ESET MAIL SECURITY

PARA MICROSOFT EXCHANGE SERVER

Manual de instalação e Guia do usuário

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Clique aqui para fazer download da versão mais recente deste documento

ESET **MAIL SECURITY**

O ESET Mail Security foi desenvolvido por ESET, spol. s r.o.

Para obter mais informações, visite www.eset.com.br.

A ESET, spol. s r.o. reserva-se o direito de alterar qualquer software aplicativo descrito sem prévio aviso.

Atendimento ao cliente: www.eset.com/support

REV. 5/2/2014

Índice

1. Introdução

O ESET Mail Security 4 para Microsoft Exchange Server é uma solução integrada que protege as caixas de correio contra vários tipos de conteúdo de malware, incluindo anexos de email infectados por worms ou cavalos de troia, documentos que contêm scripts prejudiciais, roubo de identidade e spam. O ESET Mail Security fornece três tipos de proteção: Antivírus, antispam e a aplicação de regras definidas pelo usuário. O ESET Mail Security filtra o conteúdo malicioso no nível do servidor de email, antes que ele chegue à caixa de entrada do cliente de email do destinatário.

O ESET Mail Security suporta o Microsoft Exchange Server versões 2000 e posteriores, bem como o Microsoft Exchange Server em um ambiente de agrupamento. Nas versões mais recentes (Microsoft Exchange Server 2007 e posteriores), também há suporte a funções específicas (caixa de correio, hub, edge). É possível gerenciar remotamente o ESET Mail Security em grandes redes com a ajuda do ESET Remote Administrator.

Enquanto fornece proteção ao Microsoft Exchange Server, o ESET Mail Security também tem ferramentas para assegurar a proteção do próprio servidor (proteção residente, proteção do acesso à Web, proteção do cliente de email e antispam).

1.1 O que há de novo na versão 4.5?

Em comparação com o ESET Mail Security versão 4.3, as novidades e aprimoramentos a seguir foram introduzidos na versão 4.5:

- Configurações antispam - facilmente acessíveis a partir do GUI para tornar as alterações muito mais conveniente para os administradores
- Suporte para o Microsoft Exchange Server 2013
- Suporte para o Microsoft Windows Server 2012 / 2012 R2

1.2 Requisitos do sistema

Sistemas operacionais compatíveis:

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 e x64)
- Microsoft Windows Server 2008 (x86 e x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Versões compatíveis do Microsoft Exchange Server:

- Microsoft Exchange Server 2000 SP1, SP2, SP3
- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013

Os requisitos de hardware dependem da versão do sistema operacional e da versão do Microsoft Exchange Server em uso. Recomendamos ler a documentação do Microsoft Exchange Server para obter informações mais detalhadas sobre os requisitos de hardware.

1.3 Métodos usados

Dois métodos independentes são usados para rastrear mensagens de email:

Rastreamento da caixa de correio via VSAPI 6
Filtragem de mensagens no nível do servidor SMTP 6

1.3.1 Rastreamento da caixa de correio via VSAPI

O processo de rastreamento das caixas de correio será disparado e controlado pelo Microsoft Exchange Server. Os emails no banco de dados de armazenamento do Microsoft Exchange Server serão rastreados continuamente. Dependendo da versão do Microsoft Exchange Server, da versão da interface VSAPI e das configurações definidas pelo usuário, o processo de rastreamento pode ser disparado em qualquer uma das seguintes situações:

- Quando o usuário acessa o email, por exemplo, em um cliente de email (o email é sempre rastreado com o banco de dados de assinatura de vírus mais recente)
- Em segundo plano, quando a utilização do Microsoft Exchange Server for menor
- Proativamente (com base no algoritmo interno do Microsoft Exchange Server)

A interface VSAPI atualmente é usada para rastreamento antivírus e proteção baseada em regras.

1.3.2 Filtragem de mensagens no nível do servidor SMTP

A filtragem no nível do servidor SMTP é assegurada por um plugin especializado. No Microsoft Exchange Server 2000 e 2003, o plugin em questão (*Event Sink*) é registrado no servidor SMTP como parte do Internet Information Services (IIS). No Microsoft Exchange Server 2007/2010, o plugin está registrado como um agente de transporte nas funções *Edge* ou *Hub* do Microsoft Exchange Server.

A filtragem no nível do servidor SMTP por um agente de transporte fornece proteção sob a forma de antivírus, antispam e regras definidas pelo usuário. Ao contrário da filtragem de VSAPI, a filtragem no nível do servidor SMTP é executada antes que o email rastreado chegue à caixa de correio do Microsoft Exchange Server.

1.4 Tipos de proteção

Há três tipos de proteção:

1.4.1 Proteção antivírus

A proteção antivírus é uma das funções básicas do produto ESET Mail Security. A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, e-mails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena 94.

1.4.2 Proteção antispam

A proteção antispam integra várias tecnologias (RBL, DNSBL, Impressão digital, Verificação de reputação, Análise de conteúdo, Filtragem Bayesian, Regras, Listas manuais de permissões/proibições, etc.) para atingir detecção máxima de ameaças por email. O resultado do mecanismo de rastreamento antispam é o valor da probabilidade de determinada mensagem de email ser spam, expresso como percentual (0 a 100).

Outro componente do módulo de proteção antispam é a técnica de Lista cinza (desativada por padrão). A técnica baseia-se na especificação RFC 821, que determina que, como o SMTP é considerado um meio de transporte não confiável, todo MTA (Message Transfer Agent, Agente de Transferência de Mensagens) deve tentar repetidamente entregar um email após encontrar uma falha temporária na entrega. Uma parte substancial dos spams consiste em entregas únicas (por meio de ferramentas especializadas) a uma lista em bloco de endereços de email gerada automaticamente. Um servidor que utiliza a Lista cinza calcula um valor de controle (hash) para o endereço do remetente do envelope, o endereço do destinatário do envelope e o endereço IP do MTA remetente. Se o servidor não puder encontrar o valor de controle do trio em seu banco de dados, ele se recusará a aceitar a mensagem, retornando um código de falha temporária (por exemplo, 451). Um servidor legítimo tentará entregar novamente a mensagem após um período variável. O valor de controle do trio será armazenado no banco de dados de conexões verificadas na segunda tentativa, permitindo que todos os emails com características relevantes sejam entregues

desse momento em diante.

1.4.3 Aplicação de regras definidas pelo usuário

A proteção baseada em regras definidas pelo usuário está disponível para rastreamento com a VSAPI e o agente de transporte. É possível usar a interface de usuário ESET Mail Security para criar regras individuais que também podem ser combinadas. Se uma regra usar várias condições, as condições serão vinculadas usando o operador lógico E. Consequentemente, a regra será executada somente se todas as suas condições forem atendidas. Se várias regras forem criadas, o operador lógico OU será aplicado, o que significa que o programa executará a primeira regra para a qual as condições forem atendidas.

Na sequência de rastreamento, a primeira técnica usada é a lista cinza – se estiver ativada. Os procedimentos consequentes sempre executarão as seguintes técnicas: proteção com base em regras definidas pelo usuário, seguida de um rastreamento antivírus e, por último, um rastreamento antispam.

1.5 Interface do usuário

O ESET Mail Security tem uma interface gráfica de usuário (GUI) projetada para ser o mais intuitiva possível. A GUI permite que os usuários acessem rápida e facilmente as principais funções do programa.

Além da GUI principal, há uma **árvore de configuração avançada** acessível em qualquer local do programa, pressionando a tecla F5.

Ao pressionar F5, a janela da árvore de configuração avançada se abre e exibe uma lista dos recursos do programa que podem ser configurados. Nessa janela, você pode configurar os ajustes e opções com base em suas necessidades. A estrutura em árvore divide-se em duas seções: **Proteção do servidor** e **Proteção do computador**. A seção **Proteção do servidor** contém itens relativos às configurações do ESET Mail Security, específicas para a proteção do servidor Microsoft Exchange. A seção **Proteção do computador** contém os itens configuráveis para a proteção do computador.

2. Instalação

Após comprar o ESET Mail Security, o instalador pode ser transferido do site da ESET (www.eset.com) em um pacote .msi.

Observe que você precisa executar o instalador na conta **Administrador incorporado**. Qualquer outro usuário, apesar de ser membro do grupo de administradores, não terá direitos de acesso suficientes. Portanto, é necessário usar a conta de administrador incorporado, pois você não poderá concluir a instalação com êxito em qualquer outra conta de usuário que não seja **Administrador**.

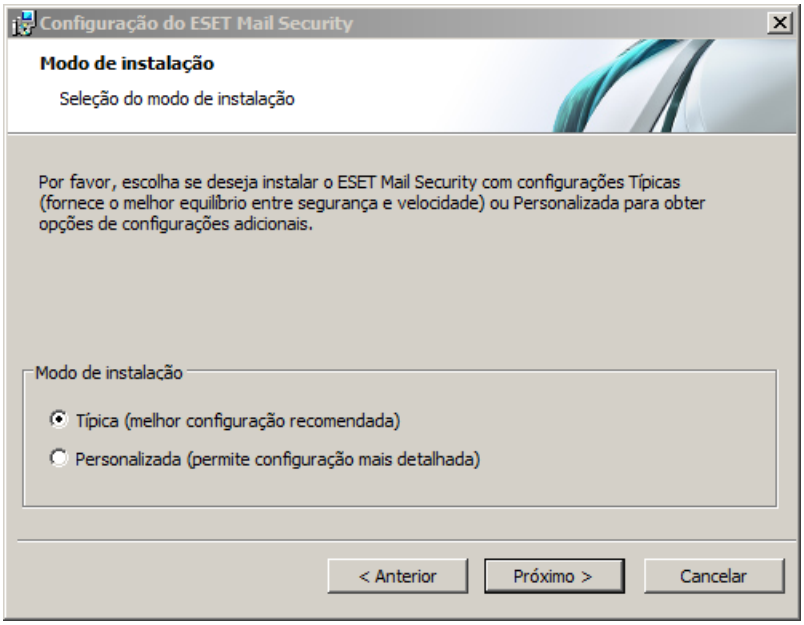
Há duas maneiras de executar o instalador:

- Você pode fazer login localmente usando as credenciais de conta do Administrador e simplesmente ao executar o instalador
- Você pode se conectar como outro usuário, mas precisa abrir o aviso de comando com **Executar como...** e digitar as credenciais de conta de Administrador para ter o cmd executando como Administrador e então digitar o comando para executar o instalador (p. ex., `msiexec /i emsx_nt64_ENU.msi` mas você precisa substituir `emsx_nt64_ENU.msi` pelo nome de arquivo exato do instalador msi que você baixou)

Após o início do instalador, o assistente de instalação o guiará pela configuração básica. Há dois tipos de instalação disponíveis com diferentes níveis de detalhes de configuração:

1. **Instalação típica**

2. **Instalação personalizada**



OBSERVAÇÃO: Recomendamos que instale o ESET Mail Security em um SO instalado e configurado recentemente, se possível. No entanto, se precisar instalá-lo em um sistema existente, o melhor a fazer é desinstalar a versão anterior do ESET Mail Security, reiniciar o servidor e instalar o novo ESET Mail Security em seguida.

2.1 Instalação típica

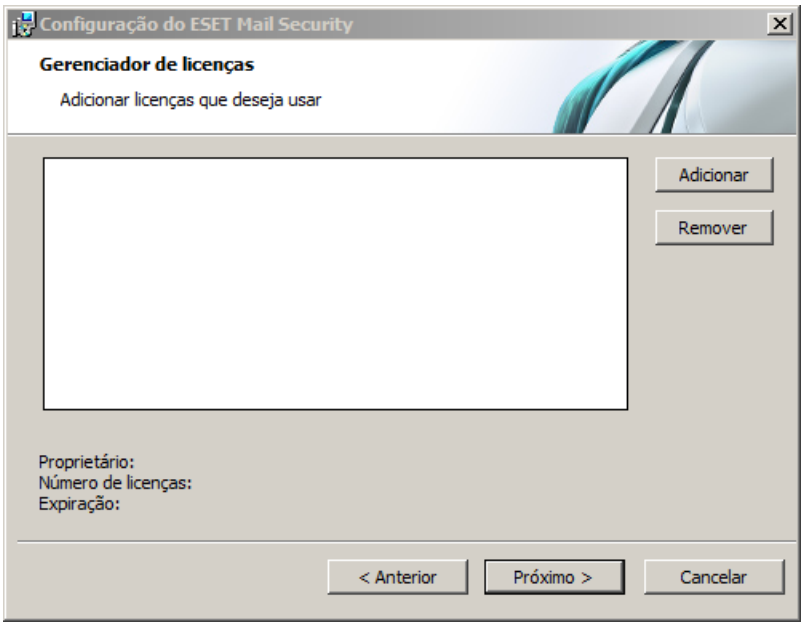
O modo de instalação Típica instala rapidamente o ESET Mail Security com a configuração mínima durante o processo de instalação. A instalação típica é o modo de instalação padrão e é recomendada se você ainda não tiver requisitos particulares para configurações específicas. Após a instalação do ESET Mail Security no sistema, é possível modificar as opções e configurações a qualquer momento. Este guia do usuário descreve essas configurações e recursos em detalhes. As configurações do modo de instalação Típica proporcionam excelente segurança, facilidade de uso e alto desempenho do sistema.

Após selecionar o modo de instalação e clicar em Avançar, você será solicitado a inserir o nome de usuário e a senha. Essa etapa tem um papel significativo no fornecimento de proteção constante ao seu sistema, pois o nome de usuário e a senha permitem as Atualizações 82 automáticas do banco de dados de assinatura de vírus.

Insira o nome de usuário e a senha recebidos após a compra ou registro do produto, nos campos correspondentes.

Caso você não tenha o nome de usuário e a senha disponíveis no momento, eles poderão ser inseridos diretamente no programa posteriormente.

Na próxima etapa - **Gerenciador de licenças** - Adicione o arquivo de licença que foi enviado por email após a compra do produto.



A próxima etapa é configurar o ThreatSense.Net Early Warning System. O ThreatSense.Net Early Warning System ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar ThreatSense.Net Early Warning System** é selecionada. Clique em **Configuração avançada...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos.

A próxima etapa do processo de instalação é a configuração da **Detecção de aplicativos potencialmente não desejados**. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Para obter mais detalhes, consulte o capítulo Aplicativos potencialmente não desejados 136.

Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET Mail Security detecte esse tipo de aplicativos. Se não desejar ativar esse recurso, selecione **Desativar detecção de aplicativos potencialmente não desejados**.

A última etapa no modo de instalação Típica é confirmar a instalação clicando no botão **Instalar**.

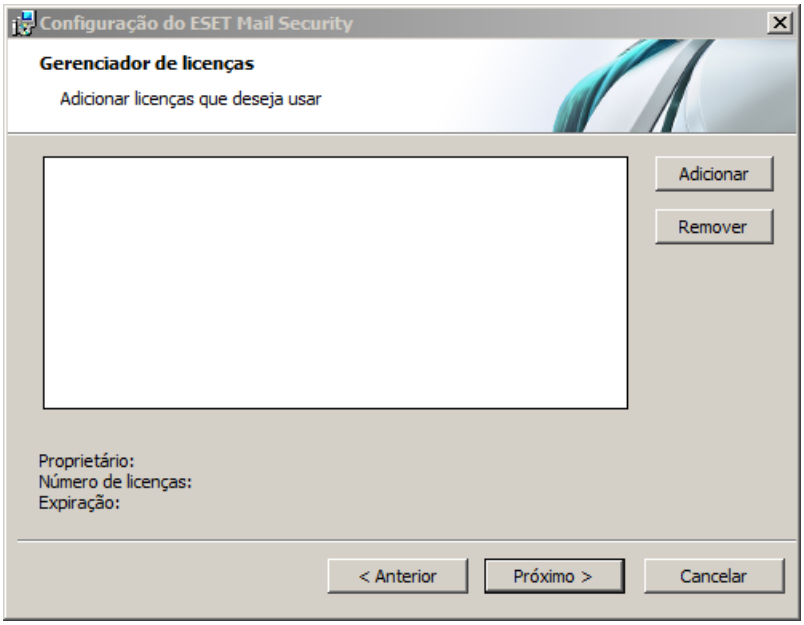
2.2 Instalação personalizada

A instalação personalizada foi desenvolvida para os usuários que desejam configurar o ESET Mail Security durante o processo de instalação.

Após selecionar o modo de instalação e clicar em **Avançar**, será exibida a solicitação para que você selecione um local de destino para a instalação. Por padrão, o programa é instalado em *C:\Program Files\ESET\ESET Mail Security*. Clique em **Procurar...** para alterar este local (não recomendado).

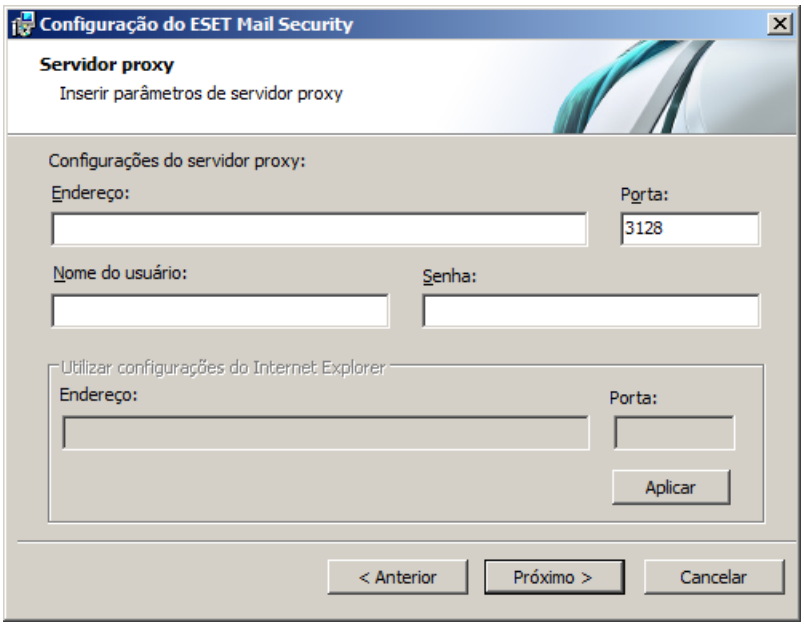
Em seguida, insira o **Nome de usuário** e **Senha**. Esta etapa é a mesma que no modo de instalação típica (consulte "Instalação típica" 8).

Na próxima etapa - **Gerenciador de licenças** – adicione o arquivo de licença que foi enviado por email após a compra do produto.



Após a inserção do nome de usuário e da senha, clique em **Avançar** para passar para **Configurar sua conexão com a Internet**.

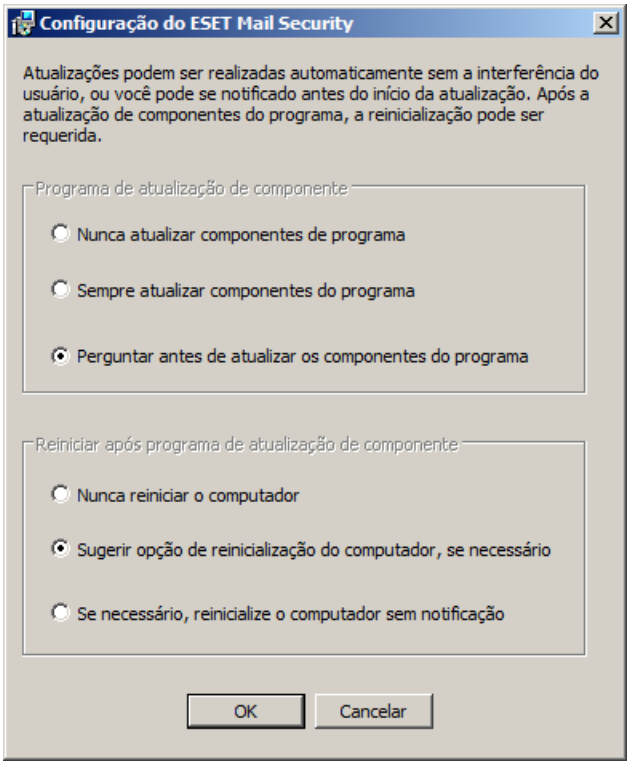
Se estiver usando um servidor proxy, ele deve estar configurado corretamente para que as atualizações do banco de dados de assinatura de vírus funcionem corretamente. Se desejar que o servidor proxy seja configurado automaticamente, selecione a configuração padrão **Não tenho certeza se minha conexão com a Internet utiliza um servidor proxy. Use as mesmas configurações usadas pelo Internet Explorer (Recomendável)** e clique em **Avançar**. Se não estiver usando um servidor proxy, selecione a opção **Eu não utilizo um servidor proxy**.



Se preferir digitar os detalhes do servidor proxy, poderá configurá-lo manualmente. Para configurar os ajustes do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **Nome de usuário** e uma **Senha** válidos a fim de obter acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Após inserir os detalhes do servidor proxy, clique em **Aplicar** e confirme a seleção.

Clique em **Avançar** para prosseguir para **Configurar definições de atualização automática**. Esta etapa permite definir se deseja que as atualizações de componentes sejam ou não automáticas no seu sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione a opção **Nunca atualizar componentes de programa**. Selecione a opção **Perguntar antes de fazer download dos componentes do programa** para exibir uma janela de confirmação antes de fazer download dos componentes de programa. Para fazer o download dos componentes do programa automaticamente, selecione a opção **Sempre atualizar componentes do programa**.



OBSERVAÇÃO: Após a atualização de um componente do programa, geralmente é necessário reiniciar o computador. Recomendamos selecionar a opção **Nunca reiniciar o computador**. As atualizações de componentes mais recentes entrarão em vigor após a próxima reinicialização do servidor agendada 92, manual ou outra). Você pode escolher **Sugerir opção de reinicialização do computador, se necessário** caso queira ser lembrado de reiniciar o servidor após a atualização dos componentes. Com esta configuração, você pode reiniciar o servidor na hora ou adiar a reinicialização e fazer isto posteriormente.

A próxima janela de instalação oferece a opção de definir uma senha para proteger as configurações do programa. Selecione a opção **Proteger as configurações por senha** e digite a senha nos campos **Nova senha** e **Confirmar nova senha**.

As próximas duas etapas da instalação, **ThreatSense.Net Early Warning System** e **Detecção de aplicativos potencialmente não desejados** são as mesmas etapas no modo de instalação Típica (consulte "Instalação típica" 8).

Clique em **Instalar** na janela **Pronto para instalar** para concluir a instalação.

2.3 Servidor de terminal

Se o ESET Mail Security estiver instalado em Windows Server que atue como Servidor de terminal, você pode desejar desativar a GUI do ESET Mail Security para evitar que ela inicie todas as vezes em que um usuário fizer login. Consulte o capítulo Desativar a GUI no servidor de terminal 121 para conhecer as etapas específicas para desativá-la.

2.4 Atualização para uma versão mais recente

As novas versões do ESET Mail Security foram lançadas para proporcionar melhorias ou consertar problemas que não podiam ser resolvidos por atualizações automáticas do módulo do programa. Você pode atualizar para a versão mais recente do ESET Mail Security usando os seguintes métodos:

1. Atualizar automaticamente por meio de uma atualização dos componentes do programa (PCU)
   Já que as atualizações dos componentes do programa são distribuídas a todos os usuários e podem ter um impacto em determinadas configurações do sistema, geralmente são lançadas após um longo período de testes, a fim de garantir um processo de atualização tranquilo em todas as configurações de sistema possíveis.
2. Manualmente, por exemplo, no caso de você precisar atualizar para uma versão mais recente imediatamente depois que for lançada ou se quiser atualizar para a próxima geração do ESET Mail Security (p. ex., da versão 4.2 ou 4.3 para a versão 4.5).

É possível executar uma atualização manual para a versão mais recente de duas maneiras, no local (a versão mais recente é instalada acima da versão existente) ou usando uma instalação limpa (a versão anterior é desinstalada primeiro e em seguida a versão mais recente é instalada).

Para realizar uma atualização manual:

1. Atualização no local: Instale a última versão sobre a versão existente do ESET Mail Security seguindo os passos no capítulo Instalação 8. Todas as configurações existentes (incluindo configurações de antispam) serão automaticamente importadas para a versão mais recente durante a instalação.

2. Instalação limpa:

a) Exporte sua configuração/configurações para um arquivo xml usando o recurso Importar e exportar configurações 128.

b) Abra este arquivo xml em um editor XML dedicado ou em um editor de texto que suporte XML (por exemplo, WordPad, Nodepad++, etc.) e então altere o número da terceira linha número ID DA SEÇÃO "1000404" para que ele fique parecido com isso:

```
<SECTION ID="1000404">
```

c) Faça download da ferramenta EMSX AntispamSettingsExport deste artigo da Base de Conhecimento. Salve `EMSX_AntispamSettingsExport.exe` para o Exchange Server que você está atualizando para a versão mais recente do ESET Mail Security.

d) Execute o `EMSX_AntispamSettingsExport.exe` . A ferramenta vai criar um `cfg.xml` arquivo contendo as configurações de antispam de sua instalação existente do ESET Mail Security.

e) Faça download do instalador msi para a versão mais recente do ESET Mail Security.

f) Copie o `cfg.xml` arquivo criado pela ferramenta EMSX AntispamSettingsExport para o mesmo local onde você salvou o arquivo instalador msi do ESET Mail Security (por exemplo `emsx_nt64_ENU.msi`).

g) Desinstale a versão existente do ESET Mail Security.

h) Execute o instalador msi para o ESET Mail Security 4.5. Configurações de antispam exportadas `cfg.xml` serão automaticamente importadas para a nova versão.

i) Quando a instalação estiver concluída, importe a configuração do arquivo xml que você salvou e alterou nas etapas a) e b) usando o recurso Importar e Exportar Configurações 128 e um editor xml para que você pode usar suas configurações anteriores na nova versão do ESET Mail Security.

Depois de realizar as etapas acima, você terá a nova versão do ESET Mail Security instalada em seu sistema com sua configuração personalizada anterior.

Para mais detalhes sobre o processo de atualização, consulte este artigo na Base de Conhecimento.

OBSERVAÇÃO: Ambos os processos de atualização manual (no local e instalação limpa) aplicam-se apenas para a atualização do ESET Mail Security versão 4.2 ou 4.3 para o ESET Mail Security versão 4.5.

2.5 Funções do Exchange Server - Edge versus Hub

Por padrão, um servidor de Transporte de Edge tem seus recursos antispam ativados e um servidor de Transporte de Hub tem seus recursos antispam desativados. Em uma organização com Exchange com o servidor de Transporte de Edge, essa é a configuração desejada. Recomenda-se ter o servidor de Transporte de Edge executando o antispam do ESET Mail Security configurado para filtrar mensagens antes de elas serem roteadas para a organização com Exchange.

A função de Edge é o local preferido para rastreamento antispam, pois permite que o ESET Mail Security rejeite spam no início do processo, sem exercer uma carga desnecessária nas camadas da rede. Ao usar esta configuração, as mensagens de entrada são filtradas pelo ESET Mail Security no servidor de Transporte Edge, para que possam ser movidas com segurança para o servidor de Transporte Hub sem a necessidade de filtragem adicional.

Se sua organização não usa o servidor de Transporte de Edge e tem somente o servidor de Transporte de Hub, recomendamos a ativação dos recursos antispam no servidor de Transporte de Hub que recebem mensagens de entrada da Internet via SMTP.

2.6 Funções do Exchange Server 2013

A arquitetura do Exchange Server 2013 é diferente das versões anteriores do Microsoft Exchange. No Exchange 2013 existem apenas duas funções de servidor, servidor Client Access e servidor Mailbox. Se você estiver planejando proteger o Microsoft Exchange 2013 com o ESET Mail Security, certifique-se de instalar o ESET Mail Security em um sistema executando o Microsoft Exchange 2013 com a função do servidor Mailbox. A função do servidor Client Access não é compatível com o ESET Mail Security.

Existe uma exceção se você estiver planejando instalar o ESET Mail Security no Windows SBS (Small Business Server). No caso do Windows SBS todas as funções do Exchange estão sendo executadas no mesmo servidor, portanto o ESET Mail Security estará em operação sem problemas e fornecerá todos os tipos de proteção, inclusive proteção a servidores de email.

Porém, se você instalar o ESET Mail Security em um sistema que esteja executando apenas a função de servidor Client Access (servidor CAS dedicado), os recursos mais importantes do ESET Mail Security não vão funcionar, especialmente os recursos de servidor de email. Neste caso, apenas a proteção em tempo real do sistema de arquivos vai funcionar, e alguns componentes da Proteção do computador 60, portanto não haverá proteção no servidor de email. É por isso que não recomendamos instalar o ESET Mail Security em um servidor com a função de servidor Client Access. Isto não se aplica ao Windows SBS (Small Business Server), como mencionado anteriormente.

OBSERVAÇÃO: Devido a determinadas restrições técnicas do Microsoft Exchange 2013, o ESET Mail Security não é compatível com a função do servidor Client Access (CAS).

2.7 Instalação em um ambiente de agrupamento

Agrupamento é um grupo de servidores (um servidor conectado a um agrupamento é denominado "nó") que trabalham juntos como um único servidor. Esse tipo de ambiente proporciona alta acessibilidade e confiabilidade dos serviços disponíveis. Se um dos nós do agrupamento falhar ou se tornar inacessível, seu funcionamento será automaticamente amparado por outro nó no agrupamento. O ESET Mail Security é totalmente compatível com os Microsoft Exchange Servers conectados em um agrupamento. Para que o ESET Mail Security funcione corretamente, é importante que cada nó em um agrupamento tenha a mesma configuração. Isso pode ser obtido pela aplicação de uma política que utilize o ESET Remote Administrator (ERA). Nos próximos capítulos descreveremos como instalar e configurar o ESET Mail Security em servidores em um ambiente de agrupamento usando o ERA.

Instalação

Este capítulo explica o método de instalação forçada; no entanto, essa não é a única forma de instalar um produto no computador de destino. Para obter informações sobre os métodos de instalação adicionais, consulte o Guia do usuário do ESET Remote Administrator.

1) Faça o download do pacote de instalação *msi* do ESET Mail Security no site da ESET para o computador em que o ERA está instalado. Na guia ERA > **Instalação remota (Remote Install)** > **Computadores (Computers)**, clique com o botão direito em um computador na lista e selecione **Gerenciar pacotes (Manage Packages)** no menu de contexto. No menu suspenso **Tipo (Type)**, selecione **Pacote de produtos de segurança ESET (ESET Security Products package)** e clique em **Adicionar... (Add...)** Em **Origem (Source)**, localize o pacote de instalação do ESET Mail Security obtido por download e clique em **Criar (Create)**.

2) Em **Editar/Selecionar configuração associada a esse pacote (Edit/Select configuration associated with this package)**, clique em**Editar (Edit)** e defina as configurações do **ESET Mail Security** de acordo com suas necessidades. As configurações do ESET Mail Security estão nas seguintes ramificações: **ESET Smart Security, ESET NOD32 Antivirus > Proteção do servidor de email (Mail server protection)** e **Proteção do servidor de email para Microsoft Exchange Server (Mail server protection for Microsoft Exchange Server)**. Também é possível definir os parâmetros de outros módulos incluídos no ESET Mail Security (por exemplo, o Módulo de atualização, Rastreamento do computador, etc.). Recomendamos exportar as configurações para um arquivo xml que pode ser usado posteriormente, por exemplo, ao criar um pacote de instalação, ao aplicar uma Tarefa de configuração ou uma Política.

3) Clique em **Fechar (Close)**. Na próxima janela de diálogo (**Deseja salvar o pacote no servidor? (Do you want to save the package into server?)**), selecione **Sim (Yes)** e digite o nome do pacote de instalação. O pacote de instalação concluído (incluindo o nome e configuração) serão salvos no servidor. Com mais frequência, esse pacote

será usado em uma Instalação forçada, mas também é possível salvá-lo como um pacote de instalação *msi* padrão e usá-lo para uma instalação direta no servidor (em **Editor de pacotes de instalação (Installation Packages Editor)** >**Salvar como... (Save As...)**).

4) Agora que o pacote de instalação está pronto, você pode iniciar a instalação remota nos nós em um agrupamento. Na guia ERA > **Instalação remota (Remote Install)** > **Computadores (Computers)**, selecione os nós nos quais deseja instalar o ESET Mail Security (Ctrl + clique com o botão esquerdo ou Shift + clique com o botão esquerdo). Clique com o botão direito em um dos computadores selecionados e selecione **Instalação forçada (Push Installation)** no menu de contexto. Usando os botões **Definir (Set)** / **Definir todos (Set All)**, defina o **Usuário (Username)** e a **Senha (Password)** de um usuário no computador de destino (este deve ser um usuário com direitos de administrador). Clique em **Avançar (Next)** para escolher o pacote de instalação e iniciar o processo de instalação remota clicando em **Concluir (Finish)**. O pacote de instalação contendo o ESET Mail Security e as configurações personalizadas será instalado nos computadores/nós de destino selecionados. Após um breve período, os clientes com o ESET Mail Security serão exibidos na guia ERA > **Clientes (Clients)**. Agora é possível gerenciar os clientes remotamente.

OBSERVAÇÃO: Para que o processo de instalação remota seja perfeito, é necessário atender a determinadas condições nos computadores de destino, bem como no servidor ERA. Para obter mais detalhes, consulte o Guia do usuário do ESET Remote Administrator.

Configuração

Para que o ESET Mail Security funcione corretamente nos nós em um agrupamento, os nós devem ter a mesma configuração em todos os momentos. Essa condição estará atendida se você tiver seguido o método de instalação forçada acima. Entretanto, há uma chance de que a configuração seja alterada por engano, causando inconsistências entre os produtos do ESET Mail Security em um agrupamento. Isso pode ser evitado utilizando uma política no ERA. Uma política é muito semelhante a uma Tarefa de configuração padrão; ela envia a configuração definida no Editor de configuração para os clientes. Uma política é diferente de uma Tarefa de configuração, pois é continuamente aplicada aos clientes. Assim, a Política pode ser definida como uma configuração que é regularmente forçada a um cliente/grupo de clientes.

Em ERA > **Ferramentas (Tools)** > **Gerenciador de políticas... (Policy Manager...)**, há várias opções para uso de uma política. A opção mais simples é usar **Política Pai padrão (Default Parent Policy)**, que também geralmente serve como **Política padrão para clientes primários (Default policy for primary clients)**. Esse tipo de política é aplicado automaticamente a todos os clientes conectados no momento (nesse caso, a todos os produtos do ESET Mail Security em um agrupamento). É possível configurar a Política clicando em **Editar... (Edit...)** ou usar configurações existentes salvas no arquivo *xml*, se você já tiver criado um.

A segunda opção é criar uma nova política (**Adicionar nova política filho (Add New Child Policy)**) e usar a opção **Adicionar clientes... (Add Clients...)** para atribuir todos os produtos do ESET Mail Security a essa política.

Essa configuração assegura que uma única política com as mesmas configurações será aplicada a todos os clientes. Se desejar modificar as configurações existentes de um servidor do ESET Mail Security em um agrupamento, basta editar a política atual. As alterações serão aplicadas a todos os clientes aos quais essa política foi atribuída.

OBSERVAÇÃO: Consulte o Guia do usuário do ESET Remote Administrator para obter informações detalhadas sobre políticas.

2.8 Licenças

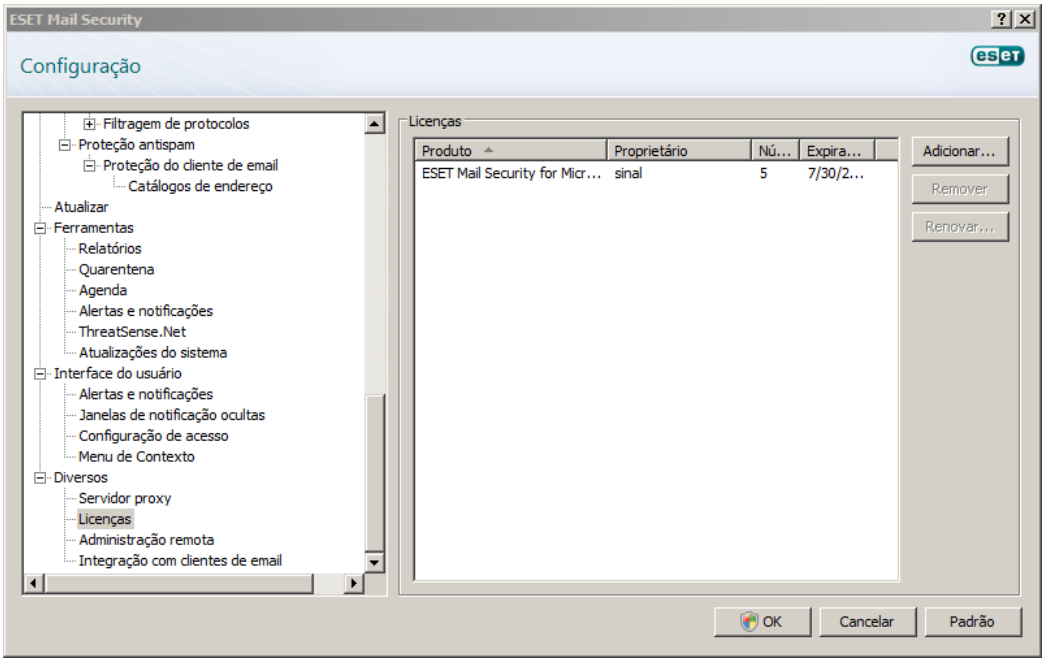
Uma etapa muito importante é inserir o arquivo de licença do ESET Mail Security para o Microsoft Exchange Server. Sem ele, a proteção de email no Microsoft Exchange Server não funcionará corretamente. Se você não adicionar o arquivo da licença durante a instalação, poderá fazê-lo posteriormente nas configurações avançadas **Diversos > Licenças**.

O ESET Mail Security permite usar várias licenças simultaneamente, mesclando-as, como descrito a seguir:

1) Duas ou mais licenças de um cliente (ou seja, licenças atribuídas ao mesmo nome de cliente) são mescladas e o número de caixas de correio rastreadas aumenta proporcionalmente. O gerenciador de licenças continuará a exibir ambas as licenças.

2) Duas ou mais licenças de clientes diferentes são mescladas. Isso ocorre exatamente da mesma maneira como no primeiro cenário (ponto 1 acima), com a única diferença de que pelo menos uma das licenças em questão deve ter um atributo especial. Esse atributo é requerido para mesclar licenças de clientes diferentes. Se estiver interessado em usar essa licença, peça ao seu distribuidor local para gerá-la para você.

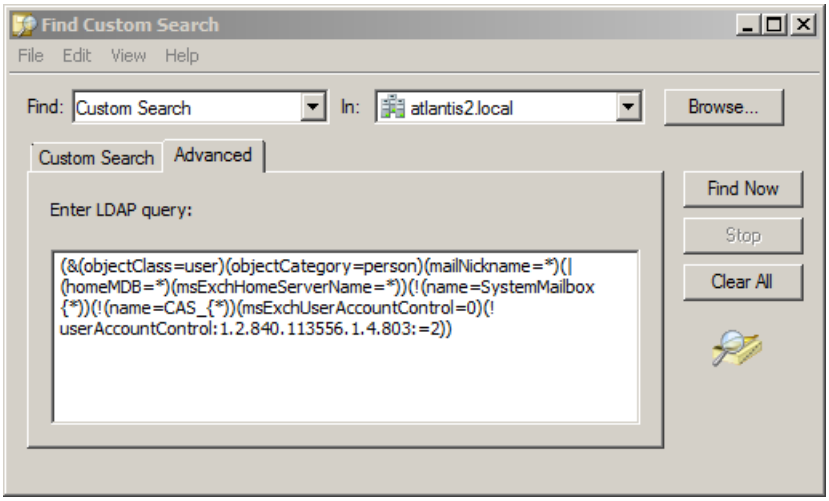
OBSERVAÇÃO: O período de validade da licença recém-criada será determinado pela primeira data de expiração entre as suas constituintes.



O ESET Mail Security para Microsoft Exchange Server (EMSX) compara o número de caixas de correio do diretório ativo com a sua contagem de licenças. Cada diretório ativo do Exchange Server é verificado para determinar a contagem total de caixas de correio. Caixas de correio do sistema, caixas de correio e aliases de email desativados não são calculados na contagem de caixas de correio. Em um ambiente de agrupamento, os nós com a função de caixa de correio em agrupamento não são calculados na contagem de caixas de correio.

Para determinar quantas caixas de correio ativadas do Exchange você tem, abra **Usuários e computadores do Active Directory** no servidor. Clique com o botão direito no domínio e clique em **Localizar...** No menu suspenso **Localizar**, selecione **Pesquisa personalizada** e clique na guia **Avançado**. Cole na consulta LDAP (Lightweight Directory Access Protocol) e clique em **Localizar agora**:

- `(&(objectClass=user)(objectCategory=person)(mailNickname=*)(|(homeMDB=*)(msExchHomeServerName=*))(!(name=SystemMailbox{*))(!(name=CAS_{*))(msExchUserAccountControl=0)(!userAccountControl:1.2.840.113556.1.4.803:=2))`



Se o número de caixas de correio em seu diretório ativo exceder a sua contagem de licenças, uma mensagem será inserida na leitura do relatório do Microsoft Exchange Server, "Status da proteção alterado devido ao número excedido de caixas de correio (contagem) cobertas pela licença (contagem)". O ESET Mail Security também o notificará alterando seu **Status da proteção** para laranja e exibindo uma mensagem informando que você tem 42 dias restantes até que a proteção seja desativada. Se você receber essa notificação, entre em contato com o seu representante de vendas para adquirir licenças adicionais.

Se o período de 42 dias expirar e você não tiver adicionado as licenças requeridas para abranger as caixas de correio excedentes, o **Status da proteção** será alterado para vermelho. A mensagem informará que a sua proteção foi desativada. Se você receber essa notificação, entre em contato imediatamente com o seu representante de vendas para adquirir licenças adicionais.

2.9 Configuração pós-instalação

Há várias opções que devem ser configuradas após a instalação do produto.

Configuração da proteção antispam

Esta seção descreve configurações, métodos e técnicas que podem ser usados para proteger sua rede contra spams. Recomendamos ler as seguintes instruções cuidadosamente antes de escolher a combinação mais adequada de configurações para a sua rede.

Gerenciamento de spam

Para assegurar alto nível de proteção antispam, é necessário definir ações a serem executadas nas mensagens já marcadas como SPAM.

Há três opções disponíveis:

1. **Exclusão de spam**
   Os critérios para que uma mensagem seja marcada como SPAM pelo ESET Mail Security são razoavelmente elevados, diminuindo as chances de exclusão de emails legítimos. Quanto mais específicas as configurações Antispam, menos provável a exclusão de emails legítimos. As vantagens desse método incluem o consumo muito baixo de recursos do sistema e menos administração. A desvantagem desse método é que se um email legítimo for excluído, ele não poderá ser restaurado localmente.

2. **Quarentena**
   Essa opção exclui o risco de exclusão de emails legítimos. As mensagens podem ser restauradas e reenviadas para os destinatários originais imediatamente. As desvantagens desse método são maior consumo de recursos do sistema e tempo adicional necessário para a manutenção da quarentena de email. É possível usar dois métodos para emails de quarentena:

   A. A quarentena interna do Exchange Server (aplica-se somente ao Microsoft Exchange Server 2007/2010):
   - Se você desejar usar a quarentena interna do sistema, certifique-se de que o campo **Quarentena comum de mensagens** no painel direito no menu de configurações avançadas (em **Proteção do servidor** > **Quarentena de mensagens**) esteja em branco. Certifique-se também de que a opção **Colocar mensagem em quarentena no sistema do servidor de email** esteja selecionada no menu suspenso na parte inferior. Esse método funciona apenas se a quarentena interna do Exchange existir. Por padrão, essa quarentena interna não está ativada no Exchange. Se desejar ativá-la, é necessário abrir o Exchange Management Shell e digitar o seguinte comando:

   Set-ContentFilterConfig -QuarantineMailbox name@domain.com

   (substitua name@domain.com pela caixa de correio real que você deseja que o Microsoft Exchange use como caixa de correio de quarentena interna, por exemplo, exchangequarantine@company.com)

   B. Caixa de correio de quarentena personalizada:
   - Se você digitar a caixa de correio desejada no campo **Quarentena comum de mensagens**, o ESET Mail Security moverá todas as mensagens de spam para a sua caixa de correio personalizada.

   Para obter mais detalhes sobre Quarentena e os diferentes métodos, consulte o capítulo Quarentena de mensagens 25.

3. **Encaminhamento de spam**

   O spam será encaminhado para o destinatário. Entretanto, o ESET Mail Security preencherá o cabeçalho MIME relevante com o valor SCL em cada mensagem. Com base no valor SCL, a ação relevante será executada pelo IMF (Filtro inteligente de mensagens) do Exchange Server.

Filtragem de spam

Lista cinza
A lista cinza é um método de proteger os usuários contra spam usando a seguinte técnica: O agente de transporte enviará o valor de retorno SMTP "*rejeitar temporariamente*" (o padrão é 451/4.7.1) para qualquer email de um remetente que ele não reconheça. Um servidor legítimo tentará reenviar a mensagem. Os remetentes de spam geralmente não tentam reenviar mensagens, porque passam por milhares de endereços de email por vez e normalmente não podem gastar mais tempo em reenvio.

Ao avaliar a origem da mensagem, o método leva em consideração as configurações da lista **Endereços IP aprovados**, da lista **Endereços IP ignorados**, das listas **Remetentes seguros** e **Permitir IP** no Exchange Server e as configurações de AntispamBypass da caixa de correio do destinatário. A lista cinza deve ser completamente configurada ou falhas operacionais não desejadas (por exemplo, atrasos na entrega de mensagens legítimas, etc.) podem ocorrer. Esses efeitos negativos diminuem continuamente, à medida que esse método preenche a lista interna de permissões com conexões confiáveis. Se você não estiver familiarizado com esse método ou se considerar seu efeito colateral negativo inaceitável, recomendamos desativar o método no menu Configurações avançadas em **Proteção antispam** > **Microsoft Exchange Server** > **Agente de transporte** > **Ativar lista cinza.**

Recomendamos desativar a lista cinza se você pretender testar os recursos básicos do produto e não desejar configurar os recursos avançados do programa.

OBSERVAÇÃO: A Lista cinza é uma camada adicional de proteção antispam e não tem efeito sobre as capacidades de avaliação de spam do módulo antispam.

Configuração da proteção antivírus

Quarentena
Dependendo do tipo do modo de limpeza que estiver utilizando, recomendamos que você configure uma ação a ser executada nas mensagens infectadas (não limpas). Essa opção pode ser definida na janela Configurações avançadas **Proteção do servidor** > **Antivírus e antispyware** > **Microsoft Exchange Server** > **Agente de transporte**.

Se a opção de mover mensagens para a quarentena de email estiver ativada, será necessário configurar a quarentena em **Proteção do servidor** > **Quarentena de mensagens** na janela Configurações avançadas.

Desempenho
Se não houver outras restrições, recomendamos aumentar o número de mecanismos de rastreamento ThreatSense na janela Configurações avançadas (F5) em **Proteção do computador** > **Antivírus e antispyware** > **Desempenho**, de acordo com esta fórmula: *número de mecanismos de rastreamento ThreatSense = (número de CPUs físicas x 2) + 1*. Além disso, o *número de encadeamentos de rastreamento* deve ser igual ao *número de mecanismos de rastreamento ThreatSense*. É possível configurar o número de mecanismos de encadeamentos em **Proteção do servidor** > **Antivírus e antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Desempenho**. Veja um exemplo:

Suponhamos que você tenha um servidor com 4 CPUs físicas. Para o melhor desempenho, de acordo com a fórmula anterior, você deve ter 9 encadeamentos de rastreamento e 9 mecanismos de rastreamento.

OBSERVAÇÃO: O valor aceitável é de 1 a 20; portanto, o número máximo de mecanismos de rastreamento do ThreatSense que você pode usar é 20. As alterações serão aplicadas somente após a reinicialização.

OBSERVAÇÃO: Recomendamos que você defina o número de encadeamentos de rastreamento igual ao número de mecanismos de rastreamento usados pelo ThreatSense. Isso não terá nenhum efeito sobre o desempenho se você usar mais encadeamentos de rastreamento que mecanismos de rastreamento.

OBSERVAÇÃO: Se estiver usando o ESET Mail Security em um Windows Server que atue como Servidor de terminal e não desejar que a GUI do ESET Mail Security inicie todas as vezes em que um usuário fizer login, consulte o capítulo Desativar a GUI no servidor de terminal 121 para conhecer as etapas específicas para desativá-la.

3. ESET Mail Security - Proteção do Microsoft Exchange Server

O ESET Mail Security fornece proteção significativa para o Microsoft Exchange Server. Há três tipos de proteção essenciais: Antivírus, antispam e a aplicação de regras definidas pelo usuário. O ESET Mail Security protege contra vários tipos de conteúdo de malware, incluindo anexos de email infectados por worms ou cavalos de troia, documentos que contêm scripts prejudiciais, roubo de identidade e spam. O ESET Mail Security filtra o conteúdo malicioso no nível do servidor de email, antes que ele chegue à caixa de entrada do cliente de email do destinatário. Os próximos capítulos descrevem todas as opções e configurações disponíveis para ajustar a proteção do Microsoft Exchange Server.

3.1 Configurações gerais

Esta seção descreve como administrar regras, relatórios, quarentena de mensagens e parâmetros de desempenho.

3.1.1 Microsoft Exchange Server

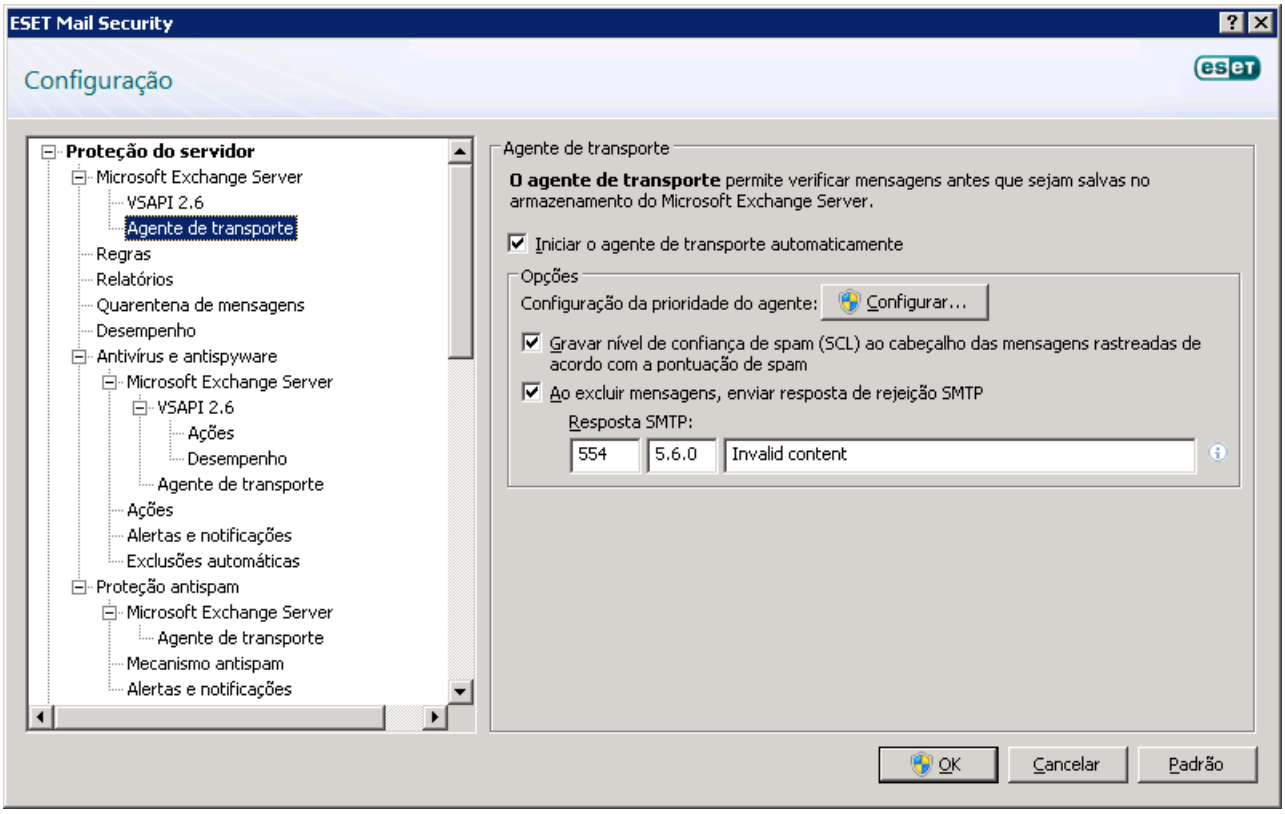
3.1.1.1 VSAPI (Virus-Scanning Application Programming Interface)

O Microsoft Exchange Server fornece um mecanismo para assegurar que cada componente da mensagem será rastreado em relação ao banco de dados de assinatura de vírus atual. Se o componente de uma mensagem não for rastreado, seus componentes correspondentes serão submetidos ao scanner antes que a mensagem seja liberada para o cliente. Toda versão compatível do Microsoft Exchange Server (2000/2003/2007/2010) fornece uma versão diferente da VSAPI.

