# Configurer la communication sécurisée entre Finesse et CTI Server

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration **CCE CTI Server Secure** Configuration sécurisée Finesse Générer un certificat PG d'agent (serveur CTI) Obtenir le certificat CSR signé par une autorité de certification Importer les certificats signés CCE PGs CA Générer un certificat Finesse Signer le certificat Finesse par une autorité de certification Importer les certificats signés de l'application Finesse et de la racine Vérification Dépannage

## Introduction

Ce document décrit comment mettre en oeuvre des certificats signés par l'autorité de certification (CA) entre Cisco Finesse et le serveur CTI (Computer Telephony Integration) dans la solution Cisco Contact Center Enterprise (CCE).

## Conditions préalables

## **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 12.0(1) du CCE
- Finesse Version 12.0(1)
- Serveur CTI

## **Components Used**

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

• Packaged CCE (PCCE) 12.0(1)

• Finesse 12.0(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Dans la version 11.5 de CCE, Cisco a commencé à prendre en charge la version 1.2 de Transport Layer Security (TLS), qui permet le transport sécurisé des messages SIP (Session Initiation Protocol) et RTP (Real-time Transport Protocol) via TLS 1.2. À partir de CCE 12.0 et dans le cadre de la sécurisation des données en mouvement, Cisco a commencé à prendre en charge TLS 1.2 sur la plupart des flux d'appels du centre de contacts : Baisse des données vocales entrantes et sortantes, multicanaux et externes. Ce document est axé sur la voix entrante, en particulier la communication entre Finesse et CTI Server.

Le serveur CTI prend en charge les modes de connexion suivants :

- Connexion sécurisée uniquement : Permet une connexion sécurisée entre le serveur CTI et les clients CTI (Finesse, dialer, CTIOS et ctitest).
- Connexion sécurisée et non sécurisée (mode mixte) : Permet la connexion sécurisée, ainsi que la connexion non sécurisée entre le serveur CTI et les clients CTI. Il s'agit du mode de connexion par défaut. Ce mode sera configuré lors de la mise à niveau des versions précédentes vers CCE 12.0(1).

Note: Le mode non sécurisé uniquement n'est pas pris en charge.

## Configuration

### **CCE CTI Server Secure**

Étape 1. Sur la station de travail administrative PCCE (AW), ouvrez le dossier **Outils Unified CCE** et double-cliquez sur **Configuration de la passerelle d'accès aux périphériques**.



Étape 2. Sélectionnez CG3A et cliquez sur Modifier.

ICM Instances	Instance Compor	ents Add
Edit	PG1A PG2A PG3A PG3A RoutesA	EdR Delete
To set up Administration Data : Interface Controller (NIC) Web	Server (Distributor AW), Route	, Logger, Network
Web Setup tool. To set up Administration Client and Setup tool.	(Client AW), use the Administr	stion Client Installer

Étape 3. Dans les propriétés du serveur CTI, cliquez sur **Suivant**. Pour la question relative à l'arrêt du service **CG3A**, sélectionnez **Oui**.

Étape 4. Dans les **propriétés des composants du serveur CTI**, sélectionnez **Activer le mode sécurisé uniquement.** Notez le **port de connexion sécurisé (46030)**, car vous devez configurer le même port dans Finesse dans l'exercice suivant. Cliquez sur **Next** (Suivant).

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

**Note**: La communication sécurisée par défaut est 42030, mais les travaux pratiques utilisés pour ce document sont 40630. Le numéro de port fait partie d'une formule qui inclut l'ID système ICM. Lorsque l'ID système est 1 (CG1a), le numéro de port par défaut est

généralement 42030. Comme l'ID système du TP est 3 (CG3a), le numéro de port par défaut est 46030.

Étape 5. Dans les **propriétés de l'interface réseau CTI**, cliquez sur **Suivant**. Vérifiez les **informations de configuration** et cliquez sur **Suivant**.

Unified ICM/CCE PGSetup: cc-CG3A	×
Check Setup Information	Z
Setup has enough information to begin the configuration operation. If you want to review or change and of the settings, click Back. If satisfied, click Next to begin configuring 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	
<	>
Installshield	
< gack Next >	Cancel

Étape 6. Cliquez sur Terminer comme indiqué dans l'image.

Unified ICM/CCE PGSetup: cc-CG3A		
1 1	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	

Étape 7. Cliquez sur **Quitter le programme d'installation** et attendez que la fenêtre de configuration se ferme comme indiqué dans l'image.

