Gérer le certificat des composants PCCE pour SPOG

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Nouvelle interface utilisateur - SPOG Exportation de certificat SSL Station de travail d'administration (AW) Finesse CEE de Cisco CUIC Cisco idS Données en direct **VVB** Importation de certificat SSL dans le magasin de clés Serveur d'appels CVP et serveur de rapports Station de travail Admin Finesse, CUIC, Cisco idS et VVB Échange de certificats entre Finesse et CUIC/LiveData

Introduction

Ce document décrit comment échanger les certificats SSL auto-signés de la station de travail Admin vers le portail vocal du client (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) et le navigateur vocal virtualisé (VVB) pour le volet de verre unique du centre de contact du package Enterprise (PCCE).

Contribué par Nagarajan Paramasivam et Robert Rogier, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Entreprises de centre de contacts unifiés/groupés (PCCE/UCCE)
- Plate-forme VOS
- Gestion des certificats

Clavier de certificat

Components Used

Les informations de ce document sont basées sur les composants suivants :

- Station de travail Admin (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- CEE de Cisco

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

Il est recommandé de lire et de comprendre le Guide d'administration et de configuration de PCCE, en particulier l'annexe Référence à la fin qui couvre la configuration et la configuration des certificats. <u>Guide d'administration et de configuration de PCCE</u>

Nouvelle interface utilisateur - SPOG

Packaged CCE 12.0 dispose d'une nouvelle interface utilisateur conforme aux autres applications du centre de contacts. L'interface utilisateur vous permet de configurer la solution via une application unique. Connectez-vous à la nouvelle administration Unified CCE à l'adresse https://<IP Address>/cceadmin. <Adresse IP> est l'adresse de l'AW Unified CCE côté A ou B ou du HDS externe facultatif.

Dans cette version, l'interface Unified CCE Administration vous permet de configurer ceci :

- Campagnes
- Avec l'aimable autorisation de Callback
- Groupes de serveurs SIP
- Transferts de fichiers : Le transfert de fichiers n'est possible que par le biais de l'AW principal (Side A AW dans le déploiement d'agents en 2000 et configuré AW dans 4000 déploiements d'agents et 12000).
- Modèles de routage : Le modèle de numéro composé dans Unified CVP Operations Console s'appelle maintenant Routing Pattern dans Unified CCE Administration.
- Emplacements : Dans Unified CCE Administration, le code de routage est désormais le préfixe d'emplacement au lieu de l'ID de site.
- Configuration de périphériques: Unified CCE Administration vous permet de configurer les périphériques suivants : Serveur CVP, serveur de rapports CVP, VVB, Finesse, service d'identité (configuration de connexion unique).
- Ressources de l'équipe : Unified CCE Administration vous permet de définir et d'associer les ressources suivantes pour les équipes d'agents : Disposition des variables d'appel, disposition du bureau, annuaires téléphoniques, Workflows, raisons (Non prêt, Déconnexion, Post-appel).
- E-mail et discussion

Avant de tenter de gérer le système via SPOG, il est nécessaire d'échanger les certificats SSL

entre Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) et Virtual Voice Browser (VVB) et Admin Workstation (AW) afin d'établir une communication de confiance.

Exportation de certificat SSL

Station de travail d'administration (AW)

Étape 1. Accédez à l'<u>URL</u> <u>https://localhost</u> dans le serveur AW et téléchargez les certificats SSL du serveur.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

10 Aug. 1	16.4	-
TETHIN	NO.	
peret number	100 HE 00 18 12 10 10 19 10	- 14
Sprature ageneration	sharting a	
Sector real approve	and that can	
Calif From	15 Arel 2018 15-41-20	
readed too	10 April 2009 18:41:20	
Address	and risk own	124

Étape 3.Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.



Finesse

Étape 1. Accédez au site https://Finesseserver:8443/cmplatform et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

	the PC + Louistie Kit + Gel.			- 6	100010
	New *	the extract	fight.	140	
é.	Carlos	12-09-2010 13-08 12-09-2010 13-08 12-09-2011 13-08	Security Centrality Security Centrality Decisity Centrality		240 240
	Spink.co	0.08.200.018	Include Cattlena		346

CEE de Cisco

Étape 1. Accédez au site https://ECEWebServer et téléchargez le certificat SSL du serveur.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

	TALFT & Loud Dok Str.	1 (M)			161	lag-or-line
	Sale.	e.)	Data Insultant	244	-	
	12 answer		2100000000	Investment		198
	and and a		5-14-2251 (212)	Incompliant for the later		110
-	12 ACEAnt		10.00.0000 10.00	Innels Carrier		1198.
	124080		10.00-010175.00	Sample Latters		1.04

CUIC

Étape 1. Accédez au site https://CUICServer:8443/cmplatform et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

	Marca	Internetical.	there .	10.0	
	C. ANALST	10-26-2819 (1):91	Territy Carllinate		101
*	C AND or	10.46-0Pt 19/6	Savorky Cardinale		118
hini i	CROKIE.	0.04-0210-0.07	Density Destitution		118
	CF CHURNER	15-24-2019-06/11	Jacoby Cathlenge		1.44
	Car House	10-09-0019 Talle	Security Centerple		218
	C2 Web.us	10.05.029.039	Saturda Earthrops		218

Cisco idS

Étape 1. Accédez au site https://IDSServer:8553/idsadmin/ et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

	tere .	The suffici	100	
÷.	12 Alphane	12-08-0419-10-08	through Landson	3.68
etc :	LL ANKLO	11-00-07111216	Security Calificate	3.488
nin 😳	To Oblance	11-00-2010-00107	Secure Cardoney	1.00
	THE CONCELSES	14-08-029-030-07	Second Laboration	1.438
	SQ FPH-OF	12-46-2010 12:00	Second Generalized	248
	To Pathon	10 cm land holds	Include Cathlands	0.000
	Cig (Children)	15-00-0291-00/07	South Cardione	248
	California (California)	15-06-0014-06/07	Security Carolinants	1.68

Données en direct

Étape 1. Accédez au <u>site https://LiveDataServer:8444/cuic/gadget/LiveData/</u> et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

	tere .	Des worthalt	101	
	C Antoniour	10/8-201-028	Security Certificate	240
÷.	Contract of the second	to de units mune	belong (militate	3.446
kie:	CE CECKINE	0.44.000.002	Balling Eartholm	1.00
	G Other	15.06.0014.0014	Accuracy (unifying	110
	C Photos	11-09-0713-15-54	Desirely Celificate	198
	C PARA IN	10.05.275.019	Security Centricity	199
	Ci Chian	10-08-00144-00-07	Investor Lintchisen	110
	G2 068.cm	11-16-1249-0017	Delarty Cartillans	149
	G townships of an	12-08-0018-0017	Service Certificate	1.000
	T2 Graduate or	0.26.2214.0037	Intelligity Coldinates	140

VVB

Étape 1. Accédez au site https://VVBServer/appadmin/main et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

there .	The worked	7,97	
Tel Address	0.04 0.010 0.00	Texasty Continues	248
THE AND OF	0.04.044.03	Investigation and a second second	248
 T2 CHCL.m	16 de 2019 de 11	Investig Carolinate	1.68
12 CMORum	100.06-2014-06.07	Density Carthouts	148
12 Mail.or	10.05-001875-008	Daniely Cardions	148
California.com	0.0101103	Density Carolicom	1.01
12-05k.ce	10.00 (000 mm) ¹¹	Tal only Carolician	148
12-018.im	20-08-10700 But	Decard Carolinate	148
Egipodeshcer .	10.04-2019 (0.07	Initially Carolines	148.
Tig lond and on	100 58-2019 50/07	territy Carefulate	1.43
12 Webser	10.05-021915-03	Description that the	148
C2 WHILE	10.00.000000000000000000000000000000000	Canada, Carolinana	1.68

Importation de certificat SSL dans le magasin de clés

Serveur d'appels CVP et serveur de rapports

Étape 1. Connectez-vous au serveur CVP et copiez les certificats AW CCE Admin sur le **site** C:\cisco\cvp\conf\security.

	Tea PC & Local Bad (1) & Char # (1)	of a cost a second		- d. mail mail
	fare 1	Descention	for	In
	13 Heynes	19-08-20912-01	vertilena.	110
18	100 0000	12-24-229-529	Swanty Calificate	2.49
internet.	10 mm	1.46.874.128	Second Generate	1.40

Étape 2. Accédez à **%CVP_HOME%\conf**\ et ouvrez security.properties pour copier le mot de passe du magasin de clés.

	termine and the second se	Sale restlies	Sec.	14	
	(and)	a statement of	International Vision		148
-	Market and a second second				
	the Lat Annual Time Help			-	

Étape 3. Ouvrez l'invite de commandes en tant qu'administrateur et exécutez la commande **cd %CVP_HOME%\jre\bin**.



Étape 4. Utilisez cette commande pour importer les certificats AW sur le serveur CVP.

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

Ching of the database in the second design of the second second

Étape 5. À l'invite du mot de passe, collez le mot de passe copié à partir du fichier security.properties.

Étape 6. Tapez **yes** pour faire confiance au certificat et vous assurer que le **certificat** de résultat **a été ajouté au keystore.**



Étape 7. Un avertissement s'affiche avec l'importation réussie. Ceci est dû au format propriétaire Keystore, vous pouvez l'ignorer.

Avertissement :

Le keystore JCEKS utilise un format propriétaire. Il est recommandé de migrer vers PKCS12, qui est un format standard de l'industrie en utilisant « keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore - deststoretype pkcs12 ».

lare lend	
the ACESS, he matrice many a prophylicities formation, its is recommended for adjoints	10.6 FB
Bill shich is an industry included fields union "hosts" Departmenting	1000 0000
Dates: CryClastar/DiPress/Property/1970/https://doi/of.ing/claster.CryClastar/DiPress/	COLUMN TWO IS NOT
A style between states the barrent barrent subscription of the states of	

Station de travail Admin

Étape 1. Connectez-vous au serveur AW et ouvrez l'invite de commande en tant qu'administrateur.

Étape 2. Accédez à C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.

	Same -	Two resided.	7,94	int.
	il entry	10-04-2010 1010	Roa Automo-	
10 C	(marine	TO DR JERY TURN		110
-	Maintenburts	This Jim total.	100710-004	110
	Courter D	10.04.009.004	No.	114/9
	product .	10104-2010 1010	AND A COMPANY OF	140
	- performantly	10104-0010-1016	many in	0.01
	(an train plotting)	2144-01111-011	RILCOM	
	In stand in some	Trade days have	CONTRACTOR OF STREET, NAME	1.00

Étape 3. Tapez la commande cd %JAVA_HOME% et saisissez.

Civid X	JAVA_HOM	Б¢	
Ci\Progr	an Files	(x86)\Java\jre1.8.8	181)_

Étape 4. Utilisez cette commande afin d'importer les certificats Finesse sur le serveur AW.

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

Conference Filter (and Conversion) E. E. Shi Serence - True Conference Statistics

Étape 5. La première fois que vous utilisez ce keytool, utilisez le mot de passe **changeit** afin de changer le mot de passe d'un magasin de certificats.

Étape 6. Saisissez un nouveau mot de passe pour le Keystore et saisissez-le à nouveau pour confirmer le mot de passe.



Étape 7. Tapez **yes** afin de faire confiance au certificat et de vous assurer que vous obtenez le **certificat** de résultat **a été ajouté à la banque de clés.**

rust this	cert	ificate	?	[no]:	yes
Certificate	Was	added	to	keysto	1.6

Note: Les étapes 1 à 7 doivent être répétées avec tous les autres noeuds Finesse et tous les noeuds CUIC également

Étape 8. Si le mot de passe de la banque de clés a été saisi à tort ou a effectué les étapes sans réinitialiser, il est attendu qu'il obtienne cette exception.

Faire confiance à ce certificat ? [non] : oui

Le certificat a été ajouté à la banque de clés

erreur keytool : java.io.FileNotFoundException : .\lib\security\cacerts (Le système ne trouve pas le chemin spécifié)

Entrez le mot de passe de la banque de clés :

erreur keytool : java.io.IOException : Le magasin de clés a été modifié ou le mot de passe est incorrect

Étape 9. Afin de modifier le mot de passe keystore, utilisez cette commande et redémarrez la procédure à partir de l'étape 4 avec le nouveau mot de passe.

keytool -storepasswd -keystore .\lib\security\cacerts

Er (Deprese Film, Gelli-Janz-Jeri J.B. Hilbertes) -energiannel -laprime -likeporter kontempointeel Per kestere painteel Per kestere painteel Per kestere painteel

Étape 10. Après l'importation réussie, utilisez cette commande pour afficher le certificat à partir du magasin de clés.

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

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



Finesse, CUIC, Cisco idS et VVB

Étape 1. Connectez-vous à la page d'administration du système d'exploitation du serveur Finesse et téléchargez les certificats SSL AW dans l'approbation tomcat.

Étape 2. Accédez à Administration du système d'exploitation > Sécurité > Gestion des certificats.

 Statistical Installer A second s				
A TOTAL STATE	Acres .			
				1000
THE R. LANSING	- 100 1	11/2/10/10	- 577	and a line specific
				il illerer -

Étape 3. Cliquez sur Upload Certificate\Certificate Chain et sélectionnez tomcat-trust dans la liste déroulante.

Étape 4. Parcourez le magasin de certificats dans le stockage local et cliquez sur le bouton Télécharger.



Étape 5. Répétez les étapes pour télécharger tous les certificats de serveur AW dans le cluster Finesse.

Note: Il n'est pas nécessaire de télécharger le certificat tomcat-trust sur le noeud secondaire, il est automatiquement répliqué.

Étape 6. Redémarrez le service tomcat afin que les modifications de certificat prennent effet.

Étape 7. Dans CUIC, IDS et VVB, suivez les étapes de 2 à 4 et téléchargez le certificat AW.

Échange de certificats entre Finesse et CUIC/LiveData

Étape 1. Conservez les certificats Finesse, CUIC et LiveData dans un dossier distinct.

	Nove .	Data-readilities	tum .	tim.	
	(2) EALAry	this present	Second Contraste		int.
60 - E	D DATE:	14-08-0218-0227	Incody Cettlenty		1.00
-	Tail Piloh cost	1244-01114	Sampy Light and		1.00
C today.or C today.or	1100 year	10.05.00 0.04	Investig-Deliferate		198
	The survey of the second secon	11-08-229-0031	Searcy Little Little		100
	The instantion	14.04.014.001	Inches Contrast		1.00

Étape 2. Connectez-vous à la page Finesse, CUIC et LiveData OS Administration.

Étape 3. Accédez à Administration du système d'exploitation > Sécurité > Gestion des certificats.

Étape 4. Cliquez sur Upload Certificate\Certificate Chain et sélectionnez tomcat-trust dans la liste déroulante.

Étape 5. Parcourez le magasin de certificats dans le stockage local et sélectionnez L'un des certificats de serveurs comme ci-dessous, puis cliquez sur le bouton Télécharger.

Dans le serveur Finesse - CUIC et LiveData comme confiance Tomcat

Dans CUIC Server - Finesse et LiveData comme confiance tomcat

In LiveData Server - CUIC et Finesse comme approbation Tomcat

Note: Il n'est pas nécessaire de télécharger le certificat tomcat-trust sur le noeud secondaire, il est automatiquement répliqué.

Étape 6. Redémarrez le service tomcat sur chaque noeud afin que les modifications de certificat prennent effet.