Esempio di installazione manuale di certificati di terze parti per ASA 7.x da utilizzare con la configurazione di WebVPN

Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Convenzioni Configurazione Passaggio 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati Passaggio 2. Generare la coppia di chiavi RSA Passaggio 3. Creazione del punto di fiducia Passaggio 4. Generare la registrazione del certificato Passaggio 5. Autenticazione del trust point Passaggio 6. Installare il certificato Passaggio 7. Configurare WebVPN per l'utilizzo del certificato appena installato Verifica Sostituisci certificato autofirmato da ASA Visualizza certificati installati Verifica del certificato installato per WebVPN con un browser Procedura per il rinnovo del certificato SSL Comandi Risoluzione dei problemi Informazioni correlate

Introduzione

In questo esempio di configurazione viene descritto come installare manualmente un certificato digitale di un fornitore terzo sull'appliance ASA per l'utilizzo con WebVPN. Nell'esempio viene utilizzato un certificato di prova della versione. Ogni passo contiene la procedura dell'applicazione ASDM e un esempio di CLI.

Prerequisiti

Requisiti

Per questo documento è necessario disporre dell'accesso a un'Autorità di certificazione (CA) per la registrazione dei certificati. I fornitori di CA di terze parti supportati sono Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA e VeriSign.

Componenti usati

Questo documento utilizza un'appliance ASA 5510 con software versione 7.2(1) e ASDM versione 5.2(1). Tuttavia, le procedure descritte in questo documento possono essere usate su qualsiasi appliance ASA con versione 7.x compatibile con ASDM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

Per installare un certificato digitale di un fornitore esterno sull'appliance PIX/ASA, attenersi alla seguente procedura:

- 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati.
- 2. Generare la coppia di chiavi RSA.
- 3. Creare il trust point.
- 4. Generare la registrazione certificati.
- 5. Autenticare il trust point.
- 6. Installare il certificato.
- 7. Configurare WebVPN per l'utilizzo del certificato appena installato.

Passaggio 1. Verificare che i valori di Data, Ora e Fuso orario siano accurati

Procedura ASDM

- 1. Fare clic su Configurazione e quindi su Proprietà.
- 2. Espandere Amministrazione periferica e scegliere Orologio.
- 3. Verificare che le informazioni elencate siano corrette.l valori di Data, Ora e Fuso orario devono essere accurati per consentire la corretta convalida del certificato.



Esempio della riga di comando

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

Passaggio 2. Generare la coppia di chiavi RSA

La chiave pubblica RSA generata viene combinata con le informazioni sull'identità dell'ASA per formare una richiesta di certificato PKCS#10. È necessario identificare chiaramente il nome della chiave con il Trustpoint per il quale si crea la coppia di chiavi.

Procedura ASDM

- 1. Fare clic su **Configurazione** e quindi su **Proprietà**.
- 2. Espandere Certificato e scegliere Coppia di chiavi.
- 3. Fare clic su

Add.

2 AL	Certificate		
NAT	Enrolment	Key Pair Name Usage Modulus Siz	e Add
SK VPN	Manage Certificates		Show Details
CSD Manager	Configuration	🖆 Add Key Pair 🔀	Delete
123	Device Access Device Administration	Name: C Use default key name	Refresh
Routing	The DHCh Services DHCh Services DHCh Services DHCh Services DHCh Services DHCh Services	(* my.verisign.key	
Global Objects	Fallover	Size: 1024	
Properties	History Metrics	Usage: C General Purpose C Special	
	P Audt Logging Priority Queue SSL SUNRPC Server TCP Options	Generate Now Cancel Help	

- 4. Immettere il nome della chiave, scegliere le dimensioni del modulo e selezionare il tipo di utilizzo. Nota: La dimensione consigliata per la coppia di chiavi è 1024.
- 5. Fare clic su **Genera**.La coppia di chiavi creata deve essere elencata nella colonna Nome coppia di chiavi.

Esempio della riga di comando

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)#

Passaggio 3. Creazione del punto di fiducia

I punti di fiducia devono dichiarare l'Autorità di certificazione (CA) che verrà utilizzata dall'appliance ASA.

Procedura ASDM

- 1. Fare clic su **Configurazione** e quindi su **Proprietà**.
- 2. Espandere Certificato, quindi TrustPoint.
- 3. Scegliere **Configurazione**, quindi fare clic su **Aggiungi**.

l	Configuration > Properties > Certificate > Trustpoint > Configuration						
	Startup Wizard	Configur	ation				
l	🗈 🚮 AAA Setup	1 . Conf	icure a Certificate Aut				
I	-B Anti-Spoofing	0	igure a certificate Au				
I	🔁 🐻 ARP						
I							
I						[]	
I	E-61 Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add	
I	Authentication						
I	-2 Enrolment					Edit	
I							
I							
I						Delete	
I	E-22 Trustpoint						
I	- So Configuration		15			Request CRL	
I	- in Export						
I							
I	E for Device Access						

- 4. Configurare i seguenti valori: **Nome trust point**: Il nome del trust deve essere rilevante per l'utilizzo previsto. In questo esempio viene utilizzato *my.verisign.trustpoint*.**Coppia di chiavi**: Selezionare la coppia di chiavi generata nel <u>passaggio 2</u>. (*my.verisign.key*)
- 5. Assicurarsi che sia selezionata l'opzione Iscrizione manuale.
- 6. Fare clic su **Parametri certificato**. Verrà visualizzata la finestra di dialogo Parametri certificato.
- 7. Fare clic su **Modifica** e configurare gli attributi elencati nella tabella:Per configurare questi valori, scegliere un valore dall'elenco a discesa Attributo, immettere il valore e fare clic su **Aggiungi**.

			Common Name (CN)	webvpn.cisco.com
Attribute to be Added			Department (OU)	TSWEB
			Company Name (O)	Cisco Systems
bute: Select Attri	oute 💌 📃	Add >>	State (St)	North Carolina
			State (St)	US
e:		Delete	Location (L)	Raleigh
,				
			,	

- 8. Una volta aggiunti i valori appropriati, fare clic su OK.
- Nella finestra di dialogo Parametri certificato immettere il nome di dominio completo nel campo Specifica nome di dominio completo.Questo valore deve essere lo stesso nome di dominio completo utilizzato per il nome comune (CN).

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh	
FQDN C Use FQDN of the device	
Specify FQDN webvpn.cisco.com	
O Use none	
E-mail:	
IP Address:	
Include device serial number	
OK Cancel Help	

- 10. Fare clic su OK.
- 11. Verificare che sia selezionata la coppia di chiavi corretta e fare clic sul pulsante di opzione **Usa registrazione manuale**.
- 12. Fare clic su **OK**, quindi su **Applica**.

Add Trustnoint Co							
Had masepoint co	nfiguration						
Trustpoint Name:	my.verisign.tr	Ispoint					
	1, 3						
🔲 Generate a self	-signed certificat	e on enrol	llment				
If this option is e	anabled, only Key	Pair and (Certificate Param	eters can l	e specified.		
Even line and California	1	. 1		1		1	1
Enroliment Settings	Revocation Ch	eck CRL	. Retrieval Policy	CRL Retr	ieval Method	OCSP Rules	Advanced
Key Pair:	my.verisign.key	•	Show Detail	s	New Key	Pair	
Challenge [_	Confirm Challen	ge			
Password:			Password:	-			
Enrollment Mode							
Enrollment Mode	e inual enrollment tomatic enrollmen						
Enrollment Mode C Use ma C Use au Enrollmer	e inual enroliment tomatic enrolimen nt URL: http	:#			_		
Enrollment Mode C Use ma C Use au Enrollmer Retry Per	e inual enroliment tomatic enrolimen nt URL: http iod: [1	:#	minutes		_		
Enrollment Mode Use ma Use au Enrollmer Retry Per Retry Cor	e inual enrollment tomatic enrollmen nt URL: http iod: [1] unt: [0]	:	minutes (Use 0 to indice	ite unlimiter	I retries)		
Enrollment Mode Use ma Use au Enrollmen Retry Per Retry Col	e inual enroliment tomatic enrolimen nt URL: http iod: 1 unt: 0		minutes (Use 0 to indica	ite unlimiter	d retries) Certificate Pa	rameters	

