KASPERSKY LAB

Kaspersky Mobile Security 7.0 Enterprise Edition

MANUAL DE ADMINISTRADOR

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Manual de Administrador

http://www.kaspersky.pt/

Data de Revisão: Novembro de 2009

Índice

CAPÍTULO 1. GESTÃO ATRAVÉS DO KASPERSKY ADMINISTRATION KIT

O **Kaspersky Administration Kit** é um sistema que fornece uma ferramenta centralizada para executar as principais tarefas administrativas relacionadas com a gestão do sistema de segurança de dispositivos móveis.

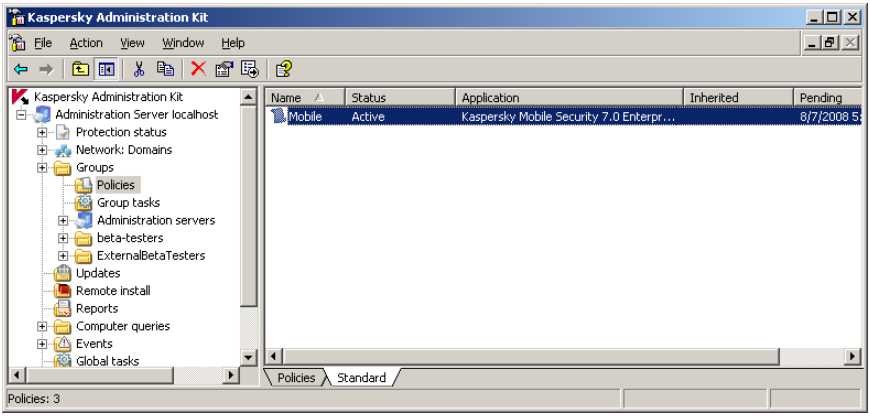

Figura 1. Consola de Administração do Kaspersky Administration Kit

No caso da administração centralizada através do Kaspersky Administration Kit, o Administrador determina as configurações das políticas e da aplicação. A protecção baseia-se nestas configurações.

Uma particularidade da administração centralizada é a organização dos dispositivos móveis em grupos e a gestão das suas configurações através da criação e definição de políticas de grupo.

Uma Política – é um conjunto de configurações do Kaspersky Mobile Security num grupo da rede lógica. As políticas são transferidas para o dispositivo móvel no decorrer de qualquer tipo de sincronização do dispositivo com o Servidor de Administração.

Nota

Para garantir que o Kaspersky Administration Kit detecta dispositivos móveis, abra o separador **Configurações** na janela de propriedades do Servidor de Administração e assinale a caixa **Porta aberta para dispositivos móveis**.

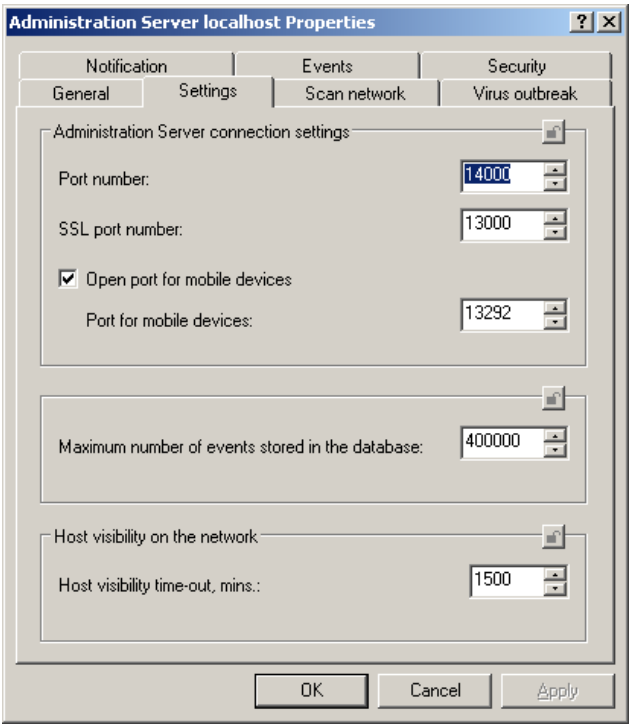

Figura 2. Separador **Configurações**

Nota!

Os dispositivos móveis ligam-se ao Servidor de Administração através do protocolo SSL. Para estabelecer este tipo de ligação, você precisa de um certificado no Servidor.

Para criar um certificado para dispositivos móveis:

1. Abra a pasta de instalação do Kaspersky Administration Kit.
2. Execute o utilitário *klmblcrt.exe*.
3. Especifique o endereço do Servidor de Administração na janela do assistente de criação do certificado que se abre (ver Figura 3)

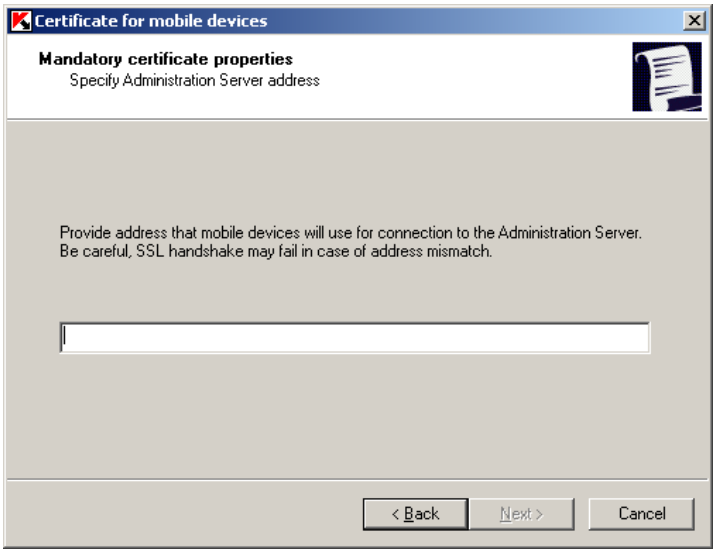

Figura 3. Criar um certificado para dispositivos móveis

4. Siga os passos do assistente para concluir a criação do certificado.

CAPÍTULO 2. DESENVOLVIMENTO DA APLICAÇÃO

Nota!

A instalação remota do Kaspersky Mobile Security é impossível se o plugin de administração do Kaspersky Mobile Security não estiver instalado na área de trabalho do administrador. O pacote de instalação do plugin está incluído no kit de distribuição do Kaspersky Mobile Security e encontra-se na pasta Plugin.

Esta secção descreve a instalação do Kaspersky Mobile Security através de uma tarefa de instalação remota e utilizando uma mensagem SMS.

2.1. Criar um pacote de instalação

A instalação remota da aplicação é efectuada através de um pacote de instalação.

Para criar um pacote de instalação:

1. Ligue-se ao Servidor de Administração.
2. Seleccione o módulo **Instalação remota** na árvore da consola, abra o menu de atalho e seleccione o comando **Novo** → **Pacote de Instalação** ou use o item correspondente no menu **Acções**. Isto irá iniciar o assistente. Siga as respectivas instruções.
3. Ser-lhe-á dada a opção de especificar o nome do pacote de distribuição e especificar a aplicação a instalar durante o passo seguinte (ver Figura 4).
4. Através da lista suspensa, seleccione a opção: **Criar pacote de instalação para a aplicação da Kaspersky Lab.** Através do botão **Procurar** seleccione o ficheiro que contém a descrição da aplicação (este ficheiro tem a extensão **.kpd** e está incluído no pacote de distribuição da aplicação). Como resultado, os campos do nome da aplicação e do número da versão serão automaticamente preenchidos.

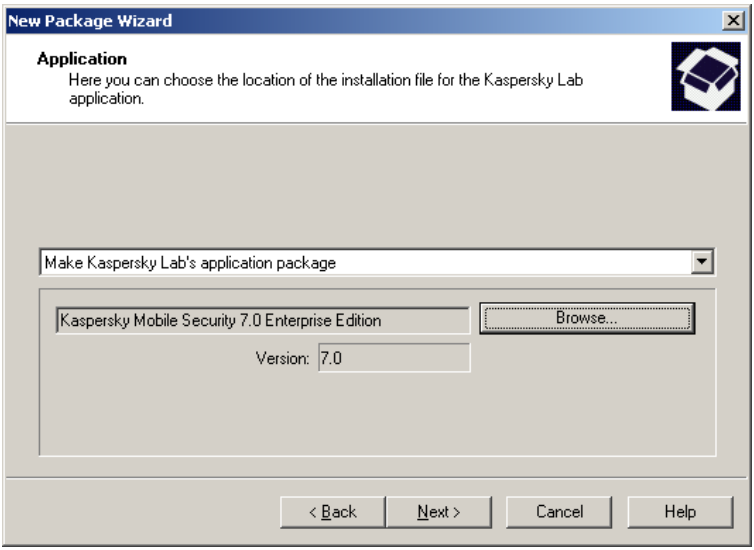

Figura 4. Criar um pacote de instalação. Seleccionar a aplicação a instalar

5. Depois disto, será transferido para uma pasta pública do Servidor de Administração um conjunto de ficheiros necessários para a instalação da aplicação em dispositivos móveis.

Após conclusão do assistente, o pacote de instalação criado será adicionado ao modo **Instalação remota** e estará visível no painel de resultados.

2.2. Instalar a aplicação através de uma tarefa de instalação remota

A instalação da aplicação através de uma tarefa de instalação remota é utilizada quando os dispositivos móveis estão ligados à rede lógica dos computadores. A instalação da aplicação é efectuada no momento em que o dispositivo é ligado ao computador.

Ao executar a tarefa, a instalação remota do software nos computadores cliente pode ser efectuada através de um de dois métodos: o método de *instalação forçada* ou *instalação através de um script de inicialização*.

A *instalação forçada* é utilizada para executar uma instalação remota do software nos computadores cliente específicos da rede lógica. Quando a tarefa é inicializada, o Servidor de Administração copia um conjunto de ficheiros necessários para a instalação a partir da pasta pública para uma pasta temporária em cada computador cliente e inicia o programa de instalação em cada computador. Para garantir o sucesso da tarefa de instalação forçada, o Servidor de Administração tem de ter os privilégios de um administrador local nos computadores cliente da rede lógica. Este método é utilizado para a instalação remota da aplicação em computadores com o Microsoft Windows NT/2000/2003/XP, que suportam esta funcionalidade ou em computadores com o Microsoft Windows 98/Me com o Agente de Rede instalado.

Nota!

Se a ligação entre o Servidor de Administração e o computador cliente for estabelecida através da Internet ou protegida com uma firewall, as pastas públicas não podem ser utilizadas para transferência de dados. Neste caso, os ficheiros necessários para a instalação têm de ser entregues ao computador cliente através do Agente de Rede. A instalação do Agente de Rede nesses computadores é executada localmente.

O segundo método – *instalação através de um script de inicialização* – permite atribuir a inicialização da tarefa de instalação remota a uma conta de utilizador específica (ou contas de utilizador). Como resultado da execução desta tarefa, no script de inicialização para os utilizadores especificados será criado um registo sobre a inicialização do pacote de instalação existente na pasta de acesso público do Servidor de Administração. Para a execução bem-sucedida desta tarefa, a conta com a qual a tarefa é executada ou o Servidor de Administração têm de ter privilégios para alterar scripts de inicialização na base de dados do controlador de domínio. Estes privilégios são concedidos ao administrador de domínio e a tarefa ou o Servidor de Administração na sua totalidade têm de ser iniciados com os direitos desse utilizador. Como resultado, quando o utilizador se regista com o domínio, será efectuada uma tentativa para instalar a aplicação no computador cliente a partir do qual o utilizador foi registado. Este método é recomendado para a instalação das aplicações da Kaspersky Lab em computadores com o Microsoft Windows 98/Me.

Nota!

Para a execução bem-sucedida da tarefa de instalação remota através de um script de inicialização, os utilizadores, para os quais são inseridas alterações nos scripts, têm de possuir direitos de administradores locais nos seus computadores.

As tarefas de grupo de instalação remota do software nos computadores cliente são executadas somente através do método de instalação forçada. Ao criar uma

tarefa global, você pode seleccionar o método desejado: o método de *instalação forçada* ou de *instalação através de um script de inicialização*.

Para criar uma tarefa global de instalação remota através do método de instalação forçada:

1. Ligue-se ao Servidor de Administração.
2. Seleccione o nódulo **Tarefas globais** na árvore da consola, abra o menu de atalho e seleccione o comando **Novo/Tarefa** ou use o item correspondente no menu **Acções**. Isto irá iniciar o assistente. Siga as respectivas instruções.
3. Especifique o nome da tarefa.
4. Ao seleccionar a aplicação e ao determinar o tipo de tarefa (ver Figura 5) defina os valores **Kaspersky Administration Kit** e **Instalação remota da aplicação** respectivamente.
5. Depois disto, especifique o pacote de instalação cuja instalação irá decorrer durante a execução desta tarefa (ver Figura 6). Seleccione o pacote criado para este Servidor de Administração ou crie um novo através do botão **Novo**.

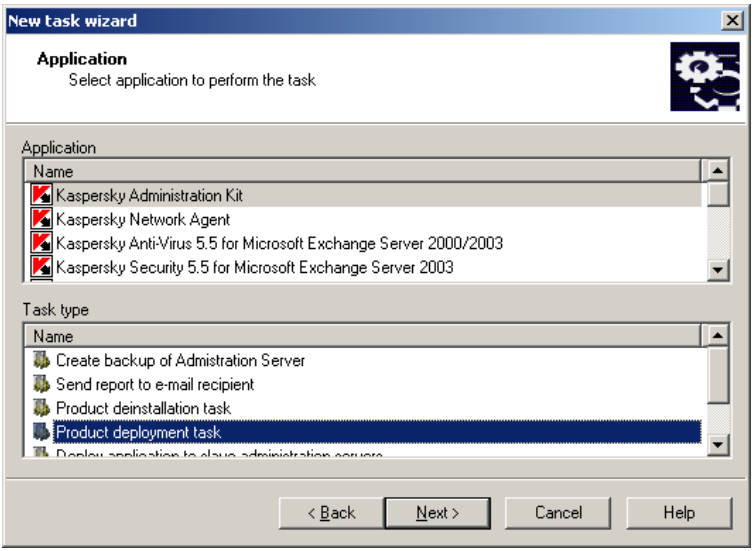

Figura 5. Determinar o tipo de tarefa

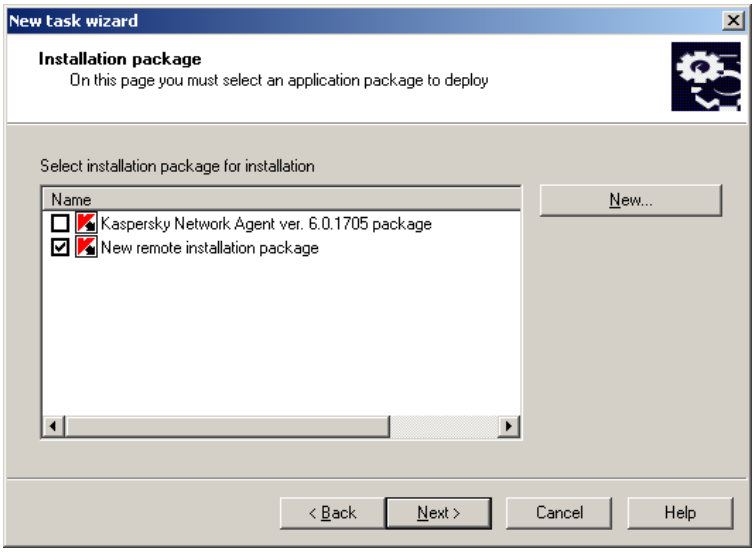

Figura 6. Seleccionar um pacote de instalação a instalar

6. Nesta etapa, seleccione a opção **Instalação forçada** (ver Figura 7).

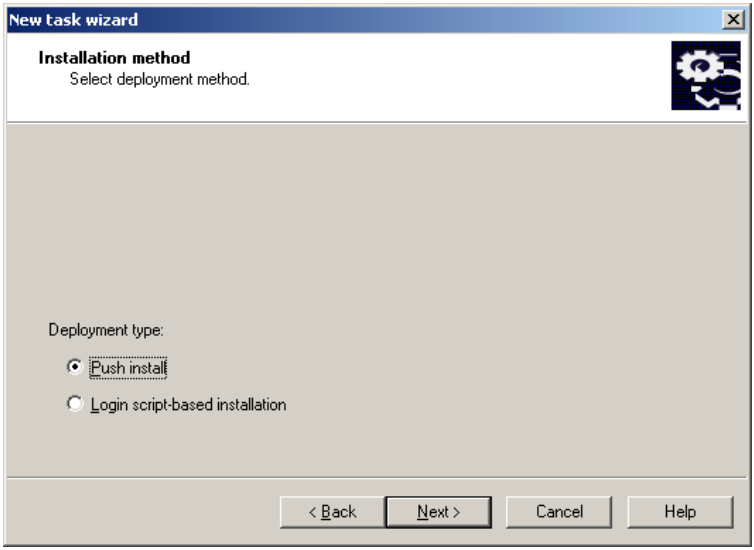

Figura 7. Determinar o tipo de instalação

7. Nesta janela do assistente, (ver Figura 8) ser-lhe-á dada a possibilidade de determinar opções adicionais de instalação:

   - Se precisa de reinstalar a aplicação, caso esta já tenha sido instalada no computador;

   - Assinale a caixa **Não instalar a aplicação se já estiver instalada** para evitar a instalação repetida da aplicação (por defeito, a caixa está assinalada). Neste caso, a tarefa não será iniciada para os computadores nos quais a aplicação já esteja instalada localmente ou como resultado da tarefa de instalação remota previamente iniciada.

     Se a caixa estiver desmarcada, a tarefa de instalação remota agendada será iniciada até que o número de tentativas de instalação tenha sido esgotado.

   - Defina o método a utilizar para entregar os ficheiros necessários para instalar a aplicação nos computadores cliente;

     Para o fazer, execute as seguintes acções no grupo de campos **Transferência do pacote de instalação**:

     - Assinale a caixa **Com ferramentas do Windows a partir da pasta de acesso público**, caso deseje que os ficheiros necessários para remover o programa sejam copiados para os computadores cliente com as ferramentas do Windows a partir da pasta de acesso público (assinalada por defeito). Esta opção de transferência é recomendada caso o Agente de Rede ligado ao Servidor de Administração específico não esteja instalado no computador onde está a ser executada a instalação.

     - Assinale a caixa **Através do Agente de Administração**, caso deseje entregar os ficheiros aos computadores cliente através do Agente de Administração instalado em cada um deles (assinalada por defeito). O Agente de Rede tem de estar ligado ao Servidor de Administração específico.

     - No campo **Número máximo de transferências em simultâneo** especifique o número máximo de computadores cliente que podem transferir informação a partir do Servidor de Administração.

   - Defina o número de tentativas de instalação quando uma tarefa é iniciada por agendamento, especificando o valor que necessita no campo **Número de tentativas**. As tentativas serão repetidas se ocorrerem erros durante a instalação anterior.

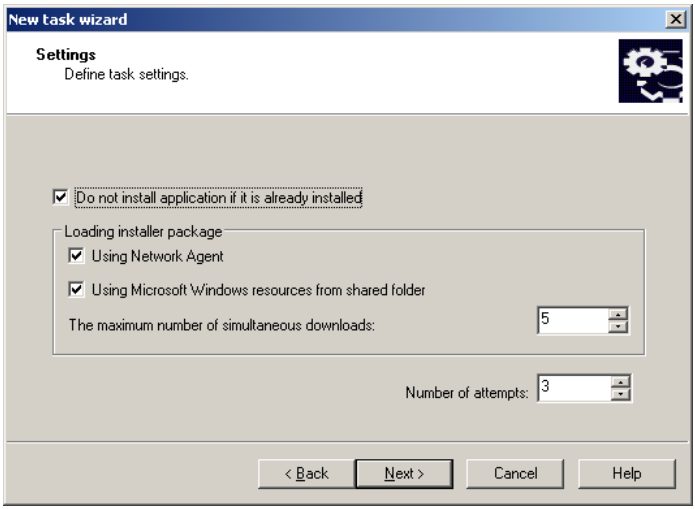

Figura 8. Opções adicionais de instalação

8. Durante este passo (ver Figura 9), ser-lhe-á dada a opção de instalar o Agente de Rede juntamente com a aplicação.

   Se o Agente de Rede não estiver instalado no computador da rede ao qual o dispositivo móvel será ligado e você desejar instalá-lo, você pode incluir o Kit de distribuição do Agente de Rede no pacote de distribuição da aplicação.

   Para o fazer, assinale a caixa **Instalar com o Agente de Rede**, assim como a caixa junto ao nome do pacote de instalação desejado. Se for necessário, crie um novo pacote de instalação através do botão **Novo**.

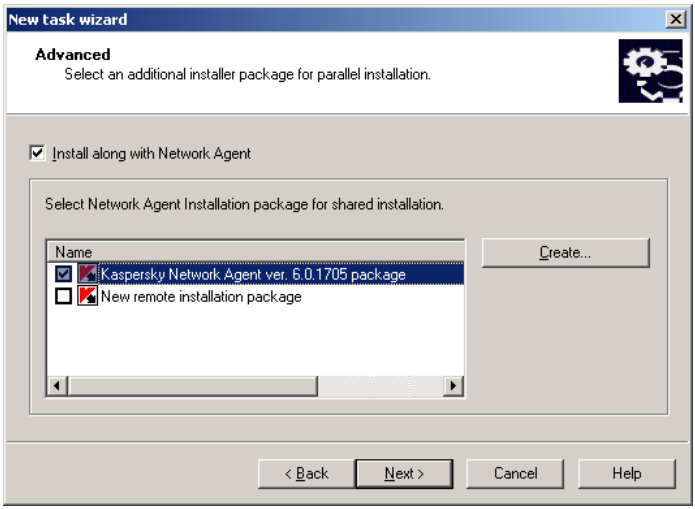

Figura 9. Seleccionar a instalação conjunta com o Agente de Rede

9. Determine o método de selecção dos computadores para os quais será criada a tarefa (ver Figura 10):

   - **Com base nos dados obtidos pela pesquisa da rede do Windows.** Neste caso, os computadores para instalação serão seleccionados com base nos dados obtidos pelo Servidor de Administração, pesquisando a rede empresarial do Windows.
   - **Com base nos endereços (endereço IP, nome NetBIOS ou nome DNS), manualmente inseridos**. Neste caso, os computadores para instalação serão manualmente seleccionados.

   Se os computadores forem seleccionados com base nos dados obtidos pela pesquisa da rede do Windows, a lista será criada através do ecrã do assistente (ver Figura 11), de forma semelhante ao procedimento para adicionar os computadores à rede lógica (para mais detalhes, consulte o Guia de Referência do Kaspersky Administration Kit). Pode seleccionar computadores cliente da rede lógica (a pasta **Grupo**) ou computadores que ainda não estão incluídos na sua estrutura (a pasta **Rede**).

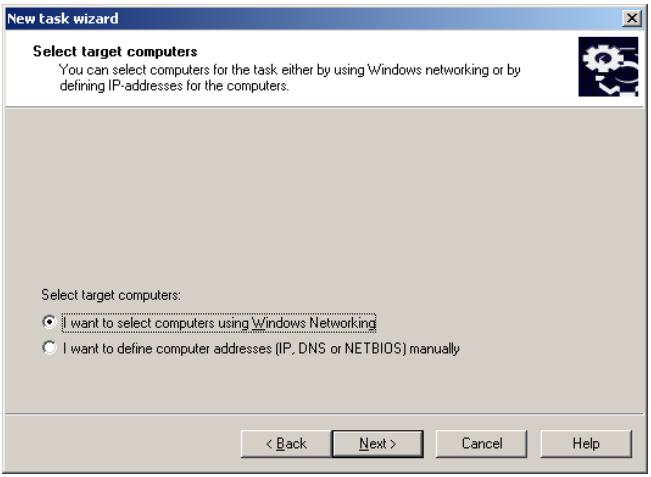

Figura 10. Determinar os métodos para seleccionar computadores cliente

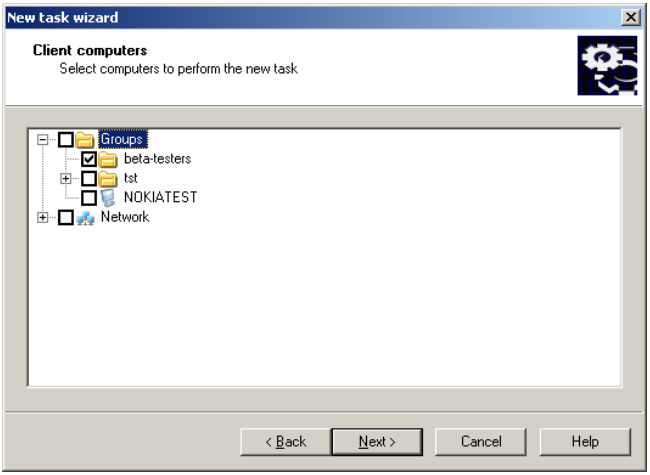

Figura 11. Criar uma lista de computadores para instalação com base nos dados da rede do Windows

Se os computadores forem manualmente seleccionados, a lista será criada através da inserção dos nomes NetBIOS ou nomes DNS, endereços IP (ou intervalos de endereços IP) dos computadores ou através da importação da lista a partir de um ficheiro *.txt* no qual cada endereço tem de ser inserido numa nova linha (ver Figura 12).

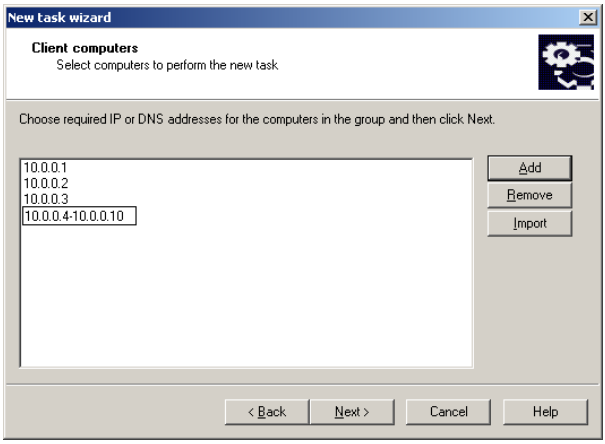

Figura 12. Criar uma lista de computadores para instalação com base nos endereços IP

10. No ecrã do assistente que se segue, especifique a conta com a qual será executada a tarefa de instalação remota nos computadores (ver Figura 13).

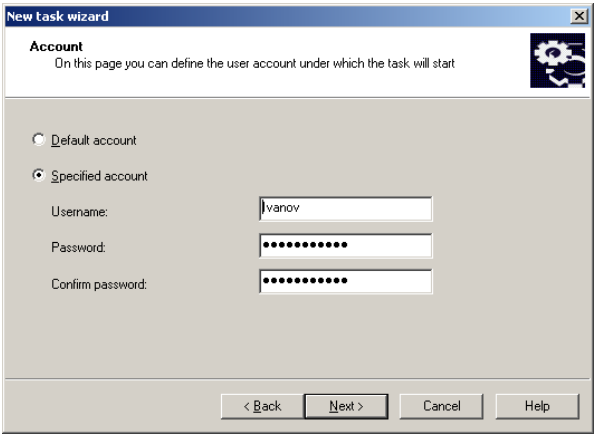

Figura 13. Seleccionar uma conta

Nota!

A conta tem de ter direitos de administrador em todos os computadores nos quais planeia executar uma instalação remota do software.

Ao instalar o software em computadores pertencentes a diferentes domínios, é necessária uma relação de confiança entre esses domínios e os domínios nos quais o Servidor de Administração está a funcionar.

Seleccione uma das seguintes opções:

- **Conta predefinida** – se o Servidor de Administração for iniciado com uma conta de um utilizador do domínio e tiver os direitos necessários para a instalação do software.
- **Especificar a conta** – se o Servidor de Administração for iniciado com uma conta de sistema ou se a conta do Servidor de Administração não tiver os direitos necessários para iniciar tarefas de instalação remota.

Nota!

Para efectuar a instalação remota do software nos computadores que não pertencem ao domínio, a tarefa de instalação remota tem de ser iniciada com uma conta de um utilizador que tenha direitos de administração nestes computadores.

Nos campos por baixo, especifique os atributos do utilizador cuja conta cumpre as condições necessárias.

11. Depois crie o agendamento de inicialização da tarefa (ver Figura 14).
    - Seleccione o modo desejado para a inicialização da tarefa a partir da lista suspensa **Inicialização agendada**:
        - **Manualmente.**
        - **A cada N hora(s).**
        - **Diariamente.**
        - **Semanalmente.**
        - **Mensalmente.**
        - **Uma vez** (neste caso a inicialização da tarefa de instalação remota nos computadores será executada apenas uma vez independentemente do resultado da sua execução).

- **Imediatamente** (imediatamente depois de ter criado a tarefa, após a conclusão do assistente).
- **Com a conclusão de outra tarefa** (neste caso a tarefa de instalação remota será iniciada apenas depois da conclusão da tarefa especificada).

- Configure as configurações de agendamento através de um grupo de campos correspondentes ao modo seleccionado (para mais detalhes, consulte o Guia de Referência do Kaspersky Administration Kit).

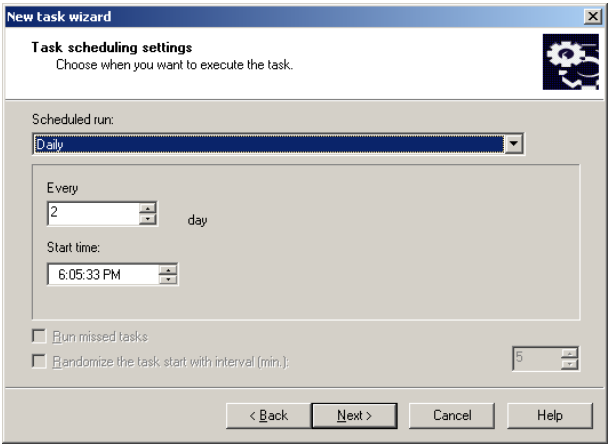

Figura 14. Inicialização diária da tarefa

Após conclusão do assistente, a tarefa de instalação remota criada será adicionada ao nódulo **Tarefa global** e estará visível no painel de resultados.

Para iniciar a tarefa de instalação remota:

seleccione o nódulo **Tarefas globais** na árvore da consola seleccione o pacote de instalação desejado, abra o menu de atalho e seleccione o comando **Instalar** ou use o item correspondente no menu **Acções**.

Depois de concluída a instalação, a aplicação *kmlisten.exe* será iniciada em segundo plano. Esta aplicação irá detectar a ligação de dispositivos móveis ao computador. Quando for detectado um dispositivo conectado, abrir-se-á uma janela (ver Figura 15) com um aviso para seleccionar um dispositivo no qual será instalada a aplicação.

Figura 15. Janela do utilitário *KMListen.exe*

Clique no botão **Instalar** para transferir o pacote de instalação da aplicação para o dispositivo móvel. Quando a transferência estiver concluída, siga as instruções do assistente de instalação em execução no dispositivo.

2.3. Instalação através de uma mensagem SMS

A instalação da aplicação em dispositivos móveis através de um SMS é utilizada quando os dispositivos móveis não estão ligados aos computadores da rede lógica.

Nota!

Para enviar um SMS, você tem de ter um modem GSM ligado ao Servidor de Administração. Também irá precisar do Microsoft .NET Framework versão 2.0 no Servidor. Caso contrário o envio de mensagens SMS será impossível.

Para instalar a aplicação através de um SMS:

1. Ligue-se ao Servidor de Administração.
2. Seleccione o nódulo **Instalação Remota** na árvore da consola.
3. Seleccione o item **Propriedades** a partir do menu de atalho do pacote de instalação da aplicação que foi criado.

4. Abra o separador **Configurações** e clique no botão **Instalar através de SMS**.

5. Na janela que se abre (ver Figura 16), especifique as configurações de instalação:

   a) Especifique as configurações de ligação do modem na secção **Modem GSM**: porta e taxa.

   b) No campo **URL do pacote de distribuição** especifique um servidor público no qual está localizado o pacote de distribuição do Kaspersky Mobile Security e a partir do qual a aplicação será instalada.

      Por exemplo:
      ftp://ftp.domain.com/distrib/KMS7EE/kmsecurity_7_0_15_beta.sis

      ou:

      http://domain_name.ru/distrib/KMS7EE/kmsecurity_ee_wm_sp_7_0_0_49_ru.cab.

   c) Crie a lista de números para os quais será enviada a mensagem SMS. Para o fazer, insira o número no campo de registo e clique no botão **Adicionar número**. O número inserido será adicionado a esta lista.

      Para guardar a lista de números num ficheiro TXT ou carregar a lista a partir de um ficheiro previamente criado, utilize os botões **Guardar em ficheiro** e **Carregar a partir de ficheiro**.

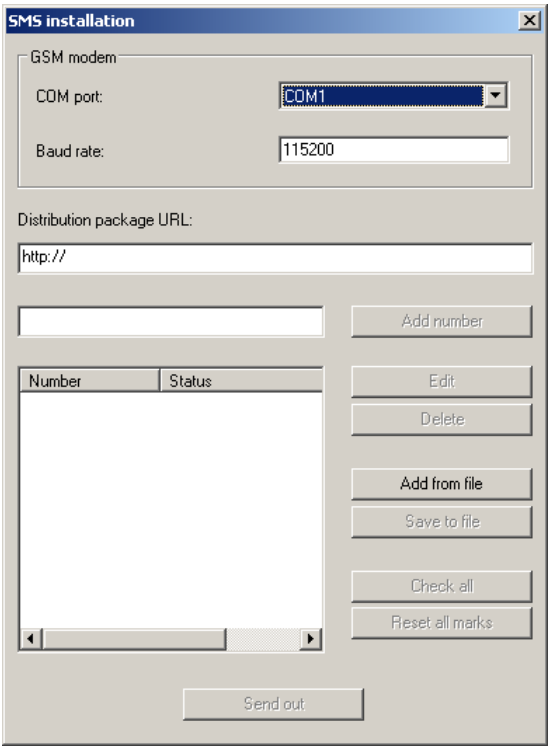

Figura 16. Configurações de envio de SMS

6. Clique no botão **Enviar** para enviar aos números especificados o SMS de instalação do Kaspersky Mobile Security.

A mensagem SMS com o URL do pacote de instalação será enviada para os dispositivos móveis cujos números se encontram na lista. Quando abre o URL, o pacote de instalação da aplicação será transferido para o dispositivo. Quando a transferência estiver concluída, siga as instruções do assistente de instalação em execução no dispositivo.

2.4. Adicionar dispositivo a um grupo

Após a instalação do Kaspersky Mobile Security, durante a pesquisa da rede, todos os dispositivos móveis serão colocados no domínio com o nome

especificado quando o pacote de instalação foi criado (por defeito – **GrupoPDA**). A política criada para dispositivos móveis não será aplicada.

Nota

Após a primeira ligação do dispositivo móvel com o serviço de Administração, aparecerá um grupo para dispositivos móveis no objecto **Rede** (no modo de visualização de domínio), desde que o Kaspersky Mobile Security esteja instalado no dispositivo.

Para mover o dispositivo móvel para dentro do grupo de administração, abra a Consola de Administração, aceda ao objecto **Rede** e seleccione o modo de visualização de domínio. Expanda o grupo **GrupoPDA** na lista de grupos de rede e arraste o dispositivo móvel para dentro do grupo de administração desejado.

Para garantir que os dispositivos móveis são automaticamente colocados no grupo desejado:

1. Abra a Consola de Administração e aceda ao objecto **Rede**.
2. Seleccione o **GrupoPDA** e abra a janela de propriedades do grupo através do menu de contexto.
3. Abra o separador **Computadores cliente** (ver Figura 17).

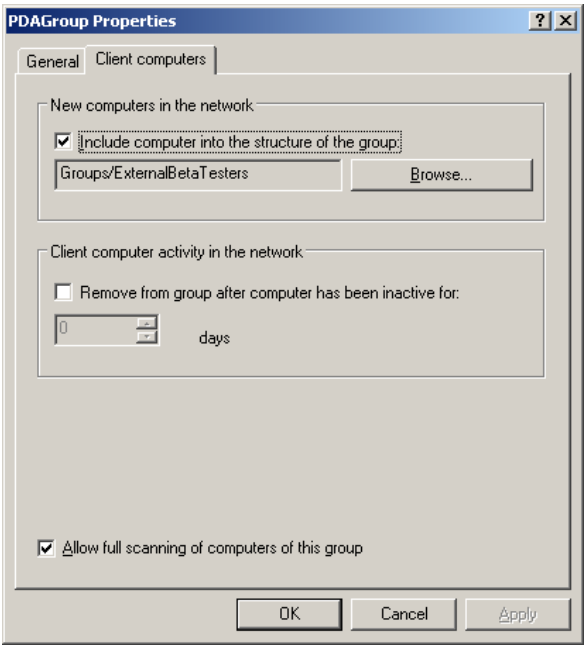

Figura 17. Propriedades do Grupo

4. Assinale a caixa **Adicionar computador ao grupo** na secção **Novo computador na rede**.
5. Clique no botão **Procurar** e, na janela que se abre, seleccione o grupo de administração no qual serão colocados os dispositivos móveis conectados mais tarde.
6. Guarde as alterações.

CAPÍTULO 3. GERIR POLÍTICAS

Esta secção contém informação sobre a criação e configuração de políticas para o Kaspersky Mobile Security 7.0 Enterprise Edition.

A política é aplicada à aplicação nos seguintes casos:

- durante a primeira ligação do dispositivo à rede;
- durante as ligações posteriores do dispositivo caso as configurações de funcionamento da aplicação ou as configurações das políticas tenham sido alteradas;
- durante a sincronização iniciada de forma manual (Manual de Utilizador do Kaspersky Mobile Security).

3.1. Criar uma política

Para criar uma política:

1. Seleccione um grupo de dispositivos móveis para os quais deseja criar uma política na árvore da consola, na pasta **Grupos**.
2. Seleccione a pasta **Políticas** incluída no grupo seleccionado, abra o menu de atalho e use o comando **Novo→Política**.

O utilitário de criação de políticas foi concebido como um assistente do Microsoft Windows e inclui uma sequência de janelas (passados), entre as quais pode navegar através dos botões **Anterior** e **Seguinte.** Pode concluir o assistente através do botão **Concluir**. Para sair do assistente em qualquer ponto, clique no botão **Cancelar**.

Nota!

Em cada passo da criação de uma política, as configurações especificadas podem ser guardadas com o botão  . Se o cadeado do botão estiver fechado, quando a política for utilizada mais tarde nos dispositivos móveis apenas serão aplicados os valores especificados pela política que está a ser criada.

Passo 1. Introduzir informação geral sobre a política

O primeiro passo do assistente é introdutório. No primeiro ecrã do assistente deve especificar o nome da política (o campo **Nome**). No segundo ecrã, seleccione a aplicação **Kaspersky Mobile Security 7.0 Enterprise Edition** a

partir da lista suspensa **Nome da aplicação**. Para aplicar as configurações da política imediatamente após a sua criação, assinale a caixa **Política Activa** na secção **Estado da Política** no terceiro ecrã.

Passo 2. Definir as configurações da verificação anti-vírus em segundo plano

Nesta etapa, terá de determinar as configurações da verificação anti-vírus do dispositivo móvel: o âmbito de verificação e o agendamento de inicialização da verificação.

Na secção **Configurações de verificação** (ver Figura 18), pode seleccionar o âmbito de protecção, escolhendo os tipos de ficheiros a verificar, e determinar se serão feitas tentativas de desinfecção de um objecto infectado:

- **Verificar apenas ficheiros executáveis** - verifica apenas ficheiros de programas executáveis.
- **Verificar arquivos** - verifica ficheiros compactados em arquivos.
- **Tentar desinfectar os objectos infectados** – tenta desinfectar objectos infectados detectados. Nem todos os objectos podem ser desinfectados.

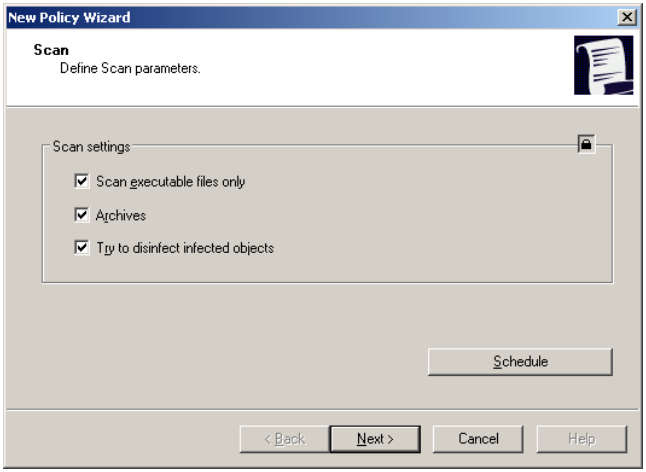

Figura 18. Configurar as definições da protecção anti-vírus

Para configurar um agendamento para a execução da verificação sob pedido, clique no botão **Agendamento**. Isto irá abrir uma caixa de diálogo na qual deve especificar a frequência da verificação:

- **Manual** – a acção será manualmente iniciada pelo utilizador.
- **Diariamente** – a acção será efectuada diariamente. A hora da verificação é determinada pela configuração **Hora**. No grupo de campos **Hora de início**, especifique a hora para executar a verificação.
- **Semanalmente** – a acção será efectuada num determinado dia da semana. No grupo de campos **Hora de início**, especifique a hora para executar a acção e seleccione um dia da semana no qual será executada a verificação sob pedido.

Passo 3. Configurar as definições da Protecção em Tempo Real

Durante esta etapa, você irá determinar as configurações de funcionamento da protecção em tempo real do sistema de ficheiros e da memória do dispositivo móvel.

Assinale a caixa **Activar Protecção em Tempo Real** (ver Figura 19) para fazer com que a aplicação verifique todos os programas executados e ficheiros abertos pelo utilizador.

Pode utilizar a secção **Configurações de verificação** para seleccionar o âmbito de verificação, escolhendo os tipos de ficheiros a verificar:

- **Verificar apenas ficheiros executáveis** - verificar apenas ficheiros de programas executáveis.

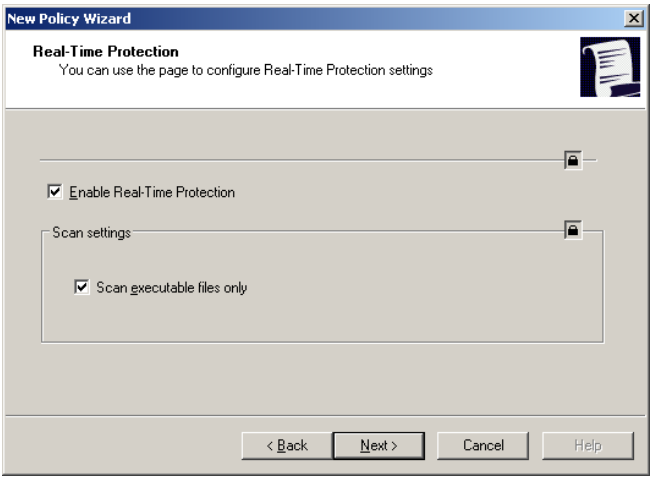

Figura 19. Configurar as definições da Protecção em Tempo Real

Passo 4. Seleccionar uma origem de actualização

Durante esta etapa, você irá determinar a origem de actualização e configurar o agendamento para a execução das actualizações.

Através da secção **Origem de Actualização** (ver Figura 20), especifique os endereços do servidor a partir do qual serão efectuadas as actualizações.

Para garantir que as actualizações são efectuadas a partir dos servidores de actualização da Kaspersky Lab, deixe o campo **Endereço do Servidor de Actualização** em branco.

Quando utilizar um recurso diferente para as actualizações, especifique o endereço da origem de actualização na secção **Origem de Actualização**. O endereço tem de ser um URL completo do ficheiro *mobile.xml*.

Por exemplo, `http://domain.com/index/mobile.xml`.

Nota!

A estrutura da pasta na origem de actualização tem de ser idêntica à estrutura correspondente do servidor de actualização da Kaspersky Lab.

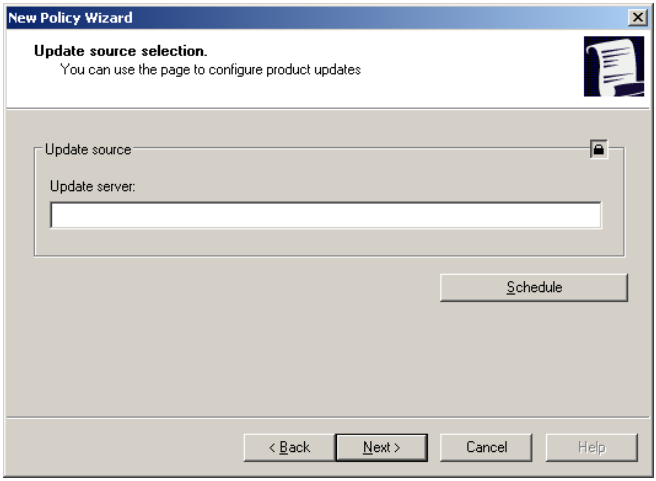

Figura 20. Seleccionar uma origem de actualização

Para além disso, pode criar um agendamento para a inicialização da actualização. Para o fazer, utilize o botão **Agendamento**. Isto irá abrir uma caixa de diálogo na qual deve especificar a frequência da actualização:

- **Manual** – a acção será manualmente iniciada pelo utilizador.

- **Diariamente** – a acção será efectuada diariamente. A hora da verificação é determinada pela configuração **Hora**. No grupo de campos **Hora de início**, especifique a hora para executar a actualização.
- **Semanalmente** – a acção será efectuada num determinado dia da semana. No grupo de campos **Hora de início**, especifique a hora para executar a acção e seleccione um dia da semana no qual será executada a actualização.

Passo 5. Configurar as definições do Anti-Spam

Durante esta etapa, pode configurar as definições do módulo Anti-Spam (ver Figura 21).

Seleccione o modo de funcionamento do Anti-Spam na secção **Anti-Spam**:

- **Desactivado.** O Anti-Spam está desactivado.
- **Apenas as mensagens da lista branca serão entregues.** Neste modo, o Anti-Spam permite as mensagens que correspondam aos critérios da “lista branca". Todas as outras mensagens serão bloqueadas.
- **Apenas as mensagens da lista negra serão bloqueadas.** Neste modo, o Anti-Spam bloqueia a recepção das mensagens que correspondam aos critérios da “lista negra". Todas as outras mensagens serão permitidas.
- **Normal**. Neste modo, o Anti-Spam filtra as mensagens recebidas através das listas "negra" e "branca". Quando for recebida uma mensagem de um número de telefone não incluído em nenhuma das listas, o Anti-Spam notificará o utilizador e dar-lhe-á a opção de bloquear ou permitir a recepção da mensagem e ainda a opção de adicionar este número de telefone à lista "branca" ou "negra".

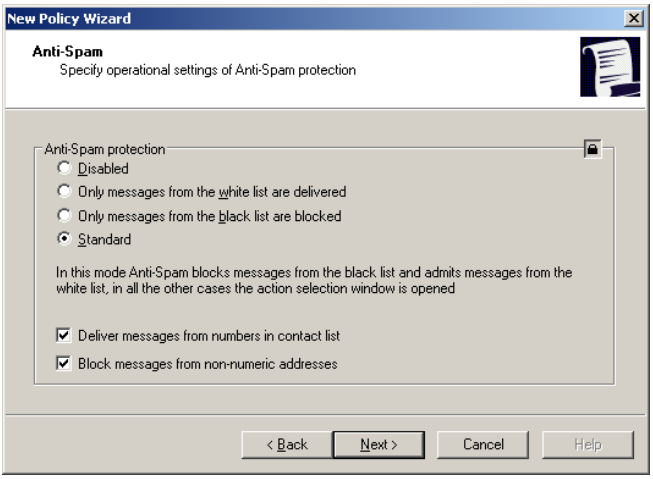

Figura 21. Configurar as definições do Anti-Spam

Assinale a caixa **Entregar mensagens de números existentes na lista de contactos** para garantir que o Anti-Spam permite a recepção de mensagens de números incluídos nas listas de contactos.

Assinale a caixa **Bloquear mensagens de números não numéricos** de forma a que o Anti-Spam bloqueie a recepção de mensagens de números não numéricos.

Passo 6. Configurar definições adicionais

Durante esta etapa, pode especificar o nível de protecção do módulo Firewall e o período de sincronização com o Servidor de Administração.

Especifique o nível de protecção do módulo Firewall na secção **Firewall** (ver Figura 22). A Firewall garante a protecção do dispositivo móvel com um dos seguintes níveis:

- **Desactivada.** Firewall desactivada.
- **Baixo**. A Firewall bloqueia todas as ligações de entrada. Todas as ligações de saída são permitidas.
- **Médio.** A Firewall bloqueia todas as ligações de entrada. São permitidas as ligações de saída a partir das portas HTTP/HTTPS/SMTP/IMAP/SSH.

- **Elevado**. A Firewall bloqueia todas as actividades de rede, com excepção das ligações ao Kaspersky Administration Kit e das actualizações das bases da aplicação.

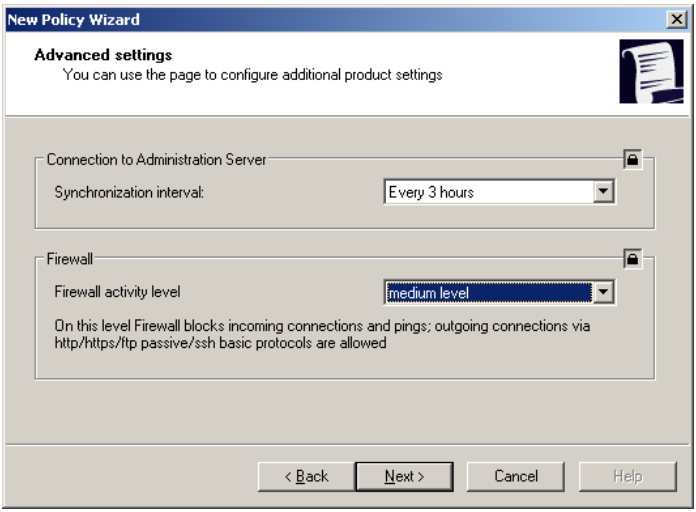

Figura 22. Configurações adicionais da aplicação

Especifique a frequência de sincronização, seleccionando o valor desejado na lista suspensa: **Período de Sincronização** na secção **Sincronização com o Servidor de Administração**. Por defeito, o dispositivo móvel irá tentar ligar-se ao Servidor de Administração a cada 6 horas.

Passo 7. Seleccionar um ficheiro de chave

Nesta etapa pode especificar um ficheiro de chave utilizado para activar o Kaspersky Mobile Security.

Clique no botão **Alterar** e seleccione o ficheiro de chave na janela que se abre. Como resultado, será apresentada a seguinte informação sobre a chave na janela do assistente:

- número;
- tipo de chave;
- data de validade da licença.
- restrições da licença.

Nota!

Para ter a certeza de que o ficheiro de chave é transferido para os dispositivos móveis, você tem de confirmar a sua selecção através do botão  . Caso contrário, o Kaspersky Mobile Security não será activado.

Passo 8. Concluir a criação da política

O último ecrã do assistente informa-o sobre a conclusão bem-sucedida do processo de criação da política (ver Figura 23).

Assim que o assistente estiver concluído, as políticas para o Kaspersky Mobile Security 7.0 Enterprise Edition serão adicionadas à pasta **Políticas** para o grupo correspondente e estarão visíveis na janela de resultados.

Pode editar as configurações da política criada e impor restrições à alteração das suas configurações, utilizando o botão  para cada grupo de configurações. O utilizador do dispositivo móvel não conseguirá alterar as configurações bloqueadas tal como acima descrito. A política será aplicada a dispositivos móveis no momento da primeira sincronização do cliente com o servidor, imediatamente depois do dispositivo móvel ter sido adicionado ao grupo de administração.

Pode copiar ou mover políticas de um grupo para outro ou apagá-las através dos comandos de atalho padrão **Copiar / Colar, Cortar / Colar** e **Apagar** ou através dos itens correspondentes no menu **Acções**.

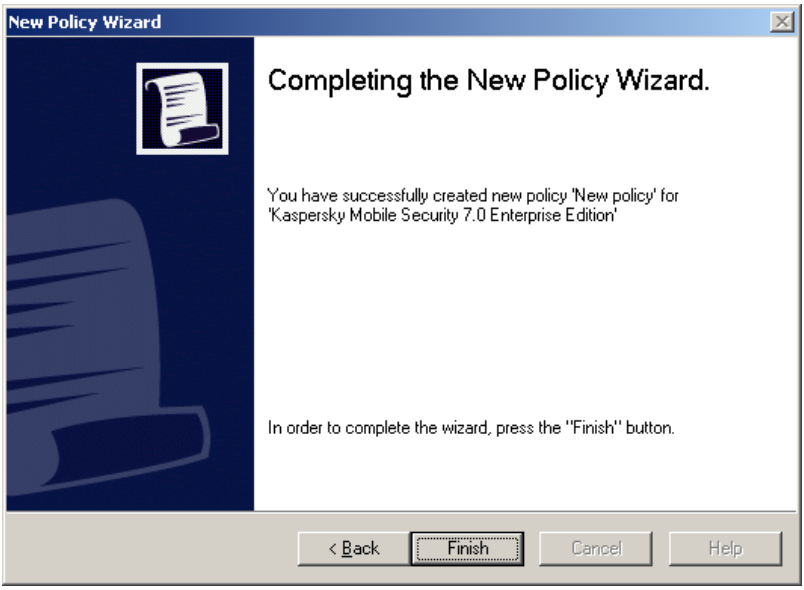

Figura 23. Concluir a criação da política

3.2. Ver e editar configurações das políticas

Na etapa de edição, pode alterar a política e bloquear a alteração das configurações em políticas de grupos aninhados e em configurações da aplicação e de tarefas.

1. Seleccione o grupo de dispositivos móveis para o qual deseja editar as configurações, a partir da árvore da consola na pasta **Grupos**.
2. Seleccione a pasta **Políticas** incluída nesse grupo. Todas as políticas criadas para esse grupo serão apresentadas no painel de resultados.
3. Na lista de políticas, seleccione a política desejada para o **Kaspersky Mobile Security 7.0 Enterprise Edition** (o nome da aplicação é especificado no campo **Aplicação**).
4. Seleccione o comando **Propriedades** no menu de atalho da política seleccionada.

Abrir-se-á uma caixa de diálogo de configuração das políticas da aplicação, contendo vários separadores.

Os separadores **Geral**, **Utilização** e **Eventos** são separadores padrão para a aplicação Kaspersky Administration Kit (para mais detalhes, consulte o Manual de Administrador do Kaspersky Administration Kit).

O resto dos separadores contêm os controlos das configurações do Kaspersky Mobile Security 7.0 Enterprise Edition. De seguida, é fornecida uma descrição de cada separador.

Nota

Ao editar as configurações de políticas, utilize o botão  para bloquear os dados das políticas inseridos. Mais tarde, o utilizador do dispositivo móvel não conseguirá editar as configurações das políticas bloqueadas tal como acima descrito.

3.2.1. Visualizar informação sobre a aplicação

No separador **Geral** é apresentada a seguinte informação sobre a política (ver Figura 24): nome da política, nome da aplicação para a qual é criada a política, data e hora de criação da política, data e hora da sua última alteração.

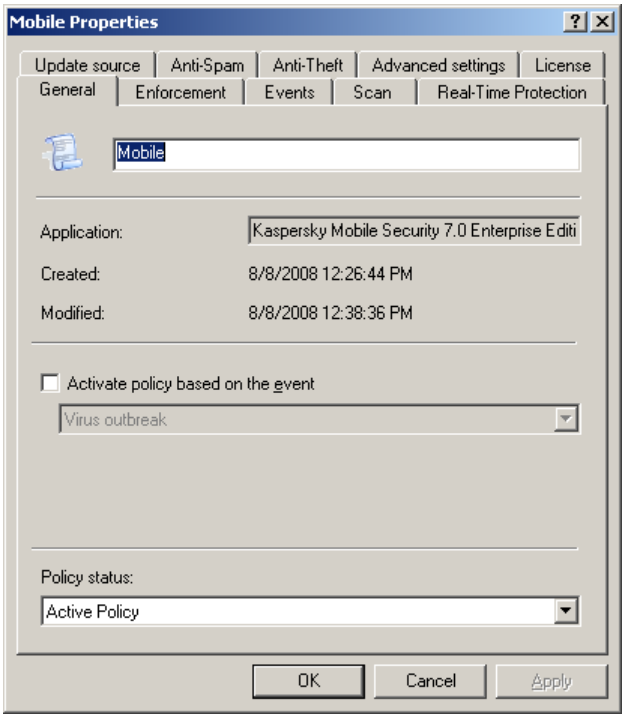

Figura 24. Separador **Geral**

Através desta janela pode alterar o nome da política, activar ou desactivá-la e configurar a activação da política quando ocorrer um determinado evento.

3.2.2. Visualizar resultados da aplicação da política

O separador **Utilização** (ver Figura 25) contém informação geral sobre a utilização de uma política em dispositivos móveis de um grupo e indica o número de dispositivos nos quais a política:

- não está determinada;
- está executada;
- ainda não está executada;
- não pôde ser executada devido a um erro.

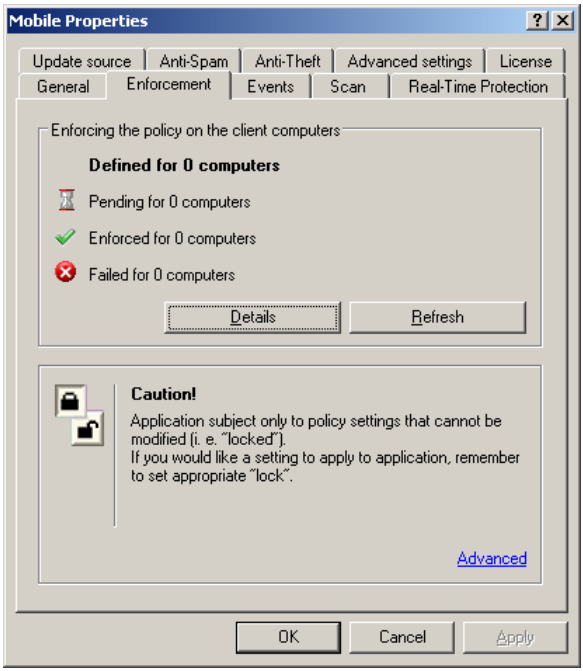

Figura 25. Separador **Utilização**

Na janela que se abre quando clica no botão **Detalhes**, pode ver detalhes sobre os resultados da utilização da política em cada computador cliente no grupo (para mais detalhes, consulte o Manual de Administrador do Kaspersky Administration Kit 6.0).

3.2.3. Configurar definições do registo de eventos do funcionamento da aplicação

No decorrer do seu funcionamento, o Kaspersky Mobile Security gera um determinado conjunto de eventos. Cada evento tem uma característica que reflecte o seu nível de gravidade. Existem quatro níveis de gravidade: evento crítico, falha funcional, aviso e mensagem informativa.

Os eventos do mesmo tipo podem ter diferentes níveis de importância, dependendo da situação em que esses eventos ocorreram.

O separador **Eventos** (ver Figura 26) apresenta os tipos de eventos ocorridos no funcionamento da aplicação e registados no relatório, assim como a localização do relatório e o modo de notificação do administrador e de outros utilizadores.

Para ver os tipos de eventos, seleccione o nível de gravidade desejado a partir da lista suspensa **Nível de gravidade**. No campo de informação por baixo serão apresentados os tipos de eventos para o nível seleccionado.

Para cada evento pode configurar se o mesmo será registado no relatório e se o administrador será notificado sobre esse evento.

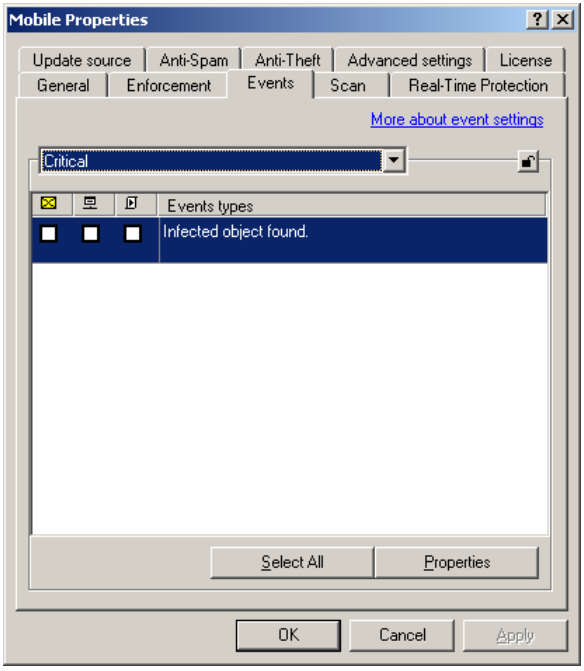

Figura 26. Separador **Eventos**

Para uma descrição detalhada das outras configurações do separador **Eventos**, consulte o Manual de Administrador do Kaspersky Administration Kit 6.0.

3.2.4. Configurar as definições da verificação anti-vírus

O separador **Verificação** (ver Figura 27) determina as configurações da verificação sob pedido: âmbito de verificação, acções a executar com objectos infectados e o agendamento com o qual a verificação será executada.

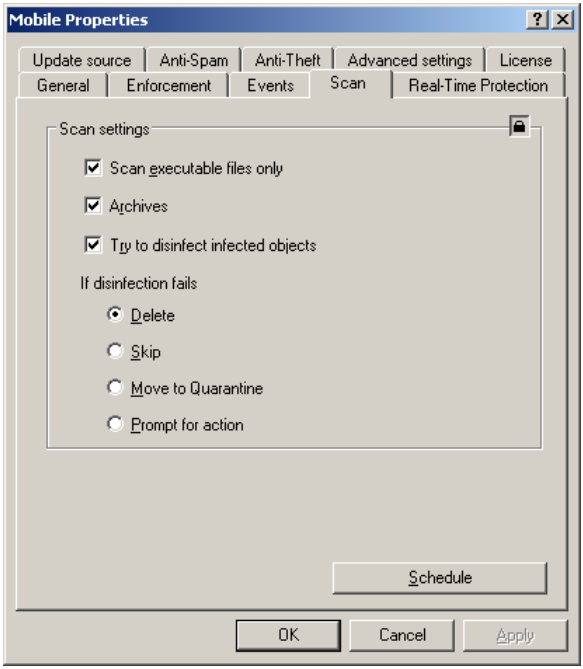

Figura 27. Separador **Verificação**

Na secção **Acções a executar com objectos infectados**, especifique a acção a executar quando é detectado um objecto infectado.

- **Apagar.**
- **Ignorar** - deixa intactos os objectos infectados detectados.
- **Quarentena** - move para a pasta da quarentena os objectos infectados detectados.
- **Perguntar o que fazer** - exibe uma mensagem no ecrã sobre a detecção de um vírus, com uma sugestão para apagar, colocar na quarentena ou deixar intacto o objecto infectado.

Se a configuração **Tentar desinfectar os objectos infectados** estiver seleccionada, então a acção seleccionada será executada apenas se o objecto não puder ser desinfectado.

As outras configurações são semelhantes às acima descritas na secção 3.1 na página 25.

3.2.5. Configurar as definições de funcionamento da Protecção em Tempo Real

O separador **Protecção em Tempo Real** (ver Figura 28) determina as configurações da Protecção em Tempo Real: âmbito de verificação, acções a executar com objectos infectados.

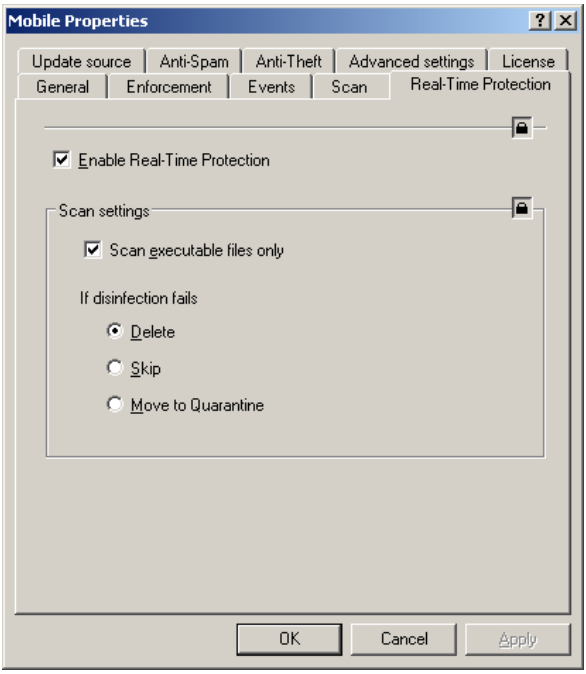

Figura 28. Separador **Protecção em Tempo Real**

3.2.6. Seleccionar a origem de actualização das bases da aplicação

O separador **Origem de Actualização** (ver Figura 29) indica a origem de actualização a partir da qual serão transferidas as actualizações das bases anti-vírus. Este separador também é utilizado para criar o agendamento de inicialização da actualização.

Para garantir que as actualizações são efectuadas a partir dos servidores de actualização da Kaspersky Lab, deixe o campo **Endereço do Servidor de Actualização** em branco.

Quando utilizar um recurso diferente para as actualizações, especifique o endereço da origem de actualização na secção **Origem de Actualização**. O endereço tem de ser um URL completo do ficheiro *mobile.xml*.

Por exemplo, `http://domain.com/index/mobile.xml`.

Nota!

A estrutura da pasta na origem de actualização tem de ser idêntica à estrutura correspondente do servidor de actualização da Kaspersky Lab.

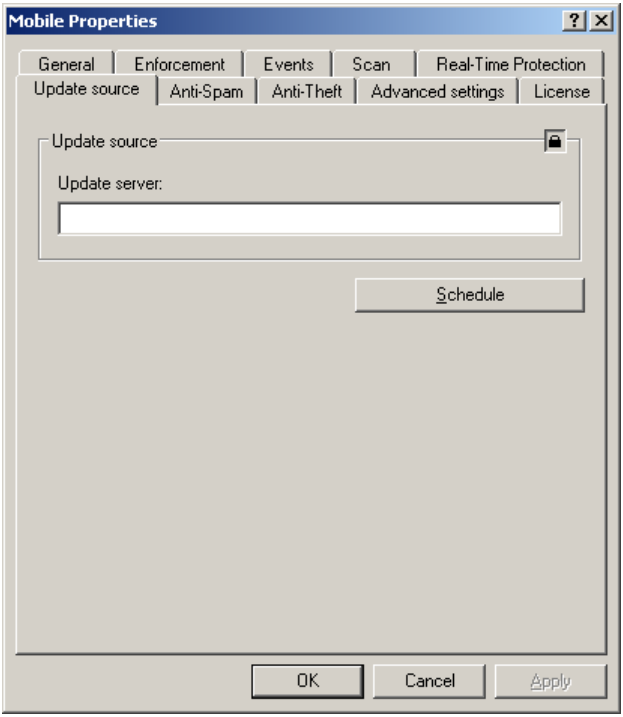

Figura 29. Separador **Origem de Actualização**

3.2.7. Configurar as definições do Anti-Spam

O separador **Anti-Spam** (ver Figura 30) é utilizado para configurar as definições de anti-spam.

Seleccione o modo de funcionamento do Anti-Spam na secção **Anti-Spam**:

- **Desactivado** – desactiva o Anti-Spam.
- **Entregar apenas as mensagens da lista branca** – o Anti-Spam verifica as mensagens face à lista branca. Se o número do remetente ou o texto da mensagem estiver incluído na lista, o Anti-Spam irá permitir essa mensagem.
- **Bloquear apenas as mensagens da lista negra** – o Anti-Spam verifica as mensagens face à lista negra. Se o número do remetente ou o texto da mensagem estiver incluído na lista, o Anti-Spam irá bloquear essa mensagem.
- **Normal** – o Anti-Spam bloqueia mensagens da lista negra, permite as mensagens da lista branca. Em todos os outros casos, abre-se uma janela onde o utilizador do dispositivo pode seleccionar a acção a executar com a mensagem.

Assinale a caixa **Entregar mensagens de números existentes na lista de contactos** para garantir que o Anti-Spam permite as mensagens de números incluídos nas listas de contactos.

Assinale a caixa **Bloquear mensagens de números não numéricos** de forma a que o Anti-Spam bloqueie a recepção de mensagens de números não numéricos.

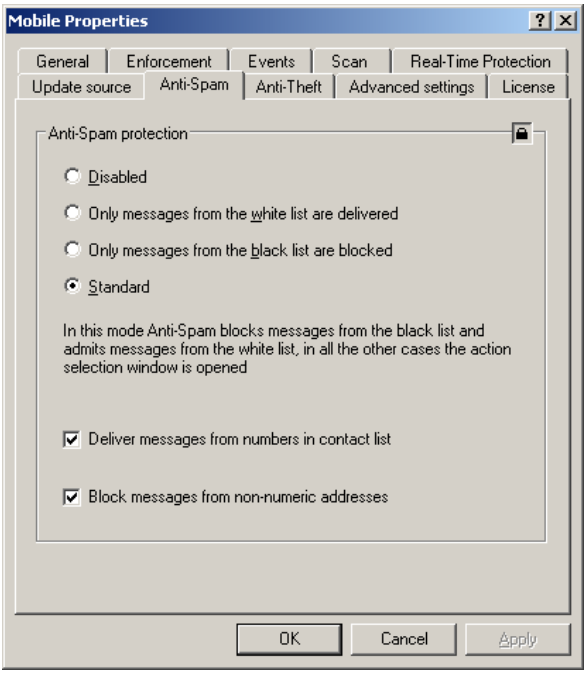

Figura 30. Separador **Anti-Spam**

3.2.8. Configurar as definições do Anti-Roubo

O módulo Anti-Roubo (secção **Anti-Roubo** (ver Figura 31) é utilizado para configurar as definições do módulo Anti-Roubo que protegem os dados armazenados no dispositivo móvel contra o acesso não-autorizado, no caso do dispositivo ser roubado ou perdido.

Assinale a caixa **Limpeza por SMS** para activar a função Limpeza por SMS. Esta função permite apagar dados pessoais do utilizador (contactos, mensagens, ficheiros, dados do cartão de memória, configurações de rede). Para utilizar a função Limpeza por SMS, envie uma mensagem SMS com o texto: “clean:password” para o dispositivo.

Clique no botão **Configurar** e, na janela que se abre, seleccione as categorias de informação que podem ser apagadas através da função Limpeza por SMS:

- **Apagar contactos** – eliminação da lista de contactos.

- **Apagar caixa entrada** – eliminação de mensagens.
- **Apagar documentos** – eliminação de dados pessoais.
- **Apagar ficheiros do cartão de memória** – eliminação de ficheiros do cartão de memória.
- **Apagar configurações de rede e configurações do ponto de acesso** – eliminação de configurações da rede pessoal.

Assinale a caixa **Bloqueio por SMS** para activar a função Bloqueio por SMS**.** Esta função permite desbloquear o dispositivo. Você pode desbloquear o dispositivo apenas depois de inserir a password. Para desbloquear o dispositivo através da função **Bloqueio por SMS**, envie uma mensagem SMS com o texto: «block:password» para o dispositivo.

Assinale a caixa **Protecção do Cartão SIM** para activar a função Protecção do Cartão SIM. Esta função permite enviar para os números especificados um novo número de telefone e assim bloquear o dispositivo roubado, caso o cartão SIM seja substituído nesse dispositivo roubado.

Clique no botão **Configurar** e, na janela que se abre, configure as definições da função Limpeza por SMS. Nos campos **Número principal** e **Número adicional** especifique os números de telefone para os quais será enviada uma mensagem SMS com um novo número de telefone, caso o cartão SIM seja substituído por um novo. Para além disso, através da respectiva caixa pode activar a função de bloqueio do dispositivo, caso o cartão SIM seja substituído.

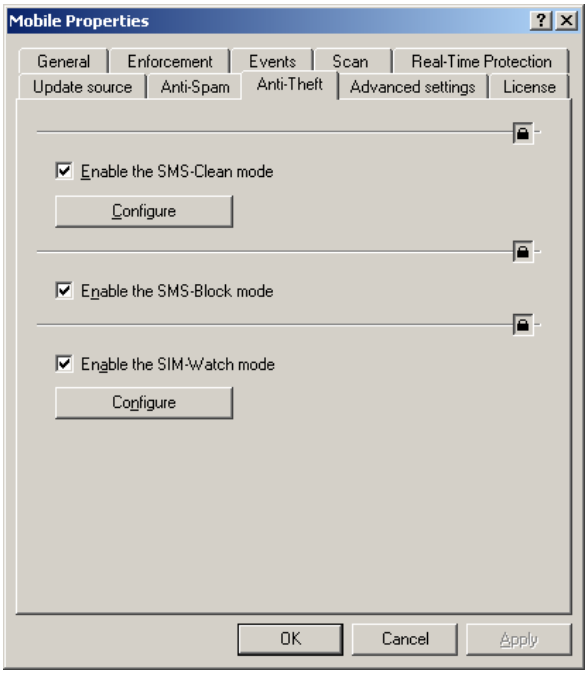

Figura 31. Separador **Anti-Roubo**

3.2.9. Configurar definições adicionais

O separador **Configurações adicionais** (ver Figura 32) é utilizado para definir o nível de protecção da Firewall e para determinar o período de sincronização do Servidor de Administração.

Especifique a frequência de sincronização, seleccionando o valor desejado na lista suspensa **Período de Sincronização** na secção **Sincronização com o Servidor de Administração**.

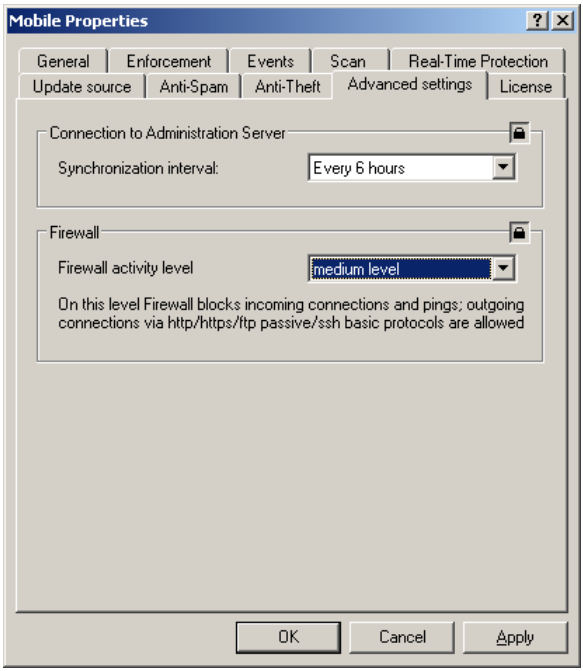

Figura 32. **Configurações Adicionais**

Seleccione o nível de protecção da Firewall na secção **Firewall**.

- **Desactivada** – Desactiva o funcionamento da Firewall.
- **Baixo -** A Firewall bloqueia todas as ligações de entrada. Todas as ligações de saída são permitidas.
- **Médio -** A Firewall bloqueia todas as ligações de entrada. São permitidas as ligações de saída a partir das portas HTTP/HTTPS/SMTP/IMAP/SSH.
- **Elevado -** A Firewall bloqueia todas as actividades de rede, com excepção das ligações com o Servidor de Administração e das actualizações das bases da aplicação.

CAPÍTULO 4. GERIR CONFIGURAÇÕES DE FUNCIONAMENTO DA APLICAÇÃO

Através das configurações da aplicação você pode alterar as configurações de funcionamento do Kaspersky Mobile Security para dispositivos móveis individuais. Apenas pode alterar as configurações que não estão bloqueadas pela política (para mais detalhes, veja a secção 3.1 na página 25).

Para alterar as configurações de funcionamento da aplicação:

1. Na pasta **Grupos** seleccione a pasta com o nome do grupo ao qual pertence o dispositivo móvel.
2. No painel de resultados, seleccione o dispositivo para o qual deseja alterar as configurações de funcionamento da aplicação. Seleccione o comando **Propriedades** no menu de atalho ou no menu **Acções**.
3. Como resultado, na janela principal da aplicação abrir-se-á uma caixa de diálogo **Propriedades: nome do computador**. Seleccione o separador **Aplicações** (ver Figura 33).

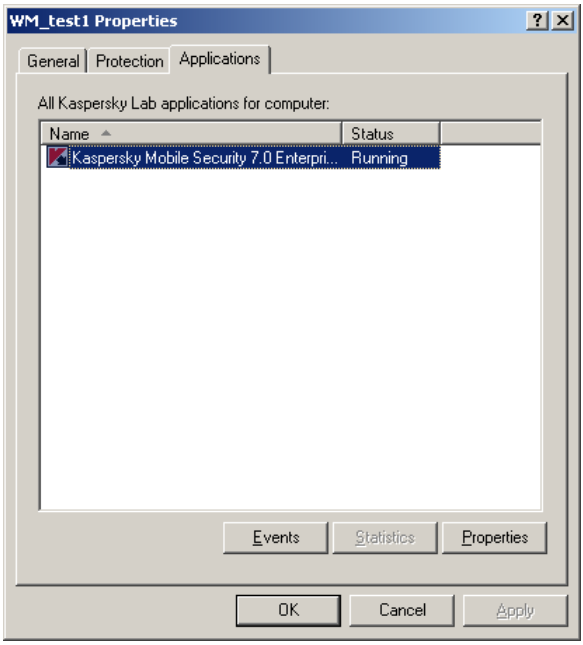

Figura 33. Janela de visualização das propriedades do dispositivo móvel. Separador **Aplicações**

4. Seleccione a aplicação **Kaspersky Mobile Security 7.0 Enterprise Edition**. A parte inferior esquerda da janela contém os seguintes botões:

   - **Eventos** – visualizar a lista de eventos do funcionamento da aplicação ocorridos no dispositivo móvel e registados no Servidor de Administração.
   - **Estatísticas** – visualizar informação estatística sobre o funcionamento da aplicação.
   - **Propriedades** – configurar a aplicação nas **configurações da aplicação Kaspersky Mobile Security 7.0 Enterprise Edition**.

4.1. Visualizar informação sobre a aplicação

No separador **Geral** (ver Figura 34) pode ver informação sobre a aplicação Kaspersky Mobile Security 7.0 Enterprise Edition.

A parte superior da janela apresenta o nome da aplicação instalada, informação sobre a versão, da instalação, estado actual (se a aplicação está em execução no dispositivo móvel) e informação sobre o estado das bases da aplicação.

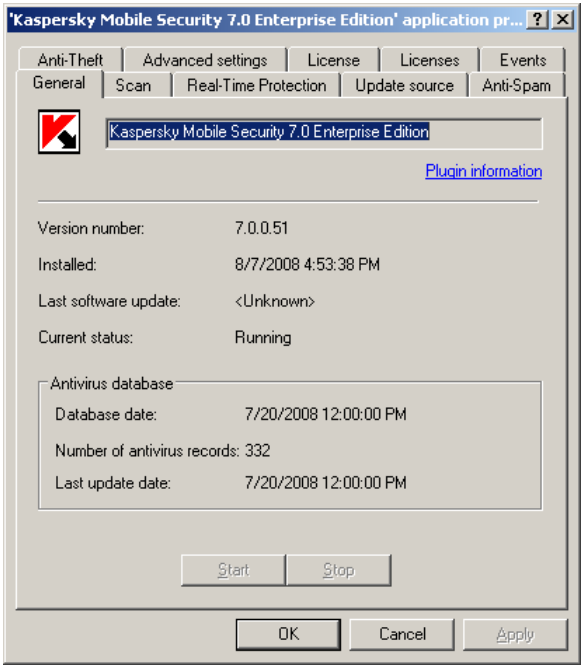

Figura 34. Janela de configuração das definições da aplicação. Separador **Geral**

4.2. Visualizar informação sobre as configurações da verificação anti-vírus

No separador **Verificação** (ver Figura 35) pode ver e alterar as configurações da verificação sob pedido: âmbito de verificação, acções a executar com objectos infectados e o agendamento com o qual a verificação será executada.

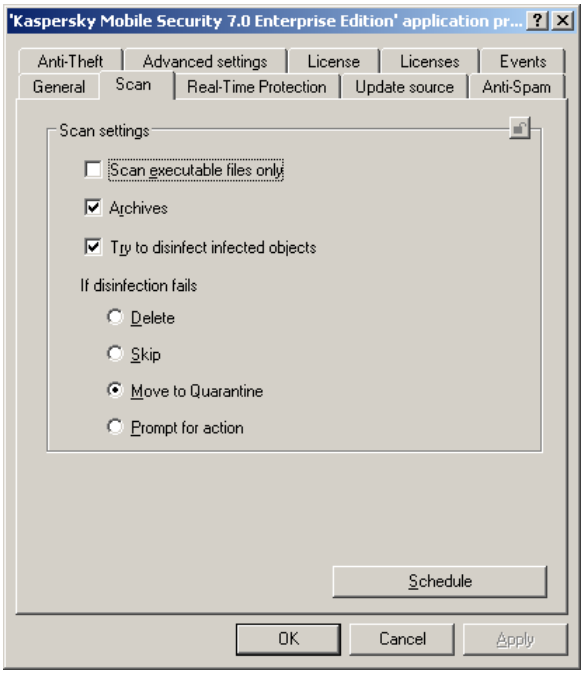

Figura 35. Separador **Verificação**

4.3. Visualizar informação sobre as configurações da Protecção em Tempo Real

No separador **Protecção em Tempo Real** (ver Figura 36) pode ver e alterar as configurações da Protecção em Tempo Real: âmbito de verificação e acções a executar com objectos infectados.

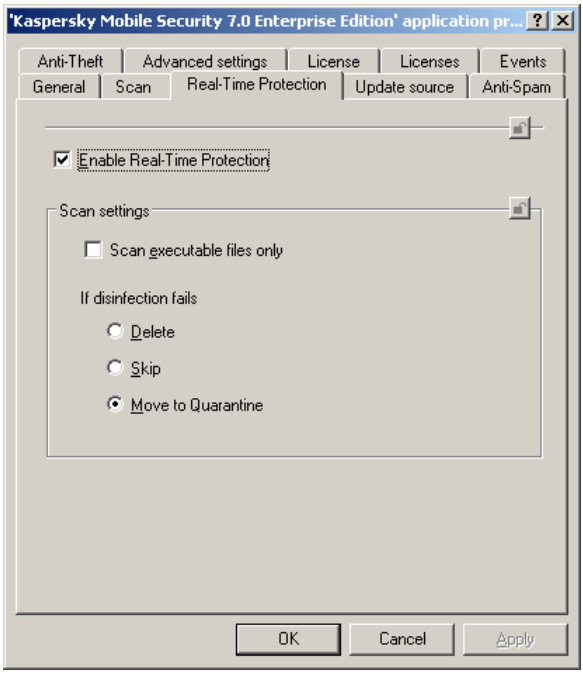

Figura 36. Separador **Protecção em Tempo Real**

4.4. Visualizar informação sobre a origem de actualização

No separador **Origem de Actualização** (ver Figura 37) pode ver informação e alterar as configurações de transferência de actualizações para o dispositivo móvel específico.

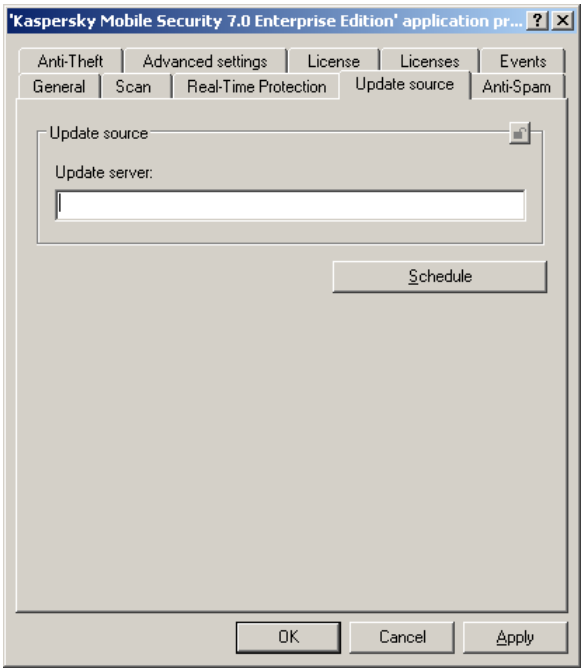

Figura 37. Separador **Origem de Actualização**

4.5. Visualizar informação sobre as configurações de funcionamento do Anti-Spam

No separador **Anti-Spam** (ver Figura 38) pode ver e alterar as configurações da protecção anti-spam do seu dispositivo móvel.

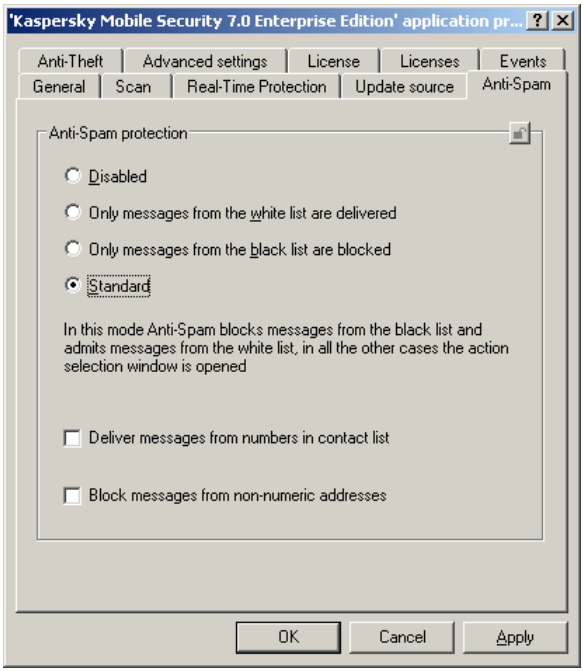

Figura 38. Separador **Anti-Spam**

4.6. Visualizar informação sobre as configurações de funcionamento do Anti-Roubo

No separador **Anti-Roubo** (ver Figura 39) pode ver e alterar as configurações de funcionamento do Anti-Roubo. Você pode:

- activar funções do módulo: Limpeza por SMS, Bloqueio por SMS, Protecção do Cartão SIM;
- configurar as definições da função Anti-Roubo através dos botões **Configurar** na secção correspondente.

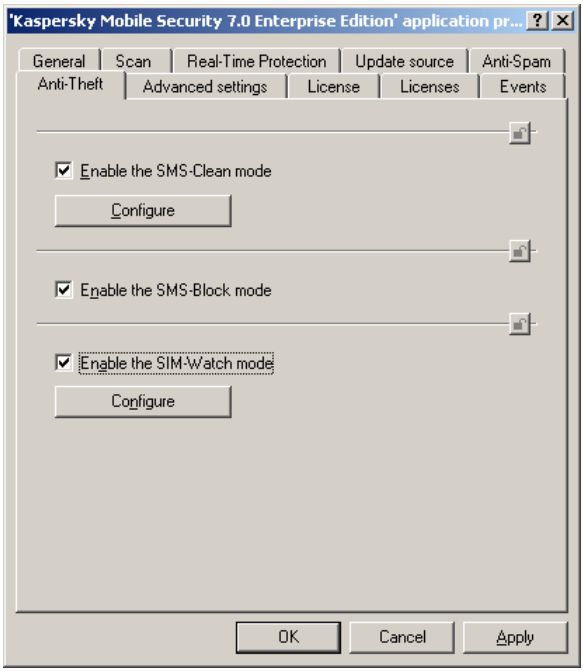

Figura 39. Separador **Anti-Roubo**

4.7. Visualizar informação sobre as configurações adicionais

No separador **Configurações Adicionais** (ver Figura 40) pode ver informação e inserir alterações nas configurações de funcionamento da Firewall, assim como alterar a frequência de ligação ao Servidor de Administração.

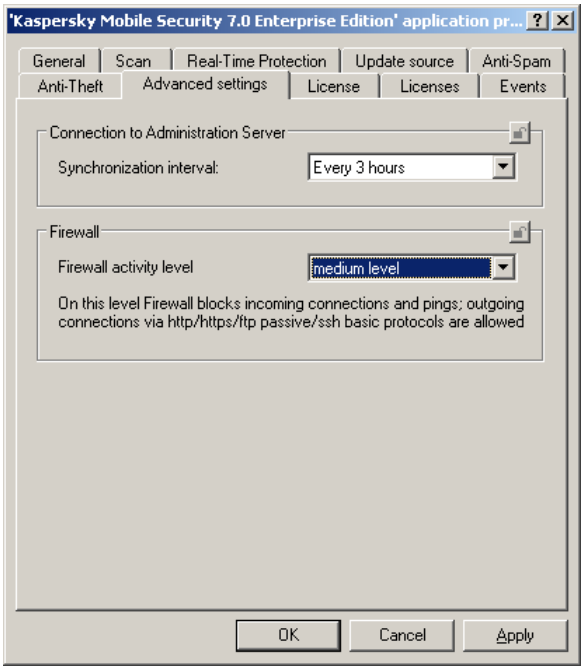

Figura 40. Separador **Configurações Adicionais**

4.8. Visualizar detalhes da chave

O separador **Licença** (ver Figura 41) contém informação sobre a chave instalada no dispositivo móvel.

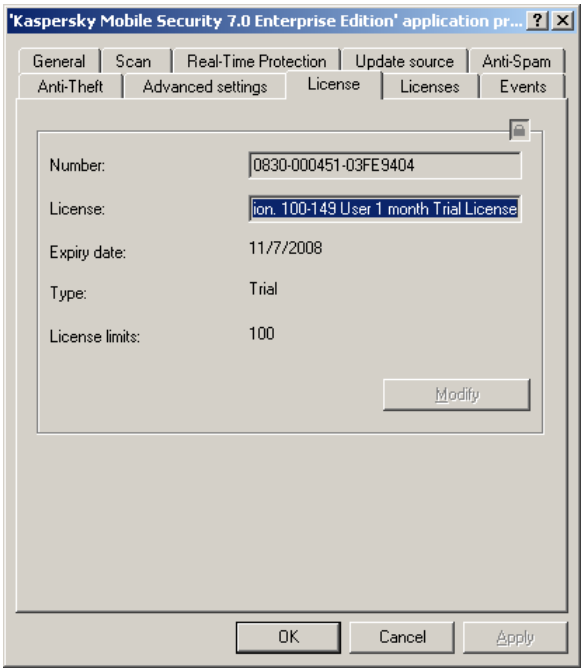

Figura 41. Separador **Licença**

4.9. Visualizar informação sobre eventos

No decorrer do seu funcionamento, o Kaspersky Mobile Security gera um determinado conjunto de eventos. Cada evento tem uma característica que reflecte o seu nível de gravidade. Existem quatro níveis de gravidade: evento crítico, falha funcional, aviso e mensagem informativa.

Os eventos do mesmo tipo podem ter diferentes níveis de importância, dependendo da situação em que esses eventos ocorreram.

O separador **Eventos** (ver Figura 42) apresenta os tipos de eventos ocorridos no funcionamento da aplicação e registados no relatório, assim como a localização do relatório e o modo de notificação do administrador e de outros utilizadores sobre a ocorrência do evento.

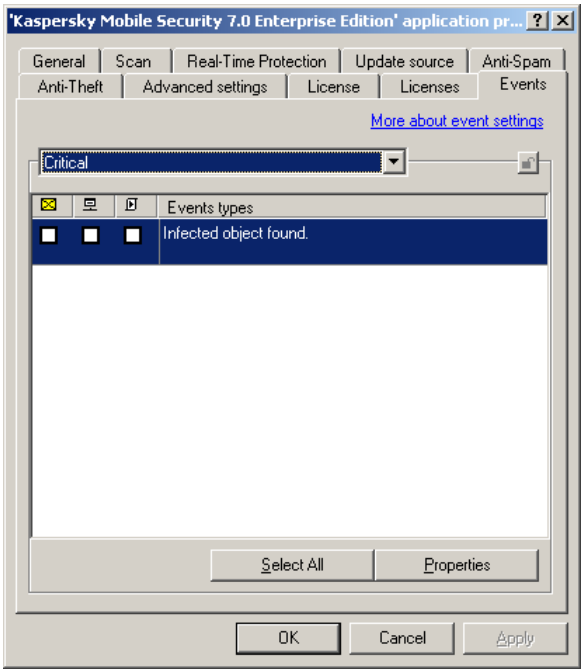

Figura 42. Separador **Eventos**

APÊNDICE A. KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997 e actualmente é a empresa russa líder no desenvolvimento de uma vasta gama de produtos de software de segurança de informação, incluindo sistemas antivírus, anti-spam e anti-hackers.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, Benelux, China, Polónia, Roménia e EUA (Califórnia). Um novo departamento da empresa, o Centro Europeu de Pesquisa Antivírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 1000 especialistas altamente qualificados, dos quais 10 têm graduações M.B.A. e 16 têm doutoramentos. Vários especialistas antivírus seniores da Kaspersky Lab são membros da Computer Anti-virus Researchers Organization (CARO).

Os bens mais valiosos da nossa empresa são a experiência e o conhecimento únicos acumulados pelos nossos especialistas ao longo de 14 anos a combater vírus de computador. Uma análise detalhada das actividades dos vírus de computador permite que os especialistas da empresa consigam prever as tendências no desenvolvimento de software malicioso e forneçam aos nossos utilizadores uma protecção atempada contra novos tipos de ataques. Esta vantagem é a base dos produtos e serviços da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente dos outros fornecedores no fornecimento de uma cobertura antivírus abrangente para os nossos clientes.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver muitos dos padrões modernos de software antivírus. O produto emblemático da empresa, o Kaspersky Anti-Virus®, protege com fiabilidade todos os tipos de sistemas de computadores contra ataques de vírus, incluindo estações de trabalho, servidores de ficheiros, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão fáceis de utilizar maximizam o nível de automação da protecção antivírus para computadores e redes empresariais. Um grande número fabricantes a nível mundial usam o núcleo do Kaspersky Anti-Virus nos seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, como a total conformidade com as necessidades específicas dos clientes. Concebemos, implementamos e damos apoio a sistemas empresariais antivírus. A base de dados antivírus da Kaspersky Lab é actualizada a cada

hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, disponível em várias línguas.

Se tiver alguma questão, comentário ou sugestão, pode contactar-nos através dos nossos distribuidores ou contactar, directamente, a Kaspersky Lab. Teremos todo o prazer em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com nossos produtos. Receberá respostas completas e abrangentes a todas as suas questões.

Site oficial da Kaspersky Lab:	http://www.kaspersky.pt
Enciclopédia de Vírus:	http://www.viruslist.com
Laboratório Antivírus:	newvirus@kaspersky.com (apenas para enviar objectos suspeitos em arquivos) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (para enviar pedidos aos analistas de vírus)
Fórum na Internet da Kaspersky Lab:	http://forum.kaspersky.com

APÊNDICE B. CONTRATO DE LICENCA DE UTILIZADOR FINAL DO KASPERSKY LAB

Contrato Padrão de Licença de Utilizador Final

AVISO LEGAL IMPORTANTE A TODOS OS UTILIZADORES: LEIA COM ATENÇÃO O SEGUINTE ACORDO LEGAL ANTES DE COMEÇAR A UTILIZAR O SOFTWARE.

AO CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU AO INTRODUZIR SÍMBOLO(S) CORRESPONDENTE(S) CONCORDA EM ESTAR VINCULADO PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESSA ACÇÃO SIMBOLIZA A SUA ASSINATURA E ESTÁ A CONCORDAR ESTAR VINCULADO AO CONTRATO, CONSTITUINDO UMA PARTE DO MESMO, E CONCORDA QUE ESTE CONTRATO É EXECUTÓRIO COMO QUALQUER OUTRO CONTRATO NEGOCIADO POR ESCRITO E ASSINADO POR SI.** SE NÃO CONCORDAR COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO O INSTALE.

O SOFTWARE PODE SER ACOMPANHADO POR UM CONTRATO ADICIONAL OU OUTRO DOCUMENTO SEMELHANTE ("CONTRATO ADICIONAL") QUE PODE DEFINIR O NÚMERO DE COMPUTADORES ONDE SE PODE USAR O SOFTWARE, O PERÍODO DE UTILIZAÇÃO DO SOFTWARE, TIPO DE OBJECTOS PRETENDIDOS COM O USO DO SOFTWARE E OUTRAS CONDIÇÕES DA COMPRA, AQUISIÇÃO E USO. ESTE CONTRATO ADICIONAL CONSTITUI PARTE ***INTEGRANTE DO CONTRATO DE LICENÇA.***

DEPOIS DE CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU APÓS TER INTRODUZIDO O(S) SÍMBOLO(S) CORRESPONDENTE(S), TEM O DIREITO DE UTILIZAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

1.1. **Software** refere-se ao software, incluindo quaisquer Actualizações e materiais relacionados.

1.2. **Detentor dos Direitos** (proprietário de todos os direitos, quer exclusivos ou relativos ao Software) refere-se à Kaspersky Lab ZAO, uma empresa incorporada de acordo com as leis da Federação Russa.

1.3. **Computador(es)** refere-se ao(s) hardware(s), incluindo os computadores pessoais, portáteis, estações de trabalho, assistentes digitais pessoais, 'smart phones', dispositivos manuais ou outros dispositivos electrónicos para os quais o Software foi concebido e onde o Software será instalado e/ou usado.

1.4. **Utilizador Final** refere-se ao(s) indivíduo(s) que instalam ou utilizam o Software a seu favor ou que utilizam legalmente uma cópia do Software; ou, se o Software for transferido ou instalado em nome de uma organização, quando se refere a um funcionário, *"Utilizador Final"* refere-se ainda à organização para a qual o Software foi transferido ou instalado ficando por este meio claramente definido que essa organização autorizou a pessoa que aceitou este contrato a fazê-lo em seu nome. Para fins deste contrato, o termo *"organização",* sem limitações, inclui quaisquer parcerias, empresas de responsabilidade limitada, corporações, associações, empresas de capitais mistos, empresas de crédito, "joint ventures", sindicatos de trabalho, empresas não constituídas em sociedade ou autoridades governamentais.

1.5. **Parceiro(s)** refere-se a organizações ou indivíduo(s), que distribuem o Software com base num contrato e numa licença do Detentor dos Direitos.

1.6. **Actualização(ões)** refere-se a todas as actualizações, revisões, correcções ("patches"), melhorias, "fixes", modificações, cópias, adições ou pacotes de manutenção, etc.

1.7. **Manual do Utilizador** refere-se ao manual do utilizador, guia do administrador, livro de referências e material explicativo ou de outro tipo relacionado.

1.8. **Aquisição do Software** refere-se à compra do Software ou à aquisição do Software nos termos definidos em contratos adicionais, incluindo a aquisição a título gratuito.

2. Concessão de licença

2.1. O Detentor de Direitos concede, por este meio, uma licença de não exclusividade ao Utilizador Final que lhe permite armazenar, carregar, instalar, executar e visualizar (para "utilizar") o Software num número específico de Computadores, tendo como finalidade ajudar a proteger o Computador do Utilizador Final no qual o Software está instalado, contra as ameaças descritas no Manual do Utilizador, de acordo com todos os requisitos técnicos descritos no Manual do Utilizador e com os termos e condições deste Contrato (a "Licença") e o utilizador final aceita esta Licença:

Versão experimental. Se recebeu, transferiu e/ou instalou uma versão experimental do Software sendo-lhe por este meio concedida uma

licença de avaliação para o Software, só pode utilizar o Software para fins de avaliação e apenas durante o período de avaliação único aplicável, a não ser se indicado o contrário, a contar da data da instalação inicial. A utilização do Software para outros fins ou para além do período de avaliação aplicável é estritamente proibida.

Software de vários ambientes; Software de vários idiomas; Software de dualidade de multimédia; várias cópias; pacotes. Se utilizar versões diferentes do Software ou edições do Software em idiomas diferentes, se receber o Software em vários suportes, se receber várias cópias do Software ou se receber o Software num pacote junto com outro software, o número total permitido de Computadores em que as versões do Software estão instaladas devem corresponder ao número total de computadores especificados nas licenças obtidas junto do Detentor dos Direitos e, *a não ser* que os termos da licença indiquem o contrário, cada licença adquirida dá-lhe o direito de instalar e utilizar o Software nessa quantidade de Computador(es), como especificado nas Cláusulas 2.2 e 2.3.

2.2. Se o Software foi adquirido num meio físico, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na embalagem do Software ou especificada no contrato adicional.

2.3. Se o Software foi adquirido através da Internet, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na Licença do Software ou no contrato adicional quando este foi adquirido.

2.4. Tem o direito de fazer uma cópia do Software apenas para fins de cópia de segurança e apenas para substituir a cópia legal caso essa cópia se perca, seja destruída ou fique inutilizada. Esta cópia de segurança não pode ser utilizada para outros fins e tem de ser destruída se perder o direito de utilização do Software ou quando a licença de Utilizador Final expirar ou for rescindida por qualquer outra razão, de acordo com a legislação em vigor no país de residência principal do Utilizador Final ou no país onde o mesmo está a utilizar o Software.

2.5. A partir do momento em que o Software foi activado ou que o ficheiro da chave de licença foi instalado (à excepção de uma versão experimental do Software), tem o direito de receber os seguintes serviços pelo período definido especificado na embalagem de Software (se o Software foi adquirido num meio físico) ou especificado durante a aquisição (se o Software foi adquirido através da Internet):

- Actualizações do Software através da Internet quando e como o Detentor dos Direitos os publicar no seu próprio website ou através de outros serviços online. Quaisquer Actualizações que possa receber passam a fazer parte do Software e os termos e condições deste Contrato aplicam-se às mesmas;

- Assistência técnica através da Internet e assistência técnica através de uma linha telefónica grátis.

3. Activação e Termo

3.1. Se o Utilizador Final modificar o seu Computador ou fizer alterações ao software de outros fabricantes instalado nesse mesmo Computador, o Detentor dos Direitos poderá exigir que repita a activação do Software ou a instalação do ficheiro da chave de licença. O Detentor dos Direitos reserva-se o direito de utilizar quaisquer meios ou procedimentos de verificação para confirmar a validade da Licença e/ou a legalidade de uma cópia instalada do Software e/ou utilizada no Computador do Utilizador Final.

3.2. Se o Software foi adquirido num meio físico, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado na embalagem. Esse período terá início a partir do momento de aceitação deste Contrato ou nos termos especificados no contrato adicional.

3.3. Se o Software foi adquirido através da Internet, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado durante a aquisição ou nos termos especificados no contrato adicional.

3.4. Tem o direito de utilizar uma versão experimental do Software, como disposto na Cláusula 2.1 sem que tenha de pagar nada durante o período de avaliação (30 dias) desde o momento em que o Software é activado, de acordo com este Contrato, *desde que* a versão experimental não de ao Utilizador Final acesso a Actualizações e a assistência técnica através da Internet e da linha telefónica.

3.5. A Licença para Utilização do Software está limitada ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (como aplicável) e o restante período pode ser visto através dos meios descritos no Manual do Utilizador.

3.6. Se tiver adquirido o Software que se destina a ser usado em mais do que um Computador, a sua Licença para Usar o Software estará limitada ao período de tempo que tem início com a data de activação do Software ou da instalação do ficheiro da chave de licença no primeiro Computador.

3.7. Sem prejuízo de quaisquer recursos legais ou de justiça natural que o Detentor dos Direitos possa ter, caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final, o Detentor dos Direitos pode, em qualquer altura e sem qualquer aviso prévio ao Utilizador Final, rescindir esta Licença de utilização do Software sem reembolsar o preço de compra ou qualquer outra parte do mesmo.

3.8. Concorda que, ao utilizar o Software e qualquer relatório ou informações derivadas resultantes da utilização deste Software, irá

cumprir todas as leis e regulamentos internacionais, nacionais, estatais, regionais e locais aplicáveis, incluindo, mas não se limitando às leis da privacidade, direitos de autor, controlo de exportação e obscenidade.

3.9. Excepto quando especificamente indicado neste documento, não pode transferir nem atribuir a terceiros nenhum dos direitos a si concedidos, ao abrigo deste Contrato, nem nenhuma das suas obrigações em conformidade com o presente.

4. Assistência técnica

A assistência técnica descrita na Cláusula 2.5 deste Contrato é fornecida ao Utilizador Final depois de ter sido instalada a mais recente Actualização do Software (excepto quando se trata de uma versão experimental do Software).
Serviço de assistência técnica: http://support.kaspersky.com

5. Limitações

5.1. Não deve emular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou inverter a engenharia do Software, nem desmontar ou criar trabalhos dele derivados e baseados no Software ou em qualquer parte do mesmo, sendo que a única excepção é a existência de um direito sem limitações concedido ao Utilizador Final pela legislação aplicável, bem como não pode reduzir qualquer parte do Software a uma forma legível, nem transferir o Software licenciado, ou qualquer outro subconjunto do Software licenciado, nem permitir que terceiros o façam, excepto até ao ponto em que as restrições indicadas sejam expressamente proibidas pela lei aplicável. Não se pode utilizar o código de binários nem a fonte do Software, nem inverter a engenharia, para recriar o algoritmo do programa, que é registado. Todos os direitos que não são aqui expressamente concedidos são reservados pelo Detentor dos Direitos e/ou pelos seus fornecedores, como aplicável. Qualquer utilização não autorizada do Software resultará na rescisão imediata e automática deste Contrato e da Licença concedida pelo mesmo e pode resultar em processos criminais e/ou civis contra o Utilizador Final.

5.2. Não pode transferir os direitos de utilização do Software para terceiros, excepto conforme disposto no contrato adicional.

5.3. Não pode fornecer o código de activação e/ou a ficheiro com a chave da licença a terceiros nem permitir que terceiros acedam ao código de activação e/ou chave da licença que são considerados dados confidenciais do Detentor dos Direitos e terá todo o cuidado em proteger o código de activação e/ou chave da licença contando que pode transferir o código de activação e/ou a chave de licença a terceiros como definido no contrato adicional.

5.4. Não pode alugar, arrendar ou emprestar o Software a terceiros.

5.5. Não pode utilizar o Software para criação de dados ou de software utilizado para a detecção, bloqueio ou tratamento das ameaças descritas no Manual do Utilizador.

5.6. O Detentor dos Direitos tem o direito de bloquear o ficheiro da chave ou rescindir a Licença de utilização do Software caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final sem qualquer reembolso.

5.7. Se o Utilizador Final está a utilizar a versão experimental do Software, não tem o direito de receber a Assistência Técnica especificada na Cláusula 4 deste Contrato e o Utilizador Final não tem o direito de transferir a licença ou os direitos de utilização do Software a terceiros.

6. Garantia limitada e Renúncias

6.1. O Detentor dos Direitos garante que o Software irá cumprir substancialmente o que lhe é devido, de acordo com as especificações e descrições indicadas no Manual do Utilizador *desde que, no entanto,* essa garantia limitada não se aplique ao seguinte: (w) As deficiências e violações relacionadas do computador para as quais o Detentor dos Direitos renuncia expressamente todas as responsabilidades da garantia; (x) avarias, defeitos ou falhas resultantes de má utilização; abuso; acidente; negligência; instalação imprópria, operação ou manutenção; roubo; vandalismo; casos fortuitos; actos de terrorismo; falhas de energia ou picos de potência; acidentes; alterações, modificações não permitidas ou reparações por qualquer parte além do Detentor de Direitos; ou as acções do Utilizador Final ou causas que estejam para além do controlo razoável do Detentor dos Direitos; (y) qualquer defeito que o Utilizador Final não tenha dado a conhecer ao Detentor de Direitos logo que possível depois de o defeito aparecer pela primeira vez; e (z) incompatibilidade provocada pelos componentes de hardware e/ou software instalados no Computador do Utilizador Final.

6.2. O Utilizador Final reconhece, aceita e concorda que não existe nenhum software isento de erros e o Utilizador Final é aconselhado a fazer cópias de segurança do Computador, com a frequência e a fiabilidade adequada para o Utilizador Final.

6.3. O Detentor dos Direitos não oferece qualquer garantia de que o Software irá funcionar correctamente em caso de violações dos termos descritos no Manual do Utilizador ou neste Contrato.

6.4. O Detentor dos Direitos não garante que o Software irá funcionar correctamente se o Utilizador Final não fizer regularmente transferências das Actualizações especificadas na Cláusula 2.5 deste Contrato.

6.5. O Detentor dos Direitos não garante protecção das ameaças descritas no Manual do Utilizador após a expiração do período especificado nas

Cláusulas 3.2 ou 3.3 deste Contrato ou após a rescisão da Licença de utilização do Software, caso ela seja rescindida por qualquer razão.

6.6. O SOFTWARE É ENTREGUE "TAL COMO ESTÁ" E O DETENTOR DOS DIREITOS NÃO FAZ QUALQUER REPRESENTAÇÃO NEM DÁ QUAISQUER GARANTIAS DA SUA UTILIZAÇÃO OU DESEMPENHO. EXCEPTO NO QUE SE REFERE A QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO NA MEDIDA EM QUE NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEI APLICÁVEL, O DETENTOR DOS DIREITOS E OS SEUS PARCEIROS NÃO CONCEDEM QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER SEJA POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, UTILIZAÇÃO OU QUALQUER OUTRO) QUE, SEM OUTRO ASSUNTO INCLUINDO, MAS NÃO SE LIMITANDO, A NÃO INFRACÇÃO DOS DIREITOS DE TERCEIROS, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE A UM FIM ESPECÍFICO. O UTILIZADOR FINAL ASSUME TODAS AS AVARIAS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE POR SELECCIONAR O SOFTWARE DE MODO A CONSEGUIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, UTILIZAÇÃO E RESULTADOS OBTIDOS DO SOFTWARE. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O DETENTOR DOS DIREITOS NÃO CONCEDE QUALQUER REPRESENTAÇÃO E NÃO DÁ GARANTIAS DE QUE O SOFTWARE NÃO CONTÉM ERROS OU NÃO ESTÁ LIVRE DE INTERRUPÇÕES OU OUTRAS FALHAS OU QUE O SOFTWARE VAI AO ENCONTRO DE TODOS E QUAISQUER REQUISITOS DO UTILIZADOR FINAL TENHAM OU NÃO SIDO DIVULGADOS AO DETENTOR DOS DIREITOS.

7. Exclusão e limitação da responsabilidade

NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM CASO ALGUM O DETENTOR DOS DIREITOS OU OS SEUS PARCEIROS SÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, ACIDENTAIS, PUNITIVOS, INDIRECTOS OU CONSEQUENCIAIS, SEJAM ELES QUAIS FOREM, (INCLUINDO, MAS NÃO SE LIMITANDO A DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS, OU OUTRAS, POR INTERRUPÇÃO DO NEGÓCIO, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDAS DE DADOS OU PROGRAMAS, POR FALHA DE PAGAMENTO DE QUAISQUER DIREITOS INCLUINDO QUAISQUER DIREITOS LEGAIS, DIREITOS DE LEALDADE OU DIREITOS DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PERDA ECONÓMICA, E POR QUALQUER PERDA PECUNIÁRIA OU OUTRA, SEJA ELA QUAL FOR) QUE SURJA DE UMA QUALQUER FORMA RELACIONADA COM A UTILIZAÇÃO OU INCAPACIDADE DE UTILIZAÇÃO DO SOFTWARE, A

DISPOSIÇÃO OU FALHA DE FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, SOFTWARE E CONTEÚDOS RELACIONADOS ATRAVÉS DO SOFTWARE OU QUE, POR OUTRO LADO, SURJA DA UTILIZAÇÃO DO SOFTWARE, OU, AO CONTRÁRIO, MEDIANTE OU EM LIGAÇÃO A QUALQUER DISPOSIÇÃO DESTE CONTRATO, OU QUE SURJA DE QUALQUER VIOLAÇÃO DO CONTRATO OU QUALQUER DELITO (INCLUINDO NEGLIGÊNCIA, MÁ REPRESENTAÇÃO OU QUALQUER OBRIGAÇÃO OU DEVER DE RESPONSABILIDADE LIMITADA), OU QUALQUER VIOLAÇÃO DOS DEVERES LEGAIS, OU QUALQUER VIOLAÇÃO DA GARANTIA DO DETENTOR DOS DIREITOS OU QUALQUER UM DOS SEUS PARCEIROS, MESMO QUE O DETENTOR DOS DIREITOS OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DESSES DANOS.

O UTILIZADOR FINAL CONCORDA QUE, CASO O DETENTOR DOS DIREITOS E/OU OS SEUS PARCEIROS SEJAM TIDOS COMO RESPONSÁVEIS, A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO SOFTWARE. EM CASO ALGUM DEVE A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS EXCEDER AS TAXAS PAGAS PELO SOFTWARE AO DETENTOR DOS DIREITOS OU AO PARCEIRO (COMO SE APLICAR).

NADA NESTE ACORDO EXCLUI OU LIMITA QUAISQUER REIVINDICAÇÕES DE MORTE E FERIMENTOS PESSOAIS. ALÉM DISSO, NO CASO DE ALGUMA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO POSSAM SER EXCLUÍDAS OU LIMITADAS DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS ESSA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NÃO SE DEVEM APLICAR AO UTILIZADOR FINAL E CONTINUA A FICAR VINCULADO POR TODAS AS RESTANTES RESPONSABILIDADES, EXCLUSÕES E LIMITAÇÃO.

8. GNU e outras licenças de terceiros

O Software pode incluir alguns programas de software licenciados (ou sublicenciados) ao utilizador no âmbito da Licença Pública Geral GNU (General Public License, GPL) ou outras licenças semelhantes de software grátis que, entre outros direitos, permite ao utilizador copiar, modificar e redistribuir determinados programas, ou partes do mesmo, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças necessitarem que, para qualquer software que é distribuído às pessoas num formato de binário executável, que o código fonte também seja tornado disponível a esses utilizadores, então o código fonte deve ser tornado disponível enviando o pedido para source@kaspersky.com ou é fornecido com o Software. Se quaisquer licenças de Software de Código Aberto precisarem que o Detentor dos Direitos forneça direitos de utilização, cópia ou modificação de um programa de Software

de Código Aberto, mais vastos do que os direitos concedidos neste Contrato, então esses direitos devem ter precedência sobre os direitos e restrições aqui indicados.

9. Posse dos direitos de propriedade

9.1 Concorda que o Software e a respectiva autoria, os sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Software, são propriedade intelectual registada e/ou segredo comercial, de grande valor, do Detentor dos Direitos ou dos seus parceiros e que o Detentor dos Direitos e os seus parceiros, conforme aplicável, estão protegidos pela lei civil e criminal e pelas leis de direitos de autor, segredos comerciais, marcas registadas e patentes da Federação Russa, União Europeia e Estados Unidos e de outros países, bem como pelos tratados internacionais. Este Contrato não concede ao Utilizador Final quaisquer direitos no que se refere à propriedade intelectual, incluindo as marcas comerciais ou as marcas dos serviços do Detentor dos Direitos e/ou dos seus parceiros ("Marcas Comerciais"). Pode utilizar as Marcas Comerciais apenas e até ao ponto de identificar resultados impressos produzidos pelo Software de acordo com a prática das marcas comerciais aceites, incluindo a identificação do nome do proprietário da Marca Comercial. A utilização de qualquer Marca Comercial não dá ao Utilizador Final quaisquer direitos de propriedade sobre essa Marca Comercial. O Detentor dos Direitos e/ou os seus parceiros são proprietários e retêm todos os direitos, títulos e interesse no Software e em relação ao mesmo, incluindo, sem limitações, quaisquer correcções de erros, melhoramentos, Actualizações ou outras modificações ao Software, quer sejam feitas pelo Detentor dos Direitos ou por quaisquer terceiros, e todos os direitos sobre direitos de autor, patentes, segredos comerciais, marcas comerciais e outras propriedades intelectuais contidas neste documento. A possessão, instalação ou utilização do Software não lhe transfere qualquer título para a propriedade intelectual no Software e não adquire quaisquer direitos ao Software excepto quando expressamente estipulado neste Contrato. Todas as cópias do Software realizadas nos termos do presente Contrato têm de conter os mesmos avisos de propriedade que aparecem no Software. Excepto como aqui indicado, este Contrato não concede ao Utilizador Final quaisquer direitos de propriedade intelectual sobre o Software e o Utilizador Final reconhece que a Licença, tal como está definida aqui, concedida nos termos deste Contrato, concede apenas o direito de utilização limitada mediante os termos e as condições deste Contrato. O Detentor dos Direitos reserva-se todos os direitos não expressamente concedidos ao Utilizador Final neste Contrato.

9.2 O Utilizador Final reconhece que o código fonte, o código de activação e/ou o ficheiro da chave da licença do Software são propriedade do

Detentor dos Direitos e constituem segredos comerciais do Detentor dos Direitos. Concorda em não modificar, adaptar, traduzir, inverter a engenharia, descompilar, desmontar ou tentar, de qualquer outro modo, descobrir o código fonte do Software seja de que forma for.

9.3 Concorda em não modificar nem alterar o Software seja de que forma for. Não pode remover nem alterar quaisquer avisos de direitos de autor ou outros avisos de propriedade em nenhuma cópia do Software.

10. Lei vigente; arbitragem

Este Contrato é regido, e será interpretado, de acordo com as leis da Federação Russa sem referência a conflitos de regras e princípios legais. Este Contrato não será regido pela Convenção das Nações Unidas referente a Contratos para a Venda Internacional de Bens, a aplicação da qual é expressamente excluída. Qualquer litígio que surja no seguimento da interpretação ou aplicação dos termos deste Contrato ou qualquer infracção ao mesmo, a não ser que se resolva por negociação directa, deverá ser resolvido no Tribunal de Arbitragem Comercial Internacional na Câmara do Comércio e Indústria da Federação Russa em Moscovo, na Federação Russa. Qualquer decisão apresentada pelo árbitro deve ser final e obrigatória para as partes e qualquer julgamento sobre essa decisão de arbitragem pode ser feita cumprir em qualquer tribunal da jurisdição competente. Nada nesta Secção 10 deve impedir que uma Parte procure e obtenha qualquer reparação equitativa de um tribunal da jurisdição competente, quer seja antes, durante ou depois dos processos de arbitragem.

11. Período para interpor acções

Nenhuma acção, independentemente da forma, que surja das transacções nos termos deste Contrato, pode ser trazida aqui por qualquer uma das partes mais de um (1) ano depois da causa da acção ter ocorrido, ou de ter sido descoberta a ocorrência, excepto que uma acção por violação dos direitos de propriedade intelectual seja trazida dentro do período legal máximo aplicável.

12. Contrato completo; redução; sem renúncia

Este Contrato constitui todo o contrato entre o Utilizador Final e o Detentor dos Direitos e substitui quaisquer outros acordos prévios, propostas, comunicações ou publicidade, oral ou escrita, referente ao Software ou ao assunto deste Contrato. O Utilizador Final reconhece que leu este Contrato, compreendeu-o e concorda em estar vinculado pelos seus termos. Se qualquer disposição deste Contrato for indicada por um tribunal de jurisdição competente como sendo inválida, nula ou inexequível por qualquer razão, no todo ou em parte, essa disposição será ainda mais restritamente interpretada de tal forma que será legal e executória, e todo o Contrato não falhará por conta do mesmo e o saldo do Contrato continuará válido e com efeitos até ao máximo permitido por lei ou equidade ao mesmo tempo que preserva, até ao máximo possível, a sua

intenção original. Nenhuma renúncia de nenhuma disposição ou condição aqui indicadas será válida a não ser por escrito e assinada pelo Utilizador Final e um representante autorizado do Detentor dos Direitos desde que nenhuma renúncia de nenhuma infracção de nenhuma disposição deste Contrato constitua uma renúncia de qualquer infracção anterior, concorrente ou subsequente. A não insistência por parte do Detentor dos Direitos no que se refere a fazer valer o desempenho rigoroso de todas as disposições deste Contrato ou nenhum direito deve ser interpretado como sendo uma renúncia de qualquer uma dessas disposições ou direitos.

13. Informações de contacto do Detentor dos Direitos

Se tiver quaisquer dúvidas referentes a este Contrato ou se, por qualquer razão, pretender contactar o Detentor dos Direitos, contacte o nosso Departamento de Apoio ao Cliente em:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscovo, 123060
Federação Russa
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Website: www.kaspersky.com