

為UCS Central配置第三方證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[建立信任點](#)

[建立金鑰環和CSR](#)

[套用金鑰環](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹在Cisco Unified Computing System Central Software (UCS Central)中配置第三方證書的最佳做法。

必要條件

需求

思科建議瞭解以下主題：

- Cisco UCS Central
- 憑證授權單位(CA)
- OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

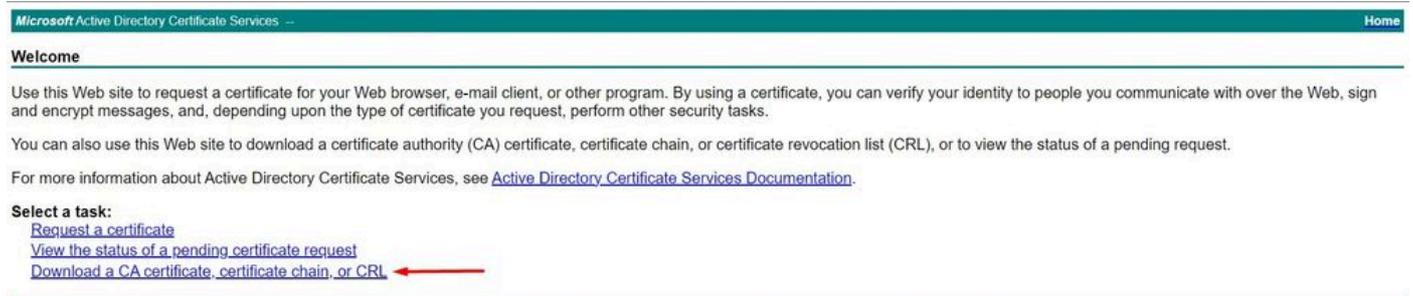
- UCS Central 2.0(1q)
- Microsoft Active Directory證書服務
- Windows 11專業版N
- OpenSSL 3.1.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

從證書頒發機構下載證書鏈。

1. 從證書頒發機構(CA)下載證書鏈。



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.

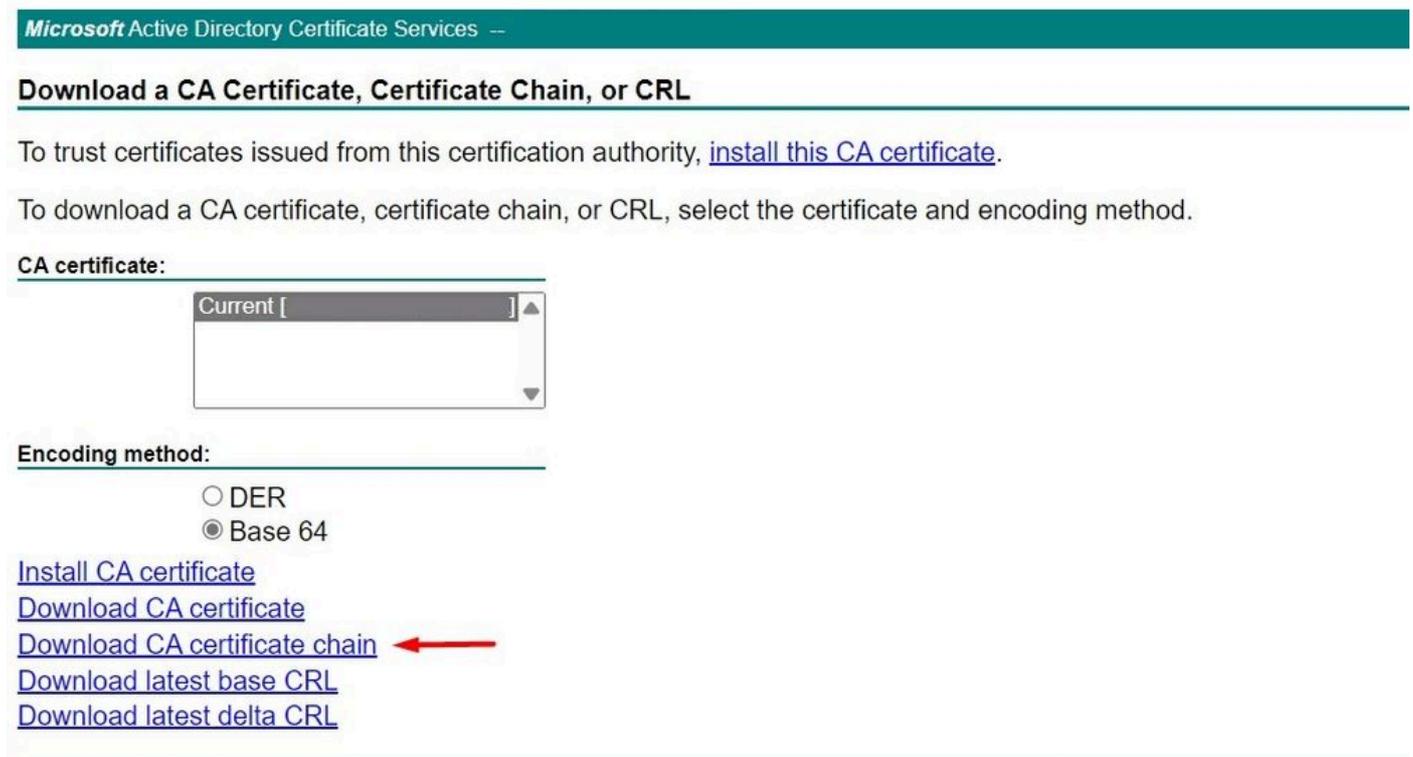
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

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

從CA下載證書鏈

2. 將編碼設定為Base 64並下載CA證書鏈。



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 []

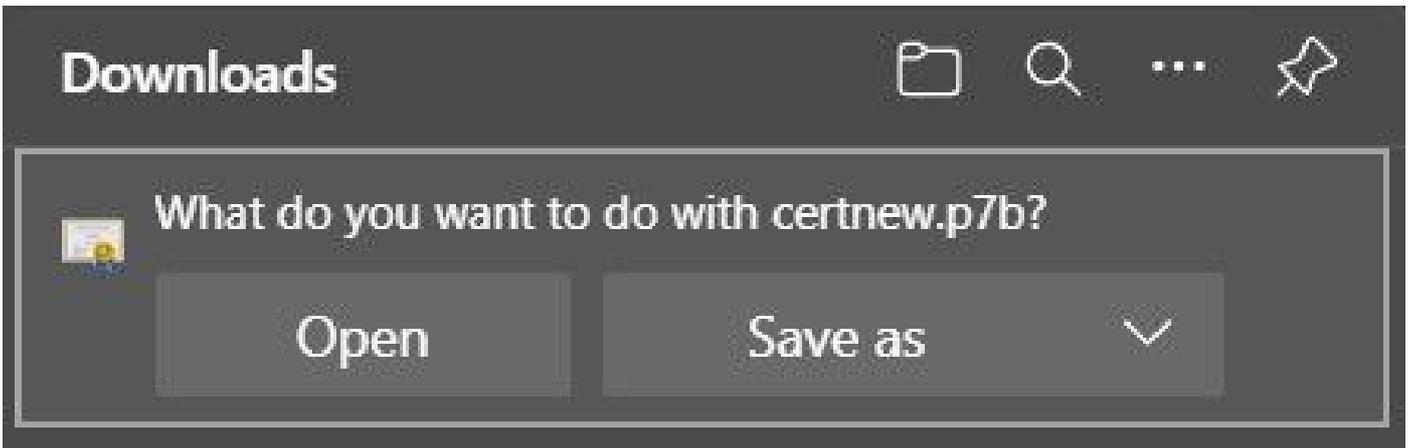
Encoding method:

- DER
- Base 64

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

將編碼設定為Base 64並下載CA證書鏈

3. 請注意，CA證書鏈為PB7格式。



憑證為P7B格式

4. 必須使用OpenSSL工具將憑證轉換為PEM格式。要檢查Windows中是否安裝了Open SSL，請使用命令`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)
```

檢查是否已安裝OpenSSL

 注意：OpenSSL安裝不在本文的討論範圍之內。

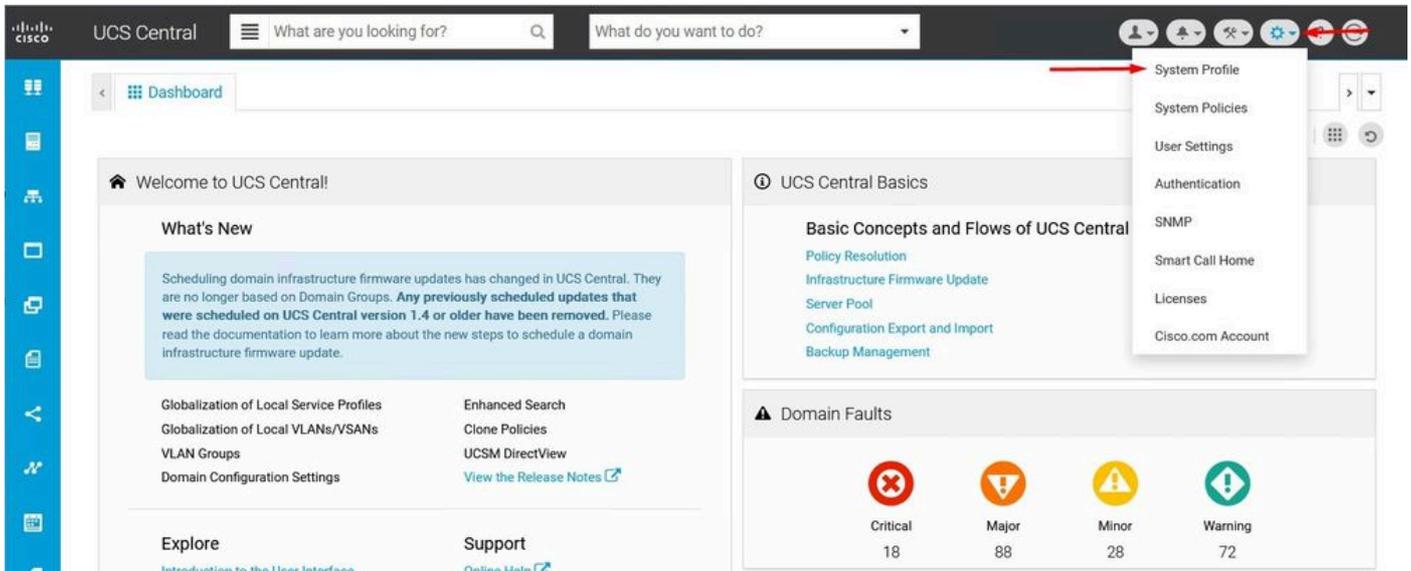
