FinesseとCTIサーバ間のセキュアな通信の設定

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 設定 CCE CTIサーバセキュア Finesseセキュア設定 <u>エージェントPG証明書の生成(CTIサーバ)</u> CAによって署名されたCSR証明書の取得 CCE PGのCA署名付き証明書のインポート Finesse証明書の生成 CAによるFinesse証明書の署名 Finesseアプリケーションおよびルート署名証明書のインポート 確認 トラブルシュート

概要

このドキュメントでは、Cisco Contact Center Enterprise(CCE)ソリューションのCisco Finesseと Computer Telephony Integration(CTI) Server間に認証局(CA)署名付き証明書を実装する方法につ 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。

- CCEリリース12.0(1)
- Finesse リリース12.0(1)
- ・CTI サーバ

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。

- Packaged CCE(PCCE)12.0(1)
- Finesse 12.0(1)

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。

背景説明

CCEバージョン11.5で、シスコはTransport Layer Security(TLS)バージョン1.2のサポートを開始 しました。これにより、Session Initiation Protocol(SIP)およびReal-time Transport Protocol(RTP)メッセージをTLS 1.2経由でで安全ににににできます。シスコは、コンタクトセン ターのほとんどのコールフローでTLS 1.2のサポートを開始しました。インバウンドおよびアウト バウンド音声、マルチチャネル、および外部データベースdip。このドキュメントでは、インバウ ンド音声、特にFinesseとCTIサーバ間の通信に焦点を当てています。

CTIサーバは、次の接続モードをサポートしています。

- ・セキュリティで保護された専用接続:CTIサーバとCTIクライアント(Finesse、ダイヤラ、 CTIOS、およびctitest)間のセキュアな接続を許可します。
- ・セキュア接続と非セキュア接続(混合モード):CTIサーバとCTIクライアント間のセキュアでない接続だけでなく、セキュリティ保護も可能です。これはデフォルトの接続モードです。
 このモードは、以前のリリースをCCE 12.0(1)にアップグレードするときに設定されます。

注:非セキュア専用モードはサポートされていません。

設定

CCE CTIサーバセキュア

ステップ1:PCCEアドミニストレーティブワークステーション(AW)で、**Unified CCE Toolsフォル** ダを開き、Peripheral Gateway Setupをダブルクリックします。



ステップ2:**CG**3Aを選択し、Editをクリックします。

| Cisco Unified ICM/Contact Center Enterprise Compor | nents Setup |
|---|---|
| ICM Instances Add Edit Delete Delete To set up Administration Data Server (Distributor AW), Router, Logger, N Interface Controller (NIC), WebView or Network Gateway components, u Web Setup tool. To set up Administration Client (Client AW), use the Administration Client and Setup tool. To set up Administration Client (Client AW), use the Administration Client and Setup tool. The Instance cc cannot be deleted because it has components set up B Web Setup or Administration Client Setup tool. You must use the applica to semove those components before deleting the instance in Peripheral O Setup. | Add EdR Delete letwork use the Installer by the bile tool Gateway |
| Help | xit Setup |

ステップ3:CTIサーバのプロパティで、[**Next**]をクリッ**クします**。CG3Aサービスの停止に関する セットア**ップに関する質問**で、[はい]を**選択します**。

ステップ4:[**CTI Server Components Properties**]で**、[Enable Secured-only mode]を選択します。** 次の演習で**は、Finesseで同じポートを設定する必要があ**るため、[Secured Connection Port (46030)]に注意してください。[next] をクリックします。

| CTI Server Component Properties |
|--|
| CTI Server configuration |
| Secured Connection Port 46030 |
| Non-Secured Connection Port 42027 |
| Agent Login Required for Client Events |
| Help < Back Next > Cancel |

注:デフォルトのセキュアな通信は42030ですが、このドキュメントで使用する実習は 40630です。ポート番号は、ICMシステムIDを含む式の一部です。システムIDが1(CG1a)の 場合、デフォルトのポート番号は通常42030です。ラボのシステムIDが3(CG3a)であるため 、デフォルトのポート番号は46030です。 ステップ5:[CTI Network **Interface Properties]で[**Next]をクリック**します**。[Setup Information]をオン**にして、[Next**]をクリ**ックします**。

| | NCCE POSetup: CC-COSM | × |
|--|---|---|
| eck Setup Information | | Z |
| Setup has enough information to beg If you want to review or change and If satisfied, click Next to begin config | in the configuration operation. of the settings, click Back. uring the CTI Gateway. | |
| Current Settings: | | |
| Setup Type: CTI Gateway, side A | | ^ |
| Target Directory: C:ljicm | | = |
| Configuration: PG node is pccealin1p CTI Gateway is simplexed DMP address is 3 | | |
| | | |

ステップ6:図に示すように、[Finish]をクリックします。

| Unified ICM/CCE PGSetup: cc-CG3A | | | |
|----------------------------------|---|--|--|
| 2 2 | Setup Complete PGSetup is complete. You may start the Unified ICM/CC Node Manager service now by checking the box below. Yes, start the Unified ICM/CC Node Manager Click Finish to Complete Setup. | | |
| < Back Finish Cancel | | | |

ステップ7:[Exit Setup]をクリックし、図に示すようにセットアップウィンドウが閉じるまで待ちます。

| ICM Instances | Instance Components | |
|---|--|---|
| Add | AW 0034 | Add |
| | LoggesA PC1A | |
| Edit | PG2A | Edit |
| Delete | PG3A RoutetA | Delete |
| | | |
| To set up Administration Data S Interface Controller (NIC), Web | erver (Distributor AW), Router, Lo View or Network Gateway compor | gger, Network ents, use the |
| To set up Administration Data S Interface Controller (NIIC), Web? Web Setup tool. To set up Administration Client (and Setup tool. | erver (Distributor AW), Router, Lo View or Network Gateway compor (Client AW), use the Administration | gger, Network ents, use the Client Installer |
| To set up Administration Data S Interface Controller (NIC), Web Web Setup tool. To set up Administration Client (and Setup tool. The Instance cc cannot be del Web Setup or Administration Cl o remove those components b Setup. | erver (Distributor AW), Router, Lo View or Network Gateway compor (Client AW), use the Administration eted because it has components s ient Setup tool. You must use the efore deleting the instance in Perip | gger, Network ents, use the Client Installer et up by the applicable tool wheral Gateway |

ステップ8:PCCEAllin1デスクトップで、[Unified CCE service Control]をダブルクリックします。

ステップ9:[Cisco ICM cc CG3A]を選択し、[Start]をクリ**ックします**。

Finesseセキュア設定

ステップ1:Webブラウザを開き、[Finesse Administration]に移動します。

ステップ2:図に示すように、[Contact Center Enterprise CTI Server Settings]セクションまで下 にスクロールします。

| Contact Center Enterprise CTI Server Settings | | | | | | |
|---|---|--|--------------|--|--|--|
| Note: Any changes made to Contact Center Enterpris | the settings on this gadget req te CTI Server Settings | uire a restart of Cisco Finesse Torncat to | take effect. | | | |
| A Side Host/IP Address* | 10.10.10.10 | B Side Host/IP Address | | | | |
| A Side Port* | 42027 | B Side Port | | | | |
| Peripheral ID* | 5000 | | | | | |
| Enable SSL encryption Save Revert | | | | | | |

ステップ3:前の演習でCG3Aに設定したセキュア通信ポートのA側ポートを変更します。 46030.「Enable SSL encryption」にチェックを入れ、「Save」をクリックします。

| Contact Center Ent | erprise CTI Server | Settings | |
|---|--|---|-------------|
| Note: Any changes made to Contact Center Enterpris | the settings on this gadge se CTI Server Settings | t require a restart of Cisco Finesse Torncat to t | ake effect. |
| A Side Host/IP Address* | 10.10.10.10 | B Side Host/IP Address | |
| A Side Port* | 46030 | B Side Port | |
| Peripheral ID* | 5000 | | |
| Enable SSL encryption | n | | |

注: 接続をテストするには、まずFinesse Tomcat Serviceを再起動するか、Finesseサーバ を再起動する必要があります。

ステップ4:[Finesse Administration]ページからログアウトします。

ステップ5:FinesseでSSHセッションを開きます。

ステップ6:FINESSEA SSHセッションで、次のコマンドを実行します。

utils system restart

システムを**再起動す**るかどうかを確認するメッセージが表示されたら、yesと入力します。



エージェントPG証明書の生成(CTIサーバ)

CiscoCertUtilsは、CCEバージョン12でリリースされた新しいツールです。このツールを使用して、着信音声のすべてのCCE証明書を管理します。このドキュメントでは、次のCiscoCertUtilsを使

用して、ペリフェラルゲートウェイ(PG)証明書署名要求(CSR)を生成します。

ステップ1:次のコマンドを実行して、CSR証明書を生成します。CiscocertUtil /generateCSR

C:\Users\Administrator.CC> C:\Users\Administrator.CC>CiscocertUtil /generateCSR Key already exists at C:\icm\ssl\keys\host.key. It will be used to generate the CSR. SSL config path = C:\icm\ssl\cfg\openssl.cfg SYSTEM command is C:\icm\ssl\bin\openssl.exe req =new =key C:\icm\ssl\keys\host. key =out C:\icm\ssl\certs\host.csr You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be adefault value. If you enter '.', the field will be left blank.

次のように、要求された情報を入力します。

国名: JP

都道府県:MA

局所名:BXB

組織名:『シスコ

組織単位:CX

一般名: PCCEAllin1.cc.lab

[Email] : jdoe@cc.lab

チャレンジパスワード:トレイン1ng!

オプションの会社名:『シスコ

ホスト証明書とキーは、C:\icm\ssl\certsおよびC:\icm\ssl\keysに保存されます。

ステップ2: C:\icm\ssl\certsフォルダに**移動**し、**host.csr**ファイルが生成さ**れていることを**確認しま す。

CSR証明書の取得 CAによる署名

CSR証明書を生成したら、サードパーティCAによって署名される必要があります。この演習では 、ドメインコントローラにインストールされたMicrosoft CAをサードパーティCAとして使用しま す。

Microsoft CAを使用する場合は、図に示すように、CAによって使用される証明書テンプレートに クライアント認証とサーバ認証が含まれていることを確認します。

| Properties of New Template | ons | |
|--|--|--|
| Subject Name Server Issuance Requirements Compatibility General Request Handling Cryptography Key Attestation Superseded Templates Extensions Security To modify an extension, select it, and then click Edit. Extensions included in this template: | tificate Templates More Actions b Server More Actions Edit Application F | (DC.cc.lab) |
| Application Policies Basic Constraints | An application policy defi | Add Application Policy |
| Certricate Template Information Issuance Policies | Application pglicies: Server Authentication | An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template. Application policies: |
| Edt Description of Application Policies: | <u>A</u> dd | Any Purpose Attestation Identity Key Certificate Certificate Request Agent Elent Authentication Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption |
| OK Cancel Apply Help | ☐ <u>Make this extension c</u> | Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator New OK Cancel |
| 1 | | |

ステップ1:Webブラウザを開き、CAに移動します。

0

ステップ2:[Microsoft Active Directory Certificate Services]で、[Request a certificate]を選択します

| C C Microsoft Active Directory × |
|---|
| Microsoft Active Directory Certificate Services cc-DC-CA Home |
| Welcome |
| Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. |
| You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. |
| For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> Documentation. |
| Select a task: Request a certificate view the status of a pending certificate request Download a CA certificate, certificate chain, or CRL |

ステップ3:拡張証明書要求オプシ**ョンを選択**します。

| Micr | rosoft Activ | e Directory Co | ertifical × + | | | | |
|----------------------|--------------------------|----------------|------------------------|-----------------|-----------|---------|--|
| \leftrightarrow | Сю | | 🛈 윮 https://dc. | clab/certsrv/en | -us/certr | qus.asp | |
| CUCM | 🛅 CUIC | 🛅 Finesse | 🛅 Remote Expert Mobile | 🛅 MediaSense | CVP | CCE | |
| Microsoft | Active Dir | ectory Certifi | icate Services cc-DC-0 | CA | | | |
| Request | a Certif | icate | | | | | |
| Select the User (| e certific Certificat | ate type: e | | | | | |
| Or, subm | it an <u>adv</u> | anced cer | rtificate request. | | | | |

ステップ4:高度な証明書**要求で、PG Agent CSR証明書の内容をコ**ピーし、[Saved Request]ボ ックスに貼り付**け**ます。

ステップ5:クライアントおよびサー**バ認証を使用**した**Web**サーバテンプレートを選択します。 ラボでは、CC Webサーバテンプレートがクライアントとサーバの認証で作成されました。

| To submit a sav Saved Request | ved request to the CA, part t box. | Copy and paste the of the expected CS | e contents SR file |
|---|---|---|-----------------------|
| Saved Request: | | | _ |
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | 3Lhn1D3GsLbIYivb7lbshW: gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg261 rArT900dxJem END CERTIFICATE RI < | fqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h c38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd CQUESTsna | • |
| Certificate Templ | ate: | | |
| C | CC Web Server | ~ | _ |
| Additional Attribu | ites: | | |
| Attributes: | | | _ |

ステップ6:[Submit]をクリ**ックします**。

ステップ7:[Base 64 encoded]を選択し、図に示すように[Download Certificate]をクリックします。

Microsoft Active Directory Certificate Services -- cc-DC-CA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

| | _ |
|--|---|
| 3.3.3.3.7 | |
| NO | |
| 0.000 | |
| Contraction of Contra | |
| | |

Download certificate Download certificate chain

ステップ8:ファイルを保存し、[OK]をクリックします。ファイルはDownloadsフォルダに保存さ れます。

ステップ9:ファイルの名前をhost.cerに変更します(**オプシ**ョン)。

ステップ10:ルート証明書も生成する必要があります。CA証明書ページに戻り、[Download a CA certificate, certificate chain, or CRL]を選択します。ルート証明書はすべてのサーバ(PGエー ジェントとFinesse)で同じになるため、この手順を1回だけ実行する必要があります。

Microsoft Active Directory Certificate Services - cc-DC-CA Welcome Use this Web site to request a certificate for your Web browser, e people you communicate with over the Web, sign and encrypt me security tasks. You can also use this Web site to download a certificate authority status of a pending request. For more information about Active Directory Certificate Services, Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRI

ステップ11:[Base 64]をクリックし、[Download CA certificate]を選択します。

| Microsoft Active Directory Certificate Services - cc-DC-CA |
|---|
| Download a CA Certificate, Certificate Chain, or CRL |
| To trust certificates issued from this certification authority, |
| To download a CA certificate, certificate chain, or CRL, se |
| CA certificate: |
| Current (cc-DC-CA) |
| Encoding method: |
| ODER ⊛Base 64 |
| Install CA certificate |
| Download CA certificate |
| Download CA certificate chain |
| Download latest base CRL |
| Download latest delta CRL |
| |

ステップ12:[Save File]をクリックし、[**OK**]を選**択します**。ファイルはデフォルトの場所であるダ ウンロ**ードに保存されます**。

CCE PGのCA署名付き証明書のインポート

ステップ1:PGエージェントでC:\icm\ssl\certsに移動し、ルートとPGエージェントの署名**されたフ** ァイルをここに貼り付けます。

ステップ2:c:\icm\ssl\certs のhost.pem証明書の名前をselfhost.pemに変更します。

ステップ3:c:\icm\ssl\certs フォルダでhost.cerの名前をhost.pemに変更します。

ステップ4:ルート証明書をインストールします。コマンドプロンプトで、CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



ステップ 5: 同じコマンドを実行するアプリケーション署名付き証明書をインストールします。 CiscoCertUtil /install C:\icm\ssl\certs\host.pem



ステップ6:PGを再起動します。Unified CCE Service Controlを開き、Cisco ICM Agent PGを再起動します。

Finesse証明書の生成

ステップ1:Webブラウザを開き、[Finesse OS Admin]に移動します。

ステップ2:OS管理者クレデンシャルでログインし、図に示すように[Security] > [Certificate Management]に移動します。



ステップ3:図に示すように、[Generate CSR]をクリックします。



ステップ4:[Generate Certificate Signing Request]で、デフォルト値を使用し、[Generate]をクリ ック**します。**

| Generate 🖳 Close | gning kequest |
|--|--|
| Status Warning: Generatin | g a new CSR for a specific certificate type will overwrite the existing CSR for that type |
| Generate Certificate : | Signing Request |
| Certificate Purpose** | tomcat |
| Distribution* | FINESSEA.cc.lab |
| Common Name* | FINESSEA.cc.lab |
| Subject Alternate Nar | mes (SANs) |
| Parent Domain | cc.lab |
| Key Type** | RSA |
| Key Length* | 2048 v |
| Hash Algorithm* | SH4256 v |
| Generate Close . indicates require . When the Certifier States and th | ed item. icate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise |

ステップ5:[Generate Certificate Signing Request]ウィンドウを閉じて、[Download CSR]を選択し

ます。

| Show * Settings * Se | ecurity * Software Upgrades * Servi | ices * Help * | |
|----------------------|--------------------------------------|--------------------------|----|
| Certificate List | | | ٦. |
| Generate Self-signed | Upload Certificate/Certificate chain | Generate CSR Download CS | R |

ステップ6:[Certificate Purpose]で[tomcat]を選択し、[Download CSR]をクリックします。

| Download Certificate Signing Request |
|--|
| Download CSR 🖳 Close |
| e Status |
| Certificate names not listed below do not have a corresponding CSR |
| Download Certificate Signing Request |
| Certificate Purpose tomcat |
| Download CSR Close |
| (i) *- indicates required item. |
| |
| < > |

ステップ7:図に示すように、[Save File]を選択して[OK]をクリックします。

| Opening tomcat.csr | | × |
|-----------------------|--|---|
| You have chosen to | o open: | |
| tomcat.csr | | |
| which is: csr | File | |
| from: https:// | /finessea.cc.lab:8443 | |
| What should Firef | <u>B</u> rowse | |
| Save File | | |
| Do this <u>a</u> utor | matically for files like this from now on. OK Cancel | |

ステップ8:[Download **Certificate Signing Request]ウィンドウを閉**じます。証明書は既定の場所に 保存されます([このPC] > [ダウンロード])。

ステップ9:エクスプローラを開き、そのフォルダに移動します。この証明書を右クリックし、名前を変更します。finessetomcat.csr

CAによるFinesse証明書の署名

このセクションでは、前の手順で使用したのと同じMicrosoft CAがサードパーティCAとして使用

注: CAによって使用される証明書テンプレートに、クライアント認証とサーバ認証が含まれていることを確認します。

ステップ1:Webブラウザを開き、CAに移動します。

ステップ2:[Microsoft Active Directory Certificate Services]で、[Request a certificate]を選択します。

| - D X |
|---|
| 🗲 🗇 🖉 https://dc.ec.lab/certsiv/en-us/ 🔎 = 🔒 🖉 Microsoft Active Directory × 🕥 🛧 🎱 |
| Microsoft Active Directory Certificate Services - cc-DC-CA Home |
| Welcome |
| Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. |
| You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. |
| For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u> . |
| Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL |

ステップ3:図に示すように、advanced certificate requestオプションを選択します。



ステップ4:高度な証明書**要求で、**Finesse CSR証明書の内容を[Saved Request]ボックスにコピ ーアンドペーストします。

ステップ5:クライアントおよびサーバ認証を使用するWebサーバテンプレートを選択します。 この実習では、CC Webサーバテンプレートはクライアントとサーバの認証で作成されました。

| Saved Reques | ved request to the CA, par t box. | Copy and paste the of the expected C | e contents SR file |
|---|---|---|-----------------------|
| Saved Request: | | | |
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | SLhnlD3GsLbIYivb7lbshW gWL/H3DRlnRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnHJ J75nKDoyAh7C+F0u9tmg26J rArT900dxJem END CERTIFICATE RJ < | fqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna | < |
| Certificate Temp | late: | | |
| Ľ | CC Web Server | ~ | _ |
| Additional Attrib | utes: | | _ |
| | | | |

ステップ6:[Submit]をクリ**ックします**。

ステップ7:[Base 64 encoded]を選択し、図に示すように[Download certificate]をクリックします

Microsoft Active Directory Certificate Services -- cc-DC-CA

Certificate Issued

0

The certificate you requested was issued to you.

ODER encoded or ●Base 64 encoded

Download certificate Download certificate chain

ステップ8:ファイルを保存し、[OK]をクリックします。ファイルはDownloadsフォルダに保存さ れます。

ステップ9:ファイル名をfinesse.cerに変更します。

Finesseアプリケーションおよびルート署名証明書のインポート

ステップ1:WebブラウザでFinesse OS Adminページを開き、[Security] > [Certificate Management]に移動します。

ステップ2:図に示すように、[Upload Certificate/Certificate chain]ボタンをクリックします。

| Certificate List | |
|---------------------------|---|
| Generate Self-signed | Upload Certificate/Certificate chain |
| Certificate List | |
| Find Certificate List whe | re Certificate |
| | |
| Generate Self-signed | Upload Certificate/Certificate chain Generate CSR |

ステップ3:ポップアップウィンドウで、[Certificate Purpose]に[tomcat-trust]を選択します。

ステップ4:[**Browse...]ボタンをクリック**し、インポートするルート証明書ファイルを選択します。 次に、[開く]ボタンを**クリック**します。

ステップ5 : 説明にtomcatrootcertのように書き込み、図に示すようにUploadボタンをクリックします。

| Upload Certificate/Certific | ate chain | |
|---|--|---|
| Dipload 🖳 Close | | |
| Status Warning: Uploading a cl Upload Certificate/Certific Certificate Purpose* Description(friendly name) Upload File | uster-wide certificate will distribute it to all servers in this cluster cate chain tomcat-trust tomcatrootcert Trowse rootAll.cer | |
| Upload Close | em. | _ |
| ¢ | | > |

ステップ6:「Success:**Certificate Uploadedメッセージ**をクリックしてウィンドウを閉じます。

システムの再起動が要求されますが、最初にFinesseアプリケーション署名付き証明書のアップロードを続行し、システムを再起動できます。

| 🛈 🚯 https://finessea.cc.lab | x8443/cmplatform/certificateUpload.do | | ${\times}$ | ☆ | ≡ |
|--|--|---|------------|---|---|
| Upload Certificate/Certifica | ite chain | | | | |
| Dipload 🔄 Close | | | | | |
| Status Success: Certificate Uplo Restart the node(s) using | aded g the CLI command, "utils system restart". | | | | |
| Upload Certificate/Certific | ate chain | | | | |
| Certificate Purpose* | tomcat-trust | ~ | | | |
| Description(friendly name) | | | | | |
| Upload File | Browse No file selected. | | | | |
| Upload Close | m. | | | | _ |
| < | | | | | > |

ステップ7:[**Upload Certificate/Certificate chain**]ボタンをクリックし**て、**Finesseアプリケーション 証明書をインポートします。

| Certificate List | |
|---------------------------|---|
| Generate Self-signed | Upload Certificate/Certificate chain |
| Contificato List | |
| Certificate List | |
| Find Certificate List whe | re Certificate 💌 begins with 💌 |
| | |
| Generate Self-signed | Upload Certificate/Certificate chain Generate CSR |

ステップ8:ポップアップウィンドウで、[Certificate Purpose]**に[tomcat]**を選**択します**。

ステップ9:[**Browse...]ボタンをクリック**し、Finesse CA署名付きファイルfinesse.cerを選択**します**。次に、[開く]ボタンを**クリック**します。

ステップ10:[Upload]ボタンをク**リック**します。

| pload Certificate/Certific | ate chain | | |
|--|--|-----------------|--|
| Upload 🖳 Close | | | |
| | | | |
| Status | | | |
| i Warning: Uploading a cl | uster-wide certificate will distribute it to all servers | in this cluster | |
| <u> </u> | | | |
| | | | |
| Upload Certificate/Certifi | cate chain | | |
| Upload Certificate/Certifi Certificate Purpose* | tomcat | ~ | |
| Upload Certificate/Certifi Certificate Purpose* Description(friendly name) | tomcat Self-signed certificate | ~ | |

ステップ11:「Success:**証明書がアップロードさ**れました。

ここでも、システムの再起動が要求されます。ウィンドウを閉じて、システムの再起動を続行します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。