O ASA 7.x instala manualmente certificados de terceiros para uso com o exemplo de configuração da WebVPN

Contents

Introduction

Este exemplo de configuração descreve como instalar manualmente um certificado digital de terceiros no ASA para uso com WebVPN. Um certificado de avaliação de versão é usado neste exemplo. Cada etapa contém o procedimento de aplicação ASDM e um exemplo de CLI.

Prerequisites

Requirements

Este documento exige que você tenha acesso a uma autoridade de certificação (AC) para a inscrição de certificado. Os fornecedores de CA de terceiros suportados são Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA e VeriSign.

Componentes Utilizados

Este documento usa um ASA 5510 que executa a versão de software 7.2(1) e a versão 5.2(1) do ASDM. No entanto, os procedimentos neste documento funcionam em qualquer dispositivo ASA executado 7.x com qualquer versão ASDM compatível.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Configurar

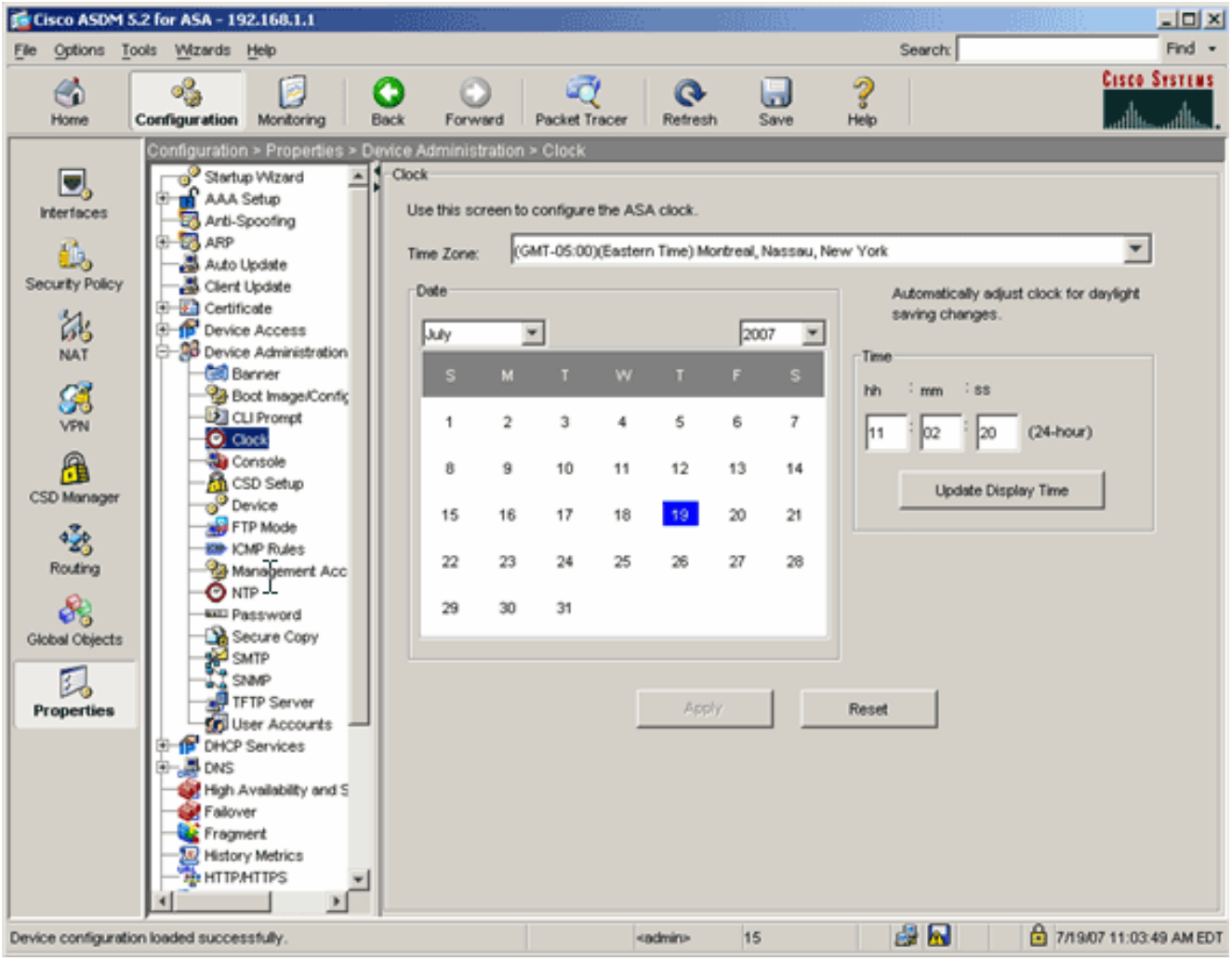
Para instalar um certificado digital de terceiros no PIX/ASA, faça o seguinte:

1. Verifique se os valores de data, hora e fuso horário estão corretos.
2. Gere o par de chaves RSA.
3. Crie o ponto de confiança.
4. Gerar a inscrição de certificado.
5. Autentique o ponto de confiança.
6. Instale o certificado.
7. Configure o WebVPN para usar o certificado recém-instalado.

Etapa 1. Verifique se os valores de data, hora e fuso horário estão corretos

Procedimento ASDM

1. Clique em Configuração e, em seguida, clique em Propriedades.
2. Expanda Administração de dispositivos e escolha Relógio.
3. Verifique se as informações listadas estão corretas.Os valores de Data, Hora e Fuso Horário devem ser precisos para que ocorra a validação adequada do certificado.



Exemplo de linha de comando

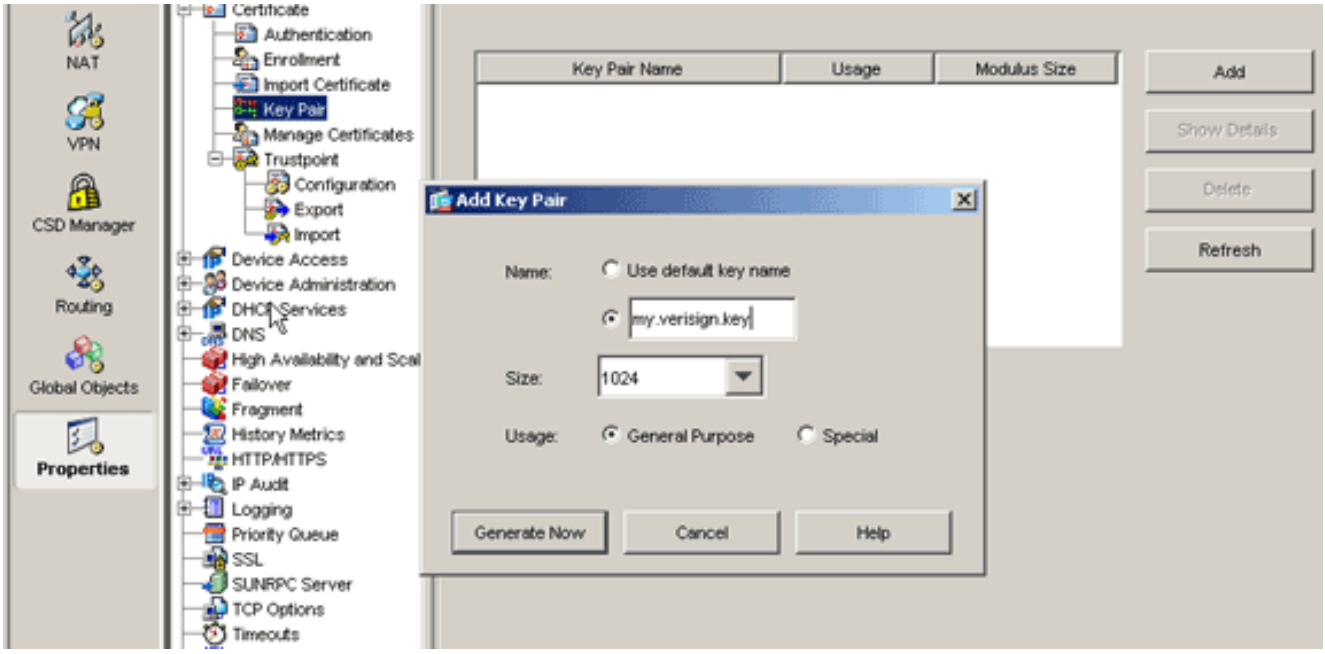
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

Etapa 2. Gerar o par de chaves RSA

A chave pública RSA gerada é combinada com as informações de identidade do ASA para formar uma solicitação de certificado PKCS#10. Você deve identificar distintamente o nome da chave com o ponto de confiança para o qual você cria o par de chaves.

Procedimento ASDM

1. Clique em **Configuração** e, em seguida, clique em **Propriedades**.
2. Expanda **Certificate** e escolha **Key Pair**.
3. Clique em
   Add.



4. Insira o nome da chave, escolha o tamanho do módulo e selecione o tipo de uso. Note: O tamanho recomendado do par de chaves é 1024.
5. Clique em **Gerar**.O par de chaves que você criou deve estar listado na coluna Nome do par de chaves.

Exemplo de linha de comando

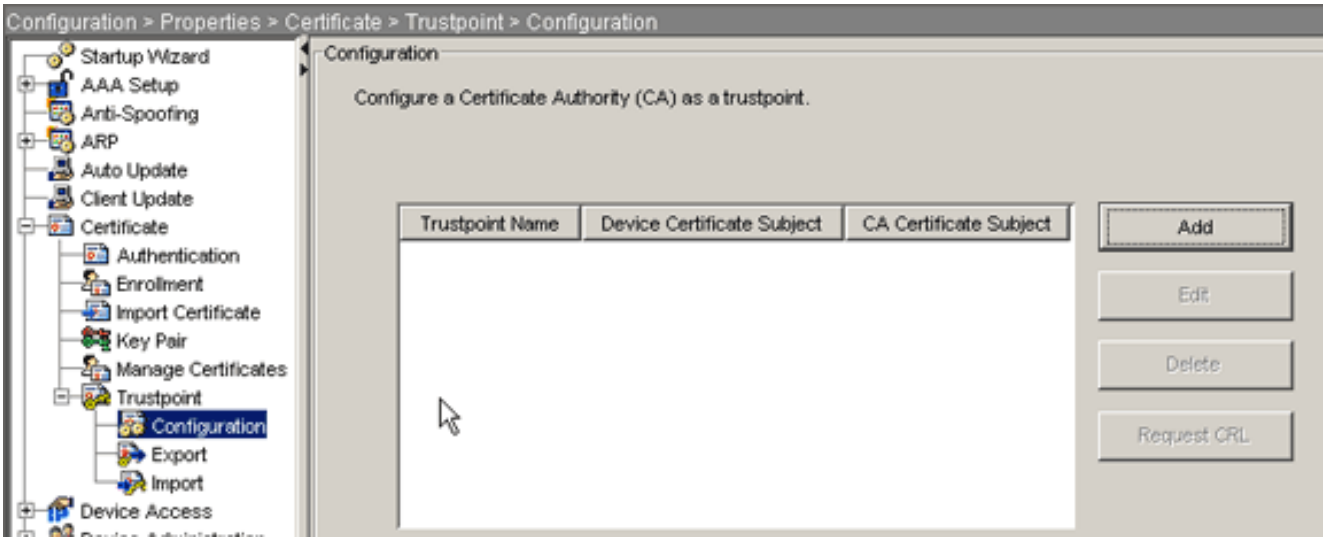
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

Etapa 3. Criar o ponto de confiança

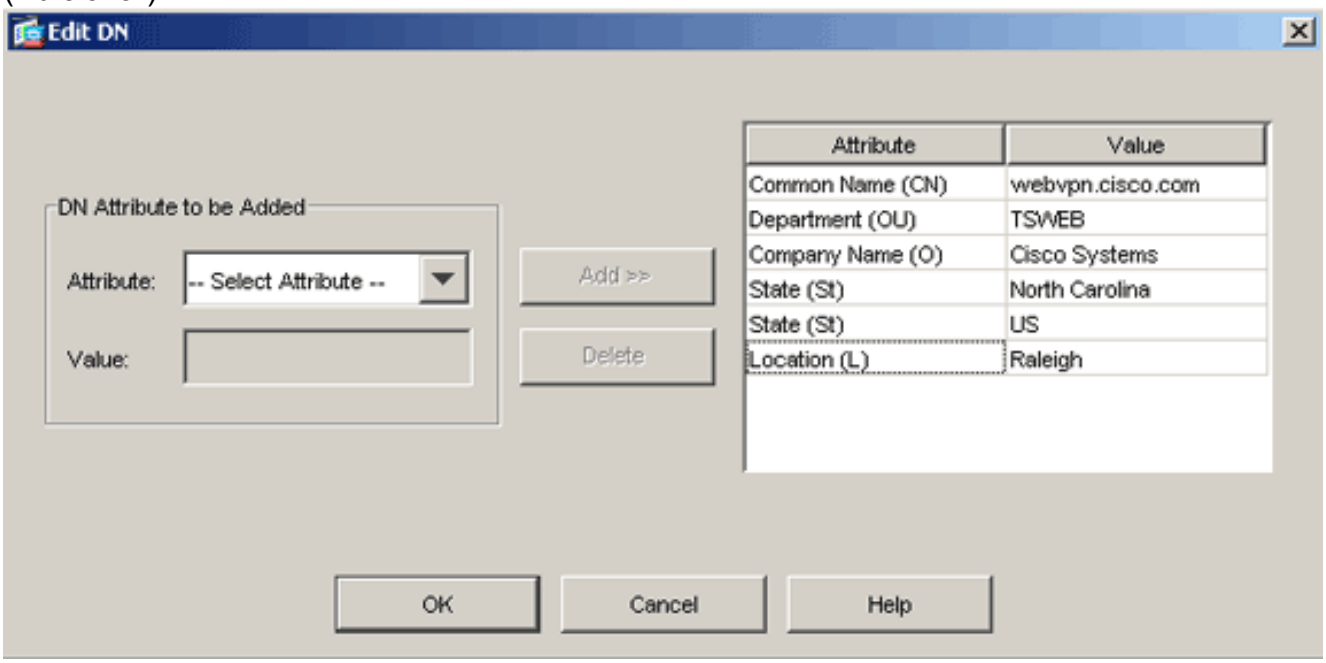
Os pontos de confiança são necessários para declarar a autoridade de certificação (CA) que o ASA usará.

Procedimento ASDM

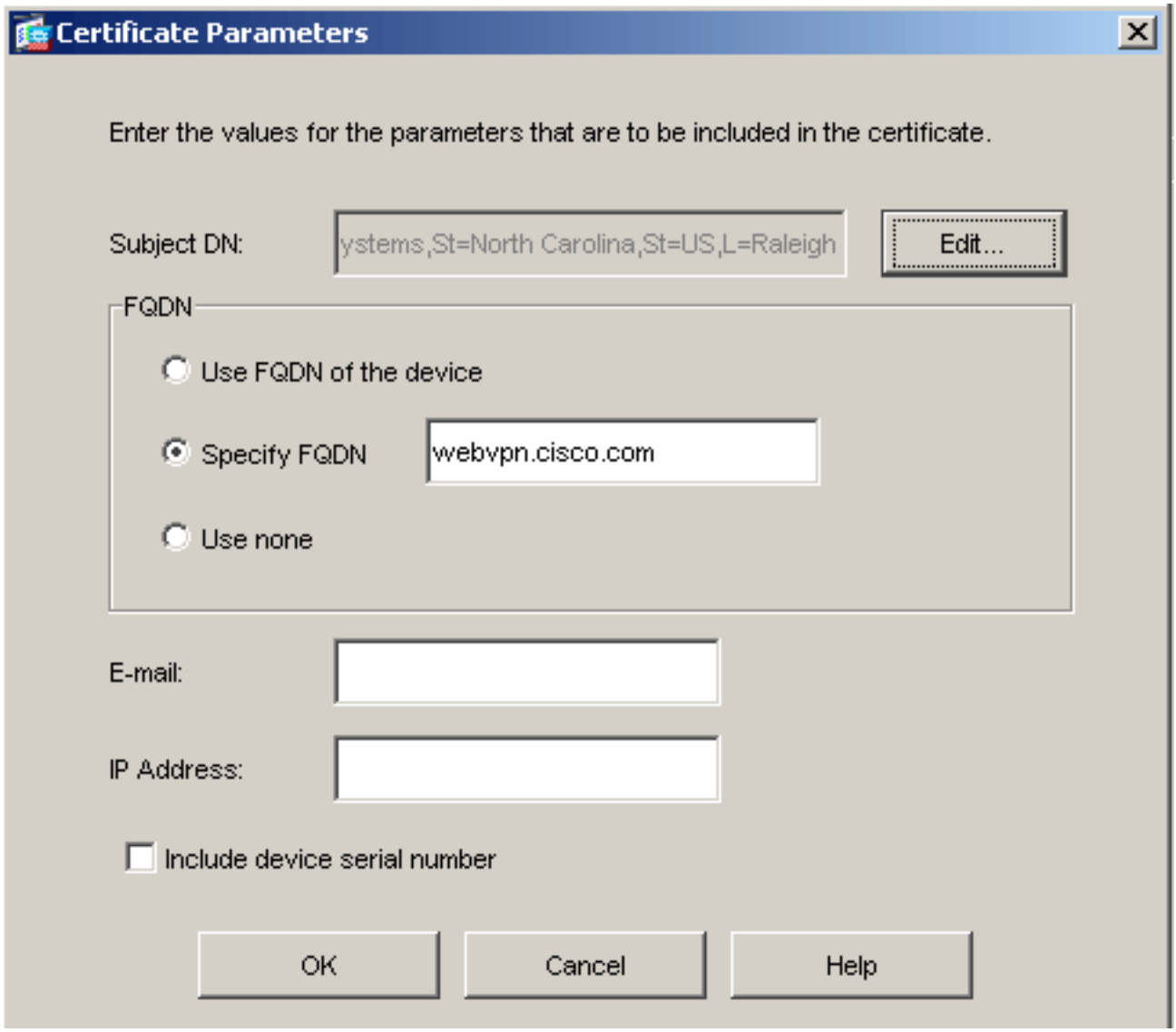
1. Clique em **Configuração** e, em seguida, clique em **Propriedades**.
2. Expanda **Certificate** e expanda **Trustpoint**.
3. Escolha **Configuração** e clique em **Adicionar**.



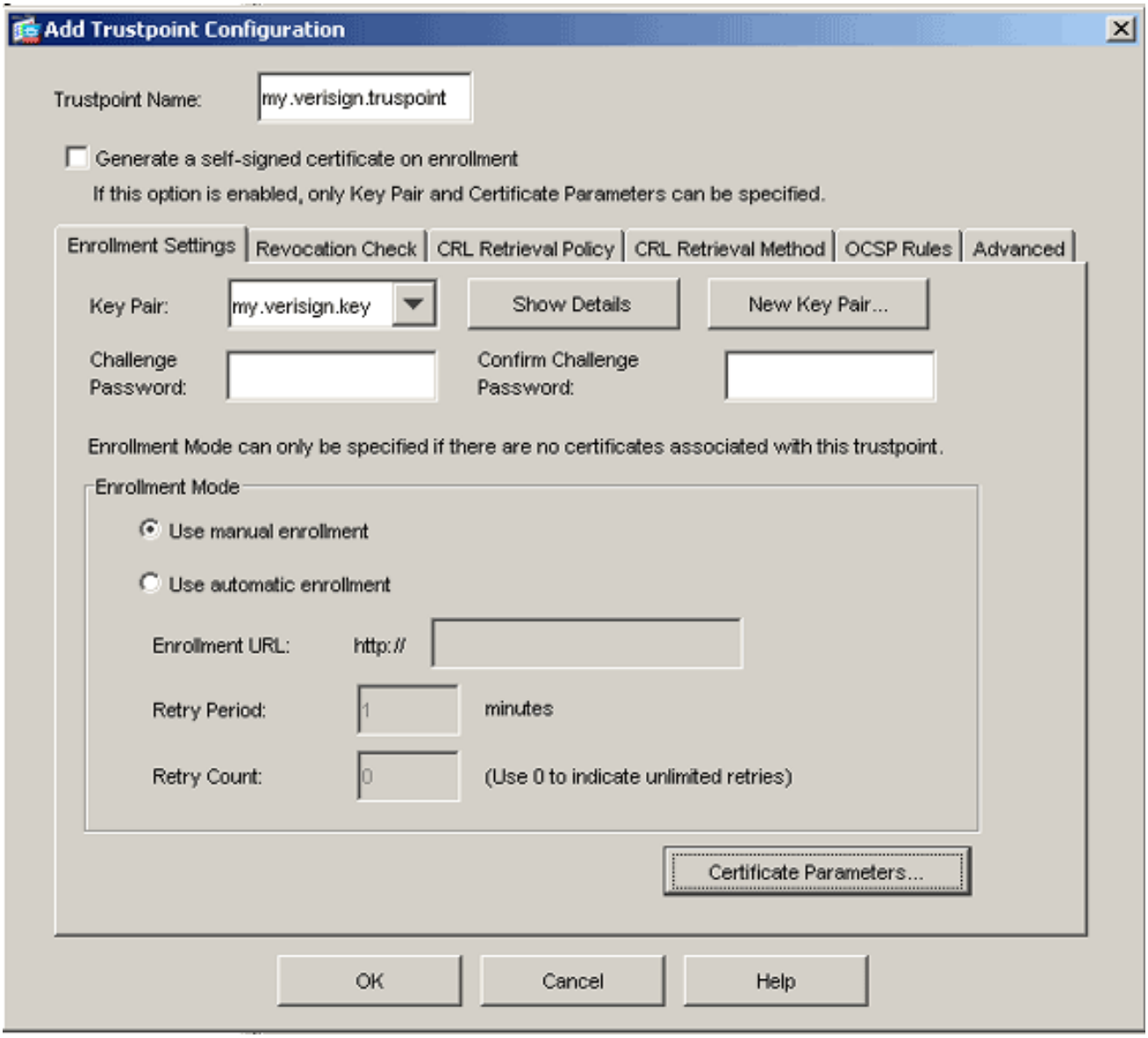
4. Configure estes valores:**Nome do ponto de confiança**: O nome do ponto confiável deve ser relevante para o uso pretendido. (Este exemplo usa *my.verisign.trustpoint*.)**Par chave**: Selecione o par de chaves gerado na Etapa 2. (*my.verisign.key*)
5. Verifique se a opção Inscrição manual está selecionada.
6. Clique em **Parâmetros de certificado**.A caixa de diálogo Parâmetros do certificado é exibida.
7. Clique em **Editar** e configure os atributos listados nesta tabela:Para configurar esses valores, escolha um valor na lista suspensa **Attribute (Atributo), insira o valor e clique em Add** (Adicionar).



8. Quando os valores adequados forem adicionados, clique em **OK**.
9. Na caixa de diálogo Parâmetros do certificado, insira o FQDN no campo Especificar FQDN.Esse valor deve ser o mesmo FQDN usado para o nome comum (CN).



10. Click **OK**.
11. Verifique se o par de chaves correto está selecionado e clique no botão de opção **Usar inscrição manual**.
12. Clique em **OK** e em **Aplicar**.



Exemplo de linha de comando

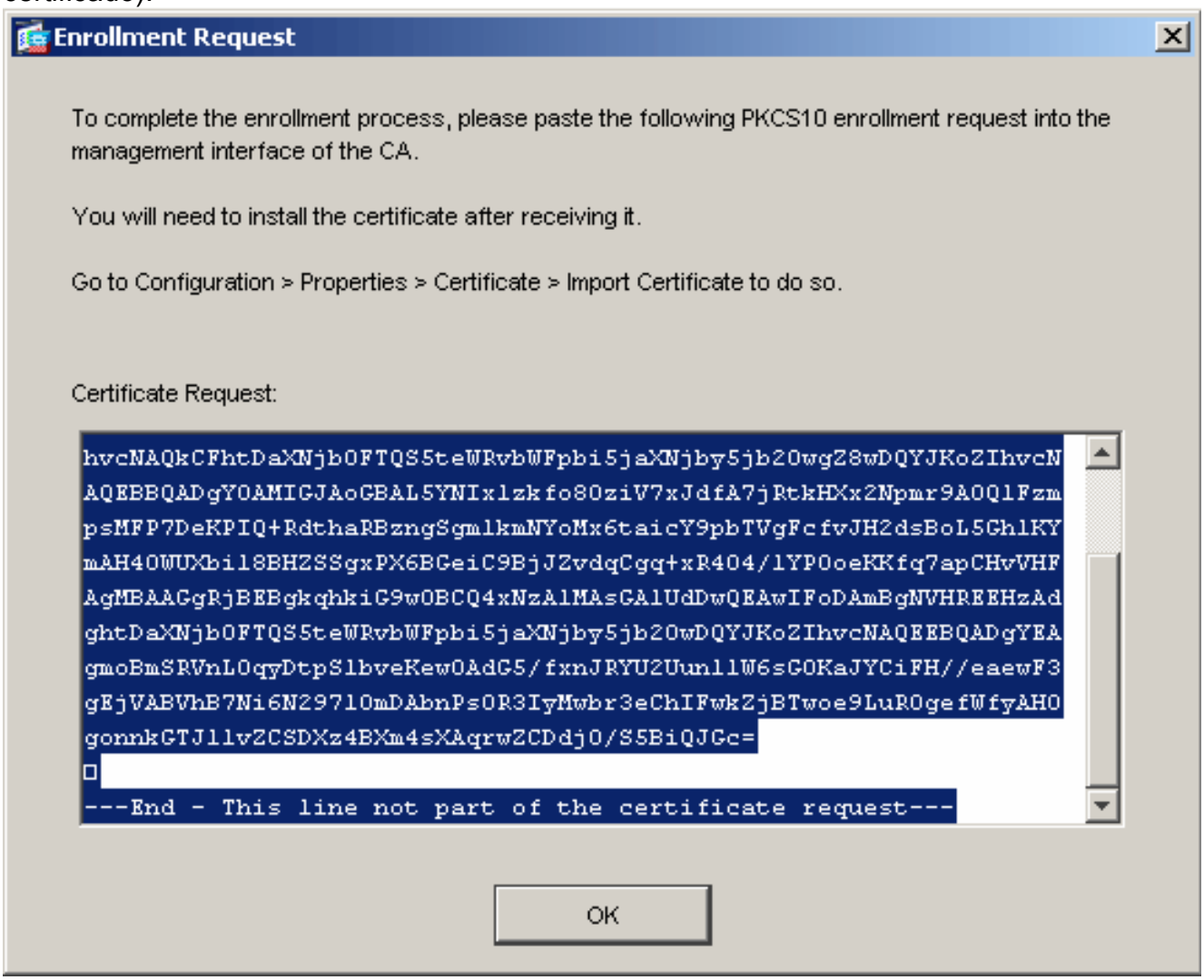
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco 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. Gerar a inscrição de certificado

Procedimento ASDM

1. Clique em **Configuração** e, em seguida, clique em **Propriedades**.
2. Expanda **Certificate** e escolha **Enrollment**.
3. Verifique se o ponto de confiança criado na Etapa 3 está selecionado e clique em **Inscrever**.Aparece uma caixa de diálogo que lista a solicitação de inscrição de certificado (também chamada de solicitação de assinatura de certificado).



4. Copie a solicitação de inscrição PKCS#10 em um arquivo de texto e envie o CSR ao fornecedor de terceiros apropriado.Depois que o fornecedor terceirizado receber o CSR, ele deverá emitir um certificado de identidade para instalação.

Exemplo de linha de comando

Nome do 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

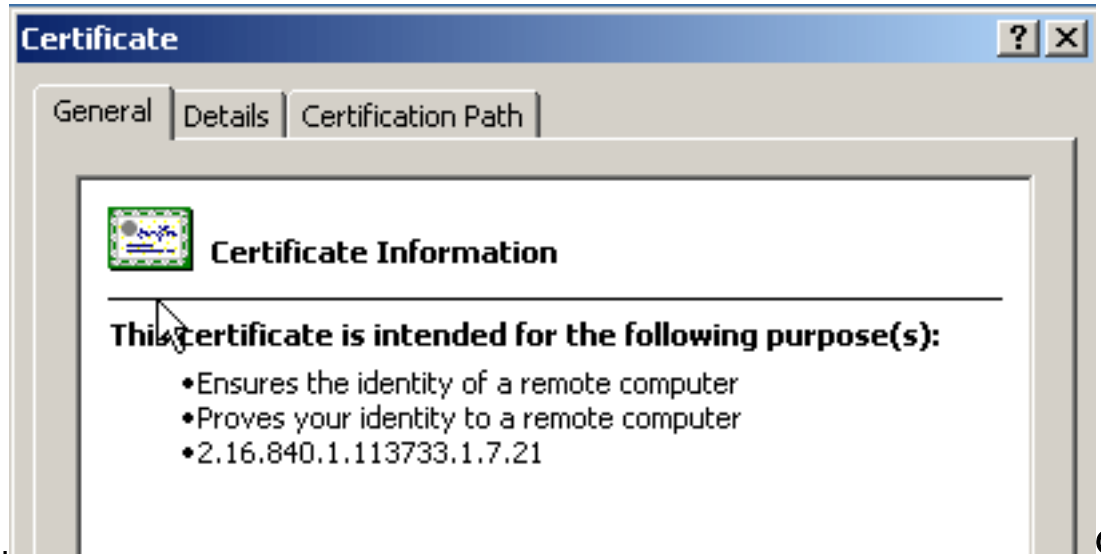
```
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the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

Etapa 5. Autenticar o ponto confiável

Depois de receber o certificado de identidade do fornecedor terceirizado, você pode prosseguir com esta etapa.

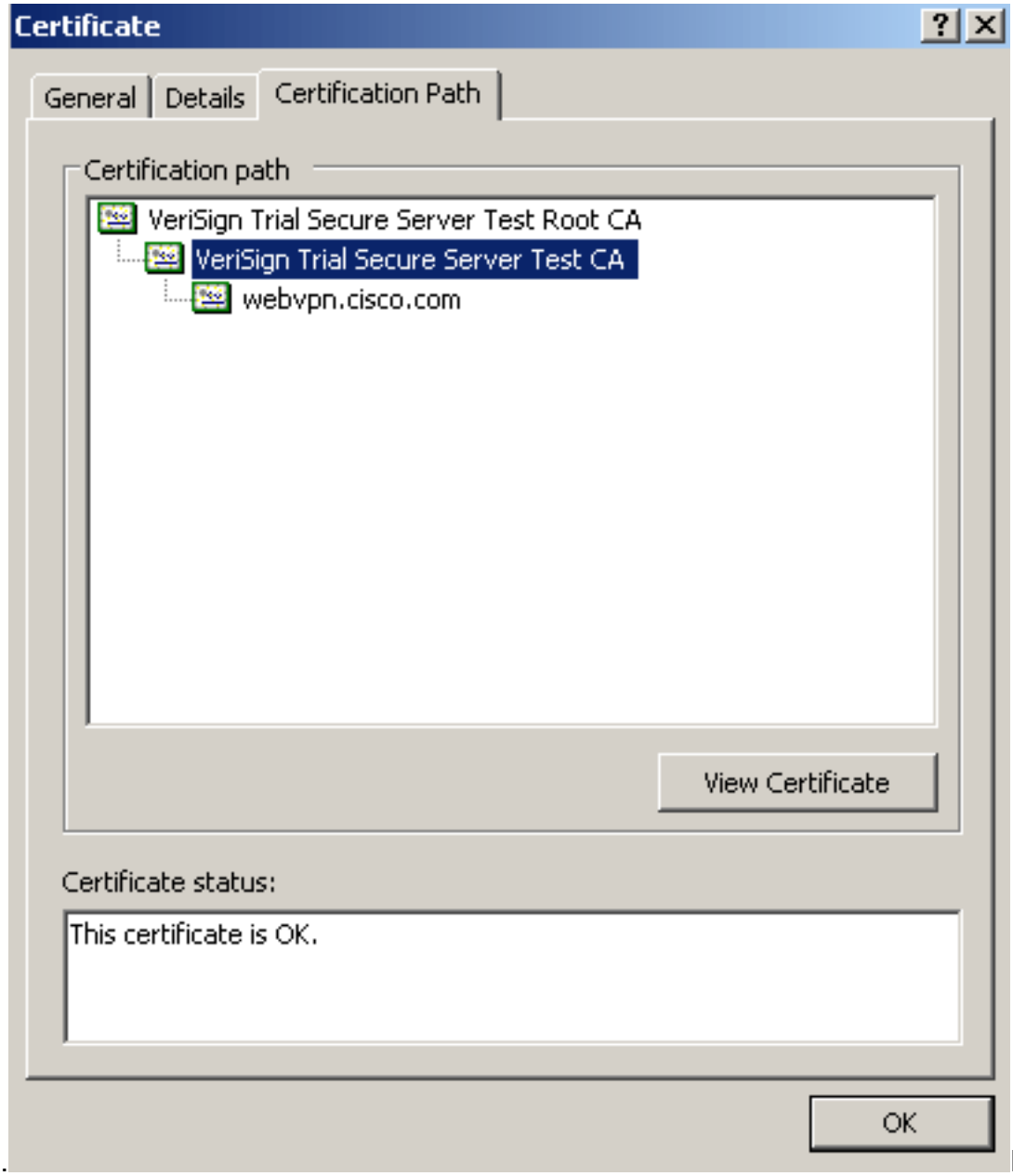
Procedimento ASDM

1. Salve o certificado de identidade no computador local.
2. Se você recebeu um certificado codificado em base64 que não veio como um arquivo, você deve copiar a mensagem base64 e colá-la em um arquivo de texto.
3. Renomeie o arquivo com uma extensão .cer.**Observação:** quando o arquivo for renomeado com a extensão .cer, o ícone do arquivo deverá ser exibido como um certificado.
4. Clique duas vezes no arquivo do certificado.A caixa de diálogo Certificado é

exibida. 

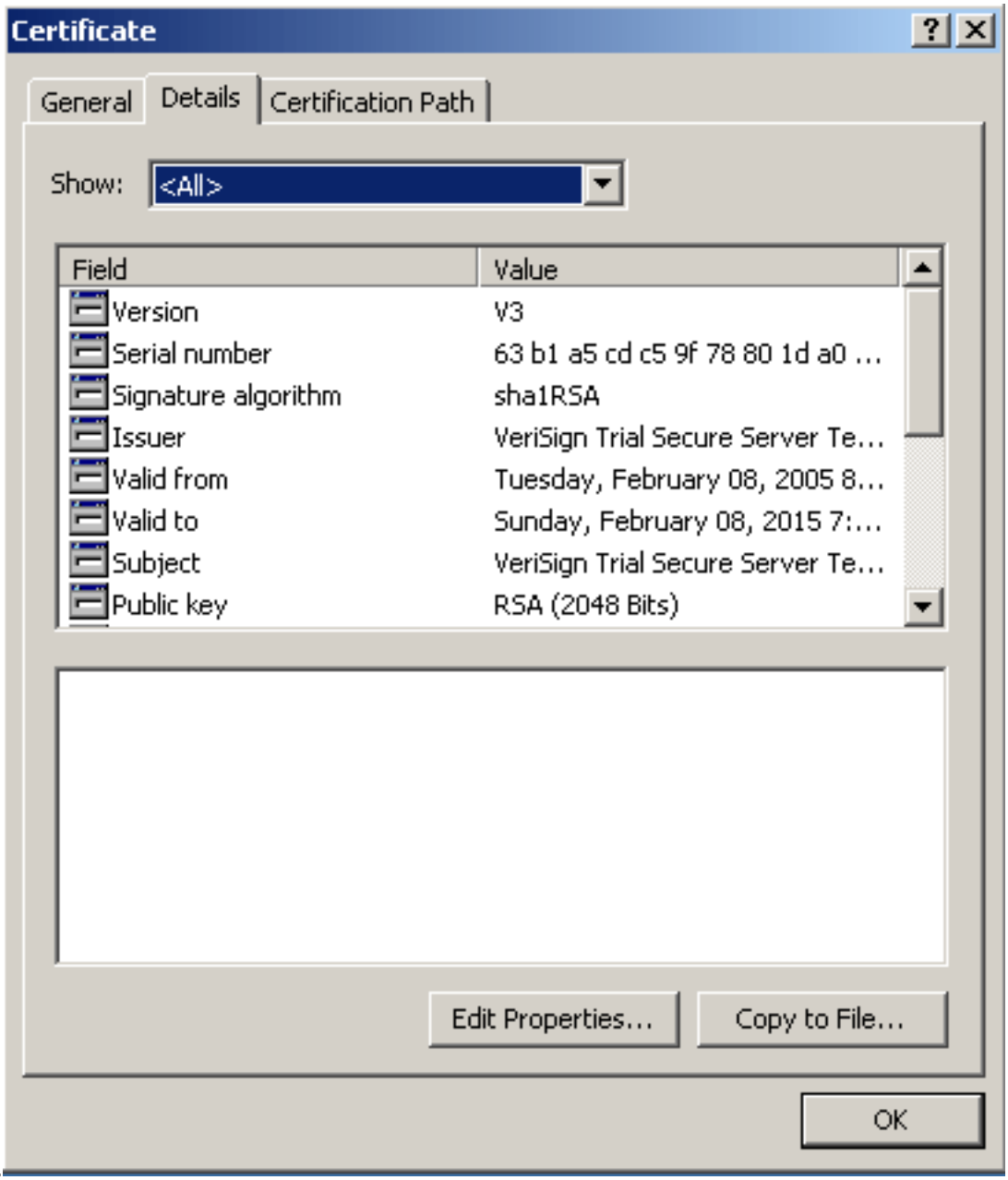
Observação: se a *mensagem* "*O Windows não tem informações suficientes para verificar esse certificado*" for exibida na guia Geral, você deverá obter a CA raiz de terceiros ou o certificado CA intermediário antes de continuar com este procedimento. Entre em contato com o fornecedor de terceiros ou o administrador de CA para obter a AC raiz ou o certificado de CA intermediário emissor.

5. Clique na guia **Caminho do certificado**.
6. Clique no certificado CA localizado acima do certificado de identidade emitido e clique em **Exibir**



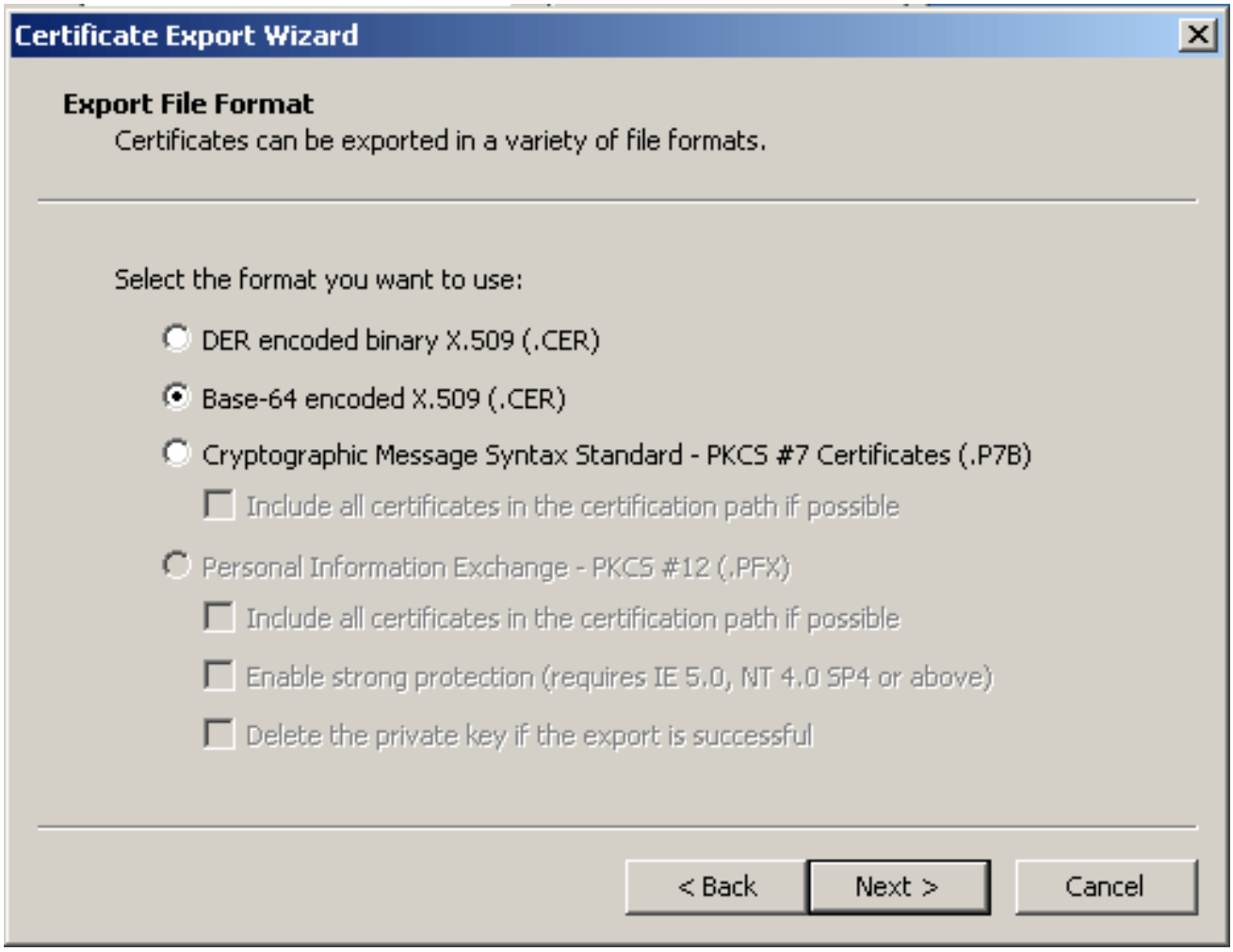
certificado. Informações detalhadas sobre o certificado CA intermediário são exibidas.**Aviso:** não instale o certificado de identidade (dispositivo) nesta etapa. Somente a raiz, raiz subordinada ou certificado CA são adicionados nesta etapa. Os certificados de identidade (dispositivo) estão instalados na Etapa 6.

7. Clique em

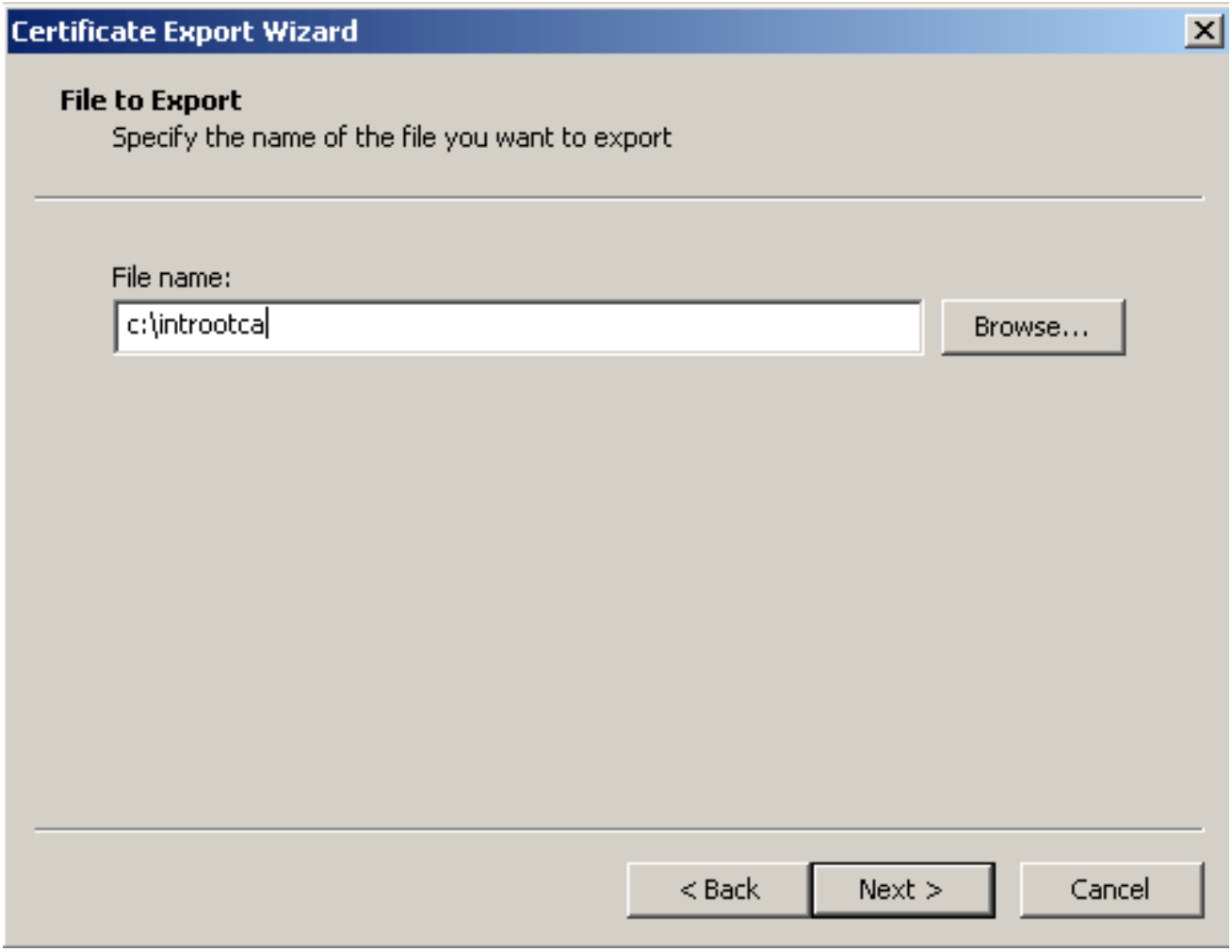


Details.

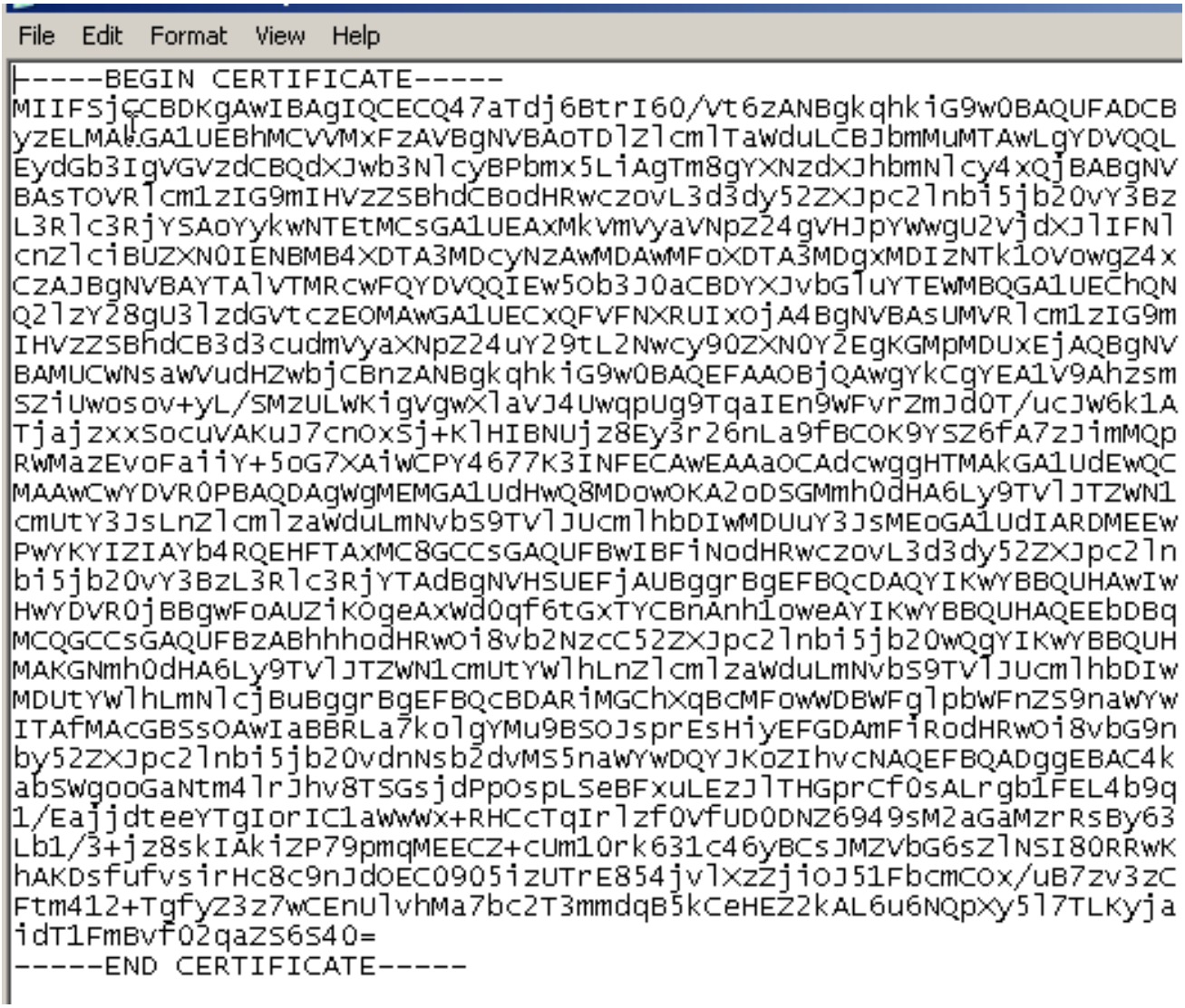
8. Clique em **Copiar para arquivo**.
9. No Assistente para exportação de certificado, clique em **Avançar.**
10. Na caixa de diálogo Export File Format (Exportar formato de arquivo), clique no botão de opção **X.509 (.CER)** codificado em Base**-64** e clique em **Next (Avançar)**.



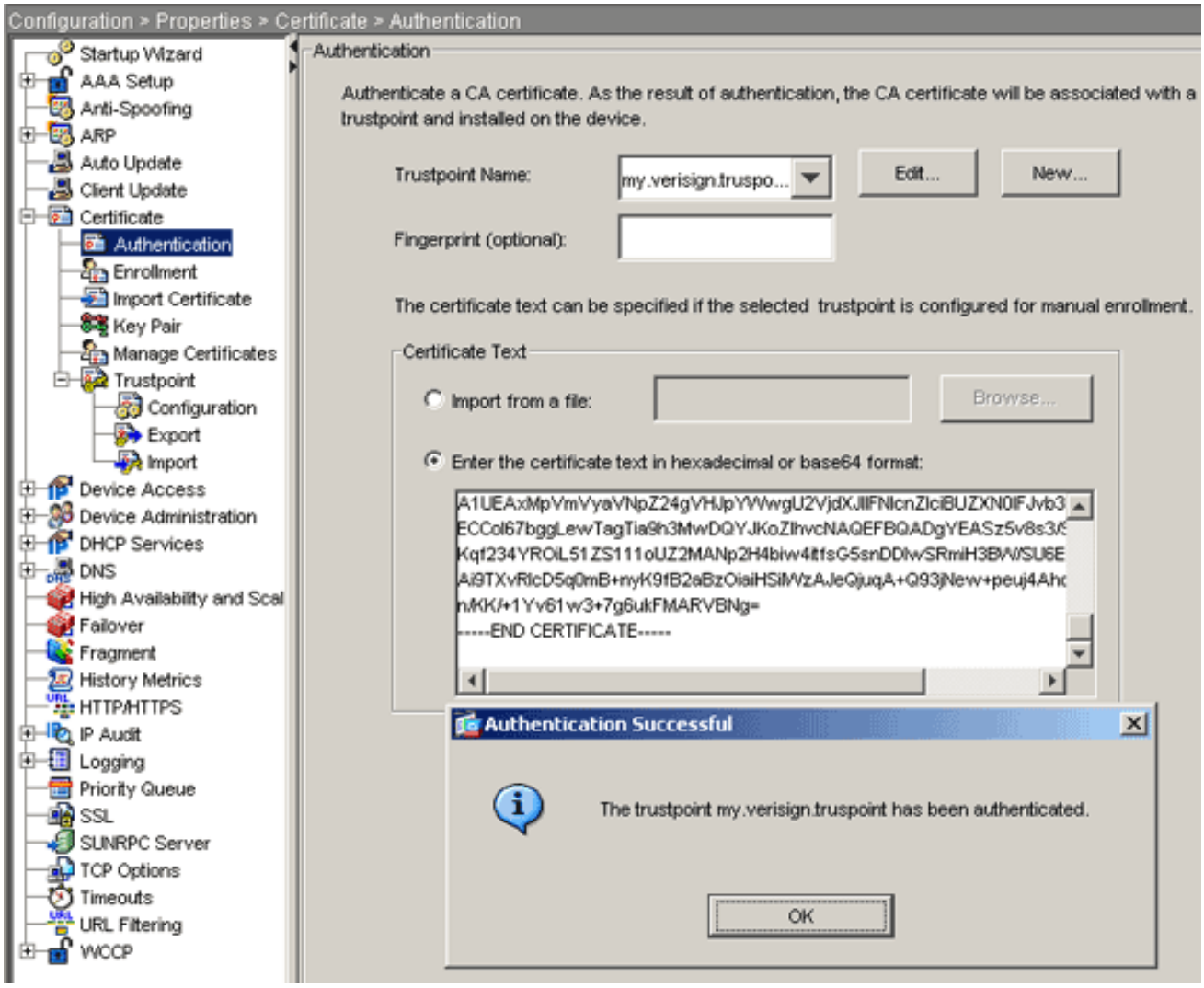
11. Insira o nome do arquivo e o local no qual deseja salvar o certificado CA.
12. Clique em Avançar e, em seguida, clique em Concluir.



13. Clique em **OK** na caixa de diálogo Exportar com êxito.
14. Navegue até o local onde você salvou o certificado CA.
15. Abra o arquivo com um editor de texto, como o Bloco de Notas. (Clique com o botão direito do mouse no arquivo e escolha **Enviar para > Bloco de Notas**.)A mensagem codificada em base64 deve ser semelhante ao certificado nesta
imagem:



16. No ASDM, clique em **Configuration** e em **Properties.**
17. Expanda **Certificate** e escolha **Authentication**.
18. Clique no botão de opção **Enter the certificate text in hexadecimal or base64 format**.
19. Cole o certificado CA formatado com base64 do editor de texto na área de texto.
20. Clique em
    Autenticar.



21. Click **OK**.

Exemplo de 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+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFN1Y3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFN1Y3VyZSBTZXJ2ZXIgVGVzdCBD
```

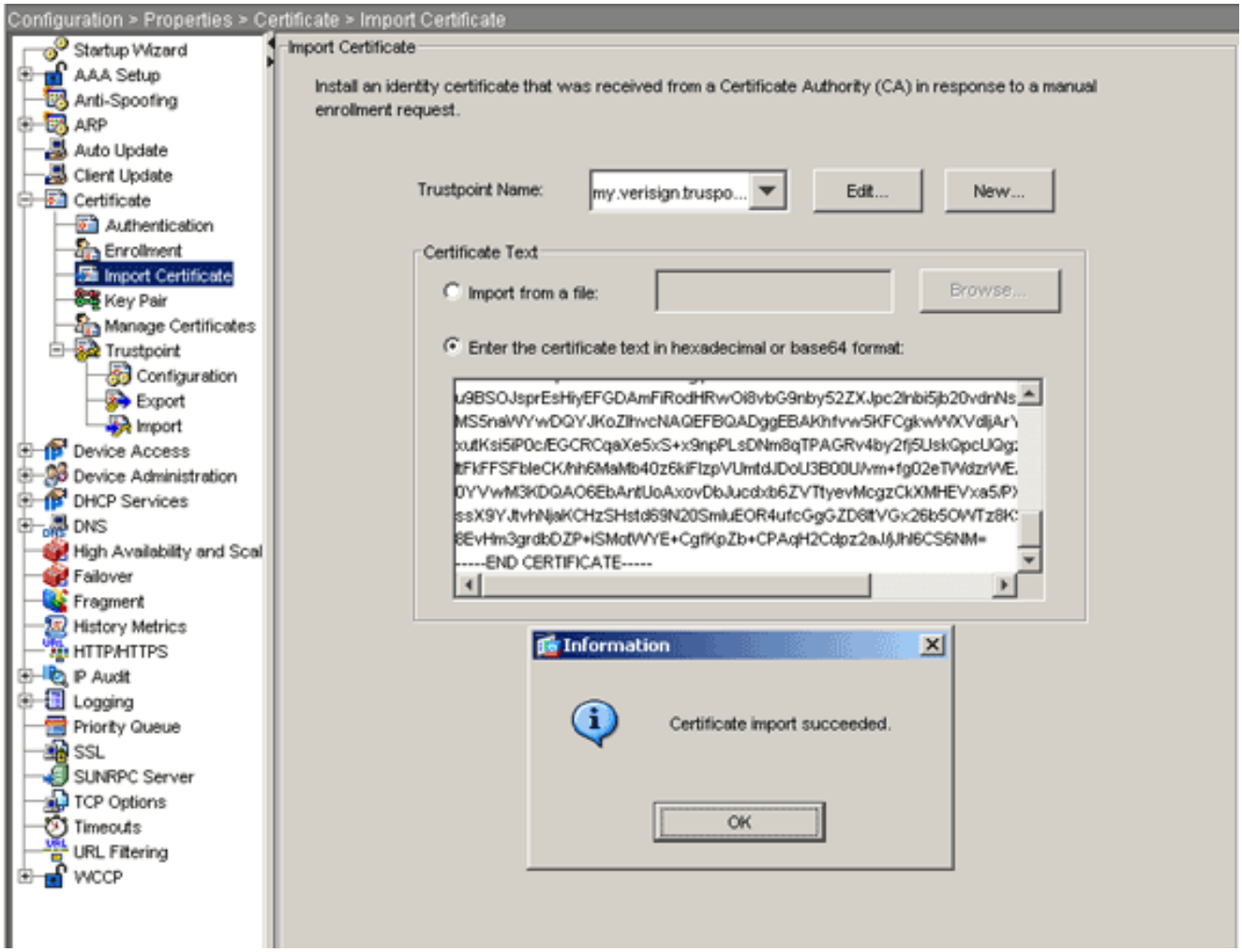
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
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. Instalar o certificado

Procedimento ASDM

Use o certificado de identidade fornecido pelo fornecedor terceirizado para executar estas etapas:

1. Clique em **Configuração** e, em seguida, clique em **Propriedades**.
2. Expanda **Certificate** e escolha **Import Certificate**.
3. Clique no botão de opção **Enter the certificate text in hexadecimal or base64 format** e cole o certificado de identidade base64 no campo de texto.



4. Clique em **Importar** e, em seguida, clique em **OK**.

Exemplo de linha de comando

ciscoasa

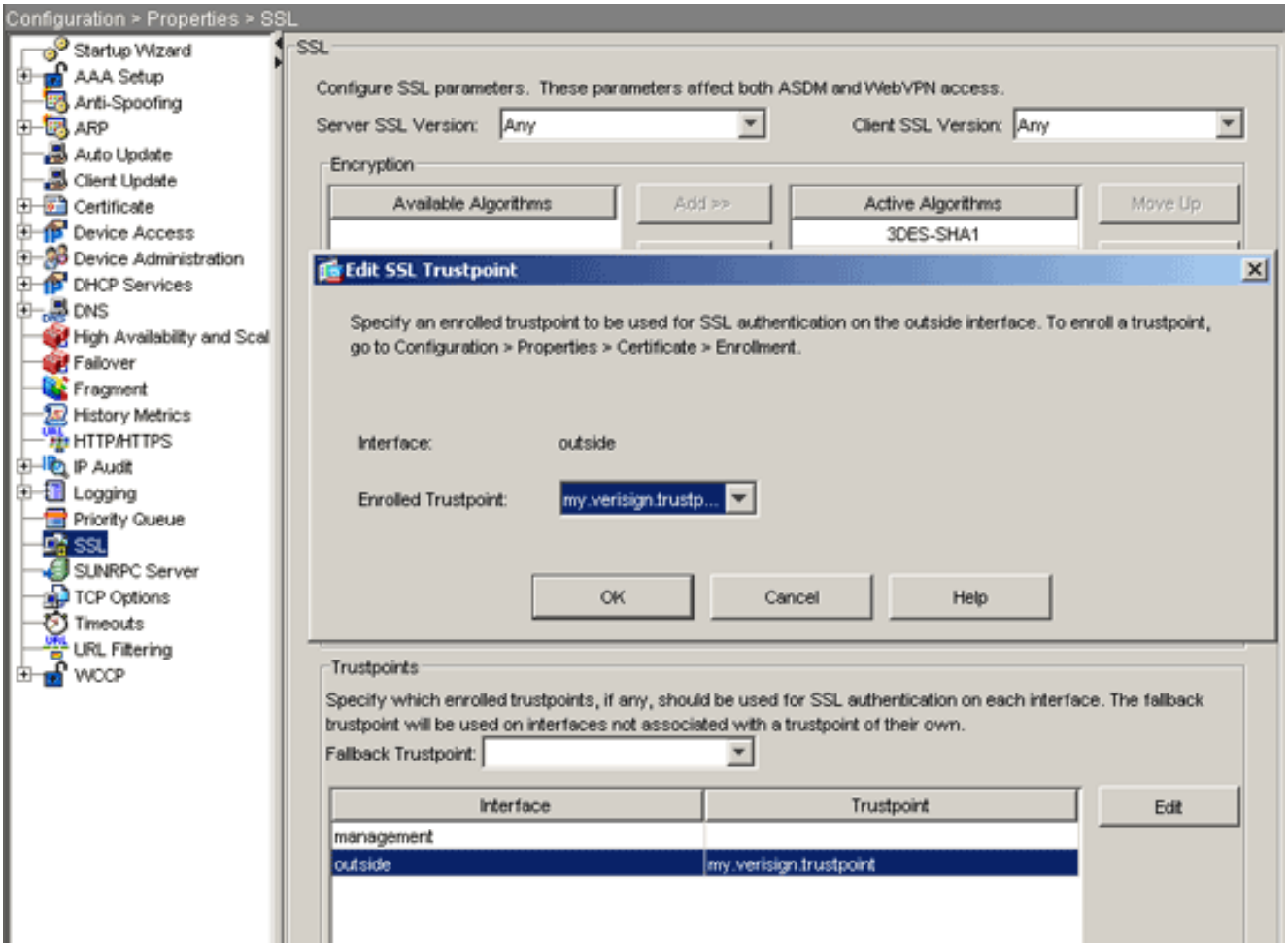
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! 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
dXJlIFN1
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)#
```

Passo 7. Configurar o WebVPN para usar o certificado recém-instalado

Procedimento ASDM

1. Clique em **Configuração**, clique em **Propriedades** e escolha **SSL**.
2. Na área Pontos confiáveis, selecione a interface que será usada para encerrar sessões WebVPN. (Este exemplo usa a interface externa.)
3. Clique em **Editar**.A caixa de diálogo Editar ponto de confiança SSL é exibida.



4. Na lista suspensa Ponto confiável inscrito, escolha o ponto confiável criado na Etapa 3.
5. Clique em **OK** e em **Aplicar**.

Seu novo certificado deve agora ser utilizado para todas as sessões WebVPN terminadas na interface especificada. Consulte a seção Verificar neste documento para obter informações sobre como verificar uma instalação bem-sucedida.

Exemplo de 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 se a instalação do certificado de fornecedor terceirizado foi bem-sucedida.

Substituir certificado autoassinado do ASA

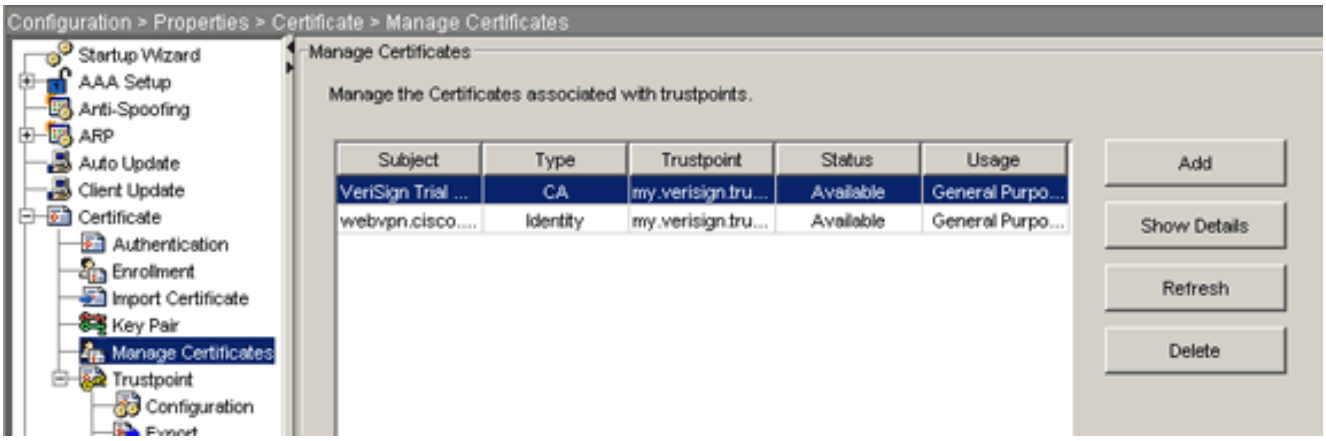
Esta seção descreve como substituir o certificado autoassinado instalado do ASA.

1. Emita uma solicitação de assinatura de certificado para Verisign.Depois de receber o certificado solicitado da Verisign, você poderá instalá-lo diretamente no mesmo ponto de confiança.
2. Digite este comando: **crypto ca enroll Verisign**Você é solicitado a responder às perguntas.
3. Para Exibir solicitação de certificado para terminal, insira **yes** e envie a saída para Verisign.
4. Depois de fornecer o novo certificado, digite este comando: **crypto ca import Verisign certificate**

Exibir certificados instalados

Procedimento ASDM

1. Clique em **Configuração** e clique em **Propriedades**.
2. Expanda **Certificado** e escolha **Gerenciar Certificados**.O certificado CA usado para autenticação de ponto confiável e o certificado de identidade emitido pelo fornecedor terceirizado devem aparecer na área Gerenciar certificados.



Exemplo de linha de comando

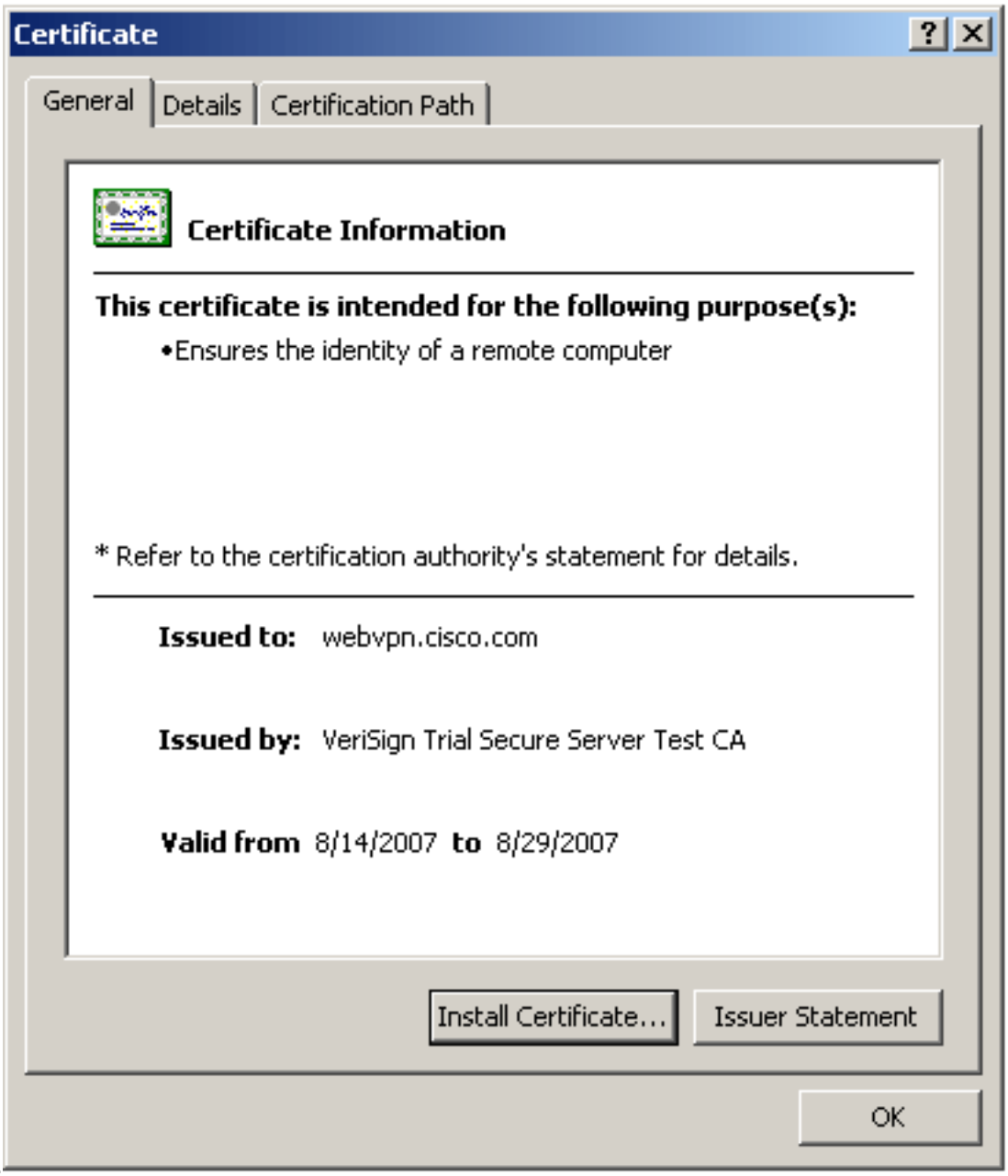
ciscoasa
ciscoasa(config)#**show crypto ca certificates** *! Displays all certificates installed on the ASA.* Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure 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.
```

Verificar o certificado instalado para WebVPN com um navegador da Web

Para verificar se o WebVPN usa o novo certificado, siga estas etapas:

1. Conecte-se à interface WebVPN por meio de um navegador da Web. Use https:// junto com o FQDN usado para solicitar o certificado (por exemplo, https://webvpn.cisco.com).Se você receber um desses alertas de segurança, execute o procedimento correspondente a esse alerta:**O nome do certificado de segurança é inválido ou não corresponde ao nome do site**Verifique se você usou o FQDN/CN correto para se conectar à interface WebVPN do ASA. Você deve usar o FQDN/CN que definiu quando solicitou o certificado de identidade. Você pode usar o comando **show crypto ca certificate trustpoint name** para verificar os certificados FQDN/CN.**O certificado de segurança foi emitido por uma empresa em que você não optou por confiar...**Conclua estes passos para instalar o certificado raiz de fornecedor terceirizado em seu navegador da Web:Na caixa de diálogo Alerta de segurança, clique em **Exibir certificado**.Na caixa de diálogo Certificado, clique na guia **Caminho do certificado**.Selecione o certificado CA localizado acima do certificado de identidade emitido e clique em **Exibir certificado**.Clique em **Install certificate** (Instalar certificado).Na caixa de diálogo Assistente de instalação de certificado, clique em **Avançar**.Selecione a opção **Selecionar automaticamente o arquivo de certificados com base no** botão de opção **tipo de certificado**, clique em **Avançar** e, em seguida, clique em **Concluir**.Clique em **Sim** quando receber o prompt de confirmação Install the certificate.No prompt A operação de importação foi bem-sucedida, clique em **OK** e, em seguida, clique em **Sim**.**Observação:** como este exemplo usa o certificado de avaliação de versão, o certificado raiz de CA de avaliação de versão deve ser instalado para evitar erros de verificação quando os usuários se conectam.
2. Clique duas vezes no ícone de cadeado exibido no canto inferior direito da página de login do WebVPN.As informações do certificado instalado devem ser exibidas.
3. Revise o conteúdo para verificar se ele corresponde ao certificado de

terceiros. 

Etapas para renovar o certificado SSL

Conclua estes passos para renovar o certificado SSL:

1. Selecione o ponto de confiança que precisa renovar.
2. Escolha **Inscrever-se**.Esta mensagem é exibida:*Se ele for inscrito com êxito novamente, o certificado atual será substituído pelos novos. Deseja continuar?*
3. Escolha **sim**.Isso gerará um novo CSR.
4. Envie o CSR para sua CA e importe o novo certificado de ID quando o receber de volta.
5. Remova e reaplique o ponto de confiança à interface externa.

Comandos

No ASA, você pode usar vários comandos show na linha de comando para verificar o status de um certificado.

- **show crypto ca trustpoint** — Exibe pontos confiáveis configurados.

- **show crypto ca certificate** — Exibe todos os certificados instalados no sistema.
- **show crypto ca crls** —Exibe listas de revogação de certificados em cache (CRL).
- **show crypto key mypubkey rsa** —Exibe todos os pares de chaves de criptografia gerados.

Troubleshoot

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

Aqui estão alguns possíveis erros que você pode encontrar:

- **% Aviso: Certificado CA não encontrado. Os certificados importados podem não ser utilizáveis.INFORMAÇÕES: Certificado importado com êxito**O certificado da AC não foi autenticado corretamente. Use o comando show crypto ca certificate trustpoint name para verificar se o certificado CA foi instalado. Procure a linha que começa com Certificado CA. Se o certificado CA estiver instalado, verifique se ele faz referência ao ponto de confiança correto.
- ERRO: Falha ao analisar ou verificar certificado importadoEsse erro pode ocorrer quando você instala o certificado de identidade e não tem o certificado CA raiz ou intermediário correto autenticado com o ponto de confiança associado. Você deve remover e reautenticar com o certificado CA intermediário ou raiz correto. Entre em contato com o fornecedor de terceiros para verificar se você recebeu o certificado de CA correto.
- O certificado não contém uma chave pública de finalidade geralEste erro pode ocorrer quando você tenta instalar seu certificado de identidade no ponto de confiança errado. Você tenta instalar um certificado de identidade inválido ou o par de chaves associado ao ponto de confiança não corresponde à chave pública contida no certificado de identidade. Use o comando **show crypto ca certificate** ***trustpoint name*** para verificar se você instalou seu certificado de identidade no ponto de confiança correto. Procure a linha que indica *Pontos de Confiança Associados:* Se o ponto de confiança errado estiver listado, use os procedimentos descritos neste documento para remover e reinstalar no ponto de confiança apropriado. Verifique também se o par de chaves não foi alterado desde que o CSR foi gerado.
- **Mensagem de Erro: %PIX|ASA-3-717023 SSL falhou ao definir o certificado do dispositivo para o ponto de confiança [nome do ponto de confiança]**Esta mensagem é exibida quando ocorre uma falha quando você define um certificado de dispositivo para o ponto confiável especificado para autenticar a conexão SSL. Quando a conexão SSL é ativada, é feita uma tentativa de definir o certificado do dispositivo que será usado. Se ocorrer uma falha, uma mensagem de erro será registrada que inclui o ponto confiável configurado que deve ser usado para carregar o certificado do dispositivo e o motivo da falha.*nome do ponto de confiança — nome do ponto de confiança para o qual o SSL falhou ao definir um certificado de dispositivo.***Ação recomendada:** Resolva o problema indicado pelo motivo reportado para a falha.Certifique-se de que o ponto confiável especificado esteja inscrito e tenha um certificado de dispositivo.Verifique se o certificado do dispositivo é válido.Registre novamente o ponto confiável, se necessário.

Informações Relacionadas

- Como obter um certificado digital de uma CA do Microsoft Windows usando o ASDM em um

ASA

- Avisos de campo do produto de segurança
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems