

# **Guide de déploiement de Volume Activation Windows 7 et Windows Server 2008 R2**

Microsoft Corporation

Date de publication : Juin 2009

## **Résumé**

Volume Activation permet aux clients détenteurs de contrats de licence en volume d'automatiser et de gérer le processus d'activation. Le présent document s'adresse aux analystes programmeurs qui ont planifié le déploiement de Volume Activation et sont maintenant prêts à examiner et à appliquer les procédures requises pour ce déploiement.

---

Le présent document et tout autre document auquel il est fait référence sont fournis à titre informatif uniquement. Microsoft exclut toute garantie, expresse ou tacite, en ce qui concerne ce document. Les informations contenues, y compris les URL et références à des sites Internet, sont sujettes à modification sans préavis. L'utilisateur assume entièrement le risque lié à l'utilisation et aux résultats de l'utilisation de ce document. Sauf indication contraire, les sociétés, organisations, produits, noms de domaine, adresses électroniques, logos, personnes, lieux et événements donnés en exemple dans le présent document sont entièrement fictifs. Toute ressemblance avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel serait fortuite et involontaire. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicables dans son pays. Sans préjudice aux droits d'auteur, aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans l'autorisation expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, de droits d'auteur ou d'autres droits de propriété intellectuelle portant sur tout ou partie des éléments faisant l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture du présent document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Windows, Windows Server et Windows Vista sont des marques du groupe de sociétés Microsoft. Les noms des sociétés et produits existants mentionnés peuvent être des marques de leur détenteur respectif.

---

## Table des matières

Table des matières .....	3
Introduction .....	5
Activation KMS .....	6
Configuration des hôtes KMS .....	6
Exécution de SImgr.vbs à distance .....	9
Configuration du Pare-feu Windows pour l'utilisation du script Software License Manager à distance .....	10
Exécution à distance sur les ordinateurs d'un groupe de travail .....	11
Configuration du système DNS .....	11
Modification des autorisations DNS par défaut des enregistrements SRV .....	12
Publication dans plusieurs domaines DNS .....	13
Création manuelle d'enregistrements SRV dans le DNS .....	15
Création manuelle d'enregistrements SRV dans un serveur DNS BIND 8.2 ou supérieur .....	16
Désactivation de la publication des enregistrements SRV KMS dans le DNS .....	17
Installation des hôtes KMS .....	18
Configuration des clients KMS .....	19
Spécification manuelle d'un hôte KMS .....	20
Activation de la découverte automatique pour un client KMS .....	21
Ajout d'entrées avec suffixe sur les clients KMS .....	22
Déploiement des clients KMS .....	23
Activation manuelle d'un client KMS .....	24
Conversion de clients MAK en KMS et de clients KMS en MAK .....	25
Conversion de versions commerciales vers Volume Activation .....	26
Activation MAK .....	27
Conversion de clients KMS en activation MAK .....	27
Installation d'une clé MAK pendant l'installation du système d'exploitation .....	28
Installation d'une clé MAK après l'installation du système d'exploitation .....	29
Désactivation de l'activation automatique .....	30
Activation des clients MAK .....	30
Activation des clients MAK sur Internet .....	31
Activation des clients MAK par le biais d'un serveur proxy .....	32
Activation des clients MAK par téléphone .....	33
Activation des clients MAK à l'aide de l'outil VAMT .....	34
Désactivation de l'activation automatique .....	35
Intégration des MAK avec Deployment Workbench .....	35

---

Réactivation d'ordinateurs .....	36
Annexe A : configurations facultatives .....	37
Autorisation de l'activation par utilisateur standard .....	37
Désactivation des notifications d'activation .....	37
Modifications de clé de registre pour les fonctions d'activation .....	38
Annexe B : exemple de fichier d'installation sans assistance .....	39

---

## Introduction

Le présent guide décrit les concepts de déploiement de Microsoft® Volume Activation. Volume Activation se compose de deux technologies, service de gestion de clés (KMS, Key Management Service) et clé d'activation multiple (MAK, Multiple Activation Key), qui permettent aux clients détenteurs de licences en volume d'activer les éditions sous licence en volume des systèmes d'exploitation Windows® 7 et Windows Server® 2008 R2. Pour plus d'informations sur les licences en volume, consultez le site du Centre de gestion des licences en volume, accessible à l'adresse <https://www.microsoft.com/licensing/servicecenter/>.

Lorsqu'une organisation prévoit d'utiliser Volume Activation, elle doit choisir entre la technologie KMS, la technologie MAK et une combinaison de ces deux méthodes. Les méthodes d'activation adoptées dépendent des besoins de l'organisation et de l'infrastructure réseau. Pour plus d'informations sur la planification d'un déploiement de Volume Activation, reportez-vous au document [Guide de planification de Volume Activation](#).

**Remarque** : le présent document décrit la procédure de déploiement de Volume Activation pour les systèmes d'exploitation Windows 7 et Windows Server 2008 R2. Il évoque également l'interopérabilité entre les deux générations de produits. Pour plus d'informations sur le déploiement de Volume Activation pour Windows Vista® et Windows Server 2008, reportez-vous à la page (en anglais) <http://go.microsoft.com/fwlink/?LinkID=75674>.

**Remarque** : le présent guide décrit des procédures qui exécutent des scripts et modifient le registre. Ces droits peuvent être délégués à des analystes programmeurs sélectionnés ; il est même possible d'attribuer des droits de modification de clés de produit et d'activation aux utilisateurs, bien que cette approche soit déconseillée par Microsoft.

Si l'activation échoue, reportez-vous au [Guide des opérations de Volume Activation](#) pour obtenir de l'aide concernant la résolution des problèmes. Ce guide répertorie notamment différents codes d'erreur et décrit les procédures de résolution des problèmes courants.

---

## Activation KMS

L'activation KMS ne requiert qu'un minimum de tâches d'administration. Si l'environnement réseau utilise le système de noms de domaine dynamique (DDNS, Dynamic Domain Name System) et autorise les ordinateurs à publier des services automatiquement, le déploiement d'un hôte KMS peut s'effectuer quasiment sans effort. Si l'organisation dispose de plusieurs hôtes KMS ou que le réseau ne prend pas en charge le système DDNS, des tâches de configuration supplémentaires pourront se révéler nécessaires.

**Avertissement** : certaines procédures de cette section requièrent la modification du registre. Toute modification incorrecte du registre par le biais de l'Éditeur du Registre ou d'une autre méthode risque d'entraîner certains problèmes qui pourraient même nécessiter la réinstallation du système d'exploitation. Microsoft ne garantit pas que ces problèmes puissent être résolus. Les informaticiens sont seuls responsables des conséquences découlant de la modification du registre.

Le reste de cette section décrit les tâches clés suivantes :

1. Configuration des hôtes KMS
2. Configuration du système DNS
3. Installation des hôtes KMS
4. Configuration des clients KMS

## Configuration des hôtes KMS

Software License Manager, parfois désigné sous le terme *SL Manager* (Slmgr.vbs), est un script permettant de configurer et de récupérer des informations concernant Volume Activation. Ce script est exécutable localement sur l'ordinateur cible ou à distance depuis un autre ordinateur, mais doit être exécuté à partir d'une invite de commandes avec élévation de privilèges. Si un utilisateur standard exécute Slmgr.vbs, certaines données de licence risquent d'être incomplètes ou incorrectes et de nombreuses opérations sont interdites.

Slmgr.vbs peut utiliser le moteur de script Wscript.exe ou Cscript.exe et les administrateurs ont la possibilité de spécifier le moteur à utiliser. Si aucun moteur de script n'est spécifié, Slmgr.vbs s'exécute à l'aide du moteur de script par défaut, wscript.exe.

---

**Remarque** : KMS requiert une exception de pare-feu sur l'hôte KMS. Si vous utilisez le port TCP par défaut, activez l'exception de trafic KMS dans le Pare-feu Windows. Si vous utilisez un autre pare-feu, ouvrez le port TCP 1688. En cas d'utilisation d'un port différent de celui par défaut, ouvrez le port TCP personnalisé dans le pare-feu.

La prise en compte des modifications requiert le redémarrage du service de gestion de licences des logiciels. Pour redémarrer ce service, utilisez le composant logiciel enfichable des services Microsoft Management Console (MMC) ou exécutez la commande ci-après à partir d'une invite de commandes avec élévation de privilèges :

```
net stop sppsvc && net start sppsvc
```

Slmgr.vbs requiert au moins un paramètre. Si le script est exécuté sans paramètres, il affiche des informations d'aide. Le Tableau 1 répertorie les options de ligne de commande du script Slmgr.vbs avec leur description. La plupart des paramètres du Tableau 1 configurent l'hôte KMS. Toutefois, les paramètres */sai* et */sri* sont transmis aux clients KMS une fois que ces derniers ont établi le contact avec l'hôte. La syntaxe générale de Slmgr.vbs est la suivante :

```
slmgr.vbs /paramètre
```

**Tableau 1 : paramètres Slmgr.vbs**

Paramètre	Description
<i>/sprt NuméroPort</i>	Sélectionnez le port de communication TCP sur un hôte KMS. Remplacez <i>NuméroPort</i> par le numéro de port TCP à utiliser. La valeur par défaut est <b>1688</b> .
<i>/cdns</i>	Désactive la publication automatique d'un hôte KMS dans le DNS.
<i>/sdns</i>	Active la publication automatique d'un hôte KMS dans le DNS.
<i>/cpri</i>	Abaisse la priorité des processus d'hôtes KMS.
<i>/spri</i>	Définit la priorité des processus d'hôtes KMS sur <b>Normal</b> .
<i>/sai IntervalleActivation</i>	Modifie la fréquence à laquelle un client KMS tente de s'activer lorsqu'il ne trouve aucun hôte KMS. Remplacez <i>IntervalleActivation</i> par un nombre de minutes. La valeur par défaut est <b>120</b> .

---

Paramètre	Description
<i>/sri</i> <i>IntervalleRenouvellement</i>	Modifie la fréquence à laquelle un client KMS tente de renouveler son activation en contactant un hôte KMS. Remplacez <i>IntervalleRenouvellement</i> par un nombre de minutes. La valeur par défaut est <b>10080</b> (7 jours). Ce paramètre prévaut sur les paramètres locaux des clients KMS.
<i>/dli</i>	Récupère le nombre d'activations KMS actuel auprès de l'hôte KMS.



---

## Exécution de SImgr.vbs à distance

Pour exécuter SImgr.vbs à distance, les administrateurs doivent spécifier des paramètres supplémentaires. Il leur faut notamment inclure le nom de l'ordinateur cible, ainsi qu'un nom d'utilisateur et un mot de passe de compte d'utilisateur doté de droits d'administrateur local sur l'ordinateur cible. Si le script est exécuté à distance sans nom d'utilisateur et mot de passe spécifiés, il utilise les informations d'identification de l'utilisateur qui l'exécute.

La syntaxe ci-après présente les paramètres supplémentaires requis pour l'exécution de SImgr.vbs à distance :

```
slmgr.vbs NomOrdinateurCible [NomUtilisateur] [MotdePasse]  
/paramètre [options]
```

---

## Configuration du Pare-feu Windows pour l'utilisation du script Software License Manager à distance

Slmgr.vbs utilisant l'Infrastructure de gestion Windows (WMI, Windows Management Instrumentation), les administrateurs doivent configurer le Pare-feu Windows afin d'autoriser le trafic WMI :

- Dans le cas d'un sous-réseau unique, autorisez l'exception **Windows Management Instrumentation (WMI)** dans le Pare-feu Windows.
- Pour autoriser le trafic WMI sur plusieurs sous-réseaux, autorisez la connexion pour **Windows Management Instrumentation (ASync-In)**, **Windows Management Instrumentation (DCOM-In)** et **Windows Management Instrumentation (WMI-In)**. Autorisez également un accès distant dans l'étendue. Configurez ces paramètres par le biais de l'option Pare-feu Windows avec sécurité avancée, accessible dans le dossier Outils d'administration.

**Remarque** : par défaut, les exceptions du Pare-feu Windows dans les profils Privé et Public s'appliquent uniquement aux exceptions du trafic émanant du sous-réseau local. Pour étendre l'exception à plusieurs sous-réseaux, modifiez les paramètres d'exception dans l'option Pare-feu Windows avec sécurité avancée ou, en cas de jonction à un domaine AD DS (services de domaine Active Directory), choisissez le Profil de domaine.

---

## Exécution à distance sur les ordinateurs d'un groupe de travail

Les administrateurs peuvent autoriser l'exécution à distance du script SImgr.vbs sur des ordinateurs appartenant à un groupe de travail. Pour effectuer cette opération, créez une valeur **DWORD** nommée **LocalAccountTokenFilterPolicy** dans la sous-clé de registre

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** sur les clients KMS. Puis définissez cette valeur sur **0x01**.

