Certificados com assinatura automática do Exchange em uma solução UCCE

Contents

Introdução

Este documento descreve como trocar certificados autoassinados na solução Unified Contact Center Enterprise (UCCE).

Contribuição de Anuj Bhatia, Robert Rogier e Ramiro Amaya, engenheiros do Cisco TAC

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Console de operações do CVP (OAMP)
- CVP Novo OAMP (NOAMP)

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

Background

Em uma solução UCCE, a configuração de novos recursos que envolvem aplicativos centrais, como ROGGERs, Gateways Periféricos (PGs), Estações de Trabalho Administrativas (AW) / Servidores de Dados Administrativos (ADS), Finesse, Cisco Unified Intelligence Center (CUIC) e assim por diante, é feita através da página de Administração do Contact Center Enterprise (CCE). Para aplicativos de Resposta de Voz Interativa (IVR - Interative Voice Response) como CVP, Cisco VB e gateways, o NOAMP controla a configuração de novos recursos. A partir do CCE 12.5(1), devido à conformidade de gerenciamento de segurança (SRC), todas as comunicações para o CCE Admin e NOAMP são estritamente feitas através do protocolo HTTP seguro.

Para obter uma comunicação segura perfeita entre esses aplicativos em um ambiente de certificado autoassinado, a troca de certificados entre os servidores torna-se uma necessidade. A próxima seção explica em detalhes as etapas necessárias para trocar o certificado autoassinado entre:

- Servidores CCE AW e servidores de aplicativos principais CCE
- Servidor CVP OAMP e servidores de componentes CVP

Procedimento

Servidores CCE AW e servidores de aplicativos principais CCE

Estes são os componentes dos quais os certificados autoassinados são exportados e os componentes para os quais os certificados autoassinados precisam ser importados.

Servidores AW CCE: este servidor requer certificado de:

- Plataforma Windows: Roteador e Agente(Rogger){A/B}, Gateway Periférico (PG){A/B} e todos os AW/ADS.

Observação: o IIS e os certificados do Diagnostic Framework Portico (DFP) são necessários.

- Plataforma VOS: Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect e outros servidores aplicáveis que fazem parte do banco de dados de inventário.

O mesmo se aplica a outros servidores AW na solução.

Roteador \ Servidor de Log: Este servidor requer certificado de:

- Plataforma Windows: todos os certificados IIS do servidor AW.

As etapas necessárias para a troca eficaz de certificados autoassinados para o CCE estão divididas nestas seções:

Seção 1: Troca de certificados entre roteador\logger, PG e servidor AW
Seção 2: Intercâmbio de certificados entre o aplicativo da plataforma VOS e o servidor AW

Seção 1: Troca de certificados entre roteador\logger, PG e servidor AW

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte certificados do IIS de Router\Logger, PG e todos os servidores AW.
Etapa 2. Exporte certificados DFP de Router\Logger, PG e todos os servidores AW.
Etapa 3. Importe certificados IIS e DFP de Router\Logger, PG e AW para servidores AW.
Etapa 4. Importe certificados do IIS para o Roteador\Agente de Log e PG dos servidores AW.

