# ASA 8.x: Rinnovare e installare il certificato SSL con ASDM

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Procedura Verifica Risoluzione dei problemi Come copiare i certificati SSL da un'appliance ASA a un'altra Informazioni correlate

# **Introduzione**

La procedura illustrata in questo documento è un esempio e può essere utilizzata come riferimento con qualsiasi fornitore di certificati o con il proprio server di certificazione radice. A volte, il fornitore del certificato richiede requisiti speciali per i parametri del certificato, ma questo documento illustra la procedura generale necessaria per rinnovare un certificato SSL e installarlo su un'appliance ASA che usa il software 8.0.

# **Prerequisiti**

### **Requisiti**

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Questa procedura è relativa alle versioni 8.x di ASA con ASDM versione 6.0(2) o successive.

La procedura illustrata in questo documento si basa su una configurazione valida con un certificato installato e utilizzato per l'accesso VPN SSL. Questa procedura non influisce sulla rete finché il certificato corrente non viene eliminato. Questa procedura descrive in modo dettagliato come emettere un nuovo CSR per un certificato corrente con lo stesso certificato radice che ha emesso la CA radice originale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. 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>

### **Procedura**

Attenersi alla seguente procedura:

1. Selezionare il certificato da rinnovare in Configurazione > Gestione dispositivi > Certificati di identità e quindi fare clic su **Aggiungi.Figura 1** 

🔂 Cisco ASDM 6.1 for ASA - 172	2.16.242.232		
<u>File Mew Tools Wigards Window</u>	w Help	Look For:	©
🚮 Home 🦓 Configuration 🔯 M	kontoring 🔚 Sava 🔇 Refresh 🔇 Back 🕥 F	nward 🦻 Help	CISCO
Device Management 🗇 🕀 🗵	Configuration > Device Management > Certification	te Monogement > Identity Certificates	
H Management: Access System Image/Configuration High Availability Caging Carthicste Management Carthicste Management Carthicstes Management Carthicstes Management Carthicstes Accentificates Action Carthicstes Action Carthiology Action Carthiology Acti	Issued To     Issued By       [Cm=*spin1.com]     [Cm=MS-CA]   Identity certificate can be used to authenticate SSL, to make such configuration.	Espiry Date 00:03:16 UTC Mar 11 2009 such as ASDM, access to the security applianc	Usage Add Centeral Purpose Show Details Delete Export Bristal Refresh
🔏 Device Setup			
📆 Fyrovaal			
Remote Access VPN			
🙀 Site-to-Site VPN			
Device Management			
?		Apply Reset	
Device configuration refreshed successfu	ily.	tiscol 15	📷 🌆 📊 🔒 8/29/08 8:52:53 PM UTC

2. In Aggiungi certificato di identità selezionare il pulsante di opzione Aggiungi nuovo certificato di identità e scegliere la coppia di chiavi dal menu a discesa.Nota: si consiglia di non utilizzare <Default-RSA-Key> perché se si rigenera la chiave SSH, il certificato viene invalidato. Se non si dispone di una chiave RSA, completare i passaggi a e b. In caso contrario, passare al punto 3.Figura 2

🖆 Add Identity Certificat	e	<b>X</b>
<ul> <li>Import the identity certif</li> </ul>	icate from a file:	
Decryption Passphrase:		
File to Import From:		Browse
<ul> <li>Add a new identity certif</li> </ul>	icate:	
Key Pair:	CertKey	Show New
Certificate Subject DN:	ASA5540.company.com	Select
🔲 Generate self-signed	certificate	
Act as local certif	icate authority and issue dynamic ce	ertificates to TLS-Proxy
		Advanced
Add Certifi	cate Cancel	Help

(Facoltativo) Completare questi passaggi se non è ancora stata configurata una chiave RSA, in caso contrario andare al passaggio 3.Fare clic su **Nuovo...**Immettere il nome della coppia di chiavi nel campo **Immettere il nuovo nome della coppia di chiavi** e fare clic su **Genera** 

🕵 Add K	ey Pair	×
Name:	🚫 Use default key pair name	
	Enter new key pair name: Certkey	]
Size:	1024	-
Usage:	⊙ General purpose ○ Special	
G	ienerate Now Cancel Help	

ora.Figura 3

- 3. Fare clic su Seleziona.
- 4. Immettere gli attributi del certificato appropriati, come mostrato nella Figura 4. Una volta completato, fare clic su OK. Fare quindi clic su Aggiungi certificato.Figura 4

🖆 Certific	ate Su	ıbject DN				×
DN A Attr Valu	attribute ribute: ue:	to be Added Common Name (CN) Common Name (CN) Department (OU) Company Name (O) Country (C) State (St) Location (L) Email Address (EA)	Add>> Delete	Attribute Common Name (CN) Department (OU) Company Name (O) Country (C) State (St)	Value ASA5540.comp LAB Cisco Systems US CA	
		ОК	Cancel	Help		

Output CLI:

crypto ca trustpoint ASDM_TrustPoint0
keypair CertKey
id-usage ssl-ipsec
fqdn 5540-uwe
<pre>subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA</pre>
enrollment terminal
crypto ca enroll ASDM_TrustPoint0

5. Nella finestra popup **Richiesta certificato di identità**, salvare la richiesta di firma del certificato (CSR) in un file di testo e fare clic su **OK.Figura 5** 

🖆 Identity Certificate Request 🛛 🛛 🔀				
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.				
You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.				
Save CSR to file: C:\Certificates\ASACertCSR.txt Browse				
OK Cancel Help				

6. (Facoltativo) Verificare in ASDM che il CSR sia in sospeso, come mostrato nella Figura 6.**Figura 6** 

🕵 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
<u>File View Tools Wigards Window</u>	v ∐elp		Look Far:	Go	duala
A Home Sa Configuration 🔯 Mo	onitoring 🔲 Save 🙉 Refresh	Back C Forward	Help		CISCO
Device Management	Configuration > Device Manag	ement > Certificate Manager	ment > Identity Certificates		
🖶 🧬 Management Access					_
🖶 🥵 System Image/Configuration					
🖶 🤐 High Availability	Issued To	Issued By	Expiry Date Double 44 UTC May 44 CODD	Usage Concert Discourse	Add
E 📆 Users(AAA	[ASA5540.company.com]	[Not Available]	Pending	Unknown	. Show Details
🖶 🛃 Certificate Management					Delete
CA Certificates					Evrort
B 🗗 DHCP					espen
Advanced					Instal
~ ~					Refresh
	Identity certificate can be used to make such configuration	to authenticate SSL, such as ASD	M, access to the security appliance	en a given interface. You can go	to <u>59, Settinos</u>
	to make such configuration				
💑 Device Setup					
📆 Firovali					
Remote Access VPN					
🙀 Ske-to-Site VPN					
Device Management					
20			Reset		
Configuration changes saved successfully	n		ciscol 15	🗟 🛃 🚹 🛛 🔒 🕸	29/08 9:56:23 PM UTC

- 7. Inviare la richiesta di certificato all'amministratore del certificato che emette il certificato sul server. A tale scopo, è possibile utilizzare un'interfaccia Web, un messaggio di posta elettronica oppure accedere direttamente al server CA radice per l'elaborazione dei certificati.
- 8. Completare questa procedura per installare il certificato rinnovato.Selezionare la richiesta di certificato in sospeso in Configurazione > Gestione dispositivi > Certificati di identità, come mostrato nella Figura 6, e fare clic su Installa.Nella finestra Installa certificato di identità, selezionare il pulsante di opzione Incolla i dati del certificato in formato base 64 e fare clic su Installa certificato.Nota: in alternativa, se il certificato viene emesso in un file con estensione cer anziché in un file di testo o in un messaggio di posta elettronica, è anche possibile selezionare Installa da un file, individuare il file appropriato nel PC, fare clic su Installa file di certificato ID e quindi su Installa certificato.Figura 7

🖆 Install Identity certificate	×
Identity Certificate	_
O Install from a file: Browse	
<ul> <li>Paste the certificate data in base-64 format:</li> </ul>	
Ng9SqvsXWWkJmS8ss9Qvz5D+K2uSLPcEAuuT7JhUVC1jbTZh1GLpqBheEeMk/8jY fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== END CERTIFICATE	
Install Certificate Cancel Help	

#### Output CLI:

#### crypto ca import ASDM\_TrustPoint0 certificate

 $\tt WIID2DCCAsCgAwIBAgIKYb9 wewAAAAAAJzANBgkqhkiG9 w0 BAQUFADAQMQ$ 

!--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. Verrà visualizzata una finestra che conferma l'installazione del certificato. Fare clic su "OK"

🕵 Informa	tion	×
<b>i</b>	Certificate import succeeded.	
	OK	

per confermare.Figura 8

10. Assicurarsi che il nuovo certificato venga visualizzato in Certificati di identità. Figura 9

🕵 Cisco ASDM 6.1 for ASA - 172	.16.242.232					
<u>File Yew Tools Wigards Window</u>	v Help			Look Far:		50
🐴 Home 🙈 Configuration 🔯 M	onitoring 🔲 Sava 🔇 Refi	resh 🙆 Back 🕥	Forward 🦻 Help			cisco
Device Management 3 4 X	Configuration > Device Ma	nagement > Certific	ate Management >	Identity Certificate		
E Management Access						
🖶 🎒 System Image/Configuration						
🕀 🤐 High Availability	Issued To	Issued By	Expire	/ Date	Usage	Add
H 🙀 Users(AAA	[cr=A5A5540.company.co	m [cn=NS-CA]	22:49:	31 UTC Aug 29 2009	General Purpose	. Show Details
😑 🛃 Certificate Management						Delete
- An Certificates						
B 💕 DHCP						Estrer
Advanced						Instal
						Refresh
	Identity certificate can be	used to authenticate SS	L, such as ASDM, acces	s to the security applie	nce on a given interface. You can	go to <u>55. Settinos</u>
	to make such configuration	h				
9.0.1.0.						
Device Setup						
📆 Firoval						
Remote Access VPN						
🔗 Site-to-Site VPN						
Device Management						
\$			Apply	Reset		
Configuration changes saved successfully	r.		cisco 1	15	B 🗟 🖬 🔒	8/29/08 10:05:53 PM UTC

11. Completare questa procedura per associare il nuovo certificato all'interfaccia:Scegliere Configurazione > Gestione dispositivi > Avanzate > Impostazioni SSL, come mostrato nella Figura 10.Selezionare l'interfaccia in Certificati e fare clic su Modifica.Figura 10

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
<u>File View Tools Wizards Window</u>	v Help		Look Par:	G	
🚮 Home 🦓 Configuration 📴 M	onitoring 🔚 Sava 🔇 Re	ifresh 🔇 Back 🕥 Forward 🐐	Help		cisco
Device Management 🗗 🕀 🔀	Configuration > Device M	lanagement > Advanced > SSL Se	ttings		
Management Access     System Image/Configuration     High Availability     Logging     Desrs/AAA     Desrs/AAA     Desrs/AAA     Defice     Defice     Ackanced     Management     St. Certificates     Advanced     Management     St. Certificates     Management     M	Configure SSL parameters. 1 Server SSL Version: Any Encryption Available Algorithms RC Certificates Specify which certificates, associated with a certificates instele outside	ihese parameters affect both ASDM an Client 59, Version: / 4405 5:9HAL if any, should be used for SSL authent to of their own. Trustpoint [cr-4, ypn].con].[cr-4]	d SSL VFN access. my V dd >>	trms RC4-SHA1 AES128-SHA1 AES256-SHA1 3DE5-SHA1 3DE5-SHA1 Fallback certificate will be used on inte	Move Up : : Move Down
Bevice Setup     Device Setup     Friewal     Remote Access VPN     Sterto Ste VPN     Device Management	Falback Certificate: N	re -	Apply Reset		
			Li a lie		
Configuration changes saved successfully	6		ciscol 15	💽 🔐 🚮 🛛 付 🕅	29/06 10:08:53 PM DTC

- 12. Scegliere il nuovo certificato dal menu a discesa, fare clic su OK, quindi su Applica. ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal
  - ssl trust-point ASDM\_TrustPoint0 outside

#### Figura 11

🖆 Select SSL Certificate 🛛 🛛 🔀					
Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.					
Interface:	outside				
Primary Enrolled Certificate:	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, 💌				
Load Balancing Enrolled Certificate:	None [cn=*.vpn1.com]:[cn=MS-CA]: 611f863000000000026				
OK Cancer Heip					

13. Salvare la configurazione in ASDM o nella CLI.

## **Verifica**

Èpossibile usare l'interfaccia CLI per verificare che il nuovo certificato sia installato correttamente sull'ASA, come mostrato nell'output di esempio:

```
ASA(config)#show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 61bf707b000000000027
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
cn=MS-CA
Subject Name:
```

cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3basel\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM\_TrustPoint0 CA Certificate Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage: Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---'old' certificate CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006 end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available Certificate Serial Number: 611f86300000000026 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=\*.vpn1.com CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009 Associated Trustpoints: test ASA(config)#

### Risoluzione dei problemi

(Facoltativo) Verificare sulla CLI che all'interfaccia sia applicato il certificato corretto:

ASA(config)**#show running-config ssl** ssl trust-point ASDM\_TrustPoint0 outside *!--- Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN.* ASA(config)**#** 

Come copiare i certificati SSL da un'appliance ASA a un'altra

Questa operazione può essere eseguita se sono state generate chiavi esportabili. È necessario esportare il certificato in un file PKCS. Ciò include l'esportazione di tutte le chiavi associate.

Utilizzare questo comando per esportare il certificato dalla CLI:

ASA(config)#crypto ca export

Nota: passphrase - utilizzata per proteggere il file pkcs12.

Utilizzare questo comando per importare il certificato tramite CLI:

SA(config)#crypto ca import

Nota: questa passphrase deve essere uguale a quella utilizzata per l'esportazione del file.

Questa operazione può essere eseguita anche tramite ASDM per una coppia di failover ASA. Per effettuare questa operazione, effettuare le seguenti operazioni:

- 1. Accedere all'ASA principale tramite ASDM e scegliere **Strumenti—> Configurazione di backup**.
- 2. Èpossibile eseguire il backup di tutti i dati o solo dei certificati.
- 3. In standby, aprire ASDM e scegliere **Strumenti —> Ripristina configurazione**.

# Informazioni correlate

- Pagina di supporto per Cisco Adaptive Security Appliance (ASA)
- Esempio di installazione manuale di certificati di terze parti per ASA 8.x da utilizzare con la configurazione di WebVPN
- Documentazione e supporto tecnico Cisco Systems