Esempio di installazione manuale di certificati di terze parti per ASA 7.x da utilizzare con la configurazione di WebVPN

Sommario

Introduzione

In questo esempio di configurazione viene descritto come installare manualmente un certificato digitale di un fornitore terzo sull'appliance ASA per l'utilizzo con WebVPN. Nell'esempio viene utilizzato un certificato di prova della versione. Ogni passo contiene la procedura dell'applicazione ASDM e un esempio di CLI.

Prerequisiti

Requisiti

Per questo documento è necessario disporre dell'accesso a un'Autorità di certificazione (CA) per la registrazione dei certificati. I fornitori di CA di terze parti supportati sono Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA e VeriSign.

Componenti usati

Questo documento utilizza un'appliance ASA 5510 con software versione 7.2(1) e ASDM versione 5.2(1). Tuttavia, le procedure descritte in questo documento possono essere usate su qualsiasi appliance ASA con versione 7.x compatibile con ASDM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

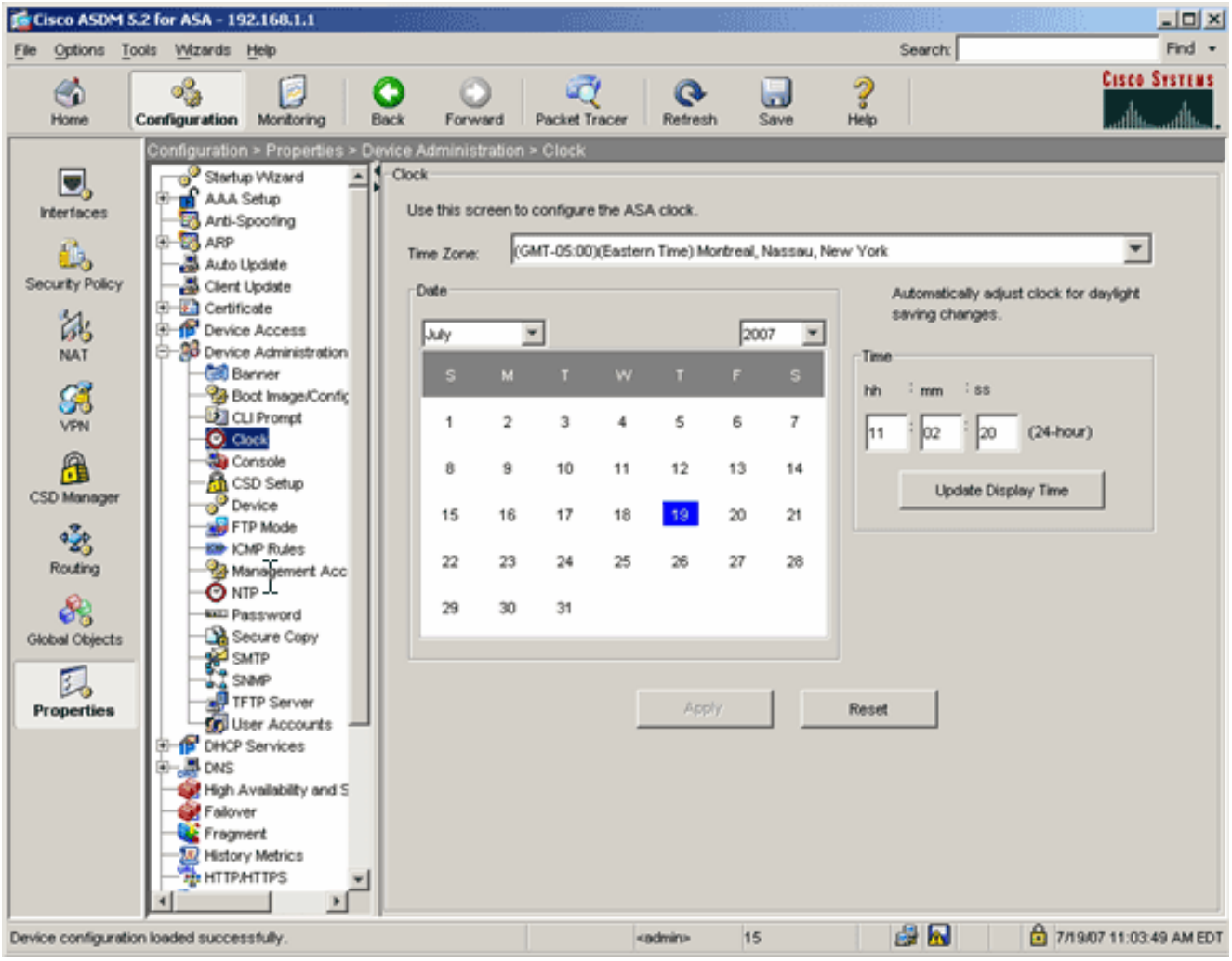
Per installare un certificato digitale di un fornitore esterno sull'appliance PIX/ASA, attenersi alla seguente procedura:

1. Verificare che i valori di Data, Ora e Fuso orario siano accurati.
2. Generare la coppia di chiavi RSA.
3. Creare il trust point.
4. Generare la registrazione certificati.
5. Autenticare il trust point.
6. Installare il certificato.
7. Configurare WebVPN per l'utilizzo del certificato appena installato.

Passaggio 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati

Procedura ASDM

1. Fare clic su Configurazione e quindi su Proprietà.
2. Espandere Amministrazione periferica e scegliere Orologio.
3. Verificare che le informazioni elencate siano corrette.I valori di Data, Ora e Fuso orario devono essere accurati per consentire la corretta convalida del certificato.



Esempio della riga di comando

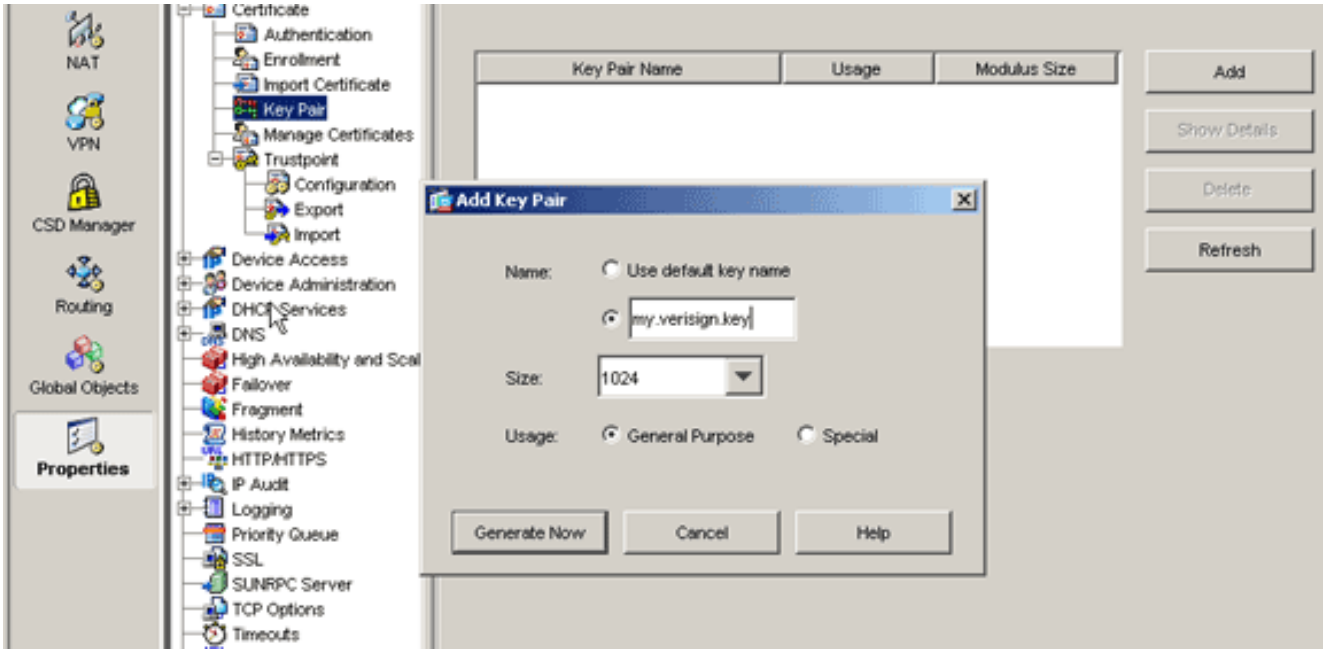
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

Passaggio 2. Generare la coppia di chiavi RSA

La chiave pubblica RSA generata viene combinata con le informazioni sull'identità dell'ASA per formare una richiesta di certificato PKCS#10. È necessario identificare chiaramente il nome della chiave con il Trustpoint per il quale si crea la coppia di chiavi.

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Proprietà**.
2. Espandere **Certificato** e scegliere **Coppia di chiavi**.
3. Fare clic su
   Add.



4. Immettere il nome della chiave, scegliere le dimensioni del modulo e selezionare il tipo di utilizzo. Nota: La dimensione consigliata per la coppia di chiavi è 1024.
5. Fare clic su **Genera**.La coppia di chiavi creata deve essere elencata nella colonna Nome coppia di chiavi.

Esempio della riga di comando

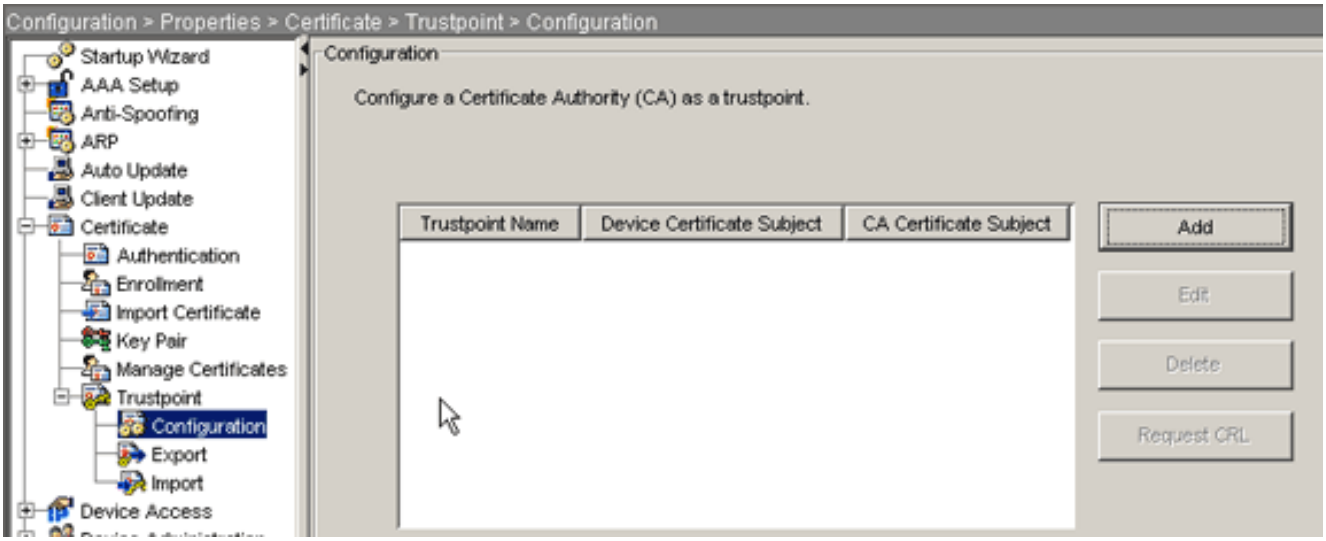
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

Passaggio 3. Creazione del punto di fiducia

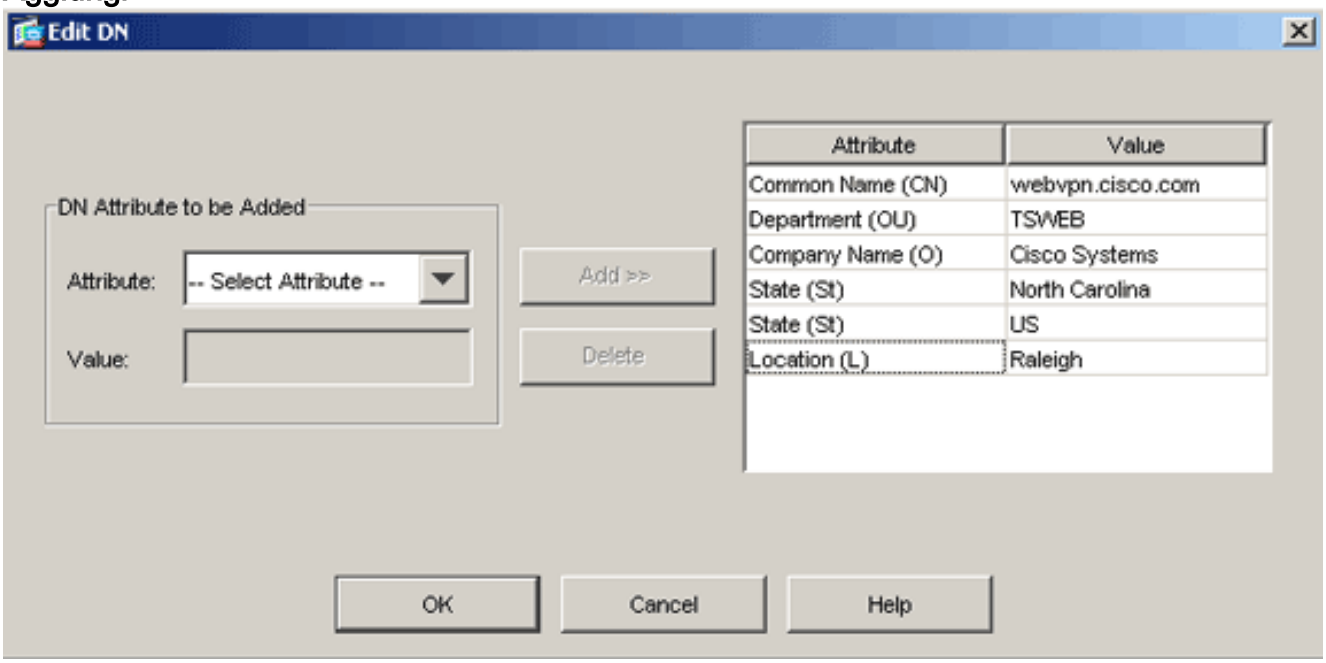
I punti di fiducia devono dichiarare l'Autorità di certificazione (CA) che verrà utilizzata dall'appliance ASA.

Procedura ASDM

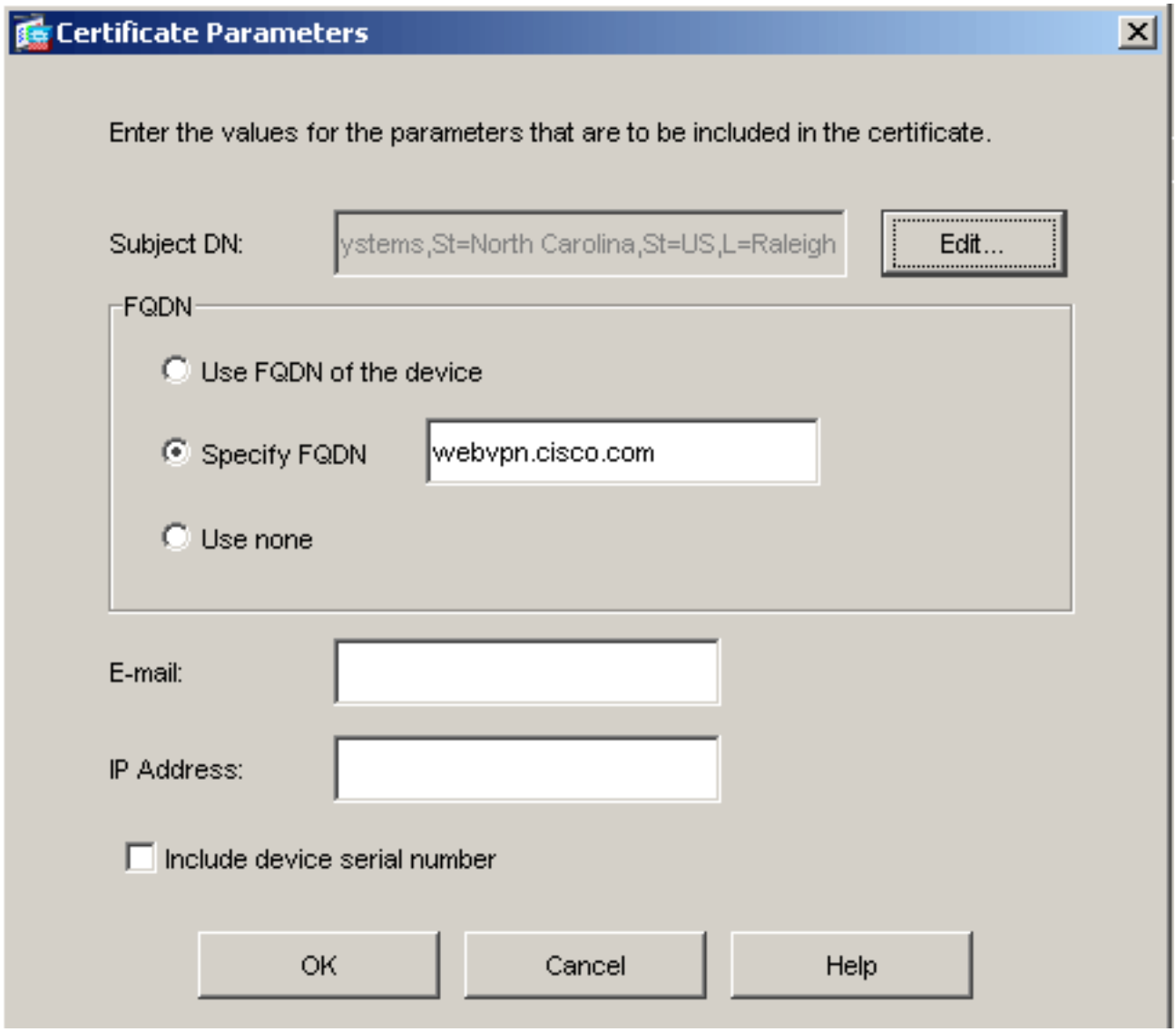
1. Fare clic su **Configurazione** e quindi su **Proprietà**.
2. Espandere **Certificato**, quindi **TrustPoint**.
3. Scegliere **Configurazione**, quindi fare clic su **Aggiungi**.



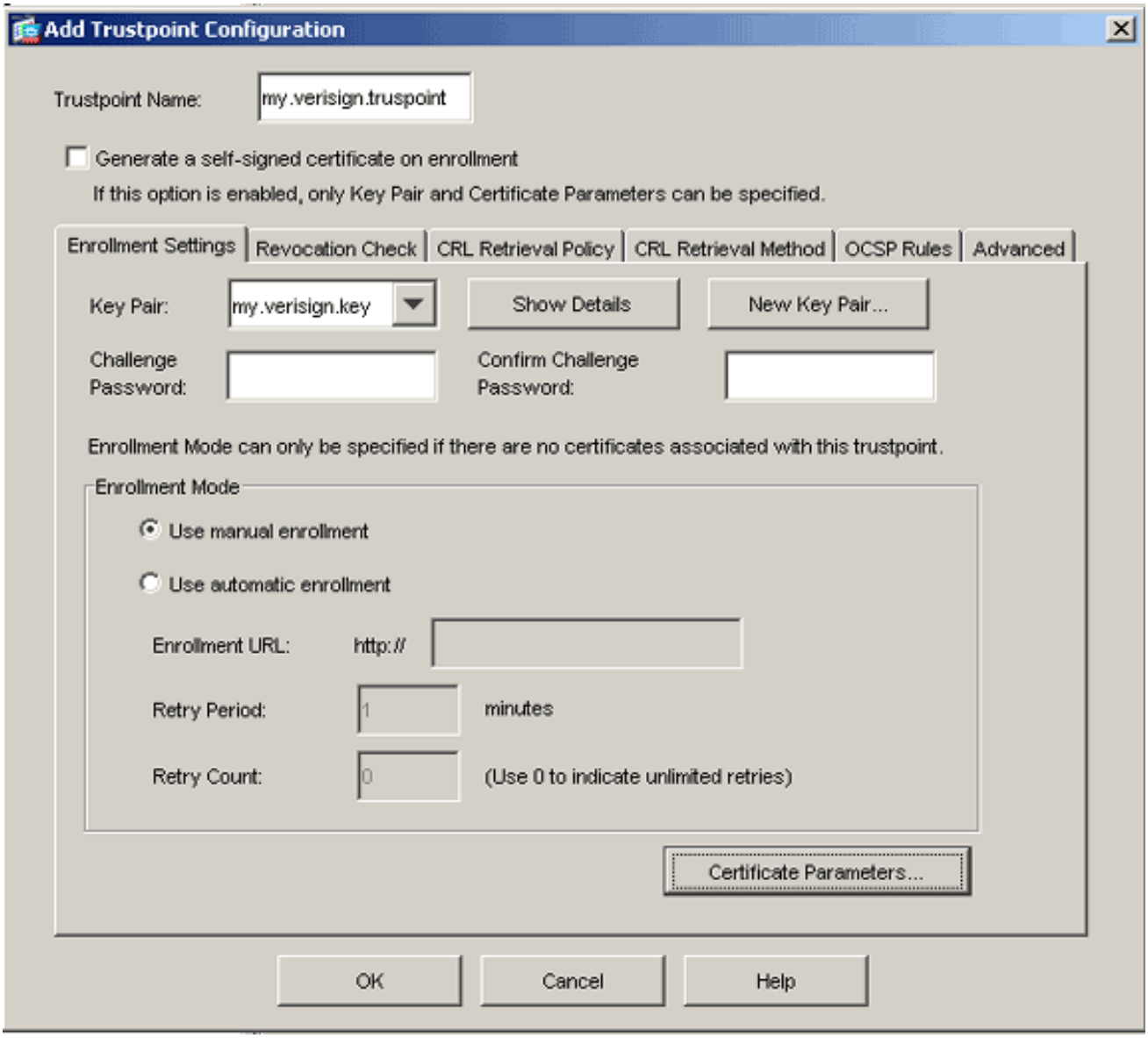
4. Configurare i seguenti valori:**Nome trust point**: Il nome del trust deve essere rilevante per l'utilizzo previsto. In questo esempio viene utilizzato *my.verisign.trustpoint*.**Coppia di chiavi**: Selezionare la coppia di chiavi generata nel passaggio 2. (*my.verisign.key*)
5. Assicurarsi che sia selezionata l'opzione Iscrizione manuale.
6. Fare clic su **Parametri certificato**.Verrà visualizzata la finestra di dialogo Parametri certificato.
7. Fare clic su **Modifica** e configurare gli attributi elencati nella tabella:Per configurare questi valori, scegliere un valore dall'elenco a discesa Attributo, immettere il valore e fare clic su **Aggiungi**.



8. Una volta aggiunti i valori appropriati, fare clic su **OK**.
9. Nella finestra di dialogo Parametri certificato immettere il nome di dominio completo nel campo Specifica nome di dominio completo.Questo valore deve essere lo stesso nome di dominio completo utilizzato per il nome comune
(CN).



10. Fare clic su **OK**.
11. Verificare che sia selezionata la coppia di chiavi corretta e fare clic sul pulsante di opzione **Usa registrazione manuale**.
12. Fare clic su **OK**, quindi su **Applica**.



Esempio della riga di comando

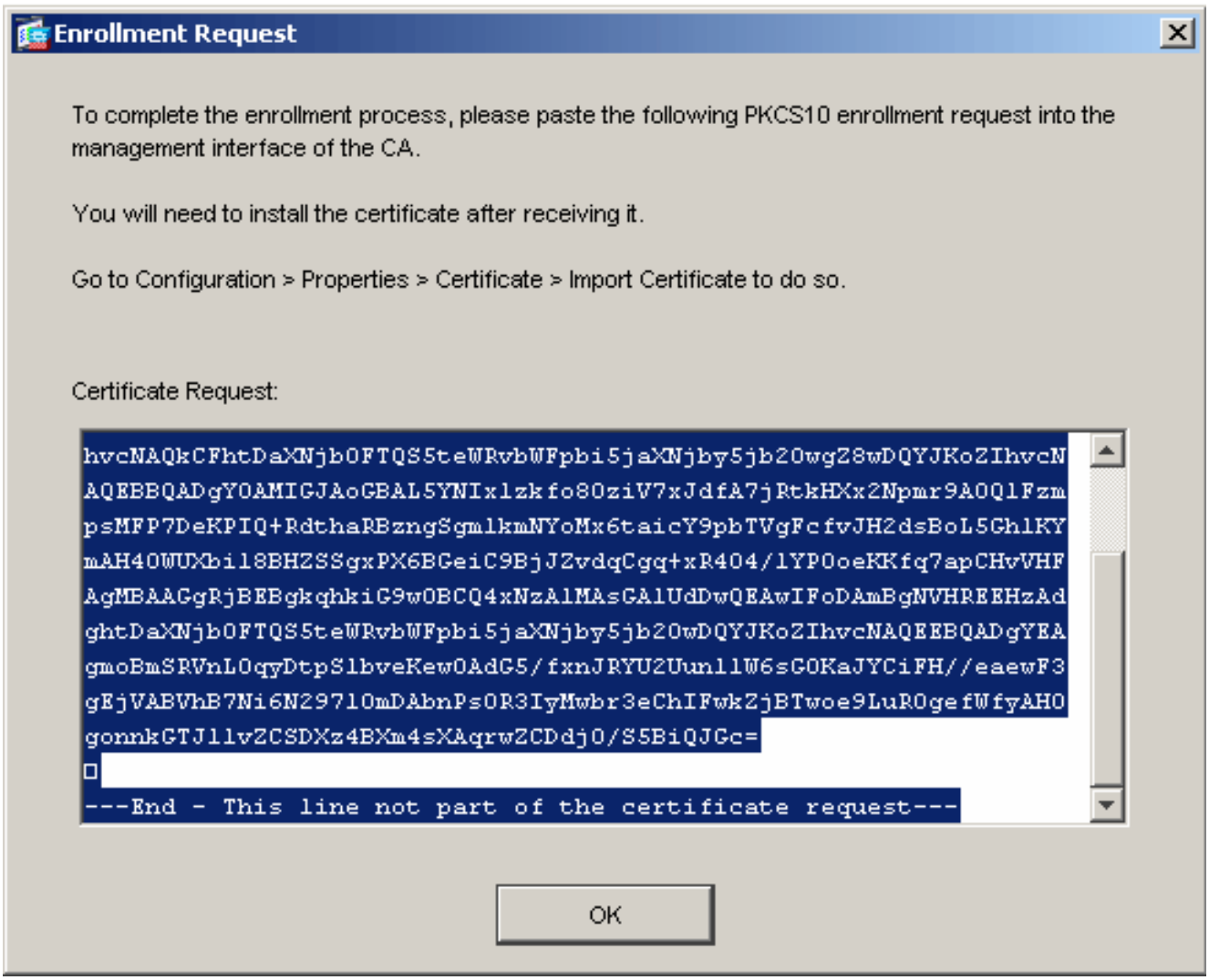
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco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

Passaggio 4. Generare la registrazione del certificato

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Proprietà**.
2. Espandere **Certificato** e scegliere **Registrazione**.
3. Verificare che il Trustpoint creato nel passaggio 3 sia selezionato e fare clic su **Registra**.Verrà visualizzata una finestra di dialogo in cui è elencata la richiesta di registrazione del certificato, definita anche richiesta di firma del certificato.



4. Copiare la richiesta di registrazione PKCS#10 in un file di testo e quindi inviare il CSR al fornitore di terze parti appropriato.Dopo aver ricevuto il CSR, il fornitore di terze parti deve rilasciare un certificato di identità per l'installazione.

