Cisco Webex Root CA Certificate Update on 2021-03-31

Contents

Introduction

This document describes how Cisco Webex will move to a new Certificate Authority, IdenTrust Commercial Root CA 1. Customers who use Expressway to dial into Webex meetings, or one of the connectors that leverages Expressway, must upload the new certificate to their Expressway devices **before 2021-03-31**.

Components Used

The information in this document is based on Video Communication Server (VCS)-Expressway or Expressway.

Problem

If Root CA certificates are not uploaded on Expressway truststore, TLS negotiation with Webex might fail for these deployments:

- You use endpoints to connect to the Cisco Webex Video Platform through a VCS-Expressway or Expressway Edge. You must add the new certificate into the Trusted Root Store of the VCS or Expressway.
- You use a Connector or Hybrid Service on a VCS-Control or Expressway Core and have not opted into Cloud Certificate Management. You must add the new certificate into the Trusted Root Store of the VCS.

- You use Cisco Webex Edge Audio through a VCS-Expressway or Expressway Edge. You must add the certificate into the trusted root store of the VCS or Expressway.
- **2021-03-23 update:** Customers that leverage Cloud Certificate Management will not see the new IdenTrust certificate in their list of certificates currently. The existing Quovadis (O=QuoVadis Limited, CN=QuoVadis Root CA 2) certificate is still valid. The IdenTrust certificate will become available to Cloud Certificate Management at a future TBD time. Customers who utilize Cloud Certificate Management will not experience any service interruptions as a result of this announcement and do not need to take any actions at this time.

- You have restricted access to URLs for checking Certificate Revocation Lists. You must allow

Webex clients to reach the Certificate Revocation List hosted at http://validation.identrust.com/crl/hydrantidcao1.crl.
Cisco has also added ***.identrust.com** into the list of URLs that must be allowed for certificate verification.

- You do not use the default Certificate Trust Stores for your operating systems. You must add the certificate into your trusted root store. This certificate is contained within the default trust store of all major operating systems by default.

Solution

These steps are also explained in the March 2021 Cisco Webex Root CA Certificate update for Expressway video.

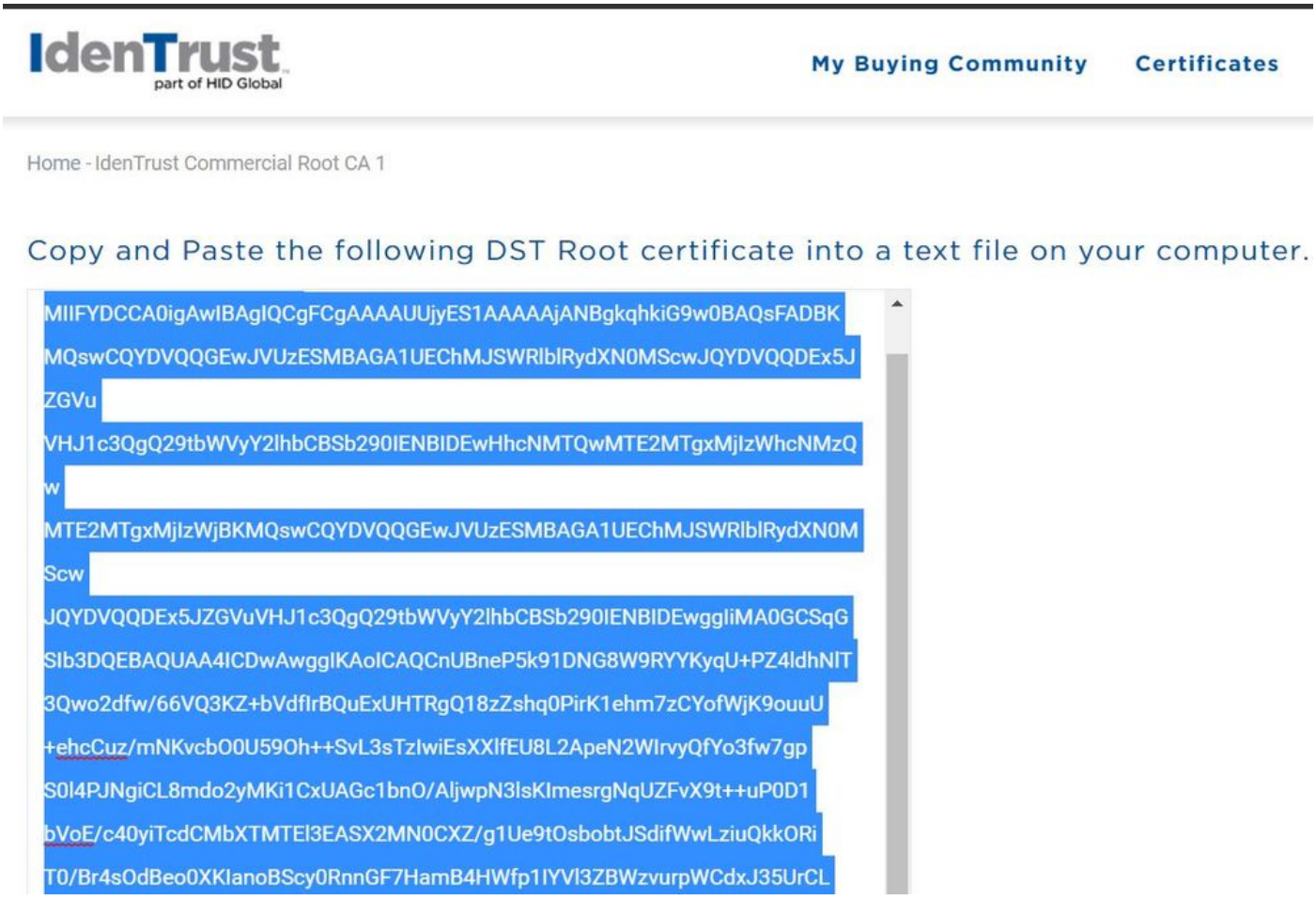
In order to upload the new certificate onto a VCS-Control, VCS-Expressway, Expressway-Core, and Expressway Edge, complete these steps.

Step 1: Download the IdenTrust Commercial Root CA 1 and save it as **identrust_RootCA1.pem** or **identrust_RootCA1.cer**.

a. Access IdenTrust Commercial Root CA 1.

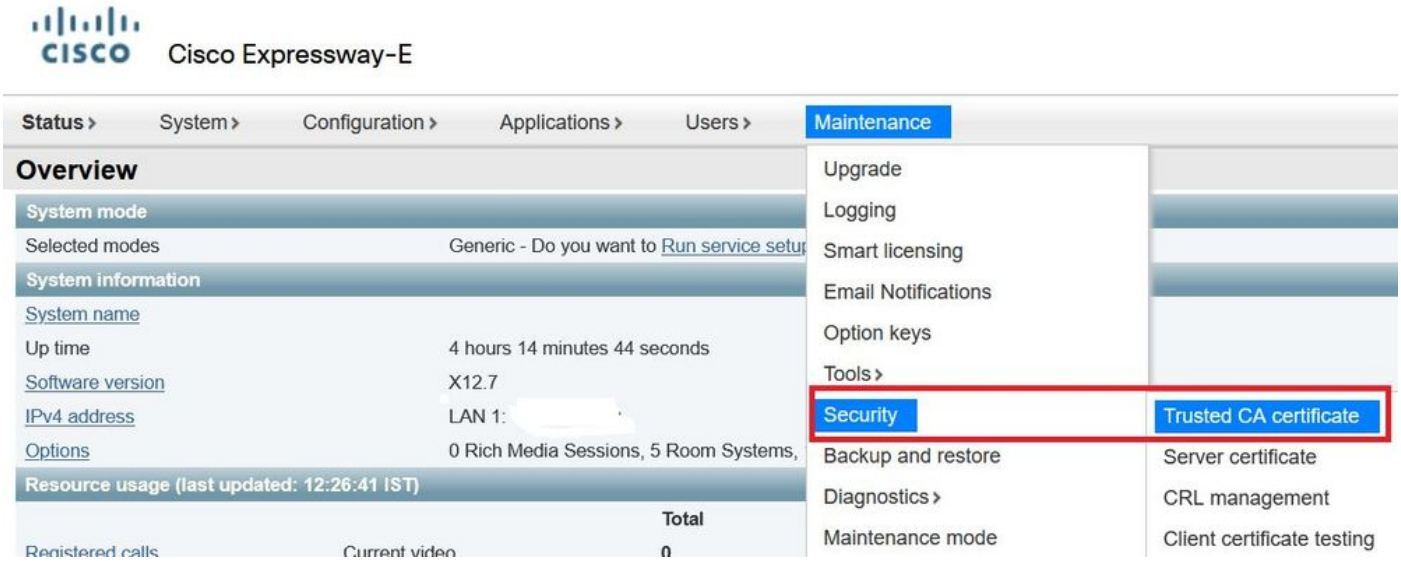
b. Copy the text inside the box.

c. Save the text on Notepad and save the file. Name the file **identrust_RootCA1.pem** or **identrust_RootCA1.cer**.



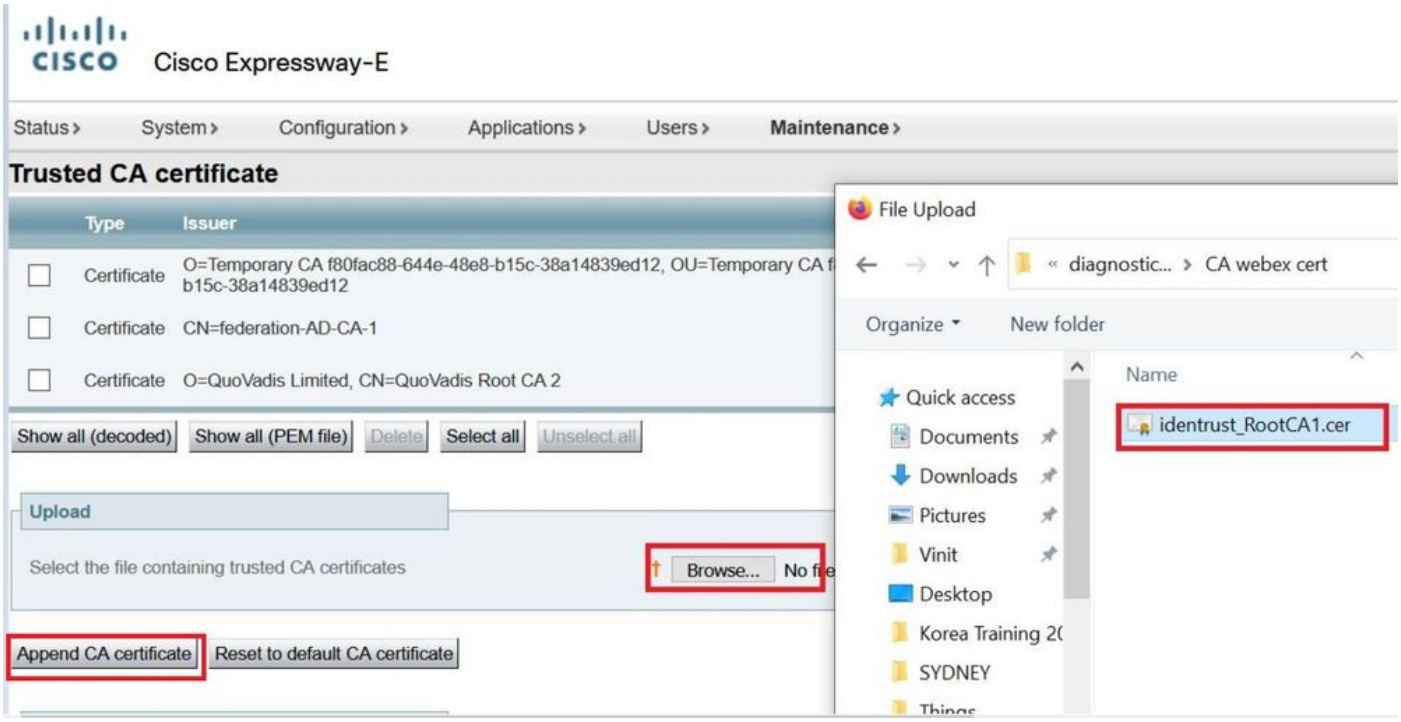
On all your Expressway devices, choose **Maintenance > Security > Trusted CA Certificate**.

Step 2: Upload the file on Expressway Trust Store.



a. In order to upload the CA certificate on Expressway Trust Store, click **Append CA certificate**.

b. Click **Browse**. Upload the identrust_RootCA1.pem or identrust_RootCA1.cer file. Append the CA certificate.



Step 3: Verify the certificate successfully uploaded and is present in the VCS / Expressway Trust Store.

No reboot or restart is required after this operation for the changes to take effect.