CC Add Edt Delete	Instance Components AW CG3A Add LoggesA PG1A PG2A PG3A PG3A RoutetA Delete
To set up Administration Data Ser Interface Controller (NIC), WebVie Web Setup tool. To set up Administration Client (Cl and Setup tool.	ver (Distributor AW), Router, Logger, Network w or Network Gateway components, use the ient AW), use the Administration Client Installer
To set up Administration Data Ser Interface Controller (NIC), WebVie Web Setup tool. To set up Administration Client (Cl and Setup tool. The Instance cc cannot be delete Web Setup or Administration Clien to remove those components befor Setup.	ver (Distributor AW), Router, Logger, Network w or Network Gateway components, use the ient AW), use the Administration Client Installer ad because it has components set up by the it Setup tool. You must use the applicable tool are deleting the instance in Peripheral Gateway

Étape 8. Sur le bureau PCCEAllin1, double-cliquez sur Unified CCE service Control.

Étape 9. Sélectionnez Cisco ICM cc CG3A et cliquez sur Démarrer.

### Configuration sécurisée Finesse

Étape 1. Ouvrez un navigateur Web et accédez à Finesse Administration.

Étape 2. Faites défiler jusqu'à la section **Paramètres du serveur CTI du centre de contacts de l'entreprise** comme indiqué dans l'image.

Contact Center Enterprise CTI Server Settings					
Note: Any changes made to Contact Center Enterpris	the settings on this gadget in se CTI Server Settings	equire 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 Reve	rt 🗌				

Étape 3. Modifiez le port latéral A du port de communication sécurisé configuré sur CG3A dans l'exercice précédent : **46030.** Cochez **Activer le chiffrement SSL** et cliquez sur **Enregistrer**.

Contact Center Ent	erprise CTI Server S	iettings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget se CTI Server Settings	require 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*	46030	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption			
Save Reve	rt		

**Remarque** : pour tester la connexion, vous devez d'abord redémarrer Finesse Tomcat Service ou redémarrer le serveur Finesse.

Étape 4. Déconnectez-vous de la page Administration Finesse.

Étape 5. Ouvrez une session SSH avec Finesse.

Étape 6. Dans la session SSH FINESSEA, exécutez la commande suivante :

#### utils system restart

Entrez **yes** lorsque vous êtes invité à redémarrer le système.

```
<sup>A</sup> Using username "administrator".
Command Line Interface is starting up, please wait ...
Welcome to the Platform Command Line Interface
VMware Installation:
2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
Disk 1: 146GB, Partitions aligned
8192 Mbytes RAM
admin:utils system restart
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

#### Générer un certificat PG d'agent (serveur CTI)

CiscoCertUtils est un nouvel outil disponible sur CCE Version 12. Cet outil vous permet de gérer tous les certificats CCE pour la voix entrante. Dans ce document, vous utilisez ces CiscoCertUtils

afin de générer les demandes de signature de certificat des passerelles de périphérique (PG).

Étape 1. Exécutez cette commande pour générer un certificat CSR : CiscocertUtil /generateCSR



Fournir les informations demandées, par exemple :

Nom du pays : États-Unis

Nom de l'État ou de la province : MA

Nom de la localité : BXB

Nom de l'organisation : Cisco

Unité organisationnelle : CX

Nom commun : PCCEAllin1.cc.lab

E-mail : jdoe@cc.lab

Mot de passe de vérification : Train1ng !

Nom de société facultatif : Cisco

Le certificat et la clé de l'hôte sont stockés dans C:\icm\ssl\certs et C:\icm\ssl\keys.

Étape 2. Accédez au dossier C:\icm\ssl\certs et vérifiez que le fichier host.csr a été généré.

### Obtenir le certificat CSR Signé par une autorité de certification

Une fois les certificats CSR générés, ils doivent être signés par une autorité de certification tierce. Dans cet exercice, l'autorité de certification Microsoft installée dans le contrôleur de domaine est utilisée comme autorité de certification tierce.

Assurez-vous que le modèle de certificat utilisé par l'autorité de certification inclut l'authentification du client et du serveur, comme indiqué dans l'image lorsque l'autorité de certification Microsoft est utilisée.

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
Certificate Template Information	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:		Any Purpose Attestation Identity Key Certificate Certificate Request Agent Editoriale Request Agent Editorial Code Station Editorial Code
	Add	CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel Apply Help		OK Cancel

Étape 1. Ouvrez un navigateur Web et accédez à l'autorité de certification.

Étape 2. Dans les services de certificats Microsoft Active Directory, sélectionnez Demander un certificat.

O      O      O      O
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

Étape 3. Sélectionnez l'option de demande de certificat avancée.

Micr	osoft Activ	e Directory Co	ertifical ×	ł				
$\leftrightarrow$	C' ŵ		i 🔒	https://dc.c	c.lab/certsrv/en	-us/certr	qus.asp	
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote E	opert Mobile	🛅 MediaSense	E CVP	🛅 CCE	
Microsoft	Active Dire	ectory Certifi	icate Services	- cc-DC-C	CA			
Request	a Certif	icate						
Select the	e certific Certificat	ate type: e						
Or, subm	it an <mark>adv</mark>	anced cer	rtificate req	uest.				

Étape 4. Sur la **demande de certificat avancée,** copiez et collez le contenu du certificat CSR de l'agent PG dans la zone **Requête enregistrée**.

Étape 5. Sélectionnez le modèle **Web Server** avec authentification client et serveur. Au cours des travaux pratiques, le modèle serveur Web CC a été créé avec l'authentification du client et du serveur.

To submit a sav Saved Request	ved request to the CA, par Copy and paste the t box. Copy and paste the of the expected CS	e contents SR file	P
Saved Request:		_	
Base-64-encoded entificate request CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7IbshWfqH1509jMcZ3uZrciC gWL/H3DR1nRpJtLKfnLGgX5kUAZqin/56HjuGb4h +L3E0yNQ+W9/SJojYzBGnHk38yo1P/I7UsueE30R J75nKDoyAh7C+F0u9tmg26DZaOZ3k9Wo5QzUTPmd rArT9OOdxJem END CERTIFICATE REQUESTsna <	< > ×	
Certificate Templ	ate:		
Additional Attribu	CC Web Server ~	_	
Attributes:		_	

Étape 6. Cliquez sur Soumettre.

Étape 7. Sélectionnez **Base 64 encodé** et cliquez sur **Télécharger le certificat** comme indiqué dans l'image.

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

### Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate Download certificate chain

Étape 8. Enregistrez le fichier et cliquez sur **OK**. Le fichier est enregistré dans le dossier **Téléchargements**.

Étape 9. Renommez le fichier en host.cer (facultatif).

Étape 10. Vous devez également générer un certificat racine. Retournez à la page de certificat de l'autorité de certification, puis sélectionnez **Télécharger un certificat de l'autorité de certification, une chaîne de certificats ou une liste de révocation de certificats**. Vous n'avez qu'à effectuer cette étape une fois, puisque le certificat racine sera le même pour tous les serveurs (Agent PG et Finesse).



Étape 11. Cliquez sur Base 64 et sélectionnez Télécharger le certificat CA.

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 (co-Dict.CA)
Encoding method:
ODER ⊛Base 64
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Étape 12. Cliquez sur Enregistrer le fichier et sélectionnez **OK**. Le fichier sera enregistré à l'emplacement par défaut, **Téléchargements**.

### Importer les certificats signés CCE PGs CA

Étape 1. Sur l'agent PG, accédez à **C:\icm\ssl\certs** et collez les fichiers racine et l'agent PG signés ici.

Étape 2. Renommez le certificat host.pem sur c:\icm\ssl\certs en tant que selfhost.pem.

Étape 3. Renommez host.cer en host.pem sur le dossier c:\icm\ssl\certs .

Étape 4. Installez le certificat racine. À l'invite de commandes, exécutez cette commande : **CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer** 



Étape 5. Installez le certificat signé de l'application exécutant la même commande : **CiscoCertUtil** /install C:\icm\ssl\certs\host.pem



Étape 6. Cycle de la PG. Ouvrez Unified CCE Service Control, puis passez en revue la PG Cisco ICM Agent.

### Générer un certificat Finesse

Étape 1. Ouvrez le navigateur Web et accédez à Finesse OS Admin.

Étape 2. Connectez-vous avec les informations d'identification de l'administrateur du système d'exploitation et accédez à **Security > Certificate Management** comme indiqué dans l'image.



Étape 3. Cliquez sur Generate CSR comme indiqué dans l'image.



Étape 4. Dans la **demande de signature de certificat**, utilisez les valeurs par défaut, puis cliquez sur **Générer.** 

Status         Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type         Generate Certificate Signing Request         Certificate Purpose**         tomcot         Distribution*         FINESSEA.cc.lab         Subject Alternate Names (SANs)         Parent Domain         Key Type**         RSA         Key Length*         2048	Generate Certificate Si	gning Request
Status         Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type         Generate Certificate Signing Request         Certificate Purpose**       v         Distribution*       FINESSEA.cc.lab         Common Name*       FENESSEA.cc.lab         Subject Alternate Names (SANs)         Parent Domain       cc.lab         Key Type**       RSA         Key Length*       2048	🔒 Generate 🛛 🖳 Close	
Status         Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type         Generate Certificate Signing Request         Certificate Purpose**         Itomcat         V         Distribution*         FINESSEA.cc.lab         Subject Alternate Names (SANs)         Parent Domain         Cc.lab         Key Type**         RSA         Key Length*         2048		
Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type         Generate Certificate Signing Request         Certificate Purpose**       v         Distribution*       FINESSEA.cc.lab         Common Name*       FENESSEA.cc.lab         Subject Alternate Names (SANs)         Parent Domain       cc.lab         Key Type**       RSA         Key Length*       2048	Status	
Generate Certificate Signing Request         Certificate Purpose**         Distribution*         FINESSEA.cc.lab         Common Name*         FINESSEA.cc.lab         Subject Alternate Names (SANs)         Parent Domain         cc.lab         Key Type**         RSA         Key Length*         2048	Warning: Generatin	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
Certificate Purpose** tomcat  V Distribution* FINESSEA.cc.lab V Common Name* FINESSEA.cc.lab Subject Alternate Names (SANs) Parent Domain cc.lab Key Type** RSA Key Length* 2048 V	Concrate Contificate	Cloning Request
Distribution* FINESSEA.cc.lab Common Name* FINESSEA.cc.lab Subject Alternate Names (SANs) Parent Domain cc.lab Key Type** RSA Key Length* 2048	Certificate Purpose**	towat v
Common Name* FENESSEA.cc.lab Subject Alternate Names (SANs) Parent Domain cc.lab Key Type** RSA Key Length* 2048	Distribution*	FINESSEA.cc.lab
Subject Alternate Names (SANs)       Parent Domain       cc.lab       Key Type**       RSA       Key Length*       2048	Common Name*	FINESSEA.cc.lab
Parent Domain cc.lab Key Type** RSA Key Length* 2048	Subject Alternate Nar	mes (SANs)
Key Type** RSA Key Length* 2048 V	Parent Domain	cc.iab
Key Length* 2048 v	Key Type**	RSA
	Key Length*	2048 v
Hash Algorithm SHA256	Hash Algorithm*	SHA256 V
	(i) *- indicates require	ed item.
•- indicates required item.	When the Certif	icate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it

Étape 5. Fermez la fenêtre Générer une demande de signature de certificat et sélectionnez

Télécharger CSR.

Show *	Settings *	Security *	Software Upgrades 🍷	Services *	Help *		
Certifica	te List						
Gen	erate Self-sign	ed 🐴 Up	load Certificate/Certificate	chain 💽	Generate CSR	Download CSR	

Étape 6. Dans l'objet du certificat, sélectionnez tomcat et cliquez sur Télécharger CSR.

Download Certificate Signing Request	
Download CSR The Close	
Certificate names not listed below do not have a corresponding CSR	
Download Certificate Signing Request	_
Certificate Purpose*	
Download CSR Close	
indicates required item.	
<	>

Étape 7. Sélectionnez Enregistrer le fichier et cliquez sur OK comme indiqué dans l'image.

Opening tomcat.csr	×
You have chosen to open:	
tomcat.csr	
which is: csr File	
from: https://finessea.cc.lab:8443	
What should Firefox do with this file?	
O Open with Browse	
Save File	
Do this automatically for files like this from now on	
OK Cancel	

Étape 8. Fermez la fenêtre **Télécharger la demande de signature de certificat**. Le certificat est enregistré à l'emplacement par défaut **(Cet ordinateur > Téléchargements)**.

Étape 9. Ouvrez l'Explorateur Windows et accédez à ce dossier. Cliquez avec le bouton droit sur ce certificat et renommez-le : **finessetomcat.csr** 

### Signer le certificat Finesse par une autorité de certification

Dans cette section, la même autorité de certification Microsoft utilisée à l'étape précédente est

utilisée comme autorité de certification tierce.

**Remarque** : assurez-vous que le modèle de certificat utilisé par l'autorité de certification inclut l'authentification du client et du serveur.

Étape 1. Ouvrez un navigateur Web et accédez à l'autorité de certification.

Étape 2. Dans les services de certificats Microsoft Active Directory, sélectionnez Demander un certificat.

- • ×
C C C Mitps//dc.ec.lub/certsn/en-us/ D = B 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

Étape 3. Sélectionnez l'option de demande de certificat avancée comme indiqué dans l'image.



Étape 4. Sur la **demande de certificat avancée,** copiez et collez le contenu du certificat CSR Finesse dans la zone **Demande enregistrée**.

Étape 5. Sélectionnez le modèle de serveur Web avec authentification client et serveur. Au cours de ces travaux pratiques, le modèle serveur Web CC a été créé avec l'authentification du client et du serveur.

Microsoft Active	Directory Certificate Services	cc-DC-CA	
Submit a Cert	ificate Request or Renew	val Request	
To submit a say Saved Reques	ved request to the CA, part to the CA, part to the CA, part to the case of the text of tex	Copy and paste the of the expected CS	e contents <sup>PK(</sup> SR file
Saved Request:			_
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7lbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojY2BGnH J75nKDoyAh7C+F0u9tmg26 rArT900dxJem END CERTIFICATE RJ <	fqH1509jMcZ3uZrciC 5kUAZqin/56HjuGb4h k38yolP/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	•
Certificate Temp	late:		_
	CC Web Server	~	_
Additional Attribution	utes:		_
Attributes:		.a	
		Submit >	_

Étape 6. Cliquez sur Soumettre.

Étape 7. Sélectionnez **Base 64 encodé** et cliquez sur **Télécharger le certificat** comme indiqué dans l'image.

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

Certificate Issued

The certificate you requested was issued to you.

ODER encoded or 
 Base 64 encoded
 Download certificate
 Download certificate chain

Étape 8. Enregistrez le fichier et cliquez sur **OK**. Le fichier est enregistré dans le dossier **Téléchargements**.

Étape 9. Renommez le fichier en finesse.cer.

Importer les certificats signés de l'application Finesse et de la racine

Étape 1. Sur un navigateur Web, ouvrez la page **Finesse OS Admin** et accédez à **Security** > **Certificate Management**.

Étape 2. Cliquez sur le bouton Upload Certificate/Certificate chain comme indiqué dans l'image.

rtificate/Certificate chain
begins with
tificate/Certificate chain   Generate CSP

Étape 3. Dans la fenêtre contextuelle, sélectionnez tomcat-trust pour l'objet du certificat.

Étape 4. Cliquez sur le bouton **Parcourir...** et sélectionnez le fichier de certificat racine à importer. Cliquez ensuite sur le bouton **Ouvrir**.

Étape 5. Dans la description, écrivez quelque chose comme **tomcatrootcert** et cliquez sur **Upload** button comme indiqué dans l'image.

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

Étape 6. Attendez de voir la réussite : Message téléchargé du certificat pour fermer la fenêtre.

Vous serez invité à redémarrer le système, mais commencez par télécharger le certificat signé de l'application Finesse, puis vous pourrez redémarrer le système.

🛈 🔏 https://finessea.cc.lab	x8443/cmplatform/certificateUpload.do		. ⊴	☆	$\equiv$
Upload Certificate/Certificate/	ate chain				
Dipload 🖳 Close					
Status Success: Certificate Uplo Restart the node(s) using	aded g the CLI command, "utils system restart".				
Upload Certificate/Certific	cate chain			-	
Certificate Purpose*	tomcat-trust	~			
Description(friendly name)					
Upload File	Browse No file selected.				
Upload Close	m.				
¢					>

Étape 7. Cliquez sur le bouton **Télécharger le certificat/la chaîne de certificats** pour importer le certificat d'application Finesse.

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

Étape 8. Dans la fenêtre contextuelle, sélectionnez tomcat pour l'objet du certificat.

Étape 9. Cliquez sur le bouton **Parcourir...** et sélectionnez le fichier signé de l'Autorité de certification Finesse, **finesse.cer**. Cliquez ensuite sur le bouton **Ouvrir**.

Étape 10. Cliquez sur le bouton Télécharger.

Ittps://finessea.cc.lat	x8443/cmplatform/certificateUpload.do		⋓	습	Ξ
pload Certificate/Certific	ate chain				
👌 Upload 🛛 🔁 Close					
- THE LEY					
Warning: Uploading a clu Upload Certificate/Certific Certificate Purpose*	uster-wide certificate will distribute it to all servers	in this clust	er		
Warning: Uploading a clu Upload Certificate/Certific Certificate Purpose* Description(friendly name)	cate chain tomcat Self-signed certificate	in this clust	er		

Étape 11. Attendez de voir la réussite : Message téléchargé du certificat.

Encore une fois, vous êtes invité à redémarrer le système. Fermez la fenêtre et continuez à redémarrer le système.

## Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.