KASPERSKY LAB

Kaspersky® Anti-Virus for Windows Servers 6.0

MANUAL DO USUÁRIO

KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Manual do Usuário

http://www.kaspersky.com.br

Data de revisão: julho de 2007

Sumário

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DOS COMPUTADORES

Com a rápida evolução da tecnologia da informação e sua penetração em várias áreas, cresce também o número e a variedade de crimes associados à violação de informações.

Os chamados criminosos virtuais têm grande interesse nas atividades de instituições governamentais e empresas privadas. Eles tentam roubar e divulgar informações confidenciais, causando danos à reputação das empresas, interferindo na continuidade dos negócios e podem prejudicar os recursos de informações das organizações. Essas ações podem causar sérios danos aos ativos tangíveis e intangíveis das empresas.

E eles não visam apenas as grandes empresas. Usuários individuais também podem ser atacados. Por meio de várias ferramentas, eles obtêm acesso a dados pessoais (números e senhas de contas bancárias e de cartões de crédito), prejudicam a operação dos sistemas e conseguem até mesmo ter acesso total ao seu computador. Esse computador pode ser usado então como parte de uma rede de zumbis, ou seja, uma rede de computadores infectados usados por hackers para atacar servidores, enviar spams, coletar informações confidenciais e disseminar novos vírus e cavalos de Tróia.

No mundo de hoje, as informações são amplamente reconhecidas como ativos valiosos que devem ser protegidos. Ao mesmo tempo, essas informações devem estar acessíveis para aqueles que realmente precisam delas (por exemplo, funcionários, clientes e parceiros de uma empresa). Conseqüentemente, existe a necessidade de criar um sistema de segurança de informações abrangente, que deve considerar todas as fontes de ameaças possíveis, sejam elas humanas, geradas pelo homem ou desastres naturais, e usar uma variedade completa de medidas defensivas nos níveis físico, administrativo e de software.

1.1. Fontes de ameaças

Um indivíduo, um grupo de pessoas ou um fenômeno não relacionado à atividade humana podem representar uma ameaça à segurança das informações. Assim, todas as fontes de ameaças podem ser classificadas em três grupos:

- **O fator humano**. Este grupo de ameaças refere-se às ações de pessoas com acesso autorizado ou não às informações. As ameaças desse grupo podem ser divididas em:
    - *Externas*, incluindo criminosos virtuais, hackers, golpistas da Internet, parceiros inescrupulosos e organizações criminosas.
    - *Internas*, incluindo ações de funcionários da empresa. As ações executadas por este grupo podem ser deliberadas ou acidentais.
- **O fator tecnológico**. Este grupo de ameaças está relacionado com problemas técnicos, como o uso de software e hardware obsoletos ou de má qualidade para o processamento das informações. Isso pode resultar em falhas nos equipamentos e, freqüentemente, na perda de dados.
- **O fator de desastres naturais**. Este grupo de ameaças inclui toda a variedade de eventos provocados pela natureza e outros que independem da atividade humana.

Essas três fontes de ameaças precisam ser consideradas no desenvolvimento de um sistema de proteção à segurança de dados. Este Manual do Usuário enfoca a área diretamente vinculada à especialidade da Kaspersky Lab, as ameaças externas que envolvem atividade humana.

1.2. Como as ameaças se disseminam

O desenvolvimento de modernas ferramentas de comunicação e de tecnologias de computação amplia as oportunidades para os hackers disseminarem ameaças. Vamos examiná-las mais detalhadamente:

A Internet

A Internet é única porque não pertence a ninguém e não tem fronteiras. Sob vários aspectos, isso promoveu o desenvolvimento dos recursos da Web e a troca de informações. Atualmente, qualquer pessoa pode acessar dados na Internet ou criar sua própria página na Web.

Entretanto, esses vários recursos da rede mundial também permitem que hackers cometam crimes virtuais, dificultando sua detecção e punição.

Os hackers inserem vírus e outros programas mal-intencionados nos sites, disfarçados como interessantes programas gratuitos. Além disso, scripts que são executados automaticamente quando você abre certas páginas da Web podem executar ações perigosas no seu computador,

incluindo a modificação do Registro do sistema, o roubo de dados pessoais e a instalação de software mal-intencionado.

Usando tecnologias de rede, os hackers conseguem atacar servidores corporativos. Esses ataques podem ocasionar o mal funcionamento de componentes do sistema ou viabilizar o acesso total dos hackers ao sistema e, conseqüentemente, às informações armazenadas nele. Eles também podem usá-los como parte de uma rede de zumbis.

Intranet

A intranet é sua rede interna, destinada à troca de informações dentro de uma empresa ou em uma rede doméstica. A intranet é um ambiente comum no qual todos os computadores da rede podem armazenar, trocar e acessar informações. Isso significa que, no caso de infecção de um dos computadores da rede, todos os demais correm um sério risco. Para evitar situações como essa, é necessário proteger tanto os limites da rede como também cada um dos computadores.

E-mail

Como a grande maioria dos computadores possui programas de e-mail instalados, e os programas mal-intencionados exploram o conteúdo dos catálogos de endereços eletrônicos, geralmente essa é a condição ideal para a disseminação desses programas. O usuário de um computador infectado pode, sem se dar conta, enviar e-mails infectados para seus amigos ou colegas de trabalho que, por sua vez, enviariam mais e-mails infectados. Por exemplo, é comum que documentos em arquivos infectados passem desapercebido quando distribuídos com informações comerciais através de um sistema de e-mail interno da empresa. Quando isso ocorre, um grande número de pessoas é infectado. Podem ser centenas ou milhares de funcionários da empresa, junto com possivelmente dezenas de milhares de assinantes.

Mídia de armazenamento removível

As mídias removíveis (disquetes, CDs/DVDs e unidades flash USB) são muito usadas no armazenamento e na transmissão de informações.

A abertura de um arquivo que contém código mal-intencionado armazenado em um dispositivo de armazenamento removível pode danificar os dados armazenados no computador local e disseminar o vírus para outras unidades do computador ou para outros computadores da rede.

1.3. Tipos de ameaças

Atualmente, existe um grande número de ameaças à segurança dos computadores. Esta seção examinará as ameaças bloqueadas pelo Kaspersky Anti-Virus for Windows Servers.

Worms

Esta categoria de programas mal-intencionados se dissemina amplamente através da exploração de vulnerabilidades nos sistemas operacionais dos computadores. A classe recebeu esse nome em alusão à forma como os worms (vermes) passam de um computador para outro, por meio de redes e e-mails. Esse recurso permite que os worms se disseminem muito rapidamente.

Os worms entram no computador, buscam endereços de rede de outros computadores e enviam um grande volume de cópias automáticas de si mesmos para esses endereços. Além disso, freqüentemente os worms utilizam dados contidos nos catálogos de endereços dos programas de e-mail. Às vezes, alguns desses programas mal-intencionados criam arquivos de trabalho nos discos do sistema, mas eles podem ser executados sem nenhum recurso do sistema além da RAM.

Vírus

Os vírus são programas que infectam outros arquivos, agregando seu próprio código a eles de maneira a controlar os arquivos infectados quando eles são abertos. Esta definição simples explica a principal ação de um vírus, a *infecção*.

Cavalos de Tróia

Os cavalos de Tróia são programas que executam ações não-autorizadas em computadores, como a exclusão de informações em unidades, o travamento do sistema, o roubo de informações confidenciais e assim por diante. Essa classe de programas mal-intencionados não se constitui em vírus, no sentido tradicional da palavra, pois eles não infectam outros computadores ou dados. Os cavalos de Tróia não conseguem invadir um computador e são disseminados por hackers, que os disfarçam como software comum. Os danos causados por eles podem exceder em muito os ataques de vírus tradicionais.

Atualmente, os worms são o tipo mais comum de programa mal-intencionado utilizado para danificar dados de computadores, seguidos dos vírus e cavalos de Tróia. Alguns programas mal-intencionados combinam recursos de duas ou até três dessas classes.

Adware

Os adwares consistem em programas incluídos no software sem o conhecimento do usuário, com o objetivo de exibir anúncios. Geralmente, o adware vem incorporado a um software distribuído gratuitamente. Os anúncios são apresentados na interface do programa. Freqüentemente, esses programas também coletam dados pessoais do usuário e os enviam para o desenvolvedor, alteram as configurações do navegador (a página inicial, páginas de busca, níveis de segurança, etc.) e geram um tráfego que não pode ser controlado pelo usuário. Tudo isso pode levar a violações de segurança e acarretar prejuízos financeiros diretos.

Spyware

Estes softwares coletam informações sobre um determinado usuário ou organização, sem o conhecimento dos mesmos. Freqüentemente, os spywares não são detectados. Em geral, o objetivo do spyware é:

- controlar as ações do usuário em um computador
- coletar informações sobre o conteúdo do seu disco rígido. Nesses casos, geralmente isso envolve a verificação de vários diretórios e do Registro do sistema para compilar uma lista dos softwares instalados no computador
- coletar informações sobre a qualidade da conexão, largura de banda, velocidade do modem, etc.

Riskware

Os riskwares consistem em software possivelmente perigoso, sem função mal-intencionada, pois contém falhas e erros, mas que pode ser usado por hackers como componente auxiliar de um programa mal-intencionado. Em determinadas situações, ter programas como esses no computador pode colocar os dados em risco. Esses programas incluem, por exemplo, alguns utilitários de administração remota, programas que interferem no layout do teclado, clientes IRC, servidores FTP e utilitários multifuncionais que interrompem ou ocultam processos.

Um outro tipo de programa mal-intencionado semelhante aos adwares, spywares e riskwares são os programas que se conectam ao navegador da Internet e redirecionam o tráfego.

Piadas

Os softwares de piadas não causam danos diretos, mas exibem mensagens informando que houve ou que haverá algum dano, sob determinadas condições. Freqüentemente, esses programas advertem o usuário sobre perigos inexistentes, como mensagens que avisam sobre a formatação do disco rígido (embora isso não ocorra realmente) ou a detecção de vírus em arquivos não infectados.

Rootkits

São utilitários usados para disfarçar a atividade mal-intencionada. Eles encobrem programas mal-intencionados, evitando que sejam detectados por programas antivírus. Os rootkits modificam funções básicas do sistema operacional do computador, ocultando sua própria existência e as ações executadas pelo hacker no computador infectado.

Outros programas perigosos

Estes programas são criados, por exemplo, para configurar ataques DoS a servidores remotos, invadir outros computadores e programas que fazem parte do ambiente de desenvolvimento de programas mal-intencionados. Esses programas incluem ferramentas de hackers, construtores de vírus, programas de varredura de vulnerabilidades, programas para a violação de senhas e outros tipos de programas para invadir os recursos da rede ou penetrar em um sistema.

Aviso!

Desse ponto em diante, usaremos o termo "vírus" para nos referirmos a programas perigosos e mal-intencionados. Enfatizaremos o tipo de programa mal-intencionado somente quando necessário.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

O Kaspersky Anti-Virus for Windows Servers 6.0 representa uma nova geração de produtos de segurança de dados.

2.1. Novidades do Kaspersky Anti-Virus for Windows Servers 6.0

Vamos examinar os novos recursos do Kaspersky Anti-Virus for Windows Servers mais detalhadamente:

Novos recursos de proteção

- A tecnologia de proteção de arquivos do programa foi alterada: agora, você pode diminuir a carga no processador central e nos subsistemas de discos e aumentar a velocidade das verificações de arquivos. Isso é possível devido ao iCheck e ao iSwift. Com essa funcionamento, o aplicativo não verificará os arquivos duas vezes.
- Agora, o processo de verificação é executado em segundo plano, permitindo que o administrador continue usando o computador. Se houver uma concorrência pelos recursos do sistema, a verificação de vírus será interrompida até que a operação do usuário seja concluída; então, ela continuará do ponto onde parou.
- As áreas críticas do servidor, nas quais uma infecção poderia levar a conseqüências sérias, são analisadas por meio de uma tarefa separada. Você pode configurar essa tarefa para ser executada automaticamente sempre que o sistema é iniciado.
- A função de notificação do usuário (consulte a seção 11.8.1 na p. 139) foi ampliada para determinados eventos que acontecem durante o funcionamento do programa. Você mesmo pode selecionar o método de notificação para cada tipo de evento: e-mails, notificações por som, mensagens pop-up.
- Os novos recursos incluem a tecnologia de autodefesa do aplicativo, a proteção contra acesso remoto não autorizado de serviços do programa,

a proteção dos arquivos do aplicativo contra modificação acesso ou não autorizado, e proteção das configurações do programa por senha.

Recursos da nova interface do programa

- A nova interface do Kaspersky Anti-Virus for Windows Servers torna as funções do programa claras e fáceis de usar. Você também pode mudar a aparência do programa usando seus próprios elementos gráficos e esquemas de cores.
- Durante sua utilização, o programa fornece dicas: o Kaspersky Anti-Virus for Windows Servers exibe mensagens informativas sobre o nível de proteção, acompanha sua operação com comentários e dicas, e inclui uma seção de Ajuda completa.

Novos recursos de atualização do programa

- Esta versão do aplicativo inaugura o procedimento de atualização aprimorada: o Kaspersky Anti-Virus verifica automaticamente os pacotes de atualização na fonte. Quando o Antivírus detectar novas atualizações, ele as baixará e instalará no computador.
- O programa baixa as atualizações de maneira incremental, ignorando os arquivos que já foram baixados. Isso diminui o tráfego de download de atualizações em até dez vezes.
- As atualizações são baixadas da fonte mais rápida.
- O programa possui um recurso de reversão da atualização que permite retornar para a versão anterior das assinaturas se, por exemplo, as assinaturas de ameaças forem danificadas ou se houver um erro na cópia.
- Foi adicionado um recurso para a distribuição de atualizações de uma pasta local, de forma que outros computadores da rede tenham acesso a elas economizando largura de banda.

2.2. Os elementos da defesa do Kaspersky Anti-Virus for Windows Servers

A proteção do Kaspersky Anti-Virus for Windows Servers inclui:

- Antivírus de Arquivos (consulte 2.2.1 na p. 17), que monitora o sistema de arquivos do computador em tempo real.

- Tarefas de verificação de vírus (consulte 2.2.2 na p. 17) que verificam vírus na memória e no sistema de arquivos do computador, como arquivos individuais, pastas, discos ou regiões.
- Ferramentas de suporte (consulte 2.2.3 na p. 18) que dão suporte para o programa e ampliam sua funcionalidade.

2.2.1. Antivírus de Arquivos

O servidor é protegido em tempo real usando o **Antivírus de Arquivos**.

Um sistema de arquivos pode conter vírus e outros programas perigosos. Programas mal-intencionados podem ser armazenados no sistema de arquivos sem aparecer durante anos, depois de infectá-los por meio de um disquete ou da Internet. Contudo, basta abrir o arquivo infectado para ativar o vírus instantaneamente.

O *Antivírus de Arquivos* é o componente que monitora o sistema de arquivos do computador. Ele verifica todos os arquivos que estão sendo abertos, executados ou salvos no servidor e em todas as unidades de disco conectadas. O Kaspersky Anti-Virus intercepta todas as tentativas de acessar arquivos e os verifica quanto à presença de vírus conhecidos. O arquivo poderá ser usado somente se não estiver infectado ou ser for neutralizado com êxito pelo Antivírus de Arquivos. Se, por algum motivo, não for possível desinfectar um arquivo, ele será excluído e sua cópia será salva no Backup (consulte 11.2 na p. 122) ou ele será movido para a Quarentena (consulte 11.1 na p. 119).

2.2.2. Tarefas de verificação de vírus

Além de monitorar constantemente todos os possíveis caminhos de programas mal-intencionados usando o Antivírus de Arquivos, é extremamente importante fazer a verificação de vírus periodicamente no computador. Isso é necessário para detectar programas mal-intencionados que não foram descobertos antes pelo programa porque, por exemplo, ele estava definido com um nível de segurança muito baixo.

O Kaspersky Anti-Virus for Windows Servers configura, por padrão, as seguintes tarefas de verificação de vírus:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus. Isso inclui a memória do sistema, os programas carregados na inicialização, os setores de inicialização no disco rígido e os diretórios do sistema do *Microsoft Windows*. Essa tarefa tem como objetivo detectar vírus ativos rapidamente sem verificar todo o computador.

Meu Computador

Verifica vírus no computador com uma inspeção completa de todas as unidades de disco, da memória e dos arquivos.

Objetos de inicialização

Verifica vírus em todos os programas carregados automaticamente na inicialização, além da RAM e dos setores de inicialização dos discos rígidos.

Há também a opção de criar outras tarefas de verificação de vírus e criar uma programação para elas.

2.2.3. Ferramentas de programas

O Kaspersky Anti-Virus for Windows Servers inclui várias ferramentas de suporte criadas para oferecer suporte a software em tempo real, expandindo os recursos do programa e o auxiliando no decorrer do trabalho.

Atualização

Para estar preparado para excluir um vírus ou qualquer outro programa perigoso, o Kaspersky Anti-Virus for Windows Servers precisa ser mantido atualizado. O componente *Atualização* foi criado para fazer exatamente isso. Ele é responsável pela atualização das assinaturas de ameaças e dos módulos do programa Kaspersky Anti-Virus for Windows Servers.

O recurso de Distribuição de atualizações permite salvar atualizações do banco de dados de assinaturas de ameaças e módulos do aplicativo recuperados dos servidores de atualização da Kaspersky Lab e, em seguida, permite que outros computadores tenham acesso a eles, economizando largura de banda.

Arquivos de dados

O Antivírus de Arquivos e cada verificação de vírus e atualização do programa cria um relatório conforme é executada. Os relatórios contêm informações sobre as operações concluídas e seus resultados. Utilizando o recurso *Relatórios*, você ficará sempre atualizado sobre o funcionamento de qualquer componente do Kaspersky Anti-Virus for Windows Servers. Se houver problemas, os relatórios poderão ser enviados para a Kaspersky Lab para que nossos especialistas estudem a situação mais detalhadamente e o ajudem o mais rápido possível.

O Kaspersky Anti-Virus for Windows Servers envia todos os arquivos suspeitos de serem perigosos para uma área específica de *Quarentena*, onde são armazenados em formato criptografado para evitar a infecção

do computador. Você pode verificar esses objetos quanto à presença de vírus, restaurá-los em seus locais anteriores, excluí-los ou adicionar arquivos manualmente à Quarentena. Os arquivos que não estiverem infectados após a conclusão da verificação de vírus serão automaticamente restaurados em seus locais anteriores.

A área de *Backup* mantém cópias dos arquivos desinfectados e excluídos pelo programa. Essas cópias são criadas caso seja necessário restaurar os arquivos ou se você precisar das informações sobre a infecção. Essas cópias de backup também são armazenadas em formato criptografado para evitar outras infecções.

Você pode restaurar manualmente um arquivo do Backup no local original e excluir a cópia.

Suporte

Todos os usuários registrados do Kaspersky Anti-Virus podem tirar proveito de nosso serviço de suporte técnico. Para saber onde você pode obter suporte técnico, use o recurso *Suporte*.

Usando os links, é possível acessar o fórum de usuários da Kaspersky Lab e navegar por uma lista de perguntas freqüentes com respostas que podem ajudá-lo a resolver seu problema. Você também pode enviar um relatório de erros ou perguntas sobre o funcionamento do programa ao Suporte Técnico preenchendo um formulário on-line.

Também é possível acessar o Suporte Técnico on-line e, claro, nossos funcionários estarão sempre prontos para ajudá-lo com o Kaspersky Anti-Virus por telefone.

2.3. Requisitos de hardware e software do sistema

Para que o Kaspersky Anti-Virus seja executado corretamente, seu computador deve atender a estes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço disponível no disco rígido
- CD-ROM (para instalar o Kaspersky Anti-Virus for Windows Servers 6.0 do CD de instalação)
- Microsoft Internet Explorer 5.5 ou superior (para atualizar as assinaturas de ameaças e módulos do programa pela Internet)
- Microsoft Windows Installer 2.0

Sistema operacional:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 ou superior, todas as atualizações disponíveis
- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, todos os Service Packs, todas as atualizações disponíveis
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition

2.4. Pacotes de software

Você pode adquirir a versão do Kaspersky Anti-Virus for Windows Servers na caixa junto a nossos revendedores ou baixá-la de lojas da Internet, incluindo a seção **Loja Virtual** em www.kaspersky.com.br.

Se comprar a versão do programa na caixa, o pacote incluirá:

- Um envelope lacrado contendo um CD de instalação com os arquivos do programa
- Uma chave de licença fornecida com o pacote de instalação ou em um disquete específico, ou um código de ativação do aplicativo na embalagem do CD
- Um Manual do Usuário
- O Contrato de Licença do Usuário Final (EULA)

Antes de abrir o lacre do envelope do disco de instalação, leia atentamente todo o EULA.

Se você comprou o Kaspersky Anti-Virus for Windows Servers em uma loja on-line, copie o produto do site da Kaspersky Lab (**Downloads** → **Product Downloads**). Você pode baixar o Manual do Usuário na seção **Downloads** → **Documentation**.

Você receberá uma chave de licença ou um código de ativação por e-mail após o recebimento do pagamento.

O Contrato de Licença do Usuário Final é um contrato legal entre você e a Kaspersky Lab que especifica os termos segundo os quais você pode usar o software que adquiriu.

Leia todo o EULA atentamente.

Se você não concordar com os termos do EULA, poderá retornar o produto na caixa para o revendedor de quem o comprou e será reembolsado da quantia paga pelo programa. Nesse caso, o envelope lacrado com o disco de instalação ainda deverá estar lacrado.

Ao abrir o disco de instalação lacrado, você aceita todos os termos do EULA.

2.5. Suporte para usuários registrados

A Kaspersky Lab fornece uma variedade de serviços que tornam o Kaspersky Anti-Virus for Windows Servers mais efetivo para seus usuários registrados.

Ao ativar o programa, você se torna um usuário registrado e terá os seguintes serviços disponíveis até que a licença expire:

- Novas versões do programa gratuitamente
- Consultoria sobre questões relativas à instalação, configuração e funcionamento do programa, por telefone e por e-mail
- Notificações sobre novas versões de produtos da Kaspersky Lab e novos vírus (esses serviços se destinam a usuários que assinarem as mensagens de notícias da Kaspersky Lab)

A Kaspersky Lab não fornece suporte técnico relativo ao uso e funcionamento do sistema operacional ou de quaisquer produtos que não sejam de sua propriedade.

CAPÍTULO 3. INSTALANDO O KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Há diversas formas de instalar o Kaspersky Anti-Virus 6.0 for Windows Servers:

- Instalação local: instala o aplicativo em um único host. É necessário ter acesso direto a esse host para executar e concluir a instalação. É possível executar uma instalação local em um dos modos a seguir:
    - instalação interativa usando o Assistente para Instalação do aplicativo (consulte 3.1 na p. 23); esse modo exige a participação do usuário para a continuidade da instalação;
    - instalação não interativa, executada da linha de comando usando configurações padrão, sem exigir a participação do usuário para a continuidade da instalação (consulte 3.3 na p. 33).
- Instalação remota: instala o aplicativo nos aplicativos em rede remotamente, da estação de trabalho do administrador, usando:
    - o conjunto de software Kaspersky Administration Kit (consulte o Manual de Implementação do Kaspersky Administration Kit);
    - diretivas de domínio de grupo do Microsoft Windows Server 2000/2003 (consulte 3.4 na p. 34).

É recomendável fechar todos os aplicativos em execução antes de instalar o Kaspersky Anti-Virus (inclusive na instalação remota).

No caso de o Kaspersky Anti-Virus 5.0 já estar instalado, ele será removido e atualizado para o Kaspersky Anti-Virus 6.0 ao executar o procedimento de instalação (para obter mais detalhes, consulte 3.5 na p. 36). As atualizações para compilações mais recentes (versões secundárias) do Kaspersky Anti-Virus 6.0 são transparentes.

3.1. Procedimento de instalação usando o Assistente para Instalação

Para instalar o Kaspersky Anti-Virus for Windows Servers no computador, abra o arquivo do Windows Installer no CD de instalação.

> Observação:
>
> A instalação do programa por meio de um pacote de instalação baixado pela Internet é igual à instalação a partir de um CD de instalação.

Um assistente para instalação do programa será aberto. Cada janela contém um conjunto de botões para navegar pelo processo de instalação. Segue uma breve explicação sobre suas funções:

- **Avançar** – aceita uma ação e avança para a próxima etapa da instalação.
- **Voltar** – volta para a etapa anterior da instalação.
- **Cancelar** – cancela a instalação do produto.
- **Concluir** – conclui o procedimento de instalação do programa.

Vamos examinar as etapas do procedimento de instalação mais detalhadamente.

Etapa 1. Verificando as condições do sistema necessárias para instalar o Kaspersky Anti-Virus for Windows Servers

Antes de o programa ser instalado no computador, o sistema operacional e os pacotes de serviços necessários para a instalação do Kaspersky Anti-Virus for Windows Servers são verificados no computador. Também são verificados os outros programas necessários e se os seus direitos de usuário permitem a instalação de software.

Se algum desses requisitos não for atendido, o programa exibirá uma mensagem informando-o. É recomendável instalar os programas e os pacotes de serviços necessários através do **Windows Update** antes de instalar o Kaspersky Anti-Virus for Windows Servers.

Etapa 2.Janela de boas-vindas da instalação

Se o sistema atender a todos os requisitos, uma janela de instalação com informações sobre como iniciar a instalação do Kaspersky Anti-Virus for Windows Servers aparecerá ao abrir o arquivo de instalação.

Para continuar a instalação, clique no botão **Avançar**. Você pode cancelar a instalação clicando em **Cancelar**.

Etapa 3.Exibindo o Contrato de Licença do Usuário Final

A janela a seguir contém o Contrato de Licença do Usuário Final firmado entre você e a Kaspersky Lab. Leia-o atentamente e, se concordar com todos os termos do contrato, selecione **Eu aceito os termos do Contrato de Licença** e clique no botão **Avançar**. A instalação continuará.

Para cancelar a instalação, clique em **Cancelar**.

Etapa 4.Selecionando uma pasta de instalação

O próximo estágio da instalação do Kaspersky Anti-Virus for Windows Servers determina o local onde o programa será instalado no computador. O caminho padrão é o seguinte:

- **<Unidade>\Arquivos de Programa\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – para sistemas de 32 bits
- **<Unidade>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – para sistemas de 64 bits

Você pode especificar outra pasta clicando no botão **Procurar** e selecionando-a na janela de seleção de pastas ou inserindo o caminho para a pasta no campo disponível.

Lembre-se de que, se você inserir o caminho completo da pasta de instalação manualmente, ele não poderá exceder 200 caracteres, nem conter caracteres especiais.

Para continuar a instalação, clique no botão **Avançar**.

Etapa 5.Usando as configurações de instalação salvas

Nesta etapa, é solicitado que você especifique se deseja usar as configurações de segurança ou as assinaturas de ameaças salvas anteriormente, caso elas tenham sido realmente salvas ao remover uma instalação anterior do Kaspersky Anti-Virus 6.0 do servidor.

Vamos examinar mais detalhadamente como usar as opções descritas acima.

Se você tiver instalado anteriormente outra versão ou compilação do Kaspersky Anti-Virus for Windows Servers no computador e tiver salvado suas assinaturas de ameaças ao desinstalá-la, poderá usá-las na versão atual. Para fazê-lo, marque **Assinaturas de ameaças**. As assinaturas de ameaças incluídas com o programa de instalação não serão copiadas no servidor.

Para usar as configurações de proteção definidas e salvas em uma versão anterior, marque **Configurações de proteção**.

Etapa 6. Selecionando um tipo de instalação

Neste estágio, selecione as partes do programa que deseja instalar no computador. Existem três opções:

Completa. Se você selecionar esta opção, todos os componentes do Kaspersky Anti-Virus for Windows Servers serão instalados. Para saber mais, consulte a Etapa 8.

Personalizada. Se você selecionar esta opção, poderá selecionar os componentes do programa que deseja instalar. Para saber mais, consulte a Etapa 7.

Para selecionar um tipo de instalação, clique no botão apropriado.

Etapa 7. Selecionando os componentes do programa a serem instalados

Esta etapa será executada somente se você selecionar o tipo de instalação **Personalizada**.

Se você selecionou a instalação Personalizada, poderá escolher os componentes do Kaspersky Anti-Virus for Windows Servers que deseja instalar. Por padrão, o Antivírus de Arquivos, o componente de verificação de vírus e o conector do Agente Administrativo para administração remota usando o Kaspersky Administration Kit são selecionados para a instalação.

Para selecionar os componentes que deseja instalar, clique no ícone ao lado do nome de um componente e selecione **Será instalado no disco rígido local** no menu exibido. Você encontrará mais informações sobre a proteção que um componente selecionado fornece e quanto espaço em disco é necessário para sua instalação na parte inferior da janela de instalação do programa.

Se não desejar instalar um componente, selecione **O recurso completo será instalado no disco rígido local** no menu de contexto.

Depois de selecionar os componentes que deseja instalar, clique em **Avançar**. Para fazer a lista retornar aos programas padrão a serem instalados, clique em **Redefinir**.

Etapa 8.Pesquisando outros programas antivírus

Neste estágio, a instalação pesquisa outros produtos antivírus instalados no servidor, incluindo produtos da Kaspersky Lab, que poderiam gerar problemas de compatibilidade com o Kaspersky Anti-Virus for Windows Servers.

A instalação exibirá na tela uma lista desses programas detectados. O programa perguntará se deseja desinstalá-los antes de continuar a instalação.

Você pode selecionar a desinstalação manual ou automática na lista de aplicativos antivírus detectados (somente os produtos da Kaspersky Lab serão excluídos automaticamente).

Para continuar a instalação, clique no botão **Avançar**.

Etapa 9.Concluindo a instalação do programa

Neste estágio, o programa solicitará que você conclua a instalação do programa no servidor.

É recomendável não desmarcar ☑ **Habilitar Autodefesa antes da instalação** ao instalar o Kaspersky Anti-Virus 6.0 pela primeira vez. Ao habilitar os módulos de proteção, você poderá reverter a instalação corretamente, se ocorrerem erros na instalação do programa. Se estiver reinstalando o programa, é recomendável desmarcar esta caixa de seleção.

Se o aplicativo for instalado remotamente por meio da **Área de Trabalho Remota do Windows**, é recomendável marcar ☑ **Habilitar Autodefesa antes da instalação**. Caso contrário, talvez o procedimento de instalação não seja concluído corretamente.

Se desejar que as exclusões recomendadas pela Microsoft para servidores sejam automaticamente adicionadas às exclusões, marque ☑ **Excluir áreas recomendadas pela Microsoft da verificação de vírus**.
Se desejar que a variável de ambiente %Path% seja adicionada ao avp.com depois da instalação, marque ☑ **Adicionar caminho de avp.com à variável do sistema %PATH%**.

Para continuar a instalação, clique no botão **Avançar**.

Aviso!

Ao instalar os componentes do Kaspersky Anti-Virus que interceptam o tráfego de rede, as conexões de rede atuais são desfeitas. A maioria delas será recuperada após algum tempo.

Etapa 10. Concluindo o procedimento de instalação

A janela **Instalação concluída** contém informações sobre como concluir o processo de instalação do Kaspersky Anti-Virus.

Para iniciar o Assistente para Instalação, clique no botão **Avançar** (consulte 3.2 na p. 27).

Se a instalação for concluída com êxito, será necessário reiniciar o computador e uma mensagem na tela o informará.

3.2. Assistente para Instalação

O Assistente para Instalação do Kaspersky Anti-Virus for Windows Servers 6.0 é iniciado depois de o programa ter concluído a instalação. Ele foi criado para ajudá-lo a definir as configurações iniciais do programa para se ajustarem aos recursos e usos do computador.

A interface do Assistente para Instalação foi criada como um assistente padrão do Windows e consiste em uma série de etapas pelas quais você pode navegar usando os botões **Avançar** e **Voltar**, ou concluir, usando o botão **Concluir**. O botão **Cancelar** interromperá o Assistente a qualquer momento.

Se você interromper o assistente para instalação fechando sua janela, o aplicativo não será executado. Cada vez que você iniciar o aplicativo, o assistente para instalação será iniciado, até que o procedimento de configuração seja concluído com êxito.

3.2.1. Usando objetos salvos na Versão 5.0

Esta janela do assistente será exibida depois de concluir o processo de instalação do aplicativo sobre o Kaspersky Anti-Virus 5.0. Será solicitado que você selecione os dados usados pela verão 5.0 que deseja importar para a versão 6.0. Podem estar incluídos os arquivos da quarentena ou do backup, ou as configurações de proteção.

Para usar esses dados na Versão 6.0, marque as caixas desejadas.

3.2.2. Ativando o programa

Antes de ativar o programa, verifique se as configurações de data do sistema do computador correspondem à data e hora atuais.

O programa é ativado pela instalação de uma chave de licença que será usada pelo Kaspersky Anti-Virus para verificar a licença e determinar sua data de validade.

A chave de licença contém as informações do sistema necessárias para o funcionamento de todos os recursos do programa e outras informações:

- Informações de suporte (que fornecem suporte ao programa e onde é possível obtê-lo)
- Nome, número e data de expiração de sua licença

3.2.2.1. Selecionando um método de ativação do programa

Dependendo de você possuir uma chave de licença do Kaspersky Anti-Virus ou precisar obtê-la do servidor da Kaspersky Lab, diferentes opções para ativar o programa estarão disponíveis:

- **Ativar usando o código de ativação**. Selecione esta opção de ativação se tiver comprado a versão completa do programa e recebido um código de ativação. Com esse código de ativação, você poderá obter um arquivo de chave que dá acesso à funcionalidade completa do aplicativo durante a vigência do contrato de licença.
- **Ativar versão de teste.** Selecione esta opção de ativação para instalar a versão de teste do programa antes de decidir comprar a versão comercial. Você receberá uma chave de licença gratuita válida por um período especificado no contrato de licença da versão de teste.
- **Aplicar chave de licença existente**. Ativa o aplicativo usando um arquivo de chave de licença do Kaspersky Anti-Virus 6.0.
- **Ativar mais tarde**. Se você escolher esta opção, o estágio de ativação será ignorado. O Kaspersky Anti-Virus for Windows Servers 6.0 será instalado no computador e você terá acesso a todos os recursos do programa, exceto as atualizações (é possível atualizar as assinaturas de ameaças somente depois de instalar o programa).

As duas primeiras opções de ativação utilizam um servidor Web da Kaspersky Lab, o que exige uma conexão com a Internet. Antes da ativação, edite suas configurações de rede (consulte 10.4.3 na p. 114) na janela que é aberta ao

clicar em **Configurações da LAN** (se necessário). Para obter informações mais detalhadas sobre a configuração da rede, entre em contato com o administrador do sistema ou seu provedor.

Se não houver uma conexão com a Internet ao instalar o programa, você poderá ativar o aplicativo posteriormente (consulte 11.5 na p. 134) usando sua interface ou poderá utilizar o acesso à Internet de outro computador para se registrar no site de Suporte Técnico da Kaspersky Lab e obter a chave usando o código de ativação.

3.2.2.2. Inserindo o código de ativação

É necessário ter um código para ativar o programa. Ao comprar o programa pela Internet, você receberá o código de ativação por e-mail. Se comprou uma versão do programa na caixa, encontrará o código de ativação no envelope do CD-ROM de instalação.

O código de ativação é uma seqüência de números e letras separados por hífens em quatro seções de cinco caracteres, sem espaços. Por exemplo, 11AA1-11AAA-1AA11-1A111. Observe que o código deve ser inserido usando caracteres latinos.

Digite suas informações de contato na parte inferior da janela: nome completo, endereço de e-mail, país e cidade de residência. Essas informações poderão ser solicitadas para identificar um usuário registrado se, por exemplo, uma chave for perdida ou roubada. Caso isso ocorra, suas informações de contato permitirão que você obtenha uma nova chave de licença.

3.2.2.3. Obtendo um arquivo de chave

O Assistente para Instalação se conecta aos servidores da Kaspersky Lab e envia seus dados de registro (o código de ativação e as informações pessoais), que são inspecionados no servidor.

Se o código de ativação passar na inspeção, o Assistente receberá um arquivo de chave. Se você instalar a versão de demonstração do programa, o Assistente para Instalação receberá o arquivo da chave de teste sem um código de ativação.

O arquivo recebido será instalado automaticamente para executar o programa e você verá uma janela de conclusão da ativação com informações detalhadas sobre a chave usada.

Se o código de ativação não passar na inspeção, você verá uma mensagem correspondente na tela. Se isso ocorrer, entre em contato com o fornecedor do software de quem você comprou o programa para obter mais informações.

3.2.2.4. Selecionando o arquivo da chave de licença

Se você possuir um arquivo de chave de licença do Kaspersky Anti-Virus for Windows Servers 6.0, o Assistente perguntará se deseja instalá-lo. Se desejar, use o botão **Procurar** e selecione o caminho do arquivo da chave com a extensão *.key* na janela de seleção de arquivos.

Depois de ter instalado a chave com êxito, você verá informações sobre a licença na parte inferior da janela: nome do proprietário do software, número da licença, tipo de licença (completo, teste beta, demonstração etc.) e data de expiração da chave.

3.2.2.5. Concluindo a ativação do programa

O Assistente para Instalação o informará que a ativação do programa foi bem-sucedida. Também serão exibidas informações sobre a chave de licença instalada: nome do proprietário do software, número da licença, tipo de licença (completo, teste beta, demonstração etc.) e data de expiração da chave.

3.2.3. Configurando a atualização

A segurança do computador depende diretamente da atualização periódica das assinaturas de ameaças e dos módulos do programa. Nesta janela, o Assistente para Instalação solicita que você selecione um modo de atualização do programa e que configure uma programação.

- **Automaticamente**. O Kaspersky Anti-Virus verifica os pacotes de atualização na fonte em intervalos definidos. É possível definir as verificações de forma que sejam mais freqüentes durante os surtos de vírus e menos freqüentes quando eles terminarem. Quando o Antivírus detectar novas atualizações, ele as baixará e instalará no computador. Essa é a configuração padrão.
- **A cada 2 hora(s)**.As atualizações serão executadas automaticamente de acordo com a programação criada. Você pode configurar a programação clicando em **Alterar**.
- **Manualmente**. Se escolher esta opção, você mesmo executará as atualizações do produto.

Observe que as assinaturas de ameaças e os módulos do programa incluídos com o software podem estar desatualizados ao instalar o programa. Por isso, é recomendável baixar as atualizações mais recentes do programa. Para fazê-lo, clique em **Atualizar agora**. Em seguida, o Kaspersky Anti-Virus for Windows

Servers baixará as atualizações necessárias dos servidores de atualização e as instalará no computador.

Para configurar as atualizações (configurar propriedades de rede, selecionar o recurso do qual as atualizações serão baixadas, configurar a tarefa de execução com uma determinada conta ou habilitar a opção de distribuição de atualizações), clique em **Configurações**.

3.2.4. Configurando uma programação de verificação de vírus

A verificação de objetos mal-intencionados em áreas selecionadas do computador é uma das principais etapas da proteção do mesmo.

Ao instalar o Kaspersky Anti-Virus for Windows Servers, três tarefas de verificação de vírus padrão são criadas. Nesta janela, o Assistente para Instalação solicita que você escolha uma configuração para a tarefa de verificação:

Objetos de inicialização

Por padrão, o Kaspersky Anti-Virus verifica automaticamente os objetos de inicialização ao ser iniciado. Você pode editar as configurações da programação em outra janela, clicando em **Alterar**.

Áreas críticas

Para verificar automaticamente as áreas críticas do computador (memória do sistema, objetos de inicialização, setores de inicialização, pastas do sistema do Windows) quanto à presença de vírus, marque a caixa apropriada. Você pode configurar a programação clicando em **Alterar**.

A configuração padrão dessa verificação automática é desabilitada.

Meu Computador

Para que uma verificação completa de vírus no seu computador seja executada automaticamente, marque a caixa apropriada. Você pode configurar a programação clicando em **Alterar**.

A configuração padrão para a execução programada dessa tarefa é desabilitada. Contudo, é recomendável executar uma verificação completa de vírus no servidor imediatamente após a instalação do programa.

3.2.5. Restringindo o acesso ao programa

O Kaspersky Anti-Virus permite que você proteja o programa por senha, pois várias pessoas podem usar o mesmo computador e programas mal-intencionados poderiam possivelmente desabilitar a proteção. O uso de uma senha pode proteger o programa de tentativas não-autorizadas de desabilitar a proteção ou alterar as configurações.

Para habilitar a proteção por senha, marque ☑ **Habilitar proteção por senha** e preencha os campos **Senha** e **Confirmar senha**.

Selecione a seguir a área na qual deseja aplicar a proteção por senha:

- ◉ **Todas as operações (exceto notificações de eventos perigosos)**. Solicita a senha se o usuário tenta executar qualquer ação no programa, exceto pelas respostas a notificações sobre a detecção de objetos perigosos.
- ◉ **Operações selecionadas:**
  - ☑ **Ao salvar configurações do programa** – solicita a senha quando um usuário tenta salvar alterações das configurações do programa.
  - ☑ **Ao sair do programa:** solicita a senha se um usuário tentar fechar o programa.
  - ☑ **Ao interromper/pausar componentes de proteção ou tarefas de verificação de vírus** – solicita a senha se o usuário tentar pausar ou desabilitar completamente qualquer componente de proteção ou tarefa de verificação de vírus.

3.2.6. Concluindo o Assistente para Instalação

Na última janela do assistente, você verá uma mensagem informando que o programa foi instalado e configurado com êxito. Você pode iniciar o aplicativo imediatamente, marcando ☑ **Iniciar produto**.

Se aconteceu algo errado durante a instalação, como um problema de incompatibilidade com outros aplicativos antivírus, será solicitado que você reinicie o computador.

3.3. Instalando o programa do prompt de comando

Para instalar o Kaspersky Anti-Virus 6.0 for Windows Servers, digite o seguinte no prompt de comando:

```
msiexec /i <nome_do_pacote>
```

O Assistente para Instalação será iniciado (consulte a seção 3.1 na p. 23). Depois que o programa for instalado, reinicie o computador.

Para instalar o aplicativo de maneira não interativa (sem executar o Assistente para Instalação), digite:

```
msiexec /i <nome_do_pacote> /qn
```

Esta opção exigirá a reinicialização manual da máquina após a conclusão da instalação. Para executar a reinicialização automática da linha de comando, digite:

```
msiexec /i <nome_do_pacote> ALLOWREBOOT=1 /qn
```

No modo não interativo, a reinicialização ocorrerá automaticamente (usando a chave /qn).

