A tarefa *Download de atualizações nos repositórios de pontos de distribuição* somente funciona em dispositivos de ponto de distribuição que executam o Windows. Os dispositivos do ponto de distribuição executando Linux ou macOS não podem baixar atualizações dos servidores de atualização Kaspersky. Se pelo menos um dispositivo executando Linux ou macOS estiver dentro do escopo da tarefa, a tarefa terá o status *Falhou*. Mesmo se a tarefa for concluída com êxito em todos os dispositivos Windows, ela retornará um erro nos dispositivos restantes.

É possível criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para um grupo de administração. Esta tarefa será executada para pontos de distribuição incluídos no grupo de administração especificado.

Você pode usar esta tarefa, por exemplo, se o tráfego entre o Servidor de Administração e 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.

Esta tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para os repositórios de pontos de distribuição. A lista de atualizações inclui:

- 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.

*Para criar a tarefa **Baixar atualizações para os repositórios de pontos de distribuição**, para um grupo de administração selecionado:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique no botão **Adicionar**.
   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, no campo **Tipo de tarefa**, selecione **Baixar atualizações para os repositórios de pontos de distribuição**.
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. Selecione um botão de opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
6. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. 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 guia **Configurações do aplicativo** da janela de propriedades da tarefa, especifique as seguintes configurações:

- **Fontes de atualizações**

  Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

  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.

  Esta opção está marcada 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.

- **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.

- **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, um ponto de distribuição está configurado para receber as atualizações de uma pasta local ou de rede. Nesse caso, é possível baixar as atualizações usando um Servidor de Administração que tenha uma conexão com a Internet e, em seguida, colocar as atualizações na pasta local no ponto de distribuição. Caso o Servidor de Administração tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa *Baixe atualizações para os repositórios de pontos de distribuição*.

Por padrão, esta opção está desativada.

10. Crie um agendamento 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 retardo aleatório automaticamente para início da tarefa

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.

11. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada, as atualizações para bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada. As atualizações baixadas somente serão usadas por pontos de distribuição que estão incluídos no grupo de administração especificado e que não têm nenhuma tarefa de download de atualização explicitamente definida para eles.

Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

As atualizações e as correções do Servidor de Administração podem ser instaladas apenas manualmente, depois da obtenção da aprovação explícita do administrador.

A instalação automática de atualizações e patches para componentes do Kaspersky Security Center é ativada por padrão durante a instalação do Agente de Rede no dispositivo. Você pode desativá-lo durante a instalação do Agente de Rede ou desativá-lo em outro momento usando uma política.

Para desativar a atualização automática e a correção para componentes do Kaspersky Security Center durante a instalação local do Agente de Rede em um dispositivo:

1. Inicie a instalação local do Agente de Rede no dispositivo.
2. Na etapa **Configurações avançadas**, desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.
3. Siga as instruções do Assistente.

O Agente de Rede com a atualização e correção automática desativada para os componentes do Kaspersky Security Center será instalado no dispositivo. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Para desativar a atualização e a correção automática dos componentes do Kaspersky Security Center durante a instalação do Agente de Rede no dispositivo através de um pacote de instalação:

2. Clique no pacote **Agente de Rede do Kaspersky Security Center <número da versão>**.

3. Na janela de propriedades, abra a guia **Configurações**.

4. Desligue o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.

   O Agente de Rede com a atualização e correção automática desativado para os componentes do Kaspersky Security Center será instalado a partir deste pacote. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Se esta caixa de seleção estiver marcada (ou desmarcada) durante a instalação do Agente de Rede no dispositivo, você pode subsequentemente ativar (ou desativar) a atualização automática usando a política de Agente de Rede.

Para ativar ou desativar a atualização e a correção automática para os componentes do Kaspersky Security Center usando a política de Agente de Rede:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

2. Clique na política do Agente de Rede.

3. Na janela de propriedades da política, abra a guia **Configurações do aplicativo**.

4. Na seção **Gerenciar patches e atualizações**, ative ou desative o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** para ativar ou desativar, respectivamente, a atualização e a aplicação de patches automáticas.

5. Defina o bloqueio (🔒) para este botão de alternância.

   A política será aplicada aos dispositivos selecionados, e a atualização e a correção automática para componentes do Kaspersky Security Center será ativada (ou desativada) nestes dispositivos.

Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows

Você pode configurar as atualizações automáticas dos bancos de dados e módulos de software do Kaspersky Endpoint Security for Windows nos dispositivos cliente.

Para configurar o download e a instalação automática das atualizações do Kaspersky Endpoint Security for Windows nos dispositivos:

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

2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo da Kaspersky Endpoint Security for Windows, selecione **Atualização** como o subtipo de tarefa.

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. Selecione o escopo da tarefa.

6. Especifique o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.

7. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

8. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.

