Certificados com assinatura automática do Exchange em uma solução PCCE 12.6

Contents

Introdução

Este documento descreve como trocar certificados autoassinados na solução Cisco Packaged Contact Center Enterprise (PCCE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PCCE Versão 12.6(2)
- Customer Voice Portal (CVP) versão 12.6(2)
- Navegador de voz virtualizado (VVB) 12.6(2)
- Servidor de data de administração (ADS) 12.6(2)
- Plataforma de colaboração com o cliente (CCP) 12.6(2)
- E-mail e bate-papo corporativo (ECE) 12.6(2)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- PCCE 12.6(2)

- CVP 12.6(2)

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

Na solução PCCE da versão 12.x, todos os dispositivos são controlados por meio do SPOG (Single Pane of Glass, painel único de vidro), que é hospedado no servidor AW principal. Devido à conformidade de gerenciamento de segurança (SRC - security-management-compliance) da 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 é obrigatória.

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) Todos os Servidores ADS: Estes servidores requerem certificado de:

- Plataforma Windows:
  - ICM: Roteador e Agente de Log (Rogger) {A/B}, Gateway Periférico (PG) {A/B}, todos os ADS e servidores ECE.

Observação: o IIS e os certificados da estrutura de diagnóstico são necessários.

  - CVP: servidores CVP, servidor de relatórios CVP.

Observação: o certificado WSM (Web Service Management) dos servidores é necessário. Os certificados devem estar com FQDN (Nome de Domínio Totalmente Qualificado).

- Plataforma VOS: Cloud Connect, Cisco Virtualized Voice Browser (VVB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligence Center (CUIC), Live Data (LD), Identity Server (IDS) e outros servidores aplicáveis.

(ii) Roteador \ Servidores de Logger: Estes servidores exigem certificado de:

- Plataforma Windows: todos os servidores ADS com certificado IIS.

(iii) Servidores PG: Estes servidores exigem certificado de:

- Plataforma Windows: todos os servidores ADS com certificado IIS.
- Plataforma VOS: CUCM publisher (somente servidores CUCM PG); Cloud Connect e CCP (somente servidor MR PG).

Observação: isso é necessário para baixar o cliente JTAPI do servidor CUCM.

(iv) Servidores CVP: Esses servidores exigem certificado de

- Plataforma Windows: todos os servidores ADS com certificado IIS
- Plataforma VOS: servidor Cloud Connect, servidor VVB.

(v) Servidor de relatórios do CVP: este servidor requer o certificado de:

- Plataforma Windows: todos os servidores ADS com certificado IIS

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

- Plataforma Windows: servidor CVP VXML, servidor CVP Call
- Plataforma VOS: servidor Cloud Connect.

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: Intercâmbio de certificados entre aplicativos da plataforma VOS e o servidor ADS.

Seção 3: Intercâmbio de Certificados 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 certificado WSM do servidor CVP para o servidor ADS.

Etapa 3. Exportar Certificado de Servidor ADS.

Etapa 4. Importar servidor ADS para servidores CVP e 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, Virtual Agent Voice (VAV) e a sincronização do CVP com SPOG podem ter problemas.

Cuidado: antes de começar, você deve fazer o seguinte:
1. Abra uma janela de comando como administrador.
2. Para 12.6.2, para identificar a senha do armazenamento de chaves, vá para a pasta %CVP_HOME%\bin e execute o arquivo DecryptKeystoreUtil.bat.
3. Para 12.6.1, para identificar a senha do armazenamento de chaves, execute o comando, **more %CVP_HOME%\conf\security.properties.**
4. Você precisa dessa senha ao executar os comandos keytool.
5. No diretório %CVP_HOME%\conf\security\, execute o comando **copy .keystore backup.keystore**.

> **Observação**: você pode simplificar os comandos usados neste documento usando o parâmetro keytool -storepass. Para todos os servidores CVP, forneça a senha do keytool que você identificou. Para os servidores ADS, a senha padrão é: **changeit**

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

(i) Listar os certificados no servidor

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

> **Observação**: 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: Comandos para excluir os certificados autoassinados:

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

Servidores de relatórios do CVP: Comandos para excluir os certificados autoassinados:

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

> **Observação**: os servidores de relatórios do CVP possuem estes 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
```

Observação: por padrão, os certificados 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 e precisarão ser assinados por uma CA antes dessa data. 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

Cuidado: dos certificados 12.5 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.

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

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\co
sm_certificate1 -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
  [Unknown]:  cvp.bora.com
What is the name of your organizational unit?
  [Unknown]:
```

Responda a 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 -genkeypai
```

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

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 -genkeypai
```

Especifique o FQDN do servidor para a consulta **qual é seu nome e sobrenome ?** e continue com as mesmas etapas como feito 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 -genkeypai
```

Reinicialize os servidores de Relatórios.

(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" pelo nome de host do servidor. Por exemplo, wsmcsa.crt, wsmcsb.crt , wsmrepa.crt , wsmrepb.crt.

Comando para exportar os certificados autoassinados:

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

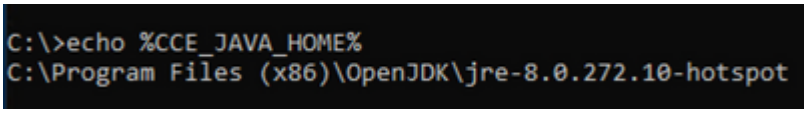
b) Copie o certificado do caminho **%CVP_HOME%\conf\security\wsm.crt**, renomeie-o para *wsmcsX.crt*

e mova-o para uma pasta temporária no servidor ADS.

Etapa 2. Importar certificado WSM de servidores CVP para servidor ADS

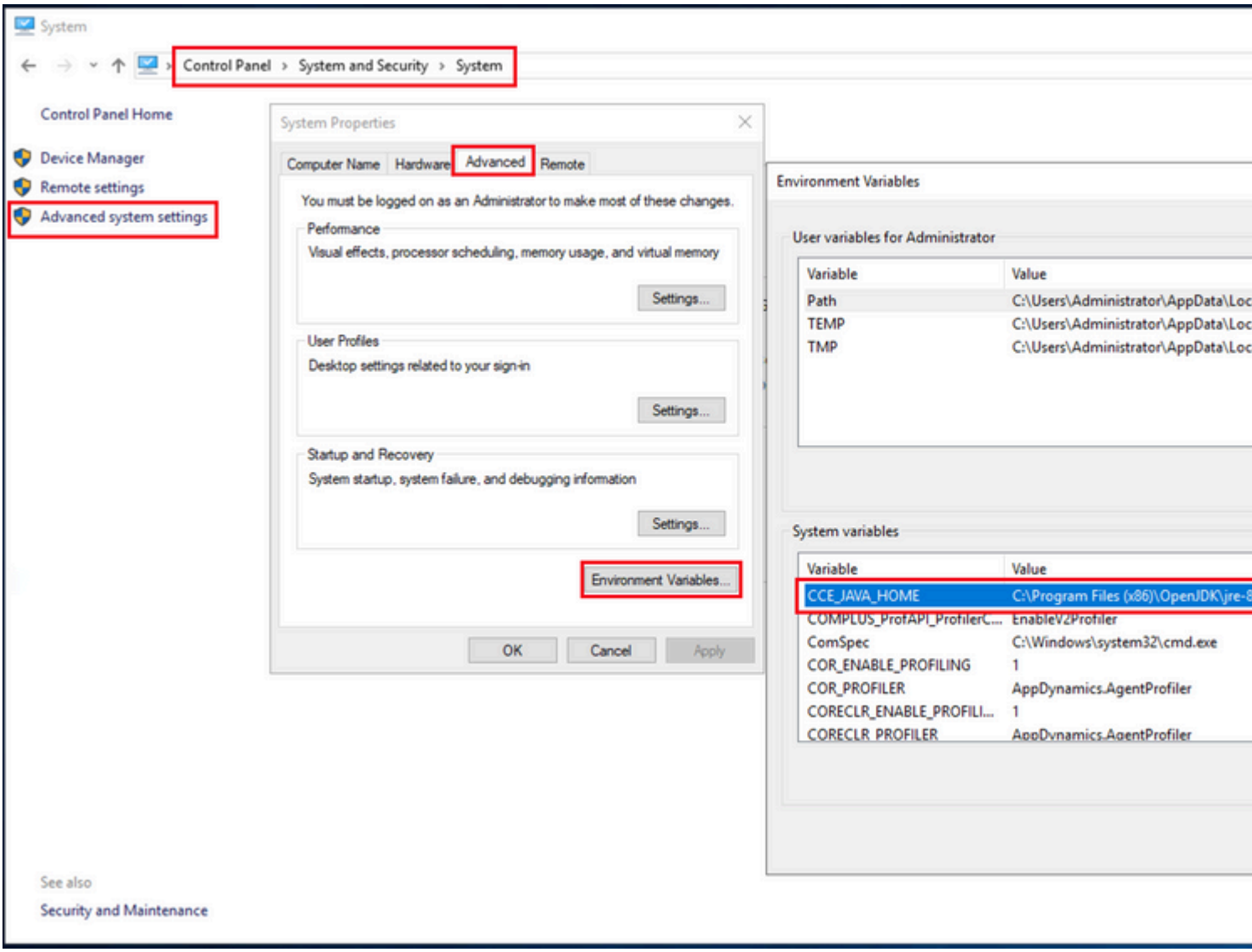
Para importar o certificado no servidor ADS, você precisa usar a ferramenta de chave, que faz parte do conjunto de ferramentas java. Há algumas maneiras de encontrar o caminho do home do java onde esta ferramenta está hospedada.

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



caminho de início de java

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



Variáveis de ambiente

No PCCE 12.6, o caminho padrão do OpenJDK é **C:\Program Arquivos (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin**

Comandos para importar os certificados autoassinados:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe -import -file C:\Temp\certs\wsmcsX.crt -alias <fqdn_of_CVP> -keystore <ICM install directory
```

