

# Configura certificato di terze parti per UCS Central

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Creare il punto attendibile](#)

[Creazione dell'anello di chiavi e di CSR](#)

[Applicazione dell'anello chiave](#)

[Convalida](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive la best practice per configurare un certificato di terze parti nel software Cisco Unified Computing System Central (UCS Central).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco UCS Central
- CA (Certificate Authority)
- OpenSSL

### Componenti usati

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

- UCS Central 2.0(1q)
- Servizi certificati Microsoft Active Directory
- Windows 11 Pro N
- OpenSSL 3.1.0

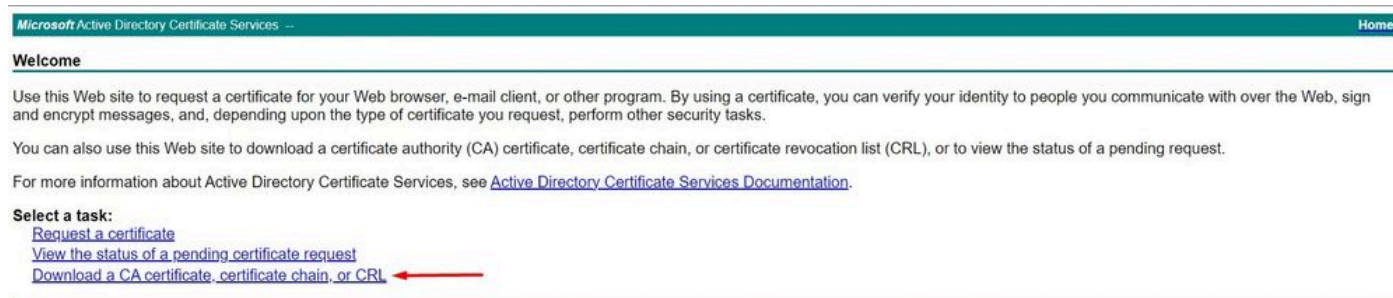
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

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

Scaricare la catena di certificati dall'autorità di certificazione.

### 1. Scaricare la catena di certificati dall'Autorità di certificazione (CA).



Microsoft Active Directory Certificate Services -- 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.

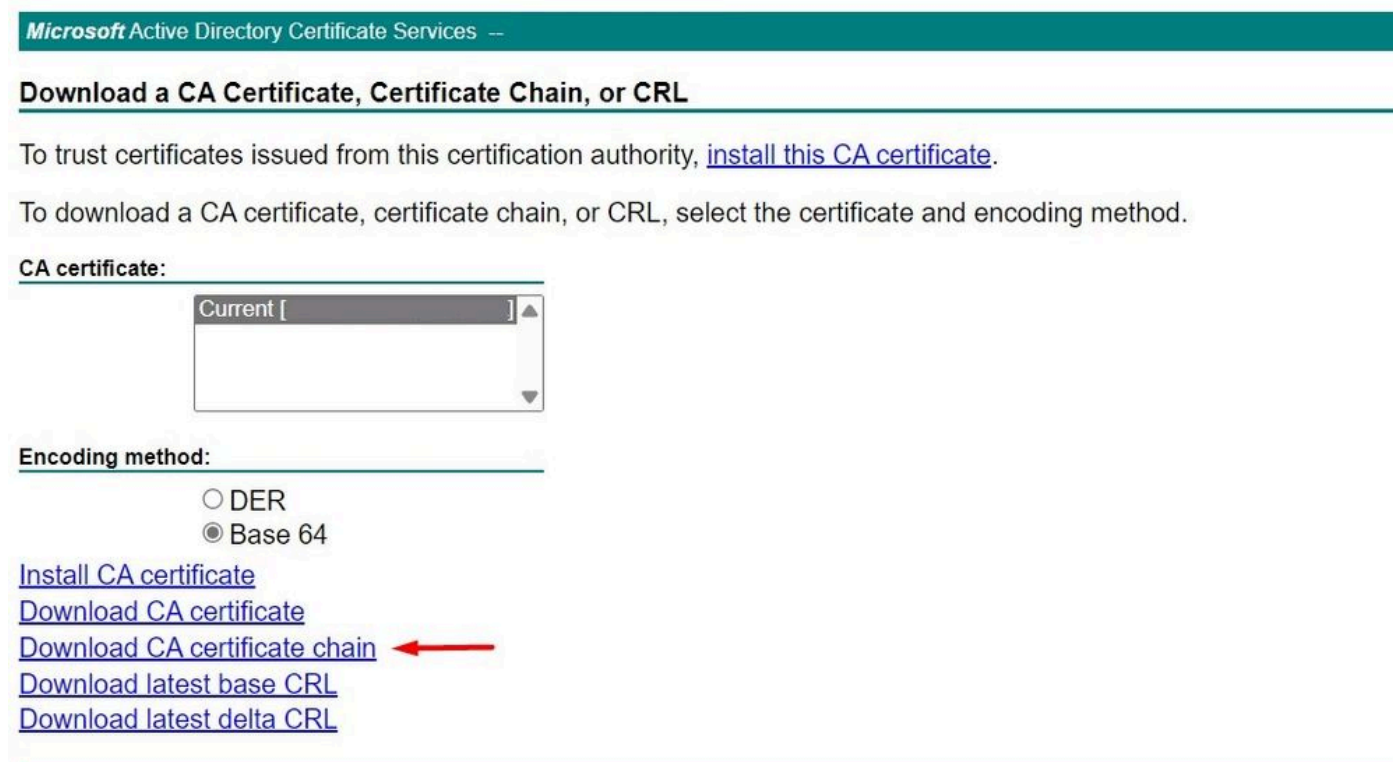
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#) ←

Scaricare una catena di certificati dalla CA

### 2. Impostare la codifica su Base 64 e scaricare la catena di certificati CA.



Microsoft Active Directory Certificate Services -- Home

**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

Current [ ] ▲▼

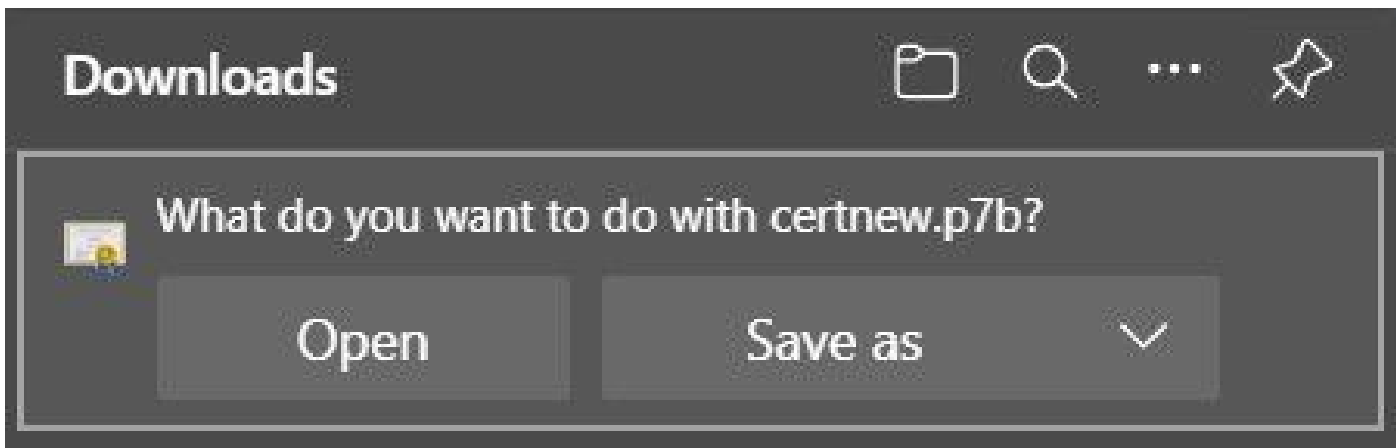
**Encoding method:**

- DER
- Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#) ←
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

Impostare la codifica su Base 64 e scaricare la catena di certificati CA

### 3. La catena di certificati CA è in formato PB7.



Il certificato è in formato PB7

4. Il certificato deve essere convertito in formato PEM con lo strumento OpenSSL. Per verificare se Open SSL è installato in Windows, utilizzare il comando `openssl version`.

```
C:\Program Files\OpenSSL-Win64\bin>openssl version
OpenSSL 3.1.0 14 Mar 2023 (Library: OpenSSL 3.1.0 14 Mar 2023)
```

Controlla se OpenSSL è installato

---

 Nota:l'installazione di OpenSSL non rientra nell'ambito di questo articolo.

