As regras de controle de aplicativos são implementadas por meio de categorias de aplicativos. Você cria categorias de aplicativos definindo critérios específicos. No Kaspersky Security Center, existem três tipos de categorias de aplicativo:

Categoria com conteúdo adicionado manualmente. Você define condições, por exemplo, metadados do arquivo, código de hash do arquivo, certificado do arquivo, categoria KL, caminho do arquivo, para incluir arquivos executáveis na categoria.

Categoria que inclui os arquivos executáveis dos dispositivos selecionados. Você especifica um dispositivo cujos arquivos executáveis são incluídos automaticamente na categoria.

Categoria que inclui os arquivos executáveis da pasta selecionada. Você especifica uma pasta da qual os arquivos executáveis são incluídos automaticamente na categoria.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

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

Kaspersky Security for Virtualization Light Agent

Obter e visualizar uma lista de aplicativos instalados nos dispositivos cliente

O Kaspersky Security Center executa um inventário de todos os softwares instalados nos dispositivos cliente gerenciados que executam o Linux e Windows.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo cliente e, a seguir, transmite esta lista para o Servidor de Administração. São necessários cerca de 10 a 15 minutos para o Agente de Rede atualizar a lista de aplicativos.

Para dispositivos cliente baseados no Windows, o Agente de Rede recebe a maioria das informações sobre os aplicativos instalados do registro do Windows. Para dispositivos cliente baseados em Linux, os gerenciadores de pacotes fornecem ao Agente de Rede informações sobre os aplicativos instalados.

Para exibir a lista de aplicativos instalados nos dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.
   A página exibe uma tabela com os aplicativos instalados nos dispositivos gerenciados. Selecione o aplicativo para visualizar suas propriedades, por exemplo, nome do fornecedor, número da versão, lista de arquivos executáveis, lista de dispositivos nos quais o aplicativo está instalado, lista de atualizações de software disponíveis e lista de vulnerabilidades de software detectadas.

2. É possível agrupar e filtrar os dados da tabela com os aplicativos instalados da seguinte forma:

   Clique no ícone de configurações ( ) no canto superior direito da tabela.
   No menu **Configurações de colunas** resultante, selecione as colunas a serem exibidas na tabela. Para visualizar o tipo de sistema operacional dos dispositivos clientes nos quais o aplicativo está instalado, selecione a coluna **Tipo de sistema operacional**.

   Clique no ícone de filtro ( ) no canto superior direito da tabela e depois, especifique e aplique o critério de filtro no menu resultante.

   A tabela filtrada de aplicativos instalados é exibida.

Para visualizar a lista de aplicativos instalados em um dispositivo gerenciado específico,

No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → **<nome do dispositivo>** → **Avançado** → **Registro de aplicativos**. Neste menu, é possível exportar a lista de aplicativos para um arquivo CSV ou TXT.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

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

  Kaspersky Security for Virtualization Light Agent

Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes

Você pode obter uma lista de arquivos executáveis armazenados em dispositivos gerenciados. Para o inventário de arquivos executáveis, você deve criar uma tarefa de inventário.

O recurso de inventário de arquivos executáveis está disponível para os seguintes aplicativos:

- Kaspersky Endpoint Security for Windows

  Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent e versões posteriores

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para fazer isso, recomendamos executar uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado.

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

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

   A lista de tarefas é exibida.

2. Clique no botão **Adicionar**.
   O Assistente para nova tarefa inicia. Siga as etapas do Assistente.

3. Na página **Nova tarefa**, na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Linux, dependendo do tipo de sistema operacional dos dispositivos clientes.

4. Na lista suspensa **Tipo de tarefa**, selecione **Inventário**.

5. Na página **Concluir a criação da tarefa**, clique no botão **Concluir**.

   Após a conclusão do Assistente para novas tarefas, a tarefa **Inventário** será criada e configurada. Se desejar, você pode alterar as configurações da tarefa criada. A tarefa recém-criada é exibida na lista de tarefas.

Para uma descrição detalhada da tarefa de inventário, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
  Ajuda do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Após a tarefa **Inventário** ser executada, a lista de arquivos executáveis armazenados nos dispositivos gerenciados é formada e você pode visualizá-la.

Durante o inventário, arquivos executáveis nos seguintes formatos são detectados: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Para exibir a lista dos arquivos executáveis armazenados nos dispositivos cliente:

No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.

A página exibe a lista de arquivos executáveis armazenados nos dispositivos cliente.

Para enviar o arquivo executável do dispositivo gerenciado para a Kaspersky:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.
2. Clique no link do arquivo executável que deseja enviar para a Kaspersky.
3. Na janela que é aberta, vá para a seção **Dispositivos** e marque a caixa de seleção do dispositivo gerenciado do qual você deseja enviar o arquivo executável.

   Antes de enviar o arquivo executável, certifique-se de que o dispositivo gerenciado tenha uma conexão direta com o Servidor de Administração marcando a **caixa de seleção Não desconectar do Servidor de Administração**.

4. Clique no botão **Enviar à Kaspersky**.

O arquivo executável selecionado é baixado para envio posterior à Kaspersky.

Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Você pode especificar um conjunto de critérios como um modelo de arquivos executáveis cuja inicialização deseja permitir ou bloquear na sua organização. Com base nos arquivos executáveis correspondentes aos critérios, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativos com conteúdo adicionado manualmente:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Categorias de aplicativos**.

   A página com uma lista de categorias de aplicativos é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Siga as etapas do Assistente.

3. Na página **Selecionar método de criação de categoria** do assistente, selecione a opção **Categoria com conteúdo adicionado manualmente. Os dados dos arquivos executáveis são adicionados manualmente à categoria**.

4. Na página **Condições** do assistente, clique no botão **Adicionar** para adicionar um critério condicional para a inclusão de arquivos na categoria sendo criada.

5. Na página **Critérios da condição**, selecione um tipo de regra para a criação de categoria na lista:

   Da categoria KL

   Se esta opção estiver selecionada, você poderá especificar uma categoria de aplicativos da Kaspersky como a condição para adicionar aplicativos da categoria do usuário. Os aplicativos da categoria da Kaspersky especificada serão adicionados à categoria de aplicativos do usuário.

   Selecionar certificado do repositório

   Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. Arquivos executáveis que tenham sido assinados de acordo com os certificados especificados serão adicionados à categoria de usuário.

   Especificar caminho para o aplicativo (máscaras aceitas)

   Se esta opção estiver selecionada, você poderá especificar o caminho para a pasta no dispositivo cliente contendo os arquivos executáveis a serem adicionados à categoria de aplicativos do usuário.

   - **Unidade removível**

     Se esta opção estiver selecionada, você pode especificar o tipo de mídia (qualquer unidade ou unidade removível) no qual o aplicativo será executado. Os aplicativos que foram executados no tipo de unidade selecionado são adicionados à categoria de aplicativo do usuário.

   - **Hash, metadados ou certificado**:

     - **Selecionar na lista de arquivos executáveis**

       Se esta opção estiver selecionada, você poderá utilizar a lista de arquivos executáveis no dispositivo cliente para selecionar e adicionar aplicativos deles à categoria.

       Selecionar do registro de aplicativos

Se esta opção for selecionada, o registro dos aplicativos será exibido. Você pode selecionar um aplicativo no registro e especificar os seguintes metadados do arquivo:

- Nome do arquivo.
- Versão do arquivo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".

  Nome do aplicativo.
- Versão do aplicativo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
- Fornecedor.

- Especificar manualmente

Se esta opção estiver selecionada, você deve especificar hash do arquivo, metadados ou certificado como a condição para adicionar aplicativos à categoria do usuário.

Hash do arquivo

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações sobre os valores de hash calculado são armazenadas no banco de dados do Servidor de Administração. O armazenamento de valores hash não aumenta significativamente o tamanho do banco de dados.

SHA-256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA-256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA-256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.
- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA-256 hash criptográfica para arquivos da categoria.
- Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

Metadados

Se esta opção for selecionada, você poderá especificar os metadados do arquivo como nome, versão e fornecedor. Os metadados serão enviados ao Servidor de Administração. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos.

Certificado

Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. Arquivos executáveis que tenham sido assinados de acordo com os certificados especificados serão adicionados à categoria de usuário.

- **Do arquivo ou do pacote MSI/pasta arquivada**

Se esta opção estiver selecionada, você poderá especificar um arquivo de instalador MSI como a condição para adicionar aplicativos à categoria de usuário. Os metadados do instalador do aplicativo serão enviados ao Servidor de Administração. Os aplicativos para os quais o instalador de metadados for o mesmo para o instalador MSI especificado, são adicionados à categoria de aplicativos do usuário.

O critério selecionado é adicionado à lista de condições.

Você pode adicionar quantos critérios para a categoria de aplicativo de criação forem necessários.

6. Na página **Exclusões** do assistente, clique no botão **Adicionar** para adicionar um critério condicional exclusivo para excluir arquivos da categoria sendo criada.
7. Na página **Critérios da condição**, selecione um tipo de regra na lista tal como você selecionou um tipo de regra para a criação da categoria.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

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

  Kaspersky Security for Virtualization Light Agent

Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados

Você pode usar arquivos executáveis de dispositivos selecionados como um modelo de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis dos dispositivos selecionados, você pode criar uma categoria de aplicativo e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativo que inclui arquivos executáveis de dispositivos selecionados:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Categorias de aplicativos**.
   A página com uma lista de categorias de aplicativos é exibida.
2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão Avançar.
3. Na página **Selecionar método de criação de categoria** do assistente, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis dos dispositivos selecionados. Esses arquivos executáveis são processados automaticamente e suas métricas são adicionadas à categoria**.
4. Clique em **Adicionar**.
5. Na janela que se abre, selecione um ou mais dispositivos cujos arquivos executáveis serão usados para criar a categoria de aplicativos.
6. Especificar as seguintes configurações:
   - **Algoritmo de cálculo do valor hash**

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações sobre os valores de hash calculado são armazenadas no banco de dados do Servidor de Administração. O armazenamento de valores hash não aumenta significativamente o tamanho do banco de dados.

SHA-256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA-256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA-256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA-256 hash criptográfica para arquivos da categoria.

Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

A caixa de seleção **Calcular o SHA-256 para arquivos nessa categoria (suportado pelo Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** é selecionada por padrão.

A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- Sincronizar dados com o repositório do Servidor de Administração

Selecione esta opção se você desejar que o Servidor de Administração verifique periodicamente as alterações na pasta (ou pastas) especificada.

Por padrão, esta opção está desativada.

Se você ativar esta opção, especifique o período (em horas) para verificar as alterações nas pastas especificadas. Por padrão, o intervalo de verificação é de 24 horas.

Tipo de arquivo

Nesta seção, você pode especificar o tipo de arquivo usado para criar a categoria de aplicativo.

