

Rinnova certificato Expressway

Sommario

[Introduzione](#)

[Premesse](#)

[Processo](#)

[A\) Ottenere informazioni dal certificato attuale](#)

[B\) Generare la richiesta di firma del certificato \(CSR\) e inviarla all'autorità di certificazione \(Certification Authority\) per la firma.](#)

[C\) Controllare l'elenco SAN e l'attributo Utilizzo chiavi esteso/avanzato nel nuovo certificato](#)

[D\) Verificare se l'autorità di certificazione che ha firmato il nuovo certificato è la stessa che ha firmato il vecchio certificato](#)

[E\) Installare il nuovo certificato](#)

Introduzione

Questo documento descrive il processo di rinnovo del certificato Expressway/Video Communication Server (VCS).

Premesse

Le informazioni di questo documento si applicano sia a Expressway che a VCS. Il documento fa riferimento a Expressway ma può essere scambiato con VCS.

 Nota: anche se questo documento è stato progettato per semplificare il processo di rinnovo del certificato, è consigliabile consultare anche la [Cisco Expressway Certificate Creation and Use Deployment Guide](#) per la propria versione.

Ogni volta che un certificato deve essere rinnovato, è necessario considerare due punti principali per verificare che il sistema continui a funzionare correttamente dopo l'installazione del nuovo certificato:

1. Gli attributi del nuovo certificato devono corrispondere a quelli del certificato precedente (principalmente il nome soggetto alternativo e l'utilizzo esteso della chiave).
2. L'autorità di certificazione che firma il nuovo certificato deve essere considerata attendibile dagli altri server che comunicano direttamente con Expressway (ad esempio CUCM, Expressway-C, Expressway-E,...).

Processo

A) Ottenere informazioni dal certificato attuale

1. Aprire Manutenzione pagine Web di Expressway > Sicurezza > Certificato server > Mostra decodificato.

2. Nella nuova finestra visualizzata, copiare le estensioni Subject Alternative name e Authority Key Identifier X509v3 in un documento del Blocco note.

```
X509v3 extensions:  
X509v3 Key Usage: critical  
Digital Signature, Key Encipherment  
X509v3 Extended Key Usage:  
TLS Web Server Authentication, TLS Web Client Authentication  
X509v3 Subject Alternative Name:  
DNS:expe.nart.com, DNS:expe2.nart.com, DNS:expe1.nart.com, DNS:guest.vngtpres.aca, DNS:join.nart.com, DNS:meeting.nart.com, DNS:meet.nart.com, DNS:guest.vngtp.aca, DNS:vngtp.lab, DNS:nart.com  
X509v3 Subject Key Identifier:  
BE:72:22:D2:61:D3:4B:FB:44:34:8B:DA:7B:D6:C9:17:14:BB:8C:31  
X509v3 Authority Key Identifier:  
keyid:45:8E:34:17:B0:6E:19:DC:6F:52:65:0F:FC:CB:01:06:18:C2:B6:27
```

Finestra Mostra certificato decodificato

B) Generare la richiesta di firma del certificato (CSR) e inviarla all'autorità di certificazione (Certification Authority) per la firma.

1. Da Manutenzione pagine Web di Expressway > Sicurezza > Certificato server > Genera CSR.

2. Nel campo Nomi alternativi aggiuntivi (separati da virgola) della finestra Genera CSR, immettere tutti i valori per Nomi alternativi soggetto salvati nella sezione A, rimuovere DNS: e separare l'elenco con una virgola.

In questa immagine, accanto al nome alternativo visualizzato, è disponibile un elenco di tutte le SAN da utilizzare nel certificato):

Alternative name

Subject alternative names: None

Additional alternative names (comma separated): expe.nart.com,expe2.nart.com,expe1.nart.com,guest:

Unified CM registrations domains: [Empty]

Alternative name as it will appear: [Empty]

Format: DNS

DNS:expe1.nart.com
DNS:expe.nart.com
DNS:expe2.nart.com
DNS:guest.vngtpres.aca
DNS:join.nart.com
DNS:meeting.nart.com
DNS:meet.nart.com
DNS:guest.vngtp.aca
DNS:vngtp.lab
DNS:nart.com

Genera voci SAN CSR

3. Inserire le altre informazioni nella sezione Ulteriori informazioni (ad esempio, paese, società, stato, ecc.) e fare clic su Genera CSR.