Use a caixa de seleção para ativar/desativar a inicialização automática da versão da VSAPI usada pelo seu Exchange Server.

3.1.1.2 Agente de transporte

Nesta seção, você pode configurar o agente de transporte para iniciar automaticamente e definir a prioridade de carregamento do agente. No Microsoft Exchange Server 2007 e posteriores, só é possível instalar um agente de transporte se o servidor estiver em uma das duas funções: *Transporte de Edge* ou *Transporte de Hub*.



OBSERVAÇÃO: O agente de transporte não está disponível no Microsoft Exchange Server 5.5 (VSAPI 1.0).

No menu **Configuração da prioridade do agente**, é possível definir a prioridade dos agentes do ESET Mail Security.

O intervalo do número da prioridade do agente depende da versão do Microsoft Exchange Server (quanto menor o número, maior a prioridade).

Gravar nível de confiança de spam (SCL) ao cabeçalho das mensagens rastreadas de acordo com a pontuação de spam - O SCL é um valor padronizado atribuído a uma mensagem que indica a probabilidade de que a mensagem seja spam (com base nas características do cabeçalho da mensagem, seu assunto, conteúdo, etc.). A classificação de 0 indica que a mensagem tem alta probabilidade de ser spam, enquanto a classificação de 9 indica que a mensagem é muito provavelmente spam. Os valores de SCL podem ser mais processados pelo Filtro inteligente de mensagens do Microsoft Exchange Server (ou Agente de filtro de conteúdo). Para obter informações adicionais, consulte a documentação do Microsoft Exchange Server.

Opção **Ao excluir mensagens, enviar resposta de rejeição SMTP**:

- Se a opção estiver desmarcada, o servidor enviará a resposta SMTP OK para o MTA (Message Transfer Agent, Agente de Transferência de Mensagens) do remetente no formato '250 2.5.0 – Ação solicitada de email correta, concluída') e depois executará a remoção silenciosa.
- Se a opção estiver marcada, uma resposta de rejeição SMTP será enviada de volta ao MTA do remetente. Você pode digitar uma mensagem de resposta no seguinte formato:

Código de resposta primária	Código de status complementar	Descrição
250	2.5.0	Ação solicitada de email correta, concluída
451	4.5.1	Ação solicitada anulada: erro local no processamento
550	5.5.0	Ação solicitada não executada: caixa de correio indisponível

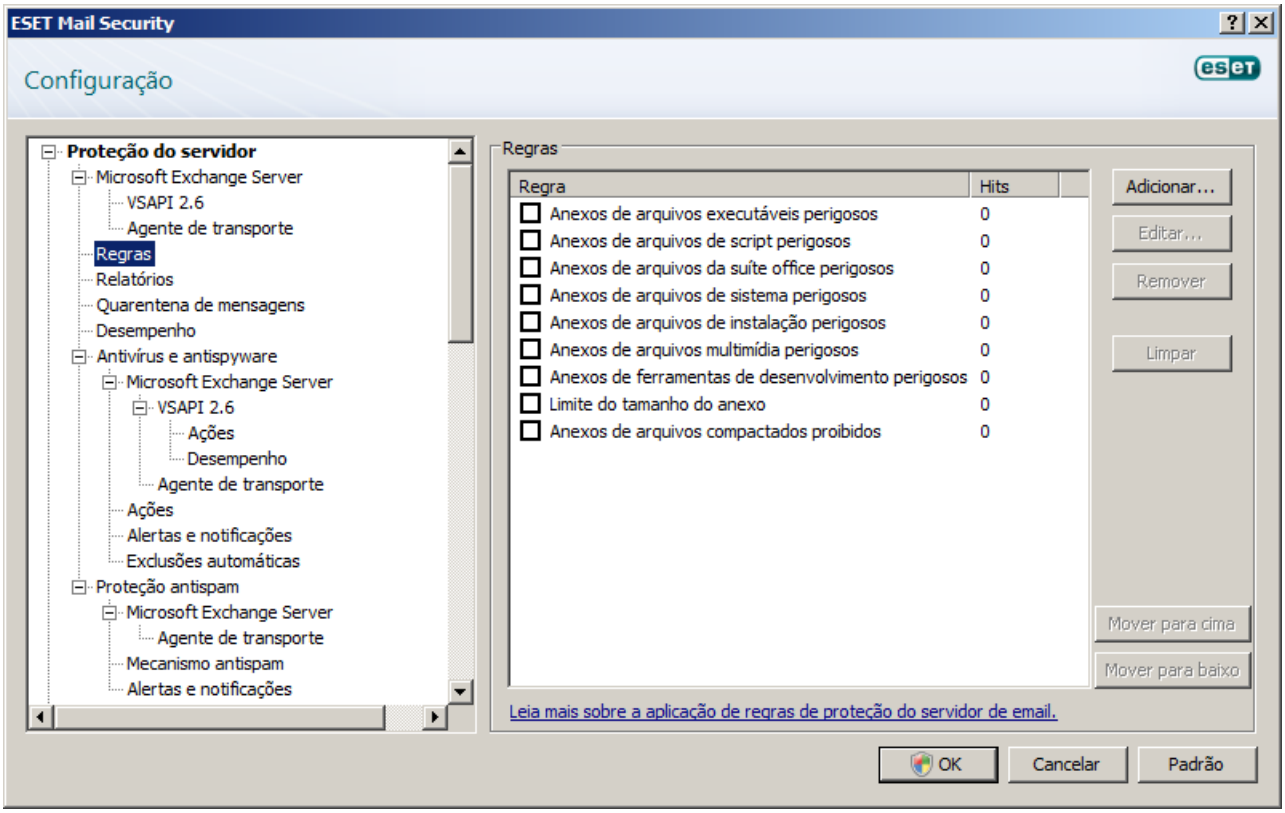
Alerta: A sintaxe incorreta dos códigos de resposta SMTP pode causar mal funcionamento dos componentes do programa e diminuição na eficácia.

OBSERVAÇÃO: Também é possível usar variáveis do sistema ao configurar Respostas de rejeição SMTP.

3.1.2 Regras

O item de menu **Regras** permite aos administradores definir manualmente as condições de filtragem de email e as ações a serem tomadas com os emails filtrados. As regras são aplicadas de acordo com um conjunto de condições combinadas. Várias condições são combinadas com o operador lógico E, aplicando a regra somente se todas as condições forem atendidas. A coluna **Número** (ao lado de cada nome de regra) exibe o número de vezes em que a regra foi aplicada com êxito.

As regras são verificadas em relação à mensagem quando ela é processada pelo agente de transporte (TA) ou pela VSAPI. Quando o TA e a VSAPI estão ativados e a mensagem corresponde às condições da regra, o contador de regras pode aumentar em 2 ou mais. Isso ocorre porque a VSAPI acessa cada parte da mensagem individualmente (corpo, anexo), o que significa que as regras são consequentemente aplicadas a cada parte individualmente. As regras também são aplicadas durante o rastreamento em segundo plano (por exemplo, rastreamento repetido do armazenamento da caixa de correio após uma atualização do banco de dados de assinatura de vírus), o que pode aumentar o contador de regras.



- **Adicionar** – adiciona uma nova regra
- **Editar...** - modifica uma regra existente
- **Remover** – remove a regra selecionada
- **Limpar** – limpa o contador de regras (a coluna Acesso)
- **Mover para cima** – move a regra selecionada para cima na lista
- **Mover para baixo** – move a regra selecionada para baixo na lista

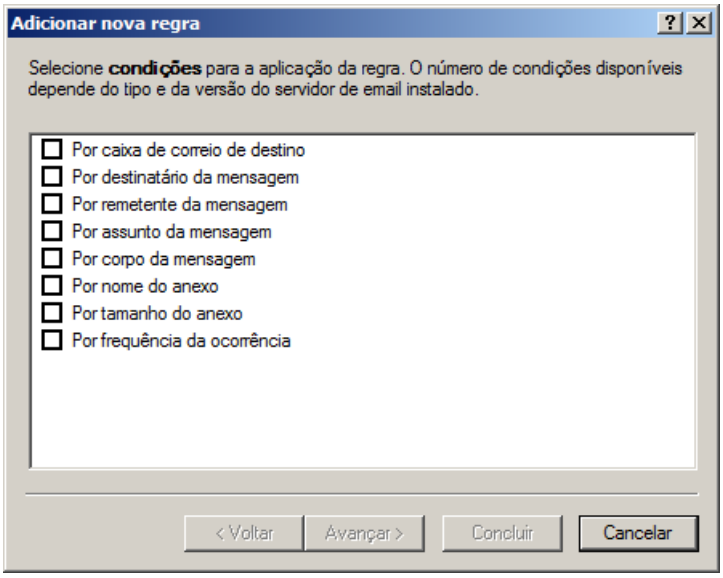
A desmarcação da caixa de seleção (à esquerda do nome de cada regra) desativa a regra atual. Isso permite que a regra seja reativada novamente, se necessário.

OBSERVAÇÃO: Também é possível usar variáveis do sistema (por exemplo, *%PATHEXT%*) ao configurar Regras.

OBSERVAÇÃO: Se uma nova regra foi adicionada ou uma regra existente foi modificada, um novo rastreamento das mensagens começará automaticamente a usar as regras novas/modificadas.

3.1.2.1 Adição de novas regras

Esse assistente o conduz pelo processo de adição de regras especificadas pelo usuário com condições combinadas.



OBSERVAÇÃO: Nem todas as condições são aplicáveis quando a mensagem é rastreada pelo agente de transporte.

- **Por caixa de correio de destino** aplica-se ao nome de uma caixa de correio (VSAPI)
- **Por destinatário da mensagem** aplica-se a uma mensagem enviada a um destinatário especificado (VSAPI + TA)
- **Por remetente da mensagem** aplica-se a uma mensagem enviada por um remetente especificado (VSAPI + TA)
- **Por assunto da mensagem** aplica-se a uma mensagem com uma linha de assunto especificada (VSAPI + TA)
- **Por corpo da mensagem** aplica-se a uma mensagem com texto específico no corpo (VSAPI)
- **Por nome do anexo** aplica-se a uma mensagem com um nome de anexo específico (VSAPI no Exchange 2000 e 2003, VSAPI + TA no Exchange 2007 e 2010)
- **Por tamanho do anexo** aplica-se a uma mensagem com um anexo que excede um tamanho definido (VSAPI no Exchange 2000 e 2003, VSAPI + TA no Exchange 2007 e 2010)
- **Por frequência da ocorrência** aplica-se a objetos (corpo ou anexo do email) cujo número de ocorrências no intervalo especificado exceda o número especificado (VSAPI). Isso é especialmente útil se você recebe constantemente muitos emails de spam com o mesmo corpo ou anexo de email.
- **Por tipo de anexo** aplica-se a uma mensagem com um anexo de tipo de arquivo especificado (o tipo de arquivo real é detectado por seu conteúdo, independentemente da extensão do arquivo) (VSAPI)

Ao especificar as condições anteriores (exceto a condição **Por tamanho do anexo**), é suficiente preencher apenas parte de uma frase desde que a opção **Coincidir palavras inteiras** não esteja selecionada. Os valores não diferenciam maiúsculas de minúsculas, exceto se a opção **Diferenciar maiúsculas de minúsculas** estiver selecionada. Se estiver usando valores que não sejam alfanuméricos, use parênteses e aspas. Também é possível criar condições usando os operadores lógicos E, OU e NÃO.

OBSERVAÇÃO: A lista de regras disponíveis depende da versão instalada do Microsoft Exchange Server.

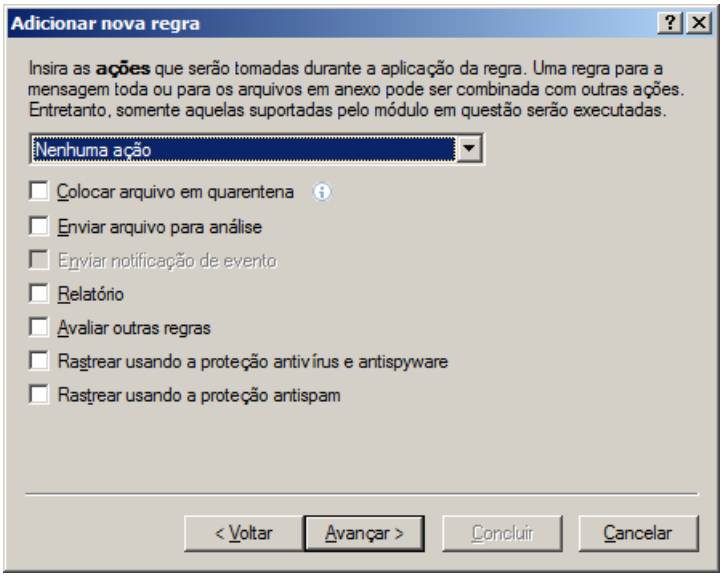
OBSERVAÇÃO: O Microsoft Exchange Server 2000 (VSAPI 2.0) classifica somente o nome do remetente/destinatário exibido, e não o endereço de email. Os endereços de email são classificados a partir do Microsoft Exchange Server 2003 (VSAPI 2.5) e posteriores.

Exemplos de inserção de condições:

Por caixa de correio de destino:	smith
Por remetente de email:	smith@mail.com
Por destinatário de email:	"J.Smith" ou "smith@mail.com"
Por assunto de email:	" "
Por nome do anexo:	".com" OU ".exe"
Por corpo do email:	("grátis" OU "loteria") E ("ganhe" OU "compre")

3.1.2.2 Ações tomadas ao aplicar regras

Esta seção permite selecionar ações a serem executadas nas mensagens e/ou anexos que correspondam às condições definidas nas regras. É possível não executar nenhuma ação, marcar a mensagem como se tivesse uma ameaça/spam ou excluir a mensagem inteira. Quando uma mensagem ou seu anexo corresponder às condições da regra, ela não será rastreada pelos módulos antivírus ou antispam por padrão, exceto se o rastreamento for explicitamente ativado marcando as caixas de seleção na parte inferior (a ação tomada dependerá das configurações antivírus/antispam).



- **Nenhuma ação** – nenhuma ação será realizada com a mensagem
- **Tomar ação para ameaça não limpa** – a mensagem será marcada como se tivesse uma ameaça não limpa (independente se ela contém uma ameaça ou não)
- **Tomar ação para email não solicitado** – a mensagem será marcada como se fosse um spam (independente se ela ser spam ou não). Essa opção funcionará somente se a proteção antispam 37 estiver ativada e a ação estiver sendo realizada no nível do agente de transporte. Caso contrário, essa ação não será realizada.
- **Excluir mensagem** - remove a mensagem inteira com conteúdo que atende às condições; no entanto, essa ação funciona somente no VSAPI 2.5 e em versões mais recentes (VSAPI 2.0 e versões posteriores não podem realizar esta ação)

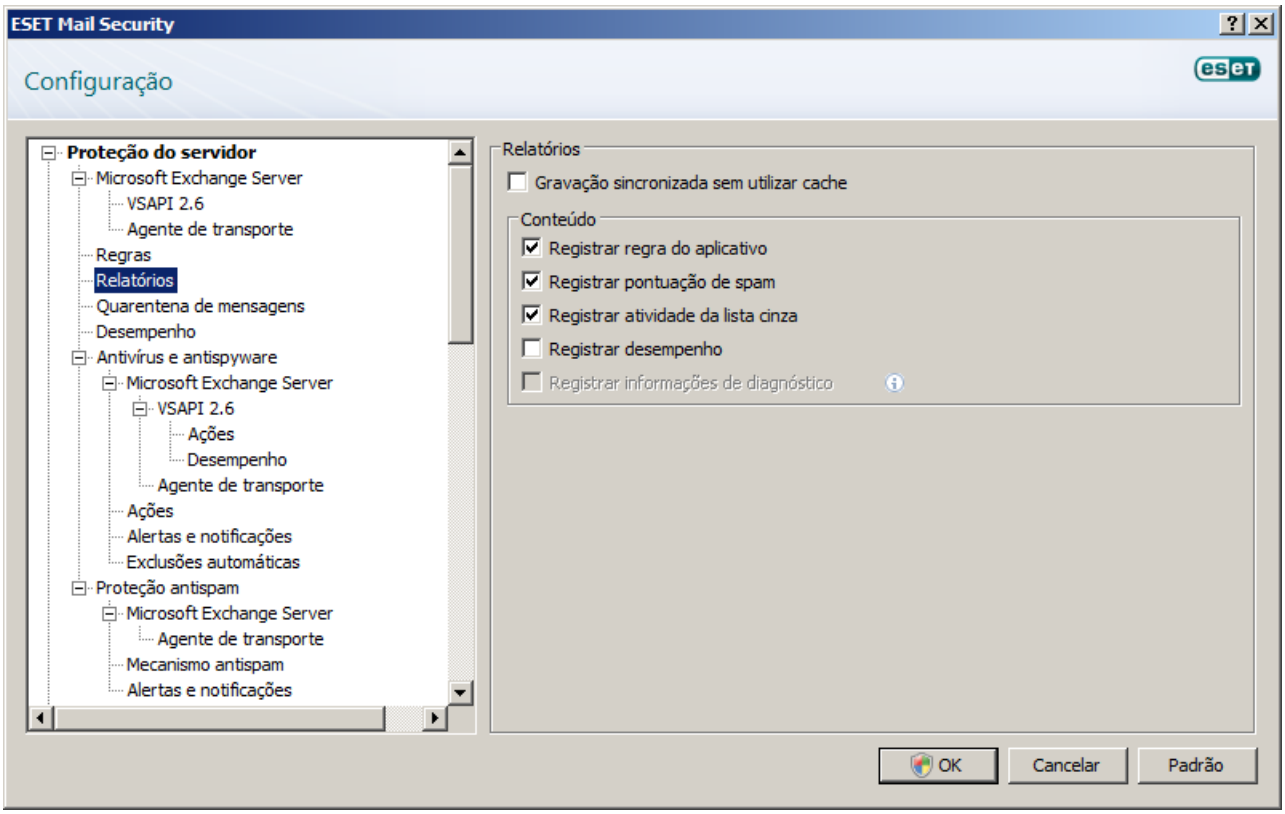
- **Colocar arquivo em quarentena** - o(s) arquivo(s) em anexo que atendem aos critérios de regra serão colocados na quarentena de arquivos do ESET Mail Security; não confunda isso com quarentena de e-mail (para obter mais informações sobre a quarentena de e-mail, consulte Quarentena de mensagens 25)
- **Enviar arquivo para análise** – envia anexos suspeitos para o laboratório da ESET para análise
- **Enviar notificação de evento** - envia uma notificação ao administrador (com base nas configurações em **Ferramentas** > **Alertas e notificações**)
- **Relatório** – salva as informações sobre a regra aplicada no relatório do programa
- **Avaliar outras regras** – permite a avaliação de outras regras, permitindo ao usuário definir vários conjuntos de condições e várias ações a serem tomadas, de acordo com as condições
- **Rastrear usando a proteção antivírus e antispyware** – rastreia a mensagem e seus anexos quanto a ameaças
- **Rastrear usando a proteção antispam** – rastreia a mensagem quanto a spam

OBSERVAÇÃO: Essa opção está disponível somente no Microsoft Exchange Server 2000 e posteriores com o agente de transporte ativado.

A última etapa no assistente de criação de novas regras é nomear cada regra criada. Também é possível adicionar um **Comentário da regra**. Essas informações serão armazenadas no relatório do Microsoft Exchange Server.

3.1.3 Relatórios

As configurações dos relatórios permitem escolher como o relatório será montado. Um protocolo mais detalhado podem conter mais informações, mas ele pode diminuir o desempenho do servidor.

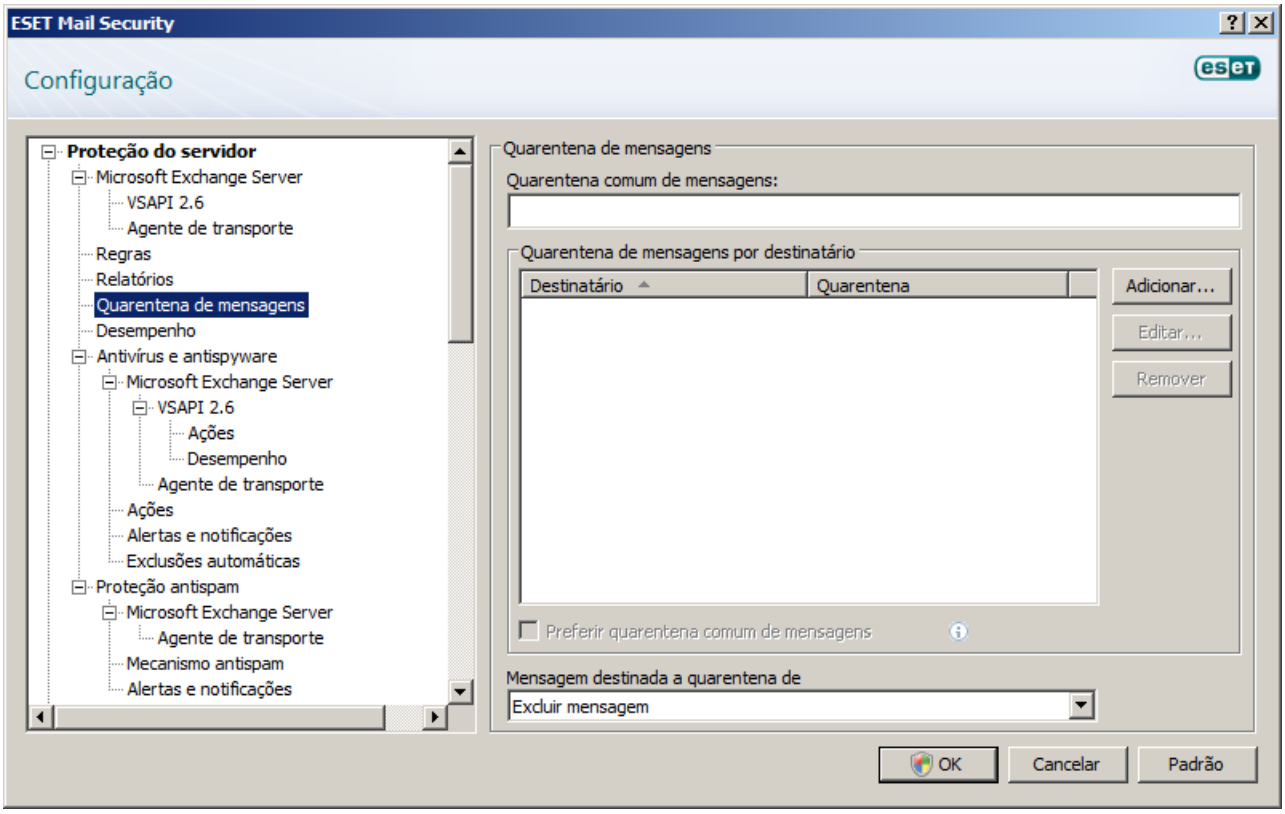


Se a opção **Gravação sincronizada sem utilizar cache** estiver ativada, todas as entradas do relatório serão imediatamente gravadas no relatório, sem serem armazenadas no cache de relatórios. Por padrão, os componentes do ESET Mail Security em execução no Microsoft Exchange Server armazenam as mensagens de relatório em seu cache interno e as enviam para o relatório do aplicativo em intervalos periódicos para manter o desempenho. Nesse caso, entretanto, as entradas de diagnóstico no relatório podem não estar na ordem correta. Recomendamos manter essa configuração desativada, exceto se for necessária para o diagnóstico. É possível especificar o tipo das informações armazenadas nos relatórios no menu **Conteúdo**.

- **Registrar regra do aplicativo** – quando essa opção estiver ativada, o ESET Mail Security gravará o nome de todas as regras ativadas no relatório.
- **Registrar pontuação de spam** – use essa opção para que as atividades relacionadas a spam sejam gravadas no Relatório antispam 96. Quando o servidor de email recebe uma mensagem de SPAM, as informações são gravadas no relatório fornecendo detalhes como a Hora/Data, Remetente, Destinatário, Assunto, Pontuação de SPAM, Motivo e Ação. Isso é útil quando for necessário controlar mensagens de SPAM recebidas, quando e qual ação foi tomada.
- **Registrar atividade da lista cinza** – ative essa opção se desejar que a atividade relacionada à lista cinza seja gravada no Relatório da lista cinza 96. Ele fornece informações como Hora/Data, domínio HELO, Endereço IP, Remetente, Destinatário, Ação, etc.
  OBSERVAÇÃO: Essa opção funciona somente se a Lista cinza estiver ativada nas opções do Agente de transporte 38 em **Proteção do servidor** > **Proteção antispam** > **Microsoft Exchange Server** > **Agente de transporte** na árvore de configuração avançada (F5).
- **Registrar desempenho** – registra informações sobre o intervalo de tempo de uma tarefa executada, tamanho do objeto rastreado, taxa de transferência (kb/s) e classificação de desempenho.
- **Registrar informações de diagnóstico** –registra as informações de diagnóstico necessárias para o ajuste do programa ao protocolo; essa opção é usada principalmente para depuração e identificação de problemas. Não recomendamos manter essa opção ativada. Para ver as informações de diagnóstico fornecidas por essa função, será necessário definir o Detalhamento mínimo de registro em relatório para **Registros de diagnóstico** na configuração **Ferramentas** > **Relatórios** > **Detalhamento mínimo de registro em relatório**.

3.1.4 Quarentena de mensagens

A **Quarentena de mensagens** é uma caixa de correio especial definida pelo administrador do sistema para armazenar mensagens potencialmente infectadas e SPAM. As mensagens armazenadas na quarentena podem ser analisadas ou limpas posteriormente por meio de um banco de dados de assinatura de vírus mais recente.



Há dois tipos de sistemas de quarentena de mensagens que podem ser usados.

Uma opção é usar o sistema de quarentena do Microsoft Exchange (isso se aplica somente ao Microsoft Exchange Server 2007/2010). Nesse caso, o mecanismo interno do Exchange é usado para armazenar mensagens potencialmente infectadas e SPAM. Além disso, é possível adicionar uma caixa de correio de quarentena separada (ou várias caixas de correio) para destinatários específicos, se necessário. Isso significa que as mensagens potencialmente infectadas, que foram originalmente enviadas para um destinatário específico, serão entregues em uma caixa de correio de quarentena separada, em vez de serem entregues na caixa de correio de quarentena interna do Exchange. Isso pode ser útil em alguns casos para manter as mensagens potencialmente infectadas e de SPAM mais organizadas.

Outra opção é usar a **Quarentena comum de mensagens**. Se você estiver usando uma versão anterior do Microsoft Exchange Server (5.5, 2000 ou 2003), basta especificar a **Quarentena comum de mensagens**, que é uma caixa de correio que será usada para armazenar as mensagens potencialmente infectadas Nesse caso, o sistema de quarentena interna do Exchange não é usado. Em vez disso, uma caixa de correio especificada pelo administrador do sistema é usada para essa finalidade. Como na primeira opção, é possível adicionar uma caixa de correio de quarentena separada (ou várias caixas de correio) para destinatários específicos. O resultado é que as mensagens potencialmente infectadas são enviadas para uma caixa de correio separada, em vez de serem entregues na quarentena comum de mensagens.

- **Quarentena comum de mensagens** - é possível especificar o endereço da quarentena comum de mensagens aqui (por exemplo, main_quarantine@company.com) ou é possível usar o sistema interno de quarentena do Microsoft Exchange Server 2007/2010, em vez de deixar esse campo em branco, e escolher **Colocar mensagem em quarentena no sistema do servidor de email** (desde que a quarentena do Exchange exista no ambiente) no menu suspenso na parte inferior. Os emails são entregues para a quarentena pelo mecanismo interno do Exchange usando suas próprias configurações.
  OBSERVAÇÃO: Por padrão, essa quarentena interna não está ativada no Exchange. Se desejar ativá-la, é necessário abrir o Exchange Management Shell e digitar o seguinte comando:

  Set-ContentFilterConfig -QuarantineMailbox name@domain.com

  (substitua name@domain.com pela caixa de correio real que você deseja que o Microsoft Exchange use como caixa de correio de quarentena interna, por exemplo, exchangequarantine@company.com)

- **Quarentena de mensagens por destinatário** – ao usar essa opção, é possível definir caixas de correio de quarentena de mensagens para vários destinatários. Toda regra de quarentena pode ser ativada ou desativada marcando ou desmarcando a caixa de seleção em sua linha.

  Adicionar – é possível adicionar uma nova regra de quarentena inserindo o endereço de email do destinatário desejado e o endereço de email da quarentena ao qual o email será encaminhado.

  Editar... – editar uma regra de quarentena selecionada

  Remover – remove uma regra de quarentena selecionada

  Preferir quarentena comum de mensagens – quando essa opção está ativada, a mensagem será entregue à quarentena comum especificada se mais de uma regra de quarentena for atendida (por exemplo, se uma mensagem tiver vários destinatários e alguns deles estiverem definidos em várias regras de quarentena)

- **Mensagem destinada a quarentena de mensagens não existentes** (se você não especificou uma quarentena comum de mensagens, terá as seguintes opções como ação a ser tomada em mensagens possivelmente infectadas e SPAM)

  Nenhuma ação – a mensagem será processada de modo padrão – entregue ao destinatário (não recomendado)
  Excluir mensagem –a mensagem será excluída se for endereçada a um destinatário sem regra de quarentena existente e se uma quarentena comum de mensagens não for especificada, isso significa que todas as mensagens possivelmente infectadas e SPAM serão automaticamente excluídas sem serem armazenadas em lugar nenhum
  Colocar mensagem em quarentena no sistema do servidor de email – uma mensagem será entregue e armazenada na quarentena do sistema interno do Exchange (não disponível no Microsoft Exchange Server 2003 e anteriores)

OBSERVAÇÃO: Também é possível usar variáveis do sistema (por exemplo, *%USERNAME%*) ao definir as configurações de Quarentena de mensagens.

3.1.4.1 Adição de nova regra de quarentena

Insira o endereço de email do destinatário e o endereço de email da quarentena nos campos apropriados.

Se desejar excluir uma mensagem de email endereçada a um destinatário que não tem uma regra de quarentena aplicada, você poderá selecionar a opção **Excluir mensagem** no menu suspenso **Mensagem destinada a quarentena de mensagens não existentes**.

3.1.5 Desempenho

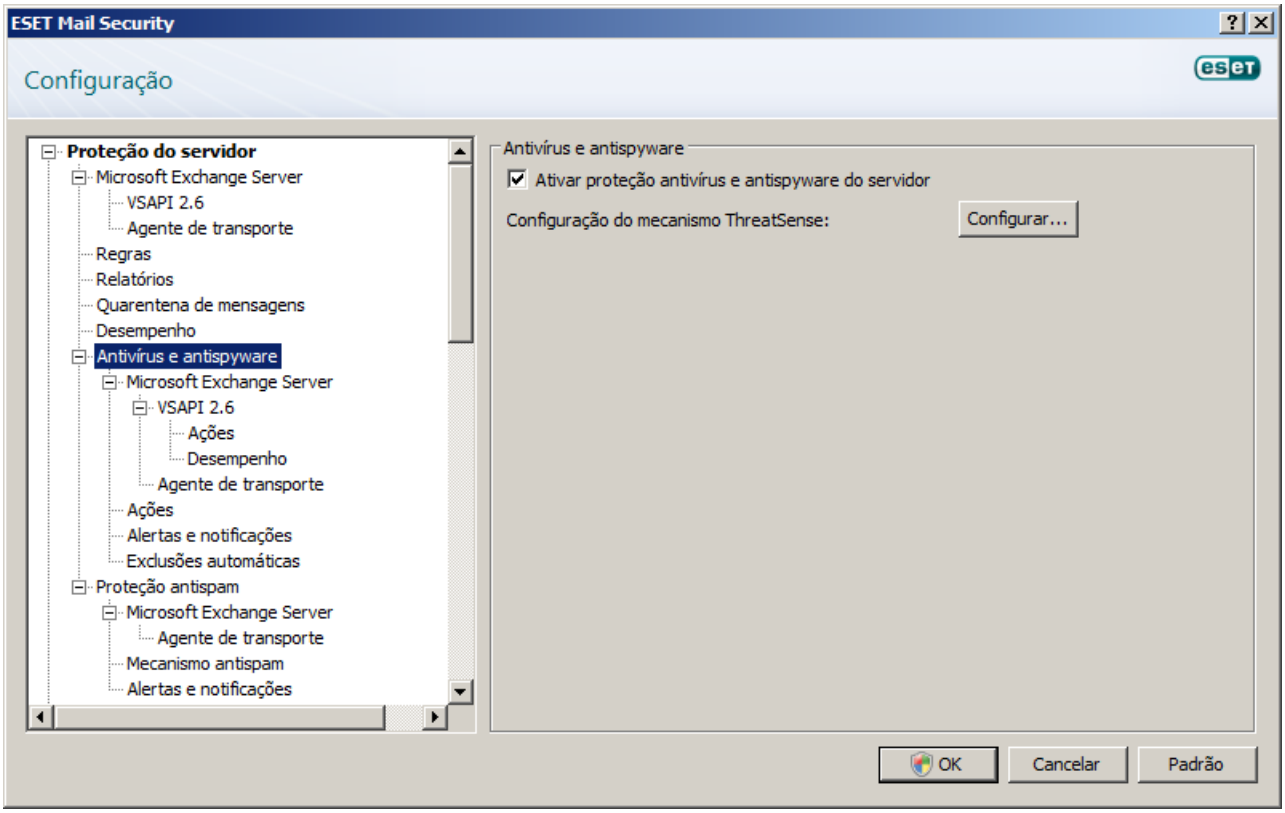
Nesta seção, é possível definir uma pasta para armazenar arquivos temporários para melhorar o desempenho do programa. Se nenhuma pasta for especificada, o ESET Mail Security criará os arquivos temporários na pasta temporária do sistema.

OBSERVAÇÃO: Para reduzir o impacto potencial de E/S e de fragmentação, recomendamos manter a Pasta temporária em uma unidade de disco rígido diferente daquela em que o Microsoft Exchange Server está instalado. Recomendamos enfaticamente evitar atribuir a Pasta temporária a uma mídia removível, como, por exemplo, disquete, USB, DVD, etc.

OBSERVAÇÃO: É possível usar variáveis do sistema (por exemplo, *%SystemRoot%\TEMP*) ao definir as configurações de Desempenho.

3.2 Configurações antivírus e antispyware

É possível ativar a proteção antivírus e antispyware do servidor de email selecionando a opção **Ativar proteção antivírus e antispyware do servidor**. Observe que a proteção antivírus e antispyware é ativada automaticamente após cada reinicialização do serviço/computador. A configuração dos parâmetros do mecanismo ThreatSense pode ser acessada clicando no botão **Configurar...**.



3.2.1 Microsoft Exchange Server

Quando se trata de proteção antivírus e antispyware, o ESET Mail Security para Microsoft Exchange Server usa dois tipos de rastreamento. Um tipo rastreia mensagens via VSAPI e o outro usa o Agente de transporte.

- A proteção que usa a VSAPI 28 rastreia as mensagens diretamente no armazenamento do Exchange Server.
- A proteção doAgente de transporte 34 rastreia o tráfego SMTP em vez do armazenamento do Exchange Server. Se esse tipo de proteção estiver ativado, todas as mensagens e seus componentes serão rastreados durante o transporte, mesmo antes de chegarem ao armazenamento do Exchange Server ou antes de serem enviadas via SMTP. A filtragem no nível do servidor SMTP é assegurada por um plugin especializado. No Microsoft Exchange Server 2000 e 2003, o plugin em questão (Event Sink) é registrado no servidor SMTP como parte do Internet Information Services (IIS). No Microsoft Exchange Server 2007/2010, o plugin está registrado como um agente de transporte nas funções Edge ou Hub do Microsoft Exchange Server.

OBSERVAÇÃO: O agente de transporte não está disponível no Microsoft Exchange Server 5.5, entretanto está disponível em todas as versões mais recentes do Microsoft Exchange Server (versão 2000 em diante).

É possível ter a proteção antivírus e antispyware da VSAPI e do Agente de transporte trabalhando ao mesmo tempo (esse é o padrão e a configuração recomendada). Como alternativa, é possível optar por usar apenas um tipo de proteção (VSAPI ou Agente de transporte). Elas podem ser ativadas ou desativadas independentemente. Recomendamos usar os dois tipos para assegurar proteção antivírus e antispyware máxima. Não recomendamos desativar ambas.

3.2.1.1 VSAPI (Virus-Scanning Application Programming Interface)

O Microsoft Exchange Server fornece um mecanismo para assegurar que cada componente da mensagem será rastreado em relação ao banco de dados de assinatura de vírus atual. Se uma mensagem não foi rastreada anteriormente, seus componentes correspondentes serão submetidos ao scanner antes que a mensagem seja liberada para o cliente. Toda versão compatível do Microsoft Exchange Server (5.5/2000/2003/2007/2010) fornece uma versão diferente da VSAPI.

3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

Essa versão do Microsoft Exchange Server inclui a VSAPI versão 1.0.

Se a opção **Rastreamento em segundo plano** estiver ativada, ela permitirá o rastreamento de todas as mensagens em segundo plano no sistema. O Microsoft Exchange Server decide se um rastreamento em segundo plano será executado ou não com base em vários fatores, como a carga do sistema atual, o número de usuários ativos, etc. O Microsoft Exchange Server mantém um relatório das mensagens rastreadas e da versão do banco de dados de assinatura de vírus usado. Se você estiver abrindo uma mensagem que não tenha sido rastreada pelo banco de dados de assinatura de vírus mais recente, o Microsoft Exchange Server enviará a mensagem para o ESET Mail Security para ela ser rastreada antes da abertura da mensagem em seu cliente de email.

Como o rastreamento em segundo plano pode afetar a carga do sistema (o rastreamento é realizado depois de cada atualização do banco de dados de assinatura de vírus), recomendamos usar rastreamento agendado fora do horário de trabalho. O rastreamento em segundo plano agendado pode ser configurado por meio de uma tarefa especial na Agenda/Planejamento. Ao agendar uma tarefa de rastreamento em segundo plano, é possível definir a hora de início, o número de repetições e outros parâmetros disponíveis na Agenda/Planejamento. Depois que a tarefa tiver sido agendada, ela será exibida na lista de tarefas agendadas e, assim como com as outras tarefas, será possível modificar seus parâmetros, excluí-la ou desativá-la temporariamente.

3.2.1.1.1.1 Ações

Nesta seção, é possível especificar as ações a serem realizadas quando uma mensagem e/ou anexo for classificado (a) como infectado(a).

O campo **Ação a ser tomada se a limpeza não for possível** permite **Bloquear** o conteúdo infectado, **Excluir** a mensagem ou não executar **Nenhuma ação** no conteúdo infectado da mensagem. Essa ação será aplicada somente se a limpeza automática (definida em **Configuração dos parâmetros do mecanismo ThreatSense** > Limpeza 79) não limpar a mensagem.

O campo **Exclusão** permite definir o **Método de exclusão do anexo** em uma destas opções:

- **Truncar arquivo no tamanho zero** – O ESET Mail Security trunca o anexo no tamanho zero e permite ao destinatário ver o nome e o tipo do arquivo anexo
- **Substituir anexo com informações sobre a ação** – O ESET Mail Security substitui o arquivo infectado por um protocolo de vírus ou descrição de regra

Ao clicar no botão **Rastrear novamente** , você executará outro rastreamento nas mensagens e arquivos que já foram rastreados.

3.2.1.1.1.2 Desempenho

Durante o rastreamento, o Microsoft Exchange Server permite limitar um tempo para a abertura dos anexos das mensagens. Esse tempo é definido no campo **Limite de tempo para resposta (ms)** e representa o período após o qual o cliente tentará acessar novamente o arquivo que estava anteriormente inacessível devido ao rastreamento.

3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

Essa versão do Microsoft Exchange Server inclui a VSAPI versão 2.0.

Se a opção **Ativar proteção antivírus e antispyware VSAPI 2.0** for desmarcada, o plug-in do ESET Mail Security para Exchange Server será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus. Entretanto, as mensagens ainda serão rastreadas quanto a spam 38 e as regras 21 serão aplicadas.

Se a opção **Rastreamento proativo** estiver ativada, as novas mensagens recebidas serão rastreadas na mesma ordem em que foram recebidas. Se essa opção estiver ativada e um usuário abrir uma mensagem que ainda não tenha sido rastreada, essa mensagem será rastreada antes das outras mensagens na fila.

A opção **Rastreamento em segundo plano** permite o rastreamento de todas as mensagens em segundo plano no sistema. O Microsoft Exchange Server decide se um rastreamento em segundo plano será executado ou não com base em vários fatores, como a carga do sistema atual, o número de usuários ativos, etc. O Microsoft Exchange Server mantém um relatório das mensagens rastreadas e da versão do banco de dados de assinatura de vírus usado. Se você estiver abrindo uma mensagem que não tenha sido rastreada pelo banco de dados de assinatura de vírus mais recente, o Microsoft Exchange Server enviará a mensagem para o ESET Mail Security para ela ser rastreada antes da abertura da mensagem em seu cliente de email.

Como o rastreamento em segundo plano pode afetar a carga do sistema (o rastreamento é realizado depois de cada atualização do banco de dados de assinatura de vírus), recomendamos usar rastreamento agendado fora do horário de trabalho. O rastreamento em segundo plano agendado pode ser configurado por meio de uma tarefa especial na Agenda/Planejamento. Ao agendar uma tarefa de rastreamento em segundo plano, é possível definir a hora de início, o número de repetições e outros parâmetros disponíveis na Agenda/Planejamento. Depois que a tarefa tiver sido agendada, ela será exibida na lista de tarefas agendadas e, assim como com as outras tarefas, será possível modificar seus parâmetros, excluí-la ou desativá-la temporariamente.

Se você desejar rastrear mensagens com texto simples, selecione a opção **Rastrear corpo das mensagens em texto simples**.

A ativação da opção **Rastrear corpo das mensagens em RTF** ativa o rastreamento do corpo das mensagens em RTF. O corpo das mensagem em RTF pode conter vírus de macro.

3.2.1.1.2.1 Ações

Nesta seção, é possível especificar as ações a serem realizadas quando uma mensagem e/ou anexo for classificado (a) como infectado(a).

O campo **Ação a ser tomada se a limpeza não for possível** permite **Bloquear** o conteúdo infectado, **Excluir** a mensagem ou não executar **Nenhuma ação** no conteúdo infectado da mensagem. Essa ação será aplicada somente se a limpeza automática (definida em **Configuração dos parâmetros do mecanismo ThreatSense >** Limpeza 79) não limpar a mensagem.

A opção **Exclusão** permite definir o **Método de exclusão da mensagem** e o **Método de exclusão do anexo**.

É possível definir o **Método de exclusão da mensagem** como:

- **Excluir corpo da mensagem** – exclui o corpo da mensagem infectada; o destinatário receberá uma mensagem vazia e os anexos que não estiverem infectados
- **Regravar corpo da mensagem com informações sobre a ação** – regrava o corpo da mensagem infectada com informações sobre as ações realizadas

É possível definir o **Método de exclusão do anexo** como:

- **Truncar arquivo no tamanho zero** – O ESET Mail Security trunca o anexo no tamanho zero e permite ao destinatário ver o nome e o tipo do arquivo anexo
- **Substituir anexo com informações sobre a ação** – O ESET Mail Security substitui o arquivo infectado por um protocolo de vírus ou descrição de regra

Ao clicar no botão **Rastrear novamente** , você executará outro rastreamento nas mensagens e arquivos que já foram rastreados.

3.2.1.1.2.2 Desempenho

Nesta seção, é possível definir o número de encadeamentos de rastreamento independentes usados por vez. Mais encadeamentos em máquinas com vários processadores pode aumentar a velocidade do rastreamento. Para o melhor desempenho do programa, aconselhamos usar um número igual de mecanismos de rastreamento e encadeamentos de rastreamento do ThreatSense.

A opção **Limite de tempo para resposta (s)** permite definir o tempo máximo que um encadeamento aguardará até que o rastreamento da mensagem seja concluído. Se o rastreamento não for concluído nesse limite de tempo, o Microsoft Exchange Server negará o acesso do cliente ao email. O rastreamento não será interrompido, e, após sua conclusão, todas as outras tentativas de acesso ao arquivo serão bem-sucedidas.

DICA: Para determinar o **Número de encadeamentos de rastreamento**, o fornecedor do Microsoft Exchange Server recomenda usar a seguinte fórmula: [número de processadores físicos] x 2 + 1.

OBSERVAÇÃO: O desempenho não melhorará significativamente se houver mais mecanismos de rastreamento do ThreatSense que encadeamentos de rastreamento.

3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

Essa versão do Microsoft Exchange Server inclui a VSAPI versão 2.5.

Se a opção **Ativar proteção antivírus e antispyware VSAPI 2.5** for desmarcada, o plug-in do ESET Mail Security para Exchange Server será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus. Entretanto, as mensagens ainda serão rastreadas quanto a spam 38 e as regras 21 serão aplicadas.

Se a opção **Rastreamento proativo** estiver ativada, as novas mensagens recebidas serão rastreadas na mesma ordem em que foram recebidas. Se essa opção estiver ativada e um usuário abrir uma mensagem que ainda não tenha sido rastreada, essa mensagem será rastreada antes das outras mensagens na fila.

A opção **Rastreamento em segundo plano** permite o rastreamento de todas as mensagens em segundo plano no sistema. O Microsoft Exchange Server decide se um rastreamento em segundo plano será executado ou não com base em vários fatores, como a carga do sistema atual, o número de usuários ativos, etc. O Microsoft Exchange Server mantém um relatório das mensagens rastreadas e da versão do banco de dados de assinatura de vírus usado. Se você estiver abrindo uma mensagem que não tenha sido rastreada pelo banco de dados de assinatura de vírus mais recente, o Microsoft Exchange Server enviará a mensagem para o ESET Mail Security para ela ser rastreada antes da abertura da mensagem em seu cliente de email.

Como o rastreamento em segundo plano pode afetar a carga do sistema (o rastreamento é realizado depois de cada atualização do banco de dados de assinatura de vírus), recomendamos usar rastreamento agendado fora do horário de trabalho. O rastreamento em segundo plano agendado pode ser configurado por meio de uma tarefa especial na Agenda/Planejamento. Ao agendar uma tarefa de rastreamento em segundo plano, é possível definir a hora de início, o número de repetições e outros parâmetros disponíveis na Agenda/Planejamento. Depois que a tarefa tiver sido agendada, ela será exibida na lista de tarefas agendadas e, assim como com as outras tarefas, será possível modificar seus parâmetros, excluí-la ou desativá-la temporariamente.

A ativação da opção **Rastrear corpo das mensagens em RTF** ativa o rastreamento do corpo das mensagens em RTF. O corpo das mensagem em RTF pode conter vírus de macro.

A opção **Mensagens de rastreamento transportadas** permite rastrear mensagens que não foram armazenadas no Microsoft Exchange Server local e que estão sendo entregues a outros servidores de email por meio do Microsoft Exchange Server local. O Microsoft Exchange Server pode ser configurado como um gateway, que encaminha mensagens para outros servidores de email. Se o rastreamento de mensagens estiver ativado, o ESET Mail Security também rastreará essas mensagens. Essa opção só está disponível quando o agente de transporte está desativado.

OBSERVAÇÃO: O corpo de email com texto simples não é rastreado pela VSAPI.

3.2.1.1.3.1 Ações

Nesta seção, é possível especificar as ações a serem realizadas quando uma mensagem e/ou anexo for classificado (a) como infectado(a).

O campo **Ação a ser tomada se a limpeza não for possível** permite **Bloquear** o conteúdo infectado, **Excluir** o conteúdo infectado da mensagem, **Excluir toda a mensagem**, incluindo o conteúdo infectado ou não executar **Nenhuma ação**. Essa ação será aplicada somente se a limpeza automática (definida em **Configuração dos parâmetros do mecanismo ThreatSense >** Limpeza 79) não limpar a mensagem.

A opção **Exclusão** permite definir o **Método de exclusão da mensagem** e o **Método de exclusão do anexo**.

É possível definir o **Método de exclusão da mensagem** como:

- **Excluir corpo da mensagem** – exclui o corpo da mensagem infectada; o destinatário receberá uma mensagem vazia e os anexos que não estiverem infectados
- **Regravar corpo da mensagem com informações sobre a ação** – regrava o corpo da mensagem infectada com informações sobre as ações realizadas
- **Excluir toda a mensagem** – exclui a mensagem inteira, incluindo anexos; é possível definir qual ação será executada ao excluir anexos

É possível definir o **Método de exclusão do anexo** como:

- **Truncar arquivo no tamanho zero** – O ESET Mail Security trunca o anexo no tamanho zero e permite ao destinatário ver o nome e o tipo do arquivo anexo
- **Substituir anexo com informações sobre a ação** – O ESET Mail Security substitui o arquivo infectado por um protocolo de vírus ou descrição de regra
- **Excluir toda a mensagem** – exclui a mensagem inteira, incluindo anexos; é possível definir qual ação será executada ao excluir anexos

Ao clicar no botão **Rastrear novamente** , você executará outro rastreamento nas mensagens e arquivos que já foram rastreados.

3.2.1.1.3.2 Desempenho

Nesta seção, é possível definir o número de encadeamentos de rastreamento independentes usados por vez. Mais encadeamentos em máquinas com vários processadores pode aumentar a velocidade do rastreamento. Para o melhor desempenho do programa, aconselhamos usar um número igual de mecanismos de rastreamento e encadeamentos de rastreamento do ThreatSense.

A opção **Limite de tempo para resposta (s)** permite definir o tempo máximo que um encadeamento aguardará até que o rastreamento da mensagem seja concluído. Se o rastreamento não for concluído nesse limite de tempo, o Microsoft Exchange Server negará o acesso do cliente ao email. O rastreamento não será interrompido, e, após sua conclusão, todas as outras tentativas de acesso ao arquivo serão bem-sucedidas.

DICA: Para determinar o **Número de encadeamentos de rastreamento**, o fornecedor do Microsoft Exchange Server recomenda usar a seguinte fórmula: [número de processadores físicos] x 2 + 1.

OBSERVAÇÃO: O desempenho não melhorará significativamente se houver mais mecanismos de rastreamento do ThreatSense que encadeamentos de rastreamento.

3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

Essa versão do Microsoft Exchange Server inclui a VSAPI versão 2.6.

Se a opção **Ativar proteção antivírus e antispyware VSAPI 2.6** for desmarcada, o plug-in do ESET Mail Security para Exchange Server será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus. Entretanto, as mensagens ainda serão rastreadas quanto a spam 38 e as regras 21 serão aplicadas.

Se a opção **Rastreamento proativo** estiver ativada, as novas mensagens recebidas serão rastreadas na mesma ordem em que foram recebidas. Se essa opção estiver ativada e um usuário abrir uma mensagem que ainda não tenha sido rastreada, essa mensagem será rastreada antes das outras mensagens na fila.

A opção **Rastreamento em segundo plano** permite o rastreamento de todas as mensagens em segundo plano no sistema. O Microsoft Exchange Server decide se um rastreamento em segundo plano será executado ou não com base em vários fatores, como a carga do sistema atual, o número de usuários ativos, etc. O Microsoft Exchange Server mantém um relatório das mensagens rastreadas e da versão do banco de dados de assinatura de vírus usado. Se você estiver abrindo uma mensagem que não tenha sido rastreada pelo banco de dados de assinatura de vírus mais recente, o Microsoft Exchange Server enviará a mensagem para o ESET Mail Security para ela ser rastreada antes da abertura da mensagem em seu cliente de email. É possível optar por **Rastrear somente mensagens com anexos** e filtrar de acordo com a hora recebida com as seguintes opções de **Nível de rastreamento**:

- **Todas as mensagens**
- **Mensagens recebidas no último ano**
- **Mensagens recebidas nos últimos 6 meses**
- **Mensagens recebidas nos últimos 3 meses**
- **Mensagens recebidas no último mês**
- **Mensagens recebidas na última semana**

Como o rastreamento em segundo plano pode afetar a carga do sistema (o rastreamento é realizado depois de cada atualização do banco de dados de assinatura de vírus), recomendamos usar rastreamento agendado fora do horário de trabalho. O rastreamento em segundo plano agendado pode ser configurado por meio de uma tarefa especial na Agenda/Planejamento. Ao agendar uma tarefa de rastreamento em segundo plano, é possível definir a hora de início, o número de repetições e outros parâmetros disponíveis na Agenda/Planejamento. Depois que a

tarefa tiver sido agendada, ela será exibida na lista de tarefas agendadas e, assim como com as outras tarefas, será possível modificar seus parâmetros, excluí-la ou desativá-la temporariamente.

A ativação da opção **Rastrear corpo das mensagens em RTF** ativa o rastreamento do corpo das mensagens em RTF. O corpo das mensagem em RTF pode conter vírus de macro.

OBSERVAÇÃO: O corpo de email com texto simples não é rastreado pela VSAPI.

3.2.1.1.4.1 Ações

Nesta seção, é possível especificar as ações a serem realizadas quando uma mensagem e/ou anexo for classificado (a) como infectado(a).

O campo **Ação a ser tomada se a limpeza não for possível** permite **Bloquear** o conteúdo infectado, **Excluir objeto** – o conteúdo infectado da mensagem, **Excluir toda a mensagem** ou não executar **Nenhuma ação**. Essa ação será aplicada somente se a limpeza automática (definida em **Configuração dos parâmetros do mecanismo ThreatSense** > Limpeza 79) não limpar a mensagem.

Como descrito anteriormente, é possível definir a **Ação a ser tomada se a limpeza não for possível** como:

- **Nenhuma ação** – não executa nenhuma ação no conteúdo infectado da mensagem
- **Bloquear** – bloqueia a mensagem antes que ela seja recebida no armazenamento do Microsoft Exchange Server
- **Excluir objeto** – exclui o conteúdo infectado da mensagem
- **Excluir toda a mensagem** – exclui a mensagem inteira, incluindo o conteúdo infectado

A opção **Exclusão** permite definir o **Método de exclusão do corpo da mensagem** e o **Método de exclusão do anexo**.

É possível definir o **Método de exclusão do corpo da mensagem** como:

- **Excluir corpo da mensagem** – exclui o corpo da mensagem infectada; o destinatário receberá uma mensagem vazia e os anexos que não estiverem infectados
- **Regravar corpo da mensagem com informações sobre a ação** – regrava o corpo da mensagem infectada com informações sobre as ações realizadas
- **Excluir toda a mensagem** – exclui a mensagem inteira, incluindo anexos; é possível definir qual ação será executada ao excluir anexos

É possível definir o **Método de exclusão do anexo** como:

- **Truncar arquivo no tamanho zero** – O ESET Mail Security trunca o anexo no tamanho zero e permite ao destinatário ver o nome e o tipo do arquivo anexo
- **Substituir anexo com informações sobre a ação** – O ESET Mail Security substitui o arquivo infectado por um protocolo de vírus ou descrição de regra
- **Excluir toda a mensagem** – exclui o anexo

Se a opção **Usar quarentena da VSAPI** estiver ativada, as mensagens infectadas serão armazenadas na quarentena do servidor de email. Observe que essa é a quarentena gerenciada da VSAPI do servidor (não a quarentena ou a caixa de correio de quarentena do cliente). As mensagens infectadas armazenadas na quarentena do servidor de email ficam inacessíveis até que sejam limpas com o banco de dados de assinatura de vírus mais recente.

Ao clicar no botão **Rastrear novamente** , você executará outro rastreamento nas mensagens e arquivos que já foram rastreados.

3.2.1.1.4.2 Desempenho

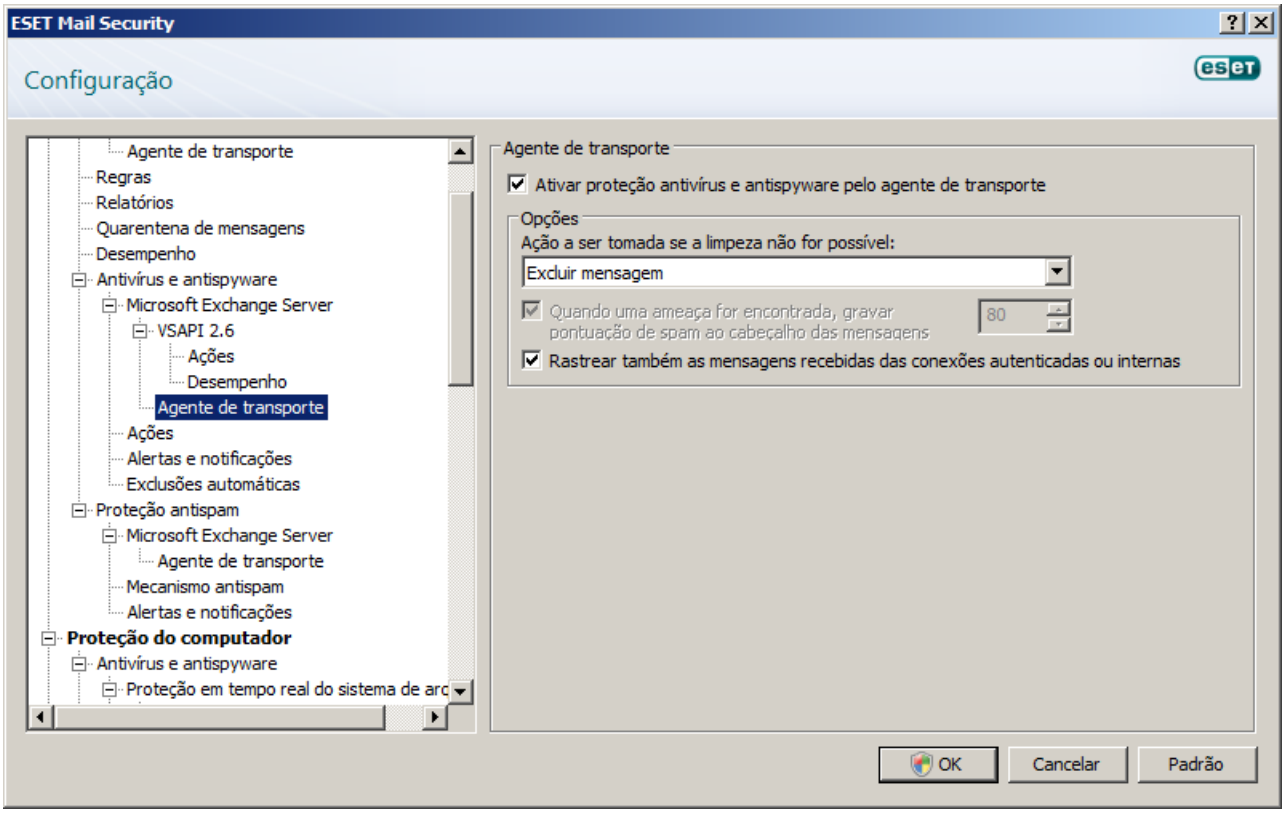
Nesta seção, é possível definir o número de encadeamentos de rastreamento independentes usados por vez. Mais encadeamentos em máquinas com vários processadores pode aumentar a velocidade do rastreamento. Para o melhor desempenho do programa, aconselhamos usar um número igual de mecanismos de rastreamento e encadeamentos de rastreamento do ThreatSense.

DICA: Para determinar o **Número de encadeamentos de rastreamento**, o fornecedor do Microsoft Exchange Server recomenda usar a seguinte fórmula: [número de processadores físicos] x 2 + 1.

OBSERVAÇÃO: O desempenho não melhorará significativamente se houver mais mecanismos de rastreamento do ThreatSense que encadeamentos de rastreamento.

3.2.1.1.5 Agente de transporte

Nesta seção, é possível ativar ou desativar a proteção antivírus e antispyware pelo agente de transporte. Para o Microsoft Exchange Server 2007 e posteriores, só é possível instalar um agente de transporte se o servidor estiver em uma das duas funções: *Transporte de Edge* ou *Transporte de Hub*.



Se houver uma mensagem que não pode ser limpa, ela será processada de acordo com as configurações na seção Agente de transporte. A mensagem pode ser excluída, enviada para a caixa de correio de quarentena ou mantida.

Se a opção **Ativar proteção antivírus e antispyware pelo agente de transporte** for desmarcada, o plug-in do ESET Mail Security para Exchange Server não será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus. Entretanto, as mensagens ainda serão rastreadas quanto a spam 38 e as regras 21 serão aplicadas.

Ao **Ativar proteção antivírus e antispyware pelo agente de transporte**, é possível definir a **Ação a ser tomada se a limpeza não for possível** :

- **Manter mensagem** – mantém uma mensagem infectada que não pôde ser limpa
- **Colocar mensagem em quarentena** – envia uma mensagem infectada para a caixa de correio de quarentena
- **Excluir mensagem** – exclui uma mensagem infectada

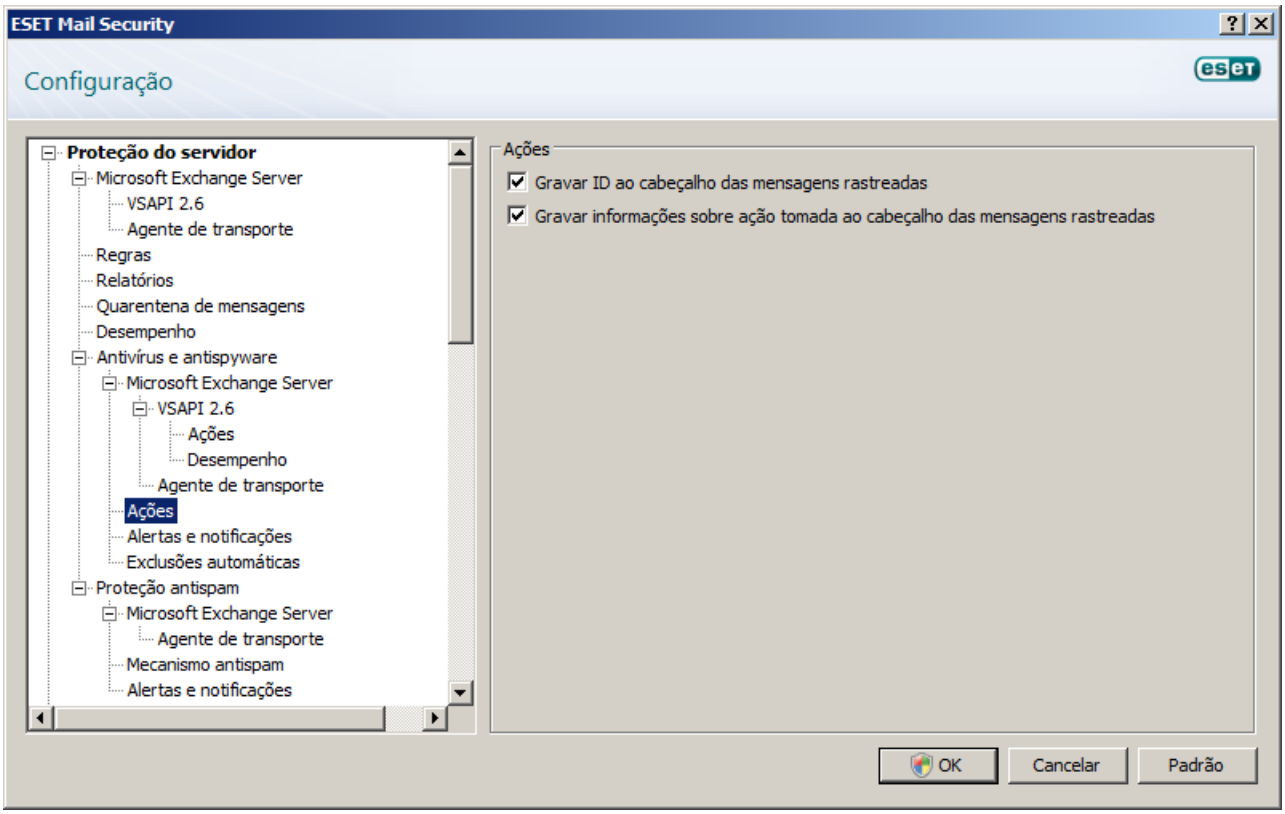
Quando uma ameaça for encontrada, gravar pontuação de spam ao cabeçalho das mensagens rastreadas (%) – define a pontuação de spam (a probabilidade de a mensagem ser spam) em um valor especificado, expresso como porcentagem

Isso significa que, se uma ameaça for encontrada, uma pontuação de spam (valor especificado em %) será gravada na mensagem rastreada. Como os botnets são responsáveis pelo envio da maioria das mensagens infectadas, as mensagens distribuídos dessa maneira serão classificadas como spam. Para que esse recurso funcione com eficácia, a opção **Gravar nível de confiança de spam (SCL) às mensagens rastreadas de acordo com a pontuação de spam** em **Proteção do servidor** > **Microsoft Exchange Server** > Agente de transporte 19 deve estar ativada.

Se a opção **Rastrear também as mensagens recebidas das conexões autenticadas ou internas** estiver ativada, o ESET Mail Security também executará o rastreamento das mensagens recebidas de origens autenticadas ou servidores locais. O rastreamento dessas mensagens é recomendado, pois aumenta a proteção, mas é opcional.

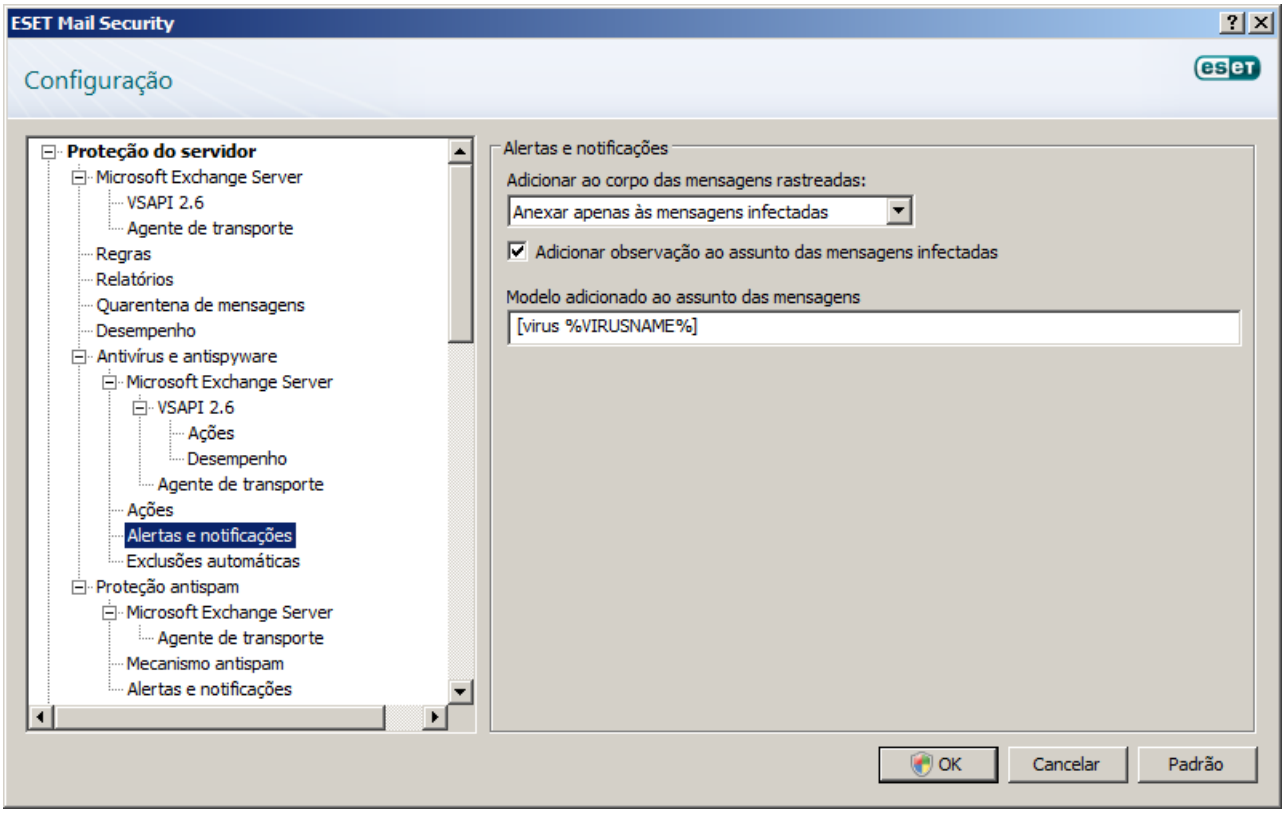
3.2.2 Ações

Nesta seção, é possível optar por anexar um ID de tarefa de rastreamento e/ou informações sobre o resultado do rastreamento ao cabeçalho das mensagens rastreadas.



3.2.3 Alertas e notificações

O ESET Mail Security permite anexar texto ao assunto ou corpo original das mensagens infectadas.



Adicionar ao corpo das mensagens rastreadas: oferece três opções:

- **Não anexar às mensagens**
- **Anexar apenas às mensagens infectadas**
- **Anexar a todas as mensagens rastreadas** (isso não se aplica a mensagens internas)

Ao ativar **Adicionar observação ao assunto das mensagens infectadas**, o ESET Mail Security anexará uma marca de notificação ao assunto do email com o valor definido no campo de texto **Modelo adicionado ao assunto das mensagens infectadas** (por padrão [*vírus %VIRUSNAME%*]). As modificações mencionadas anteriormente podem ajudar a automatizar a filtragem dos emails infectados filtrando emails com um assunto específico (se houver suporte no cliente de email) em uma pasta separada.

OBSERVAÇÃO: Também é possível usar variáveis do sistema ao adicionar um modelo ao assunto da mensagem.

3.2.4 Exclusões automáticas

Os desenvolvedores de aplicativos de servidor e sistemas operacionais recomendam excluir conjuntos de arquivos e pastas críticos de trabalho do rastreamento do antivírus para a maioria de seus produtos. Os rastreamentos de antivírus podem ter uma influência negativa no desempenho de um servidor, levar a conflitos e até impedir que alguns aplicativos sejam executados no servidor. As exclusões ajudam a reduzir o risco de possíveis conflitos e aumentam o desempenho geral do servidor ao executar o software antivírus.

O ESET Mail Security identifica aplicativos críticos de servidor e arquivos do sistema operacional do servidor e os adiciona automaticamente à lista de Exclusões. Após a adição, o processo/aplicativo do servidor pode ser ativado (por padrão) marcando-se a opção apropriada, ou desativado desmarcando-a, com o seguinte resultado:

1) Se uma exclusão de aplicativo/sistema operacional permanecer ativada, qualquer de seus arquivos e pastas críticos será adicionado à lista de arquivos excluídos do rastreamento (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões**). Sempre que o servidor for reiniciado, o sistema realiza uma verificação automática das exclusões e restaura quaisquer exclusões que possam ter sido excluídas da lista. Esta é a configuração recomendada se quiser garantir que as Exclusões automáticas recomendadas sejam sempre aplicadas.

2) Se um usuário desativar uma exclusão de aplicativo/sistema operacional, seus arquivos e pastas críticos permanecerão na lista de arquivos excluídos do rastreamento (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões**). No entanto, eles não serão verificados ou renovados automaticamente na lista **Exclusões** sempre que o servidor for reiniciado (veja o ponto 1 acima). Recomendamos esta configuração para usuários avançados, que desejam remover ou alterar algumas exclusões padrão. Se quiser remover as exclusões da lista sem reiniciar o servidor, você precisará removê-las manualmente da lista (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões)**.

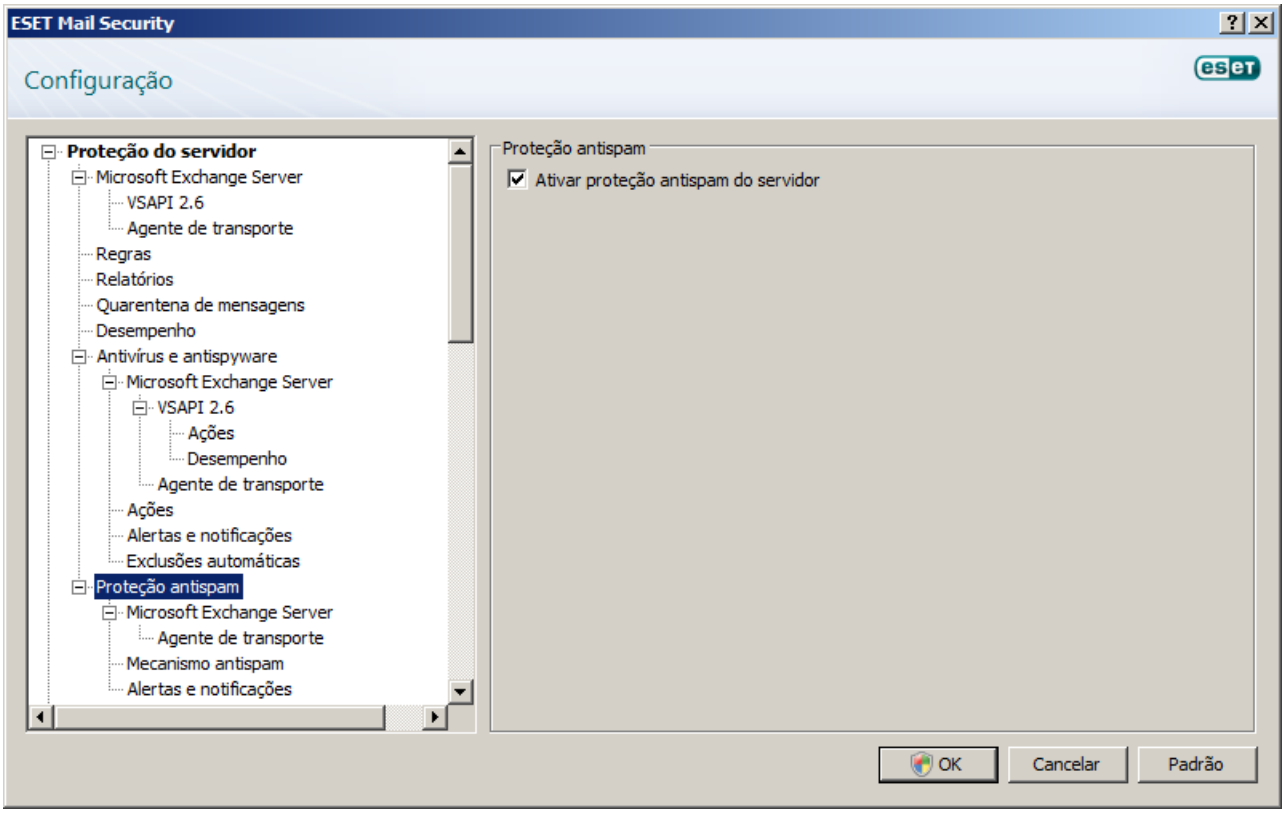
Nenhuma exclusão definida pelo usuário e inserida manualmente em **Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões** será afetada pelas configurações descritas anteriormente.

As Exclusões automáticas de aplicativos/sistemas operacionais do servidor são selecionadas com base nas recomendações da Microsoft. Para obter detalhes, consulte os seguintes links:

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

3.3 Proteção antispam

Na seção **Proteção antispam**, é possível ativar ou desativar a proteção contra spam para o servidor de email instalado, configurar os parâmetros do mecanismo antispam e definir outros níveis de proteção.



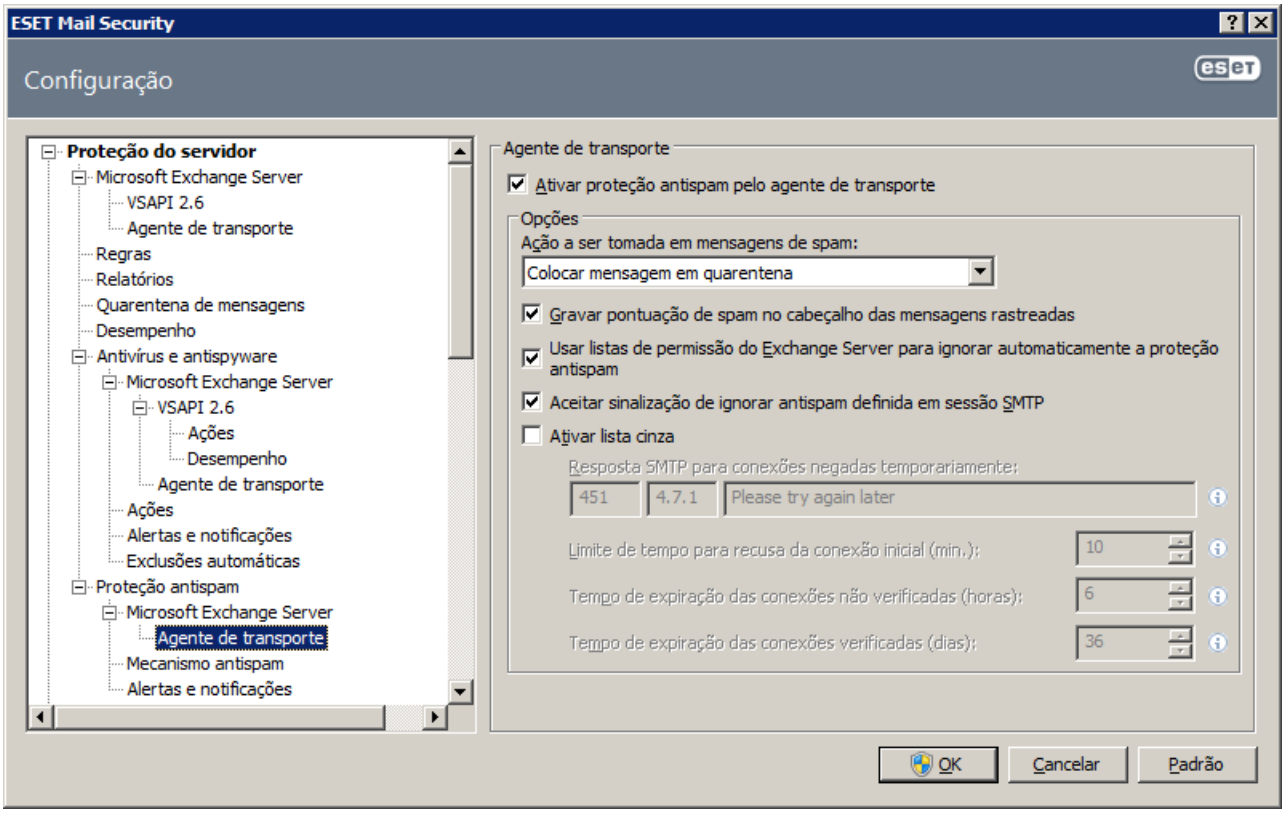
OBSERVAÇÃO: É necessário que o banco de dados Antispam seja atualizado regularmente para que o módulo Antispam forneça a melhor proteção possível. Para permitir atualizações regulares corretas do banco de dados Antispam, você precisará se certificar de que o ESET Mail Security tenha acesso a endereços IP específicos em portas específicas. Para obter mais informações sobre quais IPs e portas permitir em seu firewall de terceiros, leia este artigo da KB.

OBSERVAÇÃO: Além disso, imagens 89 não podem ser usadas para atualizações de banco de dados Antispam. Para o funcionamento adequado de atualizações de banco de dados Antispam, o ESET Mail Security precisa ter acesso a endereços IP relacionados no artigo da KB mencionado anteriormente. Sem acesso a esses IPs, o módulo Antispam não poderá fornecer os resultados mais precisos; portanto, a melhor proteção possível.

3.3.1 Microsoft Exchange Server

3.3.1.1 Agente de transporte

Nesta seção é possível configurar as opções de proteção contra spam usando o agente de transporte.



OBSERVAÇÃO: O agente de transporte não está disponível no Microsoft Exchange Server 5.5.

Ao **Ativar proteção antispam pelo agente de transporte** , é possível escolher uma das seguintes opções como em **Ação a ser tomada em mensagens de spam**:

- **Manter mensagem** – mantém a mensagem mesmo que ela esteja marcada como spam
- **Colocar mensagem em quarentena** – envia uma mensagem marcada como spam para a caixa de correio de quarentena
- **Excluir mensagem** – exclui uma mensagem marcada como spam

Se desejar incluir informações sobre a pontuação de spam da mensagem no cabeçalho, ative a opção **Gravar pontuação de spam no cabeçalho das mensagens rastreadas**.

A função **Usar as listas de permissão do Exchange Server para ignorar automaticamente proteção antispam** permite que o ESET Mail Security use "listas de permissão" do Exchange específicas. Quando ativada, o seguinte é levado em consideração:

- O envio do endereço IP do servidor está ativado na lista Permitir IP do Exchange Server
- O destinatário da mensagem tem o sinalizador Ignorar antispam definido como ativo em sua caixa de correio
- O destinatário da mensagem tem o endereço do remetente na Lista de remetentes seguros (certifique-se de que você tenha configurado a Sincronização da lista de remetentes seguros em seu ambiente do Exchange Server, incluindo Agregação da lista segura)

Se qualquer um dos acima se aplicar a uma mensagem recebida, a verificação antispam será omitida para essa mensagem, mas a mensagem não será avaliada quanto a SPAM e será entregue na caixa de correio do destinatário.

A opção **Aceitar sinalizador de ignorar antispam definidona sessão SMTP** é útil quando você tem sessões SMTP entre servidores Exchange com a configuração de ignorar antispam. Por exemplo, quando você tiver um servidor de Edge e um servidor de Hub, não há necessidade de rastreamento antispam do tráfego entre esses dois servidores. A opção **Aceitar sinalizador de ignorar antispam definidona sessão SMTP** está ativada por padrão e se aplica quando há sinalizador de ignorar antispam configurado para a sessão SMTP no Exchange Server. Se você desativar a opção **Aceitar sinalizador de ignorar antispam definidona sessão SMTP** ao desmarcar a caixa de seleção, o ESET Mail Security rastreará a sessão SMTP quanto a spam ignorando a configuração de ignorar antispam do Exchange

Server.

A função **Ativar lista cinza** ativa um recurso que protege os usuários contra spam usando a seguinte técnica: O agente de transporte enviará o valor de retorno SMTP "rejeitar temporariamente" (o padrão é 451/4.7.1) para qualquer email recebido que não seja de um remetente reconhecido. Um servidor legítimo tentará reenviar a mensagem após um atraso. Os servidores de spam normalmente não tentam reenviar a mensagem, pois costumam passar por milhares de endereços de email e não perdem tempo com reenvio. A Lista cinza é uma camada adicional de proteção antispam e não tem efeito sobre as capacidades de avaliação de spam do módulo antispam.

Ao avaliar a origem da mensagem, o método leva em consideração as configurações da lista **Endereços IP aprovados**, da lista **Endereços IP ignorados**, das listas **Remetentes seguros** e **Permitir IP** no Exchange Server e as configurações de AntispamBypass da caixa de correio do destinatário. Os emails desses endereços IP/listas de remetentes ou emails entregues a uma caixa de correio que tem a opção AntispamBypass ativada serão ignorados pelo método de detecção de lista cinza.

O campo **Resposta SMTP para conexões negadas temporariamente** define a resposta de recusa SMTP temporária enviada ao servidor SMTP se uma mensagem for recusada.

Exemplo de mensagem de resposta SMTP:

Código de resposta primária	Código de status complementar	Descrição
451	4.7.1	Ação solicitada anulada: erro local no processamento

Alerta: A sintaxe incorreta nos códigos de resposta SMTP pode causar mau funcionamento da proteção de lista cinza. Como resultado, as mensagens de spam podem ser entregues aos clientes ou as mensagens podem não ser entregues.

Limite de tempo para recusa da conexão inicial (min.) – quando uma mensagem é entregue pela primeira vez e é negada temporariamente, esse parâmetro define o período de tempo durante o qual a mensagem será sempre negada (medido a partir da primeira vez que é negada). Após o período definido ter decorrido, a mensagem será recebida com êxito. O valor mínimo que pode ser inserido é de 1 minuto.

Tempo de expiração das conexões não verificadas (horas) – esse parâmetro define o intervalo de tempo mínimo no qual os dados do trio serão armazenados. Um servidor válido deve reenviar uma mensagem desejada antes que esse período expire. Esse valor deve ser superior ao valor do **Limite de tempo para recusa da conexão inicial**.

Tempo de expiração das conexões verificadas (dias) – o número mínimo de dias em que as informações do trio serão armazenadas, durante o qual os emails de um remetente específico serão recebidos sem atraso. Esse valor deve ser superior ao valor de **Tempo de expiração das conexões não verificadas**.

OBSERVAÇÃO: Também é possível usar variáveis do sistema ao definir a resposta de rejeição SMTP.

3.3.1.2 Conector POP3 e antispam

O Microsoft Windows versão Small Business Server (SBS) inclui um Conector POP3 que permite que o servidor busque e-mails de servidores POP3 externos. A implementação deste Conector POP3 "padrão" difere de uma versão SBS para outra.

O ESET Mail Security suporta o Conector Microsoft SBS POP3 no SBS 2008 e as mensagens obtidas por download via este Conector POP3 são rastreadas quanto à presença de spam. Isso funciona porque as mensagens estão sendo transportadas para o Microsoft Exchange via SMTP. Porém o Conector Microsoft SBS POP3 no SBS 2003 não é suportada pelo ESET Mail Security, portanto as massagens não são rastreadas em busca de spam. Isso ocorre porque as mensagens ignoram a fila do SMTP.

Existem também uma série de Conectores POP3 de terceiros. Se as mensagens buscados através de certo Conector POP3 são rastreadas em busa de spam ou não depende do método real que este Conector POP está usando para buscar mensagens. Por exemplo, o GFI POP2Exchange transporta mensagens via Diretório de recebimento, portanto as mensagens não são rastreadas em busca de spam. Problemas semelhantes podem aparecer com produtos que transportam mensagens através de sessão autenticada (como o IGetMail) ou quando o Microsoft Exchange marca essas mensagens como internas para as quais o antispam é ignorado por padrão. Esta configuração pode ser alterada no arquivo de configuração. Exportar configuração em xml, alterar `AgentASScanSecureZone` valor da configuração para `"1"` e importar a configuração novamente (para mais informações

sobre como importar e exportar arquivos de configuração consulte o capítulo configurações de exportação e importação 128). Também é possível tentar desativar **Aceitar o sinalizador de desvio de antispam configurado na sessão SMTP** em F5 na árvore de configuração avançada em **Proteção do servidor > Proteção antispam > Microsoft Exchange Server > Agente de transporte**. Ao fazer isso, o ESET Mail Security rastreará a sessão SMTP em busca de spam ignorando a configuração de ignorar antispam do Exchange Server.

3.3.2 Mecanismo antispam

Aqui, é possível configurar os parâmetros do **Mecanismo antispam**. Para isso, clique no botão **Configurar...** Uma janela será exibida e você poderá configurar esses Parâmetros do Mecanismo antispam.

Categorização de mensagens

O Mecanismo antispam do ESET Mail Security atribui uma pontuação de spam de 0 a 100 para cada mensagem rastreada. Ao alterar os limites de pontuação de spam nessa seção, é possível influenciar:

1) se a mensagem será classificada como SPAM ou NÃO SPAM. Todas as mensagens com pontuação de spam igual ou superior ao valor da **Pontuação de spam para tratar uma mensagem como spam:** serão consideradas SPAM. Como consequência, as ações definidas noAgente de transporte 38 serão aplicadas a essas mensagens.
2) se uma mensagem for registrada no relatório antispam 96 (**Ferramentas** > **Relatórios** > **Antispam**). Todas as mensagens com pontuação de spam igual ou superior ao valor do **Limite de pontuação de spam para tratar uma mensagem como provável spam ou provável limpa:** serão registradas pelo relatório.
3) em qual seção das estatísticas antispam, a mensagem em questão será contada (**Status da proteção > Estatísticas > Proteção antispam do servidor de email**):

Mensagens classificadas como SPAM – a pontuação de spam da mensagem é igual ou superior ao valor definido para **Pontuação de spam para tratar uma mensagem como spam:**

Mensagens classificadas como provavelmente SPAM: – a pontuação de spam da mensagem é igual ou superior ao valor definido para **Limite de pontuação de spam para tratar uma mensagem como provável spam ou provável limpa:**

Mensagens classificadas como provavelmente NÃO SPAM – a pontuação de spam da mensagem é igual ou inferior ao valor definido para **Limite de pontuação de spam para tratar uma mensagem como provável spam ou provável limpa:**

Mensagens classificadas como NÃO SPAM – a pontuação de spam da mensagem é igual ou inferior ao valor definido para **Pontuação de spam para tratar uma mensagem como não spam:**

3.3.2.1 Configuração dos parâmetros do mecanismo antispam

3.3.2.1.1 Análise

Nesta seção, é possível configurar como as mensagens são analisadas quanto a SPAM e subsequentemente processadas.

Rastrear anexos de mensagens - Essa opção permite que você escolha se o mecanismo antispam rastreará e considerará anexos ao computador a pontuação de spam.

Usar ambas seções MIME - O mecanismo antispam analisará seções MIME de texto/sem formatação e texto/html em uma mensagem. Se for desejado desempenho adicional, é possível analisar somente uma seção. Se essa opção estiver desmarcada (desativada), então somente uma seção será analisada.

Tamanho da memória para cálculo de pontuação (em bytes): - Essa opção instrui o mecanismo antispam para não ler mais do que um número configurável de bytes do buffer da mensagem ao processar regras.

Tamanho da memória para cálculo de amostra (em bytes): - Essa opção instrui o mecanismo antispam para não ler mais do que os bytes definidos ao computar a impressão digital da mensagem. Isso é útil ao obter impressões digitais consistentes.

Usar memória de cache LegitRepute - Ativa o uso de um cache LegitRepute para reduzir falsos-positivos, especialmente para boletins informativos.

Converter em UNICODE - Aprimora a precisão e produção para corpos de mensagem de email em Unicode, especialmente idiomas de duplo byte ao converter a mensagem em bytes únicos.

Usar memória em cache de domínio - Ativa o uso de um cache de reputação de domínio. Se ativada, os domínios serão extraídos de mensagens e comparados em relação a um cache de reputação de domínio.

3.3.2.1.1.1 Amostras

Usar memória de cache - Permite o uso de um cache de impressão digital (habilitado por padrão).

Ativar MSF - Permite o uso de um algoritmo de impressão digital alternativo conhecido como MSF. Quando ativado, você poderá definir os seguintes limites:

- **Número de mensagens designando uma mensagem em bloco:** - Essa opção especifica quantas mensagens semelhantes são necessárias para considerar um bloco de mensagens.
- **Frequência de limpeza da memória de cache:** - Essa opção especifica uma variável interna, que determina com que frequência o cache MSF em memória é limpo.
- **Sensibilidade de correspondência de duas amostras:** - Essa opção especifica o limite de percentual de correspondência para duas impressões digitais. Se o percentual de correspondência for superior a esse limite, então as mensagens serão consideradas como sendo as mesmas.
- **Número de amostras armazenadas na memória:** - Essa opção especifica o número de impressões digitais MSF a serem mantidas na memória. Quanto maior for o número, mais memória será usada, mas também maior será a precisão.

3.3.2.1.1.2 SpamCompiler

Ativar SpamCompiler - Agiliza o processamento de regras, mas requer um pouco mais de memória.

Versão preferida: - Especifica qual versão do SpamCompiler usar. Quando definido como **Automático**, o mecanismo antispam escolherá o melhor mecanismo para usar.

Usar memória em cache - Se essa opção for ativada, o SpamCompiler armazenará os dados compilados no disco, em vez de memória para reduzir o uso de memória.

Lista de arquivos de memória em cache: - Essa opção especifica quais arquivos de regras são compilados no disco, em vez de na memória.

Defina índices de arquivos de regra que serão armazenados na memória em cache em disco. Para gerenciar índices de arquivo de regra, é possível:

- **Adicionar...**
- **Editar...**
- **Remover**

OBSERVAÇÃO: Somente números são caracteres aceitáveis.

3.3.2.1.2 Treinamento

Usar treinamento para pontuação de impressão digital de mensagem - Ativa o treinamento de deslocamento da pontuação de impressão digital.

Usar palavras de treinamento - Essa opção controla se a análise token de palavra Bayesian será usada. A precisão pode ser incrivelmente aprimorada, mas mais memória será usada e isso será ligeiramente mais lento.

- **Número de palavras em memória em cache:** - Essa opção especifica o número de tokens de palavra para cache a qualquer momento. Quanto maior for o número, mais memória será usada, mas também maior será a precisão. Para inserir o número, ative primeiro a opção **Usar palavras de treinamento**.

Usar banco de dados de treinamento somente para leitura: - Essa opção controla se os bancos de dados de treinamento de impressão digital, regras e palavra podem ser modificados ou são somente leitura após a carga inicial. Um banco de dados de treinamento somente leitura é mais rápido.

- **Sensibilidade de treinamento automático:** - Defijne um limite para treinamento automático. Se uma mensagem tiver pontuação em ou acima do limite alto, essa mensagem será considerada um spam definitivo e então usada para treinar todos os módulos ativados para Bayesian (regras e/ou palavra) mas não remetente ou impressão digital. Se uma mensagem tiver pontuação em ou abaixo do baixo, essa mensagem será considerada um ham definitivo e então usada para treinar todos os módulos ativados para Bayesian (regras e/ou palavra) mas não remetente ou impressão digital. Para inserir o número de limite alto e baixo, ative primeiro a opção **Usar banco de dados de treinamento somente para leitura:** .

Quantidade mínima de dados de treinamento: - Inicialmente, somente as ponderações de regra serão usadas para computar a pontuação de spam. Assim que um conjunto mínimo de dados de treinamento for atingido, os dados de treinamento de regra/palavra substitui as ponderações de regra. O padrão mínimo é 100, o que significa que ele deverá ser treinado em, pelo menos, 100 mensagens de ham conhecidas equivalentes e 100 mensagens de spam equivalentes para um total de 200 mensagens antes de os dados de treinamento substituírem as ponderações de regra. Se o número for muito baixo, então a precisão pode ser insatisfatória devido a dados insuficientes. Se o número for muito elevado, então os dados de treinamento não serão totalmente aproveitados. Um valor de 0 fará com que as ponderações de regra sempre sejam ignoradas.

Usar somente dados de treinamento - Controla se será fornecida total ponderação para dados de treinamento. Se essa opção for ativada, então a pontuação será exclusivamente com base nos dados de treinamento. Se essa opção for desativada (desmarcada), então os dados de treinamento e regras serão usados.

Número de mensagens verificadas antes de gravá-las em disco: - Durante o treinamento, o mecanismo antispam processará uma quantidade configurável de mensagens antes de gravar o banco de dados de treinamento em disco. Essa opção determinará quantas mensagens processar antes de gravar em disco. Para o máximo desempenho, esse número deverá ser o maior possível. Em um caso incomum quando um programa for inesperadamente encerrado antes de o buffer ser gravado em disco, o treinamento realizado desde a última gravação em disco será perdido. O buffer será gravado em disco no término normal.

Usar dados de país para treinamento - Controla se as informações de roteamento de país devem ser consideradas no treinamento e pontuação de mensagens.

3.3.2.1.3 Regras

Usar regras - Essa opção controla se regras heurísticas mais lentas serão usadas. A precisão pode ser incrivelmente aprimorada, mas mais memória será usada e isso será mais lento.
- **Usar extensão do conjunto de regras** - Permite a definição de regra estendida.
- **Usar extensão do conjunto de regras** - Permite a segunda extensão na definição de regra.

Ponderação de regras: - Essa opção permite a substituição de ponderações associadas a regras individuais.

Lista de arquivos de regras baixados: - Essa opção especifica quais arquivos de regra são baixados.

Ponderação de categoria: - Permite que o usuário final ajuste as ponderações de categorias usadas em sc18 e em arquivos usados em uma lista de regras personalizadas. Categoria: Nome da categoria, atualmente limitado a SPAM, PHISH, BOUNCE, ADULT, FRAUD, BLANK, FORWARD e REPLY. Esse campo faz distinção de maiúsculas e minúsculas. Pontuação: Qualquer inteiro ou BLOCK ou APPROVE. A ponderação de regras correspondendo à categoria correspondente será multiplicada pelo fator de escala, a fim de produzir uma nova ponderação eficaz.

Lista de regras personalizadas: - Permite que o usuário especifique uma lista de regras personalizadas (p. ex., spam, ham ou palavras/frases de phishing). Os arquivos de regras personalizadas contêm frases no seguinte formato em linhas separadas: frase, tipo, confiança, maiúsculas/minúsculas A frase com distinção de maiúsculas/minúsculas pode ser qualquer texto, exceto vírgulas. Quaisquer vírgulas na frase devem ser excluídas. O tipo pode ser SPAM, PHISH, BOUNCE, ADULT ou FRAUD. Se qualquer outro for especificado, o TYPE será automaticamente assumido como sendo SPAM. A confiança pode ser de 1 a 100. Se o tipo for SPAM, então 100 indica uma confiança superior de menos spam. Se o tipo for PHISH, então 100 indica uma confiança superior de menos roubo de identidade. Se o tipo for BOUNCE, então 100 indica uma confiança superior de que a frase é relacionada a devoluções. Uma confiança superior tem mais probabilidade de afetar a pontuação final. Um valor de 100 é um caso especial. Se o tipo for SPAM, então 100 pontuará a mensagem como 100. Se o tipo for PHISH, então 100 pontuará a mensagem como 100. Se o tipo for BOUNCE, então 100 pontuará a mensagem como 100. Como sempre, qualquer lista de permissão substituirá qualquer lista de proibição. O valor de distinção de maiúsculas/minúsculas de 1 significa que a frase fará distinção de maiúsculas/minúsculas; 0 significa que a frase não fará distinção de maiúsculas/minúsculas. Exemplos:

spam é divertido, SPAM, 100,0
o roubo de identidade é Phun, PHISH, 90,1
devolver ao remetente, BOUNCE, 80,0

A primeira linha significa que todas as variações de "spam é divertido" serão consideradas SPAM com uma confiança de 100. A frase faz distinção de maiúsculas/minúsculas. A segunda linha significa que todas as variações de "roubo de identidade é phun" serão consideradas PHISH com uma confiança de 90. A frase faz distinção de maiúsculas/minúsculas. A terceira linha significa que todas as variações de "devolver ao remetente" serão consideradas BOUNCE com uma confiança de 80. A frase não faz distinção de maiúsculas/minúsculas.

Apagar regras anteriores depois de sua atualização - O mecanismo antispam, por padrão, limpará os arquivos de regras anteriores do diretório de configuração quando um novo arquivo for recuperado da rede SpamCatcher. No entanto, alguns usuários do mecanismo antispam desejarão arquivar regras de arquivos anteriores. Isso pode ser feito desativando esse recurso de limpeza.

Mostrar notificação depois da atualização bem-sucedida de regras -

3.3.2.1.3.1 Ponderação de regras

Defina índices de arquivo de regra e sua ponderação. Para adicionar uma ponderação de regra, pressione o botão **Adicionar...**. Para modificar regras existentes, pressione o botão **Editar...**. Para excluir, pressione o botão **Remover**.

Especifique os valores **Índice:** e **Ponderação:** .

3.3.2.1.3.2 Lista de arquivos de regras baixados

Defina índices de arquivo de regra que devem ser baixados em disco. Use os botões **Adicionar**, **Editar** e **Remover** para gerenciar índices de arquivo de regra.

3.3.2.1.3.3 Ponderação de categoria

Defina categorias de regra e sua ponderação. Use os botões **Adicionar...**, **Editar...** e **Remover** para gerenciar categorias e sua ponderação.

Para adicionar uma ponderação de categoria, selecione uma **Categoria:** da lista. As opções disponíveis são:

- **SPAM**
- **Roubo de identidade**
- **Relatório de não entrega**
- **Mensagens com conteúdo para adultos**
- **Mensagens fraudulentas**
- **Mensagens em branco**
- **Mensagens de encaminhamento**
- **Mensagens de resposta**

Em seguida, selecione uma ação:

- **Permitir**
- **Bloquear**
- **Ponderar:**

3.3.2.1.3.4 Lista de regras personalizadas

É possível usar arquivos de pegras personalizadas que contêm frases. Esses arquivos são basicamente arquivos .txt, para mais detalhes e formatos de frase consulte o tópico Regras 42 (seção **Lista de regras personalizadas**).

Para usar arquivos contendo regras personalizadas que serão usadas para análise de mensagem, é preciso colocá-los no seguinte local:

caso de você opere o Windows Server 2008 ou uma versão mais recente, o caminho é:
C:\ProgramData\ESET\ESET Mail Security\ServerAntispam

no caso do Windows Server 2003 e versões mais antigas, o caminho é:
C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam

Para obter os arquivos carregados pressione o botão **...** (navegar), navegue até o local mencionado acima e selecione o arquivo de texto (*.txt). Use os botões **Adicionar**, **Editar** e **Remover** para gerenciar listas de regras personalizadas.

OBSERVAÇÃO: O arquivo .txt contendo regras personalizadas deve ser colocado na pasta *ServerAntispam*, caso contrário este arquivo não será carregado.

3.3.2.1.4 Filtragem

Nesta seção, é possível configurar listas permitidas, bloqueadas e ignoradas ao especificar critérios, como endereço IP ou intervalo, nome de domínio, endereço de e-mail, etc. Para adicionar, modificar ou remover critérios, basta acessar a lista que deseja gerenciar e clicar no botão apropriado para fazê-lo.

3.3.2.1.4.1 Remetentes permitidos

Os remetentes e domínios na lista de permissões podem conter um endereço de email ou domínio. Os endereços são inseridos no formato "mailbox@domain" e os domínios simplesmente no formato "domain".

OBSERVAÇÃO: O espaço em branco à direita e à esquerda é ignorado, expressões regulares não são compatíveis e o asterisco "*" também é ignorado.

3.3.2.1.4.2 Remetentes bloqueados

Os remetentes e domínios na lista de proibições podem conter um endereço de email ou domínio. Os endereços são inseridos no formato "mailbox@domain" e os domínios simplesmente no formato "domain".

OBSERVAÇÃO: O espaço em branco à direita e à esquerda é ignorado, expressões regulares não são compatíveis e o asterisco "*" também é ignorado.

3.3.2.1.4.3 Endereços IP permitidos

Essa opção permite que você especifique IPs que devem ser aprovados. Os intervalos podem ser especificados de três formas:

a) IP inicial - IP final
b) Endereço IP e máscara da rede
c) Endereço IP

Se o primeiro endereço IP não ignorado nos cabeçalhos Recebidos: corresponder a um endereço nessa lista, a pontuação da mensagem será 0 e nenhuma outra verificação será feita.

3.3.2.1.4.4 Endereços IP ignorados

Essa opção permite que você especifique IPs que devem ser ignorados ao realizar verificações da RBL. O seguinte sempre deve ser implicitamente ignorado:

10.0.0.0/8, 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0

Os intervalos podem ser especificados de três formas:

a) IP inicial - IP final
b) Endereço IP e máscara da rede
c) Endereço IP

3.3.2.1.4.5 Endereços IP bloqueados

Essa opção permite que você especifique IPs que devem ser bloqueados. Os intervalos podem ser especificados de três formas:

a) IP inicial - IP final
b) Endereço IP e máscara da rede
c) Endereço IP

Se um endereço IP nos cabeçalhos Recebidos: corresponder a um endereço nessa lista, a pontuação da mensagem será 100 e nenhuma outra verificação será feita.

3.3.2.1.4.6 Domínios permitidos

Essa opção permite que você especifique domínios de corpo e IPs que sempre devem ser aprovados.

3.3.2.1.4.7 Domínios ignorados

Essa opção permite que você especifique domínios de corpo que sempre devem ser excluídos de verificações da DNSBL e ignorados.

3.3.2.1.4.8 Domínios bloqueados

Essa opção permite que você especifique domínios de corpo e IPs que sempre devem ser bloqueados.

3.3.2.1.4.9 Remetentes falsos

Permite o bloqueio de remetentes de spam que falsificam seu nome de domínio e outros nomes de domínio. Por exemplo, remetentes de spam frequentemente usam o nome de domínio do destinatário como o nome de domínio De: . Essa lista permita que você especifique quais servidores de email têm permissão para usar quais nomes de domínio no endereço De: .

3.3.2.1.5 Verificação

A verificação é um recurso adicional da proteção Antispam. Ela permite que mensagens sejam verificadas através de servidores externos, de acordo com critérios definidos. Escolha uma lista da árvore de configuração para configurar seus critérios. As listas são as seguintes:

- **RBL** (Realtime Blackhole List, Lista de bloqueios em tempo real)
- **LBL** (Last Blackhole List, Lista de últimos bloqueios)
- **DNSBL** (Lista de bloqueio de DNS)

3.3.2.1.5.1 RBL (Realtime Blackhole List, Lista de bloqueios em tempo real)

Servidores da RBL: - Especifica uma lista de servidores da RBL (Realtime Blackhole List, Lista de bloqueios em tempo real) para consulta ao analisar mensagens. Consulte a seção da RBL neste documento para obter mais informações.

Sensibilidade de verificação da RBL: - Com as verificações da RBL podem introduzir latência e uma diminuição em desempenho, essa opção permite a execução de verificação de RBLs condicionalmente com base na pontuação antes das verificações da RBL. - Se a pontuação for superior ao valor "alto", então somente os servidores da RBL que puderão oferecer a pontuação abaixo do valor "alto" serão consultados. Se a pontuação for inferior ao valor "baixo", então somente os servidores da RBL que puderão oferecer a pontuação acima do valor "baixo" serão consultados. Se a pontuação estiver entre "baixo" e "alto", então todos os servidores da RBL serão consultados.

Limite de execução de solicitação da RBL (em segundos): - Essa opção permite a configuração de um limite de tempo máximo para a conclusão de todas as consultas da RBL. As respostas da RBL são usadas somente a partir desses servidores da RBL que responderam em tempo hábil. Se o valor for "O", então nenhum limite de tempo será forçado.

Número máximo de endereços verificados em relação à RBL: - Essa opção permite limitar quantos endereços IP são consultados em relação ao servidor da RBL. Observe que o número total de consultas da RBL será o número de endereços IP nos cabeçalhos Recebidos: (até um máximo de endereços IP de verificação máxima de RBL) multiplicado pelo número de servidores da RBL especificados na lista da RBL. Se o valor for "O", então o número ilimitado de cabeçalhos recebidos será verificado. Observe que IPs que correspondem em relação à opção de lista de IP ignorado não contam em relação ao limite de endereços IP da RBL.

Para gerenciar a lista, use os botões **Adicionar...**, **Editar...** ou **Remover**.

A lista consiste em três colunas:

Endereço
Resposta
Pontuação

3.3.2.1.5.2 LBL (Last Blackhole List, Lista de últimos bloqueios)

Servidores da LBL: - O IP da última conexão é consultado em relação ao servidor da LBL. Você pode especificar uma busca de DNS diferente para o IP de entrada da última conexão. Para o IP de entrada da última conexão, a lista de LBL é consultada, em vez da lista de RBL. Caso contrário, as opções da lista de LBL, como limite, também serão aplicadas à lista de LBL.

Endereços IP não verificados em relação à LBL: - Se o IP da última conexão corresponder a um IP na lista, então esse IP seria consultado em relação aos servidores da RBL em vez de servidores da LBL.

Para gerenciar a lista, use os botões **Adicionar...**, **Editar...** ou **Remover**.

A lista consiste em três colunas:

Endereço
Resposta
Pontuação

Aqui, você pode especificar endereços IP que serão verificados em relação à LBL. Para gerenciar a lista, use os botões **Adicionar...**, **Editar...** ou **Remover**.

3.3.2.1.5.3 DNSBL (Lista de bloqueio de DNS)

Servidores da DNSBL: - Especifica uma lista de servidores da Lista de bloqueio de DNS (DNSBL) para consulta com domínios e IPs extraídos do corpo da mensagem.

Sensibilidade de verificação da DNSBL: - Se a pontuação for superior ao valor "alto", então somente os servidores da DNSBL que puderão oferecer a pontuação abaixo do valor "alto" serão consultados. Se a pontuação for inferior ao valor "baixo", então somente os servidores da DNSBL que puderão oferecer a pontuação acima do valor "baixo" serão consultados. Se a pontuação estiver entre "baixo" e "alto", então todos os servidores da DNSBL serão consultados.

Limite de execução de solicitação da DNSBL (em segundos): - Permite a configuração de um limite de tempo máximo para a conclusão de todas as consultas da DNSBL.

Número máximo de domínios verificados em relação à DNSBL: - Permite a limitação de quantos domínios e IPs são consultados em relação ao servidor da Lista de Bloqueio de DNS.

Para gerenciar a lista, use os botões **Adicionar...**, **Editar...** ou **Remover**.

A lista consiste em três colunas:

Endereço
Resposta
Pontuação

3.3.2.1.6 DNS

Usar memória de cache - Ativa o cache interno de solicitações de DNS.

Número de solicitações de DNS armazenadas na memória: - Limita o número de entradas no cache DNS interno.

Salvar memória de cache em risco - Se ativada, o cache DNS armazenará entradas em disco no desligamento e lerá do disco na inicialização.

Endereço de servidor DNS: - Os servidores DNS agora podem ser explicitamente especificados para substituir o padrão.

Acesso DNS direto: - Quando definido como sim e se o servidor DNS não estiver especificado, o mecanismo antispam fará as solicitações LiveFeed diretamente nos servidores LiveFeed. Essa opção será ignorada se o servidor

DNS for especificado, pois ele tem precedência. Essa opção deve ser definida como **Sim** quando consultas diretas forem mais eficientes do que os servidores DNS padrão.

Tempo de vida de solicitação DNS (em segundos): - Essa opção permite configurar um TTL mínimo para entradas no cache DNS interno do mecanismo antispam. A opção é especificada em segundos. Para as respostas DNS cujo valor TTL seja inferior ao TTL mínimo especificado, o cache interno do mecanismo antispam usará o TTL especificado, em vez do valor TTL da resposta DNS.

3.3.2.1.7 Pontuação

Ativar o histórico de pontuação - Ativa o rastreamento de pontuações históricas para remetentes repetidos.

Parar análise quando o limite de pontuação de SPAM for atingido - Essa opção permite que você diga ao mecanismo antispam para parar de analisar a mensagem assim que uma pontuação for atingida. Isso pode reduzir o número de regras e outras verificações que são realizadas, melhorando assim a produção.

Usar análise acelerada antes de a pontuação de limite para uma mensagem limpa ser atingida - Essa opção permite que você diga ao mecanismo antispam para ignorar verificações lentas de regra se a mensagem provavelmente for ham.

Categorização de mensagens

- **Valor de pontuação do qual uma mensagem é ignorada como SPAM:** - O mecanismo antispam atribui à mensagem verificada uma pontuação de 0 a 100. Definir os limites do valor de pontuação afeta quais mensagens são consideradas SPAM e quais mensagens não são. Se você definir valores incorretos, isso poderá diminuir a qualidade dos resultados de detecção do mecanismo antispam.
- **O valor de pontuação que define um limite quando uma mensagem é considerada como provável SPAM ou provavelmente limpa:** - O mecanismo antispam atribui à mensagem verificada uma pontuação de 0 a 100. Definir os limites do valor de pontuação afeta quais mensagens são consideradas SPAM e quais mensagens não são. Se você definir valores incorretos, isso poderá diminuir a qualidade dos resultados de detecção do mecanismo antispam.
- **O valor de pontuação até o qual uma mensagem será considerada como certamente limpa:** - O mecanismo antispam atribui à mensagem verificada uma pontuação de 0 a 100. Definir os limites do valor de pontuação afeta quais mensagens são consideradas SPAM e quais mensagens não são. Se você definir valores incorretos, isso poderá diminuir a qualidade dos resultados de detecção do mecanismo antispam.

3.3.2.1.8 Spambait

Endereços de spam: - Se o endereço RCPT TO: do envelope SMTP corresponder a um endereço de email nessa lista, então o arquivo de estatísticas registrará tokens em mensagem de email como sendo enviados para um endereço spambait. Os endereços devem corresponder exatamente, não será compatível ignorar entradas de caractere curinga e em maiúsculas/minúsculas.

Endereços considerados como não existentes: - Se o endereço RCPT TO: do envelope SMTP corresponder a um endereço de email nessa lista, então o arquivo de estatísticas registrará tokens em mensagem de email como sendo enviados para um endereço não existente. Os endereços devem corresponder exatamente, não será compatível ignorar entradas de caractere curinga e em maiúsculas/minúsculas.

3.3.2.1.8.1 Endereços Spambait

Você pode definir endereços de email que receberão somente SPAM. Para adicionar um endereço de email, digite-o no formato padrão e pressione o botão **Adicionar**. Para modificar um endereço de email existente, use o botão **Editar**. Para excluir, pressione o botão **Remover**.

3.3.2.1.8.2 Endereços considerados como não existentes

É possível definir endereços de email que serão exibidos como não existentes para o exterior. Para adicionar um endereço de email, digite-o no formato padrão e pressione o botão **Adicionar**. Para modificar um endereço de email existente, use o botão **Editar**. Para excluir, pressione o botão **Remover**.

3.3.2.1.9 Comunicação

Duração de solicitação única de SpamLabs (em segundos): - Limite quanto tempo poderá demorar uma única solicitação para SpamLabs de proteção Antispam. O valor é especificado em unidades de segundos integrais. O valor de "0" desativa esse recurso e não haverá limite.

Usar protocolo v.4x: - Comunique-se com o SpamLabs de proteção Antispam para determinar a pontuação via protocolo v4.x anterior. Quando você definir essa opção como **Automaticamente**, ela permitirá que o mecanismo Antispam use automaticamente o recurso netcheck como um fallback para consultas LiveFeed.

- **Intervalo de uso de protocolo v4.x:** - Com as redes podem introduzir latência e uma diminuição em desempenho, essa opção permite a execução de verificações de rede condicionalmente com base na pontuação. A rede é consultada somente se a pontuação estiver em ou entre o intervalo "baixo" e "alto" especificado com essa opção.

Endereço de servidor LiveFeed: - Especifica qual servidor consultar para solicitações LiveFeed.

Tempo de vida de solicitação LiveFeed (em segundos): - Essa opção permite configurar um TTL mínimo para entradas no cache LiveFeed interno do mecanismo antispam. A opção é especificada em segundos. Para as respostas LiveFeed cujo valor TTL seja inferior ao TTL mínimo especificado, o cache interno do mecanismo antispam usará o TTL especificado, em vez do valor TTL da resposta LiveFeed.

Tipo de autenticação de servidor proxy: - Especifica qual tipo de autenticação proxy HTTP deve ser usado.

3.3.2.1.10 Desempenho

Tamanho máximo da pilha de encadeamento usada: - Define o tamanho máximo da pilha de encadeamento a ser usada. Se o tamanho da pilha de encadeamento for definido como 64 KB, então essa variável deverá ser definida como 100 ou menos. Se o tamanho da pilha de encadeamento for definido como superior a 1 MB, então essa variável deverá ser definida como 10.000 ou menos. Se essa variável estiver abaixo de 200, a precisão poderá ser reduzida em alguns percentuais.

Produção necessária (em mensagens por segundo): - Essa opção permite que você especifique a produção desejada em mensagens por segundo. O mecanismo antispam tentará atingir esse nível ao otimizar as regras que são executadas. É possível que a precisão possa ser reduzida. Um valor de 0 desativa a opção.

Ingressar arquivos incrementais em um - O mecanismo antispam, por padrão, mesclará vários arquivos incrementais e um arquivo completo em um único arquivo completo atualizado. Isso é feito para reduzir o volume de arquivos no diretório de configuração.

Baixar somente arquivos incrementais - O mecanismo antispam, por padrão, tentará baixar a combinação de tamanho mais eficiente de arquivo completo e incremental. O mecanismo antispam poderá ser forçado a baixar o arquivo incremental ao definir essa opção como sim.

Tamanho máximo de arquivos incrementais: - Para reduzir o uso de CPU enquanto os arquivos de regra são atualizados, os arquivos de cache em disco (sc*.tmp) não serão mais gerados novamente em cada atualização de regra individual. Em vez de serem gerados novamente quando há um arquivo sc*.bin.full mais recente ou quando a soma do sc*.bin.incr vai além do número de bytes especificados no tamanho máximo de arquivos incrementais.

Localização de arquivos temporários: - Esse parâmetro controla onde o mecanismo antispam criará arquivos temporários.

3.3.2.1.11 Configurações regionais

Lista de idiomas residenciais: - Essa opção permite que você defina idiomas que são preferidos em suas mensagens de email. Os códigos de país são códigos de idioma ISO-639 de dois caracteres.

Lista de países de residência: - Essa opção permite especificar uma lista de países que são considerados países "de residência". As mensagens roteadas através de um país que não está na lista serão pontuadas mais agressivamente. Se essa opção estiver vazia, então nenhuma penalidade ocorrerá.

Lista de países bloqueados: - Permite o bloqueio por país. Se um endereço IP em um cabeçalho recebido corresponder a um país relacionado no email será considerado SPAM. Os códigos de país não são aplicados aos endereços de remetente. Observe que é possível que uma mensagem passe por vários países antes de chegar ao destino final. Além disso, essa opção é somente 98% precisa; portanto, bloquear países poderá resultar em falso-positivos.

Lista de conjuntos de caracteres bloqueados: - Permite o bloqueio por conjunto de caracteres. O valor de pontuação de SPAM padrão é definido como 100, mas você pode ajustá-lo para cada conjunto de caracteres bloqueado separadamente. Observe que mapeamento de idioma no conjunto de caracteres não é 100% preciso; portanto, o bloqueio de conjuntos de caracteres pode resultar em falso-positivos.

3.3.2.1.11.1 Lista de idiomas nacionais

Defina idiomas que você considera como idiomas maternos nos quais você prefere receber mensagens. Para adicionar um idioma materno, selecione-o da coluna **Código de idioma:** e pressione o botão **Adicionar**. Isso moverá o idioma para a coluna **Idiomas "maternos"**. Para remover o idioma da coluna **Idiomas "maternos"**, selecione o código de idioma e pressione o botão **Remover**.

Bloquear idiomas não maternos: - Essa opção controla se os idiomas, que não estão relacionados na coluna "Materno", serão ou não bloqueados. Há três opções:

- **Sim**
- **Não**
- **Automaticamente**

Lista de códigos de idioma (com base em ISO 639):

Africâner	af
Amárico	am
Árabe	ar
Bielorrusso	be
Búlgaro	bg
Catalão	ca
Tcheco	cs
Galês	cy
Dinamarquês	da
Alemão	de
Grego	el
Inglês	en
Esperanto	eo
Espanhol	es
Estoniano	et
Basco	eu
Persa	fa
Finlandês	fi
Francês	fr
Frísico	fy
Irlandês	ga
Gaélico	gd
Hebraico	he
Híndi	hi
Croata	hr
Húngaro	hu
Armênio	hy
Indonésio	id

Islandês	is
Italiano	it
Japonês	ja
Georgiano	ka
Coreano	ko
Latim	la
Lituano	lt
Letão	lv
Marati	mr
Malaio	ms
Nepalês	ne
Holandês	nl
Norueguês	no
Polonês	pl
Português	pt
Quíchua	qu
Romanche	rm
Romeno	ro
Russo	ru
Sânscrito	sa
Escocês	sco
Eslovaco	sk
Esloveno	sl
Albanês	sq
Sérvio	sr
Sueco	sv
Quissuaíle	sw
Tâmil	ta
Tailandês	th
Filipino	tl
Turco	tr
Ucraniano	uk
Vietnamita	vi
Ídiche	yi
Chinês	zh

3.3.2.1.11.2 Lista de países de residência

Defina países que você considera como países de residência e dos quais você prefere receber mensagens. Para adicionar um país residencial, selecione-o da coluna **Código de país:** e pressione o botão **Adicionar**. Isso moverá o país para a coluna **Países "residenciais"**. Para remover o país da coluna **Países "residenciais"**, selecione o código de país e pressione o botão **Remover**.

Lista de códigos de país (com base em ISO 3166):

AFEGANISTÃO	AF
ILHAS ÅLAND	AX
ALBÂNIA	AL
ARGÉLIA	DZ
SAMOA AMERICANA	AS
ANDORRA	AD
ANGOLA	AO
ANGUILA	AI
ANTÁRTIDA	AQ
ANTÍGUA E BARBUDA	AG
ARGENTINA	AR
ARMÊNIA	AM
ARUBA	AW
AUSTRÁLIA	AU
ÁUSTRIA	AT
AZERBAIJÃO	AZ
BAHAMAS	BS
BAHREIN	BH
BANGLADESH	BD

BARBADOS	BB
BELARUS	BY
BÉLGICA	BE
BELIZE	BZ
BENIN	BJ
BERMUDA	BM
BUTÃO	BT
BOLÍVIA	BO
BÓSNIA E HERZEGOVINA	BA
BOTSUANA	BW
ILHA BOUVET	BV
BRASIL	BR
TERRITÓRIO BRITÂNICO DO OCEANO ÍNDICO	IO
BRUNEI DARUSSALAM	BN
BULGÁRIA	BG
BURQUINA FASO	BF
BURUNDI	BI
CAMBOJA	KH
CAMARÕES	CM
CANADÁ	CA
CABO VERDE	CV
ILHAS CAYMAN	KY
REPÚBLICA CENTRO-AFRICANA	CF
CHADE	TD
CHILE	CL
CHINA	CN
ILHA CHRISTMAS	CX
ILHAS COCOS (KEELING)	CC
COLÔMBIA	CO
ILHAS COMORES	KM
CONGO	CG
CONGO, A REPÚBLICA DEMOCRÁTICA DO	CD
ILHAS COOK	CK
COSTA RICA	CR
CÔTE D'IVOIRE	CI
CROÁCIA	HR
CUBA	CU
CHIPRE	CY
REPÚBLICA TCHECA	CZ
DINAMARCA	DK
DJIBUTI	DJ
DOMINICA	DM
REPÚBLICA DOMINICANA	DO
EQUADOR	EC
EGITO	EG
EL SALVADOR	SV
GUINÉ EQUATORIAL	GQ
ERITREIA	ER
ESTÔNIA	EE
ETIÓPIA	ET
ILHAS FALKLAND (MALVINAS)	FK
ILHAS FAROÉS	FO
FIJI	FJ
FINLÂNDIA	FI
FRANÇA	FR
GUIANA FRANCESA	GF
POLINÉSIA FRANCESA	PF
TERRITÓRIOS AUSTRAIS FRANCESES	TF
GABÃO	GA
GÂMBIA	GM
GEÓRGIA	GE

ALEMANHA	DE
GANA	GH
GIBRALTAR	GI
GRÉCIA	GR
GROENLÂNDIA	GL
GRANADA	GD
GUADALUPE	GP
GUAM	GU
GUATEMALA	GT
GUINÉ	GN
GUINÉ-BISSAU	GW
GUIANA	GY
HAITI	HT
ILHA HEARD E ILHAS MCDONALD	HM
SANTA SÉ (CIDADO DO VATICANO)	VA
HONDURAS	HN
HONG KONG	HK
HÚNGRIA	HU
ISLÂNDIA	IS
ÍNDIA	IN
INDONÉSIA	ID
IRÃ, REPÚBLICA ISLÂMICA DO	IR
IRAQUE	IQ
IRLANDA	IE
ISRAEL	IL
ITÁLIA	IT
JAMAICA	JM
JAPÃO	JP
JORDÂNIA	JO
CAZAQUISTÃO	KZ
QUÊNIA	KE
KIRIBATI	KI
COREIA, REPÚBLICA DEMOCRÁTICA POPULAR DA	KP
COREIA, REPÚBLICA DA	KR
KUWAIT	KW
QUIRGUISTÃO	KG
REPÚBLICA DEMOCRÁTICA POPULAR DO LAO	LA
LETÔNIA	LV
LÍBANO	LB
LESOTO	LS
LIBÉRIA	LR
JAMAHIRIYA ÁRABE DA LÍBIA	LY
LIECHTENSTEIN	LI
LITUÂNIA	LT
LUXEMBURGO	LU
MACAO	MO
MACEDÔNIA, ANTIGA REPÚBLICA IUGOSLAVA DA	MK
MADAGASCAR	MG
MALAUI	MW
MALÁSIA	MY
MALDIVAS	MV
MALI	ML
MALTA	MT
ILHAS MARSHALL	MH
MARTINICA	MQ
MAURITÂNIA	MR
MAURÍCIO	MU
MAYOTTE	YT
MÉXICO	MX

MICRONÉSIA, ESTADOS FEDERADOS DA	FM
MOLDOVA, REPÚBLICA DA	MD
MÔNACO	MC
MONGÓLIA	MN
MONTSERRAT	MS
MARROCOS	MA
MOÇAMBIQUE	MZ
MYANMAR	MM
NAMÍBIA	NA
NAURU	NR
NEPAL	NP
PAÍSES BAIXOS	NL
ANTILHAS HOLANDESAS	AN
NOVA CALEDÔNIA	NC
NOVA ZELÂNDIA	NZ
NICARÁGUA	NI
NÍGER	NE
NIGÉRIA	NG
NIUE	NU
ILHA NORFOLK	NF
ILHAS MARIANAS DO NORTE	MP
NORUEGA	NO
OMÃ	OM
PAQUISTÃO	PK
PALAU	PW
TERRITÓRIO PALESTINO, OCUPADO	PS
PANAMÁ	PA
PAPUA-NOVA GUINÉ	PG
PARAGUAI	PY
PERU	PE
FILIPINAS	PH
PITCAIRN	PN
POLÔNIA	PL
PORTUGAL	PT
PORTO RICO	PR
CATAR	QA
REUNIÃO	RE
ROMÊNIA	RO
FEDERAÇÃO RUSSA	RU
RUANDA	RW
SANTA HELENA	SH
SÃO CRISTÓVÃO E NÉVIS	KN
SANTA LÚCIA	LC
SÃO PEDRO E MIQUELON	PM
SÃO VICENTE E GRANADINAS	VC
SAMOA	WS
SÃO MARINHO	SM
SÃO TOMÉ E PRÍNCIPE	ST
ARÁBIA SAUDITA	SA
SENEGAL	SN
SÉRVIA E MONTENEGRO	CS
SEICHELES	SC
SERRA LEOA	SL
CINGAPURA	SG
ESLOVÁQUIA	SK
ESLOVÊNIA	SI
ILHAS SALOMÃO	SB
SOMÁLIA	SO
ÁFRICA DO SUL	ZA
ILHAS GEÓRGIA DO SUL E SANDWICH DO SUL	GS
ESPANHA	ES

SRI LANKA	LK
SUDÃO	SD
SURINAME	SR
SVALBARD E JAN MAYEN	SJ
SUAZILÂNDIA	SZ
SUÉCIA	SE
SUÍÇA	CH
REPÚBLICA ÁRABE DA SÍRIA	SY
TAIWAN, PROVÍNCIA DA CHINA	TW
TADJIQUISTÃO	TJ
TANZÂNIA, REPÚBLICA UNIDA DA	TZ
TAILÂNDIA	TH
TIMOR-LESTE	TL
TOGO	TG
TOKELAU	TK
TONGA	TO
TRINIDAD E TOBAGO	TT
TUNÍSIA	TN
TURQUIA	TR
TURCOMENISTÃO	TM
ILHAS TURCOS E CAICOS	TC
TUVALU	TV
UGANDA	UG
UCRÂNIA	UA
EMIRADOS ÁRABES UNIDOS	AE
REINO UNIDO	GB
ESTADOS UNIDOS	US
TERRITÓRIOS INSULARES DOS ESTADOS UNIDOS	UM
URUGUAI	UY
UZBEQUISTÃO	UZ
VANUATU	VU
CIDADO DO VATICANO (SANTA SÉ)	VA
VENEZUELA	VE
VIETNÃ	VN
ILHAS VIRGENS, BRITÂNICAS	VG
ILHAS VIRGENS, DOS ESTADOS UNIDOS	VI
WALLIS E FUTUNA	WF
SAARA OCIDENTAL	EH
IÊMEN	YE
ZAIRE (CONGO, A REPÚBLICA DEMOCRÁTICA DO)	CD
ZÂMBIA	ZM
ZIMBÁBUE	ZW

3.3.2.1.11.3 Lista de países bloqueados

Defina os países para os quais deseja bloquear e dos quais não quer receber mensagens. Para adicionar um país à lista **Países bloqueados:**, selecione-o da coluna **Código de país:** e pressione o botão **Adicionar**. Para remover o país da lista **Países bloqueados:**, selecione o código de país e pressione o botão **Remover**.

Para obter uma lista de códigos de país específicos, consulte o tópico Lista de países de residência 50.

3.3.2.1.11.4 Lista de conjuntos de caracteres bloqueados

Defina os conjuntos de caracteres que deseja bloquear. As mensagens nesses conjuntos de caracteres não serão recebidas. Para adicionar um conjunto de caracteres, selecione-o da coluna **Conjuntos de caracteres:** e pressione o botão **Adicionar**. Isso moverá o conjunto de caracteres para a coluna **Conjuntos de caracteres bloqueados:** . Para remover o conjunto de caracteres da coluna **Conjuntos de caracteres bloqueados:**, selecione o código de conjunto de caracteres e pressione o botão **Remover**.

Ao adicionar um conjunto de caracteres a conjuntos de caracteres bloqueados, você poderá especificar seu próprio valor para a pontuação SPAM para este conjunto de caracteres específico. O padrão é 100. Você pode definir a pontuação para cada conjunto de caracteres separadamente.

3.3.2.1.12 Relatórios

Ativar registro detalhado - Ativa o registro mais detalhado.

Arquivos de rerroteamento de saída: - Redirecione o arquivo de saída de log para o diretório especificado nesse campo. Pressione o botão **...** para procurar o diretório em vez de digitá-lo manualmente.

3.3.2.1.13 Estatísticas

Ativar registro de dados estatísticos - Registra IPs, domínios, palavras suspeitas de URL, etc., no sistema de arquivo de configuração. Os registros podem ser carregados automaticamente em servidores de análise do mecanismo antispam. Os registros podem ser convertidos em texto simples para visualização.

- **Enviar dados estatísticos para análise** - Inicia um encadeamento para carregar automaticamente arquivos de estatísticas para servidores de análise do mecanismo antispam.
- **Endereço de servidor de análise:** - URL nas quais os arquivos de estatísticas serão carregados.

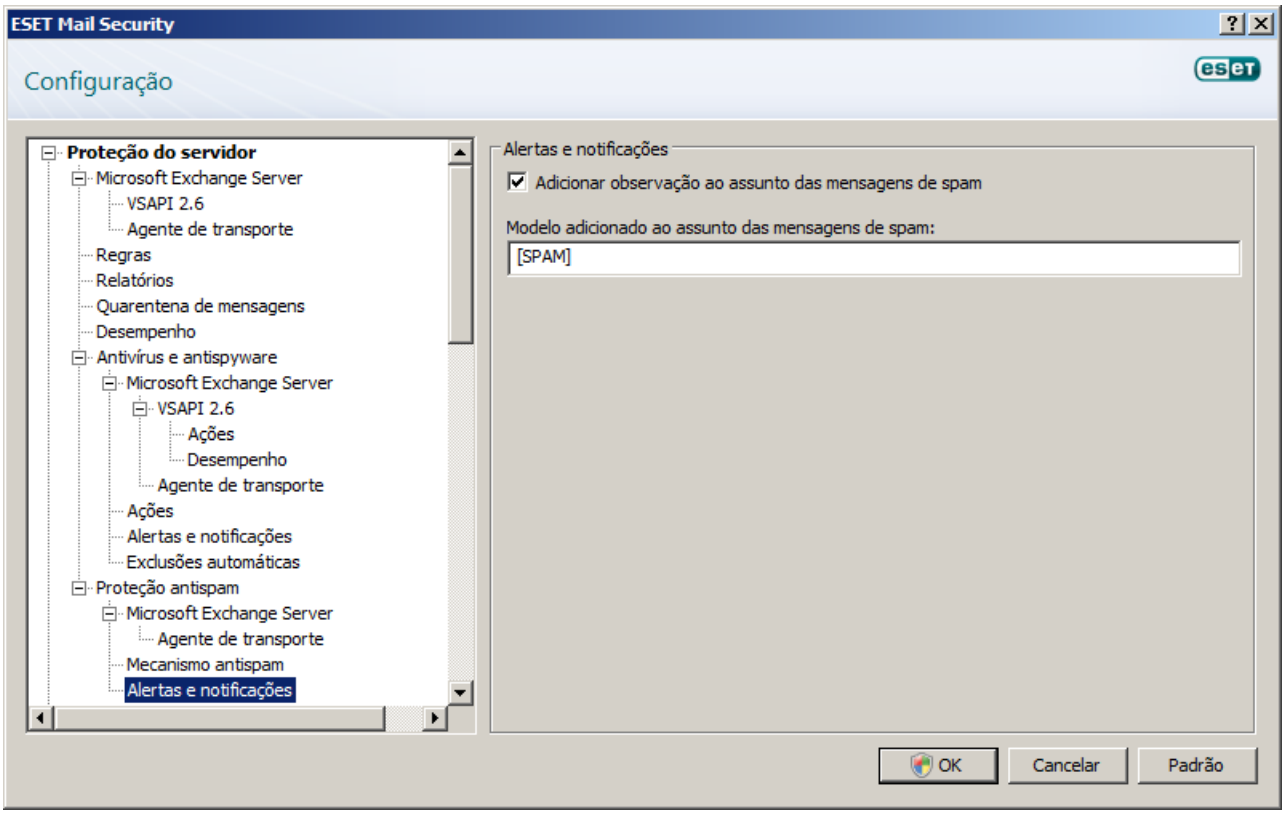
3.3.2.1.14 Opções

Configuração automática: - Defina opções com base nos requisitos de recursos, desempenho e sistema de entrada do usuário.

Criar arquivo de configuração - Cria o arquivo *antispam.cfg*, que contém a configuração do mecanismo antispam. Ele pode ser encontrado em *C:\ProgramData\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2008) ou *C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2000 e 2003).

3.3.3 Alertas e notificações

Todo email rastreado pelo ESET Mail Security e marcado como spam pode ser sinalizado anexando uma marca de notificação anexada ao assunto do email. Por padrão, a marca é [*SPAM*], embora possa ser uma cadeia de caracteres definida pelo usuário.



OBSERVAÇÃO: Também é possível usar variáveis do sistema ao adicionar um modelo ao assunto da mensagem.

3.4 FAQ

P: Após a instalação do EMSX com antispam, os emails pararam de ser entregues nas caixas de correio.

R: Se a Lista cinza estiver ativada, esse comportamento é normal. Nas primeiras horas de operação integral, os emails poderão chegar com várias horas de atraso. Se o problema persistir por um período maior, recomendamos desativar (ou reconfigurar) a Lista cinza.

P: Quando a VSAPI rastreia anexos de email, ela também rastreia o corpo das mensagens de email?

R: No Microsoft Exchange Server 2000 SP2 e posteriores, a VSAPI também rastreia o corpo das mensagens de email.

P: Por que o rastreamento de mensagens continua após a opção VSAPI ser desativada?

R: As alterações nas configurações da VSAPI são executadas de forma assíncrona, ou seja, as configurações modificadas da VSAPI devem ser iniciadas pelo Microsoft Exchange Server para entrarem em vigor. Esse processo cíclico é executado em intervalos de aproximadamente um minuto. O mesmo se aplica a todas as outras configurações da VSAPI.

P: A VSAPI pode remover uma mensagem inteira que contenha um anexo infectado?

R: Sim, a VSAPI pode remover a mensagem inteira. Entretanto, é necessário selecionar primeiro a opção **Excluir toda a mensagem** na seção **Ações** das configurações da VSAPI. Essa opção está disponível no Microsoft Exchange Server 2003 e posteriores. As versões anteriores do Microsoft Exchange Server não têm suporte à remoção de mensagens inteiras.

P: O email enviado também é rastreado pela VSAPI quanto a vírus?

R: Sim, a VSAPI rastreia os emails enviados, exceto se você tiver configurado um servidor SMTP no seu cliente de email que seja diferente do Microsoft Exchange Server. Esse recurso é aplicado no Microsoft Exchange Server 2000 Service Pack 3 e posteriores.

P: É possível adicionar texto de marca de notificação via VSAPI a cada mensagem rastreada, da mesma maneira que no Agente de transporte?

R: Não há suporte à adição de texto às mensagens rastreadas pela VSAPI no Microsoft Exchange Server.

P: Às vezes, não consigo abrir um email específico no Microsoft Outlook. Por que isso acontece?

R: A opção **Ação a ser tomada se a limpeza não for possível** nas configurações da VSAPI na seção **Ações** provavelmente está definida para **Bloquear** ou você criou uma regra que inclui a ação **Bloquear**. Essas configurações marcarão e bloquearão as mensagens infectadas e/ou as mensagens que se enquadrem na regra mencionada.

P: O que significa o item **Limite de tempo para resposta** na seção **Desempenho**?

R: Se você tiver o Microsoft Exchange Server 2000 SP2 ou posterior, o valor **Limite de tempo para resposta** representará o tempo máximo em segundos necessário para concluir o rastreamento da VSAPI em um encadeamento. Se o rastreamento não for concluído nesse limite de tempo, o Microsoft Exchange Server negará o acesso do cliente ao email. O rastreamento não será interrompido, e, após sua conclusão, todas as outras tentativas de acesso ao arquivo serão bem-sucedidas. Se você tiver o Microsoft Exchange Server 5.5 SP3 ou SP4, o valor será expresso em milissegundos e representará o período após o qual o cliente tentará acessar novamente o arquivo que estava anteriormente inacessível devido ao rastreamento.

P: Que tamanho pode ter a lista de tipos de arquivos em uma regra?

R: A lista de extensões de arquivos contém no máximo 255 caracteres em uma única regra.

P: Eu ativei a opção **Rastreamento em segundo plano** na VSAPI. Até agora, as mensagens no Microsoft Exchange Server sempre foram rastreadas após cada atualização do banco de dados de assinatura de vírus. Isso não aconteceu após a última atualização. Onde está o problema?

R: A decisão de rastrear todas as mensagens imediatamente ou na tentativa do usuário de acessar uma mensagem depende de vários fatores, como carga do servidor, tempo de CPU necessário para rastrear todas as mensagens em bloco e o número total de mensagens. O Microsoft Exchange Server rastreará todas as mensagens antes que cheguem à caixa de entrada do cliente.

P: Por que o contador de regras aumentou em mais de um após receber uma mensagem individual?

R:As regras são verificadas em relação à mensagem quando ela é processada pelo agente de transporte (TA) ou pela VSAPI. Quando o TA e a VSAPI estão ativados e a mensagem corresponde às condições da regra, o contador de regras pode aumentar em 2 ou mais. A VSAPI acessa as partes da mensagem individualmente (corpo, anexo), o que significa que as regras são consequentemente aplicadas a cada parte individualmente. Além disso, as regras podem ser aplicadas durante o rastreamento em segundo plano (por exemplo, rastreamento repetido do armazenamento da caixa de correio após uma atualização do banco de dados de assinatura de vírus), o que pode aumentar o contador de regras.

P: O ESET Mail Security 4 para Microsoft Exchange Server é compatível com o Filtro inteligente de mensagens?

R: Sim, o ESET Mail Security 4 para Microsoft Exchange Server (EMSX) é compatível com o Filtro inteligente de mensagens (IMF). O processamento de emails no caso de a mensagem ser classificada como spam é este:

- Se o antispam do ESET Mail Security tiver a opção **Excluir a mensagem** (ou **Colocar mensagem em quarentena**) ativada, a ação será executada independentemente da ação definida no IMF do Microsoft Exchange.

- Se o antispam do ESET Mail Security tiver a opção **Nenhuma ação** definida, as configurações do IMF do Microsoft Exchange serão usadas e a ação relevante será executada (por exemplo, Excluir, Rejeitar, Arquivar...). A opção **Gravar nível de confiança de spam (SCL) às mensagens rastreadas de acordo com a pontuação de spam** (em **Proteção do servidor > Microsoft Exchange Server > Agente de transporte**) deve estar ativada para que esse recurso funcione com eficácia.

P: Como configuro o ESET Mail Security para mover emails não solicitados para a pasta de spam do Microsoft Outlook definida pelo usuário?

R: As configurações padrão do ESET Mail Security fazem com que o Microsoft Outlook armazene emails indesejados na pasta **Lixo eletrônico**. Para permitir esse recurso, desmarque a opção **Gravar pontuação de spam no cabeçalho dos emails rastreados** (em **F5 > Proteção do servidor > Proteção antispam > Microsoft Exchange Server > Agente de transporte**). Se desejar que o email indesejado seja armazenado em uma pasta diferente, leia as seguintes instruções:

1) No ESET Mail Security:

- vá para a árvore de configuração avançada **F5**,

- navegue para **Proteção do servidor > Proteção antispam > Microsoft Exchange Server > Agente de transporte**

- selecione **Reter mensagem** a partir do menu suspenso **Ação a ser tomada em mensagens de spam**

- desmarque a caixa de verificação **Gravar pontuação de spam no cabeçalho das mensagens rastreadas**

- navegue para **Alertas e notificações** em **Proteção antispam**

- defina uma tag de texto a ser adicionada ao campo de assunto das mensagens indesejadas, por exemplo "[SPAM]", no campo **Modelo adicionado ao assunto das mensagens de spam**

2) No Microsoft Outlook:

– configure uma regra para garantir que as mensagens com um texto específico no assunto ("[SPAM]") serão movidas para a pasta desejada.

Para instruções e informações mais detalhadas leia este artigo da Base de conhecimento.

P: Nas estatísticas da proteção antispam, muitas mensagens se enquadram na categoria **Não rastreado**. Qual email não é rastreado pela proteção antispam?

R: A categoria **Não rastreado** é composta de:

Geral:

- Todas as mensagens que foram rastreadas enquanto a proteção antispam estava desativada em todas as camadas (mailserver, agente de transporte)

Microsoft Exchange Server 2003:

- Todas as mensagens recebidas de um **endereço IP**, que esteja na IMF na **Lista de permissões globais**
- Mensagens de remetentes autenticados

Microsoft Exchange Server 2007:

- Todas as mensagens enviadas na empresa (todas serão rastreadas pela proteção antivírus)
- Mensagens de remetentes autenticados
- Mensagens de usuários configurados para ignorar o antispam
- Todas as mensagens enviadas para a caixa de correio que tenha a opção **AntispamBypass** ativada.
- Todas as mensagens de remetentes na lista de **Remetentes seguros**.

OBSERVAÇÃO: Os endereços definidos na lista de permissões e nas configurações do mecanismo antispam não entram na categoria **Não rastreado**, pois esse grupo é composto exclusivamente de mensagens que nunca foram processadas pelo antispam.

P: Os usuários fazem download de mensagens para seus clientes de email via POP3 (ignorando o Microsoft Exchange Server), mas as caixas de correio estão armazenadas no Microsoft Exchange Server. Esses emails serão submetidos ao rastreamento antivírus e antispam pelo ESET Mail Security?

R: Nesse tipo de configuração, o ESET Mail Security rastreará os emails armazenados no Microsoft Exchange Server

somente quanto à presença de vírus (via VSAPI). O rastreamento antispam não será realizado, pois isso requer um servidor SMTP.

P: Posso definir o nível da pontuação de spam que a mensagem precisa atingir para ser classificada como SPAM?

R: É possível definir esse limite no ESET Mail Security versão 4.3 e posteriores (consulte o capítulo Mecanismo antispam 40).

P: O módulo de proteção antispam do ESET Mail Security também rastreia mensagens que foram obtidas por download via Conector POP3?

R:O ESET Mail Security suporta o Conector Microsoft SBS POP3 padrão no SBS 2008, portanto as mensagens obtidas por download via este Conector POP3 são rastreadas quanto à presença de spam. Porém o Conector Microsoft SBS POP3 padrã no SBS 2003 não é suportado. Também existem Conectores POP3 de terceiros. Se as mensagens buscadas através destes Conectores POP3 de terceiros são rastreadas em relação a spam ou não depende de como um Conector POP3 em específico é projetado e como as mensagens estão sendo buscadas através deste conector POP3. Para mais informações, consulte o tópico Conector POP3 e antispam 39.

4. ESET Mail Security - Proteção do servidor

Enquanto fornece proteção ao Microsoft Exchange Server, o ESET Mail Security também tem todas as ferramentas necessárias para assegurar a proteção do próprio servidor (proteção residente, proteção do acesso à Web, proteção do cliente de email e antispam).

4.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, e-mails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la primeiro bloqueando-a e em seguida, limpando, excluindo ou movendo-a para a quarentena.

4.1.1 Proteção em tempo real do sistema de arquivos

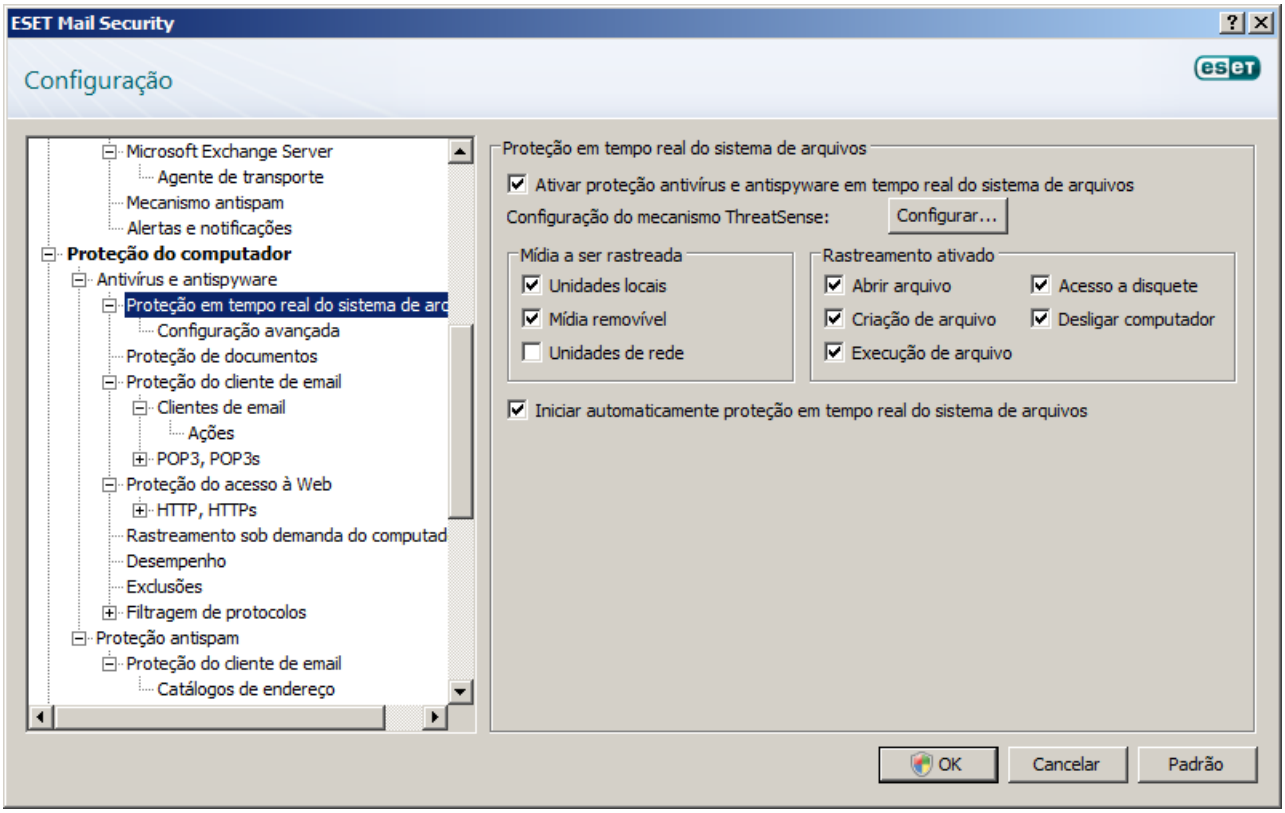
A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

4.1.1.1 Configuração de controle

A proteção do sistema de arquivos em tempo real verifica todos os tipos de mídia e é acionada por vários eventos. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense 76), a proteção do sistema de arquivos em tempo real pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Para proporcionar o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é configurado usando a Otimização inteligente. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Para modificar essa opção, abra a janela Configuração avançada e clique em **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Depois, clique no botão **Configuração...** ao lado de **Configuração do mecanismo ThreatSense**, clique em **Outros** e marque ou desmarque a opção **Ativar otimização inteligente**.

Por padrão, a proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver conflito com outro scanner em tempo real), a proteção em tempo real pode ser encerrada, desmarcando a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**.



4.1.1.1.1 Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças.

Unidades locais – Controla todas as unidades de disco rígido do sistema

Mídia removível – Disquetes, dispositivos de armazenamento USB, etc.

Unidades de rede – Rastreia todas as unidades mapeadas

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

4.1.1.1.2 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

A opção **Acesso a disquete** proporciona controle do setor de inicialização do disquete quando essa unidade for acessada. A opção **Desligar computador** proporciona controle dos setores de inicialização do disco rígido durante o desligamento do computador. Embora os vírus de inicialização sejam raros atualmente, recomendamos deixar essas opções ativadas, pois sempre há a possibilidade de infecção por um vírus de inicialização de origem alternativa.

4.1.1.1.3 Opções de rastreamento avançadas

Opções de configuração mais detalhadas podem ser encontradas em **Proteção do computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema** > **Configuração avançada**.

Parâmetros adicionais do ThreatSense para arquivos criados e modificados recentemente – A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior que em arquivos existentes. É por isso que o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, é usada a heurística avançada, que aumenta enormemente os índices de detecção. Além dos arquivos recém-criados, o rastreamento também é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo de real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em

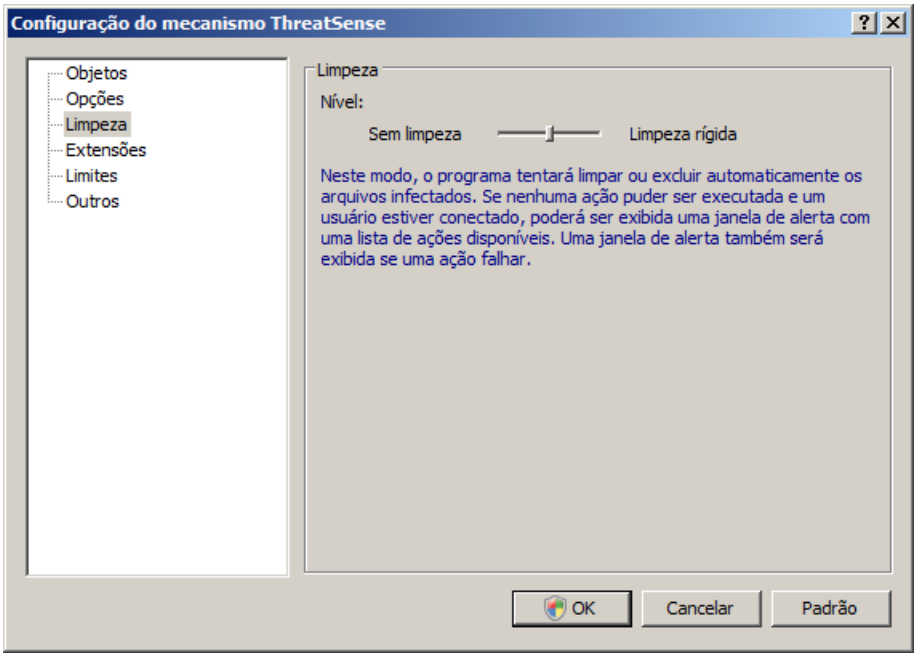
arquivos compactados, desmarque a opção Configurações padrão de rastreamento em arquivos compactados.

Parâmetros ThreatSense.Net adicionais para arquivos executados – Por padrão, a heurística avançada não é usada quando os arquivos são executados. Entretanto, em alguns casos pode ser necessário ativar essa opção (marcando a opção **Heurística avançada na execução de arquivos**). Observe que a heurística avançada pode tornar mais lenta a execução de alguns programas devido ao aumento dos requisitos do sistema.

4.1.1.2 Níveis de limpeza

A proteção em tempo real têm três níveis de limpeza. Para selecionar um nível de limpeza, clique no botão **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e clique na ramificação **Limpeza**.

- O primeiro nível, **Sem limpeza**, exibe uma janela de alerta com as opções disponíveis para cada ameaça encontrada. É necessário escolher uma ação para cada infiltração individualmente. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.
- O nível padrão escolhe e executa automaticamente uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem localizada no canto inferior direito da tela. As ações automáticas não são realizadas quando a infiltração estiver localizada dentro de um arquivo compactado (que também contém arquivos limpos) ou quando os objetos infectados não tiverem uma ação predefinida.
- O terceiro nível, **Limpeza rígida**, é o mais "agressivo" – todos os objetos infectados são limpos. Uma vez que esse nível poderia potencialmente resultar em perda de arquivos válidos, recomendamos que seja usado somente em situações específicas.



4.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Portanto, seja cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver conflito com um certo aplicativo ou scanner em tempo real de outro programa antivírus.

Após a instalação do ESET Mail Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos**).

4.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.org. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo eicar.com está disponível para download em http://www.eicar.org/download/eicar.com

OBSERVAÇÃO: Antes de executar uma verificação da proteção em tempo real, é necessário desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste.

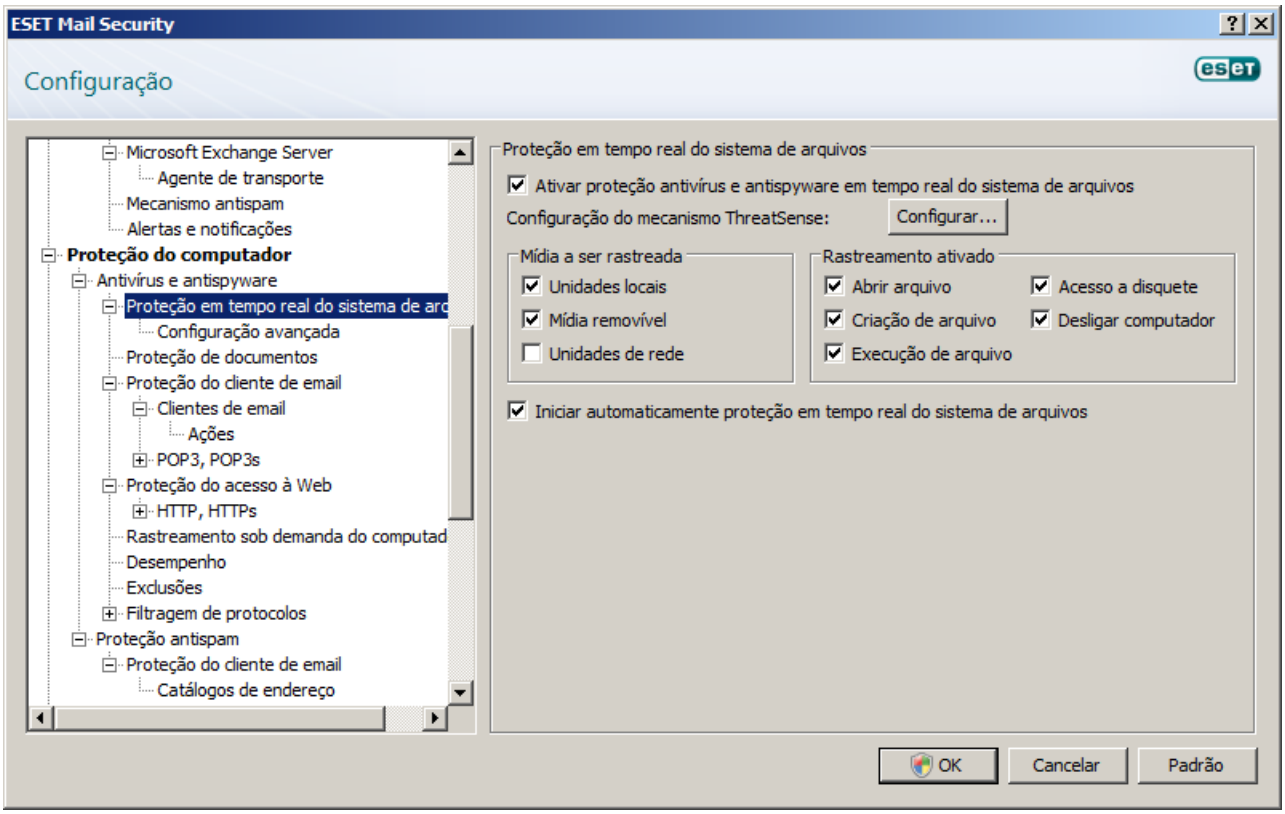
4.1.1.5 O que fazer se a proteção em tempo real não funcionar

No próximo capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

A proteção em tempo real está desabilitada

Se a proteção em tempo real tiver sido inadvertidamente desativada por um usuário, será preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** > **Antivírus e antispyware** e clique na seção **Ativar a proteção em tempo real do sistema de arquivos** da janela principal do programa.

Se a proteção em tempo real não for ativada na inicialização do sistema, isso provavelmente será devido à não ativação da opção **Inicialização automática da proteção em tempo real no sistema de arquivos**. Para ativar essa opção, navegue até Configuração avançada (F5) e clique em **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, certifique-se de que a caixa de seleção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está selecionada.



Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** estiver ativada), isso pode ser devido a conflitos com outros programas. Se for este o caso, consulte os especialistas do Serviço ao Cliente da ESET.

4.1.2 Proteção de cliente de email

A proteção de e-mail fornece controle da comunicação por e-mail recebida via protocolo POP3. Usando o plug-in para Microsoft Outlook, o ESET Mail Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP).

Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado oferecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com o banco de dados de assinaturas de vírus. O rastreamento das comunicações via protocolo POP3 é independente do cliente de email usado.

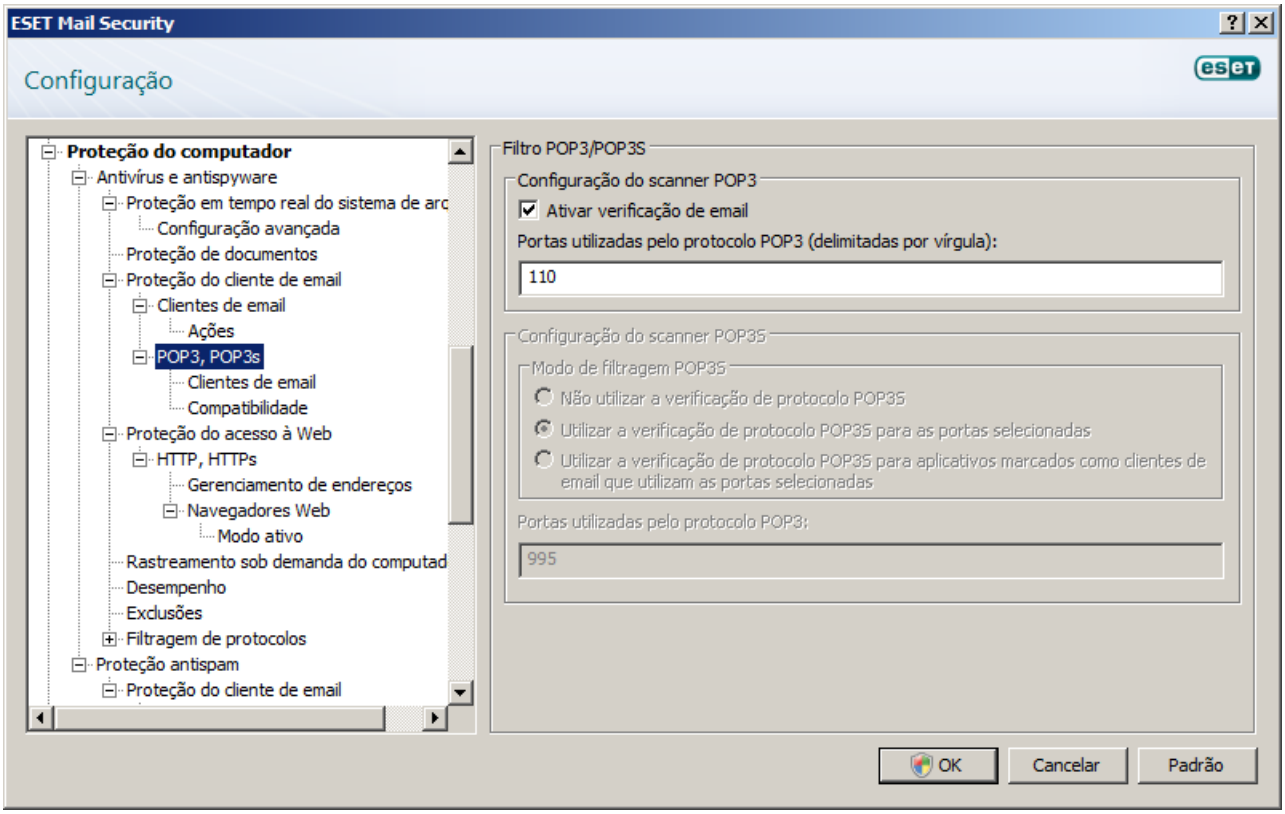
4.1.2.1 Rastreamento POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET Mail Security fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado – a verificação do POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

A comunicação criptografada não é controlada.

Para poder usar a filtragem de POP3/POP3S, é necessário ativar primeiro a Filtragem de protocolos. Se as opções de POP3/POP3S estiverem acinzentadas, navegue até **Proteção do computador** > **Antivírus e antispyware** > **Filtragem de protocolos** na árvore de configuração avançada e selecione **Ativar filtragem de conteúdo do protocolo de aplicativo**. Consulte a seção Filtragem de protocolos para obter mais detalhes sobre filtragem e configuração.



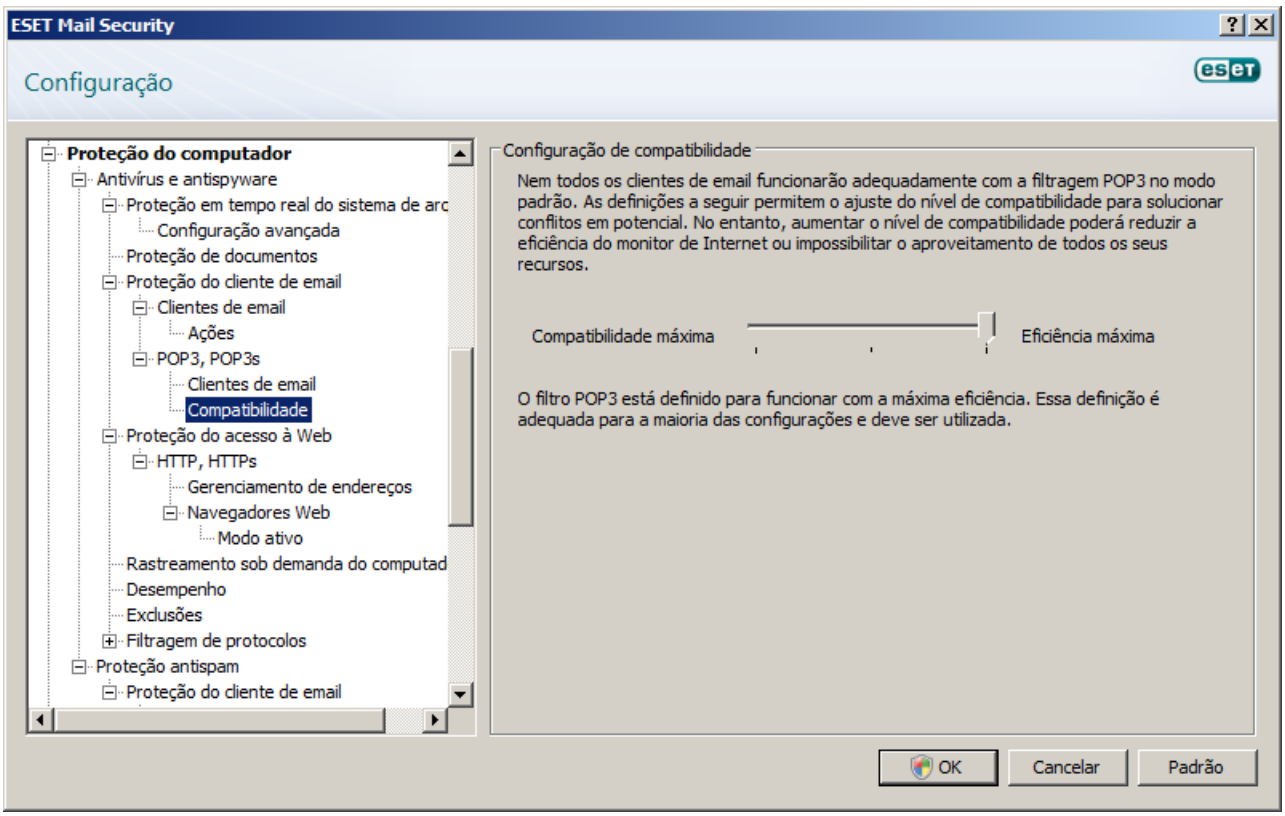
4.1.2.1.1 Compatibilidade

Determinados programas de email podem ter problemas com a filtragem POP3 (por exemplo, ao receber mensagens com uma conexão lenta de Internet, poderá ocorrer desativação por ultrapassar o limite de tempo devido à verificação). Se for este o caso, tente modificar a maneira como é feito o controle. A redução do nível de controle pode melhorar a velocidade do processo de limpeza. Para ajustar o nível de controle da filtragem POP3, na árvore Configuração avançada, navegue até **Antivírus e antispyware** > **Proteção de email** > **POP3, POP3s** > **Compatibilidade**.

Se for ativada a **Eficiência máxima**, as infiltrações serão removidas das mensagens infectadas e as informações sobre a infiltração serão inseridas na frente do assunto original do email (as opções **Excluir** ou **Limpar** devem estar ativadas ou o nível de limpeza **Rígida** ou **Padrão** deve estar ativado).

Compatibilidade média modifica a maneira como as mensagens são recebidas. As mensagens serão gradualmente enviadas ao cliente de email. Após a mensagem ser transferida, ela será rastreada quanto a infiltrações. O risco de infecção aumenta com esse nível de controle. O nível de limpeza e o processamento de mensagens de marca (alertas de notificação anexos à linha do assunto e corpo dos emails) são idênticos à configuração de eficiência máxima.

Com o nível de **Compatibilidade máxima**, você será avisado por uma janela de alerta, que informará o recebimento de uma mensagem infectada. Não é adicionada nenhuma informação sobre arquivos infectados à linha do assunto ou ao corpo do email de mensagens entregues e as infiltrações não são automaticamente removidas; é necessário excluir as infiltrações do cliente de email.

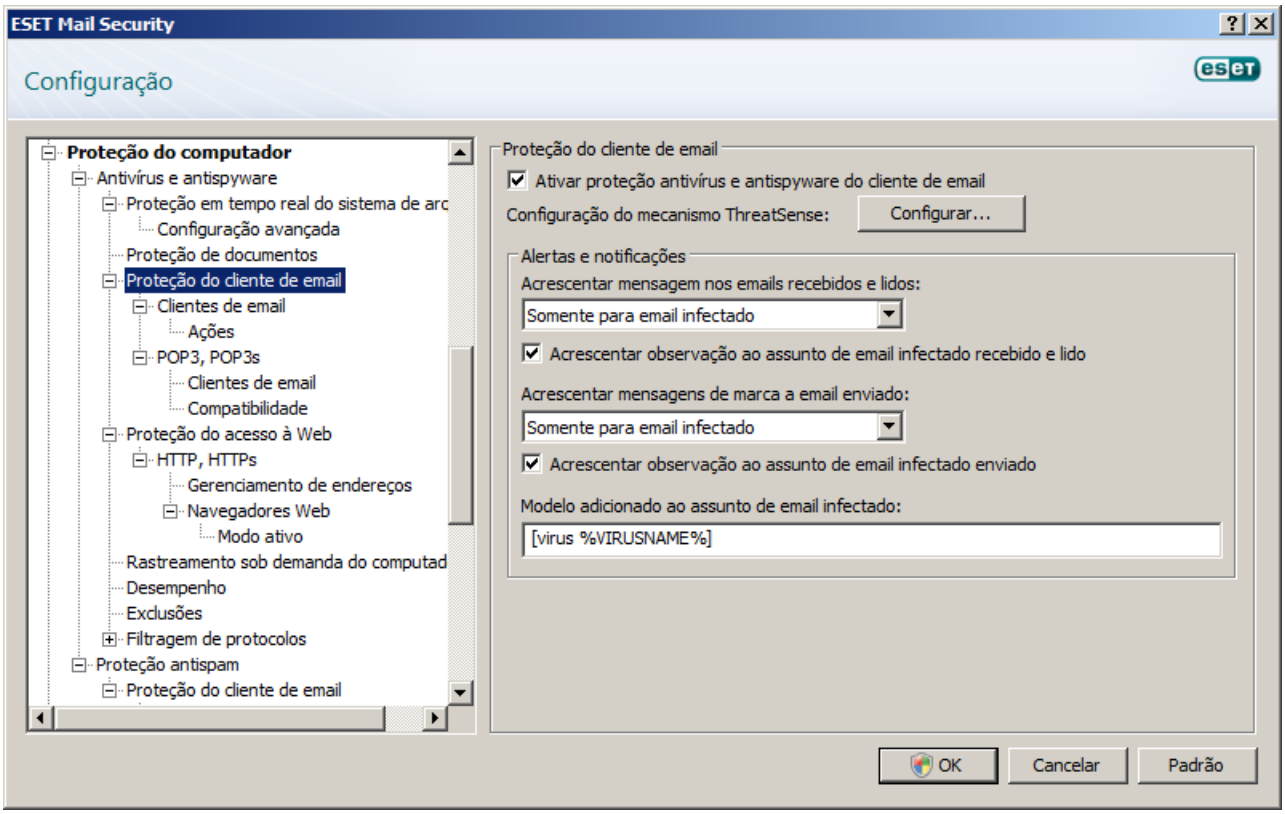


4.1.2.2 Integração com clientes de email

A integração do ESET Mail Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Mail Security. Se a integração for ativada, a barra de ferramentas do ESET Mail Security será inserida diretamente no cliente de email, permitindo proteção mais eficiente aos emails. As configurações de integração estão disponíveis em **Configuração** > **Entrar na configuração avançada...** > **Diversos** > **Integração com clientes de email**. A integração com clientes de email permite ativar a integração com os clientes de email compatíveis. Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

Selecione a opção **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao fazer download de email do Kerio Outlook Connector Store

A proteção de email é ativada clicando em **Configuração** >**Entrar na configuração avançada...** > **Antivírus e antispyware** > **Proteção do cliente de email** e selecionando a opção **Ativar proteção antivírus e antispyware do cliente de email**.



4.1.2.2.1 Anexar mensagens de marca ao corpo de um email

Todo email rastreado pelo ESET Mail Security pode ser marcado anexando uma mensagem de marca ao assunto ou ao corpo do e-mail. Esse recurso aumenta o nível de credibilidade para os destinatários e se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** > **Antivírus e antispyware** > **Proteção do cliente de email**. É possível selecionar **Acrescentar mensagem nos emails recebidos e lidos**, bem como **Acrescentar mensagens de marca a email enviado**. Também há a possibilidade de anexar mensagens de marca a todos os emails rastreados, a somente emails infectados ou a nenhum.

O ESET Mail Security também permite anexar mensagens ao assunto original de mensagens infectadas. Para permitir a anexação ao assunto, selecione as opções **Acrescentar observação ao assunto de email infectado recebido e lido** e **Acrescentar observação ao assunto de email infectado enviado**.

O conteúdo das notificações pode ser modificado no campo **Modelo adicionado ao assunto de email infectado**. As modificações mencionadas anteriormente podem ajudar a automatizar o processo de filtragem dos emails infectados, pois permite filtrar emails com um assunto específico (se houver suporte no cliente de email) em uma pasta separada.

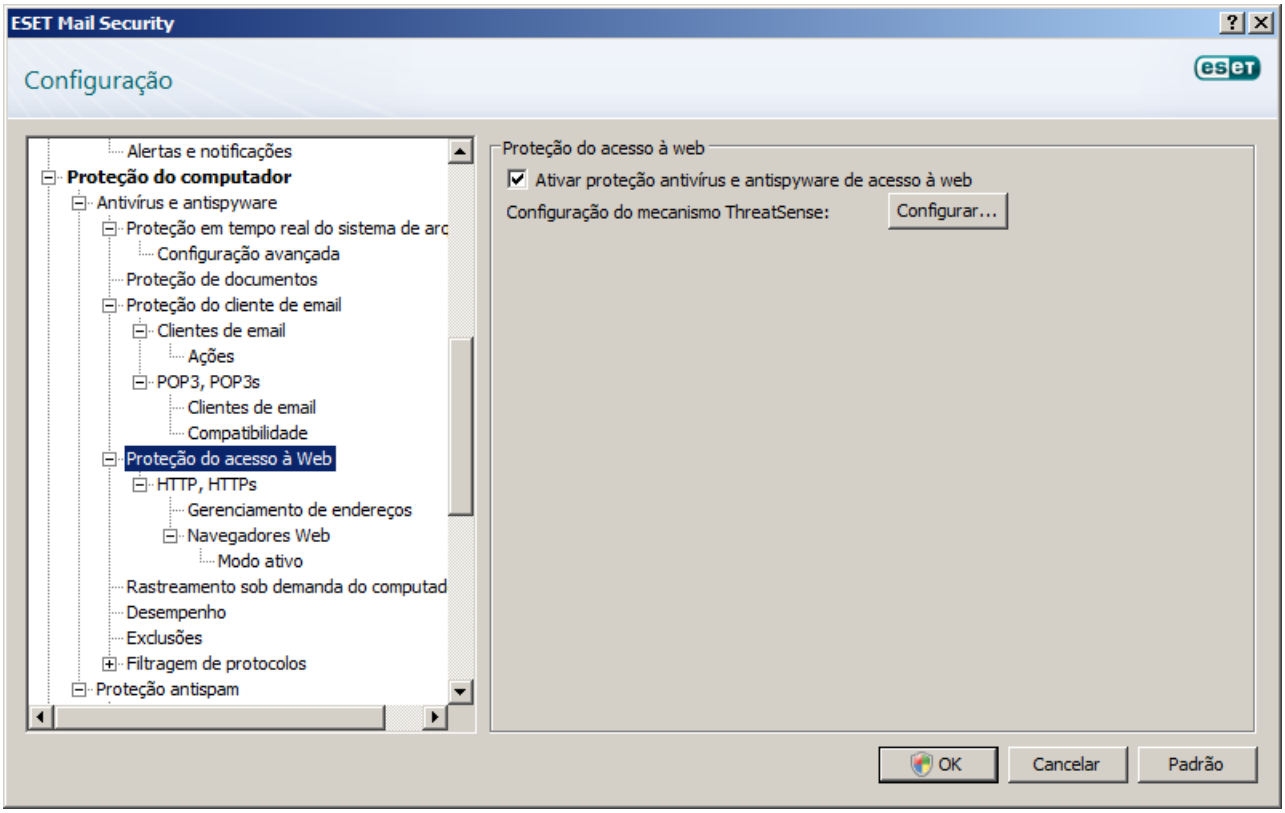
4.1.2.3 Removendo infiltrações

Se uma mensagem de email infectada for recebida, uma janela de alerta será exibida. A janela de alerta mostra o nome do remetente, o email e o nome da infiltração. Na parte inferior da janela, as opções **Limpar**, **Excluir** ou **Deixar** estarão disponíveis para cada objeto detectado. Na maioria dos casos, recomendamos selecionar **Limpar** ou **Excluir**. Em determinadas situações, se desejar receber o arquivo infectado, selecione **Deixar**.

Se a **Limpeza rígida** estiver ativada, uma janela de informações sem nenhuma opção disponível para os objetos infectados será exibida.

4.1.3 Proteção do acesso à web

A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. Por isso, é essencial refletir com atenção sobre a proteção do acesso à Web. Recomendamos enfaticamente que a opção **Ativar proteção antivírus e antispyware de acesso à web** seja selecionada. Essa opção está localizada em **Configuração** (F5) > **Antivírus e antispyware** > **Proteção do acesso à web**.

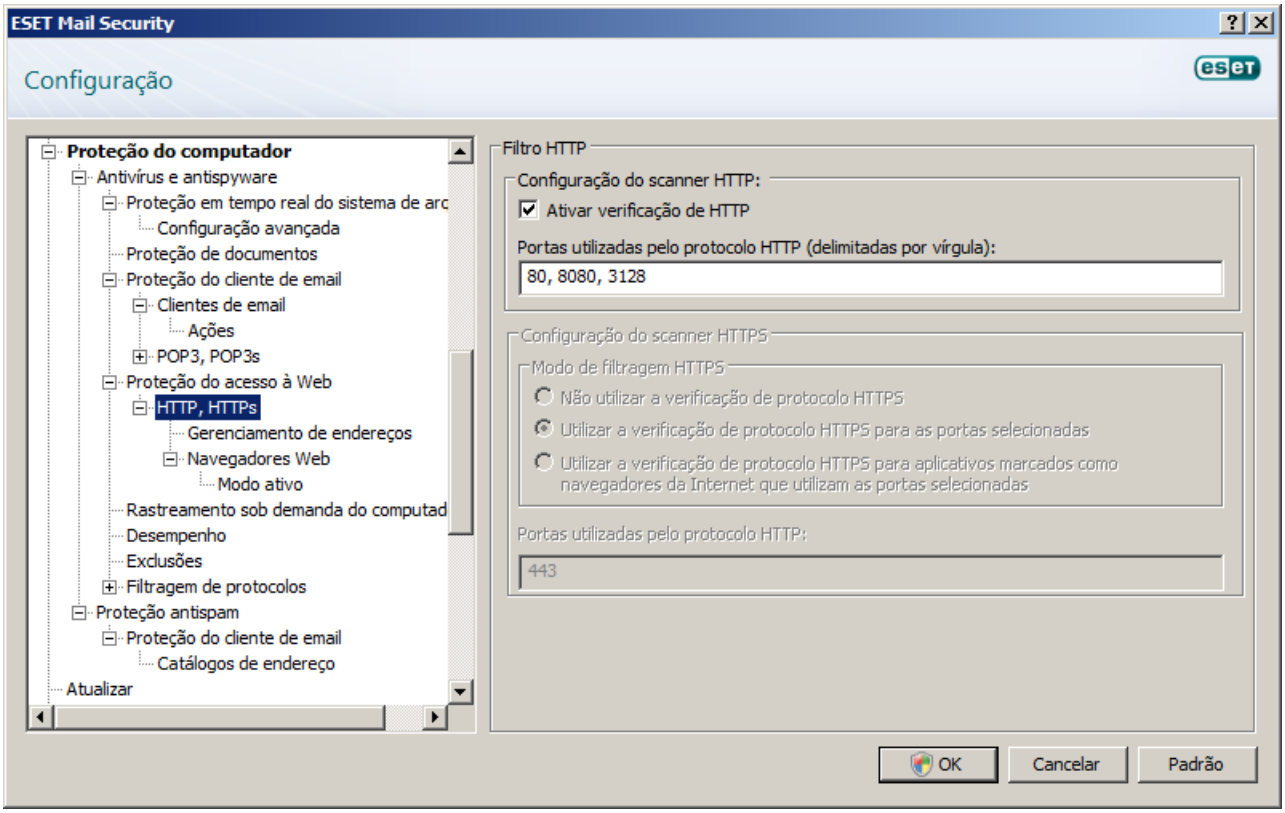


4.1.3.1 HTTP, HTTPs

A proteção de acesso à Web funciona monitorando a comunicação entre os navegadores da Internet e servidores remotos e cumprem as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPs (comunicação criptografada). Por padrão, o ESET Mail Security está configurado para usar os padrões da maioria dos navegadores de Internet. Contudo, as opções de configuração do scanner HTTP podem ser modificadas em **Configuração avançada** (F5) > **Antivírus e antispyware** > **Proteção do acesso à web** > **HTTP, HTTPS**. Na janela principal do filtro HTTP, é possível selecionar ou desmarcar a opção **Ativar verificação de HTTP**. Você também pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 estão predefinidos. A verificação de HTTPs pode ser executada nos seguintes modos:

Não utilizar a verificação de protocolo HTTPS – A comunicação criptografada não será verificada

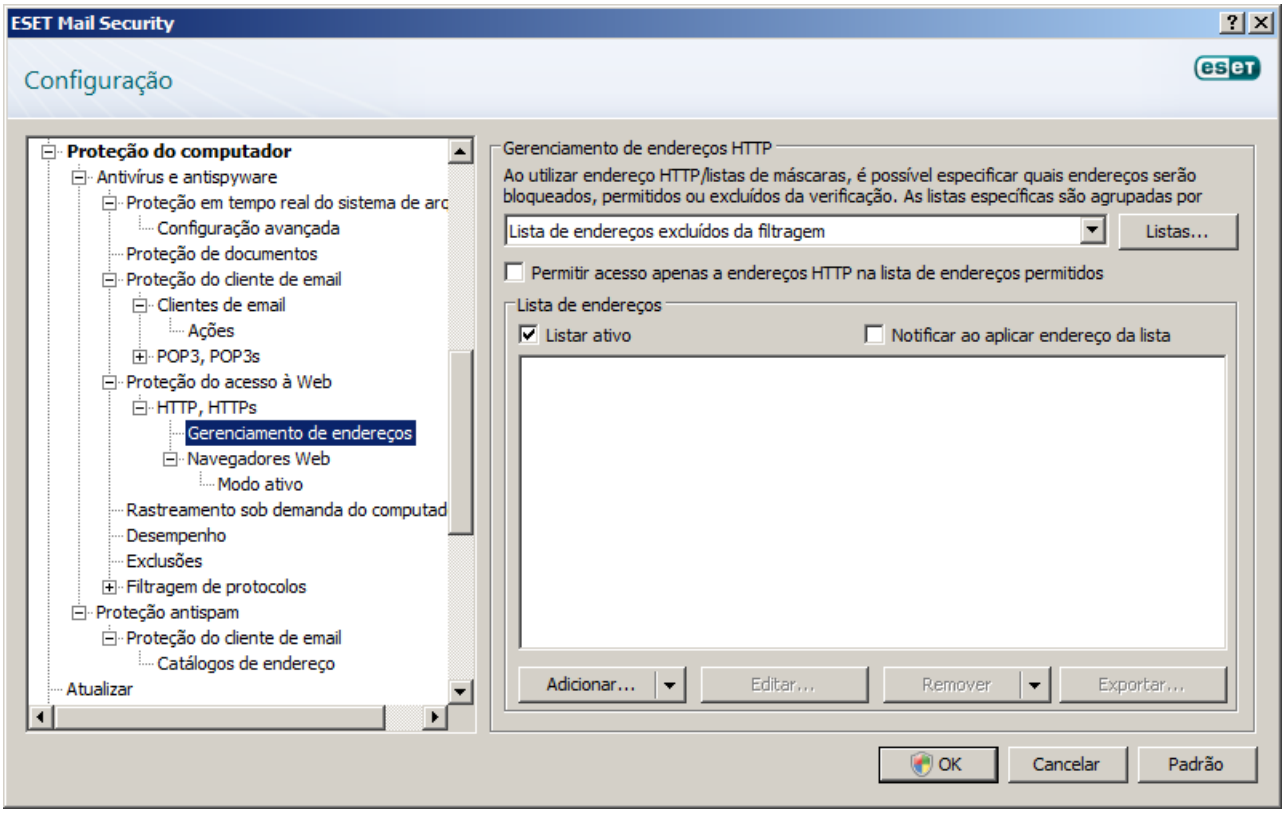
Utilizar a verificação de protocolo HTTPS para as portas selecionadas – Verificação de HTTPs apenas para as portas definidas em **Portas usadas pelo protocolo HTTPs**



4.1.3.1.1 Gerenciamento de endereços

Essa seção permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os botões **Adicionar...**,**Editar...**, **Remover** e **Exportar...** são utilizados para gerenciar as listas de endereços. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso. Se você selecionar a opção **Permitir acesso apenas a endereços HTTP na lista de endereços permitidos**, apenas endereços presentes na lista de endereços permitidos serão acessíveis, enquanto todos os outros endereços HTTP serão bloqueados.

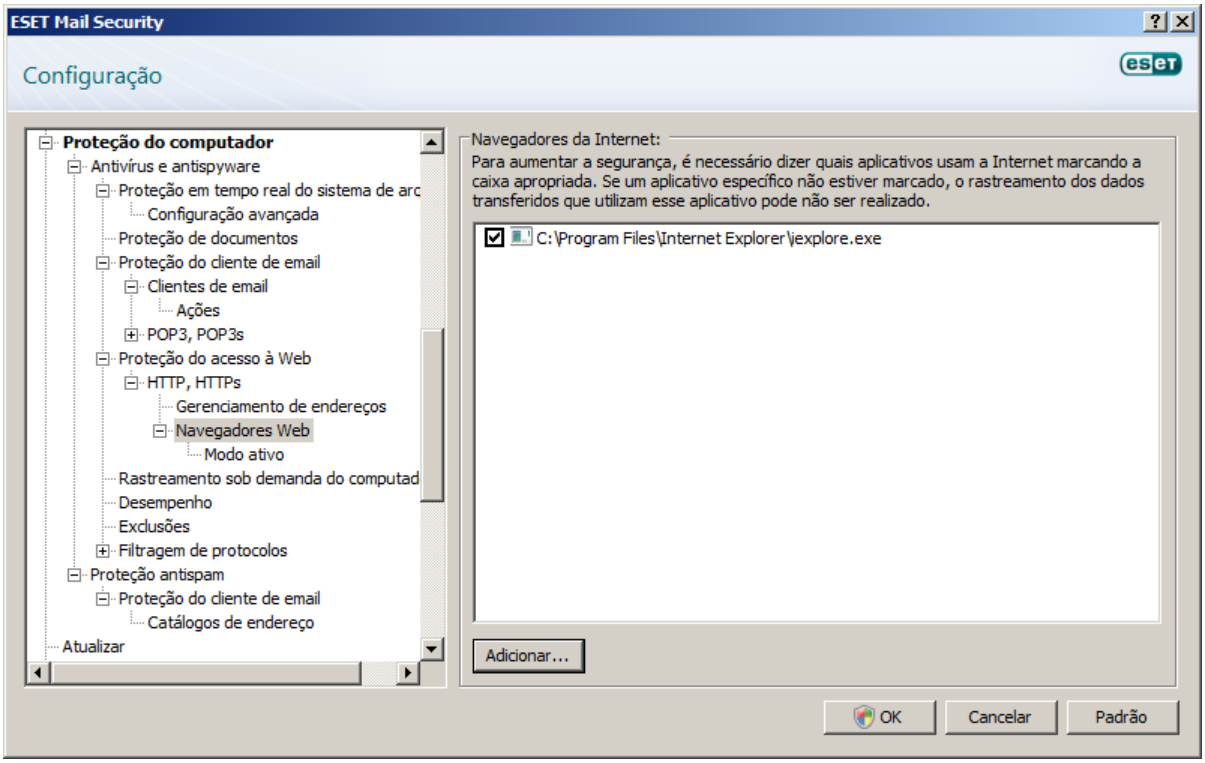
Em todas as listas, os símbolos especiais * (asterisco) e? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Para ativar uma lista, selecione a opção **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione a opção **Notificar ao aplicar endereço da lista**.



4.1.3.1.2 Modo ativo

O ESET Mail Security também contém o recurso Navegadores web, que permite definir se determinado aplicativo é um navegador ou não. Se um aplicativo for marcado como um navegador, todas as comunicações desse aplicativo serão monitoradas, independentemente do número de portas envolvidas.

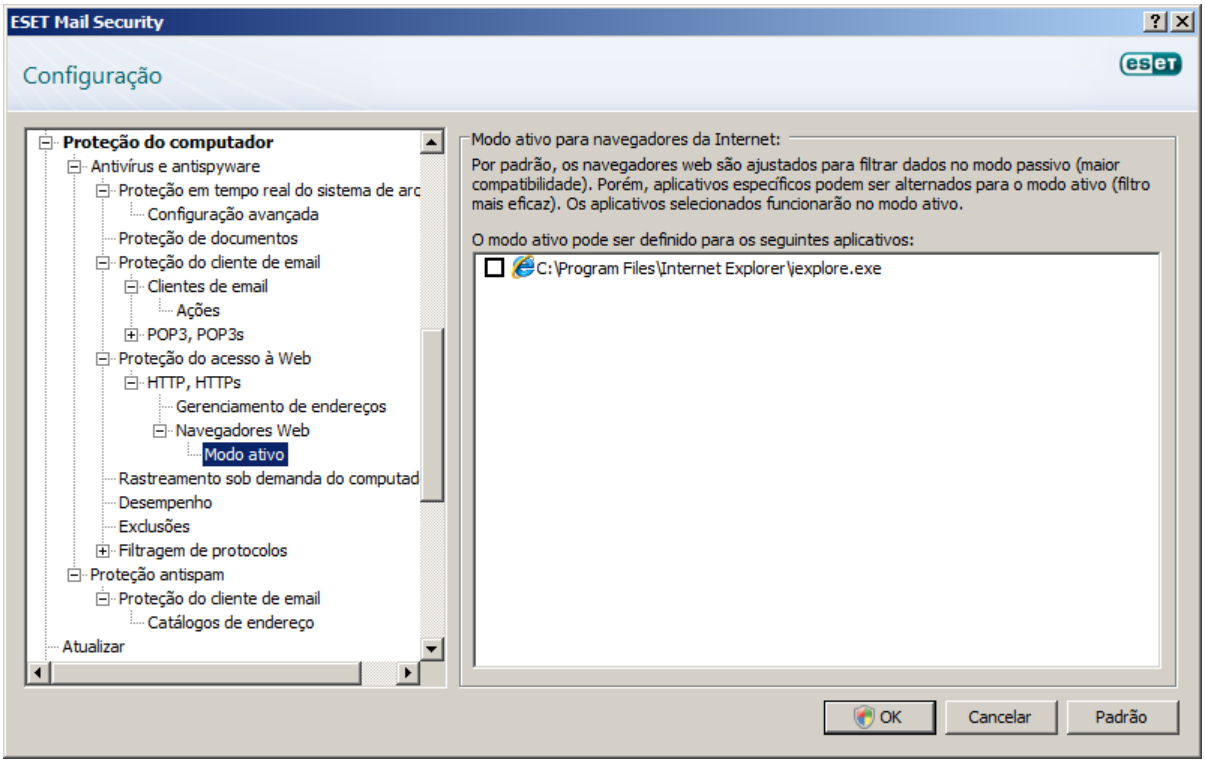
O recurso dos navegadores Web complementa o recurso de verificação HTTP, uma vez que a verificação HTTP somente acontece nas portas predefinidas. Entretanto, muitos serviços da Internet utilizam números de porta que se alteram ou desconhecidos. Para levar isso em conta, o recurso do navegador Web pode estabelecer o controle das comunicações das portas, independentemente dos parâmetros da conexão.



A lista dos aplicativos marcados como navegadores da Web pode ser acessada diretamente no submenu **Navegadores web** da ramificação **HTTP, HTTPs**. Esta seção também contém o submenu **Modo Ativo**, que define o

modo de verificação para os navegadores da Internet.

O **Modo ativo** é útil porque examina os dados transferidos como um todo. Se não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece maior compatibilidade para os aplicativos listados. Se nenhum problema ocorrer durante ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção ao lado do aplicativo desejado.



4.1.4 Rastreamento sob demanda do computador

Caso suspeite que seu computador está infectado (se ele se comportar de maneira anormal), execute um rastreamento sob demanda para examinar se há ameaças no computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. O rastreamento normal pode detectar infiltrações que não foram detectadas pelo scanner em tempo real quando foram salvas no disco. Isso pode acontecer caso o scanner em tempo real esteja desativado no momento da infecção ou se o banco de dados de assinatura de vírus não estiver atualizado.

Recomendamos que execute um Rastreamento sob demanda do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

4.1.4.1 Tipos de rastreamento

Há dois tipos de rastreamento sob demanda do computador disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado...** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

4.1.4.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. Suas principais vantagens são a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a seção Limpeza 79.

4.1.4.1.2 Rastreamento personalizado

O rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Alvos de rastreamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**.

4.1.4.2 Alvos de rastreamento

O menu suspenso Alvos de rastreamento permite selecionar arquivos, pastas e dispositivos (discos) que serão rastreados em busca de vírus.

Por configurações de perfil – Seleciona alvos definidos no perfil de rastreamento selecionado

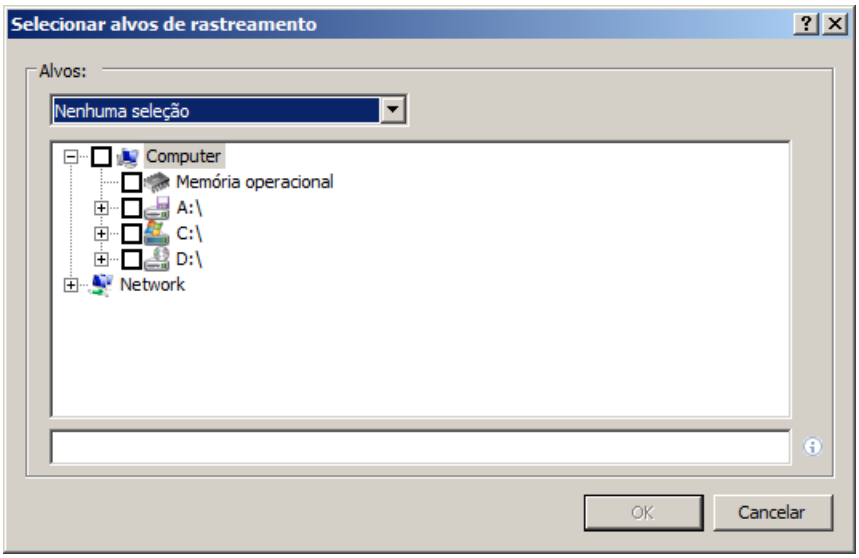
Mídia removível – Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD

Unidades locais – Seleciona todas as unidades de disco rígido do sistema

Unidades de rede – Seleciona todas as unidades mapeadas

Nenhuma seleção – Cancela todas as seleções

Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador.

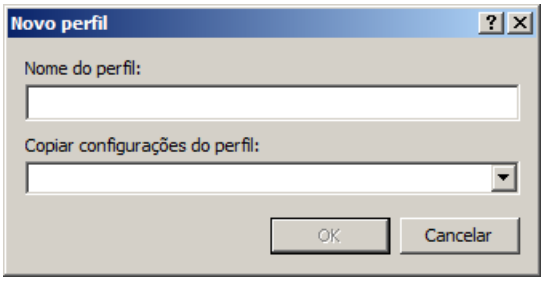


4.1.4.3 Perfis de rastreamento

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Rastreamento sob demanda do computador** > **Perfis...** A janela **Perfis de configuração** tem um menu suspenso com os perfis de rastreamento existentes, bem como a opção para criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense 76 para obter uma descrição de cada parâmetro da configuração de rastreamento.

EXEMPLO: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Digite o nome do novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil**: Depois, ajuste os demais parâmetros de maneira a atender as suas necessidades.



4.1.4.4 Linha de comando

O módulo antivírus do ESET Mail Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat").

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções gerais:

- help	mostrar ajuda e sair
- version	mostrar informações de versão e sair
- base-dir = FOLDER	carregar módulos da PASTA
- quar-dir = FOLDER	PASTA de quarentena
- aind	mostrar indicador de atividade

Alvos:

- files	rastrear arquivos (padrão)
- no-files	não rastrear arquivos
- boots	rastrear setores de inicialização (padrão)
- no-boots	não rastrear setores de inicialização
- arch	rastrear arquivos compactados (padrão)
- no-arch	não rastrear arquivos compactados
- max-archive-level = LEVEL	NÍVEL máximo de encadeamento de arquivos
- scan-timeout = LIMIT	rastrear arquivos por LIMITE segundos no máximo. Se o tempo de rastreamento atingir esse limite, o rastreamento do arquivo compactado será interrompido e o rastreamento continuará no próximo arquivo.
- max-arch-size=SIZE	somente rastreia os primeiros bytes de TAMANHO em arquivos compactados (padrão O = sem limite)
- mail	rastrear arquivos de email
- no-mail	não rastrear arquivos de email
- sfx	rastrear arquivos compactados de autoextração
- no-sfx	não rastrear arquivos compactados de autoextração
- rtp	rastrear compactadores em tempo real
- no-rtp	não rastrear compactadores em tempo real
- exclude = FOLDER	excluir PASTA do rastreamento
- subdir	rastrear subpastas (padrão)
- no-subdir	não rastrear subpastas
- max-subdir-level = LEVEL	NÍVEL máximo de compactação de subpastas (padrão O = sem limite)
- symlink	seguir links simbólicos (padrão)
- no-symlink	ignorar links simbólicos
- ext-remove = EXTENSIONS	
- ext-exclude = EXTENSIONS	excluir do rastreamento EXTENSÕES delimitadas por dois-pontos

Métodos:

- adware	rastrear se há Adware/Spyware/Riskware
- no-adware	não rastrear se há Adware/Spyware/Riskware
- unsafe	rastrear por aplicativos potencialmente inseguros
- no-unsafe	não rastrear por aplicativos potencialmente não seguros
- unwanted	rastrear por aplicativos potencialmente indesejados
- no-unwanted	não rastrear por aplicativos potencialmente indesejados
- pattern	usar assinaturas
- no-pattern	não usar assinaturas
- heur	ativar heurística
- no-heur	desativar heurística
- adv-heur	ativar heurística avançada
- no-adv-heur	desativar heurística avançada

Limpeza:

- action = ACTION	executar AÇÃO em objetos infectados. Ações disponíveis: nenhum, limpar, aviso
- quarantine	copiar os arquivos infectados para Quarentena (completa AÇÃO)
- no-quarantine	não copiar arquivos infectados para Quarentena

Relatórios:

- log-file=FILE	registrar o relatório em ARQUIVO
- log-rewrite	substituir arquivo de saída (padrão – acrescentar)
- log-all	também registrar arquivos limpos
- no-log-all	não registrar arquivos limpos (padrão)

Possíveis códigos de saída do rastreamento:

0	- nenhuma ameaça encontrada
1	- ameaça encontrada mas não limpa
10	- alguns arquivos permanecem infectados
101	- erro no arquivo compactado
102	- erro de acesso
103	- erro interno

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

4.1.5 Desempenho

Nesta seção, é possível definir o número de mecanismos de rastreamento do ThreatSense que serão usados para o rastreamento de vírus. Mais mecanismos de rastreamento do ThreatSense em máquinas com vários processadores podem aumentar a velocidade do rastreamento. O valor aceitável é 1-20.

Se não houver outras restrições, recomendamos aumentar o número de mecanismos de rastreamento ThreatSense na janela Configurações avançadas (F5) em **Proteção do computador** > **Antivírus e antispyware** > **Desempenho**, de acordo com esta fórmula: *número de mecanismos de rastreamento ThreatSense = (número de CPUs físicas x 2) + 1*. Além disso, o *número de encadeamentos de rastreamento* deve ser igual ao *número de mecanismos de rastreamento ThreatSense*. É possível configurar o número de mecanismos de encadeamentos em **Proteção do servidor** > **Antivírus e antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Desempenho**. Veja um exemplo:

Suponhamos que você tenha um servidor com 4 CPUs físicas. Para o melhor desempenho, de acordo com a fórmula anterior, você deve ter 9 encadeamentos de rastreamento e 9 mecanismos de rastreamento.

OBSERVAÇÃO: Recomendamos que você defina o número de encadeamentos de rastreamento igual ao número de mecanismos de rastreamento usados pelo ThreatSense. Isso não terá nenhum efeito sobre o desempenho se você usar mais encadeamentos de rastreamento que mecanismos de rastreamento.

OBSERVAÇÃO: As alterações feitas aqui serão aplicadas somente após a reinicialização.

4.1.6 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos POP3 e HTTP é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. O controle funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. As seguintes opções estão disponíveis para a filtragem de protocolos (se a opção **Ativar filtragem de conteúdo do protocolo de aplicativo** estiver selecionada):

Portas HTTP e POP3s – Limita o rastreamento da comunicação às portas HTTP e POP3 conhecidas.

Aplicativos marcados como navegadores da Internet e clientes de email – Ative essa opção para filtrar somente a comunicação de aplicativos marcados como navegadores (**Proteção do acesso à Web** > **HTTP, HTTPS** > **Navegadores Web**) e clientes de email (**Proteção do cliente de email** > **POP3, POP3s** > **Clientes de email**).

Portas e aplicativos marcados como navegadores da Internet ou clientes de email – Portas e navegadores são verificados quanto a malware.

OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, um novo método de filtragem de comunicações está sendo usado. Como resultado, a seção Filtragem de protocolos não está disponível.

4.1.6.1 SSL

O ESET Mail Security permite verificar protocolos encapsulados no protocolo SSL. É possível usar vários modos de rastreamento para as comunicações protegidas por SSL utilizando certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Sempre rastrear o protocolo SSL – Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado sobre o fato e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado por você como confiável (ele será adicionado à lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

Perguntar sobre sites não visitados (exclusões podem ser definidas) – Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

Não rastrear o protocolo SSL – Se essa opção estiver selecionada, o programa não rastreará as comunicações em SSL.

Caso o certificado não possa ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (**Filtragem de protocolos** > **SSL** > **Certificados**):

Perguntar sobre validade do certificado – Solicita que o usuário selecione uma ação a ser tomada.

Bloquear a comunicação que utiliza o certificado – Encerra a conexão com o site que utiliza o certificado.

Se o certificado for inválido ou estiver corrompido (**Filtragem de protocolos** > **SSL** > **Certificados**):

Perguntar sobre validade do certificado – Solicita que o usuário selecione uma ação a ser tomada.

Bloquear a comunicação que utiliza o certificado – Encerra a conexão com o site que utiliza o certificado.

4.1.6.1.1 Certificados confiáveis

Além do armazenamento integrado de Autoridades de certificação raiz confiáveis, onde o ESET Mail Security armazena os certificados confiáveis, é possível criar uma lista personalizada de certificados confiáveis que pode ser exibida em **Configuração avançada** (F5) > **Filtragem de protocolos** > **SSL** > **Certificados** > **Certificados confiáveis** .

4.1.6.1.2 Certificados excluídos

A seção Certificados excluídos contém certificados que são considerados seguros. O conteúdo das comunicações criptografadas usando os certificados da lista não será verificado quanto a ameaças. Recomendamos que exclua apenas os certificados da Web que são realmente seguros, e tenha certeza de que as comunicações que utilizam esses certificados não precisam ser verificadas.

4.1.7 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é o nome da tecnologia que consiste em métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

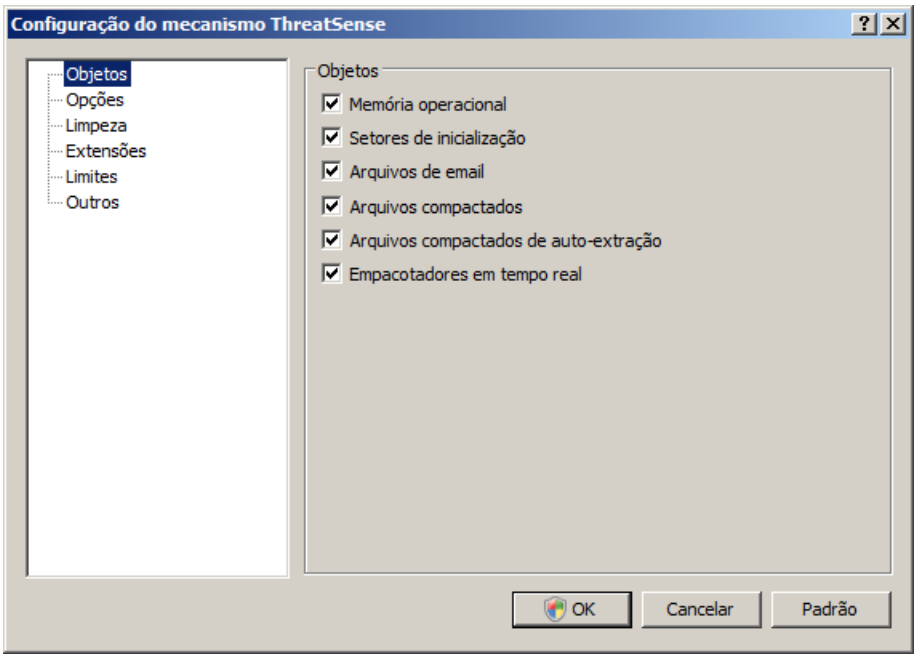
Para acessar a janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos 60
- Rastrear arquivos na inicialização do sistema
- Proteção de email 64
- Proteção do acesso à web 67
- Rastreamento sob demanda do computador 70

Os parâmetros do ThreatSense são altamente otimizados para cada módulo e a modificação pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar heurística avançada no módulo da proteção em tempo real do sistema de arquivos pode resultar em lentidão do sistema (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastreamento sob demanda do computador.

4.1.7.1 Configuração de objetos

A seção **Objetos** permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.



Memória operacional – Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização – Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

Arquivos – Fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de banco de dados etc.)

Arquivos de email – Rastreia arquivos especiais que contenham mensagens de email.

Arquivos compactados – Fornece o rastreamento de arquivos compactados (.rar, .zip, .arj, .tar, etc.).

Arquivos compactados de autoextração – Rastreia os arquivos contidos em arquivos compactados de autoextração, mas geralmente apresentados com a extensão de arquivo .exe

Empacotadores em tempo real – Diferente dos tipos de arquivos compactados padrão, os empacotadores em tempo real são descompactados na memória, além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FGS etc.).

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.7.2 Opções

Na seção **Opções**, é possível selecionar os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

Heurística – A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).

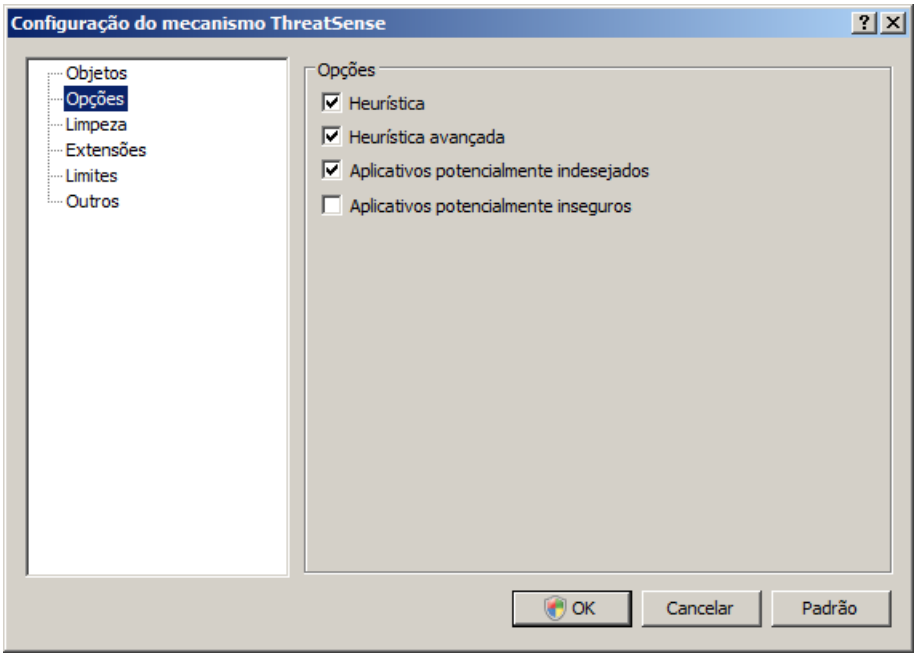
Heurística avançada – A heurística avançada é formada por um algoritmo heurístico exclusivo, desenvolvido pela ESET e otimizado para a detecção de worms e cavalos de troia de computador escritos em linguagens de programação de alto nível. Devido à heurística avançada, a inteligência da detecção do programa é significativamente superior.

Aplicativos potencialmente indesejados – Aplicativos potencialmente indesejados não são necessariamente

maliciosos, mas podem prejudicar o desempenho do computador. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.

Aplicativos potencialmente inseguros – Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

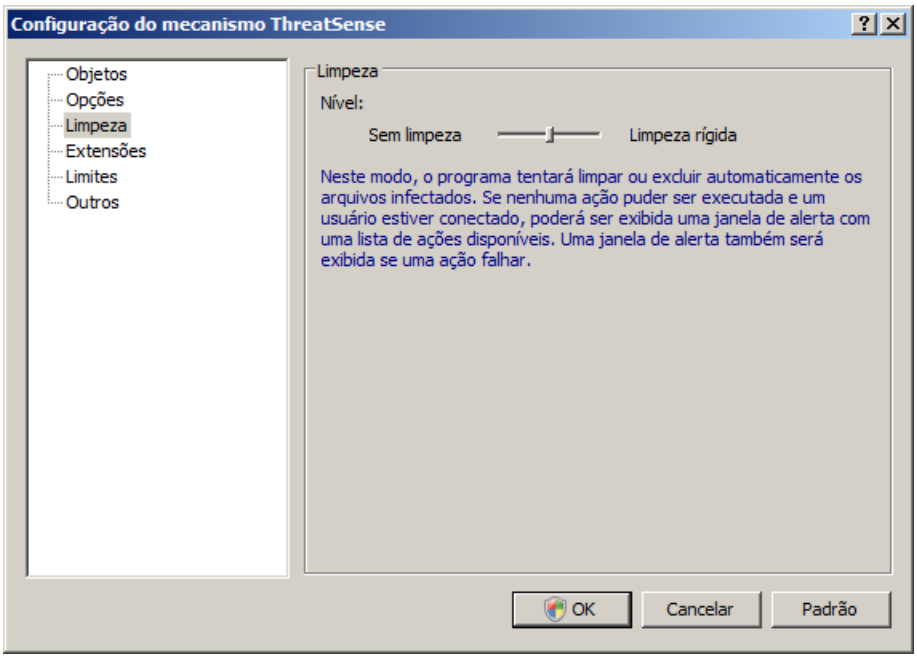
Anexos potencialmente perigosos
A opção Anexos potencialmente perigosos oferece proteção contra ameaças maliciosas que tipicamente se propagam como anexos de email, como por exemplo trojans ransomware. Um exemplo deste tipo de ameaça pode ser um arquivo executável disfarçado como um arquivo de documento padrão (por exemplo, PDF) que, quando é aberto pelo usuário, permite que a ameaça entre no sistema. A ameaça então vai tentar realizar seus objetivos maliciosos.



OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.7.3 Limpeza

As configurações de limpeza determinam o comportamento do scanner durante a limpeza dos arquivos infectados. Há três níveis de limpeza:



Sem limpeza – Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que você escolha uma ação.

Limpeza padrão – O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a serem seguidas. A escolha das ações a serem seguidas também será exibida se uma ação predefinida não for concluída.

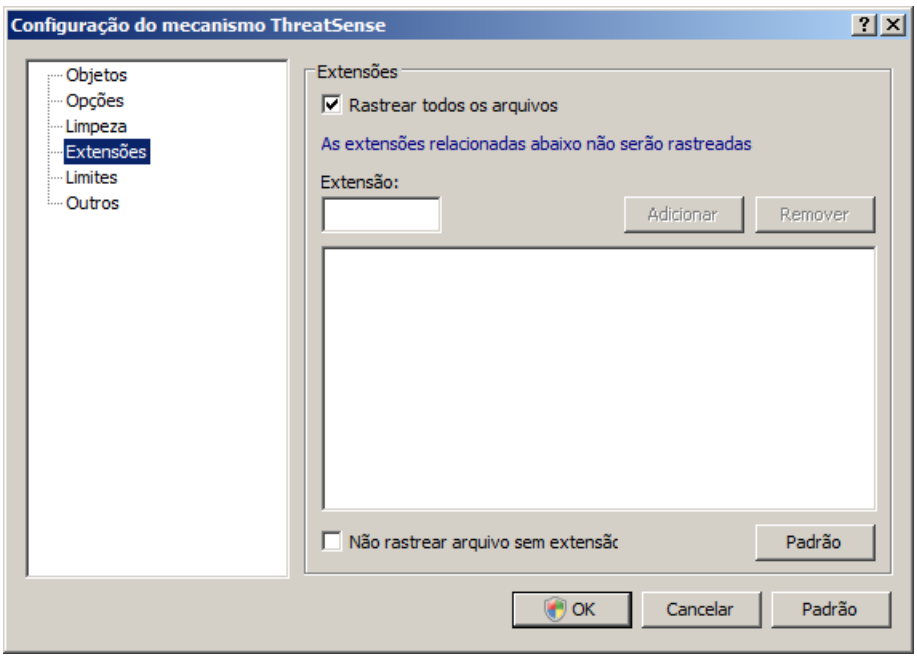
Limpeza rígida – O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos compactados). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, será oferecida a você uma ação a ser tomada na janela de aviso.

Alerta: No modo Padrão, o arquivo compactado inteiro será excluído somente se todos os arquivos do arquivo compactado estiverem infectados. Se no arquivo compactado houver arquivos legítimos, ele não será excluído. Se um arquivo do arquivo compactado infectado for detectado no modo de Limpeza rígida, todo o arquivo compactado será excluído, mesmo se houver arquivos limpos.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.7.4 Extensões

Uma extensão é a parte do nome do arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.



Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** estiver desmarcada, a lista será alterada para exibir todas as extensões de arquivos rastreados no momento. Com os botões **Adicionar** e **Remover**, você pode habilitar ou desabilitar o rastreamento das extensões desejadas.

Para habilitar o rastreamento de arquivos sem nenhuma extensão, marque a opção **Rastrear arquivos sem extensão**.

A exclusão de arquivos do rastreamento será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando as extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.7.5 Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Tamanho máximo do objeto: – Define o tamanho máximo dos objetos que serão rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Não recomendamos alterar o valor padrão, pois não há razão para modificá-lo. Essa opção deverá ser alterada apenas por usuários avançados que tenham razões específicas para excluir objetos maiores do rastreamento.

Tempo máximo do rastreamento para objeto (s): – Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento.

Nível de compactação de arquivos: – Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá desmarcado.

Tamanho máximo do arquivo no arquivo compactado: – Essa opção permite especificar o tamanho máximo dos

arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Se o rastreamento de um arquivo compactado for encerrado prematuramente por essa razão, o arquivo compactado permanecerá sem verificação.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.7.6 Outros

Rastrear fluxos dados alternativos (ADS) – Os fluxos de dados alternativos (ADS) usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade – Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

Registrar todos os objetos – Se essa opção estiver selecionada, o arquivo de relatório mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados.

Ativar otimização inteligente –Selecione essa opção para que os arquivos que já foram rastreados não sejam rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus.

Manter último registro de acesso – Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (ou seja, para uso com sistemas de backup de dados).

Relatório de rolagem – Essa opção permite ativar/desativar o rolamento do relatório. Se selecionada, as informações rolam para cima dentro da janela de exibição.

Exibir notificação sobre a conclusão do rastreamento em uma janela separada – Abre uma janela autônoma que contém as informações sobre os resultados do rastreamento.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.1.8 Uma infiltração foi detectada

As infiltrações podem alcançar o sistema a partir de vários pontos: páginas da Web, arquivos compartilhados, email ou dispositivos de computador removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Mail Security e clique em Rastreamento do computador
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte a seção Rastreamento inteligente 71)
- Após o rastreamento ter terminado, revise o relatório para informações como número dos arquivos verificados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas no ESET Mail Security, suponha que uma infiltração seja detectada pelo monitor do sistema de arquivos em tempo real, que usa o nível de limpeza Padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida a ser tomada para o módulo de proteção em tempo real, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Deixar** estão disponíveis. A seleção da opção **Deixar** não é recomendada, visto que os arquivos infectados seriam mantidos intactos. A exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado

por engano.

Limpeza e exclusão – Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou, a esse arquivo, um código malicioso. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso pelo processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Exclusão de arquivos em arquivos compactados – No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Entretanto, use precaução ao executar um rastreamento com Limpeza rígida – com esse tipo de limpeza, o arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

4.2 Atualização do programa

A atualização regular do ESET Mail Security é a premissa básica para obter o nível máximo de segurança. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras: atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

No menu principal, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

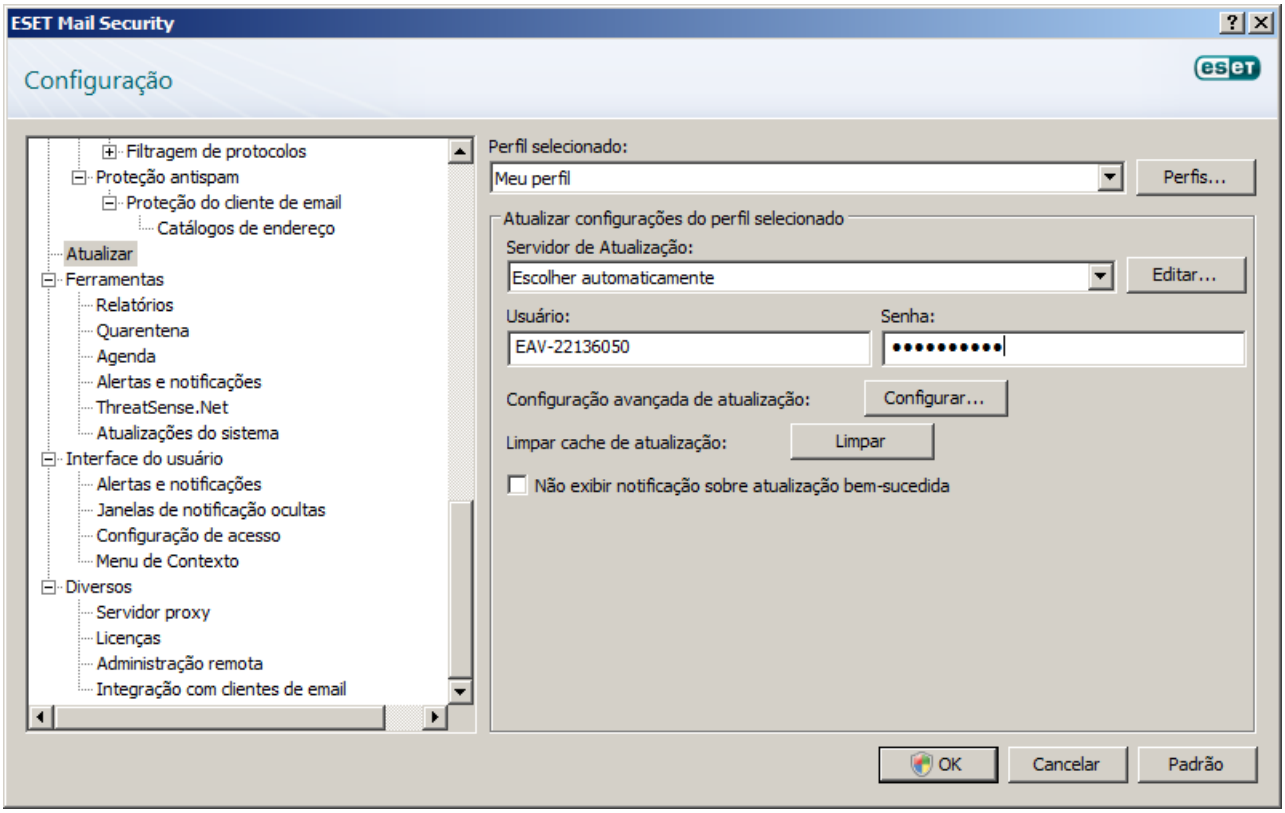
Além disso, a opção para iniciar o processo de atualização manualmente - **Atualizar banco de dados de assinatura de vírus** - está disponível, bem como as opções de configuração básica das atualizações, como o nome de usuário e a senha, para acessar os servidores de atualização da ESET.

Use o link **Ativação do produto** para abrir o formulário de registro que ativará o seu produto de segurança da ESET e enviará a você um email com seus dados de autenticação (nome de usuário e senha).

OBSERVAÇÃO: O nome de usuário e a senha são fornecidos pela ESET após a compra do ESET Mail Security.

4.2.1 Configuração da atualização

A seção de configuração da atualização especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede. As opções de configuração da atualização estão disponíveis na árvore Configuração avançada (tecla F5), em **Atualizar**.

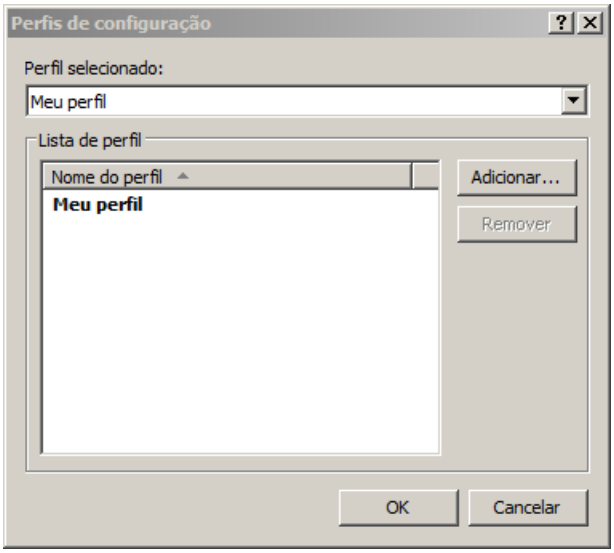


A lista de servidores de atualização disponíveis pode ser acessada pelo menu suspenso **Servidor de atualização**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**. A autenticação dos servidores de atualização é baseada no **Usuário** e na **Senha** gerados e enviados a você após a compra.

4.2.1.1 Atualizar perfis

É possível criar perfis de atualização para várias configurações e tarefas de atualização. A criação de perfis de atualização é particularmente útil para usuários móveis, que podem criar um perfil alternativo para propriedades de conexão à Internet que são alteradas com frequência.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido como o **Meu perfil** por padrão. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar as configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil**.



Na janela de configuração de perfil, especifique o servidor de atualização a partir de uma lista de servidores disponíveis ou adicione um novo servidor. A lista de servidores de atualização existentes pode ser acessada no menu suspenso **Servidor de atualização**: Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**.

4.2.1.2 Configuração avançada de atualização

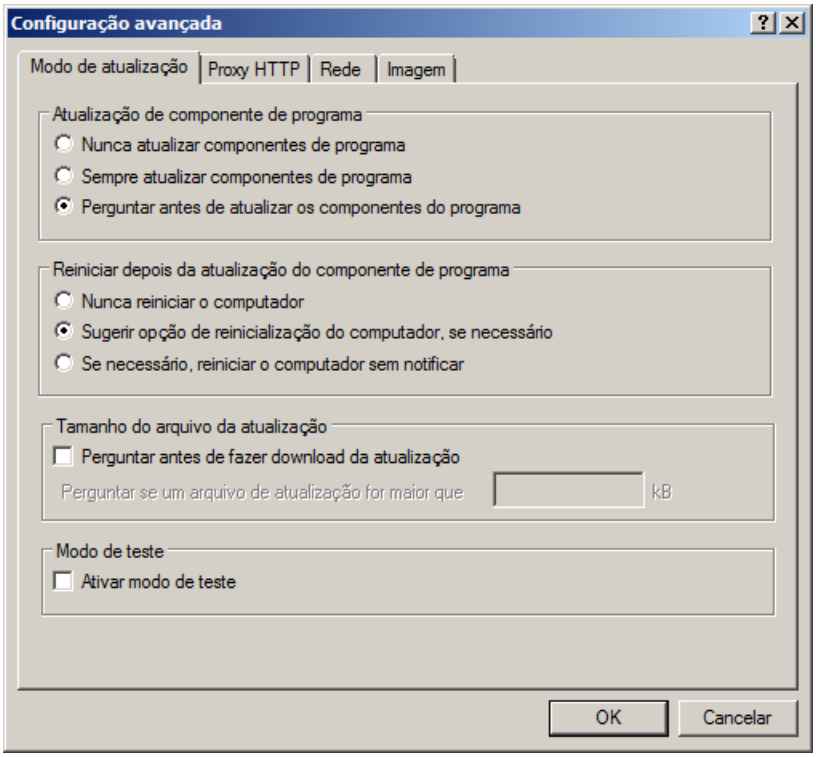
Para exibir a Configuração avançada de atualização, clique no botão **Configuração...**. As opções de configuração avançada de atualização incluem a configuração do **Modo de atualização**, **Proxy HTTP**, **Rede** e **Imagem**.

4.2.1.2.1 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa.

Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Nunca atualizar componentes de programa**: As novas atualizações de componentes do programa não serão obtidas por download.
- **Sempre atualizar componentes de programa**: As novas atualizações de componentes do programa serão feitas automaticamente.
- **Perguntar antes de fazer download dos componentes de programa**: A opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.



Após a atualização de componentes do programa, poderá ser necessário reiniciar o computador para obter uma completa funcionalidade de todos os módulos. A seção **Reiniciar depois da atualização do componente de programa** permite que o usuário selecione uma das seguintes opções:

- **Nunca reiniciar o computador**
- **Sugerir opção de reinicialização do computador, se necessário**
- **Se necessário**, **reinicialize o computador sem notificação**

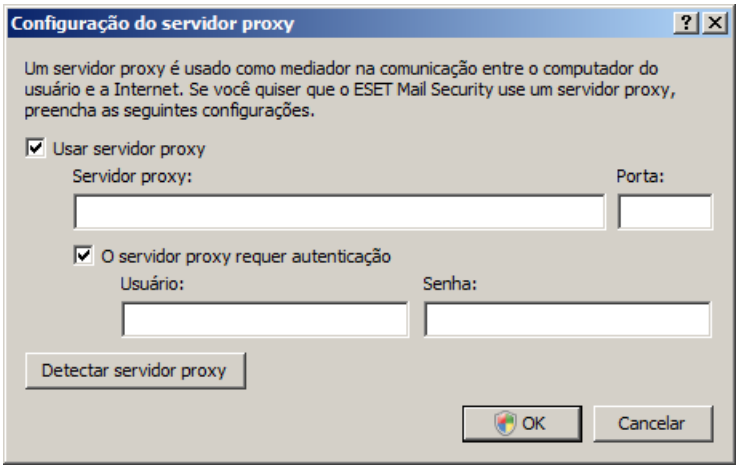
A opção padrão é **Sugerir opção de reinicialização do computador, se necessário**. A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

4.2.1.2.2 Servidor proxy

No ESET Mail Security, a configuração do servidor proxy está disponível em duas seções diferentes na árvore Configuração avançada.

Primeiramente, as configurações do servidor proxy podem ser definidas em **Diversos** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Mail Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**: além do número da **Porta** do servidor proxy.



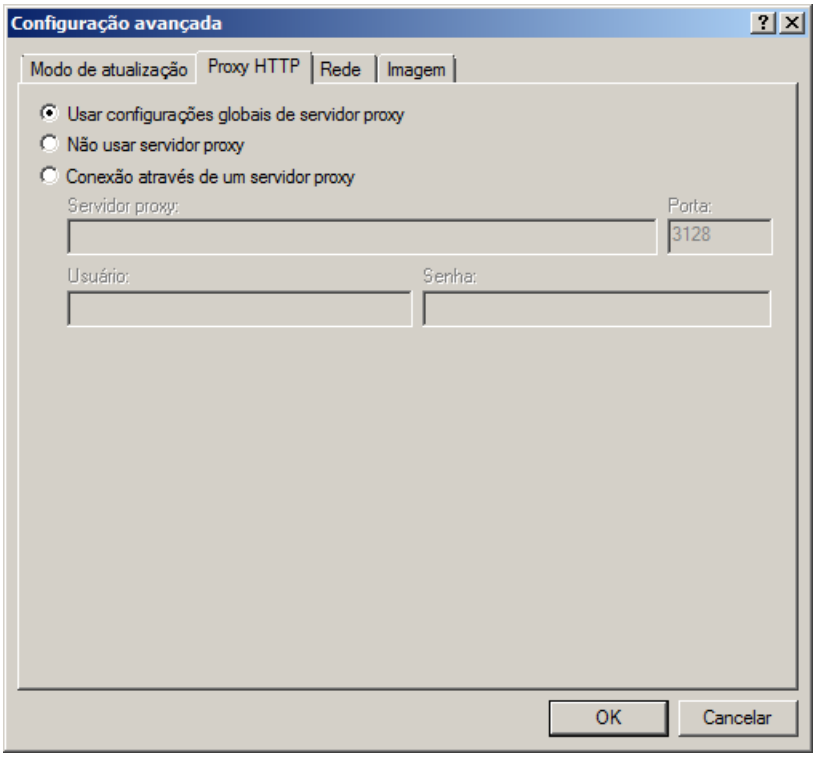
Se a comunicação com o servidor proxy requerer autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e inserir automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

OBSERVAÇÃO: Esse recurso não recupera dados de autenticação (nome de usuário e senha), que devem ser fornecidos por você.

As configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização. Essa configuração será aplicada ao perfil de atualização determinado. É possível acessar as opções de configuração do servidor proxy de determinado perfil de atualização clicando na guia **Proxy HTTP** na **Configuração avançada de atualização**. Você terá uma destas três opções:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy** (conexão definida pelas propriedades de conexão)

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Diversos** > **Servidor proxy** da árvore Configuração avançada (descritas no início desse artigo).



Selecione a opção **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Mail Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se um servidor proxy for usado para atualizar o ESET Mail Security e for diferente do servidor proxy especificado nas configurações globais (**Diversos** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação, além do **Usuário** e da **Senha** para o servidor proxy, se necessário.

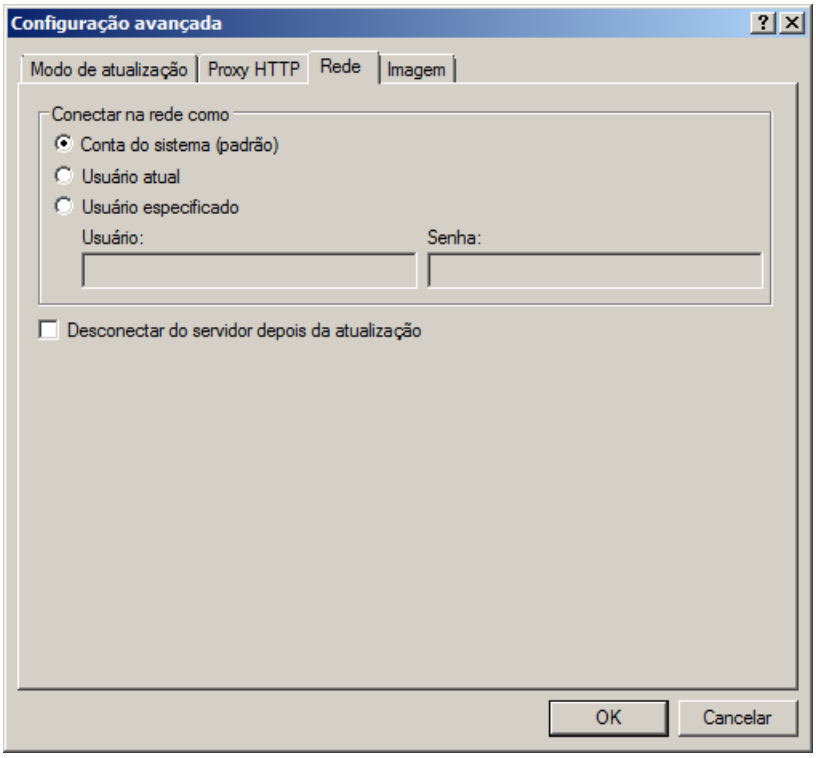
Essa opção também deve ser selecionada se as configurações do servidor proxy não tiverem sido definidas globalmente, mas o ESET Mail Security se conectará a um servidor proxy para obter atualizações.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

4.2.1.2.3 Conexão à rede

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão. Na maioria dos casos, a conta do sistema local não tem direitos de acesso suficientes para a pasta Imagem, que contém cópias dos arquivos de atualização. Se esse for o caso, insira o nome de usuário e a senha na seção de configuração da atualização ou especifique uma conta na qual o programa acessará o servidor de atualização (Imagem).

Para configurar essa conta, clique na guia **Rede**. A seção **Conectar à rede como** oferece as opções **Conta do sistema** (**padrão**), **Usuário atual** e **Usuário especificado**.



Selecione a opção **Conta do sistema** (**padrão**) para usar a conta do sistema para autenticação. Normalmente, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa seja autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

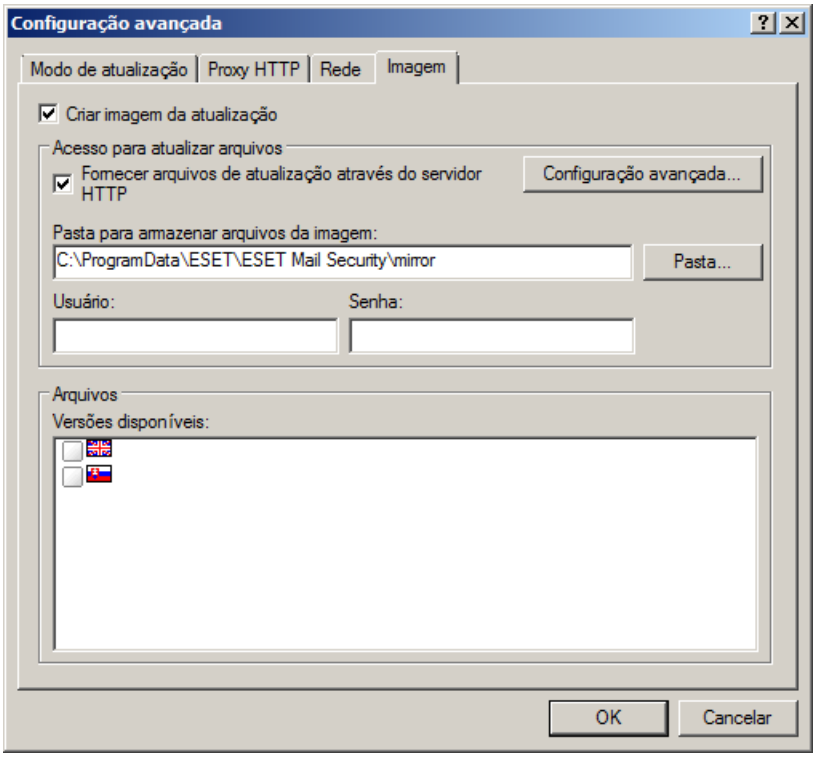
Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação.

Alerta: Quando a opção **Usuário atual** ou **Usuário especificado** estiver ativada, um erro pode ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: nome_domínio\usuário (se for um grupo de trabalho, insira nome do_grupo de trabalho_nome\nome) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

4.2.1.2.4 Criação de cópias de atualização – Imagem

O ESET Mail Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho localizadas na rede. A atualização das estações clientes a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração do servidor local da Imagem podem ser acessadas (após a inserção da chave de licença válida no gerenciador de licenças, localizado na seção Configuração avançada do ESET Mail Security) na seção **Configuração avançada de atualização**: Para acessar essa seção, pressione F5 e clique no botão **Atualizar** na árvore Configuração avançada, depois clique no botão **Configuração...** ao lado de **Configuração avançada de atualização**: e selecione a guia **Imagem**).



A primeira etapa na configuração da Imagem é selecionar a opção Criar imagem de atualização. A seleção dessa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Os métodos de ativação da Imagem estão descritos em detalhes na seção Atualização através da Imagem 90. Por enquanto, observe que há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta...** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome do usuário** e **Senha**. O nome do usuário e a senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Ao configurar a Imagem, também é possível especificar as versões de idioma dos quais se deseja fazer download das cópias de atualização. A configuração da versão de idioma pode ser acessada na seção **Arquivos** - **Versões disponíveis**:.

OBSERVAÇÃO: Não é possível que o banco de dados da proteção anti-spam seja atualizado a partir da imagem. Para obter mais informações sobre como realizar corretamente atualizações do banco de dados da proteção anti-spam, clique aqui 37.

4.2.1.2.4.1 Atualização através da Imagem

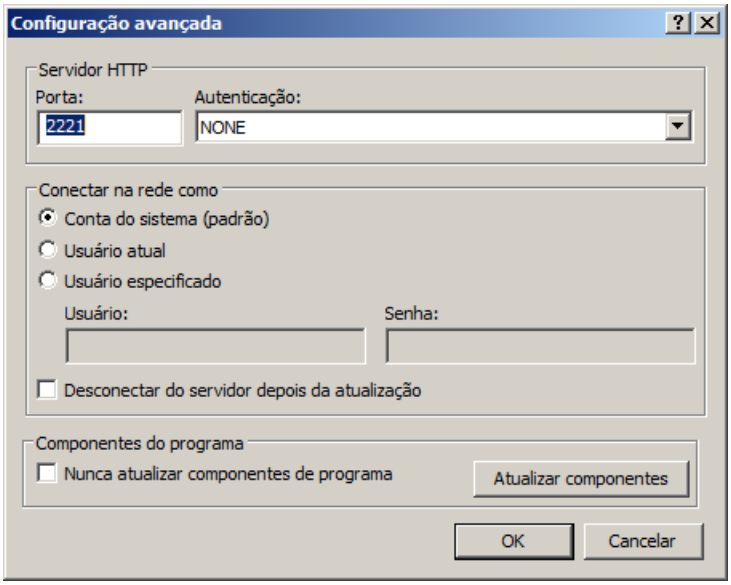
Há dois métodos básicos para configurar a Imagem – a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

Acesso à Imagem utilizando um servidor HTTP interno

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à Imagem utilizando o servidor HTTP, navegue até **Configuração avançada de atualização** (guia **Imagem**) e selecione a opção **Criar imagem da atualização**.

Na seção **Configuração avançada** da guia **Imagem**, é possível especificar a **Porta do servidor** em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **NENHUM**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Alerta: Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET Mail Security que os criou.



Após concluir a configuração da Imagem, vá até as estações de trabalho e adicione um novo servidor de atualização no formato **http://endereço_IP_do_seu_servidor:2221**. Para fazer isso, siga as etapas a seguir:

- Abra a **Configuração avançada** do ESET Mail Security e clique na ramificação **Atualizar**.
- Clique em **Editar...** à direita do menu suspenso **Atualizar servidor** e adicione um novo servidor utilizando o seguinte formato: http://endereço_IP_do_seu_servidor:2221.
- Selecione esse servidor recém-adicionado na lista de servidores de atualização.

Acesso à Imagem por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um local ou em um dispositivo de rede. Ao criar a pasta para a Imagem, é necessário fornecer acesso de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso de "leitura" para todos os usuários que atualizarão o ESET Mail Security a partir da pasta Imagem.

Depois, configure o acesso à Imagem na seção **Configuração avançada de atualização** (guia **Imagem**) desativando a opção **Fornecer arquivos de atualização através do servidor HTTP** . Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário especificar os dados de autenticação para acessar o outro computador. Para especificar os dados de autenticação, abra a Configuração avançada (F5) do ESET Mail Security e clique na ramificação **Atualizar**. Clique no botão **Configuração...** e clique na guia **Rede**. Essa configuração é a mesma para a atualização, conforme descrito na seção Conexão à rede 88.

Após concluir a configuração da Imagem, prossiga até as estações de trabalho e configure \\UNC\PATH como o servidor de atualização. Essa operação pode ser concluída seguindo estas etapas:

- Abra a Configuração avançada do ESET Mail Security e clique em **Atualizar**.
- Clique em **Editar...** ao lado de Atualizar servidor e adicione um novo servidor utilizando *formato \\UNC\PATH*.
- Selecione esse servidor recém-adicionado na lista de servidores de atualização

OBSERVAÇÃO: Para o funcionamento correto, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

4.2.1.2.4.2 Solução de problemas de atualização através da Imagem

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de Imagem são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização na Imagem ou por uma combinação dessas razões citadas. Aqui é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Imagem:

O ESET Mail Security **relata um erro ao conectar a um servidor de imagem** - Provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

O ESET Mail Security **requer um nome de usuário e senha** - Provavelmente provocado provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome de usuário*, além das senhas correspondentes. Se o servidor de Imagem puder ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por "Todos", um nome de usuário e uma senha ainda precisarão ser inseridos na seção de configuração da atualização.

O ESET Mail Security **relata um erro ao conectar a um servidor de imagem** – A comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

4.2.2 Como criar tarefas de atualização

As atualizações podem ser disparadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em Atualizar no menu principal.

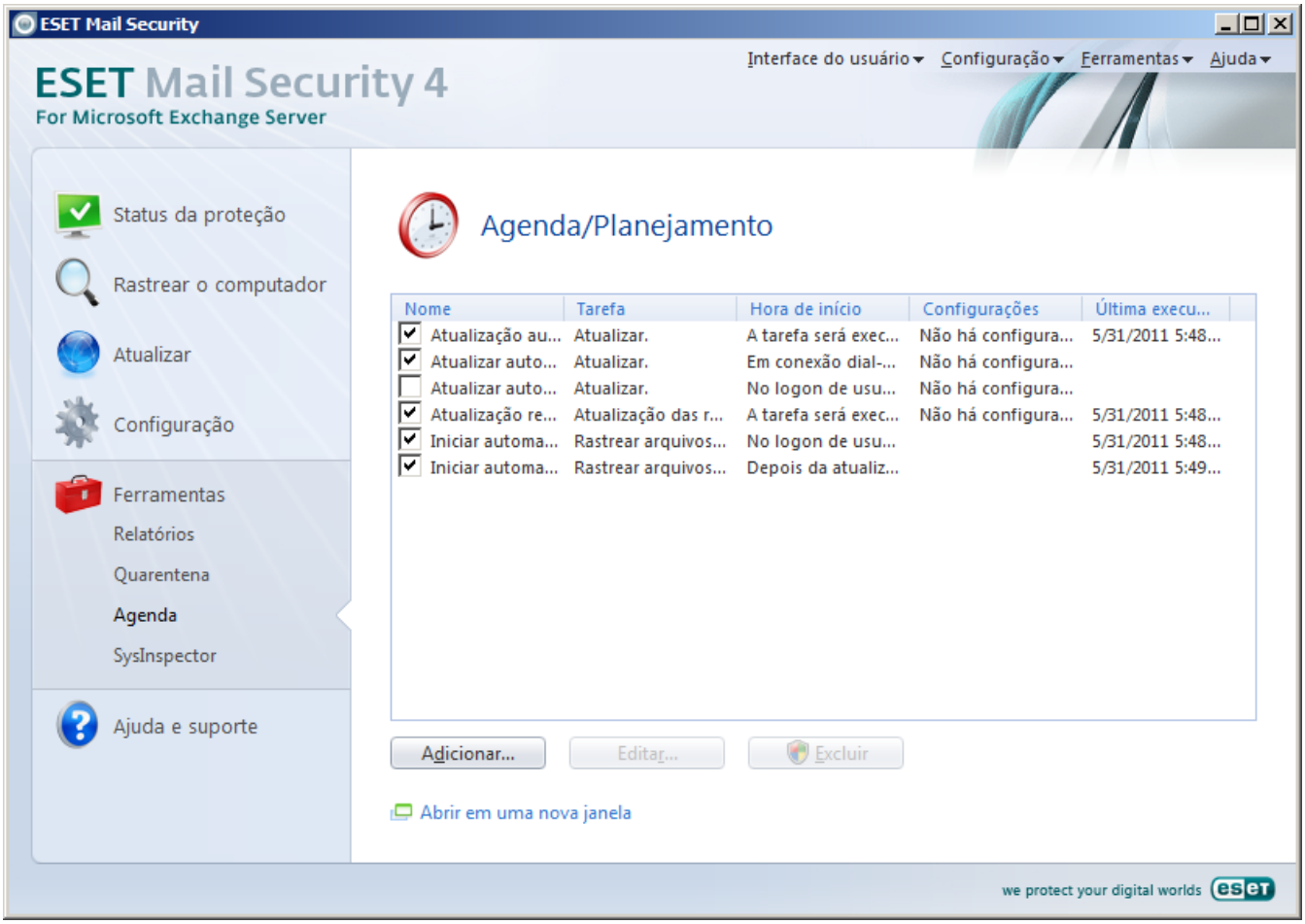
As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET Mail Security:

- **Atualização automática de rotina**
- **Atualizar automaticamente após conexão dial-up**
- **Atualizar automaticamente após logon do usuário**

Cada tarefa de atualização pode ser alterada de acordo com suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda 92.

4.3 Agenda

A Agenda ficará disponível se o Modo avançado no ESET Mail Security estiver ativado. A **Agenda** pode ser encontrada no menu principal do ESET Mail Security em **Ferramentas**. A Agenda contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.



Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Atualização automática de rotina**
- **Atualizar automaticamente após conexão dial-up**
- **Atualizar automaticamente após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após logon do usuário)**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após atualização bem sucedida do banco de dados de assinatura de vírus)**

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

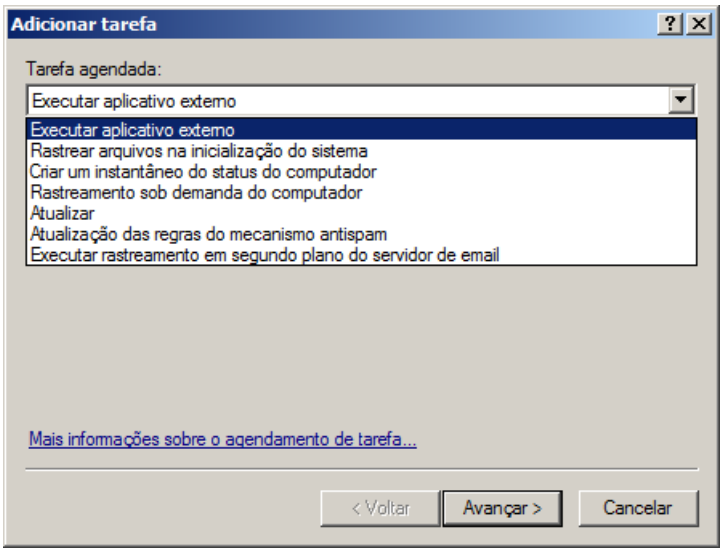
4.3.1 Finalidade do agendamento de tarefas

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

4.3.2 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo**
- **Rastrear arquivos na inicialização do sistema**
- **Criar um snapshot do status do computador**
- **Rastreamento sob demanda do computador**
- **Atualizar**



Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, nós explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada**: selecione **Atualizar**. Clique em **Avançar** e insira o nome da tarefa no campo **Nome da tarefa**: Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento disparado**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. Depois defina a ação a ser adotada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a caixa de rolagem Intervalo da tarefa)

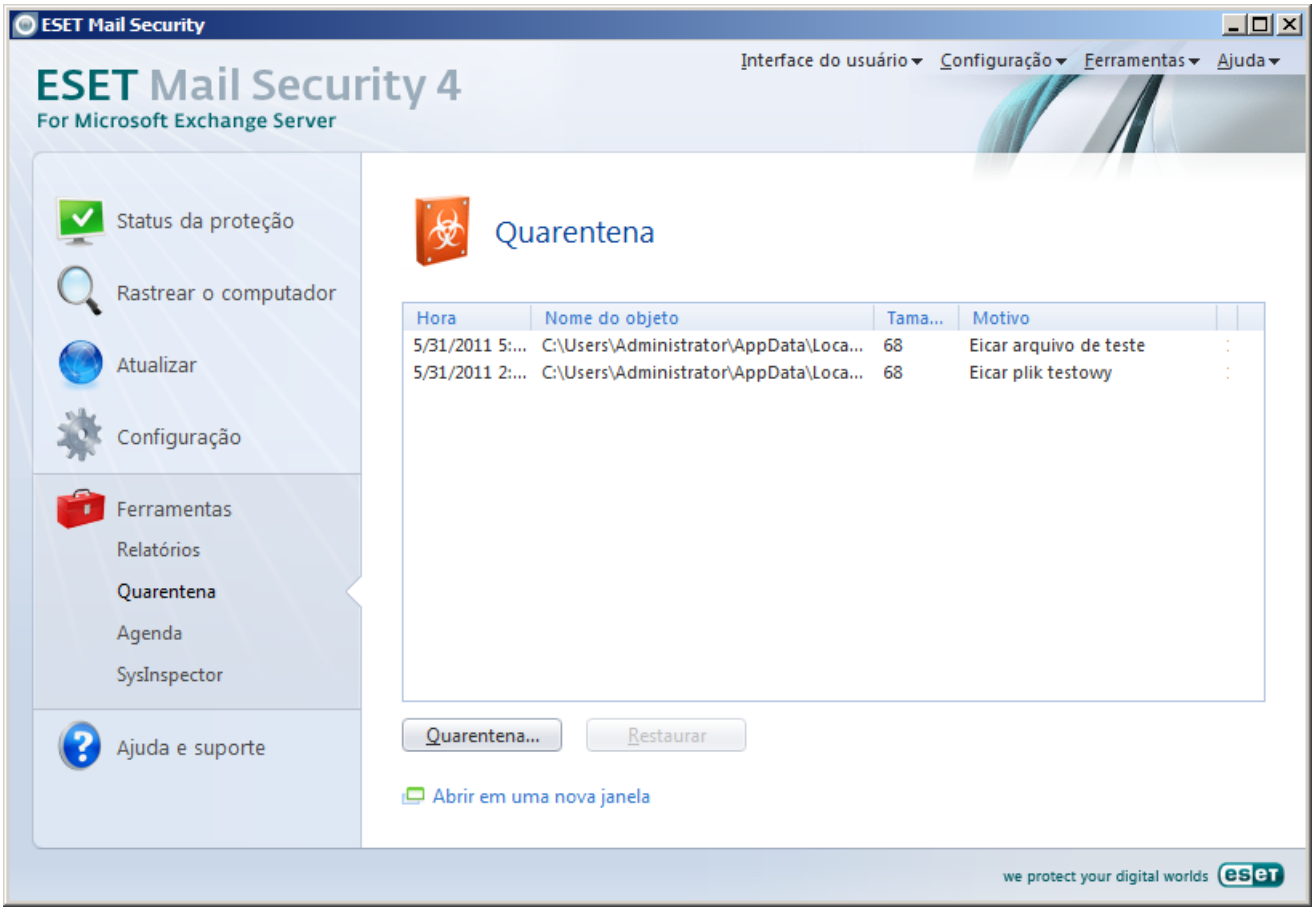
Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual será exibida; a opção **Executar a tarefa com parâmetros específicos** deve ser ativada automaticamente. Clique no botão **Concluir**.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo, que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **OK** na janela **Atualizar perfis**. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

4.4 Quarentena

A principal tarefa da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Mail Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo verificador antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de ameaças da ESET para análise.



Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (**adicionado pelo usuário...**) e o número de ameaças (por exemplo, se ele for um arquivo compactado que contém diversas infiltrações).

4.4.1 Colocação de arquivos em quarentena

O ESET Mail Security coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Quarentena...**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Adicionar...**

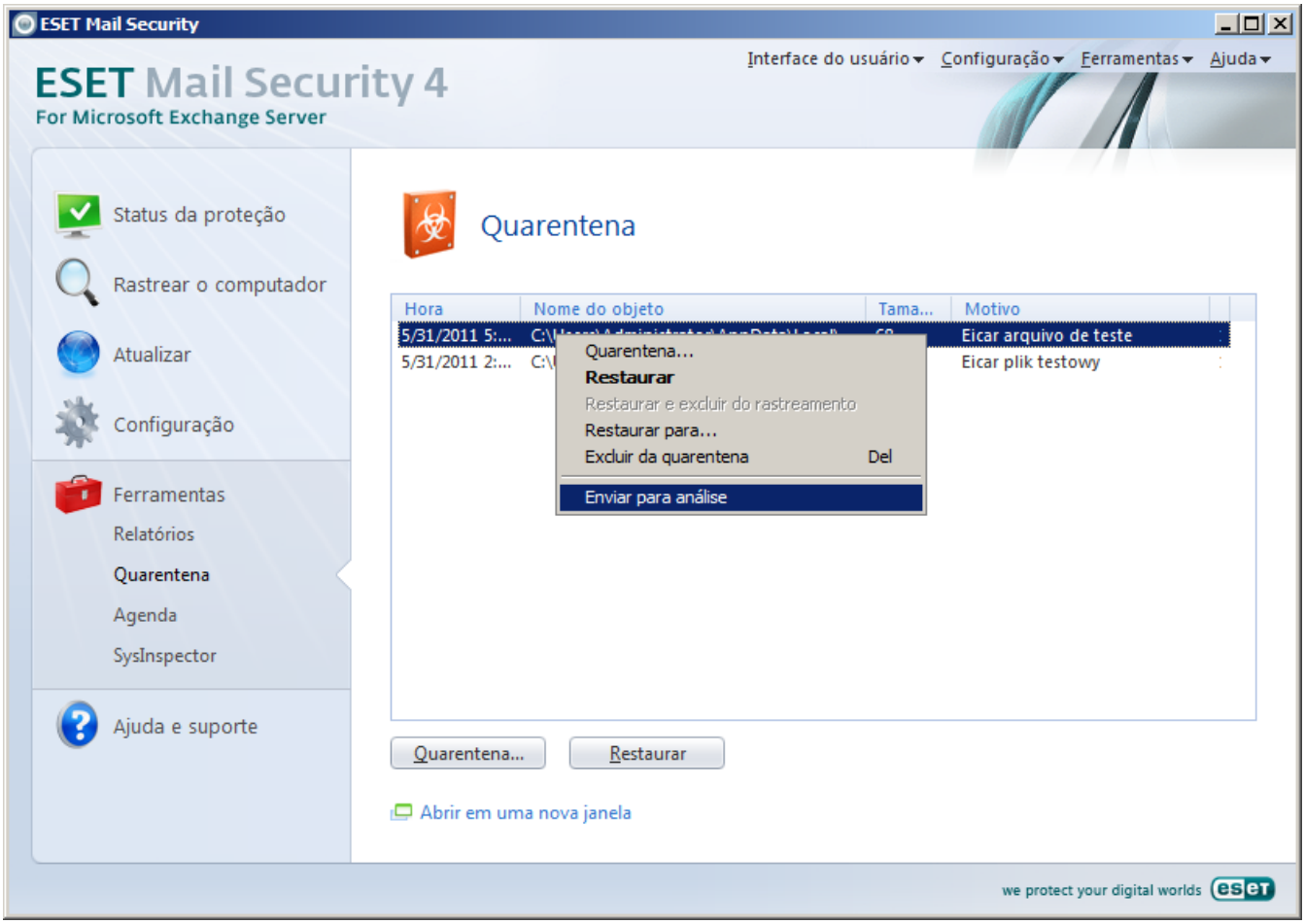
4.4.2 Restauração da Quarentena

Os arquivos colocados em quarentena podem ser restaurados para o local original. Para tanto, use o recurso **Restaurar**. A opção **Restaurar** está disponível no menu de contexto ao clicar com o botão direito do mouse no arquivo em questão na janela Quarentena. O menu de contexto oferece também a opção **Restaurar para**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO: Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

4.4.3 Envio de arquivo da Quarentena

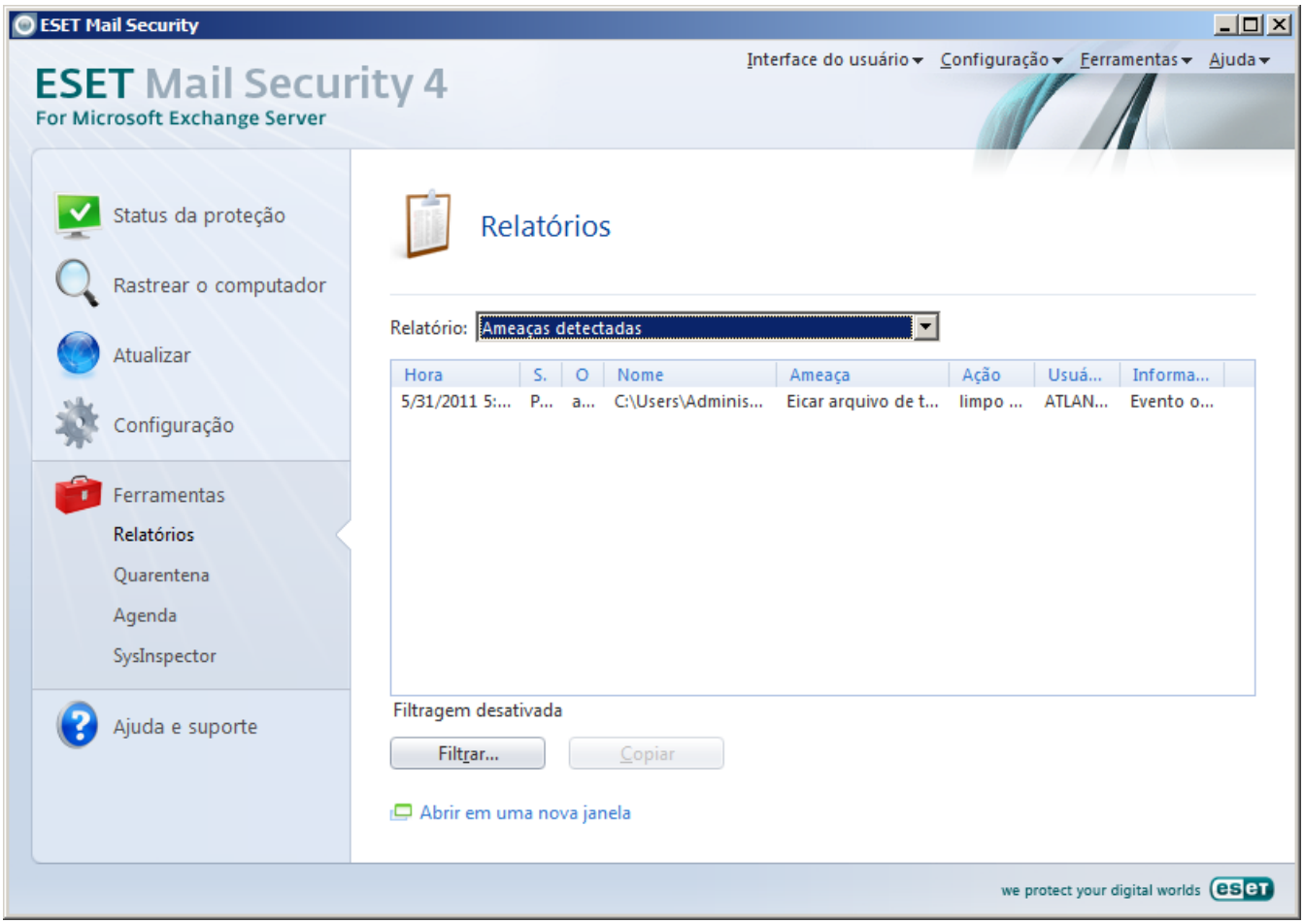
Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de ameças da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.



4.5 Relatórios

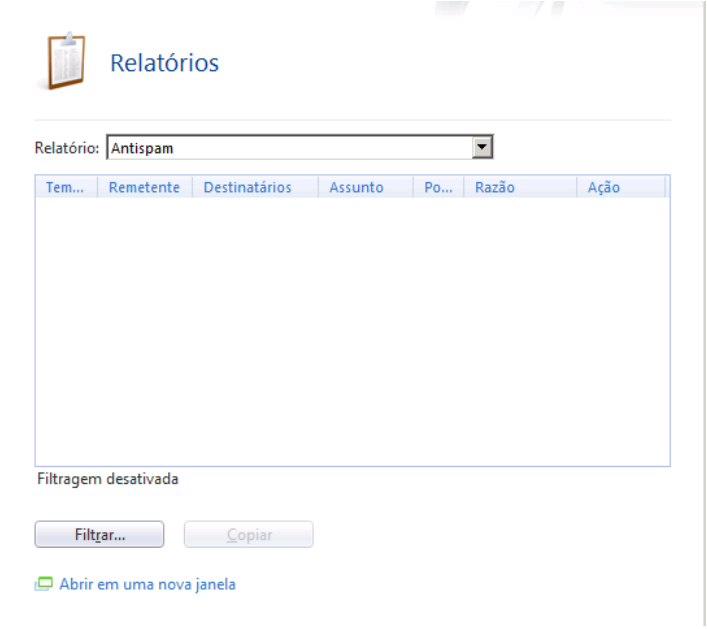
Registra em relatório as informações sobre o armazenamento de eventos importantes: infiltrações detectadas, informações sobre os relatórios de rastreamento sob demanda e scanners residentes e informações sobre o sistema.

Os relatórios da proteção antispam e da lista cinza (encontrados em "outros relatórios" em **Ferramentas** > **Relatórios**) contêm informações detalhadas sobre as mensagens submetidas ao rastreamento e as ações consequentes realizadas nessas mensagens. Os relatórios podem ser muito úteis durante a procura de emails não enviados, tentando saber por que uma mensagem foi marcada como spam, etc.



Antispam

Todas as mensagens classificadas pelo ESET Mail Security como spam ou provável spam são registradas aqui.



Descrição das colunas:

Hora – hora da entrada no relatório antispam

Remetente – endereço do remetente

Destinatário – endereço do destinatário

Assunto – assunto da mensagem

Pontuação – pontuação de spam atribuída à mensagem (no intervalo de 0 a 100)

Motivo – é o indicador que fez com que a mensagem fosse classificada como spam. O indicador exibido é o mais forte. Se desejar ver os outros indicadores, clique duas vezes na entrada. A janela **Motivo** exibirá os indicadores restantes classificados por ordem decrescente por força.

URL com reputação de spam	Os endereços de URL nas mensagens geralmente podem ser uma indicação de spam.
Formatação HTML (Fontes, cores, etc.)	A formatação dos elementos no trecho HTML da mensagem mostra sinais característicos de spam (tipo e tamanho da fonte, cor, etc.)
Truques de spam: Obscurecimento	As palavras típicas de spam tendem a ser disfarçadas utilizando outros caracteres. Um exemplo típico é a palavra "Viagra", que geralmente é grafada como "V1agra" para escapar da detecção anstispam.
Tipo de imagem HTML de spam	As mensagens de spam geralmente têm a forma de imagens como outra estratégia evasiva aplicada contra os métodos de detecção antispam. Essas imagens geralmente contêm links interativos para páginas da Web.
Formatação de URL de host de domínio do serviço	O endereço URL contém o host de domínio do serviço.
Palavra-chave relativa a spam...	A mensagem contém palavras típicas de spam.
Inconsistência no cabeçalho do email	As informações do cabeçalho são alteradas para que pareçam ser de outro remetente.
Vírus	A mensagem contém um anexo suspeito.
Roubo de identidade	A mensagem contém texto típico de mensagens de roubo de identidade.
Réplica	A mensagem contém texto típico de uma categoria de spam destinado a

	oferecer réplicas.
Indicador genérico de spam	Mensagem que contém palavras/caracteres típicos de spam, como "Caro amigo", "olá vencedor", "!!!", etc.
Indicador Ham	Esse é um indicador que tem função oposta aos outros indicadores listados. Ele analisa elementos característicos de mensagens solicitadas regulares. Ele reduz a pontuação geral de spam.
Indicador de spam não específico	A mensagem contém outros elementos de spam, como codificação base64.
Frases personalizadas de spam	Outras frases típicas de spam.
O URL está na lista de proibições	O URL na mensagem está em uma lista de proibições.
O IP %s está na RBL	O endereço IP ... está em uma lista RBL.
O URL %s está na DNSBL	O endereço URL ... está em uma lista DNSBL.
O URL %s está na RBL ou o servidor não está autorizado a enviar email	O endereço URL ... está na lista RBL ou o servidor não tem os privilégios necessários para enviar mensagens. Os endereços que fizerem parte da rota do email serão verificados em relação à lista RBL. O último endereço será testado em relação aos direitos de conectividade a servidores de email públicos. Se for impossível detectar os direitos de conectividade válidos, o endereço está na lista LBL. As mensagem marcadas como spam devido a um indicador LBL têm o seguinte texto informado no campo **Motivo**: "O servidor não está autorizado a enviar email".

