Administrar certificado de componentes PCCE para SPOG

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados **Antecedentes** Nueva interfaz de usuario - SPOG Exportación de certificado SSL Estación de trabajo de administración (AW) Finesse CEPE de Cisco CUIC IDS de Cisco LiveData **VVB** Importación de certificado SSL al almacén de claves Servidor de llamadas y servidor de informes CVP Estación de trabajo de administración Finesse, CUIC, Cisco IDS y VVB Intercambio de certificados entre Finesse y CUIC/LiveData

Introducción

Este documento describe cómo intercambiar los certificados SSL autofirmados de la estación de trabajo de administración (AW) en el portal de voz del cliente (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) y Virtualized Voice Browser (VB) para Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG).

Colaborado por Nagarajan Paramasivam y Robert Rogier, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Empresas de Contact Center empaquetadas/unificadas (PCCE/UCCE)
- Plataforma VOS
- Gestión de certificados

• Almacén de claves de certificado

Componentes Utilizados

La información de este documento se basa en estos componentes:

- Estación de trabajo de administración (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- CEPE 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se recomienda que haya leído y entendido la Guía de administración y configuración de PCCE, específicamente el apéndice de referencia al final que cubre la configuración y configuración del certificado. <u>Guía de configuración y administración de PCCE</u>

Nueva interfaz de usuario - SPOG

Packaged CCE 12.0 tiene una nueva interfaz de usuario que se ajusta a otras aplicaciones del centro de contacto. La interfaz de usuario permite configurar la solución a través de una aplicación. Inicie sesión en el nuevo Unified CCE Administration en https://<IP Address>/cceadmin. <IP Address> es la dirección del Lado A o B Unified CCE AW o del HDS externo opcional.

En esta versión, la interfaz de administración de Unified CCE le permite configurar lo siguiente:

- Campañas
- Devolución de llamada por cortesía
- Grupos de servidores SIP
- Transferencias de archivos: La transferencia de archivos solo es posible a través de AW principal (AW del lado A en la implementación de agentes en 2000 y AW configurado en implementaciones de agentes en 4000 y agentes en 12000).
- Patrones de enrutamiento: El modelo de número marcado en Unified CVP Operations Console se denomina ahora Patrón de enrutamiento en Unified CCE Administration.
- Ubicaciones: En Unified CCE Administration, el código de enrutamiento es ahora el prefijo de ubicación en lugar del ID de sitio.
- Configuración del dispositivo: Unified CCE Administration permite configurar los siguientes dispositivos: Servidor CVP, CVP Reporting Server, VVB, Finesse, Identity Service (configuración de inicio de sesión único).
- Recursos del equipo: Unified CCE Administration permite definir y asociar los siguientes recursos a los equipos de agentes: Diseño de las variables de llamada, Diseño del escritorio, Listas telefónicas, Flujos de trabajo, Motivos (No preparado, Cerrar sesión, Cierre de sesión).
- Correo electrónico y chat

Antes de intentar gestionar el sistema a través de SPOG, es necesario intercambiar los

certificados SSL entre el portal de voz del cliente (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) y Virtual Voice Browser (VB) y Admin Workstation (AW) para establecer una comunicación de confianza.

Exportación de certificado SSL

Estación de trabajo de administración (AW)

Paso 1. Acceda a la<u>URL https://localhost</u> en el servidor AW y descargue los certificados SSL del servidor.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

- (A)-	*	
and the second se	Take	-
renan Senir Aurber Signature algorithm Somature hash algorithm	10 00 et 45 3x 33 58 fb 39 db 94238855A x4x756	
law	and-rag-com	
raid from	18 April 2018 15-41-20	
waited too	10 April 3009 18-40-20	
Adapt	anti-riag-com	

Paso 3.Seleccione Base-64 codificada X.509 (CER) y guarde el certificado en el almacenamiento local.



Finesse

Paso 1. Acceda a https://Finesseserver:8443/cmplatform y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	The PC + Louis Shield (C) + Cell			+ 6	144-1-19
	New T	See endired	tin.	ine.	
	To Arthur	12-09-2019 (16:09	Internet Construction		199
÷	G 446.cm	12-05 2010 (0.0)	Security Continues	6	240
inces:	Ci maint	205.011168	Territy Detricate	č.	110
	California.	0.06.200 0.08	Include Cattlene		144

CEPE de Cisco

Paso 1. Acceda a https://ECEWebServer y descargue el certificado SSL del servidor.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	TRAFT & Louid Date	Ro a Gall			(th) [Instancion
	Sale.		Emp mathe	1. A.	-
	12 answer		2100-0210-0240	Investment	198
	Top well-top		5-14-224 12:28	Incompliant faile	110
-	GRADE AND		10.00.000 10.00	Innaki Cantinee	1198.
	12408-0		10.00.000.05.00	Salaria California	1.64

CUIC

Paso 1. Acceda a https://CUICServer:8443/cmplatform y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	THE P. P. LINE THE R. P. P. LEW.				
	Maria	interesting.	(form	10.0	
	C ANALM	10-09-009-03/06	Includy Cartilly also		110
	C AND on	10.49-301x19/W	Deverty Cardinate		118
inter la	CHOKAN	10 de - prime a con-	(Incode Destination)		118
	CF CHURNER	15.06.2019-06/01	Jacoby (without)		1.64
	The Poly of	10-09-0010 Talle	Security Cathlopie		218
	C2 Well-Las	-0-46-2019 (1-36)	Taxaty Catholics		248

IDS de Cisco

Paso 1. Acceda a https://IDSServer:8553/idsadmin/ y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	tere .	The suffici	100	
÷.	12 Address	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	Security Partness	1.48
	THE OPERATE	14-08-029-030-07	Second Laboration	0.00
	SQ FPH-OF	12-46-2010 12:00	Second General	248
	To Pathon	10 cm land holds	Include Cathlands	0.000
	Cig (Children)	15-00-0291-00/07	South California	248
	California (California)	15-06-0014-06/07	Investo Carolinani	1.00

LiveData

Paso 1. Acceda a <u>https://LiveDataServer:8444/cuic/gadget/LiveData/</u> y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	NoPC & Gold Read of a Cen-			(4) (herein
	here *	Des worthat	1.04	Sec
	C Antoniour	104-011-028	Security Gettillury	140
÷	Contract of the second	101-061-0018-01-02	betung Det/see	3.448
kon i	CE CECKINF	0.44.000.002	Balany Carthole	146
	G Other	15.06.0014.0014	Annually (unifying)	110
	Ci Phon. Lan	10-09-0715-01-04	Security Celificate	198
	(2768.cm)	10.05.275.018	Security Centilians	199
	C Chian	10-08-00144-00-07	Innerty Linthium	1.04
	(1) 000um	114.244-017	Industry Continues	140
	[] liveletator	12-08-0218-08187	Security Certificate	1.00
	T2 Graduitation	Gal 2010000	Intelligite Contributes	140

VVB

Paso 1. Acceda a https://VVBServer/appadmin/main y descargue el certificado tomcat.



Paso 2. En la ventana del certificado, vaya a la ficha Detalles y haga clic en el botón Copiar en archivo.

Paso 3. Seleccione Base-64 codificado X.509 (CER) y guarde el certificado en el almacenamiento local.

	The PC + Long the His + Cell		+ 0	1. 100-11.04
	tere .	The resided	7pr 34	
	Tel Alleboor	0.0400110.00	Terrority Constitution	2.68
÷	TH AND OF	0.04.049.038	Investig-Carefulger	248
	Tel Chica.com	16 de 2019 de 11	Investign Carolinana	1.68
	12 CHORAS	10.06-2014-06.01	Investige Carthouse	118
	12 Healing	10.05-001875-008	Daniely Cardions	148
	CONTRACT.	10-04-07911538	Dennis Cariforni	1.0
	12-05e.or	10.00.000000000	Tal with Carolinian	1.48
	12-018.m	to an internation	Design Tamilane	148
	12 webrahan	100.00-2019-00x17	Telado Cardinate	148.7
	T2 loss and on	10108-0018-0047	Security Carefulate	1.00
	12 Webser	10.05-021010-044	the units of profile pro-	148
	C2 WHILE	10.00 (MILLION ALL)	Canada, Carolinana	1.01

Importación de certificado SSL al almacén de claves

Servidor de llamadas y servidor de informes CVP

Paso 1. Inicie sesión en el servidor CVP y copie los certificados de administrador de AW CCE en el C:\cisco\cvp\conf\security.

	Tea.PC & Local Date (1) & Chan & Ch	t a cost a second		- 41	(Stands into the
	fore 1	Descention	for	100	
	13 Heylere	19-08-001-0-01	vertilena.		110
18	100 0000	12-28-2019-15:08	Swanty Celificate		1.49
id on	Carlos .	1.44.274.118	Second General		1.48

Paso 2. Navegue hasta **%CVP_HOME%\conf**\ y abra security.properties para copiar la contraseña del almacén de claves.

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

Paso 3. Abra el símbolo del sistema como administrador y ejecute el comando **cd %CVP_HOME%\jre\bin**.



Paso 4. Utilice este comando para importar los certificados AW al servidor CVP.

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

Ching Of the data begins 1, 1999, "relationship, for the Control of the Control o

Paso 5. En el mensaje de contraseña, pegue la contraseña copiada de security.properties.

Paso 6. Escriba **yes** para confiar en el certificado y asegurarse de que obtiene el resultado **Se** agregó el certificado al almacén de claves.



Paso 7. Se le solicita una advertencia junto con la importación correcta. Esto se debe al formato propietario Keystore, puede ignorarlo.

Advertencia:

El almacén de claves JCEKS utiliza un formato propietario. Se recomienda migrar a PKCS12, que es un formato estándar del sector utilizando "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore - deststoretype pkcs12".

be KIRI heustave eini a proprieture fermit, 11 it min	impicial (a adjorts to PE
All ekich is an industry incedered forest arises "houter!	- Lagend Charge Street, respectively
it p'. hepelane -finitaineriger plantif"-	CONTRACTOR OF STREET

Estación de trabajo de administración

Paso 1. Inicie sesión en el servidor AW y abra el símbolo del sistema como administrador.

Paso 2. Vaya a C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.

	Rann A.	Two resultant	Type .	int.
	a entry	10.04.000 0010	Roa Automo-	
6C - 1	in the state	10-04-DPV Turk		110
-	maintend onto	This Jin 1919	CONTRACTOR -	199
	Lines D	10.04.009.014	The .	14/9
	product .	10-04-2019 10-10	AND A DOM: N	144
	production with a	10.04.0010.10.10	manni Fa	0.01
	(an invitability)	2010/07/07 1919	Rischie	
	Throughout Streaments	Trans. Street Spice	Contract to the	1.000

Paso 3. Escriba el comando cd %JAVA_HOME% e ingrese.

C:>>ed xJAN	A HOME	Ðx.	
C:\Program	Files	(x86)\Java\jre1.8.8	181)

Paso 4. Utilice este comando para importar los certificados Finesse al servidor AW.

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

Selvergene Files dashtelsen der K. Billeren all angen Arts Selverendssische eine Mitchenfanlischer Auflichen sitter Filesterg sie Argebrei Stiftensetigter

Paso 5. La primera vez que utilice esta herramienta de claves, utilice el **cambio de** contraseña para cambiar la contraseña de un almacén de certificados.

Paso 6. Introduzca una nueva contraseña para el almacén de claves y vuelva a introducirla para confirmar la contraseña.



Paso 7. Escriba **yes** para confiar en el certificado y asegurarse de que obtiene el resultado **El certificado fue agregado al almacén de claves.**

Pust	this	cert	ificate	?	[no]:	yes
Cortif	icate	Was	added	to	ke yst	tore

Nota: Los pasos 1 a 7 deben repetirse con todos los demás nodos Finesse y con todos los nodos CUIC

Paso 8. Si la contraseña del almacén de claves se ha introducido incorrectamente o ha realizado los pasos sin restablecer, se espera que obtenga esta excepción.

¿Confía en este certificado? [no]: sí

El certificado se agregó al almacén de claves

error de la herramienta clave: java.io.FileNotFoundException: .\lib\security\cacerts (El sistema no encuentra la ruta especificada)

Introduzca la contraseña del almacén de claves: error de la herramienta clave: java.io.IOException: El almacén de claves se ha alterado o la contraseña es incorrecta

Paso 9. Para cambiar la contraseña del almacén de claves, utilice este comando y reinicie el procedimiento de nuevo desde el Paso 4 con la nueva contraseña.

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

Colongram Film (addi-Joser.jevi.4.8, Hilberten) -startgarind -kapiture -JJUFmethodomousta Mile Reactive galaxianti Mile Reactive galaxianti has head tone galaxianti

Paso 10. Después de la importación correcta, utilice este comando para ver el certificado del almacén de claves.

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

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



Finesse, CUIC, Cisco IDS y VVB

Paso 1. Inicie sesión en la página de administración del sistema operativo del servidor Finesse y cargue los certificados SSL de AW en la confianza de tomcat.

Paso 2. Vaya a Administración del sistema operativo > Seguridad > Administración de certificados.

Contraction of the local division of the loc	THE R.		100 To 100 W. W.
	Press.		
			1000
	· IET FG	All Carton	(1 m ²
	BF BE	100	il interer

Paso 3. Haga clic en Cargar certificado\cadena de certificado y seleccione tomcat-trust en el menú desplegable.

Paso 4. Examine el almacén de certificados en el almacenamiento local y haga clic en el botón Cargar.



Paso 5. Repita los pasos para cargar todo el certificado de servidor AW en el clúster de Finesse.

Nota: No es necesario cargar el certificado tomcat-trust en el nodo secundario, esto se replica automáticamente.

Paso 6. Reinicie el servicio tomcat para que los cambios del certificado tengan efecto.

Paso 7. En CUIC, IDS y VVB, siga los pasos del 2 al 4 y cargue el certificado AW.

Intercambio de certificados entre Finesse y CUIC/LiveData

Paso 1. Mantenga los certificados Finesse, CUIC y LiveData en una carpeta independiente.

				-	
	Tarra .	Data-readilities	140	tim.	
	CO FIALANT	11-10-27-01-01	Second Contrasts		i uni-
	DOD: +	14-16-127-0-1227	Investo Cettinato		3,480
**	Call Pillebacket	10.04.010.048	Sampy Light as		1.000
	10 198. ve	10.00.000.000	Investig-Contraste		198
	California Contraction	11-08-2019-0017	Searcy Linkson		100
	in instant or	1100.010.001	Desity Configure		1100

Paso 2. Inicie sesión en la página Finesse, CUIC y LiveData OS Administration.

Paso 3. Vaya a Administración del sistema operativo > Seguridad > Administración de certificados.

Paso 4. Haga clic en Cargar certificado\cadena de certificado y seleccione tomcat-trust en el menú desplegable.

Paso 5. Examine el almacén de certificados en el almacenamiento local y seleccione el certificado de servidores como se muestra a continuación y, a continuación, haga clic en el botón Cargar.

En el servidor Finesse - CUIC y LiveData como confianza de Tomcat

En el servidor CUIC: Finesse y LiveData como confianza de tomcat

En LiveData Server: CUIC y Finesse como confianza de Tomcat

Nota: No es necesario cargar el certificado tomcat-trust en el nodo secundario, esto se replica automáticamente.

Paso 6. Reinicie el servicio tomcat en cada nodo para que los cambios del certificado surtan efecto.