ASA 7.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例

目次

概要

この設定例では、WebVPN で使用するサードパーティ ベンダーのデジタル証明書を、ASA 上で手動でインストールする方法について説明しています。 この例では、Verisign Trial Certificate を使用しています。 各ステップには、ASDM アプリケーションの手順と CLI の例が記載されています。

前提条件

要件

このドキュメントでは、証明書を登録するために Certificate Authority（CA; 認証局）にアクセス

する必要があります。 サポートされるサード パーティ CA ベンダーは、Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA、および VeriSign です。

使用するコンポーネント

このドキュメントでは、ソフトウェア バージョン 7.2(1) および ASDM バージョン 5.2(1) が稼働する ASA 5510 を使用しています。 ただし、このドキュメントの手順は、互換性のある ASDM バージョンと共に 7.x を実行する ASA アプライアンス上で動作します。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

PIX/ASA 上にサード パーティ ベンダーのデジタル証明書をインストールするには、次の手順を実行します。

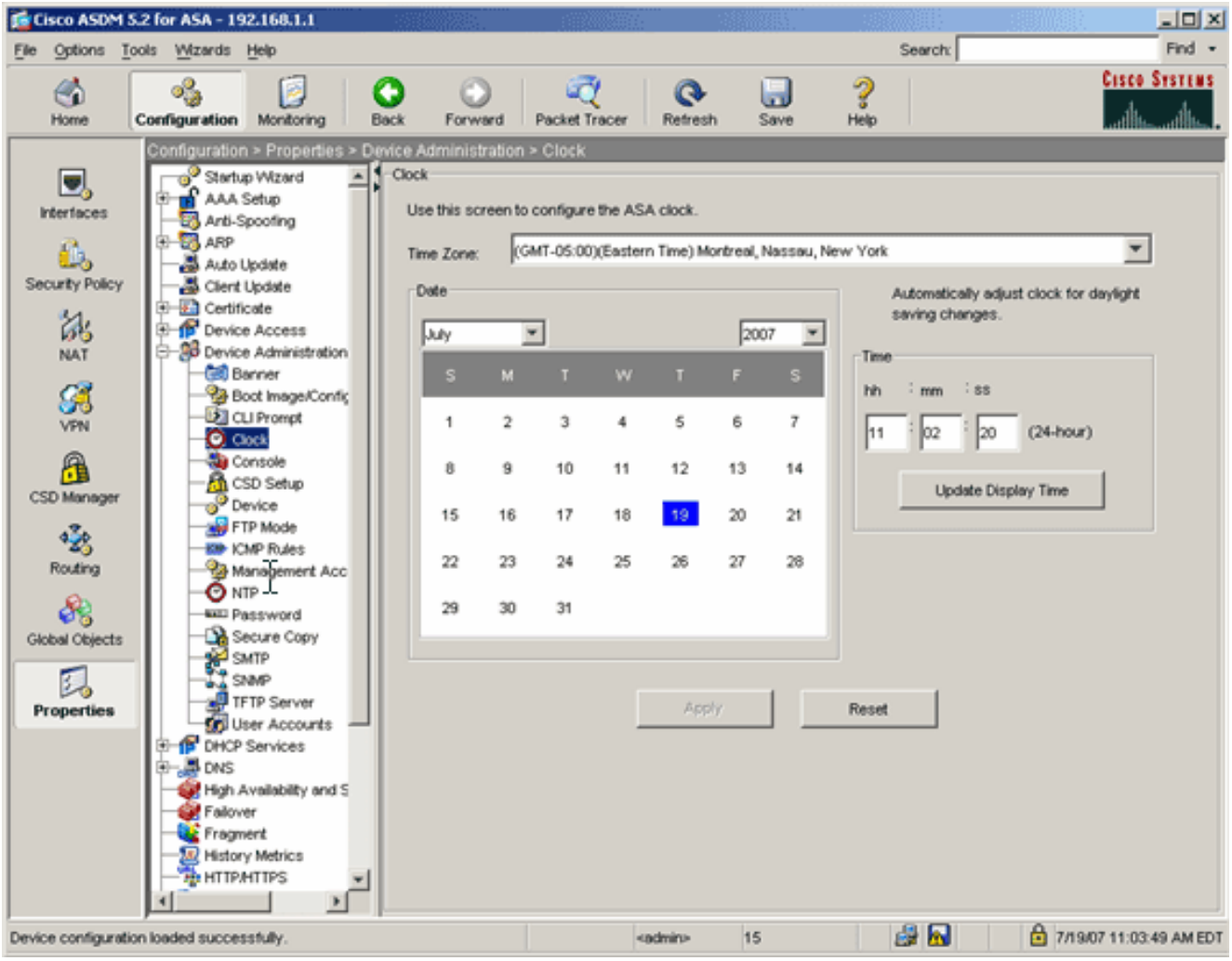
1. 日付、時刻、およびタイム ゾーンが正しいことを確認する。
2. RSA キー ペアを生成する。
3. トラストポイントを作成する。
4. 証明書の登録を生成する。
5. トラストポイントを認証する。
6. 証明書をインストールする。
7. 新規インストールされた証明書を使用するための WebVPN を設定する。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ステップ 1：日付、時刻、および時間帯（Time Zone）の値が正しいことを確認する

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Device Administration] を展開し、[Clock] を選択します。
3. 表示されている情報が正しいことを確認します。証明書の検証が適切に行われるために、Date、Time、および Time Zone の値は正確である必要があります。



コマンドラインの例

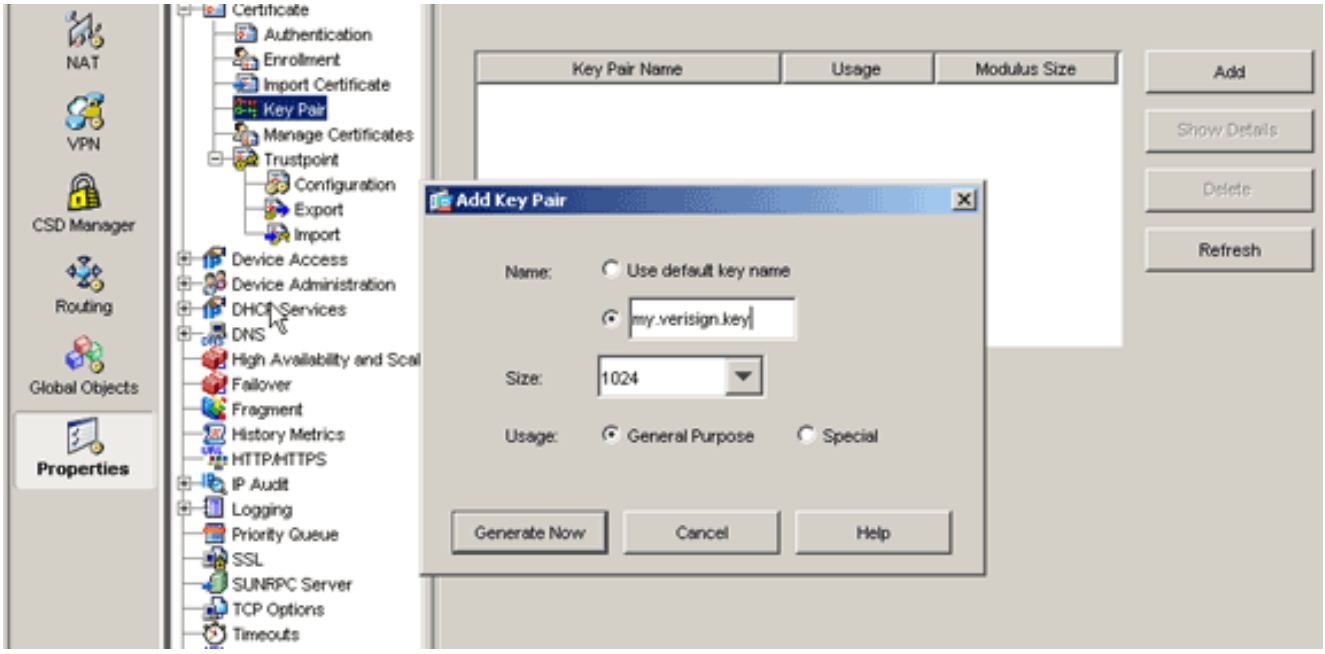
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

ステップ 2. RSA キー ペアを生成する

生成された RSA 公開キーは、ASA の ID 情報と結合され、PKCS#10 証明書要求が形成されます。 キー ペアを作成するトラストポイントでキー名を明確に特定する必要があります。

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Key Pair] を選択します。
3. [Add] をクリックします。



4. キー名を入力し、モジュール サイズを選択し、使用タイプを選択します。 注： 推奨されるキー ペアのサイズは 1024 です。
5. [Generate] をクリックします。作成したキー ペアが [Key Pair Name] 列に表示されます。

コマンドラインの例

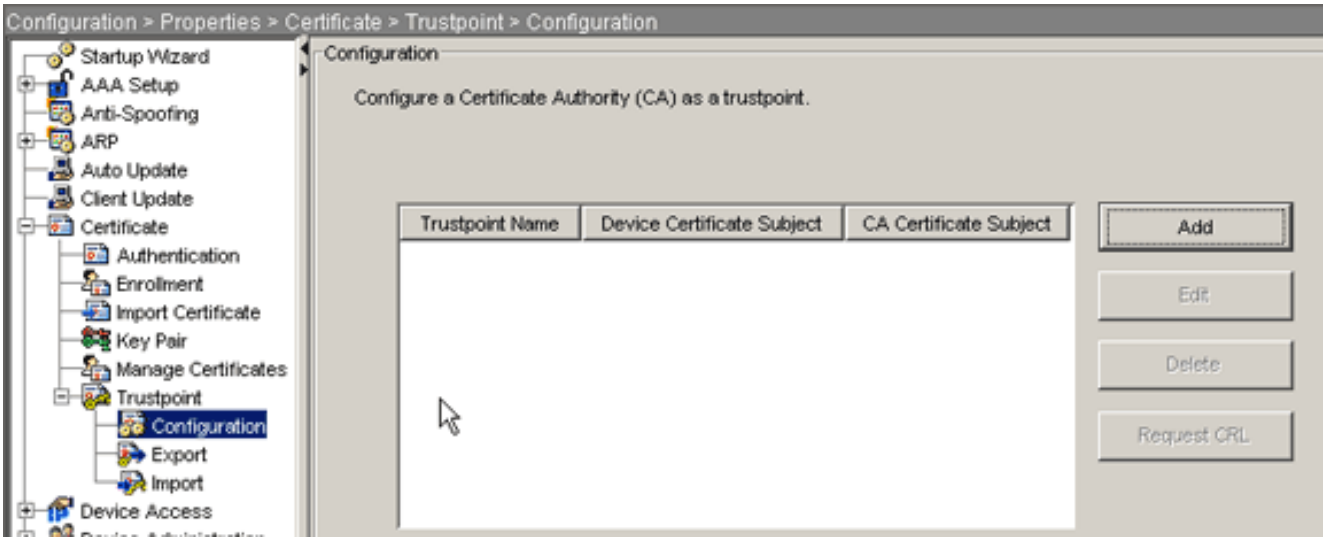
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

ステップ 3. トラストポイントを作成する

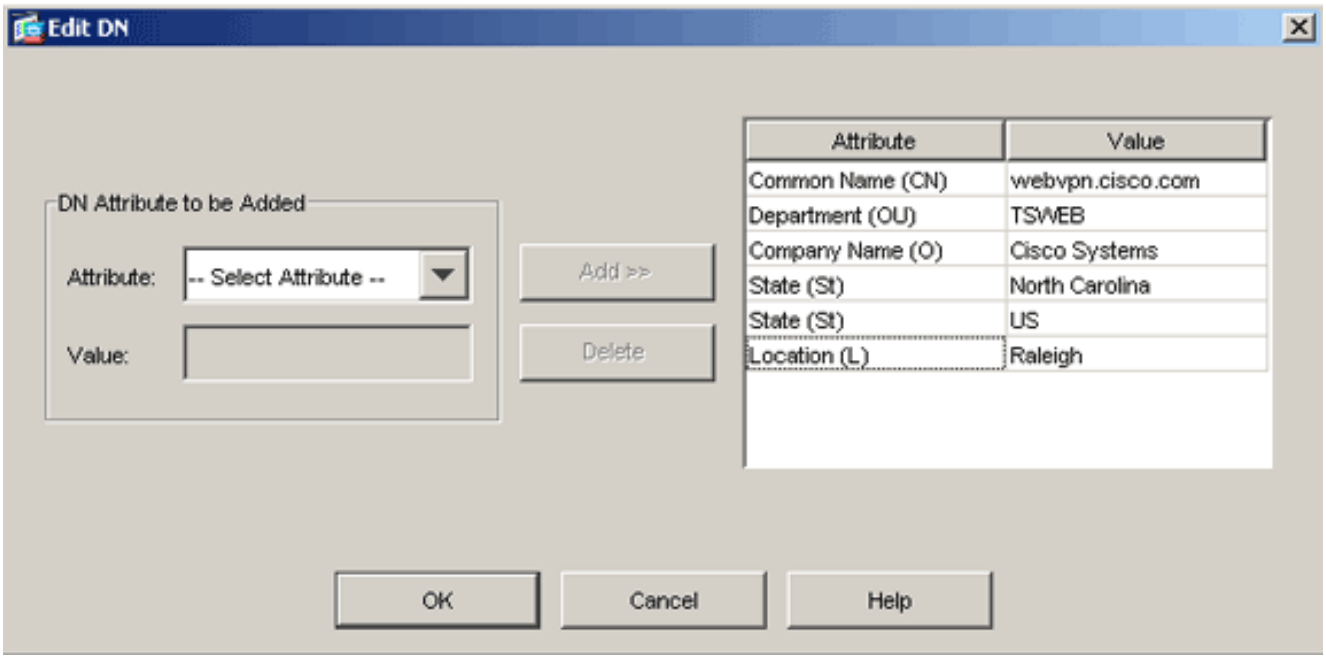
トラストポイントは、ASA が使用する認証局（CA）を宣言する必要があります。

ASDM の手順

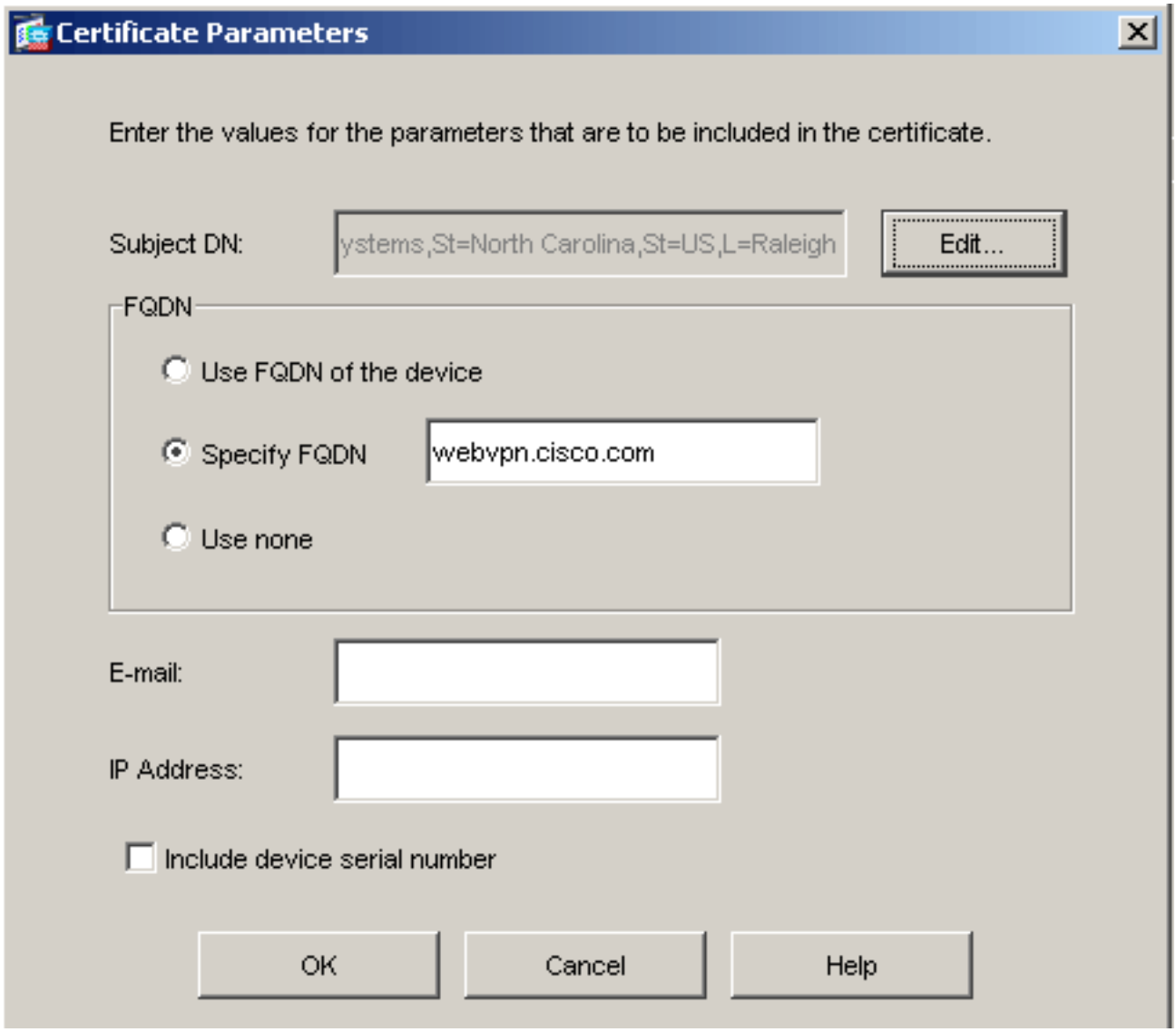
1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Trustpoint] を展開します。
3. [Configuration] を選択し、[Add] をクリックします。



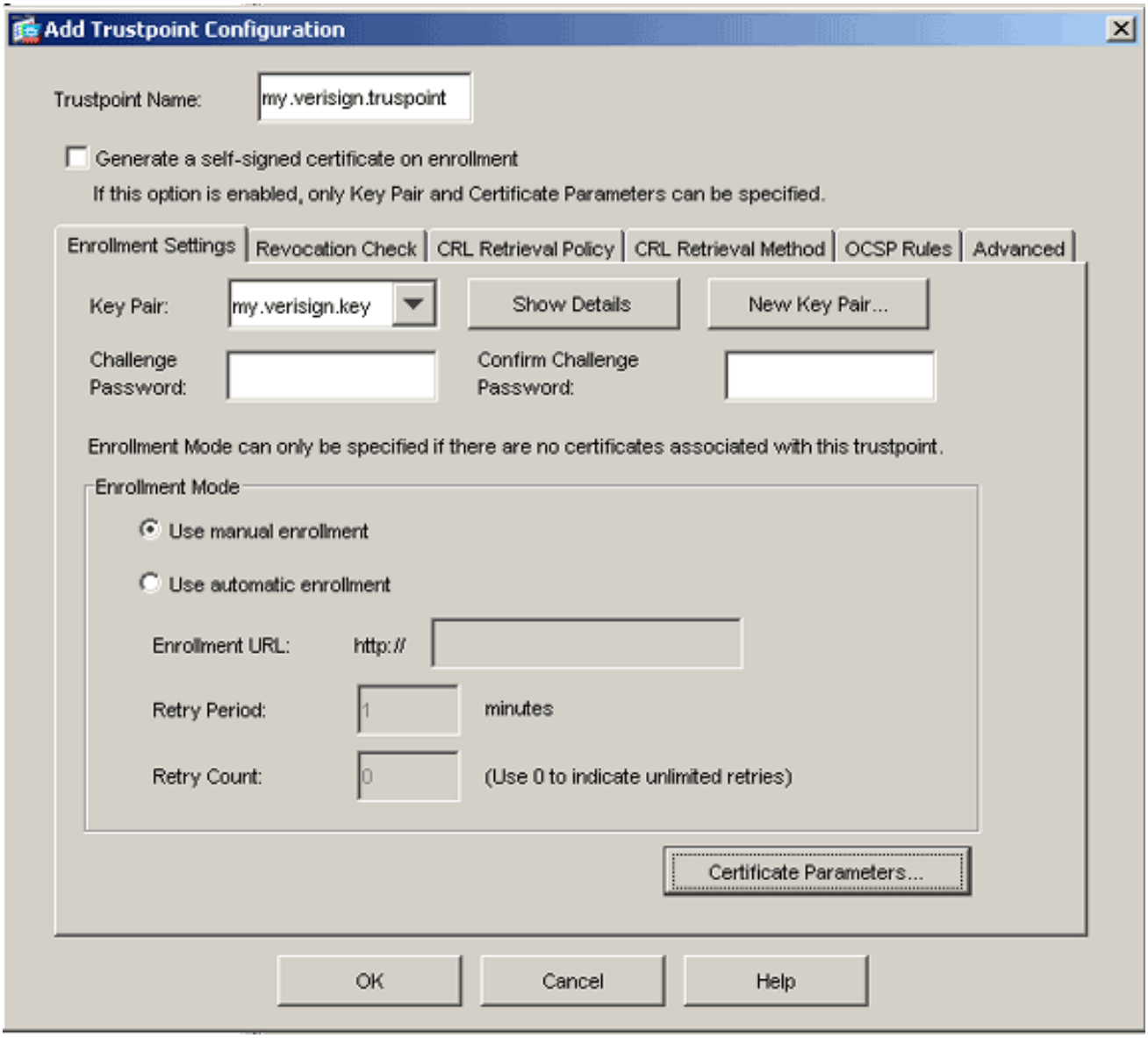
4. 以下の値を設定します。**トラストポイント名**： トラストポイント名は目的の用途に関連する名前にします この例では *my.verisign.trustpoint* を使用しています。**キー ペア**： 手順 2 で生成したキー ペア（ *my.verisign.key* ）を選択します。
5. [Manual Enrollment] を選択していることを確認します。
6. [Certificate Parameters] をクリックします。[Certificate Parameters] ダイアログ ボックスが表示されます。
7. [Edit] をクリックし、次の表に示す属性を設定します。これらの値を設定するために、Attribute ドロップダウン リストから値を選択し、値を入力して、**Add** をクリックします。



8. 適切な値を追加したら、**OK** をクリックします。
9. [Certificate Parameters] ダイアログボックスで、[Specify FQDN] フィールドに FQDN を入力します。この値は、Common Name（ CN ）に使用したものと同じ FQDN である必要があります。



10. [OK] をクリックします。
11. 正しいキー ペアが選択されていることを確認し、[Use manual enrollment] オプション ボタンをクリックします。
12. [OK] をクリックして、[Apply] をクリックします。



コマンドラインの例

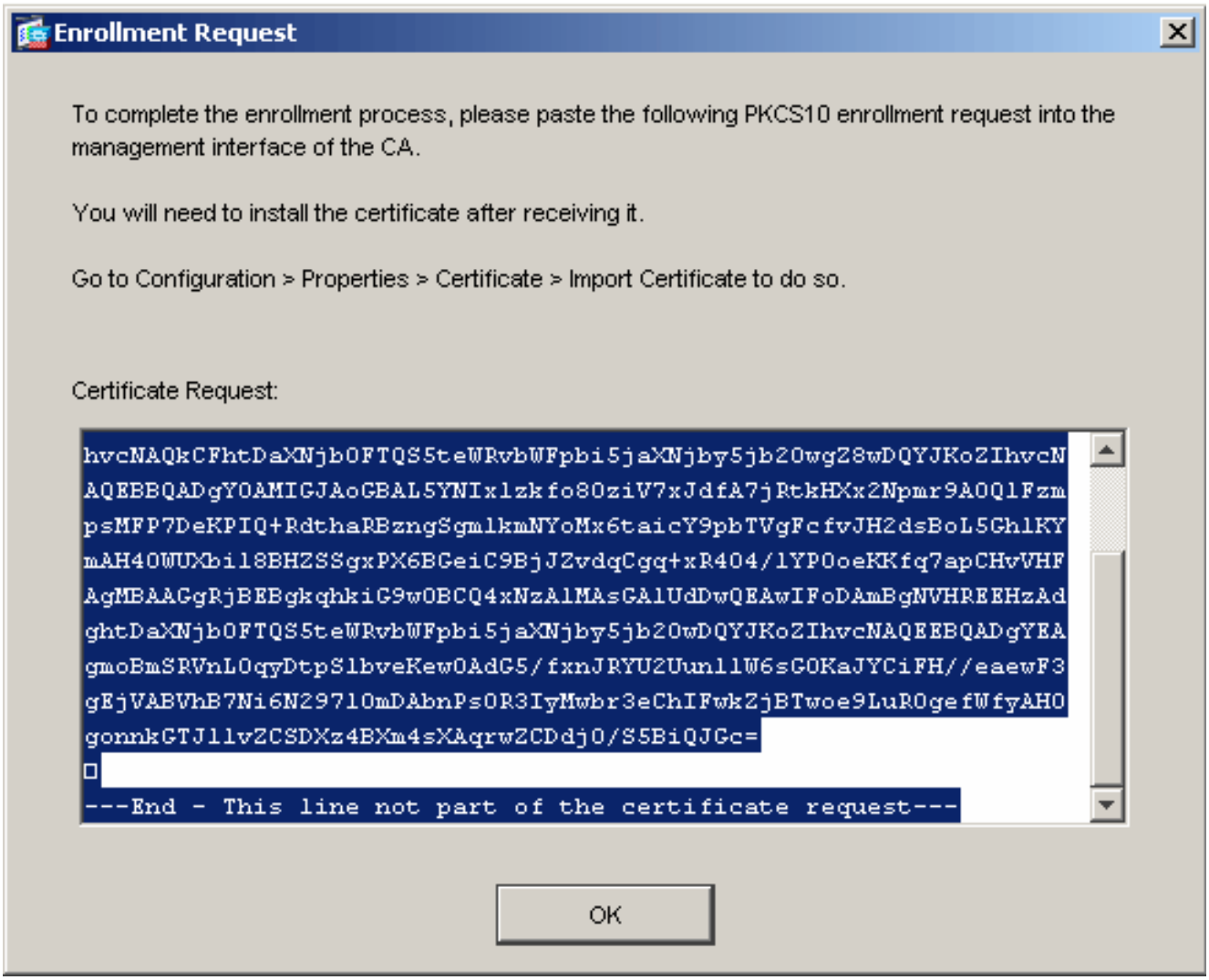
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco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

ステップ 4. 証明書登録を生成する

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Enrollment] を選択します。
3. ステップ 3 で作成したトラストポイントが選択されていることを確認して、[Enroll] をクリックします。ダイアログ ボックスに証明書登録要求（証明書署名要求とも呼ばれる）が一覧表示されます。



4. PKCS#10 登録要求をテキスト ファイルにコピーして、適切なサード パーティ ベンダーに CSR を送信します。サード パーティ ベンダーは CSR を受信した後、インストール用の ID 証明書を発行します。

コマンドラインの例

デバイス名 1

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

! Initiates CSR. This is the request to be ! submitted
via web or email to the 3rd party vendor. % Start
certificate enrollment .. % The subject name in the
certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
```

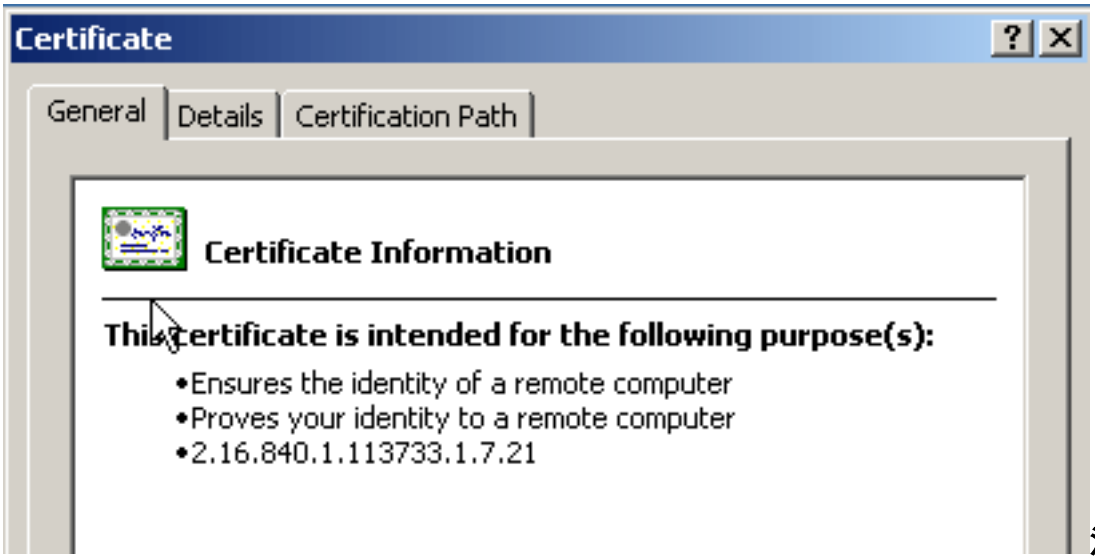
```
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal?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

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

ステップ 5. トラストポイントを認証する

サードパーティ ベンダーから ID 証明書を受信したら、引き続きこのステップを実行します。

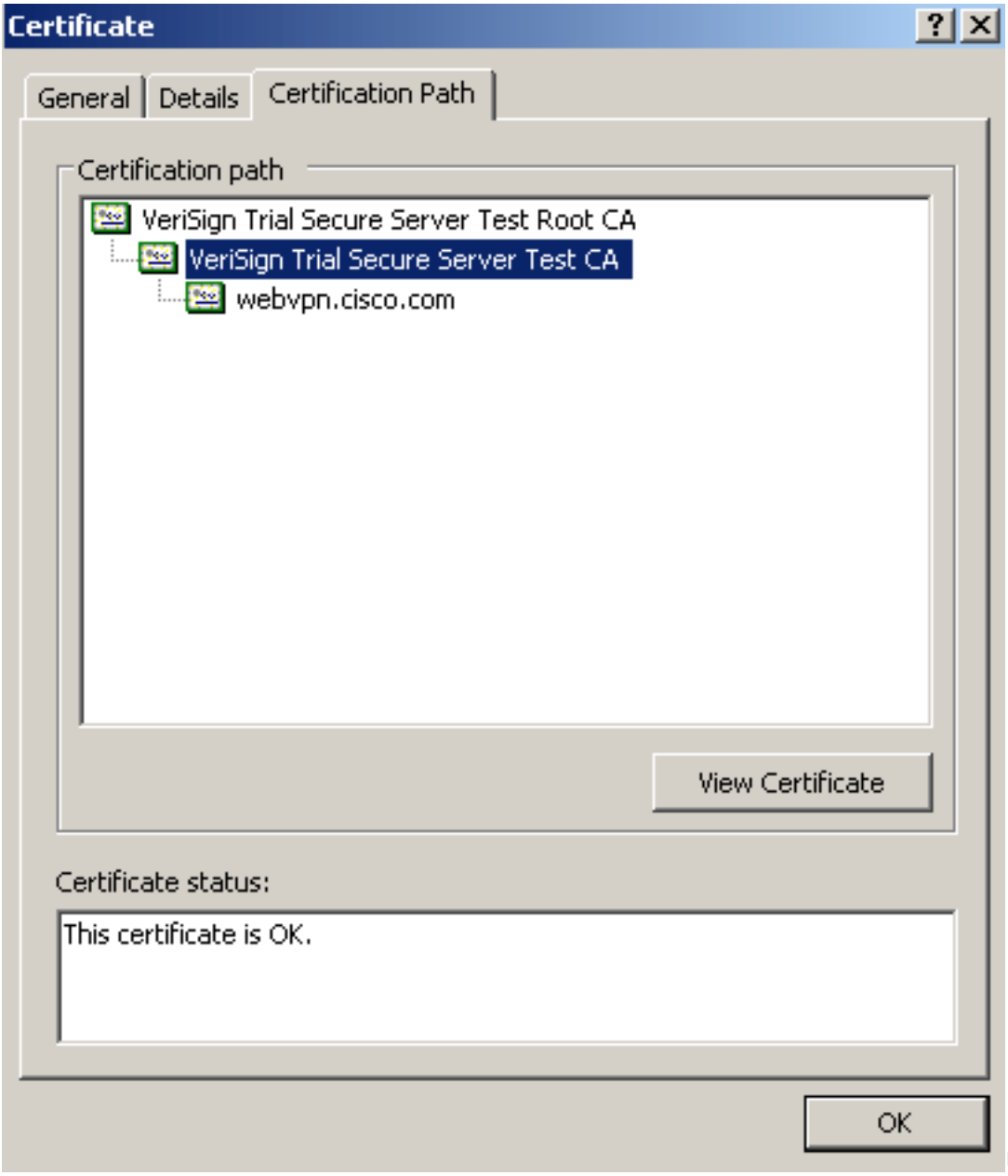
ASDM の手順

1. ID 証明書をローカル コンピュータに保存します。
2. ファイル形式ではない Base64 で符号化された証明書が提供された場合、Base64 メッセージをコピーし、テキスト ファイルに貼り付ける必要があります。
3. .cer 拡張子を使用してファイルの名前を変更します。**注:** .cer 拡張子を使用してファイルの名前を変更すると、ファイルのアイコンは証明書として表示されます。
4. 証明書ファイルをダブルクリックします。Certificate ダイアログ ボックスが表示されます。



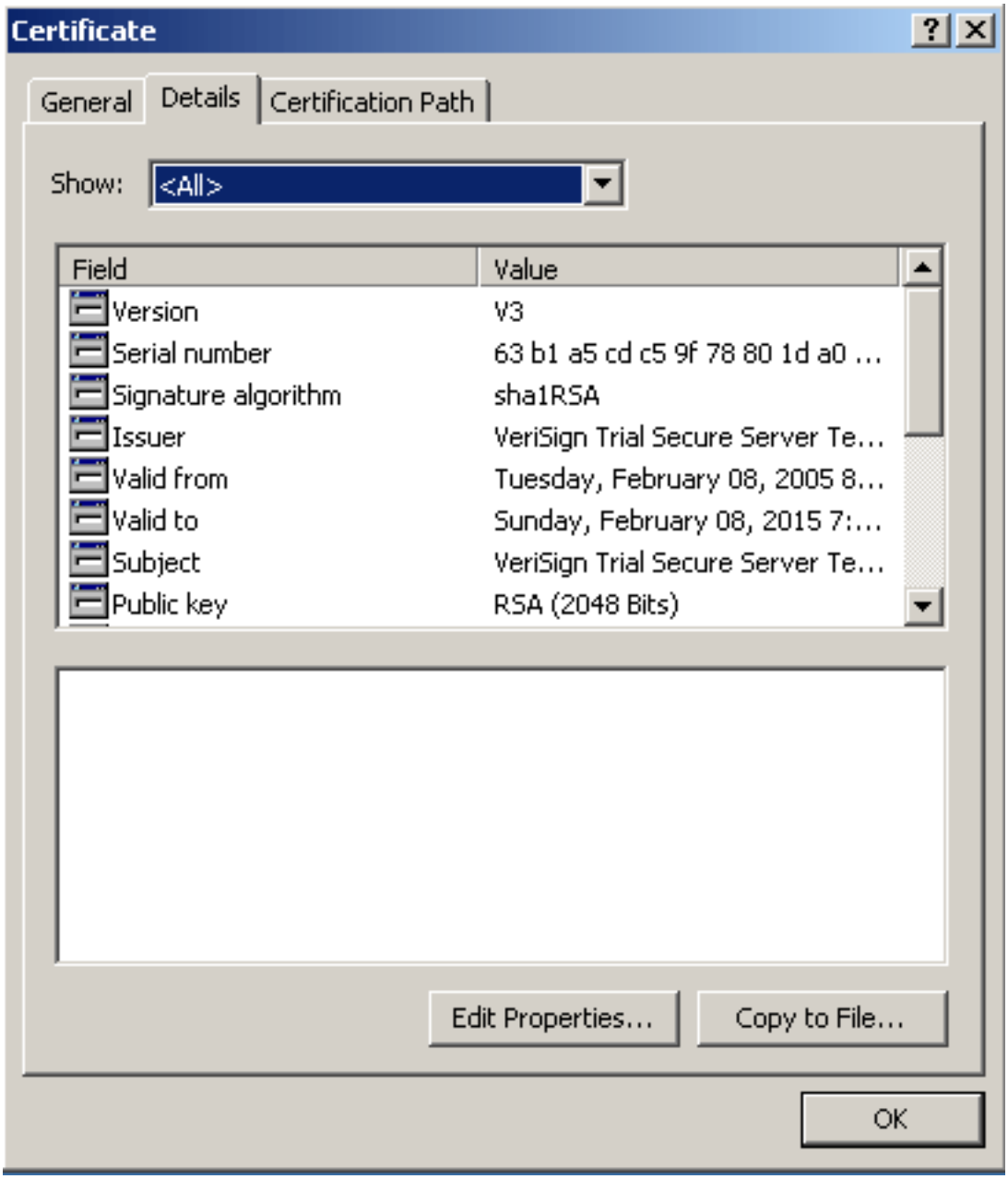
注: General タブに「Windows does not have enough information to verify this certificate」というメッセージが表示された場合、この手順を継続する前に、サードパーティ ベンダーのルート CA または中間 CA 証明書を入手する必要があります。 ルート CA または中間 CA 証明書を入手するには、サードパーティ ベンダーまたは CA 管理者に問い合せてください。

5. [Certificate Path] タブをクリックします。
6. 発行された ID 証明書の上にある CA 証明書をクリックし、[View Certificate] をクリックし

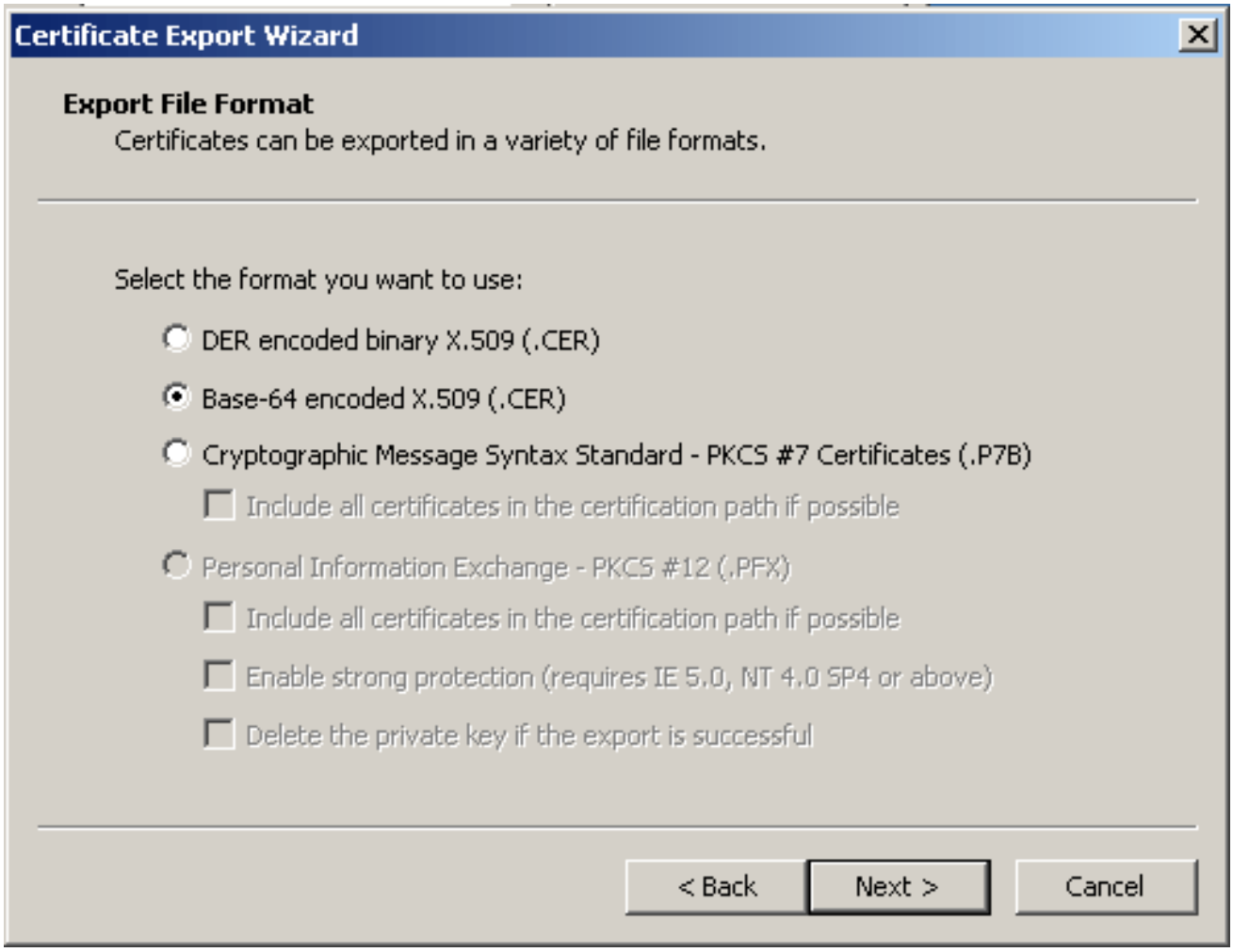


ます。中間 CA 証明書に関する詳細情報が表示されます。**警告：** この手順では ID（デバイス）証明書をインストールしないでください。 このステップでは、ルート、下位ルート、または CA 証明書のみを追加します。 ID（デバイス）証明書は手順 6 でインストールします。

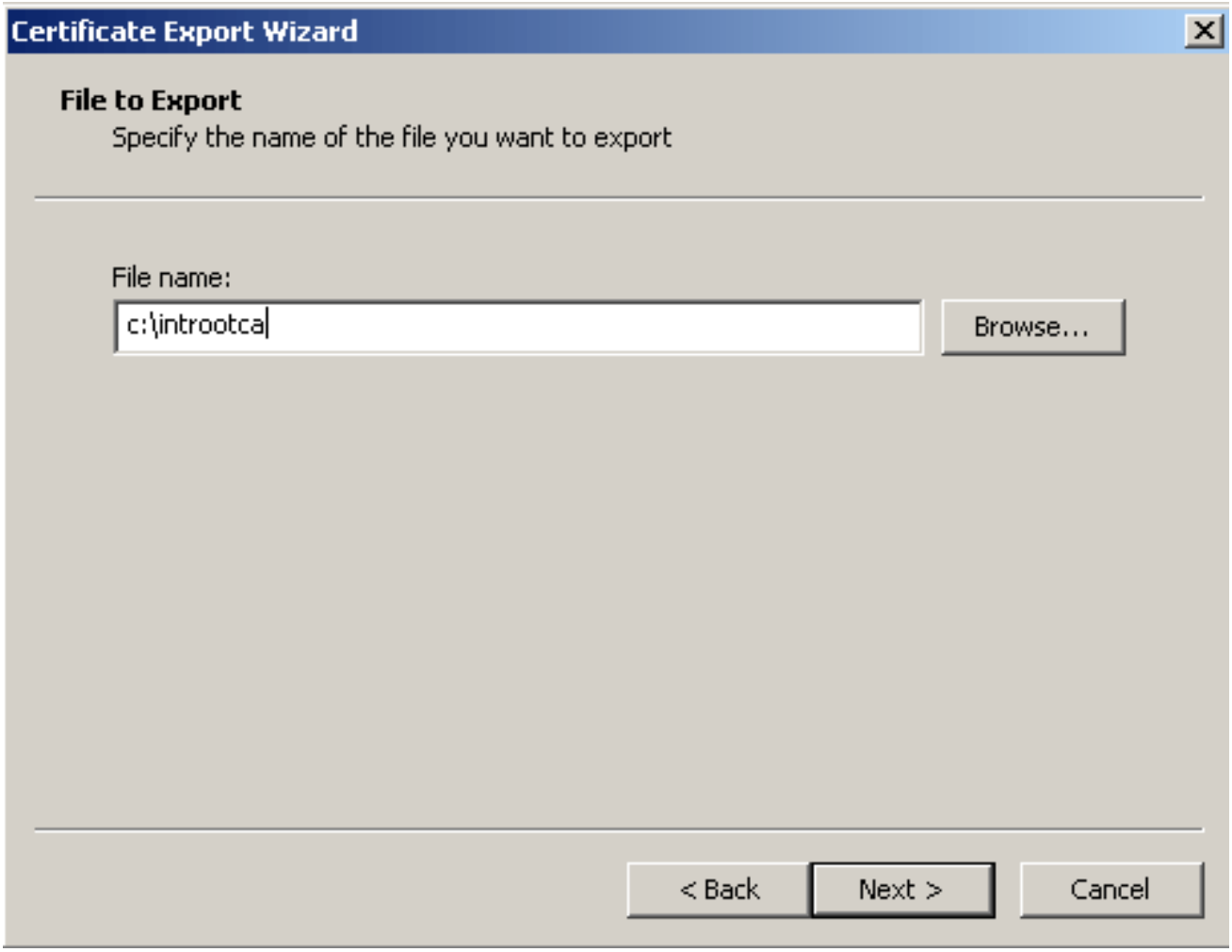
7. **[Details]** をクリックします。



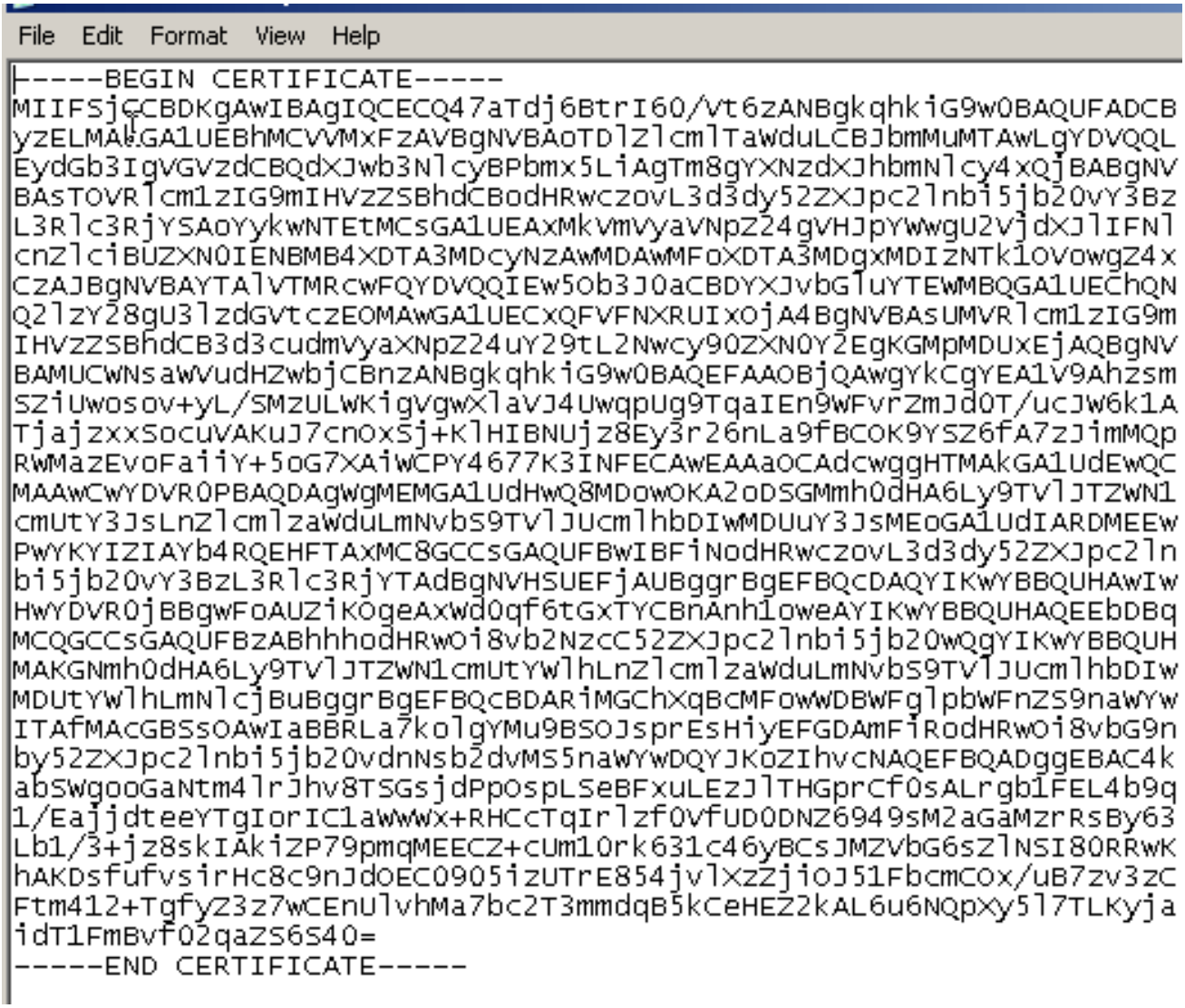
8. [Copy to File] をクリックします。
9. Certificate Export Wizard 内で **Next** をクリックします。
10. Export File Format ダイアログ ボックスで **Base-64 encoded X.509 (.CER)** オプション ボタンをクリックし、**Next** をクリックします。



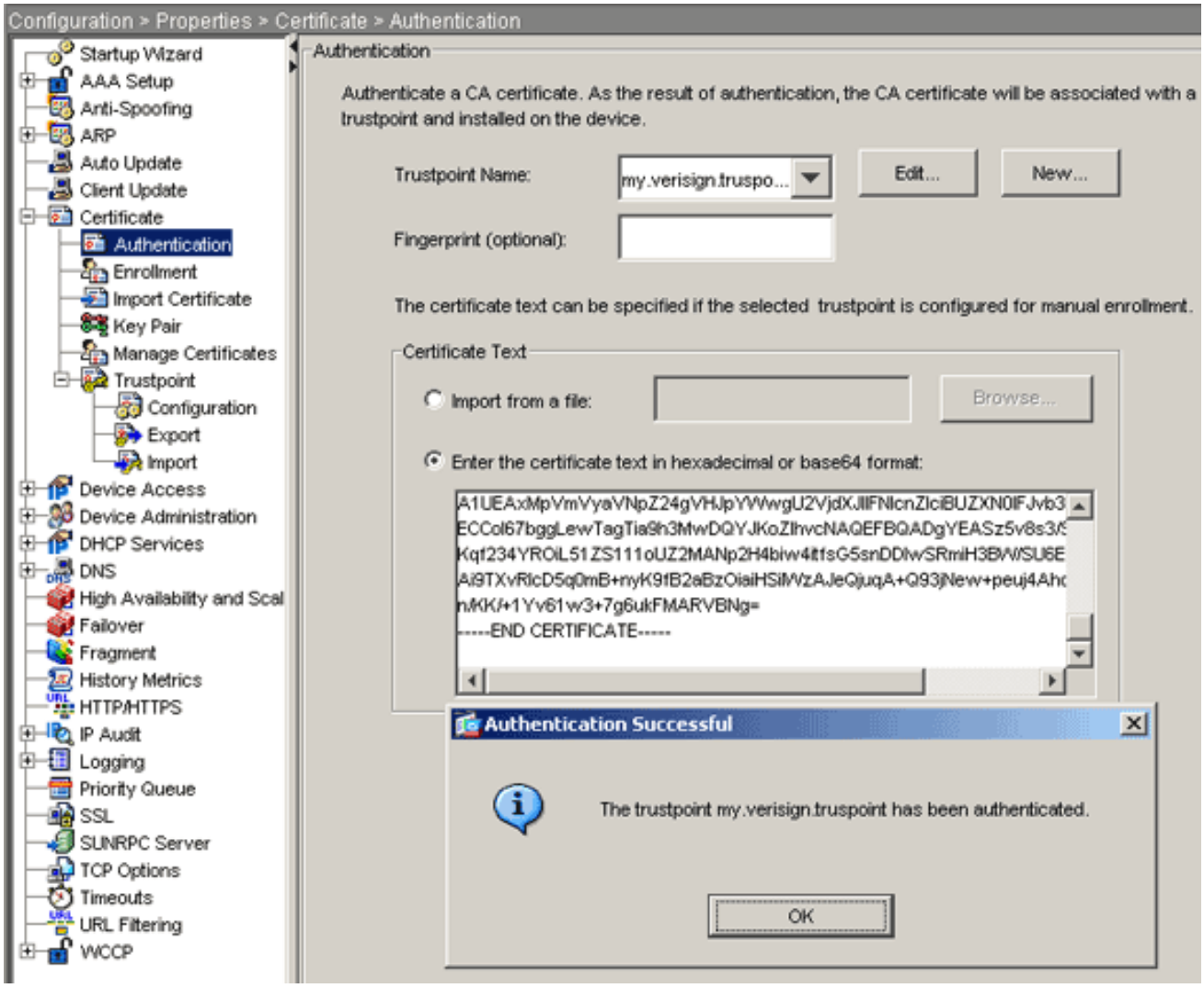
11. ファイル名と、CA 証明書を保存する場所を入力します。
12. [**Next**] をクリックし、次に [**Finish**] をクリックします。



13. Export Successful ダイアログ ボックスで **OK** をクリックします。
14. CA 証明書を保存した場所を表示します。
15. メモ帳などのテキスト エディタでファイルを開きます。（ファイルを右クリックし、[Send To] > [Notepad] の順に選択します）。Base64 で符号化されたメッセージは、次の画像の証明書のようになります。



16. ASDM で [Configuration] をクリックし、[Properties] をクリックします。
17. [Certificate] を展開し、[Authentication] を選択します。
18. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックします。
19. Base64 形式で作成された CA 証明書をテキスト エディタからテキスト領域に貼り付けます。
20. [Authenticate] をクリックします。



21. [OK] をクリックします。

コマンドラインの例

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
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD
```

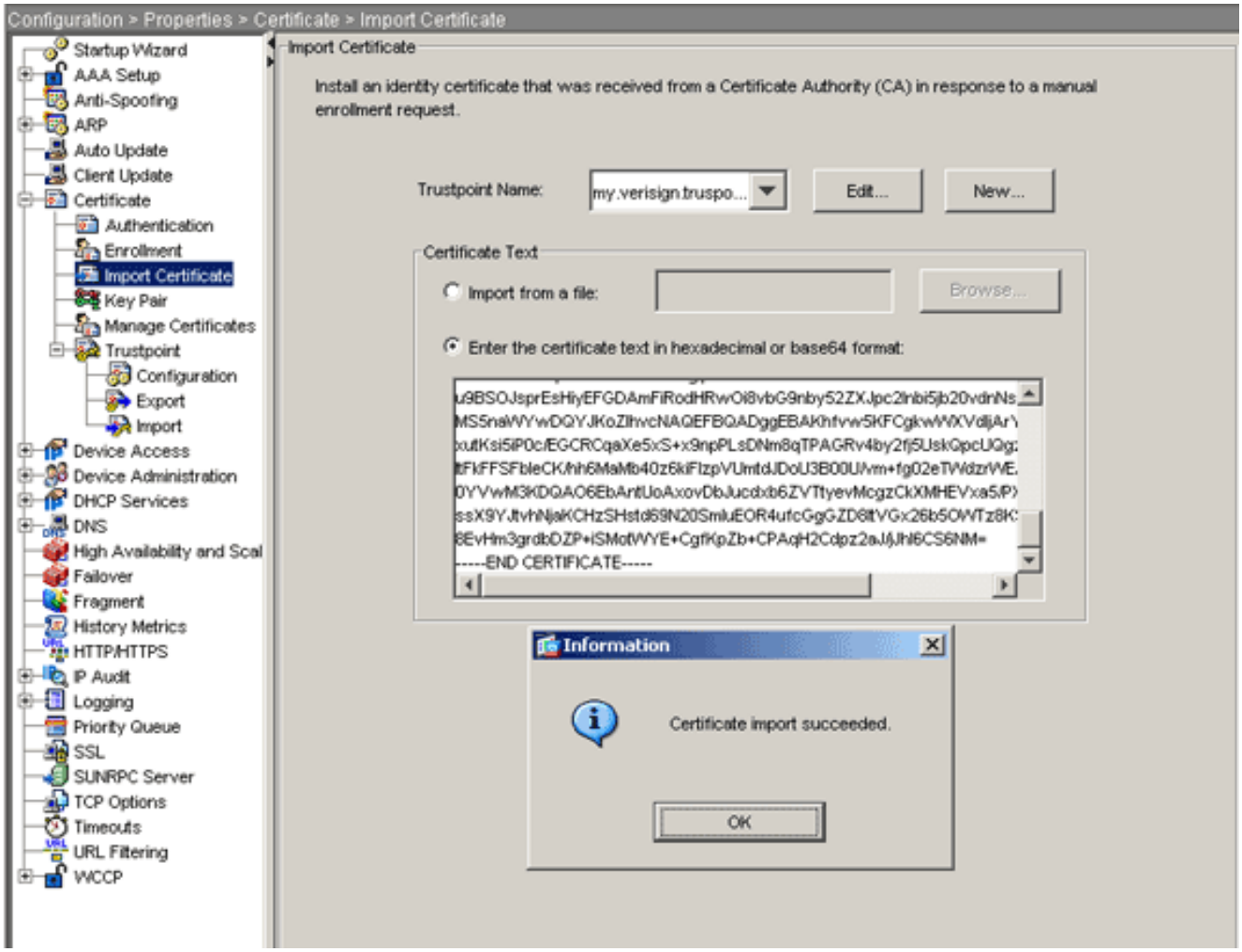
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo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



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

ステップ 6. 証明書をインストールする

ASDM の手順

次の手順を実行するには、サードパーティ ベンダーにより提供された ID 証明書を使用します。

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Import Certificate] を選択します。
3. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックし、テキスト フィールドに Base64 ID 証明書を貼り付けます。



4. [Import] をクリックし、[OK] をクリックします。

コマンドラインの例

ciscoasa

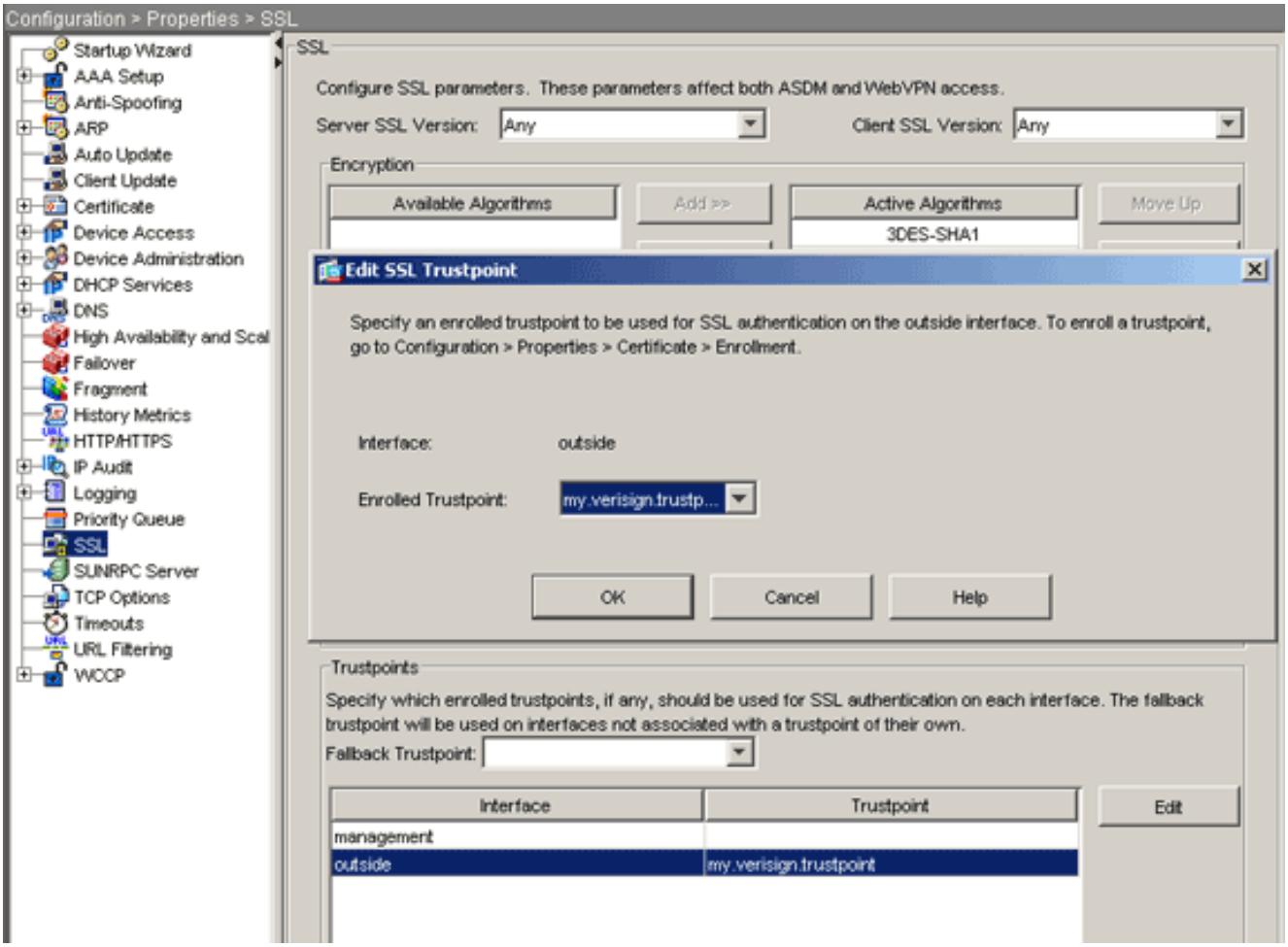
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

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

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

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

手順 7：新規インストールされた証明書を使用するための WebVPN を設定する

ASDM の手順

1. [Configuration] をクリックし、[Properties] をクリックし、次に SSL を選択します。
2. [Trustpoints] エリアで、WebVPN セッションを終端するために使用するインターフェイスを選択します。（この例では、外部インターフェイスを使用します）。
3. [Edit] をクリックします。[Edit SSL Trustpoint] ダイアログボックスが表示されます。



4. [Enrolled Trustpoint] ドロップダウン リストから、手順 3 で作成したトラストポイントを選択します。
5. [OK] をクリックして、[Apply] をクリックします。

新しい証明書が、指定のインターフェイス上で終端するすべての WebVPN セッションに使用されます。 適切なインストールを確認する方法については、このドキュメントの「確認」セクションを参照してください。

コマンドラインの例

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.
```

確認

このセクションでは、サード パーティ ベンダーの証明書のインストールが成功したことを確認する方法を説明します。

ASA からの自己署名証明書の置き換え

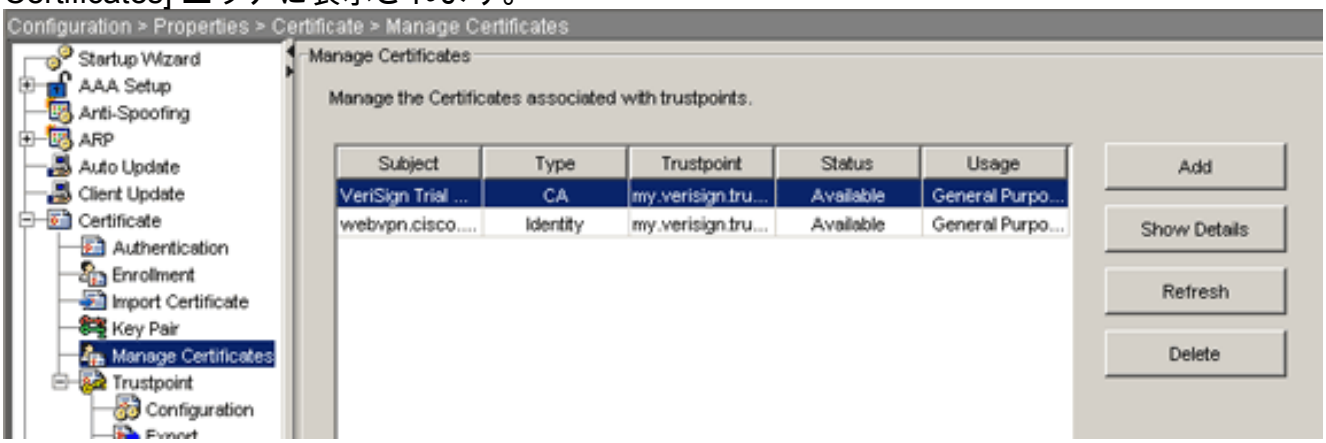
このセクションでは、ASA からインストールされた自己署名証明書を置き換える方法を説明します。

1. 証明書署名要求を Verisign に発行します。要求した証明書を Verisign から受信した後、それを同じトラストポイントに直接インストールします。
2. 次のコマンドを入力します。 **crypto ca enroll Verisign**質問に回答するよう求められます。
3. [Display Certificate Request to terminal] に [yes] と入力し、その出力を Verisign に送信します。
4. Verisign から新しい証明書を受け取ったら、次のコマンドを入力します。 **crypto ca import Verisign certificate**

インストールされた証明書の表示

ASDM の手順

1. [Configuration]、[Properties] の順にクリックします。
2. [Certificate] を展開し、[Manage Certificates] を選択します。トラストポイントの認証に使用する CA 証明書およびサード パーティ ベンダーから発行された ID 証明書が [Manage Certificates] エリアに表示されます。



コマンドラインの例

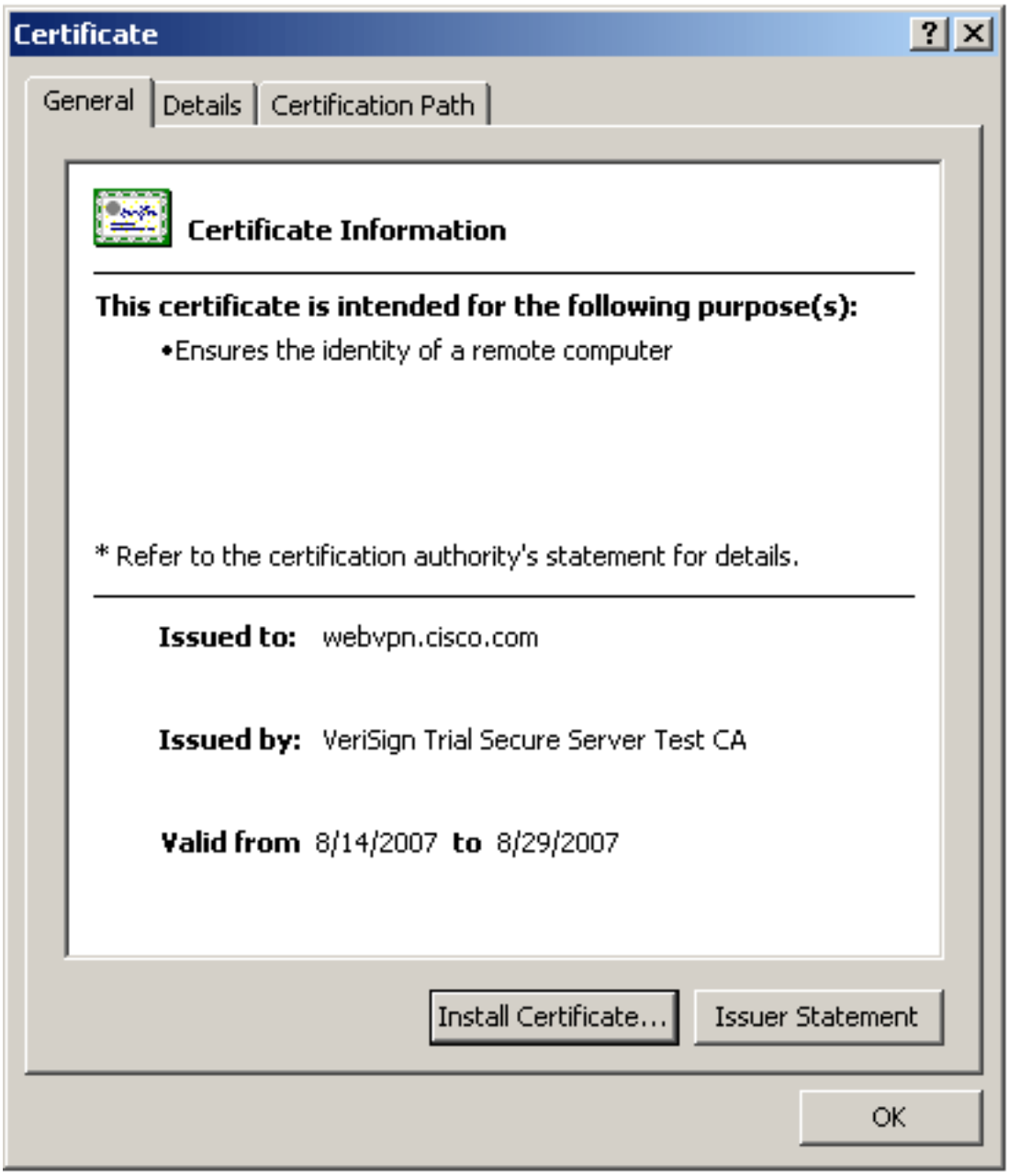
ciscoasa
ciscoasa(config)#**show crypto ca certificates** *! Displays all certificates installed on the ASA.* Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=VeriSign Trial Secure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

Web ブラウザによる WebVPN 用にインストールされた証明書の確認

WebVPN が新しい証明書を使用していることを確認するには、次の手順を実行します。

1. Web ブラウザを介して WebVPN インターフェイスに接続します。 証明書を要求するために使用した FQDN とともに https:// を使用します (たとえば、https://webvpn.cisco.com のようにします) 。次のいずれかのセキュリティ アラートが表示された場合、そのアラートに対応する手順を実行します。**The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site**ASA の WebVPN インターフェイスに接続するために正しい FQDN/CN を使用したことを確認します。 ID 証明書を要求したときに定義した FQDN/CN を使用する必要があります。 **show crypto ca certificates** *trustpointname* コマンドを使用すると、証明書の FQDN/CN を確認できます。**The security certificate was issued by a company you have not chosen to trust...**Web ブラウザにサードパーティ ベンダーのルート証明書をインストールするには、次の手順を実行します。[Security Alert] ダイアログ ボックスで、[View Certificate] をクリックします。[Certificate] ダイアログ ボックスで、[Certificate Path] タブをクリックします。発行された ID 証明書の上にある CA 証明書を選択し、[View Certificate] をクリックします。**Install Certificate** をクリックします。Certificate Install Wizard ダイアログ ボックスで **Next** をクリックします。**Automatically select the certificate store based on the type of certificate** オプション ボタンを選択し、**Next** をクリックし、次に **Finish** をクリックします。証明書のインストールを確認するプロンプトが表示されたら、**Yes** をクリックします。*Import operation was successful* プロンプトで、**OK** をクリックし、次に **Yes** をクリックします。**注:** この例では Verisign Trial Certificate を使用しているため、ユーザが接続する際の確認エラーを回避するには、Verisign Trial CA Root Certificate がインストールされている必要があります。
2. WebVPN login ページの右下隅に表示されているロック アイコンをダブルクリックします。インストールされている証明書の情報が表示されます。
3. 内容を確認し、サードパーティ ベンダーの証明書に合致することを確認します。



SSL 証明書の更新手順

SSL 証明書を更新するには、次の手順を実行します。

1. 更新するトラストポイントを選択します。
2. [enroll] を選択します。次のメッセージが表示されます。*If it is successfully enrolled again, the current cert will be replaced with the new ones. Do you want to continue?*
3. [Yes] を選択します。これにより、新しい CSR が生成されます。
4. CSR を CA に送信し、返信された新しい ID 証明書をインポートします。
5. 外部インターフェイスへのトラストポイントを削除し、再度適用します。

コマンド

ASA では、コマンド ラインで各種の show コマンドを使用し、証明書の状況を確認できます。

- **show crypto ca trustpoint** — 設定されているトラストポイントを表示します。
- **show crypto ca certificate** — システムにインストールされているすべての証明書を表示しま

す。

- **show crypto ca crls** — キャッシュされている Certificate Revocation List（CRL; 証明書失効リスト）を表示します。
- **show crypto key mypubkey rsa** — 生成されたすべての暗号鍵ペアを表示します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

発生する可能性のあるエラーを次に示します。

- **%% Warning: CA cert is not found. The imported certs might not be usable.INFO: Certificate successfully imported**CA 証明書が正しく認証されていません。 CA 証明書がインストールされていることを確認するには、show crypto ca certificate trustpointname コマンドを使用します。 CA 証明書で始まる行を探します。 CA 証明書がインストールされている場合は、正しいトラストポイントを参照していることを確認します。
- ERROR: Failed to parse or verify imported certificateこのエラーが発生する可能性があるのは、ID 証明書をインストールしたけれども、関連付けられたトラストポイントで認証された正しい中間証明書またはルート CA 証明書がない場合です。 正しい中間証明書またはルート CA 証明書を使用して削除と再認証を行う必要があります。 正しい CA 証明書を受け取っていることを確認するには、サードパーティ ベンダーに問い合せてください。
- Certificate does not contain general purpose public keyこのエラーが発生する可能性があるのは、正しくないトラストポイントに ID 証明書をインストールしようとした場合です。 無効な ID 証明書をインストールしようとしているか、トラストポイントと関連付けられた鍵ペアが ID 証明書に含まれている公開鍵と合致しません。 正しいトラストポイントに ID 証明書をインストールしたことを確認するには、**show crypto ca certificates trustpointname** コマンドを使用します。 *Associated Trustpoints* がある行を探します。 正しくないトラストポイントが表示されている場合は、このドキュメントで説明されている手順に従って、トラストポイントを削除して適切なトラストポイントを再インストールします。また、CSR が生成されてからキーペアが変更されていないことも確認します。
- **エラー メッセージ： %%PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint [trustpoint name]**このメッセージが表示されるのは、SSL 接続を認証するために、指定のトラストポイント用のデバイス証明書を設定したときにエラーが発生した場合です。 SSL 接続がアップ状態になると、使用されるデバイス証明書が設定されます。 エラーが発生すると、デバイス証明書のロードに使用される必要がある設定済みのトラストポイントと、エラーの理由が含まれるエラー メッセージがログに記録されます。*trustpoint name* : SSL がデバイス証明書を設定できなかったトラストポイントの名前**推奨処置：** 障害に対して報告された理由で示された問題を解決します。指定のトラストポイントは登録済みであり、デバイス証明書があることを確認します。デバイス証明書が有効であることを確認します。必要に応じてトラストポイントを再度登録します。

関連情報

- ASA で ASDM を使用して Microsoft Windows CA からデジタル証明書を取得する方法
- Cisco PIX Firewall ソフトウェア

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカル サポートとドキュメント – Cisco Systems