

# Genera nuovo certificato Expressway con le informazioni del certificato corrente.

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1. Individuare le informazioni sul certificato corrente.](#)

[Passaggio 2. Creare un nuovo CSR con le informazioni ottenute in precedenza.](#)

[Passaggio 3. Verificare e scaricare il nuovo CSR.](#)

[Passaggio 4. Verificare le informazioni contenute nel nuovo certificato.](#)

[Passaggio 5. Caricare i nuovi certificati CA nell'archivio attendibile dei server, se applicabile.](#)

[Passaggio 6. Caricare il nuovo certificato nel server Expressway.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come generare una nuova richiesta di firma di certificato (CSR) con le informazioni contenute nel certificato Expressway esistente.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Attributi certificato
- Expressways o Video Communication Server (VCS)

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

## Passaggio 1. Individuare le informazioni sul certificato corrente.

Per ottenere le informazioni contenute nel certificato corrente, selezionare **Manutenzione > Sicurezza > Certificato server** nell'interfaccia grafica utente di Expressway.

Individuare la sezione **Dati certificato server** e selezionare **Mostra (decodificato)**.

Cercare le informazioni nei campi **Nome comune (CN)** e **Nome alternativo soggetto (SAN)** come illustrato nell'immagine:

### Certificate:

#### Data:

Version: 3 (0x2)

Serial Number:

35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1

Signature Algorithm: sha256WithRSAEncryption

Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA

Validity

Not Before: Dec 2 04:39:57 2019 GMT

Not After : Nov 28 00:32:43 2020 GMT

Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, **CN=expe.domain.com**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

-----

#### X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication, TLS Web Server Authentication

X509v3 Subject Alternative Name:

DNS:expe.domain.com, DNS:domain.com

X509v3 Subject Key Identifier:

92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B

X509v3 Authority Key Identifier:

keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32

Ora che si conoscono il CN e la SAN, è possibile copiarli in modo che possano essere aggiunti al nuovo CSR.

Facoltativamente è possibile copiare le informazioni aggiuntive per il certificato, ovvero Paese (C), Stato (ST), Località (L), Organizzazione (O), Unità organizzativa (OU). Queste informazioni sono accanto alla CN.

## Passaggio 2. Creare un nuovo CSR con le informazioni ottenute in precedenza.

Per creare il CSR, selezionare **Manutenzione > Sicurezza > Certificato server**.

Individuare la sezione **Richiesta di firma del certificato (CSR)** e selezionare **Genera CSR** come illustrato nell'immagine:

**Certificate signing request (CSR)**

Certificate request There is no certificate signing request in progress

**Generate CSR**

Immettere i valori raccolti dal certificato corrente.

Impossibile modificare il CN se non è un cluster. Nel caso di un cluster, è possibile selezionare il CN come nome di dominio completo (FQDN) di Expressway o FQDN del cluster. Nel presente documento viene utilizzato un singolo server e quindi la CN corrisponde a quanto ottenuto dal certificato corrente, come mostrato nell'immagine:

**Generate CSR**

**Common name**

Common name FQDN of Expressway

Common name as it will appear expe.domain.com

Per le SAN, è necessario immettere i valori manualmente nel caso in cui non vengano popolati automaticamente. A tale scopo, è possibile immettere i valori nei **nomi alternativi aggiuntivi**, se si dispone di più SAN, ad esempio devono essere separati da virgole: example1.domain.com, example2.domain.com, example3.domain.com. Una volta aggiunte, le SAN sono elencate nella sezione **Nome alternativo**, come mostrato nell'immagine:

**Alternative name**

Additional alternative names (comma separated)  ⓘ

Unified CM registrations domains  Format DNS ⓘ

Alternative name as it will appear DNS:domain.com

Le **informazioni aggiuntive** sono obbligatorie; se non sono inserite automaticamente o devono essere modificate, devono essere inserite manualmente come mostrato nell'immagine:

Additional information	
Key length (in bits)	4096 <input type="button" value="i"/>
Digest algorithm	SHA-256 <input type="button" value="i"/>
Country	* MX <input type="button" value="i"/>
State or province	* CDMX <input type="button" value="i"/>
Locality (town name)	* CDMX <input type="button" value="i"/>
Organization (company name)	* TAC <input type="button" value="i"/>
Organizational unit	* TAC <input type="button" value="i"/>
Email address	<input type="text"/> <input type="button" value="i"/>

Al termine, selezionare **Genera CSR**.

