Certificados com assinatura automática do Exchange em uma solução PCCE

Contents

Introduction

Este documento descreve como trocar certificados autoassinados entre o servidor de administração principal (ADS/AW) e outro servidor de aplicativos na solução Cisco Packaged Contact Center Enterprise (PCCE).

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

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PCCE Versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- PCCE 12.5(1)
- CVP 12.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Na solução PCCE da versão 12.x, todos os dispositivos são controlados por meio do SPOG (Single Pane of Glass), que é hospedado no servidor AW principal. Devido à conformidade de gerenciamento de segurança (SRC - security-management-compliance) na versão PCCE 12.5(1), toda a comunicação entre o SPOG e outros servidores na solução é feita estritamente através do protocolo HTTP seguro.

Os certificados são usados a fim de obter uma comunicação segura transparente entre o SPOG e os outros dispositivos. Em um ambiente de certificado autoassinado, a troca de certificados entre os servidores torna-se obrigatória. Essa troca de certificado também é necessária para habilitar novos recursos presentes na versão 12.5(1), como Smart Licensing, Webex Experience Management (WXM) e Customer Virtual Assistant (CVA).

Procedimento

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 AW principal: Este servidor requer certificado de:

- Plataforma Windows: ICM Roteador e Agente(Rogger){A/B}, Gateway Periférico (PG){A/B}, todos os servidores ADS e de E-mail e Bate-papo (ECE). Note: O IIS e os certificados da estrutura de diagnóstico são necessários.CVP Servidores CVP, servidor de relatórios CVP. Nota 1: O certificado WSM (Gerenciamento de serviços da Web) dos servidores é necessário.Nota 2: Os certificados devem estar com FQDN (Nome de Domínio Totalmente Qualificado).
- Plataforma VOS: Cloud Connect, Cisco Virtual Voice Browser (VVB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) e outros servidores aplicáveis.

O mesmo se aplica a outros servidores ADS na solução.

(ii) Roteador \ Servidor de Logger: Este servidor requer certificado de:

- Plataforma Windows: Todos os certificados IIS de servidores ADS.

(iii) Servidor CUCM PG: Este servidor requer certificado de:

- Plataforma VOS: Editor de CUCM. Note: Isso é necessário para baixar o cliente JTAPI do servidor CUCM.

(iv) Servidor CVP: Este servidor requer um certificado de

- Plataforma Windows: Todos os certificados IIS de servidores ADS
- Plataforma VOS: Servidor Cloud Connect para Integração WXM, Servidor VB para comunicação SIP e HTTP segura.

v) Servidor de relatórios do CVP: Este servidor requer certificado de:

- Plataforma Windows: Todos os certificados IIS de servidores ADS

(vi) Servidor VB: Este servidor requer certificado de:

- Plataforma Windows: Servidor CVP VXML (HTTP seguro), servidor de chamada CVP (SIP seguro)

As etapas necessárias para a troca eficaz de certificados autoassinados na solução estão divididas em três seções.

Seção 1: Troca de certificados entre servidores CVP e servidores ADS.

Seção 2: Troca de Certificados entre Aplicativos da Plataforma VOS e Servidor ADS.

Seção 3: Troca de Certificado entre Roggers, PGs e Servidor ADS.

Seção 1: Troca de certificados entre servidores CVP e ADS

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exportar certificados WSM do servidor CVP.

Etapa 2. Importar o certificado WSM do servidor CVP para o servidor ADS.

Etapa 3. Exportar Certificado de Servidor ADS.

Etapa 4. Importar o servidor ADS para os servidores CVP e o servidor de relatórios CVP.

Etapa 1. Exportar certificados do servidor CVP

Antes de exportar os certificados dos servidores CVP, você precisa gerar novamente os certificados com o FQDN do servidor; caso contrário, poucos recursos como Smart Licensing, CVA e a sincronização CVP com SPOG podem ter problemas.

> **Caution**: Antes de começar, você deve fazer o seguinte:

- Obtenha a senha do armazenamento de chaves. Execute este comando: more %CVP_HOME%\conf\security.properties
- Copie a pasta %CVP_HOME%\conf\security para outra pasta.
- Abra uma janela de comando como Administrador para executar os comandos.

