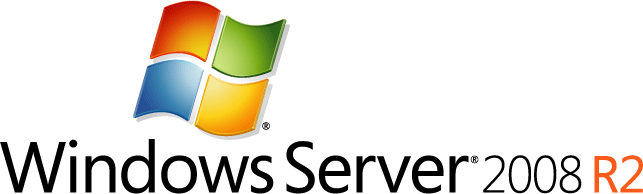
****

****

**Volume Activation Guia de Referência Técnica**

**Windows 7 e Windows Server 2008 R2**

Microsoft Corporation

Publicado em: julho de 2009

Resumo

Este guia de referência é voltado para implementadores de TI (tecnologia da informação) cujas organizações planejem implantar versões com Volume Activation dos sistemas operacionais Windows® 7 e Windows Server® 2008 R2. Ele é um complemento ao *Guia de Planejamento do Volume Activation*, *Guia de Implantação do Volume Activation* e *Guia de Operações do Volume Activation*.

Este documento, assim como qualquer outro mencionado aqui, é fornecido apenas para fins informativos, e a Microsoft não oferece nenhuma garantia, explícita ou implícita, com relação a ele. As informações deste documento, inclusive URLs e outras referências a sites da Internet, estão sujeitas a alterações sem aviso. O usuário assume todos os riscos quanto ao uso ou aos resultados do uso deste documento. A menos que indicado de outra forma, empresas, organizações, produtos, nomes de domínio, endereços de email, logotipos, pessoas, locais e eventos citados aqui são fictícios. Não deve haver associação com nenhum(a) empresa, organização, produto, nome de domínio, endereço de email, logotipo, pessoa, local ou evento real. A conformidade com todas as leis de direitos autorais aplicáveis 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, Hyper-V, 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**

[Introdução 1](#_Toc237163686)

[Experiência de usuário 2](#_Toc237163687)

[Opções de Slmgr.vbs 5](#_Toc237163688)

[Configurações do registro 12](#_Toc237163689)

[Configurações do objeto de diretiva de grupo 15](#_Toc237163690)

[Tempo de ativação do KMS 17](#_Toc237163691)

[Ordem de pesquisa para descoberta do KMS 18](#_Toc237163692)

[Cenários de ativação 19](#_Toc237163693)

[Cenários KMS 19](#_Toc237163694)

[Implementação KMS padrão para uma rede em local único 19](#_Toc237163695)

[Implementação KMS em uma rede complexa e global 20](#_Toc237163696)

[Cenários MAK 23](#_Toc237163697)

[Ativação independente de MAK 24](#_Toc237163698)

[Ativação proxy MAK 28](#_Toc237163699)

[Suporte VAMT para ativação KMS 35](#_Toc237163700)

[Convertendo KMS em ativação por MAK 36](#_Toc237163701)

[Chaves do host do KMS para produtos 38](#_Toc237163702)

[Valores da diretiva de ativação 40](#_Toc237163703)

[Chaves de instalação do Cliente KMS 41](#_Toc237163704)

[Códigos de erro de ativação 43](#_Toc237163705)

[Log de eventos do Windows 53](#_Toc237163706)

[Propriedades e métodos WMI 57](#_Toc237163707)

[Glossário 66](#_Toc237163708)

[Links para recursos 68](#_Toc237163709)

# Introdução

Este guia fornece informações de referência técnica para o [Guia de Planejamento do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926), para o [Guia de Implantação do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150083) e para o [Guia de Operações do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084). Para uma visão geral do Microsoft® Volume Activation e de seus componentes, consulte o [Guia de Planejamento do Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926). Este guia de referência contém:

* Experiência de usuário
* Opções de Slmgr.vbs
* Configurações do Registro
* Configurações do GPO (Objeto de Diretiva de Grupo)
* Tempo de ativação do Serviço de Gerenciamento de Chaves (KMS)
* Ordem de pesquisa para descoberta do KMS
* Cenários de ativação
* Chaves do host do KMS para produtos
* Valores da diretiva de ativação
* Chaves de instalação do cliente KMS
* Códigos de erros de ativação
* Log de eventos do Windows®
* Propriedades e métodos para Instrumentação de Gerenciamento do Windows (WMI)
* Glossário
* Recursos

**Observação**Para suporte de outro software utilizando o Volume Activation, consulte os documentos escritos especificamente para esses aplicativos.

Este guia utiliza as seguintes convenções:

* Linhas de comando e opções de linha de comando aparecem em negrito.
* Os espaços reservados nas opções de linha de comando possuem colchetes angulares (<>) entre eles.
* Opções de linha de comando opcionais possuem colchetes ([]) entre elas.
* Subchave de registro e nomes de valores aparecem em negrito.

# Experiência de usuário

O Windows® 7 e o Windows Server® 2008 R2 exibem notificações e caixas de diálogo direcionadas a problemas específicos de ativação. A Tabela 1 descreve como essas notificações e caixas de diálogo correspondem a cada problema.

**Observação**   As edições básicas do Windows Server 2008 não fornecem as notificações de experiência ao usuário.

Tabela 1. Balões e caixas de diálogo para o estado de notificações

| **Problema** | **Balão de notificação** | **Caixa de diálogo correspondente** |
| --- | --- | --- |
| Uma cópia recém-instalada do Windows não foi ativada no final do período de tolerância da ativação. |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |
| Uma cópia previamente ativada do Windows detecta alterações no hardware do computador ou no BIOS e exige reativação do Windows. Além disso, um cliente KMS ativado não se reativa em 180 dias. |  | 37-HW OOT.jpg |
| O Windows foi ativado com o uso do KMS e sua ativação não foi renovada em 180 dias, além de 30 dias de um período de tolerância. |  | 37-KMS OOT.jpg |
| Falha na validação online ou detecção na exploração da ativação permitem que cópias não autorizadas do Windows burlem a ativação do produto. |  | 37-NG.jpg |
| O Windows detecta que um componente de licença foi alterado. |  | 37 - No Key.jpg |
| O Windows detecta que seus arquivos de licenciamento foram alterados. |  | 37 - Reinstall.jpg |

# Opções de Slmgr.vbs

Devido a alterações WMI no Windows 7 e no Windows Server 2008 R2, o script Slmgr.vbs não se destina ao uso em outras plataformas. O uso do Slmgr.vbs para gerenciar um sistema Windows 7 ou Windows Server 2008 R2 do sistema operacional Windows Vista® não é suportado. Tentar gerenciar um sistema de baixo nível do Windows 7 ou Windows Server 2008 R2 irá gerar um erro de divergência em uma versão específica. Por exemplo, executar **cscript slmgr.vbs <vista\_machine\_name> /dlv** produz o seguinte resultado:

Microsoft (R) Windows Script Host Versão 5.8  
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

A máquina remota não suporta essa versão do SLMgr.vbs

Para gerenciar clientes remotos, utilize a Ferramenta de Gerenciamento do Volume Activation (VAMT) versão 1.2 ou posterior ou crie scripts WMI personalizados que reconheçam as diferenças entre plataformas. Para mais informações sobre as propriedades e os métodos WMI do Volume Activation, consulte a seção, “WMI Properties and Methods,” posteriormente neste guia de referência.

A seguir, veja a descrição da sintaxe do script Slmgr.vbs e a Tabela 2, que descreve cada opção de linha de comando:

slmgr.vbs [MachineName [User Password]] [<Option>]

**Observação**Para suporte de outro software utilizando o Volume Activation, consulte os documentos escritos especificamente para esses aplicativos.

Tabela 2. Opções de linha de comando Slmgr.vbs

| **Opção** | **Descrição** |
| --- | --- |
| **[MachineName]** | Nome de uma máquina remota (padrão é a máquina local) |
| **[User]** | Conta com privilégios exigidos na máquina remota |
| **[Password]** | Senha para conta com privilégios exigidos na máquina remota |
| **Opções globais** | |
| **/ipk product\_key** | Tenta instalar uma chave de produto 5x5. A chave de produto fornecida pelo parâmetro é confirmada como válida e aplicável ao sistema operacional instalado. Caso contrário, um erro será retornado.  Se a chave for válida e aplicável, ela será instalada. Se a chave já estiver instalada, ela será silenciosamente substituída.  Para evitar instabilidades no serviço de licença, o sistema ou o Serviço de Proteção de Software deve ser reiniciado.  Esta operação deve ser executada em um prompt de comando elevado, ou o valor de registro de **Operações de Usuário Padrão** deve ser definido para permitir que usuários não privilegiados obtenham acesso extra ao Serviço de Proteção de Software. |
| **/ato [Activation ID]** | Para edições comerciais e sistemas de volume com uma chave de host do KMS ou MAK (Chave de Ativação Múltipla) instalada, **/ato** aparece no Windows para tentar uma ativação online.  Para sistemas com Chave de Licença de Volume Genérica (GVLK) instalada, isso aparece como uma tentativa de ativação KMS. Os sistemas que foram configurados para suspender as tentativas automáticas de ativação KMS (**/stao**) ainda tentam uma ativação KMS quando **/ato** é executado.  O parâmetro **[Activation ID]** expande o suporte **/ato** para identificar uma edição do Windows instalada no computador. Especificar o parâmetro **[Activation ID]** isola os efeitos da opção da edição associada ao ID de ativação. Execute **Slmgr.vbs /dlv all** para obter os IDs de ativação da versão instalada do Windows. Se você precisar do suporte para outros aplicativos, consulte as orientações fornecidas com o aplicativo para mais instruções.  A ativação KMS não exige privilégios elevados. Porém, a ativação online exige elevação, ou o valor de registro **Operações de Usuário Padrão** deve ser definido para permitir que usuários não privilegiados obtenham acesso extra ao Serviço de Proteção de Software. |
| **/dli [Activation ID | All]** | Exibe informações da licença.  Por padrão, **/dli** exibe as informações da licença para a edição ativa instalada do Windows. Especificar o parâmetro **[Activation ID]** exibe as informações da licença para a edição especificada associada ao ID de ativação. Especificar o **[All]** como parâmetro exibirá todas as informações de licença dos produtos aplicáveis instalados.  A operação não exige privilégios elevados. |
| **/dlv [Activation ID | All]** | Exibe informações detalhadas da licença.  Por padrão, **/dlv** exibe as informações da licença para o sistema operacional instalado. Especificar o parâmetro **[Activation ID]** exibe as informações da licença para a edição especificada associada ao ID de ativação. Especificar o parâmetro **[All]** exibe todas as informações de licença dos produtos aplicáveis instalados.  A operação não exige privilégios elevados. |
| **/xpr [Activation ID]** | Exibe a data de expiração da ativação do produto. Por padrão, isso se refere a edição atual do Windows e é principalmente útil para clientes KMS, porque a ativação comercial e MAK é perpétua.  Especificar o parâmetro **[Activation ID]** exibe a data de expiração da ativação de uma edição específica associada ao ID de ativação.  A operação não exige privilégios elevados. |
| **Opções avançadas** | |
| **/cpky** | Algumas operações de manutenção exigem que a chave de produto esteja disponível no registro durante operações OOBE (Out-of-Box Experience). A opção **/cpky** remove a chave de produto do registro para evitar que essa chave seja roubada por códigos maliciosos.  Para instalações comerciais que implantem chaves, a prática recomendada é executar essa opção. Essa opção não é exigida para chaves de host MAK e KMS, já que esse é o comportamento padrão para essas chaves. Essa opção só é necessária para outros tipos de chave, onde o comportamento padrão não é claro para a chave do registro.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/ilc <license\_file>** | Esta opção instala o arquivo de licença especificado pelo parâmetro solicitado. Essas licenças podem ser instaladas como uma medida de resolução de problemas, para suportar ativações com base em token ou como parte de uma instalação manual de um aplicativo integrado.  As licenças não são validadas durante esse processo: a validação de licença está fora do escopo para o Slmgr. Em vez disso, a validação é tratada pelo Serviço de Proteção de Software no tempo de execução.  Esta operação deve ser executada em um prompt de comando elevado, ou o valor de registro de **Operações de Usuário Padrão** deve ser definido para permitir que usuários não privilegiados obtenham acesso extra ao Serviço de Proteção de Software. |
| **/rilc** | Essa opção reinstala todas as licenças armazenadas em %SystemRoot%\system32\oem e %SystemRoot%\System32\spp\tokens. Essas são cópias "bem conhecidas" armazenadas durante a instalação.  Qualquer licença combinada no Armazenamento Confiável é substituída. Qualquer licença adicional – por exemplo, as Licenças de Publicação (ILs), de Autoridade de Confiança (TA) e licenças para aplicativos – não é editada.  Esta operação deve ser executada em um prompt de comando elevado, ou o valor de registro de **Operações de Usuário Padrão** deve ser definido para permitir que usuários não privilegiados obtenham acesso extra ao Serviço de Proteção de Software. |
| **/rearm** | Esta opção redefine os temporizadores de ativação. O processo **/rearm** também é chamado de **sysprep /generalize**.  Essa operação não fará nada se a subchave de registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm for igual a **1**. Consulte a seção “”, posteriormente neste guia, para detalhes sobre a subchave de registro.  Esta operação deve ser executada em um prompt de comando elevado, ou o valor de registro de **Operações de Usuário Padrão** deve ser definido para permitir que usuários não privilegiados obtenham acesso extra ao Serviço de Proteção de Software. |
| **/upk [ActivationID]** | Esta opção desinstala a chave de produto de uma edição atual do Windows. Após uma reinicialização, o sistema estará em um estado não licenciado, a não ser que uma nova chave de produto seja instalada.  Opcionalmente, você pode utilizar o parâmetro **[Activation ID]** para especificar um produto instalado de maneira diferente.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **Licenciamento de Volume: opções de cliente KMS** | |
| **/skms Name[:Port] | : port [Activation ID] [Activation ID]** | Esta opção especifica o nome e, de maneira opcional, a porta do computador host KMS para entrar em contato. Configurar esse valor desativa a autodetecção do host KMS.  Se o host KMS utilizar apenas o Protocolo de Internet 6 (IPv6), o endereço deverá ser especificado no formato [hostname]:port. Os endereços IPv6 contêm dois pontos (:), os quais serão seguidos pelo script Slmgr.vbs.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/ckms [Activation ID]** | Esta opção remove o nome do host KMS especificado, seu endereço e informações sobre a porta do registro e restaura o comportamento de descoberta automática do KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/skhc** | Esta opção ativa o cache de host KMS (padrão), que bloqueia o uso da **prioridade** e do **peso** do DNS após a descoberta inicial de um host KMS em funcionamento. Se o sistema não puder mais contatar o host KMS em funcionamento, será preciso realizar a descoberta novamente.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/ckhc** | Esta opção desativa o cache do host KMS. Essa configuração instrui o cliente a utilizar a descoberta automática do DNS cada vez que tenta ativar o KMS (recomendada ao se utilizar **prioridade** e **peso**).  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **Configuração de host KMS** | |
| **/sai <interval>** | Esta opção define o intervalo em minutos para que os clientes inativos tentem a conexão KMS. O intervalo de ativação deve ter entre 15 minutos e 30 dias, embora o padrão (2 horas) seja recomendado.  O cliente KMS inicialmente obtém esse intervalo no registro, mas alterna para a configuração do KMS após receber a primeira resposta do KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/sri <interval>** | Esta opção define o intervalo em minutos para que os clientes ativos tentem a conexão KMS. O intervalo de renovação deve ter entre 15 minutos e 30 dias. Essa opção foi definida inicialmente no servidor KMS e nos clientes. O padrão é de 10080 minutos (7 dias).  O cliente KMS inicialmente obtém esse intervalo no registro, mas alterna para a configuração do KMS após receber a primeira resposta do KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/sprt <port>** | Esta opção estabelece a porta na qual o host KMS escuta as solicitações de ativação do cliente. A porta TCP padrão é 1688.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/sdns** | Ativa a publicação do DNS por um host KMS (padrão).  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/cdns** | Desativa a publicação do DNS por um host KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/spri** | Define a prioridade KMS como normal (padrão).  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/cpri** | Define a prioridade KMS como baixa.  Utilize essa opção para minimizar a contenção do KMS em um ambiente co-hospedado. Observe que isso pode levar o KMS à privação, dependendo de quais outros aplicativos ou funções do servidor estiverem ativas. Use com cuidado.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **Configuração da ativação baseada em token** | |
| **/lil** | Lista as licenças de publicação com ativação baseada em token. |
| **/ril <ILID> <ILvID>** | Remove a licença de publicação com ativação baseada em token instalada.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/stao** | Define o sinalizador **Ativação apenas com base em token**, desativando a ativação automática do KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/ctao** | Limpa o sinalizador (padrão) **Ativação apenas com base em token**, permitindo a ativação automática do KMS.  Essa operação deve ser executada diretamente em um prompt de comando elevado. |
| **/ltc** | Lista certificados válidos de ativação com base em token que podem ativar software instalado. |
| **/fta <Certificate Thumbprint> [PIN]** | Força a ativação com base em token utilizando o certificado identificado. O número de identificação pessoal opcional (PIN) é fornecido para desbloquear a chave privada sem um prompt de PIN ao se utilizar certificados protegidos por hardware (por exemplo, cartões inteligentes). |

# Configurações do registro

A Tabela 3 descreve as configurações de registro que o Volume Activation suporta.

Tabela 3. Configurações de registro

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subchave do registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **Valor** | **Tipo** | | **Descrição** | | **Escopo** |
| **Activation\AlternateURL** | **REG\_SZ** | | Opcionalmente, contém uma URL fornecida pelo administrador. Se essa chave for preenchida, algumas caixas de diálogo de ativação terão um novo link – **Saiba mais sobre ativação online** – que será aberto no navegador padrão. | | Tudo |
| **DisableDnsPublishing** | **REG\_DWORD** | | Define em um valor diferente de zero a fim de bloquear a publicação automática para DNS pelo host KMS. | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **Formato:** nome\_de\_domínio, <prioridade>, <peso>  Opcionalmente, contém uma lista de domínios totalmente qualificados que o KMS usa para publicar automaticamente o registro do serviço DNS (SRV). O domínio inicial do KMS sempre é usado, portanto, não é necessário incluí-lo aqui. Isso depende do valor **DisableDnsPublishing**.   Os parâmetros **priority** (prioridade) e **weight** (peso) são opcionais. Se não forem fornecidos, serão definidos como **0** no registro SRV. | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | Defina em um valor diferente de zero para minimizar a contenção do KMS em um ambiente co-hospedado. Observe que, em um sistema ocupado, isso pode evitar que o host KMS mantenha uma contagem suficiente. | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | Defina este valor no host KMS para forçar o KMS a escutar na porta TCP especificada. O host utilizará a porta TCP 1688 se o valor não for especificado. | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | Defina esse valor para forçar o uso de um host KMS específico pelo cliente KMS. Sem padrão.  Se uma App-ID ou SKU-ID for especificada, ela será criada em uma subchave em que o valor está armazenado:  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName | | Cliente KMS |
| **KeyManagementServicePort** | **REG\_SZ** | | Defina esse valor para forçar o uso de uma porta TCP específica pelo cliente KMS quando ele se comunicar com um KMS. O cliente utilizará a porta TCP 1688 se esse valor não for especificado.  Se uma App-ID ou SKU-ID for especificada, ela será criada em uma subchave em que o valor está armazenado:  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort | | Cliente KMS |
| **KeyManagementServiceVersion** | **REG\_SZ** | | Defina este valor para a descoberta automática do KMS no MOM (Microsoft Operation Manager) 2005. Exclua este valor se o KMS não estiver mais em operação na máquina. | | KMS |
| **UserOperations** | **REG\_DWORD** | | Este valor não existe por padrão, e o padrão é **0**, o que exige elevação. Crie esse valor e defina-o como **1** para permitir que usuários padrão instalem as chaves de produto, ativem e rearmem as máquinas sem exigir elevação.  Essa configuração também pode ser feita por GPOs, que estão armazenados na subchave de registro **\policies**. | | Tudo (não apenas KMS) |
| **VLActivationInterval** | **REG\_DWORD** | | Inicialmente definido nos clientes e servidores KMS. O padrão é de 120 minutos (2 horas). O cliente KMS inicialmente obtém esse intervalo no registro, mas alterna para a configuração do KMS após receber a primeira resposta do KMS. O valor mínimo é de 15 minutos, e o máximo, de 43.200 minutos (30 dias). | | Cliente e servidor KMS |
| **VLRenewalInterval** | **REG\_DWORD** | | Inicialmente definido nos clientes e servidores KMS. O padrão é de 10.080 minutos (7 dias). O cliente KMS inicialmente obtém esse intervalo no registro, mas alterna para a configuração do KMS após receber a primeira resposta do KMS. Como resultado, a configuração do cliente nunca será utilizada. O valor mínimo é de 15 minutos, e o máximo, de 43.200 minutos (30 dias). | | Cliente e servidor KMS |
| **Subchave do registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **Valor** | **Tipo** | **Descrição** | | **Escopo** | |
| **Manual** | **REG\_DWORD** | **0** = Permite ativação automática online (padrão)  **1** = Desabilita ativação automática | | Host MAK e KMS, mas não cliente KMS | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = Os avisos e balões de ativação serão exibidos (padrão)  **1** = Todos os avisos relacionados à ativação serão ocultos se o Windows não estiver em estado de Notificação ou Não Licenciado. Não recomendado. | | Tudo (não apenas KMS) | |

# Configurações do objeto de diretiva de grupo

A Tabela 4 descreve as configurações de Diretiva de Grupo que as organizações podem utilizar para evitar que o sistema operacional altere a área de trabalho para preto no estado Notificações.

Tabela 4. Configurações do objeto de diretiva de grupo

| **Nome da diretiva** | **Descrição** |
| --- | --- |
| **Configuração do Usuário -> Ferramentas Administrativas -> Painel de Controle -> Personalização -> Impedir a alteração de plano de fundo da área de trabalho** | Impede que os usuários adicionem ou alterem o design do plano de fundo da área de trabalho.  Por padrão, os usuários podem utilizar a página **Plano de Fundo da Área de Trabalho** no item Personalização ou Vídeo do Painel de Controle para adicionar um design de plano de fundo (papel de parede) à área de trabalho.  Se você ativar essa configuração, o usuário não poderá alterar nenhuma das configurações do Plano de Fundo da Área de Trabalho.  Para especificar o papel de parede para um grupo, utilize a configuração **Papel de Parede da Área de Trabalho**.  **Observação**   Você também deve ativar a configuração **Papel de Parede da Área de Trabalho** para impedir que os usuários alterem o papel de parede da área de trabalho. Consulte o artigo de Ajuda e Suporte da Microsoft, “É possível alterar o papel de parede da Área de Trabalho após o administrador selecionar a opção ‘Impedir alteração de papel de parede" na Diretiva de grupo", em <http://support.microsoft.com/kb/Q327998> para mais informações.  Além disso, veja a configuração **Permitir somente papel de parede de bitmap**. |
| **Configuração do Usuário -> Ferramentas Administrativas -> Área de Trabalho -> Área de Trabalho -> Papel de Parede da Área de Trabalho** | Especifica o plano de fundo da área de trabalho ("papel de parede") exibido nas áreas de trabalho de todos os usuários.  Essa configuração permite que você especifique o papel de parede das áreas de trabalho e evita que os usuários alterem a imagem ou a apresentação. O papel de parede que você especifica pode ser armazenado em um arquivo bitmap (\*.bmp) ou JPEG (\*.jpg).  Para utilizar essa configuração, digite o caminho totalmente qualificado e o nome do arquivo que armazena a imagem do papel de parede. Você pode digitar o caminho local, como C:\Windows\web\wallpaper\home.jpg, ou o UNC (Convenção de Nomenclatura Universal), como \\Server\Share\Corp.jpg. Se o arquivo especificado não estiver disponível quando o usuário fizer o logon, nenhum papel de parede será exibido. Os usuários não podem especificar papéis de parede alternativos. Você também pode utilizar essa configuração para especificar se a imagem do papel de parede ficará centralizada, lado a lado ou ajustada à tela. Os usuários não podem alterar essa especificação.  Se você desativar essa configuração ou não configurá-la, nenhum papel de parede será exibido. Porém, os usuários podem selecionar o papel de parede preferido.  Além disso, veja a configuração **Permitir somente papel de parede de bitmap** no mesmo local e a configuração **Impedir alteração de papel de parede** em Configuração do Usuário\Modelos Administrativos\Painel de Controle.  **Observação**   Essa configuração não se aplica às sessões de servidor de área de trabalho remota. |
| **Configuração do Usuário -> Ferramentas Administrativas -> Painel de Controle -> Personalização -> Impedir a alteração de ícones da área de trabalho** | Evita que os usuários alterem os ícones da área de trabalho.  Por padrão, os usuários podem utilizar a caixa de diálogo **Configurações dos Ícones da Área de Trabalho** no item Personalização ou Vídeo do Painel de Controle para exibir, ocultar ou alterar os ícones da área de trabalho.  Se você ativar essa configuração, o usuário não poderá alterar nenhum dos ícones da área de trabalho.  Para sistemas operacionais anteriores ao Windows Vista, essa configuração também oculta a guia **Área de Trabalho** no item Vídeo do Painel de Controle. |

# Tempo de ativação do KMS

O tempo de ativação do KMS é controlado por duas configurações: temporizadores de ativação e renovação:

* O Intervalo de Ativação do KMS determina com que frequência o cliente KMS tenta a ativação antes de realmente ser ativado e durante Notificações e Cortesia. O valor é definido no cliente ao se executar **slmgr.vbs /sai *interval***. O intervalo é expresso em minutos, e 120 minutos é o padrão. Consulte as seções “Slmgr.vbs Options” e “Registry Settings” para mais informações. Assim que um sistema entrar em contato com um host KMS, a configuração do host KMS substituirá a configuração do cliente local.
* O Intervalo de Renovação KMS determina com que frequência o cliente KMS tenta a reativação com o KMS, uma vez que tenha sido ativado. Esse valor pode ser definido ao se utilizar **slmgr /sri *interval***. O intervalo é definido em minutos. O valor padrão é de 10.080 minutos (7 dias). Esse valor pode ser definido no cliente, mas será substituído pelo valor que o host KMS fornece.

