

在 ASA 8.x 上手动安装第三方供应商证书以便与 WebVPN 一起使用的配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[步骤 1. 验证 Date、Time 和 Time Zone 值是否准确](#)

[步骤 2. 生成证书签名请求](#)

[步骤 3. 验证信任点](#)

[步骤 4. 安装证书](#)

[步骤 5. 将 WebVPN 配置为使用新安装的证书](#)

[验证](#)

[查看已安装的证书](#)

[使用 Web 浏览器验证为 WebVPN 安装的证书](#)

[命令](#)

[故障排除](#)

[相关信息](#)

简介

此配置示例描述如何在 ASA 上手动安装第三方供应商数字证书，以便与 WebVPN 一起使用。此示例中使用 Verisign Trial Certificate。每个步骤都包含 ASDM 应用程序步骤和 CLI 示例。

先决条件

要求

本文档要求您能够访问证书机构 (CA) 以便进行证书注册。例如，第三方 CA 供应商包括 (但不限于) Baltimore、Cisco、Entrust、Geotrust、Godaddy、iPlanet/Netscape、Microsoft、RSA、Thawte 和 VeriSign。

使用的组件

本文档使用运行软件版本 8.0(2) 和 ASDM 版本 6.0(2) 的 ASA 5510。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始 (默认) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

要在 ASA 上安装第三方供应商数字证书，请完成以下步骤：

1. [验证伊达市、时间和时间区域值是准确的](#)
2. [生成证书签名请求](#)
3. [验证信任点](#)
4. [安装证书](#)
5. [配置WebVPN最近使用预装证书](#)

注意： 使用 [命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

[步骤 1. 验证 Date、Time 和 Time Zone 值是否准确](#)

ASDM 步骤

1. 单击 **Configuration**，然后单击 Device Setup。
2. 展开 **System Time**，然后选择 Clock。
3. 验证列出的信息是否准确。要正确通过证书验证，Date、Time 和 Time Zone 值必须准确。

命令行示例

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

[步骤 2. 生成证书签名请求](#)

证书签名请求(CSR)要求为了第三方CA能发行身份证书。CSR 包含 ASA 的可分辨名称 (DN) 字符串与 ASA 的已生成公钥。ASA 将使用生成的私钥对 CSR 进行数字签名。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Device Management。
2. 展开 **Certificate Management**，然后选择 Identity Certificates。
3. 单击 **Add**。
4. 单击 **Add a new identity certificate** 单选按钮。
5. 对于 Key Pair，单击 **New**。**注意：** 如果使用 2048 个位证书，请生成关键 2048 的位。
6. 单击 **Enter new key pair name** 单选按钮。您应该明确标识密钥对名称以进行识别。
7. 单击 **Generate Now**。现在应已创建密钥对。
8. 要定义“Certificate Subject DN”，请单击 **Select**，然后配置下表中所示的属性：**表 4.1：DN 属性**要配置这些值，可以从 Attribute 下拉列表中选择值或输入值，然后单击 **Add**。**注意：** 某些第三方供应商在颁发身份证书之前要求提供特定属性。如果不确定需要提供什么属性，请与您的供应商联系以了解详细信息。

9. 添加相应的值之后，单击 **OK**。将会出现 Add Identity Certificate 对话框，并显示已填入的 Certificate Subject DN。
10. 单击 **Advanced**。
11. 在“FQDN”字段中，输入将用于从 Internet 访问设备的 FQDN。此值应与用于公用名称 (CN) 的 FQDN 相同。
12. 单击 **OK**，然后单击 Add Certificate。系统会提示您将 CSR 保存到本地计算机上的文件中。
13. 单击 **Browse**，选择用于保存 CSR 的位置，然后使用 .txt 扩展名保存文件。**注意**：使用 .txt 扩展名保存文件后，您可以使用文本编辑器（例如记事本）打开此文件，并查看 PKCS#10 请求。
14. 将保存的 CSR 提交给第三方供应商。将 CSR 提交给第三方供应商后，他们将为您提供要在 ASA 上安装的身份证书。

命令行示例

在 ASDM 6.x 中，当生成 CSR 或安装 CA 证书后，将自动创建信任点。在 CLI 中，必须手动创建信任点。

```

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:
MIICHjCCAYcCAQAwgaAxEDAObgNVBACTB1JhbGVpZ2gxZmZAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA

```

```
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBdfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dz0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKULaRc783w4BMO5lulIEhHgRqAxrTbQn0B7JPI
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)#
```

步骤 3. 验证信任点

从第三方供应商处收到身份证书后，您可以继续执行此步骤。

ASDM 步骤

1. 将身份证书保存到本地计算机中。
2. 如果您收到的是非文件形式的 base64 加密证书，则必须复制此 base64 消息，并将其粘贴到文本文件中。
3. 将文件扩展名改为 .cer。注意：使用扩展名 .cer 重命名文件后，文件图标将显示为证书。
4. 双击此证书文件。此时，将显示“Certificate”对话框。注意：如果 General 选项卡中显示“Windows does not have enough information to verify this certificate”信息，则在继续执行此步骤之前，您必须获取第三方供应商的根 CA 或中间 CA 证书。请与第三方供应商或 CA 管理员联系，以获得其发放的根 CA 或中间 CA 证书。
5. 单击 **Certificate Path** 选项卡。
6. 单击位于所发放的身份证书上方的 CA 证书，然后单击 **View Certificate**。此时，将显示中间 CA 证书的详细信息。警告：请勿在此步骤中安装身份（设备）证书。在此步骤中仅添加根、辅助根或 CA 证书。身份（设备）证书在[步骤 4](#) 中安装。
7. 单击 **Details**。
8. 单击 **Copy to File**。
9. 在“Certificate Export Wizard”中，单击 **Next**。
10. 在“Export File Format”对话框中，单击 **Base-64 encoded X.509 (.CER)** 单选按钮，然后单击“Next”。
11. 输入文件名以及要用于保存 CA 证书的位置。
12. 单击 **Next**，然后单击“Finish”。
13. 在“Export Successful”对话框中，单击 **OK**。
14. 浏览到 CA 证书的保存位置。
15. 使用文本编辑器打开文件，例如记事本。（右键单击文件，然后选择 **Send To > Notepad**。）将会显示类似于下图中证书的 base64 编码信息：
16. 在 ASDM 中，单击 **Configuration**，然后单击 **Device Management**。
17. 展开 **Certificate Management**，然后选择 **CA Certificates**。
18. 单击 **Add**。
19. 单击 **Paste certificate in PEM Format** 单选按钮，然后将第三方供应商提供的 base64 CA 证书粘贴到文本字段中。
20. 单击 **Install Certificate**。确认安装是成功的对话框出现。

命令行示例

```
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
jDELMakGA1UEBhmCVVMxZAVBgnVBAoTD1Zlcm1TaWduLCBjbmuMTAw
LgYDVQQL
EydGb3IgvGVzdCBQdXJwb3NlcyBpbm5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgvGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMfoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwSW5jLjEwMC4GA1UECXMnRm9yIFRlc3Qg
UHVycG9z
ZXMGt25seS4gIE5vIGFzc3VyYW5jZXMUMUIwQAYDVQQLZ1UZXXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgvGVzdCBD
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
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNPZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICB0byBhc3NlcmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNPZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLeWTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY21
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/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
```



```

bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBGwNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXNO
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwa jAkBggrBgEFBQcwAYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZlIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBAQUAA4IBAQAAnym4GVThPIyL/9y1DBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHsa jmmMryjpydxfk6CIddMtMGotCavRHD9T12tvwgrBock/v/
54o021kB
SmLzVV7crlYJEUhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cnevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE----- quit INFO: Certificate
successfully imported ciscoasa(config)#

```

步骤 5. 将 WebVPN 配置为使用新安装的证书

ASDM 步骤

1. 单击 **Configuration**，然后单击 **Device Management**。
2. 展开 **Advanced**，然后展开“**SSL Settings**”。
3. 在证书下，请选择使用终止 WebVPN 会话的接口。在本例中，使用外部接口。
4. 单击 **Edit**。
5. 在“Certificate”下拉列表中，选择在 [步骤 4](#) 中安装的证书。
6. 单击 **Ok**。
7. 单击 **Apply**。现在，在指定接口上终止的所有 WebVPN 会话应该已使用新的证书。
8. 要确认安装过程是否成功，请参阅 [验证](#) 部分。

命令行示例

```

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)# wr mem Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08 8808
bytes copied in 3.630 secs (2936 bytes/sec) [OK]
ciscoasa(config)# ! Save configuration.

```

验证

请使用以下步骤验证第三方供应商证书和使用的成功的安装WebVPN连接的。

[查看已安装的证书](#)

ASDM 步骤

1. 单击 **Configuration**，然后单击“Device Management”。
2. 展开 **Certificate Management**，然后选择 Identity Certificates。此时应显示第三方供应商颁发的身份证书。

命令行示例

```
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:
63bla5cdc59f78801da0636cf975467b 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.
```

[使用 Web 浏览器验证为 WebVPN 安装的证书](#)

要验证 WebVPN 是否使用新证书，请完成以下步骤：

1. 通过 Web 浏览器连接到 WebVPN 接口。将 https:// 以及用于请求证书的 FQDN (例如，https://webvpn.cisco.com)。如果收到以下安全警报之一，请执行与该警报对应的步骤：
The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site 验证您使用的 FQDN/CN 是否正确，以便连接到 ASA 的 WebVPN 接口。必须使用请求身份证书时定义的 FQDN/CN。可以使用 `show crypto ca certificates trustpointname` 命令验证证书 FQDN/CN。
The security certificate was issued by a company you have not chosen to trust... 要将第三方供应商根证书安装到 Web 浏览器，请完成以下步骤：在“Security Alert”对话框中，单击 **View Certificate**。在“Certificate”对话框中，单击 **Certificate Path** 选项卡。选择位

于为您颁发的身份证书上方的 CA 证书，然后单击 **View Certificate**。单击 **Install Certificate**。在“Certificate Install Wizard”对话框中，单击 **Next**。单击 **自动地精选根据证书单选按钮种类的证书存储**，其次单击和然后单击 **芬通社**。当收到安装证书确认提示时，单击 **Yes**。显示 *Import operation was successful* 提示时，单击 **OK**，然后单击“**Yes**”。**注意：**由于此示例使用 Verisign Trial Certificate，因此必须安装 Verisign Trial CA Root Certificate，以避免用户连接时出现验证错误。

2. 双击 WebVPN 登录页右下角显示的锁图标。此时应显示已安装证书的信息。
3. 查看这些内容，以验证是否与您的第三方供应商证书相匹配。

命令

在 ASA 上，可以在命令行中使用若干 show 命令验证证书的状态。

- **show crypto ca trustpoint** — 显示已配置的信任点。
- **show crypto ca certificate** — 显示系统上安装的所有证书。
- **show crypto ca crls** — 显示缓存的证书撤销列表 (CRL)。
- **show crypto key mypubkey rsa** — 显示所有生成的加密密钥对。

[命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

本部分提供的信息可用于对配置进行故障排除。

以下是您可能会遇到的一些可能的错误：

- **%亚里桑：CA cert is not found.The imported certs might not be usable.INFO:Certificate successfully imported**对 CA 证书的身份验证不正确。请使用 **show crypto ca certificate trustpointname** 命令验证是否安装了 CA 证书。如果 CA 证书存在，请验证它是否引用了正确的信任点。
- **ERROR:Failed to parse or verify imported certificate**在安装身份证书时，如果您不具有通过相关信任点验证的正确的中间或根 CA 证书验证，则可能会出现此错误。您必须删除此身份证书，然后使用正确的中间或根 CA 证书重新验证身份。请与您的第三方供应商联系以验证您收到的 CA 证书是否正确。
- **Certificate does not contain general purpose public key**当您尝试将身份证书安装到错误的信任点时，可能会出现此错误。这是因为您尝试安装无效的身份证书，或者与信任点关联的密钥对不匹配身份证书中包含的公钥。请使用 **show crypto ca certificates trustpointname** 命令以验证您是否将身份证书安装到正确的信任点。请查找以 **Associated Trustpoints** 开头的行：如果所列出的信任点是错误的，请使用本档中介绍的步骤删除信任点，然后重新安装正确的信任点。同时，请验证在生成 CSR 之后密钥对是否未更改。
- **错误消息：%PIX|ASA-3-717023 SSL失败设置信任点[trustpoint name]的设备证书**当为给定信任点设置设备证书以对 SSL 连接进行身份验证时，如果发生故障，则会显示此消息。当 SSL 连接恢复正常时，会尝试设置将要使用的设备证书。如果发生故障，则会记录一条错误消息，其中包括将用于加载设备证书的已配置信任点以及发生故障的原因。**信任点名称—SSL 未能设置设备证书的信任点名称。建议操作：**解决所报告的故障原因指出的问题。确保指定的信任点已注册并具有设备证书。确保设备证书有效。重新注册信任点（如果需要）。

相关信息

- [如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书](#)
- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX \)](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)