Esempio della riga di comando

Nome 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

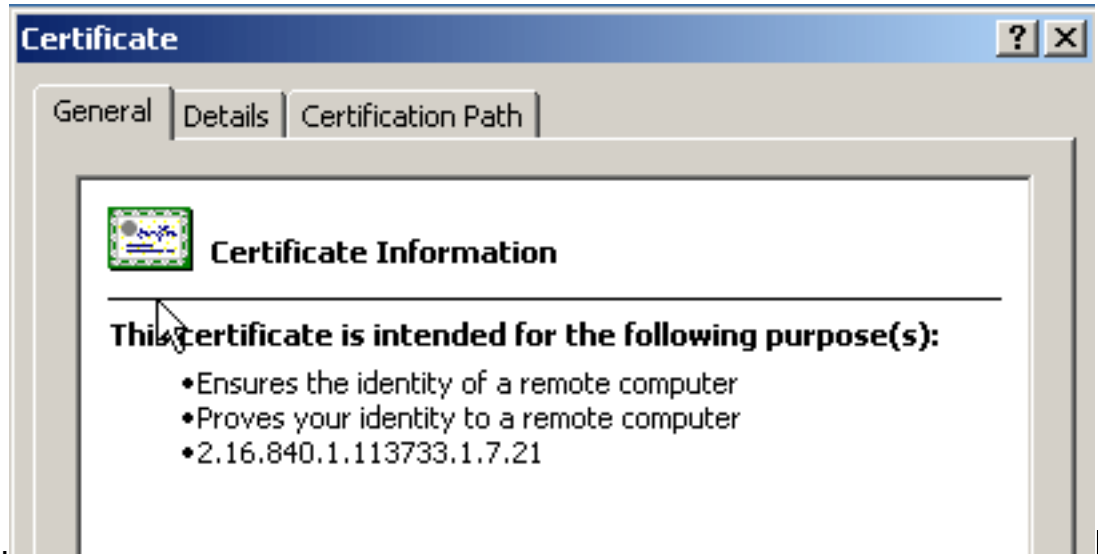
```
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the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

Passaggio 5. Autenticazione del trust point

Dopo aver ricevuto il certificato di identità dal fornitore di terze parti, è possibile procedere con questo passaggio.

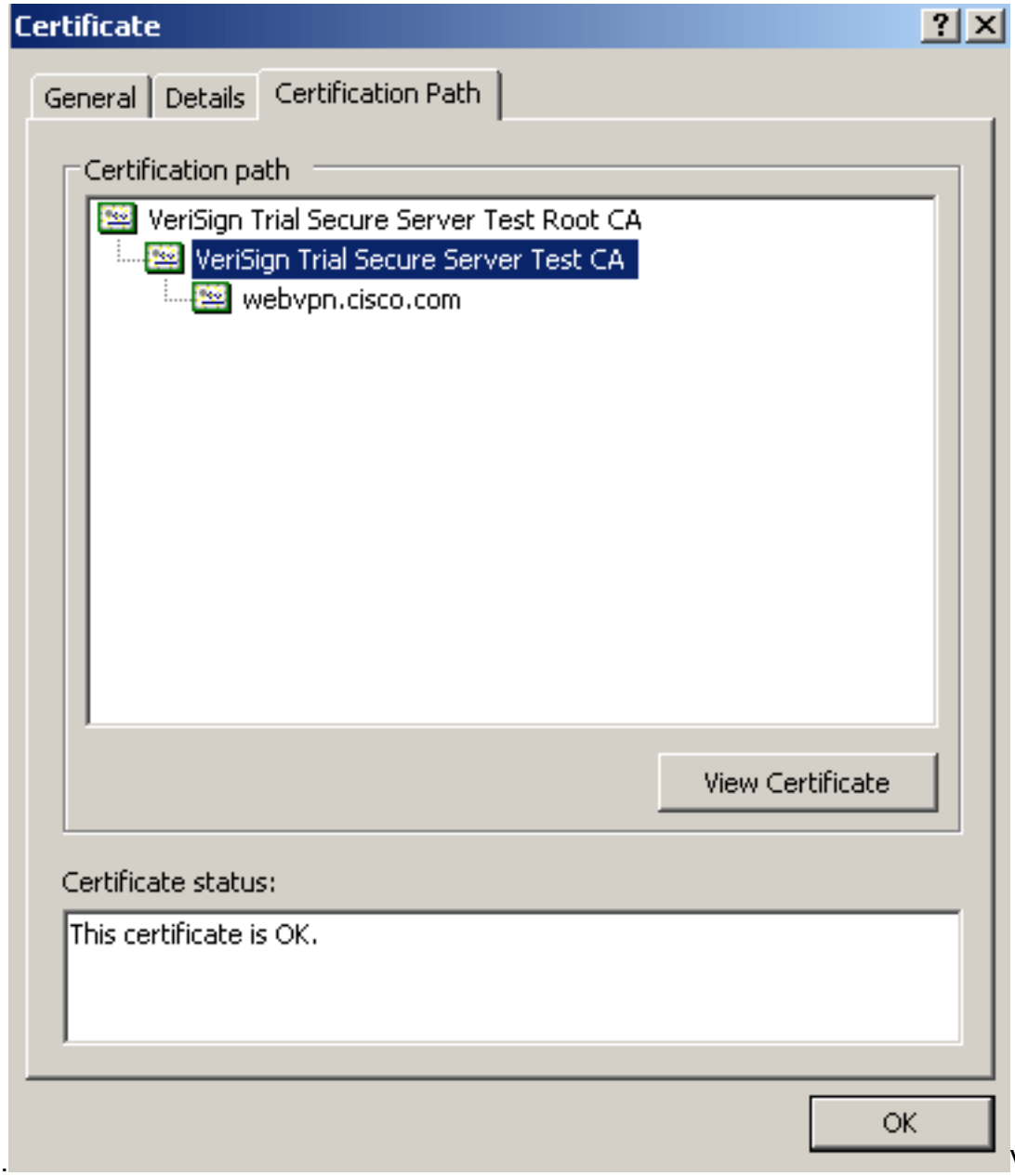
Procedura ASDM

1. Salvare il certificato di identità nel computer locale.
2. Se è stato fornito un certificato con codifica base64 non fornito come file, è necessario copiare il messaggio base64 e incollarlo in un file di testo.
3. Rinominare il file con estensione cer.**Nota:** una volta rinominato il file con estensione cer, l'icona del file dovrebbe essere visualizzata come certificato.
4. Fare doppio clic sul file del certificato.Verrà visualizzata la finestra di dialogo

Certificato. 

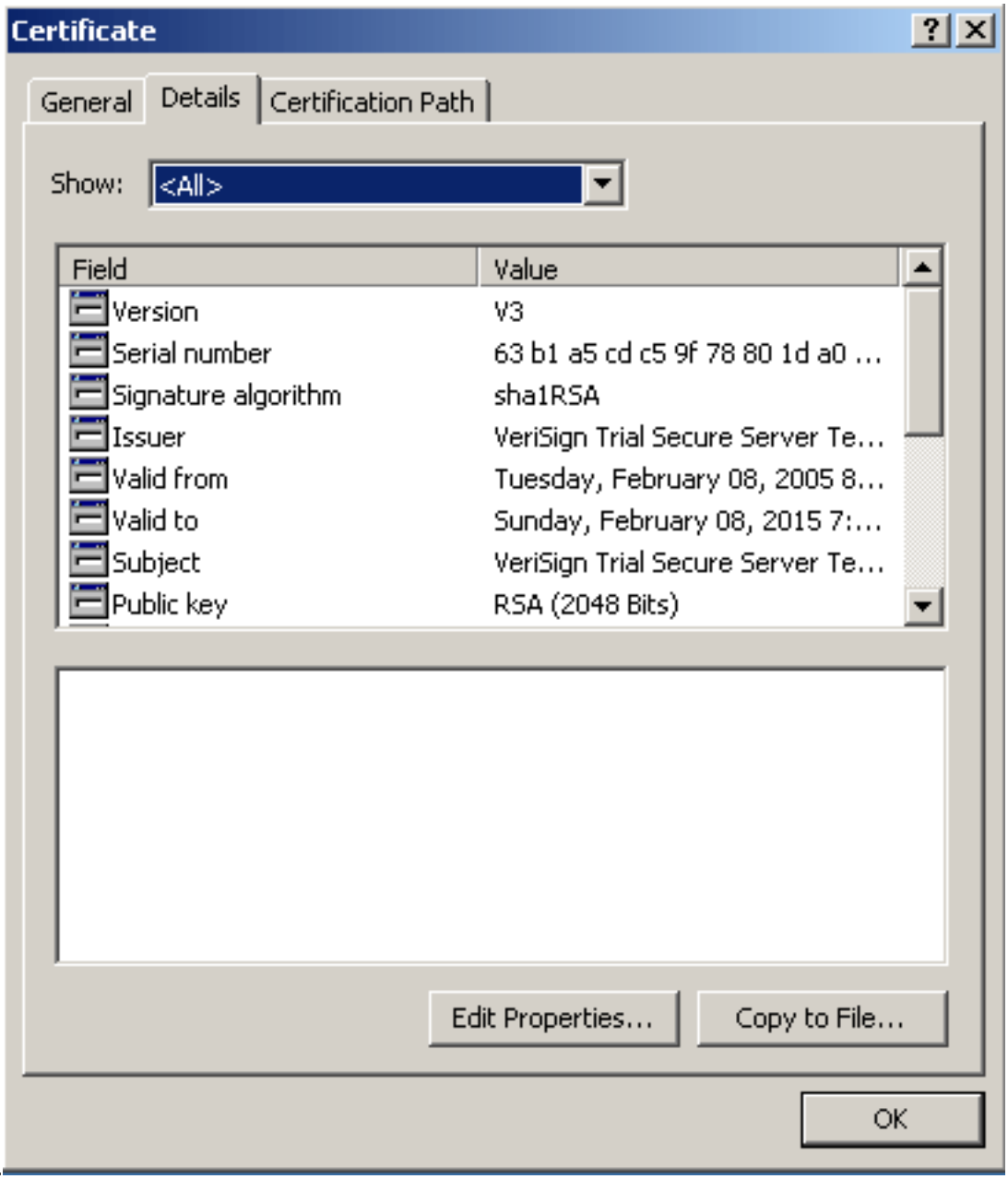
Nota: se nella scheda Generale viene visualizzato il messaggio "*Windows non dispone di informazioni sufficienti per verificare questo certificato*", è necessario ottenere il certificato CA radice o CA intermedia del fornitore di terze parti prima di continuare con questa procedura. Contattare il fornitore di terze parti o l'amministratore della CA per ottenere la CA radice o il certificato della CA intermedia di emissione.

5. Fare clic sulla scheda **Percorso certificato**.
6. Fare clic sul certificato CA situato sopra il certificato di identità rilasciato e fare clic su **Visualizza**



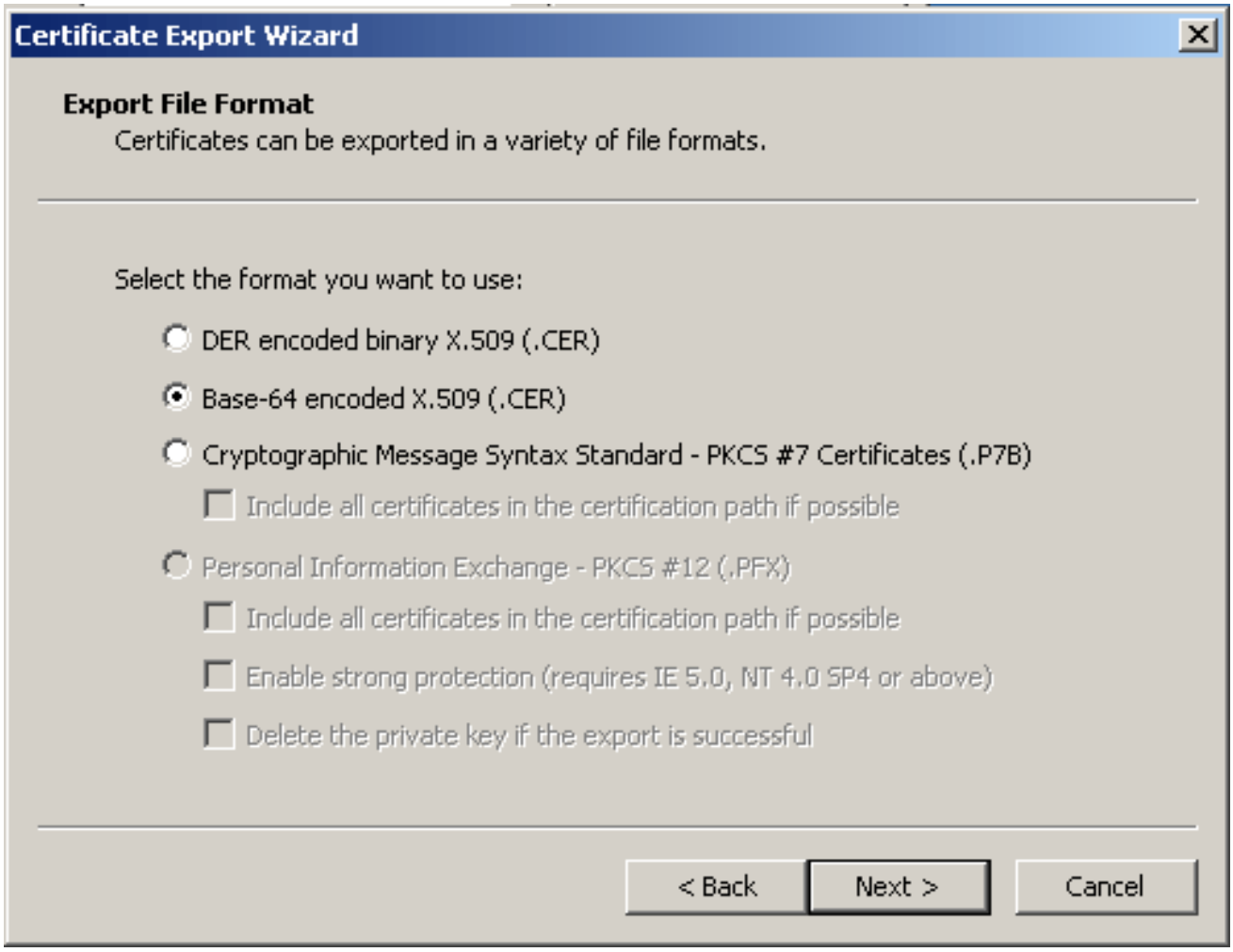
certificato. Vengono visualizzate informazioni dettagliate sul certificato CA intermedio.**Avviso:** non installare il certificato di identità (dispositivo) in questo passaggio. In questo passaggio vengono aggiunti solo il certificato radice, la radice subordinata o la CA. I certificati di identità (dispositivo) sono installati nel passaggio 6.

7. Fare clic su

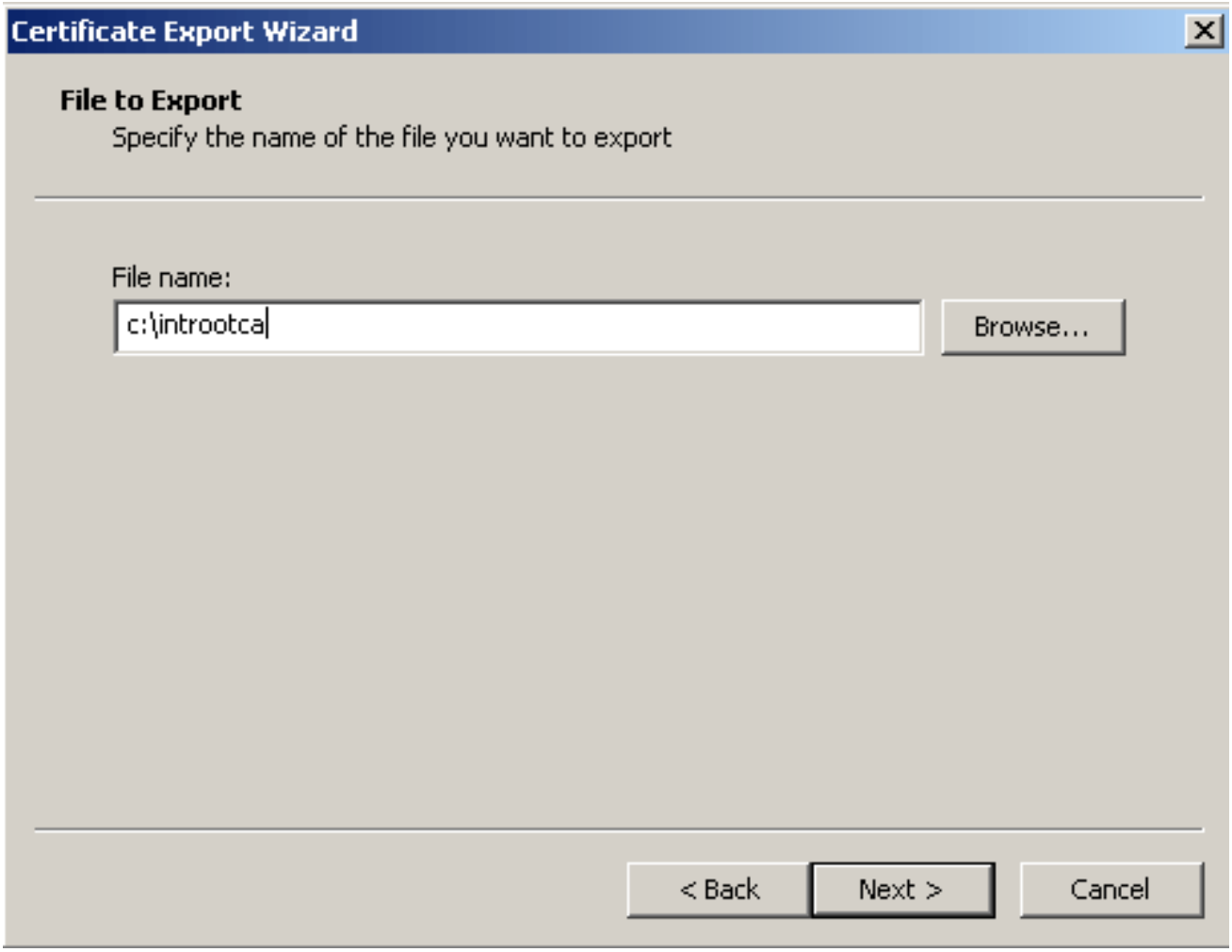


Dettagli.

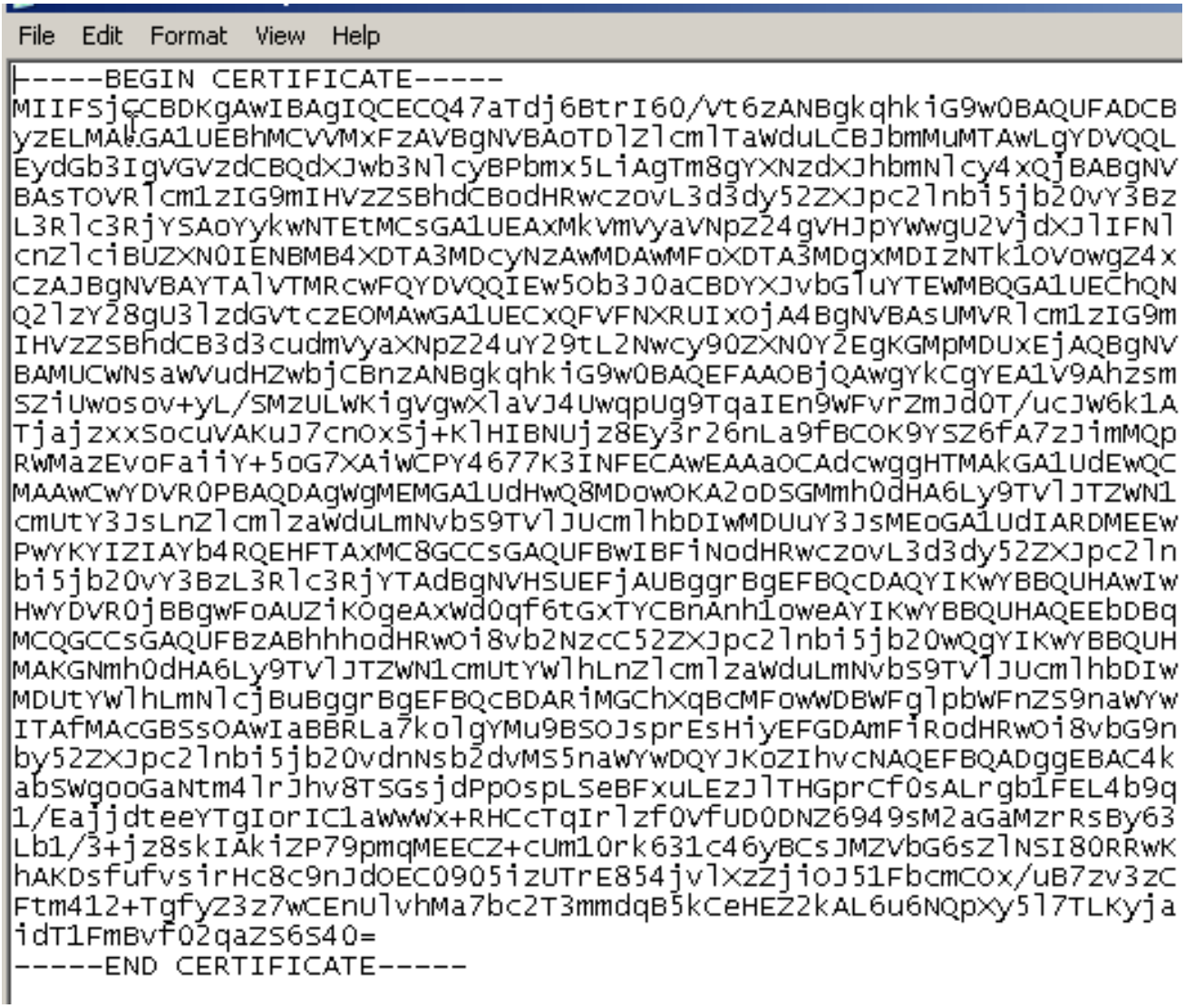
8. Fare clic su **Copia su file**.
9. Nell'Esportazione guidata certificati fare clic su **Avanti.**
10. Nella finestra di dialogo Formato file di esportazione, fate clic sul pulsante di scelta **X.509 (.CER)** con **codifica Base 64** e fate clic su **Avanti**.



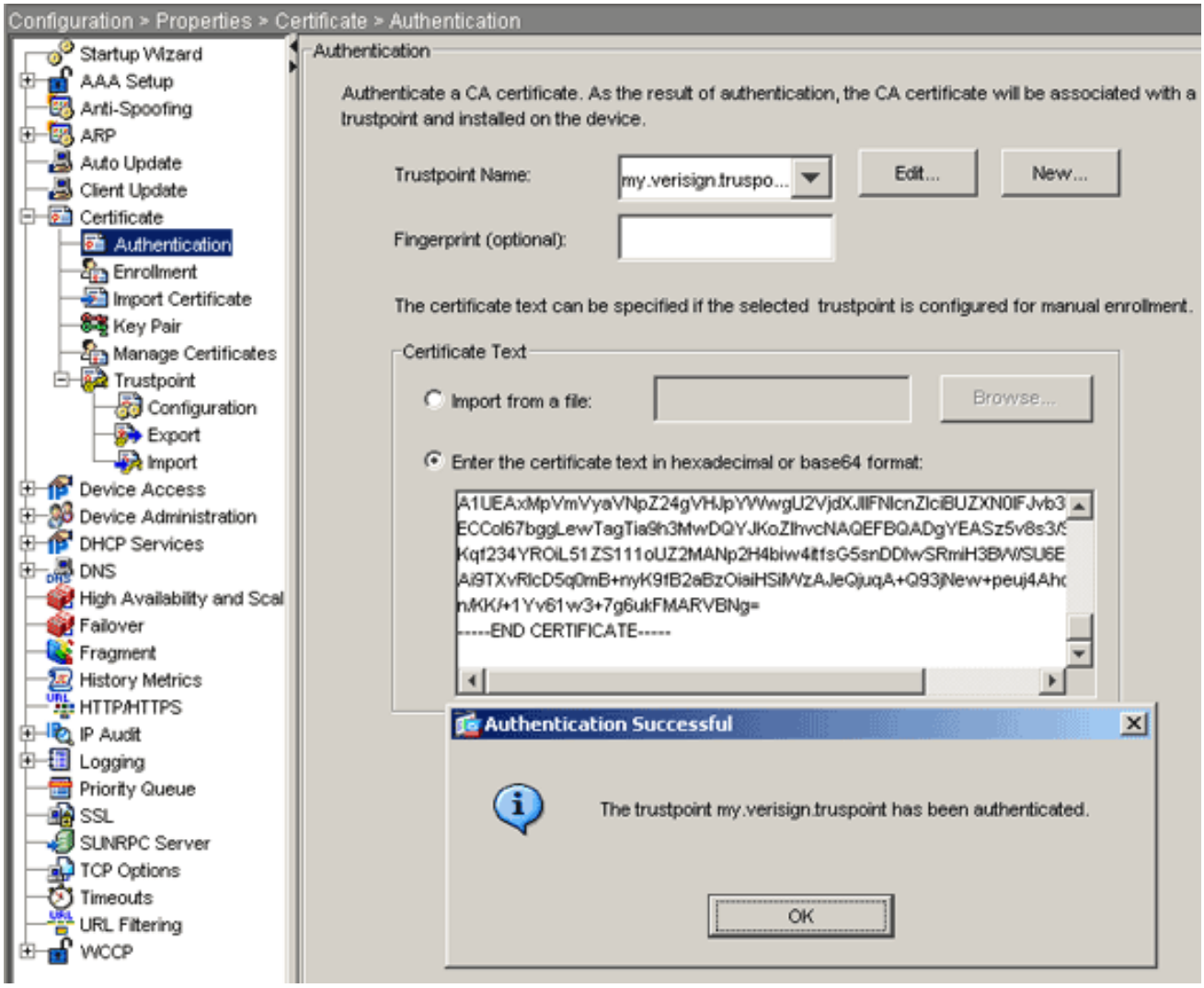
11. Immettere il nome file e il percorso in cui si desidera salvare il certificato CA.
12. Fare clic su **Avanti** e quindi su **Fine**.



13. Fare clic su **OK** nella finestra di dialogo Esportazione riuscita.
14. Selezionare il percorso in cui è stato salvato il certificato CA.
15. Aprire il file con un editor di testo, ad esempio Blocco note. Fate clic con il pulsante destro del mouse sul file e scegliete **Invia a > Blocco note**.Il messaggio con codifica base64 dovrebbe essere simile al certificato in questa immagine:



16. In ASDM, fare clic su **Configurazione**, quindi su **Proprietà.**
17. Espandere **Certificato** e scegliere **Autenticazione**.
18. Fare clic sul pulsante di opzione **Immettere il testo del certificato in formato esadecimale o base64**.
19. Incollare il certificato CA in formato base64 dall'editor di testo nell'area di testo.
20. Fare clic su **Autentica**.



21. Fare clic su **OK**.

Esempio della riga di 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
```

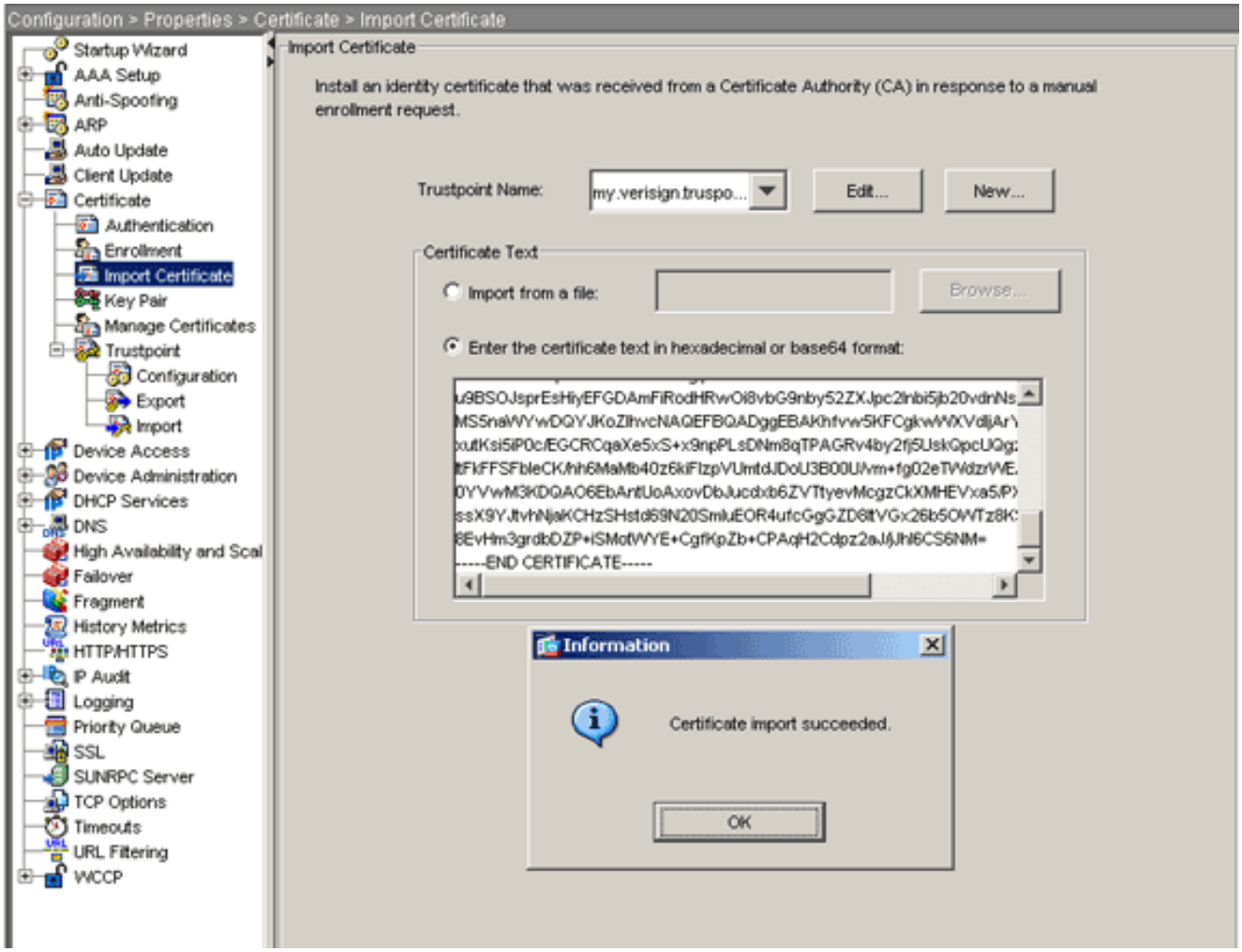
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo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

Passaggio 6. Installare il certificato

Procedura ASDM

Utilizzare il certificato di identità fornito dal fornitore di terze parti per eseguire i seguenti passaggi:

1. Fare clic su **Configurazione** e quindi su **Proprietà**.
2. Espandere **Certificato**, quindi scegliere **Importa certificato**.
3. Fare clic sul pulsante di opzione **Immettere il testo del certificato in formato esadecimale o base64** e incollare il certificato di identità base64 nel campo di testo.



4. Fare clic su **Importa** e quindi su **OK**.

Esempio della riga di comando

ciscoasa

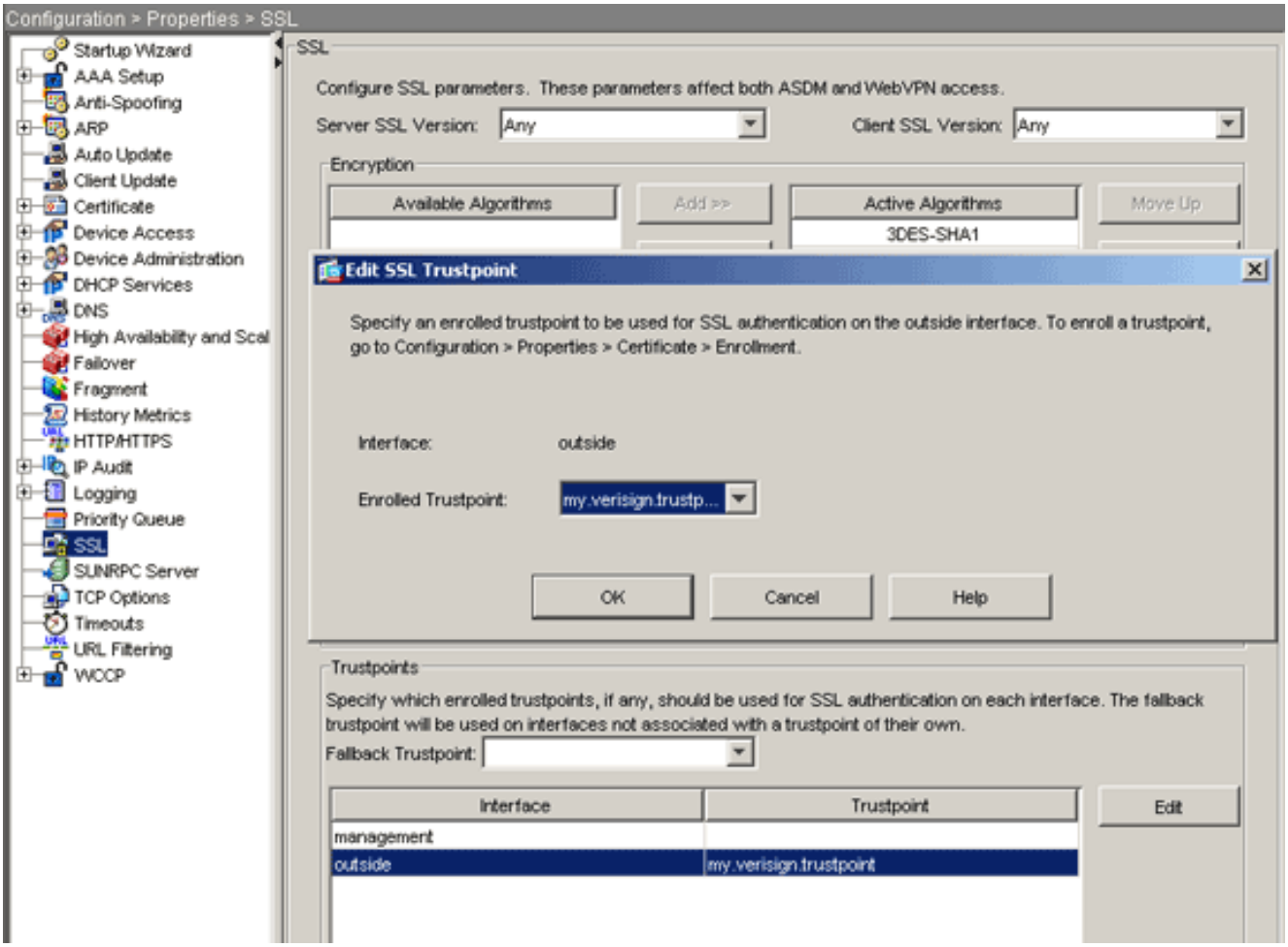
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! 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)#
```

Passaggio 7. Configurare WebVPN per l'utilizzo del certificato appena installato

Procedura ASDM

1. Fare clic su **Configurazione**, su **Proprietà** e quindi su **SSL**.
2. Nell'area Trustpoints selezionare l'interfaccia che verrà utilizzata per terminare le sessioni WebVPN. In questo esempio viene utilizzata l'interfaccia esterna.
3. Fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica trust SSL.



4. Dall'elenco a discesa Trustpoint registrato scegliere il trust point creato nel passaggio 3.
5. Fare clic su **OK**, quindi su **Applica**.

Il nuovo certificato dovrebbe essere ora utilizzato per tutte le sessioni WebVPN che terminano sull'interfaccia specificata. Per informazioni su come verificare la riuscita dell'installazione, vedere la sezione Verifica di questo documento.

Esempio della riga di 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.*

Verifica

In questa sezione viene descritto come verificare che l'installazione del certificato del fornitore di terze parti sia stata completata correttamente.

Sostituisci certificato autofirmato da ASA

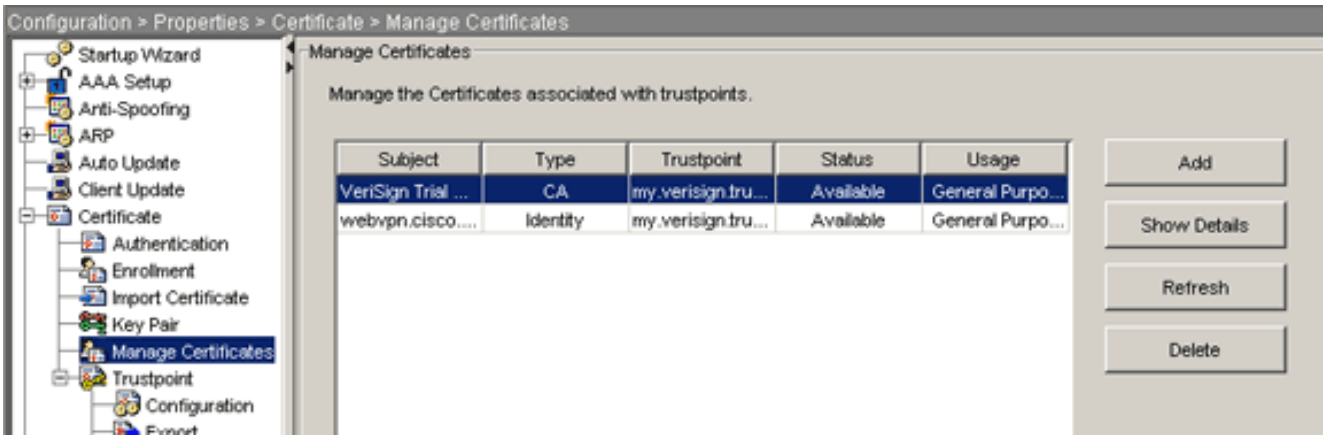
In questa sezione viene descritto come sostituire il certificato autofirmato installato dall'appliance ASA.

1. Inviare una richiesta di firma del certificato a Verisign.Dopo aver ricevuto il certificato richiesto da Verisign, è possibile installarlo direttamente nello stesso trust point.
2. Digitare il comando: **crypto ca enroll Verisign**Viene chiesto di rispondere alle domande.
3. In Visualizza richiesta certificato al terminale, immettere **yes** e inviare l'output a Verisign.
4. Dopo aver ottenuto il nuovo certificato, digitare questo comando: **crypto ca importa certificato di Verisign**

Visualizza certificati installati

Procedura ASDM

1. Fare clic su **Configurazione** e quindi su **Proprietà**.
2. Espandere **Certificato** e scegliere **Gestisci certificati**.Il certificato CA utilizzato per l'autenticazione Trustpoint e il certificato di identità rilasciato dal fornitore di terze parti devono essere visualizzati nell'area Gestisci certificati.



Esempio della riga di comando

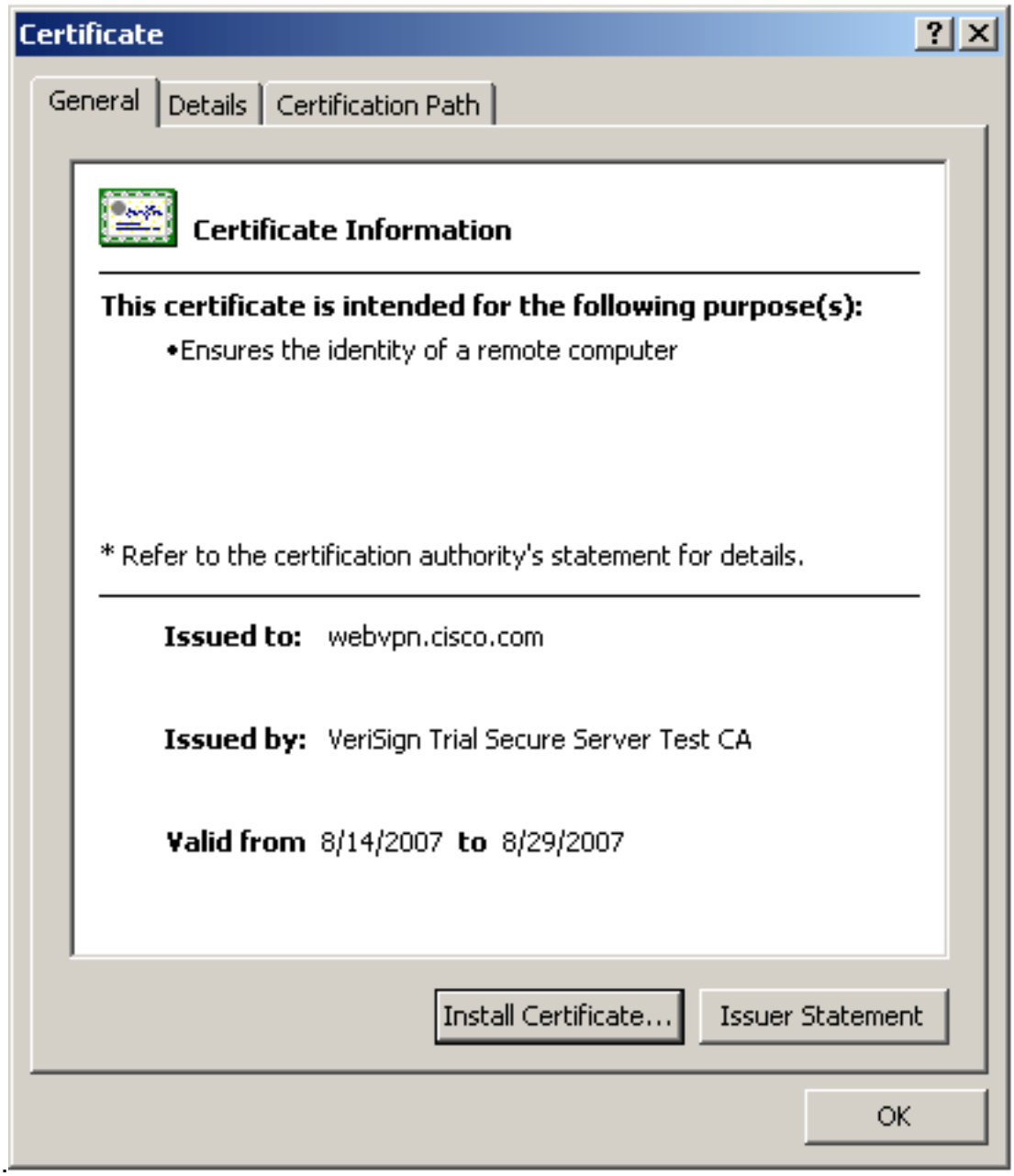
ciscoasa
ciscoasa(config)#**show crypto ca certificates** *! Displays all certificates installed on the ASA.* Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure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

Verifica del certificato installato per WebVPN con un browser

Per verificare che WebVPN utilizzi il nuovo certificato, eseguire la procedura seguente:

1. Connettersi all'interfaccia WebVPN tramite un browser Web. Utilizzare https:// insieme al nome di dominio completo utilizzato per richiedere il certificato, ad esempio https://webvpn.cisco.com.Se si riceve uno di questi avvisi di protezione, eseguire la procedura corrispondente:**Il nome del certificato di protezione non è valido o non corrisponde al nome del sito**Verificare di aver utilizzato il nome FQDN/CN corretto per connettersi all'interfaccia WebVPN dell'ASA. È necessario utilizzare l'FQDN/CN definito quando è stato richiesto il certificato di identità. È possibile utilizzare il comando **show crypto ca certificates trustpointname** per verificare i certificati FQDN/CN.**Il certificato di protezione è stato emesso da una società che si è scelto di non considerare attendibile...**Completare questa procedura per installare il certificato radice del fornitore di terze parti nel browser Web:Nella finestra di dialogo Avviso di protezione fare clic su **Visualizza certificato**.Nella finestra di dialogo Certificato fare clic sulla scheda **Percorso certificato**.Selezionare il certificato CA sopra il certificato di identità rilasciato e fare clic su **Visualizza certificato**.Fare clic su **Installa certificato**.Nella finestra di dialogo Installazione guidata certificato fare clic su **Avanti**.Selezionare il pulsante di opzione **Seleziona automaticamente l'archivio certificati in base al tipo di certificato**, fare clic su **Avanti** e quindi su **Fine**.Fare clic su **Sì** quando viene visualizzata la richiesta di conferma dell'installazione del certificato.Al prompt Importazione completata, fare clic su **OK** e quindi su **Sì**.**Nota:** poiché in questo esempio viene utilizzato il certificato di prova Verisign, è necessario installare il certificato radice CA di prova Verisign per evitare errori di verifica durante la connessione degli utenti.
2. Fare doppio clic sull'icona del lucchetto visualizzata nell'angolo inferiore destro della pagina di accesso di WebVPN.Verranno visualizzate le informazioni sul certificato installato.
3. Esaminare il contenuto per verificare che corrisponda al certificato del fornitore di terze



parti.

Procedura per il rinnovo del certificato SSL

Per rinnovare il certificato SSL, completare la procedura seguente:

1. Selezionare il trust point da rinnovare.
2. Scegliere **Registra**.Viene visualizzato questo messaggio:*Se la registrazione ha esito positivo, il certificato corrente verrà sostituito con quelli nuovi. Continuare?*
3. Scegliere **sì**.Questo genererà una nuova RSI.
4. Inviare il CSR alla CA e quindi importare il nuovo certificato di identità quando viene restituito.
5. Rimuovere e riapplicare il trust point all'interfaccia esterna.

Comandi

Sull'appliance ASA, è possibile utilizzare diversi comandi show dalla riga di comando per verificare lo stato di un certificato.

- **show crypto ca trustpoint**: visualizza i trust point configurati.
- **show crypto ca certificate**: visualizza tutti i certificati installati nel sistema.
- **show crypto ca crls**: visualizza gli elenchi di revoche di certificati (CRL) memorizzati nella cache.
- **show crypto key mypubkey rsa**: visualizza tutte le coppie di chiavi crittografiche generate.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Di seguito sono riportati alcuni possibili errori:

- **% avviso: Certificato CA non trovato. I certificati importati potrebbero non essere usable.INFO: Importazione del certificato completata**Il certificato CA non è stato autenticato correttamente. Per verificare che il certificato CA sia stato installato, utilizzare il comando show crypto ca certificate trustpointname. Cercare la riga che inizia con il certificato CA. Se il certificato CA è installato, verificare che faccia riferimento al trust point corretto.
- ERRORE: Impossibile analizzare o verificare il certificato importatoQuesto errore può verificarsi quando si installa il certificato di identità e non si dispone del certificato CA intermedio o radice corretto autenticato con il trust point associato. È necessario rimuovere e rieseguire l'autenticazione con il certificato CA intermedio o radice corretto. Contattare il fornitore di terze parti per verificare di aver ricevuto il certificato CA corretto.
- Il certificato non contiene la chiave pubblica genericaÈpossibile che questo errore si verifichi quando si tenta di installare il certificato di identità nel punto di attendibilità errato. Si sta tentando di installare un certificato di identità non valido oppure la coppia di chiavi associata al trust point non corrisponde alla chiave pubblica contenuta nel certificato di identità. Utilizzare il comando **show crypto ca certificates *trustpointname*** per verificare che il certificato di identità sia stato installato nel trust point corretto. Cercare la riga che indica i *trust point associati:* Se è elencato un trust point errato, utilizzare le procedure descritte in questo documento per rimuovere e reinstallare il trust point appropriato. Verificare inoltre che la coppia di chiavi non sia cambiata dopo la generazione del CSR.
- **Messaggio di errore: %PIX|ASA-3-717023 Impossibile impostare il certificato del dispositivo per il trust point [nome trust]**Questo messaggio viene visualizzato quando si verifica un errore durante l'impostazione di un certificato di dispositivo per il trust point specificato al fine di autenticare la connessione SSL. Quando viene attivata la connessione SSL, viene eseguito un tentativo di impostare il certificato del dispositivo che verrà utilizzato. Se si verifica un errore, viene registrato un messaggio di errore che include il trust point configurato da utilizzare per caricare il certificato del dispositivo e la causa dell'errore.*nome trust point: nome del trust point per il quale SSL non è riuscito a impostare un certificato di dispositivo.***Azione consigliata:** Risolvere il problema indicato dal motivo segnalato per l'errore.Verificare che il trust point specificato sia registrato e disponga di un certificato di dispositivo.Verificare che il certificato del dispositivo sia valido.Se necessario, registrare nuovamente il trust point.

Informazioni correlate

- Come ottenere un certificato digitale da una CA di Microsoft Windows utilizzando ASDM su

un'appliance ASA
- Avvisi sui prodotti per la sicurezza
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems