

Configurazione dei certificati del server applicazioni di provisioning con firma CA in Prime Collaboration Provisioning

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisito](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura per caricare e verificare i certificati CA (Certification Authority) - Server applicazioni di provisioning firmato in Prime Collaboration Provisioning (PCP).

Prerequisiti

Requisito

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PCP e CA interna Microsoft
- Snapshot della macchina virtuale o backup PCP più recente prima di caricare il certificato

Componenti usati

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

- PCP versione 12.3
- Mozilla Firefox 5.0
- CA interna Microsoft

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.

Configurazione

Passaggio 1. Accedere a PCP e selezionare **Amministrazione > Aggiornamenti > Sezione Certificati SSL**.

Passaggio 2. Fare clic su **Genera richiesta di firma del certificato**, immettere l'attributo obbligatorio e fare clic su **Genera** come mostrato nell'immagine.

Nota: L'attributo Nome comune deve corrispondere al nome di dominio completo (FQDN) di PCP.

Generate Certificate Signing Request



 **Warning: Generating a new certificate signing request will overwrite an existing CSR.**

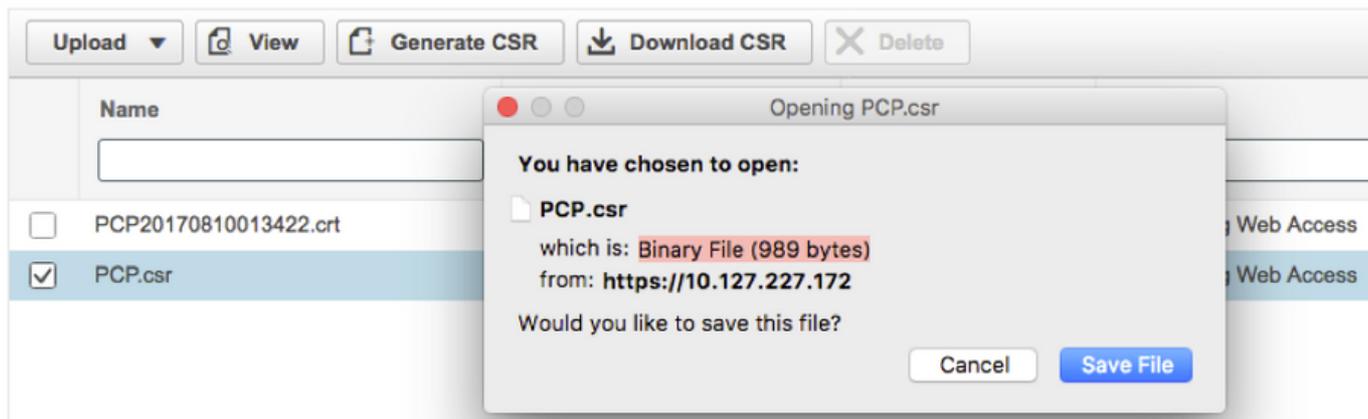
* Certificate Name	<input type="text" value="PCP"/>
* Country Name	<input type="text" value="IN"/>
* State or Province	<input type="text" value="KA"/>
* Locality Name	<input type="text" value="BLR"/>
* Organization Name	<input type="text" value="Cisco"/>
* Organization Unit Name	<input type="text" value="PCP"/>
* Common Name	<input type="text" value="pcp12.uc.com"/>
Email Address	<input type="text" value="Standard format email address"/>
Key Type	RSA
Key Length	2048
Hash Algorithm	SHA256

Cancel

Generate

Passaggio 3. Fare clic su **Scarica CSR** per generare il certificato come mostrato nell'immagine.

▼ SSL Certificates



Passaggio 4. Utilizzare questa richiesta di firma del certificato (CSR) per generare il certificato firmato dalla CA pubblica con l'aiuto del provider della CA pubblica.

Se si desidera firmare il certificato con una CA interna o locale, eseguire la procedura seguente:

Passaggio 1. Accedere alla CA interna e caricare il CSR come mostrato nell'immagine.

Microsoft Active Directory Certificate Services -- uc-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

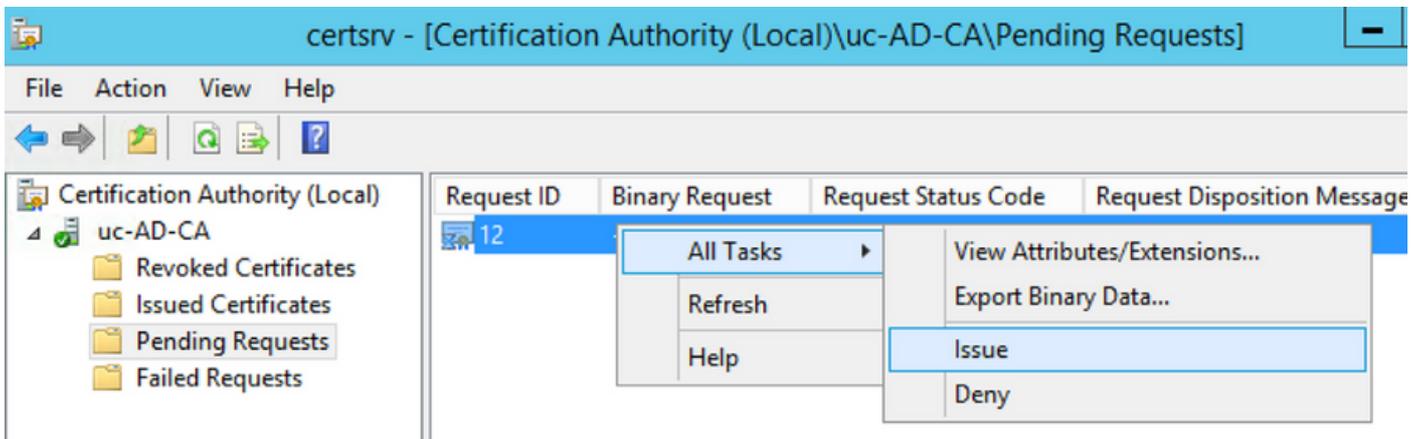
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

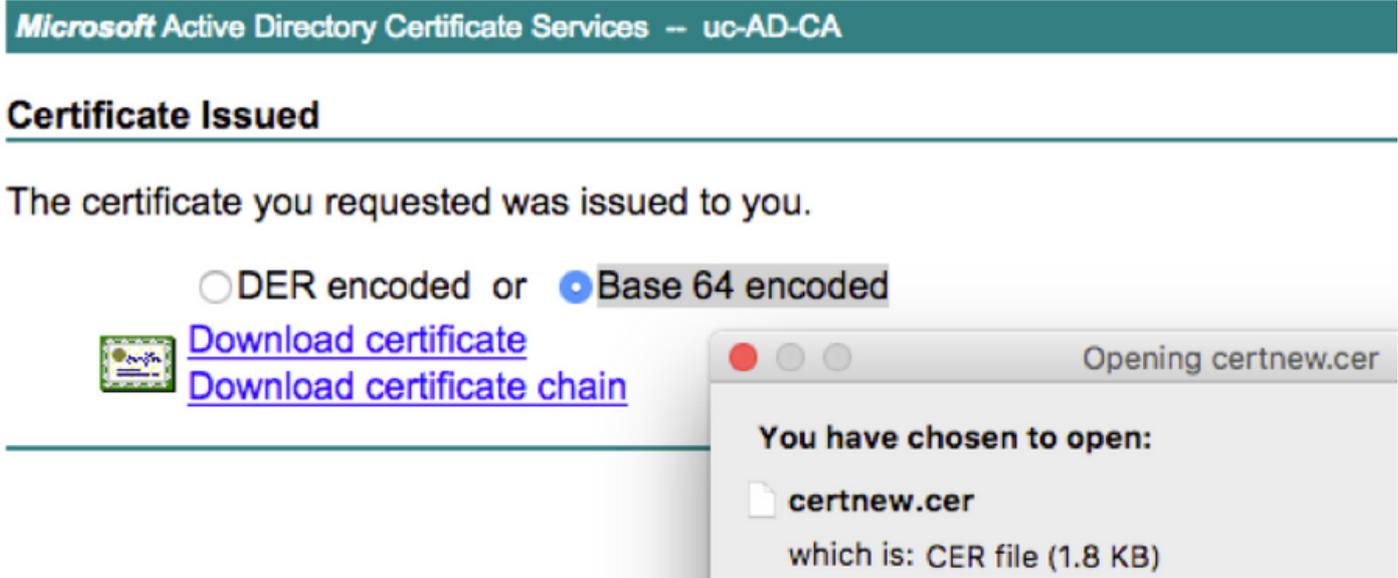
Attributes:

Submit >

Passaggio 2. Connettersi al server CA interno, fare clic con il pulsante destro del mouse su **Richieste in sospeso > Tutte le attività > Seleziona problema** per ottenere un certificato firmato, come mostrato nell'immagine.

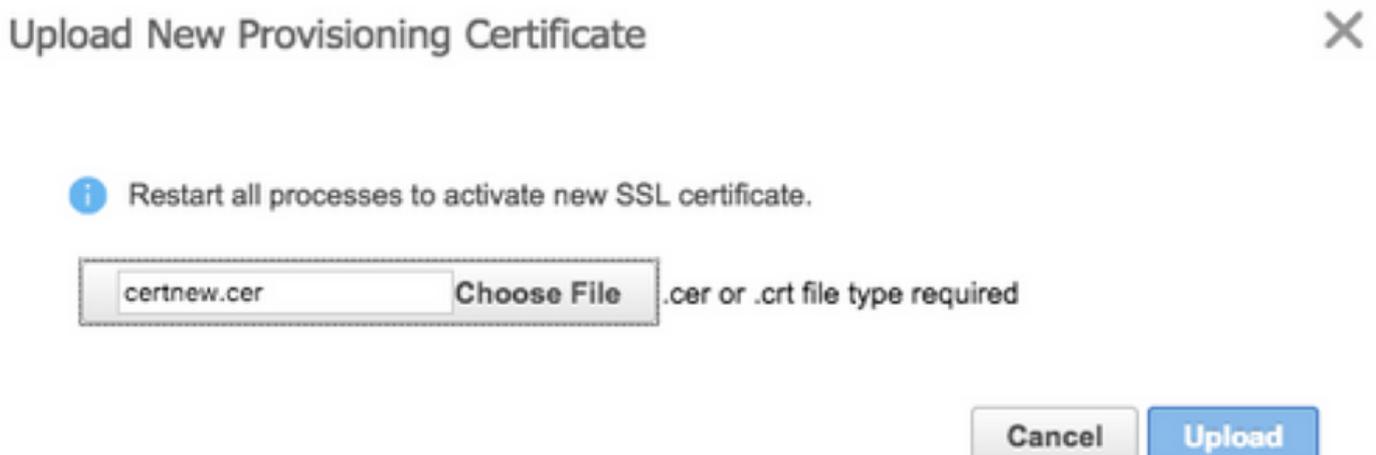


Passaggio 3. Quindi, selezionare il pulsante di opzione **Codificato in formato Base 64** e fare clic su **Scarica certificato** come mostrato nell'immagine.

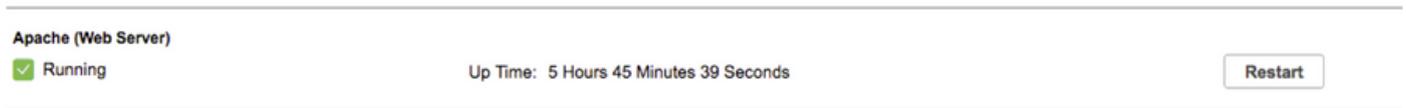


Passaggio 4. Nella GUI Web di PCP, selezionare **Amministrazione > Aggiornamenti > Sezione Certificati SSL**, fare clic su **Carica**, scegliere il certificato generato e fare clic su **Carica**, come mostrato nell'immagine.

Nota: È necessario caricare solo il certificato del server Web PCP. Non è necessario caricare i certificati radice poiché PCP è un server a nodo singolo.



Passaggio 5. Dopo aver caricato il certificato firmato dalla CA, selezionare **Amministrazione > Gestione processi** e fare clic su **Riavvia** servizi Apache (server Web) come mostrato nell'immagine.



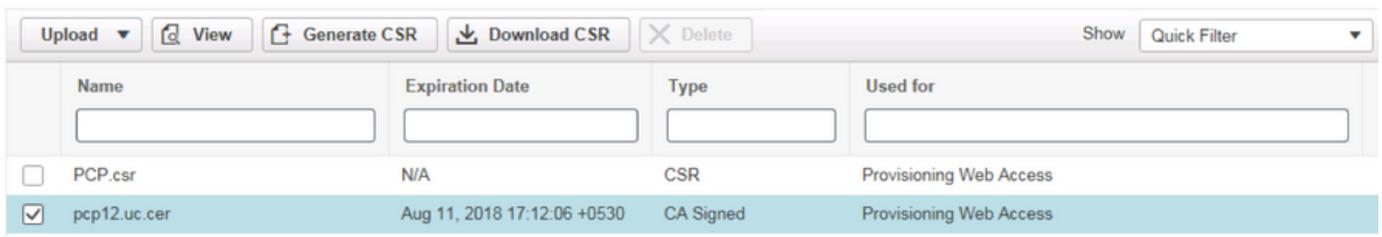
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Di seguito viene riportata la procedura per verificare che il certificato firmato dall'autorità di certificazione sia caricato nel provider di servizi di audioconferenza.

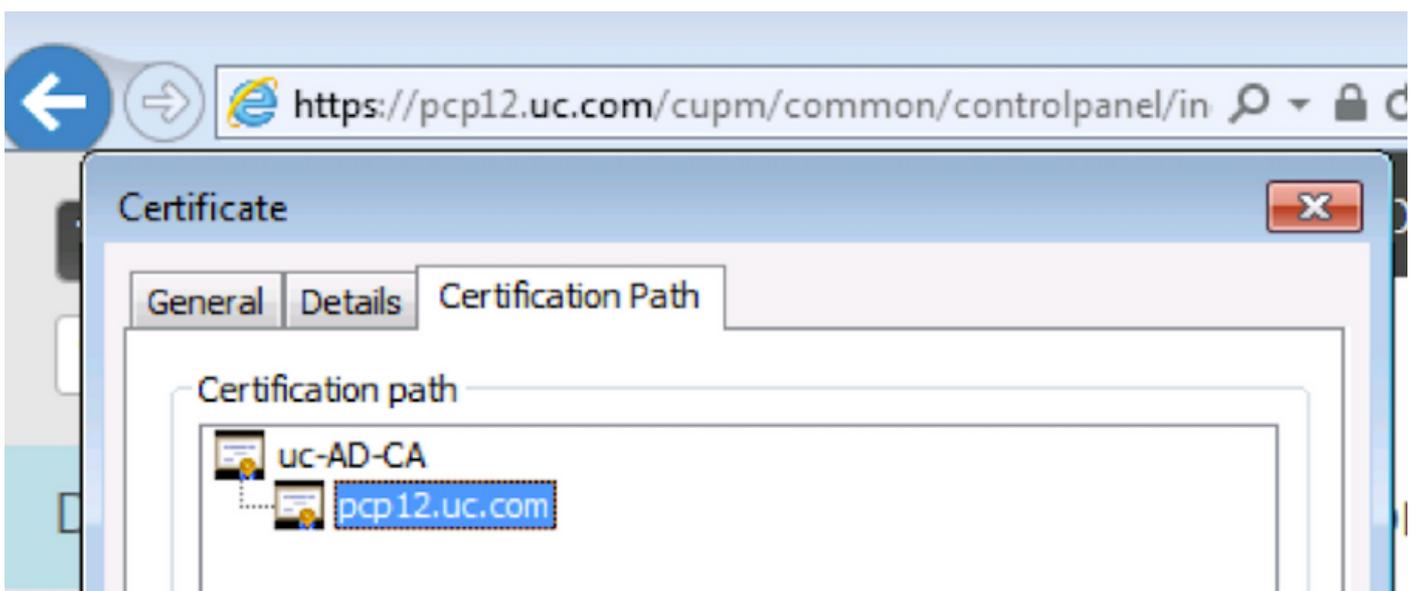
Passaggio 1. Il caricamento del certificato firmato dall'autorità di certificazione sostituisce il certificato autofirmato di PCP e il Tipo viene visualizzato come CA firmato con la data di scadenza, come mostrato nell'immagine.

▼ SSL Certificates



	Name	Expiration Date	Type	Used for
<input type="checkbox"/>	PCP.csr	N/A	CSR	Provisioning Web Access
<input checked="" type="checkbox"/>	pcp12.uc.cer	Aug 11, 2018 17:12:06 +0530	CA Signed	Provisioning Web Access

Passaggio 2. Accedere a PCP con l'FQDN e fare clic sul **simbolo di blocco sicuro** nel browser. Fare clic su **More information** (Ulteriori informazioni) e verificare il **Percorso certificazione**, come mostrato nell'immagine.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Da PCP 12.X, non è possibile accedere a CLI/Secure Shell (SSH) come root. Per qualsiasi problema, per caricare il certificato o se l'interfaccia Web PCP non è accessibile dopo il caricamento del certificato, contattare il Technical Assistance Center (TAC) di Cisco.

Informazioni correlate

- [Cisco Prime Collaboration Provisioning](#)
- [Raccolta dei log ShowTech dalla GUI di Prime Collaboration Provisioning](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)