---

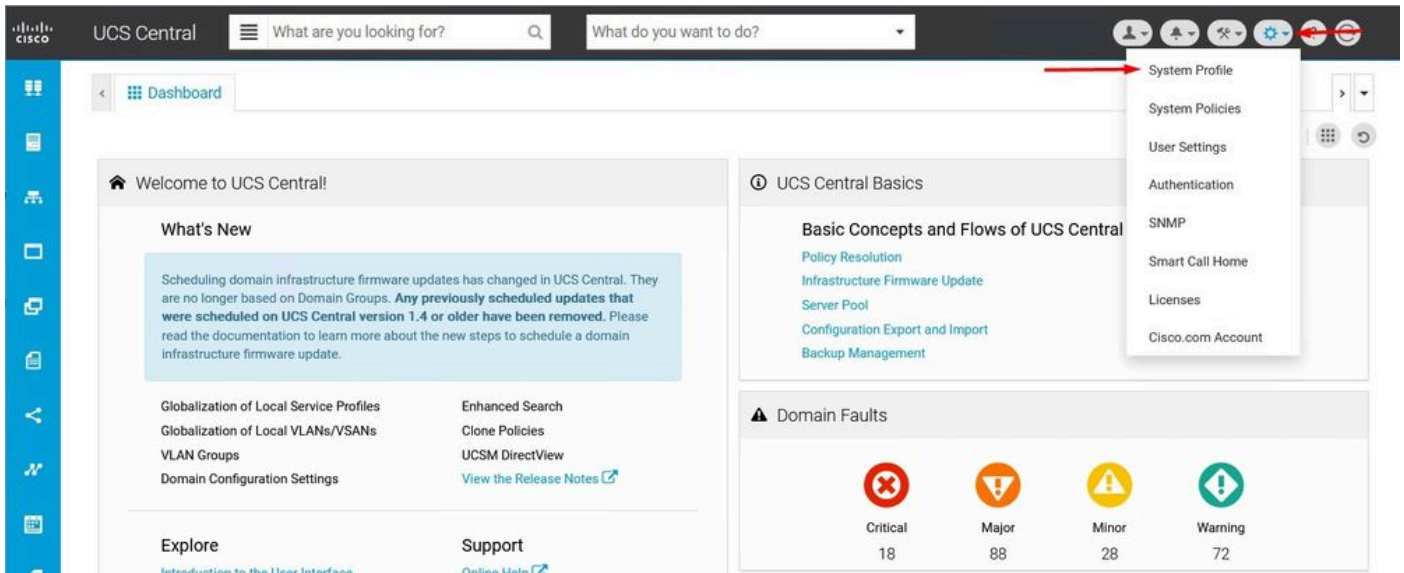
5.Se è installato OpenSSL, eseguire il comando `openssl pkcs7 -print_certs -in <nome_cert>.p7b -out <nome_cert>.pem` per eseguire la conversione. Assicurarsi di utilizzare il percorso in cui è stato salvato il certificato.

