

UCCEソリューションでの自己署名証明書の交換

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[手順](#)

[CCE AWサーバおよびCCEコアアプリケーションサーバ](#)

[セクション 1.Router\Logger、PG、およびAWサーバ間の証明書交換](#)

[セクション 2.VOSプラットフォームアプリケーションとAWサーバ間の証明書交換](#)

[CVP OAMPサーバおよびCVPコンポーネントサーバ](#)

[セクション 1.CVP OAMPサーバとCVPサーバおよびレポーティングサーバ間の証明書交換](#)

[セクション 2.CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換](#)

[セクション 3.CVPサーバとVVBサーバ間の証明書交換](#)

[CVP Call Studio Webサービスの統合](#)

[関連情報](#)

はじめに

このドキュメントでは、Unified Contact Center Enterprise(UCCE)ソリューションで自己署名証明書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。

- UCCEリリース12.5(1)
- Customer Voice Portal(CVP)リリース12.5(1)
- Cisco Virtualized Voice Browser(VVB)

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。

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5

- CVP Operations Console (OAMP)
- CVPの新しいOAMP(NOAMP)

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。

背景説明

UCCEソリューションでは、ROGGER、Peripheral Gateway(PG)、Admin Workstation(AW)/Administration Data Server(ADS)、Finesse、Cisco Unified Intelligence Center(CUIC)などのコアアプリケーションに関連する新機能の設定は、Contact Center Enterprise(CCE)の管理ページで行います。CVP、Cisco VVB、ゲートウェイなどの自動音声応答(IVR)アプリケーションでは、NOAMPが新機能の設定を制御します。CCE 12.5(1)以降は、security-management-compliance(SRC)のため、CCE AdminおよびNOAMPへのすべての通信は、セキュアHTTPプロトコルを介して厳密に行われます。

自己署名証明書でこれらのアプリケーション間のシームレスで安全な通信を実現するには、サーバ間での証明書の交換が必須になります。次のセクションでは、次の間で自己署名証明書を交換するために必要な手順について詳しく説明します。

- CCE AWサーバおよびCCEコアアプリケーションサーバ
- CVP OAMPサーバおよびCVPコンポーネントサーバ

手順

CCE AWサーバおよびCCEコアアプリケーションサーバ

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。

CCE AW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：Router and Logger(ROGGER){A/B}、Peripheral Gateway(PG){A/B}、およびすべてのAW/ADS。



注:IISおよびDiagnostic Framework Portico(DFP)証明書が必要です。

- VOSプラットフォーム：Finesse、CUIC、ライブデータ(LD)、アイデンティティサーバ(IDS)、Cloud Connect、およびその他の該当するサーバは、インベントリデータベースに含まれます。

同じことが、ソリューション内の他のAWサーバにも当てはまります。

Router\Logger Server：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AWサーバのIIS証明書。

CCE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、次のセクションに分かれています。

セクション 1.Router\Logger、PG、およびAWサーバ間の証明書交換。

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

セクション 1.Router\Logger、PG、およびAWサーバ間の証明書交換

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：Router\Logger、PG、およびすべてのAWサーバからIIS証明書をエクスポートします。

ステップ 2：Router\Logger、PG、およびすべてのAWサーバからDFP証明書をエクスポートします。

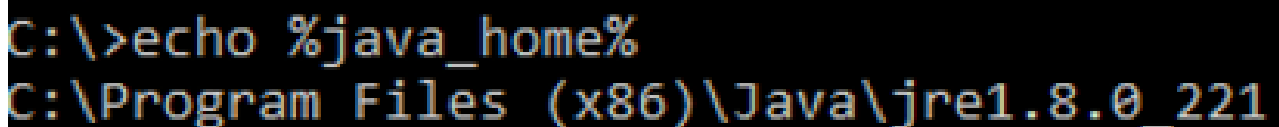
ステップ 3：IISおよびDFP証明書をRouter\Logger、PG、およびAWからAWサーバにインポートします。

ステップ 4：AWサーバからRouter\LoggerおよびPGにIIS証明書をインポートします。

⚠ 注意：作業を開始する前に、キーストアをバックアップし、コマンドプロンプトを管理者として開く必要があります。

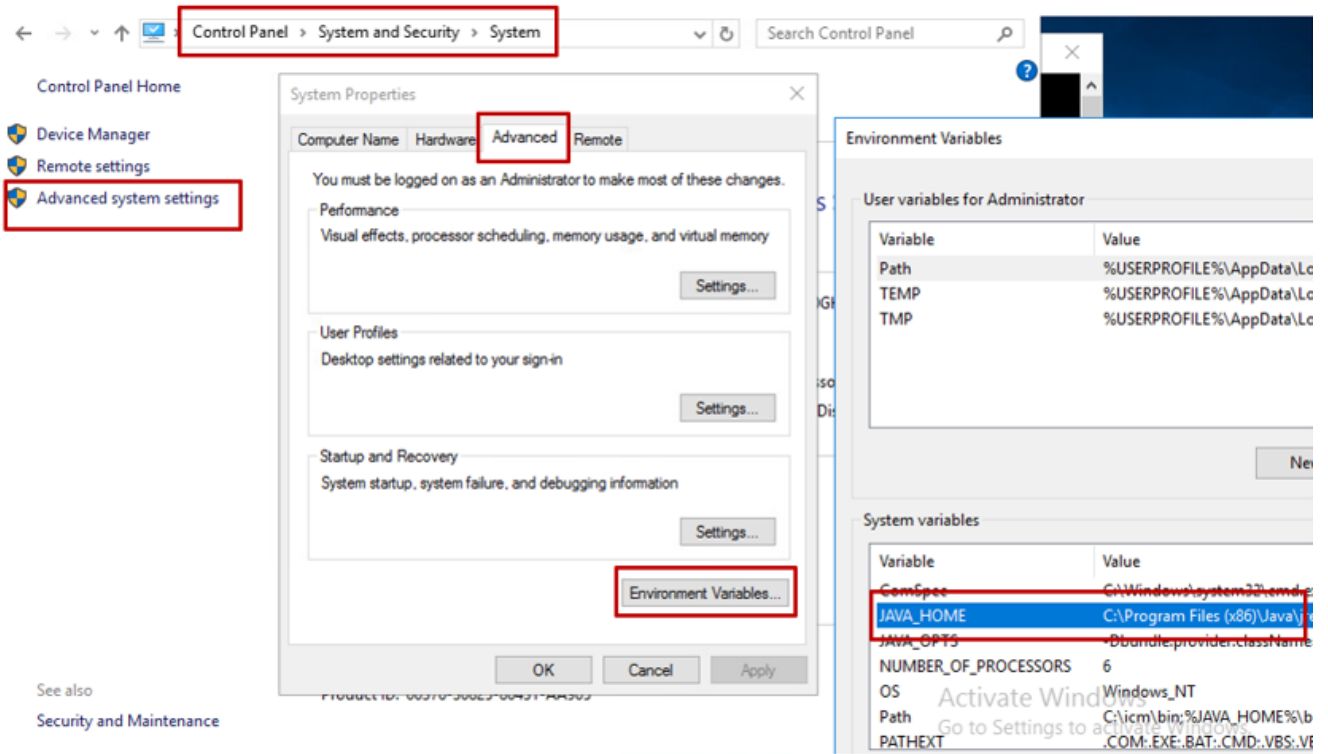
1. Javaキーツールがホストされている場所を確認するために、Javaのホームパスを把握します。Javaホームパスを見つける方法はいくつかあります。


オプション 1CLI コマンド: `echo %JAVA_HOME%`



```
C:\>echo %java_home%
C:\Program Files (x86)\Java\jre1.8.0_221
```

オプション 2図に示すように、Advancedシステム設定を使用して手動で設定します。



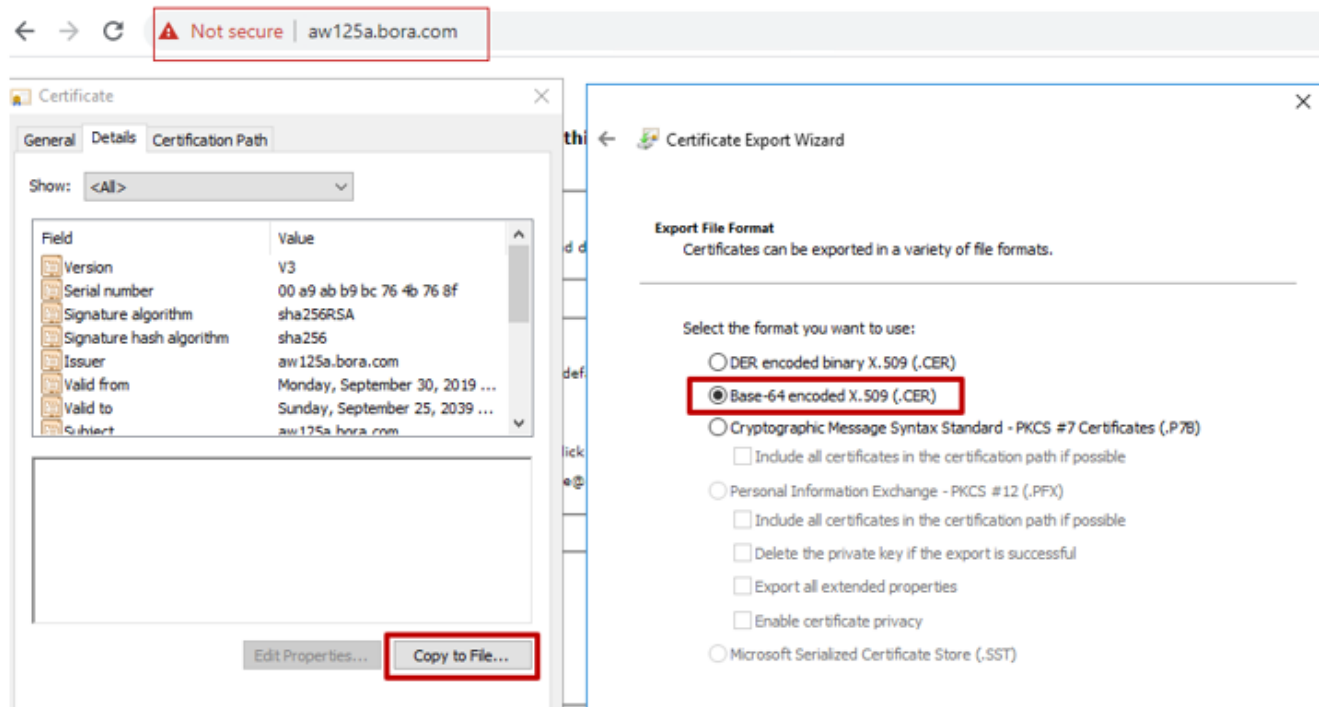
 注:UCCE 12.5では、デフォルトパスはC:\Program Files (x86)\Java\jre1.8.0_221\binです。
%CCE_JAVA_HOME% ただし、12.5 (1a)インストーラを使用している場合、または12.5 ES55 (必須のOpenJDK ES) がインストールされている場合は、OpenJDKを使用してデータストアのパスが変更されているため%JAVA_HOME%、の代わりに使用します。CCEおよびCVPでのOpenJDKの移行についての詳細は、次のドキュメントを参照してください。[CCE 12.5\(1\)でのOpenJDKのインストールと移行](#)および[CVP 12.5\(1\)でのOpenJDKのインストールと移行](#)。

2. フォルダからcacerts ファイルをバックアップ {JAVA_HOME}\lib\security します。別の場所にコピーできます。

ステップ 1 : Router\Logger、PG、およびすべてのAWサーバからIIS証明書をエクスポートします。

1. ブラウザからAWサーバで、サーバ (ROgger、PG、その他のAWサーバ) の URL <https://{servername}> に移動します。

CCE via Chrome Browser



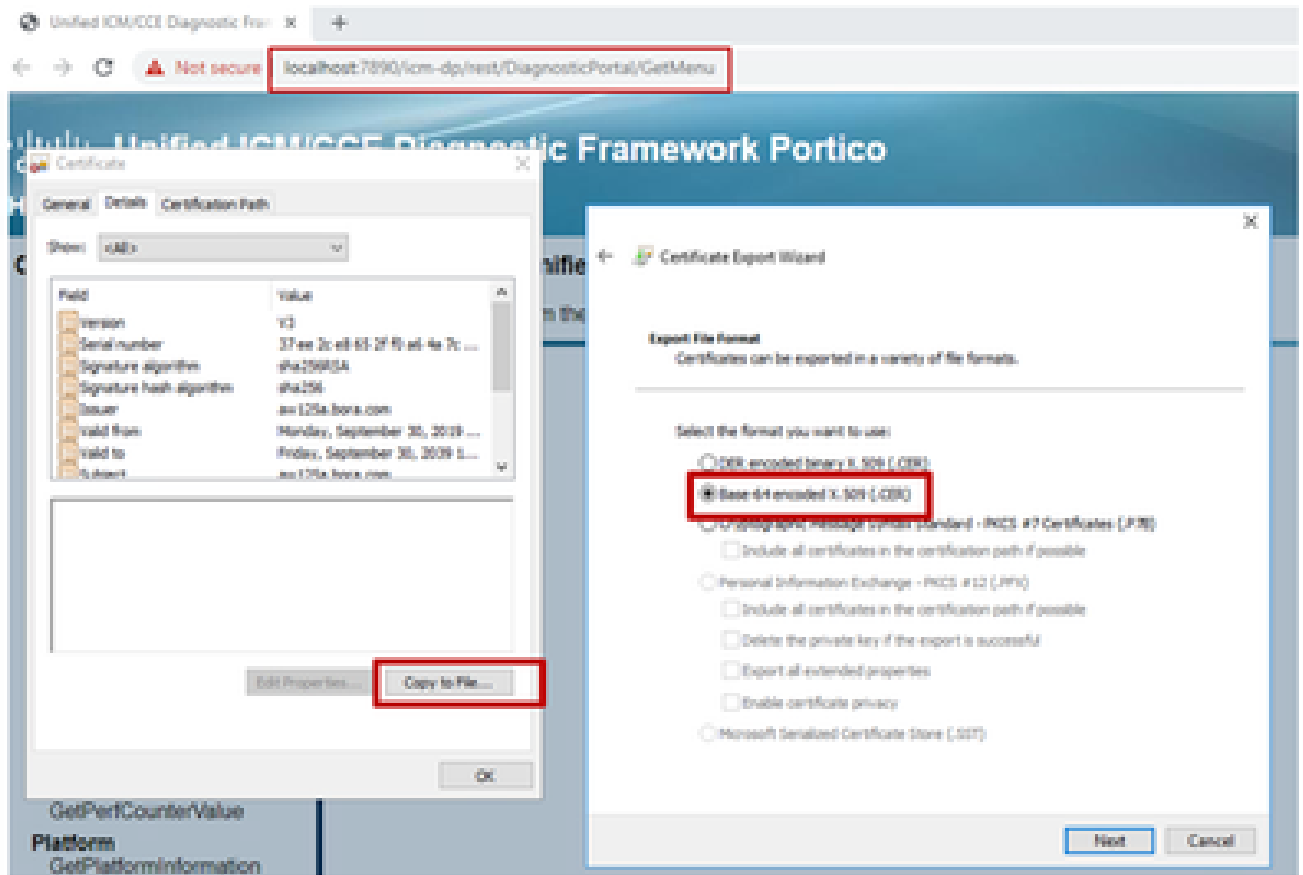
- たとえば、証明書を一時フォルダに保存し `c:\temp\certs`、証明書に `ICM{svr}[ab].cer` という名前を付けます。

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

ステップ 2：Router\Logger、PG、およびすべてのAWサーバからDFP証明書をエクスポートします。

- AWサーバでブラウザを開き、サーバ (Router、LoggerまたはROGGER、PG、AW) のDFP URL `https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion` に移動します。


Portico via Chrome Browser



2. Exampleフォルダに証明書を保存しc:\temp\certs、名前をdfp{svr}[ab].cerとして証明書に付けます。


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

ステップ 3：IISおよびDFP証明書をRouter\Logger、PG、およびAWからAWサーバにインポートします。

 注：この例のコマンドでは、デフォルトのキーストアパスワードとしてchangeitを使用します。システムのパスワードを変更した場合は、これを変更する必要があります。

IIS自己署名証明書をAWサーバにインポートするコマンド。keytoolを実行するパスは%JAVA_HOME%\binです。

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

 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AWサーバにインポートします。

AWサーバにDFP自己署名証明書をインポートするコマンド：

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file  
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```


 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AWサーバにインポートします。

AWサーバでApache Tomcatサービスを再起動します。

ステップ 4：AWサーバからRouter\LoggerおよびPGにIIS証明書をインポートします。

AW IIS自己署名証明書をRouter\LoggerおよびPGサーバにインポートするコマンド：

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file  
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myawa.domain.com
```

 注:A側とB側のRouter\LoggerサーバとPGサーバにエクスポートされたすべてのAW IISサーバ証明書をインポートします。

Router\Logger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 2.VOSプラットフォームアプリケーションとAWサーバ間の証明書交換

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：AWサーバへのVOS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されます。

- 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. tomcat-trustフォルダに移動しSecurity > Certificate Management、アプリケーションのプライマリサーバ証明書をを見つけます。

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | administrator | About | Logout

Home > Settings > Security > Software Updates > Services > Help >

Certificate List

Generate Self-Signed | Visual Certificate/Certificate chain | Generate CSR

tomcat-trust	Issuer	Self-Signed	EC	Key	Subject
Class_BOC_Boot_CA	Self-Signed	EC	Class_BOC_Boot_CA	Class_BOC_Boot_CA	
Hellenic_Academic_and_Research_Institutions_BootCA_2021	Self-Signed	RSA	Hellenic_Academic_and_Research_Institutions_BootCA_2021	Hellenic_Academic_and_Research_Institutions	
CCITL_WebServer_Global_Boot_CA	Self-Signed	RSA	CCITL_WebServer_Global_Boot_CA	CCITL_WebServer_Global_Boot_CA	
Amazon_Boot_CA_4	Self-Signed	EC	Amazon_Boot_CA_4	Amazon_Boot_CA_4	
DIT_Boot_CA_X3	Self-Signed	RSA	DIT_Boot_CA_X3	DIT_Boot_CA_X3	
AddTrust_External_CA_Boot	Self-Signed	RSA	AddTrust_External_CA_Boot	AddTrust_External_CA_Boot	
ccp.bora.com	Self-Signed	RSA	ccp.bora.com	ccp.bora.com	
T-Trustee_GlobalRoot_Class_3	Self-Signed	RSA	T-Trustee_GlobalRoot_Class_3	T-Trustee_GlobalRoot_Class_3	
DigCert_Global_Boot_CA	Self-Signed	RSA	DigCert_Global_Boot_CA	DigCert_Global_Boot_CA	

iii. 証明書を選択してクリックしDownload .PEM File、AWサーバの一時フォルダに保存します。

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
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Delete | **Download .PEM File** | Download .DER File

注：サブスクリバに対して同じ手順を実行します。


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

キーツールを実行するパス： {JAVA_HOME}\bin

自己署名証明書をインポートするコマンド：


```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\tem
```

AWサーバでApache Tomcatサービスを再起動します。

 注：他のAWサーバでも同じタスクを実行します。

CVP OAMPサーバおよびCVPコンポーネントサーバ

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. CVP OAMP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：CVPサーバおよびレポートサーバからのWeb Services Manager(WSM)証明書。
- VOSプラットフォーム：Customer Virtual Agent(CVA)統合用のCisco VVB、Webex Experience Management(WXM)統合用のCloud Connectサーバ。

ii. 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：OAMPサーバからのWSM証明書。
- VOSプラットフォーム：WXM統合用Cloud ConnectサーバおよびCisco VVBサーバ。

iii. CVP Reporting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：OAMPサーバからのWSM証明書。

iv. Cisco 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：CVPサーバからのVXML証明書とCVPサーバからのコールサーバ証明書。

CVP環境で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、次の3つのセクションで説明されています。

セクション 1.CVP OAMPサーバとCVPサーバおよびレポートサーバ間での証明書交換

セクション 2.CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換。

セクション 3.CVPサーバとVVBサーバ間の証明書交換。


セクション 1.CVP OAMPサーバとCVPサーバおよびレポートサーバ間の証明書交換

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、レポートサーバ、およびOAMPサーバからWSM証明書をエクスポートします。

ステップ 2：CVPサーバおよびレポートサーバからOAMPサーバにWSM証明書をインポートします。

ステップ 3 : CVP OAMPサーバのWSM証明書をCVPサーバとレポートサーバにインポートします。

 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.キーストアのパスワードを確認するには、 `more %CVP_HOME%\conf\security.properties` コマンドを実行します。
3. `keytool` コマンドを実行する場合は、このパスワードが必要です。
- 4.ディレクトリから `%CVP_HOME%\conf\security\`、 コマンドを実行し `copy .keystore backup.keystore` ます。

ステップ 1 : CVPサーバ、レポートサーバ、およびOAMPサーバからWSM証明書をエクスポートします。

i. WSM証明書を各サーバから一時的な場所にエクスポートし、証明書の名前を任意の名前に変更します。このファイルはという名前に変更でき `wsmX.crt` ます。Xはサーバのホスト名で置き換えます。たとえば、 `wsmcsa.crt`、 `wsmcsb.crt`、 `wsmrepa.crt`、 `wsmrepb.crt`、 `wsmoamp.crt` 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 -a
```

ii.各サーバからのパスから証明書をコピーし `C:\Cisco\CVP\conf\security\wsm.crt`、サーバのタイプに基づいて名前を変更 `wsmX.crt` します。

ステップ 2 : CVPサーバおよびレポートサーバからOAMPサーバにWSM証明書をインポートします。

i. WSM証明書を各CVPサーバおよびレポートサーバ(`wsmX.crt`)からOAMPサーバ上のディレクトリにコピー `%CVP_HOME%\conf\security` します。

ii.次のコマンドを使用して、これらの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 -a
```

iii.サーバをリブートします。

ステップ 3 : CVP OAMPサーバからCVPサーバおよびレポートサーバにWSM証明書をインポートします。

i. OAMPサーバのWSM証明書(`wsmoampX.crt`)をすべてのCVPサーバとレポートサーバの `%CVP_HOME%\conf\security` ディレクトリにコピーします。

ii.次のコマンドを使用して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 -a
```

iii.サーバをリブートします。

セクション 2.CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換

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プラットフォームからアプリケーション証明書をエクスポートします。

ステップ 2 : OAMPサーバにVOSアプリケーション証明書をインポートします。

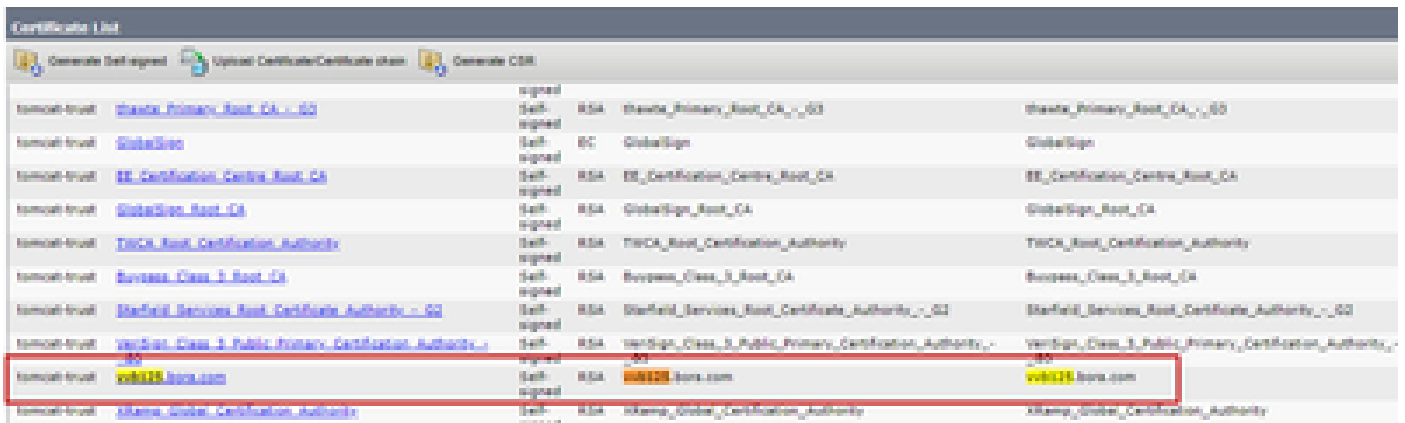
このプロセスは、次のようなVOSアプリケーションに適用できます。

- CUCM
- VVB
- Cloud Connect

ステップ 1 : VOSプラットフォームからアプリケーション証明書をエクスポートします。

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


ii. tomcat-trustフォルダに移動しSecurity > Certificate Management、アプリケーションのプライマリサーバ証明書を見つけます。



Name	Status	Key Algorithm	Issuer	Validity
tomcat-trust: GlobalSign_Primary_Root_CA_-_G2	Self-signed	RSA	GlobalSign_Primary_Root_CA_-_G2	GlobalSign_Primary_Root_CA_-_G2
tomcat-trust: GlobalSign	Self-signed	EC	GlobalSign	GlobalSign
tomcat-trust: EE_Certification_Centre_Root_CA	Self-signed	RSA	EE_Certification_Centre_Root_CA	EE_Certification_Centre_Root_CA
tomcat-trust: GlobalSign_Root_CA	Self-signed	RSA	GlobalSign_Root_CA	GlobalSign_Root_CA
tomcat-trust: TruCA_Root_Certification_Authority	Self-signed	RSA	TruCA_Root_Certification_Authority	TruCA_Root_Certification_Authority
tomcat-trust: Business_Class_3_Root_CA	Self-signed	RSA	Business_Class_3_Root_CA	Business_Class_3_Root_CA
tomcat-trust: Starfield_Services_Root_Certificate_Authority_-_G2	Self-signed	RSA	Starfield_Services_Root_Certificate_Authority_-_G2	Starfield_Services_Root_Certificate_Authority_-_G2
tomcat-trust: VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3	Self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3
tomcat-trust: vob111.bom.com	Self-signed	RSA	vob111.bom.com	vob111.bom.com
tomcat-trust: Xkemp_Global_Certification_Authority	Self-signed	RSA	Xkemp_Global_Certification_Authority	Xkemp_Global_Certification_Authority

iii.証明書を選択してクリックしDownload .PEM File、OAMPサーバの一時フォルダに保存します。

Status

 Status: Ready

Certificate Settings

File Name	vvb125.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: 68FE55F56F863110B44D835B825D84D3
Signature Algorithm: SHA256withRSA (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 Dec 05 06:51:10 PST 2019
To: Tue Dec 03 06:51:09 PST 2024
Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dacc81013bd693614684c27e05de2004553004
```

ステップ 2 : OAMPサーバにVOSアプリケーション証明書をインポートします。

- i. VOS証明書をOAMPサーバ上のディレクトリにコピー%`CVP_HOME%\conf\security`します。
- ii. 次のコマンドを使用して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 -a
```

- iii. サーバをリブートします。

セクション 3.CVPサーバとVVBサーバ間の証明書交換

これは、CVPと他のコンタクトセンターコンポーネント間のSIP通信を保護するためのオプションの手順です。 詳細については- 製品が影響を受けるかどうかを確認するには、このアドバイザリの「CVP設定ガイド : [CVP設定ガイド-セキュリティ](#)を参照。

CVP Call Studio Webサービスの統合

Web Services Element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、『[Cisco Unified CVP VXML ServerおよびCisco Unified Call Studioリリース12.5\(1\):Webサービス統合\[Cisco Unified Customer Voice Portal\] : シスコのユーザガイド](#)』を参照してください。

関連情報

- [CVP設定ガイド – セキュリティ](#)
- [UCCEセキュリティガイド](#)
- [PCCE管理ガイド – セキュリティ](#)
- [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 PCCE自己署名証明書 – PCCE 12.6](#)
- [CA署名付き証明書の実装 : CCE 12.6](#)
- [CCE OpenJDKの移行](#)
- [CVP OpenJDKの移行](#)
- [証明書交換ユーティリティ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

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。