**Guia de Implantação do Volume Activation**

**Windows 7 e Windows Server 2008 R2**

Microsoft Corporation

Publicado em: junho de 2009

Resumo

O Volume Activation ajuda os clientes de Licenciamento por Volume a automatizar e gerenciar o processo de ativação. Este documento destina-se a implementadores de TI (Tecnologia da Informação) que planejaram uma implantação do Volume Activation e estão prontos para examinar e executar os procedimentos necessários.

Este documento, assim como qualquer outro mencionado aqui, é fornecido apenas para fins informativos, e a Microsoft não oferece nenhuma garantia, explícita ou implícita, sobre ele. As informações deste documento, inclusive URLs e outras referências a sites da Internet, estão sujeitas a alterações sem aviso. O usuário assume inteiro risco quanto ao uso ou aos resultados do uso deste documento. A menos que indicado o contrário, as empresas, as organizações, os produtos, os nomes de domínios, os endereços de email, os logotipos, as pessoas, os lugares e os eventos descritos nos exemplos aqui contidos são fictícios. Nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de email, logotipo, pessoa, lugar ou acontecimento real é intencional ou deve ser inferida. Obedecer às leis de direitos autorais é responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa, por escrito, da Microsoft Corporation.

A Microsoft pode ter patentes ou requisições para obtenção de patente, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual que abrangem o conteúdo deste documento. A posse deste documento não lhe confere nenhum direito sobre as citadas patentes, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual, salvo aqueles expressamente mencionados em um contrato de licença, por escrito, da Microsoft.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Windows, Windows Server e Windows Vista são marcas comerciais do grupo de empresas Microsoft.

Os nomes de empresas e produtos reais aqui mencionados podem ser marcas comerciais de seus respectivos proprietários.

Conteúdo

[Conteúdo 3](#_Toc234138589)

[Introdução 5](#_Toc234138590)

[Ativação por KMS 6](#_Toc234138591)

[Configurar hosts KMS 6](#_Toc234138592)

[Executar o Slmgr.vbs Remotamente 8](#_Toc234138593)

[Configurar o Firewall do Windows para Operações Remotas do Gerenciador de Licenças de Software 9](#_Toc234138594)

[Operações Remotas Focadas em Computadores de Grupos de Trabalho 10](#_Toc234138595)

[Configurar DNS 10](#_Toc234138596)

[Mudar as Permissões Padrão de DNS para Registros SRV 11](#_Toc234138597)

[Publicar em Vários Domínios DNS 12](#_Toc234138598)

[Criar Manualmente Registros SRV no DNS 13](#_Toc234138599)

[Criar Registros SRV Manualmente em um Servidor DNS BIND 8.2 ou Maior 14](#_Toc234138600)

[Desativar a Publicação dos Registros de SRV do KMS no DNS 15](#_Toc234138601)

[Instalar Hosts KMS 16](#_Toc234138602)

[Configurar Clientes KMS 17](#_Toc234138603)

[Especificar Manualmente um Host KMS 18](#_Toc234138604)

[Ativar a Descoberta Automática de um Cliente KMS 19](#_Toc234138605)

[Adicionar Entradas Sufixadas a Clientes KMS 20](#_Toc234138606)

[Implementar Clientes KMS 21](#_Toc234138607)

[Ativar Manualmente um Cliente KMS 22](#_Toc234138608)

[Converter Clientes MAK em Clientes KMS e Vice-versa 23](#_Toc234138609)

[Converter Edições Comerciais em Volume Activation 24](#_Toc234138610)

[Ativação por MAK 25](#_Toc234138611)

[Converter Clientes KMS em Ativação por MAK 25](#_Toc234138612)

[Instalar uma MAK Durante a Instalação do Sistema Operacional 26](#_Toc234138613)

[Instalar uma MAK Após a Instalação do Sistema Operacional 27](#_Toc234138614)

[Desativar a Ativação Automática 28](#_Toc234138615)

[Ativar Clientes MAK 28](#_Toc234138616)

[Ativar Clientes MAK pela Internet 29](#_Toc234138617)

[Ativar Clientes MAK por Meio de Servidor Proxy 30](#_Toc234138618)

[Ativar Clientes MAK Usando Telefone 31](#_Toc234138619)

[Ativar os Clientes MAK Usando a VAMT 32](#_Toc234138620)

[Desativar a Ativação Automática 33](#_Toc234138621)

[Integrar MAKs ao Deployment Workbench 33](#_Toc234138622)

[Reativar Computadores 34](#_Toc234138623)

[Apêndice A: Configurações Opcionais 35](#_Toc234138624)

[Ativação por Usuário Padrão 35](#_Toc234138625)

[Desativar as Notificações de Ativação 35](#_Toc234138626)

[Alterações de Chaves de Registro para Recursos de Ativação 36](#_Toc234138627)

[Apêndice B: Arquivo de Exemplo de Instalação Autônoma 37](#_Toc234138628)

# Introdução

Este guia descreve os conceitos de implantação do Microsoft® Volume Activation. O Volume Activation consiste de duas tecnologias — KMS (Serviço de Gerenciamento de Chaves) e MAK (Chaves de Ativação Múltipla) — que permitem que os clientes de Licenciamento por Volume ativem as edições de Licenciamento por Volume dos sistemas operacionais Windows® 7 e do Windows Server® 2008 R2. O Centro de Atendimento de Licenciamento por Volume em <https://www.microsoft.com/licensing/servicecenter/> oferece mais informações sobre o Licenciamento por Volume.

Ao planejar o uso do Volume Activation, a organização deve escolher entre KMS, MAK ou uma combinação das duas. Os métodos de ativação escolhidos dependem das necessidades da organização e da infraestrutura da rede. Para obter mais informações sobre o planejamento de uma implantação do Volume Activation, consulte o [Guia de Planejamento do Volume Activation.](http://go.microsoft.com/fwlink/?LinkId=155926)

**Observação**   Este documento fornece orientações sobre a implantação do Volume Activation para os sistemas operacionais Windows 7 e Windows Server 2008 R2. Mas este guia não lida com a interoperabilidade entre ambas as gerações de produtos. Para mais informações sobre a implantação do Volume Activation para o Windows Vista® e o Windows Server 2008, consulte <http://go.microsoft.com/fwlink/?LinkID=75674>.

**Observação**   Este guia descreve procedimentos que executam scripts e fazem alterações no registro. Esses direitos podem ser delegados a implementadores de TI (Tecnologia da Informação), e os direitos para alterar chaves de produto e executar ativações podem ser atribuídos até mesmo aos usuários, embora a Microsoft não recomende essa prática.

Se a ativação falhar, consulte o [Guia de Operações do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084) para obter orientação para a solução de problemas. Este guia inclui uma referência aos códigos de erro com etapas para a solução de problemas comuns.

# Ativação por KMS

A ativação por KMS funciona com intervenções administrativas mínimas. Se o ambiente de rede tiver DDNS (Sistema de Nomes de Domínio Dinâmico) e permitir aos computadores publicar serviços automaticamente, implantar um host KMS pode exigir muito pouco trabalho. Se a organização tiver mais de um host KMS ou se a rede não tiver suporte a DDNS, pode ser necessário executar algumas tarefas de configuração adicionais.

Aviso   Alguns procedimentos nesta seção exigem alterações no registro. Podem ocorrer problemas se o registro for modificado incorretamente usando o Editor do Registro ou outro método, e esses problemas podem exigir a reinstalação do sistema operacional. A Microsoft não pode garantir que esses problemas possam ser resolvidos. Os profissionais de TI podem modificar o registro por sua conta e risco.

O restante desta seção descreve as seguintes tarefas importantes:

1. Configurar hosts KMS
2. Configurar DNS
3. Instalar hosts KMS
4. Configurar clientes KMS

## Configurar hosts KMS

O Gerenciador de Licenças de Software, geralmente chamado de SL Manager (Slmgr.vbs), é um script usado para configurar e recuperar informações do Volume Activation. O script pode ser executado localmente no computador de destino ou remotamente de outro computador, mas deve ser executado em um prompt de comando com privilégios elevados. Se um usuário padrão executar o Slmgr.vbs, algum dado da licença pode estar ausente ou incorreto, e muitas operações são proibidas.

O Slmgr.vbs pode usar o Wscript.exe ou o Cscript.exe, e os administradores podem especificar qual mecanismo de script usar. Se nenhum mecanismo de script for especificado, o Slmgr.vbs será executado usando o mecanismo padrão, wscript.exe.

**Observação**O KMS exige uma exceção no firewall do host KMS. Se a porta TCP padrão for usada, ative a exceção de tráfego KMS no Firewall do Windows. Se um firewall diferente for usado, abra a porta TCP 1688. Se uma porta diferente da padrão for usada, abra a porta TCP personalizada no firewall.

O Serviço de Licenciamento de Software deve ser reiniciado para que as alterações sejam efetivadas. Para reiniciar o Serviço de Licenciamento de Software, use ou execute o snap-in MMC (Console de Gerenciamento Microsoft) ou execute este comando em um prompt de comando com privilégios elevados:

net stop sppsvc && net start sppsvc

O Slmgr.vbs requer ao menos um parâmetro. Se o script for executado sem parâmetros, as informações de ajuda serão exibidas. A Tabela 1 lista as opções de linha de comando do Slmgr.vbs, além de suas respectivas descrições. A maioria dos parâmetros da Tabela 1 configura o host KMS. Mas os parâmetros /sai e /sri são passados aos clientes KMS depois que eles fazem contato com o host. A sintaxe geral do Slmgr.vbs é esta:

slmgr.vbs /parâmetro

Tabela 1   Parâmetros do Slmgr.vbs

| Parâmetro | Descrição |
| --- | --- |
| /sprt NúmeroDaPorta | Estabelece a porta de comunicações TCP em um host KMS. Substitua NúmeroDaPorta pelo número da porta TCP que deseja usar. A configuração padrão é **1688**. |
| /cdns | Desativa a publicação automática do DNS por um host KMS. |
| /sdns | Ativa a publicação automática do DNS por um host KMS. |
| /cpri | Reduz a prioridade dos processos do host KMS. |
| /spri | Define a prioridade dos processos do host KMS como **Normal**. |
| /sai IntervaloDeAtivação | Altera a frequência com que um cliente KMS tenta se ativar quando não encontra um host KMS. Substitua IntervaloDeAtivação por um número de minutos. A configuração padrão é **120**. |
| /sri IntervaloDeRenovação | Altera a frequência com que o cliente KMS tenta renovar sua ativação contatando um host KMS. Substitua IntervaloDeRenovação por um número de minutos. A configuração padrão é **10080** (7 dias). Essa configuração substitui as configurações locais do cliente KMS. |
| /dli | Recupera a contagem de ativações atuais do KMS do host KMS. |