4. Dopo aver generato il CSR, nella pagina Manutenzione > Sicurezza > Certificato server viene visualizzata un'opzione che consente di ignorare il CSR e di scaricare. Scegliere Download e inviare il CSR alla CA per la firma.

 Nota: non eliminare CSR prima dell'installazione del nuovo certificato. Se è stata eseguita l'operazione Elimina CSR e si tenta di installare un certificato firmato con il CSR che è stato

 scartato, l'installazione del certificato avrà esito negativo.

C) Controllare l'elenco SAN e l'attributo Utilizzo chiavi esteso/avanzato nel nuovo certificato

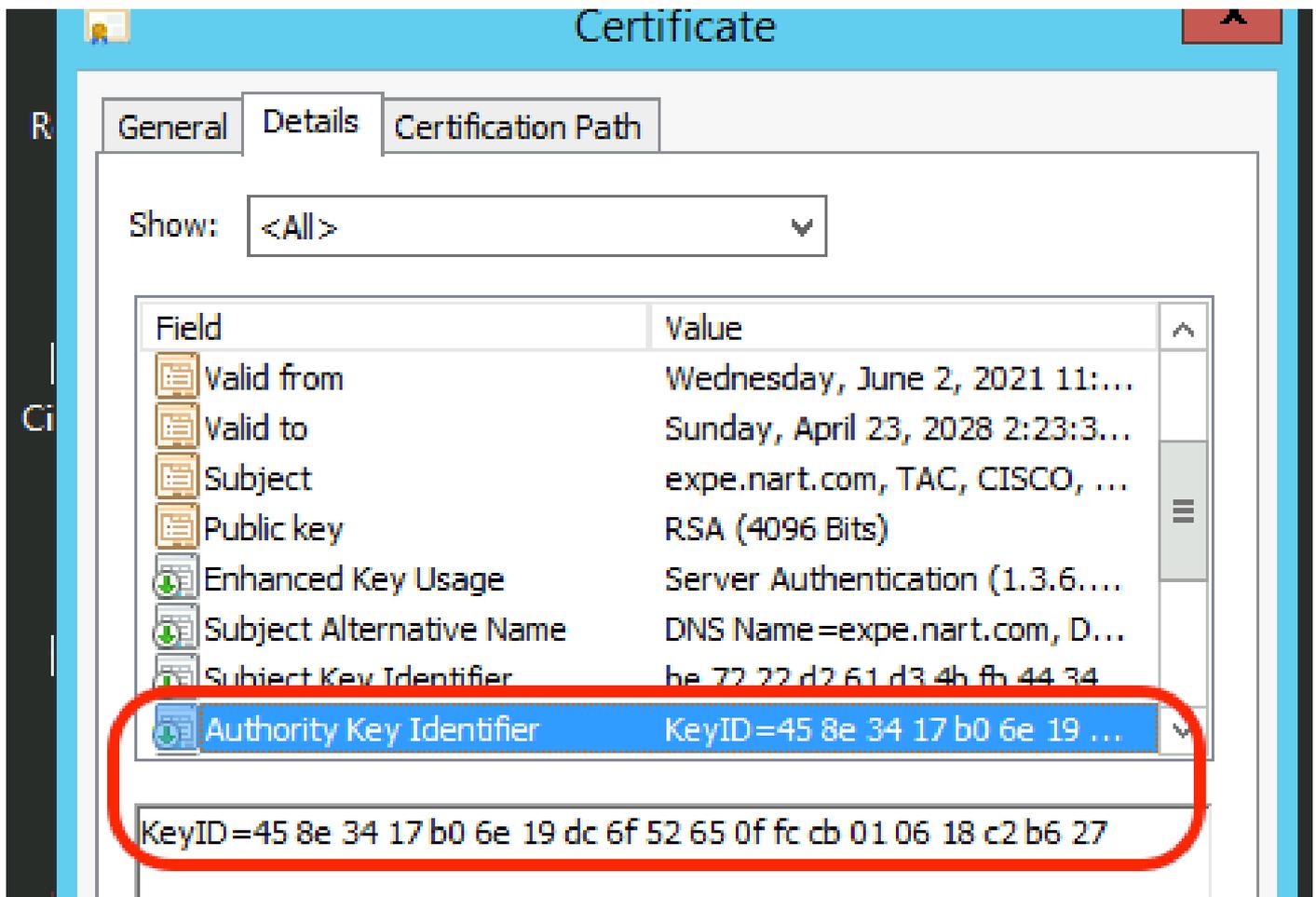
Aprire il certificato appena firmato in Gestione certificati di Windows e verificare quanto segue:

1. L'elenco SAN corrisponde all'elenco SAN salvato nella sezione A utilizzata per generare il CSR.
2. L'attributo "Utilizzo chiave esteso/avanzato" deve includere sia l'autenticazione client che l'autenticazione server.

