

# Certificados com assinatura automática do Exchange em uma solução UCCE 12.6

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Procedimento](#)

[Servidores CCE AW e servidores de aplicativos principais CCE](#)

[Seção 1: Troca de certificados entre roteador/logger, PG e servidor AW](#)

[Seção 2: Intercâmbio de certificados entre aplicativos da plataforma VOS e o servidor AW](#)

[Servidor CVP OAMP e servidores de componentes CVP](#)

[Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios](#)

[Seção 2: Troca de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS](#)

[Seção 3: Troca de certificados entre o servidor CVP e os aplicativos da plataforma VOS](#)

[Integração do serviço Web CallStudio do CVP](#)

[Informações Relacionadas](#)

## Introdução

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

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE versão 12.6(2)
- Customer Voice Portal (CVP) versão 12.6(2)
- Cisco Virtualized Voice Browser (VVB)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VB 12.6(2)
- 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.

## Informações de Apoio

Na configuração da solução UCCE de novos recursos que envolvem aplicativos centrais, como Roggers, Gateways Periféricos (PG), Estações de Trabalho Administrativas (AW)/Servidor de Dados de Administração (ADS), Finesse, Cisco Unified Intelligent Center (CUIC) e assim por diante, é feito através da página de Administração do Contact Center Enterprise (CCE). Para aplicativos de Resposta de Voz Interativa (IVR - Interactive 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), toda a comunicação com o CCE Admin e o NOAMP é feita estritamente 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 é uma obrigação. 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

---

**Observação:** este documento se aplica SOMENTE ao CCE versão 12.6. Consulte a seção de informações relacionadas para obter links para outras versões.

---

## 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 o 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 de servidores AW.

As etapas necessárias para a troca eficaz de certificados autoassinados para o CCE estão divididas nessas 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 o certificado 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 um prompt de comando como Administrador.