### Executar o Slmgr.vbs Remotamente

Para executar o Slmgr.vbs remotamente, os administradores devem fornecer parâmetros adicionais. Eles devem incluir o nome dos computadores de destino, bem como o nome de usuário e senha de uma conta que tenha direitos administrativos locais no computador de destino. Se for executado remotamente sem um nome de usuário e senha especificados, o script usará as credenciais do usuário que executar o script.

A sintaxe abaixo mostra os parâmetros adicionais necessários para executar o Slmgr.vbs remotamente:

slmgr.vbs NomeDoComputadorDeDestino [nomedeusuário] [senha] /parâmetro [opções]

### Configurar o Firewall do Windows para Operações Remotas do Gerenciador de Licenças de Software

O Slmgr.vbs usa a WMI (Instrumentação de Gerenciamento do Windows), portanto os administradores podem configurar o Firewall do Windows para que permita o tráfego WMI:

* Para uma única subrede, permita uma exceção para a **WMI (Instrumentação de Gerenciamento do Windows)** no Firewall do Windows.
* Para permitir o tráfego WMI em várias subredes, permita a conexão para **Instrumentação de Gerenciamento do Windows (ASync-In)**, **Instrumentação de Gerenciamento do Windows (DCOM-In)** e **Instrumentação de Gerenciamento do Windows (WMI-In)**. Além disso, permita o acesso remoto no escopo. Defina essas configurações usando o Firewall do Windows com a Segurança Avançada, que está na pasta Ferramentas Administrativas.

Observação   Por padrão, as exceções do Firewall do Windows nos perfis Privado e Público se aplicam somente ao tráfego originado na subrede local. Para expandir a exceção para que se aplique a várias subredes, altere as configurações de exceções no Firewall do Windows com a Segurança Avançada ou, se estiver associado a um domínio do AD DS, selecione o Perfil do Domínio.

### Operações Remotas Focadas em Computadores de Grupos de Trabalho

Os administradores podem permitir a execução remota do Slmgr.vbs em computadores que pertençam a um grupo de trabalho. Para isso, crie o valor **DWORD** **LocalAccountTokenFilterPolicy** na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** nos clientes KMS. Defina o valor como **0x01**.

## Configurar DNS

As seções a seguir descrevem conceitos para configurar o DNS para trabalhar com Volume Activation:

* Se mais de um host KMS for usado, consulte a seção “Mudar as Permissões Padrão de DNS para Registros SRV.”
* Para habilitar clientes KMS usando servidores DNS diferentes para encontrar hosts KMS, consulte a seção “Publicar em Vários Domínios DNS.”
* Para adicionar registros de recursos SRV manualmente a hosts KMS, consulte as seções “Criar Manualmente Registros SRV no DNS”, “Criar Manualmente Registros SRV em um Servidor DNS BIND 8.2 ou Maior” e “Desativar a Publicação dos Registros SRV do KMS no DNS.”

Observação   As mudanças de DNS podem não ser refletidas até que todos os servidores DNS tenham sido replicados.

### Mudar as Permissões Padrão de DNS para Registros SRV

Se houver apenas um host KMS em uso, talvez não seja necessário configurar as permissões no DNS. O comportamento padrão é permitir que um computador crie um registro de recurso SRV para então atualizá-lo. Porém, se houver mais de um host KMS (o que geralmente acontece), os outros hosts não poderão atualizar o registro de recurso SRV exceto se as permissões padrão forem alteradas.

O procedimento de alto nível a seguir é um exemplo do próprio ambiente da Microsoft. Ele não oferece etapas detalhadas, que podem ser diferentes de uma organização para a outra, e essa não é a única maneira de se alcançar o resultado desejado:

1. Crie um grupo de segurança global no Active Directory® para ser usado por seus hosts KMS. Um exemplo é o *Grupo do Serviço de Gerenciamento de Chaves*.
2. Adicione os hosts KMS ao grupo. Todos eles devem ingressar no mesmo domínio.
3. Depois que o primeiro host KMS for criado, ele criará o registro SRV original. Se o primeiro host KMS não puder criar o registro de recurso SRV, sua organização pode ter mudado as permissões padrão. Nesse caso, crie manualmente os registros de recurso SRV como descrito na seção “Criar Manualmente Registros SRV no DNS”.
4. Defina as permissões para o grupo SRV, permitindo atualizações pelos membros do grupo de segurança global.