> **Note**: Você pode simplificar os comandos usados neste documento usando o parâmetro keytool -storepass. Para todos os servidores CVP, cole a senha obtida do arquivo security.properties especificado. Para os servidores ADS, digite a senha: **changeit**

Para gerar novamente o certificado nos servidores CVP, siga estas etapas:

(i) Listar os certificados no servidor

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

> **Note**: Os servidores CVP têm estes certificados autoassinados: wsm_certificate , vxml_certificate , callserver_certificate. Se você usar o parâmetro -v da keytool, poderá ver informações mais detalhadas de cada certificado. Além disso, você pode adicionar o símbolo ">" no final do comando de lista keytool.exe para enviar a saída para um arquivo de texto, por exemplo: > test.txt

(ii) Suprimir os antigos certificados autoassinados

Servidores CVP: comando para excluir os certificados autoassinados:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias vxml_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias callserver_certificate
```

Servidores de relatórios CVP: comando para excluir os certificados autoassinados:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias callserver_certificate
```

> **Note**: Os servidores de relatórios do CVP têm esses certificados autoassinados wsm_certificate, callserver_certificate.

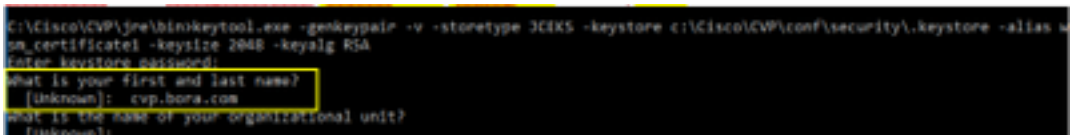
(iii) Gerar os novos certificados autoassinados com o FQDN do servidor

servidores CVP

Comando para gerar o certificado autoassinado para WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Especifique o FQDN do servidor na pergunta **qual é seu nome e sobrenome**?



Responda estas outras perguntas:

Qual é o nome da sua unidade organizacional?

[Desconhecido]: <especificar UO>

Qual é o nome da sua empresa?

[Desconhecido]: <especifique o nome da organização>

Qual é o nome da sua cidade ou localidade?

[Desconhecido]: <especifique o nome da cidade/localidade>

Qual é o nome do seu estado ou província?

[Desconhecido]: <especifique o nome do estado/província>

Qual é o código de duas letras do país para essa unidade?

[Desconhecido]: <especifique o código de país com duas letras>

Especifique **yes** para as duas entradas seguintes.

Execute as mesmas etapas para vxml_certificate e callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Reinicialize o servidor de chamadas do CVP.

Servidores de relatórios CVP

Comando para gerar certificados autoassinados para WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Especifique o FQDN do servidor para a consulta **qual é seu nome e sobrenome?** e siga os mesmos passos que foram dados com os servidores CVP.

Execute as mesmas etapas para callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Reinicialize os servidores de Relatórios.

Note: Por padrão, os certificados autoassinados são gerados por dois anos. Use -valid XXXX para definir a data de expiração quando os certificados forem gerados novamente; caso contrário, os certificados serão válidos por 90 dias. Para a maioria desses certificados, 3 a 5 anos devem ser um tempo de validação razoável.

Aqui estão algumas entradas de validade padrão:

Um ano	365
Dois anos	730
Três anos	1095
Quatro anos	1460
Cinco anos	1895
Dez anos	3650

Caution: Em 12.5, os certificados devem ser **SHA 256**, Key Size **2048** e encryption Algorithm **RSA**, use estes parâmetros para definir estes valores: -keyalg RSA e -keysize 2048. É importante que os comandos keystore do CVP incluam o parâmetro -storetype JCEKS. Se isso não for feito, o certificado, a chave, ou pior, o armazenamento de chaves pode se tornar corrompido.

(iv) Exportar wsm_Certificate do CVP e servidores de relatórios

a) Exporte o certificado WSM de cada servidor CVP para um local temporário e renomeie o certificado com o nome desejado. Você pode renomeá-lo como wsmcsX.crt. Substitua "X" por um número ou letra exclusivo. que é wsmcsa.crt, wsmcsb.crt.

Comando para exportar os certificados autoassinados:

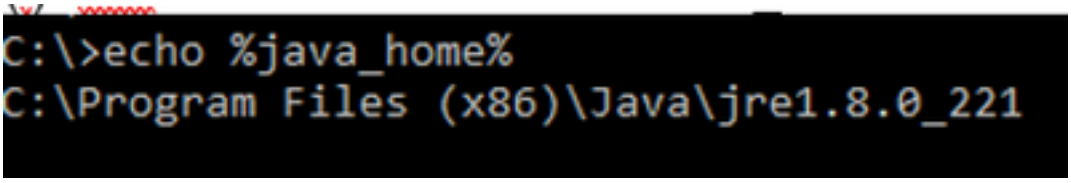
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copie o certificado do caminho **C:\Cisco\CVP\conf\security\wsm.crt**, renomeie-o para *wsmcsX.crt* e mova-o para uma pasta temporária no servidor ADS.

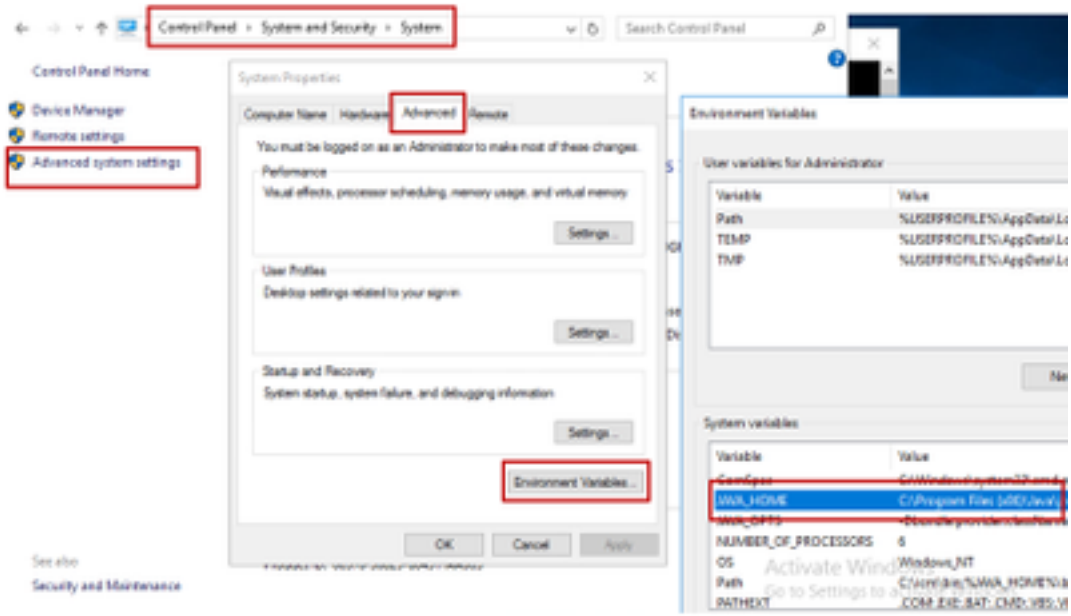
Etapa 2. Importar o certificado WSM dos servidores CVP para o servidor ADS

Para importar o certificado no servidor ADS, você precisa usar a ferramenta de chave que faz parte do conjunto de ferramentas java. Há algumas maneiras de encontrar o caminho do home java onde esta ferramenta está hospedada.

(i) Comando CLI > **echo %JAVA_HOME%**



(ii) Manualmente via **configuração avançada do sistema,** como mostrado na imagem.



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

Comando para importar os certificados autoassinados:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -storepass changeit -alias {fqdn_of_cvp} -file c:\temp\certs\wsmcsX.crt
```

> **Note**: Repita os comandos para cada CVP na implantação e execute a mesma tarefa em outros servidores ADS

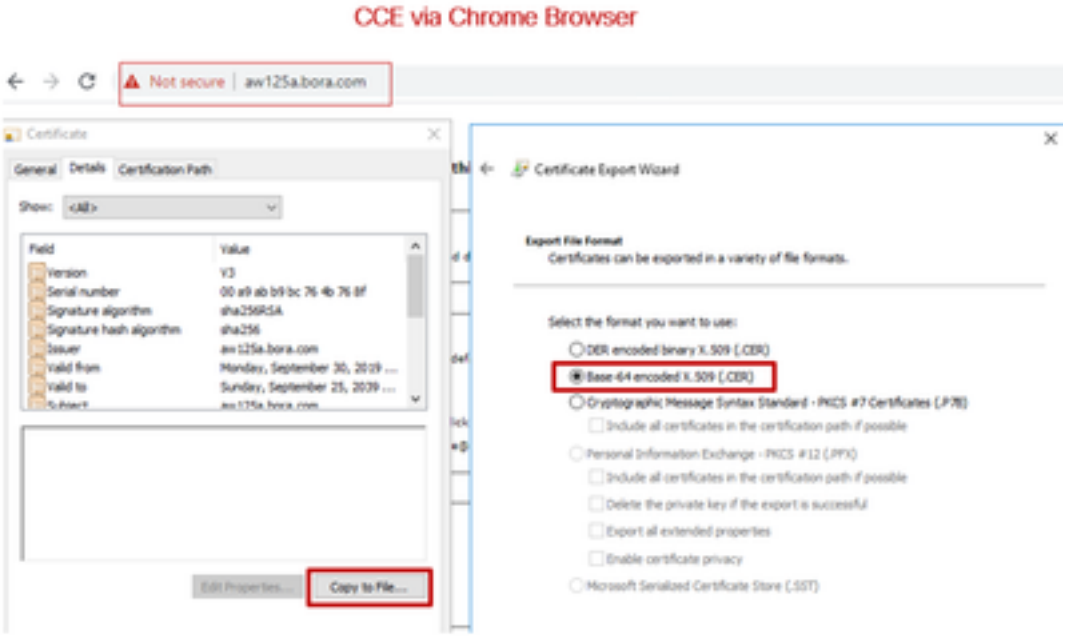
d) Reinicie o serviço Apache Tomcat nos servidores ADS.

Etapa 3. Exportar Certificado de Servidor ADS

Para o servidor de relatórios do CVP, você precisa exportar o certificado ADS e importá-lo para o servidor de relatórios. Aqui estão as etapas:

(i) No servidor ADS de um navegador, navegue até a URL do servidor : **https://{servername}**

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



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

Etapa 4. Importar o servidor ADS para servidores CVP e servidor de relatórios

(i) Copie o certificado para os servidores CVP e o servidor de relatórios CVP no diretório **C:\Cisco\CVP\conf\security.**

(ii) importe o certificado para servidores CVP e servidor de relatórios CVP.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ICM{svr}[ab].cer
```

Execute as mesmas etapas para outros servidores ADS.

(iii) Reiniciar os servidores CVP e o servidor de relatórios

Seção 2: Troca de certificados entre aplicativos da plataforma VOS e servidor ADS

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 servidor ADS.

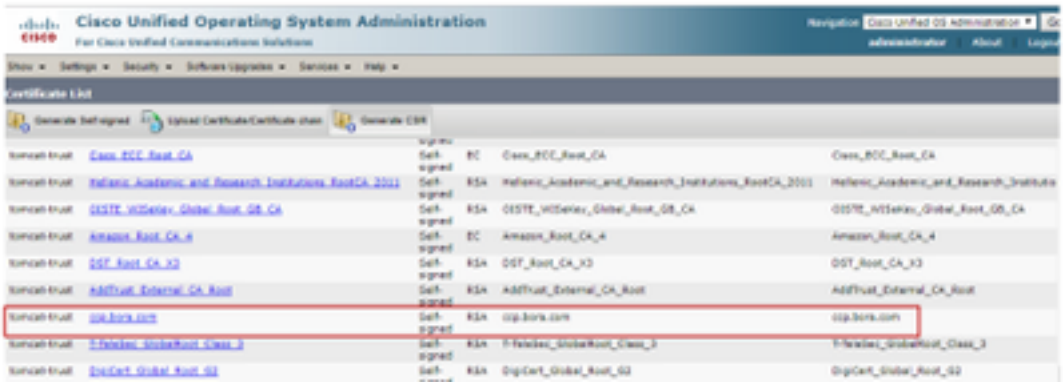
Esse processo se aplica a todos os aplicativos de VOS, como:

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

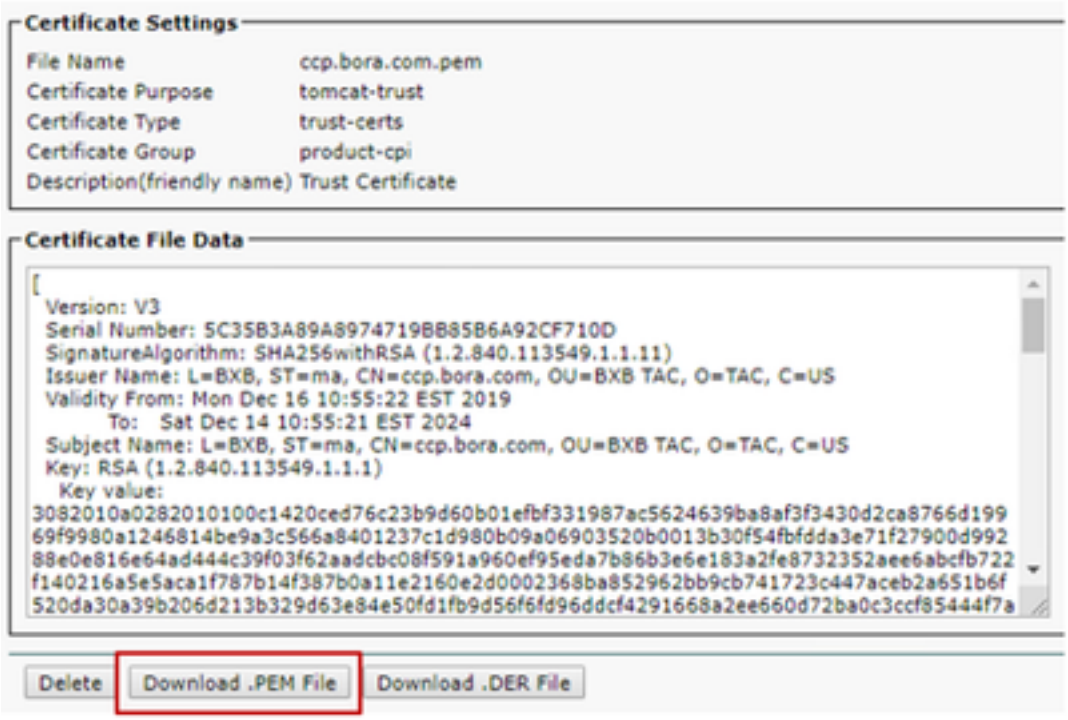
Etapa 1. Exportar certificados do servidor de aplicativos da plataforma VOS.

(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 no arquivo .PEM de download para salvá-lo em uma pasta temporária no servidor ADS.



Note: Execute as mesmas etapas para o assinante.

Etapa 2. Importar o aplicativo da plataforma VOS para o servidor ADS

Caminho para executar a ferramenta Chave: **C:\Program Arquivos (x86)\Java\jre1.8.0_221\bin**

Comando para importar os certificados autoassinados:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_vos}  -file c:\temp\certs\vosapplicationX.cer
```

Reinicie o serviço Apache Tomcat nos servidores ADS.

Note: Executar a mesma tarefa em outros servidores ADS

Seção 3: Troca de Certificados entre Servidores Roggers , PG e ADS

As etapas necessárias para concluir essa troca com êxito são:

Passo 1: Exportar Certificado IIS de Rogger e Servidores PG

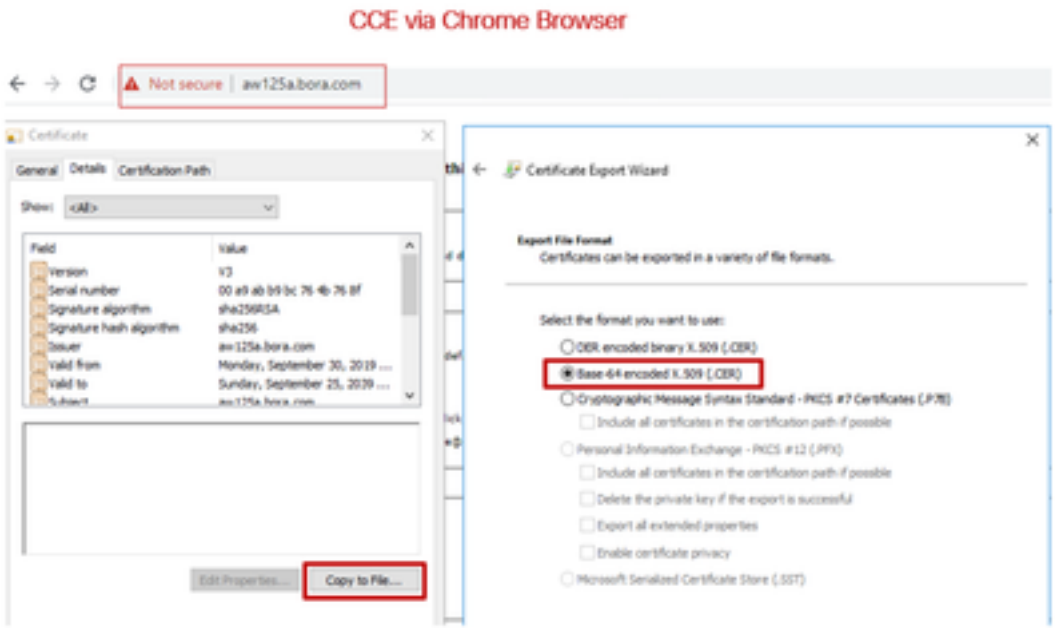
Passo 2: Exportar Certificado DFP (Diagnostic Framework Portico) de Rogger e servidores PG

Passo 3: Importar certificados para servidores ADS

Etapa 1. Exportar Certificado IIS de Servidores Rogger e PG

(i) No servidor ADS de um navegador, navegue até os servidores (Roggers , PG) 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**

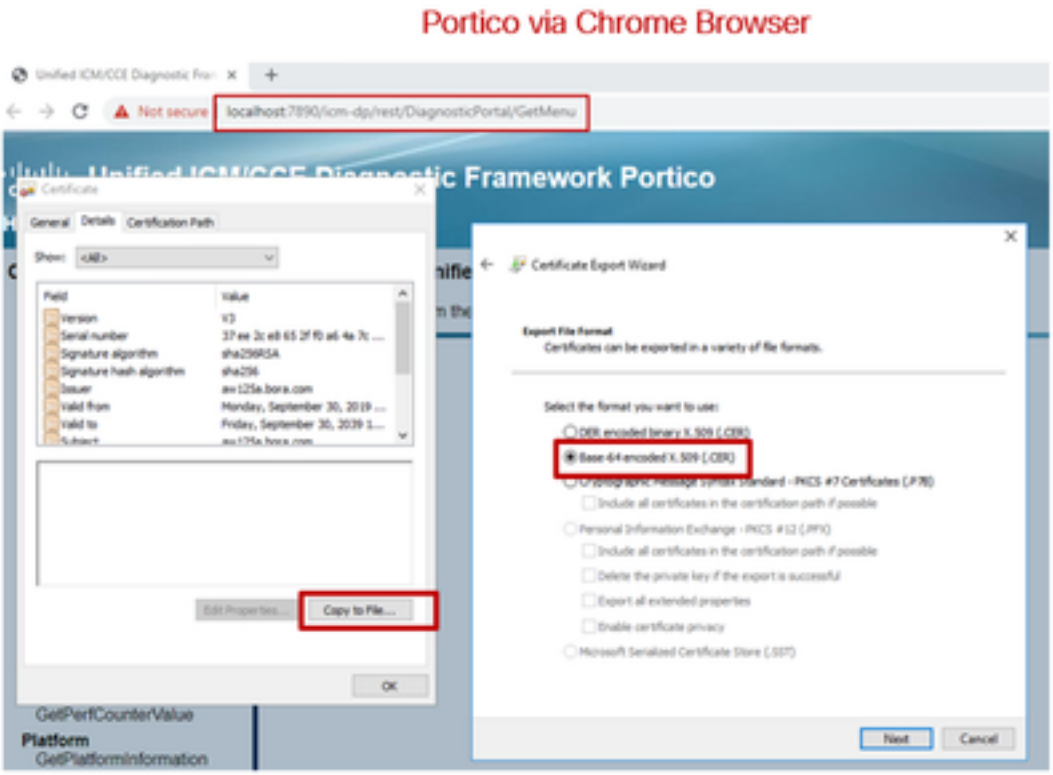


Note: Selecione a opção X.509 (.CER) codificado na Base 64.

Etapa 2. Exportar Certificado DFP (Diagnostic Framework Portico) de Rogger e servidores PG

(i) No servidor ADS de um navegador, navegue até o url DFP dos servidores (Roggers, PGs): *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



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

Etapa 3. Importar Certificados para o Servidor ADS

Comando para importar os certificados autoassinados do IIS para o servidor ADS. O caminho para executar a ferramenta Chave: **C:\Program Arquivos (x86)\Java\jre1.8.0_221\bin.**

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

Note: Importe todos os certificados de servidor exportados para todos os servidores ADS.

Comando para importar os certificados de diagnóstico autoassinados para o servidor ADS

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

Note: Importe todos os certificados de servidor exportados para todos os servidores ADS.

Reinicie o serviço Apache Tomcat nos servidores ADS.

Seção 4: Integração do CVP CallStudio WEBService

Para obter informações detalhadas sobre como estabelecer uma comunicação segura para o elemento de serviços 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: Guia de configuração do CVP - Segurança
- Guia de configuração do UCCE: Guia de configuração UCCE - Segurança
- Guia de administração do PCCE: Guia de administração do PCE - Segurança
- Certificados UCCE Autoassinados: Exchange Certificados UCCE AutoAssinados
- Instalar e migrar para OpenJDK no CCE 12.5(1): Migração OpenJDK do CCE
- Instalar e migrar para OpenJDK no CVP 12.5(1): migração do CVP OpenJDK