

ISCTE-IUL

SIIC - URCS

Manual VPN

(Junho/2015)

“Renovação de Certificados”

Índice

Conteúdo

Versão do Manual	2
Sistemas Operativos Testados.....	2
Material necessário	2
Renovação de Certificados	3
Contactos.....	12

Versão do Manual

Versão	Autor	Data	Observações
1.0	SIIC-URCS	17/06/2015	

Sistemas Operativos Testados

- Sistema Operativo:
 - ✓ Windows XP
 - ✓ Windows 7 (32/64 bits)
 - ✓ Windows 8 / 8.1 (32/64 bits)
 - ✓ Windows 10 (32/64 bits)

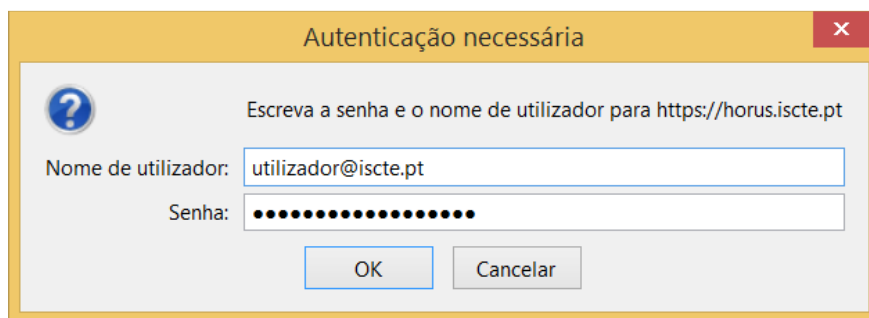
- Browser:
 - ✓ Firefox (desde a versão 4.0)

Material necessário

- Cisco VPN Client “5.0.07.0290-k9” 32/64 bits (instalado)
- Firefox (4.0 ou versões superiores)
- Utilizador do ISCTE-IUL com a sua respetiva Palavra-Passe

Renovação de Certificados

1. Abra o seu navegador **Firefox** e aceda a <http://certsrv.iscte.pt>.
Na caixa de diálogo "**Autenticação necessária**" introduza as suas credenciais de acesso e pressione o botão "**OK**" (as mesmas credenciais de acesso ao Fénix)



2. Surge a página de entrada da autoridade de certificação do ISCTE – ISCTECA. Em "**Select a task**",
Aceda a "**Request a certificate**":

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

3. Aceda a "**User Certificate**", conforme ilustrado:

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

- Confirme que o "Key Strength" está configurado com "2048 (Grau elevado)" e em seguida aceda a "Submit".

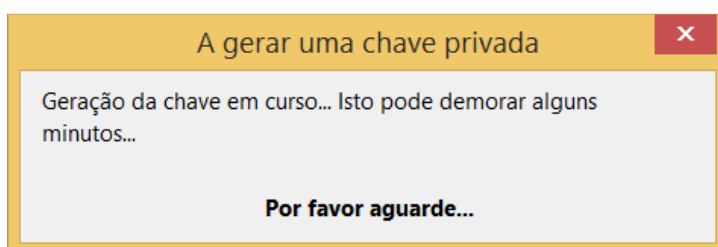
User Certificate - Identifying Information

No further identifying information is required.

Please select a key strength:

Key Strength: 2048 (Grau elevado) ▾

Submit >



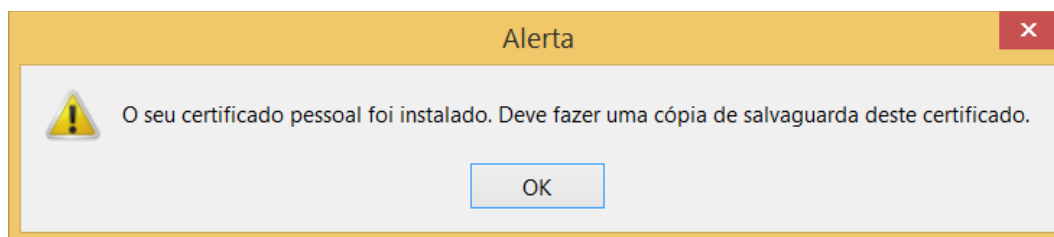
- Pressione "Install this certificate" e em seguida "OK".