**Observação** Um administrador de domínio pode delegar a habilidade de realizar as etapas anteriores a administradores da organização. Para isso, crie um grupo de segurança no Active Directory, dê a esse grupo permissão para alterar os registros SRV e em seguida adicione os que receberão esse poder.

### Publicar em Vários Domínios DNS

Por padrão, o host KMS é registrado apenas no domínio DNS ao qual o host pertence. Se o ambiente de rede tiver apenas um domínio DNS, não é necessária mais nenhuma ação.

Se houver mais de um nome de domínio DNS, será possível criar uma lista de domínios DNS para um host KMS usar durante a publicação de seu RR SRV. A definição desse valor do registro suspende o comportamento padrão do host KMS de publicar somente o domínio especificado como sufixo DNS primário.

Outra opção é adicionar os parâmetros priority (prioridade) e weight (peso) ao valor de registro **DnsDomainPublishList** para o KMS. Esse recurso permite que um administrador estabeleça grupos de prioridade e de peso do host KMS em cada grupo para definir qual host KMS tentar primeiro e distribuir o tráfego entre vários hosts KMS.

Observação   As mudanças de DNS podem não ser refletidas até que todos os servidores DNS tenham sido replicados. Alterações realizadas com muita frequência (tempo < tempo de replicação) podem deixar registros mais antigos se a alteração for realizada em um servidor que não tenha sido replicado.

Para publicar automaticamente o KMS em vários domínios DNS, adicione cada sufixo de domínio DNS ao que quer que o KMS deva publicar no valor de registro multi-string **DnsDomainPublishList em HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**. Depois de mudar o valor, reinicie o Serviço de Licenciamento de Software para criar os RRs de SRV.

Observação   Essa chave mudou em relação à localização do Windows Vista® em **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.

Após a configuração de um host KMS para publicar em vários domínio, exporte a chave de registro e importe-a nos registros dos hosts KMS adicionais. Para verificar se esse procedimento teve êxito, verifique o log de eventos do aplicativo em cada host KMS. Uma ID de evento 12294 indica que o host KMS teve êxito na criação dos RRs de SRV. Uma ID de evento 12293 indica que a tentativa de criar os RRs de SRV não teve êxito. Para obter a lista completa de códigos de erro, consulte o [Guia de Operações do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084).

### Criar Manualmente Registros SRV no DNS

Se o ambiente não suportar DDNS, os RRs de SRV devem ser criados manualmente para publicar o host KMS. Os ambientes sem suporte a DDNS devem desativar a publicação em todos os hosts KMS para impedir que os logs de evento coletem eventos de publicação de DNS falhos. Para desativar a publicação, use o script Slmgr.vbs com a opção de linha de comando **/cdns**. Consulte a seção “Configurar KMS” para obter mais informações sobre o script Slmgr.vbs.

Observação   Os RRs de SRV criados manualmente podem coexistir com os RRs de SRV publicados automaticamente pelos hosts KMS em outros domínios, contanto que todos os registros sejam mantidos para evitar conflitos.

Com o Gerenciador DNS, na zona de procura direta, crie um novo RR de SRV usando as informações apropriadas para o local. O KMS, por padrão, escuta na porta TCP 1688, e o serviço é \_VLMCS. A Tabela 2 contém exemplos de configurações para um RR de SRV.

Tabela 2   Registro de Recurso de SRV

| Nome | Configuração |
| --- | --- |
| Serviço | \_VLMCS |
| Protocolo | \_TCP |
| Número da porta | 1688 |
| Host que oferece o serviço | FQDN em Host KMS |

### Criar Registros SRV Manualmente em um Servidor DNS BIND 8.2 ou Maior

Se a organização usar um servidor DNS que não seja Microsoft, os RRs de SRV necessários podem ser criados desde que o servidor DNS seja compatível com o BIND (Berkeley Internet Name Domain) 8.2 ou maior. Ao criar o registro, inclua as informações mostradas na Tabela 3. As configurações **Priority** (prioridade) e **Weight** (peso) mostradas na Tabela 3 são usadas apenas pelo Windows 7 e pelo Windows Server 2008 R2.

Tabela 3   Informações de RR de SRV

|  |  |
| --- | --- |
| Nome | Configuração |
| Nome | \_vlmcs.\_tcp |
| Tipo | SRV |
| Prioridade | 0 |
| Peso | 0 |
| Porta | 1688 |
| Nome do host | FQDN em Host KMS |

Para configurar um servidor DNS BIND 8.2 ou maior para oferecer suporte à publicação automática do KMS, configure o servidor BIND para ativar atualizações de RR dos hosts KMS. Por exemplo, adicione a linha abaixo à definição da zona em named.conf:

allow-update { any; };

Observação   Uma instrução allow-update também pode ser adicionada em named.conf.options para permitir o DDNS para todas as zonas hospedadas nesse servidor.

### Desativar a Publicação dos Registros de SRV do KMS no DNS

Os hosts KMS publicam automaticamente sua existência criando RRs de SRV no DNS. Para desativar a publicação automática por um host KMS, use o script Slmgr.vbs com a opção de linha de comando **/cdns**.

É preferível usar o script Slmgr.vbs para desativar a publicação automática de DNS, mas essa tarefa também pode ser realizada criando-se um novo valor **DWORD** chamado **DisableDnsPublishing** no registro, definindo seu valor como **1**. Esse valor está em **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** no registro. Para reativar o comportamento padrão de publicação de registros de SRV do KMS no DNS, defina seu valor como **0**.

## Instalar Hosts KMS

Para ativar a funcionalidade do KMS, uma chave KMS será instalada em um host KMS, depois o host será ativado pela Internet ou pelo telefone usando os serviços de ativação da Microsoft. Os computadores que executam o Windows 7 ou o Windows Server 2008 R2 podem atuar como hosts KMS.

O Windows Vista, o Windows Server 2003 e o Windows Server 2008 também podem servir como hosts KMS. Os clientes KMS que podem ser ativados por um host KMS dependem da chave do host usada para ativar o host KMS. Para mais informações sobre o uso de chaves do host KMS, consulte o [*Guia de Planejamento do Volume Activation*](http://go.microsoft.com/fwlink/?LinkId=155926).

Instale e ative uma chave KMS em um computador com Windows 7 ou Windows Server 2008 R2 usando um prompt de comando com privilégios elevados:

* Para instalar uma chave KMS, digite **slmgr.vbs /ipk <ChaveKMS>** em um prompt de comando.
* Para ativar online, digite **slmgr.vbs /ato** em um prompt de comando.
* Para ativar pelo telefone, digite **slui.exe 4** em um prompt de comando.

Depois de ativar a chave KMS, reinicie o Serviço de Proteção do Software.

O Windows 7 e o Windows Server 2008 R2 exibem o aviso mostrado na Figura 1 sempre que os administradores instalam uma chave de host KMS usando a interface de usuário (os usuários não verão esse aviso se instalarem uma chave de host KMS usando o script Slmgr.vbs). Essa mensagem evita a instalação acidental de uma chave KMS em computadores que os administradores não pretendam transformar em hosts KMS.

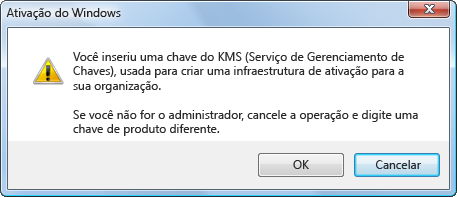


Figura 1   O aviso de chave KMS

Para confirmar se o host KMS está corretamente configurado, verifique a contagem do KMS para ver se ela está aumentando. Na janela do prompt de comando do host KMS, digite **slmgr.vbs /dli** para exibir a contagem atual do KMS. Os administradores também podem verificar o log do Serviço de Gerenciamento de Chaves na pasta Logs de Aplicativos e Serviços para obter os eventos de ID 12290. O log do Serviço de Gerenciamento de Chaves registra as solicitações de ativação dos clientes KMS. Todos os eventos exibem o nome do computador e a data/hora de cada solicitação de ativação.

## Configurar Clientes KMS

Esta seção descreve os conceitos de instalação e configuração de computadores como clientes KMS. Por padrão, as edições de Licenciamento por Volume do Windows Vista, do Windows 7, do Windows Server 2008 e do Windows Server 2008 R2 são clientes KMS. Se os computadores que a organização deseja ativar usando o KMS estiverem usando um desses sistemas operacionais e a rede permitir descoberta automática de DNS, nenhuma configuração adicional será necessária.

Se um cliente KMS estiver configurado para procurar por um host KMS usando DNS, mas não receber registros de SRV do DNS, o Windows 7 e o Windows Server 2008 R2 registram o erro no log de eventos.

### Especificar Manualmente um Host KMS

Os administradores podem atribuir manualmente um host KMS a clientes KMS usando o cache de host KMS. A atribuição manual de um host KMS desativa a descoberta automática do KMS no cliente KMS. Para atribuir manualmente um host KMS a um cliente KMS, execute:

slmgr.vbs /skms <valor>:<porta>

onde valor é KMS\_FQDN, IPv4Address ou NetbiosName do host KMS, e porta é a porta TCP no host KMS.

### Ativar a Descoberta Automática de um Cliente KMS

Por padrão, os clientes KMS tentam descobrir os hosts KMS automaticamente. A descoberta automática pode ser desativada atribuindo manualmente um host KMS a um cliente KMS. Essa ação também remove o nome do host KMS do cache do cliente KMS. Se a descoberta automática estiver desativada, ela pode ser reativada executando **slmgr.vbs /ckms** em um prompt de comando.

### Adicionar Entradas Sufixadas a Clientes KMS

Adicionando o endereço de um servidor DNS contendo os RRs de SRV como uma entrada sufixada nos clientes KMS, os administradores podem anunciar hosts KMS em um servidor DNS e permitir que clientes KMS com outros servidores DNS primários o encontrem. Para obter mais informações sobre a configuração de uma lista de pesquisa de sufixo de domínio em clientes KMS, consulte o artigo da Ajuda e Suporte da Microsoft “Como Configurar uma Lista de Pesquisa de Sufixo de Domínio nos Clientes do Sistema de Nomes de Domínio”, em <http://support.microsoft.com/kb/275553>.

