Generazione e download dei certificati CSR sui WLC di Catalyst 9800

Sommario

Introduzione

Questo documento descrive il processo generale per generare, scaricare e installare certificati su Catalyst 9800

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare il WLC 9800, il punto di accesso (AP) per le operazioni di base
- Come utilizzare l'applicazione OpenSSL
- Infrastruttura a chiave pubblica (PKI) e certificati digitali

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800-L, Cisco IOS® XE versione 17.3.3
- Applicazione OpenSSL

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.

Configurazione

Nella versione 16.10.X, 9800 non supporta un certificato diverso per l'autenticazione e l'amministrazione Web. Il certificato predefinito viene sempre utilizzato per l'accesso al portale Web.

Nella versione 16.11.X è possibile configurare un certificato dedicato per l'autenticazione Web, definire il trust point all'interno della mappa dei parametri globali.

Ci sono due opzioni per ottenere un certificato per un WLC 9800.

1. Generare una richiesta di firma del certificato (CSR) con OpenSSL o qualsiasi altra applicazione SSL. Ottenere un certificato PKCS12 firmato dall'autorità di certificazione (CA) e caricarlo direttamente sul WLC 9800. La chiave privata viene fornita insieme al certificato.
2. Usare la CLI del WLC 9800 per generare una CSR, apporre la firma di un'autorità di certificazione e quindi caricare manualmente ogni certificato nella catena sul WLC 9800.

Usa quello che meglio si adatta alle tue esigenze.

Opzione 1 - Caricare un certificato firmato PKCS12 preesistente

Definisci una richiesta di firma

Se il certificato non è ancora disponibile, è necessario generare una richiesta di firma da inviare alla CA.

Modificare il file **openssl.cnf** dalla directory corrente (su un computer portatile in cui è installato OpenSSL), copiare e incollare queste righe per includere il campo Nomi alternativi soggetto (SAN) nei CSR appena creati.

```
[ req ]
default_bits       = 4096
distinguished_name = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
stateOrProvinceName         = State or Province Name (full name)
localityName                = Locality Name (eg, city)
organizationName            = Organization Name (eg, company)
commonName                  = Common Name (e.g. server FQDN or YOUR name)
[ req_ext ]
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1   = testdomain.com
DNS.2   = example.com
DNS.3   = webadmin.com
```

Sostituire i nomi DNS.X con la rete SAN. Sostituire i campi principali con i dettagli del certificato necessari. Assicurarsi di ripetere il Nome comune nei campi SAN (DNS.x). Google Chrome richiede che il nome presente nell'URL sia nei campi SAN per poter considerare attendibile il certificato.

Nel caso dell'amministratore Web, è inoltre necessario popolare i campi SAN con variazioni dell'URL (ad esempio solo nome host o nome di dominio completo (FQDN) completo) in modo che il certificato corrisponda a prescindere da quello che l'amministratore digita nell'URL nella barra degli indirizzi del browser.

Generare il CSR da OpenSSL con questo comando:

```
openssl req -out myCSR.csr -newkey rsa:4096 -nodes -keyout private.key -config openssl.cnf
```

Il CSR viene generato come **myCSR.csr** e la relativa chiave come **private.key** nella directory da cui viene eseguito OpenSSL a meno che non venga fornito il percorso completo del comando.

Assicurarsi di mantenere il file **private.key** protetto poiché viene utilizzato per crittografare le comunicazioni.

Èpossibile verificarne il contenuto con:

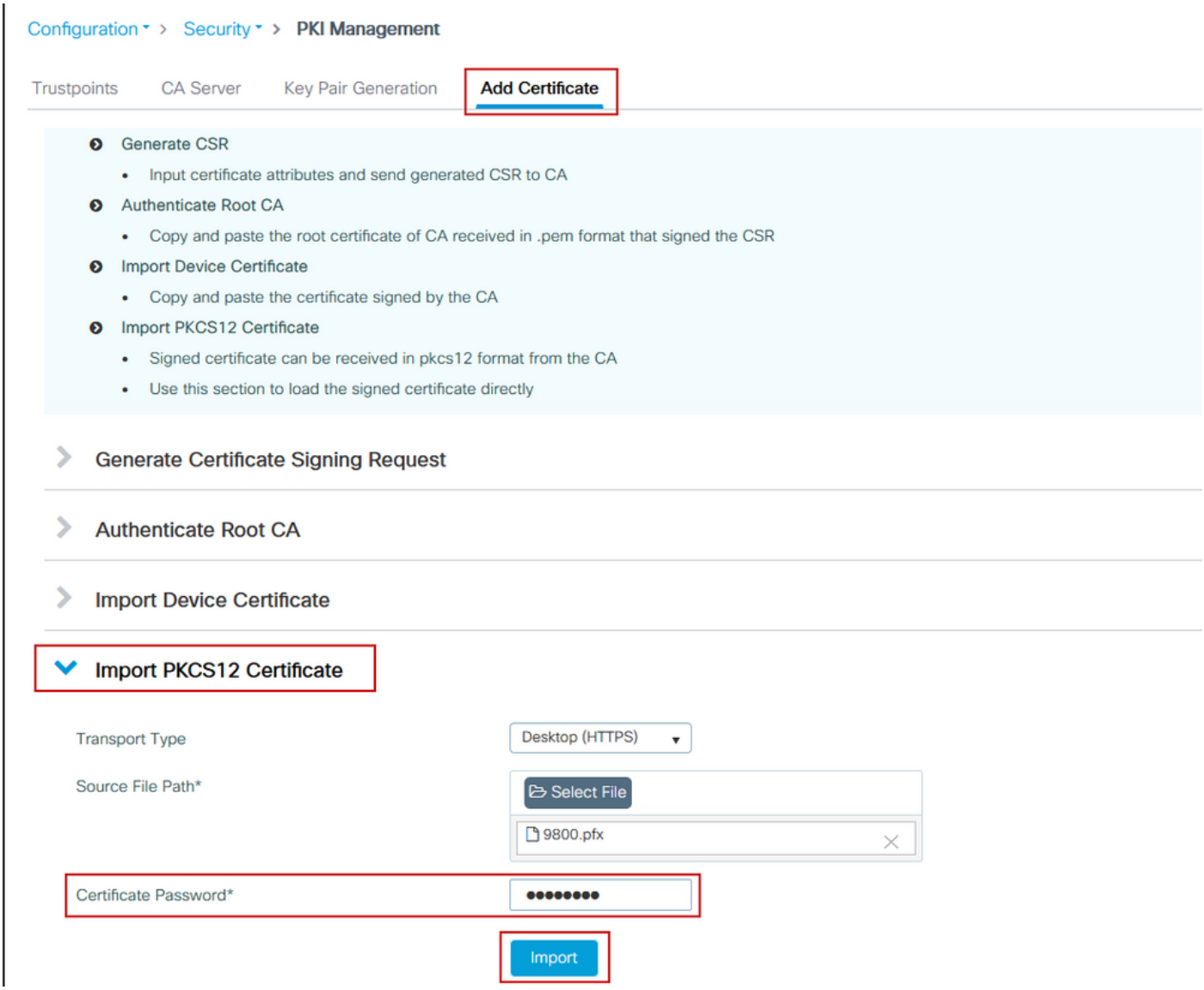
```
openssl req -noout -text -in myCSR.csr
```

Èquindi possibile fornire questo CSR alla CA per firmarlo e ricevere nuovamente un certificato. Verificare che la catena completa venga scaricata dalla CA e che il certificato sia in formato Base64 in caso sia necessario modificarlo ulteriormente.

