instalados foi solicitada com êxito		
As informações gerais sobre o dispositivo móvel foram solicitadas com êxito	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dias
As informações de segurança foram solicitadas com êxito	SECURITYINFO_COMMAND_SUCCESSFULL	30 dias
O dispositivo móvel foi bloqueado com êxito	DEVICELOCK_COMMAND_SUCCESSFULL	30 dias
A senha foi redefinida com êxito	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dias
Os dados foram limpos do dispositivo móvel	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dias
O aplicativo foi instalado com êxito	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dias
O código de resgate para o aplicativo foi definido com êxito	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dias
A lista de aplicativos gerenciados foi solicitada com êxito	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dias
O aplicativo gerenciado foi removido com êxito	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dias
As configurações de roaming foram aplicadas com êxito	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dias

Eventos do Servidor de dispositivos móveis Microsoft Exchange

Esta seção contém informações sobre os eventos relativos a um Servidor de dispositivos móveis do Microsoft Exchange.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de

		armazenamento padrão
Falha em limpar os dados no dispositivo móvel	WIPE_FAILED	30 dias
Não foi possível excluir as informações sobre a conexão do dispositivo móvel da caixa de correio	DEVICE_REMOVE_FAILED	30 dias
Não é possível aplicar a política ActiveSync à caixa de correio	POLICY_APPLY_FAILED	30 dias
Erro de funcionamento do aplicativo	PRODUCT_FAILURE	30 dias
Falha ao modificar o estado da funcionalidade ActiveSync	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 dias

Eventos informativos do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Um novo dispositivo móvel foi conectado	NEW_DEVICE_CONNECTED	30 dias
Os dados foram limpos do dispositivo móvel	WIPE_SUCCESSFULL	30 dias

Bloqueio de eventos frequentes

Esta seção fornece informações sobre como gerenciar e remover o bloqueio de eventos frequentes.

Sobre o bloqueio de eventos frequentes

Um aplicativo gerenciado, por exemplo, Kaspersky Endpoint Security for Windows, instalado em um ou vários dispositivos gerenciados, pode enviar muitos eventos do mesmo tipo ao Servidor de Administração. Receber eventos frequentes pode sobrecarregar o banco de dados do Servidor de Administração e sobrepor-se a outros eventos. O Servidor de Administração começa a bloquear os eventos mais frequentes quando o número de todos os eventos recebidos excede o limite especificado para o banco de dados.

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes. Você não pode bloquear os eventos frequentes ou escolher quais eventos bloquear.

Caso queira saber se um evento está bloqueado, é possível visualizar a lista de notificações ou visualizar se o evento está presente na seção **Bloqueando eventos frequentes** das propriedades do servidor de administração. Se o evento estiver bloqueado, você pode fazer o seguinte:

Se deseja evitar a substituição do banco de dados, pode continuar bloqueando o recebimento desse tipo de evento.

- Se deseja, por exemplo, localizar o motivo do envio de eventos frequentes ao Servidor de Administração, pode desbloquear os eventos frequentes e continuar recebendo os eventos deste tipo de qualquer maneira.
- Se quiser continuar recebendo os eventos frequentes até que sejam bloqueados novamente, pode remover o bloqueio dos eventos frequentes.

Gerenciando o bloqueio de eventos frequentes

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes, mas você pode desbloquear e continuar a recebê-los. Você também pode bloquear o recebimento de eventos frequentes que desbloqueou anteriormente.

Para gerenciar o bloqueio de eventos frequentes:

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 **Bloqueando eventos frequentes**.
3. Na seção **Bloqueando eventos frequentes**:
   - Se deseja desbloquear o recebimento de eventos frequentes:
     a. Selecione os eventos frequentes que deseja desbloquear e clique no botão **Excluir**.
     b. Clique no botão **Salvar**.

   Se deseja bloquear o recebimento de eventos frequentes:
     a. Selecione os eventos frequentes que deseja bloquear e clique no botão **Bloquear**.
     b. Clique no botão **Salvar**.

O Servidor de Administração recebe os eventos frequentes desbloqueados e não recebe os eventos frequentes bloqueados.

Removendo o bloqueio de eventos frequentes

Você pode remover o bloqueio de eventos frequentes e começar a recebê-los até que o Servidor de Administração os bloqueie novamente.

Para remover o bloqueio de eventos frequentes:

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 **Bloqueando eventos frequentes**.

3. Na seção **Bloqueando eventos frequentes**, selecione os tipos de eventos frequentes para os quais deseja remover o bloqueio.

4. Clique no botão **Remover do bloqueio**.

O evento frequente é removido da lista de eventos frequentes. O Servidor de Administração receberá eventos deste tipo.

Recebendo eventos do Kaspersky Security for Microsoft Exchange Servers

As informações sobre os eventos durante a operação de aplicativos gerenciados, como o Kaspersky Endpoint Security for Windows, são transferidas de dispositivos gerenciados e registradas no banco de dados do Servidor de Administração. Por padrão, os eventos do Kaspersky Security for Microsoft Exchange Servers versão 9.0 MR6 e anteriores não são registrados no banco de dados do Servidor de Administração. Caso o Kaspersky Security for Microsoft Exchange Servers versão 9.0 MR6 e anterior esteja instalado nos dispositivos gerenciados na sua organização e caso queira receber os eventos deste aplicativo, ative o registro de eventos para o aplicativo com o uso do utilitário klscflag.

Para habilitar o registro de eventos para o Kaspersky Security for Microsoft Exchange Servers:

1. No dispositivo do Servidor de Administração, execute o prompt de comando do Windows em uma conta com direitos de administrador.

2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center (geralmente, C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Execute um dos seguintes comandos:

   - Para o Servidor de Administração instalado em um cluster de failover do Windows Server:

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Para o Servidor de Administração instalando em um nó de cluster de failover da Kaspersky Security Center:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Para o Servidor de Administração que não está funcionando em um cluster:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

   O registro de eventos do Kaspersky Security for Microsoft Exchange Servers está ativado.

Para o Kaspersky Security for Microsoft Exchange Servers, não é possível definir o prazo de armazenamento para os eventos ou selecionar quais eventos devem ser salvos no repositório do Servidor de Administração. É possível definir o número máximo de eventos que podem ser salvos no repositório. A configuração é aplicada aos eventos ebidos de todos os aplicativos da Kaspersky

Notificações e status do dispositivo

Esta seção contém informações sobre como visualizar notificações, configurar a entrega de notificações, usar os status do dispositivo e habilitar a alteração de status do dispositivo.

Usar as notificações

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- Notificações na tela

  Notificações por SMS

- Notificações por e-mail

  Notificações por arquivo executável ou script

Notificações na tela

As notificações na tela alertam para eventos agrupados por níveis de importância (*Crítico*, *Aviso* e *Informativo*).

A notificação na tela pode ter um de dois status:

Revisado. Significa que você executou a ação recomendada para a notificação ou atribuiu esse status da notificação manualmente.

- *Não Revisado*. Significa que você não executou a ação recomendada para a notificação ou não atribuiu esse status da notificação manualmente.

Por padrão, a lista de notificações inclui notificações no status *Não Revisado*.

Você pode monitorar a rede da sua organização visualizando notificações na tela e dando resposta a elas em tempo real.

Notificações por e-mail, por SMS e por arquivo executável ou um script

O Kaspersky Security Center oferece a capacidade de controlar a rede da sua organização enviando notificações sobre qualquer evento que você considera importante. Para qualquer evento, você pode configurar notificações por e-mail, SMS ou executando um arquivo executável ou um script.

Para receber notificações por e-mail ou SMS, você pode decidir a sua resposta para um evento. Essa resposta deve ser a mais apropriada para a rede da sua organização. Executando um arquivo executável ou um script, você predefine uma resposta para um evento. Você também pode considerar a execução de um arquivo executável ou um script como uma resposta primária para um evento. Após a execução do arquivo executável, você pode tomar :ras medidas para responder ao evento.

Visualização de notificações na tela

Você pode visualizar notificações na tela de três maneiras:

Na seção **Monitoramento e relatórios** → **Notificações**. Aqui, você pode exibir notificações relacionadas a categorias predefinidas.

Em uma janela separada que pode ser aberta, não importa qual seção está sendo usada no momento. Neste caso, você pode marcar notificações como revisadas.

- No widget **Notificações por nível de gravidade selecionado** na seção **Monitoramento e relatórios** → **Painel**.
  No widget, você pode exibir apenas notificações de eventos que estão nos níveis de importância *Crítico* e *Aviso*.

Você pode realizar ações, por exemplo, responder a um evento.

Para visualizar notificações de categorias predefinidas:

1. No menu principal, vá para **Monitoramento e relatórios** → **Notificações**.

   A categoria **Todas as notificações** é selecionada no painel esquerdo, e no painel direito todas as notificações são exibidas.

2. No painel esquerdo, selecione uma das categorias:

   - **Implementação**
   - **Dispositivos**

     Proteção
   - **Atualizações** (esta inclui notificações sobre aplicativos Kaspersky disponíveis para download e notificações sobre atualizações de banco de dados de antivírus que foram baixadas)
   - **Prevenção de Exploit**
   - **Servidor de Administração** (esta inclui eventos relacionados apenas ao Servidor de Administração)
   - **Links úteis** (esta inclui links para recursos da Kaspersky, por exemplo, Suporte Técnico da Kaspersky, fórum da Kaspersky, página de renovação de licença ou a Enciclopédia de TI da Kaspersky)

     Notícias da Kaspersky (esta inclui informações sobre versões de aplicativos Kaspersky)

   Uma lista de notificações da categoria selecionada é exibida. A lista contém o seguinte:

- Ícone relacionado ao tópico da notificação: implementação ( ), proteção ( ), atualizações ( ), gerenciamento de dispositivo ( ), Prevenção de Exploits ( ), Servidor de Administração ( ).
- Nível de importância da notificação. As notificações dos seguintes níveis de importância são exibidas: **Notificações críticas** ( ), **Notificações de advertência** ( ), **Notificações de informação**. As notificações na lista são agrupadas por níveis de importância.
- **Notificação**. Contém uma descrição da notificação.

- **Ação**. Contém um link para uma ação rápida que recomendamos que você execute. Por exemplo, clicando neste link, você pode prosseguir para o repositório e instalar aplicativos de segurança em dispositivos ou visualizar uma lista de dispositivos ou uma lista de eventos. Depois que executar a ação recomendada para a notificação, essa notificação será atribuída ao status *Revisado*.
- **Status registrado**. Contém o número de dias ou horas que se passaram a partir do momento em que a notificação foi registrada no Servidor de Administração.

Para exibir notificações na tela em uma janela separada pelo nível de importância:

1. No canto superior direito do Kaspersky Security Center Web Console, clique no ícone sinalizador ( ).

   Caso o ícone sinalizador tenha um ponto vermelho, isso significa que há notificações que não foram analisadas.

   Uma janela é exibida listando as notificações. Por padrão, a guia **Todas as notificações** está selecionada, e as notificações estão agrupadas pelo nível de importância: *Crítico*, *Aviso* e *Informativo*.

2. Selecione a guia **Sistema**.

   A lista de notificações de níveis de importância *Crítico* ( ) e *Advertência* ( ) é exibida. A lista de notificações inclui o seguinte:

   - Marcador de cores. As notificações críticas estão marcadas em vermelho. As notificações de aviso estão marcadas em amarelo.
   - Ícone que indica o tópico da notificação: implementação ( ), proteção ( ), atualizações ( ), gerenciamento de dispositivo ( ), Prevenção de Exploits ( ), Servidor de Administração ( ).
   - Descrição da notificação.
   - Ícone sinalizador. O ícone sinalizador ficará cinza caso as notificações tenham recebido o status *Não Analisado*. Quando o ícone sinalizador cinza é selecionado e o status *Analisado* é atribuído para uma notificação, a cor do ícone muda para branca.
   - Link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.
   - O número de dias que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.

3. Selecione a guia **Mais**.

   A lista de notificações de nível de importância *Informativo* é exibida.

   A organização da lista é a mesma da lista na guia **Sistema** (veja a descrição acima). A única diferença é a ausência de um marcador de cores.

Você pode filtrar notificações pelo intervalo de datas quando elas tiverem sido registradas no Servidor de Administração. Use a caixa de seleção **Mostrar filtro** para gerenciar o filtro.

Para exibir notificações na tela no widget:

1. Na seção **Painel**, selecione **Adicionar ou restaurar widget da Web**.
2. Na janela exibida, clique na categoria **Outro**, selecione o widget **Notificações por nível de gravidade selecionado** e clique em Adicionar.

O widget agora aparece na guia **Painel**. Por padrão, as notificações do nível de importância *Crítico* são exibidas no widget.
Você pode clicar no botão **Configurações** no widget e alterar as configurações de widget para exibir notificações do nível de importância *Aviso*. Ou você pode adicionar outro widget: **Notificações por nível de gravidade selecionado**, com um nível de importância *Aviso*.
A lista de notificações no widget é limitada pelo seu tamanho e inclui duas notificações. Essas duas notificações estão relacionadas aos eventos mais recentes.

A lista de notificações no widget inclui o seguinte:

- Ícone relacionado ao tópico da notificação: implementação ( ), proteção ( ), atualizações ( ), gerenciamento de dispositivo ( ), Prevenção de Exploits ( ), Servidor de Administração ( ).
- Descrição da notificação com um link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.
- O número de dias ou o número de horas que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.
- Link para outras notificações. Clicando nesse link, você é transferido para a visualização de notificações na seção **Notificações** em **Monitoramento e relatórios**.

Sobre os status do dispositivo

O Kaspersky Security Center atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*
- *Advertência* ou *Advertência/Visível*
- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	▪ O botão de alternar é ativado. ▪ O botão de alternar é desativado.

Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de *verificação de malwares*, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	Parado. ▪ Pausada. Executando.
A verificação de vírus não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.
A reinicialização é necessária	O dispositivo está visível na rede, mas um aplicativo requer o reinício do dispositivo por mais tempo do que o intervalo de tempo especificado e para um dos motivos selecionados.	Mais de 0 minuto.
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	▪ O botão de alternar é desativado. ▪ O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	▪ Crítico. ▪ Alto. Médio. ▪ Ignorar se a vulnerabilidade não puder ser corrigida. Ignorar se uma

		atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	▪ O botão de alternar é desativado. ▪ O botão de alternar é ativado.
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Mais de 0 dias.
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa *executar a sincronização com o Windows Update* não foi executada dentro do intervalo de tempo especificado.	Mais de 1 dia.
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	▪ Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). ▪ Não está em conformidade com a política devido a um erro. ▪ Reiniciar é necessário ao aplicar a política. ▪ Nenhuma política de criptografia está especificada. ▪ Sem suporte. ▪ Ao aplicar a política.
As configurações do dispositivo	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	O botão de alternar é

móvel não estão em conformidade com a política		▪ O botão de alternar é ativado.
Incidentes não processados detectados	Alguns incidentes não processados foram encontrados no dispositivo. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador.	O botão de alternar é desativado. ▪ O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado.	▪ O botão de alternar é desativado. O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB.
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	▪ O botão de alternar é desativado. ▪ O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é diferente do seguinte: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	O botão de alternar é desativado. ▪ O botão de alternar é ativado.

O Kaspersky Security Center lhe permite definir a troca automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendida. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, se por padrão a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente recebe o status *Advertência*. Se o valor for **Mais de 7 dias**, é atribuído o status *Crítico*.

Se você atualizar o Kaspersky Security Center da versão anterior, os valores do **Os bancos de dados estão desatualizados** condição para atribuir o status *Crítico* ou *Advertência* não mudam.

Quando o Kaspersky Security Center atribui um status a um dispositivo, para algumas condições (consulte a coluna Descrição da condição), o sinalizador de visibilidade é levado em consideração. Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição Os bancos de dados estão desatualizados foi atendida e, mais tarde, o sinalizador de visibilidade foi definido para o dispositivo, então o dispositivo recebe o status *OK*.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Se especificados, definir como Crítico**, ative a condição para alterar o status de um dispositivo para *Crítico*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.
6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.
   Os valores não podem ser definidos e para cada condição.
9. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.

3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.
5. No painel direito, na seção **Se especificados, definir como Advertência**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Configurar a entrega de notificações

Você pode configurar a notificação sobre eventos que ocorrem no Kaspersky Security Center. Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- E-mail – Sempre que ocorre um evento, Kaspersky Security Center envia uma notificação para os endereços de e-mail especificados.
- SMS – Sempre que ocorre um evento, Kaspersky Security Center envia uma notificação para os números de telefone especificados.

  Arquivo executável – sempre que ocorre um evento, o arquivo executável é executado no Servidor de Administração.

Para configurar a entrega de notificação de eventos que ocorrem no Kaspersky Security Center:

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

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Clique na seção **Notificação** e, no painel direito, selecione a guia do método de notificação desejado:

   - E-mail

A guia **E-mail** permite-lhe configurar a notificação do evento por e-mail.
No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.
No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

Endereço IPv4 ou IPv6

- Nome da rede Windows (nome NetBIOS) do dispositivo

Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Se você ativar a opção **Usar a autenticação ESMTP**, pode especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar certificados para uma conexão TLS clicando no link **Especificar certificados**:

Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável.
O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

No campo **Assunto**, especifique o assunto do e-mail. Você pode deixar este campo vazio.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável determinada pelo modelo selecionado é colocada automaticamente no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.
O campo **Mensagem de notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.
Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

- SMS

A guia **SMS** permite-lhe configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS são enviadas por meio de um gateway de correio.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Caso a opção **Usar a autenticação ESMTP** seja ativada, será possível especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar o arquivo de certificado do servidor SMTP clicando no link **Especificar certificados**:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável.

O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Assunto**, especifique o assunto do e-mail.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável segundo o modelo selecionado é inserida no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso. Aviso: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

No campo **Números de telefone dos destinatários de mensagens SMS**, especifique os números de celular dos destinatários da notificação de SMS.

O campo **Mensagem de notificação**, especifique um texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto pode incluir parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.
Clique em **Enviar mensagem de teste** para verificar se você configurou as notificações adequadamente: o aplicativo envia uma notificação de teste ao destinatário especificado.

- **Arquivo executável a ser executado**

Se este método de notificação estiver selecionado, no campo de entrada, você pode especificar o aplicativo que será iniciado quando ocorre um evento.

No campo **O arquivo executável que será executado no Servidor de Administração quando um evento ocorrer**, especifique a pasta e o nome do arquivo a ser executado. Antes de especificar o arquivo, prepare-o e especifique os espaços reservados que definem os detalhes do evento a serem enviados na mensagem de notificação. A pasta e o arquivo especificados devem estar localizados no Servidor de Administração.

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

3. Na guia, defina as configurações de notificação.

4. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

As configurações de entrega de notificação salvas são aplicadas a todos os eventos que ocorrem no Kaspersky Security Center.

Você pode ignorar as configurações de entrega de notificações para certos eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, de uma política ou de um aplicativo.

Notificações de evento exibidas executando um arquivo executável

O Kaspersky Security Center pode notificar o administrador sobre os eventos nos dispositivos cliente, executando um arquivo executável. O arquivo executável deve conter outro arquivo executável com marcadores de posição do evento a enviar para o administrador.

Marcadores de posição para descrever um evento

Marcador de posição	Descrição do marcador de posição
%SE\	

%COMPUTER%	Nome do dispositivo onde ocorreu o evento
%DOMAIN%	Domínio
%EVENT%	Evento
%DESCR%	Descrição de evento
%RISE_TIME%	Hora de criação
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome da tarefa
%KL_PRODUCT%	Agente de Rede
%KL_VERSION%	Número da versão do Agente de Rede
%HOST_IP%	Endereço IP
%HOST_CONN_IP%	Endereço IP de conexão

Exemplo:

As notificações de eventos são enviadas através de um arquivo executável (como script1.bat) dentro do qual outro arquivo executável (como script2.bat) com o marcador de posição %COMPUTER% é executado.

Quando um evento ocorrer, o arquivo script1.bat é executado no dispositivo do administrador, o qual, por sua vez, executa o arquivo script2.bat com o marcador de posição %COMPUTER%. O administrador recebe o nome do dispositivo no qual o evento ocorreu.

Novidades da Kaspersky

Esta seção descreve como usar, configurar e desativar o recebimento de Novidades da Kaspersky.

Sobre as Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios** → **Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. O Kaspersky Security Center atualiza periodicamente as informações da seção, removendo informações antigas e adicionando novas.

O Kaspersky Security Center mostra apenas os anúncios da Kaspersky relacionados ao Servidor de Administração conectado atualmente e aos aplicativos Kaspersky instalados nos dispositivos gerenciados deste Servidor de Administração. Os anúncios são mostrados individualmente para qualquer tipo de Servidor de Administração, seja principal, secundário ou virtual.

O Servidor de Administração deve ter uma conexão com a internet para receber os informativos da Kaspersky.

Os informativos incluem informações dos seguintes tipos:

- Comunicados relacionados à segurança

Os informativos relacionados à segurança têm como objetivo manter os aplicativos da Kaspersky instalados em sua rede atualizados e totalmente funcionais. Os informativos podem incluir informações sobre atualizações críticas para aplicativos da Kaspersky, correções para vulnerabilidades encontradas e maneiras de corrigir outros problemas em aplicativos da Kaspersky. Informativos relacionados à segurança são ativados por padrão. Se não deseja receber informações sobre novidades da Kaspersky, pode desativar este recurso.

Para mostrar a você as informações que correspondem à sua configuração de proteção de rede, o Kaspersky Security Center envia dados para os servidores em nuvem da Kaspersky e recebe apenas os informativos relacionados aos aplicativos Kaspersky instalados na rede. O conjunto de dados que pode ser enviado aos servidores é descrito no Contrato de Licença do Usuário Final aceito por você ao instalar o Servidor de Administração do Kaspersky Security Center.

- Informativos de marketing

  Informativos de marketing incluem informações sobre ofertas especiais para os aplicativos da Kaspersky, anúncios e notícias da Kaspersky. Informativos de marketing estão desativados por padrão. Você recebe esse tipo de informativo apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar os informativos de marketing desativando a KSN.

  Para que você visualize apenas informações relevantes que podem ser úteis na proteção de seus dispositivos de rede e em suas tarefas diárias, o Kaspersky Security Center envia dados para os servidores Kaspersky na nuvem e coleta os informativos apropriados. O conjunto de dados que pode ser enviado aos servidores é descrito na seção Dados Processados do Declaração da KSN.

As novas informações são divididas nas seguintes categorias, de acordo com a importância:

1. Informações críticas
2. Notícias importantes
3. Advertência
4. Informação

Quando as novas informações são exibidas na seção Novidades Kaspersky, o Kaspersky Security Center Web Console exibe um rótulo com uma notificação correspondente ao nível de importância da informação. Você pode clicar no rótulo para ver a notícia na seção Novidades Kaspersky.

Você pode especificar as configurações de Novidades Kaspersky, incluindo as categorias de informações que deseja receber e onde exibir o rótulo de notificação.

Especificando configurações para receber as Novidades Kaspersky

Na seção Novidades Kaspersky, você pode especificar as configurações de Novidades Kaspersky, incluindo as categorias de notícias que deseja receber e onde exibir o rótulo de notificação.

Para desativar o recebimento das Novidades Kaspersky:

1. No menu principal, vá para **Monitoramento e relatórios** → **Novidades Kaspersky**.
2. Clique no link **Configurações**.

   A janela de configurações de Novidades Kaspersky é aberta.
3. Especificar as seguintes configurações:

- Selecione o nível de importância para as novidades que você deseja ver. As novidades sobre outras categorias não serão exibidas.
- Selecione onde você deseja que o rótulo de notificação seja exibido. O rótulo pode ser exibido em todas as seções do console ou na seção **Monitoramento e relatórios** e suas subseções.

4. Clique no botão **OK**.

   As configurações da seção Novidades Kaspersky estão especificadas.

Desativando o recebimento de Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios** → **Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Os informativos da Kaspersky incluem dois tipos de informações: informativos relacionados à segurança e de marketing. Você pode desativar os informativos de cada tipo separadamente.

Para desativar informativos relacionados à segurança:

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 **Novidades Kaspersky**.
3. Alterne o botão para a posição **Comunicados relacionados à segurança Desativado**.
4. Clique no botão **Salvar**.

   O recebimento de novidades sobre a Kaspersky está desativado.

Informativos de marketing estão desativados por padrão. Você recebe informativos de marketing apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar este tipo de informativo desativando a KSN.

Para desativar os informativos de marketing:

1. No menu principal, clique no ícone de configurações (🔧) ao lado do nome do Servidor de Administração necessário.
   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.
3. Desative a opção **Usar a Kaspersky Security Network Ativado**.
4. Clique no botão **Salvar**.

   Os informativos de marketing estão desativados.

Visualizando informações sobre detecção de ameaças

É possível ativar ou desativar a exibição de informações sobre alertas.

*Para ativar ou desativar a exibição da seção **Alertas** no menu principal:*

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface.**
2. Na janela aberta de **opções de interface**, ative ou desative a opção **Exibir alertas EDR**.
3. Clique em **Salvar**.

O console exibe a subseção **Alertas** na seção **Monitoramento e relatórios** do menu principal. Na subseção **Alertas**, você pode ver informações sobre a detecção de ameaças nos dispositivos de endpoints. Se você adicionar uma chave de licença para EDR Optimum, o Kaspersky Security Center Web Console exibe automaticamente a subseção **Alertas** na seção **Monitoramento e relatórios** do menu principal. Além disso, você pode adicionar um widget que exibe informações sobre alertas. Além disso, se você instalou o plugin EDR Optimum, pode visualizar informações detalhadas sobre as ameaças detectadas clicando no link **mais detalhes**.

Use o menu **Filtro** para filtrar alertas por data e valores de campo.

O campo **Tipo de objeto** contém os seguintes valores:

desconhecido

- Link de phishing
- vírus
- Cavalo de Troia
- ferramenta maliciosa

backdoor

- worm

outro aplicativo

- Adware
- Pornware
- Programa perigoso empacotado
- Comportamento perigoso

O campo **Resposta automática** contém os seguintes valores:

- Objeto malicioso detectado
- Objeto excluído
- Objeto desinfectado
- Falha ao desinfectar o objeto
- Obje

- Arquivo comprimido protegido por senha detectado

  Vírus detectado

Baixando e excluindo arquivos da quarentena e backup

Esta seção fornece informações sobre como baixar e excluir arquivos da quarentena e backup no Kaspersky Security Center Web Console.

Baixando arquivos da quarentena e backup

É possível baixar os arquivos da quarentena e backup apenas se uma das duas condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo ou se um gateway da conexão estiver em uso. Caso contrário, o download não será possível.

Para salvar uma cópia do arquivo da Quarentena ou Backup para o disco rígido:

1. Execute uma das seguintes ações:

   - Caso queira salvar uma cópia do arquivo da Quarentena, No menu principal, vá para **Operações** → **Repositórios** → **Quarentena**.

     Caso queira salvar uma cópia do arquivo a partir do Backup, No menu principal, vá para **Operações** → **Repositórios** → **Backup**.

2. Na janela que se abre, selecione um arquivo que deseja baixar e clique em **Baixar**.

O download é iniciado. Uma cópia do arquivo que foi colocado em Quarentena no dispositivo cliente é salva na pasta especificada.

Sobre a remoção de objetos dos repositórios de Quarentena, Backup ou Ameaças ativas

Quando os aplicativos de segurança da Kaspersky instalados em dispositivos cliente colocam objetos nos repositórios de Quarentena, Backup ou Ameaças ativas, eles enviam informações sobre os objetos adicionados às seções **Quarentena**, **Backup** ou **Ameaças ativas** no Kaspersky Security Center. Ao abrir uma dessas seções, selecionar um objeto da lista e clicar no botão **Remover**, o Kaspersky Security Center executa uma das seguintes ações ou ambas as ações:

- Remove o objeto selecionado da lista
- Exclui o objeto selecionado do repositório

A ação a ser executada é definida pelo aplicativo da Kaspersky que colocou o objeto selecionado no repositório. O aplicativo da Kaspersky é especificado no campo **Entrada adicionada por**. Consulte a documentação do aplicativo da Kaspersky para obter detalhes sobre qual ação deve ser executada.

Registro da atividade do Kaspersky Security Center Web Console

O registro em log de atividades do Kaspersky Security Center Web Console pode ajudar a investigar as causas de um defeito de software. Quando você contata o Suporte Técnico da Kaspersky sobre um defeito do Kaspersky Security Center Web Console, os especialistas de Suporte Técnico da Kaspersky podem solicitar os arquivos de log do Kaspersky Security Center Web Console a você. Os arquivos de log do Kaspersky Security Center Web Console são armazenados na <pasta de instalação do Kaspersky Security Center Web Console>/logs todo o tempo que você usar o aplicativo. Os arquivos de registro não são enviados a especialistas de Suporte Técnico da Kaspersky automaticamente.

Para ativar o registro da atividade do Kaspersky Security Center Web Console,

Marque a caixa de seleção **Ativar registro de log das atividades do Kaspersky Security Center Web Console** na janela **Configurações de conexão do Kaspersky Security Center Web Console** do Assistente de instalação do Kaspersky Security Center Web Console.

Os arquivos de registro estão no formato de texto.

Os nomes de arquivo de registro estão nos registros de formato-<nome do componente>. <nome do dispositivo>-<número de revisão do arquivo>.AAAA-MM-DD, em que:

<nome do componente> é o nome do componente do Kaspersky Security Center ou é o nome do plugin de gerenciamento do Kaspersky Security Center Web Console.

- <nome de dispositivo> é o nome do dispositivo no qual o <nome do componente> está em execução.
- <número de revisão de arquivo> é o número do arquivo de registro criado para o <nome do componente> que está na operação no <nome do dispositivo>. Em um dia, vários arquivos de registro do mesmo <nome do componente> e <nome do dispositivo> podem ser criados. O tamanho máximo de um arquivo de registro é de 50 megabytes (MB). Quando o tamanho máximo do arquivo for atingido, um novo arquivo de registro será criado. Um novo arquivo de registro <número de revisão de arquivo> é aumentado em 1.
- AAAA, MM e DD são o ano, o mês e o dia quando o registro foi criado pela primeira vez. Quando um novo dia inicia, é criado um novo arquivo de registro.

Integração entre o Kaspersky Security Center e outras soluções

Esta seção descreve como configurar o acesso a partir do Kaspersky Security Center Web Console a outro aplicativo Kaspersky, como o Kaspersky Managed Detection and Response. Esta seção também descreve como configurar a exportação para sistemas SIEM.

Configurar o acesso ao Console da Web KATA / KEDR

O Kaspersky Anti Targeted Attack (KATA) e o Kaspersky Endpoint Detection and Response (KEDR) são dois blocos funcionais da Kaspersky Anti Targeted Attack Platform. Você pode gerenciar esses blocos funcionais através do Console da Web da Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Se você usar o Kaspersky Security Center Web Console e o KATA / KEDR Web Console, poderá configurar o acesso ao KATA / KEDR Web Console diretamente da interface do Kaspersky Security Center Web Console.

Para configurar o acesso ao KATA / KEDR Web Console:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Na guia **Integração**, selecione a seção **KATA**.
3. Digite a URL do Console da Web KATA/KEDR no campo **URL para KATA/KEDR Web Console**.
4. Clique no botão **Salvar**.

A lista suspensa **Gerenciamento avançado** é adicionada à parte superior da janela principal do aplicativo. Você pode usar este menu para abrir o KATA / KEDR Web Console. Depois de clicar em **Advanced Cybersecurity Platform**, uma nova guia é aberta no navegador com a URL especificada.

Estabelecendo uma conexão em segundo plano

Para permitir que o Kaspersky Security Center Web Console execute as tarefas em segundo plano, é preciso estabelecer uma conexão em segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração. Você pode estabelecer uma conexão somente se sua conta tiver o direito de **Modificar ACLs** de objeto na área funcional **Recursos gerais: Permissões de usuário**.

Caso o plug-in do Kaspersky Endpoint Security for Windows 12.3 seja instalado ou caso o plug-in do Kaspersky Endpoint Security for Windows seja atualizado a partir de uma versão anterior a 11.7 e uma conexão em segundo plano ainda não tenha sido estabelecida, uma notificação será exibida informando que é necessário estabelecer uma conexão em segundo plano. Além disso, você terá que conceder à conta de serviço os direitos da área funcional **Recursos gerais: Operações no Servidor de Administração**.

Para estabelecer uma conexão em segundo plano:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Na guia **Integração**, alterne o botão de alternância para estabelecer uma conexão em segundo plano para a posição: **Estabelecer uma conexão em segundo plano para integração Ativado**.
3. Na seção aberta **O serviço que estabelece uma conexão em segundo plano será iniciado no Kaspersky Security Center Web Console Server está instalado**, clique no botão **OK**.

A conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração é estabelecida. O Servidor de Administração cria uma conta para a conexão em segundo plano e essa conta é usada como uma conta de serviço para manter a interação entre o Kaspersky Security Center e outro aplicativo ou solução Kaspersky. O nome desta conta de serviço contém o prefixo NWCSvcUser.

Por motivos de segurança, o Servidor de Administração muda automaticamente a senha da conta de serviço a cada 30 dias. Você não pode excluir a conta de serviço manualmente. O Servidor de Administração exclui esta conta automaticamente se você desativar uma conexão entre serviços. O Servidor de Administração cria uma única conta de serviço para cada Console de Administração e atribui todas as contas de serviço ao grupo de segurança com o nome ServiceNwcGroup. O Servidor de Administração cria este grupo de segurança automaticamente durante o processo de instalação do Kaspersky Security Center. Você não pode excluir este grupo de segurança manualmente.

Trabalhar com o Kaspersky Security Center Web Console em um ambiente de nuvem

Esta seção fornece informações sobre os recursos do Kaspersky Security Center Web Console relacionados à implementação e manutenção do Kaspersky Security Center em ambientes em nuvem, como Amazon Web Services, Microsoft Azure ou Google Cloud.

Para trabalhar em um ambiente em nuvem, é necessária uma licença especial. Se você não tiver essa licença, os elementos da interface relacionados aos dispositivos na nuvem não serão exibidos.

Configuração de ambiente em nuvem no Kaspersky Security Center Web Console

Para configurar o Kaspersky Security Center com o uso deste ambiente, é necessário ter o seguinte:

Credenciais específicas para um ambiente em nuvem:

- Uma função do IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem ou uma conta de usuário IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem (para trabalhar com Amazon Web Services)
- ID do Aplicativo Azure, senha e assinatura (para trabalhar com Microsoft Azure)

  E-mail do cliente do Google, ID do projeto e chave privada (para trabalhar com o Google Cloud)

- Pacotes de instalação:

  Agente de Rede para Windows

  - Agente de Rede para Linux
  - Kaspersky Endpoint Security for Linux

  Plug-in da Web para o Kaspersky Endpoint Security for Linux

- Pelo menos um dos seguintes itens:

  Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)

  - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

O assistente Configurar o ambiente em nuvem inicia automaticamente na primeira conexão com o Servidor de Administração pelo Console de Administração caso o Kaspersky Security Center seja implementado a partir de uma imagem pronta para usar. Também é possível iniciar o assistente de início rápido manualmente a qualquer momento.

Para iniciar o assistente Configurar o ambiente em nuvem manualmente,

No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Configurar ambiente em nuvem**.

O assistente é iniciado.

A média da sessão de trabalho para configuração do ambiente em nuvem é de aproximadamente 15 minutos.

Etapa 1. Verificação dos plug-ins e pacotes de instalação necessários

Essa etapa não será exibida caso tenha todos os plug-ins da Web e pacotes de instalação necessários e listados abaixo.

Para configurar um ambiente na nuvem, é necessário ter os seguintes componentes:

- Pacotes de instalação:
  - Agente de Rede para Windows

    Agente de Rede para Linux
  - Kaspersky Endpoint Security for Linux

  Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
  - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)

    O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server Recomendamos usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server.

O Kaspersky Security Center detecta automaticamente os componentes possuídos e lista apenas os que estão faltando. Baixe os componentes listados clicando no botão **Selecionar os aplicativos para download** e, em seguida, selecione os plug-ins e pacotes de instalação necessários. Depois de baixar um componente, será possível usar o botão **Atualizar** para atualizar a lista de componentes ausentes.

Etapa 2. Licenciar o aplicativo

Esta etapa será exibida apenas se você estiver usando uma BYOL AMI e não tiver ativado o aplicativo com uma licença do Kaspersky Security for Virtualization ou uma licença do Kaspersky Hybrid Cloud Security.

Especifique a chave de licença e clique em **Avançar** para continuar.

A chave de licença é adicionada ao armazenamento do Servidor de Administração.

Se você executar o assistente novamente, essa etapa não será exibida.

Etapa 3. Seleção do ambiente em nuvem e autorização

Esta seção descreve os recursos aplicáveis apenas ao Kaspersky Security Center 12.1 ou a uma versão posterior.

Especificar as seguintes configurações:

- Ambiente em nuvem

  Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center: AWS, Azure ou Google Cloud.

  Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

  Nome da conexão

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.
  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

AWS

Se você selecionou AWS como tipo de segmento da nuvem, precisará de uma função do IAM ou de uma chave de acesso AWS IAM para amostragem adicional do segmento da nuvem.

- **Função do AWS IAM atribuída à instância EC2**

  Selecione esta opção caso tenha uma função do IAM com os direitos necessários para o Servidor de Administração.

- **usuário do AWS IAM**

  Selecione esta opção caso tenha uma chave de acesso AWS IAM. Insira os dados da sua chave:

  - ID da chave de acesso

    A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

  - Chave secreta

A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Azure

Se você selecionou Azure como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

ID do aplicativo Azure

Você criou este ID do aplicativo no portal do Azure.

É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID da assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

Chave de acesso ao armazenamento do Azure

Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para trabalhar com o Kaspersky Security Center.

A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Se você selecionou Google Cloud como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

- **Endereço de e-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

A conexão especificada é salva nas configurações do aplicativo.

O assistente Configurar o ambiente em nuvem permite especificar apenas um segmento. Posteriormente, você poderá especificar mais conexões para gerenciar outros segmentos da nuvem.

Clique em **Avançar** para prosseguir.

Etapa 4. Amostragem de segmentos, configuração da sincronização com a Nuvem e seleção de ações adicionais

Neste passo, a sondagem de segmentos da nuvem é iniciada e um grupo de administração especial para dispositivos na nuvem é criado automaticamente. Os dispositivos detectados durante a sondagem são colocados neste grupo. O agendamento de sondagem de segmentos da nuvem é configurado (a cada 5 minutos, por padrão; é possível alterar essa configuração posteriormente).

Uma regra automática para mover **Sincronizar com a Nuvem** também é criada. Para cada verificação subsequente da rede na nuvem, os dispositivos virtuais detectados serão movidos ao subgrupo correspondente dentro do grupo **Dispositivos gerenciados\Cloud**.

Defina as seguintes configurações:

- **Sincronizar grupos de administração com estrutura de nuvem**

Se essa opção é ativada, o grupo **Nuvem** é automaticamente criado dentro do grupo **Dispositivos gerenciados** e uma descoberta de dispositivos na nuvem é iniciada. As instâncias e máquinas virtuais detectadas durante cada verificação da rede na nuvem são colocadas no grupo Nuvem. A estrutura dos subgrupos de administração dentro deste grupo corresponde à estrutura do seu segmento da nuvem (no AWS, as zonas de disponibilidade e os grupos de posicionamento não são representados na estrutura; no Azure, as sub-redes não são representadas na estrutura). Os dispositivos que não foram identificados como instância no ambiente nuvem estão no grupo **Dispositivos não atribuídos**. Esta estrutura de grupo permite usar tarefas de instalação de grupo para instalar aplicativos antivírus nas instâncias, assim como definir políticas diferentes para grupos diferentes.

Se esta opção estiver desativada, o grupo **Nuvem** também será criado, e a descoberta de dispositivos de nuvem também será iniciada; contudo, os subgrupos que correspondem à estrutura do segmento da nuvem não serão criados no grupo. Todas as instâncias detectadas estão no grupo de administração **Nuvem**, portanto elas são exibidos em uma lista única. Se o seu trabalho com o Kaspersky Security Center necessitar da sincronização, você pode modificar as propriedades da regra **Sincronizar com a nuvem** e forçá-la. Forçar esta regra alterará a estrutura dos subgrupos no grupo Nuvem para que ele coincida com a estrutura do seu segmento da nuvem.

Por padrão, esta opção está desativada.

- **Implementar a proteção**

  Se esta opção estiver selecionada, o assistente cria uma tarefa para instalar aplicativos de segurança nas instâncias. Após a conclusão do assistente, o Assistente de implementação da proteção automaticamente inicia nos dispositivos em seus segmentos da nuvem, e você será capaz de instalar o Agente de Rede e aplicativos de segurança neles.

  O Kaspersky Security Center pode executar a implementação com suas ferramentas nativas. Se você não tiver permissões para instalar os aplicativos nas instâncias do EC2 ou nas máquinas virtuais do Azure, você pode configurar a tarefa de **Instalação remota** manualmente e especificar uma conta com as permissões necessárias. Neste caso, a tarefa de Instalação remota não funcionará para os dispositivos descobertos usando API AWS ou Azure. Essa tarefa só funcionará para os dispositivos descobertos usando a sondagem do Active Directory, de domínios do Windows ou de conjuntos de IPs.

  Se esta opção não está selecionada, o Assistente de implementação da proteção não é iniciado e as tarefas para instalar aplicativos de segurança nas instâncias não são criadas. Você pode executar manualmente ambas estas ações em outro momento.

Se você selecionar a opção Implementar a proteção, a seção **Reiniciando dispositivos** fica disponível. Nesta seção, você deverá escolher o que fazer quando o sistema operacional de um dispositivo de destino precisar ser reiniciado. Selecione se as instâncias deverão ser reiniciadas caso o sistema operacional precise ser reiniciado durante a instalação de aplicativos:

Não reiniciar

Se esta opção for selecionada, o dispositivo não será reiniciado após a instalação do aplicativo de segurança.

- **Reiniciar**

  Se esta opção for selecionada, o dispositivo será reiniciado após a instalação do aplicativo de segurança.

Clique em **Avançar** para prosseguir.