### Implementar Clientes KMS

As informações desta seção destinam-se a clientes do Licenciamento por Volume usando o Windows AIK (Kit de Instalação Automatizada do Windows) para implantar e ativar um sistema operacional Windows. Prepare os clientes KMS para a implantação usando a Ferramenta de Preparação do Sistema (Sysprep) ou o script Slmgr.vbs:

* **Sysprep.** Antes de capturar uma imagem, execute o Sysprep com a opção de linha de comando **/generalize** para redefinir o timer de ativação, o identificador de segurança (SID) e outras configurações importantes. A redefinição do timer de ativação impede que o período de cortesia da imagem expire antes que a imagem seja implementada. A execução do Sysprep.exe não remove a chave de produto instalada, e os administradores não serão solicitados a inserir uma nova chave durante a mini-instalação. Se não restarem rearmações, a operação do Sysprep é concluída, mas os timers de ativação não são alterados e um erro é retornado, explicando a situação.
* **Slmgr.vbs.**Ao construir máquinas virtuais (VM) de demonstração para uso interno (por exemplo, para o departamento de vendas da organização ou para configurar um ambiente temporário de treinamento), a execução do script Slmgr.vbs com a opção de linha de comando **/rearm** estende o período de cortesia por mais 30 dias, o que por sua redefine o timer de ativação mas não faz outras alterações no computador. O timer de ativação pode ser redefinido três vezes em computadores executando o Windows 7 ou o Windows Server 2008 R2.

### Ativar Manualmente um Cliente KMS

Por padrão, os clientes KMS tentam se ativar automaticamente em intervalos predeterminados. Para ativar clientes KMS manualmente (por exemplo, clientes desconectados) antes de distribuí-los aos usuários, use o item Sistema no Painel de Controle, ou execute **slmgr.vbs /ato** em um prompt de comando com privilégios elevados. O script Slmgr.vbs relatará se houve êxito ou falha na ativação e oferecerá um código de resultado. Para realizar a ativação, o cliente KMS deve ter acesso a um host KMS na rede da organização.

### Converter Clientes MAK em Clientes KMS e Vice-versa

Por padrão, os sistemas operacionais Windows 7 e Windows Server 2008 R2 usam o KMS para ativação. Para alterar os clientes KMS existentes em clientes MAK, basta instalar uma chave MAK. De modo semelhante, para mudar clientes MAK para clientes KMS, execute:

slmgr.vbs /ipk <ChaveDeInstalaçãoKms>

onde ChaveDeInstalaçãoKms é uma das chaves de instalação mostradas na Tabela 4. Depois de instalar a chave de instalação KMS, ative o cliente KMS executando **cscript slmgr.vbs /ato**.

Tabela 4   Chaves de Instalação do Cliente KMS

| Edição do Sistema Operacional | Chave do Produto |
| --- | --- |
| Windows 7 | |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| Windows Server 2008 R2 | |
| Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Windows Server 2008 R2 para sistemas baseados no 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 |

### Converter Edições Comerciais em Volume Activation

As edições comerciais do Windows 7 Professional e do Windows Server 2008 R2 podem ser convertidas em clientes KMS, desde que a organização tenha adquirido as licenças de volume corretas e esteja em conformidade com os Direitos de Uso do Produto. Para converter o Windows 7 Professional e todas as edições do Windows Server 2008 R2 de comerciais em clientes KMS, ignore a página da **Chave do Produto** durante a instalação do sistema operacional. Quando a instalação for concluída, abra uma janela do Prompt de Comando com privilégios elevados e digite:

Slmgr.vbs /ipk <ChaveDeInstalação>

onde ChaveDeInstalação é a chave de instalação do cliente KMS da Tabela 4 que corresponde à edição do Windows 7 ou do Windows Server 2008 R2.

# Ativação por MAK

A ativação por MAK é usada para ativações únicas por meio dos serviços de ativação hospedados na Microsoft, sem necessidade de renovações. Para obter mais informações sobre a ativação por MAK, consulte o [Guia de Planejamento do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926).

## Converter Clientes KMS em Ativação por MAK

O Windows 7 e o Windows Server 2008 R2 são instalados automaticamente como clientes KMS. Para converter um cliente KMS em ativação por MAK, instale uma MAK. A MAK pode ser instalada durante ou após a instalação do sistema operacional.

Uma chave MAK pode ser instalada em uma imagem de referência do Windows 7 e do Windows Server 2008 R2 para fazer com que todas as instalações daquela imagem usem ativação por MAK em vez da ativação por KMS padrão. Isso reduz a necessidade de especificar uma MAK em um arquivo de instalação autônoma.

### Instalar uma MAK Durante a Instalação do Sistema Operacional

Os administradores podem converter um cliente KMS em cliente MAK durante a instalação inicial do Windows 7 ou do Windows Server 2008 R2 incluindo uma MAK em um arquivo de instalação autônoma (Unattend.xml). O arquivo Unattend.xml pode ser usado com o Setup.exe ou com os Serviços de Implantação do Windows. Para obter mais informações, consulte o arquivo de ajuda Referência da Instalação Autônoma do Windows no Windows AIK (Kit de Instalação Automatizada do Windows) em <http://go.microsoft.com/fwlink/?LinkId=136976>. Para obter um exemplo de arquivo de instalação autônoma, consulte o “Apêndice B: Arquivo de Exemplo de Instalação Autônoma.”

