## Fases

A atualização de software de terceiros prossegue em fases:

1. **Procurar atualizações necessárias**

   Para encontrar as atualizações de softwares de terceiros necessárias para os dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de Início Rápido do Servidor de Administração. Caso não tenha executado o assistente, crie a tarefa ou execute o Assistente de Início Rápido rápido agora.

   Instruções de como proceder:

   - Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias
   - Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de atualizações encontradas**

   Exiba a lista **Atualizações de software** e decida quais atualizações devem ser instaladas. Para visualizar informações detalhadas sobre cada atualização, clique no nome da atualização na lista. Para cada atualização na lista, você também pode visualizar as estatísticas sobre a instalação da atualização nos dispositivos cliente.

   Instruções de como proceder:

   Console de administração: Visualizando informações sobre atualizações disponíveis

   - Kaspersky Security Center Web Console: Visualizando informações sobre atualizações de software de terceiros disponíveis

3. **Configurar instalação de atualizações**

   Quando o Kaspersky Security Center receber a lista de atualizações de software de terceiros, será possível instalá-las em dispositivos clientes usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Crie uma dessas tarefas. Você pode criar essas tarefas na guia **Tarefas** ou usando a lista **Atualizações de software**.

   A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de produtos de outros fornecedores. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

   A tarefa *Instalar as atualizações do Windows Update* não requer uma licença, mas pode ser usada para instalar apenas atualizações do Windows Update.

   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software. Se você recusar o EULA, a atualização do software não será instalada.

   Você pode iniciar uma tarefa de instalação de atualizações. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

   Instruções de como proceder:

   - Console de administração: Corrigindo vulnerabilidades em aplicativos, exibindo informações sobre atualizações disponíveis

- Kaspersky Security Center Web Console: Criando a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, Criando a tarefa Instalar as atualizações do Windows Update, Visualizando informações sobre atualizações de software de terceiros disponíveis

### 4 Agendar as tarefas

Para garantir que a lista de atualizações esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempos em tempos. Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Instalar as atualizações do Windows Update*, observe que, para essa tarefa, é necessário definir a lista de atualizações todas as vezes antes de iniciá-la.

Ao agendar as tarefas, certifique-se de que uma tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

### 5 Aprovar e recusar atualizações de software (opcional)

Se você tiver criado a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, poderá especificar regras para instalação da atualização nas propriedades da tarefa. Se você criou a tarefa Instalar as atualizações do Windows Update, pule esta etapa.

Para cada regra, você pode definir as atualizações a serem instaladas, dependendo do status da atualização: *Indefinido*, *Aprovado* ou *Recusado*. Por exemplo, convém criar uma tarefa específica para servidores e definir uma regra para essa tarefa para permitir a instalação apenas de atualizações do Windows Update e somente aquelas com status *Aprovado*. Depois disso, você define manualmente o status *Aprovado* para as atualizações que deseja instalar. Nesse caso, as atualizações do Windows Update com status *Indefinido* ou *Recusado* não serão instaladas nos servidores especificados para a tarefa.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Recusado* na lista **Atualizações de software** (**Operações** → **Gerenciamento de patches** → **Atualizações de software**).

Instruções de como proceder:

- Console de Administração: Aprovação e recusa de atualizações de software
- Kaspersky Security Center Web Console: Aprovando e recusando atualizações de software de terceiros

### 6 Configurando o Servidor de Administração para funcionar como servidor WSUS (Serviços de atualização do Windows Server) (opcional)

Por padrão, as atualizações do Windows Update são baixadas para os dispositivos gerenciados diretamente dos servidores da Microsoft. Você pode alterar essa configuração para usar o Servidor de Administração como servidor WSUS. Nesse caso, o Servidor de Administração sincroniza os dados da atualização com o Windows Update na frequência especificada e fornece atualizações no modo centralizado para o Windows Update nos dispositivos em rede.

Para usar o Servidor de Administração como servidor WSUS, crie a tarefa de sincronização Executar o Windows Update e marque a caixa de seleção **Usar Servidor de Administração como servidor WSUS** na política do Agente de Rede.

Instruções de como proceder:

Console de Administração: Sincronizando atualizações do Windows Update com o Servidor de Administração, Configurando atualizações do Windows em uma política de Agente de Rede

- Kaspersky Security Center Web Console: Criação da tarefa Executar a sincronização com o Windows Update

7. **Executar uma tarefa de instalação de atualização**

   Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Quando você inicia essas tarefas, as atualizações são baixadas e instaladas nos dispositivos gerenciados. Após a conclusão da tarefa, verifique se ela possui o status *Concluída com êxito* na lista de tarefas.

8. **Criar o relatório sobre os resultados da instalação da atualização de software de terceiros (opcional)**

   Para ver estatísticas detalhadas sobre a instalação de atualização, gere um **Relatório de resultados da instalação de atualizações de software de terceiros**.

   Instruções de como proceder:

   - Console de Administração: Criando e visualizando um relatório
   - Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

### Resultados

Se você tiver criado e configurado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as atualizações serão instaladas nos dispositivos gerenciados automaticamente. Quando novas atualizações são baixadas no repositório do Servidor de Administração, o Kaspersky Security Center verifica se elas atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão instaladas automaticamente na próxima tarefa executada.

Se você tiver criado a tarefa *Instalar atualizações do Windows Update*, apenas as atualizações especificadas nas propriedades da tarefa *Instalar atualizações do Windows Update* serão instaladas. No futuro, caso deseje instalar novas atualizações baixadas no repositório do Servidor de Administração, será preciso adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma nova tarefa *Instalar atualizações do Windows Update*.

## Sobre as atualizações de software de terceiros

O Kaspersky Security Center permite gerenciar as atualizações do software de terceiros instalado em dispositivos gerenciados e corrigir vulnerabilidade em aplicativos da Microsoft e de produtos de outros fornecedores através da instalação das atualizações necessárias.

O Kaspersky Security Center procura atualizações por meio da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Servidor de Administração recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa. Após visualizar as informações sobre as atualizações disponíveis, você pode instalar as mesmas nos dispositivos.

O Kaspersky Security Center atualiza alguns aplicativos ao remover a versão anterior do aplicativo e ao instalar uma nova versão.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

### Tarefas para instalação das atualizações de software de terceiros

Quando os metadados das atualizações de software de terceiros são baixados para o repositório, você pode instalar as atualizações nos dispositivos clientes usando as seguintes tarefas:

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de produtos de outros fornecedores. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

Quando essa tarefa é concluída, as atualizações são instaladas nos dispositivos gerenciados automaticamente. Quando os metadados das novas atualizações são baixados no repositório do Servidor de Administração, o Kaspersky Security Center verifica se as atualizações atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão baixadas e instaladas automaticamente na próxima tarefa executada.

A tarefa *Instalar as atualizações do Windows Update*

A tarefa *Instalar as atualizações do Windows Update* não requer uma licença, mas pode ser usada para instalar apenas atualizações do Windows Update.

Quando esta tarefa é concluída, apenas as atualizações especificadas nas propriedades da tarefa são instaladas. No futuro, caso deseje instalar novas atualizações baixadas no repositório do Servidor de Administração, será preciso adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma nova tarefa Instalar atualizações do Windows Update.

### Usar Servidor de Administração como servidor WSUS

As informações sobre atualizações disponíveis são fornecidas pelo serviço do Windows Update. O Servidor de Administração pode ser usado como um servidor Windows Server Update Services (WSUS). Para usar o Servidor de Administração como o servidor WSUS, crie a tarefa de sincronização Executar a sincronização do Windows Update e selecione a opção **Usar o Servidor de Administração como servidor WSUS** na política do Agente de Rede. Após ter configurado a sincronização dos dados com o Windows Update, o Servidor de Administração fornece atualizações de serviços do Windows Update nos dispositivos no modo centralizado e com a frequência definida.

## Instalar atualizações de software de terceiros

É possível instalar atualizações de softwares de terceiros em dispositivos gerenciados criando e executando uma das seguintes tarefas:

- *Instalar as atualizações necessárias e corrigir vulnerabilidades*

  A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Você pode usar esta tarefa para instalar as atualizações do Windows Update fornecidas pela Microsoft e atualizações de produtos de outros fornecedores.

- *Instalar as atualizações do Windows Update*

  Você pode usar a tarefa *Instalar as atualizações do Windows Update* para instalar apenas atualizações do Windows Update.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para instalar as atualizações necessárias das seguintes maneiras:

- Abrindo a lista de atualizações e especificando quais atualizações instalar.
  Como resultado, é criada uma nova tarefa para instalar as atualizações selecionadas. Como opção, você pode adicionar as atualizações selecionadas a uma tarefa existente.
- Executando o assistente de Instalação de atualizações.

  O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

  O assistente simplifica a criação e a configuração de uma tarefa de instalação de atualização e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações para instalação.

## Instalar atualizações de softwares de terceiros usando a lista de atualizações

*Para instalar atualizações de software de terceiros usando a lista de atualizações:*

1. Abra uma das listas de atualizações:

   Para abrir a lista geral de atualização, No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   - Para abrir a lista de atualização para um dispositivo gerenciado, No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Atualizações disponíveis**.
   - Para abrir a lista de atualização para um aplicativo específico, No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Atualizações disponíveis**.

   Aparece uma lista das atualizações disponíveis.

2. Marque as caixas de seleção ao lado das atualizações que deseja baixar.

3. Clique no botão **Instalar as atualizações**.
   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA). Se você recusar o EULA, a atualização do software não é instalada.

4. Selecione uma das seguintes opções:

   **Nova tarefa**
   O Assistente para nova tarefa inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será pré-selecionada. Se você não tiver a licença, a tarefa *Instalar as atualizações do Windows Update* será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   **Instalar a atualização (adicionar a regra à tarefa especificada)**
   Selecione uma tarefa à qual deseja adicionar as atualizações selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Uma nova regra para instalar as atualizações selecionadas será adicionada automaticamente à tarefa escolhida. Se você não tiver a licença, selecione a tarefa *Instalar as atualizações do Windows Update*. As atualizações selecionadas serão adicionadas às propriedades da tarefa.
   A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Dispositivos → Tarefas**. Se você optou por adicionar as atualizações a uma tarefa existente, as atualizações serão salvas nas propriedades da tarefa.

Para instalar atualizações de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. É possível iniciar qualquer uma dessas tarefas manualmente ou especificar configurações de agendamento nas propriedades da tarefa iniciada. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

## Instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações

O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

*Para criar uma tarefa para instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações:*

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.
   Aparece uma lista das atualizações disponíveis.

2. Marque a caixa de seleção ao lado da atualização que deseja instalar.

3. Clique no botão **Executar o assistente de instalação de atualização**.
   O assistente de Instalação de atualizações é iniciado. A página **Selecionar tarefa de instalação da atualização** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Instalar as atualizações do Windows Update*

     *Corrigir vulnerabilidades*

Você não pode modificar as tarefas dos dois últimos tipos para instalar novas atualizações. Para instalar novas atualizações, você só pode usar as tarefas do tipo *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Caso deseje que o assistente exiba apenas as tarefas que instalam a atualização selecionada, ative a opção **Exibir apenas tarefas que instalam esta atualização**.

5. Selecione o que deseja fazer:

   Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.

   - Para adicionar uma nova regra a uma tarefa existente:

     a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

     b. Na página aberta, configure a nova regra:

     - Regra de instalação de atualizações deste nível de importância

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.
       Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     - Regra de instalação de atualizações deste nível de importância de acordo com o MSRC

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

       Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     Regra de instalação para atualizações deste fornecedor

       Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

       Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações do tipo**

  **Regra de instalação para a atualização selecionada**

- Aprovar atualizações selecionadas

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

  - Regra de instalação de atualizações deste nível de importância

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
    Por padrão, esta opção está desativada.

  Regra de instalação de atualizações deste nível de importância de acordo com o MSRC

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

- Regra de instalação para atualizações deste fornecedor

  Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.
  Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações do tipo**

- **Regra de instalação para a atualização selecionada**

- Aprovar atualizações selecionadas

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.
  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.
  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente de Instalação de atualizações é exibida no Assistente para Novas Tarefas. Ao concluir o assistente, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será adicionada na lista de tarefas.

## Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias

Através da tarefa Encontrar as vulnerabilidades e as atualizações necessárias, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiro instalado nos dispositivos gerenciados.

A tarefa Encontrar as vulnerabilidades e as atualizações necessárias é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

*Para criar uma tarefa Encontrar as vulnerabilidades e as atualizações necessárias:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.
   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
7. Clique no botão **Criar**.
   A tarefa é criada e exibida na lista de tarefas.
8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
9. Na janela Propriedades da tarefa, especifique as configurações gerais da tarefa.
10. Na guia **Configurações do aplicativo**, especifique as seguintes configurações:
    - Buscar por vulnerabilidades e atualizações listadas pela Microsoft

Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Se esta opção estiver desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações do Microsoft Windows aplicáveis recebidas da fonte de atualizações da Microsoft anteriormente e que estão armazenadas no cache do dispositivo.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualizações para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo** no grupo de configurações no modo **Modo de pesquisa do Windows Update** é selecionado.

- O Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows que foram recebidas da fonte de atualizações da Microsoft anteriormente e armazenadas no cache do dispositivo, se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Passivo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada, ou se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada.
- Independente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), se a opção **Desativado** no grupo de configurações **Modo de pesquisa do Windows Update** estiver selecionada, o Kaspersky Security Center não solicita nenhuma informação sobre as atualizações.

- **Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky**

  Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

  Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.
  Por padrão, esta opção está desativada.

  **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

11. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

# As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Além das configurações gerais da tarefa, é possível especificar as seguintes configurações ao criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou mais recentes, ao configurar as propriedades da tarefa criada:

**Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

**Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Se esta opção estiver desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações do Microsoft Windows aplicáveis recebidas da fonte de atualizações da Microsoft anteriormente e que estão armazenadas no cache do dispositivo.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualizações para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo** no grupo de configurações no modo **Modo de pesquisa do Windows Update** é selecionado.

- O Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows que foram recebidas da fonte de atualizações da Microsoft anteriormente e armazenadas no cache do dispositivo, se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Passivo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada, ou se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada e a opção **Ativo**, no grupo de configurações **Modo de pesquisa do Windows Update**, estiver selecionada.
- Independente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), se a opção **Desativado** no grupo de configurações **Modo de pesquisa do Windows Update** estiver selecionada, o Kaspersky Security Center não solicita nenhuma informação sobre as atualizações.

Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

**Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

## Recomendações sobre o agendamento de tarefas

Ao agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, certifique-se de que as duas opções **Executar tarefas ignoradas** e **Usar retardo aleatório automaticamente para início da tarefa** estejam desativadas.

Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente. Caso as regras do local de trabalho da organização ofereçam o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem ligados novamente, ou seja, na manhã do dia seguinte. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

## Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.

- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

*Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.
   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
   Se a tarefa não for exibida, verifique se sua conta tem direitos para **Ler**, **Modificar** e **Executar** na área funcional **Administração de sistema**: **Gerenciamento de Patches e Vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:
   - **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

Por padrão, esta opção está desativada.

- Instalar os componentes gerais do sistema necessários

Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional

Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.
Por padrão, esta opção está desativada.

Permitir a instalação de novas versões dos aplicativos durante atualizações

Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.
Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

Por padrão, esta opção está ativada.

A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

Baixar atualizações para o dispositivo sem instalá-las

Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.
As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

Por padrão, esta opção está desativada.

- Pasta para download de atualizações

Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- Ativar diagnóstico avançado

Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente.

Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.
Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.
Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

**Reiniciar após (min.)**

Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

**Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).
Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.
Por padrão, esta opção está desativada.

8. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.
10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.
12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

## Adicionar regras para instalação da atualização

Esse recurso está disponível apenas sob a licença do Gerenciamento de patches e vulnerabilidades.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.

Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

*Para adicionar uma nova regra para todas as atualizações:*

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

*Para adicionar uma nova regra para atualizações do Windows Update:*

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

   Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

   Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

   Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

   Por padrão, esta opção está desativada.

   - Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.
5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.
6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

*Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:*

1. Clique no botão **Adicionar**.
   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.
3. Na página **Critérios gerais**, especifique as seguintes configurações:

- Conjunto de atualizações a instalar

  Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

  - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.

    **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.

    **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.
5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

## Criar a tarefa Instalar atualizações do Windows Update

A tarefa *Instalar as atualizações do Windows Update* permite instalar as atualizações de software fornecidas pelo serviço Windows Update em dispositivos gerenciados.

Se você não possui uma licença do Gerenciamento de patches e vulnerabilidades, não pode criar novas tarefas do tipo *Instalar as atualizações do Windows Update*. Para instalar novas atualizações, adicione-as a uma tarefa *Instalar as atualizações do Windows Update* existente. Recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Instalar as atualizações do Windows Update*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você. Além disso, essa tarefa permite instalar atualizações de fornecedores de software que não sejam a Microsoft.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

*Para criar a tarefa Instalar atualizações do Windows Update:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações do Windows Update**.
4. Especifique o nome da tarefa que está criando.

O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Clique no botão **Adicionar**.
A lista de atualizações é aberta.

7. Selecione as atualizações do Windows Update que deseja instalar e, a seguir, clique em **OK**.

8. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

  **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.
  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.
  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.
  Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

   - **Conta padrão**

     A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

     Por padrão, esta opção está selecionada.

   - **Especificar conta**

     Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

     **Conta**

     Conta sob a qual a tarefa é executada.

     **Senha**

     Senha da conta sob a qual a tarefa será executada.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

# Exibir informações sobre atualizações disponíveis para software de terceiros

Você pode visualizar a lista de atualizações disponíveis para software de terceiros, incluindo software da Microsoft, instalado em dispositivos cliente.

*Para exibir uma lista de atualizações disponíveis para aplicativos de terceiros instalados em dispositivos cliente,*

No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

Aparece uma lista das atualizações disponíveis.

Você pode especificar um filtro para visualizar a lista de atualizações de software. Clique no ícone **Filtro** (⚙) no canto superior direito da lista de atualizações de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

*Para visualizar as propriedades de uma atualização:*

1. Clique no nome da atualização de software necessária.
2. A janela de propriedades da atualização é aberta, exibindo informações agrupadas nas seguintes guias:
   - Geral

     Esta guia exibe detalhes gerais da atualização selecionada:

     - Status de aprovação da atualização (pode ser alterado manualmente, selecionando um novo status na lista suspensa)
     - Categoria do Windows Server Update Services (WSUS) à qual a atualização pertence

       Data e hora em que a atualização foi registrada
     - Data e hora em que a atualização foi criada
     - Nível de importância da atualização

       Requisitos de instalação impostos pela atualização
     - Família de aplicativos à qual a atualização pertence

       Aplicativo ao qual a atualização se aplica
     - Número da revisão de atualização
   - Atributos

Esta guia exibe um conjunto de atributos que você pode usar para obter mais informações sobre a atualização selecionada. Este conjunto difere, dependendo se a atualização é publicada pela Microsoft ou por um fornecedor terceiro.

A guia exibe as seguintes informações para uma atualização da Microsoft:

- O nível de importância da atualização, conforme definido pelo Microsoft Security Response Center (MSRC)
- Link para o artigo na Base de Dados de Conhecimento Microsoft que descreve a atualização

  Link para o artigo no Boletim de Segurança da Microsoft que descreve a atualização
- Identificador da atualização (ID)

A guia exibe as seguintes informações para uma atualização de terceiros:

  Se a atualização é um patch ou um pacote de distribuição completo
- Idioma de localização da atualização

  Se a atualização é instalada automática ou manualmente
- Se a atualização foi revogada após ser aplicada
- Link para baixar a atualização

- **Dispositivos**

  Esta guia exibe uma lista de dispositivos nos quais a atualização selecionada foi instalada.

- **Vulnerabilidades corrigidas**

  Esta guia exibe uma lista de vulnerabilidades que a atualização selecionada pode corrigir.

- **Cruzamento de atualizações**

  Esta guia exibe possíveis redundâncias entre várias atualizações publicadas para o mesmo aplicativo, ou seja, se a atualização selecionada pode substituir outras atualizações ou, vice-versa (disponíveis apenas para atualizações Windows).

- **Tarefas para instalar esta atualização**

  Esta guia exibe uma lista de tarefas cujo escopo inclui a instalação da atualização selecionada. A guia também permite que você crie uma nova tarefa de instalação remota para a atualização.

*Para exibir as estatísticas de uma instalação de atualização:*

1. Selecione a caixa de seleção ao lado da atualização de software necessária.
2. Clique no botão **Estatísticas de status da instalação de atualizações**.

O diagrama dos status de instalação da atualização é exibido. Clicar em um status abre uma lista de dispositivos nos quais a atualização tem o status selecionado.

Você pode visualizar informações sobre atualizações de software disponíveis para software de terceiros, incluindo software da Microsoft, instalado no dispositivo gerenciado selecionado que executa o Windows.

*Para visualizar uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:*

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar atualizações de software de terceiros.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Atualizações disponíveis**. Caso deseje visualizar apenas as atualizações instaladas, ative a opção **Exibir atualizações instaladas**.

A lista de atualizações de software de terceiros disponíveis para o dispositivo selecionado é exibida.

## Exportando a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de atualizações para software de terceiros, incluindo o software Microsoft, exibido no momento para os arquivos CSV e TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

*Para exportar como arquivo de texto a lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:*

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   A página exibe uma lista de atualizações disponíveis para software de terceiros instalado em todos os dispositivos gerenciados.

2. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, é baixado para o dispositivo usado no momento.

*Para exportar como arquivo de texto uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:*

1. Abra a lista de atualizações de software de terceiros disponíveis no dispositivo gerenciado selecionado.

2. Selecione as atualizações de software que você deseja exportar.

   Ignore esta etapa se desejar exportar uma lista completa de atualizações de software.

   Se você deseja exportar a lista completa de atualizações de software, apenas as vulnerabilidades exibidas na pági

Se deseja exportar apenas as atualizações instaladas, marque a caixa **Exibir atualizações instaladas**.

3. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, instalados no dispositivo gerenciado é baixado para o dispositivo usado no momento.

## Aprovando e recusando atualizações de software de terceiros

Ao configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível criar uma regra que exija um status específico das atualizações a serem instaladas. Por exemplo, uma regra de atualização pode permitir a instalação do seguinte:

- Somente atualizações aprovadas

  Somente atualizações aprovadas e indefinidas

- Todas as atualizações, independentemente dos status de atualização

Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

*Para aprovar ou recusar uma ou várias atualizações:*

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.
   Aparece uma lista das atualizações disponíveis.

2. Selecione as atualizações que deseja aprovar ou recusar.

3. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

   O valor padrão é *Indefinido*.

As atualizações selecionadas têm os status que você definiu.

Como opção, você pode alterar o status de aprovação nas propriedades de uma atualização específica.

*Para aprovar ou recusar uma atualização em suas propriedades:*

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Clique no nome da atualização que deseja aprovar ou recusar.
   A janela Propriedades da atualização é aberta.