 Nota: se il certificato ha estensione .pem, rinominarlo in .cer o .crt per aprirlo con Gestione certificati di Windows. Una volta aperto il certificato con Gestione certificati di Windows, è possibile passare alla scheda Dettagli > Copia su file ed esportarlo come file con codifica Base64; un file con codifica Base64 in genere presenta "—BEGIN CERTIFICATE—" nella parte superiore e "—END CERTIFICATE—" nella parte inferiore quando viene aperto in un editor di testo

D) Verificare se l'autorità di certificazione che ha firmato il nuovo certificato è la stessa che ha firmato il vecchio certificato

Aprire il certificato appena firmato in Gestione certificati di Windows, copiare il valore Identificatore chiave autorità e confrontarlo con il valore Identificatore chiave autorità salvato nella sezione A.



Nuovo certificato aperto con Gestione certificati di Windows

Se entrambi i valori sono uguali, significa che per firmare il nuovo certificato è stata utilizzata la stessa CA di quella utilizzata per firmare il vecchio certificato ed è possibile passare alla sezione E per caricare il nuovo certificato.

Se i valori sono diversi, significa che la CA utilizzata per firmare il nuovo certificato è diversa dalla CA utilizzata per firmare il vecchio certificato e le operazioni da eseguire prima di passare alla sezione E sono le seguenti:

1. Ottenere tutti i certificati CA intermedi, se presenti, e il certificato CA radice.
2. Selezionare Manutenzione > Sicurezza > Certificato CA attendibile , fare clic su Sfoglia, quindi cercare il certificato CA intermedio nel computer e caricarlo. Eseguire la stessa operazione per tutti gli altri certificati CA intermedi e per il certificato CA radice.
3. Eseguire la stessa operazione su qualsiasi Expressway-E (se il certificato da rinnovare è un certificato Expressway-C) connesso a questo server o su qualsiasi Expressway-C (se il certificato da rinnovare è un certificato Expressway-E) connesso a questo server.
4. Se il certificato da rinnovare è un certificato Expressway-C e si dispone di MRA o di zone protette per CUCM
 - Verificare che CUCM consideri attendibile la nuova CA radice e intermedia.
 - Caricare i certificati CA radice e intermedia negli archivi CUCM per attendibilità del

catalizzatore e per attendibilità del gestore chiamate.

- Riavviare i relativi servizi su CUCM.

E) Installare il nuovo certificato

Dopo aver controllato tutti i punti precedenti, è possibile installare il nuovo certificato in Expressway scegliendo Manutenzione > Protezione > Certificato server.

Fare clic su Sfoglia e selezionare il nuovo file di certificato dal computer e caricarlo.

È necessario riavviare Expressway dopo aver installato un nuovo certificato.

 Nota: verificare che il certificato da caricare in Expressway da Manutenzione > Sicurezza > Certificato server contenga solo il certificato del server Expressway e non la catena di certificati completa e verificare che sia un certificato Base64.

Aggiunta di un singolo certificato a più espressioni:

- Creare un singolo certificato per l'intero cluster expressway-e.
- Creare un CSR che contenga tutti gli FQDN più le funzioni aggiuntive che si utilizzano sulle superstrade (se CMS webrtc, l'URL di join e il dominio, se MRA, le registrazioni/domini di login)

Esempio:

Exwycluster.dominio

Exwy1.domain

Exwy2.domain

Exwy3.domain

Exwy4.domain

Funzionalità aggiuntive (domini o URL CMS)

- Al termine della CSR, è possibile estrarre la chiave privata di questo CSR utilizzando un programma SFTP (vi consiglio WinSCP, lo usiamo molto)
- Aprire WinSCP e connettersi a expressway-e che ha creato il CSR
- Passare a tandberg/persistent/certs/ CSR o alla richiesta di firma del certificato (potrebbe essere visualizzato o in sospeso)
- Copiare la chiave privata da expressway-e sul desktop,
- Al termine dell'operazione, sarà possibile utilizzare lo stesso certificato per tutti i 4 nodi.

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).