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

Save response



- Acuda novamente à página de entrada da autoridade de certificação do ISCTE (<http://certsrv.iscte.pt>). Após o acesso à página de entrada siga a ligação "Download a CA certificate, certificate chain, or CRL":

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

- Em "Encoding method", seleccione a opção "Base 64" (1) e siga a ligação "Download CA certificate chain" (2), conforme ilustrado:
Mais tarde aceda a "Guardar ficheiro".

Nota: A pasta pré-definida do Firefox é "C:\Users\utilizador\Downloads".

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [ISCTECA(2)]

Encoding method:

DER
 Base 64 ¹

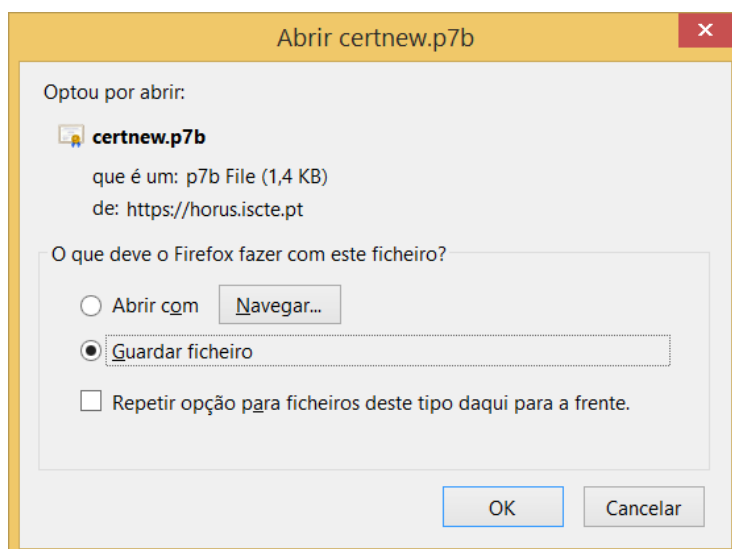
[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#) ²

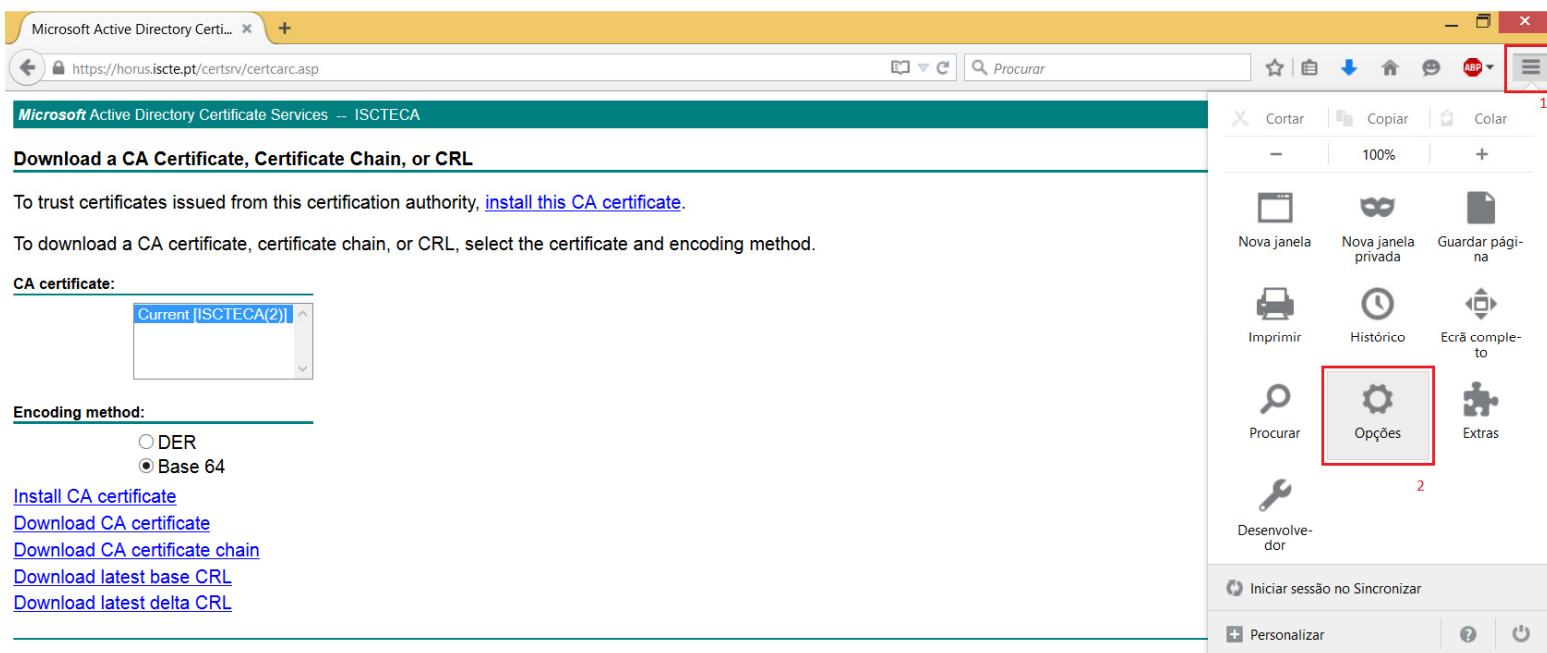
[Download latest base CRL](#)

[Download latest delta CRL](#)

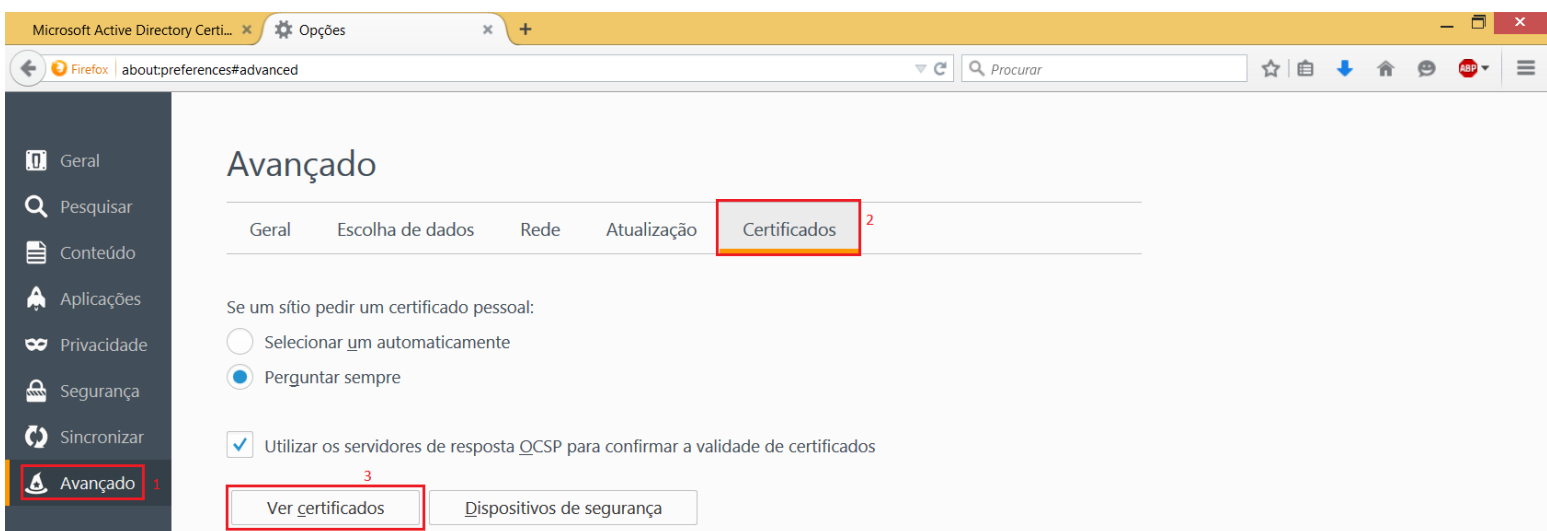


8. Aceda ao símbolo de "Ferramentas" do Firefox no canto superior direito e selecione "Opções", conforme ilustrado:

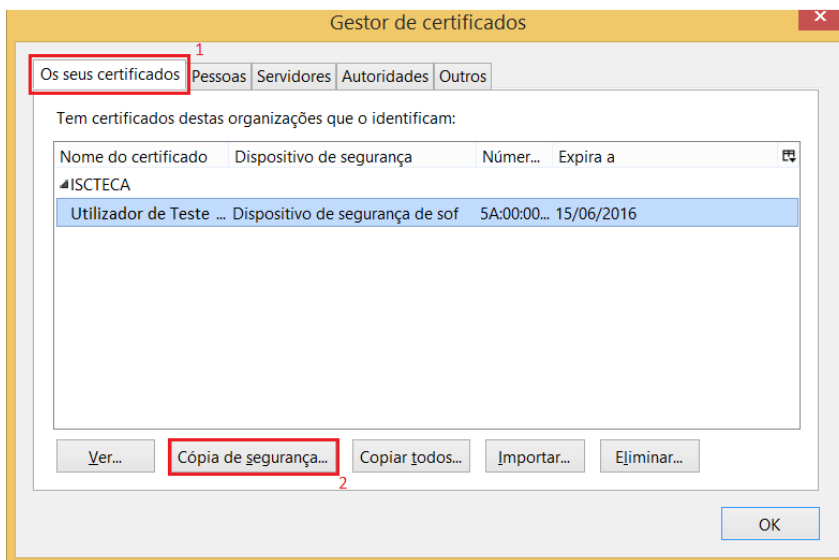
Nota: Caso utilize uma versão com mais de 2 anos, pressione no seu teclado a tecla "ALT" e em seguida aceda ao menu "Ferramentas" e selecione "Opções"



9. Selecione "Avançado" (1), escolha o separador "Certificados" (2) e por fim aceda ao "Ver Certificados" (3).

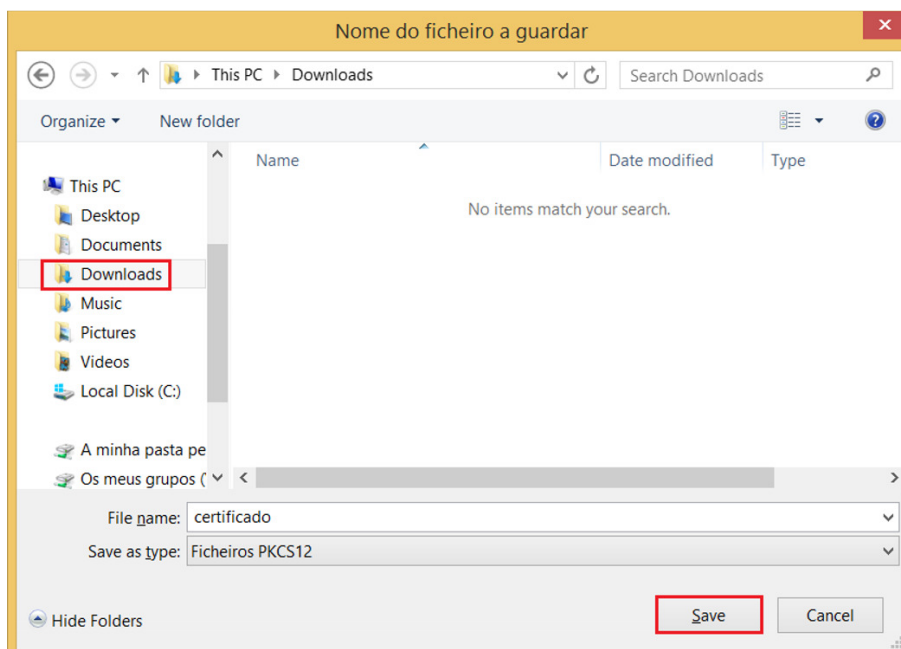


10. Aceda ao separador "Os seus certificados" (1) e selecione, com o rato, o certificado que deverá existir com o seu nome.
Em seguida, pressione o botão "Cópia de segurança" (2).

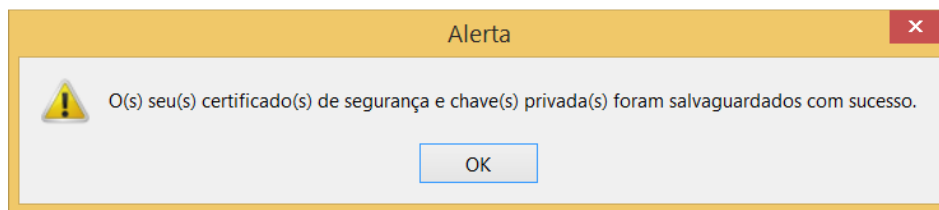
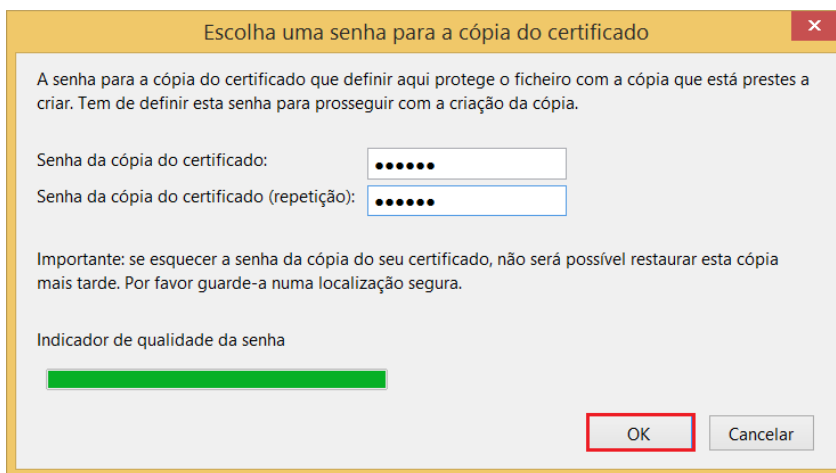


11. Escolha a pasta onde pretende guardar o seu certificado e pressione "**Guardar**".

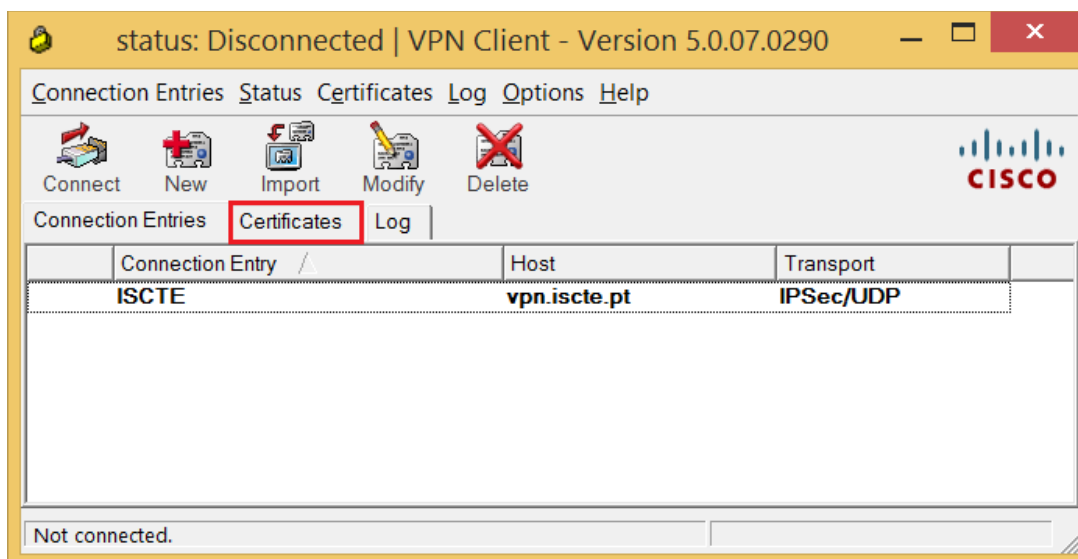
Nota: A nossa sugestão é guardar em "C:\Users\utilizador\Downloads", para que fique na mesma pasta do certificado guardado anteriormente.



12. Introduza uma palavra-passe para guardar o certificado e pressione o botão "OK".



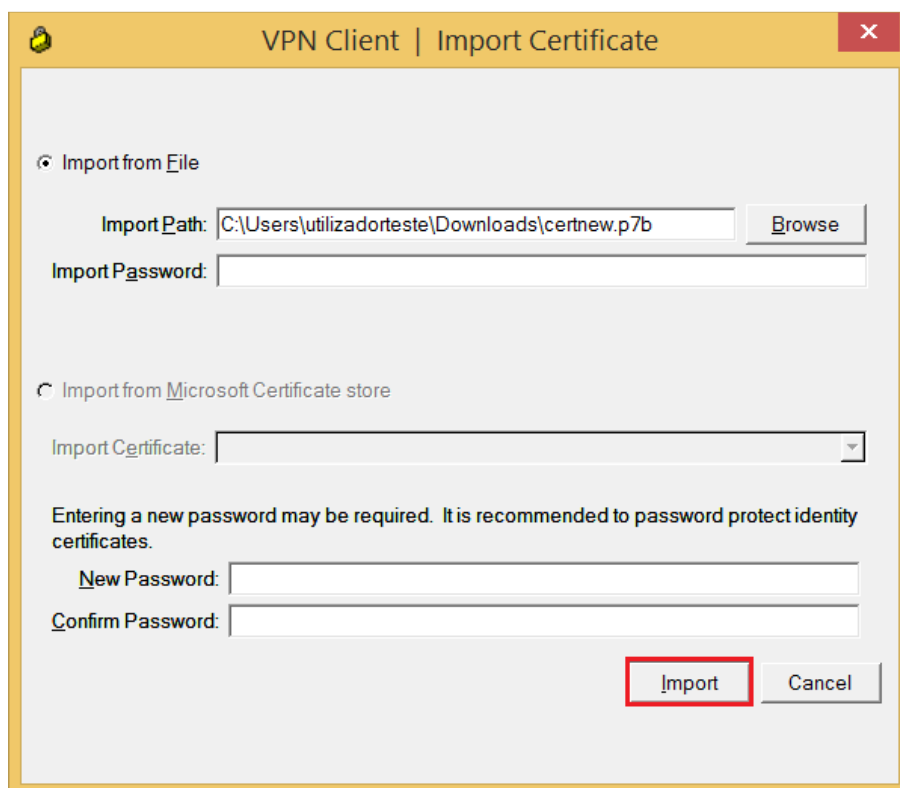
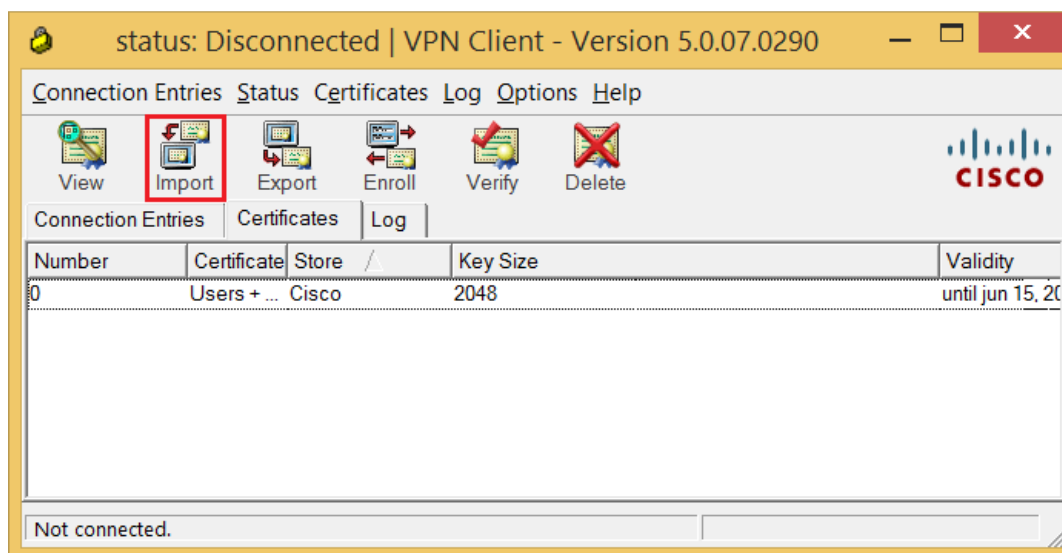
13. Uma vez importados os certificados torna-se necessário proceder à configuração do cliente VPN. Aceda ao cliente de VPN e selecione o separador "Certificates".

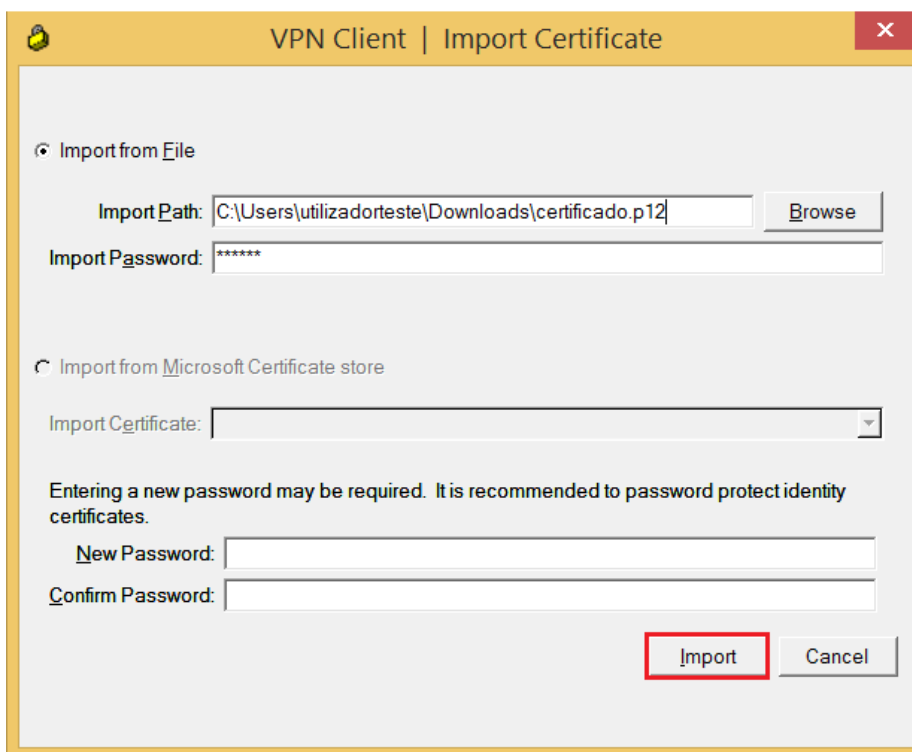


14. Aceda a "Import", procure a pasta onde guardou os certificados e selecione o certificado "certnew.p7b".

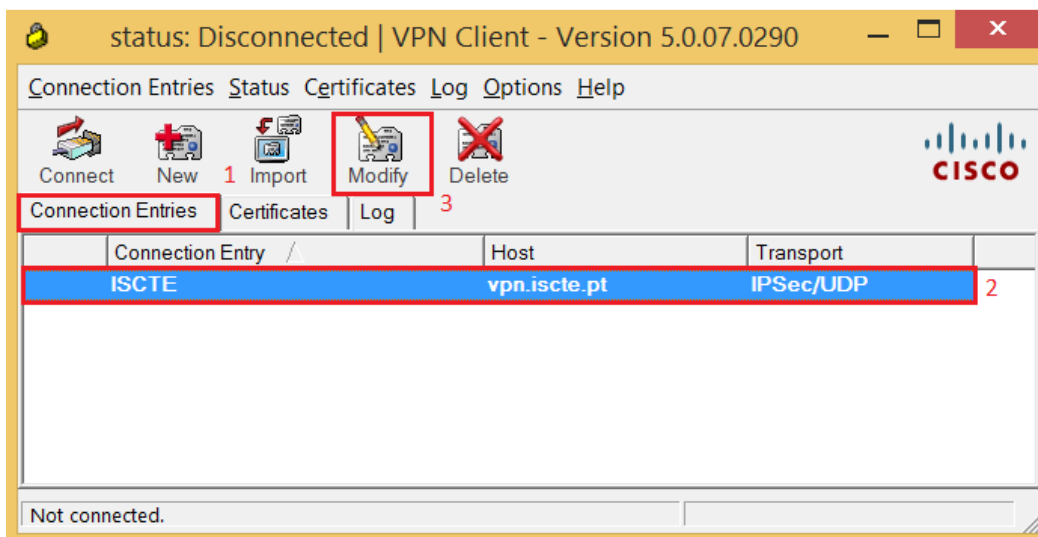
Após a importação do primeiro certificado, importe agora o segundo certificado "certificado.p12" e coloque a "palavra-passe" que criou no passo 10.

Nota: A importação do primeiro certificado "certnew.p7b" não é visível no cliente VPN.

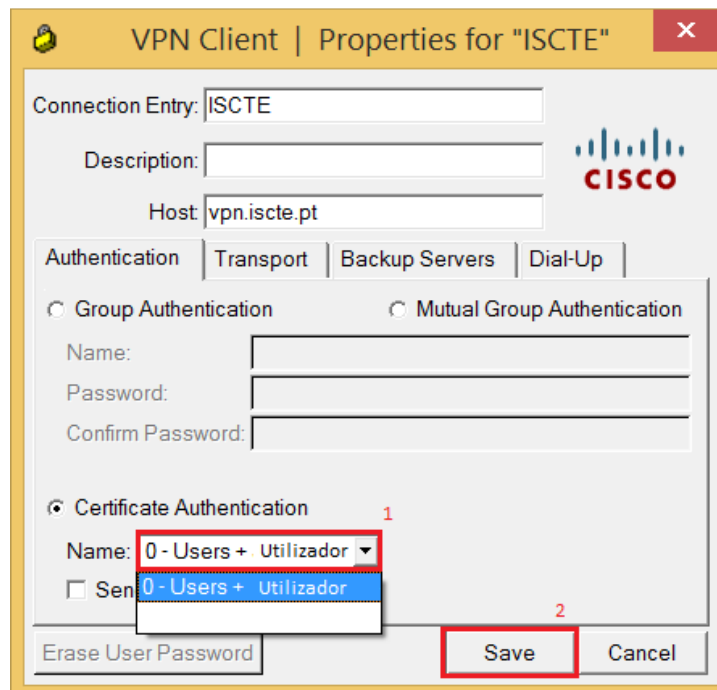




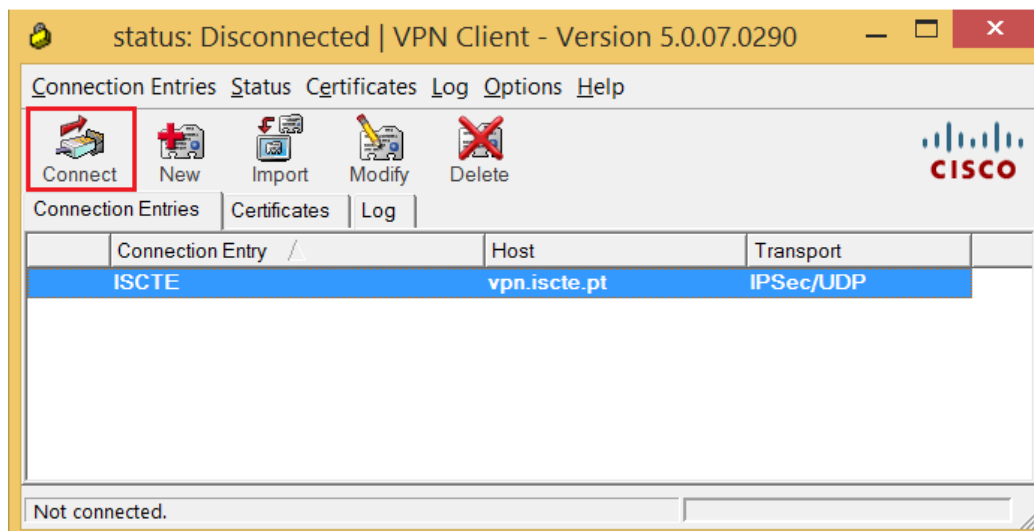
15. No separador "Connection Entry" (1) selecione a ligação "ISCTE" e pressione o botão "Modify".



16. Defina as propriedades da ligação alterando o "Certificate Authentication" (1) para o novo certificado e pressione "OK" (2).



17. Pode agora testar o acesso premindo "Connect".



Contactos

- Em caso de necessidade pode contactar o apoio dos Serviços de Infraestrutura Informática e Comunicações presencialmente na **Sala de Apoio**, no edifício I (junto ao Multibanco), telefonicamente +351 210 464 010 ou por e-mail com a sua conta ISCTE-IUL para “iajuda@iscte.pt”.