# PCCE 12.6ソリューションでの自己署名証明書の交換

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
背景
<u></u> 手順
ーンコート ヤクション1・CVPサーバとADSサーバ間の証明書の交換
<u> ステップ1:CVPサーバ証明書のエクスポート</u>
ー ステップ2:CVPサーバのWSM証明書のADSサーバへのインポート
<u>ステップ 3:ADSサーバー証明書のエクスポート</u>
<u>ステップ4:CVPサーバおよびレポーティングサーバへのADSサーバ証明書のインポート</u>
<u>セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書の交換</u>
<u> ステップ1:VOSプラットフォームアプリケーションサーバ証明書のエクスポート</u>
<u>ステップ2:VOSプラットフォームアプリケーション証明書のADSサーバへのインポート</u>
<u>ステップ 3:CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のイン</u> <u>ポート</u>
<u>セクション3:Rogger、PG、およびADSサーバ間での証明書の交換</u>
<u>ステップ1:RoggerサーバとPGサーバからのIIS証明書のエクスポート</u>
<u>ステップ2:RoggerサーバとPGサーバからのDFP証明書のエクスポート</u>
<u>ステップ 3:ADSサーバへの証明書のインポート</u>
<u>ステップ4:RoggerサーバとPGサーバへのADS証明書のインポート</u>
<u>セクション4:CVP CallStudio Webサービスの統合</u>
関連情報

# はじめに

このドキュメントでは、Cisco Packaged Contact Center Enterprise(PCCE)ソリューションで自己 署名証明書(SSC)を交換する方法について説明します。

# 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

- PCCEリリース12.6(2)
- ・ Customer Voice Portal(CVP)リリース12.6(2)
- Virtualized Voice Browser(VVB)12.6(2)
- ・ 管理ワークステーション(AW)/管理日付サーバ(AW/ADS)12.6(2)

- Cisco Unified Intelligenceサーバ(CUIC)
- ・ カスタマーコラボレーションプラットフォーム(CCP)12.6(2)
- エンタープライズチャットおよび電子メール(ECE)12.6(2)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- PCCE 12.6(2)
- CVP 12.6(2)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

#### 背景

12.x以降のPCCEソリューションでは、すべてのデバイスがプリンシパルAWサーバでホストされ るSingle Pane of Glass(SPOG)を介して制御されます。PCCE 12.5(1)バージョンのsecuritymanagement-compliance(SRC)により、ソリューション内のSPOGと他のサーバ間のすべての通 信は、セキュアHTTPプロトコルを使用して厳密に行われます。

証明書は、SPOGとその他のデバイス間でシームレスで安全な通信を実現するために使用されま す。自己署名証明書の環境では、サーバ間の証明書交換が必須です。

#### 手順

これらは、自己署名証明書のエクスポート元のコンポーネントと、自己署名証明書のインポート 先のコンポーネントです。

(i)すべてのAW/ADSサーバ:これらのサーバには次の証明書が必要です。

- Windowsプラットフォーム:
  - ICM:Router and Logger(Rogger){A/B}、ペリフェラルゲートウェイ(PG){A/B}、すべてのAW/ADS、およびECEサーバ。

💊 注:IISと診断フレームワークポート(DFP)が必要です。

- 。CVP:CVPサーバ、CVPレポートサーバ。
  - ✤ 注:すべてのサーバからのWebサービス管理(WSM)証明書が必要です。証明書 は完全修飾ドメイン名(FQDN)で指定する必要があります。
- VOSプラットフォーム: Cloud Connect、Cisco Virtualized Voice Browser(VVB)、Cisco Unified Communication Manager(CUCM)、Finesse、Cisco Unified Intelligence

Center(CUIC)、ライブデータ(LD)、アイデンティティサーバ(IDS)、およびその他の該当するサーバ。

(ii) Router \ Logger Servers:これらのサーバには次の証明書が必要です。

• Windowsプラットフォーム:すべてのAW/ADSサーバはIIS証明書です。

(iii)PGサーバ:次の証明書が必要なサーバです。

- Windowsプラットフォーム:すべてのAW/ADSサーバはIIS証明書です。
- VOSプラットフォーム: CUCMパブリッシャ(CUCM PGサーバのみ)、Cloud Connectお よびCCP(MR PGサーバのみ)。

💊 注:これは、CUCMサーバからJTAPIクライアントをダウンロードするために必要です。

(iv) CVPサーバ:このサーバには、次の証明書が必要です。

- Windowsプラットフォーム:すべてのADSサーバーIIS証明書
- VOSプラットフォーム: Cloud Connectサーバ、VVBサーバ

(v) CVPレポーティングサーバ:このサーバには、次のURLの証明書が必要です。

• Windowsプラットフォーム:すべてのADSサーバーIIS証明書

(vi) VVBサーバ:このサーバには次の証明書が必要です。

- Windowsプラットフォーム:すべてのADSサーバがIIS証明書、CVPサーバからのVXML証 明書、およびCVPサーバからのCallserver証明書
- VOSプラットフォーム: Cloud Connectサーバ

ソリューション内の自己署名証明書を効果的に交換するために必要な手順は、3つのセクションに 分かれています。

セクション1:CVPサーバとADSサーバ間での証明書の交換。

セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書交換。

セクション3:Rogger、PG、およびADSサーバ間での証明書の交換。

セクション1:CVPサーバとADSサーバ間の証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ1:CVPサーバのWSM証明書のエクスポート

- ステップ2:CVPサーバのWSM証明書をADSサーバにインポートします。
- ステップ3: ADSサーバー証明書をエクスポートします。

ステップ4:ADSサーバをCVPサーバおよびCVPレポーティングサーバにインポートします。

ステップ1:CVPサーバ証明書のエクスポート

CVPサーバから証明書をエクスポートする前に、サーバのFQDNで証明書を再生成する必要があります。そうしないと、Smart Licensing、Virtual Agent Voice(VAV)、およびSPOGとのCVP同期などのいくつかの機能で問題が発生する場合があります。

 注意:作業を開始する前に、次の操作を行う必要があります。
 1.管理者としてコマンド・ウィンドウを開きます。
 2.12.6.2の場合、キーストアパスワードを識別するには、%CVP\_HOME%\binフォルダに移動し、DecryptKeystoreUtil.batファイルを実行します。
 3.12.6.1の場合、キーストアパスワードを識別するには、more %CVP\_HOME%\conf\security.propertiesコマンドを実行します。
 4. このパスワードは、keytoolコマンドを実行するときに必要です。
 5. %CVP\_HOME%\conf\security\ディレクトリから、copy .keystore backup.keystoreコマンドを実行します。

注:このドキュメントで使用するコマンドは、keytoolパラメータ – storepassを使用して合 理化できます。すべてのCVPサーバについて、識別したkeytoolパスワードを入力します。 ADSサーバのデフォルトパスワードはchangeitです。

CVPサーバで証明書を再生成するには、次の手順を実行します。

(i)サーバ内の証明書を一覧表示する

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore list

◇ 注:CVPサーバには、wsm\_certificate、vxml\_certificate、callserver\_certificateの自己署名証 明書があります。keytoolのパラメータ – vを使用すると、各証明書の詳細情報を確認できま す。また、keytool.exe listコマンドの最後に「>」記号を追加して、出力をテキストファイ ルに送信できます(例: > test.txt)。

二旧自己署名証明書の削除

CVPサーバ:自己署名証明書を削除するコマンド

%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 CVP Reportingサーバ:自己署名証明書を削除するコマンド:

%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

◆ 注:CVPレポーティングサーバには、wsm\_certificate、callserver\_certificateという自己署名 証明書があります。

(iii)サーバのFQDNを使用して新しい自己署名証明書を生成する

CVPサーバ

WSMの自己署名証明書を生成するコマンド:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias wsm\_certificate -keysize 2048 -keyalg RSA -validity XXXX

◆ 注:デフォルトでは、証明書は2年間生成されます。-validity XXXXを使用して、証明書を再 生成する有効期限を設定します。有効期限を設定しない場合、証明書は90日間有効であり 、この時間の前にCAによって署名される必要があります。これらの証明書のほとんどでは 、3 ~ 5年は妥当な検証期間である必要があります。

標準的な有効性入力の一部を次に示します。

1年	365
二年	730
三年	1095
4年間	1460
五年	1895

十年

3650

▲ 注意:12.5以降の証明書はSHA 256、キーサイズ2048、暗号化アルゴリズムRSAにする必要 があります。次のパラメータを使用して値を設定します:-keyalg RSAおよび – keysize 2048。CVPキーストアコマンドに – storetype JCEKSパラメータが含まれていることが重要 です。これを行わないと、証明書、キー、または悪い場合にはキーストアが破損する可能性 があります。

サーバのFQDNを指定します。質問の最初と最後の名前は何ですか。

C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore -al	ias w
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?	
[Helenous] +	

次の質問に答えてください。

組織単位の名前は何ですか。

[不明]: <OUを指定>

組織の名前は何ですか。

[不明]: <組織の名前を指定>

市区町村の名前は何ですか。

[不明]: <市区町村の名前を指定>

都道府県の名前を入力してください。

[不明]: <都道府県の名前を指定>

このユニットの2文字の国番号は何ですか。

#### [不明]: <2文字の国番号を指定>

次の2つの入力にはyesを指定します。

vxml\_certificateとcallserver\_certificateに対して同じ手順を実行します。

%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 CVPコールサーバをリブートします。

CVP Reportingサーバ

WSMの自己署名証明書を生成するコマンド:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias wsm\_certificate -keysize 2048 -keyalg RSA -validity XXXX

クエリ用のサーバのFQDN(最初と最後の名前)を指定し、CVPサーバで行った手順と同じ手順を続 行します。

callserver\_certificateについても同じ手順を実行します。

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias callserver\_certificate -keysize 2048 -keyalg RSA -validity XXXX

レポートサーバをリブートします。

(iv) CVPサーバおよびレポートサーバからのwsm\_Certificateのエクスポート

a)各CVPサーバから一時的な場所にWSM証明書をエクスポートし、証明書の名前を任意の名前に 変更します。名前はwsmcsX.crtに変更できます。「X」をサーバのホスト名に置き換えます。た とえば、wsmcsa.crt、wsmcsb.crt、wsmrepa.crt、wsmrepb.crtなどです。

自己署名証明書をエクスポートするコマンド:

%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)証明書をパス%CVP\_HOME%\conf\security\wsm.crtからコピーし、名前をwsmcsX.crtに変更し て、ADSサーバ上の一時フォルダに移動します。

ステップ2:CVPサーバのWSM証明書のADSサーバへのインポート

ADSサーバーに証明書をインポートするには、Javaツールセットの一部であるキーツールを使用 する必要があります。このツールがホストされているJavaホームパスを見つける方法がいくつか あります。

(i) CLIコマンド>echo %CCE\_JAVA\_HOME%

## C:\>echo %CCE\_JAVA\_HOME% C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot

Javaホームパス

#### (ii)図に示すように、高度なシステム設定を手動で実行します。

🔿 👻 🛧 🔛 🛛 Control Pa	anel > System and Security > System		~ Ö	Search Control Panel
ntrol Panel Home	System Properties			
vice Manager mote settings	Computer Name Hardware Advanced Remote You must be logged on as an Administrator to make most of these changes.	Environment Variables		
vanced system settings	Performance Visual effects, processor scheduling, memory usage, and virtual memory	User variables for Administrator		
		Variable	Value	
	Settings	Path TEMP	C:\Users\Administrator\AppData\Local\Microsoft\WindowsA	pps;
	User Profiles	TMP	C:\Users\Administrator\AppData\Local\Temp	
	Desktop settings related to your sign-in Settings			
	Startup and Recovery		Neu	Edit Dalata
	System starup, system raiure, and deougging information		IVEW	Edit Delete
	Settings	System variables		
	Environment Variables	Variable	Value	
		CCE_JAVA_HOME	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot	
	OK Cancel Archy	ComSpec	C:\Windows\system32\cmd.exe	
	On Cancer oppy	COR_ENABLE_PROFILING	1	
		CORECLR_ENABLE_PROFILI	AppDynamics.AgentProfiler 1	
		CORECLR PROFILER	AppDynamics.ApentProfiler	
			New	Edit Delete
			Г	OK Cancel

環境変数

PCCE 12.6では、OpenJDKのデフォルトパスはC:\Program Files (x86)\OpenJDK\jre-8.0.272.10hotspot\binです。

自己署名証明書をインポートするコマンド:

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

# ✤ 注:導入環境内の各CVPに対してコマンドを繰り返し、他のADSサーバで同じタスクを実行します

(iii) ADSサーバでApache Tomcatサービスを再起動します。

ステップ3: ADSサーバー証明書のエクスポート

次に、ADS証明書をエクスポートする手順を示します。

(i) ADSサーバで、ブラウザからサーバURL https://<servername>に移動します。

(ii)証明書を一時フォルダ(例:c:\temp\certs)に保存し、証明書にADS<svr>[ab].cerという名前を付 けます。

← → C ▲ Not secure   Miljek//ucce-aw.covebex.com	
Centificate X General Details Centification Path Prov: cAllo V Petid Value A Vorsion V3 Serval number 000 008127917/th0660	<ul> <li>Certificate Export Waard</li> <li>Export Rise Format Certificates can be exported in a variety of the formats.</li> </ul>
Sgrature algorithm ana25605A. Sgrature hash-algorithm sha256 Dawer UCCE-AVI.covebex.com Valid from Nuesday, Hebruary 21, 2012 4 Valid to Monday, Petruary 38, 2043 4 Subsect INCE-AUI.covebex.com	Select the ferrent you want to use: ODDR encoded brany X.509 (.CDD) Blace 64 encoded 15.500 (.CDD) Orystographic Message Syntax Standard - PKCS #2 Certificates (.P70) Dirclude al certificates in the certification path if possible Personal Information Exchange - PKCS #22 (.PTS) Dirclude al certificates in the certification path if possible Delete the private key if the export is successful Dirclude al certificate privacy
Edit Properties Copy to File	O Morseeft Serialized Certificate Store (1557) Next Cancel

ADS証明書のエクスポート

注:オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ4:CVPサーバおよびレポーティングサーバへのADSサーバ証明書のインポート

(i)証明書をディレクトリ%CVP\_HOME%\conf\securityにあるCVPサーバおよびCVPレポートサー バにコピーします。

(ii) CVPサーバおよびCVPレポーティングサーバに証明書をインポートします。

%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\ADS{svr}[ab].cer

他のADSサーバーの証明書についても同じ手順を実行します。

(iii) CVPサーバとレポートサーバを再起動する

セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ1:VOSプラットフォームアプリケーションサーバ証明書のエクスポート

ステップ2: VOSプラットフォームアプリケーション証明書をADSサーバにインポートします。

ステップ3: CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のインポート

このプロセスは、次のようなすべてのVOSアプリケーションに適用できます。

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

ステップ1:VOSプラットフォームアプリケーションサーバ証明書のエクスポート

(i) Cisco Unified Communications Operating System Administrationページ (https://FQDN:8443/cmplatform)に移動します。

(ii) Security > Certificate Managementの順に移動し、tomcat-trustフォルダ内にアプリケーション プライマリサーバ証明書があることを確認します。

deads. Cisco Unified Operating System Admin For Case Unified Communications Solutions	vistrat	ion		Navipation Communication - 20 administration Almost Legen
Shou e. Settings e. Security e. Software Upgrades e. Services e. Help e.				
Cartilicate Unt				
🚯 Generale Set agreet 🐴 Lipitud Cathodis Cathodis daas 🔒 Generale	054			
ternal-lowt Case. ECC. Rest. C6	Self- agenti	00	Cecs, RCC, And, CA	Coos_BCC_Root_CA
toweshired Indexic Academic and Assessch Institutions Root24, 2011	Self-	854	Melanic, Academic, and Jasearch, Institutions, RootCA, 2012	Melanic, Academic, and J. Research, Institution
tumost-trust CESTE Indianay Chilai Rust CB Ca	Self- appeal	858	CISTE_WIDeXey_Globel_Root_GB_CA	00578_WDIerkey_Ghobel_Root_GB_CA
toreat-trust Amazon Root CA.4	Self-	00	Amazon_Root_CA_4	Amazon, Rost, CA, 4
tomost-trust <u>DET_Revt_CA_X3</u>	Self- apped	858	DST_Reet_CA_X3	047_Reet_CA_X3
tomot-bust Additud Deternal CA Real	Dell-	838	AddTrust_Enternal_CA_Root	AddTrust_Deternal_CA_Root
Romcal-Inval <u>coalages.com</u>	Deff- algoed	104	og.tow.com	capitors.com
Normal-Invalid Tripping Costs Root Case 2	Sect.	10.0	MeinSet_GlobalRoot_Cass_3	1-ferelac_GobsRoot_Cass_3
tompatitivat <u>DisCet Global Root G2</u>	Setting	1054	Dig/Cert_Oldeal_Root_02	DigiCert_Stubal_Root_S2

(iii)証明書を選択し、「download .PEM file」をクリックしてADSサーバの一時フォルダに保存します。

#### Certificate Settings

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

#### Certificate File Data

Version: V3	
Serial Number: 5C35B3A89A8974719BB885B6A92CF710D	
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=U	S
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=I	JS
Key: RSA (1.2.840.113549.1.1.1)	
Key value:	
3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3-	430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdd	a3e71f27900d992
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe873	2352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c	447aceb2a651b6f 🔛
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d7	2ba0c3ccf85444f7a 🏑

Delete

Download .PEM File

Download .DER File

### 💊 注:サブスクライバに対して同じ手順を実行します。

ステップ2: VOSプラットフォームアプリケーション証明書のADSサーバへのインポート

キーツールを実行するパス: %CCE\_JAVA\_HOME%\bin

自己署名証明書をインポートするコマンド:

%CCE\_JAVA\_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias
{fqdn\_of\_VOS>} -keystore {ICM install directory}\ssl\cacerts

ADSサーバでApache Tomcatサービスを再起動します。

# 💊 注:他のADSサーバでも同じタスクを実行します

ステップ3: CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のインポート

キーツールを実行するパス: %CCE\_JAVA\_HOME%\bin

#### 自己署名証明書をインポートするコマンド:

%CCE\_JAVA\_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias
{fqdn\_of\_cucm>} -keystore {ICM install directory}\ssl\cacerts

PGサーバでApache Tomcatサービスを再起動します。

💊 注:他のCUCM PGサーバでも同じタスクを実行します

セクション3:Rogger、PG、およびADSサーバ間での証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ1:RoggerサーバとPGサーバからのIIS証明書のエクスポート

ステップ2:RoggerサーバとPGサーバからのDFP証明書のエクスポート

ステップ3: ADSサーバへの証明書のインポート

ステップ4:RoggerサーバとPGサーバへのADS証明書のインポート

ステップ1:RoggerサーバとPGサーバからのIIS証明書のエクスポート

(i)ブラウザからADSサーバで、サーバ(Rogger、PG)のURL:https://{servername}に移動します。

(ii)証明書を一時フォルダ(c:\temp\certsなど)に保存し、証明書の名前をICM<svr>[ab].cerとします。

← → C A Not secure   Mijex//ucce-aw.covebex.com	
Centificate Pedia Pedia Value Pedia Value Value Centificate Pedia Value Value Centificate Value Centificate Value Value Centificate Value Centificate Value Value Centificate Value	<ul> <li>Certificate Expert Waard</li> <li>Expert Ris Format         <ul> <li>Certificates Can be exported in a variety of the formats.</li> <li>Select the format you want to use:</li></ul></li></ul>
Edit Properties Copy to File	Bruble ortificate privacy     Ortificate Store (357)
06	Net Cancel

IIS証明書のエクスポート

💊 注:オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ 2: RoggerサーバとPGサーバからのDFP証明書のエクスポート

(i)ブラウザからADSサーバで、サーバ(Rogger、PG)のDFP url:https://{servername}:7890/icmdp/rest/DiagnosticPortal/GetProductVersionに移動します。

(ii)証明書をフォルダexample c:\temp\certsに保存し、証明書にdfp{svr}[ab].cerという名前を付け ます

ereral Details Certificate	e fath	×	+ 🖟 Cetificate Export Wigard
Shere: elite Peid Version Spreture algorithm Spreture hash algorith Sauer valid from valid to Subsect	V Value V2 SNO-Marce0.05-KUE3H SNA-258/KSA sha258 UCCE-AWLoomebex.o Tuesday, Petruary 2 Setunday, Petruary 2 Setunday, Petruary 2 Setunday, Petruary 2	1221ar2 pn 1, 2201 4 1, 2240 m	Select the format proviment to use:
	Edit Properties	oy to Me	

DFP証明書のエクスポート

💊 注:オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ3: ADSサーバへの証明書のインポート

IIS自己署名証明書をADSサーバにインポートするコマンド。キーツールを実行するパス: %CCE\_JAVA\_HOME%\bin

%CCE\_JAVA\_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias
{fqdn\_of\_server}\_IIS -keystore {ICM install directory}\ssl\cacerts

Subscription State St

診断のための自己署名証明書をADSサーバーにインポートするコマンド

%CCE\_JAVA\_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias
{fqdn\_of\_server}\_DFP -keystore {ICM install directory}\ssl\cacerts

Ŷ 注:エクスポートされたすべてのサーバ証明書をすべてのADSサーバにインポートします。

ADSサーバでApache Tomcatサービスを再起動します。

ステップ4:RoggerサーバとPGサーバへのADS証明書のインポート

IIS自己署名証明書をRoggerおよびPGサーバにインポートするコマンド。キーツールを実行する パス: %CCE\_JAVA\_HOME%\bin

%CCE\_JAVA\_HOME%\bin\keytool -keystore ..\lib\security\cacerts -import -storepass changeit alias {fqdn\_of\_server}\_IIS -file c:\temp\certs\ICM{svr}[ab].cer

✤ 注:すべてのRoggerおよびPGサーバにエクスポートされたすべてのADSサーバIIS証明書を インポートします。

RoggerサーバとPGサーバでApache Tomcatサービスを再起動します。

セクション4:CVP CallStudio Webサービスの統合

Webサービス要素とRest\_Client要素のセキュアな通信を確立する方法の詳細については、

詳細については、『<u>Cisco Unified CVP VXML ServerおよびCisco Unified Call Studioリリース</u> <u>12.6(2) - Webサービスの統合[Cisco Unified Customer Voice Portal] – シスコのユーザガイド</u>』

#### 関連情報

- <u>CVP設定ガイド セキュリティ</u>
- <u>UCCEセキュリティガイド</u>
- <u>PCCE管理ガイド</u>
- Exchange PCCE自己署名証明書 PCCE 12.5
- Exchange UCCE自己署名証明書 UCCE 12.5
- Exchange UCCE自己署名証明書 UCCE 12.6
- ・ <u>CA署名付き証明書の実装 CCE 12.6</u>
- <u>Contact Center Uploaderツールを使用した証明書の交換</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。