SUMÁRIO

Sistemas Operacional

Lista de Produtos

SafeNet eToken Pro 72k

SafeNet eToken 5100

SafeNet eToken 5110

Gemalto IDPrime MD 830

Gemalto IDPrime MD 3840

Guia de Prático de Utilização

Descrição das funções do Gerenciador (Botões)

WINDOWS

Plataformas suportadas

SafeNet Cliente de Autenticação 10.2 suporta os seguintes sistemas operacionais:
Windows Vista SP2 (32 bit, 64 bit)
Windows 7 SP1 (32-bit, 64-bit)
Windows 8 (32-bit, 64-bit)
Windows 8.1 (32 bits, 64 bit)
Windows 10 (32 bit, 64 bit)
Windows Server 2008 SP2 (32 bit, 64 bit)
Windows Server 2008 R2 SP1 (64 bit)
Windows Server 2012 (64-bit)
Windows Server 2012 RC1 (64 bit)

Navegadores compatíveis

Firefox 45 e superiores
Internet Explorer 11 e superiores
Chrome Versão 47 e superiores

Tokens suportados

SafeNet Cliente de Autenticação 10.2 suporta os seguintes tokens:
eToken PRO 72k
eToken 5100
eToken 5110

Senha padrão

Dispositivos SafeNet eToken são fornecidos com a seguinte senha padrão Token: 12345. É altamente Recomendável que você altere a senha token após a recepção do tokens.

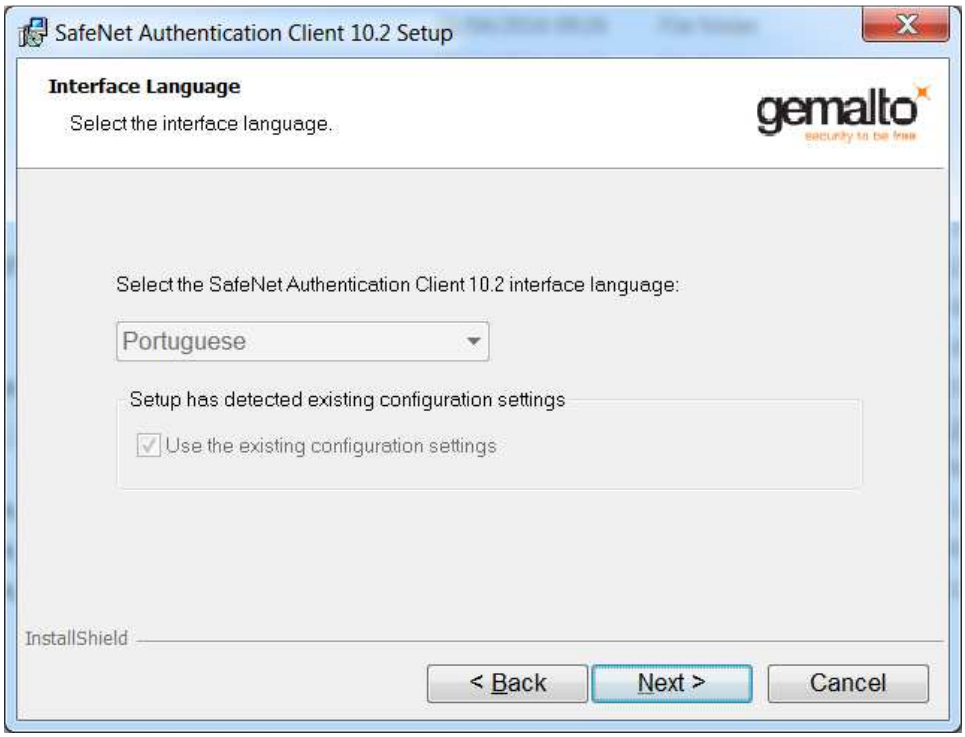
Instalação

Execute o arquivo SAC 10.2 – através do link a seguir:

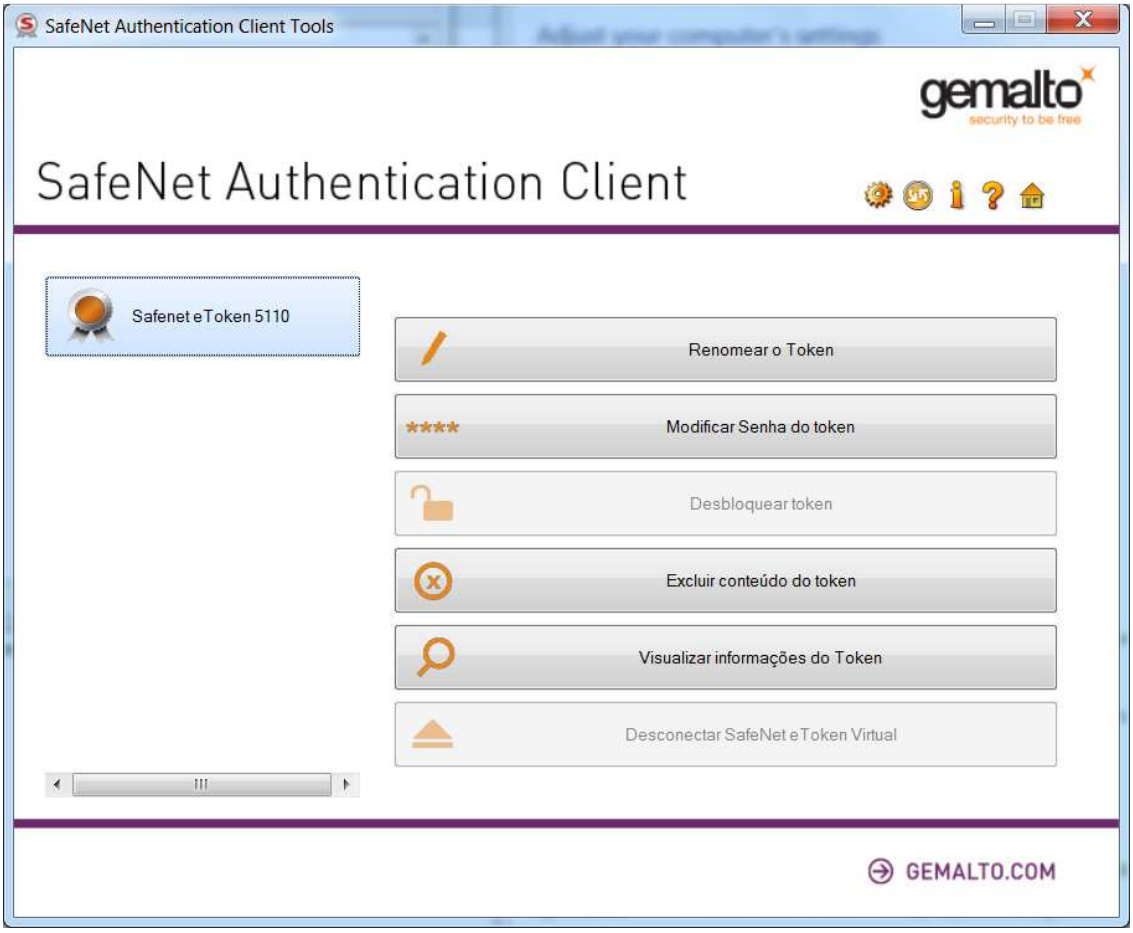
1) http://www.proteq.com.br/download/sac/sac10.2_windows.zip

2) Clique em next para instalação do Software SafeNet Authentication Client e driver do Token;

3) Clique em next em todas as opções padrão para instalar o produto.



4) Visualize seu token conectado do lado esquerdo “SafeNet eToken 5110”, pronto para ser utilizado;



LINUX

Plataformas suportadas

SafeNet Autenticação de cliente (Linux) 9.1 suporta o seguinte:

Sistemas operativos:

Red Hat Enterprise 6.6 (32 bits e 64 bits) em kernel 3.2

CentOS 6.6 (32 bits e 64 bits) em kernel 3.2

SUSE Linux Enterprise 11.3 (32 bits e 64 bits) em kernel 3.2

Fedora 20 (32 bits e 64 bits)

Ubuntu 13.04 ao 15.10 (32 bits e 64 bits) em kernel 3.2

Navegadores compatíveis

Firefox 41
Chorme 47

Tokens suportados

SafeNet Cliente de Autenticação 9.1 suporta os seguintes tokens:
eToken Pro 72k
eToken 5100
eToken 5110

Senha padrão

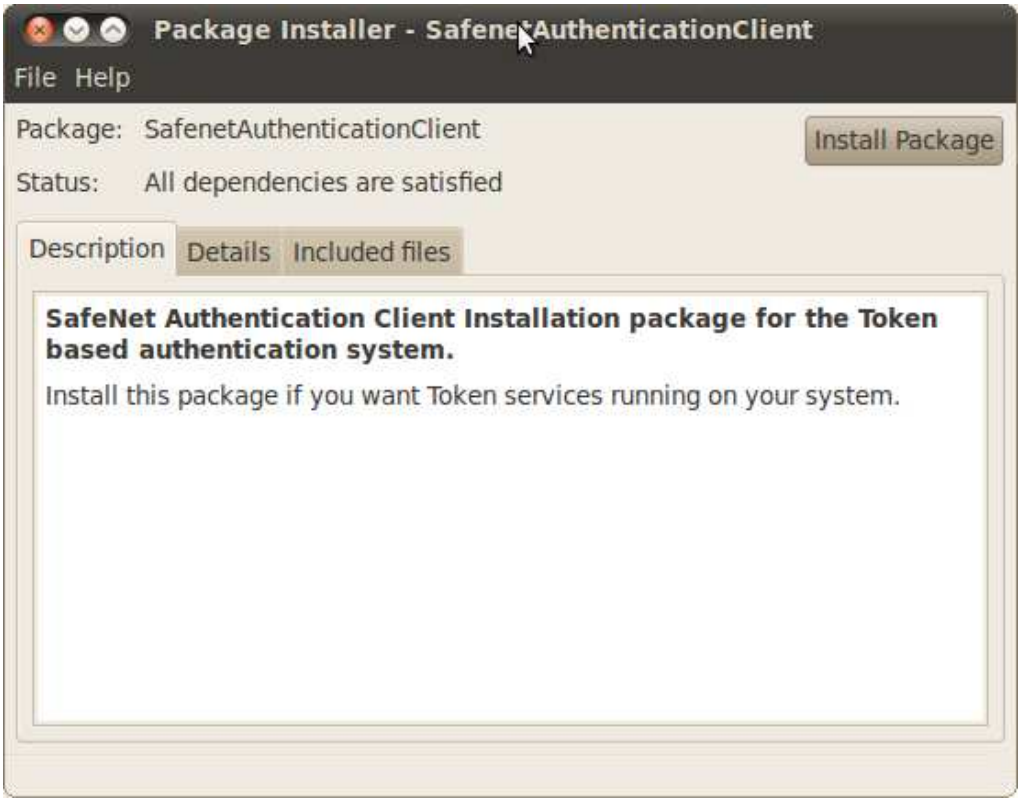
Dispositivos SafeNet eToken são fornecidos com a seguinte senha padrão Token: 1234. É altamente recomendável que você altere a senha token após a recepção do tokens.

Instalação

1) Execute o arquivo SAC 9.1 – através do link a seguir

Linux - http://www.proteq.com.br/download/sac/sac9.1_linux.zip

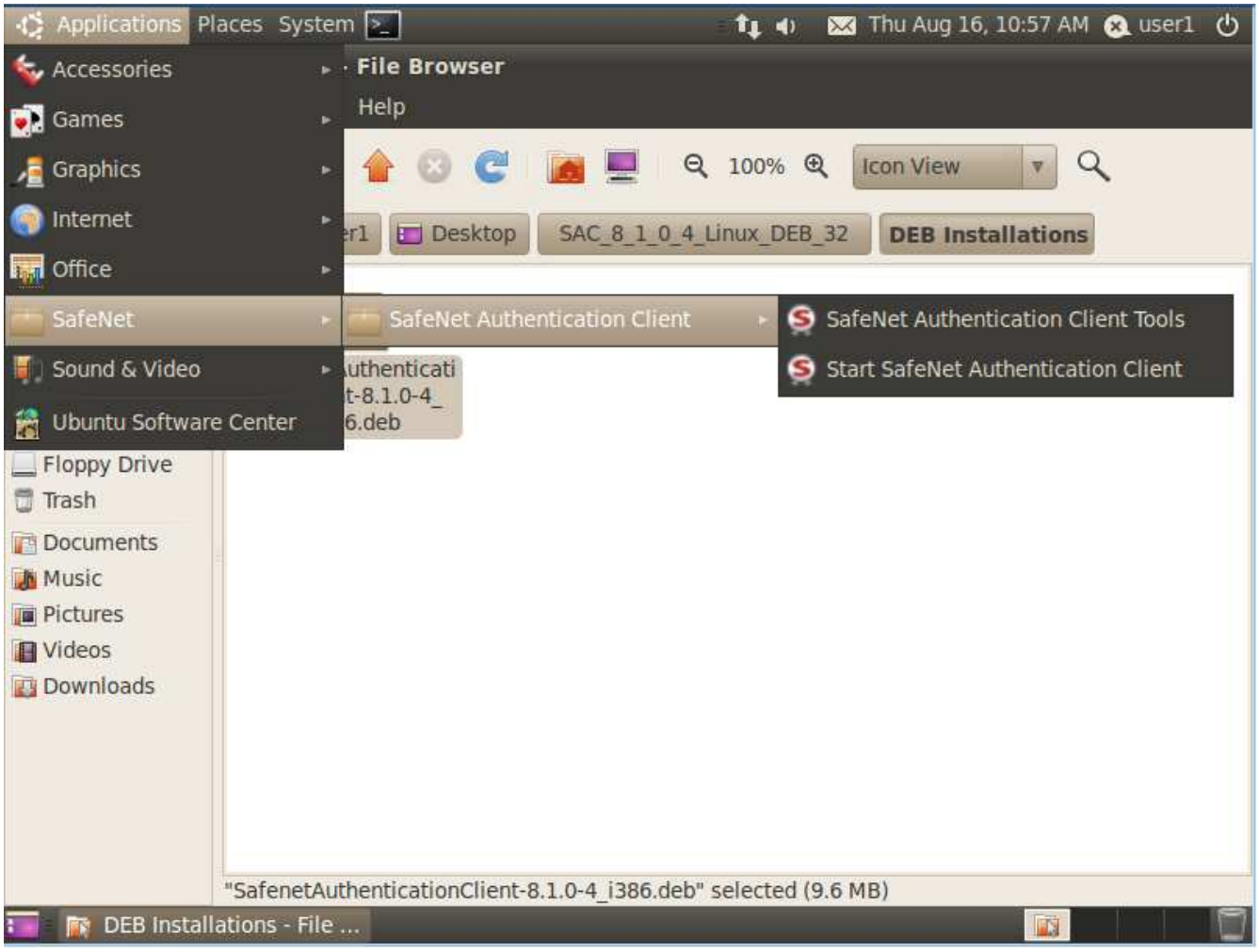
2) Clique em Install Package para instalação do Software SafeNet Authentication Client e driver do Token;



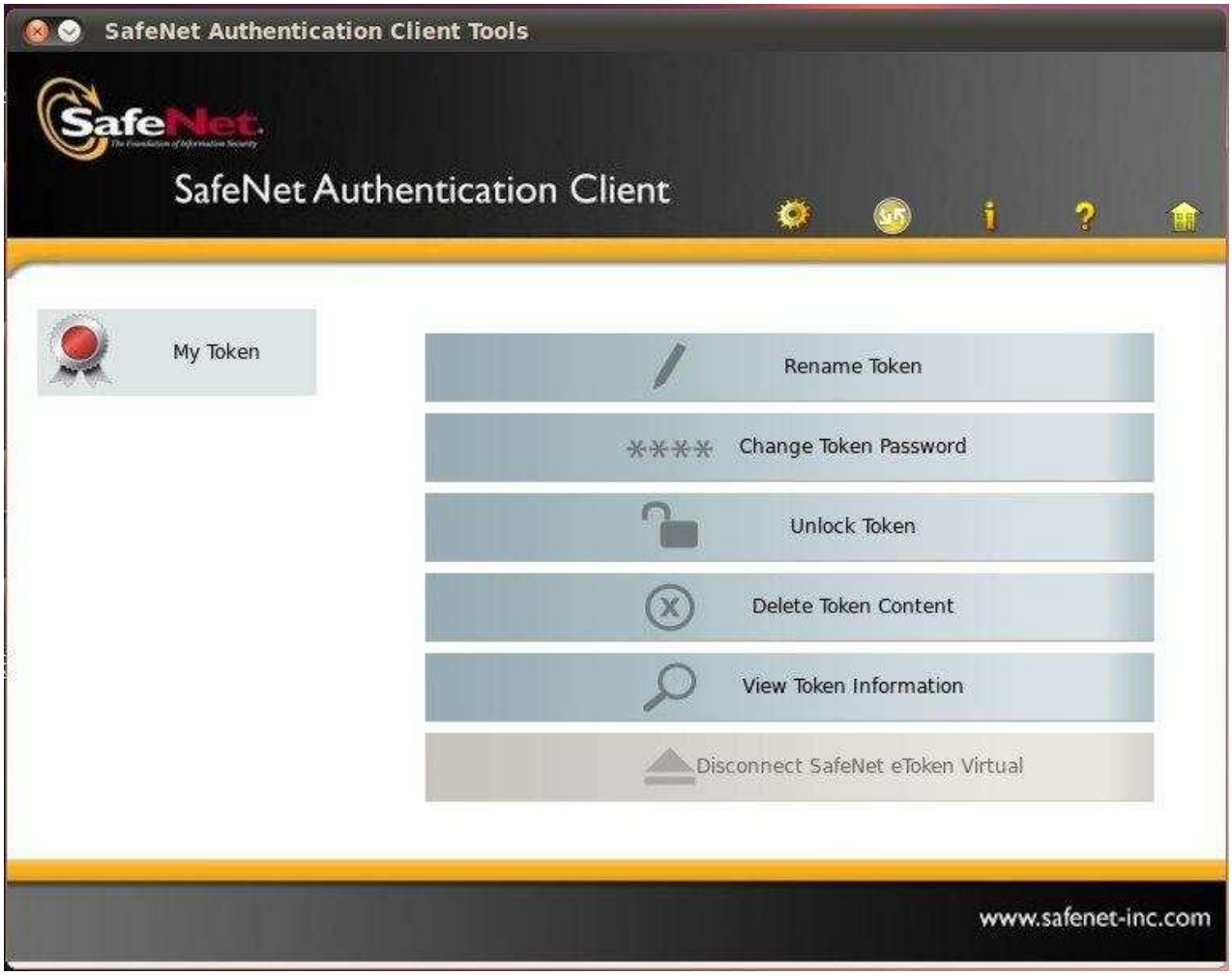
3) Aguarda até que a instalação seja concluída.

4) Instalação concluída click em (close) em seguida reinicie seu computador;

5) Após reiniciar seu computador clique em aplicativos e abra o SafeNet Authentication Client Tools em seguida conecte seu token;



6) Visualize seu token conectado do lado esquerdo “My Token”, pronto para ser utilizado;



MAC OS X

Plataformas suportadas

SafeNet Autenticação de Cliente (Mac) 10.0 suporta o seguinte:

Sistemas operativos:

Mac OS X 10.11 (El Capitan)

Mac OS X 10.12 (Sierra)

Navegadores compatíveis

Firefox

Safari

Chrome

Tokens suportados

SafeNet Cliente de Autenticação 10.0 suporta os seguintes tokens:

eToken Pro 72k

eToken 5100

eToken 5110

Senha padrão

Dispositivos SafeNet eToken são fornecidos com a seguinte senha padrão Token: 1234. É altamente recomendável que você altere a senha token após a recepção do tokens.

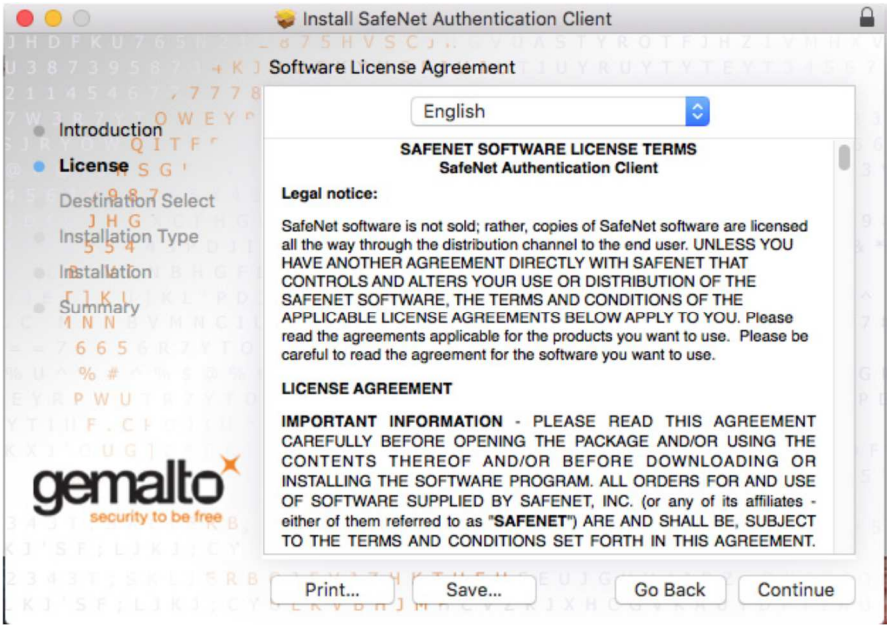
Instalação

1) Execute o arquivo SAC 10.0 – através do link a seguir

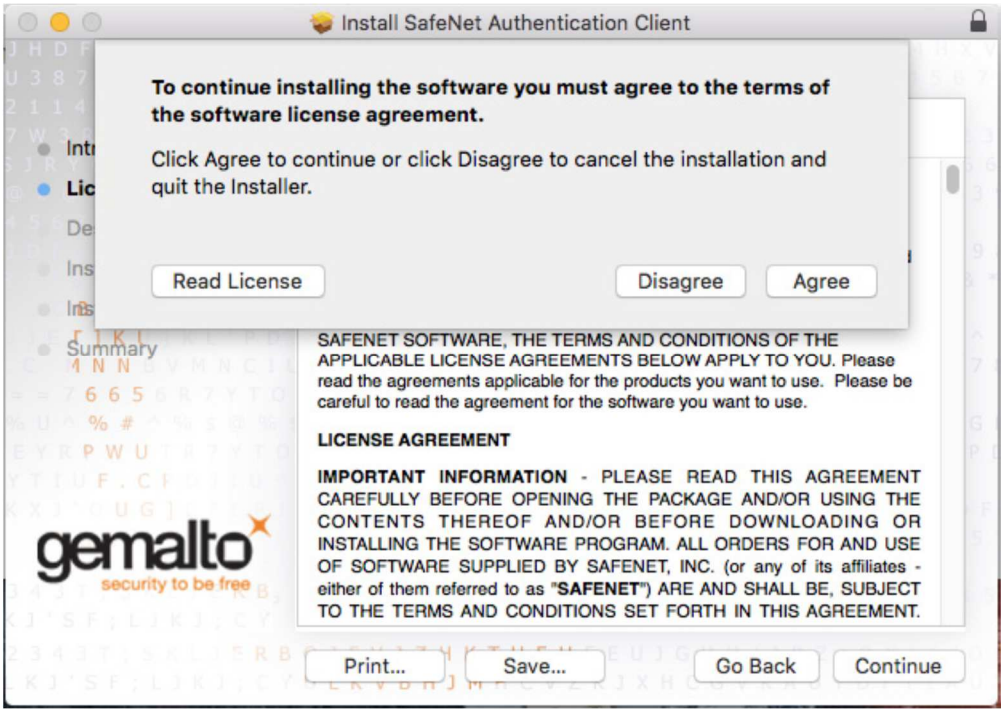
Mac - http://proteq.com.br/download/sac/Sac10.0_mac.zip

2) Duplo clique SafeNet Authentication Client 10.0;

Clique em Continue

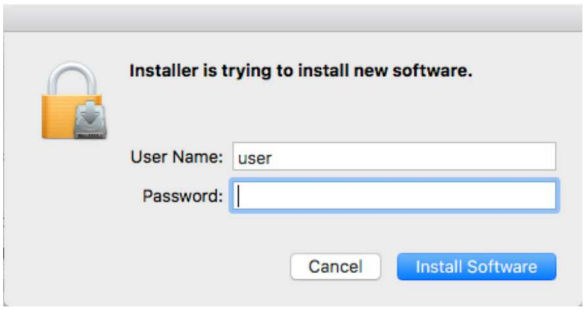


Clique em Continue

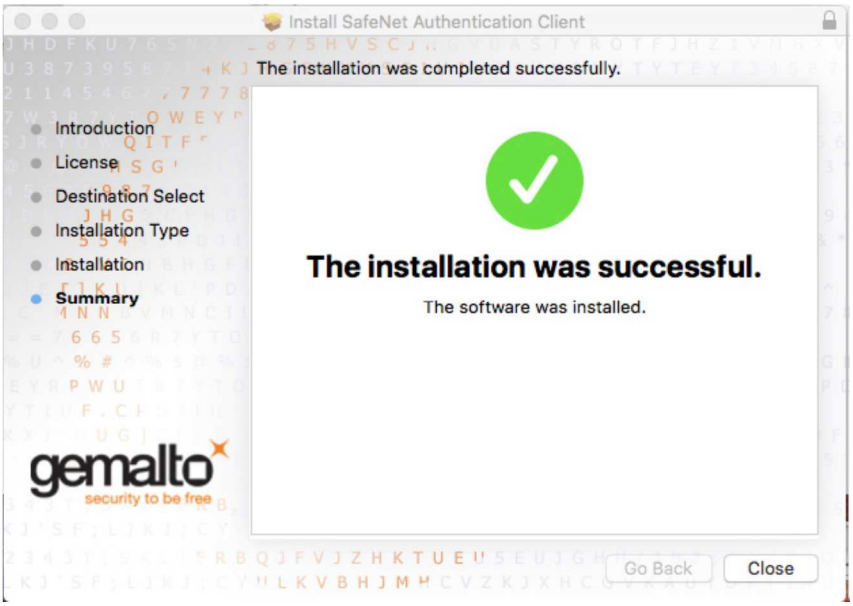


Clique Agree

Clique Install

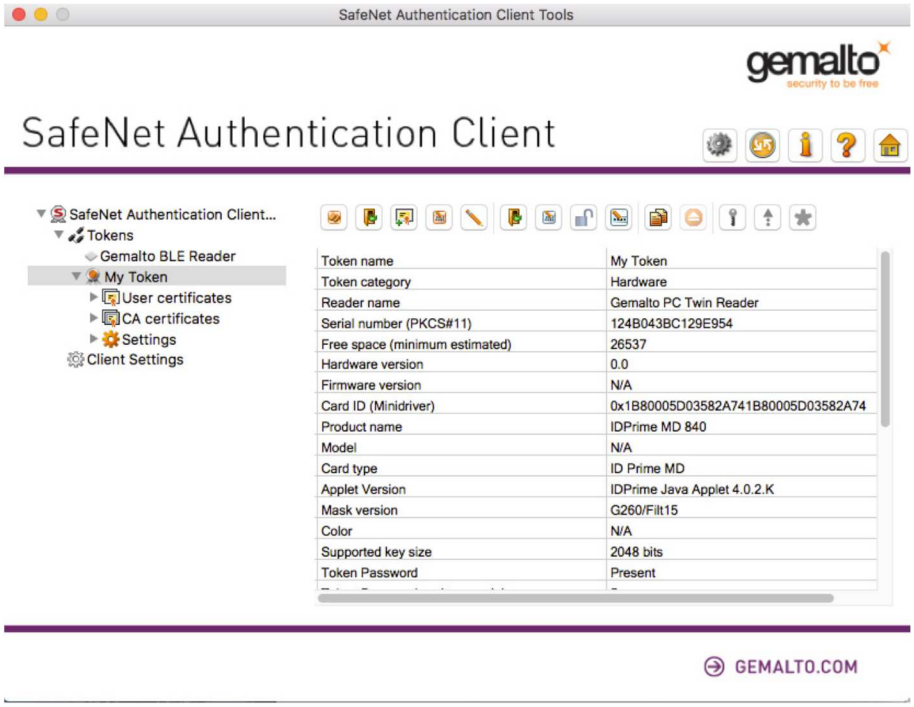


Entre com o nome de usuário e senha para instalação.

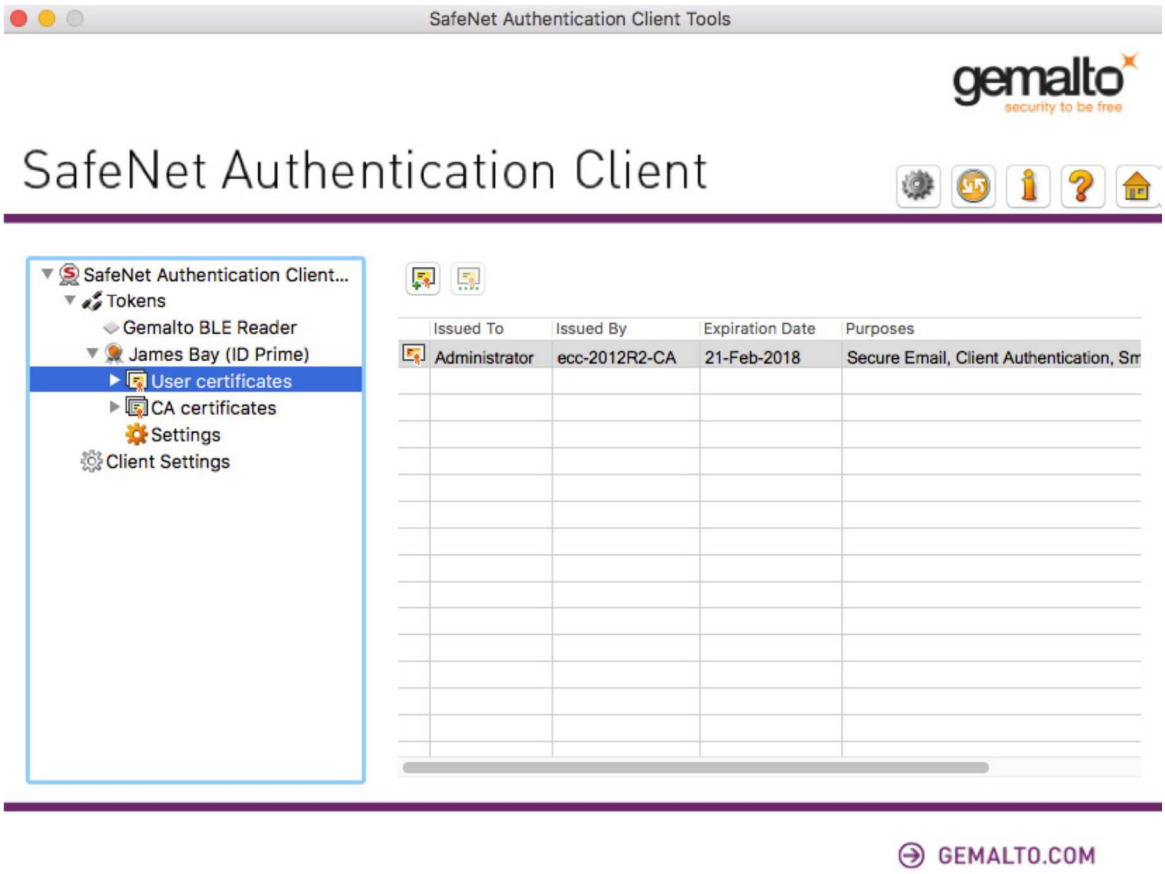


Clique em Close

Vista avançada



Certificado do Usuário, pronto para ser utilizado.

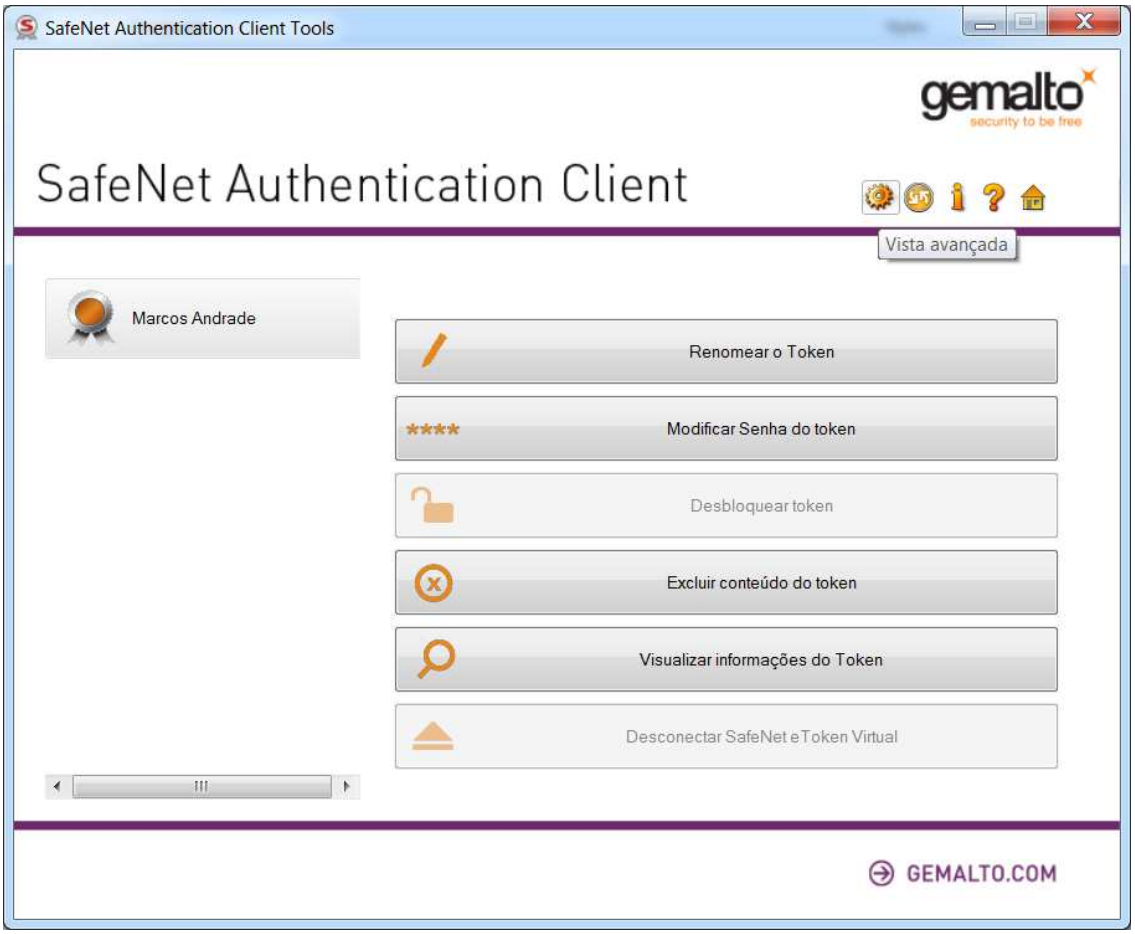


Guia de Prático de Utilização

1) Conecte o seu token na porta USB;