Observação   A MAK é armazenada em texto não criptografado no arquivo Unattend.xml. Durante a instalação autônoma, o arquivo Unattend.xml ou AutoUnattend.xml é copiado para a pasta %SystemRoot%\Panther do computador de destino. Entretanto, no final do processo de instalação, o programa de instalação o substitui por “SENSITIVE\*DATA\*DELETED.”

### Instalar uma MAK Após a Instalação do Sistema Operacional

Uma edição de volume do Windows 7 ou do Windows Server 2008 R2 pode ser configurada para usar ativação por MAK usando o item Sistema do Painel de Controle ou executando o script Slmgr.vbs:

* Para instalar uma MAK usando o aplicativo de Sistema, clique no link **Altere a chave de produto** e digite a MAK na caixa de diálogo **Altere a chave do produto para ativação**.
* Para instalar uma MAK usando o Slmgr.vbs, execute o comando a seguir em um prompt de comando:

slmgr.vbs /ipk <ChaveDeAtivaçãoMúltipla>

onde ChaveDeAtivaçãoMúltipla é a MAK.

Se os usuários instalarem uma MAK usando a interface de usuário, o cliente MAK tenta se ativar pela Internet uma vez. Se os usuários instalarem uma chave MAK usando o script Slmgr.vbs, o cliente MAK não tenta se ativar automaticamente.

### Desativar a Ativação Automática

Para desativar a ativação automática em qualquer cliente MAK, defina o valor de registro **DWORD** **Manual** como **1**. Esse valor está na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Ativar Clientes MAK

O cliente MAK tenta se ativar pela Internet no próximo intervalo programado. Os administradores podem forçar a ativação imediatamente pela Internet, por telefone ou usando a VAMT (Ferramenta de Gerenciamento do Volume Activation).

Para confirmar a ativação, verifique se na bandeja do sistema há uma notificação afirmando que “O Windows foi ativado.” Se preferir, digite **slmgr.vbs /dli** em um prompt de comando para exibir o status de ativação do computador.

### Ativar Clientes MAK pela Internet

Um cliente MAK pode ser ativado pela Internet de duas maneiras:

* Clique no link **Clique aqui para ativar o Windows agora** no item Sistema do Painel de Controle. O Windows relatará se houve êxito na ativação. Se a ativação for mal-sucedida, o assistente oferecerá opções adicionais.
* Execute o **slmgr.vbs /ato** em um prompt de comando. Não são apresentadas opções adicionais quando o slmgr.vbs é usado.

### Ativar Clientes MAK por Meio de Servidor Proxy

A ativação pela Internet poderá ser bloqueada se o servidor proxy exigir autenticação do usuário. No Microsoft ISA (Internet Security and Acceleration) Server, essa configuração é denominada Autenticação Básica. Como as solicitações de ativação não informam as credenciais do usuário ao servidor proxy, a Microsoft não recomenda o uso da Autenticação Básica com o ISA Server ou outros servidores proxy. Entretanto, se for necessário usar a Autenticação Básica ou um mecanismo similar no servidor proxy, adicione estes URLs à lista de **Exclusão da Autenticação de 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

### Ativar Clientes MAK Usando Telefone

Para ativar computadores conectados à rede da organização, mas que não tenham conectividade com a Internet, use o Slmgr.vbs. Na janela do Prompt de Comando, digite:

slmgr.vbs NomeDoComputadorDeDestino <NomeDeUsuário> <Senha> /dti

para exibir as informações necessárias para concluir a ativação por telefone. Para obter o número de telefone de uma Central de Atendimento de Ativação em sua região, execute **slui.exe 4**. Use o sistema Interativo de Resposta por Voz para obter a ID de confirmação (CID); em seguida, execute:

slmgr.vbs NomeDoComputadorDeDestino <NomeDeUsuário> <Senha> /atp <CID>

para instalar a CID. Se as ativações forem realizadas frequentemente ou se vários computadores forem ativados, pode ser mais útil automatizar o processo usando o script Slmgr.vbs.

### Ativar os Clientes MAK Usando a VAMT

A VAMT permite a automatização da implantação MAK e a ativação pela rede distribuindo MAKs de um console centralizado, como mostra a Figura 2. A VAMT consulta os servidores de ativação da Microsoft para obter o número de ativações remanescentes de uma determinada MAK, e em seguida lista o status de ativação de todos os sistemas ativados por MAK no ambiente. A contagem é um instantâneo de um momento, e não uma contagem em tempo real. A versão 1.2 da VAMT vem incluída no Windows AIK (Kit de Instalação Automatizada do Windows), que está disponível no Centro de Download da Microsoft em <http://go.microsoft.com/fwlink/?LinkId=136976>.



Figura 2   A interface de usuário da VAMT

### Desativar a Ativação Automática

A ativação automática pode ser desativada em qualquer cliente KMS definindo o valor **DWORD** existente **Manual** como **1**. Esse valor está na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**.

## Integrar MAKs ao Deployment Workbench

O MDT (Microsoft Deployment Toolkit) também oferece uma solução para a implantação de MAKs. No Deployment Workbench, os administradores configuram a MAK em sequências de tarefas, que adicionam a MAK ao arquivo Unattend.xml usado durante a instalação. Os administradores podem preparar a imagem de referência para ativação por KMS, e em seguida, durante a implantação, o MDT ativa a instalação usando uma MAK, desde que não detecte uma infraestrutura de KMS. O MDT aplica a MAK após a instalação da imagem. Para mais informações sobre o MDT, consulte o **Deployment TechCenter** em <http://technet.microsoft.com/en-us/deployment/default.aspx>.

# Reativar Computadores

O Windows 7 e o Windows Server 2008 R2 verificam periodicamente a configuração de hardware do computador no qual o sistema operacional está instalado. Se o sistema operacional detectar que o hardware está muito diferente, a reativação será necessária. Os fatores reais de ponderação e os valores de limite podem variar, já que esses valores devem acompanhar o mercado dinâmico de hardware para computadores. Em geral, os computadores que usam a ativação por MAK usam as mesmas regras de reativação da ativação do varejo. Os clientes KMS concentram-se mais nas alterações na unidade de disco rígido para determinar a necessidade de reativação.

As ativações de clientes são válidas por 180 dias. Esse período é chamado intervalo de validade de ativação. Os clientes KMS devem renovar suas ativações conectando-se ao host KMS a cada 180 dias, no mínimo, para se manterem ativados. Por padrão, os computadores clientes KMS tentam renovar suas ativações a cada sete dias. Após a renovação de uma ativação de cliente, o intervalo de validade de ativação é reiniciado.

# Apêndice A: Configurações Opcionais

O Volume Activation tem suporte a configurações opcionais que podem funcionar em alguns ambientes, mas que não são recomendadas para a todos. Os procedimentos deste apêndice requerem o reinício do Serviço de Proteção do software para terem efeito.

## Ativação por Usuário Padrão

Para habilitar a ativação por usuário padrão em um cliente KMS, adicione um novo valor de registro **DWORD** chamado **UserOperations** e defina seu valor como **1**. Crie esse valor na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**.

Depois disso, os direitos administrativos não serão mais necessários para algumas operações, como a instalação de uma chave de produto (**slmgr.vbs /ipk**), a instalação de uma licença (**slmgr.vbs /ilc**) ou o rearmamento (**slmgr.vbs /rearm**). Isso significa que um usuário padrão pode alternar de um cliente KMS para ativação por MAK, ativar manualmente um computador e, se necessário, substituir uma MAK existente por uma nova. Isso não é recomendado porque reduz a segurança no computador.

Observação   Se um usuário padrão instalar uma chave MAK ou KMS, os valores do registro **ProductID** não serão atualizados. Esse comportamento afeta principalmente o suporte ao produto e os Serviços de suporte ao cliente Microsoft estão cientes dessa situação.

## Desativar as Notificações de Ativação

Embora isso não seja recomendado, as notificações de licenciamento de software podem ser desativadas adicionando-se um novo valor **DWORD** ao registro chamado **NotificationDisabled**, com valor **1**. Crie-o na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation**. Esse valor desativa todas as notificações de licenciamento de software, como balões, assistentes e caixas de diálogo de tarefas.

## Alterações de Chaves de Registro para Recursos de Ativação

O Windows 7 e o Windows Server 2008 R2 incluem uma nova chave de SPP (Plataforma de Proteção de Software) no registro. Para a ativação de produtos em ambientes gerenciados, configure a caixa de diálogo **Ativar o Windows agora** para que exiba um link opcional **Informações sobre ativação online**, como mostra a Figura 3.

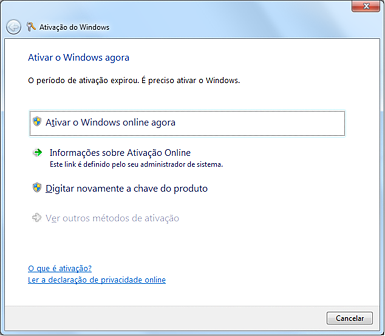


Figura 3 Informações sobre ativação online

Ao clicar nesse link personalizado, o navegador padrão do usuário abrirá o URL definido pelo administrador. O URL pode apontar para uma página da Web personalizada ou para outro arquivo armazenado no computador local ou em um compartilhamento de rede. Um cliente do Licenciamento por Volume pode usar o link para oferecer informações específicas para o cliente sobre a ativação. Para exibir o link, é preciso definir o valor **REG\_SZ** **ActivationAlternateURL** como o URL da página da Web a ser exibida ao clique do usuário. O valor **ActivationAlternateURL** está na subchave de registro **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**.

# Apêndice B: Arquivo de Exemplo de Instalação Autônoma

<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">

    <settings pass="windowsPE">

        <component name="Microsoft-Windows-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <UserData>

                <AcceptEula>true</AcceptEula>

            </UserData>

</component>

    </settings>

    <settings pass="specialize">

        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <ProductKey>MAK Product Key</ProductKey>

        </component>

    </settings>

<cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-com:cpi" />

</unattend>