

# O ASA 8.x instala manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Etapa 1. Verifique que a data, o tempo, e os valores da zona de hora \(fuso horário\) são exatos](#)

[Etapa 2. Gerencia uma solicitação de assinatura de certificado](#)

[Etapa 3. Autentique o ponto confiável](#)

[Etapa 4. Instale o certificado](#)

[Etapa 5. Configurar o WebVPN para usar o certificado recentemente instalado](#)

[Verificar](#)

[Veja Certificados instalados](#)

[Verifique o certificado instalado para o WebVPN com um navegador da Web](#)

[Comandos](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este exemplo de configuração descreve como instalar manualmente um certificado digital do vendedor da 3ª parte no ASA para o uso com WebVPN. Um certificado experimental de Verisign é usado neste exemplo. Cada etapa contém o procedimento do aplicativo ASDM e um exemplo CLI.

## [Pré-requisitos](#)

### [Requisitos](#)

Este documento exige que você tem o acesso a um Certificate Authority (CA) para o certificado de registro. Os exemplos de vendedores de CA da 3ª parte incluem, mas não são limitados a, Baltimore, Cisco, confiam, Geotrust, Godaddy, iPlanet/Netscape, Microsoft, RSA, Thawte, e Verisign.

## Componentes Utilizados

Este documento usa um ASA 5510 que execute a versão de software 8.0(2) e a versão 6.0(2) ASDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Configurar

A fim instalar um certificado digital do vendedor da 3ª parte no ASA, termine estas etapas:

1. [Verifique que a data, o tempo, e os valores da zona de hora \(fuso horário\) são exatos](#)
2. [Gerencia uma solicitação de assinatura de certificado](#)
3. [Autentique o ponto confiável](#)
4. [Instale o certificado](#)
5. [Configurar o WebVPN para usar o certificado recentemente instalado](#)

**Nota:** Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

### Etapa 1. Verifique que a data, o tempo, e os valores da zona de hora (fuso horário) são exatos

#### Procedimento ASDM

1. Clique a **configuração**, e clique então a **instalação de dispositivo**.
2. Expanda o **tempo de sistema**, e escolha o **pulso de disparo**.
3. Verifique que a informação alistada é exata. Os valores para a data, o tempo, e a zona de hora (fuso horário) devem ser exatos para que a validação certificada apropriada ocorra.

#### Exemplo da linha de comando

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

### Etapa 2. Gerencia uma solicitação de assinatura de certificado

Uma solicitação de assinatura de certificado (CSR) é exigida para que a 3ª parte CA para emitir um certificado de identidade. O CSR contém a corda do nome destacado (DN) do seu ASA junto com a chave pública gerada do ASA. O ASA usa a chave privada gerada para assinar digitalmente o CSR.

## Procedimento ASDM

1. A **configuração do clique**, e clica então o **Gerenciamento de dispositivos**.
2. Expanda o **gerenciamento certificado**, e escolha **certificados de identidade**.
3. Clique em **Add**.
4. Clique **adicionar um** botão de rádio **novo do certificado de identidade**.
5. Para o par de chaves, clique **novo**.**Nota:** Se você usa um certificado de 2048 bit, gerencia um bit 2048 chave também.
6. Clique o botão de rádio **novo do nome do par de chaves da entrada**. Você deve distintamente identificar o nome do par de chaves para finalidades do reconhecimento.
7. O clique **gerencie agora**.O par de chaves deve agora ser criado.
8. Para definir o assunto DN do certificado, o clique **seleto**, e configurar os atributos alistados nesta tabela:**Tabela 4.1: Atributos DNA** fim configurar estes valores, para escolher um valor da lista de drop-down do atributo, para incorporar o valor, e o clique **adicionar**.**Nota:** Alguns vendedores da 3ª parte exigem atributos particulares ser incluídos antes que um certificado de identidade esteja emitido. Se você é incerto dos atributos requerido, verifique com seu vendedor para ver se há detalhes.
9. Uma vez que os valores apropriados são adicionados, clique a **APROVAÇÃO**.A caixa de diálogo do certificado de identidade adicionar aparece com o campo do assunto DN do certificado povoado.
10. Clique **avançado**.
11. No campo FQDN, incorpore o FQDN que será usado para alcançar o dispositivo do Internet.Este valor deve ser o mesmo FQDN que você se usou para o Common Name (CN).
12. Clique a **APROVAÇÃO**, e clique-a então **adicionam o certificado**.Você é alertado salvar o CSR a um arquivo em sua máquina local.
13. Clique **consultam**, escolhem um lugar em que para salvar o CSR, e para salvar o arquivo com a extensão de .txt.**Nota:** Quando você salvar o arquivo com uma extensão de .txt, você pode abrir o arquivo com um editor de texto (tal como o bloco de notas) e ver o pedido PKCS#10.
14. Submeta o CSR salvar a seu vendedor da 3ª parte. Uma vez que você submete o CSR a seu vendedor da 3ª parte, fornecer-lhe-ão o certificado de identidade a ser instalado no ASA.

### Exemplo da linha de comando

Em ASDM 6.x, o ponto confiável está criado automaticamente quando um CSR é gerado ou quando o certificado de CA está instalado. No CLI, o ponto confiável deve ser criado manualmente.

```
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)#crypto ca trustpoint
my.verisign.trustpoint ciscoasa(config-ca-
trustpoint)#subject-name CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh !
Defines x.500 distinguished name. Use the attributes !
defined in table 4.1 in Step 2 as a guide.
```

```

ciscoasa(config-ca-trustpoint)#keypair my.verisign.key !
Specifies key pair generated in Step 3. ciscoasa(config-
ca-trustpoint)#fqdn webvpn.cisco.com ! Specifies the
FQDN (DNS:) to be used as the subject ! alternative
name. ciscoasa(config-ca-trustpoint)#enrollment terminal
! Specifies manual enrollment. ciscoasa(config-ca-
trustpoint)#exit ciscoasa(config)#crypto ca enroll
my.verisign.trustpoint ! Initiates certificate signing
request. 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:
MIICHjCCAYcCAQAwgAAXEDAOBgNVBACTB1JhbGVpZ2gxZzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1u0j0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFAqfyNxYt
3oMXSNPO
m1dZ0xJVnRip9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlARc783w4BMO5lulIEhHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5Q1Kx2Y/vrqs+Hg5SLHpbhj/
Uo13yWcE 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no ciscoasa(config)#

```

### [Etapa 3. Autentique o ponto confiável](#)

Uma vez que você recebe o certificado de identidade do vendedor da 3ª parte, você pode continuar com esta etapa.

#### **Procedimento ASDM**

1. Salvar o certificado de identidade a seu computador local.
2. Se seu foram fornecidos um certificado base64-encoded que não venha como um arquivo, você deve copiar a mensagem base64, e cola-a em um arquivo de texto.
3. Rebatize o arquivo com uma extensão de .cer. Nota: O arquivo é rebatizado uma vez com a extensão de .cer, o ícone do arquivo deve indicar como um certificado.

4. Fazer duplo clique o arquivo certificado. A caixa de diálogo do certificado aparece. **Nota:** Se “*Windows não tem bastante informação a verificar que a mensagem deste certificado*” parece no tab geral, você deve obter a CA raiz do vendedor da 3ª parte ou o certificado de CA intermediário antes que você continue com este procedimento. Contacte seu vendedor da 3ª parte ou administrador de CA a fim obter a CA raiz de emissão ou o certificado de CA intermediário.
5. Clique a aba do **trajeto do certificado**.
6. Clique o certificado de CA situado acima de seu certificado de identidade emitido, e clique o **certificado da vista**. A informação detalhada sobre o certificado de CA intermediário aparece. **aviso:** Não instale o certificado da identidade (dispositivo) nesta etapa. Somente a raiz, a raiz subordinada, ou o certificado de CA são adicionados nesta etapa. Os Certificados da identidade (dispositivo) são instalados em [etapa 4](#).
7. Clique em **Details**.
8. **Cópia do clique a arquivar**.
9. Dentro do assistente da exportação do certificado, clique **em seguida**.
10. Na caixa de diálogo do formato do arquivo da exportação, clique (**.CER**) o botão de rádio **X.509 codificado Base-64**, e clique-o **em seguida**.
11. Entre no nome de arquivo e no lugar a que você quer salvar o certificado de CA.
12. Clique em **Avançar e**, em seguida, clique em **Concluir**.
13. Clique a **APROVAÇÃO** na caixa de diálogo bem sucedida da exportação.
14. Consulte ao lugar onde você salvar o certificado de CA.
15. Abra o arquivo com um editor de texto, tal como o bloco de notas. (Clicar com o botão direito o arquivo, e o escolha **enviam a > bloco de notas**.) A mensagem base64-encoded deve parecer similar ao certificado nesta imagem:
16. Dentro do ASDM, a **configuração do clique**, e clica então o **Gerenciamento de dispositivos**.
17. Expanda o **gerenciamento certificado**, e escolha **certificados de CA**.
18. Clique em **Add**.
19. Clique o **certificado da pasta** no botão de rádio do **formato PEM**, e cole o certificado de CA base64 fornecido pelo vendedor da 3ª parte no campo de texto.
20. O clique **instala o certificado**. Uma caixa de diálogo aparece que confirme a instalação seja bem sucedida.

### Exemplo da linha de comando

```

ciscoasa
ciscoasa(config)#crypto ca authenticate
my.verisign.trustpoint ! Initiates the prompt for paste-
in of base64 CA intermediate certificate. ! This should
be provided by the 3rd party vendor. Enter the base 64
encoded CA certificate. End with the word "quit" on a
line by itself -----BEGIN CERTIFICATE-----
MIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNS+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMaKGA1UEBhmCVVMxZmZAVBgnVBAoTDlZlcm1TaWduLCBjbmuMTAw
LgYDVQQL
EydGbz3IgvGVzdBQdXJwb3NlcYBPbm55LiAgTm8gYXNzdXJhbmNlcY4x
MjAwBgNV
BAMTKVZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgvGVzdBQSB290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsczCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECzMnRm9yIFRlc3Qg
UHVycG9z

```

```

ZXMGt25ses4gIE5vIGFzc3VyYW5jZXMUMUwQAYDVQQLZlUZXJtcyBv
ZiBlc2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgaGVhZCBd
QTCCASiW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuudamv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxx2EQJdnDXuTw0+4t1qj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJcK4pGbcf8DOPvOfGRulwpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwgggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcm1zaWdu
LmNvbS9j
cHMvdGVzdG9hLzA0BgNVHQ8BAf8EBAMCAQYwEQYJYIZIAAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBRRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGN
oYGSspIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXR0IFB1cnBvc2VzIE9ubHkuICB0byBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1cnZlciBUZXR0IFJv
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)# ciscoasa(config-ca-trustpoint)# exit

```

## [Etapa 4. Instale o certificado](#)

### Procedimento ASDM

Use o certificado de identidade fornecido pelo vendedor da 3ª parte para executar estas etapas:

1. Clique a **configuração**, e clique então o **Gerenciamento de dispositivos**.
2. Expanda o **gerenciamento certificado**, e escolha então **certificados de identidade**.
3. Selecione o certificado de identidade que você criou em [etapa 2](#). (a data de expiração deve indicar *pendente*.)
4. O clique **instala**.
5. Clique a **pasta os dados do certificado** no botão de rádio do **formato base-64**, e cole o

certificado de identidade fornecido pelo vendedor da 3ª parte no campo de texto.

6. O clique **instala o certificado**. Uma caixa de diálogo aparece que confirme a importação seja bem sucedida.

### Exemplo da linha de comando

```
ciscoasa
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate ! Initiates prompt to paste the base64
identity ! certificate provided by the 3rd party vendor.
% The fully-qualified domain name in the certificate
will be: webvpn.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself ! Paste the base 64 certificate provided by the
3rd party vendor. -----BEGIN CERTIFICATE-----
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGsf0mYjftANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxMzZAVBgNVBAoTD1ZlcmlTaWduLCBjb20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCSGA1UEAxMkVmVyaVNPZ24gVHJpYWwgU2Vj
dXJlIFNl
cnZlcjBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G
A1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQ2Y28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUIx
OjA4BgNVBASUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNPZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNjby5jb20w
gZ8wDQYJ
KoZlhcNAQEBBQAdgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZba70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxs1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjaAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWVyaXNPZ24uY29t
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybdBKBGNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNPZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNPZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lubi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZlIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMfgwVhYJaW1hZ2UvZ21mMCEwHZAHBgUrDgMCGGQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNPZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCsGSIb3DQEBBQUAA4IBAQAany4GVThPIyL/9y1DBd8N
```

```
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHsa jmMMRy jpydxfk6CIdDMtMGotCavRHD9T12tvwgrBock/v/
54o021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju50
-----END CERTIFICATE----- quit INFO: Certificate
successfully imported ciscoasa(config)#
```

## [Etapa 5. Configurar o WebVPN para usar o certificado recentemente instalado](#)

### Procedimento ASDM

1. A configuração do clique, e clica então o **Gerenciamento de dispositivos**.
2. Expanda **avançado**, e expanda então **ajustes SSL**.
3. Sob Certificados, selecione a relação que é usada para terminar sessões de VPN da Web. Neste exemplo, a interface externa é usada.
4. O clique **edita**.
5. Na lista de drop-down do certificado, escolha o certificado instalado em [etapa 4](#).
6. Clique em **OK**.
7. Clique em **Apply**. Seu certificado novo deve agora ser utilizado para todas as sessões de VPN da Web que terminam na relação especificada.
8. Veja a seção da [verificação](#) a fim confirmar que o processo de instalação era bem sucedido.

### Exemplo da linha de comando

```
ciscoasa
ciscoasa(config)#ssl trust-point my.verisign.trustpoint
outside ! Specifies the trustpoint that will supply the
! SSL certificate for the defined interface.
ciscoasa(config)# wr mem Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08 8808
bytes copied in 3.630 secs (2936 bytes/sec) [OK]
ciscoasa(config)# ! Save configuration.
```

## [Verificar](#)

Use as seguintes etapas para verificar a instalação bem-sucedida do certificado e do uso do vendedor da 3ª parte para conexões VPN da Web.

## [Veja Certificados instalados](#)

### Procedimento ASDM

1. Configuração do clique, e Gerenciamento de dispositivos do clique.
2. Expanda o gerenciamento certificado, e escolha certificados de identidade. O certificado de identidade emitido por seu vendedor da 3ª parte deve aparecer.

### Exemplo da linha de comando



## ciscoasa

```
ciscoasa(config)#show crypto ca certificates ! Displays all certificates installed on the ASA. Certificate Status: Available Certificate Serial Number: 32cfe85eebbd2b5ele30649fd266237d 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 ©)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 ©)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 ©)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.
```

## [Verifique o certificado instalado para o WebVPN com um navegador da Web](#)

A fim verificar que o WebVPN usa o certificado novo, termine estas etapas:

1. Conecte a sua relação WebVPN com um navegador da Web. Use https:// junto com o FQDN que você se usou para pedir o certificado (por exemplo, https://webvpn.cisco.com). Se você recebe uma das seguintes alertas de segurança, execute o procedimento que corresponde àquele alerta: **O nome do Security Certificate é inválido ou não combina o nome do local** Verifique que você usou o FQDN/CN correto a fim conectar à relação WebVPN do ASA. Você deve usar o FQDN/CN que você definiu quando você pediu o certificado de identidade. Você pode usar o comando **cripto do trustpointname dos Certificados Ca da mostra** a fim verificar os Certificados FQDN/CN. **O Security Certificate foi emitido por uma empresa que você não escolheu confiar...** Termine estas etapas a fim instalar o certificado de raiz do vendedor da 3ª parte a seu navegador da Web: Na caixa de diálogo da alerta de segurança, clique o **certificado da vista**. Na caixa de diálogo do certificado, clique a aba do **trajeto do certificado**. Selecione o certificado de CA situado acima de seu certificado de identidade emitido, e clique o **certificado da vista**. O clique **instala o certificado**. No certificado instale a caixa de diálogo do assistente, clique **em seguida**. Clique o **automaticamente seletor a loja do certificado baseada no tipo de** botão de rádio do **certificado**, clique-o **em seguida**, e clique-o então o **revestimento**. Clique **sim** quando você recebe a instalação a alerta da confirmação do certificado. Na operação da importação era a alerta bem sucedida, clica a **APROVAÇÃO**, e clica-a então **sim**. **Nota:** Desde que este exemplo usa o certificado experimental de Verisign o certificado de raiz de CA experimental deve ser instalado a fim evitar erros da

verificação quando os usuários conectam.

2. Fazer duplo clique o ícone do fechamento que aparece no canto inferior direito da página de login WebVPN. A informação instalada do certificado deve aparecer.
3. Reveja os índices para verificar que combina seu certificado dos vendedores da 3ª parte.

## Comandos

No ASA você pode usar diversos comandos show na linha de comando verificar o estado de um certificado.

- **mostre o ponto confiável cripto Ca** — Os indicadores configuraram pontos confiáveis.
- **mostre o certificado Ca cripto** — Indica todos os Certificados instalados no sistema.
- **mostre crls criptos Ca** — Os indicadores puseram em esconderijo listas revogação de certificado (CRL).
- **rsa do mypubkey do show crypto key** — Indica todos os pares de chave de criptografia gerados.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

## Troubleshooting

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

Estão aqui alguns possíveis erros que você pôde encontrar:

- **% do aviso: O CERT de CA não é encontrado. Os certs importados não puderam ser usable.** **INFORMATION: Certificado importado com sucesso** O certificado de CA não foi autenticado corretamente. Use o comando **cripto do trustpointname do certificado Ca da mostra** a fim verificar que o certificado de CA esteve instalado. Se o certificado de CA existe, verifique que provê o ponto confiável correto.
- **ERRO: Não analisam gramaticalmente nem não verificam o certificado importado** Este erro pode ocorrer quando você instala o certificado de identidade e não tem o intermediário ou o certificado CA raiz correto autenticado com o ponto confiável associado. Você deve remover e reauthenticate com o intermediário ou o certificado CA raiz correto. Contacte seu vendedor da 3ª parte a fim verificar que você recebeu o certificado de CA correto.
- **O certificado não contém a chave pública de uso geral** Este erro pode ocorrer quando você tenta instalar seu certificado de identidade ao ponto confiável errado. Você tenta instalar um certificado de identidade inválido, ou o par de chaves associado com o ponto confiável não combina a chave pública contida no certificado de identidade. Use o comando **cripto do trustpointname dos Certificados Ca da mostra** a fim verificar que você instalou seu certificado de identidade ao ponto confiável correto. Procure a linha que indica *pontos confiáveis associados*: Se o ponto confiável errado está listado, use os procedimentos descritos neste documento a fim remover e reinstalar o ponto confiável apropriado. Também, verifique que o par de chaves não mudou desde que o CSR foi gerado.
- **Mensagem de erro: %PIX|ASA-3-717023 SSL não ajustou o certificado do dispositivo para o [trustpoint name] do ponto confiável** Este exibições de mensagem quando uma falha ocorrer quando você ajustar um certificado do dispositivo para o ponto confiável dado a fim autenticar

a conexão SSL. Quando a conexão SSL vem acima, uma tentativa está feita para ajustar o certificado do dispositivo que será usado. Se uma falha ocorre, um Mensagem de Erro está registrado que inclua o ponto confiável configurado que deve ser usado para carregar o certificado do dispositivo e a razão para a falha. *nome do ponto confiável — Nome do ponto confiável para que o SSL não ajustou um certificado do dispositivo.***Ação recomendada:** Resolva a edição indicada pela razão relatada para a falha. Assegure-se de que o ponto confiável especificado esteja registrado e tenha um certificado do dispositivo. Certifique-se que o certificado do dispositivo é válido. Reenroll o ponto confiável, se for necessário.

## Informações Relacionadas

- [Como obter um certificado digital de Microsoft Windows CA usando o ASDM em um ASA](#)
- [Cisco PIX Firewall Software](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)