Ejemplo de Configuración de ASA 7.x Instalación Manual de Certificados de Proveedores de Terceros para su Uso con WebVPN

Contenido

Introducción

Este ejemplo de configuración describe cómo instalar manualmente un certificado digital de un proveedor externo en el ASA para su uso con WebVPN. En este ejemplo se utiliza un certificado de prueba de Verisign. Cada paso contiene el procedimiento de aplicación ASDM y un ejemplo de CLI.

Prerequisites

Requirements

Este documento requiere que tenga acceso a una autoridad de certificación (CA) para la inscripción de certificados. Los proveedores de CA de terceros admitidos son Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA y VeriSign.

Componentes Utilizados

Este documento utiliza un ASA 5510 que ejecuta la versión de software 7.2(1) y la versión ASDM 5.2(1). Sin embargo, los procedimientos de este documento funcionan en cualquier dispositivo ASA que ejecute 7.x con cualquier versión ASDM compatible.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

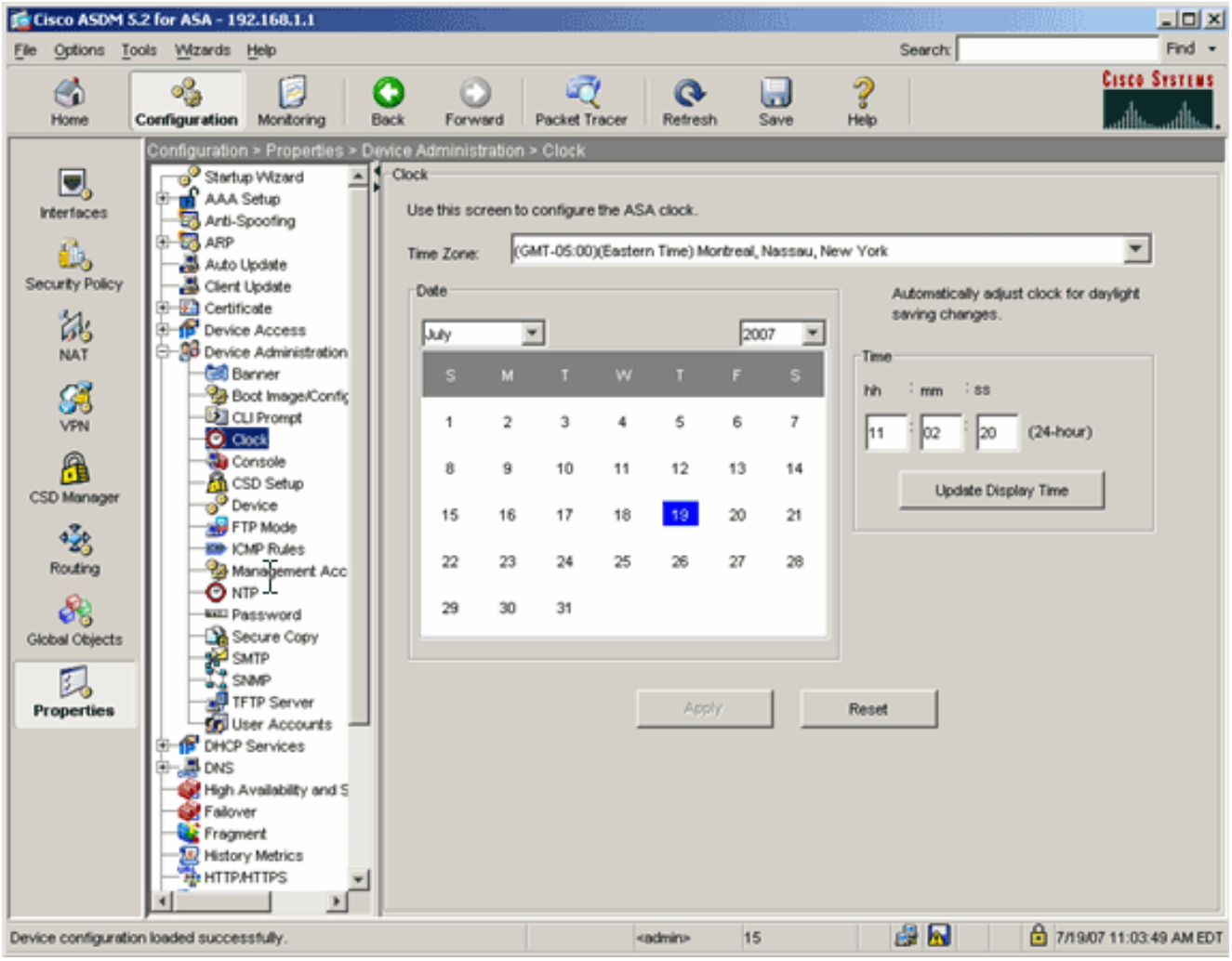
Para instalar un certificado digital de un proveedor externo en el PIX/ASA, complete estos pasos:

1. Verifique que los valores de fecha, hora y zona horaria sean Precisos.
2. Genere el Par de Llaves RSA.
3. Cree el Trustpoint.
4. Genere la inscripción de certificados.
5. Autentique el Trustpoint.
6. Instale el certificado.
7. Configure WebVPN para Utilizar el Certificado recién Instalado.

Paso 1. Verifique que los valores de la fecha, hora y zona horaria sean precisos

Procedimiento ASDM

1. Haga clic en Configuration (Configuración) y, a continuación, en Properties (Propiedades).
2. Expanda Device Administration (Administración de dispositivos) y elija Clock (Reloj).
3. Verifique que la información enumerada sea exacta.Los valores de Fecha, Hora y Zona horaria deben ser exactos para que se produzca la validación correcta del certificado.



Ejemplo de línea de comandos

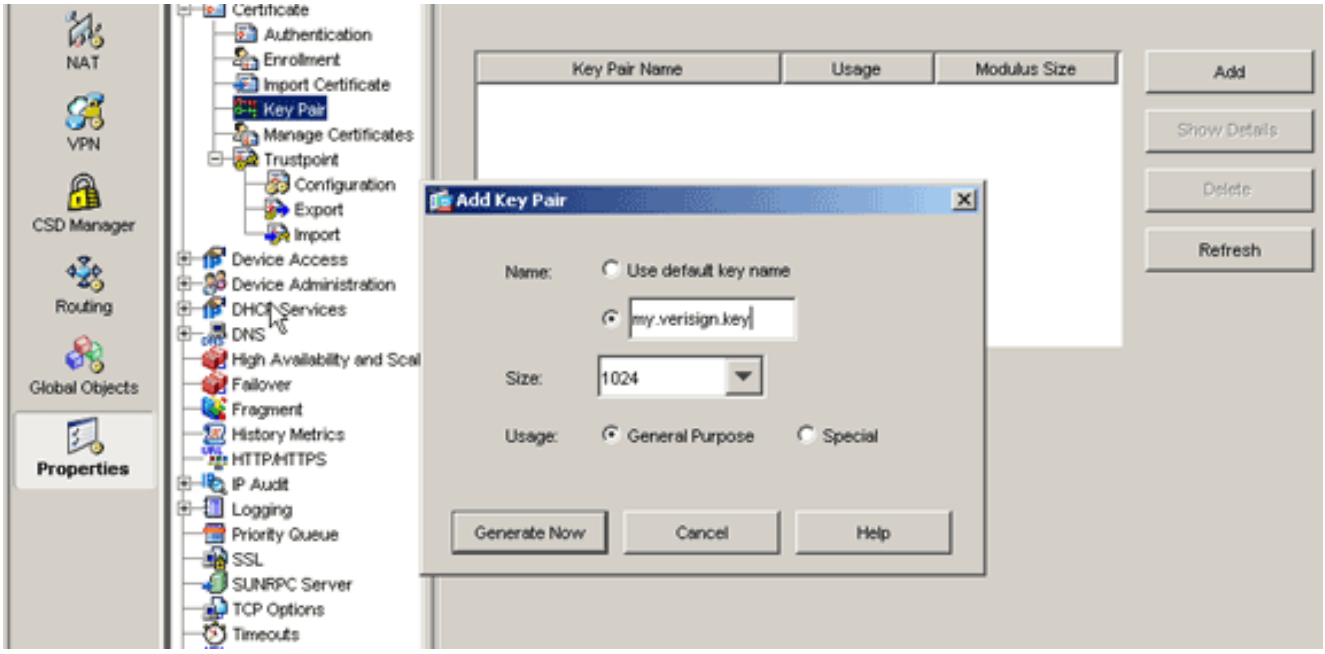
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

Paso 2. Generar el Par de Llaves RSA

La clave pública RSA generada se combina con la información de identidad de ASA para formar una solicitud de certificado PKCS#10. Debe identificar claramente el nombre de la clave con el punto de confianza para el que crea el par de claves.

Procedimiento ASDM

1. Haga clic en **Configuration** y, a continuación, haga clic en **Properties**.
2. Expanda **Certificate** y elija **Key Pair**.
3. Haga clic en Add
   (Agregar).



4. Introduzca el nombre de la clave, elija el tamaño del módulo y seleccione el tipo de uso. Nota: El tamaño del par de claves recomendado es 1024.
5. Haga clic en **Generar**.El par de claves que ha creado debe aparecer en la columna Nombre del par de claves.

