UCCE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>
<u>背景説明</u>
<u>手順</u>
<u>CCE AWサーバおよびCCEコアアプリケーションサーバ</u>
<u>セクション 1.Router\Logger、PG、およびAWサーバ間の証明書交換</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AWサーバ間の証明書交換</u>
<u>CVP OAMPサーバおよびCVPコンポーネントサーバ</u>
<u>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</u>
<u>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</u>
<u>セクション 3.CVPサーバとVVBサーバ間の証明書交換</u>
<u>CVP Call Studio Webサービスの統合</u>
<u>関連情報</u>

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。

自己署名証明書の環境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。

- - 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%



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。

🔶 🐳 👻 🛧 🔛 i Control Pan	el > System and Security > System v 🖉 Sea	rch Co	ntrol Panel 🔎	×
Control Panel Home	System Properties	×	8	^
Device Manager	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	s	User variables for Admini	strator
	Visual effects, processor scheduling, memory usage, and virtual memory		Variable	Value
			Path	%USERPROFILE%\AppData\Lc
	Settings	G	TEMP	%USERPROFILE%\AppData\Lc
	Liser Profiles		TMP	%USERPROFILE%\AppData\Lc
	Desktop settings related to your sign-in	iso		
	Settings	Di		
	Startup and Recovery System startup, system failure, and debugging information	H		Ne
	Settings		System variables	
			Variable	Value
	Environment Variables		ComSpee	Ci\Windows\system32\emdig
		1	JAVA_HOME	C:\Program Files (x86)\Java\j e
			JAVA_OPTS	Dbundle.provider.className
6	OK Cancel Apply		NUMBER_OF_PROCESS	ORS 6
See also	FIGURETID. 00310-30023-00431-204303	_	os Activate	Wind Windows_NT
Security and Maintenance			PATHEXT Go to Settin	c:\icm\bin:%JAVA_HOME%\b .COM:.EXE:.BAT:.CMD:.VBS:.VE

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。
 <u>CCE 12.5(1)でのOpenJDKのインストールと移行</u>および<u>CVP 12.5(1)でのOpenJDKのインストールと移行</u>

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 URLhttps://{servername}に移動します。

CCE via Chrome Browser

how: <all> Field Value Wersion V3 Serial number 00 a9 ab b9 bc 76 4b 76 8f Signature algorithm sha256RSA Signature hash algorithm sha256R Value Value Value Signature algorithm sha256RSA Signature hash algorithm sha256 Valid from Monday, September 30, 2019 Valid to Sunday, September 25, 2039 Valid to Sunday, September 25, 2039 Ick Cryptogr Ick O Personal</all>	e exported in a variety of file formats.
Field Value Export File Format Version V3 Serial number 00 a9 ab b9 bc 76 4b 76 8f Signature algorithm sha256RSA Signature hash algorithm sha256 Issuer aw125a.bora.com Valid from Monday, September 30, 2019 Valid to Sunday, September 25, 2039 Subject aw125a hora.com Valid to Sunday, September 25, 2039 Subject aw125a hora.com Valid to Sunday, September 26, 2039 Valid to Personal	e exported in a variety of file formats.
Serial number 00 a9 ab 59 bc 76 46 76 8f Signature algorithm sha256RSA Signature hash algorithm sha256. Issuer aw 125a.bora.com Valid from Monday, September 30, 2019 Valid to Sunday, September 25, 2039 Subject aw 125a.bora.com Cryptogr ick Indu @@ Personal	
	t you want to use: ded binary X.509 (.CER) incoded X.509 (.CER) phic Message Syntax Standard - PKCS #7 Certificates (.P78) ie all certificates in the certification path if possible information Exchange - PKCS #12 (.PFX) ie all certificates in the certification path if possible
Delet	the private key if the export is successful t all extended properties e certificate privacy

- 2. 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。

1. 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 URLhttps://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersionに移動します。

O Unified ICM/CCE Diagnostic From X + localhost:7890/icm-dp/rest/DiagnosticPortal/GetMenu July Unified ICHICCE Disgnostic Framework Portico Certificate General Definity Certification Pade ж Press (AD) 👉 Certificate Export Waard sifie Paid Table 1 n th 10 Service's **Expert** File Bern Serial number 37 ee 20 ell-65 27 fb el-4e 7c -Certificates can be exported in a variety of file formate. Separate appointer. 100.000000 Scruben had also the \$12,256 aw 125a hora.com Sec. all told from Monday, September 35, 2019 ... Select the format you want to use: Friday, September 30, 2009 L Valid to Of Revenues of Streety K. 509 C.CER. S. Acar an Ola bera ces Blace 64 encoded X, 509 (1000) Sand - INCS #7 Certificates (JP20) tes in the certification path if possible Non Exchange - PKCS #12 (JPN) Include all certificates in the certification path if poss Delete the private key if the export is accessful Depart all extended properties Copy to File. Enable certificate privace Morosoft Serialized Certificate Store (1997) 00 **GetPertCounterValue** Not Cancel Platform GetPlatforminformation

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

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 (<u>https://{FQDN}:8443/cmplatform</u>)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。

esce ,	Cisco Unified Operating System Admin or Coce Unified Communications Solutions	istrat	ion		enipelos Casa Unifed da Administration 🔹 🗟 administrature About Lopin
Show e Sette	gs + Security + Software Upgrades + Securities + Halp +				
Certificate Lie	8				
🔼 German 1	lef spect 🐴 Upter Cettors Cettors dan 🔍 General I	(M)			
tomcal-trust	Case BCC Asst. Ch	Self- agend	60	Core, BCC, And, CA	Coos,BCC,Asot,CA
tom ad-invest	Selenic Academic and Research Institutions Root24, 2011	Self-	854	Helenic, Academic, and Januarch, Institutions, RootCA, 2015	Indusic_Academic_and_Research_Dratitution
torncad-trust	COSTE MODerlay, Chibel Runt, GB, CA	Self- agend	154	01578_W15erey_Givbel_Root_GB_CA	OSTE_WSSeriey_Global_Root_GB_CA
torn of front	Amazon, Acol. CA. 4	Self- appeal	ec.	Amazon_Root_CA_4	Amazon, Rook, CA, 4
torn of front	DST Revt CA X3	Self- append	834	DIT_ReeK_CA_X3	067_Red_C6_X3
torecal-trust	Additivest, Determal, CA, Rent	Self-	834	AddTrust_External_CA_Root	AddTroat_External_CA_Root
tomat-trust	008.0078.0079	Self- signal	104	og-bow.com	012-2018-004
formati truat	Effective Galacture Case2	Self-	10.0	Pfeieler_GubaRost_Cass_3	T-fereface, Globalkovi, Cass, 3
formation with	Dis Cert. Clubal Root. 62	Self	10.00	DipCet_Cole=_Root_C2	DigiCert_Clubal_Rolt_G2

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。

cp.bora.com.pem
omcat-trust
rust-certs
roduct-cpi
rust Certificate

Certificate File Data

[*
Version: V3	
Serial Number: 5C35B3A89A8974719BB85B6A92CF710D	
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	11

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: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ティング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 (<u>https://{FQDN}:8443/cmplatform</u>)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。

Certificate Li					
R. Correcto	Set agreet 🖓 Uptoor Certificate Certificate states 限 General	018			
		superior.			
tempet-trust	thanks Romany, Real, CA 60	Self- regreed	854	thanks, himany, And, 54, -, 63	thanks_Primary_Root_CA00
formulation and	SisterSies	Self- signed	86	ClubalSign	GabelSign
formost-trust	EE Certification Centre Root, CA	Salt- agend	8.54	EE_Dertification_Dertite_Root_DA	RE_Certification_Centre_Root_CA
tomost-trust	SisterSion April CA	Salf- signed	8,54	GlobalSign_Root_CA	Global Sign_Asst_CA
formulation and	TRCA And, Certification Authority	Sall- support	8.54	TeCA, Root, Certification, Authority	TitiCA_Root_Certification_Authority
tempat-trust	Reviews, Case, 3, Root, CA	Self- regreed	854	hvypen, Cees_3_Root_GA	Become, Cam, 3, Root, CA
formulation wat	Darfield Services Asiat Certificate Authority - 52	Self- signed	8.54	Darfeld_Services_Root_Certificate_Authority_~_52	Barfaid_Services_Root_Certificate_Authority62
tomost-trust	Verbier, Dass 3, Public, Nimary, Cathletion, Autority, 1	545	854	verdigs, Cess, 3, Adds, Primary, Certification, Authority, -	verlige, Daw, 3, Public, Primary, Certification, Authority,
					200
tomost trust	NUMBER OF COMPANY	served.	1.54	COLUMN TOLLOW	APPR DATES
Internal level	Manu Citizi Celification Authority	Contra da	10.00	Rang_Didal_Cellication_Authority	xRamp_Clubal_Cartification_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 -

L	Version: V3		
	Serial Number: 68FE55F56F863110B44D835B825D84D3		
L	SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)	-	
L	Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US		
L	Validity From: Thu Dec 05 06:51:10 PST 2019		
L	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		
L	Key: RSA (1.2.840.113549.1.1.1)		
L	Key value:		
	3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb		
	9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065		
	7096e81d65bdcd0cadbcbdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c	_	
	a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e	-	
	c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004	1	

Delete

Download .PEM File

Download .DER File

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: <u>CVP設定ガイド – セキュリティ</u>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、『 <u>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</u> <u>合[Cisco Unified Customer Voice Portal]:シスコのユーザガイド</u>』を参照してください。

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 セキュリティ</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 PCCE自己署名証明書 PCCE 12.6
- <u>CA署名付き証明書の実装: CCE 12.6</u>
- ・ <u>CCE OpenJDKの移行</u>
- ・ <u>CVP OpenJDKの移行</u>
- 証明書交換ユーティリティ
- ・ <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。