

Renew Expressway Certificate

Contents

[Introduction](#)

[Background information](#)

[Process](#)

[A\) Get information from the current certificate](#)

[B\) Generate the CSR\(Certificate Signing Request\) and send it to the CA\(Certification Authority\) for signing.](#)

[C\) Check the SAN list and Extended/Enhanced key usage attribute in the new certificate](#)

[D\) Check if the CA which signed the new certificate is the same as the CA which signed the old certificate](#)


[E\) Install the new certificate](#)

Introduction

This document describes the Expressway/Video Communication Server (VCS) certificate renewal process.

Background information

The information in this document applies to both Expressway and VCS. The document references Expressway but this can be interchanged with VCS.

 **Note:** While this document is designed to help you with the certificate renewal process, it is a good idea to also check the [Cisco Expressway Certificate Creation and Use Deployment Guide](#) for your version.

Whenever a certificate is to be renewed, two main points must be considered in order to verify that the system continues to function properly after the new certificate is installed:

1. The attributes of the new certificate must match those of the old certificate (mainly the Subject Alternate Name and Extended key usage).
2. The CA(Certification Authority) that signs the new certificate must be trusted by other servers that communicate directly with the Expressway (for example CUCM, Expressway-C, Expressway-E,...).

Process

A) Get information from the current certificate

1. Open Expressway **Webpage Maintenance > Security > Server certificate > Show decoded.**
2. In the new window that opens, copy the **Subject Alternative name** and **Authority Key Identifier X509v3** extensions to a notepad document.

X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
DNS:expe.nart.com, DNS:expe2.nart.com, DNS:expe1.nart.com, DNS:guest.vngtpres.aca, DNS:join.nart.com, DNS:meeting.nart.com, DNS:meet.nart.com, DNS:guest.vngtp.aca, DNS:vngtp.lab, DNS:nart.com
X509v3 Subject Key Identifier:
BE:72:22:D2:61:D3:4B:FB:44:34:8B:DA:7B:D6:C9:17:14:BB:8C:31
X509v3 Authority Key Identifier:
keyid:45:8E:34:17:B0:6E:19:DC:6F:52:65:0F:FC:CB:01:06:18:C2:B6:27

"Show decoded" certificate window

B) Generate the CSR(Certificate Signing Request) and send it to the CA(Certification Authority) for signing.

1. From Expressway **Webpage Maintenance > Security > Server certificate > Generate CSR.**

2. In the Generate CSR window, in the **Additional alternative names (comma separated)** field, enter all the values for **Subject Alternative Names** that were saved in the section A, and remove **DNS:** and separate the list with commas.

In this image, next to **Alternative name as it appears**, there is a list of all the SANs to be used in the certificate):

Alternative name

Subject alternative names: None

Additional alternative names (comma separated): expe.nart.com,expe2.nart.com,expe1.nart.com,guest.

Unified CM registrations domains: Format: DNS


Alternative name as it will appear:

- DNS:expe1.nart.com
- DNS:expe.nart.com
- DNS:expe2.nart.com
- DNS:guest.vngtpres.aca
- DNS:join.nart.com
- DNS:meeting.nart.com
- DNS:meet.nart.com
- DNS:guest.vngtp.aca
- DNS:vngtp.lab
- DNS:nart.com

Generate CSR SAN entries

3. Input the rest of the information under the **Additional Information** section (such as country, company, state,...) and click on **Generate CSR.**

4. After you have generated the CSR, the page **Maintenance > Security > Server Certificate** shows an option to **Discard CSR** and **Download.** Choose **Download** and send the CSR to the CA for signing.


 **Note:** Do not **Discard CSR** before the new certificate is installed. If **Discard CSR** was done and then an attempt is made to install a certificate signed with the CSR that was discarded, the certificate install fails.

C) Check the SAN list and Extended/Enhanced key usage attribute in the new certificate

Open the newly signed certificate in Windows certificate manager and verify:

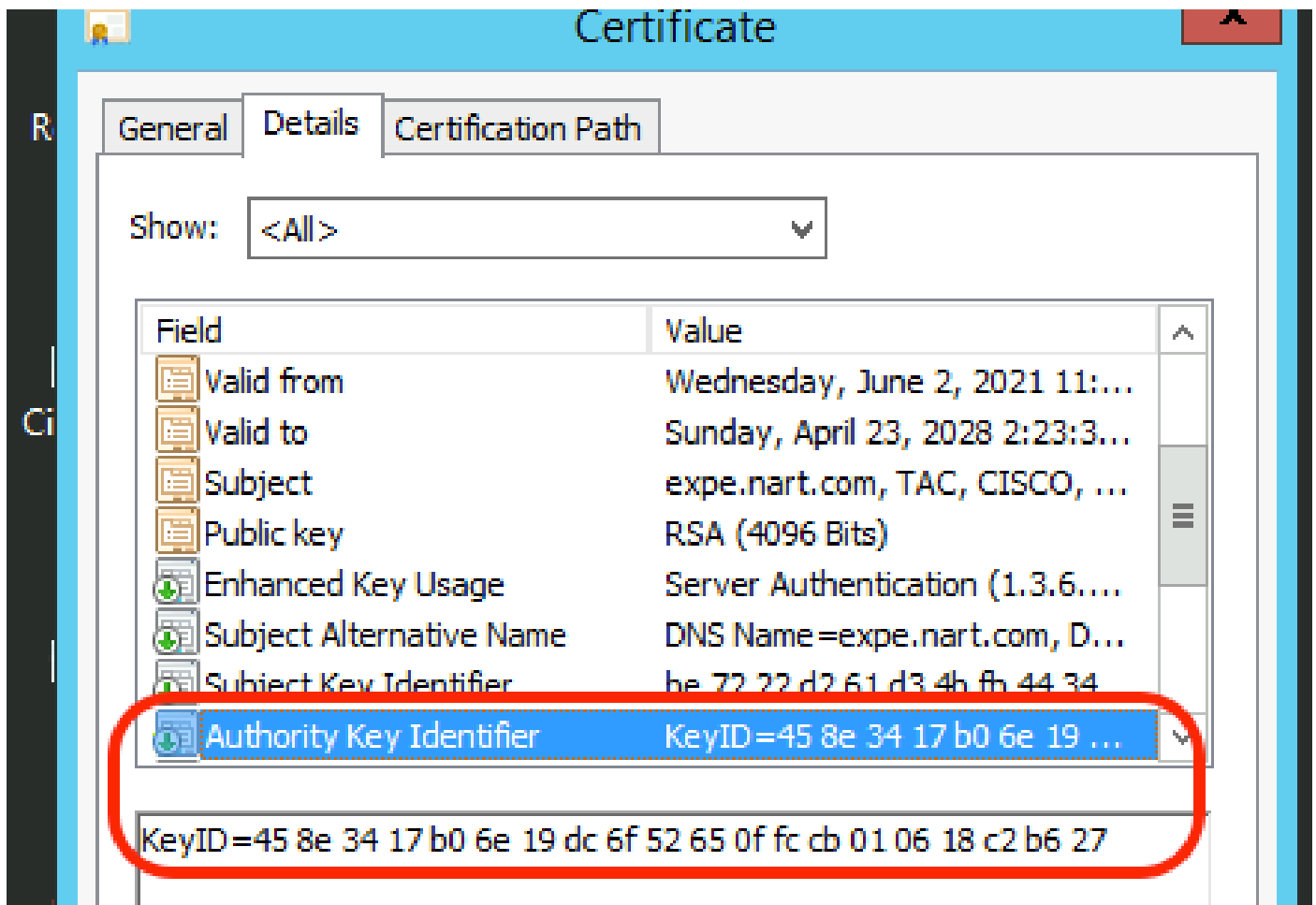
1. The SAN list matches the SAN list that we saved in the section A which we used we generated the CSR.
2. The "**Extended/Enhanced key usage**" attribute must include both **Client Authentication** and **Server**

Authentication.

 **Note:** If the certificate has the .pem extension, rename it to .cer or .crt to be able to open it with Windows Certificate Manager. Once the certificate is open with Windows Certificate Manager, you can go to the **Details** tab > **Copy to File** and export it as a Base64 encoded file, a base64 encoded file normally has "-----BEGIN CERTIFICATE-----" at the top and "-----END CERTIFICATE-----" at the bottom when opened in a text editor

D) Check if the CA which signed the new certificate is the same as the CA which signed the old certificate

Open the newly signed certificate in Windows certificate manager and copy the **Authority Key Identifier** value and compare it with the **Authority Key Identifier** value that we saved in section A.



New certificate opened with Windows Certificate Manager

If both values are the same, that means the same CA was used to sign the new certificate as the one that was used to sign the old certificate, and you can proceed to section E to upload the new certificate.

If the values are different, this means that the CA used to sign the new certificate is different than the CA used to sign the old certificate, and the steps to take before you can proceed to section E are:

1. Get all the Intermediate CA certificate(s), if any, and the Root CA certificate.
2. Go to **Maintenance > Security > Trusted CA certificate**, click **Browse** then search for the intermediate CA certificate on your computer and upload it. Do the same for any other intermediate CA certificates and

the root CA certificate.

3. Do the same on any Expressway-E (if the certificate to be renewed is an Expressway-C certificate) that connects to this server or any Expressway-C (if the certificate to be renewed is an Expressway-E certificate) that connects to this server.

4. If the certificate to be renewed is an Expressway-C certificate and you have MRA or have secure zones to CUCM


- Verify that CUCM trusts the new root and intermediate CA.
- Upload the root and intermediate CA certificates to CUCM tomcat-trust and callmanager-trust stores.
- Restart the relevant services on CUCM.

E) Install the new certificate

Once all the previous points have been checked, you can install the new certificate on the Expressway from **Maintenance > Security > Server Certificate** .

Click on **Browse** and select the new certificate file from your computer and upload it.

You must restart the Expressway after you install a new certificate.

 **Note:** Verify that the certificate to be uploaded to Expressway from **Maintenance > Security > Server Certificate** contains only the Expressway server certificate and *not* the full certificate chain and verify that it is a Base64 certificate.

Adding a Single Certificate to Multiple Expressways:

- Create a single certificate for the whole expressway-e cluster.
- Create a CSR that contains all the FQDNs plus the extra features that you use on your expressways (if CMS web rtc, the join url and domain, if MRA, your registrations/login domains)

Example:

Exwycluster.domain

Exwy1.domain

Exwy2.domain

Exwy3.domain

Exwy4.domain

Extra features (domains or CMS URL)

- After the CSR is done, you can extract the private key of this CSR by using a SFTP program (I recommend you WinSCP, we use it a lot)
- Open WinSCP and connect to the expressway-e that created the CSR
- Navigate to tandberg/persistent/certs/ CSR or certificate signing request (might show as well as pending)
- Copy the private key from the expressway-e into your desktop,
- After that is done, we can use the same certificate for all your 4 nodes.