Kaseya 2

Endpoint Security

Guia do usuário

Version 7.0

Português

Setembro 17, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Conteúdo

Bem-vindo

Assistência on-line ao usuário do Endpoint Security

Some things to keep in mind as you navigate online help:

- Enable Internet Explorer to accept cookies and JavaScript.
- Click  to display context-sensitive help for the currently selected function.

Documentation

You can download a PDF version of the following documents. You must have Acrobat Reader installed on your system to view the PDF files.

Endpoint Security Guia do usuário *(http://help.kaseya.com/webhelp/PTB/KES/7000000/PTB_kesguide70.pdf#zoom=70&navpanes=0)*	Este conteúdo é idêntico ao da assistência on-line ao usuário do Endpoint Security.
Notas de versão *(http://help.kaseya.com/webhelp/PTB/RN/7000000/index.asp#KESReleaseNotes.htm)*	É o histórico de alterações de versão do Endpoint Security.

Consulte a **a ajuda on-line e guias de usuário para outros produtos** *(http://help.kaseya.com/WebHelp/PTB/doc/7000000/index.asp#home.htm)*.

Esta versão 7.0 da assistência on-line ao usuário do Endpoint Security foi gerada em 9/17/2014.

Visão geral da segurança

O **Endpoint Security** (KES) fornece proteção de segurança para máquinas gerenciadas, com a tecnologia anti-malware totalmente integrada da AVG Technologies. O termo **malware** engloba vírus, spyware, adware e outros tipos de programas indesejados. O **Endpoint Security** limpa ou remove automaticamente arquivos infectados e outras ameaças, como cavalos de tróia, worms e spyware. O **Endpoint Security** monitora continuamente o status de segurança de todos os servidores, estações de trabalho e notebooks Windows instalados com proteção de segurança. Oa alarmes podem ser acionados pelos eventos de proteção de segurança e podem incluir o envio de notificações por e-mail, procedimentos em execução e a criação de tickets de trabalho.

Os perfis de segurança centralmente gerenciados são definidos e implementados em máquinas que usam a interface de console do VSA. As alterações em um perfil de segurança atualizam automaticamente todas as máquinas que usam esse perfil. O **Endpoint Security** vem com um perfil de segurança padrão predefinido e permite que você crie perfis de segurança personalizados.

Todos os eventos de proteção de segurança são registrados no sistema e estão disponíveis para o resumo executivo e relatórios gerenciais detalhados. Uma vez implementado, as atualizações são automaticamente tratadas em base agendada sem a necessida da interação do usuário.

Proteção anti-vírus

Com base no perfil de segurança, o **Endpoint Security** remove arquivos infectados ou bloqueia o acesso a eles:

- **Varre o registro do sistema** por entradas suspeitas, arquivos temporários da Internet, cookies de rastreamento e outro tipos de objetos indesejados.
- **Detecta os vírus de computador** por:

  - **Varredura** - Executa a varedura no aesso e sob demanda.
  - **Análise heurística** - Emula de forma dinâmica as instruções de objeto varrido dentro de um ambiente de computação virtual.
  - **Detecção genérica** - Detecta característica de insruções de um vírus ou de um grupo de vírus.
  - **Detecção de vírus conhecido** - Pesquisa por características de sequência de caracteres de um vírus.
- **Varredura de e-mail** - Verifica os e-mails de entrada e saída ao usar plug-ins projetados para os programas de e-mail de usao mais frequente. Uma vez detectado, o vírus é limpo ou colocado em quarentena. Algusn clientes de e-mail podem suportar mensagens com texto que certificam que o e-mail enviado e recebido foi varrido quanto a existência de vírus. Além disso, para um nível maior de segurança ao trabalhar com e-mail, um filtro de anexo pode ser definido ao definir arquivos indesejáveis ou suspeitos.
- **Proteção residente na memória** - Varre os arquivos quando estes são copiados, abertos ou salvos. Se um vírus é descoberto, o acesso ao arquivo é interrompido e o vírus não tem a permissão de ativar-se. A proteção residente na memória e carregada na memória do computador durante a inicialização do sistema, e fornece proteção vital para as áreas do sistema do computador.
- **Varreduras sob demanda** - As varreduras podem ser executadas sob demanda ou agendadas para serem executadas em horário conveniente.
- **Varredura de MS Exchange Servers** - Faz a varredura de mensagens de e-mail de entreda e saída e pastas da caixa de correio em MS Exchange Servers contra vírus/spyware/ameaças de malware r os exclui imediatamente antes que os destinatários de e-mail do MS Exchange Server infectados.
- **Varredura de websites e downloads** - Efetua a varredura de websites e de links de websites. Também efetua a varrdura dos arquivos baixados para seu computador. Fornece uma classificação de segurança para links retornados por populares mecanismos de busca.
- **Proteção da ID** - Previne a ameaça alvo contra senhas, detalhes de conta bancária, números de cartão de crédito e outros ativos digitais, usando a "análise comportamental" para identificar atividade supeita em uma máquina.

Anti-Spyware

O spyware é um software que coleta informações de um cpmputador sem o conhecimento ou consentimento do usuário. Alguns aplicativos de spyware também podem ser secretamente instalados e com frequência contêm anuncios, janelas supensas ou difernets tipos de software desagradável. No momento, a origem mais comum de infecção são os websites com conteúdo potencialmente perigoso. Outros métodos de transmissão incluem e-mail ou transmissão por worms e vírus. A proteção mais importante contra spyware é o uso de uma **defesa residente na memória**, como o avançado componente de spyware **Endpoint Security**. Uma defesa residente na memória varre os aplicativos em segundo plano à medida que eles são executados. A proteção antispyware do **Endpoint Security** detecta spywares, adwares, cavalos de tróia DLL, registradores de chave, malwares ocultos em fluxos de dados, arquivos mortos, entradas de spyware no registro do Windows e outros tipos de objetos indesejados.

> **Nota:** *Consulte os Requisitos de sistema do Endpoint Security.*

Licenciamento do Endpoint Security

Cada licença de instalação do MSE KES permite que o cliente instale e use um agente MSE KES perpetuamente, além de receber atualizações durante um período de assinatura de 365 dias consecutivos. O período de assinatura de atualizações tem um prazo independente para cada instalação e começa na data de instalação do agente MSE KES em uma máquina. Durante esse período, a instalação poderá receber todas as atualizações do KES que forem lançadas. Todas as atualizações liberadas durante o período de assinatura também serão licenciadas perpetuamente, desde que, após o término do período de assinatura ou caso este não seja renovado, o direito de receber novas atualizações do KES seja revogado.

A emissão de um novo período de assinatura de instalações para uma máquina com um Termo de Assinatura existente faz com que os períodos se mesclem e, portanto, adiciona 365 dias ao tempo ainda restante no Termo de Assinatura de instalações. Qualquer transferência de tal Termo mesclado para uma nova máquina irá causar a transferência dos dias remanescentes de ambas as duas instalações anteriores.

A licença de instalação apropriada do KES precisa ser obtida para cada máquina e/ou caixa de correio do Exchange protegida. O cliente só pode implementar o MSE KES em uma máquina que tenha uma licença válida do VSA. As licenças do MSE KES podem ser gerenciadas centralmente com o uso da interface de usuário da Web da Kaseya. O licenciamento é obrigatório, e uma licença é necessária para cada caixa de correio em uso.

Nota: As licenças do KES são alocadas a IDs de grupos em Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm).*

Funções	Descrição
Painel *(página 4)*	Fornece uma exibição de painel do status das máquinas instaladas com o Endpoint Security.
Status da segurança *(página 11)*	Exibe o status da segurança atual das IDs de máquina.
Atualização manual *(página 9)*	Agenda as atualizações da versão mais recente dos arquivo de definição de proteção de segurança.
Agendar varredura *(página 11)*	Agenda as varreduras de proteção de segurança de IDs de máquina.
Visualizar ameaças *(página 12)*	Lista os arquivos que foram colocados em quarentena devido a ameaça suspeita ou confirmada.
Visualizar registros *(página 14)*	Exibe o registro de evento de proteção de segurança de IDs de máquina.
Estender/Retornar *(página 14)*	Estende a contagem de licença anual para IDs de máquina selecionadas ou devolve as licenaças anuais de IDs de máquinas selecionadas.
Notificar *(página 16)*	Fornece uma notificação automática sobre a expiração de licenças do Endpoint Security.
Instalação *(página 17)*	Instala ou remove a proteção de segurança para IDs de máquina.
Definir perfil *(página 22)*	Gerencia os perfis de segurança. Cada perfilde segurança represneta um conjunto diferente de opções de segurança ativadas ou desativadas.
Atribuir perfil *(página 29)*	Atribui os perfis de segurança para IDs de máquina.
Configurações de registro *(página 30)*	Especifica o número de dias para reter dados de registro de proteção de segurança.
Status do Exchange *(página 31)*	Exibe o status da proteção de e-mail em servidores MS Exchange nos quais o Endpoint Security está instalado.
Definir conjuntos de alarme *(página 32)*	Define conjuntos de condições de alerta usadas para acionar alertas com o uso da página Aplicar conjuntos de alarme.
Aplicar conjuntos de alarme *(página 33)*	Cria alarmes em resposta para eventos proteção de segurança.

Requisitos do módulo Endpoint Security

servidor da Kaseya

- O módulo Endpoint Security 7.0 requer o VSA 7.0.
- Acesso a `http://download.avg.com`

Requisitos para cada máquina gerenciada

- 256 MB de RAM
- 60 MB de espaço livre em disco
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Nota: Consulte **Requisitos gerais do sistema** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/reqs/index.asp#home.htm).*

Painel

Segurança > Painel

- Informações semelhantes são fornecidas em Centro de informações > Emissão de relatórios > Relatórios > Segurança.

A página **Painel** fornece uma exibição de painel do status das máquinas instaladas com o **Endpoint Security**.

- **Estatísticas de segurança de ponto final**
- **Status da licença**
- **Contagem de licenças**
- **Principais máquinas com ameaças**
- **Principais ameaças descobertas**

Nota: A lista de IDs de máquinas exibida depende do filtro ID de máquinas/ID de grupos e dos grupos de máquinas que o usuário está autorizado a ver utilizando Sistema > Segurança do usuário > Escopos.

Estatísticas de segurança de ponto final

A seção **Estatísticas de segurança de endpoint** fornece diversas estatísticas sobre o status de segurança de endpoints e o status das definições de segurança.

- <N> Os endpoints precisam de reinicialização
- <N> Versões de assinatura anteriores a '<versão>'
- <N> Endpoints com versões mais antigas do **Endpoint Security**
- <N> Endpoints sem uma varredura completada nesta semana
- <N> Endpoints que executam uma varredura no momento
- <N> Endpoints com o Resident Shield desativado

Clique em quaisquer destas estatísticas com hiperlink para visualizar um caixa de diálogo tabulada mostrando cada membro que pertence àquela estatística.

Status da licença

Um gráfico circulas exibe o percentual de máquinas que têm licenças expiradas ou que terão licenças expiradas em 30, 60, 90 ou 91+ dias. Clique em qualquer fatia do gráfico de círculo ou em qualquer legenda para exibir uma lista de máquinas individuais que pertencem àquela fatia.

Contagem de licenças

Listas contagens de licenças para o seguinte:

- Licenças adquiridas
- Licenças completas disponíveis (Adquiridas mas não atribuídas, instaladas ou expiradas)
- Licenças alocadas (Agendadas para instalação, mas a instalação ainda não foi concluída)
- Licenças aplicadas (Licença ativa aplicada a uma máquina)
- Licenças parciais disponíveis (Anteriormente atribuídas a uma máquina, mas retornadas ao grupo antes da expiração)
- Licenças parciais alocadas (Disponíveis parcialmente que foram agendadas para instalação, mas a instalação ainda não foi concluída)
- Total de licenças (Licenças adquiridas, menos licenças vencidas)
- Licenças vencidas

Principais máquinas com ameaças

Lista as máquinas com o maior número de ameaças atuais. O número de ameaças no valut do vírus também será listado. Clicar em uma ID de máquina com hiperlink exibe as ameaças pertencentes àquela ID de máquina na página **Visualizar ameças** *(página 12)*.

Principais ameaças descobertas

Um gráfico circular exibe quais ameças forma encontradas no maior percentual de máquinas. Clique em qualquer fatia do gráfico de círculo ou em qualquer legenda para exibir uma lista de máquinas individuais que pertencem àquela fatia na página **Visualizar ameças**.

Status da segurança

Segurança > Status da segurança

- Informações semelhantes são fornecidas em Centro de informações > Emissão de relatórios > Relatórios > Segurança *(página 36)*.

A página **Status da segurança** exibe o status atual de segurança de cada ID de máquina licenciada para usar o **Endpoint Security**. A lista de IDs de máquinas exibida depende do filtro ID de máquinas/ID de grupos e dos grupos de máquinas que o usuário está autorizado a ver utilizando Sistema > Segurança do usuário > Escopos. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Os indicadores incluem a proteção residente, proteção de correio, o número de ameaças não solucionadas detectadas, o número de ameaças no valut do vírus e a versão da proteção de segurança instalada em cada ID de máquina.

Ações

- **Ativar o escudo residente** - Clique para ativar a proteção residente na memória anti-malware em IDs de máquina selecionadas..
- **Desativar o escudo residente** - Clique para desativar a proteção residente na memória anti-malware em IDs de máquina selecionadas..

  Nota: Em alguns casos, a proteção de segurança precisa ser desativada para instalar ou configurar o software em uma máquina gerenciada.

  Nota: Você também pode **Ativar/Desativar o Resident Shield por procedimento de agente** *(página 8)*.

- **Ativar e-mail** - Clique para ativar a proteção de e-mail em IDs de máquina seleciondas.

- **Desativar e-mail** - Clique para desativar a proteção de e-mail em IDs de máquina seleciondas.
- **Esvaziar o vault** - Clique para esvaziar o valut de vírus de todas as IDs de malware en quarentena.
- **Reinicializar agora** - Reinicializa as IDs de máquina selecionadas. Algumas atualizações de segurança requerem uma reinicialização para instalar a atualização. Se uma reinicialização estiver pendente, um ícone de reinicialização é exibido junto ao número da versão de pré-atualização e a máquina ainda está protegida.

Informações do cabeçalho

- **Versão atual disponível de assinatura:**: a versão mais recente de proteção de segurança disponível. Você pode atualizar uma ou mais IDs de máquinas com a **Versão atual disponível** em Segurança >**Atualizações manuais** *(página 33)*.
- **Versão atual do instalador**: o número da versão do instalador do AVG a ser usado em novas instalações.

Colunas de tabelas

- **Ícones de verificação** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Nome do perfil**: o perfil de segurança atribuído à ID de máquina.
- **Status**: o estado atual da proteção de segurança para uma ID de máquina é indicado pelo conjunto de ícones de status exibidos na coluna **Status**. Os ícones de status possíveis incluem:


Escudo residente ativado


Escudo residente desativado


Escudo residente parcial


Ativação/Desativação do escudo residente pendente


Varredura de e-mail ativada


Varredura de e-mail desativada


Varredura de e-mail parcial


Ativação/Desativação de varredura de e-mail pendente


Varredura de link ativada


Varredura de link desativada


Varredura de link parcial


Ativação/Desativação de varredura de link pendente


Escudo da web ativado


Escudo da web desativado


Escudo da web parcial


Ativação/Desativação do escudo da web pendente

- **Ameaças**: o número de ameças não solucionadas detectadas na ID de máquina. Estas são as ameaças atuais que exigem a atenção do usuário. Você pode clicar no número com hiperlinl em qualquer linha para exibir estas ameças na guia **Ameaças atuais** da página **Visualizar ameaças** *(página 12)*.
- **Vault de vírus**: o número de ameaças armazenadas no vault de vírus da ID de máquina. Esses itens são colocados em quarentena com segurança e serão automaticamente excluídos se as configurações de perfil forem aplicáveis. Você pode clicar no número com hiperlink em qualquer linha para exibir essas ameaças na guia **Vault de vírus** da página **Visualizar ameaças** *(página 12)*>.
- **Versão** - A versão da proteção de segurança atualmente utilizada por esta ID de máquina. Por exemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: a versão do programa AVG instalado.
  - `270.12.6/2084`: a versão completa do *banco de dados* de vírus. `270.12.6` representa a versão da *definição* e `2084` é a versão da *assinatura*. É Exibida em texto vermelho se a versão da *assinatura* é mais antiga que as últimas 5 versões de *assinatura* disponíveis ou a versão de *definição* é mais antiga do que as 2 últimas versões de *definição* disponíveis, e o agente está ativo.

Nota: Se a versão da ID de máquina está desatualizada, é possível atualizar manualmente a ID de máquina em Segurança >**Atualização manual** *(página 9)*.

Nota: Algumas atualizações de segurança requerem uma reinicialização para instalar a atualização. Se uma reinicialização estiver pendente, um ícone de reinicialização é exibido junto ao número da versão de pré-atualização e a máquina ainda está protegida.

Ativar/Desativar o escudo residente por procedimento de agenet

É possível ativar/desativar o **Escudo residente** usando o seguinte **executeShellCommand()** em um procedimento de agente. No **diretório de trabalho** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#368.htm)* do agente, execute:

```
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 0   ;disables Resident Shield
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 1   ;enables Resident Shield
```

```
Script Name: KES_Enable Resident Shield
Script Description: Enables Resident Shield temporarily (until next scan or
reboot...unless it is enabled by default and is being re-enabled after being
temporarily disabled)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 1
     Parameter 3 : 3
         OS Type : 0
ELSE
```

```
Script Name: KES_Disable Resident Shield
Script Description: Disables Resident Shield temporarily (until next scan or
reboot)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 0
     Parameter 3 : 3
         OS Type : 0
ELSE
```

Atualização manual

Segurança > Atualização manual

A página **Atualizações manuais** controla a atualização das IDs de máquina licenciadas para usar o **Endpoint Security** com a versão mais recente da proteção de segurança disponível. *As atualizações são agendadas automaticamente por padrão.* Você pode desativar e reativar a atualização automa´tica por máquina. Utilize esta função para rever o status da atualização de agenets ou para forçar uma verificação imediata de atualização, se necessário.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Atualizar** - Clique para agendar uma atualização de definiçãode vírus em IDs de máquina selecionadas usando as opções de atualização previamente selecionadas.
- **Cancelar atualização** - Clique para limpar uma atualização agendada.
- **Ativar atualizações automáticas** - Ativa as atualizações de definição de vírus.
- **Desativar atualizações automáticas** - Desativa as atualizações de definição de vírus. Isso previne as atualizações de definição de vírus de tornar lenta a rede durante as hoas de pico de trabalho. Em uma versão futura, você será capaz de agendar quando atualizar as definições de vírus. Se as atualizações automáticas estão desativadas, então um ícone com cruz vermelha é exibido na coluna **Horário agendado** , mesmo se uma atualização manual estiver agendada.

Informações do cabeçalho

- **Versão atual disponível**: a versão mais recente da proteção de segurança disponível. Verifique a coluna de versão nessa página para determinar se existem IDs de máquinas sem a versão mais recente da proteção de segurança ou o último software cliente **Endpoint Security** disponível.
- **Versão atual do cliente KES**: o software cliente KES mais recente disponível.

Configurações de agendamento

- **Imediato**: marque para agendar essa tarefa imediatamente.
- **Data/hora**: insira o ano, o mês, o dia, a hora e o minuto para agendar essa tarefa.
- **Escalonar por**: você pode distribuir a carga na rede programando essa tarefa. Se você definir esse parâmetro como cinco minutos, a tarefa em cada ID de máquina será programada para ocorrer a cada cinco minutos. Por exemplo, a máquina 1 é executada às 10 horas, a máquina 2 às 10 horas e 5 minutos e a máquina três, às 10 horas e 10 minutos, ...
- **Ignorar se a máquina estiver off-line**: se uma marca de seleção for exibida e a máquina estiver off-line, ignore e execute o próximo período e hora agendados. Se nenhuma marca de verificação estiver exibida, execute essa tarefa assim que a máquina se conectar, após a hora agendada.
- **Atualizar do KServer (Substituir o arquivo de origem)**: se essa opção estiver selecionada, as atualizações serão obtidas por download do servidor da Kaseya. Se ela estiver em branco, as atualizações serão obtidas por download por meio do método especificado em Gerenciamento de correções > **Origem do arquivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#366.htm)*.

Colunas de tabela

- **Status de entrada** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria

- Agente on-line
- Agente e usuário conectados no momento.
- Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
- No momento o Agente está desconectado
- O Agente nunca efetuou a entrada
- O Agente está conectado mas o controle remoto foi desativado
- O Agente foi suspenso

- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Origem**: se uma origem de arquivo for definida via Gerenciamento de correções > Origem do arquivo, as atualizações serão originadas desse local. Caso contrário, as atualizações se originam da Internet. Se a opção **Fazer download da Internet caso a máquina não consiga se conectar ao servidor de arquivos** estiver selecionada em Gerenciamento de correções > Origem do arquivo:
  - Durante a instalação de um endpoint do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, o instalador será obtido por download do servidor da Kaseya e concluirá a instalação do endpoint.
  - Durante uma atualização manual do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, a atualização será obtida por download da Internet.

  Em ambos os casos acima, a página **Visualizar registros** *(página 14)* exibe uma mensagem de erro informando o porque da falha da origem do arquivo e que está tentando fazer o download da Internet.
- **Última atualização** - Esta marcação de tempo mostra quando a ID de máquina foi por último atualizada. Quando essa data for alterada, a nova atualização estará disponívei para uso.
- **Versão** - A versão da proteção de segurança atualmente utilizada por esta ID de máquina. Por exemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: a versão do programa AVG instalado.
  - `270.12.6/2084`: a versão completa do *banco de dados* de vírus. `270.12.6` representa a versão da *definição* e `2084` é a versão da *assinatura*. É Exibida em texto vermelho se a versão da *assinatura* é mais antiga que as últimas 5 versões de *assinatura* disponíveis ou a versão de *definição* é mais antiga do que as 2 últimas versões de *definição* disponíveis, e o agente está ativo.
  - `[KES 2.1.0.87]`: a versão do software cliente **Endpoint Security**.
- **Hora agendada**: carimbo de data/hora que mostra a próxima atualização agendada, caso nenhuma tenha sido agendada manual ou automaticamente. Para uma máquina selecionada:
  - Se as *atualizações automa´ticas estão ativadas* para máquinas selecionadas e o KES detecta uma atualização do AVG, uma marcação de tempoé exibida. Quando múltiplas máquinas estão agendadas, as marcações de tempo serão diferentes, porque as atualizações automa´tics usam um agendamento por etapas.
  - Se as *atualizações automáticas estão ativadas* mas nenhuma atualização do AVG é detectada, a célula da tabela está em branco, a não ser que uma atualização manual também esteja agendada.
  - Se as *atualizações automáticas estão desativadas*, então um ícone com cruz vermelha é exibido, mesmo se uma atualização manual estiver agendada.
  - Se uma *atualização manual estiver agendada*, uma marcação de tempo é exibida.

Agendar varredura

Segurança > Agendar varredura

A página **Agendar varredura** agenda varreduras de proteção de segurança das IDs de máquinas selecionadas licenciadas para usar o **Endpoint Security**. A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Varredura** - Clique para agendar uma varredura de uma ID de máquina selecionada usando as opções de varredura previamente selecionadas.
- **Cancelar** - Clique para limpar uma varredura agendada.

Configurações de agendamento

- **Imediato**: marque para agendar essa tarefa imediatamente.
- **Data/hora**: insira o ano, o mês, o dia, a hora e o minuto para agendar essa tarefa.
- **Escalonar por**: você pode distribuir a carga na rede programando essa tarefa. Se você definir esse parâmetro como cinco minutos, a tarefa em cada ID de máquina será programada para ocorrer a cada cinco minutos. Por exemplo, a máquina 1 é executada às 10 horas, a máquina 2 às 10 horas e 5 minutos e a máquina três, às 10 horas e 10 minutos, ...
- **Ignorar se a máquina estiver off-line**: se uma marca de seleção ✓ for exibida e a máquina estiver off-line, ignore e execute o próximo período e hora agendados. Se nenhuma marca de verificação estiver exibida, execute essa tarefa assim que a máquina se conectar, após a hora agendada.
- **A cada N períodos** - Marque a caixa para tornar a tarefa recorrente. Insira o número de períodos a aguardar antes que a tarefa seja executada novamente.

Colunas de tabela

- **Status de entrada** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Última varredura**: esse carimbo de data/hora mostra quando a última varredura ocorreu. Quando essa data for alterada, novos dados da varredura estarão disponíveis para visualização.
- **Próxima varredura/agendada** - Essa marca de data/hora mostra a próxima verificação agendada. Marcações de data/hora vencidas são exibidas como texto vermelho com destaque amarelo. A marca de verificação verde ✓ indica que a verificação é recorrente.

Visualizar ameaças

Segurança > Visualizar ameaças

- Informações semelhantes são fornecidas em Centro de informações > Emissão de relatórios > Relatórios > Segurança *(página 36)*.

A página **Visualizar ameaças** exibe as ameaças contra as quais você pode agir contra. As ameaçãs são agrupadas por seu status em duas diferentes guias:

- **Ameaças atuais** - Lista as ameaças descobertas nas máquinas e que puderam ser automaticamente solucionadas. Cada ameaça não solucionada permanece inalterada na máquina, requerendo a ação do usuário. A exclusão de uma ameaça na guia **Ameaças atuais** exclui imediatamente o arquivo, sem movê-lo para o **Vault de vírus**.

  Nota: Quando uma máquina é varrida, todas as suas ameaças atuais são removidas e marcadas como solucionadas. Se a ameaça continua a existir, ela é redescoberta e adicionada de volta para a lista de ameaças atuais.

- **Vault do vírus** - As ameaças são descobertas pela varedura ou pelo escudo residente. A solução da ameaça substitui o arquivo original por uma cópia se ameaças. O arquivo original não solucionado é movido para uma partição oculta no disco rígido do computador denominada como o **Vault de vírus**. Em efeito, o **Vault de vírus** age como um tipo de "lixeira" para ameaças, permitindo que sejam recuperadas antes de serem permanentemente excluídas das máquinas.

Solucionando

A solução envolve as seguintes etapas:

1. É feita uma tentativa de limpar o arquivo.
2. Caso a tentativa falhe, é feita uma tentativa de mover o arquivo para o **Vault de vírus**.
3. Se esta tentaitva falha, é feita uma tentativa de excluir o arquivo.
4. Se esta tentativa falha, o arquivo permanece inalterado na máquina e é listado na guia **Ameaças atuais** da página **Visualizar amesças**.

Ameaças do MS Exchange Server

Qualquer malware detectado pela proteção de e-mail do MS Exchange Server é imeditamente excluído do MS Exchange Server e *somente* é exibido na guia **Vault do vírus**.

Guia Ameaças atuais

Ações

- **Solucionar** - Tenta solucionar o arquivo sem excluir o mesmo. As ameças solucionadas são removidas da guia **Ameaças atuais** e são exibidas na guia **Vault de vírus**.
- **Excluir** - Tenta excluir o arquivo. As ameaças excluídas são removidas imediatamente do computador.

  Nota: Caso a correção e a exclusão venham a falhar, isso pode significar que o arquivo está aberto. Parar quaisquer processos mantendo o arquivo aberto e tentar novamente excluir o arquivo.

- **Remover desta lista** - Remove a ameaça da página **Visualizar ameaças** sem executar qualquer outra ação.
- **Cancelar a operação pendente** - Cancela quaisquer outras ações, caso ainda não tenham sido completadas.
- **Incluir na lista de exclusão PUP**: uma ameaça é identificada como um programa potencialmente indesejado (PUP, Potential Unwanted Program) por meio da exibição de um `(P)` junto ao nome

da ameaça na página **Visualizar ameaças**. As ameaças PUP podem ser adicionadas na lista de exclusão para o perfil atribuído à maquina onde foram encontradas. A exclusão significa que o arquivo não mais é varrido como uma ameaça potencial em *todas* as máquinas às quais ete perfil está atribuído. Somente execute esta ação se tiver certeza que o arquivo é seguro para ser usado. A manutenção da lista de exclusão de PUP é feita na guia **Definir perfil** *(página 22)* > Exclusões de PUP.

Nota: Ameaças que não são PUP não podem ser adicionadas à lista de exclusões de PUP.

Guia Vault de vírus

Ações

- **Restaurar** - Restaura o arquivo original identificado como uma ameaça. Somente execute esta ação se tiver certeza que o arquivo é seguro para ser usado.
- **Excluir** - Exclui o arquivo original identificado como uma ameaça do **Vault de vírus**.

Nota: Não é possível recuperar um arquivo excluído do **Vault de vírus**.

- **Remover desta lista** - Remove a ameaça da página **Visualizar ameaças** sem executar qualquer outra ação.
- **Cancelar a operação pendente** - Cancela quaisquer outras ações, caso ainda não tenham sido completadas.
- **Incluir na lista de exclusão PUP**: uma ameaça é identificada como um programa potencialmente indesejado (PUP, Potential Unwanted Program) por meio da exibição de um `(P)` junto ao nome da ameaça na página **Visualizar ameaças**. As ameaças PUP podem ser adicionadas na lista de exclusão para o perfil atribuído à maquina onde foram encontradas. A exclusão significa que o arquivo não mais é varrido como uma ameaça potencial em *todas* as máquinas às quais ete perfil está atribuído. Somente execute esta ação se tiver certeza que o arquivo é seguro para ser usado. A manutenção da lista de exclusão de PUP é feita na guia **Definir perfil** *(página 22)* > Exclusões de PUP.

Nota: Ameaças que não são PUP não podem ser adicionadas à lista de exclusões de PUP.

Aplicar filtro / Redefinir filtro

Clique em **Aplicar filtro** para filtrar as linhas exibidas pelotexto inserido nos campos **Grupode máquinas**, **Caminho da ameaça** ou **Nome da ameaça**. A filtragem de **Hora** e a classificação das **Ações** ocorrem imediatamente. Clique em **Redefinir filtro** para exibir todas as linhas de dados.

Filtrar colunas

Filtre a exibição de ameaças usando campos de texto, uma faixa de datas e/ou listas suspensas. Inclua o curinga asterisco (*) com o texto inserido para corresponder a vários registros.

- **Grupo de máquinas** - Filtre pela ID de máquina.ID de grupo das máquinas gerenciadas que reportam ameças.
- **Caminho da ameaça** - Filtre pela localização de nome de caminhode arquivos em máquinas gerenciadas com ameaças reportadas.
- **Hora** - Filtre por uma faixa de datas e horas em que as ameaças foram por *último* detectadas. A filtragem de **Hora** ocorre automaticamente.
- **Nome da ameaça** - Filtre pelo nome d ameaça, como designado pelas definições de anti-malware usadas para detectar uma ameaça.
- **Ação** - Filtre por ações pendentes ou completadas executadas contra registros de visualização de ameaças. Selecione `All OFF` ou `All ON` para ativar ou desativar ações. A ação de classificação ocorre imediatamente;

Visualizar registros

Segurança > Visualizar logs

- Informações semelhantes são fornecidas em Centro de informações > Emissão de relatórios > Relatórios > Segurança *(página 36)*.

A página **Visualizar logs** exibe o log de eventos da proteção de segurança de cada ID de máquina licenciada para usar o **Endpoint Security**. A lista de IDs de máquinas exibida depende do filtro ID de máquinas/ID de grupos e dos grupos de máquinas que o usuário está autorizado a ver utilizando Sistema > Segurança do usuário > Escopos. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Clique na ID de máquina;ID de grupo para exibir um registro de eventos. Cada evento exibe a **Hora**, um **Código** de evento, e na maioria dos casos uma **Mensagem** contendo informações adicionais. Os códigos de evento de proteção de segurança descrevem um dos três tipos de entrada do registro:

- Erros
- Eventos
- Comandos

Aplicar filtro / Redefinir filtro

Clique em **Aplicar filtro** para filtrar as linhas pela faixa de datas inserida no campo **Hora** e/ou pelo texto inserido no campo **Mensagem**. Clique em **Redefinir filtro** para exibir todas as linhas de dados.

Filtrar colunas

Filtre a exibição de ameaças usando campos de texto, uma faixa de datas e/ou listas suspensas. Inclua o curinga asterisco (*) com o texto inserido para corresponder a vários registros. As linhas de paginação podem ser classificadas clicando nos links de cabeçalho das colunas.

- **Tempo, Mín, Máx** - Filtrar por uma faixa de datas e horas.
- **Código** - Filtrar pela categoria do registro de evento reportado. Selecione `All OFF` ou `All ON` para ativar ou desativar todas as categorias.
- **Mensagem** - Filtrar pelo texto da mensagem.

Estender/Retornar

Segurança > Estender/Retornar

A página **Estender/Retornar** estende a contagem de licença anual para IDs de máquina selecionadas ou devolve as licenças anuais de IDs de máquinas selecionadas. Uma licença anual pode ser devolvida de uma ID de máquina e ser aplicada à outra ID de máquina. Cada ID de máquina pode ter alocada múltiplos anos de proteção de segurança. As licenças do **Endpoint Security** são alocadas a IDs de grupos em Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm)*.

Nota: Consulte **Licenciamento do Endpoint Security** no tópico **Visão geral da segurança** *(página 1)*.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Estender** - Estende a contagem de licença anual para IDs de máquina selecionada.
- **Retornar** - Retorna as licenças anuais de IDs de máquina selecionadas.
- **Auto-estender** - Ativa a alocação automática de uma nova licença nodia de expiração da licença antiga para IDs de máquina selecionadas. Somente licenças integrais são alocadas com o uso da **Extensão automática**. Caso não existam licenças adicionais, a alocação falha e a proteção de segurança expira para o endpoint. Ativado por padrão.
- **Remover auto-estender** - Desativa auto-estender para IDs de máquina selecionadas.
- **Contagem de licenças**: exibe uma janela pop-up das seguintes contagens de licenças:
  - Licenças adquiridas
  - Licenças completas disponíveis (Adquiridas mas não atribuídas, instaladas ou expiradas)
  - Licenças alocadas (Agendadas para instalação, mas a instalação ainda não foi concluída)
  - Licenças aplicadas (Licença ativa aplicada a uma máquina)
  - Licenças parciais disponíveis (Anteriormente atribuídas a uma máquina, mas retornadas ao grupo antes da expiração)
  - Licenças parciais alocadas (Disponíveis parcialmente que foram agendadas para instalação, mas a instalação ainda não foi concluída)
  - Total de licenças (Licenças adquiridas, menos licenças vencidas)
  - Licenças vencidas
- **Mostrar somente licenças com expiração dentro de 30 dias**: limita a exibição de licenças na área de paginação somente àquelas que expirarão dentro de 30 dias.

Colunas de tabela

- **(Status de entrada)** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Retornável**: o número de licenças anuais retornáveis de uma ID de máquina. Uma ID de máquina com somente uma licença anual não pode retornar licenças anuais adicionais.
- **Expira em**: a data de expiração da proteção de segurança de uma ID de máquina, com base no número de licenças anuais que ela possui.
- **Extensão automática**: se essa opção estiver selecionada, a extensão automática será ativada para essa ID de máquina.
- **No limite**: se o número máximo de licenças anuais disponíveis para uma ID de grupo estiver sendo usado, cada ID de máquina licenciada nessa ID de grupo exibirá `Yes` na coluna **No limite**. Isso alerta o usuário de que mais licenças anuais poderão ser necessárias para essa ID de grupo. As licenças do **Endpoint Security** são alocadas a IDs de grupos via Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm)*.

Notificar

Segurança > Notificar

A página **Notificar** fornece notificações automáticas sobre a expiração de licenças do **Endpoint Security**. Clientes, usuários do VSA e usuários de máquinas podem receber notificações um número especificado de dias antes da expiração da licença do **Endpoint Security**. As licenças do **Endpoint Security** são alocadas a IDs de grupos em Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm)*.

Nota: Consulte **Licenciamento do Endpoint Security** no tópico **Visão geral da segurança** *(página 1)*.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Enviar notificação quando a licença for expirar em N dias**: insira o número de dias antes da data de expiração de uma licença do **Endpoint Security** para notificar clientes e usuários.
- **Destinatários de e-mail (separar os endereços com vírgula)**: especifique os endereços de e-mail para enviar mensagens de notificação. Múltiplos endereços de e-mail precisam ser separados por vírgulas.
- **Aplicar**: clique para aplicar parâmetros às IDs de máquinas selecionadas. Confirme se os parâmetros foram corretamente aplicados na lista de IDs de máquina.
- **Limpar**: clique para remover todas as configurações de parâmetros das IDs de máquinas selecionadas.

Colunas de tabela

- **(Status de entrada)** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **Selecionar tudo/Cancelar seleção**: Clique no link **Selecionar todas** para marcar todas as linhas da página. Clique no link **Desmarcar seleção de todas** para desmarcar todas as linhas da página.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Dias**: mostra o número de dias antes da data de expiração da licença em que a notificação será enviada.
- **Lista de endereços de e-mail**: lista os endereços de e-mail para os quais se enviarão notificações.
- **Notificar**: se essa opção estiver selecionada, os destinatários do e-mail serão alertados de que a licença de segurança da ID de máquina em questão está prestes a expirar. Se estiver em branco, a notificação não será enviada.

Instalação: Segurança

Segurança > Instalação

A página **Instalação** instala ou remove a proteção de segurança para IDs de máquinas selecionadas.

- A lista de IDs de máquinas exibida depende do filtro ID de máquinas/ID de grupos e dos grupos de máquinas que o usuário está autorizado a ver utilizando Sistema > Segurança do usuário > Escopos.
- O Controle de acesso do usuário (UAC, User Access Control) deve ser desativado antes da instalação ou da atualização de clientes endpoint.
- Após a instalação do **Endpoint Security** 2.3 no VSA, instaladores de endpoint serão obtidos por download da AVG.
  - Novos instaladores de endpoint do **Endpoint Security** 2.3 se baseiam no AVG 2012 SP1, mas o **Endpoint Security** continua a oferecer suporte para endpoints existentes do AVG 9.
  - Os instaladores de endpoint dependem do tipo de estação de trabalho, servidor e CPU: 32 bits versus 64 bits. O instalador apropriado é selecionado durante a instalação em um endpoint.
  - O instalador de endpoint do servidor contém componentes de instalação do Exchange.
  - O tempo para fazer download de instaladores de endpoint na AVG pode variar, com base em um pacote de entrega de aproximadamente 500 MB.
  - Uma reinicialização condicional do VSA pode ser necessária.
- O AVG 2012 não se registra na Central de segurança do Windows.
- As licenças do **Endpoint Security** são alocadas a IDs de grupos em Sistema > **Gerenciador de licenças** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2924.htm)*.

Como reinicializar o endpoint durante instalações e atualizações

A instalação do AVG 2012 pode reiniciar o endpoint após a conclusão do procedimento. A atualização do AVG 2012 reinicializará o endpoint após a desinstalação do software cliente **Endpoint Security** anterior e depois mais uma vez após a instalação do AVG 2012.

Nota: Convém realizar a instalação e a atualização para o AVG 2012 fora do horário de pico, para evitar interrupções no trabalho do usuário. Existe uma opção para solicitar que o usuário final prossiga com a instalação ou o upgrade, antes de continuar com a instalação.

AVG 8 sem suporte

Aviso: Endpoints AVG 8 não têm suporte no Endpoint Security 2.3. Convém que os usuários façam upgrade dos endpoints para o AVG 9 antes do upgrade para o KES 2.3, ou desinstalem totalmente os endpoints AVG 8 e, em seguida, os reinstalem em endpoints AVG 2012 após a instalação do KES 2.3.

Diretrizes para opções de instalação

A instalação das seguintes opções não é recomendada em *servidores*.

- Scanner de e-mail

Em *servidores instalados com o Exchange*, as seguintes opções não são recomendadas.

- Escudo da Web
- Vincular o scanner
- Proteção de identidade

Tanto para *servidores* quanto para *estações de trabalho*, o AVG Firewall não tem suporte para endpoints AVG 2012, mas ainda têm suporte para endpoints AVG 9.

Ações

Cada página fornece as seguintes ações:

- **Instalar**: instala o **Endpoint Security** em IDs de máquinas selecionadas. Consulte **Como instalar ou fazer upgrade de um endpoint** *(página 20)*.

  > **Aviso:** Desinstale todos os softwares antivírus/spyware/malware da máquina gerenciada antes de instalar o software cliente **Endpoint Security**.

- **Fazer upgrade**: faz upgrade de clientes endpoint AVG 9 para AVG 2012. A coluna **Status da instalação** identifica endpoints qualificados para upgrade. Consulte **Como instalar ou fazer upgrade de um endpoint** *(página 20)*.
- **Cliente Connect**: instala *somente o serviço cliente Endpoint Security* no endpoint. Isso permite que você faça o seguinte:
  - Verifique se existe um mecanismo AVG com suporte no terminal.
  - Faça upgrade ou reinstale apenas o serviço cliente **Endpoint Security**, sem afetar o componente AVG. Isso pode ser necessário se o serviço cliente **Endpoint Security** estiver desatualizado ou corrompido.
- **Remover** : remove o **Endpoint Security** de IDs de máquinas selecionadas.
- **Cancelar a operação pendente**: cancela qualquer uma das três primeiras ações, caso ainda não tenham sido concluídas.
- **Editar prompts do usuário** - Edita o prompt de aviso exibido para usuários, se um prompt de aviso for exibido. Você também pode especificar o número de minutos pelo qual o usuário tem permissão para adiar a instalação.
- **Opções de instalação**: define *opções de instalação* padrão ou em **nível de módulo** *(página 21)* para instalações ou upgrades.
- **Reinicializar**: reinicializa o computador selecionado. Periodicamente, a AVG lança uma atualização que requer uma reinicialização. A indicação `Reboot Required` é exibida na coluna **Versão**.
- **Contagem de licenças**: exibe uma janela pop-up das seguintes contagens de licenças:
  - Licenças adquiridas
  - Licenças completas disponíveis (Adquiridas mas não atribuídas, instaladas ou expiradas)
  - Licenças alocadas (Agendadas para instalação, mas a instalação ainda não foi concluída)
  - Licenças aplicadas (Licença ativa aplicada a uma máquina)
  - Licenças parciais disponíveis (Anteriormente atribuídas a uma máquina, mas retornadas ao grupo antes da expiração)
  - Licenças parciais alocadas (Disponíveis parcialmente que foram agendadas para instalação, mas a instalação ainda não foi concluída)
  - Total de licenças (Licenças adquiridas, menos licenças vencidas)
  - Licenças vencidas

Colunas de tabela

- **(Status de entrada)** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada

- O Agente está conectado mas o controle remoto foi desativado
- O Agente foi suspenso

- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Status da instalação**: os tipos de mensagens incluem:
  - (em branco): o software cliente **Endpoint Security** *não* está instalado na ID da máquina. Não há nenhum pré-requisito que o impeça de instalar o cliente nessa máquina.
  - `Application Conflict` <nome do produto>: um produto antivírus já está instalado nesta máquina e gera conflitos com a instalação do **Endpoint Security**.
  - `Requires Agent Update`: o software do agente é anterior à versão 4.7.1. Vá a página Agente >**Atualizar agente** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#549.htm)* para atualizar esse agente.
  - `Install Pending` <data/hora>: a instalação está agendada para uma data e hora específicas. Marcações de data/hora vencidas são exibidas como texto vermelho com destaque amarelo.
  - `Waiting for Service`: o serviço usado pelo agente para se comunicar com o mecanismo AVG iniciou a instalação. Essa mensagem ficará exibida até que a instalação seja concluída.
  - : a instalação foi concluída. É possível exibir as opções de instalação aplicadas a uma ID de máquina clicando nesse ícone.
  - `FAILED at <time/date and error message>`: mostra detalhes de falhas da instalação, se disponíveis, registrados pelo software cliente AVG.
  - `AVG Removed by User` : o usuário da máquina removeu o cliente AVG manualmente.
- **Origem da instalação**: se uma origem de arquivo for definida via Gerenciamento de correções > **Origem do arquivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#366.htm)*, as instalações serão originadas desse local. Caso contrário, as instalações se originam da Internet. Se a opção **Fazer download da Internet caso a máquina não consiga se conectar ao servidor de arquivos** estiver selecionada em Gerenciamento de correções > Origem do arquivo:
  - Durante a instalação de um endpoint do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, o instalador será obtido por download do servidor da Kaseya e concluirá a instalação do endpoint.
  - Durante uma atualização manual do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, a atualização será obtida por download da Internet.

  Em ambos os casos acima, a página **Visualizar registros** *(página 14)* exibe uma mensagem de erro informando o porque da falha da origem do arquivo e que está tentando fazer o download da Internet.
- **Instalado em**: a data em que o software cliente **Endpoint Security** foi instalado na ID de máquina.
- **Versão** - A versão da proteção de segurança atualmente utilizada por esta ID de máquina. Por exemplo: `8.5.322 270.12.6/2084`
  - `8.5.322`: a versão do programa AVG instalado.
  - `270.12.6/2084`: a versão completa do *banco de dados* de vírus. `270.12.6` representa a versão da *definição* e `2084` é a versão da *assinatura*. É Exibida em texto vermelho se a versão da *assinatura* é mais antiga que as últimas 5 versões de *assinatura* disponíveis ou a versão de *definição* é mais antiga do que as 2 últimas versões de *definição* disponíveis, e o agente está ativo.
  - `[KES 2.1.0.87]`: a versão do software cliente **Endpoint Security**.

Como instalar ou fazer upgrade de um endpoint

Segurança > Instalação > Instalar ou Fazer upgrade

Defina as seguintes opções depois de clicar nos botões **Instalar** ou **Fazer upgrade**. As configurações padrão são definidas com o uso do botão **Opções de instalação** *(página 21)*. Após a instalação do cliente **Endpoint Security** em uma ID de máquina, as opções de instalação aplicadas a essa ID de máquina podem ser visualizadas clicando na marca de seleção verde da coluna **Status da instalação**.

Seleção de perfil

- **Selecionar perfil**: seleciona o perfil a ser usado durante uma instalação.

Opções do instalador

- **Instalar/fazer upgrade do KServer (substituir a origem do arquivo)**: se essa opção estiver marcada, as instalações serão obtidas por download do servidor da Kaseya. Se ela estiver em branco, as instalações serão obtidas por download com o uso do método especificado em Gerenciamento de correções > **Origem do arquivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#366.htm)*.
- **Avisar o usuário antes de instalar/Forçar a instalação sem avisar o usuário**: a instalação requer um reinicialização da máquina gerenciada. Se **Avisar ao usuário antes de instalar** estiver selecionado, o usuário tem a opção de adiar a instalação por um número especificado de minutos. Caso contrário, **Forçar a instalação sem avisar o usuário** causa a instalação do software na hora agendada sem avisar ao usuário.

> **Nota:** Clique em **Editar prompts de usuário** para especificar por quantos minutos o usuário tem permissão de adiar a instalação.

Programar

- **Imediato**: selecione a caixa Imediato para iniciar a instalação assim que você clicar em Instalar.
- **Data/hora**: insira o ano, o mês, o dia, a hora e o minuto para agendar essa tarefa.
- **Escalonar por**: você pode distribuir a carga na rede programando essa tarefa. Se você definir esse parâmetro como cinco minutos, a tarefa em cada ID de máquina será programada para ocorrer a cada cinco minutos. Por exemplo, a máquina 1 é executada às 10 horas, a máquina 2 às 10 horas e 5 minutos e a máquina três, às 10 horas e 10 minutos, ...
- **Ignorar se a máquina estiver off-line**: marque essa opção para realizar essa tarefa apenas na hora agendada. Se a máquina estiver off-line, ignore e execute no próximo período e hora agendados. Desmarque para executar essa tarefa assim que a máquina se conectar depois da hora agendada.

Componentes

Componentes de estação de trabalho

- **Varredura do link** - Bloqueia websites perigodos e verifica os links retornados pelos mecanismos de busca mais populares. Não instala em navegadores sendo executados no Windows Server O/S.
  - **Busca segura ativa** - Efetua a varredura de um link exibido em uma página da web, ante que você clique no mesmo.
  - **Escudo de busca** - Identifica a classificação de segurança de um link de busca listado nas buscas do Google, Yahoo e MSN.
- **Escudo da web** - Efetua a varredura de arquivos baixados e trocados usando a mensagem instânea.

- **Varredura de e-mail** - Se selecionado, a instalação detecta o cliente de e-mail padrão em uma máquina e automaticamente instala o respectivo plug-in de varredura de e-mail.
- **Proteção de ID** - Se selecionado, a opção de proteção de identidade do AVG é ativada. Previne a ameaça alvo contra senhas, detalhes de conta bancária, números de cartão de crédito e outros ativos digitais, usando a "análise comportamental" para identificar atividade supeita em uma máquina.
- **Firewall (Não gerenciado pelo Kaseya)** - Se selecionado, a opção de firewall do AVG é ativada. Bloqueia o acesso não-autorizado, mas permite as comunicações autorizadas. *O cliente* **Endpoint Security** *não pode ser usado para manter as listas de bloqueios e as listas de permissões necessárias para essa opção.*

Componentes de servidor

- **Complemento do Sharepoint Server**: se essa opção estiver selecionada, a proteção do **Endpoint Security** será instalada para documentos no Sharepoint Server.
- **Plug-in do Exchange Server**: se essa opção estiver selecionada, a proteção de e-mail do **Endpoint Security** será instalada em instâncias do MS Exchange Server. Essa configuração é ignorada quando o cliente **Endpoint Security** está instalado em uma máquina sem o MS Exchange Server.

Instalando

Exceções de licenciamento são indicadas na área de mensagens da caixa de diálogo.

Opções de instalação

Segurança > Instalação > Opções de instalação

Certas **Opções de instalação** servem como padrões que podem ser substituídos durante a **instalação ou o upgrade de um endpoint** *(página 20)*.

Outras **Opções de instalação** servem como configurações em *nível de módulo* que são normalmente aplicadas a todas as instalações. Configurações em nível de módulo não podem ser substituídas por uma instalação ou um upgrade específico, mas se aplicam a qualquer instalação que você venha a executar posteriormente.

Opções de instalação

- **Nome do usuário** - *nível de módulo*: se marcada, insira um nome associado a essa instalação do **Endpoint Security**.
- **Nome da empresa** - *nível de módulo*: se marcada, insira o nome da empresa associada a essa instalação do **Endpoint Security**.
- **Diretório alvo** - *nível de módulo*: se marcada, insira um diretório de destino. Se estiver em branco, o diretório padrão de instalação é usado.
- **Selecionar perfil**: seleciona o perfil a ser usado durante uma instalação.
- **Desativar todos os aplicativos em execução que impedem a instalação** - nível de módulo: se essa opção estiver marcada, todos os aplicativos em execução que possam impedir a instalação bem-sucedida serão interrompidos.
- **Desativar o Windows Defender** - *nível de módulo*: a execução do Windows Defender degrada significativamente o desempenho do **Endpoint Security** e deve ser desativada por padrão com o uso dessa opção.
- **Ativar as varreduras do diretório do usuário final** - *nível de módulo*: adiciona uma opção de clique com o botão direito do mouse ao Windows Explorer, permitindo que o usuário realize a varredura de um arquivo individual ou diretório imediatamente.

Opções de procedimento do agente

- **Procedimento do agente a ser executado antes da instalação** - *nível de módulo*: selecione um procedimento de agente.
- **Procedimento do agente a ser executado depois da instalação** - *nível de módulo*: selecione um procedimento de agente.

Componentes

Componentes de estação de trabalho

- **Varredura do link** - Bloqueia websites perigodos e verifica os links retornados pelos mecanismos de busca mais populares. Não instala em navegadores sendo executados no Windows Server O/S.
  - **Busca segura ativa** - Efetua a varredura de um link exibido em uma página da web, ante que você clique no mesmo.
  - **Escudo de busca** - Identifica a classificação de segurança de um link de busca listado nas buscas do Google, Yahoo e MSN.
- **Escudo da web** - Efetua a varredura de arquivos baixados e trocados usando a mensagem instânea.
- **Varredura de e-mail** - Se selecionado, a instalação detecta o cliente de e-mail padrão em uma máquina e automaticamente instala o respectivo plug-in de varredura de e-mail.
- **Proteção de ID** - Se selecionado, a opção de proteção de identidade do AVG é ativada. Previne a ameaça alvo contra senhas, detalhes de conta bancária, números de cartão de crédito e outros ativos digitais, usando a "análise comportamental" para identificar atividade supeita em uma máquina.

Componentes de servidor

- **Complemento do Sharepoint Server**: se essa opção estiver selecionada, a proteção do **Endpoint Security** será instalada para documentos no Sharepoint Server.
- **Plug-in do Exchange Server**: se essa opção estiver selecionada, a proteção de e-mail do **Endpoint Security** será instalada em instâncias do MS Exchange Server. Essa configuração é ignorada quando o cliente **Endpoint Security** está instalado em uma máquina sem o MS Exchange Server.

Definir perfil

Segurança > Definir perfil

A página **Definir perfil** gerencia os perfis de segurança. Cada perfil de segurança represneta um conjunto diferente de opções de segurança ativadas ou desativadas. As alterações em um perfil de segurança afetam todas as IDs de máquina que têm aquele perfil de segurança atribuído. Um perfil de segurança é atribuído à ID de máquina via Segurança > **Atribuir perfil** *(página 29)*. Normalmente, diferentes tipos de máquinas ou redes requerem difernetes perfis de segurança. Um amostra de perfil é fornecida. Você não pode alterar o perfil de amostra, mas pode salvá-lo com um novo nome e efetuar as alterações na cópia. O mesmo perfil pode ser usado para gerenciar endpoints AVG 9 e AVG 2012.

Esta página lhe fornece as seguintes ações:

- **Salvar** - Salva as alterações de um perfil de segurança.
- **Ssalvar como** - Cria um novo perfil de segurança ao salvá-lo usando um nome diferente.
- **Excluir** - Exclui um perfil de segurança existente.

- **Compartilhar** - Compartilha um perfil de segurança privado. Outros usuários não pode ver os perfis de segurança privados. O compartilhamento de um perfil de segurança privado o torna um perfil de segurança público. Os direitos de compartilhamento são atribuídos *por objeto*. Existem três opções de caixa de seleção de compartilhamento. As duas primeiras caixas de seleção são *mutuamente exclusivas* e determinam quais direitos de compartilhamento são atribuídos. Se nenhuma das duas primeiras caixas de seleção forem selecionadas, o objeto compartilhado somente pode ser visto por usuários com direitos de compartilhamento atribuídos, mas o objeto não pode ser usado ou editado. As caixas das listas **Compartilhado** e **Não compartilhado** e a terceira caixa de seleção determinam quem pode *ver* o objeto.
  - **Permitir que outros administradores modifiquem** - Se selecionado, os direitos de compartilhamento para o objeto incluem a capacidade de usá-lo, visualizar seus detalhes e editá-lo.
  - **Outros administradores podem usar, mas podem não visualizar ou editar** - Se selecionado, os direitos de compartilhamento para o objeto somente permitem utilizá-lo.
  - **Tornar público (visto por todos os administradores)**: se selecionado, assegura que *todos* os usuários do VSA, atuais e futuros, possam *ver* o objeto. Se deixado em branco, somente as função de usuário e usuários selecionados podem ver o objeto compartilhado. Se deixado em branco, e novos usuários ou funções de usuário forem adicionados posteriormente, será preciso retornar a esta caixa de diálogo para permitir que eles vejam o objeto específico.
- **Obter a propriedade** - Obtém a **propriedade** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#5537.htm)* de qualquer perfil de segurança público.

Para definir ou manter um perfil de segurança

1. Selecione um perfil de segurança na lista suspensa **Selecionar perfil**.
2. Defina as opções nas guias do perfil de segurança:
   - **Geral**
   - **Resident Shield**
   - **Scanner de e-mail**
   - **Varredura completa**
   - **Exchange**
   - **Excluir diretórios**
   - **Excluir PUPs**
   - **Atualizações**
3. Clique no botão **Salvar** ou **Salvar como** para salvar o perfil de segurança.

Geral

Senha da GUI da área de trabalho do AVG

- **Proteger GUI da área de trabalho do AVG com senha**: insira uma senha para forçar o usuário a inserir uma senha antes de ocultar a área de trabalho, o ícone de bandeja e os atalhos do menu Iniciar do AVG. Se essa opção estiver em branco, não será necessário inserir uma senha.

Vault de vírus

- **Limitar o tamanho do vault** - Se selecionado, limita o tamanho do vault como especificado usando as seguintes opções:
  - **Tamanho máximo do Vault: <N>% do disco local**: insira a porcentagem máxima de espaço em disco a ser alocado para armazenar ameaças em quarentena.
  - **Espaço mínimo disponível remanescente no disco local** - Insira o número mínimo em megabytes a ser alocado no disco para armazenar as ameaças em quarentena.

- **Exclusão automa´tica de arquivo** - Se selecionado, exckui automaticamente os arquivos como especificado pelas seguintes opções:
  - **Excluir arquivos mais antigos que <N> dias**: insira o número de dias para armazenar ameaças em quarentena antes que elas sejam automaticamente excluídas.
  - **Número máximo de arquivos a serem armazenados** - Insira o número máximo de ameaças em quarentena a serem armazenadas.

Notificações na bandeja do sistema

- **Exibir notificações na bandeja do sistema** - Se selecionado, as seguintes notificações na bandeja do sistema podem ser opcionalmente ativadas. Todas as mensagens de notificação são exibidas na máquina gerenciada junto a bandeja do sistema.
- **Exibir notificações sobre atualização na bandeja**: se selecionada, essa opção exibirá uma mensagem de notificação informando que o software **Endpoint Security** está sendo atualizado.
- **Exibir notificações na bandeja sobre a varredura** - Se selecionado, exibe uma mensagem de notificação de que está sendo efetuada a varredura da máquina.
- **Exibir notificações na bandeja do sistema relativas ao escudo residente (ação automática)** - Se selecionado, exibe uma mensagem de notificação de que o escudo residente executou uma ação contra uma ameaça.
- **Exibir notificação sobre alteração do status do componente**: se selecionada, essa opção exibirá uma mensagem de notificação informando que o status de um dos componentes do **Endpoint Security** mudou.
- **Exibir notificações relativas a avrredura de e-mail** - Se selecionado, exibe uma mensagem de notificação de que a varredura de e-mail executou uma ação contra uma ameaça de e-mail.

Menu Ícone do Agente

- **Exibir a opção para ativar/desativar o escudo residente no menu Ícone do Agente** - Se selecionado:
  - As opções **Ativar segurança** e **Cancelar varredura** são exibidas no menu de tarefas do agente da máquina gerenciada.
  - O usuário pode clicar na opção **Ativar segurança** no menu do agente para ativar ou desativar a proteção de segurança.
  - O usuário pode clicar na opção **Cancelar varredura** no menu do agente para cancelar uma varredura de proteção de segurança em andamento.

> **Nota:** O usuário também pode ativar/desativar remotamente a proteção de segurança via Segurança > **Status da segurança** *(página 5)*.

Resident Shield

O escudo residente é um recurso residente na memória.

- **Ativar o escudo residente** - Se selecionado, os seguintes tipos de arquivos são varridos quando forem copiados, abertos ou salvos. Se estiver em branco, nenhum outra opção do **Escudo residente** é avaliada.

> **Nota:** Você também pode **Ativar/Desativar o Resident Shield por procedimento de agente** *(página 8)*.

Tipos de arquivos

- **Varrer todos os arquivos** - Se selecionado, todos os arquivos na máquina gerenciada são varridos.
- **Varrer arquivos infectáveis e tipos de documentos selecionados** - Se selecionado, especifica as extensões *adicionais* de arquivos de programas e documentos a serem incluídos ou excluídos usando as seguintes opções:

- **Excluir os arquivos com as seguintes extensões da varredura** - Especifica as extensões de arquivos de programas de documentos a serem excluídas de uma varredura. As extensões excluídas têm precedência sobre extensões incluídas. Insira cada extensão separa por um caractere de ponto e vírgula (;).
- **Sempre varrer os arquivos com as seguintes extensões** - Especifica as extensões de arquivos de programas de documentos a serem incluídas em uma varredura. Insira cada extensão separa por um caractere de ponto e vírgula (;). O esdudo residente varre as seguintes extensões de arquivo sem a necessidade de serem especificadas. 386; ASP; BAT; BIN; BMP; BOO; CHM; CLA; CLASS; CMD; CNM; COM; CPL; DEV; DLL; DO*; DRV; EML; EXE; GIF; HLP; HT*; INI; JPEG*; JPG; JS*; LNK; MD*; MSG; NWS; OCX; OV*; PCX; PGM; PHP*; PIF; PL*; PNG; POT; PP*; SCR; SHS; SMM; SYS; TIF; VBE; VBS; VBX; VXD; WMF; XL*; XML; ZL*;
- **Varrer os arquivos sem uma extensão** - Se selecionado, a avrredura inclui os arquivos sem uma extensão.

Opções adicionais

- **Varrer por cookies de rastreamento** - Se selecioando, a varredura inclui os cookies de rastreamento de navegação na Internet. Os cookies de rastreamentoencontrados são imediatamente excluídos e não são movidos para o vault de vírus.
- **Varrer os programas potencialmente indesejados e ameaças de spyware** - Se selecionado, a avrredura detecta aplicativos executáveis ou bibliotecas DLL que poderiam ser programas potencialmente indesejados. Alguns programas, especialmente os gratuitos, incluem adware e podem ser detectados e reportados pelo **Endpoint Security** como **programas potencialmente indesejados**.
- **Varrer arquivos ao fechar** - Se selecionado, os arquivos são varridos quando são fechados.
- **Verrer o setor de boot da mídia removível** - Se selecionado, a avarredura inclui o setor de boot da mídia removível.
- **Usar heuristica** - Se selecionado, a varredura inclui a análise heurística. A análise heurística executa uma emulação dinâmica das instruções de objeto varrido dentro de um ambiente de computação virtual.

Scanner de e-mail

- **Ativar a varredura de e-mail** - Se selecionado, o e-mail de entrada e saída e os anexos são varridos quanto a vírus. Se estiver em branco, nenhuma outra opção da **Proteção de e-mail** é avaliada.

> **Nota: Scanner de e-mail** não é recomendado para *servidores*. Consulte a guia **Exchange** abaixo.

Varredura de e-mail

- **Verificar e-mail de entrada** - Se selecionado, o e-mail de entrada é varrido.

> **Certificação:** Alguns clientes de e-mail suportam a anexação de texto em mensagens de e-mail que certificam que o e-mail foi varrido quanto ao vírus.

  - **Não certificar o e-mail** - Se selecionado, o e-mail de entrada não é certificado.
  - **Certificar todos os e-mails** - Se selecionado, todos os e-mails de entrada são certificados.
  - **Somente certificar e-mails com anexos** - Se selecionado, somente os e-mails de entrada com anexos são certificados.
  - **Certificação de e-mail de entrada** - Texto de certificação anexado ao e-mail de entrada.
- **Verificar e-mail de saída** - Se selecionado, o e-mail de saída é varrido.
  - **Não certificar o e-mail** - Se selecionado, o e-mail de saída não é certificado.
  - **Certificar todos os e-mails** - Se selecionado, todos os e-mails de saída são certificados.

  - **Somente certificar e-mails com anexos** - Se selecionado, somente os e-mails de saída com anexos são certificados.
  - **Certificação de e-mail de saída** - Texto de certificação anexado ao e-mail de saída.
- **Modificar o assunto das mesagens marcadas como vírus** - Adiciona texto de prefixo ao assunto de uma mensagem que contêm vírus.

Propriedades da varredura

- **Usar heurística** - Aplica em uma mensagem de e-mail. Se selecionado, a varredura inclui a análise heurística. A análise heurística executa uma emulação dinâmica das instruções de objeto varrido dentro de um ambiente de computação virtual.
- **Verrer programas potencialmente indesejados e ameças de spyware threats** - Se selecionado, a varredura de e-mail inclui a varredura por spyware, adware, e programas potencialemente indesejados.
- **Varrer dentro de arquivos** (RAR, RAR 3.0, ZIP, ARJ, CAB) - Se selecionado, os arquivos de e-mail são varridos.

Relatório de anexos de e-mail (como uma ameaça)

- **Reportar os arquivos protegidos por senha** - Se selecionado, reporta os anexos (zip, rar, etc) de arquivos protegidos por senha no e-mail como ameaças.
- **Reportar os documentos protegidos por senha** - Se selecionado, reporta os documentos anexos protegidos por senha no e-mail como ameaças.
- **Reportar arquivos contendo macros** - Se selecionado, reporta os arquivos contendo macros anexados ao e-mail como ameaças.
- **Reportar extensões ocultas** - Se selecionado, reporta os arquivos que usam uma extensão oculta. Alguns vírus se escondem ao duplicar sua extensão de arquivo. Por exemplo, o vírus `VBS/Iloveyou` anexa um arquivo, `ILOVEYOU.TXT.VBS`, a e-mails. A configuração padrão do Windows é ocultar extensões conhecidas e, portanto, o arquivo se parece com `ILOVEYOU.TXT`. Ao abri-lo, você na verdade não abre um arquivo de texto `.TXT`, e sim executa um arquivo de procedimentos `.VBS`.
- **Mover anexos reportados para o vault de vírus (somente e-mail de entrada)** - Se selecionado, os anexos de e-mail reportados são movidos para o vault de vírus. Eles são exibidos na guia **Vault de vírus** da página **Visualizar ameaças** *(página 5)* ao invés de na guia **Ameças atuais**.

Varredura completa

Configurações de varredura

- **Varrer os programas potencialmente indesejados e ameaças de spyware** - Se selecionado, a avrredura detecta aplicativos executáveis ou bibliotecas DLL que poderiam ser programas potencialmente indesejados. Alguns programas, especialmente os gratuitos, incluem adware e podem ser detectados e reportados pelo **Endpoint Security** como **programas potencialmente indesejados**.
- **Varrer por cookies de rastreamento** - Se selecioando, a varredura inclui os cookies de rastreamento de navegação na Internet. Os cookies de rastreamentoencontrados são imediatamente excluídos e não são movidos para o vault de vírus.
- **Varrer dentro de arquivos** - Se selecionado, a varredura inclui arquivos de arquivamento—como arquivos ZIP e RAR.
- **Usar heuristica** - Se selecionado, a varredura inclui a análise heurística. A análise heurística executa uma emulação dinâmica das instruções de objeto varrido dentro de um ambiente de computação virtual.
- **Varrer o ambiente do sistema** - Se selecionado, as áreas do sistema são varridas antes de iniciar a varredura completa.

- **Varrer somente os arquivos infectáveis** - Se selecionado, os arquivos "infectáveis" são varridos com base em seu conteúdo a despeito de suas extensões de arquivo. Por exemplo, um arquivo EXE poderia ser renomeado mas ainda pode estar infectado. Os seguintes tipos de arquivos são considerados arquivos "infectáveis":
  - **tipo EXE** - COM; DRV; EXE; OV?; PGM; SYS; BIN; CMD; DEV; 386; SMM; VXD; DLL; OCX; BOO; SCR; ESL; CLA; CLASS; BAT; VBS; VBE; WSH; HTA; HTM; HTML; ?HTML; CHM; INI; HTT; INF; JS; JSE; HLP; SHS; PRC; PDB; PIF; PHP; ZL?; ASP; LNK; EML; NWS; CPL; WMF
  - **tipo DOC** - DO?; XL?; VBX; RTF; PP?; POT; MDA; MDB; XML; DOC?; DOT?; XLS?; XLT?; XLAM; PPT?; POT?; PPS?; SLD?; PPAM; THMX

Desempenho

- **Selecionar a prioridade de sistema para a varredura** - Define como quão rápido a varredura é executada e quanto de recursos do sistema a varredura usa. Você pode definir a varredura para que seja executada o mais rápido possível enquanto torna mais lento notadamente o computador, ou é possível escolher que a varredura use o menos de recursos possível do sistema, ao prolongar o tempo de varredura.

Exchange

- **Ativar o AVG para o Exchange Server** - Ativar ou desativar a varredura de e-mail para MS Exchange Servers atribuídos.

> **Nota:** Se você instalar a proteção de e-mail em uma ou mais instâncias do MS Exchange Server, crie um único perfil e somente o aplique a essas instâncias. A guia **Definir perfil** > Exchange deve ser apenas ativada e aplicada a instâncias do MS Exchange Server.

Certificação de e-mails

- **Ativar**: se marcada, essa opção adicionará uma nota de certificação a e-mails verificados em instâncias do MS Exchange Server. Personalize a nota de certificação no campo de texto.

Desempenho

- **Executar as varreduras em segundo plano** - Ativar ou desativar a varredura em segundo plano. A varredura em segundo plano é um dos recursos da interface do aplicativo VSAPI 2.0/2.5. Ela fornece a varredura por ameaça de bancos de dados de mensagens do Exchange. Sempre que um item não tenha sido varrido antes de ser encontrado nas pastas de caixas de correio do usuário, ele é submetido ao AVG para varredura do Exchange 2000/2003 Server. A varredura e pesquisa por objetos não exemindos é executada em paralelo. Uma ameaça específica de baixa prioridade é usada para cada banco de dados, o que garante outras tarefas, por exemplo, o armazenamento de mensagens de e-mail no banco de dados do Microsoft Exchange, sejam sempre executadas preferencialmente.
- **Varrer de forma pró-ativa** - Ativa ou desatiba a varredura pró-ativa do VSAPI 2.0/2.5. A varredura pró-ativa envolve o gerenciamento de prioridade dinâmica de itens na fila de varredura. Itens de menor prioridade não são varridos a não ser que outros de maior prioridade tenham sido varridos. A prioridade de um item aumenta se um cliente tenta usá-lo, portanto, a precedência do item muda dinamicamente de acordo com atividade do usuário.
- **Verrer arquivos RTF** - Especifica se os arquivos RTF devem ou não ser varridos.
- **Varredura de ameaças** - O processo de varredura é organizado por padrão para aumentar o desempenho geral da varredura por um determinado nível de paralelismo. O número de organizações é calculado em 2 vezes o "number_ of_processors" +1.
- **Expiração da varredura** - O intervalo máximo contínuo, em segundo, para que uma organização acesse a mesagem que está sendo varrida.

Excluir diretórios

Excluir diretórios

Aviso: Apenas exclua diretórios se o seu conteúdo for conhecido como sem ameaças.

- **Adicionar novos registros** - Adiciona diretórios excluídos de uma varredura. Algus diretórios podem estar livres de organização que foram erroneamente interpretados como malware.
  - **Nome do arquivo**: insira o nome do diretório.

Excluir arquivos do Resident Shield

Excluir arquivos do Resident Shield (Opção disponível apenas no AVG2012 Resident Shield, ignorada no AVG9)

Aviso: Apenas exclua arquivos se o seu conteúdo for conhecido como sem ameaças.

Use essa guia para excluir arquivos específicos *manualmente*. Essa lista de exclusões só fica ativa com a varredura ativa do Resident Shield.

- **Adicionar novo registro** - Adiciona arquivos PUP a serem excluídos de uma varredura. Alguns arquivos podem ser livres de organização, mas podem ser erroneamente interpretados como programas potencialmente indesejados (PUPs).
  - **Nome do arquivo** - Insira o nome do arquivo.

Excluir PUPs

Exclui programas potencialmente indesejados

Aviso: Apenas exclua arquivos se o seu conteúdo for conhecido como sem ameaças.

Use esta guia para excluir programas potencialmente indesejados, ou PUPs, *manualmente*. Ameaças que não são PUP não podem ser adicionadas à lista de exclusões de PUP. A página Visualizar ameaças fornece um método mais rápido de identificar e excluir PUPs.

- **Adicionar novo registro** - Adiciona arquivos PUP a serem excluídos de uma varredura. Alguns arquivos podem ser livres de organização, mas podem ser erroneamente interpretados como programas potencialmente indesejados (PUPs).
  - **Nome do arquivo** - Insira o nome do arquivo.
  - **Checksum** - Insira o valor de checksum do arquivo. Para determinar o valor do checksum, abre a **IU do AVG** em uma máquina que contenha o arquivo. Selecione **Ferramentas > Configurações avançadas**. Selecioe a folha de propriedades **Exceções de PUP**. Clique no botão **Adicionar exceção**. Selecione o arquivo ao navegar no diretório local da máquina. O valor de checksum correspondente é exibido. Copie e cole o valor da soma de verificação da **Interface de usuário do AVG** na caixa de diálogo **Adicionar novo registro** da guia **Excluir PUPs**, em Segurança > **Definir perfil**.
  - **Tamanho do arquivo** - Insira o tamanho do arquivo em bytes. Para determinar o tamanho do arquivo, clique com o botão direito do mouse no Windows Explorer e verifique o valor de **Tamnho** em bytes.

Atualizações

Use esta guia para configurar com as atualizações do AVG são baixadas.

Configurações de proxy

Ativa/desativa usando um servidor de proxy para baixar atualizações do AVG.

- **Não usar proxy** - Desativa as configurações de proxy.
- **Usar proxy** - Ativa as configurações de proxy.
- **Tentar conectar usando proxy, e se falhar, conectar diretamente** - Ativa as configurações de proxy. Se o proxy falhar, conecta diretamente.

As configurações **Manual** e **Automática** serão aplicáveis se uma opção de proxy acima for selecionada.

- **Manual** - Define manualmente as configurações de proxy.
  - **Servidor** - Insira um nome de servidor de proxy válido ou um endereço IP.
  - **Porta** - Insira um número de porta.
  - **Usar autenticação de PROXY** - Se selecionado, a autenticação de proxy é necessária.
    - ✓ **Nome do usuário** - Se **Usar autenticação de PROXY** estiver selecionado, insira um nome de usuário válido.
    - ✓ **Senha** - Se **Usar autenticação de PROXY** estiver selecionado, insira uma senha válida.
- **Auto** - Define automaticamente as configurações de proxy.
  - **Do navegador** - Selecione um navegador padrão no memu suspenso para definir as configurações de proxy.
  - **Do script** - Insira o caminho compelto de um script que especifica o endereço do servidor proxy.
  - **Auto-detectar** - Tenta obter as configurações diretamente do servidor proxy.

Atualizar URL

O AVG fornece um URL padrão para baixar atualizações. Você pode baixar preferencialmente de um RUL personalizado.

- **Usar URL personalizado para atualização** - Selecione esta opção para baixar preferencialmente as atualizações de um URL personalizado.
  - **Nome** - Insira o nome do URL personalizado de atualização.
  - **URL** - Insira o URL.

Atribuir perfil

Segurança > Atribuir perfil

A página **Atribuir perfil** atribui os perfis de segurança a IDs de máquinas licenciadas para usar o **Endpoint Security**. Perfis de segurança são definidos em Segurança > **Definir perfil** *(página 22)*.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Aplicar configuração**: clique em **Aplicar configuração** para aplicar o perfil de segurança exibido na caixa suspensa **Selecionar perfil** às IDs de máquinas selecionadas.
- **Selecionar perfil**: selecione um perfil de segurança a ser aplicado a IDs de máquinas selecionadas.
- **Somente exibir máquinas com o perfil selecionado**: se marcada, essa opção filtrará a área de paginação de acordo com o perfil de segurança selecionado.

Colunas de tabela

- **Status de entrada** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.

- Conectada mas aguardando o término da primeira auditoria
- Agente on-line
- Agente e usuário conectados no momento.
- Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
- No momento o Agente está desconectado
- O Agente nunca efetuou a entrada
- O Agente está conectado mas o controle remoto foi desativado
- O Agente foi suspenso

- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Nome do perfil**: exibe o perfil de segurança atribuído à ID de máquina. Exibe o status da ID de máquina caso haja um problema.

Configurações de registro: Segurança

Segurança > Configurações de logs

A página **Configurações de logs** especifica por quantos dias manter dados de log da proteção de segurança para IDs de máquinas licenciadas para usar o **Endpoint Security**. Determinadas ma´quinas, como servidores da web, podem garantir a manutenção de um histótico mais longo de ataques de vírus do que outros tipos de máquinas.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Ações

- **Aplicar configuração**: clique em **Aplicar configuração** para aplicar o número de dias especificado no campo **<N> dias para manter as entradas de logs** às IDs de máquinas selecionadas.
- **<N> dias para manter as entradas de log**: insira o número de dias para manter dados de log da proteção de segurança.

Colunas de tabela

- **Status de entrada** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.

- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Dias antes de expirar o log**: mostra por quantos dias os dados de log da proteção de segurança são mantidos para uma ID de máquina.

Status do Exchange

Segurança > Status do Exchange

A página **Status do Exchange** mostra o status da proteção de e-mail em instâncias do MS Exchange Server que têm o **Endpoint Security** instalado. Durante a instalação do **Endpoint Security** em uma máquina, se o MS Exchange for detectado, o plug-in para a proteção de e-mail do MS Exchange será automaticamente instalado. A proteção da caixa de correio pode ser excluída de servidores com o Exchange na página **Definir perfil** *(página 22)*.

Nota: Qualquer malware detectado pela proteção de e-mail do MS Exchange Server será imediatamente excluído do MS Exchange Server e *somente* será exibido na guia **Vault de vírus** da página **Visualizar ameaças** *(página 12)*.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Também, a ID de máquina precisa ter o MS Exchange Server instalado.

Caixas de correio / Licenças de caixa de correio

Exibe o número de caixas de correio do Exchange Server protegidas e o número de licenças de caixa de correio usadas e disponíveis. O licenciamento é obrigatório, e uma licença é necessária para cada caixa de correio em uso.

Nota: Consulte **Licenciamento do Endpoint Security** no tópico **Visão geral da segurança** *(página 1)*.

Ações

- **Remover**: remove a instalação do Exchange.
- **Cancelar ação pendente**: cancela a remoção da proteção do Exchange.

Colunas de tabela

- **Status de entrada** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos
  - No momento o Agente está desconectado
  - O Agente nunca efetuou a entrada
  - O Agente está conectado mas o controle remoto foi desativado
  - O Agente foi suspenso
- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.

- **Status da instalação**: se essa opção estiver marcada, o software cliente **Endpoint Security** será instalado na ID da máquina. Se o software do agente for anterior à versão 4.7.1, a mensagem `Requires Agent Update` será exibida. Se essa opção ficar em branco, o software cliente **Endpoint Security** *não* será instalado na ID de máquina.
- **Origem da instalação**: se uma origem de arquivo for definida via Gerenciamento de correções > **Origem do arquivo** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#366.htm)*, as instalações serão originadas desse local. Caso contrário, as instalações se originam da Internet. Se a opção **Fazer download da Internet caso a máquina não consiga se conectar ao servidor de arquivos** estiver selecionada em Gerenciamento de correções > Origem do arquivo:
  - Durante a instalação de um endpoint do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, o instalador será obtido por download do servidor da Kaseya e concluirá a instalação do endpoint.
  - Durante uma atualização manual do **Endpoint Security** v2.x, se a origem do arquivo estiver inativa ou se as credenciais forem inválidas, a atualização será obtida por download da Internet.

  Em ambos os casos acima, a página **Visualizar registros** *(página 14)* exibe uma mensagem de erro informando o porque da falha da origem do arquivo e que está tentando fazer o download da Internet.
- **Caixas de correio**: o número de contas de e-mail no MS Exchange Server.
- **Instalado em**: a data em que a proteção de e-mail do MS Exchange Server foi instalada na ID da máquina.

Definir conjuntos de alarme

Segurança > Definir conjuntos de alarme

A página **Definir conjuntos de alarme** define os conjuntos de condições de alarme usadas para acionar alarmes usando a página **Aplicar conjuntos de alarme** *(página 33)*.

Ações

- **Salvar** - Salva o conjunto de alarmes.
- **Salvar como** - Salva uma conjunto de alarmes com um novo nome.
- **Excluir** - Exclui um conjunto de alarmes.
- **Compartilhar** - É exibido se você possui um conjunto de alarmes selecionado. Compartilhe este conjunto de alarmes com usuários, funções de usuário ou para tornar público para todos os usuários. Os direitos de compartilhamento são atribuídos *por objeto*. Existem três opções de caixa de seleção de compartilhamento. As duas primeiras caixas de seleção são *mutuamente exclusivas* e determinam quais direitos de compartilhamento são atribuídos. Se nenhuma das duas primeiras caixas de seleção forem selecionadas, o objeto compartilhado somente pode ser visto por usuários com direitos de compartilhamento atribuídos, mas o objeto não pode ser usado ou editado. As caixas das listas **Compartilhado** e **Não compartilhado** e a terceira caixa de seleção determinam quem pode *ver* o objeto.
  - **Permitir que outros administradores modifiquem** - Se selecionado, os direitos de compartilhamento para o objeto incluem a capacidade de usá-lo, visualizar seus detalhes e editá-lo.
  - **Outros administradores podem usar, mas podem não visualizar ou editar** - Se selecionado, os direitos de compartilhamento para o objeto somente permitem utilizá-lo.
  - **Tornar público (visto por todos os administradores)**: se selecionado, assegura que *todos* os usuários do VSA, atuais e futuros, possam *ver* o objeto. Se deixado em branco, somente as função de usuário e usuários selecionados podem ver o objeto compartilhado. Se deixado em branco, e novos usuários ou funções de usuário forem adicionados posteriormente, será preciso retornar a esta caixa de diálogo para permitir que eles vejam o objeto específico.

- **Pegar a propriedade** - É exibido se você *possui* um conjunto de alarmes selecionado. Clique para pegar a **propriedade** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#5537.htm)* e efetuar alterações no conjunto de alarmes.

Para criar um novo conjunto de alarmes

1. Selecione `<No Alarm Sets Saved>` na lista suspensa **Selecionar perfil**. Alternativamente, você pode selecionar um conjunto de alarmes existente e clicar em **Salvar como**.
2. Marque uma ou mais caixas de seleção de condição de alerta.
3. Use **Ignorar outros alarmes por <N><períodos>** para especificar por quantos minutos ignorar o mesmo conjunto de condições de alertas. Defina 0 para acionar um alarme sempre que uma condição de alerta ocorrer.
4. Clique em **Salvar** para salvar o conjunto de alarmes.

