SPOGのPCCEコンポーネント証明書の管理

内容

概要

このドキュメントでは、Admin Workstation(AW)の自己署名SSL証明書をCustomer Voice Portal(CVP)、Finesse、Cisco Enterprise Chat and Email(ECE)、Cisco Unified Intelligence Center(CUIC)、Cisco Identity Service(idS)、およびVirtualized Voice Browser(VVB)にに交換するの方法について説明しますPackage Contact Center Enterprise(PCCE)Single Pane of Glass(SPOG)。

著者：Cisco TACエンジニア、Nagarajan ParamasivamおよびRobert Rogier

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。

- Packaged/Unified Contact Center Enterprises(PCCE/UCCE)
- VOSプラットフォーム
- 証明書管理
- 証明書キーストア

使用するコンポーネント

このドキュメントの情報は、次のコンポーネントに基づいています。

- アドミンワークステーション(CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC、IDS
- VVB
- Cisco ECE

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、初期（デフォルト）設定の状態から起動しています。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。

PCCE PCCE

新しいユーザインターフェイス – SPOG

Packaged CCE 12.0には、他のコンタクトセンターアプリケーションに従った新しいユーザインターフェイスがあります。ユーザインターフェイスを使用すると、1つのアプリケーションでソリューションを設定できます。新しいUnified CCE Administration(https://<IP Address>/cceadmin)にサインインします。<IP Address>は、サイドAまたはサイドBのUnified CCE AWのアドレス、またはオプションの外部HDSのアドレスです。

このリリースでは、Unified CCE Administrationインターフェイスを使用して、次の設定を行うことができます。

- キャンペーン
- Courtesy Callback
- SIP サーバ グループ
- ファイル転送：ファイル転送は、プリンシパルAW（2000エージェント展開ではサイドA AW、4000エージェント展開および12000エージェント展開では設定AW）でのみ可能です。
- ルーティングパターン：Unified CVP Operations Consoleの着信番号パターンは、Unified CCE Administrationではルーティングパターンと呼ばれるようになりました。
- 場所：Unified CCE Administrationでは、ルーティングコードがサイトIDではなくロケーションプレフィックスになりました。
- デバイス設定:Unified CCE Administrationでは、次のデバイスを設定できます。CVPサーバ、CVPレポートサーバ、VVB、Finesse、アイデンティティサービス（シングルサインオンのセットアップ）。
- チームリソース：Unified CCE Administrationでは、エージェントチームに次のリソースを定義して関連付けることができます。コール変数のレイアウト、デスクトップレイアウト、電話帳、ワークフロー、理由（受信不可、サインアウト、まとめ）
- 電子メールとチャット

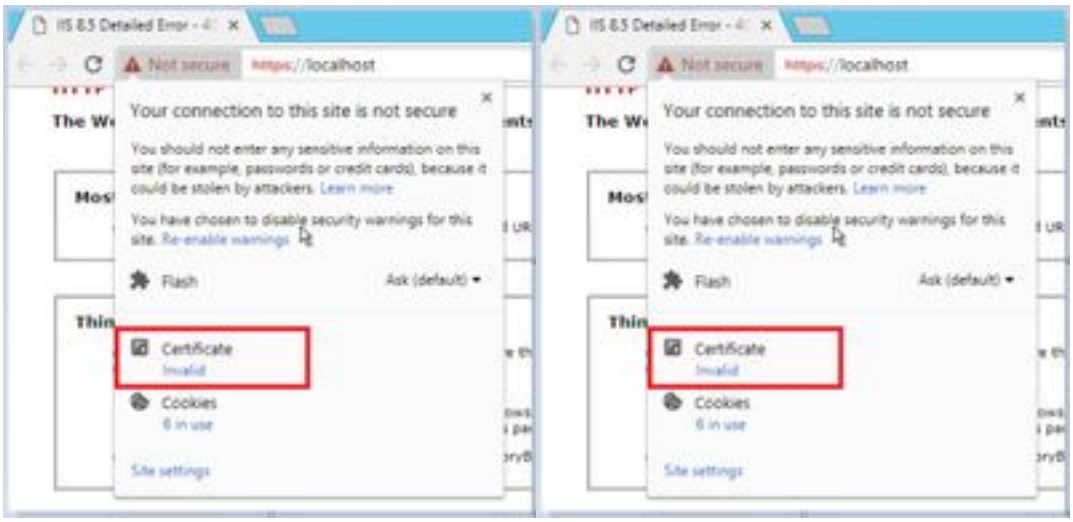
SPOGを通じてシステムを管理する前に、Customer Voice Portal(CVP)、Finesse、Cisco Enterprise Chat and Email(ECE)、Cisco Unified Intelligence Center(CUIC)、Cisco Identity Service(idS)、Virtual Voice Browser(VVB)間で証明書をを交換する必要がありますとAdmin

Workstation(AW)を使用して、信頼関係を確立します。

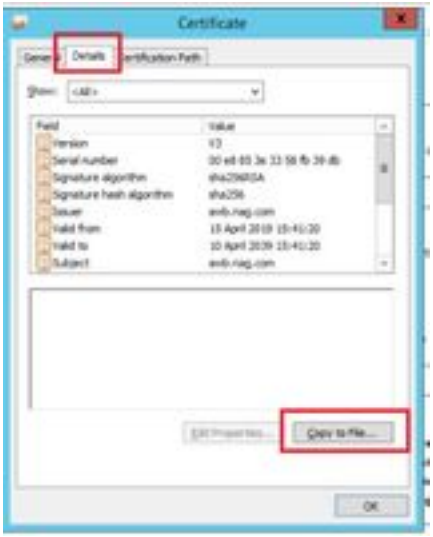
SSL証明書のエクスポート

Administration Workstation(AW)

ステップ1:AWサーバのhttps://localhost URLにアクセスし、サーバSSL証明書をダウンロードします。



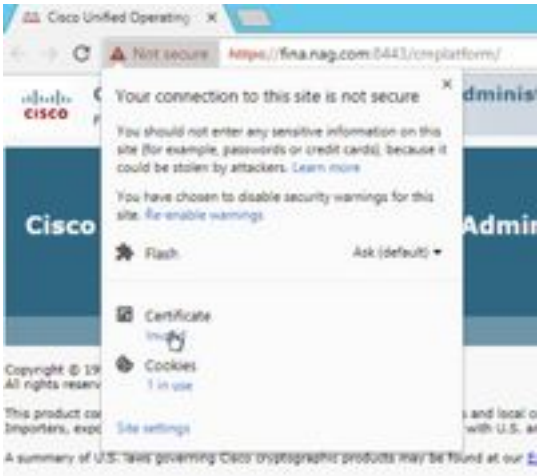
ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。



ステップ3:Base-64 encoded X.509(CER)を選択し、証明書をローカルストレージに保存します。

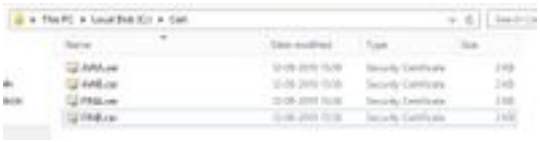
Finesse

ステップ1:https://Finesseserver:8443/cmplatformにアクセスし、tomcat証明書をダウンロードします。



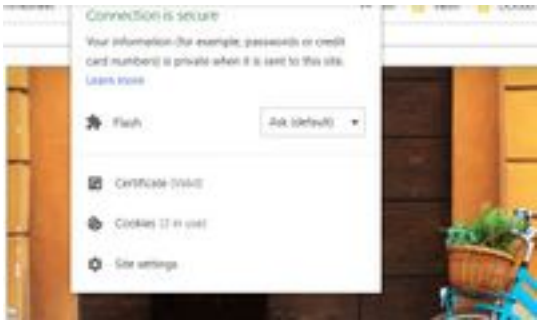
ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。



Cisco ECE

ステップ1:https://ECEWebServerにアクセスし、サーバのSSL証明書をダウンロードします。



ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

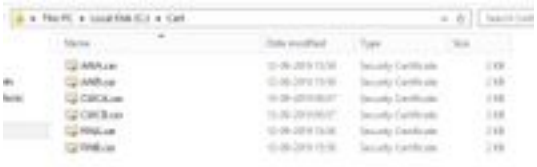
ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

CUIC

ステップ1:https://CUICServer:8443/cmplatformにアクセスし、tomcat証明書をダウンロードします。

ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

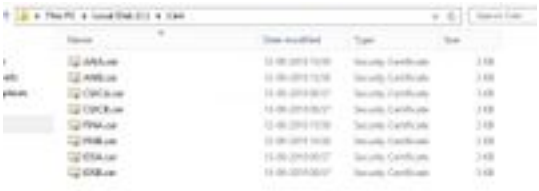


Cisco IDS

ステップ1:https://IDSServer:8553/idsadmin/にアクセスし、tomcat証明書をダウンロードします。

ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。

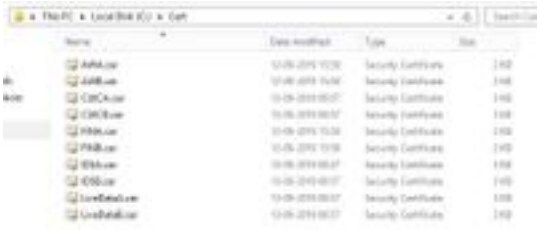


ライブデータ

ステップ1:https://LiveDataServer:8444/cuic/gadget/LiveData/にアクセスし、tomcat証明書をダウンロードします。

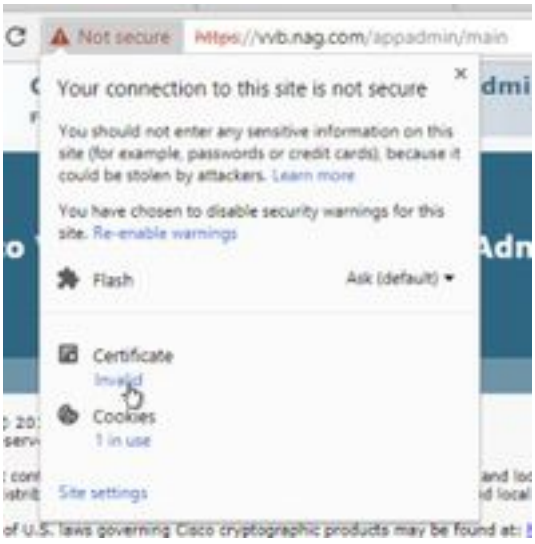
ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。



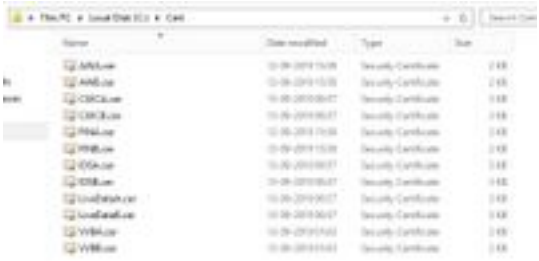
VVB

ステップ1:https://VVBServer/appadmin/mainにアクセスし、tomcat証明書をダウンロードします。



ステップ2：証明書ウィンドウで、[Details]タブに移動し、[Copy To File]ボタンをクリックします。

ステップ3:[Base-64 encoded X.509 (CER)]を選択し、証明書をローカルストレージに保存します。



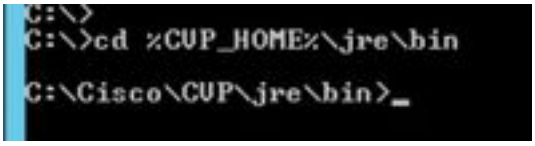
キーストアへのSSL証明書のインポート

CVPコールサーバおよびレポートサーバ

ステップ1:CVPサーバにログインし、AW CCE Admin証明書を**C:\cisco\cvp\conf\security**にコピーします。

ステップ2:%**CVP_HOME%\conf\に移動し、**security.propertiesを開いてキーストアパスワードをコピーします。

ステップ3：コマンドプロンプトをadministratorとして開き、コマンド**cd %CVP_HOME%\jre\binを実行します。**



ステップ4：このコマンドを使用して、AW証明書をCVPサーバにインポートします。

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

ステップ5：パスワードプロンプトで、security.propertiesからコピーしたパスワードを貼り付けます。

ステップ6：証明書を信頼**する**ためにyesと入力し、結果が**Certificate was added to keystoreであることを確認します。**

ステップ7：インポートの成功とともに警告が表示されます。これは、独自の形式であるキーストアが原因で、無視できます。

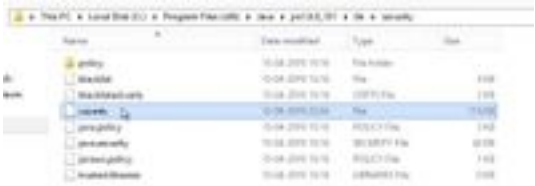
警告：

JCEKSキーストアは独自の形式を使用します。「keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12」を使用して、業界標準の形式であるPKCS12に移行することを推奨します。

アドミンワークステーション

ステップ1:AWサーバにログインし、管理者としてコマンドプロンプトを開きます。

ステップ2:C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file existに移動します。



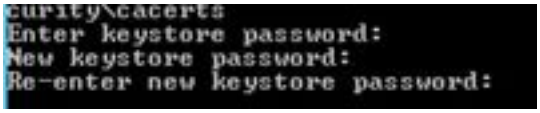
ステップ3：**コマンドcd %JAVA_HOME%を入力し**て入力します。

ステップ4：このコマンドを使用して、Finesse証明書をAWサーバにインポートします。

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-keystore.\lib\security\cacerts

ステップ5：このキーツールを初めて使用するときは、パスワードchangeitを使用して、証明書ストアのパスワードを変更します。

ステップ6：キーストアの新しいパスワードを入力し、パスワードを確認するために再入力します。



ステップ7：証明書を信頼するために「yes」と入力し、結果「Certificate was added to keystore.

注：ステップ1 ~ 7は、他のすべてのFinesseノードとすべてのCUICノードでも繰り返す必要があります

ステップ8：キーストアのパスワードが誤って入力された場合、またはリセットせずにステップを実行した場合、この例外が発生すると予想されます。

この証明書を信頼しますか？[no]: あり

証明書がキーストアに追加されました

keytoolエラー：java.io.FiNotFoundException:.\lib\security\cacerts （指定されたパスが見つかりません）

キーストアのパスワードを入力：
keytoolエラー：java.io.IO例外：キーストアが改ざんされているか、パスワードが正しくありません

ステップ9：キーストアパスワードを変更するには、このコマンドを使用して、ステップ4から新しいパスワードを使用して手順を再度再起動します。

keytool -storepasswd -keystore \lib\security\cacerts

ステップ10：インポートが成功したら、次のコマンドを使用してキーストアからの証明書を表示します。

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse、CUIC、Cisco idS、およびVVB

ステップ1:FinesseサーバのOS管理ページにログインし、tomcat信頼でAW SSL証明書をアップロードします。

ステップ2:[OS Administration] > [Security] > [Certificate Management]に移動します。

ステップ3:[Upload Certificate\Certificate Chain]をクリックし、ドロップダウンから[tomcat-trust]を選択します。

ステップ4：ローカルストレージの証明書ストアを参照し、[Upload]ボタンをクリックします。

ステップ5：手順を繰り返して、すべてのAWサーバ証明書をFinesseクラスタにアップロードします。

tomcat-trust

ステップ6：証明書の変更を有効にするには、tomcatサービスを再起動します。

ステップ7:CUIC、IDS、およびVVBでは、2 ~ 4の手順に従ってAW証明書をアップロードします。

FinesseとCUIC/LiveData間の証明書交換

ステップ1:Finesse、CUIC、およびLiveData証明書を別のフォルダに保存します。

2:[Finesse][CUIC][LiveData OS Administration]ページにログインします。

ステップ3:[OS Administration] > [**Security**] > [**Certificate Management]に移動します。**

ステップ4:[Upload Certificate\Certificate Chain]をクリックし、ドロップダウンから[tomcat-trust]を選択します。

ステップ5：ローカルストレージ内の証明書ストアを参照し、次のように[いずれかのサーバ証明書]を選択し、[アップロード]ボタンをクリックします。

Finesseサーバ：Tomcat信頼としてのCUICおよびLiveData

CUICサーバの場合 – FinesseおよびLiveDataをtomcat信頼として

LiveData Server - Tomcat信頼としてのCUICおよびFinesse

> **注：**tomcat-trust証明書をセカンダリノードにアップロードする必要はありません。これは自動的に複製されます。

ステップ6：証明書の変更を有効にするために、各ノードでtomcatサービスを再起動します。