2. No instalador do Servidor de Administração, especifique as contas de domínio que foram criadas para os serviços.

Selecionar um DBMS

Ao selecionar um sistema de gerenciamento de banco de dados (DBMS) a ser usado por um Servidor de Administração, você deve levar em conta o número de dispositivos cobertos por um Servidor de Administração.

A tabela a seguir lista as opções válidas de DBMS, assim como as recomendações e restrições quanto ao seu uso.

Recomendações e restrições no DBMS

DBMS	Recomendações e restrições
SQL Server Express Edition 2012 ou posterior	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Você pode limitar o número máximo de eventos no repositório de eventos para evitar a sobrecarga do banco de dados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados. O uso do componente Controle de Aplicativos não é recomendado. O uso simultâneo do SQL Server Express Edition DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido. O banco de dados Microsoft SQL Express não é compatível com a tarefa **Executar a sincronização com o Windows Update**.
Edição local do SQL Server, que não seja a Express, 2014 ou posterior	Nenhuma limitação.
Edição remota do SQL Server, que não seja a Express, 2014 ou posterior	Válido somente se ambos os dispositivos estiverem no mesmo domínio do Windows®; se os domínios forem diferentes, uma relação de confiança bidirecional deve ser estabelecida entre eles.
MySQL 5.5, 5.6 ou 5.7 local ou remoto (as versões 5.5.1, 5.5.2, 5.5.3, 5.5.4 e 5.5.5 do MySQL não têm mais suporte)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
MySQL 8.0.20 remoto ou local, e versões posteriores	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
MariaDB local ou remoto (visualizar as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos.

	Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
PostgreSQL, Postgres Pro (ver versões compatíveis)	Use um desses DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.

Se estiver usando o SQL Server 2019 como um DBMS e não tiver o patch cumulativo CU12 ou posterior, será necessário fazer o seguinte após instalar o Kaspersky Security Center:

1. Conecte-se ao SQL Server usando o SQL Management Studio.
2. Execute os seguintes comandos (se escolher um nome diferente para o banco de dados, use esse nome em vez do KAV):

```
USE KAV

GO

ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF

GO
```

3. Reinicie o serviço SQL Server 2019.

Caso contrário, usando Servidor SQL 2019 pode resultar em erros com "Há memória de sistema suficientes no pool de recursos 'internos' para executar esta consulta."

Especificar o endereço do Servidor de Administração

Ao instalar o Servidor de Administração, você deve especificar o endereço externo do Servidor de Administração. Este endereço será usado como o endereço padrão ao criar pacotes de instalação do Agente de Rede. Após isso, você será capaz de modificar o endereço do host do Servidor de Administração usando as ferramentas do Console de Administração; o endereço não se modificará automaticamente em pacotes de instalação do Agente de Rede que já tiverem sido criados.

Configurar a proteção em uma rede da organização cliente

Após a instalação de Servidor de Administração ter sido concluída, o Console de Administração é iniciado e lhe solicita executar a configuração inicial através do Assistente relevante. Quando o Assistente de início rápido estiver em execução, as seguintes políticas e as tarefas são criadas no grupo de administração raiz:

- Política do Kaspersky Endpoint Security

  Tarefa de grupo para atualizar o Kaspersky Endpoint Security
- Tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

Política de Agente de Rede

- Tarefa de verificação de vulnerabilidades (tarefa do Agente de Rede)

  Tarefa de instalação de atualizações e correção de vulnerabilidades (tarefa do Agente de Rede)

As políticas e tarefas são criadas com as configurações padrão, que podem resultar em sub-ótimas ou até inadmissíveis para a organização. Portanto, você deve verificar as propriedades dos objetos que foram criados e os modificá-las manualmente, se necessário.

Esta seção contém informações sobre a configuração manual de políticas, tarefas e outras configurações do Servidor de Administração, e as informações sobre o ponto de distribuição, criando uma estrutura de grupo de administração e a hierarquia de tarefas e outras configurações.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security, que é criada pelo Assistente de início rápido. Você pode executar a configuração na janela de propriedades da política.

Ao editar uma configuração, tenha em mente que você deve clicar no ícone de fechadura acima da configuração relevante para permitir usar o seu valor em uma estação de trabalho.

Configurar a política na seção Proteção Avançada Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Avançada contra Ameaças**, você pode configurar o uso da Kaspersky Security Network para o Kaspersky Endpoint Security for Windows. Você também pode configurar os módulos do Kaspersky Endpoint Security for Windows, tal como a Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host e Mecanismo de Correção.

Na subseção **Kaspersky Security Network**, recomendamos que você ative a opção **Usar proxy da KSN**. Use esse recurso para redistribuir e otimizar o tráfego na rede. Se a opção **Usar proxy da KSN** estiver desativada, você poderá ativar o uso direto de servidores KSN.

Configurar a política na seção Proteção Essencial Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção essencial contra ameaças** da janela de propriedades da política, recomendamos que você especifique configurações adicionais nas subseções **Firewall** e **Proteção contra ameaças ao arquivo**.

A subseção **Firewall** contém configurações que permitem controlar a atividade de rede dos aplicativos nos dispositivos clientes. Um dispositivo cliente usa uma rede à qual um dos seguintes status é atribuído: pública, local ou confiável. Dependendo do status da rede, o Kaspersky Endpoint Security pode permitir ou negar atividade de rede em um dispositivo. Ao adicionar uma nova rede à sua organização, você deve atribuir um status de rede apropriado a ela. Por exemplo, se o dispositivo cliente for um laptop, recomendamos que esse dispositivo use a rede pública ou confiável, porque o laptop nem sempre está conectado à rede local. Na subseção **Firewall**, você pode verificar se atribuiu corretamente os status às redes usadas em sua organização.

Para verificar a lista de redes:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Firewall**.
2. Na seção **Redes disponíveis**, clique no botão **Configurações**.
3. Na janela **Firewall** que se abre, vá para a guia **Redes** para visualizar a lista de redes.

Na subseção **Proteção Contra Ameaças ao Arquivo**, você pode desativar a verificação de unidades de rede. A verificação das unidades de rede pode colocar uma carga significativa nas unidades de rede. É mais conveniente executar a verificação indireta em servidores de arquivos.

Para desativar a verificação de unidades de rede:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças ao Arquivo**.
2. Na seção **Nível de segurança**, clique no botão **Configurações**.
3. Na janela **Proteção Contra Ameaças ao Arquivo** que se abre, na guia **Geral**, desmarque a caixa de seleção **Toda as unidades de rede**.

Configurar a política na seção Configurações Gerais

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Configurações gerais** da janela de propriedades da política, recomendamos que você especifique configurações adicionais nas subseções **Relatórios e armazenamentos** e **Interface**.

Na subseção **Relatórios e armazenamentos**, vá para a seção **Transferência de dados para o Servidor de Administração**. A caixa de seleção **Sobre o aplicativo iniciado** especifica se o banco de dados do Servidor de Administração salva as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Se esta caixa de seleção for marcada, as informações salvas poderão necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center (dúzias de gigabytes). Desmarque a caixa de seleção **Sobre os aplicativos iniciados** se estiver selecionada na política de nível superior.

Se o Console de Administração gerenciar a proteção antivírus na rede da organização no modo centralizado, desative a exibição da interface do usuário do Kaspersky Endpoint Security for Windows nas estações de trabalho. Para fazer isso, na subseção **Interface**, acesse a seção **Interação com o usuário** e, em seguida, marque a opção **Não exibir**.

Para ativar a proteção por senha nas estações de trabalho, na subseção **Interface**, acesse a seção **Proteção por**
nha, clique no botão **Configurações** e, em seguida, marque a caixa de seleção **Ativar proteção por senha**.

Configurando a política na seção Configuração de eventos

Na seção **Configuração do eventos**, você deve desativar a função de salvar quaisquer eventos no Servidor de Administração, exceto os seguintes:

- Na guia **Evento crítico**:
  - A execução automática do aplicativo está desativada

    Acesso negado
  - Proibida a inicialização do aplicativo

    Não é possível desinfetar
  - Contrato de Licença infringido
  - Não foi possível carregar o módulo de criptografia

    Não foi possível iniciar duas tarefas ao mesmo tempo
  - Ameaça ativa detectada. Iniciar Desinfecção Avançada

    Ataque de rede detectado
  - Nem todos os componentes foram atualizados
  - Erro de ativação
  - Erro ao ativar o modo portátil
  - Erro na interação com o Kaspersky Security Center

    Erro ao desativar o modo portátil
  - Erro ao alterar os componentes do aplicativo
  - Erro ao aplicar as regras de criptografia/descriptografia
  - A política não pode ser aplicada
  - Processo concluído

    Atividade de rede bloqueada
- Na guia **Falha funcional**: configurações de tarefa inválidas. Configurações não aplicadas

  Na guia **Advertência**:
  - Autodefesa desativada
  - Chave de reserva incorreta
  - C

- Na guia **Informações**: inicialização do aplicativo proibida no modo de teste

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

As informações desta subseção somente são aplicáveis ao Kaspersky Security Center 10 Maintenance Release 1 e versões posteriores.

Se o Servidor de Administração atuar como a fonte de atualização, a opção de agendamento ótima e recomendada para o Kaspersky Endpoint Security 10 e versões posteriores é **Quando novas atualizações são baixadas no repositório** com a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Para uma tarefa de atualização de grupo na versão 8 do Kaspersky Endpoint Security você deve especificar explicitamente o atraso da inicialização (1 hora ou mais) e marcar a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Se uma tarefa local para baixar as atualizações dos servidores da Kaspersky para o repositório que for criado em cada ponto de distribuição, o agendamento periódico será ótimo e recomendado para a tarefa de atualização em grupo do Kaspersky Endpoint Security. Neste caso, o valor de intervalo de randomização deve ser estabelecido em 1 hora.

Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

O Assistente de início rápido cria uma tarefa de grupo para verificar um dispositivo. Por padrão, à tarefa é atribuído um agendamento **Executar às sextas-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver desmarcada.

Isto significa que se os dispositivos em uma organização são desligados às sextas-feiras, por exemplo, às 18:30, a tarefa de verificação de dispositivo nunca será executada. Você deve definir o agendamento mais conveniente para esta tarefa com base nas regras do local de trabalho adotadas na organização.

Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias

O Assistente de início rápido cria a tarefa *Encontrar vulnerabilidades e atualizações necessárias* para o Agente de Rede. Por padrão, à tarefa é atribuído um agendamento **Executar às terças-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver marcada.

Se as regras do local de trabalho da organização proverem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar vulnerabilidades e atualizações necessárias* será executada após os dispositivos serem novamente ligados, ou seja, na quarta-feira pela manhã. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades

O Assistente de início rápido cria uma tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades para o Agente de Rede. Por padrão, a tarefa é configurada para ser executada todos os dias à 1h, com randomização automática, e a opção **Executar tarefas perdidas** não está habilitada.

Se as regras do local de trabalho da organização proverem o desligamento dos dispositivos durante a noite, a instalação da atualização nunca será executada. Você deve definir o agendamento mais conveniente da tarefa de verificação de vulnerabilidades com base nas regras do local de trabalho adotadas na organização. Também é importante ter em mente que a instalação das atualizações pode necessitar o reinício do dispositivo.

Criação de uma estrutura de grupos de administração e atribuir pontos de distribuição

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, a abrangência das políticas é definida com tags, localizações de dispositivos nas unidades organizacionais do Active Directory, associação nos grupo de segurança do Active Directory etc.

- Define o escopo de 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 organograma da empresa e da topologia da rede adotado pelo MSP cliente, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único

- Múltiplos pequenos escritórios desanexados

Configuração de cliente MSP padrão: 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 des ou segmentos de rede) vinculadas por canais estreitos.

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

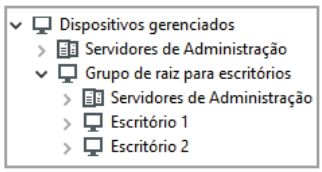
Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. 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. Neste caso, você deve 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. Neste caso, cada um dos Agentes de Rede irá conectar-se 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 de cliente MSP padrão: múltiplos pequenos escritórios remotos

Esta configuração padrão provê um número de pequenos escritórios remotos, que podem ser comunicados com a sede por meio 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 múltiplos pontos de distribuição deve ser atribuído 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.

Essa seção fornece informações sobre como aplicar políticas aos dispositivos em grupos de administração. Esta seção também fornece informações sobre os perfis da política.

Hierarquia de políticas

No Kaspersky Security Center, você usa políticas para definir uma coleção única de configurações para múltiplos dispositivos. Por exemplo, o escopo do aplicativo P definido para o grupo de administração G inclui dispositivos gerenciados com o aplicativo P instalado o que foi implementado no grupo G e em todos dos seus subgrupos, exceto para os subgrupos onde a caixa de seleção **Herdar do grupo de origem** estiver desmarcada nas propriedades.

Uma política diferencia-se de qualquer configuração local pelos ícones de cadeado (🔒) ao lado das suas configurações. Se uma configuração (ou um grupo de configurações) estiver bloqueada nas propriedades da política, será necessário, em primeiro lugar, usar essa configuração (ou o grupo de configurações) ao criar configurações efetivas e, em segundo lugar, salvar as configurações ou o grupo de configurações no fluxo abaixo da política.

A criação das configurações efetivas em um dispositivo pode ser descrita como se segue: os valores de todas as configurações que não foram bloqueadas são tiradas da política, então elas são sobregravadas com os valores das configurações locais, e então a coleção resultante é sobregravada com os valores de configurações bloqueadas tiradas da política.

As políticas do mesmo aplicativo se afetam entre si através da hierarquia de grupos de administração: as configurações bloqueadas da política de fluxo acima substituem as mesmas políticas do fluxo abaixo.

Há uma política especial para usuários fora do escritório. Esta política entra em vigor em um dispositivo quando o dispositivo muda para o modo de fora do escritório. As políticas de ausência não afetam outras políticas através da hierarquia de grupos de administração.

> A política de ausência não será suportada em versões futuras do Kaspersky Security Center. Os perfis de política serão usados em vez de políticas de ausência.

Perfis da política

Aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente em muitas circunstâncias. Pode ser necessário criar diversas instâncias de uma política única que se diferem em uma ou duas configurações para diferentes grupos de administração e que sincronizam os conteúdos destas políticas no futuro.

Para ajudar você a evitar tais problemas, o Kaspersky Security Center suporta os *perfis da política*. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo cliente (computador ou dispositivo móvel). A ativação de um perfil modifica as configurações da política que estavam ativas no dispositivo antes do perfil ser ativado. Essas configurações assumem valores que foram especificados no perfil.

As seguintes restrições são atualmente impostas aos perfis da política:

- Uma política pode incluir no máximo 100 perfis.
- Um p[illegible]

- Uma política não pode conter configurações de notificação.

Conteúdo de um perfil

Um perfil da política contém as seguintes partes constituintes:

- Os perfis com nomes idênticos afetam um ao outro através da hierarquia de grupos de administração com regras comuns.
- Subconjunto de configurações da política. Diferente da política, que contém todas as configurações, um perfil somente contém configurações que são de fato necessárias (configurações bloqueadas).

  Condição de ativação é uma expressão lógica com as propriedades do dispositivo. Um perfil está ativo (complementa a política) somente quando a condição de ativação de perfil se torna verdadeira. Em todos os outros casos, o perfil está inativo e é ignorado. As seguintes propriedades de dispositivo podem estar incluídas naquela expressão lógica:

  - Status do modo ausente.

    Propriedades do ambiente de rede: nome da regra ativa para a conexão do Agente de Rede.

  - Presença ou ausência de identificadores especificados no dispositivo.

    A alocação do dispositivo em uma unidade organizacional (UO) do Active Directory: explícita (o dispositivo está diretamente na UO especificada), ou implícito (o dispositivo está em uma UO, que está dentro da UO especificada em qualquer nível de aninhamento).

  - A associação do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
  - A associação do proprietário do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
- Desativando a caixa de seleção Perfil. Os perfis desativados sempre serão ignorados e as suas respetivas condições de ativação não serão verificadas.

  Prioridade do perfil. As condições de ativação de perfis diferentes são independentes, portanto vários perfis podem ser ativados simultaneamente. Se os perfis ativos contiverem coleções de configurações não de sobreposição, nenhum problema surgirá. No entanto, se dois perfis ativos contiverem valores diferentes da mesma configuração, uma ambiguidade ocorrerá. Esta ambiguidade deve ser evitada através das prioridades do perfil: o valor da variável ambígua será tomado do perfil que tiver a prioridade mais alta (aquele que é classificado como mais alto na lista de perfis).

O comportamento de perfis quando as políticas afetam uma a outra através da hierarquia

Os perfis com o mesmo nome são mesclados de acordo com as regras de mesclagem de política. Os perfis de uma política com fluxo acima têm uma prioridade mais alta do que os perfis de uma política de fluxo abaixo. Se a edição das configurações for proibida na política de fluxo acima (está bloqueada), a política de fluxo abaixo usa as condições de ativação da política de fluxo acima. Se a edição das configurações for permitida na política de fluxo acima, as condições de ativação do perfil da política de fluxo abaixo são usadas.

Como um perfil da política pode conter a propriedade **O dispositivo está offline** em sua condição de ativação, os perfis substituem completamente as políticas de usuário ausente, que não são mais compatíveis.

a política de usuário ausente pode conter perfis, mas os seus perfis somente podem ser ativados após que o

Tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios

  Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração

  Manutenção do banco de dados
- Sincronização com o Windows Update
- Criação de um pacote de instalação com base na imagem do sistema operacional (SO) de um dispositivo de referência

Os seguintes tipos de tarefas são executados nos dispositivos:

Tarefas locais – Tarefas que são executadas em um dispositivo específico
As tarefas locais podem ser modificadas pelo administrador, usando as ferramentas do Console de Administração ou por um usuário de um dispositivo remoto (por exemplo, através da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.
- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados das tarefas são salvos no log de eventos do Microsoft Windows e no log de eventos do Kaspersky Security Center, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Regras de migração de dispositivos

Recomendamos que você automatize a alocação de dispositivos aos grupos de administração no servidor virtual que corresponde a um cliente MSP, usando *regras para mover dispositivo*. Uma regra para migrar dispositivo compõe-se de três partes principais: um nome, uma condição de execução (expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica os atributos do dispositivo quanto a se eles atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Também, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center na lista de regras para mover. A lista está localizada no Console de Administração, nas propriedades do grupo **Dispositivos não atribuídos**.

Por padrão, uma regra para mover dispositivo é destinada para a alocação inicial de uma só vez de dispositivos aos grupos de administração. A regra move os dispositivos do grupo **Dispositivos não atribuídos** somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo **Dispositivos não atribuídos** manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isto, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar regras para mover aos dispositivos que já foram alocados à alguns dos grupos de administração, aumenta significativamente a carga do Servidor de Administração.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

Tais cenários não são compatíveis, porque eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis de política, tarefas para seleções de dispositivo, atribuição de Agentes de Rede de acordo com o cenário padrão, e assim por diante.

Categorização de software

A ferramenta principal para monitorar a execução dos aplicativos são as *categorias da Kaspersky* (aqui referidas como *categorias da KL*). As categorias da KL ajudam os administradores do Kaspersky Security Center a simplificar o suporte da categorização de software e minimizar o tráfego indo para os dispositivos gerenciados.

As categorias de usuário somente devem ser criadas para aplicativos que não podem ser classificados em nenhuma das categorias da KL existentes (por exemplo, para o software criado de forma personalizada). As categorias de usuário são criadas com base em um pacote de instalação do aplicativo (MSI) ou uma pasta com pacotes de instalação.

Se uma grande coleção de software estiver disponível, que não foi categorizada através de categorias da KL, pode ser útil criar uma categoria automaticamente atualizada. Os checksums de arquivos executáveis serão automaticamente adicionados a esta categoria em cada modificação da pasta que contém os pacotes de distribuição.

Não crie categorias de software atualizadas automaticamente para as pastas Meus Documentos, %windir%, %ProgramFiles% e %ProgramFiles(x86)%. O conjunto de arquivos nestas pastas está sujeito a modificações frequentes, que conduz a um aumento da no Servidor de Administração e no aumento do tráfego da rede.
Você deve criar uma pasta dedicada com a coleção de software e periodicamente adicionar-lhe novos itens.

Sobre os aplicativos para múltiplos usuários

O Kaspersky Security Center permite que os administradores de provedores de serviço e administradores de usuários usem os aplicativos Kaspersky com o suporte para múltiplos usuários. Após um aplicativo da Kaspersky para múltiplos usuários ter sido instalado na infraestrutura de um provedor de serviços, os usuários podem começar a usar o aplicativo.

Para separar as tarefas e políticas relativas a diferentes usuários, você precisa criar um Servidor de Administração virtual no Kaspersky Security Center para cada usuário. Todas as tarefas e políticas para aplicativos de múltiplos usuários sendo executadas para um usuário devem ser criadas para o grupo de administração Dispositivos gerenciados do Servidor de Administração virtual correspondente àquele usuário. As tarefas criadas para os grupos de administração relativos ao Servidor de Administração principal não afetam os dispositivos dos tenants.

Diferente dos administradores do provedor de serviços, um administrador de usuários pode criar e exibir tarefas e políticas do aplicativo somente para os dispositivos do usuário correspondente. Os conjuntos de configurações de tarefas e políticas disponíveis para os administradores do provedor de serviços e para os administradores de usuários são diferentes. Algumas das configurações de tarefas e políticas não estão disponíveis para os administradores de usuários.

Na estrutura hierárquica de um usuário, as políticas criadas para aplicativos para múltiplos usuários são herdadas de grupos de administração de nível mais baixo, assim como de grupos de administração de nível superior: a política é propagada à todos os dispositivos cliente que pertencem ao usuário.

Cópia backup e restauração das configurações do Servidor de Administração

O backup das configurações do Servidor de Administração e de seu banco de dados é executado pela tarefa de backup e com o utilitário klbackup. Uma cópia backup inclui todas as principais configurações e objetos pertencentes ao Servidor de Administração, como certificados, chaves primárias para criptografia de unidades em dispositivos gerenciados, chaves para várias licenças, estrutura de grupos de administração com todo o seu conteúdo, tarefas, políticas etc. Com uma cópia backup, é possível recuperar a operação de um Servidor de Administração o mais rápido possível, gastando de uma dúzia de minutos a algumas horas nisso.

Se nenhuma cópia backup estiver disponível, uma falha pode levar a uma perda irrevogável de certificados e de todas as configurações do Servidor de Administração. Isto exigirá reconfigurar o Kaspersky Security Center do zero e executar a implementação inicial do Agente de Rede novamente na rede da organização. Todas as chaves primárias para a criptografia das unidades em dispositivos gerenciados também serão perdidas, arriscando a perda irrevogável dos dados criptografados nos dispositivos com Kaspersky Endpoint Security. Portanto, não negligencie os backups regulares do Servidor de Administração usando a tarefa de backup padrão.

O Assistente de Início Rápido cria a tarefa de backup para as configurações do Servidor de Administração e o configura para ser executado diariamente, às 4h. As cópias de backup são salvas por padrão na pasta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Se uma instância do Microsoft SQL Server instalado em outro dispositivo for usado como o DBMS, você deve modificar a tarefa de backup especificando um caminho UNC, que está disponível para gravar tanto pelo serviço Servidor de Administração como pelo serviço SQL Server, como a pasta para armazenar as cópias backup. Este requisito deriva de um recurso especial do backup no Microsoft SQL Server DBMS.

Se uma instância local do Microsoft SQL Server for usada como DBMS, também recomendamos salvar as cópias de backup em uma mídia dedicada para assegurar que elas estejam protegidas contra danos, em conjunto com o Servidor de Administração.

Como uma cópia backup contém dados importantes, a tarefa de backup e o utilitário klbackup fornecem a proteção por senha das cópias backup. Por padrão, a tarefa de backup é criada com uma senha em branco. Você deve definir uma senha nas propriedades da tarefa de backup. Negligenciar este requisito causa uma situação em que todas as chaves de certificados do Servidor de Administração, as chaves para as licenças e as chaves primárias para a criptografia de unidades em dispositivos gerenciados permanecem não criptografadas.

Além do backup regular, você também deve criar uma cópia backup antes de cada mudança significativa, incluindo a instalação de atualizações e patches do Servidor de Administração.

Se você usar o Microsoft SQL Server como DBMS, poderá minimizar o tamanho das cópias de backup. Para isso, ative a opção **Compactar o backup** nas configurações do SQL Server.

A restauração de uma cópia backup é executada com o utilitário klbackup em uma instância operável do Servidor de Administração que acaba de ser instalado e que tenha a mesma versão (ou posterior) para o qual a cópia backup foi criada.

A instância do Servidor de Administração no qual a restauração deve ser executada, deve usar um DBMS do mesmo tipo (por exemplo, o mesmo SQL Server ou MariaDB) e a mesma versão ou posterior. A versão do Servidor de Administração pode ser a mesma (com uma correção idêntica ou posterior), ou posterior.

Esta seção descreve os cenários padrão para restaurar as configurações e objetos do Servidor de Administração.

Um dispositivo com o Servidor de Administração está inoperável

Se um dispositivo com o Servidor de Administração estiver inoperável devido a uma falha, você é recomendado a executar as seguintes ações:

- Ao novo Servidor de Administração deve ser atribuído o mesmo endereço: nome NetBIOS, FQDN ou IP estático (dependendo de qual deles foi definido quando os Agentes de Rede foram implementados).
- Instale o Servidor de Administração, usando um DBMS do mesmo tipo ou da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.
- No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

As configurações do Servidor de Administração ou o do banco de dados estão corrompidas

Se o Servidor de Administração estiver inoperável devido a configurações ou aos bancos de dados corrompidas (p. ex., após uma oscilação de corrente), você é recomendado a usar o seguinte cenário de restauração:

1. Verifique o sistema de arquivos no dispositivo danificado.
2. Desinstale a versão inoperável do Servidor de Administração.
3. Reinstale o Servidor de Administração usando um DBMS do mesmo tipo e da mesma (ou posterior) versão.
   Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.
4. No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

É proibido restaurar o Servidor de Administração usando qualquer outro modo que não seja através do utilitário klbackup.

Qualquer tentativa de restaurar o Servidor de Administração através de software de terceiros levará inevitavelmente a dessincronização dos dados nos nós do aplicativo Kaspersky Security Center distribuído e, consequentemente, ao funcionamento impróprio do aplicativo.

Implementar o Agente de Rede e o aplicativo de segurança

Para gerenciar dispositivos em uma organização, você deve instalar o Agente de Rede em cada um deles. A implementação do Kaspersky Security Center distribuído nos dispositivos corporativos normalmente começa com a instalação do Agente de Rede neles.

No Microsoft Windows XP, o Agente de Rede pode não executar as seguintes operações corretamente: baixar atualizações diretamente dos servidores da Kaspersky (como um ponto de distribuição); funcionar como servidor proxy da KSN (como um ponto de distribuição); e detectar vulnerabilidades de terceiros (se Gerenciamento de patches e vulnerabilidades for usado).

Implementação inicial

Se um Agente de Rede já tiver sido instalado em um dispositivo, a instalação remota de aplicativos naquele dispositivo é executada através deste Agente de Rede. O pacote de distribuição de um aplicativo a ser instalado é transferido através de canais de comunicação entre Agentes de Rede e o Servidor de Administração, junto com as configurações de instalação definidas pelo administrador. Para transferir o pacote de distribuição, é possível usar nós de distribuição de transmissão, ou seja, pontos de distribuição, entrega multicast, etc. Para obter mais detalhes sobre como instalar aplicativos em dispositivos gerenciados com o Agente de Rede já instalado, consulte o conteúdo a seguir nesta seção.

Você pode executar a instalação inicial do Agente de Rede em dispositivos que executam o Windows, usando um dos seguintes métodos:

- Com ferramentas de terceiros para a instalação remota de aplicativos.

  Com políticas de grupo do Windows: usar ferramentas padrão de gerenciamento do Windows para políticas de grupo.

  No modo forçado, usando opções especiais na tarefa de instalação remota do Kaspersky Security Center.
- Enviando aos usuários de dispositivo links para pacotes independentes pelo Kaspersky Security Center. Os pacotes independentes são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados com as suas configurações definidas.
- Manualmente, executando os instaladores do aplicativo em dispositivos.

Em plataformas outras do que o Microsoft Windows, você tem de executar a instalação inicial do Agente de Rede em dispositivos gerenciados através da ferramentas de terceiros existentes, ou manualmente, enviando aos usuários um arquivo compactado com um pacote de distribuição pré-configurado. Você pode fazer um upgrade do Agente de Rede para uma nova versão ou instalar outros aplicativos Kaspersky em plataformas que não sejam o Windows, usando Agentes de Rede (já instalado em dispositivos) para executar tarefas de instalação remotas. Neste caso, a instalação é idêntica a nos dispositivos que executam o Microsoft Windows.

Ao selecionar um método e uma estratégia para a implementação de aplicativos em uma rede gerenciada, é necessário considerar um número de fatores (lista parcial):

- Configuração da rede corporativa
- Número total de dispositivos

  A presença de domínios do Windows na rede gerenciada, com a possibilidade de modificar as políticas de grupo do Active Directory nesses domínios

- A ciência das contas de usuário com direitos de administrador locais em dispositivos nos quais a implementação inicial de aplicativos Kaspersky foi planejada (ou seja, a disponibilidade de uma conta de usuário de domínio com direitos de administrador local ou a presença de contas de usuários locais unificadas com direitos de administrador naqueles dispositivos)

- Tipo de conexão e a banda larga de canais de rede entre o Servidor de Administração e redes cliente MSP, assim como a banda larga de canais dentro daquelas redes
- Configurações de segurança aplicadas em dispositivos remotos no início da implementação (tal como o uso do modo UAC e de Compartilhamento de arquivo simples)

Configurar os instaladores

Antes da implementação inicial de aplicativos Kaspersky em uma rede, você deve especificar as configurações de instalação, ou seja, as definidas durante a instalação do aplicativo. Ao instalar o Agente de Rede, você deve especificar, no mínimo, um endereço para a conexão ao Servidor de Administração e as configurações proxy; algumas configurações avançadas também podem ser necessárias. Dependendo do método Instalação que você selecionou, poderá definir configurações de diferentes maneiras. No caso mais simples (instalação interativa manual em um dispositivo selecionado), todas as configurações relevantes podem ser definidas através da interface de usuário do Instalador, portanto, em alguns casos, a implementação inicial pode até ser executada enviando aos usuários um link ao pacote de distribuição do Agente de Rede junto com as configurações (endereço de Servidor de Administração, etc.) que o usuário deve inserir na interface do Instalador.

Este método não é recomendado para uso, já que é inconveniente para os usuários, implicando um alto risco de erros ao definir as configurações manualmente; também é não é utilizável com a instalação silenciosa de aplicativos em grupos de dispositivos. Em geral, o administrador deve especificar os valores das configurações no modo centralizado; estes valores podem ser posteriormente usados para a criação de pacotes independentes. Os pacotes independentes são arquivos compactados de auto-extração que contêm pacotes de distribuição com configurações definidas pelo administrador. Os pacotes autônomos podem ser localizados em recursos que permitam baixar pelos usuários finais (por exemplo, no Servidor Web do Kaspersky Security Center) e pela instalação silenciosa em dispositivos em rede selecionados.

Pacotes de instalação

O primeiro e principal método de definir as configurações da instalação de aplicativos é útil para muitas finalidades e assim adequado para todos os métodos de instalação, para os métodos de instalação com as ferramentas do Kaspersky Security Center e com a maior parte de ferramentas de terceiros. Este método consiste na criação de pacotes de instalação de aplicativos no Kaspersky Security Center.

Os pacotes de Instalação são gerados usando os seguintes métodos:

- Automaticamente, a partir de pacotes de distribuição especificados, com base em *descritores* incluídos (arquivos com a extensão .kud que contêm regras para a instalação e análise de resultados e outras informações)
- A partir dos arquivos executáveis de instaladores ou de instaladores no formato do Microsoft Windows Installer (MSI) são para aplicativos padrão ou suportados

Os pacotes de instalação gerados são organizados hierarquicamente como pastas com subpastas e arquivos. Além do pacote de distribuição original, um pacote de instalação contém configurações editáveis (incluindo as configurações do instalador e as regras para processar os casos tal como necessidade de reiniciar o sistema operacional para concluir a instalação), assim como os módulos auxiliares secundários.

Os valores das configurações de instalação que são específicos para um aplicativo selecionado a ser suportado podem ser especificados na interface do usuário do Console de Administração ao criar um pacote de instalação (mais configurações podem ser encontradas nas propriedades de um pacote de instalação que já foi criado). Ao executar a instalação remota de aplicativos através das ferramentas do Kaspersky Security Center, os pacotes de instalação são entregues aos dispositivos alvo para que ao executar o instalador de um aplicativo, torna todas as configurações definidas pelo administrador à disposição daquele aplicativo. Ao usar as ferramentas de terceiros para a instalação de aplicativos Kaspersky, você somente tem de assegurar a disponibilidade de todo o pacote de instalação no dispositivo alvo, ou seja, a disponibilidade do pacote de distribuição e de suas configurações. Os pacotes de Instalação são criados e armazenados pelo Kaspersky Security Center em uma subpasta dedicada da pasta de dados compartilhados.

Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.

Para obter instruções sobre a utilização deste método de configuração para aplicativos Kaspersky antes da implementação através de ferramentas de terceiros, consulte a seção "Implementar usando políticas de grupo do Microsoft Windows".

Imediatamente após a instalação do Kaspersky Security Center, alguns pacotes de instalação são automaticamente gerados; eles estão prontos para a instalação e incluem pacotes de Agente de Rede e pacotes de aplicativos de segurança para o Microsoft Windows.

Em alguns casos, a utilização de pacotes de instalação para a implementação de aplicativos em uma rede cliente MSP implica na necessidade de criar pacotes de instalação em Servidores virtuais que correspondam aos clientes MSP. A criação de pacotes de instalação em Servidores virtuais permite usar diferentes configurações de instalação para diferentes clientes MSP. Na primeira instância, isso é útil ao manusear pacotes de instalação de Agente de Rede, já que os Agentes de Rede implementados nas redes de diferentes clientes MSP usam diferentes endereços para conectar-se ao Servidor de Administração. De fato, o endereço de conexão determina o Servidor ao qual o Agente de Rede se conecta.

Além da possibilidade de criar novos pacotes de instalação imediatamente em um Servidor de Administração virtual, o modo de operação principal para os pacotes de instalação em Servidores de Administração virtuais é a "distribuição" de pacotes de instalação do Servidor de Administração principal para os virtuais. Você pode distribuir pacotes de instalação selecionados (ou todos) aos Servidores de Administração virtuais selecionados (incluindo todos os Servidores com um grupo de administração selecionado) utilizando a tarefa de Servidor de Administração correspondente. Você também pode selecionar a lista de pacotes de instalação do Servidor de Administração principal criando um novo Servidor de Administração virtual. Os pacotes selecionados serão imediatamente distribuídos a um Servidor de Administração virtual recentemente criado.

Ao distribuir um pacote de instalação, seu conteúdo não é inteiramente copiado. O repositório de arquivo em um Servidor de Administração virtual, que corresponde ao pacote de instalação sendo distribuído, somente armazena arquivos de configurações que são específicos para aquele Servidor virtual. A parte principal do pacote de instalação (incluindo o pacote de distribuição do aplicativo sendo instalado) permanece inalterada e é somente armazenada no repositório do Servidor de Administração principal. Isto permite aumentar o desempenho do sistema drasticamente e reduzir o volume de disco necessário. Ao tratar pacotes de instalação distribuídos aos Servidores de Administração virtuais (ou seja, executando tarefas de instalação remotas ou criando pacotes de instalação independentes), os dados do pacote de instalação original do Servidor de Administração principal são "mesclados" com os arquivos de configurações, que correspondem ao pacote distribuído no Servidor de Administração virtual.

Embora a chave de licença para um aplicativo possa ser definida nas propriedades do pacote de instalação, é aconselhável evitar este método de distribuição da licença porque é fácil obter acidentalmente o acesso de leitura aos arquivos na pasta. Você deve usar as chaves automaticamente distribuídas ou as tarefas de instalação para chaves de licença.

Propriedades MSI e arquivos de transformação

Outro modo de configurar a instalação na plataforma Windows é o de definir as propriedades MSI e arquivos de transformação. Este método pode ser usado ao executar a instalação através de ferramentas de terceiros para os instaladores no formato do Microsoft Installer, assim como ao executar a instalação através der políticas de grupo do Windows usando ferramentas padrão da Microsoft ou outras ferramentas de terceiros projetadas para tratar políticas de grupo do Windows.

Implementação com ferramentas de terceiros para a instalação remota de aplicativos

Quando qualquer ferramenta para a instalação remota de aplicativos (tal como o Microsoft System Center) estiver disponível em uma organização, é conveniente executar a implementação inicial usando estas ferramentas.

As seguintes ações devem ser executadas:

- Selecione o método para configurar a instalação melhor adequada para a ferramenta implementação a ser usada.
- Defina o mecanismo para a sincronização entre a modificação das configurações dos pacotes de instalação (através da interface do Console de Administração) e a operação das ferramentas de terceiros selecionadas e usadas para a implementação de aplicativos a partir dos dados do pacote de instalação.

Informação geral sobre as tarefas de instalação remotas no Kaspersky Security Center

O Kaspersky Security Center fornece uma ampla gama de métodos para a instalação remota de aplicativos, que são implementados como tarefas de instalação remotas. Você pode criar uma tarefa de instalação remota para um grupo de administração especificado e para dispositivos específicos ou para uma seleção de dispositivos (tais tarefas são exibidas no Console de Administração, na pasta **Tarefas**). Ao criar uma tarefa, você pode selecionar pacotes de instalação (aqueles do Agente de Rede e / ou outro aplicativo) a ser instalado dentro desta tarefa, assim como especificar determinadas configurações que definem o método da instalação remota.

As tarefas para grupos de administração afetam ambos os dispositivos incluídos em um grupo especificado e todos os dispositivos em todos os subgrupos dentro daquele grupo de administração. Uma tarefa cobre dispositivos de Servidores de Administração secundários incluídos em um grupo ou algum dos seus subgrupos se a configuração correspondente estiver ativada na tarefa.

As tarefas para dispositivos específicos atualizam a lista de dispositivos cliente em cada execução de acordo com o conteúdo da seleção no momento em que a tarefa é iniciada. Se uma seleção incluir dispositivos que foram conectados aos Servidores de Administração secundários, a tarefa também será executada naqueles dispositivos.

Para assegurar-se de uma operação bem-sucedida de uma tarefa de instalação remota nos dispositivos conectados aos Servidores de Administração secundários, você deve usar a tarefa de distribuição para distribuir os pacotes de instalação usados por sua tarefa aos Servidores de Administração secundários correspondentes com antecedência.

Recomenda-se que você execute a implementação inicial de Agentes de Rede através da políticas de grupo do Microsoft Windows se as seguintes condições forem atendidas:

- Este dispositivo é membro de um domínio Active Directory.

  O acesso ao controlador do domínio é concedido com os direitos de administrador, que lhe permite criar e modificar políticas de grupo do Active Directory.

- Os pacotes de instalação configurados podem ser movidos para a rede que hospeda os dispositivos gerenciados alvo (para uma pasta compartilhada que está disponível para leitura por todos os dispositivos alvo).

- O esquema de implementação permite esperar pelo reinício da próxima rotina de dispositivos alvo antes da implementação inicial de Agentes de Rede neles (ou você pode forçar uma política de grupo do Windows a ser aplicada àqueles dispositivos).

Este esquema de implementação consiste no seguinte:

- O pacote de distribuição do aplicativo no formato do Microsoft Installer (pacote MSI) está localizado em uma pasta compartilhada (uma pasta onde as contas de LocalSystem de dispositivos alvo têm permissões de leitura).

- Na política de grupo do Active Directory, um objeto Instalação é criado para o pacote de distribuição.

- O escopo da instalação é definido especificando a unidade organizacional (UO) e/ou o grupo de segurança, que inclua os dispositivos alvo.

- Na próxima vez que um dispositivo alvo se conecta ao domínio (antes que os usuários do dispositivo se conectem ao sistema), todos os aplicativos instalados são verificados quanto a presença do aplicativo necessário. Se o aplicativo não for encontrado, o pacote de distribuição é baixado do recurso especificado na política e então é instalado.

Uma vantagem deste esquema de implementação é que os aplicativos atribuídos são instalados nos dispositivos alvo enquanto o sistema operacional está sendo carregado, ou seja, até antes que o usuário se conecte ao sistema. Mesmo se um usuário com direitos suficientes remova o aplicativo, ele será reinstalado na próxima inicialização do sistema operacional. Este problema do esquema implementação é que as modificações feitas pelo administrador à política de grupo não entrarão em vigor até que os dispositivos sejam reiniciados (se nenhuma ferramenta adicional estiver envolvida).

Você pode usar políticas de grupo para instalar o Agente de Rede assim como outros aplicativos se os seus respetivos instaladores estiverem no formato do Windows Installer.

Além disso, quando você seleciona este método de implementação, terá que avaliar a carga no recurso de arquivo do qual os arquivos serão copiados para os dispositivos após a política de grupo do Windows ter sido aplicada. Você também tem de escolher o método de entrega do pacote de instalação configurado àquele recurso, assim como o método de sincronizar as modificações relevantes nas suas configurações.

Tratar políticas do Microsoft Windows através da tarefa de instalação remota do Kaspersky Security Center

Este método de implementação somente está disponível se o acesso ao controlador do domínio, que contém os dispositivos alvo, for possível do dispositivo a partir do Servidor de Administração, enquanto a pasta compartilhada do Servidor de Administração (a que armazena os pacotes de instalação) for acessível para litura de dispositivos alvo. Devido aos motivos acima, este método de implementação não visto como aplicável ao MSP.

O administrador pode criar os objetos necessários para a instalação em uma política de grupo do Windows em seu nome. Neste caso, você tem de carregar os pacotes para um servidor de arquivos independente e fornecer-lhes um link.

Os seguintes cenários de instalação são possíveis:

- O administrador cria um pacote de instalação e define suas propriedades no Console de Administração. Então o administrador copia a toda a subpasta EXEC deste pacote da pasta compartilhada do Kaspersky Security Center para uma pasta em um recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização.
- O administrador baixa o pacote de distribuição do aplicativo (incluindo o do Agente de Rede) da Internet e carrega ele no recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização. As configurações de instalação são definidas ao configurar as propriedades MSI ou ao configurar os arquivos de transformação MST.

Implementação forçada através da tarefa de instalação remota do Kaspersky Security Center

Para executar a implementação inicial de Agentes de Rede ou outros aplicativos, você pode forçar a instalação de pacotes de instalação selecionados usando a tarefa de instalação remota do Kaspersky Security Center – contanto que cada dispositivo tenha uma conta de usuário com direitos de administrador local e pelo menos um dispositivo com o Agente de Rede instalado atuando como um ponto de distribuição em cada subrede.

Neste caso, você pode especificar os dispositivos alvo explicitamente (com uma lista) ou selecionando o grupo de administração do Kaspersky Security Center ao qual eles pertencem, ou criando uma seleção de dispositivos com base em um critério específico. A hora início da instalação é definida pelo agendamento da tarefa. Se a configuração **Executar tarefas ignoradas** for ativada nas propriedades da tarefa, a tarefa pode ser executada imediatamente após que os dispositivos alvo sejam ligados, ou quando eles forem movidos para o grupo de administração alvo.

A instalação forçada consiste na entrega de pacotes de instalação aos pontos de distribuição, na cópia subsequente de arquivos ao recurso admin$ em cada um dos dispositivos alvo e no registro remoto de serviços de suporte naqueles dispositivos. A entrega de pacotes de instalação aos pontos de distribuição é executada através de um recurso do Kaspersky Security Center que assegura a interação na rede. As seguintes condições devem ser atendidas neste caso:

- Os dispositivos-alvo são acessíveis do lado do ponto de distribuição.
- A solução do nome dos dispositivos-alvo funciona apropriadamente na rede.
- Os compartilhamentos administrativos (admin$) permanecem ativados nos dispositivos-alvo.

  O serviço do sistema do Servidor está em execução nos dispositivos-alvo (por padrão, está em execução).
- As seguintes portas estão abertas nos dispositivos-alvo para permitir o acesso remoto através das ferramentas do Windows: TCP 139, TCP 445, UDP 137 e UDP 138.
- Em dispositivos-alvo que executam o Microsoft Windows XP, o modo Compartilhamento Simples de Arquivo está desativado.

  Nos dispositivos-alvo, o compartilhamento de acesso e o modelo de segurança estão definidos como *Clássico – os usuários locais autenticam como si próprios*; não pode ser de nenhuma forma *Somente*

convidado – os usuários locais autenticam como Convidado.

Os dispositivos-alvo são membros do domínio, ou as contas uniformes com direitos de administrador são criadas nos dispositivos-alvo com antecedência.

Os dispositivos em grupos de trabalho podem ser ajustados de acordo com os requisitos acima ao usar o utilitário riprep.exe, que está descrito no site de Suporte Técnico da Kaspersky.

Durante a instalação em novos dispositivos que ainda não foram alocados à nenhum dos grupos de administração do Kaspersky Security Center, você pode abrir as propriedades da tarefa de instalação remota e especificar o grupo de administração para o qual os dispositivos serão movidos após a instalação do Agente de Rede.

Ao criar uma tarefa de grupo, tenha em mente que cada tarefa de grupo afeta todos os dispositivos em todos os grupos aninhados dentro de um grupo selecionado. Portanto, você deve evitar duplicar tarefas de instalação em subgrupos.

A instalação automática é um modo simplificado para criar tarefas para a instalação forçada de aplicativos. Para fazer isto, abra as propriedades de grupo de administração, abra a lista de pacotes de instalação e selecione aqueles que devem ser instalados nos dispositivos neste grupo. Como resultado, os pacotes de instalação selecionados serão automaticamente instalados em todos os dispositivos neste grupo e em todos os seus subgrupos. O intervalo de tempo sobre o qual os pacotes serão instalados depende da produtividade da rede e o número total de dispositivos na rede.

Para permitir a instalação forçada, você deve assegurar-se de que os pontos de distribuição estejam presentes em cada uma das subredes isoladas que hospedam dispositivos alvo.

Observe que este método de instalação coloca uma carga significativa nos dispositivos que atuam como pontos de distribuição. Portanto, recomenda-se que você selecione dispositivos potentes com unidades de armazenamento de alto desempenho como pontos de distribuição. Além disso, o espaço livre em disco na partição com a pasta *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* deve exceder, muitas vezes, o tamanho total dos pacotes de distribuição de aplicativos instalados.

Executar pacotes independentes criados pelo Kaspersky Security Center

Os métodos acima descritos da implementação inicial do Agente de Rede e de outros aplicativos nem sempre podem ser implementados porque não é possível atender todas as condições aplicáveis. Em tais casos, você pode criar um arquivo executável comum denominado como *pacote de instalação independente* através do Kaspersky Security Center, usando pacotes de instalação com as configurações de instalação relevantes que foram preparados pelo administrador. Um pacote de instalação independente pode ser publicado em um da Servidor da Web interno (incluído no Kaspersky Security Center) se isto for considerado razoável (fora do acesso àquele Servidor Web que foi configurado para usuários de dispositivo alvo), ou em um Servidor da Web exclusivamente implementado incluído no Kaspersky Security Center Web Console. Você também pode copiar pacotes independentes para outro Servidor da Web.

Você pode usar o Kaspersky Security Center para enviar aos usuários selecionados uma mensagem de e-mail contendo um link para o arquivo do pacote independente no Servidor da Web no momento em uso, solicitando-lhes que executem o arquivo (no modo interativo ou com a chave "-s" para a instalação silenciosa). Você pode anexar o pacote de instalação independente a uma mensagem de e-mail e então enviá-lo aos usuários dos dispositivos que não tenham acesso ao Servidor da Web. O administrador também pode copiar o pacote independente em um dispositivo externo, entregá-lo a um dispositivo relevante, e então executá-lo mais tarde.

Você pode criar um pacote independente a partir de um pacote de Agente de Rede, de um pacote de outro aplicativo (por exemplo, o aplicativo de segurança), ou ambos. Se o pacote independente foi criado a partir do Agente de Rede e de outro aplicativo, a instalação inicia com o Agente de Rede.

Ao criar um pacote independente com o Agente de Rede, você pode especificar o grupo de administração ao qual os novos dispositivos (aqueles que não foram alocados à nenhum dos grupos de administração) serão automaticamente movidos quando a instalação do Agente de Rede for concluída neles.

Os pacotes independentes podem ser executados no modo interativo (por padrão), exibindo o resultado da instalação de aplicativos que eles contêm, ou eles podem ser executados no modo silencioso (quando executados com a chave "-s"). O modo silencioso pode ser usado para a instalação de scripts, por exemplo, de scripts configurados para ser executados após a implementação da imagem do sistema operacional. O resultado da instalação no modo silencioso é determinado pelo código de retorno do processo.

Opções para a instalação manual de aplicativos

Os administradores ou os usuários experientes podem instalar os aplicativos manualmente no modo interativo. Eles podem usar pacotes de distribuição originais ou pacotes de instalação gerados a partir deles e armazenados na pasta compartilhada do Kaspersky Security Center. Por padrão, instaladores são executados no modo interativo e solicitam aos usuários todos os valores necessários. No entanto, ao executar o processo setup.exe a partir da raiz de um pacote de instalação com a chave "-s", o instalador será executado no modo silencioso e com as configurações que foram definidas ao configurar o pacote de instalação.

Ao executar o setup.exe a partir da raiz de um pacote de instalação, o pacote será primeiro copiado para uma pasta local temporária e, a seguir, o instalador do aplicativo será executado a partir da pasta local.

Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado

Se um Agente de Rede operável conectado ao Servidor de Administração principal (ou a algum dos seus Servidores secundários) for instalado em um dispositivo, você poderá fazer um upgrade do Agente de Rede neste dispositivo, assim como instalar, atualizar ou remover qualquer aplicativo compatível através do Agente de Rede.

Você pode ativar esta opção ao selecionar a caixa de seleção **Usando Agente de Rede** nas propriedades da tarefa de instalação remota.

Se esta caixa de seleção for selecionada, os pacotes de instalação com configurações de instalação definidas pelo administrador serão transferidos para os dispositivos alvo através dos canais de comunicação entre o Agente de Rede e o Servidor de Administração.

Para otimizar a carga do Servidor de Administração e minimizar o tráfego entre o Servidor de Administração e os dispositivos, é útil atribuir pontos de distribuição em cada rede remota ou em cada domínio emissor (consulte as seções Sobre os pontos de distribuição e Criar uma estrutura de grupos de administração e atribuir pontos de distribuição). Neste caso, os pacotes de instalação e as configurações do instalador são distribuídos a partir do Servidor de Administração para os dispositivos alvo através de pontos de distribuição.

Além disso, você pode usar pontos de distribuição para transmitir (multicast) a entrega de pacotes de instalação, que permite reduzir significativamente o tráfego de rede ao implementar aplicativos.

Ao transferir pacotes de instalação para dispositivos alvo através dos canais de comunicação entre os Agentes de Rede e o Servidor de Administração, todos os pacotes de instalação que tenham sido preparados para transferência, também serão colocados em cache na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Ao usar múltiplos grandes pacotes de instalação de vários tipos e ao envolver um grande número de pontos de distribuição, o tamanho desta pasta pode aumentar drasticamente.

Os arquivos não podem ser excluídos da pasta FTServer manualmente. Quando os pacotes de instalação originais forem excluídos, os dados correspondentes serão automaticamente excluídos da pasta FTServer.

Todos os dados recebidos nos pontos de distribuição são salvos na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Os arquivos não podem ser excluídos da pasta de $FTCITmp manualmente. Quando as tarefas usando dados desta pasta forem concluídas, o conteúdo desta pasta será automaticamente excluído.

Como os pacotes de instalação são distribuídos sobre os canais de comunicação entre o Servidor de Administração e os Agentes de Rede a partir de um repositório intermediário em um formato otimizado para transferências na rede, nenhuma modificação é permitida nos pacotes de instalação armazenados na pasta original de cada pacote de instalação. Estas modificações não serão automaticamente registradas pelo Servidor de Administração. Se você tiver de modificar os arquivos de pacotes de instalação manualmente (embora seja recomendado evitar este cenário), deverá editar qualquer configuração necessária de um pacote de instalação no Console de Administração. Editar as configurações de um pacote de instalação no Console de Administração faz com que o Servidor de Administração atualize a imagem do pacote na memória no cache que foi preparado para a transferência aos dispositivos alvo.

O gerenciamento do dispositivo reinicia na tarefa de instalação remota

Os dispositivos muitas vezes precisam de um reinício para concluir a instalação remota de aplicativos (em particular no Windows).

Caso a tarefa de instalação remota do Kaspersky Security Center seja usada, no assistente para novas tarefas ou na janela de propriedades da tarefa que foi criada (seção **Reinício do sistema operacional**), será possível selecionar a ação a ser executada quando o dispositivo Windows precisar ser reiniciado:

- **Não reiniciar o dispositivo**. Neste caso, nenhum reinício automático será executado. Para concluir a instalação, você deve reiniciar o dispositivo (por exemplo, manualmente ou através da tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário serão salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas de instalação em servidores e em outros dispositivos onde a operação contínua é crítica.
- **Reiniciar o dispositivo**. Neste caso, o dispositivo sempre é reiniciado automaticamente se um reinício for necessário para a conclusão da instalação. Esta opção é útil para tarefas de instalação em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).
- **Perguntar ao usuário o que fazer**. Neste caso, o lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). A opção **Perguntar ao usuário o que fazer** é a mais adequada para estações de trabalho onde os usuários precisam da possibilidade de selecionar a hora mais conveniente para um reinício.

Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de antivírus

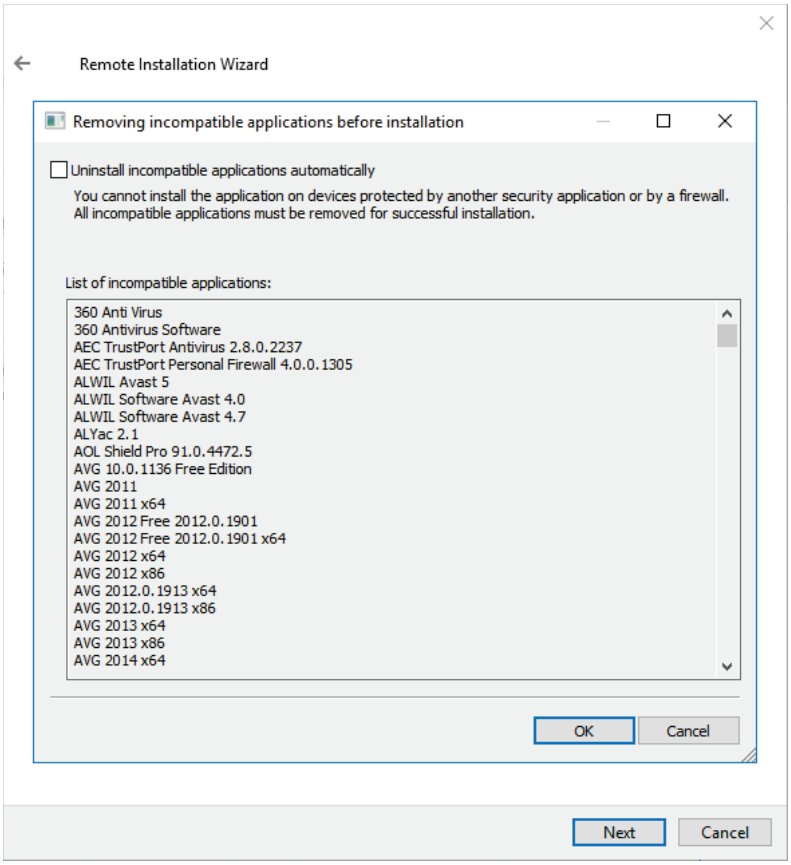
Antes de iniciar a implementação da proteção, você deve ter em mente a possibilidade de atualizar os bancos de dados antivírus (incluindo os módulos de patches automáticas), fornecidos junto com o pacote de distribuição do aplicativo de segurança. É útil atualizar os bancos de dados no pacote de instalação do aplicativo antes de iniciar a implementação (por exemplo, usando o comando correspondente no menu de contexto de um pacote de instalação selecionado). Isto reduzirá o número de reinícios necessários para a conclusão da implementação da proteção em dispositivos alvo. Se a sua instalação remota envolve pacotes de instalação que foram retransmitidos aos Servidores virtuais pelo Servidor de Administração principal, você precisa somente atualizar os bancos de dados no pacote original no Servidor principal. Neste caso, você não tem de atualizar os bancos de dados em pacotes encaminhados em Servidores virtuais.

Removendo aplicativos de segurança de terceiros incompatíveis

A Instalação de aplicativos de segurança da Kaspersky através do Kaspersky Security Center pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. Há dois modos principais para remover os aplicativos de terceiros.

Remoção automática de aplicativos incompatíveis usando o instalador

Ao executar o instalador, ele mostra uma lista de aplicativos incompatíveis com um aplicativo da Kaspersky:



A lista de aplicativos incompatíveis exibida no Assistente de instalação remota

O Kaspersky Security Center detecta softwares incompatíveis. Assim, você pode selecionar a caixa de seleção **Desinstalar automaticamente aplicativos incompatíveis** para continuar a instalação. Se você desmarcar esta caixa de seleção e não desinstalar o software incompatível, um erro ocorre e o aplicativo Kaspersky não é instalado.

A remoção automática de aplicativos incompatíveis tem suporte em vários tipos de instalação.

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis, use a tarefa *Desinstalar aplicativo remotamente*. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar **Na conclusão de outra tarefa** como tipo de agendamento em que a outra tarefa é *Desinstalar aplicativo remotamente*.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Usar as ferramentas da instalação remota de aplicativos no Kaspersky Security Center para executar arquivos executáveis relevantes em dispositivos gerenciados

Usando o Assistente de novo pacote, você pode selecionar qualquer arquivo executável e definir as configurações da linha de comando para ele. Para isto você pode adicionar ao pacote de instalação o próprio arquivo selecionado ou a pasta inteira na qual este arquivo está armazenado. Então você deve criar a tarefa de instalação remota e selecionar o pacote de instalação que foi criado.

Enquanto a tarefa estiver em execução, o arquivo executável especificado com as configurações definidas do prompt de comando serão executadas em dispositivos alvo.

Se você usar instaladores no formato do Microsoft Windows Installer (MSI), o Kaspersky Security Center analisa os resultados da instalação por meio de ferramentas padrão.

Se a licença do Gerenciamento de patches e vulnerabilidades estiver disponível, o Kaspersky Security Center (ao criar um pacote de instalação de qualquer aplicativo suportado no ambiente corporativo), também usa as regras para a instalação e análise dos resultados de instalação que estão no seu banco de dados atualizável.

De outra forma, a tarefa padrão para arquivos executáveis espera pela conclusão do processo de execução e de todos os seus processos secundários. Após a conclusão de todos os processos em execução, a tarefa será concluída dom êxito a despeito do código de retorno do processo inicial. Para modificar tal comportamento desta tarefa, antes de criar a tarefa, você deve modificar manualmente os arquivos .kpd gerados pelo Kaspersky Security Center na pasta do pacote de instalação recentemente criado e suas subpastas.

Para que a tarefa não espere pela conclusão do processo em execução, defina o valor da configuração Wait como 0 na seção [SetupProcessResult]:

Exemplo:

```
[SetupProcessResult]
Wait=0
```

Para a tarefa somente esperar pela conclusão do processo em execução no Windows, não para a conclusão de todos os processos secundários, defina o valor da configuração WaitJob como 0 na seção [SetupProcessResult], por exemplo:

Exemplo:

```
[SetupProcessResult]
WaitJob=0
```

Para que a tarefa seja concluída com êxito ou retorne um erro dependendo do código de retorno do processo em execução, liste os códigos de retorno bem sucedidos na seção [SetupProcessResult_SuccessCodes], por exemplo:

Exemplo:

[SetupProcessResult_SuccessCodes]
0=
3010=

Neste caso, qualquer outro código que os dos listados resultará em um erro retornado.

Para exibir uma sequência de caracteres com um comentário sobre a conclusão bem sucedida da tarefa ou sobre um erro nos resultados da tarefa, insira breves descrições dos erros que correspondem aos códigos de retorno do processo na seção [SetupProcessResult_SuccessCodes] e [SetupProcessResult_ErrorCodes], por exemplo:

Exemplo:

[SetupProcessResult_SuccessCodes]

0 = Instalação concluída com êxito
3010=Um reinício é necessário para concluir a instalação

[SetupProcessResult_ErrorCodes]

1602=Instalação cancelada pelo usuário
1603=Erro fatal durante a instalação

Para usar as ferramentas do Kaspersky Security Center para gerenciar o reinício do dispositivo (se um reinício for necessário para concluir uma operação), liste os códigos de retorno do processo que indicam que um reinício deve ser executado, na seção [SetupProcessResult_NeedReboot]:

Exemplo:

[SetupProcessResult_NeedReboot]
3010=

Monitorar a implementação

Para monitorar a implementação do Kaspersky Security Center e assegurar-se de que um aplicativo de segurança e um Agente de Rede sejam instalados nos dispositivos gerenciados, você deve verificar o sinal luminoso na seção **Implementação**. Este sinal luminoso está localizado no espaço de trabalho do nó Servidor de Administração na janela principal do Console de Administração. O sinal luminoso reflete o status da implementação atual. O número de dispositivos com Agente de Rede e aplicativos de segurança instalados é exibido ao lado do sinal luminoso. Quando qualquer tarefa de instalação estiver em execução, você pode monitorar aqui seu andamento. Se algum erro de instalação ocorrer, o número de erros é aqui exibido. Você pode exibir os detalhes de qualquer erro clicando no link.

Você também pode usar o esquema de implementação no espaço de trabalho da pasta **Dispositivos gerenciados** na guia **Grupos**. O gráfico reflete o processo de implementação, mostrando o número de dispositivos sem o Agente de Rede, com o Agente de Rede, ou com o Agente de Rede e um aplicativo de segurança.

Para obter mais detalhes sobre o andamento da implementação (ou da operação de uma tarefa de instalação específica) abra a janela de resultados da tarefa de instalação remota relevante: clique com o botão direito do mouse na tarefa e selecione **Resultados** no menu de contexto. A janela exibe duas listas: a superior contém os status da tarefa em dispositivos, enquanto a mais baixa contém os eventos de tarefas no dispositivo que está atualmente selecionado na lista superior.

As informações sobre erros de implementação são adicionadas ao Log de Eventos Kaspersky no Servidor de Administração. As informações sobre os erros também estão disponíveis na seleção correspondente de eventos pasta **Relatórios e notificações**, na subpasta **Eventos**.

Configurar os instaladores

Esta seção fornece informações sobre os arquivos de instaladores do Kaspersky Security Center e as configurações de instalação, assim como recomendações sobre como instalar o Servidor de Administração e o Agente de Rede no modo silencioso.

Informações gerais

Os Instaladores dos componentes do Kaspersky Security Center 14.2 (Servidor de Administração, Agente de Rede e Console de Administração) são desenvolvidos com base na tecnologia do Windows Installer. Um pacote MSI é o núcleo de um instalador. Este formato de empacotar permite usar todas das vantagens fornecidas pelo Windows Installer: dimensionalidade, disponibilidade de um sistema de correção, sistema de transformação, instalação centralizada através de soluções de terceiros e o registro transparente com o sistema operacional.

Instalação em modo silencioso (com um arquivo de resposta)

Os instaladores do Servidor de Administração e do Agente de Rede têm o recurso de funcionar com o arquivo de resposta (ss_install.xml), onde os parâmetros para a instalação no modo silencioso sem a participação de usuário estão integradas. O arquivo ss_install.xml está localizado na mesma pasta que o pacote MSI; ele é usado automaticamente durante a instalação no modo silencioso. Você pode ativar o modo de instalação silenciosa com a tecla de linha de comando "/s".

Uma visão geral de uma execução de exemplo segue:

```
setup.exe /s
```

Antes de iniciar o instalador no modo silencioso, leia o Contrato de Licença do Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo no site da Kaspersky.

O arquivo ss_install.xml é uma instância do formato interno dos parâmetros do instalador do Kaspersky Security Center. Os pacotes de distribuição contêm o arquivo ss_install.xml com os parâmetros padrão.

Não modifique manualmente o arquivo ss_install.xml. Este arquivo pode ser modificado pelas ferramentas do Kaspersky Security Center ao editar os parâmetros de pacotes de instalação no Console de Administração.

Para modificar o arquivo de resposta para instalação do Servidor de Administração:

1. Abra o pacote de distribuição do Kaspersky Security Center. Caso use um pacote completo com arquivo EXE, é necessário descompactá-lo.
2. A partir da pasta Servidor, abra a linha de comando e, em seguida, execute o seguinte comando:

   ```
   setup.exe /r ss_install.xml
   ```

   O instalador do Kaspersky Security Center é iniciado.

3. Siga as etapas do assistente para configurar a instalação do Kaspersky Security Center.

Ao concluir o assistente, o arquivo de resposta é modificado automaticamente de acordo com as novas configurações especificadas.

Instalação do Agente de Rede no modo silencioso (sem um arquivo de resposta)

Você pode instalar o Agente de Rede com um pacote .msi único, especificando os valores das propriedades MSI no modo padrão. Este cenário permite que o Agente de Rede seja instalado usando políticas de grupo. Para evitar conflitos entre configurações definidas através dos parâmetros MSI e os parâmetros definidos no arquivo de resposta, você pode desativar o arquivo de resposta ao definir a propriedade `DONT_USE_ANSWER_FILE=1`. O arquivo MSI está localizado no pacote de distribuição do Kaspersky Security Center, na pasta Packages\NetAgent\exec. Um exemplo de uma execução do instalador do Agente de Rede com um pacote .msi é como segue.

A instalação do Agente de Rede no modo silencioso requer o aceite dos termos do Contrato de Licença de Usuário Final. Use o parâmetro `EULA=1` somente se você tiver lido, entende e aceita por completo os termos do Contrato de Licença do Usuário Final.

Exemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Você também pode definir os parâmetros de instalação para um pacote .msi ao preparar o arquivo de resposta com antecedência (um com uma extensão .mst). Este comando aparece como segue:

Exemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Você pode especificar vários arquivos de resposta em um comando único.

Configuração de instalação parcial através de setup.exe

Ao executar a instalação de aplicativos por meio do setup.exe, é possível adicionar os valores de qualquer propriedade de MSI ao pacote MSI.

Este comando aparece como segue:

Exemplo:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parâmetros de instalação do Servidor de Administração

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Servidor de Administração. Todos os parâmetros são opcionais, exceto para o EULA e PRIVACYPOLICY.

Parâmetros da instalação do Servidor de Administração no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do	

	Contrato de Licença (necessária)	termos do Contrato de Licença do Usuário Final. ▪ Outro valor ou nenhum valor – Não aceito os termos do Contrato de Licença (a instalação não é executada).
PRIVACYPOLICY	Aceitação dos termos da Política de Privacidade (necessária)	1 – Estou ciente e concordo que meus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que Eu li e entendo por completo a Política de Privacidade. ▪ Outro valor ou nenhum valor – Não aceito os termos da Política de Privacidade (a instalação não é executada).
INSTALLATIONMODETYPE	Tipo de instalação do Servidor de Administração	Padrão. ▪ Personalizado.
INSTALLDIR	Pasta de instalação do aplicativo	Valor da sequência de caracteres.
ADDLOCAL	Lista de componentes para instalar (separado por vírgulas)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para a instalação correta do Servidor de Administração: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Tamanho da rede	▪ NRT_1_100 – De 1 a 100 dispositivos. NRT_100_1000 – De 101 a 1000 dispositivos. NRT_GREATER_1000 – Mais de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Modo de especificar o usuário para a operação do serviço Servidor de Administração	SrvAccountDefault – A conta de usuário será criada automaticamente. ▪ SrvAccountUser – A conta de usuário é definida manualmente.
SERVERACCOUNTNAME		