Échanger des certificats auto-signés dans une solution UCCE 12.6

Table des matières

Introduction Conditions préalables **Exigences** Composants utilisés Informations générales **Procédure** Serveurs CCE AW et serveurs d'applications de base CCE Section 1 : échange de certificats entre le routeur/enregistreur, le PG et le serveur AW Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur AW Serveur CVP OAMP et serveurs de composants CVP Section 1 : Échange de certificats entre le serveur CVP OAMP et le serveur CVP et les serveurs de rapports Section 2 : Échange de certificats entre le serveur CVP OAMP et les applications de la plateforme VOS Section 3 : Échange de certificats entre le serveur CVP et les applications de la plate-forme VOS Intégration du service Web CVP CallStudio Informations connexes

Introduction

Ce document décrit comment échanger des certificats auto-signés dans une solution Unified Contact Center Enterprise (UCCE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCCE version 12.6(2)
- Customer Voice Portal (CVP) version 12.6(2)
- Navigateur vocal virtualisé Cisco (VVB)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VB 12.6(2)
- Console des opérations CVP (OAMP)
- CVP New OAMP (NOAMP)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans la solution UCCE, la configuration des nouvelles fonctionnalités impliquant des applications principales telles que Rogers, Peripheral Gateways (PG), Admin Workstations (AW)/ Administration Data Server (ADS), Finesse, Cisco Unified Intelligence Center (CUIC), etc., s'effectue via la page d'administration Contact Center Enterprise (CCE). Pour les applications de réponse vocale interactive (IVR) telles que CVP, Cisco VVB et les passerelles, NOAMP contrôle la configuration des nouvelles fonctionnalités. À partir de CCE 12.5(1), en raison de la conformité à la gestion de la sécurité (SRC), toutes les communications vers CCE Admin et NOAMP sont strictement effectuées via le protocole HTTP sécurisé.

Pour assurer une communication sécurisée et transparente entre ces applications dans un environnement de certificats auto-signés, l'échange de certificats entre les serveurs est indispensable. La section suivante explique en détail les étapes nécessaires pour échanger un certificat auto-signé entre :

- Serveurs CCE AW et serveurs d'applications de base CCE
- Serveur CVP OAMP et serveurs de composants CVP

Remarque : ce document s'applique UNIQUEMENT à la version 12.6 du CCE. Consultez la section Informations connexes pour obtenir des liens vers d'autres versions.

Procédure

Serveurs CCE AW et serveurs d'applications de base CCE

Il s'agit des composants à partir desquels les certificats auto-signés sont exportés et des composants dans lesquels les certificats auto-signés doivent être importés.

Serveurs CCE AW : ce serveur requiert un certificat de :

 Plate-forme Windows : Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B} et tous les AW/ADS.

Remarque : IIS et le protocole DFP (Diagnostic Framework Portico) sont nécessaires.

 Plate-forme VOS : Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect et d'autres serveurs applicables faisant partie de la base de données d'inventaire. Il en va de même pour les autres serveurs AW de la solution.

Router \ Logger Server : ce serveur requiert un certificat de :

• Plate-forme Windows : certificat IIS de tous les serveurs AW.

Les étapes nécessaires à l'échange efficace des certificats auto-signés pour CCE sont divisées en ces sections.

Section 1 : échange de certificats entre le routeur/enregistreur, le PG et le serveur AW Section 2 : Échange de certificats entre l'application de la plate-forme VOS et le serveur AW

Section 1 : échange de certificats entre le routeur/enregistreur, le PG et le serveur AW

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exportez les certificats IIS depuis Router\Logger, PG et tous les serveurs AW. Étape 2. Exportez les certificats DFP depuis Router\Logger, PG et tous les serveurs AW. Étape 3. Importez des certificats IIS et DFP depuis Router\Logger, PG et AW vers des serveurs AW.

Étape 4. Importez le certificat IIS dans Router\Logger et PG à partir des serveurs AW.

Attention : avant de commencer, vous devez sauvegarder la banque de clés et ouvrir une invite de commandes en tant qu'administrateur.

(i) Connaître le chemin d'accès au répertoire d'origine Java pour savoir où l'outil de saisie Java est hébergé. Il existe plusieurs façons de trouver le chemin d'accès java.

Option 1 : commande CLI : echo %CCE_JAVA_HOME%

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

Option 2 : manuellement via le paramètre système avancé, comme illustré dans l'image

x A 🔽 x Control Da	nel > Surtem and Security > Surtem			Search Control Danel
control Pa	nei > System and Security > System		• 0	Search Control Pariel
ntrol Panel Home	System Properties ×	1		
rice Manager	Computer Name Hardware Advanced Remote			
note settings	You must be logged on as an Administrator to make most of these changes.	Environment Variables		
vanced system settings	Performance	User variables for Administrator		
	Visual effects, processor scheduling, memory usage, and virtual memory	Variable	Value	
	Settings	Path	C:\Users\Administrator\AppData\Local\Microsoft\WindowsAp	ps;
	User Profiles	TEMP	C:\Users\Administrator\AppData\Local\Temp	
	Desktop settings related to your sign-in	1 IMP	C:\Users\Administrator\AppUata\Local\Temp	
	Settings	1		
	Startup and Recovery	1		
	System startup, system failure, and debugging information		New	Edit Delete
	Settings	System variables		
	Environment Variables	Variable	Value	
	Civitoniles, valiables	CCE_JAVA_HOME	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot	
	OK Court Inte	COMPLUS_ProtAPI_ProfilerC	C:\Windows\system32\cmd.exe	
	OK Cancel Apply	COR_ENABLE_PROFILING	1	
		COR_PROFILER CORECLE ENABLE PROFILI	AppDynamics.AgentProfiler 1	
		CORECLR PROFILER	AppDvnamics.AgentProfiler	
			New	Edit Delete
				OK Cancel

(ii) Sauvegardez le fichier cacerts à partir du dossier <ICM install directory>ssl\ . Vous pouvez le copier à un autre emplacement.

Étape 1. Exportez les certificats IIS depuis Router\Logger, PG et tous les serveurs AW.

(i) Sur un serveur AW à partir d'un navigateur, accédez à l'URL des serveurs (Rogers, PG, autres serveurs AW) : https://{servername}.

← → C ▲ Not secure https://ucce-aw.ccwebex.com	
General Details Certification Path Show: <all> Field Value V3 Value V3 Value V3 V</all>	 Export File Format Certificates can be exported in a variety of file formats.
Serial number 009108327979780660 Signature algorithm sha256RSA Signature hash algorithm sha256 Issuer UCCE-AW.ccwebex.com Valid from Tuesday, February 21, 2023 4 Valid to Monday, February 16, 2043 4	Select the format you want to use: DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties
Edit Properties Copy to File	Enable certificate privacy Microsoft Serialized Certificate Store (.SST)
ОК	Next Cancel

(ii) Enregistrez le certificat dans un dossier temporaire. Par exemple, c:\temp\certs et nommez le certificat ICM{svr}[ab].cer.

Remarque : sélectionnez l'option X.509 codé en base 64 (.CER).

Étape 2. Exportez les certificats DFP depuis Router\Logger, PG et tous les serveurs AW.

(i) Sur le serveur AW, ouvrez un navigateur et accédez aux serveurs (Router, Logger ou Rogers, PGs) URL DFP : https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.

erenal Details Certificatio	245	×	← JP Cetificate Depot Ward
Pheid value Peid value Senal number 216 Sgreture algorithm she Signature hash algorithm she	Value V3 294644ase00044003402 sha2885A sha2865A UC02-AW conebex.com Tuesday, Pebruary 21, Saturday, Pebruary 21, Saturday, Pebruary 21, Saturday, Pebruary 21, Saturday, Pebruary 21,	21442 2123 4 2040	Select the format you want to use: ODDI encoded theory 3, 509 (CDD) ODDI encoded 15.009 (CDD) ODDI encoded 15.009 (CDD) ODDI protographic Message Syntax Standard - MCS #7 Certificates (JP.76) ODDI certificates in the certificates peth if possible
	Edit Properties	ox to File	Presonal Information Exchange - PRCS #12 (JPR) Delete the private key if the export is successful Deport all extended properties Defect private key (Strip) Morsonit Serialized Certificate Store (Strip)

(ii) Enregistrez le certificat dans le dossier exemple c:\temp\certs et nommez le certificat dfp{svr}[ab].cer

Remarque : sélectionnez l'option X.509 codé en base 64 (.CER).

Étape 3. Importez des certificats IIS et DFP depuis Router\Logger, PG et AW vers des serveurs AW.

Commande pour importer les certificats auto-signés IIS dans le serveur AW. Chemin d'exécution de l'outil Clé : %CCE_JAVA_HOME%\bin :

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

Remarque : importez tous les certificats de serveur exportés vers tous les serveurs AW.

Commande pour importer les certificats autosignés DFP dans les serveurs AW :

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

Remarque : importez tous les certificats de serveur exportés vers tous les serveurs AW.

Redémarrez le service Apache Tomcat sur les serveurs AW.

Étape 4. Importez le certificat IIS dans Router\Logger et PG à partir des serveurs AW.

Commande pour importer les certificats auto-signés IIS AW dans les serveurs Router\Logger et PG :

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

Remarque : importez tous les certificats de serveur IIS AW exportés vers les serveurs Rogger et PG sur les côtés A et B.

Redémarrez le service Apache Tomcat sur les serveurs Router\Logger et PG.

Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur AW

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS. Étape 2. Importez les certificats d'application de la plate-forme VOS sur le serveur AW.

Ce processus s'applique aux applications VOS telles que :

- Finesse
- CUIC \ LD \ IDS
- Connexion au cloud

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

(i) Accédez à la page Cisco Unified Communications Operating System Administration : <u>https://FQDN:8443/cmplatform</u>. (ii) Accédez à Security > Certificate Management et recherchez les certificats du serveur principal d'application dans le dossier tomcat-trust.

61560	Cisco Unified Operating System Admir or Cisco Unified Communications Solutions	vistrat	ion		Navigation Com Unifed (1) Administration • 30 administration About Legen
Show will be the	ngs + Security + Bollican Upgrades + Security + Halp +				
Cartilicate Li	AN CONTRACTOR OF CONTRACTOR				
Constanting of the second	Satayool 🍙 Upical Cothesis Cothesis dan 渡 Gorovits	054			
tomat-front	Case BCC Rest. CA	Self- septed	80	Cecs, BCC, Aud., CA	Coco_ECC_Root_CA
tomat-trust	Infanic Academic and Research Institutions Root24, 2023	Self-	858	Helenic, Academic, and Jasearch, Institutions, RootCA, 201	1 Helenic, Academic, and Jassanch, Institutio
tomat-trust	OTSTE WIDEKEY, Shibel Aust, GB, CA	Salt- appeal	858	00578_W05exex_Globel_Root_GB_CA	01175_WISHINY_Global_Root_GB_CA
torecal-trust	Amazon, Root, CA. 4	Self- append	00	Amazon_Root_CA_4	Amazon, Rook, CA, 4
torn addressed	DIT Red CA X3	Self-	858	DST_ReeK_CA_X3	0.07_Reet_CA_X3
tomat-trust	Additude Deternal CA. Read	Self- pared	834	AddTrust_External_CA_Root	AddTrust_Enternal_CA_Root
tomat-trust	ostorum	Dell- signed	104	02.30%.00%	esp.hore.com
tomat trust	Effected Galacters Case 3	Safe agreed	134	Meider_GulaRot_Cost_3	T-Neisler_GobaRoot_Cass_3
toward front.	DisiCert Outer Root 62	Set	104	DipiCert_Distral_Root_02	DipiCert_Global_Root_G2

(iii) Sélectionnez le certificat et cliquez sur télécharger le fichier .PEM pour l'enregistrer dans un dossier temporaire sur le serveur AW.

۲(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
Caral Numbers 5/250240040074710000505403/67100
Seual infludel: 3r33D3v0Av0Av4/1ADD03D0vA5rL/1nh
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
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a

Delete

Download .PEM File

Download .DER File

Remarque : effectuez les mêmes étapes pour l'abonné.

Étape 2. Importez l'application de plate-forme VOS sur le serveur AW.

Chemin d'exécution de l'outil Clé : %CCE_JAVA_HOME%\bin

Commande pour importer les certificats auto-signés :

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

Redémarrez le service Apache Tomcat sur les serveurs AW.

Remarque : effectuez la même tâche sur d'autres serveurs AW.

Serveur CVP OAMP et serveurs de composants CVP

Il s'agit des composants à partir desquels les certificats auto-signés sont exportés et des composants dans lesquels les certificats auto-signés doivent être importés.

(i) Serveur CVP OAMP : ce serveur requiert un certificat de

- Plate-forme Windows : certificat WSM (Web Services Manager) du serveur CVP et des serveurs de rapports.
- Plate-forme VOS : serveur Cisco VVB et Cloud Connect.

(ii) Serveurs CVP : ce serveur requiert un certificat de

- Plate-forme Windows : certificat WSM du serveur OAMP.
- Plate-forme VOS : serveur Cloud Connect et serveur Cisco VVB.

(iii) Serveurs CVP Reporting : ce serveur requiert un certificat de

• Plate-forme Windows : certificat WSM du serveur OAMP

(iv) Serveurs Cisco VVB : ce serveur requiert un certificat de

- Plate-forme Windows : certificat VXML du serveur CVP et certificat Callserver du serveur CVP
- Plate-forme VOS : serveur Cloud Connect

Les étapes nécessaires à l'échange efficace des certificats auto-signés dans l'environnement CVP sont expliquées dans ces trois sections.

Section 1 : Échange de certificats entre le serveur CVP OAMP et le serveur CVP et les serveurs de rapports

Section 2 : Échange de certificats entre le serveur CVP OAMP et les applications de la plateforme VOS

Section 3 : Échange de certificats entre le serveur CVP et les applications de la plate-forme VOS

Section 1 : Échange de certificats entre le serveur CVP OAMP et le serveur CVP et les serveurs de rapports

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exportez le certificat WSM à partir du serveur CVP, du serveur Reporting et du serveur OAMP.

Étape 2. Importez les certificats WSM du serveur CVP et du serveur de rapports dans le serveur OAMP.

Étape 3. Importez le certificat WSM du serveur CVP OAMP dans les serveurs CVP et les serveurs de rapports.

Attention : avant de commencer, vous devez procéder comme suit :

1. Ouvrez une fenêtre de commande en tant qu'administrateur.

2. Pour la version 12.6.2, pour identifier le mot de passe de la banque de clés, accédez au dossier %CVP_HOME%\bin et exécutez le fichier DecryptKeystoreUtil.bat.

3. Pour la version 12.6.1, pour identifier le mot de passe de la banque de clés, exécutez la commande more %CVP_HOME%\conf\security.properties.

4. Vous avez besoin de ce mot de passe lorsque vous exécutez les commandes keytool.

5. À partir du répertoire %CVP_HOME%\conf\security\, exécutez la commande copy .keystore backup.keystore.

Étape 1. Exportez le certificat WSM depuis CVP Server, Reporting et OAMP Server.

(i) Exportez le certificat WSM de chaque serveur CVP vers un emplacement temporaire et renommez le certificat avec le nom souhaité. Vous pouvez le renommer wsmX.crt. Remplacez X par le nom d'hôte du serveur. Par exemple, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmamp.crt.

Commande pour exporter les certificats auto-signés :

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

(ii) Copiez le certificat à partir du chemin d'accès %CVP_HOME%\conf\security\wsm.crt à partir de chaque serveur et renommez-le wsmX.crt en fonction du type de serveur.

Étape 2. Importez les certificats WSM du serveur CVP et du serveur de rapports dans le serveur OAMP.

(i) Copiez chaque certificat WSM du serveur CVP et du serveur Reporting (wsmX.crt) dans le répertoire %CVP_HOME%\conf\security du serveur OAMP.

(ii) Importez ces certificats avec la commande suivante :

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

(iii) Redémarrez le serveur.

Étape 3. Importez le certificat WSM du serveur CVP OAMP dans les serveurs CVP et les serveurs de rapports.

(i) Copiez le certificat WSM du serveur OAMP (wsmoampX.crt) dans le répertoire %CVP_HOME%\conf\security sur tous les serveurs CVP et les serveurs de rapports.

(ii) Importez les certificats avec la commande suivante :

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

(iii) Redémarrez les serveurs.

Section 2 : Échange de certificats entre le serveur CVP OAMP et les applications de la plateforme VOS

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exportez le certificat d'application depuis la plate-forme VOS.

Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

Ce processus s'applique aux applications VOS telles que :

- CUCM
- VVB
- · Connexion au cloud

Étape 1. Exportez le certificat d'application depuis la plate-forme VOS.

(i) Accédez à la page Cisco Unified Communications Operating System Administration : <u>https://FQDN:8443/cmplatform</u>.

(ii) Accédez à Security > Certificate Management et recherchez les certificats du serveur principal de l'application dans le dossier tomcat-trust.

Certificate L	int .				
Consulta	Self agreed 🖓 Upsaid CarlinderCarlinder states 🔍 Caracea	CDR.			
		sugard.			
Isomout-Invest	theate Atimes, Root, CA 62	Sect.	R5A	Dante, himery, Aust, 64, - ,63	thanks, Primary, Root, CA, -, 60
formulati finanti	SubaSie	Self- signed	80	CisterSign	GibeSiph
tempet-trust	EE Certification Centre Aust. Ch	Self-	854	EE_Dertification_Dertins_Root_CA	BE_Certification_Centre_Asst_CA
tempet trust	StateSize.Aut.Ol	Safe agenation	854	Gisba/Sign_Root_CA	Side/Spr_Rot_CA
tomost-trust	TIGA And Californias Autority	Self-	8.54	TerCA_Root_Certification_Authority	TitlCA_Root_Continues_Authority
tempet-trust	Bernann Cana 3 April 48	Self-	854	Bergana, Casa, 3, Root, GA	Becques, Cam, 3, Reet, CA
formulation and	Statistic Services Aust. Cartificate: Authority - 52	Self-	834	Disefeld_Services_Root_Certificate_Authority_~_52	Stanfant_Services_Root_Certificate_AuthorityG2
tempet-trust	Verbier, Case 3, Public Arinary, Cathleston, Autority, a	545	154	terdige, Cess, 3, Adric, Primary, Certification, Authority,	Verlöge, Dass, 3, Public, Primary, Carthoption, Authority,
tomost towat	whith how can	Safe algorith	8.54	unitizationa.com	weille how.com
Internal local	Allama Clubal Carbfration Authority	Sec.	1.24	Many_Cole_Certification_Authority	XRamp_Criter_Certification_Actionty

(iii) Sélectionnez le certificat et cliquez sur télécharger le fichier .PEM pour l'enregistrer dans un dossier temporaire sur le serveur 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	
(Version: V3 Serial Number: 68FE SignatureAlgorithm:	55F56F863110B44D835B825D84D3 SH4256with854 (1,2,840,113549,1,1,11)	-
Issuer Name: L=rtp,	ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US	
Validity From: Thu D	ec 05 06:51:10 PST 2019	
Subject Name: L=rts Key: RSA (1.2.840.1), ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US 13549.1.1.1)	
3082010a0282010100)f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb	
9fe42726c826e36113	207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065	
7096e81d65bdcd0cad	bcbdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c /hgd1d761h53fdh3aa7df0h3dh7f8d34dqrf53gfrf7561rf1h0d3345358f35000r	Ŧ
c77de1da40e15f1c0ae	40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004	1

Delete

Download .PEM File

Download .DER File

Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

(i) Copiez le certificat VOS dans le répertoire %CVP_HOME%\conf\security du serveur OAMP.

(ii) Importez les certificats avec la commande suivante :

(ii) Redémarrer le serveur.

Section 3 : Échange de certificats entre le serveur CVP et les applications de la plate-forme VOS

Il s'agit d'une étape facultative pour sécuriser la communication SIP entre CVP et d'autres composants du centre de contact. Pour plus d'informations, reportez-vous au Guide de configuration CVP - <u>Sécurité</u>.

Intégration du service Web CVP CallStudio

Pour obtenir des informations détaillées sur l'établissement d'une communication sécurisée pour les éléments Web Services et Rest_Client

reportez-vous au <u>Guide de l'utilisateur de Cisco Unified CVP VXML Server et de Cisco Unified Call</u> <u>Studio version 12.6(2) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco</u>

Informations connexes

- Guide de configuration CVP Sécurité
- Guide de sécurité UCCE
- Guide d'administration PCCE
- <u>Certificats autosignés PCCE Exchange PCCE 12.5</u>
- <u>Certificats auto-signés UCCE Exchange UCCE 12.5</u>
- <u>Certificats autosignés PCCE Exchange PCCE 12.6</u>
- Implémenter des certificats signés par une autorité de certification CCE 12.6
- Exchange Certificates with Contact Center Uploader Tool
- <u>Assistance et documentation techniques Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.