

Generate New Expressway Certificate with the Information from the Current Certificate.

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Step 1. Locate the Current Certificate Information.](#)

[Step 2. Create a New CSR with the Information Obtained Above.](#)

[Step 3. Verify and Download the New CSR.](#)

[Step 4. Verify the Information Contained in the New Certificate.](#)

[Step 5. Upload the New CA Certificates to the Servers Trusted Store if Applicable.](#)

[Step 6. Upload the new Certificate to the Expressway Server.](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to generate a new Certificate Signing Request (CSR) with the information in the existing Expressway certificate.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Certificate Attributes
- Expressways or Video Communication Server (VCS)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step 1. Locate the Current Certificate Information.

In order to obtain the information contained in the current certificate, navigate to **Maintenance > Security > Server Certificate** on the Expressway Graphical User Interface (GUI).

Locate the section **Server certificate data** and select **Show (decoded)**.

Look for the information in the **Common Name (CN)** and **Subject Alternative Name (SAN)** as shown in the image:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1

Signature Algorithm: sha256WithRSAEncryption

Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA

Validity

Not Before: Dec 2 04:39:57 2019 GMT

Not After : Nov 28 00:32:43 2020 GMT

Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, **CN=expe.domain.com**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

-----BEGIN-----

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication, TLS Web Server Authentication

X509v3 Subject Alternative Name:

DNS:expe.domain.com, DNS:domain.com

X509v3 Subject Key Identifier:

92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B

X509v3 Authority Key Identifier:

keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32

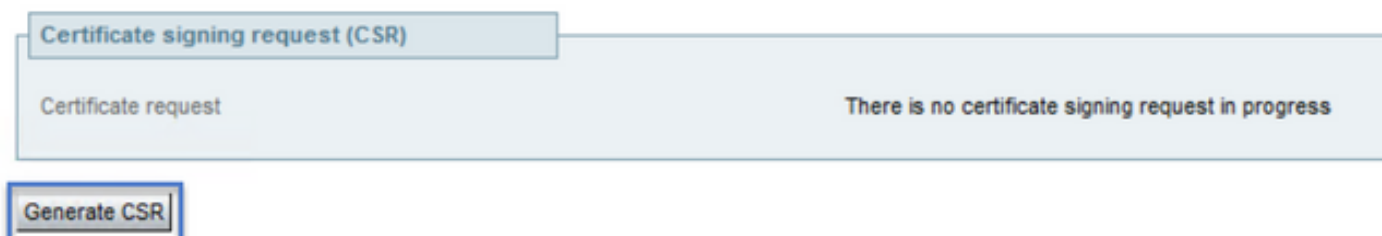
Now that you know the CN and the SAN's copy them so they can be added to the new CSR.

Optionally you can copy the additional information for the certificate which is Country (C), State (ST), Locality (L), Organization (O), Organizational Unit (OU). This information is next to the CN.

Step 2. Create a New CSR with the Information Obtained Above.

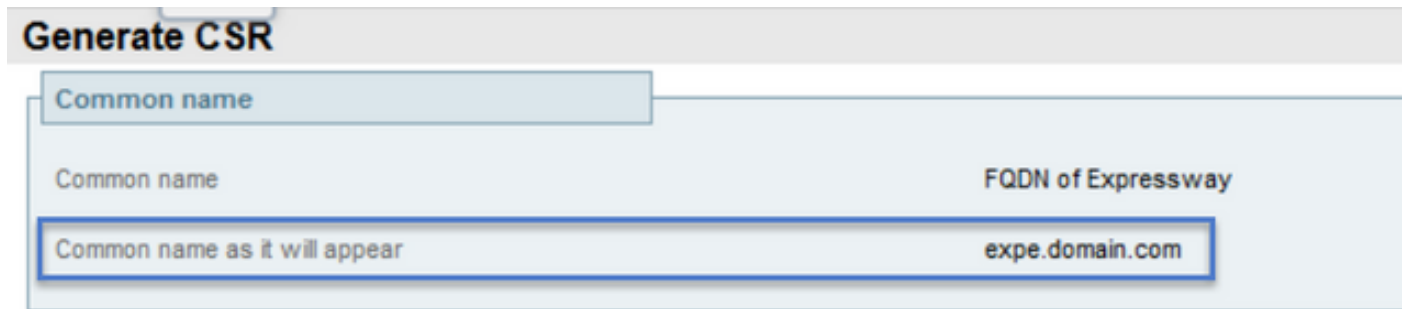
In order to create the CSR navigate to **Maintenance > Security > Server Certificate**.

Locate the section **Certificate signing request (CSR)** and select **Generate CSR** as shown in the image:



Enter the values collected from the current certificate.

The CN cannot be modified unless it is a cluster. In case of a cluster you can select the CN to be the Expressway Fully Qualified Domain Name (FQDN) or the cluster FQDN. In this document a single server is used and hence the CN corresponds to what you obtained from the current certificate as shown in the image:



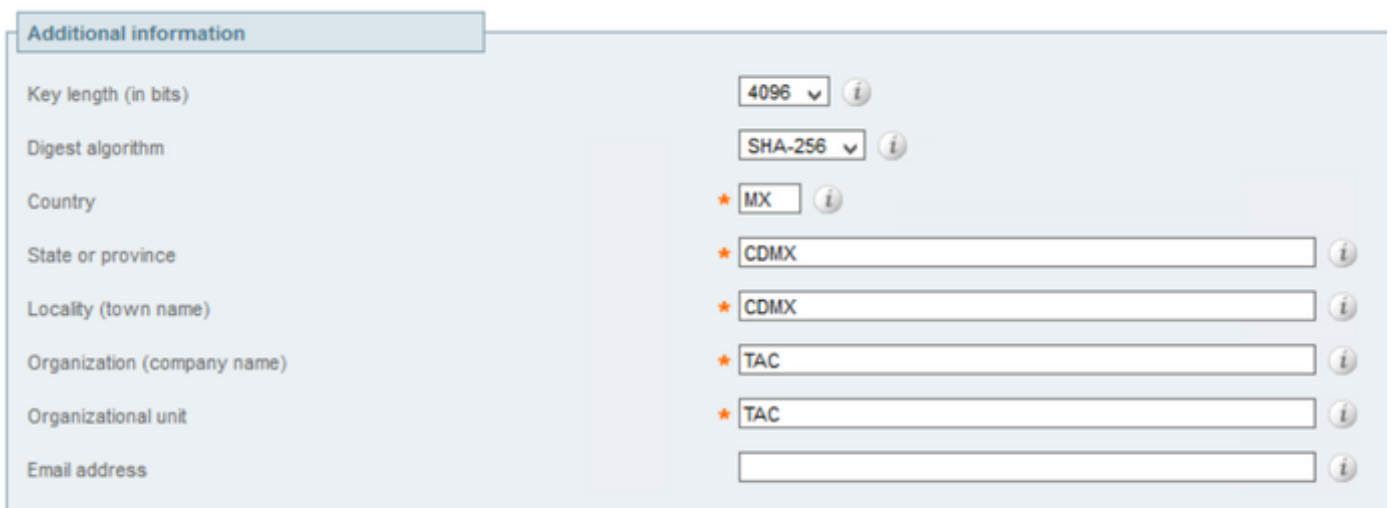
The screenshot shows the 'Generate CSR' section of a web interface. A tab labeled 'Common name' is selected. Below it, there are two input fields. The first is labeled 'Common name' and the second is labeled 'FQDN of Expressway'. The 'Common name as it will appear' field contains the text 'expe.domain.com'.

For the SANs you have to enter the values manually in case they are not autopopulated, in order to do it you can enter the values on the **Additional alternative names**, if you have multiple SANs they have to be comma separated for example: example1.domain.com, example2.domain.com, example3.domain.com. Once added the SANs are listed on the **Alternative name as it will appear** section, as shown in the image:



The screenshot shows the 'Alternative name' section of a web interface. A tab labeled 'Alternative name' is selected. Below it, there are three input fields. The first is labeled 'Additional alternative names (comma separated)' and contains the text 'domain.com'. The second is labeled 'Unified CM registrations domains' and is empty. The third is labeled 'Alternative name as it will appear' and contains the text 'DNS:domain.com'. There is also a 'Format' dropdown menu set to 'DNS'.

The **Additional information** is required, if it is not autopopulated or has to be changed, it has to be manually entered as shown in the image:



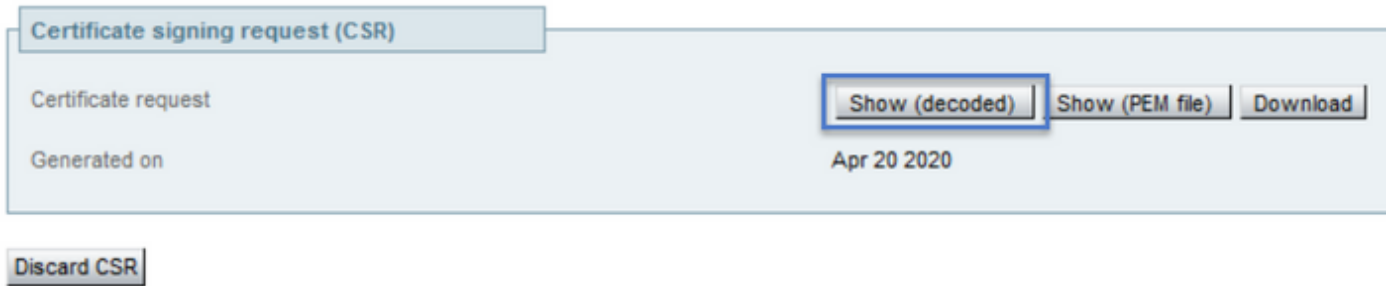
The screenshot shows the 'Additional information' section of a web interface. A tab labeled 'Additional information' is selected. Below it, there are several input fields and dropdown menus. The fields are: 'Key length (in bits)' with a dropdown set to '4096'; 'Digest algorithm' with a dropdown set to 'SHA-256'; 'Country' with a dropdown set to 'MX'; 'State or province' with a text input set to 'CDMX'; 'Locality (town name)' with a text input set to 'CDMX'; 'Organization (company name)' with a text input set to 'TAC'; 'Organizational unit' with a text input set to 'TAC'; and 'Email address' with an empty text input.

Generate CSR

Once finished, select **Generate CSR**.

Step 3. Verify and Download the New CSR.

Now that the CSR is generated you can select **Show (decoded)** on the **Certificate signing request (CSR)** section to verify that all the SANs are present, as shown in the image:



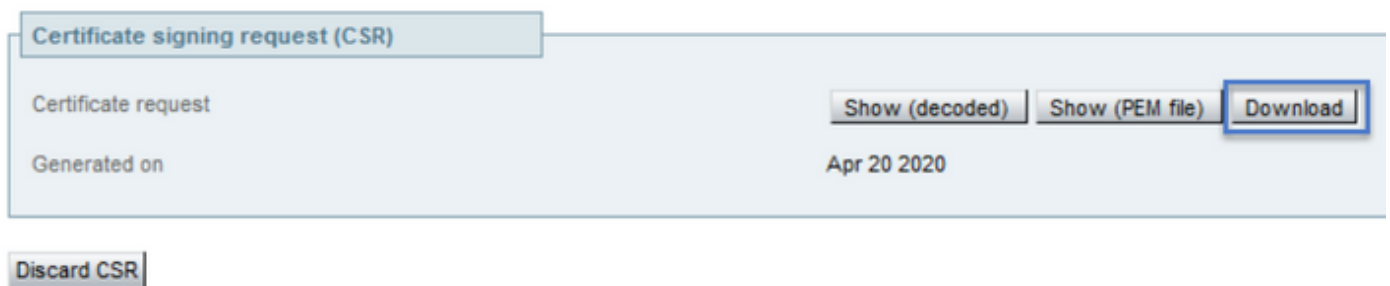
In the new window look for the **CN** and the **Subject Alternative Name** as shown in the image:

```
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
```

The CN is always added as a SAN automatically:

```
X509v3 Extended Key Usage:
  TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
  DNS:expe.domain.com, DNS:domain.com
Signature Algorithm: sha256WithRSAEncryption
```

Now that the CSR has been verified you can close the new window and select **Download (decoded)** on the **Certificate signing request (CSR)** section as shown in the image:

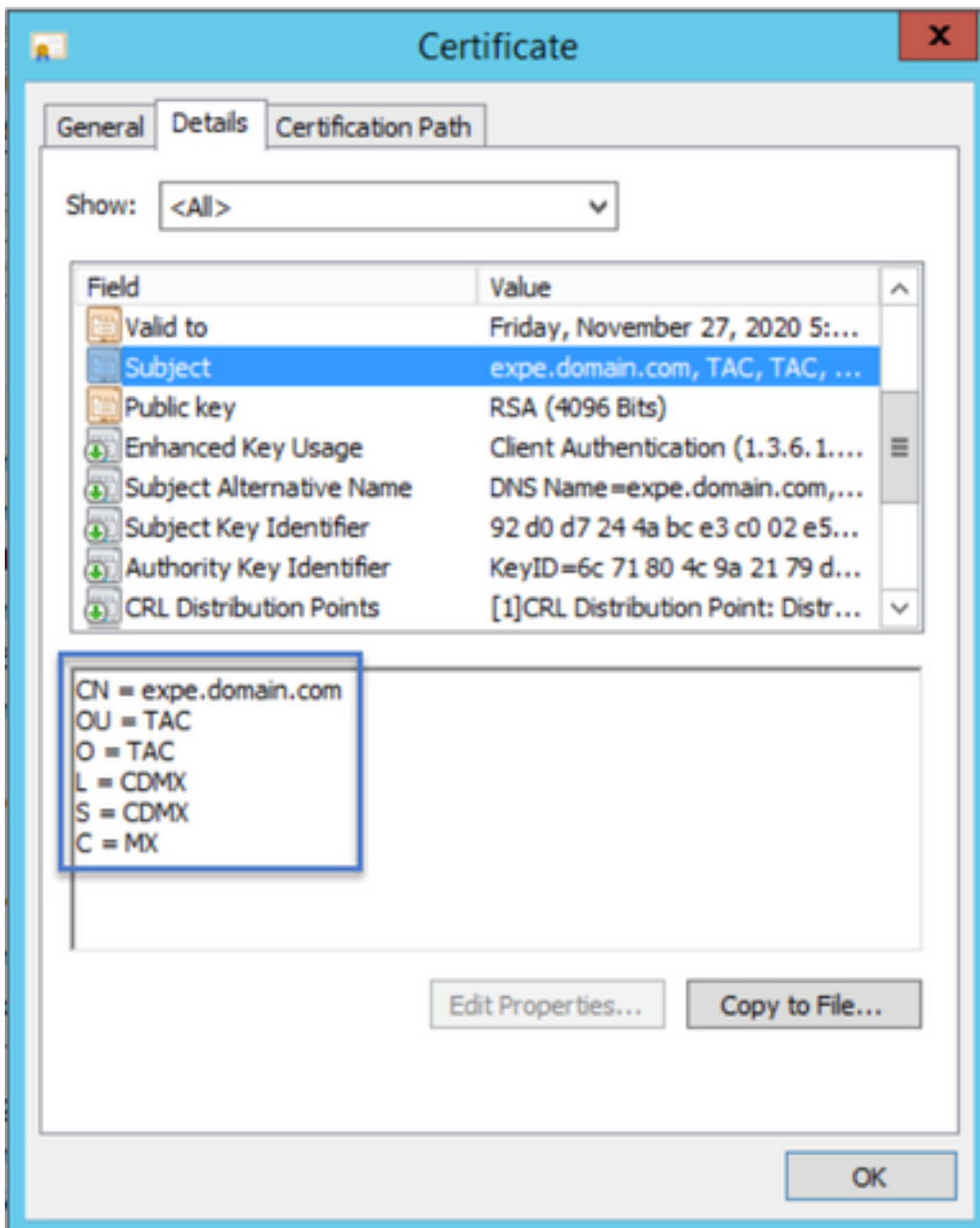


After it is downloaded you can send the new CSR to your Certificate Authority (CA) to be signed.

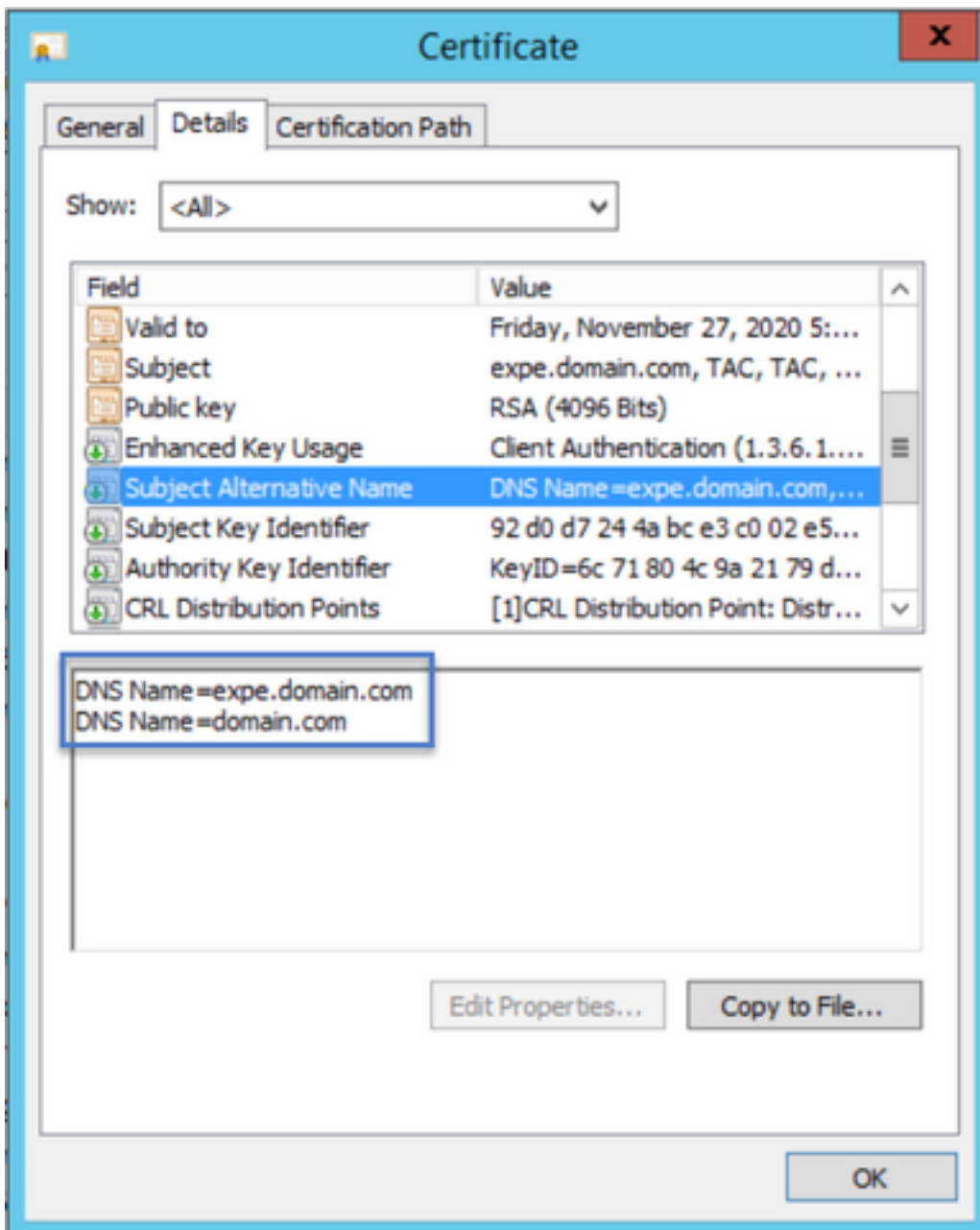
Step 4. Verify the Information Contained in the New Certificate.

Once the new certificate is returned from the CA you can verify if all the SANs are present in the certificate. In order to do that, you can open the certificate and look for the SANs attributes. In this document a Windows PC is used to see the attributes, this is not the only method as long as you can open or decode the certificate to review the attributes.

Open the certificate and navigate to the **Details** tab and look for **Subject**, it should contain the CN and the Additional Information as shown in the image:



Also look for the **Subject Alternative Name** section, it must contain the SANs you entered in the CSR as shown in the image:



If all the SANs you entered in the CSR are not present in the new certificate contact you CA to see if extra SANs are permitted for your certificate.

Step 5. Upload the New CA Certificates to the Servers Trusted Store if Applicable.

If the CA is the same that signed your old Expressway certificate you can discard this step. If it is a different CA then you have to upload the new CA certificates to the trusted CA list in each of the Expressway servers. If you have Transport Layer Security (TLS) zones between the Expressways, for example between an Expressway-C and an Expressway-E you have to upload the new CAs on both servers so that they can trust each other.

In order to do that you can upload your CA certificates one by one. Navigate to **Maintenance > Security > Trusted CA certificates** on the Expressway's.

1. Select **Browse**.
2. On the new page Select the CA Certificate.
3. Select **Append CA Certificate**.

This procedure has to be done for each CA certificate in the certificate chain (Root and Intermediates) and has to be done in all the Expressway servers even if they are clustered.

Step 6. Upload the new Certificate to the Expressway Server.

If all the information in the new certificate is correct, in order to upload the new certificate navigate to: **Maintenance > Security > Server Certificate.**

Locate the **Upload new certificate** section as shown in the image:

1. Select **Browse** on the **Select the server certificate file** section.
2. Select the new certificate.
3. Select **Upload server certificate data.**

Upload new certificate

Select the server private key file

Select the server certificate file

System will use the private key file generated at the same time as the CSR.

Browse... ExpECertNew.cer

Upload server certificate data

If the new certificate is accepted by the Expressway, the Expressway prompts for a restart to apply the changes and the message displays the new expiration date for the certificate, as shown in the image:

Server certificate

Files uploaded: Server certificate updated, however a restart is required for this to take effect.

Certificate info: This certificate expires on Nov 28 2020.

Server certificate data

Server certificate	Show (decoded)	Show (PEM file)
Currently loaded certificate expires on	Nov 28 2020	
Certificate Issuer	anmiron-SRV-AD-CA	

Reset to default server certificate

In order to restart the Expressway select **restat**.

Verify

Once the server is back the new certificate must have been installed, you can navigate to: **Maintenance > Security > Server Certificate** in order to confirm.

Locate the **Server certificate data** and look for the **Currently loaded certificate expires on** section, it displays the new expiration date for the certificate as shown in the image:

Server certificate

Server certificate data

Server certificate

Show (decoded)

Show (PEM file)

Currently loaded certificate expires on

Nov 28 2020

Certificate Issuer

anmiron-SRV-AD-CA

Reset to default server certificate

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.