Aggiornamento del certificato CA radice Cisco Webex su 2021-03-31

Sommario

Introduzione

Questo documento descrive come Cisco Webex passerà a una nuova Autorità di certificazione, IdenTrust Commercial Root CA 1. I clienti che usano Expressway per connettersi alle riunioni Webex, o uno dei connettori che usa Expressway, devono caricare il nuovo certificato nei loro dispositivi Expressway **prima del 2021-03-31**.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Video Communication Server (VCS)-Expressway o Expressway.

Problema

Se i certificati CA radice non vengono caricati in un truststore Expressway, la negoziazione TLS con Webex potrebbe non riuscire per queste distribuzioni:

- Gli endpoint vengono utilizzati per connettersi alla piattaforma Cisco Webex Video tramite VCS-Expressway o Expressway Edge. È necessario aggiungere il nuovo certificato nell'archivio radice attendibile di VCS o Expressway.
- Si utilizza un connettore o un servizio ibrido su un VCS-Control o Expressway Core e non si è optato per la gestione dei certificati cloud. È necessario aggiungere il nuovo certificato nell'archivio radice attendibile del software VCS.

- Cisco Webex Edge Audio viene utilizzato tramite VCS-Expressway o Expressway Edge. È necessario aggiungere il certificato nell'archivio radice attendibile di VCS o Expressway.
- **Aggiornamento 2021-03-23:** I clienti che utilizzano Gestione certificati cloud non vedranno il nuovo certificato IdenTrust nel loro elenco di certificati. Il certificato Quovadis esistente (O=QuoVadis Limited, CN=QuoVadis Root CA 2) è ancora valido. Il certificato IdenTrust sarà disponibile per la gestione dei certificati cloud in un futuro TBD. I clienti che utilizzano Cloud Certificate Management non subiranno alcuna interruzione del servizio a seguito di questo annuncio e non dovranno intraprendere alcuna azione al momento.

- Èstato limitato l'accesso agli URL per la verifica degli elenchi di revoche di certificati. È necessario consentire ai client Webex di raggiungere l'elenco di revoche di certificati

disponibile all'indirizzo http://validation.identrust.com/crl/hydrantidcao1.crl.
Cisco ha inoltre aggiunto ***.identrust.com** nell'elenco di URL che devono essere autorizzati per la verifica dei certificati.

- Gli archivi certificati attendibili predefiniti non vengono utilizzati per i sistemi operativi. È necessario aggiungere il certificato all'archivio radice attendibile. Per impostazione predefinita, questo certificato è contenuto nell'archivio di attendibilità predefinito di tutti i principali sistemi operativi.

Soluzione

Questi passaggi sono spiegati anche nell'aggiornamento del certificato CA radice Cisco Webex per Expressway del marzo 2021.