Para excluir um conjunto de alarmes

1. Selecione um conjunto de alarmes na lista suspensa **Selecionar perfil**.
2. Clique em **Excluir** para excluir o conjunto de alarmes.

Ignorar alarmes adicionais por <N> <períodos>

Especifique o número de períodos que deseja que o mesmo tipo de alarme a ser ignorado após o primeiro alarme ter sido acionado.

Condições de alarme

Selecione qualquer um dos seguintes tipos de condições de alarme para incluí-lo em um conjunto de alarmes do **Endpoint Security**.

- **Ameaça detectada e não solucionada** - Uma ameaça foi adicionada na guia **Ameaças atuais** da página **Visualizar ameaças** *(página 12)* que não puderam ser automaticamente solucionadas.
- **Proteção desativada** - A proteção de segurança foi desativada.
- **Definição atualizada**: a proteção de segurança foi atualizada com a versão mais recente do **Endpoint Security**.
- **Varredura agendada completada** - Uma varredura de proteção de segurança foi completada.
- **Reincialização requerida** - Uma reinicialização é requerida.
- **Proteção ativada** - A proteção de segurança foi ativada.
- **Erro no serviço**: o serviço do **Endpoint Security** foi interrompido.
- **Definição não atualizada em <N> dias**: a proteção de segurança não foi atualizada durante o número de dias especificado.
- **A varredura agendada não foi completada** - Uma varredura de proteção de segurança agendada não foi completada.
- **AVG removido pelo usuário** - Um usuário da máquina desinstalou o cliente AVG da máquina gerenciada.

Aplicar conjuntos de alarme

Segurança > Aplicar conjuntos de alarmes

A página **Aplicar conjuntos de alarmes** cria alertas em resposta a condições de alerta da proteção de segurança definidas com o uso de **Definir conjuntos de alarmes** *(página 32)*. Os conjuntos de alarmes são aplicados às IDs de máquinas selecionadas licenciadas para usar o **Endpoint Security**.

A lista de IDs da máquina que você pode selecionar depende do filtro ID de máquinas/ID de grupos e do escopo que você está utilizando. Para serem exibidas nessa página, as IDs de máquina devem ter o software cliente **Endpoint Security** instalado na máquina gerenciada na página Segurança > **Instalação** *(página 17)*.

Esta página lhe fornece quatro ações:

- **Aplicar** - Aplicar um conjunto de alarmes selecionado em IDs de máquina selecionadas.
- **Remover** - Remove um conjunto de alarmes selecionado de IDs de máquina selecionadas.
- **Remover todos** - Remove todos os conjuntos de alarmes atribuídos às IDs de ma´quina selecionadas.

Para criar um alerta

1. Marque estas caixas de seleção para realizar suas ações correspondentes quando uma condição de alerta for encontrada:
   - Criar um **a**larme
   - Criar **t**icket
   - Executar o **s**cript
   - Destinatários de **e**-mail
2. Definir parâmetros adicionais para e-mails.
3. Selecione um conjunto de alarmes.
4. Selecione as IDs de máquina às quais aplicar o conjunto de alarmes.
5. Clique em **Aplicar** para atribuir o conjunto de alarmes para IDs de máquina selecionadas.

Para cancelar um alerta

1. Selecione as caixas de seleção de ID de máquina.
2. Clique em **Remover** para remover o conjunto de alarmes atribuídos às IDs de máquina selecionadas.

Opções

- **Criar alarme**: se essa opção estiver selecionada e uma condição de alerta for detectada, um alarme será criado. Alarmes são exibidos em Monitor > Lista de painéis, Monitor > Resumo de alarmes e em Centro de informações > Emissão de relatórios > Relatórios > Logs > Log de alarmes.
- **Criar ticket**: se essa opção estiver selecionada e uma condição de alerta for detectada, será criado um ticket.
- **Executar script após o alerta** - Se a opção estiver selecionada e uma condição de alerta for encontrada, um procedimento do agente será executado. É necessário clicar no link **selecionar procedimento de agente** para escolher um procedimento de agente a ser executado. Você pode, como opção, direcionar o procedimento do agente para ser executado em uma faixa especificada de IDs de máquinas clicando no link **ID desta máquina**. Estas IDs de máquinas especificadas não precisam corresponder à ID da máquina que encontrou a condição do alerta.
- **Destinatários de e-mail**: se essa opção estiver marcada e uma condição de alerta for detectada, e-mails serão enviados aos endereços especificados. Os e-mails serão enviados diretamente do VSA para os endereços especificados no alerta. Defina o **Endereço de origem** em Sistema > E-mail de saída.
- **Selecionar um conjunto de alarmes**: selecione um conjunto de alarmes a ser aplicado às IDs de máquinas selecionadas.

Colunas de tabela

- **(Status de entrada)** - Esses ícones indicam o status de entrada do agente em cada máquina gerenciada. Passar o cursor do mouse sobre o ícone de entrada exibe a janela Visualização rápida do agente.
  - Conectada mas aguardando o término da primeira auditoria
  - Agente on-line
  - Agente e usuário conectados no momento.
  - Agente e usuário conectados no momento, mas usuário inativo há 10 minutos

 No momento o Agente está desconectado
 O Agente nunca efetuou a entrada
 O Agente está conectado mas o controle remoto foi desativado
 O Agente foi suspenso

- **(Caixa de seleção "Selecionar tudo")**: clique nesta caixa de seleção para selecionar todas as linhas na área de paginação. Se selecionada, clique nesta caixa de seleção para cancelar a seleção todas as linhas na área de paging.
- **ID Machine.Group**: Nome de ID de máquina/ID de grupo/ID de organização exclusivo para uma máquina no VSA.
- **Conjunto de alarmes**: lista os conjuntos de alarmes atribuídos à cada ID de máquina.
- **ATSE**: o código de resposta ATSE atribuído a IDs de máquinas ou dispositivos SNMP:
  - A = Criar **a**larme
  - T = Criar **t**icket
  - S = Executar procedimento do agente
  - E = Destinatários de **e**-mail
- **Endereço de e-mail**: uma lista de endereços de e-mail separados por vírgula para os quais as notificações serão enviadas.

Relatórios de segurança

Os seguintes conjuntos de dados estão disponíveis para dar suporte à criação de definições de relatórios personalizadas e a modelos de relatórios do **Endpoint Security**. Eles estão localizados em Centro de informações > Configurar & Design > **Partes de relatórios**.

- Conjunto de alarmes do KES
- Atribuição de conjunto de alarmes do KES
- Logs de eventos do KES
- Status do Exchange do KES
- Status da máquina do KES
- Ameaças do KES
- Estatísticas de ameaças do KES

Além disso, as seguintes definições de relatórios com "formato fixo" herdadas são fornecidas.

Nesta seção

Resumo executivo - Segurança de endpoints

Resumo executivo

O relatório em Centro de informações > Emissão de relatórios > Relatórios > Resumo executivo inclui uma seção denominada **Segurança de endpoints desde os últimos N dias**. Ele inclui as seguintes estatísticas.

- Total de ameaças detectadas

- Ameaças ativas atuais
- Ameaças atuais em vaults
- Ameaças resolvidas
- Verificações Concluídas
- Atualizações Feitas
- Máquinas com o KES instalado

A **pontuação de saúde rede** do **Resumo Executivo** inclui uma categoria **pontuação de endpoint**. Ameaças não tratadas são as ameaças listadas na guia **Ameaças atuais** da página Segurança > **Visualizar ameaças** *(página 12)*. As ameaças não tratadas representam problemas potenciais ao sistema. O número de ameaças não tratadas geradas por cada máquina durante o período especificado é calculado assim:

0 ameaças não tratadas	100%
De 1 a 4 ameaças não tratadas	75%
De 5 a 10 ameaças não tratadas	50%
mais de 10 ameaças não tratadas	25%

Você pode ajustar a gravidade com que cada categoria afeta a **pontuação de saúde da rede** total ao ajustar o valor do **peso** para cada categoria. Os pesos variam de 0 a 100. Defina o peso para zero para desativar aquela categoria.

Segurança - Configuração

Centro de informações > Emissão de relatórios > Relatórios > Segurança > Configuração

- É exibido apenas se o módulo de complemento do SEgurança estiver instalado.
- Informações similares são fornecidas em > Status da segurança *(página 5)*, Visualizar logs *(página 14)* e Visualizar ameaças *(página 12)*.

A definição do relatório **Segurança - Configuração** gera relatórios para os seguintes tipos de dados de segurança mantidos pelo VSA.

- Tempo de Instalação
- Instalador
- Versão
- Data de Validade da Licença
- Perfil Associado
- Detalhes do Perfil
- Configurações do Alarme

Segurança - Segurança

Centro de informações > Emissão de relatórios > Relatórios > Segurança > Ameaças atuais

- É exibido apenas se o módulo de complemento do SEgurança estiver instalado.
- Informações similares são fornecidas em > Status da segurança *(página 5)*, Visualizar logs *(página 14)* e Visualizar ameaças *(página 12)*.

A definição do relatório **Segurança - Ameaças atuais** gera relatórios para os seguintes tipos de dados de segurança mantidos pelo VSA.

- Resumo
- Sumário de Categorias de Ameaças
- Ameaças atuais

Seleção de tempo

- **Selecionar o tipo de intervalo de tempo** - Filtra por um tipo definido de intervalo de tempo.
- **Número de dias**: se aplica somente se `Last N Days` for selecionado no tipo de intervalo de tempo.
- **Personalizar data e hora iniciais**: se aplica somente se `Fixed Range` for selecionado no tipo de intervalo de tempo.
- **Personalizar data e hora finais**: se aplica somente se `Fixed Range` for selecionado no tipo de intervalo de tempo.

Segurança - Ameças históricas

Centro de informações > Emissão de relatórios > Relatórios > Segurança > Ameaças históricas

- É exibido apenas se o módulo de complemento do SEgurança estiver instalado.
- Informações similares são fornecidas em > Status da segurança *(página 5)*, Visualizar logs *(página 14)* e Visualizar ameaças *(página 12)*.

A definição do relatório **Segurança - Ameaças históricas** gera relatórios para os seguintes tipos de dados de segurança mantidos pelo VSA.

- Resumo
- Sumário de Categorias de Ameaças
- Ameaças atuais

Seleção de tempo

- **Selecionar o tipo de intervalo de tempo** - Filtra por um tipo definido de intervalo de tempo.
- **Número de dias**: se aplica somente se `Last N Days` for selecionado no tipo de intervalo de tempo.
- **Personalizar data e hora iniciais**: se aplica somente se `Fixed Range` for selecionado no tipo de intervalo de tempo.
- **Personalizar data e hora finais**: se aplica somente se `Fixed Range` for selecionado no tipo de intervalo de tempo.

Segurança - Log KES

Centro de informações > Emissão de relatórios > Relatórios > Segurança - log KES

- É exibido apenas se o módulo de complemento do SEgurança estiver instalado.
- Agente > Logs do agente exibe as entradas de logs por tipo de log e ID de máquina.

A definição de relatório do Log KES gera um relatório das entradas de logs do Endpoint Security por ID de máquina.

Configure o relatório usando estes parâmetros:

- **Número de dias a serem consultados no registro*** - Número de dias anteriores à data/hora a serem incluídos no relatório.
- **Exibir entradas correspondentes à esta descrição (use * para caracteres curinga)** - Insira uma sequência para filtrar entradas pela descrição. Inclua o curinga asterisco (*) com o texto inserido para corresponder a vários registros.
- **Ignorar as máquinas sem dados -** Marque essa caixa para exibir somente as IDs de máquinas que tenham dados que correspondam aos outros parâmetros do filtro.

Índice