Importa il certificato

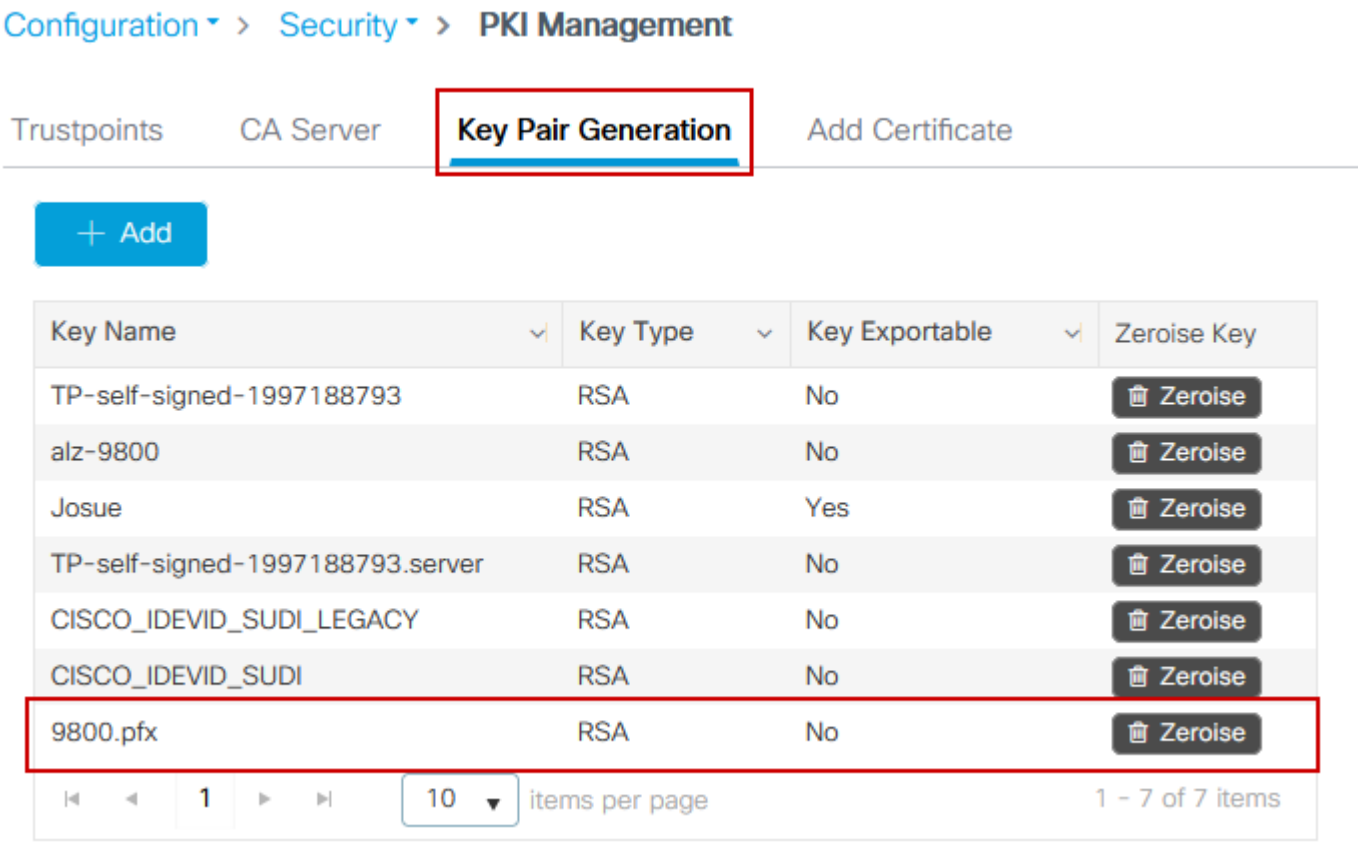
Passaggio 1. Salvare il certificato PKCS12 su un server TFTP (Trivial File Transfer Protocol) raggiungibile dal WLC 9800. Il certificato PKCS12 deve contenere la chiave privata e la catena di certificati fino alla CA radice.

Passaggio 2. Aprire la GUI del WLC 9800 e selezionare **Configurazione > Sicurezza > Gestione PKI**, fare clic sulla scheda **Aggiungi certificato.** Espandere il menu **Importa certificato PKCS12** e immettere i dettagli TFTP. In alternativa, l'opzione **Desktop (HTTPS)** nell'elenco a discesa **Transport Type** (Tipo di trasporto) consente il caricamento HTTP tramite il browser. **Password certificato** si riferisce alla password utilizzata al momento della generazione del certificato PKCS12.



Passaggio 3. Verificare che le informazioni siano corrette e fare clic su **Importa.** Quindi, nella scheda **Generazione coppia di chiavi** verrà visualizzata la nuova coppia di chiavi del certificato per il nuovo trust point installato. Una volta completata l'importazione, il WLC 9800 crea anche un trust point aggiuntivo per le CA multilivello.

> **Nota**: al momento, il WLC 9800 non presenta l'intera catena di certificati ogni volta che uno specifico trust point viene utilizzato per webauth o webadmin, ma presenta il certificato del dispositivo e il suo emittente immediato. Questo errore viene registrato con l'ID bug Cisco CSCwa23606 , risolto in Cisco IOS® XE 17.8.



CLI:

```
9800# configure terminal
9800(config)#crypto pki import
```

Nota: è importante che il nome del file del certificato e il nome del trust point corrispondano esattamente a quelli del WLC 9800 per creare ulteriori trust point per CA multilivello.

Conversione del formato PKCS12 e catena di certificati in scenari CA multilivello.

Èpossibile che il file della chiave privata e il certificato in formato PEM o CRT vengano combinati in un formato PKCS12 (.pfx) per caricarli nel WLC 9800. A tale scopo, immettere questo comando:

```
openssl pkcs12 -export -in
```

Nel caso in cui si disponga di una catena di certificati (una o più CA intermedie e CA radice) in formato PEM, è necessario combinare tutto in un unico file con estensione pfx.

In primo luogo, combinare manualmente i certificati CA in un unico file. Copiare e incollare il

contenuto (salvare il file in formato .pem):

```
----- BEGIN Certificate --------
<intermediate CA cert>
------END Certificate --------
-----BEGIN Certificate -----
<root CA cert>
-----END Certificate--------
```

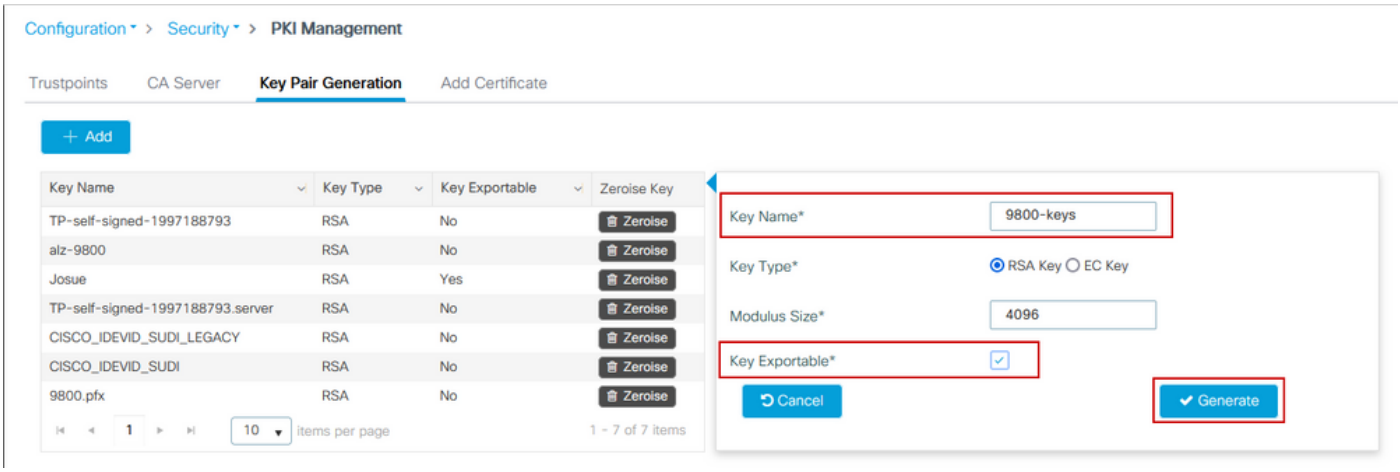
In seguito sarà possibile combinare tutto in un unico file di certificato PKCS12 con:

```
openssl pkcs12 -export -out chaincert.pfx -inkey
```

Fare riferimento alla sezione Verifica alla fine dell'articolo per verificare l'aspetto del certificato finale.

Opzione 2 - Definizione di una chiave e di una richiesta di firma (CSR) sul WLC 9800

Passaggio 1. Generare una coppia di chiavi RSA generica. Passare a **Configurazione > Sicurezza > Gestione PKI**, scegliere la scheda **Generazione coppia di chiavi** e fare clic su **+ Aggiungi**. Immettere i dettagli, verificare che la casella di controllo **Chiave esportabile** sia selezionata e quindi fare clic su **Genera**.



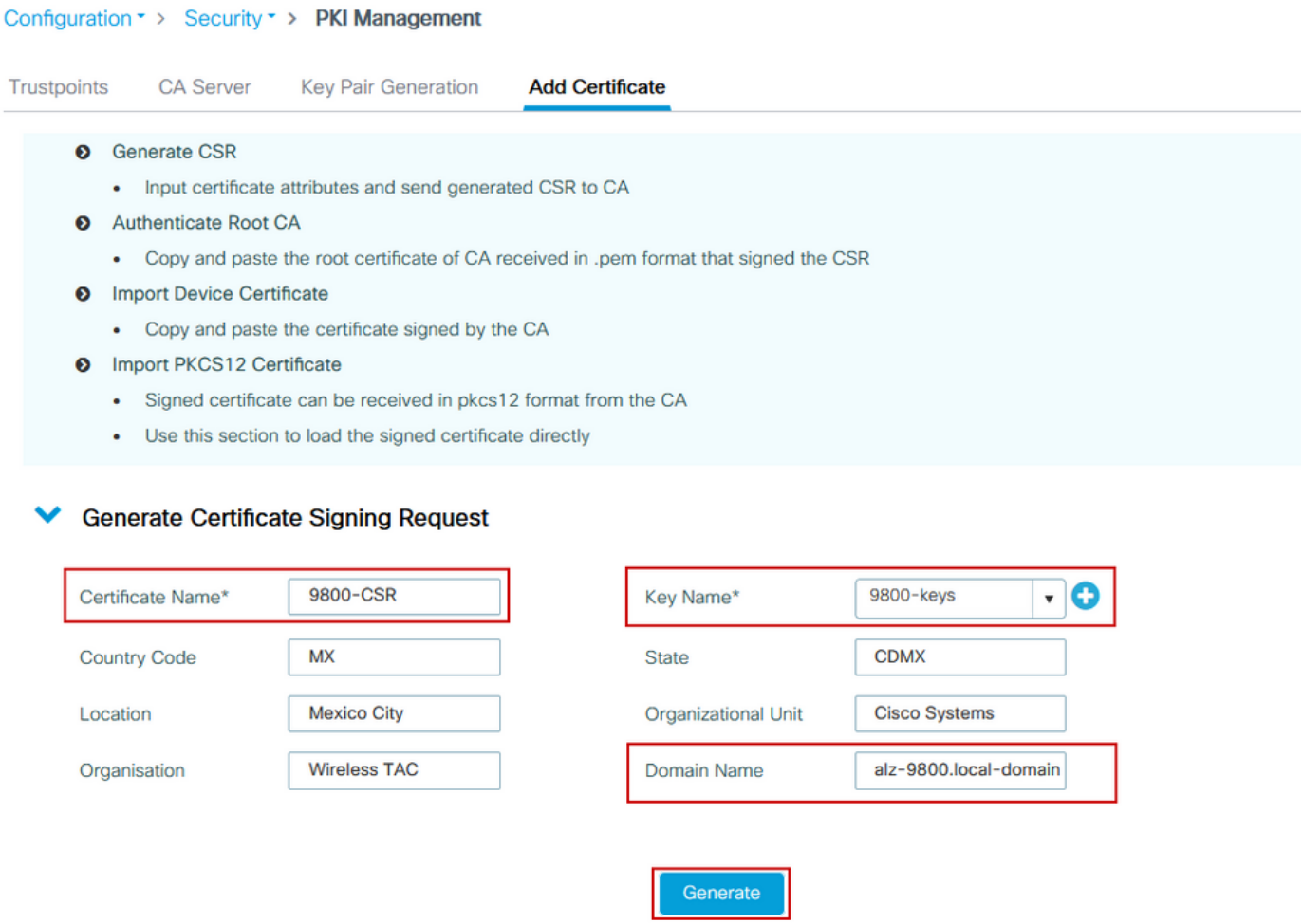
Configurazione CLI:

```
9800(config)#crypto key generate rsa general-keys label 9800-keys exportable
The name for the keys will be: 9800-keys
Choose the size of the key modulus in the range of 512 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [1024]: 4096
% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 9 seconds)
```

Passaggio 2. Generare un CSR per il WLC 9800. Passare alla scheda **Aggiungi certificato** ed espandere **Genera richiesta di firma del certificato**, immettere i dettagli e scegliere la coppia di

chiavi creata in precedenza dall'elenco a discesa. È importante che **Domain Name** corrisponda all'URL definito per l'accesso client sul WLC 9800 (pagina di amministrazione Web, pagina di autenticazione Web e così via), **Certificate Name** (Nome certificato) è il nome del trust in modo che sia possibile assegnare un nome in base al relativo utilizzo.

Nota: i WLC 9800 supportano i certificati con parametri jolly all'interno del nome comune.



Verificare che le informazioni siano corrette, quindi fare clic su **Genera**. Il CSR verrà visualizzato in una casella di testo accanto al modulo originale.

Copia consente di salvare una copia negli Appunti in modo da poterla incollare in un editor di testo e salvare il file CSR. Se si seleziona **Save to device**, il WLC 9800 crea una copia del CSR e la memorizza in **bootflash:**/csr. Ad esempio, eseguire i seguenti comandi:

```
9800#dir bootflash:/csr
Directory of bootflash:/csr/
```

```
1046531 -rw- 1844 Sep 28 2021 18:33:49 +00:00 9800-CSR1632856570.csr

26458804224 bytes total (21492699136 bytes free)
9800#more bootflash:/csr/9800-CSR1632856570.csr
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Configurazione CLI:

```
9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#enrollment terminal pem
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#subject-name C=MX, ST=CDMX, L=Mexico City, O=Cisco Systems, OU=Wireless TaC,
CN=alz-9800.local-domain.com
9800(ca-trustpoint)#rsakeypair 9800-keys
9800(ca-trustpoint)#subject-alt-name domain1.mydomain.com,domain2.mydomain.com
9800(ca-trustpoint)#exit

(config)#crypto pki enroll 9800-CSR
% Start certificate enrollment ..

% The subject name in the certificate will include: C=MX, ST=CDMX, L=Mexico City, O=Cisco
Systems, OU=Wireless TaC, CN=alz-9800.local-domain.com
% The subject name in the certificate will include: alz-9800
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

Parametri disponibili per la configurazione del nome soggetto:

C: Paese, deve essere composto solo da due lettere maiuscole.

ST: Qualche stato, fa riferimento al nome dello stato o della provincia.

L: Nome località, si riferisce alla città.

O: Nome organizzazione, si riferisce alla società.

OU: nome dell'unità organizzativa, può fare riferimento alla sezione.

CN: (nome comune)In riferimento al soggetto a cui viene rilasciato il certificato, è necessario specificare l'indirizzo IP specifico a cui accedere (IP di gestione wireless, IP virtuale e così via) o configurare il nome host con FQDN.

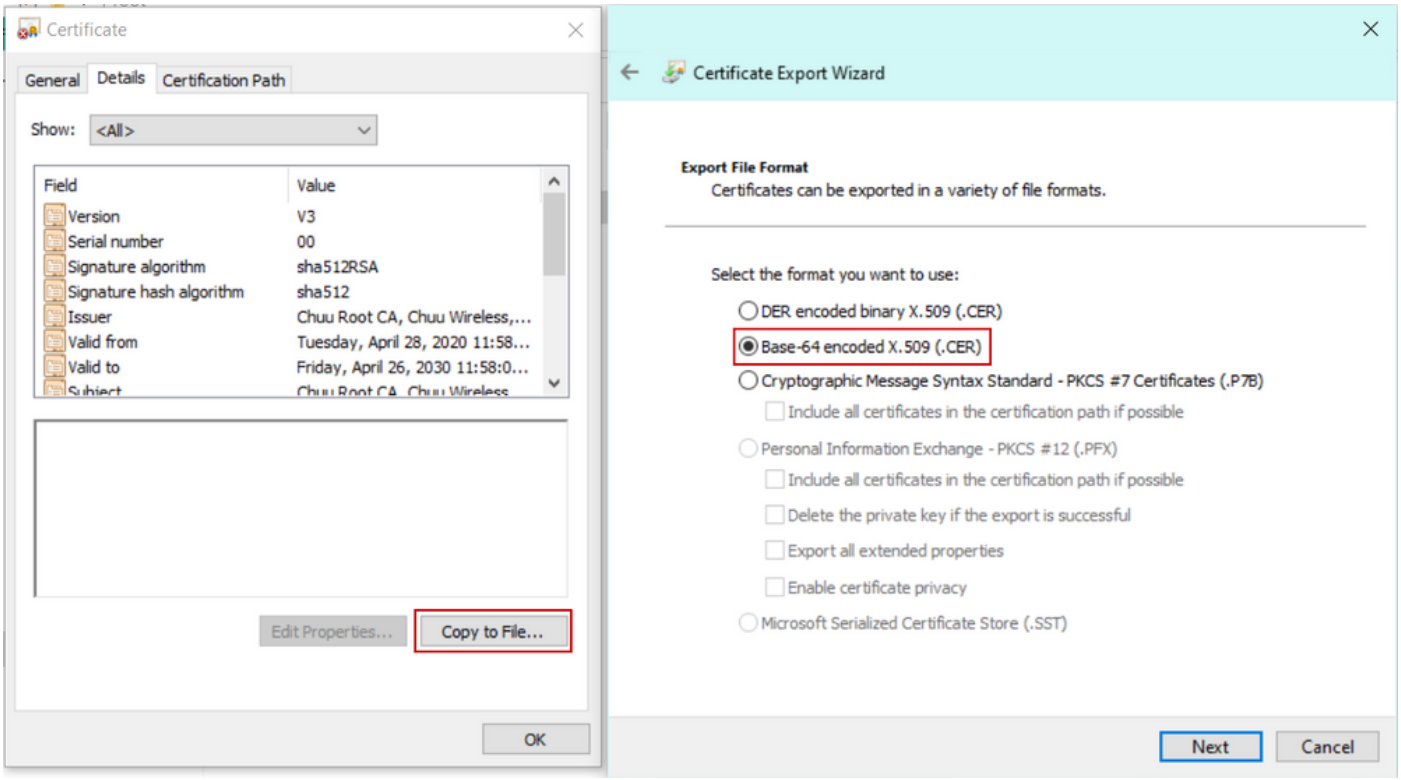
> **Nota**: se si desidera aggiungere un nome soggetto alternativo, non è possibile farlo sulle versioni Cisco IOS XE precedenti alla 17.8.1 a causa dell'ID bug Cisco CSCvt1517 . Questo scenario può generare alcuni avvisi del browser a causa dell'assenza della SAN. Per evitare

questo problema, creare la chiave e la CSR nella casella di configurazione off-box, come mostrato nell'opzione 1.

Passaggio 3. Firmare il CSR dall'Autorità di certificazione (CA). È necessario inviare la stringa completa alla CA per ottenerne la firma.

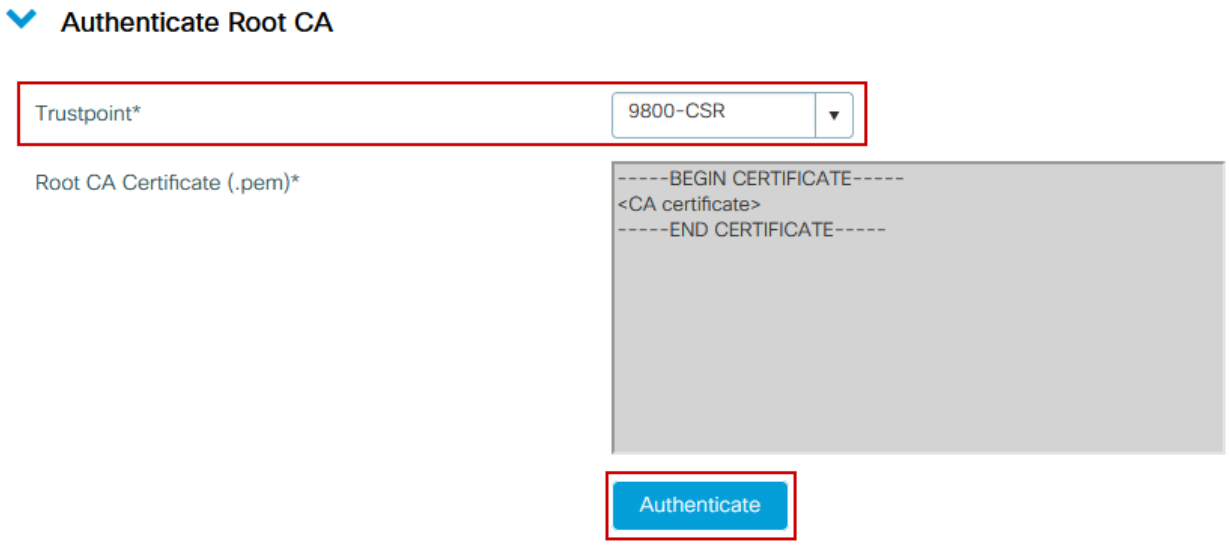
```
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Se si utilizza una CA di Windows Server per firmare il certificato, scaricare il certificato firmato in formato Base64. In caso contrario, è necessario eseguire l'esportazione con utilità quali Gestione certificati di Windows.



Nota: il processo di autenticazione del trust point dipende dal numero di CA che hanno firmato il CSR. Se è presente una CA a livello singolo, controllare il **passaggio 4a.** Se è presente una CA multilivello, andare al **passo 4b**. Questa operazione è necessaria perché in un trust point è possibile archiviare solo due certificati alla volta, ovvero il certificato soggetto e il certificato emittente.

Passaggio 4a. Rendere 9800 attendibile la CA emittente. Scaricare il certificato CA dell'autorità emittente in formato .pem (Base64). Espandere la sezione **Autenticazione CA radice** all'interno dello stesso menu, scegliere il trust point definito in precedenza dall'elenco a discesa **TrustPoint** e incollare il certificato CA dell'autorità emittente. Verificare che i dettagli siano configurati correttamente e fare clic su **Autentica**.



Configurazione CLI:

```
9800(config)# crypto pki authenticate 9800-CSR

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
Certificate has the following attributes: Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809 % Do you accept this certificate?
[yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

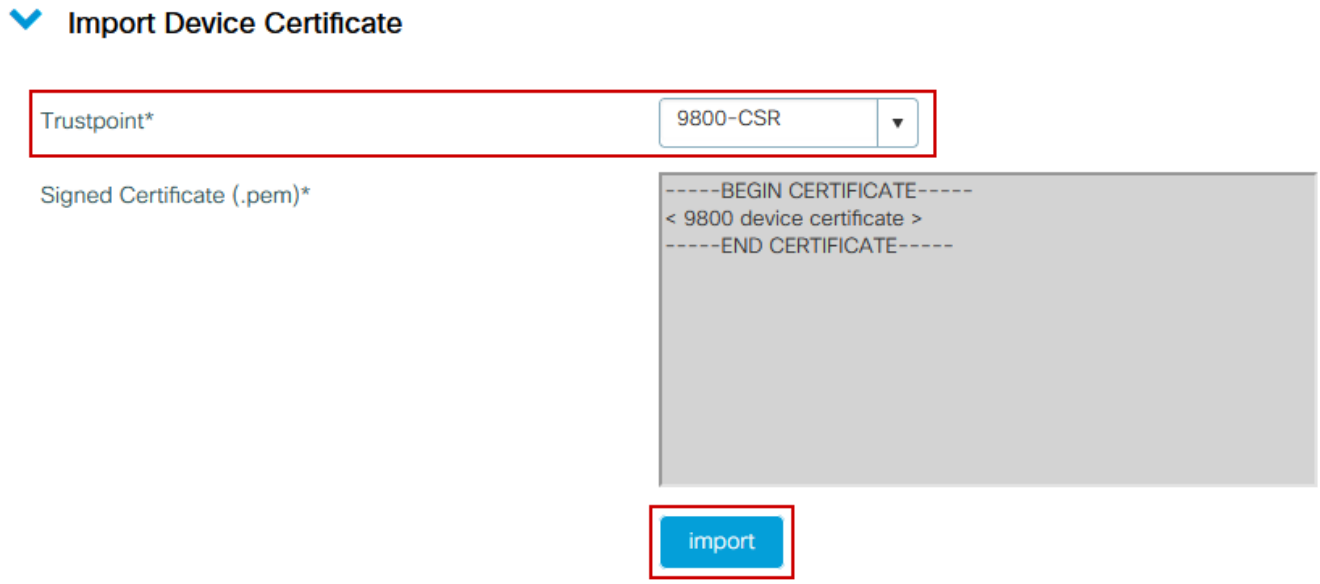
Passaggio 4b. Nello scenario in cui esistono più livelli di autorizzazione, è necessario un nuovo trust point per ogni livello CA. Questi trust point contengono solo il certificato di autenticazione e puntano al livello di autenticazione successivo. Questo processo viene eseguito solo nella CLI e nell'esempio riportato di seguito sono presenti una CA intermedia e una CA radice:

```
9800(config)#crypto pki trustpoint root
9800(ca-trustpoint)#enrollment terminal
9800(ca-trustpoint)#chain-validation stop
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#exit
9800(config)#crypto pki authenticate root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 6CAC00D5 C5932D01 B514E413 D41B37A8
Fingerprint SHA1: 5ABD5667 26B7BD0D 83BDFC34 543297B7 3D3B3F24

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#chain-validation continue root
9800(config)#crypto pki authenticate 9800-CSR

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----




-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

> **Nota**: se nella catena di certificazione sono presenti più CA intermedie, è necessario generare un nuovo punto di accesso per ogni livello di certificazione aggiuntivo. Questi punti di trust devono fare riferimento al punto di trust che contiene il livello di certificazione successivo con il comando **chain-validation continue <nome-punto-di-trust>**.

Passaggio 5. Caricare il certificato firmato nel WLC 9800. Espandere la sezione **Importa certificato dispositivo** nello stesso menu. Scegliere il **trust point** definito in precedenza e incollare il certificato di dispositivo firmato fornito dalla CA. Quindi fare clic su **import** (Importa) dopo aver verificato le informazioni sul certificato.



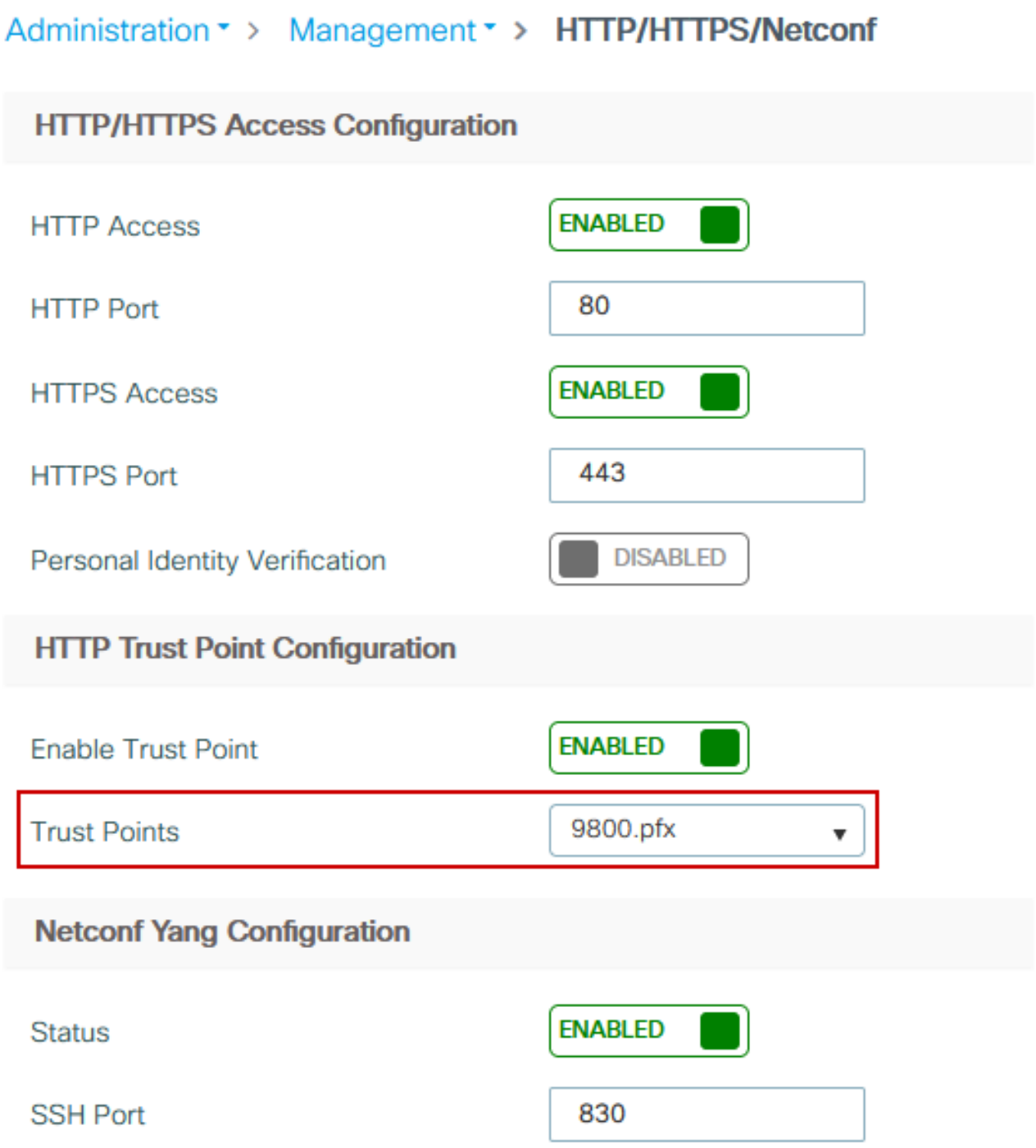
Configurazione CLI:

```
9800(config)#crypto pki import 9800-CSR certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
<9800 device certificate >
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

Usa il nuovo certificato

Amministrazione Web

Passare a **Amministrazione > Gestione > HTTP/HTTPS/Netconf** e scegliere il certificato importato dall'elenco a discesa **Trust Point**.

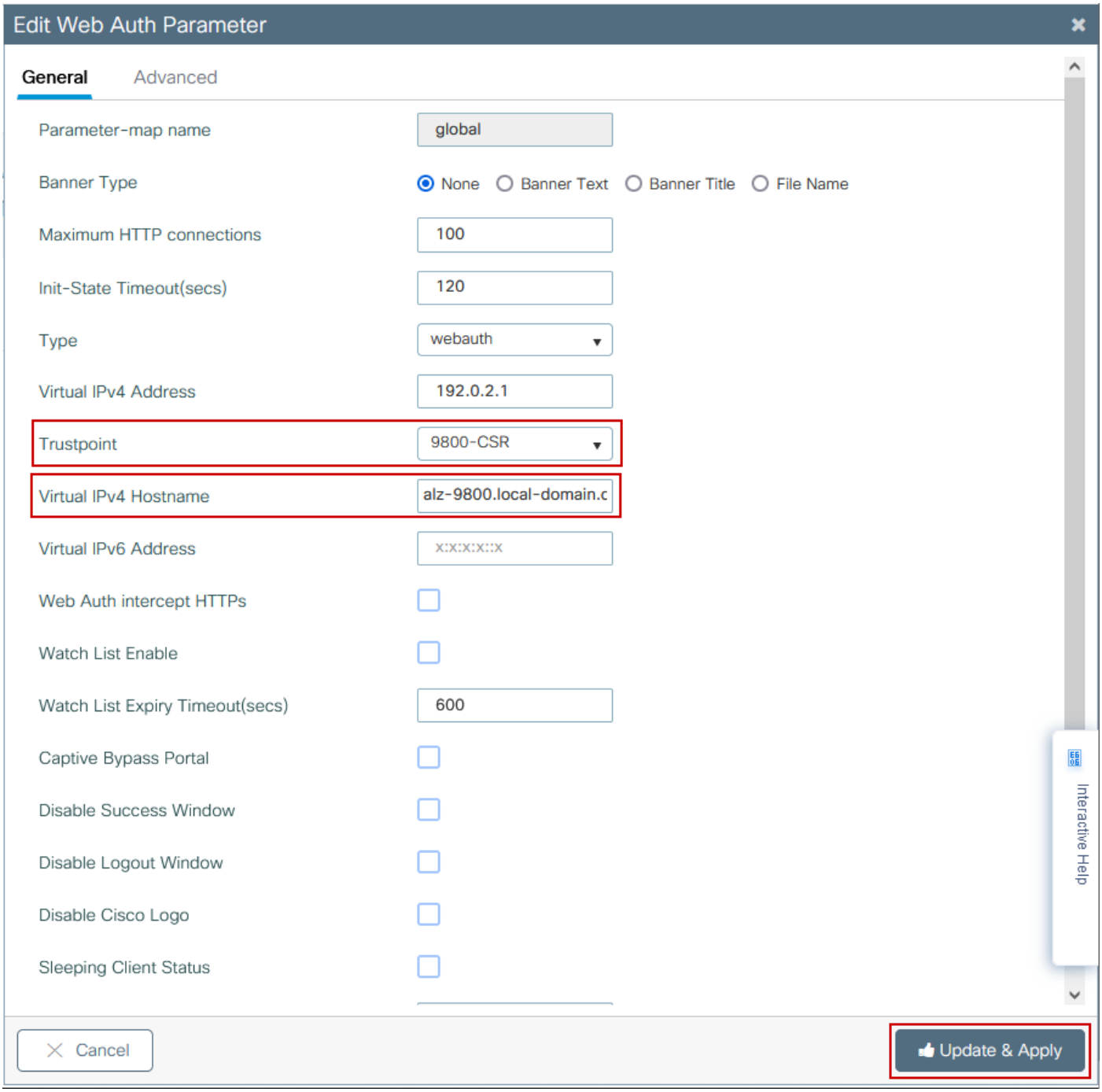


Configurazione CLI:

```
9800(config)#ip http secure-trustpoint 9800.pfx
9800(config)#no ip http secure-server
9800(config)#ip http secure-server
```

Autenticazione Web locale

Passare a **Configurazione > Sicurezza > Autenticazione Web**, scegliere la mappa dei parametri **globali** e scegliere il trust point importato dall'elenco a discesa **TrustPoint**. Fare clic su **Aggiorna e applica** per salvare le modifiche. Verificare che il nome host **IPv4 virtuale** corrisponda al nome comune nel certificato.



Configurazione CLI:

```
9800(config)#parameter-map type webauth global
9800(config-params-parameter-map)#type webauth
9800(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1 virtual-host alz-9800.local-domain.com
9800(config-params-parameter-map)#trustpoint 9800-CSR
```

Per aggiornare l'utilizzo dei certificati, riavviare i servizi HTTP:

```
9800(config)#no ip http server
9800(config)#ip http server
```

.

Considerazioni sull'alta disponibilità

Su una coppia 9800 configurata per lo standard HA (Stateful Switchover High Availability), tutti i certificati vengono replicati dal server primario al server secondario durante la sincronizzazione di massa iniziale. Sono inclusi i certificati in cui la chiave privata è stata generata sul controller stesso, anche se la chiave RSA è configurata per non essere esportabile. Una volta stabilita la coppia HA, qualsiasi nuovo certificato installato viene installato su entrambi i controller e tutti i certificati vengono replicati in tempo reale.

In caso di errore, l'ex controller secondario ora attivo utilizza in modo trasparente i certificati ereditati dal controller primario.

Verifica dell'attendibilità del certificato da parte dei browser Web

Per garantire l'attendibilità di un certificato da parte dei browser Web, è necessario tenere presenti alcune considerazioni importanti:

- Il relativo nome comune (o campo SAN) deve corrispondere all'URL visitato dal browser.
- Deve essere compreso nel suo periodo di validità.
- Deve essere rilasciato da una CA o da una catena di CA la cui radice è considerata attendibile dal browser. A tale scopo, il certificato fornito dal server Web deve contenere tutti i certificati della catena fino a quando non viene incluso un certificato considerato attendibile dal browser client (in genere la CA radice).
- Se contiene elenchi di revoche, il browser deve essere in grado di scaricarli e il certificato CN non deve essere elencato.

Verifica

Èpossibile utilizzare i seguenti comandi per verificare la configurazione dei certificati:

```
9800#show crypto pki certificate 9800.pfx

Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx
```

```
CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx
```

```
9800#show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: 9800.pfx
HTTP secure server active session modules: ALL
```

Èpossibile verificare la catena di certificati sul modello 9800. Nel caso di un certificato di dispositivo rilasciato da una CA intermedia, a sua volta rilasciato da una CA radice, si dispone di un trust point per gruppi di due certificati, in modo che ogni livello disponga di un trust point specifico. In questo caso, il WLC 9800 ha 9800.pfx con il certificato del dispositivo (certificato WLC) e la relativa CA di rilascio (CA intermedia). Quindi un altro trust point con la CA radice che ha emesso la CA intermedia.

```
9800#show crypto pki certificate 9800.pfx
Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
```

```
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx

CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx

9800#show crypto pki certificate 9800.pfx-rrr1
CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Validity Date:
start date: 04:58:05 Pacific Apr 29 2020
end date: 04:58:05 Pacific Apr 27 2030
Associated Trustpoints: 9800-CSR 9800.pfx-rrr1
```

Verifica dei certificati con OpenSSL

OpenSSL può essere utile per verificare il certificato stesso o eseguire alcune operazioni di conversione.

Per visualizzare un certificato con OpenSSL:

```
openssl x509 -in
```

Per visualizzare il contenuto di un CSR:

```
openssl req -noout -text -in
```

Se si desidera verificare il certificato finale sul WLC 9800 ma si desidera utilizzare un altro strumento oltre al browser, OpenSSL può eseguire questa operazione e fornire molti dettagli.

```
openssl s_client -showcerts -verify 5 -connect
```

Èpossibile sostituire <wlcURL> con l'URL di webadmin del modello 9800 o con l'URL del portale guest (IP virtuale). È inoltre possibile inserire un indirizzo IP. Indica la catena di certificati ricevuta, ma la convalida dei certificati non può mai essere corretta al 100% quando si utilizza un indirizzo IP anziché un nome host.

Per visualizzare il contenuto e verificare un certificato PKCS12 (con estensione pfx) o una catena di certificati:

```
openssl pkcs12 -info -in
```

Di seguito è riportato un esempio di questo comando su una catena di certificati in cui il certificato del dispositivo viene rilasciato al Technical Assistance Center (TAC) da una CA intermedia chiamata "intermediate.com", a sua volta rilasciata da una CA radice chiamata "root.com":

```
openssl pkcs12 -info -in chainscript2.pfx
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/CN=TAC
issuer=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
-----BEGIN CERTIFICATE-----
<Device certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
```

```
-----BEGIN CERTIFICATE-----
<Intermediate certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
-----BEGIN CERTIFICATE-----
<Root certificate >
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Private key >
-----END ENCRYPTED PRIVATE KEY-----
```

Risoluzione dei problemi

Utilizzare questo comando per la risoluzione dei problemi. Se l'operazione viene eseguita in una sessione remota (SSH o telnet), è necessario un **monitor del terminale** per visualizzare le uscite:

```
9800#debug crypto pki transactions
```

Output del comando debug scenario completato

Questo output visualizza l'output previsto quando l'importazione di un certificato su un 9800 ha esito positivo. Utilizzare questo per riferimento e identificare lo stato di errore:

```
Sep 28 17:35:23.242: CRYPTO_PKI: Copying pkcs12 from bootflash:9800.pfx
Sep 28 17:35:23.322: CRYPTO_PKI: Creating trustpoint 9800.pfx
Sep 28 17:35:23.322: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx created succesfully
Sep 28 17:35:23.324: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.324: CRYPTO_PKI: issuerName=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: subjectname=e=user@example.com,cn=alz-9800,ou=Cisco
Systems,o=Wireless TAC,l=CDMX,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: adding RSA Keypair
Sep 28 17:35:23.324: CRYPTO_PKI: bitValue of ET_KEY_USAGE = 140
Sep 28 17:35:23.324: CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
Sep 28 17:35:23.324: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named 9800.pfx has been generated or
imported by pki-pkcs12
Sep 28 17:35:23.331: CRYPTO_PKI: adding as a router certificate.Public key in cert and stored
public key 9800.pfx match

Sep 28 17:35:23.333: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.333: CRYPTO_PKI: issuerName=cn=Chuu Root CA,ou=Chuu Wireless,o=Chuu
Inc,l=Iztapalapa,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: subjectname=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: no matching private key presents.

[...]
```

```
Sep 28 17:35:23.335: CRYPTO_PKI: Setting the key_type as RSA
Sep 28 17:35:23.335: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.335: CRYPTO_PKI:Peer's public inserted successfully with key id 21
Sep 28 17:35:23.336: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.337: CRYPTO_PKI: Deleting cached key having key id 31
Sep 28 17:35:23.337: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.337: CRYPTO_PKI:Peer's public inserted successfully with key id 32
Sep 28 17:35:23.338: CRYPTO_PKI: (A0323) Session started - identity selected (9800.pfx)
Sep 28 17:35:23.338: CRYPTO_PKI: Rcvd request to end PKI session A0323.
Sep 28 17:35:23.338: CRYPTO_PKI
alz-9800#: PKI session A0323 has ended. Freeing all resources.
Sep 28 17:35:23.338: CRYPTO_PKI: unlocked trustpoint 9800.pfx, refcount is 0
Sep 28 17:35:23.338: CRYPTO_PKI: Expiring peer's cached key with key id 32Public key in cert and
stored public key 9800.pfx match

Sep 28 17:35:23.341: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.341: CRYPTO_PKI: cert verified and inserted.
Sep 28 17:35:23.402: CRYPTO_PKI: Creating trustpoint 9800.pfx-rrr1
Sep 28 17:35:23.402: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx-rrr1 created succesfully
Sep 28 17:35:23.403: CRYPTO_PKI: Setting the key_type as RSA
Sep 28 17:35:23.404: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.404: CRYPTO_PKI:Peer's public inserted successfully with key id 22
Sep 28 17:35:23.405: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.406: CRYPTO_PKI: no CRLs present (expected)
Sep 28 17:35:23.406: %PKI-6-PKCS12_IMPORT_SUCCESS: PKCS #12 import in to trustpoint 9800.pfx
successfully imported.
```

Provare a importare un certificato PKCS12 privo di CA

Se si importa un certificato e viene visualizzato il messaggio di errore "Impossibile trovare il certificato CA", significa che il file con estensione pfx non contiene l'intera catena o che una CA non è presente.

```
9800(config)#crypto pki import pkcs12.pfx pkcs12 bootflash:pks12.pfx password
```

```
% Importing pkcs12...
Source filename [pks12.pfx]?
Reading file from bootflash:pks12.pfx
% Warning: CA cert is not found. The imported certs might not be usable.
```

Se si esegue il comando **openssl pkcs12 -info -in <percorso del certificato>** e viene visualizzato un solo certificato con una chiave privata, significa che la CA non è presente. In genere, questo comando elenca l'intera catena di certificati. Non è necessario includere la CA radice principale superiore se è già nota ai browser client.

Un modo per risolvere il problema consiste nel decostruire il PKCS12 in PEM e ricostruire la catena in modo corretto. Nell'esempio successivo era presente un file con estensione pfx contenente solo il certificato del dispositivo (WLC) e la relativa chiave. È stato rilasciato da una CA intermedia (che non era presente nel file PKCS12) che a sua volta è stata firmata da una CA radice nota.

Passaggio 1. Esporta la chiave privata in uscita.

```
openssl pkcs12 -in
```

Passaggio 2. Esporta il certificato come PEM.

```
openssl pkcs12 -in
```

Passaggio 3. Scaricare il certificato CA intermedio come PEM.

L'origine della CA dipende dalla natura della CA. Se si tratta di una CA pubblica, è sufficiente una ricerca in linea per trovare il repository. In caso contrario, l'amministratore della CA deve fornire i certificati nel formato Base64 (.pem). Se sono presenti più livelli di CA, raggrupparli in un unico file come quello presentato al termine del processo di importazione dell'**opzione 1**.

Passaggio 4. Ricostruire il PKCS 12 dalla chiave, dal certificato del dispositivo e dal certificato della CA.

```
openssl pkcs12 -export -out fixedcertchain.pfx -inkey cert.key -in certificate.pem -certfile
CA.pem
```

A questo punto è disponibile il file "fixedcertchain.pfx" che è possibile importare in Catalyst 9800!

Note e limitazioni

- Cisco IOS® XE non supporta certificati CA con ID bug Cisco oltre il 2099: CSCvp64208
- Cisco IOS® XE non supporta il bundle PKCS 12 con message digest SHA256 (sono supportati i certificati SHA256, ma non se il bundle PKCS12 è firmato con SHA256) : ID bug Cisco CSCvz41428
- È possibile verificare la frammentazione se il WLC deve trasportare certificati utente e l'appliance NAC/ISE è raggiungibile tramite Internet (ad esempio, in una distribuzione SD-WAN). I certificati sono quasi sempre più grandi di 1500 byte (ossia vengono inviati diversi pacchetti RADIUS per trasportare il messaggio del certificato) e se si hanno diverse MTU sul percorso di rete, può verificarsi una frammentazione eccessiva dei pacchetti RADIUS stessi. In questi casi, si consiglia di inviare tutti i datagrammi UDP per il traffico WLC sullo stesso percorso per evitare problemi di ritardo/jitter che possono essere causati da condizioni meteo su Internet

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).