## Configuration du système DNS

Les sections qui suivent décrivent les concepts de configuration du DNS pour l'utilisation de Volume Activation :

- Si vous utilisez plusieurs hôtes KMS, reportez-vous à la section « Modification des autorisations DNS par défaut des enregistrements SRV ».
- Pour permettre aux clients KMS utilisant différents serveurs DNS de trouver les hôtes KMS, reportez-vous à la section « Publication dans plusieurs domaines DNS ».
- Pour ajouter manuellement des enregistrements de ressource SRV pour les hôtes KMS, reportez-vous aux sections « Création manuelle d'enregistrements SRV dans le DNS », « Création manuelle d'enregistrements SRV dans un serveur DNS BIND 8.2 ou supérieur » et « Désactivation de la publication des enregistrements SRV KMS dans le DNS ».

**Remarque** : il est possible que les modifications du DNS ne soient pas reflétées tant que tous les serveurs DNS n'ont pas été répliqués.

---

## Modification des autorisations DNS par défaut des enregistrements SRV

Si vous n'utilisez qu'un seul hôte KMS, la configuration d'autorisations dans le DNS peut se révéler inutile. Le comportement par défaut consiste à autoriser un ordinateur à créer un enregistrement de ressource SRV, puis à le mettre à jour.

Toutefois, si vous disposez de plusieurs hôtes KMS (cas le plus courant), les autres hôtes ne pourront pas mettre à jour l'enregistrement de ressource SRV, sauf en cas de modification des autorisations SRV par défaut.

La procédure de haut niveau ci-après est un exemple issu du propre environnement de Microsoft. Elle ne comporte pas d'étapes détaillées (celles-ci pouvant varier d'une organisation à l'autre) et ne constitue pas le seul moyen d'obtenir le résultat souhaité :

1. Créez dans Active Directory® un groupe de sécurité global qui sera utilisé pour vos hôtes KMS. Par exemple, créez *Groupe KMS*.
2. Ajoutez chacun de vos hôtes KMS à ce groupe. Les hôtes doivent tous être joints au même domaine.
3. Une fois le premier hôte KMS créé, ce dernier génère l'enregistrement SRV d'origine. Si le premier hôte KMS ne parvient pas à créer l'enregistrement de ressource SRV, ce problème peut découler de la modification des autorisations par défaut par votre organisation. Si tel est le cas, créez l'enregistrement de ressource SRV manuellement en suivant les instructions de la section « Création manuelle d'enregistrements SRV dans le DNS ».
4. Définissez les autorisations du groupe SRV pour permettre aux membres du groupe de sécurité global d'effectuer des mises à jour.

**Remarque** : un administrateur de domaine peut déléguer l'exécution des étapes qui précèdent à des administrateurs de l'organisation. Pour effectuer cette opération, créez un groupe de sécurité dans Active Directory, autorisez ce groupe à modifier les enregistrements SRV, puis ajoutez-y les délégués.

---

## Publication dans plusieurs domaines DNS

Par défaut, l'hôte KMS est uniquement enregistré dans le domaine DNS auquel il appartient. Si l'environnement réseau ne comporte qu'un seul domaine DNS, aucune autre action n'est requise.

Si vous disposez de plusieurs noms de domaine DNS, vous pouvez créer une liste de domaines DNS qu'un hôte KMS utilisera en publiant son enregistrement de ressource SRV. En définissant cette valeur de registre, vous annulez le comportement par défaut de l'hôte KMS qui consiste à restreindre la publication au domaine spécifié comme suffixe DNS principal.

En outre, ajoutez les paramètres *priority* et *weight* à la valeur de registre **DnsDomainPublishList** pour KMS. Cette fonction permet à un administrateur d'établir des groupements de priorités d'hôte KMS et une pondération dans chaque groupe pour définir l'hôte KMS à tenter en premier et pour équilibrer le trafic entre les différents hôtes KMS.

**Remarque** : il est possible que les modifications du DNS ne soient pas reflétées tant que tous les serveurs DNS n'ont pas été répliqués. Des modifications trop fréquentes (durée < intervalle de réplication) risquent de laisser d'anciens enregistrements si ces modifications sont effectuées sur un serveur non répliqué.

Pour publier automatiquement un hôte KMS dans plusieurs domaines DNS, ajoutez le suffixe de chaque domaine DNS dans lequel publier l'hôte KMS dans la valeur de registre multichaîne **DnsDomainPublishList in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**. Après avoir modifié cette valeur, redémarrez le service de gestion de licences des logiciels pour créer les enregistrements de ressource SRV.

**Remarque** : cette clé a été transférée depuis l'emplacement de Windows Vista® **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.

Après avoir configuré la publication d'un hôte KMS dans plusieurs domaines, exportez la clé de registre, puis importez-la dans le registre des autres hôtes KMS. Pour vous assurer que cette procédure a réussi, vérifiez le journal des événements d'application sur chaque hôte KMS. L'ID d'événement 12294 indique que l'hôte KMS

---

est parvenu à créer les enregistrements de ressource SRV. L'ID d'événement 12293 signale que la tentative de création des enregistrements SRV a échoué. Pour obtenir la liste complète des codes d'erreur, reportez-vous au [Guide des opérations de Volume Activation](#).

---

## Création manuelle d'enregistrements SRV dans le DNS

Si l'environnement ne prend pas en charge le DDNS, vous devez créer les enregistrements de ressource SRV manuellement pour la publication de l'hôte KMS. Les environnements ne prenant pas en charge le DDNS doivent désactiver la publication sur tous les hôtes KMS pour empêcher les journaux des événements de collecter les événements d'échec de publication DNS. Pour désactiver la publication automatique, utilisez le script SImgr.vbs avec l'option de ligne de commande **/cdns**. Pour plus d'informations sur le script SImgr.vbs, reportez-vous à la section « Configuration des hôtes KMS ».

**Remarque** : les enregistrements de ressource SRV créés manuellement peuvent coexister avec ceux que les hôtes KMS publient automatiquement dans d'autres domaines, à condition que tous les enregistrements soient gérés de façon à éviter les conflits.

Dans la zone de recherche directe appropriée du Gestionnaire DNS, créez un nouvel enregistrement de ressource SRV à l'aide des informations d'emplacement adéquates. Par défaut, KMS écoute sur le port TCP 1688, et le service est `_VLMCS`. Le Tableau 2 présente un exemple de paramétrage d'un enregistrement de ressource SRV.

**Tableau 2 : enregistrement de ressource SRV**

Nom	Valeur
Service	<code>_VLMCS</code>
Protocole	<code>_TCP</code>
Numéro de port	1688
Hôte offrant le service	Nom de domaine complet (FQDN) de l'hôte KMS

---

## Création manuelle d'enregistrements SRV dans un serveur DNS BIND 8.2 ou supérieur

Si l'organisation utilise un serveur DNS non-Microsoft, vous pouvez créer les enregistrements de ressource SRV requis à condition que le serveur DNS soit conforme à Berkeley Internet Name Domain (BIND) 8.2 ou supérieur. Lorsque vous créez l'enregistrement, spécifiez les informations figurant dans le Tableau 3. Les paramètres **Priority** et **Weight** présentés dans ce tableau sont uniquement utilisés par Windows 7 et Windows Server 2008 R2.

**Tableau 3 : informations d'enregistrement de ressource SRV**

Nom	Valeur
Name	_vlmcs._tcp
Type	SRV
Priority	0
Weight	0
Port	1688
Hostname	Nom de domaine complet (FQDN) de l'hôte KMS

Pour configurer un serveur DNS BIND 8.2 ou supérieur pour la prise en charge de la publication KMS automatique, configurez le serveur BIND de façon à activer les mises à jour d'enregistrements de ressource à partir des hôtes KMS. Par exemple, ajoutez la ligne ci-après à la définition de zone dans `named.conf` :

```
allow-update { any; };
```

**Remarque** : il est également possible d'ajouter une instruction `allow-update` à `named.conf.options` afin d'autoriser le DDNS pour toutes les zones hébergées sur ce serveur.



---

## Désactivation de la publication des enregistrements SRV KMS dans le DNS

Les hôtes KMS publient automatiquement leur existence en créant des enregistrements de ressource SRV dans le DNS. Pour désactiver la publication automatique d'un hôte KMS dans le DNS, utilisez le script SImgr.vbs avec l'option de ligne de commande **/cdns**.

La désactivation de la publication automatique dans le DNS au moyen du script SImgr.vbs est recommandée, mais vous pouvez également effectuer cette tâche en créant dans le registre une valeur **DWORD** nommée **DisableDnsPublishing**, puis en lui attribuant la valeur **1**. Cette valeur figure à l'emplacement **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** dans le registre. Pour réactiver le comportement par défaut de publication des enregistrements SRV KMS dans le DNS, configurez la valeur sur **0**.

---

## Installation des hôtes KMS

Pour activer la fonctionnalité KMS, une clé KMS est installée sur un hôte KMS, puis ce dernier est activé sur Internet ou par téléphone à l'aide des services d'activation de Microsoft. Les ordinateurs exécutant Windows 7 ou Windows Server 2008 R2 peuvent jouer le rôle d'hôtes KMS.

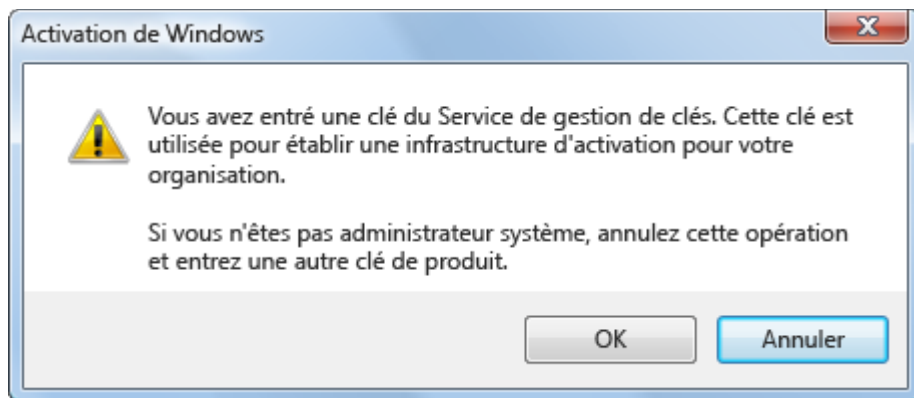
Les ordinateurs exécutant Windows Vista, Windows Server 2003 et Windows Server 2008 peuvent également servir d'hôtes KMS. Les clients KMS activables par un hôte KMS dépendent de la clé d'hôte utilisée pour l'activation de l'hôte. Pour plus d'informations sur les clés d'hôte KMS, reportez-vous au document [Guide de planification de Volume Activation](#).

Installez et activez une clé KMS sur un ordinateur Windows 7 ou Windows Server 2008 R2 en utilisant une invite de commandes avec élévation de privilèges :

- Pour installer une clé KMS, tapez **slmgr.vbs /ipk <CléKMS>** à partir d'une invite de commandes.
- Pour activer la clé en ligne, tapez **slmgr.vbs /ato** à partir d'une invite de commandes.
- Pour activer la clé par téléphone, tapez **slui.exe 4** à partir d'une invite de commandes.

Après avoir activé la clé KMS, redémarrez le service de protection logicielle.

Windows 7 et Windows Server 2008 R2 affichent le message d'avertissement présenté à la Figure 1 chaque fois que les administrateurs installent une clé d'hôte KMS à l'aide de l'interface utilisateur (les utilisateurs n'obtiennent pas ce message s'ils installent une clé d'hôte KMS au moyen du script Slmgr.vbs). Ce message empêche toute installation accidentelle d'une clé KMS sur des ordinateurs non destinés à être définis comme hôtes KMS par les administrateurs.



**Figure 1 : message d'avertissement concernant la clé KMS**

Pour vous assurer que l'hôte KMS est correctement configuré, vérifiez si le décompte KMS augmente. Dans la fenêtre Invite de commandes sur l'hôte KMS, tapez **slmgr.vbs /dli** pour afficher le décompte KMS actuel. Les administrateurs peuvent également rechercher l'ID d'événement 12290 dans le journal du service de gestion de clés situé dans le dossier Journaux des applications et des services. Ce journal enregistre les demandes d'activation des clients KMS. Chaque événement affiche le nom de l'ordinateur et l'horodatage de chaque demande d'activation.

## Configuration des clients KMS

Cette section décrit les concepts d'installation et de configuration d'ordinateurs en tant que clients KMS. Par défaut, les éditions sous licence en volume de Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2 constituent des clients KMS. Si les ordinateurs que l'organisation souhaite activer par la méthode KMS utilisent l'un de ces systèmes d'exploitation et que le réseau autorise la découverte automatique DNS, aucune configuration supplémentaire n'est requise.

Si un client KMS est configuré pour la recherche d'un hôte KMS à l'aide du DNS mais ne reçoit aucun enregistrement SRV du DNS, Windows 7 et Windows Server 2008 R2 consignent cette erreur dans le journal des événements.

---

## Spécification manuelle d'un hôte KMS

Les administrateurs peuvent attribuer manuellement un hôte KMS à des clients KMS en utilisant la mise en cache de l'hôte KMS. L'attribution manuelle d'un hôte KMS désactive la découverte automatique de KMS sur le client KMS. Vous pouvez attribuer manuellement un hôte KMS à un client KMS en exécutant la commande :

```
slmgr.vbs /skms <valeur>:<port>
```

où *valeur* correspond aux données *KMS\_FQDN*, *IPv4Address* ou *NetbiosName* de l'hôte KMS et où *port* est le port TCP de l'hôte KMS.

---

## **Activation de la découverte automatique pour un client KMS**

Par défaut, les clients KMS tentent automatiquement de détecter les hôtes KMS. Vous pouvez désactiver la fonction de découverte automatique en attribuant manuellement un hôte KMS à un client KMS. Cette action supprime également le nom d'hôte KMS du cache du client KMS. Si la découverte automatique est désactivée, vous pouvez la réactiver en exécutant **slmgr.vbs /ckms** à partir d'une invite de commandes.

---

## **Ajout d'entrées avec suffixe sur les clients KMS**

En ajoutant l'adresse d'un serveur DNS contenant l'enregistrement de ressource SRV sous la forme d'une entrée avec suffixe sur les clients KMS, les administrateurs peuvent publier des hôtes KMS sur un même serveur DNS et permettre la détection de ce dernier par des clients KMS configurés avec d'autres serveurs DNS principaux. Pour plus d'informations sur la configuration d'une liste de recherche de suffixes de domaine sur les clients KMS, reportez-vous à l'article du site Microsoft Aide et Support « Comment faire pour configurer une liste de recherche de suffixe de domaine sur les clients DNS (Domain Name System) », accessible à l'adresse <http://support.microsoft.com/kb/275553>.

---

## Déploiement des clients KMS

Les informations de cette section sont destinées aux clients détenteurs de licences en volume qui utilisent le Kit d'installation automatisée (ou Windows AIK, Windows Automated Installation Kit) pour déployer et activer un système d'exploitation Windows. Préparez les clients KMS pour le déploiement en utilisant l'Outil de préparation système (Sysprep) ou le script SImgr.vbs :

- **Sysprep.** Avant de capturer une image, exécutez Sysprep avec l'option de ligne de commande **/generalize** pour réinitialiser le compteur d'activation, l'identificateur de sécurité (SID), ainsi que d'autres paramètres importants. La réinitialisation du compteur d'activation empêche la période de grâce de l'image d'arriver à expiration avant le déploiement de l'image. L'exécution de Sysprep.exe ne supprime pas la clé de produit installée, et les administrateurs ne sont pas invités à fournir une nouvelle clé durant la mini-installation. Si aucun réarmement ne subsiste, l'opération Sysprep s'achève, mais les compteurs d'activation ne sont pas modifiés et une erreur décrivant la situation est renvoyée.
- **SImgr.vbs.** Lors de la création d'ordinateurs virtuels de démonstration à des fins d'utilisation interne (par exemple, pour le service des ventes de l'organisation ou pour configurer un environnement de formation temporaire), l'exécution du script SImgr.vbs avec l'option de ligne de commande **/rearm** allonge la période de grâce de 30 jours supplémentaires, ce qui réinitialise le compteur d'activation mais n'entraîne aucune autre modification sur l'ordinateur. Le compteur d'activation peut être réinitialisé à trois reprises pour les ordinateurs exécutant Windows 7 ou Windows Server 2008 R2.

---

## Activation manuelle d'un client KMS

Par défaut, les clients KMS tentent automatiquement de s'activer à intervalles prédéfinis. Pour activer manuellement des clients KMS (des clients déconnectés, par exemple) avant de les distribuer aux utilisateurs, utilisez l'option Système du Panneau de configuration ou exécutez **slmgr.vbs /ato** à partir d'une invite de commandes avec élévation de privilèges. Le script Slmgr.vbs signale la réussite ou l'échec de l'activation et fournit un code de résultat. L'activation exige que le client KMS ait accès à un hôte KMS sur le réseau de l'organisation.



---

## Conversion de clients MAK en KMS et de clients KMS en MAK

Par défaut, les systèmes d'exploitation Windows 7 et Windows Server 2008 R2 utilisent KMS pour l'activation. Pour convertir des clients KMS existants en clients MAK, il vous suffit d'installer une clé MAK. De la même façon, pour convertir des clients MAK en clients KMS, exécutez la commande :

```
slmgr.vbs /ipk <CléInstallationKMS>
```

où *CléInstallationKMS* est l'une des clés d'installation figurant dans le Tableau 4. Après avoir installé la clé d'installation KMS, activez le client KMS en exécutant **cscrip slmgr.vbs /ato**.

**Tableau 4 : clés d'installation de client KMS**

Édition du système d'exploitation	Clé de produit
<b>Windows 7</b>	
Windows 7 Professionnel	FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4
Windows 7 Professionnel N	MRPKT-YTG23-K7D7T-X2JMM-QY7MG
Windows 7 Entreprise	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH
Windows 7 Entreprise N	YDRBP-3D83W-TY26F-D46B2-XCKRJ
Windows 7 Entreprise E	C29WB-22CC8-VJ326-GHFJW-H9DH4
<b>Windows Server 2008 R2</b>	
Windows Server 2008 R2 Édition HPC	FKJQ8-TMCVP-FRMR7-4WR42-3JCD7
Windows Server 2008 R2 Datacenter	74YFP-3QFB3-KQT8W-PMXWJ-7M648
Windows Server 2008 R2 Entreprise	489J6-VHDMP-X63PK-3K798-CPX3Y
Windows Server 2008 R2 pour les systèmes Itanium	GT63C-RJFQ3-4GMB6-BRFB9-CB83V
Windows Server 2008 R2 Standard	YC6KT-GKW9T-YTKYR-T4X34-R7VHC
Windows Web Server 2008 R2	6TPJF-RBVHG-WBW2R-86QPH-6RTM4

---

## Conversion de versions commerciales vers Volume Activation

Les versions commerciales de Windows 7 Professionnel et de Windows Server 2008 R2 peuvent être converties en clients KMS, à condition que l'organisation ait acquis les licences en volume appropriées et se conforme aux droits d'utilisation des produits. Pour convertir Windows 7 Professionnel et toutes les éditions commerciales de Windows Server 2008 R2 en clients KMS, ignorez la page **Clé du produit** lors de l'installation du système d'exploitation. Une fois l'installation terminée, ouvrez une fenêtre Invite de commandes avec élévation de privilèges, puis tapez la commande :

```
Slmgr.vbs /ipk <CléInstallation>
```

où *CléInstallation* est la clé d'installation de client KMS figurant dans le Tableau 4 qui correspond à l'édition de Windows 7 ou de Windows Server 2008 R2.

---

## **Activation MAK**

L'activation MAK est utilisée dans le cadre d'une activation unique n'exigeant aucun renouvellement par l'intermédiaire des services d'activation hébergés de Microsoft. Pour plus d'informations sur l'activation MAK, reportez-vous au document [Guide de planification de Volume Activation](#).

## **Conversion de clients KMS en activation MAK**

Windows 7 et Windows Server 2008 R2 s'installent automatiquement en tant que clients KMS. Pour convertir un client KMS en activation MAK, installez une clé MAK. Vous pouvez installer une clé MAK pendant l'installation du système d'exploitation ou à tout moment par la suite.

Vous pouvez installer une clé MAK sur une image de référence de Windows 7 et de Windows Server 2008 R2 pour que toutes les installations effectuées depuis cette image utilisent l'activation MAK plutôt que l'activation KMS par défaut. Cette opération élimine la nécessité de spécifier une clé MAK dans un fichier d'installation sans assistance.

---

## Installation d'une clé MAK pendant l'installation du système d'exploitation

Les administrateurs peuvent convertir un client KMS en client MAK pendant l'installation initiale de Windows 7 ou de Windows Server 2008 R2 en incluant une clé MAK dans un fichier d'installation sans assistance (Unattend.xml). Le fichier Unattend.xml est utilisable avec Setup.exe ou avec les services de déploiement Windows. Pour plus d'informations, reportez-vous au fichier d'aide (en anglais) *Unattended Windows Setup Reference* (Guide de référence de l'installation sans assistance utilisateur de Windows) de Windows AIK, accessible à l'adresse <http://www.microsoft.com/downloads/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&displaylang=fr>. Pour visualiser un exemple de fichier d'installation sans assistance, reportez-vous à la section « Annexe B : exemple de fichier d'installation sans assistance ».

**Remarque** : la clé MAK est stockée en texte clair dans le fichier Unattend.xml. Lors d'une installation sans assistance, le fichier Unattend.xml ou AutoUnattend.xml est copié dans le dossier %SystemRoot%\Panther de l'ordinateur cible. Toutefois, à la fin du processus d'installation, le programme remplace cette information par la mention « SENSITIVE\*DATA\*DELETED ».

---

## Installation d'une clé MAK après l'installation du système d'exploitation

Vous pouvez configurer une édition en volume de Windows 7 et de Windows Server 2008 R2 pour l'activation MAK en utilisant l'option Système du Panneau de configuration ou en exécutant le script SImgr.vbs :

- Pour installer une clé MAK à l'aide de l'application Système, cliquez sur le lien **Changer la clé du produit**, puis tapez la clé MAK dans la boîte de dialogue **Changer de clé de produit pour l'activation**.
- Pour installer une clé MAK par le biais du script SImgr.vbs, exécutez la commande ci-après à partir d'une invite de commandes :

```
slmgr.vbs /ipk <CléActivationMultiple>
```

où *CléActivationMultiple* correspond à la clé MAK.

Si les utilisateurs installent une clé MAK à l'aide de l'interface utilisateur, le client MAK tente de s'activer une seule fois sur Internet. En cas d'installation d'une clé MAK au moyen du script SImgr.vbs, le client MAK ne tente pas de s'activer automatiquement.

---

## Désactivation de l'activation automatique

Pour désactiver l'activation automatique sur un client MAK, définissez la valeur de registre **DWORD** nommée **Manual** sur **1**. Cette valeur figure dans la sous-clé de registre **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Activation des clients MAK

Le client MAK tente de s'activer sur Internet au prochain intervalle planifié. Les administrateurs peuvent imposer une activation immédiate sur Internet, par téléphone ou au moyen de l'outil Volume Activation Management Tool (VAMT).

Pour confirmer l'activation, vérifiez dans la barre d'état système l'existence d'une notification indiquant « Windows est activé ». Vous pouvez également taper **slmgr.vbs /dli** à partir d'une invite de commandes pour visualiser l'état d'activation d'un ordinateur.

---

## Activation des clients MAK sur Internet

Vous disposez de deux méthodes pour activer un client MAK sur Internet :

- Cliquez sur le lien **Cliquez ici pour activer Windows maintenant** dans l'option Système du Panneau de configuration. Windows vous indique alors si l'activation a réussi. En cas d'échec de l'activation, un Assistant vous propose d'autres options.
- Exécutez **slmgr.vbs /ato** à partir d'une invite de commandes. Si vous utilisez le script `slmgr.vbs`, aucune autre option ne vous est présentée.

---

## Activation des clients MAK par le biais d'un serveur proxy

L'activation sur Internet peut être bloquée si le serveur proxy nécessite une authentification de l'utilisateur. Dans Microsoft Internet Security and Acceleration (ISA) Server, ce paramètre est appelé *Authentification de base*. Les demandes d'activation ne présentant pas les informations d'identification de l'utilisateur au serveur proxy, Microsoft recommande de ne pas utiliser l'Authentification de base avec ISA Server ou d'autres serveurs proxy. Toutefois, si vous devez utiliser l'Authentification de base ou un mécanisme comparable sur le serveur proxy, ajoutez les URL ci-après à la liste d'**exclusions de l'authentification proxy** :

<http://go.microsoft.com/>\*

<https://sls.microsoft.com/>\*

<https://sls.microsoft.com:443>

<http://crl.microsoft.com/pki/crl/products/MicrosoftRootAuthority.crl>

<http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl>

<http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl>

<http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl>

<http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl>



---

## Activation des clients MAK par téléphone

Utilisez la procédure ci-après pour activer des ordinateurs connectés au réseau de l'organisation mais non dotés d'une connexion Internet en utilisant SImgr.vbs. Dans la fenêtre Invite de commandes, tapez la commande :

```
slmgr.vbs NomOrdinateurCible <NomUtilisateur> <MotdePasse> /dti
```

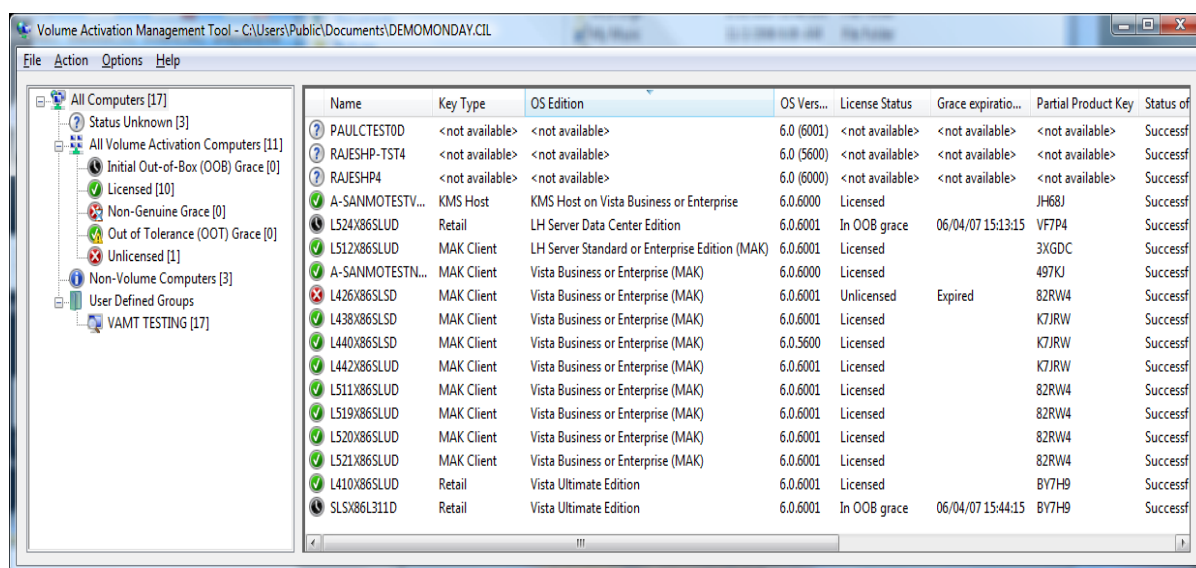
pour afficher les informations requises pour une activation par téléphone. Pour obtenir le numéro de téléphone d'un Centre d'appels d'activation dans votre région, exécutez **slui.exe 4**. Utilisez le système de réponse vocale interactive pour obtenir l'ID de confirmation (CID), puis exécutez la commande :

```
slmgr.vbs NomOrdinateurCible <NomUtilisateur> <MotdePasse> /atp  
<CID>
```

pour installer le CID. En cas d'activation fréquente ou d'activation de plusieurs ordinateurs, il peut se révéler plus utile d'automatiser le processus à l'aide du script SImgr.vbs.

## Activation des clients MAK à l'aide de l'outil VAMT

L'outil VAMT permet d'automatiser le déploiement et l'activation de MAK sur le réseau en distribuant les clés MAK à partir d'une console centralisée, comme illustré à la Figure 2. VAMT interroge les serveurs d'activation Microsoft pour obtenir le nombre d'activations restantes pour une clé MAK donnée, puis indique l'état d'activation de tous les systèmes activés par MAK dans l'environnement. Ce décompte est un instantané capturé à un instant t, et non un décompte en temps réel. L'outil VAMT version 1.2 est inclus dans Windows AIK, lequel est accessible à partir du Centre de téléchargement Microsoft à l'adresse <http://www.microsoft.com/downloads/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&displaylang=fr>



Name	Key Type	OS Edition	OS Vers...	License Status	Grace expiratio...	Partial Product Key	Status of
PAULCTEST0D	<not available>	<not available>	6.0 (6001)	<not available>	<not available>	<not available>	Successf
RAJESH-P-TST4	<not available>	<not available>	6.0 (5600)	<not available>	<not available>	<not available>	Successf
RAJESH-P4	<not available>	<not available>	6.0 (6000)	<not available>	<not available>	<not available>	Successf
A-SANMOTESTV...	KMS Host	KMS Host on Vista Business or Enterprise	6.0.6000	Licensed		JH68J	Successf
LS24X86SLUD	Retail	LH Server Data Center Edition	6.0.6001	In OOB grace	06/04/07 15:13:15	VF7P4	Successf
LS12X86SLUD	MAK Client	LH Server Standard or Enterprise Edition (MAK)	6.0.6001	Licensed		3XGDC	Successf
A-SANMOTESTN...	MAK Client	Vista Business or Enterprise (MAK)	6.0.6000	Licensed		497KJ	Successf
L426X86SLSD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Unlicensed	Expired	82RW4	Successf
L438X86SLSD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		K7JRW	Successf
L440X86SLSD	MAK Client	Vista Business or Enterprise (MAK)	6.0.5600	Licensed		K7JRW	Successf
L442X86SLUD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		K7JRW	Successf
LS11X86SLUD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		82RW4	Successf
LS19X86SLUD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		82RW4	Successf
LS20X86SLUD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		82RW4	Successf
LS21X86SLUD	MAK Client	Vista Business or Enterprise (MAK)	6.0.6001	Licensed		82RW4	Successf
L410X86SLUD	Retail	Vista Ultimate Edition	6.0.6001	Licensed		BY7H9	Successf
SLSX86L311D	Retail	Vista Ultimate Edition	6.0.6001	In OOB grace	06/04/07 15:44:15	BY7H9	Successf

Figure 2 : interface utilisateur de l'outil VAMT

---

## Désactivation de l'activation automatique

Vous pouvez désactiver l'activation automatique sur n'importe quel client KMS en définissant la valeur **DWORD Manual** existante sur **1**. Cette valeur figure dans la sous-clé de registre **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Intégration des MAK avec Deployment Workbench

La boîte à outils Microsoft Deployment Toolkit (MDT) offre également une solution pour le déploiement des MAK. Dans Deployment Workbench, les administrateurs configurent la clé MAK en séquences de tâches qui ajoutent cette clé au fichier Unattend.xml utilisé lors de l'installation. Les administrateurs peuvent préparer l'image de référence pour l'activation KMS ; puis, lors du déploiement, MDT active l'installation en utilisant une clé MAK tant qu'il ne détecte aucune infrastructure KMS. MDT applique la clé MAK après avoir installé l'image. Pour plus d'informations concernant MDT, consultez le site **TechCenter Déploiement de postes de travail**, accessible à l'adresse <http://technet.microsoft.com/fr-fr/deployment/default.aspx>.

