Manual do Usuário do Aker Secure Roaming

Introdução

Este é o manual do usuário do Aker Secure Roaming. Nos capítulos seguintes, você vai aprender como instalar e configurar os produtos que compoem o Aker Secure Roaming. Esta introdução descreve a organização do manual e as convenções usadas para escrevê-lo.

O que é Aker Secure Roaming?

O sistema Secure Roaming torna possível usuários remotos conectarem em um servidor e estabecer um canal seguro (VPN) para a rede corporativa. Esta VPN é especial por dar um endereço IP dessa rede para o cliente, habilitando-o a trabalhar do mesmo modo que quando ele está fisicamente ligada a ela.

O sistema é constituído de dois produtos:

- **Aker Secure Roaming Server**

  O servidor roda sobre plataformas Windows 2000 (ou mais recente) , FreeBSD 4.7 , FreeBSD 4.9 , RedHat 7.3 e RedHat 9.0.
  Ele recebe conexões e seleciona uma configuração de rede para o usuário de acordo com parâmetros pré-definidos, fazendo o processo de estabelecimento da VPN seja muito simples do ponto de vista do usuário final.

- **Aker Secure Roaming Client**

  O Cliente roda em plataformas Windows 98, Windows 2000 (ou mais recente), Linux com kernel 2.4 e FreeBSD 4.9 (ou mais recente).
  Possui interface do usuário bem simples com pouca coisa a ser configurada além do endereço IP do servidor. Poder ser ajustado para sincronizar a conexão VPN e romper com o status do Windows dialup.

Como este manual se encontra organizado?

Este manual é constituído de diversos capítulos. Cada um deles explica como configurar algumas características do programa. Ele explica também como realizar um melhor ajuste das opções apresentadas para obter um melhor desempenho.

Ainda que você encontre screenshots de sistemas operacionais diferentes ao seu, as interfaces gráficas do usuário (GUIs) aparentam e comportam-se exatamente do mesmo modo em diferentes SOs. A única mudança significativa é o estilo do gerenciador de janelas (*skin*).

Nós recomendamos fortemente que seja lido todo o manual pelo menos uma vez.

Ao longo do manual, você encontrará o simbolo  seguido por algum texto em vermelho. Esse texto descreve algum fato importante que deve ser compreendido completamente para a correta operação do sistema.

1-0 Instalando Aker Secure Roaming

Neste capitulo iremos aprender a instalar e remover os produtos que compoem o Aker Secure Roaming

1-1 Requerimentos de Sistema

- **Aker Secure Roaming Server**
    1. Windows 2000 ou mais recente
    2. Linux (kernel 2.4.x)
    3. FreeBSD 4.7 ou mais recente

- **Aker Secure Roaming Client**
    1. Windows 2000 ou mais recente
    2. Windows 98
    3. Linux (kernel 2.4.x) com KDE ou Gnome
    4. FreeBSD 4.7 ou mais recente com KDE ou Gnome

O hardware mínimo varia muito de acordo com o número de clientes simultâneos e seus respectivos links. O mínimo absoluto requerido é o mesmo dos Sistemas Operacionais citados acima.

O **Client** não consome mais do que 5MB de memória física, sendo capaz de atingir no mínimo uma velocidade de 100Kb/s sem sacrificar uma parcela significativa da CPU em plataformas Pentium-2 de 500MHz .

O **Servidor** consome aproximadamente 50 kB de memória por cliente conectado no além de um valor mínimo de 3MB. O servidor consome CPU instantaneamente de acordo com a velocidade de conexão agregada . Como regra básica deve-se pemitir 300 Mhz de frequência para cada Mbit/s agregado (sem compressão).

Todos periféricos do computador necessitam ser explicitamente suportados pelo sistema operacional utilizado.

1-2 Instalando os produtos

A instalação é simples e objetiva. Siga os passos abaixo.

Instalação Windows

Caso você tenha o arquivo **`AkerSecureRoaming-client-win-1.5-br.exe`** faça o seguinte:

1. Click no botão **Iniciar** para mostrar seu menu.
2. Escolha o ítem **Executar...**
3. Procure pelo arquivo **`AkerSecureRoaming-client-win-1.5-br.exe`** e clique sobre ele.
4. Siga as instruções que aparecem na tela.

Instalação Linux

No linux, os produtos Secure Roaming vêm como um pacote RPM. Este pode ser instalado com a digitação do seguinte comando num shell.

```
rpm -ivh <package-file-name>
```

Altenativamente, você pode usar um gerenciador de pacotes com interface gráfica da sua escolha.

Instalação FreeBSD

No FreeBSD, os produtos Secure Roaming vêm como pacotes padrões. Este pode ser instalado com a digitação do seguinte comando num shell.

```
pkg_add <package-file-name>
```
Altenativamente, você pode usar um gerenciador de pacotes com interface gráfica da sua escolha.

Nota aos usuários Linux e FreeBSD : A interface gráfica do usuário usa a biblioteca QT 3.2.1 . Ela deve ser instalada automaticamente quando o KDE é instalado. Se a biblioteca não estiver instalada sua versão é incompátivel. Por favor, vá para a seção de download do site da Aker e busque pelas bibliotecas necessárias.

1-3 Removendo produtos

Instalação Windows

1. Abra o Painel de Controle
2. Click em `Adicionar ou Remover Programas`
3. Escolha o produto Aker Secure Roaming que você deseja remover.
4. Click no botão `Remover`
5. Siga as instruções da tela

Linux installations

Para Remover os produtos Secure Roaming de seu computador, você pode ou usar seu gerenciador de pacotes gráfico ou digitar o seguinte comando em um shell:

```
rpm -e <package_name>
```

Se você não souber o nome do pacote, digite o seguinte comando para descobrir:

```
rpm -qa | grep Aker
```

FreeBSD installations

Para Remover os produtos Secure Roaming de seu computador, você pode ou usar seu gerenciador de pacotes gráfico ou digitar o seguinte comando em um shell:

```
pkg_delete <package_name>
```

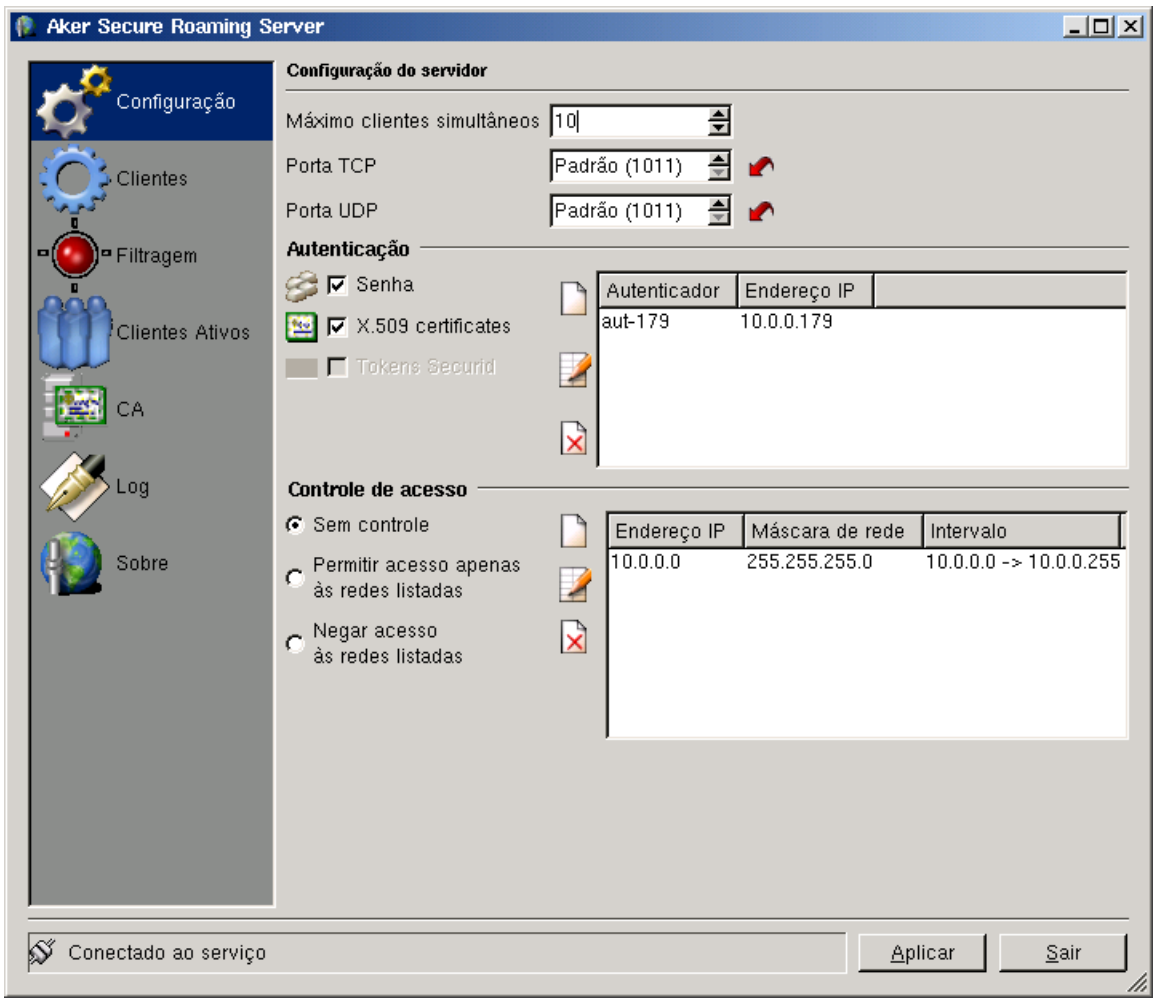
Se você não souber o nome do pacote, digite o seguinte comando para descobrir:

```
pkg_info | grep Aker
```

2-0 Configurando e administrando Aker Secure Roaming Server

Aqui você encontra as instruções necessarias para configurar e administrar corretamente seu Secure Roaming Server.

2-1 Página de configuração do servidor

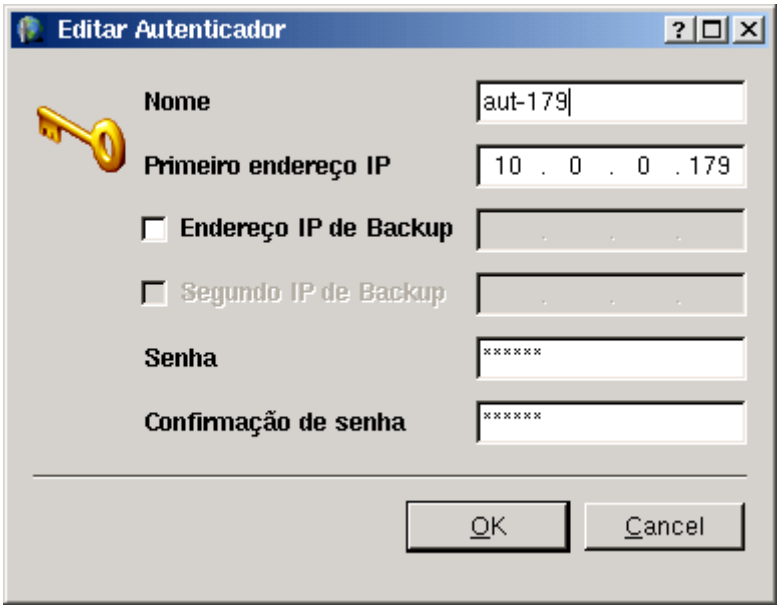


Nesta página você encontra importantes opções de configuração do servidor:

- **Máximo clientes simultâneos**: Aqui você pode configurar o número máximo de clientes pemitidos simultaneamente em um determinado tempo. Use esta opção para evitar com que o servidor tenha uma sobrecarga por excesso de clientes, o que pode diminuir a perfomance.
  Por favor, note que este número não pode ser superior ao de sua licença.
- **Porta TCP/UDP**: Este controle permite configurar a porta usada pelo servidor para escutar conexões e dados de clientes, respectivamente. Por exemplo, você pode configurar o servidor para usar as portas TCP/443 e UDP/53, em ordem

para burlar firewalls e/ou outros dispositivos de filtragem entre servidores e clientes, que recusariam uma conexão VPN, mas não uma conexão HTTP segura e uma requisição DNS, respectivamente.
A porta padrão é **1011** tanto para TCP e UDP .
Alterações na porta TCP são de efeito imediato. Na porta UDP, necessitam que o serviço seja reiniciado.

- **Autenticação**: Aqui você vai selecionar qual o método de autenticação (a versão corrente suporta autenticadores usuário/password e certificados X.509) permitido aos seus clientes.
  Na lista da direita, você pode adicionar, editar ou remover autenticadores usados. Um autenticador é um computador que roda o agente de autenticação Aker para exportar seu diretorio de uma forma completamente encriptada. Pelo menos um autenticador será necessário para que os clientes efetuem logon utilizando nomes de usuário e senhas. Quando adicionar ou editar um novo autenticador, a seguinte janela vai aparecer:

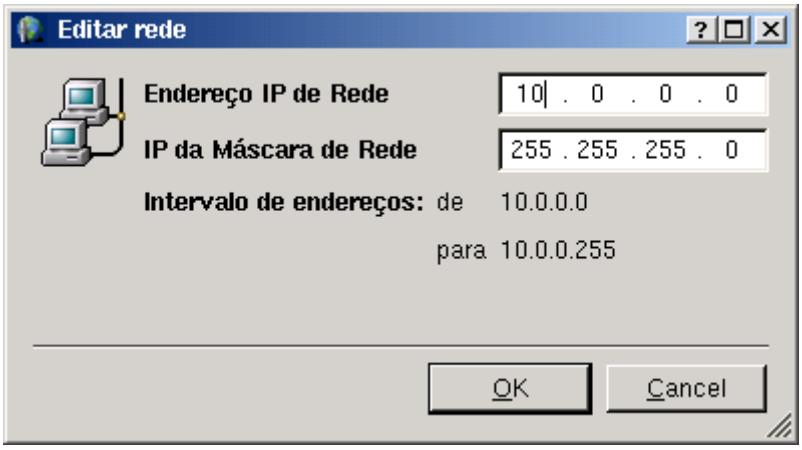


  Neste diálogo, você pode configurar o nome, o endereço IP primário, o backup, e o password do seu autenticador. Lembre-se de que o password deve ser o mesmo que você colocou no Agente de Autenticação Aker.
  Para maiores informações a respeito do Agente de Autenticação, refira-se ao Firewall Aker Manual do Usuário, que pode ser encontrado no website da Aker .
  Para que você possa habilitar a autenticação via certificados X.509, você deve instalar pelo menos um certificado de CA (Autoridade Certificadora) confiável no servidor (como fazer isso será descrito mais a frente). Para os clientes lograrem acessos ao sistema, eles deverão então aprensentar um certificado assinado por uma CA cujo certificado esteja instalado e provarem posse da chave privada correspondente. Isso tudo é feito automaticamente pelo Secure Roaming Client.

- **Controle de Acesso**: Aqui você configura de quais clientes quer aceitar conexões:
  1. **Sem controle**: Todo cliente tem permissão para conectar ao servidor.

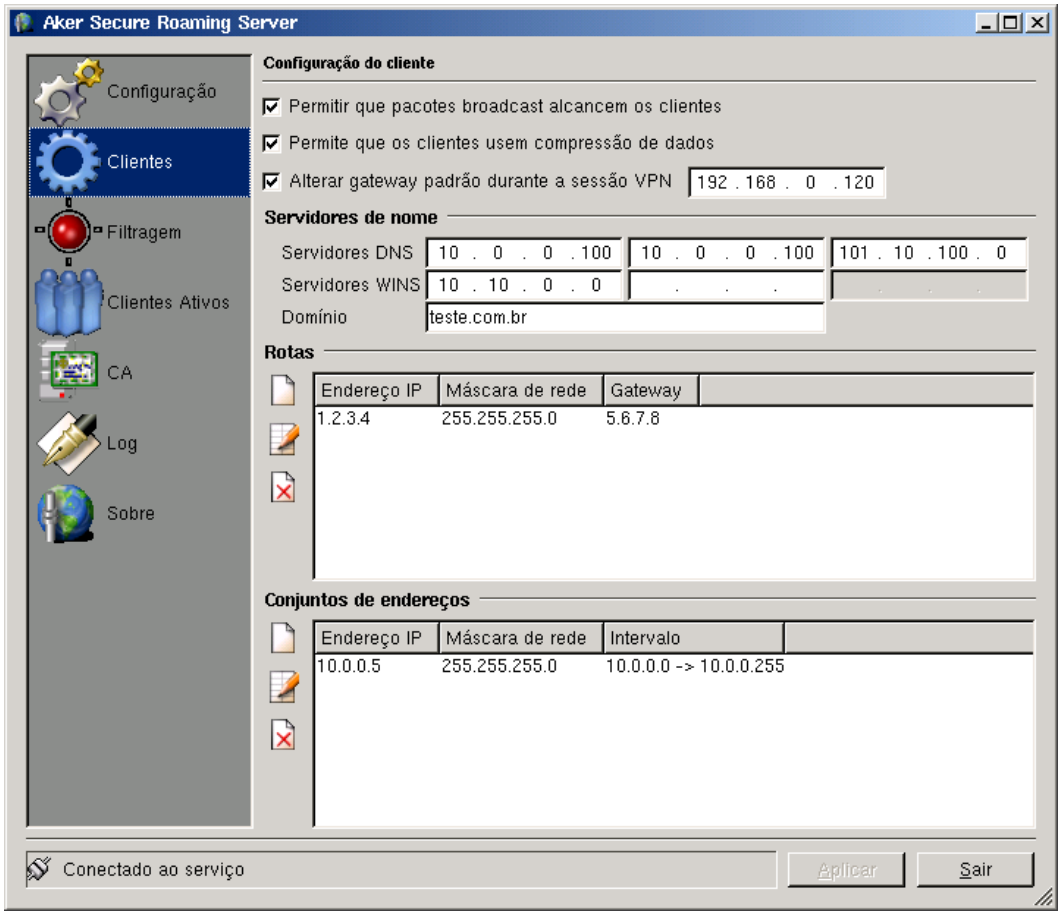
2. **Permitir o acesso apenas às redes listadas**: Somente clientes que tem endereço IP pertencentes a redes na lista da direita vão estabelecer conexão VPN.
3. **Negar acesso às redes listadas**: Os clientes que têm endereço IP pertecente a alguma rede na lista da direita não serão capazes de estabelecer conexão VPN. Os outros serão.

Quando editar ou criar uma nova entrada na lista de redes da direita, você será levado para o diálogo seguinte:



Nesta janela você vai poder entrar o endereço IP da rede e a máscara de rede (netmask). Por favor, note que endereços ou máscaras invalidas não serão aceitas, i.e. você não conseguirá digita-los.
Após digitar endereços e máscaras validas, a faixa de endereçamento IP será calculada automaticamente. Esta faixa **inclui** o primeiro endereço (endereço de rede) e o último (endereço de broadcast), já que não é especificado uma sub-rede no roteador, mas uma faixa de endereços IP.

2-2 Página de configuração do Cliente

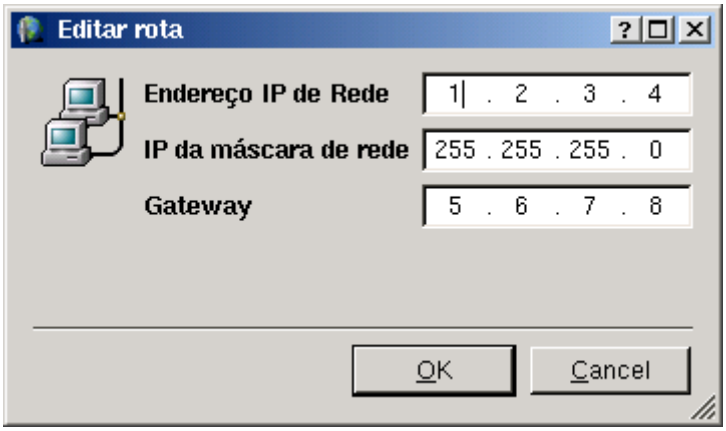


Nesta página você irá encontrar as configurações relevantes aos clientes que conectam ao servidor:

- **Permitir que pacotes broadcast alcancem os clientes**: Esta opção desabilita o bloqueio do servidor à transmissão de pacotes de broadcast. Pacotes de broadcast são necessários em alguns protocolos como SMB/Netbios (Redes Microsoft Windows). Uma rede mal configurada pode vir a receber muitos pacotes deste tipo, que se puderem alcançar o cliente, podem simplesmente sobrecarregar um link dial-up típico usado por muitos usuários.
- **Permite que os clientes usem compressão de dados**: Esta opção permite que todo o tráfego entre o cliente e o servidor use compressão de dados, fazendo com que seja gasto menos banda da conexão.
- **Alterar gateway padrão durante a sessão VPN**: Esta opção faz o servidor alterar o gateway padrão dos clientes durante uma sessão VPN. Habilitar essa opção faz o computador dos clientes ter exatamente o mesmo comportamento que ele teria se conectado ao interior da rede, mas também redirecionará todo o tráfego destinado à Internet para o *link* de sua rede interna.
Se você tem poucas rotas conhecidas, é melhor inseri-las na lista abaixo, o que fará com que o tráfego destinado à Internet não seja enviado por dentro da VPN.
- **Servidores de Nome**: Para o computador do usuário final se comportar exatamente do mesmo modo como quando conectado a sua rede caseira, ele necessita resolver nomes usando os serviços DNS e WINS. Por favor, preencha-os da esquerda para

direita, observando que o próximo espaço ficará disponível quando o anterior estiver com um endereço IP válido (você não terá permissão de digitar nada diferente de um endereço IP).
Do mesmo modo que o gateway padrão, os servidores DNS e WINS do cliente serão restaurados quando a conexão VPN terminar.

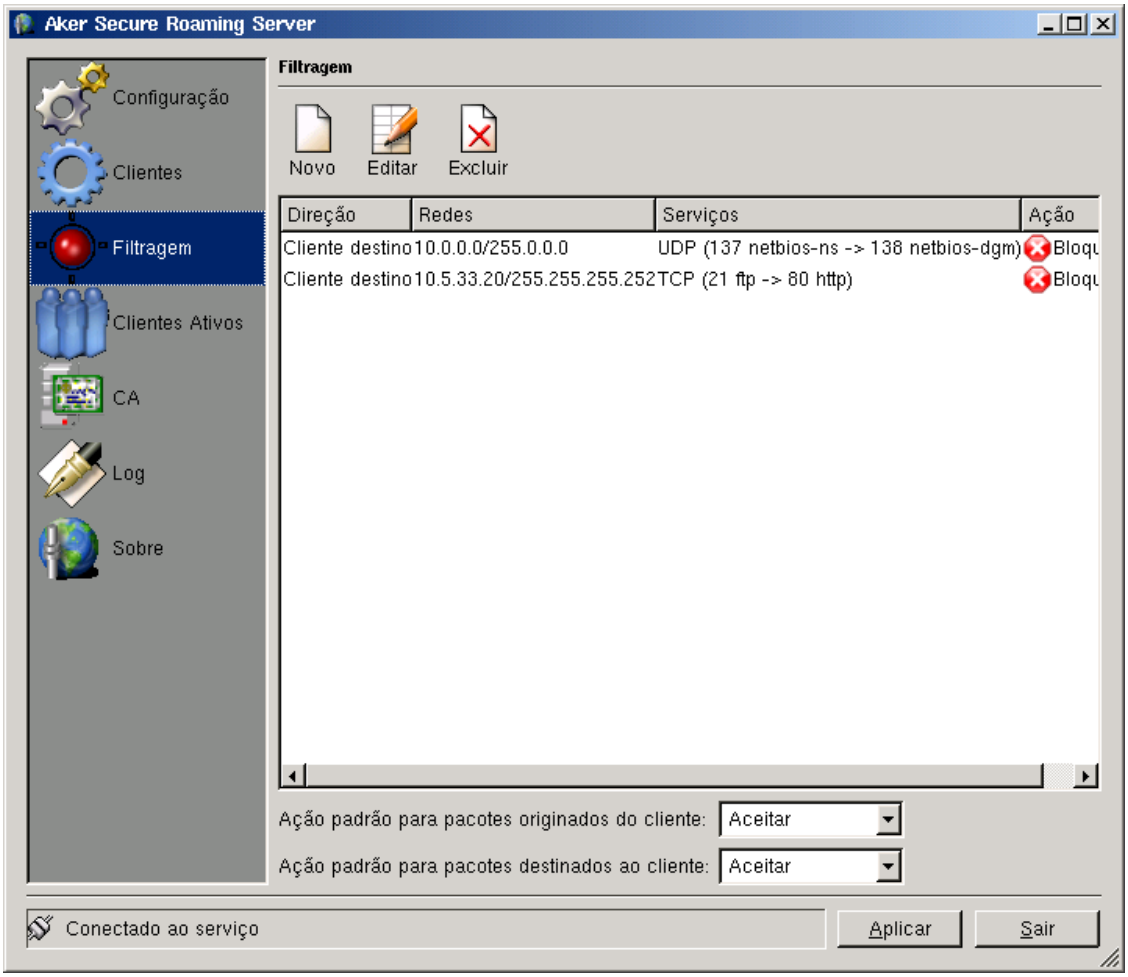
- **Rotas:** Para que o computador do usuário tenha acesso a outras partes da intranet, por exemplo, ele necessitará de rotas para as mesmas. Quando editar ou criar uma nova entrada na lista de redes da direita, o diálogo seguinte será exibido:



Nesta janela você vai poder entrar o endereço IP da rede, a máscara de rede (netmask) e o gateway para este rede. Por favor, note que endereços, máscaras ou gateways inválidos não serão aceitos, i.e. você não conseguirá digita-los.

- **Conjunto de Endereços**: O endereço IP atribuído ao cliente será extraído do conjunto de endereços abaixo de forma seqüencial. Note que esses conjuntos não especificam redes, eles especificam uma faixa de endereços IP. O diálogo usado para edita-los é o mesmo usado na lista de controle de acesso.

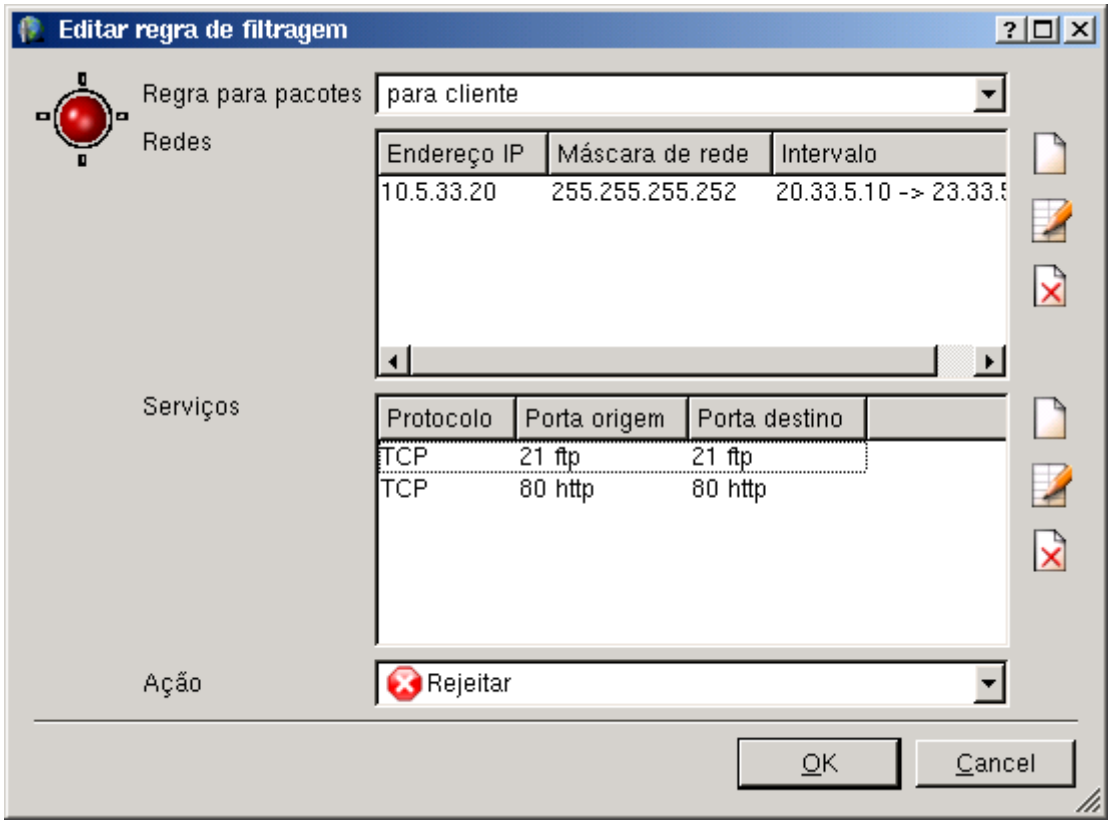
2-3 Página de Configuração dos filtros



Nesta página, você irá criar filtros para controlar o tráfego entre o cliente e a rede caseira. Isto pode ser usado tanto para aumentar o nivel de segurança quanto para restringir o tráfego de dados desnecessários de modo que informações críticas obtenham maior performance na escassa largura de banda do usuário final.

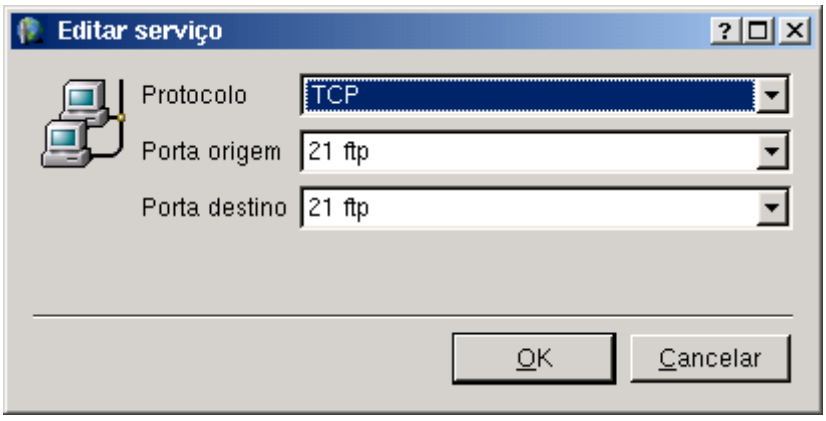
- **Lista de Regras**: Nesta lista você pode ver as regras atualmente impostas. Há dois tipos de regras:
    1. **Regras para tráfego originado dos clientes**, que são marcadas como *do cliente*
    2. **Regras para trafico destinado aos clientes**, são marcadas como *para cliente*

    As regras podem também **bloquear** ou **permitir** o tráfego.
    As regras são percorridas seqüencialmente. Isto significa que uma regra mais gênerica anterior pode eclipsar uma mais específica.
    Ao editar novas ou velhar regras, o diálogo seguinte irá aparecer:



Neste diálogo, os seguintes controles estão disponíveis:

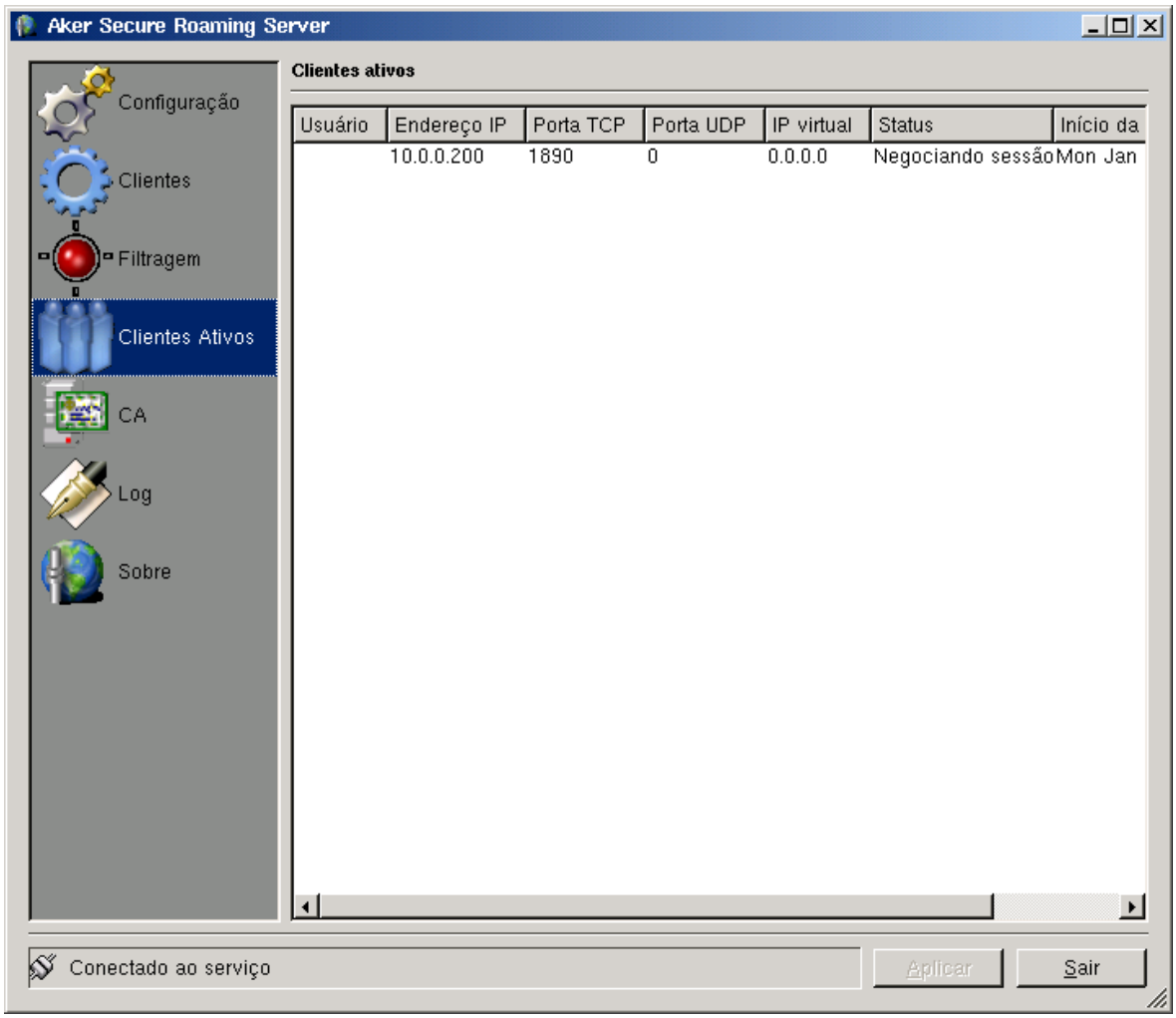
- **Regra para Pacotes**: Aqui você pode escolher o tipo de regra: pacotes vindos do cliente (**do cliente**) ou pacotes destinados ao cliente (**para cliente**).
- **Redes**: Esta lista contém as redes onde o outro endereço IP (IP de destino para regras originada de clientes ou IP origem para regras destinadas a clientes) deve coincidir. Elas podem ser editadas usando o mesmo diálogo usado na edição das listas de controle de acesso.
- **Serviços**: Esta lista contém os serviços (*porta de destino* em pacotes TCP ou UDP, *tipo de serviço* em pacotes ICMP ou *protocolo* em pacotes IP *raw*) que devem estar presentes no pacote para satisfazer a regra. Você pode editar estas usando o seguinte diálogo:



        - **Protocolo**: Esse é o tipo de serviço que vôce deseja, i.e. qual a definição do serviço que você deseja usar dos listados acima.
        - **Porta origem / Porta destino**: Os serviços em que a regra deve ser aplicada são aqueles com números (porta, tipo de serviço ou protocolo) entre esses dois valores, inclusive.
    - **Ação**: Define se a regra será aceitar ou bloquear o pacote.

      As regras são checadas no lado do cliente e no lado do servidor. Isto assegura a máxima performance (nenhum pacote entra no VPN para ser descartado na outra ponta) e a segurança máxima (um cliente adulterado não terá permissão de injetar tráfego não permitido na rede interna).
- **Ações Padrão**: Podem ser entendidas como as últimas regras. Elas se aplicam a todo pacote que não se encaixar nas demais regras.

2-4 Página dos clientes ativos



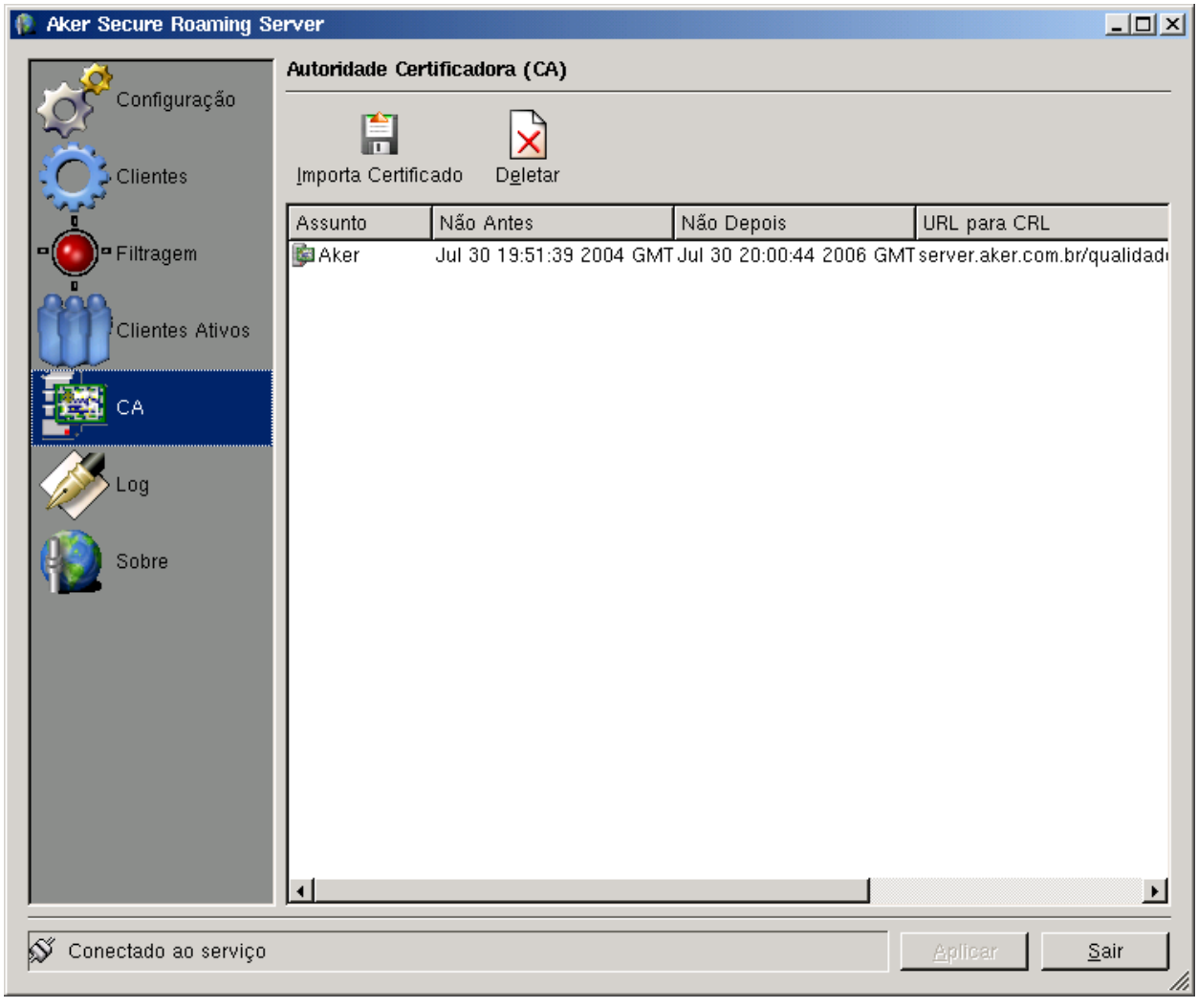
Aqui você pode ver os clientes que estão conectados no momento e suas propriedades:

- **Usuário**: Este campo inclui o nome e domínio do usuário que fez login. Pode conter também outras informações pertinentes a outros métodos de autenticação.
- **Endereço IP**: Este campo mostra o endereço de onde o cliente está conectado, como visto pelo servidor. Fique atento ao fato de que o cliente pode estar atrás

de um dispositivo de *IP masquerading*, que pode efetivamente esconder o endereço real usado por ele.

- **Porta TCP / UDP**: Este campo mostra as portas através de onde o cliente está conectado. A observação acima se aplica aqui também, i.e., os números podem ser alterados pelo dispositivo *IP masquerading*.
- **IP Virtual**: Este campo mostra o endereço IP atribuído ao cliente do conjunto previamente definido.
- **Status**: Neste campo você encontra um texto descrevendo o status da VPN. Um dos mais importantes são *Autenticando*, que significa que o cliente forneceu dados de autenticação e o servidor está aguardando por uma resposta positiva do autenticador, e *Estabelecida*, que significa que o cliente se encontra ativo e operante.
- **Inicio de Sessão**: Este campo mostra a data e hora em que o cliente conectou.

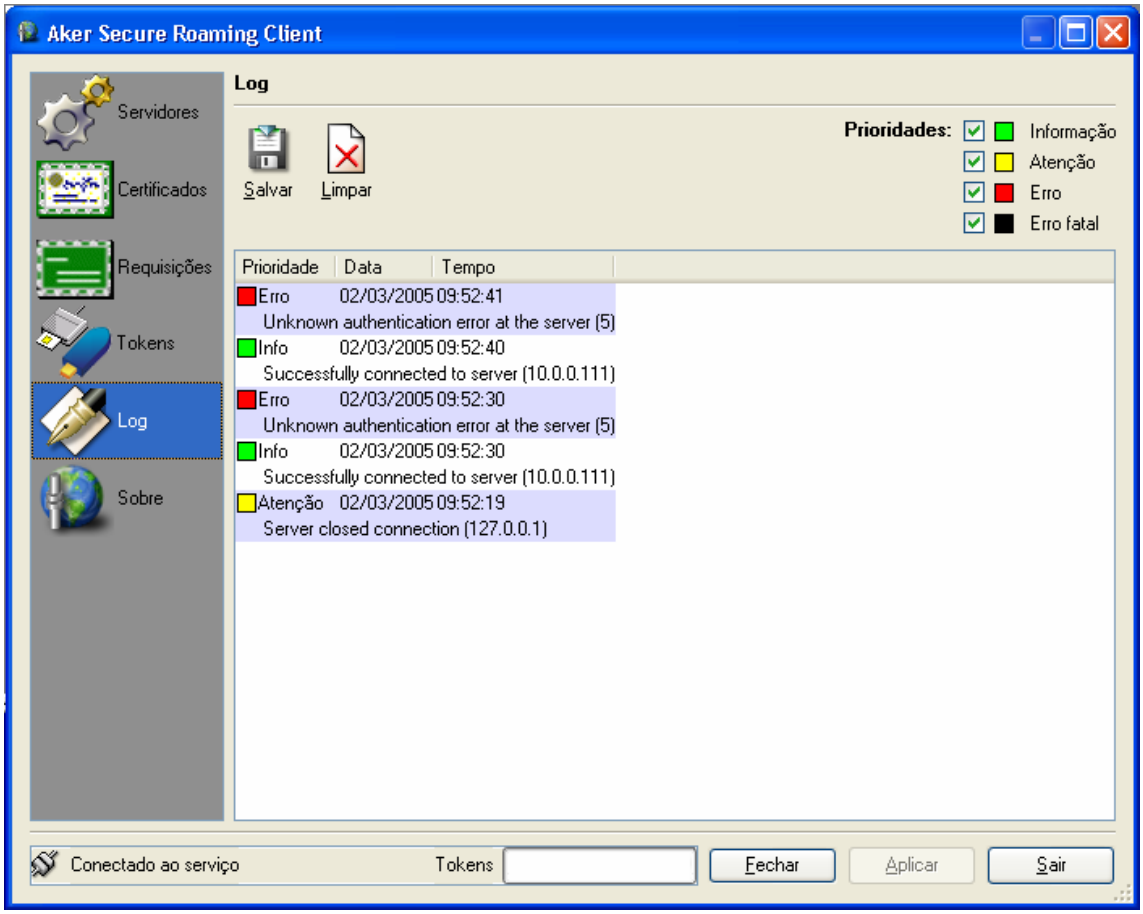
2-5 Página de Autoridade Certificadora



Aqui você pode incluir e excluir os certificados das CAs em que você confia. Essa relação de confiança será plena, os certificados que forem assinados por elas serão aceitos como credenciais válidas para estabelecimento de VPN.
Para Incluir uma CA clique no botão Importa Certificado e escolha o arquivo do certificado da CA. Para excluir uma CA clique na mesma e depois clique no botão

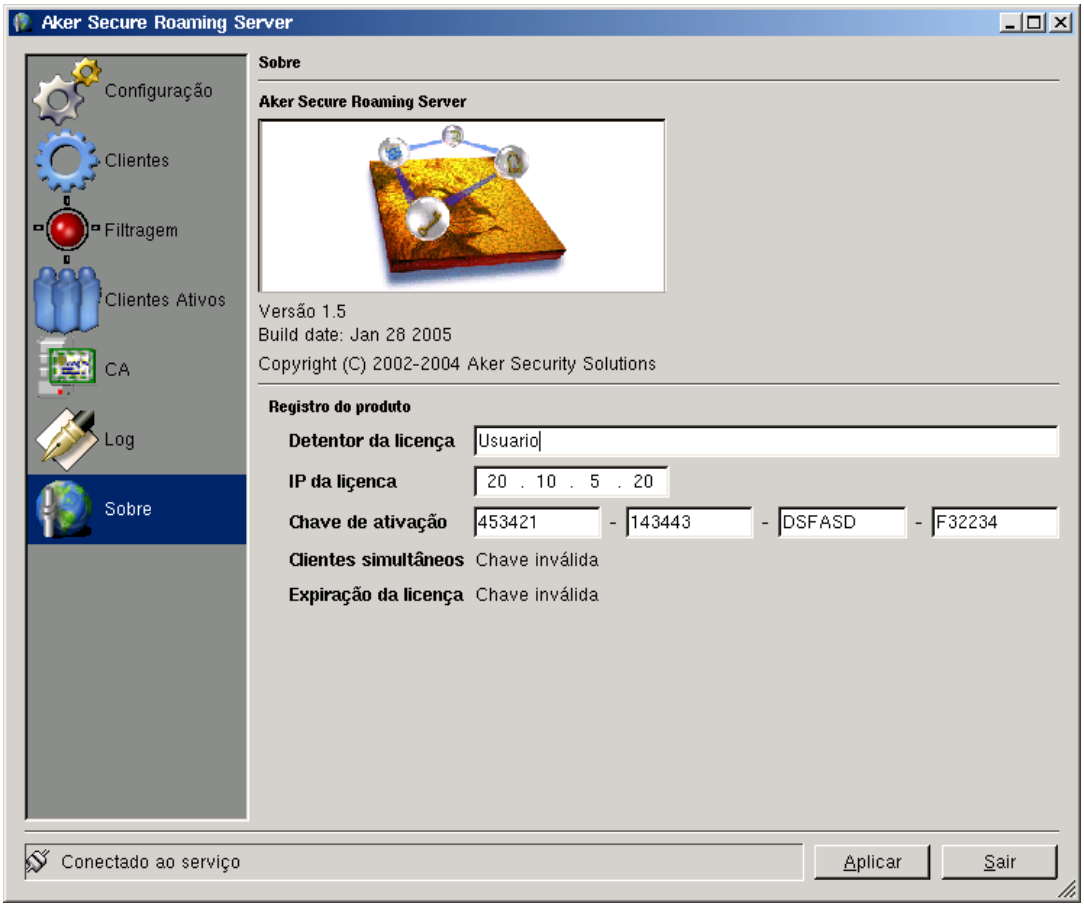
deletar.
Nessa tela também temos a opção de informar a localização de publicação da CRL (lista de certificados revogados) de cada CA. A CRL é a lista de certificados revogados pela CA. Quando acontece algum problema com o certificado, como comprometimento da chave privada, o dono procura a CA e pede a revogação do certificado. A CA então revoga o certificado e publica uma lista com os certificados revogados. Esses certificados passam então a não ser mais aceitos para fins de autenticação.
Para entrar com a URL da CRL da CA, clique com o botão direito do mouse na CA correspondente ou dê um duplo clique na CA.
As listas de certificados revogados são baixadas todos os dias se o serviço estiver ativo, de 24 em 24 horas e durante a inicialização do serviço do Secure Roaming Server.

2-6 página de Log



Aqui você pode examinar o log do sistema e configurar se ele será enviado ao syslog (Unix) ou Visualizador de Eventos(Windows).
A *combo box* do syslog (só em sistemas Unix) define qual *facility* do syslog o Aker Secure Roaming Server deve usar.

2-7 Página Sobre



Nesta última página, vôce precisa colocar a informação de registro de acordo com a licença que você recebeu da Aker Security Solution. Por favor verifique os limites (número máximo de clientes simultâneos e a data de expiração).

Se você digitar algo de forma incorreta, sua licença será considerada inválida; você precisa digitar o nome do licenciado, o endereço IP e a chave de ativação,**exatamente** como escrito em seu termo de licença.

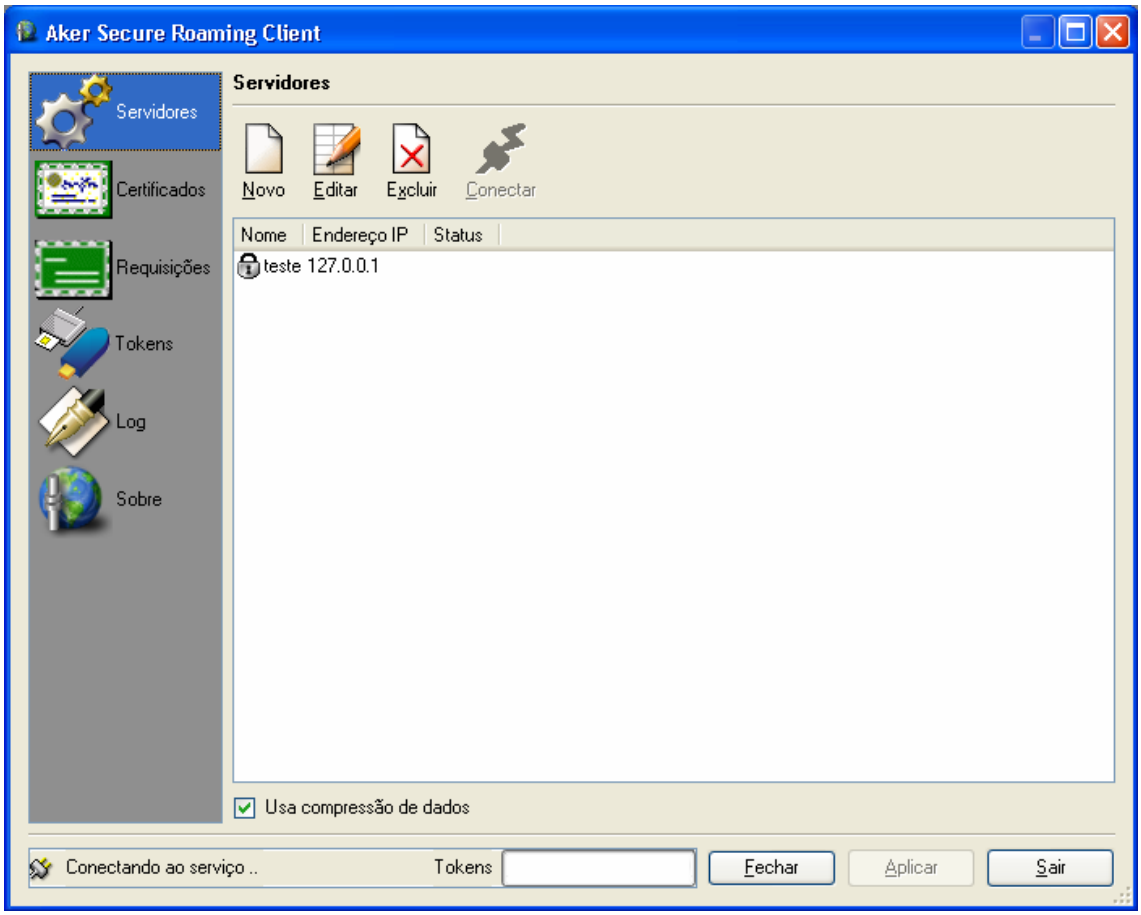
---

3. Configurando e administrando o Aker Secure Roaming Client

Aqui você encontra as instruções necessárias para configurar e administrar corretamente o Aker Secure Roaming Client. Ele foi projetado para ser muito mais simples do que o Servidor, facilitando o seu uso pelo usuário final.

3.1. Servidores

Nesta seção você poderá configurar em quais servidores você se conectará. Você também poderá editar as opções de acesso e autenticação. A página de Servidores possui o seguinte formato:



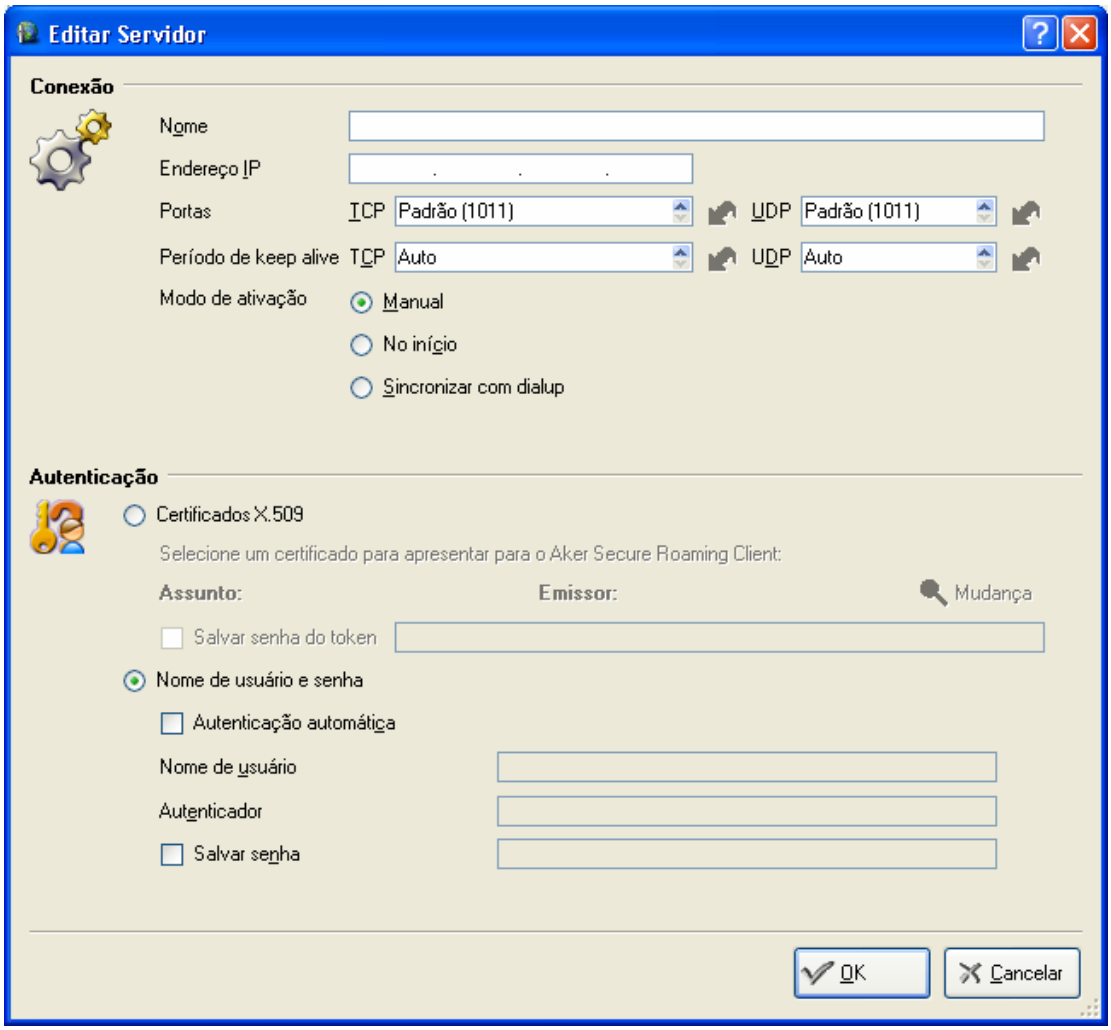
Os opções disponíveis são: **Novo**, **Editar**, **Excluir** e **Conectar/Desconectar:**

- O botão **Novo** cria uma nova configuração para conexão. Uma nova janela irá abrir com as configuração possíveis.

- O botão **Editar** modifica uma nova conexão existente. A mesma janela de **Novo** irá abrir permintindo modificar as configurações.
- O botão **Excluir** remove uma conexão criada.
- O botão **Conectar/Desconectar** conecta ou desconecta de um servidor *Aker Secure Roaming Server*. Quando você estiver conectando o botão momentaneamente irá apresentar o título **Abortar**, indicando que ao pressionar o botão você poderá abortar o processo de conexão.

Clicando em **Novo**/**Editar** a seguinte tela irá aparecer, permitindo que você crie ou um novo ou edite uma configuração existente:

Lembre-se que para efetivar qualquer configuração criada/editada você deve clicar no botão **Aplicar** na janela principal.



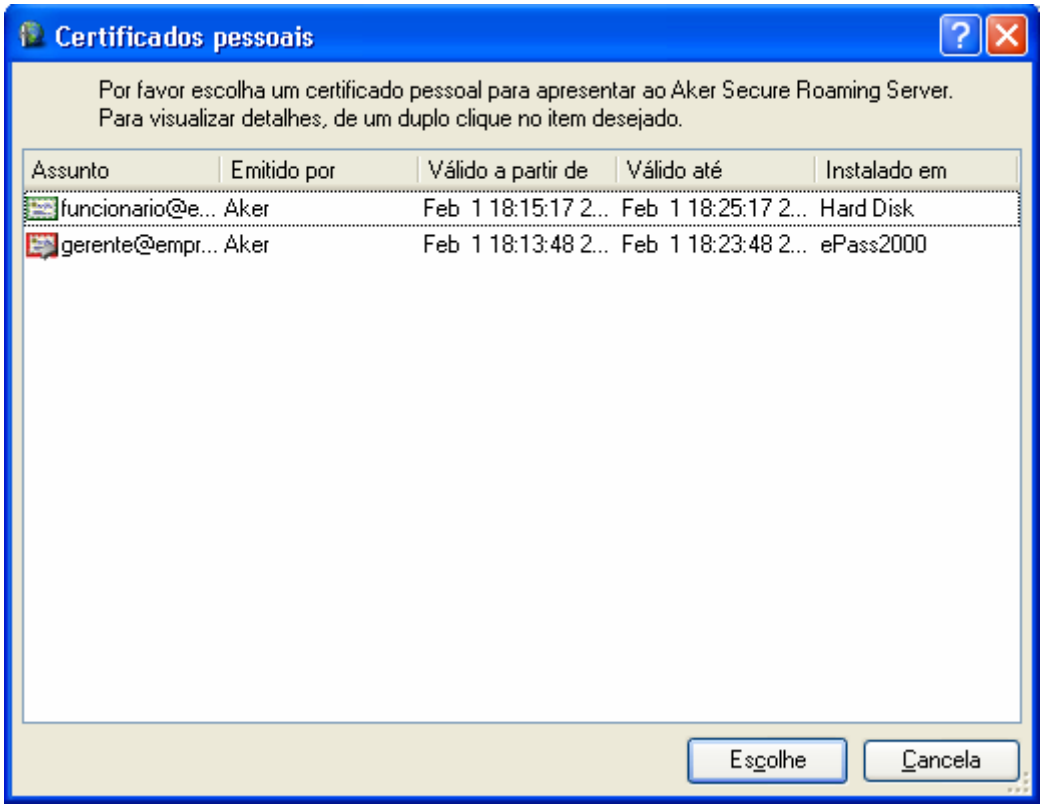
Na parte de **Conexões** você poderá editar as configurações necessárias para você poder conectar no Secure Roaming Server. Os seguintes campos estão disponíveis:

- **Nome**: Este nome é para sua referência somente. Pode ser qualquer texto que lhe ajude a identificar o Secure Roaming Server em que você se vai conectar.

- **Endereço IP**: O endereço IP do servidor, visto pelo cliente. Esse número pode ser diferente do endereço real do servidor, se ele se encontrar atrás de um gateway que faça NAT (tradução de endereços). Observe que você não conseguirá digitar qualquer coisa a não ser o endereço IP neste campo.
- **Portas**: Portas TCP e UDP em que o servidor espera os dados para conexão. Esses números precisam ser os mesmos que aqueles entrados quando da configuração do servidor ou, como no caso endereço IP, os números de porta traduzidos se o servidor estiver com suas portas traduzidas por um gateway de NAT.
- **Período keep-alive**: Este período é o máximo tempo de inatividade das conexões TCP e sequências de pacotes UDP. Mude-os se os valores padrão fizerem com que a conexão entre o servidor e cliente seja perdida ou com que os números de porta UDP sejam trocados (comporamente típico em dispositivos que fazem NAT N-1). Tenha em mente que usar números pequenos *por segurança* não é uma boa idéia, porque você pode acabar usando muito da estreita largura de banda com pacotes keep-alive entre o cliente e o servidor.
- **Modo de ativação**: Este ajuste define quando a conexão VPN deve começar e terminar. As escolhas possíveis são:
    1. **Manual**: A conexão vai ser estabelecida e derrubada em resposta a comandos do usuário. Se algum problema fizer com que a conexão seja perdida, o usuário terá que restabelecê-la manualmente.
    2. **No início**: O cliente tentará manter a coneção sempre ativa. Este método é mais que útil para clientes conectados permanentemente a rede, como nas linhas DSL ou em redes locais.
    3. **Sincronizar com dialup**: (*Somente para Windows*) O estado da conexão vai ser sincronizado com o adaptador dial-up: a VPN será estabelecida quando o usuário conectar-se a um servidor dial-up e derrubada quando ele desconectar. Este método é o mais recomendado para usuários que não têm acesso permanente à Internet.

Na parte de **Autenticação** você poderá escolher o método para autenticação com o Secure Roaming Server. As opções possíveis são:

- **Certificados X.509:** neste modo você terá que possuir um certificado X.509 previamente instalado pelo Secure Roaming Client. Para selecionar um certificado da lista de disponíveis, pressione o botão **Mudança**. Ao pressionar o botão, a lista de certificados instalados aparecerá como na figura a seguir:



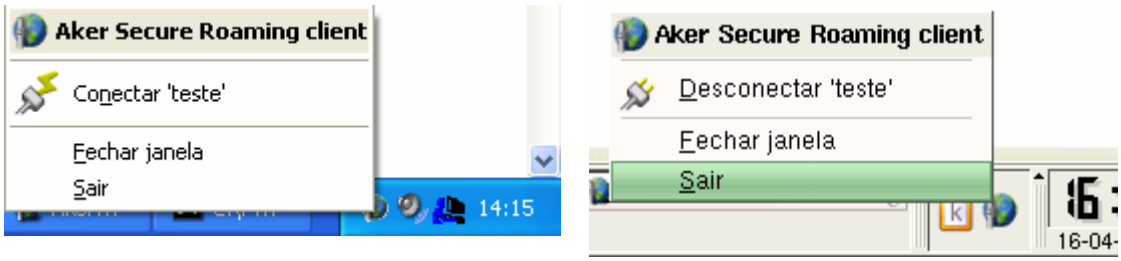
As tela mostrará os certificados disponíveis e as informações relevantes sobre eles. Para escolher qual usar selecione-o e pressione o botão **Escolhe** ou dê um duplo clique sobre o ítem.

- **Salvar senha do token**: essa opção apenas será ativada quando o certificado escolhido estiver instalado em um token criptográfico. Marque a opção para que não seja necessário entrar com a informação quando a sessão VPN é estabelecida. Fique atento ao fato que sua senha será salva criptografada dentro do arquivo de configuração.

- **Nome de usuário e senha**: esse é o modo mais tradicional de autenticação: o usuário apresenta como credenciais um par nome de usuário/senha. Se você quer que o sistema lhe autentique automaticamente, por favor marque *Autenticação Automática* e preencha os campos necessários:
  - **Nome de usuário**: seu nome de usuário na rede em que está conectando.
  - **Domínio**: o nome do autenticador usado no servidor. Se você deixar este campo vazio, o servidor tenta usar todos autenticadores que ele tem conhecimento.

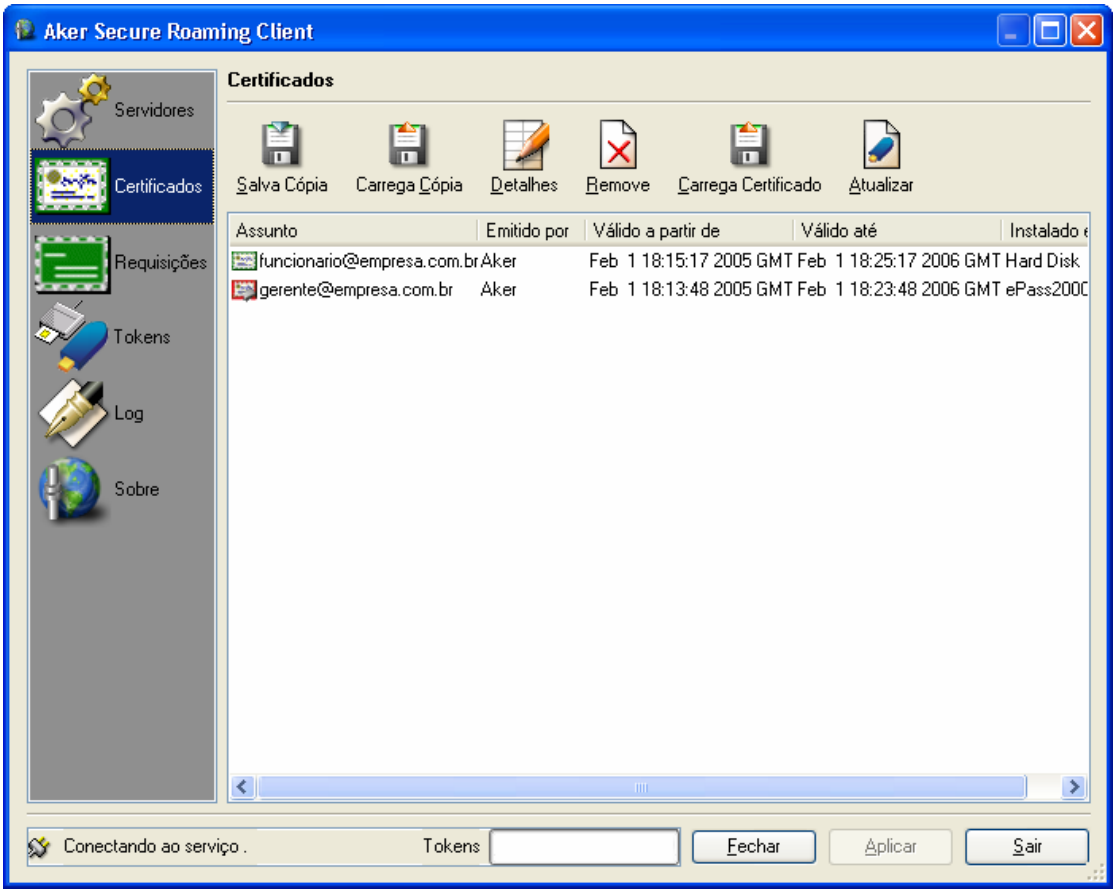
    Este campo não é o nome do domínio NT onde está seu agente de autenticação, mas sim o nome dado ao autenticador no Secure Roaming Server
  - **Salvar senha**: sua senha pode ser salva de modo que você não precise entrar informações quando a sessão VPN é estabelecida. Se voce marcar este método fique atento ao fato de que sua senha será salva criptografada no arquivo de configuração. Essa opção permite executar o cliente sem a interface gráfica do usuário (apenas o daemon/serviço em background), o que pode ser útil para usuários Unix sem uma sessão X.

Algumas funcionalidades desta página podem ser acessadas clicando com a direita no ícone na barra de ferramentas do sistema:



3.2. Certificados

Nessa seção você poderá gerênciar todos os certificados que serão usados para autenticação. A página possui o seguinte formato:



As opções disponíveis são: **Salva Backup**, **Carrega Backup, Detalhes, Remove, Carrega Certificado, Atualiza:**

- Os botões de **Salva/Carrega Cópia** salvam ou carregam um certificado e seu par de chaves no formato PKCS#12. Nesse formato você empacota seu certificado juntamente com sua chave privada protegende seu acesso com uma senha (que deve ser informada).
- O botão de **Detalhes** mostra informações adicionais sobre os certificados, tanto sobre o Emissor quando sobre o Assunto.

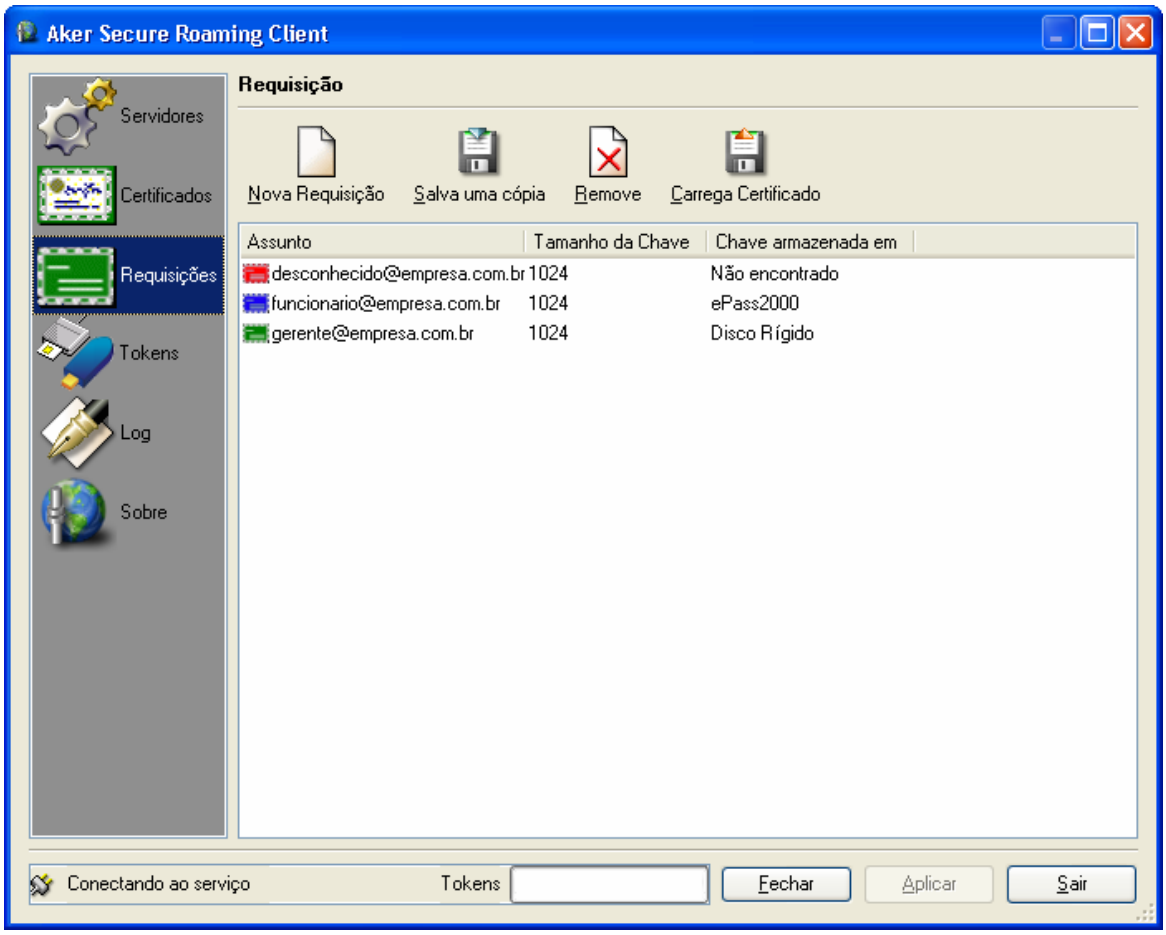
- O botão de **Remover** remove tanto o certificado como sua chave privada associada. Caso o certificado a ser deletado esteja em um token criptográfico será necessário informar a senha do token para poder remover o certificado do token.
- O botão de **Carrega Certificado** carrega um arquivo de certificado, podendo este estar codificado tanto em DER como Base 64. Esse arquivo é gerado pela CA a partir da requisição criada anteriormente.
- O botão de **Atualizar** apenas é útil quando você estiver utilizando algum token criptográfico. Ele serve para procurar por novos certificados caso algum token seja inserido durente a execução do Secure Roaming Client. Durante a atualização dos certificados, uma barra animada se moverá na parte inferior da tela (mostrada ao lado do **Tokens**) parando quando todas os certificados forem atualizados.

De acordo onde a chave privada do certificado estiver instalada um tipo de ícone será usado:

-  Chave privada em disco rígido. A chave está instalada na pasta *x509/key*, dentro da pasta de instalação.
-  Chave privada em token criptográfico. O token criptográfico será mostrada no campo *Instalado em*.

3.3. Requisições

Nessa seção você poderá gerênciar suas requisições de certificados. A página de Requisições possui o seguinte formato:

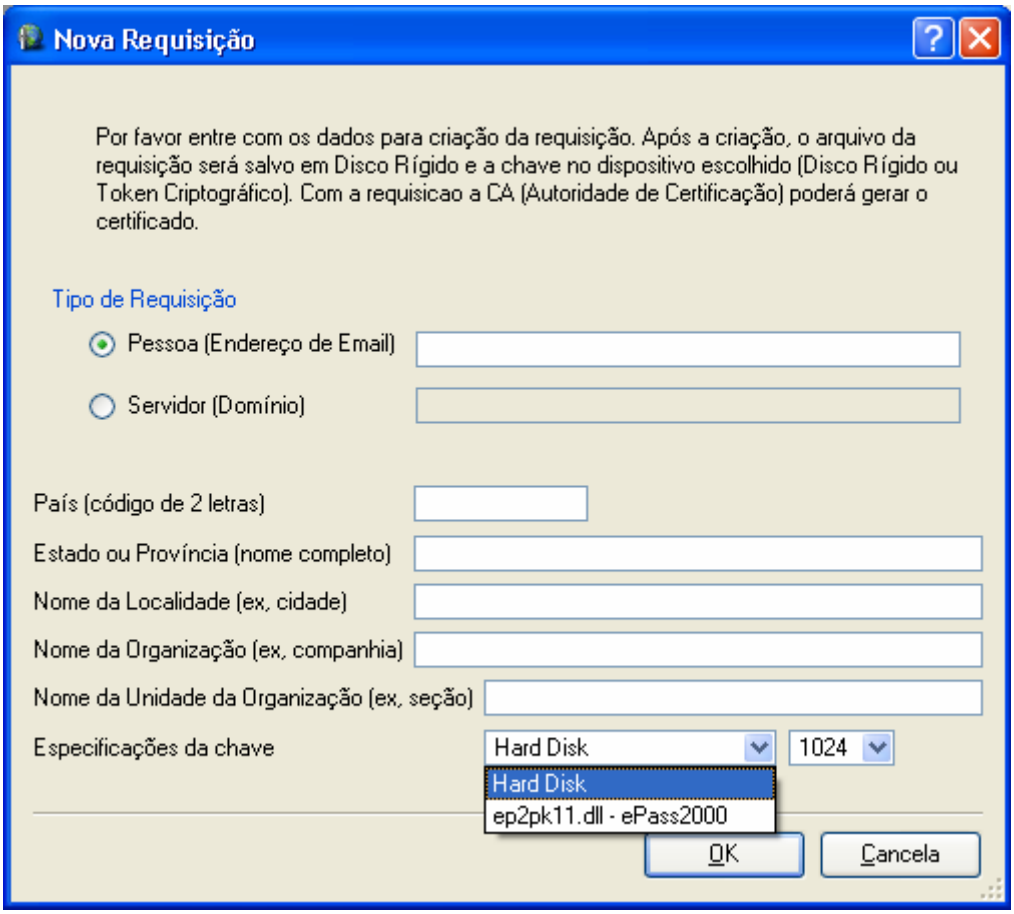


As opções disponíveis são: **Nova Requisição**, **Salva uma cópia, Remove, Carrega Certificado.**

- O botão **Nova Requisição** abre uma janela para a criação de novas requisições e chaves privadas.
- O botão **Salva uma cópia** em disco da requisição ja criada. O arquivo é salvo com a extensão '.csr' e pode ser usado pela CA para emitir um certificado.
- O botão **Remove** remove uma requisição e sua chave privada associada. Caso a Requisição seja criada em um token criptográfico será necessário que você insira a senha do token em questão (apontado pelo campo **Chave armazenada em**) para deletar a chave privada.
- O botão **Carrega Certificado** carrega um certificado criado por uma CA a partir de uma requisição.

  Quando um certificado é caregado sua requisição é removida do disco. Caso você deseje usar a mesma requisição para criar certificados a partir de CA diferentes faça cópias de segurança com o botão **Salva uma cópia**.

Para criar uma requisição clique no botão **Nova Requisição**. Uma janela será mostrada com a seguinte configuração:



Na janela você poderá entrar com as informações necessárias para a criação da Requisição. As informações necessárias para a criação de uma requisição são:

- **Tipo de Requisição:** determina básicamente qual campo do certificado X.509 será usado para identificá-lo. Duas opções são possíveis **Pessoa** e **Servidor**.
- **País:** código de 2 letras (BR para Brasil por exemplo).
- **Estado ou Província:** identificação do estado (Brasília, São Paulo, etc.).
- **Nome da Localidade:** nome da cidade, bairro, etc.
- **Nome da Requisição:** nome completou ou outro identificador da Organização.
- **Nome da Unidade da Organização:** nome da seção, departamento, etc.
- **Especificações da Chave:** nessa opção você poderá especificar onde será gerada a chave (Hard Disk ou um token criptográfico) e partir do meio de geração a aba seguinte mostrará os tamanhos (em bits) possíveis. Os tokens são indicados pela sua biblioteca seguida de seu nome.

  De acordo com o meio de geração do par de chaves assimétricas, a criação do certificado pode demorar alguns segundos. Assim durante a geração da chave e janela de criação de requisições será desabilitada.

De acordo com o tipo de geração de chave um ícone diferente será usado:

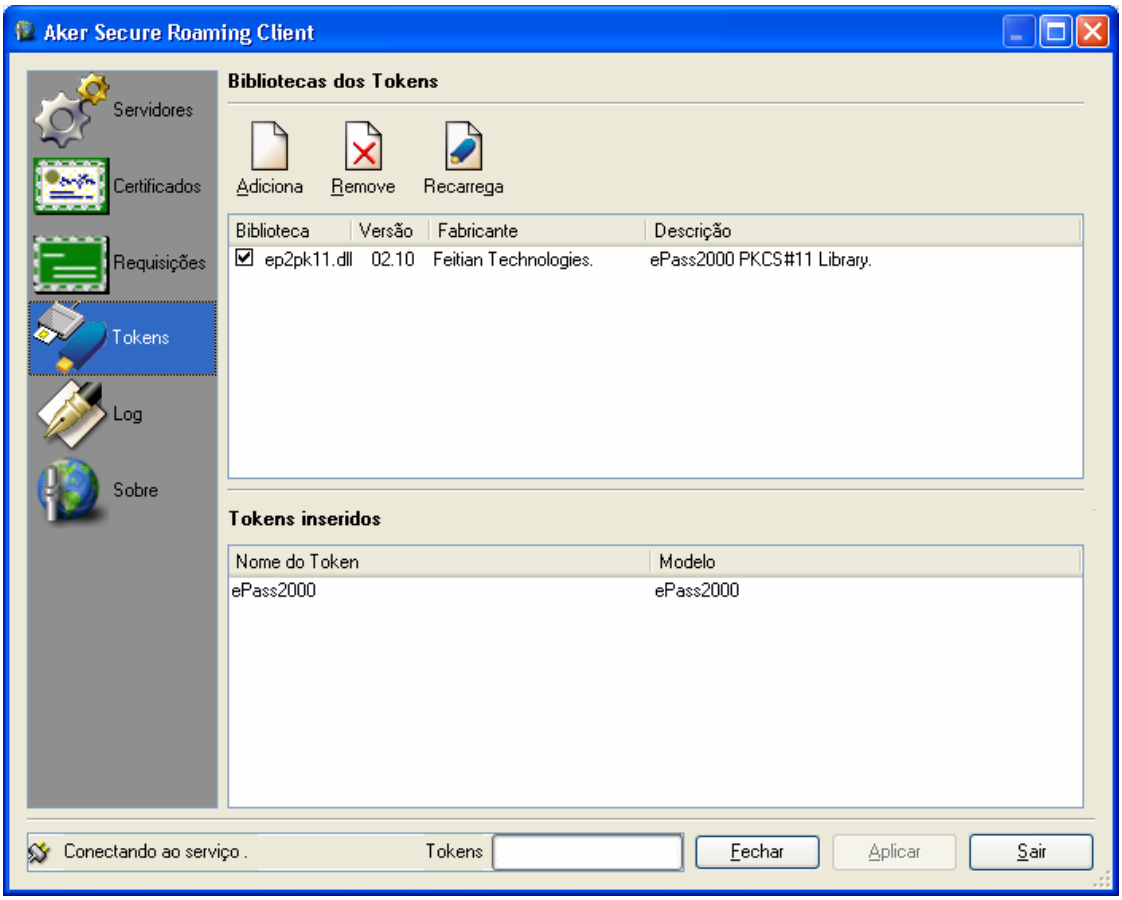
- Geradas em disco rídigo. A chave está instalada na pasta *x509/key*, dentro da pasta de instalação.
- Geradas em tokens criptográficos. O token onde a chave foi gerada será especificado pelo campo *Chave armazenada em* na janela principal.

- Chave privada não encontrada. A chave pode ter sido apagada ou não estar em um token criptográfico não conectado ao sistema.

Uma requisição com uma chave não encontrada não é necessariamente inválida. A chave pode estar em um token criptográfico e quando este for conectado e reconhecido pelo *Aker Secure Roaming Cliente* a chave será reconhecida como pertencente à requisição.

3.4. Tokens

Nessa seção você poderá gerênciar as bibliotecas dinâmicas PKCS#11 para acesso ao tokens conectados em seu computador. A janela de Token possui o seguinte formato:



A janela superior mostra as bibliotecas dinâmicas PKCS#11 instaladas enquanto a janela inferior mostra os tokens conectados.
As opções disponíveis são: **Adiciona**, **Remove** e **Recarrega:**

- O botão **Adiciona** instala uma nova biblioteca dinâmica e a disponibiliza para poder ser carregada.
- O botão **Remove** remove uma biblioteca da lista das bibliotecas instaladas.
- O botão **Recarrega** carrega uma biblioteca instalada e obtém todos os tokens conectados no sistema. Note após inserir ou remover qualquer token do sistema é necessário clicar no botão para limpar ou atualizar a lista de certificados.

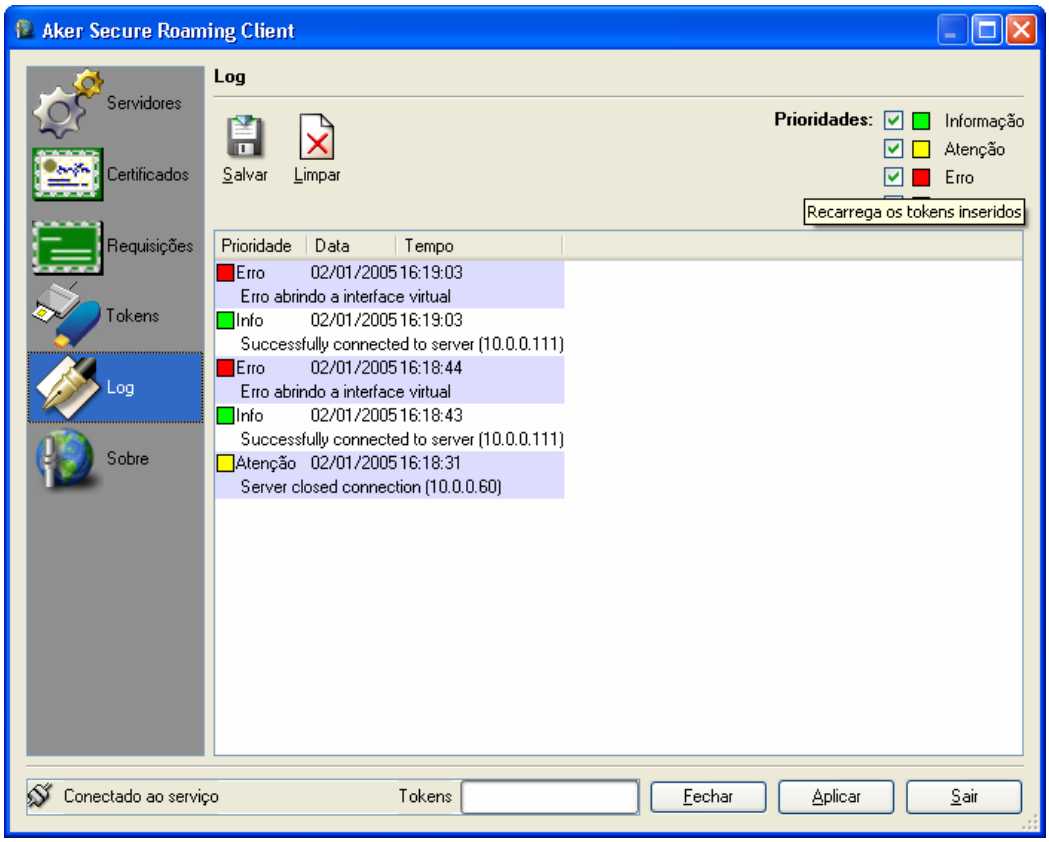
Note que apenas quando a biblioteca for carregada que os tokens ou certificados presentes no token serão carregados

Para carregar uma nova biblioteca primeiro clique no botão **Adiciona** e procure pelo arquivo com extensão *dll* (Windows) ou *so* (Unix) da biblioteca e clique para instalar. Em seguida seleciona clicando no quadrado a direita do nome e em seguida clique em **Recarregar**. Caso o arquivo selecionado seja uma biblioteca válidas informações adicionais seão mostradas na janela, caso contrário uma mensagem de erro será mostrada.

Caso você não esteja conseguindo achar a biblioteca dinâmica do seu token ou este não for reconhecido pelo seu sistema entre em contado com seu revendedor para obter maiores informações de como utilizar as funções PKCS#11 do token.

3.5. Página de Log

Essa seção mostra o log de atividade do Secure Roaming Client. Ela pode ser útil para o administrador de rede no diagnóstico de uma conexão que não funcione. A página possui o seguinte formato:



As opções disponíveis são **Salvar** e **Limpar**:

- O botão **Salvar** permite exportar o log para o arquivo texto que pode ser mandado para o sua equipe de suporte. O arquivo de texto gerado possui todas as informações mostrada na janela de Log.
- O botão **Limpar** remove todas as mensagens de Log.

 Note que apenas as mensagens presentes na janela serão exportadas para o arquivo de Log. Qualquer mensagem que for apagada usando o botão **Limpar** não será exportada para o arquivo de log.

Alternando o estado das marcas coloridas no alta à direita, você pode controlar quais mensagens serão acrescentadas à janela de log. Note que as mensagens já inclusas na lista somente podem ser removidas com o botão *Limpar*.

---

3. Termos e Definições

Aqui você encontra as definições e termos citados nesse manual de utilização.

Certificados Digitais: são documentos que associam as informações de uma identidade a uma chave pública. Eles são os equivalentes digitais de uma carteira de identidade. Um certificado digital contém informações (nome, endereço, etc.) sobre quem é o organismo ou pessoa para qual o certificado foi emitido (assunto) e também sobre quem emitiu o certificado (CA). A assinatura é um operação matemática que certifica a associação entre a chave pública e os dados. A assinatura também provê a integradade do certificado, garantindo que, caso o certificado seja alterado, sua assinatura se torne inválida. A chave pública tem como propósito oferecer um meio de criptografica assimétrica, é o equivalente da foto, da impressão digital ou da assinatura do portador em uma carteira de identidade convencional.

Requisições: são documentos criados quando uma entidade deseja requisitar um certificado digital à uma CA. Primeiro um par de chave assimétrico é gerado. Em seguida a chave publica é anexada às informações da entidade (nome, endereço, etc.). Por fim, tudo é assinado com a chave privada do par. O documento resultante pode então ser enviado a uma CA e as informações contidas nele podem ser usadas para gerar um certificado.

CA: acrônimo para *Certificate Authority*, Autoridade Certificadora. É a entidade confiável que assina requisições e gera certificados, atrelando identidades a pares de chaves. Para uso no Secure Roaming, é recomendável a manutenção de uma CA coorporativa que emita certificados apenas para usuários autorizados a estabelecer VPN.

Tokens: nesse contexto, são dispositivos criptográficos externos que armazenam chaves e certificados de forma segura e incopiável. Eles permitem a utilização de um esquema de autenticação de dois fatores: posse (do token) e conhecimento (da senha ou pin).
O suporte do Aker Secure Roaming Client para token criptográficos é baseado na especificação PKCS#11 2.20. Para que o token seja suportado, é necessário que ele possua suporte à PKCS#11 por meio de uma biblioteca dinâmica (arquivos com extensão *dll*, windows, ou *so*, unix) que provem funções de acesso padronizadas. Cada token possui sua biblioteca dinâmica PKCS#11 que pode ser obtida com seu fabricante.

NAT: acrônimo para *Network Address Translation*. É um método na qual o endereço de IP do destino ou fonte são reescritos para passarem por um roteador ou firewall. É comumentente usado quando é necessário múltiplos clientes acessarem a Internet ou outra rede de uma rede privada usando apenas um endereço externo.

VPN: acrônimo para *Virtual Private Network*. É uma rede comunicação que usa uma infraestrutura pública de rede para fazer as conexões privadas. O *Aker Secure Roaming Cliente/Server* provê um rede segura de comunicação usando de um tunelamento criptográfico, de forma a prover confidencialidade, autenticação e integridade das mensagens.

PKCS#12: documento distribuído pela RSA Laboratories que define um de formato de arquivo usado para guardar uma chaves privada e seu certificado correspondente protegidos por um senha baseada em uma chave simétrica.

DER: acrônimo de *Distinguished Encoding Rules*, é um método para codificar dados, com um certificado X.509, para ser digitalmente assinado ou para ter sua assinatura conferida.

Base 64: método de codificação de dados na qual a representação binária do dados é convertida para caracteres ASCII que podem ser impressos.