Configurazione e risoluzione dei problemi dei certificati MRA (Collaboration Edge)

Sommario

Introduzione

In questo documento vengono descritti i certificati relativi alle distribuzioni MRA (Mobile Remote Access).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

CA (Public vs. Private Certificate Authority)

Sono disponibili diverse opzioni per la firma dei certificati nei server Expressway-C ed E. È possibile scegliere di firmare la richiesta di firma del certificato (CSR) da un'autorità di certificazione pubblica, ad esempio GoDaddy, Verisign o altre, oppure è possibile firmarla internamente se si utilizza un'autorità di certificazione personalizzata, che può essere autofirmata con OpenSSL o un'autorità di certificazione aziendale interna, ad esempio un server Microsoft Windows. Per ulteriori informazioni su come creare e firmare i CSR utilizzati da uno di questi metodi, vedere la Guida alla creazione dei certificati di Video Communication Server (VCS).

L'unico server che deve essere firmato da una CA pubblica è Expressway-E. Si tratta dell'unico server in cui i client visualizzano il certificato quando eseguono l'accesso tramite Autorità registrazione integrità. Utilizzare pertanto una CA pubblica per assicurarsi che gli utenti non debbano accettare manualmente il certificato. Expressway-E può funzionare con un certificato interno firmato dalla CA, ma al primo utente verrà richiesto di accettare il certificato non attendibile. La registrazione MRA dei telefoni serie 7800 e 8800 non funziona con i certificati interni perché non è possibile modificare l'elenco di certificati attendibili. Per semplicità, è consigliabile che i certificati Expressway-C ed Expressway-E siano entrambi firmati dalla stessa CA. Tuttavia, non si tratta di un requisito se gli elenchi di CA attendibili sono stati configurati correttamente in entrambi i server.

Funzionamento delle catene di certificati

I certificati sono collegati in una catena di due o più elementi utilizzata per verificare l'origine che ha firmato il certificato del server. In una catena sono presenti tre tipi di certificati: il certificato client/server, il certificato intermedio (in alcuni casi) e il certificato radice (denominato anche CA radice, in quanto si tratta dell'autorità di livello più alto che ha firmato il certificato).

I certificati contengono due campi principali che costituiscono la catena, ovvero l'oggetto e l'autorità emittente.

Il soggetto è il nome del server o dell'autorità rappresentata dal certificato. Nel caso di un dispositivo Expressway-C o Expressway-E (o altri dispositivi UC), viene generato dal nome di dominio completo (FQDN).

L'autorità emittente è l'autorità che ha convalidato il certificato specifico. Dal momento che chiunque può firmare un certificato (che include il server da cui è stato creato il certificato, per cominciare, anche noto come certificati autofirmati), i server e i client dispongono di un elenco di autorità di certificazione o CA ritenute autentiche.

Una catena di certificati termina sempre con un certificato di primo livello autofirmato o un certificato radice. Quando ci si sposta all'interno della gerarchia dei certificati, ogni certificato ha un'autorità emittente diversa in relazione al soggetto. Alla fine, si troverà la CA radice in cui il soggetto e l'autorità emittente corrispondono. Ciò indica che si tratta del certificato di primo livello e quindi di quello che deve essere considerato attendibile da un elenco di CA attendibili di un client o di un server.

Riepilogo handshake SSL

Nel caso della zona di attraversamento, Expressway-C agisce sempre come client mentre Expressway-E è sempre il server. Lo scambio semplificato funziona come illustrato di seguito.

Expressway-C Expressway-E

â€”Salve al clienteâ€”>

<â€”Salve serverâ€”

<â€”Certificato serverâ€”

<â€”Richiesta certificatoâ€”

â€”Certificato clientâ€”>

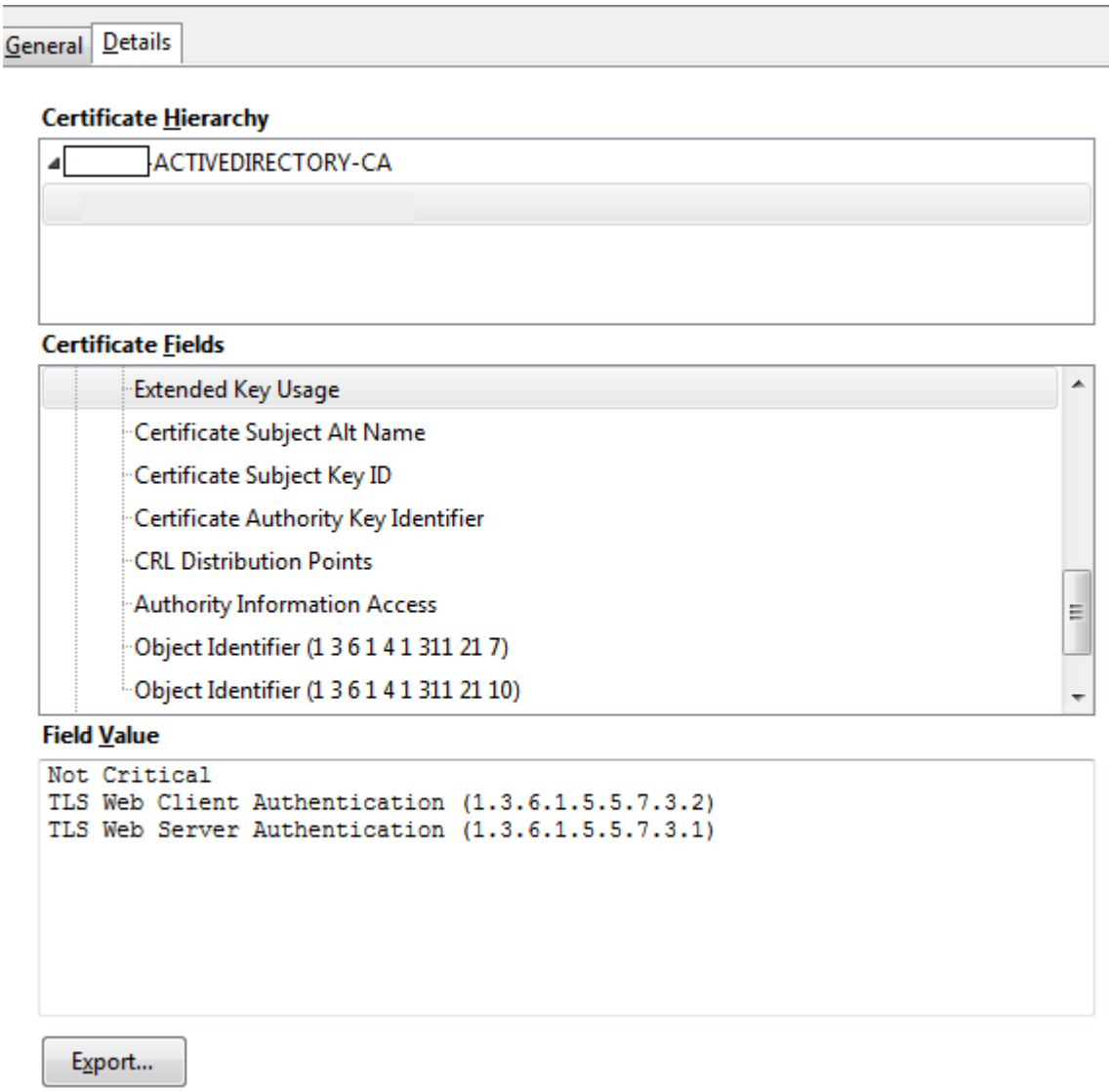
La chiave qui è nello scambio in quanto Expressway-C avvia sempre la connessione, e quindi è sempre il client. Expressway-E è il primo a inviare il proprio certificato. Se Expressway-C non è in grado di convalidare il certificato, viene interrotto l'handshake e non è in grado di inviarne uno a Expressway-E.

Un altro aspetto importante da notare è l'autenticazione client Web Transport Layer Security (TLS) e gli attributi di autenticazione server Web TLS sui certificati. Questi attributi vengono determinati sulla CA che ha firmato il CSR (se viene utilizzata una CA di Windows, ciò viene determinato dal modello selezionato) e indicano se il certificato è valido nel ruolo del client o del server (o di entrambi). Poiché per un sistema VCS o Expressway può essere basato sulla situazione (è sempre lo stesso per una zona trasversale) e il certificato deve avere attributi di autenticazione sia client che server.

Expressway-C ed Expressway-E restituiscono un errore quando vengono caricati in un nuovo certificato server, se non vengono applicati entrambi.

Se non si è certi che un certificato abbia questi attributi, è possibile aprire i dettagli del certificato in un browser o nel sistema operativo e controllare la sezione Utilizzo chiave esteso (vedere l'immagine). Il formato può variare a seconda di come viene visualizzato il certificato.

Esempio:



Configurazione

Area/trust attraversamento Expressway-C ed Expressway-E

Genera e firma CSR

Come descritto in precedenza, i certificati Expressway-C ed Expressway-E devono essere firmati da una CA interna o esterna oppure da OpenSSL per l'autofirma.

> **Nota**: non è possibile utilizzare il certificato temporaneo disponibile nel server Expressway perché non è supportato. Se si utilizzano certificati jolly in cui si dispone di un certificato di firma CA e la riga dell'oggetto non è definita in modo specifico, non è supportata.

Il primo passaggio consiste nella generazione del CSR e nella firma con il tipo di CA preferito. La procedura è descritta in modo specifico nella Guida alla creazione dei certificati. Durante la creazione del CSR, è importante tenere presenti i nomi alternativi del soggetto (SAN, Subject Alternative Names) necessari da includere nei certificati. Questo argomento è inoltre elencato nella guida ai certificati e nella guida alla distribuzione di Mobile Remote Access. Consultate le versioni più recenti della guida per ulteriori informazioni sulle nuove funzioni disponibili. Elenco delle SAN comuni da includere in base alle funzionalità utilizzate:

Expressway-C

- Qualsiasi dominio (interno o esterno) aggiunto all'elenco dei domini.
- Qualsiasi alias di nodo di chat persistente se viene utilizzata la federazione XMPP.
- Proteggere i nomi dei profili di dispositivo in CUCM se vengono utilizzati profili di dispositivo sicuri.

Expressway-E

- Qualsiasi dominio configurato in Expressway-C.
- Qualsiasi alias di nodo di chat persistente se viene utilizzata la federazione XMPP.
- Qualsiasi dominio annunciato per le federazioni XMPP.

> **Nota**: se il dominio di base utilizzato per le ricerche dei record di servizio esterno (SRV) non è incluso come rete SAN nel certificato Expressway-E (xxx.com o collab-edge.xxx.com), i client Jabber richiedono ancora all'utente finale di accettare il certificato sulla prima connessione e gli endpoint TC non riusciranno a connettersi.

Configurare Expressway-C ed Expressway-E in modo che siano reciprocamente attendibili

Affinché la zona di attraversamento di Unified Communications stabilisca una connessione, Expressway-C ed Expressway-E devono considerare attendibili i rispettivi certificati. In questo esempio si presuppone che il certificato Expressway-E sia stato firmato da una CA pubblica che utilizza questa gerarchia.

Certificato 3

Autorità emittente: GoDaddy Root CA

Oggetto: GoDaddy Root CA

Certificato 2

Autorità emittente: GoDaddy Root CA

Oggetto: Autorità intermedia GoDaddy

Certificato 1

Emittente: GoDaddy Intermediate Authority

Oggetto: Expressway-E.lab

Expressway-C deve essere configurato con il certificato di attendibilità 1. Nella maggior parte dei casi, in base ai certificati attendibili applicati al server, invia solo il certificato del server di livello più basso. Ciò significa che affinché Expressway-C consideri attendibile il certificato 1, è necessario caricare entrambi i certificati 2 e 3 nell'elenco delle CA attendibili di Expressway-C (**Manutenzione> Sicurezza > Elenco CA attendibili**). Se si omette il certificato intermedio 2 quando Expressway-C riceve il certificato Expressway-E, non è possibile collegarlo alla CA radice GoDaddy attendibile, pertanto il certificato verrà rifiutato.

Certificato 3

Autorità emittente: GoDaddy Root CA

Oggetto: GoDaddy Root CA

Certificato 1

Autorità di certificazione: autorità intermedia GoDaddy - non attendibile.

Oggetto: Expressway-E.lab

Inoltre, se si carica solo il certificato intermedio senza la radice nell'elenco delle CA attendibili di Expressway-C, si vedrebbe che l'Autorità intermedia GoDaddy è attendibile, ma è firmata da un'autorità superiore, in questo caso la CA radice GoDaddy non è attendibile, quindi non funzionerebbe.

Certificato 2

Autorità emittente: GoDaddy Root CA - Non attendibile!

Oggetto: Autorità intermedia GoDaddy

Certificato 1

Emittente: GoDaddy Intermediate Authority

Oggetto: Expressway-E.lab

Con tutti i certificati intermedi e la radice aggiunta all'elenco delle CA attendibili, è possibile verificare il certificato...

Certificato 3

Autorità emittente: GoDaddy Root CA - Il certificato di primo livello autofirmato è attendibile e la catena è stata completata.