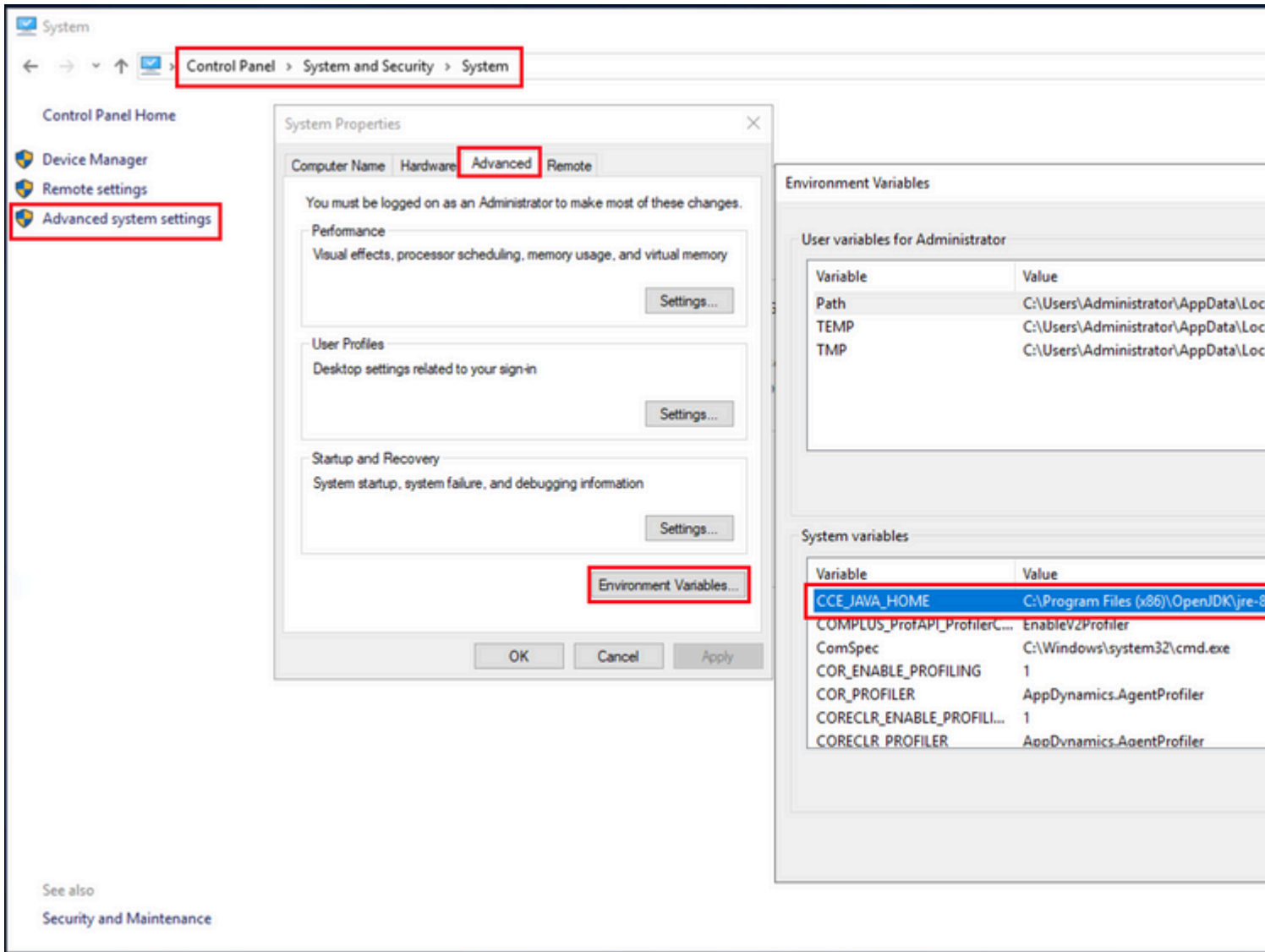
---

(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 %CCE\_JAVA\_HOME%**

```
C:\>echo %CCE_JAVA_HOME%  
C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
```