Para instalar o aplicativo com uma senha de desinstalação, digite:

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=******`, ao executar uma instalação interativa;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** /qn`, ao executar uma instalação não interativa sem inicialização do sistema;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, ao executar uma instalação não interativa com inicialização do sistema;

Se você instalar o Kaspersky Anti-Virus no modo não interativo, poderá acessar o arquivo *setup.ini*, que contém as configurações gerais para a instalação do aplicativo (consulte A.4 na p. 190), a configuração *install.cfg* (consulte 13.7 na p. 178) e o arquivo da chave de licença. Esses arquivos devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus.

3.4. Procedimento para a instalação do Objeto de Diretiva de Grupo

Há suporte para este recurso em computadores que executam o Microsoft Windows 2000 Server ou superior.

Com o **Editor de Objeto de Diretiva de Grupo**, você pode instalar, atualizar e desinstalar o Kaspersky Anti-Virus em estações de trabalho empresariais no domínio sem usar o Kaspersky Administration Kit.

3.4.1. Instalando o programa

Para instalar o Kaspersky Anti-Virus:

1. Crie uma pasta compartilhada no computador que é o controlador de domínio e copie o pacote de instalação *.msi* do Kaspersky Anti-Virus para ela.

   Você também pode copiar o arquivo *setup.ini*, que contém as configurações gerais para a instalação do aplicativo (consulte A.4 na p. 190), a configuração *install.cfg* (consulte 13.7 na p. 178) e o arquivo da chave de licença.

2. Abra o **Editor de Objeto de Diretiva de Grupo** via MMC (para obter informações mais detalhadas sobre o uso do Objeto de Diretiva de Grupo, consulte a ajuda do Microsoft Windows Server).

3. Crie um novo pacote. Para fazê-lo, na árvore do console, selecione **Objeto de Diretiva de Grupo** / **Configuração do Computador** / **Configurações de Software** / **Instalação de software** e use o comando **Novo** / **Pacote** no menu de contexto.

   Na janela que é aberta, especifique o caminho da pasta compartilhada no instalador do Anti-Virus (veja 1). Selecione **Atribuir** na caixa de diálogo **Selecione o Método de Implantação** e clique em **OK**.

A diretiva de grupo será imposta em cada estação de trabalho da próxima vez que o computador for registrado no domínio. Então, o Kaspersky Anti-Virus será instalado em todos os computadores.

3.4.2. Atualizando o programa

Para atualizar o Kaspersky Anti-Virus:

1. Copie o pacote do instalador que contém a atualização do Kaspersky Anti-Virus no formato *.msi* para a pasta compartilhada.
2. Abra o **Editor de Objeto de Diretiva de Grupo** e crie um novo pacote usando as etapas acima.
3. Selecione o novo pacote e, em seguida, o comando **Propriedades** no menu de contexto. Na janela de propriedades do pacote, vá para a guia **Atualizações** e especifique o pacote que contém o instalador da versão anterior do Kaspersky Anti-Virus. Para instalar a atualização do Kaspersky Anti-Virus e manter as configurações da proteção, selecione esta opção ao atualizar a versão anterior.

A diretiva de grupo será imposta em cada estação de trabalho da próxima vez que o computador for registrado no domínio.

Não é possível atualizar o Kaspersky Anti-Virus com o Editor de Objeto de Diretiva de Grupo em computadores que executam o Microsoft Windows 2000 Server.

3.4.3. Desinstalando o programa

Para desinstalar o Kaspersky Anti-Virus:

1. Abra o **Editor de Objeto de Diretiva de Grupo**.
2. Para fazê-lo, na árvore do console, selecione **Objeto de Diretiva de Grupo** / **Configuração do Computador** / **Configurações de Software** / **Instalação de software**.

   Selecione o pacote do Kaspersky Anti-Virus na lista. Abra o menu de contexto e selecione o comando **Todas as Tarefas** / **Remover**.

   Na caixa de diálogo **Remover Software**, selecione **Desinstalar imediatamente o software dos usuários e computadores** para que o Kaspersky Anti-Virus seja desinstalado da próxima vez que o computador for reiniciado.

3.5. Atualizando da versão 5.0 para a versão 6.0

Se o Kaspersky Anti-Virus 5.0 for Windows File Servers estiver instalado no seu servidor, você poderá atualizá-lo para o Kaspersky Anti-Virus 6.0 for Windows Servers.

Depois de iniciar o programa de instalação do Kaspersky Anti-Virus 6.0, você terá a opção de primeiro desinstalar a versão 5.0 já instalada. Quando o programa tiver sido desinstalado, reinicie o computador e a instalação da versão 6.0 será iniciada.

Aviso!

Se você estiver instalando o Kaspersky Anti-Virus 6.0 for Windows Servers de uma pasta de rede protegida por senha sobre uma versão anterior do programa, observe o seguinte. Depois de desinstalar a versão 5.0 do aplicativo e reiniciar o computador, o programa de instalação não permitirá que você acesse a pasta de rede na qual o pacote do instalador do aplicativo está localizado. Assim, a instalação do programa será interrompida. Para instalar o programa corretamente, execute o instalador somente de uma pasta local.

CAPÍTULO 4. INTERFACE DO PROGRAMA

O Kaspersky Anti-Virus for Windows Servers possui uma interface direta e amigável. Este capítulo aborda seus recursos básicos:

- Ícone da bandeja do sistema (consulte a seção 4.1 na p. 37)
- Menu de contexto (consulte a seção 4.2 na p. 38)
- Janela principal (consulte a seção 4.3 na p. 39)
- Janela de configurações do programa (consulte a seção 4.4 na p. 41)

4.1. Ícone da bandeja do sistema

Logo após a instalação do Kaspersky Anti-Virus for Windows Servers, seu ícone aparecerá na bandeja do sistema.

O ícone indica as funções do Kaspersky Anti-Virus for Windows Servers. Ele reflete o status da proteção e mostra várias funções básicas executadas pelo programa.

Se o ícone estiver ativo  (colorido), seu computador estará protegido. Se o ícone estiver inativo  (preto e branco), a proteção em tempo real estará desabilitada.

O ícone do Kaspersky Anti-Virus for Windows Servers muda dependendo da operação em execução:

	Um arquivo que você ou algum programa está abrindo, salvando ou executando está sendo verificado.
	As assinaturas de ameaças e módulos do Kaspersky Anti-Virus estão sendo atualizados.
	Ocorreu um erro em algum componente do Kaspersky Anti-Virus.

O ícone também dá acesso aos principais itens da interface do programa: o menu de contexto (consulte a seção 4.2 na p. 38) e a janela principal (consulte a seção 4.3 na p. 39).

Para abrir o menu de contexto, clique com o botão direito do mouse no ícone do programa.

Para abrir a janela principal do Kaspersky Anti-Virus for Windows Servers na seção **Proteção** (a primeira tela padrão ao abrir o programa), clique duas vezes no ícone do programa. Se você clicar uma vez, a janela principal será aberta na seção que estava ativa quando foi fechada pela última vez.

4.2. O menu de contexto

Você pode executar tarefas de proteção básicas do menu de contexto (veja a Figura 1).

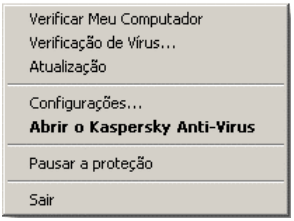


Figura 1. O menu de contexto

O menu do Kaspersky Anti-Virus for Windows Servers contém os seguintes itens:

Verificar Meu Computador – inicia uma verificação completa do computador. Os arquivos em todas as unidades, incluindo mídias de armazenamento removíveis, serão verificados.

Verificação de Vírus… – seleciona objetos e inicia sua verificação quanto à presença de vírus. A lista padrão contém vários arquivos, como a memória do sistema, a pasta Inicialização, bancos de dados de e-mail, todas as unidades do computador, etc. Você pode completar a lista, selecionar arquivos para serem verificados e iniciar verificações de vírus.

Atualização – inicia a atualização dos módulos do programa e das assinaturas de ameaças, e os instala no computador.

Ativar – ativa o programa. É necessário ativar sua versão do Kaspersky Internet Security para obter o status de usuário registrado, que permite o acesso à funcionalidade integral do aplicativo e ao Suporte Técnico. Este item de menu estará disponível somente se o programa não estiver ativado.

Configurações... – exibe e configura o Kaspersky Anti-Virus for Windows Servers.

Abrir o Kaspersky Anti-Virus – abre a janela principal do programa (consulte 4.3 na página 39).

Pausar a Proteção / Reiniciar a Proteção – desabilita temporariamente ou habilita o Antivírus de Arquivos (consulte 2.2.1 na p. 17). Este item do menu não afeta tarefas de atualização do programa ou de verificação de vírus.

Sair – fecha o Kaspersky Anti-Virus for Windows Servers (ao selecionar esta opção, o aplicativo será descarregado da RAM do computador).

Se uma tarefa de pesquisa de vírus estiver em execução, o menu de contexto exibirá seu nome com um medidor de porcentagem de andamento. Ao selecionar a tarefa, você poderá abrir a janela de relatório para exibir os resultados de desempenho atuais.

4.3. Janela principal do programa

A janela principal do Kaspersky Anti-Virus for Windows Servers (veja a Figura 2) pode ser dividido logicamente em duas partes:

Figura 2. Janela principal do Kaspersky Anti-Virus for Windows Servers

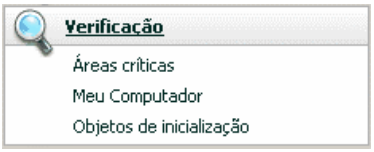
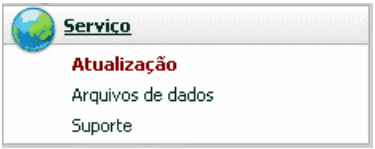
- à esquerda da janela, o painel de navegação o orienta de maneira rápida e fácil para qualquer componente, o desempenho da tarefa de

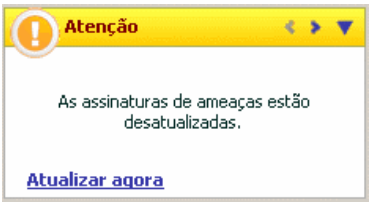
atualização e verificação de vírus ou as ferramentas de suporte do programa;

- à direita da janela, o painel informativo contém informações sobre o componente de proteção selecionado à esquerda e exibe as configurações de cada um deles, fornecendo ferramentas para executar verificações de vírus, trabalhar com arquivos em quarentena e cópias de backup, gerenciar chaves de licença, etc.

Ao selecionar uma seção à esquerda da janela, você encontrará informações correspondentes à direita.

Agora, vamos examinar mais detalhadamente os elementos do painel de navegação da janela principal.

Seção da janela principal	Finalidade
Essencialmente, esta janela o informa sobre o status de proteção do seu computador. A seção **Proteção** foi criada exatamente para isso. 	Aqui, você encontrará informações gerais sobre as operações do Kaspersky Anti-Virus for Windows Servers, sendo possível verificar se tudo está sendo executado corretamente e examinar as estatísticas gerais.
Para verificar programas ou arquivos mal-intencionados no computador, use a seção **Verificação** específica na janela principal. 	Esta seção contém uma lista de objetos que podem ser verificados quanto à presença de vírus. As tarefas mais comuns e mais importantes são incluídas nesta seção. Elas incluem tarefas de verificação de vírus em áreas críticas, em programas de inicialização e a verificação completa do computador.
A seção **Serviço** inclui recursos adicionais do Kaspersky Anti-Virus for Windows Servers. 	Aqui, você pode atualizar o aplicativo, exibir relatórios sobre as tarefas e componentes concluídos e em execução, e trabalhar com objetos em quarentena e de backup, examinar informações de suporte técnico e gerenciar chaves de licença.

A seção de **comentários e dicas** o acompanha durante o uso do aplicativo.  	Nesta seção, existem dicas de como aumentar o nível de proteção do servidor. Você também encontrará comentários sobre o desempenho atual do aplicativo e suas configurações.

Cada elemento do painel de navegação é acompanhado por um menu de contexto específico. Assim, o menu contém pontos para o Antivírus de Arquivos e as ferramentas que ajudam a configurá-los rapidamente, gerenciá-los e exibir relatórios. Existe um item de menu adicional para tarefas de verificação de vírus e de atualização que permite que você crie sua própria tarefa modificando uma cópia de uma tarefa selecionada.

Você pode mudar a aparência do programa criando e usando seus próprios elementos gráficos e esquemas de cores.

4.4. Janela de configurações do programa

Você pode abrir a janela de configurações do Kaspersky Anti-Virus for Windows Servers a partir da janela principal (consulte 4.3 na página 39). Para fazê-lo, clique em Configurações na parte superior da janela.

A janela de configurações (veja a Figura 3) tem um layout semelhante ao da janela principal:

- à esquerda da janela, você tem acesso rápido e fácil às configurações de cada tarefa de atualização e verificação de vírus e do Antivírus de Arquivos, e às ferramentas do programa;
- à direita da janela, existe uma lista detalhada de configurações do item selecionado à esquerda.

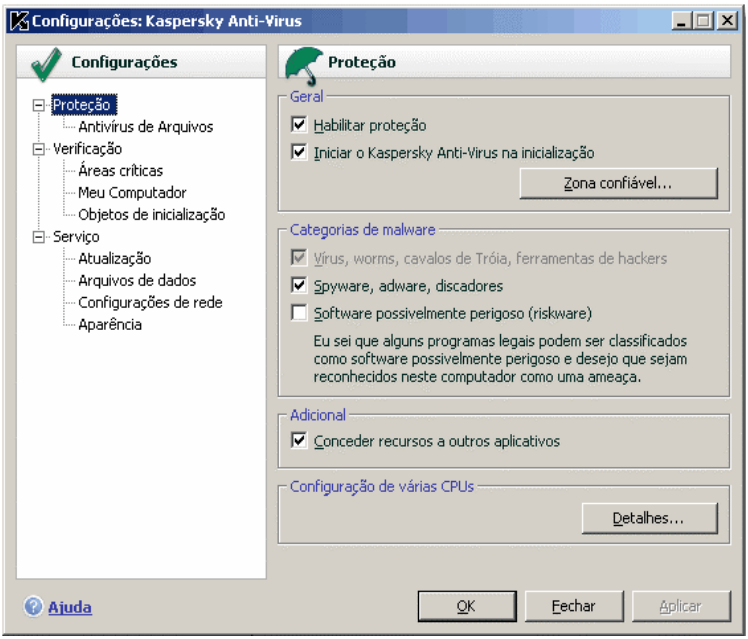


Figura 3. Janela de configurações do Kaspersky Anti-Virus for Windows Servers

Ao selecionar qualquer seção, componente ou tarefa à esquerda da janela de configurações, a parte direita exibirá suas configurações básicas. Para definir configurações avançadas, você pode abrir janelas de configurações de segundo e terceiro níveis. Uma descrição detalhada das configurações do programa encontra-se nas seções correspondentes do Manual do Usuário.

CAPÍTULO 5. INTRODUÇÃO

Uma das principais metas da Kaspersky Lab na criação do Kaspersky Anti-Virus for Windows Servers é o fornecimento de uma configuração ótima para todas as opções do programa.

Para tornar mais fácil começar, combinamos todos os estágios preliminares de configuração em um Assistente para Instalação (consulte a seção 3.2 na p. 27) que é iniciado assim que o programa é instalado. Seguindo as instruções do Assistente, você pode ativar o programa, configurar as atualizações e verificações de vírus, além de proteger o acesso ao programa por senha.

Depois de instalar e iniciar o programa, é recomendável executar as seguintes etapas:

- Verifique o status de proteção atual (consulte 5.1 na página 43) para certificar-se de que o Kaspersky Anti-Virus for Windows Servers está sendo executado no nível apropriado.
- Atualize o programa (consulte a seção 5.5 na p. 51) se o Assistente para Instalação não o fizer automaticamente depois de instalar o programa.
- Verifique o computador (consulte a seção 5.2 na p. 49) quanto à presença de vírus.

5.1. Qual é o status de proteção do computador?

Informações complexas sobre a proteção do computador são fornecidas na janela principal do programa, na seção **Proteção**. O *status de proteção atual* do computador e as *estatísticas gerais de desempenho* do programa são exibidos aqui.

O **status de proteção** exige o estado atual de proteção do computador usando indicadores especiais (consulte 5.1.1 na página 43). As estatísticas (consulte 5.1.2 na página 47) analisam a sessão atual do programa.

5.1.1. Indicadores de proteção

O **status de proteção** é determinado por três indicadores (veja a Figura 4) que refletem aspectos diversos da proteção do computador a qualquer momento e que indicam problemas nas configurações e no desempenho do programa.

Cada indicador tem três aparências possíveis:

– *a situação é normal*; o indicador mostra que a proteção do computador está adequada e que não há problemas na configuração ou no desempenho do programa.

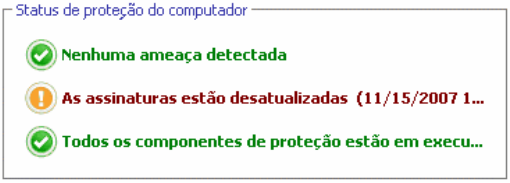


Figura 4. Indicadores que refletem o status de proteção do computador

– *existem um ou mais desvios* no desempenho do Kaspersky Anti-Virus for Windows Servers com relação ao nível recomendado, o que poderia afetar a segurança das informações. Preste atenção às ações recomendadas pela Kaspersky Lab, fornecidas em links.

– *o status de segurança do computador é crítico*. Siga rigorosamente as recomendações para aprimorar a proteção do computador. São fornecidos links para as ações recomendadas.

Agora, vamos examinar os indicadores de proteção e as situações indicadas por cada um deles mais detalhadamente.

O primeiro indicador reflete a situação de arquivos e programas mal-intencionados no computador. Os três valores deste indicador significam o seguinte:

	Nenhuma ameaça detectada O Kaspersky Anti-Virus for Windows Servers não detectou nenhum arquivo ou programa perigoso no computador.
	Todas as ameaças foram neutralizadas O Kaspersky Anti-Virus for Windows Servers neutralizou todos os arquivos e programas infectados, e excluiu os que não puderam ser neutralizados.

	*Foram detectadas ameaças* Existe risco de infecção no computador. O Kaspersky Anti-Virus for Windows Servers detectou programas mal-intencionados (vírus, cavalos de Tróia, worms, etc.) que devem ser neutralizados. Para fazê-lo, use o link Neutralizar tudo. Clique no link Detalhes para ver informações mais detalhadas sobre os objetos mal-intencionados.

O segundo indicador mostra a eficiência da proteção do computador. O indicador assume um dos seguintes valores:

	*Assinaturas liberadas: (data, hora)* O aplicativo e as assinaturas de ameaças usadas pelo Kaspersky Anti-Virus for Windows Servers são as versões mais recentes.
	*As assinaturas estão desatualizadas* Os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus for Windows Servers não foram atualizados por vários dias. Você está correndo o risco de infectar o computador com novos programas mal-intencionados que apareceram desde a última atualização do programa. É recomendável atualizar o Kaspersky Anti-Virus for Windows Servers. Para fazê-lo, use o link Atualização.
	As assinaturas estão parcialmente corrompidas Os arquivos de assinaturas de ameaças estão parcialmente corrompidos. Se isso ocorrer, é recomendável executar as atualizações do programa novamente. Se a mesma mensagem de erro aparecer novamente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab.
	Reinicie o computador Reinicie o sistema para que o programa seja executado corretamente. Salve e feche todos os arquivos com os quais está trabalhando e use o link Reiniciar computador.
	As atualizações do programa estão desabilitadas O serviço de atualização das assinaturas de ameaças e de módulos do programa está desabilitado. Para manter a proteção em tempo real, é recomendável habilitar as atualizações.

	*As assinaturas estão obsoletas* O Kaspersky Anti-Virus for Windows Servers não é atualizado há algum tempo. Os dados correm um grande risco. Atualize o programa assim que possível. Para fazê-lo, use o link Atualização.
	As assinaturas estão corrompidas Os arquivos de assinaturas de ameaças estão totalmente danificados. Se isso ocorrer, é recomendável executar as atualizações do programa novamente. Se a mesma mensagem de erro aparecer novamente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

O terceiro indicador mostra a funcionalidade atual do programa. O indicador assume um dos seguintes valores:

	*Todos os componentes de proteção estão em execução* O Kaspersky Anti-Virus for Windows Servers está protegendo o computador em todos os canais pelos quais programas mal-intencionados poderiam entrar.
	A proteção não está instalada Quando o Kaspersky Anti-Virus for Windows Servers foi instalado, nenhum dos componentes de monitoramento foi instalado. Isso significa que você pode apenas verificar vírus. Para obter segurança máxima, instale os componentes de proteção no computador.
	*Todos os componentes de proteção estão pausados* O componente de proteção foi pausado. Para restaurá-lo, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.
	Todos os componentes de proteção estão desabilitados A proteção está totalmente desabilitada. O componente de proteção não está em execução. Para restaurá-lo, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.
	*Alguns componentes de proteção tiveram mau funcionamento* O componente do Kaspersky Anti-Virus encontrou erros internos. Se isso ocorrer, é recomendável habilitar o componente ou reiniciar o computador, pois é possível que os drivers dos componentes precisem ser registrados depois de serem atualizados.

5.1.2. Status dos componentes do Kaspersky Anti-Virus for Windows Servers

Para determinar como o Kaspersky Anti-Virus for Windows Servers protege o sistema de arquivos ou para exibir o andamento de uma tarefa de verificação de vírus ou atualização de assinaturas de ameaças, abra a seção correspondente da janela principal do programa.

Por exemplo, para exibir o status atual do Antivírus de Arquivos, selecione **Antivírus de Arquivos** à esquerda da janela principal. O painel direito exibirá um resumo das informações sobre o funcionamento do componente.

Para o Antivírus de Arquivos, o painel direito contém a **barra de status**, a caixa **Status** e a caixa **Estatísticas**.

Para o Antivírus de Arquivos, a *barra de status* aparece da seguinte maneira:

- *Antivírus de Arquivos: em execução* – a proteção de arquivos está ativa para o nível selecionado (consulte 7.1 na p. 72).
- *Antivírus de Arquivos: em pausa* - o Antivírus de Arquivos está desabilitado por um determinado período. O componente continuará seu funcionamento automaticamente depois que o período atribuído expirar ou depois que o programa for reiniciado. Você também pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.
- *Antivírus de Arquivos: interrompido* – o componente foi interrompido pelo usuário. Você pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.
- *Antivírus de Arquivos: não executando* – por algum motivo, a proteção de arquivos não está disponível.
- *Antivírus de Arquivos: desabilitado (erro)* – o componente encontrou um erro.

  Se um componente encontrar um erro, tente reiniciá-lo. Se houver o erro ao reiniciar, examine o relatório do componente, que deve conter o motivo da falha. Se não conseguir solucionar o problema, salve o relatório do componente em um arquivo usando **Ação → Salvar Como** e entre em contato com o Suporte Técnico da Kaspersky Lab.

As configurações usadas na operação do componente são fornecidas na seção **Status**:

- *Antivírus de Arquivos* – o status atual do componente (em execução, não executando, em pausa, etc.).
- *Nível de segurança* – o conjunto total de parâmetros de funcionamento do componente, de acordo com os quais o programa protege os arquivos. Por padrão, o nível de segurança **Recomendado** será selecionado, verificando apenas objetos no sistema de arquivos sujeito a infecções. Por exemplo, arquivos executáveis (.exe).
- A *ação* executada quando um objeto mal-intencionado é detectado.

Não há uma caixa **Status** para tarefas de verificação de vírus e atualização. A caixa **Configurações** relaciona o nível de segurança e a ação aplicada a programas perigosos nas tarefas de verificação de vírus e o modo de execução nas atualizações.

A caixa **Estatísticas** contém informações sobre o funcionamento dos componentes de proteção, atualizações ou tarefas de verificação de vírus.

5.1.3. Estatísticas de desempenho do programa

As **estatísticas do programa** podem ser encontradas na caixa **Estatísticas** da seção **Proteção** (veja a Figura 5) na janela principal do programa, e exibem informações gerais sobre a proteção do computador, registradas a partir da instalação do Kaspersky Anti-Virus for Windows Servers.

Figura 5. A caixa de estatísticas gerais do programa

Você pode clicar em qualquer lugar na caixa para exibir um relatório com informações detalhadas. As guias exibem:

- Informações sobre objetos encontrados (consulte 11.3.2 na página 129) e o status atribuído a eles
- Log de eventos (consulte 11.3.3 na página 129)
- Estatísticas gerais de verificação (consulte 11.3.4 na página 131) do computador

- Configurações de operação do programa (consulte 11.3.5 na página 131)

5.2. Como verificar seu servidor quanto à presença de vírus

Após a instalação, o programa certamente o informará por meio de uma mensagem no canto inferior esquerdo da janela do programa que o servidor ainda não foi verificado e recomendará que você o faça imediatamente.

O Kaspersky Anti-Virus inclui uma tarefa padrão predefinida para a verificação de vírus no computador. Ela fica na janela principal do programa, na seção **Verificação**.

Depois de selecionar a tarefa **Meu Computador**, você poderá exibir as estatísticas das configurações das tarefas e da verificação mais recentes do computador: o nível de proteção selecionado e as ações que serão executadas com relação aos objetos perigosos.

Para verificar programas mal-intencionados no computador,

1. Abra a janela principal do programa e selecione a tarefa **Meu Computador** na **seção** Verificação.
2. Clique no botão **Verificação**.

Como resultado, o programa começará a verificar o servidor e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela com informações sobre o andamento da instalação ficará oculta, mas a verificação não será interrompida.

5.3. Como verificar áreas críticas do computador

É extremamente importante proteger essas áreas críticas para assegurar que o computador continue funcionando. Existe uma tarefa de verificação de vírus específica para essas áreas, localizada na janela principal do programa, na seção **Verificação**.

Depois de selecionar a tarefa **Áreas críticas**, você poderá ver as estatísticas da verificação mais recente do computador e as configurações da tarefa: as estatísticas da verificação mais recente dessas áreas; as configurações da tarefa; o nível de proteção selecionado e as ações que serão aplicadas às

ameaças de segurança. Aqui, você também pode selecionar as áreas críticas que deseja verificar e iniciar imediatamente a verificação nessas áreas.

Para verificar programas mal-intencionados nas áreas críticas do computador,

1. Abra a janela principal do programa e selecione a tarefa **Áreas críticas** na seção **Verificação**.
2. Clique no botão **Verificação**.

Ao fazê-lo, será iniciada uma verificação das áreas selecionadas e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela com informações sobre o andamento da instalação ficará oculta, mas a verificação não será interrompida.

5.4. Como verificar vírus em um arquivo, uma pasta ou um disco

Às vezes, é necessário verificar vírus em objetos individuais e não em todo o computador: por exemplo, em um dos discos rígidos. Você pode selecionar um objeto para ser verificado com as ferramentas padrão do sistema operacional Microsoft Windows Server (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**, etc.).

Para verificar um objeto,

Coloque o cursor sobre o nome do objeto selecionado, abra o menu de contexto do Microsoft Windows Server clicando com o botão direito do mouse e selecione **Verificar vírus** (veja a Figura 6).

Será iniciada então uma verificação do objeto selecionado e os detalhes serão mostrados em uma janela específica. Ao clicar no botão Fechar, a janela com informações sobre o andamento da instalação ficará oculta, mas a verificação não será interrompida.

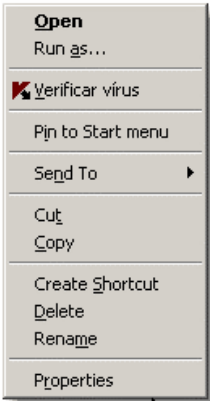


Figura 6. Verificando um objeto selecionado usando
um menu de contexto padrão do Microsoft Windows Server

5.5. Como atualizar o programa

A Kaspersky Lab atualiza as assinaturas de ameaças e módulos do Kaspersky Anti-Virus for Windows Servers usando servidores de atualização dedicados.

Os *servidores de atualização da Kaspersky Lab* são os sites da Kaspersky Lab na Internet, onde são armazenadas as atualizações do programa.

Aviso!

Será necessária uma conexão com a Internet para atualizar o Kaspersky Anti-Virus for Windows Servers.

Por padrão, o Kaspersky Anti-Virus for Windows Servers verifica automaticamente as atualizações nos servidores da Kaspersky Lab. Se o servidor tiver as atualizações mais recentes, o Kaspersky Anti-Virus as baixará e instalará no modo silencioso.

Para atualizar o Kaspersky Anti-Virus for Windows Servers manualmente,

selecione o componente **Atualização** na seção **Serviço** da janela principal do programa e clique no botão **Atualizar agora!** à direita da janela.

Como resultado, o Kaspersky Anti-Virus for Windows Servers começará o processo de atualização e exibirá os detalhes em uma janela específica.

5.6. O que fazer se a proteção não for executada

Se houver problemas ou erros no funcionamento do Antivírus de Arquivos, verifique seu status. Se o status do componente for *não executando* ou *erro de funcionamento*, tente reiniciar o programa.

Se o problema não for resolvido após reiniciar o programa, é recomendável corrigir os possíveis erros usando o recurso de restauração do aplicativo (**Iniciar → Programas → Kaspersky Anti-Virus 6.0 for Windows Servers → Modificar, restaurar ou remover**).

Se o procedimento de restauração do aplicativo não ajudar, entre em contato com o Suporte Técnico da Kaspersky Lab. Pode ser necessário salvar um relatório sobre a operação do componente ou de todo o aplicativo em um arquivo e enviá-lo para o Suporte Técnico para investigação.

Para salvar o relatório em um arquivo:

1. Selecione Antivírus de Arquivos na seção **Proteção** da janela principal do programa e clique em qualquer lugar na caixa **Estatísticas**.
2. Clique no botão **Salvar como** e, na janela que é aberta, especifique o nome do arquivo para o relatório de desempenho do componente.

Para salvar um relatório da inicialização ou do status de todos os componentes do Kaspersky Anti-Virus de uma vez (Antivírus de Arquivos, tarefas de verificação de vírus, recursos de suporte),

1. Selecione a seção **Proteção** na janela principal do programa e clique em qualquer local da caixa **Estatísticas**.

   ou

   Clique em Todos os relatórios na janela de relatório de qualquer componente. Em seguida, a guia **Relatórios** relacionará os relatórios de todos os componentes do programa.
2. Clique no botão **Salvar como** e, na janela que é aberta, especifique o nome do arquivo do relatório de operação do programa.

CAPÍTULO 6. SISTEMA DE GERENCIAMENTO DA PROTEÇÃO

O Kaspersky Anti-Virus for Windows Servers permite que você execute várias tarefas de gerenciamento da segurança dos computadores:

- Habilitar, desabilitar e pausar (consulte 6.1 na p. 53) o programa
- Definir os tipos de programas perigosos (consulte 6.2 na p.a 58) dos quais o Kaspersky Anti-Virus for Windows Servers protegerá seu computador
- Criar uma lista de exclusões (consulte 6.3 na p. 59) para a proteção
- Criar suas próprias tarefas de atualização e verificação de vírus (consulte 6.4 na p. 65)
- Configurar uma programação de verificação de vírus (consulte 6.5 na p. 66)
- Configurar a produtividade (consulte a seção 6.6 na p. 68) de proteção do computador

6.1. Interrompendo e reiniciando a proteção do computador

Por padrão, o Kaspersky Anti-Virus é aberto na inicialização e protege o computador durante todo o tempo em que você o utiliza. As palavras *Kaspersky Anti-Virus 6.0* no canto superior direito da tela indicam que a proteção está ativa. O Antivírus de Arquivos (consulte 2.2.1 na p. 17) está em execução.

Você pode desabilitar a proteção do Kaspersky Anti-Virus for Windows Servers.

Aviso!

A Kaspersky Lab recomenda enfaticamente que você **não desabilite a proteção**, pois isso poderia levar a uma infecção no computador e à conseqüente perda de dados.

Observe que, nesse caso, a proteção é discutida no contexto do Antivírus de Arquivos. Desabilitá-lo ou pausá-lo não afeta o desempenho das tarefas de verificação de vírus e atualizações do programa.

6.1.1. Pausando a proteção

Pausar a proteção significa desabilitar o Antivírus de Arquivos temporariamente.

Para pausar uma operação do Kaspersky Anti-Virus for Windows Servers:

1. Selecione **Pausar proteção** no menu de contexto do programa (consulte a seção 4.2 na p. 38).
2. Na janela **Pausar proteção** que é aberta (veja a Figura 7), selecione em quanto tempo deseja que a proteção volte a funcionar:
   - **Em <intervalo de tempo>** – a proteção será habilitada após este período. Para selecionar um período, use o menu suspenso.
   - **Na próxima reinicialização do programa** – a proteção será reiniciada se você abrir o programa no Menu Iniciar ou após reiniciar o computador (desde que o programa esteja definido para iniciar ao ligar o computador; consulte 6.1.5 na página 57).
   - **Somente por solicitação do usuário** – a proteção será interrompida até que você mesmo a inicie. Para habilitar a proteção, selecione **Continuar proteção** no menu de contexto do programa.

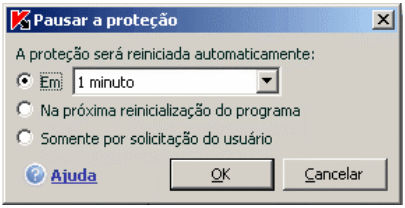


Figura 7. Janela Pausar proteção

Dica:

Você também pode interromper a proteção do computador por meio de um dos seguintes métodos:

- Clique no botão na seção Proteção.
- Selecione Sair no menu de contexto. Nesse caso, o programa será descarregado da memória do computador.

Se você pausar a proteção, o Antivírus de Arquivos será pausado. Isso é indicado por:

- Nome inativo (cinza) do Antivírus de Arquivos na seção **Proteção** da janela principal.
- Ícone inativo (cinza) na bandeja do sistema.
- O terceiro indicador de proteção (consulte 5.1.1 na p. 43) no computador, que mostra que **Todos os componentes de proteção estão pausados**.

6.1.2. Interrompendo a proteção do servidor

Interromper a proteção significa desabilitar totalmente o Antivírus de Arquivos. As verificações de vírus e atualizações continuam funcionando neste modo.

Se a proteção for interrompida, ela só poderá ser reiniciada pelo administrador: o Antivírus de Arquivos não continuará automaticamente depois da reinicialização do sistema ou do programa. Lembre-se que se, de alguma forma, o Kaspersky Anti-Virus for Windows Servers estiver em conflito com outros programas instalados no computador, você poderá pausar o Antivírus de Arquivos ou criar uma lista de exclusões (consulte 6.3 na p. 59).

Para interromper toda a proteção:

1. Abra a janela de configurações do Kaspersky Anti-Virus e selecione a seção **Proteção**.
2. Desmarque **Habilitar proteção**.

Depois de desabilitar a proteção, o Antivírus de Arquivos será interrompido. Isso é indicado por:

1. Nome inativo (cinza) do Antivírus de Arquivos na seção **Proteção** da janela principal.

2. Ícone inativo (cinza) na bandeja do sistema.
3. O terceiro indicador de proteção (consulte 5.1.1 na p. 43) no computador, que mostra que  **Todos os componentes de proteção estão desabilitados**.

6.1.3. Pausando / interrompendo a proteção

Existem várias formas de interromper o Antivírus de Arquivos, uma verificação de vírus ou uma atualização. Antes de fazê-lo, é estritamente recomendável estabelecer o motivo da interrupção. É provável que o problema possa ser resolvido de outra maneira, por exemplo, alterando o nível de segurança. Se, por exemplo, você estiver trabalhando com um banco de dados que certamente não contém vírus, simplesmente adicione seus arquivos como uma exclusão (consulte a seção 6.3 na p. 59).

Para pausar o Antivírus de Arquivos, verificações de vírus e tarefas de atualização:

Selecione o componente ou a tarefa à esquerda da janela principal e clique no botão  na barra de status.

O status do componente/tarefa mudará para ***em pausa***. O componente ou a tarefa ficará em pausa até que você o reinicie, clicando no botão  .

Ao pausar o componente ou a tarefa, as estatísticas da sessão atual do Kaspersky Anti-Virus são salvas e continuarão sendo registradas após a atualização do componente.

Para interromper tarefas ou o componente de proteção:

Clique no botão  na barra de status. Você também pode interromper o componente na janela de configurações do programa, desmarcando a caixa de seleção **Habilitar <nome do componente>** na seção **Geral**.

O status do componente/tarefa mudará para *interrompido (desabilitado)*. O componente ou a tarefa será interrompido até que você o habilite, clicando no botão  . Para tarefas de atualização e verificação de vírus, você poderá escolher dentre as seguintes opções: continuar a tarefa que foi interrompida ou reiniciá-la do início.

Ao interromper o componente ou a tarefa, todas as estatísticas do trabalho anterior serão limpas e, quando o componente for iniciado, serão substituídas.

6.1.4. Restaurando a proteção no computador

Se, em algum momento, você pausou ou interrompeu a proteção no computador, será possível reiniciá-la usando um dos seguintes métodos:

- *No menu de contexto*.

  Para fazê-lo, selecione **Reiniciar proteção**.

- *Na janela principal do programa*.

  Para fazê-lo, clique no botão ▶ na barra de status, na seção **Proteção** da janela principal.

O status de proteção muda imediatamente para *em execução*. O ícone do programa na bandeja do sistema fica ativo (colorido). O terceiro indicador de proteção (consulte 5.1.1 na p. 43) também informará que **Todos os componentes de proteção estão habilitados**.

6.1.5. Desligando o programa

Se for necessário desligar o Kaspersky Anti-Virus for Windows Servers, selecione **Sair** no menu de contexto do programa (consulte 4.2 na p. 38). Isso fechará o programa, deixando seu computador desprotegido.

Após fechar o programa, você pode habilitar a proteção do computador novamente abrindo o Kaspersky Anti-Virus for Windows Servers (**Iniciar → Programas → Kaspersky Anti-Virus 6.0 for Windows Servers → Kaspersky Anti-Virus 6.0 for Windows Servers**).

Também será possível reiniciar a proteção automaticamente depois de reiniciar o sistema operacional. Para habilitar este recurso, selecione a seção **Proteção** na janela de configurações do programa e marque ☑ **Iniciar o Kaspersky Anti-Virus na inicialização**.

6.2. Tipos de programas mal-intencionados que serão monitorados

O Kaspersky Anti-Virus for Windows Servers o protege de vários tipos de programas mal-intencionados. Independentemente das suas configurações, o Kaspersky Anti-Virus sempre protege o computador dos tipos mais perigosos de programas mal-intencionados, como vírus, cavalos de Tróia e ferramentas de hackers. Esses programas podem causar danos significativos ao computador. Para tornar o computador mais seguro, você pode expandir a lista de ameaças que o programa detectará, fazendo-o monitorar outros tipos de programas perigosos.

Para escolher os programas mal-intencionado dos quais o Kaspersky Anti-Virus for Windows Servers o protegerá, selecione a seção **Proteção** na janela de configurações do programa (consulte 4.4 na p. 41).

A caixa **Categorias de malware** contém os tipos de ameaças (consulte 1.1 na p. 9):

- **Vírus, worms, cavalos de Tróia, ferramentas de hackers**. Esse grupo combina as categorias mais comuns e perigosas de programas mal-intencionados. Este é o nível de segurança mínimo admissível. Por recomendação dos especialistas da Kaspersky Lab, o Kaspersky Anti-Virus sempre monitora esta categoria de programas mal-intencionados.
- **Spyware, adware, discadores**. Esse grupo inclui softwares possivelmente perigosos que poderiam causar inconveniências ao usuário ou resultar em danos significativos.
- **Software possivelmente perigoso (riskware)**. Este grupo inclui programas que não são mal-intencionados ou perigosos. Contudo, em determinadas situações, eles poderiam ser usados para danificar o seu computador.

Os grupos listados acima compreendem toda a variedade de ameaças que o programa detecta ao verificar objetos.

Se todos os grupos forem selecionados, o Kaspersky Anti-Virus for Windows Servers fornecerá a proteção antivírus mais completa possível para o computador. Se o segundo e o terceiro grupos estiverem desabilitados, o programa o protegerá apenas dos programas mal-intencionados mais comuns. Isso não inclui programas possivelmente perigosos e outros que poderiam estar instalados no seu computador e que poderiam danificar seus arquivos, roubar seu dinheiro ou ocupar seu tempo.

A Kaspersky Lab não recomenda desabilitar o monitoramento do segundo grupo. Se o Kaspersky Anti-Virus classificar um programa que você não considera perigoso como um programa possivelmente perigoso, é recomendável criar uma exclusão para ele (consulte 6.3 na p. 59).

6.3. Criando uma zona confiável

Uma *zona confiável* consiste em uma lista de objetos, criada pelo administrador, que não serão monitorados pelo Kaspersky Anti-Virus for Windows Servers. Em outras palavras, é um conjunto de programas excluídos da proteção.

O administrador cria uma zona de proteção com base nas propriedades dos arquivos que usa e nos programas instalados no seu computador. Poderá ser necessário criar uma lista de exclusões se, por exemplo, o Kaspersky Anti-Virus for Windows Servers bloquear o acesso a um objeto ou programa e você tiver certeza de que ele é absolutamente seguro.

Você pode excluir da verificação arquivos de determinados formatos, usar uma máscara de arquivos ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objetos, de acordo com a classificação da Enciclopédia de Vírus (o status que o programa atribui aos objetos durante uma verificação).

Aviso!

Os objetos excluídos não são verificados quando o disco ou a pasta em que se localizam é verificado. Contudo, se você selecionar esse objeto especificamente, a regra de exclusão não será aplicada.

Para criar uma lista de exclusões,

1. Abra a janela de configurações do aplicativo e selecione a seção **Proteção**.
2. Clique no botão **Zona confiável** na seção **Geral**.

Configure as regras de exclusão para objetos e crie uma lista de aplicativos confiáveis na janela que é aberta (veja a Figura 8).

