ASA 7.x Manuelles Installieren von Zertifikaten von Drittanbietern zur Verwendung mit WebVPN - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Konfigurationsbeispiel wird beschrieben, wie Sie ein digitales Zertifikat eines Drittanbieters manuell auf der ASA installieren, um es mit WebVPN zu verwenden. In diesem Beispiel wird ein Verisign Trial Certificate verwendet. Jeder Schritt enthält die ASDM-Anwendungsverfahren und ein CLI-Beispiel.

Voraussetzungen

Anforderungen

Für dieses Dokument benötigen Sie Zugriff auf eine Zertifizierungsstelle (Certificate Authority, CA), um sich für Zertifikate zu registrieren. Unterstützte Drittanbieter von CA sind Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA und VeriSign.

Verwendete Komponenten

In diesem Dokument wird eine ASA 5510 verwendet, auf der die Softwareversion 7.2(1) und ASDM Version 5.2(1) ausgeführt werden. Die in diesem Dokument beschriebenen Verfahren funktionieren jedoch auf allen ASA-Appliances, die 7.x mit jeder kompatiblen ASDM-Version ausführen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

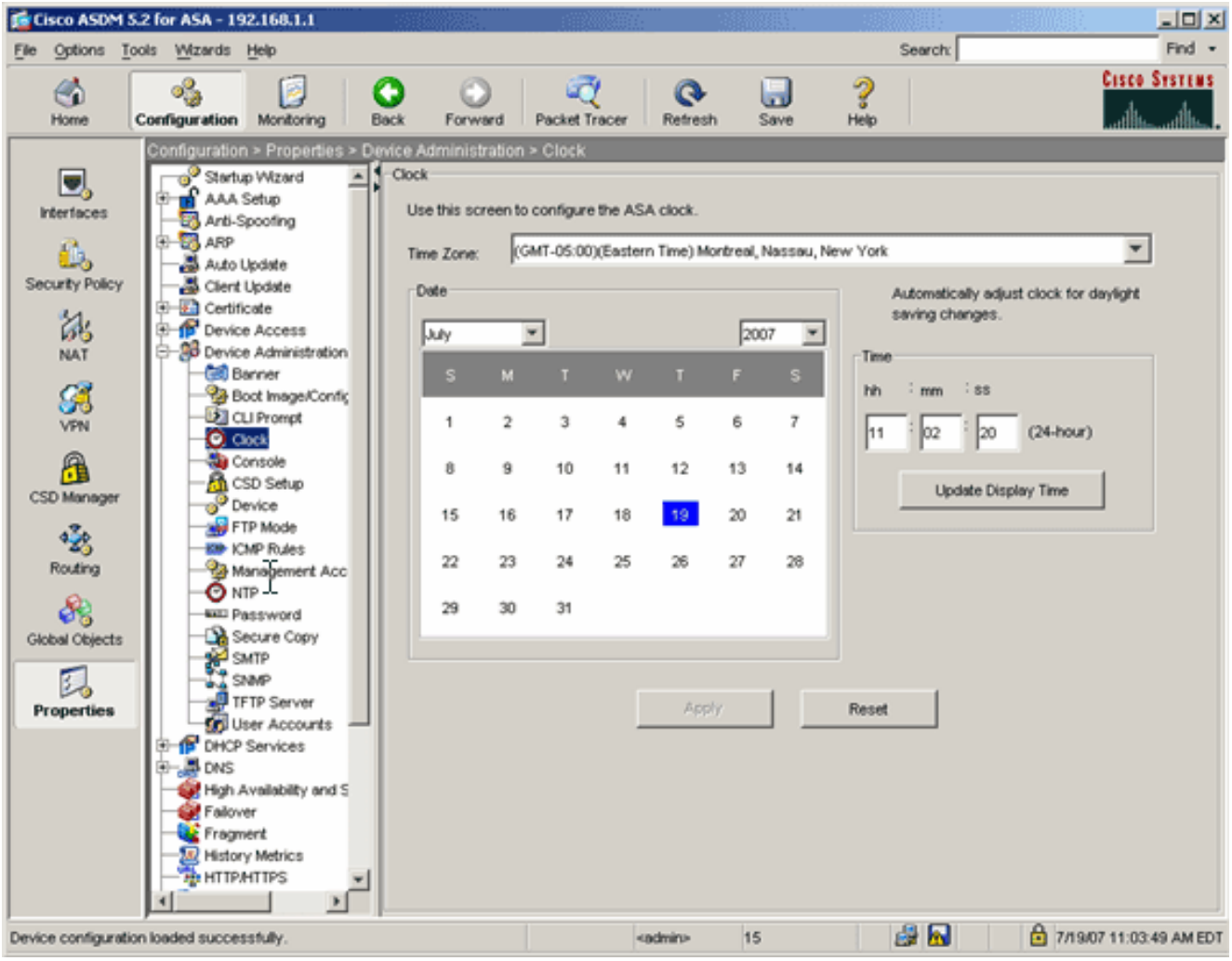
Gehen Sie wie folgt vor, um ein digitales Zertifikat eines Drittanbieters auf PIX/ASA zu installieren:

1. Überprüfen Sie, ob die Werte für Datum, Uhrzeit und Zeitzone korrekt sind.
2. Generieren Sie das RSA-Schlüsselpaar.
3. Erstellen Sie den Trustpoint.
4. Generieren der Zertifikatsregistrierung.
5. Authentifizieren Sie den Trustpoint.
6. Installieren Sie das Zertifikat.
7. Konfigurieren Sie WebVPN für die Verwendung des neu installierten Zertifikats.

Schritt 1: Überprüfen der Genauigkeit der Werte für Datum, Uhrzeit und Zeitzone

ASDM-Verfahren

1. Klicken Sie auf Konfiguration und anschließend auf Eigenschaften.
2. Erweitern Sie Device Administration (Geräteverwaltung), und wählen Sie Clock (Uhr) aus.
3. Überprüfen der Richtigkeit der angegebenen InformationenDie Werte für Datum, Uhrzeit und Zeitzone müssen genau sein, damit eine ordnungsgemäße Zertifikatsvalidierung erfolgt.



Befehlszeilenbeispiel

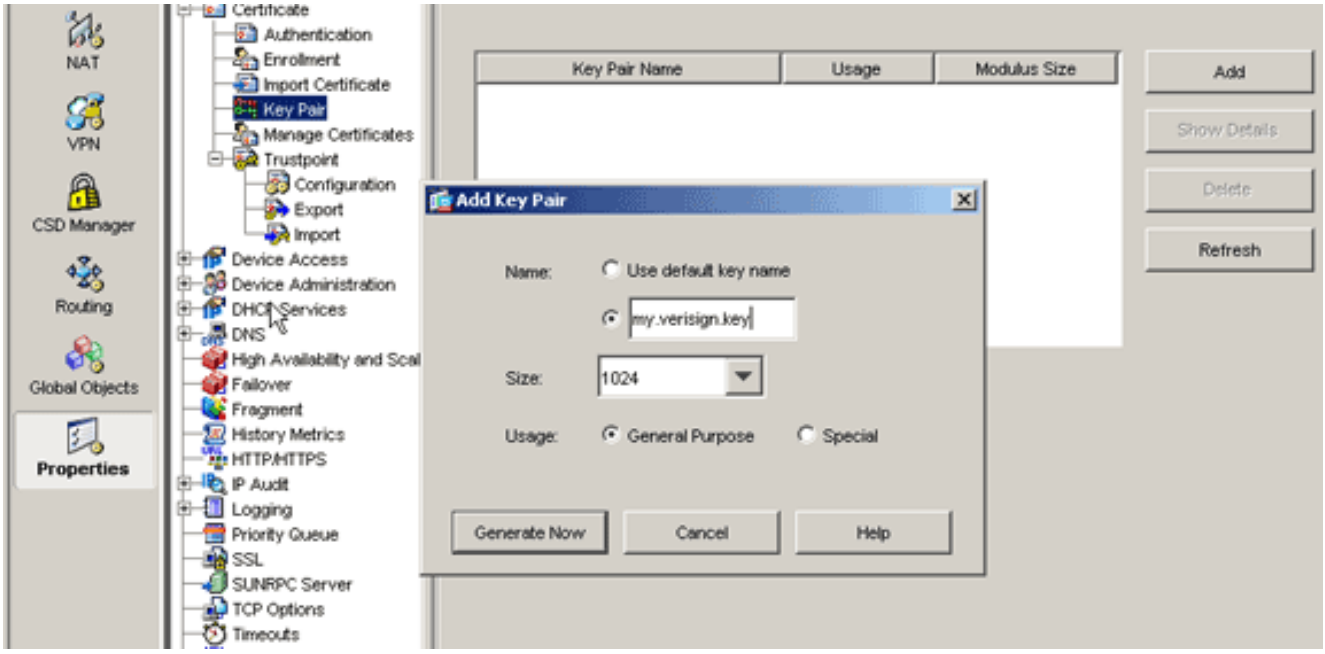
Ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

Schritt 2: Generieren des RSA-Schlüsselpaars

Der generierte öffentliche RSA-Schlüssel wird mit den Identitätsinformationen der ASA kombiniert, um eine PKCS#10-Zertifikatsanforderung zu erstellen. Sie sollten den Schlüsselnamen deutlich mit dem Trustpoint identifizieren, für den Sie das Schlüsselpaar erstellen.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Schlüsselpaar aus**.
3. Klicken Sie auf **Hinzufügen**.



4. Geben Sie den Schlüsselnamen ein, wählen Sie die Modulusgröße aus, und wählen Sie den Verwendungsart aus. Hinweis: Die empfohlene Schlüsselpaargröße ist 1024.
5. Klicken Sie auf **Generieren**.Das von Ihnen erstellte Schlüsselpaar sollte in der Spalte Key Pair Name (Name des Schlüsselpaares) aufgeführt werden.

Befehlszeilenbeispiel

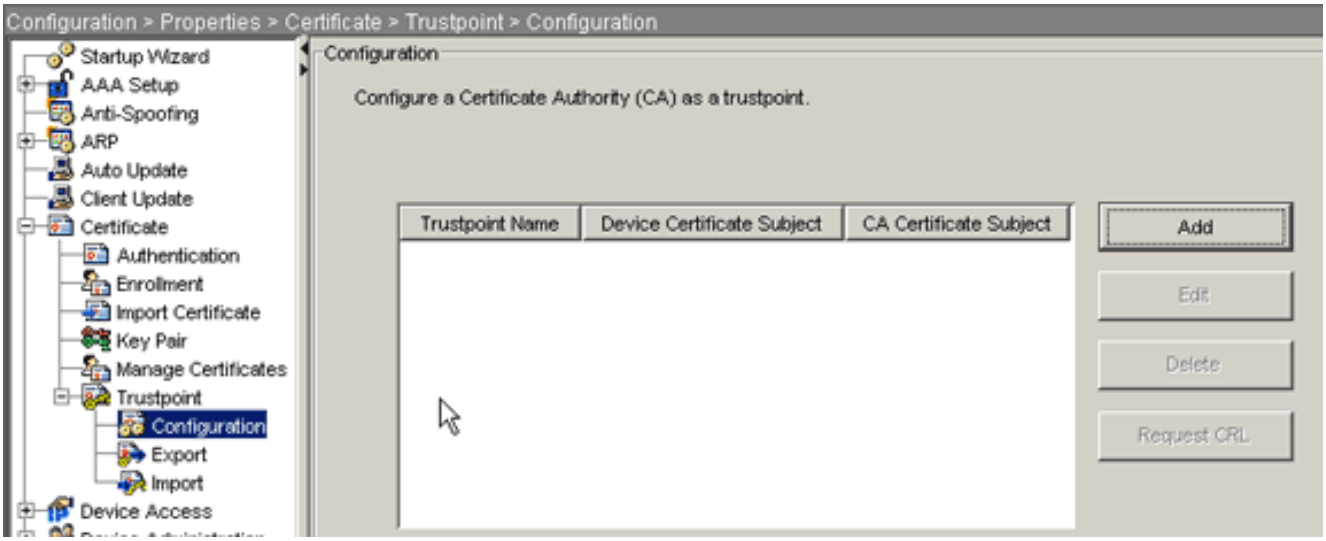
Ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

Schritt 3: Erstellen Sie den Trustpoint.

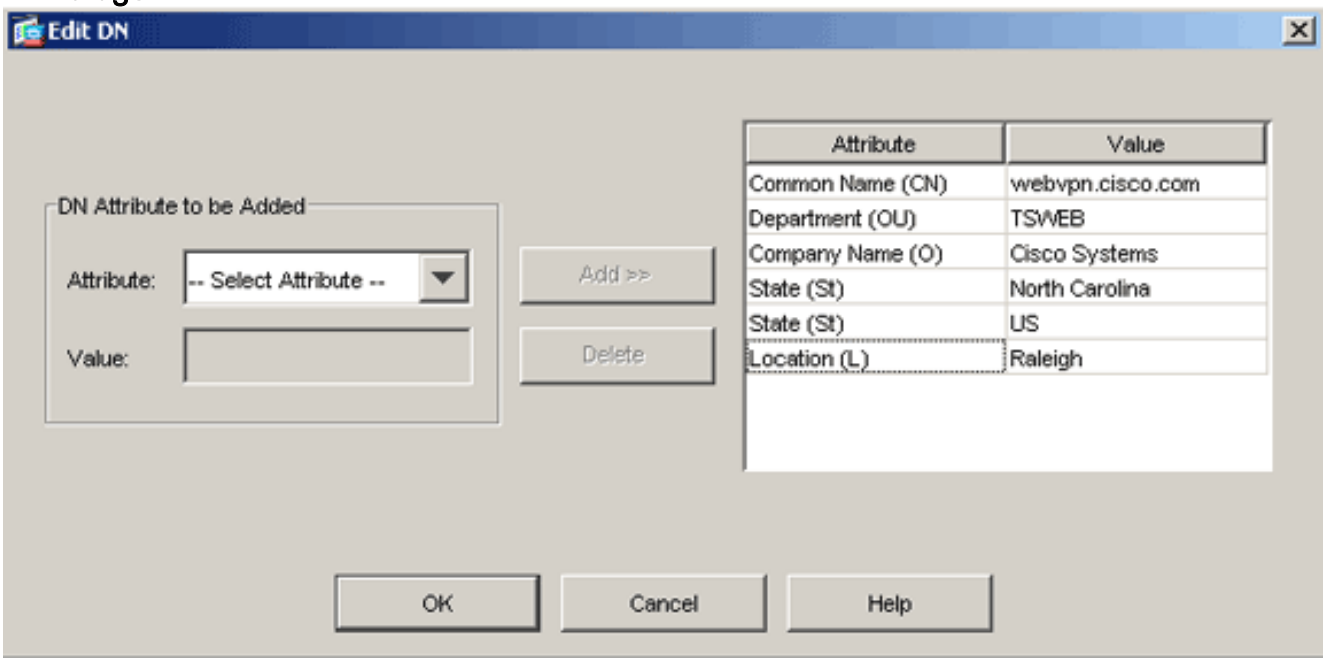
Trustpoints sind erforderlich, um die Zertifizierungsstelle (Certificate Authority, CA) zu deklarieren, die von Ihrer ASA verwendet wird.

ASDM-Verfahren

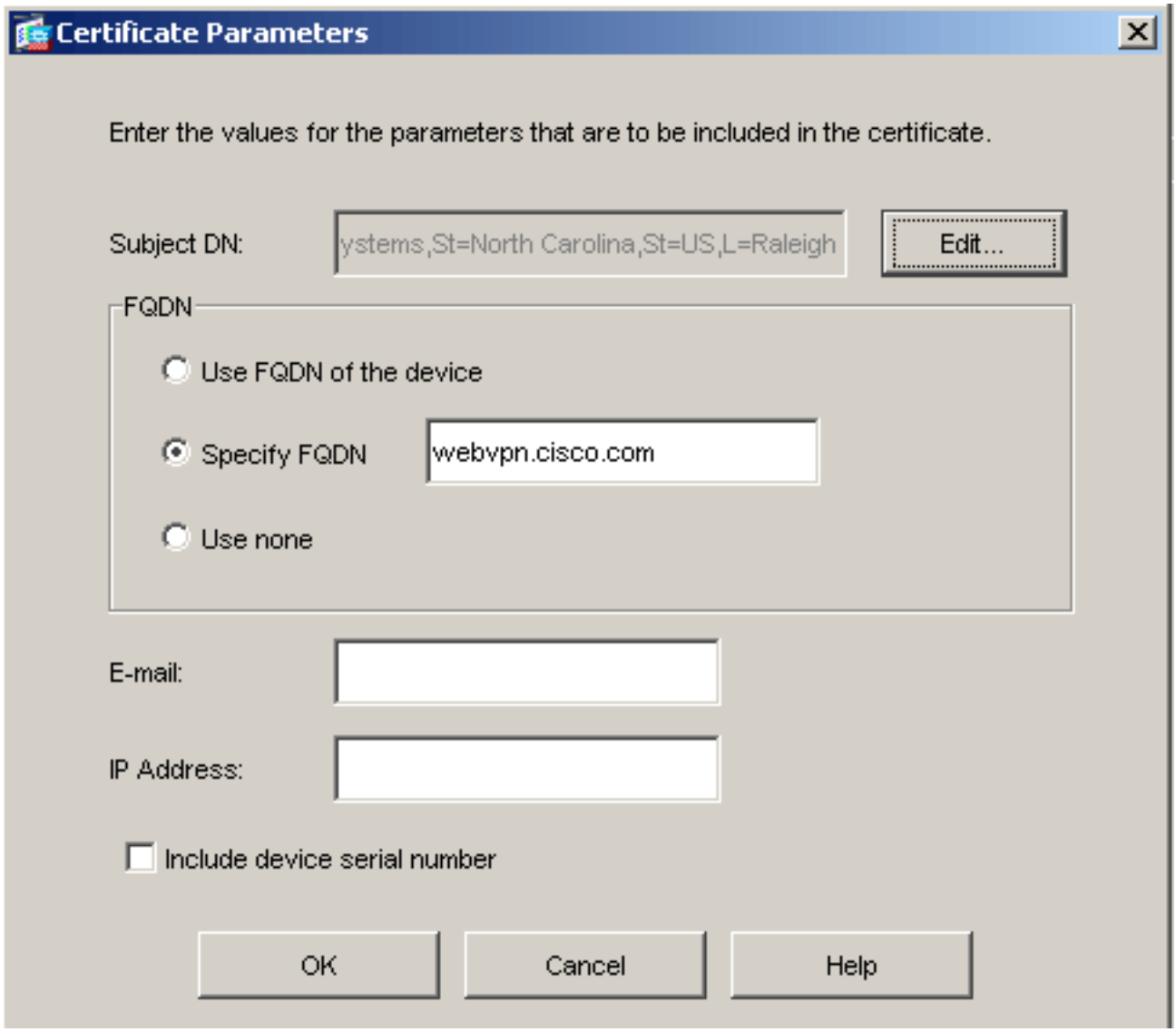
1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Certificate**, und erweitern Sie dann **Trustpoint**.
3. Wählen Sie **Konfiguration aus**, und klicken Sie auf **Hinzufügen**.



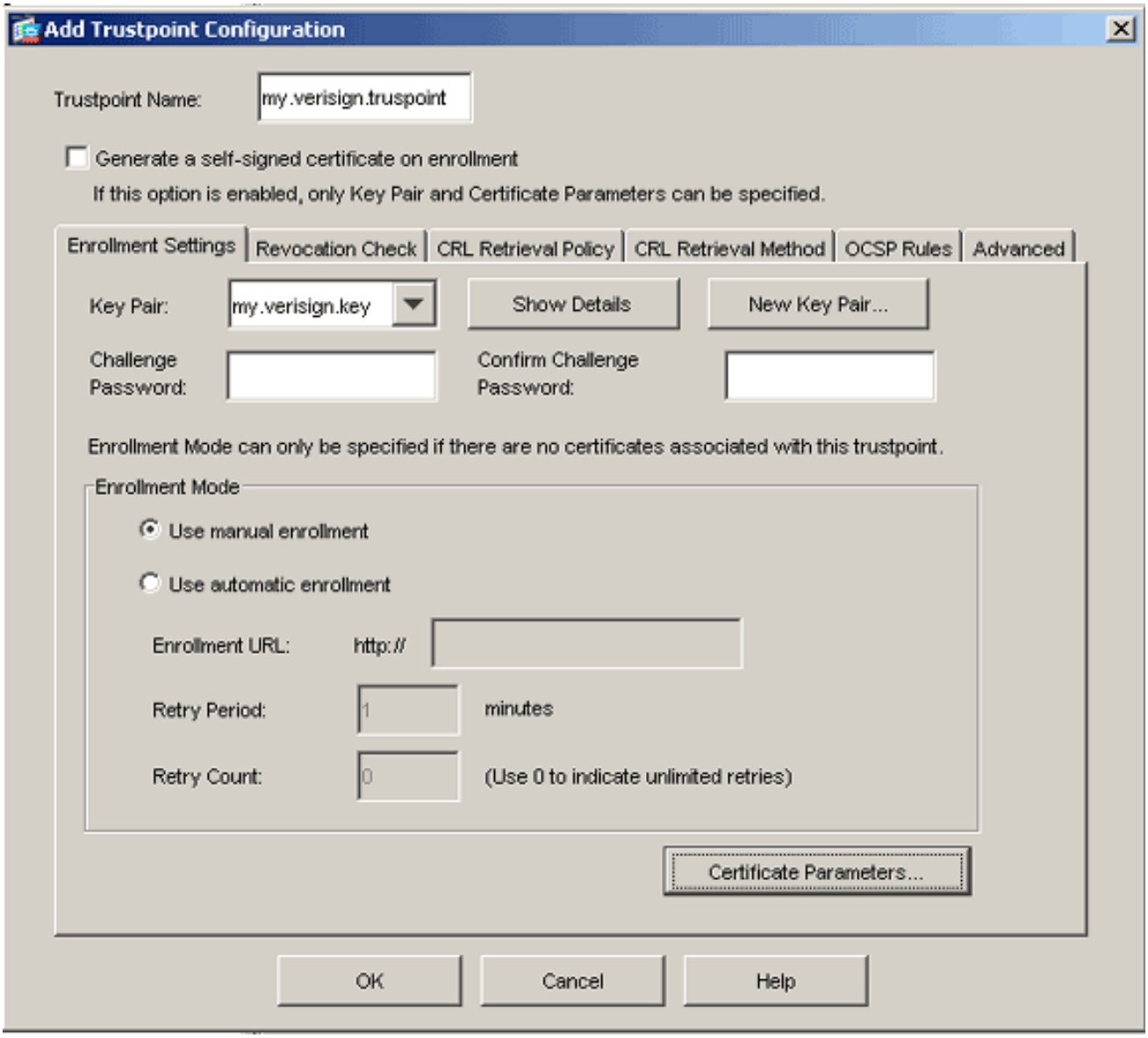
4. Konfigurieren Sie die folgenden Werte:**Trustpoint-Name**: Der Trustpoint-Name sollte für die beabsichtigte Verwendung relevant sein. (In diesem Beispiel wird *my.verisign.trustpoint* verwendet.)**Schlüsselpaar**: Wählen Sie das in Schritt 2 generierte Schlüsselpaar aus. (*my.verisign.key*)
5. Stellen Sie sicher, dass die Option Manuelle Anmeldung ausgewählt ist.
6. Klicken Sie auf **Zertifikatsparameter**.Das Dialogfeld Zertifikatparameter wird angezeigt.
7. Klicken Sie auf **Bearbeiten**, und konfigurieren Sie die in dieser Tabelle aufgelisteten Attribute:Um diese Werte zu konfigurieren, wählen Sie in der Dropdown-Liste Attribute einen Wert aus, geben Sie den Wert ein, und klicken Sie auf **Hinzufügen**.



8. Klicken Sie nach dem Hinzufügen der entsprechenden Werte auf **OK**.
9. Geben Sie im Dialogfeld Zertifikatsparameter im Feld FQDN angeben den FQDN ein.Dieser Wert sollte der gleiche FQDN sein, den Sie für den Gemeinsamen Namen (CN) verwendet haben.



10. Klicken Sie auf **OK**.
11. Überprüfen Sie, ob das richtige Schlüsselpaar ausgewählt ist, und klicken Sie auf das Optionsfeld **Manuelle Anmeldung verwenden**.
12. Klicken Sie auf **OK** und dann auf **Übernehmen**.



Befehlszeilenbeispiel

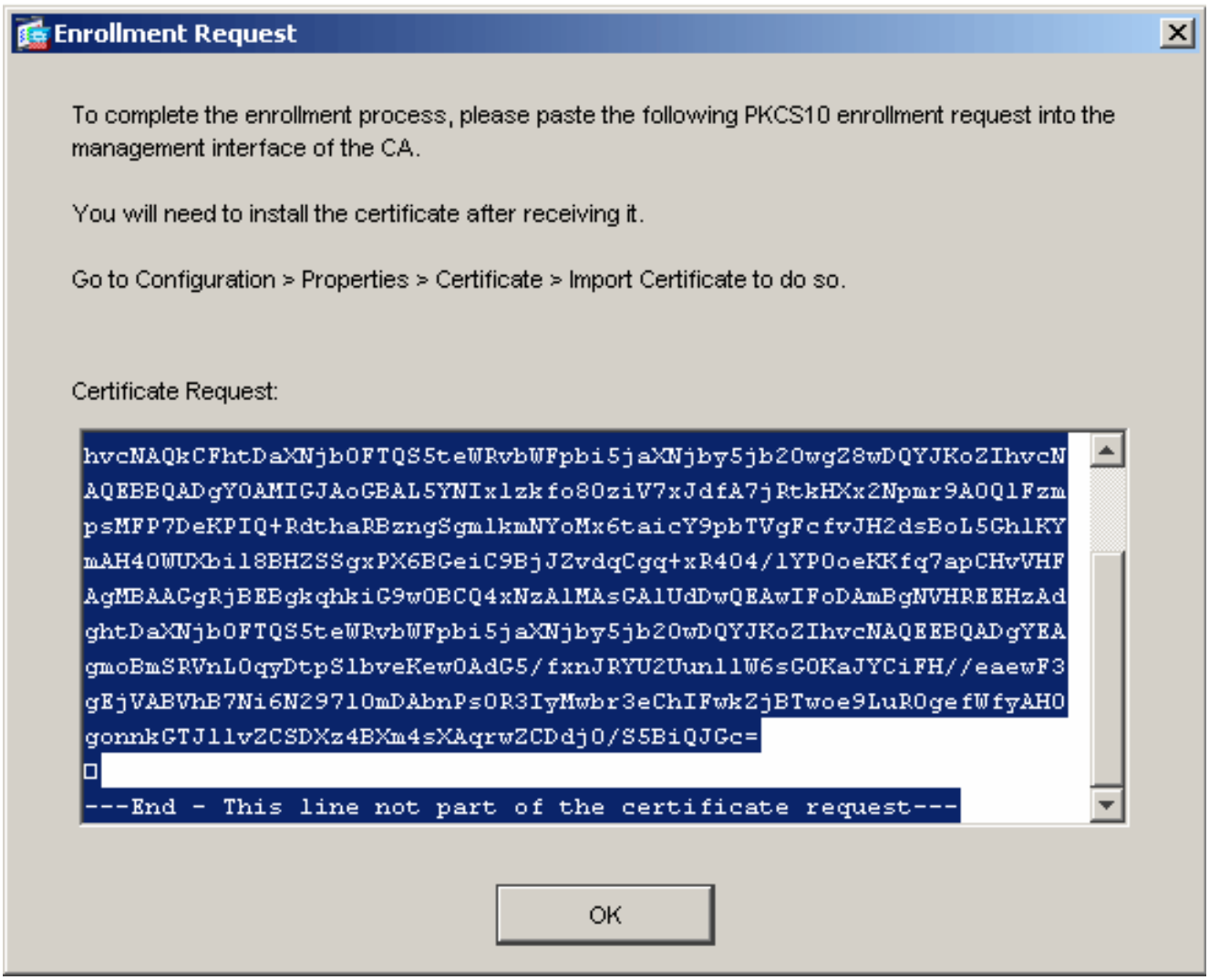
Ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco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

Schritt 4: Generieren der Zertifikatsregistrierung

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Registrierung** aus.
3. Überprüfen Sie, ob der in Schritt 3 erstellte Trustpoint ausgewählt ist, und klicken Sie auf **Registrieren**.Es wird ein Dialogfeld angezeigt, in dem die Anforderung für die Zertifikatsregistrierung (auch als Zertifikatssignierungsanfrage bezeichnet) aufgeführt ist.



4. Kopieren Sie die PKCS#10-Registrierungsanfrage in eine Textdatei und senden Sie die CSR dann an den entsprechenden Drittanbieter.Nachdem der Drittanbieter die CSR-Anfrage erhalten hat, sollte er ein Identitätszertifikat zur Installation ausstellen.

Befehlszeilenbeispiel

Gerätename 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

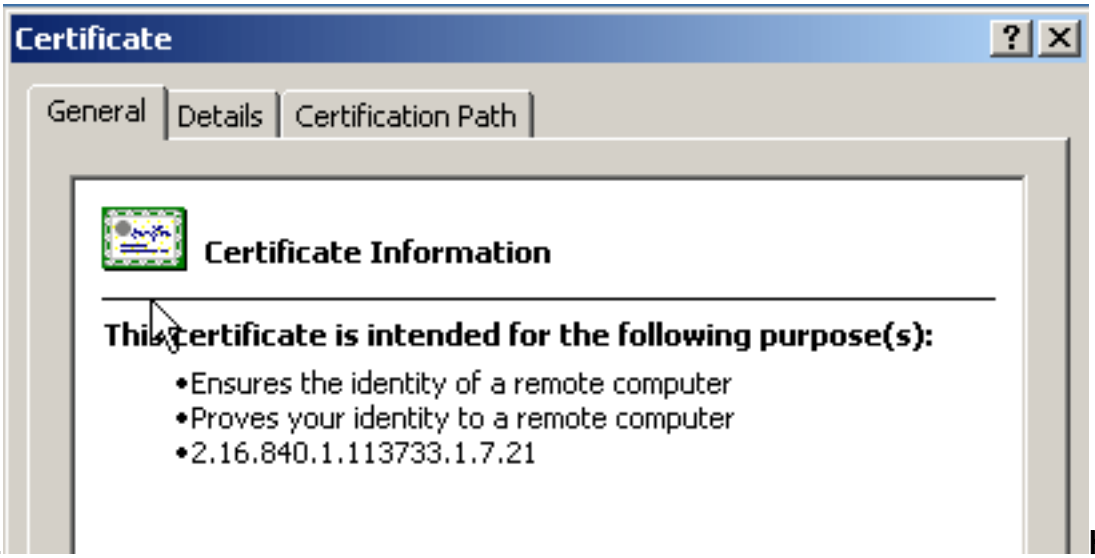
```
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the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

Schritt 5: Authentifizierung des Trustpoints

Sobald Sie das Identitätszertifikat des Fremdherstellers erhalten haben, können Sie mit diesem Schritt fortfahren.

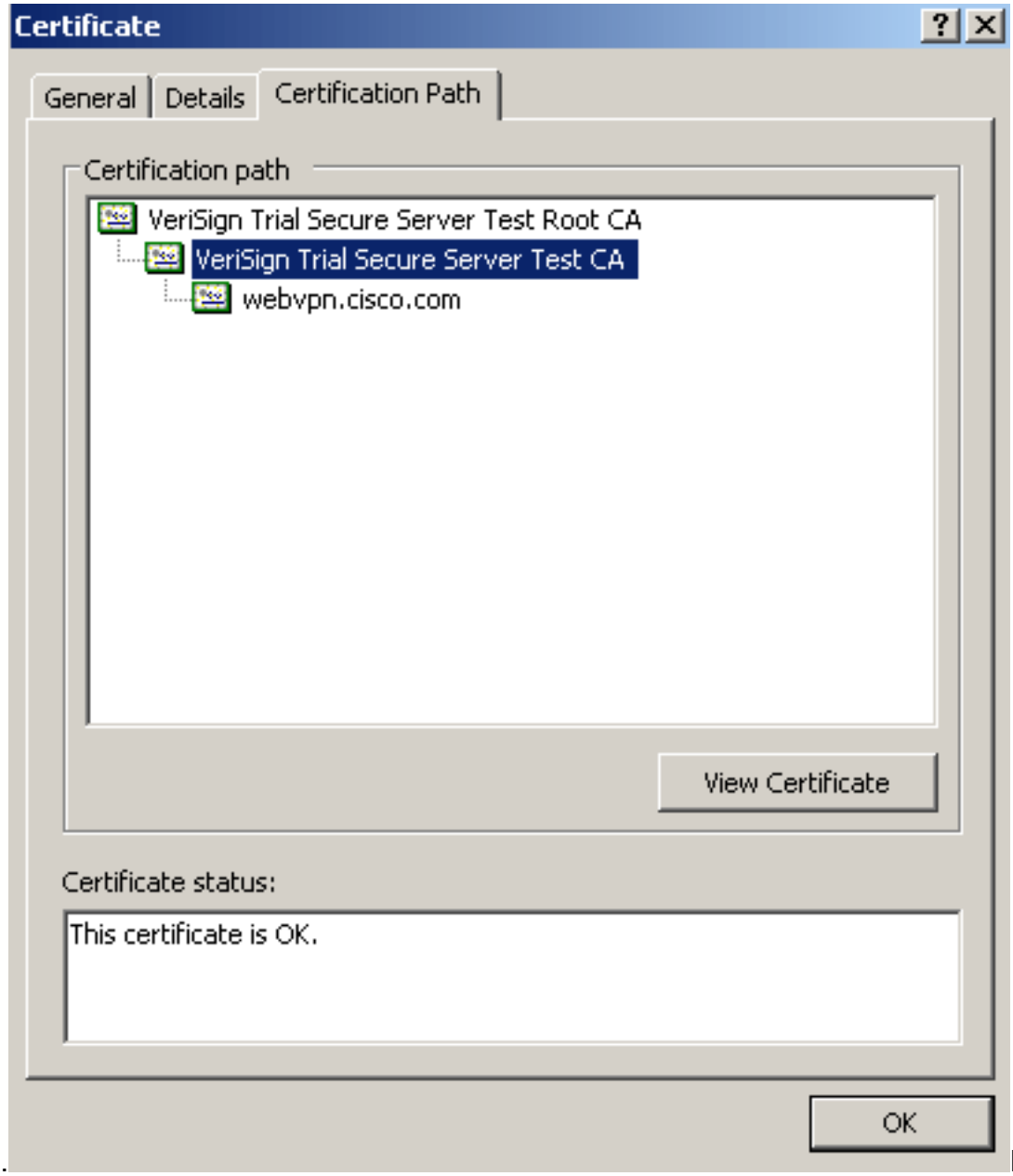
ASDM-Verfahren

1. Speichern Sie das Identitätszertifikat auf Ihrem lokalen Computer.
2. Wenn Ihnen ein Base64-kodiertes Zertifikat bereitgestellt wurde, das nicht als Datei geliefert wurde, müssen Sie die base64-Nachricht kopieren und in eine Textdatei einfügen.
3. Benennen Sie die Datei mit der Erweiterung .cer um.**Hinweis:** Sobald die Datei mit der Erweiterung .cer umbenannt wurde, sollte das Dateisymbol als Zertifikat angezeigt werden.
4. Doppelklicken Sie auf die Zertifikatsdatei.Das Dialogfeld Zertifikat wird



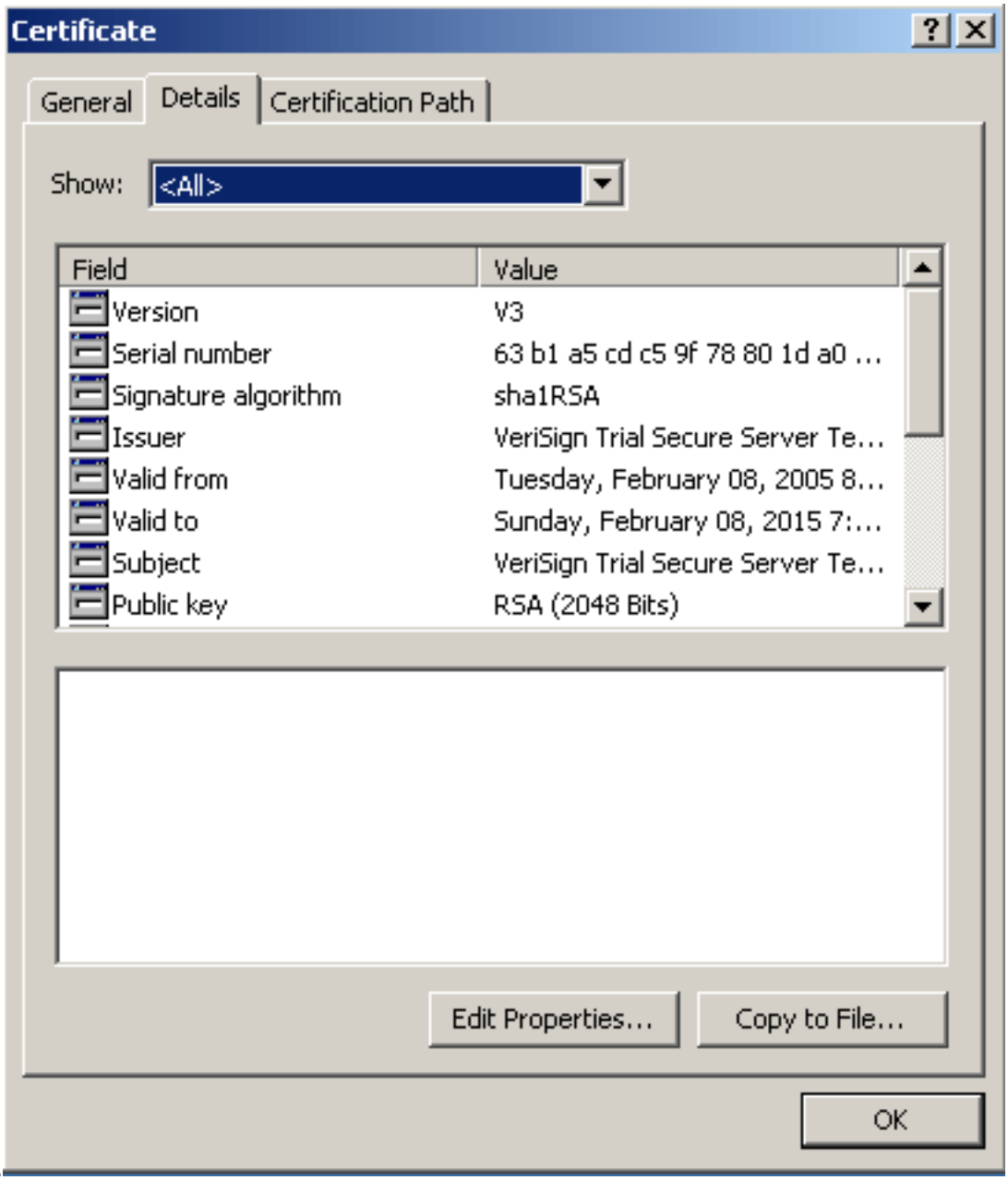
angezeigt. **Hinweis:** Wenn die Meldung "*Windows verfügt nicht über genügend Informationen, um dieses Zertifikat zu überprüfen*" auf der Registerkarte "Allgemein" angezeigt wird, müssen Sie die Root-Zertifizierungsstelle oder das Zwischenzertifikat des Fremdherstellers abrufen, bevor Sie mit diesem Verfahren fortfahren. Wenden Sie sich an Ihren Fremdhersteller oder CA-Administrator, um das ausstellende Root-CA- oder Zwischenzertifikat zu erhalten.

5. Klicken Sie auf die Registerkarte **Zertifikatspfad**.
6. Klicken Sie auf das Zertifizierungsstellenzertifikat oberhalb Ihres ausgestellten Identitätszertifikats, und klicken Sie auf **Zertifikat**



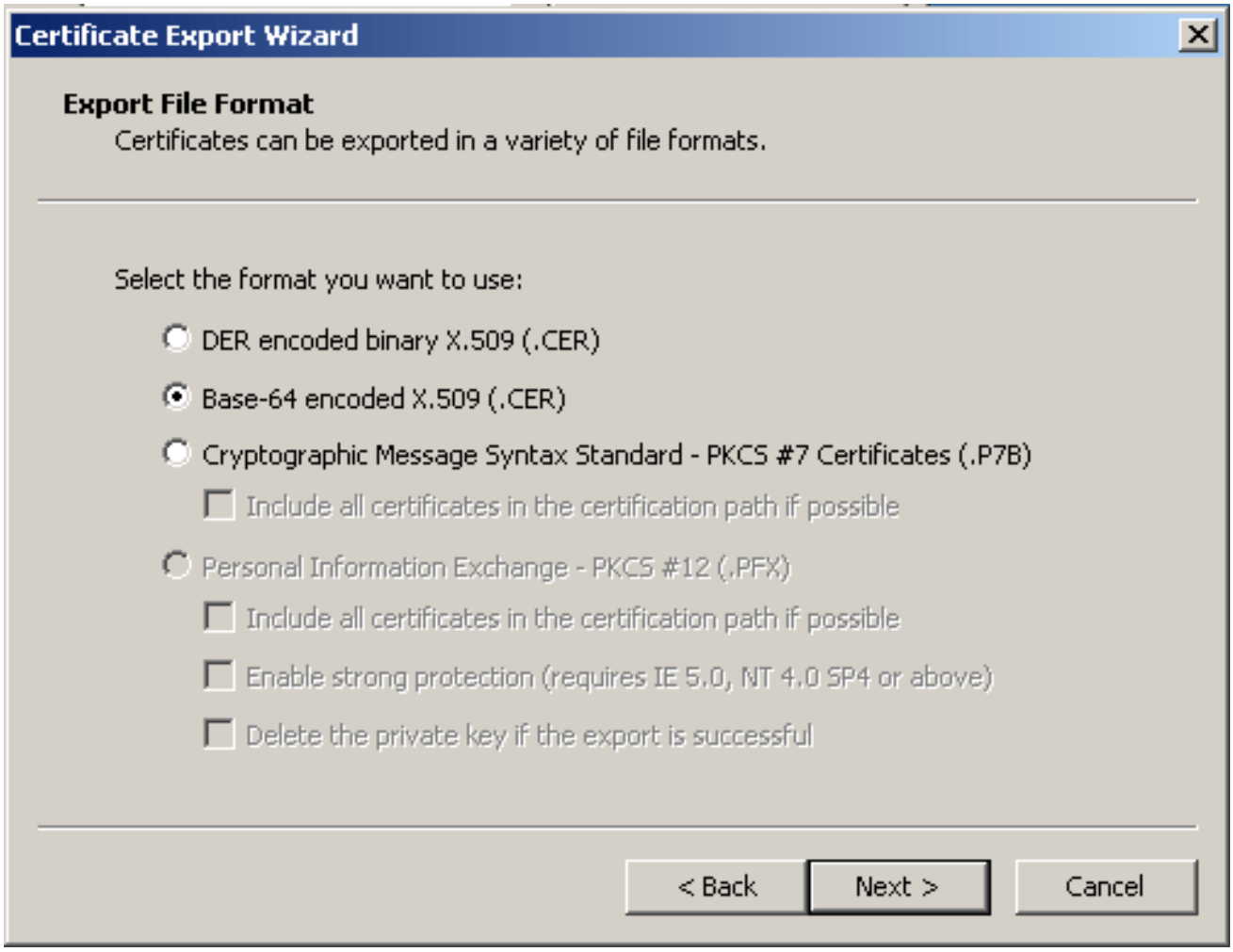
anzeigen. Detaillierte Informationen zum Zertifikat der Zertifizierungsstelle (CA) werden angezeigt.**Warnung:** Installieren Sie in diesem Schritt nicht das Identitäts-(Geräte-)Zertifikat. In diesem Schritt werden nur das Root-, untergeordnete Root- oder CA-Zertifikat hinzugefügt. Die Identitäts-(Geräte-)Zertifikate werden in Schritt 6 installiert.

7. Klicken Sie auf

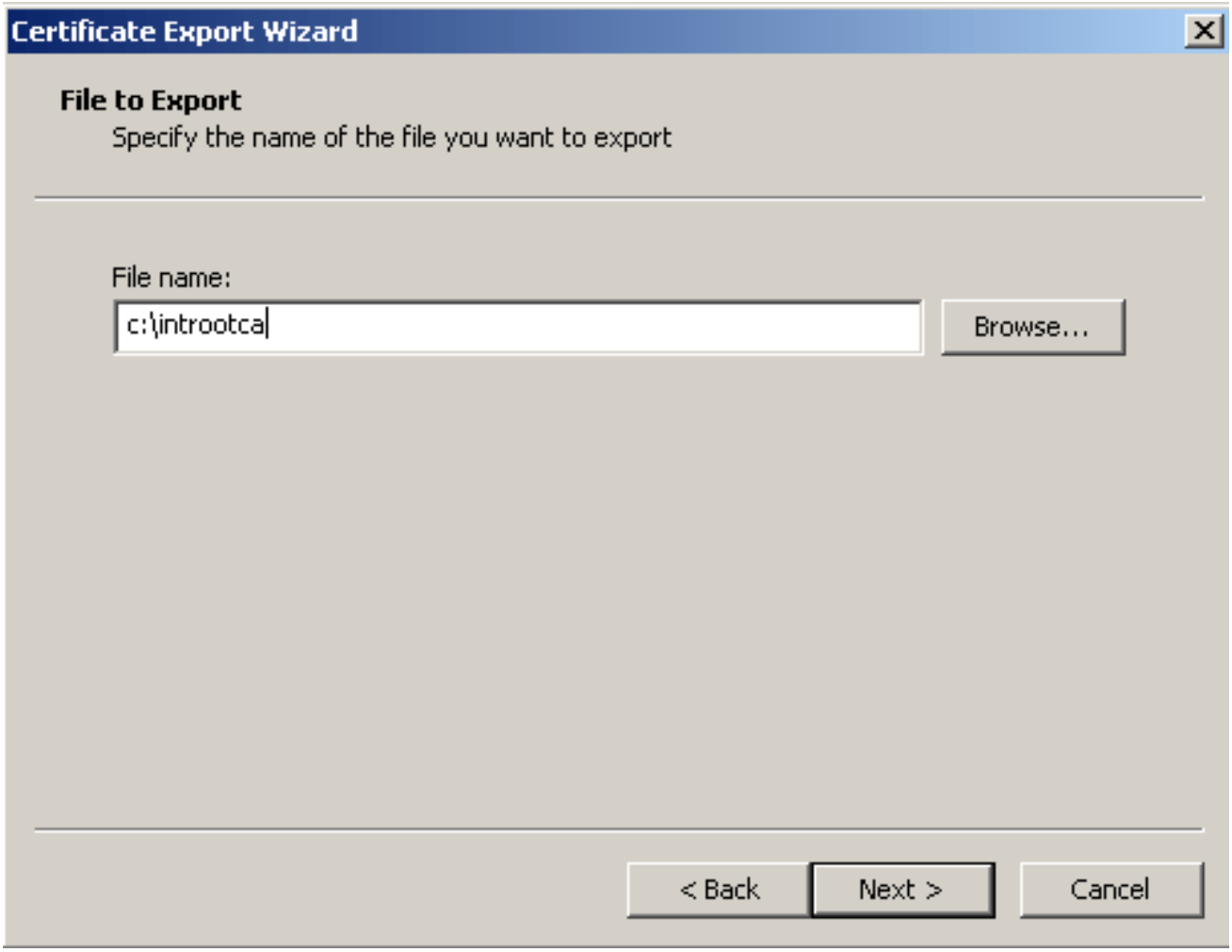


Details.

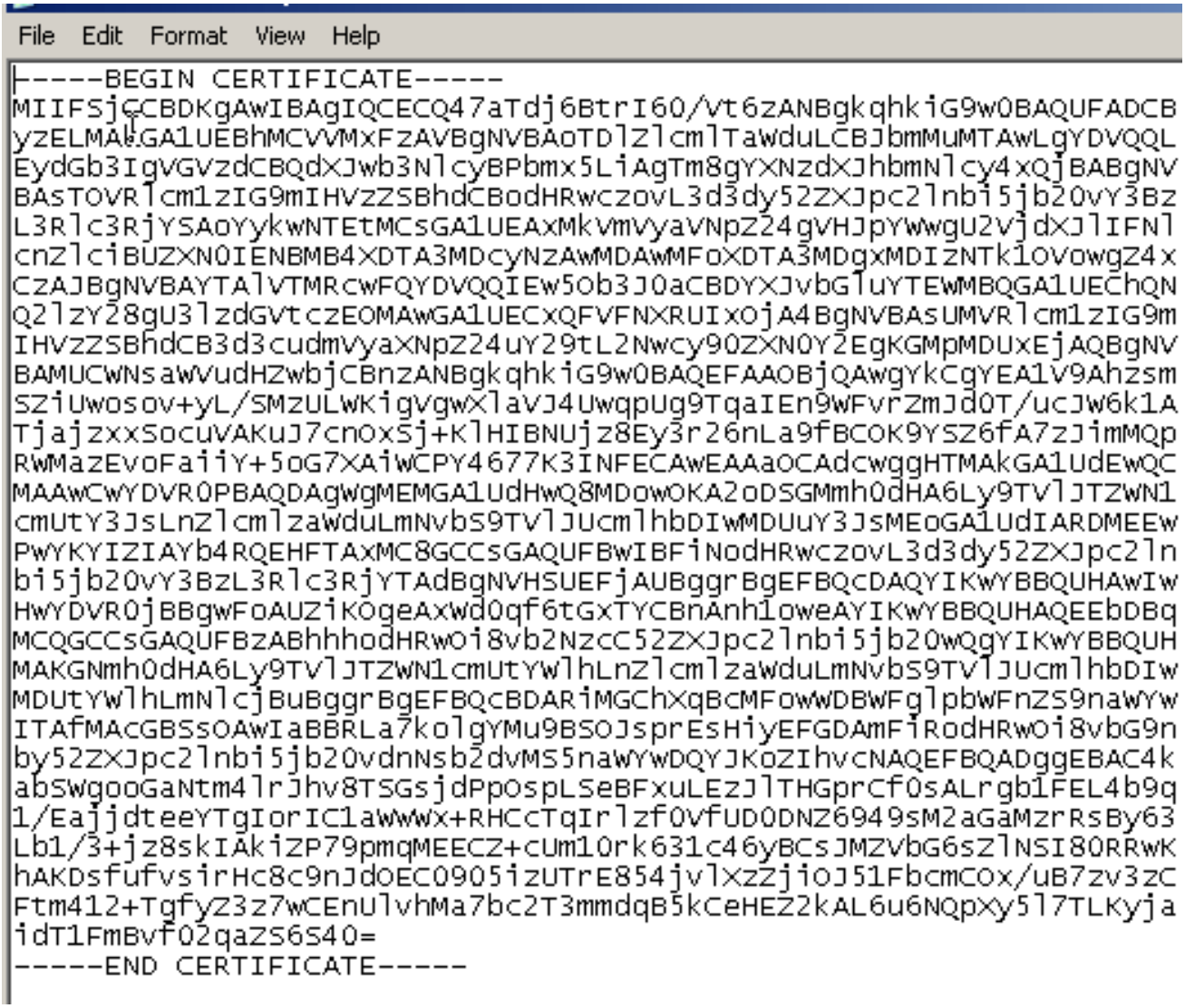
8. Klicken Sie auf **In Datei kopieren**.
9. Klicken Sie im Assistenten für den Zertifikatsexport auf **Weiter.**
10. Klicken Sie im Dialogfeld Dateiformat exportieren auf das Optionsfeld **Base-64-codierte X.509 (.CER)** und anschließend auf **Weiter**.



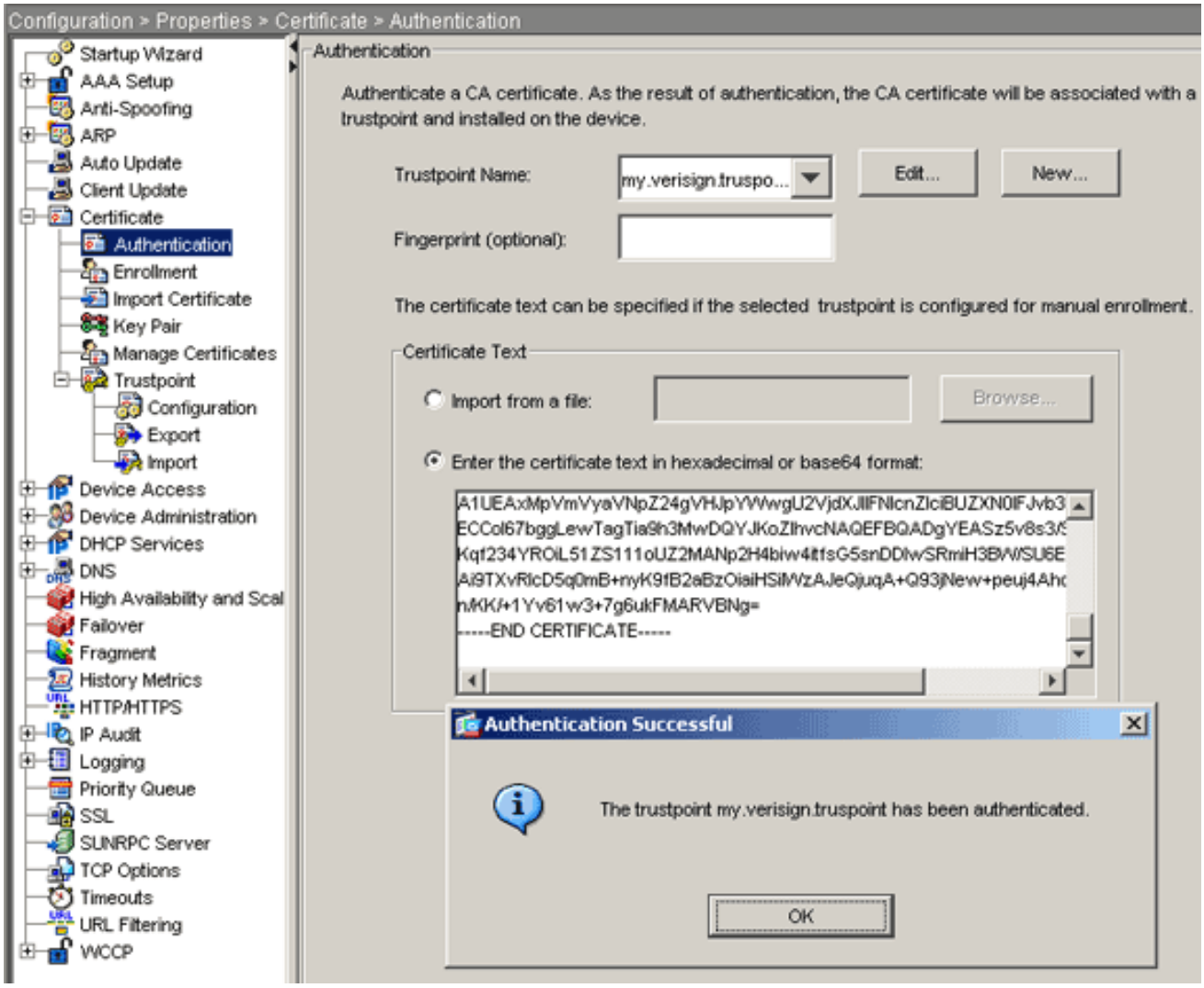
11. Geben Sie den Dateinamen und den Speicherort ein, in dem Sie das Zertifizierungsstellenzertifikat speichern möchten.
12. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.



13. Klicken Sie im Dialogfeld "Exportieren erfolgreich" auf **OK**.
14. Navigieren Sie zu dem Speicherort, an dem Sie das Zertifizierungsstellenzertifikat gespeichert haben.
15. Öffnen Sie die Datei mit einem Texteditor, z. B. Notepad. (Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Senden an > Editor**.)Die Base64-codierte Nachricht sollte ähnlich wie das Zertifikat in diesem Bild aussehen:



16. Klicken Sie im ASDM auf **Konfiguration** und dann auf **Eigenschaften.**
17. Erweitern Sie **Zertifikat**, und wählen Sie **Authentifizierung aus**.
18. Klicken Sie auf das Optionsfeld **Zertifikattext im Hexadezimal- oder Base64-Format eingeben**.
19. Fügen Sie das Base64-formatierte CA-Zertifikat aus dem Texteditor in den Textbereich ein.
20. Klicken Sie auf **Authentifizierung**.



21. Klicken Sie auf **OK**.

Befehlszeilenbeispiel

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
```

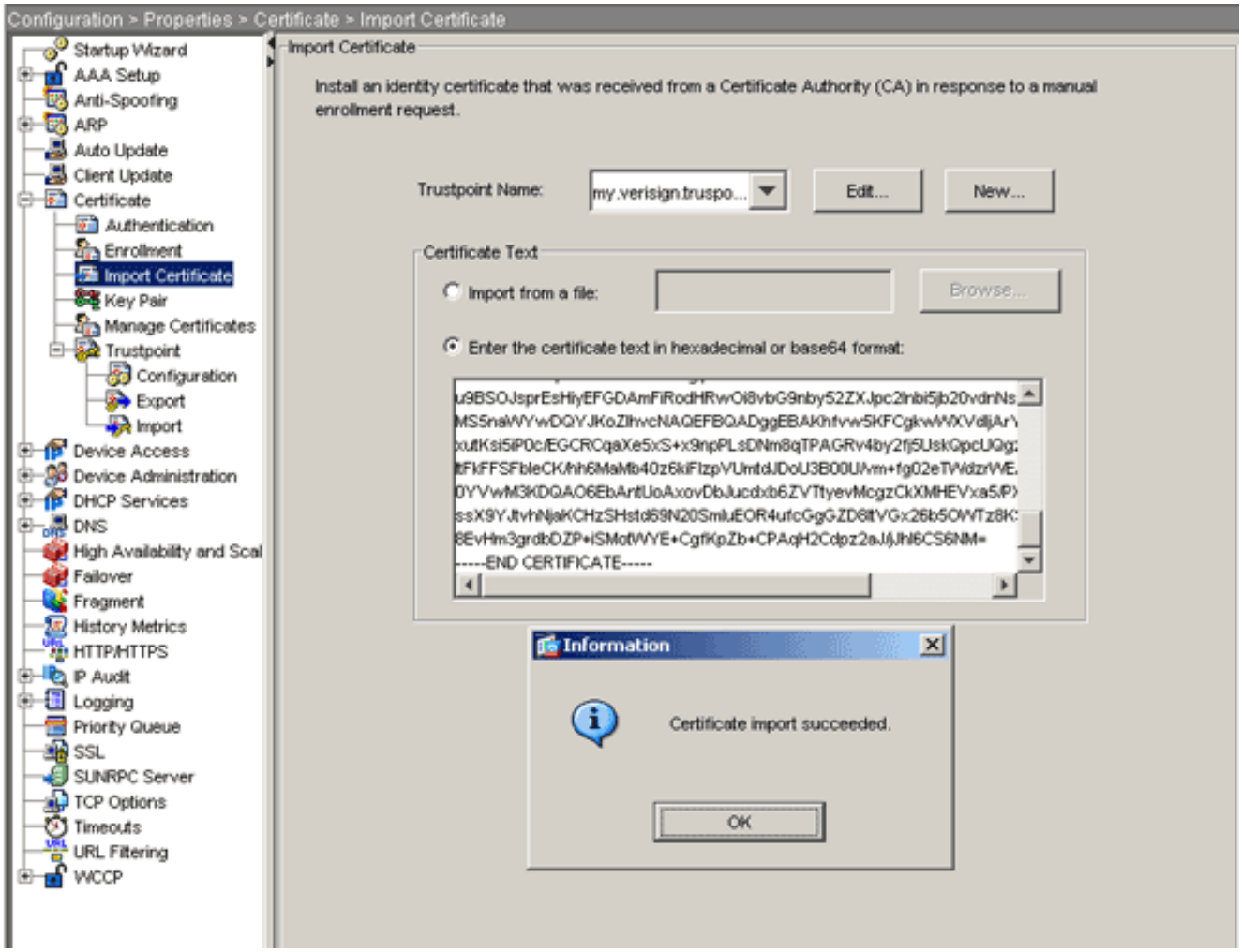
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo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

Schritt 6: Installieren des Zertifikats

ASDM-Verfahren

Führen Sie die folgenden Schritte mit dem vom Fremdhersteller bereitgestellten Identitätszertifikat durch:

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Zertifikat importieren aus**.
3. Klicken Sie auf das Optionsfeld **Zertifikattext im Hexadezimalformat oder im Base64-Format eingeben**, und fügen Sie das Base64-Identitätszertifikat in das Textfeld ein.



4. Klicken Sie auf **Importieren** und anschließend auf **OK**.

Befehlszeilenbeispiel

Ciscoasa

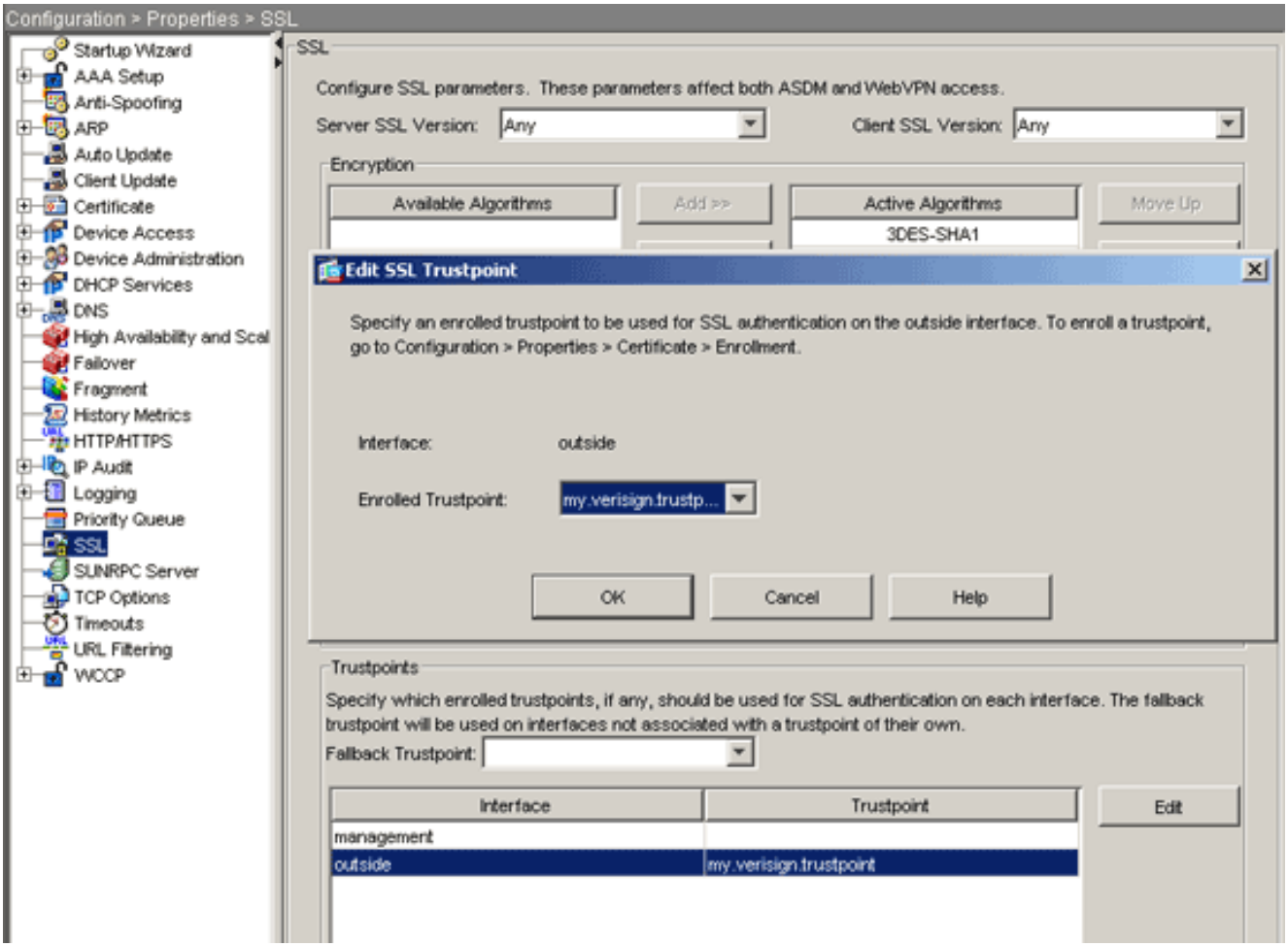
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! 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)#
```

Schritt 7: Konfigurieren von WebVPN zur Verwendung des neu installierten Zertifikats

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration**, klicken Sie auf **Eigenschaften**, und wählen Sie **SSL** aus.
2. Wählen Sie im Bereich Trustpoints die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. (In diesem Beispiel wird die externe Schnittstelle verwendet.)
3. Klicken Sie auf **Bearbeiten**.Das Dialogfeld "SSL-Vertrauenspunkt bearbeiten" wird angezeigt.



4. Wählen Sie aus der Dropdown-Liste für registrierte Vertrauenswürdigkeit den Vertrauenspunkt aus, den Sie in Schritt 3 erstellt haben.
5. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Ihr neues Zertifikat sollte nun für alle WebVPN-Sitzungen verwendet werden, die auf der angegebenen Schnittstelle enden. Weitere Informationen zum Überprüfen einer erfolgreichen Installation finden Sie im Abschnitt Überprüfen dieses Dokuments.

Befehlszeilenbeispiel

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.
```

Überprüfen

In diesem Abschnitt wird beschrieben, wie Sie bestätigen können, dass das Zertifikat Ihres Fremdherstellers erfolgreich installiert wurde.

Selbstsigniertes Zertifikat von ASA ersetzen

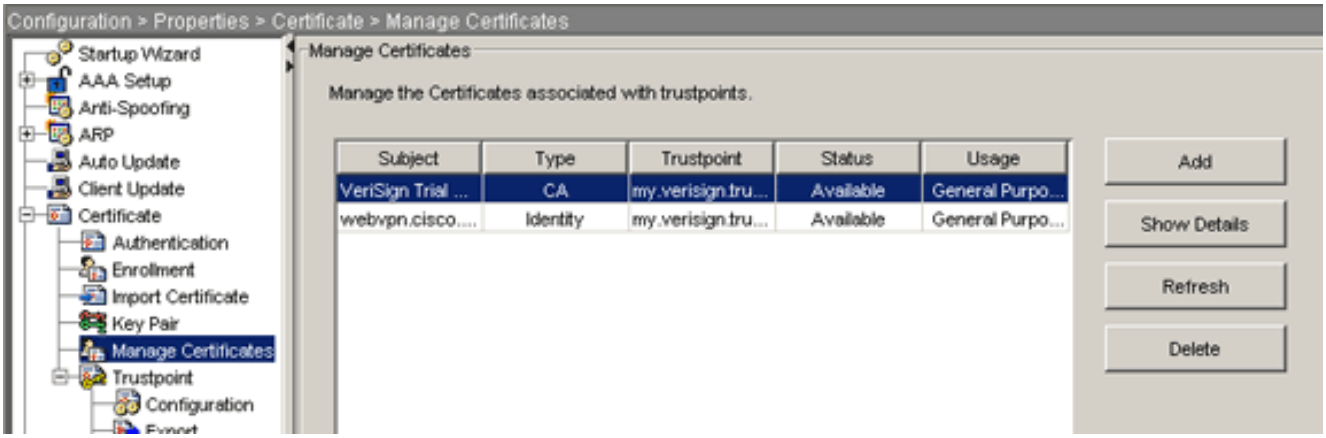
In diesem Abschnitt wird beschrieben, wie das installierte selbstsignierte Zertifikat von der ASA ersetzt wird.

1. Stellen Sie eine Zertifikatssignierungsanfrage an Verisign aus.Nachdem Sie das angeforderte Zertifikat von Verisign erhalten haben, können Sie es direkt unter demselben Vertrauenspunkt installieren.
2. Geben Sie diesen Befehl ein: **crypto ca enroll Verifier**Sie werden aufgefordert, Fragen zu beantworten.
3. Geben Sie als Anforderung zur Ausstellung eines Zertifikats an terminal **yes ein**, und senden Sie die Ausgabe an Verisign.
4. Geben Sie den folgenden Befehl ein, sobald Sie das neue Zertifikat erhalten haben: **crypto ca import Verifier-Zertifikat**

Installierte Zertifikate anzeigen

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Zertifikate verwalten aus**.Das für die Trustpoint-Authentifizierung verwendete Zertifizierungsstellenzertifikat und das vom Fremdhersteller ausgestellte Identitätszertifikat sollten im Bereich Zertifikate verwalten angezeigt werden.



Befehlszeilenbeispiel

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\,

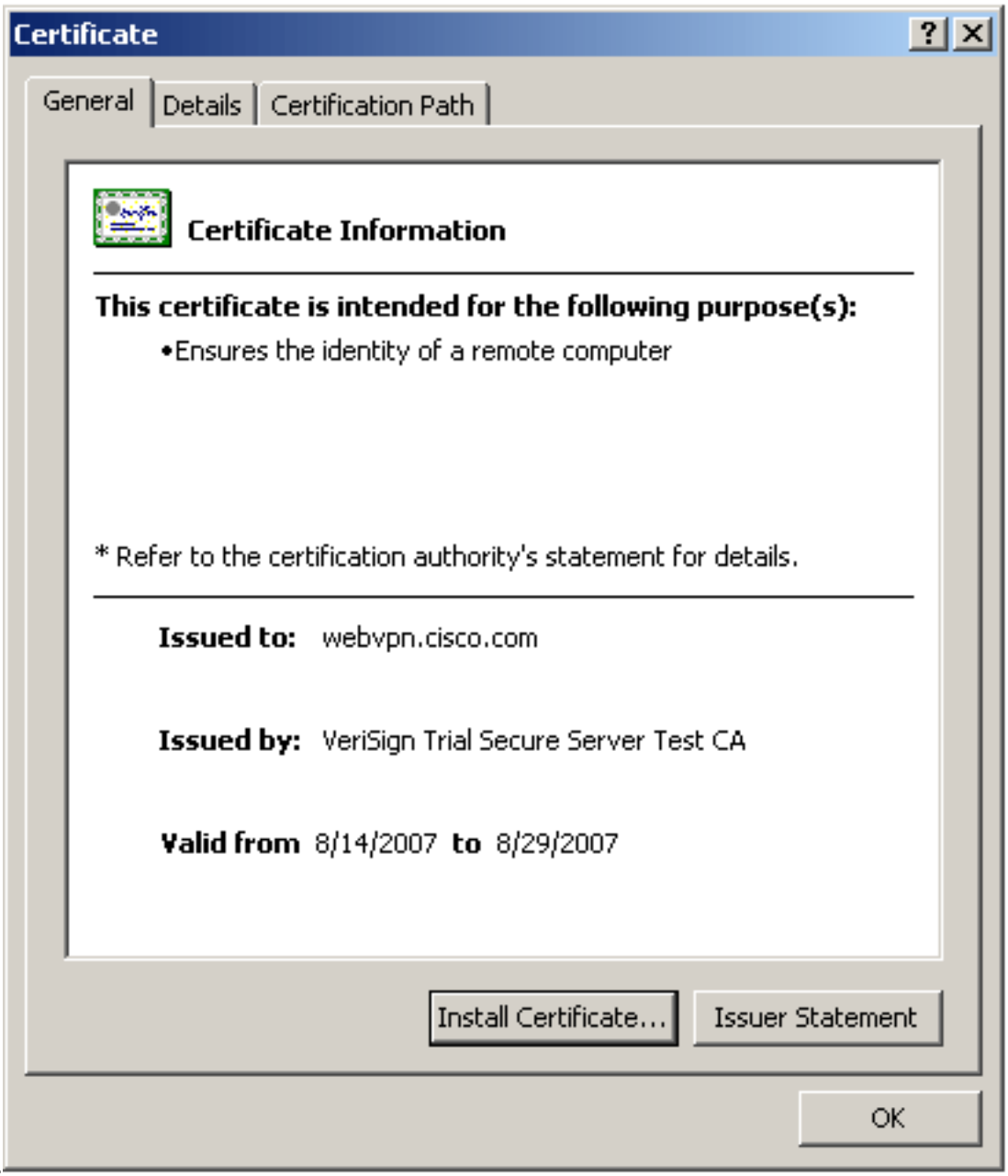
```
Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of
use at www.verisign.com/cps/testca (c)05 ou=TSWEB
o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP
AIA: URL: http://ocsp.verisign.com CRL Distribution
Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start
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.
```

Überprüfen des installierten Zertifikats für WebVPN mit einem Webbrowser

Gehen Sie wie folgt vor, um zu überprüfen, ob WebVPN das neue Zertifikat verwendet:

1. Stellen Sie über einen Webbrowser eine Verbindung zur WebVPN-Schnittstelle her. Verwenden Sie https:// zusammen mit dem FQDN, mit dem Sie das Zertifikat angefordert haben (z. B. https://webvpn.cisco.com).Wenn Sie eine dieser Sicherheitswarnungen erhalten, gehen Sie wie folgt vor:**Der Name des Sicherheitszertifikats ist ungültig oder stimmt nicht mit dem Namen der Site überein.**Überprüfen Sie, ob Sie den richtigen FQDN/CN verwendet haben, um eine Verbindung zur WebVPN-Schnittstelle der ASA herzustellen. Sie müssen den FQDN/CN verwenden, den Sie bei Anforderung des Identitätszertifikats definiert haben. Sie können den Befehl **show crypto ca certificate trustpointname** verwenden, um die Zertifikate FQDN/CN zu überprüfen.**Das Sicherheitszertifikat wurde von einem Unternehmen ausgestellt, dem Sie nicht vertrauen..**Führen Sie die folgenden Schritte aus, um das Root-Zertifikat des Fremdherstellers in Ihrem Webbrowser zu installieren:Klicken Sie im Dialogfeld Sicherheitswarnung auf **Zertifikat anzeigen**.Klicken Sie im Dialogfeld Zertifikat auf die Registerkarte **Zertifikatspfad**.Wählen Sie das Zertifizierungsstellenzertifikat über Ihrem ausgestellten Identitätszertifikat aus, und klicken Sie auf **Zertifikat anzeigen**.Klicken Sie auf **Zertifikat installieren**.Klicken Sie im Dialogfeld Assistent für die Zertifikatsinstallation auf **Weiter**.Wählen Sie das Optionsfeld **Automatisch den Zertifikatsspeicher entsprechend des Zertifikatstyps aus**, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**.Klicken Sie auf **Ja**, wenn Sie die Bestätigungsaufforderung für die Installation des Zertifikats erhalten.Klicken Sie bei der Eingabeaufforderung Importvorgang war erfolgreich auf **OK** und dann auf **Ja**.**Hinweis:** Da in diesem Beispiel das Verisign Trial Certificate verwendet wird, muss das Stammzertifikat der Verisign Trial CA installiert werden, um Überprüfungsfehler zu vermeiden, wenn Benutzer eine Verbindung herstellen.
2. Doppelklicken Sie auf das Sperrsymbol, das in der rechten unteren Ecke der WebVPN-Anmeldeseite angezeigt wird.Die Informationen zum installierten Zertifikat sollten angezeigt werden.

3. Überprüfen Sie den Inhalt, um sicherzustellen, dass er mit dem Zertifikat Ihres Drittanbieters übereinstimmt.



Schritte zur Verlängerung des SSL-Zertifikats

Gehen Sie wie folgt vor, um das SSL-Zertifikat zu erneuern:

1. Wählen Sie den Vertrauenspunkt aus, den Sie verlängern möchten.
2. Wählen Sie **Einschreiben aus**.Diese Meldung wird angezeigt:*Wenn das Zertifikat erneut erfolgreich registriert wurde, wird es durch die neuen Zertifikate ersetzt. Möchten Sie fortfahren?*
3. Wählen Sie **Ja aus**.Dadurch wird eine neue CSR-Anfrage erstellt.
4. Senden Sie die CSR an Ihre CA, und importieren Sie dann das neue ID-Zertifikat, wenn Sie es zurückerhalten.
5. Entfernen Sie den Vertrauenspunkt, und wenden Sie ihn erneut auf die externe Schnittstelle an.

Befehle

Auf der ASA können Sie mehrere Befehle zur Anzeige in der Befehlszeile verwenden, um den Status eines Zertifikats zu überprüfen.

- **show crypto ca trustpoint**: Zeigt konfigurierte Trustpoints an.
- **show crypto ca certificate**: Zeigt alle Zertifikate an, die auf dem System installiert sind.
- **show crypto ca crls**: Zeigt zwischengespeicherte Zertifikatswiderruflisten (CRL) an.
- **show crypto key mypubkey rsa**: Zeigt alle generierten Krypto-Schlüsselpaare an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hier einige mögliche Fehler, die Sie möglicherweise feststellen:

- **% Warnung: CA-Zertifikat wurde nicht gefunden. Die importierten Zertifikate sind möglicherweise nicht verwendbar.INFO: Zertifikat erfolgreich importiert**Das Zertifikat der Zertifizierungsstelle wurde nicht korrekt authentifiziert. Verwenden Sie den Befehl show crypto ca certificate trustpointname, um zu überprüfen, ob das CA-Zertifikat installiert wurde. Suchen Sie nach der Zeile, die mit dem Zertifizierungsstellenzertifikat beginnt. Wenn das Zertifizierungsstellenzertifikat installiert ist, stellen Sie sicher, dass es auf den richtigen Vertrauenspunkt verweist.
- FEHLER: Importiertes Zertifikat konnte nicht analysiert oder verifiziert werden.Dieser Fehler kann auftreten, wenn Sie das Identitätszertifikat installieren und nicht das richtige Zwischen- oder Stammzertifikat der CA mit dem zugehörigen Vertrauenspunkt authentifiziert haben. Sie müssen das richtige Zwischen- oder Stammzertifikat der CA entfernen und erneut authentifizieren. Wenden Sie sich an Ihren Fremdhersteller, um zu überprüfen, ob Sie das richtige Zertifizierungsstellenzertifikat erhalten haben.
- Das Zertifikat enthält keinen allgemeinen öffentlichen Schlüssel.Dieser Fehler kann auftreten, wenn Sie versuchen, Ihr Identitätszertifikat auf dem falschen Trustpoint zu installieren. Sie versuchen, ein ungültiges Identitätszertifikat zu installieren, oder das Schlüsselpaar, das dem Trustpoint zugeordnet ist, stimmt nicht mit dem öffentlichen Schlüssel überein, der im Identitätszertifikat enthalten ist. Verwenden Sie den **Befehl show crypto ca certificate *trustpointname*, um zu überprüfen, ob Sie Ihr Identitätszertifikat auf dem richtigen Vertrauenspunkt installiert haben.** Suchen Sie nach dem Posten, der *Associated Trustpoints* angibt*:* Wenn der falsche Vertrauenspunkt aufgeführt ist, verwenden Sie die in diesem Dokument beschriebenen Verfahren, um den richtigen Vertrauenspunkt zu entfernen und neu zu installieren. Überprüfen Sie außerdem, ob sich die Tastatur seit der Generierung des CSR nicht geändert hat.
- **Fehlermeldung: %PIX|ASA-3-717023 SSL konnte das Gerätezertifikat nicht für Trustpoint [trustpoint name] festlegen.**Diese Meldung wird angezeigt, wenn ein Fehler auftritt, wenn Sie ein Gerätezertifikat für den angegebenen Vertrauenspunkt zur Authentifizierung der SSL-Verbindung festlegen. Beim Herstellen der SSL-Verbindung wird versucht, das verwendete Gerätezertifikat festzulegen. Wenn ein Fehler auftritt, wird eine Fehlermeldung protokolliert, die den konfigurierten Trustpoint enthält, der zum Laden des Gerätezertifikats verwendet werden soll, sowie den Grund für den Fehler.*trustpoint name (Vertrauenspunktname): Name des Trustpoints, für den SSL kein Gerätezertifikat festgelegt hat.***Empfohlene Aktion:** Beheben Sie das Problem, das durch den gemeldeten Fehlergrund angegeben wurde.Stellen Sie sicher, dass der angegebene Trustpoint registriert ist und über ein Gerätezertifikat

verfügt.Vergewissern Sie sich, dass das Gerätezertifikat gültig ist.Registrieren Sie ggf. den Trustpoint erneut.

Zugehörige Informationen

- So erhalten Sie ein digitales Zertifikat von einer Microsoft Windows CA mithilfe von ASDM auf einer ASA
- Problemhinweise zu Sicherheitsprodukten
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems