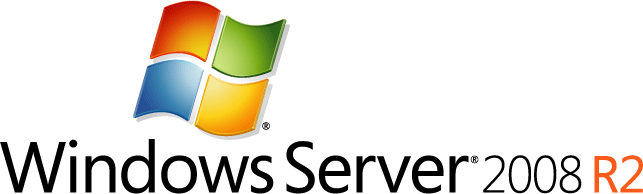
****

**  
  
Guía de referencia técnica de Volume Activation**

**Windows 7 y Windows Server 2008 R2**

Microsoft Corporation

Fecha de publicación: julio de 2009

Resumen

Esta guía de referencia está dirigida a los implementadores de tecnología de la información (TI) cuyas organizaciones planean implementar versiones de Volume Activation de los sistemas operativos Windows® 7 y Windows Server® 2008 R2. Acompaña a la *Guía de planificación de Volume Activation*, a la *Guía de implementación de Volume Activation* y a la *Guía de operaciones de Volume Activation*.

Este documento y cualquier otro documento aquí mencionado se proporcionan solo con fines informativos, y Microsoft no establecerá ninguna garantía, expresa o implícita, en este documento. La información de este documento, incluidas las referencias a direcciones URL y a otros sitios web de Internet, está sujeta a cambios sin previo aviso. El usuario será el único responsable del uso o de las consecuencias derivadas del uso que haga de este documento. A menos que se especifique lo contrario, las empresas, las organizaciones, los productos, los nombres de dominio, las direcciones de correo electrónico, los logotipos, las personas, los lugares y los acontecimientos que se describen aquí a modo de ejemplo son ficticios. No se pretende indicar ni debe deducirse ninguna asociación con compañías, organizaciones, productos, nombres de dominio, direcciones de correo electrónico, logotipos, personas, lugares o acontecimientos reales. El usuario tendrá la responsabilidad de cumplir todas las leyes de derecho de autor aplicables. Sin limitar los derechos de autor aplicables, ninguna parte de este documento se podrá reproducir, almacenar o insertar en un sistema de recuperación, ni transmitir de ninguna forma, por ningún medio (electrónico, mecánico, mediante fotocopias o grabación, o de cualquier otro tipo) o propósito, sin la previa autorización expresa por escrito de Microsoft Corporation.

Microsoft puede ser titular de patentes, solicitudes de patentes, marcas, derechos de autor u otros derechos de propiedad intelectual sobre el contenido de este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual, a menos que se prevea en un contrato por escrito de licencia de Microsoft.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Hyper-V, Windows, Windows Server y Windows Vista son marcas registradas del grupo de empresas de Microsoft.

Los nombres de empresas y productos reales mencionados aquí pueden ser marcas comerciales de sus respectivos propietarios.

**Contenido**

[Introducción 1](#_Toc237084655)

[Experiencia del usuario 2](#_Toc237084656)

[Opciones de Slmgr.vbs 6](#_Toc237084657)

[Configuración del Registro 14](#_Toc237084658)

[Configuración del objeto de directivas de grupo 18](#_Toc237084659)

[Intervalo de activación de KMS 20](#_Toc237084660)

[Orden de búsqueda de detección de KMS 22](#_Toc237084661)

[Escenarios de activación 23](#_Toc237084662)

[Escenarios de KMS 23](#_Toc237084663)

[Implementación predeterminada de KMS para redes de un único sitio 23](#_Toc237084664)

[Implementación de KMS en una red global compleja 24](#_Toc237084665)

[Escenarios con claves MAK 27](#_Toc237084666)

[Activación independiente de MAK 29](#_Toc237084667)

[Activación de proxy de MAK 33](#_Toc237084668)

[Compatibilidad de VAMT con la activación de KMS 40](#_Toc237084669)

[Conversión de la activación KMS en MAK 41](#_Toc237084670)

[Claves de hosts KMS para productos 43](#_Toc237084671)

[Valores de la directiva de activación 45](#_Toc237084672)

[Claves de configuración del cliente KMS 46](#_Toc237084673)

[Códigos de error de activación 48](#_Toc237084674)

[Registro de eventos de Windows 58](#_Toc237084675)

[Propiedades y métodos de WMI 63](#_Toc237084676)

[Glosario 73](#_Toc237084677)

[Vínculos de recursos 75](#_Toc237084678)

# Introducción

Esta guía proporciona información técnica para la [Guía de planificación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926), la [Guía de implementación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150083) y la [Guía de operaciones de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084). Para obtener una descripción general de Microsoft® Volume Activation y sus componentes, consulte la [Guía de planificación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926). La referencia contiene:

* Experiencia del usuario
* Opciones de Slmgr.vbs
* Configuración del registro
* Configuración del objeto de directivas de grupo (GPO)
* Intervalo de activación del Servicio de administración de claves (KMS)
* Orden de búsqueda de detección de KMS
* Escenarios de activación
* Claves de hosts KMS para productos
* Valores de la directiva de activación
* Claves de configuración del cliente KMS
* Códigos de error de activación
* Registro de eventos de Windows®
* Propiedades y métodos del Instrumental de administración de Windows (WMI)
* Glosario
* Recursos

**Nota:** Para conocer la compatibilidad con otro software que usa Volume Activation, consulte los documentos específicos de esas aplicaciones.

Esta guía usa las siguientes convenciones:

* Las líneas de comando y sus opciones aparecen en negrita.
* Los marcadores de las líneas de comando se encuentran entre corchetes angulares (<>).
* Las opciones de las líneas de comando opcionales se encuentran entre corchetes ([]).
* La subclave del registro y los nombres de los valores aparecen en negrita.

# Experiencia del usuario

Windows® 7 y Windows Server® 2008 R2 muestran notificaciones y cuadros de diálogo diseñados para problemas de activación. La Tabla 1 describe la forma en la que las notificaciones y los cuadros de diálogo corresponden a cada problema.

**Nota:** Las ediciones centrales de Windows Server 2008 no ofrecen al usuario la experiencia con notificaciones.

Tabla 1. Diálogos y cuadros de diálogo del estado de notificaciones

| **Problema** | **Globo de notificación** | **Cuadro de diálogo correspondiente** |
| --- | --- | --- |
| No se activó una copia de Windows instalada recientemente al finalizar el período de gracia de activación. |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |
| Una copia de Windows instalada con anterioridad detecta hardware informático o cambios en el sistema básico de entrada y salida (BIOS) que requieren la reactivación de Windows. Además, un cliente KMS activado no se reactiva en 180 días. |  | 37-HW OOT.jpg |
| Windows se activó mediante KMS y no ha renovado su activación en el plazo de 180 días más un período de gracia de 30 días. |  | 37-KMS OOT.jpg |
| Se produjo un error en la validación en línea o se detectó una vulnerabilidad de seguridad en la activación, que permite que copias no autorizadas de Windows omitan la activación del producto. |  | 37-NG.jpg |
| Windows detecta que se ha cambiado un componente de la licencia de Windows. |  | 37 - No Key.jpg |
| Windows detecta que se han modificado los archivos de licencia. |  | 37 - Reinstall.jpg |

# Opciones de Slmgr.vbs

Debido a los cambios de WMI en Windows 7 y Windows Server 2008 R2, el script Slmgr.vbs no está diseñado para funcionar en diferentes plataformas. El uso de Slmgr.vbs para administrar sistemas Windows 7 o Windows Server 2008 R2 desde el sistema operativo Windows Vista® no es compatible. Si se intenta administrar un sistema de nivel inferior desde Windows 7 o Windows Server 2008 R2, se generará un error de versión incorrecta específico. Por ejemplo, la ejecución de **cscript slmgr.vbs <nombre\_equipo\_vista> /dlv** muestra el siguiente resultado:

Microsoft (R) Windows Script Host Versión 5.8  
Copyright (C) Microsoft Corporation. Reservados todos los derechos.

El equipo remoto no es compatible con esta versión de SLMgr.vbs

Para administrar clientes remotos, use Volume Activation Management Tool (VAMT) versión 1.2 o posterior, o cree scripts de WMI personalizados que distingan plataformas. Para obtener información adicional acerca de las propiedades y métodos de WMI para Volume Activation, consulte la sección “WMI Properties and Methods”, que aparece más adelante en esta guía de referencia.

A continuación, se describe la sintaxis del script Slmgr.vbs, y la Tabla 2 describe las opciones de la línea de comandos:

slmgr.vbs [Nombre\_de\_equipo [Contraseña de usuario]] [<Opción>]

**Nota:**Para conocer la compatibilidad con otro software que usa Volume Activation, consulte los documentos específicos de esas aplicaciones.

Tabla 2. Opciones de la línea de comandos de Slmgr.vbs

| **Opción** | **Descripción** |
| --- | --- |
| **[Nombre\_de\_equipo]** | Nombre de un equipo remoto (el equipo predeterminado es el equipo local). |
| **[Usuario]** | Cuenta con el privilegio requerido en el equipo remoto. |
| **[Contraseña]** | Contraseña de cuenta con los privilegios requeridos en el equipo remoto. |
| **Opciones globales** | |
| **/ipk clave\_producto** | Intentos de instalación de una clave de producto 5×5. La clave de producto proporcionada por el parámetro es válida y se aplicó al sistema operativo instalado. En caso contrario, se muestra un mensaje de error.  Si la clave es válida y aplicable, se instalará. Si ya se instaló la clave, se reemplazará sin notificación.  Para evitar la inestabilidad en el servicio de licencias, se debe reiniciar el sistema o el Servicio de protección de software.  Esta operación debe ejecutarse desde un símbolo del sistema con privilegios elevados, o se debe establecer el valor del Registro **Operaciones de usuario estándar** de modo que permita que los usuarios sin privilegios obtengan acceso adicional al Servicio de protección de software. |
| **/ato [Id.\_de\_activación]** | Para las ediciones comerciales y los sistemas de volúmenes con clave de host KMS o con clave de activación múltiple (MAK) instalada, **/ato** solicita a Windows que intente la activación en línea.  Para los sistemas que tienen una clave de licencia por volumen genérico (GVLK), se solicita el intento de activación en KMS. Los sistemas configurados para suspender los intentos de activación automática en KMS (**/stao**) siguen intentando la activación en KMS al ejecutar **/ato**.  El parámetro **[Id.\_de\_activación]** expande la compatibilidad de **/ato** para identificar la versión de Windows instalada en el equipo. Si se especifica el parámetro **[Id.\_De\_activación]**, se aíslan los efectos de la opción de la edición asociada al Id. de activación. Ejecute **Slmgr.vbs /dlv** para obtener los Id. de activación de la versión instalada de Windows. Si debe extender la compatibilidad a otras aplicaciones, consulte la guía de las aplicaciones para obtener más instrucciones.  La activación de KMS no requiere privilegios elevados. Sin embargo, la activación en línea requiere privilegios elevados, o se debe establecer el valor del Registro **Operaciones de usuario estándar** de modo que permita que los usuarios sin privilegios obtengan acceso adicional al Servicio de protección de software. |
| **/dli [Id.\_de\_activación | Todos]** | Muestra la información de licencia.  De forma predeterminada, **/dli** muestra la información de licencia para la edición instalada y activa de Windows. Si se especifica el parámetro **[Id.\_de\_activación]**, se muestra la información de licencia de la edición asociada al Id. de activación. Si se especifica el parámetro **[Todos]** se muestra la información de licencia de todos los productos instalados que correspondan.  Esta operación no requiere privilegios elevados. |
| **/dlv [Id.\_de\_activación | Todos]** | Muestra la información de licencia detallada.  De forma predeterminada, **/dlv** muestra la información de licencia para el sistema operativo instalado. Si se especifica el parámetro **[Id.\_de\_activación]**, se muestra la información de licencia de la edición asociada al Id. de activación. Si se especifica el parámetro **[Todos]**, se muestra la información de licencia de todos los productos instalados que correspondan.  Esta operación no requiere privilegios elevados. |
| **/xpr [Id.\_de\_activación]** | Muestra la fecha de expiración de la activación del producto. De forma predeterminada, esto hace referencia a la edición actual de Windows y se usa principalmente para los clientes KMS, ya que la activación de claves MAK y de versiones comerciales es perpetua.  Si se especifica el parámetro **[Id.\_de\_activación]**, se muestra la fecha de expiración de la activación de la edición especificada correspondiente a ese Id. de activación.  Esta operación no requiere privilegios elevados. |
| **Opciones avanzadas** | |
| **/cpky** | Algunas operaciones de servicio requieren que la clave del producto esté disponible en el registro durante las operaciones de configuración rápida (OOBE). La opción **/cpky** quita la clave del producto del registro para impedir que sea robada por códigos malintencionados.  Para la instalación de versiones comerciales que implementan claves, las mejores prácticas recomiendan ejecutar esta opción. La opción no se requiere para las claves MAK y de hosts KMS, ya que este es el comportamiento predeterminado de esas claves. Esta opción es necesaria solamente para otros tipos de claves en los que el comportamiento predeterminado es no eliminar la clave del registro.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/ilc <archivo\_licencia>** | Esta opción instala el archivo de licencia especificado por el parámetro requerido. Las licencias pueden instalarse como medida de solución de problemas, para admitir la activación basada en token o como parte de la instalación manual de una aplicación integrada.  Durante este proceso, no se validan licencias: la validación de licencias se encuentra fuera del ámbito de Slmgr. En su lugar, el Servicio de protección de software se encarga de la validación en el tiempo de ejecución.  Esta operación debe ejecutarse desde un símbolo del sistema con privilegios elevados, o se debe establecer el valor del Registro **Operaciones de usuario estándar** de modo que permita que los usuarios sin privilegios obtengan acceso adicional al Servicio de protección de software. |
| **/rilc** | Esta opción reinstala todas las licencias almacenadas en %SystemRoot%\system32\oem y %SystemRoot%\System32\spp\tokens. Estas son copias aceptables almacenadas durante la instalación.  Se reemplazan las licencias que coinciden en el almacén de datos de confianza. No se modifican las licencias adicionales, por ejemplo, las licencias de emisión (IL) de autoridad de confianza (TA) y licencias para aplicaciones.  Esta operación debe ejecutarse desde un símbolo del sistema con privilegios elevados, o se debe establecer el valor del Registro **Operaciones de usuario estándar** de modo que permita que los usuarios sin privilegios obtengan acceso adicional al Servicio de protección de software. |
| **/rearm** | Esta opción restablece los temporizadores de activación. El proceso **/rearm** también se denomina **sysprep /generalize**.  La operación no se realizará si la subclave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm es igual a **1**. Para obtener más información sobre la subclave del Registro, consulte la sección “” más adelante en esta guía.  Esta operación debe ejecutarse desde un símbolo del sistema con privilegios elevados, o se debe establecer el valor del Registro **Operaciones de usuario estándar** de modo que permita que los usuarios sin privilegios obtengan acceso adicional al Servicio de protección de software. |
| **/upk [Id. de activación]** | Esta opción desinstala la clave de producto de la edición actual de Windows. Después del reinicio, el sistema estará en estado Sin licencia, a menos que se instale una nueva clave de producto.  Puede usar el parámetro **[Id. de activación]** para especificar otro producto instalado.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **Licencias por volumen: opciones de cliente KMS** | |
| **/skms Name[:puerto] | : puerto [Id. de activación] [Id. de activación]** | Esta opción especifica el nombre y, opcionalmente, el puerto del equipo host KMS con el que se debe conectar. Al establecer este valor, se deshabilita la detección automática del host KMS.  Si el host KMS usa únicamente el protocolo de Internet versión 6 (IPv6), se debe especificar la dirección en el formato [nombre de host]:puerto. Las direcciones de IPv6 contienen dos puntos (:), que serán analizados de manera errónea por el script Slmgr.vbs.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/ckms [Id. de activación]** | Esta opción elimina el nombre de host KMS, la dirección y la información de puerto especificados en el Registro, y restablece el comportamiento de la detección automática de KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/skhc** | Esta opción habilita el almacenamiento en caché en el host KMS (predeterminado), que bloquea el uso de **prioridad** e **importancia** del Sistema de nombres de dominio (DNS) después de la detección inicial de un host KMS en ejecución. Si el sistema ya no puede conectarse con el host KMS en ejecución, se volverá a intentar la detección.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/ckhc** | Esta opción deshabilita el almacenamiento en caché del host KMS. La configuración indica al cliente que use la detección automática del DNS en cada intento de activación de KMS (recomendado si se usan **prioridad** e **importancia**).  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **Configuración del host KMS** | |
| **/sai <intervalo>** | Esta opción establece el intervalo en minutos para intentos de conexión KMS de los clientes no activados. El intervalo de activación debe ser de 15 minutos como mínimo y 30 días como máximo. Se recomienda usar el valor predeterminado (2 horas).  El cliente KMS detecta este intervalo del Registro, pero pasa a KMS después de recibir la primera respuesta de KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/sri <intervalo>** | Esta opción establece el intervalo de renovación en minutos para intentos de conexión KMS de los clientes activados. El intervalo de renovación debe ser de 15 minutos como mínimo y 30 días como máximo. La opción se establece inicialmente en el servidor KMS y en el cliente. La configuración predeterminada es 10 080 minutos (7 días).  El cliente KMS detecta este intervalo del Registro, pero pasa a KMS después de recibir la primera respuesta de KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/sprt <puerto>** | Esta opción establece el puerto en el que el host KMS busca solicitudes de activación de clientes. El puerto TCP predeterminado es 1688.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/sdns** | Habilita la publicación de DNS por parte del host KMS (predeterminado).  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/cdns** | Deshabilita la publicación de DNS por parte del host KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/spri** | Establece la prioridad de KMS como Normal (predeterminado).  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/cpri** | Establece la prioridad de KMS como Baja.  Use esta opción para minimizar la contención de KMS en un entorno hospedado. Tenga en cuenta que esto puede dar como resultado un colapso de KMS; según qué otras aplicaciones o roles de servidores estén activos. Use esta opción con precaución.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **Configuración de la activación basada en token** | |
| **/lil** | Muestra las licencias de emisión de activación basada en token instaladas. |
| **/ril <ILID> <ILvID>** | Quita una licencia de emisión de activación basada en token instalada.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/stao** | Establece la marca **Activación basada en token únicamente** para deshabilitar la activación automática de KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/ctao** | Quita la marca **Activación basada en token únicamente** (predeterminado) para habilitar la activación automática de KMS.  La opción se debe ejecutar desde un símbolo del sistema con privilegios elevados. |
| **/ltc** | Muestra los certificados válidos de activación basada en token que pueden activar el software instalado. |
| **/fta <Huella digital de certificado> [PIN]** | Aplica la activación basada en token mediante el certificado identificado. Se proporciona el número de identificación personal (PIN) para desbloquear la clave privada sin solicitud de PIN al usar certificados protegidos por hardware (por ejemplo, las tarjetas inteligentes). |

# Configuración del Registro

La Tabla 3 describe la configuración del Registro compatible con Volume Activation.

Tabla 3. Configuración del Registro

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subclave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **Valor** | **Tipo** | | **Descripción** | | **Ámbito** |
| **Activation\AlternateURL** | **REG\_SZ** | | Como opción, contiene una URL proporcionada por un administrador. Si se completó la clave, algunos de los cuadros de diálogo de activación incluirán un nuevo vínculo, **Obtener información adicional sobre la activación en línea**, que abrirá el explorador predeterminado. | | Todo |
| **DisableDnsPublishing** | **REG\_DWORD** | | Establezca este parámetro con un valor que no sea cero para bloquear la publicación automática a DNS por parte del host KMS. | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **Formato:** nombre\_dominio, <prioridad>, <importancia>  Como opción, contiene una lista de dominios totalmente calificados que KMS usará para publicar automáticamente el registro (SRV) del servicio DNS. El dominio principal de KMS se usa siempre, por lo que no es necesario incluirlo aquí. Depende del valor **DisableDnsPublishing**.  Los parámetros **prioridad** e **importancia** son opcionales. Si no se proporcionan, se establecen en **0** en el registro SRV. | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | Establezca este parámetro con un valor que no sea cero para minimizar la contención de KMS en un entorno hospedado. Tenga en cuenta que en un sistema ocupado, esto puede impedir que el host KMS mantenga una cuenta suficiente. | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | Establezca el parámetro en el host KMS para forzar a KMS a escuchar en el puerto TCP especificado. El host usa el puerto TCP 1688 si no se especificó el valor. | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | Establezca este valor para forzar el uso de un host KMS específico por parte del cliente KMS. No existen valores predeterminados.  Si se especifica un Id. de aplicación o un Id. de SKU, se creará en una subclave en la que se almacenará el valor:  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName. | | Cliente KMS |
| **KeyManagementServicePort** | **REG\_SZ** | | Establezca este valor para forzar el uso de un puerto TCP específico por parte del cliente KMS cuando se comunica con un KMS. El cliente usa el puerto 1688 si no se especificó el valor.  Si se especifica un Id. de aplicación o un Id. de SKU, se creará en una subclave en la que se almacenará el valor:  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort. | | Cliente KMS |
| **KeyManagementServiceVersion** | **REG\_SZ** | | Establezca este valor para que Microsoft Operations Manager (MOM) 2005 detecte automáticamente el KMS. Elimine este valor si el KMS ya no funciona en el equipo. | | KMS |
| **UserOperations** | **REG\_DWORD** | | Este valor no existe de forma predeterminada, y el valor predeterminado es **0**, que requiere elevación. Cree este valor y establézcalo en **1** para habilitar a los usuarios estándar a instalar claves de producto, activar y rearmar equipos sin requerir elevación.  Este ajuste también se puede configurar mediante los objetos de directiva de grupo (GPO), almacenados en la subclave del Registro **\policies**. | | Todo (no solamente KMS) |
| **VLActivationInterval** | **REG\_DWORD** | | Este parámetro se establece inicialmente en el servidor KMS y en el cliente. La configuración predeterminada es 120 minutos (2 horas). El cliente KMS detecta este intervalo del Registro, pero pasa a KMS después de recibir la primera respuesta de KMS. El valor mínimo es 15 minutos y el máximo es 43 200 minutos (30 días). | | Cliente y servidor KMS |
| **VLRenewalInterval** | **REG\_DWORD** | | Este parámetro se establece inicialmente en el servidor KMS y en el cliente. La configuración predeterminada es 10 080 minutos (7 días). El cliente KMS detecta este intervalo del Registro, pero pasa a KMS después de recibir la primera respuesta de KMS. Como resultado, nunca se usará la configuración del cliente. El valor mínimo es 15 minutos y el máximo es 43 200 minutos (30 días). | | Cliente y servidor KMS |
| **Subclave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **Valor** | **Tipo** | **Descripción** | | **Ámbito** | |
| **Manual** | **REG\_DWORD** | **0** = permitir activación automática (valor predeterminado).  **1** = deshabilitar activación automática. | | Clave MAK y host KMS, pero no cliente KMS | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = se mostrarán los avisos y globos de activación (predeterminado).  **1** = se ocultarán todos los avisos relacionados con la activación, si Windows no se encuentra en estado de notificación o sin licencia. No se recomienda. | | Todo (no solamente KMS) | |

# Configuración del objeto de directivas de grupo

La Tabla 4 describe la configuración del objeto de directivas de grupo que las organizaciones pueden usar para impedir que el sistema operativo oscurezca el escritorio en el estado de notificaciones.

Tabla 4. Configuración del objeto de directivas de grupo

| **Nombre de la directiva** | **Descripción** |
| --- | --- |
| **Configuración de usuario -> Plantillas administrativas -> Panel de control -> Personalización -> Impedir cambios en el fondo de pantalla** | Evita que los usuarios agreguen diseños de escritorio o los modifiquen.  De forma predeterminada, los usuarios pueden usar la página **Fondo de escritorio** en el elemento Personalización o Panel de control de pantalla para agregar un diseño de fondo (papel tapiz) a sus escritorios.  Si habilita esta configuración, el usuario no puede cambiar ninguno de los valores de configuración de Fondo de escritorio.  Para especificar un papel tapiz para un grupo, use la configuración **Papel tapiz del escritorio**.  **Nota:** También debe habilitar la configuración **Papel tapiz del escritorio** para evitar que los usuarios cambien el papel tapiz del escritorio. Para obtener información adicional, consulte el artículo de Ayuda y soporte técnico de Microsoft, “Puede cambiar la configuración del papel tapiz del escritorio después de que el administrador seleccione "Impedir cambios en el papel tapiz" en Directiva de grupo” en <http://support.microsoft.com/kb/Q327998>.  Consulte también la configuración de **Permitir solamente papel tapiz de mapa de bits**. |
| **Configuración de usuario -> Plantillas administrativas -> Escritorio -> Escritorio-> Papel tapiz del escritorio** | Especifica el fondo de escritorio ("papel tapiz") que aparece en los escritorios de todos los usuarios.  Esta configuración le permite especificar el papel tapiz de los escritorios de los usuarios y evita que los usuarios modifiquen la imagen de su presentación. El papel tapiz que especifique puede almacenarse en un archivo de mapa de bits (\*.bmp) o JPEG (\*.jpg).  Para usar esta configuración, escriba la ruta de acceso completa y el nombre del archivo que almacena la imagen del papel tapiz. Puede escribir una ruta local, por ejemplo, C:\Windows\web\wallpaper\home.jpg o una ruta de acceso UNC (Convención de nomenclatura universal), por ejemplo \\Server\Share\Corp.jpg. Si el archivo especificado no se encuentra disponible cuando el usuario inicia sesión, no se muestra ningún papel tapiz. Los usuarios no pueden especificar un papel tapiz alternativo. También puede usar esta configuración para especificar que la imagen del papel tapiz se centre, se coloque en mosaico o se expanda. Los usuarios no pueden cambiar la especificación.  Si deshabilita este valor o no lo configura, no se mostrará ningún papel tapiz. Sin embargo, los usuarios pueden seleccionar el papel tapiz que elijan.  Consulte también el valor **Permitir solamente papel tapiz de mapa de bits** en la misma ubicación y el valor **Impedir cambios en el papel tapiz** en Configuración de usuario\Plantillas administrativas\Panel de control.  **Nota:** Esta configuración no se aplica a las sesiones de servidores de escritorios remotos. |
| **Configuración de usuario -> Plantillas administrativas -> Panel de control -> Personalización -> Impedir cambiar iconos del escritorio** | Impide que los usuarios cambien los iconos del escritorio.  De forma predeterminada, los usuarios pueden usar el cuadro de diálogo **Configuración de iconos de escritorio**, en el elemento Personalización o Panel de control de pantalla, para mostrar, ocultar o cambiar los iconos del escritorio.  Si habilita este valor, el usuario no podrá cambiar ninguno de los iconos del escritorio.  Para los sistemas operativos anteriores a Windows Vista, esta configuración también oculta la ficha **Escritorio** en el elemento Panel de control de pantalla. |

# Intervalo de activación de KMS

Dos valores controlan el intervalo de activación de KMS: los temporizadores de activación y renovación:

* El Intervalo de activación de KMS determina la frecuencia con la que el cliente KMS intenta realizar la activación antes de la activación y durante el período de gracia y las notificaciones. El valor se establece en el cliente al ejecutar **slmgr.vbs /sai *intervalo***. El intervalo se establece en minutos y el valor predeterminado es 120 minutos. Para obtener información, consulte las secciones “Slmgr.vbs Options” y “Registry Settings”. Una vez que el sistema se comunica con un host KMS, la configuración del host KMS reemplaza la del cliente local.
* El Intervalo de renovación de KMS determina la frecuencia con la que el cliente KMS intenta realizar la reactivación con KMS una vez activado. El valor se puede establecer mediante **slmgr /sri *intervalo***. El intervalo se establece en minutos. El valor predeterminado es 10 080 minutos (7 días). El valor se puede establecer en el cliente, pero será reemplazado por el valor que proporciona el host KMS.

En funcionamiento, el cliente KMS intenta conectarse con un host KMS en el momento del inicio y vuelve a intentarlo reiteradamente después de que pasan los minutos que indica el intervalo de activación al producirse un error. De forma predeterminada, se realiza cada dos horas. Cuando la activación de KMS se realiza correctamente, el cliente recibe y almacena el intervalo de renovación del host KMS, y Windows se activa por 180 días. La renovación de la activación funciona como una ventana deslizante, similar a una concesión del Protocolo de configuración dinámica de host (DHCP). El cliente se activa por 180 días, pero continúa intentando realizar la reactivación con intermedios de tantos minutos como se ha indicado en el intervalo de renovación (el valor predeterminado es 7 días). Si lo logra, se restablece el período de 180 días. Si falla, el sistema buscará cambios en la red u otros eventos de calificación para realizar otro intento. Después de 15 minutos, el sistema deja de buscar eventos de la calificación pero continúa realizando intentos con intermedios de tantos minutos como se ha indicado en el intervalo de renovación.

Si transcurren 180 días sin una reactivación correcta, el cliente pasa al período de gracia fuera de tolerancia (OOT). Si no se activa en 30 días a partir de la transición a OOT, pasa al modo de notificación.

# Orden de búsqueda de detección de KMS

Si la detección automática de KMS está habilitada (predeterminado) y el almacenamiento en caché de KMS no está deshabilitado, los clientes KMS usarán el siguiente orden para determinar qué KMS usar (intentarán realizar cada paso hasta que responda un host KMS con la clave correcta):

* Valor específico de SKU en el valor del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ
* Valor específico de Id. de aplicación del valor en el Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ
* Valor global en el valor del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ
* Host KMS almacenado en caché específica de SKU (es la identidad almacenada en caché del host usado en la última activación correcta de KMS)
* Detección automática de DNS (se respetan la **importancia** y la **prioridad**)

Si el KMS almacenado en caché no responde, se realiza la detección.

# Escenarios de activación

Las secciones siguientes describen escenarios clave para la activación de KMS y claves MAK.

## Escenarios de KMS

KMS es compatible con redes simples de un único sitio y con redes globales. Los siguientes escenarios muestran:

* La implementación predeterminada de KMS.
* La implementación expandida para admitir redes globales.

### Implementación predeterminada de KMS para redes de un único sitio

Contoso tiene 100 clientes de Windows 7 Enterprise y un conjunto combinado de sistemas Windows Vista, Windows Server 2008 y Windows Server 2008 R2. Contoso es un dominio plano (Contoso.com), como lo muestra la Figura 1. El servidor DNS se ejecuta en Microsoft DNS y es su configuración predeterminada. Esta configuración es compatible con el registro de DNS dinámico y la limpieza de registros de DNS para quitar los registros antiguos.



Figura 1. Implementación predeterminada de KMS para redes de un único sitio

Contoso adquiere un acuerdo de licencia que proporciona una clave B de KMS, que activará todos los sistemas. El administrador de tecnología de la información (TI) instala la clave de host KMS de Contoso (CSVLK) en dos hosts KMS que ejecutan Windows Server 2008 R2 mediante la ejecución local del siguiente comando en un símbolo del sistema con privilegios elevados:

Slmgr.vbs /ipk <KMS\_host\_key>

Luego, el administrador de TI crea un grupo de seguridad en Servicios de dominio de Active Directory® (AD DS) llamado *KMS\_Hosts.* El administrador agrega los servidores KMS\_1 y KMS\_2 al grupo de pertenencia KMS\_Hosts.

El host KMS\_1 se activa en Microsoft a través de Internet: **Slmgr.vbs /ato**. KMS\_1 publica automáticamente sus registros de recursos (RR) RSV en DNS. El administrador de TI obtiene acceso al servidor DNS, ubica el RR for \_vlmcs.\_tcp.contoso.com y cambia sus permisos para otorgar permisos de lectura, escritura y eliminación de KMS\_Hosts al registro. Luego, el host KMS\_2 se activa en Microsoft a través de Internet: **Slmgr.vbs /ato***.*

Por último, el administrador confirma que se habilitó la exclusión del host KMS en Firewall de Windows. Se debe habilitar la excepción de firewall del Servicio de administración de claves.

Los clientes KMS de la red Contoso consultan el dominio DNS y reciben los registros SRV para ambos hosts KMS. Los clientes eligen uno de los dos hosts y se activan (inmediatamente después de que el número de KMS supera el umbral). Para obtener información acerca de los requisitos de número de KMS, consulte la sección “Activation Policy Values”.

### Implementación de KMS en una red global compleja

Contoso se ha expandido a dos dominios, east.contoso.com y west.contoso.com, como lo muestra la Figura 2. El tráfico de red puede pasar de forma privada entre las dos redes a través del vínculo de una red de área extensa (WAN) protegida con firewall. Este vínculo tiene un ancho de banda limitado; por lo tanto, los recursos (incluido DNS) se replican en ambos extremos del vínculo de la WAN para reducir el tráfico, siempre que sea posible.



Figura 2. Implementación de KMS en redes globales complejas

Contoso usa la implementación basada en imágenes. Sus sistemas cliente se estandarizan en Windows Vista, pero los sistemas de Windows Vista están siendo reemplazados por clientes de Windows 7.

Los usuarios, generalmente, se trasladan geográficamente y su conexión de red cambia de un dominio a otro. DHCP proporciona de forma dinámica la dirección IP de los clientes, incluida la especificación del host DNS local, la dirección de la puerta de enlace local, etc.

Para proporcionar compatibilidad con la activación a los clientes de Windows Vista existentes y a los clientes de Windows 7 nuevos, Contoso instala cuatro hosts (con la clave B de KMS). Dos de los hosts KMS están configurados en east.contoso.com y los otros dos en west.contoso.com.

El administrador de TI configura los hosts KMS para que los registros SRV de DNS dirijan a los clientes de Windows 7 y Windows Server 2008 R2 del dominio este a KMS\_E1, si se encuentra disponible, o a KMS\_E2. Si ninguno se encuentra disponible, los clientes intentarán en KMS\_W1 y, por último, en KMS\_W2. De modo similar, el servidor DNS del dominio oeste se configura de modo tal que los clientes de Windows 7 del dominio oeste prefieran comunicarse con KMS\_W1, luego, con KMS\_W2 y, solo si estos fallan, intenten la activación con KMS\_E1 y KMS\_E2 en el extremo lejano del vínculo de la WAN.

El administrador de TI logra esto mediante los siguientes cambios de configuración (consulte la Tabla 5):

* Se agregan hosts KMS\_E\* al grupo de seguridad KMS\_E. El grupo recibe derechos de lectura, escritura y eliminación para el registro \_vlmcs.\_tcp.east.contoso.com.
* Se agregan hosts KMS\_W\* al grupo de seguridad KMS\_W. El grupo recibe derechos de lectura, escritura y eliminación para el registro \_vlmcs.\_tcp.west.contoso.com.
* Los servidores DHCP están configurados para agregar east.contoso.com y west.contoso.com a la lista de búsqueda de sufijos DNS.
* Los firewall entre los dominios este y oeste están configurados para permitir el tráfico RCP a los hosts KMS en el puerto 1688.

Tabla 5. Configuración del host KMS

| **Descripción** | **Configuración** | **Host** |
| --- | --- | --- |
| Configure la prioridad y la importancia del servidor SRV de east.contoso.com para que los clientes se comuniquen con los hosts KMS\_E\* disponibles antes de intentar comunicarse con los hosts KMS\_W\*. El tráfico se dividirá: el 75% a los hosts KMS\_\*1 y el 25% a los hosts KMS\_\*2. | 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 |
| Configure la prioridad y la importancia de SRV de west.contoso.com para que los clientes se comuniquen con los hosts KMS\_W\* disponibles antes de intentar comunicarse con los hosts KMS\_E\*. El tráfico se dividirá: el 75% a los hosts KMS\_\*1 y el 25% a los hosts KMS\_\*2. | 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 |

Luego, el administrador confirma que las excepciones de Firewall de Windows están configuradas para permitir el tráfico de los equipos cliente KMS, según lo describe la Tabla 6.

Tabla 6. Configuración del cliente KMS

| **Descripción** | **Configuración** |
| --- | --- |
| Deshabilitar almacenamiento en caché del host KMS. | **Slmgr /ckhc** |
| Se establece una URL cliente para dirigir los usuarios con problemas de activación al soporte técnico de Contoso. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  AlternateURL = http://contoso.com/help |

El equipo cliente de referencia se activa mediante KMS y, a continuación, se ejecuta **sysprep /generalize**. El sistema se cierra y se digitaliza mediante ImageX desde el Kit de instalación automatizada de Windows 7 (Windows AIK). La descarga de Windows AIK se encuentra disponible en <http://go.microsoft.com/fwlink/?LinkId=136976>.

## Escenarios con claves MAK

Las secciones siguientes describen escenarios de activación de claves MAK, que se basan en el escenario de la Figura 3. La figura muestra entornos de red y de grupos de redes que son típicos en grandes empresas.

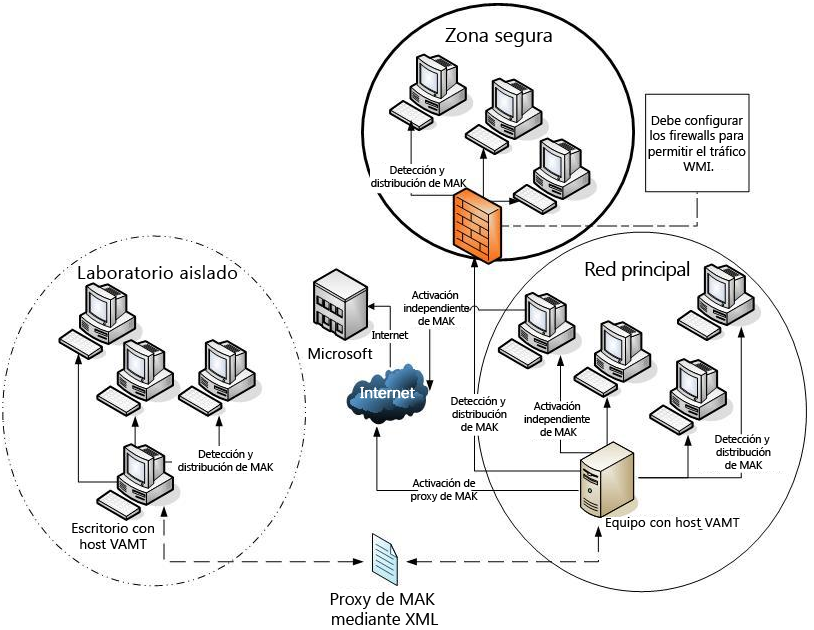


Figura 3. Entornos empresariales

En el entorno de red principal, todos los equipos se encuentran dentro de una red común administrada por AD DS. La zona segura representa los equipos de la red principal con nivel de seguridad más alto que tienen protección adicional de firewall.

El entorno de laboratorio aislado es un grupo de trabajo que se encuentra físicamente separado de la red principal y cuyos equipos no tienen acceso a Internet. La directiva de seguridad de redes establece que no se debe transferir hacia fuera del laboratorio aislado ningún tipo de información que pueda identificar a un equipo o usuario específico.

### Activación independiente de MAK

VAMT permite automatizar la implementación y la activación de claves MAK en la red mediante la distribución de las claves MAK desde una consola centralizada, como se muestra en la Figura 2. VAMT consulta los servidores de activación de Microsoft para obtener la cantidad de activaciones restantes en una clave MAK determinada y, a continuación, enumera el estado de activación de todos los sistemas activados con MAK del entorno. Esta cantidad es una instantánea puntual, no se actualiza en tiempo real. VAMT versión 1.2 está incluida en Windows AIK.

En este escenario, VAMT se implementa en el entorno de la red principal que aparece en la Figura 3. VAMT está instalada en un equipo central con acceso de red a todos los equipos cliente. El host VAMT y los equipos cliente tienen acceso a Internet. Las instrucciones siguientes describen cómo realizar una activación independiente:

1. Instale e inicie VAMT en un equipo host conectado en red:
   1. Instale Windows AIK en el equipo host.
   2. Haga clic en Inicio y, a continuación, en **VAMT** para abrir la consola VAMT.
2. Configure la excepción de firewall del Instrumental de administración de Windows (WMI) en los equipos de destino. Asegúrese de que la excepción de firewall de WMI se haya habilitado para todos los equipos de destino, según se muestra en la Figura 4.

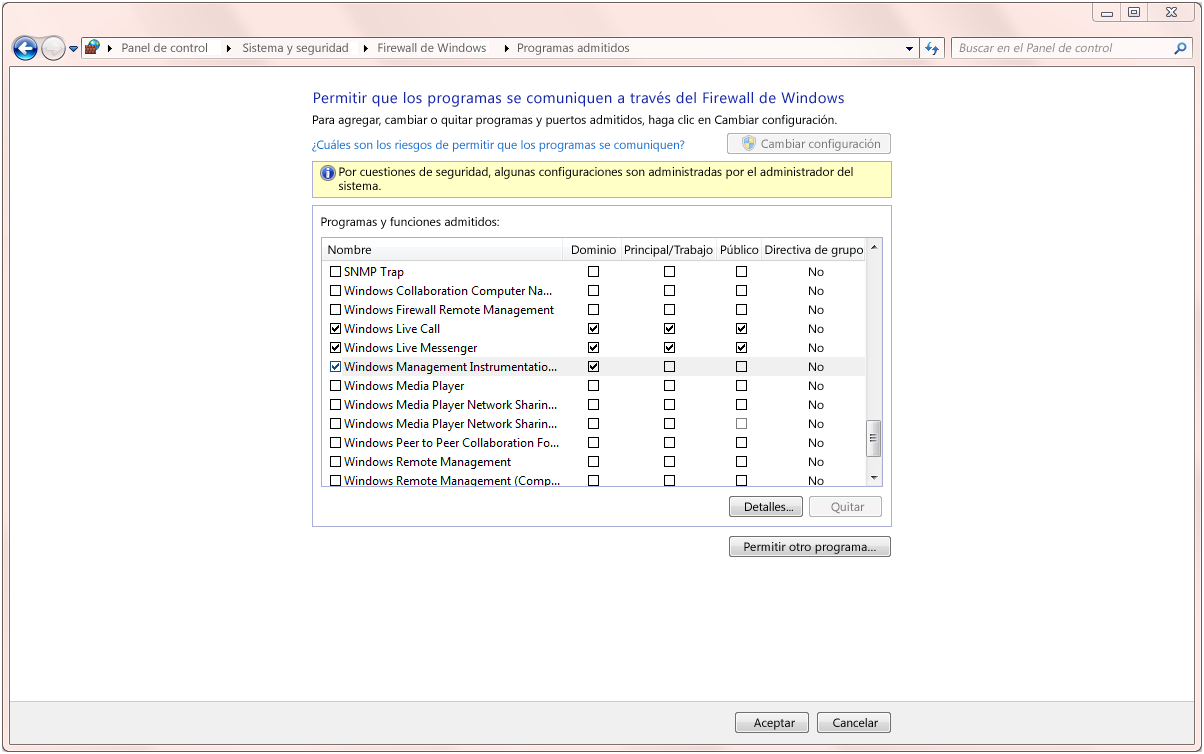


Figura 4. Excepción del Instrumental de administración de Windows (WMI)

1. Agregue equipos a la lista de información de equipos (CIL):
   1. En la consola VAMT haga clic en **Acción** y, a continuación, en **Agregar equipos** para mostrar el cuadro de diálogo **Agregar equipos**.
   2. Introduzca un nombre para el grupo de equipos, por ejemplo, *Grupo de redes principales*, para identificar el grupo de equipos que va a activar.
   3. Haga clic en la lista desplegable para seleccionar una opción de búsqueda. Puede buscar equipos en un grupo de trabajo, en un dominio AD DS o por nombre de equipo individual o dirección IP.
   4. Si desea buscar un equipo por nombre individual o dirección IP, introduzca la información correspondiente en el cuadro de texto debajo de la lista desplegable.
   5. Si desea buscar un dominio o un grupo de trabajo, seleccione el dominio o el grupo de trabajo en la lista desplegable adicional que aparece para esas opciones. Use el campo **Filtrar por nombre de equipo** para buscar un equipo específico dentro del dominio o del grupo de trabajo.
   6. Haga clic en **Aceptar**.

VAMT consulta el servicio de directorio de Active Directory (AD DS) a través del Protocolo ligero de acceso a directorios (LDAP) y agrega los equipos que encuentra a la lista CIL.

1. Recopile la información de estado en los equipos detectados:
   1. Para que VAMT realice una acción en un equipo, debe tener datos de estado de la licencia actual del equipo. Recopile los estados de los equipos individuales. Para ello seleccione directamente uno o varios equipos del panel de vista de la lista de equipos. Para realizar operaciones para un grupo completo, en el panel de vista de árbol, seleccione el nodo Estado desconocido, el nodo Grupos definidos por el usuario o el nodo Grupo de red principal.
   2. Haga clic con el botón secundario en el grupo o en los equipos deseados y, a continuación, en **Actualizar estado de equipo**.
   3. Si desea activar equipos que requieren credenciales de administrador diferentes de las que usa actualmente, seleccione **Usar credenciales alternativas**.
   4. Haga clic en **Aceptar**.
   5. Indique una cuenta del administrador de dominio (para recopilar los estados de todos los equipos del dominio) y la contraseña cuando se lo pidan.

VAMT muestra el cuadro de diálogo **Recopilando información del equipo** mientras recopila el estado de todos los equipos seleccionados. Al finalizar el proceso, aparece el estado actualizado de cada equipo en el panel de vista de la lista de equipos de la consola VAMT.

**Nota:** Para recuperar el estado de la licencia de los equipos seleccionados, VAMT debe tener permisos administrativos en los equipos remotos y debe poder tener acceso a la instrumentación WMI a través del Firewall de Windows. Además, para los equipos de un grupo de trabajo, se debe crear una clave de Registro para habilitar acciones administrativas remotas en el Control de cuentas de usuario (UAC). Consulte la ayuda de VAMT para obtener información adicional acerca de la configuración de sistemas para la administración remota de VAMT.

1. Agregue una clave MAK y determine su cuenta de activación restante:
   1. Haga clic en **Opciones** y, a continuación, en **Administrar MAK** para abrir el cuadro de diálogo **Administrar claves MAK**.
   2. Haga clic en **Agregar** para introducir una clave MAK.
   3. Introduzca la clave MAK y, luego, haga clic en **Validar**.

Una vez realizada la validación, se completa automáticamente el campo **Edición**.

* 1. Escriba una descripción válida y, a continuación, en **Agregar**.

Ahora, la clave MAK aparece en el cuadro de diálogo **Administrar claves MAK**.

* 1. Haga clic en **Actualizar cuenta restante** para recuperar de Microsoft el número de activaciones restantes para las claves MAK mencionadas. (Este paso requiere conectividad a Internet).
  2. Haga clic en **Salir** para cerrar el cuadro de diálogo.

1. Instale la clave MAK y active los equipos cliente:
   1. Seleccione los equipos que desea activar, ya sea mediante un clic en un grupo del panel de vista de árbol o mediante la selección de equipos individuales en el panel de vista de la lista.
   2. Haga clic con el botón secundario en el grupo o los equipos seleccionados y, a continuación, en **Activación independiente de MAK** para mostrar el cuadro de diálogo **Activación independiente de MAK**.
   3. Seleccione la clave MAK correspondiente de la lista **Instalar MAK**.
   4. Seleccione las casillas **Instalar MAK (sobrescribir existente)** y **Activar ahora** para indicar a los equipos seleccionados que se activen inmediatamente mediante el contacto con Microsoft Windows Activation a través de Internet.

Si aparece un asterisco (\*) junto al texto de las casillas de verificación, la acción se aplicará únicamente a los equipos posibles. Por ejemplo, un equipo instalado con la edición comercial de Windows Vista no se puede activar con una clave MAK.

* 1. Si desea activar equipos que requieren credenciales de administrador diferentes de las que usa actualmente, seleccione **Usar credenciales alternativas**.
  2. Haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Asignando claves de producto** y, a continuación, el cuadro de diálogo **Activando equipos** hasta que se completa la acción solicitada. Si seleccionó **Usar credenciales alternativas**, se le solicitará que introduzca las credenciales antes de que aparezcan estos cuadros de diálogo.

### Activación de proxy de MAK

En este escenario, se usa VAMT para activar equipos del grupo de trabajo dentro del entorno de laboratorio aislado que se muestra en la Figura 3. Para este tipo de grupos de trabajo, que están completamente aislados de la red más grande, puede realizar la activación del proxy de la clave MAK mediante la instalación de una segunda VAMT en un equipo que se encuentre dentro del grupo de trabajo aislado y con un medio extraíble para transferir la lista CIL de VAMT del equipo a otro host VAMT que tenga acceso a Internet. Consulte la ayuda de VAMT para obtener información adicional acerca de la configuración de sistemas para la administración remota de VAMT. Los pasos siguientes explican cómo usar VAMT para la activación del proxy:

1. Instale VAMT en un equipo del grupo de trabajo en el laboratorio aislado:
   1. Instale Windows AIK en un equipo host en el grupo de trabajo Laboratorio aislado.

El equipo puede estar ejecutando Windows XP con Service Pack2 (SP2), Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2.

* 1. Haga clic en Inicio y, a continuación, en **VAMT** para abrir la consola VAMT.
  2. Configure la excepción de firewall del Instrumental de administración de Windows (WMI) en los equipos de destino. Asegúrese de que la excepción de firewall de WMI se haya habilitado para todos los equipos de destino.

1. Agregue equipos a la lista CIL:
   1. En la consola VAMT haga clic en **Acción** y, a continuación, en **Agregar equipos** para abrir el cuadro de diálogo **Agregar equipos**.
   2. Introduzca un nombre para el grupo de equipos, por ejemplo, *Grupo Laboratorio aislado* para identificar el grupo de equipos que va a activar.
   3. Seleccione la opción **Grupo de trabajo**, especifique el grupo de trabajo y, a continuación, haga clic en **Aceptar**.

VAMT busca el grupo de trabajo de los equipos.

**Nota:** Para que VAMT detecte los equipos cliente de un grupo de trabajo, se debe habilitar la excepción de Firewall de Windows para detección de redes.

1. Recopile el estado de los equipos detectados:
   1. Para que VAMT realice una acción en un equipo, debe tener datos de estado de la licencia actual del equipo. Recopile los estados de los equipos individuales. Para ello seleccione directamente uno o varios equipos del panel de vista de la lista de equipos. Para realizar operaciones para un grupo completo, en el panel izquierdo, seleccione el nodo Estado desconocido, el nodo Grupos definidos por el usuario o el nodo Grupo de laboratorios aislados.
   2. Haga clic con el botón secundario en el grupo o en los equipos deseados y, a continuación, haga clic en **Actualizar estado de equipo**.
   3. Si desea activar equipos que requieren credenciales de administrador diferentes de las que usa actualmente, seleccione **Usar credenciales alternativas**.
   4. Haga clic en **Aceptar**. Cuando se le solicite, introduzca las credenciales para una cuenta que tenga derechos administrativos locales en los equipos del grupo de trabajo seleccionado.

VAMT muestra el cuadro de diálogo **Recopilando información del equipo** mientras recopila el estado de todos los equipos seleccionados. Al finalizar el proceso, aparece el estado actualizado de cada equipo en el panel de vista de la lista de equipos de la consola VAMT.

**Nota:** Para recuperar el estado de la licencia de los equipos seleccionados, VAMT debe tener permisos administrativos en los equipos remotos y debe poder tener acceso a la instrumentación WMI a través del Firewall de Windows. Además, para los equipos de un grupo de trabajo, se debe crear una clave de Registro para habilitar acciones administrativas remotas en el Control de cuentas de usuario (UAC).

1. Agregue una clave MAK:
   1. Haga clic en **Opciones** y, a continuación, en **Administrar MAK** para abrir el cuadro de diálogo **Administrar claves MAK**.
   2. Haga clic en **Agregar** para introducir una clave MAK.
   3. Introduzca la clave MAK y, luego, haga clic en **Validar**.

Una vez realizada la validación, se completa automáticamente el campo **Edición**.

* 1. Escriba una descripción válida y, a continuación, haga clic en **Agregar**.

Ahora, la clave MAK aparece en el cuadro de diálogo **Administrar claves MAK**.

* 1. Haga clic en **Salir** para cerrar el cuadro de diálogo.

**Nota:** Debido a que VAMT no se ha instalado en un equipo con acceso a Internet, la opción **Actualizar cuenta restante** no funcionará. Esta función requiere conectividad a Internet.

1. Instale la clave MAK y active los equipos del laboratorio aislado:
   1. Seleccione el grupo Laboratorio aislado en el panel de vista de árbol.
   2. Haga clic con el botón secundario en el grupo seleccionado y, a continuación, en **Activar proxy de MAK** para mostrar el cuadro de diálogo **Activar proxy de MAK**.
   3. Seleccione la clave MAK correspondiente de la lista **Instalar MAK**.
   4. Seleccione **Instalar MAK (sobrescribir existente)**.

Si aparece un asterisco (\*) junto al texto de la casilla, la acción se aplicará únicamente a los equipos posibles. Por ejemplo, un equipo instalado con la edición comercial de Windows Vista no se puede activar con una clave MAK.

* 1. Desactive la casilla **Obtener Id. de confirmación de Microsoft**, ya que el equipo no tiene acceso a Internet.
  2. Desactive la casilla **Aplicar Id. de confirmación y activar**, ya que aún no se han solicitado los Id. de confirmación (CID).
  3. Si desea activar equipos que requieren credenciales de administrador diferentes de las que usa actualmente, seleccione **Usar credenciales alternativas** y, a continuación, haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Asignando claves de producto** hasta que se completa la acción solicitada. Si seleccionó **Usar credenciales alternativas**, se le solicitará que introduzca las credenciales antes de que aparezca el cuadro de diálogo.

**Nota:** La selección de la casilla **Instalar MAK (sobrescribir existente)** fuerza la instalación de una clave MAK en un equipo cliente. Realice esta acción con sumo cuidado. Si en el equipo hubo una versión de Windows Vista anterior a SP1 durante más de 30 días, el período de gracia inicial ha expirado y el equipo pasará al modo de funcionalidad reducida (RFM) si no se realiza una activación correcta antes del próximo inicio de sesión. Sin embargo, puede usar la activación de proxy MAK para recuperar los equipos correctamente configurados del modo RFM mientras el host VAMT tenga acceso a ellos. El modo RFM se aplica solamente a los sistemas que ejecutan la versión de Windows Vista anterior a SP1. Los equipos que ejecuten Windows Vista con SP1 o posterior, Windows 7, Windows Server 2008 y Windows Server 2008 R2 no pasarán a modo RFM.

1. Guarde la lista CIL:

En este paso, se guarda la lista CIL completa en el host VAMT local (es decir, en el grupo de trabajo). En la activación de proxy MAK, es fundamental conservar este archivo, ya que VAMT lo usa para aplicar los CID a los equipos correspondientes.

* 1. Use la vista de árbol de VAMT o el panel de vista de listas para seleccionar el grupo o los equipos individuales que recibieron la clave MAK correctamente.
  2. En el menú **Archivo**, haga clic en **Guardar** para ver el cuadro de diálogo **Guardar la lista de información del equipo**.
  3. Seleccione un directorio y, a continuación, introduzca un nombre de archivo de CIL, por ejemplo, *IsolatedLabGroup.CIL.*
  4. Haga clic en **Guardar**.

1. Exporte la lista CIL:

Como se mencionó anteriormente, la directiva de seguridad empresarial establece que no se debe transferir hacia fuera del laboratorio aislado ningún tipo de información que pueda identificar un equipo o un usuario específico. Por lo tanto, este tipo de datos debe excluirse del archivo de CIL para transferirlo al host VAMT de la red principal.

* 1. Use la vista de árbol de VAMT o el panel de vista de listas para seleccionar el grupo o los equipos individuales que recibieron la clave MAK correctamente.
  2. Haga clic con el botón secundario en el grupo o en los equipos seleccionados y, a continuación, en **Exportar equipos** para ver el cuadro de diálogo **Guardar la lista de información del equipo**.
  3. Seleccione **Excluir la información confidencial del entorno**.
  4. Haga clic en **Examinar** para ver el cuadro de diálogo **Guardar como**.
  5. Seleccione un directorio y, a continuación, introduzca un nombre de archivo de CIL, por ejemplo, *IsolatedLabGroupSecureExport.CIL.*
  6. Haga clic en **Guardar**.
  7. Copie el archivo IsolatedLabGroupSecureExport.CIL en una unidad extraíble (unidad de disco, CD/DVD o unidad flash USB [UFD]).

**Nota:** La selección de la casilla **Excluir la información confidencial del entorno** impide que se guarde la información de identificación personal (PII) en el archivo de CIL. Como resultado, se debe importar nuevamente el archivo de CIL a este host VAMT y al archivo de CIL de almacenamiento completo para que se puedan asignar correctamente las listas CIL solicitadas por Microsoft a los equipos del grupo Laboratorio aislado.

1. Importe el archivo de CIL a un host VAMT con acceso a Internet:
   1. Copie IsolatedLabGroupSecureExport.CIL desde la unidad extraíble en una unidad en un host VAMT que tenga acceso a Internet.
   2. Abra la consola VAMT:
   3. En el menú **Archivo**, haga clic en **Importar** para abrir el cuadro de diálogo **Abrir lista de información del equipo**.
   4. Busque y seleccione **IsolatedLabGroupSecureExport.CIL** y, a continuación, haga clic en **Abrir** para cargar el archivo de CIL en VAMT.
   5. Compruebe que los nombres del equipo, el grupo y el grupo de trabajo no estén visibles.
2. Solicite los CID a Microsoft:
   1. Haga clic con el botón secundario en los equipos importados y, a continuación, en **Activar proxy MAK** para abrir el cuadro de diálogo **Activar proxy MAK**.
   2. Desactive la casilla **Instalar MAK (sobrescribir existente)**.
   3. Desactive la casilla **Obtener Id. de confirmación de Microsoft**.
   4. Desactive la casilla **Aplicar Id. de confirmación y activar**, ya que el host VAMT no se encuentra en la misma red que los equipos seleccionados.
   5. Haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Adquiriendo Id. de confirmación en línea** mientras se conecta a Microsoft y recopila los CID.

1. Exporte el archivo de CIL desde el host VAMT conectado a Internet:
   1. Una vez recuperados los CID de todos los equipos, guarde el archivo de CIL. En la consola VAMT, desplácese hacia la derecha y compruebe que la columna **CID pendiente** contenga valores.
   2. En el menú **Archivo**, haga clic en **Guardar como** e introduzca un nuevo nombre para el archivo, por ejemplo, *IsolatedLabGroupSecureExportwithCID.CIL.*
   3. Copie el archivo actualizado IsolatedLabGroupSecureExportwithCID.CIL en una unidad extraíble (unidad de disco, CD/DVD o unidad flash USB [UFD]).
2. Importe el archivo de CIL al host VAMT original dentro del laboratorio aislado:
   1. Copie IsolatedLabGroupSecureExportwithCID.CIL desde la unidad extraíble en una unidad en un host VAMT del laboratorio aislado.
   2. Abra la consola VAMT:
   3. En el menú **Archivo**, haga clic en **Abrir** para ver el cuadro de diálogo **Abrir lista de información del equipo**.
   4. Busque y seleccione IsolatedLabGroup.CIL y, a continuación, haga clic en **Abrir** para cargar el archivo de CIL en VAMT.

Esto muestra los equipos detectados con anterioridad y los estados de sus licencias en el panel de vista de la lista de equipos.

* 1. En el menú **Archivo**, haga clic en **Importar** y busque el archivo que contiene los CID (IsolatedLabGroupSecureExportwithCID.CIL).

Esto inicia el proceso de combinación que une los CID a los IID de los equipos.

* 1. En el menú **Archivo**, haga clic en **Guardar** y, a continuación, introduzca un nombre de archivo, por ejemplo, *IsolatedLabGroupwithCID.CIL*, para guardar el archivo que asocia los IID con los CID correspondientes.

**Importante:** En los escenarios restantes es fundamental guardar este archivo. Se recomienda realizar una copia de seguridad del archivo y protegerlo contra sobrescritura.

1. Aplique los CID y active los equipos del laboratorio aislado:
   1. Haga clic con el botón secundario en el grupo Laboratorio aislado en el panel de vista de listas y, a continuación, en **Activar proxy MAK** para abrir el cuadro de diálogo **Activar proxy MAK**.
   2. Desactive la casilla **Instalar MAK (sobrescribir existente)**, ya que los equipos seleccionados ya tienen una clave MAK instalada.
   3. Desactive la casilla **Obtener Id. de confirmación de Microsoft**.
   4. Seleccione la casilla **Aplicar Id. de confirmación y activar** para indicar a VAMT que active los equipos seleccionados mediante la instalación de sus CID.
   5. Haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Asignando Id. de confirmación** mientras instala los CID en los equipos seleccionados.

1. Puede reactivar los equipos cuyas imágenes se crearon nuevamente en el laboratorio aislado:

Si se han creado nuevamente las imágenes de los equipos del laboratorio aislado, pero el hardware subyacente no se modificó, VAMT puede reactivarlos usando el archivo IsolatedLabGroupwithCID.CIL.

* 1. Vuelva a implementar Windows en los equipos con los mismos nombres de equipo que usó anteriormente.
  2. Abra la consola VAMT en el host VAMT local (grupo de trabajo).
  3. En el menú **Archivo**, haga clic en **Abrir** y, a continuación, seleccione el archivo IsolatedLabGroupwithCID.CIL.
  4. En el panel de vista de árbol, haga clic con el botón secundario en el grupo **Laboratorio aislado** y, a continuación, en **Volver a aplicar Id. de confirmación** para ver el cuadro de diálogo **Reactivar proxy MAK**.
  5. Desactive la casilla **Instalar MAK (sobrescribir existente)** seleccionada y asegúrese de que la MAK que se usó se haya seleccionado de la lista.
  6. Deje activada la casilla **Volver a aplicar Id. de confirmación y reactivar** seleccionada para volver a aplicar los CID almacenados desde el archivo IsolatedLabGroupwithCID.CIL.
  7. Deje seleccionada la casilla **Exigir coincidencia exacta de IID** seleccionada si no se ha modificado el hardware desde la activación inicial de proxy MAK y si está usando la misma clave MAK para reactivar el equipo.

Desactive la casilla si se ha modificado el hardware pero aún desea que VAMT intente realizar la reactivación con el CID almacenado antes. Tenga en cuenta que es posible que Windows no se active correctamente en este escenario.

* 1. Si desea activar un equipo que requiere credenciales de administrador diferentes de las que usa actualmente, seleccione la casilla **Usar credenciales alternativas**.
  2. Haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Asignando claves de producto** mientras aplica la clave MAK al grupo Laboratorio aislado.

VAMT muestra el cuadro de diálogo **Asignando Id. de confirmación** mientras instala los CID en los equipos seleccionados.

**Nota:**La selección de la casilla **Instalar MAK (sobrescribir existente)**  fuerza la instalación de una clave MAK. Realice esta acción con sumo cuidado. Si en el equipo hubo una versión de Windows Vista anterior a SP1 durante más de 30 días, el período de gracia inicial ha expirado y el equipo pasará al modo de funcionalidad reducida (RFM) si no se realiza una activación correcta antes del próximo inicio de sesión. Se puede usar VAMT para recuperar los equipos correctamente configurados del modo RFM mientras se pueda tener acceso a ellos dentro de la red. El modo RFM se aplica solamente a los sistemas que ejecutan la versión de Windows Vista anterior a SP1. Los equipos que ejecuten Windows Vista con SP1 o posterior, Windows 7, Windows Server 2008 y Windows Server 2008 R2 no pasarán a modo RFM.

### Compatibilidad de VAMT con la activación de KMS

En este escenario, se usa VAMT para instalar y activar las claves de cliente KMS en los equipos de la red principal o del laboratorio aislado. El procedimiento descrito a continuación presupone que VAMT se ha instalado y que los equipos se han agregado a la lista CIL. Las tareas se describen en los pasos 1 a 4 del Escenario 1 (para la red principal) o en el Escenario 2 (para el grupo de trabajo Laboratorio aislado).

1. Abra la consola VAMT:
2. Seleccione los equipos que desea activar, ya sea mediante un clic en un grupo del panel de vista de árbol o mediante la selección de equipos individuales en el panel de vista de la lista.
3. Haga clic con el botón secundario en el grupo o en los equipos seleccionados y, a continuación, en **Configurar para la activación de KMS** para ver el cuadro de diálogo **Configuración de KMS**.
4. Seleccione **Instalar clave de cliente KMS (sobrescribir existente)** para indicar a VAMT que instale una clave de cliente KMS en un equipo cliente.
5. Seleccione la opción de activación adecuada:

* **Detectar automáticamente el host KMS mediante DNS.** Primero, VAMT elimina todos los hosts KMS configurados anteriormente en el equipo y, a continuación, indica al equipo que consulte a DNS para localizar un host KMS e intente realizar la activación.
* **Usar un host y un puerto KMS específicos.** VAMT establece el nombre del host y del puerto KMS en el equipo de destino y, a continuación, indica al equipo que intente realizar la activación con el host KMS específico.

1. Si desea activar equipos que requieren credenciales de administrador diferentes de las que usa actualmente, seleccione la casilla **Usar credenciales alternativas** y, a continuación, haga clic en **Aceptar**.

VAMT muestra el cuadro de diálogo **Asignando claves de producto** y, a continuación, el cuadro de diálogo **Activando equipos** hasta que se completa la acción solicitada. Si seleccionó la casilla **Usar credenciales alternativas**, se le solicitará que introduzca las credenciales antes de que aparezcan estos cuadros de diálogo.

### Conversión de la activación KMS en MAK

Windows 7 y Windows Server 2008 R2 se instalan automáticamente como clientes KMS. Para convertir un cliente KMS en una activación MAK, instale una clave MAK. Las claves MAK se pueden instalar durante la instalación del sistema operativo o en cualquier momento después de haberlo instalado.

Se puede instalar una clave MAK en una imagen de referencia de Windows 7 y Windows Server 2008 R2 para que todas las instalaciones realizadas a partir de esa imagen utilicen la activación MAK en lugar de la activación KMS predeterminada. Así se elimina la necesidad de especificar una clave MAK en un archivo de instalación desatendida.

#### Instalación de una MAK durante la instalación del sistema operativo

Puede convertir un cliente KMS en cliente MAK durante la instalación inicial de Windows 7 o Windows Server 2008 R2 mediante la inclusión de una clave MAK en un archivo de instalación desatendida (Unattend.xml). El archivo Unattend.xml se puede usar con Setup.exe o con los Servicios de implementación de Windows. Para obtener más información, consulte el archivo de ayuda Referencia para la configuración desatendida de Windows en Windows AIK, disponible en <http://go.microsoft.com/fwlink/?LinkId=136976>.

**Nota:** La clave MAK se almacena en texto sin cifrar en el archivo Unattend.xml. Durante una instalación desatendida, se copia el archivo Unattend.xml o AutoUnattend.xml en la carpeta %SystemRoot%\Panther del equipo de destino. Sin embargo, al concluir el proceso de configuración, el programa de configuración la reemplaza por “SENSITIVE\*DATA\*DELETED” (Datos confidenciales eliminados).

#### Instalación de una MAK después de la instalación del sistema operativo

Puede configurar una edición de volumen de Windows 7 o Windows Server 2008 R2 para usar la activación MAK mediante el elemento Sistema del Panel de control o mediante la ejecución del script Slmgr.vbs.

* Para instalar una clave MAK mediante la aplicación Sistema, haga clic en el vínculo **Cambiar la clave de producto** y, a continuación, escriba la clave MAK en el cuadro de diálogo **Cambie la clave de producto para efectuar la activación**.
* Para instalar una clave MAK mediante Slmgr.vbs, ejecute el siguiente comando en el símbolo del sistema:

slmgr.vbs /ipk <ClavedeActivaciónMúltiple>

ClavedeActivaciónMúltiple es la clave MAK.

Si los usuarios instalan una clave MAK desde la interfaz de usuario (IU), el cliente MAK intentará realizar la activación por Internet una vez. Si los usuarios instalan una clave MAK mediante el script Slmgr.vbs, el cliente MAK no intentará realizar la activación automática. El usuario puede usar **Slmgr.vbs /ato** para activar la clave MAK por Internet.

# Claves de hosts KMS para productos

La Tabla 7 describe los productos que puede activar cada host KMS.

Tabla 7. Claves de host KMS que coinciden con los productos que activan

| **Grupo de productos por volumen** | **Productos de Windows** | **Tipo de clave** | **Productos activados por tipo de clave** |
| --- | --- | --- | --- |
| 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  Grupo de servidores A | Windows Web Server® 2008 R2  Windows Server 2008 R2 HPC Edition  Windows HPC Server 2008 R2 | KMS\_A | Windows Server 2008 R2 grupo A  Windows Server 2008 grupo A  Windows Vista Volume Editions  Windows 7 Volume Editions |
| Windows Server 2008 R2  Grupo de servidores B | Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise | KMS\_B | Windows Server 2008 R2 grupo A  Windows Server 2008 grupo A  Windows Server 2008 R2 grupo B  Windows Server 2008 grupo B  Windows Vista Volume Editions  Windows 7 Volume Editions |
| Windows Server 2008 R2  Grupo de servidores C | Windows Server 2008 R2 Datacenter  Windows Server 2008 R2 para sistemas basados en Itanium | KMS\_C | Windows Server 2008 R2 grupo A  Windows Server 2008 grupo A  Windows Server 2008 R2 grupo B  Windows Server 2008 grupo B  Windows Server 2008 R2 grupo C  Windows Server 2008 grupo C  Windows Vista Volume Editions  Windows 7 Volume Editions |
| Las claves KMS de Windows Server 2008 R2 respetan la misma jerarquía (grupos A, B, C) que Windows Server 2008, con el agregado de Windows Server 2008 Datacenter sin Hyper-V™, Windows Server 2008 Enterprise sin Hyper-V y Windows Server 2008 Standard sin Hyper-V. La principal diferencia es que las claves KMS de Windows Server 2008 R2 pueden usarse para activar un host KMS que activará Windows Server 2008, Windows 7 y Windows Vista.  Las claves de Windows Server 2008 y Windows Vista no pueden activar los sistemas de Windows 7 ni Windows Server 2008 R2. | | | |

# Valores de la directiva de activación

En la Tabla 8, se muestran los valores de la directiva para Windows 7 y Windows Server 2008 R2.

Tabla 8. Valores de la directiva para Windows 7 y Windows Server 2008 R2

| **Elemento** | **Valor de cliente** | **Valor de servidor** | **Intervalo** |
| --- | --- | --- | --- |
| Límite de rearmado | 3 | 3 | No configurable |
| Umbral de cantidad de clientes KMS | 25 | 5 | No configurable |
| Duración de la activación KMS | 180 días | 180 días | No configurable |
| Puerto de escucha del host KMS | 1688 | 1688 | Cualquier puerto TCP abierto |
| Período de gracia OOB | 30 días | 30 días | No configurable |
| Período de gracia OOT | 30 días | 30 días | No configurable |
| Reactivación del cliente KMS (en minutos) | 10 080 minutos  (7 días, predeterminado) | 10 080 minutos  (7 días, predeterminado) | De 15 a 43 000 minutos  (30 días, predeterminado) |
| Intervalo de reintento silencioso de KMS (se produce al fallar la activación KMS) | 120 minutos | 120 minutos | De 15 a 43 000 minutos  (120 minutos, predeterminado) |

# Claves de configuración del cliente KMS

De forma predeterminada, los sistemas operativos Windows 7 y Windows Server 2008 R2 usan KMS para la activación. En las instalaciones por volumen, la clave de configuración se instala de forma predeterminada, lo que convierte el sistema en un cliente KMS. Si desea convertir un equipo de host KMS a MAK o una edición comercial de Windows a un cliente KMS, instale la clave de configuración correspondiente (GVLK) de la Tabla 9 mediante **slmgr /ipk <clave de configuración>**.

Tabla 9. Claves de configuración del cliente KMS

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

# Códigos de error de activación

En la Tabla 10 se proporciona ayuda para la solución de problemas que ocurren al activar ediciones por volumen de los sistemas operativos Windows 7 y Windows Server 2008 R2.

Tabla 10. Códigos de error y descripciones

| **Código de error** | **Mensaje de error** | **Tipo de activación** | **Causa posible** | **Pasos de solución de problemas** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | El servidor de activación determinó que la clave de producto especificada no es válida. | MAK | La clave MAK introducida no es válida. | Compruebe que la clave sea la MAK proporcionada por Microsoft.  Póngase en contacto con el [Centro de atención telefónica de activaciones de Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) para comprobar que la clave MAK sea válida. |
| 0xC004C003 | El servidor de activación determinó que la clave de producto especificada está bloqueada. | MAK | La MAK está bloqueada en el servidor de activaciones. | Póngase en contacto con el [Centro de atención telefónica de activaciones de Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) para obtener una nueva clave MAK e instalar o activar el sistema. |
| 0xC004C008 | El servidor de activación determinó que la clave de producto especificada no puede usarse. | KMS | La clave KMS ha superado el límite de activaciones. | Las claves de host KMS se activan hasta 10 veces en seis equipos distintos. Si son necesarias más activaciones, póngase en contacto con el [Centro de atención telefónica de activaciones de Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C020 | El servidor de activación informó que la clave de activación múltiple ha superado su límite. | MAK | La clave MAK ha superado el límite de activaciones. | Las claves MAK están diseñadas para proporcionar una cantidad limitada de activaciones. Póngase en contacto con el [Centro de activaciones de Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C021 | El servidor de activación informó que la clave de activación múltiple ha superado su límite de extensión. | MAK | La clave MAK ha superado el límite de activaciones. | Las claves MAK están diseñadas para proporcionar una cantidad limitada de activaciones. Póngase en contacto con el [Centro de activaciones de Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004F009 | El Servicio de protección de software informó que ha expirado el período de gracia. | MAK | El período de gracia expiró antes de la activación del sistema. Ahora, el sistema se encuentra en estado de notificaciones. | Consulte la sección “User Experience.” |
| 0xC004F00F | El Servidor de licencias de software informó que el enlace del Id. de hardware supera el nivel de tolerancia. | MAK/cliente KMS/host KMS | El hardware ha cambiado o se actualizaron los controladores del sistema. | **MAK:** reactive el sistema durante el período de gracia OOT mediante la activación telefónica o en línea.  **KMS:** reinicie o ejecute **slmgr.vbs /ato**. |
| 0xC004F014 | El Servicio de protección de software informó que la clave de producto no está disponible. | MAK/cliente KMS | No hay claves de producto instaladas en el sistema. | Instale una clave de producto MAK o la clave de instalación de KMS que se encuentra en el archivo \sources\pid.txt de la unidad de instalación. |
| 0xC004F02C | El Servicio de protección de software informó que el formato de los datos de activación fuera de línea es incorrecto. | MAK/cliente KMS | El sistema detectó que los datos introducidos durante la activación telefónica no son válidos. | Compruebe que ha introducido correctamente el CID. |
| 0xC004F035 | Este código de error equivale a “El Servicio de protección de software informó que no pudo activarse el equipo con una clave de producto de licencia por volumen”. Este texto de error es correcto, pero es ambiguo.  Este error indica que en el equipo falta un marcador de Windows en BIOS (que aparece en los sistemas OEM para indicar que los productos se envían con ediciones válidas de Windows, lo cual es un requisito para la activación del cliente KMS).  Error: clave de licencia por volumen no válida  Para efectuar la activación, necesita cambiar la clave de producto a fin de que sea una clave de activación múltiple (MAK) o una clave comercial.  Debe tener una licencia autorizada de sistema operativo y una licencia de actualización de Windows 7 de licencias por volumen o una licencia completa para Windows 7 adquirida en un establecimiento.  CUALQUIER OTRA INSTALACIÓN DE ESTE SOFTWARE CONSTITUYE UNA INFRACCIÓN DEL ACUERDO Y DE LAS LEYES DE DERECHOS DE AUTOR APLICABLES. | Cliente KMS/host KMS | Las ediciones por volumen de Windows 7 tienen licencia solamente para actualización. No se admitirá la instalación de un sistema operativo por volumen en un equipo que no tenga un sistema operativo instalado que cumpla con los requisitos. | Instale una versión de un sistema operativo de Microsoft que cumpla con los requisitos y realice la instalación del SO con la clave MAK. |
| 0xC004F038 | El Servicio de protección de software informó que no se pudo activar el equipo. El número informado por el Servicio de administración de claves (KMS) no es suficiente. Póngase en contacto con el administrador del sistema. | Cliente KMS | El número de hosts KMS es demasiado bajo. El número de KMS debe ser ≥ 5 para Windows Server y ≥ 25 para el cliente Windows. | Se necesitan más equipos en el grupo KMS para activar los clientes KMS. Ejecute **Slmgr.vbs /dli** para obtener el número actual de hosts KMS. |
| 0xC004F039 | El Servicio de protección de software informó que no se pudo activar el equipo. No está habilitado el Servicio de administración de claves (KMS). | Cliente KMS | Este error se produce cuando no se responde a una solicitud de KMS. | Realice un diagnóstico de problemas en la conexión de red entre el host KMS y el cliente. Asegúrese de que el puerto TCP 1688 (predeterminado) no esté bloqueado por un firewall o filtrado de otra manera. |
| 0xC004F041 | El Servicio de protección de software determinó que el Servidor de administración de claves (KMS) no está activado. Es necesario activar el KMS. | Cliente KMS | El host KMS no está activado. | Active el host KMS mediante la activación telefónica o en línea. |
| 0xC004F042 | El Servicio de protección de software determinó que no puede usarse el Servicio de administración de claves (KMS) especificado. | Cliente KMS | El cliente KMS y el host KMS no coinciden. | Este error se produce cuando un cliente KMS se comunica con un host KMS que no puede activar el software cliente. Esto puede ser común en entornos combinados que contienen hosts KMS específicos de aplicaciones y del sistema operativo, por ejemplo. |
| 0xC004F050 | El Servicio de protección de software informó que la clave de producto no es válida. | KMS, cliente KMS, MAK | Esto se puede deber a un error tipográfico de la clave KMS o a un error de introducción de una clave Beta en una versión publicada del sistema operativo. | Instale la clave KMS adecuada en la versión correspondiente de Windows. Controle que esté escrita correctamente. Si está copiando y pegando la clave, asegúrese de que no se estén sustituyendo los guiones largos por guiones cortos. |
| 0xC004F051 | El Servicio de protección de software informó que la clave de producto está bloqueada. | MAK/KMS | La clave de producto en el servidor de activación está bloqueada por Microsoft. | Obtenga una nueva clave MAK/KMS, instálela en el sistema y lleve a cabo la activación. |
| 0xC004F064 | El Servicio de protección de software informó que ha expirado el período de gracia para productos no originales. | MAK | La Herramienta de activación de Windows (WAT) ha determinado que el sistema no es original. | Consulte la Guía de operaciones de Volume Activation. |
| 0xC004F065 | El Servicio de protección de software informó que la aplicación se está ejecutando dentro del período válido para productos no originales. | MAK/cliente KMS | La Herramienta de activación de Windows ha determinado que el sistema no es original. El sistema continuará ejecutándose durante el período de gracia para productos no originales. | Obtenga e instale una clave de producto original y active el sistema durante el período de gracia. De lo contrario, el sistema pasará al estado de notificaciones al concluir el período de gracia. |
| 0xC004F06C | El Servicio de protección de software informó que no se pudo activar el equipo. El Servicio de administración de claves (KMS) determinó que la marca de tiempo de la solicitud no es válida. | Cliente KMS | La hora del sistema del equipo cliente difiere demasiado de la hora del host KMS. | La sincronización horaria es importante para la seguridad del sistema y la red por una amplia variedad de motivos. Puede resolver este problema cambiando la hora del sistema del cliente para que coincida con el KMS. Se recomienda usar un origen de hora de NTP (Protocolo de tiempo de redes) o Servicios de dominio de Active Directory para la sincronización de la hora. Esto usa la hora UTP, independientemente de la zona horaria que se seleccione. |
| 0x80070005 | Acceso denegado. La acción solicitada requiere privilegios elevados. | Cliente KMS/MAK/host KMS | UAC (Control de cuentas de usuario) prohíbe que los procesos de activación se ejecuten en un símbolo del sistema no elevado. | Ejecute slmgr.vbs desde un símbolo del sistema con privilegios elevados. Haga clic con el botón secundario en cmd.exe y, a continuación, en Ejecutar como administrador. |
| 0x8007232A | Falla del servidor DNS. | Host KMS | El sistema tiene problemas de red o DNS. | Realice un diagnóstico de problemas en la red y el servidor DNS. |
| 0x8007232B | El nombre de DNS no existe. | Cliente KMS | El cliente KMS no puede encontrar registros de recursos SRV de KMS en DNS.  Si un host KMS no existe en la red, se debe instalar una clave MAK. | Confirme que se haya instalado un host KMS y que la publicación de DNS esté habilitada (predeterminado).  Si DNS no está disponible, dirija el cliente KMS al host KMS mediante **slmgr.vbs /skms <*nombre\_host\_kms>***.  Puede obtener e instalar una clave MAK y, a continuación, activar el sistema.  Por último, realice un diagnóstico de problemas en el servidor DNS. |
| 0x800706BA | El servidor RPC no está disponible. | Cliente KMS | Los parámetros del firewall no están configurados en el host KMS, o los registros SRV del DNS han expirado. | Asegúrese de que la excepción de firewall del Servicio de administración de claves esté habilitada en el equipo host KMS.  Asegúrese de que los registros SRV se dirijan a un host KMS válido.  Realice un diagnóstico de problemas en las conexiones de red. |
| 0x8007251D | No se encontraron registros para la consulta de DNS. | Cliente KMS | El cliente KMS no puede encontrar registros de recursos SRV de KMS en DNS. | Realice un diagnóstico de problemas en las conexiones en red y en el servidor DNS. |
| 0xC004F074 | El Servicio de protección de software informó que no se pudo activar el equipo. No se pudo establecer comunicación con un servicio de administración de claves (KMS). Para conocer más detalles, consulte el registro de eventos de aplicación. | Cliente KMS | Todos los sistemas host KMS mostraron un error. | Ejecute la solución de problemas para los errores de cada Id. de evento 12288 relacionado con el intento de activación. |

# Registro de eventos de Windows

En la Tabla 11 se muestran los eventos que KMS registra en el Registro de eventos de Windows. A continuación, se describen los datos comunes de cada evento:

* **Nombre del archivo de registro para todo (excepto 12290):** Windows Logs\Application
* **Nombre del archivo de registro 12290:** Applications and Services Logs\Key Management Service
* **Nombre del proveedor de eventos:** Microsoft-Windows-Security-Licensing-SLC
* **Nombre de la fuente:** Servicio de protección de software

Tabla 11. Eventos de KMS registrados en el registro de eventos de Windows

| **Id. de evento** | **Registrado por** | **Descripción** | **Mensaje** | **Parámetros**  **Campos incluidos en cadena separada por comas** | | | **Ejemplos** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Nombre** | **Descripción** | |  |
| 12288 | Cliente | Error de generación de solicitud o después del envío de RPC (cliente) | El cliente envió una solicitud de activación al equipo de servicio de administración de claves.%nInfo:%n%1 | HRESULT | Código de devolución | | 0x0 |
|  | | | | Estado | Marcas (nota 1) | | 0x8 |
| Servidor: puerto | Nombre: puerto | | kms01.contoso.com:1688 |
| CMID | Id. del equipo cliente | | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be |
| Hora del cliente | Marca de tiempo de la solicitud | | 2006/1/14 2:30 |
| Información de VM | Sin usar | | 1 |
| Estado de licencia | Estado de licencia  0: sin licencia  1: con licencia (activado)  2: período de gracia OOB  3: período de gracia OOT  4: período de gracia para productos no originales  5: notificaciones  6: período de gracia extendido | | 2 |
|  | | | | Tiempo antes de expiración | Tiempo restante (minutos) | | 40 123 |
| ActID | Id. de activación: identifica la licencia | | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| Directiva N | Número mínimo que el cliente necesita para activar | | 25 |
| 12289 | Cliente | Después de validación de respuesta de KMS (cliente) | El cliente procesó una respuesta de activación al equipo de servicio de administración de claves.%nInfo:%n%1 | HRESULT | Código de devolución | | 0x0 |
|  | | | | Estado | Marcas (nota 1) | | 0x4000008 |
| fBound | Marca activada | | 0 |
| Sin usar | Sin usar, omitir | | 0 |
| Número | Número actual de KMS | | 4 |
| Intervalo de activación | Intervalo entre solicitudes cuando no está activado (minutos) | | 120 |
| Intervalo de renovación | Intervalo entre solicitudes cuando está activado (minutos) | | 10 080 |
| Hora del cliente | Marca de tiempo de la solicitud | | 1/14/2006 2:30 |
| 12290 | KMS | Registro del servidor KMS para cada solicitud | Se procesó una solicitud de activación.%nInfo:%n%1 | HRESULT | Código de devolución | | 0x0 |
|  | | | | Directiva N | Número mínimo de productos que el cliente necesita para activar | | 25 |
| Equipo | Nombre del equipo cliente | | kms03.site5.contoso.com |
| CMID | Id. del equipo cliente | | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | Hora del cliente | Marca de tiempo de la solicitud | | 2006/1/14 22:36 |
| Información de VM | El SO del cliente se ejecuta en un equipo virtual | | 1 |
| Estado de licencia | Estado de licencia  0: sin licencia  1: con licencia (activado)  2: período de gracia OOB  3: OOT/Período de gracia  4: período de gracia para productos no originales  5: notificaciones  6: período de gracia extendido | | 2 |
| Tiempo antes de expiración | Tiempo restante (minutos) | | 40 123 |
| ActID | Id. de activación: identifica la licencia | | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | Falla de inicialización de KMS | El cliente de licencias por volumen no pudo inicializar el temporizador de renovación del Servicio de administración de claves.%nInfo:%n%1 | HRESULT | Código de devolución | |  |
| 12292 | KMS | Falla de inicialización del temporizador de renovación | El Servicio de administración de claves (KMS) no pudo inicializar el temporizador de renovación.%nInfo:%n%1 | HRESULT | Código de devolución | |  |
| 12293 | KMS | Falla de publicación de RR de DNS | Error de publicación del Servicio de administración de claves (KMS) a DNS en el dominio '%2'.%nInfo:%n%1 | P1: HRESULT  P2: dominio DNS | P1: código de devolución  P2: nombre de dominio DNS | | |
| 12294 | KMS | Publicación correcta de RR de DNS | La publicación del Servicio de administración de claves (KMS) a DNS en el dominio '%1' se llevó a cabo correctamente.%n | Dominio DNS | Nombre de dominio DNS |  | |

# Propiedades y métodos de WMI

En la Tabla 12, se muestran las propiedades y los métodos de WMI para la plataforma de protección de software. Las propiedades de la plataforma de protección de software se definen en el archivo %WinDir%\System32\wbem\sppwmi.mof.

Tabla 12. Propiedades y métodos de WMI para la plataforma de protección de software