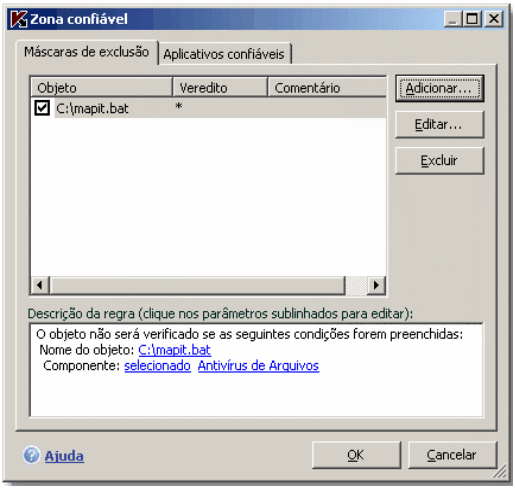


Figura 8. Criando uma zona confiável

6.3.1. Regras de exclusão

As *regras de exclusão* são conjuntos de condições que o Kaspersky Anti-Virus for Windows Servers usa para determinar que não deve verificar um objeto.

Você pode excluir da verificação arquivos com determinados formatos, usar uma máscara de arquivos ou excluir uma determinada área, como uma pasta ou um programa, processos de programas ou objetos, de acordo com sua classificação na Enciclopédia de Vírus.

O *veredito* é o status que o Kaspersky Anti-Virus atribui a um objeto durante a verificação. Um status é atribuído com base na classificação de programas mal-intencionados e possivelmente perigosos encontrados na Enciclopédia de Vírus da Kaspersky Lab.

O software possivelmente perigoso não tem função mal-intencionada, mas pode ser usado como componente auxiliar de um código mal-intencionado, pois contém falhas e erros. Essa categoria inclui, por exemplo, programas de administração remota, clientes IRC, servidores FTP, utilitários multifuncionais para interromper ou ocultar processos, registradores de uso do teclado, macros de senha, discadores automáticos etc. Esses programas não são classificados como vírus. Eles podem ser divididos em vários tipos, por exemplo, Adware, Piadas, Riskware, etc. (para obter mais informações sobre programas possivelmente perigosos detectados pelo Kaspersky Anti-Virus for Windows Servers, consulte a Enciclopédia de Vírus em www.viruslist.com). Depois da verificação, esses programas podem ser bloqueados. Como vários deles são

muito comuns, você tem a opção de excluí-los da verificação. Para fazê-lo, adicione o nome ou a máscara de ameaças do objeto à zona confiável usando a classificação da Enciclopédia de Vírus.

Por exemplo, imagine que você usa um programa de Administração Remota freqüentemente no seu trabalho. Trata-se de um sistema de acesso remoto com o qual você pode trabalhar de um computador remoto. O Kaspersky Anti-Virus for Windows Servers considera este tipo de atividade de aplicativo como possivelmente perigoso e pode bloqueá-lo. Para impedir que o aplicativo seja bloqueado, crie uma regra de exclusão que especifica not-a-virus:RemoteAdmin.Win32.RAdmin.22 como veredito.

Ao adicionar uma exclusão, será criada uma regra que o Antivírus de Arquivos e as tarefas de verificação de vírus podem usar posteriormente. É possível criar regras de exclusão em uma janela específica que pode ser aberta da janela de configurações do programa, do aviso sobre a detecção do objeto e da janela de relatório.

*Para adicionar exclusões na guia **Máscara de exclusão**:*

1. Clique no botão **Adicionar** na guia **Máscara de exclusão**.
2. Na janela que é aberta (veja a Figura 9), clique no tipo de exclusão na seção **Propriedades**:

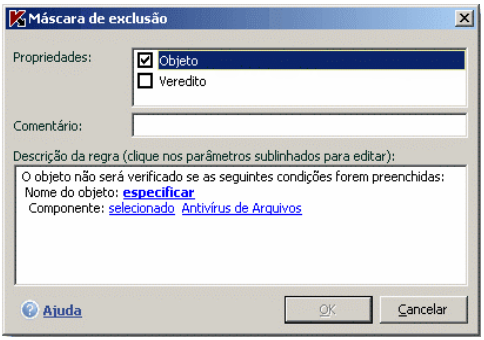


Figura 9. Criando uma regra de exclusão

- **Objeto** – exclusão das verificações de um determinado objeto, diretório ou arquivos que correspondem a uma determinada máscara.
- **Veredito** – exclusão de um objeto das verificações com base em seu status na classificação da Enciclopédia de Vírus.

Se você marcar as duas caixas ao mesmo tempo, será criada uma regra para aquele objeto com um determinado status conforme a classificação da Enciclopédia de Vírus. Nesse caso, as seguintes regras se aplicam:

- Se você especificar um determinado arquivo como **Objeto** e um determinado status na seção **Veredito**, o arquivo especificado será uma exclusão somente se for classificado como sendo a ameaça selecionada durante a verificação.
- Se você selecionar uma área ou pasta como **Objeto** e o status (ou máscara) como **Veredito**, os objetos com esse status serão excluídos da verificação somente nessa área ou pasta.

3. Atribua valores **aos** tipos de exclusão selecionados. Para fazê-lo, clique na seção **Descrição da regra** no link de especificação localizado ao lado do tipo de exclusão:
   - Para o tipo **Objeto**, insira seu nome na janela que é aberta (pode ser um arquivo, uma pasta específica ou uma máscara de arquivos (consulte a seção A.2 na p. 190). Marque ☑ **Incluir subpastas** para que o objeto (arquivo, máscara de arquivos, pasta) seja excluído recursivamente da verificação.
   - Insira o nome completo da ameaça que deseja excluir das verificações, como mostrado na Enciclopédia de Vírus, ou use a máscara para o **Veredito** (consulte A.3 na p. 190).

     Para alguns objetos de classificação, você pode atribuir condições avançadas para a aplicação de regras no campo **Configurações avançadas**.
4. Defina quais componentes do Kaspersky Anti-Virus for Windows Servers usarão esta regra. Se a opção selecionada for qualquer, a regra se aplicará a todos os componentes. Se desejar restringir a regra a um ou a vários componentes, clique em qualquer, que mudará para selecionado. Na janela que é aberta, marque as caixas dos componentes aos quais deseja que essa regra de exclusão se aplique.

Para criar uma regra de exclusão a partir de um aviso do programa informando que foi detectado um objeto perigoso:

1. Use o link Adicionar à zona confiável na janela da notificação.
2. Na janela que é aberta, verifique se todas as configurações das regras de exclusão correspondem às suas necessidades. O programa preencherá o nome do objeto e o tipo de ameaça automaticamente, com base nas informações contidas na notificação. Para criar a regra, clique em **OK**.

Para criar uma regra de exclusão na janela de relatório:

1. Selecione o objeto no relatório que você deseja adicionar às exclusões.

2. Abra o menu de contexto e selecione **Adicionar à zona confiável** (veja a Figura 10).

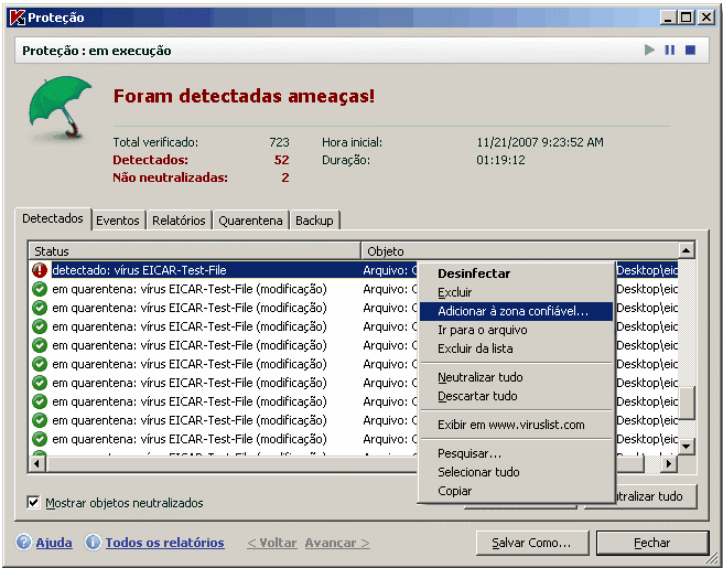


Figura 10. Criando uma regra de exclusão a partir do relatório

6.3.2. Aplicativos confiáveis

O Kaspersky Anti-Virus for Windows Servers pode criar uma lista de aplicativos confiáveis, que não precisam ter a atividade de seus arquivos monitorados, considerados suspeitos, etc.

Por exemplo, você acha que os objetos e processos usados pelo **Bloco de Notas** do Windows Server são seguros e não precisam ser verificados. Para excluir os objetos usados por esse processo da verificação, adicione o **Bloco de Notas** à lista de aplicativos confiáveis. Contudo, o arquivo executável e o processo do aplicativo confiável serão verificados quanto à presença de vírus, como anteriormente. Para excluir totalmente o aplicativo da verificação, use regras de exclusão (consulte 6.3.1 na p. 60).

Além disso, algumas ações classificadas como perigosas são perfeitamente normais para vários programas. Por exemplo, programas de alternância de layout do teclado interceptam normalmente o texto digitado no teclado. Para acomodar esses programas e interromper o monitoramento de sua atividade, é recomendável adicioná-los à lista de aplicativos confiáveis.

A exclusão de aplicativos confiáveis também resolve possíveis conflitos de compatibilidade entre o Kaspersky Anti-Virus for Windows Servers e outros aplicativos (por exemplo, o tráfego de rede de outro computador que já foi verificado pelo aplicativo antivírus) e pode aumentar a produtividade do computador.

Por padrão, o Kaspersky Anti-Virus for Windows Servers verifica os objetos abertos, executados ou salvos por qualquer processo do programa.

Você pode criar uma lista de aplicativos confiáveis na guia específica **Aplicativos confiáveis** (veja a Figura 11). Por padrão, essa lista contém os aplicativos que não serão monitorados com base nas recomendações da Kaspersky Lab ao instalar o Kaspersky Anti-Virus. Se você não confiar em um aplicativo da lista, desmarque a caixa de seleção correspondente. É possível editar a lista usando os botões **Adicionar**, **Editar** e **Excluir** à direita.

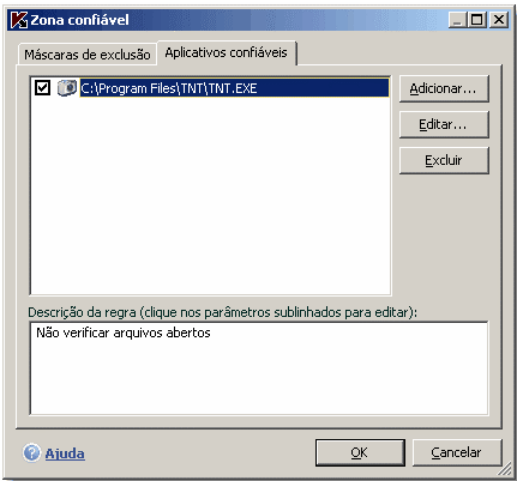


Figura 11. Lista de aplicativos confiáveis

Para adicionar um programa à lista de aplicativos confiáveis:

1. Clique no botão **Adicionar** à direita da guia **Aplicativos confiáveis**.
2. Na janela **Aplicativo confiável** (veja a Figura 12) que é aberta, selecione o aplicativo usando o botão **Procurar**. Um menu de contexto será aberto e, ao clicar em **Procurar**, você poderá ir para a janela de seleção de arquivos e selecionar o caminho do arquivo executável ou, ao clicar em **Aplicativos**, poderá ir para uma lista de aplicativos em execução no momento e selecioná-los conforme necessário.

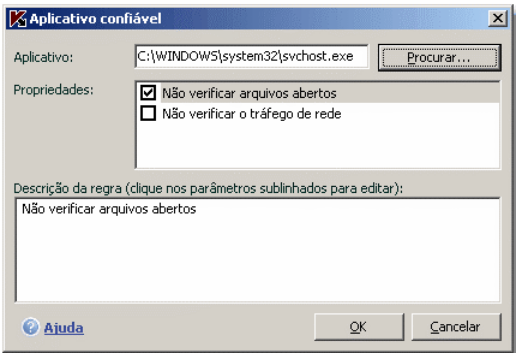


Figura 12. Adicionando um aplicativo à lista de aplicativos confiáveis

Ao selecionar um programa, o Kaspersky Anti-Virus for Windows Servers registra os atributos internos do arquivo executável e os usa para identificar o programa confiável durante as verificações.

O caminho do arquivo é inserido automaticamente quando você seleciona seu nome.

3. Em seguida, se necessário, especifique as ações executadas por esse processo que não serão monitoradas pelo Kaspersky Anti-Virus:

   Não verificar arquivos abertos – exclui da verificação todos os arquivos processados pelo aplicativo confiável.

6.4. Iniciando tarefas em outro perfil

O Kaspersky Anti-Virus for Windows Servers 6.0 possui um recurso que permite iniciar tarefas de verificação com outro perfil de usuário. Por padrão, esse recurso está desabilitado e as tarefas são executadas no perfil com o qual você se conectou ao sistema.

Este recurso é útil se, por exemplo, você precisa de direitos de acesso a um determinado objeto durante uma verificação. Ao usá-lo, você pode configurar tarefas para serem executadas no perfil de um outro usuário que possui os privilégios necessários.

As atualizações do produto podem ser feitas de uma fonte à qual você não tem acesso (por exemplo, a pasta de atualização da rede) ou direitos de usuário autorizado para um servidor proxy. Você pode usar esse recurso para executar a Atualização em outro perfil que possua esses direitos.

Para configurar uma tarefa de verificação que é iniciada em outro perfil de usuário:

1. Selecione o nome da tarefa na seção **Verificação** (para verificações de vírus) ou na seção **Serviço** (para tarefas de atualização) da janela principal e use o link Configurações para abrir a janela de configurações da tarefa.
2. Clique no botão **Configurações** na janela de configurações da tarefa e vá para a guia **Adicional** na janela que é aberta (veja a Figura 13).
3. Para habilitar este recurso, marque ☑ **Executar esta tarefa como**. Insira os dados de logon com os quais deseja iniciar a tarefa, como: nome de usuário e senha.

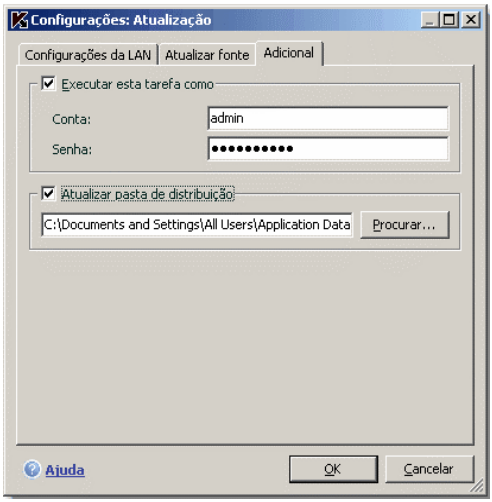


Figura 13. Configurando uma tarefa de atualização em outro perfil

6.5. Configurando notificações e tarefas programadas

As configurações de programação são idênticas para tarefas de verificação de vírus, atualizações do aplicativo e notificações de eventos do Kaspersky Anti-Virus.

Por padrão, as tarefas de verificação de vírus criadas na instalação do aplicativo estão desabilitadas. A exceção são os objetos de inicialização, que são verificados sempre que Kaspersky Anti-Virus é iniciado. Por padrão, as atualizações são configuradas para serem executadas automaticamente conforme são disponibilizadas nos servidores de atualização da Kaspersky Lab.

Se desejar, você poderá reconfigurar a programação. Selecione uma tarefa pelo nome em **Verificação de vírus** (para tarefas de verificação de vírus) ou em **Serviço** (para atualizações e distribuição de atualizações) e abra a janela de configurações correspondente clicando em Configurações.

Para que as tarefas sejam iniciadas de acordo com uma programação, marque a caixa de início automático de tarefas na seção **Modo de execução**. Você pode editar o horário para iniciar a tarefa de verificação na janela **Programação** (veja a fig. Figura 14) que é aberta ao clicar em **Alterar**.

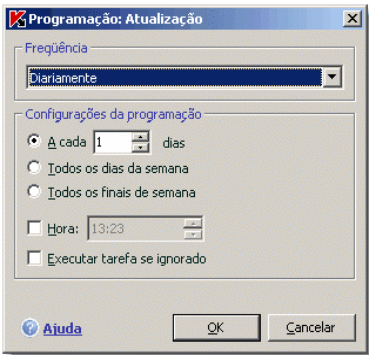


Figura 14. Configurando uma programação de tarefas

A principal configuração a ser definida é a freqüência de um evento (notificação ou execução da tarefa). Selecione a opção desejada em **Freqüência** (veja a Figura 14). Em seguida, especifique as configurações da opção selecionada em Configurações da atualização. As seguintes opções estão disponíveis:

- **Hora.** Inicia uma tarefa ou envia uma notificação na data e hora especificadas.
- **Ao iniciar o aplicativo.** Executa uma tarefa ou envia uma notificação sempre que o Kaspersky Anti-Virus é iniciado. Também pode ser especificado um atraso com relação ao início do aplicativo para que uma tarefa seja executada.
- **Após cada atualização.** A tarefa é executada após cada atualização das assinaturas de ameaças (esta opção se aplica somente a tarefas de verificação de vírus).
- **Minutos.** O intervalo entre as verificações ou notificações será de vários minutos. Especifique o período em minutos nas configurações da programação. Ele não deve exceder 59 minutos.
- **Horas.** O intervalo entre as verificações ou notificações será de várias horas. Se esta opção estiver selecionada, especifique o intervalo nas configurações da programação: **A cada n horas** e especifique *n*. Por

exemplo, insira **A cada 1 hora** se desejar que a tarefa seja executada a cada hora.

- **Dias.** A tarefa é iniciada ou a notificação é enviada com um intervalo de vários dias. Especifique o intervalo nas configurações da programação:

  - Selecione **A cada n dias** e especifique o valor de n, se desejar um intervalo de vários dias. Selecione **Todos os dias da semana**, se desejar que a tarefa seja executada diariamente, de segunda a sexta-feira.
  - **Todos os finais de semana** para executar a tarefa ou enviar a notificação somente aos sábados e domingos.

    No campo **Hora**, especifique o horário em que a tarefa de verificação será executada.

- **Semanas.** A tarefa é iniciada ou a notificação é enviada em determinados dias da semana. Se você selecionar esta opção, marque os dias da semana nos quais deseja que a tarefa seja executada. Insira a hora do dia no campo **Hora**.
- **Mensal.** A tarefa é iniciada ou a notificação é enviada uma vez por mês, na hora especificada.

Se, por algum motivo, a tarefa não puder ser executada (por exemplo, se o programa de e-mail não estiver instalado ou o computador estiver desligado), você poderá configurar a tarefa para ser executada automaticamente assim que possível.Marque ☑ **Executar tarefa se ignorado** na janela da programação.

6.6. Opções de energia

As verificações de vírus aumentam a carga nos subsistemas do processador central e do disco, fazendo os outros programas serem executados mais lentamente. Por padrão, se isso acontecer, o aplicativo pausará as verificações de vírus e liberará os recursos do sistema para os aplicativos do usuário.

Entretanto, há vários programas que podem ser iniciados assim que os recursos do processador forem liberados e executados em segundo plano. Se não desejar que as verificações de vírus dependam do funcionamento desses programas, desmarque ☑ **Conceder recursos a outros aplicativos** (veja a Figura 15).

Observe que esta configuração pode ser definida individualmente para cada tarefa de verificação de vírus. Se você escolher esta opção, a configuração de uma tarefa específica terá uma prioridade superior.

Na janela que é aberta ao clicar no botão **Configuração de várias CPUs**, você pode atribuir configurações para o Kaspersky Anti-Virus ser executado em um servidor com vários processadores (consulte 6.7 na p. 69).

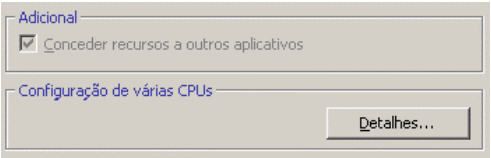


Figura 15. Configurando a energia

Para configurar a energia:

Selecione a seção **Proteção** da janela principal do programa e clique no link Configurações. Configure a energia na caixa **Adicional**.

6.7. Configuração do servidor com vários processadores

Nesta janela, você pode configurar a produtividade do servidor ao usar vários processadores.

Número de instâncias do kernel antivírus – número de cópias do kernel antivírus a serem carregadas quando o Kaspersky Anti-Virus é executado no servidor. Esse número determina os processos antivírus executados paralelamente.

Quanto mais cópias do mecanismo antivírus estiverem em execução, mais rápido as operações antivírus serão processadas. Contudo, isso afeta o desempenho geral do servidor.

Além disso, executar vários processos antivírus no servidor ao mesmo tempo assegura que o servidor está sempre protegido, caso haja erro em um dos mecanismos.

Para distribuir automaticamente os processos antivírus entre os processadores do servidor, marque ☑ **Usar driver específico para gerenciar processos paralelos**.

Se esta caixa de seleção estiver desmarcada, você poderá regular manualmente a carga no servidor, por exemplo, reservando parte dos processadores para o processamento antivírus e para as tarefas diretas do servidor. Para fazê-lo, desmarque os processadores dedicados ao servidor na caixa **Processadores utilizados**.

A Kaspersky Lab recomenda reservar pelo menos um processador para as tarefas do servidor, no caso de um servidor com vários processadores.

CAPÍTULO 7. PROTEÇÃO ANTIVÍRUS DO SISTEMA DE ARQUIVOS DO SERVIDOR

O Kaspersky Anti-Virus inclui o *Antivírus de Arquivos*, que protege os arquivos do computador contra infecções. Ele é carregado ao iniciar o sistema operacional, sendo executado na RAM do computador, e verifica todos os arquivos abertos, salvos ou executados.

A atividade do componente é indicada pelo ícone do Kaspersky Anti-Virus for Windows Servers na bandeja do sistema, que tem a seguinte aparência  sempre que um arquivo está sendo verificado.

Por padrão, o Antivírus de Arquivos verifica somente *arquivos novos ou modificados*, ou seja, apenas os arquivos que foram adicionados ou alterados desde a verificação anterior. Os arquivos são verificados usando o seguinte algoritmo:

1. O componente intercepta as tentativas de acessar qualquer arquivo feitas por usuários ou programas.
2. O Antivírus de Arquivos verifica as informações do arquivo interceptado nos bancos de dados do iChecker™ e do iSwift™. A decisão de verificar o arquivo ou não se baseia nas informações recuperadas.

O processo de verificação inclui as seguintes etapas:

1. O arquivo é analisado quando à presença de vírus. Os objetos mal-intencionados são detectados por comparação com as *assinaturas se ameaças*, que contêm descrições de todos os programas mal-intencionados e ameaças conhecidos até o momento e os métodos para neutralizá-los.
2. Depois da análise, existem três medidas a serem tomadas:
    a. Se for detectado um código mal-intencionado no arquivo, o Antivírus de Arquivos bloqueará o arquivo, colocará uma cópia do mesmo no *Backup* e tentará neutralizar o arquivo. Se o arquivo for desinfectado com êxito, ele ficará disponível novamente. Caso contrário, o arquivo será excluído.
    b. Se for detectado em um arquivo um código que parece ser mal-intencionado, mas sem garantias disso, o arquivo será enviado para a *Quarentena*.

c. Se nenhum código mal-intencionado for descoberto no arquivo, ele será restaurado imediatamente.

7.1. Selecionando um nível de segurança de arquivos

O Antivírus de Arquivos protege os arquivos que você está usando em um dos seguintes níveis (veja a Figura 16):

- **Alto** – o nível com o monitoramento mais abrangente dos arquivos abertos, salvos ou executados.
- **Recomendado** – a Kaspersky Lab recomenda este nível de configuração. As seguintes categorias de objetos serão verificadas:
  - Programas e arquivos por conteúdo
  - Objetos novos e modificados desde a última verificação
  - Objetos OLE incorporados
- **Baixo** – o nível com configurações que permitem usar tranqüilamente aplicativos que exigem recursos significativos do sistema, pois o escopo dos arquivos verificados é menor.

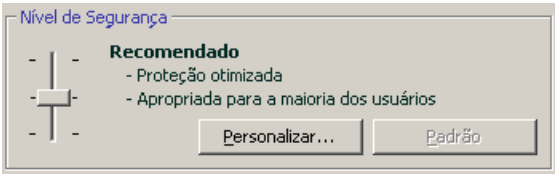


Figura 16. Nível de segurança do Antivírus de Arquivos

A configuração padrão do Antivírus de Arquivos é **Recomendado**.

Você pode aumentar ou diminuir o nível de proteção dos arquivos usados selecionando o nível desejado ou alterando as configurações do nível atual.

Para alterar o nível de segurança:

Ajuste os controles deslizantes. Ao ajustar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de arquivos verificados: quanto menos arquivos verificados quanto à presença de vírus, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de arquivos definidos atender às suas necessidades, você poderá personalizar as configurações de proteção. Para

fazê-lo, selecione o nível mais próximo do necessário como ponto inicial e edite suas configurações. Nesse caso, o nível será definido como **Personalizado**. Vamos examinar um exemplo de quando os níveis de segurança de arquivos definidos pelo usuário seriam úteis.

Exemplo:

> O trabalho que você executa no computador usa muitos tipos de arquivos, alguns dos quais podem ser bastante grandes. Você não deseja correr o risco de ignorar algum arquivo na verificação devido ao seu tamanho ou extensão, mesmo que isso afete de alguma forma a produtividade do computador.

Dica para selecionar um nível:

> Com base nos dados fornecidos, é possível concluir que você tem um risco bastante alto de ser infectado por um programa mal-intencionado. O tamanho e o tipo dos arquivos usados é bem variado e ignorá-los na verificação colocaria seus dados em risco. Você deseja verificar os arquivos que utiliza por conteúdo, não por extensão.
>
> É recomendável iniciar com o nível de segurança **Recomendado** e fazer as seguintes alterações: remova a restrição sobre os tamanhos dos arquivos verificados e otimize a operação do Antivírus de Arquivos verificando apenas arquivos novos e modificados. Assim, a verificação não ocupará tantos recursos do sistema e você poderá usar outros aplicativos tranqüilamente.

Para modificar as configurações de um nível de segurança:

> Clique no botão **Configurações** na janela de configurações do Antivírus de Arquivos. Edite as configurações do Antivírus de Arquivos na janela que é aberta e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Personalizado**, que contém as configurações de proteção definidas.

7.2. Configurando o Antivírus de Arquivos

Suas configurações determinam como o Antivírus de Arquivos defenderá o seu computador. Elas podem ser divididas nos seguintes grupos:

- Configurações que definem os tipos de arquivos (consulte a seção 7.2.1 na p. 74) que deverão ser verificados quanto à presença de vírus
- Configurações que definem o escopo da proteção (consulte a seção 7.2.2 na p. 77)

- Configurações que definem como o programa responderá a objetos perigosos (consulte a seção 7.2.5 na p. 81)
- Configurações adicionais do Antivírus de Arquivos (consulte 7.2.3 na p. 78)

As seções a seguir abordarão esses grupos detalhadamente.

7.2.1. Definindo os tipos de arquivos que serão verificados

Ao selecionar os tipos de arquivos que serão verificados, você estabelece quais os formatos e tamanhos de arquivo, e quais as unidades que, ao serem abertos, executados ou salvos, serão verificados quanto à presença de vírus.

Para facilitar a configuração, todos os arquivos estão divididos em dois grupos: *simples* e *compostos*. Os arquivos simples, por exemplo, arquivos .txt, não contêm nenhum objeto. Os objetos compostos podem incluir vários objetos, sendo que cada um deles também pode conter outros objetos. Existem vários exemplos: arquivos comprimidos, arquivos contendo macros, planilhas, e-mails com anexos, etc.

Os tipos de arquivos verificados são definidos na seção **Tipos de arquivos** (veja a Figura 17). Selecione uma das três opções:

- **Verificar todos os arquivos**. Com esta opção selecionada, todos os objetos do sistema de arquivos que forem abertos, executados ou salvos serão verificados, sem exceções.
- **Verificar programas e documentos (por conteúdo)**. Se você selecionar este grupo de arquivos, o Antivírus de Arquivos verificará apenas os arquivos possivelmente infectados; aqueles nos quais um vírus poderia ser incorporado.

  > Observação:
  >
  > Há vários formatos de arquivos que têm um risco bem menor de conter código mal-intencionado infiltrado e, conseqüentemente, de estar ativados. Um exemplo são os arquivos .txt.
  >
  > Por outro lado, há formatos de arquivos que contêm ou podem conter código executável. Exemplos incluem os formatos .exe, .dll ou .doc. O risco de infiltração e ativação de código mal-intencionado nesses arquivos é bastante alto.

  Antes de pesquisar vírus em um arquivo, seu cabeçalho interno é analisado com relação ao formato do arquivo (txt, doc, exe, etc.). Se a análise mostrar que o formato do arquivo não pode ser infectado, ele não será verificado

quanto à presença de vírus e retornará imediatamente ao usuário. Se o formato do arquivo puder ser infectado, ele será verificado quanto à presença de vírus.

- **Verificar programas e documentos (por extensão)**. Se você selecionar esta opção, o Antivírus de Arquivos verificará apenas os arquivos possivelmente infectados, mas o formato do arquivo será determinado pela extensão do nome do arquivo. Usando o link extensão, você pode analisar uma lista de extensões de arquivos (consulte a seção A.1 na p. 186) que são verificados com essa opção.

> Dica:
>
> Não esqueça que alguém pode enviar para o seu computador um vírus com uma extensão (por exemplo, .txt) que, na verdade, é um arquivo executável renomeado como .txt. Se você selecionar **Verificar programas e documentos (por extensão)**, a verificação ignoraria esse arquivo. Mas se a opção **Verificar programas e documentos (por conteúdo)** estiver selecionada, a extensão será ignorada, e a análise dos cabeçalhos do arquivo descobrirá que o arquivo é, na verdade, um arquivo .exe. O Antivírus de Arquivos verificaria o arquivo quanto à presença de vírus.

Na seção **Produtividade**, você pode especificar a verificação de vírus apenas nos arquivos novos e modificados desde a verificação anterior. Esse modo reduz sensivelmente o tempo de verificação e aumenta a velocidade de operação do programa. Para selecionar este modo, marque **Verificar somente arquivos novos e alterados**. Esse modo se aplica a arquivos simples e compostos.

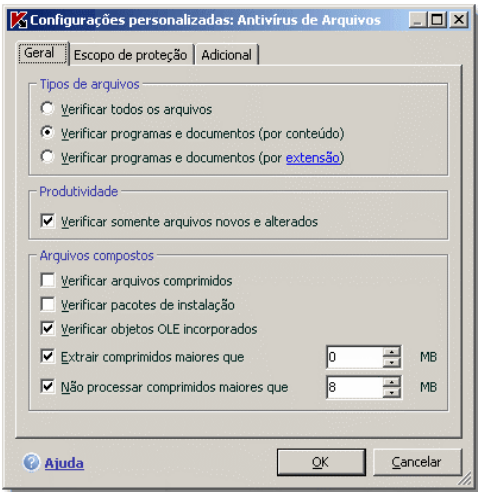


Figura 17. Selecionando os tipos de arquivos a serem verificados

Na seção **Arquivos compostos**, especifique os arquivos compostos que devem ser verificados quanto à presença de vírus:

- **Verificar todos/somente novos arquivos comprimidos** – verifica arquivos comprimidos .zip, .cab, .rar e .arj.
- **Verificar todos/somente novos pacotes de instalação** – verifica arquivos comprimidos de extração automática quanto à presença de vírus.
- **Verificar tudo/somente novos objetos OLE incorporados** – verifica objetos incorporados em arquivos (por exemplo, planilhas ou macros do Microsoft Office Excel incorporados em um arquivo do Microsoft Office Word, anexos de e-mail etc.).

Você pode selecionar e verificar todos os arquivos ou somente os novos, para cada tipo de arquivo composto. Para fazê-lo, clique no link ao lado do nome do objeto para alternar seu valor. Se a seção **Produtividade** tiver sido configurada para verificar somente arquivos novos e modificados, você não poderá selecionar o tipo de arquivos compostos que serão verificados.

Para especificar os arquivos compostos que não devem ser verificados quanto à presença de vírus, use as seguintes configurações:

- **Extrair comprimidos maiores que... MB**. Se o tamanho de um objeto composto exceder esta restrição, o programa o verificará como um único objeto (analisando o cabeçalho) e o disponibilizará novamente. Os objetos contidos nele serão verificados posteriormente. Se esta opção não estiver marcada, o acesso a arquivos maiores que o tamanho indicado será bloqueado até que tenham sido verificados.

☑ **Não processar comprimidos maiores que... MB**. Com esta opção marcada, arquivos maiores que o tamanho especificado serão ignorados na verificação.

7.2.2. Definindo o escopo da proteção

Por padrão, o Antivírus de Arquivos verifica todos os arquivos usados, independentemente de onde estão armazenados, seja em um disco rígido, um CD/DVD-ROM ou uma unidade flash.

Você pode limitar o escopo da proteção. Para fazê-lo:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Configurações** e selecione a guia **Escopo de proteção** (veja a Figura 18) na janela que é aberta.

A guia exibe uma lista de objetos que serão verificados pelo Antivírus de Arquivos. Por padrão, a proteção é habilitada para todos os objetos em discos rígidos, mídia removível e unidades de rede conectadas ao seu computador. É possível acrescentar itens e editar a lista usando os botões **Adicionar, Editar** e **Excluir**.

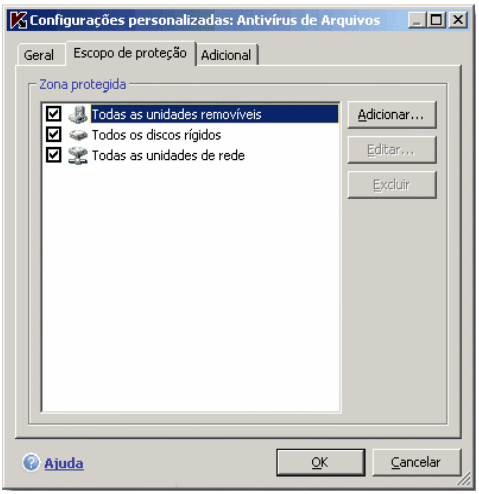


Figura 18. Criando uma zona de proteção

Se desejar proteger menos objetos, você pode fazê-lo usando os seguintes métodos:

- Especifique somente as pastas, unidades e arquivos que precisam ser protegidos.
- Crie uma lista de objetos que não precisam ser protegidos (consulte 6.3 na p. 59).
- Combine os dois métodos anteriores; crie um escopo de proteção que exclua vários objetos.

Você pode usar máscaras ao adicionar objetos para verificação. Observe que só é possível inserir máscaras com caminhos de objetos absolutos:

- **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
- **C:\dir*.exe** - todos os arquivos com a extensão .exe na pasta *C:\dir*
- **C:\dir*.ex?** - todos os arquivos com a extensão .ex? na pasta *C:\dir* , onde ? representa qualquer caractere
- **C:\dir\teste** - somente o arquivo *C:\dir\teste*

Para que a verificação seja executada recursivamente, marque ☑ **Incluir subpastas**.

Aviso!

Lembre-se de que o Antivírus de Arquivos verificará apenas os arquivos incluídos no escopo de proteção criado. Os arquivos que não estão incluídos nesse escopo estarão disponíveis para uso sem serem verificados. Isso aumenta o risco de infecção no seu computador.

7.2.3. Definindo as configurações avançadas

Nas configurações adicionais do Antivírus de Arquivos, você pode especificar o modo de verificação do sistema de arquivos e configurar as condições para pausar o componente temporariamente.

Para definir configurações adicionais do Antivírus de Arquivos:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando no link Configurações.
2. Clique no botão **Personalizar** e selecione a guia **Adicional** na janela que é aberta (veja a Figura 19).

O modo de verificação de arquivos determina as condições de processamento do Antivírus de Arquivos. Você tem as seguintes opções:

- **Modo inteligente**. Este modo tem como objetivo acelerar o processamento de arquivos e retorná-los para o usuário. Quando está selecionado, a decisão de verificação se baseia na análise das operações executadas com o arquivo.

  Por exemplo, ao usar um arquivo do Microsoft Office, o Kaspersky Anti-Virus o verifica quando é aberto pela primeira vez e fechado pela última vez. Todas as operações intermediárias que substituem o arquivo não são verificadas.

  O modo inteligente é o padrão.

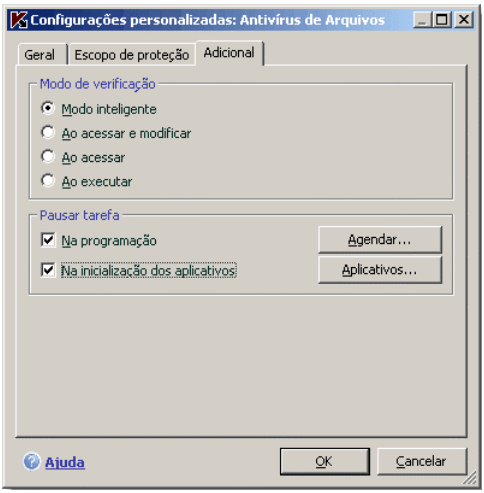


Figura 19. Definindo as configurações avançadas do Antivírus de Arquivos

- **Ao acessar e modificar** – o Antivírus de Arquivos verifica os arquivos quando são abertos ou editados.
- **Ao acessar** – verifica os arquivos apenas ao tentar abri-los.
- **Ao executar** – verifica os arquivos apenas ao tentar executá-los.

Pode ser necessário pausar o Antivírus de Arquivos ao executar tarefas que exigem recursos significativos do sistema operacional. Para diminuir a carga e assegurar que o usuário tenha novamente acesso aos arquivos rapidamente, é recomendável configurar que o componente seja desabilitado em uma determinada hora ou enquanto determinados programas estão em uso.

Para pausar o componente, marque ☑ **Na programação** e selecione um período para interromper e iniciar o componente na janela que é aberta (veja a Figura 20) ao clicar no botão **Programação**. Para fazê-lo, insira um valor no formato HH:MM nos campos correspondentes.

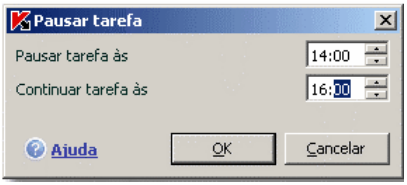


Figura 20. Pausando o componente

Para desabilitar o componente ao trabalhar com programas que exigem recursos significativos, marque **Na inicialização dos aplicativos** e edite a lista de programas na janela que é aberta (veja Figura 21) clicando em **Aplicativos**.

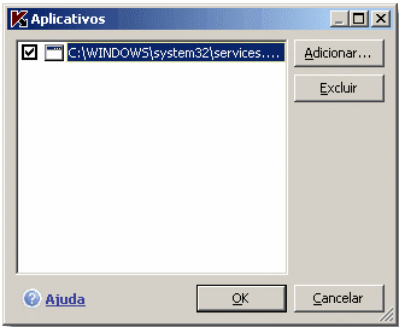


Figura 21. Criando uma lista de aplicativos

Para adicionar um aplicativo à lista, use o botão **Adicionar**. Um menu de contexto será aberto e, ao clicar em **Procurar**, você poderá ir para a janela de seleção de arquivos padrão e selecionar arquivo executável do aplicativo a ser adicionado. Alternativamente, vá para a lista de aplicativos em execução no item **Aplicativos** e selecione o desejado.

Para excluir um aplicativo, selecione-o em uma lista e clique em **Excluir**.

Você pode desabilitar temporariamente a pausa no Antivírus de Arquivos ao usar um aplicativo específico. Para fazê-lo, desmarque o nome do aplicativo. Não é necessário excluí-lo da lista.

7.2.4. Restaurando as configurações padrão do Antivírus de Arquivos

Ao configurar o Antivírus de Arquivos, você sempre pode retornar às configurações de desempenho padrão. A Kaspersky Lab as considera ideais e as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações padrão do Antivírus de Arquivos:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

Se você modificou a lista de objetos incluídos na zona protegida ao configurar o Antivírus de Arquivos, o programa perguntará se deseja salvar essa lista para usar no futuro, ao restaurar as configurações iniciais. Para salvar a lista de objetos, marque **Zona de proteção** na janela **Restaurar configurações** que é aberta.

7.2.5. Selecionando ações para objetos

Se o Antivírus de Arquivos descobrir ou suspeitar de uma infecção em um arquivo ao verificá-lo quanto à presença de vírus, as próximas etapas do programa dependerão do status do objeto e da ação selecionada.

O Antivírus de Arquivos pode rotular um objeto com um dos seguintes status:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*) (consulte 1.1 na p. 9).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o programa detectou no arquivo uma seqüência de código de um vírus desconhecido ou de código modificado de um vírus conhecido.

Por padrão, todos os arquivos infectados estão sujeitos à desinfecção e, se estiverem possivelmente infectados, serão enviados para a Quarentena.

Para editar uma ação para um objeto:

selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações. Todas as ações possíveis são exibidas nas seções apropriadas (veja a Figura 22).

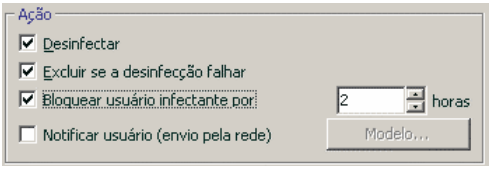


Figura 22. Possíveis ações do Antivírus de Arquivos para objetos perigosos

Se a ação selecionada for	Ao detectar um objeto perigoso
☑ **Desinfectar** ☐ **Excluir se a desinfecção falhar**	O acesso ao objeto é bloqueado, sendo feita uma tentativa de desinfectá-lo. Uma cópia do objeto é armazenada no Backup. Se a desinfecção for bem-sucedida, ele será retornado ao usuário para uso normal. Se o objeto não puder ser neutralizado, ele será movido para a Quarentena. Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.
☑ **Desinfectar** ☑ **Excluir se a desinfecção falhar**	O acesso ao objeto é bloqueado, sendo feita uma tentativa de desinfectá-lo. Uma cópia do objeto é armazenada no Backup. Se a desinfecção for bem-sucedida, ele será retornado ao usuário para uso normal. Se o objeto não puder ser desinfectado, ele será excluído.
☐ **Desinfectar** ☑ **Excluir**	O Antivírus de Arquivos bloqueará o acesso ao objeto e o excluirá.
☑ **Bloquear usuário infectante por ... horas**	Bloqueia o acesso ao servidor ou computador do qual foi feita a tentativa de copiar o arquivo infectado ou possivelmente infectado. Essa ação pode ser aplicada também às ações relacionadas com o processamento do arquivo (desinfecção ou exclusão).

Se a ação selecionada for	Ao detectar um objeto perigoso
	Observe que, se o usuário sair de uma sessão e fizer logon no sistema novamente, o Kaspersky Anti-Virus considerará essa conexão como sendo uma nova conexão e o impedimento será suspenso.
☑ **Notificar usuário (envio pela rede)**	Notifica o usuário de cujo computador foi feita a tentativa de copiar o arquivo infectado ou possivelmente infectado para o servidor, através de envio pela rede. Para configurar o modelo de notificação, clique no botão **Modelo** (consulte 7.2.6 na p. 83).

Ao desinfectar ou excluir um objeto, o Kaspersky Anti-Virus cria uma cópia do mesmo e a envia para o Backup, caso seja necessário restaurar o objeto ou surja uma oportunidade de neutralizá-lo.

Aviso! As ações **Bloquear usuário** e **Envio pela rede** não ficam disponíveis quando o aplicativo é executado no Microsoft Windows NT Server.

7.2.6. Criando um modelo de notificação

Nesta janela, você pode formatar o texto do modelo de notificação para o usuário cujo computador tentou copiar um arquivo infectado/possivelmente infectado para o servidor.

O texto da notificação pode conter macros para fornecer mais informações: o caminho do objeto perigoso e nome da ameaça. Para adicionar macros ao texto de notificação, clique em **Macros**.

Para restaurar o texto inicial usado para o modelo de notificação, clique no botão **Padrão**.

7.3. Desinfecção adiada

No Kaspersky Anti-Virus for Windows Servers, o acesso aos arquivos infectados será bloqueado se eles estiverem sendo desinfectados e se forem excluídos, quando não puderem ser desinfectados ou excluídos.

No Kaspersky Anti-Virus for Windows Servers, o acesso aos arquivos infectados será bloqueado se eles estiverem sendo desinfectados e se forem excluídos, quando não puderem ser desinfectados.

Para obter novamente o acesso a objetos bloqueados, eles devem ser desinfectados. Para fazê-lo:

1. Selecione **Antivírus de Arquivos** na janela principal do programa e clique em qualquer local da caixa **Estatísticas**.
2. Selecione os objetos que o interessam na guia **Detectados** e clique no botão **Ação** → **Neutralizar tudo**.

Os arquivos desinfectados com êxito serão retornados ao usuário. Os que não puderem ser neutralizados, poderão ser *excluídos* ou *ignorados*. No último caso, o acesso ao arquivo será restaurado. Contudo, isso aumenta significativamente o risco de infecção no seu computador. É altamente recomendável não ignorar objetos mal-intencionados.

CAPÍTULO 8. VERIFICANDO O COMPUTADOR QUANTO A PRESENÇA DE VIRUS

O Kaspersky Anti-Virus for Windows Servers pode verificar itens individuais, arquivos, pastas, discos, dispositivos plug-and-play ou todo o computador. A verificação de vírus impede a disseminação de códigos mal-intencionados não detectados pelo Antivírus de Arquivos.

O Kaspersky Anti-Virus for Windows Servers inclui as seguintes tarefas de verificação padrão:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus, incluindo: a memória do sistema, os programas carregados na inicialização, os setores de inicialização no disco rígido e os diretórios do sistema *Windows* e *system32*. A tarefa tem como objetivo detectar vírus ativos rapidamente no sistema sem verificar todo o computador.

Meu Computador

Verifica vírus no computador por meio de uma inspeção completa de todas as unidades de disco, memória e arquivos.

Objetos de inicialização

Verifica vírus em todos os programas carregados na inicialização do sistema operacional.

As configurações padrão dessas tarefas são as recomendadas. É possível editar essas configurações (consulte 8.4 na p. 89) ou criar uma programação (consulte 6.5 na p. 66) para a execução das tarefas.

Você também pode criar suas próprias tarefas (consulte a seção 8.3 na p. 88) e criar uma programação para elas. Por exemplo, é possível programar uma tarefa de verificação semanal dos bancos de dados de e-mail ou uma tarefa de verificação de vírus na pasta **Meus Documentos**.

Além disso, você pode verificar qualquer objeto quanto à presença de vírus sem criar uma tarefa de verificação específica. É possível selecionar um objeto para ser verificado na interface do Kaspersky Anti-Virus for Windows Servers ou com as ferramentas padrão do sistema operacional Windows Server (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**).

Você pode exibir uma lista completa das tarefas de verificação de vírus no computador clicando em **Verificação** no painel esquerdo da janela principal do programa.

8.1. Gerenciando tarefas de verificação de vírus

Você pode executar uma tarefa de verificação de vírus manual ou automaticamente por meio de uma programação (consulte 6.5 na p. 66).

Para iniciar uma tarefa de verificação de vírus manualmente:

Marque a caixa ao lado do nome da tarefa na seção **Verificação** da janela principal do programa e clique no botão na barra de status.

As tarefas em execução (incluindo aquelas criadas com o Kaspersky Administration Kit) são exibidas no menu de contexto clicando com o botão direito do mouse no ícone da bandeja do sistema.

Para pausar uma tarefa de verificação:

Clique no botão na barra de status. O status da tarefa mudará para *em pausa*. A verificação será pausada até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação.

Para interromper uma tarefa de verificação:

Clique no botão na barra de status. O status da tarefa mudará para *interrompida*. A verificação será interrompida até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação. Na próxima vez que você executar a tarefa, o programa perguntará se deseja continuar a tarefa do ponto em que foi interrompida ou iniciá-la novamente.

8.2. Criando uma lista de objetos para verificação

Para exibir uma lista dos objetos que devem ser verificados por uma determinada tarefa, selecione o nome da tarefa (por exemplo, **Meu Computador**) na seção **Verificação** da janela principal do programa. A lista de objetos será exibida à direita da janela, abaixo da barra de status (veja a Figura 23).

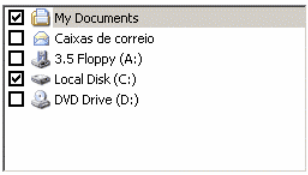


Figura 23. Lista de objetos a serem verificados

As tarefas padrão já possuem listas de objetos para verificação criadas na instalação do programa. Você pode criar uma lista de objetos ao criar suas próprias tarefas ou selecionar um objeto para uma tarefa de verificação de vírus.

É possível adicionar ou editar uma lista de objetos para verificação usando os botões à direita da lista. Para adicionar um novo objeto para verificação à lista, clique no botão **Adicionar** e, na janela que é aberta, selecione o objeto a ser verificado.

Para sua conveniência, é possível adicionar categorias a uma área de verificação, como caixas de correio, RAM, objetos de inicialização, backup do sistema operacional e arquivos da pasta Quarentena do Kaspersky Anti-Virus.

Além disso, ao adicionar uma pasta que contém objetos incorporados em uma área de verificação, você pode editar a recursão. Para fazê-lo, selecione um objeto na lista correspondente, abra seu menu de contexto e use a opção **Incluir subpastas**.

Para excluir um objeto, selecione-o na lista (ao fazê-lo, o nome do objeto será realçado em cinza) e clique no botão **Excluir**. É possível desabilitar temporariamente a verificação de objetos individuais para qualquer tarefa sem excluí-los da lista. Para fazê-lo, desmarque a caixa ao lado do objeto que não deseja verificar.

Para iniciar uma tarefa de verificação, clique no botão **Verificação**, selecione **Iniciar** no menu que é aberto ao clicar no botão **Ações**.

Além disso, você pode selecionar um objeto para ser verificado usando as ferramentas padrão do sistema operacional Windows Server (por exemplo, na janela do programa Explorer ou na Área de Trabalho, etc.) (veja a Figura 24). Para fazê-lo, selecione o objeto, abra o menu de contexto do Windows Server clicando com o botão direito do mouse e selecione **Verificar vírus**.

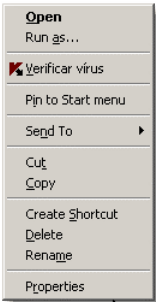


Figura 24. Verificando objetos a partir do menu de contexto do Windows

8.3. Criando tarefas de verificação de vírus

Para verificar objetos no computador quanto à presença de vírus, você pode usar as tarefas de verificação internas incluídas no programa e criar suas próprias tarefas. As novas tarefas de verificação são criadas usando tarefas existentes como modelo.

Para criar uma nova tarefa de verificação de vírus:

1. Selecione a tarefa com as configurações mais próximas do necessário na seção **Verificação** da janela principal do programa.
2. Abra o menu de contexto clicando com o botão direito do mouse no nome da tarefa ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Salvar como...**.
3. Insira o nome da nova tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá na lista de tarefas na seção **Verificação** da janela principal do programa.

Aviso!

O número de tarefas que podem ser criadas é limitado. O máximo são quatro tarefas.

A nova tarefa é uma cópia daquela na qual foi baseada. É necessário continuar sua configuração por meio da criação de uma lista de objetos para verificação (consulte 8.2 na página 86), da configuração de propriedades que controlarão a tarefa (consulte 8.4 na página 89) e, se necessário, da configuração de uma programação (consulte 6.5 na página 66) para executar a tarefa automaticamente.

Para renomear uma tarefa criada:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Renomear**.

Insira o novo nome da tarefa na janela que é aberta e clique em **OK**. O nome da tarefa também será mudado na seção **Verificação**.

Para excluir uma tarefa criada:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Excluir**.

Você deverá confirmar que deseja excluir a tarefa. A tarefa será então excluída da lista de tarefas na seção **Verificação**.

Aviso!

É possível renomear e excluir somente as tarefas criadas por você.

8.4. Configurando tarefas de verificação de vírus

Os métodos utilizados para verificar objetos no computador são determinados pelas propriedades atribuídas a cada tarefa.

Para configurar tarefas:

abra a janela de configurações do aplicativo e selecione o nome da tarefa na seção **Verificação**.

Você pode usar a janela de configurações de cada tarefa para:

- selecionar o nível de segurança que será usado pela tarefa (consulte a seção 8.4.1 na p. 90)
- editar configurações avançadas:
    - definir os tipos de arquivos que devem ser verificados quanto à presença de vírus (consulte a seção 8.4.2 na p. 91)
    - configurar o início da tarefa usando um perfil de usuário diferente (consulte 6.4 na p. 65)
    - definir as configurações avançadas de verificação (consulte 8.4.5 na p. 97)

- restaurar as configurações padrão de verificação (consulte a seção 8.4.3 na p. 94)
- selecionar uma ação que o programa aplicará ao detectar um objeto infectado ou possivelmente infectado (consulte a seção 8.4.4 na p. 95)
- criar uma programação (consulte 6.5 na p. 66) para executar tarefas automaticamente.

Além disso, você pode definir configurações globais (consulte a seção 8.4.6 na p. 99) para executar todas as tarefas.

As seções a seguir examinam detalhadamente as configurações de tarefas listadas acima.

8.4.1. Selecionando um nível de segurança

É possível atribuir um nível de segurança a cada tarefa de verificação de vírus (veja a Figura 25):

Alta – a verificação mais completa de todo o computador ou de discos, pastas ou arquivos individuais. É recomendável usar este nível no caso de suspeita de que um vírus infectou o computador.

Recomendado – os especialistas da Kaspersky Lab recomendam este nível. Serão verificados os mesmos arquivos que na configuração **Alto**, exceto pelos bancos de dados de e-mails.

Baixo – o nível com configurações que permitem usar tranqüilamente aplicativos que consomem muitos recursos, pois o escopo dos arquivos verificados é menor.

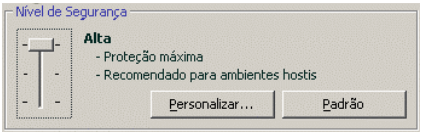


Figura 25. Selecionando um nível de segurança de verificação de vírus

Por padrão, a verificação de arquivos é definida como **Recomendado**.

Você pode aumentar ou diminuir o nível de segurança da verificação selecionando o nível desejado ou alterando as configurações do nível atual.

Para editar o nível de segurança:

Ajuste os controles deslizantes. Ao ajustar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de arquivos verificados: quanto menos arquivos verificados quanto à presença de vírus, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de arquivos atender às suas necessidades, você poderá personalizar as configurações da verificação. Para fazê-lo, selecione o nível mais próximo do necessário como ponto inicial e edite suas configurações. Se o fizer, o nível será renomeado para **Personalizado**.

Para modificar as configurações de um nível de segurança:

clique no botão **Configurações** na janela de configurações de tarefas. Edite as configurações de verificação na janela que é aberta e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Personalizado**, que contém as configurações de verificação definidas.

8.4.2. Especificando os tipos de objetos para verificação

Ao especificar os tipos de objetos que devem ser verificados, você estabelece os formatos, tamanhos e unidades de arquivos nos quais serão verificados vírus quando essa tarefa for executada.

Os tipos de arquivos verificados são definidos na seção **Tipos de arquivos** (veja a Figura 26). Selecione uma das três opções:

- **Verificar todos os arquivos**. Com esta opção, todos os arquivos serão verificados, sem exceção.
- **Verificar programas e documentos (por conteúdo)**. Se você selecionar este grupo de programas, apenas os arquivos possivelmente infectados serão verificados; aqueles nos quais um vírus poderia ter se infiltrado.

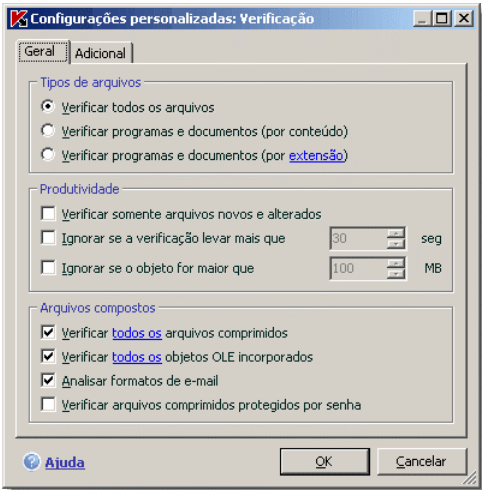


Figura 26. Configurando a verificação

> Observação:
>
> Existem arquivos nos quais os vírus não podem se inserir, pois em seu conteúdo não há nada onde o vírus possa se prender. Um exemplo são os arquivos .txt.
>
> Além disso, por outro lado, há formatos de arquivos que contêm ou podem conter código executável. Exemplos incluem os formatos .exe, .dll ou .doc. O risco de infiltração e ativação de código mal-intencionado nesses arquivos é bastante alto.

Antes de pesquisar um objeto quanto à presença de vírus, seu cabeçalho interno é analisado com relação ao formato do arquivo (txt, doc, exe, etc.).

- **Verificar programas e documentos (por extensão)**. Nesse caso, o programa verificará apenas os arquivos possivelmente infectados e, ao fazê-lo, o formato do arquivo será determinado pela extensão de seu nome. Usando o link, você pode analisar uma lista de extensões de arquivos verificados com essa opção (consulte a seção A.1 na p. 186).

Dica:

Não esqueça que um vírus em um arquivo com a extensão .txt, na verdade, poderia ser um arquivo executável renomeado como .txt. Se você selecionar a opção **Programas e documentos (por extensão)**, a verificação ignorará esse arquivo. Se a opção **Verificar programas e documentos (por conteúdo)** for selecionada, o programa analisará os cabeçalhos dos arquivos, descobrindo que o arquivo é um arquivo .exe e o verificando extensivamente quanto à presença de vírus.

Na seção **Produtividade**, você pode especificar que apenas os arquivos novos e modificados desde a verificação anterior serão verificados. Esse modo reduz sensivelmente o tempo de verificação e aumenta a velocidade de operação do programa. Para fazê-lo, marque **Verificar somente arquivos novos e alterados**. Esse modo estende-se a arquivos simples e compostos.

Você também pode definir limites de tempo e de tamanho de arquivo para a verificação na seção **Produtividade**.

- **Ignorar se a verificação levar mais que... seg.** Marque esta opção e insira o tempo máximo de verificação de um objeto. Se esse tempo for excedido, o objeto será removido da fila de verificação.
- **Ignorar se o objeto for maior que… MB**. Marque esta opção e insira o tamanho máximo de um objeto. Se esse tamanho for excedido, o objeto será removido da fila de verificação.

Na seção **Arquivos compostos**, especifique os arquivos compostos que devem ser analisados quanto à presença de vírus:

- **Verificar todos os/somente novos arquivos comprimidos** – verifica arquivos comprimidos .rar, .arj, .zip, .cab, .lha, .jar e .ice.

Aviso!

O Kaspersky Anti-Virus não exclui automaticamente os arquivos comprimidos em formatos aos quais ele não dá suporte (por exemplo, .ha, .uue, .tar), mesmo se você optar pela neutralização ou exclusão automática no caso de não ser possível neutralizar os objetos.

Para excluir esses arquivos comprimidos, clique no link Excluir arquivos comprimidos na notificação de detecção de objetos perigosos. A tela exibe esta mensagem quando a opção **Perguntar o que fazer na verificação/Perguntar o que fazer ao concluir a verificação** está selecionada (consulte a seção 8.4.4 na p. 95). Você também pode excluir os arquivos comprimidos infectados manualmente.

- **Verificar todos os/somente novos objetos OLE incorporados** – verifica objetos incorporados em arquivos (por exemplo planilhas do Excel ou uma

macro incorporada em um arquivo do Microsoft Word, anexos de e-mail, etc.).

Você pode selecionar e verificar todos os arquivos ou somente os novos de cada tipo de arquivo composto. Para fazê-lo, use o link ao lado do nome do objeto. Ele muda seu valor quando você clica nele. Se a seção **Produtividade** tiver sido configurada para verificar somente arquivos novos e modificados, você não poderá selecionar o tipo de arquivos compostos que serão verificados.

☑ **Analisar formatos de e-mail** – verifica arquivos e bancos de dados de e-mails. Se esta caixa de seleção estiver desmarcada, os arquivos com formato de e-mail serão verificados como arquivos binários (sem dissecar o formato) e, se o arquivo não estiver infectado e a opção Verificar todos os arquivos estiver selecionada, as informações com o status *OK* serão inseridas no relatório. Se as configurações da verificação de arquivos tiverem sido selecionadas por tipo e extensão, o objeto será ignorado com o veredito *excluído por tipo*.

Observe que, ao verificar bancos de dados de e-mail protegidos por senha:

- O Kaspersky Anti-Virus for Windows Servers detecta código mal-intencionado em bancos de dados do Microsoft Outlook 2000, mas não os neutraliza;
- O Kaspersky Anti-Virus for Windows Servers não dá suporte a verificações de código mal-intencionado em bancos de dados protegidos do Microsoft Outlook 2003.

☑ **Verificar arquivos comprimidos protegidos por senha** – verifica arquivos comprimidos protegidos por senha. Com este recurso, uma janela solicitará uma senha antes de verificar objetos de arquivos comprimidos. Se a caixa não estiver marcada, os arquivos comprimidos protegidos por senha serão ignorados.

8.4.3. Restaurando configurações de verificação padrão

Ao definir as configurações de tarefas de verificação, é sempre possível retornar para as configurações recomendadas. A Kaspersky Lab as considera ideais e as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações de verificação padrão:

1. Selecione o nome da tarefa na seção **Verificação** da janela principal e use o link Configurações para abrir a janela de configurações da tarefa.

2. Clique no botão **Padrão** na seção **Nível de segurança**.

8.4.4. Selecionando ações para objetos

Se, durante uma verificação, for descoberto que um arquivo está infectado ou é suspeito, as próximas etapas do programa dependerão do status do objeto e da ação selecionada.

Um dos seguintes status pode ser atribuído ao objeto após a verificação:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. É provável que o programa tenha detectado uma seqüência de código de um vírus desconhecido ou de um vírus conhecido modificado.

Por padrão, todos os arquivos infectados são desinfectados e, se estiverem possivelmente infectados, serão enviados para a Quarentena.

Para editar uma ação para um objeto:

selecione o nome da tarefa na seção **Verificação** da janela principal do programa e use o link Configurações para abrir a janela de configurações da tarefa. Todas as respostas possíveis são exibidas nas seções apropriadas (veja a Figura 27).

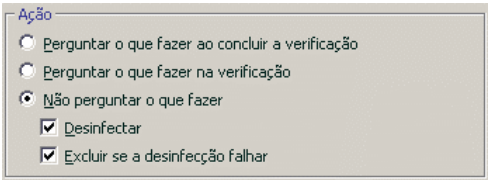


Figura 27. Selecionando ações para objetos perigosos

Se a ação selecionada for	Ao detectar um objeto mal-intencionado ou possivelmente infectado
◉ **Perguntar o que fazer ao concluir a verificação**	O programa não processa os objetos até o final da verificação. Quando a verificação for concluída, a janela de estatísticas será aberta com uma lista dos objetos detectados, solicitando uma ação para cada objeto.
◉ **Perguntar o que fazer na verificação**	O programa emitirá uma mensagem de aviso com informações sobre o código mal-intencionado que infectou, ou possivelmente infectou, o arquivo e permite que você escolha uma das ações a seguir.
◉ **Não perguntar o que fazer**	O programa registra as informações sobre os objetos detectados no relatório, sem processá-los ou emitir uma notificação. Não é recomendável usar esta opção, pois os objetos infectados e possivelmente infectados permanecem no computador, sendo praticamente impossível evitar a infecção.
◉ **Não perguntar o que fazer** ☑ **Desinfectar**	O programa tenta neutralizar o objeto detectado sem solicitar uma confirmação. Se for possível desinfectar o arquivo, ele será movido para o Backup para ser desinfectado mais tarde. Se o programa não puder desinfectar o objeto, o acesso a ele será bloqueado.
◉ **Não perguntar o que fazer** ☑ **Desinfectar** ☑ **Excluir se a desinfecção falhar**	O programa tenta neutralizar o objeto detectado sem solicitar uma confirmação. Se o objeto não puder ser desinfectado, ele será excluído. Uma cópia será armazenada no Backup.

Se a ação selecionada for	Ao detectar um objeto mal-intencionado ou possivelmente infectado
◉ **Não perguntar o que fazer** ☐ **Desinfectar** ☑ **Excluir**	O programa exclui o objeto automaticamente.

Ao desinfectar ou excluir um objeto, o Kaspersky Anti-Virus for cria uma cópia do mesmo e a envia para o Backup (consulte 12.2 na p. 155), caso seja necessário restaurá-lo ou surja uma oportunidade de neutralizá-lo.

Com o status *possivelmente infectado*, o objeto é movido para a Quarentena sem tentar desinfectá-lo.

8.4.5. Outras configurações de verificação de vírus

Além de definir as configurações básicas de verificação de vírus, você também pode usar configurações avançadas (veja a Figura 28):

☑ **Habilitar tecnologia iChecker** – usa a tecnologia que pode aumentar a velocidade de verificação por meio da exclusão de determinados objetos. Um objeto é excluído da verificação usando um algoritmo específico que leva em conta a data de lançamento das assinaturas de ameaças, a data mais recente em que o objeto foi verificado e as modificações das configurações de verificação.

Por exemplo, você tem um arquivo armazenado que o programa verificou e ao qual atribuiu o status de não infectado. Na próxima verificação, o programa ignorará esse arquivo, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Mas o programa verificará o arquivo comprimido novamente se sua estrutura tiver mudado porque foi adicionado um novo objeto a ele, se as configurações de verificação tiverem sido alteradas ou se as assinaturas de ameaças tiverem sido atualizadas.

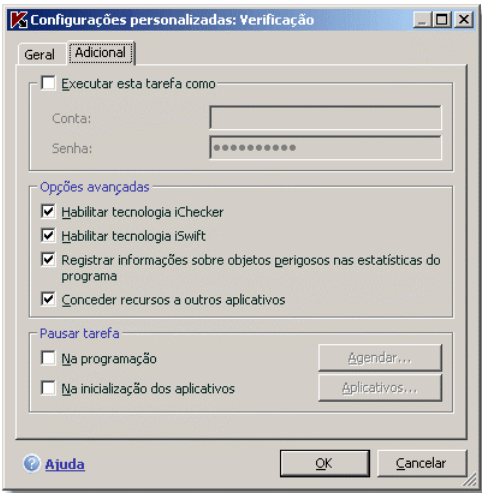


Figura 28. Configurações avançadas de verificação

A tecnologia iChecker™ tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo Kaspersky Anti-Virus for Windows Servers (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

Habilitar tecnologia iSwift. Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam o sistema de arquivos NTFS. A tecnologia iSwift tem algumas limitações: ela é ligada a um local específico para o arquivo do sistema de arquivos e pode ser aplicada somente a objetos em um sistema de arquivos NTFS.

Registrar informações sobre objetos perigosos nas estatísticas do programa – salva informações sobre objetos perigosos detectados nas estatísticas gerais do programa e exibe uma lista de ameaças detectadas durante a verificação na guia **Detectados** da janela do relatório (consulte a seção 11.3.2 na p. 129). Se esta opção ficar desmarcada, as informações sobre objetos perigosos não serão exibidas no relatório e será impossível processar dados.

Conceder recursos a outros aplicativos – pausa a tarefa de verificação de vírus se o processador estiver ocupado com outros aplicativos.

8.4.6. Definindo configurações globais de verificação para todas as tarefas

Cada tarefa de verificação é executada de acordo com suas próprias configurações. Por padrão, as tarefas criadas ao instalar o programa no computador usam as configurações recomendadas pela Kaspersky Lab.

Você pode definir configurações globais de verificação para todas as tarefas. Como ponto de partida, você usará um conjunto de propriedades utilizadas para verificar vírus em um objeto individual.

Para atribuir configurações globais de verificação para todas as tarefas:

1. Selecione a seção **Verificação** à esquerda da janela principal do programa e clique em Configurações.
2. Na janela de configurações que é aberta, defina as configurações de verificação: Selecione o nível de segurança (consulte 8.4.1 na p. 90), defina as configurações de nível avançado e selecione uma ação (consulte 8.4.4 na p. 95) para os objetos.
3. Para aplicar essas novas configurações a todas as tarefas, clique no botão **Aplicar** na seção **Outras configurações de tarefas**. Confirme as configurações globais selecionadas na caixa de diálogo pop-up.

CAPÍTULO 9. TESTANDO O KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Depois de instalar e configurar o Kaspersky Anti-Virus, é recomendável verificar se as configurações e se a operação do programa estão corretas usando um vírus de teste e suas variações.

9.1. O vírus de teste da EICAR e suas variações

O vírus de teste foi especialmente desenvolvido pela eicar (The European Institute for Computer Antivirus Research) pra testar a funcionalidade dos antivírus.

O vírus de teste NÃO É UM VÍRUS e não contém nenhum código de programa que possa danificar seu computador. Contudo, a maioria dos programas antivírus o identificarão como um vírus.

Nunca use vírus reais para testar a funcionalidade de um antivírus!

Você pode baixar o vírus de teste do site oficial da **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

O arquivo que é baixado do site da **EICAR** contém o corpo de um vírus de teste padrão. O Kaspersky Anti-Virus o detectará, o rotulará como um **vírus** e executará a ação definida para esse tipo de objeto.

Para testar as reações do Kaspersky Anti-Virus quando diferentes tipos de objetos são detectados, você pode modificar o conteúdo do vírus de teste padrão, adicionando um dos prefixos mostrados na tabela.

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
Sem prefixo, vírus de teste padrão	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	O aplicativo identificará o objeto como sendo mal-intencionado e não passível de neutralização, e o excluirá.
CORR-	Corrompido.	O aplicativo poderia acessar o objeto, mas não verificá-lo, pois ele está corrompido (por exemplo, a estrutura do arquivo foi violada ou tem um formato de arquivo inválido).
SUSP- WARN-	O arquivo contém um vírus de teste (modificação). Não é possível desinfectar o objeto.	Esse objeto é uma modificação de um vírus conhecido ou desconhecido. No momento da detecção, os bancos de dados de assinaturas de ameaças não contêm uma descrição do procedimento para neutralizar esse objeto. O aplicativo o colocará na Quarentena para que seja processado posteriormente com assinaturas de ameaças atualizadas.
ERRO-	Erro de processamento.	Ocorreu um erro ao processar o objeto: o aplicativo não pode acessar o objeto que está sendo verificado, pois a integridade do mesmo foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o objeto estiver sendo verificado em uma unidade de rede).

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
CURE-	O arquivo contém um vírus de teste. Ele pode ser neutralizado. O objeto é passível de desinfecção, e o texto do corpo do vírus mudará para CURE.	O objeto contém um vírus que pode ser neutralizado. O aplicativo verificará o objeto quanto à presença de vírus e, em seguida, será totalmente neutralizado.
DELE-	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	Esse objeto contém um vírus que não pode ser desinfectado ou que é um cavalo de Tróia. O aplicativo exclui esses objetos.

A primeira coluna da tabela contém os prefixos que precisam ser adicionados ao início da seqüência de caracteres de um vírus de teste padrão. A segunda coluna descreve o status e a reação do Kaspersky Anti-Virus aos vários tipos de vírus de teste. A terceira coluna contém informações sobre objetos com o mesmo status que o aplicativo processou.

Os valores das configurações de verificação de vírus determinam a medida tomada sobre cada um dos objetos.

9.2. Testando o Antivírus de Arquivos

Para testar a funcionalidade do Antivírus de Arquivos;

1. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte a seção 9.1 na p. 100) e as modificações do vírus de teste que você criou para essa pasta.
2. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque ☑ **Registrar eventos não críticos** na janela de configurações do relatório (consulte 11.3.1 na p. 128).
3. Execute o vírus de teste ou uma de suas modificações.

O Antivírus de Arquivos interceptará a tentativa de acessar o arquivo, verificará o arquivo e o excluirá.

Ao selecionar opções diferentes de configurações predefinidas para lidar com os objetos detectados, você pode testar a reação do Antivírus de Arquivos ao detectar vários tipos de objetos.

Você pode ver os detalhes do desempenho do Antivírus de Arquivos no relatório do componente.

9.3. Testando as tarefas de verificação de vírus

Para testar as tarefas de verificação de vírus:

1. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte a seção 9.1 na p. 100) e as modificações do vírus de teste que você criou para essa pasta.
2. Crie uma nova tarefa de verificação de vírus (consulte a seção 8.3 na p. 88) e selecione a pasta que contém o conjunto de vírus de teste para ser verificada (consulte a seção 9.1 na p. 100).
3. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque ☑ **Registrar eventos não críticos** na janela de configurações do relatório.
4. Execute a tarefa de verificação de vírus (consulte a seção 8.1 na p. 86).

Ao executar uma verificação, conforme os objetos suspeitos ou infectados forem detectados, serão exibidas notificações na tela com informações sobre os objetos, perguntando ao usuário sobre a próxima medida a ser tomada:

Figura 29. Objeto perigoso detectado

Dessa forma, ao selecionar diferentes opções de configuração predefinidas para as ações, você pode testar as reações do Kaspersky Anti-Virus ao detectar vários tipos de objetos.

Você pode ver os detalhes do desempenho da tarefa de verificação de vírus no relatório do componente.

CAPÍTULO 10. ATUALIZAÇÕES DO PROGRAMA

Manter o software antivírus atualizado é um investimento na segurança. Com o aparecimento diário de novos vírus, cavalos de Tróia e software mal-intencionado, é importante atualizar periodicamente o aplicativo para manter suas informações sempre protegidas.

A atualização do aplicativo envolve o download e a instalação dos seguintes componentes no computador:

- **Assinaturas de ameaças**

  O aplicativo usa assinaturas de ameaças para proteger as informações contidas no computador. Os componentes de software que oferecem proteção usam o banco de dados de assinaturas de ameaças para pesquisar e desinfectar objetos nocivos no computador. As assinaturas são completadas a cada hora, com registros de novas ameaças e métodos para combatê-las. Assim, é recomendável atualizá-las periodicamente.

  As versões anteriores dos aplicativos da Kaspersky Lab davam suporte a conjuntos de bancos de dados *padrão* e *estendido*. Cada banco de dados era responsável por proteger o computador de diferentes tipos de objetos perigosos. Com o Kaspersky Anti-Virus for Windows Servers, você não precisa se preocupar com a seleção do conjunto de assinaturas de ameaças apropriado. Agora, nossos produtos usam assinaturas de ameaças que o protegem de objetos mal-intencionados e possivelmente perigosos, e de ataques de hackers.

- **Módulos do aplicativo**

  Além das assinaturas, você pode atualizar os módulos do Kaspersky Anti-Virus for Windows Servers. Novas atualizações do aplicativo surgem periodicamente.

As principais fontes de atualização do Kaspersky Anti-Virus for Windows Servers são os servidores de atualização da Kaspersky Lab.

Para baixar as atualizações disponíveis dos servidores de atualização, é necessário que o computador esteja conectado à Internet.

Se você não tiver acesso aos servidores de atualização da Kaspersky Lab (por exemplo, se o computador não estiver conectado à Internet), é possível ligar para o escritório central da Kaspersky Lab nos números +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 e solicitar informações de contato

dos parceiros da Kaspersky Lab que podem fornecer atualizações compactadas em disquetes ou CDs.

É possível baixar as atualizações de um dos seguintes modos:

- *Automaticamente*. O Kaspersky Anti-Virus verifica os pacotes de atualização na fonte em intervalos definidos. É possível definir as verificações de forma que sejam mais freqüentes durante os surtos de vírus e menos freqüentes quando eles terminarem. Quando o Antivírus detectar novas atualizações, ele as baixará e instalará no computador. Essa é a configuração padrão.
- *Na programação*. A atualização é programada para iniciar em uma hora especificada.
- *Manualmente*. Com esta opção, você inicia a Atualização manualmente.

Durante a atualização, o aplicativo compara as assinaturas de ameaças e os módulos do aplicativo no computador com as versões disponíveis no servidor de atualização. Se o servidor possuir a versão mais recente das assinaturas e módulos, será exibida uma observação sobre isso na janela do aplicativo. Se as assinaturas e os módulos no computador forem diferente daqueles no servidor de atualização, somente as partes ausentes das atualizações serão baixadas. A Atualização não baixa assinaturas de ameaças e módulos que você já possui, o que aumenta significativamente a velocidade de download e economiza tráfego da Internet.

Antes de atualizar as assinaturas de ameaças, o Kaspersky Anti-Virus for Windows Servers cria cópias delas, que podem ser usadas se for necessário executar uma reversão (consulte 10.2 na página 107). Se, por exemplo, o processo de atualização corromper as assinaturas de ameaças e inutilizá-las, você poderá facilmente reverter para a versão anterior e tentar atualizar as assinaturas mais tarde.

Você pode distribuir as atualizações recuperadas em uma fonte local enquanto atualiza o aplicativo (consulte 10.4.4 na p.115). Esse recurso permite atualizar os bancos de dados e os módulos usados pelos aplicativos 6.0 em computadores em rede para economizar largura de banda.

10.1. Iniciando a Atualização

É possível iniciar o processo de atualização a qualquer momento. Ele será executado a partir da fonte de atualização selecionada (consulte a seção 10.4.1 na p. 109).

Você pode iniciar a Atualização:

- do menu de contexto (consulte a seção 4.2 na p. 38).

- da janela principal do programa (consulte a seção 4.3 na p. 39)

Para iniciar a Atualização no menu de atalho:

1. Clique com o botão direito do mouse no ícone do aplicativo na bandeja do sistema para abrir o menu de atalho.
2. Selecione **Atualização**.

Para iniciar a Atualização na janela principal do programa:

1. Selecione **Atualização** na seção **Serviço**.
2. Clique no botão **Atualizar agora** no painel direito da janela principal ou use o botão na barra de status.

O andamento da atualização será exibido em uma janela específica, que pode ser ocultada clicando em **Fechar**. A atualização continuará com a janela oculta.

Observe que as atualizações são distribuídas para a fonte local durante o processo de atualização, desde que esse serviço esteja habilitado (consulte a seção 10.4.4 na p. 115).

10.2. Revertendo para a atualização anterior

Sempre que você iniciar a Atualização, o Kaspersky Anti-Virus for Windows Servers criará uma cópia de backup das assinaturas de ameaças atuais antes de começar o download das atualizações. Dessa forma, você poderá voltar a usar a versão anterior das assinaturas, se a atualização falhar.

Para reverter para a versão anterior das assinaturas de ameaças:

1. Selecione o componente **Atualização** na seção **Serviço** da janela principal do programa.
2. Clique no botão **Reverter** no painel direito da janela principal do programa.

10.3. Criando tarefas de atualização

O Kaspersky Anti-Virus possui uma tarefa de atualização interna para atualizar módulos do programa e assinaturas de ameaças. Você também pode criar suas próprias tarefas de atualização com várias configurações e programações de início.

Por exemplo, você instalou o Kaspersky Anti-Virus em um laptop que usa em casa e no escritório. Em casa, você atualiza o programa dos servidores de atualização da Kaspersky Lab e, no escritório, de uma pasta local que armazena as atualizações necessárias. Use duas tarefas diferentes para não precisar alterar as configurações de atualização a cada vez que mudar de local.

Para criar uma tarefa de atualização avançada:

1. Selecione **Atualização** na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Salvar como**.
2. Insira o nome da tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá então na seção **Serviço** da janela principal do programa.

Aviso!

O número de tarefas de atualização que podem ser criadas pelo usuário no Kaspersky Anti-Virus é limitado. Número máximo: duas tarefas.

A nova tarefa herda todas as propriedades da tarefa na qual foi baseada, exceto as configurações de programação. A configuração padrão dessa verificação automática é desabilitada. Continue a configuração especificando a fonte de atualização (consulte 10.4.1 na página 109), as configurações de rede (consulte 10.4.3 na página 114) e, se necessário, habilitando as tarefas com privilégios (consulte 6.4 na página 65) e configurando a programação (consulte 6.5 na p. 66).

Para renomear uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Renomear**.

Insira o novo nome da tarefa na janela que é aberta e clique em **OK**. O nome da tarefa será mudado então na seção **Serviço**.

Para excluir uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Excluir**.

Confirme se você deseja excluir a tarefa na janela de confirmação. A tarefa será então excluída da lista de tarefas na seção **Serviço**.

Aviso!

Somente as tarefas personalizadas poderão ser renomeadas e excluídas.

10.4. Configurando a atualização

As configurações da Atualização especificam os seguintes parâmetros:

- A fonte para o download e a instalação das atualizações (consulte a seção 10.4.1 na p. 109);
- O modo de atualização do aplicativo e os itens específicos atualizados (consulte a seção 10.4.2 na p. 112);
- A freqüência da atualização, caso as atualizações sejam executadas por programação (consulte a seção 6.5 na p. 66);
- A conta na qual a atualização será executada (consulte 6.4 na p. 65);
- O requisito para copiar as atualizações baixadas em um diretório local (consulte a seção 10.4.4 na p. 115);
- As ações que devem ser executadas após a conclusão da atualização (consulte a seção 10.4.5 na p. 117)

As seções a seguir examinam estes aspectos detalhadamente.

10.4.1. Selecionando uma fonte de atualização

A *fonte de atualização* é algum recurso que contém as atualizações das assinaturas das ameaças e dos módulos do aplicativo Kaspersky Anti-Virus.

Você pode usar as seguintes fontes de atualização:

- *Servidor de Administração* – um repositório de atualizações centralizado que reside no Servidor Administrativo do Kaspersky Administration Kit (para obter mais detalhes, consulte o Manual do Usuário do Administrador do Kaspersky Administration Kit 6.0).
- *Servidores de atualização da Kaspersky Lab* – sites específicos que contêm atualizações disponíveis de assinaturas de ameaças e módulos dos aplicativos de todos os produtos da Kaspersky Lab.
- *Servidor FTP ou HTTP, pasta local ou de rede* – pasta ou servidor local que contém as atualizações mais recentes.

Se não for possível acessar os servidores de atualização da Kaspersky Lab (por exemplo, se não houver uma conexão com a Internet), você poderá ligar para a sede da Kaspersky Lab pelos telefones +7 (495) 797-87-00, 7 (495) 645-79-39 ou +7 (495) 956-70-00 para solicitar informações de contato dos parceiros da

Kaspersky Lab, que podem fornecer atualizações compactadas em disquetes ou CDs.

Aviso!

Ao solicitar atualizações em mídia removível, especifique se deseja receber também as atualizações dos módulos do aplicativo.

Você pode copiar as atualizações de um disco e carregá-las em um site FTP ou HTTP, ou salvá-las em uma pasta local ou de rede.

Selecione a fonte de atualização na guia **Fonte de atualização** (veja a Figura 30).

Por padrão, as atualizações são baixadas dos servidores de atualização da Kaspersky Lab. A lista de endereços representados por este item não pode ser editada. Durante a atualização, o Kaspersky Anti-Virus for Windows Servers chama essa lista, seleciona o endereço do primeiro servidor e tentar baixar os arquivos desse servidor. Se não for possível baixar as atualizações do primeiro servidor, o aplicativo tentará se conectar a cada servidor, até ser bem-sucedido.

Para baixar atualizações de outro site FTP ou HTTP:

1. Clique em **Adicionar**.
2. Na caixa de diálogo **Selecionar fonte de atualização**, selecione o site FTP ou HTTP de destino ou especifique o endereço IP, o nome do caractere ou endereço da URL desse site no campo **Fonte**. Ao selecionar um site FTP como fonte de atualização, insira as configurações de autenticação na URL do servidor, no formato ftp://<nome_do_usuário>:<senha>@<host>:<porta>.

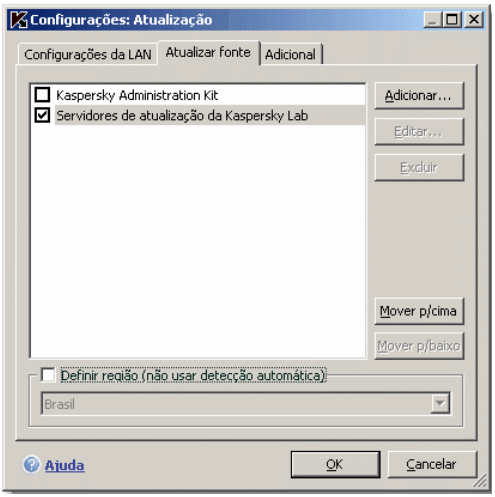


Figura 30. Selecionando uma fonte de atualização

Aviso!

Se um recurso localizado fora da rede local for selecionado como fonte de atualização, é necessário ter uma conexão com a Internet para a atualização.

Para atualizar de uma pasta local:

1. Clique em **Adicionar**.
2. Na caixa de diálogo **Selecionar fonte de atualização**, selecione uma pasta ou especifique o caminho completo da pasta no campo **Fonte**.

O Kaspersky Anti-Virus for Windows Servers adiciona novas fontes de atualização ao início da lista e habilita a fonte automaticamente, marcando a caixa ao lado do nome da fonte.

Se vários recursos forem selecionados como fontes de atualização, o aplicativo tentará se conectar a cada um deles, começando pelo primeiro na lista, e recuperará as atualizações da primeira fonte disponível. Você pode alterar a ordem das fontes na lista, usando os botões **Mover para cima** e **Mover para baixo**.

Para editar a lista, use os botões **Adicionar**, **Editar** e **Remover**. Não é possível editar ou excluir os servidores de atualização da Kaspersky Lab ou do Kaspersky Administration Kit.

Se você usar os servidores de atualização da Kaspersky Lab como fonte de atualização, poderá selecionar o local de servidor ideal para o download das atualizações. A Kaspersky Lab possui servidores em vários países. A escolha do servidor de atualização da Kaspersky Lab mais próximo economizará tempo e o download das atualizações será mais rápido.

Para escolher o servidor mais próximo, marque **Definir região (não usar detecção automática)** e selecione o país mais próximo do seu local atual na lista suspensa. Se você marcar essa caixa de seleção, as atualização serão executadas levando em conta a região selecionada na lista. Por padrão, essa caixa de seleção está desmarcada, sendo usadas as informações sobre a região atual do Registro do sistema operacional.

10.4.2. Selecionando um método de atualização e o que atualizar

Ao definir as configurações de atualização, é importante especificar o que será atualizado e qual método de atualização será usado.

Objetos de atualização (veja a Figura 31) são os componentes que serão atualizados:

- Assinaturas de ameaças
- Módulos do programa

As assinaturas de ameaças são atualizadas sempre, enquanto os módulos do aplicativo são atualizados somente se essa for a configuração.

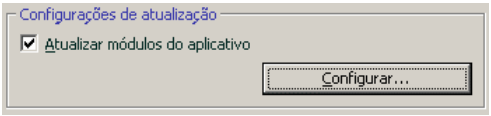


Figura 31. Selecionando objetos de atualização

Se desejar baixar e instalar atualizações dos módulos do programa:

Marque **Atualizar módulos do programa** na janela **Atualização**.

Se houver atualizações de módulos do aplicativo na fonte de atualização, o aplicativo baixará as atualizações necessárias e as aplicará quando o computador for reiniciado. As atualizações de módulos baixadas não serão instaladas até que o computador seja reiniciado.

Se a próxima atualização do programa ocorrer antes que o computador seja reiniciado e que as atualizações dos módulos do programa

anteriores sejam instaladas, somente as assinaturas de ameaças serão atualizadas.

O método de atualização (veja a Figura 32) define como a Atualização será iniciada. No **Modo de execução**, você pode selecionar um dos seguintes métodos:

- **Automaticamente**. O Kaspersky Anti-Virus verifica a fonte de atualizações dos pacotes de atualização em intervalos definidos (consulte a seção 10.4.1 na p. 109). Quando o Antivírus detectar novas atualizações, ele as baixará e instalará no computador.

  Se um recurso de rede for especificado como fonte de atualização, o Kaspersky Anti-Virus tentará iniciar a Atualização depois de algum tempo, conforme especificado no pacote de atualização anterior.

  Se uma pasta local for selecionada como fonte de atualização, o aplicativo tentará baixar as atualizações a partir da pasta local com a mesma freqüência especificada no pacote de atualização baixado na atualização anterior. Esta opção permite que a Kaspersky Lab regule a freqüência com que o programa será atualizado no caso de surtos de vírus e outras situações possivelmente perigosas. Seu aplicativo receberá as atualizações mais recentes de assinaturas de ameaças, ataques de rede e módulos de software oportunamente, evitando assim a invasão do servidor por software mal-intencionado.

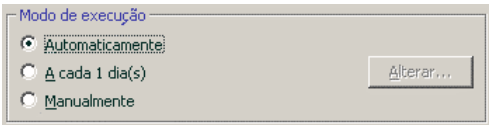


Figura 32. Selecionando um modo de execução da atualização

- **Na programação**. A atualização é programada para iniciar em uma hora especificada. Por padrão, as atualizações programadas ocorrerão a cada 2 horas. Para editar a programação padrão, clique no botão **Alterar...** ao lado do título do modo e faça as alterações necessárias na janela que é aberta (para obter mais detalhes, consulte a seção 6.5 na p. 66). Este é o modo utilizado por padrão.
- **Manualmente**. Com esta opção, você inicia a Atualização manualmente. O Kaspersky Anti-Virus for Windows Servers o notificará quando precisar ser atualizado:

  - Primeiro, uma mensagem pop-up informando que a atualização é necessária aparece acima do ícone do aplicativo na bandeja do sistema (se as notificações estiverem habilitadas; consulte a seção 11.8.1 na p. 139)

- O segundo indicador na janela principal do programa informa que seu computador está desatualizado (consulte 5.1.1 na p. 43)
- Uma recomendação de que é necessário atualizar o aplicativo aparece na seção de mensagens na janela principal do programa (consulte 4.3 na p. 39)

10.4.3. Configurando a conexão

Se você configurar o programa para recuperar atualizações dos servidores de atualização da Kaspersky Lab ou de outros sites FTP ou HTTP, é recomendável verificar primeiro suas configurações de conexão.

Todas as configurações estão agrupadas em uma guia específica – **Configurações da LAN** (veja a Figura 33).

Marque **Se possível, usar modo de FTP passivo** se você baixar as atualizações de um servidor FTP no modo passivo (por exemplo, através de um firewall). Se estiver trabalhando no modo FTP ativo, desmarque essa caixa de seleção.

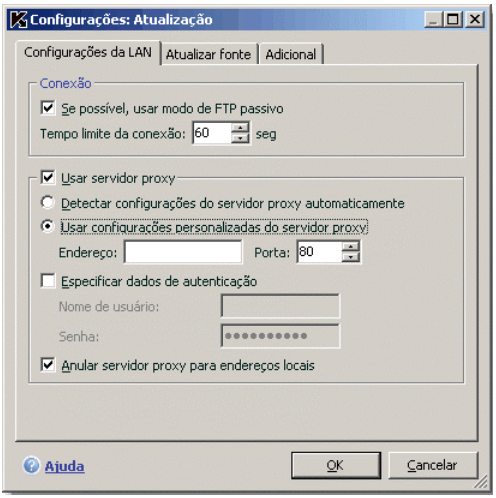


Figura 33. Definindo as configurações de atualização de rede

No campo **Tempo limite da conexão… (seg)**, atribua o tempo alocado para a conexão com o servidor de atualização. Se a conexão falhar e esse período tiver acabado, o programa tentará conectar-se ao próximo servidor de atualização. Isso continuará até que uma conexão seja bem-sucedida ou até que se tenha tentado todos os servidores de atualização disponíveis.

Marque **Usar servidor proxy** se estiver usando um servidor proxy para acessar a Internet e, se necessário, selecione as configurações a seguir:

- Selecione as configurações do servidor proxy que serão usadas durante a atualização:

  Detectar configurações do servidor proxy automaticamente. Se você selecionar esta opção, as configurações de proxy serão detectadas automaticamente usando o WPAD (Web Proxy Auto-Discovery Protocol). Se esse protocolo não conseguir detectar o endereço, o Kaspersky Anti-Virus usará as configurações de servidor proxy especificadas no Microsoft Internet Explorer.

  Usar configurações personalizadas do servidor proxy – Usa um proxy diferente daquele especificado nas configurações de conexão do navegador. No campo **Endereço**, digite o endereço IP ou o nome simbólico do servidor proxy e especifique o número da porta proxy no campo **Porta**.

- Especifique se o servidor proxy requer autenticação. *Autenticação* é o processo de verificação dos dados de registro do usuário para fins de controle de acesso.

  Se a autenticação for necessária para conectar-se ao servidor proxy, marque **Especificar dados de autenticação** e defina o nome de usuário e a senha nos campos a seguir. Nesse caso, serão tentadas primeiro a autenticação NTLM e depois a autenticação BASIC.

  Se esta caixa de seleção não estiver marcada ou se os dados não forem inseridos, será tentada a autenticação NTLM utilizando a conta de usuário que foi usada para iniciar a atualização (consulte 6.4 na p. 65).

  Se o servidor proxy exigir **autenticação** e você não inseriu o nome de usuário e a **senha** ou se, por algum motivo, os dados especificados não foram aceitos pelo servidor proxy, uma janela pop-up será exibida ao iniciar as atualizações, solicitando um nome de usuário e uma senha para autenticação. Se a autenticação for bem-sucedida, o nome de usuário e a senha serão usados nas próximas atualizações. Caso contrário, as configurações de autenticação serão solicitadas novamente.

Para evitar o uso de um proxy quando a fonte de atualização for uma pasta local, selecione **Anular servidor proxy para endereços locais**.

10.4.4. Distribuição de atualizações

O recurso de cópia de atualizações torna possível otimizar a carga na rede empresarial. As atualizações são copiadas em dois estágios:

1. Um dos computadores na rede recupera um pacote de atualização do aplicativo e da assinatura de ameaças nos servidores da Kaspersky Lab ou de outros recursos da Web que hospedem um conjunto de atualizações. As atualizações recuperadas são colocadas em uma pasta de acesso público.
2. Os outros computadores da rede acessam essa pasta para recuperar as atualizações do aplicativo.

Para habilitar a distribuição de atualizações, marque a caixa de seleção **Atualizar pasta de distribuição** na guia **Adicional** (veja a Figura 34) e, no campo a seguir, especifique a pasta compartilhada na qual serão colocadas as atualizações recuperadas. Você pode inserir o caminho manualmente ou selecioná-lo na janela que é aberta ao clicar em **Procurar**. Se a caixa de seleção estiver marcada, as atualizações serão copiadas automaticamente para essa pasta quando forem recuperadas.

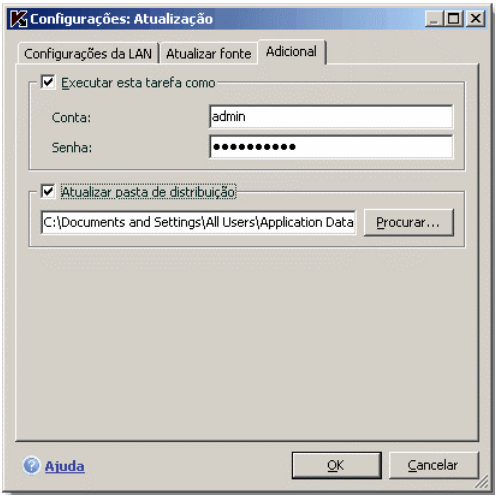


Figura 34. Configurações da ferramenta de cópia de atualizações

Você também pode especificar o método de distribuição de atualizações:

- *completo*, copia as atualizações de assinaturas de ameaças e de componentes de todos os aplicativos da versão 6.0 da Kaspersky Lab. Para selecionar as atualizações completas, marque a caixa de seleção **Copiar atualizações de todos os componentes**.
- *personalizado*, copia apenas as assinaturas de ameaças e atualizações dos componentes do Kaspersky Anti-Virus 6.0 que estão instalados. Se desejar selecionar este método de atualização, desmarque a caixa de seleção **Copiar atualizações de todos os componentes**.

Se desejar que outros computadores na rede sejam atualizados da pasta que contém atualizações copiadas da Internet, execute as seguintes etapas:

1. Conceda acesso público a esta pasta.
2. Especifique a pasta compartilhada como fonte de atualização nos computadores da rede, nas configurações da Atualização.

10.4.5. Ações após a atualização do programa

Cada atualização de assinaturas de ameaças contém novos registros que protegem seu computador das ameaças mais recentes.

A Kaspersky Lab recomenda verificar os *objetos em quarentena* e os *objetos de inicialização* sempre que o banco de dados for atualizado.

Por que esses objetos devem ser verificados?

A área de quarentena contém objetos que foram sinalizados pelo programa como suspeitos ou possivelmente infectados (consulte a seção 11.1 na p. 119). Usando a versão mais recente das assinaturas de ameaças, talvez o Kaspersky Anti-Virus for Windows Servers possa identificar a ameaça e eliminá-la.

Por padrão, o aplicativo verifica os objetos em quarentena depois de cada atualização das assinaturas de ameaças. Também é recomendável verificar periodicamente os objetos em quarentena porque o status dos mesmos pode mudar após várias verificações. Alguns objetos podem ser então restaurados para os locais anteriores e você poderá continuar trabalhando com eles.

Para desabilitar as verificações de objetos em quarentena, desmarque **Verificar quarentena novamente** na seção **Ação após a atualização**.

Os objetos de inicialização são críticos para a segurança do computador. Se algum deles estiver infectado com um aplicativo mal-intencionado, isso pode provocar uma falha na inicialização do sistema operacional. O Kaspersky Anti-Virus for Windows Servers possui uma tarefa interna de verificação de objetos de inicialização (consulte Capítulo 8 na p. 85). É recomendável configurar uma programação para essa tarefa de forma que ela seja iniciada automaticamente depois de cada atualização das assinaturas de ameaças (consulte 6.5 na p. 66).

CAPÍTULO 11. OPÇÕES AVANÇADAS

O Kaspersky Anti-Virus for Windows Servers possui outros recursos que expandem sua funcionalidade.

O programa coloca alguns objetos em áreas de armazenamento específicas para garantir a proteção máxima dos dados, com o mínimo de perdas.

- O Backup contém cópias de objetos que o Kaspersky Anti-Virus for Windows Servers alterou ou excluiu (consulte 11.2 na p. 122). Se não foi possível recuperar integralmente um objeto que continha informações importantes para você durante o processamento do antivírus, sempre é possível restaurá-lo a partir de sua cópia de backup.
- A Quarentena contém objetos possivelmente infectados que não puderam ser processados usando as assinaturas de ameaças atuais (consulte 11.1 na p. 119).

É recomendável examinar periodicamente a lista de objetos armazenados. Alguns deles já podem estar desatualizados e alguns podem ter sido restaurados.

As opções avançadas incluem diversos recursos úteis. Por exemplo:

- O Suporte Técnico fornece assistência abrangente ao Kaspersky Anti-Virus for Windows Servers (consulte 11.6 na p. 135) A Kaspersky fornece vários canais de suporte, incluindo o suporte on-line e um fórum de perguntas e comentários para usuários dos programas.
- O recurso de Notificações configura as notificações do usuário sobre momentos-chave no Kaspersky Anti-Virus for Windows Servers (consulte 11.8.1 na p. 139). Podem ser eventos de natureza informativa ou sobre erros críticos que devem ser eliminados imediatamente.
- A Autodefesa protege os próprios arquivos do programa contra modificações ou danos provocados por hackers, bloqueia o uso dos recursos do programa pela administração remota e restringe a realização de determinadas ações no Kaspersky Anti-Virus for Windows Servers por indivíduos com direitos de administrador do servidor no computador (consulte 11.8.2 na p. 144). Por exemplo, alterar o nível de proteção pode influir significativamente sobre a segurança das informações no computador.

- O Gerenciador de Chaves de Licença pode obter informações detalhadas sobre a licença usada, ativar sua cópia do programa e gerenciar arquivos de chave de licença (consulte 11.5 na p. 134).

O programa também fornece uma seção de Ajuda (consulte 11.4 na p. 133) e relatórios detalhados (consulte 11.3 na p. 125) sobre a operação do Antivírus de Arquivos e das tarefas de atualização e verificação de vírus.

Você também pode alterar a aparência do Kaspersky Anti-Virus for Windows Servers e personalizar a interface do programa (consulte 11.7 na p. 137).

As seções a seguir abordam estes recursos mais detalhadamente.

11.1. Quarentena de objetos possivelmente infectados

A **Quarentena** é uma área de armazenamento específica que mantém os objetos possivelmente infectados.

Os **objetos possivelmente infectados** são aqueles que se suspeita estarem infectados com vírus ou modificações deles.

Por que *possivelmente infectados*? Por vários motivos, nem sempre é possível determinar se um objeto está infectado:

- O código do objeto verificado se parece com uma ameaça conhecida, mas está parcialmente modificado.

  As assinaturas de ameaças contêm ameaças que já foram estudadas pela Kaspersky Lab. Se um programa mal-intencionado for modificado por um hacker mas essas alterações ainda não tiverem sido inseridas nas assinaturas, o Kaspersky Anti-Virus for Windows Servers classificará o objeto infectado com esse programa mal-intencionado como possivelmente infectado e indicará a ameaça com a qual a infecção se parece.

- O código do objeto detectado se parece, estruturalmente, com um programa mal-intencionado; contudo, não há nada semelhante registrado nas assinaturas de ameaças.

  É bastante possível que se trate de um novo tipo de ameaça, então o Kaspersky Anti-Virus for Windows Servers classifica o objeto como possivelmente infectado.

O analisador de *código heurístico* detecta possíveis vírus. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Um objeto possivelmente infectado pode ser detectado e colocado em quarentena pelo Antivírus de Arquivos ou durante uma verificação de vírus.

Você pode colocar um objeto em quarentena clicando em **Quarentena**, na notificação pop-up que é exibida quando um objeto possivelmente infectado é detectado.

Quando você coloca um objeto na Quarentena, ele é movido, não copiado. O objeto é excluído do disco ou do e-mail e salvo na pasta Quarentena. Os arquivos em Quarentena são salvos em um formato específico e não são perigosos.

11.1.1. Ações sobre objetos em quarentena

O número total de objetos em Quarentena é exibido selecionando o item **Arquivos de dados** na área **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Quarentena* exibe:

- o número de objetos possivelmente infectados detectados durante a operação do Kaspersky Anti-Virus for Windows Servers;
- o tamanho atual da Quarentena.

Você pode excluir todos os objetos da quarentena com o botão **Esvaziar**. Observe que, ao fazê-lo, os arquivos de Backup e de relatório também serão excluídos.

Para acessar os objetos na Quarentena:

clique em qualquer parte da seção **Quarentena**.

As seguintes ações podem ser executadas na guia **Quarentena** (veja a Figura 35):

- Mover para a Quarentena um arquivo que você suspeita estar infectado, mas que o programa não detectou. Para fazê-lo, clique em **Adicionar** e selecione o arquivo na janela de seleção padrão. Ele será adicionado à lista com o status *adicionado pelo usuário*.
- Verificar e desinfectar todos os objetos possivelmente infectados na Quarentena usando as assinaturas de ameaças atuais, clicando em **Verificar tudo**.

  Depois de verificar e desinfectar qualquer objeto em quarentena, seu status pode mudar para *infectado, possivelmente infectado, falso positivo, OK,* etc.

  O status *infectado* significa que o objeto foi identificado como infectado, mas não pôde ser neutralizado. É recomendável excluí-lo.

Todos os objetos marcados como *falso positivo* podem ser restaurados, pois seu status *possivelmente infectado* anterior não foi confirmado pelo programa após nova verificação.

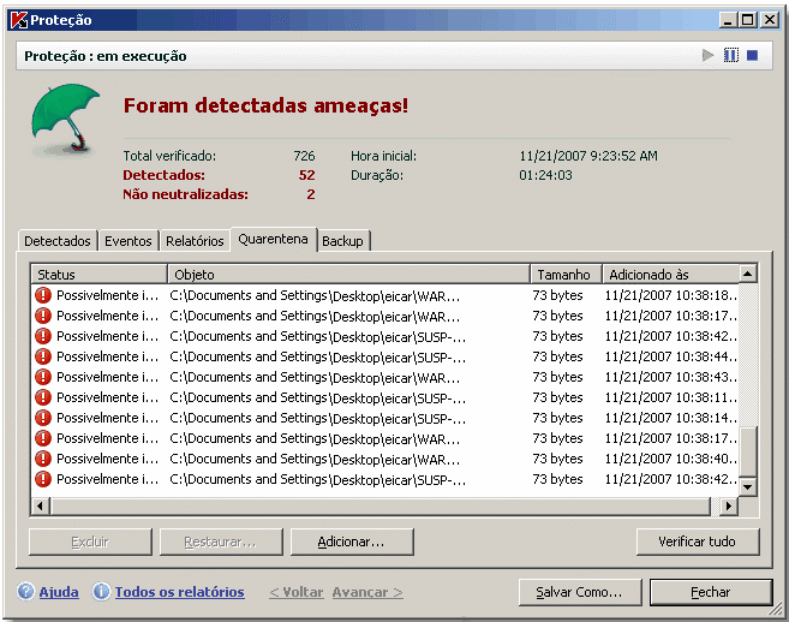


Figura 35. Lista de objetos em quarentena

- Restaurar os arquivos para uma pasta selecionada ou para sua pasta original antes da Quarentena (padrão). Para restaurar um objeto, selecione-o na lista e clique em **Restaurar**. Ao restaurar objetos de arquivos comprimidos, bancos de dados de e-mails e arquivos em formato de e-mail da Quarentena, selecione também o diretório no qual serão restaurados.

> Dica:
>
> É recomendável restaurar apenas objetos com status *falso positivo, OK* e *desinfectado*, pois a restauração de outros objetos pode levar à infecção do computador.

- Excluir todos os objetos ou grupos de objetos selecionados em quarentena. Exclua os objetos apenas se não puderem ser desinfectados. Para excluir os objetos, selecione-os na lista e clique em **Excluir**.

11.1.2. Configurando a Quarentena

Você pode configurar o layout e o funcionamento da Quarentena, mais especificamente:

- Configurar verificações automáticas de objetos em Quarentena após cada atualização das assinaturas de ameaças (para obter mais detalhes, consulte 10.4.4 na p. 115).

  > Aviso!
  >
  > O programa não poderá verificar objetos em quarentena imediatamente após a atualização das assinaturas de ameaças, se você estiver acessando a área de Quarentena.

- Definir o tempo máximo de armazenamento na Quarentena.

  O tempo de armazenamento padrão é de 30 dias e, ao término dele, os objetos são excluídos. Você pode alterar o tempo de armazenamento da Quarentena ou desabilitar totalmente esta restrição.

Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Servers clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Na seção **Quarentena e Backup** (veja a Figura 36), insira o período depois do qual os objetos na Quarentena serão excluídos automaticamente. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

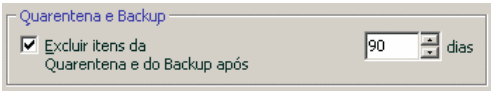


Figura 36. Configurando o período de armazenamento na Quarentena

11.2. Cópias de backup de objetos perigosos

Às vezes, quando os objetos são desinfectados, sua integridade é perdida. Se um arquivo desinfectado contiver informações importantes que foram parcial ou totalmente corrompidas, você pode tentar restaurar o objeto original a partir de uma cópia de backup.

Uma **cópia de backup** é uma cópia do objeto perigoso original criada antes de o objeto ser desinfectado ou excluído. Ela é salva no Backup.

O **Backup** é uma área de armazenamento específica que mantém cópias de backup dos objetos perigosos. Os arquivos no Backup são salvos em um formato específico e não são perigosos.

11.2.1. Ações sobre cópias de backup

O número total de cópias de objetos no Backup é exibido em **Arquivos de dados**, na seção **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Backup* exibe:

- o número de cópias de backup de objetos criados pelo Kaspersky Anti-Virus for Windows Servers
- o tamanho atual do Backup.

Aqui, você pode excluir todas as cópias do Backup com o botão **Esvaziar**. Observe que, ao fazê-lo, os objetos na Quarentena e arquivos de relatório também serão excluídos.

Para acessar as cópias de objetos perigosos:

clique em qualquer parte da seção **Backup**.

Uma lista de cópias de backup será exibida na guia **Backup** (veja a Figura 37). As seguintes informações são exibidas para cada cópia: o nome e o caminho do objeto, o status do objeto atribuído pela verificação e seu tamanho.

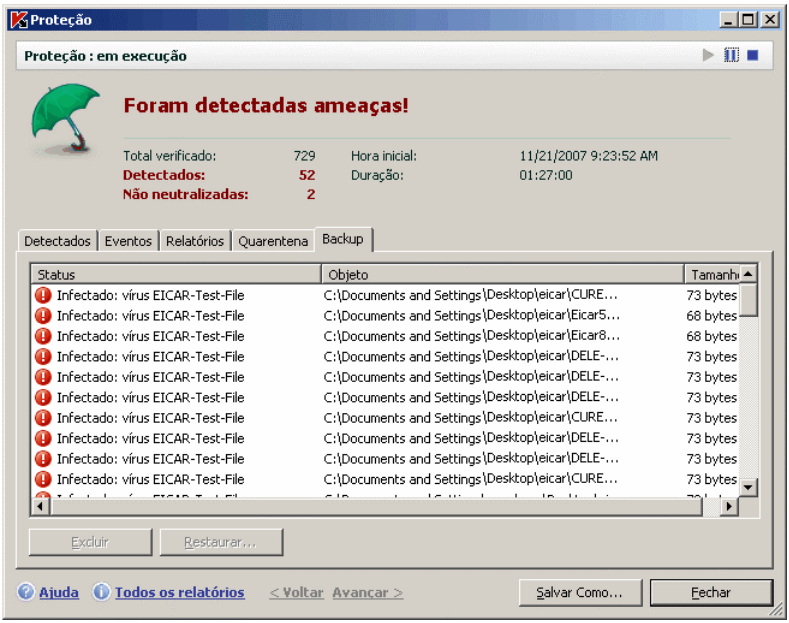


Figura 37. Cópias de backup de objetos excluídos ou desinfectados

Você pode restaurar cópias selecionadas usando o botão **Restaurar**. O objeto é restaurado do Backup com o mesmo nome que tinha antes da desinfecção.

Se houver um objeto com esse nome no local original (isto é possível se foi feita uma cópia do objeto que está sendo restaurado antes da desinfecção), será exibido um aviso. Você pode alterar o local do objeto restaurado ou renomeá-lo.

É recomendável verificar os objetos de backup quanto à presença de vírus imediatamente após sua restauração. É possível que, com as assinaturas atualizadas, você consiga desinfectá-lo sem perder a integridade do arquivo.

É recomendável **não** restaurar cópias de backup de objetos, exceto quando absolutamente necessário. Isto pode levar à infecção do computador.

É recomendável examinar a área de Backup e esvaziá-la usando o botão **Excluir** periodicamente. Você também pode configurar o programa de modo a excluir automaticamente as cópias mais antigas de Backup (consulte a seção 11.2.2 na p. 125).

11.2.2. Configurando o Backup

Você pode definir o tempo máximo que as cópias permanecem na área de Backup.

O tempo de armazenamento padrão do Backup é 90 dias e, ao término dele, as cópias são excluídas. Você pode alterar o tempo de armazenamento ou remover totalmente esta restrição. Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Servers clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Defina a duração do armazenamento de cópias de backup no repositório na seção **Quarentena e Backup** (veja a Figura 36) à direita da tela. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

11.3. Relatórios

O Antivírus de Arquivos, as tarefas de verificação de vírus e as atualizações são registradas em relatórios.

O número total de relatórios criados pelo programa e seu tamanho total são exibidos clicando em **Arquivos de dados**, na seção **Serviço** da janela principal do programa. As informações são exibidas na caixa *Relatórios*.

Para exibir relatórios:

Clique em qualquer local da caixa *Relatórios* para abrir a janela Proteção, que resume a proteção fornecida pelo aplicativo. Será aberta uma janela na guia **Relatórios** (veja a Figura 38).

A guia Relatórios lista os relatórios mais recentes do Antivírus de Arquivos e das tarefas de atualização e verificação de vírus executadas nesta sessão do Kaspersky Anti-Virus for Windows Servers. O status é mostrado ao lado do Antivírus de Arquivos ou da tarefa, por exemplo, *interrompido* ou *concluído*. Se desejar exibir o histórico completo da criação do relatório da sessão atual do programa, marque ☑ **Mostrar histórico de relatórios**.

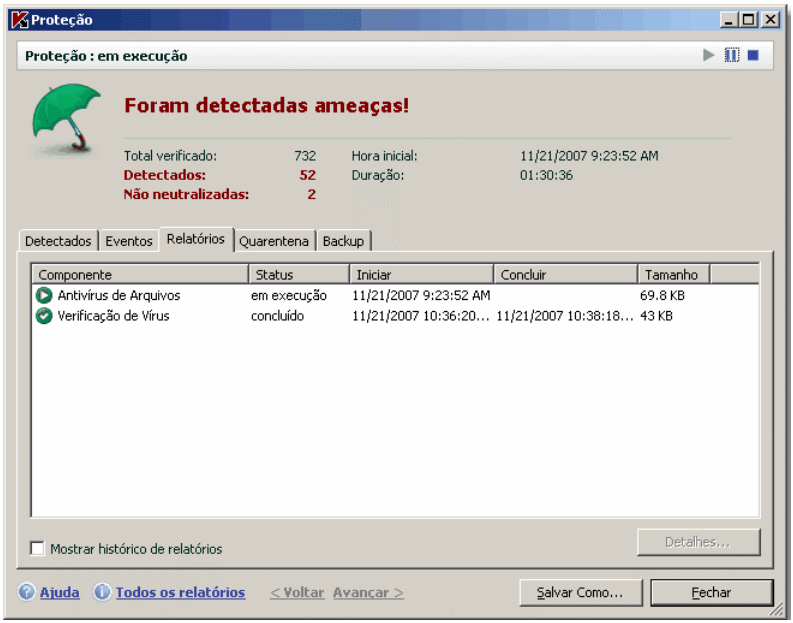


Figura 38. Relatórios de funcionamento do componente

Para analisar todos os eventos registrados para o Antivírus de Arquivos ou uma tarefa:

Selecione Antivírus de Arquivos ou a tarefa na guia **Relatórios** e clique no botão **Detalhes**.

Uma janela será aberta, contendo informações detalhadas sobre o desempenho do Antivírus de Arquivos ou da tarefa. As estatísticas de desempenho resultantes são exibidas na parte superior da janela e informações detalhadas são fornecidas nas guias.

- A guia **Detectados** contém uma lista de objetos perigosos detectados pelo Antivírus de Arquivos ou por uma tarefa de verificação de vírus executada.
- A guia **Eventos** exibe os eventos do Antivírus de Arquivos ou da tarefa.
- A guia **Estatísticas** contém estatísticas detalhadas de todos os objetos verificados.
- A guia **Configurações** exibe as configurações usadas pelo Antivírus de Arquivos, verificações de vírus ou atualizações de assinaturas de ameaças.

- A guia **Usuários banidos** exibe uma lista de usuários cujos computadores foram banidos ao tentar copiar um arquivo infectado ou possivelmente infectado para o servidor.

Você pode exportar todo o relatório como um arquivo de texto. Este recurso é útil quando ocorre um erro no Antivírus de Arquivos que você não consegue eliminar sozinho e você precisa de assistência do Suporte Técnico. Se isso acontecer, o relatório deve ser enviado como um arquivo .txt para o Suporte Técnico, para que nossos especialistas possam estudar o problema detalhadamente e solucioná-lo assim que possível.

Para exportar um relatório como arquivo de texto:

Clique em **Salvar como** e especifique o local onde deseja salvar o arquivo do relatório.

Depois de terminar o trabalho com o relatório, clique em **Fechar**.

Existe um botão Ações em todas as guias (exceto em **Configurações** e **Estatísticas**) que você pode usar para definir respostas aos objetos na lista. Ao clicar nele, um menu de contexto é aberto, com uma seleção dos seguintes itens de menu (i menu é diferente dependendo do componente; todas as opções possíveis estão relacionadas a seguir):

Desinfectar – tenta desinfectar um objeto perigoso. Se o objeto não for desinfectado com êxito, você pode deixá-lo nesta lista para que seja verificado posteriormente com assinaturas de ameaças atualizadas ou excluí-lo. Você pode aplicar esta ação a um único objeto na lista ou a vários objetos selecionados.

Descartar – exclui o registro de detecção do objeto do relatório.

Adicionar à zona confiável – exclui o objeto da proteção. Será aberta uma janela com uma regra de exclusão para o objeto.

Ir para o arquivo – abre a pasta na qual o objeto está localizado no Windows Explorer.

Desinfectar tudo – neutraliza todos os objetos da lista. O Kaspersky Anti-Virus for Windows Servers tentará processar os objetos usando as assinaturas de ameaças.

Descartar tudo – limpa o relatório sobre objetos detectados. Ao usar esta função, todos os objetos perigosos detectados permanecem no computador.

Pesquisar www.viruslist.com – vai para uma descrição do objeto na Enciclopédia de Vírus no site da Kaspersky Lab.

Pesquisar www.google.com – localiza informações sobre o objeto usando este mecanismo de pesquisa.

Pesquisar – insere termos de pesquisa para objetos da lista, por nome ou status.

Além disso, você pode classificar as informações exibidas na janela em ordem crescente e decrescente, para cada coluna, clicando no cabeçalho da coluna.

Os objetos perigosos detectados pelo Kaspersky Anti-Virus são processados usando o botão **Desinfectar** (para um objeto ou grupo de objetos selecionados) ou **Desinfectar tudo** (para processar todos os objetos da lista). Ao processar cada objeto, será exibida uma notificação na tela, na qual você decide as ações que serão tomadas a seguir.

Se você marcar **Aplicar a todos** na janela de notificação, a ação selecionada será aplicada a todos os objetos com o status selecionado na lista, antes de iniciar o processamento.

11.3.1. Configurando relatórios

Para configurar a criação e a forma como os relatórios são salvos:

Abra a janela de configurações do Kaspersky Anti-Virus for Windows Servers clicando em Configurações na janela principal do programa.

1. Selecione **Arquivos de dados** na árvore de configurações.
2. Edite as configurações na caixa **Relatórios** (veja a Figura 39) da seguinte maneira:
   - Permita ou desabilite o registro de eventos informativos. Geralmente, estes eventos não são importantes para a segurança. Para registrar os eventos, marque **Registrar eventos não críticos**.
   - Escolha relatar apenas os eventos que ocorreram desde a última vez que a tarefa foi executada. Isto economiza espaço em disco por reduzir o tamanho do relatório. Se **Manter apenas eventos recentes** estiver marcado, o relatório será iniciado do zero sempre que você reiniciar a tarefa. Entretanto, apenas as informações não críticas serão substituídas.
   - Defina o tempo de armazenamento dos relatórios. Por padrão, o tempo de armazenamento de relatórios é de 90 dias e, ao término dele, os relatórios são excluídos. Você pode alterar o tempo máximo de armazenamento ou remover totalmente esta restrição.

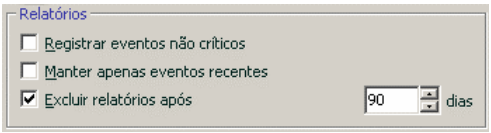


Figura 39. Configurando relatórios

11.3.2. A guia *Detectados*

Esta guia (veja a Figura 40) contém uma lista de objetos perigosos detectados pelo Kaspersky Anti-Virus for Windows Servers. O caminho e o nome completo de cada objeto são mostrados, com o status atribuído a ele pelo programa na sua verificação ou processamento.

Se desejar que a lista contenha os objetos perigosos e os objetos neutralizados com êxito, marque ☑ **Mostrar objetos neutralizados**.

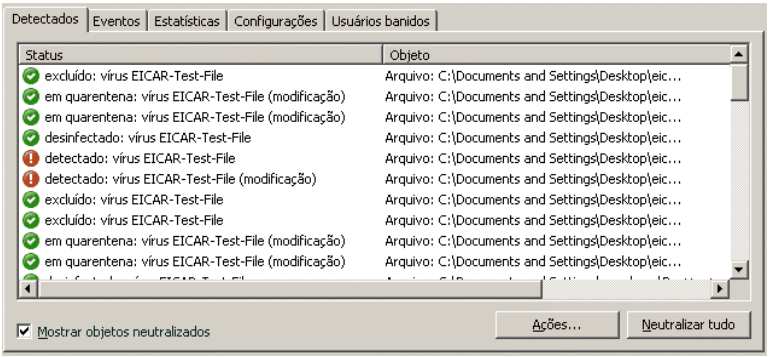


Figura 40. Lista de objetos perigosos detectados

Os objetos perigosos detectados pelo Kaspersky Anti-Virus são processados usando o botão **Neutralizar** (para um objeto ou grupo de objetos selecionados) ou **Neutralizar tudo** (para processar todos os objetos da lista). Ao processar cada objeto, será exibida uma notificação na tela, na qual você decide as ações que serão tomadas a seguir.

Se você marcar ☑ **Aplicar a todos** na janela de notificação, a ação selecionada será aplicada a todos os objetos com o status selecionado na lista, antes de iniciar o processamento.

11.3.3. A guia *Eventos*

Esta guia (veja a Figura 41) fornece uma lista completa de todos os eventos importantes no funcionamento do Antivírus de Arquivos, verificações de vírus e atualizações de assinaturas de ameaças.

Estes eventos podem ser:

Eventos críticos são aqueles de importância crítica que indicam problemas na operação do programa ou vulnerabilidades do seu computador. Por exemplo, *vírus detectado*, *erro de funcionamento*.

Eventos importantes são aqueles que devem ser investigados, pois refletem situações importantes no funcionamento do programa. Por exemplo, *interrompido*.

Mensagens informativas são mensagens do tipo de referência, que geralmente não contêm informações importantes. Por exemplo, *OK, não processado*. Esse eventos serão exibidos no log de eventos somente se **Mostrar todos os eventos** estiver marcado.

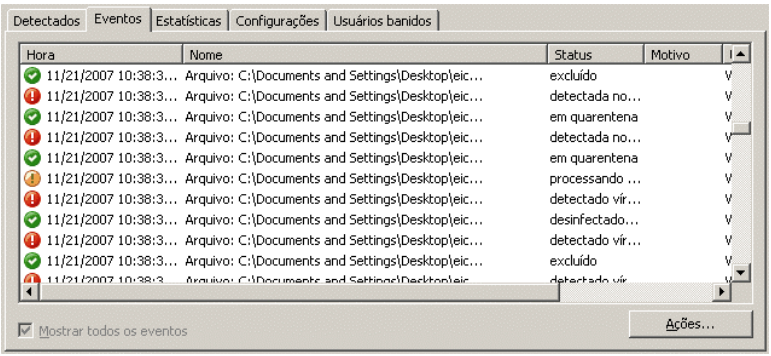


Figura 41. Eventos processados pelo componente.

O formato para exibição de eventos no log de eventos pode variar de acordo com o componente ou tarefa. Para tarefas de atualização, são fornecidas as seguintes informações:

- Nome do evento
- Nome do objeto envolvido no evento
- Hora em que o evento ocorreu
- Tamanho do arquivo carregado

Para tarefas de verificação de vírus, o log de eventos contém o nome do objeto verificado e o status atribuído a ele pela verificação/processamento.

11.3.4. A guia Estatísticas

Esta guia (veja a Figura 42) fornece estatísticas detalhadas sobre o Antivírus de Arquivos e tarefas de verificação de vírus. Aqui, você pode descobrir:

- Quantos objetos foram verificados quanto a indícios perigosos nesta sessão do Antivírus de Arquivos ou após a conclusão de uma tarefa. É exibido o número de arquivos comprimidos, arquivos compactados e arquivos protegidos por senha verificados, e de objetos corrompidos.
- Quantos objetos perigosos foram detectados, não desinfectados, excluídos e colocados em Quarentena.

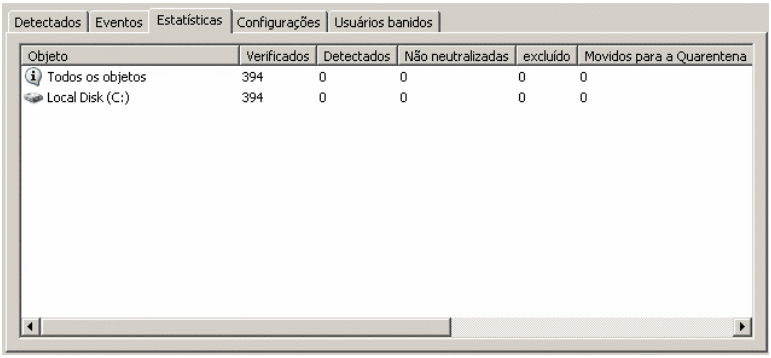


Figura 42. Estatísticas do componente

11.3.5. A guia Configurações

A guia **Configurações** (veja a Figura 43) exibe uma visão geral completa das configurações do Antivírus de Arquivos, verificações de vírus e atualizações do programa. Você pode descobrir o nível de segurança atual do Antivírus de Arquivos ou da verificação de vírus, quais ações são executadas com relação a objetos perigosos ou quais configurações são usadas para as atualizações do programa. Use o link Alterar configurações para configurar o componente.

Você pode definir configurações avançadas para verificações de vírus:

- Estabeleça a prioridade das tarefas de verificação usadas, se o processador estiver sobrecarregado. Por padrão, a caixa ☑ **Conceder recursos a outros aplicativos** está marcada. Com este recurso, o programa controla a carga nos subsistemas do processador e do disco, de acordo com a atividade de outros aplicativos. Se a carga do processador aumentar de forma significativa e impedir a operação normal dos aplicativos do usuário, o programa reduzirá a atividade de

verificação. Isto aumenta o tempo de verificação e libera os recursos para os aplicativos do usuário.

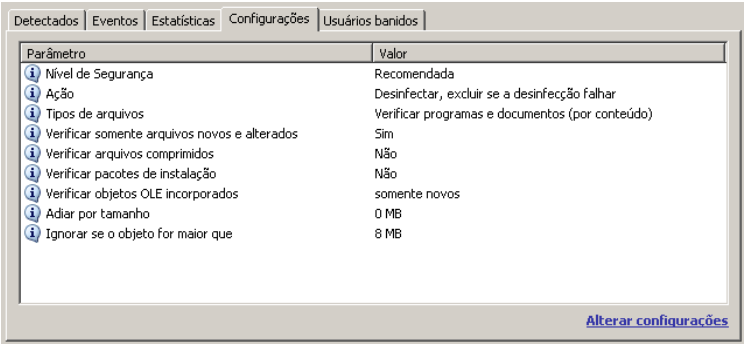


Figura 43. Configurações do componente

- Defina o modo de operação do computador após a conclusão de uma verificação de vírus. Você pode configurar o computador para desligar, reiniciar ou entrar em modo em espera ou em suspensão. Para selecionar uma opção, clique no link até a opção desejada ser exibida.

11.3.6. A guia *Usuários banidos*

(veja a Figura 44). Todos os computadores que tentaram copiar um arquivo infectado ou possivelmente infectado para o servidor são bloqueados. Banir um computador também pode se aplicar às ações relacionadas com o processamento do arquivo (desinfecção ou exclusão).

Esta guia informa quais computadores foram banidos, junto com a data e a hora em que isso ocorreu e quantas horas faltam para que isso seja cancelado.

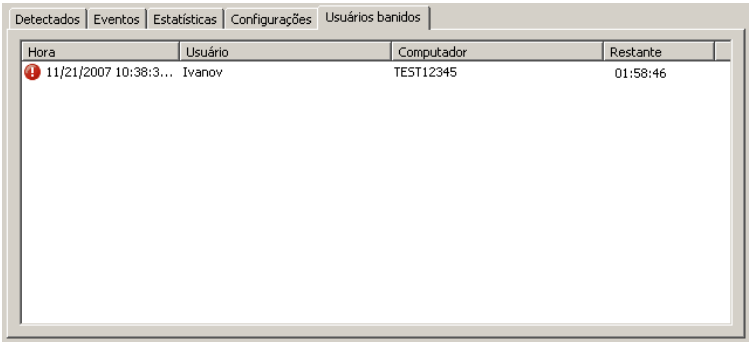


Figura 44. Lista de usuários banidos

11.4. Informações gerais sobre o programa

Você pode exibir informações gerais sobre o programa na seção **Serviço** da janela principal (veja a Figura 45).

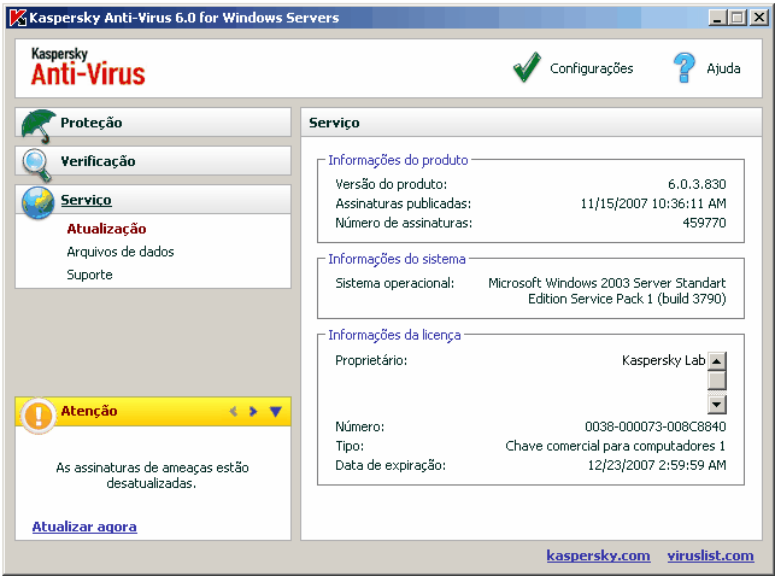


Figura 45. Informações sobre o programa, a licença e o sistema em que está instalado

Todas as informações estão divididas em três seções:

- A versão do programa, a data da última atualização e o número de ameaças conhecidas até o momento são exibidos na caixa **Informações do produto**.
- As informações básicas sobre o sistema operacional instalado no computador são mostradas na caixa **Informações do sistema**.
- Informações básicas sobre a licença do Kaspersky Anti-Virus que você comprou estão na caixa **Informações da licença**.

Você precisará de todas essas informações quando entrar em contato com o Suporte Técnico da Kaspersky Lab (consulte 11.6 na p. 135).

11.5. Gerenciando licenças

O Kaspersky Anti-Virus for Windows Servers precisa de uma *chave de licença* para funcionar. Você recebe uma chave ao adquirir o programa. Ela lhe concede o direito de usar o programa a partir do dia em quem instala a chave.

Sem uma chave de licença, a menos que uma versão de teste do aplicativo tenha sido ativada, o Kaspersky Anti-Virus será executado no modo de uma atualização. O programa não baixará novas atualizações.

Se uma versão de teste do programa tiver sido ativada, depois de expirado o período de teste, o Kaspersky Anti-Virus não será executado.

Quando a chave de licença comercial expirar, o programa continuará funcionando, exceto pelo fato de você não poder atualizar as assinaturas de ameaças. Como antes, você poderá verificar seu computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com as assinaturas de ameaças que você tinha antes de a licença expirar. Não podemos garantir que você estará protegido contra os vírus que surgirem depois que a licença do programa expirar.

Para evitar infectar o computador com novos vírus, é recomendável estender a licença do Kaspersky Anti-Virus for Windows Servers. O programa o notificará duas semanas antes da expiração da licença e, durante essas semanas, essa mensagem será exibida sempre que for aberto.

Para renovar a licença, compre e instale uma nova chave de licença ou digite o código de ativação do aplicativo. Para fazê-lo:

Entre em contato com o fornecedor do produto e adquira uma chave de licença ou um código do aplicativo.

ou:

Adquira uma chave de licença ou um código de ativação diretamente da Kaspersky Lab, clicando no link Comprar licença na janela da chave de licença (veja a Figura 46). Preencha o formulário no site. Depois que o pagamento for feito, será enviado um link para o e-mail que você inseriu no formulário de pedido. Esse link permitirá que você baixe uma chave de licença do aplicativo ou obtenha um código de ativação.

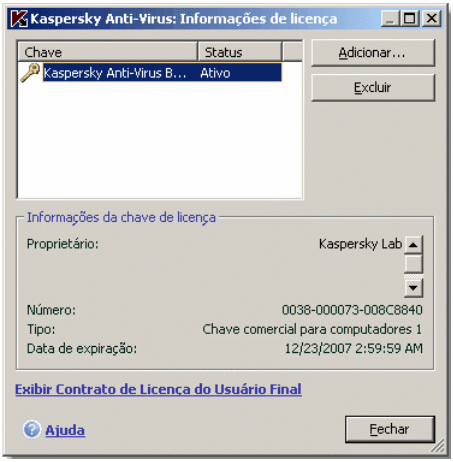


Figura 46. Informações da licença

Periodicamente, a Kaspersky Lab lança ofertas de extensões de licença de nossos produtos. Verifique as ofertas no site da Kaspersky Lab, em **Products → Sales and special offers**.

Informações sobre a chave de licença usada estão disponíveis na caixa **Informações de licença** na seção **Serviço** na janela principal do programa. Para abrir a janela do gerenciador de licenças, clique em qualquer local da caixa. Na janela que é aberta (veja a Figura 46), você pode ver informações sobre a chave atual, adicionar ou excluir uma chave.

Ao selecionar uma chave na lista da caixa **Informações de licença**, serão exibidas informações sobre o número, o tipo e a data de expiração da licença. Para adicionar uma nova chave de licença, clique em **Adicionar** e ative o aplicativo usando o assistente de ativação (consulte 11.5 na p. (consulte a seção 11.6 na p. 135)). Para excluir uma chave da lista, use o botão **Excluir**.

Para examinar os termos do EULA, clique em Exibir Contrato de Licença do Usuário Final. Para adquirir uma licença através do formulário no site da Kaspersky Lab, clique em Comprar licença.

11.6. Suporte Técnico

O Kaspersky Anti-Virus for Windows Servers fornece uma grande variedade de opções para dúvidas e problemas relacionados com o funcionamento do programa. Elas estão localizadas em **Suporte** (veja a Figura 47), na seção **Serviço**.

Dependendo do problema, fornecemos vários serviços de suporte técnico:

Fórum de usuários. Este recurso é uma seção dedicada do site da Kaspersky Lab com perguntas, comentários e sugestões de usuários do programa. Você pode examinar os tópicos básicos do fórum e deixar um comentário. Talvez também encontre a resposta para sua pergunta.

Para acessar este recurso, use o link Fórum de usuários.

Base de dados de conhecimento. Este recurso também é uma seção dedicada do site da Kaspersky Lab e contém recomendações de Suporte Técnico para o uso do software da Kaspersky Lab e respostas para perguntas freqüentes. Tente encontrar uma resposta para sua pergunta ou uma solução para seu problema com este recurso.

Para obter suporte técnico on-line, clique no link Base de dados de conhecimento.

Comentários sobre a operação do programa. Este serviço foi criado para postar comentários sobre o funcionamento do programa ou descrever um problema que apareceu durante sua operação. É necessário preencher um formulário específico no site da empresa, descrevendo a situação detalhadamente. Para lidar com o problema da melhor forma, a Kaspersky Lab precisará de algumas informações sobre o sistema. Você pode descrever a configuração do sistema sozinho ou usar o coletor de informações automático no seu computador.

Para ir para o formulário de comentários, use o link Enviar um relatório de erro ou uma sugestão.

Suporte técnico. Se você precisar de ajuda ao usar o Kaspersky Anti-Virus, clique no link localizado na caixa **Serviço de Suporte Local**. O site da Kaspersky Lab será aberto com informações sobre como contatar nossos especialistas.

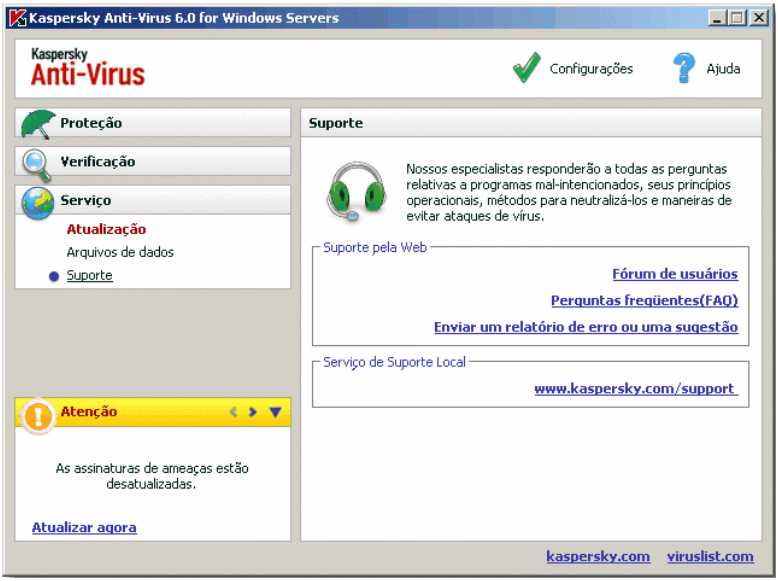


Figura 47. Informações sobre o suporte técnico

11.7. Configurando a interface do Kaspersky Anti-Virus for Windows Servers

O Kaspersky Anti-Virus for Windows Servers lhe dá a opção de alterar a aparência do programa, criando e usando capas. Você também pode configurar o uso dos elementos de interface ativos, como o ícone da bandeja do sistema e as mensagens pop-up.

Para configurar a interface do programa, execute as seguintes etapas:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Servers clicando no link Configurações na janela principal.
2. Selecione **Aparência** na seção **Serviço** da árvore de configurações do programa (veja a Figura 48).

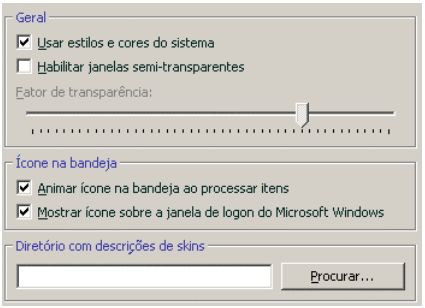


Figura 48. Configurando a aparência do programa

À direita da janela de configurações, você pode determinar:

- Se o indicador de proteção do Kaspersky Anti-Virus for Windows Servers será exibido quando o sistema operacional for iniciado.

  Por padrão, esse indicador aparece no canto superior direito da tela quando o programa é carregado. Ele informa se o computador está protegido de todos os tipos de ameaça. Se não desejar usar o indicador de proteção, desmarque **Mostrar ícone sobre a janela de logon do Microsoft Windows**.

- Se a animação será usada no ícone da bandeja do sistema.

  Dependendo da operação do programa realizada, o ícone da bandeja do sistema muda. Por padrão, a animação do ícone está ativada. Se desejar desativar a animação, desmarque **Animar ícone na bandeja ao processar itens**. Em seguida, o ícone indicará apenas o status de proteção do computador. Se a proteção estiver habilitada, o ícone ficará colorido e, se a proteção for pausada ou desabilitada, o ícone ficará cinza.

- Grau de transparência das mensagens pop-up.

  Todas as operações do Kaspersky Anti-Virus for Windows Servers que devem ser informadas a você imediatamente ou que exigem que você tome uma decisão são apresentadas como mensagens pop-up acima do ícone da bandeja do sistema. As janelas de mensagem são transparentes, de modo a não interferir nas outras operações. Se você mover o cursor sobre a mensagem, a transparência desaparecerá. Você pode alterar o grau de transparência dessas mensagens. Para fazê-lo, ajuste a escala do **Fator de transparência** para a posição desejada. Para remover a transparência da mensagem, desmarque **Habilitar janelas semi-transparentes**.

- Use suas próprias capas para a interface do programa.

Todas as cores, fontes, ícones e textos usados na interface do Kaspersky Anti-Virus for Windows Servers podem ser alterados. Você pode criar seus próprios elementos gráficos para o programa ou localizá-los em outro idioma. Para usar uma capa, especifique o diretório com suas configurações no campo **Diretório com descrições de capas**. Use o botão **Procurar** para selecionar o diretório.

Por padrão, as cores e estilos do sistema são usados na capa do programa. Você pode removê-los, desmarcando ☑ **Usar estilos e cores do sistema**. Então, os estilos especificados nas configurações do tema da tela serão usados.

Observe que as alterações das configurações da interface do Kaspersky Anti-Virus não serão salvas se você restaurar as configurações de operação padrão ou desinstalar o programa.

11.8. Usando opções avançadas

O Kaspersky Anti-Virus for Windows Servers fornece os seguintes recursos avançados:

- Notificações sobre determinados eventos que ocorrem no programa.
- Autodefesa do Kaspersky Anti-Virus for Windows Servers contra a desabilitação, exclusão ou edição de módulos, além da proteção do programa por senha.
- Resolução de conflitos entre o Kaspersky Anti-Virus e outros programas.

Para configurar estes recursos:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.

À direita da tela, você pode definir se vai ou não usar os recursos adicionais na operação do programa.

11.8.1. Notificações de eventos do Kaspersky Anti-Virus for Windows Servers

Vários tipos de eventos ocorrem no Kaspersky Anti-Virus for Windows Servers. Eles podem ser de natureza informativa ou conter informações importantes. Por

exemplo, um evento pode informá-lo de que o programa foi atualizado com êxito ou registrar um erro em um componente que deve ser eliminado imediatamente.

Para receber atualizações sobre o funcionamento do Kaspersky Anti-Virus for Windows Servers, você pode usar o recurso de notificação.

Os avisos podem ser entregues de várias formas:

- Mensagens pop-up acima do ícone de programa, na bandeja do sistema
- Mensagens sonoras
- E-mails
- Registrar evento

Para usar este recurso:

1. Marque **Habilitar notificações** na caixa **Interação com o usuário** (veja a Figura 49).

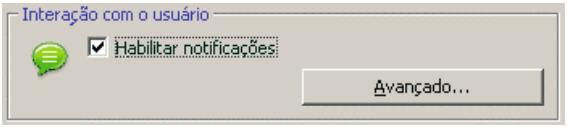


Figura 49. Habilitando notificações

2. Defina os tipos de eventos do Kaspersky Anti-Virus for Windows Servers sobre os quais você deseja ser notificado e o método de entrega das notificações (consulte a seção 11.8.1.1 na p. 140).
3. Configure a entrega de notificações por e-mail, se esse for o método de notificação usado (consulte a seção 11.8.1.2 na p. 142).

11.8.1.1. Tipos de eventos e métodos de entrega de notificações

Durante o funcionamento do Kaspersky Anti-Virus for Windows Servers, ocorrem os seguintes tipos de eventos:

Notificações críticas envolvem eventos de importância crítica. As notificações são altamente recomendadas, pois indicam problemas no funcionamento do programa ou vulnerabilidades do computador. Por exemplo, *assinaturas de ameaças corrompidas* ou *licença expirada*.

Falha funcional – eventos que levam ao não funcionamento do aplicativo. Por exemplo, quando não existe uma licença ou assinaturas de ameaças.

Notificações importantes são eventos que devem ser investigados, pois refletem situações importantes no funcionamento do programa. Por exemplo, *proteção desabilitada* ou *não é feita uma verificação de vírus no computador há muito tempo*.

Notificações sem importância são mensagens de referência que, em geral, não contêm informações importantes. Por exemplo, *todos os objetos perigosos foram desinfectados*.

Para especificar quais eventos o programa deve notificar e de que forma:

1. Clique no link Configurações na janela principal do programa.
2. Na janela de configurações do programa, selecione **Serviço**, marque ☑ **Habilitar notificações** e edite as configurações detalhadas, clicando no botão **Configurações**.

Você pode configurar os seguintes métodos de notificação dos eventos listados acima, na janela **Configurações de notificação** que é aberta (veja a Figura 50):

- *Mensagens pop-up* acima do ícone de programa, na bandeja do sistema, que contêm uma mensagem informativa sobre o evento que ocorreu.

  Para usar esse tipo de notificação, marque ☑ na seção **Balão** para o evento sobre o qual você deseja ser informado.

- *Notificação sonora*

  Se desejar que este aviso seja acompanhado de um som, marque ☑ **Som** para o evento.

- *Notificação por e-mail*

  Para usar este tipo de aviso, marque a coluna ☑ **E-mail** para o evento sobre o qual você deseja ser informado e defina as configurações para o envio de avisos (consulte 11.8.1.2 na p. 142).

- *Registrar evento*

  Para registrar informações sobre qualquer evento que ocorra no log, marque a caixa ☑ para ele no diagrama **registrar** e configure o log de eventos (consulte a seção 11.8.1.3 na p. 143).

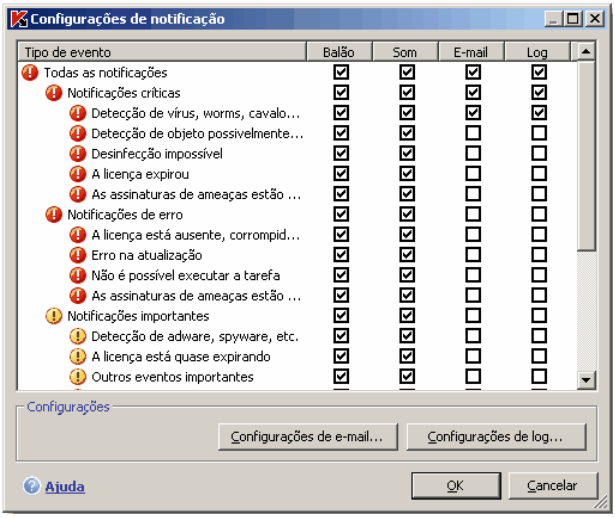


Figura 50. Eventos do programa e métodos de notificação de eventos

11.8.1.2. Configurando a notificação por e-mail

Depois de selecionar os eventos (consulte a seção 11.8.1.1 na p. 140) sobre os quais você deseja receber notificações por e-mail, configure a entrega de notificações. Para fazê-lo:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na seção **Interação com o usuário**, à direita da tela.
4. Na guia **Configurações de notificação**, marque a caixa de seleção ☑ no gráfico de **E-mail** para os eventos que devem acionar uma mensagem de e-mail.
5. Na janela que é aberta ao clicar em **Configurações de e-mail**, configure o seguinte para o envio de notificações por e-mail:
    - Atribua a configuração de notificação de envio para **De: endereço de e-mail**.

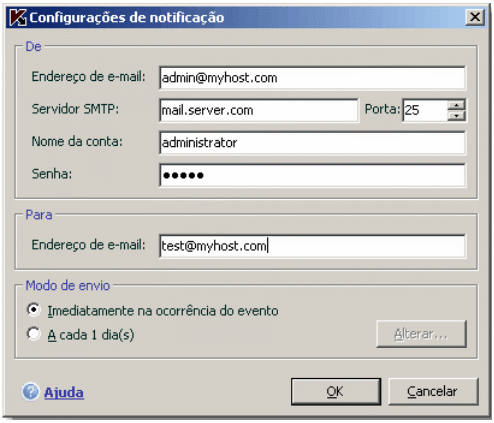


Figura 51. Configurando a notificação por e-mail

- Especifique o endereço de e-mail para o qual os avisos serão enviados em **Para: endereço de e-mail**.
- Atribua um método de entrega de notificações por e-mail em **Modo de envio**. Se desejar que o programa envie um e-mail assim que o evento ocorrer, selecione **Imediatamente na ocorrência do evento**. Para notificações sobre eventos após de um determinado período, preencha a programação de envio de e-mails informativos clicando em **Alterar**. Notificações diárias são o padrão.

11.8.1.3. Configurando o log de eventos

Para configurar o log de eventos:

1. Abra a janela de configuração do aplicativo com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na seção **Interação com o usuário**, à direita da tela.

Na janela **Configurações de notificação**, selecione a opção de registrar informações de um evento e clique no botão **Configurações de log**.

O Kaspersky Anti-Virus permite registrar informações sobre eventos ocorridos durante a execução do programa, no log de eventos geral do MS Windows (**Aplicativo**) ou em um log de eventos dedicado do Kaspersky Anti-Virus (**Log de Eventos Kaspersky**).

Os logs podem ser exibidos em **Visualizar Eventos** do Microsoft Windows, que pode ser aberto em **Iniciar** → **Configurações** → **Painel de Controle** → **Ferramentas Administrativas** → **Visualizar Eventos**.

11.8.2. Autodefesa e restrição de acesso

O Kaspersky Anti-Virus for Windows Servers garante a segurança do computador contra programas mal-intencionados e, por isso, ele próprio pode ser alvo de programas mal-intencionados que tentam bloqueá-lo ou excluí-lo do computador.

Além disso, várias pessoas, com níveis diferentes de experiência em informática, podem usar um computador. Permitir o acesso ao programa e suas configurações pode diminuir bastante a segurança do computador como um todo.

Para assegurar a estabilidade do sistema de segurança do computador, os mecanismos de Autodefesa, defesa contra acesso remoto e proteção por senha foram adicionados ao programa.

Para habilitar a Autodefesa:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.

Defina as seguintes configurações na caixa **Autodefesa** (veja a Figura 52):

- **Habilitar Autodefesa**. Se esta caixa estiver marcada, o programa protegerá seus próprios arquivos, processos na memória e entradas no registro do sistema contra exclusão e modificação.
- **Desabilitar controle de serviço externo**. Se esta caixa estiver marcada, qualquer programa de administração remota que tentar usar o programa será bloqueado.

Se houver alguma tentativa de executar as ações relacionadas, aparecerá uma mensagem sobre o ícone do programa na bandeja do sistema (a menos que o usuário tenha desabilitado as notificações).

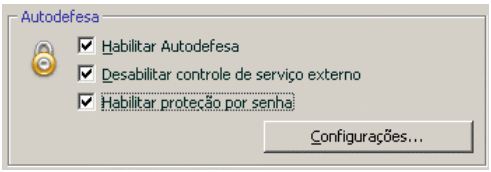


Figura 52. Configuração da defesa do programa

Para proteger o programa por senha, marque **Habilitar proteção por senha**. Clique no botão **Configurações** para abrir a janela **Proteção por senha** e insira a senha e a área a ser coberta pela restrição de acesso (veja a Figura 53).

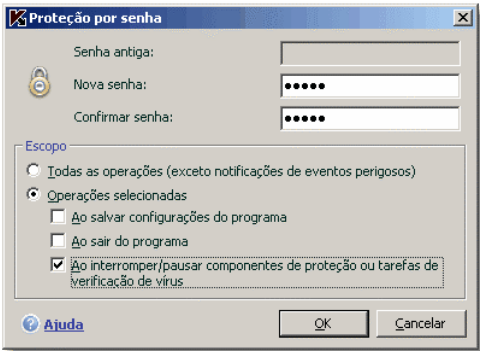


Figura 53. Configurações de proteção do programa por senha

Você pode bloquear todas as operações do programa, exceto notificações de detecção de objetos perigosos, ou evitar que qualquer das seguintes ações sejam executadas:

- Alterar as configurações de desempenho do programa
- Fechar o Kaspersky Anti-Virus for Windows Servers
- Desabilitar ou pausar a proteção do computador

Cada uma dessas ações diminui o nível de proteção do computador; assim, estabeleça quem poderá trabalhar no servidor.

Agora, sempre que um usuário tentar executar as ações no servidor selecionado, o programa solicitará uma senha.

11.8.3. Resolvendo conflitos com outros aplicativos

Em alguns casos, o Kaspersky Anti-Virus pode causar conflitos com outros aplicativos instalados em um computador. Isso ocorre porque esses programas possuem mecanismos de autodefesa internos que são ativados quando o Kaspersky Anti-Virus tenta inspecioná-los. Esses aplicativos incluem o plug-in do Authentica para Acrobat Reader, que verifica o acesso a arquivos .pdf, o Oxygen Phone Manager II e alguns jogos que possuem ferramentas de gerenciamento de direitos digitais.

Para corrigir este problema, marque ☑ **Modo de compatibilidade para programas que usam métodos de autoproteção** na seção **Serviço** da janela de configurações do aplicativo. Reinicie o sistema operacional para que esta alteração tenha efeito.

11.9. Importando e exportando as configurações do Kaspersky Anti-Virus for Windows Servers

O Kaspersky Anti-Virus for Windows Servers permite que você importe e exporte suas configurações.

As configurações são salvas em um arquivo de configuração específico.

Para exportar as configurações atuais do programa:

1. Abra a janela principal do Kaspersky Anti-Virus for Windows Servers.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Salvar** na seção **Gerenciador de configurações**.
4. Insira um nome para o arquivo de configuração e selecione um destino para salvá-lo.

Para importar configurações de um arquivo de configuração:

1. Abra a janela principal do Kaspersky Anti-Virus for Windows Servers.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Carregar** e selecione o arquivo do qual deseja importar configurações do Kaspersky Anti-Virus for Windows Servers.

11.10. Redefinindo as configurações padrão

Sempre é possível retornar às configurações padrão do programa, que são consideradas ideais e recomendadas pela Kaspersky Lab. Isso pode ser feito usando o Assistente para Instalação.

Para redefinir as configurações de proteção:

1. Selecione a seção **Serviço** e clique em Configurações para ir para a janela de configurações do programa.

2. Clique no botão **Redefinir** na seção **Gerenciador de configurações**.

A janela que é aberta solicita que você defina as configurações que devem ser restauradas para seus valores padrão.

Por padrão, o programa salva todas as configurações personalizadas na lista (elas estão desmarcadas). Se você não precisar salvar uma das configurações, marque a caixa correspondente.

Depois de concluir a configuração, clique no botão **Avançar** (consulte a seção 3.2 na p. 27). O Assistente para Instalação será aberto. Siga suas instruções.

Depois de concluir o Assistente para Instalação, o nível de segurança **Recomendado** será definido para o Antivírus de Arquivos, exceto pelas configurações que você decidiu manter. Além disso, as configurações feitas no Assistente para Instalação também serão aplicadas.

CAPÍTULO 12. ADMINISTRANDO O PROGRAMA COM O KASPERSKY ADMINISTRATION KIT

O **Kaspersky Administration Kit** é um sistema para gerenciar centralmente as principais tarefas administrativas na operação do sistema de segurança de uma rede corporativa, com base nos aplicativos incluídos no Kaspersky Anti-Virus Business Optimal e no Kaspersky Corporate Suite.

O Kaspersky Anti-Virus 6.0 for Windows Servers é um dos produtos da Kaspersky Lab que pode ser administrado de sua própria interface, da linha de comando (esses métodos estão descritos acima, nesta documentação) ou usando o Kaspersky Administration Kit (se o computador fizer parte de um sistema de administração remota centralizada).

Execute as seguintes etapas para gerenciar o Kaspersky Anti-Virus 6.0 for Windows Servers usando o Kaspersky Administration Kit:

- Implemente o *Servidor de Administração* na rede; instale o *Console de Administração* no local de trabalho do administrador (para obter mais detalhes, consulte o Manual do Usuário do Administrador para implementar o Kaspersky Administration Kit 6.0);
- Em servidores de arquivos em rede, implante o Kaspersky Anti-Virus 6.0 for Windows Servers e o *NAgent* (fornecido com o Kaspersky Administration Kit) nos computadores da rede. Para saber mais sobre a instalação remota do Kaspersky Anti-Virus nos computadores da rede, consulte o Manual do Administrador para implementar o Kaspersky Administration Kit 6.0.

Depois de atualizar o plug-in de administração da Kaspersky Lab por meio do Kaspersky Administration Kit, feche o Console de Administração.

O *Console de Administração* (veja a Figura 54) permite administrar o aplicativo por meio do Kaspersky Administration Kit. Trata-se de uma **interface integrada ao MMC** (Microsoft Management Console) padrão e permite que o administrador execute as seguintes funções:

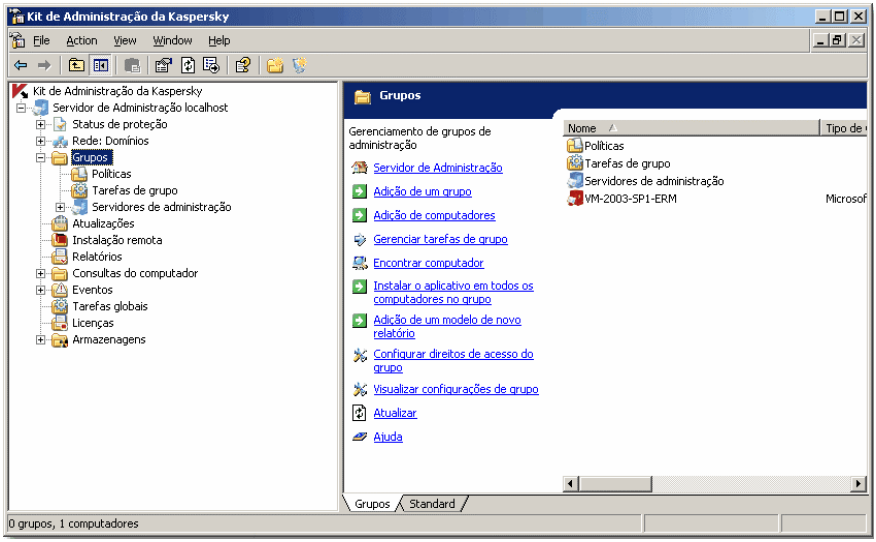


Figura 54. Console de Administração do Kaspersky Administration Kit

- Instalar remotamente o Kaspersky Anti-Virus 6.0 for Windows Servers e o *NAgent* nos computadores da rede
- Configurar remotamente o Kaspersky Anti-Virus nos computadores da rede
- Atualizar as assinaturas de ameaças e módulos do Kaspersky Anti-Virus
- Gerenciar licenças do aplicativo nos computadores da rede
- Exibir informações sobre o funcionamento do programa nos computadores cliente

Ao trabalhar no Kaspersky Administration Kit, o programa é administrado pelas configurações de diretivas, de tarefas e do aplicativos definidas pelo administrador.

As **configurações do aplicativo** são um conjunto de configurações de operação do programa, incluindo configurações gerais de proteção, configurações de Backup e Quarentena, configurações de geração de relatórios etc.

Uma **tarefa** é uma ação específica executada pelo aplicativo. As tarefas do Kaspersky Anti-Virus for Windows Servers são divididas por tipo, de acordo com sua função (tarefas de verificação de vírus, de atualização do programa, reversão de atualizações e tarefas de instalação da chave de licença). Cada

tarefa específica possui um conjunto de configurações do Kaspersky Anti-Virus que são usadas quando executada *(configurações da tarefa)*.

O principal recurso da administração centralizada é o agrupamento de computadores remotos e o gerenciamento de suas configurações através da criação e configuração de diretivas de grupo.

Uma **Diretiva** é um grupo de configurações de funcionamento do programas nos computadores de grupos de trabalho da rede, além de grupos de restrições de redefinição dessas configurações do aplicativo ou das tarefas em um computador cliente individual.

Uma diretiva inclui configurações de todos os recursos do programa. Assim, as diretivas incluem configurações do programa e de todos os tipos de tarefa, exceto as configurações específicas de um determinado tipo de tarefa.

12.1. Administrando o aplicativo

O Kaspersky Administration Kit oferece a oportunidade de iniciar e pausar remotamente o Kaspersky Anti-Virus em computadores cliente individuais, além de definir as configurações gerais do aplicativo, como habilitar/desabilitar a proteção do computador, definir as configurações do Backup e da Quarentena e configurar a criação de relatórios.

Para gerenciar as configurações do aplicativo:

1. Selecione a pasta do grupo que contém o computador cliente na pasta **Grupos** (veja a Figura 54).
2. No painel de resultados, selecione o computador no qual deseja modificar as configurações do aplicativo. No menu de contexto ou no menu **Ações**, selecione o comando **Propriedades**.
3. A guia **Aplicativos** na janela de propriedades do computador cliente (veja a Figura 55) exibe uma lista completa dos aplicativos da Kaspersky Lab instalados no computador cliente.

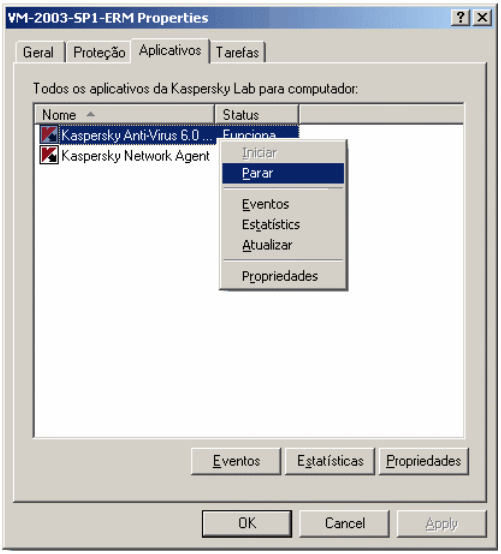


Figura 55. Lista de aplicativos da Kaspersky Lab

Sob a lista de programas, há botões de controle que podem ser usados para:

- Exibir uma lista de eventos de funcionamento do aplicativo que ocorreram no cliente e que foram registrados no Servidor de administração
- Exibir as estatísticas atuais de funcionamento do programa
- Configurar o programa (consulte a seção 12.1.2 na página 152)

12.1.1. Iniciando/interrompendo o aplicativo

Você pode iniciar ou pausar o Kaspersky Anti-Virus em um computador remoto usando os comandos do menu de contexto na janela de propriedades do computador (veja a Figura 55).

Você pode executar as mesmas ações usando os botões **Iniciar/Interromper** na janela de configurações, na guia **Geral** (veja a Figura 56).

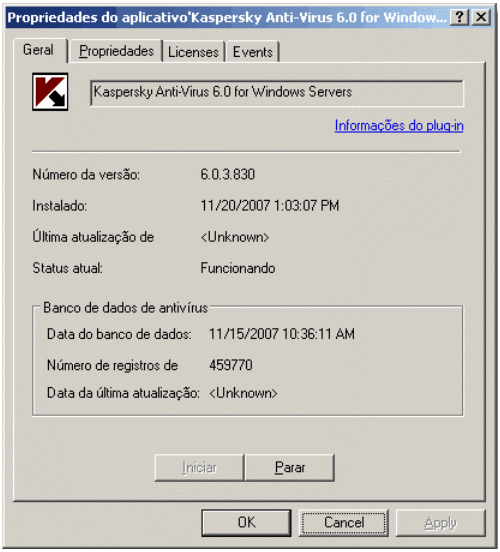


Figura 56. Configurando o Kaspersky Anti-Virus.
A guia **Geral**

Na parte superior da janela, você encontrará o nome do aplicativo instalado, as informações de versão, a data de instalação, seu status (se o aplicativo está em execução ou pausado no computador local) e informações sobre o status do banco de dados de assinaturas de ameaças.

12.1.2. Configurando o aplicativo

Para exibir ou modificar as configurações do aplicativo:

1. Abra a janela de propriedades do computador cliente na guia **Aplicativos** (veja a Figura 54).
2. Selecione **Kaspersky Anti-Virus 6.0 for Windows Servers**. Clique no botão **Propriedades** para abrir a janela de configurações do aplicativo.

Todas as guias, exceto a guia **Propriedades**, são padrão do Kaspersky Administration Kit. Para saber mais sobre as guias padrão, consulte o Manual do Administrador.

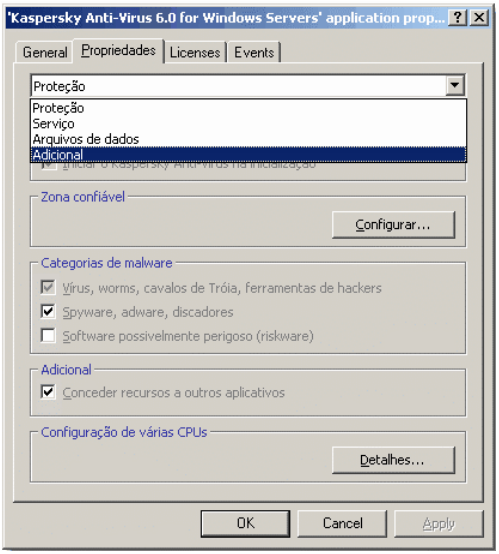


Figura 57. Configurando o Kaspersky Anti-Virus.
A guia **Propriedades**

Se tiver sido criada uma diretiva para o aplicativo (consulte 12.3.1 na página 162) que impede a redefinição de algumas configurações, elas não poderão ser editadas ao configurar o aplicativo.

Na guia **Configurações**, é possível definir as configurações gerais e do serviço de proteção do Kaspersky Anti-Virus, o Backup e a Quarentena, e as configurações de criação de relatórios. Para fazê-lo, selecione o valor desejado no menu suspenso na parte superior da janela e defina as configurações:

Proteção
Nesta janela, você pode: • Habilitar/desabilitar a proteção de um computador (consulte a seção 6.1 na p. 53) • Configurar a inicialização automática do aplicativo quando o computador é ligado (consulte a seção 6.1.5 na p. 57) • Criar uma zona confiável ou uma lista de exclusões (consulte a seção 6.3 na p. 59) • Selecionar os tipos de programas mal-intencionados que o aplicativo vai

monitorar (consulte a seção 6.2 na p. 58) • Configurar a produtividade do aplicativo e as configurações de vários processadores (consulte a seção 6.7 na p. 69).
Serviço
A configuração do serviço inclui: • Configuração de notificações de eventos ocorridos (consulte a seção 11.8.1 na p. 139) • Gerenciamento do recurso de autodefesa do aplicativo e das configurações da proteção do aplicativo por senha (consulte a seção 11.8.2 na p. 144) • Configuração da aparência do aplicativo (consulte a seção 12.3.1 na página 162) • Configuração da compatibilidade do Kaspersky Anti-Virus com outros programas (consulte a seção 11.8.3 na p. 145)
Arquivos de dados
Nesta janela, você pode configurar a geração de estatísticas de relatórios de funcionamento do programa (consulte a seção 11.3.1 na p. 128) e especificar por quanto tempo os arquivos são armazenados no (consulte a seção 11.2.2 na p. 123) e na Quarentena (consulte a seção 11.1.2 na p. 120).

12.1.3. Definido configurações específicas

Ao administrar o Kaspersky Anti-Virus por meio do Kaspersky Administration Kit, você pode habilitar/desabilitar a interatividade e editar informações de Suporte Técnico. Para fazê-lo:

1. Abra a janela de propriedades do computador cliente na guia **Aplicativos** (veja a Figura 55).
2. Selecione **Kaspersky Anti-Virus 6.0 for Windows Servers** e use o botão **Propriedades**. Como resultado, será aberta uma janela de configurações do aplicativo (veja a Figura 57). Selecione **Serviço** no menu suspenso na parte superior da janela.

Na guia **Serviço** da seção **Aparência**, você pode habilitar/desabilitar a interatividade do Kaspersky Anti-Virus em um computador remoto: habilitando o ícone do Kaspersky Anti-Virus na bandeja do sistema, emitindo notificações

sobre eventos que ocorrem com o aplicativo (por exemplo, a detecção de um objeto perigoso).

Se **Permitir interatividade** estiver marcado, um usuário que trabalha em um computador remoto verá o ícone e as mensagens pop-up do antivírus e poderá decidir sobre o que fazer nas janelas de notificação dos eventos ocorridos. Para desabilitar a interatividade do aplicativo, desmarque a caixa de seleção.

Na guia **Informações sobre suporte personalizado** da janela que é aberta ao clicar no botão **Configurações**, você pode editar as informações sobre suporte técnico do usuário exibidas na seção **Serviço** do item **Suporte** no Kaspersky Anti-Virus (veja a Figura 47).

Para alterar as informações no campo superior, insira o texto atual sobre o suporte fornecido. No campo inferior, você pode editar os hiperlinks exibidos na caixa **Suporte técnico on-line** que é aberta ao selecionar **Suporte** na seção **Serviço**.

É possível editar a lista de fontes usando os botões **Adicionar**, **Editar** e **Excluir**. O Kaspersky Anti-Virus adicionará um novo link à parte superior da lista. Para alterar a ordem dos links na lista, use os botões **Para cima** e **Para baixo**.

Se a janela não contiver dados, as informações padrão sobre o suporte técnico não poderão ser editadas.

12.2. Gerenciando tarefas

Esta seção inclui informações sobre o gerenciamento de tarefas do Kaspersky Anti-Virus 6.0 for Windows Servers. Para obter mais detalhes sobre o conceito de gerenciamento de tarefas usando o Kaspersky Administration Kit 6.0, consulte o Manual do Administrador do programa.

Uma conjunto de tarefas do sistema é criada para cada computador ao instalar o aplicativo. Esta lista (veja a Figura 58) inclui tarefas de proteção em tempo real (Antivírus de Arquivos), tarefas de verificação de vírus (Meu Computador, Objetos de inicialização, Áreas críticas) e tarefas de atualização (atualizações de assinaturas de ameaças e módulos do aplicativo, reversões de atualizações e distribuição de atualizações).

Você pode iniciar tarefas do sistema, definir suas configurações e programações, mas elas não podem ser excluídas.

Além disso, você pode criar suas próprias tarefas, como verificações de vírus, atualizações do aplicativo e reversões de atualizações, além de tarefas de instalação da chave de licença.

Para exibir uma lista das tarefas criadas para um computador cliente:

1. Selecione a pasta do grupo que contém o computador cliente na pasta **Grupos** (veja a Figura 54).
2. No painel de resultados, selecione o computador para o qual deseja criar uma tarefa local e use o comando **Tarefas** no menu de contexto ou no menu **Ações**. Em seguida, na janela principal será aberta uma janela exibindo as propriedades do computador cliente.
3. A guia **Tarefas** (veja a Figura 58) exibe uma lista completa de tarefas criadas para esse computador cliente.

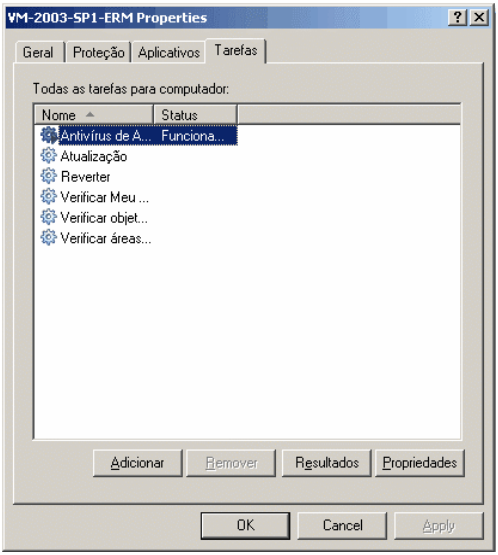


Figura 58. Lista de tarefas do aplicativo

12.2.1. Iniciando e interrompendo tarefas

As tarefas serão iniciadas no computador cliente somente se o aplicativo correspondente estiver em execução (consulte a seção 12.1.1 na p. 151). Se o aplicativo estiver parado, todas as tarefas serão encerradas.

As tarefas são iniciadas e pausadas automaticamente, de acordo com uma programação, ou manualmente, usando comandos do menu de contexto e da janela Exibir configurações de tarefas. Você também pode pausar e reiniciar tarefas.

Para iniciar/interromper/pausar/continuar uma tarefa manualmente:

Selecione a tarefa desejada no painel de resultados, abra o menu de contexto e selecione **Iniciar/Interromper/Pausar/Continuar** ou use os mesmos comandos no menu **Ação**.

Você pode iniciar operações semelhantes na janela de configurações da tarefa na guia **Geral** (veja a Figura 59) usando os botões correspondentes.

12.2.2. Criando tarefas

Ao trabalhar com o aplicativo por meio do Kaspersky Administration Kit, você pode criar:

- Tarefas locais, configuradas para computadores individuais
- Tarefas de grupos, configuradas para computadores unidos em um grupo de rede
- Tarefas globais, configuradas para qualquer conjunto de computadores de qualquer grupo de rede

Você pode modificar as configurações das tarefas, monitorar seu desempenho, copiar e mover tarefas de um grupo para outro e também excluí-las usando os comandos padrão **Copiar/Colar**, **Recortar/Colar** e **Excluir** no menu de contexto ou no menu **Ação**.

12.2.2.1. Criando tarefas locais

Para criar uma tarefa local, execute as seguintes etapas:

1. Abra a janela de propriedades do computador cliente na guia **Tarefas** (veja a Figura 58).
2. Use o botão **Adicionar** para adicionar uma nova tarefa. Assim, será aberta a janela Criar nova tarefa, com um design semelhante a um assistente padrão do Windows e consiste em uma série de etapas pelas quais você pode navegar usando os botões **Voltar** e **Avançar**, ou que pode encerrar usando o botão **Concluído**. O botão **Cancelar** interromperá o processo a qualquer momento.

Etapa 1.Inserindo dados gerais na tarefa

A primeira janela-mestre é introdutória: nela, especifique o nome da tarefa (o campo **Nome**).

Etapa 2.Selecionando um aplicativo e um tipo de tarefa

Nesta etapa, você deve especificar o aplicativo para o qual a tarefa está sendo criada (Kaspersky Anti-Virus 6.0 for Windows Servers). Também é necessário selecionar o tipo de tarefa. As opções de tarefas para o Kaspersky Anti-Virus 6.0 são:

- *Verificação de vírus* – verifica vírus nas áreas especificadas pelo usuário
- *Atualização* – recupera e aplica os pacotes de atualização do programa
- *Reversão da atualização* – reverte para última atualização do programa
- *Instalação da chave de licença* – adiciona uma nova chave de licença para usar o aplicativo

Etapa 3.Configurando o tipo de tarefa selecionado

Dependendo do tipo de tarefa selecionado na etapa anterior, o conteúdo das janelas seguintes pode variar:

VERIFICAÇÃO DE VÍRUS

A janela de configuração da tarefa de verificação de vírus exige que você crie uma lista de objetos a serem verificados (consulte a seção 8.2 na p. 86) e especifique a ação que o Kaspersky Anti-Virus deverá executar ao detectar um objeto perigoso (consulte a seção 8.4.4 na p. 95).

UPDATE

Para as tarefas de atualização das assinaturas de ameaças e módulos do aplicativo, é necessário especificar a fonte que será usada para baixar as atualizações (consulte a seção 10.4.1 na p. 109). A fonte de atualização padrão é o servidor de atualizações do Kaspersky Administration Kit.

REVERSÃO DA ATUALIZAÇÃO

Não há configurações específicas para reverter a atualização mais recente.

INSTALAÇÃO DA CHAVE DE LICENÇA

Para tarefas de instalação da chave de licença, especifique o caminho do arquivo da chave com o botão **Procurar**. Para fazer o backup de uma chave adicionada, marque ☑ **Adicionar como chave de backup**. A chave de licença de backup será ativada quando a chave de licença atual expirar.

Informações sobre a chave adicionada (número, tipo e data de validade da licença) são exibidas no campo a seguir.

Etapa 4. Configurando o início da tarefa usando uma conta de usuário diferente

Nesta etapa, é solicitado que você configure tarefas para serem iniciadas em uma conta de usuário com privilégios suficientes para acessar o objeto que está sendo verificado ou a fonte de atualização (consulte a seção 6.4 na p. 65).

Etapa 5. Configurando uma programação

Depois de configurar a tarefa, será solicitado que você configure uma programação automática de tarefas.

Para fazê-lo, selecione a freqüência de execução da tarefa no menu suspenso e ajuste as configurações da programação na parte inferior da janela.

Etapa 6. Concluindo a criação de uma tarefa

A última janela do assistente informará que você foi bem-sucedido na criação de uma tarefa.

12.2.2.2. Criando tarefas em grupo

Para criar uma tarefa em grupo, execute as seguintes etapas:

1. Selecione o grupo para o qual deseja criar uma tarefa na árvore do console.
2. Selecione a pasta **Tarefas em grupo**, abra o menu de contexto e selecione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Ação**. O assistente para criação de tarefas será iniciado, de maneira semelhante ao assistente para criação de tarefas locais (para saber mais, consulte 12.2.2.1 na página 157). Siga suas instruções.

Quando o assistente for concluído, a tarefa será adicionada à pasta **Tarefas em grupo** desse grupo e todos os grupos sob ele, e estará visível no painel de resultados.

12.2.2.3. Criando tarefas globais

Para criar uma tarefa global, execute as seguintes etapas:

1. Selecione o nó **Tarefas globais** na árvore do console, abra o menu de contexto e selecione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Ação**.
2. O assistente para criação de tarefas será iniciado, de maneira semelhante ao assistente para criação de tarefas locais (para saber

mais, consulte 12.2.2.1 na página 157). A exceção é que existe um estágio para a criação de uma lista de computadores cliente da rede para os quais a tarefa global está sendo criada.

3. Selecione da rede os computadores que executarão a tarefa. Você pode selecionar computadores de várias pastas ou selecionar uma pasta inteira (para obter mais detalhes, consulte o Manual do Administrador do Kaspersky Administration Kit 6.0).

As tarefas globais são executadas apenas em um conjunto selecionado de computadores. Se novos computadores cliente forem adicionados a um grupo com computadores para os quais foi criada uma tarefa de instalação remota, essa tarefa não será executada para eles. Crie uma nova tarefa ou faça as alterações correspondentes às configurações da tarefa existente.

Quando o assistente for concluído, uma tarefa global será adicionada a nó **Tarefas globais** da árvore do console e estará visível no painel de resultados.

12.2.3. Configurando tarefas

Para exibir e modificar as configurações de tarefas do computador cliente:

1. Abra a janela de propriedades do computador cliente na guia **Tarefas** (veja a Figura 58).
2. Selecione a tarefa na lista e clique no botão **Propriedades**. Como resultado, será aberta uma janela de configurações de tarefas (veja a Figura 60).

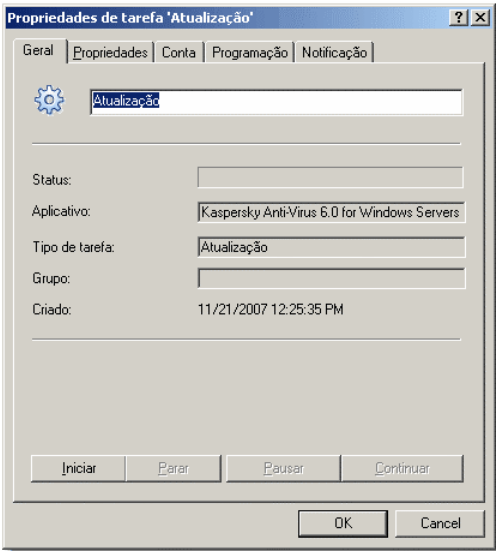


Figura 59. Configurando tarefas

Todas as guias, exceto a guia **Configurações**, são padrão do Kaspersky Administration Kit 6.0. Elas são abordadas mais detalhadamente no Manual do Usuário do Administrador. A guia **Configurações** contém configurações específicas do Kaspersky Anti-Virus. O conteúdo dessa guia varia, dependendo do tipo de tarefa selecionado.

A configuração de tarefas do programa por meio da interface do Kaspersky Administration Kit é semelhante à configuração pela interface do Kaspersky Anti-Virus local, com exceção das configurações específicas daquela tarefa. Consulte Capítulo 7 – Capítulo 10 nas pp. 71 – 105 desse Manual do Usuário para obter uma descrição mais detalhada da configuração de tarefas.

Se tiver sido criada uma diretiva para o aplicativo (consulte a seção 12.3 na p. 161) que bloqueia a redefinição de algumas configurações, elas não poderão ser editadas ao configurar as tarefas.

12.3. Gerenciado diretivas

A configuração de diretivas permite aplicar configurações universais a aplicativos e tarefas nos computadores cliente que pertencem a um único grupo de rede.

Esta seção inclui informações sobre a criação e configuração de diretivas do Kaspersky Anti-Virus 6.0 for Windows Servers. Para obter mais detalhes sobre o conceito de gerenciamento de diretivas usando o Kaspersky Administration Kit 6.0, consulte o Manual do Administrador do programa.

12.3.1. Criando diretivas

Para criar uma diretiva para o Kaspersky Anti-Virus, execute as seguintes etapas:

1. Na pasta **Grupos** (veja a Figura 54), selecione o grupo de computadores para os quais você deseja criar uma diretiva.
2. Selecione a pasta **Diretivas** que pertence ao grupo selecionado, abra o menu de contexto e use o comando **Criar→Diretiva**. Uma janela Criar nova diretiva aparecerá.

   A janela Criar diretiva foi criada como um Assistente do Microsoft Windows padrão e consiste em uma série de etapas pelas quais você pode navegar usando os botões **Voltar** e **Avançar**, ou encerrar usando o botão **Concluído**. O botão **Cancelar** interromperá o Assistente a qualquer momento.

Durante cada etapa da criação de uma diretiva, as configurações inseridas podem ser bloqueadas com o botão  . Se o cadeado no botão estiver fechado, no futuro os valores atribuídos pela diretiva criada serão usados ao usar a diretiva em computadores cliente.

Etapa 1.Inserindo dados gerais na diretiva

As primeiras janelas do assistente são introdutórias. Nelas, é necessário especificar o nome da diretiva (campo **Nome**), selecionar **Kaspersky Anti-Virus 6.0 for Windows Servers** no menu suspenso **Nome do aplicativo**. Se desejar que as configurações da diretiva entrem em vigor imediatamente após sua criação, marque **Tornar diretiva ativa**.

Etapa 2.Selecionando um status de diretiva

Esta janela solicitará que você especifique o status da diretiva. Para fazê-lo, mova o controle deslizante para a posição desejada: diretiva ativa ou diretiva inativa.

Várias diretivas podem ser criadas em um grupo para um aplicativo, mas apenas uma delas pode ser a diretiva (ativa) atual.

Etapa 3. Selecionando e configurando os componentes de proteção

Neste estágio, você pode habilitar/desabilitar a proteção do computador e o Antivírus de Arquivos. Por padrão, a proteção está habilitada e o Antivírus de Arquivos está em execução.

Para fazer o ajuste fino das configurações de proteção ou para configurar o Antivírus de Arquivos, selecione-o na lista e clique no botão **Configurações**.

Etapa 4. Configurando tarefas de verificação de vírus

Neste estágio, é solicitado que você defina as configurações que serão usadas para as tarefas de verificação de vírus.

Na caixa **Nível de segurança**, selecione um dos três níveis predefinidos (consulte a seção 7.1 na p. 72): Para fazer o ajuste fino do nível selecionado, clique no botão **Configurações**. Para restaurar as configurações do nível de proteção **Recomendado**, use o botão **Padrão**.

Na seção **Ação**, especifique a ação que o Anti-Virus deverá executar quando um objeto perigoso for detectado (consulte a seção 8.4.4 na p. 95).

Etapa 5. Configurando a atualização

Nesta janela, configure o recurso de distribuição de atualizações do Kaspersky Anti-Virus.

Na seção **Configurações de atualização**, especifique se os módulos do programa devem ser atualizados (consulte a seção 10.4.2 na p. 109). Na janela que é aberta ao clicar no botão **Configurações**, atribua as configurações de rede local (consulte a seção 10.4.3 na p. 114) e especifique a fonte de atualização (consulte a seção 10.4.1 na p. 109).

Na seção **Ações após a atualização**, habilite/desabilite a verificação da Quarentena após receber um novo pacote de atualizações (consulte a seção 10.4.4 na p. 115).

Etapa 6. Imposição da diretiva

Neste estágio, é solicitado que você selecione um método de distribuição da diretiva para os clientes do grupo (para obter mais detalhes, consulte o Manual do Administrador do Kaspersky Administration Kit 6.0).

Etapa 7. Determinando um método para impor a diretiva pela primeira vez

Nesta etapa, selecione um método para impor a diretiva pela primeira vez em computadores cliente do grupo na janela **Impor diretiva** (para obter mais detalhes, consulte o Manual do Administrador do Kaspersky Administration Kit 6.0).

Etapa 8. Concluindo a criação de uma diretiva

A última janela do assistente informa que você foi bem-sucedido na criação de uma diretiva.

Ao concluir o assistente, a diretiva do Kaspersky Anti-Virus será adicionada à pasta **Diretivas** do grupo correspondente e estará visível no painel de resultados.

Você pode editar as configurações da diretiva criada e definir restrições para a modificação de suas configurações usando o botão  para cada grupo de configurações. Um usuário no computador cliente não poderá alterar as configurações, se elas estiverem bloqueadas dessa forma. A diretiva será aplicada aos computadores cliente na primeira vez que eles sincronizarem com o servidor.

Você pode copiar ou mover as diretivas de um grupo para outro e excluí-las usando os comandos padrão **Copiar**/**Colar**, **Recortar**/**Colar** e **Excluir** no menu de contexto ou no menu Ação.

12.3.2. Exibindo e editando configurações de diretivas

No estágio de edição, você pode modificar a diretiva e bloquear a modificação de configurações em diretivas de grupos aninhados e em configurações de aplicativos e tarefas.

Para exibir e editar as configurações de diretivas:

1. Selecione o grupo de computadores para os quais as configurações devem ser editadas na árvore do console, na pasta **Grupos**.
2. Selecione a pasta **Diretivas** que pertence a esse grupo. Ao fazê-lo, o painel de resultados exibirá todas as diretivas criadas para o grupo.
3. Selecione a diretiva desejada na lista de diretivas do **Kaspersky Anti-Virus 6.0 for Windows Servers** (o nome do aplicativo está especificado no campo **Aplicativo**).

4. Abra o menu de contexto da diretiva selecionada e clique no comando **Propriedades**. A tela exibirá a janela de configurações da diretiva para o Kaspersky Anti-Virus 6.0 (veja a Figura 60).

Todas as guias, exceto a guia **Configurações**, são padrão do Kaspersky Administration Kit 6.0. Elas são abordadas mais detalhadamente no Manual do Usuário do Administrador.

A guia **Configurações** exibe as configurações de diretivas do Kaspersky Anti-Virus 6.0. As configurações de diretivas incluem configurações do programa (consulte a seção 12.1.2 na p. 152) e as configurações de tarefas (consulte a seção 12.2 na p. 155).

Para definir as configurações, selecione o valor desejado no menu suspenso na parte superior da janela.

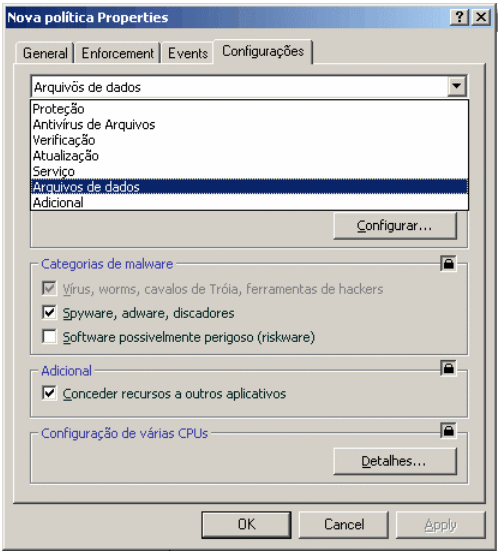


Figura 60. Configurando a diretiva

CAPÍTULO 13. TRABALHANDO COM O PROGRAMA NO PROMPT DE COMANDO

Você pode usar o Kaspersky Anti-Virus for Windows Servers a partir do prompt de comando. É possível executar as seguintes operações:

- Iniciar, interromper, pausar e reiniciar a atividade do Antivírus de Arquivos
- Iniciar, interromper, pausar e reiniciar as verificações de vírus
- Obter informações sobre o status atual do Antivírus de Arquivos e das tarefas, além de suas estatísticas
- Verificar objetos selecionados
- Atualizar assinaturas de ameaças e módulos do programa
- Acessar a Ajuda sobre a sintaxe do prompt de comando
- Acessar Ajuda sobre a sintaxe de comandos

A sintaxe do prompt de comando é a seguinte:

```
avp.com <comando> [configurações]
```

Acesse o programa do prompt de comando na pasta de instalação do programa ou especificando o caminho completo do avp.com.

As seguintes instruções podem ser usadas como **<comando>**:

ADDKEY	Ativa o aplicativo usando um arquivo de chave de licença (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
ACTIVATE	Ativa o aplicativo on-line usando um código de ativação
START	Inicia o Antivírus de Arquivos ou uma tarefa
PAUSE	Pausa o Antivírus de Arquivos ou uma tarefa (o comando só poderá ser executado se a senha atribuída pela interface do programa for inserida)

RESUME	Reinicia o Antivírus de Arquivos ou uma tarefa
STOP	Interrompe o Antivírus de Arquivos ou uma tarefa (o comando só poderá ser executado se a senha atribuída pela interface do programa for inserida)
STATUS	Exibe o status do Antivírus de Arquivos ou da tarefa na tela
STATISTICS	Exibe estatísticas do Antivírus de Arquivos ou da tarefa na tela
HELP	Ajuda da sintaxe de comandos e da lista de comandos
SCAN	Verifica objetos quanto à presença de vírus
UPDATE	Inicia a atualização do programa
ROLLBACK	Reverte para a última atualização do programa (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
EXIT	Fecha o programa (este comando só pode ser executado com a senha atribuída na interface do programa)
IMPORT	Importa configurações do Kaspersky Anti-Virus for Windows Servers (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
EXPORT	Exporta configurações do Kaspersky Anti-Virus for Windows Servers

Cada comando usa suas próprias configurações específicas do componente do Kaspersky Anti-Virus for Windows Servers.

13.1. Ativando o aplicativo

Existem duas formas de ativar o aplicativo:

- on-line, usando um código de ativação (comando ACTIVATE)
- usando um arquivo de chave de licença (comando ADDKEY).

Sintaxe do comando:

```
ACTIVATE <código_de_ativação>
ADDKEY <nome_do_arquivo> /password=<sua_senha>
```

Parâmetros:

<nome_do_arquivo>	nome do arquivo de chave do aplicativo com a extensão *.key.
<código_de_ativação>	O código de ativação do aplicativo fornecido na compra.
<sua_senha>	A senha do Kaspersky Anti-Virus definida pela interface do programa.
Observe que este comando não será aceito sem uma senha.	

Exemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<sua_senha>
```

13.2. Gerenciando o Antivírus de Arquivos e as tarefas

Sintaxe do comando:

```
avp.com <comando> <perfil|nome_da_tarefa>
[/R[A]:<arquivo_de_log>]
avp.com STOP|PAUSE <perfil|nome_da_tarefa>
/password=<sua_senha> [/R[A]:<arquivo_de_relatório>]
```

Parâmetros:

<comando>	O Kaspersky Anti-Virus oferece gerenciamento de tarefas e componentes da linha de comando usando os seguintes comandos: **START** – inicia uma tarefa ou componente

	de proteção em tempo real. **STOP** – interrompe uma tarefa ou componente de proteção em tempo real. **PAUSE** – pausa uma tarefa ou componente de proteção em tempo real. **RESUME** – continua uma tarefa ou componente de proteção em tempo real. **STATUS** – exibe o status atual da tarefa ou componente de proteção em tempo real. **STATISTICS** – exibe as estatísticas de tempo de execução da tarefa ou componente de proteção em tempo real. Observe que PAUSE e STOP são protegidos por senha.
<perfil|nome_da_tarefa>	Ao parâmetro **<perfil>** pode ser atribuído qualquer módulo ou componente de segurança em tempo real do aplicativo, tarefa de verificação por demanda ou atualização como um valor (os valores padrão usados pelo aplicativo são mostrados a seguir). Os valores válidos para o parâmetro **<nome_da_tarefa>** incluem o nome de qualquer atualização ou tarefa de verificação por demanda definida pelo usuário.
<sua_senha>	A senha do Kaspersky Anti-Virus definida pela interface do programa.
/R[A]:<arquivo_de_relatório>	**R:<arquivo_de_relatório>**: registra apenas eventos importantes. **/RA:<arquivo_de_relatório>**: registra todos os eventos. Pode ser usado um caminho absoluto ou relativo de um arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Um dos seguintes valores é atribuído a **<perfil>**:

RTP	Todos os componentes de proteção O comando `avp.com START RTP` iniciará o Antivírus de Arquivos se ele tiver sido pausado usando o botão ⏸ na interface gráfica do usuário ou com o comando `PAUSE` no prompt de comando. Se o componente foi desabilitado usando o botão ■ na interface gráfica do usuário ou o comando `STOP` do prompt de comando, execute o comando `avp.com START FM` para que ele seja iniciado.
FM	Antivírus de Arquivos
UPDATER	Atualização
RetranslationCfg	Distribuição de atualizações para uma fonte de atualizações local
Rollback	Reverte para a última atualização do programa
SCAN_OBJECTS	Tarefa de verificação de vírus
SCAN_MY_COMPUTER	Tarefa Meu Computador
SCAN_CRITICAL_AREAS	Tarefa Áreas críticas
SCAN_STARTUP	Tarefa Objetos de inicialização
SCAN_QUARANTINE	Tarefa de verificação de objetos em Quarentena
Os componentes e tarefas iniciados no prompt de comando são executados de acordo com as configurações definidas na interface do programa.	

Exemplos:

Para habilitar o Antivírus de Arquivos, digite no prompt de comando:

```
avp.com START FM
```

Para interromper uma tarefa de verificação de Meu Computador do prompt de comando, digite*:*

```
avp.com STOP SCAN_MY_COMPUTER /password=<sua senha>
```

13.3. Verificações antivírus

Em geral, a sintaxe para iniciar a verificação de vírus em uma determinada área e processar objetos mal-intencionados a partir do prompt de comando tem a seguinte aparência:

```
avp.com SCAN [<objeto verificado>] [<ação>] [<tipos
de arquivos>] [<exclusões>] [<arquivo_configuração>]
[<configurações relatório>] [<configurações
avançadas>]
```

Para verificar objetos, você também pode iniciar uma das tarefas criadas no Kaspersky Anti-Virus for Windows Servers do prompt de comando (consulte 13.2 na p. 168). A tarefa será executada de acordo com as configurações definidas na interface do programa.

Descrição dos parâmetros:

<objeto verificado> - este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código mal-intencionado. Pode incluir vários valores da seguinte lista, separados por espaços.	
<arquivos>	Lista dos caminhos dos arquivos e/ou pastas a serem verificados. Você pode inserir caminhos absolutos ou relativos. Os itens da lista são separados por um espaço. Observações: Se o nome do objeto contiver um espaço, será necessário colocá-lo entre aspas Se você selecionar uma pasta específica, todos os arquivos contidos nela serão verificados.
/MEMORY	Objetos da memória do sistema
/STARTUP	Objetos de inicialização
/MAIL	Bancos de dados de e-mail

/REMDRIVES	Todas as unidades de mídia removíveis
/FIXDRIVES	Todas as unidades internas
/NETDRIVES	Todas as unidades de rede
/QUARANTINE	Objetos em quarentena
/ALL	Verificação completa
/@:<filelist.lst>	Caminho para o arquivo que contém uma lista de objetos e pastas a serem incluídos na verificação. O arquivo deve estar no formato de texto e cada objeto da verificação deve iniciar uma nova linha. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se contiver espaços, o caminho deverá estar entre aspas.
<ação> - este parâmetro define as respostas para objetos mal-intencionados detectados durante a verificação. Se este parâmetro não for definido, o valor padrão será **/i8**.	
/i0	Não é tomada nenhuma ação com relação ao objeto; suas informações são registradas no relatório.
/i1	Neutraliza os objetos infectados e, se falhar, os ignora.
/i2	Neutraliza objetos infectados e, se falhar, os exclui. Exceções: não exclui objetos infectados de objetos compostos; exclui objetos compostos com cabeçalhos executáveis, ou seja, arquivos comprimidos sfx (padrão).
/i3	Neutraliza objetos infectados e, se falhar, os exclui. Também exclui todos os objetos compostos completamente, se não for possível excluir o conteúdo infectado.

/i4	Neutraliza objetos infectados e, se falhar, os exclui. Também exclui todos os objetos compostos completamente, se não for possível excluir o conteúdo infectado.
/i8	Pergunta o que fazer se for detectado um objeto infectado.
/i9	Pergunta o que fazer no final da verificação.
<tipos de arquivos> - este parâmetro define os tipos de arquivos que passarão pela verificação antivírus. Se este parâmetro não for definido, o valor padrão será /fi.	
/fe	Verifica somente os arquivos possivelmente infectados, por extensão.
/fi	Verifica somente os arquivos possivelmente infectados, por conteúdo (padrão).
/fa	Verifica todos os arquivos
<exclusões> - este parâmetro define os objetos que serão excluídos da verificação. Pode incluir vários valores da lista fornecida, separados por espaços.	
-e:a	Não verifica arquivos comprimidos
-e:b	Não verifica bancos de dados de e-mail
-e : m	Não verifica e-mails em texto sem formatação
-e:<máscara_arquivos>	Não verifica objetos por máscara
-e:<segundos>	Ignora objetos cujo tempo de verificação ultrapassa o tempo especificado pelo parâmetro **<segundos>**.
-es:<tamanho>	Ignora arquivos maiores (em MB) que o valor atribuído por **<tamanho>**.

<arquivo de configuração> - define o caminho do arquivo de configuração que contém as configurações de verificação do programa. O arquivo de configuração é salvo no formato binário (*.dat*), a menos que seja especificado outro formato ou se o formato não for atribuído, e poderá ser usado posteriormente para importar as configurações do aplicativo em outros computadores. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores especificados na interface do Kaspersky Anti-Virus for Windows Servers.	
/C:<nome_do_arquivo>	Use os valores de configuração atribuídos no arquivo de configuração **<nome_do_arquivo>**
<configurações do relatório> - este parâmetro determina o formato do relatório sobre os resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.	
/R:<arquivo_relatório>	Registra somente os eventos importantes nesse arquivo
/RA:<arquivo_relatório>	Registra todos os eventos nesse arquivo
<configurações avançadas> – configurações que definem o uso de tecnologias de verificação antivírus.	
/iChecker=<ativado|desativado>	Habilita/desabilita o iChecker.
/iSwift=<ativado|desativado>	Habilita/desabilita o iSwift.

Exemplos:

*Iniciar a verificação da RAM, dos programas de inicialização, dos bancos de dados de e-mail, dos diretórios **Meus Documentos** e **Arquivos de Programas** e do arquivo **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\Todos os Usuários\Meus Documentos"
"C:\Arquivos de Programas" "C:\Downloads\test.exe"
```

Pausar a verificação de objetos selecionados e iniciar uma verificação completa do computador; continuar a verificação de vírus nos objetos selecionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<sua_senha>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Verificar a RAM e os objetos relacionados no arquivo **object2scan.txt**: Use o arquivo de configuração **scan_setting.txt**. Após a verificação, gerar um relatório que registre todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Exemplo de arquivo de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Atualizações do programa

A sintaxe para atualizar os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus for Windows Servers a partir do prompt de comando é a seguinte:

```
avp.com UPDATE [<fonte_de_atualização>]
[/R[A]:<arquivo_de_relatório>] [/C:<nome_do_arquivo>]
[/APP=<on|off>]
```

Descrição dos parâmetros:

<fonte_de_atualização>	Servidor HTTP ou FTP ou diretório de rede para baixar as atualizações. O valor do parâmetro pode estar no formato de um caminho completo para uma fonte de atualização ou uma URL. Se nenhum caminho for especificado, uma fonte de atualização será copiada das configurações de atualização do aplicativo.

/R[A]:<arquivo_de_relatório>	**/R:<arquivo_relatório>** – registra somente os eventos importantes no relatório. **/R[A]:<arquivo_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
/C:<nome_do_arquivo>	Caminho do arquivo de configuração com as definições para atualizações do programa. O arquivo de configuração é um arquivo de texto que contém um grupo de configurações de prompt de comando para atualizar o programa. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores especificados na interface do Kaspersky Anti-Virus for Windows Servers.
/APP=<on|off>	Habilita / desabilita as atualizações de módulos do aplicativo

Exemplos:

Atualizar as assinaturas de ameaças e registrar todos os eventos no relatório:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Atualizar os módulos do programa Kaspersky Anti-Virus for Windows Servers usando as definições do arquivo de configuração **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Exemplo de arquivo de configuração:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

13.5. Configurações de reversão

Sintaxe do comando:

```
ROLLBACK [/R[A]:<arquivo_de_relatório>]
[/password=<sua_senha>]
```

/R[A]:<arquivo_de_relatório>	**/R:<arquivo_relatório>** – registra somente os eventos importantes no relatório. **/R[A]:<arquivo_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
<sua_senha>	Senha para acessar o Kaspersky Anti-Virus atribuída na interface do programa.
Observe que não será possível executar este comando sem informar a senha.	

Exemplos:

```
avp.com ROLLBACK /RA:rollback.txt
[/password=<sua_senha>]
```

13.6. Exportando configurações

Sintaxe do comando:

```
avp.com EXPORT <perfil> <nome_do_arquivo>
```

Descrição dos parâmetros:

<perfil>	Antivírus de Arquivos ou tarefa cujas configurações estão sendo exportadas. Em **<perfil>**, você pode usar qualquer valor que esteja listado em 13.2 na p. 168.

<nome_do_arquivo>	Caminho do arquivo para o qual as configurações do Kaspersky Anti-Virus for Windows Servers serão exportadas. Você pode usar um caminho absoluto ou relativo. O arquivo de configuração é salvo no formato binário (*.dat*), a menos que seja especificado outro formato ou se o formato não for atribuído, e poderá ser usado posteriormente para importar as configurações do aplicativo em outros computadores. O arquivo de configuração pode ser salvo como um arquivo de texto. Para fazê-lo, especifique a extensão *.txt* no nome do arquivo. Não é possível importar configurações de proteção de um arquivo de texto. Este arquivo pode ser usado somente para especificar as configurações principais de funcionamento do programa.

Exemplos:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importando configurações

Sintaxe do comando:

```
avp.com IMPORT <nome_do_arquivo>
[/password=<sua_senha>]
```

<nome_do_arquivo>	Caminho do arquivo do qual as configurações do Kaspersky Anti-Virus for Windows Servers serão importadas. Você pode usar um caminho absoluto ou relativo. As configurações podem ser importadas somente de arquivos binários. Se você instalar o programa no modo oculto usando o prompt de comando ou o Editor de Objeto de Diretiva de Grupo, o nome que consta no arquivo de configuração deverá ser *install.cfg*. Caso contrário, o programa não o reconhecerá.

<sua_senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
Observe que este comando não será aceito sem uma senha.	

Exemplos:

```
avp.com IMPORT c:\ settings.dat /password=<sua_senha>
```

13.8. Iniciando o programa

Sintaxe do comando:

```
avp.com
```

13.9. Interrompendo o programa

Sintaxe do comando:

```
EXIT /password=<senha>
```

<senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
Observe que este comando não será aceito sem uma senha.	

Observe que não será possível executar este comando sem informar a senha.

13.10. Obtendo um arquivo de rastreamento

Talvez seja necessário um arquivo de rastreamento, no caso de problemas em tempo de execução do aplicativo, para que os especialistas do Suporte Técnico possam trabalhar em uma solução de problemas mais direcionada.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off]
[<nível_de_rastreamento>]
```

[on|off]	Habilita/desabilita a geração do arquivo de rastreamento.
[file]	Obtém um rastreamento e salva em arquivo.
<nível_de_rastreamento>	Este parâmetro pode ter valores numéricos de 0 (nível mais baixo, somente para eventos críticos) a 700 (nível mais alto, todos os eventos). Quando uma solicitação é enviada para o Suporte Técnico, um especialista deve especificar o nível de rastreamento necessário. Se não for especificado, o nível recomendado será 500.
Cuidado! A geração do arquivo de rastreamento deve estar habilitada somente para solucionar um problema específico. A ativação contínua da funcionalidade de rastreamento pode reduzir o desempenho do computador e fazer o disco rígido ficar cheio.	

Exemplos:

Desabilitar rastreamento:

```
avp.com TRACE file off
```

Gerar um arquivo de rastreamento para o Suporte Técnico com um nível de rastreamento máximo de 500:

avp.com TRACE file on 500

13.11. Exibindo a Ajuda

Este comando está disponível para exibir a Ajuda sobre a sintaxe do prompt de comando:

```
avp.com [ /? | HELP ]
```

Para obter ajuda sobre a sintaxe de um comando específico, use um dos comandos a seguir:

```
avp.com <comando> /?
avp.com HELP <comando>
```

13.12. Códigos de retorno da interface da linha de comando

Esta seção contém uma lista de códigos de retorno da linha de comando. Os códigos gerais podem ser retornados por qualquer comando da linha de comando. Os códigos de retorno incluem códigos gerais e códigos específicos de um determinado tipo de tarefa.

Códigos de retorno gerais	
0	Operação concluída com êxito
1	Valor de configuração inválido
2	Erro desconhecido
3	Erro na conclusão da tarefa
4	Tarefa cancelada
Códigos de retorno da tarefa de verificação de vírus	
101	Todos os objetos perigosos foram processados
102	Objetos perigosos detectados

CAPÍTULO 14. MODIFICANDO, REPARANDO E REMOVENDO O PROGRAMA

O aplicativo pode ser desinstalado das maneiras a seguir:

- usando o Assistente para Instalação do aplicativo (consulte a seção 14.2 na p. 184);
- do prompt de comando (consulte a seção 14.2 na p. 184);
- usando o Kaspersky Administration Kit (consulte o Manual de Implementação do Kaspersky Administration Kit);
- usando as diretivas de domínio de grupo do Microsoft Windows Server 2000/2003 (consulte a seção 3.4.3 na p. 35).

14.1. Modificando, reparando e removendo o programa usando o Assistente para Instalação

Talvez seja necessário reparar o programa, se você detectar erros no funcionamento depois de uma configuração incorreta ou da corrupção de arquivos.

Para reparar ou modificar componentes ausentes do Kaspersky Anti-Virus for Windows Servers ou excluir o programa:

1. Insira o CD de instalação utilizado para instalar o programa na unidade de CD-ROM. Se você instalou o Kaspersky Anti-Virus for Windows Servers de outra fonte (pasta de acesso público, pasta no disco rígido, etc.), verifique se o pacote de instalação se encontra na origem especificada e se você tem acesso a ela.
2. Selecione **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Modificar, reparar ou remover**.

Um assistente para instalação do programa será aberto. Vamos examinar mais detalhadamente as etapas necessárias para reparar, modificar ou excluir o programa.

Etapa 1.Janela de boas-vindas da instalação

Se você executar todas as etapas descritas acima, necessárias para reparar ou modificar o programa, a janela de boas-vindas da instalação do Kaspersky Anti-Virus for Windows Servers aparecerá. Para continuar, clique no botão **Avançar**.

Etapa 2.Selecionando uma operação

Neste estágio, selecione a operação que deseja executar. Você pode modificar os componentes do programa, reparar os componentes instalados ou remover componentes ou o programa todo. Para executar a operação desejada, clique no botão apropriado. A resposta do programa dependerá da operação selecionada.

A modificação do programa se assemelha à instalação personalizada do mesmo, na qual você pode especificar os componentes que deseja instalar (consulte a Etapa 7 na p. 25) e excluir.

O reparo do programa depende dos componentes instalados. Serão reparados os arquivos de todos os componentes instalados e o nível de segurança Recomendado será definido para cada um deles.

Aviso!

Se o Kaspersky Anti-Virus 6.0 for desinstalado remotamente, o servidor não será reiniciado automaticamente. Contudo, para remover completamente os componentes do aplicativo e para que o computador funcione corretamente no futuro, é recomendável reiniciar manualmente.

Se você remover o programa, poderá selecionar os dados criados e usados pelo programa que deseja salvar no computador. Para excluir todos os dados do Kaspersky Anti-Virus for Windows Servers, selecione **Desinstalação completa**. Para salvar os dados, selecione **Salvar objetos do aplicativo** e especifique os objetos que não deverão ser excluídos da lista:

- *Dados de ativação* – informações sobre a ativação do programa.
- *Assinaturas de ameaças* – conjunto completo de assinaturas de programas perigosos, vírus e outras ameaças da atualização mais recente.
- *Arquivos de backup* – cópias de backup dos objetos excluídos ou desinfectados. É recomendável salvar esses arquivos, caso possam ser restaurados posteriormente.
- *Arquivos da Quarentena* – arquivos possivelmente infectados por vírus ou suas modificações. Esses arquivos contêm códigos semelhantes ao código de um vírus conhecido, mas é difícil determinar se eles são mal-

intencionados. É recomendável salvá-los, pois eles podem não estar infectados ou talvez possam ser desinfectados após a atualização das assinaturas de ameaças.

- *Configurações do aplicativo* – configurações do Antivírus de Arquivos
- *Dados do iSwift* – banco de dados com informações sobre os objetos verificados nos sistemas de arquivos NTFS, que podem aumentar a velocidade de verificação. Ao usar esse banco de dados, o Kaspersky Anti-Virus for Windows Servers verifica somente os arquivos modificados desde a última verificação.

Aviso!

Se passar muito tempo entre a desinstalação de uma versão do Kaspersky Anti-Virus for Windows Servers e a instalação de outra, não é recomendável usar o banco de dados do *iSwift* de uma instalação anterior. Um programa perigoso poderia invadir o computador durante este período e seus efeitos não seriam detectados pelo banco de dados, o que poderia resultar em uma infecção.

Para iniciar a operação selecionada, clique no botão **Avançar**. O programa começará a copiar os arquivos necessários para o computador ou a excluir os componentes e dados selecionados.

Etapa 3. Concluindo a modificação, o reparo ou a remoção do programa

O processo de modificação, reparo ou remoção será exibido na tela, sendo informado a seguir sobre sua conclusão.

Em geral, a remoção do programa exige a reinicialização do computador, pois é necessário informar essas modificações ao sistema. O programa perguntará se deseja reiniciar o computador. Clique em **Sim** para reiniciar imediatamente. Para reiniciar mais tarde, clique em **Não**.

14.2. Desinstalando o programa do prompt de comando

Para desinstalar o Kaspersky Anti-Virus 6.0 for Windows Servers do prompt de comando, digite:

```
msiexec /i <nome_do_pacote>
```

O Assistente para Instalação será aberto. Você pode usá-lo para desinstalar o aplicativo (consulte o Capítulo 14 na p. 182).

Para desinstalar o aplicativo no modo não interativo sem reiniciar o computador (o computador deverá ser reiniciado manualmente após a desinstalação), digite:

```
msiexec /i <nome_do_pacote> /qn
```

Para desinstalar o aplicativo em segundo plano e reiniciar o computador, digite:

```
msiexec /x <nome_do_pacote> ALLOWREBOOT=1 /qn
```

Se você optou pela proteção da desinstalação do programa por senha ao instalá-lo, será necessário inserir essa senha. Caso contrário, o programa não poderá ser desinstalado.

Para remover o aplicativo inserindo uma senha como prova do privilégio de remoção, digite:

`msiexec /x <nome_do_pacote> KLUNINSTPASSWD=******` – para remover o aplicativo no modo interativo;

`msiexec /x <nome_do_pacote> KLUNINSTPASSWD=****** /qn` – para remover o aplicativo no modo não interativo;

APÊNDICE A. INFORMAÇÕES DE REFERÊNCIA

Este apêndice contém material de referência sobre os formatos de arquivos e máscaras de extensão usados nas configurações do Kaspersky Anti-Virus for Windows Servers.

A.1. Lista de arquivos verificados por extensão

Se você selecionar **Verificar programas e documentos (por extensão)**, o Antivírus de Arquivos verificará detalhadamente os arquivos com as extensões a seguir quanto à presença de vírus.

com – arquivo executável de um programa

exe – arquivo executável ou arquivo comprimido de extração automática

sys – driver do sistema

prg – texto de programa do dBase, Clipper ou Microsoft Visual FoxPro, ou de um programa de criação de arquivos WAV

bin - arquivo binário

bat – arquivo em lotes

cmd – arquivo de comando do Microsoft Windows NT (semelhante a um arquivo .bat do DOS), OS/2

dpl – biblioteca compactada do Borland Delphi

dll – biblioteca de carga dinâmica

scr – tela de abertura do Microsoft Windows

cpl – módulo do painel de controle do Microsoft Windows

ocx – objeto OLE (Object Linking and Embedding) da Microsoft

tsp – programa executado em modo split-time

drv – driver de dispositivo

vxd – driver virtual de dispositivo do Microsoft Windows

pif – arquivo de informações do programa

lnk – arquivo de link do Microsoft Windows

reg – arquivo de chave do Registro do sistema do Microsoft Windows

ini – arquivo de inicialização

cla – classe Java

vbs – script do Visual Basic

vbe – extensão de vídeo do BIOS

js, *jse* – texto de origem JavaScript

htm – documento de hipertexto

htt – cabeçalho de hipertexto do Microsoft Windows

hta – programa de hipertexto do Microsoft Internet Explorer

asp – script de Active Server Pages

chm – arquivo HTML compilado

pht – HTML com scripts PHP incorporados

php – script incorporado em arquivos HTML

wsh – arquivo Microsoft Windows Script Host

wsf – script do Microsoft Windows

the – papel de parede da área de trabalho do Microsoft Windows 95

hlp – arquivo da Ajuda do Win

eml – arquivo de e-mail do Microsoft Outlook Express

nws – arquivo de e-mail de notícias do Microsoft Outlook Express

msg – arquivo de e-mail do Microsoft Mail

plg – e-mail

mbx – extensão de e-mails salvos do Microsoft Office Outlook

*doc** – um documento do Microsoft Word, como: *doc* – um documento do Microsoft Word, *docx* – um documento do Microsoft Word 2007 com suporte a XML, *docm* – um documento do Microsoft Word 2007 com suporte de macro

*dot** – um modelo de documento do Microsoft Word, como *dot* – um modelo de documento do Microsoft Word, *dotx* – um modelo de documento do Microsoft Word 2007, *dotm* – um modelo de documento do Microsoft Word 2007 com suporte de macro

fpm – programa de banco de dados, arquivo inicial do Microsoft Visual FoxPro

rtf – documento RTF

shs – fragmento do Shell Scrap Object Handler

dwg – banco de dados de blueprints do AutoCAD

msi – pacote do Microsoft Windows Installer

otm – projeto VBA do Microsoft Office Outlook

pdf – documento do Adobe Acrobat

swf – arquivo flash do Shockwave

jpg, jpeg, png – formato de imagem gráfica compactada

emf – Meta arquivos do sistema operacional Microsoft Windows da próxima geração em formato Enhanced Metafile. Os arquivos EMF não têm suporte no Microsoft Windows de 16 bits.

ico – arquivo de ícone

ov? – arquivos executáveis do Microsoft DOC

*xl** – documentos e arquivos do Microsoft Office Excel, como: *xla* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento. *xlsx* – uma pasta de trabalho do Microsoft Excel 2007, *xltm* – uma pasta de trabalho do Microsoft Excel 2007 com suporte de macro, *xlsb* – um Microsoft Excel 2007 em formato binário (não XML), *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de macro, *xlam* – um plug-in do Microsoft Excel 2007 com suporte de macro.

*pp** – documentos e arquivos do Microsoft Office Excel, como: *xla* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento. *xlsx* – uma pasta de trabalho do Microsoft Excel 2007, *xltm* – uma pasta de trabalho do Microsoft Excel 2007 com suporte de macro, *xlsb* – um Microsoft Excel 2007 em formato binário (não XML), *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de macro, *xlam* – um plug-in do Microsoft Excel 2007 com suporte de macro.

*md** – documentos e arquivos do Microsoft Office Access, como: *mda* – grupo de trabalho do Microsoft Office Access, mdb - banco de dados, etc.

sldx – um slide do Microsoft PowerPoint 2007.

sldm – um slide do Microsoft PowerPoint 2007 com suporte de macro.

thmx – um tema do Microsoft Office 2007.

Lembre-se de que o formato real de um arquivo pode não corresponder ao formato indicado por sua extensão.

A.2. Possíveis máscaras de exclusão de arquivos

Vamos examinar alguns exemplos de máscaras que podem ser usadas na criação de listas de exclusão de arquivos:

- Máscaras sem caminhos de arquivos:
    - ***.exe** - todos os arquivos com extensão *.exe*

- ***.ex?** – todos os arquivos com extensão *.ex?*, onde ? representa qualquer caractere
- **teste** - todos os arquivos com o nome *teste*

- Máscaras com caminhos de arquivos absolutos:
  - **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
  - **C:\dir*.exe** – todos os arquivos da pasta *C:\dir* com extensão .exe
  - **C:\dir*.ex?** – todos os arquivos com extensão .ex? da pasta *C:\dir*, onde ? representa qualquer caractere
  - **C:\dir\teste** - somente o arquivo *C:\dir\teste*
  - Se não desejar que o programa verifique os arquivos nas subpastas dessa pasta, desmarque ☑ **Incluir subpastas** ao criar a máscara.
- Máscaras com caminhos de arquivos relativos:
  - **dir*.***, **dir*** ou **dir** - todos os arquivos em todas as pastas de *dir*
  - **dir\teste** - todos os arquivos *teste* nas pastas *dir*
  - **dir*.exe** - todos os arquivos com a extensão *.exe* em todas as pastas *dir*
  - **dir*.ex?** – todos os arquivos com a extensão .ex? em todas as pastas *C:\dir\,* onde ? representa qualquer caractere

  Se não desejar que o programa verifique os arquivos nas subpastas dessa pasta, desmarque ☑ **Incluir subpastas** ao criar a máscara.

Dica:

As máscaras de exclusão *.* e * poderão ser usadas somente se você atribuir um veredito a uma ameaça excluída de acordo com a Enciclopédia de Vírus. Caso contrário, a ameaça especificada não será detectada em nenhum objeto. O uso dessas máscaras sem a escolha de um veredito basicamente desabilita o monitoramento.

Também não é recomendável selecionar uma unidade virtual criada com base em um diretório do sistema de arquivos que use o comando *subst* como exclusão. Não há motivo para fazer isso, pois durante a verificação o programa trata essa unidade virtual como uma pasta e a verifica.

A.3. Máscaras de exclusão possíveis de acordo com a classificação da Enciclopédia de Vírus

Ao adicionar ameaças com um determinado status na classificação da Enciclopédia de Vírus como exclusões, você pode especificar:

- o nome completo da ameaça, como aparece na Enciclopédia de Vírus (em inglês), em www.viruslist.com (por exemplo, **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**);
- o nome da ameaça por máscara. Por exemplo:
  - **not-a-virus*** – exclui programas possivelmente perigosos da verificação, além de programas de piadas.
  - ***Riskware.*** – exclui riskware da verificação.
  - ***RemoteAdmin.*** – exclui todos os programas de administração remota da verificação.

A.4. Visão geral das configurações em *setup.ini*

O arquivo *setup.ini*, localizado na pasta de instalação do Kaspersky Anti-Virus, é usado ao instalar o programa no modo não interativo do prompt de comando (consulte a seção 3.3 na p. 33) ou usando o Editor de Objeto de Diretiva de Grupo (consulte a seção 3.4 na p. 34). O arquivo contém as seguintes configurações:

[Setup] – configurações gerais de instalação do programa.

InstallDir=<caminho da pasta de instalação do programa>.

Reboot=yes|no – se o computador deve ser reiniciado depois da instalação do programa (não reinicia por padrão).

SelfProtection=yes|no – se o Kaspersky Anti-Virus deve habilitar a Autodefesa durante a instalação (habilitado por padrão).

MSExclusions=yes|no – se as exclusões recomendadas pela Microsoft para servidores devem ser adicionadas à lista de exclusões do Kaspersky Anti-Virus.

AddPath=yes|no – se o caminho de avp.com será adicionado à variável de ambiente do sistema %Path%.

[Components] – seleciona os componentes a serem instalados. Se esse grupo não contiver nenhum item, todos serão instalados.

FileMonitor=yes|no – instala o Antivírus de Arquivos.

[Tasks] – habilita as tarefas do Kaspersky Anti-Virus, caso nenhuma tarefa seja especificada; todas as tarefas serão executadas após a instalação. Se nenhuma tarefa for especificadas, todas as tarefas que não estão listadas serão desabilitadas.

ScanMyComputer=yes|no – tarefa de verificação completa do computador

ScanStartup=yes|no – tarefa de verificação dos objetos de inicialização

ScanCritical=yes|no – tarefa de verificação das áreas críticas

Updater=yes|no – tarefa de atualização das assinaturas de ameaças e módulos do programa

Em vez do valor **yes**, você pode usar os valores **1**, **on**, **enable** ou **enabled** e, em vez do valor **no**, pode usar **0**, **off**, **disable** ou **disabled** .

APÊNDICE B. KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab é conhecida como líder no segmento de tecnologias de segurança da informação. A empresa produz uma grande variedade de softwares de segurança de dados, fornecendo soluções abrangentes e de alto desempenho para a proteção de computadores e redes contra todos os tipos de programas mal-intencionados, mensagens de e-mail não solicitadas e indesejadas, e ataques de hackers.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa possui representações oficiais no Reino Unido, França, Alemanha, Japão, EUA (CA), Países Baixos, China, Polônia e Romênia. Um novo departamento da empresa foi aberto recentemente na França, o Centro Europeu de Pesquisa Antivírus. A rede de parceiros da Kaspersky Lab incorpora mais de 500 empresas no mundo inteiro.

Atualmente, a Kaspersky Lab emprega mais de 450 especialistas, todos peritos em tecnologias de antivírus, sendo que dez deles são graduados com MBAs, 16 com PhDs e vários especialistas sêniores, membros da Organização de Pesquisadores de Antivírus de Computador (Computer Anti-Virus Researchers Organization - CARO).

A Kaspersky Lab oferece as melhores soluções de segurança do mercado, com base em sua experiência única e nos conhecimentos obtidos em mais de 14 anos na batalha contra os vírus de computador. Uma análise completa das atividades de vírus de computador habilita a empresa a fornecer proteção abrangente contra ameaças atuais e futuras. A resistência a ataques futuros é a diretivo básica implementada em todos os produtos da Kaspersky Lab. Os produtos da empresa estão sempre pelo menos um passo à frente de vários outros fornecedores na oferta de cobertura abrangente de antivírus, tanto para usuários domésticos quanto para clientes corporativos.

Anos de muito trabalho fizeram da empresa um dos principais fabricantes de softwares de segurança. A Kaspersky Lab foi uma das primeiras empresas do segmento a desenvolver os mais altos padrões para a defesa antivírus. O principal produto da empresa, o Kaspersky Anti-Virus, fornece proteção integral para todos os níveis de uma rede, incluindo estações de trabalho, servidores de arquivos, sistemas de e-mail, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento convenientes e fáceis de usar asseguram a automação avançada para uma proteção rápida em toda a empresa. Vários fabricantes conhecidos usam o kernel do Kaspersky Anti-Virus, incluindo Nokia ICG (EUA), F-Secure (Finlândia), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab tiram proveito de uma vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a

conformidade com requisitos comerciais específicos. O banco de dados de antivírus da Kaspersky Lab é atualizado a cada hora. A empresa fornece a seus clientes serviço de suporte técnico 24 horas, disponível em vários idiomas para atender a seus clientes internacionais.

B.1. Outros produtos da Kaspersky Lab

Kaspersky Lab News Agent

O News Agent destina-se ao envio oportuno de notícias publicadas pela Kaspersky Lab, de notificações sobre o status atual das atividades de vírus e notícias recentes. O programa lê a lista de feeds de notícias disponíveis e seu conteúdo no servidor de notícias da Kaspersky Lab com a freqüência especificada.

O News Agent permite:

- Ver a previsão atual de vírus na bandeja do sistema
- Assinar e cancelar a assinatura de feeds de notícias
- Recuperar notícias de todos os feeds selecionados com a freqüência especificada e receber notificações sobre notícias recentes
- Examinar as notícias nos feeds selecionados
- Examinar a lista de feeds e seus status
- Abrir o texto completo do artigo no navegador

O News Agent é um aplicativo autônomo do Microsoft Windows que pode ser usado independentemente ou agregado com várias soluções integradas oferecidas pela Kaspersky Lab.

Kaspersky® OnLine Scanner

Este programa é um serviço gratuito oferecido aos visitantes do site corporativo da Kaspersky Lab. Ele permite uma verificação antivírus on-line eficiente de seu computador. O Kaspersky OnLine Scanner é executado diretamente no navegador da Web. Assim, os usuários sabem rapidamente as respostas às suas dúvidas referentes a possíveis infecções em seus computadores. Usando o serviço, os visitantes podem:

- Excluir arquivos comprimidos e bancos de dados de e-mail da verificação
- Selecionar bancos de dados padrão/estendido para a verificação
- Salvar um relatório sobre os resultados da verificação nos formatos txt ou html

Kaspersky® OnLine Scanner Pro

O programa é um serviço de assinatura disponível para os visitantes do site corporativo da Kaspersky Lab. Ele oferece uma verificação antivírus on-line eficiente de seu computador e a desinfecção de arquivos perigosos. O Kaspersky OnLine Scanner Pro é executado diretamente no navegador da Web. Usando o serviço, os visitantes podem:

- Excluir arquivos comprimidos e bancos de dados de e-mail da verificação
- Selecionar bancos de dados padrão/estendido para a verificação
- Salvar um relatório sobre os resultados da verificação nos formatos txt ou html

Kaspersky Anti-Virus® 7.0

O Kaspersky Anti-Virus 7.0 foi projetado para proteger PCs contra software mal-intencionado, combinando métodos convencionais de proteção antivírus e novas tecnologias proativas.

O programa oferece verificações antivírus complexas, incluindo:

- Verificação antivírus do tráfego de e-mail no nível do protocolo de transmissão de dados (POP3, IMAP e NNTP para e-mails recebidos e SMTP para mensagens enviadas), independentemente do programa de e-mail usado, bem como a desinfecção de bancos de dados de e-mail.
- Verificação antivírus em tempo real do tráfego da Internet transferido via HTTP.
- Verificação antivírus de arquivos, pastas ou unidades individuais. Além disso, uma tarefa de verificação predefinida pode ser usada para iniciar a análise de antivírus exclusivamente em áreas críticas do sistema operacional e em objetos de inicialização do Microsoft Windows.

A proteção proativa oferece os seguintes recursos:

Controle de alterações no sistema de arquivos. O programa permite que os usuários criem uma lista de aplicativos que serão controlados por componente. Isso ajuda a proteger a integridade dos aplicativos contra a influência de software mal-intencionado.

Monitoramento de processos na memória RAM. O Kaspersky Anti-Virus 7.0 notifica oportunamente os usuários sempre que detecta processos perigosos, suspeitos ou ocultos, ou quando ocorrem alterações não autorizadas de processos ativos.

Monitoramento de alterações no Registro do sistema operacional devido ao controle interno do Registro do sistema.

Monitoramento de processos ocultos ajuda a proteger de códigos mal-intencionados escondidos no sistema operacional utilizando tecnologias de rootkit.

Analisador heurístico. Ao verificar um programa, o analisador emula sua execução e registra toda a atividade suspeita, como a abertura ou gravação de um arquivo, a interrupção de interceptações de vetores etc. É tomada uma decisão com base neste procedimento com relação à possível infecção do programa por um vírus. A emulação ocorre em um ambiente virtual isolado que protege o computador contra infecções.

Restauração do sistema depois de ataques de malware, registrando todas as alterações do Registro e do sistema de arquivos do computador e revertendo-os conforme o desejo do usuário.

Kaspersky® Internet Security 7.0

O Kaspersky Internet Security 7.0 é uma solução integrada para a proteção de PCs contra as principais ameaças relacionadas a informações, como vírus, hackers, spams e spyware. Os usuários podem configurar e gerenciar todos os componentes do programa em uma única interface.

Os recursos de proteção antivírus incluem:

Verificação antivírus do tráfego de e-mail no nível do protocolo de transmissão de dados (POP3, IMAP e NNTP para e-mails recebidos e SMTP para mensagens enviadas), independentemente do programa de e-mail usado. O programa inclui plug-ins para os programas de e-mail conhecidos (como Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) e The Bat!) e dá suporte à desinfecção de seus bancos de dados de e-mail.

Verificação antivírus em tempo real do tráfego da Internet transferido via HTTP.

Proteção do sistema de arquivos: Verificação antivírus de arquivos, pastas ou unidades individuais. Além disso, o aplicativo pode executar a análise de antivírus exclusivamente em áreas críticas do sistema operacional e em objetos de inicialização do Microsoft Windows.

Proteção proativa: o programa monitora constantemente a atividade de aplicativos e processos em execução na memória RAM, evitando alterações perigosas ao sistema de arquivos e ao Registro, e restaura o sistemas após influências mal-intencionadas.

A **proteção contra fraudes da Internet** é garantida pelo reconhecimento de ataques de phishing, o que ajuda a evitar vazamentos de dados confidenciais (principalmente todos os números de senhas, contas bancárias e cartões de crédito) e bloquear a execução de scripts perigosos em páginas da Web, janelas pop-up e banners de anúncios. O recurso de **bloqueio de discagem automática** ajuda a identificar softwares que tentam usar o modem para

conexões não autorizadas ocultas com serviços telefônicos pagos e as bloqueia. O módulo *Controle de Privacidade* mantém suas informações confidenciais protegidas do acesso e da transmissão não autorizados. O *Controle dos Pais* é um componente do Kaspersky Internet Security que monitora o acesso do usuário à Internet.

O Kaspersky Internet Security 7.0 **registra as tentativas de verificar as portas do computador** que freqüentemente antecedem ataques de rede, protegendo-o desses ataques com êxito. O programa usa **regras definidas como base** para o controle de todas as transações de rede, rastreando todos os **pacotes de dados enviados e recebidos**. O **modo invisível** (devido à tecnologia SmartStealth™) **impede a detecção externa do computador**. Quando você alterna para o Modo Invisível, o sistema bloqueia toda a atividade de rede, exceto algumas transações permitidas nas regras definidas pelo usuário.

O programa utiliza uma abordagem inclusiva para a filtragem de spam das mensagens de e-mail recebidas:

- Verificação com relação às listas negra e branca de destinatários (incluindo endereços de sites de phishing)
- Inspeção de frases no corpo da mensagem
- Análise do texto da mensagem usando um algoritmo de aprendizagem
- Reconhecimento de spam enviado em arquivos de imagens

Kaspersky Anti-Virus Mobile

O Kaspersky® Anti-Virus Mobile oferece proteção antivírus para dispositivos móveis que executam os sistemas operacionais Symbian e Microsoft Windows Mobile. O programa oferece verificações de vírus abrangentes, incluindo:

- **Verificação por demanda** da memória on-board do dispositivo móvel, de cartões de memória, pastas individuais ou arquivos específicos; se for detectado um arquivo infectado, ele será movido para a Quarentena ou excluído
- **Verificação em tempo real –** todos os arquivos enviados e recebidos são verificados automaticamente, assim como os arquivos acessados
- **Proteção contra spam em mensagens de texto**

Kaspersky Anti-Virus for File Servers

Este pacote de softwares oferece uma proteção confiável para sistemas de arquivos em servidores que executam o Microsoft Windows, Novell NetWare, Linux e Samba contra todos os tipos de malware. O conjunto inclui os seguintes aplicativos da Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Recursos e funcionalidade:

- *Proteção dos sistemas de arquivos do servidor em tempo real*: Todos os arquivos do servidor são verificados ao serem abertos ou salvos no servidor;
- *Prevenção de surtos de vírus*;
- *Verificações por demanda* de todo o sistema de arquivos ou de pastas e arquivos individuais;
- *Utilização de tecnologias de otimização* ao verificar objetos no sistema de arquivos do servidor;
- *Reversão do sistema após ataques de vírus*;
- *Escalabilidade do pacote de software* no escopo dos recursos do sistema disponíveis;
- *Monitoramento do balanceamento de carga do sistema*;
- *Criação de uma lista de processos confiáveis* cuja atividade no servidor não é controlada pelo pacote de software;
- *Administração remota* do pacote de software, incluindo a instalação, configuração e administração centralizada;
- *Gravação de cópias de backup de objetos infectados e excluídos* caso seja necessário restaurá-los;
- *Armazenamento de objetos suspeitos na Quarentena*;
- *Envio de notificações em eventos* de funcionamento do programa para o administrador do sistema;
- *Registro de relatórios detalhados*;
- *Atualização automática* dos bancos de dados do programa.

Kaspersky Open Space Security

O Kaspersky Open Space Security é um pacote de software com uma nova abordagem à segurança para as redes corporativas atuais de qualquer

dimensão, oferecendo proteção centralizada dos sistemas de informação e suporte para escritórios remotos e usuários móveis.

O conjunto inclui quatro programas:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

As especificidades de cada programa são apresentadas a seguir.

O **Kaspersky WorkSpace Security** é um programa para a proteção centralizada de estações de trabalho dentro e fora de redes corporativas contra todas as ameaças atuais da Internet (vírus, spyware, ataques de hackers e spam).

Recursos e funcionalidade:

- *Proteção abrangente contra vírus, spyware, ataques de hackers e spam*;
- *Defesa Proativa contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;*
- *Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;*
- *Reversão de modificações mal-intencionadas ao sistema;*
- *Proteção contra ataques de phishing e lixo eletrônico;*
- *Redistribuição dinâmica de recursos durante as verificações completas do sistema;*
- *Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;*
- *Suporte para Cisco® NAC (Network Admission Control);*
- *Verificação de e-mails e do tráfego da Internet em tempo real;*
- *Bloqueio de janelas pop-up e banners de anúncios na Internet;*
- *Operação segura em qualquer tipo de rede, inclusive Wi-Fi;*
- *Ferramentas de criação de disco de recuperação que permitem restaurar o sistema após um surto de vírus;*
- *Um abrangente sistema de relatórios sobre o status da proteção;*

- *Atualizações automáticas do banco de dados;*
- *Suporte completo para sistemas operacionais de 64 bits;*
- *Otimização do desempenho do programa em notebooks (tecnologia Intel® Centrino® Duo);*
- *Recurso de desinfecção remota (Intel® Active Management, Intel® vPro™).*

O **Kaspersky Business Space Security** oferece a proteção ideal para os recursos de informação de sua empresa contra as ameaças atuais da Internet. O Kaspersky Business Space Security protege estações de trabalho e servidores de arquivos de todos os tipos de vírus, cavalos de Tróia e worms, evita surtos de vírus e protege as informações, fornecendo acesso instantâneo aos recursos de rede.

Recursos e funcionalidade:

- *Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;*
- *Suporte para Cisco® NAC (Network Admission Control);*
- *Proteção de estações de trabalho e servidores de arquivos de todos os tipos de ameaças da Internet;*
- *Tecnologia iSwift para evitar repetir a verificação de arquivos na rede;*
- *Distribuição de carga entre os processadores do servidor;*
- *Armazenamento de objetos suspeitos das estações de trabalho em quarentena;*
- *Reversão de modificações mal-intencionadas ao sistema;*
- *Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;*
- *Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;*
- *Verificação de e-mails e do tráfego da Internet em tempo real;*
- *Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;*
- *Proteção ao usar redes Wi-Fi;*
- *Autodefesa contra programas mal-intencionados;*

- *Armazenamento de objetos suspeitos na Quarentena;*
- *Atualizações automáticas do banco de dados.*

Kaspersky Enterprise Space Security

Este programa inclui componentes para a proteção de estações de trabalho e servidores conectados contra todas as ameaças atuais da Internet. Ele exclui vírus dos e-mails, mantendo as informações protegidas e fornecendo acesso seguro aos recursos de rede.

Recursos e funcionalidade:

- *Proteção de estações de trabalho e servidores de arquivos contra vírus, cavalos de Tróia e worms;*
- *Proteção dos servidores de e-mail Sendmail, Qmail, Postfix e Exim;*
- *Verificação de todos os e-mails no Microsoft Exchange Server, incluindo as pastas compartilhadas;*
- *Processamento de e-mails, bancos de dados e outros objetos de servidores Lotus Domino;*
- *Proteção contra ataques de phishing e lixo eletrônico;*
- *Prevenção de envio de e-mails em massa e surtos de vírus;*
- *Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;*
- *Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;*
- *Suporte para Cisco® NAC (Network Admission Control);*
- *Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;*
- *Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;*
- *Operação segura ao usar redes Wi-Fi;*
- *Verificação do tráfego da Internet em tempo real;*
- *Reversão de modificações mal-intencionadas ao sistema;*

- *Redistribuição dinâmica de recursos durante as verificações completas do sistema;*
- *Armazenamento de objetos suspeitos na Quarentena;*
- *Um abrangente sistema de relatórios sobre o status da proteção do sistema;*
- *Atualizações automáticas do banco de dados.*

Kaspersky Total Space Security

Esta solução monitora todos os fluxos de dados enviados e recebidos (e-mail, Internet e todas as interações de rede). Ela inclui componentes para a proteção de estações de trabalho e dispositivo móveis, mantém as informações protegidas e oferece acesso seguro aos recursos de informação da empresa e à Internet, além de garantir comunicações seguras por e-mail.

Recursos e funcionalidade:

- *Proteção abrangente contra vírus, spyware, ataques de hackers e spam em todos os níveis da rede corporativa, das estações de trabalho aos gateways da Internet;*
- *Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;*
- *Proteção dos servidores de e-mail e servidores conectados;*
- *Verificação do tráfego da Internet (HTTP/FTP) que entra na rede local em tempo real;*
- *Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;*
- *Bloqueio do acesso de estações de trabalho infectadas;*
- *Prevenção de surtos de vírus;*
- *Relatórios centralizados sobre o status da proteção;*
- *Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;*
- *Suporte para Cisco® NAC (Network Admission Control);*
- *Suporte para hardware de servidores proxy;*
- *Filtragem do tráfego da Internet usando uma lista de servidores, tipos de objetos e grupos de usuários confiáveis;*

- *Tecnologia iSwift para evitar repetir a verificação de arquivos na rede;*
- *Redistribuição dinâmica de recursos durante as verificações completas do sistema;*
- *Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;*
- *Operação segura para usuários em qualquer tipo de rede, inclusive Wi-Fi;*
- *Proteção contra ataques de phishing e lixo eletrônico;*
- *Recurso de desinfecção remota (Intel® Active Management, Intel® vPro™);*
- *Reversão de modificações mal-intencionadas ao sistema;*
- *Autodefesa contra programas mal-intencionados;*
- *Suporte completo para sistemas operacionais de 64 bits*;
- *Atualizações automáticas do banco de dados*;

Kaspersky Security for Mail Servers

Este programa protege servidores de e-mail e servidores conectados contra programas mal-intencionados e spam. O programa inclui aplicativos para a proteção de todos os servidores de e-mail padrão (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix e Exim), além de permitir a configuração de um gateway de e-mail dedicado. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Seus recursos incluem:

- *Proteção confiável contra programas mal-intencionados ou possivelmente perigosos*;
- *Filtragem de lixo eletrônico*;
- *Verificação de e-mails e anexos enviados e recebidos*;
- *Verificação de todos os e-mails* no Microsoft Exchange Server quanto à presença de vírus, incluindo as pastas compartilhadas;

- *Processamento de e-mails, bancos de dados e outros objetos de servidores Lotus Domino*;
- *Filtragem* de e-mails por tipo de anexo;
- Armazenamento de objetos suspeitos na *Quarentena*;
- *Sistema de administração do programa fácil de usar*;
- *Prevenção de surtos de vírus*
- *Monitoramento do status de proteção do sistema* usando notificações;
- *Sistema de relatórios* de funcionamento do programa;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;
- *Atualizações automáticas do banco de dados*;

Kaspersky Security for Internet Gateways

Este programa oferece acesso seguro à Internet para todos os funcionários da organização, excluindo automaticamente os malwares e riskwares dos dados recebidos por HTTP/FTP. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Seus recursos incluem:

- *Proteção confiável contra programas mal-intencionados ou possivelmente perigosos*;
- *Verificação do tráfego da Internet* (HTTP / FTP) em tempo real;
- *Filtragem do tráfego da Internet* usando uma lista de servidores, tipos de objetos e grupos de usuários confiáveis;
- Armazenamento de objetos suspeitos na *Quarentena*;
- *Sistema de administração fácil de usar*;
- *Sistema de relatórios de funcionamento do programa*;
- *Suporte para hardware de servidores proxy*;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;

- *Atualizações automáticas do banco de dados*.

Kaspersky® Anti-Spam

O Kaspersky® Anti-Spam é um conjunto inovador de softwares projetado para ajudar as organizações com redes de pequeno e médio porte na batalha contra os ataques de e-mail indesejados (spam). O produto combina a revolucionária tecnologia de análise lingüística com métodos modernos de filtragem de e-mail, incluindo listas negras de DNS e recursos de cartas formais. Sua exclusiva combinação de serviços permite aos usuários identificar e eliminar até 95% do tráfego indesejado.

O Kaspersky® Anti-Spam, instalado na entrada de uma rede, onde monitora spams no tráfego de e-mail recebido, atua como uma barreira aos e-mails não solicitados. O produto é compatível com qualquer sistema de e-mail e pode ser instalado em servidores de e-mail existentes ou em dedicados.

O alto desempenho do Kaspersky® Anti-Spam é assegurado por atualizações diárias do banco de dados de filtragem de conteúdo, adicionando amostras fornecidas pelos especialistas do laboratório de lingüística da empresa. Os bancos de dados são atualizados a cada 20 minutos.

Kaspersky Anti-Virus® for MIMESweeper

O Kaspersky Anti-Virus® for MIMESweeper fornece verificação em alta velocidade do tráfego em servidores que executam o Clearswift MIMESweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

O programa é um plug-in e verifica vírus e processa o tráfego de e-mail enviado e recebido em tempo real.

B.2. Entre em contato conosco

Se tiver dúvidas, comentários ou sugestões, envie-os para um de nossos distribuidores ou diretamente para a Kaspersky Lab. Será um prazer ajudá-lo em qualquer assunto relacionado ao nosso produto, por telefone ou e-mail. Esteja certo de que todas as recomendações e sugestões serão analisadas e consideradas.

Suporte técnico	Consulte as informações de suporte técnico em http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html

Informaçõe s gerais	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APÊNDICE C. CONTRATO DE LICENÇA

Contrato de Licença do Usuário Final Padrão

AVISO A TODOS OS USUÁRIOS: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") RELATIVO À LICENÇA DO KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS (“SOFTWARE”), PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE VOCÊ ADQUIRIU ESTE SOFTWARE PELA INTERNET, CLICANDO NO BOTÃO ACEITAR, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DO PRESENTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DO CONTRATO E NÃO INSTALE O SOFTWARE.

SE VOCÊ ADQUIRIU ESTE SOFTWARE EM UMA MÍDIA FÍSICA, AO QUEBRAR O LACRE DO CD, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDA COM TODOS OS TERMOS DESTE CONTRATO, NÃO QUEBRE O LACRE DO CD, NÃO FAÇA DOWNLOAD, INSTALE OU USE ESTE SOFTWARE.

DE ACORDO COM A LEGISLAÇÃO RELATIVA AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS E COMPRADOS NO SITE DA KASPERSKY LAB OU DE SEUS PARCEIROS, O CLIENTE DEVERÁ TER UM PERÍODO DO CATORZE (14) DIAS ÚTEIS A PARTIR DA ENTREGA DO PRODUTO PARA DEVOLVÊ-LO AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE O SOFTWARE ESTEJA SELADO.

COM RELAÇÃO AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS NÃO ADQUIRIDO ON-LINE, PELA INTERNET, ESSE SOFTWARE NÃO PODERÁ SER DEVOLVIDO OU TROCADO, EXCETO POR PROVISÕES CONTRÁRIAS DO PARCEIRO QUE COMERCIALIZA O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO ESTARÁ SUJEITA ÀS CLÁUSULAS DO PARCEIRO.

O DIREITO DE DEVOLUÇÃO E REEMBOLSO SE ESTENDE APENAS AO COMPRADOR ORIGINAL.

1. *Concessão de Licença*. Sujeito ao pagamento das taxas de licença aplicáveis e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede a você, por meio da presente, o direito não exclusivo e intransferível de usar uma cópia da versão especificada do Software e a documentação que o acompanha

(a “Documentação”) durante a vigência deste Contrato, unicamente para seus próprios fins comerciais internos.

1.1 *Uso*. O número de computadores que o Usuário pode proteger com o Software é especificado no Arquivo da chave de licença e indicado na janela “Serviço”. O Software não pode ser usado para proteger redes com um número de servidores de arquivos maior que esse.

1.1.1 O Software está “em uso” em um computador quando está carregado na memória temporária (ou seja, a memória RAM) ou instalado na memória permanente (por exemplo, no disco rígido, no CD-ROM ou em outro dispositivo de armazenamento) desse computador. Esta licença o autoriza a fazer quantas cópias de backup do Software forem necessárias para sua utilização dentro dos termos da lei e unicamente para fins de backup, desde que todas essas cópias contenham todos os avisos sobre propriedade do Software. Você deverá manter registros do número e do local de todas as cópias do Software e da Documentação, e deverá adotar todas as precauções necessárias para proteger o Software de uso ou cópia não autorizados.

1.1.2 O Software protege o computador contra vírus cujas assinaturas estão contidas nos bancos de dados de assinaturas de ameaças disponíveis nos servidores de atualização da Kaspersky Lab.

1.1.3 Se você vender o computador no qual o Software está instalado, deverá verificar se todas as cópias do Software foram excluídas anteriormente.

1.1.4 Você não deverá descompilar, aplicar engenharia reversa, desmontar ou reduzir de qualquer outra forma qualquer parte deste Software a um formato legível, nem permitir que qualquer terceiro o faça. As informações de interface necessárias para obter a interoperabilidade do Software com programas de computador criados independentemente serão fornecidas pela Kaspersky Lab quando solicitado, mediante pagamento dos custos plausíveis e das despesas relativas à busca e ao fornecimento dessas informações. No caso de a Kaspersky Lab o notificar de que não pretende disponibilizar essas informações por qualquer motivo, incluindo custos (sem limitações), deverá ser permitido que você tome as medidas necessárias para conseguir a interoperabilidade, desde que seja feita a engenharia reversa ou descompilação do Software apenas até os limites permitidos pela lei.

1.1.5 Você não poderá fazer correções de erros ou de alguma outra forma modificar, adaptar ou converter o Software, nem criar trabalhos derivados do mesmo, nem permitir que terceiros o copiem (a menos que expressamente permitido pelo presente).

1.1.6 Você não poderá alugar, locar ou emprestar o Software a terceiros, nem transferir ou sublicenciar seus direitos de licença a qualquer outra pessoa.

1.1.7 Você não deverá usar este Software em ferramentas automáticas, semi-automáticas ou manuais projetadas para criar assinaturas de vírus, rotinas de

detecção de vírus, qualquer outro código ou dados para detecção de código ou dados mal-intencionados.

1.1.8 A Kaspersky Lab pode solicitar que o Usuário instale a versão mais recente do Software (a versão e o pacote de manutenção mais recentes).

1.1.9 Remoção de produtos potencialmente nocivos. Você aceita e concorda que, além de detectar software nocivo e mal-intencionado, o Produto também pode identificar, remover e/ou desabilitar produtos potencialmente nocivos, incluindo aqueles considerados ou classificados como Adware, Riskware, Pornware, etc.

2. *Suporte*.

(i) A Kaspersky fornecerá serviços de suporte ("Serviços de Suporte") conforme definido a seguir, por um período especificado no arquivo da chave de licença e indicado na janela "Serviço", a partir do momento da compra, desde:

   (a) o pagamento dos então atuais encargos relativos ao suporte e:

   (b) O serviço de suporte técnico da Kaspersky Lab também é liberado para solicitações a partir do registro adicional do Usuário Final para concessão de identificador para o fornecimento de Serviços de Suporte.

   (c) Até a ativação do Software e/ou a obtenção do identificador do Usuário Final (Identificação do Cliente), o serviço de suporte técnico oferece assistência apenas na ativação do Software e no registro do Usuário Final.

(ii) Ao preencher o Formulário de Assinatura de Serviços de Suporte, você concorda com os termos da Diretiva de Privacidade da Kaspersky Lab, localizada em www.kaspersky.com/privacy, e concorda explicitamente com a transferência de dados para outros países, diferentes do seu, conforme definido na Diretiva de Privacidade.

(iii) Os Serviços de Suporte serão encerrados, a menos que sejam renovados anualmente, com o pagamento dos então atuais encargos de suporte anuais e o novo preenchimento bem-sucedido do Formulário de Assinatura de Serviços de Suporte.

(iv) Por "Serviços de Suporte" entendem-se:

   (a) Atualizações a cada hora do banco de dados de antivírus;

   (b) Atualizações gratuitas de software, incluindo as atualizações de versão;

   (c) Suporte técnico pela Internet e pela linha direta de suporte fornecida pelo Fornecedor e/ou Revendedor;

(d) Atualizações de detecção e desinfecção de vírus 24 horas por dia.

(v) Os Serviços de Suporte serão fornecidos somente se e quando você tiver a versão mais recente do Software (incluindo os pacotes de manutenção), disponível no site oficial da Kaspersky Lab (www.kaspersky.com), instalado no seu computador.

3. *Direitos de Propriedade*. O Software é protegido por leis de direitos autorais. A Kaspersky Lab e seus fornecedores possuem e detêm todos os direitos, títulos de interesses no e para o Software, incluindo todos os direitos autorais, patentes, marcas comerciais e outros direitos de propriedade intelectual relacionados. A posse, instalação ou uso do Software por você não lhe transfere qualquer título à propriedade intelectual do Software, e você não adquirirá quaisquer direitos ao Software, exceto aqueles expressamente definidos no presente Contrato.

4. *Confidencialidade*. Você concorda que o Software e a Documentação, incluindo o projeto e a estrutura específicos de programas individuais, constituem informações proprietárias confidenciais da Kaspersky Lab. Você não deverá divulgar, fornecer ou disponibilizar de qualquer outra maneira essas informações confidenciais, em qualquer forma, para terceiros, sem o consentimento prévio por escrito da Kaspersky Lab. Você deverá implementar medidas de segurança aceitáveis para proteger essas informações confidenciais mas, sem limitação a isso, deverá usar os melhores meios para manter a segurança do código de ativação.

5. *Garantia Limitada*.

(i) A Kaspersky Lab garante que, por seis (6) meses a partir do primeiro download ou da instalação, o Software adquirido em mídia física terá um desempenho significativamente de acordo com a funcionalidade descrita na Documentação, quando operado corretamente e da forma especificada na Documentação.

(ii) Você assume toda a responsabilidade pela seleção deste Software para preencher seus requisitos. A Kaspersky Lab não garante que o Software e/ou a Documentação serão adequados para suas necessidades, nem que sua utilização será ininterrupta ou isenta de erros.

(iii) A Kaspersky Lab não garante que este Software identifique todos os vírus conhecidos, nem que ocasionalmente o Software não possa relatar erroneamente um vírus em um título não infectado por esse vírus.

(iv) A Kaspersky Lab não garante que este Software ofereça proteção após sua data de expiração (consulte a seção.2 (i))

(v) A única solução e toda a responsabilidade da Kaspersky Lab por violações da garantia descrita no parágrafo (i) será, como opção da Kaspersky Lab, que ela repare, substitua ou reembolse o Software, se tal

fato for relatado à Kaspersky Lab ou seu representante durante o período da garantia. Você deverá fornecer todas as informações necessárias satisfatórias para auxiliar o Fornecedor na resolução do item com defeito.

(vi) A garantia (i) não se aplicará se você (a) fizer ou causar alterações neste Software sem o consentimento da Kaspersky Lab, (b) usar o Software de uma forma para a qual ele não se destina ou (c) usar o Software de forma diferente daquela permitida por este Contrato.

(vii) As garantias e condições declaradas neste Contrato substituem todas as outras condições, garantias ou outros termos relativos ao fornecimento ou suposto fornecimento de, à falha ou atraso no fornecimento do Software ou da Documentação que podem, exceto por este parágrafo (vi), ter valor entre a Kaspersky Lab e você, ou que de outra forma poderiam estar implícitas ou incorporadas neste Contrato ou em qualquer contrato paralelo, seja por estatuto, pela lei comum ou outra, todos excluídos pela presente (incluindo, sem limitações, as condições, garantias ou outros termos implícitos, como os relativos à qualidade satisfatória, adequação às finalidades ou ao uso de habilidades e cuidados satisfatórios).

6. *Limitação de Responsabilidade*.

(i) Nenhuma parte deste Contrato excluirá ou limitará a responsabilidade da Kaspersky Lab por (a) delitos de fraude, (b) morte ou danos pessoais causados por violações de “duty of care” da lei comum ou de qualquer violação por negligência de um termo deste Contrato ou (c) qualquer outra responsabilidade que não possa ser excluída pela lei.

(ii) Sujeita ao parágrafo (i) acima, a Kaspersky Lab não se responsabilizará (seja por contrato, agravo, restituição ou outros) por nenhuma das seguintes perdas e danos (quer essas perdas e danos tenham sido previstos, previsíveis, conhecidos ou de outra forma):

(a) Perda de rendimentos;

(b) Perda de lucros reais ou previstos (incluindo a perda de lucros em contratos);

(c) Perda do uso de dinheiro;

(d) Perda de economias previstas;

(e) Perda de negócios;

(f) Perda de oportunidades;

(g) Perda de boa-fé;

(h) Perda de reputação;

(i) Perda de, danos a ou corrupção de dados ou:

(j) Qualquer perda ou dano indireto ou conseqüente causado de alguma forma (incluindo, para evitar dúvidas, os casos em que

essas perdas e danos sejam dos tipos especificados nos parágrafos (ii), (a) a (ii), (i).

(iii) Sujeita ao parágrafo (i), a responsabilidade da Kaspersky Lab (seja por contrato, agravo, restituição ou outros) decorrente de ou em correlação com o fornecimento do Software em nenhuma circunstância excederá o valor igual ao igualmente pago por você pelo Software.

7. Neste Contrato está contido o entendimento integral entre as partes com relação ao assunto do mesmo, tendo prevalência sobre todos e quaisquer entendimentos, compromissos e promessas anteriores entre você e a Kaspersky Lab, sejam eles orais ou por escrito, que tenham sido definidos ou que possam estar implícitos em qualquer elemento escrito ou declarado nas negociações entre nós ou nossos representantes antes deste Contrato e todos os contratos anteriores entre as partes, relacionados aos assuntos mencionados previamente terão sua validade suspensa a partir da Data de Efetivação.

O uso do software de demonstração, não lhe concedo o direito ao Suporte Técnico especificado na Cláusula 2 deste EULA, nem o direito de vender essa cópia a terceiros.

Você tem o direito de usar o software para fins de demonstração, durante o período especificado no arquivo da chave de licença, a partir do momento da ativação (esse período pode ser exibido na janela Serviço da interface do usuário do software).