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs7 -print_certs -in C://Users/ /Desktop/certnew.p7b -out C://Users/ /Desktop/certnew.pem
```

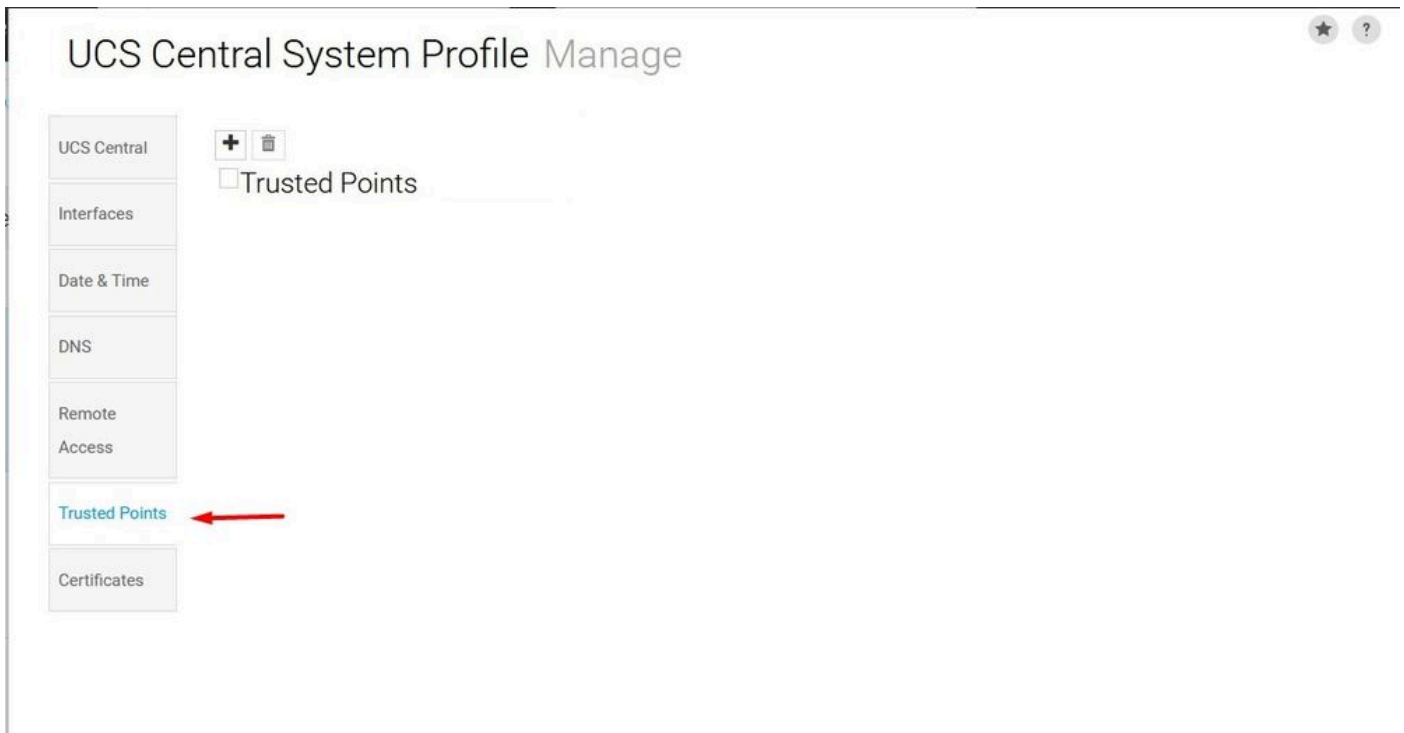
Converte il certificato P7B nel formato PEM

## Creare il punto attendibile

1. Fare clic su Icona Configurazione di sistema > Profilo di sistema > Trusted Points.



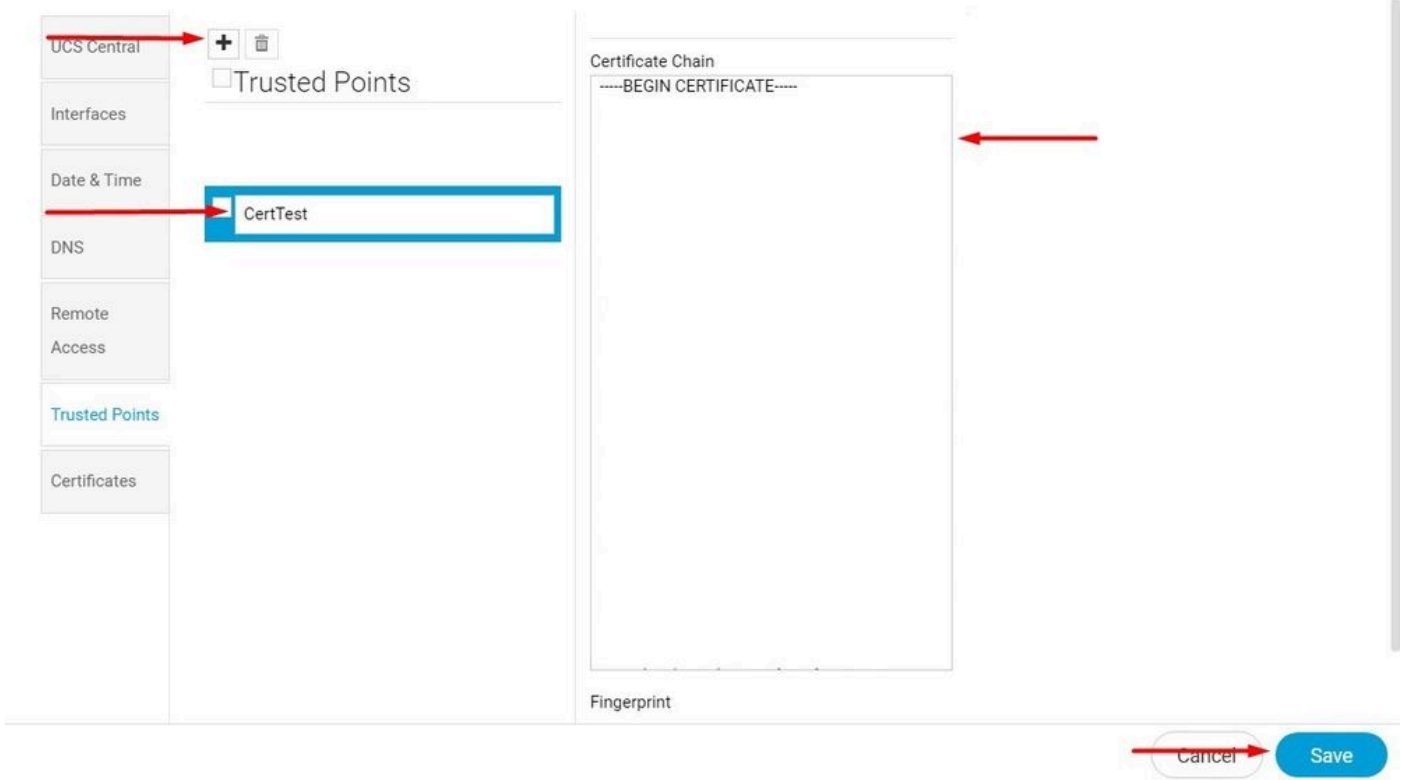
UCS Central System



ProfileUCS Central Trusted Point

2. Fare clic sull'icona + (più) per aggiungere un nuovo Trusted Point. Scrivere un nome e incollarlo nel contenuto del certificato PEM. Fare clic su Salva per applicare le modifiche.

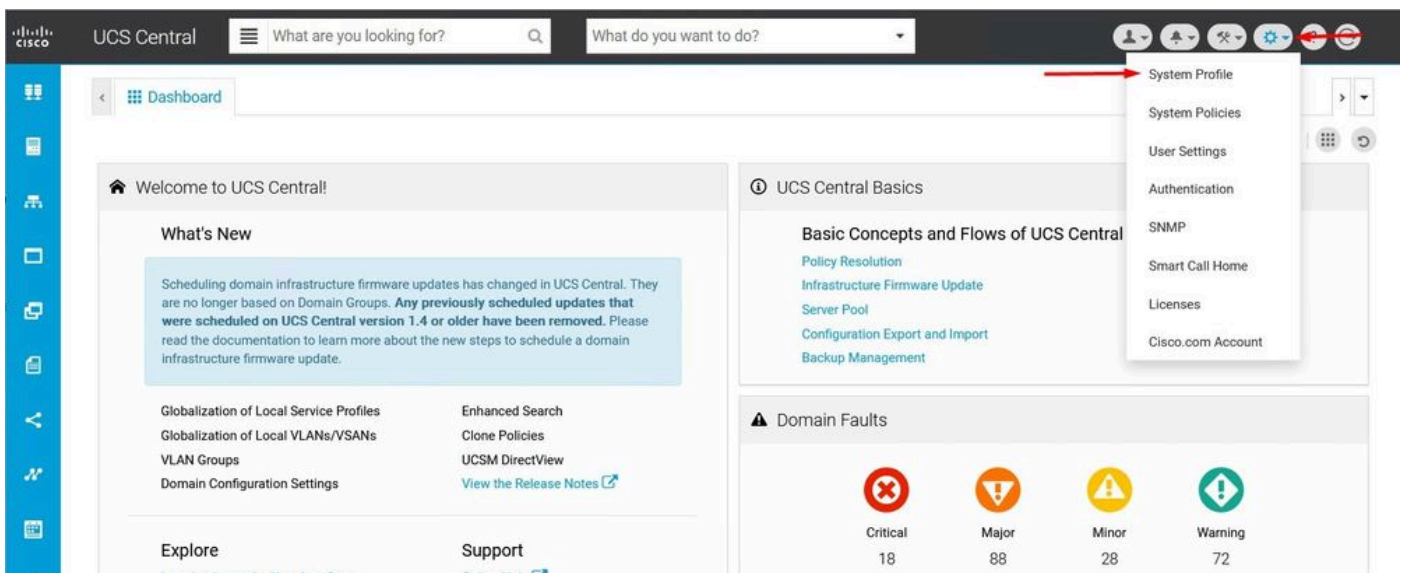
# UCS Central System Profile Manage



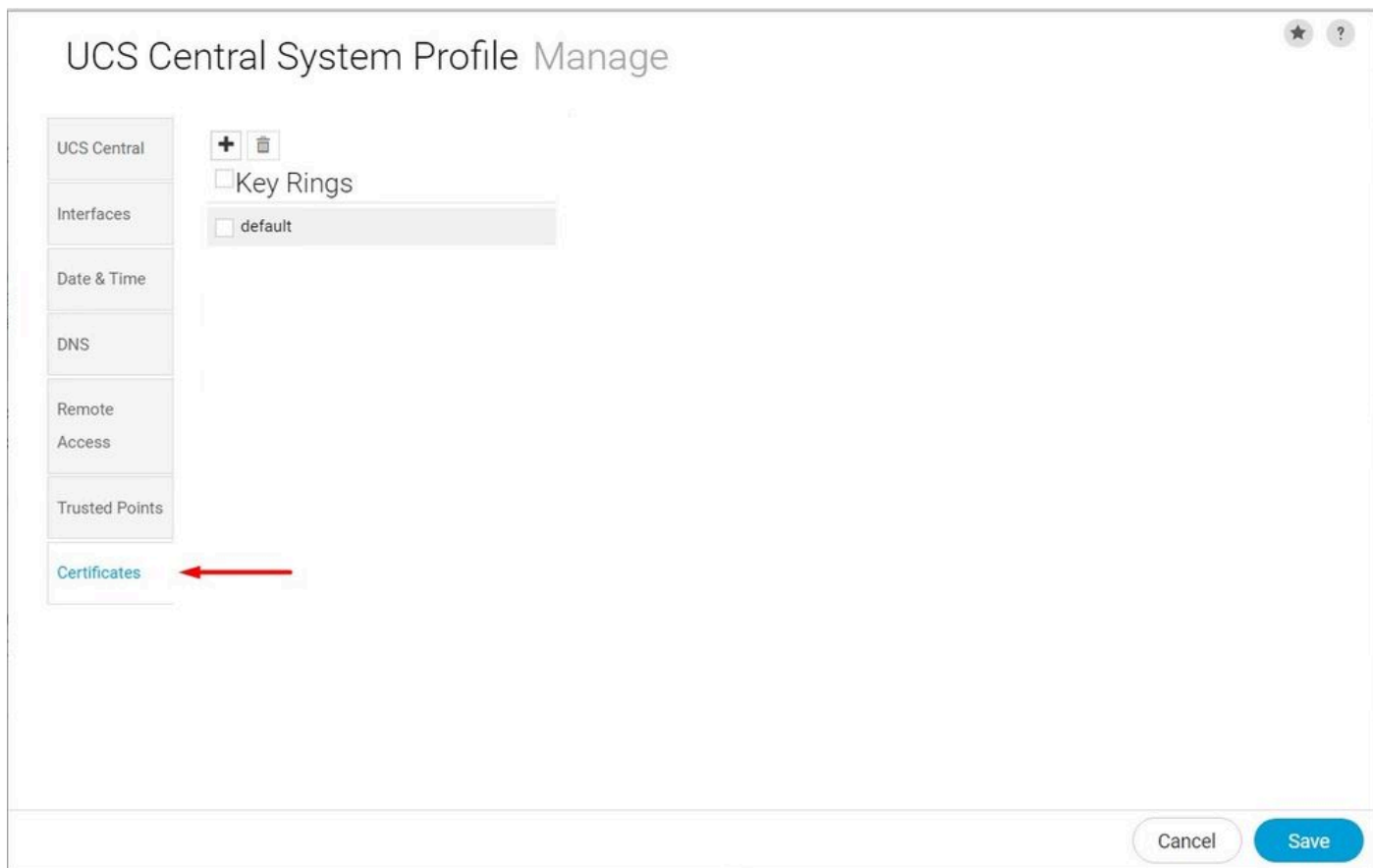
Copia catena di certificati

## Creazione dell'anello di chiavi e di CSR

1. Fare clic su Icona Configurazione di sistema > Profilo di sistema > Certificati.



UCS Central System



ProfileCertificati UCS Central

2. Fare clic sul pulsante più per aggiungere un nuovo Anello tasti. Scrivere un nome, lasciare il modulo con il valore predefinito (o modificarlo se necessario) e selezionare il punto di accesso sicuro creato in precedenza. Dopo aver impostato questi parametri, passare a Richiesta certificato.

# UCS Central System Profile Manage



UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+  Key Rings

default

KeyRingTest

Basic Certificate Request

Modulus: mod2048

Trusted Point: CertTest

Certificate Status: Valid

Certificate Chain

Cancel Save

Crea un nuovo anello chiavi

3. Inserire i valori necessari per richiedere un certificato e fare clic su Salva.

# UCS Central System Profile Manage



UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+  Key Rings

default

KeyRingTest

Basic Certificate Request

DNS

Locality

State

Country

Organization Name

Organization Unit Name

Email

Subject

Cancel Save

Immettere i dettagli per generare un certificato

#### 4. Tornare all'anello di chiavi creato e copiare il certificato generato.

The screenshot shows the 'UCS Central System Profile Manage' interface. On the left, a sidebar lists various system settings: UCS Central, Interfaces, Date & Time, DNS, Remote Access, Trusted Points, and Certificates. Under 'Key Rings', 'KeyRingTest' is selected. A red arrow points from this selection to the main content area. The main area has two tabs: 'Basic' and 'Certificate Request'. The 'Certificate Request' tab is active, showing a 'Certificate Chain' field with the text '-----BEGIN CERTIFICATE REQUEST-----'. Below this are fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.


Copia il certificato generato

#### 5. Accedere alla CA e richiedere un certificato.

The screenshot shows the Microsoft Active Directory Certificate Services website. The page title is 'Microsoft Active Directory Certificate Services - mxsvlab-ADMXSV-CA'. The 'Welcome' section contains the following text: '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 [Active Directory Certificate Services Documentation](#). Select a task: [Request a certificate](#), [View the status of a pending certificate request](#), [Download a CA certificate, certificate chain, or CRL](#).' A red arrow points to the 'Request a certificate' link.

Richiedi certificato da CA

#### 6. Incollare il certificato generato in UCS Central e nella CA selezionare il modello Server Web e client. Fare clic su Invia per generare il certificato.

 **Nota:** quando si genera una richiesta di certificato in Cisco UCS Central, verificare che il certificato risultante includa gli utilizzi delle chiavi di autenticazione client e server SSL. Se si utilizza una CA dell'organizzazione (Enterprise) di Microsoft Windows, utilizzare il modello Computer o un altro modello appropriato che includa entrambi gli utilizzi principali, se il modello Computer non è disponibile.



### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

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

-----END CERTIFICATE REQUEST-----

**Certificate Template:**

Web Server and Client

**Additional Attributes:**

Attributes:

Submit >

Genera un certificato da utilizzare nell'anello chiave creato

7. Convertire il nuovo certificato in PEM utilizzando il comando `openssl pkcs7 -print_certs -in <nome_cert>.p7b -out <nome_cert>.pem`.

8. Copiare il contenuto del certificato PEM e passare all'anello chiave creato per incollare il contenuto. Selezionare il Trusted Point creato e salvare la configurazione.

## UCS Central System Profile Manage

UCS Central

Interfaces

Date & Time

DNS

Remote Access

Trusted Points

Certificates

+ -

Key Rings

default

KeyRingTest

Basic Certificate Request

**KeyRingTest**

Modulus

mod2048

Trusted Point

CertTest

Certificate Status

Empty Cert

Certificate Chain

-----BEGIN CERTIFICATE-----

Cancel Save

Incollare il certificato richiesto nell'anello della chiave

## Applicazione dell'anello chiave

1. Passare a Profilo di sistema > Accesso remoto > Gruppo di chiavi, selezionare il gruppo di chiavi creato e fare clic su Salva. UCS Central chiude la sessione corrente.

# UCS Central System Profile Manage



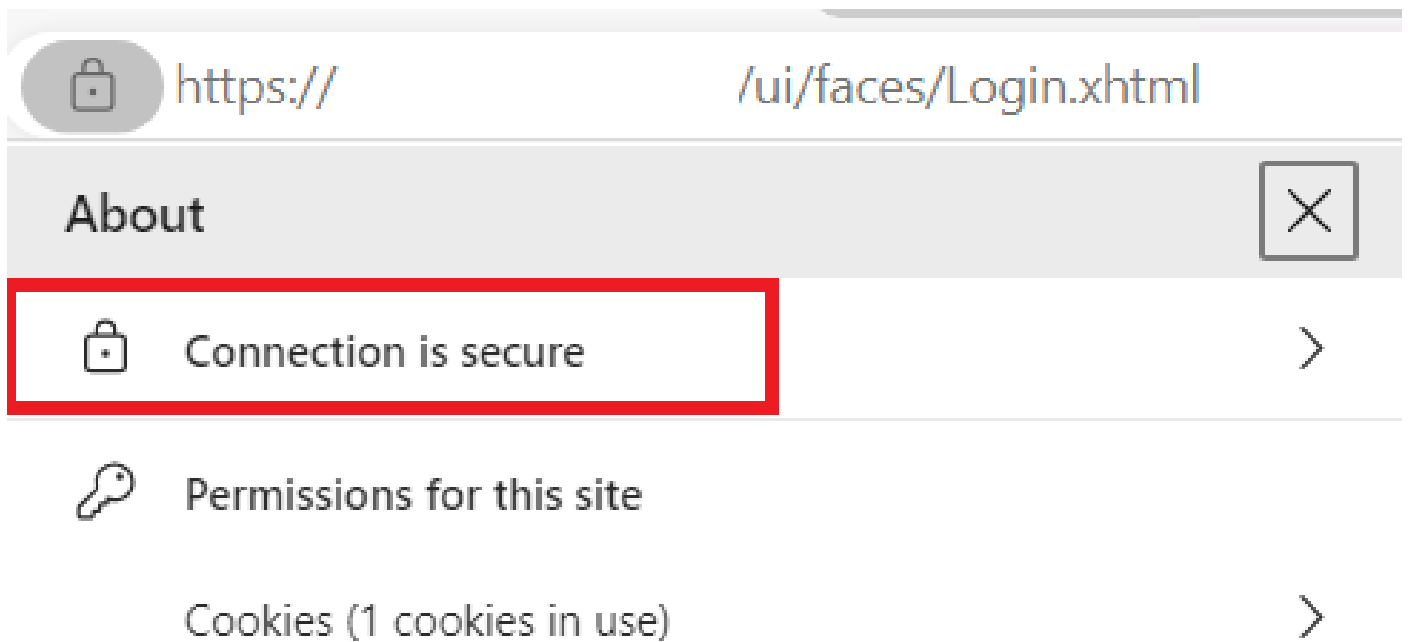
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Cancel Save

Selezionare la ghiera di chiave creata

## Convalida

1. Attendere che UCS Central sia accessibile e fare clic sul blocco accanto a https://. Il sito è protetto.



UCS Central è sicuro

# Risoluzione dei problemi

Verificare se il certificato generato include gli utilizzi delle chiavi di autenticazione client e server SSL.

Quando il certificato richiesto alla CA non include la chiave di autenticazione server e client SSL, viene visualizzato un messaggio di errore che indica "Certificato non valido. Impossibile utilizzare il certificato per l'autenticazione del server TLS. Viene visualizzato il messaggio "verificare le estensioni di utilizzo della chiave".

**Invalid certificate: This certificate cannot be used for TLS server authentication, check key usage extensions.**

Errore relativo alle chiavi di autorizzazione del server TLS

Per verificare se il certificato in formato PEM creato dal modello selezionato nella CA dispone degli utilizzi corretti della chiave di autenticazione server, è possibile utilizzare il comando `openssl x509 -in <certificato_utente>.pem -text -noout`. È necessario visualizzare Autenticazione server Web e Autenticazione client Web nella sezione Utilizzo chiave esteso.

```
21:75
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Subject Alternative Name: critical
    DNS:
  X509v3 Subject Key Identifier:

  X509v3 Authority Key Identifier:

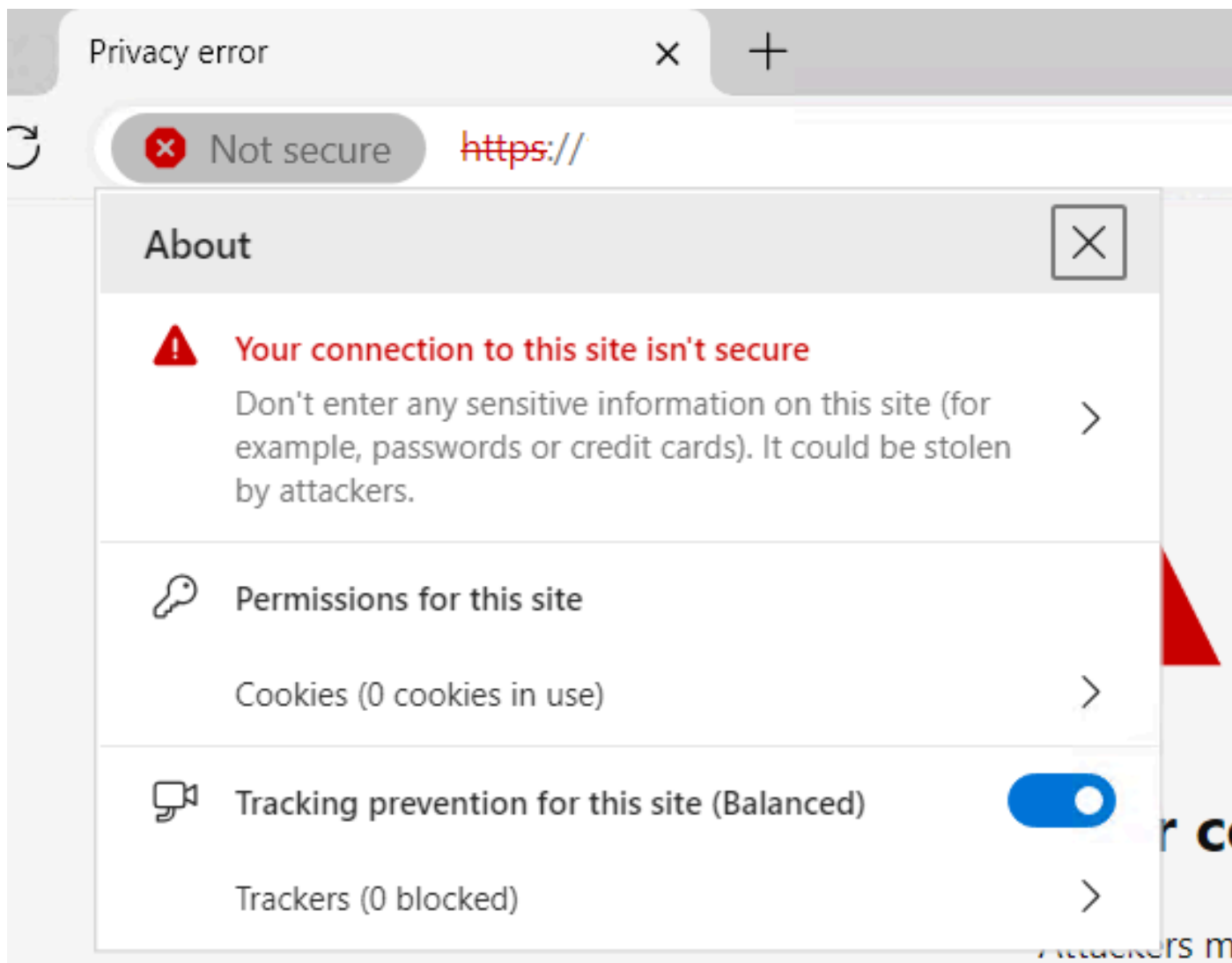
  X509v3 CRL Distribution Points:
    Full Name:

  Authority Information Access:
```

Chiave di autorizzazione server Web e client Web nel certificato richiesto

UCS Central è ancora contrassegnato come sito non sicuro.

Talvolta, dopo la configurazione del certificato di terze parti, la connessione è ancora contrassegnata dal browser.



UCS Central è ancora un sito non protetto

Per verificare se il certificato viene applicato correttamente, verificare che il dispositivo consideri attendibile l'Autorità di certificazione.

## Informazioni correlate

- [Cisco UCS Central Administration Guide, versione 2.0](#)
- [Supporto tecnico Cisco e download](#)

## 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).