

Gerar novo certificado Expressway com as informações do certificado atual.

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Etapa 1. Localize as informações atuais do certificado.](#)

[Etapa 2. Crie um novo CSR com as informações obtidas acima.](#)

[Etapa 3. Verifique e faça o download do novo CSR.](#)

[Etapa 4. Verifique as informações contidas no novo certificado.](#)

[Etapa 5. Carregue os novos certificados CA para a Loja confiável de servidores, se aplicável.](#)

[Etapa 6. Carregue o novo certificado no servidor Expressway.](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como gerar uma nova solicitação de assinatura de certificado (CSR) com as informações no certificado Expressway existente.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Atributos de certificado
- Expressways ou Video Communication Server (VCS)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1. Localize as informações atuais do certificado.

Para obter as informações contidas no certificado atual, navegue para **Manutenção > Segurança > Certificado do servidor** na Interface Gráfica do Usuário (GUI) do Expressway.

Localize a seção **Dados do certificado do servidor** e selecione **Mostrar (decodificado)**.

Procure as informações no **Common Name (CN)** e no **Subject Alternative Name (SAN)**, conforme mostrado na imagem:

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:

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

Agora que você conhece o CN e a SAN, copie-os para que possam ser adicionados ao novo CSR.

Opcionalmente, você pode copiar as informações adicionais para o certificado que é País (C), Estado (ST), Localidade (L), Organização (O), Unidade Organizacional (OU). Essas informações estão ao lado do CN.

Etapa 2. Crie um novo CSR com as informações obtidas acima.

Para criar o CSR, navegue para **Manutenção > Segurança > Certificado do servidor**.

Localize a seção **Solicitação de assinatura de certificado (CSR)** e selecione **Gerar CSR** conforme mostrado na imagem:

Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

[Generate CSR](#)

Insira os valores coletados do certificado atual.

A CN não pode ser modificada a menos que seja um cluster. No caso de um cluster, você pode selecionar o CN para ser o FQDN (Nome de domínio totalmente qualificado) do Expressway ou o FQDN do cluster. Neste documento, um único servidor é usado e, portanto, o CN corresponde ao que você obteve do certificado atual, como mostrado na imagem:

Generate CSR

Common name FQDN of Expressway

Common name as it will appear expe.domain.com

Para as SANs, é necessário inserir os valores manualmente caso não sejam preenchidos automaticamente, para que você possa inserir os valores nos **nomes alternativos adicionais**, se houver várias SANs, elas terão que ser separadas por vírgula, por exemplo: example1.domain.com, example2.domain.com, example3.domain.com. Depois de adicionadas, as SANs são listadas no **nome alternativo**, pois serão exibidas, como mostrado na imagem:

Alternative name

Additional alternative names (comma separated) ⓘ

Unified CM registrations domains Format DNS ⓘ

Alternative name as it will appear DNS:domain.com

As **informações adicionais** são obrigatórias, se não forem preenchidas automaticamente ou tiverem de ser alteradas, elas devem ser inseridas manualmente conforme mostrado na imagem:

Additional information	
Key length (in bits)	4096 <input type="button" value="i"/>
Digest algorithm	SHA-256 <input type="button" value="i"/>
Country	* MX <input type="button" value="i"/>
State or province	* CDMX <input type="button" value="i"/>
Locality (town name)	* CDMX <input type="button" value="i"/>
Organization (company name)	* TAC <input type="button" value="i"/>
Organizational unit	* TAC <input type="button" value="i"/>
Email address	<input type="text"/> <input type="button" value="i"/>

Quando terminar, selecione **Gerar CSR**.

Etapa 3. Verifique e faça o download do novo CSR.

Agora que o CSR é gerado, você pode selecionar **Mostrar (decodificado)** na seção **Solicitação de assinatura de certificado (CSR)** para verificar se todas as SANs estão presentes, como mostrado na imagem:

Certificate signing request (CSR)	
Certificate request	<input type="button" value="Show (decoded)"/> <input type="button" value="Show (PEM file)"/> <input type="button" value="Download"/>
Generated on	Apr 20 2020

Na nova janela, procure o **CN** e o **nome alternativo do assunto**, como mostrado na imagem:

Certificate Request:

Data:

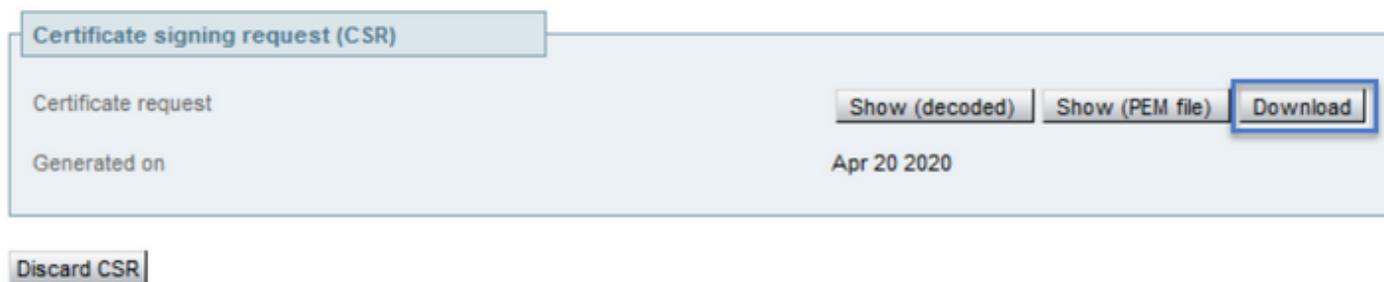
```
Version: 0 (0x0)
Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (4096 bit)
  Modulus:
```

O CN é sempre adicionado como uma SAN automaticamente:

```
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
```

Agora que o CSR foi verificado, você pode fechar a nova janela e selecionar **Download**

(**decodificado**) na seção **Solicitação de assinatura de certificado (CSR)** como mostrado na imagem:

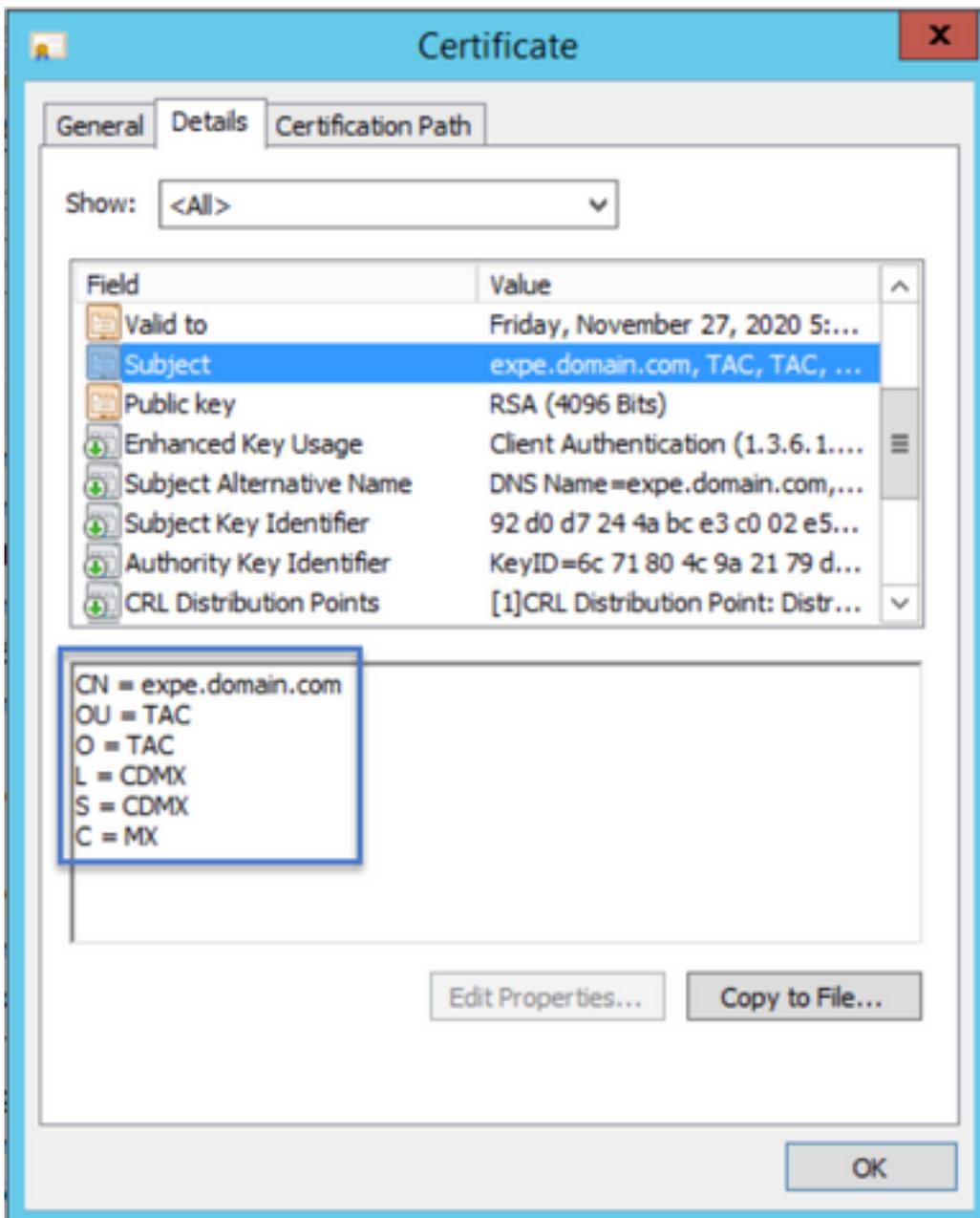


Depois de fazer o download, você pode enviar o novo CSR para sua autoridade de certificação (CA) a ser assinada.

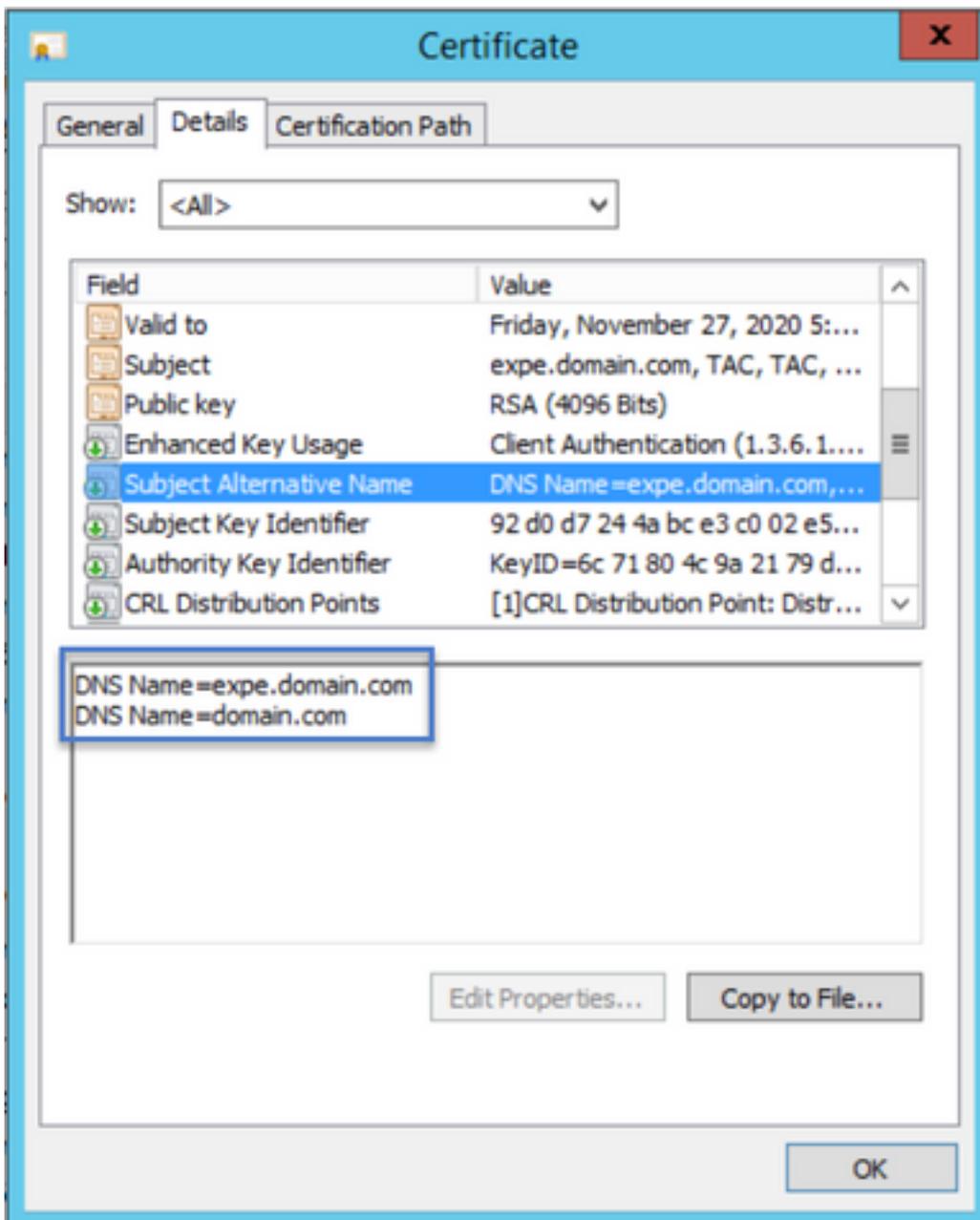
Etapa 4. Verifique as informações contidas no novo certificado.

Quando o novo certificado for devolvido da CA, você poderá verificar se todas as SANs estão presentes no certificado. Para fazer isso, você pode abrir o certificado e procurar os atributos de SANs. Neste documento, um PC Windows é usado para ver os atributos, não é o único método, desde que você possa abrir ou decodificar o certificado para revisar os atributos.

Abra o certificado e navegue até a guia **Detalhes** e procure **Assunto**, ele deve conter o CN e as informações adicionais, como mostrado na imagem:



Procure também a seção **Subject Alternative Name**, ela deve conter as SANs que você inseriu no CSR, como mostrado na imagem:



Se todas as SANs que você inseriu no CSR não estiverem presentes no novo certificado, entre em contato com a CA para ver se há permissão para SANs adicionais para o certificado.

Etapa 5. Carregue os novos certificados CA para a Loja confiável de servidores, se aplicável.

Se a CA for a mesma que assinou o certificado antigo do Expressway, você poderá descartar esta etapa. Se for uma CA diferente, você terá que carregar os novos certificados CA na lista de CAs confiáveis em cada um dos servidores Expressway. Se você tiver zonas de TLS (Transport Layer Security) entre os Expressways, por exemplo, entre um Expressway-C e um Expressway-E, será necessário fazer o upload das novas CAs em ambos os servidores para que eles possam confiar um no outro.

Para fazer isso, você pode carregar seus certificados CA um por um. Navegue até **Manutenção > Segurança > Certificados de CA confiáveis** no Expressway.

1. Selecione **Procurar**.
2. Na nova página, selecione o certificado CA.

3. Selecione **Anexar certificado CA**.

Esse procedimento deve ser feito para cada certificado CA na cadeia de certificados (raiz e intermediários) e deve ser feito em todos os servidores Expressway mesmo que estejam em cluster.

Etapa 6. Carregue o novo certificado no servidor Expressway.

Se todas as informações no novo certificado estiverem corretas, para carregar o novo certificado, navegue para: **Manutenção > Segurança > Certificado de Servidor**.

Localize a seção **Carregar novo certificado** conforme mostrado na imagem:

1. Selecione **Procurar** na seção **Selecionar o arquivo de certificado do servidor**.
2. Selecione o novo certificado.
3. Selecione **Carregar dados do certificado de servidor**.

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

Se o novo certificado for aceito pelo Expressway, o Expressway solicitará uma reinicialização para aplicar as alterações e a mensagem exibirá a nova data de expiração do certificado, como mostrado na imagem:

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

Para reiniciar o Expressway, selecione **reiniciar**.

Verificar

Quando o servidor estiver de volta, o novo certificado deve ter sido instalado, você pode navegar para: **Maintenance > Security > Server Certificate** para confirmar.

Localize os **dados do certificado do servidor** e procure a **expiração do certificado carregado atualmente** na seção, ela exibirá a nova data de expiração do certificado como mostrado na imagem:

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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.