

Certificato (importazione/esportazione/generazione di CSR) sui router serie RV160 e RV260

Obiettivo

Lo scopo di questo documento è mostrare come generare una richiesta di firma di certificato (CSR), nonché importare ed esportare certificati sui router serie RV160 e RV260.

Introduzione

I certificati digitali sono importanti nel processo di comunicazione. Fornisce l'identificazione digitale per l'autenticazione. Un certificato digitale include informazioni che identificano un dispositivo o un utente, ad esempio il nome, il numero di serie, la società, il reparto o l'indirizzo IP.

Le autorità di certificazione (CA) sono autorità attendibili che "firmano" i certificati per verificarne l'autenticità, il che garantisce l'identità del dispositivo o dell'utente. Garantisce che il titolare del certificato sia effettivamente chi afferma di essere. Senza un certificato firmato attendibile, i dati potrebbero essere crittografati, ma la persona con cui si sta comunicando potrebbe non essere quella che si ritiene più appropriata. L'autorità di certificazione utilizza l'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) per l'emissione di certificati digitali che utilizzano la crittografia a chiave pubblica o privata per garantire la protezione. Le CA sono responsabili della gestione delle richieste di certificati e dell'emissione di certificati digitali. Alcuni esempi di CA sono: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign e molti altri ancora.

I certificati vengono utilizzati per le connessioni SSL (Secure Sockets Layer), TLS (Transport Layer Security), DTLS (Datagram TLS), ad esempio HTTPS (Hypertext Transfer Protocol) e LDAPS (Secure Lightweight Directory Access Protocol).

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.00.15

Sommario

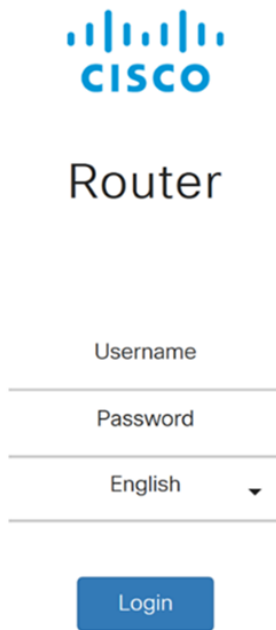
Tramite questo articolo è possibile:

1. [Genera CSR/certificato](#)

2. [Visualizzazione del certificato](#)
3. [Esporta certificato](#)
4. [Importa certificato](#)
5. [Conclusioni](#)

Genera CSR/certificato

Passaggio 1. Accedere alla pagina di configurazione Web.

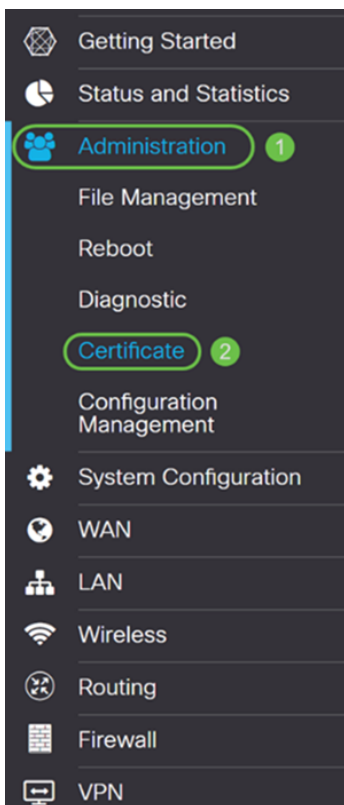


The image shows the Cisco Router login page. At the top is the Cisco logo, which consists of a stylized signal icon above the word "CISCO". Below the logo is the word "Router". There are three input fields: "Username", "Password", and "English" (with a dropdown arrow). Below the input fields is a blue "Login" button.

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Passaggio 2. Passare a **Amministrazione > Certificato**.



Passaggio 3. Nella pagina *Certificato*, fare clic sul pulsante **Genera CSR/Certificato....**

Certificate

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		

Import Certificate... **Generate CSR/Certificate...** Show built-in 3rd party CA Certificates... Select as Primary Certificate...

Passaggio 4. Selezionare il tipo di certificato da generare da una delle seguenti opzioni nell'elenco a discesa.

- **Certificato autofirmato** - Si tratta di un certificato SSL (Secure Sockets Layer) firmato dal proprio creatore. Il certificato è meno attendibile, in quanto non può essere annullato se la chiave privata è compromessa da un utente non autorizzato. Specificare la durata valida in giorni.
- **Certificato CA** - Selezionare questo tipo di certificato per fare in modo che il router agisca come un'autorità di certificazione interna e emetta certificati. Dal punto di vista della sicurezza, è simile a un certificato autofirmato. Può essere utilizzata per OpenVPN.
- **Richiesta di firma del certificato** - Infrastruttura a chiave pubblica (PKI) inviata all'autorità di certificazione per richiedere un certificato di identità digitale. È più sicuro della firma automatica in quanto la chiave privata viene mantenuta segreta. Questa opzione è consigliata.

- **Certificato firmato dall'autorità di certificazione (CA)** - Selezionare questo tipo di certificato e fornire i dettagli necessari per ottenere il certificato firmato dall'autorità di certificazione interna.

In questo esempio verrà selezionata la **richiesta di firma del certificato**.

Generate CSR/Certificate

Type: Certificate Signing Request

Certificate Name: ✘
Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

Passaggio 5. Immettere il *nome del certificato*. In questo esempio, verrà immesso **CertificateTest**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name:

IP Address FQDN Email

Passaggio 6. Nel campo *Nome alternativo soggetto*, **selezionare una delle opzioni seguenti: Indirizzo IP, FQDN** (nome di dominio completo) o **posta elettronica** e quindi immettere il nome appropriato dalla selezione effettuata. Questo campo consente di specificare ulteriori nomi host.

Nell'esempio, verrà selezionato **FQDN** e immesso **ciscoesupport.com**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: ciscoesupport.com

IP Address FQDN Email

Passaggio 7. Selezionare un **paese** dall'elenco a discesa *Nome paese (C)*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text"/>
Locality Name (L):	<input type="text"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Passaggio 8. Inserire il **nome** di una **provincia** o di **uno stato** nel campo *Nome provincia*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Passaggio 9. In *Nome località*, inserire un nome di **città**.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Passaggio 10. Inserire il nome dell'**organizzazione** nel campo *Nome organizzazione*.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text" value="Cisco"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

Passaggio 11. Inserire il nome dell'**unità organizzativa** (ad esempio, Formazione, Supporto e così via).

In questo esempio, verrà inserito **eSupport** come nome dell'unità organizzativa.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	
Email Address (E):	
Key Encryption Length:	2048

Passaggio 12. Inserire un **nome comune**. Il nome di dominio completo del server Web che riceverà il certificato.

Nell'esempio, il nome comune è **ciscosmbsupport.com**.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	
Key Encryption Length:	2048

Passaggio 13. Immettere un **indirizzo di posta elettronica**.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

Passaggio 14. Selezionare **Lunghezza crittografia chiave** dal menu a discesa. Le opzioni sono: **512**, **1024** o **2048**. Maggiore è la dimensione della chiave, più sicuro sarà il certificato. Maggiore è la dimensione della chiave, maggiore sarà il tempo di elaborazione.

Procedure ottimali: Si consiglia di scegliere la lunghezza di crittografia della chiave più elevata, che consente una crittografia più complessa.

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

Passaggio 15. Fare clic su **Genera**.

Generate CSR/Certificate Generate Cancel

Certificate Name:

Subject Alternative Name:
 IP Address FQDN Email

Country Name (C):

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length:

Passaggio 16. Viene visualizzato un popup *Informazioni* con la dicitura "Generazione del certificato completata". messaggio. Fare clic su **OK** per continuare.

Information ✕

Generate certificate successfully!

OK

Passaggio 17. Esportare il CSR dalla *tabella Certificati*.

Certificate Table ▲							
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		

Import Certificate...
Generate CSR/Certificate...
Show built-in 3rd party CA Certificates...
Select as Primary Certificate...

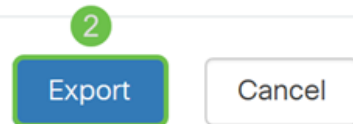
Passaggio 18. Viene visualizzata la finestra *Esporta certificato*. Selezionare **PC** per *Esporta in*, quindi fare clic su **Esporta**.

Export Certificate



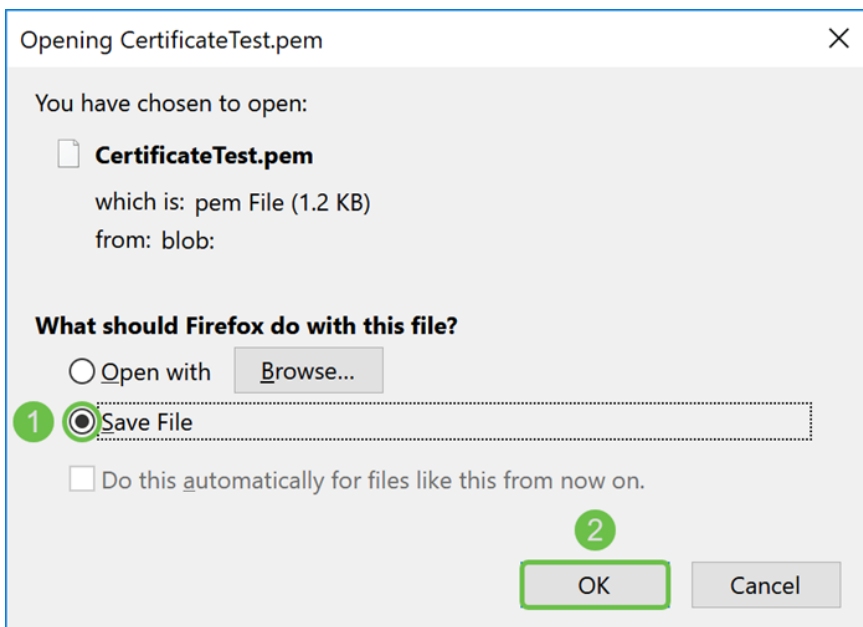
Export as PEM format

Export to:



Passaggio 19. Dovrebbe essere visualizzata un'altra finestra in cui viene chiesto se aprire o salvare il file.

