Probleemoplossing voor expresswaycertificaten

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten
- Achtergrondinformatie
  - Definities
  - Grondbeginsel

Veelvoorkomende problemen

- Uploaden van expresswaycertificaten mislukt
- Traverse Zone omlaag met fout TLS-onderhandelingsfout
- Traverse Zone omhoog maar SSH-tunnels omlaag na een certificaatverlenging
- Aanmelden bij mobiele en externe toegang mislukt na een upgrade of verlenging van het certificaat
- Certificaatalarm bij Jabber bij aanmelding van mobiele en externe toegang

Gerelateerde informatie

Inleiding

Dit document beschrijft hoe certificaten werken en de meest voorkomende problemen en tips voor certificaten in Expressway-servers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- VCS-servers (Expressway- en Video Communications Server)
- Secure Sockets Layer (SSL)
- Certificaten
- TelePresence-apparaten
- Mobiele en externe toegang
- Implementaties van collaboration

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Expressway x14

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SSL en Certificaten zijn een standaard en werken hetzelfde voor andere apparaten en merken. Dit document concentreert zich op het certificaatgebruik in Expressways.

Definities

Certificaten worden gebruikt om een veilige verbinding tussen twee apparaten tot stand te brengen. Ze zijn een digitale handtekening die een server of apparaat-identiteit authenticeert. Sommige protocollen zoals HTTPS (Hypertext Transfer Protocol) of SIP (Session Initiation Protocol) Transport Layer Security (TLS) vereisen het gebruik van certificaten om te kunnen functioneren.

Verschillende termen die worden gebruikt wanneer u over certificaten spreekt:

- Certificaat-Ondertekeningsaanvraag (CSR): een sjabloon gemaakt met de namen die een apparaat identificeren om later te worden ondertekend en omgezet in een client- of servercertificaat
- Certificaat: een MVO dat is ondertekend. Dit is een type identiteit en is geïnstalleerd op een apparaat voor gebruik bij SSL onderhandelingen. Zij kunnen door henzelf of door een certificeringsinstantie worden ondertekend.
- Handtekening van het certificaat: de identiteit waarmee het certificaat in kwestie wordt geverifieerd, is legitiem; deze wordt in de vorm van een ander certificaat gepresenteerd.
- Zelfondertekend Certificaat: een client- of servercertificaat dat door zichzelf is ondertekend
- Certificaatautoriteit (CA): entiteit die certificaten ondertekent
    - Intermediate Certificate: CA-certificaat dat niet door zichzelf maar door een ander CA-certificaat is ondertekend, gewoonlijk ondertekend door een Root Certificate, maar kan ook door een ander Intermediate Certificate worden ondertekend
    - Root Certificaat: CA Certificaat dat door zichzelf is ondertekend

Grondbeginsel

Wanneer een client met een server praat en een SSL-gesprek start, ruilen ze certificaten uit, die later worden gebruikt om verkeer tussen de apparaten te versleutelen. Als deel van de uitwisseling, bepalen de apparaten ook of de certificaten worden vertrouwd op. Er moet aan meerdere voorwaarden worden voldaan om te bepalen of een certificaat wordt vertrouwd, sommige zijn:

- De volledig gekwalificeerde domeinnaam (FQDN) die aanvankelijk wordt gebruikt om contact op te nemen met de server, komt overeen met een naam in het certificaat dat door de server wordt aangeboden.
    - Wanneer u bijvoorbeeld een webpagina opent in een browser, lost cisco.com het IP

van een server op die een certificaat verstrekt, dat cisco.com als naam moet bevatten om te kunnen worden vertrouwd.

- Het CA-certificaat dat het servercertificaat ondertekende dat door de server wordt aangeboden (of hetzelfde servercertificaat als het zelfondertekende certificaat) is aanwezig in de CA Trusted Certificate-lijst van het apparaat.
  - Apparaten hebben een lijst met CA-certificaten die worden vertrouwd, computers bevatten vaak een vooraf samengestelde lijst met bekende openbare certificeringsinstanties.

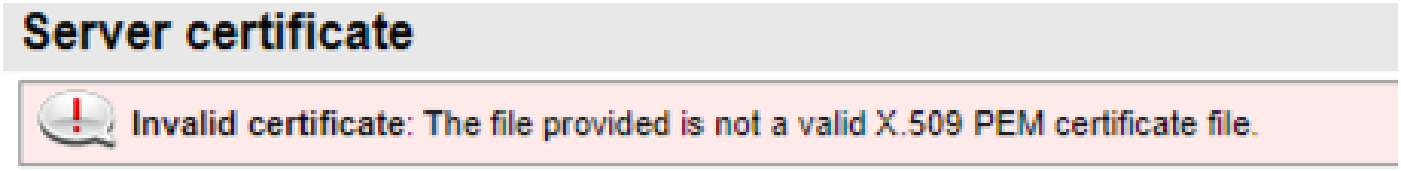
- De huidige datum en het huidige tijdstip vallen binnen de geldigheidsperiode van het certificaat.
  - Certificaatautoriteiten ondertekenen alleen CSR's voor een bepaalde tijd, dit wordt bepaald door de bevoegde autoriteit.

- Het certificaat wordt niet ingetrokken.
  - Openbare certificeringsinstanties nemen vaak een URL voor de intrekkingslijst van certificaten op in het certificaat. Dit is zo dat de partij die het certificaat ontvangt kan bevestigen dat het niet is ingetrokken door de CA.

Veelvoorkomende problemen

Uploaden van expresswaycertificaten mislukt

Er zijn een paar voorwaarden die dit kunnen veroorzaken. Ze veroorzaken een andere beschrijvende fout.



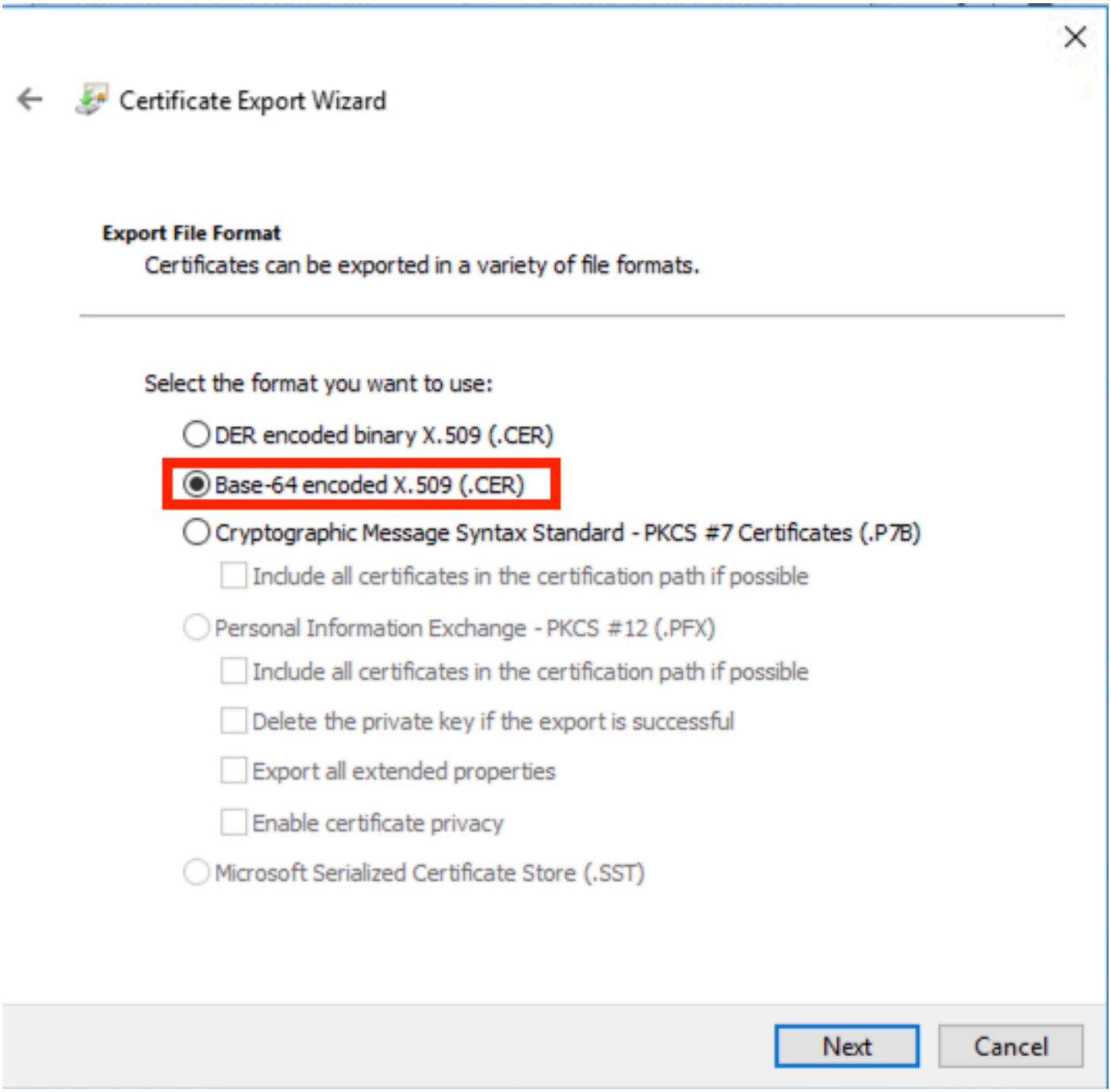
Ongeldige certificaatindeling

Deze eerste fout treedt op wanneer het certificaat niet in een geldig formaat is. De bestandsextensie is niet belangrijk.

Als het certificaat niet wordt geopend, kan er in het juiste formaat een nieuw certificaat worden aangevraagd bij de bevoegde instantie

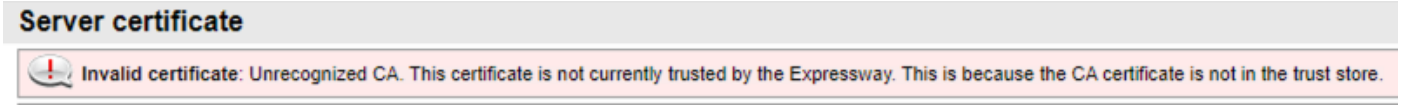
Als het certificaat niet wordt geopend, volgt u de volgende stappen:

Stap 1. Open het certificaat en navigeer naar het tabblad Details.
Stap 2. Selecteer Kopiëren naar bestand.
Stap 3. Volg de wizard en controleer of Base-64 encoded is geselecteerd.



Selecteren van certificaatindeling

Stap 4. Nadat u het bestand hebt opgeslagen, kunt u het uploaden naar de Expressway.



Onbetrouwbare CA-certificaatketen

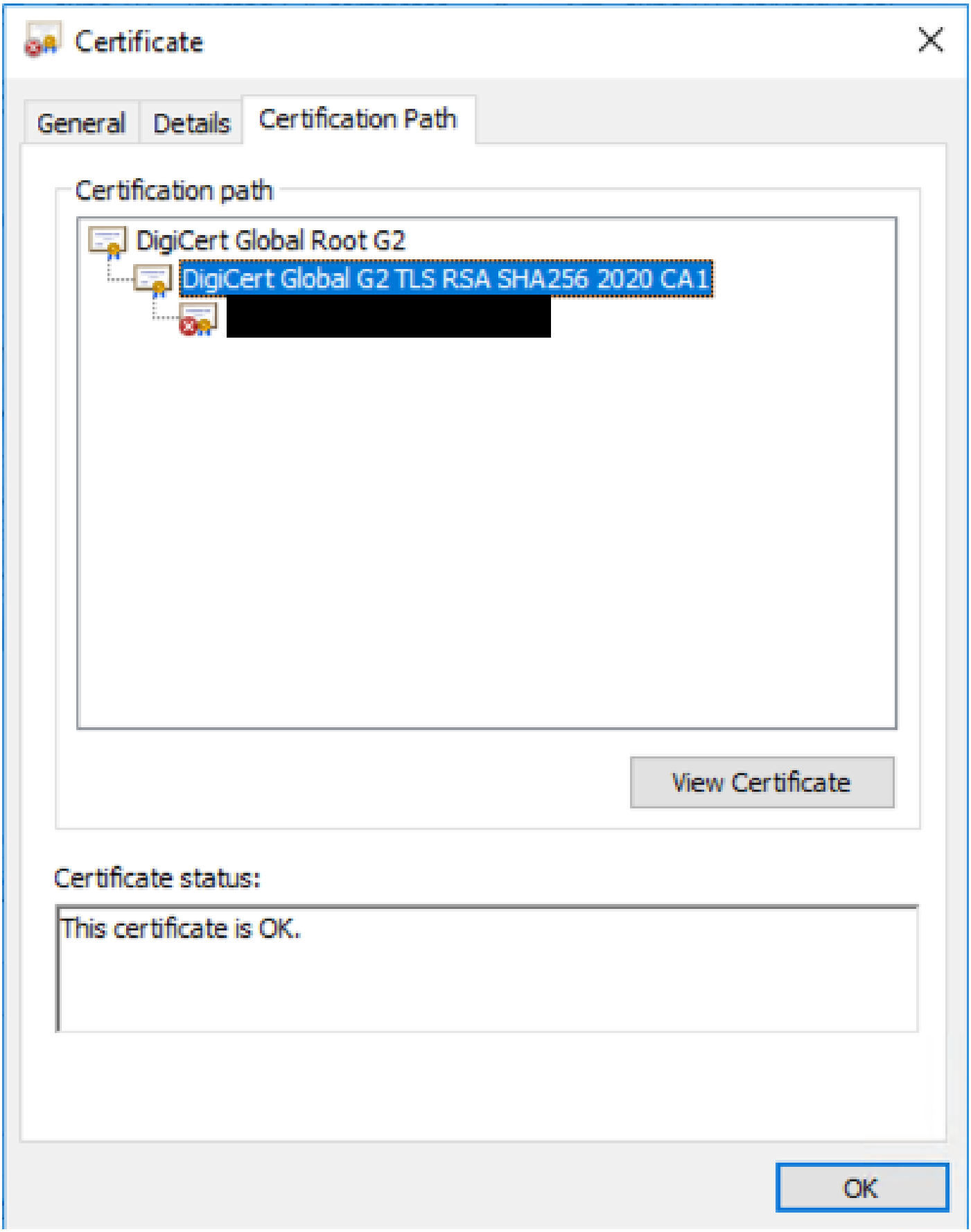
Deze fout treedt op wanneer de CA-certificaten die het servercertificaat hebben ondertekend, niet worden vertrouwd. Voordat u een servercertificaat uploadt, moet de server alle CA-certificaten in de keten vertrouwen.

Normaal verstrekt CA de certificaten van CA samen met het ondertekende servercertificaat. Als

deze beschikbaar zijn, gaat u verder met stap 6 hieronder.

Als de CA-certificaten niet beschikbaar zijn, kunnen deze worden verkregen bij het servercertificaat. Ga als volgt te werk:

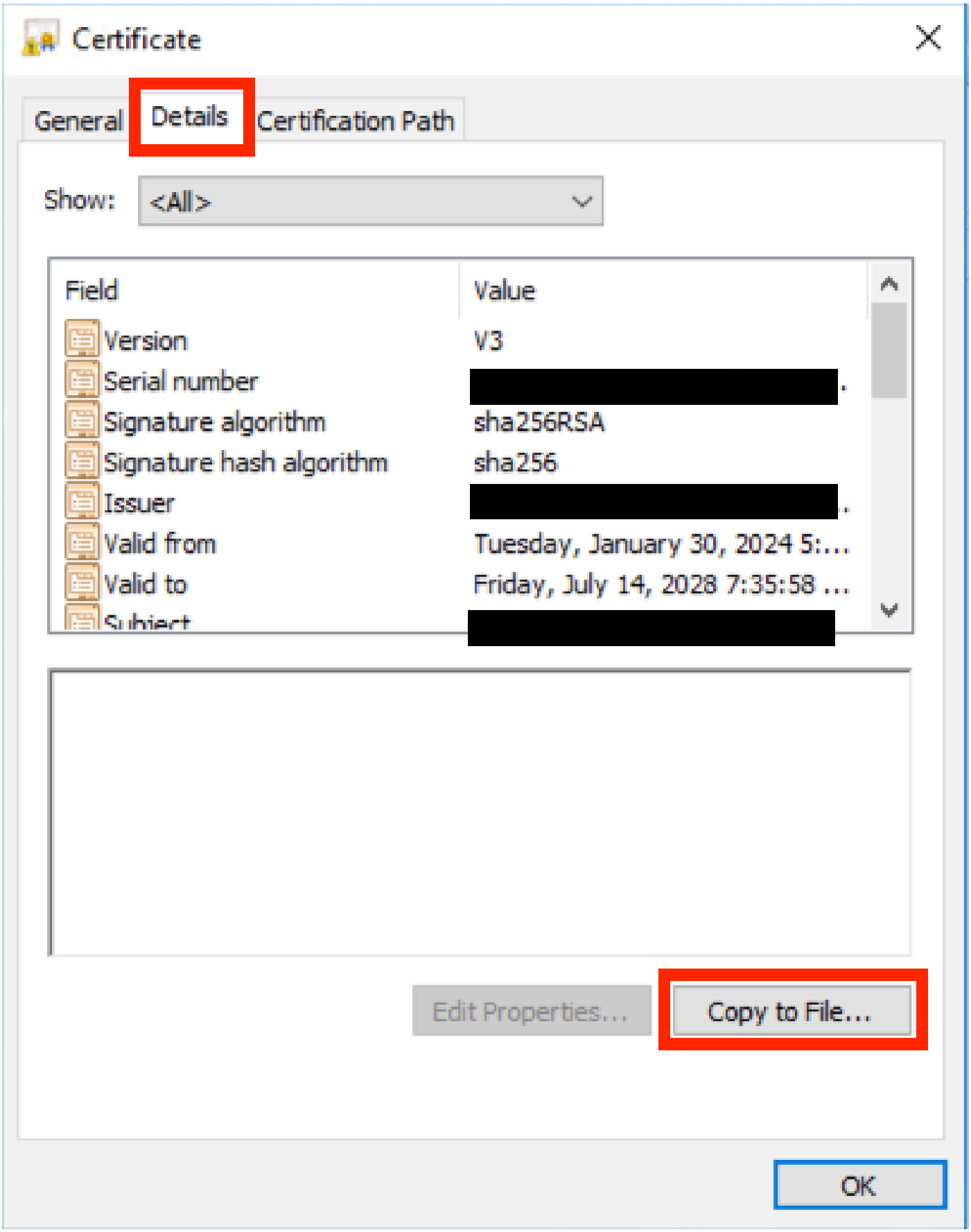
Stap 1. Open het servercertificaat.
Stap 2. Navigeer naar het tabblad Certificeringspad. Het hoogste certificaat wordt beschouwd als het basiscertificaat van CA. De onderste is het servercertificaat en alles daartussen wordt beschouwd als Tussentijdse CA-certificaten.
Stap 3. Kies een CA-certificaat en selecteer Certificaat bekijken.



Certificeringspad

Stap 4. Navigeer naar het tabblad Details en volg de vorige stappen om het certificaat op te slaan

in een afzonderlijk bestand.
Stap 5. Herhaal deze stappen voor alle CA-certificaten die aanwezig zijn.



Tabblad Certificaatgegevens

Zodra alle CA-certificaten beschikbaar zijn, kunt u deze uploaden naar de Expressway Trusted CA-certificaatlijst:

Stap 6. Ga naar Onderhoud > Beveiliging > Betrouwbaar CA-certificaat op de Expressway-server.
Stap 7. Selecteer Bestand kiezen en uploaden.
Stap 8. Herhaal stap 7 voor elk CA-certificaat.
Stap 9. Nadat alle CA-certificaten zijn geüpload op de vertrouwenslijst, kunt u het servercertificaat uploaden naar de server.

Traverse Zone omlaag met fout TLS-onderhandelingsfout

Deze fout treedt op wanneer de SSL-uitwisseling tussen Expressway-C en Expressway-E niet met succes is voltooid. Een paar voorbeelden die dit kunnen veroorzaken:

- De hostnaam komt niet overeen met een naam in het gepresenteerde certificaat.
  - Zorg ervoor dat het peer-adres dat is geconfigureerd op de Expressway-C traverse zone overeenkomt met ten minste een van de namen op het Expressway-E-servercertificaat
- De TLS verify-naam komt niet overeen met een naam in het gepresenteerde certificaat.
  - Zorg ervoor dat de TLS verify-naam die is geconfigureerd in de snelweg-E-zone overeenkomt met een van de namen op het Expressway-C-servercertificaat. Als het om een clusterconfiguratie gaat, wordt aanbevolen om de Expressway-C-cluster FQDN als TLS te configureren. Controleer de naam zoals deze naam op alle knooppunten van het cluster aanwezig moet zijn.
- De CA-certificaten worden niet vertrouwd door de servers
  - Net zoals elke server zijn eigen CA-certificaten moet vertrouwen voordat u het servercertificaat erop uploadt, moeten andere servers ook vertrouwen op die CA-certificaten om het servercertificaat te vertrouwen. Hiervoor dient u ervoor te zorgen dat alle CA-certificaten van het certificatiepad van beide Expressway-servers aanwezig zijn op de vertrouwde CA-lijst van alle betrokken servers. De CA-certificaten kunnen worden geëxtraheerd met de stappen die eerder in dit document zijn vermeld.

Traverse Zone omhoog maar SSH-tunnels omlaag na een certificaatverlenging

SSH-tunnelfout

Deze fout gebeurt vaak na een certificaatvernieuwing wanneer een of meer van de tussentijdse CA-certificaten niet worden vertrouwd, de Root CA-certificaatvertrouwen maakt de transversale zoneverbinding mogelijk, maar de SSH-tunnels zijn een gedetailleerdere verbinding en kunnen falen wanneer de gehele keten niet wordt vertrouwd, tussentijdse CA-certificaten worden vaak gewijzigd door certificeringsinstanties, zodat de vernieuwing van een certificaat dit probleem kan

veroorzaken. Zorg ervoor dat alle tussenliggende CA-certificaten op alle Expressway-vertrouwenslijsten zijn geüpload.

Aanmelden bij mobiele en externe toegang mislukt na een upgrade of verlenging van het certificaat

Er zijn vele manieren waarin een login wegens certificaten kan ontbreken maar op recentere versies van software Expressway werden sommige softwareveranderingen uitgevoerd die, om veiligheidsredenen, certificaatcontrole dwingen waar het niet voordien werd gedaan.

Dit wordt hier beter uitgelegd: Traffic Server dwingt certificaatverificatie af

Als de tijdelijke oplossing is ingesteld, zorg ervoor dat de Expressway-C CA-certificaten op de Cisco Unified Communications Manager zijn geüpload als tomcat-trust en CallManager-trust en start de vereiste services opnieuw.

Certificaatalarm bij Jabber bij aanmelding van mobiele en externe toegang

Jabber onbetrouwbare certificaatwaarschuwing

Dit gedrag gebeurt wanneer het domein dat op de applicatie wordt gebruikt, niet overeenkomt met een alternatieve onderwerpnaam op het Expressway-E servercertificaat.
Zorg ervoor dat het voorbeeld .com of de alternatieve collab-edge.voorbeeld .com is een van de alternatieve onderwerpnamen op het certificaat.

Gerelateerde informatie

Cisco Technical Support en downloads

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.