Verlengen expressway-certificaat

Inhoud

Inleiding

Dit document beschrijft het proces voor de verlenging van het certificaat voor Expressway/Video Communication Server (VCS).

De informatie in dit document is van toepassing op zowel Expressway als VCS. De documentreferenties Expressway maar dit kan worden uitgewisseld met VCS.

> **Opmerking:** Hoewel dit document is ontworpen om u te helpen met het proces voor de verlenging van het certificaat, is het een goed idee om ook de gids voor de creatie en implementatie van Cisco Expressway-certificaat voor uw versie te controleren.

Achtergrondinformatie

Wanneer een certificaat moet worden vernieuwd, zijn er twee hoofdpunten die in aanmerking moeten worden genomen om ervoor te zorgen dat het systeem naar behoren blijft functioneren nadat het nieuwe certificaat is geïnstalleerd:

1. De kenmerken van het nieuwe certificaat moeten overeenkomen met die van het oude certificaat (hoofdzakelijk de alternatieve onderwerpnaam en het gebruik van de uitgebreide sleutel)

2. De CA(Certification Authority) die moet worden gebruikt voor de ondertekening van het nieuwe certificaat moet worden vertrouwd door andere servers die rechtstreeks communiceren met de Expressway (bijvoorbeeld CUCM, Expressway-C, Expressway-E..etc)

Proces

A) Ontvang informatie van het huidige certificaat

1. Open Expressway Webpage **Onderhoud > Beveiliging > Servercertificaat > Gedecodeerd tonen.**

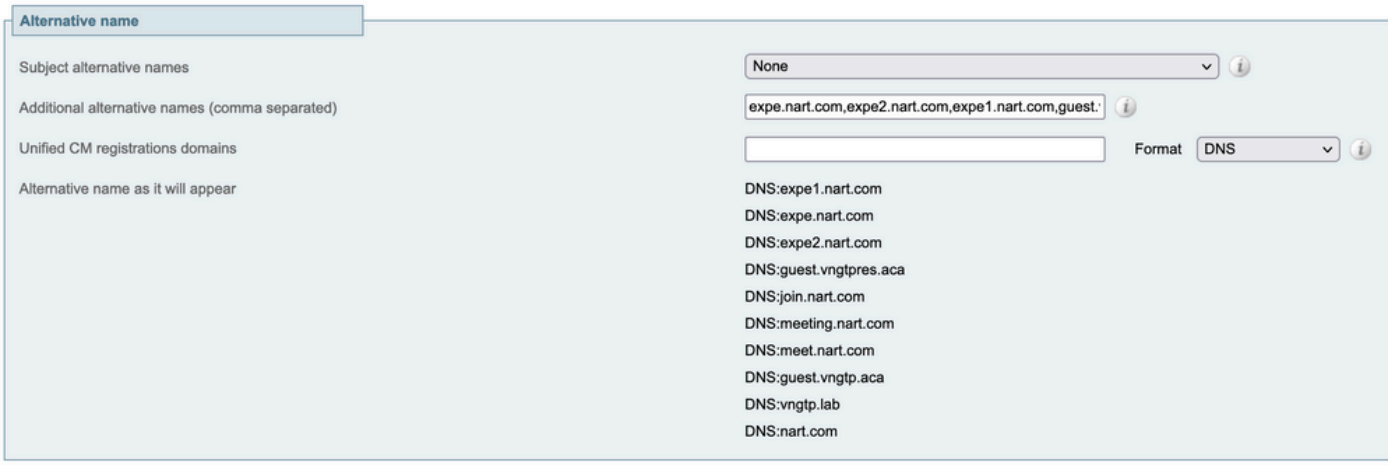
2. Kopieer in het nieuwe venster de extensies "Onderwerp Alternatieve naam" en "Authority Key Identifier" X509v3 naar een notitieblok document.

venster voor "gedecodeerd" certificaat tonen

B) Genereert de CSR(Certificate Signing Request) en stuurt deze voor ondertekening naar de CA(Certification Authority).

1. Van Expressway Webpage **Onderhoud > Beveiliging > Servercertificaat > MVO genereren.**

2. In het venster Generate CSR vul in het veld **Aanvullende alternatieve namen (komma gescheiden)** alle waarden in voor "Onderwerp alternatieve namen" die we in sectie A hebben opgeslagen, en zorg ervoor dat u "DNS:" verwijdert en de lijst met komma's scheidt, zie afbeelding (naast "Alternatieve naam zoals deze zal verschijnen" kunt u een lijst zien van alle SAN's die in het certificaat moeten worden gebruikt):



MVO SAN-vermeldingen genereren

3. Vul de rest van de informatie in onder de sectie **Aanvullende informatie** zoals land, bedrijf, staat... en klik op **Generate CSR.**

4. Zodra u de CSR hebt gegenereerd, wordt op de pagina **Maintenance > Security > Server Certificate** een optie getoond om **CSR** en **Download** te **verwijderen**, moet u **Download** kiezen en de CSR naar CA sturen voor ondertekening.

> **Opmerking:** Zorg ervoor dat u **CSR** niet **verwerpt** voordat het nieuwe certificaat is geïnstalleerd, als **verwerping CSR** is gedaan en vervolgens een poging wordt gedaan om een certificaat te installeren dat is ondertekend met de CSR dat is verwijderd, het certificaat is niet geïnstalleerd.

C) Controleer de SAN-lijst en het kenmerk Extended/Enhanced Key Use in het nieuwe certificaat

Open het nieuwe certificaat in Windows-certificaatbeheer en controleer op:

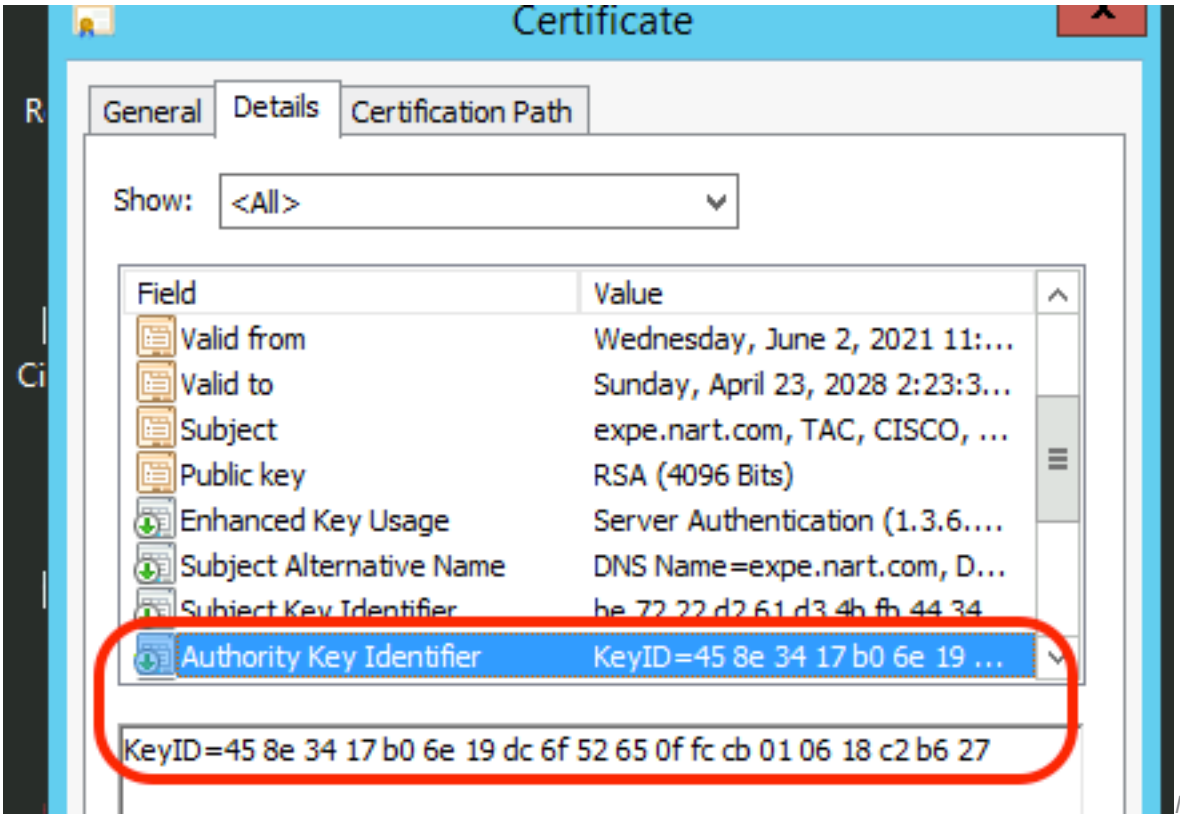
1. De SAN-lijst komt overeen met de SAN-lijst die we hebben opgeslagen in de sectie A die we hebben gebruikt voor de CSR.

2. Het kenmerk "Extended/Enhanced Key Use" moet zowel "Clientverificatie" als "Serververificatie" omvatten.

> **Opmerking:** Als het certificaat de extensie .pem heeft, hernoem het dan naar .cer of .crt om het te kunnen openen met Windows Certificate Manager. Zodra het certificaat is geopend met Windows Certificate Manager, kunt u naar het tabblad **Details > Kopiëren naar bestand** gaan en het als een Base64 gecodeerd bestand exporteren, een base64 gecodeerd bestand heeft normaal gesproken "-----BEGIN CERTIFICAAT-----" bovenaan en "-----END CERTIFICAAT-----" onderaan wanneer geopend in een teksteditor

D) Controleer of de CA die het nieuwe certificaat heeft ondertekend, dezelfde is als de CA die het oude certificaat heeft ondertekend

Open het nieuwe certificaat in Windows-certificaatbeheer en kopieer de waarde "Authority Key Identifier" en vergelijk deze met de waarde "Authority Key Identifier" die we in sectie A hebben opgeslagen.



Nieuw certificaat geopend met Windows-certificaatbeheer

Als beide waarden hetzelfde zijn, betekent dit dat dezelfde CA is gebruikt om het nieuwe certificaat te ondertekenen als de CA die is gebruikt om het oude certificaat te ondertekenen, en kunt u verdergaan naar deel E om het nieuwe certificaat te uploaden.

Als de waarden verschillend zijn, betekent dit dat CA die wordt gebruikt om het nieuwe certificaat te ondertekenen verschillend is dan CA die wordt gebruikt om het oude certificaat te ondertekenen, en de stappen die u moet volgen alvorens u aan sectie E kunt verdergaan zijn:

1. Ontvang alle tussenliggende CA-certificaten en het root CA-certificaat.

2. Ga naar **Onderhoud > Beveiliging > Betrouwbaar CA-certificaat**, klik op **Bladeren** en zoek vervolgens naar het tussenliggende CA-certificaat op uw computer en upload het. Doe hetzelfde voor alle andere tussenliggende CA-certificaten en het root CA-certificaat.

3. Doe hetzelfde op een Expressway-E (als het certificaat dat verlengd moet worden een Expressway-C certificaat is) die verbinding maakt met deze server of op een Expressway-C (als het certificaat dat vernieuwd moet worden een Expressway-E certificaat is) die verbinding maakt met deze server.

4. Als het te vernieuwen certificaat een Expressway-C certificaat is en u MRA hebt of beveiligde zones hebt naar CUCM, moet u ervoor zorgen dat CUCM vertrouwt op de nieuwe wortel en tussenpersoon CA en de wortel en tussenpersoon CA certificaten uploaden naar CUCM tomcat-trust en callmanager-trust winkels en de herstart van de relevante services op CUCM.

E) Installeer het nieuwe certificaat

Nadat alle vorige punten zijn gecontroleerd, kunt u nu het nieuwe certificaat installeren op de snelweg van **Onderhoud > Beveiliging > Servercertificaat** klik op **Bladeren** en selecteer het nieuwe certificaatbestand van uw computer en upload het.

U moet de Expressway opnieuw opstarten nadat u een nieuw certificaat installeert.

> **Opmerking:** Zorg ervoor dat het certificaat dat u uploadt naar Expressway van **Onderhoud > Beveiliging > Servercertificaat** alleen het Expressway-servercertificaat en NIET de volledige certificaatketen bevat en zorg ervoor dat het een Base64-certificaat bevat

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.