eToken PKI Client

Versão 4.5

Manual de Referência

Setembro de 2007

Índice

Capítulo 1 – Introdução **3**
Panorama 4
Capítulo 2 – Requisitos do sistema **5**
Capítulo 3 – Instalação **6**
Upgrade 7
Instalação através do Assistente 8
Capítulo 4 – Aplicativo eToken Properties **10**
Panorama do eToken Properties 12
Funções rápidas 15
Modos de exibição 15
Login 15
Modo de exibição Simples 17
Renomeando o eToken 19
Alterando a senha do eToken 19
Desbloqueando o eToken utilizando a Pergunta/Resposta 21
Exibindo as informações do eToken 23
Desconectando o eToken Virtual 24
Modo de exibição Avançado 25
eTokens & Readers 26
Inserindo o eToken virtual 27
Exibindo o eToken inserido 28
Inicializando o eToken 29
Login como usuário 34
Login como administrador 34
Importando um certificado 34
Certificados 38
Definindo um certificado como padrão, agente de inscrição ou auxiliar 41
Configurações 43

Capítulo 1 – Introdução

Este capítulo apresenta o eToken PKI Client da Aladdin, o software que permite operações com o eToken USB e a implementação de soluções que utilizem o eToken PKI.

Este capítulo aborda:

- Panorama
- Arquitetura do sistema
- Novos recursos

Panorama

A Infra-Estrutura de Chave Pública (PKI) é uma estrutura para criar um método seguro de troca de informações com o uso da criptografia de chave pública, prevendo que terceiros confiáveis verifiquem e atestem as identidades dos usuários. Trata-se de uma estrutura que consiste em um sistema de certificados digitais, Autoridades Certificadoras e outras autoridades de registro que verificam e autenticam a validade de cada parte envolvida em uma transação na internet.

O eToken PKI Client da Aladdin permite a integração com vários aplicativos de segurança. Ele permite que aplicativos de segurança eToken e aplicativos de outros fornecedores se comuniquem com o dispositivo eToken para que ele funcione com várias soluções e vários aplicativos de segurança. Entre elas estão soluções de PKI eToken utilizando o PKCS#11 ou CAPI, aplicativos eToken próprios, como SSO (Sign-On Único), eToken for Network Logon, e soluções de gerenciamento, como eToken TMS – um Sistema de Gerenciamento de Tokens que constitui uma estrutura completa para gerenciar todos os aspectos da atribuição, implantação e personalização de tokens em uma empresa.

O eToken PKI Client permite a implementação de uma autenticação bifatorial de alta segurança, utilizando certificados padrão e criptografia e assinatura digital de dados. A integração genérica com as interfaces de segurança CAPI e PKCS#11 da Microsoft permite a interoperabilidade original com vários aplicativos de segurança, proporcionando acesso seguro pela Web e por VPNs, login seguro na rede, segurança de PCs e dados, email seguro, e muito mais. As chaves e os certificados de PKI podem ser criados, armazenados e usados com segurança a partir de dispositivos de smart card eToken.

O eToken PKI Client pode ser implementado e atualizado através de qualquer sistema padrão de distribuição de software, inclusive GPO e SMS.

O aplicativo eToken Properties e o PKI Client Monitor Service são instalados com o eToken PKI Client, oferecendo ferramentas intuitivas de configuração para usuários e administradores.

Capítulo 2 – Requisitos do sistema

Sistemas operacionais suportados	Windows 2000® com SP4 ou posterior
	Windows Server 2003®
	Windows XP® 32 e 64 bits com SP2 ou posterior
	Windows Vista™ de 32 e 64 bits
Navegadores suportados	IE 6 e 7
	Firefox 2
	Netscape 7.2
Dispositivos eToken suportados	eToken PRO (Siemens CardOS e Java Card)
	eToken NG-OTP
	eToken NG-FLASH
	eToken PRO Smartcard
Requisitos de hardware	Porta USB 1.0 a 2.0
Resolução de tela recomendada	1024 x 768 pixels ou mais (para o eToken Properties)

Observações:
Não são permitidas as APIs de baixo nível usadas no eToken RTE 3.65 e versões anteriores.
A versão de avaliação suporta sistemas operacionais de 64 bits.

Capítulo 3 – Instalação

O eToken PKI Client contém todos os arquivos e drivers necessários à integração do eToken. Ele também contém a ferramenta de configuração eToken Properties, que facilita o gerenciamento da senha e do nome do eToken pelo usuário.

Este capítulo aborda:

- Upgrade
- Instalação através do Assistente
- Instalação através da Linha de Comando
- Instalação no Modo Discreto
- Desinstalação

Upgrade

O eToken RTE 3.65 e suas versões posteriores são automaticamente atualizados durante a instalação do eToken PKI Client 4.5.

As versões do eToken RTE anteriores à 3.65 devem ser desinstaladas ou atualizadas para o eToken RTE 3.65 antes da instalação do eToken PKI Client 4.5.

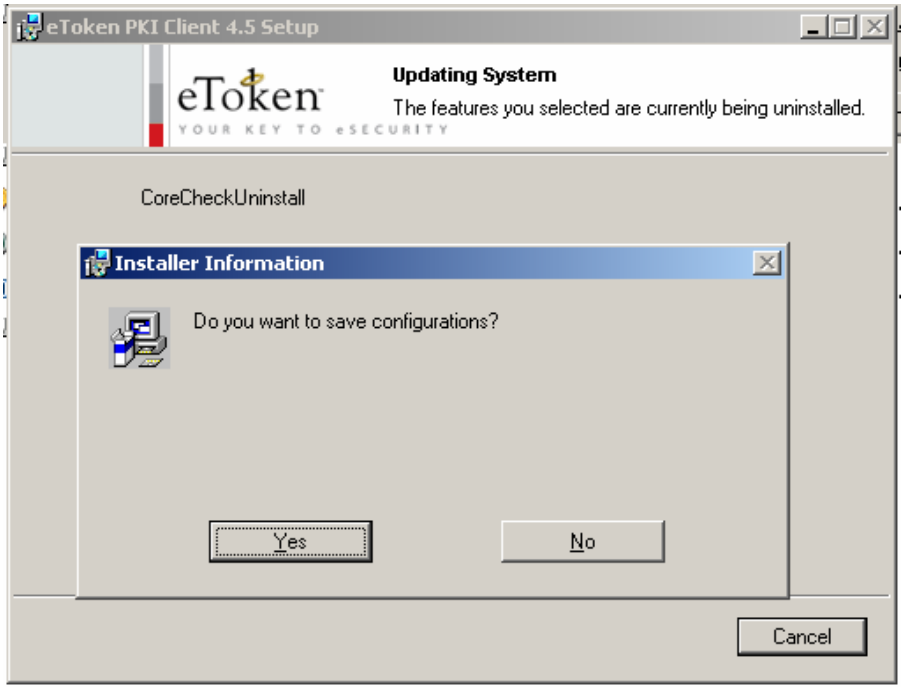
As configurações de máquina e cadastro de usuários não são apagadas quando as versões do PKI Client anteriores à 4.5 são atualizadas ou desinstaladas.

Para apagar todos os registros criados por qualquer implementação do PKI Client:

1. Desinstale qualquer versão do eToken RTE anterior à 3.65.

2. Instale o eToken PKI Client 4.5.

3. Desinstale o eToken PKI Client 4.5. Uma caixa de diálogo de gravação de configurações *(save configurations)* será aberta.



4. Clique em **Não**. A desinstalação prosseguirá e as configurações anteriores serão excluídas.

Instalação através do Assistente

O eToken PKI Client deve ser instalado em cada computador em que um dispositivo eToken for utilizado. A instalação deve ser realizada por um usuário com privilégios de administrador.

Para instalar através do assistente:

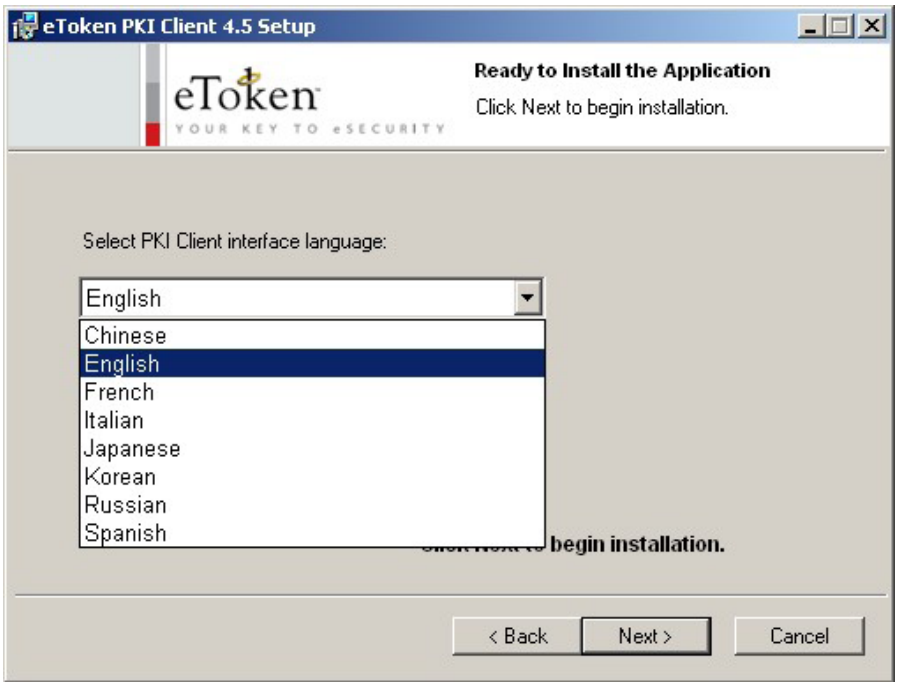
1. Efetue o login como administrador.

2. Feche todos os aplicativos

3. Clique duas vezes no arquivo msi apropriado do PKIClient (32 ou 64 bits). O *Assistente de Instalação do eToken PKI Client 4.5* será aberto.

4. Clique em **Next *(Avançar)***. Se o eToken PKI Client já estiver instalado, a reparação será iniciada.

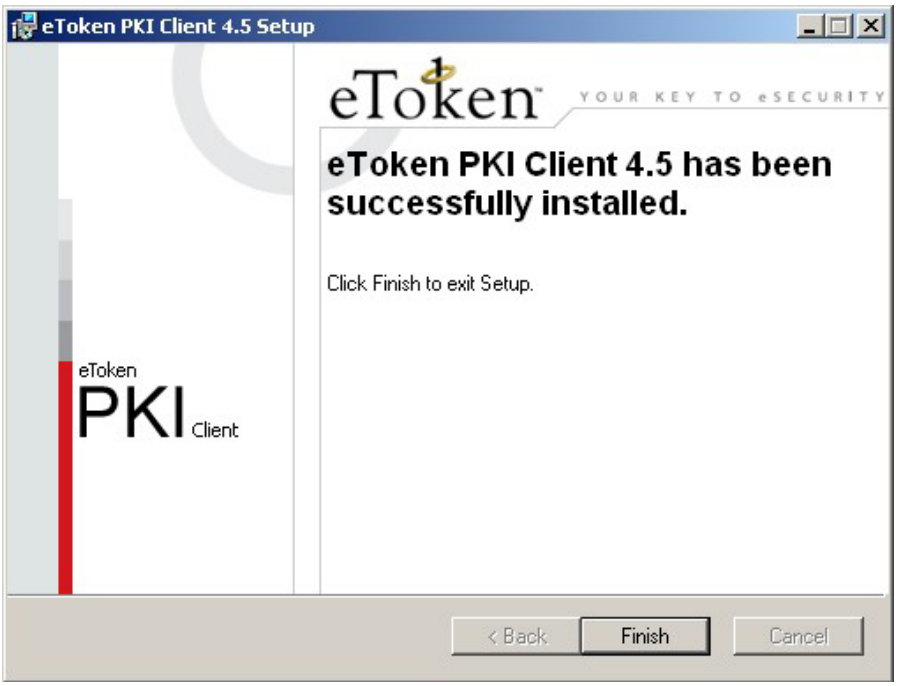
5. Se o eToken PKI Client não estiver instalado, a caixa de diálogo *Select interface language (Escolha o idioma da interface)* será exibida.



6. Na lista suspensa, escolha o idioma em que as telas do PKI Client serão exibidas para o usuário, e clique em **Next**. O Contrato de Licenciamento será exibido.

7. Leia atentamente o contrato de licenciamento e selecione a opção **I accept the license agreement *(Aceito o contrato de licença)***.

8. Clique em **Next** para iniciar a instalação. Durante a instalação, uma janela *Updating Sistema (Atualizando o Sistema)* será exibida, apresentando o andamento da instalação. Quando a instalação for concluída, uma mensagem *successfully installed (instalação bem-sucedida)* será exibida.



9. Clique em **Finish *(Encerrar)***. O eToken PKI Client 4.5 está instalado.

10. Siga as instruções para reiniciar o computador se elas forem exibidas.

Capítulo 4 – Aplicativo eToken Properties

Este capítulo explica o aplicativo eToken Properties e as diversas opções de configuração à disposição do administrador e do usuário.

Este capítulo descreve:

- Panorama do eToken Properties
- Funções rápidas
- Modos de exibição
- Login
- Modo de exibição Simples
- Modo de exibição Avançado

Panorama do eToken Properties

Os administradores devem usar o eToken Properties para criar políticas do eToken. Os usuários utilizam o eToken Properties para realizar funções básicas de gerenciamento do eToken, como alteração de senhas e visualização dos certificados nos tokens. Além disso, o eToken Properties proporciona aos usuários e administradores uma maneira fácil e rápida de transferir certificados e chaves digitais entre um computador e um token.

O eToken Properties possui um recurso de inicialização que permite aos administradores inicializar tokens de acordo com necessidades ou modos de segurança específicos da empresa, e um recurso de qualidade de senha que define parâmetros para calcular a classificação de qualidade de uma senha do eToken.

Cuidado: Não retire o token da porta USB durante uma operação! Muitas operações, como geração de chaves, inscrição de certificados e retirada de certificados, exigem mais de uma ação. Se o token for removido durante uma dessas ações, a estrutura de dados do token poderá ser danificada e existe a possibilidade de perda de dados. Por isso, pode ser necessário reinicializar o eToken.

O eToken Properties apresenta informações sobre o eToken, inclusive sua identificação e seus recursos. Ele tem acesso a informações armazenadas no token, como chaves e certificados, e permite o gerenciamento apenas do conteúdo (por exemplo, perfis de senha) compreendido pelo usuário (ou seja, não são objetos do PKCS#11) e pelo PKI Client.

Funções rápidas

As seguintes funções podem ser acessadas rapidamente pelo menu na bandeja do sistema:

- **Open eToken Properties *(Abrir o eToken Properties)***
- **Generate OTP**: gera uma OTP do eToken Virtual
- **Change eToken Password *(Alterar a senha do eToken)***
- **eTokens**: seleciona o token ativado se mais de um estiver inserido
- **About *(Sobre)***: exibe as informações do produto
- **Hide *(Ocultar)***: oculta o ícone

Acessando o menu de funções rápidas

Para acessar o menu de funções rápidas:

• Clique com o botão direito no ícone eToken  na bandeja do sistema. O menu de funções rápidas será aberto.

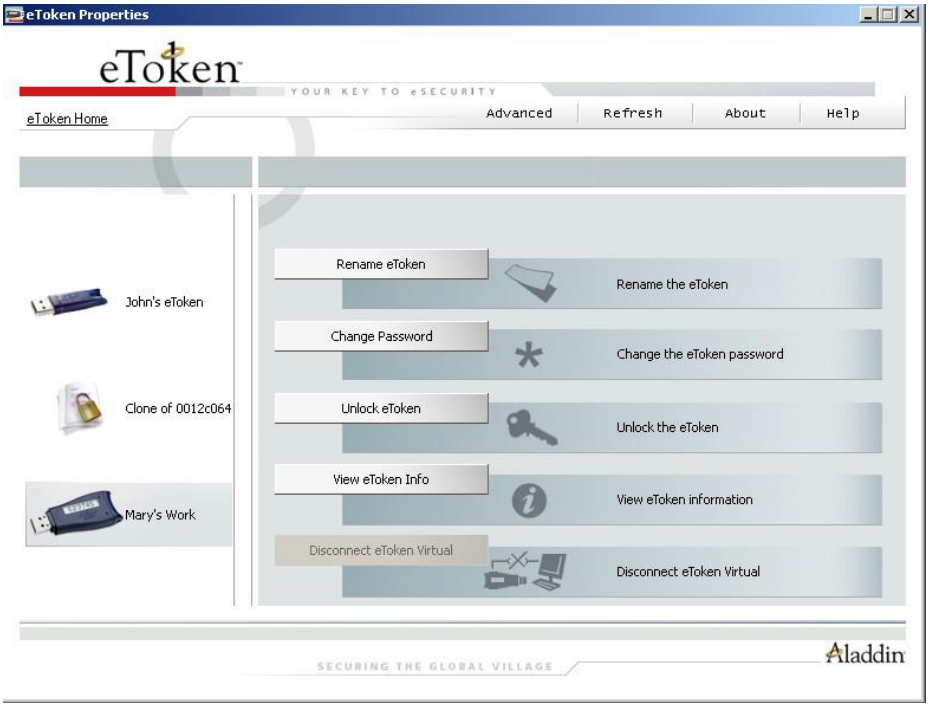
Abrindo o eToken Properties

Para abrir o eToken Properties:

• Selecione **Open eToken Properties *(Abrir o eToken Properties)***

Observação: o eToken Properties também pode ser iniciado em **Iniciar > Programas > eToken > eToken Properties**.

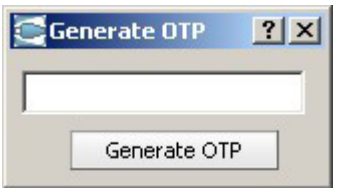
A janela *eToken Properties* é aberta no modo de exibição Simples, exibindo todos os tokens conectados ao seu computador.



Gerando uma Senha Única (OTP)

Para gerar uma OTP:

1. Selecione **Generate OTP**. A caixa de diálogo *Generate OTP* será aberta.



2. Clique em **Generate OTP**. A caixa de diálogo *Log On to eToken (Login no eToken)* será exibida.

3. Insira a senha do eToken. A OTP gerada será exibida na caixa de diálogo *Generate OTP*.

Alterando a senha do eToken

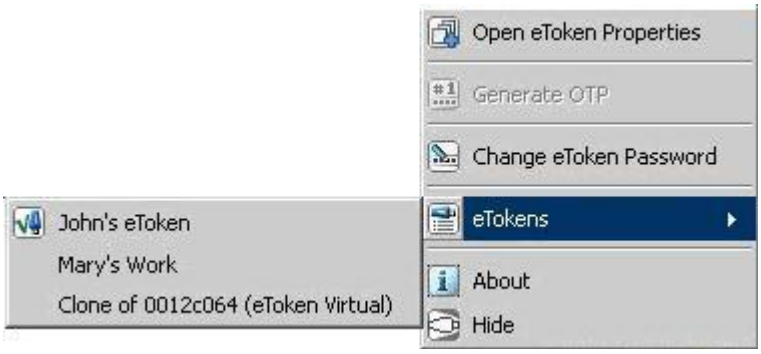
Para alterar a senha do eToken:

• Selecione **Change eToken Password *(Alterar a senha do eToken)*** A caixa de diálogo *Change Password (Alterar Senha)* será aberta. Veja a seção *Alterando a Senha do eToken*.

Selecionando o eToken ativo

Para selecionar o eToken ativo:

1. Selecione **eTokens**. Uma lista dos eTokens inseridos será exibida.



2. Selecione o eToken desejado.

Exibindo as informações do produto

Para exibir as informações do produto:

• Selecione **About *(Sobre)***.

Ocultando e reexibindo o menu de funções rápidas

Para ocultar o menu de funções rápidas:

• Selecione **Hide *(Ocultar)***.

Para reexibir o menu de funções rápidas:

Você tem duas opções

• Remova e reinsira o token

• Reinicie o computador

Modos de exibição

O eToken Properties tem duas opções de exibição:

- Modo de exibição Simples: para realizar tarefas básicas e comuns, consulte a seção Modo de exibição Simples na página 44.
- Modo de exibição Avançado: para ter controle total sobre o PKI Client e os tokens inseridos, consulte a seção Modo de exibição Avançado na página 52.

Cada modo de exibição apresenta dois painéis:

- O painel esquerdo indica qual token (modo de exibição Simples) ou qual objeto (modo de exibição Avançado) deve ser gerenciado.
- O painel direito permite que o usuário realize ações específicas com o token ou objeto selecionado.

Uma barra de ferramentas no alto da tela permite iniciar determinadas ações em ambos os modos de exibição.

Login

Algumas operações que alteram as configurações do token exigem a digitação da senha de usuário do eToken ou da senha de administrador do eToken.

Quando a senha de usuário do eToken for solicitada, a caixa de diálogo *Log On to eToken (Login no eToken)* será exibida:

Insira a senha do eToken e clique em **OK**.

Você pode realizar o login como administrador apenas se houver uma senha de administrador presente no token.

Quando a senha de administrador do eToken for solicitada, a caixa de diálogo *Administrator Logon to eToken (Login de Administrador no eToken)* será exibida:

Insira a senha de administrador do eToken e clique em **OK**.

Observação: se você estiver conectado como administrador e quiser ter acesso a funções que exigem uma senha de usuário, a caixa de diálogo *Log On to eToken* será exibida, solicitando a senha de usuário do eToken.

Modo de exibição Simples

Quando o eToken Properties for iniciado, a janela *eToken Properties* será aberta no modo de exibição Simples.

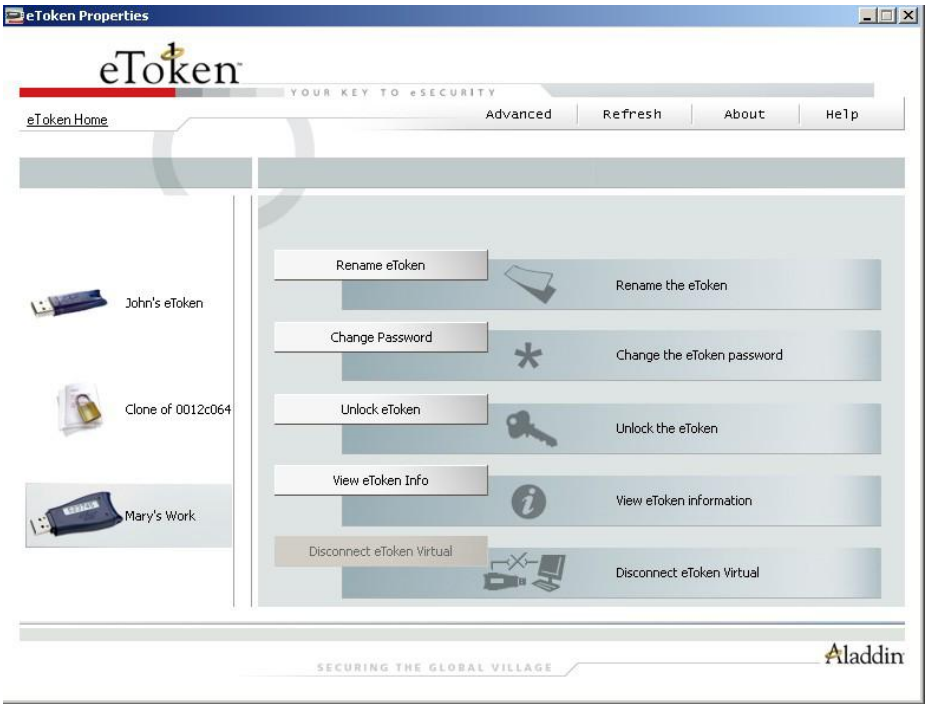
Quando um token for inserido ou quando um eToken Virtual estiver presente, um ícone específico do dispositivo, que representa o token inserido, será exibido no painel esquerdo.

Cada token tem um nome à direita do ícone. *eToken* é o nome predefinido se nenhum nome for atribuído ao token.

O token selecionado será marcado com um retângulo sombreado no painel esquerdo.

Ícones do eToken

	eToken PRO
	eToken Virtual
	eToken NG-OTP
	eToken NG-FLASH
	Leitor de Smart Card – sem cartão
	Leitor de Smart Card – com cartão
	eToken com dados corrompidos
	Token desconhecido



No painel direito, o usuário pode selecionar qualquer uma das seguintes ações disponíveis:

• **Rename eToken *(Renomear eToken)*** – define o nome do token

• **Change Password *(Alterar Senha)*** – altera a senha de usuário do eToken

• **Unlock eToken *(Desbloquear eToken)*** – recupera a senha do usuário através de um mecanismo de pergunta/resposta (ativo apenas quando uma senha de administrador tiver sido inicializada no token)

• **View eToken Info *(Exibir informações do eToken)*** – apresenta informações detalhadas sobre o token

• **Disconnect eToken Virtual *(Desconectar o eToken Virtual)*** – desconecta o eToken Virtual, com a opção de excluí-lo

A barra de ferramentas no alto contém as seguintes funções:

• **Advanced *(Avançado)*** – muda para o modo de exibição Avançado

• **Refresh *(Atualizar)*** – atualiza os dados de todos os tokens conectados

• **About *(Sobre)*** – exibe informações sobre a versão do produto

• **Help *(Ajuda)*** – inicia a ajuda eletrônica

Um hiperlink para o site do eToken, *eToken Home*, é exibido no canto superior esquerdo da tela.

Renomeando o eToken

O nome do token pode ser personalizado.

Para renomear um token:

1. No painel esquerdo da janela *eToken Properties*, selecione o token a ser renomeado.

2. Clique em **Rename eToken *(Renomear o eToken)*** no painel direito. A caixa de diálogo *Rename eToken* será exibida.

3. Insira o novo nome no campo New eToken name *(Novo nome do eToken)*.

4. Clique em **OK**. O novo nome do token será exibido na janela *eToken Properties*.

Alterando a senha do eToken

Todos os dispositivos eToken são configurados com a senha original de fábrica 1234567890. Para garantir uma alta segurança bifatorial, é importante que o usuário altere a senha do eToken para uma senha particular do usuário assim que o novo eToken for recebido.

Quando uma senha do eToken é alterada, a nova senha é usada para todos os aplicativos eToken que utilizem o token. O usuário é responsável por memorizar a senha do eToken. Sem ela, o usuário não poderá usar o token.

A criação de uma senha de administrador no token permite que o administrador desbloqueie um token bloqueado, redefinindo uma nova senha para o usuário se ela for esquecida. Recomendamos inicializar todos os tokens com uma senha de administrador.

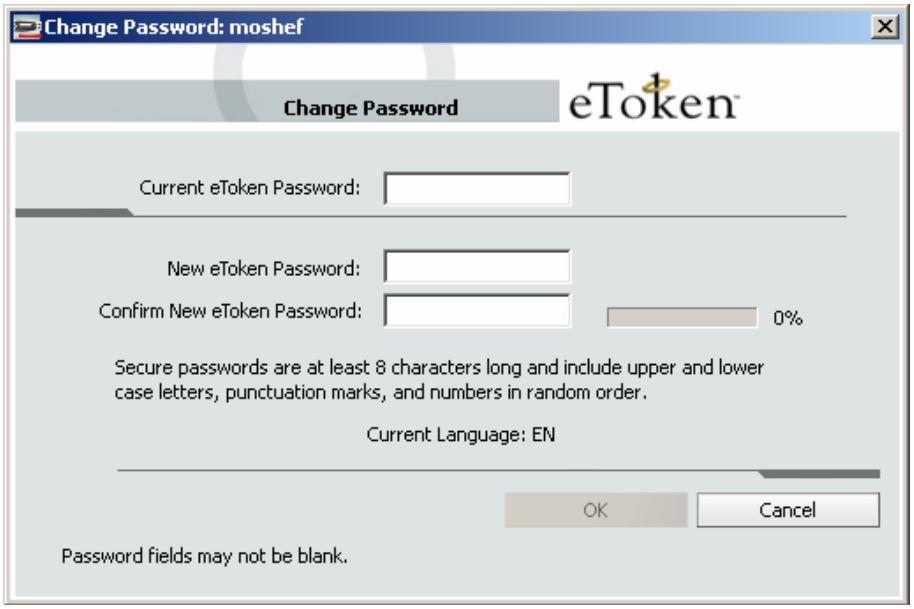
O recurso de Qualidade de Senha do eToken permite que o administrador agregue uma certa complexidade e requisitos de uso à senha. Veja a seção Qualidade da senha.

Observação: A senha de usuário do eToken é uma medida importante de segurança para proteger as informações confidenciais da sua empresa. As melhores senhas têm pelo menos oito caracteres e contêm letras maiúsculas e minúsculas, sinais de pontuação e números criados em ordem aleatória. Não recomendamos o uso de senhas que possam ser facilmente descobertas, como nomes ou datas de nascimento de familiares.

Para alterar a senha do eToken:

1. No painel esquerdo da janela *eToken Properties*, selecione o token ao qual a nova senha será atribuída.

2. Clique em **Change Password *(Alterar Senha)*** no painel direito. A caixa de diálogo *Change Password* será exibida.



3. Insira a senha atual do eToken no campo Current eToken Password *(Senha atual do eToken).*

4. Insira a nova senha do eToken nos campos New eToken Password *(Nova senha do Token)* e Confirm *(Confirme).*

OBSERVAÇÃO: Durante a digitação da nova senha, o indicador de qualidade da senha à direita mostrará uma pontuação percentual, indicando o nível da nova senha em relação à política de qualidade de senhas.

5. Clique em **OK**. A senha do eToken foi alterada.

Desbloqueando o eToken utilizando a Pergunta/Resposta

O token será bloqueado se a senha do eToken for incorretamente digitada muitas vezes.

Se o token tiver sido inicializado com uma senha de administrador, e se o administrador estiver presente, o token poderá ser desbloqueado através do modo de exibição Avançado do eToken Properties. Veja a seção Criando a senha do usuário.

Quando o administrador estiver em outra localidade, por exemplo, quando um funcionário estiver fora do escritório, pode ser utilizado um método de autenticação por Pergunta/Resposta para desbloquear o token. Nesse método, o usuário envia ao administrador os Dados de Pergunta fornecidos pelo eToken Properties e, em seguida, digita os Dados de Resposta fornecidos pelo administrador. Então, o usuário insere uma nova senha, e o token é desbloqueado.

Para desbloquear um token usando o método de Pergunta/Resposta:

1. No painel esquerdo da janela *eToken Properties*, selecione o token a ser desbloqueado.

2. Clique em **Unlock eToken *(Desbloquear o eToken)*** no painel direito. A caixa de diálogo *Unlock eToken* será exibida.

3. Entre em contato com o administrador e forneça os Dados de Pergunta.

Cuidado: após fornecer os Dados de Pergunta ao administrador, o usuário NÃO DEVERÁ realizar nenhuma atividade que use o token antes de receber os Dados de Resposta e concluir o procedimento de desbloqueio.

Se ocorrer alguma outra atividade com o eToken durante esse processo, ela afetará o contexto do processo de Pergunta/Resposta e invalidará o procedimento.

4. O administrador fornece os Dados de Resposta para serem inseridos.

5. Insira a nova senha do eToken nos campos Password *(Senha)* e Confirm *(Confirme)*.

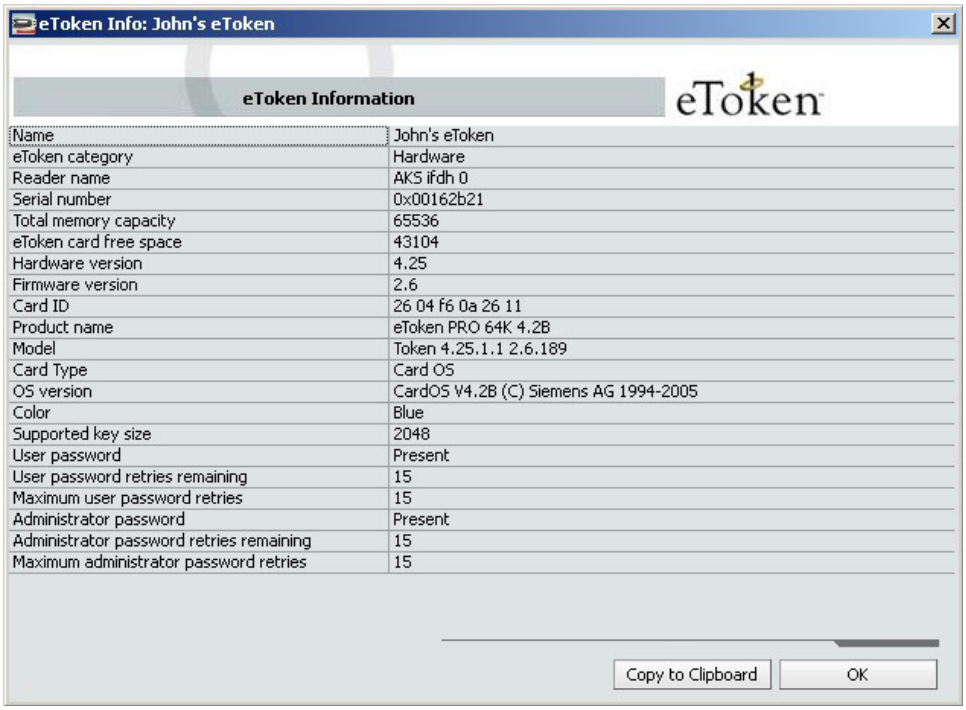
6. Selecione **Change password on first logon *(Alterar a senha no primeiro login)*** se a nova senha for conhecida por outras pessoas e precisar ser alterada.

7. Clique em **OK**. O token será desbloqueado e uma mensagem de confirmação será exibida.

Observação: a criação dos Dados de Resposta depende do aplicativo de retaguarda usado pela empresa. Consulte na respectiva documentação os detalhes de como gerar os Dados de Resposta.

Exibindo as informações do eToken

As informações relacionadas a um token específico podem ser exibidas, bastando selecionar o token no painel esquerdo da janela *eToken Properties* e clicar em **View eToken Info *(Exibir Informações do eToken)*** no painel direito. A caixa de diálogo *eToken Information (Informações do eToken)* será exibida:



As informações desta caixa de diálogo podem ser copiadas para a área de transferência.

Para colar as informações em um aplicativo:

1. Clique em **Copy to Clipboard *(Copiar para a Área de Transferência)***.

2. Posicione o cursor no aplicativo de destino e cole as informações.

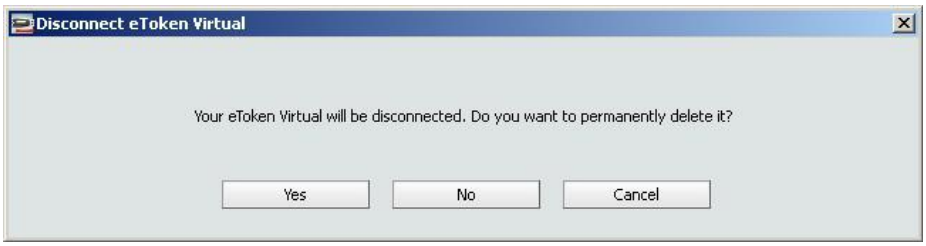
Desconectando o eToken Virtual

Quando o eToken Virtual não for mais necessário, desconecte-o do seu leitor.

Para desconectar um eToken Virtual:

1. No painel esquerdo da janela *eToken Properties*, selecione o eToken Virtual a ser desconectado.

2. Clique em **Disconnect eToken Virtual *(Desconectar o eToken Virtual)*** no painel direito. A caixa de diálogo *Disconnect eToken Virtual* será exibida.



3. Para manter o eToken Virtual no computador, clique em **No**, e apenas a conexão do eToken Virtual com o eToken Properties será desfeita.

4. Para remover o arquivo eToken Virtual do computador, clique em **Yes**.

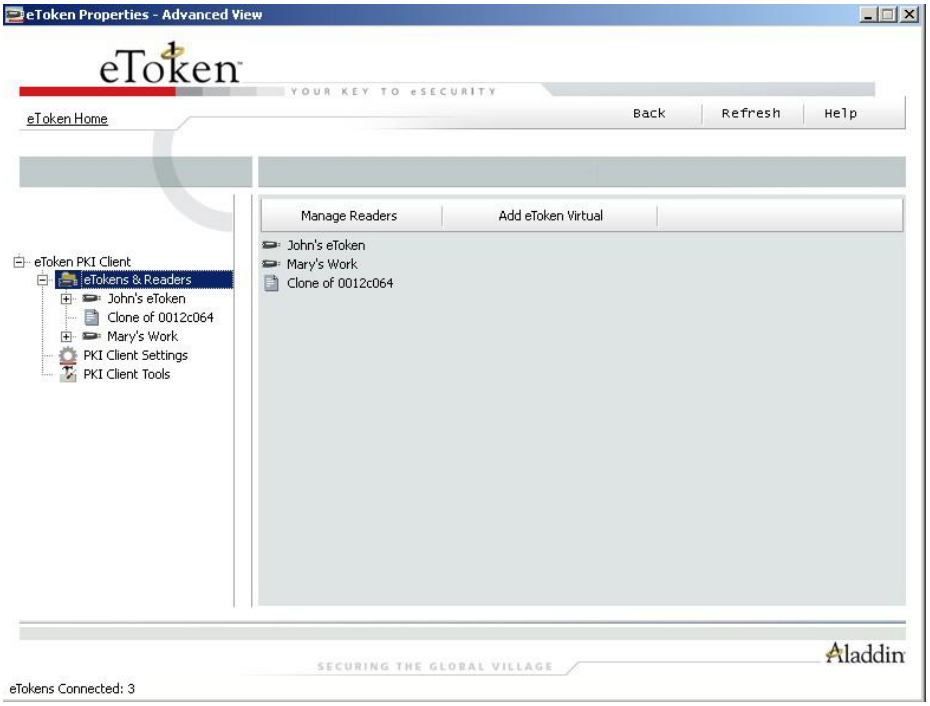
Observação: a desconexão do eToken Virtual a remoção total é uma ação que pode ser efetuada quando o usuário não estiver no escritório e precisar usar o eToken Virtual posteriormente quando também não estiver no escritório.

Quando o eToken perdido for reposto, o eToken Virtual deverá ser completamente removido do computador.

Modo de exibição Avançado

O modo de exibição Avançado do eToken Properties oferece mais funções de gerenciamento de tokens.

Clique em **Advanced *(Avançado)*** na barra de ferramentas do modo de exibição Simples, e a janela *eToken Properties* será aberta no modo de exibição Avançado.



A barra de ferramentas no alto oferece as seguintes funções:

• **Back *(Voltar)***: muda para o modo de exibição Simples

• **Refresh *(Atualizar)***: atualiza os dados de todos os tokens conectados

• **Help *(Ajuda)***: inicia a ajuda eletrônica

Um hiperlink para o site do eToken, *eToken Home*, é exibido no canto superior esquerdo da tela.

Uma barra de status na parte inferior da janela exibe mais informações sobre o objeto destacado, como o número de leitores conectados, ou o estado atual de login.

O painel esquerdo apresenta um modo de exibição de árvore dos vários objetos a serem gerenciados. A árvore se expande para mostrar os objetos dos tokens inseridos.

- Clique com o botão esquerdo em um objeto na árvore para exibir as informações sobre esse objeto no painel direito.

- Clique com o botão direito em um objeto na árvore para exibir um menu de contexto com comandos para esse objeto.

eTokens & Readers

Este nó gerencia os leitores (slots) disponíveis no sistema.

Quando o nó eTokens & Readers for selecionado, a barra de ferramentas exibirá o seguinte:

• Manage Readers *(Gerenciar Leitores)*

• Add eToken Virtual *(Adicionar eToken Virtual)*

Os mesmos comandos ficam disponíveis quando você clica com o botão direito no nó eTokens & Readers.

Gerenciando leitores

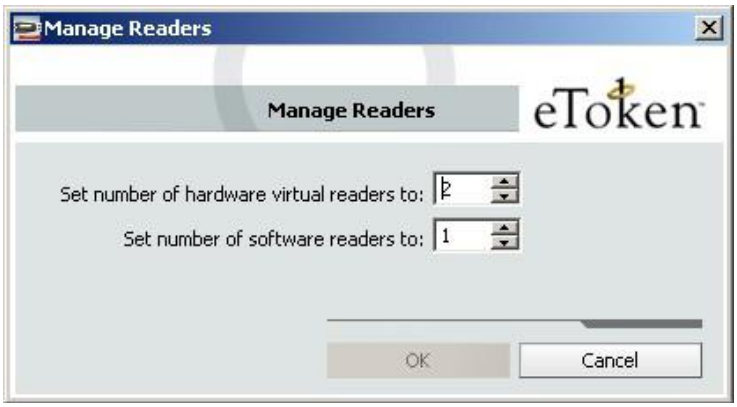
Durante a instalação do eToken PKI Client, o eToken Properties instala dois leitores de *smart cards* virtuais e um leitor eToken Virtual.

Quando um eToken é inserido em uma porta USB, ou quando um eToken Virtual é adicionado, ou quando um *smart card* é inserido no leitor, o efeito é o mesmo de inserir um *smart card* em um dos leitores.

O número de leitores predefinidos em um computador pode ser alterado por um usuário com direitos de administrador local nesse computador.

Para alterar o número de leitores:

1. Clique em **Manage Readers *(Gerenciar Leitores)*** na barra de ferramentas, ou clique com o botão direito em **eTokens & Readers** e selecione **Manage Readers** no menu de atalho. A caixa de diálogo *Manage Readers* será aberta.



2. Defina o número de leitores físicos e lógicos no campo apropriado, com o número desejado.

O número predefinido de leitores disponíveis é:

- Leitores físicos: 2
- Leitores lógicos: 1

3. Clique em **OK** para fechar a caixa de diálogo. O número de leitores disponíveis foi alterado.

4. Reinicie o eToken Properties para aplicar as alterações.

Inserindo um eToken Virtual

O PKI Client 4.5 aceita o eToken Virtual, um token lógico. O eToken Virtual fica armazenado em um arquivo no computador.

O eToken Virtual foi especialmente projetado como uma solução para problemas de "funcionários fora do escritório", quando a substituição de um eToken perdido ou esquecido não é viável.

Para incluir um eToken Virtual:

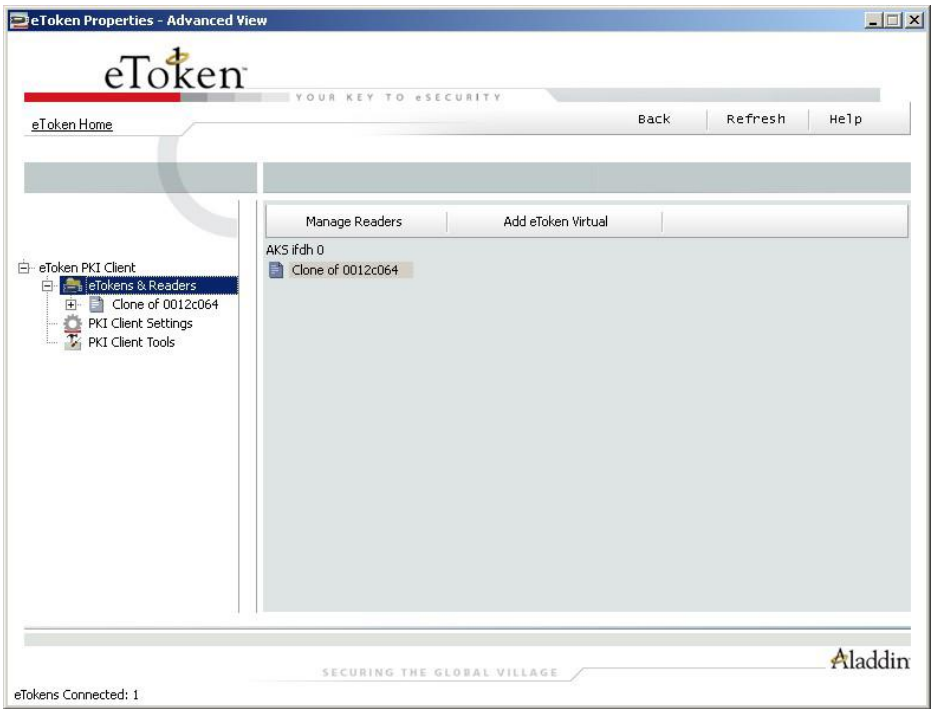
1. clique em **Add eToken Virtual *(Adicionar eToken Virtual)*** na barra de ferramentas, ou clique com o botão direito em **eTokens & Readers** e selecione **Add eToken Virtual** no menu de atalho.

3. Navegue até o arquivo do eToken Virtual (*.etv) e clique duas vezes nele. O eToken Virtual foi incluído e uma caixa de diálogo de confirmação será exibida.

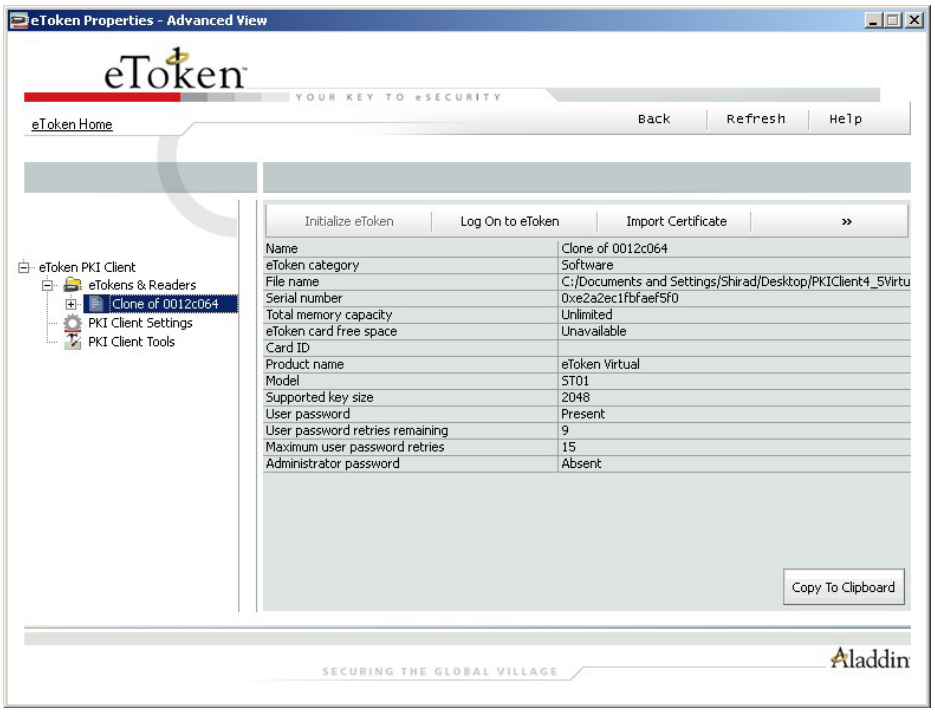
3. Clique em **OK**.

Exibindo eTokens inseridos

Quando o nó eTokens & Readers for expandido, os nomes de todos os tokens inseridos (tanto físicos como virtuais) serão exibidos.



Para exibir todas as informações sobre um token no painel direito, selecione-o no painel esquerdo.



Essas são as mesmas informações exibidas no comando Viewing eToken Info *(Exibindo Informações do eToken)* do modo de exibição Simples.

A barra de ferramentas exibe os principais comandos que podem ser realizados com este objeto ou nele, como login e importação de certificados.

A seta de expansão à direita da barra de ferramentas mostra todos os outros comandos disponíveis para este objeto.

Esses comandos também ficarão disponíveis se você clicar com o botão direito do mouse no painel esquerdo.

Alguns comandos ficam desativados se eles não forem pertinentes. Por exemplo, as funções de administrador ficam desativadas em um eToken Virtual.

Alguns comandos do modo de exibição Avançado são idênticos aos comandos do modo de exibição Simples:

- Rename eToken *(Renomear eToken)*
- Change Password *(Alterar Senha)*
- Unlock eToken *(Desbloquear eToken)*
- Disconnect eToken Virtual *(Desconectar eToken Virtual)*

Inicializando o eToken

A opção de inicialização do eToken devolve um eToken ao seu estado inicial. Ele elimina todos os objetos armazenados no eToken desde a fabricação, libera a memória e recupera a senha original do eToken, permitindo que os

administradores inicializem o eToken de acordo com as necessidades ou os modos de segurança específicos da empresa.

Inicializar o eToken é útil, por exemplo, depois que um funcionário deixou de trabalhar na empresa. A inicialização apaga completamente do eToken os certificados individuais e outros dados pessoais do funcionário, preparando o eToken para ser usado por outro funcionário.

Os seguintes dados são inicializados:

• Nome do eToken

• Senha do usuário

• Senha do administrador (opcional)

• Número máximo de tentativas incorretas de login (para as senhas de usuário e administrador)

• Mudança obrigatória de senha no primeiro login

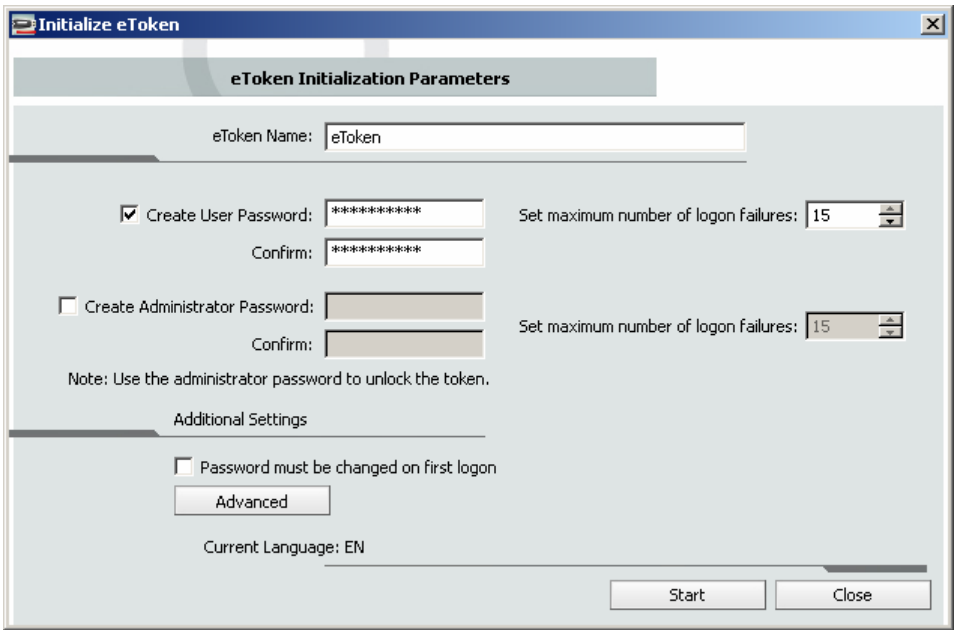
• Chave de inicialização

O processo de inicialização carrega o sistema de arquivos da Aladdin no eToken.

Utilizando parâmetros personalizáveis, você pode selecionar parâmetros específicos que valerão para alguns eTokens. Esses parâmetros poderão ser necessários se você quiser usar o eToken para determinados aplicativos ou se você precisar de uma senha específica de usuário ou administrador em todos os tokens da empresa.

Para inicializar um eToken:

1. Clique em **Initialize eToken *(Inicializar o eToken)*** na barra de ferramentas, ou clique com o botão direito no nome do token no painel esquerdo e selecione **Initialize eToken *(Inicializar eToken)*** no menu de atalho. A caixa de diálogo *eToken Initialization Parameters (Parâmetros de Inicialização do eToken)* será aberta.



2. Insira um nome para o eToken no campo *eToken Name (Nome do eToken)*. Se nenhum nome for inserido, o nome padrão "eToken" será aplicado.

3. Selecione **Create User Password *(Criar senha do usuário)*** para inicializar o token com uma senha de usuário do eToken. Caso contrário, o token será inicializado sem uma senha do eToken e não será possível usá-lo para aplicativos do eToken.

4. Se for selecionada a opção **Create User Password**, insira uma nova senha de usuário do eToken nos campos *Create User Password* e *Confirm*.

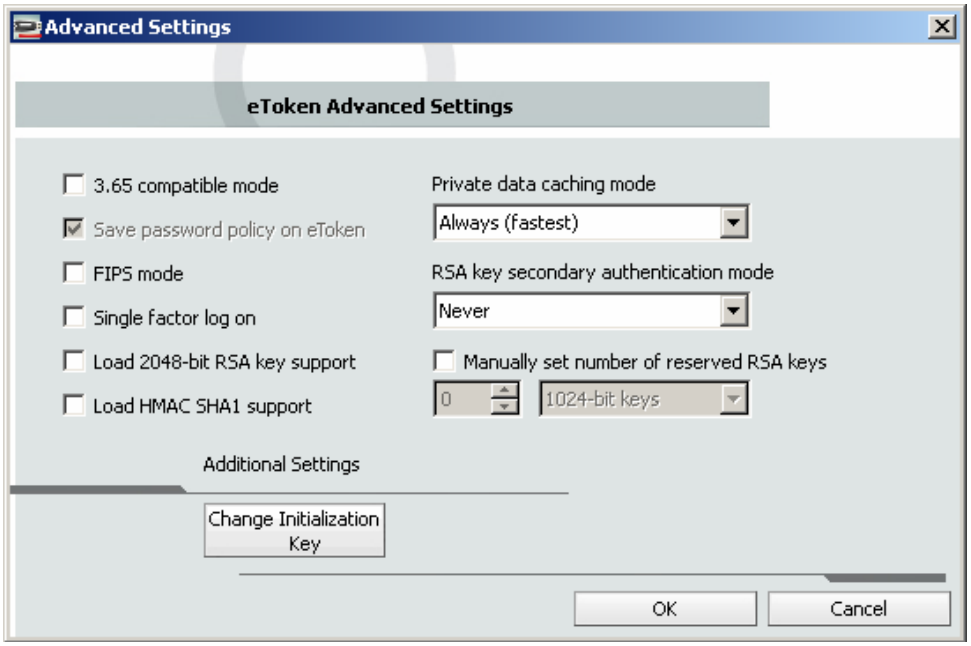
5. Para inicializar uma senha de administrador, selecione **Create Administrator Password *(Criar senha de administrador)*** e insira uma senha nos campos *Create Administrator Password* e *Confirm*. A senha deve ter no mínimo 4 caracteres.

Observação: A criação de uma senha de administrador permite a realização de certas funções no token, como recuperar a senha do usuário em um token bloqueado.

6. No campo **Set maximum number of logon failures fields *(Definir o número máximo de tentativas de login)***, insira um valor entre 1 e 15. Esse contador especifica o número de vezes que o usuário ou administrador poderá tentar realizar o login no eToken com uma senha incorreta antes que o eToken seja bloqueado. O valor inicial para o número máximo de tentativas incorretas de login é 15.

7. Se for necessário, selecione **Password must be changed on first logon *(A senha deve ser alterada no primeiro login)***.

8. Para configurar as opções avançadas, clique em **Advanced *(Avançadas)***. A caixa de diálogo *eToken Advanced Settings (Configurações Avançadas do eToken)* será aberta.



9. Preencha os campos da maneira indicada abaixo:

Campo	Descrição
3.65 compatible mode	Selecione para manter a compatibilidade com o eToken RTE 3.65.
Save password policy on eToken	Selecione para manter a política de senha no dispositivo eToken.
FIPS mode	Selecione para permitir a operação com FIPS. A FIPS (Norma Federal de Processamento de Informações) é um conjunto de normas aprovadas pelo governo dos EUA para melhorar a utilização e o gerenciamento de sistemas de informática e sistemas correlatos de telecomunicações. O eToken PRO pode ser configurado no modo FIPS.
Single factor logon	Padrão: Desativado. Quando o login monofatorial estiver ativado, apenas a presença do eToken será necessária para o login nos aplicativos. A senha é dispensada. Observação: por motivos de segurança, o login monofatorial não é aplicado ao eToken Properties.
Load 2048-bit RSA key support	Selecione para ativar o suporte à chave RSA de 2.048 bits (em um token compatível).
Load HMAC SHA1 support	Selecione para ativer o suporte à HMAC SHA1 (em um token compatível).

Private data caching mode	No PKI Client 4.5, as informações públicas armazenadas no eToken ficam em cache para aumentar a velocidade. Essa opção define quando as informações privadas (exceto as chaves privadas no eToken PRO / NG OTP / Smartcard) podem ser armazenadas fora do eToken. Selecione uma das seguintes opções: **Always (a mais veloz):** sempre armazena as informações privadas na memória do aplicativo. Isso acelera o processamento, pois algumas informações ficam armazenadas na máquina host. Entretanto, essa opção é menos segura do que não permitir o armazenamento em cache. **While user is logged on (*enquanto o usuário estiver conectado)*:** armazena os dados privados em um cache fora do eToken pelo tempo em que o usuário estiver conectado ao eToken. Quando o usuário realizar o logout, todos os dados privados do cache serão apagados. **Never *(Nunca):*** não armazena em cache os dados privados.
RSA key secondary authentication mode	Uma senha de autenticação pode ser criada para uma chave RSA. Se esta opção for utilizada, além de ter o eToken e conhecer a senha do eToken, o acesso à chave RSA exigirá que se saiba a senha definida para essa chave específica. Essa opção define a política de uso dessa autenticação secundária das chaves RSA. **Always *(Sempre)*:** sempre que uma chave RSA for gerada, você deverá informar uma senha secundária para acessar essa chave. Se você clicar em **OK**, a chave será gerada e a senha inserida será usada como senha RSA secundária para essa chave. Se você clicar em **Cancel**, a chave não será gerada. **Always prompt user *(Sempre perguntar ao usuário)*:** sempre que uma chave RSA for gerada, uma senha secundária de acesso a essa chave será solicitada. Entretanto, o usuário pode optar por ignorar a solicitação (clicando em **Cancel**), e a geração da chave continuará sem o uso de uma senha secundária para a chave RSA gerada. **Prompt on application request *(Perguntar na solicitação do aplicativo)*:** permite que os aplicativos que usam a autenticação secundária para chaves RSA utilizem esse recurso no eToken (ao criar a chave na Crypto API com um indicador de proteção pelo usuário). **Never*:*** não serão criadas senhas para nenhuma chave RSA, e o método de autenticação utilizará apenas a senha do eToken para acessar a chave.
Manually set number of reserved RSA keys	Define o número de chaves RSA reservadas, para reservar espaço na memória do token. Isso garante que sempre haja memória disponível para as chaves.
Change Initialization Key	A chave de inicialização protege contra a inicialização acidental e exige a digitação de uma senha separada antes que a inicialização ocorra.

10. Se for necessário, clique em **Change Initialization Key *(Alterar a chave de inicialização)***. A caixa de diálogo *eToken Initialization Key (Chave de Inicialização do eToken)* será aberta.

11. Preencha os campos da maneira indicada abaixo:

Campo	Descrição
Use Default Initialization Key	Selecione para usar o padrão original de fábrica.
Use Specified Initialization Key	Insira a senha configurada anteriormente no campo This Value *(Este Valor)* abaixo.
Change Initialization Key to:	**Default *(Padrão)***: voltar ao padrão. **Random *(Aleatório)***: se for selecionado, nunca será possível reinicializar o eToken. **This Valor *(Este Valor)***: selecione e confirme uma senha.

12. Clique em **OK** para retornar à caixa de diálogo *eToken Advanced Settings (Configurações Avançadas do eToken)*, e, em seguida, clique novamente em **OK** para retornar à caixa de diálogo e*Token Initialization Parameters (Parâmetros de Inicialização do eToken)*.

13. Clique em **Start *(Iniciar)***. Quando o processo de inicialização for concluído, uma mensagem de confirmação será exibida.

Login como usuário

Para realizar o login como usuário:

1. Clique em **Log On to eToken *(Login no eToken)*** na barra de ferramentas, ou clique com o botão direito do mouse no nome do token no painel esquerdo e selecione **Log On** no menu de atalho. A caixa de diálogo *Log On to eToken (Login no eToken)* será exibida.

2. Insira a senha de usuário do eToken no campo Password *(Senha)* e clique em **OK**. O usuário está conectado.

Login como administrador

Um administrador tem direitos limitados de acesso a um token. Nenhuma alteração pode ser realizada em nenhuma informação do usuário, e a segurança do usuário não pode ser afetada. As funções do administrador estão restritas a Change Administrator Password *(Alterar senha do administrador)*, Set User Password *(Criar senha do usuário)* e Change Password Quality Settings *(Alterar configurações de qualidade da senha)* armazenadas no token.

Para efetuar o login como administrador:

1. Clique em **Administrator Logon *(Login como administrador)*** na barra de ferramentas, ou clique com o botão direito do mouse no nome do token no painel esquerdo e selecione **Administrator Logon** no menu de atalho. A caixa de diálogo A*dministrator Logon s*erá exibida.

2. Insira a senha de administrador no campo Password *(Senha)* e clique em **OK**. O usuário está conectado como Administrador.

Importando um certificado

Os seguintes tipos de certificado são aceitos:

• .pfx

• .p12

• .cer

Se for selecionado um arquivo PFX, a chave privada e o respectivo certificado serão importados para o eToken. Será perguntado se os certificados da CA devem ser importados para o eToken, e será solicitado que você insira a senha (se existir) que protege o arquivo PFX.

No caso de um arquivo CER (que contém apenas certificados X.509), o programa verifica se existe uma chave privada no eToken. Se a chave privada for encontrada, o certificado será armazenado com ela. Se não for encontrada uma chave privada, será perguntado se você deseja armazenar o certificado como um certificado de CA.

Ao transferir um certificado para o computador e depois importar o certificado no eToken, retire o certificado do repositório local e reinsira o eToken antes de usar o certificado para assinar e criptografar emails. Isso garante que você use o certificado e as chaves armazenados no eToken.

Para importar um certificado:

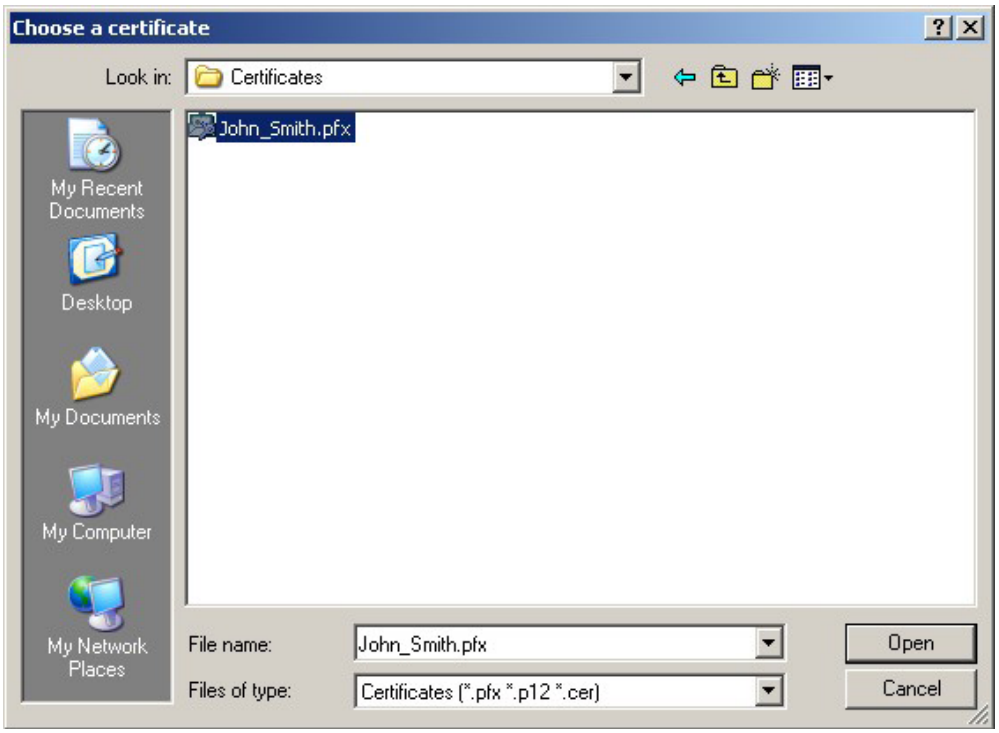
1. Clique em **Import Certificate *(Importar certificado)*** na barra de ferramentas, ou clique com o botão direito no nome do token no painel esquerdo e selecione **Import Certificate** no menu de atalho. A caixa de diálogo *Import Certificate* será aberta.

2. Selecione se o certificado a ser importado está no seu repositório pessoal de certificados no computador, ou em um arquivo. Se você selecionar "*personal certificate store*" (*repositório pessoal de certificados*), uma lista dos certificados disponíveis será exibida. Serão listados apenas os certificados que puderem ser importados no eToken. Esses certificados são:

   • Certificados com uma chave privada que já está no eToken

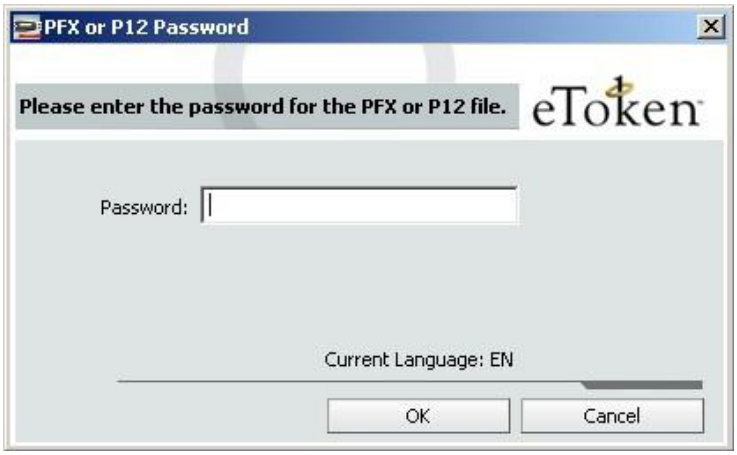
   • Certificados que podem ser importados do computador junto com sua chave privada

3. Se você selecionar **Import a certificate from a file *(Importar um certificado de um arquivo)***, será exibida a caixa de diálogo *Choose a certificate (escolha um certificado)*.



4. Selecione o certificado a ser importado e clique em **Abrir**.

5. Se o certificado solicitar uma senha, será aberta uma caixa de diálogo *Password (Senha)*.



6. Insira a senha do certificado. Uma caixa de diálogo será aberta se você quiser armazenar os certificados da CA no eToken.

7. Escolha **Yes** ou **No**. Todos os certificados solicitados serão importados, e uma mensagem de confirmação será exibida.

Alterando a senha do administrador

Para alterar a senha do administrador:

1. Clique em **Change Administrator Password *(Alterar a senha do administrador)*** na barra de ferramentas, ou clique com o botão direito do mouse no nome do token no painel esquerdo e selecione **Change Administrator Password** no menu de atalho. A caixa de diálogo *Change Administrator Password* será aberta.

2. Insira a senha atual do administrador no campo Current Password *(Senha atual)*.

3. Insira a nova senha do administrador nos campos New Password *(Nova senha)* e Retype *(Digite novamente)*.

4. Clique em **OK**. A senha do administrador foi alterada.

Criando a senha do usuário

Uma senha de usuário para desbloquear um eToken poderá ser criada apenas se uma senha de administrador tiver sido criada durante a inicialização.

Um sistema de autenticação por pergunta/respostas também pode ser usado para desbloquear um eToken bloqueado. Veja a seção Desbloqueando o eToken utilizando a Pergunta/Resposta.

Para desbloquear um utilizando Set User Password *(Criar senha do usuário)*:

1. Efetue login como administrador no token selecionado. Consulte a seção Login como Administrador na página 62.

2. Clique em **Set User Password *(Criar senha do usuário)*** na barra de ferramentas, ou clique com o botão direito do mouse no nome do token no painel esquerdo e selecione **Set User Password** no menu de atalho. A caixa de diálogo *Set eToken Password (Criar senha do eToken)* será aberta.

3. Insira a nova senha nos campos New Password *(Nova senha)* e Confirm *(Confirme)*.

4. Insira um valor de 0 a 15 no campo Set Error Retry Counter *(Configurar contador de tentativas incorretas)*.

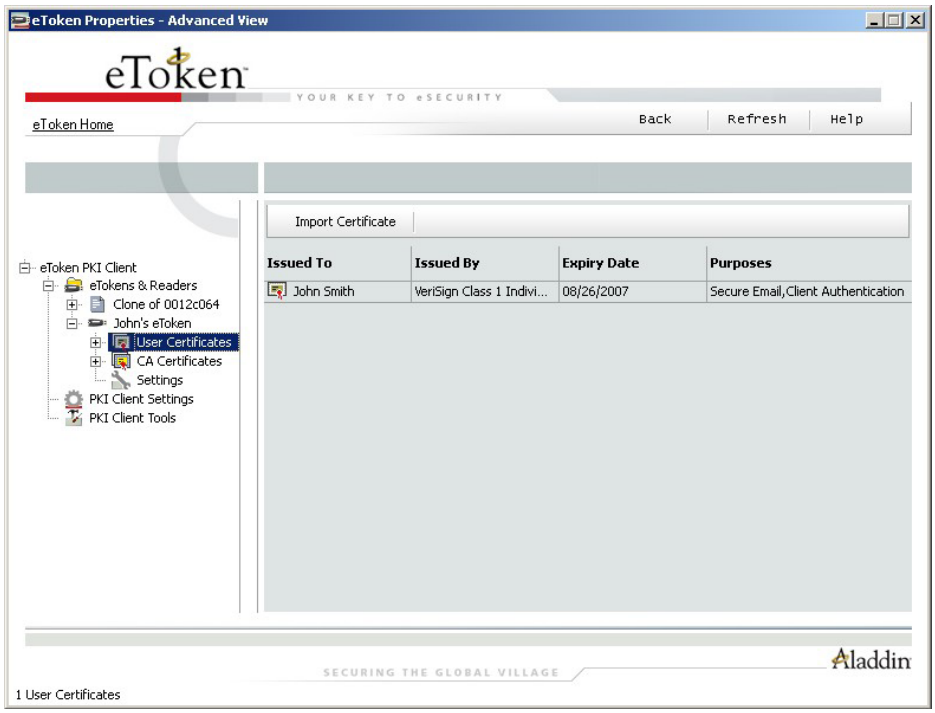
5. Clique em **OK**. O eToken está desbloqueado.

Agora você pode efetuar o login como usuário com a nova senha.

Certificados

Quando um nó do eToken for expandido, os nós dos certificados serão exibidos se o token contiver certificados.

Clique no nó User Certificates *(Certificados de usuários)* ou CA Certificates *(Certificados da CA)* para listar os certificados no painel direito, ou para importar outro certificado.



Expanda o nó Certificates para selecionar certificados individuais.

Selecione um certificado para ativar os seguintes comandos:

- Delete Certificate *(Excluir certificado)*
- Export Certificate *(Exportar certificado)*

• Set as Enrollment Agent *(Definir como agente de inscrição)*

• Set as Default (*Definir como padrão*)

• Set as Auxiliary (*Definir como auxiliar*)

• Copy to Clipboard *(Copiar para a Área de Transferência)*

Para iniciar a atividade do certificado, você tem duas opções:

• Selecione o certificado no painel esquerdo e clique na ação apropriada na barra de ferramentas

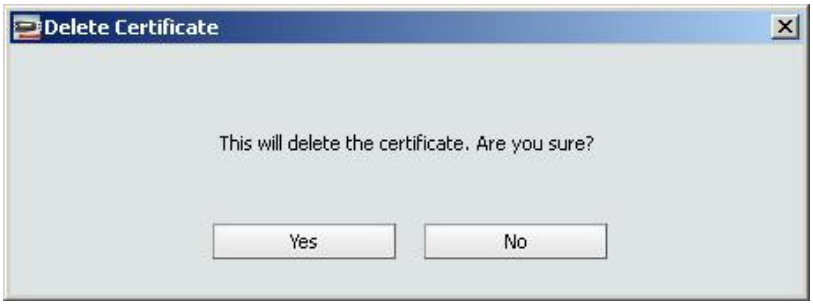
• Clique com o botão direito no nome do certificado no painel esquerdo e selecione a ação apropriada no menu de atalho

Excluindo um certificado

O eToken PKI Client copia certificados do eToken no repositório de registros. Quando o aplicativo é encerrado, os certificados são excluídos do repositório de registros e permanecem no eToken. Com isso, os certificados serão copiados novamente quando o token for inserido da próxima vez, a menos que sejam excluídos do token.

Para excluir um certificado:

1. Selecione **Delete Certificate *(Excluir certificado)***. A caixa de diálogo *Delete Certificate* será aberta.



2. Clique em Yes.

Exportando um certificado

Um eToken físico exporta apenas o certificado, ao passo que um eToken Virtual exporta o certificado com sua respectiva chave.

Para exportar um certificado:

1. Selecione **Export Certificate *(Exportar certificado)***. A caixa de diálogo *Export Certificate* será aberta.

2. Escolha onde o certificado será armazenado e clique em **OK**.

Definindo um certificado como padrão, agente de inscrição ou auxiliar

Você pode definir um certificado como:

• **Default *(Padrão)***

• **Enrollment Agent *(Agente de inscrição)***

• **Auxiliary *(Auxiliar)***

Cada opção será ativada apenas se a ação puder ser realizada nesse certificado ou nessa chave em especial.

A tabela a seguir descreve o uso dessas configurações:

Configuração	Descrição	Situação
Default	O login do Smart Card usa o certificado utilizado no login anterior como padrão. Se o certificado usado no login anterior não for o certificado necessário, defina o certificado necessário como Default.	Seu eToken contém dois certificados. Um é para o login no domínio A e o outro é para o login no domínio B. Seu login anterior foi no domínio A. Portanto, o certificado para o login no domínio A será, agora, o padrão. Caso, agora em outro computador, você efetuar o login no domínio B, o login não será realizado porque você tentou usar o certificado do domínio A. Se, agora, você definir o certificado do domínio B como padrão, o login utilizará o certificado correto e o login será bem-sucedido.
Enrollment Agent	Se o seu token contiver um certificado que permite realizar a inscrição em nome de outros usuários, e se o seu token contiver mais de um certificado, defina o certificado necessário como Enrollment Agent.	O administrador do sistema deseja realizar o login como agente de inscrição no domínio A, onde a conta do usuário está localizada. Como também existe um certificado para o domínio B no eToken, o administrador define o certificado do domínio A como Enrollment Agent, para garantir que ele seja usado como certificado Enrollment Agent padrão.
Auxiliary	Na maioria dos aplicativos da Microsoft, é usado o Login por Smart Card. Entretanto, alguns aplicativos usam a Autenticação no Cliente. A Autenticação no Cliente dá acesso a menos recursos de sistema do que o Login por Smart Card. O PKI Client permite um processo de login para aplicativos, como VPN, com o login de Autenticação no Cliente. Entretanto, se mais de um certificado no token tiver a Autenticação no Cliente como Finalidade Prevista, será necessário definir um como padrão. Isso é feito definindo este certificado como Auxiliary.	Seu eToken contém um certificado previsto para a conexão por VPN, mas existe outro certificado que também possui a Authentication no Cliente como Finalidade Prevista. O certificado para a conexão por VPN deve ser definido como Auxiliary, a fim de garantir que ele seja usado como padrão para o login na VPN.

Para definir um Certificado como Padrão, Agente de Inscrição ou Auxiliar:

1. No modo de exibição Avançado, selecione o certificado necessário.
2. Clique no ícone >> e selecione a configuração necessária (Default, Enrollment Agent ou Auxiliary).
3. Insira a senha do token e clique em **OK**.

Configurações

O nó Settings sob um objeto específico refere-se às configurações exclusivas desse objeto. Há dois tipos de configurações:

• **Password Quality *(Qualidade da senha)***: configura a política de senhas no eToken

• **Other *(Outras)***: configura os parâmetros relacionados às políticas de cache e à autenticação RSA secundária

Qualidade da senha

Assim que os parâmetros de qualidade da senha forem definidos, todas as senhas futuras serão automaticamente comparadas com esses parâmetros para determinar o nível de aceitabilidade da senha.

Se o eToken tiver sido inicializado em versões anteriores do RTE, nenhuma política de senha estará armazenada no token.

Os parâmetros de qualidade de senha são os seguintes:

• **Minimum password length *(Comprimento mínimo da senha)*:** o padrão é 6 caracteres

• **Maximum usage period *(Validade máxima)*:** Em dias; o padrão é 0 = nenhuma

• **Minimum usage period *(Validade mínima)*:** o padrão é 0 dias

• **Password expiry warning period *(Período de aviso de vencimento de senha)*:** define o momento (em dias) a partir do qual uma mensagem de aviso de vencimento da senha; o padrão é 0 = nenhum

• **Password history size *(Período de histórico de senhas)*:** define quantas senhas antigas não podem ser reutilizadas (o padrão é 10)

• **Password must meet complexity requirements *(A senha deve cumprir os requisitos de complexidade)*:** define se caracteres mistos são obrigatórios na senha do eToken; padrão = sim