# Implementazione di certificati firmati CA in una soluzione CCE 12.6

# Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Introduzione Procedura Server CCE basati su Windows 1. Generare CSR 2. Ottenere i certificati firmati dalla CA 3. Caricare i certificati firmati dalla CA 4. Associare il certificato firmato dalla CA a IIS 5. Associare il certificato firmato dalla CA al portico di diagnostica 6. Importare il certificato principale e intermedio in Java Keystore Soluzione CVP 1. Genera certificati con FODN 2. Generare il CSR 3. Ottenere i certificati firmati CA 4. Importazione dei certificati firmati dalla CA Server VOS 1. Genera certificato CSR 2. Ottenere i certificati firmati dalla CA 3. Caricare l'applicazione e i certificati radice Verifica Risoluzione dei problemi InformazioniCorrelate

# Introduzione

In questo documento viene descritto come implementare i certificati firmati da un'Autorità di certificazione (CA) nella soluzione Cisco Contact Center Enterprise (CCE).

# Prerequisiti

# Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Unified Contact Center Enterprise (UCCE) release 12.6.2
- Package Contact Center Enterprise release 12.6.2
- Customer Voice Portal (CVP) release 12.6.2
- Cisco Virtualized Voice Browser (VB)
- Cisco CVP Operations and Administration Console (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

# Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- PCCE 12.6.2
- CVP 12.6.2
- Cisco VB 12.6.2
- Finesse 12.6.2
- CUIC 12.6.2
- Windows 2019

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Introduzione

I certificati vengono utilizzati per garantire la sicurezza delle comunicazioni con l'autenticazione tra client e server. Gli utenti possono acquistare certificati da una CA o utilizzare certificati autofirmati.

I certificati autofirmati (come indica il nome) sono firmati dalla stessa entità di cui certificano l'identità, anziché da un'autorità di certificazione. I certificati autofirmati non sono considerati sicuri come i certificati CA, ma vengono utilizzati per impostazione predefinita in molte applicazioni.

Nella soluzione Package Contact Center Enterprise (PCCE) versione 12.x, tutti i componenti della soluzione sono controllati da Single Pane of Glass (SPOG), che è ospitato nel server AW (Admin Workstation) principale.

A causa di Security Management Compliance (SRC) nella versione PCCE 12.5(1), tutte le comunicazioni tra SPOG e gli altri componenti della soluzione avvengono tramite il protocollo HTTP protetto.

In questo documento vengono illustrati in dettaglio i passaggi necessari per implementare i certificati firmati dall'autorità di certificazione in una soluzione CCE per la comunicazione HTTP protetta. Per qualsiasi altra considerazione sulla sicurezza UCCE, fare riferimento alle <u>linee guida sulla sicurezza UCCE</u>.

Per qualunque comunicazione aggiuntiva protetta da CVP diversa da HTTP protetta, consultare le linee guida sulla sicurezza nella guida alla configurazione di CVP: <u>Linee guida per la sicurezza di CVP</u>.

**Nota**: questo documento si applica solo alla versione 12.6 di CCE. Per i collegamenti ad altre versioni, vedere la sezione relativa alle informazioni correlate.

# Procedura

# Server CCE basati su Windows

# 1. Generare CSR

In questa procedura viene illustrato come generare una richiesta di firma di certificato (CSR) da Gestione Internet Information Services (IIS).

Passaggio 1. Accedere a Windows e scegliere **Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS)**.

Passaggio 2. Nel riquadro Connessioni fare clic sul nome del server. Viene visualizzato il riquadro Home del server.



Passaggio 3. Nell'area IIS fare doppio clic su Certificati server.



Passaggio 4. Nel riquadro Azioni fare clic su Crea richiesta certificato.

Connections	0			Actions
Q 🖬 ( 🖄 ) 🖗.	Server Certifica	tes		import_
Sart Pape	Use this feature to request and m websites configured for SSL. Filter	anage certificates that the Web set	ver can use with	Create Certificate Request Complete Certificate Request. Create Domain Certificate
	Name	Issued To	Issued By	Create Self-Signed Certificate.
	Cisca ICM Diagnostic Framew Cisca ICM 59, Certificate	PCCLANA.PCCERCDN.cisco.c., PCCLANA.PCCERCDN.cisco.c.,	PCCEANA.PCCERCE PCCEANA.PCCERCE	Enable Automatic Rebind of Renewed Certificate
				0 Help

Passaggio 5. Nella finestra di dialogo Richiedi certificato eseguire le operazioni seguenti:

Specificare le informazioni richieste nei campi visualizzati e fare clic su Avanti.

Request Certificate		?	x
Distinguished N	ame Properties		
Specify the required informati official names and they canno	on for the certificate. State/province and City/locality must be specified as t contain abbreviations.		
Common name:	pcceawa.pccercdn.cisco.com		
Organization:	Cisco		
Organizational unit:	CX		
City/locality	RCDN		
State/province:	TX		
Country/region:	US v		
			_
	Previous Next Finish	Cancel	

Lasciare invariata l'impostazione predefinita nell'elenco a discesa Provider del servizio di crittografia.

Dall'elenco a discesa Lunghezza bit selezionare 2048.

Request Certificate	?	x
Cryptographic Service Provider Properties		
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines t certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater b length may decrease performance. Cryptographic service provider:	he sit	
Microsoft RSA SChannel Cryptographic Provider		
Bit length:		
Previous Next Finish	Cancel	1

Passaggio 6. Specificare un nome file per la richiesta di certificato e fare clic su Fine.

Request Certificate	?	x
File Name		
Specify the file name for the certificate request. This information can be sent to a certification authority fo signing.	e	
Specify a file name for the certificate request: PCCEAULPCCERCDN.eisco.com		
Previous Next Finish	Cancel	

#### 2. Ottenere i certificati firmati dalla CA

Passaggio 1. Firmare il certificato su una CA.

**Nota**: verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server.

Passaggio 2. Ottenere i certificati CA firmati dall'autorità di certificazione (radice, applicazione e intermedio, se presenti).

## 3. Caricare i certificati firmati dalla CA

Passaggio 1. Accedere a Windows e scegliere **Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS)**.



Passaggio 2. Nel riquadro Connessioni fare clic sul nome del server.

Connections A • 🗔   🖄   🚱	en en	CEAWA H	ome				
Start Page     PCCEAWA (PCCERCDN/pcceadmin)	Filter		• \$ Go - 1	Show All	Group by:		1
	Connection Strings	SMTP E-mail					
	Authentic	2 Compression	Default	Directory Browsing	Error Pages	Handler Mappings	
	HTTP	HTTP Respon	ISAPI and CGI Restri	SAPI Filters	Logging	MML Types	
	Modules	Output Caching	8 Request Filtering	Server Certificates	Worker Processes		
	Manageme		F			^	ļ
	Configurat	Feature	Shared				

Passaggio 3. Nell'area IIS fare doppio clic su Certificati server.

Connections	en en	CEAWA H	ome				
Start Page	Filter		• \$ 60 -	Show All	Group by:		l
	Connection Strings	SMTP E-mail					
	Authentic	Compression	Default	Directory Browsing	Error Pages	Handler Mappings	
	HTTP	HTTP Respon	ISAPI and CGI Restri-	SAPI Filters	Logging	MML Types	
	Modules	Output Caching	8 Request Filtering	Server Certificates	Worker Processes		
	Manageme		E			*	
	Configurat	Feature	Shared				k

Passaggio 4. Nel riquadro Azioni fare clic su Completa richiesta certificato.

Connections	Ca constant			Actions
Q 🗟   🖄   😣	Server Certhical	les		import
Start Page     PCCEARIA (PCCERCDN pcceadmin)	Use this feature to request and ma websites configured for SSL	mage certificates that the Web ser	ver can use with	Create Cetificate Request.
	Film: • Y	Go - 😨 Show All   Group by:		Create Domain Certificate
	Name .	Issued To	Issued By	Create Self-Signed Certificate
	Cisco ICM Diagnostic Framew Cisco ICM SSL Certificate	PCOLMAR.PCCBRCDN.cisco.c., PCOLMAR.PCCBRCDN.cisco.c.,	PCCEANA.PCCERCI PCCEANA.PCCERCI	Enable Automatic Rebind of Renewed Certificate
				e Help

Passaggio 5. Nella finestra di dialogo Completa richiesta certificato completare i campi seguenti:

Nel campo Nome file contenente la risposta dell'Autorità di certificazione fare clic sul pulsante ....

Individuare il percorso in cui è archiviato il certificato dell'applicazione firmato e quindi fare clic su Apri.

**Nota**: se si tratta di un'implementazione di CA a 2 livelli e il certificato radice non è già presente nell'archivio certificati del server, è necessario caricare la radice nell'archivio di Windows prima di importare il certificato firmato. Fare riferimento a questo documento se è necessario caricare la CA radice in Windows Store <u>Microsoft - Installazione del certificato radice attendibile</u>.

Nel campo Nome descrittivo immettere il nome di dominio completo (FQDN) del server o qualsiasi nome significativo. Verificare che l'elenco a discesa **Selezionare un archivio certificati per il nuovo certificato** 

## rimanga Personale.

Complete Certificate Request	?	×
Specify Certificate Authority Response		
Complete a previously created certificate request by retrieving the file that contains the certificate author response.	ity's	
File name containing the certification authority's response:		
Friendly name: PCCEAWA.pccercdn.cisco.com		
Select a certificate store for the new certificate:		
Personal		
OK	Cance	el 🛛

Passaggio 6. Scegliere OK per caricare il certificato.

Se il caricamento del certificato ha esito positivo, il certificato verrà visualizzato nel riquadro Certificati server.

🍞 Internet Information Services (ID) Manager		= 0 X
		10 H (s) 10 +
File View Help		
Connections	Server Certificates	Actions
9 El 10 18.	- Server Certificates	import_
Start Page S PCCEANA (PCCERCDN pcceadmin)	Use this feature to request and manage certificates that the Web server can use with websites configured for \$32.	Create Certificate Request Complete Certificate Request
	Filter • 🐨 Go - 😨 Show All   Group by:	Create Domain Certificate
	Name Insued To Issued By	Create Self-Signed Certificate
	Caco ICM Diagnostic Framework servi. PCCLANA.PCCDFCDI.clean.c., PCCLANA.P Caco ICM SS, Certificate PCCLANA.PCCDFCDI.clean.c., PCCLANA.P	Enable Automatic Rebind of Renewed Certificate
	PCCERRA poperadivideo.com proteina prot	<b>0</b> He

## 4. Associare il certificato firmato dalla CA a IIS

In questa procedura viene illustrato come associare un certificato firmato da una CA in Gestione IIS.

Passaggio 1. Accedere a Windows e scegliere **Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS)**.

Connections	Star PC	CEAWA H	lome				
Ø,• EE   ⊠   Ø,	-10						
Start Page	Filter		• 7 Go -	Show All	Group by:		4
	Connection	SMTP E-mail					^
	Authentic	Compression	Ocfault	Directory	Error Pages	andler A	
			Document	Browsing		Mappings	
	100	- <b>1</b>	5	3		17.	
	HTTP Redirect	HTTP Respon	ISAPI and CGI Restri	ISAPI Filters	Logging	MME Types	
	- 4	1	81		2		
	Modules	Output Caching	Request Filtering	Server Certificates	Worker Processes		
	Managem	ent				^	
		1	麵				
	Configurat.	Feature	Shared				

Passaggio 2. Nel riquadro Connessioni scegliere **<nome\_server> > Siti > Sito Web predefinito**.



Passaggio 3. Nel riquadro Azioni fare clic su Associazioni....

🍞 Internet Information Services (IS) Manager		_ 0 X
🕡 💿 🖌 PCCEANA + Sites + Default W	vb Ste 🔹	$\mathbf{m} = \mathbf{S} \cdot \mathbf{\Theta} \cdot$
File View Help		
Connections	Default Web Site Home	Actions
No. Ini IZ     [9].       Stan Rys     Second Sec	Filter • T Go • Show At Group by:	Lepton     Lepton     Let     Vene Applications     Vene Vetal Decision     Nange Webbe     Parts     Sans
	Authentic Compension Default Authentic Compension Default Disconce Default HTTP: HTTP: Referst Regen Cutotic Default HTTP: HTTP: Referst Regen Cutotic Default HTTP: HTTP: Referst Regen Cutotic Default Regen Cutotic Default Default Regen Cutotic Default Default Regen Cutotic Default Default Regen Cutotic Default De	Browse Webste

Passaggio 4. Fare clic sul tipo https con porta 443, quindi su Modifica....



Passaggio 5. Dall'elenco a discesa Certificato SSL selezionare il certificato con lo stesso nome descrittivo indicato nel passaggio precedente.

		1.00
mer tions	Default Web Site Home	Actions
101 M 184	Di Badani di	Capitore
D DOCLARA (DOCLARCON) AND	and the second se	Lot Permissions
Application Peols	Type Host Name Pot IP Address Binding Informa	Ldt Site
v 🖌 Stel	http 80	
> 😔 Default Web Site	Mtps 440 Edt.	U tesc service
	Tanco	Ties Applications
	Edit Ster Binding 7 🗶	The second second
		Manage Wroute
	Type Paddess Port	a fear
	teps v Al Grassigned v 40	
	Host name	Response Westwide
		C Browse "40 (http)
	Require Server Name Indication	E Browse (443 (https)
		Advanced Settings
		Configure
	SSL certificate	Links
	PCCLAstApocerode.coon v Select View	0 Heb

Passaggio 6. Fare clic su OK.

Passaggio 7. Passare a **Start > Esegui > services.msc** e riavviare il servizio Amministrazione di IIS.

Artista Marc	No.					
1021 00 0						_
nices (Local)	<ol> <li>Services (Local)</li> </ol>					
	Apache Tomcat 9	Name	Description	Status	Statup Type	Let n
		Q, Hyper-V Data Exchange Service	Provides a mechanism to exchange data betwee		Manual (Trip	Lo
	Stop the service	Q Hyper-V Guest Service Interface	Provides an interface for the Hyper-V heat to int		Manual (Trig	Lo
	Restart the service	Q Hyper-Y Guest Shutdown Service	Provides a mechanism to shut down the operati		Manual (Trig	Lo
		Q Hyper-Y Heatbeat Service	Monitors the state of this virtual machine by rep		Manual (Trig	Los
	Description	A Hyper-Y PowerShell Direct Service	Provides a mechanism to manage virtual machi		Manual (Trig	Los
	Apache Torncat 9.0 Server -	Q, Hyper-V Remote Desistop Virtualizatio	Provides a platform for communication betwee		Manual (Trig	Loi.
	Mip//tomcat.apache.org/tomcat/	Q, Hyper-V Time Synchronization Service	Synchronizes the system time of this virtual mac		Manual (Trig	Let B
		Chippen's Volume Shadow Copy Reput	Coordinates the communications that are requir		Manual (Trig	Let .
		122,15 Admin Senice	Enables this server to administer the IS metabas	Running	Automatic	Los
		Co. KE and ButhiP Pres Keying Modules	The REEXT service heats the Internet Key Excha-	Running	Automatic (T	Los
		Q Interactive Services Detection	Enables user notification of user input for intera		Disabled	Lo
		Q Internet Connection Sharing (ICS)	Provides network address translation, addressin		Disabled	Lo
		CQ, IP Helper	Provides tunnel connectivity using IPv6 transitio	Running	Automatic	Lo
		Puec Policy Agent	Internet Protocol security (Psec) supports netw-	Running	Manual (Trig	Net
		CALKDC Proxy Server service (KPS)	KDC Proxy Server service runs on edge servers to	-	Manual	Net
		C. Desiles for Distributed Transaction C	Coordinates transactions between the Distribute		Manual (Trin-	No

## 5. Associare il certificato firmato dalla CA al portico di diagnostica

In questa procedura viene illustrato come associare un certificato firmato da un'autorità di certificazione nel portico di diagnostica.

Passaggio 1. Aprire il prompt dei comandi (Esegui come amministratore).

Passaggio 2. Passare alla home directory di Diagnostic Portico. Eseguire questo comando:

cd c:\icm\serviceability\diagnostics\bin

Passaggio 3. Rimuove il binding del certificato corrente al portico di diagnostica. Eseguire questo comando:

DiagFwCertMgr /task:UnbindCert



Passaggio 4. Aprire il certificato firmato e copiare il contenuto hash (senza spazi) del campo Identificazione personale.

**Nota**: assicurarsi di rimuovere tutti i caratteri nascosti dall'inizio o dalla fine del contenuto hash. Un editor come Blocco note++ consente di identificare questi caratteri nascosti.

Seneral	Details	Certification F	ath	
Show:	<all></all>		~	
Field	thority K L Distribut thority In rtificate T plication I y Usage umbprint	ey Identifier Ition Points Iformation Acce Femplate Inform Policies algorithm	Value KeyID=03 2f 51 02 27 8c c7 [1]CRL Distribution Point: Dis ss [1]Authority Info Access: Ac n Template=CC Web Server(1 [1]Application Certificate Pol Digital Signature, Key Enciph sha1 97 93 74 00 99 19 53 d6 4e	^ 3 str .3 ic rer ≡ 0b ↓
97 9 96 3	374( 6dc4	00 99 19 9 4b cb	53 d6 4e Ob c5 6e c4	4c bd
			Edit Properties Copy to	File

Passaggio 5. Eseguire questo comando e incollare il contenuto hash.

DiagFwCertMgr /task:BindCertFromStore /certhash:<hash\_value>

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:979374 dc4bcb

c:\icm\serviceability\diagnostics\bin>

Se il binding dei certificati ha esito positivo, viene visualizzato il messaggio Il binding dei certificati è VALIDO.

Passaggio 6. Convalida se il binding dei certificati è riuscito. Eseguire questo comando:

DiagFwCertMgr /task:ValidateCertBinding

c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding
*************************
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager ************************************
Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>

Nota: per impostazione predefinita, DiagFwCertMgr utilizza la porta 7890.

Se il binding dei certificati ha esito positivo, viene visualizzato il messaggio Il binding dei certificati è VALIDO.

Passaggio 7. Riavviare il servizio Framework di diagnostica. Eseguire i seguenti comandi:

net stop DiagFwSvc
net start DiagFwSvc

Se Diagnostic Framework viene riavviato correttamente, gli avvisi relativi agli errori dei certificati non vengono visualizzati all'avvio dell'applicazione.

#### 6. Importare il certificato principale e intermedio in Java Keystore

**Attenzione**: prima di iniziare, è necessario eseguire il backup del keystore ed eseguire i comandi dalla java home come amministratore.

Passaggio 1. Conoscere il percorso della directory principale Java per verificare dove è ospitato lo strumento chiave Java. Ci sono due modi per trovare il percorso di casa java.

Opzione 1: comando CLI: echo %CCE\_JAVA\_HOME%



Opzione 2: Manualmente tramite Impostazioni di sistema avanzate, come mostrato nell'immagine

System			
← → × ↑ 🔛 > Control P	Panel > System and Security > System		
Control Panel Home	System Properties		
Device Manager	Computer Name Hardware Advanced Remote	Environment Variabler	
<ul> <li>Remote settings</li> <li>Advanced system settings</li> </ul>	You must be logged on as an Administrator to make most of these changes. Performance	- User variables for Administrator	
	Visual effects, processor scheduling, memory usage, and virtual memory	Variable	Value
	Settings	Path	C:\Users\Administrator\AppData\Lo
	User Profiles Desktop settings related to your sign-in Settings	TEMP	C:\Users\Administrator\AppData\Lo C:\Users\Administrator\AppData\Lo
	Startup and Recovery System startup, system failure, and debugging information Settings	System variables	
	E-investigation	Variable	Value
	OK Cancel Apply	CCE_JAVA_HOME COMPLUS_ProTAPI_ProfilerC ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDvnamics.AgentProfiler
See also			
Security and Maintenance			

Passaggio 2. Eseguire il backup del file **cacerts** dalla cartella **<ICM install directory>\ssl\.** È possibile copiarlo in un'altra posizione.

Passaggio 3. Aprire una finestra di comando come Amministratore ed eseguire i seguenti comandi:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe â€"keystore <ICM install directory>\ssl\cacerts -trustcacerts -import -file <path where the</pre>
```

**Nota**: i certificati specifici richiesti dipendono dalla CA utilizzata per firmare i certificati. In una CA a due livelli, tipica delle CA pubbliche e più sicura delle CA interne, è necessario importare i certificati radice e intermedi. In una CA standalone senza componenti intermedi, generalmente presente in un'autorità di certificazione lab o in una CA interna più semplice, è sufficiente importare solo il certificato radice.

## **Soluzione CVP**

1. Genera certificati con FQDN

In questa procedura viene illustrato come generare certificati con FQDN per i servizi Web Service Manager (WSM), Voice XML (VXML), Call Server e Operations Management (OAMP).

**Nota**: quando si installa CVP, il nome del certificato include solo il nome del server e non il nome di dominio completo, pertanto è necessario rigenerare i certificati.

Attenzione: prima di iniziare, eseguire questa operazione:

1. Aprire una finestra di comando come amministratore.

2. Per la versione 12.6.2, per identificare la password del keystore, passare alla cartella

%CVP\_HOME%\bin ed eseguire il file DecryptKeystoreUtil.bat.

3. Per la versione 12.6.1, per identificare la password del keystore, eseguire il comando more

#### %CVP\_HOME%\conf\security.properties.

4. Questa password è necessaria per eseguire i comandi keytool.

- 5. Dalla directory %CVP\_HOME% \conf\security\, eseguire il comando copy . keystore
- backup.keystore.

#### Server CVP

Passaggio 1. Per eliminare i certificati dei server CVP, eseguire i comandi seguenti:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -a

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -al

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -a

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

Quando richiesto, immettere la password del keystore.

**Nota**: per impostazione predefinita, i certificati vengono generati per due anni. Utilizzare -valid XXXX per impostare la data di scadenza per la rigenerazione dei certificati. In caso contrario, i certificati saranno validi per 90 giorni e dovranno essere firmati da una CA prima di questo periodo. Per la maggior parte di questi certificati, 3-5 anni devono essere un periodo di convalida ragionevole.

Di seguito sono riportati alcuni input di validità standard:

Un anno	365
Due anni	730

Tre anni	1095
Quattro anni	1460
Cinque anni	1895
Dieci anni	3650

Attenzione: da 12.5 i certificati devono essere SHA 256, Key Size 2048 e encryption Algorithm RSA, utilizzare questi parametri per impostare i seguenti valori: -keyalg RSA e -keysize 2048. È importante che i comandi del keystore CVP includano il parametro -storetype JCEKS. In caso contrario, il certificato, la chiave o, peggio, il keystore potrebbe danneggiarsi.

Specificare il nome di dominio completo (FQDN) del server, alla domanda qual è il nome e il cognome?



Rispondere alle seguenti domande:

Qual è il nome dell'unità organizzativa?

[Sconosciuto]: <specificare OU>

Qual è il nome dell'organizzazione?

[Sconosciuto]: <specificare il nome dell'organizzazione>

Indicare il nome della città o della località.

[Sconosciuto]: <specificare il nome della città/località>

*Qual è il nome della provincia?* 

[Sconosciuto]: <specificare il nome della provincia>

Qual è il codice paese di due lettere per questo apparecchio?

[Sconosciuto]: <specifica il codice paese a due lettere>

Specificare yes per i due input successivi.

Passaggio 3. Eseguire la stessa procedura per vxml\_certificate e callserver\_certificate:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

#### Server di report CVP

Passaggio 1. Per eliminare i certificati di WSM e del server di report, eseguire i comandi seguenti:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -al %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -al

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

Quando richiesto, immettere la password del keystore.

Specificare il nome di dominio completo (FQDN) del server per la query **che cos'è il nome e il cognome?** e continuare con la stessa procedura utilizzata per i server CVP.

Passaggio 3. Eseguire la stessa procedura per callserver\_certificate:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

Quando richiesto, immettere la password del keystore.

#### **CVP OAMP (distribuzione UCCE)**

Poiché nella soluzione PCCE versione 12.x tutti i componenti della soluzione sono controllati da SPOG e OAMP non è installato, questi passaggi sono necessari solo per una soluzione di distribuzione UCCE.

Passaggio 1. Per eliminare i certificati del server WSM e OAMP, eseguire i comandi seguenti:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -al %CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -delete -al

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

Quando richiesto, immettere la password del keystore.

Specificare il nome di dominio completo (FQDN) del server per la query **che cos'è il nome e il cognome?** e continuare con la stessa procedura utilizzata per i server CVP.

Passaggio 3. Eseguire la stessa procedura per oamp\_certificate:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -genkeypair

Quando richiesto, immettere la password del keystore.

#### 2. Generare il CSR

**Nota**: il browser conforme allo standard RFC5280 richiede che in ogni certificato sia incluso il nome alternativo del soggetto (SAN, Subject Alternative Name). A tale scopo, è possibile utilizzare il parametro -ext con SAN durante la generazione di CSR.

#### Nome alternativo soggetto

Il parametro -ext consente all'utente di utilizzare estensioni specifiche. Nell'esempio riportato viene aggiunto un nome alternativo del soggetto (SAN) con il nome di dominio completo (FQDN) del server e localhost. È possibile aggiungere ulteriori campi SAN come valori separati da virgole.

I tipi di SAN validi sono:

ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com

Ad esempio:

-ext san=dns:mycvp.mydomain.com,dns:localhost

#### Server CVP

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, wsm\_certificate):

Quando richiesto, immettere la password del keystore.

Passaggio 2. Eseguire la stessa procedura per vxml\_certificate e callserver\_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Quando richiesto, immettere la password del keystore.

#### Server di report CVP

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, wsmreport\_certificate):

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -certreq -a

Quando richiesto, immettere la password del keystore.

Passaggio 2. Eseguire la stessa procedura per callserver\_certificate:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -certreq -a

Quando richiesto, immettere la password del keystore.

#### CVP OAMP (solo distribuzione UCCE)

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, wsmoamp\_certificate):

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -certreq -a

Quando richiesto, immettere la password del keystore.

Passaggio 2. Eseguire la stessa procedura per oamp\_certificate:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -certreq -a

Quando richiesto, immettere la password del keystore.

## 3. Ottenere i certificati firmati CA

Passaggio 1. Firmare i certificati su una CA (WSM, Callserver e server VXML per il server CVP; WSM e OAMP per il server CVP OAMP e WSM e Callserver per il server CVP Reporting).

Passaggio 2. Scaricare i certificati dell'applicazione e il certificato radice dall'autorità CA.

Passaggio 3. Copiare il certificato radice e i certificati firmati dalla CA nella cartella **%CVP\_HOME%\conf\security\** di ogni server.

## 4. Importazione dei certificati firmati dalla CA

Applica questi passaggi a tutti i server della soluzione CVP. Solo i certificati per i componenti su tale server devono avere il certificato firmato dalla CA importato.

Passaggio 1. Importare il certificato radice. Eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -import -tr

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Se è presente un certificato intermedio, eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -ti
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 2. Importare il modulo WSM firmato dalla CA per il certificato server (CVP, Reporting and OAMP). Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -ti
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 3. Nei server CVP e nei server di report importare il certificato firmato dalla CA del server di chiamata. Eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -import -ti

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 4. Nei server CVP importare il certificato firmato dalla CA del server VXML. Eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -import -tr

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 5. Nel server CVP OAMP (solo per UCCE) importare il certificato firmato dalla CA del server OAMP. Eseguire questo comando:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore -import -tr

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare **Sì**.

Passaggio 6. Riavviare i server.

**Nota**: nella distribuzione UCCE, assicurarsi di aggiungere i server (CVP Reporting, CVP Server e così via) in CVP OAMP con il nome di dominio completo fornito durante la generazione del CSR.

# **Server VOS**

#### 1. Genera certificato CSR

In questa procedura viene illustrato come generare il certificato CSR Tomcat da una piattaforma basata su VOS (Cisco Voice Operating System).

Questo processo è applicabile alle applicazioni basate su VOS, quali:

- Finesse
- CUIC \ Live Data (LD) \Identity Server(IDS)
- Cloud Connect
- Cisco VB

Passaggio 1. Passare alla pagina di amministrazione del sistema operativo Cisco Unified Communications: https://FQDN :<8443 o 443>/cmplatform.

Passaggio 2. Passare a Sicurezza > Gestione certificati e selezionare Genera CSR.

ertificate List	
🛐 Generale Self-signed 🔤 Upload Certificate/Certificate chain 💽	Generate CSR
End Cartificate List where Cartificate v bacins with v	End Play Eller & m
Contrast of the Contrast Contrast of	No active query. Please enter your search orderia using the options above.
Generate Self-signed Upload Certificate/Certificate chain	Generate CSR

Passaggio 3. Una volta generato il certificato CSR, chiudere la finestra e selezionare Download CSR.

ertificate List		
🖁 Generate Setf-signed 🛛 Upload Centrical	e/Certificate chain 🧕 Generate CSR	Download CSR
Certificate List		
ind Certificate List where Certificate	✓ begins with	Find Clear Filter 💠 👄
		and a second sec

Passaggio 4. Verificare che lo scopo del certificato sia tomcat e fare clic su Download CSR.



Passaggio 5. Fare clic su Salva file. Il file viene salvato nella cartella Download.

Opening tomcat.cs	r	×
You have chosen t	o open:	
itomcat.csr		
which is: CS	R file	
from: https:	//10.201.224.234	
What should Fire	fox do with this file?	
○ <u>O</u> pen with	Applications\notepad.exe (default)	•
• Save File		
-		
	OK Cancel	

## 2. Ottenere i certificati firmati dalla CA

Passaggio 1. Firmare il certificato tomcat esportato su una CA.

Passaggio 2. Scaricare l'applicazione e la radice certificata dall'autorità CA.

## 3. Caricare l'applicazione e i certificati radice

Passaggio 1. Passare alla pagina di amministrazione del sistema operativo Cisco Unified Communications: <u>https://FQDN</u>:<8443 o 443>/cmplatform.

Passaggio 2. Passare a **Protezione > Gestione certificati** e selezionare **Carica catena certificati/certificati**.



Passaggio 3. Nella finestra Carica catena di certificati/certificati selezionare tomcat-trust nel campo Scopo del certificato e caricare il certificato radice.

Upload Certificate/Certifica	te chain	
Upload 🖳 Close		
Warning: Uploading a clu	ster-wide certificate will distribute it to all servers in this c	luster
Upload Certificate/Certificate	ate chain	
Certificate Purpose*	tomcat-trust	
Description(friendly name)		
Upload File	Choose File No file chosen	
Upload Close		

Passaggio 4. Caricare un certificato intermedio (se presente) come tomcat-trust.

Passaggio 5. Nella finestra Carica certificato/catena di certificati selezionare ora per passare al campo Scopo certificato e caricare il certificato firmato dalla CA dell'applicazione.

Upload Certificate/Certificate chain			
Dipload 🖳 Close			
Status           Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster			
Certificate Purpose*	tomcat		
Description(friendly name)	Self-signed certificate		
Upload File	Browse No file selected.		
Upload Close			
<	>		

Passaggio 6. Riavviare il server.

# Verifica

Dopo aver riavviato il server, eseguire la procedura seguente per verificare l'implementazione della CA firmata:

Passaggio 1. Aprire un browser Web e cancellare la cache.

Passaggio 2. Chiudere e aprire di nuovo il browser.

A questo punto è necessario visualizzare l'opzione del certificato per iniziare il certificato firmato dalla CA e l'indicazione nella finestra del browser che il certificato è autofirmato e quindi non attendibile deve scomparire.

# Risoluzione dei problemi

In questa Guida non è disponibile alcuna procedura per la risoluzione dei problemi relativi all'implementazione dei certificati firmati da un'autorità di certificazione.

# Informazioni correlate

- Guida alla configurazione di CVP Sicurezza
- UCCE Security Guide
- <u>Guida per l'amministratore PCCE</u>
- <u>Certificati autofirmati PCCE di Exchange PCCE 12.5</u>
- <u>Certificati autofirmati Exchange UCCE UCCE 12.5</u>
- <u>Certificati autofirmati PCCE di Exchange PCCE 12.6</u>
- <u>Certificati autofirmati Exchange UCCE UCCE 12.6</u>
- Documentazione e supporto tecnico Cisco Systems

# Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).