Todos os arquivos. Todos os arquivos são levados em consideração durante a criação da categoria. Por padrão, esta opção está selecionada.

Somente arquivos fora das categorias de aplicativos. Somente arquivos fora das categorias de aplicativos são levados em consideração durante a criação da categoria.

- Pastas

  Nesta seção, você pode especificar quais pastas dos dispositivos selecionados contendo arquivos usados para criar a categoria de aplicativos.

  Todas as pastas. Todas as pastas são levadas em consideração para a categoria de criação. Por padrão, esta opção está selecionada.

  Pasta especificada. Somente a pasta especificada é levada em consideração para a categoria de criação. Se você selecionar esta opção, deverá especificar o caminho para a pasta.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Criar uma categoria de aplicativo que inclua arquivos executáveis da pasta selecionada

Você pode usar arquivos executáveis da pasta selecionada como um padrão de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis da pasta selecionada, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativo que inclui arquivos executáveis da pasta selecionada:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.
   A página com uma lista de categorias de aplicativos é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na página **Selecionar método de criação de categoria** do assistente, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis de uma pasta específica. Os arquivos executáveis de aplicativos copiados para a pasta especificada são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Especifique a pasta cujos arquivos executáveis serão usados para criar a categoria do aplicativo.

5. Defina as seguintes configurações:

   Incluir bibliotecas de link dinâmico (DLL) nessa categoria

   A categoria de aplicativo inclui bibliotecas de link dinâmico (arquivos no formato de DLL), e o componente Controle de Aplicativos registra as ações de tais bibliotecas que ocorrem no sistema. A inclusão de arquivos DLL na categoria pode abaixar o desempenho do Kaspersky Security Center.

   Por padrão, esta caixa de seleção está desmarcada.

   Incluir dados de script nesta categoria

A categoria do aplicativo inclui dados sobre scripts, e os scripts não são bloqueados pelo Proteção Contra Ameaças da Web. Incluir os dados de script na categoria pode diminuir o desempenho do Kaspersky Security Center.

Por padrão, esta caixa de seleção está desmarcada.

- Algoritmo de cálculo do valor hash: **Calcular o SHA-256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores) / Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações sobre os valores de hash calculado são armazenadas no banco de dados do Servidor de Administração. O armazenamento de valores hash não aumenta significativamente o tamanho do banco de dados.

SHA-256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA-256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA-256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA-256 hash criptográfica para arquivos da categoria.

Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

A caixa de seleção **Calcular o SHA-256 para arquivos nessa categoria (suportado pelo Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** é selecionada por padrão.

A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

Forçar verificação da pasta para procurar alterações

Se esta opção estiver ativada, o aplicativo verifica regularmente a pasta de inclusão de conteúdo à categoria, buscando por alterações. Você pode especificar a frequência de verificações (em horas) no campo de entrada próximo da caixa de seleção. Por padrão, o tempo de intervalo entre verificações forçadas é de 24 horas.
Se esta opção estiver ativada, o aplicativo não força nenhuma verificação da pasta. O Servidor tenta acessar arquivos se eles tiverem sido modificados, adicionados ou excluídos.

Por padrão, esta opção está desativada.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativo na configuração do Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows

  Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Visualizando a lista de categorias de aplicativo

Você pode visualizar a lista de categorias de aplicativos configuradas e as configurações de cada uma delas.

Para visualizar a lista de categorias de aplicativos,

No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Categorias de aplicativos**.

A página com uma lista de categorias de aplicativos é exibida.

Para visualizar propriedades de uma categoria de aplicativos,

Clique no nome da categoria de aplicativos.

A janela de propriedades da categoria de aplicativos é exibida. As propriedades estão agrupadas em várias guias.

Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

Após você criar as categorias do Controle de Aplicativos, poderá usá-las para configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows.

Para configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows:

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

Uma página com uma lista de políticas é exibida.

2. Clique na Política do **Kaspersky Endpoint Security for Windows**.

   A janela Propriedades da política será aberta.

3. Acesse **Configurações do aplicativo** → **Controles de Segurança** → **Controle de Aplicativos**.

   A janela **Controle de Aplicativos** com as configurações de Controle de Aplicativos é exibida.

4. A opção **Controle de Aplicativos** está ativada por padrão. Certifique-se de que o botão de alternância **Controle de Aplicativos DESABILITADO** esteja na posição desabilitada.

5. No configurações de bloqueio **Configurações de Controle de Aplicativos**, ative o modo de operação para aplicar as Regras de Controle de Aplicativos e permita que o Kaspersky Endpoint Security for Windows bloqueie a inicialização de aplicativos.

   Se você quiser testar as Regras de Controle de Aplicativos, na seção **Configurações de Controle de Aplicativos**, ative o modo de teste. No modo de teste, o Kaspersky Endpoint Security for Windows não bloqueia a inicialização de aplicativos, mas registra no relatório informações sobre as regras acionadas. Clique no link **Ver relatório** para visualizar esta informação.

6. Ative a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore o carregamento dos módulos DLL quando os aplicativos forem iniciados pelos usuários. As informações sobre o módulo e o aplicativo que carregou o módulo serão salvas em um relatório.

   O Kaspersky Endpoint Security for Windows monitora apenas os módulos DLL e drivers carregados após a opção **Controlar carregamento dos módulos DLL** tiver sido selecionada. Reinicie o computador após selecionar a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security for Windows ter sido iniciado.

7. (Opcional) No bloco **Modelos de mensagem**, altere o modelo da mensagem exibida quando um aplicativo é impedido de iniciar e o modelo da mensagem de e-mail enviada para você.

8. Nas configurações de bloqueio **Modo de Controle de Aplicativos**, selecione o modo **Lista de bloqueio** ou **Lista de permissão**.
   Por padrão, o modo **Lista de bloqueio** é selecionado.

9. Clique no link **Configurações das listas de regras**.

   A janela **Listas de bloqueio e permissão** é aberta para permitir a adição de uma categoria de aplicativo. Por padrão, a guia **Lista de bloqueio** é selecionada se o modo **Lista de bloqueio** estiver selecionado ou a guia **Lista de aprovação** é selecionada se o modo **Lista de aprovação** estiver selecionado.

10. Na janela **Listas de bloqueio e de aprovação**, clique no botão **Adicionar**.

    A janela **Regra de Controle de Aplicativos** abre.

11. Clique no link **Escolha uma categoria**.
    A janela **Categoria de Aplicativo** é aberta.

12. Adicione a categoria de aplicativo (ou categorias) que você criou anteriormente.

    Você pode editar as configurações de uma categoria criada clicando no botão **Editar**.
    Você pode criar uma nova categoria clicando no botão **Adicionar**.

    Você pode excluir uma categoria da lista clicando no botão **Excluir**.

13. Após lista de categorias de aplicativos estiver completa, clique no botão **OK**.
    A janela **Categoria de Aplicativos** é fechada.

14. Na janela Regra de **Controle de Aplicativos**, na seção **Pessoas e seus direitos**, crie uma lista de usuários e grupos de usuários para aplicar a regra de Controle de Aplicativos.
15. Clique no botão **OK** para salvar as configurações e fechar a janela **Regra de Controle de Aplicativos**.
16. Clique no botão **OK** para salvar as configurações e fechar a janela **Listas de bloqueio e de aprovação**.
17. Clique no botão **OK** para salvar as configurações e fechar a janela **Controle de Aplicativos**.
18. Feche a janela com as configurações da política do Kaspersky Endpoint Security for Windows.

O Controle de Aplicativos está configurado. Após a política ter sido propagada para os dispositivos cliente, a inicialização dos arquivos executáveis é gerenciada.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Após configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows, os seguintes eventos serão exibidos na lista de eventos:

Inicialização do aplicativo proibida (evento *Crítico*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras.

Proibida a inicialização do aplicativo em modo de teste (evento *Informativo*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para testar regras.

- **Mensagem ao administrador sobre a proibição de inicialização do aplicativo** (evento de *Advertência*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras e um usuário tiver solicitado acesso ao aplicativo bloqueado para inicialização.

É recomendável criar seleções de eventos para visualizar eventos relacionados à operação do Controle de Aplicativos.

Você pode adicionar arquivos executáveis relacionados aos eventos do Controle de Aplicativos à uma categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode adicionar arquivos executáveis apenas à categoria de aplicativos com conteúdo adicionado manualmente.

Para adicionar arquivos executáveis relativos aos eventos de Controle de Aplicativos para uma categoria de aplicativos:

1. No menu principal, acesse **Monitoramento e relatórios** → **Seleções de eventos**.

   A lista de seleção de eventos é exibida.

2. Selecione a seleção de eventos para visualizar os eventos relacionados ao Controle de Aplicativos e iniciar essa sele

Se você não criou uma seleção de eventos relacionada ao Controle de Aplicativos, poderá selecionar e iniciar uma seleção predefinida, por exemplo, **Eventos recentes**.
A lista de eventos é exibida.

3. Selecione os eventos cujos arquivos executáveis associados você deseja adicionar à categoria de aplicativos e clique no botão **Atribuir à categoria**.
O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

4. Na página do assistente, especifique as configurações relevantes:

   - Na seção **Ação em arquivo executável relacionado ao evento**, selecione uma das seguintes opções:

     - Adicionar a uma nova categoria de aplicativos

       Selecione esta opção se desejar criar uma nova categoria de aplicativo com base nos arquivos executáveis relacionados ao evento.

       Por padrão, esta opção está selecionada.
       Se você selecionou esta opção, especifique um novo nome de categoria.

       Adicionar a uma categoria de aplicativos existente

       Selecione esta opção se você quiser adicionar arquivos executáveis relativos ao evento a uma categoria de aplicativo existente.
       Por padrão, esta opção não está selecionada.

       Se você selecionou essa opção, selecione a categoria de aplicativo com conteúdo adicionado manualmente ao qual você deseja adicionar arquivos executáveis.

   - Na seção **Tipo de regra**, selecione uma das seguintes opções:

     Regras para adicionar às inclusões

     - **Regras para adicionar às exclusões**

   - Na seção **Parâmetro usado como condição**, selecione uma das seguintes opções:

     - Detalhes do certificado (ou hashes SHA-256 para arquivos sem certificado)

       Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

       Cada arquivo tem a sua própria função SHA-256 hash única. Quando você seleciona uma função SHA-256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

       Selecione esta opção se você quiser adicionar às regras de categoria os detalhes do certificado de um arquivo executável (ou a função SHA-256 hash de arquivos sem um certificado).
       Por padrão, esta opção está selecionada.

       Detalhes do certificado (arquivos sem um certificado serão ignorados)

Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

Selecione esta opção se você quiser adicionar os detalhes do certificado de um arquivo executável às regras de categoria. Se o arquivo executável não tiver um certificado, este arquivo será ignorado. Nenhuma informação sobre este arquivo será adicionada à categoria.

- **Somente SHA-256 (arquivos sem hash serão ignorados)**

  Cada arquivo tem a sua própria função SHA-256 hash única. Quando você seleciona uma função SHA-256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função SHA-256 hash do arquivo executável.

- **Somente MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada arquivo tem a sua própria função MD5 hash única. Quando você seleciona uma função MD5 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função MD5 hash do arquivo executável. O cálculo função MD5 hash é suportado por versões do Service Pack 1 do Kaspersky Endpoint Security 10 for Windows e posteriores.

5. Clique em **OK**.

Quando o assistente for concluído, os arquivos executáveis relacionados aos eventos do Controle de Aplicativos serão adicionados à categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode visualizar as configurações da categoria de aplicativos que modificou ou criou.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky

O Kaspersky Security Center Web Console permite executar a instalação remota de aplicativos de terceiros usando pacotes de instalação. Esses aplicativos de terceiros são incluídos em um banco de dados dedicado da Kaspersky. O banco de dados da Kaspersky é criado automaticamente quando a tarefa *Baixar as atualizações no repositório do Servidor de Administração* for executada pela primeira vez.

Para criar um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
2. Clique no botão **Adicionar**.
3. Na página do Assistente de novo pacote aberta, selecione a opção **Selecione um aplicativo no banco de dados da Kaspersky para criar um pacote de instalação** e clique em **Avançar**.
4. Na lista de aplicativos aberta, selecione o aplicativo relevante e clique em **Avançar**.
5. Selecione o idioma de localização relevante na lista suspensa e clique em **Avançar**.

   Esta etapa só será exibida se o aplicativo oferecer várias opções de idioma.

6. Se for solicitado que você aceite um Contrato de Licença para a instalação, na página **Contrato de Licença de Usuário Final** que é aberta, clique no link para ler o Contrato de Licença no site do fornecedor e selecione a caixa de seleção **Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final**.
7. Na página **Nome do novo pacote de instalação** aberta, no campo **Nome do pacote**, digite o nome do pacote de instalação e clique em **Avançar**.

Aguarde até que o pacote de instalação recém-criado seja carregado no Servidor de Administração. Quando o Assistente de novo pacote exibir a mensagem de que o processo de criação do pacote foi realizado com êxito, clique em **Concluir**.

O pacote de instalação recém-criado aparece na lista de pacotes de instalação. Você pode selecionar esse pacote ao criar ou reconfigurar a tarefa *Instalar aplicativo remotamente*.

Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

Se você já criou algum pacote de instalação de aplicativos de terceiros listados no banco de dados da Kaspersky, poderá visualizar e modificar as configurações desse pacote posteriormente.

A modificação das configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky está disponível apenas para a licença de Gerenciamento de patches e vulnerabilidades.

Para visualizar e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
2. Na lista de pacotes de instalação aberta, clique no nome do pacote relevante.
3. Na página de propriedades aberta, modifique as configurações, conforme necessário.

Cliq

As configurações que você modificou são salvas.

Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

As configurações do pacote de instalação de um aplicativo de terceiros são agrupadas nas seguintes guias:

Apenas uma parte das configurações listadas abaixo são exibidas por padrão, então você pode adicionar as colunas correspondentes clicando no botão **Filtro** e selecionando nomes de colunas relevantes da lista.

Guia **Geral**:

- Campo de entrada que contém o nome do pacote de instalação que pode ser editado manualmente

  Aplicativo

  O nome do aplicativo de terceiros para o qual o pacote de instalação foi criado.

  Versão

  O número da versão do aplicativo de terceiros para o qual o pacote de instalação foi criado.

- **Tamanho**

  O tamanho do pacote de instalação de terceiros (em kilobytes).

- **Criação**

  A data e hora em que o pacote de instalação de terceiros foi criado.

- **Caminho**

  O caminho para a pasta de rede em que o pacote de instalação de terceiros está localizado.

- Guia **Procedimento de instalação**:

  Instalar os componentes gerais do sistema necessários

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

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

  Por padrão, esta opção está desativada.

- Tabela que exibe as propriedades de atualização e contendo as seguintes colunas:

O nome da atualização.

- **Descrição**

  A descrição da atualização.

- **Origem**

  A fonte da atualização, isto é, se foi lançada pela Microsoft ou por outro desenvolvedor terceiro.

- **Tipo**

  O tipo da atualização, ou seja, se é destinada a um driver ou aplicativo.

- **Categoria**

  A categoria WSUS (Windows Server Update Services) exibida para atualizações da Microsoft (atualizações críticas, atualizações de definições, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, pacotes cumulativos de atualizações, atualizações ou upgrades).

- **Nível de importância de acordo com o MSRC**

  O nível de importância da atualização definido pelo Microsoft Security Response Center (MSRC).

- **Nível de importância**

  O nível de importância da atualização definido pela Kaspersky.

- **Nível de importância do patch (para patches destinados aos aplicativos Kaspersky)**

  O nível de importância do patch caso se destine a um aplicativo Kaspersky.

- **Artigo**

  O identificador (ID) do artigo na Base de Conhecimento que descreve a atualização.

- **Boletim**

  O ID do boletim de segurança que descreve a atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação.

- **A ser instalado**

  Exibe se a atualização tem o status A ser instalada.

- **Instalando**

  Exibe se a atualização tem o status Instalando.

- **Instalado**

  Exibe se a atualização tem o status Instalada.

  Falhou

  Exibe se a atualização tem o status Falha.

  A reinicialização é necessária

  Exibe se a atualização tem o status Reinicialização necessária.

- **Registrado**

  Exibe a data e a hora em que a atualização foi registrada.

- **Instalado no modo interativo**

  Exibe se a atualização requer interação com o usuário durante a instalação.

- **Revogado**

  Exibe a data e a hora em que a atualização foi revogada.

- **Status de aprovação da atualização**

  Exibe se a atualização está aprovada para instalação.

- **Revisão**

  Exibe o número da revisão atual da atualização.

  ID de atualização

  Exibe o ID da atualização.

  Versão do aplicativo

  Exibe o número da versão para a qual o aplicativo deve ser atualizado.

- **Substituído**

  Exibe outras atualizações que podem substituir a atualização.

Exibe outras atualizações que podem ser substituídas pela atualização.

- **Você deve aceitar os termos do Contrato de Licença**

  Exibe se a atualização requer aceitação dos termos de um Contrato de Licença do Usuário Final (EULA).

URL de descrição

Exibe o nome do fornecedor da atualização.

- **Família do aplicativo**

  Exibe o nome da família de aplicativos à qual a atualização pertence.

- **Aplicativo**

  Exibe o nome do aplicativo ao qual a atualização pertence.

- **Idioma da localização**

  Exibe o idioma da localização da atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação (nova versão).

- **Requer a instalação de pré-requisitos**

  Exibe se a atualização tem o status de instalação Requer pré-requisitos.

- **Modo de download**

  Exibe o modo de download da atualização.

É um patch

Exibe se a atualização é um patch.

Não instalado

Exibe se a atualização tem o status Não instalada.

- Guia **Configurações** que exibe as configurações do pacote de instalação, com seus nomes, descrições e valores usados como parâmetros de linha de comando durante a instalação. Se o pacote não fornecer estas configurações, a mensagem correspondente será exibida. Você pode modificar os valores destas configurações.

- **Revisão**

  Exibe o número da revisão dos pacotes de instalação.

- **Hora**

  Exibe a hora em que a revisão foi criada.

  Usuário

  Exibe o nome da conta do usuário sob a qual a revisão foi criada.

  Ação

  Lista as ações executadas no pacote de instalação dentro da revisão.

- **Descrição**

  Exibe a descrição de texto adicionada para a revisão.

Tags de aplicativo

Esta seção descreve as tags do aplicativo e fornece instruções para criá-los e modificá-los, bem como para aplicar tag em aplicativos de terceiros.

Sobre as tags de aplicativos

O Kaspersky Security Center permite identificar aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky). Uma tag é o rótulo de um aplicativo que pode ser usada para agrupar ou encontrar dispositivos. Uma tag destinada a aplicativos pode servir como uma condição em seleções de dispositivos.

Por exemplo, você pode criar a tag `[Browsers]` e atribuí-la a todos os navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox etc.

Criando uma tag de aplicativo

Para criar um tag de aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Tags de aplicativos**.
2. Clique em **Adicionar**.
   Uma nova janela de tag é exibida.

4. Clique em **OK** para salvar as alterações.

A nova tag aparece na lista de tags de aplicativos.

Renomeando uma tag de aplicativo

Para renomear um identificador de aplicativos:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Tags de aplicativos**.
2. Marque a caixa de seleção ao lado do identificador que deseja renomear e clique em **Editar**.
   A janela de propriedades do identificador é exibida.
3. Altere o nome do identificador.
4. Clique em **OK** para salvar as alterações.

A tag atualizado aparece na lista de tags de aplicativos.

Atribuindo uma tag de aplicativos

Para atribuir uma ou várias tags a um aplicativo:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.
2. Clique no nome do aplicativo ao qual deseja atribuir tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.
4. Para as tags que deseja atribuir, marque as caixas de seleção na coluna **Tag atribuída**.
5. Clique em **Salvar** para salvar as alterações.

As tags são atribuídas ao aplicativo.

Removendo tags atribuídas de um aplicativo

Para remover uma ou várias tags de um aplicativo:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.
2. Clique no nome do aplicativo do qual deseja remover tags.

A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.

4. Para tags que deseja remover, desmarque as caixas de seleção na coluna **Tag atribuída**.

5. Clique em **Salvar** para salvar as alterações.

As tags são removidas do dispositivo.

As tags de aplicativos removidas não são excluídas. Se quiser, você pode excluí-los manualmente.

Excluir uma tag de aplicativos

Para excluir um identificador de aplicativos:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Tags de aplicativos**.

2. Na lista, selecione o identificador de aplicativos que deseja excluir.

3. Clique no botão **Excluir**.

4. Na janela que se abre, clique em **OK**.

O identificador de aplicativos é excluído. O identificador excluído é automaticamente removido de todos dos aplicativos aos quais foi atribuído.

Monitoramento e relatórios

Esta seção descreve os recursos de monitoramento e emissão de relatórios no Kaspersky Security Center. Esses recursos fornecem a você uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a melhor atender às suas necessidades.

Cenário: Monitoramento e relatórios

Esta seção fornece um cenário para a configuração do recurso de monitoramento e de relatórios no Kaspersky Security Center.

Pré-requisitos

Após ter implementado o Kaspersky Security Center na rede de uma organização, você poderá iniciar o seu monitoramento e gerar relatórios sobre o seu funcionamento.

O monitoramento e relatórios em na rede de uma organização prossegue em estágios:

1. **Configurar a alternância dos status do dispositivo**

   Conheça as configurações para os status do dispositivo dependendo de condições específicas. Modificando essas configurações, você pode alterar o número de eventos com os níveis de importância *Crítico* ou *Advertência*. Ao configurar a alternância dos status do dispositivo, esteja seguro do seguinte:

   - As novas configurações não entram em conflito com as políticas de segurança de informações da sua organização.
   - Você pode reagir a eventos de segurança importantes na rede da sua organização de maneira oportuna.

2. **Configurar as notificações de eventos em dispositivos cliente**

   Instruções de como proceder:

   Configure a notificação (por e-mail, SMS ou executando um arquivo executável) de eventos em dispositivos cliente

3. **Alteração da resposta da sua rede de segurança para o evento de Surto de vírus**

   Você pode alterar os limites específicos nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência do evento.

4. **Execução das ações recomendadas para as notificações Crítico e Advertência**

   Instruções de como proceder:

   Execute as ações recomendadas para a rede da sua organização

5. **Análise do status de segurança da rede da sua organização**

   Instruções de como proceder:

   - Revise o widget Status da proteção
   - Gere e revise o Relatório do status da proteção
   - Gere e revise o Relatório de erros

6. **Localize dispositivos cliente que não estão protegidos**

   Instruções de como proceder:

   - Revise o widget Novos dispositivos
   - Gere e revise o Relatório de implementação de proteção

7. **Verificação da proteção de dispositivos cliente**

   Instruções de como proceder:

   - Gere e revise os relatórios das categorias Status da proteção e Estatísticas de ameaças
   - Inicie e analise a seleção de eventos de Crítico

8. **Avaliação e limitação da carga de eventos no banco de dados**

As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

Instruções de como proceder:

- Cálculo do espaço do banco de dados
- Limitação do número máximo de eventos

9. **Análise de informações de licença**

   Instruções de como proceder:

   - Adicione o widget de Uso de chaves de licença ao painel e o analise
   - Gere e revise o Relatório de uso das chaves de licença

Resultados

Após a conclusão do cenário, você é informado sobre a proteção da rede da sua organização e, portanto, poderá planejar ações para proteção adicional.

Sobre os tipos do monitoramento e relatórios

As informações sobre eventos de segurança na rede de uma organização são armazenadas no banco de dados do Servidor de Administração. Com base nos eventos, o Kaspersky Security Center Web Console fornece os seguintes tipos de monitoramento e relatórios na rede da sua organização:

- Painel

  Relatórios

- Seleções de eventos
- Notificações

Painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

Relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

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.

Painel e widgets

Esta seção contém informações sobre o painel e os widgets que o painel fornece. A seção inclui instruções sobre como gerenciar e definir as configurações dos widgets.

Usar o painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

O painel está disponível no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Painel**.

O painel fornece widgets que podem ser personalizados. Você pode selecionar um grande número de widgets diferentes, apresentadas como gráficos de pizza ou gráficos de rosca, tabelas, gráficos, gráficos de barras e listas. As informações exibidas nos widgets são atualizadas automaticamente em um intervalo de dois minutos. O intervalo entre atualizações varia para widgets diferentes. Você pode atualizar dados sobre um widget manualmente a qualquer momento por meio do menu de configurações.

Por padrão, os widgets contém informações sobre todos os eventos armazenados no banco de dados do Servidor de Administração.

O Kaspersky Security Center Web Console tem um conjunto padrão de widgets para as seguintes categorias:

- **Status da proteção**
- **Implementação**

  Atualizando
- **Estatísticas de ameaças**

  Outro

Alguns widgets têm informações de texto com links. Você pode exibir informações detalhadas clicando em um link.

Ao configurar o painel, você pode adicionar os widgets de que precisa, ocultar widgets de que não precisa, modificar o tamanho ou a aparência de widgets, mover widgets e modificar suas configurações.

Adição de widgets ao painel

Para adicionar widgets ao painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no botão **Adicionar ou restaurar widget da Web**.
3. Na lista de widgets disponíveis, selecione os widgets que deseja adicionar ao painel.
   Os widgets são agrupados por categoria. Para visualizar a lista de widgets incluídos em uma categoria, clique no ícone de insígnia (>) ao lado do nome da categoria.
4. Clique no botão **Adicionar**.

Os widgets selecionados são adicionados no final do painel.

Você pode editar agora a representação e os parâmetros dos widgets adicionados.

Ocultação de um widget do painel

Para ocultar um widget exibido do painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja ocultar.
3. Selecione **Ocultar widget da Web**.
4. Na janela **Advertência** que se abre, clique em **OK**.

O widget selecionado fica oculto. Depois, você pode adicionar esse widget ao painel novamente.

Movimentação de um widget no painel

Para mover um widget no painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Migrar**.

4. Clique no lugar para o qual deseja mover o widget. Você pode selecionar apenas outro widget.

Os lugares dos widgets selecionados são trocados.

Alteração do tamanho ou da aparência do widget

Para widgets que exibem um gráfico, você pode alterar sua representação: um gráfico de barras ou um gráfico de linhas. Para alguns widgets, você pode alterar seu tamanho: compacto, médio ou máximo.

Para alterar a representação do widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja editar.
3. Execute uma das seguintes ações:
   - Para exibir o widget como um gráfico de barras, selecione **Tipo de gráfico: barras**.

     Para exibir o widget como um gráfico de linhas, selecione **Tipo de gráfico: linhas**.
   - Para alterar a área ocupada pelo widget, selecione um dos valores:
     - **Compacto**
     - **Compacto (somente barra)**
     - **Médio (gráfico de rosca)**

       Médio (gráfico de barras)
     - **Máximo**

A representação do widget selecionado é alterada.

Alteração das configurações do widget

Para alterar as configurações de um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja alterar.
3. Selecione **Mostrar configurações**.
4. Na janela de configurações de widget exibida, modifique as configurações de widget conforme necessário.
5. Clique em **Salvar** para salvar as alterações.

O conjunto de configurações depende do widget específico. Abaixo estão algumas configurações comuns:

Escopo do widget da Web (o conjunto de objetos para os quais o widget exibe informações): por exemplo, um grupo de administração ou uma seleção de dispositivos.

Selecionar tarefa (a tarefa para a qual o widget exibe informações).

- **Intervalo de tempo** (o intervalo de tempo durante o qual as informações são exibidas no widget): entre as duas datas especificadas; desde a data especificada até o dia atual; ou do dia atual menos o número especificado de dias até o dia atual.
- **Se especificados, definir como Crítico** e **Se especificados, definir como Advertência** (as regras que determinam a cor de um semáforo).

Depois de alterar as configurações do widget, você pode atualizar os dados manualmente.

Para atualizar dados e um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Atualizar**.

Os dados no widget são atualizados.

Sobre o modo somente painel

É possível configurar o modo somente painel para funcionários que não gerenciam a rede, mas que desejam visualizar as estatísticas de proteção da rede no Kaspersky Security Center (por exemplo, um gerente superior). Quando um usuário tem esse modo ativado, apenas um painel com um conjunto predefinido de widgets é exibido para o usuário. Assim, ele pode monitorar as estatísticas especificadas nos widgets, por exemplo, o status de proteção de todos os dispositivos gerenciados, o número de ameaças detectadas recentemente ou a lista das ameaças mais frequentes na rede.

Quando um usuário trabalha no modo somente painel, as seguintes restrições são aplicadas:

- O menu principal não é exibido para o usuário, portanto, ele não pode alterar as configurações de proteção de rede.
- O usuário não pode realizar nenhuma ação com widgets, por exemplo, adicioná-los ou ocultá-los. Portanto, não é necessário colocar todos os widgets requeridos para o usuário no painel e configurá-los, por exemplo, para definir a regra de contagem de objetos ou especificar o intervalo de tempo.

Não é possível atribuir o modo somente painel a si mesmo. Caso queira trabalhar nesse modo, entre em contato com um administrador do sistema, o Provedor de Serviços Gerenciados (MSP) ou um usuário com o direito Modificar ACLs de objetos na área funcional **Recursos gerais: Permissões do usuário**.

Configurando o modo somente painel

tes d

- O usuário tem o direito de **Modificar ACLs de objetos** na área funcional **Recursos gerais: permissões do usuário**. Caso não tenha esse direito, a guia para configurar o modo estará ausente.
- O usuário tem o direito de **Leitura** na área funcional **Recursos gerais: funcionalidade básica**.

Caso uma hierarquia de Servidores de Administração esteja organizada em sua rede, para configurar o modo somente Painel, acesse o servidor onde a conta de usuário está disponível na seção **Usuários e funções → Usuários**. Pode ser um servidor principal ou um servidor secundário físico. Não é possível ajustar o modo em um servidor virtual.

Para configurar o modo somente painel:

1. No menu principal, vá para **Usuários e funções → Usuários**.
2. Clique no nome da conta de usuário para a qual deseja ajustar o painel com widgets.
3. Na janela aberta de configurações do usuário, selecione a guia **Painel**.

   Na guia aberta, o mesmo painel é exibido para você e para o usuário.
4. Caso o **modo Exibir o console no modo somente painel** estiver habilitado, alterne o botão de alternância para desativá-la.

   Quando essa opção está habilitada, também não será possível alterar o painel. Depois de desativar a opção, será possível gerenciar widgets.
5. Configure a aparência do painel. O conjunto de widgets preparados na guia **Painel** está disponível para o usuário com a conta personalizável. Ele ou ela não pode alterar nenhuma configuração ou tamanho dos widgets, adicionar ou remover quaisquer widgets do painel. Portanto, ajuste-os para o usuário, para que ele possa visualizar as estatísticas de proteção da rede. Para isso, na guia **Painel** é possível executar as mesmas ações com widgets como na seção **Monitoramento e relatórios → Painel**:

   Adicionar novos widgets ao painel.

   - Ocultar widgets que o usuário não precisa.
   - Mover widgets em uma ordem específica.

   Alterar o tamanho ou a aparência de widgets.

   - Alterar as configurações do widget.
6. Alterne o botão de alternância para habilitar a opção **Exibir o console no modo somente painel**.
   Depois disso, apenas o painel ficará disponível para o usuário. Ele ou ela pode monitorar as estatísticas, mas não pode alterar as configurações de proteção de rede e a aparência do painel. Como o mesmo painel é exibido para você e para o usuário, você também não pode alterar o painel.
   Caso mantenha a opção desativada, o menu principal será exibido ao usuário, para que ele possa realizar várias ações no Kaspersky Security Center, inclusive alterar as configurações de segurança e os widgets.
7. Clique no botão **Salvar** quando terminar de configurar o modo somente painel. Somente depois disso o dashboard preparado será exibido ao usuário.
8. Caso o usuário queira visualizar as estatísticas de aplicativos Kaspersky compatíveis e precisar de direitos de acesso para isso, configure os direitos para o usuário. Depois disso, os dados dos aplicativos Kaspersky são exibidos para o usuário nos widgets desses aplicativos.