Oggetto: GoDaddy Root CA

Certificato 2

Autorità emittente: GoDaddy Root CA

Oggetto: Autorità intermedia GoDaddy

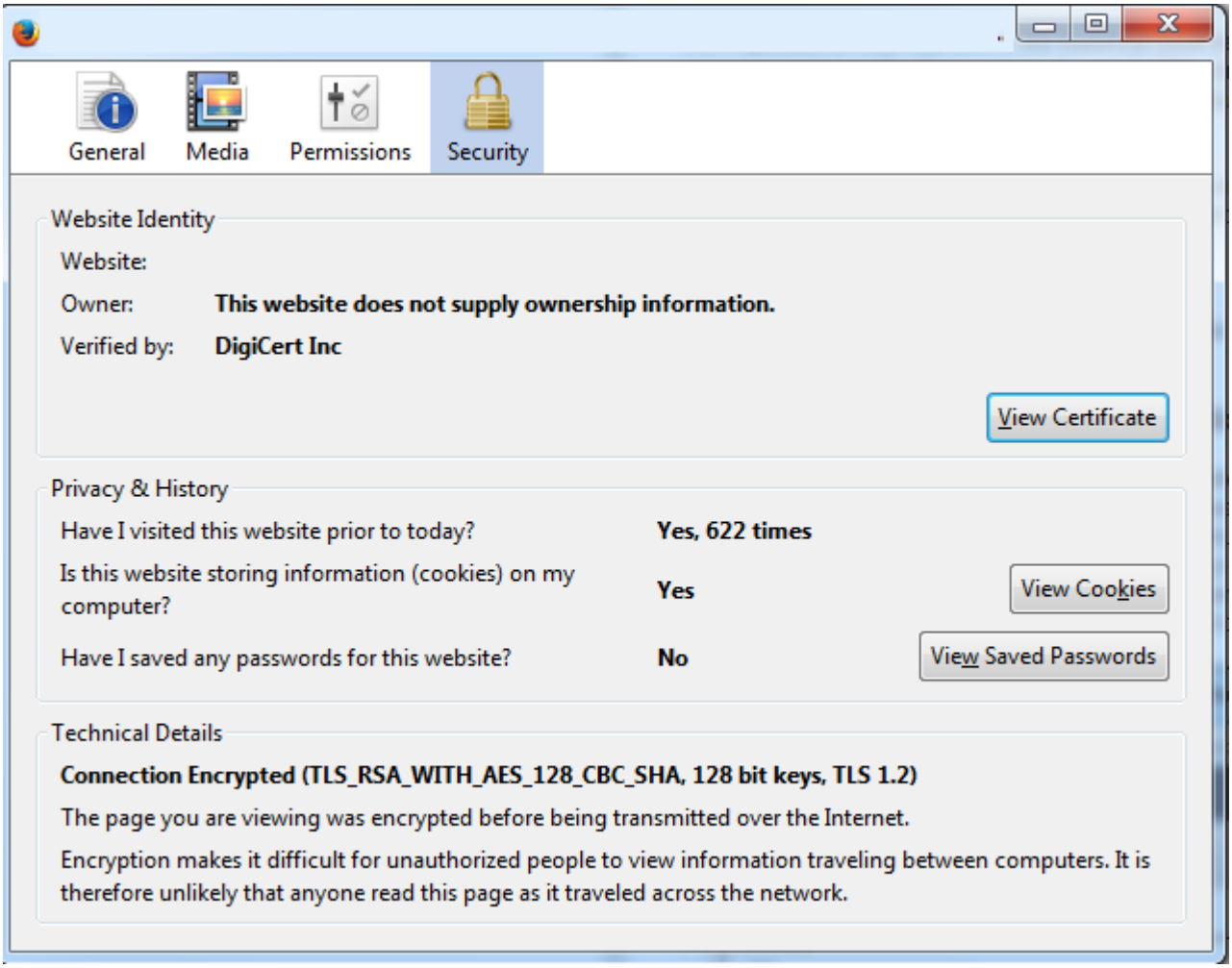
Certificato 1

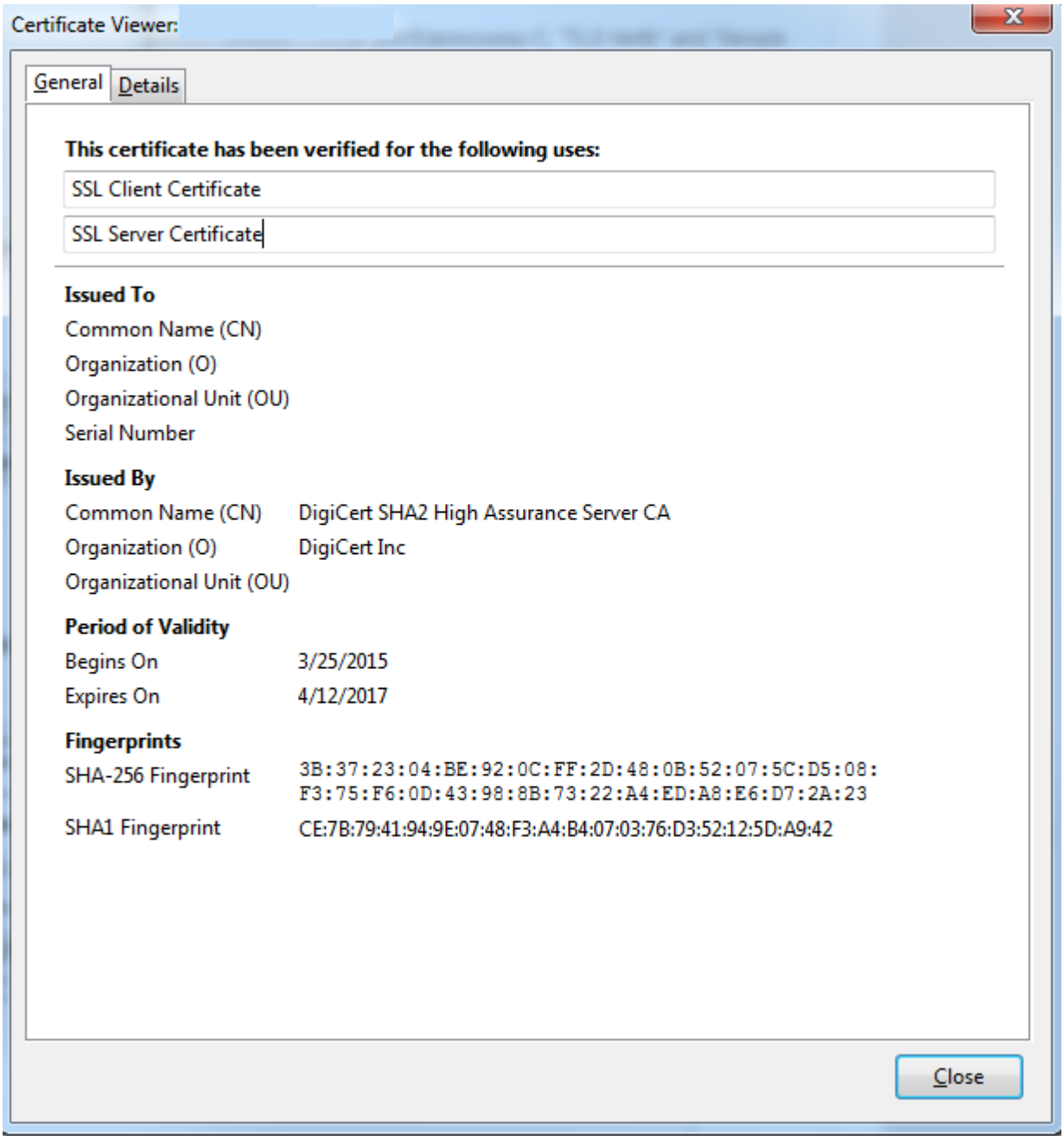
Emittente: GoDaddy Intermediate Authority

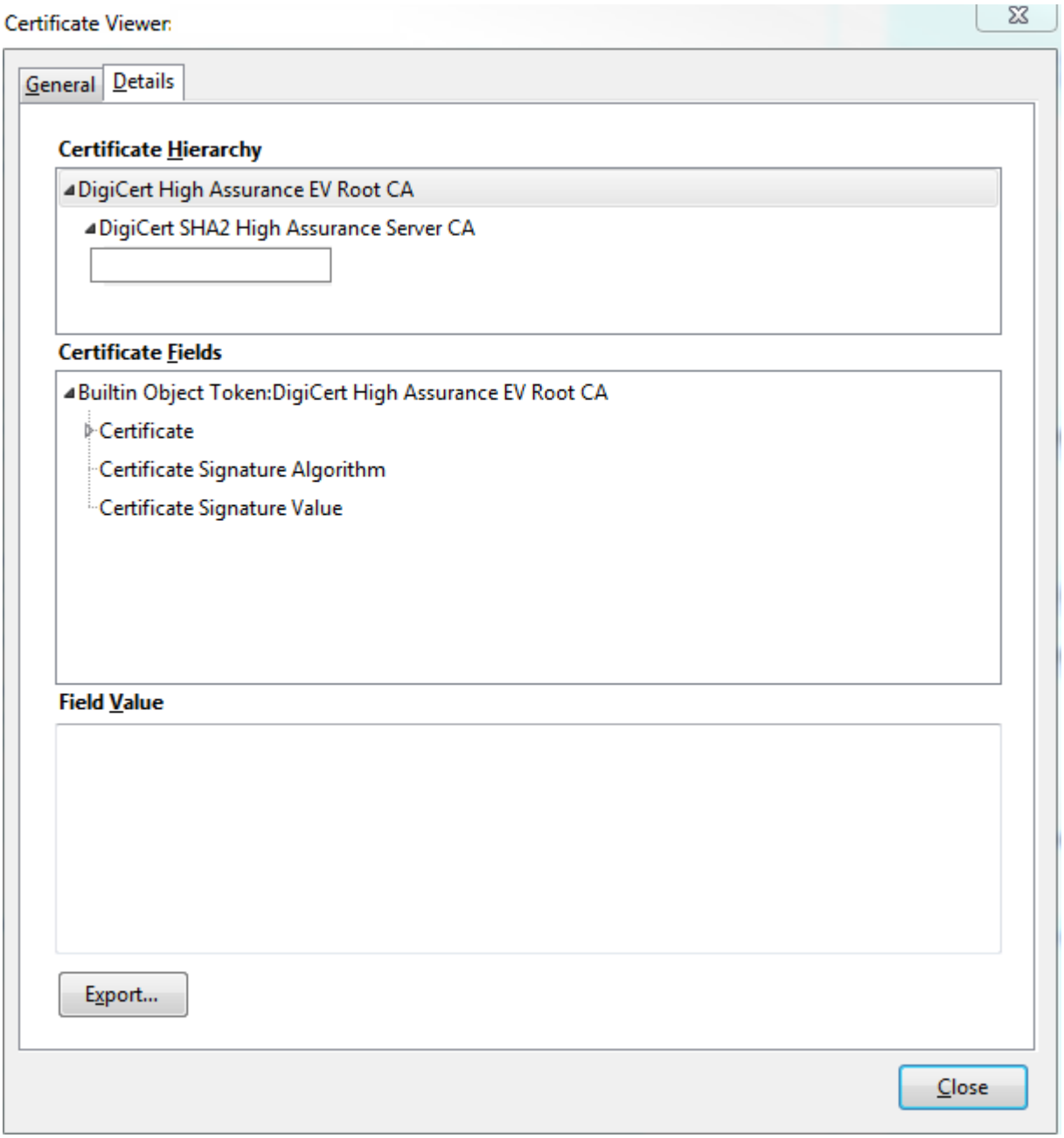
Oggetto: Expressway-E.lab

Se non si è certi della catena di certificati, è possibile controllare il browser quando si è connessi all'interfaccia Web di Expressway specifico. Il processo varia leggermente in base al browser, ma in Firefox è possibile fare clic sull'icona del lucchetto all'estrema sinistra della barra degli indirizzi. Quindi, nel popup, fare clic su **Ulteriori informazioni > Visualizza certificato > Dettagli**. Se il browser è in grado di assemblare l'intera catena, potete vederla dall'alto verso il basso. Se il certificato di primo livello non ha un soggetto e un'autorità emittente corrispondenti, significa che la catena non è completata. Se si fa clic su **esporta** con il certificato desiderato evidenziato, è inoltre possibile esportare singolarmente ogni certificato

della catena. Ciò è utile se non si è certi al 100% di aver caricato i certificati corretti nell'elenco di certificati attendibili della CA.




Certificate Viewer:
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Issued To
Common Name (CN)
Organization (O)
Organizational Unit (OU)
Serial Number
Issued By
Common Name (CN) DigiCert SHA2 High Assurance Server CA
Organization (O) DigiCert Inc
Organizational Unit (OU)
Period of Validity
Begins On 3/25/2015
Expires On 4/12/2017
Fingerprints
SHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23
SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42
Close



Ora che Expressway-C considera attendibile il certificato di Expressway-E, verificare che funzioni nella direzione opposta. Se il certificato Expressway-C è firmato dalla stessa CA che ha firmato Expressway-E, il processo è semplice. Caricare nell'elenco CA attendibili di Expressway-E gli stessi certificati già caricati nell'unità C. Se la C è firmata da un'autorità di certificazione diversa, è necessario utilizzare lo stesso processo illustrato nell'immagine, ma utilizzare la catena con cui è stato firmato il certificato Expressway-C.

Comunicazione sicura tra Cisco Unified Communications Manager (CUCM) ed Expressway-C

Panoramica

A differenza della zona di attraversamento tra Expressway-C ed Expressway-E, tra Expressway-C e CUCM NON è richiesta la segnalazione protetta. A meno che ciò non sia consentito dai criteri di sicurezza interni, è necessario configurare sempre l'Autorità registrazione integrità in modo che funzioni con profili di dispositivo non protetti su CUCM prima di confermare che il resto della distribuzione sia corretto prima di continuare con questo passaggio.

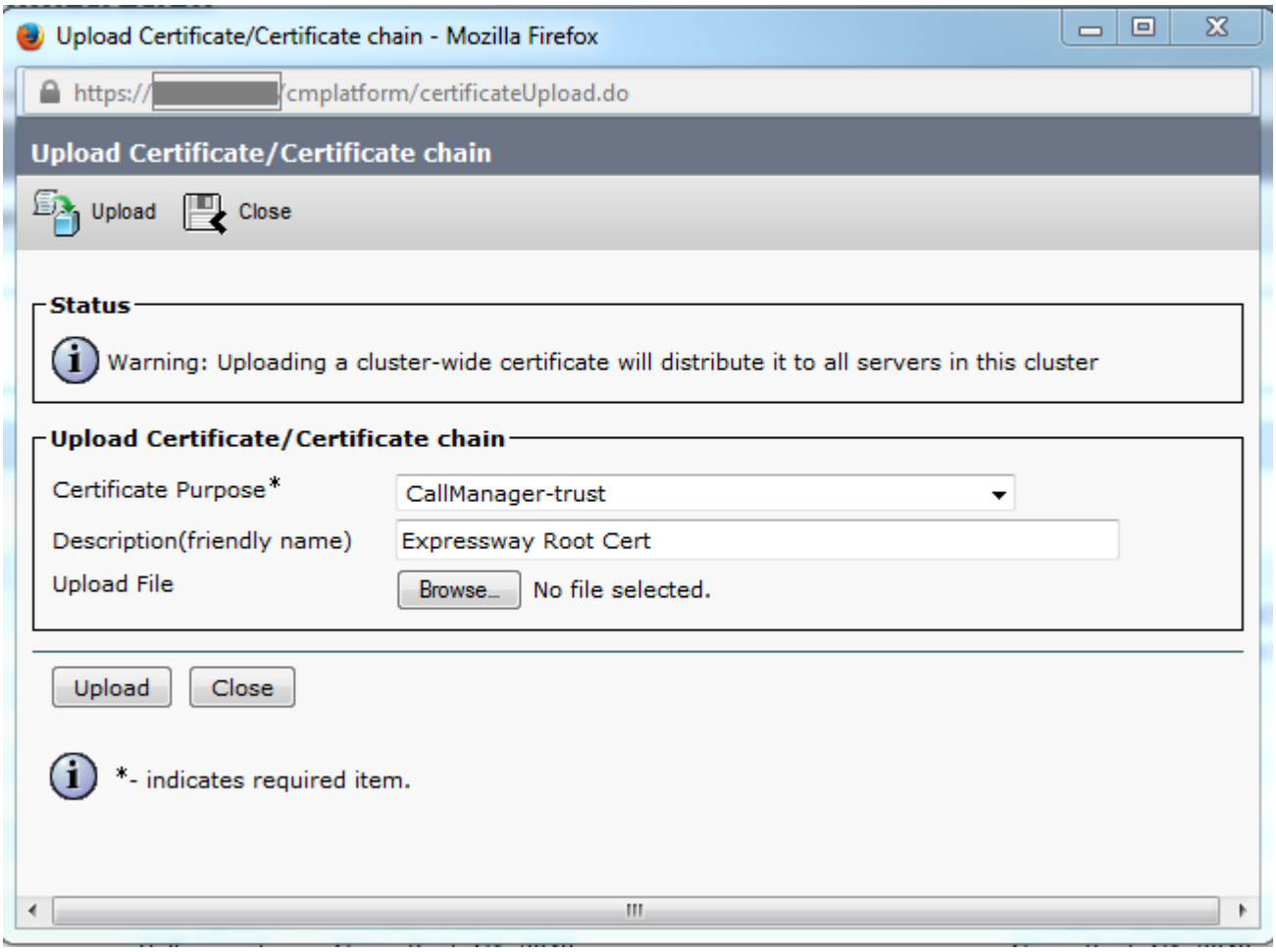
Tra CUCM ed Expressway-C è possibile abilitare due funzioni principali di sicurezza: la verifica TLS e la registrazione sicura dei dispositivi. Esiste un'importante distinzione tra questi due tipi di certificato, in quanto utilizzano due certificati diversi dal lato CUCM nell'handshake SSL.

Verifica TLS - certificato tomcat

Registrazioni SIP protette - Certificato CallManager

Configura trust tra CUCM ed Expressway-C

Il concetto, in questo caso, è esattamente lo stesso utilizzato tra Expressway-C ed Expressway-E. Il CUCM deve innanzitutto considerare attendibile il certificato server di Expressway-C. Ciò significa che sul CUCM, i certificati intermedi e radice di Expressway-C devono essere caricati come un certificato tomcat-trust per la funzione di verifica TLS e un CallManager-trust per registrazioni sicure dei dispositivi. Per ottenere questo risultato, selezionare **Cisco Unified OS Administration** nell'angolo superiore destro della GUI Web di CUCM, quindi **Security**> **Certificate Management** (Gestione certificati). Fare clic su **Carica certificato/catena di certificati** e selezionare il formato di attendibilità corretto oppure fare clic su **Trova** per visualizzare l'elenco dei certificati attualmente caricati.

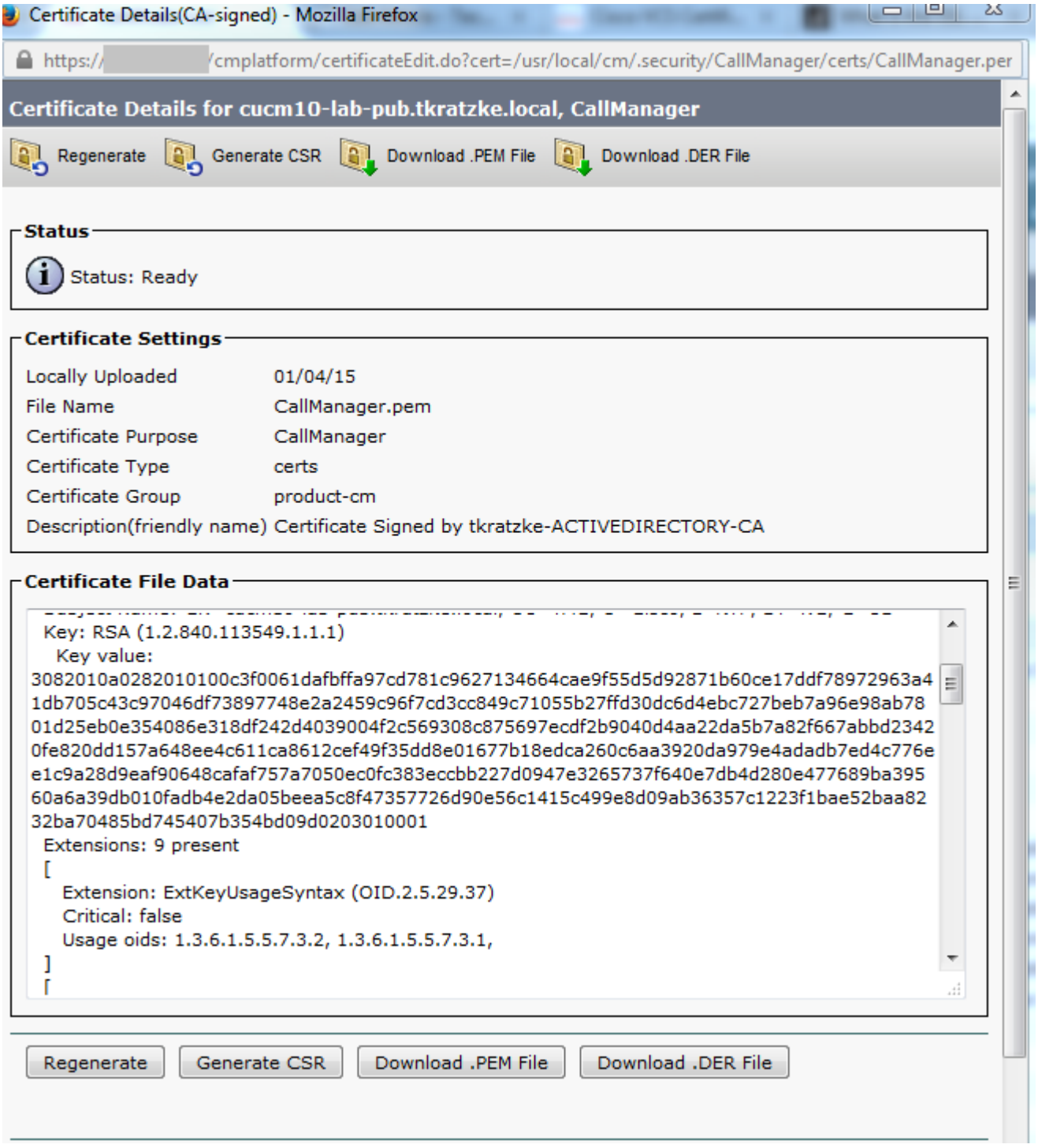


È necessario verificare che Expressway-C consideri attendibile la CA che ha firmato i certificati CUCM. Ciò è possibile se le si aggiunge all'elenco delle CA attendibili. In quasi tutti i casi, se i certificati CUCM sono stati firmati con una CA, i certificati tomcat e CallManager devono essere firmati dalla stessa CA. Se sono diverse, è necessario considerare attendibili entrambe se si utilizzano la verifica TLS e le registrazioni protette.

Per le registrazioni SIP protette, è inoltre necessario verificare che il nome del profilo del dispositivo protetto nel CUCM applicato al dispositivo sia elencato come SAN nel certificato Expressway-C. Se non

contiene i messaggi di registro protetti, il sistema non riuscirà con un errore 403 del CUCM, che indica un errore TLS.

Nota: quando l'handshake SSL viene eseguito tra CUCM ed Expressway-C per una registrazione SIP protetta, vengono eseguiti due handshake. In primo luogo, Expressway-C agisce come client e avvia la connessione con CUCM. Una volta completato correttamente, CUCM avvia un altro handshake come client a cui rispondere. Ciò significa che, proprio come Expressway-C, il certificato CallManager su CUCM deve avere entrambi gli attributi di autenticazione TLS Web Client e TLS Web Server applicati. La differenza consiste nel fatto che CUCM consente il caricamento di questi certificati senza entrambi, mentre le registrazioni protette interne funzionano correttamente se CUCM dispone solo dell'attributo di autenticazione server. È possibile confermarlo su CUCM se si cerca il certificato CallManager nell'elenco e lo si seleziona. In questa sezione è possibile esaminare gli ID di utilizzo nella sezione Estensione. È possibile vedere la versione 1.3.6.1.5.5.7.3.2 per l'autenticazione del client e la versione 1.3.6.1.5.7.3.1 per l'autenticazione del server. Da questa finestra è inoltre possibile scaricare il certificato.



> **Nota**: i certificati di attendibilità applicati al server di pubblicazione in un cluster devono essere replicati nei Sottoscrittori. È buona norma accedervi separatamente su una nuova configurazione.

> **Nota**: per consentire a Expressway-C di convalidare correttamente il certificato da CUCM, i server CUCM DEVONO essere aggiunti in Expressway-C con il nome FQDN, non con l'indirizzo IP. L'unico modo in cui l'indirizzo IP può funzionare è se l'IP di ciascun nodo CUCM viene aggiunto come SAN nel certificato, il che non è quasi mai stato fatto.

Server CUCM con certificati autofirmati

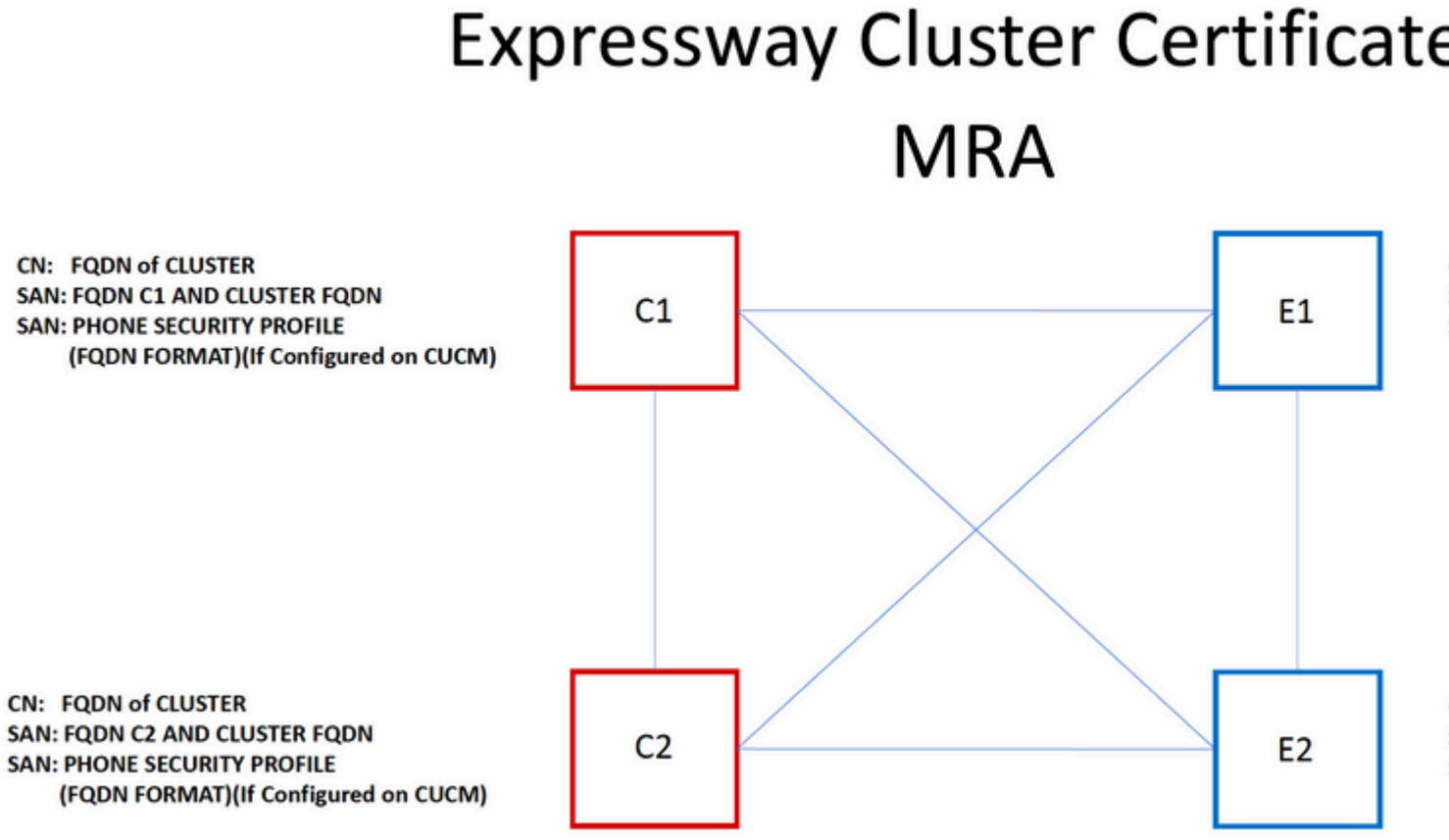
Per impostazione predefinita, un server CUCM viene fornito con certificati autofirmati. Se sono già

disponibili, non è possibile utilizzare contemporaneamente sia la verifica TLS che la registrazione sicura dei dispositivi. Entrambe le funzionalità possono essere utilizzate da sole, ma poiché i certificati sono autofirmati, è necessario caricare nell'elenco delle CA attendibili di Expressway-C sia i certificati Tomcat autofirmati che i certificati CallManager autofirmati. Quando Expressway-C esegue una ricerca nel proprio elenco di attendibilità per convalidare un certificato, si interrompe quando ne trova uno con un oggetto corrispondente. Per questo motivo, a seconda di quale delle due è più alta nell'elenco di attendibilità, tomcat o CallManager, la funzionalità funzionerà correttamente. Quella inferiore fallirebbe come se non fosse presente. La soluzione consiste nel firmare i certificati CUCM con una CA (pubblica o privata) e considerare attendibile tale CA da sola.

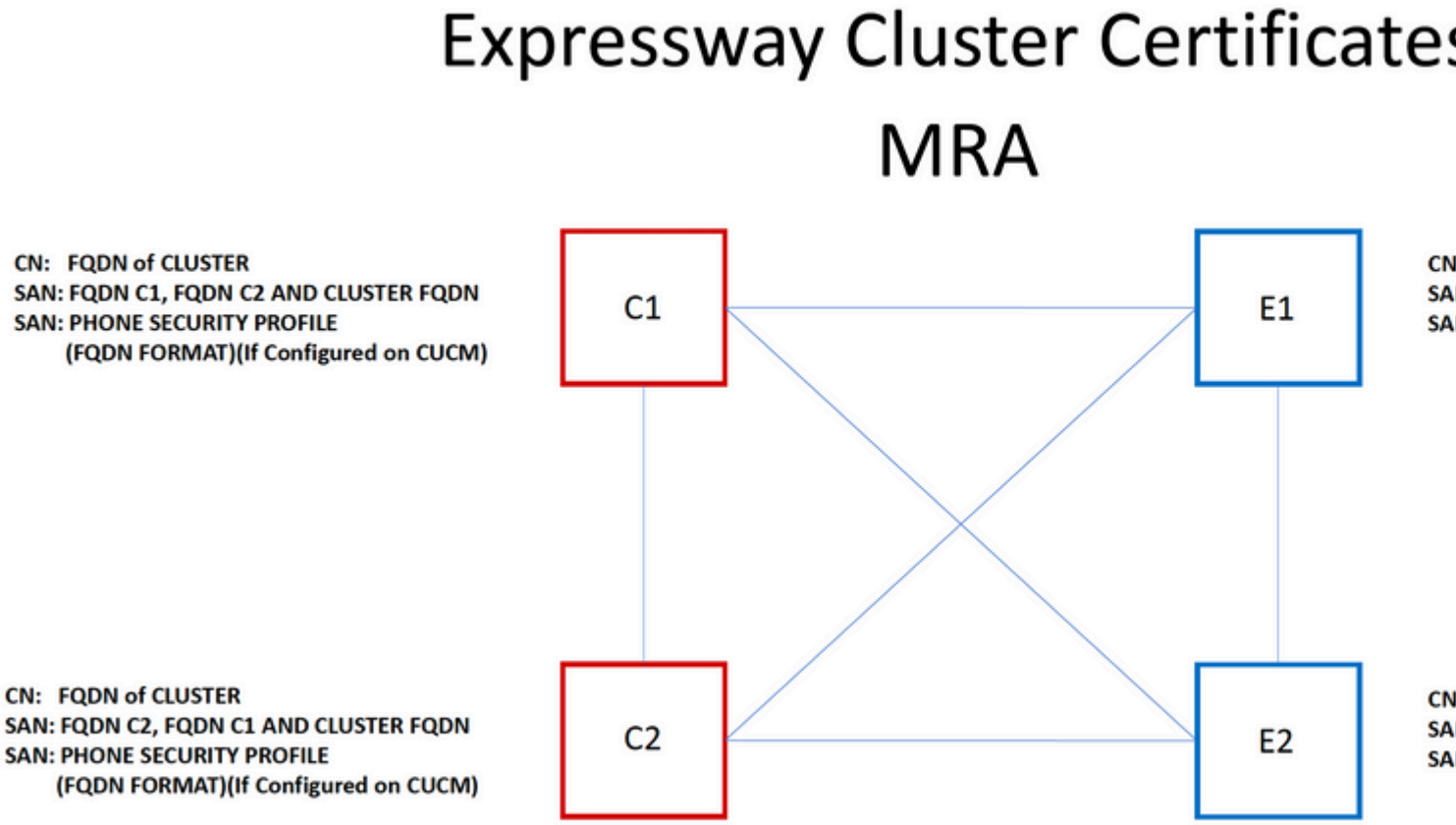
Considerazioni sui cluster Expressway-C ed Expressway-E

Certificati cluster

Se si dispone di un cluster di server Expressway-C o Expressway-E per la ridondanza, è consigliabile generare un CSR separato per ogni server e firmarlo con una CA. Nello scenario precedente, il nome comune (CN) di ogni certificato peer sarebbe lo stesso nome di dominio completo (FQDN) del cluster e le SAN sarebbero l'FQDN del cluster e l'FQDN dei rispettivi peer, come mostrato nell'immagine:



È possibile utilizzare l'FQDN del cluster come FQDN CN e ogni FQDN peer e l'FQDN del cluster nella SAN per utilizzare lo stesso certificato per tutti i nodi del cluster ed evitare quindi il costo di più certificati firmati da una CA pubblica.



> **Nota**: i nomi dei profili di sicurezza telefono nel certificato Cs sono necessari solo se si utilizzano i profili di sicurezza telefono protetto nell'UCM. Il dominio esterno o collab-edge.example.com (dove example.com è il tuo dominio) è un requisito solo per la registrazione degli endpoint IP Phone e TC su MRA. Questa opzione è facoltativa per la registrazione di Jabber su MRA. Se non è presente, jabber richiederà di accettare il certificato quando jabber esegue l'accesso tramite MRA.

Se assolutamente necessario, è possibile eseguire questa operazione con il processo successivo oppure è possibile utilizzare OpenSSL per generare manualmente sia la chiave privata che la CSR:

Passaggio 1. Generare un CSR sul server primario del cluster e configurarlo per elencare l'alias del cluster come CN. Aggiungere tutti i peer nel cluster come nomi alternativi, insieme a tutte le altre SAN richieste.

Passaggio 2. Firmare il CSR e caricarlo nel peer primario.

Passaggio 3. Accedere al database primario come root e scaricare la chiave privata in /Tandberg/persistent/certs.

Passaggio 4. Caricare il certificato firmato e la chiave privata corrispondente tra loro nel cluster.

> **Nota**: questa opzione non è consigliata per i seguenti motivi:
> 1. È un rischio per la sicurezza perché tutti i peer utilizzano la stessa chiave privata. Se una delle due viene compromessa, l'autore di un attacco può decrittografare il traffico proveniente da qualsiasi server.
> 2. Se è necessario apportare una modifica al certificato, è necessario eseguire nuovamente l'intero processo anziché una semplice generazione e firma di CSR.

Elenchi CA CA attendibili

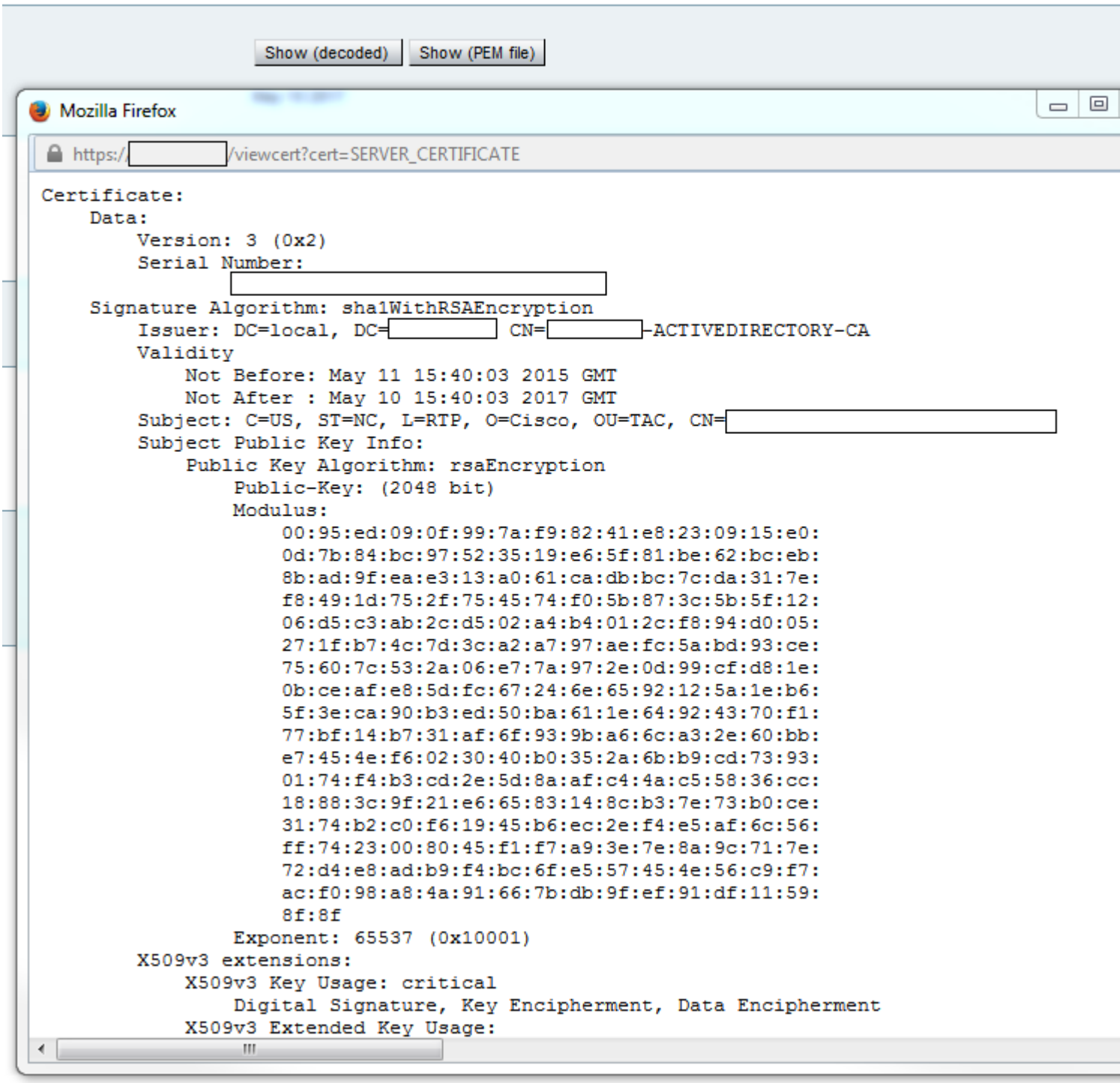
A differenza dei sottoscrittori CUCM in un cluster, l'elenco delle CA attendibili NON viene replicato da un peer all'altro in un cluster Expressway o VCS. Ciò significa che se si dispone di un cluster, è necessario caricare manualmente i certificati attendibili nell'elenco CA di ogni peer.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica le informazioni sul certificato corrente

È possibile controllare le informazioni in un certificato esistente in diversi modi. La prima opzione è tramite il browser Web. Utilizzare il metodo illustrato nella sezione precedente che può essere utilizzato anche per esportare un certificato specifico nella catena. Se è necessario verificare le SAN o altri attributi aggiunti al certificato del server Expressway, è possibile farlo direttamente tramite l'interfaccia grafica utente (GUI) Web, passare a **Manutenzione > Certificati di sicurezza > Certificato server**, quindi fare clic su **Mostra decodificato**.

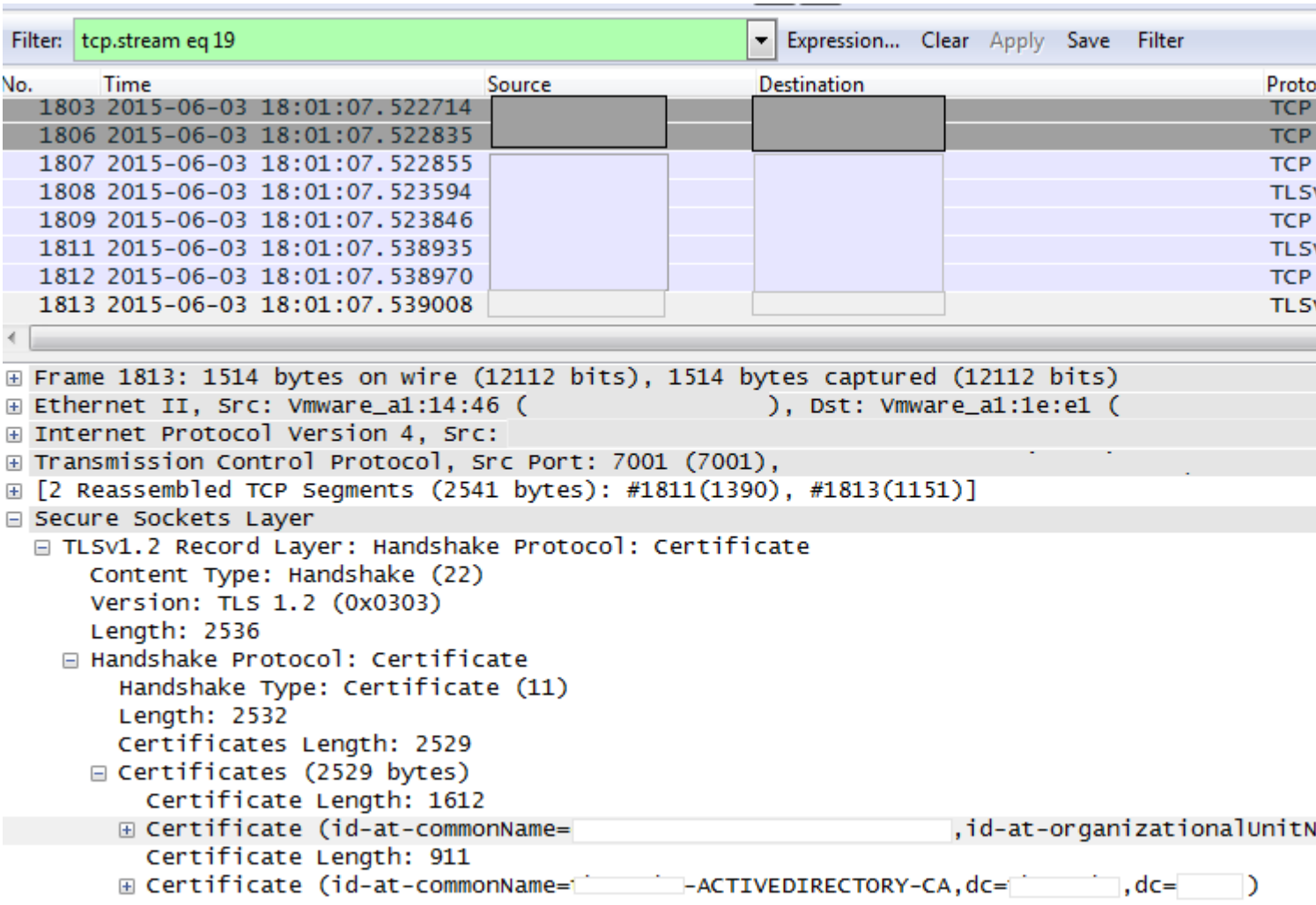


Qui puoi vedere tutti i dettagli specifici del certificato senza doverlo scaricare. È inoltre possibile eseguire la stessa operazione per un CSR attivo se il certificato firmato associato non è stato ancora caricato.

Lettura/Esportazione di un certificato in Wireshark

Se si dispone di un'acquisizione Wireshark dell'handshake SSL che include lo scambio di certificati, Wireshark può effettivamente decodificare il certificato ed è possibile esportare qualsiasi certificato nella catena (se viene scambiata l'intera catena) dall'interno di. Filtra l'acquisizione dei pacchetti per la porta specifica dello scambio di certificati (generalmente 7001 nel caso della zona trasversale). Quindi, se i pacchetti hello del client e del server non vengono visualizzati insieme all'handshake SSL, fare clic con il pulsante destro del mouse su uno dei pacchetti nel flusso TCP e selezionare **decodifica come**. Selezionare

SSL e fare clic su **Applica**. A questo punto, se è stato acquisito il traffico corretto, è necessario visualizzare lo scambio di certificati. Trovare il pacchetto dal server corretto che contiene il certificato nel payload. Espandere la sezione SSL nel riquadro inferiore fino a visualizzare l'elenco dei certificati come mostrato nell'immagine:



In questa finestra è possibile espandere qualsiasi certificato per visualizzare tutti i dettagli. Se si desidera esportare il certificato, fare clic con il pulsante destro del mouse sul certificato desiderato nella catena (se sono presenti più certificati) e selezionare **Esporta byte pacchetto selezionato**. Immettere un nome per il certificato e fare clic su **Salva**. A questo punto, è necessario essere in grado di aprire il certificato in Visualizzatore certificati di Windows (se si assegna l'estensione cer) oppure di caricarlo in qualsiasi altro strumento per l'analisi.

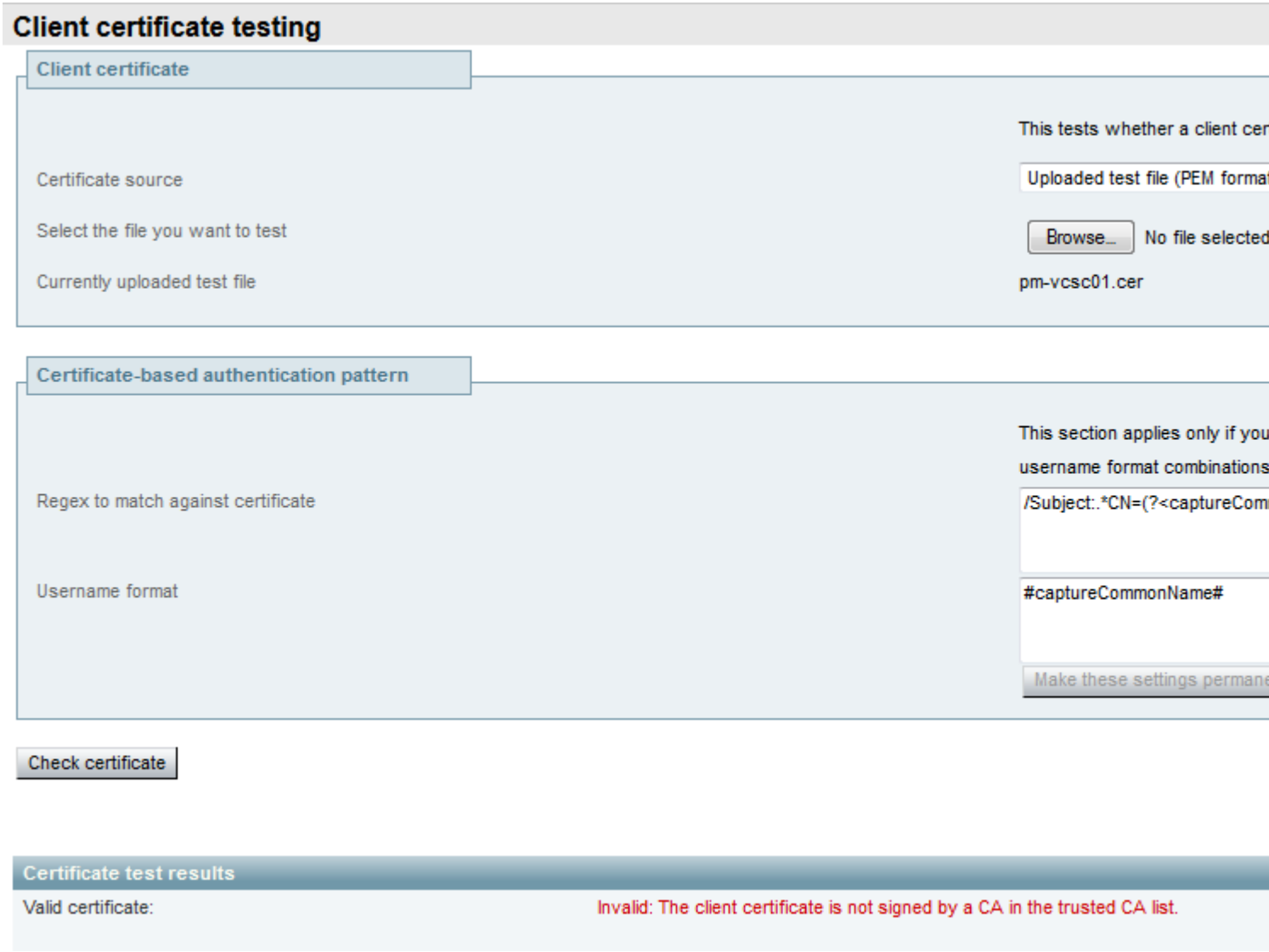
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

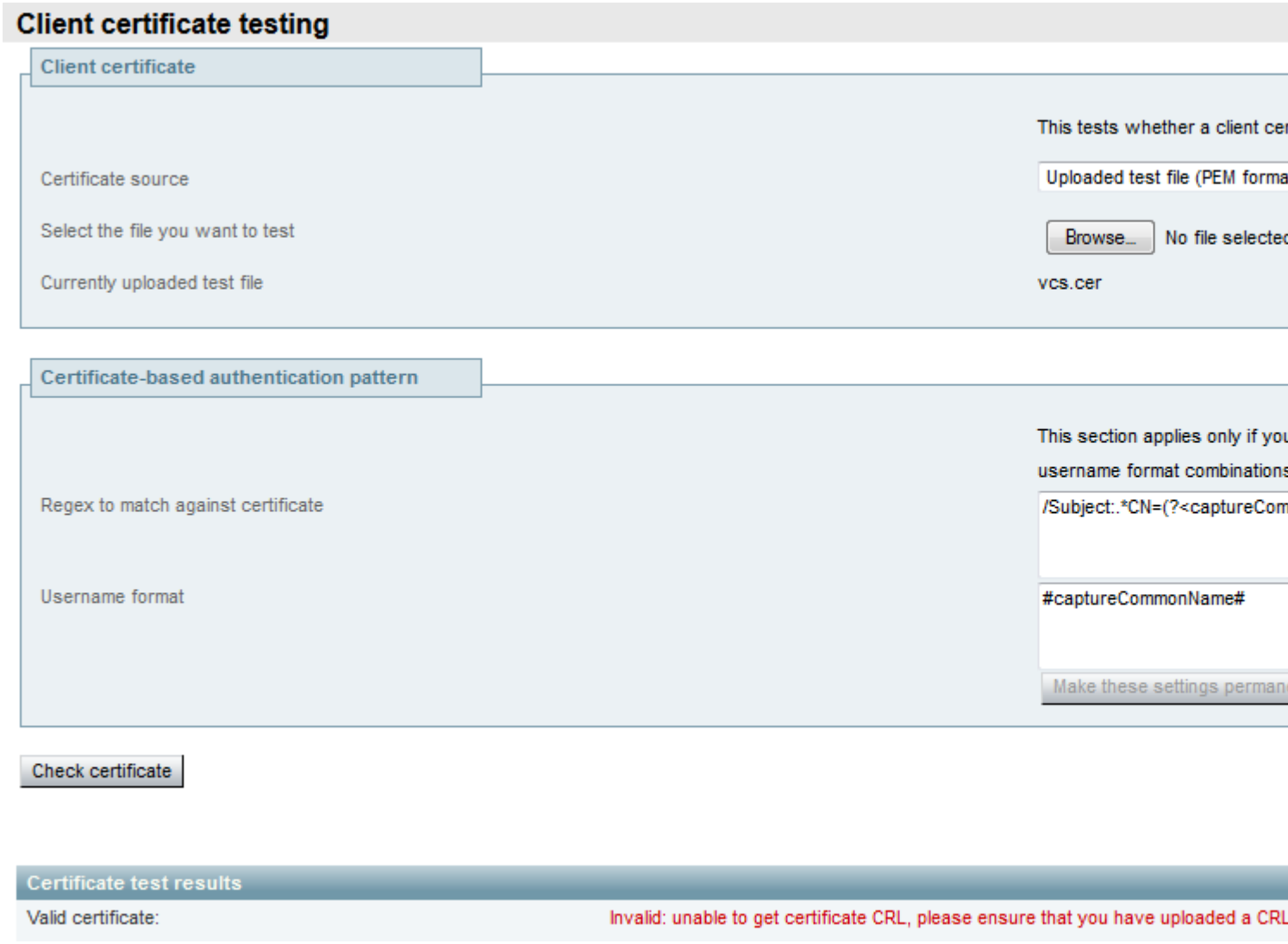
Verifica Dell'Attendibilità Di Un Certificato In Expressway

Sebbene il metodo migliore sia controllare manualmente la catena di certificati e assicurarsi che tutti i membri siano inclusi nell'elenco delle CA attendibili di Expressway, è possibile verificare rapidamente che Expressway consideri attendibile un certificato di un determinato client con l'aiuto di **Client Certificate Testing** in **Manutenzione > Certificati di sicurezza** nell'interfaccia GUI Web. Mantenere invariate tutte le impostazioni predefinite. Selezionare **Upload Test File** (formato pem) dall'elenco a discesa e selezionare il

certificato client da verificare. Se il certificato non è attendibile, verrà visualizzato un errore, come illustrato nell'immagine, che spiega il motivo del rifiuto. L'errore visualizzato è rappresentato dalle informazioni decodificate del certificato caricato come riferimento.



Se viene visualizzato un errore che indica che Expressway non è in grado di ottenere il CRL del certificato, ma Expressway non utilizza il controllo CRL, significa che il certificato sarebbe attendibile e avrebbe superato tutti gli altri controlli di verifica.



Endpoint Synergy Light (telefoni serie 7800/8800)

Questi nuovi dispositivi vengono forniti con un elenco di certificati attendibili precompilato, che include un numero elevato di CA pubbliche conosciute. L'elenco di attendibilità non può essere modificato, pertanto il certificato Expressway-E DEVE essere firmato da una delle CA pubbliche corrispondenti per poter funzionare con questi dispositivi. Se è firmata da una CA interna o da un'altra CA pubblica, la connessione non riesce. Non è disponibile alcuna opzione per l'utente per accettare manualmente il certificato come avviene con i client Jabber.

Nota: per alcune implementazioni è stato rilevato che l'uso di un dispositivo come Citrix NetScaler con una CA inclusa nell'elenco dei telefoni serie 7800/8800 può essere registrato su MRA anche se Expressway-E utilizza una CA interna. La CA radice NetScalers deve essere caricata in Expressway-E, mentre la CA radice interna deve essere caricata in Netscaler affinché l'autenticazione SSL funzioni. È stato dimostrato che funziona, e il suo supporto è il migliore sforzo possibile.

Nota: se l'elenco delle CA attendibili contiene tutti i certificati corretti ma viene comunque rifiutato, verificare che non sia presente un altro certificato più in alto nell'elenco con lo stesso soggetto in conflitto con quello corretto. Se tutto il resto non funziona, è sempre possibile esportare la catena direttamente dal browser o da Wireshark e caricare tutti i certificati nell'elenco dei server di

---

destinazione opposti. In questo modo si garantisce che si tratti del certificato attendibile.

Nota: quando si esegue la risoluzione di un problema di zona di attraversamento, a volte il problema può sembrare correlato a un certificato, ma in realtà si tratta di un problema del software. Verificare che il nome utente e la password dell'account utilizzati per l'attraversamento siano corretti.

Nota: VCS o Expressway non supporta più di 999 caratteri nel campo SAN di un certificato. Le SAN che superano questo limite (che richiedono molti nomi alternativi) verranno ignorate come se non fossero presenti.

Risorse video

In questa sezione vengono fornite informazioni nel video che consentono di eseguire in modo semplificato tutti i processi di configurazione dei certificati.

Genera un CSR per MRA o Espressioni cluster

Installa certificato server in Expressway

Come configurare l'attendibilità dei certificati tra le espressioni

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).