Ação – a ação executada na mensagem. Possíveis ações:

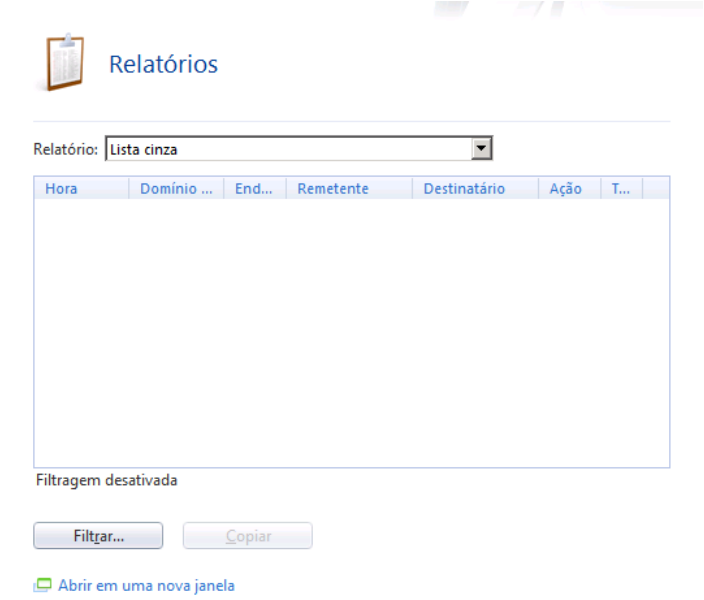
Mantida	Nenhuma ação foi executada na mensagem.
Colocada em quarentena	A mensagem foi movida para a quarentena.
Limpa e enviada à quarentena	O vírus foi removido da mensagem e a mensagem foi colocada em quarentena.
Rejeitada	A mensagem foi recusada e a Resposta de rejeição SMTP 19 foi enviada ao remetente.
Excluída	A mensagem foi excluída usando a remoção silenciosa 19.

Recebida – hora em que a mensagem foi recebida pelo servidor.

OBSERVAÇÃO: Se os emails forem recebidos via servidor de email, a hora nos campos **Hora** e **Recebida** será praticamente idêntica.

Lista cinza

Todas as mensagens que forem classificadas usando o método de lista cinza são registradas nesse relatório.



Descrição das colunas:

Hora – hora da entrada no relatório antispam

Domínio HELO – nome do domínio usado pelo servidor remetente para identificar-se para o servidor destinatário

Endereço IP – endereço IP do remetente

Remetente – endereço do remetente

Destinatário – endereço do destinatário

Ação – pode conter os seguintes status:

Rejeitada	A mensagem recebida foi rejeitada usando o preceito básico de lista cinza (primeira tentativa de entrega)
Rejeitada (não verificada)	A mensagem recebida foi enviada novamente pelo servidor remetente, mas o limite de tempo para recusar a conexão ainda não expirou (**Limite de tempo para recusa da conexão inicial**).
Verificada	A mensagem recebida foi enviada novamente várias vezes pelo servidor remetente, o **Limite de tempo para recusa da conexão inicial** expirou e a mensagem foi verificada e entregue com êxito. Consulte também Agente de transporte 38.

Tempo restante –o tempo restante até que o **Limite de tempo para recusa da conexão inicial** seja atingido

Ameaças detectadas

O relatório de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelos módulos do ESET Mail Security. As informações incluem a hora da detecção, tipo do scanner, tipo do objeto, nome do objeto, nome da infiltração, local, ação realizada e o nome do usuário conectado no momento em que a infiltração foi detectada. Para copiar ou excluir uma ou mais linhas do relatório (ou para excluir um relatório inteiro), use o menu de contexto (clique com o botão direito do mouse no item).

Eventos

O relatório contém informações sobre eventos e erros que ocorreram no programa. Com frequência, informações encontradas aqui podem ajudá-lo a encontrar uma solução para o problema ocorrido no programa.

Rastreamento sob demanda do computador

O relatório do scanner armazena informações com os resultados do rastreamento manual ou programado. Cada

linha corresponde a um rastreamento no computador. Contém as seguintes informações: data e hora do rastreamento, número total de arquivos verificados, infectados e limpos, bem como o status do rastreamento atual.

Em **Rastreamento sob demanda do computador**, clique duas vezes no relatório para exibir seu conteúdo detalhado em uma janela separada.
Use o menu de conteúdo (clique com o botão direito do mouse) para copiar uma ou mais entradas marcadas (em todos os tipos de relatórios).

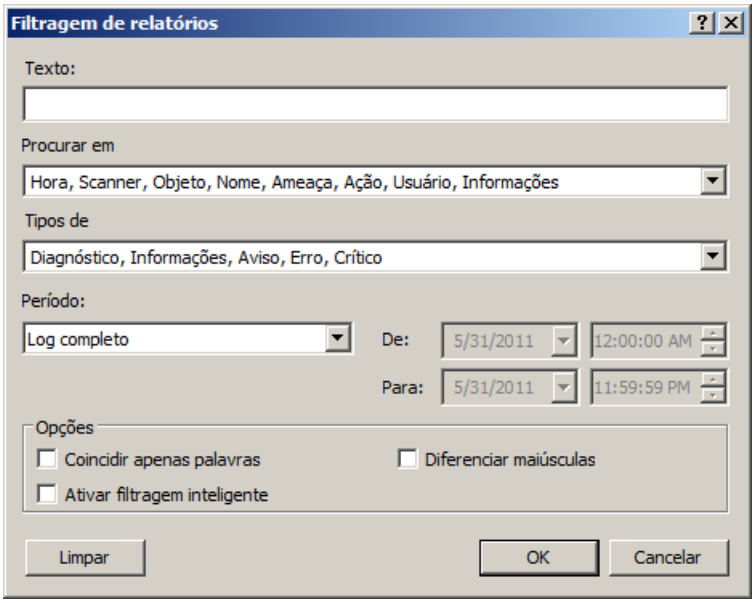
4.5.1 Filtragem de relatórios

A filtragem de relatórios é um recurso útil que o ajuda a encontrar registros nos relatórios, especialmente quando há muitos registros e é difícil encontrar a informação específica que você precisa.

Ao usar a filtragem, digite uma cadeia de caracteres **O que** para filtrar, especificar em quais **colunas procurar**, selecionar os **Tipos de registro** e definir um **Período de tempo** para limitar a quantidade de registros. Ao especificar determinadas opções de filtragem, apenas os registros relevantes (de acordo com as opções de filtragem) serão exibidos na janela **Relatórios** para acesso rápido e fácil.

Para abrir a janela **Filtragem de relatórios**, pressione o botão **Filtrar...** uma vez em **Ferramentas** > **Relatórios** ou use as teclas de atalho Ctrl + Shift + F.

OBSERVAÇÃO: Para pesquisar um registro específico, você pode usar o recurso Localizar no relatório ou em conjunto com a Filtragem de relatórios.



Ao especificar determinadas opções de filtro, apenas os registros relevantes (de acordo com as opções de filtragem) serão exibidos na janela Relatórios. Isso preencherá/limitará a quantidade de registros, fazendo, assim, com que seja mais fácil encontrar exatamente o que você está procurando. Quanto mais específicas forem as opções de filtro usadas, mais limitados serão os resultados.

O que: - Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Somente os registros que contém essa cadeia de caracteres serão exibidos. O restante dos registros não ficará visível para que seja mais fácil visualizar.

Procurar em colunas: - Selecione quais colunas deverão ser consideradas na filtragem. Você pode marcar uma ou mais colunas para usar na filtragem. Por padrão, todas as colunas são marcadas:

- **Hora**
- **Módulo**
- **Evento**
- **Usuário**

Tipos de objetos: - Permite escolher que tipo de registros exibir. É possível escolher um tipo específico de registro, vários tipos ao mesmo tempo ou exibir todos os tipos de registros (por padrão):

- **Diagnóstico**
- **Informações**
- **Alerta**
- **Erro**
- **Crítico**

Período de tempo: - Use esta opção para filtrar registros por um determinado período de tempo. Você pode escolher um dos seguintes:

- **Log completo** (padrão) – não filtra por período, pois mostra todo o relatório
- **Último dia**
- **Última semana**
- **Último mês**
- **Intervalo** – ao selecionar o intervalo, é possível especificar o período de tempo exato (data e hora) para exibir somente os registros que ocorreram no período de tempo especificado.

Além das configurações de filtragem anteriores, há também várias **Opções**:

Coincidir apenas palavras inteiras – Mostra apenas os registros que correspondam à cadeia de caracteres como uma palavra inteira na caixa de texto **O que**.

Diferenciar maiúsculas de minúsculas – Mostra apenas os registros que correspondam à cadeia de caracteres com maiúsculas e minúsculas exatas na caixa de texto **O que**.

Ativar filtragem inteligente – Use essa opção para que o ESET Mail Security execute a filtragem usando seus próprios métodos.

Após terminar de escolher as opções de filtragem, pressione o botão **OK** para aplicar o filtro. A janela **Relatórios** exibirá apenas os registros correspondentes de acordo com as opções do filtro.

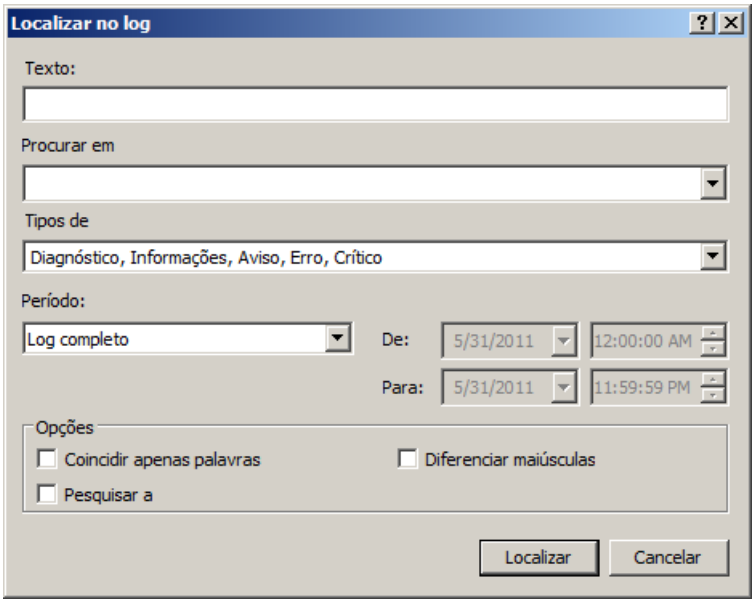
4.5.2 Localizar no log

Além da Filtragem de relatórios 100, é possível usar o recurso de pesquisa nos relatórios e usá-lo independente da filtragem de relatórios. Isso é útil quando você está procurando registros específicos nos relatórios. Assim como a Filtragem de relatórios, este recurso de pesquisa o ajudará a encontrar as informações que está procurando, especialmente quando há muitos registros.

Ao usar Localizar no relatório, você pode digitar uma cadeia de caracteres com **O que** para encontrar, especificar em quais **colunas procurar**, selecionar os **Tipos de registro** e definir um **Período de tempo** para pesquisar apenas por registros que ocorreram nesse período de tempo. Ao especificar determinadas opções de pesquisa, apenas os registros relevantes (de acordo com as opções de filtro) serão pesquisados na janela Relatórios.

Para pesquisar nos relatórios, abra a janela **Localizar no relatório** pressionando as teclas Ctrl + F.

OBSERVAÇÃO: Você pode usar o recurso Localizar no relatório em conjunto com a Filtragem de relatórios 100. Pode limitar primeiro a quantidade de registros usando a Filtragem de relatórios e, em seguida, iniciar a pesquisa somente nos registros filtrados.



O que: - Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Somente os registros que contém essa cadeia de caracteres serão localizados. O restante dos registros será omitido.

Procurar em colunas: - Selecione quais colunas deverão ser consideradas na pesquisa. Você pode marcar uma ou mais colunas para usar na pesquisa. Por padrão, todas as colunas estão marcadas:

- **Hora**
- **Módulo**
- **Evento**
- **Usuário**

Tipos de objetos: - Permite escolher que tipo de registros localizar. Você pode escolher um tipo de registro específico, vários tipos ao mesmo tempo ou pesquisar em todos os tipos de registro (por padrão):

- **Diagnóstico**
- **Informações**
- **Alerta**
- **Erro**
- **Crítico**

Período de tempo: - Use esta opção para localizar registros que ocorreram apenas dentro de determinado período de tempo. Você pode escolher um dos seguintes:

- **Log completo** (padrão) – não pesquisa no período de tempo, mas em todo o relatório
- **Último dia**
- **Última semana**
- **Último mês**
- **Intervalo** – ao selecionar o intervalo, é possível especificar o período de tempo exato (data e hora) para pesquisar somente os registros que ocorreram no período de tempo especificado.

Além das configurações de localização anteriores, há também várias **Opções**:

Coincidir apenas palavras inteiras – Localiza apenas os registros que correspondam à cadeia de caracteres como uma palavra inteira na caixa de texto **O que**.

Diferenciar maiúsculas de minúsculas – Localiza apenas os registros que correspondam à cadeia de caracteres com maiúsculas e minúsculas exatas na caixa de texto **O que**.

Pesquisar acima – Pesquisa da posição atual para cima.

Após configurar as opções de pesquisa, clique no botão **Localizar** para iniciar a pesquisa. A pesquisa pára quando encontrar o primeiro registro correspondente. Clique no botão **Localizar** novamente para continuar pesquisando. A pesquisa ocorre de cima para baixo nos Relatórios, começando na posição atual (registro destacado).

4.5.3 Manutenção de relatórios

A configuração de relatórios do ESET Mail Security pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Relatórios**. Você pode especificar as seguintes opções para relatórios:

- **Excluir registros automaticamente**: As entradas do relatório mais antigas que o número de dias especificado serão automaticamente excluídas
- **Otimizar automaticamente relatórios**: Ativa a desfragmentação automática de relatórios se a porcentagem especificada de relatórios não utilizados foi excedida.
- **Detalhamento mínimo de registro em relatório**: Especifica o nível de detalhamento de registro em relatório. Opções disponíveis:

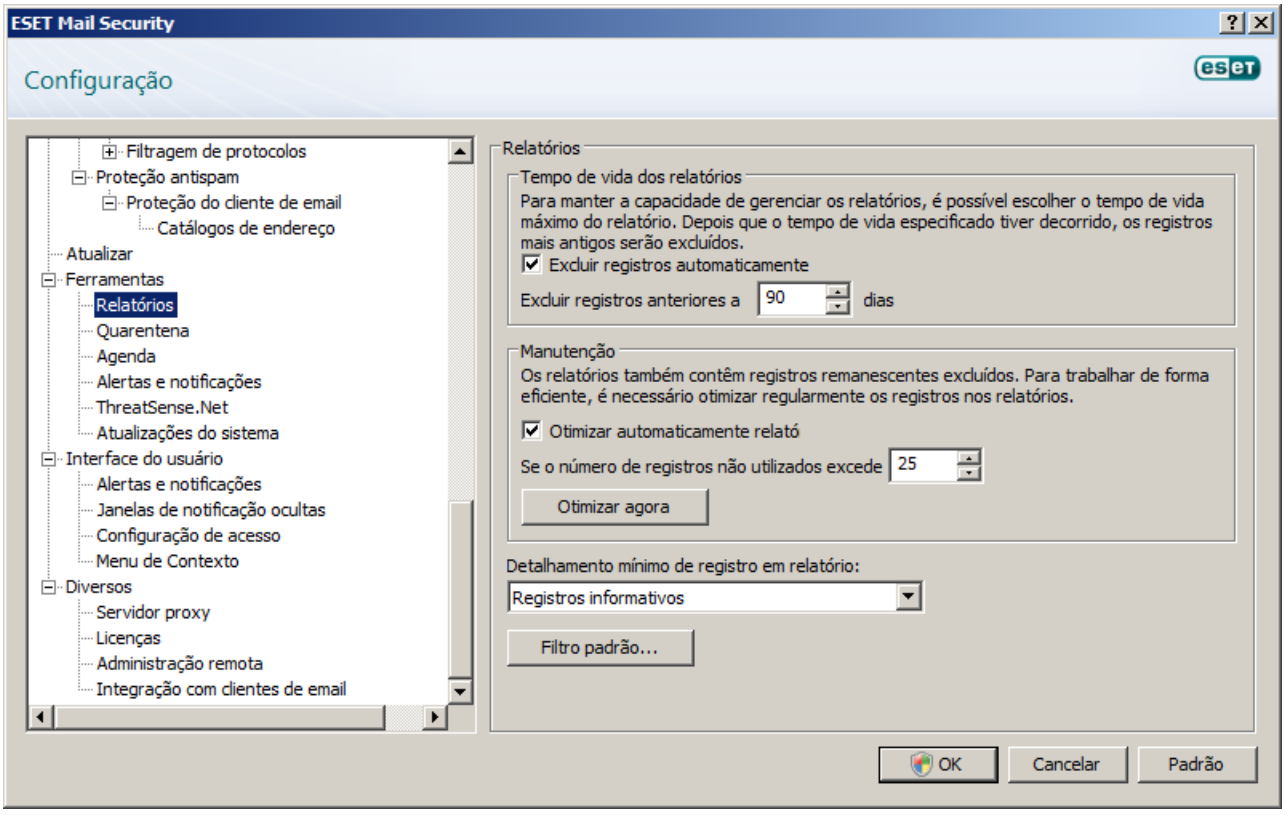
- **Registros de diagnóstico** – Registra as informações necessárias para ajustar o programa e todos os registros mencionados anteriormente

- **Registros informativos** – Registra as mensagens informativas, incluindo atualizações bem-sucedidas e todos os registros mencionados anteriormente

- **Avisos** – Registra mensagens de erros críticos e de avisos

- **Erros** – Somente as mensagens do tipo "Erro ao fazer download de arquivo" e erros críticos serão registrados

- **Avisos críticos** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc.)



4.6 ESET SysInspector

4.6.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada em soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões são idênticas em função e têm os mesmos controles de programa. A única diferença é como os resultados são gerenciados. As versões integrada e separada permitem exportar snapshots do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os snapshots do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator). Para obter mais informações, consulte a seção ESET SysInspector como parte do ESET Mail Security 115.

Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

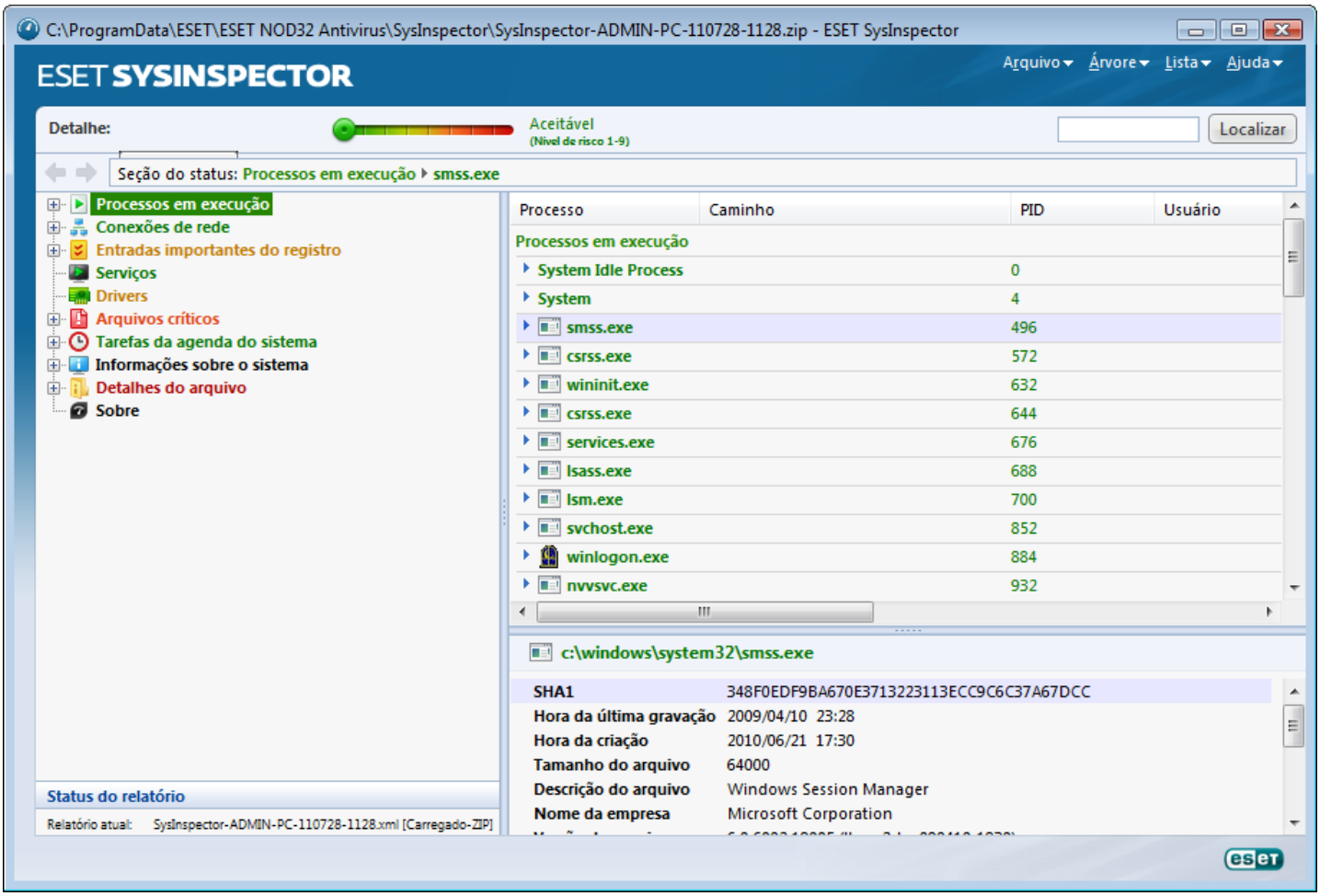
4.6.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo *SysInspector.exe* obtido por download no site da ESET. Se você já tiver uma das soluções ESET Security instalada, poderá executar o ESET SysInspector diretamente do Menu Iniciar (**Programas** > **ESET** > **ESET Mail Security**).

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos, dependendo do hardware e dos dados a serem coletados.

4.6.2 Interface do usuário e uso do aplicativo

Para facilitar o uso, a janela principal é dividida em quatro seções: Controles do programa, localizados na parte superior da janela principal, a janela de navegação à esquerda, a janela de descrição à direita e no centro, e a janela de detalhes à direita, na parte inferior da janela principal. A seção Status do relatório lista os parâmetros básicos de um relatório (filtro usado, tipo do filtro, se o relatório é resultado de uma comparação, etc.).



4.6.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um relatório armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um relatório **Adequado para envio**. Neste formulário, o relatório omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela principal, para que seja mais fácil trabalhar com estas informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe menos detalhes usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para solucionar problemas muito específicos.

Filtragem de itens

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver totalmente à esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante totalmente à direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens classificados como risco 6 a 9 podem ser um risco à segurança. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrar esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Pesquisar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, verifique se os arquivos são realmente perigosos ou desnecessários.

4.6.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou, como alternativa, clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do relatório. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo e o nível de risco do arquivo.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do

arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como Serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de tarefas do Windows em um intervalo/horário especificado.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas e direitos do usuário.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista de módulos do programa.

4.6.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	abre o relatório existente
Ctrl+S	salva os relatórios criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	aceitável, nível de risco 1-9, os itens são exibidos

2	aceitável, nível de risco 2-9, os itens são exibidos
3	aceitável, nível de risco 3-9, os itens são exibidos
4, U	desconhecido, nível de risco 4-9, os itens são exibidos
5	desconhecido, nível de risco 5-9, os itens são exibidos
6	desconhecido, nível de risco 6-9, os itens são exibidos
7, B	perigoso, nível de risco 7-9, os itens são exibidos
8	perigoso, nível de risco 8-9, os itens são exibidos
9	perigoso, nível de risco 9, os itens são exibidos
-	diminui o nível de risco
+	aumenta o nível de risco
Ctrl+9	modo de filtragem, nível igual ou superior
Ctrl+O	modo de filtragem, somente nível igual

Exibir

Ctrl+5	exibição por fornecedor, todos os fornecedores
Ctrl+6	exibição por fornecedor, somente Microsoft
Ctrl+7	exibição por fornecedor, todos os outros fornecedores
Ctrl+3	exibe detalhes completos
Ctrl+2	exibe detalhes da mídia
Ctrl+1	exibição básica
Backspace	move um passo para trás
Espaço	move um passo para a frente
Ctrl+W	expande a árvore
Ctrl+Q	recolhe a árvore

Outros controles

Ctrl+T	vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	exibe informações básicas sobre um item
Ctrl+A	exibe informações completas sobre um item
Ctrl+C	copia a árvore do item atual
Ctrl+X	copia itens
Ctrl+B	localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	abre a entrada correspondente no editor do registro
Ctrl+Z	copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	alterna para o campo de pesquisa
Ctrl+D	fecha os resultados da pesquisa
Ctrl+E	executa script de serviços

Comparação

Ctrl+Alt+O	abre o relatório original/comparativo
Ctrl+Alt+R	cancela a comparação
Ctrl+Alt+1	exibe todos os itens
Ctrl+Alt+2	exibe apenas os itens adicionados; o relatório mostrará os itens presentes no relatório atual
Ctrl+Alt+3	exibe apenas os itens removidos; o relatório mostrará os itens presentes no relatório anterior
Ctrl+Alt+4	exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	exibe apenas as diferenças entre os relatórios
Ctrl+Alt+C	exibe a comparação
Ctrl+Alt+N	exibe o relatório atual
Ctrl+Alt+P	exibe o relatório anterior

Diversos

F1	exibe a ajuda
Alt+F4	fecha o programa
Alt+Shift+F4	fecha o programa sem perguntar
Ctrl+I	estatísticas de relatórios

4.6.2.3 Comparar

O recurso Comparar permite que o usuário compare dois relatórios existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os relatórios. Ele é adequado se você deseja manter controle das alterações no sistema; é uma ferramenta útil para detectar a atividade de código malicioso.

Após ser iniciado, o aplicativo criará um novo relatório que será exibido em uma nova janela. Navegue até **Arquivo** > **Salvar relatório** para salvar um relatório em um arquivo. Os relatórios podem ser abertos e visualizados posteriormente. Para abrir um relatório existente, utilize o menu **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um relatório de cada vez.

O benefício de comparar dois relatórios é que você pode visualizar um relatório ativo no momento e um relatório salvo em um arquivo. Para comparar relatórios, utilize a opção **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O relatório selecionado será comparado com o relatório ativo na janela principal do programa. O relatório comparativo exibirá apenas as diferenças entre esses dois relatórios.

OBSERVAÇÃO: Caso compare dois relatórios, selecione **Arquivo** > **Salvar relatório** e salve-o como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir este arquivo posteriormente, os relatórios contidos serão comparados automaticamente.

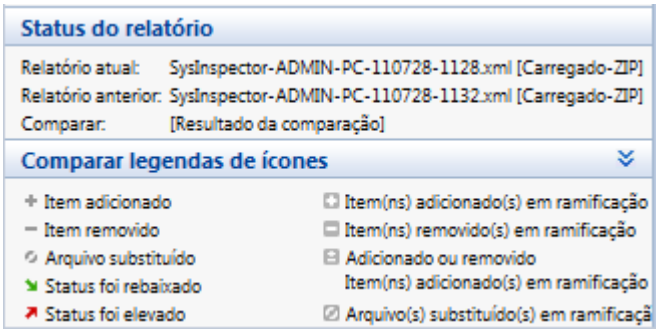
Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os relatórios comparados.

Os itens marcados por um – apenas podem ser encontrados no relatório ativo e não estavam presentes no relatório comparativo aberto. Os itens marcados por um + estavam presentes apenas no relatório aberto e estavam ausentes no relatório ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- + novo valor, não presente no relatório anterior
- a seção de estrutura em árvore contém novos valores
- – valor removido, presente apenas no relatório anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no relatório anterior
- o nível de risco aumentou / era menor no relatório anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos relatórios que estão sendo comparados.



Qualquer relatório comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois relatórios, navegue até **Arquivo** > **Comparar relatórios**. O programa criará um relatório comparativo mostrando as diferenças entre os relatórios.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

4.6.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar um relatório diretamente a partir da linha de comando sem executar a GUI
/privacy	gerar um relatório excluindo informações confidenciais
/zip	armazenar o relatório resultante diretamente no disco em um arquivo compactado
/silent	ocultar a exibição da barra de progresso da geração de relatórios
/help, /?	exibir informações sobre os parâmetros da linha de comando

Exemplos

Para carregar um relatório específico diretamente no navegador, use: *SysInspector.exe "c:\clientlog.xml"*
Para gerar um relatório em um local atual, use: *SysInspector.exe /gen*
Para gerar um relatório em uma pasta específica, use: *SysInspector.exe /gen="c:\folder\"*
Para gerar um relatório em um arquivo/local específico, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para gerar um relatório que exclua informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dois relatórios, use: *SysInspector.exe "current.xml" "original.xml"*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

4.6.4 Script de serviços

O script de serviços é uma ferramenta que oferece ajuda a clientes que usam o ESET SysInspector, removendo facilmente objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o relatório modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As alterações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador esteja infectado por um vírus que não é detectado pelo seu programa antivírus, siga as instruções passo-a-passo a seguir:

- Execute o ESET SysInspector para gerar um novo snapshot do sistema.
- Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Ctrl e selecione o último item para marcar todos os itens.
- Clique com o botão direito nos objetos selecionados e selecione a opção do menu de contexto **Exportar as seções selecionadas para script de serviços**.
- Os objetos selecionados serão exportados para um novo relatório.
- Esta é a etapa mais crucial de todo o procedimento: abra o novo relatório e altere o atributo – para + para todos os objetos que desejar remover. Certifique-se de não marcar nenhum arquivo/objeto importante do sistema operacional.
- Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o seu script.
- Clique em **OK** para executar o script.

4.6.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois relatórios estiverem sendo comparados.

4.6.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, há informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do relatório (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

O5) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

O6) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de O byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

O7) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

O8) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando você executar o script, os drivers selecionados serão interrompidos. Observe que alguns drivers não permitirão eles mesmos a interrupção.

O9) Arquivos críticos

Esta seção contém informações sobre os arquivos críticos para o sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos, ou serão restaurados seus valores padrão originais.

4.6.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma caixa de diálogo confirmará que o script foi executado com sucesso.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

4.6.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um relatório?

O ESET SysInspector pode criar um relatório da configuração do computador. Para salvar um relatório, selecione **Arquivo** > **Salvar relatório** no menu principal. Os relatórios são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*\, com uma convenção de nomenclatura de arquivos de "SysInpsector-%NOMECOMPUTADOR%-AAMMDD-HHMM.XML". Você pode alterar o local e o nome do relatório para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o relatório do ESET SysInspector?

Para visualizar um relatório criado pelo ESET SysInspector, execute o programa e selecione **Arquivo** > **Abrir relatório** no menu principal. Você também pode arrastar e soltar relatórios no aplicativo ESET SysInspector. Se você precisar visualizar os relatórios do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os relatórios para visualização. Por motivo de segurança, os Windows Vista/7 podem não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do relatório? E um SDK?

Atualmente, não há uma especificação para o relatório nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro deles.

Um nível de risco "6 – Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles também podem examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporta como um rootkit, o usuário será exposto ao risco de danos ou roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validando usando essas informações. Se uma assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Se o arquivo CAT pertinente for encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Arquivos de Programas\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

4.6.6 ESET SysInspector como parte do ESET Mail Security

Para abrir a seção do ESET SysInspector no ESET Mail Security, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com snapshots: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar... ou excluir snapshots, utilize os botões correspondentes localizados abaixo da lista de snapshots na janela do ESET SysInspector. Essas opções também estão disponíveis no menu de contexto. Para exibir o snapshot do sistema selecionado, utilize a opção do menu de contexto **Exibir**. Para exportar o snapshot selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**.

Abaixo, há uma descrição detalhada das opções disponíveis:

- **Comparar** – permite comparar dois relatórios existentes. Ela é adequada se você desejar controlar alterações entre o relatório atual e um relatório anterior. Para que essa opção entre em vigor, é necessário selecionar dois snapshots a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para localizar o progresso de criação do snapshot (do snapshot gerado no momento), veja a coluna **Status**. Todos os snapshots concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** - Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

4.7 ESET SysRescue

ESET SysRescue é um utilitário que permite criar um disco inicializável que contém uma das soluções ESET Security - pode ser o ESET NOD32 Antivirus, ESET Smart Security ou até mesmo alguns dos produtos orientados a servidor. A principal vantagem do ESET SysRescue é o fato de que a solução ESET Security é executada de maneira independente do sistema operacional host, ao mesmo tempo em que possui um acesso direto ao disco e a todo o sistema de arquivos. Isso possibilita remover as infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

4.7.1 Requisitos mínimos

O ESET SysRescue funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista.

O Windows PE faz parte dos pacotes gratuito do Windows Automated Installation Kit (Windows AIK) ou Windows Assessment and Deployment Kit (Windows ADK), portanto o Windows AIK ou ADK deve ser instalado antes da criação do ESET SysRescue (<%http://go.eset.eu/AIK%>) ou (<%http://go.eset.eu/ADK%>). Qual desses kits deverá ser instalado em seu sistema dependerá da versão do sistema operacional que você está executando. Devido ao suporte da versão de 32 bits do Windows PE, é necessário usar o pacote de instalação de 32 bits da solução ESET Security ao criar o ESET SysRescue em sistemas de 64 bits. O ESET SysRescue é compatível com o Windows AIK 1.1 e posteriores, bem como com o Windows ADK.

OBSERVAÇÃO: Como o Windows AIK tem mais de 1 GB em tamanho e o Windows ADK tem 1,3 GB em tamanho, é necessária uma conexão com a internet de alta velocidade para um download perfeito.

O ESET SysRescue está disponível em soluções ESET Security versão 4.0 e posteriores.

O ESET SysRescue écompatível com os seguintes sistemas operacionais:

- Windows Server 2003 Service Pack 1 com KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

O Windows AIK é compatível com:

- Windows Server 2003
- Windows Server 2008

O Windows ADK é compatível com:

- Windows Server 2012

4.7.2 Como criar o CD de restauração

Para iniciar o assistente do ESET SysRescue, clique em **Iniciar** > **Programas** > **ESET** > **ESET Mail Security** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK ou ADK e de um dispositivo adequado para a criação da mídia de inicialização. Se o Windows AIK ou Windows ADK não estiver instalado no computador (ou estiver corrompido ou instalado incorretamente), o assistente dará a opção de instalá-lo ou de inserir o caminho para a pasta do Windows AIK (<%http://go.eset.eu/AIK%>) ou Windows ADK (<%http://go.eset.eu/ADK%>).

OBSERVAÇÃO: Como o Windows AIK tem mais de 1 GB em tamanho e o Windows ADK tem 1,3 GB em tamanho, é necessária uma conexão com a internet de alta velocidade para um download perfeito.

Na próxima etapa 116, selecione a mídia de destino em que o ESET SysRescue estará localizado.

4.7.3 Seleção de alvos

Além de CD/DVD/USB, você pode escolher salvar o ESET SysRescue em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VMWare ou VirtualBox).

Se você selecionar USB como a mídia-alvo, a reinicialização pode não funcionar em determinados computadores. Algumas versões de BIOS podem relatar problemas com o BIOS – comunicação com o gerenciador de inicialização (por exemplo, no Windows Vista), e a inicialização é encerrada com a seguinte mensagem de erro:

```
arquivo: \boot\bcd
status: 0xc000000e
informações: an error occurred while attemping to read the boot configuration data (ocorreu um erro ao tentar ler os d
```

Se você encontrar essa mensagem, recomendamos selecionar o CD, em vez da mídia USB.

4.7.4 Configurações

Antes de iniciar a criação do ESET SysRescue, o assistente de instalação exibirá os parâmetros de compilação na última etapa do assistente do ESET SysRescue. Esses parâmetros podem ser alterados clicando no botão **Alterar...**. As opções disponíveis incluem:

- Pastas 116
- Antivírus ESET 117
- Avançado 117
- Protoc. Internet 117
- Dispositivo USB inicializável 118 (quando o dispositivo USB de destino estiver selecionado)
- Gravação 118 (quando a unidade de CD/DVD de destino estiver selecionada)

O botão **Criar** estará inativo se nenhum pacote de instalação MSI for especificado ou se nenhuma solução ESET Security estiver instalada no computador. Para selecionar um pacote de instalação, clique no botão **Alterar** e vá para a guia **Antivírus ESET**. Além disso, se você não preencher o nome de usuário e a senha (**Alterar** > **Antivírus ESET**), o botão **Criar** estará acinzentado.

4.7.4.1 Pastas

A **Pasta temporária** é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

Pasta ISO é uma pasta, em que o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas das pastas aqui estão localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode ser encerrada prematuramente devido a espaço livre em disco insuficiente.

Aplicativos externos - Permite especificar os programas adicionais que serão executados ou instalados após a inicialização a partir de uma mídia do ESET SysRescue.

Incluir aplicativos externos - Permite adicionar programas externos à compilação do ESET SysRescue.

Pasta selecionada - Pasta na qual os programas a serem adicionados ao disco do ESET SysRescue estão localizados.

4.7.4.2 Antivírus ESET

Para criação do CD do ESET SysRescue, é possível selecionar duas fontes de arquivos da ESET para serem utilizadas pelo compilador.

Pasta ESS/EAV - Arquivos já contidos na pasta na qual a solução ESET Security está instalada no computador.

Arquivo MSI - Os arquivos contidos no instalador do MSI são usados.

A seguir, você pode escolher atualizar o local dos arquivos (.nup). Geralmente, a opção padrão **Pasta ESS/EAV/ Arquivo MSI** está definida. Em alguns casos, uma **Pasta atualiz** personalizada pode ser escolhida, p.ex., para usar uma versão mais recente ou mais antiga do banco de dados de assinatura de vírus.

É possível utilizar uma das seguintes fontes de nome de usuário e senha:

ESS/EAV instalado - O nome de usuário e a senha são copiados da solução ESET Security instalada no momento.

Do usuário - O nome de usuário e a senha digitados nas caixas de texto correspondentes serão utilizados.

OBSERVAÇÃO: O ESET Security no CD do ESET SysRescue é atualizado na Internet ou na solução ESET Security instalada no computador em que o CD do ESET SysRescue for executado.

4.7.4.3 Configurações avançadas

A guia **Avançado** permite otimizar o CD do ESET SysRescue de acordo com o tamanho da memória do computador. Selecione **576 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 576 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Na seção **Drivers externos**, é possível inserir drivers para o seu hardware específico (geralmente adaptador de rede). Embora o WinPE seja baseado no Windows Vista SP1, que suporta hardware de larga escala, algumas vezes o hardware não é reconhecido. Isso requer que o driver seja adicionado manualmente. Há duas maneiras de inserir o driver em uma compilação do ESET SysRescue – manualmente (botão **Adicionar**) e automaticamente (botão **Pesquisa auto**). No caso de inclusão manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). No caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador específico. Recomendamos usar a inclusão automática apenas se o ESET SysRescue for usado em um computador com o mesmo adaptador de rede usado no computador em que o CD do ESET SysRescue foi criado. Durante a criação, o driver do ESET SysRescue é inserido na compilação para que você não precise procurá-lo depois.

4.7.4.4 Protocolo da Internet

Esta seção permite configurar as informações básicas de rede e as conexões predefinidas após o ESET SysRescue.

Selecione **Endereço IP privado autom.** para obter o endereço IP automaticamente do servidor DHCP (Dynamic Host Configuration Protocol).

Alternativamente, esta conexão de rede pode usar um endereço IP especificado manualmente (também conhecido como IP estático). Selecione **Personalizado** para configurar os ajustes de IP correspondentes. Se selecionar esta opção, é necessário especificar um **Endereço IP** e, para conexões de rede e de banda larga, uma **Másc subrede**. Em **Serv. DNS prefer.** e **Serv. DNS altern.**, digite os endereços dos servidores de DNS primário e secundário.

4.7.4.5 Dispositivo USB inicializável

Se você selecionou o dispositivo USB como mídia de destino, é possível selecionar uma das mídias USB disponíveis na guia **Dispositivo USB inicializável** (caso haja mais dispositivos USB).

Selecione o **Dispositivo** alvo apropriado em que o ESET SysRescue será instalado.

Alerta: O dispositivo USB selecionado será formatado durante o processo de criação do ESET SysRescue. Todos os dados no dispositivo serão excluídos.

Se escolher a opção **Formato rápido**, a formatação remove todos os arquivos da partição, mas não procura setores corrompidos no disco. Use esta opção se seu dispositivo USB tiver sido formatado anteriormente e você tiver certeza de que não está danificado.

4.7.4.6 Gravar

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia **Gravar**.

Excluir arquivo ISO - Marque essa opção para excluir o arquivo ISO temporário após o CD do ESET SysRescue ser criado.

Exclusão ativada - Permite selecionar o apagamento rápido e concluí-lo.

Dispositivo de gravação - Selecione a unidade a ser utilizada para gravação.

Aviso: Essa é a opção padrão. Se um CD/DVD regravável for usado, todos os dados contidos no CD/DVD serão apagados.

A seção Mídia contém informações sobre a mídia no seu dispositivo de CD/DVD.

Velocidade de gravação - Selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser considerados na seleção da velocidade da gravação.

4.7.5 Trabalhar com o ESET SysRescue

Para o CD/DVD/USB de restauração funcionar de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Como alternativa, você pode usar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas F9 ou F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização da mídia, a solução ESET Security será iniciada. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos do programa presentes na versão padrão da solução ESET Security não são necessários; a lista é limitada ao **Rastreamento do computador**, **Atualizar** e algumas seções na **Configuração**. A capacidade de atualizar o banco de dados de assinaturas de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastreamento do computador.

4.7.5.1 Utilização do ESET SysRescue

Suponha que os computadores na rede tenham sido infectados por um vírus que modifica os arquivos executáveis (.exe). A solução ESET Security é capaz de limpar todos os arquivos infectados, exceto *explorer.exe*, que não pode ser limpo, mesmo no modo de segurança. Isso ocorre porque o *explorer.exe*, como um dos processos essenciais do Windows, também é iniciado no modo de segurança. A solução ESET Security não poderia realizar ações com o arquivo e ele permaneceria infectado.

Nesse tipo de cenário, seria possível usar o ESET SysRescue para solucionar o problema. O ESET SysRescue não requer componentes do sistema operacional host, portanto ele pode processar (limpar, excluir) qualquer arquivo no disco.

4.8 Opções da interface do usuário

As opções de configuração da interface do usuário no ESET Mail Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** da árvore Configuração avançada do ESET Mail Security.

Na seção **Elementos da interface do usuário**, a opção **Modo avançado** proporciona aos usuários a capacidade de alternar para o Modo avançado. O Modo avançado exibe as configurações mais detalhadas e os controles adicionais do ESET Mail Security.

A opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do computador ou provocarem outros problemas. A interface gráfica também pode precisar ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais usados para leitura do texto exibido na tela.

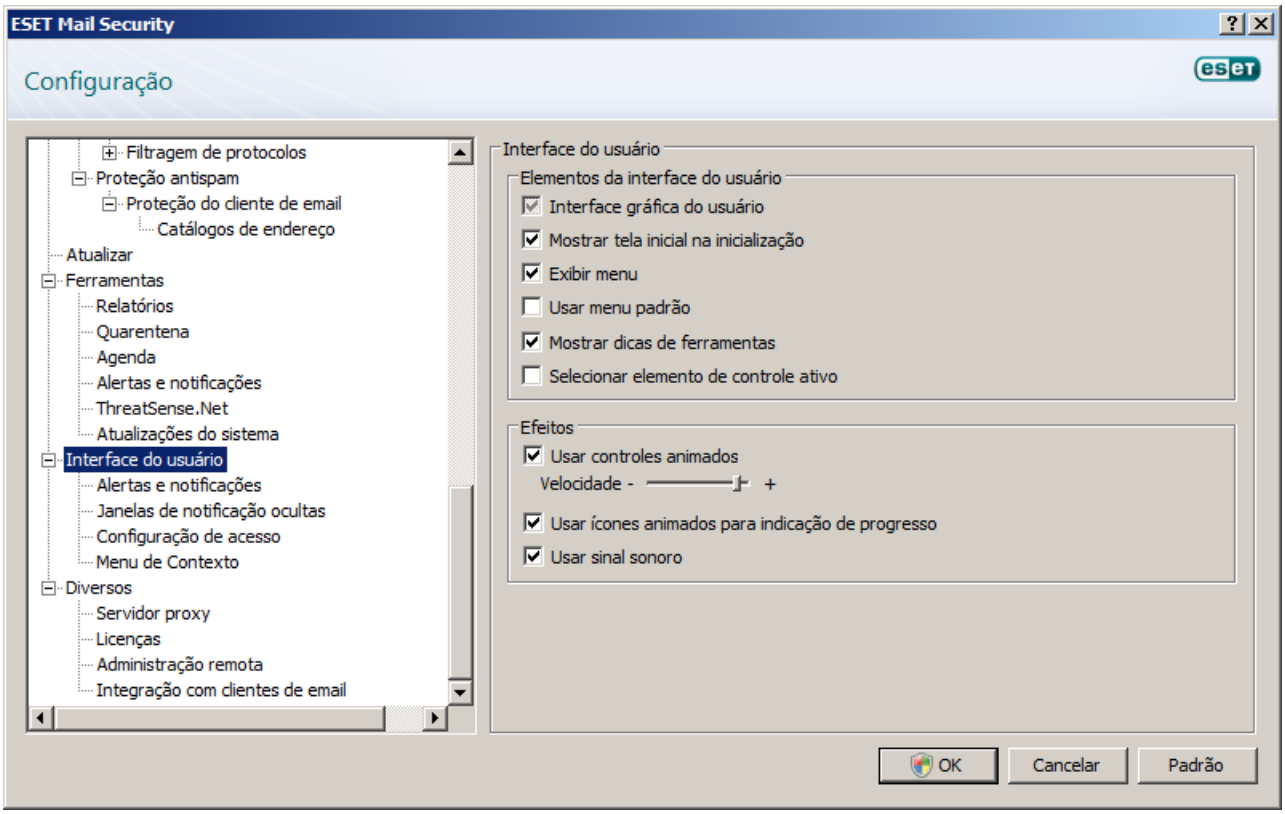
Se desejar desativar a tela inicial do ESET Mail Security, desmarque a opção **Mostrar tela inicial na inicialização**.

No parte superior da janela principal do tela do ESET Mail Security, há um menu padrão que pode ser ativado ou desativado com base na opção **Usar menu padrão**.

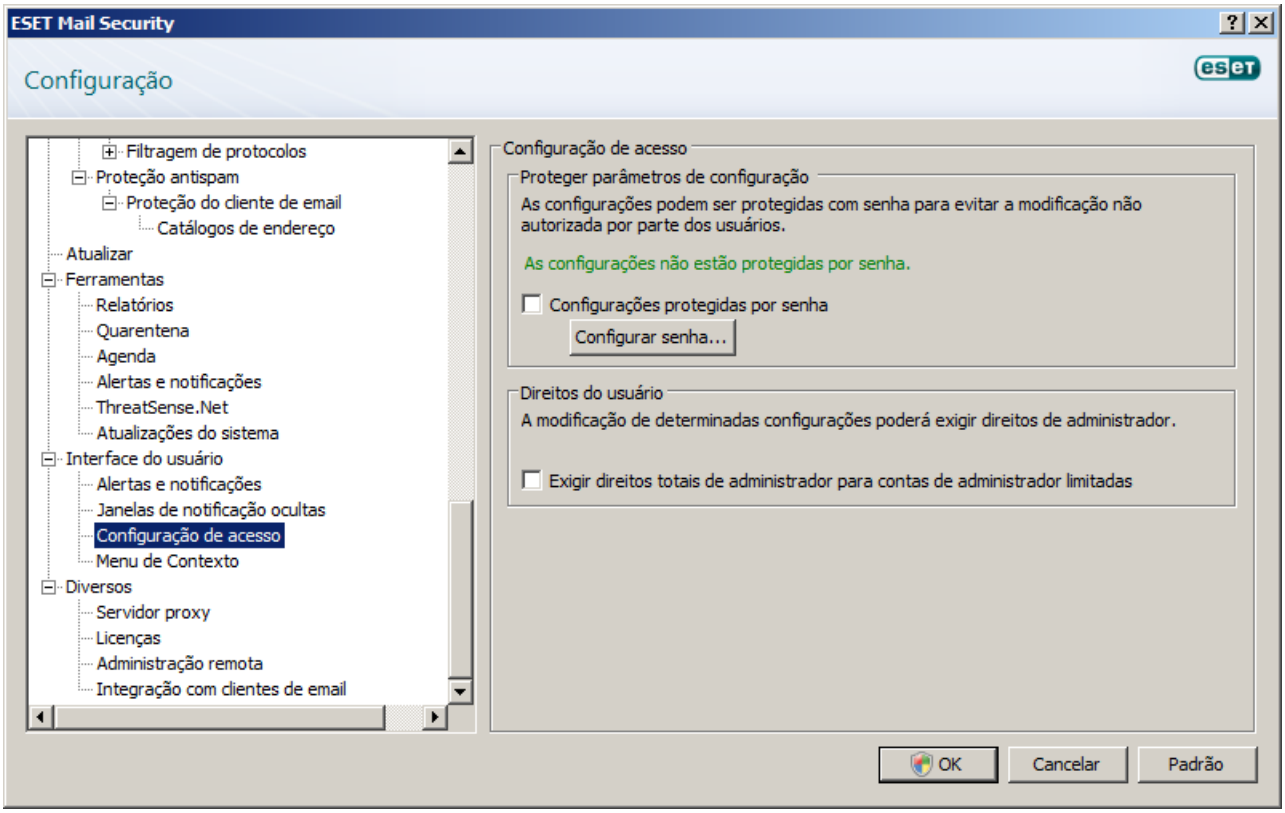
Se a opção **Mostrar dicas de ferramentas**, uma descrição breve será exibida se o cursor for colocado em cima da opção. A opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento realçado será ativado após um clique no mouse.

Para diminuir ou aumentar a velocidade dos efeitos animados, selecione a opção **Usar controles animados** e mova a barra deslizante **Velocidade** para a esquerda ou para a direita.

Para ativar o uso de ícones animados para exibir o andamento de várias operações, selecione a opção **Usar ícones animados para indicação de progresso**. Se desejar que o programa emita um aviso sonoro se um evento importante ocorrer, selecione a opção **Usar sinal sonoro**.



O recurso **Interface do usuário** também inclui a opção de proteger por senha os parâmetros de configuração do ESET Mail Security. Essa opção está localizada no submenu **Proteção de configurações** em **Interface do usuário**. Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma senha para proteger os parâmetros de configuração, clique em **Configurar senha...**



4.8.1 Alertas e notificações

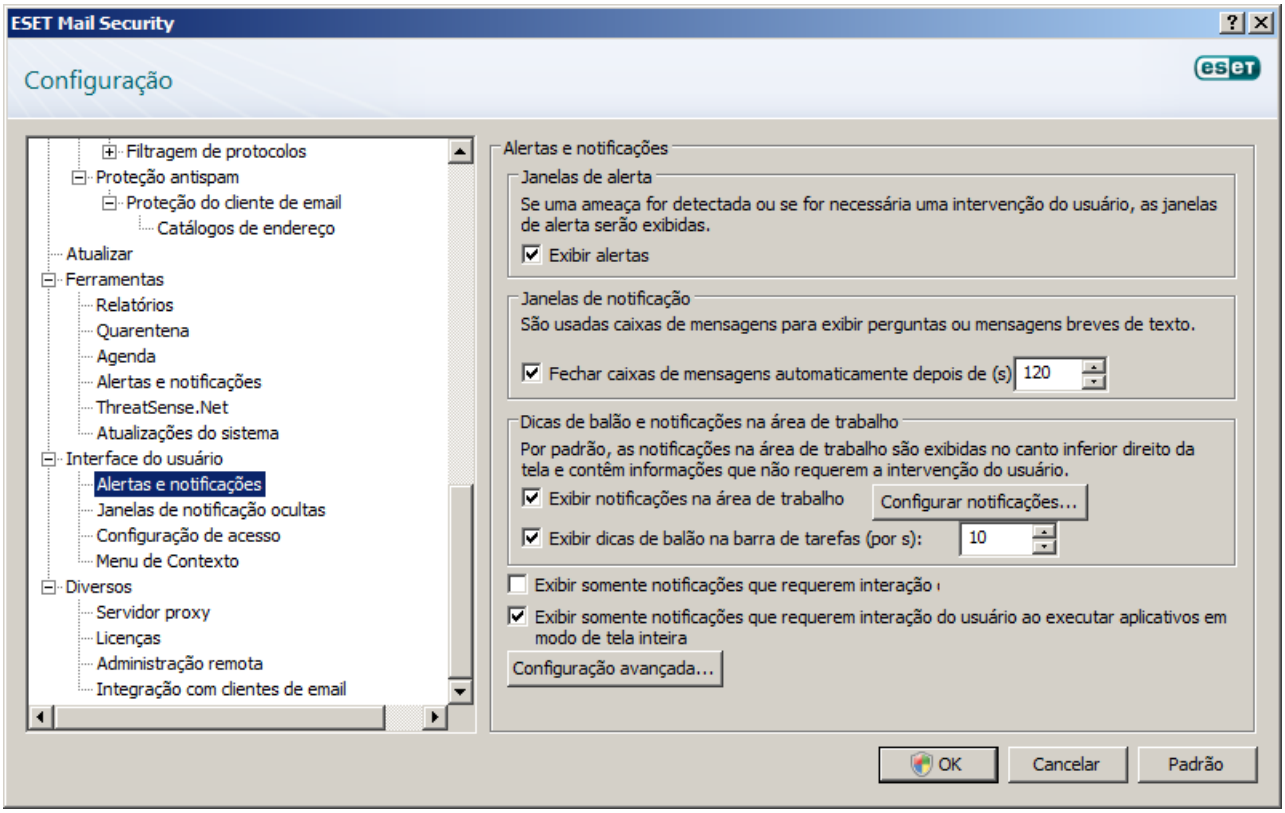
A seção **Configuração de alertas e notificações** em **Interface do usuário** permite que você configure o modo como os alertas de ameaças e as notificações do sistema são tratados no ESET Mail Security.

O primeiro item é **Exibir alertas**. A desativação dessa opção cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente depois de (s)**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente depois de expirado o tempo especificado.

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem nem proporcionam interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar a exibição de notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas - o tempo de exibição e a transparência da janela de notificação podem ser modificados clicando no botão **Configurar notificações...**

Para visualizar o comportamento das notificações, clique no botão **Visualizar**. Para configurar a duração da exibição das dicas de balão, consulte a opção **Exibir dicas de balão na barra de tarefas (por s)**.



Clique em **Configuração avançada...** para inserir opções de configuração de **Alertas e notificações** adicionais que incluem **Exibir somente notificações que requerem interação do usuário**. Essa opção permite ativar/desativar a exibição de alertas e notificações que não requeiram interação do usuário. Selecione **Exibir somente notificações que requerem interação do usuário ao executar aplicativos em modo de tela inteira** para suprimir todas as notificações que não sejam interativas. No menu suspenso **Detalhamento mínimo de eventos para exibir**, é possível selecionar o nível de gravidade inicial dos alertas e das notificações a serem exibidos.

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário**: permite definir quem receberá notificações importantes do ESET Mail Security. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Essa opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

4.8.2 Desativar a GUI no servidor de terminal

Este capítulo descreve como desativar a GUI do ESET Mail Security em execução no servidor de terminal do Windows para sessões de usuário.

Normalmente, a GUI do ESET Mail Security é iniciada toda vez que um usuário remoto faz login no servidor e cria uma sessão de terminal. Isso geralmente é indesejável em servidores de terminal. Se desejar desativar a GUI para sessões de terminal, siga estas etapas:

1. Execute *regedit.exe*
2. Navegue até *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Clique com o botão direito do mouse no Valor *egui* e selecione *Modificar...*
4. Adicione uma alternância de comando `/terminal` ao fim da cadeia de caracteres existente

Veja um exemplo de como devem ser os dados do Valor de *egui* :

```
"C:\Arquivos de Programas\ESET\ESET Mail Security\egui.exe" /hide /waitservice /terminal
```

Se desejar reverter essa configuração e ativar a inicialização automática da GUI do ESET Mail Security, remova a alternância `/terminal` Para acessar o Valor do registro *egui*, repita as etapas de 1. a 3.

4.9 eShell

O eShell (abreviação de ESET Shell) é a interface de linha de comando do ESET Mail Security. É uma alternativa à interface gráfica do usuário (GUI). O eShell possui todos os recursos e opções que a GUI geralmente oferece. O eShell permite configurar e administrar todo o programa sem usar a GUI.

Além de todas as funções e recursos disponíveis na GUI, o eShell também oferece a possibilidade de obter automação executando scripts para configurar, alterar configurações ou realizar uma ação. O eShell também pode ser útil para quem prefere usar linhas de comando em vez da GUI.

OBSERVAÇÃO: Um manual separado do eShell está disponível para você para download aqui. Ele relaciona todos os comandos com sintaxe e descrição.

Esta seção explica como navegar e como usar o eShell, e lista todos os comandos com uma descrição da função de cada comando específico.

Há dois modos em que o eShell pode ser executado:

- Modo interativo: útil quando se deseja trabalhar com o eShell (não apenas executar um único comando), por exemplo para tarefas como alterar a configuração, visualizar relatórios, etc. Também é possível usar o modo interativo se ainda não estiver familiarizado com todos os comandos. O modo interativo facilita a navegação pelo eShell . Também exibe os comandos disponíveis que podem ser usados em este contexto específico.
- Comando único/Modo de lote: use este modo se deseja apenas executar um comando, sem entrar no modo interativo do eShell. Isso pode ser feito no prompt de comando do Windows, digitando `eshell` com os parâmetros apropriados. Por exemplo:

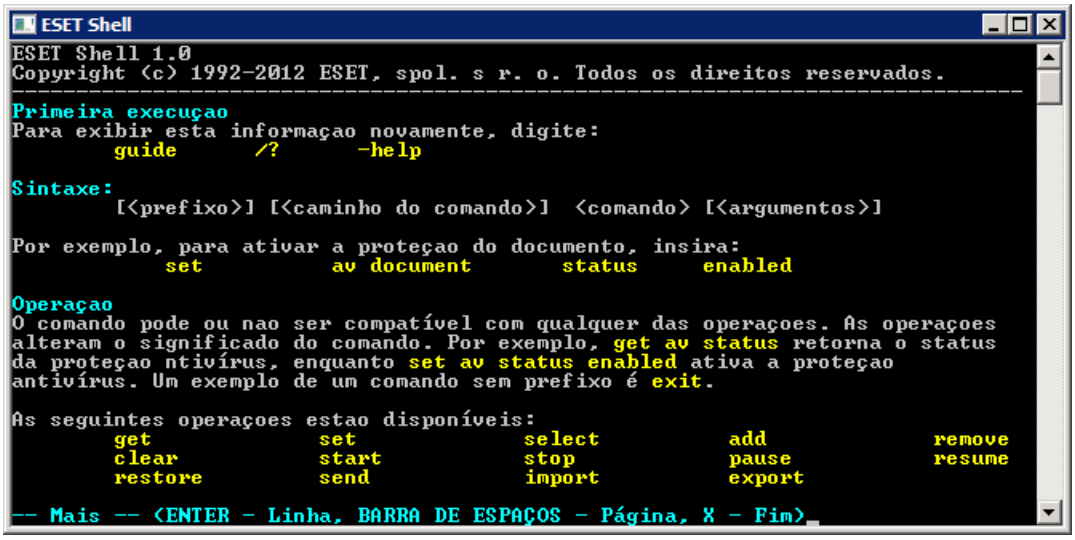
```
eshell set av document status enabled
```

OBSERVAÇÃO: Para executar comandos do eShell no prompt de comando do Windows ou para executar arquivos em lote, é preciso ativar essa função primeiro (o comando `set general access batch always` precisa ser executado no modo interativo). Para obter mais informações sobre o comando set batch, clique aqui 126.

Para entrar no modo interativo do eShell, você pode usar um dos seguintes dois métodos:

- No menu Iniciar do Windows: **Iniciar** > **Todos os programas** > **ESET** > **ESET File Security** > **ESET shell**
- No prompt de comando do Windows, digite `eshell` e pressione a tecla Enter

Ao executar o eShell no modo interativo pela primeira vez, será exibida uma tela de primeira execução.



Ela exibe alguns exemplos básicos de como usar o eShell com Sintaxe, Prefixo, Caminho de comando, Formas abreviadas, Aliases, etc. Basicamente, é um guia rápido do eShell.

OBSERVAÇÃO: Se quiser exibir esta tela no futuro, digite o comando `guide` .

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

4.9.1 Uso

Sintaxe
Os comandos devem ser formatados na sintaxe correta para que funcionem e podem ser compostos de um prefixo, contexto, argumentos, opções, etc. Esta é a sintaxe geral utilizada em todo o eShell:

[<prefixo>] [<caminho de comando>] <comando> [<argumentos>]

Exemplo (isto ativa a proteção de documentos):
`SET AV DOCUMENT STATUS ENABLED`

`SET` - um prefixo
`AV DOCUMENT` - caminho para um comando específico, um contexto a que este comando pertence
`STATUS` - o comando em si
`ENABLED` - um argumento para o comando

Ao usar `HELP` ou `?` com um comando, você verá a sintaxe para aquele comando específico. Por exemplo, o prefixo `CLEANLEVEL HELP` exibirá a sintaxe do comando `CLEANLEVEL` :

SINTAXE:
```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Observe que `[get]` está entre colchetes. Isso é o que denomina o prefixo `get` como padrão para o comando `cleanlevel` . Isso significa que, ao executar o comando `cleanlevel` sem especificar nenhum prefixo, será usado o prefixo padrão (que neste caso é `get cleanlevel`). Use comandos sem prefixos para economizar tempo ao digitar. Normalmente, `get` é o padrão para a maioria dos comandos, mas é necessário certificar-se qual é o prefixo padrão para um comando específico, e se é exatamente aquele que deseja executar.

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Prefixo/Operação
Um prefixo é uma operação. A `GET` fornecerá a informação de como um determinado recurso do ESET Mail Security está configurado ou exibirá um status (como `GET AV STATUS` exibirá o status de proteção atual). O prefixo `SET` configurará o recurso ou alterará seu status (`SET AV STATUS ENABLED` ativará a proteção).

Estes são os prefixos que o eShell permite que você use. Um comando pode ou não ser compatível com qualquer um dos prefixos:

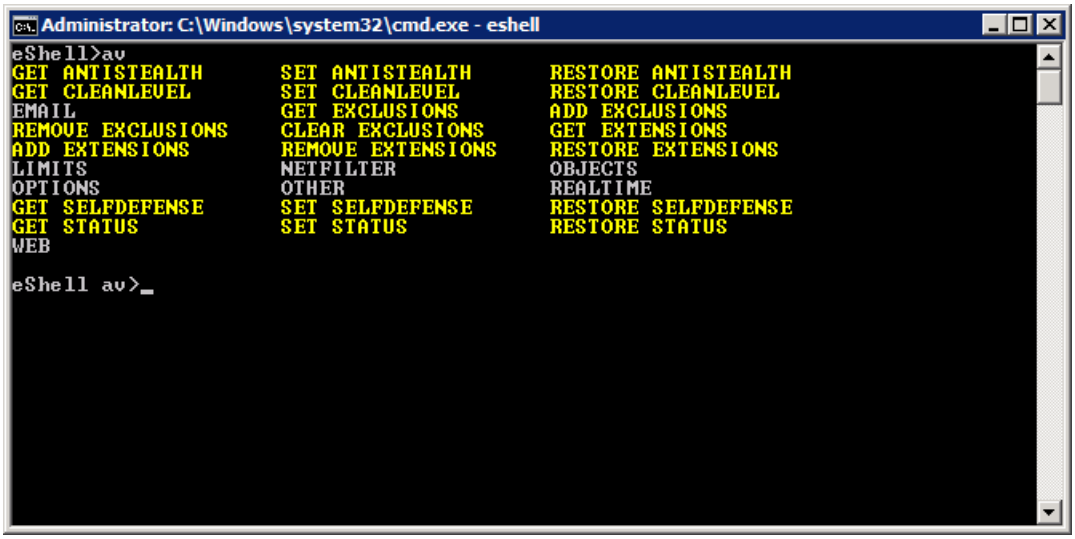
`GET` - retorna as configurações/status atuais
`SET` - define o valor/status
`SELECT` - seleciona um item
`ADD` - adiciona um item
`REMOVE` - remove um item
`CLEAR` - remove todos os itens/arquivos
`START` - inicia uma ação
`STOP` - interrompe uma ação
`PAUSE` - pausa uma ação
`RESUME` - retoma uma ação
`RESTORE` - restaura as configurações/objeto/arquivo padrão
`SEND` - envia um objeto/arquivo
`IMPORT` - importa de um arquivo
`EXPORT` - exporta para um arquivo

Prefixos como `GET` e `SET` são usados com vários comandos, mas alguns comandos, como `EXIT`, não usam prefixos.

Caminho de comando/Contexto
Os comandos são colocados em contextos que formam uma estrutura de árvore. O nível superior da árvore é a raiz. Ao executar o eShell, você está no nível raiz:

```
eShell>
```

Você pode executar o comando a partir daqui ou entrar um nome de contexto para navegar dentro da árvore. Por exemplo, ao entrar no contexto `TOOLS` , ele listará todos os comandos e subcontextos disponíveis ali.



Os que estão em amarelo são comandos que podem ser executados, os que estão em cinza são subcontextos nos quais você pode entrar. Um subcontexto contém outros comandos.

Se precisar voltar para um nível superior, use `..` (dois pontos). Por exemplo, se estiver em:

```
eShell av options>
```

digite `..` e você será levado um nível acima para:

```
eShell av>
```

Se quiser voltar à raiz de `eShell av options>` (que é dois níveis abaixo da raiz), digite apenas `.. ..` (dois pontos e dois pontos separados por espaço). Fazendo isso, você subirá dois níveis, que neste caso é a raiz. Você pode usar este método também quando estiver ainda mais profundo na árvore de contexto. Use a quantidade adequada de `..` para chegar ao nível desejado.

O caminho é relativo ao contexto atual. Se o comando estiver no contexto atual, não insira um caminho. Por exemplo, para executar `GET AV STATUS` digite:

`GET AV STATUS` - se estiver no contexto raiz (a linha de comando exibe `eShell>`)
`GET STATUS` - se estiver no contexto `AV` (a linha de comando exibe `eShell av>`)
`.. GET STATUS` - se estiver no contexto `AV OPTIONS` (a linha de comando exibe `eShell av options>`)

Argumento
Um argumento é uma ação realizada em um comando específico. Por exemplo, o comando `CLEANLEVEL` pode ser usado com os seguintes argumentos:

`none` - Não limpar
`normal` - Limpeza padrão
`strict` - Limpeza rígida

Outro exemplo são os argumentos `ENABLED` ou `DISABLED`, que são usados para ativar ou desativar determinados recursos.

Forma abreviada/Comandos encurtados
O eShell possibilita encurtar contextos, comandos e argumentos (desde que o argumento seja um alternador ou uma opção alternativa). Não é possível encurtar um prefixo ou um argumento que seja um valor concreto, como um número, nome ou caminho.

Exemplos de forma abreviada:

```
set status enabled => set stat en
add av exclusions C:\caminho\arquivo.ext => add av exc C:\caminho\arquivo.ext
```

Se houver dois comandos ou contextos começando com as mesmas letras, por exemplo ABOUT e AV, e você digitar A como comando abreviado, o eShell não conseguirá decidir qual comando você deseja executar. Será exibida uma mensagem de erro e uma lista de comandos começando com "A" que poderão ser utilizados:

```
eShell>a
O seguinte comando não é exclusivo: a

Os seguintes comandos estão disponíveis neste contexto:
 ABOUT - Exibe informações sobre o programa
 AV - Alterações ao contexto av
```

Adicionar uma ou mais letras (p. ex., AB em vez de apenas A) o eShell executará o comando ABOUT , já que este é o único com estas letras.

OBSERVAÇÃO: Quando quiser ter certeza de que um comando será executado exatamente como deseja, recomendamos que não abrevie comandos, argumentos, etc. e use a forma completa. Dessa forma o comando será executado exatamente como deseja e isso evita erros indesejados. Especialmente no caso de arquivos/scripts em lote.

Aliases

Um alias é um nome alternativo que pode ser usado para executar um comando (desde que o comando tenha um alias atribuído a ele). Há alguns aliases padrão:

`(global) help` - ?
`(global) close` - sair
`(global) quit` - sair
`(global) bye` - sair
`warnlog` - eventos de registro das ferramentas
`virlog` - detecções de registro das ferramentas

"(global)" significa que o comando pode ser usado em qualquer lugar, independente do contexto atual. Um comando pode ter vários aliases atribuídos a ele, por exemplo o comando EXIT tem os aliases CLOSE, QUIT e BYE. Quando quiser sair do eShell, pode usar o comando EXIT ou qualquer um de seus aliases. Alias VIRLOG é um alias para o comando DETECTIONS , que está localizado no contexto TOOLS LOG . Portanto, as detecções do comando estão disponíveis no contexto ROOT , e são mais fáceis de acessar (não é necessário entrar nos contextos TOOLS e LOG , pode executá-lo diretamente de ROOT).

O eShell permite definir seus próprios aliases.

Comandos protegidos

Alguns comandos estão protegidos e só podem ser executados após inserir uma senha.

Guia

Ao executar o comando GUIDE , será exibida uma tela explicando como usar o eShell. Esse comando está disponível no contexto ROOT (`eShell>`).

Ajuda

Quando o comando HELP for usado sozinho, listará todos os comandos disponíveis com prefixos e subcontextos dentro do contexto atual. Também fornecerá uma breve descrição para cada comando/subcontexto. Ao usar HELP como um argumento com um comando específico (p.ex. CLEANLEVEL HELP), serão exibidos os detalhes para aquele comando. Serão exibidos a SINTAXE, as OPERAÇÕES, os ARGUMENTOS e os ALIASES para o comando com uma breve descrição de cada.

Histórico de comandos

O eShell mantém um histórico dos comandos executados anteriormente. Isso se aplica apenas à sessão interativa atual do eShell. Quando você sair do eShell, o histórico do comando será removido. Use as teclas de seta para cima e para baixo em seu teclado para navegar pelo histórico. Quando encontrar o comando que está procurando, pode executá-lo ou alterá-lo sem ter que digitar todo o comando desde o início.

CLS/Limpar tela

O comando CLS pode ser usado para limpar a tela. Ele funciona da mesma forma que no prompt de comando do Windows ou interface de linha de comando similar.

EXIT/CLOSE/QUIT/BYE

Para fechar ou sair do eShell, você pode usar qualquer desses comandos (EXIT, CLOSE, QUIT ou BYE).

4.9.2 Comandos

Esta seção relaciona alguns comandos básicos do eShell com descrição como exemplo. Para obter a lista completa de comandos, consulte o manual do eShell, que pode ser obtido por download aqui.

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Comandos do contexto **ROOT**:

ABOUT

Lista informações sobre o programa. Exibe o nome do produto instalado, o número da versão, os componentes instalados (incluindo número de versão de cada componente) e as informaçoes básicas sobre o servidor e o sistema operacional em que o ESET Mail Security está sendo executado.

CAMINHO DO CONTEXTO:

`raiz`

BATCH

Inicia o modo de lote do eShell. Isto é muito útil ao executar arquivos/scripts em lote e recomendamos usá-lo com arquivos em lote. Coloque `START BATCH` como o primeiro comando no arquivo de lote ou script para ativar o modo de lote. Ao ativar esta função, não será solicitado nada (p.ex. inserção de senha) e os argumentos faltantes serão substituídos pelos padrões. Isso garante que o arquivo em lote não pare no meio porque o eShell está esperando o usuário fazer algo. Dessa forma, o arquivo em lote será executado sem paradas (a menos que haja um erro ou que os comandos no arquivo em lote estejam incorretos).

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[start] batch`

OPERAÇÕES:

`start` - Inicia o eShell no modo de lote

CAMINHO DO CONTEXTO:

`raiz`

EXEMPLOS:

`start batch` - Inicia o modo de lote do eShell

GUIDE

Exibe a tela da primeira execução.

CAMINHO DO CONTEXTO:

`raiz`

PASSWORD

Geralmente, para executar comandos protegidos por senha você é solicitado uma senha por motivos de segurança. Isso se aplica a comandos como os que desativam a proteção antivírus e os que podem afetar os recursos do ESET Mail Security. Será solicitada uma senha sempre que executar um desses comandos. Para evitar inserir uma senha a cada vez, você pode definir esta senha. Ela será lembrada pelo eShell e será usada automaticamente quando um comando protegido por senha for executado. Isso significa que não será preciso inseri-la.

OBSERVAÇÃO: A senha definida funciona somente na sessão interativa atual do eShell. Quando você sair do eShell, esta senha definida será removida. Ao iniciar o eShell novamente, a senha precisará ser definida novamente.

Essa senha definida também é bastante útil ao executar arquivos/scripts em lote. Eis um exemplo de um arquivo em lote:

```
eshell start batch "&" set password plain <suasenha> "&" set status disabled
```

Este comando concatenado acima inicia um modo de lote, define a senha que será usada e desativa a proteção.

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[get] | restore password`

`set password [plain <senha>]`

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou limpar a senha

`restore` - Limpar a senha

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

EXEMPLOS:

`set password plain <suasenha>` - Define uma senha que será usada para comandos protegidos por senha

`restore password` - Limpa a senha

EXEMPLOS:

`get password` - Use este comando para ver se a senha está configurada (isto apenas exibe asteriscos "*", não lista a senha em si), quando não forem exibidos asteriscos, significa que não há uma senha definida

`set password plain <suasenha>` - Use para definir a senha definida

`restore password` - Este comando limpa a senha definida

STATUS

Exibir informações sobre o status atual de proteção do ESET Mail Security (similar à GUI).

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[get] | restore status`

`set status disabled | enabled`

OPERAÇÕES:

`get` - Exibir o status da proteção antivírus

`set` - Ativar/Desativar a proteção antivírus

`restore` - Restaura as configurações padrão

ARGUMENTOS:

`disabled` - Desativar a proteção antivírus

`enabled` - Ativar a proteção antivírus

EXEMPLOS:

`get status` - Exibe o status de proteção atual

`set status disabled` - Desativa a proteção

`restore status` - Restaura a proteção às configurações padrão (ativada)

VIRLOG

Este é um alias do comando `DETECTIONS` . É útil para visualizar informações sobre infiltrações detectadas.

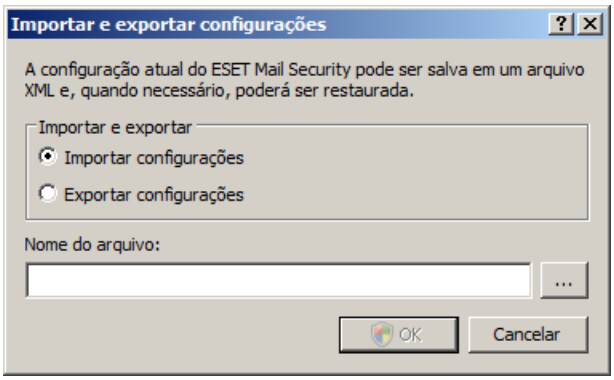
WARNLOG

Este é um alias do comando `EVENTS` . É útil para visualizar informações sobre vários eventos.

4.10 Importar e exportar configurações

A importação e a exportação de configurações do ESET Mail Security está disponível em **Configurar** clicando em **Importar e exportar configurações**.

Tanto a importação quanto a exportação utilizam arquivos .xml. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET Mail Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET Mail Security em diversos sistemas. Os usuários podem importar facilmente um arquivo .xml para transferir as configurações desejadas.



4.11 ThreatSense.Net

O ThreatSense.Net Early Warning System mantém a ESET contínua e imediatamente informada sobre novas infiltrações. O sistema de alerta bidirecional do ThreatSense.Net Early Warning System tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que veremos novas ameaças assim que elas aparecerem é mantermos "link" com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

1. Você pode optar por não ativar o ThreatSense.Net Early Warning System. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.

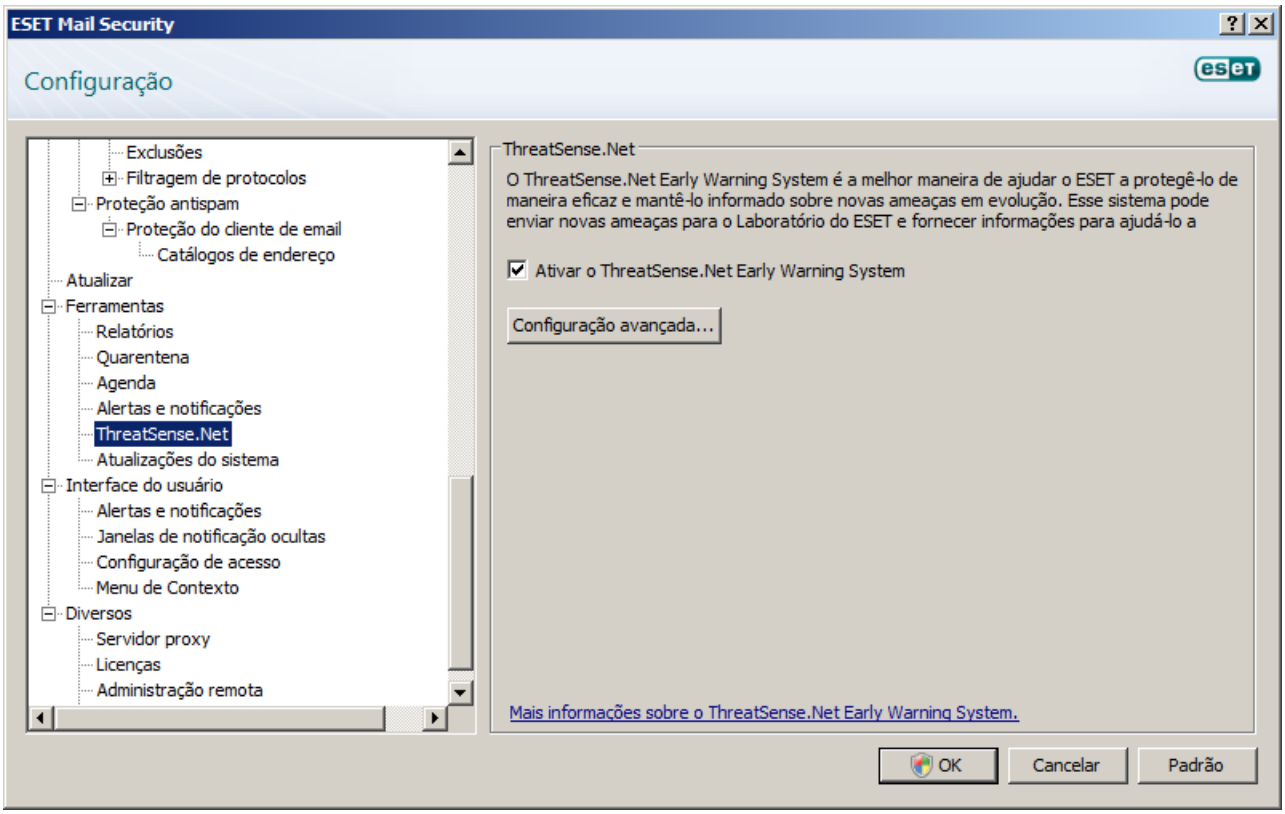
2. É possível configurar o ThreatSense.Net Early Warning System para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ThreatSense.Net Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador (usuários em um caminho de diretório, etc.) para o Laboratório de ameaças da ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

Por padrão, o ESET Mail Security é configurado para perguntar antes de enviar arquivos suspeitos ao Laboratório de ameaças da ESET para análise detalhada. Os arquivos com certas extensões, como .doc ou .xls, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

A configuração do ThreatSense.Net pode ser acessada na árvore Configuração avançada, em **Ferramentas** > **ThreatSense.Net**. Selecione a opção **Ativar o ThreatSense Early Warning System** para ativá-lo e clique no botão **Configuração avançada...**

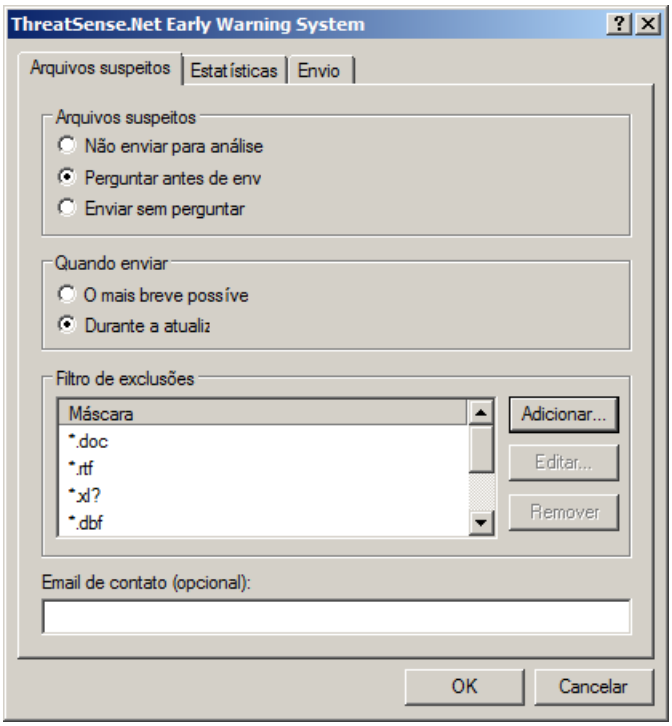


4.11.1 Arquivos suspeitos

A guia **Arquivos suspeitos** permite configurar a maneira como as ameaças serão enviadas ao Laboratório de ameaças da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

O envio de arquivos pode ser definido para ocorrer automaticamente ou selecione a opção **Perguntar antes de enviar**, se desejar saber quais arquivos foram enviados para análise e confirmar o envio.



Se não desejar que os arquivos sejam enviados, selecione a opção **Não enviar para análise**. A seleção da opção de não envio de arquivos para análise não influencia o envio das informações estatísticas, que são definidas em sua própria configuração. (consulte a seção Estatísticas 130).

Quando enviar - Por padrão, a opção **O mais breve possível** fica selecionada para que os arquivos suspeitos sejam enviados ao Laboratório de ameaças da ESET. Esta é a opção recomendada se uma conexão permanente com a Internet estiver disponível e os arquivos suspeitos puderem ser enviados sem atraso. Selecione a opção **Durante a atualização** para que o upload de arquivos suspeitos seja feito para o ThreatSense.Net durante a próxima atualização.

Filtro de exclusões – O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Email de contato – Seu **Email de contato (opcional)**pode ser enviado com qualquer arquivo suspeito e pode ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

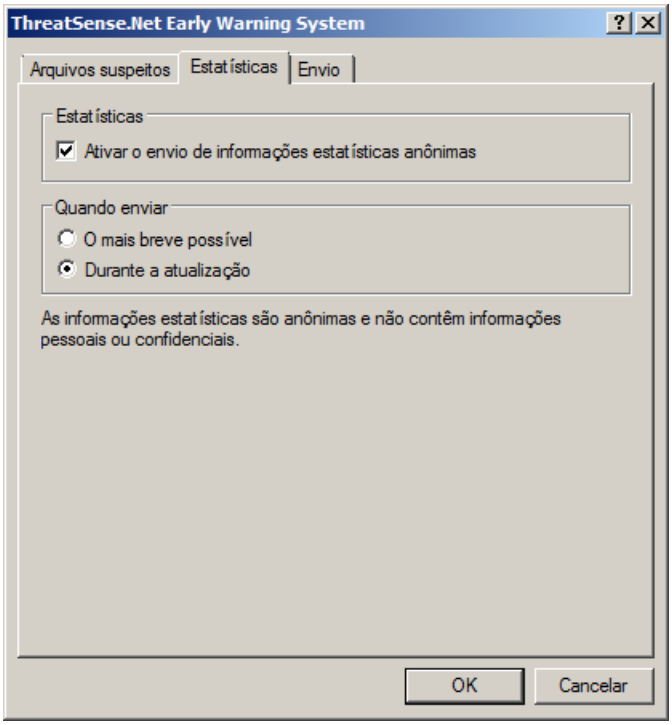
4.11.2 Estatísticas

O ThreatSense.Net Early Warning System coletará informações anônimas sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. As estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

A seguir há um exemplo de um pacote estatístico enviado:

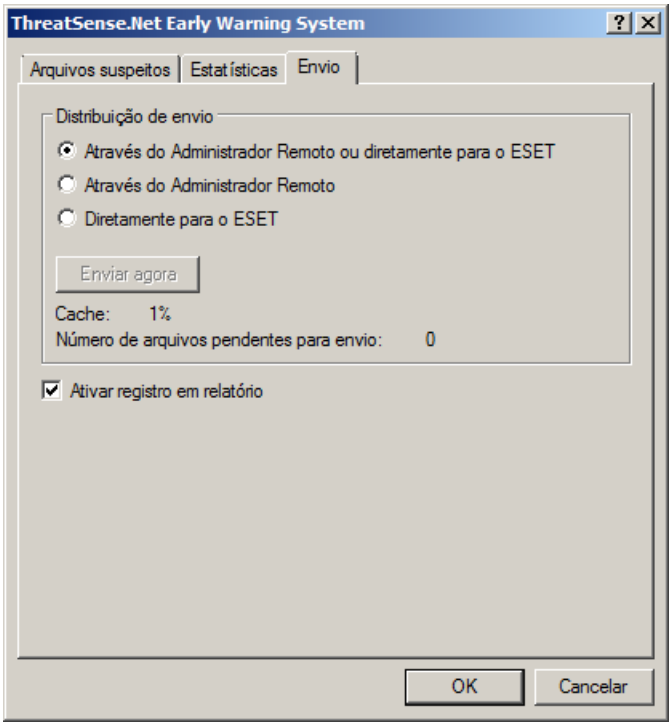
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

Quando enviar - Você pode definir o momento em que as informações estatísticas serão enviadas. Se optar por enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Esta configuração é adequada se um conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, todas as informações estatísticas serão enviadas em grupo durante a próxima atualização.



4.11.3 Envio

Você pode selecionar como os arquivos e as informações estatísticas serão enviados à ESET. Selecione a opção **Através do Administrador Remoto ou diretamente para a ESET** para enviar arquivos e estatísticas por qualquer meio disponível. Selecione a opção **Através do Administrador Remoto** para enviar os arquivos e as estatísticas ao servidor da administração remota, que assegurará o envio posterior ao Laboratório de ameaças da ESET. Se a opção **Diretamente para a ESET** estiver selecionada, todos os arquivos suspeitos e informações estatísticas serão enviados para o laboratório de vírus da ESET diretamente do programa.



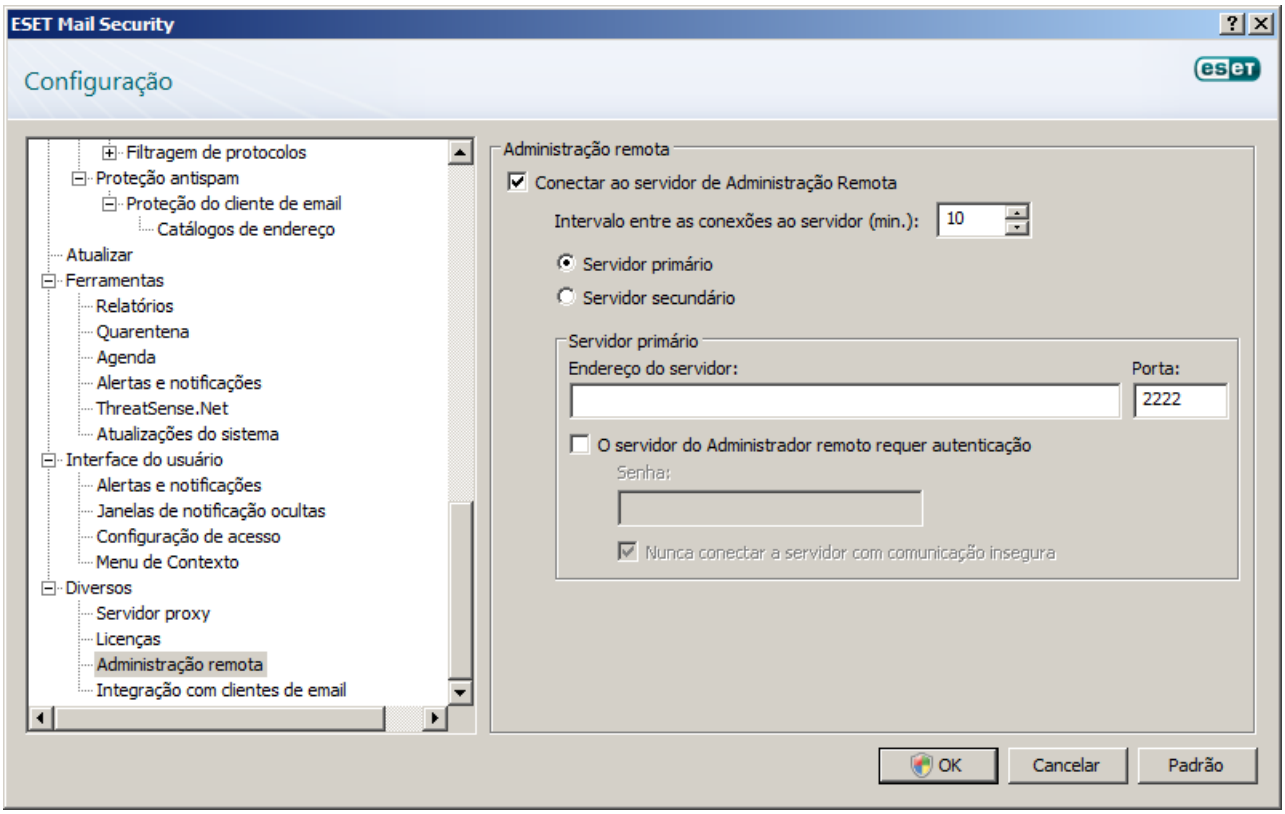
Quando houver arquivos com envio pendente, o botão **Enviar agora** estará ativado. Clique nesse botão para enviar arquivos e informações estatísticas imediatamente.

Selecione a opção **Ativar registro em relatório** para criar um relatório para registrar os envios de arquivos e informações estatísticas.

4.12 Administração remota

O ESET Remote Administrator (ERA) é uma ferramenta poderosa para gerenciar a política de segurança e para obter uma visão geral de toda a segurança em uma rede. É especialmente útil quando aplicada a redes maiores. O ERA não aumenta somente o nível de segurança, mas também fornece facilidade de uso no gerenciamento do ESET Mail Security em estações de trabalho clientes.

As opções de configuração de administração remota estão disponíveis na janela principal do programa ESET Mail Security. Clique em **Configuração (Setup)** > **Entrar na configuração avançada... (Enter the entire advanced setup tree...)** > **Diversos (Miscellaneous)** > **Administração remota (Remote administration)**.



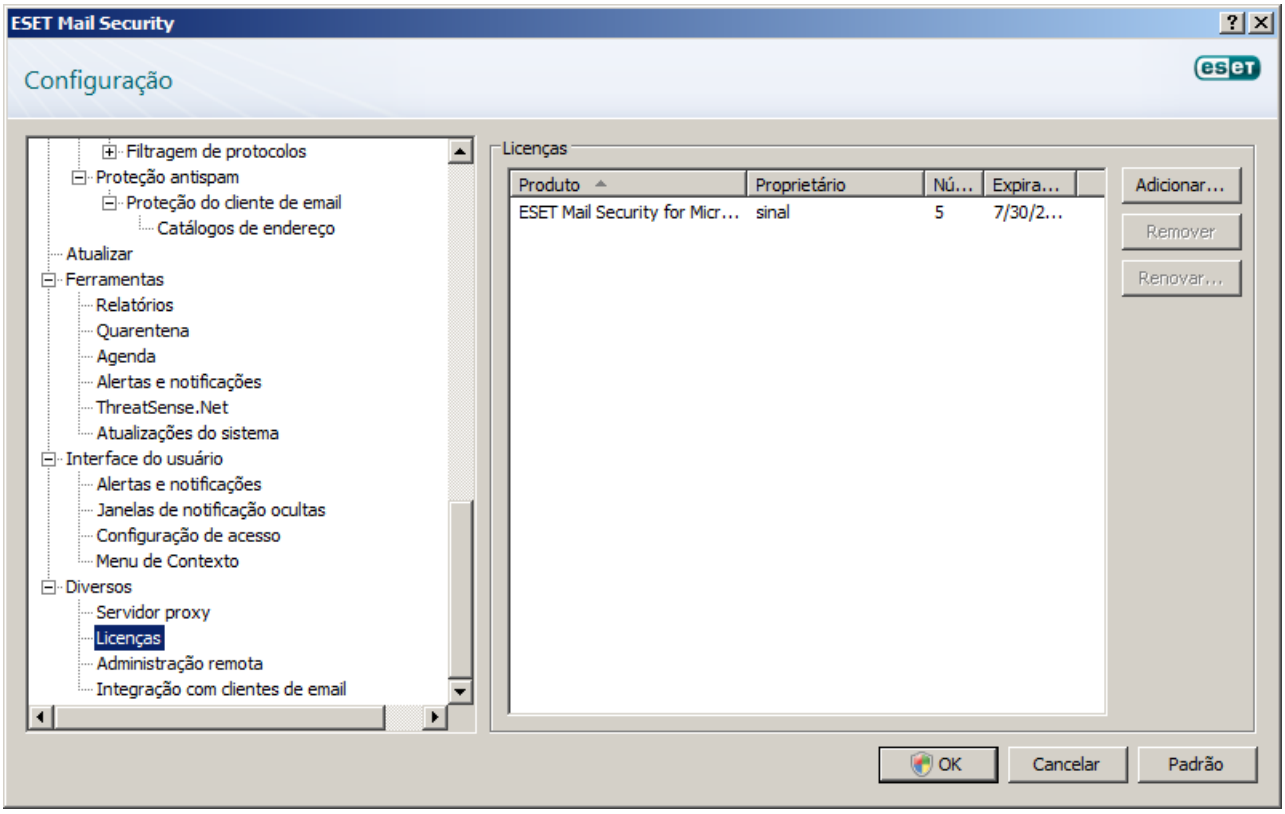
Ative a administração remota selecionando a opção **Conectar ao servidor de Administração Remota (Connect to Remote Administration server)**. É possível acessar as outras opções descritas a seguir:

- **Intervalo entre as conexões ao servidor (min.) (Interval between connections to server (min.)):** Isso designa a frequência com que o ESET Mail Security se conectará ao servidor ERA. Se estiver configurado como 0, as informações serão enviadas a cada 5 segundos.
- **Endereço do servidor (Server address):** Endereço de rede do servidor em que o servidor ERA está instalado.
- **Porta:** Esse campo contém um valor predefinido utilizado para conexão. Recomendamos que você deixe a configuração de porta padrão em 2222
- **O servidor do Administrador remoto requer autenticação (Remote Administrator server requires authentication):** Permite inserir a senha para conexão com o servidor ERA, se necessário.

Clique em **OK** para confirmar as alterações e aplicar as configurações. O ESET Mail Security as usará para conectar-se ao servidor ERA.

4.13 Licenças

A ramificação **Licenças** permite gerenciar as chaves de licença do ESET Mail Security e de outros produtos da ESET, como a ESET Mail Security etc. Após a compra, as chaves de licença são fornecidas com o nome de usuário e a senha. Para **Adicionar/Remover** uma chave de licença, clique no botão correspondente na janela do gerenciador de licenças. O gerenciador de licenças pode ser acessado na árvore Configuração avançada em **Diversos** > **Licenças**.



A chave de licença é um arquivo de texto que contém informações sobre o produto comprado: o proprietário, o número de licenças e a data de expiração.

A janela do gerenciador de licenças permite fazer upload e visualizar o conteúdo de uma chave de licença usando o botão **Adicionar...** – as informações contidas serão exibidas no gerenciador. Para excluir os arquivos de licença da lista, clique em **Remover**.

Se uma chave de licença tiver expirado e você estiver interessado em adquirir a renovação, clique no botão **Solicitar...**; você será redirecionado à nossa loja on-line.

5. Glossário

5.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

5.1.1 Vírus

Um vírus de computador é uma infiltração que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que o usuário, acidental ou deliberadamente, execute ou abra ele mesmo o programa malicioso.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus (quando comparados a cavalos de troia ou spyware) estão se tornando cada vez mais raros, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é frequentemente usado de maneira incorreta para cobrir todos os tipos de infiltrações. Essa utilização está gradualmente sendo superada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

Os exemplos de vírus são: OneHalf, Tenga, e Yankee Doodle.

5.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms são propagados por meio dos endereços de e-mail da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais férteis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas ou em até em minutos, após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversos transtornos: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

5.1.3 Cavalos de troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de infiltração que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Mas é importante observar que isso era verdadeiro para os cavalos de troia do passado – hoje não há necessidade de eles se disfarçarem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** – Um programa malicioso com a capacidade de fazer o download de outras infiltrações a partir da Internet
- **Dropper** – Um tipo de cavalo de troia desenvolvido para instalar outros tipos de softwares maliciosos em computadores comprometidos
- **Backdoor** – Um aplicativo que se comunica com os agressores remotos, permitindo que obtenham acesso ao sistema e assumam o controle dele
- **Keylogger** – (keystroke logger) – Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos
- **Dialer** – Dialers são programas desenvolvidos para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modems discados que não são mais usados regularmente.

Os cavalos de troia geralmente tomam a forma de arquivos executáveis com extensão .exe. Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele quase sempre contém códigos maliciosos.

Os exemplos dos cavalos de troia bem conhecidos são: NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo em que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows, etc. Por este motivo, é quase impossível detectá-los usando técnicas de teste comuns.

Há dois níveis de detecção para impedir rootkits:

1) Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).

2) Quando eles estão ocultos para os testes usuais. Os usuários do ESET Mail Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

5.1.5 Adware

Adware é a abreviação de advertising-supported software (software patrocinado por propaganda). Os programas que exibem material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a página inicial do navegador. O adware é frequentemente vinculado a programas freeware, permitindo que seus desenvolvedores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso — os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware também pode executar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Determinados programas não serão instalados sem o adware, ou as suas funcionalidades ficarão limitadas. Isso

significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

5.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de e-mail da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINS, números de contas bancárias, etc. O Spyware freqüentemente é vinculado a versões gratuitas de um programa pelo seu autor a fiim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

5.1.7 Arquivos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Mail Security fornece a opção de detectar tais ameaças.

"Aplicativos potencialmente inseguros" é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers 135 (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo potencialmente inseguro presente e sendo executado em seu computador (e que você não instalou), consulte o seu administrador de rede ou remova o aplicativo.

5.1.8 Aplicativos potencialmente indesejados

Aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o desempenho do computador. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- São abertas novas janelas que você não via anteriormente
- Ativação e execução de processos ocultos
- Uso aumentado de recursos do sistema
- Alterações nos resultados de pesquisa
- O aplicativo comunica-se com servidores remotos

5.2 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. É flexível, rápido e direto, e teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com os altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso – malware. A inconveniência e o perigo para você aumentam pelo fato de que o custo de enviar um spam é mínimo, e os autores do spam têm muitas ferramentas para adquirir novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas para pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou na sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" – por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

5.2.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. Suas principais vantagens de marketing são custos mínimos e um alto nível de objetividade, e o mais importante, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por e-mail para se comunicar de forma eficaz com os seus clientes atuais e potenciais.

Esse tipo de publicidade é legítimo, desde que o usuário esteja interessado em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Em tais casos, a publicidade por e-mail ultrapassa o razoável e se torna spam.

A quantidade de emails não solicitados se tornou um problema e não demonstra sinais de que vá diminuir. Os autores de emails não solicitados geralmente tentam disfarçar o spam enviando-o como mensagens legítimas.

5.2.2 Hoaxes

Um hoax é uma informação falsa propagada pela Internet. Os hoaxes geralmente são enviados por email ou ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes pedem que os destinatários encaminhem as mensagens a seus contatos, perpetuando-o. Há hoaxes de celulares, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Geralmente é impossível identificar a intenção do criador.

Se você vir uma mensagem solicitando que você a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites na Internet que podem verificar se um email é legítimo. Antes de encaminhar, execute uma pesquisa na Internet sobre qualquer mensagem que você suspeita que seja um hoax.

5.2.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um e-mail passando-se por uma pessoa ou negócio confiável (p. ex. instituição financeira, companhia de seguros). O e-mail parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, empresas de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

5.2.4 Reconhecimento de fraudes em spam

Geralmente, há poucos indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam:

- O endereço do remetente não pertence a alguém da sua lista de contatos
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais: números de contas bancárias, nomes de usuário e senhas, etc.
- Está escrito em um idioma estrangeiro
- Você é solicitado a comprar um produto no qual não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original)
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo "vaigra", em vez de "viagra" etc.

5.2.4.1 Regras

No contexto das soluções antispam e dos clientes de e-mail, as regras são as ferramentas para manipular as funções do e-mail. Elas são constituídas por duas partes lógicas:

1) Condição (por exemplo, uma mensagem recebida de um determinado endereço)

2) Ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada)

O número e a combinação de diversas regras com a solução Antispam. Essas regras servem como medidas contra spam (e-mail não solicitado). Exemplos típicos:

- Condição: Uma mensagem recebida contém algumas palavras geralmente vistas nas mensagens de spam 2. Ação: Excluir a mensagem
- Condição: Uma mensagem recebida contém um anexo com a extensão .exe 2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio
- Condição: Uma mensagem recebida chega do seu patrão 2. Ação: Mover a mensagem para a pasta "Trabalho"

Recomendamos que você use uma combinação de regras nos programas antispam a fim de facilitar a administração e filtrar os spams com mais eficiência.

5.2.4.2 Filtro Bayesian

A filtragem de spam Bayesian é uma forma eficiente de filtragem de e-mail usada por quase todos os produtos antispam. Ela é capaz de identificar emails não solicitados com grande precisão e pode funcionar com base em cada usuário.

A funcionalidade baseia-se no seguinte princípio: O processo de aprendizagem acontece na primeira fase. O usuário marca manualmente um número suficiente de mensagens como mensagens legítimas ou spam (normalmente 200/200). O filtro analisa as duas categorias e aprende, por exemplo, que o spam geralmente contém as palavras "rolex" ou "viagra", e as mensagens legítimas são enviadas por familiares ou de endereços na lista de contatos do usuário. Desde que haja uma quantidade suficiente de mensagens processadas, o filtro Bayesian é capaz de atribuir um "índice de spam" específico a cada mensagem, para determinar se é ou não spam.

A principal vantagem de um filtro Bayesian é a sua flexibilidade. Por exemplo, se um usuário for um biólogo, todas as mensagens de e-mail referentes à biologia ou aos campos de estudo relacionados serão geralmente recebidas com um índice de baixa probabilidade. Se uma mensagem incluir palavras que normalmente a qualificariam como não solicitada, mas que foi enviada por alguém da lista de contatos do usuário, ela será marcada como legítima, porque os remetentes de uma lista de contatos diminuem a probabilidade geral de spam.

5.2.4.3 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceitas, ou para os quais foi concedida permissão. O termo "lista de permissões de e-mail" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de e-mail, nomes de domínio, endereços de IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço de IP não serão recebidas. Se não forem exclusivas, tais mensagens não serão excluídas, mas filtradas de algum outro modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições 139. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

5.2.4.4 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições. As criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

É fundamental usar as listas de proibições para bloquear spams com sucesso, mas é muito difícil mantê-las, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos que use uma lista de permissões 139 e uma de proibições para filtrar o spam com mais eficácia.

5.2.4.5 Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os spams em massa com base no número de mensagens recebidas e as reações dos usuários. Cada mensagem deixa uma "impressão digital" exclusiva no servidor com base no conteúdo da mensagem. O número de ID exclusivo não informa nada sobre o conteúdo do email. Duas mensagens idênticas terão impressões digitais idênticas, enquanto mensagens diferentes terão impressões digitais diferentes.

Se uma mensagem for marcada como spam, sua impressão digital será enviada ao servidor. Se o servidor receber mais de uma impressão digital idêntica (correspondendo a uma determinada mensagem de spam), a impressão digital será armazenada no banco de dados das impressões digitais. Ao rastrear as mensagens de entrada, o programa envia as impressões digitais das mensagens ao servidor. O servidor retorna as informações sobre que impressões digitais correspondem às mensagens já marcadas pelos usuários como spam.