O ASA 7.x instala manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN

Índice

Introdução

Este exemplo de configuração descreve como instalar manualmente um certificado digital do vendedor da 3ª parte no ASA para o uso com WebVPN. Um certificado experimental de Verisign é usado neste exemplo. Cada etapa contém o procedimento do aplicativo ASDM e um exemplo CLI.

Pré-requisitos

Requisitos

Este documento exige que você tem o acesso a um Certificate Authority (CA) para o certificado

de registro. 3ª parte que apoiada vendedores de CA é Baltimore, Cisco, confiam, iPlanet/Netscape, Microsoft, RSA, e Verisign.

Componentes Utilizados

Este documento usa um ASA 5510 que execute a versão de software 7.2(1) e a versão 5.2(1) ASDM. Contudo, os procedimentos neste documento trabalham em todo o dispositivo ASA que executar 7.x com qualquer versão compatível ASDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

A fim instalar um certificado digital do vendedor da 3ª parte no PIX/ASA, termine estas etapas:

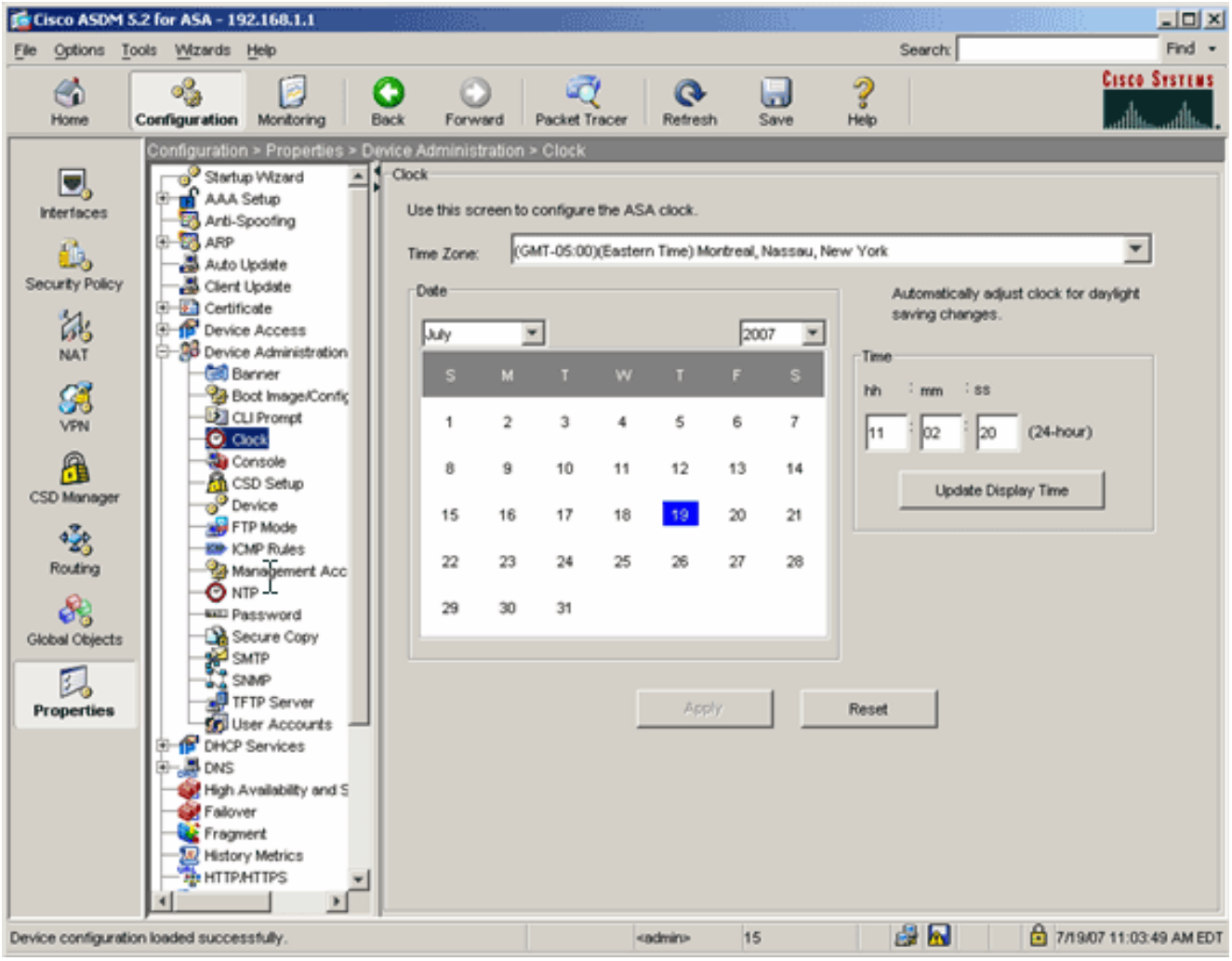
1. Verifique que a data, o tempo, e os valores da zona de hora (fuso horário) são exatos.
2. Gerencia o par de chaves RSA.
3. Crie o ponto confiável.
4. Gerencia o certificado de registro.
5. Autentique o ponto confiável.
6. Instale o certificado.
7. Configurar o WebVPN para usar o certificado recentemente instalado.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Etapa 1. Verifique que a data, o tempo, e os valores da zona de hora (fuso horário) são exatos

Procedimento ASDM

1. A configuração do clique, e clica então propriedades.
2. Expanda a administração do dispositivo, e escolha o pulso de disparo.
3. Verifique que a informação alistada é exata.Os valores para a data, o tempo, e a zona de hora (fuso horário) devem ser exatos para que a validação certificada apropriada ocorra.



Exemplo da linha de comando

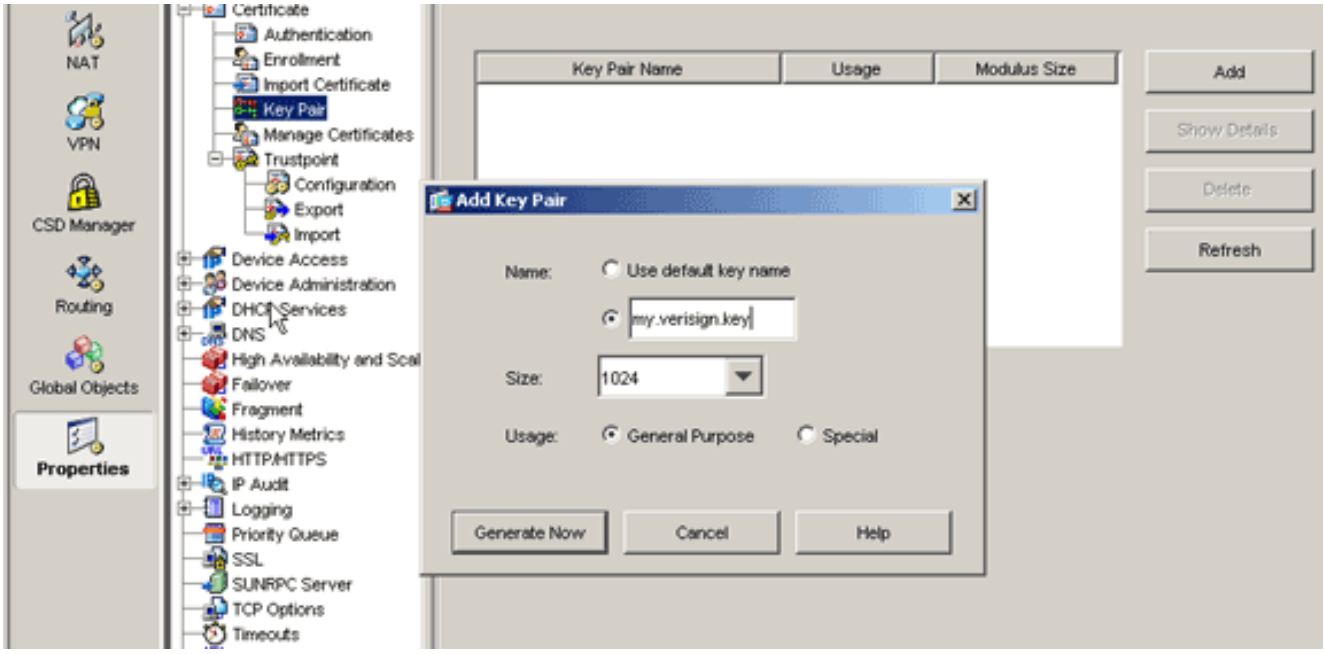
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

Etapa 2. Gerencia o par de chaves RSA

A chave pública gerada RSA é combinada com a informação de identidade do ASA para formar um pedido do certificado PKCS#10. Você deve distintamente identificar o nome chave com o ponto confiável para que você cria o par de chaves.

Procedimento ASDM

1. **A configuração do** clique, e clica então **propriedades**.
2. Expanda o **certificado**, e escolha o **par de chaves**.
3. Clique em
   Add.



4. Dê entrada com o nome chave, escolha o tamanho do módulo, e selecione o tipo do uso. Nota: O tamanho recomendado do par de chaves é 1024.
5. O clique **gerencie**.O par de chaves que você criou deve ser alistado na coluna do nome do par de chaves.

Exemplo da linha de comando

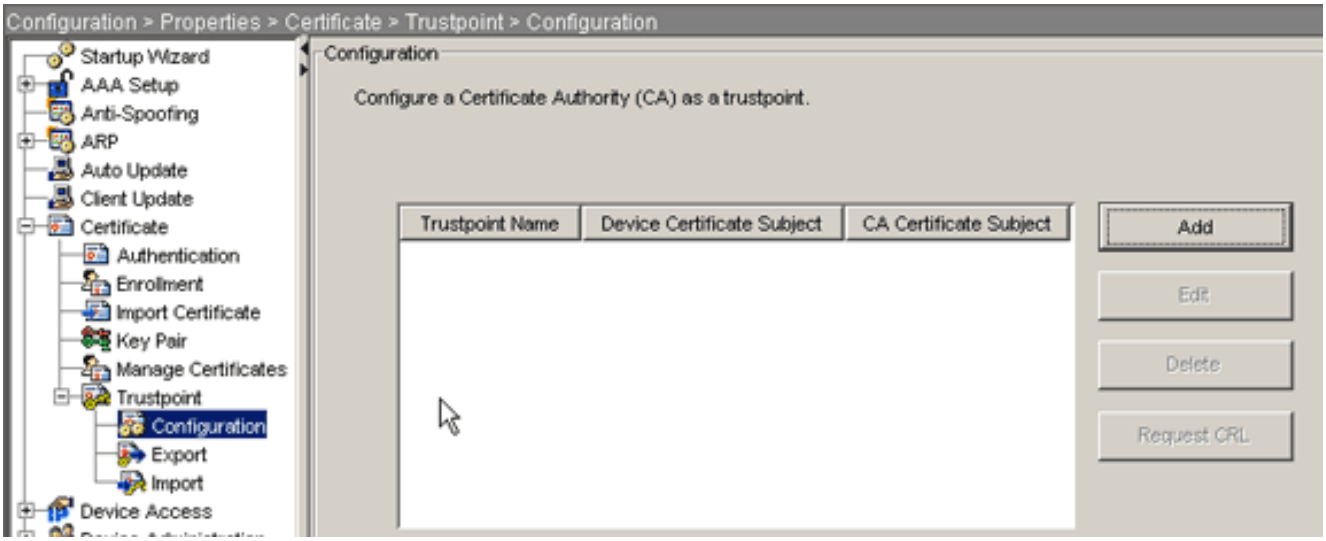
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

Etapa 3. Crie o ponto confiável

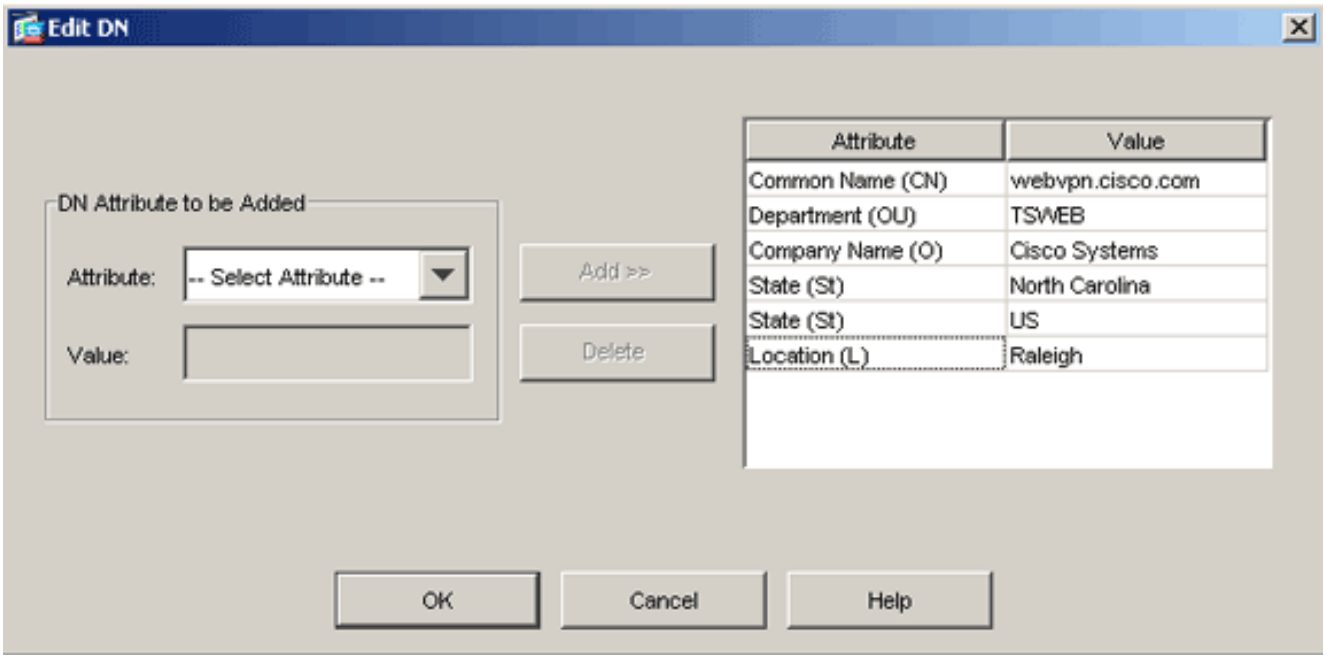
Os pontos confiáveis são exigidos declarar o Certificate Authority (CA) que seu ASA usará.

Procedimento ASDM

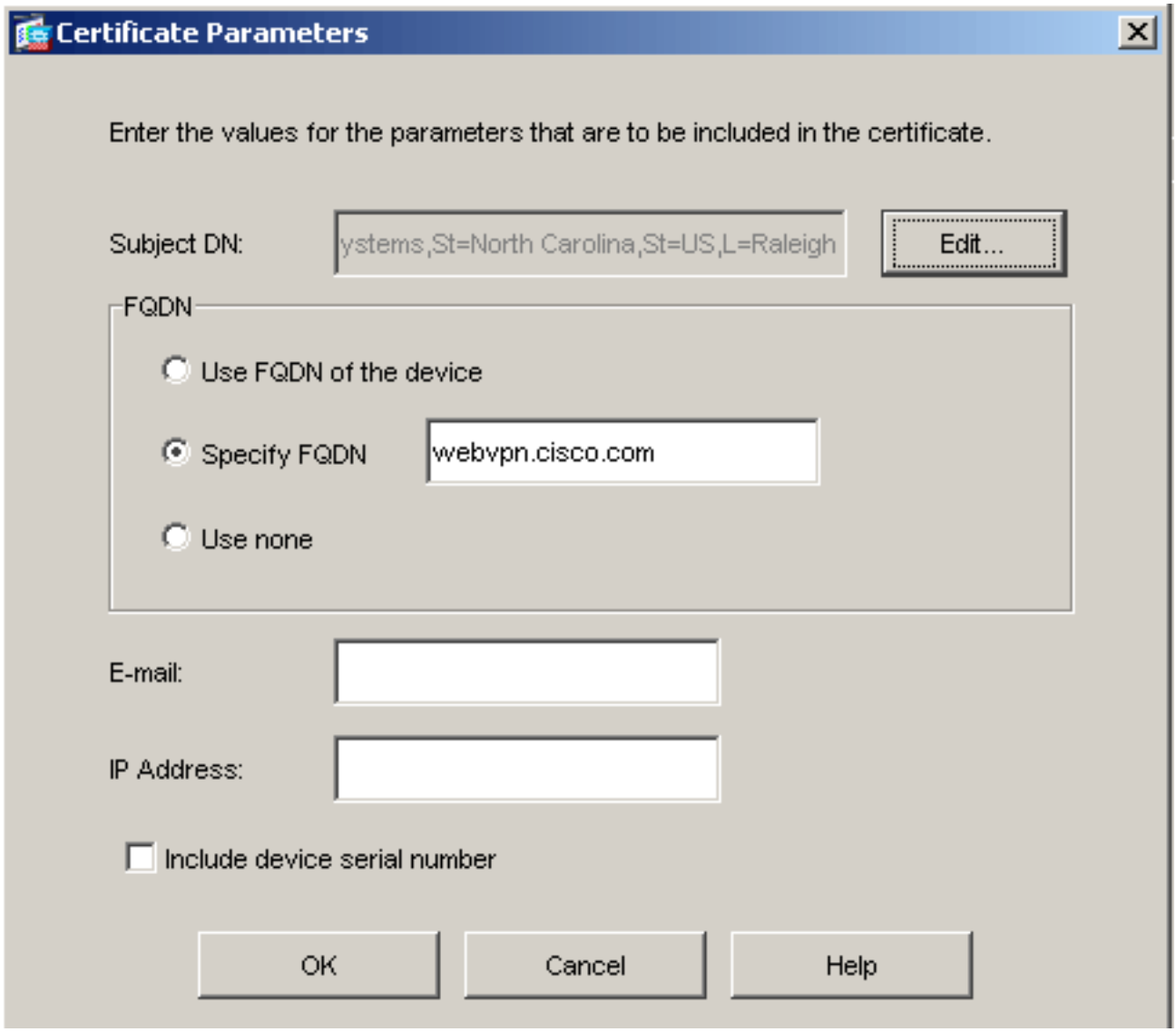
1. **A configuração do** clique, e clica então **propriedades**.
2. Expanda o **certificado**, e expanda então o **ponto confiável**.
3. Escolha a **configuração**, e o clique **adiciona**.