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

(iii) 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 para a URL do servidor : **https://<servername>**.

(ii) Salve o certificado em uma pasta temporária, por exemplo: **c:\temp\certs** e nomeie o certificado como

```
keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias <fqdn_of_VOS> -keystore <ICM install
```

Reinicie o serviço Apache Tomcat nos servidores ADS.

Observação: execute a mesma tarefa em outros servidores ADS

Seção 3: Intercâmbio de certificados entre servidores Roggers , PG e ADS

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1: exportar o certificado IIS de servidores Rogger e PG

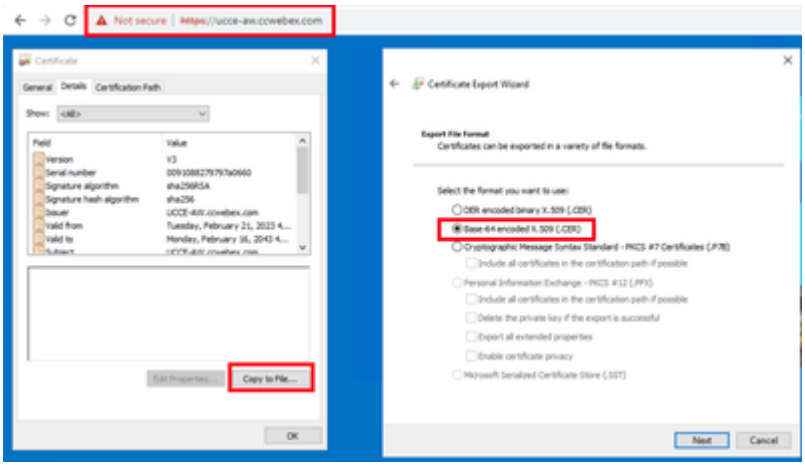
Etapa 2: Exportar o certificado DFP (Diagnostic Framework Portico) de servidores Rogger e PG

Etapa 3: Importar Certificados para Servidores ADS

Etapa 1. Exportar Certificado do IIS de Rogger e Servidores PG

(i) Em um servidor ADS a partir 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**



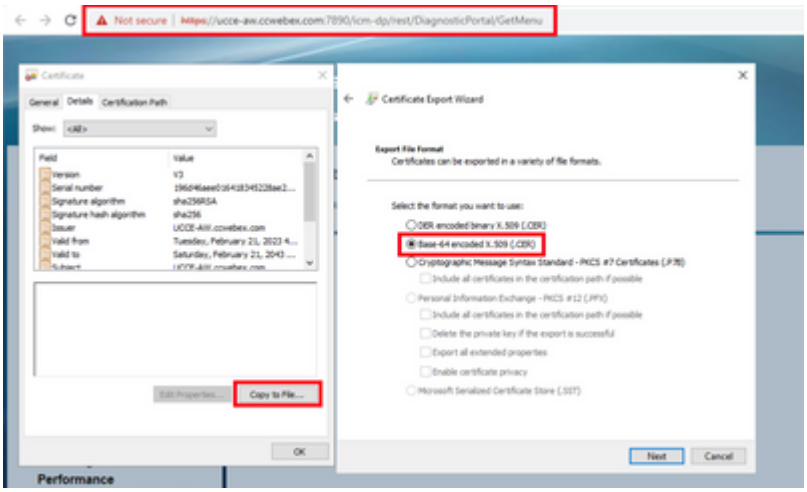
Exportar Certificado do IIS

Observação: 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



Exportar Certificado DFP

Observação: 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)\OpenJDK\jre-8.0.272.10-hotspot\bin.**

```
keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias <fqdn_of_server>_IIS -keystore <ICM inst
```

Observação: 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.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias <fqdn_of_server>_DFP -keystore <ICM inst
```

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

Reinicie o serviço Apache Tomcat nos servidores ADS.

Seção 4: 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 12.6(2) - 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 de administração do PCCE**
- **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 UCCE - UCCE 12.6**
- **Implementar certificados assinados por CA - CCE 12.6**
- **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.