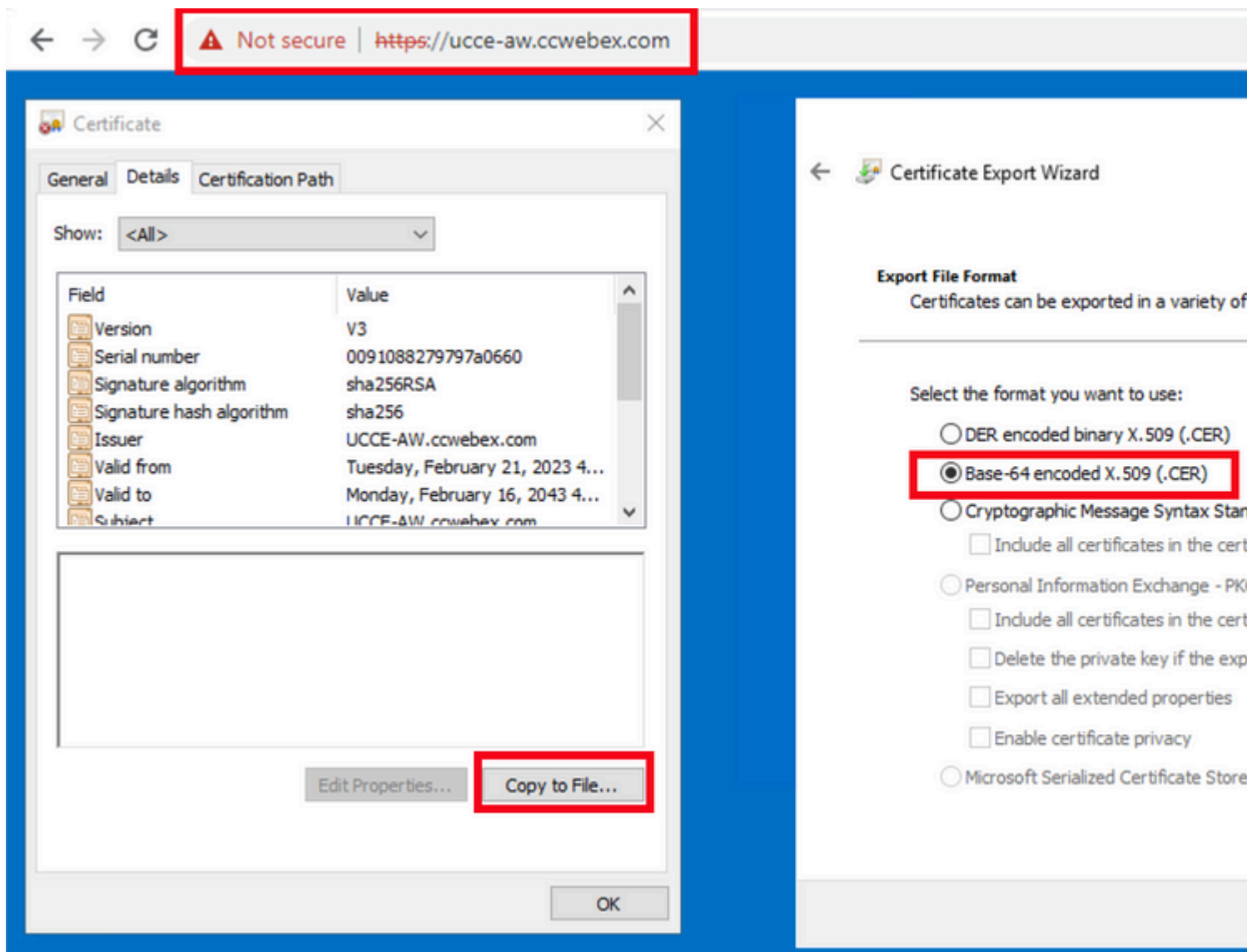
Opção 2: manualmente via configuração de sistema avançada, como mostrado na imagem



(ii) Faça backup do arquivo cacerts da pasta <diretório de instalação do ICM>ssl\ . Você pode copiá-lo para outro local.

Etapa 1. Exporte certificados do IIS de Roteador\Agente de Log, PG e todos os Servidores AW.

(i) No servidor AW 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`.

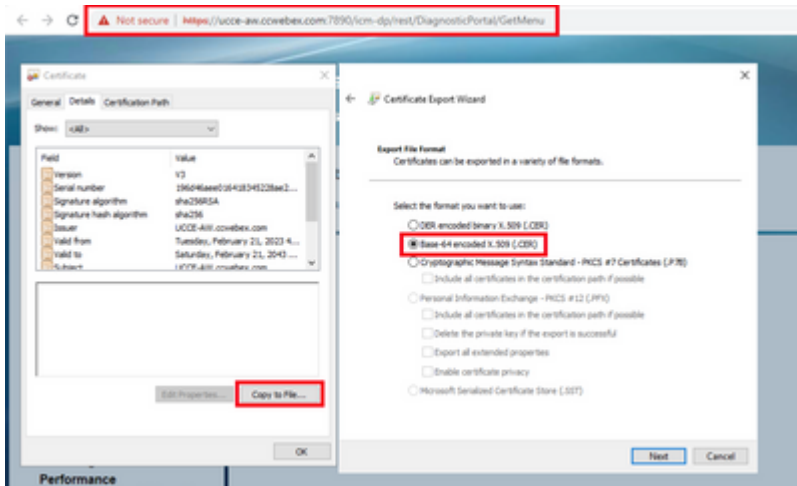
---

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

---

Etapa 2. Exporte 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) 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. Importe certificados IIS e DFP de Router\Logger, PG e AW para servidores AW.

Comando para importar os certificados autoassinados do IIS para o servidor AW. O caminho para executar a ferramenta de Chave: %CCE\_JAVA\_HOME%\bin:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

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

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

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystore
```

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

Reinicie o serviço Apache Tomcat nos servidores AW.

Etapa 4. Importe o certificado 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:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

**Observação:** importe todos os certificados do servidor AW IIS exportados para servidores Rogger 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:

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

Etapas 2. Importar certificados de aplicativos da plataforma VOS para o AW Server.

Esse processo é aplicável a aplicativos VOS, como:

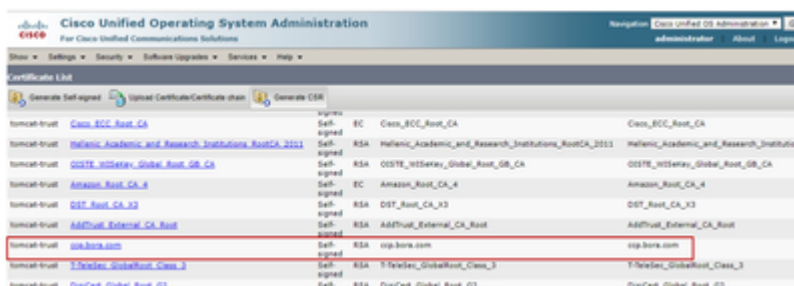
- Finesse
- CUIC \ LD \ IDS
- Conexão em nuvem

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

(i) Navegue até a página Cisco Unified Communications Operating System Administration:

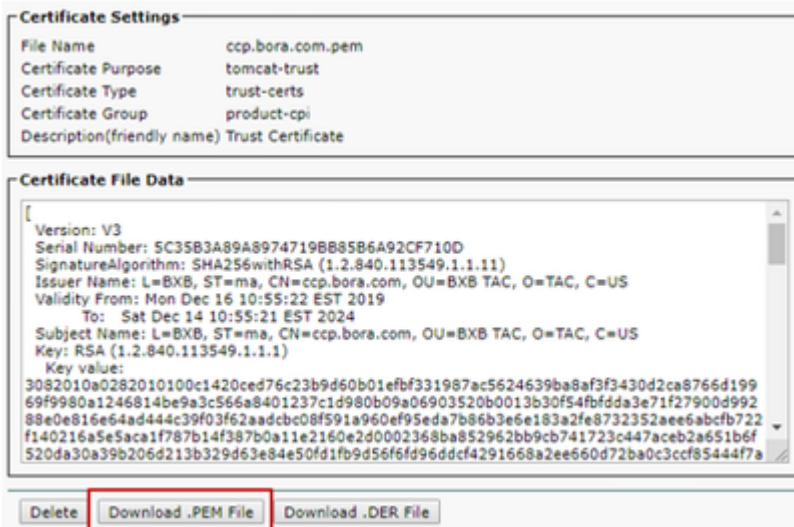
<https://FQDN:8443/cmplatform>.

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



tomcat-trust	Class	EC	Self-signed	Class
tomcat-trust	Class_ECC_Root_CA	EC	Self-signed	Class_ECC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	EC	Self-signed	Hellenic_Academic_and_Research_Institutions
tomcat-trust	OSITE_WISetKey_Global_Root_GB_CA	EC	Self-signed	OSITE_WISetKey_Global_Root_GB_CA
tomcat-trust	Amazon_Root_CA_4	EC	Self-signed	Amazon_Root_CA_4
tomcat-trust	DST_Root_CA_X3	EC	Self-signed	DST_Root_CA_X3
tomcat-trust	AddTrust_External_CA_Root	EC	Self-signed	AddTrust_External_CA_Root
tomcat-trust	ccp.bora.com	EC	Self-signed	ccp.bora.com
tomcat-trust	T-Trustee_GlobalRoot_Class_3	EC	Self-signed	T-Trustee_GlobalRoot_Class_3
tomcat-trust	DigCert_Global_Root_G2	EC	Self-signed	DigCert_Global_Root_G2

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



**Certificate Settings**

File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

**Certificate File Data**

```
Version: V3
Serial Number: 5C35B3A89A89747198B85B6A92CF710D
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Validity From: Mon Dec 16 10:55:22 EST 2019
To: Sat Dec 14 10:55:21 EST 2024
Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54bfdada3e71f27900d992
88e0e816e64ad44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1f9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Buttons: Delete, Download .PEM File, Download .DER File

---

**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: %CCE\_JAVA\_HOME%\bin

Comando para importar os certificados autoassinados:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -keystore C:\Temp\certs\keystore.jks  
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keystore C:\Temp\certs\keystore.jks
```

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 requer certificado de

- Plataforma Windows: certificado do Gerenciador de Serviços Web (WSM) do servidor CVP e dos servidores de Relatórios.
- Plataforma VOS: Cisco VVB e servidor Cloud Connect.

(ii) Servidores CVP: Este servidor requer certificado de

- Plataforma Windows: certificado WSM do servidor OAMP.
- Plataforma VOS: servidor Cloud Connect e servidor Cisco VB.

(iii) Servidores de relatórios do CVP: Este servidor requer certificado do

- Plataforma Windows: certificado WSM do servidor OAMP

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

- Plataforma Windows: certificado VXML do servidor CVP e certificado Callserver do servidor CVP
- Plataforma VOS: servidor Cloud Connect

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

Seção 3: Troca de certificados entre o servidor CVP e os aplicativos da plataforma VOS

### 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:

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

Etapas 2. Importe os certificados WSM do servidor CVP e do servidor de relatórios para o servidor OAMP.

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

---

**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**.
- 

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

(i) Exporte o certificado WSM de cada servidor CVP 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 -a
```

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

Etapas 2. Importe certificados WSM do servidor CVP e do servidor de relatórios para o servidor OAMP.

(i) Copie cada certificado WSM do servidor CVP e do 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 -a
```

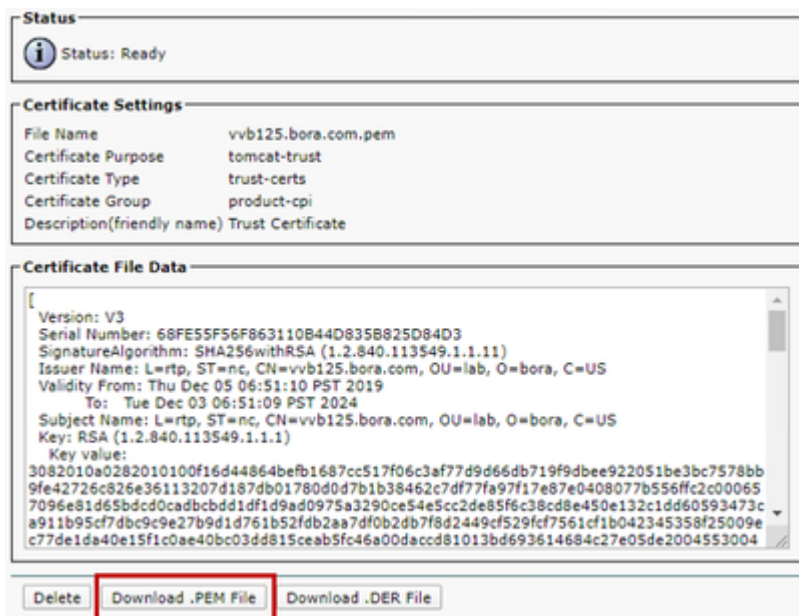
(iii) Reinicialize o servidor.

Etapas 3. Importe o certificado WSM do servidor OAMP do CVP para 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:





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 -a
```

- (ii) Reinicialize o servidor.

### Seção 3: Troca de certificados entre o servidor CVP e os aplicativos da plataforma VOS

Esta é uma etapa opcional para proteger a comunicação SIP entre o CVP e outros componentes do Contact Center. Para obter mais informações, consulte o 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 12.6\(2\) - 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 PCCE - PCCE 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.