Renovar certificado do Expressway

Contents

Introduction

Este documento descreve o processo de renovação de certificado do Expressway/Video Communication Server (VCS).

As informações neste documento se aplicam ao Expressway e ao VCS. O documento faz referência ao Expressway, mas pode ser trocado com o VCS.

> **Note**: Embora este documento seja projetado para ajudá-lo com o processo de renovação de certificado, é uma boa ideia verificar também o Guia de implantação de criação e uso de certificado do Cisco Expressway para sua versão.

Informações de Apoio

Sempre que um certificado deve ser renovado, há dois pontos principais que devem ser considerados para garantir que o sistema continue a funcionar adequadamente após a instalação do novo certificado:

1. Os atributos do novo certificado devem corresponder aos do certificado antigo (principalmente o nome alternativo do assunto e o uso da chave estendida)

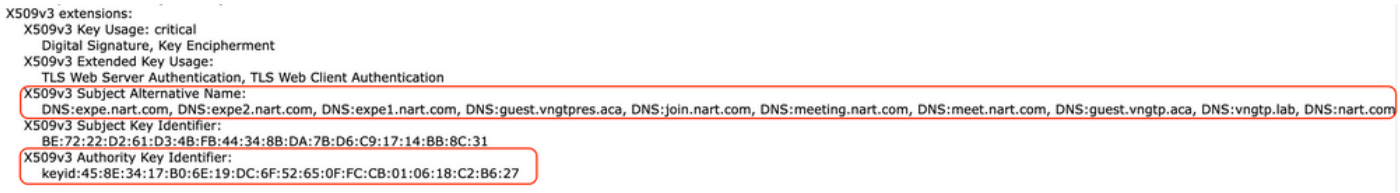
2. A CA (Autoridade de Certificação) a ser usada para assinar o novo certificado deve ser confiável por outros servidores que se comunicam diretamente com o Expressway (por exemplo, CUCM, Expressway-C, Expressway-E..etc)

Processo

A) Obter informações do certificado atual

1. Abra Expressway **Manutenção da** página Web **> Segurança > Certificado do servidor > Mostrar decodificado.**

2. Na nova janela que será aberta, copie as extensões X509v3 "Nome alternativo do assunto" e "Identificador da chave de autoridade" em um documento do bloco de notas.

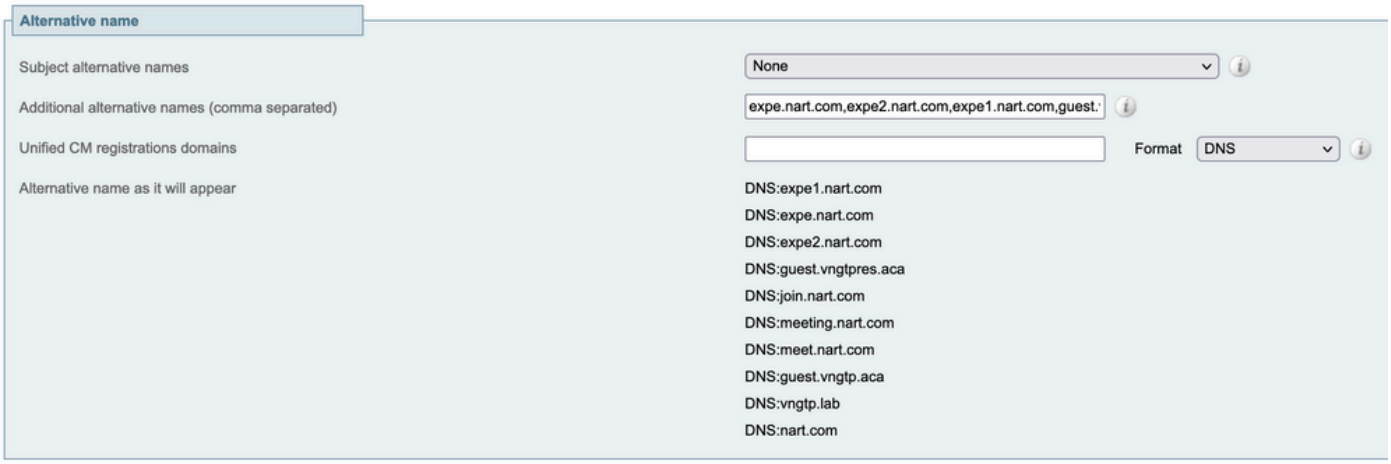


Janela "Mostrar certificado decodificado"

B) Gere o CSR (Certificate Signing Request, Solicitação de assinatura de certificado) e envie-o à CA (Autoridade de certificação) para assinatura.

1. A partir do Expressway **Manutenção de** Página Web **> Segurança > Certificado de Servidor > Gerar CSR.**

2. Na janela Gerar CSR, no campo **Nomes alternativos adicionais (separados por vírgula)**, preencha todos os valores para "Nomes alternativos de assunto" que salvamos na seção A, e certifique-se de remover "DNS:" e separar a lista com vírgulas, consulte a imagem (Ao lado de "Nome alternativo como aparecerá" você pode ver uma lista de todas as SANs a serem usadas no certificado):



Gerar entradas CSR SAN

3. Preencha o restante das informações na seção **Informações adicionais**, como país, empresa, estado etc., e clique em **Gerar CSR.**

4. Depois de gerar o CSR, a página **Manutenção > Segurança > Certificado do Servidor** mostra uma opção para **Descartar CSR** e **Download**, você deve escolher **Download** e enviar o CSR à CA para assinatura.

> **Note**: Certifique-se de não **Descartar CSR** antes de instalar o novo certificado. Se **Descartar CSR** tiver sido feito e, em seguida, for feita uma tentativa de instalar um certificado assinado com o CSR que foi descartado, a instalação do certificado falhará.

C) Verifique a lista SAN e o atributo de uso de chave estendida/aprimorada no novo certificado

Abra o certificado recém-assinado no gerenciador de certificados do Windows e verifique:

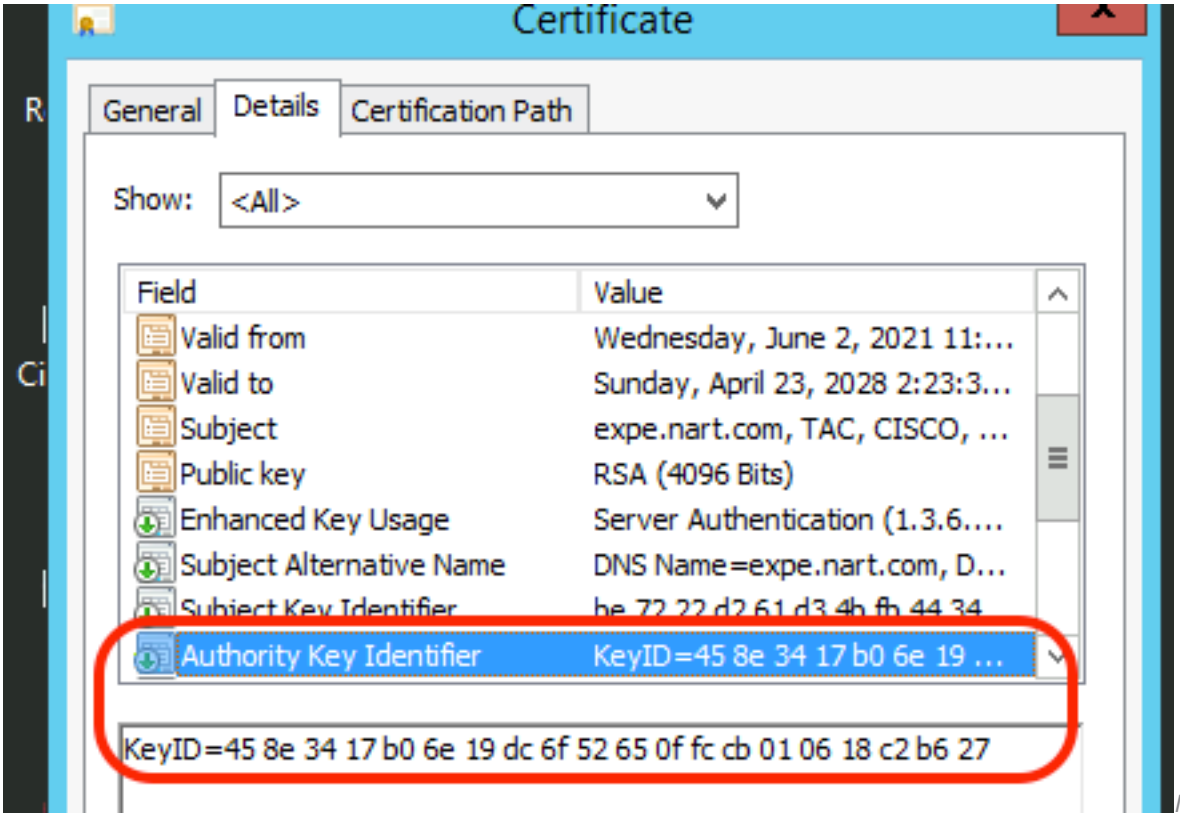
1. A lista SAN corresponde à lista SAN que salvamos na seção A que usamos para gerar o CSR.

2. O atributo "Extended/Enhanced key usage" deve incluir tanto a "Client Authentication" (Autenticação do cliente) como a "Server Authentication" (Autenticação do servidor).

> **Note**: Se o certificado tiver a extensão .pem, renomeie-o como .cer ou .crt para poder abri-lo com o Gerenciador de Certificados do Windows. Quando o certificado estiver aberto com o Gerenciador de Certificados do Windows, você pode ir para a guia **Detalhes > Copiar para Arquivo** e exportá-lo como um arquivo codificado na Base64, um arquivo codificado na Base64 normalmente tem "-----BEGIN CERTIFICATE-----" na parte superior e "-----END CERTIFICATE-----" na parte inferior quando aberto em um editor de texto

D) Verifique se a CA que assinou o novo certificado é a mesma que assinou o certificado antigo

Abra o certificado recém-assinado no gerenciador de certificados do Windows, copie o valor do "Identificador de Chave de Autoridade" e compare-o com o valor do "Identificador de Chave de Autoridade" que salvamos na seção A.



Novo certificado aberto com o Gerenciador de Certificados do Windows

Se os dois valores forem iguais, significa que a mesma CA foi usada para assinar o novo certificado e a que foi usada para assinar o certificado antigo, e você poderá prosseguir para a seção E para carregar o novo certificado.

Se os valores forem diferentes, isso significa que a CA usada para assinar o novo certificado é diferente da CA usada para assinar o certificado antigo, e as etapas que você deve seguir antes de continuar com a seção E são:

1. Obtenha todos os certificados de CA intermediários (se houver) e o certificado de CA raiz.

2. Vá para **Maintenance > Security > Trusted CA certificate** , clique em **Browse** e procure o

certificado intermediário da autoridade de certificação no seu computador e carregue-o. Faça o mesmo para qualquer outro certificado intermediário de CA e o certificado raiz de CA.

3. Faça o mesmo em qualquer Expressway-E (se o certificado a ser renovado for um certificado Expressway-C) que se conecte a este servidor ou em qualquer Expressway-C (se o certificado a ser renovado for um certificado Expressway-E) que se conecte a este servidor.

4. Se o certificado a ser renovado for um certificado Expressway-C e você tiver MRA ou tiver zonas seguras para CUCM, você deverá se certificar de que o CUCM confia na nova raiz e CA intermediária e carregar os certificados de CA raiz e intermediária para os armazenamentos CUCM tomcat-trust e callmanager-trust e reiniciar os serviços relevantes no CUCM.

E) Instalar o novo certificado

Depois que todos os pontos anteriores tiverem sido verificados, você pode agora instalar o novo certificado no Expressway em **Manutenção > Segurança > Certificado do servidor**, clicar em **Procurar** e selecionar o novo arquivo de certificado do seu computador e carregá-lo.

Você deve reiniciar o Expressway após instalar um novo certificado.

> **Note**: Certifique-se de que o certificado que você carregar no Expressway de **Manutenção > Segurança > Certificado do Servidor** contenha apenas o certificado do servidor Expressway e NÃO toda a cadeia de certificados e certifique-se de que seja um certificado Base64

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.