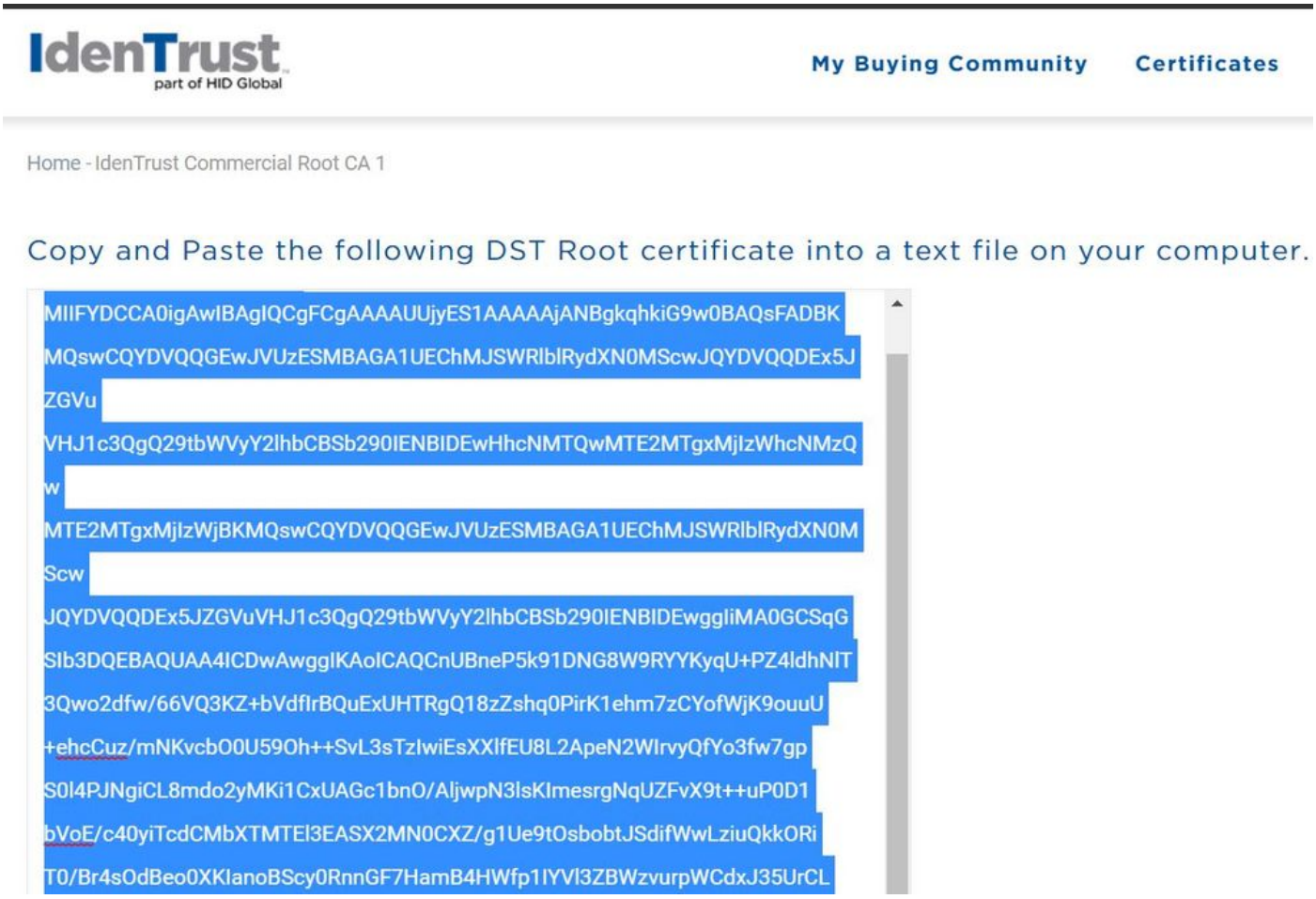
Per caricare il nuovo certificato su VCS-Control, VCS-Expressway, Expressway-Core ed Expressway Edge, attenersi alla seguente procedura.

Passaggio 1: Scaricare IdenTrust Commercial Root CA 1 e salvarlo con il nome **identrust_RootCA1.pem** o **identrust_RootCA1.cer**.

r. Accedere alla CA radice commerciale IdenTrust 1.

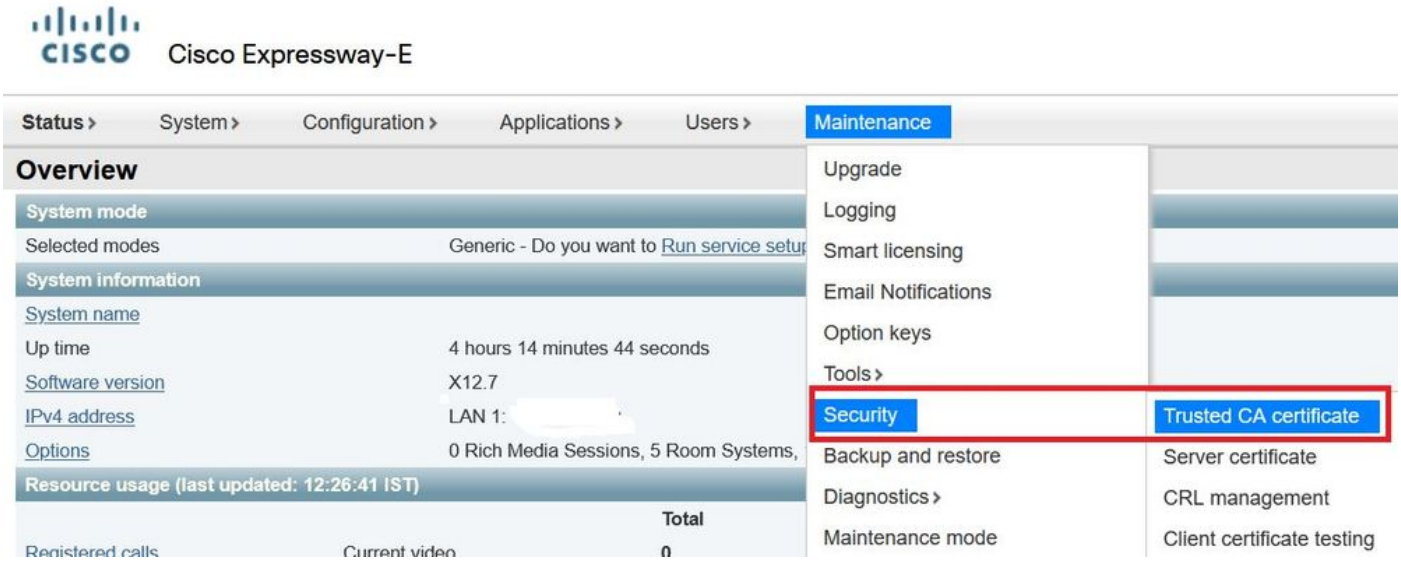
b. Copiare il testo all'interno della casella.

c. Salvare il testo sul Blocco note e salvare il file. Assegnare al file il nome **identrust_RootCA1.pem** o **identrust_RootCA1.cer**.



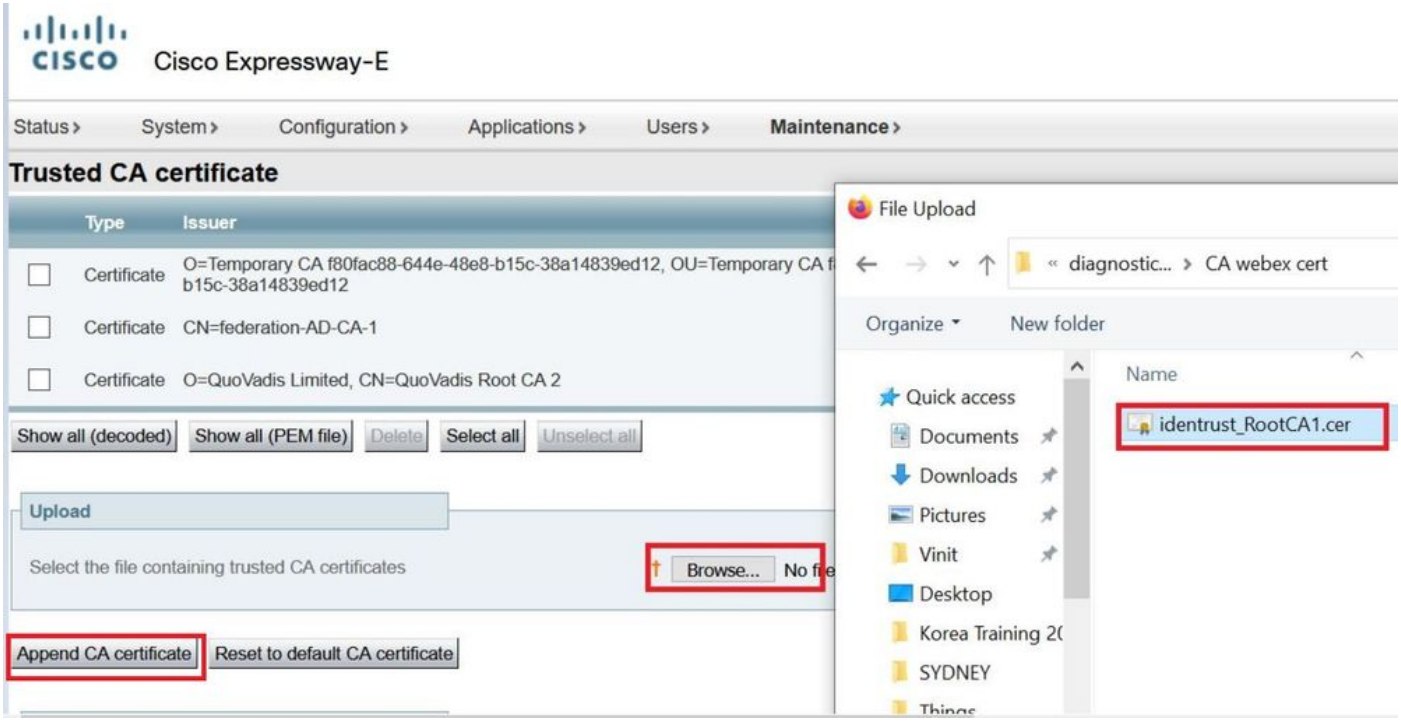
Su tutti i dispositivi Expressway, scegliere **Manutenzione > Sicurezza > Certificato CA attendibile**.

Passaggio 2: Caricare il file nell'archivio attendibile di Expressway.



r. Per caricare il certificato CA nell'archivio di attendibilità di Expressway, fare clic su **Aggiungi certificato CA**.

b. Fare clic su **Sfoglia**. Caricare il file identrust_RootCA1.pem o identrust_RootCA1.cer. Aggiungere il certificato CA.



Passaggio 3: Verificare che il certificato sia stato caricato correttamente e che sia presente nell'archivio di attendibilità di VCS/Expressway.

Dopo questa operazione non è necessario riavviare il sistema per rendere effettive le modifiche.