### Passaggio 3. Verificare e scaricare il nuovo CSR.

Dopo aver generato la CSR, è possibile selezionare **Mostra (decodificato)** nella sezione **Richiesta di firma del certificato (CSR)** per verificare che tutte le SAN siano presenti, come mostrato nell'immagine:

Certificate signing request (CSR)	
Certificate request	<input type="button" value="Show (decoded)"/> <input type="button" value="Show (PEM file)"/> <input type="button" value="Download"/>
Generated on	Apr 20 2020

Nella nuova finestra cercare la **CN** e il **Nome alternativo soggetto**, come mostrato nell'immagine:

#### Certificate Request:

##### Data:

```
Version: 0 (0x0)
Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (4096 bit)
  Modulus:
```

La CN viene sempre aggiunta automaticamente come SAN:

```
X509v3 Extended Key Usage:
  TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
  DNS:expe.domain.com, DNS:domain.com
Signature Algorithm: sha256WithRSAEncryption
```

Una volta verificato il CSR, è possibile chiudere la nuova finestra e selezionare **Download**

(decodificato) nella sezione **CSR (Certificate Signature Request)** come illustrato nell'immagine:

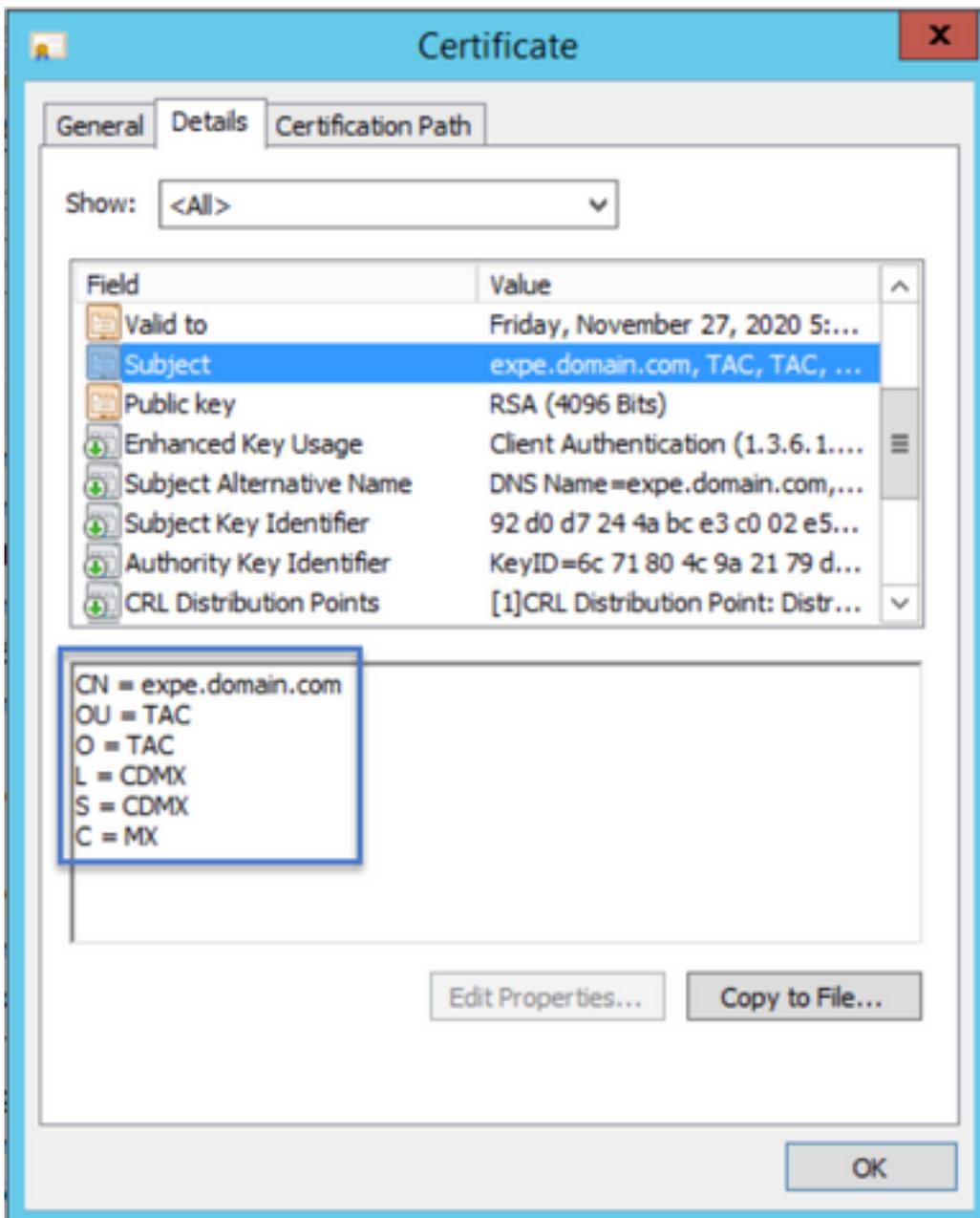


Una volta scaricato, è possibile inviare il nuovo CSR all'autorità di certificazione (CA) da firmare.

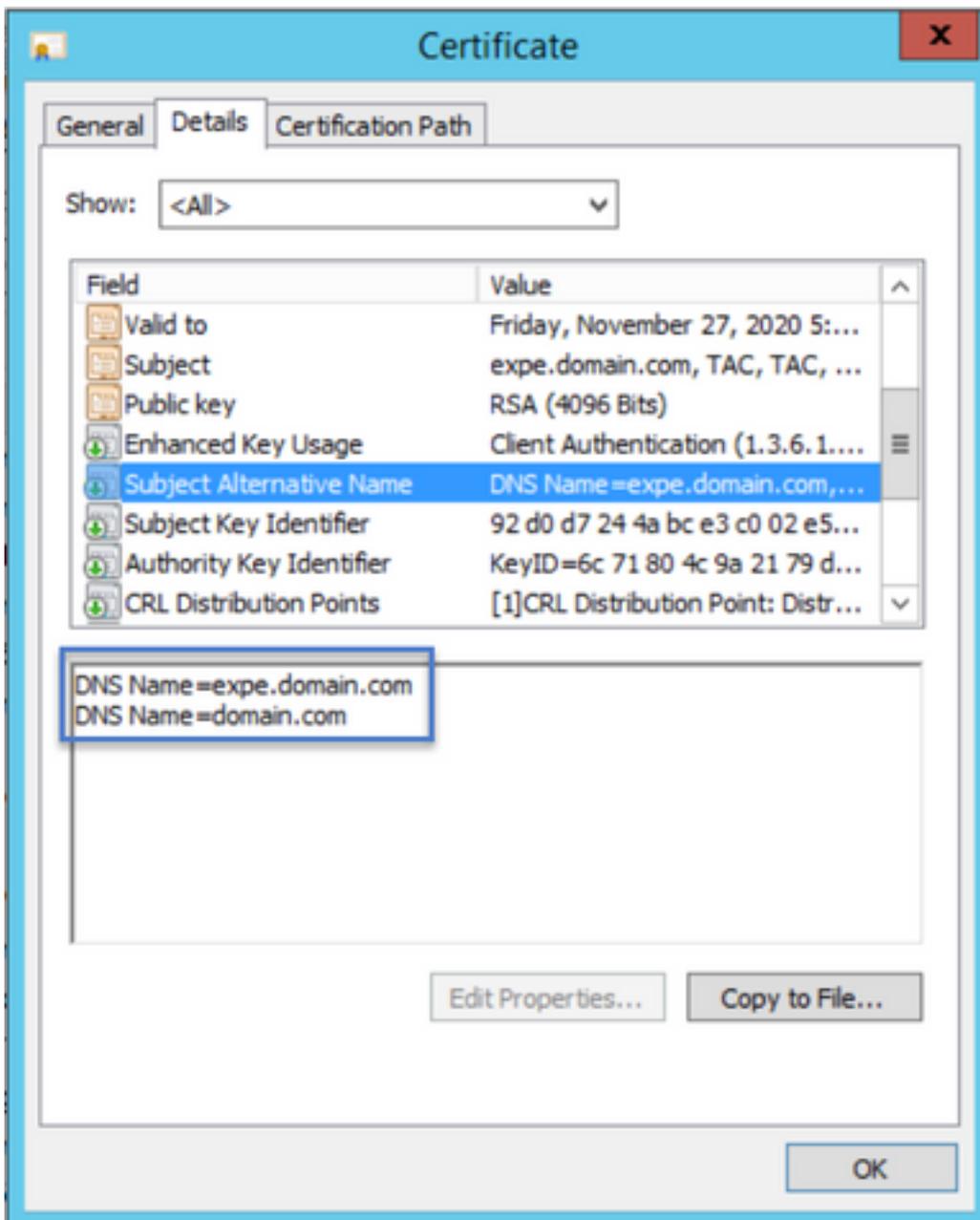
#### **Passaggio 4. Verificare le informazioni contenute nel nuovo certificato.**

Una volta restituito il nuovo certificato dalla CA, è possibile verificare se tutte le SAN sono presenti nel certificato. A tale scopo, è possibile aprire il certificato e cercare gli attributi SAN. In questo documento viene utilizzato un PC Windows per visualizzare gli attributi, non è l'unico metodo a condizione che sia possibile aprire o decodificare il certificato per esaminare gli attributi.

Aprire il certificato, passare alla scheda **Dettagli** e cercare **Oggetto**. Il certificato deve contenere la CN e le Informazioni aggiuntive, come mostrato nell'immagine:



Cercare inoltre la sezione **Nome alternativo soggetto**, che deve contenere le SAN immesse nel CSR, come mostrato nell'immagine:



Se tutte le SAN immesse nel CSR non sono presenti nel nuovo certificato, contattare l'autorità per verificare se sono consentite altre SAN per il certificato.

### **Passaggio 5. Caricare i nuovi certificati CA nell'archivio attendibile dei server, se applicabile.**

Se la CA è la stessa che ha firmato il vecchio certificato di Expressway, è possibile ignorare questo passaggio. Se si tratta di una CA diversa, è necessario caricare i nuovi certificati CA nell'elenco delle CA attendibili in ogni server Expressway. Se sono presenti zone Transport Layer Security (TLS) tra Expressways, ad esempio tra Expressway-C e Expressway-E, è necessario caricare le nuove CA in entrambi i server in modo che possano considerarsi attendibili.

A tale scopo, è possibile caricare i certificati CA uno alla volta. Passare a **Manutenzione > Protezione > Certificati CA attendibili** in Expressway.

1. Selezionare **Sfoglia**.
2. Nella nuova pagina selezionare il certificato CA.
3. Selezionare **Aggiungi certificato CA**.

Questa procedura deve essere eseguita per ogni certificato CA nella catena di certificati (radice e intermedi) e deve essere eseguita in tutti i server Expressway anche se sono cluster.

## Passaggio 6. Caricare il nuovo certificato nel server Expressway.

Se tutte le informazioni nel nuovo certificato sono corrette, per caricare il nuovo certificato passare a: **Manutenzione > Protezione > Certificato server**.

Individuare la sezione **Carica nuovo certificato** come mostrato nell'immagine:

1. Selezionare **Browse** nella sezione **Select the server certificate file** (Seleziona file certificato server).
2. Selezionare il nuovo certificato.
3. Selezionare **Carica dati certificato server**.

The screenshot shows the 'Upload new certificate' section. It includes a header 'Upload new certificate', a note 'System will use the private key file generated at the same time as the CSR.', and two 'Select' fields: 'Select the server private key file' and 'Select the server certificate file'. A 'Browse...' button is next to the second field, with 'ExpECertNew.cer' displayed. Below this is a button labeled 'Upload server certificate data'.

Se il nuovo certificato viene accettato da Expressway, Expressway richiede un riavvio per applicare le modifiche e nel messaggio viene visualizzata la nuova data di scadenza del certificato, come illustrato nell'immagine:

The screenshot shows the 'Server certificate' status page. It features a yellow notification bar with an information icon and the text: 'Files uploaded: Server certificate updated, however a restart is required for this to take effect.' Below this is another yellow bar with 'Certificate info: This certificate expires on Nov 28 2020.' The main section is titled 'Server certificate data' and contains a table with the following data:

Server certificate	Show (decoded)	Show (PEM file)
Currently loaded certificate expires on	Nov 28 2020	
Certificate Issuer	anmiron-SRV-AD-CA	

At the bottom of the page is a button labeled 'Reset to default server certificate'.

Per riavviare Expressway, selezionare **riavvia**.

## Verifica

Una volta che il server è tornato, il nuovo certificato deve essere stato installato, è possibile passare a: **Manutenzione > Protezione > Certificato server** per la conferma.

Individuare i **dati** del **certificato server** e cercare la sezione **Scadenza certificato attualmente**

caricato in, in cui viene visualizzata la nuova data di scadenza del certificato, come illustrato nell'immagine:

**Server certificate**

Server certificate data

Server certificate Show (decoded) Show (PEM file)

Currently loaded certificate expires on **Nov 28 2020**

Certificate Issuer **anmiron-SRV-AD-CA**

Reset to default server certificate

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.