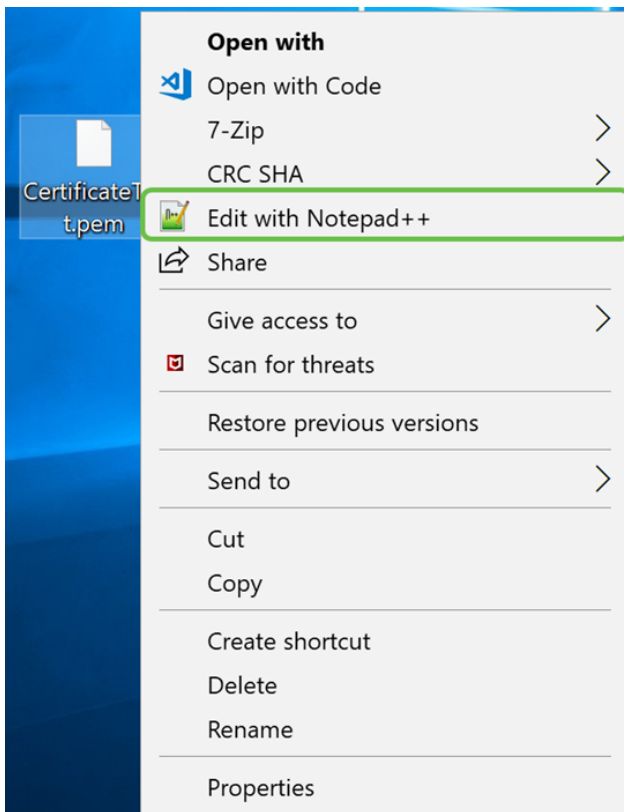
In questo esempio verrà selezionato **Salva file** e quindi fare clic su **OK**.



Passaggio 20. Individuare la posizione in cui è stato salvato il file .pem. **Fare clic con il pulsante destro** del mouse sul file .pem e aprirlo con l'editor di testo preferito.

In questo esempio verrà aperto il file con estensione pem con Blocco note++.

Nota: È possibile aprirlo con il Blocco note.



Passaggio 21. Verificare che **—BEGIN CERTIFICATE REQUEST—** e **—END CERTIFICATE REQUEST—** si trovino su una riga distinta.



Nota: Alcune parti del certificato sono state sfocate.

```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [sfocato] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwWlU2FuIEpvc2UxZDdjAMBgNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY2lzMzY2ZmVzZjZdXBwb3J0 [sfocato]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFoLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [sfocato]
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqgLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAACBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAUw [sfocato].gXg
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY2lzMzY2ZmVzZjZdXBwb3J0 [sfocato]
15 TqFZ2wQx3r29E1SOWU5bmqCj+9IfrsFLR9O9VdAIJXoUP16CJtc4JJy5+XEhYSnu
16 [sfocato]
17 [sfocato]
18 [sfocato]
19 [sfocato]
20 [sfocato]
21 -----END CERTIFICATE REQUEST----- 2
22 [sfocato]
```

Passaggio 22. Quando si dispone del CSR, è necessario andare ai servizi di hosting o a un sito dell'autorità di certificazione (ad esempio, GoDaddy, Verisign, ecc.) e richiedere un certificato. Dopo l'invio, la richiesta verrà inviata al server di certificazione per verificare che non vi siano motivi per non rilasciare il certificato.







Nota: Contattare l'autorità di certificazione o il supporto del sito di hosting se non si è a conoscenza della posizione della richiesta di certificato sul sito.

Passaggio 23. Scaricare il certificato una volta completato. Deve essere un file **.cer** o **.crt**. In questo esempio sono stati forniti entrambi i file.

Name	Date modified	Type	Size
 CertificateTest.cer	4/10/2019 2:03 PM	Security Certificate	2 KB
 CertificateTest.crt	4/10/2019 2:04 PM	Security Certificate	3 KB

Passaggio 24. Tornare alla pagina *Certificato* nel router e importare il file del certificato facendo clic sulla **freccia che punta all'icona del dispositivo**.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		  

Passaggio 25. Nel campo *Nome certificato* immettere il **nome** del **certificato**. Non può avere lo stesso nome della richiesta di firma del certificato. Nella sezione *Carica file di certificato* selezionare **Importa da PC** e fare clic su **Sfoglia...** per caricare il file di certificato.

Import Signed-Certificate

Type: Local Certificate

Certificate Name: 1

Upload Certificate file

2

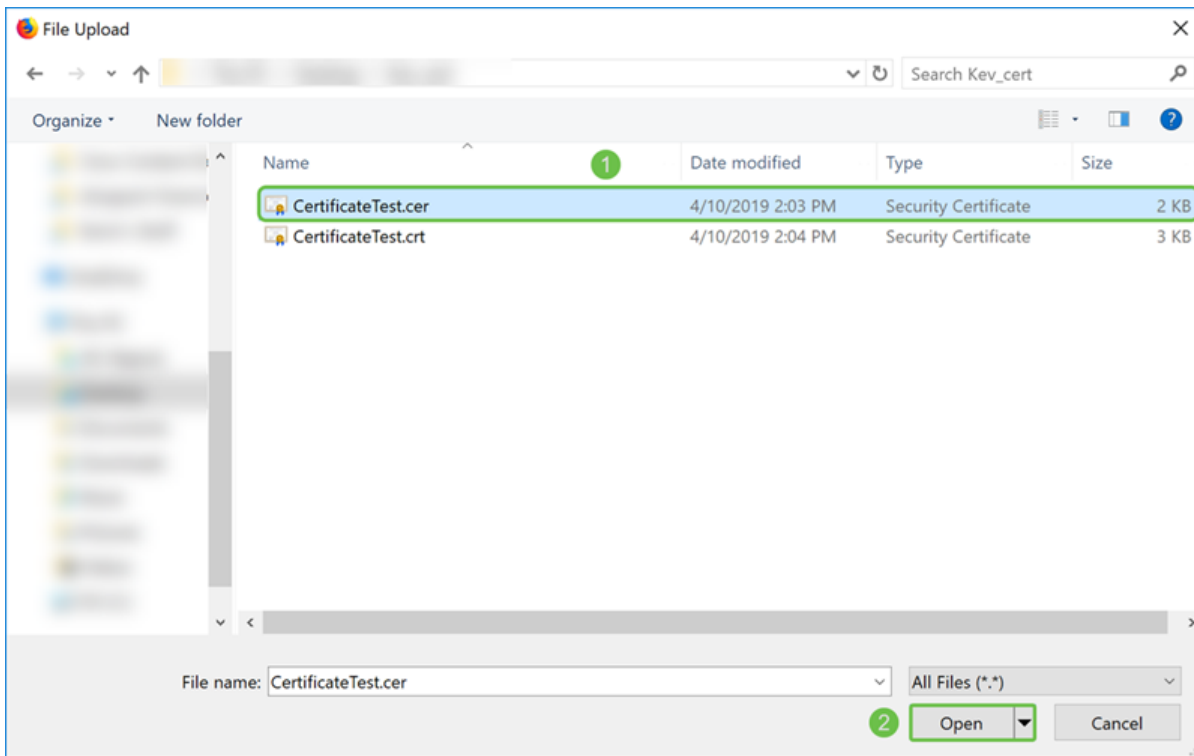
Import from PC

3 No file is selected

Import from USB 

No file is selected

Passaggio 26. Viene visualizzata la finestra *Caricamento file*. Passare alla posizione del file di certificato. Selezionare il file di **certificato** che si desidera caricare e fare clic su **Apri**. Nell'esempio è stato selezionato **CertificateTest.cer**.



Passaggio 27. Fare clic sul pulsante **Upload** per avviare il caricamento del certificato sul router.

Nota: Se viene visualizzato un errore che indica che non è possibile caricare il file con estensione cer, è possibile che il router richieda che il certificato sia incluso in una codifica pem. È necessario convertire la codifica der (estensione file cer) in una codifica pem (estensione file crt).

Import Signed-Certificate ✕

Type: Local Certificate

Certificate Name:

Upload Certificate file

Import from PC

CertificateTest.cer

Import from USB



No file is selected






Passaggio 28. Se l'importazione ha avuto esito positivo, viene visualizzata una finestra di *informazioni* che informa che l'operazione è stata completata. Fare clic su **OK** per continuare.

 Import certificate successfully!

OK

Passaggio 29. È necessario aggiornare il certificato. Dovrebbe essere possibile vedere da chi è stato firmato il certificato. Nell'esempio il certificato è stato firmato da *CiscoTest-DC1-CA*. Per impostare il certificato come principale, selezionarlo utilizzando il pulsante di opzione a sinistra e fare clic sul pulsante **Seleziona come certificato principale**.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action	
<input type="radio"/>	1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input checked="" type="radio"/>	2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		 

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... **Select as Primary Certificate...**

Nota: La modifica del certificato primario potrebbe riportare l'utente a una pagina di avviso. Se si utilizza Firefox e la pagina viene visualizzata come pagina vuota grigia, è necessario regolare alcune configurazioni su Firefox. Questo documento sul wiki di Mozilla fornisce alcune spiegazioni al riguardo: [CA/AddRootToFirefox](#). Per poter visualizzare di nuovo la pagina di avviso, [seguire i passaggi indicati nella pagina di supporto della community Mozilla](#).

Passaggio 30. Nella pagina di avviso di Firefox, fare clic su **Avanzate...** e quindi su **Accetta il rischio e continua** per tornare al router.

Nota: Queste schermate di avvertenze variano da browser a browser ma eseguono le stesse funzioni.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.2.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

Advanced...

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.2.1. The certificate is only valid for ciscoesupport.com.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

Passaggio 31. Nella tabella Certificati, si dovrebbe notare che NETCONF, WebServer, e RESTCONF sono passati al nuovo certificato anziché utilizzare il *certificato predefinito*.

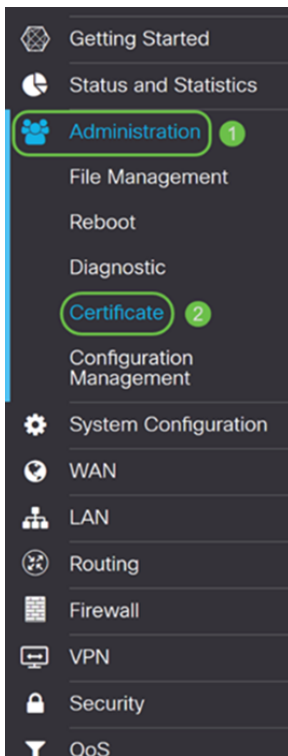
Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

A questo punto è necessario aver installato correttamente un certificato sul router.

Visualizzazione del certificato

Passaggio 1. Se si è usciti dalla pagina *Certificato*, passare ad **Amministrazione > Certificato**.



Passaggio 2. Nella *tabella Certificati* fare clic sull'icona **Dettagli** nella sezione *Dettagli*.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
○ 1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
⦿ 2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Passaggio 3. Viene visualizzata la pagina *Dettagli certificato*. Dovrebbe essere possibile visualizzare tutte le informazioni sul certificato.

Certificate Detail

x

Name: CiscoSMB
Country: US
State Province: CA
Subject Alternative Name: ciscoesupport.com
Subject Alternative Type: Fqdn-Type
Subject-DN: C=US,ST=CA,L=San Jose,O=Cisco,OU=eSupport,CN=ciscosmbsupport.com,emailAddress=k[redacted]@cisco.com
Locality: San Jose
Organization: Cisco
Organization Unit Name: eSupport
Common: ciscosmbsupport.com
Email: k[redacted]@cisco.com
Key Encryption Length: 2048

Close

Passaggio 4. Fare clic sull'icona **Lock** situata sul lato sinistro della barra dell'URL (Uniform Resource Locator).

Nota: I seguenti passaggi sono utilizzati in un browser Firefox.

Cisco RV160 VPN Router

https://192.168.2.1/#/certificate

RV160--router5680AA

cisco(admin) English

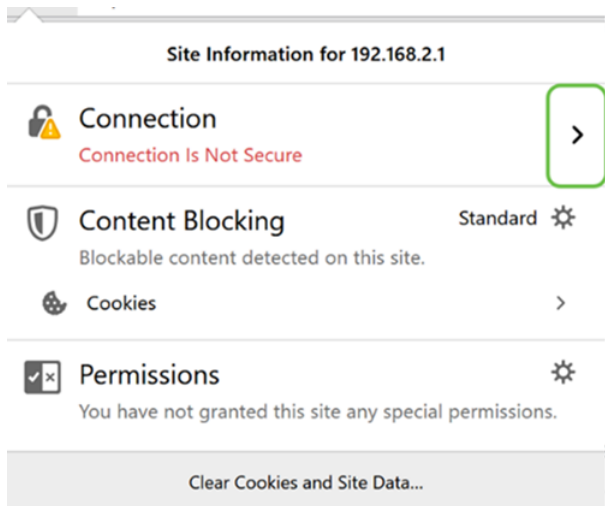
Certificate

Certificate Table

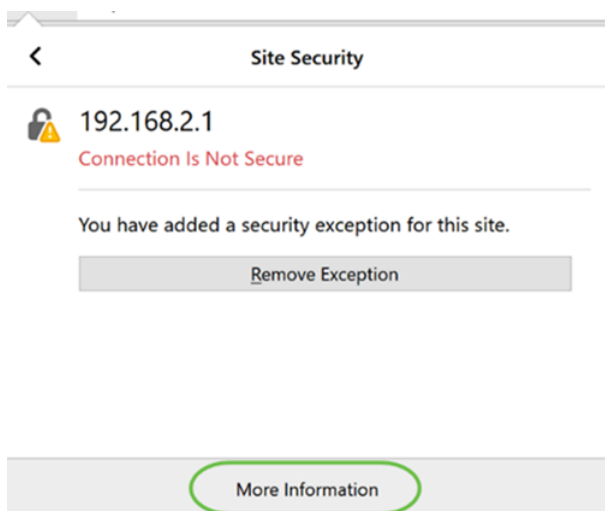
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... Select as Primary Certificate...

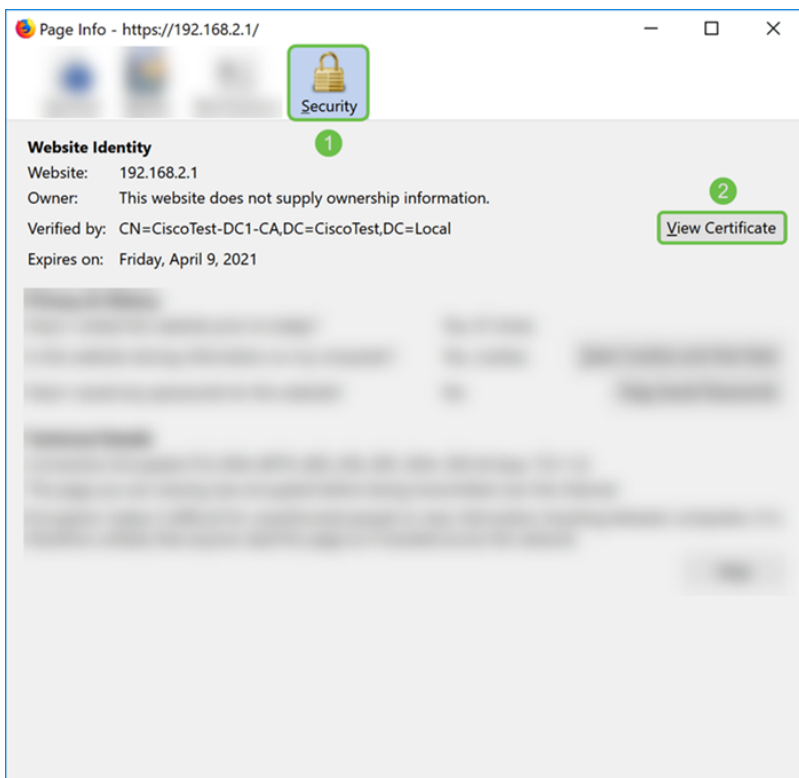
Passaggio 5. Viene visualizzato un elenco a discesa di opzioni. Fare clic sull'icona **Freccia** accanto al campo *Connessione*.