Na operação, o cliente KMS tenta entrar em contato com um host KMS na inicialização e novamente nos minutos do intervalo de ativação após a falha. Por padrão, isso ocorre a cada duas horas. Quando a ativação do KMS for realizada com êxito, o cliente receberá e armazenará o intervalo de renovação do host KMS, e o Windows o ativará por 180 dias. A renovação de ativação opera como uma janela deslizante, igual à concessão do protocolo DHCP (Dynamic Host Configuration Protocol). O cliente é ativado por 180 dias, mas ainda tenta a reativação nos minutos do intervalo de renovação – por padrão, 7 dias. Se essa operação for feita com êxito, o período de 180 dias será reiniciado. Se falhar, o sistema observará as alterações de rede ou outros eventos qualificados para disparar outra tentativa. Após 15 minutos, o sistema para de monitorar os eventos qualificados, mas ainda faz tentativas nos minutos do intervalo de ativação.

Se os 180 dias passarem sem uma reativação realizada com êxito, o cliente fará transições para Cortesia OOT (Out of Tolerance). Se não for ativado nos 30 dias de transição para OOT, ele entrará no modo de Notificação.

# Ordem de pesquisa para descoberta do KMS

Quando a descoberta automática do KMS estiver ativada (padrão) e o cache do host KMS não estiver desativado, os clientes KMS usarão a seguinte ordem para determinar qual KMS utilizar (eles tentarão cada etapa até que um host KMS ativado com a chave correta responda):

* O valor específico de SKU no valor de registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ
* O valor específico de AppID no valor de registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ
* O valor global no valor de registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ
* Host KMS com cache específico de SKU (essa é a identidade em cache do host utilizado na última ativação KMS com êxito).
* Descoberta automática do DNS (**weight** e **priority** considerados)

Se um KMS em cache não responder, a descoberta será realizada.

# Cenários de ativação

As seguintes seções descrevem os cenários principais para a ativação KMS e MAK.

## Cenários KMS

O KMS pode suportar redes simples em um único local e redes globais. Os seguintes cenários mostram:

* A implementação padrão do KMS.
* A implementação expandida para suportar uma rede global.

### Implementação KMS padrão para uma rede em local único

A Contoso possui 100 clientes Windows 7 Enterprise e um conjunto misto de sistemas Windows Vista, Windows Server 2008 e Windows Server 2008 R2. A Contoso é um domínio genérico (Contoso.com), conforme exibido na Figura 1. O servidor DNS executa Microsoft DNS em sua configuração padrão. Essa configuração suporta o registro DNS dinâmico e o registro de procura para remover registros obsoletos.



Figura 1. Implementação KMS padrão para rede em um único local

A Contoso adquire um acordo de licença que fornece a chave KMS B, a qual ativará todos os sistemas. O administrador de TI (tecnologia de informação) instala a chave do host KMS da Contoso (CSVLK) em dois hosts KMS executando o Windows Server 2008 R2 ao utilizar o seguinte comando executado localmente em um prompt de comando elevado:

Slmgr.vbs /ipk <chave\_host\_KMS>

O administrador de TI então cria um Grupo de Segurança no AD DS (Active Directory® Domain Services) denominado *KMS\_Hosts.* O administrador adiciona os servidores KMS\_1 e KMS\_2 à associação KMS\_Hosts.

O host KMS\_1 é ativado na Microsoft pela Internet: **Slmgr.vbs /ato**. O KMS\_1 publica automaticamente os registros de recurso (RRs) SRV para o DNS. O administrador de TI acessa o servidor DNS, localiza o RR para \_vlmcs.\_tcp.contoso.com e altera suas permissões para fornecer permissão de Leitura, Gravação e Exclusão do KMS\_Hosts no registro. O host KMS\_2 agora é ativado na Microsoft pela Internet: **Slmgr.vbs /ato***.*

Por fim, o administrador confirma que a exclusão do host KMS está ativada no Firewall do Windows. A exceção de firewall do Serviço de Gerenciamento de Chaves precisa ser ativada.

Os clientes KMS na rede Contoso consultam o DNS e recebem os registros SRV para ambos os hosts KMS. Os clientes escolhem um ou o outro host e são ativados (assim que a contagem do KMS ultrapassar o limite). Consulte a seção, “Activation Policy Values,” para mais informações sobre os requisitos de contagem do KMS.

### Implementação KMS em uma rede complexa e global

A Contoso se expandiu para dois domínios, east.contoso.com e west.contoso.com, conforme exibido na Figura 2. O tráfego de rede pode passar, de maneira particular, entre duas redes através de um link com firewall da WAN (wide area network). Esse link limitou a largura de banda. Dessa forma, os recursos (incluindo DNS) são replicados nos dois lados do link WAN para reduzir o tráfego, quando possível.



Figura 2. Implementação KMS em uma rede complexa e global

A Contoso utiliza implantação com base em imagens. Os sistemas do cliente são padronizados no Windows Vista, mas os sistemas Windows Vista estão sendo substituídos por clientes Windows 7.

Os usuários normalmente viajam, e a conexão de rede é alterada de um domínio para outro. O endereço IP dos clientes é fornecido dinamicamente pelo DHCP, incluindo a especificação do host DNS local, endereço de gateway local etc.

Para oferecer o suporte de ativação aos clientes existentes Windows Vista e aos novos clientes Windows 7, a Contoso instala quatro hosts KMS (utilizando a chave KMS B). Dois hosts KMS estão configurados em east.contoso.com e dois, em west.contoso.com.

O administrador de TI configura os hosts KMS para que os registros DNS SRV direcionem os clientes Windows 7 e Windows Server 2008 R2 no domínio leste para KMS\_E1, se disponível, ou para KMS\_E2. Se nenhum dos dois estiver disponível, os clientes tentarão KMS\_W1 e, finalmente, KMS\_W2. Da mesma forma, o DNS no domínio oeste está configurado para que os clientes Windows 7 no domínio oeste prefiram contatar KMS\_W1 e KMS\_W2 e, apenas em caso de falha, a ativação será tentada em KMS\_E1 e KMS\_E2 no lado distante do link WAN.

O administrador de TI consegue isso ao fazer as seguintes alterações na configuração (ver Tabela 5):

* Os hosts KMS\_E\* são adicionados ao grupo de segurança KMS\_E. Esse grupo recebe os direitos de Leitura, Gravação e Exclusão para o registro \_vlmcs.\_tcp.east.contoso.com.
* Os hosts KMS\_W\* são adicionados ao grupo de segurança KMS\_W. Esse grupo recebe os direitos de Leitura, Gravação e Exclusão para o registro \_vlmcs.\_tcp.west.contoso.com.
* Os servidores DHCP foram configurados para adicionar o east.contoso.com e o west.contoso.com à lista de pesquisa do sufixo DNS para todos os clientes.
* Os firewalls entre os domínios leste e oeste estão configurados para permitir o tráfego RPC aos hosts KMS na porta 1688.

Tabela 5. Configuração do host KMS

| **Descrição** | **Configuração** | **Host** |
| --- | --- | --- |
| Configura a prioridade e o peso SRV de east.contoso.com para que os clientes entrem em contato com hosts KMS\_E\* se disponível antes de tentar os hosts KMS\_W\* O tráfego será dividido: 75% para os hosts KMS\_1\* e 25% para os 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 |
| Configura a prioridade e o peso SRV de west.contoso.com para que os clientes entrem em contato com hosts KMS\_W\* se disponível antes de tentar os hosts KMS\_E\* O tráfego será dividido: 75% para os hosts KMS\_1\* e 25% para os 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 |

Em seguida, o administrador confirma que as exceções do Firewall do Windows são definidas para permitir o tráfego do cliente KMS e configura os computadores cliente, como a Tabela 6 descreve.

Tabela 6. Configuração do cliente KMS

| **Descrição** | **Configuração** |
| --- | --- |
| Desativa o cache do host KMS | **Slmgr /ckhc** |
| Uma URL do cliente é configurada para direcionar os usuários com problemas de ativação para o suporte técnico da Contoso | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  AlternateURL = http://contoso.com/help |

O computador cliente de referência é ativado pelo KMS, e **sysprep /generalize** é executado. O sistema é desligado e bloqueado com o uso do ImageX do Windows AIK (Kit de Instalação Automatizada) do Windows 7. O Windows AIK está disponível para download em <http://go.microsoft.com/fwlink/?LinkId=136976>.

## Cenários MAK

As seguintes seções descrevem os cenários para ativação MAK, os quais estão baseados no cenário exibido na Figura 3. Essa figura exibe ambientes de rede e de grupo de trabalho que são típicos das grandes empresas.

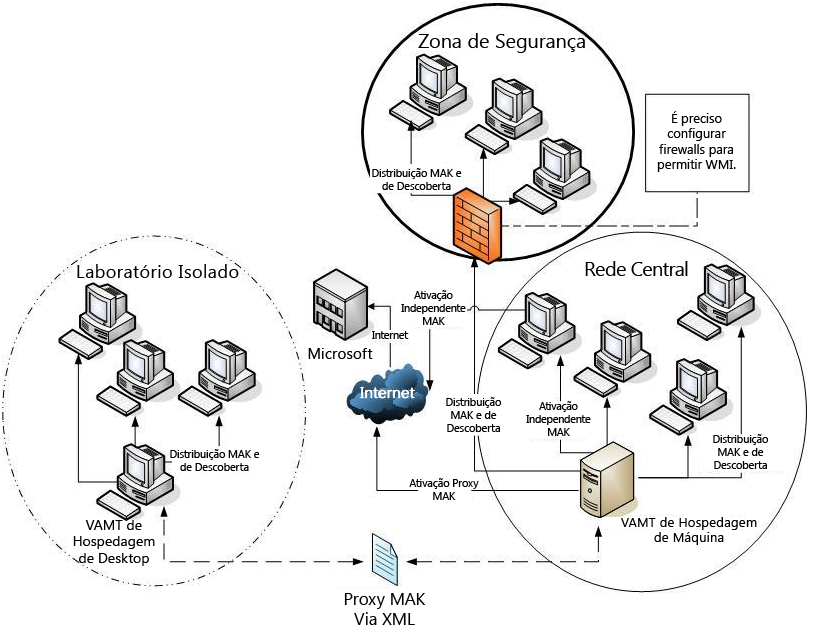


Figura 3. Ambientes corporativos

No ambiente de Rede Principal, todos os computadores estão em uma rede comum gerenciada pelo AD DS. A Zona de Segurança representa computadores de Rede Principal de maior segurança que possuem proteção adicional de firewall.