Ejemplo de línea de comandos

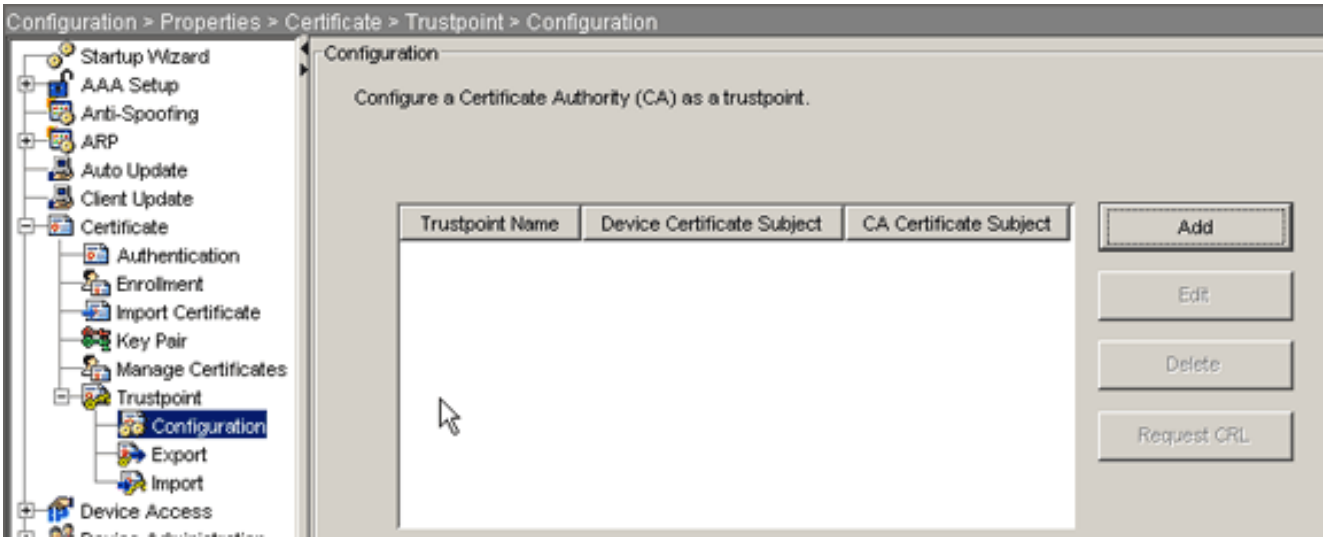
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

Paso 3. Crear el punto de confianza

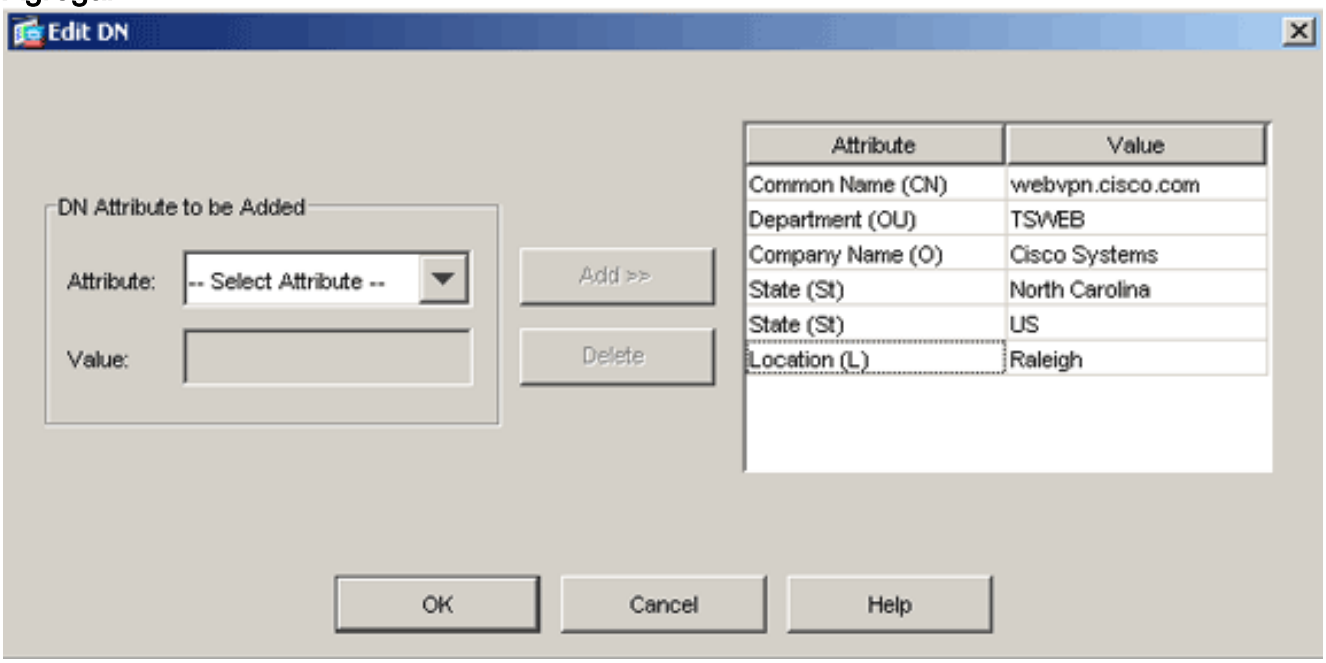
Se necesitan puntos de confianza para declarar la Autoridad de Certificación (CA) que utilizará su ASA.

Procedimiento ASDM

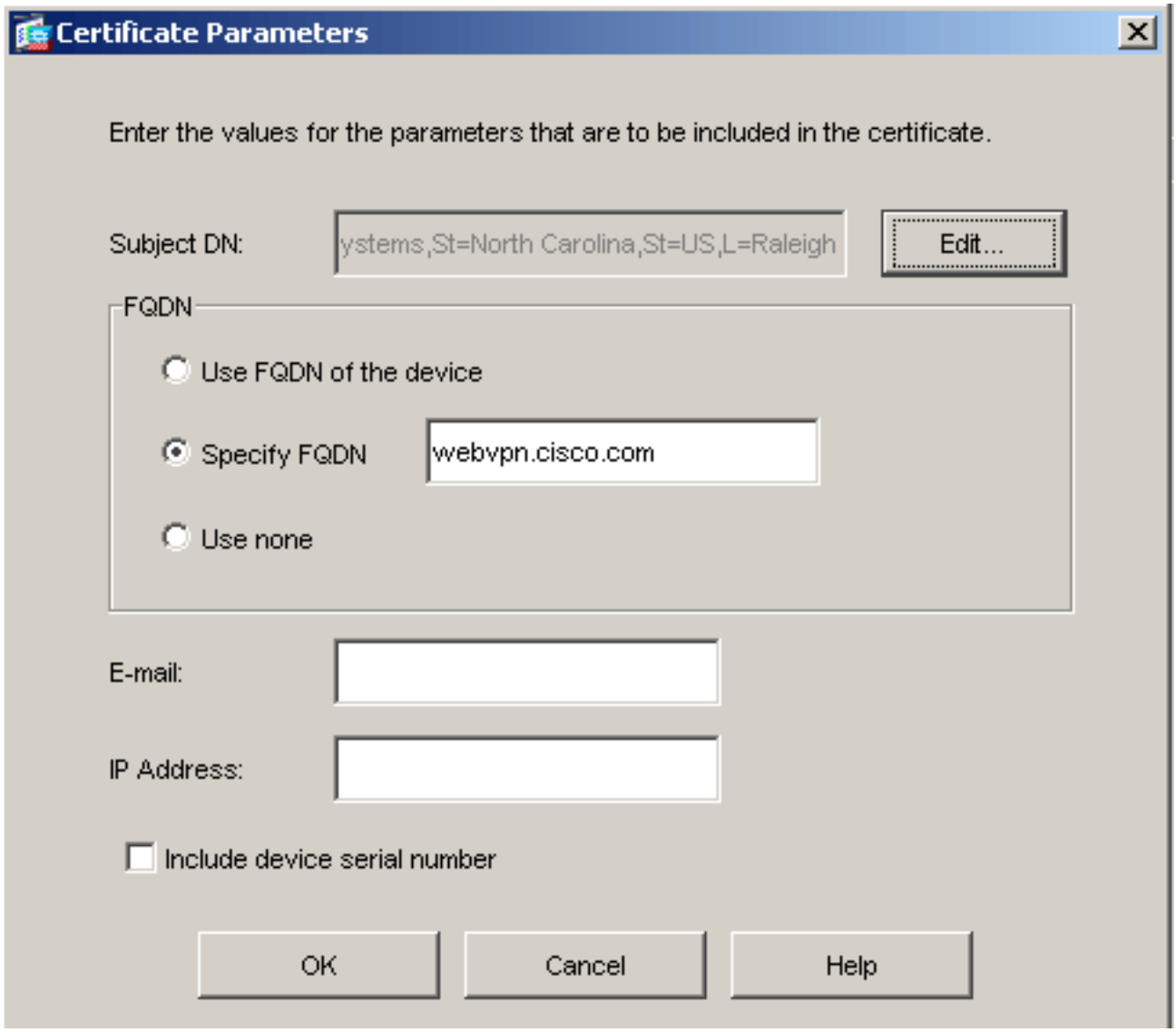
1. Haga clic en **Configuration** y, a continuación, haga clic en **Properties**.
2. Expanda **Certificate** y luego **Trustpoint**.
3. Elija **Configuration**, y haga clic en **Add**.



