Risoluzione dei problemi relativi ai certificati Expressway

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
  - Premesse
    - Definizioni
    - Principio di base
- Problemi comuni
  - Caricamento del certificato Expressway non riuscito
  - Area trasversale inattiva con errore Errore di negoziazione TLS
  - Area trasversale attiva ma SSH tunnel inattiva dopo un rinnovo del certificato
  - Accesso a Mobile e Remote Access non riuscito dopo un aggiornamento o un rinnovo del certificato
  - Avviso certificato su Jabber all'accesso di Mobile e Remote Access
- Informazioni correlate

Introduzione

In questo documento viene descritto il funzionamento dei certificati e vengono forniti i problemi e i suggerimenti più comuni per i certificati nei server Expressway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server Expressway e Video Communications Server (VCS)
- SSL (Secure Sockets Layer)
- Certificati
- Dispositivi Di Telepresenza
- Accesso mobile e remoto
- Implementazioni Collaboration

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Expressway x14

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.

Premesse

SSL e Certificati sono uno standard e funzionano allo stesso modo su altri dispositivi e marchi. In questo documento viene illustrato l'utilizzo del certificato in Expressways.

Definizioni

I certificati vengono utilizzati per creare una connessione protetta tra due dispositivi. Si tratta di una firma digitale che autentica l'identità di un server o di un dispositivo. Alcuni protocolli, ad esempio HTTPS (Hypertext Transfer Protocol Secure) o TLS (Session Initiation Protocol), richiedono l'utilizzo di certificati per funzionare.

Termini diversi utilizzati per i certificati:

- Richiesta di firma del certificato (CSR): modello creato con i nomi che identificano un dispositivo per poterlo successivamente firmare e convertire in un certificato client o server
- Certificato: un CSR firmato. Si tratta di un tipo di identità installato in un dispositivo per l'utilizzo nelle negoziazioni SSL. Possono essere firmati da soli o da un'autorità di certificazione.
- Firma certificato: l'identità che verifica il certificato in questione è legittima e viene presentata sotto forma di un altro certificato.
- Certificato autofirmato: un certificato client o server firmato da se stesso
- CA (Certification Authority): entità che firma certificati
    - Certificato intermedio: certificato CA non firmato da se stesso ma da un altro certificato CA, in genere firmato da un certificato radice ma che può essere firmato anche da un altro certificato intermedio.
    - Certificato radice: certificato CA firmato da se stesso

Principio di base

Quando un client comunica con un server e avvia una conversazione SSL, scambia certificati, che vengono utilizzati successivamente per crittografare il traffico tra i dispositivi. Come parte dello scambio, i dispositivi determinano anche se i certificati sono attendibili. Per stabilire se un certificato è attendibile, è necessario che siano soddisfatte più condizioni, ad esempio:

- Il nome di dominio completo (FQDN) inizialmente utilizzato per contattare il server corrisponde a un nome all'interno del certificato presentato dal server.
    - Ad esempio, quando si apre una pagina Web in un browser, cisco.com risolve

l'indirizzo IP di un server che fornisce un certificato, che deve includere cisco.com come nome per essere considerato attendibile.

- Il certificato CA che ha firmato il certificato del server presentato dal server (o lo stesso certificato del server se autofirmato) è presente nell'elenco dei certificati attendibili CA del dispositivo.
  - I dispositivi dispongono di un elenco di certificati CA attendibili. I computer spesso includono un elenco precompilato con autorità di certificazione pubbliche note.

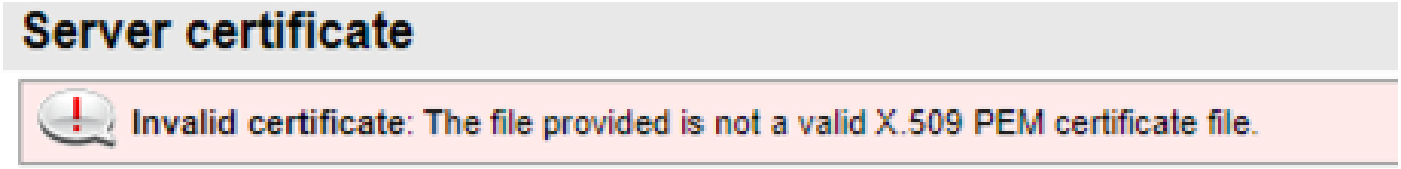
- La data e l'ora correnti rientrano nel periodo di validità del certificato.
  - Le autorità di certificazione firmano i CSR solo per un determinato periodo di tempo, determinato dalla CA.

- Certificato non revocato.
  - Le autorità pubbliche di certificazione includono spesso un URL dell'elenco di revoche di certificati all'interno del certificato. In questo modo la parte che riceve il certificato può confermare che non è stato revocato dalla CA.

Problemi comuni

Caricamento del certificato Expressway non riuscito

Ci sono un paio di condizioni che possono causare questo. Generano un errore descrittivo diverso.



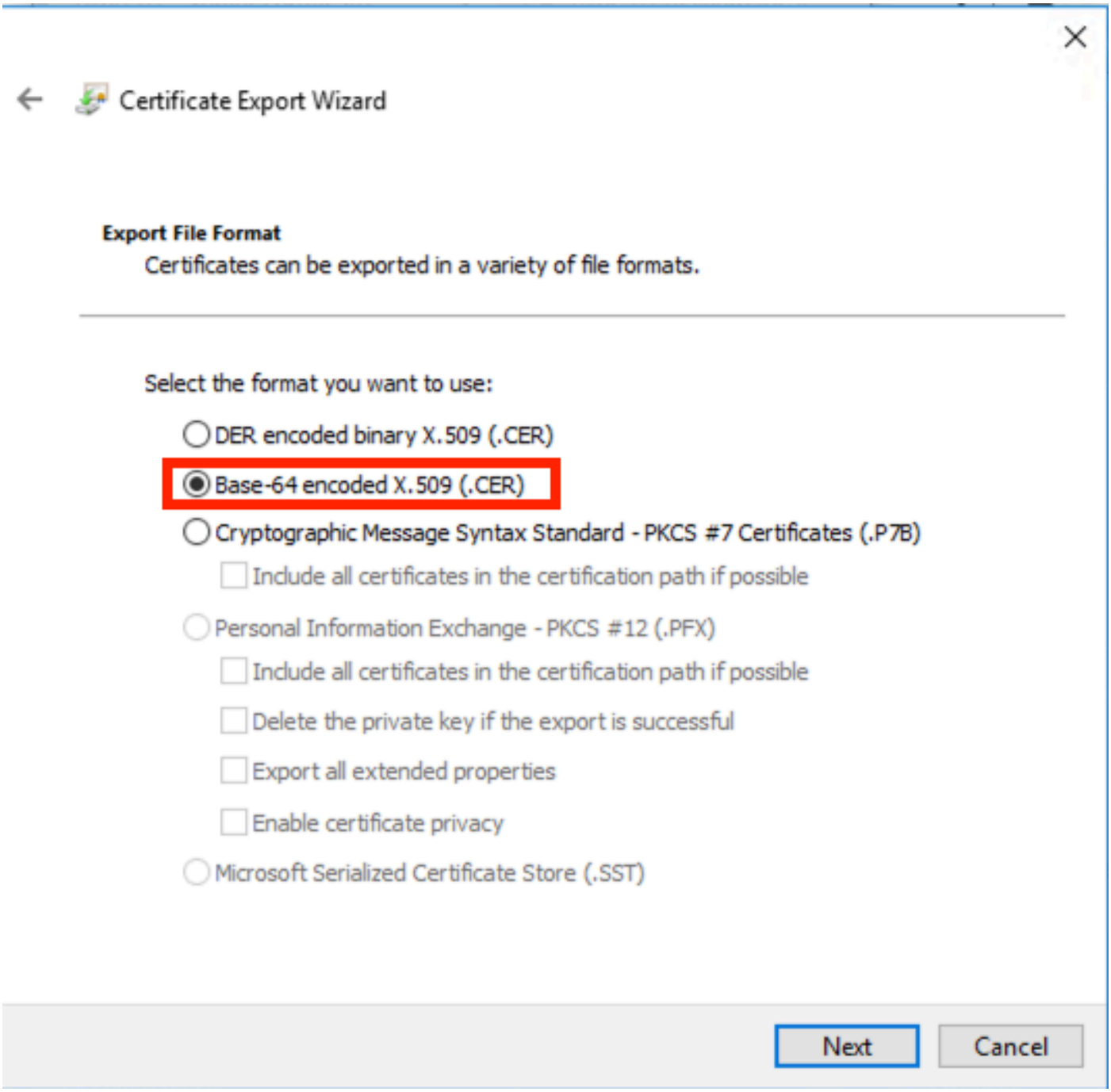
Formato del certificato non valido

Questo primo errore si verifica quando il formato del certificato non è valido. L'estensione del file non ha importanza.

Se il certificato non si apre, è possibile richiederne uno nuovo alla CA nel formato corretto

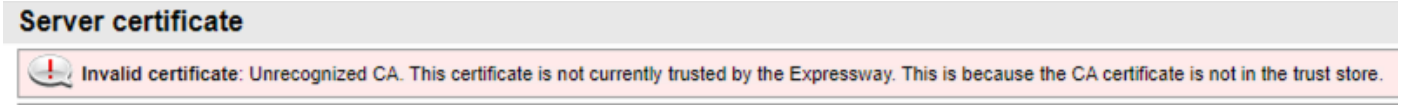
Se il certificato viene aperto, eseguire la procedura seguente:

Passaggio 1. Aprire il certificato e passare alla scheda Dettagli.
Passaggio 2. Selezionare Copia su file.
Passaggio 3. Seguire la procedura guidata e assicurarsi che sia selezionata la codifica Base 64.



Selezione formato certificato

Passaggio 4. Una volta salvato, carica il nuovo file in Expressway.