O ambiente Laboratório Isolado é um grupo de trabalho fisicamente separado da Rede Principal, e seus computadores não possuem acesso à Internet. A diretiva de segurança da rede afirma que nenhuma informação que possa identificar um computador ou usuário específico pode ser transferida para fora do Laboratório Isolado.

### Ativação independente de MAK

A VAMT permite a automatização da implantação MAK e a ativação pela rede por meio da distribuição de 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 VAMT versão 1.2 está inclusa no Windows AIK.

Nesse cenário, a VAMT é implantada no ambiente de Rede Principal exibido na Figura 3. A VAMT é instalada no computador central com acesso à rede para todos os computadores cliente. O host VAMT e os computadores cliente possuem acesso à Internet. As seguintes instruções descrevem como executar uma ativação independente:

1. Instale e inicie a VAMT em um computador host conectado a uma rede:
2. Instale o Windows AIK no computador host.
3. Clique em Iniciar e clique em **VAMT** para abrir o console VAMT.
4. Configure a exceção de firewall da Instrumentação do Gerenciamento do Windows (WMI) nos computadores de destino. Verifique se a exceção do firewall WMI foi ativada para todos os computadores de destino, conforme exibido na Figura 4.

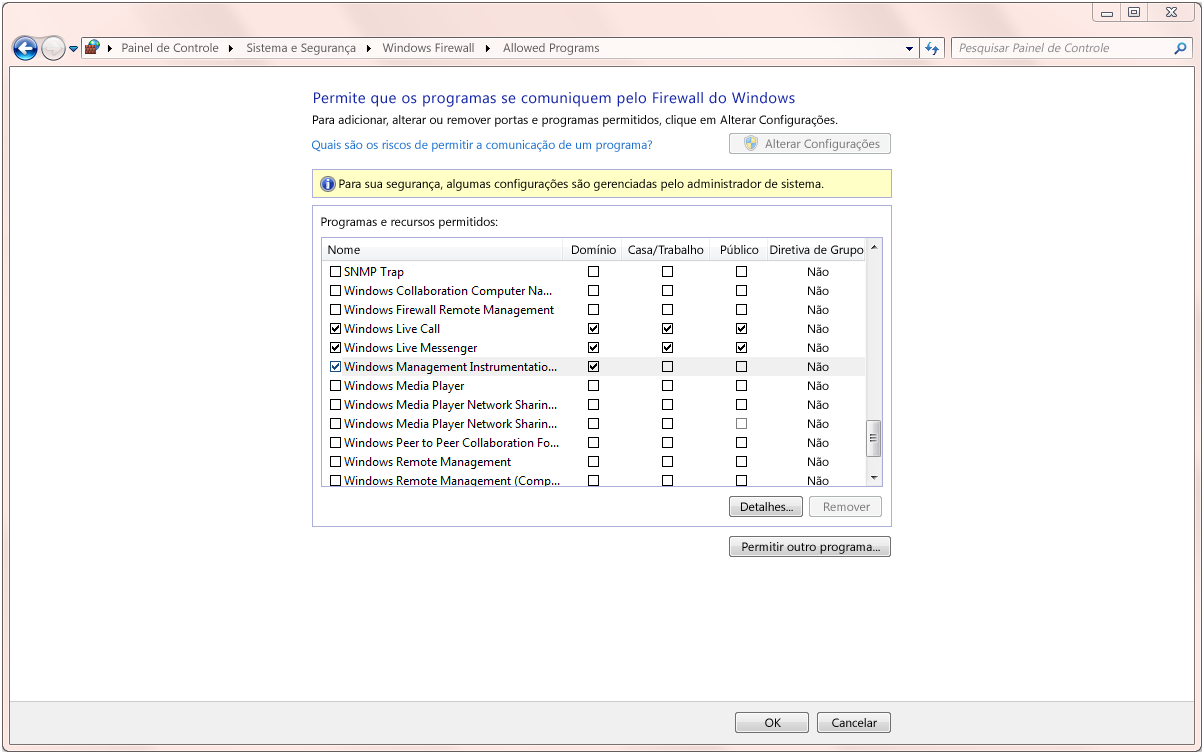


Figura 4. Exceção da Instrumentação do Gerenciamento do Windows (WMI)

1. Adicione computadores à CIL (lista de informações sobre o computador):
2. No console VAMT, clique em **Ação**, clique em **Adicionar Computadores** para exibir a caixa de diálogo **Adicionar Computadores**.
3. Digite um nome para o Grupo de Computadores como *Grupo de Rede Principal* para identificar o grupo de computadores que você está ativando.
4. Clique na lista suspensa para selecionar uma opção de pesquisa. Você pode pesquisar computadores em um grupo de trabalho, em um domínio AD DS ou pelo nome individual do computador ou endereço IP.
5. Se você estiver pesquisando por nome individual do computador ou endereço IP, digite as informações na caixa de texto abaixo da lista suspensa.
6. Se você estiver pesquisando um domínio ou grupo de trabalho, selecione-os em uma lista suspensa adicional exibida para essas opções. Utilize o campo **Filtrar por nome do computador** para pesquisar um computador específico dentro do domínio ou grupo de trabalho.
7. Clique em **OK**.

A VAMT consulta o AD DS (Active Directory Directory Services) via Protocolo LDAP (Lightweight Directory Access Protocol) e adiciona os computadores encontrados à CIL.

1. Coletar informações de status dos computadores descobertos:
2. Para a VAMT realizar uma ação em um computador, é preciso ter dados atuais do status de licença desse computador. Colete o status de computadores individuais ao selecionar diretamente um ou mais computadores no painel de exibição da lista de computadores. Para realizar operações para um grupo inteiro, no painel de exibição em árvore, selecione o nó Status Desconhecido ou o nó Grupos Definidos pelo Usuário\Grupo de Rede Principal.
3. Clique com o botão direito do mouse no grupo ou nos computadores desejados e clique em **Atualizar Status do Computador**.
4. Se você estiver ativando computadores que exijam credenciais de administrador diferentes das que você já utiliza, selecione **Utilizar Credenciais Alternativas**.
5. Clique em **OK**.
6. Forneça uma conta de Administrador de Domínio (para coletar status de todos os computadores do domínio) e senha, quando solicitado.

A VAMT exibe a caixa de diálogo **Coletar Informações do Computador** enquanto coleta o status de todos os computadores selecionados. Quando o processo for finalizado, o status atualizado de cada computador aparecerá no painel de exibição em lista de computadores no console VAMT.

**Observação**   Para recuperar o status da licença nos computadores selecionados, a VAMT deve ter permissões administrativas nos computadores remotos, e a WMI deve estar acessível pelo Windows Firewall. Além disso, para computadores de grupos de trabalho, uma chave de registro deve ser criada para ativar as ações administrativas remotas no Controle de Conta de Usuário (UAC). Para mais informações sobre configuração de sistemas para o gerenciamento remoto da VAMT, consulte a ajuda VAMT.

1. Adicione uma MAK e determine a contagem de ativação restante:
2. Clique em **Opções**, clique em **Gerenciar MAKs** para abrir a caixa de diálogo **Gerenciar Chaves MAK**.
3. Clique em **Adicionar** para incluir uma MAK.
4. Inclua uma MAK e clique em **Validar**.

Uma vez validado, o campo **Edição** é automaticamente preenchido.

1. Forneça uma descrição significativa e clique em **Adicionar**.

A MAK agora está listada na caixa de diálogo **Gerenciar Chaves MAK**.

1. Clique em **Atualizar Contagem Restante** para recuperar o número de ativações restantes da Microsoft para as MAKs listadas (essa etapa exige conexão com a Internet).
2. Clique em **Sair** para fechar a caixa de diálogo.
3. Instale a MAK e ative os computadores cliente:
4. Selecione os computadores a serem ativados, clicando em um grupo no painel de exibição em árvore ou selecionando computadores individuais no painel de exibição em lista.
5. Clique com o botão direito do mouse no grupo selecionado ou nos computadores e clique em **Ativar MAK Independente** para exibir a caixa de diálogo **Ativar MAK Independente**.
6. Selecione a MAK apropriada na lista **Instalar MAK**.
7. Selecione as caixas de seleção **Instalar MAK (substituir existente)** e **Ativar Agora** para instruir os computadores selecionados a serem ativados imediatamente ao contatar o Microsoft Windows Activation pela Internet.

Se um asterisco (\*) aparecer próximo ao texto dessas caixas de verificação, a ação será aplicada apenas aos computadores aplicáveis. Por exemplo, um computador com a edição comercial do Windows Vista instalada não pode ser ativado com uso de uma MAK.

1. Se estiver ativando computadores que exijam credenciais de administrador diferentes das que você já utiliza, selecione **Usar Credenciais Alternativas**.
2. Clique em **OK**.

A VAMT exibe a caixa de diálogo **Atribuir Chaves de Produto** e exibe a caixa de diálogo **Ativar Computadores** até que a ação solicitada seja concluída. Se tiver selecionado **Utilizar Credenciais Alternativas**, você precisará digitar as credenciais antes dessas caixas de diálogo.

### Ativação proxy MAK

Nesse cenário, a VAMT é utilizada para ativar os computadores de grupo de trabalho dentro do ambiente de Laboratório Isolado exibido na Figura 3. Para grupos de trabalho como esse, que estão completamente isolados da rede maior, você pode executar a ativação proxy MAK ao instalar uma segunda VAMT no computador dentro do grupo de trabalho isolado e utilizar mídia removível para transferir as CILs da VAMT entre o computador e outro host VAMT que possui acesso à Internet. Para mais informações sobre configuração de sistemas para o gerenciamento remoto da VAMT, consulte a ajuda VAMT. As seguintes etapas descrevem como utilizar a ferramenta VAMT para ativação de proxy:

1. Instale a VAMT em um computador de grupo de trabalho no Laboratório Isolado:
2. Instale o Windows AIK em um computador host no grupo de trabalho de Laboratório Isolado.

Este computador pode executar Windows XP with Service Pack 2 (SP2), Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2.

1. Clique em Iniciar e clique em **VAMT** para abrir o console VAMT.
2. Configure a exceção de firewall da Instrumentação do Gerenciamento do Windows (WMI) nos computadores de destino. Verifique se a exceção de firewall WMI foi ativada em todos os computadores de destino.
3. Adicione computadores à CIL:
4. No console VAMT, clique em **Ação**, clique em **Adicionar Computadores** para abrir a caixa de diálogo **Adicionar Computadores**.
5. Digite um nome para o Grupo de Computadores, como *Grupo Laboratório Isolado*, para identificar o grupo de computadores que você está ativando.
6. Selecione a opção **Grupo de Trabalho** e especifique o nome do grupo de trabalho e, em seguida, clique em **OK**.

A VAMT pesquisa o grupo de trabalho por computadores.

**Observação**   Para a VAMT descobrir os computadores cliente em um grupo de trabalho, a exceção do Firewall do Windows para a descoberta de rede deve estar ativada.

1. Colete o status dos computadores descobertos:
2. Para a VAMT realizar uma ação em um computador, é preciso ter dados atuais do status de licença desse computador. Colete o status de computadores individuais ao selecionar diretamente um ou mais computadores no painel de exibição da lista de computadores. Para realizar operações para um grupo inteiro, no painel esquerdo, selecione o nó Status Desconhecido ou o nó Grupos Definidos pelo Usuário\Grupo de Laboratório Isolado.
3. Clique com o botão direito do mouse no grupo ou nos computadores desejados e clique em **Atualizar Status do Computador**.
4. Se estiver ativando computadores que exijam credenciais de administrador diferentes das que você já utiliza, selecione **Usar Credenciais Alternativas**.
5. Clique em **OK**. Ao ser solicitado, forneça as credenciais para uma conta que possua direitos administrativos locais nos computadores do grupo de trabalho selecionado.

A VAMT exibe a caixa de diálogo **Coletar Informações do Computador** enquanto coleta o status de todos os computadores selecionados. Quando o processo for finalizado, o status atualizado de cada computador aparecerá no painel de exibição em lista de computadores no console VAMT.

**Observação**   Para recuperar o status da licença nos computadores selecionados, a VAMT deve ter permissões administrativas nos computadores remotos, e a WMI deve estar acessível pelo Windows Firewall. Além disso, para computadores de grupos de trabalho, uma chave de registro deve ser criada para ativar as ações administrativas remotas no UAC.