Passaggio 6. Fare clic su **Ulteriori informazioni**.

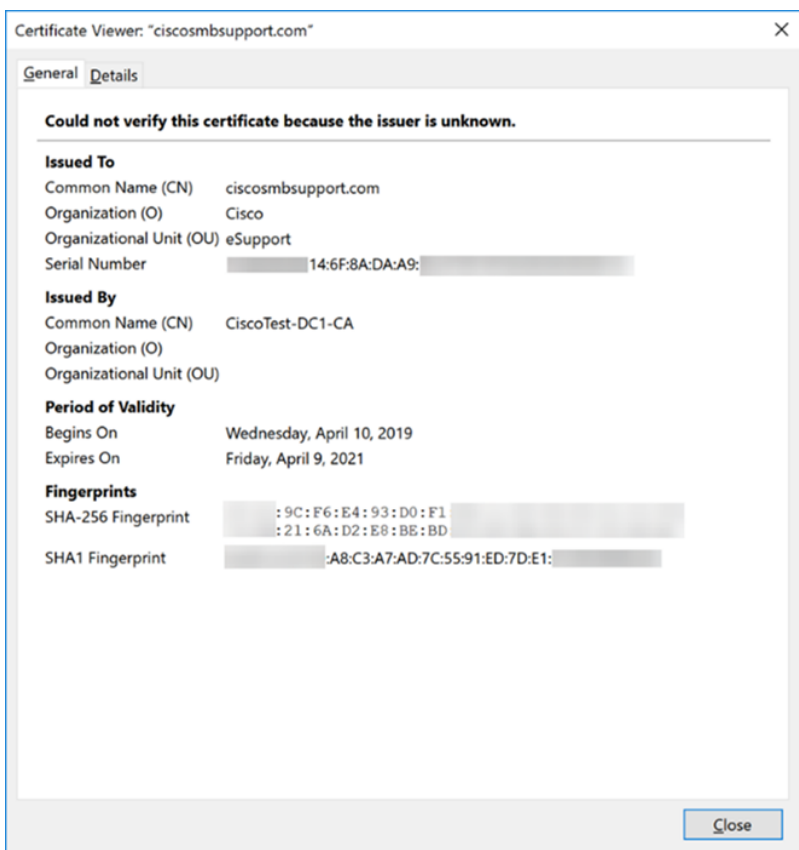


Passaggio 7. Nella finestra *Informazioni pagina*, dovrebbe essere possibile visualizzare una breve informazione sul certificato nella sezione *Identità sito Web*. Verificare di essere nella scheda **Protezione** e quindi fare clic su **Visualizza certificato** per visualizzare ulteriori informazioni sul certificato.



Passaggio 8. Viene visualizzata la pagina *Visualizzatore certificati*. Dovresti essere in grado di vedere tutte le informazioni relative al tuo certificato, al periodo di validità, alle impronte digitali e a chi è stato rilasciato.

Nota: Poiché il certificato è stato rilasciato dal server dei certificati di prova, l'autorità emittente è sconosciuta.



Esportazione del certificato

Per scaricare il certificato e importarlo su un altro router, eseguire la procedura seguente.

Passaggio 1. Nella pagina *Certificato* fare clic sull'icona **Esporta** accanto al certificato che si desidera esportare.

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
○ 1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
⦿ 2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Passaggio 2. Viene visualizzato il *certificato di esportazione*. Selezionare un formato per esportare il certificato. Le opzioni sono:

- **PKCS#12** - Public Key Cryptography Standards (PKCS) #12 è un certificato esportato con estensione .p12. Per crittografare il file e proteggerlo durante l'esportazione, l'importazione e l'eliminazione è necessaria una password.
- **PEM** - La funzionalità di protezione avanzata della posta (PEM, Privacy Enhanced Mail) viene spesso utilizzata per i server Web per la capacità di essere facilmente tradotti in dati leggibili utilizzando un semplice editor di testo come il Blocco note.

Selezionare **Esporta come formato PKCS#12**, immettere una **password** e **confermare la password**. Quindi selezionare **PC** come destinazione *di esportazione*: campo. Fare clic su **Esporta** per avviare l'esportazione del certificato nel computer.

Nota: Memorizzare la password perché verrà utilizzata durante l'importazione in un router.

Export Certificate



1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC USB

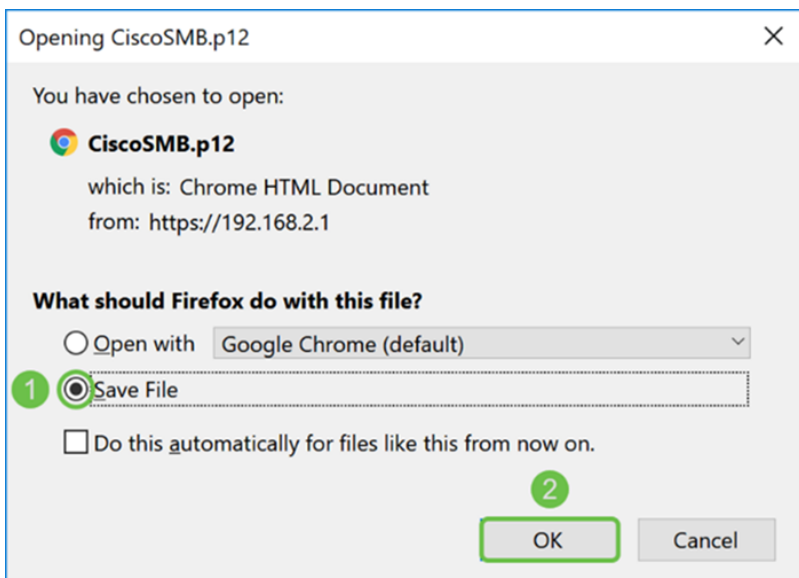


4

Export

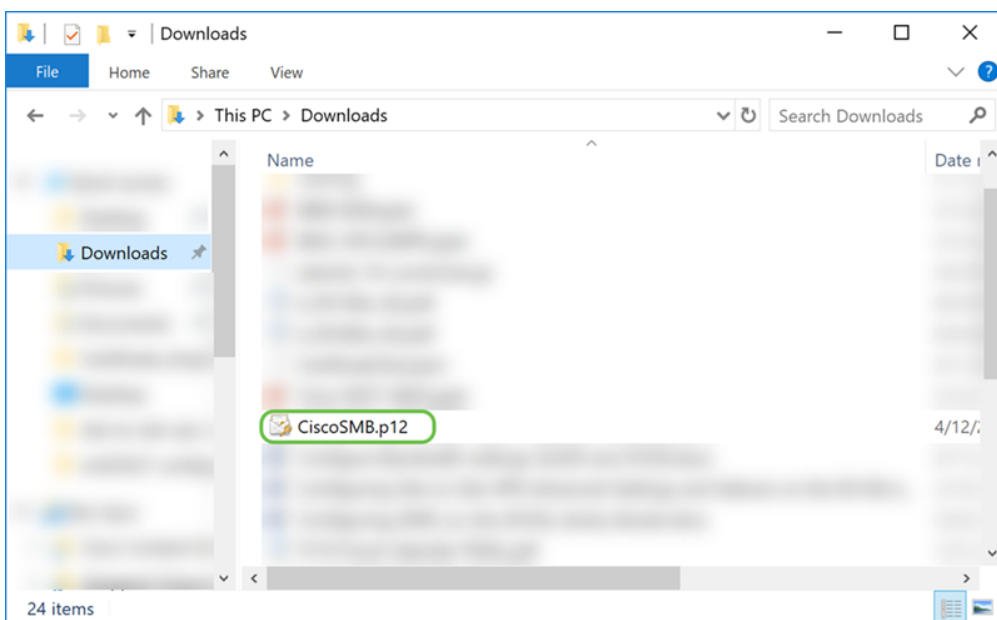
Cancel

Passaggio 3. Viene visualizzata una finestra in cui viene chiesto come si utilizza il file. In questo esempio verrà selezionato **Salva file**, quindi fare clic su **OK**.



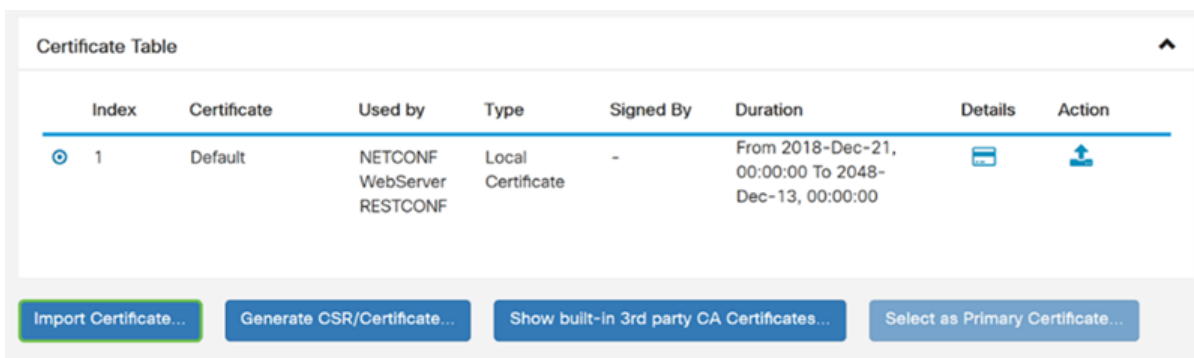
Passaggio 4. Il file deve essere salvato nel percorso di salvataggio predefinito.

Nell'esempio il file è stato salvato nella cartella *Download* del computer.



Importazione certificato

Passaggio 1. Nella pagina *Certificato*, fare clic sul pulsante **Importa certificato...**



Passaggio 2. Selezionare il **tipo** di certificato da importare dall'elenco a discesa *Tipo* nella sezione *Importa certificato*. Le opzioni sono definite come:

- **Certificato CA** - Certificato certificato da un'autorità di terze parti attendibile che ha

confermato l'accuratezza delle informazioni contenute nel certificato.

- **Certificato dispositivo locale** - Certificato generato sul router.
- **PKCS#12 Encoded File** - Public Key Cryptography Standards (PKCS) #12 è un certificato esportato con estensione .p12.

Nell'esempio, è stato selezionato **PKCS#12 Encoded File** (File codificato PKCS#12) come tipo. Immettere un **nome** per il certificato e quindi la **password** utilizzata.

Import Certificate

Type: PKCS#12 Encoded File 1

Certificate Name: CiscoSMB 2

Import Password: ●●●●●●●●●● 3

Upload Certificate file

Import from PC

Import from USB

Browse... No file is selected

Browse... No file is selected

Passaggio 3. Nella sezione *Carica file di certificato*, selezionare **Importa da PC** o **Importa da USB**. In questo esempio è stata selezionata l'opzione **Importa da PC**. Fare clic su **Sfogli...** per scegliere un file da caricare.

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

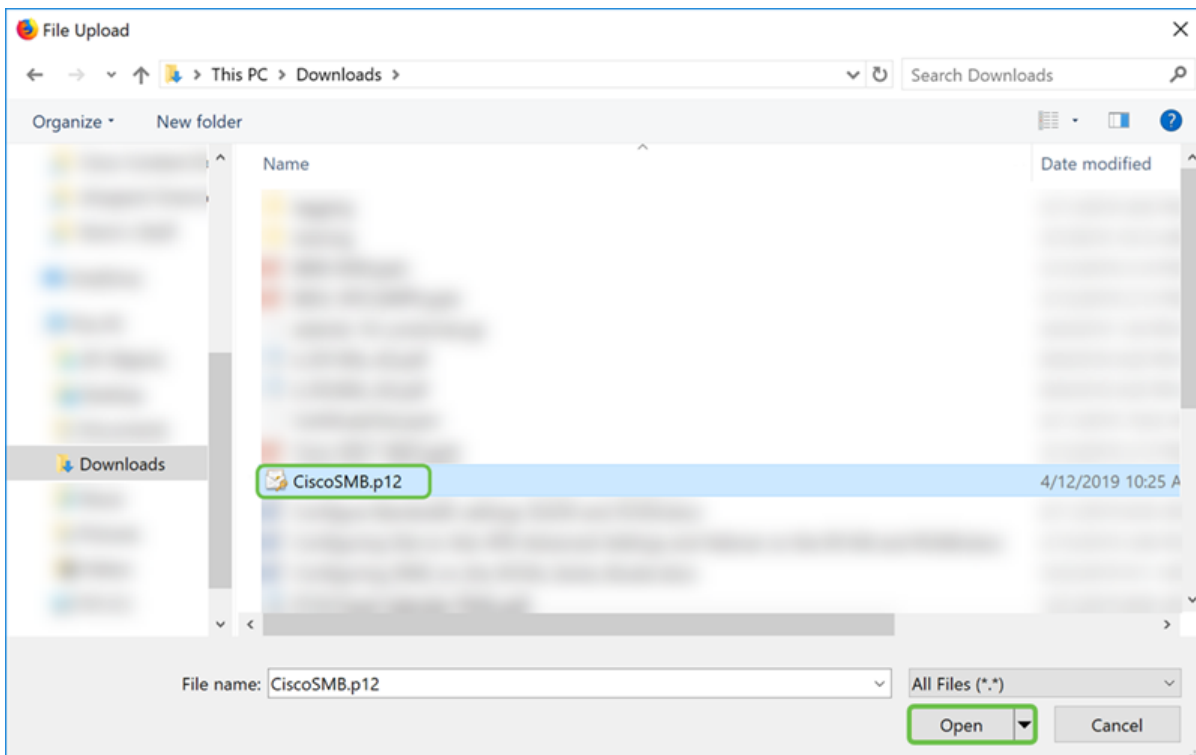
Import from PC

No file is selected

Import from USB 

No file is selected

Passaggio 4. Nella finestra *Caricamento file*, passare alla posizione in cui si trova il file codificato PKCS#12 (estensione .p12). Selezionare il file .p12 e fare clic su **Apri**.



Passaggio 5. Fare clic su **Upload** per avviare il caricamento del certificato.

Certificate

Upload
Cancel

Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●

Upload Certificate file

Import from PC

Browse... CiscoSMB.p12

Import from USB ↻

Browse... No file is selected

Passaggio 6. Verrà visualizzata una finestra di *informazioni* che informa che il certificato è stato importato correttamente. Fare clic su **OK** per continuare.

Information
✕

i
Import certificate successfully!

OK

Passaggio 7. Il certificato è stato caricato.

Certificate Table ^

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		

Conclusioni

È necessario aver imparato come generare un CSR, importare e scaricare un certificato sui router delle serie RV160 e RV260.