Rinnova certificato Expressway

Sommario

Introduzione

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

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 progettato per agevolare il processo di rinnovo del certificato, è consigliabile consultare anche la Cisco Expressway Certificate Creation and Use Deployment Guide per la propria versione.

Premesse

Ogni volta che un certificato deve essere rinnovato, è necessario prendere in considerazione due punti principali per garantire 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 (CA) da utilizzare per firmare il nuovo certificato deve essere considerata attendibile dagli altri server che comunicano direttamente con Expressway (ad esempio CUCM, Expressway-C, Expressway-E, ecc.)

Processo

A) Ottenere informazioni dal certificato attuale

1. Aprire Expressway Web Page **Maintenance > Security > Server certificate > Show decoded.**

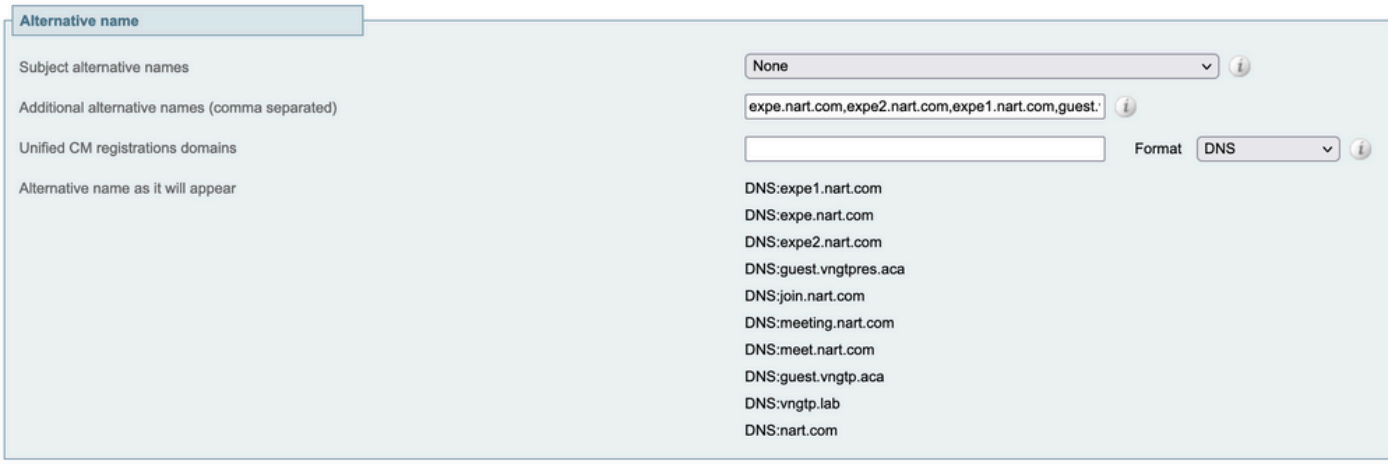
2. Nella nuova finestra visualizzata, copiare le estensioni "Subject Alternative name" e "Authority Key Identifier" X509v3 in un documento del Blocco note.

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 e assicurarsi di rimuovere "DNS:" e separare l'elenco con una virgola, vedere l'immagine (accanto a "Nome alternativo come verrà visualizzato" è possibile visualizzare un elenco di tutte le SAN da utilizzare nel certificato):



Genera voci SAN CSR

3. Completare le altre informazioni nella sezione **Ulteriori informazioni**, ad esempio paese, società, stato e così via e fare clic su **Genera CSR.**

4. Una volta generato il CSR, nella pagina **Manutenzione > Sicurezza > Certificato server** viene visualizzata un'opzione che consente di **ignorare il CSR** e di eseguire il **download**, è necessario scegliere **Scarica** e inviare il CSR alla CA per la firma.

> **Nota:** Assicurarsi di non **eliminare CSR** prima di installare il nuovo certificato, se **si** è tentato di installare un certificato firmato con CSR che è stato scartato, l'installazione del certificato non riuscirà.

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:

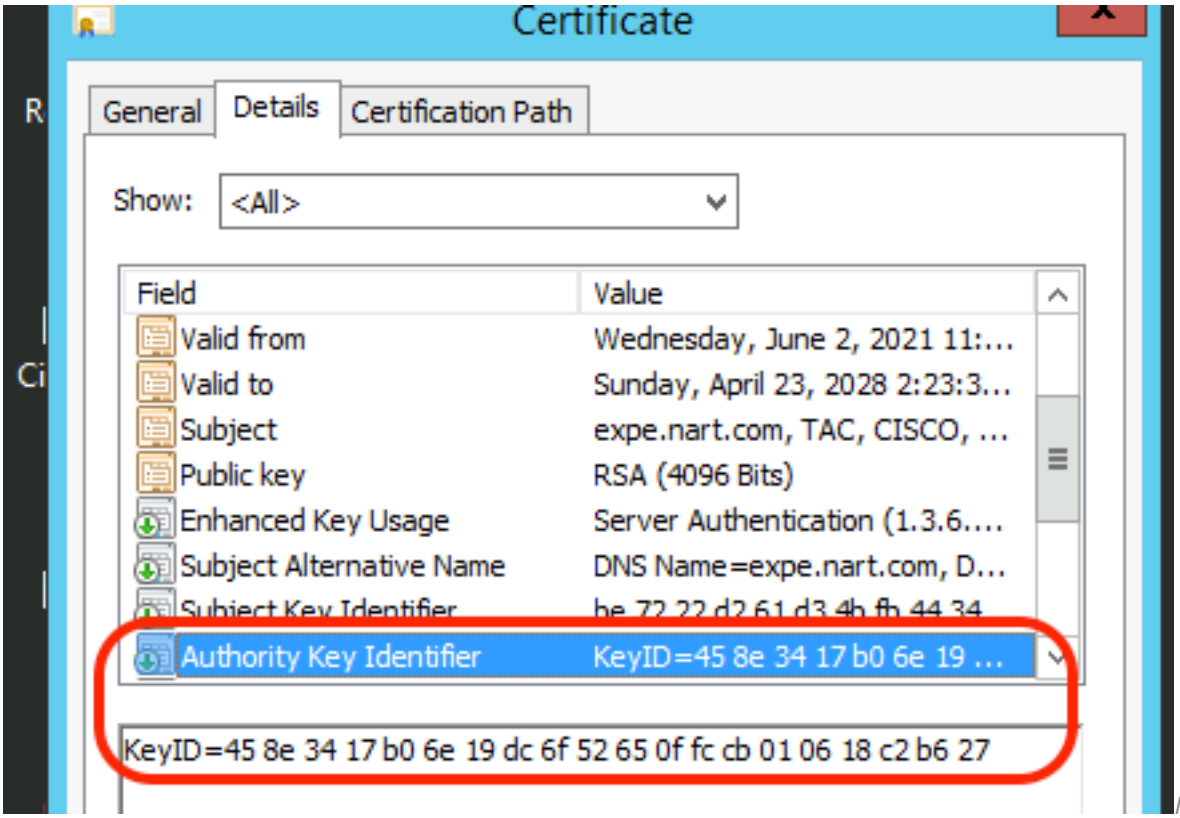
1. L'elenco SAN corrisponde all'elenco SAN salvato nella sezione A utilizzata per generare il CSR.

2. L'attributo "Utilizzo chiavi avanzato/esteso" deve includere sia "Autenticazione client" che "Autenticazione server".

> **Nota:** Se il certificato ha l'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 la CA 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 i passaggi da seguire prima di procedere alla sezione E sono:

1. Ottenere tutti i certificati CA intermedi (se disponibili) 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) che si connette a questo server o su qualsiasi Expressway-C (se il certificato da rinnovare è un certificato Expressway-E) che si connette 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, è necessario verificare che CUCM consideri attendibile la nuova CA radice e intermedia e caricare i certificati CA radice e intermedia negli archivi CUCM-cat-trust e callmanager-trust e riavviare i servizi pertinenti in CUCM.

E) Installare il nuovo certificato

Dopo aver controllato tutti i punti precedenti, è possibile installare il nuovo certificato in Expressway da **Manutenzione > Sicurezza > Certificato server** fare clic su **Sfoglia** e selezionare il nuovo file di certificato dal computer e caricarlo.

Ènecessario riavviare Expressway dopo aver installato un nuovo certificato.

> **Nota:** Verificare che il certificato caricato in Expressway da **Manutenzione > Sicurezza > Certificato server** contenga solo il certificato del server Expressway e NON la catena di certificati completa e che il relativo certificato Base64

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).