ASA 7.x手動安裝第三方供應商證書以用於 WebVPN配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 設定 步驟1.檢驗日期、時間和時區值是否準確 步驟2.生成RSA金鑰對 步驟3.建立信任點 步驟4.生成證書註冊 步驟5.驗證信任點 步驟6.安裝證書 步驟7.配置WebVPN以使用新安裝的證書 驗證 替換來自ASA的自簽名證書 檢視安裝的證書 使用Web瀏覽器驗證WebVPN的安裝證書 更新SSL證書的步驟 指令 疑難排解 相關資訊

簡介

此配置示例描述如何在ASA上手動安裝第三方供應商數位證書以用於WebVPN。本示例中使用的是 Verisign試用證書。每個步驟都包含ASDM應用程式過程和CLI示例。

必要條件

需求

本文檔要求您有權訪問證書頒發機構(CA)進行證書註冊。受支援的第三方CA供應商包括 Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA和VeriSign。

採用元件

本文使用的是運行軟體版本7.2(1)和ASDM版本5.2(1)的ASA 5510。 但是,本文檔中的過程適用於 任何運行7.x且帶有任何相容ASDM版本的ASA裝置。 本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

要在PIX/ASA上安裝第三方供應商數位證書,請完成以下步驟:

- 1. <u>驗證日期、時間和時區值是否準確</u>。
- 2. <u>生成RSA金鑰對</u>。
- 3. 建立信任點。
- 4. <u>生成證書註冊</u>。
- 5. <u>驗證信任點</u>。
- 6. <u>安裝證書</u>。
- 7. <u>配置WebVPN以使用新安裝的證書</u>。

步驟1.檢驗日期、時間和時區值是否準確

- 1. 按一下配置, 然後按一下屬性。
- 2. 展開Device Administration,然後選擇Clock。
- 3. 驗證列出的資訊是否準確。Date、Time和Time Zone的值必須準確無誤,才能進行正確的證書 驗證。



命令列示例

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

步驟2.生成RSA金鑰對

生成的RSA公鑰與ASA的身份資訊結合起來形成PKCS#10證書請求。您應該使用為其建立金鑰對的 信任點明確標識金鑰名稱。

- 1. 按一下Configuration,然後按一下Properties。
- 2. 展開Certificate, 然後選擇Key Pair。
- 3. 按一下「Add」。

a.	E Certificate		
68	- Authentication		
NAT		Key Pair Name Usage Modulus Size	Add
<u>21</u>	Key Pair		1
VPN			Show Details
	E- A Trustpoint		
A .	- Configuration		Delete
	- Sport	Add Key Pair	
CSD Manager			Different [
130	E Bevice Access	Name C Line defend key name	Retresh
- 25	E-B Device Administration	reame. • Ose determine	
Routing	E-f DHC Services	G my verition key	
on	🕀 🚜 DNS 🛰	[[]].().().()]	
68	High Availability and Scal		
Global Objects	Failover	Size: 1024	
	Fragment		
3		Usage: 📀 General Purpose 🔿 Special	
Properties	HTTP/HTTPS		
	🔁 🔩 IP Audit		
	🔁 🚺 Logging		
	Priority Queue	Generate Now Cancel Help	
	- 🙀 SSL		
	SUNRPC Server		
	TCP Options		
	Timeouts		

- 4. 輸入金鑰名稱,選擇模數大小,然後選擇使用型別。附註:建議的金鑰對大小為1024。
- 5. 按一下「Generate」。您建立的金鑰對應該列在「金鑰對名稱」列中。

命令列示例

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)#

步驟3.建立信任點

需要信任點來宣告您的ASA將使用的證書頒發機構(CA)。

- 1. 按一下Configuration,然後按一下Properties。
- 2. 展開Certificate,然後展開Trustpoint。
- 3. 選擇Configuration,然後點選Add。

Configuration > Properties > Cer	rtificate > Trustpoint > Configuration	
Startup Wizard	Configuration	
🕀 🚮 AAA Setup	Configure a Certificate Authority (CA) as a trustopint	
	comigure a ceruncale Automity (CA) as a trasponit.	
🕀 📆 ARP		
-B Client Update		
E-E Certificate	Trustpoint Name Device Certificate Subject CA Certificate Subject Add	
Authentication		
-2 Enrolment	Edit	
Import Certificate		
- The Key Pair	Defete	
Manage Certificates	Detere	
Se Configuration	Request CRL	
Export		
Device Access		

- 4. 配置以下值:**信任點名**:信任點名稱應與預期用途相關。(此示例使用*my.verisign.trustpoint*。)**金鑰對**:選擇<u>步驟2</u>中生成的金鑰對。(*my.verisign.key*)
- 5. 確保選中「手動註冊」。
- 6. 按一下「Certificate Parameters」。系統將顯示Certificate Parameters對話方塊。
- 7. 按一下Edit,然後配置下表中列出的屬性:若要設定這些值,請從「屬性」下拉式清單中選擇 一個值,輸入該值,然後按一下Add。

			Common Name (CN)	webvpn.cisco.com
N Attribute to be	Added	7	Department (OU)	TSWEB
		0.44	Company Name (O)	Cisco Systems
Attribute: Se	elect Attribute	Add >>	State (St)	North Carolina
			State (St)	US
/alue:		Delete	Location (L)	Raleigh

- 8. 新增適當的值後,按一下確定。
- 9. 在「證書引數」對話方塊中,在「指定FQDN」欄位中輸入FQDN。此值應與用於公用名 (CN)的FQDN相同。

Enter	r the values for the parameters that are to be included in the certificate.
Subje	ect DN: ystems,St=North Carolina,St=US,L=Raleigh
FQ	ON Use FQDN of the device
	Specify FQDN webvpn.cisco.com
	O Use none
E-ma	il:
IP Ac	ldress:
	Include device serial number
	OK Cancel Help
10. 按一下「 O ł	<□(確定)。

🖆 Add Trustpoint Configuration	
Trustpoint Name: my.verisign.truspoint	
Generate a self-signed certificate on enrollment	
If this option is enabled, only Key Pair and Certificate Parameters can be specified.	
Enrollment Settings Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Adva	anced
Key Pair: my.verisign.key Show Details New Key Pair	
Challenge Confirm Challenge	
Password: Password:	
Enrollment Mode can only be energified if there are no certificates accorded with this tructment	
Enrolment Mode can only be specified in there are no certificates associated with this trustpoint.	
Enrolment Mode	
Use manual enrolment	
C Use automatic enrollment	
Encolmant LIPL: http://	
Enrolment one. http://	
Retry Period: 1 minutes	
Retry Count: 0 (Use 0 to indicate unlimited retries)	
Certificate Parameters	
OK Cancel Help	

命令列示例

ciscoasa
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint
! Creates the trustpoint.
ciscoasa(config-ca-trustpoint)# enrollment terminal
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>
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 <u>Step 3</u> . ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

步驟4.生成證書註冊

ASDM過程

- 1. 按一下Configuration,然後按一下Properties。
- 2. 展開Certificate,然後選擇Enrollment。
- 3. 驗證是否已選中<u>步驟3</u>中建立的信任點,然後按一下Enroll。出現一個對話方塊,其中列出了證 書註冊請求(也稱為證書簽名請求)。

To complete management	the enrollment process, please paste the following PKCS10 enrollment request into the interface of the CA.
You will nee	to install the certificate after receiving it.
Go to Config	uration ≻ Properties > Certificate > Import Certificate to do so.
Certificate R	aquest.
hvcNAQkC	FhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN
AQEBBQAD	gYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm
psMFP7De	KPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5Gh1KY
mAH40WUX	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF
mAH40WUX AgMBAAGg	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd
mAH40WUX AgMBAAGg ghtDaXNj	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA
mAH40WUX AgMBAAGg ghtDaXNj gmoBmSRV	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpSlbveKew0AdG5/fxnJRYU2UunllW6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh gonnkGTJ	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYPOoeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQSSteWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 llvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh gonnkGTJ	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpSlbveKew0AdG5/fxnJRYU2UunllW6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 llvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh gonnkGTJ 0 End -	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQSSteWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpSlbveKew0AdG5/fxnJRYU2UunllW6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 llvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= This line not part of the certificate request
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh gonnkGTJ 0 End -	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpSlbveKew0AdG5/fxnJRYU2UunllW6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 llvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= This line not part of the certificate request
mAH4OWUX AgMBAAGg ghtDaXNj gmoBmSRV gEjVABVh gonnkGTJ 0 End -	bil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF RjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQBAwIFoDAmBgNVHREEHzAd b0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA nL0qyDtpSlbveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 B7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 llvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= This line not part of the certificate request

4. 將PKCS#10註冊請求複製到文本檔案,然後將CSR提交給相應的第三方供應商。在第三方供 應商收到CSR後,他們應該發出身份證書以進行安裝。

命令列示例

裝置名稱1
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint
<pre>! 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</pre>

```
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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVt.czE0
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4vTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
GWIDAOAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3vEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
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]:
ciscoasa(config)#
```

步驟5.驗證信任點

收到來自第三方供應商的身份證書後,您可以繼續執行此步驟。

- 1. 將身份證書儲存到本地電腦。
- 2. 如果您獲得的base64編碼證書不是作為檔案提供的,則必須複製base64消息並將其貼上到文 本檔案中。
- 8. 將檔案重新命名為.cer副檔名。注意:使用.cer副檔名重新命名檔案後,檔案圖示應顯示為證書。
- 4. 按兩下證書檔案。出現「Certificate(證書)」對話方塊。

ertificate	? ×
General Details Certification Path	
	-
Certificate Information	
Thistertificate is intended for the following purpose(s):	
 Ensures the identity of a remote computer Proves your identity to a remote computer 	
•2.16.840.1.113733.1.7.21	
— operal,百쬷山顕云「Windows does not have opeyab information	to vorify

General」頁籤中顯示「Windows does not have enough information to verify this certificate」 消息,則必須先獲取第三方供應商根CA或中間CA證書,然後才能繼續此過程。請聯絡您的第 三方供應商或CA管理員,以獲取頒發的根CA或中間CA證書。

- 5. 按一下Certificate Path頁籤。
- 6. 按一下位於已頒發身份證書上方的CA證書,然後按一下View Certificate。

ertificate	<u>? ×</u>
General Details Certification Path	
Certification path VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA webvpn.cisco.com	
	View Certificate
Certificate status:	
This certificate is OK.	
	ОК

書的詳細資訊。**警告:**不要在此步驟中安裝身份(裝置)證書。在此步驟中只新增根、從根或 CA證書。身份(裝置)證書安裝在<u>步驟6</u>中。

7. 按一下「**Details**」。

Certificate	<u>? ×</u>
General Details Certification Path	1
	<u> </u>
Show: <all></all>	
	Value
	V3
	63 b1 a5 cd c5 9F 78 80 1d a0
	shaiRSA
	Tuesday, Estructure Server Te
	Supday, February 08, 2005 0
	VeriSign Trial Secure Server Te
	RSA (2048 Bits)
	it Dues outline
Ec	Copy to File

- 8. 按一下「Copy to File」。
- 9. 在「Certificate Export Wizard(證書匯出嚮導)」中,按一下「Next(下一步)」。
- 10. 在「匯出檔案格式」對話方塊中,按一下Base-64 encoded X.509(.CER)單選按鈕,然後按 一下下一步。

tificate Export Wizard Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
C Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
< Back Next > Canc	3I

11. 輸入要儲存CA證書的檔名和位置。

12. 按一下**Next**,然後按一下**Finish**。

icate Export Wizard		
l e to Export Specify the name of the file you wa	ant to export	
File name:		
c:\introotca		Browse
		bromsenn
	< Back Nevt >	Cape

13. 在「匯出成功」對話方塊中按一下確定。

- 14. 瀏覽到儲存CA證書的位置。
- 15. 使用文字編輯器(例如記事本)開啟檔案。(按一下右鍵該檔案,然後選擇「傳送到」>「記事本」。)Base64編碼的訊息應該顯示與此圖中的憑證類似

File Edit Format View Help

----BEGIN CERTIFICATE---MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24qVHJpYWwqU2VjdXJlIFNl cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTkloVowgZ4x CZAJB9NVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q2lzY28qU3lzdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BgNVBAsUMVRlcm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBWIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52zXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9TvljTZWN1cmUtyWlhLnZlcmlzaWduLmNvbS9TvljUcmlhbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zxJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKozIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTgIorIClawwwx+RHCcTqIrlzf0VfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvl×zŹji0J51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja |idT1FmBvf02qaZS6S40= ----END CERTIFICATE----

- 16. 在ASDM中,按一下**Configuration**,然後按一下**Properties。**
- 17. 展開Certificate,然後選擇Authentication。
- 18. 按一下Enter the certificate text in hexadecimal or base64 format單選按鈕。
- 19. 從文本編輯器將base64格式的CA證書貼上到文本區域。
- 20. 按一下「Authenticate」。

Configuration > Properties > C	ertificate > Authentication
Startup Wizard	Authentication
AAA Setup AAA Setup Anti-Spoofing ARP	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a trustpoint and installed on the device.
Auto Update	Trustpoint Name: wy.verisign.truspo Edit New
Authentication	Fingerprint (optional):
- Si Import Certificate - Si Key Pair	The certificate text can be specified if the selected trustpoint is configured for manual enrollment.
Manage Certificates Trustpoint Configuration Export Import Device Access Device Administration DHCP Services DHCP Services Failover Failover History Metrics	Certificate Text
IP Audit IP Audit IP Gring Priority Queue SSL SUNRPC Server	Authentication Successful The trustpoint my.verisign.truspoint has been authenticated.
TCP Options	ОК

21. 按一下「**OK**」(確定)。 **命令列示例**

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
itselfBEGIN CERTIFICATE
MILEWDCCBCmgAwlBAglQY/GIzCWIelAdoGNS+XVGezANBgkqhklG9W0B
JDELMARGATOEBIIMCVVMXFZAVBGNVBAOTDIZICIIITAWGULCBUDIIMUMTAW
LGIDVQQD FydGb3TauGUzdCB0dX.Tyb3Nl cyBDbmy5I.i barm8aYXNzdX.TbbmNl cy4y
MjawBaNV
BAMTKVZlcmlTaWduIFRvaWFsIFNlY3VvZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
${\tt BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD}$

QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8D0Pv0fGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
CHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
OYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BASTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
AlUEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
Kq12341RO1L512S1110022MANp2H4D1W41CISG5SHDD1WSRm1H3BW/S0
AISTAVRICDSQUMD+NYKSIBZABZOIAINSIIWZAJEQJUQA+QSSJNEW+DEU
$\int 4A H dV G N$
II/KK/TIIVOIWST/GOUKFMARVDNG-
mit
Aut.
/ Manually pasted certificate into CLT_INFO.
Certificate has the following attributes: Fingerprint:
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this
certificate? [ves/no]: ves Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)#

步驟6.安裝證書

ASDM過程

使用第三方供應商提供的身份證書執行以下步驟:

- 1. 按一下Configuration,然後按一下Properties。
- 2. 展開Certificate, 然後選擇Import Certificate。
- 3. 按一下Enter the certificate text in hexadecimal or base64 format單選按鈕,然後將base64身 份證書貼上到文本欄位中。

Configuration > Properties > C	ertificate > Import Certificate
- 39 Startup Wizard	Import Certificate
🕀 🚮 AAA Setup	Install an identity cartificate that was received from a Cartificate Authority (CA) in response to a menual
- 🐯 Anti-Spoofing	enrolled nerved
🕀 🐻 ARP	er i deller i fogletet.
	Trustenist Name
E Certificate	my vensign truspo Edit New
Authentication	
- 2 Enrolment	Certificate Text
Import Certificate	C Insert from a file
Key Pair	s import from a file:
Manage Certificates	
- Sa Trustpoint	1. Enter the certificate text in nexadecimal or baseb4 format:
Configuration	
Export	MS5odAD/wDOV_Ko7ikwaNAGEEROADwaERA/MitawSKECodwaAA/V/diaky
import	missian with the analysis in the analysis of t
Device Access	tFkFFSFbleCK/hh6MaMb40z6kiFizo/Umt6JDoU3B00U/vm+tq02eTV/dz/VE
B-B Device Administration	0YVwM3KDQAC6EbArtUoAxovDbJucdxb6ZVTtyevMcgzCkXMHEVxa5/P)
E-B DNS	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4ufcGgGZD6itVGx26b5OWTz8K:
High Availability and Scal	8EvHm3grdbDZP+ISMotWYE+CgfKpZb+CPAqH2Cdpz2pJiJih6CS6NM=
Failover	END CERTIFICATE
- K Fragment	
- Istory Metrics	
-THE HTTP/HTTPS	🔂 Information
🖲 📲 🔁 IP Audit	
E-1 Logging	
- Priority Queue	Certificate import succeeded.
SUNRPC Server	
TCP Options	
Timeouts	UK
URL Fittering	
1	

4. 按一下Import,然後按一下OK。

命令列示例

ciscoasa
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate
I 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 itselfBEGIN
CERTIFICATE
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVR1cm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j
b20vY3Bz
L3R1c3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTA1VTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G
AluebxQH
UmFsZW1naDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECxQF
VFNXRUIX

OjA4BgNVBAsUMVR1cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxS1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRw0i8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc21nbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9T12tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
END CERTIFICATE
quit
INFO: Certificate successfully imported
CISCOASA(CONIIG)#

步驟7.配置WebVPN以使用新安裝的證書

- 1. 按一下「Configuration」,按一下「Properties」,然後選擇「SSL」。
- 2. 在Trustpoints區域中,選擇將用於終止WebVPN會話的介面。(此示例使用外部介面。)
- 3. 按一下「Edit」。系統將顯示Edit SSL Trustpoint對話方塊。

Configuration > Properties > S	3L
	SSL
🕀 🖬 AAA Setup	Configure CCI assessments These exceptions official both ACDM and MANN (CAI assess
-B Anti-Spoofing	Configure SSL parameters. These parameters affect both ASDM and WebVPN access.
E-B ARP	Server SSL Version: Any Client SSL Version: Any
🛃 Auto Update	Formation
	Line year
🔁 🔂 Certificate	Available Algorithms Add >> Active Algorithms Move Up
E f Device Access	30ES-SHA1
E-B Device Administration	Se Edit SSI Taustaniat
E BHCP Services	
🔄 🚚 DNS	Specify an enrolled trustopint to be used for SSL at theritication on the outside interface. To enroll a trustopint
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.
- Failover	
- Fragment	
HTTP/HTTPS	Interface: outside
E-IQ IP Audit	
E Logging	Enrolled Trustpoint: my.verisign.trustp 💌
Priority Queue	
SUNKPC Server	
Thread to	Circei nep
LIFL Effering	
H- VALCE	Trustpoints
a woor	Specify which enrolled trustopints if any should be used for SSL authentication on each interface. The fallback
	trustpoint will be used on interfaces not associated with a trustpoint of their own.
	Fallback Trustmint
	Interface Trustpoint Edit
	management
	outside my verisign trustpoint

4. 從Registered Trustpoint下拉選單中,選擇您在<u>步驟</u>3中建立的信任點。

5. 按一下「OK」,然後按一下「Apply」。

現在,您的新證書應該用於終止於指定介面的所有WebVPN會話。有關如何驗證成功安裝的資訊 ,請參閱本文檔中的驗證部分。

命令列示例

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



本節介紹如何確認第三方供應商證書安裝成功。

替換來自ASA的自簽名證書

本節介紹如何從ASA替換已安裝的自簽名證書。

- 1. 向Verisign發出證書簽名請求。從Verisign收到請求的證書後,可以直接在同一信任點下安裝。
- 2. 鍵入以下命令: crypto ca enroll Verisign系統將提示您回答問題。
- 3. 對於終端顯示證書請求,輸入**yes**,並將輸出傳送到Verisign。
- 4. 一旦他們向您提供新證書,請鍵入以下命令: crypto ca import Verisign certificate

檢視安裝的證書

ASDM過程

- 1. 按一下Configuration,然後按一下Properties。
- 2. 展開**Certificate**,然後選擇**Manage Certificates**。用於Trustpoint身份驗證的CA證書和第三方供 應商頒發的身份證書應顯示在Manage Certificates區域中。

Startup Wizard	Manage Certificates					
AAA Setup	Manage the Certificates associated with trustpoints.					
E-B ARP	Subject	Tune	Trustroint	Status	lleane	a did
-B Client Update	VeriSign Trial	CA	my.verisign.tru	Available	General Purpo	Add
E Certificate	webvpn.cisco	Identity	my.verisign.tru	Available	General Purpo	Show Details
- Enrolment						
- Import Certificate						Refresh
Key Pair						Delete
E-war inustpoint						

אן יניניע נו או

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://SVRSecurecrl.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.

使用Web瀏覽器驗證WebVPN的安裝證書

若要確認WebVPN是否使用新憑證,請完成以下步驟:

- 1. 通過Web瀏覽器連線到WebVPN介面。使用https://以及您用來請求證書的FQDN(例如 https://webvpn.cisco.com)。如果收到以下安全警報之一,請執行與該警報對應的過程:安全 證書的名稱無效或與站點名稱不匹配驗證您使用正確的FQDN/CN以連線到ASA的WebVPN介 面。必須使用您在請求身份證書時定義的FQDN/CN。您可以使用show crypto ca certificates trustpointname命令驗證證書FQDN/CN。安全證書由您未選擇信任的公司頒發......完成以下步 驟,將第三方廠商根憑證安裝到Web瀏覽器中:在「安全警報」對話方塊中,按一下檢視證書 。在「證書」對話方塊中,按一下證書路徑頁籤。選擇位於您頒發的身份證書上方的CA證書 ,然後按一下View Certificate。按一下「Install Certificate」。在「證書安裝嚮導」對話方塊 中,按一下下一步。選擇Automatically select the certificate store based on the type of certificate單選按鈕,按一下Next,然後按一下Finish。當您收到Install the certificate confirmation提示時,按一下Yes。在「匯入操作成功」提示符下,按一下OK,然後按一下 Yes。注意:由於此示例使用Verisign試用證書,因此必須安裝Verisign試驗CA根證書,以避 免使用者連線時出現驗證錯誤。
- 2. 按兩下WebVPN登入頁面右下角顯示的鎖定圖示。應顯示安裝的證書資訊。
- 3. 檢視內容,確認其與您的第三方供應商證書相匹配。

Cert	tificate	? ×
Ge	eneral Details Certification Path	1
	Certificate Information	
	This certificate is intended for the following purpose(s): •Ensures the identity of a remote computer	-
	* Refer to the certification authority's statement for details.	- 11
	Issued to: webypn.cisco.com	
	Issued by: VeriSign Trial Secure Server Test CA	
	Valid from 8/14/2007 to 8/29/2007	
	Install Certificate Issuer Stateme	nt
	0	<

更新SSL證書的步驟

完成以下步驟即可續訂SSL憑證:

- 1. 選擇需要續訂的信任點。
- 2. 選擇enroll。出現以下消息:如果再次成功註冊,則當前證書將替換為新證書。是否要繼續?
- 3. 選擇yes。這會產生新的CSR。
- 4. 將CSR傳送到CA,然後在您傳回新ID憑證時將其匯入。
- 5. 刪除信任點並將其重新應用到外部介面。

指令

在ASA上,您可以在命令列中使用幾個show命令來驗證證書的狀態。

- show crypto ca trustpoint 顯示已配置的信任點。
- show crypto ca certificate 顯示系統上安裝的所有證書。
- show crypto ca crls 顯示快取的證書吊銷清單(CRL)。

• show crypto key mypubkey rsa — 顯示所有生成的加密金鑰對。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下是您可能會遇到的一些可能錯誤:

- •%警告:未找到CA證書。匯入的證書可能不是usable.INFO:已成功匯入證書CA證書未正確驗證 。使用show crypto ca certificate trustpointname命令以驗證CA證書是否已安裝。尋找以CA憑 證開頭的行。如果安裝了CA證書,請驗證它是否引用了正確的信任點。
- ・錯誤:無法分析或驗證匯入的證書安裝身份證書並且沒有用關聯的信任點進行身份驗證的正確 的中間或根CA證書時,可能出現此錯誤。您必須移除並使用正確的中間CA或根CA證書重新進 行身份驗證。請與您的第三方供應商聯絡,以驗證您是否收到了正確的CA證書。
- 證書不包含通用公鑰當您嘗試將身份證書安裝到錯誤的信任點時,可能會發生此錯誤。您試圖 安裝無效的身份證書,或者與信任點關聯的金鑰對與身份證書中包含的公鑰不匹配。使用show crypto ca certificates trustpointname 命令以驗證您的身份證書是否已安裝到正確的信任點。查 詢說明Associated Trustpoints:如果列出錯誤的信任點,請使用本文檔中介紹的過程以刪除並重 新安裝到適當的信任點,同時驗證金鑰對自生成CSR以來是否未更改。
- 錯誤消息:%PIX|ASA-3-717023 SSL無法為信任點[trustpoint name]設定裝置證書</mark>當您為給定 信任點設定裝置證書以驗證SSL連線時,將顯示此消息。當SSL連線啟動時,將嘗試設定將使 用的裝置證書。如果發生故障,則會記錄一條錯誤消息,其中包括用於載入裝置證書的已配置 信任點和故障原因。trustpoint name - SSL無法為其設定裝置證書的信任點的名稱。建議的操作 :解決故障報告原因所指示的問題。確保指定的信任點已註冊並具有裝置證書。確保裝置證書 有效。如果需要,重新註冊信任點。

相關資訊

- 如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書
- <u>安全產品現場通知</u>
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems