戶端，也具有一組混合著 Windows Vista、Windows Server 2008 和 Windows Server 2008 R2 的系統。如「圖 1」所示，Contoso 採用單層網域 (Contoso.com)。DNS 伺服器以預設設定執行 Microsoft DNS。此設定支援動態 DNS 登錄和 DNS 記錄清除，以移除過期的記錄。



圖 1. 單一網站網路的預設 KMS 實作

Contoso 購買一份提供 KMS B 金鑰的授權合約，此金鑰可以啟用其所有系統。資訊技術 (IT) 系統管理員在升級的命令提示字元下執行下列命令，將 Contoso 的 KMS 主機金鑰 (CSVLK) 安裝在兩部執行 Windows Server 2008 R2 的 KMS 主機上：

Slmgr.vbs /ipk <KMS 主機金鑰>

接著，IT 系統管理員在 Active Directory® 網域服務 (AD DS) 中建立一個名稱為*KMS\_主機* 的安全性群組。系統管理員將伺服器 KMS\_1 和 KMS\_2 新增至KMS\_主機成員資格中。

透過網際網路向 Microsoft 啟用主機 KMS\_1：**Slmgr.vbs /ato**。KMS\_1 自動將其 SRV 資源記錄 (RR) 發佈至 DNS。IT 系統管理員存取 DNS 伺服器，並尋找 \_vlmcs.\_tcp.contoso.com 的 RR，然後變更其權限，將此記錄的讀取、寫入和刪除權限授與KMS\_主機。現在透過網際網路向 Microsoft 啟用主機 KMS\_2：**Slmgr.vbs /ato***。*

最後，系統管理員確認 Windows 防火牆中已啟用 KMS 主機排除。需要啟用金鑰管理服務防火牆例外。

Contoso 網路上的 KMS 用戶端會查詢 DNS，並接收這兩部 KMS 主機的 SRV 記錄。用戶端會挑選其中一部主機，接著就啟用（一旦 KMS 計數超過臨界值就立即啟用）。如需 KMS 計數需求的詳細資訊，請參閱「」一節。

### 複雜、全域網路中的 KMS 實作

如「圖 2」所示，Contoso 已擴充成兩個網域：east.contoso.com 和 west.contoso.com。網路流量可以經由受防火牆保護的廣域網路 (WAN) 連結，而在這兩個網路之間私下流通。由於此連結的頻寬有限，所以會儘可能在 WAN 連結的兩端複寫資源（包括 DNS），以減少流量。



圖 2. 複雜、全域網路中的 KMS 實作

Contoso 採用基於映像的部署。其用戶端系統全部採用 Windows Vista，但 Windows Vista 系統正由 Windows 7 用戶端所取代。

使用者會定期到各地旅行，而其網路連線會隨著不同的網域而變更。用戶端的 IP 位址由 DHCP 動態提供，包括指定當地 DNS 主機、當地閘道位址等等。

為了對現有的 Windows Vista 用戶端和新的 Windows 7 用戶端提供啟用支援，Contoso 安裝四部 KMS 主機（使用 KMS B 金鑰）。其中的兩部 KMS 主機在 east.contoso.com 中設定，另外兩部主機在 west.contoso.com 中設定。

IT 系統管理員設定 KMS 主機，讓 DNS SRV 記錄決定將 east 網域中的 Windows 7 和 Windows Server 2008 R2 用戶端導向 KMS\_E1（如果可用的話）或 KMS\_E2。如果兩者都無法使用，用戶端會先嘗試 KMS\_W1，最後才嘗試 KMS\_W2。同樣地，west 網域中的 DNS 也設定為讓 west 網域中的 Windows 7 用戶端優先聯繫 KMS\_W1，然後才聯繫 KMS\_W2，且只有當這些都失敗時，才會嘗試啟用 WAN 連結遠端的 KMS\_E1 和 KMS\_E2。

IT 系統管理員進行下列設定變更來完成此工作（請參閱表 5）：

* 將 KMS\_E\* 主機新增至安全性群組 KMS\_E。將記錄 \_vlmcs.\_tcp.east.contoso.com 的讀取、寫入和刪除權限授與此群組。
* 將 KMS\_W\* 主機新增至安全性群組 KMS\_W。將記錄 \_vlmcs.\_tcp.west.contoso.com 的讀取、寫入和刪除權限授與此群組。
* 設定 DHCP 伺服器，將 east.contoso.com 和 west.contoso.com 新增至所有用戶端的 DNS 尾碼搜尋清單。
* 設定 east 和 west 網域之間的防火牆，允許 RPC 流量傳送至 KMS 主機的連接埠 1688。

表 5. KMS 主機設定

| **描述** | **設定** | **主機** |
| --- | --- | --- |
| 設定 east.contoso.com SRV 優先順序和權數，讓用戶端在嘗試 KMS\_W\* 主機之前先聯繫 KMS\_E\* 主機（如果可用的話）。流量會分割為：75% 流向 KMS\_\*1 主機，25% 流向 KMS\_\*2 主機。 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_E1, 10, 75  KMS\_E2, 10, 25  KMS\_W1, 90, 75  KMS\_W2, 90, 25 | KMS\_E1  KMS\_E2 |
| 設定 west.contoso.com SRV 優先順序和權數，讓用戶端在嘗試 KMS\_E\* 主機之前先聯繫 KMS\_W\* 主機（如果可用的話）。流量會分割為：75% 流向 KMS\_\*1 主機，25% 流向 KMS\_\*2 主機。 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_W1, 10, 75  KMS\_W2, 10, 25  KMS\_E1, 90, 75  KMS\_E2, 90, 25 | KMS\_W1  KMS\_W2 |

然後，系統管理員確認已設定 Windows 防火牆例外來允許 KMS 用戶端流量，並如表 6 所述來設定用戶端電腦。

表 6. KMS 用戶端設定

| **描述** | **設定** |
| --- | --- |
| 停用 KMS 主機快取 | **Slmgr /ckhc** |
| 設定客戶 URL，將發生啟用問題的使用者導向 Contoso 服務中心 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  AlternateURL = http://contoso.com/help |

用戶端參照電腦透過 KMS 啟用，接著會執行 **sysprep /generalize**。系統會關機，並使用 Windows 7 Windows 自動化安裝套件 (Windows AIK) 的 ImageX 進行映像處理。可從   
<http://go.microsoft.com/fwlink/?LinkId=136976> 下載 Windows AIK。

## MAK 案例

以下各節描述 MAK 啟用的案例，這些案例以「圖 3」所示的案例為基礎。此圖顯示大型企業內常見的網路和工作群組環境。

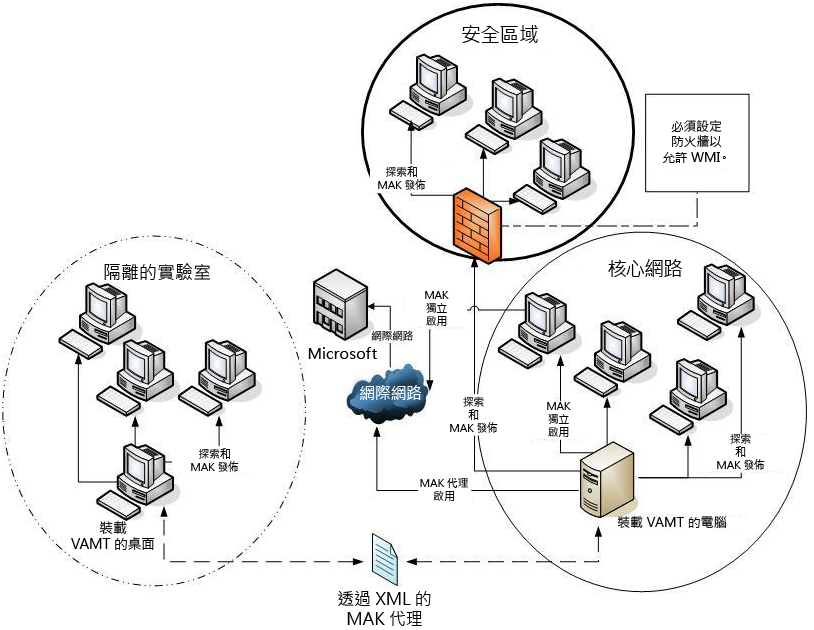


圖 3. 企業環境

在核心網路環境中，所有電腦都位於 AD DS 所管理的一般網路內。安全區域代表具有額外防火牆  
保護的高安全性核心網路電腦。

隔離的實驗室環境是一個工作群組，實際上與核心網路分開，其電腦無法存取網際網路。網路安全性原則指出不可從隔離的實驗室往外傳輸任何可識別特定電腦或使用者的資訊。

### MAK 獨立啟用

VAMT 允許從集中控制台散佈 MAK，以透過網路自動進行 MAK 部署及啟用，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。Windows AIK 包含 VAMT 1.2 版。

在本案例中，VAMT 部署在核心網路環境中，如「圖 3」所示。VAMT 安裝在可透過網路存取所有用戶端電腦的一部中心電腦上。VAMT 主機與用戶端電腦都可存取網際網路。下列指示描述如何執行獨立啟用：

1. 在連接網路的主機電腦上安裝並啟動 VAMT：
   1. 在主機電腦上安裝 Windows AIK。
   2. 按一下「開始」，然後按一下 **VAMT**，以開啟 VAMT 主控台。
2. 在目標電腦上設定 Windows Management Instrumentation (WMI) 防火牆例外。確定已針對所有目標電腦啟用 WMI 防火牆例外，如「圖 4」所示。

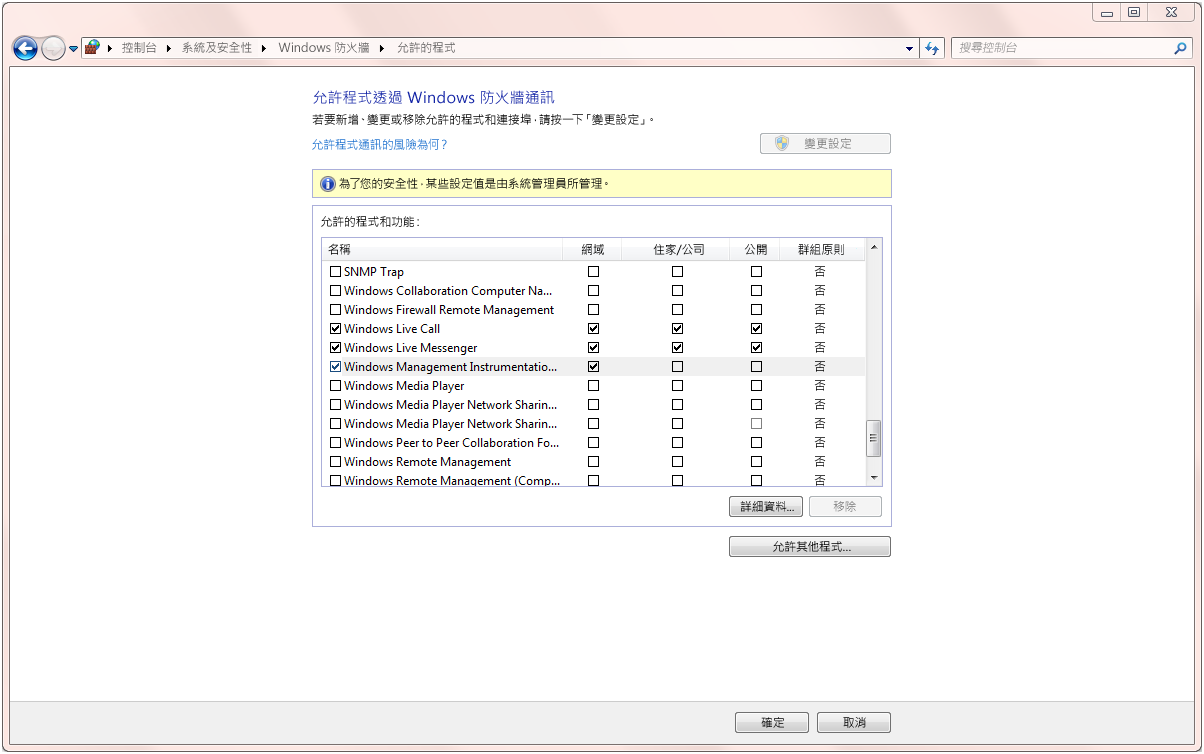


圖 4. Windows Management Instrumentation (WMI) 例外

1. 將電腦新增至電腦資訊清單 (CIL)：
   1. 在 VAMT 主控台，按一下**動作**，然後按一下**新增電腦**，以顯示**新增電腦**對話方塊。
   2. 輸入電腦群組名稱，例如*核心網路群組*，以識別您所啟用的電腦群組。
   3. 按下拉式清單以選取搜尋選項。您可以搜尋工作群組或 AD DS 網域中的電腦，或依個別電腦名稱或 IP 位址來搜尋電腦。
   4. 如果您依個別電腦名稱或 IP 位址來搜尋，請在下拉式清單下方的文字方塊中輸入該資訊。
   5. 如果您搜尋網域或工作群組，請從這些選項所顯示的額外下拉式清單中選取此網域或工作群組。請使用**依電腦名稱篩選**欄位來搜尋網域或工作群組內的特定電腦。
   6. 按一下**確定**。

VAMT 會透過輕量型目錄存取通訊協定 (LDAP) 來查詢 Active Directory 目錄服務 (AD DS)，然後將找到的電腦新增至 CIL。

1. 從已探索到的電腦收集狀態資訊：
   1. 為了讓 VAMT 在電腦上執行動作，它必須取得該電腦的最新授權狀態資料。請直接在電腦清單檢視窗格中選取一或多部電腦，以收集個別電腦的狀態。若要對整個群組執行操作，請在樹狀檢視窗格中選取「狀態不明」節點或「使用者定義的群組\核心網路群組」節點。
   2. 以滑鼠右鍵按一下群組或想要的電腦，然後按一下**重新整理電腦狀態**。
   3. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**。
   4. 按一下**確定**。
   5. 出現提示時，請提供網域系統管理員帳戶（用來收集網域中所有電腦的狀態）和密碼。

VAMT 在收集所有選取的電腦的狀態時，會顯示**正在收集電腦資訊**對話方塊。程序完成時，VAMT 主控台的電腦清單檢視窗格中會顯示每一部電腦已重新整理的狀態。

**注**：為了抓取所選取之電腦的授權狀態，VAMT 必須具有遠端電腦的系統管理權限，且必須可通過 Windows 防火牆來存取 WMI。此外，對於工作群組電腦，必須建立一個登錄機碼，以允許在使用者帳戶控制 (UAC) 下執行遠端系統管理動作。如需設定系統以進行 VAMT 遠端管理的詳細資訊，請參閱 VAMT 說明。

1. 新增 MAK，並決定其剩餘啟用計數：
   1. 按一下**選項**，然後按一下**管理 MAK**，以開啟**管理 MAK 金鑰**對話方塊。
   2. 按一下**新增**以輸入 MAK。
   3. 輸入 MAK，然後按一下**驗證**。

通過驗證之後，就會自動填入**版本**欄位。

* 1. 提供有意義的描述，然後按一下**新增**。

**管理 MAK 金鑰**對話方塊中現在會列出此 MAK。

* 1. 按一下**重新整理剩餘計數**，以從 Microsoft 抓取所列出的 MAK 的剩餘啟用次數（此步驟需要網際網路連線）。
  2. 按一下**結束**以關閉對話方塊。

1. 安裝 MAK，並啟用用戶端電腦：
   1. 在樹狀檢視窗格中按一下群組，或在清單檢視窗格中選取個別電腦，以選取要啟用的電腦。
   2. 以滑鼠右鍵按一下所選取的群組或電腦，然後按一下 **MAK 獨立啟用**，以顯示 **MAK 獨立啟用**對話方塊。
   3. 從**安裝 MAK** 清單中選取適當的 MAK。
   4. 選取**安裝 MAK (覆寫現有的)** 和**立即啟用**核取方塊，以指示所選取的電腦立即透過網際網  
      路聯繫 Microsoft Windows 啟用來進行啟用。

如果這些核取方塊的旁邊出現星號 (\*)，則動作只會套用至適用的電腦。例如，無法使用 MAK 來啟用已安裝 Windows 零售版本的電腦。

* 1. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**。
  2. 按一下**確定**。

VAMT 會顯示**正在指派產品金鑰**對話方塊，接著顯示**正在啟用電腦**對話方塊，直到完成要求的動作為止。如果您選取**使用備用認證**，則在出現這些對話方塊之前會提示您輸入認證。

### MAK 代理啟用

在本案例中，使用 VAMT 來啟用「圖 3」所示之隔離的實驗室環境內的工作群組電腦。針對這類工作群組（與更大的網路完全分開），您可以在隔離的工作群組內的一部電腦上安裝第二個 VAMT，並使用卸除式媒體在該電腦與另一個可存取網際網路的 VAMT 主機之間傳輸 VAMT CIL，以執行 MAK 代理啟用。如需設定系統以進行 VAMT 遠端管理的詳細資訊，請參閱 VAMT 說明。下列步驟描述如何使用 VAMT 工具進行代理啟用：

1. 在隔離的實驗室中的一部工作群組電腦上安裝 VAMT：
   1. 在隔離的實驗室工作群組中的一部主機電腦上安裝 Windows AIK。

此電腦可以執行 Windows XP（含 Service Pack 2 (SP2)）、Windows Server 2003、Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2。

* 1. 按一下「開始」，然後按一下 **VAMT**，以開啟 VAMT 主控台。
  2. 在目標電腦上設定 Windows Management Instrumentation (WMI) 防火牆例外。確定已針對所有目標電腦啟用 WMI 防火牆例外。

1. 將電腦新增至 CIL：
   1. 在 VAMT 主控台，按一下**動作**，然後按一下**新增電腦**，以開啟**新增電腦**對話方塊。
   2. 輸入群組名稱，例如*隔離的實驗室群組*，以識別您所啟用的電腦群組。
   3. 選取**工作群組**選項，並指定工作群組的名稱，然後按一下**確定**。

VAMT 會在工作群組中搜尋電腦。

**注**：為了讓 VAMT 可以探索工作群組中的用戶端電腦，必須啟用網路探索 Windows 防火牆例外。

1. 從已探索到的電腦收集狀態：
   1. 為了讓 VAMT 在電腦上執行動作，它必須取得該電腦的最新授權狀態資料。請直接在電腦清單檢視窗格中選取一或多部電腦，以收集個別電腦的狀態。若要對整個群組執行操作，請在左邊窗格中選取「狀態不明」節點或「使用者定義的群組\隔離的實驗室群組」節點。
   2. 以滑鼠右鍵按一下群組或想要的電腦，然後按一下**重新整理電腦狀態**。
   3. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**。
   4. 按一下**確定**。出現提示時，請針對在選取的工作群組電腦上具有本機系統管理權限的帳戶提供認證。

VAMT 在收集所有選取的電腦的狀態時，會顯示**正在收集電腦資訊**對話方塊。程序完成時，VAMT 主控台的電腦清單檢視窗格中會顯示每一部電腦已重新整理的狀態。

**注**：為了抓取所選取之電腦的授權狀態，VAMT 必須具有遠端電腦的系統管理權限，且必須可通過 Windows 防火牆來存取 WMI。此外，對於工作群組電腦，必須建立一個登錄機碼，以允許在 UAC 下執行遠端系統管理動作。

1. 新增 MAK：
   1. 按一下**選項**，然後按一下**管理 MAK**，以開啟**管理 MAK 金鑰**對話方塊。
   2. 按一下**新增**以輸入 MAK。
   3. 輸入 MAK，然後按一下**驗證**。

通過驗證之後，就會自動填入**版本**欄位。

* 1. 提供有意義的描述，然後按一下**新增**。

**管理 MAK 金鑰**對話方塊中現在會列出此 MAK。

* 1. 按一下**結束**以關閉對話方塊。

**注**：因為 VAMT 不是安裝在可存取網際網路的電腦上，所以**重新整理剩餘計數**選項不會有作用。此功能需要存取網際網路。

1. 在隔離的實驗室電腦上安裝 MAK：
   1. 在樹狀檢視窗格中選取「隔離的實驗室」群組。
   2. 以滑鼠右鍵按一下所選取的群組，然後按一下 **MAK 代理啟用**，以顯示 **MAK 代理啟用**對話方塊。
   3. 從**安裝 MAK** 清單中選取適當的 MAK。
   4. 選取**安裝 MAK (覆寫現有的)**。

如果此核取方塊的旁邊出現星號 (\*)，則動作只會套用至適用的電腦。例如，無法使用 MAK   
來啟用已安裝 Windows 零售版本的電腦。

* 1. 清除**從 Microsoft 取得確認識別碼**核取方塊，因為此電腦無法存取網際網路。
  2. 清除**套用確認識別碼並啟用**核取方塊，因為尚未要求確認識別碼 (CID)。
  3. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**，然後按一下**確定**。

VAMT 會顯示**正在指派產品金鑰**對話方塊，直到完成要求的動作為止。如果您選取**使用備用認證**，則在出現此對話方塊之前會提示您輸入認證。

**注**：選取**安裝 MAK (覆寫現有的)** 核取方塊會在用戶端電腦上強制安裝 MAK。請小心執行此步驟。如果 Windows Vista SP1 以前的版本已安裝在電腦上超過 30 天，則其初始寬限期已到期，如果在下次登入前未成功完成啟用，電腦會進入精簡功能模式 (RFM)。不過，只要 VAMT 主機可存取適當設定的電腦，您就可以使用 MAK 代理啟用，將這些電腦從 RFM 中復原。RFM 僅適用於 Windows Vista SP1 以前的版本。Windows Vista（含 SP1 或更高版本）、Windows 7、Windows Server 2008 或   
Windows Server 2008 R2 不會進入 RFM。

1. 儲存 CIL：

在此步驟中，完整 CIL 會儲存在本機（即工作群組）VAMT 主機上。執行 MAK 代理啟用時，必須保留此檔案，因為 VAMT 會使用它將 CID 套用至適當的電腦。

* 1. 使用 VAMT 樹狀檢視或清單檢視窗格，選取已成功接收 MAK 的群組或個別電腦。
  2. 從**檔案**功能表中，按一下**儲存檔案**，以顯示**儲存電腦資訊清單**對話方塊。
  3. 選取目錄，然後輸入 CIL 檔案名稱，例如 *IsolatedLabGroup.CIL*。
  4. 按一下**儲存**。

1. 匯出 CIL：

如先前所述，企業的安全性原則指出不可從隔離的實驗室往外傳輸任何可識別特定電腦或使用者的資訊。因此，必須從 CIL 檔案中排除這種資料，才能傳輸至核心網路 VAMT 主機。

* 1. 使用 VAMT 樹狀檢視或清單檢視窗格，選取已成功接收 MAK 的群組或個別電腦。
  2. 以滑鼠右鍵按一下所選取的群組或電腦，然後按一下**匯出電腦**，以顯示**儲存電腦資訊清單**對話方塊。
  3. 選取**排除任何敏感性環境資料**。
  4. 按一下**瀏覽**，以顯示**另存新檔**對話方塊。
  5. 選取目錄，然後輸入 CIL 檔案名稱，例如 *IsolatedLabGroupSecureExport.CIL*。
  6. 按一下**儲存**。
  7. 將 IsolatedLabGroupSecureExport.CIL 檔案複製到卸除式媒體（磁碟機、CD/DVD 或 USB 快閃磁碟機 [UFD]）。

**注**：選取**排除任何敏感性環境資料**核取方塊就不會在 CIL 中儲存個人識別資訊 (PII)。因此，必須在此 VAMT   
主機中重新匯入 CIL 並匯入至完整儲存的 CIL 檔案中，如此一來，向 Microsoft 要求的 CID 才能正確指派給隔離的實驗室群組中的電腦。

1. 在可存取網際網路的 VAMT 主機上匯入 CIL：
   1. 將卸除式媒體中的 IsolatedLabGroupSecureExport.CIL 複製到可存取網際網路的 VAMT 主機上的磁碟機。
   2. 開啟 VAMT 主控台。
   3. 從**檔案**功能表中，按一下**匯入**，以開啟**開啟電腦資訊清單**對話方塊。
   4. 尋找並選取 **IsolatedLabGroupSecureExport.CIL**，然後按一下**開啟**，將 CIL 載入至 VAMT 中。
   5. 確認沒有看到電腦、群組及工作群組名稱。
2. 向 Microsoft 要求 CID：
   1. 以滑鼠右鍵按一下已匯入的電腦，然後按一下 **MAK 代理啟用**，以開啟 **MAK 代理啟用**對話方塊。
   2. 清除**安裝 MAK (覆寫現有的)** 核取方塊。
   3. 清除**從 Microsoft 取得確認識別碼**核取方塊。
   4. 清除**套用確認識別碼並啟用**核取方塊，因為此 VAMT 主機與選取的電腦不是位於相同的網路。
   5. 按一下**確定**。

VAMT 在聯繫 Microsoft 來收集 CID 時，會顯示**正在線上取得確認識別碼**對話方塊。

1. 從連接網際網路的 VAMT 主機匯出 CIL：
   1. 抓取所有電腦的 CID 之後，儲存 CIL 檔案。在 VAMT 主控台，向右捲動並確認 **PendingCID** 欄位有值。
   2. 從**檔案**功能表中，按一下**另存新檔**，並提供檔案的新名稱，例如 *IsolatedLabGroupSecureExportwithCID.CIL*。
   3. 將更新的檔案 IsolatedLabGroupSecureExportwithCID.CIL 複製到卸除式媒體（磁碟機、CD/DVD 或 UFD）。
2. 在隔離的實驗室內的原始 VAMT 主機上匯入 CIL：
   1. 將卸除式媒體中的 IsolatedLabGroupSecureExportwithCID.CIL 複製到隔離的實驗室中的 VAMT 主機上的磁碟機。
   2. 開啟 VAMT 主控台。
   3. 從**檔案**功能表中，按一下**開啟舊檔**，以顯示**開啟電腦資訊清單**對話方塊。
   4. 尋找並選取 IsolatedLabGroup.CIL，然後按一下**開啟**，將 CIL 載入至 VAMT 中。

這會在電腦清單檢視窗格中顯示先前探索到的電腦及其授權狀態。

* 1. 從**檔案**功能表中，按一下**匯入**，並瀏覽至含有 CID 的檔案 (IsolatedLabGroupSecureExportwithCID.CIL)。

這樣會啟動合併程序，以比對 CID 與電腦的 IID。

* 1. 從**檔案**功能表中，按一下**儲存檔案**，然後輸入檔案名稱，例如 *IsolatedLabGroupwithCID.CIL*，以儲存此檔案，此檔案將 IID 與對應的 CID 產生  
     關聯。

**重要**：為了對案例重新進行映像處理，必須儲存此檔案。強烈建議您備份此檔案，並防止覆寫。

1. 套用 CID，並啟用隔離的實驗室電腦：
   1. 在樹狀檢視窗格中以滑鼠右鍵按一下隔離的實驗室群組，然後按一下 **MAK 代理啟用**，以開啟 **MAK 代理啟用**對話方塊。
   2. 清除**安裝 MAK (覆寫現有的)** 核取方塊，因為所選取的電腦已安裝 MAK。
   3. 清除**從 Microsoft 取得確認識別碼**核取方塊。
   4. 選取**套用確認識別碼並啟用**核取方塊，以指示 VAMT 安裝所選取之電腦的 CID，以啟用所選取的電腦。
   5. 按一下**確定**。

VAMT 在選取的電腦上安裝 CID 時，會顯示**正在指派確認識別碼**對話方塊。

1. 選擇性地，重新啟用隔離的實驗室中已重新進行映像處理的電腦：

如果隔離的實驗室中的電腦已重新進行映像處理，但基本的硬體沒有變動，VAMT 可以使用 IsolatedLabGroupwithCID.CIL 檔案重新啟用這些電腦。

* 1. 使用先前相同的電腦名稱，將 Windows 重新部署至每一部電腦。
  2. 在本機（工作群組）VAMT 主機上開啟 VAMT 主控台。
  3. 從**檔案**功能表中，按一下**開啟舊檔**，然後選取 IsolatedLabGroupwithCID.CIL 檔案。
  4. 在樹狀檢視窗格中，以滑鼠右鍵按一下**隔離的實驗室**群組，然後按一下**重新套用確認識別碼**，以顯示 **MAK 代理重新啟用**對話方塊。
  5. 保持選取**安裝 MAK (覆寫現有的)** 核取方塊，並確定從清單中選取先前使用的 MAK。
  6. 保留選取**重新套用確認識別碼並重新啟用**核取方塊，以從 IsolatedLabGroupwithCID.CIL 檔案中重新套用已儲存的 CID。
  7. 如果自從初始 MAK 代理啟用之後硬體沒有變動，且您使用相同的 MAK 來重新啟用電腦，請保持選取**需要 IID 完全相符**核取方塊。

如果硬體已變更，但您仍想要讓 VAMT 使用先前儲存的 CID 來嘗試重新啟用，請清除此核取方塊。請注意，在此情況中，可能無法成功重新啟用 Windows。

* 1. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**核取方塊。
  2. 按一下**確定**。

VAMT 在將 MAK 套用隔離的實驗室群組時，會顯示**正在指派產品金鑰**對話方塊。

VAMT 在選取的電腦上安裝 CID 時，會顯示**正在指派確認識別碼**對話方塊。

**注：**選取**安裝 MAK (覆寫現有的)** 核取方塊會強制安裝 MAK。請小心執行此步驟。如果 Windows Vista SP1 以前的版本已安裝超過 30 天，則其初始寬限期已到期，如果在下次登入前未成功完成啟用，它會進入 RFM。只要可透過網路存取適當設定的遠端電腦，就可以使用 VAMT 將這些電腦從 RFM 中復原。RFM 僅適用於 Windows Vista SP1 以前的版本。Windows Vista（含 SP1 或更高版本）、Windows 7、Windows Server 2008 及 Windows Server 2008 R2 不會進入 RFM。

### VAMT 對於 KMS 啟用的支援

在本案例中，使用 VAMT 在核心網路電腦或隔離的實驗室電腦上安裝和啟用 KMS 用戶端金鑰。下列描述的程序假設已安裝 VAMT，且電腦已新增至 CIL。案例 1（核心網路）或案例 2（隔離的實驗室工作群組）的步驟 1–4 中描述這些工作。

1. 開啟 VAMT 主控台。
2. 在樹狀檢視窗格中按一下群組，或在清單檢視窗格中選取個別電腦，以選取要啟用的電腦。
3. 以滑鼠右鍵按一下所選取的群組或電腦，然後按一下**設定 KMS 啟用**，以顯示 **KMS 設定**對話方塊。
4. 選取**安裝 KMS 用戶端金鑰 (覆寫現有的)**，以指示 VAMT 在用戶端電腦上安裝 KMS 用戶端  
   金鑰。
5. 選取適當的啟用選項：

* **使用 DNS 自動探索 KMS 主機。**VAMT 先清除目標電腦上先前已設定的任何 KMS 主機，然後指示電腦查詢 DNS 來尋找 KMS 主機並嘗試啟用。
* **使用特定的 KMS 主機和連接埠。**VAMT 在目標電腦上設定指定的 KMS 主機名稱和連接埠，然後指示電腦使用特定的 KMS 主機來嘗試啟用。

1. 如果您啟用的電腦所需的系統管理員認證不是您目前所使用的認證，請選取**使用備用認證**核取方塊，然後按一下**確定**。

VAMT 會顯示**正在指派產品金鑰**對話方塊，接著顯示**正在啟用電腦**對話方塊，直到完成要求的動作為止。如果您選取**使用備用認證**核取方塊，則在出現這些對話方塊之前會提示您輸入認證。

### 將 KMS 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

您可以在最初安裝 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>)。

**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

您可以使用「控制台」「系統」項目或執行 Slmgr.vbs 指令碼，以設定 Windows 7 和 Windows Server 2008 R2 大量授權版本來使用 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。

如果使用者使用使用者介面 (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。使用者  
可以使用 **Slmgr.vbs /ato**，以透過網際網路來手動啟用 MAK。

# KMS 主機金鑰與產品的對照

表 7 描述每一部 KMS 主機可以啟用的產品。

表 7. KMS 主機金鑰與其啟用之產品的對照

| **大量授權產品群組** | **Windows 產品** | **金鑰 類型** | **金鑰類型所啟用的產品** |
| --- | --- | --- | --- |
| Windows Vista | Windows Vista Business  Windows Vista Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise |
| Windows 7 | Windows 7 Professional  Windows 7 Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise  Windows 7 Professional  Windows 7 Enterprise |
| Windows Server 2008 R2  伺服器群組 A： | Windows Web Server® 2008 R2  Windows Server 2008 R2 HPC Edition  Windows HPC Server 2008 R2 | KMS\_A | Windows Server 2008 R2 群組 A  Windows Server 2008 群組 A  Windows Vista 大量 授權版本  Windows 7 大量授權 版本 |
| Windows Server 2008 R2  伺服器群組 B | Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise | KMS\_B | Windows Server 2008 R2 群組 A  Windows Server 2008 群組 A  Windows Server 2008 R2 群組 B  Windows Server 2008 群組 B  Windows Vista 大量 授權版本  Windows 7 大量授權 版本 |
| Windows Server 2008 R2  伺服器群組 C | Windows Server 2008 R2 Datacenter  Itanium 型系統適用的 Windows Server 2008 R2 | KMS\_C | Windows Server 2008 R2 群組 A  Windows Server 2008 群組 A  Windows Server 2008 R2 群組 B  Windows Server 2008 群組 B  Windows Server 2008 R2 群組 C  Windows Server 2008 群組 C  Windows Vista 大量 授權版本  Windows 7 大量授權 版本 |
| Windows Server 2008 R2 KMS 金鑰所採用的階層（群組 A、B、C）與 Windows Server 2008 相同，另外再加上 Windows Server 2008 Datacenter（不含 Hyper-V™）、Windows Server  2008 Enterprise（不含 Hyper-V）及 Windows Server 2008 Standard（不含 Hyper-V）。主要差別在於 Windows Server 2008 R2 KMS 金鑰可用來啟用 KMS 主機，再由主機啟用 Windows Server 2008、Windows 7 及 Windows Vista。  Windows Server 2008 和 Windows Vista 金鑰無法啟用 Windows 7 或  Windows Server 2008 R2 系統。 | | | |

# 啟用原則值

表 8 列出 Windows 7 和 Windows Server 2008 R2 的原則值。

表 8. Windows 7 和 Windows Server 2008 R2 原則值

| **元素** | **用戶端值** | **伺服器值** | **範圍** |
| --- | --- | --- | --- |
| 重設授權狀態限制 | 3 | 3 | 無法設定 |
| KMS 用戶端計數臨界值 | 25 | 5 | 無法設定 |
| KMS 啟用持續時間 | 180 天 | 180 天 | 無法設定 |
| KMS 主機接聽連接埠 | 1688 | 1688 | 任何開啟的 TCP 連接埠 |
| OOB 寬限期 | 30 天 | 30 天 | 無法設定 |
| OOT 寬限期 | 30 天 | 30 天 | 無法設定 |
| KMS 用戶端重新啟用（分鐘） | 10,080 分鐘  （7 天 -  預設值） | 10,080 分鐘  （7 天 -  預設值） | 15–43,200 分鐘  （30 天 -  預設值） |
| 自動 KMS 重試間隔 - 在 KMS 啟用失敗時 發生 | 120 分鐘 | 120 分鐘 | 15–43,200 分鐘  （120 分鐘 -  預設值） |

# KMS 用戶端安裝金鑰

依預設，Windows 7 與 Windows Server 2008 R2 作業系統使用 KMS 進行啟用。進行大量授權安裝時，依預設會安裝安裝金鑰，這欄會使系統成為 KMS 用戶端。如果您將電腦從 KMS 主機、MAK 或 Windows 零售版本轉換為 KMS 用戶端，請使用 **slmgr /ipk <安裝金鑰>**，從表 9 中安裝適當的安裝金鑰 (GVLK)。

表 9. KMS 用戶端安裝金鑰

| **平台** | **作業系統版本** | **產品金鑰** |
| --- | --- | --- |
| **Windows 7 與 Windows Server 2008 R2** | | |
| 用戶端 | Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| 用戶端 | Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| 用戶端 | Windows 7 Professional E | W82YF-2Q76Y-63HXB-FGJG9-GF7QX |
| 用戶端 | Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| 用戶端 | Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| 用戶端 | Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| 伺服器 | Windows Server 2008 R2 Web | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |
| 伺服器 | Windows Server 2008 R2 HPC  版本 | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| 伺服器 | Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| 伺服器 | Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| 伺服器 | Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| 伺服器 | Itanium 型系統適用的  Windows Server 2008 R2 | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| **Windows Vista 與 Windows Server 2008** | | |
| 用戶端 | Windows Vista Business | YFKBB-PQJJV-G996G-VWGXY-2V3X8 |
| 用戶端 | Windows Vista Business N | HMBQG-8H2RH-C77VX-27R82-VMQBT |
| 用戶端 | Windows Vista Enterprise | VKK3X-68KWM-X2YGT-QR4M6-4BWMV |
| 用戶端 | Windows Vista Enterprise N | VTC42-BM838-43QHV-84HX6-XJXKV |
| 伺服器 | Windows Web Server 2008 | WYR28-R7TFJ-3X2YQ-YCY4H-M249D |
| 伺服器 | Windows Server 2008 Standard | TM24T-X9RMF-VWXK6-X8JC9-BFGM2 |
| 伺服器 | 無 Hyper-V 的 Windows Server 2008 Standard | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ |
| 伺服器 | Windows Server 2008 Enterprise | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V |
| 伺服器 | 無 Hyper-V 的 Windows Server 2008 Enterprise | 39BXF-X8Q23-P2WWT-38T2F-G3FPG |
| 伺服器 | Windows Server 2008 Datacenter | 7M67G-PC374-GR742-YH8V4-TCBY3 |
| 伺服器 | 無 Hyper-V 的 Windows Server 2008 Datacenter | 22XQ2-VRXRG-P8D42-K34TD-G3QQC |
| 伺服器 | Itanium 型系統適用的 Windows Server 2008 | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK |

# 啟用錯誤碼

表 10 針對啟用 Windows 7 和 Windows Server 2008 R2 大量授權版本作業系統時發生的問題，提供疑難排解說明。

表 10. 錯誤碼和描述

| **錯誤碼** | **錯誤訊息** | **啟用類型** | **可能原因** | **疑難排解步驟** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | 啟用伺服器判定指定的產品金鑰無效。 | MAK | 輸入的 MAK 無效 | 請確認金鑰是 Microsoft 提供的 MAK。  請聯絡[Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 啟用客服中心），以確定 MAK 有效。 |
| 0xC004C003 | 啟用伺服器判定指定的產品金鑰遭到封鎖。 | MAK | MAK 在啟用伺服器上遭到封鎖。 | 請聯絡[Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 啟用客服中心），以取得新的 MAK，並安裝/啟用系統。 |
| 0xC004C008 | 啟用伺服器判定無法使用指定的產品金鑰。 | KMS | KMS 金鑰 已超出啟用 限制。 | KMS 主機金鑰最多可以在六部不同的電腦上啟用 10 次。如果需要更多啟用，請聯絡[Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 啟用客服中心）。 |
| 0xC004C020 | 啟用伺服器回報多重啟用金鑰已超出限制。 | MAK | MAK 已超出啟用限制。 | MAK 預設有限定數量的啟用。請聯絡[Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 啟用客服中心）。 |
| 0xC004C021 | 啟用伺服器回報已超出多重啟用金鑰延伸限制。 | MAK | MAK 已超出啟用限制。 | MAK 預設有限定數量的啟用。請聯絡[Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 啟用客服中心）。 |
| 0xC004F009 | 軟體保護服務 回報寬限期已 到期。 | MAK | 在啟用系統之前，寬限期已到期。現在，系統處於通知狀態。 | 請參閱「」一節。 |
| 0xC004F00F | 軟體授權伺服器回報硬體識別碼繫結超出有效容許寬限期外。 | MAK/KMS  用戶端/KMS 主機 | 已在系統上變更硬體或更新驅動程式。 | **MAK：**在 OOT 寬限期內，使用線上或電話啟用來重新啟用系統。  **KMS：**重新啟動或執行 **slmgr.vbs / ato**。 |
| 0xC004F014 | 軟體保護服務回報無法取得產品金鑰。 | MAK/KMS 用戶端 | 未在系統上安裝產品金鑰。 | 安裝 MAK 產品金鑰，或安裝在安裝媒體的 \sources\pid.txt 中找到的 KMS 安裝金鑰。 |
| 0xC004F02C | 軟體保護服務回報離線啟用資料的格式不正確。 | MAK/KMS 用戶端 | 系統偵測到 電話啟用期 間輸入的資 料無效。 | 驗證所輸入的 CID 正確。 |
| 0xC004F035 | 此錯誤碼相當於「軟體保護服務回報無法使用大量授權產品金鑰來啟用電腦...」。這句錯誤文字雖然正確，但含糊不清。  此錯誤指出電腦的 BIOS 中遺失 Windows 標記， –在 OEM 系統上是指搭售 Windows 合格版本的電腦，而這是 KMS 用戶端啟用的必要條件。  錯誤：無效的大量授權金鑰  要啟用，您必須將產品金鑰變更為有效的多重啟用金鑰 (MAK) 或零售金鑰。  您必須有合格的作業系統授權以及大量授權的 Windows 7 升級授權，或從零售來源取得的 Windows 7 完整授權。  此軟體的任何其他安裝都違反您的合約及適用的著作權法。 | KMS 用戶端/ KMS 主機 | Windows 7 大量授權版本僅授權供升級之用。不支援在未安裝合格作業系統的電腦上安裝大量授權作業系統。 | 安裝 Microsoft 合格版本作業系統，然後使用 MAK 進行啟用。 |
| 0xC004F038 | 軟體保護服務回報無法啟用電腦。金鑰管理服務 (KMS) 所回報的計數不足。請聯絡系統管  理員。 | KMS 用戶端 | KMS 主機上的計數不足。Windows Server 的 KMS 計數必須大於或等於 5，而 Windows 用戶端的 KMS 計數必須大於或等於 25。 | KMS 集區中需要有更多電腦，KMS 用戶端才能啟用。請執行 **Slmgr.vbs /dli**，以取得 KMS 主機上的目前計數。 |
| 0xC004F039 | 軟體保護服務回報無法啟用電腦。無法啟用金鑰管理服務 (KMS)。 | KMS 用戶端 | 此錯誤是在未回覆 KMS 要求時產生。 | 對 KMS 主機與用戶端之間網路連線進行疑難排解。請確認 TCP連接埠 1688（預設值）未遭到防火牆封鎖或以其他方式篩選。 |
| 0xC004F041 | 軟體保護服務判定未啟用金鑰管理伺服器 (KMS)。需要啟用 KMS。 | KMS 用戶端 | 未啟用 KMS 主機。 | 透過線上或電話啟用來啟用 KMS 主機。 |
| 0xC004F042 | 軟體保護服務判定無法使用特定的金鑰管理服務 (KMS)。 | KMS 用戶端 | KMS 用戶端和 KMS 主機不相符。 | 當 KMS 用戶端所聯繫的 KMS 主機無法啟用用戶端軟體時，就會發生此錯誤。例如，在含有應用程式和作業系統專用的 KMS 主機的混合環境中，這種情況很常見。 |
| 0xC004F050 | 軟體保護服務 回報產品金鑰 無效。 | KMS、KMS 用戶端、MAK | 這可能是因為 KMS 金鑰輸入錯誤，或在作業系統的已發行版本中輸入 Beta 金鑰所導致。 | 在相對應的 Windows 版本上安裝適當的 KMS 金鑰。請檢查拼字。如果是複製貼上金鑰，請確認金鑰中的破折號未變成長破折號。 |
| 0xC004F051 | 軟體保護服務回報產品金鑰遭到封鎖。 | MAK/KMS | 啟用伺服器上的產品金鑰遭到 Microsoft 封鎖。 | 取得新的 MAK/KMS 金鑰，然後在系統上安裝該金鑰並進行 啟用。 |
| 0xC004F064 | 軟體保護服務回報非正版寬限期已到期。 | MAK | Windows 啟用工具 (WAT) 已判定系統不是 正版。 | 請參閱 *Volume Activation Operations Guide*（大量啟用操作 指南）。 |
| 0xC004F065 | 軟體保護服務回報應用程式正在有效的非正版期間內執行。 | MAK/KMS 用戶端 | Windows 啟用工具已判定系統不是正版。這個系統將繼續在非正版寬限期執行。 | 取得並安裝正版的產品金鑰，並在寬限期內啟用系統。否則，在寬限期結束時，系統會進入通知狀態。 |
| 0xC004F06C | 軟體保護服務 回報無法啟用電腦。金鑰管理服務 (KMS) 判定要求時間戳記 無效。 | KMS 用戶端 | 用戶端電腦的系統時間與 KMS 主機的時間大不相同。 | 基於許多原因，時間同步對於系統和網路安全性來說相當重要。將用戶端的系統時間變更為與 KMS 的時間同步，以解決這個問題。建議使用網路時間通訊協定 (NTP) 時間來源或 Active Directory 網域服務來進行時間同步化。這個問題是因為使用 UTP 時間，並且與時區選擇沒有關聯。 |
| 0x80070005 | 存取遭拒。要求的動作要求較高的權限。 | KMS 用戶端/MAK/KMS 主機 | 使用者存取控制 (UAC) 禁止在非升級的命令提示字元下執行啟用 程序。 | 從升級的命令提示字元下執行 slmgr.vbs。以滑鼠右鍵按一下 cmd.exe，然後按一下「以系統管理員身分執行」。 |
| 0x8007232A | DNS 伺服器 失敗。 | KMS 主機 | 系統出現網 路或 DNS  問題。 | 進行網路或 DNS 的疑難排解。 |
| 0x8007232B | DNS 名稱不 存在。 | KMS 用戶端 | KMS 用戶端在 DNS 中找不到 KMS SRV RR。  如果 KMS 主機不存在於網路上，則應該安裝 MAK。 | 確認已安裝 KMS 主機，且已啟用 DNS 發佈（預設值）。  如果 DNS 無法使用，請使用 **slmgr.vbs / skms <*kms 主機名稱>***，讓 KMS 用戶端指向 KMS  主機。  選擇性地取得並安 裝 MAK，然後啟用系統。  最後，進行 DNS 疑難排解。 |
| 0x800706BA | 無法使用RPC 伺服器。 | KMS 用戶端 | KMS 主機上未設定防火牆設定，或 DNS SRV 記錄已過期。 | 請確定 KMS 主機電腦上已啟用金鑰管理服務防火牆例外。  請確定 SRV 記錄指向有效的 KMS 主機。  進行網路連接的疑難排解。 |
| 0x8007251D | 找不到 DNS 查詢的記錄。 | KMS 用戶端 | KMS 用戶端在 DNS 中找不到 KMS SRV RR。 | 進行網路連接和 DNS 的疑難排解。 |
| 0xC004F074 | 軟體保護服務回報無法啟用電腦。無法聯繫金鑰管理服務 (KMS)。如需其他資訊，請參閱應用程式事件記錄檔。 | KMS 用戶端 | 所有 KMS 主機系統都傳回錯誤。 | 根據與啟用嘗試相關聯的每一個事件識別碼 12288，進行錯誤疑難排解。 |

# Windows 事件記錄檔

表 11 列出 KMS 在 Windows 事件記錄檔中記錄的事件。以下描述每一個事件的一般資料：

* **所有事件的記錄檔名稱 (12290 除外)：**Windows 記錄\應用程式
* **記錄檔名稱 12290：**應用程式及服務記錄檔\金鑰管理服務
* **事件提供者名稱：**Microsoft-Windows-Security-Licensing-SLC
* **來源名稱：**軟體保護服務

表 11. Windows 事件記錄檔中記錄的 KMS 事件

| **事件 識別碼** | **記錄者** | **描述** | **訊息** | **參數**  **逗號分隔字串中包含的欄位** | | **範例** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **名稱** | **描述** |  |
| 12288 | 用戶端 | 要求產生失敗或在 RPC 提交之後  (用戶端) | 用戶端已經將啟用要求傳送至金鑰管理服務電腦。%n資訊：%n%1 | HRESULT | 傳回碼 | 0x0 |
|  | | | | Status | 旗標 (備註 1) | 0x8 |
| Server: Port | 名稱：連接埠 | kms01.contoso.com:1688 |
| CMID | 用戶端電腦 識別碼 | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be, |
| Client Time | 要求時間戳記 | 2006/1/14 2:30, |
| VM Info | 未使用 | 1 |
| Licensing Status | 授權狀態  0 – 未授權  1 - 已授權  (已啟用)  2 – OOB 寬限期  3 – OOT 寬限期  4 – 非正版寬限期  5 – 通知  6 – 延長的寬限期 | 2 |
|  | | | | Time to Expiration | 剩餘時間 (分鐘) | 40123 |
| ActID | 啟用識別碼 – 識別授權 | cf67834d-db4a-402c-ab1f-2c134f02b700, |
| N-Policy | 需要啟用的最小用戶端計數 | 25 |
| 12289 | 用戶端 | 在 KMS 回應驗證後  (用戶端) | 用戶端已經處理金鑰管理服務電腦發出的啟用回應。%n資訊：%n%1 | HRESULT | 傳回碼 | 0x0 |
|  | | | | Status | 旗標 (備註 1) | 0x4000008 |
| fBound | 已啟用的旗標 | 0 |
| Unused | 未使用 – 忽略 | 0 |
| Count | KMS 目前計數 | 4 |
| Activation Interval | 未啟用時的要求間隔 (分鐘) | 120 |
| Renewal Interval | 啟用時的要求間隔 (分鐘) | 10080 |
| Client Time | 要求時間戳記 | 1/14/2006 2:30 |
| 12290 | KMS | 每個要求的 KMS 伺服器端記錄檔 | 已處理啟用要求。%n資訊：%n%1 | HRESULT | 傳回碼 | 0x0 |
|  | | | | N-Policy | 需要啟用的最小用戶端產品計數 | 25 |
| Machine | 用戶端電腦名稱 | kms03.site5.contoso.com |
| CMID | 用戶端電腦 識別碼 | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | Client Time | 要求時間戳記 | 2006/1/14 22:36 |
| VM Info | 用戶端作業系統正執行於虛擬電腦中 | 1 |
| Licensing Status | 授權狀態  0 – 未授權  1 - 已授權  (已啟用)  2 – OOB 寬限期  3 – OOT 寬限期  4 – 非正版寬限期  5 – 通知  6 – 延長的寬限期 | 2 |
| Time to Expiration | 剩餘時間 (分鐘) | 40123 |
| ActID | 啟用識別碼 –  識別授權 | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | KMS 初始化失敗 | 大量授權用戶端無法初始化金鑰管理服務更新計時器。%n資訊：%n%1 | HRESULT | 傳回碼 |  |
| 12292 | KMS | 更新計時器初始化失敗 | 金鑰管理服務 (KMS) 無法初始化更新計時器。%n資訊：%n%1 | HRESULT | 傳回碼 |  |
| 12293 | KMS | DNS RR 發佈失敗 | 無法將金鑰管理服務 (KMS) 發佈至「%2」網域中的 DNS。%n資訊：%n%1 | P1：HRESULT  P2：DNS domain | P1：傳回碼  P2：DNS 網域名稱 | |
| 12294 | KMS | DNS RR 發佈成功 | 順利將金鑰管理服務 (KMS) 發發佈至「%1」網域中的 DNS。%n | DNS domain | DNS 網域名稱 |  |

# WMI 屬性和方法

表 12 列出軟體保護平台的 WMI 屬性和方法。軟體保護平台的屬性是在檔案 %WinDir%\System32\wbem\sppwmi.mof 中定義。

表 12. 軟體保護平台 WMI 屬性和方法

|  |  |
| --- | --- |
| **//屬性 SoftwareLicensingService 類別** | |
| **Version** | 軟體保護服務的版本 |
| **KeyManagementServiceMachine** | KMS 主機的名稱。如果未呼叫 **SetKeyManagementServiceMachine**，則傳回 Null。 |
| **KeyManagementServicePort** | 用戶端用來傳送 KMS 啟用要求的 TCP 連接埠。如果未呼叫 **SetKeyManagementServicePort**，則傳回 **0**。 |
| **IsKeyManagementServiceMachine** | 指出電腦上是否已啟用 KMS：**0** 表示未啟用，**1** 表示已啟用。 |
| **VLActivationInterval** | 在授權用戶端之前，用戶端多久聯繫一次 KMS 主機的頻率，以分鐘為單位。 |
| **VLRenewalInterval** | 在授權用戶端之後，用戶端多久聯繫一次 KMS 主機的頻率，以分鐘為單位。 |
| **KeyManagementServiceCurrentCount** | KMS 主機上目前使用中的 KMS 用戶端數量。**-1** 表示主機未啟用作為 KMS，或尚未收到任何用戶端授權要求。 |
| **RequiredClientCount** | 需要連接至 KMS 主機以啟用大量授權的最小用戶端數量。 |
| **PolicyCacheRefreshRequired** | 指出是否需要更新授權原則快取：**0**=不需要，**1**=需要重新 整理。 |
| **ClientMachineID** | 用於向 KMS 主機識別 KMS  用戶端的全域唯一識別碼 (GUID)。用戶端在其傳送給 KMS 的要求中會包含此識 別碼。 |
| **RemainingWindowsReArmCount** | 用戶端可成功重設授權狀態的剩餘次數。 |
| **KeyManagementServiceListeningPort** | KMS 主機用來接聽啟用要求的 TCP 連接埠。 |
| **KeyManagementServiceDnsPublishing** | 指出 KMS 主機的 DNS 發佈狀態：**0**=已停用，**1**=已啟用自動發佈（預設值）。 |
| **KeyManagementServiceLowPriority** | 指出 KMS 服務的執行緒優先順序狀態：**0**=一般優先順序（預設值），**1**=低優先順序。 |
| **KeyManagementServiceHostCaching** | 指出 KMS 主機名稱和連接埠的快取狀態：**0**=已停用快取，**1**=已啟用快取（預設值）。 |
| **KeyManagementServiceUnlicensedRequests** | 用戶端發出的授權狀態為 0（未授權）的 KMS 要求數量。 |
| **KeyManagementServiceLicensedRequests** | 用戶端發出的授權狀態為 1（已授權）的 KMS 要求數量。 |
| **KeyManagementServiceOOBGraceRequests** | 用戶端發出的授權狀態為 2（OOB 寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceOOTGraceRequests** | 用戶端發出的授權狀態為 3（OOT 寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceNonGenuineGraceRequests** | 用戶端發出的授權狀態為 4 （非正版寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceNotificationRequests** | 用戶端發出的授權狀態為 5（通知）的 KMS 要求數量。 |
| **KeyManagementServiceTotalRequests** | 有效 KMS 要求的總計數。 |
| **KeyManagementServiceFailedRequests** | 無效 KMS 要求的數量。 |
| **KeyManagementServiceActivationDisabled** | 指出是否停用透過 KMS 進行大量啟用。 |
| **//方法 SoftwareLicensingProduct 類別** | |
| **InstallProductKey** | 安裝產品金鑰。 |
| **InstallLicense** | 安裝授權。 |
| **InstallLicensePackage** | 安裝目前產品的授權封裝。 |
| **SetKeyManagementServiceMachine** | 設定用於大量啟用的 KMS 主機名稱。 |
| **ClearKeyManagementServiceMachine** | 清除先前已設定的任何 KMS 主機名稱。 |
| **SetKeyManagementServicePort** | 設定供用戶端用來提出 KMS 主機要求的 TCP 連接埠。如果未指定，則使用連接埠 1688。 |
| **ClearKeyManagementServicePort** | 清除先前已指定的任何連接埠 號碼。 |
| **SetVLActivationInterval** | 在 KMS 用戶端變成已授權之前，KMS 用戶端多久聯繫一次 KMS 主機的啟用頻率，以分鐘為單位。此頻率必須大於或等於 15 且小於或等於 43,200。如果呼叫此方法但電腦不是 KMS，則傳回錯誤。 |
| **SetVLRenewalInterval** | 在 KMS 用戶端變成已授權之後，KMS 用戶端多久聯繫一次 KMS 主機的更新頻率，以分鐘為單位。此頻率必須大於或等於 15 且小於或等於 43,200。如果呼叫此方法但電腦不是 KMS，則傳回錯誤。 |
| **ClearProductKeyFromRegistry** | 清除登錄中的產品金鑰。 |
| **AcquireGenuineTicket** | 執行線上正版產品驗證。呼叫 此方法可能會變更電腦的正版 狀態。 |
| **ReArmWindows** | 將電腦的授權狀態重設為 OOB 寬限期（請參閱 **LicenseStatus**）。  **注**：您必須重新啟動用戶端，變更才會生效。 |
| **RefreshLicenseStatus** | 更新 Windows 的授權狀態，以使應用程式能夠存取最新的授權資訊。 |
| **SetKeyManagementServiceListeningPort** | 設定供 KMS 主機用來接聽啟用要求的 TCP 連接埠。僅適用於 KMS 主機。如果未指定，則使用連接埠 1688。 |
| **ClearKeyManagementServiceListeningPort** | 清除先前已指定的任何接聽連接埠。僅適用於 KMS 主機。 |
| **DisableKeyManagementServiceDnsPublishing** | 啟用/停用 KMS 主機電腦上 的 DNS 發佈：**0**=啟用， **1**=停用。 |
| **EnableKeyManagementServiceLowPriority** | 啟用/停用以低優先順序執行的 KMS 服務：**0**=停用，**1**=啟用。 |
| **DisableKeyManagementServiceHostCaching** | 啟用/停用在大量啟用的用戶端電腦上快取 KMS 主機名稱和連接埠：**0**=啟用，**1**=停用。 |
| **DisableKeyManagementServiceActivation** | 啟用/停用透過 KMS 電腦進行大量啟用：**0**=啟用，**1**=停用。 |
| **DiscoveredKeyManagementServiceMachineName** | 上次透過 DNS 探索到的 KMS 主機名稱。 |
| **DiscoveredKeyManagementServiceMachinePort** | 上次透過 DNS 探索到的 KMS 主機連接埠。 |
| **//屬性 SoftwareLicensingService 類別** | |
| **ID** | 產品識別碼 |
| **名稱** | 產品名稱 |
| **描述** | 產品說明 |
| **ApplicationID** | 目前產品之應用程式的識別碼 |
| **ProcessorURL** | 處理程序憑證的軟體授權伺服器 URL |
| **MachineURL** | 繫結憑證的軟體授權伺服器 URL |
| **ProductKeyURL** | 產品憑證的軟體授權伺服器 URL |
| **UseLicenseURL** | 使用者授權的軟體授權伺服器 URL |
| **LicenseStatus** | 此產品之應用程式的授權狀態：  **0**=未授權， **1**=已授權， **2**=OOB 寬限期， **3**=OOT 寬限期， **4**=非正版寬限期， **5**=通知， **6**=延長的寬限期 |
| **LicenseStatusReason** | 指出電腦為何處於特定授權狀態的診斷碼。 |
| **GracePeriodRemaining** | 上層應用程式進入通知模式之前的剩餘時間，以分鐘為單位。對於大量授權用戶端來說，這是要求重新啟用之前的剩餘時間。 |
| **EvaluationEndDate** | 此產品之應用程式的到期日。超過此日期之後，**LicenseStatus** 會變成**未授權**，且無法啟用。 |
| **OfflineInstallationId** | 此產品之應用程式的識別碼，可用於電話啟用或離線啟用。如果未安裝產品金鑰，則傳回 Null。 |
| **PartialProductKey** | 此產品金鑰的最後五個字元。如果未安裝產品金鑰，則傳回 Null。 |
| **ProductKeyID** | 產品金鑰識別碼。如果未安裝產品金鑰，則傳回 Null。 |
| **LicenseFamily** | SKU 的系列識別碼，可用於決定附加元件的授權關聯。 |
| **LicenseDependsOn** | SKU 系列的相依性識別碼，可用於決定附加元件的授權關聯。 |
| **LicenseIsAddon** | 如果產品視為附加元件授權，則傳回 **True**。 |
| **VLActivationInterval** | 在授權產品之前，用戶端多久聯繫一次 KMS 主機的頻率，以分鐘為單位。 |
| **VLRenewalInterval** | 在授權產品之後，用戶端多久聯繫一次 KMS 主機的頻率，以分鐘為單位。 |
| **KeyManagementServiceProductKeyID** | KMS 產品金鑰識別碼。如果不適用，則傳回 Null。 |
| **KeyManagementServiceMachine** | KMS 主機的名稱。如果未呼叫 **SetKeyManagementServiceMachine**，則傳回 Null。 |
| **KeyManagementServicePort** | 用戶端用來傳送 KMS 啟用要求的 TCP 連接埠。如果未呼叫 **SetKeyManagementServicePort**，則傳回 **0**。 |
| **DiscoveredKeyManagementServiceMachineName** | 上次透過 DNS 探索到的 KMS 主機名稱。 |
| **DiscoveredKeyManagementServiceMachinePort** | 上次透過 DNS 探索到的 KMS 主機連接埠。 |
| **IsKeyManagementServiceMachine** | 指出電腦上是否已啟用 KMS：**1** 表示已啟用，**0** 表示未啟用。 |
| **KeyManagementServiceCurrentCount** | KMS 主機上目前使用中的 KMS 用戶端數量。**-1** 表示電腦未啟用作為 KMS，或尚未收到任何用戶端授權要求。 |
| **RequiredClientCount** | 需要連接至 KMS 主機以啟用大量授權的最小用戶端數量。 |
| **KeyManagementServiceUnlicensedRequests** | 用戶端發出的授權狀態為 0（未授權）的 KMS 要求數量。 |
| **KeyManagementServiceLicensedRequests** | 用戶端發出的授權狀態為 1（已授權）的 KMS 要求數量。 |
| **KeyManagementServiceOOBGraceRequests** | 用戶端發出的授權狀態為 2（OOB 寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceOOTGraceRequests** | 用戶端發出的授權狀態為 3（OOT 寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceNonGenuineGraceRequests** | 用戶端發出的授權狀態為 4 （非正版寬限期）的 KMS 要求數量。 |
| **KeyManagementServiceTotalRequests** | 有效 KMS 要求的總計數。 |
| **KeyManagementServiceFailedRequests** | 失敗的 KMS 要求的數量。 |
| **KeyManagementServiceNotificationRequests** | 用戶端發出的授權狀態為 5（通知）的 KMS 要求數量。 |
| **GenuineStatus** | 此產品之應用程式的正版狀態。 |
| **ExtendedGrace** | 上層應用程式變成未授權狀態之前已延長的寬限期，以分鐘為 單位。 |
| **TrustedTime** | 顯示系統中目前儲存的信任時間。 |
| **DisableKeyManagementServiceHostCaching** | 啟用/停用在大量啟用的用戶端電腦上快取 KMS 主機名稱和連接埠：0=啟用，1=停用。 |
| **//方法 SoftwareLicensingProduct 類別** | |
| **UninstallProductKey** | 解除安裝目前產品的產品金鑰。 |
| **啟用** | 啟用目前產品。 |
| **DepositOfflineConfirmationId** | 執行電話啟用或離線啟用時，為產品儲放一個離線確認識別碼，以啟用此產品。 |
| **GetPolicyInformationDWord** | 取得 DWORD 類型的授權原則資訊。 |
| **GetPolicyInformationString** | 取得字串類型的原則資訊。 |
| **SetKeyManagementServiceMachine** | 設定用於大量啟用的 KMS 主機名稱。 |
| **ClearKeyManagementServiceMachine** | 清除先前已設定的任何 KMS 主機名稱。 |
| **SetKeyManagementServicePort** | 設定供用戶端用來提出 KMS 主機要求的 TCP 連接埠。如果未指定，則使用連接埠 1688。 |
| **ClearKeyManagementServicePort** | 清除先前已指定的任何連接埠 號碼。 |

# 詞彙

|  |  |
| --- | --- |
| **術語** | **定義** |
| **ACID** | 在軟體版本內用來識別啟用方法的 GUID。 |
| **AD DS** | Active Directory 網域服務。 |
| **AppID** | 定義用來組合一組 SKU ID 的 GUID，如同姓氏一樣。所有 Windows 版本具有相同的 AppID。 |
| **DNS** | 網域名稱服務。 |
| **FQDN** | 完整網域名稱（例如，phred.microsoft.com）。 |
| **GVLK** | 一般大量授權金鑰，為版本特定的產品金鑰，依預設會安裝在 Windows 的所有大量授權版本中。亦稱為預設 KMS 用戶端安裝金鑰。如需詳細資訊，請參閱表 9。 |
| **KMS** | 金鑰管理服務。 |
| **KMSID** | KMS 用戶端傳送給 KMS 主機進行啟用的 GUID 可以在多個 ACID 之間 共用。 |
| **電腦憑證存放區** | 嘗試執行權杖型啟用的使用者，必須能夠存取此憑證及其私密金鑰。 |
| **MAK** | 多重啟用金鑰。 |
| **N-Policy** | 授權原則，指定 KMS 傳回的電腦最小計數，供用戶端用來判定是否自行啟用。 |
| **PIN** | 個人識別碼，搭配智慧卡一起使用作為驗證認證。 |
| **SKU** | 描述 Windows 或其他軟體的特定版本。 |
| **SKUId** | 同上述 ACID |
| **SPPSVC** | 軟體保護服務，為 Windows 7 和 Windows Server 2008 R2 內建立的服務平台，負責管理 Windows 及其他應用程式的授權活動。 |
| **SRV** | DNS 中支援的一種資源記錄（請參閱要求建議 [RFC] 2782） |
| **權杖** | x509 憑證及其相關聯的私密金鑰可在允許進行權杖型啟用的電腦上用來啟用 Windows。 |
| **VL** | 大量授權。 |
| **WMI** | Windows Management Instrumentation。 |

# 資源連結

* 大量啟用：
* TechNet 上的大量啟用：<http://go.microsoft.com/fwlink/?LinkId=150083>
* Key Management Service 1.2 for Windows Server 2003 SP1 and Later（適用於 Windows Server 2003 SP1 及更高版本的金鑰管理服務 1.2）：  
  <http://go.microsoft.com/fwlink/?LinkId=155083>
* Product Activation and Key Information（產品啟用和金鑰資訊）：  
  <http://go.microsoft.com/fwlink/?LinkId=74008>
* Volume Activation Deployment Guide（大量啟用部署指南）：<http://go.microsoft.com/fwlink/?LinkId=150083>
* Volume Activation Operations Guide（大量啟用操作指南）：<http://go.microsoft.com/fwlink/?LinkId=150084>
* Volume Activation Deployment Guide（大量啟用部署指南）：<http://go.microsoft.com/fwlink/?LinkId=155926>
* Volume Activation Technical Reference Guide（大量啟用技術參考指南）：<http://go.microsoft.com/fwlink/?LinkId=152550>
* 部署工具：
* Windows Automated Installation Kit (AIK) for Windows 7（適用于 Windows 7 的 Windows 自動安裝套件 (AIK) ）：  
  <http://go.microsoft.com/fwlink/?LinkId=136976>
* 管理工具：
* System Center Pack Catalog（系統中心組件目錄）：  
  <http://go.microsoft.com/fwlink/?LinkID=110332>
* 大量授權：
* Genuine Microsoft Software（正版 Microsoft 軟體）：  
  <http://go.microsoft.com/fwlink/?LinkId=151993>
* 正版 Microsoft 軟體驗證網頁：<http://go.microsoft.com/fwlink/?LinkId=64187>
* Microsoft Activation Centers Worldwide Telephone Numbers（Microsoft 全球啟用中心電話號碼）：<http://go.microsoft.com/fwlink/?LinkId=107418>
* Microsoft Volume Licensing（Microsoft 大量授權）：  
  <http://go.microsoft.com/fwlink/?LinkId=73076>
* Microsoft 大量授權服務中心：<http://go.microsoft.com/fwlink/?LinkId=107544>
* Windows Vista Privacy Notice Highlights（Windows Vista 隱私權注意事項醒目提示）：  
  <http://go.microsoft.com/fwlink/?LinkID=52526>