Solução do pacote CCE: Procedimento para obter e transferir arquivos pela rede certificados de CA da terceira

Índice

Introdução

A fim usar o HTTPS para uma comunicação segura entre a fineza e o Cisco unificou server Center da inteligência (CUIC), Certificados que da Segurança a instalação é precisada. À revelia estes server fornecem os certifcates auto-assinados que são usados ou os clientes podem obter e instalar Certificados do Certificate Authority (CA). Estes certs de CA podem ser obtidos de um fornecedor de terceira parte como Verisign, Thawte, GeoTrust ou podem ser produzidos internaly.

Este documento aponta explicar em detalhe as etapas envolvidas para obter e instalar um certificado do Certification Authority (CA), gerado de um fornecedor de terceira parte para estabelecer uma conexão de HTTPS entre a fineza e server unificados Cisco do centro da inteligência (CUIC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco empacota a empresa do centro de contato (PCCE)
- Cisco unificou o centro da inteligência (CUIC)

- Fineza de Cisco
- Certificados de CA

Componentes Utilizados

A informação usada no documento é baseada na versão da solução PCCE 11.0(1).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, certifique-se de que você compreende o impacto potencial de toda a etapa.

Procedimento

Estabelecendo Certificados para uma comunicação HTTPS na fineza e o centro unificado Cisco da inteligência (CUIC) os server exigem as seguintes etapas

- Gerencia e transfira a solicitação de assinatura de certificado (CSR).
- Obtenha a raiz, o intermediário (se aplicável) e o certificado do aplicativo do Certificate Authority usando o CSR.
- Transfira arquivos pela rede Certificados aos server.

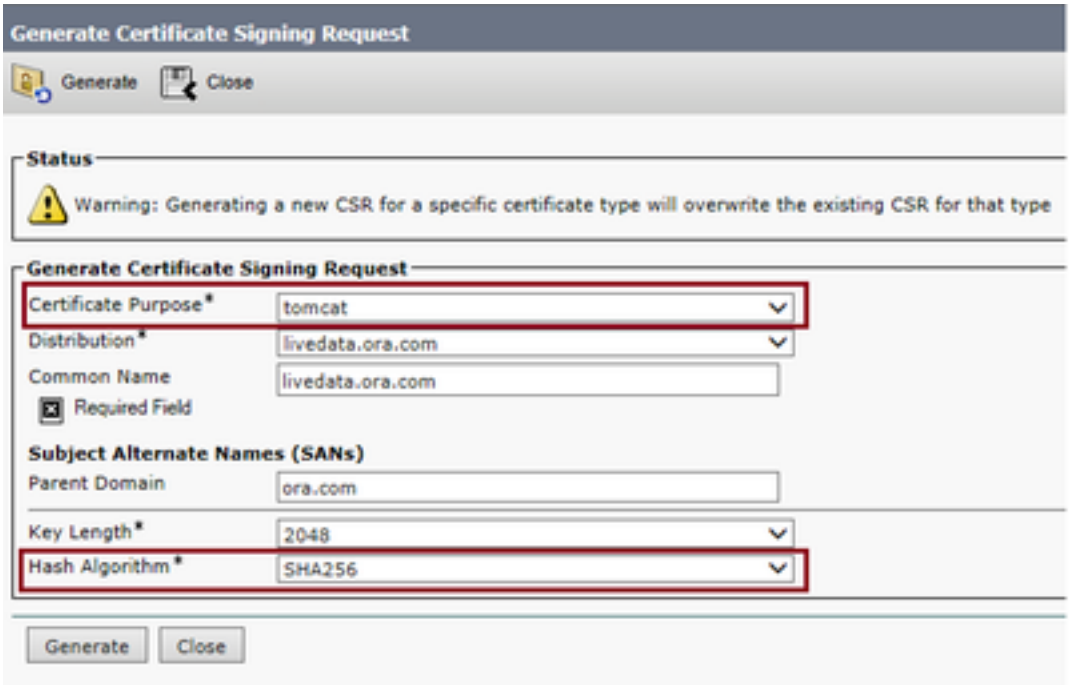
Passo 1: Gerencia e transfira a solicitação de assinatura de certificado (o CSR)

---

1. As etapas descritas abaixo gerando e transferindo o CSR são mesmas para a fineza e os server CUIC.

2. Abra a página de administração do sistema operacional das comunicações unificadas de Cisco usando a URL indicada abaixo e assine-a dentro com a conta admin do OS criada durante o processo de instalação
https://hostname do servidor primário/cmplatform

3. Gerencia a solicitação de assinatura de certificado (o CSR)

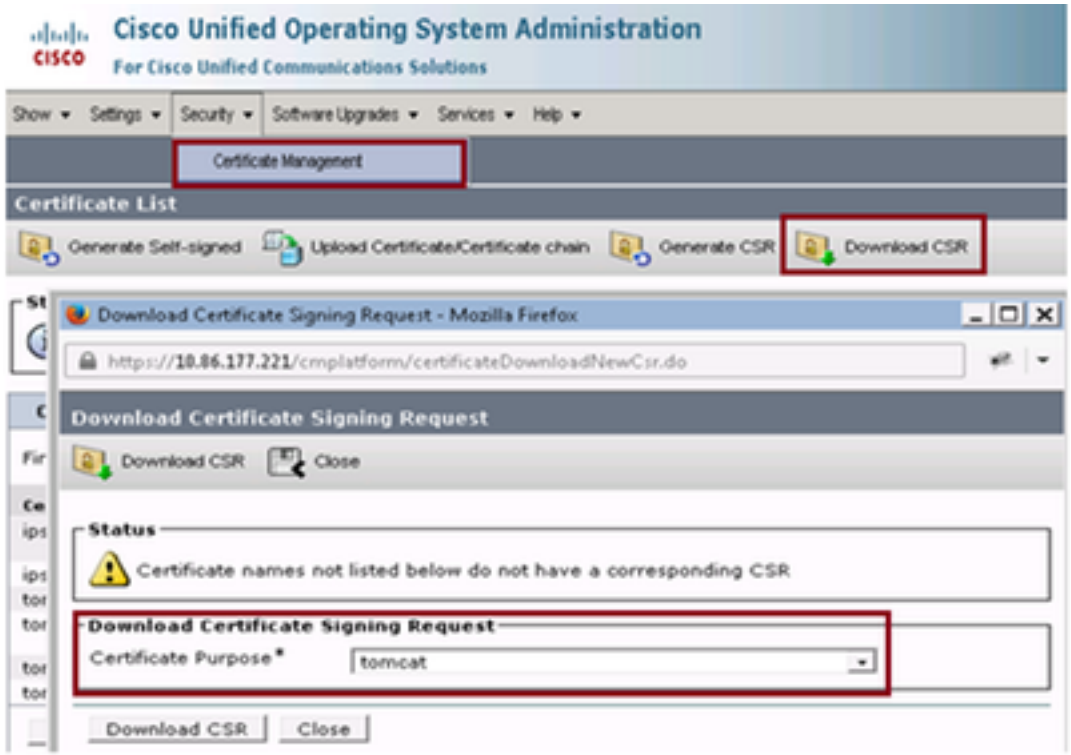


a) O > gerenciamento de certificado seleto da Segurança > gerencie o CSR.

b) Da lista de drop-down do nome da finalidade do certificado, selecione TomCat.

c) Selecione o algoritmo de hash como SHA256
d) O clique gerencie o CSR.

4. Solicitação de assinatura de certificado da transferência (CSR)



a) > gerenciamento de certificado da Segurança > transferência seletos CSR.
b) Da lista de drop-down do nome do certificado, selecione TomCat.
c) Clique a transferência CSR.

Note:

Execute as etapas acima mencionadas no server secondory usando a URL "https://hostname do server/cmplatform secondory" para obter CSR para o Certificate Authority.

Passo 2: Obtenha o certificado da raiz, do intermediário (se aplicável) e do aplicativo do Certificate Authority

---

1. Forneça a informação preliminar e secondory da solicitação de assinatura de certificado dos server (CSR) à autoridade de Certifcate da terceira parte (CA) como Verisign, Thawte, GeoTrust etc.

2. Da autoridade de Certifcate (CA) um deve receber o seguinte certificate chain para os server preliminares e secondory.

- **Server da fineza: Certificado da raiz, do intermediário e do aplicativo**
- **Server CUIC: Certificado da raiz e do aplicativo**

Passo 3: Certificados da transferência de arquivo pela rede aos server

---

Esta seção descreve em como transferir arquivos pela rede corretamente o certificate chain na fineza e em server unificados Cisco do centro da inteligência (CUIC).

Server da fineza:

==========
1. **Certificado preliminar da raiz de servidor da fineza da transferência de arquivo pela rede**

a) Na página de administração do sistema operacional das comunicações unificadas de Cisco do servidor primário, seleta

> gerenciamento de certificado da Segurança > certificado da transferência de arquivo pela rede.

b) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
d) Arquivo da transferência de arquivo pela rede do clique.

2. **Certificado preliminar do intermediário do server da fineza da transferência de arquivo pela rede.**

a) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
b) No certificado de raiz arquivado, dê entrada com o nome do certificado de raiz que você transferiu arquivos pela rede na etapa precedente.

Este é um arquivo do .pem que seja gerado quando a raiz/certificado público foi instalada. Para ver este arquivo navegue ao gerenciamento certificado > ao ClickFind. No nome de arquivo do .pem da lista do certificado esteja listado contra a Tomcat-confiança.

c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado intermediário.
d) Arquivo da transferência de arquivo pela rede do clique.

Note:
Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede a raiz de servidor da fineza ou o certificado preliminar do intermediário ao server secundário da fineza.

3. Certificado preliminar do aplicativo de servidor da fineza da transferência de arquivo pela rede.

a) Da lista de drop-down do nome do certificado, selecione TomCat.

b) No campo do certificado de raiz, dê entrada com o nome do certificado intermediário que você transferiu arquivos pela rede na etapa precedente. Inclua a extensão do .pem (por exemplo, TEST-SSL-CA.pem).

c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado do aplicativo.
d) Arquivo da transferência de arquivo pela rede do clique.

4. Raiz de servidor da fineza da transferência de arquivo pela rede e certificado secondory do intermediário.

a) Siga as mesmas etapas como mencionado acima em (1) e em (2) no server secondory para seus Certificados

Note:
Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede a raiz de servidor da fineza ou o certificado secondory do intermediário ao server preliminar da fineza.

5. Certificado secondory do aplicativo de servidor da fineza da transferência de arquivo pela rede.

a) Siga as mesmas etapas como mencionado acima dentro (3) no server secondory para seus próprios Certificados.

6. Reinicie server

Alcance o CLI nos server preliminares e secondory da fineza e incorpore o comando dos “reinício do sistema utils” reiniciar os server.

Server CUIC:

==========

1. Certificado cuic da raiz do servidor primário da transferência de arquivo pela rede (público)

a) Na página de administração do sistema operacional das comunicações unificadas de Cisco do servidor primário, seleta

> gerenciamento de certificado da Segurança > certificado da transferência de arquivo pela rede.

b) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
d) Arquivo da transferência de arquivo pela rede do clique.

Note:
Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede o certificado preliminar da raiz de servidor CUIC aos server secundários CUIC.

2. Certificado (preliminar) cuic do aplicativo de servidor primário da transferência de arquivo pela rede
a) Da lista de drop-down do nome do certificado, selecione TomCat.
b) No campo do certificado de raiz, dê entrada com o nome do certificado de raiz que você transferiu arquivos pela rede na etapa precedente.

Este é um arquivo do .pem que seja gerado quando a raiz/certificado público foi instalada. Para ver este arquivo navegue ao gerenciamento certificado > ao ClickFind. No nome de arquivo do .pem da lista do certificado esteja listado contra a Tomcat-confiança. Inclua essa extensão do .pem (por exemplo, TEST-SSL-CA.pem).

c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado (preliminar) do aplicativo.
d) Arquivo da transferência de arquivo pela rede do clique

3. Certificado secondory cuic da raiz de servidor da transferência de arquivo pela rede (público)

a) No server cuic secondory siga as mesmas etapas como mencionado em etapa (1) para seu certificado de raiz.

Note:
Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede o certificado secondory da raiz de servidor de CUIc ao server preliminar CUIC.

certificado (preliminar) secondory cuic do aplicativo de servidor 4.Upload.
a) Siga o mesmo processo como exposto em etapa (2) no server secondory para seu próprio certificado.

6. Reinicie server

Alcance o CLI nos server preliminares e secondory CUIC e incorpore o comando dos “reinício do sistema utils” reiniciar os server.

Note:

Para evitar a exceção do certificado que adverte o deve alcançar os server usando o nome do nome de domínio totalmente qualificado (FQDN).

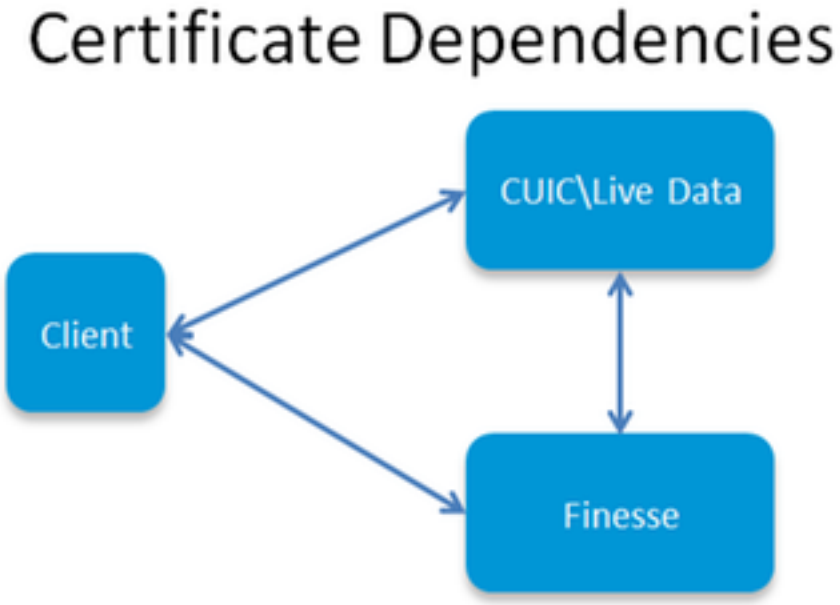
Dependências do certificado:

==========

Como

Os agentes e os supervisores da fineza utilizam dispositivos CUIC relatando as finalidades uma têm que transferir arquivos pela rede certificados de raiz destes server também no seguinte ordem manter dependências do certificado para uma comunicação HTTPS entre estes server.

- Transfira arquivos pela rede o certificado de raiz dos server CUIC no saque preliminar da fineza
- Transfira arquivos pela rede a raiz da fineza \ certificado intermediário no servidor primário CUIC



a) **Transfira arquivos pela rede o certificado de raiz dos server CUIC no servidor primário da fineza**

---

a página de administração aberta do sistema operacional das comunicações unificadas de Cisco do server preliminar da fineza 1.On usando a URL indicada abaixo e assina dentro com a conta admin do OS criada durante os provcess da instalação

https://hostname do server/cmplatform preliminares da fineza

certificado de raiz preliminar 2.Upload CUIC.
a) Selecione o > gerenciamento de certificado da Segurança > o certificado da transferência de arquivo pela rede.
b) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
d) Arquivo da transferência de arquivo pela rede do clique.

certificado de raiz 3.Upload Secondory CUIC.

a) Selecione o > gerenciamento de certificado da Segurança > o certificado da transferência de arquivo pela rede.
b) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao

arquivo de certificado de raiz.
d) Arquivo da transferência de arquivo pela rede do clique.

Note:
Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede os certificados de raiz CUIC ao server secundário da fineza.

4. Alcance o CLI nos server preliminares e secondory da fineza e incorpore o comando dos "reinício do sistema utils" reiniciar os server.

b) Transfira arquivos pela rede a raiz da fineza \ certificado intermediário no servidor primário CUIC

---

a página de administração aberta do sistema operacional das comunicações unificadas de Cisco CUIC do server preliminar 1.On usando a URL indicada abaixo e assina dentro com a conta admin do OS criada durante os provcess da instalação
https://hostname do server preliminar/cmplatform CUIC

certificado de raiz preliminar da fineza 2.Upload.
a) Selecione o > gerenciamento de certificado da Segurança > o certificado da transferência de arquivo pela rede.
b) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
c) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
d) Arquivo da transferência de arquivo pela rede do clique.

3. Certificado preliminar do intermediário da fineza da transferência de arquivo pela rede

i) Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
ii) No certificado de raiz arquivado, dê entrada com o nome do certificado de raiz que você transferiu arquivos pela rede na etapa precedente.
iii) No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado intermediário.
iv) Arquivo da transferência de arquivo pela rede do clique.

4. Execute as mesmas etapas (2 & 3) para a raiz secondory da fineza \ Certificados intermediários no servidor de dados vivo preliminar.

Note:

Enquanto a loja da Tomcat-confiança replicated entre os server preliminares e secondory não está precisada de transferir arquivos pela rede o certificado de /intermediate da raiz da fineza aos server secundários CUIC.

5. Alcance o CLI nos server preliminares e secondory CUIC e incorpore o comando dos "reinício do sistema utils" reiniciar os server.