Catena di certificati CA non attendibili

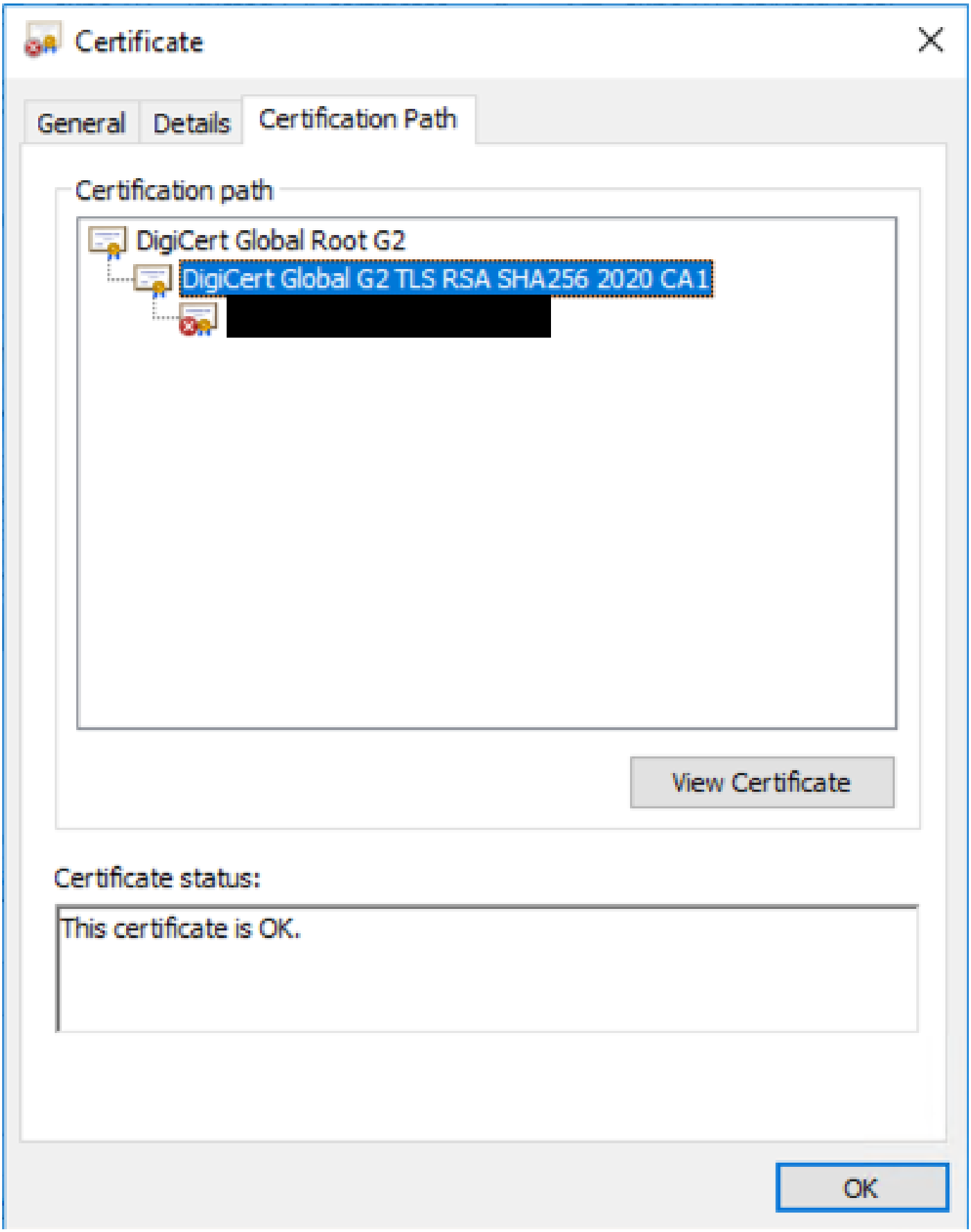
Questo errore si verifica quando i certificati CA che hanno firmato il certificato server non sono attendibili. Prima di caricare un certificato server, il server deve considerare attendibili tutti i certificati CA nella catena.

Normalmente la CA fornisce i certificati della CA insieme al certificato del server firmato. Se sono

disponibili, andare al passaggio 6.

Se i certificati CA non sono disponibili, è possibile ottenerli dal certificato del server. Attenersi alla procedura seguente:

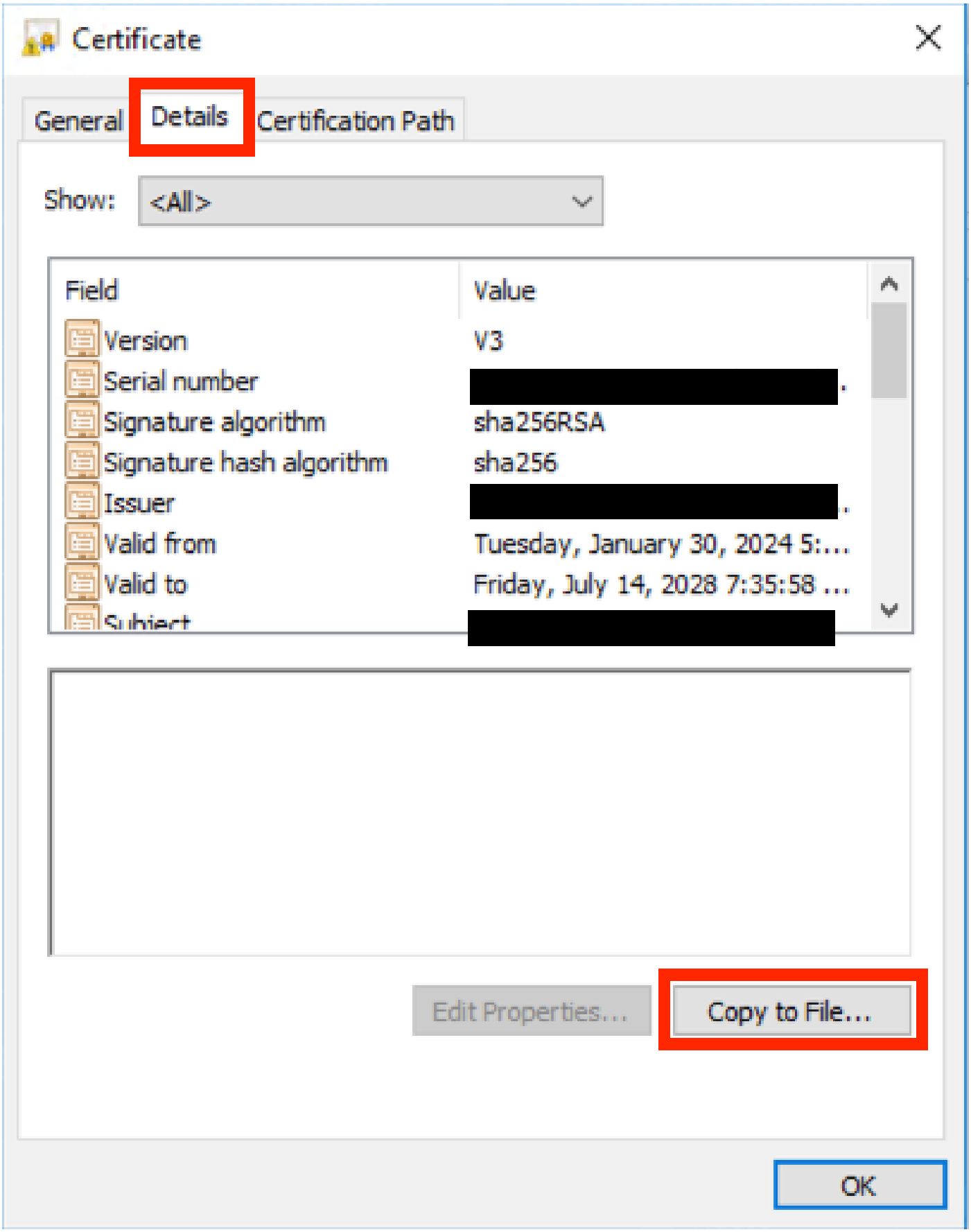
Passaggio 1. Aprire il certificato server.
Passaggio 2. Passare alla scheda Percorso certificazione. Il primo certificato è considerato il certificato CA radice. In basso è riportato il certificato del server e tutti gli elementi intermedi sono considerati certificati CA intermedi.
Passaggio 3. Scegliere un certificato CA e selezionare Visualizza certificato.



Percorso certificazione

Passaggio 4. Passare alla scheda Dettagli e seguire i passaggi precedenti per salvare il certificato

in un file separato.
Passaggio 5. Ripetere questi passaggi per tutti i certificati CA presenti.



Scheda Dettagli certificato

Dopo aver reso disponibili tutti i certificati CA, caricarli nell'elenco dei certificati CA attendibili di Expressway:

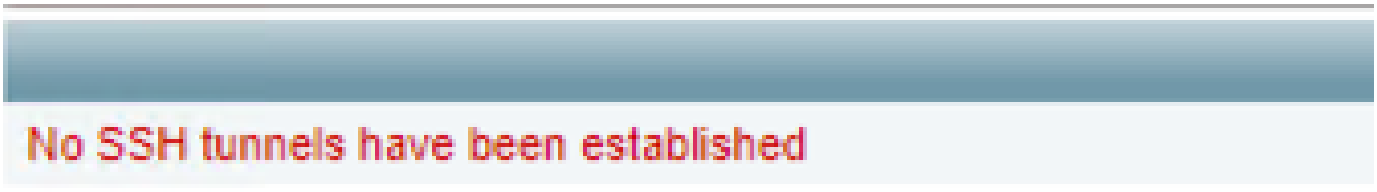
Passaggio 6. Passare a Manutenzione > Protezione > Certificato CA attendibile sul server Expressway.
Passaggio 7. Selezionare Scegli file e carica.
Passaggio 8. Ripetere i passaggi 7 per ogni certificato CA.
Passaggio 9. Una volta caricati tutti i certificati CA nell'elenco di attendibilità, caricare il certificato del server nel server.

Area trasversale inattiva con errore Errore di negoziazione TLS

Questo errore si verifica quando lo scambio SSL tra Expressway-C ed Expressway-E non viene completato correttamente. Ecco alcuni esempi che possono causare questa situazione:

- Il nome host non corrisponde a un nome nel certificato presentato.
  - Verificare che l'indirizzo peer configurato nella zona di attraversamento Expressway-C corrisponda ad almeno uno dei nomi nel certificato del server Expressway-E
- Il nome della verifica TLS non corrisponde a un nome nel certificato presentato.
  - Verificare che il nome di verifica TLS configurato nella zona trasversale Expressway-E corrisponda a uno dei nomi nel certificato del server Expressway-C. Se si tratta di una configurazione cluster, si consiglia di configurare l'FQDN del cluster Expressway-C come TLS. Verificare che il nome specificato sia presente in tutti i nodi del cluster.
- I certificati CA non sono considerati attendibili dai server
  - Come ogni server deve considerare attendibili i propri certificati CA prima di caricarvi il certificato server, anche gli altri server devono considerare attendibili tali certificati CA per poter considerare attendibile il certificato server. A tale scopo, verificare che tutti i certificati CA del percorso di certificazione di entrambi i server Expressway siano presenti nell'elenco delle CA attendibili di tutti i server interessati. I certificati CA possono essere estratti seguendo la procedura descritta in precedenza in questo documento.

Area trasversale attiva ma SSH tunnel inattiva dopo un rinnovo del certificato



Errore del tunnel SSH

Questo errore si verifica in genere dopo il rinnovo di un certificato quando uno o più certificati CA intermedi non sono considerati attendibili, l'attendibilità del certificato CA radice abilita la connessione alla zona di attraversamento, ma i tunnel SSH sono una connessione più dettagliata e possono non riuscire se l'intera catena non è considerata attendibile. I certificati CA intermedi vengono spesso modificati dalle autorità di certificazione in modo che il rinnovo di un certificato

possa causare il problema. Verificare che tutti i certificati CA intermedi siano caricati in tutti gli elenchi di attendibilità di Expressway.

Accesso a Mobile e Remote Access non riuscito dopo un aggiornamento o un rinnovo del certificato

Ci sono molti modi in cui un accesso può non riuscire a causa dei certificati ma nelle versioni più recenti del software Expressway sono state implementate alcune modifiche software che, per motivi di sicurezza, forzano la verifica dei certificati dove non è stato fatto prima.

Questa spiegazione è più precisa: il server del traffico applica la verifica dei certificati

Come indicato nella soluzione, verificare che i certificati CA Expressway-C siano caricati in Cisco Unified Communications Manager come tomcat-trust e callmanager-trust e riavviare i servizi richiesti.

Avviso certificato su Jabber all'accesso di Mobile e Remote Access

Avviso certificato non attendibile Jabber

Questo comportamento si verifica quando il dominio utilizzato nell'applicazione non corrisponde a un nome soggetto alternativo nel certificato del server Expressway-E.
Verificare che il nome .com di esempio o il nome alternativo collab-edge.example .com sia uno dei nomi alternativi del soggetto presenti nel certificato.

Informazioni correlate

Supporto tecnico Cisco e download

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).