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

10. Na guia **Configurações do aplicativo** da janela de propriedades de tarefa, defina as configurações da tarefa de atualização no modo local ou de dispositivos móveis:

    - **Modo local**: a conexão é estabelecida entre o dispositivo e o Servidor de Administração.

      Modo móvel: nenhuma conexão é estabelecida entre o Kaspersky Security Center e o dispositivo (por exemplo, quando o dispositivo não está conectado à Internet).

11. Ative as fontes de atualização que deseja usar para atualizar bancos de dados e módulos de aplicativo do Kaspersky Endpoint Security for Windows. Se necessário, altere as posições das fontes na lista usando os botões **Para cima** e **Para baixo**. Se várias fontes de atualizações forem ativadas, o Kaspersky Endpoint Security for Windows tentará se conectar a elas uma após a outra, começando pelo topo da lista, e executará a tarefa de atualização recuperando o pacote de atualização da primeira fonte disponível.

12. Ative a opção **Instalar apenas atualizações aprovadas** para baixar e instalar atualizações dos módulos de software junto com bancos de dados do aplicativo.

    Se a opção estiver ativada, o Kaspersky Endpoint Security for Windows notifica o usuário sobre as atualizações dos módulos de software disponíveis e inclui atualizações nos módulos de software no pacote de atualização ao executar a tarefa de atualização. O Kaspersky Endpoint Security for Windows instala somente as atualizações para as quais você definiu o status *Aprovado*; elas serão instaladas localmente por meio da interface do aplicativo ou do Kaspersky Security Center.

    Você também pode ativar a opção **Instalar atualizações críticas do módulo de aplicativo automaticamente**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security for Windows as instala com o status *Crítico*; as atualizações remanescentes serão instaladas após a sua aprovação.

    Se a atualização do módulo de software requerer a revisão e aceitação dos termos do Contrato de Licença e da Política de Privacidade, o aplicativo instala as atualizações após os termos do Contrato de Licença e da Política de Privacidade terem sido aceitos pelo usuário.

13. Marque a caixa de seleção **Copiar atualizações para uma pasta** para que o aplicativo salve as atualizações baixadas em uma pasta e especifique o caminho da pasta.

14. Agende a tarefa. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório**.

15. Clique em **Salvar**.

Ao executar a tarefa de **Atualização**, o aplicativo envia solicitações aos servidores de atualização Kaspersky.

Algumas atualizações necessitam da instalação das versões mais recentes dos plug-ins de gerenciamento.

Aprovar e recusar atualizações de software

As configurações de uma tarefa de instalação de atualização podem necessitar da aprovação de atualizações que devem ser instaladas. Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações nos dispositivos cliente.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Operações** → **Aplicativos Kaspersky** → **Atualizações contínuas**.

   Aparece uma lista das atualizações disponíveis.

   As atualizações de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center. Se esta versão for posterior à versão atual, essas atualizações serão exibidas, mas não poderão ser aprovadas. Além disso, nenhum pacote de instalação pode ser criado a partir dessas atualizações até que você atualize o Kaspersky Security Center. Você receberá uma solicitação para atualizar sua instância do Kaspersky Security Center para a versão mínima necessária.

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 às quais você atribui o status *Aprovado* são colocadas em uma fila para instalação.

As atualizações às quais você atribui o status *Negado* são desinstaladas (se possível) de todos os dispositivos nos quais elas foram anteriormente instaladas. Além disso, elas não serão instaladas em outros dispositivos no futuro.

Algumas atualizações para aplicativos da Kaspersky não podem ser desinstaladas. Se você definir o status *Negado* para elas, o Kaspersky Security Center não desinstalará estas atualizações dos dispositivos nos quais elas foram anteriormente instaladas. No entanto, essas atualizações nunca serão instaladas em outros dispositivos no futuro.

Se você definir o status *Negado* para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver as atualizações, poderá exclui-las de forma manual localmente.

Atualizando o Servidor de Administração

Você pode instalar as atualizações do Servidor de Administração usando o Assistente de atualização do Servidor de Administração.

Para instalar uma atualização do Servidor de Administração:

1. No menu principal, vá para **Operações** → **Aplicativos Kaspersky** → **Atualizações contínuas**.
2. Execute o Assistente de atualização do Servidor de Administração de uma das seguintes maneiras:
   - Clique no nome de uma atualização do Servidor de Administração na lista de atualizações e, na janela que é aberta, clique no link **Executar o assistente de atualização do Servidor de Administração**.
   - Clique no link **Executar o assistente de atualização do Servidor de Administração** no campo de notificação na parte superior da janela.
3. Na janela Assistente de atualização do Servidor de Administração, selecione uma das seguintes opções para especificar quando instalar uma atualização:

   Instalar agora. Selecione esta opção se deseja instalar a atualização agora.
   - **Adiar instalação**. Selecione esta opção se deseja instalar a opção mais tarde. Nesse caso, uma notificação sobre esta atualização será exibida.
   - **Ignorar atualização**. Selecione esta opção se não deseja instalar uma atualização e não deseja receber notificações sobre esta atualização.
4. Selecione a opção **Criar cópia backup do Servidor de Administração antes da instalação da atualização** se deseja criar um backup do Servidor de Administração antes de instalar a atualização.
5. Clique no botão **OK** para encerrar o Assistente.

Se um processo de backup é interrompido, o processo de instalação da atualização também é interrompido.

Ativar e desativar o modelo offline de download da atualização

Recomendamos que você evite desativar o modelo offline de download da atualização. Sua desativação pode causar falhas na entrega da atualização aos dispositivos. Em determinados casos, o especialista de Suporte Técnico da Kaspersky pode recomendar que você desabilite a opção **Baixar atualizações e bancos de dados de antivírus do Servidor de Administração com antecedência**. Então, você terá que assegurar-se de que a tarefa para receber atualizações para aplicativos Kaspersky foi configurada.

Para ativar ou desativar o modelo offline de download da atualização para um grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Cliq[illegible] em **Grupos**

3. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você precisa ativar o modelo off-line para o download das atualizações.
4. Clique na política do Agente de Rede.

   A janela de propriedades da política do Agente de Rede se abre.

   Por padrão, as configurações de políticas secundárias são herdadas das políticas principais e não podem ser modificadas. Se a política que você deseja modificar for herdada, primeiro será necessário criar uma nova política para o Agente de Rede no grupo de administração necessário. Na política recém-criada, você pode modificar as configurações que não estão bloqueadas na política principal.

5. Na guia **Configurações do aplicativo**, selecione a seção **Gerenciar patches e atualizações**.
6. Ative ou desative a opção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** para ativar ou desativar, respectivamente, o modelo offline de download da atualização.

   Por padrão, o modelo offline para download das atualizações está ativado.

O modelo offline de download da atualização será ativado ou desativado.

Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline

A atualização dos bancos de dados e dos módulos de software da Kaspersky em dispositivos gerenciados é uma tarefa importante para manter a proteção dos dispositivos contra vírus e outras ameaças. Os administradores normalmente configuram atualizações regulares por meio do uso do repositório do Servidor de Administração ou repositórios de pontos de distribuição.

Quando for preciso atualizar bancos de dados e módulos do software em um dispositivo (ou um grupo de dispositivos) que não está conectado ao Servidor de Administração (principal ou secundário), a um ponto de distribuição ou à Internet, você terá de usar fontes alternativas de atualizações, como um servidor FTP ou uma pasta local. Nesse caso, você precisa entregar os arquivos das atualizações necessárias usando um dispositivo de armazenamento em massa, como um pen drive ou um disco rígido externo.

Você pode copiar as atualizações necessárias de:

- O Servidor de Administração.

  Para ter certeza de que o repositório do Servidor de Administração contém as atualizações necessárias para o aplicativo de segurança instalado em um dispositivo offline, pelo menos um dos dispositivos online gerenciados deve ter o mesmo aplicativo de segurança instalado. Esse aplicativo deve ser configurado para receber as atualizações do repositório do Servidor de administração através da tarefa Baixar atualizações no repositório do Servidor de Administração.

  Qualquer dispositivo que tem o mesmo aplicativo de segurança instalado e configurado para receber as atualizações do repositório do Servidor de Administração, um repositório de ponto de distribuição ou diretamente dos servidores de atualização Kaspersky.

Abaixo há um exemplo de configuração de atualizações de bancos de dados e módulos de software copiando-os do repositório do Servidor de Administração.

1. Conecte a unidade removível ao dispositivo onde o Servidor de Administração está instalado.

2. Copie os arquivos de atualizações para a unidade removível.
   Por padrão, as atualizações estão localizadas em: \\<nome do servidor>\KLSHARE\Updates.

   Como alternativa, você pode configurar o Kaspersky Security Center para copiar regularmente as atualizações para a pasta selecionada. Para isso, use a opção **Copiar as atualizações baixadas em pastas adicionais** nas propriedades da tarefa Baixar atualizações no repositório do Servidor de Administração. Se você especificar uma pasta localizada em um pendrive ou um disco rígido externo como uma pasta de destino dessa opção, esse dispositivo de armazenamento em massa sempre conterá a versão mais recente das atualizações.

3. Em dispositivos offline, configure o aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows) para receber atualizações de uma pasta local ou um recurso compartilhado, como um Servidor FTP ou uma pasta compartilhada.

4. Copie os arquivos de atualizações da unidade removível para a pasta local ou o recurso compartilhado que deseja usar como uma fonte de atualização.

5. No dispositivo offline que requer a instalação de atualização, inicie a tarefa de atualização do Kaspersky Endpoint Security for Windows.

Depois que a tarefa de atualização for concluída, os bancos de dados e os módulos de software da Kaspersky serão atualizados no dispositivo.

Fazendo backup e restaurando plug-ins da web

O Kaspersky Security Center Web Console permite fazer backup do estado atual de um plug-in da web para poder restaurar o estado salvo posteriormente. Por exemplo, é possível fazer backup de um plug-in da web antes de atualizá-lo para uma versão mais recente. Após a atualização, caso a versão mais recente não atenda aos requisitos ou expectativas, será possível restaurar a versão anterior do plug-in da web a partir do backup.

Para fazer backup de plug-ins da web:

1. No menu principal, vá para **Configurações do console** → **Plug-ins da web**.
   A janela **Configurações do console** se abre.

2. Na guia **Plug-ins da web**, selecione os plug-ins da web que deseja fazer backup e clique no botão **Criar cópia backup**.

Os plug-ins da web selecionados são submetidos a backup. É possível visualizar os backups criados na aba **Backups**.

Para restaurar um plug-in da web a partir de um backup:

1. No menu principal, vá para **Configurações do console** → **Backups**.

   A janela **Configurações do console** se abre.

2. Na guia **Backups**, selecione o backup do plug-in da web que deseja restaurar e clique no botão **Restaurar do backup**.

O plug-in da web é restaurado a partir do backup selecionado.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center executa as seguintes funções:

Define o escopo das políticas

Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*. Neste caso, defina o escopo das políticas com tags, localizações de dispositivos nas unidades organizacionais do Active Directory ou associação nos grupos de segurança do Active Directory.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do esquema da organização e da topologia da rede, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

Escritório único

- Múltiplos pequenos escritórios remotos

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Configuração padrão de pontos de distribuição: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.

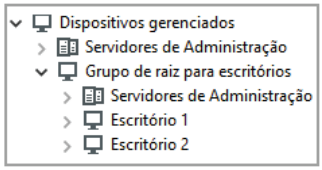
- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Nesse caso, é necessário desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos

na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Sobre os pontos de distribuição atribuídos

É possível atribuir um dispositivo gerenciado como um ponto de distribuição manualmente ou automaticamente.

Caso um dispositivo gerenciado como um ponto de distribuição seja atribuído manualmente, será possível selecionar qualquer dispositivo na rede.

Caso os pontos de distribuição sejam atribuídos automaticamente, o Kaspersky Security Center poderá selecionar apenas o dispositivo gerenciado que atenda às seguintes condições:

- O dispositivo tem ao menos 50 GB de espaço livre no disco.

  O dispositivo gerenciado é conectado diretamente ao Kaspersky Security Center (não pelo gateway).

- O dispositivo gerenciado não é um laptop.

> Caso a rede não tenha dispositivos que atendam às condições especificadas, o Kaspersky Security Center não atribuirá nenhum dispositivo como ponto de distribuição automaticamente.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Para atribuir os pontos de distribuição automaticamente:

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 **Pontos de distribuição**.
3. Selecione a opção **Atribuir automaticamente os pontos de distribuição**.

> Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

4. Clique no botão **Salvar**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Atribuir os pontos de distribuição manualmente

O Kaspersky Security Center permite que você atribua dispositivos manualmente para agirem como pontos de distribuição.

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos. No entanto, se você tiver de optar por não atribuir pontos de distribuição automaticamente por algum motivo (por exemplo, se você quiser usar servidores exclusivamente atribuídos), poderá atribuir manualmente os pontos de distribuição após calcular seu número e configuração.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Para atribuir manualmente os dispositivos para agir como ponto de distribuição:

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 **Pontos de distribuição**.

3. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

4. Clique no botão **Atribuir**.

5. Selecione o dispositivo que você quer atribuir como ponto de distribuição.
   Ao selecionar um dispositivo, tenha em mente os recursos da operação de pontos de distribuição e os requisitos definidos para o dispositivo que age como ponto de distribuição.

6. Selecione o grupo de administração que você quer incluir no escopo do ponto de distribuição selecionado.

7. Clique no botão **OK**.

   O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

8. Clique no ponto de distribuição recém-adicionado na lista para abrir sua janela de propriedades.

9. Configure o ponto de distribuição na janela de propriedades:

   - A seção **Geral** contém a configuração de interação entre o ponto de distribuição e os dispositivos clientes:

     Porta SSL

     O número da porta SSL para a conexão criptografada entre dispositivos cliente e o ponto de distribuição usando SSL.
     Por padrão, a porta 13000 é usada.

     - **Usar multicast**

       Se esta opção estiver ativada, o IP multicasting será usado para distribuição automática de pacotes de instalação para dispositivos cliente dentro do grupo.

       O multicast de IP diminui o tempo necessário para instalar um aplicativo de um pacote de instalação em um grupo de dispositivos cliente, mas aumenta o tempo de instalação quando você instala um aplicativo em um único dispositivo cliente.

     - **Endereço IP multicast**

       O endereço IP que será usado para multicasting. Você pode definir um endereço IP no conjunto de 224.0.0.0 – 239.255.255.255

       Por padrão, o Kaspersky Security Center atribui automaticamente um endereço IP multicast exclusivo dentro do conjunto especificado.

     - **Número da porta de IP multicast**

Número da porta para multicasting de IP.

Por padrão, o número de porta é 15001. Se o dispositivo com o Servidor de Administração instalado for especificado como o ponto de distribuição, por padrão a porta 13001 é usada para conexão SSL.

- **Endereço do ponto de distribuição para dispositivos remotos**

  O endereço IPv4 por meio do qual os dispositivos remotos estabelecem conexão com o ponto de distribuição.

- **Implementar atualizações**

  As atualizações são distribuídas para dispositivos gerenciados a partir das seguintes fontes:

  - Este ponto de distribuição, caso esta opção esteja ativada.
  - Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

  Caso utilize os pontos de distribuição para implantar atualizações, será possível economizar tráfego, pois o número de downloads será reduzido. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

  Caso essa opção seja desativada, o número de downloads de atualização e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Implementar pacotes de instalação**

  Os pacotes de instalação são distribuídos para dispositivos gerenciados a partir das seguintes fontes:

  - Este ponto de distribuição, caso esta opção esteja ativada.
  - Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

  Se você usar pontos de distribuição para implementar pacotes de instalação, poderá economizar tráfego porque reduz o número de downloads. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

  Caso essa opção seja desativada, o número de downloads de pacotes de instalação e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Executar servidor push**

  No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

- **Porta do servidor push**

  O número da porta para o servidor push. É possível especificar o número de qualquer porta livre.

- Na seção **Escopo**, especifique o escopo ao qual o ponto de distribuição distribuirá as atualizações (grupos de administração e/ou um local de rede).

  Somente os dispositivos sendo executados no sistema operacional Windows podem determinar a sua localização na rede. A localização da rede não pode ser determinada para dispositivos que executam outros sistemas operacionais.

- Caso o ponto de distribuição funcione em uma máquina diferente do Servidor de Administração, na seção **Fonte de atualizações**, é possível selecionar uma fonte de atualizações para o ponto de distribuição:

  - **Fonte de atualizações**

    Selecione uma fonte de atualizações para o ponto de distribuição:

    - Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.

      Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:

      - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.
      - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

  - **Baixar arquivos diff**

    Esta opção ativa o recurso de download dos arquivos diff.

    Por padrão, esta opção está ativada.

Na subseção **Configurações de conexão com a Internet**, você pode especificar as configurações de acesso à Internet:

- **Usar o servidor proxy**

  Se esta caixa de seleção estiver selecionada, você pode configurar nos campos de entrada a conexão ao servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

- **Endereço do servidor proxy**

  Endereço do servidor proxy.

- **Número da porta**

O número da porta que é usada para conexão.

- **Ignorar servidor proxy para endereços locais**

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.
  Por padrão, esta caixa de seleção está desmarcada.

  Nome do usuário

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida.

  Senha

  Senha da conta sob a qual a tarefa será executada.

- Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações do KSN a partir dos dispositivos gerenciados:

  Ativar Proxy KSN no lado do ponto de distribuição

  O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.
  O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração sobre coleta de dados do KSN, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.
  Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito se as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estiverem ativadas na janela de propriedades do Servidor de Administração.
  É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- **Encaminhar solicitações da KSN para o Servidor de Administração**

  O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

  Por padrão, esta opção está ativada.

- **Acessar a KSN Cloud/KSN Privada diretamente pela internet**

O ponto de distribuição encaminha solicitações à KSN dos dispositivos gerenciados para a KSN Cloud ou KSN Privada. As solicitações KSN geradas no próprio ponto de distribuição também são enviadas diretamente à KSN Cloud ou à KSN Privada.

Os pontos de distribuição com o Agente de Rede versão 11 (ou anterior) instalado não podem acessar diretamente a KSN Privada. Se você deseja reconfigurar os pontos de distribuição para enviar solicitações à KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição.

Os pontos de distribuição com o Agente de Rede versão 12 (ou posterior) instalado podem acessar diretamente a KSN Privada.

- Ignorar configurações do Servidor Proxy ao conectar à KSN Privada

  Ative esta opção, se tiver as configurações do servidor proxy definidas nas propriedades do ponto de distribuição ou na política do Agente de Rede, mas sua arquitetura de rede requer o uso direto da KSN Privada. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

  Esta alternativa estará disponível caso a opção **Acessar a KSN Cloud/KSN Privada diretamente pela internet** seja selecionada.

- Porta

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

  Usar porta UDP

  Se você desejar que os dispositivos gerenciados sejam conectados ao proxy da KSN através de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de Porta UDP. Por padrão, esta opção está ativada.

- Porta UDP

  O número da porta UDP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. A porta UDP padrão para se conectar ao servidor proxy KSN é 15111.

Caso o ponto de distribuição funcione em uma máquina diferente do Servidor de Administração, na seção **Gateway de conexão**, será possível configurar o ponto de distribuição para atuar como um gateway para conexão entre as instâncias do Agente de Rede e o Servidor de Administração:

- Gateway de conexão

  Caso uma conexão direta entre o Servidor de Administração e os Agentes de Rede não possa ser estabelecida em função da organização de sua rede, será possível usar o ponto de distribuição para atuar como o gateway de conexão entre o Servidor de Administração e os Agentes de Rede.

  Ative essa opção caso você precise que o ponto de distribuição atue como um gateway de conexão entre os Agentes de Rede e o Servidor de Administração. Por padrão, esta opção está desativada.

  Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)

Caso o Servidor de Administração esteja localizado fora da zona desmilitarizada (DMZ), na rede local, os Agentes de Rede instalados em dispositivos remotos não poderão se conectar com o Servidor de Administração. É possível usar um ponto de distribuição como o gateway de conexão com conectividade reversa (o Servidor de Administração estabelece uma conexão com o ponto de distribuição).

Ative essa opção caso seja necessário conectar o Servidor de Administração ao gateway de conexão na DMZ.

- **Abrir porta local do Kaspersky Security Center 14 Web Console**

  Ative essa opção caso seja necessário que o gateway de conexão na DMZ abra uma porta para o Web Console que esteja na DMZ ou na Internet. Especifique o número da porta que será usada para conexão do Web Console com o ponto de distribuição. O número da porta padrão é 13299.
  Essa opção estará disponível caso a opção **Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)** seja ativada.

- **Abrir porta para dispositivos móveis (apenas autenticação SSL do Servidor de Administração)**

  Ative essa opção caso seja necessário que o gateway de conexão abra uma porta para dispositivos móveis e especifique o número da porta que os dispositivos móveis usarão para estabelecer conexão com o ponto de distribuição. O número da porta padrão é 13292. Ao estabelecer a conexão, somente o Servidor de Administração será autenticado.

- **Abrir porta para dispositivos móveis (autenticação SSL bidirecional)**

  Ative essa opção caso seja necessário que o gateway de conexão abra uma porta que será usada para autenticação bidirecional do Servidor de Administração e dispositivos móveis. Especifique os seguintes parâmetros:

  - Número da porta que os dispositivos móveis usarão para conexão com o ponto de distribuição. O número da porta padrão é 13293.

    Nomes de domínio DNS do gateway de conexão que serão usados por dispositivos móveis. Separe os nomes de domínio com vírgulas. Os nomes de domínio especificados serão incluídos no certificado do ponto de distribuição. Caso os nomes de domínio usados pelos dispositivos móveis não correspondam ao nome comum no certificado do ponto de distribuição, os dispositivos móveis não se conectarão com ponto de distribuição.

    O nome de domínio DNS padrão é o nome FQDN do gateway de conexão.

- Configure a amostragem de domínios do Windows, Active Directory e faixas IP pelo ponto de distribuição:

  - **Domínios do Windows**

    Você pode ativar a descoberta de dispositivos para domínios do Windows e definir o agendamento para a localização.

  - **Active Directory**

Você pode ativar a sondagem da rede para o Active Directory e definir o agendamento da sondagem.

Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

- **Sondar o domínio atual do Active Directory**.
- **Sondar a floresta de domínios do Active Directory**.
- **Criar sondagem apenas de domínios selecionados do Active Directory**. Se você selecionar esta opção, adicione um ou mais domínios do Active Directory à lista.

Se você usar um ponto de distribuição do Linux com o Agente de Rede versão 15 instalado, poderá sondar somente domínios do Active Directory para os quais o endereço e as credenciais do usuário foram especificados. A sondagem do domínio atual do Active Directory e da floresta de domínios do Active Directory não está disponível.

- Intervalos de IP

Você pode ativar a descoberta de dispositivos para conjuntos IPv4 e redes IPv6.

Ao ativar a opção **Ativar sondagem de conjuntos**, você poderá adicionar conjuntos verificados e definir seu agendamento. Você pode adicionar conjuntos de IPs à lista de conjuntos verificados.

Ao ativar a opção **Usar Zeroconf para sondar redes IPv6**, o ponto de distribuição sonda automaticamente a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Nesse caso, os conjuntos IP especificados são ignorados, pois o ponto de distribuição sonda toda a rede. A opção **Usar Zeroconf para sondar redes IPv6** estará disponível caso o ponto de distribuição execute Linux. Para usar a sondagem do Zeroconf IPv6, é necessário instalar o utilitário avahi-browse no ponto de distribuição.

- Na seção **Avançado**, especifique a pasta que o ponto de distribuição deve usar para armazenar os dados distribuídos:
  - Usar pasta padrão

Se você selecionar esta opção, o aplicativo usa a pasta de Instalação do Agente de Rede no ponto de distribuição.

  - Usar pasta especificada

Se selecionar esta opção, você pode, no campo abaixo, especificar o caminho até a pasta. Pode ser uma pasta local no ponto de distribuição ou pode ser uma pasta em qualquer dispositivo na rede corporativa.
A conta do usuário usada no ponto de distribuição para executar o Agente de Rede deve ter acesso de leitura/gravação à pasta especificada.

10. Clique no botão **OK**.

Os dispositivos selecionados agirão como pontos de distribuição.

odificar a lista de pontos de distribuição para um grupo de administração

Você pode visualizar a lista de pontos de distribuição atribuídos a um grupo de administração específico e modificá-la adicionando ou removendo pontos de distribuição.

Para visualizar e modificar a lista de pontos de distribuição atribuídos a um grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. No campo **Caminho atual**, acima da lista de dispositivos gerenciados, clique no link do caminho.
3. No painel aberto à esquerda, selecione o grupo de administração para o qual deseja visualizar os pontos de distribuição atribuídos.
   Isso ativa o item de menu **Pontos de distribuição**.
4. No menu principal, vá para **Dispositivos** → **Pontos de distribuição**.
5. Para adicionar novos pontos de distribuição para o grupo de administração, clique no botão **Atribuir** acima da lista de dispositivos gerenciados e selecione os dispositivos no painel que se abre.
6. Para remover os pontos de distribuição atribuídos, selecione os dispositivos na lista e clique no botão **Desatribuir**.

Dependendo das suas modificações, os novos pontos de distribuição serão adicionados à lista ou os pontos de distribuição existentes serão removidos da lista.

Sincronização forçada

Embora o Kaspersky Security Center sincronize automaticamente status, configurações, tarefas e políticas dos dispositivos gerenciados, em alguns casos você pode querer forçar a sincronização para um dispositivo especificado. Você pode executar a sincronização forçada para os seguintes dispositivos:

- Dispositivos com Agente de Rede instalado

  Dispositivos executando o KasperskyOS
  Antes de executar a sincronização forçada para um dispositivo KasperskyOS, certifique-se de que o dispositivo está incluído em um escopo de ponto de distribuição e que um servidor push está ativado no ponto de distribuição.

- Dispositivos iOS

  Dispositivos Android
  Antes de executar a sincronização forçada para um dispositivo Android, você deve configurar o Google Firebase Cloud Messaging.

Sincronizar um único dispositivo

Para forçar a sincronização entre o Servidor de Administração e um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

Uma

3. Clique no botão **Forçar a sincronização**.

O aplicativo sincroniza o dispositivo selecionado com o Servidor de Administração.

Sincronizar vários dispositivos

Para forçar a sincronização entre o Servidor de Administração e vários dispositivos gerenciados:

1. Abra a lista de dispositivos de um grupo de administração ou uma seleção de dispositivos:
   - No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**, clique no link do caminho no campo **Caminho atual** acima da lista de dispositivos gerenciados e, a seguir, selecione o grupo de administração que contém os dispositivos a serem sincronizados.
   - Execute uma seleção de dispositivos para visualizar a lista de dispositivos.
2. Marque as caixas de seleção ao lado dos dispositivos que deseja sincronizar com o Servidor de Administração.
3. Acima da lista de dispositivos gerenciados, clique no botão de reticências (...) e, a seguir, clique no botão **Forçar a sincronização**.

   O aplicativo sincroniza os dispositivos selecionados com o Servidor de Administração.
4. Na lista de dispositivos, verifique se a hora da última conexão com o Servidor de Administração foi alterada para os dispositivos selecionados para a hora atual. Se a hora não tiver sido alterada, atualize o conteúdo da página clicando no botão **Atualizar**.

Os dispositivos selecionados são sincronizados com o Servidor de Administração.

Visualização da hora da entrega de uma política

Após alterar uma política de um aplicativo da Kaspersky no Servidor de Administração, o administrador pode verificar se a política alterada foi entregue a um dispositivo gerenciado específico. Uma política pode ser entregue durante uma sincronização normal ou uma sincronização forçada.

Para visualizar a data e a hora que uma política de aplicativo foi fornecida a um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.
   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Selecione a guia **Aplicativos**.
4. Selecione o aplicativo do qual do qual deseja visualizar a data de sincronização da política.
   A janela de política do aplicativo é exibida com a seção **Geral** selecionada e a data e a hora de entrega da política exibidas.

Ativando um servidor push

No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

É possível querer usar pontos de distribuição como servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. A conectividade contínua é necessária para algumas operações, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Caso um ponto de distribuição seja usado como servidor push, não será necessário usar a opção **Não desconecte do Servidor de Administração** nos dispositivos gerenciados ou enviar pacotes para a porta UDP do agente de rede.

Um servidor push suporta a carga de até 50.000 conexões simultâneas.

Para ativar o servidor push em um ponto de distribuição:

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 **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição no qual deseja ativar o servidor push.
   A janela Propriedades do ponto de distribuição é aberta.

4. Na seção **Geral**, selecione a opção **Executar servidor push**.

5. No campo **Porta do servidor push**, digite o número da porta. Você pode especificar o número de qualquer porta livre.

6. No campo **Endereço para hosts remotos**, especifique o endereço IP ou o nome do dispositivo do ponto de distribuição.

7. Clique no botão **OK**.

O servidor push é ativado no ponto de distribuição selecionado.

Gerenciar aplicativos de terceiros em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao gerenciamento de aplicativos de terceiros instalados nos dispositivos cliente.

Sobre aplicativos de terceiros

O Kaspersky Security Center pode ajudar a atualizar o software de terceiros, instalado em dispositivos clientes, e corrigir as vulnerabilidades do software de terceiros. O Kaspersky Security Center pode atualizar o software de terceiros apenas da versão atual para a versão mais recente. A lista a seguir representa o software de terceiros que você pode atualizar com o Kaspersky Security Center:

A lista de softwares de terceiros pode ser atualizada e ampliada com novos aplicativos. Você pode verificar se é possível atualizar o software de terceiros (instalado nos dispositivos dos usuários) com o Kaspersky Security Center ao visualizar a lista de atualizações disponíveis no Kaspersky Security Center Web Console.

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC

    Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander

  Apache Software Foundation: Apache Tomcat
- Apple:

    Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory

  Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA

  Cisco: Cisco Jabber
- Code Sector: TeraCopy
- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full

    K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard

- DbVis Software AB: DbVisualizer

Decho Corp.:

- Mozy Enterprise

Mozy Home

- Mozy Pro

- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS

Dropbox, Inc.: Dropbox

- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler

EverNote: EverNote

- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager: FAR Manager

FastStone Soft: FastStone Image Viewer

- FileZilla Project: FileZilla
- Firebird Developers: Firebird
- Foxit Corporation:
  - Foxit Reader

Foxit Reader Enterprise

- Free Download Manager.ORG: Free Download Manager

GIMP project: GIMP

- GlavSoft LLC.: TightVNC

  GNU Project: Gpg4win

- Google:

  Google Earth

  - Google Chrome

  - Google Chrome Enterprise

  - Google Earth Pro

- Inkscape Project: Inkscape

  IrfanView: IrfanView

- iterate GmbH: Cyberduck

- Logitech: SetPoint

- LogMeIn, Inc.:

  - LogMeIn

    Hamachi

  - LogMeIn Rescue Technician Console

  Martin Prikryl: WinSCP

- Mozilla Foundation:

  - Mozilla Firefox

  - Mozilla Firefox ESR

  - Mozilla SeaMonkey

    Mozilla Thunderbird

- New Cloud Technologies Ltd: MyOffice Standard. Home Edition

- OpenOffice.org: OpenOffice

- Opera Software: Opera

- Oracle Corporation:

  Oracle Java JRE

  - Oracle VirtualBox

  PDF44: PDF24 MSI/EXE

- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (completo/mínimo)
- Simon Tatham: PuTTY
- Skype Technologies: Skype para Windows
- Sober Lemur S.a.s:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer
- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:

- Git for Windows

  Git LFS

- The Pidgin developer community: Pidgin

  TortoiseSVN Developers: TortoiseSVN

- VideoLAN: VLC media player

- VMware:

  - VMware Player

  - VMware Workstation

  WinRAR Developers: WinRAR

- WinZip: WinZip

- Wireshark Foundation: Wireshark

- Wrike: Wrike

- Zimbra: Zimbra Desktop

Instalar atualizações de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center relacionados à instalação de atualizações para aplicativos de terceiros instalados nos dispositivos cliente.

Cenário: Atualizando software de terceiros

Esta seção fornece um cenário para a atualização software de terceiros instalados nos dispositivos cliente.

Software de terceiros incluem aplicativos da Microsoft e de outros fornecedores de software. As atualizações para aplicativos Microsoft são fornecidas pelo serviço Windows Update.

Pré-requisitos

O Servidor de Administração deve ter uma conexão com a Internet para instalar atualizações de software de terceiros que não sejam software Microsoft.

Por padrão, a conexão com a Internet não é necessária para que o Servidor de Administração instale atualizações de software da Microsoft nos dispositivos gerenciados. Por exemplo, os dispositivos gerenciados podem baixar as atualizações de software da Microsoft diretamente dos servidores de Atualizações da Microsoft ou do Windows Server com o Microsoft Windows Server Update Services (WSUS) implementado na rede da sua organização. O Servidor de Administração deve estar conectado à Internet quando você usa o Servidor de Administração como servidor WSUS.