Solução unificada CCE: Procedimento para obter e transferir arquivos pela rede certificados de CA da terceira (versão 11.x)

Índice

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise (UCCE)
- Dados do cisco live (LD)
- Cisco unificou o centro da inteligência (CUIC)
- Fineza de Cisco
- Habilitado de CA

Componentes Utilizados

A informação usada no documento é baseada na versão da solução UCCE 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.

Informações de Apoio

A fim usar o HTTPS para uma comunicação segura entre a fineza, CUIC e os servidores de dados vivos, instalação dos Certificados da Segurança são precisados. À revelia estes server fornecem os certifcates auto-assinados que são usados ou os clientes podem obter e instalar certificados assinados 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.

Configurar

Estabelecendo o certificado para uma comunicação HTTPS na fineza, CUIC e os servidores de dados vivos exigem estas etapas:

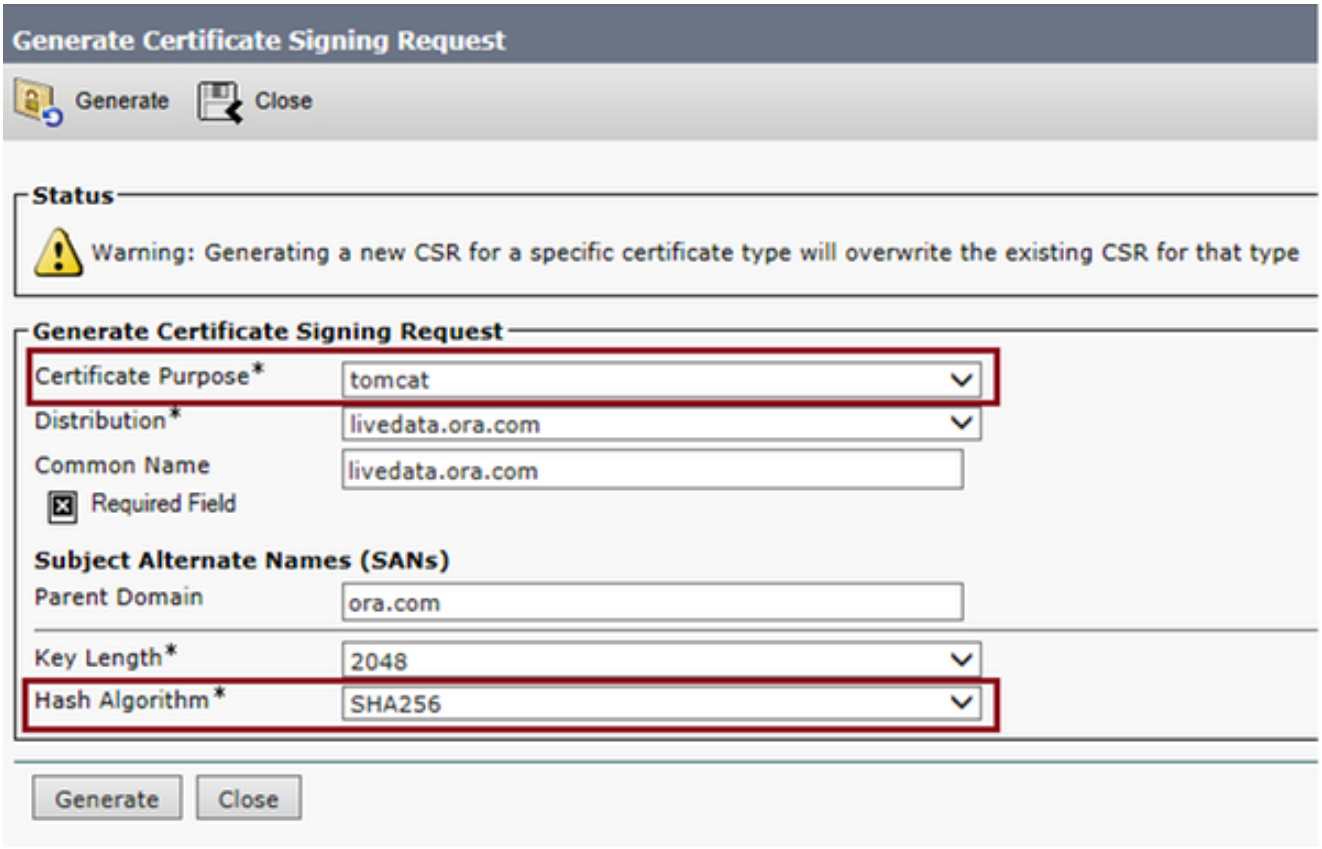
1. Gerencia e transfira a solicitação de assinatura de certificado (CSR).
2. Obtenha a raiz, o intermediário (se aplicável) e o certificado do aplicativo do Certificate Authority usando o CSR.
3. Transfira arquivos pela rede Certificados aos server.

Etapa 1. Gerencia e transfira a solicitação de assinatura de certificado (CSR).

1. As etapas descritas aqui gerando e transferindo o CSR são mesmas para a fineza, CUIC e os dados vivos separam.

2. Abra a **página de administração do sistema operacional das comunicações unificadas de Cisco** usando a URL indicada e assine-a dentro com a conta admin do OS criada durante o processo de instalação
https://FQDN:8443/cmplatform

3. Gerencia a solicitação de assinatura de certificado (CSR) segundo as indicações da imagem:

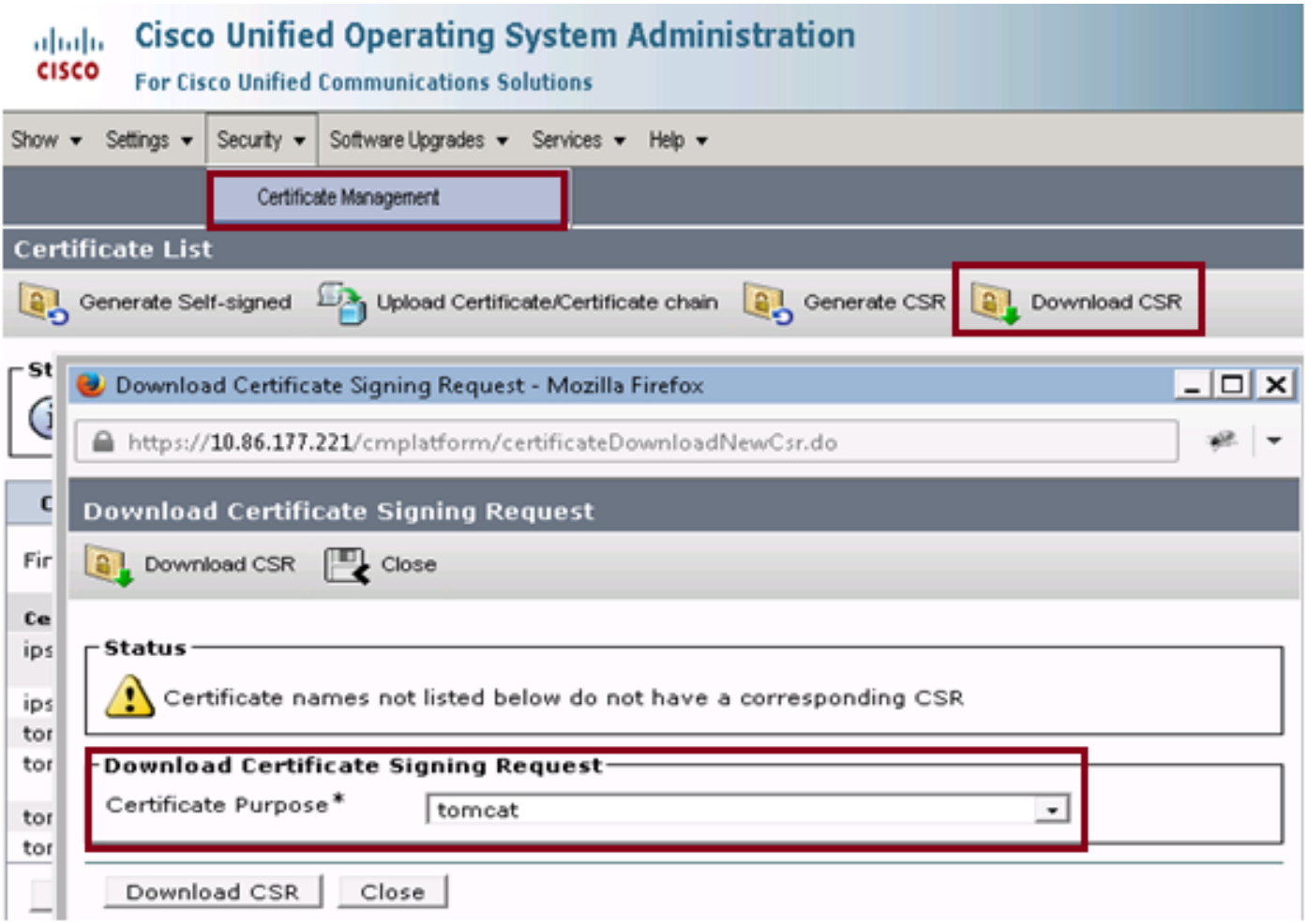


Etapa 1. Navegue ao **> gerenciamento de certificado da Segurança > gerenciem o CSR**.Etapa 2. Da lista de drop-down do nome da finalidade do certificado, selecione TomCat.Etapa 3. Selecione o algoritmo de hash e o comprimento chave que depeding em cima das necessidades de negócio.

- Comprimento chave: 2048 \ algoritmo de hash: SHA256 é recomendado

Etapa 4. O clique **gerencie o CSR**.Nota: Se o negócio exige o pai sujeito dos nomes alternativos (sem) o campo do domínio que a ser enchido com o Domain Name satisfaz então esteja ciente dos endereços da edição no documento [“sem a edição com um certificado assinado da terceira parte na fineza”.]

4. Transfira a solicitação de assinatura de certificado (CSR) segundo as indicações da imagem:



Etapa 1. Navegue ao **> gerenciamento de certificado da Segurança > à transferência CSR**.
Etapa 2. Da lista de drop-down do nome do certificado, selecione TomCat.
Etapa 3. **Transferência CSR do** clique.

Nota:

> Nota: Execute as etapas acima mencionadas no servidor secundário usando a URL **https://FQDN:8443/cmplatform** para obter CSR para o Certificate Authority

Etapa 2. Obtenha a raiz, intermediário (se applicableStep 5. e certificado do aplicativo do Certificate Authority.

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

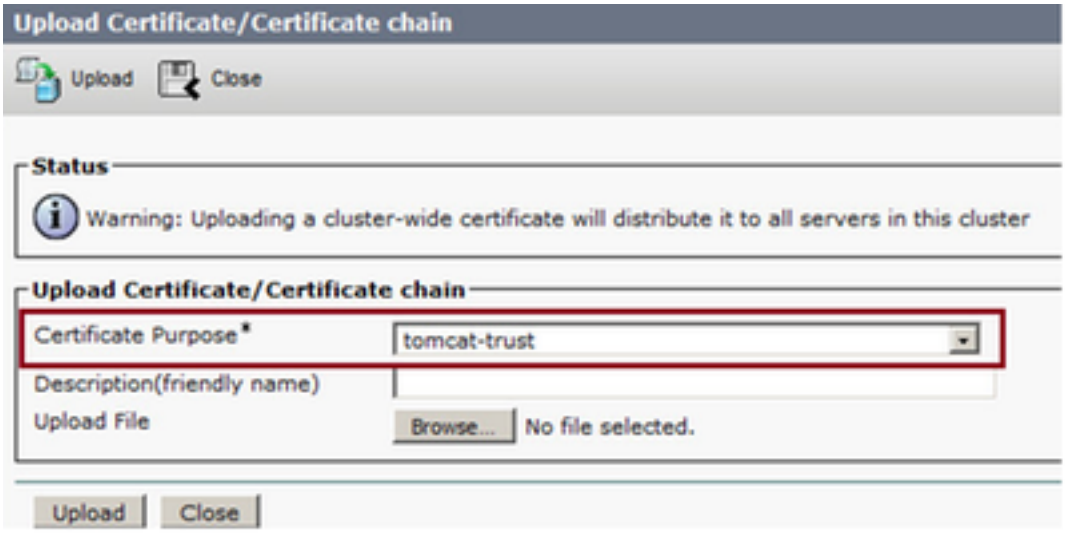
2. Da autoridade do certifcate uma deve receber o seguinte certificate chain para os server preliminares e secondory.

- **Server da fineza:** Certificado enraíze, do intermediário (opcional) e do aplicativo
- **Server CUIC:** Certificado enraíze, do intermediário (opcional) e do aplicativo
- **Saques vivos dos dados:** Certificado enraíze, do intermediário (opcional) e do aplicativo

Etapa 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, CUIC e viver servidores de dados.

Server da fineza

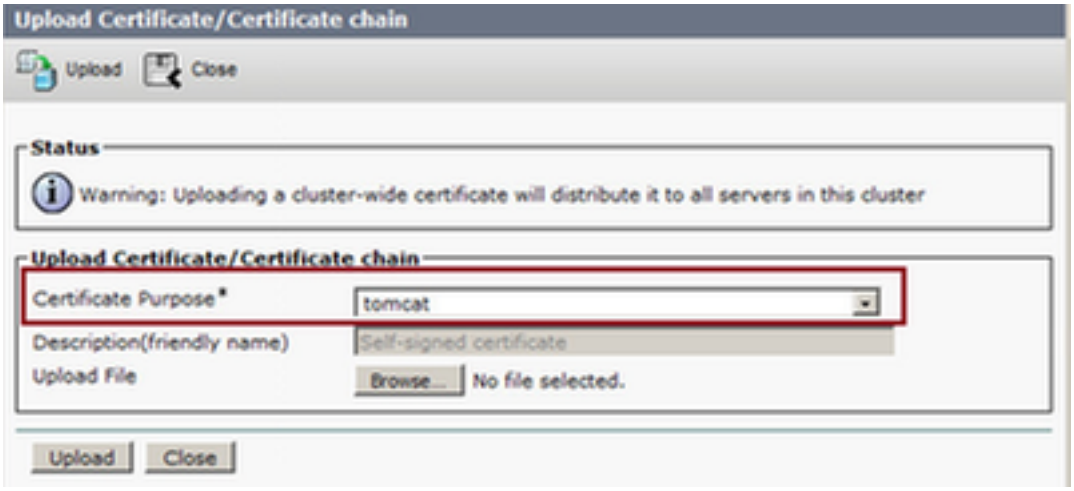


1. Transfira arquivos pela rede o certificado de raiz no server preliminar da fineza com a ajuda destas etapas:

   Etapa 1. 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.**
   Etapa 2. Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
   Etapa 3. No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
   Etapa 4. Arquivo da transferência de arquivo pela rede do clique.

2. Transfira arquivos pela rede o certificado intermediário no server preliminar de Fineese com a ajuda destas etapas:

   Etapa 1. As etapas em transferir arquivos pela rede o certififcate intermediário são mesmas que o certificado de raiz segundo as indicações de etapa 1.
   Etapa 2. 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.**
   Etapa 3. Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
   Etapa 4. No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado intermediário.
   Etapa 5. **Transferência de arquivo pela rede do** clique.Nota: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e servidores secundários não está precisada de transferir arquivos pela rede a raiz ou o certificado do intermediário ao server secundário da fineza.
3. Transfira arquivos pela rede o certificado preliminar do aplicativo de servidor da fineza segundo as indicações da imagem:



Etapa 1. Da lista de drop-down do nome do certificado, selecione TomCat.Etapa 2. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta ao arquivo certificado do aplicativo.
Etapa 3. **Transferência de arquivo pela rede do** clique para transferir arquivos pela rede o arquivo.

4. Transfira arquivos pela rede o certificado secundário do aplicativo de servidor de Fineese.
   Nesta etapa siga o mesmo processo como mencionado em etapa 3 no servidor secundário para seu próprio certificado do aplicativo.

5. Agora você pode reiniciar os server.
   Alcance o CLI nos server preliminares e secundários da fineza e entre no **reinício do sistema dos utils do** comando para reiniciar os server.

Server CUIC (que não supõem nenhum Certificados intermediário atual no certificate chain)

1. Transfira arquivos pela rede o certificado de raiz no server preliminar CUIC.

   Etapa 1. Na página de administração do sistema operacional das comunicações unificadas de Cisco do servidor primário, navegue ao **> gerenciamento de certificado da Segurança > ao certificado/certificate chain da transferência de arquivo pela rede**.
   Etapa 2. Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
   Etapa 3. No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo de certificado de raiz.
   Etapa 4. Arquivo da transferência de arquivo pela rede do clique.Nota: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e servidores secundários não está precisada de transferir arquivos pela rede o certificado de raiz ao server secundário CUIC.

2. Certificado preliminar do aplicativo de servidor da transferência de arquivo pela rede CUIC.

   Etapa 1. Da lista de drop-down do nome do certificado, selecione TomCat.
   Etapa 2. No campo de arquivo da transferência de arquivo pela rede, o clique consulta e consulta ao arquivo certificado do aplicativo.
   Etapa 3. Arquivo da transferência de arquivo pela rede do clique.
3. Certificado secundário do aplicativo de servidor da transferência de arquivo pela rede CUIC.

Siga o mesmo processo como exposto em etapa (2) no servidor secundário para seu próprio certificado do aplicativo

4. Reinicie server
   Alcance o CLI nos server preliminares e secundários CUIC e incorpore o comando dos **"reinício do sistema utils"** reiniciar os server.
   Nota: Se a autoridade de CA fornece o certificate chain que inclui Certificados intermediários então as etapas mencionadas nos server que da fineza a seção é aplicável aos saques CUIC também.

Servidores de dados vivos

1. As etapas envolveram nos server Vivo-DATA para transferir arquivos pela rede os Certificados são idênticas à fineza ou aos server CUIC segundo o certificate chain.

2. Certificado de raiz da transferência de arquivo pela rede no server Vivo-DATA preliminar.

   Etapa 1. 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**.
   Etapa 2. Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
   Etapa 3. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta ao arquivo de certificado de raiz.
   Etapa 4. **Transferência de arquivo pela rede do** clique.

3. Certificado intermediário da transferência de arquivo pela rede no server Vivo-DATA preliminar.

   Etapa 1. As etapas em transferir arquivos pela rede o certififcate intermediário são mesmas que o certificado de raiz segundo as indicações de etapa 1.
   Etapa 2. 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**.
   Etapa 3. Da lista de drop-down do nome do certificado, selecione a Tomcat-confiança.
   Etapa 4. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta ao arquivo certificado intermediário.
   Etapa 5. **Transferência de arquivo pela rede do** clique.
   Nota: Enquanto a loja da Tomcat-confiança replicated entre o preliminar e servidores secundários não está precisada de transferir arquivos pela rede a raiz ou o certificado do intermediário ao server Vivo-DATA secundário.
4. Certificado preliminar do aplicativo de servidor Vivo-DATA da transferência de arquivo pela rede.

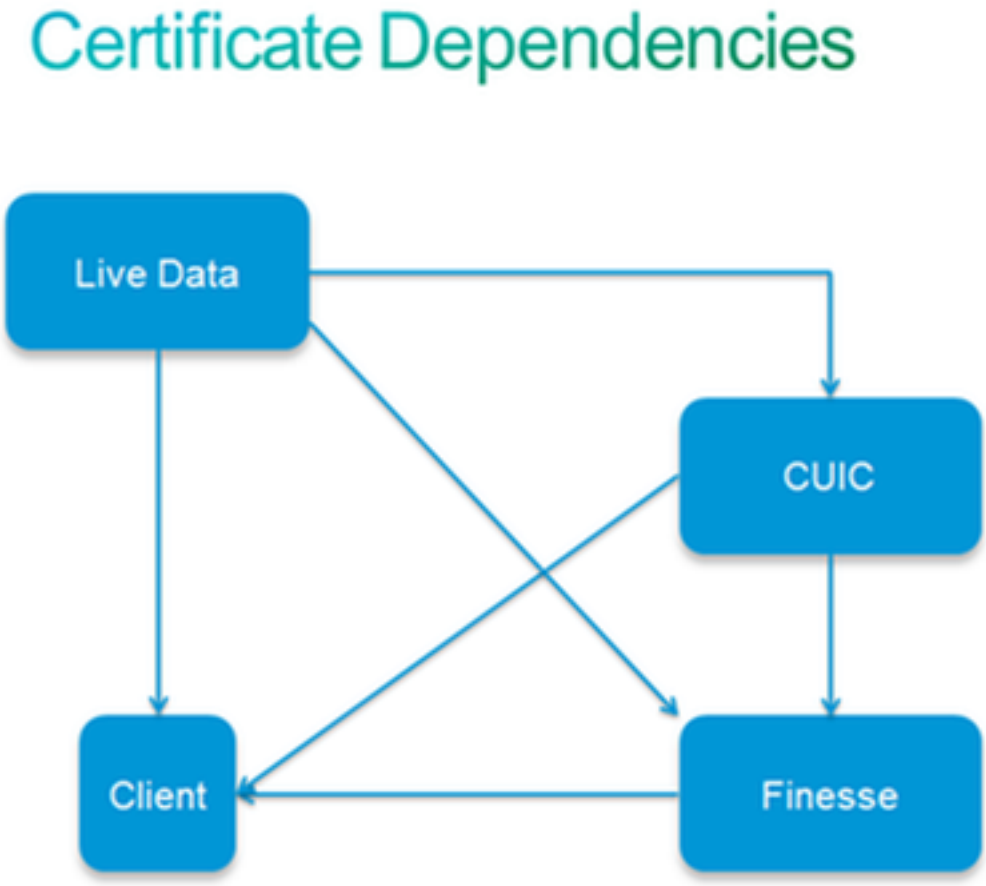
   Etapa 1. Da lista de drop-down do nome do certificado, selecione TomCat.
   Etapa 2. No campo de arquivo da transferência de arquivo pela rede, o clique **consulta** e consulta ao arquivo certificado do aplicativo.
   Etapa 3. **Transferência de arquivo pela rede do** clique.

5. Certificado secundário do aplicativo de servidor Vivo-DATA da transferência de arquivo pela rede.
   Siga as mesmas etapas como mencionado acima dentro (4) no server secondory para seu próprio certificado do aplicativo.

6. Reinicie server
   Alcance o CLI nos server preliminares e secundários da fineza e incorpore o comando dos **"reinício do sistema utils"** reiniciar os server.

Vivem as dependências do certificado de servidores de dados

Como servidores de dados vivos interage com o CUIC e os server da fineza, está umas dependências do certificado entre estes server segundo as indicações da imagem:



Com respeito à corrente de certificado de CA da terceira parte os Certificados da raiz e do intermediário são mesmos para todos os server na organização. Em consequência para que o servidor de dados Live trabalhe corretamente, você tem que assegurar-se de que a fineza e os server CUIC tenham os Certificados da raiz e do intermediário carregados corretamente lá em uns recipientes da Tomcat-confiança.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

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