Esempio della riga di comando

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>
! Defines x.500 distinguished name. ciscoasa(config-ca- trustpoint)#keypair my.verisign.key
<i>! Specifies key pair generated in <u>Step 3</u>.</i> ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

Passaggio 4. Generare la registrazione del certificato

Procedura ASDM

- 1. Fare clic su Configurazione e quindi su Proprietà.
- 2. Espandere Certificato e scegliere Registrazione.
- Verificare che il Trustpoint creato nel passaggio 3 sia selezionato e fare clic su Registra. Verrà visualizzata una finestra di dialogo in cui è elencata la richiesta di registrazione del certificato, definita anche richiesta di firma del certificato.

付 Enrollment Request X To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA. You will need to install the certificate after receiving it. Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: ۰ hvcNAQkCFhtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN AQEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH40WUXbil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA qmoBmSRVnLOqyDtpSlbveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= -End - This line not part of the certificate request---OK.

4. Copiare la richiesta di registrazione PKCS#10 in un file di testo e quindi inviare il CSR al fornitore di terze parti appropriato.Dopo aver ricevuto il CSR, il fornitore di terze parti deve rilasciare un certificato di identità per l'installazione.

Esempio della riga di comando

Nome dispositivo 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
30MXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request --- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

Passaggio 5. Autenticazione del trust point

Dopo aver ricevuto il certificato di identità dal fornitore di terze parti, è possibile procedere con questo passaggio.

Procedura ASDM

- 1. Salvare il certificato di identità nel computer locale.
- 2. Se è stato fornito un certificato con codifica base64 non fornito come file, è necessario copiare il messaggio base64 e incollarlo in un file di testo.
- 3. Rinominare il file con estensione cer.**Nota:** una volta rinominato il file con estensione cer, l'icona del file dovrebbe essere visualizzata come certificato.
- 4. Fare doppio clic sul file del certificato. Verrà visualizzata la finestra di dialogo



se nella scheda Generale viene visualizzato il messaggio "*Windows non dispone di informazioni sufficienti per verificare questo certificato*", è necessario ottenere il certificato CA radice o CA intermedia del fornitore di terze parti prima di continuare con questa procedura. Contattare il fornitore di terze parti o l'amministratore della CA per ottenere la CA radice o il certificato della CA intermedia di emissione.

- 5. Fare clic sulla scheda Percorso certificato.
- 6. Fare clic sul certificato CA situato sopra il certificato di identità rilasciato e fare clic su **Visualizza**

Certificate	? ×	1
General Details Certification Path		
Certification path VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA Weisign Trial Secure Server Test CA Webvpn.cisco.com		
	View Certificate	
Certificate status: This certificate is OK.		
	ОК	Vengo

certificato.

no visualizzate informazioni dettagliate sul certificato CA intermedio.**Avviso:** non installare il certificato di identità (dispositivo) in questo passaggio. In questo passaggio vengono aggiunti solo il certificato radice, la radice subordinata o la CA. I certificati di identità (dispositivo) sono installati nel <u>passaggio 6</u>.

7. Fare clic su

Certificate	<u>? ×</u>
General Details Certification Path	1
	·
Show: <a>	
Field	Value
E Version	V3
Serial number	63 b1 a5 cd c5 9f 78 80 1d a0
Signature algorithm	sha1RSA
	Veribign Trial Secure Server Te
	Sunday, February 08, 2015 7:
E Subject	VeriSign Trial Secure Server Te
Public key	RSA (2048 Bits)
1	
E	dit Properties Copy to File
	ОК

Dettagli.

- 8. Fare clic su Copia su file.
- 9. Nell'Esportazione guidata certificati fare clic su Avanti.
- Nella finestra di dialogo Formato file di esportazione, fate clic sul pulsante di scelta X.509 (.CER) con codifica Base 64 e fate clic su Avanti.

ertificate Export Wizard	
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C 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)	
\square 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 > Ca	ancel

- 11. Immettere il nome file e il percorso in cui si desidera salvare il certificato CA.
- 12. Fare clic su **Avanti** e quindi su **Fine**.

Specify the name of the file you want to export	
File name:	
c:\introotca Bri	owse
< Back Next >	Cancel

- 13. Fare clic su **OK** nella finestra di dialogo Esportazione riuscita.
- 14. Selezionare il percorso in cui è stato salvato il certificato CA.
- 15. Aprire il file con un editor di testo, ad esempio Blocco note. Fate clic con il pulsante destro del mouse sul file e scegliete Invia a > Blocco note. Il messaggio con codifica base64 dovrebbe essere simile al certificato in questa immagine:

File Edit Format View Help

----BEGIN CERTIFICATE--MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzELMÁ&GA1UÉBhMCVVMxFzAVBqNVBÁoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3R]c3RjYSAoYykwNTEtMCsGA1UEAXMkVmVyaVNpZ24gVHJpYWwqU2VjdXJ1FN] cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIZNTk1OVowgZ4x CZAJBGNVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q21zY28qU31zdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BqNVBAsUMVR1cm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuvAKuJ7cnoxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAWCWYDVR0PBAQDAqWqMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PwYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQŪFBzABhhhodHRwoi8vb2NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9Tv]JTZWN1cmUtyW]hLnZ]cm]zaWduLmNvbS9Tv[JUcm]hbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMAcGBSsOAwIaBBRLa7kolgYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTqIorIClawwwx+RHCcTqIrlzf0vfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvlXzŽjiOJ51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja |idT1FmBvf02qaZS6S40= ----END CERTIFICATE-----

- 16. In ASDM, fare clic su **Configurazione**, quindi su **Proprietà.**
- 17. Espandere Certificato e scegliere Autenticazione.
- 18. Fare clic sul pulsante di opzione **Immettere il testo del certificato in formato esadecimale o base64**.
- 19. Incollare il certificato CA in formato base64 dall'editor di testo nell'area di testo.
- 20. Fare clic su

Autentica.

Configuration > Properties > C	ertificate > Authentication
Startup Wizard	Authentication
E 🔂 AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a
Anti-Spoofing	trustopint and installed on the device.
E-B ARP	
Auto Update	Trustopint Name: Edit New
Client Update	my vensign ruspo
E S Certificate	
Authentication	Fingerprint (optional):
Enrolment	
Import Certificate	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.
- Seg Key Pair	
Manage Certificates	Certificate Text
E-62 Trustpoint	Churat from a flat
Configuration	so import from a rile.
Export	
import	(e) Enter the certificate text in hexadecimal or base64 format:
Device Access	A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJIIFNIcnZiciBUZXN0IFJvb3
Device Administration	ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/5
B DHCP Services	Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BA//SU6E
High Augilahithu and Saal	Al9TXvRlcD5q0mB+nyK9fB2aBzOlaiHSlfWzAJeQjuqA+Q93jNew+peuj4Ahc
Felower	n/KK/+1Yv61w3+7g6ukFMARVBNg=
Fragment	END CERTIFICATE
History Matrice	
	🔂 Authentication Successful
Priority Queue	
- R SSL	 The trustpoint my.verisign.truspoint has been authenticated.
SUNRPC Server	Y
- Detions	
- Timeouts	
	OK
E of wccp	
-	

21. Fare clic su OK. Esempio della riga di comando

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
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
$\verb"jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw"$
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3N1cyBPbmx5LiAgTm8gYXNzdXJhbmN1cy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFR1c3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZ1cmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD

DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu wElv6IJ/ DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6 1BBD6Zqk d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45 1P4qoyqS E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6507bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBz0i8vd3d3LnZ1cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAXMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQQGC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YR0iL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
<pre>wElv6IJ/ DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6 1BBD6Zqk d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45 1P4qoyqS E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZ0 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu LmNv5S9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECC0167bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU</pre>
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6 1BBD6Zqk d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45 1P4qoyqS E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIE1uYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCo167bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
1BBD6Zqk d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45 1P4qoyqS E0bdru16quZ+II2cGFAGIoSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3Ln21cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHwjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVU2EXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45 1P4qoyqS E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3Ln21cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQEwJVUZEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UdaxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
1P4qoyqS E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVWYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOFvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUZEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1 D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPv0fGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBz0i8vd3d3LnZ1cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
D/OCCmZO 5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cm1zaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
xjKfV6sb tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCcol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
<pre>tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6 QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi</pre>
QMECAwEA AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
BgpghkgB hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G AlUdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG AlUEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
LmNvbS9j cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD AgEGMB0G A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
AgEGMBUG A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
ALUGDGQWBBRmI06B4DFZ3Sp/qUbFNgIGCCeHWjCBsgYDVR0jBIGqMIGn oYGSpIGP MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
orgspige MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x MDAuBgNV BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
MIGMMQSWCQYDVQQGEWJVUZEXMBUGAIUECHMOVMVYAVNpZ24SIEIUYY4X MDAuBgNV BASTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
MDAUBGNV BASTJOZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
LjEyMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJ1IFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
LJEYMDAG A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1cnZ1ciBUZXN0IFJv b3QgQ0GC ECCo167bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
b3QgQ0GC ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU 6EEzD9oi
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/ SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU 6EEzD9oi
SjzRvY21 Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU 6EEzD9oi
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU 6EEzD9oi
6EEZD90i
02225702
Ai9TXvRIcD5g0mB+nvK9fB2aBz0iaiHSiIWzAJe0jugA+093jNew+peu
i4AhdvGN
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)#

Passaggio 6. Installare il certificato

Procedura ASDM

Utilizzare il certificato di identità fornito dal fornitore di terze parti per eseguire i seguenti passaggi:

- 1. Fare clic su **Configurazione** e quindi su **Proprietà**.
- 2. Espandere Certificato, quindi scegliere Importa certificato.
- 3. Fare clic sul pulsante di opzione **Immettere il testo del certificato in formato esadecimale o base64** e incollare il certificato di identità base64 nel campo di testo.

Configuration > Properties > C	ertificate > Import Certificate
Startup Wizard	mport Certificate
🖲 🖬 AAA Setup	Install an identity cartificate that was received from a Cartificate Authority (CA) in resource to a menual
- B Anti-Spoofing	errollinet received
🟵 🐻 ARP	en ennen i respisat.
	Trustedirt Manuel
E Certificate	my.vensign truspo Edit New
- Authentication	
- 2 Enrolment	Certificate Text
Import Certificate	C heart from a flat
Key Pair	s importiron a lie.
Manage Certificates	
E-82 Trustpoint	1. Enter the certificate text in nexadecimal or baseb4 format.
Configuration	
- Seport	MS5pdaVueDOV Ko7kupNa OEEBO a DapER AVada a SKEOria AAVVati a v
import	masharvi moori shozi moneque baseggeberni virish oga intervient mitkisiSPDn EGCROaxeSvS+v9ncPLsDNm8aTPAGRvdbv265LiskOpci Lon:
E Device Access	tFKFFSFbleCK/hh6MaMb40z6kiFlzp/UmtdJDoU3B00U/vm+tg02eTWdz/WE
P-P DHCP Services	0YVvwM3KDQAO6EbAntUoAxovDbJucdxb6ZVTtyevMcgzCkXMHEVxa5/P)
P-B DNS	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4utcGgGZD8ltVGx26b5OWTz8K
High Availability and Scal	8EvHm3grdbOZP+ISMotVVYE+CgfKpZb+CPAqH2Cdpz2pJfjJhl6CS6NM=
Failover	END CERTIFICATE
- K Fragment	
-12 History Metrics	
- TP/HTTPS	🔂 Information
🖲 📲 🔁 P Audit	
E-Cogging	
- Priority Queue	Certificate import succeeded.
SSL .	
SUNRPC Server	
TCP Options	
Timeouts	
UKL Fittering	
A MUCH	
I	

4. Fare clic su Importa e quindi su OK.

Esempio della riga di 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 itselfBEGIN
CERTIFICATE
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMTAw
EydGD31gVGvZdCBQdXJwD3N1CyBPDmx5L1Ag1m8gYXNZdXJhDmN1Cy4x
BASTOVRICMIZIG9MIHVZZSBNCCBOCHRwCZOVL3d3dy52ZXJpC2Inb15j
L3R1C3RJ1SAOYYKWNTETMCSGAIUEAXMKVMVYAVNp224gVHJp1WWgU2VJ
CHZICIBOZANOIENBMB4ADTASMDCYN JAWMDAWMFOADTASMDGWOTIZNTRI OWewshew
2111FD-OU
ALCEBAUN
VENYDIIT

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9ker2jQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+1iIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc21nbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ21mMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9y1DBd8N
7/yW30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
END CERTIFICATE
quit
INFO: Certificate successfully imported
ciscoasa(config)#

Passaggio 7. Configurare WebVPN per l'utilizzo del certificato appena installato

Procedura ASDM

- 1. Fare clic su **Configurazione**, su **Proprietà** e quindi su **SSL**.
- 2. Nell'area Trustpoints selezionare l'interfaccia che verrà utilizzata per terminare le sessioni WebVPN. In questo esempio viene utilizzata l'interfaccia esterna.
- 3. Fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica trust SSL.

Configuration > Properties > S	SL .					
Startup Wizard	SSL					
🕀 🚽 AAA Setup	Configure SSI parameters. These parameters affect both ASDM and Méh///EN access					
-3 Anti-Spoofing	Contrigure SSL parameters. These parameters affect our ASDM and Web YPH access.					
ti-🐻 ARP	Server SSL Version: Any Client SSL Version: Any					
	Encryption					
	and poor					
🕀 🔂 Certificate	Available Algorithms Add >> Active Algorithms Move Up					
E Device Access	30ES-SHA1					
1 Device Administration	file Edit SSL Trustopint					
E DHCP Services						
E-B DNS	Specify an enrolled trustpoint to be used for SSL authentication on the outside interface. To enroll a trustpoint					
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.					
Fallover						
- Fragment						
History Metrics						
HTTP/HTTPS	Interface: outside					
H Audit						
Logging	Enroled Trustpoint: my.verisign.trustp					
Priority Queue						
SUNKPC Server						
Threats	OK Cancel nep					
UNI LIEL Ellering						
	Trustpoints					
Specify which enrolled trustpoints, 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					
	Falback Trustpoint					
	Interface Trustpoint Edit					
	management					
	o i faide mu variation trustopiet					
	a de la companya de la					
I I I						

- 4. Dall'elenco a discesa Trustpoint registrato scegliere il trust point creato nel passaggio 3.
- 5. Fare clic su OK, quindi su Applica.

Il nuovo certificato dovrebbe essere ora utilizzato per tutte le sessioni WebVPN che terminano sull'interfaccia specificata. Per informazioni su come verificare la riuscita dell'installazione, vedere la sezione Verifica di questo documento.

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

Verifica

In questa sezione viene descritto come verificare che l'installazione del certificato del fornitore di terze parti sia stata completata correttamente.

Sostituisci certificato autofirmato da ASA

In questa sezione viene descritto come sostituire il certificato autofirmato installato dall'appliance ASA.

- 1. Inviare una richiesta di firma del certificato a Verisign.Dopo aver ricevuto il certificato richiesto da Verisign, è possibile installarlo direttamente nello stesso trust point.
- 2. Digitare il comando: crypto ca enroll VerisignViene chiesto di rispondere alle domande.
- 3. In Visualizza richiesta certificato al terminale, immettere **yes** e inviare l'output a Verisign.
- 4. Dopo aver ottenuto il nuovo certificato, digitare questo comando: crypto ca importa certificato di Verisign

Visualizza certificati installati

Procedura ASDM

- 1. Fare clic su **Configurazione** e quindi su **Proprietà**.
- 2. Espandere **Certificato** e scegliere **Gestisci certificati**.Il certificato CA utilizzato per l'autenticazione Trustpoint e il certificato di identità rilasciato dal fornitore di terze parti devono essere visualizzati nell'area Gestisci

Configuration > Properties > Ce	rtificate > Manage Cei	rtificates				
Startup Wizard	Manage Certificates					
🕀 🚮 AAA Setup	Manage the Certifica	tes associate	stripots ut differ b			
-B Anti-Spoofing	manage are contined	100 00000000	or the first of output into .			
E-B ARP			[[]	1
- Auto Update	Subject	Туре	Trustpoint	Status	Usage	Add
Client Update	VeriSign Trial	CA	my.verisign.tru	Available	General Purpo	
□-III Certificate	webvpn.cisco	Identity	my.verisign.tru	Available	General Purpo	Show Details
Authentication						
- an Enrolment						Refresh
Import Certificate						
Seg Key Par						Dalata
4 Manage Certificates						Delete
Configuration						
Configuration						

Esempio della riga di comando

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.

Verifica del certificato installato per WebVPN con un browser

Per verificare che WebVPN utilizzi il nuovo certificato, eseguire la procedura seguente:

- 1. Connettersi all'interfaccia WebVPN tramite un browser Web. Utilizzare https:// insieme al nome di dominio completo utilizzato per richiedere il certificato, ad esempio https://webvpn.cisco.com.Se si riceve uno di questi avvisi di protezione, eseguire la procedura corrispondente: Il nome del certificato di protezione non è valido o non corrisponde al nome del sitoVerificare di aver utilizzato il nome FQDN/CN corretto per connettersi all'interfaccia WebVPN dell'ASA. È necessario utilizzare l'FQDN/CN definito guando è stato richiesto il certificato di identità. È possibile utilizzare il comando show crypto ca certificates trustpointname per verificare i certificati FQDN/CN.Il certificato di protezione è stato emesso da una società che si è scelto di non considerare attendibile...Completare questa procedura per installare il certificato radice del fornitore di terze parti nel browser Web:Nella finestra di dialogo Avviso di protezione fare clic su Visualizza certificato. Nella finestra di dialogo Certificato fare clic sulla scheda Percorso certificato. Selezionare il certificato CA sopra il certificato di identità rilasciato e fare clic su Visualizza certificato. Fare clic su Installa certificato.Nella finestra di dialogo Installazione guidata certificato fare clic su Avanti.Selezionare il pulsante di opzione Seleziona automaticamente l'archivio certificati in base al tipo di certificato, fare clic su Avanti e quindi su Fine. Fare clic su Sì quando viene visualizzata la richiesta di conferma dell'installazione del certificato. Al prompt Importazione completata, fare clic su OK e quindi su Sì. Nota: poiché in questo esempio viene utilizzato il certificato di prova Verisign, è necessario installare il certificato radice CA di prova Verisign per evitare errori di verifica durante la connessione degli utenti.
- 2. Fare doppio clic sull'icona del lucchetto visualizzata nell'angolo inferiore destro della pagina di accesso di WebVPN.Verranno visualizzate le informazioni sul certificato installato.
- 3. Esaminare il contenuto per verificare che corrisponda al certificato del fornitore di terze

Certificate	<u>? ×</u>
General Details Certification Path	
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.	
	-
Issued to: webvpn.cisco.com	
Issued by: VeriSian Trial Secure Server Test CA	
Valid from 8/14/2007 to 8/29/2007	
Install Certificate Issuer Statemer	nt
	, ,
	•

Procedura per il rinnovo del certificato SSL

Per rinnovare il certificato SSL, completare la procedura seguente:

- 1. Selezionare il trust point da rinnovare.
- 2. Scegliere **Registra**.Viene visualizzato questo messaggio:*Se la registrazione ha esito positivo, il certificato corrente verrà sostituito con quelli nuovi. Continuare?*
- 3. Scegliere sì.Questo genererà una nuova RSI.
- 4. Inviare il CSR alla CA e quindi importare il nuovo certificato di identità quando viene restituito.
- 5. Rimuovere e riapplicare il trust point all'interfaccia esterna.

Comandi

Sull'appliance ASA, è possibile utilizzare diversi comandi show dalla riga di comando per verificare lo stato di un certificato.

- show crypto ca trustpoint: visualizza i trust point configurati.
- show crypto ca certificate: visualizza tutti i certificati installati nel sistema.
- **show crypto ca crls**: visualizza gli elenchi di revoche di certificati (CRL) memorizzati nella cache.
- show crypto key mypubkey rsa: visualizza tutte le coppie di chiavi crittografiche generate.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Di seguito sono riportati alcuni possibili errori:

- % avviso: Certificato CA non trovato. I certificati importati potrebbero non essere usable.INFO: Importazione del certificato completatall certificato CA non è stato autenticato correttamente. Per verificare che il certificato CA sia stato installato, utilizzare il comando show crypto ca certificate trustpointname. Cercare la riga che inizia con il certificato CA. Se il certificato CA è installato, verificare che faccia riferimento al trust point corretto.
- ERRORE: Impossibile analizzare o verificare il certificato importatoQuesto errore può verificarsi quando si installa il certificato di identità e non si dispone del certificato CA intermedio o radice corretto autenticato con il trust point associato. È necessario rimuovere e rieseguire l'autenticazione con il certificato CA intermedio o radice corretto. Contattare il fornitore di terze parti per verificare di aver ricevuto il certificato CA corretto.
- Il certificato non contiene la chiave pubblica genericaÈpossibile che questo errore si verifichi quando si tenta di installare il certificato di identità nel punto di attendibilità errato. Si sta tentando di installare un certificato di identità non valido oppure la coppia di chiavi associata al trust point non corrisponde alla chiave pubblica contenuta nel certificato di identità. Utilizzare il comando show crypto ca certificates trustpointname per verificare che il certificato di identità sia stato installato nel trust point corretto. Cercare la riga che indica i trust point associati: Se è elencato un trust point errato, utilizzare le procedure descritte in questo documento per rimuovere e reinstallare il trust point appropriato. Verificare inoltre che la coppia di chiavi non sia cambiata dopo la generazione del CSR.
- Messaggio di errore: %PIX|ASA-3-717023 Impossibile impostare il certificato del dispositivo per il trust point [nome trust]Questo messaggio viene visualizzato quando si verifica un errore durante l'impostazione di un certificato di dispositivo per il trust point specificato al fine di autenticare la connessione SSL. Quando viene attivata la connessione SSL, viene eseguito un tentativo di impostare il certificato del dispositivo che verrà utilizzato. Se si verifica un errore, viene registrato un messaggio di errore che include il trust point configurato da utilizzare per caricare il certificato del dispositivo e la causa dell'errore.*nome trust point: nome del trust point per il quale SSL non è riuscito a impostare un certificato di dispositivo.*Azione consigliata: Risolvere il problema indicato dal motivo segnalato per l'errore.Verificare che il trust point specificato sia registrato e disponga di un certificato di dispositivo.Verificare che il certificato del dispositivo sia valido.Se necessario, registrare nuovamente il trust point.

Informazioni correlate

• Come ottenere un certificato digitale da una CA di Microsoft Windows utilizzando ASDM su

un'appliance ASA

- Avvisi sui prodotti per la sicurezza
- RFC (Requests for Comments)
- Documentazione e supporto tecnico Cisco Systems