2) Abra o gerenciador do token através de Iniciar > Todos os Programas > SafeNet > Safenet Autentication Client Tools;

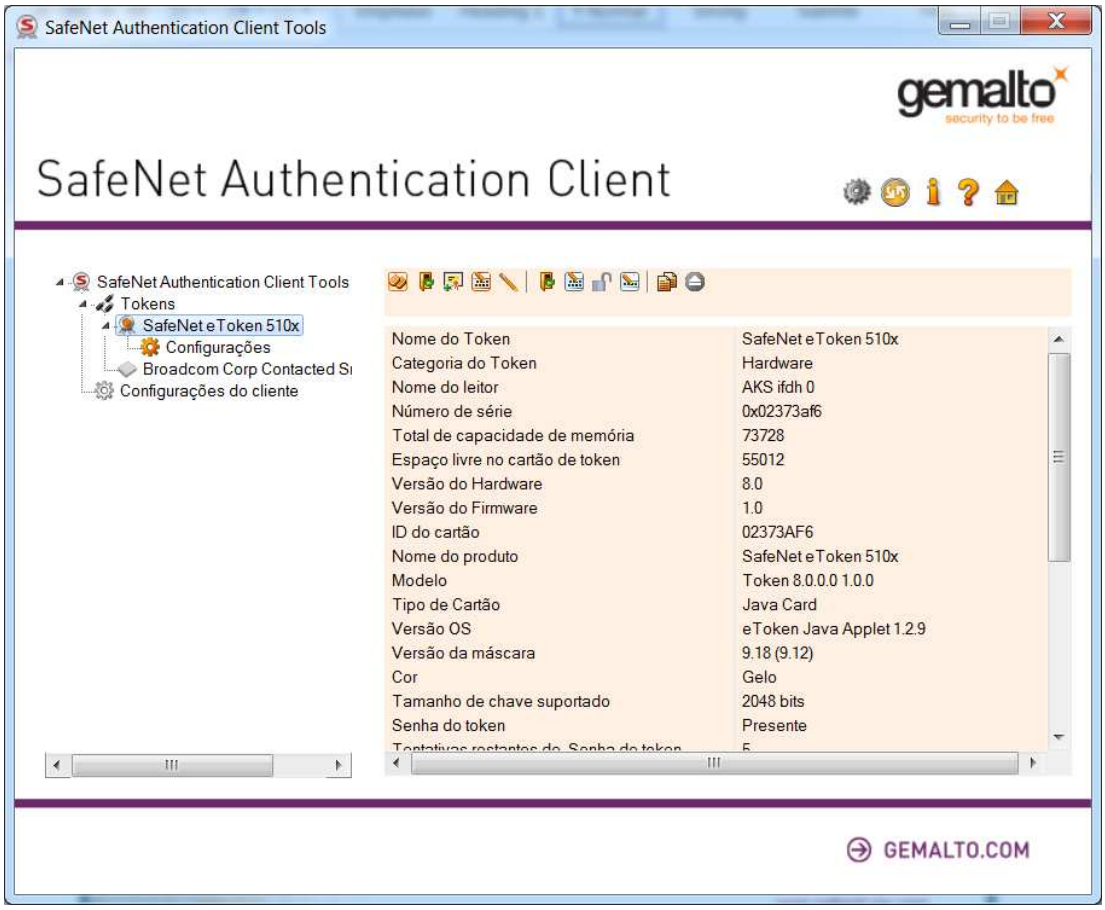
3) Clique em Vista avançada conforme imagem abaixo;



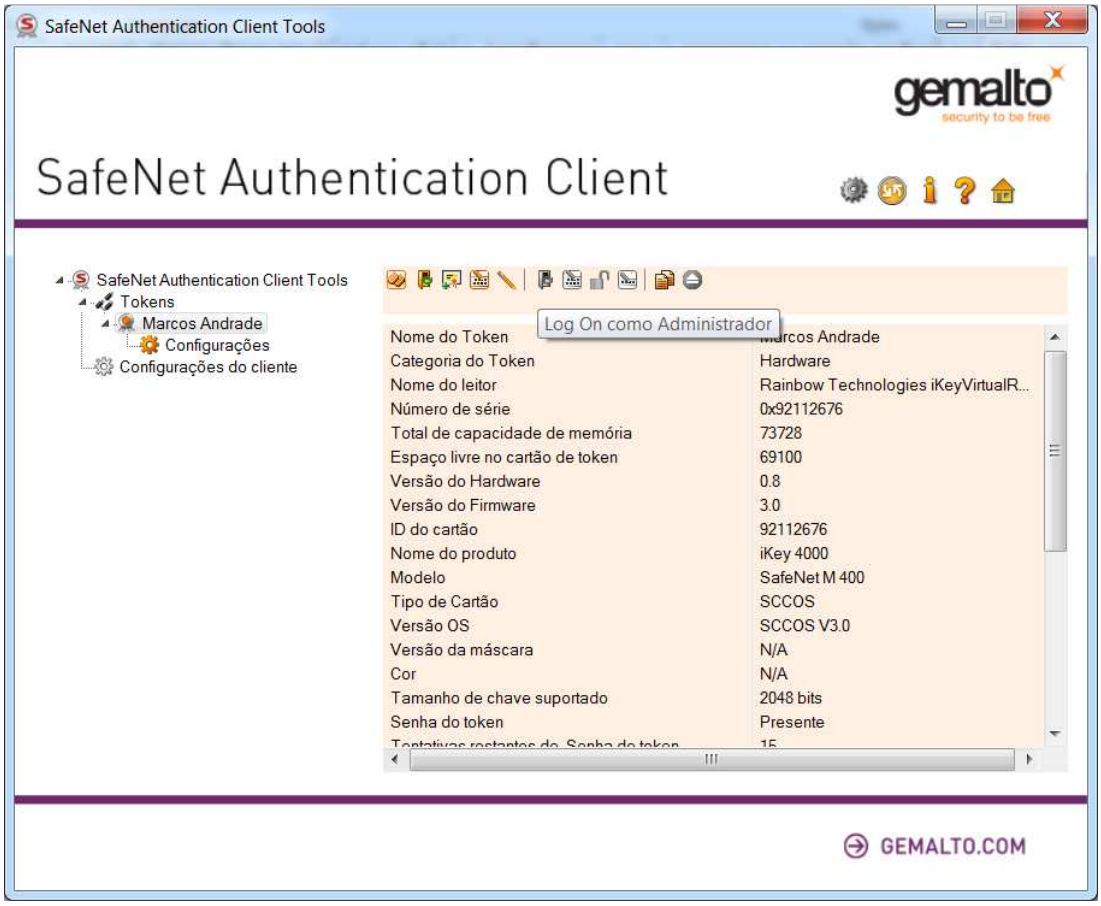
4) Clique em Log On no My Token Digite o PIN de seu eToken:

-caso a senha de fábrica ainda não tenha sido alterada, o PIN inicial é **12345**;

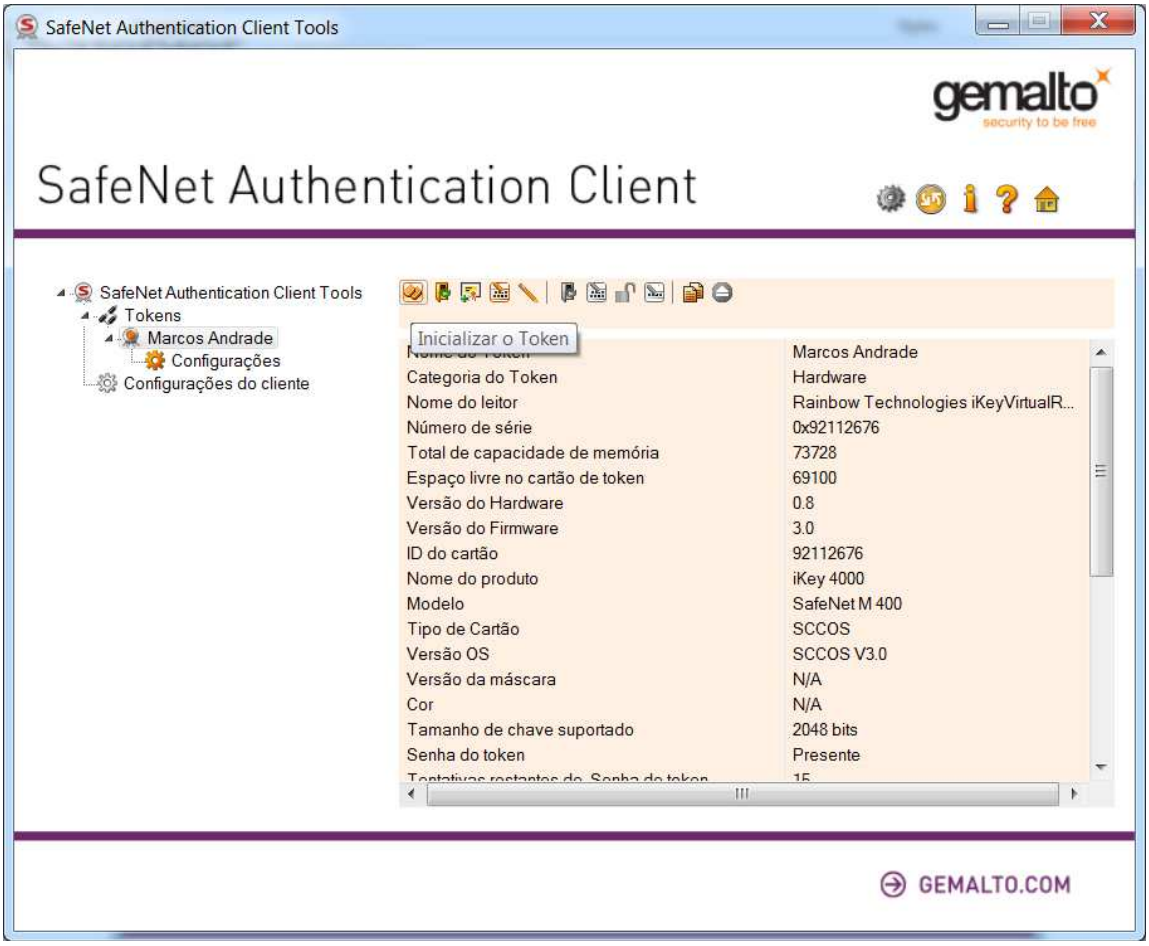
-cuidado para não digitar o PIN incorreto por 5 vezes para não bloquear o seu eToken;



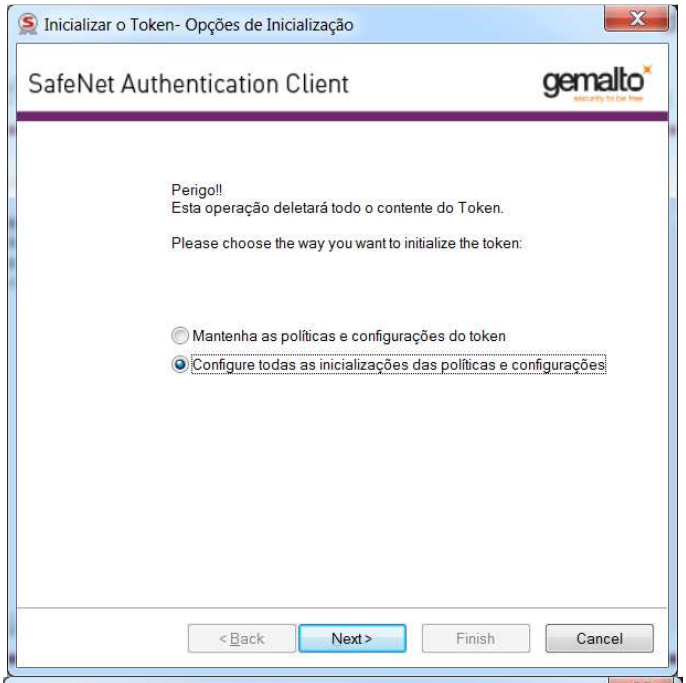
5) Caso queira habilitar as opções não disponíveis como padrão, como senha administrador (PUK) conforme imagem abaixo clique em inicializar eToken. **Lembramos que o processo a seguir poderá ser feito por usuários que ainda não possuem um certificado digital armazenado no eToken, se você já possui um certificado desconsidere esse processo**.

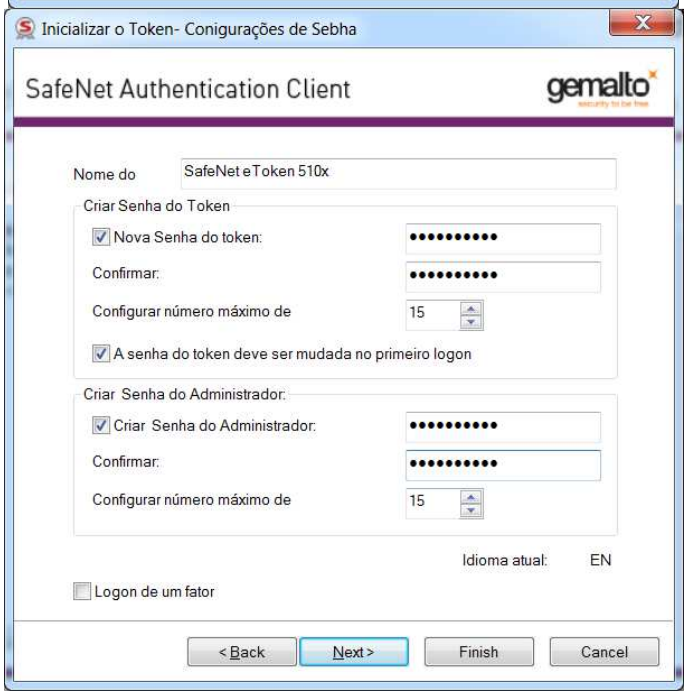


6) Para ativar a opção de Administrador será necessário inicializar o token selecione “Criar Senha do Administrador”;

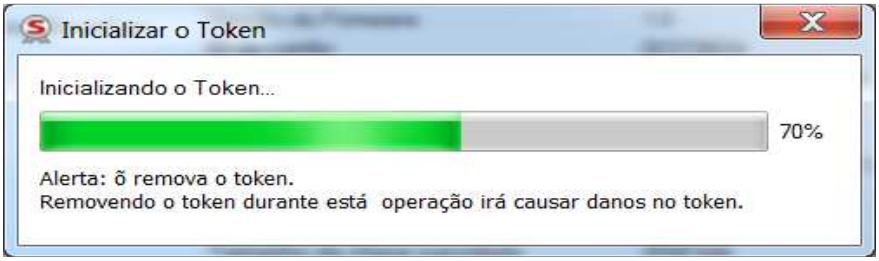


7) Nesse passo você pode renomear seu token substituindo o nome “My Token” pelo nome do e-CPF ou e-CNPJ. Cadastre a senha forte do token (PIN) e habilite a senha forte Administrador (PUK), a senha administrador(PUK) é definitiva e não será alterada ao menos que o usuário deseje troca-la. Desmarque a opção “A Senha do token deve ser mudada no primeiro logon” em seguida clique em iniciar;

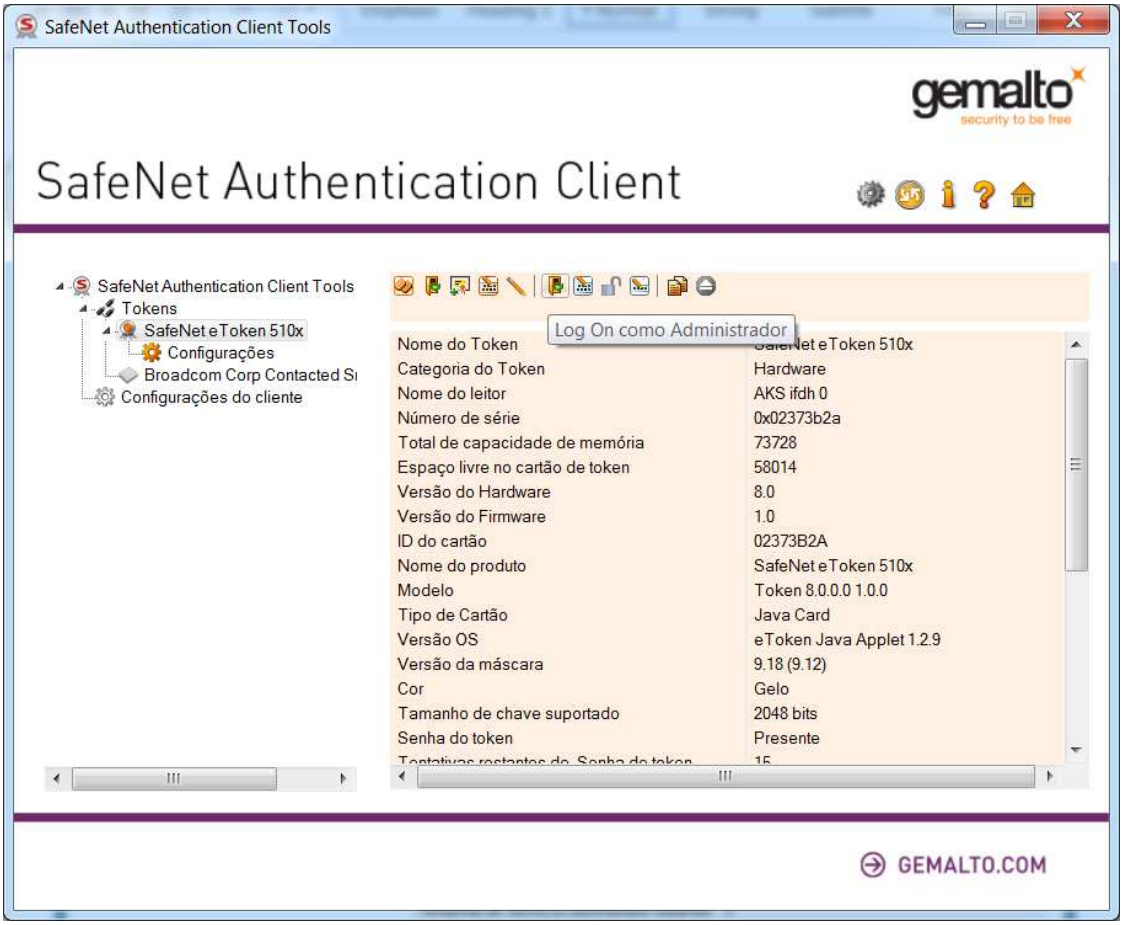




Atenção, esta operação irá excluir todo o conteúdo do eToken clique em OK caso tenha certeza de que não há nenhum certificado armazenado em seu eToken.

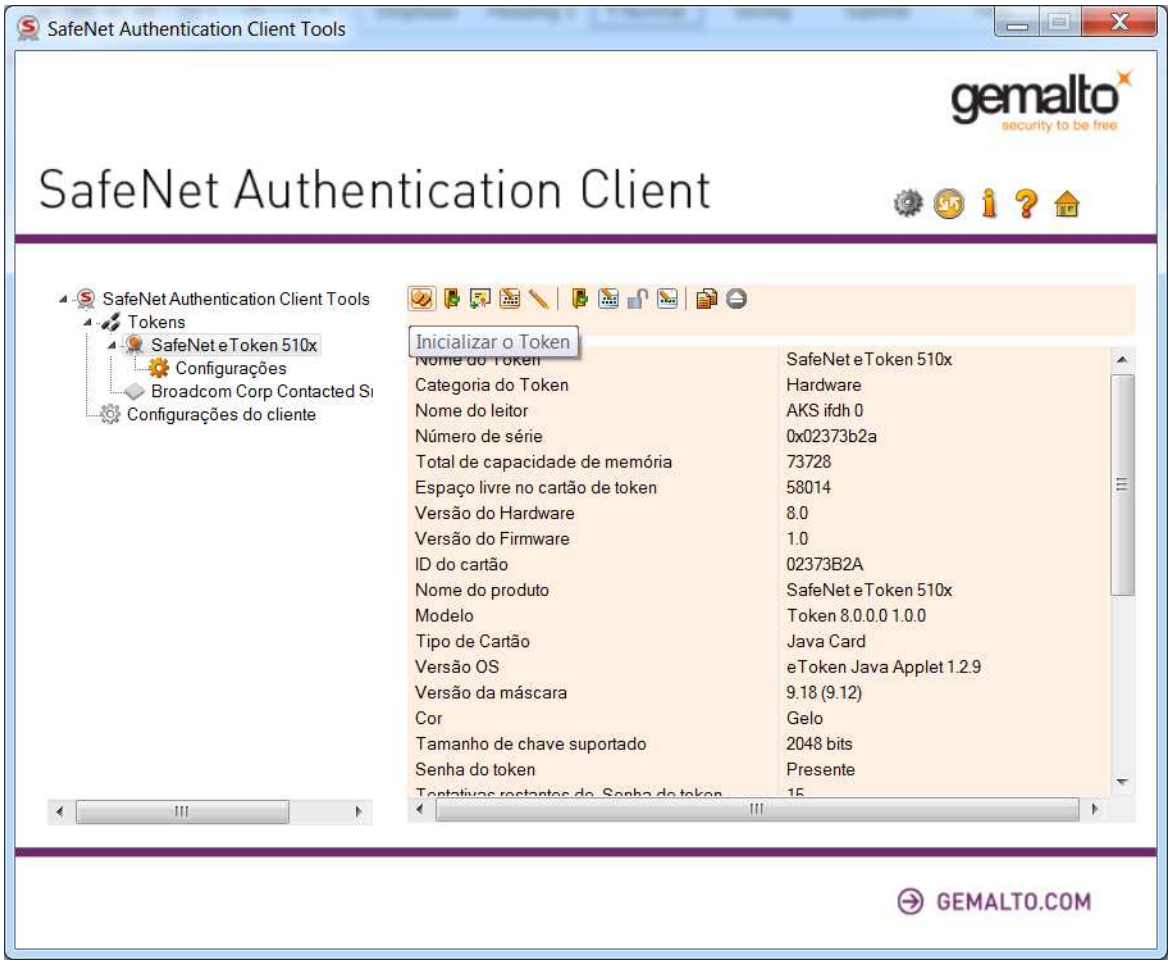


8) Conforme imagem abaixo seu eToken esta inicializado e pronto para ser utilizado e a opção Administrador (PUK) está habilitada possibilitando o desbloqueio da senha do usuário através do Administrador sem precisar inicializá-lo;

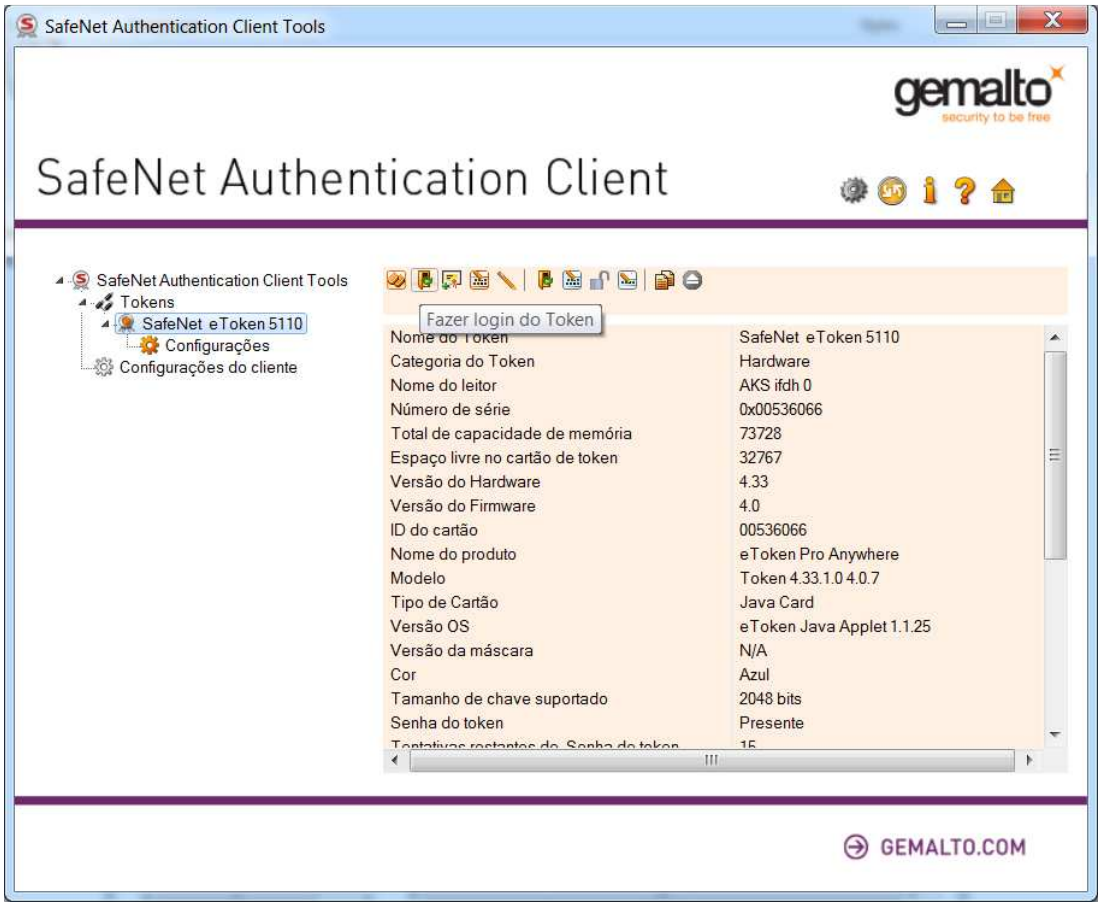


Descrição das funções do Gerenciador (Botões)

Inicilizar eToken – Formata e inicializa o eToken apagando todo o conteúdo de sua memória deixando-o como o padrão de fábrica e após esse processo o PIN volta a ser “12345”, é possivel habilitar a função Administrador (**ATENÇÃO**), não o faça se já tiver importado o certificado para o eToken.

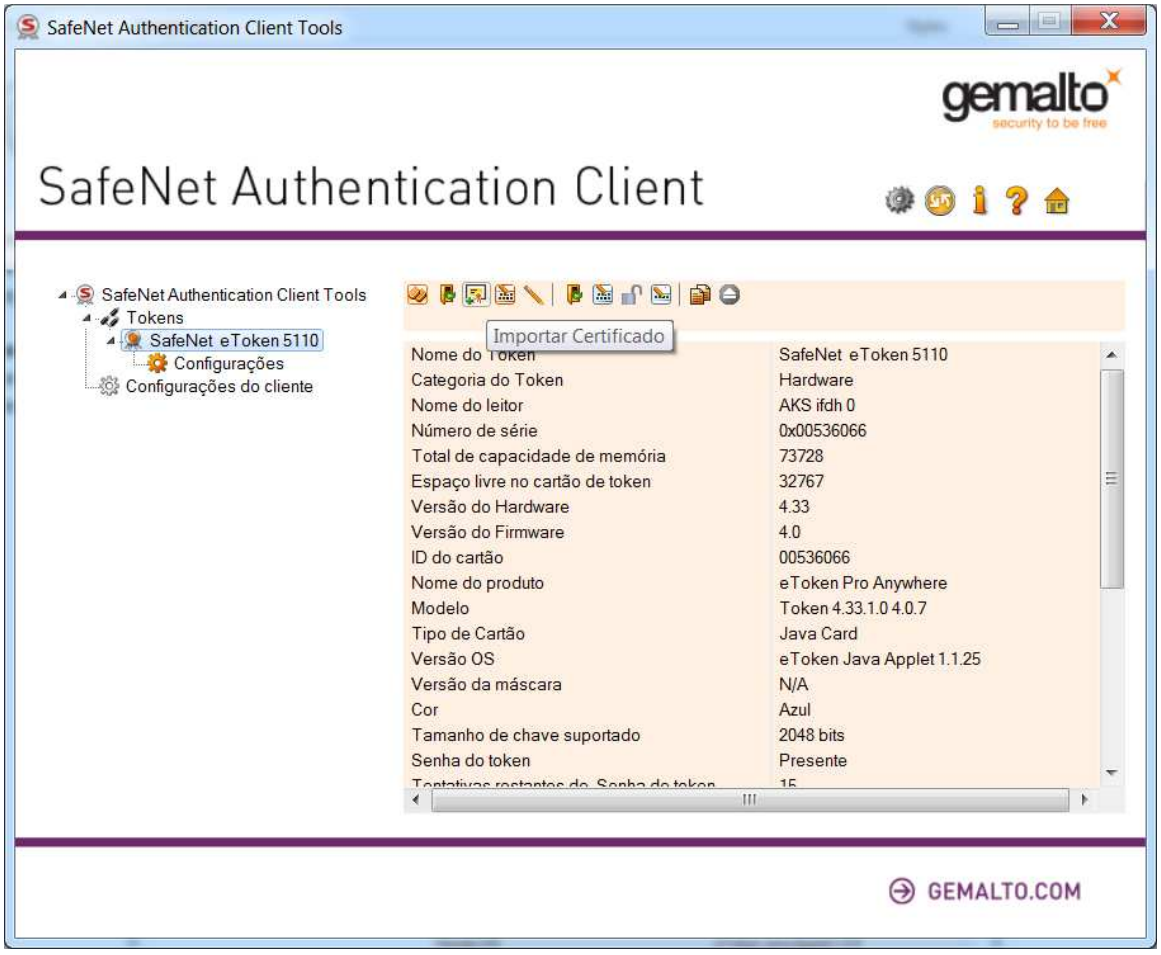


Realizar Logon no eToken – Configura e faz o login no eToken para habilitar as outras funções e também pode ser usado para trocar o PIN/Senha de acesso ao eToken;

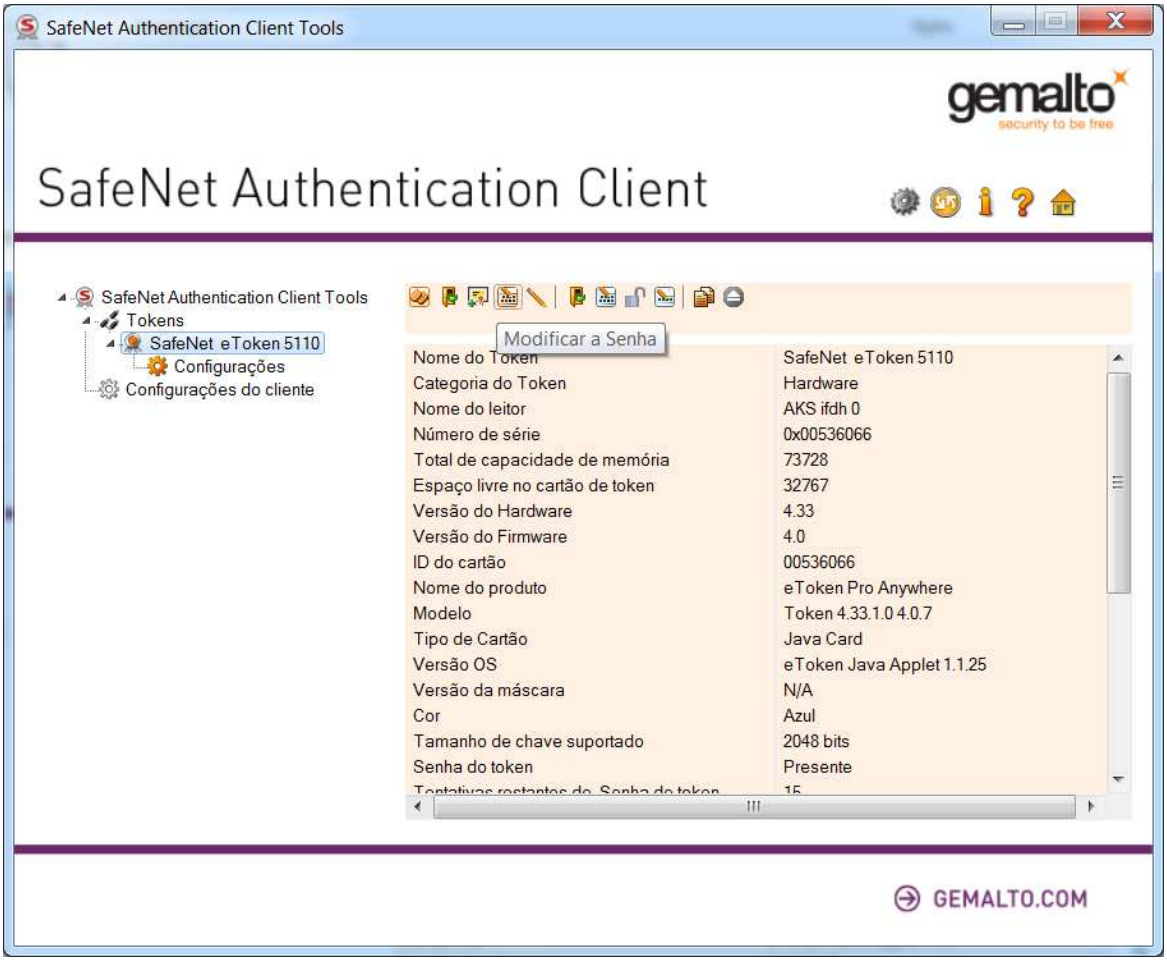


Importar Certificados – importa certificados com extensão .**cer,** é usado para importar a cadeia de certificados para dentro do eToken, este recurso é importante para trazer portabilidade a cadeia, que existe para que seu certificado seja reconhecido e autorizado a funcionar no Windows;

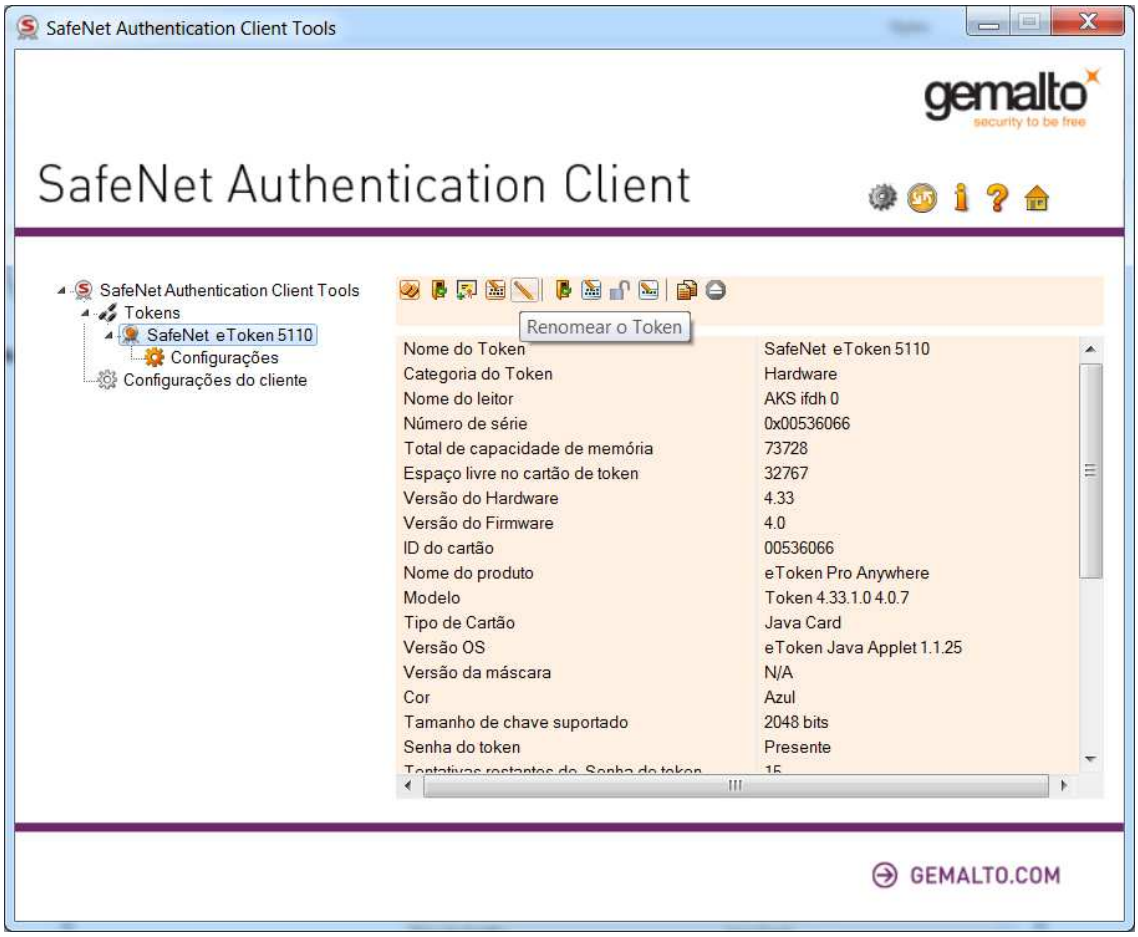
Importar Certificados – importa certificados com extensão **pfx** ou **p12**, este recurso é usado para importar certificados e suas chaves geradas em software para dentro do eToken, para isso você deve preencher o nome que deseja dar ao certificado dentro do dispositivo e a senha usada para criptografar o .pfx / .p12.;



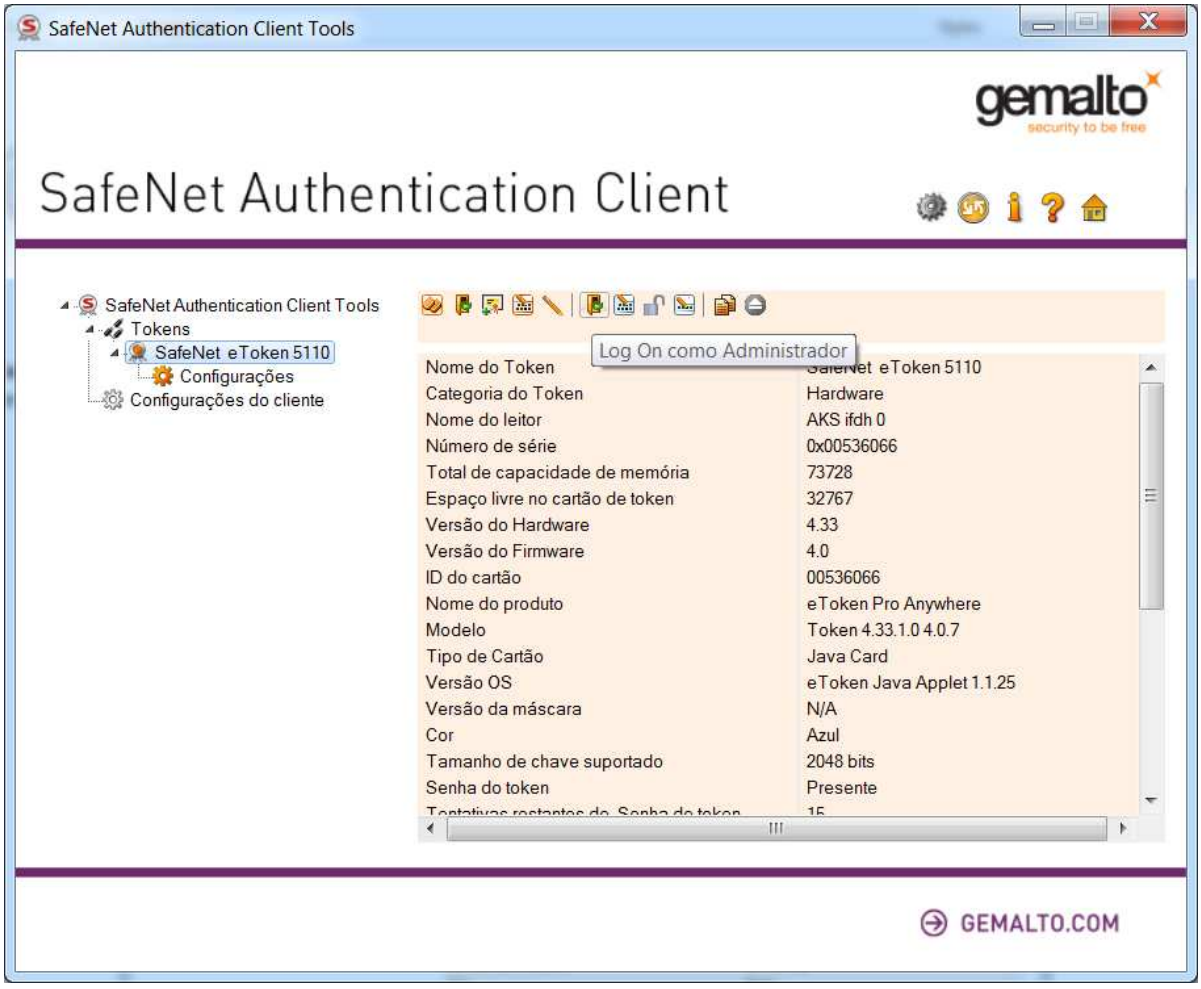
Modificar Senha – Possibilita a alteração da senha do usuário sem excluir o certificado;



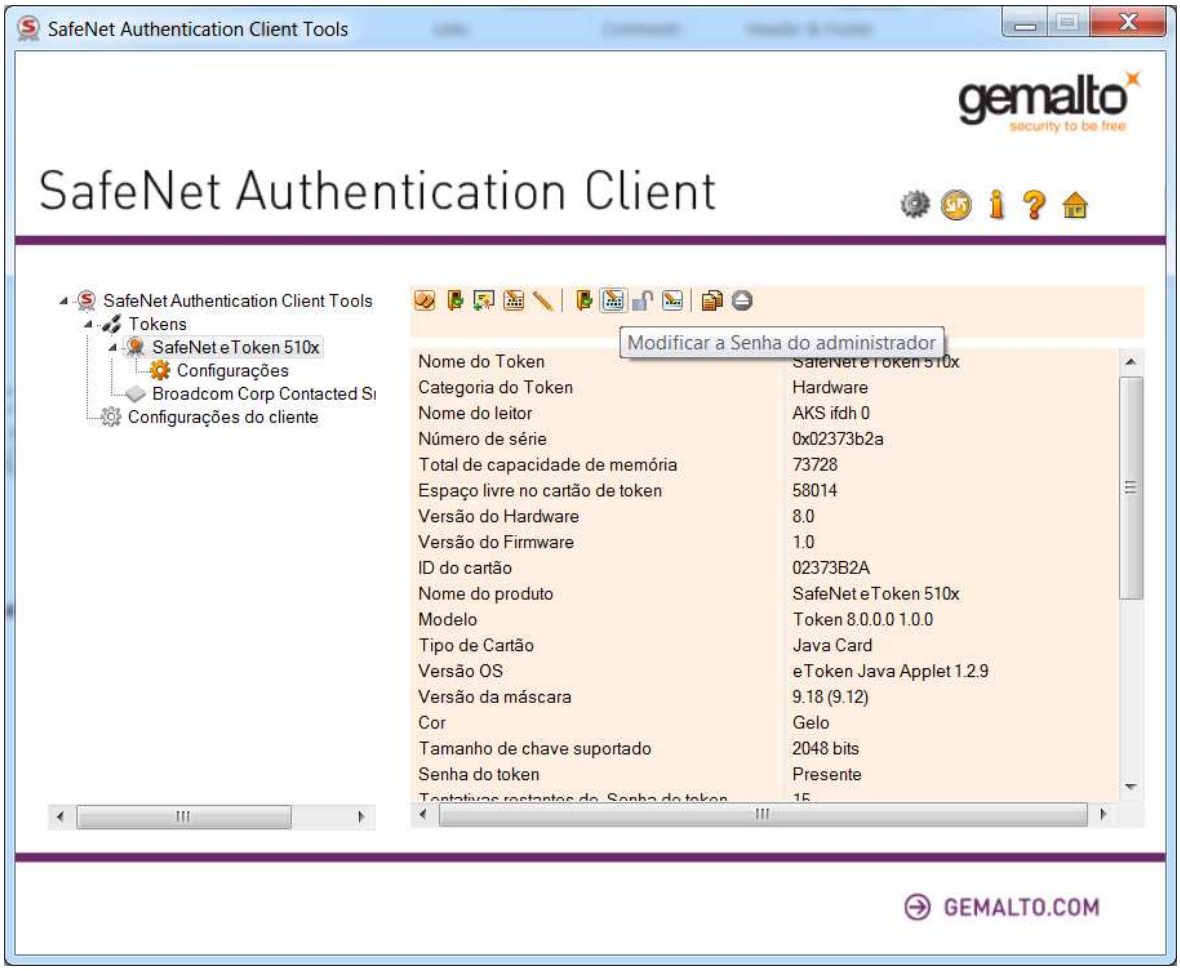
Modificar o nome do eToken – modifica o nome usado para identificação do proprietário do eToken;



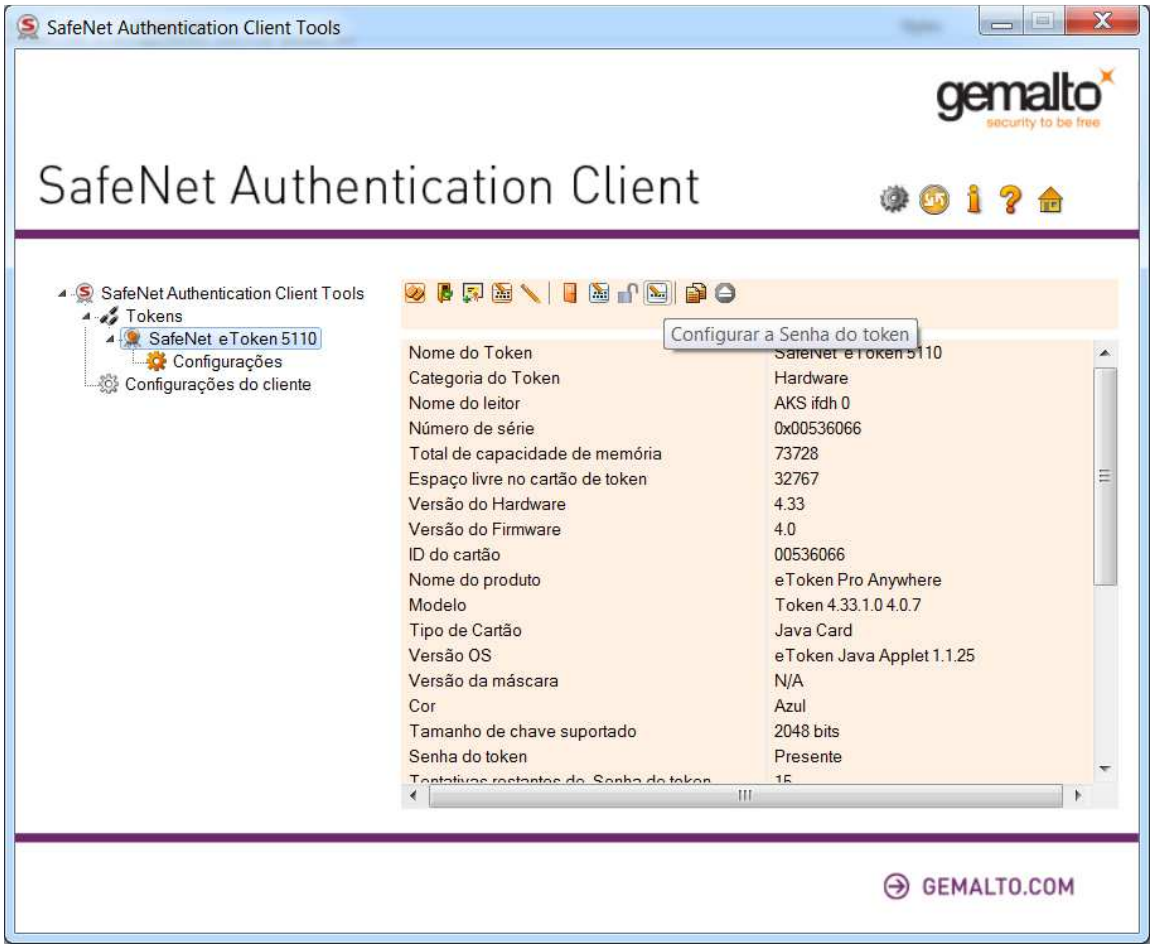
Fazer Logon como Administrador – Configura e faz o login no eToken habilita todas ass funções e também pode ser usado para trocar a Senha de acesso e/ou desbloquear senha do usuário do eToken;



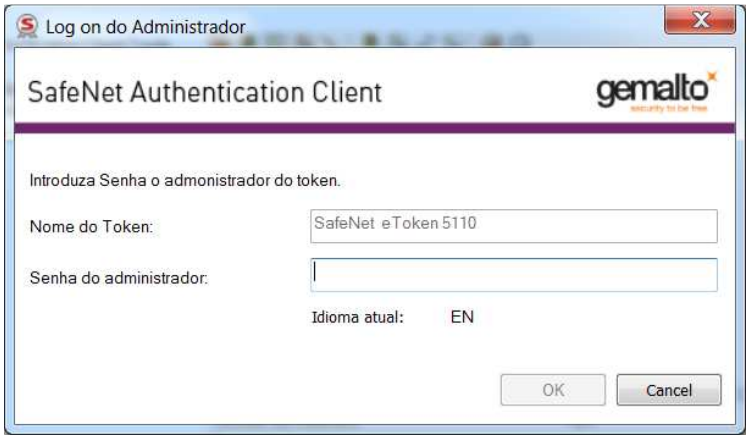
Modificar senha do Administrador – Possibilita a alteração da senha Administrador sem excluir o certificado;



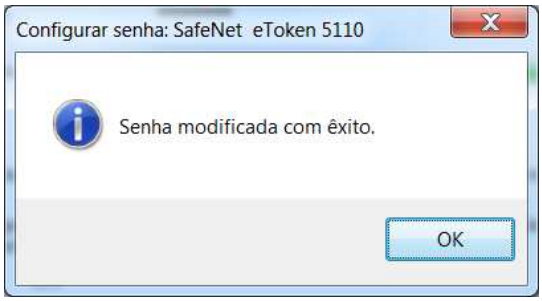
Configurar Senha do Usuário – cadastra a nova senha do usuário no caso usuário tenha excedido o número de tentativas e bloqueado senha usuário.



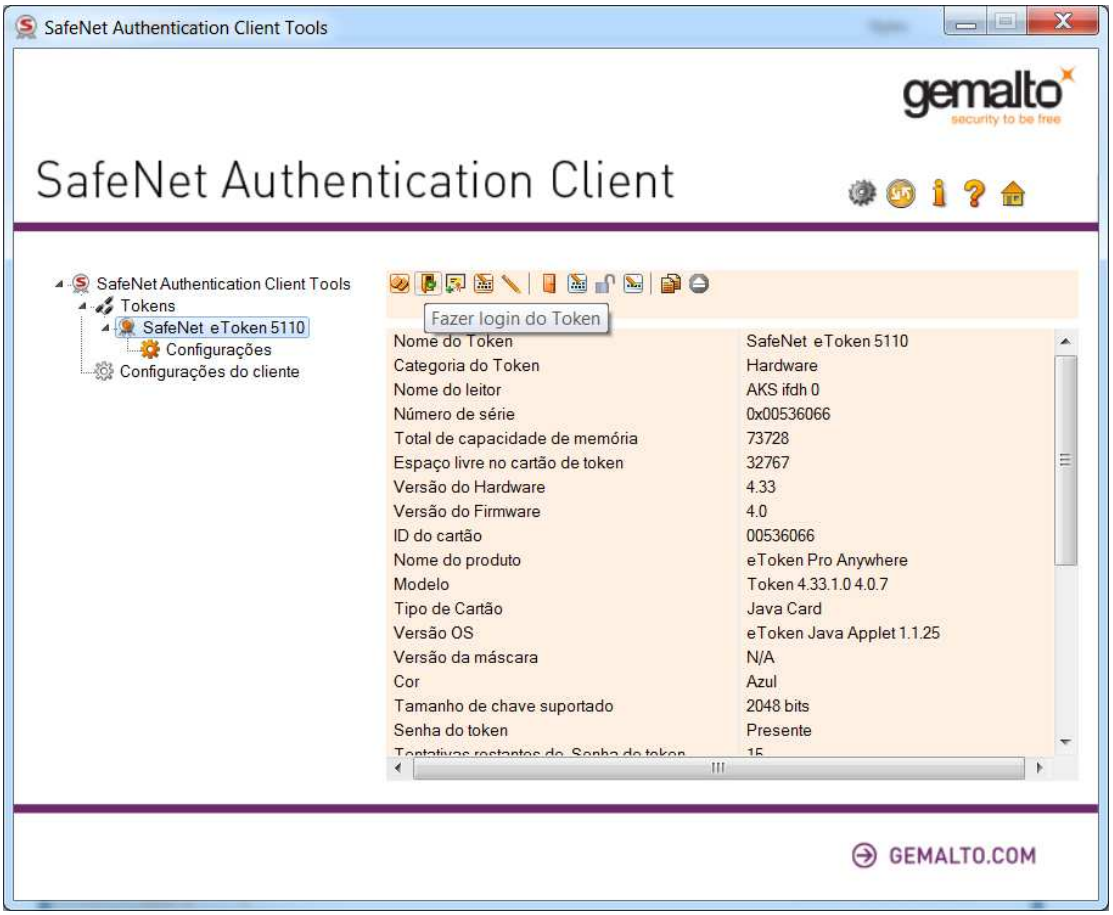
Entre com a senha administrador;

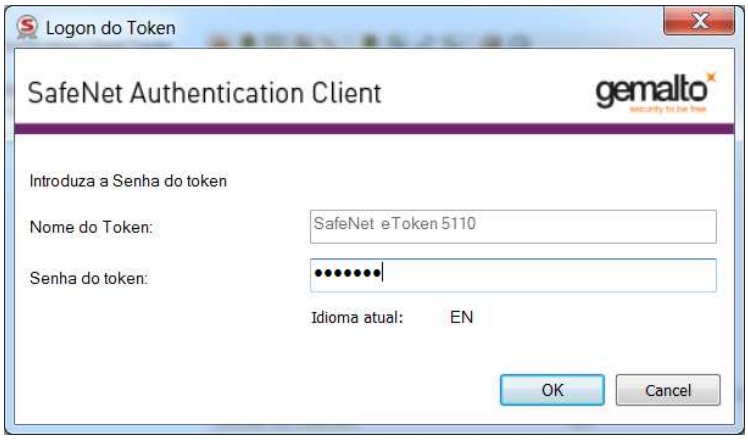


Cadastre a nova senha para o usuário;

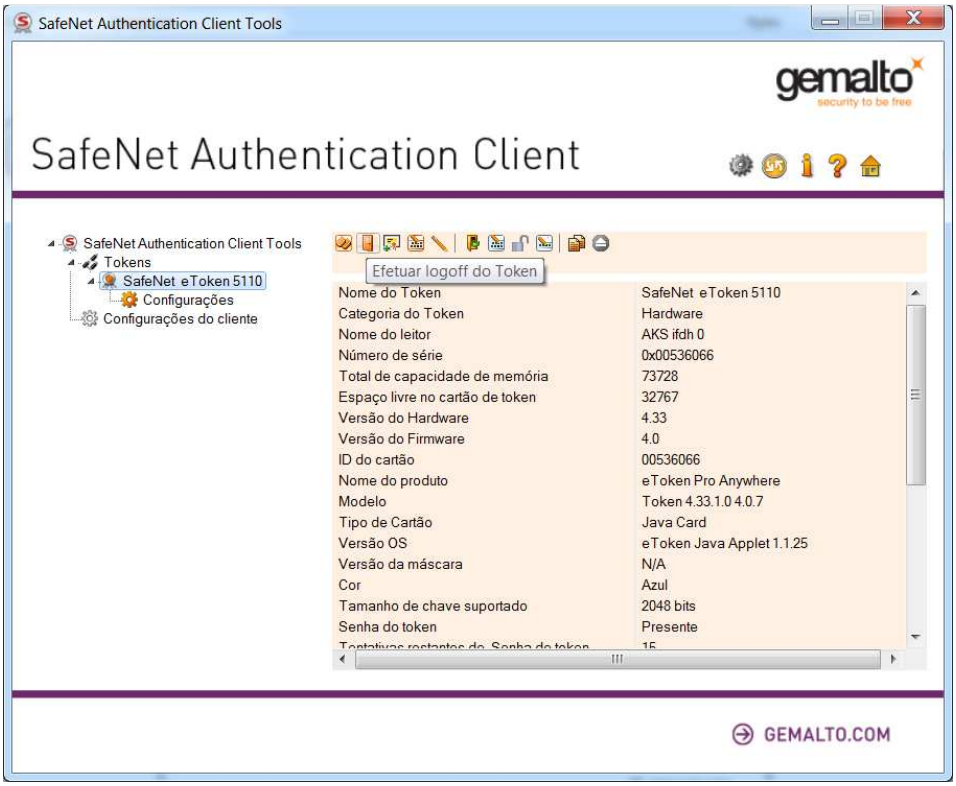


Para testar a nova senha de usuário faça o logon como usuário;





O mesmo icone após o logon feito com sucesso indicará Efetuar logoff do token;



FIM DO DOCUMENTO