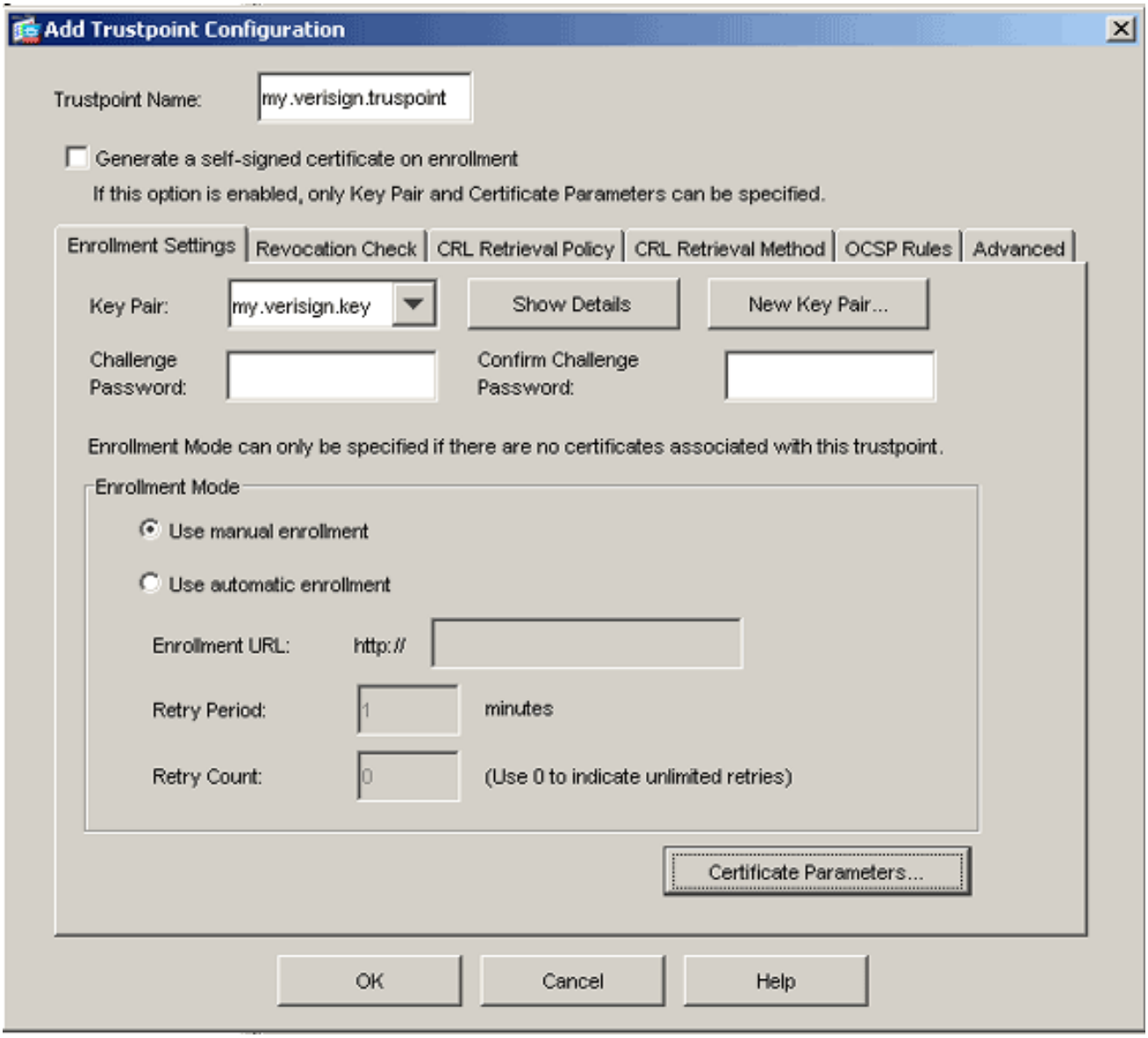
4. Configure estos valores:**Nombre del punto de confianza**: El nombre del punto de confianza debe ser relevante para el uso esperado. (Este ejemplo utiliza *my.verisign.trustpoint.*)**Par de claves**: Seleccione el par de claves generado en el Paso 2. (*my.verisign.key*)
5. Asegúrese de que la inscripción manual esté seleccionada.
6. Haga clic en **Parámetros de certificado**.Aparecerá el cuadro de diálogo Parámetros de certificado.
7. Haga clic en **Editar** y configure los atributos enumerados en esta tabla:Para configurar estos valores, elija un valor de la lista desplegable Atributo, ingrese el valor y haga clic en **Agregar**.



8. Una vez agregados los valores adecuados, haga clic en **Aceptar**.
9. En el cuadro de diálogo Parámetros de certificado, introduzca el FQDN en el campo Especificar FQDN.Este valor debe ser el mismo FQDN que utilizó para el nombre común (CN).



10. Click OK.
11. Verifique que el par de claves correcto esté seleccionado y haga clic en el botón de opción **Usar inscripción manual**.
12. Haga clic en **Aceptar** y luego en **Aplicar**.



Ejemplo de línea de comandos

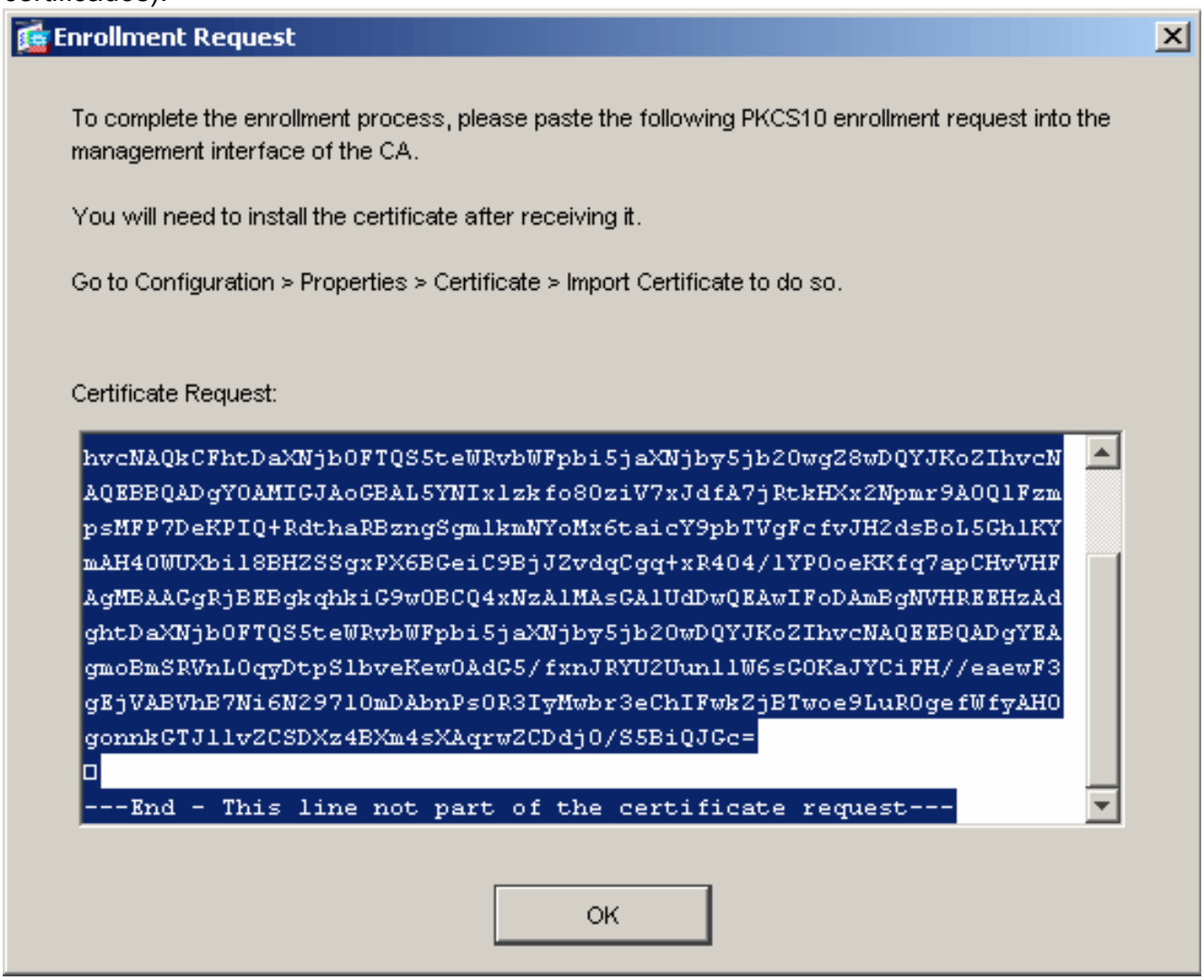
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco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

Paso 4. Generar inscripción de certificados

Procedimiento ASDM

1. Haga clic en **Configuration** y, a continuación, haga clic en **Properties**.
2. Expanda **Certificate** y elija **Enrollment**.
3. Verifique que el Trustpoint creado en el Paso 3 esté seleccionado y haga clic en **Inscribirse**.Aparece un cuadro de diálogo que muestra la solicitud de inscripción de certificados (también denominada solicitud de firma de certificados).



4. Copie la solicitud de inscripción PKCS#10 en un archivo de texto y, a continuación, envíe la CSR al proveedor de terceros adecuado.Después de que el proveedor externo reciba la CSR, debe emitir un certificado de identidad para la instalación.

Ejemplo de línea de comandos

Nombre del 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

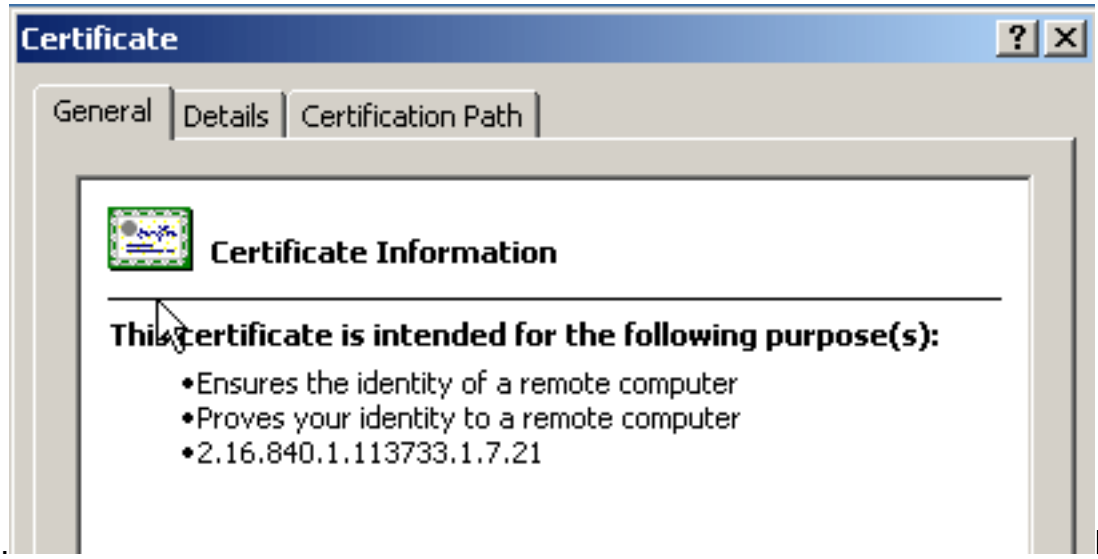
```
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the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

Paso 5. Autenticar el punto de confianza

Una vez que reciba el certificado de identidad del proveedor externo, puede continuar con este paso.

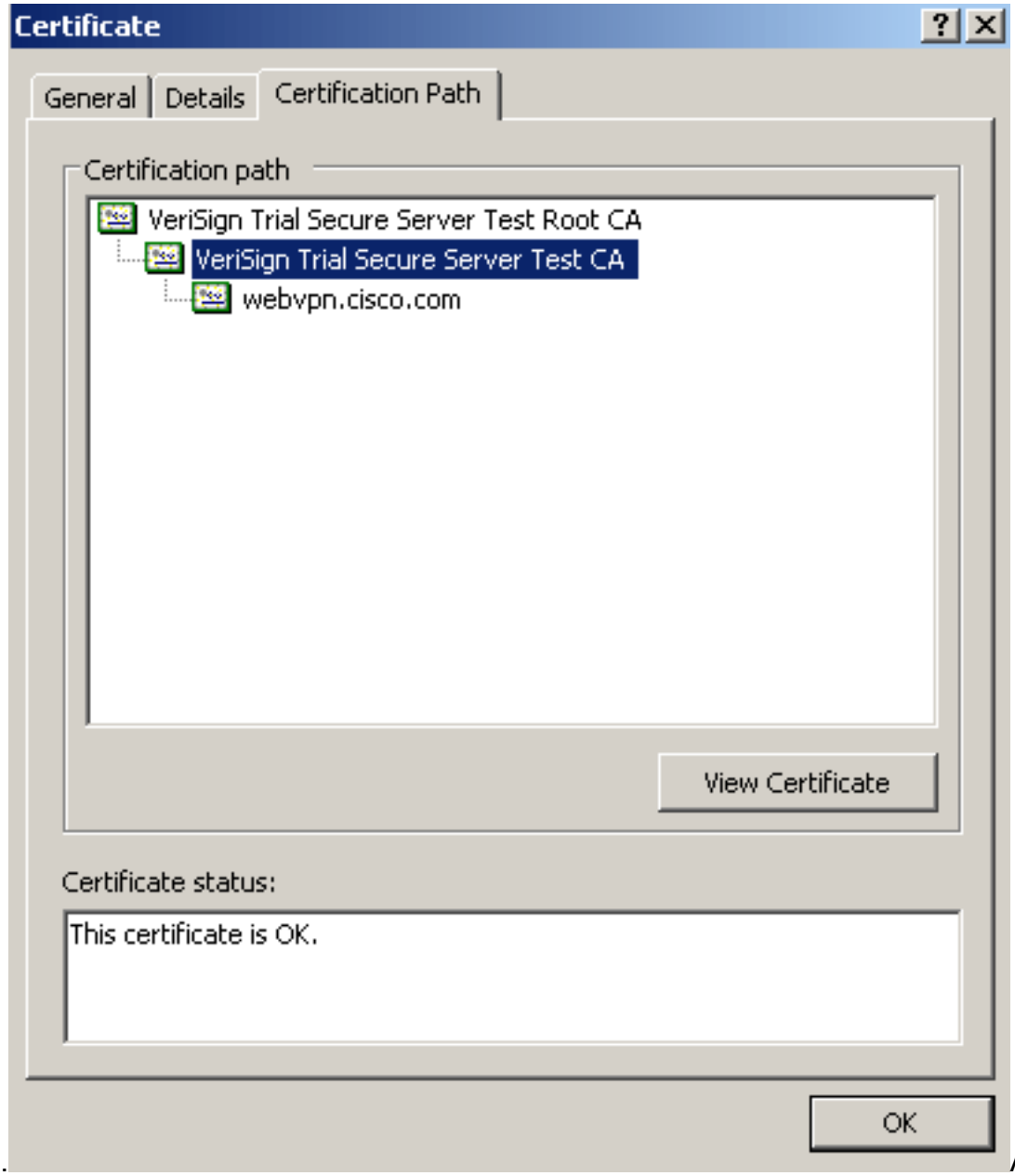
Procedimiento ASDM

1. Guarde el certificado de identidad en el equipo local.
2. Si se le proporcionó un certificado codificado en base64 que no se presentó como archivo, debe copiar el mensaje base64 y pegarlo en un archivo de texto.
3. Cambie el nombre del archivo con una extensión .cer.**Nota:** Una vez que se cambia el nombre del archivo con la extensión .cer, el icono del archivo debe mostrarse como un certificado.
4. Haga doble clic en el archivo de certificado.Aparecerá el cuadro de diálogo

Certificado. 

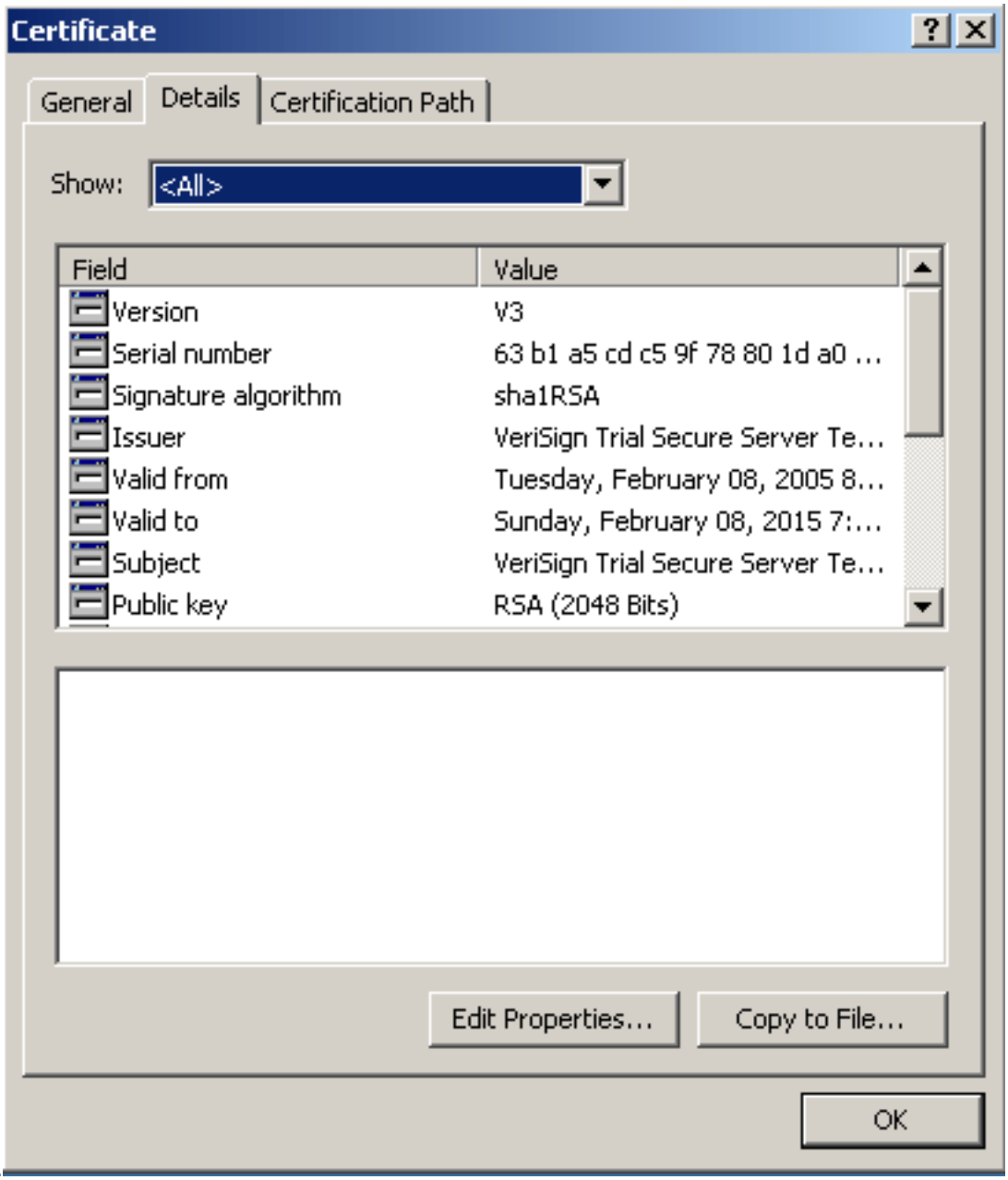
Nota: Si el mensaje "*Windows no tiene suficiente información para verificar este certificado*" aparece en la ficha General, debe obtener la CA raíz del proveedor externo o el certificado CA intermedio antes de continuar con este procedimiento. Póngase en contacto con su proveedor de terceros o administrador de CA para obtener el certificado de CA raíz o intermedio de emisión.

5. Haga clic en la pestaña **Ruta de certificado**.
6. Haga clic en el certificado de CA ubicado encima del certificado de identidad emitido y haga clic en **Ver**



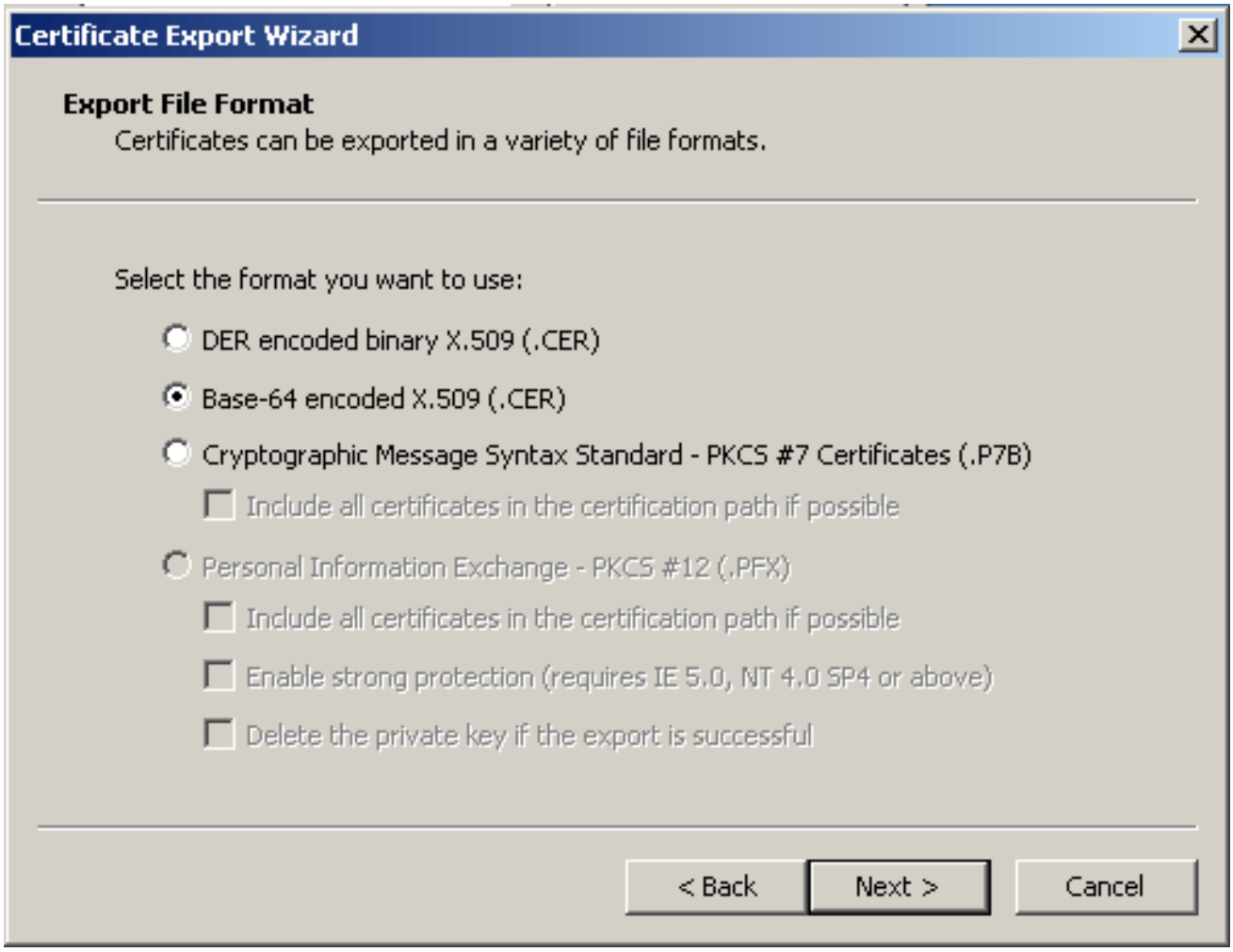
certificado. Aparecerá información detallada sobre el certificado de CA intermedio.**Advertencia:** No instale el certificado de identidad (dispositivo) en este paso. En este paso sólo se agregan el certificado raíz, la raíz subordinada o la CA. Los certificados de identidad (dispositivo) se instalan en el Paso 6.

7. Haga clic en

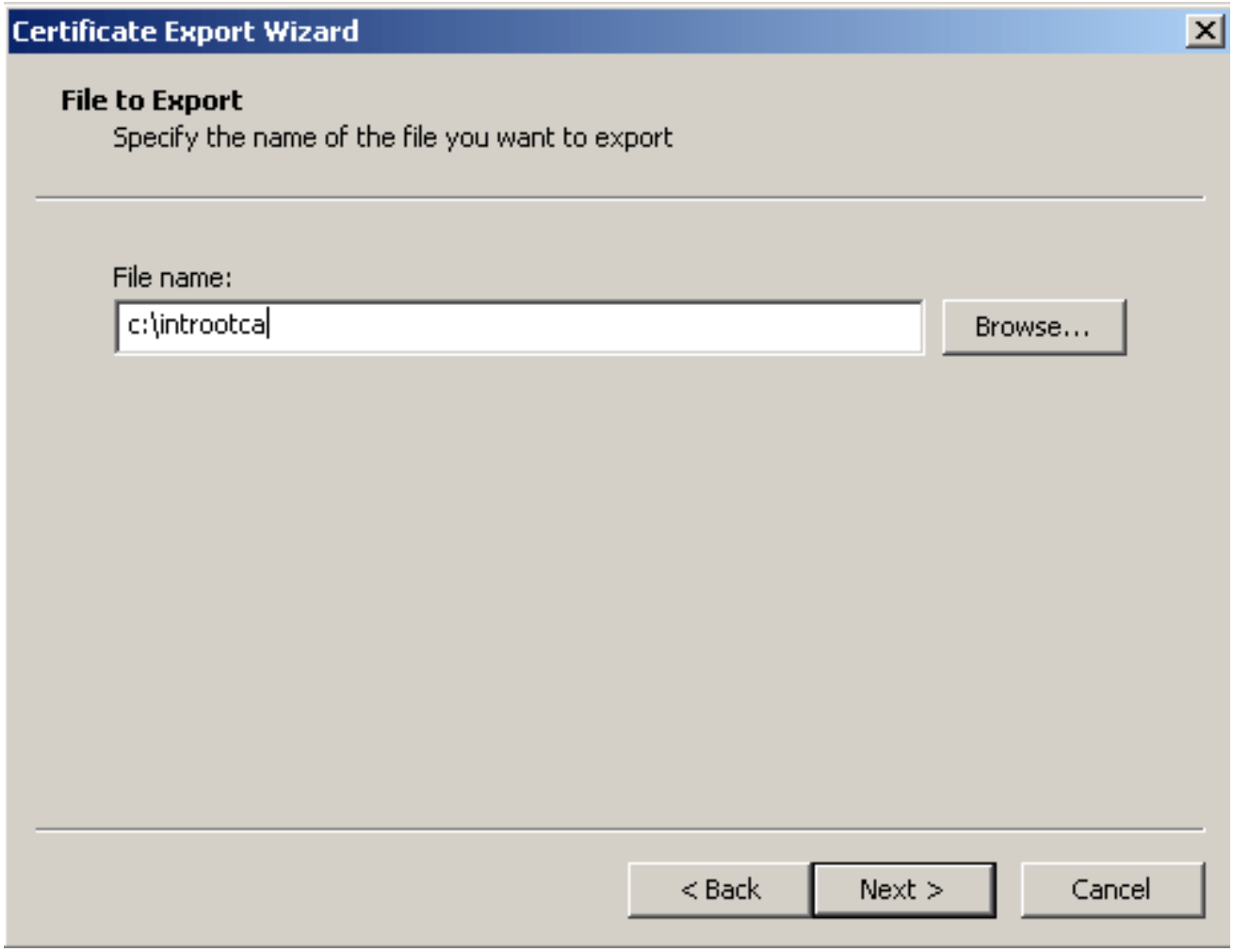


Details.

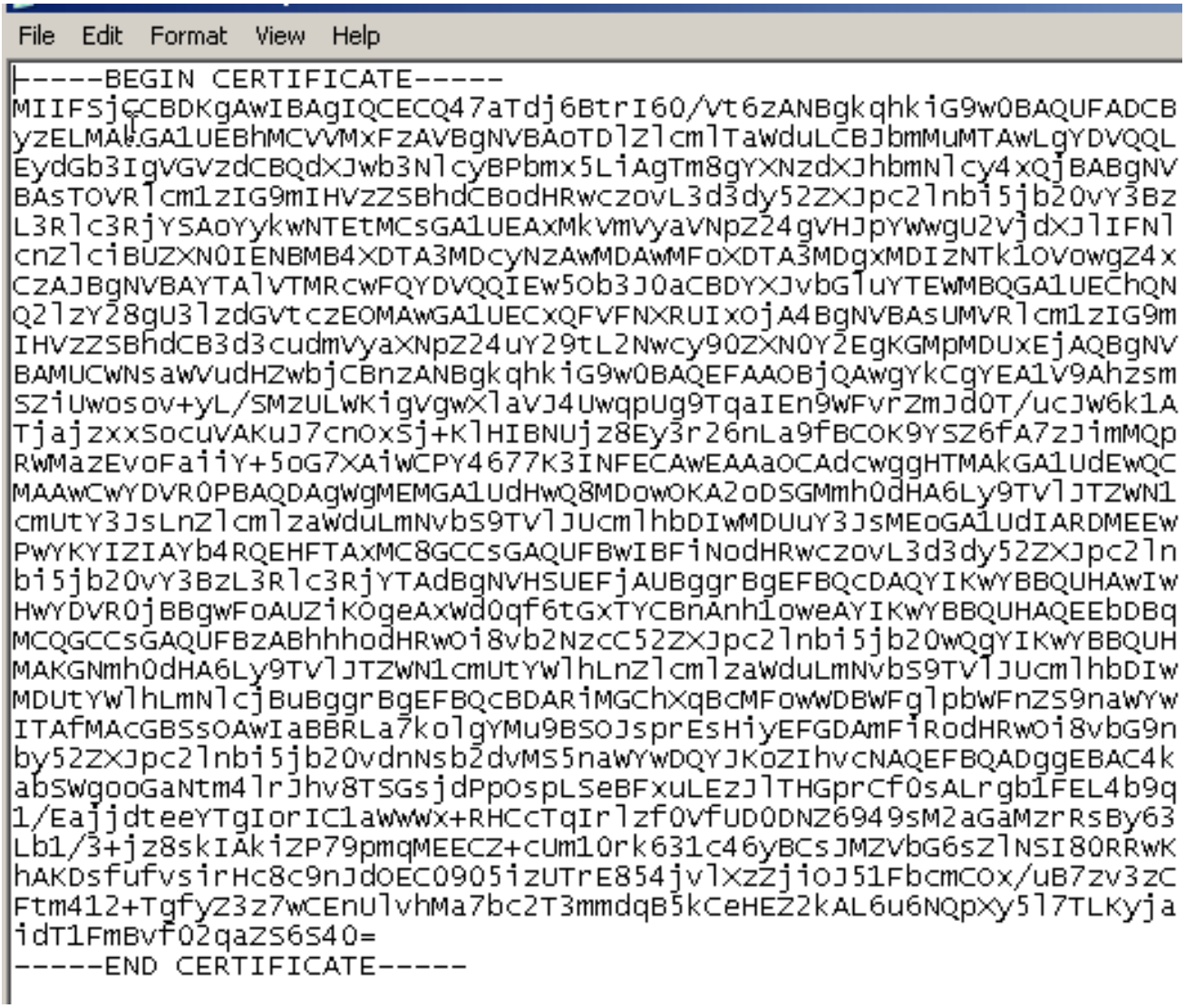
8. Haga clic en **Copiar a archivo**.
9. Dentro del Asistente para exportación de certificados, haga clic en **Siguiente.**
10. En el cuadro de diálogo Formato de archivo de exportación, haga clic en el botón de opción **Base-64 codificado X.509 (.CER)** y haga clic en **Siguiente**.



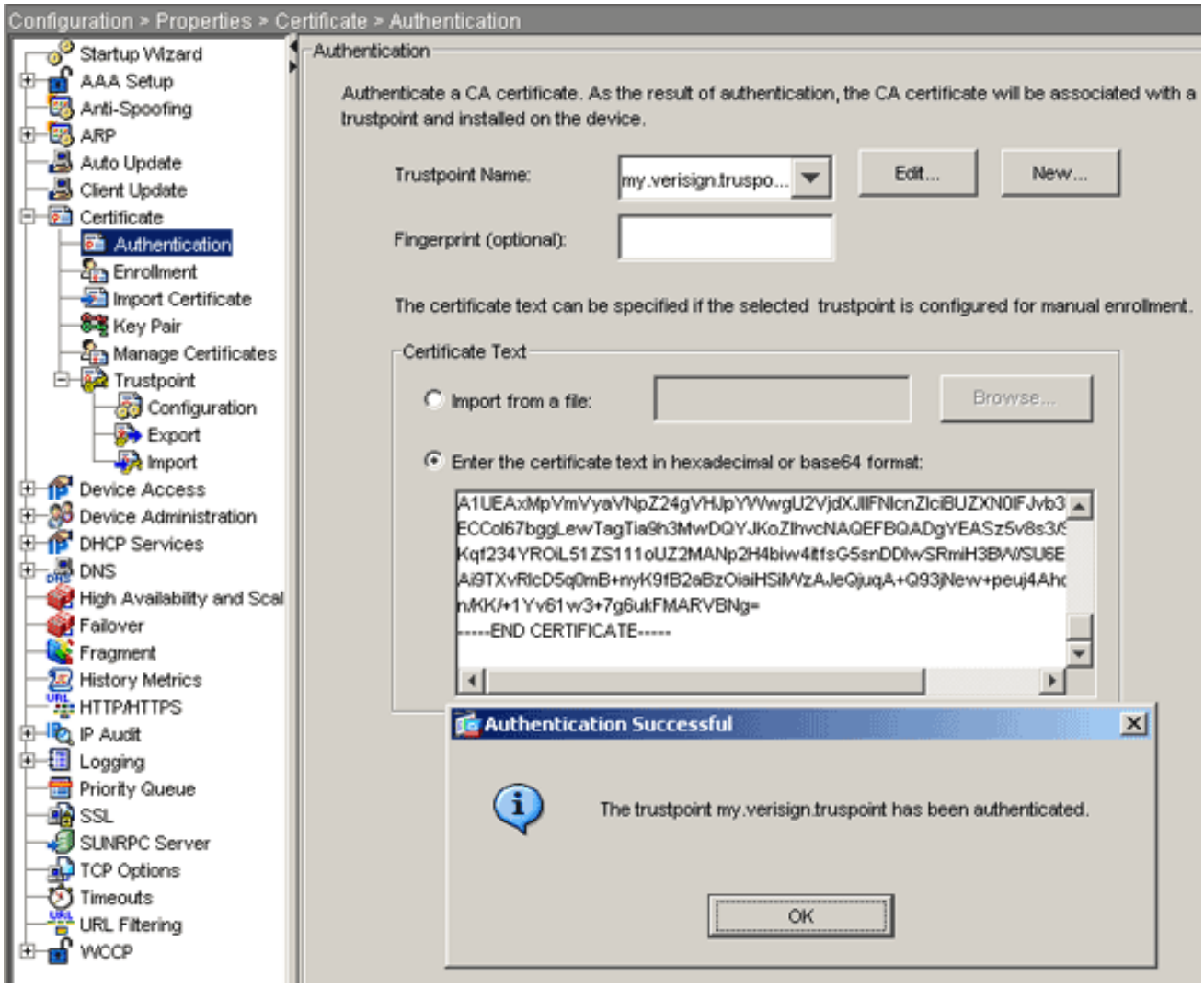
11. Introduzca el nombre de archivo y la ubicación en la que desea guardar el certificado de CA.
12. Haga clic en Next (Siguiente) y luego en Finish (Finalizar).



13. Haga clic en **Aceptar** en el cuadro de diálogo Exportar correcto.
14. Busque la ubicación en la que guardó el certificado de CA.
15. Abra el archivo con un editor de texto, como el Bloc de notas. (Haga clic con el botón derecho del ratón en el archivo y elija **Enviar a > Bloc de notas**.)El mensaje codificado en base64 debe aparecer similar al certificado en esta imagen:



16. Dentro de ASDM, haga clic en **Configuration** y, a continuación, haga clic en **Properties.**
17. Expanda **Certificate** y elija **Authentication**.
18. Haga clic en el botón de opción **Introducir el texto del certificado en formato hexadecimal o base64**.
19. Pegue el certificado CA con formato base64 del editor de texto en el área de texto.
20. Haga clic en **Autenticar**.



21. Click OK.

Ejemplo de línea de comandos

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
```

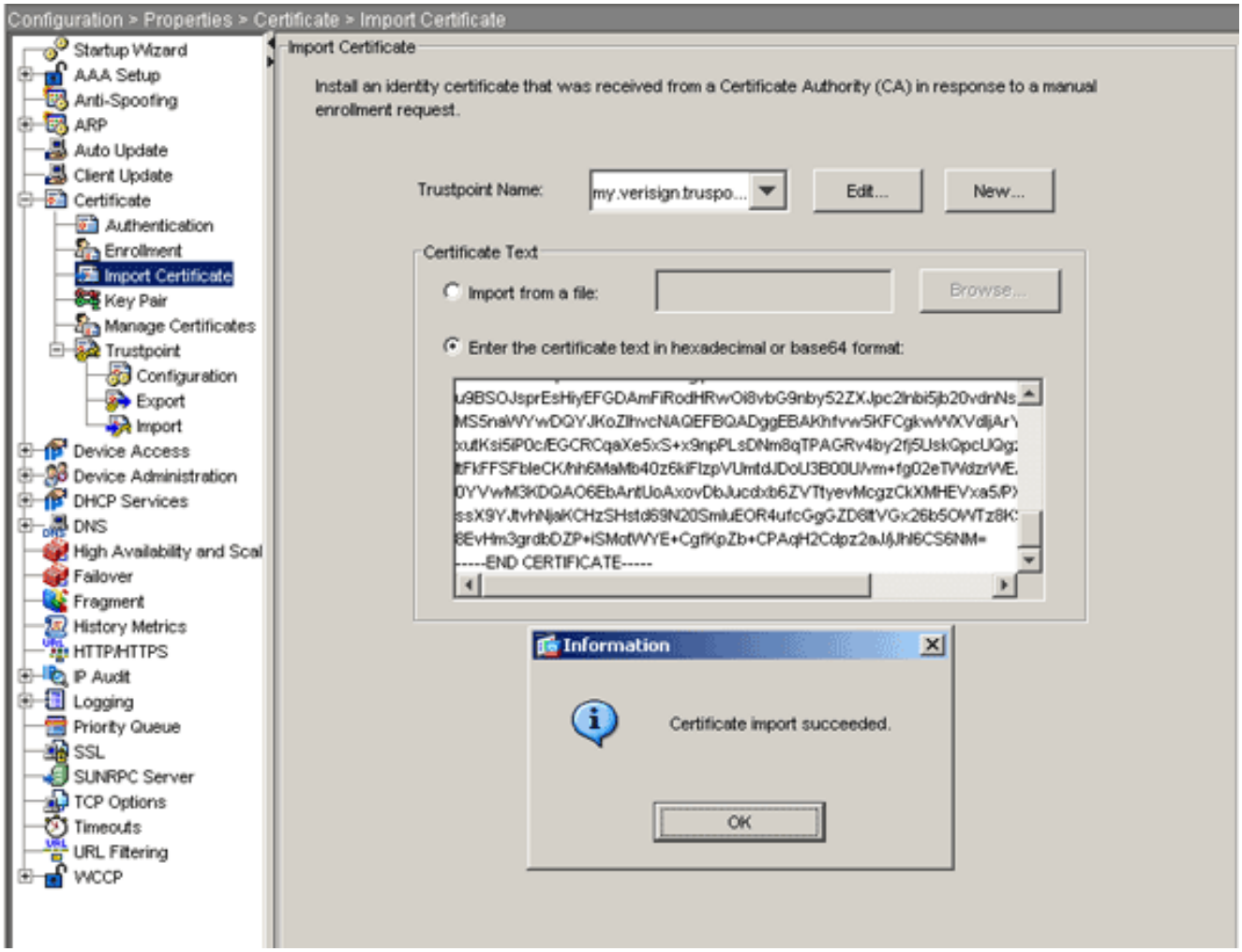
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
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)#
```

Paso 6. Instalación del certificado

Procedimiento ASDM

Utilice el certificado de identidad proporcionado por el proveedor externo para realizar estos pasos:

1. Haga clic en **Configuration** y, a continuación, haga clic en **Properties**.
2. Expanda **Certificate** y luego elija **Import Certificate**.
3. Haga clic en el botón de opción **Introducir el texto del certificado en formato hexadecimal o base64** y pegue el certificado de identidad base64 en el campo de texto.



4. Haga clic en **Importar** y, a continuación, haga clic en **Aceptar**.

Ejemplo de línea de comandos

ciscoasa

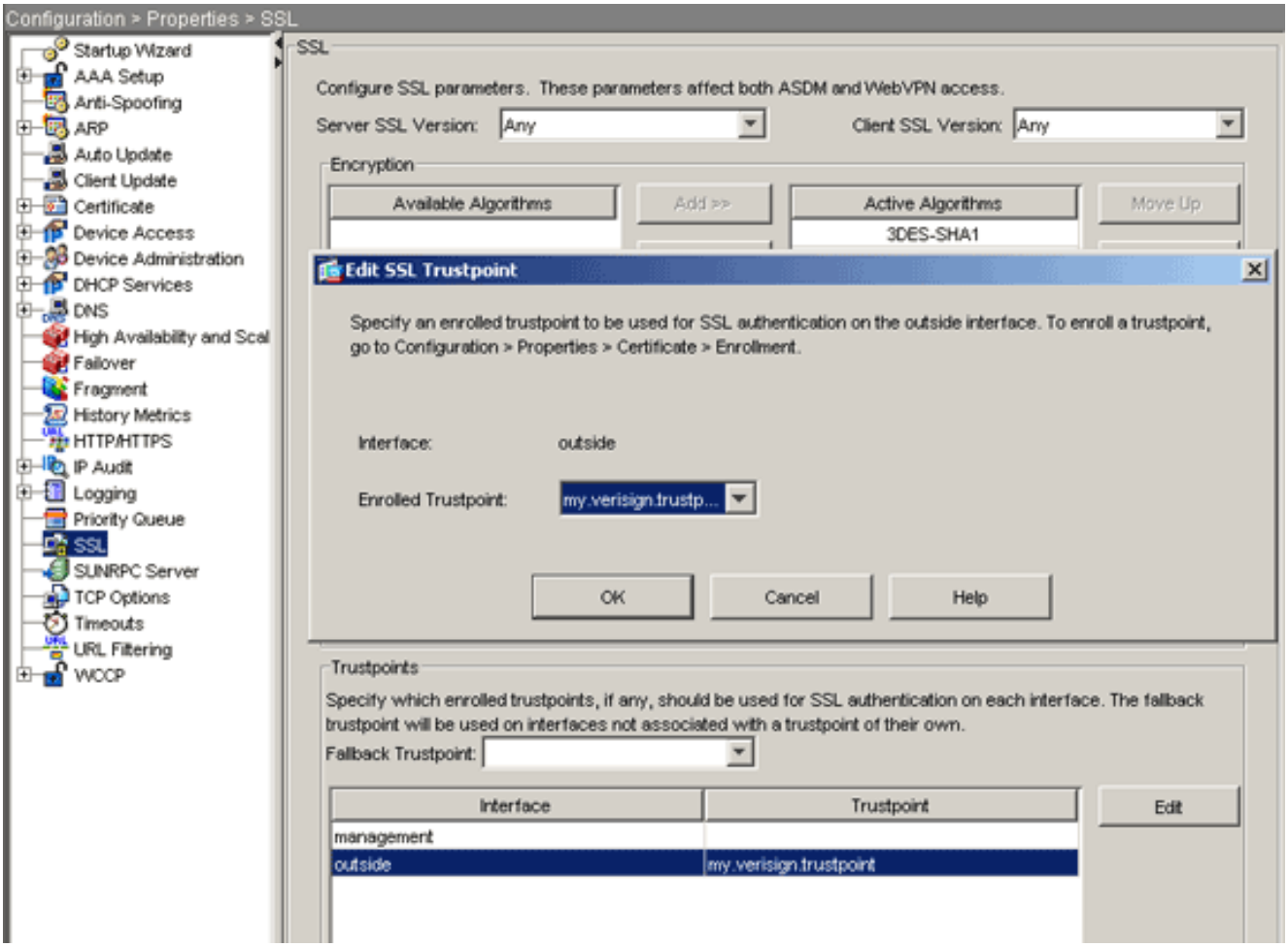
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! 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)#
```

Paso 7. Configuración de WebVPN para utilizar el certificado recién instalado

Procedimiento ASDM

1. Haga clic en **Configuration**, haga clic en **Properties** y luego elija **SSL**.
2. En el área Trustpoints, seleccione la interfaz que se utilizará para finalizar las sesiones WebVPN. (Este ejemplo utiliza la interfaz externa.)
3. Haga clic en **Editar**.Aparecerá el cuadro de diálogo Editar punto de confianza SSL.



4. En la lista desplegable Punto de confianza registrado, elija el punto de confianza que creó en el Paso 3.
5. Haga clic en **Aceptar** y luego en **Aplicar**.

El nuevo certificado se debe utilizar ahora para todas las sesiones WebVPN que finalizan en la interfaz especificada. Consulte la sección Verificación de este documento para obtener información sobre cómo verificar una instalación correcta.

Ejemplo de línea de comandos

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.
```

Verificación

En esta sección se describe cómo confirmar que la instalación del certificado de proveedor externo se ha realizado correctamente.

Reemplace el certificado firmado automáticamente desde ASA

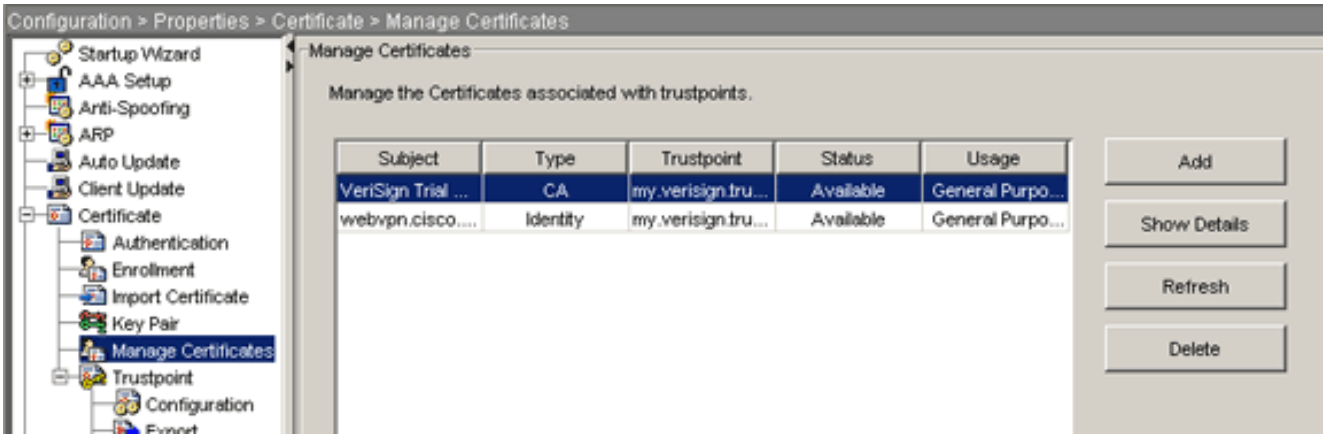
Esta sección describe cómo reemplazar el certificado autofirmado instalado del ASA.

1. Ejecute una solicitud de firma de certificado para Verisign.Después de recibir el certificado solicitado de Verisign, puede instalarlo directamente bajo el mismo punto de confianza.
2. Escriba este comando: **crypto ca enroll Verisign**Se le pedirá que responda a las preguntas.
3. Para Mostrar Solicitud de Certificado a terminal, ingrese **yes** y envíe el resultado a Verisign.
4. Una vez que le den el nuevo certificado, escriba este comando: **crypto ca import Verisign certificate**

Ver certificados instalados

Procedimiento ASDM

1. Haga clic en **Configuration** y haga clic en **Properties**.
2. Expanda **Certificate** y elija **Manage Certificates**.El certificado CA utilizado para la autenticación de punto de confianza y el certificado de identidad emitido por el proveedor externo deben aparecer en el área Administrar certificados.



Ejemplo de línea de comandos

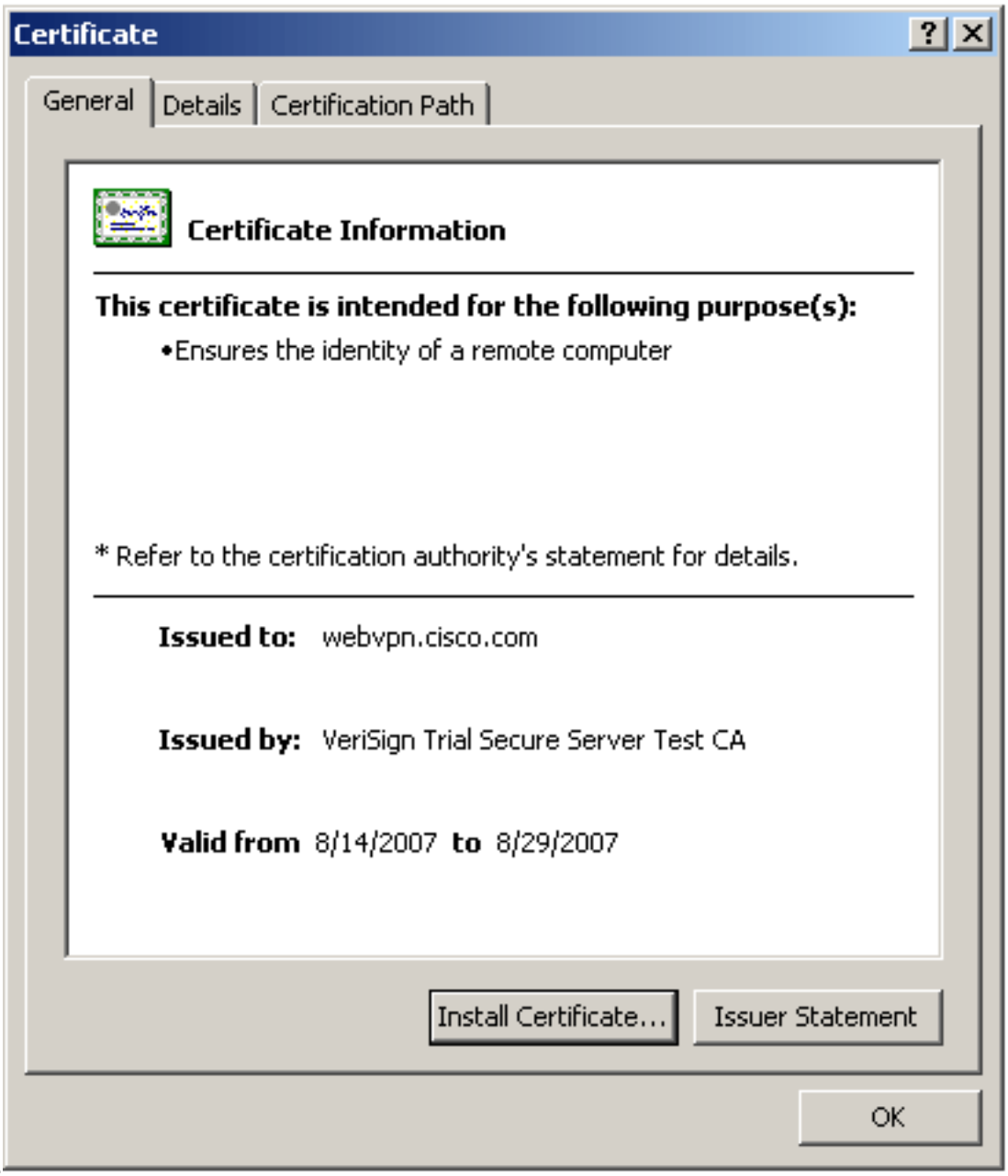
ciscoasa
ciscoasa(config)#**show crypto ca certificates** *! Displays all certificates installed on the ASA.* Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure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

Para verificar que WebVPN utiliza el nuevo certificado, complete estos pasos:

1. Conéctese a la interfaz WebVPN a través de un explorador Web. Utilice https:// junto con el FQDN que utilizó para solicitar el certificado (por ejemplo, https://webvpn.cisco.com).Si recibe una de estas alertas de seguridad, lleve a cabo el procedimiento correspondiente a esa alerta:**El nombre del certificado de seguridad no es válido o no coincide con el nombre del sitio**Verifique que haya utilizado el FQDN/CN correcto para conectarse a la interfaz WebVPN del ASA. Debe utilizar el FQDN/CN que definió cuando solicitó el certificado de identidad. Puede utilizar el comando **show crypto ca certificates trustpointname** para verificar los certificados FQDN/CN.**El certificado de seguridad fue emitido por una empresa en la que no ha decidido confiar...**Complete estos pasos para instalar el certificado raíz del proveedor de terceros en su navegador web:En el cuadro de diálogo Alerta de seguridad, haga clic en **Ver certificado**.En el cuadro de diálogo Certificado, haga clic en la ficha **Ruta de certificado**.Seleccione el certificado de CA ubicado encima del certificado de identidad emitido y haga clic en **Ver certificado**.Haga clic en **Instalar certificado**.En el cuadro de diálogo Asistente para instalación de certificados, haga clic en **Siguiente**.Seleccione el botón de opción **Automatically select the certificate store based on the type of certificate**, haga clic en **Next** y luego haga clic en **Finish**.Haga clic en **Yes** cuando reciba el mensaje Install the certificate confirm.Cuando la operación de importación se realizó correctamente, haga clic en **Aceptar** y, a continuación, haga clic en **Sí**.**Nota:** Dado que este ejemplo utiliza el certificado de prueba Verisign, el certificado raíz de CA de la prueba Verisign debe estar instalado para evitar errores de verificación cuando los usuarios se conectan.
2. Haga doble clic en el icono de bloqueo que aparece en la esquina inferior derecha de la página de inicio de sesión WebVPN.Debe aparecer la información del certificado instalado.
3. Revise el contenido para verificar que coincide con el certificado de su proveedor

externo. 

Pasos para la Renovación del Certificado SSL

Complete estos pasos para renovar el certificado SSL:

1. Seleccione el punto de confianza que debe renovar.
2. Elija **inscribirse**.Aparece este mensaje:*Si se inscribe de nuevo correctamente, el certificado actual será reemplazado por los nuevos. ¿Desea continuar?*
3. Elija **yes**.Esto generará una nueva RSE.
4. Envíe la CSR a su CA y, a continuación, importe el nuevo certificado de ID cuando lo recupere.
5. Quite y vuelva a aplicar el punto de confianza a la interfaz externa.

Comandos

En el ASA, puede utilizar varios comandos show en la línea de comandos para verificar el estado de un certificado.

- **show crypto ca trustpoint**: muestra los puntos de confianza configurados.
- **show crypto ca certificate**—Muestra todos los certificados instalados en el sistema.
- **show crypto ca crls**—Muestra listas de revocación de certificados almacenados en caché (CRL).
- **show crypto key mypubkey rsa**—Muestra todos los pares de claves crypto generados.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Estos son algunos de los posibles errores que podría encontrar:

- **%Warning: No se ha encontrado la certificación CA. Es posible que los certificados importados no se puedan utilizar.INFO: Certificado importado correctamente**El certificado de CA no se autenticó correctamente. Utilice el comando show crypto ca certificate trustpoint name para verificar que el certificado de CA se haya instalado. Busque la línea que comienza con el certificado CA. Si el certificado de CA está instalado, verifique que haga referencia al punto de confianza correcto.
- ERROR: No se pudo analizar o verificar el certificado importadoEste error puede ocurrir cuando instala el certificado de identidad y no tiene el certificado de CA intermedio o raíz correcto autenticado con el punto de confianza asociado. Debe quitar y volver a autenticarse con el certificado de CA intermedio o raíz correcto. Póngase en contacto con su proveedor externo para verificar que ha recibido el certificado de CA correcto.
- El certificado no contiene clave pública de uso generalEste error puede ocurrir cuando intenta instalar el certificado de identidad en el Trustpoint incorrecto. Intenta instalar un certificado de identidad no válido o el par de claves asociado al punto de confianza no coincide con la clave pública contenida en el certificado de identidad. Utilice el comando **show crypto ca certificates** ***trustpointname para verificar que ha instalado su certificado de identidad en el punto de confianza correcto.*** Busque la línea que indica *Puntos de confianza asociados:* Si aparece el punto de confianza incorrecto, utilice los procedimientos descritos en este documento para quitar y reinstalar al punto de confianza apropiado, también verifique que el par de claves no haya cambiado desde que se generó el CSR.
- **Mensaje de error: %PIX|ASA-3-717023 SSL no pudo establecer el certificado del dispositivo para trustpoint [nombre del punto de confianza]**Este mensaje se muestra cuando se produce un error cuando se configura un certificado de dispositivo para el punto de confianza dado para autenticar la conexión SSL. Cuando se activa la conexión SSL, se intenta establecer el certificado de dispositivo que se utilizará. Si se produce un error, se registra un mensaje de error que incluye el punto de confianza configurado que se debe utilizar para cargar el certificado del dispositivo y el motivo del error.*nombre de punto de confianza: nombre del punto de confianza para el que SSL no pudo establecer un certificado de dispositivo.***Acción Recomendada:** Resuelva el problema indicado por el motivo informado para el error.Asegúrese de que el punto de confianza especificado esté inscrito y tenga un certificado de dispositivo.Asegúrese de que el certificado del dispositivo es válido.Vuelva a inscribir el punto de confianza, si es necesario.

Información Relacionada

- Cómo obtener un certificado digital de una CA de Microsoft Windows mediante ASDM en un ASA
- Avisos de campo de productos de seguridad
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems