Editar uma função de usuário

Para editar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja editar.
3. Na janela de propriedades da função exibida, altere as configurações da função:
   - Na guia **Geral**, edite o nome da função.

     Você não pode editar o nome de uma função predefinida.

     Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.
4. Clique em **Salvar** para salvar as alterações.

A função atualizada aparece na lista de funções de usuário.

Editar o escopo de uma função de usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Para adicionar usuários, grupos de segurança e grupos de administração ao escopo de uma função de usuário, você pode usar qualquer dos seguintes métodos:

Método 1:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Marque as caixas de seleção ao lado dos usuários e grupos de segurança que deseja adicionar ao escopo da função de usuário.
3. Clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Na página **Selecionar função** do assistente, selecione a função de usuário que deseja atribuir.
5. Na página **Definir escopo** do assistente, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Clique no botão **Atribuir função** para fechar a janela.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao es

Método 2:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função para a qual deseja definir o escopo.
3. Na janela de propriedades da função exibida, selecione a guia **Configurações**.
4. Na seção **Escopo da função**, clique em **Adicionar**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
5. Na página **Definir escopo** do assistente, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Na página **Selecionar usuários** do assistente, selecione os usuários e os grupos de segurança que deseja adicionar ao escopo da função de usuário.
7. Clique no botão **Atribuir função** para fechar a janela.
8. Clique no botão **Fechar** (✕) para fechar a janela de propriedades da função.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Excluir uma função de usuário

Para excluir uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Marque a caixa de seleção ao lado do nome da função que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A função de usuário é excluída.

Associação de perfis da política a funções

Você pode associar funções de usuário a perfis da política. Nesse caso, a regra de ativação desse perfil da política é baseada na função: o perfil da política fica ativo para um usuário com a função especificada.

Por exemplo, a política proíbe qualquer software de navegação de GPS em todos os dispositivos em um grupo de administração. O software de navegação de GPS é necessário em um dispositivo único no grupo de administração de Usuários, notadamente que for de propriedade do courier. Nesse caso, você pode atribuir uma função "Courier" ao seu proprietário e criar um perfil da política, permitindo que o software de navegação de GPS seja executado apenas nos dispositivos a cujos proprietários é atribuída a função "Courier". Todas as outras configurações de política são preservadas. Somente o usuário com a função "Courier" poderá executar o software de navegação de GPS. Depois, se outro funcionário receber a função "Courier", o novo funcionário também poderá executar o software de navegação no dispositivo da sua organização. Executar o software de navegação de GPS ainda será proibido em outros dispositivos no mesmo grupo de administração.

Para associar uma função a um perfil da política:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja associar a um perfil da política.
   A janela de propriedades da função é exibida com a guia **Geral** selecionada.
3. Selecione a guia **Configurações** e role para baixo até a seção **Políticas e perfis**.
4. Clique em **Editar**.
5. Para associar a função a:

   Um perfil da política existente – Clique no ícone de insígnia (>) ao lado do nome de política necessário e marque a caixa de seleção ao lado do perfil ao qual você deseja associar a função.

   Um novo perfil da política:

   a. Marque a caixa de seleção ao lado da política para a qual deseja criar um perfil.

   b. Clique em **Novo perfil de política**.

   c. Especifique um nome para o novo perfil e defina as configurações de perfil.

   d. Clique no botão **Salvar**.

   e. Selecione a caixa de seleção junto ao novo perfil.
6. Clique em **Atribuir à função**.

O perfil é associado à função e aparece nas propriedades da função. O perfil se aplica automaticamente a qualquer dispositivo cujo proprietário seja atribuído à função.

Gerenciar objetos no Kaspersky Security Center Web Console

Esta seção contém informações sobre o gerenciamento de revisão de objeto. O Kaspersky Security Center lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma *revisão* é criada. Cada revisão tem um número.

Os objetos do aplicativo suportam o gerenciamento de revisão incluem:

Servidores de Administração

- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Você pode executar as seguintes ações nas revisões do objeto:

- Comparar uma revisão selecionada à atual
- Compare selected revisions
- Comparar um objeto com uma revisão selecionada de outro objeto do mesmo tipo
- Exibir uma revisão selecionada
- Reverter as modificações feitas a um objeto para uma revisão selecionada
- Salve as revisões como um arquivo .txt

Na janela de propriedades de qualquer objeto que suporta o gerenciamento de revisão, a seção **Histórico de revisões** exibe uma lista de revisões de objeto com os seguintes detalhes:

- Número de revisão do objeto
- Data e hora em que o objeto foi modificado
- Nome do usuário que modificou o objeto
- A ação executada no objeto
- A descrição da revisão relativa à modificação feita nas configurações do objeto

Por padrão, a descrição da revisão do objeto está em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Descrição**. Na janela **Descrição da revisão do objeto**, insira algum texto para a descrição da revisão.

Adicionar uma descrição da revisão

O Kaspersky Security Center lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma revisão é criada. Cada revisão tem um número.

Você pode adicionar uma descrição da revisão para simplificar a procura por revisões na lista.

Para adicionar uma descrição para uma revisão:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione a revisão para a qual você precisa adicionar uma descrição.

3. Clique no botão **Editar descrição**.

   A janela **Descrição** se abre.

4. Na janela **Descrição**, insira algum texto para a descrição da revisão.

   Por padrão, a descrição da revisão do objeto está em branco.

5. Clique no botão **Salvar**.

A descrição é adicionada na revisão do objeto.

Exclusão de objetos

Esta seção fornece informações sobre como excluir objetos e como exibir as informações sobre os objetos após a sua exclusão.

Você pode excluir objetos, como os seguintes:

- Políticas
- Tarefas

  Pacotes de instalação
- Servidores de Administração virtual
- Usuários
- Grupos de segurança
- Grupos de administração

Quando você exclui um objeto, as informações sobre ele permanecem no banco de dados. O período de armazenamento das informações sobre os objetos excluídos é igual ao período de armazenamento das revisões de objetos (o período recomendado é de 90 dias). Você pode alterar o prazo de armazenamento somente se tiver a permissão **Modificar** na área de direitos **Objetos excluídos**.

Sobre a exclusão de dispositivos cliente

Quando um dispositivo gerenciado é excluído de um grupo de administração, o aplicativo move o dispositivo para o grupo dispositivos não atribuídos. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados, o Agente de Rede e qualquer aplicativo de segurança, por exemplo, o Kaspersky Endpoint Security, permanecem no dispositivo.

O Kaspersky Security Center gerencia os dispositivos no grupo Dispositivos não atribuídos de acordo com as seguintes regras:

- Caso tenha configurado as regras de movimentação de dispositivo e um dispositivo atenda aos critérios de uma regra de movimentação, o dispositivo é automaticamente movido para um grupo de administração de acordo com a regra.

  O dispositivo é armazenado no grupo dispositivos não atribuídos e é automaticamente removido do grupo de acordo com as regras de retenção de dispositivos.

As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

Ao excluir um dispositivo com unidade criptografada, os dados necessários para descriptografar a unidade também são excluídos. Nesse caso, para descriptografar o dispositivo, as seguintes condições devem ser atendidas:

- O dispositivo é reconectado ao Servidor de Administração para restaurar os dados necessários para descriptografar a unidade.
- O usuário do dispositivo lembra a senha de descriptografia.
- O aplicativo de segurança usado para criptografar o dispositivo, por exemplo, o Kaspersky Endpoint Security for Windows, ainda está instalado nele.

Caso o dispositivo seja criptografado pela tecnologia Kaspersky Disk Encryption, também é possível tentar recuperar os dados usando o utilitário de restauração FDERT.

Quando um dispositivo é excluído manualmente do grupo dispositivos não atribuídos, o aplicativo remove o dispositivo da lista. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados (se houver) permanecem no dispositivo. Assim, caso o dispositivo ainda esteja visível para o Servidor de Administração e a sondagem de rede regular tenha sido configurada, o Kaspersky Security Center descobre o dispositivo durante a sondagem e o recoloca no grupo Dispositivos não atribuídos. Portanto, é razoável excluir um dispositivo manualmente somente se o dispositivo estiver invisível para o Servidor de Administração.

Kaspersky Security Network (KSN)

Essa seção descreve como usar uma infraestrutura de serviços on-line, denominada Kaspersky Security Network (KSN). A seção fornece os detalhes sobre a KSN, assim como instruções sobre como ativar a KSN, configurar o acesso à KSN e visualizar as estatísticas sobre o uso do Servidor proxy da KSN.

Sobre a KSN

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços on-line que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso de dados a partir da Kaspersky Security Network garante uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhora a efetividade de alguns componentes de proteção e reduz o risco de falsos positivos. A KSN permite usar os bancos de dados de reputação da Kaspersky para obter informações sobre os aplicativos instalados nos dispositivos gerenciados.

O Kaspersky Security Center oferece suporte às seguintes soluções de infraestrutura KSN:

- *KSN Global* é uma solução que permite trocar informações com a Kaspersky Security Network. Se você participar da KSN, você concorda em enviar informações à Kaspersky, no modo automático, sobre a operação dos aplicativos Kaspersky instalados nos dispositivos cliente gerenciados por meio do Kaspersky Security Center. As informações são transferidas de acordo com as configurações de acesso da KSN atuais. Os analistas da Kaspersky também averiguam as informações recebidas e as incluem nos bancos de dados estatísticos e de reputação da Kaspersky Security Network. O Kaspersky Security Center usa essa solução por padrão.

- A *KSN Privada* é uma solução que permite aos usuários de dispositivos com aplicativos Kaspersky instalados obter acesso aos bancos de dados de reputação da Kaspersky Security Network, bem como a outros dados estatísticos, sem enviar dados para a KSN de seus próprios computadores. A Kaspersky Private Security Network (KSN Privada) foi projetada para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

  - Os dispositivos do usuário não estão conectados à Internet.

    A transmissão de quaisquer dados fora do país ou fora da LAN corporativa é proibida pela lei ou limitada por políticas de segurança corporativas.

  Você pode definir configurações de acesso da Kaspersky Private Security Network na seção **Configurações de Proxy da KSN** da janela de propriedades do Servidor de Administração.

O aplicativo solicita a você participar da KSN durante a execução do Assistente de início rápido. Você pode iniciar ou parar de usar a KSN em qualquer momento durante o uso do aplicativo.

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se recusar, continuará usando a KSN de acordo com a versão Declaração KSN aceita anteriormente.

Quando o KSN está habilitado, o Kaspersky Security Center verifica se os servidores da KSN estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que o nível de segurança seja mantido para os dispositivos gerenciados.

Os dispositivos cliente gerenciados pelo Servidor de Administração interagem com a KSN por meio do servidor proxy da KSN. O servidor proxy da KSN fornece os seguintes recursos:

- Os dispositivos cliente podem enviar solicitações à KSN e transferir informações para a KSN mesmo que não tenham acesso direto à Internet.

  O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Você pode configurar o Servidor Proxy KSN na seção **Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

Configurar o acesso à KSN

Você pode configurar o acesso ao Kaspersky Security Network (KSN) no Servidor de Administração e em um ponto de distribuição.

Para configurar o acesso do Servidor de Administração à KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.
   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

Os dados são enviados dos dispositivos cliente para a KSN de acordo com a política do Kaspersky Endpoint Security que estiver ativa naqueles dispositivos cliente. Se essa caixa de seleção estiver desmarcada, nenhum dado será serão enviado a KSN do Servidor de Administração e de dispositivos cliente através do Kaspersky Security Center. No entanto, os dispositivos cliente podem enviar dados para a KSN diretamente (evitando o Kaspersky Security Center), de acordo com suas respectivas configurações. A política do Kaspersky Endpoint Security, que está ativa nos dispositivos cliente, determina quais dados serão enviados diretamente (evitando o Kaspersky Security Center) pelos dispositivos para a KSN.

4. Alterne o botão para a posição **Usar a Kaspersky Security Network Ativado**.

Se essa opção estiver ativada, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar esta opção, certifique-se de ler e aceitar os termos da Declaração da KSN.
Se estiver usando a KSN Privada, alterne o botão para a posição **Usar a Kaspersky Private Security Network Ativado** e clique no botão **Selecionar arquivo com config. proxy da KSN** para baixar as configurações da KSN Privada (arquivos com as extensões pkcs7 e pem). Após as configurações serem baixadas, a interface exibe o nome do provedor e os contatos, assim como a data de criação do arquivo com as configurações da KSN Privada.

> Ao ativar a KSN Privada, preste atenção aos pontos de distribuição configurados para enviar solicitações da KSN diretamente ao Cloud KSN. Os pontos de distribuição que possuem o Agente de Rede versão 11 (ou anterior) instalado continuarão a enviar solicitações da KSN ao Cloud KSN. Para reconfigurar os pontos de distribuição para enviar solicitações da KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição. Você pode ativar esta opção nas propriedades do ponto de distribuição ou na política do Agente de Rede.

Ao alternar o botão para a posição **Usar a Kaspersky Private Security Network Ativado**, é exibida uma mensagem com detalhes sobre a KSN Privada.
Os seguintes aplicativos Kaspersky são compatíveis com a KSN privada:

Kaspersky Security Center

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless
- Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent

Se você ativar a opção KSN Privada no Kaspersky Security Center, esses aplicativos receberão informações sobre compatibilidade com a KSN Privada. Na janela de configurações do aplicativo, na subsecção **Kaspersky Security Network** da seção **Proteção Avançada Contra Ameaças**, **Provedor da KSN: KSN Privada** é exibido. Caso contrário, **Provedor da KSN: KSN Global** será exibido.

> Se você usa versões do aplicativo anteriores ao Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless ou anteriores ao Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent ao executar a KSN Privada, recomendamos que você use Servidores de Administração secundários para os quais o uso da KSN Privada não foi ativado.

> O Kaspersky Security Center não enviará nenhum dado estatístico à Kaspersky Security Network se a KSN Privada estiver configurada na seção **Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

5. Se você tiver as configurações do servidor proxy definidas nas propriedades do Servidor de Administração, mas sua arquitetura de rede requer o uso direto da KSN Privada, ative a opção **Ignorar configurações do Servidor Proxy ao conectar à KSN Privada**. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

6. Configure a conexão do Servidor de Administração ao serviço de proxy da KSN:

   - Em **Configurações de conexão**, para a **Porta TCP**, especifique o número da porta TCP que será usada para se conectar ao Servidor proxy da KSN. A porta padrão para conectar-se ao servidor proxy da KSN é 13111.
   - Se desejar que o Servidor de Administração seja conectado ao servidor proxy da KSN por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de porta para **Porta UDP**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta UDP padrão para se conectar ao servidor proxy da KSN será 15111.

7. Alterne o botão para a posição **Conectar os Servidores de Administração secundários na KSN pelo Servidor de Administração principal Ativado**.

   Se esta opção estiver ativada, Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy KSN. Se esta opção estiver desativada, os Servidores de Administração secundários conectam-se à KSN por conta própria. Neste caso, os dispositivos gerenciados usam Servidores de Administração secundários como servidores proxy KSN.

   > Os Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy se, no painel direito da seção **Configurações de Proxy da KSN** nas propriedades do Servidores de Administração secundários, o botão estiver alternado para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

8. Clique no botão **Salvar**.

As configurações de acesso à KSN serão salvas.

Você também pode configurar o acesso ao ponto de distribuição à KSN, por exemplo, se quiser reduzir a carga no Servidor de Administração. O ponto de distribuição que atua como um servidor proxy da KSN envia solicitações da KSN de dispositivos gerenciados para a Kaspersky diretamente, sem usar o Servidor de Administração.

Para configurar o acesso dos pontos de distribuição ao Kaspersky Security Network (KSN):

1. Certifique-se de que o ponto de distribuição seja atribuído manualmente.

2. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

3. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

4. Clique no nome do ponto de distribuição para abrir a janela de propriedades da tarefa.

5. Na janela de propriedades do ponto de distribuição, na seção **Proxy da KSN**, ative a opção **Ativar Proxy KSN no lado do ponto de distribuição** e, em seguida, ative a opção **Acessar a KSN Cloud/KSN Privada diretamente pela internet**.

6. Clique em **OK**.

O ponto de distribuição atuará como um servidor proxy da KSN.

Ativar e desativar a KSN

Para ativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

   O serviço de Proxy da KSN será ativado.

4. Alterne o botão para a posição **Usar a Kaspersky Security Network Ativado**.

   A KSN será ativada.

   Se o botão de alternância estiver ativado, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar este botão de alternância, você deve ler e aceitar os termos da Declaração da KSN.

5. Clique no botão **Salvar**.

Para desativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Desativado** para desativar o serviço de proxy da KSN ou alterne para a posição **Usar a Kaspersky Security Network Desativado**.
   Se um desses botões estiver desativado, os dispositivos cliente não enviarão resultados da instalação de patches para a Kaspersky.

   Se estiver usando a KSN Privada, alterne o botão para a posição **Usar a Kaspersky Private Security Network Desativado**.

   A KSN será desativada.

4. Clique no botão **Salvar**.

Visualizando a Declaração da KSN aceita

Ao ativar o Kaspersky Security Network (KSN), você deve ler e aceitar a Declaração da KSN. Você pode ver a Declaração da KSN aceita a qualquer momento.

Para visualizar a declaração KSN aceita:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.
3. Clique no link **Ver Declaração sobre coleta de dados do KSN**.

Na janela aberta, você pode ver o texto da Declaração KSN aceita.

Aceitando uma declaração da KSN atualizada

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Caso a declaração seja recusada, o usuário continuará usando a KSN de acordo com a versão Declaração da KSN aceita anteriormente.

Após atualizar ou atualizar o Servidor de Administração, a declaração da KSN atualizada é exibida automaticamente. Se você recusar a declaração da KSN atualizada, você poderá ainda vê-la e aceitá-la posteriormente.

Para visualizar e aceitar ou recusar uma Declaração da KSN atualizada:

1. Clique no link **Exibir notificações** no canto superior direito da janela do aplicativo principal.

   A janela **Notificações** se abre.

2. Clique no link **Ver a Declaração da KSN atualizada**.

   A janela **Atualização da Declaração da Kaspersky Security Network** se abre.

3. Leia a Declaração da KSN e, em seguida, decida-se clicando em um dos seguintes botões:

   - **Eu aceito a declaração da KSN atualizada**
   - **Usar KSN sob as condições da Declaração anterior**

Dependendo da sua escolha, a KSN continuará funcionando de acordo com os termos da Declaração da KSN em vigor ou atualizada. Você pode ver o texto da Declaração da KSN aceita nas propriedades do Servidor de Administração a qualquer momento.

Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Em um dispositivo gerenciado atribuído como ponto de distribuição é possível ativar o servidor proxy da KSN. Um dispositivo gerenciado funciona como servidor proxy da KSN quando o serviço ksnproxy está sendo executado no dispositivo. É possível verificar, ativar ou desativar esse serviço localmente no dispositivo.

Você pode atribuir um dispositivo baseado em Windows ou Linux como um ponto de distribuição. O método de verificação do ponto de distribuição depende de seu sistema operacional.

Para verificar se o ponto de distribuição baseado em Windows funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, no Windows, abra **Serviços** (**Todos os programas** → **Ferramentas administrativas** → **Serviços**).

   Na lista de serviços, verifique se o serviço ksnproxy está sendo executado.

Se o serviço ksnproxy estiver em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Se desejar, você pode desativar o serviço ksnproxy. Nesse caso, o Agente de Rede no ponto de distribuição para de participar da Kaspersky Security Network. Isso requer direitos de administrador local.

Para verificar se o ponto de distribuição baseado em Linux funciona como servidor proxy da KSN:

1. No dispositivo do ponto de distribuição, exiba a lista de processos em execução.
2. Na lista de processos em execução, verifique se o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` está em execução.

Caso o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` esteja em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Atualização dos bancos de dados e dos aplicativos da Kaspersky

Esta seção descreve as etapas que você deve seguir para atualizar regularmente o seguinte:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após ter concluído o Cenário de configuração de proteção da rede, você precisará manter a confiabilidade do sistema de proteção para ter certeza de que os Servidores de Administração e os dispositivos gerenciados estejam permanentemente protegidos contra várias ameaças, incluindo vírus, ataques à rede e ataques de phishing.

A proteção da rede é mantida atualizada por atualizações regulares dos seguintes:

Bancos de dados e módulos de software da Kaspersky

- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Quando concluir este cenário, você poderá ter certeza do seguinte:

- A sua rede está protegida pelo software da Kaspersky mais recente, inclusive aplicativos de segurança e componentes do Kaspersky Security Center.
- Os bancos de dados de antivírus e outros bancos de dados da Kaspersky críticos para a segurança de rede são sempre atualizados.

Pré-requisitos

Os dispositivos gerenciados devem ter uma conexão com o Servidor de Administração. Se eles não tiverem uma conexão, considere atualizar os bancos de dados, módulos de software e aplicativos da Kaspersky manualmente ou diretamente nos servidores de atualização da Kaspersky.

O Servidor de Administração deve ter uma conexão com a Internet.

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança da Kaspersky nos dispositivos gerenciados de acordo com o cenário de implementação de aplicativos Kaspersky através do Kaspersky Security Center Web Console.
2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o cenário de configuração da proteção de rede.
3. Atribuído um volume apropriado de pontos de distribuição conforme o número de dispositivos gerenciados e a topologia de rede.

A atualização dos bancos de dados e dos aplicativos da Kaspersky prossegue em estágios:

1 Seleção de um esquema de atualização

Há vários esquemas que você pode usar para instalar atualizações para componentes e aplicativos de segurança do Kaspersky Security Center. Selecione o esquema ou vários esquemas que atendem aos requisitos de sua melhor rede.

2 Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração

Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Se você não tiver executado o assistente, crie a tarefa agora.

Essa tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para o repositório do Servidor de Administração, bem como atualizar bancos de dados e módulos do software da Kaspersky para o Kaspersky Security Center. Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

Se a rede tiver pontos de distribuição atribuídos, as atualizações serão baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Nesse caso, os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.

Instruções de como proceder:

- Console de Administração: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração
- Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração

3 Criar a tarefa para baixar as atualizações para os repositórios de pontos de distribuição (opcional)

Por padrão, as atualizações são baixadas para os pontos de distribuição do Servidor de Administração. Você pode configurar o Kaspersky Security Center para baixar as atualizações para os pontos de distribuição diretamente dos servidores de atualização da Kaspersky. Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

Quando a rede tiver atribuído pontos de distribuição e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for criada, os pontos de distribuição baixarão atualizações dos servidores de atualização d

Instruções de como proceder:

- Console de Administração: Criar a tarefa ao baixar atualizações nos repositórios dos pontos de distribuição
- Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para os repositórios de pontos de distribuição

4 Configurar os pontos de distribuição

Quando a sua rede tem pontos de distribuição atribuídos, certifique-se de que a opção **Implementar atualizações** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção é desativada para um ponto de distribuição, os dispositivos incluídos no escopo das atualizações de download do ponto de distribuição do repositório do Servidor de Administração.

Se quiser que os dispositivos gerenciados recebam atualizações somente dos pontos de distribuição, ative a opção **Distribuir os arquivos somente através dos pontos de distribuição** na política de Agente de Rede.

5 Otimizando o processo de atualização usando o modelo offline de download de atualização ou arquivos diff (opcionais)

Você pode otimizar o processo de atualização usando o modelo offline de download de atualização (ativado por padrão) ou usando arquivos diff. Para cada segmento de rede, você precisa escolher qual desses dois recursos ativar, porque eles não podem funcionar simultaneamente.

Quando o modelo offline de download das atualizações for ativado, o Agente de Rede baixará as atualizações necessárias para o dispositivo gerenciado quando as atualizações forem baixadas para o repositório do Servidor de Administração, antes de o aplicativo de segurança solicitar as atualizações. Isso melhora a confiabilidade do processo de atualização. Para usar o recurso, ative a opção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** na política do agente de rede.

Se não usar o modelo offline de download das atualizações, você poderá otimizar o tráfego entre o Servidor de Administração e os dispositivos gerenciados usando arquivos diff. Quando esse recurso for ativado, o Servidor de Administração ou um ponto de distribuição baixará arquivos diff em vez de arquivos inteiros de bancos de dados ou módulos de software da Kaspersky. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. Por isso, um arquivo diff ocupa menos espaço do que um arquivo inteiro. Isso resulta na redução no tráfego entre o Servidor de Administração ou os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e/ou da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

Instruções de como proceder:

- Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky
- Console de Administração: Ativar e desativar o modelo offline para o download das atualizações
- Kaspersky Security Center Web Console: Ativar e desativar o modelo offline para o download das atualizações

6 Verificação das atualizações baixadas (opcional)

Antes de instalar as atualizações baixadas, é possível verificar as atualizações pela tarefa de *Verificação de atualizações*. Essa tarefa executa em sequência as tarefas de atualização de dispositivo e as tarefas de verificação de malwares configuradas por meio configurações da coleção especificada de dispositivos de teste. Para obter os resultados da tarefa, o Servidor de Administração inicia ou bloqueia a propagação de atualização para os dispositivos restantes.

A tarefa de *Verificação de atualizações* pode ser executada como parte da tarefa *Baixar atualizações para o repositório do Servidor de Administração*. Nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*, ative a opção **Verificar atualizações antes de distribuir** no Console de Administração ou na opção **Executar verificação de atualizações** no Kaspersky Security Center Web Console.

Instruções de como proceder:

- Console de Administração: Verificação das atualizações baixadas
- Kaspersky Security Center Web Console: Verificar as atualizações baixadas

7 Aprovar e recusar atualizações de software

Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Negado*. As atualizações aprovadas sempre são instaladas. Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados. As atualizações não definidas só podem ser instaladas no Agente de Rede e em outros componentes do Kaspersky Security Center conforme as configurações de política do Agente de Rede. As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos. Se uma atualização recusada para um aplicativo de segurança tiver sido instalada anteriormente, o Kaspersky Security Center tentará desinstalar a atualização de todos os dispositivos. As atualizações de componentes do Kaspersky Security Center não podem ser desinstaladas.

Instruções de como proceder:

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

8 Configuração da instalação automática de atualizações e correções para componentes do Kaspersky Security Center

As atualizações e os patches baixados para o Agente de Rede e outros componentes do Kaspersky Security Center são instalados automaticamente. Se você deixou a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** ativada nas propriedades do Agente de Rede, todas as atualizações serão instaladas automaticamente após o download no repositório (ou em vários repositórios). Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

Instruções de como proceder:

- Console de Administração: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center
- Kaspersky Security Center Web Console: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

9 Instalação de atualizações para o Servidor de Administração

As atualizações de software para o Servidor de Administração não dependem dos status de atualização. Elas não são instaladas automaticamente e devem ser previamente aprovadas pelo administrador na guia **Monitoramento** no Console de Administração (**Servidor de Administração** `<nome do servidor>` → **Monitoramento**) ou na seção **Notificações** no Kaspersky Security Center Web Console (**Monitoramento e relatórios** → **Notificações**). Depois disso, o administrador deve executar explicitamente a instalação das atualizações.

10 Configuração da instalação automática de atualizações para os aplicativos de segurança

Crie as tarefas de *atualização* para os aplicativos gerenciados para que forneçam prontamente as atualizações para os aplicativos, módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Para garantir atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** quando configurar a agenda de tarefas.

Se sua rede inclui somente dispositivos IPv6 e você deseja atualizar regularmente os aplicativos de segurança instalados neles, certifique-se de que o Servidor de Administração (versão não inferior a 13.2) e o Agente de Rede (versão não inferior a 13.2) estejam instalados nos dispositivos gerenciados.

Por padrão, atualizações para o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Security for Linux são instaladas apenas depois que você modifica o status de atualização para *Aprovado*. É possível alterar as configurações de atualização na tarefa de *atualização*.

Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados.

Instruções de como proceder:

- Console de Administração: A instalação automática do Kaspersky Endpoint Security atualiza em dispositivos
- Kaspersky Security Center Web Console: Instalação automática de atualizações do Kaspersky Endpoint Security em dispositivos

Resultados

Após a conclusão do cenário, o Kaspersky Security Center será configurado para atualizar os bancos de dados da Kaspersky e os aplicativos da Kaspersky instalados após o download das atualizações no repositório do Servidor de Administração ou nos repositórios de pontos de distribuição. Você poderá prosseguir para monitorar o status da rede.

Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky

Para ter certeza de que a proteção dos seus Servidores de Administração e dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações oportunas dos seguintes:

- Bancos de dados e módulos de software da Kaspersky

  Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que os bancos de dados antivírus sejam atualizados e que o nível de segurança seja mantido para os dispositivos gerenciados.

- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

- Ao usar uma única tarefa: *Baixar atualizações no repositório do Servidor de Administração*

  Usando duas tarefas:

  - A tarefa *Baixar atualizações no repositório do Servidor de Administração*
  - A tarefa *Baixar atualizações para os repositórios de pontos de distribuição*

- Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP
- Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados
- Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Usando a tarefa Baixar atualizações no repositório do Servidor de Administração

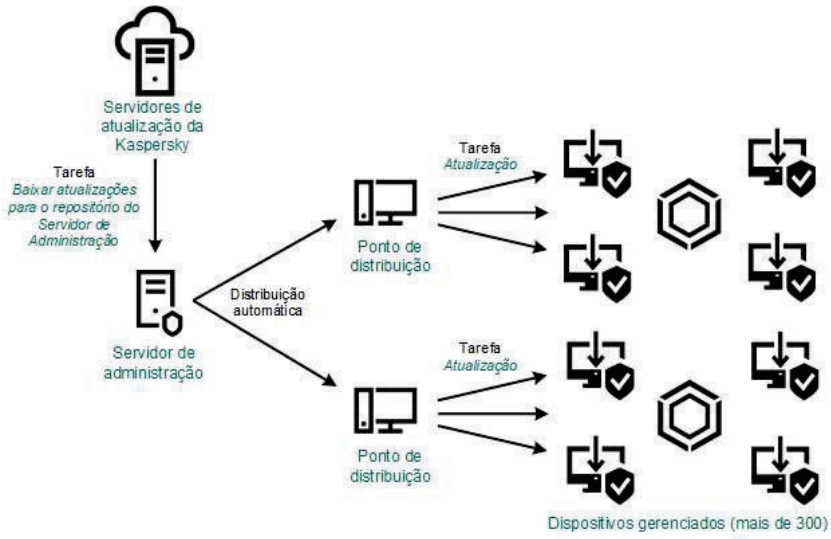
Nesse esquema, o Kaspersky Security Center baixa as atualizações através da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Em redes pequenas que contêm menos de 300 dispositivos gerenciados em um segmento de rede único ou menos de 10 dispositivos gerenciados em cada segmento de rede, as atualizações são distribuídas aos dispositivos gerenciados diretamente do repositório do Servidor de Administração (veja a figura abaixo).

Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração sem pontos de distribuição

Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

Se a rede contiver mais de 300 dispositivos gerenciados em um segmento de rede único ou se a rede consistir vários segmentos de rede com mais de 9 dispositivos gerenciados em cada segmento de rede, recomendamos o uso de pontos de distribuição para propagar as atualizações aos dispositivos gerenciados (veja a figura abaixo). Os pontos de distribuição reduzem a carga no Servidor de Administração e otimizam o tráfego entre o Servidor de Administração e os dispositivos gerenciados. Você pode calcular o número e a configuração de pontos de distribuição necessários para a rede.

Nesse esquema, as atualizações são baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração com pontos de distribuição

Quando a tarefa *Baixar atualizações no repositório do Servidor de Administração* for concluída, as seguintes atualizações serão baixadas no repositório do Servidor de Administração:

- Módulos de software e bancos de dados do Kaspersky para o Kaspersky Security Center

Essas atualizações são instaladas automaticamente.

Módulos de software e bancos de dados da Kaspersky para os aplicativos de segurança nos dispositivos gerenciados

Essas atualizações são instaladas por meio da tarefa de Atualização para o Kaspersky Endpoint Security for Windows.

- Atualizações para o Servidor de Administração

  Essas atualizações não são instaladas automaticamente. O administrador deve explicitamente aprovar e executar a instalação das atualizações.

  É necessário ter direitos de administrador local para a instalação de patches no Servidor de Administração.

  Atualizações dos componentes do Kaspersky Security Center
  Por padrão, essas atualizações são instaladas automaticamente. Você pode alterar as configurações na política do Agente de rede.

- Atualizações dos aplicativos de segurança
  Por padrão, o Kaspersky Endpoint Security for Windows instala apenas as atualizações aprovadas por você. (Você pode aprovar atualizações pelo Console de Administração ou pelo Kaspersky Security Center Web Console). As atualizações são instaladas pela tarefa de *Atualização* e podem ser configuradas nas propriedades desta tarefa.

A tarefa *Baixar atualizações para o repositório do Servidor de Administração* não está disponível nos Servidores de Administração virtuais. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal.

Você pode configurar as atualizações a serem verificadas quanto a operabilidade e erros em um conjunto de dispositivos de teste. Se a verificação for bem-sucedida, as atualizações serão distribuídas para outros dispositivos gerenciados.

Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as que são solicitadas por qualquer aplicativo. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, o Servidor de Administração envia automaticamente as seguintes informações para os servidores de atualização da Kaspersky para assegurar o download das versões relevantes dos bancos de dados e dos módulos de software da Kaspersky:

- ID e versão do aplicativo
- ID de instalação do aplicativo

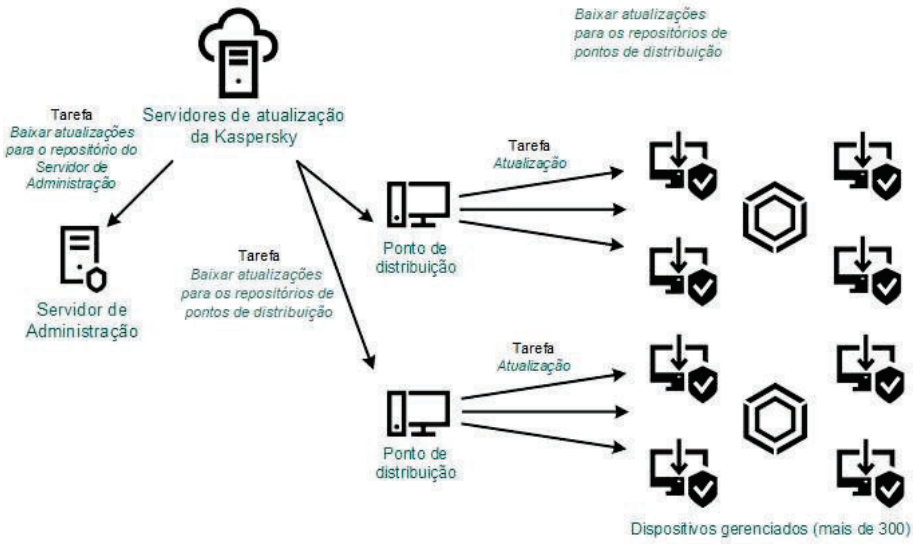
  ID da chave ativa

- ID de execução da tarefa *Baixar atualizações para o repositório do Servidor de Administração*

Nenhuma das informações transmitidas contém informações pessoais ou outros dados confidenciais. A AO Kaspersky Lab protege as informações de acordo com os requisitos estabelecidos por lei.

ando duas tarefas: a tarefa Baixar atualizações no repositório do Servidor de Administração
 tar

Você pode baixar atualizações para os repositórios de pontos de distribuição diretamente dos servidores de atualização Kaspersky em vez de do repositório do Servidor de Administração e distribuir as atualizações para os dispositivos gerenciados (veja a figura abaixo). Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Por padrão, o Servidor de Administração e os pontos de distribuição comunicam-se com Servidores de atualização Kaspersky e baixam de atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração e/ou os pontos de distribuição para usar o protocolo HTTP em vez de HTTPS.

Para implementar esse esquema, crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* além da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Depois disso, os pontos de distribuição baixarão atualizações dos servidores de atualização Kaspersky e não do repositório do Servidor de Administração.

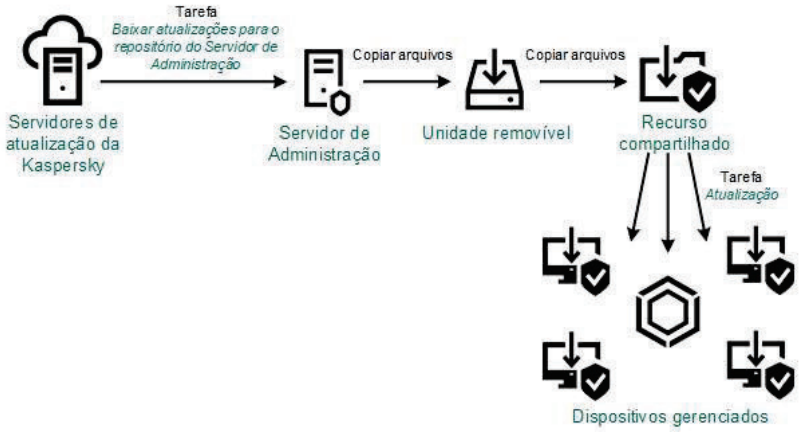
Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* também é necessária para esse esquema, porque essa tarefa é usada para baixar módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center.

Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Se os dispositivos cliente não tiverem uma conexão com o Servidor de Administração, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para atualizar bancos de dados, módulos de software e aplicativos Kaspersky. Nesse esquema, você precisa copiar as atualizações necessárias do repositório do Servidor de Administração para uma unidade removível e depois copiar as atualizações para a pasta local ou o recurso compartilhado especificado como uma fonte de atualização nas configurações do Kaspersky Endpoint Security (veja a figura abaixo).



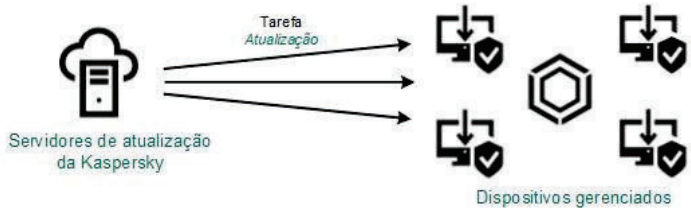
Atualização por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Para obter mais informações sobre fontes de atualizações no Kaspersky Endpoint Security, consulte a seguinte ajuda:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security para receber atualizações diretamente dos servidores de atualização da Kaspersky (veja a figura abaixo).



Atualização de aplicativos de segurança diretamente dos servidores de atualização da Kaspersky

Nesse esquema, o aplicativo de segurança não usa os repositórios fornecidos pelo Kaspersky Security Center. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização na interface do aplicativo de segurança. Para obter mais informações sobre essas configurações, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

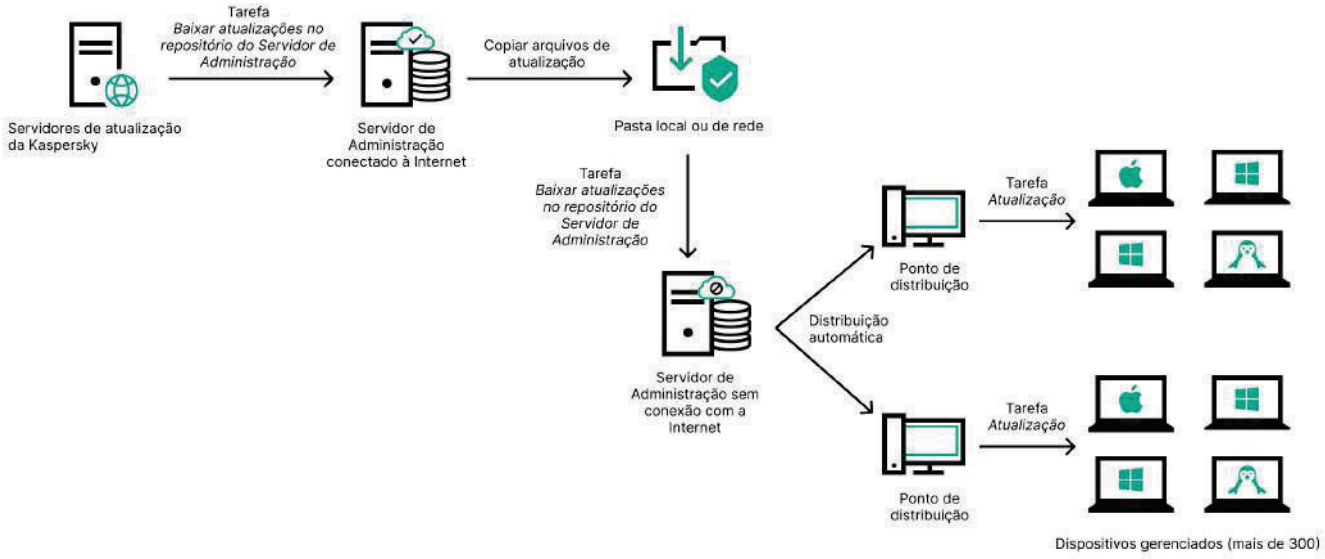
Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Se o Servidor de Administração não tiver conexão com a Internet, você poderá configurar a tarefa *Baixar atualizações no repositório do Servidor de Administração* para baixar atualizações de uma pasta local ou de rede. Nesse caso, você deve copiar os arquivos de atualização necessários para a pasta especificada de tempos em tempos. Por exemplo, você pode copiar os arquivos de atualização necessários de uma das seguintes fontes:

- Servidor de Administração que possui conexão com a Internet (veja a figura abaixo)

  Como um Servidor de Administração baixa apenas as atualizações solicitadas pelos aplicativos de segurança, os conjuntos de aplicativos de segurança gerenciados pelos Servidores de Administração (o que tem conexão com a Internet e o que não tem) devem corresponder.

  Se o Servidor de Administração que você usa para baixar atualizações tiver a versão 13.2 ou anterior, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.



Atualização por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

  Utilitário de atualização da Kaspersky

  Como este utilitário usa o esquema antigo para baixar atualizações, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.

Criação da tarefa baixar atualizações no repositório do Servidor de Administração

A tarefa *Baixar atualizações no repositório do Servidor de Administração* do Servidor de Administração é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. É possível criar apenas uma tarefa de *Baixar atualizações no repositório do Servidor de Administração*. Portanto, é possível criar uma tarefa *Baixar atualizações no repositório do Servidor de Administração* somente se essa tarefa tiver sido removida da lista de tarefas do Servidor de Administração.

Essa tarefa deve baixar atualizações dos servidores de atualização Kaspersky para o repositório do Servidor de Administração. A lista de atualizações inclui:

- Atualizações para bancos de dados e módulos do software do Servidor de Administração

- Atualizações para bancos de dados e módulos do software de aplicativos de segurança Kaspersky

  Atualizações para componentes do Kaspersky Security Center

- Atualizações para aplicativos de segurança Kaspersky

Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

Antes de distribuir as atualizações para os dispositivos gerenciados, é possível executar a tarefa de *Verificação de atualizações*. Isso permite ter a certeza de que o Servidor de Administração instalará as atualizações baixadas corretamente e que um nível de segurança não diminuirá devido às atualizações. Para verificá-las antes de distribuir, configure a opção **Executar verificação de atualizações** nas configurações de tarefas *Baixar atualizações no repositório do Servidor de Administração*.

*Para criar uma tarefa **Baixar atualizações no repositório do Servidor de Administração**:*

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 **Baixar atualizações no repositório do Servidor de Administração**.
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. 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.
6. Clique no botão **Criar**.
   A tarefa é criada e exibida na lista de tarefas.
7. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
8. Na janela de propriedades da tarefa, na guia **Configurações do aplicativo**, especifique as seguintes configurações:

   Fontes de atualizações

Os seguintes recursos podem ser utilizados como uma origem das atualizações do Servidor de Administração:

- Servidores de atualização da Kaspersky

  Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo. Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

  Selecionado por padrão.

  Servidor de Administração Principal

  Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

- Pasta local ou de rede

  Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

  Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

Caso uma pasta compartilhada que contenha atualizações seja protegida por senha, ative a opção **Especificar conta para acesso à pasta compartilhada da fonte de atualização (se houver)** e insira as credenciais da conta necessárias para o acesso.

Pasta para armazenar atualizações

O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

Outras configurações:

- Forçar a atualização de Servidores de Administração secundários

  Se esta opção estiver ativada, o Servidor de Administração inicia as tarefas de atualização nos Servidores de Administração secundários assim que as novas atualizações são baixadas. Caso contrário, as tarefas de atualização nos Servidores de Administração secundários são iniciadas segundo os seus agendamentos.
  Por padrão, esta opção está desativada.

  Copiar as atualizações baixadas em pastas adicionais

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas das sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Por padrão, esta opção está desativada.

Não forçar a atualização de dispositivos e Servidores de Administração secundários a não ser que a cópia tenha sido concluída

As tarefas de download das atualizações nos dispositivos cliente e no Servidor de Administração secundário somente inicia depois das atualizações serem copiadas da pasta principal das atualizações para as pastas de atualização adicionais.

Essa opção deve ser ativada se os de dispositivos cliente e os Servidores de Administração secundários baixam atualizações de pastas adicionais da rede.

Por padrão, esta opção está desativada.

- **Conteúdo das atualizações**:
  - **Baixar arquivos diff**

    Esta opção ativa o recurso de download dos arquivos diff.
    Por padrão, esta opção está desativada.

Baixar atualizações usando o esquema antigo

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13.2 ou versão anterior

  Por exemplo, o Servidor de Administração 1 não possui uma conexão com a Internet. Nesse caso, é possível baixar as atualizações usando o Servidor de Administração 2, desde que ele tenha conexão com a Internet e, em seguida, colocar as atualizações em uma pasta local ou de rede para usá-la como fonte de atualização para o Servidor de Administração 1. Caso o Servidor de Administração 2 tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa para o Servidor de Administração 1.

Por padrão, esta opção está desativada.

- **Executar verificação de atualizações**

O Servidor de Administração baixa as atualizações da fonte, salva-as num repositório temporário e executa a tarefa definida no campo **Tarefa de verificação de atualizações**. Se a tarefa for concluída com êxito, as atualizações serão copiadas do repositório temporário para uma pasta compartilhada no Servidor de Administração e distribuídas a todos os dispositivos para os quais o Servidor de Administração atua como a fonte de atualizações (tarefas com o agendamento de **Quando novas atualizações são baixadas no repositório** forem iniciadas). A tarefa de download de atualizações para o repositório é concluída somente após o término da *Tarefa de verificação de atualizações*.

Por padrão, esta opção está desativada.

9. Na janela de propriedades da tarefa, na guia **Agendamento**, crie uma programação para o início da tarefa. Se necessário, especifique as seguintes configurações:

Início agendado:

Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.
  Por padrão, esta opção está ativada.

A cada N minutos

A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

A cada N horas

A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.
Por padrão, a tarefa é executada a cada seis horas, iniciando na data e hora atuais do sistema.

A cada N dias

A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N semanas**

A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.
Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

Diariamente (não é compatível com horário de verão)

A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

A tarefa é executada regularmente, nos dias da semana e na hora especificados.
Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

A tarefa é executada regularmente, no dia do mês e na hora especificados.
Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

Todos os meses em dias especificados das semanas selecionadas

A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **No surto de vírus**

A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

- Antivírus para estações de trabalho e servidores de arquivo
- Antivírus para defesa de perímetro
- Antivírus para sistemas de correio

Por padrão, todos os tipos de aplicativos estão selecionados.
Você pode precisar executar tarefas diferentes, dependendo do tipo de aplicativo antivírus que informa um ataque de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa de *Verificação de malware*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.
Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas nos dispositivos cliente; para **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas somente são executadas naqueles dispositivos cliente que estiverem visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está ativada.

Usar atraso randomizado automaticamente para início da tarefas

Se esta opção for ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos cliente aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos cliente aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

Parar a tarefa se ela for executada por mais que (min.)

Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

10. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Quando o Servidor de Administração executa a tarefa *Baixar atualizações no repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada do Servidor de Administração. Se você criar esta tarefa para um grupo de administração, ela somente será aplicada aos Agentes de Rede incluídos no grupo de administração especificado.

As atualizações são distribuídas aos dispositivos cliente e aos Servidores de Administração secundários da pasta compartilhada do Servidor de Administração.

Verificação das atualizações baixadas

Antes de instalar as atualizações nos dispositivos gerenciados, é possível verificar primeiro as atualizações sobre operabilidade e erros por meio da tarefa de *Verificação de atualizações*. A tarefa de *Verificação de atualizações* é executada automaticamente como parte da tarefa *Baixar atualizações no repositório do Servidor de Administração*. O Servidor de Administração baixa as atualizações da origem, salva-as no armazenamento temporário e executa a tarefa de *Verificação de atualizações*. Caso a tarefa seja concluída com êxito, as atualizações são copiadas do repositório temporário para a pasta compartilhada do Servidor de Administração. Elas são distribuídas à todos os dispositivos cliente para os quais o Servidor de Administração for a fonte de atualizações.

Caso os resultados da tarefa de *Verificação de atualizações* demostrarem que as atualizações localizadas no repositório temporário estão incorretas ou se a tarefa de *Verificação de atualizações* concluir com erro, as atualizações não serão copiadas para a pasta compartilhada. O Servidor de Administração retém o conjunto anterior de atualizações. Além disso, as tarefas que têm o tipo de agendamento **Quando novas atualizações são baixadas no repositório** não são iniciadas. Essas operações são realizadas no próximo início da tarefa *Baixar atualizações no repositório do Servidor de Administração* se a verificação das novas atualizações for concluída com êxito.

Um conjunto de atualizações é considerado inválido se uma das seguintes condições for atendida em pelo menos um dispositivo de teste:

- Ocorreu um erro na tarefa de atualização.

  O status da proteção em tempo real do aplicativo de segurança foi modificado após a aplicação das atualizações.

- Um objeto infectado foi detectado durante a execução da tarefa de verificação sob demanda.

- Ocorreu um erro de tempo de execução de um aplicativo da Kaspersky.

Caso nenhuma das condições listadas sejam verdadeiras em nenhum dispositivo de teste, o conjunto de atualizações é considerado como válido, e a tarefa de *Verificação de atualizações* será considerada com êxito na conclusão.

Antes de começar a criar a tarefa de *Verificação de atualizações*, execute os pré-requisitos:

1. Criar um grupo de administração com vários dispositivos de teste. Esse grupo será necessário para verificar as atualizações.

   Recomenda-se usar os dispositivos com a proteção mais confiável e com a configuração de aplicativo mais popular na rede. Essa abordagem aumenta a qualidade e a probabilidade de detecção de vírus durante as verificações e minimiza o risco de falsos positivos. Caso sejam detectados vírus nos dispositivos de teste, a tarefa de *Verificação de atualizações* será considerada malsucedida.

2. Crie as tarefas de atualização e verificação de malwares para um aplicativo compatível com o Kaspersky Security Center, por exemplo, Kaspersky Endpoint Security for Windows ou Kaspersky Security for Windows Server. Ao criar as tarefas de atualização e verificação de malwares, especifique o grupo de administração com os dispositivos de teste.

   A tarefa de *verificação de atualizações* executa sequencialmente as tarefas de atualização e verificação de malwares em dispositivos de teste para verificar se todas as atualizações são válidas. Além disso, ao criar a tarefa de *Verificação de atualizações*, será necessário especificar as tarefas de atualização e verificação de malwares.

3. Crie a tarefa *Baixar atualizações no repositório do Servidor de Administração*.

Para que o Kaspersky Security Center verifique as atualizações baixadas antes de distribuí-las para os dispositivos cliente:

No n

2. Clique na tarefa **Baixar atualizações no repositório do Servidor de Administração**.

3. Na janela de propriedades do aplicativo que se abre, acesse a guia **Configurações do aplicativo** e, então, habilite a opção **Executar verificação de atualizações**.

4. Caso a tarefa *Verificação de atualizações* exista, clique no botão **Selecionar tarefa**. Na janela aberta, selecione a tarefa de *Verificação de atualizações* no grupo de administração com dispositivos de teste.

5. Caso não tenha criado a tarefa de *Verificação de atualizações* anteriormente, faça o seguinte:

   a. Clique no botão **Nova tarefa**.

   b. No Assistente para novas tarefas aberto, especifique o nome da tarefa caso queira alterar o nome da predefinição.

   c. Selecione o grupo de administração com os dispositivos de teste criado anteriormente.

   d. Primeiro, selecione a tarefa de atualização de um aplicativo necessário e compatível com o Kaspersky Security Center, em seguida, selecione a tarefa de verificação de malwares.
   Depois disso, as seguintes opções aparecem. Recomendamos deixá-las ativadas:

   Reiniciar o dispositivo após a atualização do banco de dados

   Depois que os bancos de dados antivírus forem atualizados em um dispositivo, recomendamos reinicializar o dispositivo.

   Por padrão, a opção está ativada.

   - Verificar o status de proteção em tempo real após atualização do banco de dados e o reinício do dispositivo

     Caso esta opção esteja habilitada, a tarefa de *Verificação de atualizações* verifica se as atualizações baixadas para o repositório do Servidor de Administração são válidas e se o nível de proteção diminuiu após a atualização do banco de dados antivírus e a reinicialização do dispositivo.

     Por padrão, esta opção está ativada.

   e. Especifique uma conta a partir da qual a tarefa de *Verificação de atualizações* será executada. É possível usar a conta e deixar a opção **Conta padrão** habilitada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

6. Clique em **Salvar** para fechar a janela de propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

A verificação de atualizações automática é ativada. Agora, é possível executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, e ela começará a partir da verificação de atualização.

Criar as atualizações de download para a tarefa dos repositórios dos pontos de distribuição