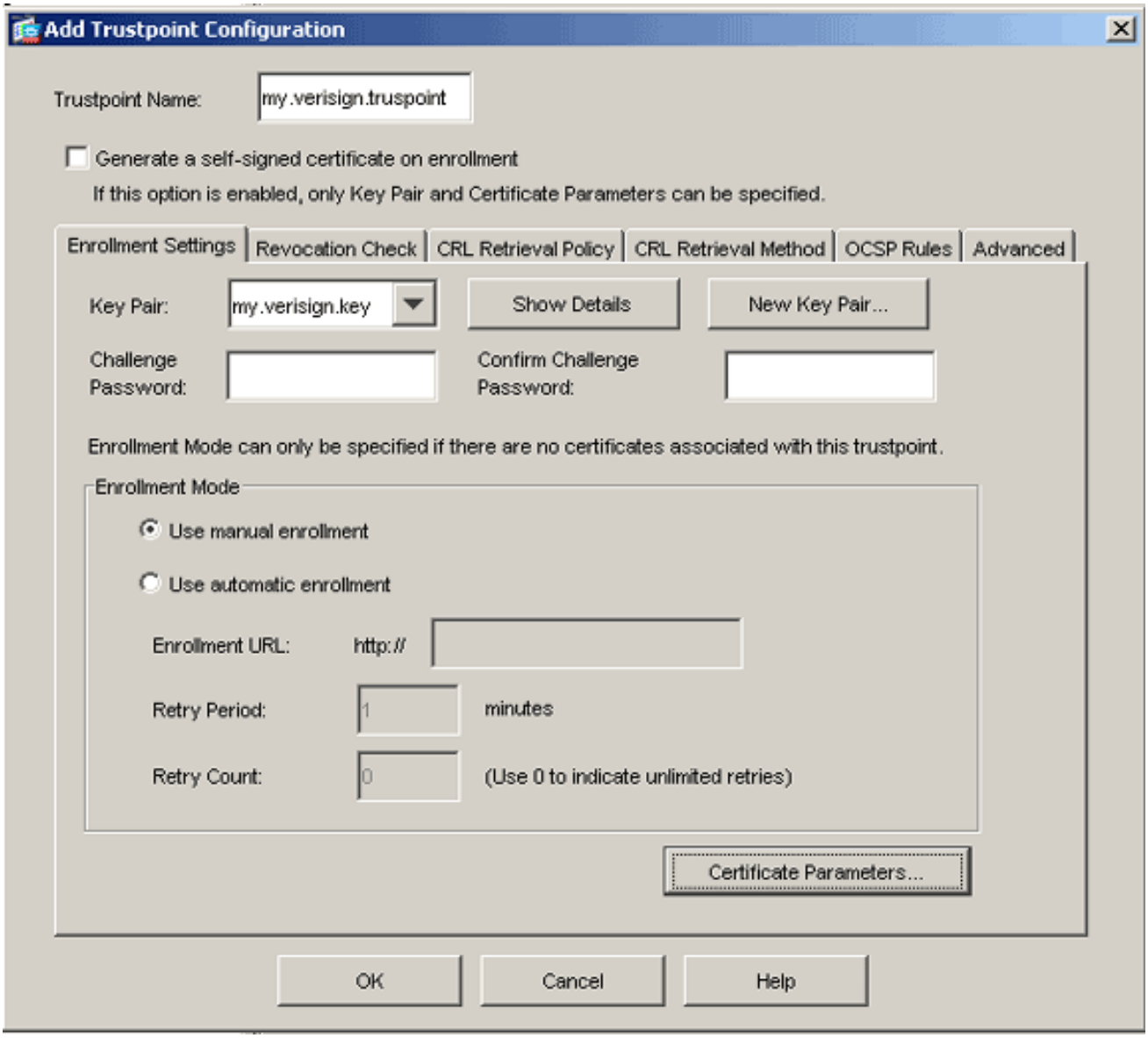
4. Configurar estes valores:**Nome do ponto confiável**: O nome do ponto confiável deve ser relevante ao uso pretendido. (Este exemplo usa *my.verisign.trustpoint.)***Par de chaves**: Selecione o par de chaves gerado em etapa 2. (*my.verisign.key)*
5. Assegure-se de que a Inscrição manual esteja selecionada.
6. Clique **parâmetros do certificado**.A caixa de diálogo dos parâmetros do certificado aparece.
7. Clique **editam**, e configuram os atributos alistados nesta tabela:A fim configurar estes valores, para escolher um valor da lista de drop-down do atributo, para incorporar o valor, e o clique
adicionar.



8. Uma vez que os valores apropriados são adicionados, clique a **APROVAÇÃO**.
9. Na caixa de diálogo dos parâmetros do certificado, incorpore o FQDN ao campo FQDN da especificação.Este valor deve ser o mesmo FQDN que você se usou para o Common Name (CN).



10. Click **OK**.
11. Verifique que o par de chaves correto está selecionado, e clique o botão de rádio da **Inscrição manual do uso**.
12. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.



Exemplo da linha de comando

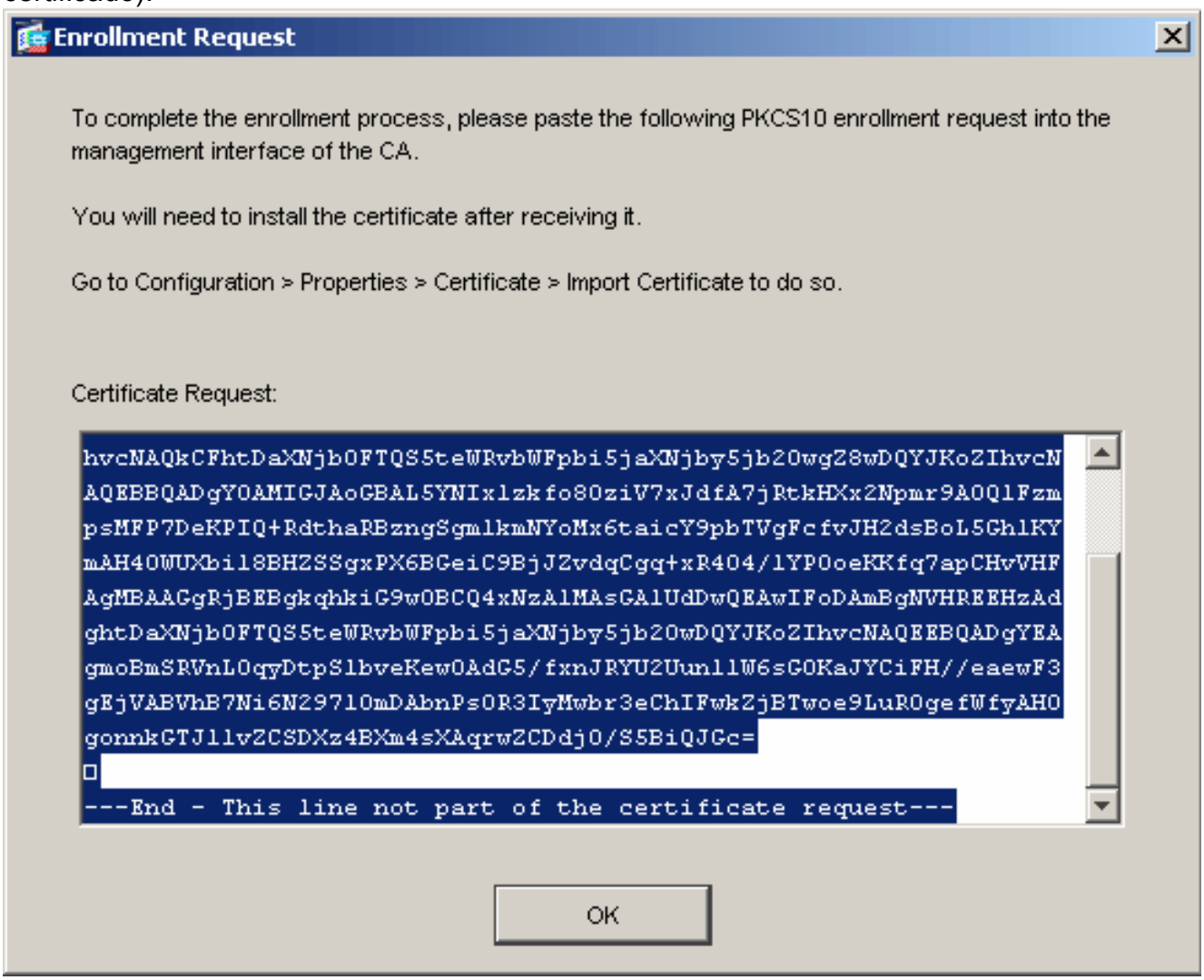
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh** *! Defines x.500 distinguished name.* ciscoasa(config-ca-trustpoint)#**keypair my.verisign.key** *! Specifies key pair generated in Step 3.* ciscoasa(config-ca-trustpoint)#**fqdn webvpn.cisco.com** *! Specifies subject alternative name (DNS:).*

```
ciscoasa(config-ca-trustpoint)#exit
```

Etapa 4. Gerencia o certificado de registro

Procedimento ASDM

1. **A configuração do** clique, e clica então **propriedades**.
2. Expanda o **certificado**, e escolha o **registro**.
3. Verifique que o ponto confiável criado em etapa 3 está selecionado, e o clique **se registra**.Uma caixa de diálogo parece que alista o pedido do certificado de registro (igualmente referido como uma solicitação de assinatura de certificado).



4. Copie o pedido do registro PKCS#10 a um arquivo de texto, e submeta então o CSR ao vendedor apropriado da 3ª parte.Depois que o vendedor da 3ª parte recebe o CSR, devem emitir um certificado de identidade para a instalação.

Exemplo da linha de comando

Nome de dispositivo 1
ciscoasa(config)#**crypto ca enroll my.verisign.trustpoint** *! Initiates CSR. This is the request to be ! submitted via web or email to the 3rd party vendor.* % Start certificate enrollment .. % The subject name in the

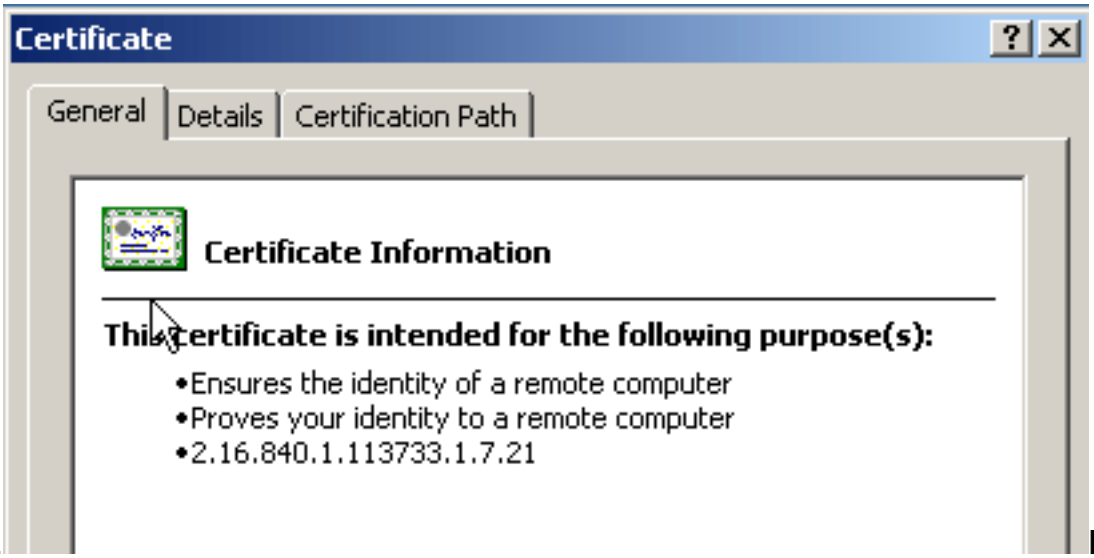
```
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes

! Displays the PKCS#10 enrollment request to the
terminal. ! You will need to copy this from the terminal
to a text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no
ciscoasa(config)#
```

Etapa 5. Autentique o ponto confiável

Uma vez que você recebe o certificado de identidade do vendedor da 3ª parte, você pode continuar com esta etapa.

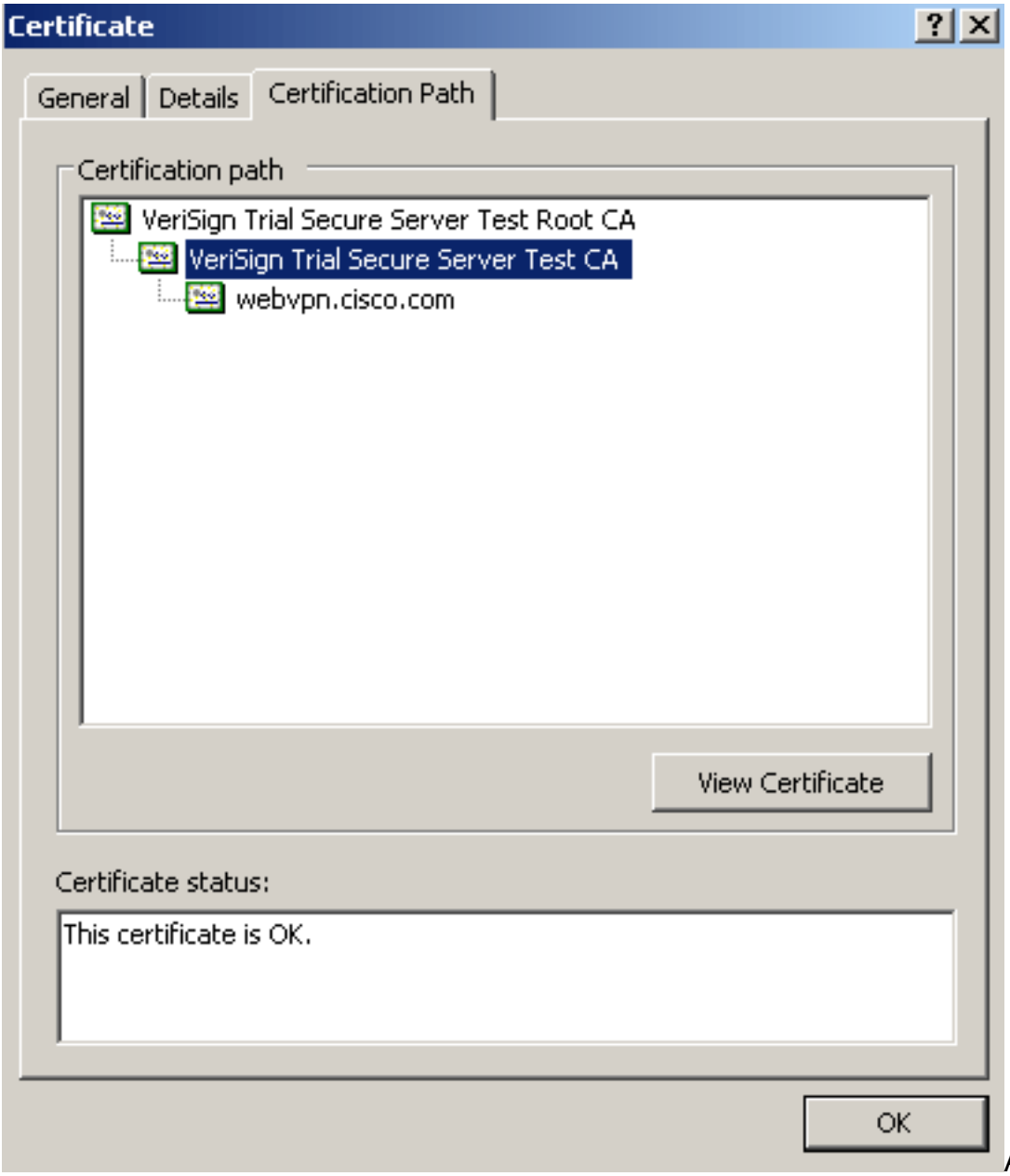
Procedimento ASDM

1. Salvar o certificado de identidade a seu computador local.
2. Se você foi fornecido um certificado base64-encoded que não venha como um arquivo, você deve copiar a mensagem base64, e cola-a em um arquivo de texto.
3. Rebatize o arquivo com uma extensão de .cer.**Note**: O arquivo é rebatizado uma vez com a extensão de .cer, o ícone do arquivo deve indicar como um certificado.
4. Fazer duplo clique o arquivo certificado.A caixa de diálogo do certificado

aparece. 

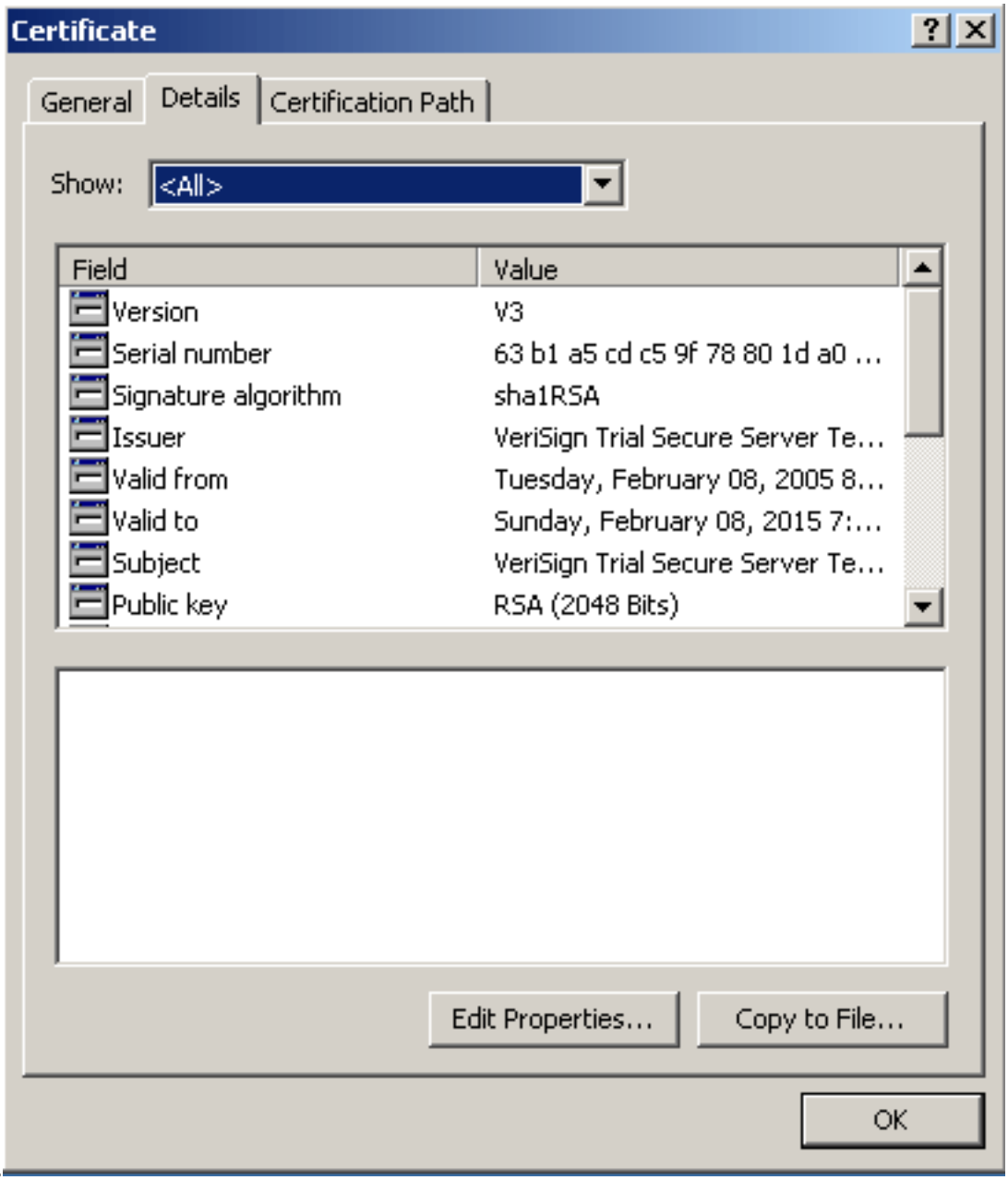
Note: Se "*Windows não tem bastante informação a verificar que a* mensagem d*este certificado*" parece no tab geral, você deve obter a CA raiz do vendedor da 3ª parte ou o certificado de CA intermediário antes que você continue com este procedimento. Contacte seu vendedor da 3ª parte ou administrador de CA a fim obter a CA raiz de emissão ou o certificado de CA intermediário.

5. Clique a aba do **trajeto do certificado**.
6. Clique o certificado de CA situado acima de seu certificado de identidade emitido, e clique o **certificado da**



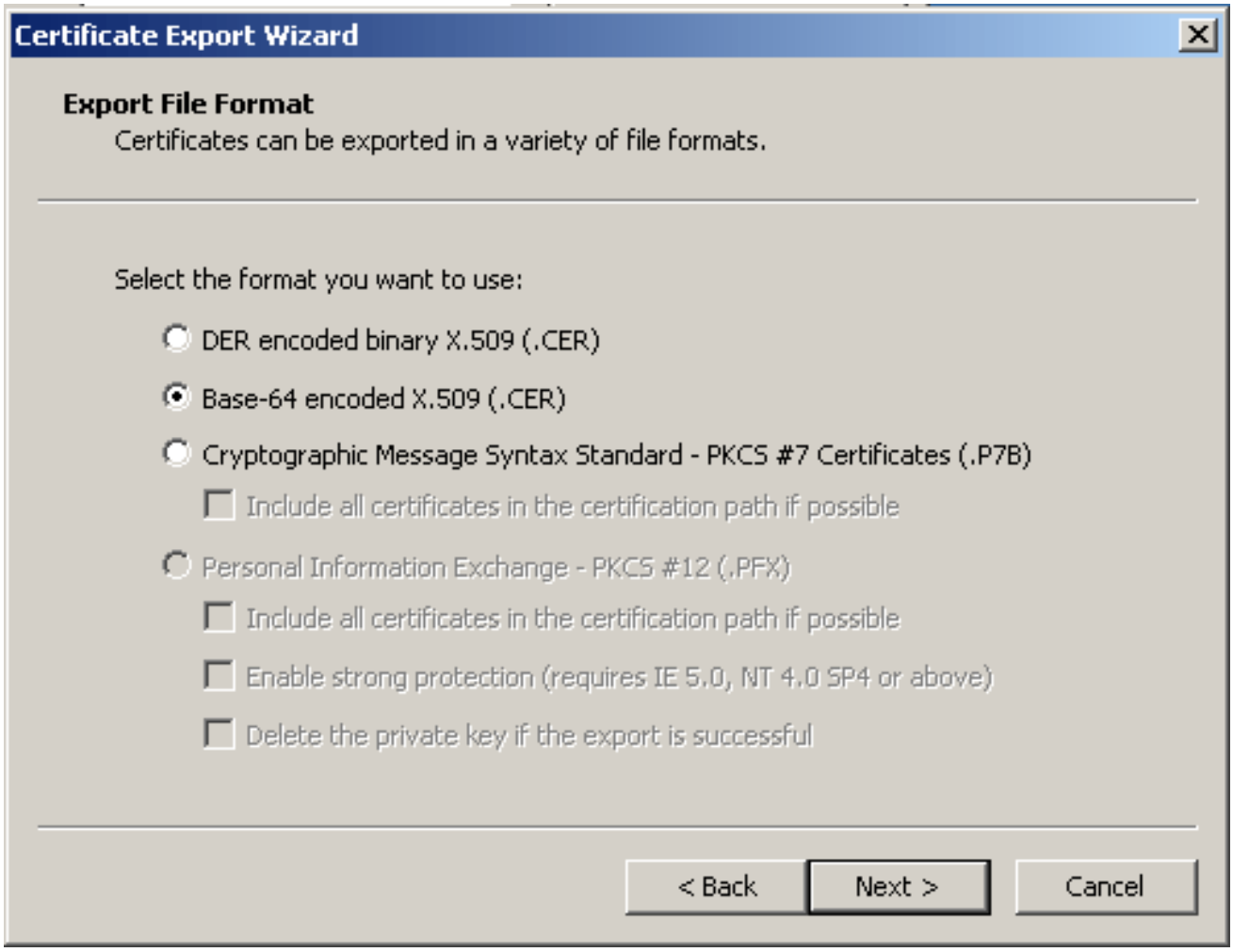
vista. A informação detalhada sobre o certificado de CA intermediário aparece.**aviso:** Não instale o certificado da identidade (dispositivo) nesta etapa. Somente a raiz, a raiz subordinada, ou o certificado de CA são adicionados nesta etapa. Os Certificados da identidade (dispositivo) são instalados na etapa 6.

7. Clique em

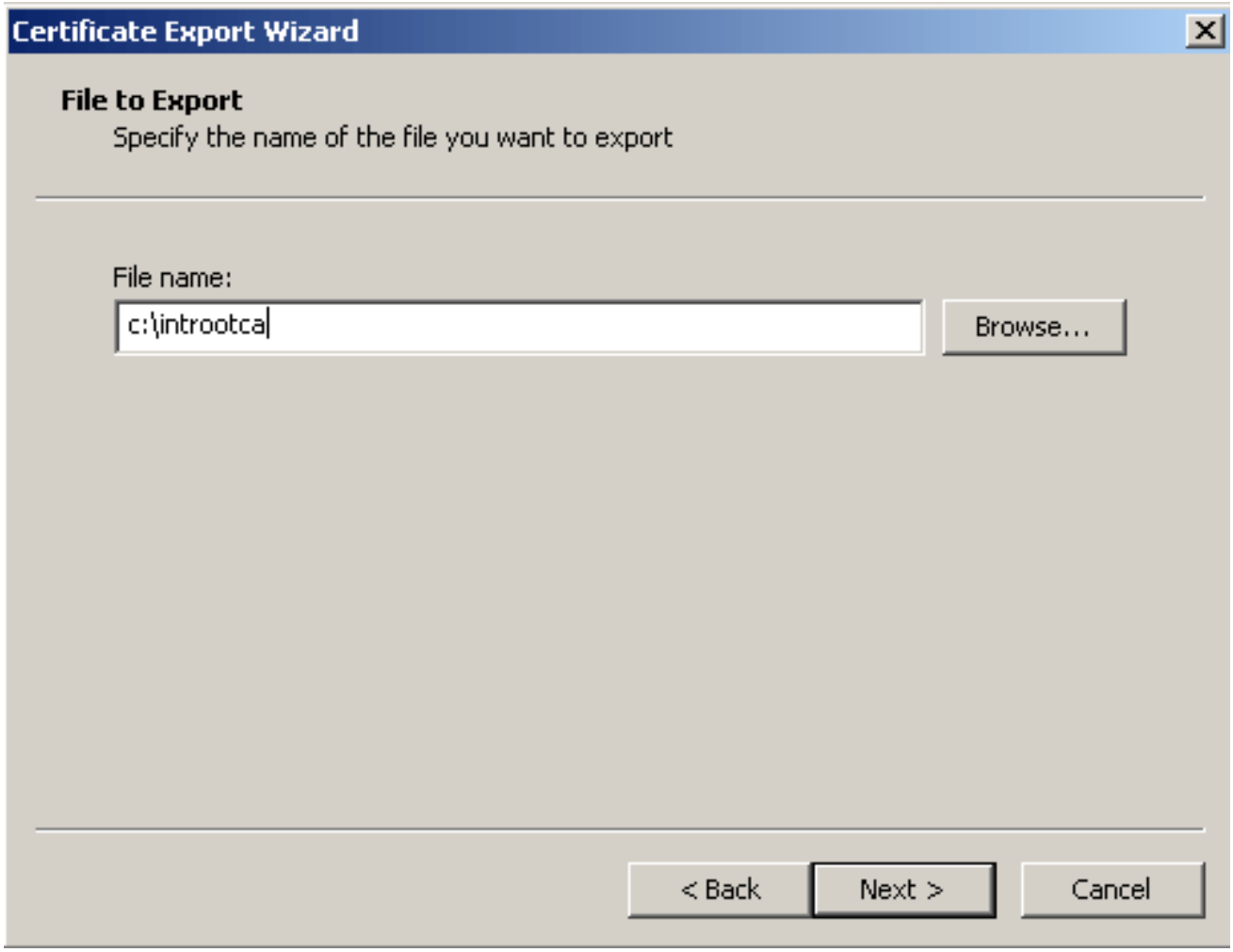


Details.

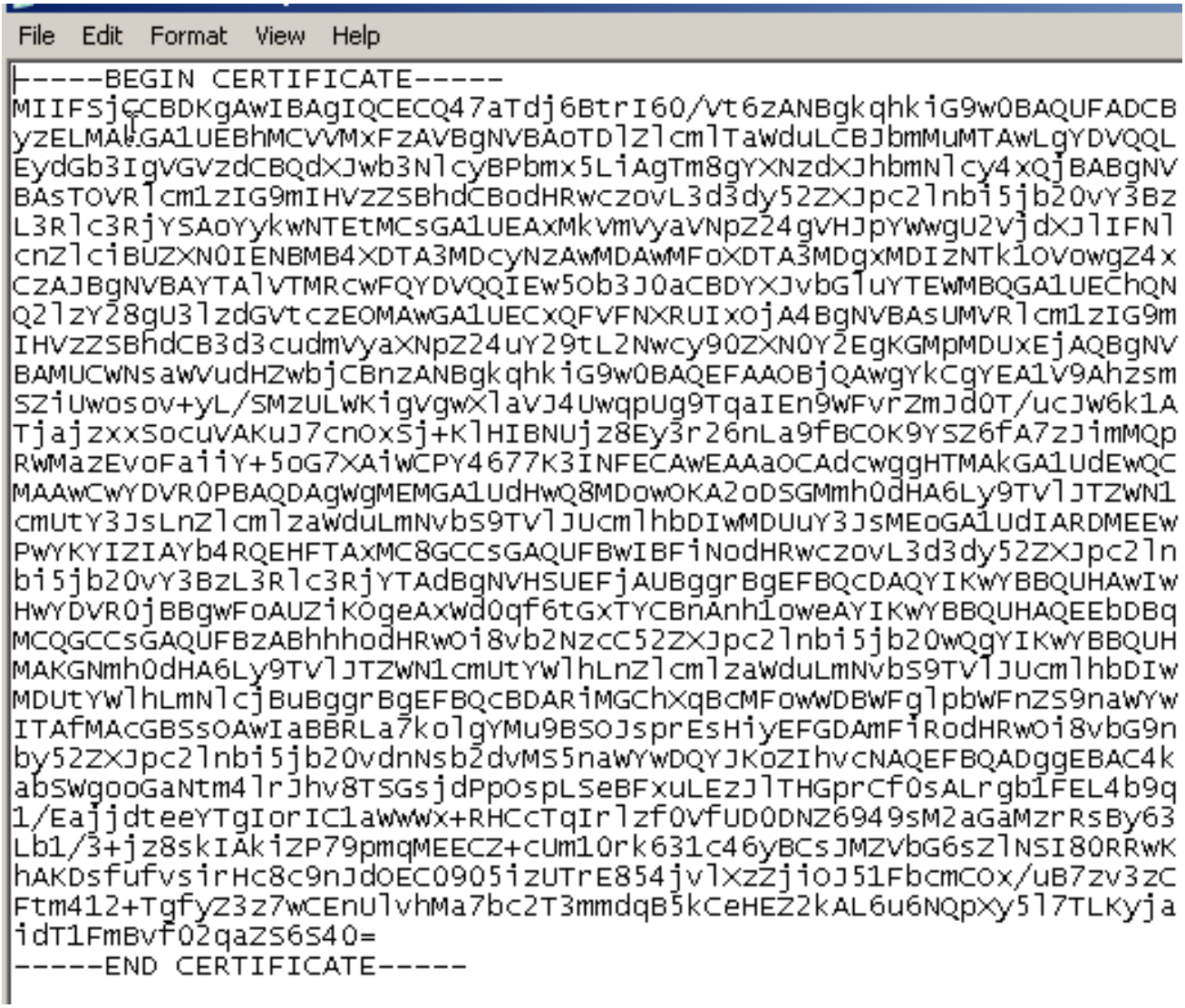
8. **Cópia do** clique **a arquivar**.
9. Dentro do assistente da exportação do certificado, clique **em seguida.**
10. Na caixa de diálogo do formato do arquivo da exportação, clique **(.CER) o** botão de rádio **X.509 codificado Base-64**, e clique-o **em seguida**.



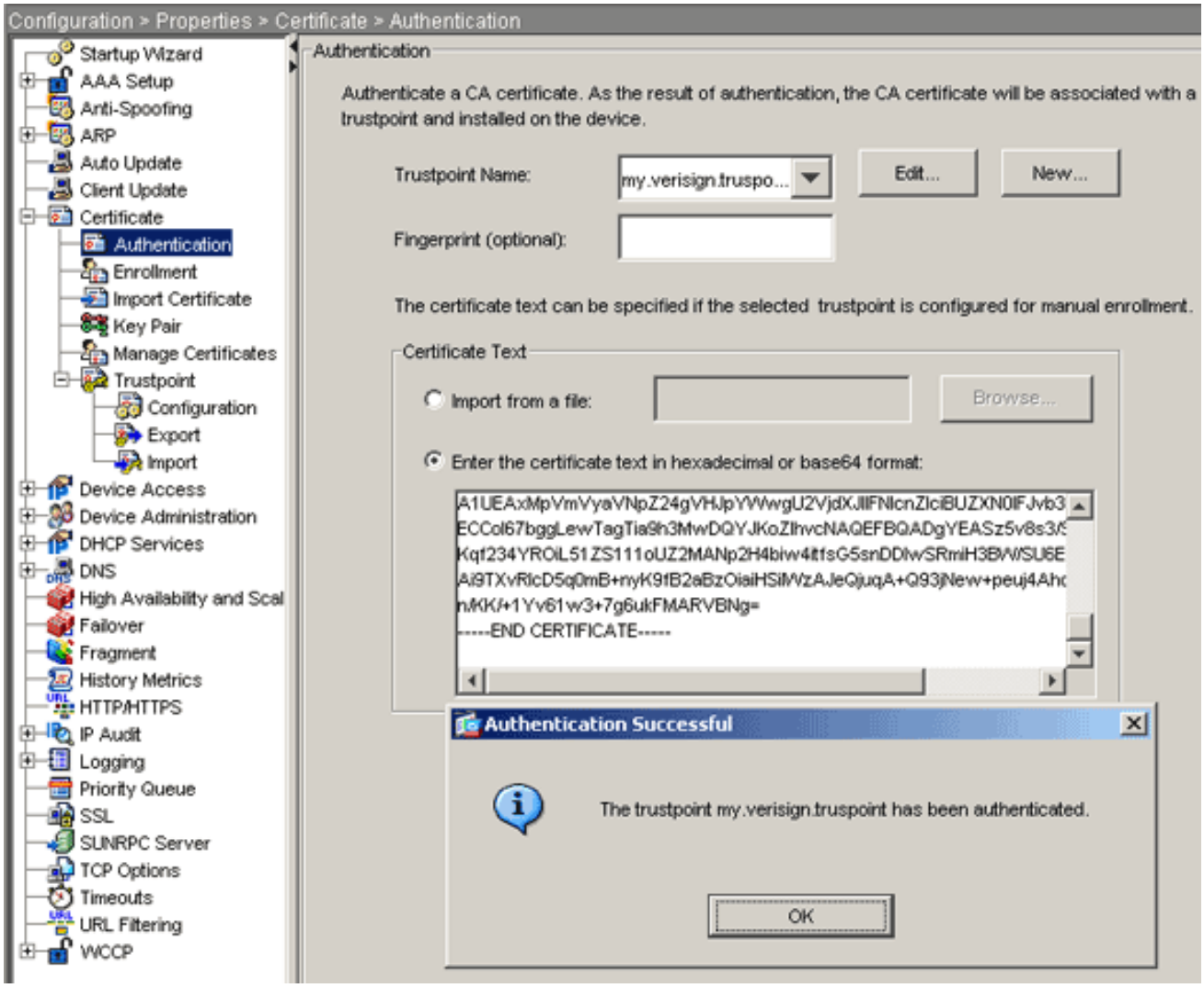
11. Entre no nome de arquivo e no lugar a que você quer salvar o certificado de CA.
12. Clique em Avançar e, em seguida, clique em Concluir.



13. Clique a **APROVAÇÃO na** caixa de diálogo bem sucedida da exportação.
14. Consulte ao lugar onde você salvar o certificado de CA.
15. Abra o arquivo com um editor de texto, tal como o bloco de notas. (Clicar com o botão direito o arquivo, e o escolha **enviam a > bloco de notas**.)A mensagem base64-encoded deve parecer similar ao certificado nesta
imagem:



16. Dentro do ASDM, a **configuração do** clique, e clica então **propriedades.**
17. Expanda o **certificado**, e escolha a **autenticação**.
18. Clique a **entrada o texto do certificado no** botão de rádio do **hexadecimal ou do formato base64**.
19. Cole o certificado de CA base64-formatted de seu editor de texto na área de texto.
20. O clique
    autentica.



21. Click **OK**.

Exemplo da linha de comando

ciscoasa
ciscoasa(config)#**crypto ca authenticate my.verisign.trustpoint** *! Initiates the prompt to paste in the base64 CA root ! or intermediate certificate.* Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself **-----BEGIN CERTIFICATE-----** **MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQUFADCB** **jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL** **EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xMjAwBgNV** **BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290IENBMB4X** **DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYTAlVTMRcw** **FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3QgUHVycG9z** **ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBvZiB1c2Ug** **YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxLTAr** **BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD**

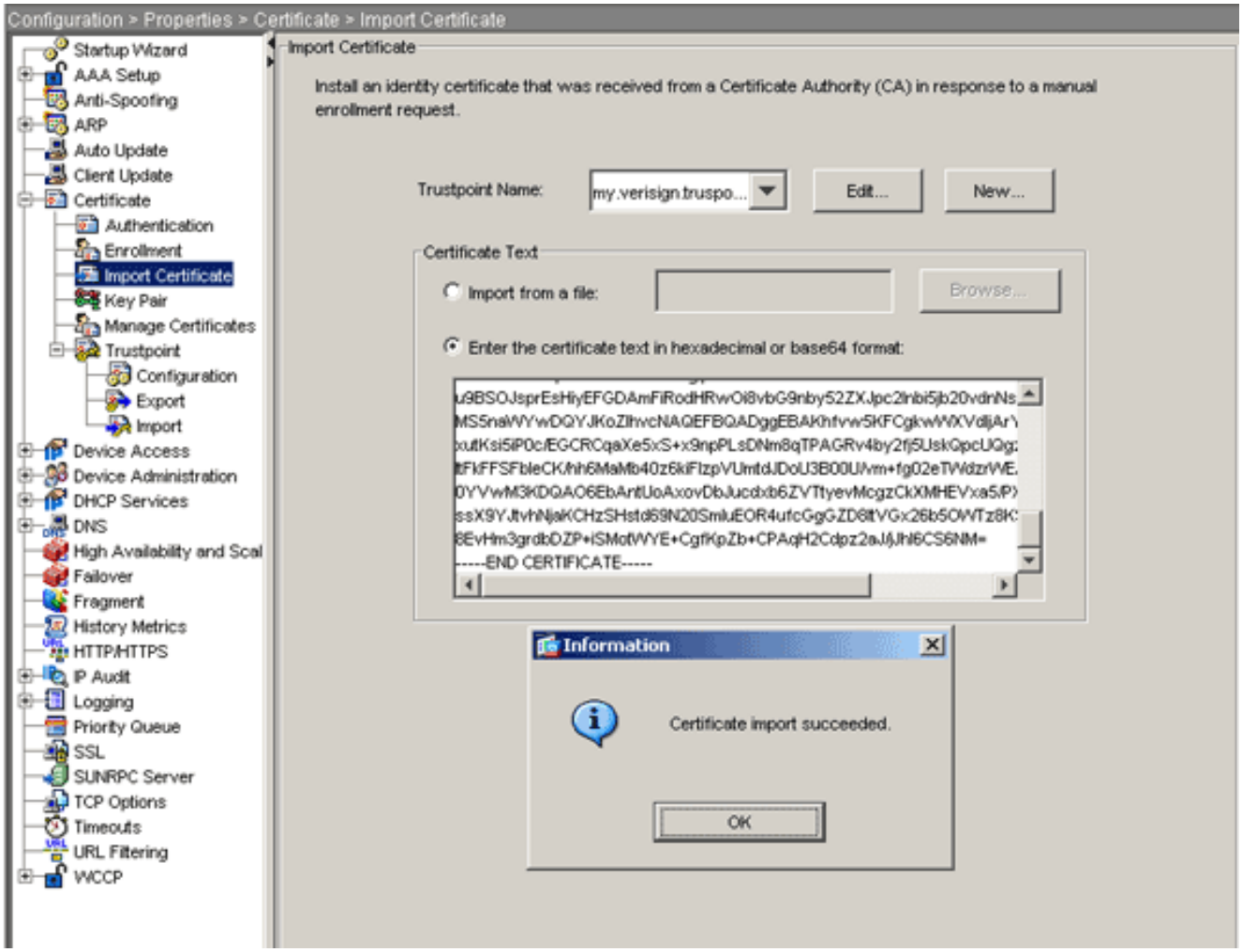
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNg=
-----END CERTIFICATE-----
quit



! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this
certificate? [yes/no]: yes Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)#
```

Etapa 6. Instale o certificado

Procedimento ASDM

Use o certificado de identidade fornecido pelo vendedor da 3ª parte para executar estas etapas:

1. Clique a **configuração**, e clique então **propriedades**.
2. Expanda o **certificado**, e escolha então o **certificado de importação**.
3. Clique a **entrada o texto do certificado no** botão de rádio do **hexadecimal ou do formato base64**, e cole o certificado de identidade base64 no campo de texto.



4. Clique a **importação**, e clique então a **APROVAÇÃO**.

Exemplo da linha de comando

ciscoasa

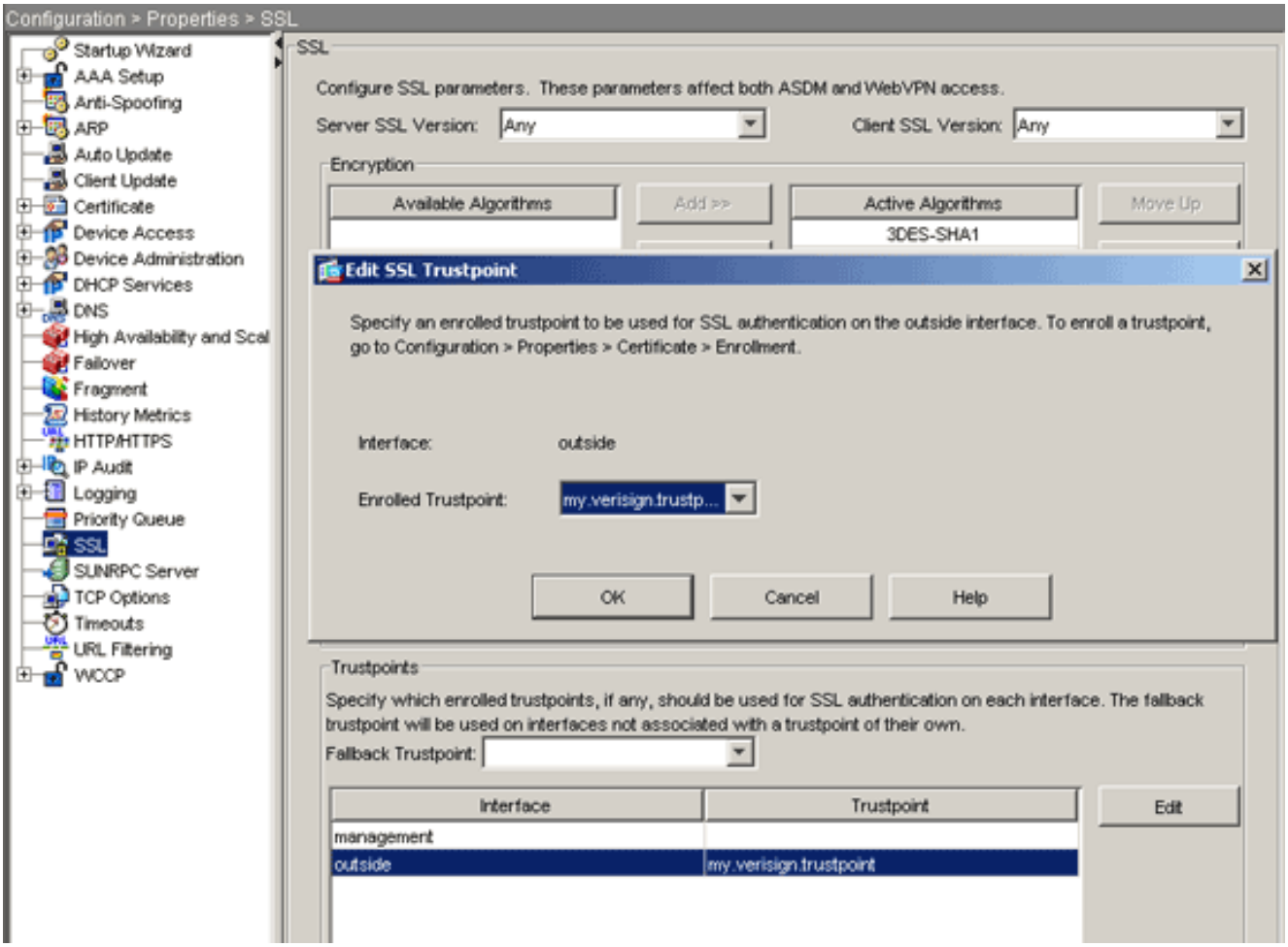
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! Initiates prompt to paste the base64 identity
certificate ! provided by the 3rd party vendor. % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself -----BEGIN
CERTIFICATE-----
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G
A1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUIx
```

```
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
ciscoasa(config)#
```

Etapa 7. Configurar o WebVPN para usar o certificado recentemente instalado

Procedimento ASDM

1. Clique a **configuração**, clique **propriedades**, e escolha então o **SSL**.
2. Na área dos pontos confiáveis, selecione a relação que será usada para terminar sessões de VPN da Web. (Este exemplo usa a interface externa.)
3. O clique **edita**.A caixa de diálogo do ponto confiável da edição SSL aparece.



4. Da lista de drop-down registrada do ponto confiável, escolha o ponto confiável que você criou em etapa 3.
5. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.

Seu certificado novo deve agora ser utilizado para todas as sessões de VPN da Web que terminam na relação especificada. Veja a seção da verificação neste documento para obter informações sobre de como verificar uma instalação bem-sucedida.

Exemplo da linha de comando

ciscoasa
ciscoasa(config)#**ssl trust-point my.verisign.trustpoint outside** *! Specifies the trustpoint that will supply the SSL ! certificate for the defined interface.* ciscoasa(config)#**write memory** Building configuration... Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08 8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)# *! Save configuration.*

Verificar

Esta seção descreve como confirmar que a instalação de seu certificado do vendedor da 3ª parte era bem sucedida.

Substitua o certificado auto-assinado do ASA

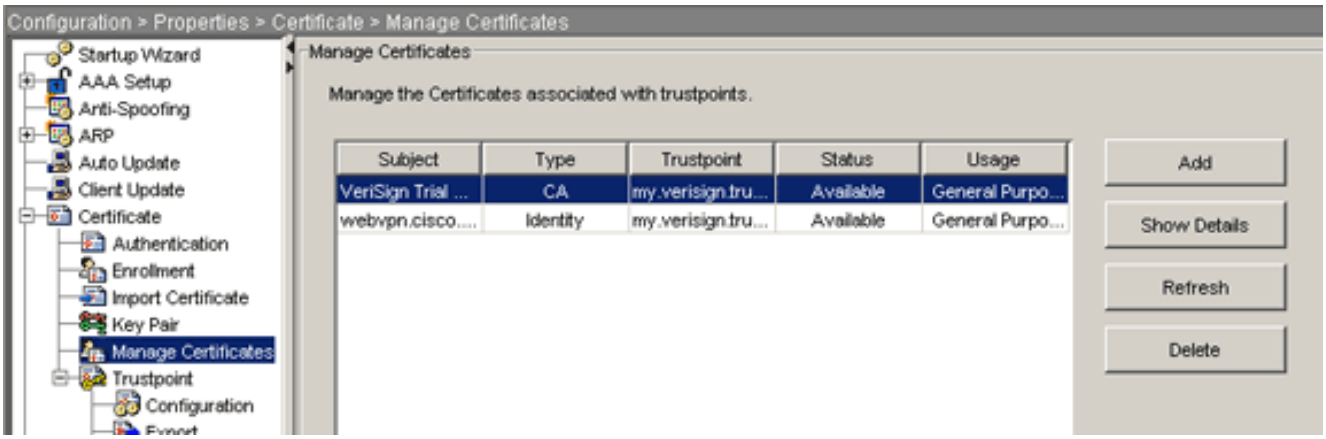
Esta seção descreve como substituir o certificado auto-assinado instalado do ASA.

1. Emita uma solicitação de assinatura de certificado a Verisign.Depois que você recebe o certificado pedido de Verisign, você pode instalá-lo diretamente sob o mesmo ponto confiável.
2. Datilografe este comando: **o Ca cripto registra Verisign**Você é alertado responder a perguntas.
3. Para o pedido do certificado do indicador ao terminal, entre **sim**, e envie a saída a Verisign.
4. Uma vez que lhe dão o certificado novo, datilografe este comando: **certificado Verisign cripto da importação Ca**

Certificados instalados vista

Procedimento ASDM

1. **Configuração do** clique, e **propriedades do** clique.
2. Expanda o **certificado**, e escolha-o **controlam Certificados**.O certificado de CA usado para a autenticação do ponto confiável e o certificado de identidade que foi emitido pelo vendedor da 3ª parte deve aparecer na área dos Certificados do controlo.



Exemplo da linha de comando

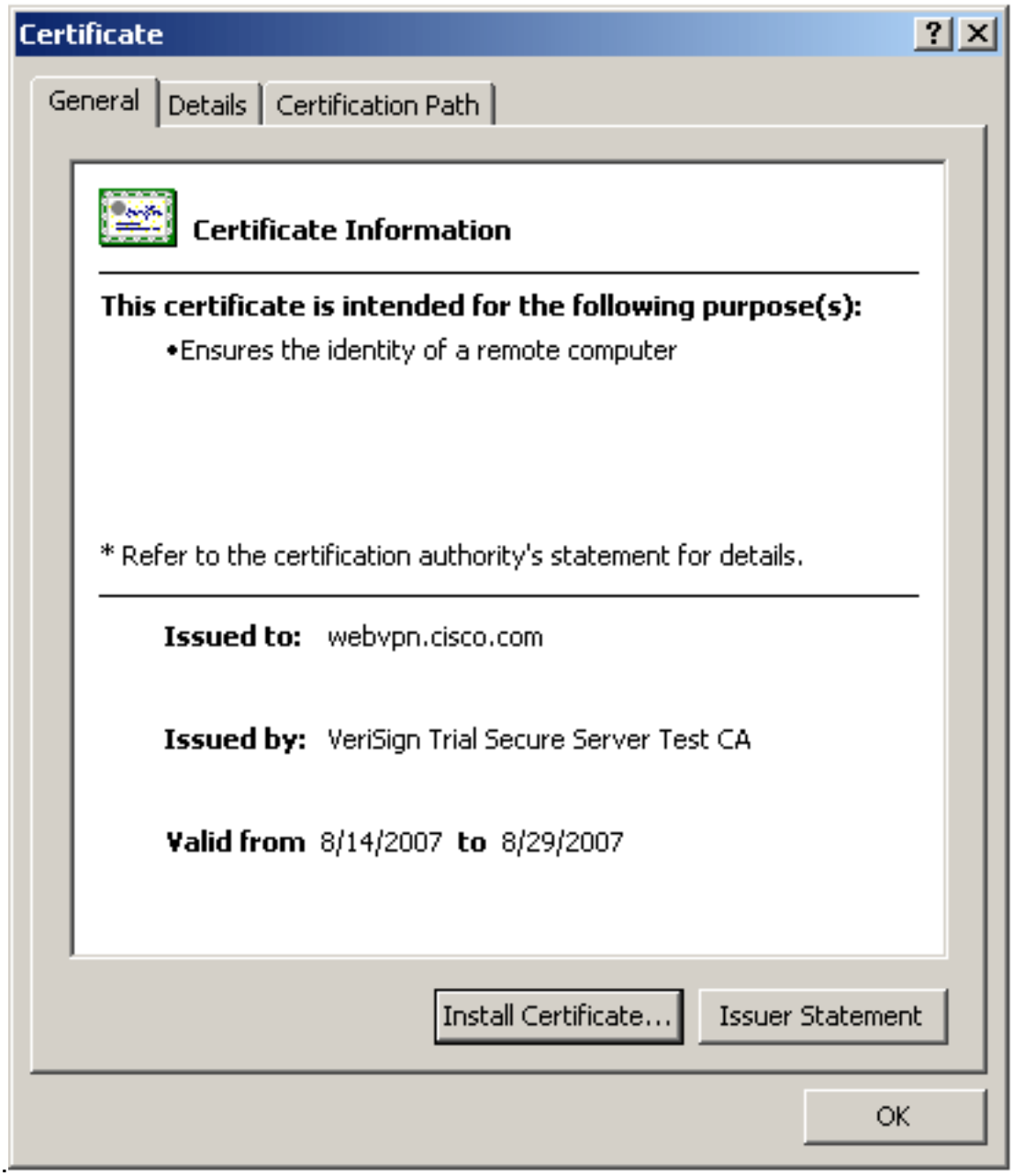
ciscoasa
ciscoasa(config)#**show crypto ca certificates** *! Displays all certificates installed on the ASA.* Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure Server Test CA ou=Terms of use at https://www.verisign.com/cps/testca (c)05 ou=For Test Purposes Only. No assurances. o=VeriSign\, Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of use at www.verisign.com/cps/testca (c)05 ou=TSWEB o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP

```
AIA: URL: http://ocsp.verisign.com CRL Distribution
Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start
date: 00:00:00 UTC Jul 19 2007 end date: 23:59:59 UTC
Aug 2 2007 Associated Trustpoints:
my.verisign.trustpoint ! Identity certificate received
from 3rd party vendor displayed above. CA Certificate
Status: Available Certificate Serial Number:
63b1a5cdc59f78801da0636cf975467b Certificate Usage:
General Purpose Public Key Type: RSA (2048 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test Root CA
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=VeriSign Trial Secure Server
Test CA ou=Terms of use at
https://www.verisign.com/cps/testca (c)05 ou=For Test
Purposes Only. No assurances. o=VeriSign\, Inc. c=US
Validity Date: start date: 00:00:00 UTC Feb 9 2005 end
date: 23:59:59 UTC Feb 8 2015 Associated Trustpoints:
my.verisign.trustpoint ! CA intermediate certificate
displayed above.
```

Verifique o certificado instalado para o WebVPN com um navegador da Web

A fim verificar que o WebVPN usa o certificado novo, termine estas etapas:

1. Conecte a sua relação WebVPN com um navegador da Web. Use https:// junto com o FQDN que você se usou para pedir o certificado (por exemplo, https://webvpn.cisco.com).Se você recebe uma destas alertas de segurança, execute o procedimento que corresponde àquele alerta:**O nome do Security Certificate é inválido ou não combina o nome do local**Verifique que você usou o FQDN/CN correto a fim conectar à relação WebVPN do ASA. Você deve usar o FQDN/CN que você definiu quando você pediu o certificado de identidade. Você pode usar o comando **cripto do trustpointname dos Certificados Ca da mostra** a fim verificar os Certificados FQDN/CN.**O Security Certificate foi emitido por uma empresa que você não escolheu confiar…**Termine estas etapas a fim instalar o certificado de raiz do vendedor da 3ª parte a seu navegador da Web:Na caixa de diálogo da alerta de segurança, clique o **certificado da vista**.Na caixa de diálogo do certificado, clique a aba do **trajeto do certificado**.Selecione o certificado de CA situado acima de seu certificado de identidade emitido, e clique o **certificado da vista**.O clique **instala o certificado**.No certificado instale a caixa de diálogo do assistente, clique **em seguida**.Selecione o **automaticamente seleto a loja do certificado baseada no tipo de** botão de rádio do **certificado**, clique-o **em seguida**, e clique-o então o **revestimento**.Clique **sim** quando você recebe a instalação a alerta da confirmação do certificado.Na operação da importação era a alerta bem sucedida, clica a **APROVAÇÃO**, e clica-a então **sim**.**Note**: Desde que este exemplo usa o certificado experimental de Verisign Verisign o certificado de raiz de CA experimental deve ser instalado a fim evitar erros da verificação quando os usuários conectam.
2. Fazer duplo clique o ícone do fechamento que aparece no canto inferior direito da página de login WebVPN.A informação instalada do certificado deve aparecer.
3. Reveja os índices para verificar que combina seu certificado dos vendedores da 3ª



parte.

Etapas para renovar o certificado SSL

Termine estas etapas a fim renovar o certificado SSL:

1. Selecione o confiança-ponto que você precisa de renovar.
2. Choose **registra-se**.Esta mensagem aparece:*Se é registrada com sucesso outra vez, o CERT atual estará substituído com os novos. Você quer continuar?*
3. Escolha **sim**.Isto gerará um CSR novo.
4. Envie o CSR a seu CA e importe então o CERT novo ID quando você o recebe de volta.
5. Remova e reaplique o confiança-ponto à interface externa.

Comandos

No ASA, você pode usar diversos comandos show na linha de comando verificar o estado de um certificado.

- **mostre o ponto confiável cripto Ca** — Os indicadores configuraram pontos confiáveis.

- **mostre o certificado Ca cripto** — Indica todos os Certificados instalados no sistema.
- **mostre crls criptos Ca** — Os indicadores puseram em esconderijo listas revogação de certificado (CRL).
- **rsa do mypubkey do show crypto key** — Indica todos os pares de chave de criptografia gerados.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estão aqui alguns possíveis erros que você pôde encontrar:

- **% do aviso: O CERT de CA não é encontrado. Os certs importados não puderam ser usable.INFORMATION: Certificado importado com sucesso**O certificado de CA não foi autenticado corretamente. Use o comando cripto do trustpointname do certificado Ca da mostra a fim verificar que o certificado de CA esteve instalado. Procure a linha que começa com o certificado de CA. Se o certificado de CA é instalado, verifique que provê o ponto confiável correto.
- ERRO: Não analisam gramaticalmente nem não verificam o certificado importadoEste erro pode ocorrer quando você instala o certificado de identidade e não tem o intermediário ou o certificado CA raiz correto autenticado com o ponto confiável associado. Você deve remover e reauthenticate com o intermediário ou o certificado CA raiz correto. Contacte seu vendedor da 3ª parte a fim verificar que você recebeu o certificado de CA correto.
- O certificado não contém a chave pública de uso geralEste erro pode ocorrer quando você tenta instalar seu certificado de identidade ao ponto confiável errado. Você tenta instalar um certificado de identidade inválido, ou o par de chaves associado com o ponto confiável não combina a chave pública contida no certificado de identidade. Use o comando **cripto do *trustpointname dos* Certificados Ca da mostra** a fim verificar que você instalou seu certificado de identidade ao ponto confiável correto. Procure a linha que indica *pontos confiáveis associados:* Se o ponto confiável errado está listado, use os procedimentos descritos neste documento a fim remover e para reinstalar ao ponto confiável apropriado, igualmente verifique que o keypair não tem a mudança desde que o CSR foi gerado.
- **Mensagem de erro: %PIX|ASA-3-717023 SSL não ajustou o certificado do dispositivo para o [trustpoint name] do ponto confiável**Este exibições de mensagem quando uma falha ocorrer quando você ajustar um certificado do dispositivo para o ponto confiável dado a fim autenticar a conexão SSL. Quando a conexão SSL vem acima, uma tentativa está feita para ajustar o certificado do dispositivo que será usado. Se uma falha ocorre, um Mensagem de Erro está registrado que inclua o ponto confiável configurado que deve ser usado para carregar o certificado do dispositivo e a razão para a falha.*nome do ponto confiável — Nome do ponto confiável para que o SSL não ajustou um certificado do dispositivo.***Ação recomendada:** Resolva a edição indicada pela razão relatada para a falha.Assegure-se de que o ponto confiável especificado esteja registrado e tenha um certificado do dispositivo.Certifique-se que o certificado do dispositivo é válido.Reenroll o ponto confiável, se for necessário.

Informações Relacionadas

- Como obter um certificado digital de Microsoft Windows CA usando o ASDM em um ASA
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems