

F-Secure Mobile Security™ for S60

1. Instalação e ativação

Versão anterior Não é necessário desinstalar a versão anterior do F-Secure Mobile Anti-Virus. Verifique as configurações do F-Secure Mobile Security depois de instalar a nova versão.

Instalação **Para instalar:**

- Faça o download do arquivo de instalação para o computador e mova o arquivo para o aparelho,
- Faça o download do arquivo de instalação para o computador e instale o produto através do Nokia PC Suite ou
- Faça o download da instalação diretamente para o aparelho. A instalação é iniciada automaticamente.

Após a instalação, reinicie o dispositivo se isso for solicitado. Quando a instalação estiver concluída, é necessário ativar o produto. Se o produto não for ativado, o dispositivo não estará protegido.

Ativação **Para iniciar a ativação:**

1. Abra o aplicativo. A tela de boas-vindas é exibida.
2. Pressione **Continuar**.
3. Selecione o tipo de ativação:
 - Para ativar o produto apenas com o recurso Antirroubo ativado, selecione **Apenas Antirroubo** como o tipo de ativação e pressione **Continuar**.
 - Para obter a versão totalmente licenciada, selecione **Número da assinatura** como o tipo de ativação e pressione **Continuar**. Digite o número da assinatura e pressione **OK**.
4. Pressione **Sim** e selecione o ponto de acesso à Internet para conectar-se ao servidor de atualização e começar a fazer o download das atualizações. O aplicativo conecta-se ao serviço de atualização e envia o seu número de assinatura. Durante a primeira atualização, o aplicativo faz o download do banco de dados de definições de vírus mais recente.
5. Após o produto ter feito o download de todas as atualizações necessárias, o aplicativo estará completo. Pressione **Continuar** para concluir a ativação.

Após a conclusão da ativação, verifique a presença de vírus no dispositivo para garantir que ele esteja limpo. Consulte a seção [Verificação da presença de vírus](#) abaixo.



Você deve verificar o dispositivo sempre que o aplicativo solicitar.

2. Verificação da presença de vírus

O F-Secure Mobile Security funciona em segundo plano e verifica os arquivos automaticamente.

1. O F-Secure Mobile Security notifica-o caso encontre um vírus durante a verificação em tempo real. Pressione **Sim** para exibir os arquivos infectados imediatamente ou **Não** para visualizá-los mais tarde.
2. A exibição de infecções contém uma lista de arquivos infectados no dispositivo e se o arquivo está em quarentena ou liberado no momento.

Para visualizar mais detalhes sobre um arquivo infectado:

1. Role até o arquivo infectado e pressione a tecla de seleção.
2. Selecione **Ver**.
3. A exibição de detalhes da infecção mostra o caminho e nome do arquivo infectado, assim como o nome do vírus que o infectou.

Processamento de arquivos infectados

Para processar arquivos infectados:

1. Na exibição de infecções, avance até o arquivo infectado a ser processado.
2. Pressione a tecla de seleção.
3. Selecione uma das seguintes ações:
 - **Excluir** - exclui o arquivo infectado. Essa é a opção recomendada. O arquivo será removido completamente do dispositivo.
 - **Colocar em quarentena** - coloca o arquivo infectado em quarentena se ele ainda não estiver posto em quarentena. O arquivo em quarentena é bloqueado e não pode danificar o dispositivo quando o F-Secure Mobile Security está ativado.
 - **Liberar** - libera o arquivo em quarentena. Se liberar um arquivo, ele não estará mais bloqueado. Você pode acessá-lo por sua conta e risco.

3. Bloqueio do tráfego de rede não autorizado

O firewall do F-Secure Mobile Security funciona silenciosamente em segundo plano. Ele monitora o tráfego de entrada e de saída da Internet e da rede, e protege contra tentativas de invasão. Os níveis de firewall predefinidos permitem a alteração do nível de proteção, de acordo com as suas necessidades.


Seleção do nível de segurança

Para selecionar o nível de segurança:

1. Vá até **Configurações** e pressione a tecla de seleção.
2. Selecione **Firewall** na lista de seleção de configurações.
3. Selecione o nível de firewall desejado:
 - **Negar tudo** - interrompe todo o tráfego de rede.
 - **Alta** - permite os aplicativos mais usados e bloqueia todo o tráfego de entrada.
 - **Normal** - permite todas as conexões de saída e bloqueia todo o tráfego de entrada.
 - **Permitir tudo** - permite todo o tráfego de rede.
 - **Personalizado** - permite o tráfego de rede baseado em suas regras personalizadas. Para editar o conjunto de regras personalizadas, selecione **Opções > Editar regras personalizadas** quando o nível de segurança **Personalizado** estiver selecionado.

4. Proteção de informações confidenciais

Com o Anti-Theft, é possível assegurar que seu dispositivo ou os dados armazenados no dispositivo não serão usados de forma inadequada em caso de roubo.


 *Já que cartões de memória podem ser facilmente removidos, armazene suas informações confidenciais na memória do dispositivo, que pode ser bloqueada ou removida com o Anti-Theft.*

Uso do bloqueio do dispositivo

Anti-Theft bloqueia automaticamente o dispositivo quando o cartão SIM é alterado. É possível desbloquear o dispositivo apenas com o código de segurança.

Para ativar o bloqueio de dispositivo:

1. Vá até **Configurações** e pressione a tecla de seleção.
2. Selecione **Anti-Theft** na lista de seleção de configurações.
3. Digite o **Código de segurança**. O código de segurança precisa ter pelo menos 5 caracteres. Guarde-o em local seguro.

 *Seu código de segurança protege as configurações do Anti-Theft. É necessário digitar o código de segurança atual antes de alterar as configurações do Anti-Theft.*

4. Se você deseja bloquear o seu dispositivo quando um cartão SIM for alterado, selecione **Sim** em **Bloquear se o SIM for alterado**.

Uso do antirroubo remoto

Com o sistema antirroubo remoto, você pode enviar uma mensagem de texto SMS contendo o seu código de segurança para o seu dispositivo para localizá-lo ou bloqueá-lo ou um código de limpeza para limpar todas as informações contidas nele.

Para ativar o bloqueio remoto:

1. Vá até **Configurações** e pressione a tecla de seleção.
2. Selecione **Anti-Theft** na lista de seleção de configurações.
3. Se desejar ter a opção de bloquear seu dispositivo remotamente, siga estas instruções:
 - a. Insira um **Código de segurança**, se ainda não tiver criado um.
 - b. Ative o **Bloqueio remoto**.

É possível desbloquear o dispositivo apenas com o código de segurança.

4. Se desejar ter a opção de limpar o dispositivo remotamente, siga estas instruções:
 - a. Digite o **Código de limpeza**. O código de limpeza deve ter pelo menos 8 caracteres. Guarde-o em local seguro.
 - b. Ative a **Limpeza remota**.

Quando o dispositivo é limpo, todos os dados armazenados nele são removidos.

Para bloquear ou apagar as informações do seu dispositivo remotamente:

Envie a seguinte mensagem de texto SMS para o seu aparelho.

- Para bloquear o aparelho, envie:
#LOCK#<código de segurança> (Por exemplo: #LOCK#abcd1234)
- Para limpar o aparelho, envie:
#WIPE#<código de limpeza> (Por exemplo: #WIPE#abcd1234)
- Para localizar o aparelho, envie:
#LOCATE#<código de segurança> (Por exemplo:
#LOCATE#abcd1234)



Anti-Theft não armazena nenhum dado de localização, as únicas informações de localização estão na mensagem de texto SMS que é enviada a você.

5. Proteção da navegação da web

A Proteção de navegação protege você de sites que podem roubar suas informações pessoais, como números de cartão de crédito, informações da conta do usuário e senhas.

A Proteção de navegação verifica os sites nos quais você navega com o navegador padrão do seu aparelho. Se você usar um navegador de terceiros, a Proteção de navegação não protege a sua navegação.



Feche o navegador e apague o cache antes de começar a usar a Proteção de navegação.

Para ativar a Proteção de navegação:

1. Vá até **Configurações** e pressione a tecla de seleção.
2. Selecione **Proteção de navegação** na lista de seleção de configurações.
3. Ative a **Proteção de navegação**.
4. Em **Rede a ser usada**, selecione se deseja usar a Proteção de navegação o tempo todo ou apenas quando estiver navegando na web por meio da rede da sua própria operadora:
 - Selecione **Apenas a minha operadora** para usar a Proteção de navegação apenas quando estiver usando a rede da sua própria operadora.
 - Selecione a configuração **Todas as operadoras** para manter a proteção ativada quando estiver viajando e fora da rede da sua operadora.

Modo de privacidade

A Proteção de navegação pode enviar informações de sites que contenham conteúdo perigoso para análise automaticamente para manter a qualidade do serviço. Você pode escolher quais informações deseja enviar para análise.

Para alterar as configurações do modo de privacidade:

1. Vá até **Configurações** e pressione a tecla de seleção.
2. Selecione **Outras configurações** na lista de seleção de configurações.
3. Em Modo de privacidade, selecione
 - Selecione **Apenas estatísticas** para enviar apenas as estatísticas da proteção de navegação e as informações de conexão do servidor.
 - Selecione **Permitir tudo** para enviar estatísticas e informações sobre sites que ainda não foram analisadas ou que contêm conteúdo perigoso.



*Para obter a maior qualidade do serviço, recomendamos que você mantenha a configuração do modo de privacidade como **Permitir tudo**.*

Declaração de privacidade

O envio das informações não compromete a sua privacidade.

Apesar de as informações enviadas serem consideradas pessoais em algumas jurisdições, a sua privacidade é protegida durante o processo. Transferimos as informações de modo seguro, removemos quaisquer informações pessoais desnecessárias, e processamos as informações de modo anônimo e em formato agregado. Desta forma, as informações não podem ser conectadas a você de nenhuma maneira. Nenhuma informação da conta do usuário, do endereço IP ou da licença é incluída nas informações que você envia. Protegemos a sua privacidade ainda mais usando criptografia quando transferimos as informações.

As informações enviadas são usadas para melhorar os recursos de proteção dos nossos serviços e produtos.

6. Manutenção da atualização do produto

Atualizações automáticas

O F-Secure Mobile Security inclui serviços de atualização automática, o que significa que o banco de dados de definições de vírus do aplicativo é atualizado regularmente. Somente um banco de dados de definições de vírus atualizado pode proteger o dispositivo contra os vírus mais recentes. As atualizações automáticas começam a ser usadas após a ativação do produto.

O aplicativo precisa de uma conexão ativa com a internet para fazer as atualizações. Quando há uma conexão com a internet disponível, o aplicativo verifica quando o banco de dados de definições de vírus foi atualizado pela última vez e faz o download de novas atualizações, se necessário.

Atualizações manuais

Para atualizar o aplicativo manualmente:

1. Vá até **Proteção antivírus** e pressione a tecla de seleção.
2. Selecione **Atualizar agora**.
3. Selecione o ponto de acesso à internet para conectar-se ao servidor de atualização. O aplicativo faz o download do banco de dados de definições de vírus e começa a usá-lo imediatamente.
4. Quando a atualização for concluída, pressione **Sim** para verificar a presença de vírus no dispositivo se for solicitado a fazer isso. Consulte a seção **Verificação da presença de vírus** acima.

Atualizações manuais

Quando uma nova versão do F-Secure Mobile Security estiver disponível, uma mensagem será exibida perguntando se você deseja fazer o download. O aplicativo reinicia automaticamente quando a atualização é concluída.

Suporte técnico

A exibição principal da interface do usuário exibe a visão geral da segurança e o status atual.

Se o status exibe que o seu aparelho não está protegido, siga estas instruções:

1. Vá até **Visão geral de segurança** e pressione a tecla de seleção.
2. Selecione o item com o ícone de status amarelo ou vermelho e pressione a tecla de seleção para solucionar o problema.

Para obter mais informações, faça o download do *F-Secure Mobile Security for S60 User's Guide* (em inglês) no site <http://mobile.f-secure.com/>

Se você tiver dúvidas sobre o aplicativo que não estiverem esclarecidas nos guias ou nos serviços on-line do site, entre em contato com o distribuidor F-Secure em sua região ou diretamente com a F-Secure Corporation.

ISENÇÃO DE RESPONSABILIDADE

"F-Secure" e o símbolo de triângulo são marcas registradas da F-Secure Corporation e os nomes de produto da F-Secure assim como símbolos e logotipos são marcas comerciais ou registradas da F-Secure Corporation. Todos os nomes de produtos a que se fez referência neste documento são marcas comerciais ou registradas de suas respectivas empresas. A F-Secure Corporation renuncia o interesse de propriedade nas marcas e nomes de terceiros. Ainda que a F-Secure Corporation faça todo o esforço para garantir que essas informações sejam precisas, a F-Secure Corporation não será responsabilizada por erros ou omissões de fatos contidos neste documento. A F-Secure Corporation reserva o direito de modificar as especificações citadas neste documento sem aviso prévio.

Empresas, nomes e dados usados em exemplos neste documento são fictícios, a menos que tenha sido informado o contrário. Nenhuma parte deste documento pode ser reproduzido ou transmitido de nenhuma forma ou por nenhum meio, eletrônico ou mecânico, para nenhum propósito, sem a permissão expressa e por escrito da F-Secure Corporation.

Esse produto pode estar coberto por uma ou mais patentes da F-Secure, incluindo as seguintes:

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2009 F-Secure Corporation. Todos os direitos reservados

