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

Índice

Introdução

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

A fim usar o HTTPS para uma comunicação segura entre a fineza e os server CUIC, a instalação dos Certificados da Segurança é precisada. À revelia, estes server fornecem os certificados auto-assinados que são usados ou os clientes podem obter e instalar certificados de CA. Estes certificados de CA podem ser obtidos de um fornecedor de terceira parte como Verisign, Thawte, GeoTrust ou podem ser produzidos internamente.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco empacota a empresa do centro de contato (PCCE)
- CUIC
- Fineza de Cisco
- Certificados de CA

Componentes Utilizados

A informação usada no original é baseada na versão da solução 11.0 PCCE (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

A fim estabelecer Certificados para uma comunicação HTTPS na fineza e nos server CUIC, siga estas etapas:

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

Gerencia e transfira o CSR

1. As etapas descritas aqui são a fim gerar e transferir o CSR. Estas etapas são as mesmas para a fineza e os server CUIC.

2. Abra a **página de administração do sistema operacional das comunicações unificadas de Cisco** com a URL e assine-a dentro com a conta admin do operating system (OS) criada na altura do processo de instalação. **https://hostname do servidor primário/cmplatform**

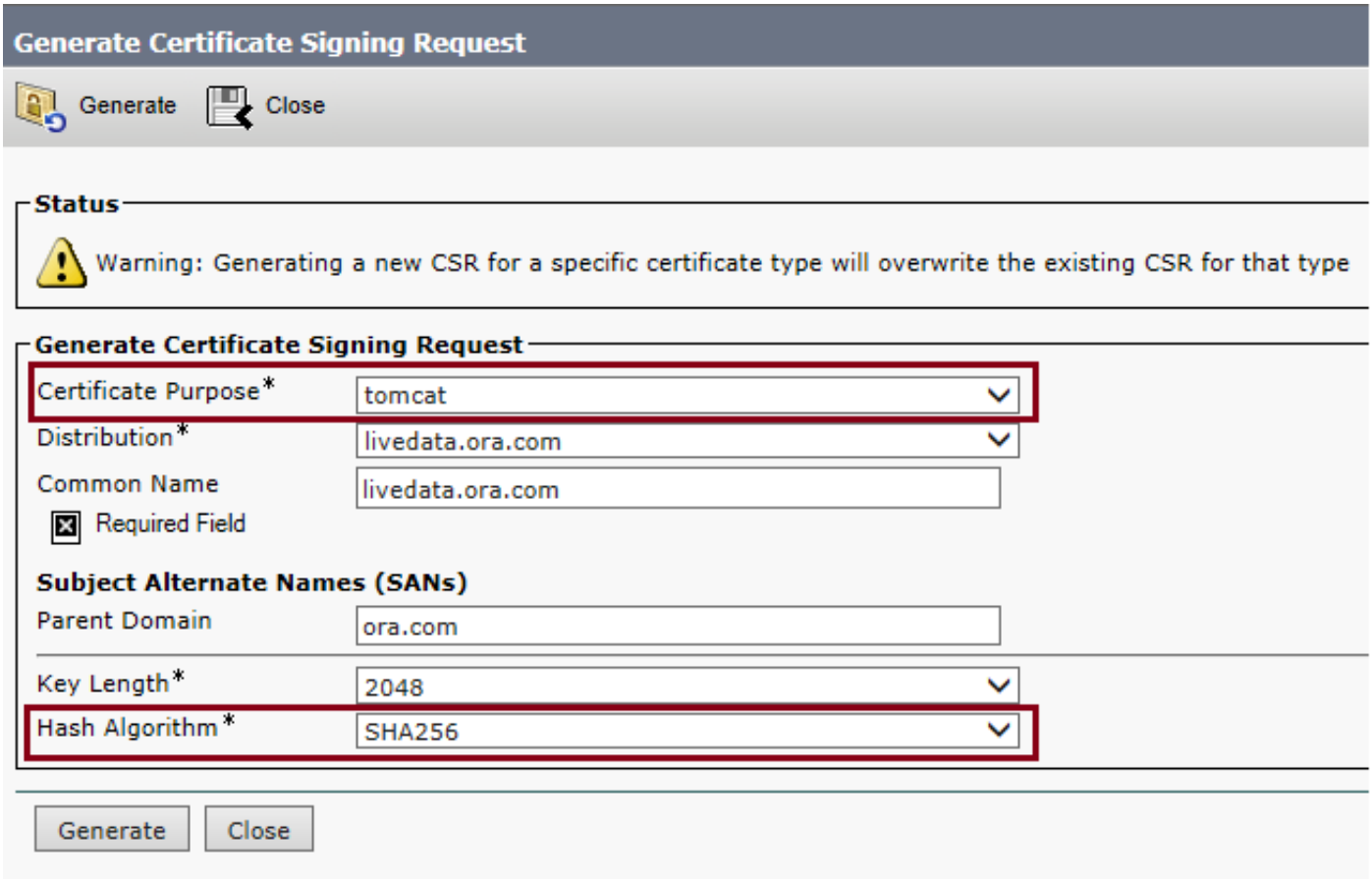
3. Gerencia a solicitação de assinatura de certificado.

a. Navegue ao **> gerenciamento de certificado da Segurança > gerenciem o CSR**.

b. Da lista de drop-down de Purpose* do certificado, selecione **TomCat**.

c. Selecione o algoritmo de hash como **SHA256**.

d. O clique **gerencie** segundo as indicações da imagem.

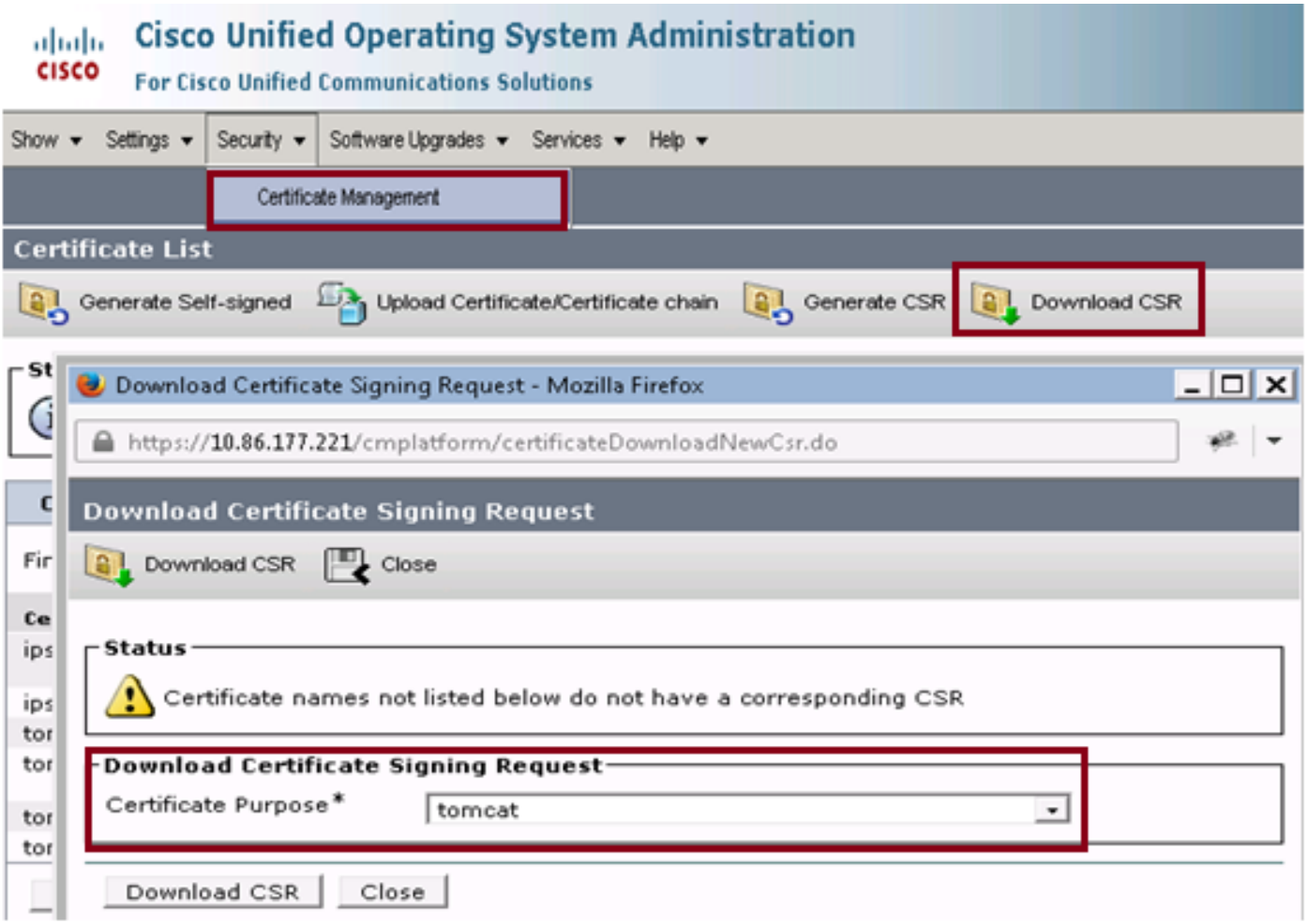


4. Transferência CSR.

a. Navegue ao **> gerenciamento de certificado da Segurança > à transferência CSR**.

b. Da lista de drop-down de Purpose* do certificado, selecione **TomCat**.

c. Clique a **transferência CSR** segundo as indicações da imagem.



Note: Execute estas etapas no servidor secundário com a URL **https://hostname do servidor secundário/cmplatform** a fim obter CSR para CA.

Obtenha a raiz, o intermediário (se aplicável) e o certificado do aplicativo de CA

1. Forneça a informação preliminar e do servidor secundário CSR à terceira parte CA como Verisign, Thawte, GeoTrust etc.

2. De CA, você deve receber este o certificate chain para o preliminar e os servidores secundários:

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

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 nos server 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, navegue ao **> gerenciamento de certificado da Segurança > ao certificado da transferência de arquivo pela rede**.

b. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo de certificado de raiz**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

2. Do server preliminar da fineza da transferência de arquivo pela rede certificado intermediário:

a. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

b. No certificado de raiz arquivado, dê entrada com o nome do certificado de raiz que é transferido arquivos pela rede na etapa precedente. Este é um arquivo do **.pem** que seja gerado quando a raiz/certificado público foi instalada.

A fim ver este arquivo, navegue ao **gerenciamento certificado > ao achado**. Na lista do certificado, o nome de arquivo do **.pem** está listado contra a Tomcat-confiança.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo certificado intermediário**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

> **Note**: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e os servidores secundários, 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 da finalidade do certificado, selecione **TomCat**.

b. No campo do certificado de raiz, dê entrada com o nome do certificado intermediário que é transferido 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 o **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 secundários do intermediário:

a. Siga as mesmas etapas como mencionado em etapas 1 e 2 no servidor secundário para seus Certificados.

> **Note**: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e os servidores secundários, não está precisada de transferir arquivos pela rede a raiz de servidor da fineza

ou o certificado secundário do intermediário ao server preliminar da fineza.

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

a. Siga as mesmas etapas como mencionado em etapa 3. no servidor secundário para seus próprios Certificados.

6. Server do reinício:

a. Alcance o CLI nos server preliminares e secundários da fineza e execute o **reinício do sistema dos utils do** comando a fim reiniciar os server.

Server CUIC

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

a. **Na página de administração do sistema operacional das comunicações unificadas de Cisco do** servidor primário, navegue ao **> gerenciamento de certificado da Segurança > ao certificado da transferência de arquivo pela rede**.

b. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo de certificado de raiz**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

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

2. Certificado (preliminar) do aplicativo de servidor primário da transferência de arquivo pela rede CUIC:

a. Da lista de drop-down da finalidade do certificado, selecione **TomCat**.

b. No campo do certificado de raiz, dê entrada com o nome do certificado de raiz que é transferido arquivos pela rede na etapa precedente.

Este é um arquivo do **.pem** que seja gerado quando a raiz/certificado público foi instalada. A fim ver este arquivo, navegue ao **gerenciamento certificado > ao achado**.

No .pem da lista do certificado o nome de arquivo está 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 o **arquivo certificado (preliminar) do aplicativo**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

3. Certificado da raiz do servidor secundário da transferência de arquivo pela rede CUIC (público):

a. No server secundário CUIC, siga as mesmas etapas como mencionado em etapa 1. para seu certificado de raiz.

> **Note**: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e os servidores secundários, não está precisada de transferir arquivos pela rede o certificado secundário da raiz de servidor CUIC ao server preliminar CUIC.

4. Certificado (preliminar) do aplicativo de servidor secundário da transferência de arquivo pela rede CUIC:

a. Siga o mesmo processo como exposto em etapa 2. no servidor secundário para seu próprio certificado.

5. Server do reinício:

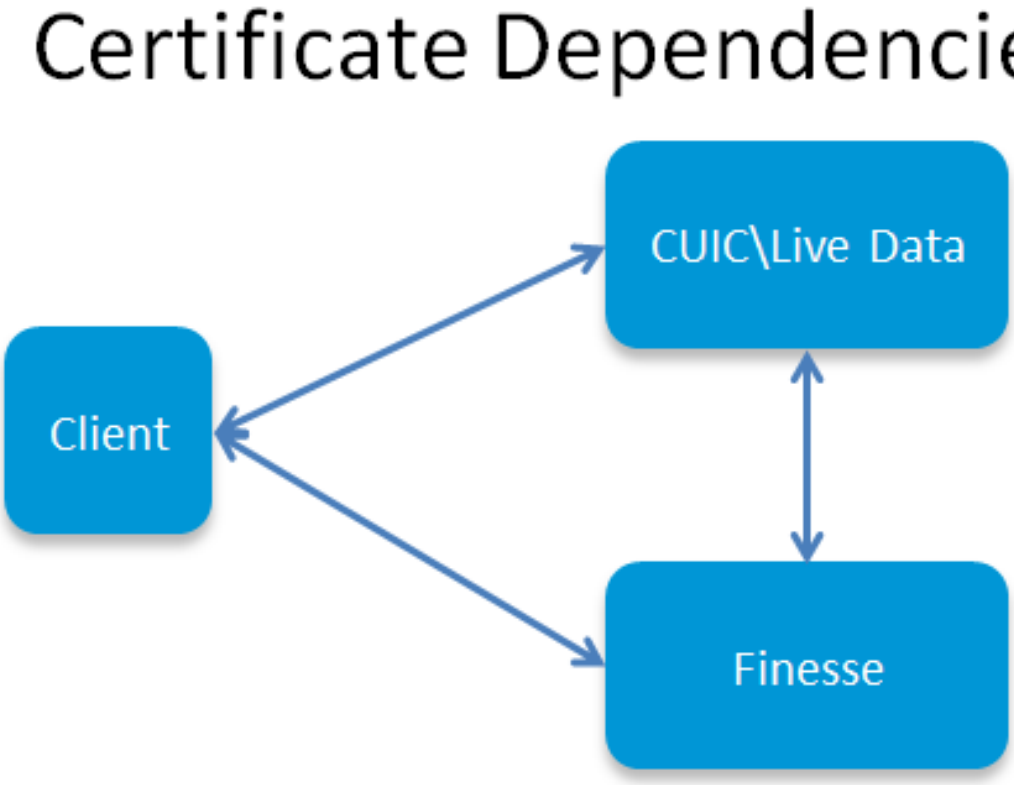
a. Alcance o CLI nos server preliminares e secundários CUIC e execute o **reinício do sistema dos utils do** comando a fim reiniciar os server.

> **Note**: A fim evitar o aviso da exceção do certificado, você deve alcançar os server com o uso do nome de domínio totalmente qualificado (FQDN).

Dependências do certificado

Porque os agentes e os supervisores da fineza utilizam dispositivos CUIC relatando finalidades, você tem que transferir arquivos pela rede certificados de raiz destes server também, na ordem mencionada aqui para manter dependências do certificado para uma comunicação HTTPS entre estes server e segundo as indicações da imagem.

- Certificado de raiz dos server da transferência de arquivo pela rede CUIC no servidor primário da fineza
- Transfira arquivos pela rede a raiz da fineza \ certificado intermediário no servidor primário CUIC



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

1. No server preliminar da fineza, a **página de administração** aberta do **sistema operacional das comunicações unificadas de Cisco** com a URL e assina dentro com a conta admin do OS criada na altura do processo de instalação:

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

2. Certificado de raiz preliminar da transferência de arquivo pela rede CUIC.

a. Navegue ao **> gerenciamento de certificado da Segurança > ao certificado da transferência de arquivo pela rede**.

b. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo de certificado de raiz**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

3. Certificado de raiz secundário da transferência de arquivo pela rede CUIC.

a. Navegue ao **> gerenciamento de certificado da Segurança > ao certificado da transferência de arquivo pela rede**.

b. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo de certificado de raiz**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

> **Note**: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e os servidores secundários, 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 secundários da fineza e execute o **reinício do sistema dos utils do** comando a fim reiniciar os server.

Transfira arquivos pela rede a raiz da fineza/certificado intermediário no servidor primário CUIC

1. No server preliminar CUIC, a **página de administração** aberta do **sistema operacional das comunicações unificadas de Cisco** com a URL e assina dentro com a conta admin do OS criada na altura do processo de instalação:

https://hostname do server preliminar/cmplatform CUIC

2. Certificado de raiz preliminar da fineza da transferência de arquivo pela rede:

a. Navegue ao **> gerenciamento de certificado da Segurança > ao certificado da transferência de arquivo pela rede**.

b. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo de certificado de raiz**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

certificado intermediário da fineza 3.Upload preliminar:

a. Da lista de drop-down da finalidade do certificado, selecione a Tomcat-**confiança**.

b. No certificado de raiz arquivado, dê entrada com o nome do certificado de raiz que é transferido arquivos pela rede na etapa precedente.

c. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta o **arquivo certificado intermediário**.

d. **Arquivo da transferência de arquivo pela rede do** clique.

4. Execute mesma etapa 2 e etapa 3. para a raiz secundária da fineza \ Certificados intermediários no servidor de dados vivo preliminar.

> **Note**: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e os servidores secundários, 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 secundários CUIC e execute o **reinício do sistema dos utils do** comando a fim reiniciar os server.