1. Adicione uma MAK:
2. Clique em **Opções**, clique em **Gerenciar MAKs** para abrir a caixa de diálogo **Gerenciar Chaves MAK**.
3. Clique em **Adicionar** para incluir uma MAK.
4. Inclua uma MAK e clique em **Validar**.

Uma vez validado, o campo **Edição** é automaticamente preenchido.

1. Forneça uma descrição significativa e clique em **Adicionar**.

A MAK agora está listada na caixa de diálogo **Gerenciar Chaves MAK**.

1. Clique em **Sair** para fechar a caixa de diálogo.

**Observação**   Como a VAMT não está instalada em um computador com acesso à Internet, a opção **Atualizar Contagem Restante** não ficará disponível. Esse recurso exige acesso à Internet.

1. Instale a MAK em computadores de Laboratório Isolado:
2. Selecione o grupo de Laboratório Isolado no painel de exibição em árvore.
3. Clique com o botão direito do mouse no grupo selecionado ou nos computadores e clique em **Ativar Proxy MAK** para exibir a caixa de diálogo **Ativar Proxy MAK**.
4. Selecione a MAK apropriada na lista **Instalar MAK**.
5. Selecione **Instalar MAK (substituir existente)**.

Se um asterisco (\*) aparecer próximo ao texto dessa caixa de seleção, a ação será aplicada apenas aos computadores aplicáveis. Por exemplo, um computador com a edição comercial do Windows Vista instalada não pode ser ativado com uso de uma MAK.

1. Desmarque a caixa de seleção **Obter ID Confirmação da Microsoft**, pois esse computador não possui acesso à Internet.
2. Desmarque a caixa de seleção **Aplicar ID de Confirmação e Ativar**, pois os IDs de confirmação (CIDs) ainda não foram solicitados.
3. Se você estiver ativando computadores que exijam credenciais de administrador diferentes das que você já utiliza, selecione **Usar Credenciais Alternativas** e clique em **OK**.

A VAMT exibe a caixa de diálogo **Atribuir Chaves de Produto** até a ação solicitada ser concluída. Se tiver selecionado **Utilizar Credenciais Alternativas**, você precisará digitar as credenciais antes dessa caixa de diálogo.

**Observação**   Marcar a caixa de seleção **Instalar MAK (substituir existente)** força a instalação de uma MAK no computador cliente. Isso deve ser feito com cuidado. Se a versão pré-SP1 do Windows Vista estiver instalada no computador por mais de 30 dias, o seu período de cortesia inicial terá expirado, e o computador entrará no Modo de Funcionalidade Reduzida (RFM) se a ativação não for concluída com êxito antes do logon seguinte. Porém, você pode utilizar a ativação do proxy MAK para recuperar computadores configurados corretamente do RFM, contanto que os computadores estejam acessíveis ao host VAMT. O RFM apenas se aplica à versão pré-SP1 do Windows Vista. Windows Vista SP1 ou mais recente, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 não entrará no RFM.

1. Salve a CIL:

Nesta etapa, a CIL completa é salva no host VAMT local (isto é, grupo de trabalho). Na ativação do proxy MAK, é essencial reter esse arquivo, pois a VAMT o utiliza para aplicar os CIDs aos computadores corretos.

1. Ao utilizar o painel de exibição em lista ou em árvore da VAMT, selecione o grupo ou os computadores individuais que receberam uma MAK com êxito.
2. No menu **Arquivo**, clique em **Salvar** para exibir a caixa de diálogo **Salvar Lista de Informações do Computador**.
3. Selecione um diretório e digite um nome de arquivo CIL, como *IsolatedLabGroup.CIL.*
4. Clique em **Salvar**.
5. Exporte a CIL:

Conforme mencionado anteriormente, a diretiva de segurança da rede da empresa afirma que nenhuma informação que possa identificar um computador ou usuário específico pode ser transferida para fora do Laboratório Isolado. Portanto, esse tipo de dado deve ser excluído do arquivo CIL para ser transferido para o host VAMT da Rede Principal.

1. Ao utilizar o painel de exibição em lista ou em árvore da VAMT, selecione o grupo ou os computadores individuais que receberam uma MAK com êxito.
2. Clique com o botão direito do mouse no grupo selecionado ou nos computadores e clique em **Exportar Computadores** para exibir a caixa de diálogo **Salvar Lista de Informações do Computador**.
3. Selecione **Excluir dados sensíveis de ambiente**.
4. Clique em **Procurar** para exibir a caixa de diálogo **Salvar como**.
5. Selecione um diretório e digite um nome de arquivo CIL, como *IsolatedLabGroupSecureExport.CIL.*
6. Clique em **Salvar**.
7. Copie o arquivo IsolatedLabGroupSecureExport.CIL para uma mídia removível (disquete, CD/DVD ou unidade flash USB [UFD]).

**Observação**   Se a caixa de seleção **Excluir dados sensíveis de ambiente** for marcada, as PII (Informações de Identificação Pessoal) não serão salvas na CIL. Como resultado, a CIL deve ser reimportada nesse host VAMT e no arquivo CIL totalmente salvo para que os CIDs solicitados pela Microsoft possam ser atribuídos corretamente aos computadores do grupo Laboratório Isolado.

1. Importe a CIL em um host VAMT com acesso à Internet:
2. Copie IsolatedLabGroupSecureExport.CIL de uma mídia removível para uma unidade no host VAMT que possua acesso à Internet.
3. Abra o console VAMT.
4. No menu **Arquivo**, clique em **Importar** para abrir a caixa de diálogo **Abrir Lista de Informações do Computador**.
5. Localize e selecione **IsolatedLabGroupSecureExport.CIL** e clique em **Abrir** para carregar a CIL na VAMT.
6. Confirme se os nomes do computador, do grupo e do grupo de trabalho não estão visíveis.
7. Solicite os CIDs da Microsoft:
8. Clique com o botão direito do mouse nos computadores importados e clique em **Ativar Proxy MAK** para abrir a caixa de diálogo **Ativar Proxy MAK**.
9. Desmarque a caixa de seleção **Instalar MAK (substituir existente)**.
10. Desmarque a caixa de seleção **Obter ID de Confirmação da Microsoft**.
11. Desmarque a caixa de seleção **Aplicar ID de Confirmação e Ativar**, pois esse host VAMT não está na mesma rede dos computadores selecionados.
12. Clique em **OK**.

A VAMT exibe a caixa de diálogo **Adquirir ID de Confirmação Online** enquanto entra em contato com a Microsoft e coleta os CIDs.

1. Exporte a CIL do host VAMT conectado à Internet:
2. Após os CIDs terem sido recuperados para todos os computadores, salve o arquivo CIL. No console VAMT, role para a direita e confirme se a coluna **PendingCID** possui valores.
3. No menu **Arquivo**, clique em **Salvar como** e forneça um novo nome para o arquivo, como *IsolatedLabGroupSecureExportwithCID.CIL.*
4. Copie o arquivo atualizado IsolatedLabGroupSecureExportwithCID.CIL para uma mídia removível (disquete, CD/DVD ou UFD).
5. Importe a CIL no host VAMT original dentro do Laboratório Isolado:
6. Copie IsolatedLabGroupSecureExportwithCID.CIL de uma mídia removível para uma unidade no host VAMT do Laboratório Isolado.
7. Abra o console VAMT.
8. No menu **Arquivo**, clique em **Abrir** para exibir a caixa de diálogo **Abrir Lista de Informações do Computador**.
9. Localize e selecione IsolatedLabGroup.CIL e clique em **Abrir** para carregar a CIL na VAMT.

Isso exibe computadores previamente descobertos e os estados das licenças no painel de exibição em lista do computador.

1. No menu **Arquivo**, clique em **Importar** e navegue até o arquivo que contém os CIDs (IsolatedLabGroupSecureExportwithCID.CIL).

Isso inicia o processo de mesclagem que vincula os CIDs aos IIDs dos computadores.

1. No menu **Arquivo**, clique em **Salvar** e digite o nome de um arquivo, como *IsolatedLabGroupwithCID.CIL*, para salvar esse arquivo que associa os IIDs aos CIDs correspondentes.

**Importante**   Salvar esse arquivo é essencial para a recriação de cenários. É altamente recomendável que você faça o backup desse arquivo e o proteja contra substituição.

1. Aplique os CIDs e ative os computadores de Laboratório Isolado:
2. Clique com o botão direito do mouse no grupo Laboratório Isolado no painel de exibição em árvore e clique em **Ativar Proxy MAK** para abrir a caixa de diálogo **Ativar Proxy MAK**.
3. Desmarque a caixa de seleção **Instalar MAK (substituir existente)**, pois os computadores selecionados já possuem uma MAK instalada.
4. Desmarque a caixa de seleção **Obter ID de Confirmação da Microsoft**.
5. Marque a caixa de seleção **Aplicar ID de Confirmação e Ativar** para instruir a VAMT a ativar os computadores selecionados a instalarem seus CIDs.
6. Clique em **OK**.

A VAMT exibe a caixa de diálogo **Atribuir IDs de Confirmação** enquanto instala os CIDs em todos os computadores selecionados.

1. Opcionalmente, reative os computadores com nova imagem feita no Laboratório Isolado:

Se os computadores no Laboratório Isolado tiverem uma nova imagem feita, mas o hardware subjacente não tiver mudado, a VAMT poderá reativá-los usando o arquivo IsolatedLabGroupwithCID.CIL.

1. Reimplante o Windows em cada computador utilizando os mesmos nomes de computador de antes.
2. Abra o console VAMT no host VAMT local (grupo de trabalho).
3. No menu **Arquivo**, clique em **Abrir** e selecione o arquivo IsolatedLabGroupwithCID.CIL.
4. No painel de exibição em árvore, clique com o botão direito do mouse no grupo **Laboratório Isolado**, clique em **Reaplicar ID de Confirmação** para exibir a caixa de diálogo **Reativar Proxy MAK**.
5. Deixe a caixa de seleção **Instalar MAK (substituir existente)** selecionada e verifique se a MAK previamente utilizada está selecionada na lista.
6. Deixe a caixa de seleção **Reaplicar ID de Confirmação e Reativar** selecionada para reaplicar os CIDs armazenados do arquivo IsolatedLabGroupwithCID.CIL.
7. Deixe a caixa de seleção **Solicitar correspondência exata do IID** selecionada se o hardware não tiver sido alterado desde a Ativação Proxy MAK e se você estiver usando a mesma MAK para reativar o computador.

Desmarque a caixa de seleção se o hardware tiver sido alterado, mas você ainda pode fazer com que a VAMT tente uma reativação utilizando o CID previamente armazenado. Observe que o Windows pode não ter sido reativado com êxito nesse cenário.

1. Se estiver ativando um computador que exija credenciais de administrador diferentes das que você já utiliza, marque a caixa de seleção **Utilizar Credenciais Alternativas**.
2. Clique em **OK**.

A VAMT exibe a caixa de diálogo **Atribuir Chaves de Produto** enquanto aplica a MAK ao grupo de Laboratório Isolado.

A VAMT exibe a caixa de diálogo **Atribuir IDs de Confirmação** enquanto instala os CIDs em todos os computadores selecionados.

**Observação**Marcar a caixa de seleção **Instalar MAK (substituir existente)** força a instalação de uma MAK. Isso deve ser feito com cuidado. Se a versão pré-SP1 do Windows Vista estiver instalada no computador por mais de 30 dias, seu período de cortesia inicial terá expirado, e o computador entrará no RFM se a ativação não for concluída com êxito antes do logon seguinte. A VAMT pode ser utilizada para recuperar corretamente os computadores remotos configurados do RFM, contanto que estejam acessíveis na rede. O RFM apenas se aplica à versão pré-SP1 do Windows Vista. Windows Vista SP1 ou mais recente, Windows 7, Windows Server 2008 e Windows Server 2008 R2 não entrarão no RFM.

### Suporte VAMT para ativação KMS

Neste cenário, a VAMT é utilizada para instalar e ativar as chaves do cliente KMS ou em computadores do Laboratório Isolado ou da Rede Principal. O procedimento descrito abaixo parte do princípio de que a VAMT foi instalada e os computadores foram adicionados à CIL. Essas tarefas são descritas nas etapas 1-4 no Cenário 1 (para a Rede Principal) ou no Cenário 2 (para o grupo de trabalho de Laboratório Isolado).

1. Abra o console VAMT.
2. Selecione os computadores a serem ativados, clicando em um grupo no painel de exibição em árvore ou selecionando computadores individuais no painel de exibição em lista.
3. Clique com o botão direito do mouse no grupo selecionado ou nos computadores e clique em **Configurar para Ativação KMS** para exibir a caixa de diálogo **Configuração KMS**.
4. Selecione **Instalar Chave de Cliente KMS (substituir existente)** para instruir a VAMT a instalar a chave do cliente KMS em um computador cliente.
5. Selecione a opção de ativação apropriada:

* **Descoberta automática do host KMS utilizando DNS.** A VAMT primeiramente limpa qualquer host KMS previamente configurado no computador de destino e instrui o computador a consultar o DNS para localizar o host KMS e tentar a ativação.
* **Utilizar host e porta KMS específico.** A VAMT define o nome e a porta do host KMS específico no computador de destino e instrui o computador a tentar a ativação com esse host KMS específico.

1. Se estiver ativando computadores que exijam credenciais de administrador diferentes das que você já utiliza, marque a caixa de seleção **Utilizar Credenciais Alternativas** e clique em **OK**.

A VAMT exibe a caixa de diálogo **Atribuir Chaves de Produto** e exibe a caixa de diálogo **Ativar Computadores** até que a ação solicitada seja concluída. Se tiver marcado a caixa de seleção **Utilizar Credenciais Alternativas**, você precisará digitar as credenciais antes dessas caixas de diálogo.

### Convertendo 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

Você pode 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>.

**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

É possível configurar uma edição de volume do Windows 7 ou Windows Server 2008 R2 para usar ativação por MAK usando o item Sistema no 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>

em que ChaveDeAtivaçãoMúltipla é a MAK.

Se os usuários instalarem uma MAK usando a interface de usuário (UI), o cliente MAK tentará se ativar pela Internet uma vez. Se os usuários instalarem uma chave MAK usando o script Slmgr.vbs, o cliente MAK não tentará se ativar automaticamente. O usuário pode utilizar o **Slmgr.vbs /ato** para ativar a MAK manualmente pela Internet.

# Chaves do host do KMS para produtos

A Tabela 7 descreve os produtos que cada host do KMS pode ativar.

Tabela 7. Chaves do host do KMS correspondentes aos produtos que podem ativar

| **Grupo de produtos de volume** | **Produtos Windows** | **Tipo de chave** | **Produtos ativados por tipo de chave** |
| --- | --- | --- | --- |
| 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 baseados no 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 |
| As chaves KMS do Windows Server 2008 R2 seguem a mesma hierarquia (grupos A, B e C) do Windows Server 2008 com a adição do Windows Server 2008 Datacenter sem Hyper-V™, Windows Server 2008 Enterprise sem Hyper-V e Windows Server 2008 Standard sem Hyper-V. A diferença principal é observar se as chaves KMS do Windows Server 2008 R2 podem ser utilizadas para ativar um host KMS que irá, por sua vez, ativar o Windows Server 2008, Windows 7 e Windows Vista.  As chaves do Windows Server 2008 e o Windows Vista não podem ativar os sistemas Windows 7 ou Windows Server 2008 R2. | | | |

# Valores da diretiva de ativação

A Tabela 8 lista os valores de diretiva para o Windows 7 e para o Windows Server 2008 R2.

Tabela 8. Valores de diretiva do Windows 7 e do Windows Server 2008 R2

| **Elemento** | **Valor do cliente** | **Valor do servidor** | **Intervalo** |
| --- | --- | --- | --- |
| Limite de rearmação | 3 | 3 | Não configurável |
| Limite de contagem do cliente KMS | 25 | 5 | Não configurável |
| Duração de ativação KMS | 180 dias | 180 dias | Não configurável |
| Porta de escuta do host KMS | 1688 | 1688 | Qualquer porta TCP aberta |
| Cortesia OOB | 30 dias | 30 dias | Não configurável |
| Cortesia OOT | 30 dias | 30 dias | Não configurável |
| Reativação do cliente KMS (em minutos) | 10.080 minutos  (7 dias – padrão) | 10.080 minutos  (7 dias – padrão) | 15-43.200 minutos  (30 dias – padrão) |
| Intervalo de nova tentativa silenciosa KMS – ocorre na falha de ativação do KMS | 120 minutos | 120 minutos | 15-43.200 minutos  (120 minutos – padrão) |

# Chaves de instalação do Cliente KMS

Por padrão, os sistemas operacionais Windows 7 e Windows Server 2008 R2 usam o KMS para ativação. Nas instalações de volume, a chave de configuração é instalada por padrão, o que torna o sistema um cliente KMS. Se você estiver convertendo um computador de um host KMS, MAK ou uma edição comercial do Windows para um cliente KMS, instale a chave de configuração aplicável (GVLK) da Tabela 9 usando **slmgr /ipk <setup key>**.

Tabela 9. Chaves de instalação do cliente KMS

| **Plataforma** | **Edição do sistema operacional** | **Chave do produto** | | | |
| --- | --- | --- | --- | --- | --- |
| **Windows 7 e 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 para sistemas baseados no Itanium | | | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| **Windows Vista e 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 sem Hyper-V | | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ | |
| Servidor | Windows Server 2008 Enterprise | | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V | |
| Servidor | Windows Server 2008 Enterprise sem Hyper-V | | 39BXF-X8Q23-P2WWT-38T2F-G3FPG | |
| Servidor | Windows Server 2008 Datacenter | | 7M67G-PC374-GR742-YH8V4-TCBY3 | |
| Servidor | Windows Server 2008 Datacenter sem Hyper-V | | 22XQ2-VRXRG-P8D42-K34TD-G3QQC | |
| Servidor | Windows Server 2008 para sistemas baseados no Itanium | | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK | |

# Códigos de erro de ativação

A Tabela 10 fornece ajuda para a solução de problemas que podem ocorrer ao se ativar edições de volume dos sistemas operacionais Windows 7 e Windows Server 2008 R2.

Tabela 10. Códigos e descrições de erro

| **Código de erro** | **Mensagem de erro** | **Tipo de ativação** | **Causa possível** | **Etapas da solução de problemas** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | O servidor de ativação determinou que a chave de produto especificada é inválida | MAK | Uma MAK inválida foi digitada. | Verifique se a chave é a MAK fornecida pela Microsoft.  Contate a [Central de Atendimento de Ativação Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) para verificar se a MAK é válida. |
| 0xC004C003 | O servidor de ativação determinou que a chave de produto especificada está bloqueada | MAK | A MAK está bloqueada no servidor de ativação. | Contate a [Central de Atendimento de Ativação Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) para obter uma nova MAK e instalar/ativar o sistema. |
| 0xC004C008 | O servidor de ativação determinou que a chave de produto especificada não pôde ser usada | KMS | A chave KMS excedeu o limite de ativações. | As chaves do host KMS ativam até 10 vezes em 6 computadores diferentes. Se mais ativações forem necessárias, contate a [Central de Atendimento de Ativação Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C020 | O servidor de ativação relatou que a Chave de Ativação Múltipla excedeu seu limite. | MAK | A MAK excedeu o limite de ativações. | Por padrão, as MAKs têm um número limitado de ativações. Contate a [Central de Atendimento de Ativação Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C021 | O servidor de ativação relatou que a extensão da Chave de Ativação Múltipla foi excedida. | MAK | A MAK excedeu o limite de ativações. | Por padrão, as MAKs têm um número limitado de ativações. Contate a [Central de Atendimento de Ativação Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004F009 | O Serviço de Proteção de Software relatou que o período de cortesia expirou. | MAK | O período de cortesia expirou antes de o sistema ser ativado. Agora, o sistema está no estado de Notificações. | Consulte a seção “User Experience.” |
| 0xC004F00F | O servidor de licenciamento de software relatou que a vinculação da ID do hardware está além do nível de tolerância. | Cliente MAK/KMS/host KMS | O hardware foi alterado ou os drivers foram atualizados no sistema. | **MAK:** Reative o sistema durante o período de cortesia OOT usando a ativação online ou por telefone.  **KMS:** Reinicie ou execute **slmgr.vbs /ato**. |
| 0xC004F014 | O Serviço de Proteção de Software relatou que a chave de produto não está disponível. | Cliente MAK/KMS | Nenhuma chave de produto está instalada no sistema. | Instale uma chave de produto MAK ou a chave de instalação KMS encontrada em \sources\pid.txt na mídia de instalação. |
| 0xC004F02C | O serviço de Proteção de Software relatou que o formato dos dados de ativação offline está incorreto. | Cliente MAK/KMS | O sistema detectou que os dados inseridos durante a ativação por telefone não são válidos. | Verifique se o CID foi digitado corretamente. |
| 0xC004F035 | Esse código de erro equivale a “O serviço de Proteção de Software relatou que o computador não pôde ser ativado com uma chave de produto de licença para volume…”. O texto desse erro está correto, mas é ambíguo.  Esse erro indica que está faltando um marcador no BIOS do Windows - fornecido nos sistemas OEM para indicar os computadores entregues com edições qualificadas do Windows, o que é um requisito para a ativação do cliente KMS.  Erro: Chave de Licença de Volume inválida  Para realizar a ativação, é preciso alterar a chave de produto para uma MAK (Chave de Ativação Múltipla) ou para uma chave comercial válida.  É necessário possuir uma licença de sistema operacional qualificada E uma licença de atualização para o Windows 7 com licença por volume, ou uma licença completa para o Windows 7 de uma fonte comercial.  QUALQUER OUTRA INSTALAÇÃO DESTE SOFTWARE É UMA VIOLAÇÃO DO CONTRATO E DA LEI DE DIREITOS AUTORAIS APLICÁVEIS. | Cliente/ host KMS | As edições de volume do Windows 7 são licenciadas somente para atualização. A instalação de um sistema operacional de volume em um computador que não tenha um sistema operacional qualificado instalado não é permitida. | Instale uma versão qualificada de um sistema operacional da Microsoft e o ative com uso da MAK. |
| 0xC004F038 | O Serviço de Proteção de Software relatou que o computador não pôde ser ativado. A contagem reportada pelo KMS (Serviço de Gerenciamento de Chaves) é insuficiente. Contate o administrador do sistema. | Cliente KMS | A contagem no host KMS não é alta o suficiente. A contagem do KMS deve ser ≥5 para Windows Server ou ≥25 para cliente Windows. | Mais computadores são necessários no pool KMS para ativar clientes KMS. Execute **Slmgr.vbs /dli** para obter a contagem atual no host KMS. |
| 0xC004F039 | O Serviço de Proteção de Software relatou que o computador não pôde ser ativado. O KMS (Serviço de Gerenciamento de Chaves) não está ativado. | Cliente KMS | Esse erro ocorre quando uma solicitação do KMS não é respondida. | Solucione os problemas de conexão de rede entre o host KMS e o cliente. Verifique se a porta TCP1688 (padrão) não está bloqueada por firewall ou se não está sendo filtrada. |
| 0xC004F041 | O Serviço de Proteção de Software determinou que o KMS não está ativado. O KMS precisa ser ativado. | Cliente KMS | O host KMS não está ativado. | Ative o host KMS por ativação online ou por telefone. |
| 0xC004F042 | O Serviço de Proteção de Software determinou que o KMS especificado não pode ser usado. | Cliente KMS | Divergência entre o cliente KMS e o host KMS. | Esse erro ocorre quando um cliente KMS contata um host KMS que não pode ativar o software cliente. Isso pode ser comum em ambientes mistos que contenham aplicativos e sistemas operacionais específicos para hosts KMS, por exemplo. |
| 0xC004F050 | O Serviço de Proteção de Software relatou que a chave de produto é inválida. | KMS, cliente KMS, MAK | Isso pode ser causado por erro de digitação na chave KMS ou por digitação de uma chave Beta em uma versão liberada do sistema operacional. | Instale a chave KMS correta na versão correspondente do Windows. Verifique a digitação. Se a chave estiver sendo copiada e colada, certifique-se de que os travessões não tenha sido substituídos por traços na chave. |
| 0xC004F051 | O Serviço de Proteção de Software relatou que a chave de produto está bloqueada. | MAK/KMS | A chave de produto no servidor de ativação foi bloqueada pela Microsoft. | Obtenha uma nova chave MAK/KMS, instale-a no sistema e ative. |
| 0xC004F064 | O Serviço de Proteção de Software relatou que o período de cortesia não original expirou. | MAK | O WAT (Windows Activation Tools) determinou que o sistema não é original. | Consulte o Guia de Operações do Volume Activation. |
| 0xC004F065 | O Serviço de Proteção de Software relatou que o aplicativo está sendo executado durante o período não original válido. | Cliente MAK/KMS | O WAT (Windows Activation Tools) determinou que o sistema não é original. O sistema continuará a ser executado durante o período de cortesia não original. | Obtenha e instale uma chave de produto original e ative o sistema durante o período de cortesia. Por outro lado, o sistema entrará no estado Notificações no final do período de cortesia. |
| 0xC004F06C | O Serviço de Proteção de Software relatou que o computador não pôde ser ativado. O KMS (Serviço de Gerenciamento de Chaves) determinou que o carimbo de data/hora da solicitação é inválido. | Cliente KMS | A hora do sistema no computador cliente é muito diferente daquela no host KMS. | A sincronização da hora é importante para a segurança do sistema e da rede por vários motivos. Corrija o problema alterando a hora do sistema no cliente para sincronizar com o KMS. A utilização de uma fonte de tempo do Protocolo NTP ou do Active Directory Domain Services para a sincronização de tempo é recomendada. Esse problema usa a hora UTP e é independente da seleção de fuso horário. |
| 0x80070005 | Acesso negado. A ação solicitada requer privilégios elevados. | Cliente KMS/host MAK/KMS | O UAC (Controle de Conta do Usuário) proíbe que os processos de ativação sejam executados em um prompt de comando não elevado. | Execute slmgr.vbs em um prompt de comando elevado. Clique com o botão direito do mouse em cmd.exe e clique em Executar como Administrador. |
| 0x8007232A | Falha do servidor DNS. | Host KMS | O sistema tem problemas de rede ou DNS. | Solucione problemas de rede e DNS. |
| 0x8007232B | O nome DNS não existe. | Cliente KMS | O cliente KMS não conseguiu encontrar os RRs SRV do KMS no DNS.  Se um host KMS não existir em uma rede, a MAK deverá estar instalada. | Confirme se o host KMS está instalado e a publicação DNS está habilitada (padrão).  Se o DNS estiver indisponível, aponte o cliente KMS para o host KMS utilizando **slmgr.vbs /skms <*kms\_host\_name>***.  Opcionalmente, obtenha e instale a MAK; em seguida, ative o sistema.  Finalmente, solucione o problema do DNS. |
| 0x800706BA | O servidor RPC está indisponível. | Cliente KMS | As configurações do firewall não estão definidas no host KMS ou os registros SRV do DNS estão obsoletos. | Verifique se a exceção do firewall do Serviço de Gerenciamento de Chaves está habilitada na máquina host KMS.  Verifique se os registros SRV apontam para um host KMS válido.  Solucione os problemas de conexão da rede. |
| 0x8007251D | Nenhum registro encontrado para a consulta do DNS. | Cliente KMS | O cliente KMS não conseguiu encontrar os RRs SRV do KMS no DNS. | Solucione problemas de conexão de rede e DNS. |
| 0xC004F074 | O Serviço de Proteção de Software relatou que o computador não pôde ser ativado. Nenhum KMS (Serviço de Gerenciamento de Chaves) pôde ser contatado. Verifique o Log de Eventos de Aplicativos para mais informações. | Cliente KMS | Todos os sistemas host KMS retornaram um erro. | Solucione erros de cada ID de evento 12288 associado à tentativa de ativação. |

# Log de eventos do Windows

A Tabela 11 lista os eventos que o KMS registra no log de eventos do Windows. Descrição de dados comuns para cada evento:

**Nome do arquivo de log para todos, exceto 12290:** Windows Logs\Application

**Nome do arquivo de log 12290:** Serviço de gerenciamento de logs de Aplicativos e Serviços\Chave

**Nome do provedor do evento:** Microsoft-Windows-Security-Licensing-SLC

**Nome de origem:** Serviço de Proteção de Software

Tabela 11. Eventos KMS registrados no log de eventos do Windows

| **Event ID** | **Regis trado por** | **Descrição** | **Mensagem** | **Parâmetros**  **Campos inclusos em cadeia delimitada por vírgulas** | | **Exemplos** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Nome** | **Descrição** |  |
| 12288 | Cliente | Falha ao gerar a solicitação ou após o envio da RPC (cliente) | O cliente enviou uma solicitação de ativação ao computador ao KMS.%nInfo:%n%1 | HRESULT | Código de retorno | 0x0 |
|  | | | | Status | Sinalizadores (nota 1) | 0x8 |
| Server: Port | Name:port | kms01.contoso.com:1688 |
| CMID | Identificação da máquina cliente | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be, |
| Hora do cliente | Carimbo de data/hora da solicitação | 2006/1/14 2:30, |
| Informa ção de VM | Não usado | 1 |
| Status do licencia mento | Status da licença  0 – Não licenciado  1 - Licenciado (Ativado)  2 - Cortesia OOB  3 - Cortesia OOT  4 - Cortesia não original  5 - Notificações  6 - Cortesia estendida | 2 |
|  | | | | Prazo de vencimen to | Tempo restante (minutos) | 40123 |
| ActID | ID de ativação – identifica a licença | cf67834d-db4a-402c-ab1f-2c134f02b700, |
| N-Policy | O cliente com contagem mínima precisa ser ativado | 25 |
| 12289 | Cliente | Após a validação da resposta do KMS (cliente) | O cliente processou uma resposta de ativação do computador do serviço de gerenciamento de chaves.%nInfo:%n%1 | HRESULT | Código de retorno | 0x0 |
|  | | | | Status | Sinalizadores (nota 1) | 0x4000008 |
| fBound | Sinalizador ativado | 0 |
| Não usado | Não usado - ignorar | 0 |
| Contagem | Contagem atual do KMS | 4 |
| Intervalo de ativação | Intervalo de solicitação quando não ativado (minutos) | 120 |
| Intervalo de renovação | Intervalo de solicitação quando ativado (minutos) | 10080 |
| Hora do cliente | Carimbo de data/hora da solicitação | 1/14/2006 2:30 |
| 12290 | KMS | Log do servidor KMS de cada solicitação | Uma solicitação de ativação foi processada.%nInfo:%n%1 | HRESULT | Código de retorno | 0x0 |
|  | | | | N-Policy | A contagem mínima de produtos do cliente precisava ser ativada | 25 |
| Máquina | Nome do computador cliente | kms03.site5.contoso.com |
| CMID | Identificação da máquina cliente | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | Hora do cliente | Carimbo de data/hora da solicitação | 2006/1/14 22:36 |
| Informação de VM | O sistema operacional do cliente está sendo executado em uma máquina virtual | 1 |
| Status do licenciamento | Status da licença  0 – Não licenciado  1 - Licenciado (Ativado)  2 - Cortesia OOB  3 - Cortesia OOT  4 - Cortesia não original  5 - Notificações  6 - Cortesia estendida | 2 |
| Prazo de vencimento | Tempo restante (minutos) | 40123 |
| ActID | ID de ativação – identifica a licença | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | Falha de inicialização do KMS | O cliente licenciado por volume não pode inicializar o timer de renovação do Serviço de Gerenciamento de Chaves.%nInfo:%n%1 | HRESULT | Código de retorno |  |
| 12292 | KMS | Falha na inicialização do timer de renovação | Falha do Serviço de Gerenciamento de Chaves (KMS) ao inicializar o timer de renovação. %nInfo:%n%1 | HRESULT | Código de retorno |  |
| 12293 | KMS | Falha na publicação do DNS-RR | Falha ao publicar o Serviço de Gerenciamento de Chaves (KMS) no DNS no domínio '%2'.%nInfo:%n%1 | P1: HRESULT  P2: Domínio DNS | P1: Código de retorno  P2: Nome do domínio DNS | |
| 12294 | KMS | Êxito na publicação do RR do DNS | Êxito na publicação do Serviço de Gerenciamento de Chaves (KMS) no DNS no domínio '%1'.%n | Domínio DNS | Nome do domínio DNS |  |

# Propriedades e métodos WMI

A Tabela 12 lista as propriedades e os métodos WMI para a Plataforma de Proteção de Software. As propriedades da Plataforma de Proteção de Software estão definidas no arquivo %WinDir%\System32\wbem\sppwmi.mof.

Tabela 12. Propriedades e métodos WMI da plataforma de proteção de software

|  |  |
| --- | --- |
| **//properties SoftwareLicensingService Class** | |
| **Versão** | Versão do Serviço de Proteção de Software. |
| **KeyManagementServiceMachine** | O nome do host KMS. Retornará nulo se **SetKeyManagementServiceMachine** não tiver sido chamado. |
| **KeyManagementServicePort** | A porta TCP utilizada por clientes para enviar solicitações de ativação KMS. Retornará **0** se **SetKeyManagementServicePort** não tiver sido chamado. |
| **IsKeyManagementServiceMachine** | Indica se o KMS está habilitado no computador: **0** se for falso, **1** se for verdadeiro. |
| **VLActivationInterval** | A frequência, em minutos, de quantas vezes um cliente irá contatar o host KMS antes de um cliente ser licenciado. |
| **VLRenewalInterval** | A frequência, em minutos, de quantas vezes um cliente irá contatar o host KMS depois de um cliente ser licenciado. |
| **KeyManagementServiceCurrentCount** | A contagem dos clientes KMS atualmente ativos no host KMS. **-1** indica se um host não está habilitado como KMS ou não recebeu nenhuma solicitação de licença do cliente. |
| **RequiredClientCount** | O número mínimo de clientes necessários para conexão com um host KMS para habilitar o Licenciamento por Volume. |
| **PolicyCacheRefreshRequired** | Indica se o cache da diretiva de licenciamento precisa ser atualizado: **0**=não solicitado, **1**=Atualização solicitada. |
| **ClientMachineID** | O identificador global exclusivo (GUID) identifica um cliente KMS para um host KMS. O cliente inclui isso nas solicitações que envia ao KMS. |
| **RemainingWindowsReArmCount** | Número restante de vezes que o cliente pode ser rearmado com êxito. |
| **KeyManagementServiceListeningPort** | A porta TCP que o host KMS utiliza para escutar solicitações de ativação. |
| **KeyManagementServiceDnsPublishing** | Indica o status de publicação DNS de um host KMS: **0**=Desativado, **1**=Publicação automática habilitada (padrão). |
| **KeyManagementServiceLowPriority** | Indica o status de prioridade de thread do serviço KMS: **0**=Prioridade normal (padrão), **1**=Baixa prioridade. |
| **KeyManagementServiceHostCaching** | Indica o status do cache do nome e da porta do host KMS: **0**=Cache desabilitado, **1**=Cache habilitado (padrão). |
| **KeyManagementServiceUnlicensedRequests** | Contagem de solicitações KMS dos clientes com Status de licença=0 (Não licenciado). |
| **KeyManagementServiceLicensedRequests** | Contagem de solicitações KMS dos clientes com Status de licença=1 (Licenciado). |
| **KeyManagementServiceOOBGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=2 (OOBGrace). |
| **KeyManagementServiceOOTGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=3 (OOTGrace). |
| **KeyManagementServiceNonGenuineGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=4 (Cortesia não original). |
| **KeyManagementServiceNotificationRequests** | Contagem de solicitações KMS dos clientes com Status de licença=5 (Notificação). |
| **KeyManagementServiceTotalRequests** | Contagem total de solicitações válidas do KMS. |
| **KeyManagementServiceFailedRequests** | Contagem de solicitações inválidas do KMS. |
| **KeyManagementServiceActivationDisabled** | Indica se a ativação de volume pelo KMS está desabilitada. |
| **//methods SoftwareLicensingProduct Class** | |
| **InstallProductKey** | Instala uma chave de produto. |
| **InstallLicense** | Instala uma licença. |
| **InstallLicensePackage** | Instala um pacote de licenças para o produto atual. |
| **SetKeyManagementServiceMachine** | Define um nome de host do KMS a ser utilizado para ativação de volume. |
| **ClearKeyManagementServiceMachine** | Apaga qualquer nome de host KMS previamente configurado. |
| **SetKeyManagementServicePort** | Define a porta TCP utilizada por um cliente para fazer solicitações do host KMS. Se não for especificada, a porta 1688 será utilizada. |
| **ClearKeyManagementServicePort** | Apaga qualquer número de porta previamente especificada. |
| **SetVLActivationInterval** | A frequência de ativação, em minutos, de quantas vezes os clientes KMS entrarão em contato com o host KMS antes de se tornarem licenciados. A frequência deve ser de ≥15 e ≤43.200. Um erro será retornado se o método for chamado e o computador não for um KMS. |
| **SetVLRenewalInterval** | A frequência de renovação, em minutos, de quantas vezes os clientes KMS entrarão em contato com o host KMS depois de se tornarem licenciados. A frequência deve ser de ≥15 e ≤43.200. Um erro será retornado se o método for chamado e o computador não for um KMS. |
| **ClearProductKeyFromRegistry** | Remove a chave de produto do registro. |
| **AcquireGenuineTicket** | Executa uma validação original online. Chamar esse método pode alterar o status Original do computador. |
| **ReArmWindows** | Redefine o status de licença do computador como Cortesia OOB (consulte **LicenseStatus**).  **Observação**   Você deve reiniciar o cliente para que as alterações façam efeito. |
| **RefreshLicenseStatus** | Atualiza o status de licenciamento do Windows para que os aplicativos tenham acesso às informações atuais sobre licenciamento. |
| **SetKeyManagementServiceListeningPort** | Define a porta TCP utilizada pelo host KMS para escutar as solicitações de ativação. Aplica-se apenas aos hosts KMS. Se não for especificada, a porta 1688 será utilizada. |
| **ClearKeyManagementServiceListeningPort** | Apaga qualquer porta de escuta previamente especificada. Aplica-se apenas aos hosts KMS. |
| **DisableKeyManagementServiceDnsPublishing** | Habilita/desabilita a Publicação DNS em um computador host KMS: **0**=Habilitar, **1**=Desabilitar. |
| **EnableKeyManagementServiceLowPriority** | Habilita/desabilita o serviço KMS executado com baixa prioridade: **0**=Desabilitar, **1**=Habilitar. |
| **DisableKeyManagementServiceHostCaching** | Habilita/desabilita o cache do nome e da porta do host KMS em um computador cliente com ativação de volume: **0**=Habilitar, **1**=Desabilitar. |
| **DisableKeyManagementServiceActivation** | Habilita/desabilita a ativação de volume por meio de uma máquina KMS: **0**=Habilitar, **1**=Desabilitar. |
| **DiscoveredKeyManagementServiceMachineName** | Última descoberta do nome do host KMS através do DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Última descoberta da porta do host KMS através do DNS. |
| **//properties SoftwareLicensingService Class** | |
| **ID** | Identificador do produto |
| **Nome** | Nome do produto |
| **Descrição** | Descrição do produto |
| **ApplicationID** | Identificação do aplicativo atual do produto |
| **ProcessorURL** | URL do servidor de licenciamento de software do certificado de processo |
| **MachineURL** | URL do servidor de licenciamento de software do certificado de associação |
| **ProductKeyURL** | URL do servidor de licenciamento de software do certificado do produto |
| **UseLicenseURL** | URL do servidor de licenciamento de software da licença do usuário |
| **LicenseStatus** | Status da licença do aplicativo do produto:  **0**=Não licenciado, **1**=Licenciado, **2**=OOBGrace, **3**=OOTGrace, **4**=Cortesia não original, **5**=Notificação, **6**=Cortesia estendida |
| **LicenseStatusReason** | Um código de diagnóstico que indica porque um computador está em um estado de licença específico. |
| **GracePeriodRemaining** | Tempo restante em minutos para que o aplicativo pai entre no modo de Notificação. Para os clientes de volume, esse é o tempo restante para que a reativação seja solicitada. |
| **EvaluationEndDate** | Data de vencimento do aplicativo desse produto. Após essa data, o **LicenseStatus** ficará **Não licenciado** e não poderá ser ativado. |
| **OfflineInstallationId** | Um identificador para o aplicativo do produto que pode ser utilizado para ativação offline ou por telefone. Retornará nulo se a chave de produto não estiver instalada. |
| **PartialProductKey** | Últimos cinco caracteres da chave desse produto. Retornará nulo se a chave de produto não estiver instalada. |
| **ProductKeyID** | ID da chave de produto. Retornará nulo se a chave de produto não estiver instalada. |
| **LicenseFamily** | Identificador de família de SKUs usadas para determinar relacionamentos de licença dos complementos. |
| **LicenseDependsOn** | Identificador de dependência da família de SKUs usadas para determinar relacionamentos de licença dos complementos. |
| **LicenseIsAddon** | Retornará **Verdadeiro** se o produto estiver identificado como licença de complemento. |
| **VLActivationInterval** | A frequência, em minutos, de quantas vezes um cliente entrará em contato com o host KMS antes de um produto ser licenciado. |
| **VLRenewalInterval** | A frequência, em minutos, de quantas vezes um cliente entrará em contato com o host KMS depois de um produto ser licenciado. |
| **KeyManagementServiceProductKeyID** | ID da chave de produto KMS. Retornará nulo se não aplicável. |
| **KeyManagementServiceMachine** | O nome do host KMS. Retornará nulo se **SetKeyManagementServiceMachine** não tiver sido chamado. |
| **KeyManagementServicePort** | A porta TCP utilizada por clientes para enviar solicitações de ativação KMS. Retornará **0** se **SetKeyManagementServicePort** não tiver sido chamado. |
| **DiscoveredKeyManagementServiceMachineName** | Última descoberta do nome do host KMS através do DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Última descoberta da porta do host KMS através do DNS. |
| **IsKeyManagementServiceMachine** | Indica se o KMS está ativado no computador: **1** se for verdadeiro, **0** se for falso. |
| **KeyManagementServiceCurrentCount** | A contagem dos clientes KMS atualmente ativos no host KMS. **-1** indica se um computador não está ativado como KMS ou não recebeu nenhuma solicitação de licença do cliente. |
| **RequiredClientCount** | O número mínimo de clientes necessários para conexão com um host KMS para habilitar o Licenciamento por Volume. |
| **KeyManagementServiceUnlicensedRequests** | Contagem de solicitações KMS dos clientes com Status de licença=0 (Não licenciado). |
| **KeyManagementServiceLicensedRequests** | Contagem de solicitações KMS dos clientes com Status de licença=1 (Licenciado). |
| **KeyManagementServiceOOBGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=2 (OOBGrace). |
| **KeyManagementServiceOOTGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=3 (OOTGrace). |
| **KeyManagementServiceNonGenuineGraceRequests** | Contagem de solicitações KMS dos clientes com Status de licença=4 (Cortesia não original). |
| **KeyManagementServiceTotalRequests** | Contagem total de solicitações válidas do KMS. |
| **KeyManagementServiceFailedRequests** | Contagem de solicitações com falha do KMS. |
| **KeyManagementServiceNotificationRequests** | Contagem de solicitações KMS dos clientes com Status de licença=5 (Notificação). |
| **GenuineStatus** | Status original para o aplicativo desse produto. |
| **ExtendedGrace** | Tempo de cortesia estendido em minutos para que o aplicativo pai se torne não licenciado. |
| **TrustedTime** | Exibe a hora atual confiável armazenada no sistema. |
| **DisableKeyManagementServiceHostCaching** | Habilita/desabilita o cache do nome e da porta do host KMS em um computador cliente com ativação de volume: 0=Habilitar, 1=Desabilitar. |
| **//methods SoftwareLicensingProduct Class** | |
| **UninstallProductKey** | Desinstala uma chave de produto para o produto atual. |
| **Activate** | Ativa o produto atual. |
| **DepositOfflineConfirmationId** | Ativa um produto depositando um Identificador de Confirmação Offline desse produto durante a ativação offline ou por telefone. |
| **GetPolicyInformationDWord** | Obtém informações de diretiva de licença do tipo DWORD. |
| **GetPolicyInformationString** | Obtém informações de diretiva de licença do tipo string. |
| **SetKeyManagementServiceMachine** | Define um nome de host do KMS a ser utilizado para ativação de volume. |
| **ClearKeyManagementServiceMachine** | Apaga qualquer nome de host KMS previamente configurado. |
| **SetKeyManagementServicePort** | Define a porta TCP utilizada por um cliente para fazer solicitações do host KMS. Se não for especificada, a porta 1688 será utilizada. |
| **ClearKeyManagementServicePort** | Apaga qualquer número de porta previamente especificada. |

# Glossário

|  |  |
| --- | --- |
| **Termo** | **Definição** |
| **ACID** | GUID usado para identificar um método de ativação dentro de uma edição de software. |
| **AD DS** | Active Directory Domain Services. |
| **AppID** | Um GUID definido para agrupar uma coleção de IDs SKU como um nome de família. Todas as edições do Windows possuem o mesmo AppID. |
| **DNS** | Serviços de Nome de Domínio. |
| **FQDN** | Nome de domínio totalmente qualificado (por exemplo, phred.microsoft.com). |
| **GVLK** | Chave de Licença de Volume Genérica, uma chave de produto específica de edição instalada em todas as edições de volume do Windows por padrão. Também conhecida como chave de configuração padrão do cliente KMS. Para mais informações, consulte a Tabela 9. |
| **KMS** | Serviço de Gerenciamento de Chaves. |
| **KMSID** | Um GUID enviado pelo CLIENTE KMS para ativação com um host KMS. Pode ser compartilhado em diversos ACIDs. |
| **Armazenamento do Certificado da Máquina** | Esse certificado e sua chave privada devem estar acessíveis para a tentativa de ativação com base em token pelo usuário. |
| **MAK** | Chave de Ativação Múltipla. |
| **N-Policy** | Diretiva de licença que especifica a contagem mínima de máquinas retornada por um KMS que o cliente irá utilizar para determinar se realiza ativação automática. |
| **PIN** | Número de identificação pessoal, utilizado com um cartão inteligente como credencial de autenticação. |
| **SKU** | Descreve uma edição distinta do Windows ou outro software. |
| **SKUId** | Similar ao ACID acima |
| **SPPSVC** | Serviço de Proteção de Software, a plataforma de serviço desenvolvida no Windows 7 e no Windows Server 2008 R2 que gerencia as atividades de licença para o Windows e outros aplicativos. |
| **SRV** | Um tipo de registro de recurso suportado no DNS (consulte Request for Comments [RFC] 2782) |
| **Token** | Um certificado x509 com sua chave privada associada é usado para ativar o Windows em computadores habilitados para ativação com base em token. |
| **VL** | Licenciamento por Volume. |
| **WMI** | Instrumentação de Gerenciamento do Windows. |

# Links para recursos

* Volume Activation:
* Volume Activation no TechNet: <http://go.microsoft.com/fwlink/?LinkId=150083>
* KMS 1.2 para Windows Server 2003 SP1 e mais recentes: <http://go.microsoft.com/fwlink/?LinkId=155083>
* Ativação de produto e informações de chave: <http://go.microsoft.com/fwlink/?LinkId=74008>
* Guia de Implantação do Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=150083>
* Guia de Operações do Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=150084>
* Guia de Planejamento do Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=155926>
* Guia de Referência Técnica do Volume Activation: <http://go.microsoft.com/fwlink/?LinkId=152550>
* Ferramentas de implantação:
* Windows AIK (Kit de Instalação Automatizada do Windows) para Windows 7: <http://go.microsoft.com/fwlink/?LinkId=136976>
* Ferramentas de gerenciamento:
* Catálogo de pacotes do System Center: <http://go.microsoft.com/fwlink/?LinkID=110332>
* Licenciamento por volume:
* Software original Microsoft: <http://go.microsoft.com/fwlink/?LinkId=151993>
* Página de validação de software original Microsoft: <http://go.microsoft.com/fwlink/?LinkId=64187>
* Números de telefone dos centros de ativação Microsoft no mundo: <http://go.microsoft.com/fwlink/?LinkId=107418>
* Licenciamento por volume Microsoft: <http://go.microsoft.com/fwlink/?LinkId=73076>
* Centro de serviço de licenciamento por volume Microsoft: <http://go.microsoft.com/fwlink/?LinkId=107544>
* Destaques dos avisos de privacidade do Windows Vista: <http://go.microsoft.com/fwlink/?LinkID=52526>