---

## Réactivation d'ordinateurs

À intervalles réguliers, Windows 7 et Windows Server 2008 R2 vérifient la configuration matérielle de l'ordinateur sur lequel le système d'exploitation est installé. Si le système d'exploitation détecte que le matériel a fait l'objet de modifications majeures, une réactivation est nécessaire. Les facteurs de pondération réels et les valeurs de seuil varient, car ces valeurs doivent suivre le rythme du marché du matériel informatique en constante évolution. En général, les ordinateurs qui utilisent l'activation MAK appliquent les mêmes règles de réactivation que l'activation des éditions commerciales. Les clients KMS se concentrent davantage sur les modifications de disque dur pour déterminer la nécessité d'une réactivation.

Les activations des clients restent valides pendant 180 jours. Cette période est désignée sous le terme *d'intervalle de renouvellement d'activation*. Les clients KMS doivent renouveler leur activation en se connectant à l'hôte KMS au moins une fois tous les 180 jours, sans quoi ils seront désactivés. Par défaut, les ordinateurs clients KMS tentent de renouveler leur activation tous les 7 jours. Une fois l'activation renouvelée, l'intervalle de renouvellement d'activation est remis à zéro.

---

## Annexe A : configurations facultatives

Volume Activation prend en charge des configurations facultatives qui peuvent fonctionner dans certains environnements, mais ne sont pas recommandées pour la plupart. Les procédures de cette annexe nécessitent un redémarrage du service de protection logicielle avant d'être prises en compte.

### Autorisation de l'activation par utilisateur standard

Pour autoriser l'activation par utilisateur standard sur un client KMS, ajoutez une valeur de registre **DWORD** nommée **UserOperations**, puis définissez sa valeur sur

**1**. Créez cette valeur dans la sous-clé de registre

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform.**

Une fois cette opération achevée, les droits d'administration ne sont plus requis pour certaines tâches, telles que l'installation d'une clé de produit (**slmgr.vbs /ipk**), l'installation d'une licence (**slmgr.vbs /ilc**) ou le réarmement (**slmgr.vbs /rearm**). Ceci signifie qu'un utilisateur standard peut faire passer un client KMS à l'activation MAK, activer manuellement un ordinateur et, si nécessaire, remplacer une clé MAK existante par une nouvelle clé MAK. Toutefois, cette procédure est déconseillée car elle compromet la sécurité de l'ordinateur.

**Remarque** : si un utilisateur standard installe une clé MAK ou KMS, les valeurs de registre **ProductID** ne sont pas mises à jour. Ce comportement affecte principalement la prise en charge du produit ; les Services de support client Microsoft (CSS) sont conscients de cette situation.

### Désactivation des notifications d'activation

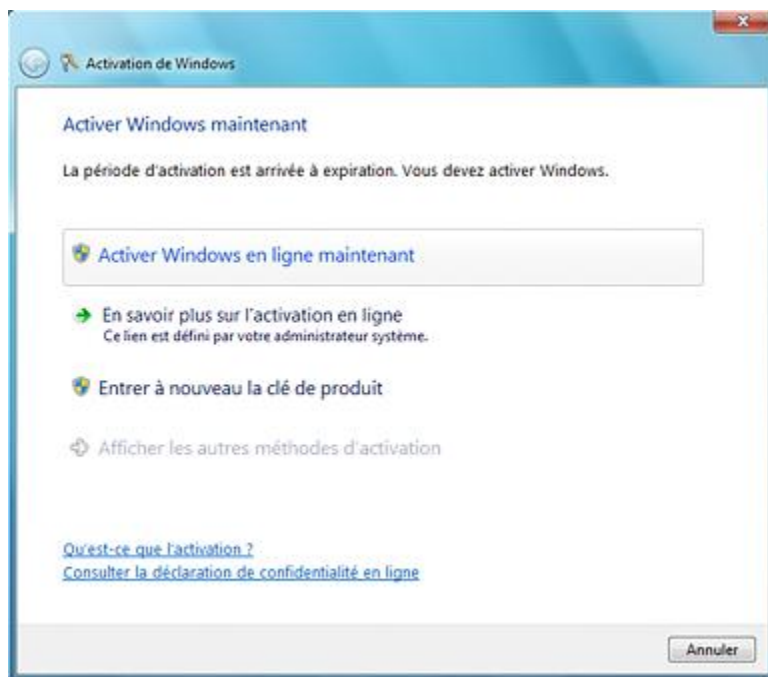
Bien que cette procédure soit déconseillée, vous pouvez désactiver les notifications de licences logicielles en ajoutant au registre une nouvelle valeur **DWORD** nommée

**NotificationDisabled** et en lui attribuant la valeur **1**. Créez cette valeur dans la sous-clé de registre **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**. Cette valeur désactive toutes les notifications de licences logicielles, y compris les bulles, les Assistants et les boîtes de dialogue de tâche.

---

## Modifications de clé de registre pour les fonctions d'activation

Windows 7 et Windows Server 2008 R2 intègrent une nouvelle clé de plateforme de protection de licence logicielle (SPP, Software Protection Platform) dans le registre. Pour l'activation de produits dans des environnements gérés, configurez la boîte de dialogue **Activer Windows maintenant** pour afficher un lien facultatif **En savoir plus sur l'activation en ligne**, comme illustré à la Figure 3.



**Figure 3 : lien En savoir plus sur l'activation en ligne**

La sélection de ce lien personnalisé charge une URL définie par l'administrateur dans le navigateur par défaut de l'utilisateur. Cette URL peut pointer vers une page Web personnalisée ou vers un autre fichier stocké sur l'ordinateur local ou sur un partage réseau. Un client sous licence en volume peut utiliser ce lien pour fournir des informations qui lui sont spécifiques concernant l'activation. L'affichage de ce lien nécessite la définition de la valeur **REG\_SZ** nommée **ActivationAlternateURL** sur l'URL de la page Web qui doit s'afficher lorsque l'utilisateur clique sur le lien. La valeur **ActivationAlternateURL** est située dans la sous-clé de registre **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**.

---

## Annexe B : exemple de fichier d'installation sans assistance

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <UserData>
        <AcceptEula>true</AcceptEula>
      </UserData>
    </component>
  </settings>
  <settings pass="specialize">
    <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <ProductKey>Clé de produit MAK</ProductKey>
    </component>
  </settings>
  <cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-
microsoft-com:cpi" />
</unattend>
```