|  |  |
| --- | --- |
| **//properties SoftwareLicensingService Class** | |
| **Version** | Versión del Servicio de protección de software. |
| **KeyManagementServiceMachine** | Nombre del host KMS. Devuelve un valor nulo si no se llamó a **SetKeyManagementServiceMachine**. |
| **KeyManagementServicePort** | Puerto TCP usado por los clientes para enviar solicitudes de activación KMS. Devuelve **0** si no se llamó a **SetKeyManagementServicePort**. |
| **IsKeyManagementServiceMachine** | Indica si KMS está habilitado en el equipo: **0** si es falso, **1** si es verdadero. |
| **VLActivationInterval** | Frecuencia de activación, en minutos, con la que un cliente debe ponerse en contacto con el host KMS antes de otorgar una licencia al cliente. |
| **VLRenewalInterval** | Frecuencia, en minutos, en la que un cliente debe ponerse en contacto con el host KMS después de otorgar una licencia al cliente. |
| **KeyManagementServiceCurrentCount** | Número de clientes KMS actualmente activos en el host KMS. **-1** indica que el host no está habilitado como Servicio de administración de claves o no ha recibido solicitudes de licencia de clientes. |
| **RequiredClientCount** | Cantidad mínima de clientes necesarios para conectarse a un equipo con Servicio de administración de claves y habilitar las licencias por volumen. |
| **PolicyCacheRefreshRequired** | Indica si la memoria caché de directivas de licencias debe actualizarse: **0** = actualización no requerida, **1** = actualización requerida. |
| **ClientMachineID** | Identificador único global (GUID) que identifica un cliente KMS en un host KMS. El cliente lo incluye en las solicitudes que envía al KMS. |
| **RemainingWindowsReArmCount** | Cantidad restante de veces que el cliente puede reinstalarse correctamente. |
| **KeyManagementServiceListeningPort** | Puerto TCP usado por el host KMS para buscar solicitudes de activación. |
| **KeyManagementServiceDnsPublishing** | Indica el estado de la publicación de DNS de un host KMS: **0** = deshabilitado, **1** = publicación automática habilitada (predeterminado). |
| **KeyManagementServiceLowPriority** | Indica el estado de prioridad de subproceso del servicio KMS: **0** = prioridad normal (predeterminado), **1** = prioridad baja. |
| **KeyManagementServiceHostCaching** | Indica el estado de almacenamiento en caché del nombre y el puerto del host KMS: **0** = almacenamiento en caché deshabilitado, **1** = almacenamiento en caché habilitado (predeterminado). |
| **KeyManagementServiceUnlicensedRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 0 (sin licencia). |
| **KeyManagementServiceLicensedRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 1 (con licencia). |
| **KeyManagementServiceOOBGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 2 (período de gracia OOB). |
| **KeyManagementServiceOOTGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia =3 (período de gracia OOT). |
| **KeyManagementServiceNonGenuineGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 4 (período de gracia para productos no originales). |
| **KeyManagementServiceNotificationRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 5 (notificación). |
| **KeyManagementServiceTotalRequests** | Número total de solicitudes de KMS válidas. |
| **KeyManagementServiceFailedRequests** | Número total de solicitudes de KMS no válidas. |
| **KeyManagementServiceActivationDisabled** | Indica si la activación por volumen mediante KSM está deshabilitada. |
| **//methods SoftwareLicensingProduct Class** | |
| **InstallProductKey** | Instala una clave de producto. |
| **InstallLicense** | Instala una licencia. |
| **InstallLicensePackage** | Instala un paquete de licencia para el producto actual. |
| **SetKeyManagementServiceMachine** | Establece el uso del nombre del host KMS para la activación por volumen. |
| **ClearKeyManagementServiceMachine** | Elimina los nombres de host KMS activados con anterioridad. |
| **SetKeyManagementServicePort** | Establece que el puerto TCP usado por un cliente realice solicitudes a un host KMS. Si no se especificó el valor, se usa el puerto 1688. |
| **ClearKeyManagementServicePort** | Elimina los números de puerto especificados con anterioridad. |
| **SetVLActivationInterval** | Frecuencia de activación, en minutos, con la que un cliente KMS debe ponerse en contacto con el host KMS antes de otorgar una licencia al cliente. La frecuencia debe ser ≥ 15 y ≤ 43 200. Si se llama al método y el equipo no tiene Servicio de administración de claves, se devuelve un error. |
| **SetVLRenewalInterval** | Frecuencia de renovación, en minutos, con la que un cliente KMS debe ponerse en contacto con el host KMS después de otorgar una licencia al cliente. La frecuencia debe ser ≥ 15 y ≤ 43 200. Si se llama al método y el equipo no tiene Servicio de administración de claves, se devuelve un error. |
| **ClearProductKeyFromRegistry** | Borra la clave de producto del registro. |
| **AcquireGenuineTicket** | Realiza la validación en línea que indica que es original. La llamada de este método puede cambiar el estado original del equipo. |
| **ReArmWindows** | Restablece el estado de licencia del equipo al período de gracia OOB (consulte **Estado de la licencia**).  **Nota:** Debe reiniciar el cliente para que los cambios tengan efecto. |
| **RefreshLicenseStatus** | Actualiza el estado de licencia de Windows de modo que las aplicaciones tengan acceso a información sobre las licencias actuales. |
| **SetKeyManagementServiceListeningPort** | Establece que el puerto TCP usado por el host KMS debe buscar solicitudes de activación. Se aplica solamente a los hosts KMS. Si no se especificó el valor, se usa el puerto 1688. |
| **ClearKeyManagementServiceListeningPort** | Elimina los puertos de escucha especificados con anterioridad. Se aplica solamente a los hosts KMS. |
| **DisableKeyManagementServiceDnsPublishing** | Habilitar o deshabilitar la publicación de DNS en un equipo host KMS. **0** = habilitar, **1** = deshabilitar. |
| **EnableKeyManagementServiceLowPriority** | Habilitar o deshabilitar el servicio KMS que se ejecuta con prioridad baja: **0** = deshabilitar, **1** = habilitar. |
| **DisableKeyManagementServiceHostCaching** | Habilitar o deshabilitar el almacenamiento en caché del nombre y el puerto del host KMS en el equipo cliente de activación por volumen: **0** = habilitar, **1** = deshabilitar. |
| **DisableKeyManagementServiceActivation** | Habilitar o deshabilitar la activación por volumen mediante un equipo KMS. **0** = habilitar, **1** = deshabilitar. |
| **DiscoveredKeyManagementServiceMachineName** | Nombre del último host KMS detectado mediante DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Nombre del último puerto KMS detectado mediante DNS. |
| **//properties SoftwareLicensingService Class** | |
| **ID** | Identificador del producto. |
| **Name** | Nombre del producto. |
| **Description** | Descripción del producto. |
| **ApplicationID** | Id. de aplicación del producto actual. |
| **ProcessorURL** | URL de servidor de licencias de software del certificado de proceso. |
| **MachineURL** | URL de servidor de licencias de software del certificado de enlace. |
| **ProductKeyURL** | URL de servidor de licencias de software del certificado de producto. |
| **UseLicenseURL** | URL de servidor de licencias de software de la licencia de usuario. |
| **LicenseStatus** | Estado de la licencia de esta aplicación del producto:  **0** = sin licencia, **1** = con licencia, **2** = período de gracia OOB, **3** = período de gracia OOT, **4** = período de gracia para productos no originales, **5** = notificación, **6** = período de gracia extendido. |
| **LicenseStatusReason** | El código de diagnóstico indica por qué un equipo tiene en un estado de licencia específico. |
| **GracePeriodRemaining** | Tiempo restante en minutos antes de que la aplicación principal pase al modo de notificación. Para los clientes por volumen, este es el tiempo restante antes de que sea necesario volver a llevar a cabo la activación. |
| **EvaluationEndDate** | Fecha de expiración de la aplicación de este producto. Después de esta fecha, el **Estado de la licencia** será **Sin licencia**, y no se podrá activar el producto. |
| **OfflineInstallationId** | Identificador de la aplicación de este producto que puede usarse para la activación telefónica o en línea. Devuelve un valor nulo si no está instalada la clave de producto. |
| **PartialProductKey** | Últimos cinco caracteres de la clave de este producto. Devuelve un valor nulo si no está instalada la clave de producto. |
| **ProductKeyID** | Id. de la clave de producto. Devuelve un valor nulo si no está instalada la clave de producto. |
| **LicenseFamily** | Identificador de la familia de SKU, usado para determinar las relaciones de licencia para los complementos. |
| **LicenseDependsOn** | Identificador de dependencia de la familia de SKU, usado para determinar las relaciones de licencia para los complementos. |
| **LicenseIsAddon** | Devuelve **True** si el producto se identifica como licencia de complemento. |
| **VLActivationInterval** | Frecuencia de activación, en minutos, con la que un cliente debe ponerse en contacto con el host KMS antes de otorgar una licencia. |
| **VLRenewalInterval** | Frecuencia, en minutos, con la que un cliente debe ponerse en contacto con el host KMS después de otorgar una licencia. |
| **KeyManagementServiceProductKeyID** | Id. de clave de producto de KMS. Devuelve un valor nulo si no corresponde. |
| **KeyManagementServiceMachine** | Nombre del host KMS. Devuelve un valor nulo si no se llamó a **SetKeyManagementServiceMachine**. |
| **KeyManagementServicePort** | Puerto TCP usado por los clientes para enviar solicitudes de activación KMS. Devuelve **0** si no se llamó a **SetKeyManagementServicePort**. |
| **DiscoveredKeyManagementServiceMachineName** | Nombre del último host KMS detectado mediante DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Nombre del último puerto KMS detectado mediante DNS. |
| **IsKeyManagementServiceMachine** | Indica si KMS está habilitado en el equipo: **1** si es verdadero, **0** si es falso. |
| **KeyManagementServiceCurrentCount** | Número de clientes KMS actualmente activos en el host KMS. **-1** indica que el equipo no está habilitado como Servicio de administración de claves o no ha recibido solicitudes de licencia de clientes. |
| **RequiredClientCount** | Cantidad mínima de clientes necesarios para conectarse a un equipo con Servicio de administración de claves y habilitar las licencias por volumen. |
| **KeyManagementServiceUnlicensedRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 0 (sin licencia). |
| **KeyManagementServiceLicensedRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 1 (con licencia). |
| **KeyManagementServiceOOBGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 2 (período de gracia OOB). |
| **KeyManagementServiceOOTGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia =3 (período de gracia OOT). |
| **KeyManagementServiceNonGenuineGraceRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 4 (período de gracia para productos no originales). |
| **KeyManagementServiceTotalRequests** | Número total de solicitudes de KMS válidas. |
| **KeyManagementServiceFailedRequests** | Número de solicitudes de KMS con error. |
| **KeyManagementServiceNotificationRequests** | Número de solicitudes KMS de clientes con el estado de licencia = 5 (notificación). |
| **GenuineStatus** | Estado Original de la aplicación de este producto. |
| **ExtendedGrace** | Período de gracia extendido, en minutos, antes de que la aplicación principal pase al modo sin licencia. |
| **TrustedTime** | Muestra la hora de confianza almacenada actualmente en el sistema. |
| **DisableKeyManagementServiceHostCaching** | Habilitar o deshabilitar el almacenamiento en caché del nombre y el puerto del host KMS en el equipo cliente de activación por volumen: 0 = habilitar, 1= deshabilitar. |
| **//methods SoftwareLicensingProduct Class** | |
| **UninstallProductKey** | Instala una clave de producto para el producto actual. |
| **Activate** | Activa el producto actual. |
| **DepositOfflineConfirmationId** | Activa este producto al depositar el Identificador de confirmación fuera de línea correspondiente al llevar a cabo la activación telefónica o fuera de línea. |
| **GetPolicyInformationDWord** | Obtiene información de la directiva de licencias tipo DWORD. |
| **GetPolicyInformationString** | Obtiene información de la directiva tipo cadena. |
| **SetKeyManagementServiceMachine** | Establece el uso del nombre del host KMS para la activación por volumen. |
| **ClearKeyManagementServiceMachine** | Elimina los nombres de host KMS activados con anterioridad. |
| **SetKeyManagementServicePort** | Establece que el puerto TCP usado por un cliente realice solicitudes a un host KMS. Si no se especificó el valor, se usa el puerto 1688. |
| **ClearKeyManagementServicePort** | Elimina los números de puerto especificados con anterioridad. |

# Glosario

|  |  |
| --- | --- |
| **Término** | **Definición** |
| **ACID** | GUID usado para identificar un método de activación dentro de una edición de software. |
| **AD DS** | Servicios de dominio de Active Directory |
| **Almacén de certificados del equipo** | El usuario que intenta realizar una activación basada en token debe tener acceso a este certificado y a su clave privada. |
| **AppID** | GUID definido para agrupar un conjunto de Id. de SKU como un nombre de grupo. Todas las ediciones de Windows tienen el mismo AppID. |
| **Directiva N** | Directiva de licencias que especifica la cantidad mínima de equipos devueltos por un KMS y que el cliente usará para determinar si realiza su propia activación. |
| **DNS** | Servicio de nombres de dominios. |
| **FQDN** | Nombre de dominio completo (por ejemplo, phred.microsoft.com). |
| **GVLK** | Clave de licencia por volumen genérico: una clave de producto específica de la edición, que se instala en todas las ediciones de volumen de Windows, de forma predeterminada. Además, se la conoce como clave de configuración del cliente KMS. Para obtener más información, consulte la Tabla 9. |
| **Id de SKU** | Igual que lo especificado para ACID. |
| **KMS** | Servicio de administración de claves. |
| **KMSID** | GUID enviado por el CLIENTE KMS para la activación mediante un host KMS. Puede ser compartido por múltiples ACID. |
| **MAK** | Clave de activación múltiple. |
| **PIN** | Número de identificación personal; se usa con una tarjeta inteligente como credencial de autenticación. |
| **SKU** | Describe una edición distinta de Windows o de otro software. |
| **SPPSVC** | Servicio de protección de software: es la plataforma de servicio incorporada de Windows 7 y Windows Server 2008 R2, que administra las actividades de licencia de Windows y otras aplicaciones. |
| **SRV** | Tipo de registro de recursos compatible con DNS (consulte Solicitud de comentarios [RFC] 2782). |
| **Token** | Se usan un certificado x509 y su clave privada para activar Windows en equipos habilitados para la activación con token. |
| **VL** | Licencias por volumen. |
| **WMI** | Instrumental de administración de Windows. |

# Vínculos de recursos

* Volume Activation:
* Volume Activation en TechNet: <http://go.microsoft.com/fwlink/?LinkId=150083>
* Servicio de administración de claves 1.2 para Windows Server 2003 SP1 y posterior: <http://go.microsoft.com/fwlink/?LinkId=155083>
* Activación de productos e información sobre claves: <http://go.microsoft.com/fwlink/?LinkId=74008>
* Guía de implementación de Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=150083>
* Guía de operaciones de Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=150084>
* Guía de planificación de Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=155926>
* Guía de referencia técnica de Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=152550>
* Herramientas de implementación:
* Kit de instalación automatizada de Windows (Windows AIK) para Windows 7: <http://go.microsoft.com/fwlink/?LinkId=136976>
* Herramientas de administración:
* Catálogo de System Center Pack: <http://go.microsoft.com/fwlink/?LinkID=110332>
* Licencias por volumen:
* Software original de Microsoft: <http://go.microsoft.com/fwlink/?LinkId=151993>
* Página de validación del software original de Microsoft: <http://go.microsoft.com/fwlink/?LinkId=64187>
* Números telefónicos de los centros de activación de Microsoft de todo el mundo: <http://go.microsoft.com/fwlink/?LinkId=107418>
* Licencias por volumen de Microsoft: <http://go.microsoft.com/fwlink/?LinkId=73076>
* Centro de Servicios de licencias por volumen de Microsoft: <http://go.microsoft.com/fwlink/?LinkId=107544>
* Aspectos importantes del aviso de privacidad de Windows Vista: <http://go.microsoft.com/fwlink/?LinkID=52526>