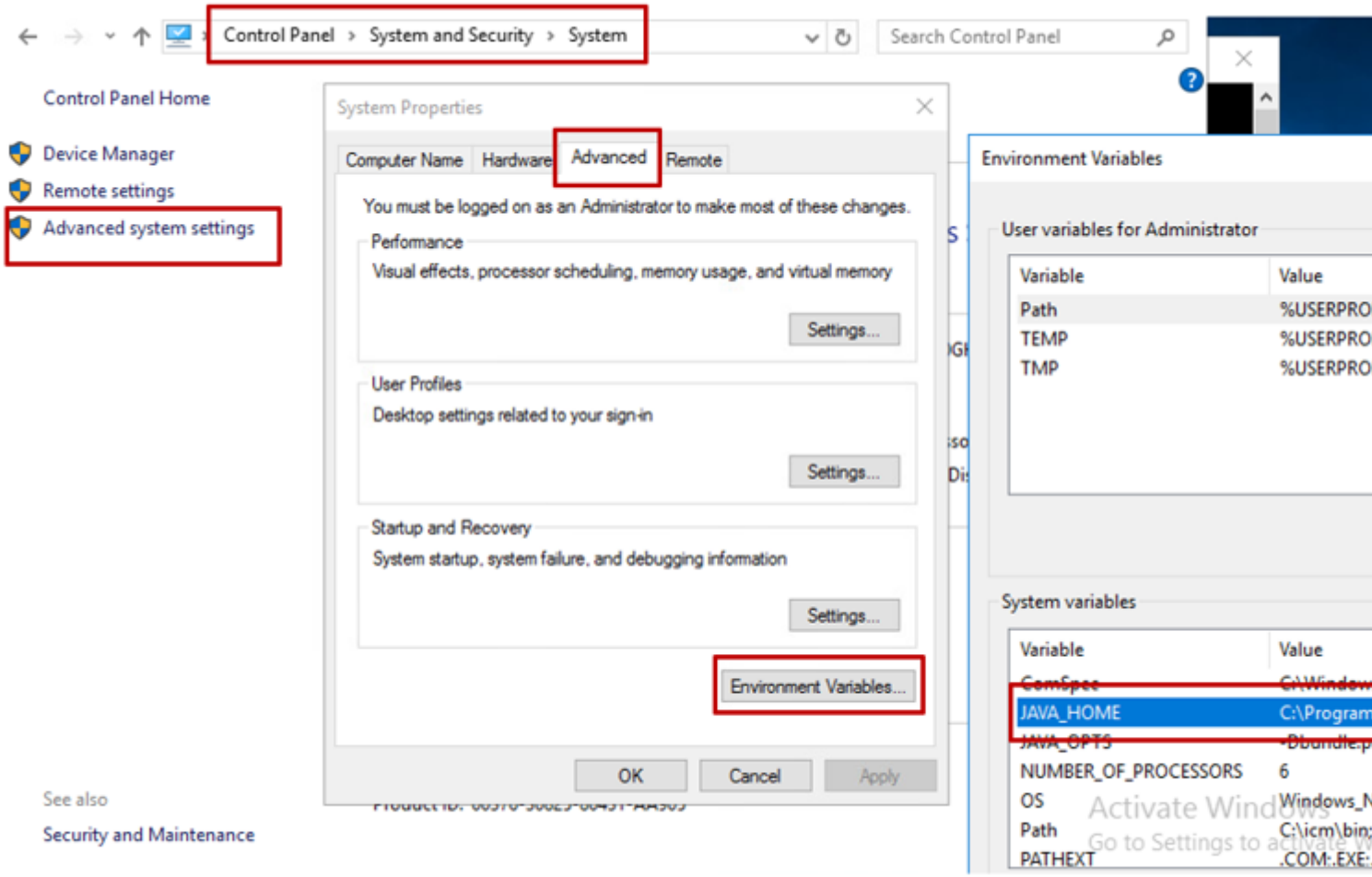
> **Cuidado**: antes de começar, você deve fazer backup do armazenamento de chaves e abrir o prompt de comando como Administrador.

(i) Conheça o caminho do home do java para garantir onde o java keytool está hospedado. Há algumas maneiras de encontrar o caminho do início java.

Opção 1: Comando CLI: **echo %JAVA_HOME%**

```
C:\>echo %java_home%
C:\Program Files (x86)\Java\jre1.8.0_221
```

Opção 2: manualmente, por meio da configuração Avançada do sistema, conforme mostrado na imagem.



> **Observação**: no UCCE 12.5, o caminho padrão é C:\Program Files (x86)\Java\jre1.8.0_221\bin. No

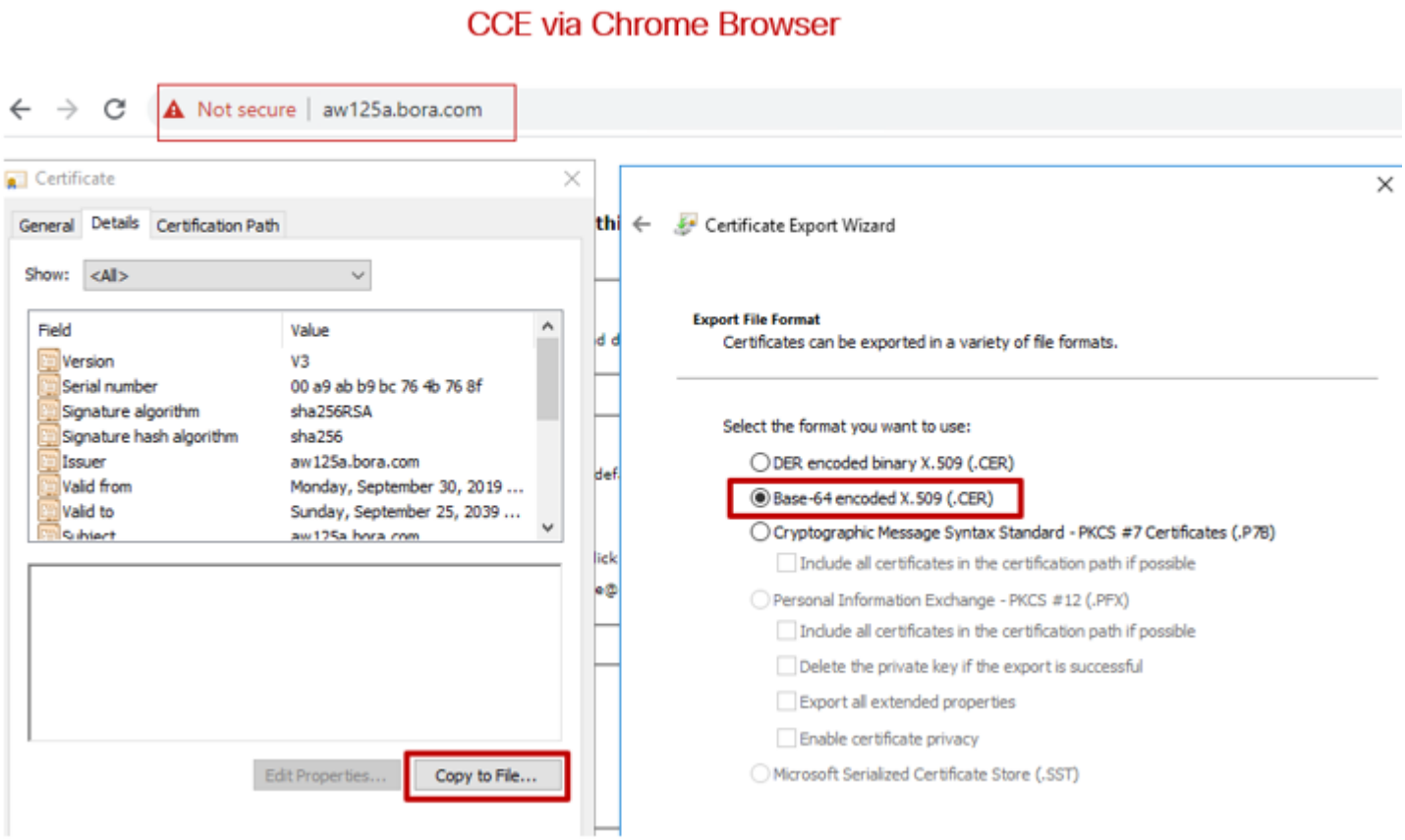
---

entanto, se você tiver usado o instalador 12.5(1a) ou tiver o 12.5 ES55 instalado (OpenJDK ES obrigatório), use o %CCE_JAVA_HOME% em vez do %JAVA_HOME%, pois o caminho do armazenamento de dados foi alterado com o OpenJDK. Mais informações sobre a migração do OpenJDK no CCE e no CVP nestes documentos: Instalar e migrar para o OpenJDK no CCE 12.5(1) e Instalar e migrar para o OpenJDK no CVP 12.5(1).

(ii) Faça backup do arquivo **cacerts** da pasta **{JAVA_HOME}\lib\security.** Você pode copiá-lo para outro local.

Etapa 1. Exportar certificados do IIS de Router\Logger, PG e todos os servidores AW

(i) Em um servidor AW a partir de um navegador, navegue até os servidores (ROGGERs , PG , outros servidores AW) url: **https://{servername}.**

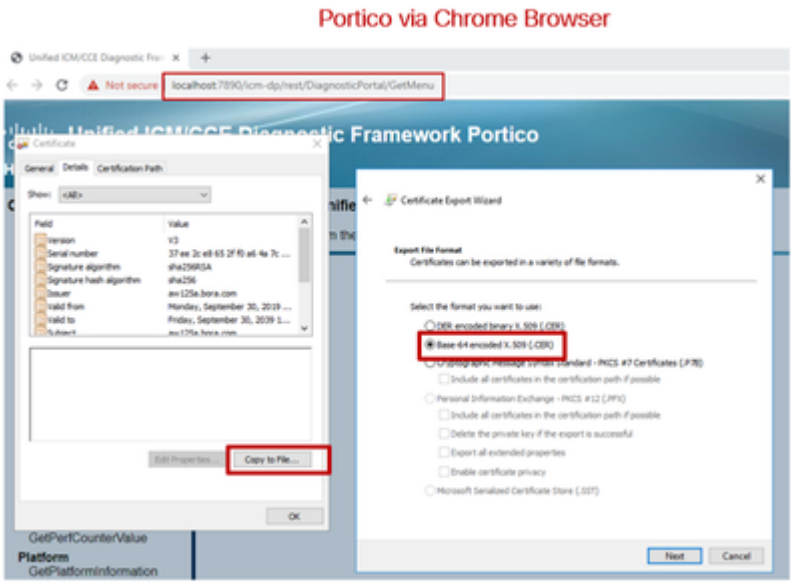


(ii) Salve o certificado em uma pasta temporária, por exemplo c:\temp\certs e nomeie o certificado como ICM{svr}[ab].cer.

Nota:Selecione a opção X.509 (.CER) codificado na Base 64.

Etapa 2. Exportar certificados DFP de Router\Logger, PG e todos os servidores AW

(i) No servidor AW, abra um navegador e navegue até os servidores (Router, Logger ou ROGGERs, PGs, AWs) DFP url : **https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.**



(ii) Salve o certificado na pasta exemplo c:\temp\certs e nomeie o certificado como dfp{svr}[ab].cer

---

Observação: selecione a opção X.509 (.CER) codificado na Base 64.

Etapa 3. Importar certificados do IIS e DFP de Router\Logger, PG e AW para servidores AW

Observação: os comandos de exemplo usam a senha de keystore padrão de "changeit". Você deve alterar isso se tiver modificado a senha em seu sistema.

Comando para importar os certificados autoassinados do IIS para o servidor AW. O caminho para executar a Keytool: **%JAVA_HOME%\bin**:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com_
```

Observação: importe todos os certificados de servidor exportados para todos os servidores AW.

Comando para importar os certificados autoassinados do DFP para servidores AW:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com_
```

Observação: importe todos os certificados de servidor exportados para todos os servidores AW.

Reinicie o serviço Apache Tomcat nos servidores AW.

Etapa 4. Importe certificados do IIS para o Roteador\Agente de Log e PG dos servidores AW.

Comando para importar os certificados autoassinados do AW IIS para os servidores Router\Logger e PG:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myawa.domain.com_I
```

> **Observação**: importe todos os certificados do servidor AW IIS exportados para os servidores Router\Logger e PG nos lados A e B.

Reinicie o serviço Apache Tomcat nos servidores Router\Logger e PG.

Seção 2: Intercâmbio de certificados entre aplicativos da plataforma VOS e o servidor AW

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exportar certificados do servidor de aplicativos da plataforma VOS.
Etapa 2. Importar certificados de aplicativos da plataforma VOS para o AW Server.

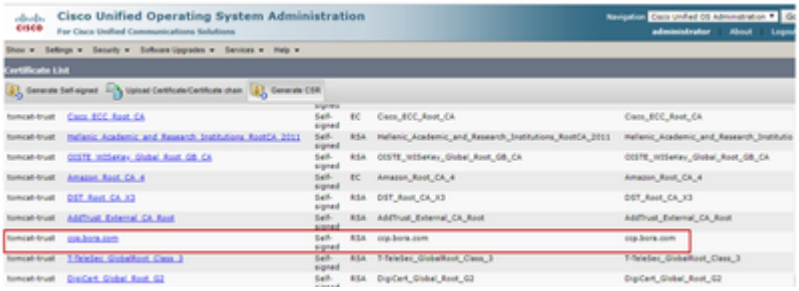
Esse processo se aplica a todos os aplicativos de VOS, como:

- Finesse
- CUIC \ LD \ IDS
- Conexão em nuvem

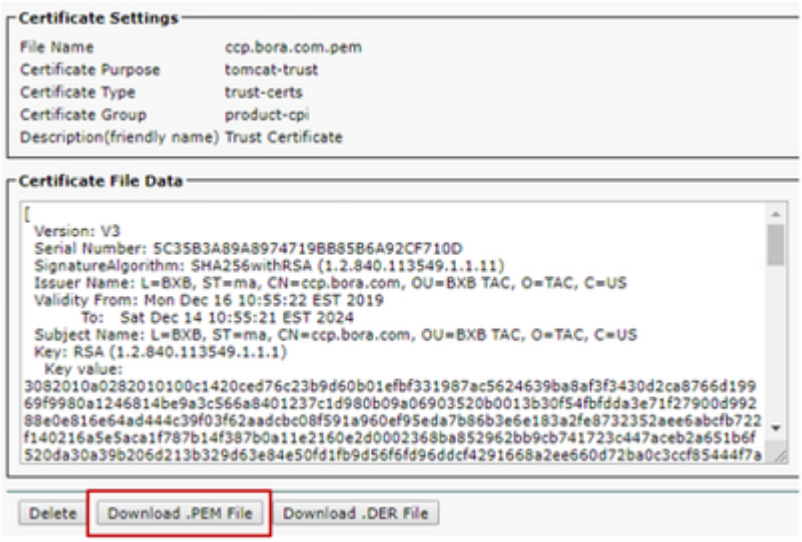
Etapa 1. Exportar certificados do servidor de aplicativos da plataforma VOS.

(i) Navegue até a página Cisco Unified Communications Operating System Administration: **https://{FQDN}:8443/cmplatform**.

(ii) Navegue para **Segurança > Gerenciamento de Certificados** e localize os certificados do servidor primário de aplicativos na pasta tomcat-trust.



(iii) Selecione o certificado e clique em baixar arquivo .PEM para salvá-lo em uma pasta temporária no servidor AW.



Observação: Execute as mesmas etapas para o assinante.

Etapa 2. Importe o aplicativo da plataforma VOS para o AW Server.

Caminho para executar a ferramenta de Chave: **{JAVA_HOME}\bin**

Comando para importar os certificados autoassinados:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\temp
```

Reinicie o serviço Apache Tomcat nos servidores AW.

Observação: execute a mesma tarefa em outros servidores AW.

Servidor CVP OAMP e servidores de componentes CVP

Estes são os componentes dos quais os certificados autoassinados são exportados e os componentes para os quais os certificados autoassinados precisam ser importados.

(i) Servidor CVP OAMP: este servidor exige certificado de:

- Plataforma Windows: certificado do Gerenciador de Serviços Web (WSM) do servidor CVP e dos servidores de Relatórios.
- Plataforma VOS: Cisco VB para integração com o Customer Virtual Agent (CVA), servidor Cloud Connect para integração com o Webex Experience Management (WXM).

(ii) Servidores CVP: Este servidor requer certificado de:

- Plataforma Windows: certificado WSM do servidor OAMP.
- Plataforma VOS: servidor Cloud Connect para integração WXM e servidor Cisco VVB.

(iii) Servidores de relatórios do CVP: este servidor exige certificado do

- Plataforma Windows: certificado WSM do servidor OAMP.

(iv) servidores Cisco VB:este servidor requer certificado de:

- Plataforma Windows: certificado VXML do servidor CVP e certificado Callserver do servidor CVP.

As etapas necessárias para a troca eficaz de certificados autoassinados no ambiente do CVP são explicadas nessas três seções.

Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios.
Seção 2: Intercâmbio de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS.
Seção 3: Troca de certificados entre o servidor CVP e os servidores VVB.

Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte o certificado WSM do servidor CVP, do servidor de relatórios e do servidor OAMP.
Etapa 2. Importe certificados WSM do servidor CVP e do servidor de Relatórios para o servidor OAMP.
Etapa 3. Importe o certificado WSM do servidor CVP OAMP para o servidor CVP e o servidor de relatórios.

> **Cuidado**: antes de começar, você deve fazer o seguinte:
> 1. Abra uma janela de comando como administrador.
> 2. Para identificar a senha do armazenamento de chaves, execute o comando, **more %CVP_HOME%\conf\security.properties**.
> 3. Você precisa dessa senha ao executar os comandos keytool.
> 4. No diretório %CVP_HOME%\conf\security\, execute o comando **copy .keystore backup.keystore**.

Etapa 1. Exporte o certificado WSM do servidor CVP, do servidor de relatórios e do servidor OAMP.

(i) Exporte o certificado WSM de cada servidor para um local temporário e renomeie o certificado com um nome desejado. Você pode renomeá-lo como wsmX.crt. Substitua X pelo nome de host do servidor. Por exemplo, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Comando para exportar os certificados autoassinados:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -al
```

(ii) Copie o certificado do caminho C:\Cisco\CVP\conf\security\wsm.crt de cada servidor e renomeie-o como wsmX.crt com base no tipo de servidor.

Etapa 2. Importe os certificados WSM dos servidores CVP e dos servidores de relatórios para o servidor OAMP.

(i) Copie o certificado WSM de cada servidor CVP e servidor de Relatórios (wsmX.crt) para o diretório %CVP_HOME%\conf\security no servidor OAMP.

(ii) Importe esses certificados com o comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -al
```

(iii) Reinicialize o servidor.

Etapa 3. Importe o certificado WSM do servidor CVP OAMP para os servidores CVP e servidores de relatórios.

(i) Copie o certificado WSM do servidor OAMP (wsmoampX.crt) para o diretório %CVP_HOME%\conf\security em todos os servidores CVP e servidores de Relatórios.

(ii) Importar os certificados com o comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -al
```

(iii) Reinicialize os servidores.

Seção 2: Troca de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte o certificado do aplicativo da plataforma VOS.

Etapa 2. Importe o certificado do aplicativo VOS para o servidor OAMP.

Esse processo é aplicável a aplicativos VOS, como:

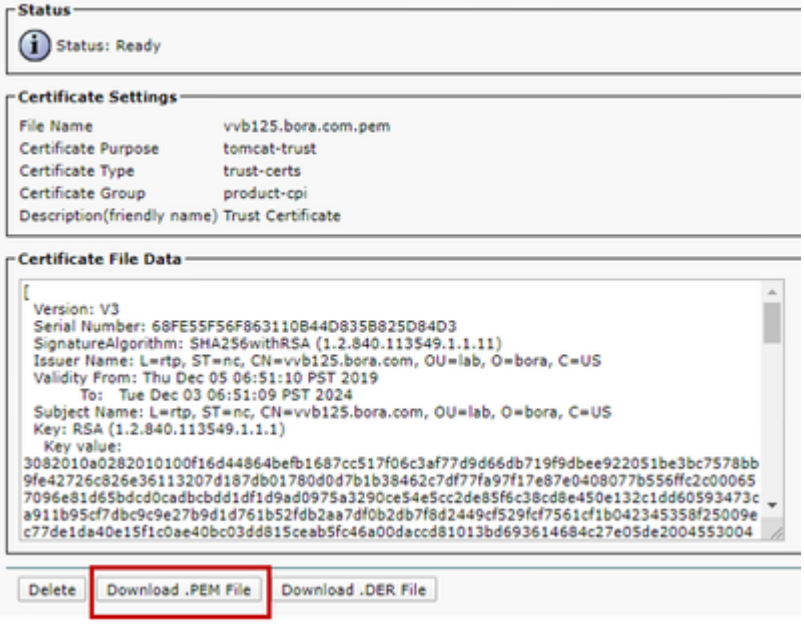
- CUCM
- VVB
- Conexão em nuvem

Etapa 1. Exporte o certificado do aplicativo da plataforma VOS.

(i) Navegue até a página Cisco Unified Communications Operating System Administration: https://{FQDN}:8443/cmplatform.

(ii) Navegue para **Segurança > Gerenciamento de Certificados** e localize os certificados do servidor primário de aplicativos na pasta tomcat-trust.

(iii) Selecione o certificado e clique em fazer download do arquivo .PEM para salvá-lo em uma pasta temporária no servidor OAMP.



Etapa 2. Importe o certificado do aplicativo VOS para o servidor OAMP.

(i) Copie o certificado VOS para o diretório %CVP_HOME%\conf\security no servidor OAMP.

(ii) Importar os certificados com o comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -al
```

(ii) Reinicialize o servidor.

Seção 3: Troca de certificados entre servidores CVP e VVB

Esta é uma etapa opcional para proteger a comunicação SIP entre o CVP e outros componentes do Contact Center. Para obter mais informações consulte a seção Guia de configuração do CVP: Guia de configuração do CVP - Segurança.

Integração do serviço Web CallStudio do CVP

Para obter informações detalhadas sobre como estabelecer uma comunicação segura para o elemento de serviços da Web e o elemento Rest_Client

Consulte o Guia do usuário do Cisco Unified CVP VXML Server e do Cisco Unified Call Studio Release 12.5(1) - Integração de serviços da Web [Cisco Unified Customer Voice Portal] - Cisco

Informações Relacionadas

- Guia de configuração do CVP - Segurança
- Guia de segurança do UCCE
- Guia do administrador do PCCE - Segurança
- Certificados com assinatura automática do Exchange PCCE - PCCE 12.5
- Certificados com assinatura automática do Exchange UCCE - UCCE 12.5
- Certificados com assinatura automática do Exchange PCCE - PCCE 12.6

- Implementar certificados assinados por CA - CCE 12.6
- Migração OpenJDK do CCE
- Migração OpenJDK do CVP
- Suporte Técnico e Documentação - Cisco Systems

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.