# 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 Secvidor 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 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 - 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), 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%



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

Control Panel Home	and a system and second a system		
	System Properties ×		
Remote settings	Computer Name Hardware Advanced Remote	Environment Variables	
Advanced system settings	You must be logged on as an Administrator to make most of these changes. Performance Meral effects innocessor scheduling memory usage and virtual memory	User variables for Administrator	
	House encous, processor surrouning, memory usage, and theat memory	Variable	Value
	Settings	Path	C:\Users\Administrator\AppData\Lo
	User Profiles	TEMP	C:\Users\Administrator\AppData\Lo
	Desktop settings related to your sign-in	IMP	C:\Users\Administrator\AppData\Lo
	Startup and Recovery System startup, system failure, and debugging information		
	System startep, system railare, and debugging memorial		
	Settings	System variables	
	Settings	System variables Variable	Value
	Settings	System variables Variable CCE_JAVA_HOME	Value C:\Program Files (x86)\OpenJDK\jre-
	Settings	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC.	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler
	Settings  OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. COMSPEC	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe
	Settings  Christen Action of the Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler
	Settings  Environment Variables  OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProTAPI_ProTilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1
	Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 ApoDynamics.AgentProfiler
	Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AcoDynamics.AgentProfiler
	OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProtilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AppDynamics.AgentProfiler
	Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDynamics.AgentProfiler
	Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDynamics.AgentProfiler
See also	Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDvnamics.AgentProfiler

(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}.

General Details Certification Path		🗧 🌽 Certificate Export Wizard
Show: <all> Field Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Subject</all>	Value V3 0091088279797a0660 sha256RSA sha256 UCCE-AW.ccwebex.com Tuesday, February 21, 2023 4 Monday, February 16, 2043 4	Export File Format Certificates can be exported in a variety of Select the format you want to use: O DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Sta
Ec	lit Properties Copy to File OK	<ul> <li>Personal Information Exchange - Pi</li> <li>Indude all certificates in the cer</li> <li>Delete the private key if the ex</li> <li>Export all extended properties</li> <li>Enable certificate privacy</li> <li>Microsoft Serialized Certificate Store</li> </ul>

(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}\_DFF 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:

**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:

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 é aplicável a aplicativos VOS, como:

- Finesse
- $CUIC \setminus LD \setminus IDS$
- 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: <u>https://FQDN:8443/cmplatform</u>.

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

obode Cisco Unified Op Erstee For Cisco Unified Commun	erating System Administr interest Solutions	ation		Navigation Case Unified 03 Administration • Ga
Shou + Settings + Security + Suffici	n Uppades + Services + Help +			
Certificate List				
🔍 Cerende Self eigend 🐴 Viplaat Ce	Munie Centrum chan 🔒 Generalis (SR			
tomost-trust Case ECC Rest CA	Saft.	4C	Core_BCC_Anot_CA	Coox_BCC_Root_CA
toreat-trust (telenic Academic and )	tesearch institutions Root(A 2011 Self-	RSA.	Nelaric, Academic, and Jasearch, Institutions, RootCA, 201	1 Nelenic, Academic, and J.Research, Institution
torical-trust COSTE VICENEY Clubal	Aust GB_CA Self-	RSA.	01578_W15eKey_Globel_Root_GB_CA	00578_WDerkey_Global_Root_GB_CA
torecal-brust Amazon Root CA.4	545	a ac	Amazon_Root_CA_4	Amazon_Root_CA_4
tomost-trust 017 Aust CA X2	Sel-	RSA.	DST_ReeK_CA_K3	DST_Reet_CA_X3
toreat-trust Additud Edenal CA.R.	al Sel-	RSA.	AddTrust_External_CA_Root	AddTrust_External_CA_Root
tumcat-trust coalbora.com	Def-	AGA.	ogsbore.com	capitors.com
tomat-trust <u>Edular Galaftest Co</u>	un_3 Safe	ASA.	*TeleSec_GobaRoot_Class_3	T-felelet_GobaRoot_Case_3
Isoncal-Invol DisiCert Global Root G2	Self	854	DigiCet_Distal_Root_02	DipCert_Global_Root_62

(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 na	me) Trust Certificate		
Certificate File Data			
[ Version: V3 Serial Number: SC35 SignatureAlgorithm: Issuer Name: L=BX8 Validity From: Mon D To: Sat Dec 1 Subject Name: L=BX Key: RSA (1.2.840.1 Key value:	B3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) , ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US ec 16 10:55:22 EST 2019 4 10:55:21 EST 2024 B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 13549.1.1.1)		
3082010a0282010100 69f9980a1246814be9 88e0e816e64ad444c3 f140216a5e5aca1f787 520da30a39b206d213	lc1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 9f03f62aadcbc08f591a960ef95ed37b863be613a32f8e733352aee6abcfb722 b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a	•	
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} -ke Example: %CCE\_JAVA\_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keystop

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:

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

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 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.

Etapa 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 -al

(iii) Reinicialize o servidor.

Etapa 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:

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

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

Certificate Li					
Consulta	Self agreed 🖓 Upitaal Certificate/Certificate share 🔣 General	COR.			
		speed			
tomost-trust	thanks Pomary April DA - 60	supred	R5A	thavite_Primary_Root_CA60	thanks, Primary, Asid, CA, -, 60
tomost-trust	Subalive	Safe signed	6C	ClubalSign	Gidellign
tomost-trust	EE Certification Centre Aust. Ch	Saf-	RSA	EE_Detification_Derite_Root_CA	EE_Certification_Centre_Root_CA
tomost-trust	SisterSive Aust. CA	Salt- signed	854	GlobalSign_Root_CA	GlobalSign_Root_CA
tomost-trust	TRCA Real Carlification Authority	Self- signed	RSA	TWCA_Root_Certification_Authority	TeCA_Root_Certification_Authority
temost-trust	Burrana Casa 3 April Cit	Sall-	854	Buypens_Cees_3_Root_GA	Bogana_Cana_3_Root_CA
tomost-trust	Refeit Service Aust Certificate Authority - 62	Saf-	R5A	Danfald_Services_Root_Certificate_AuthorityG2	Barfald_Benios_Root_Certificate_Authority62
tempet-trust	Verbier, Case 3. Public Arinary, Cathlation, Authority, J	545	854	tention_Cess_3_Public_Primary_Centification_Authority	Verdign_Class_3_Public_Primary_Certification_Authority
formulat trust	wkills.box.com	Salt-	854	million term	veb128.box.com
formost-trust	Many Dolal Carlination Autority	Dail-	854	Kamp_Gobal_Certification_Authority	Many_Unite_Certification_Authority

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

Status	
i Status: Ready	
Certificate Settings-	
File Name	vvb125.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly na	me) Trust Certificate
certificate File Data	
1	
Version: V3	
Serial Number: 68FE	55F56F863110B44D835B825D84D3
SignatureAlgorithm:	SHA256withRSA (1.2.840.113549.1.1.11)
Validity From: Thu Dr	51=nc, CN=VVD125.bora.com, OU=iab, O=bora, C=U5
To: Tue Dec 0	3 06:51:09 PST 2024
Subject Name: L=rtp	, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.1)	13549.1.1.1)
Key value:	
9fe42726c826e361132	716044864060168/cc51/f06c38f//d906600/19f900669220510630c/5/800
7096e81d65bdcd0cad	bcbdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27	b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae	40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004
Delete Download .	PEM File Download .DER File

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 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: <u>Guia de configuração do</u> <u>CVP - Segurança</u>.

#### 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 <u>Guia do usuário do Cisco Unified CVP VXML Server e do Cisco Unified Call Studio Release</u> 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
- <u>Certificados com assinatura automática do Exchange PCCE PCCE 12.5</u>
- <u>Certificados com assinatura automática do Exchange UCCE UCCE 12.5</u>
- 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.