5. 如果已安裝OpenSSL，請執行命令`openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem`來執行轉換。請確定使用儲存憑證的路徑。

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

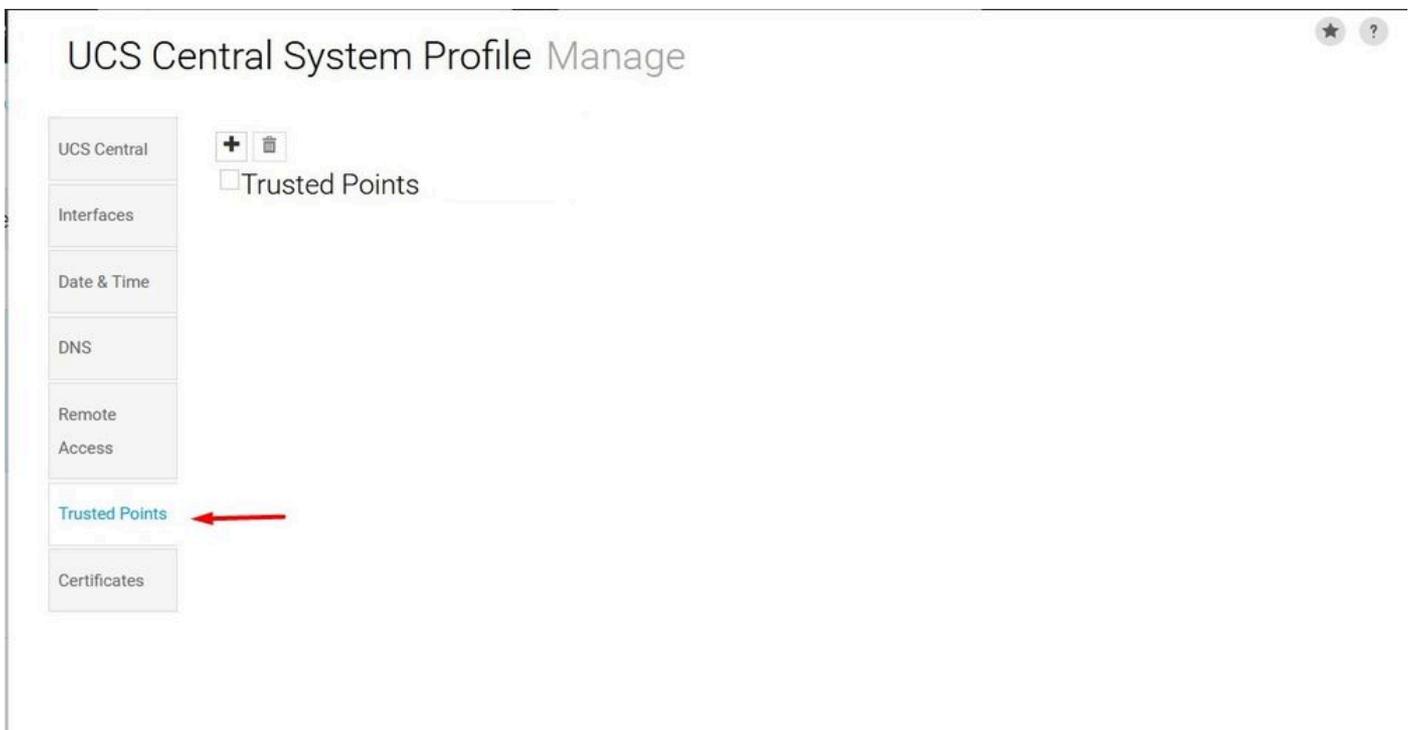
將P7B證書轉換為PEM格式

建立信任點

1. 按一下系統配置圖示>系統配置檔案>受信任點。



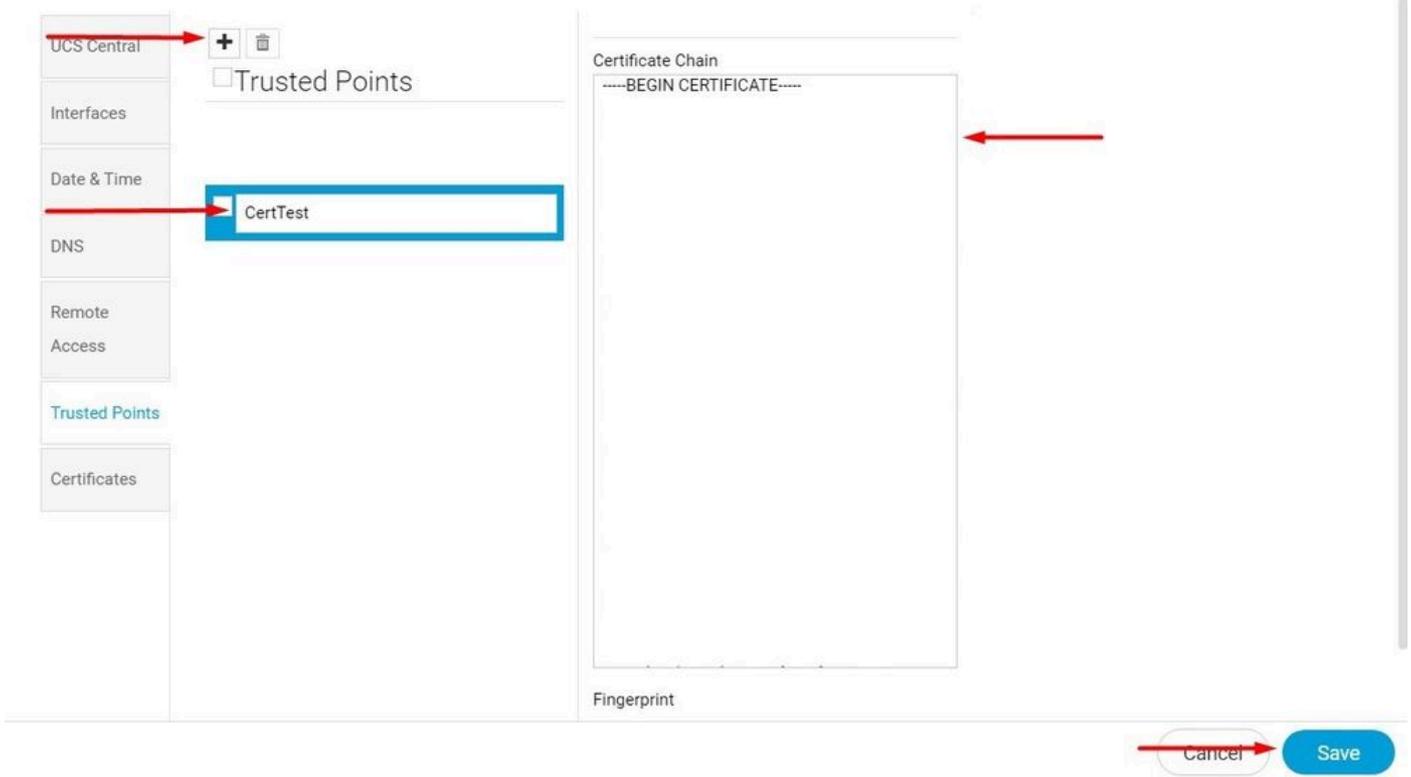
UCS中心系統



配置檔案UCS中心受信任點

2. 按一下+ (加號) 圖示以新增信任點。寫下名稱並貼上到PEM證書的內容中。按一下Save以應用更改。

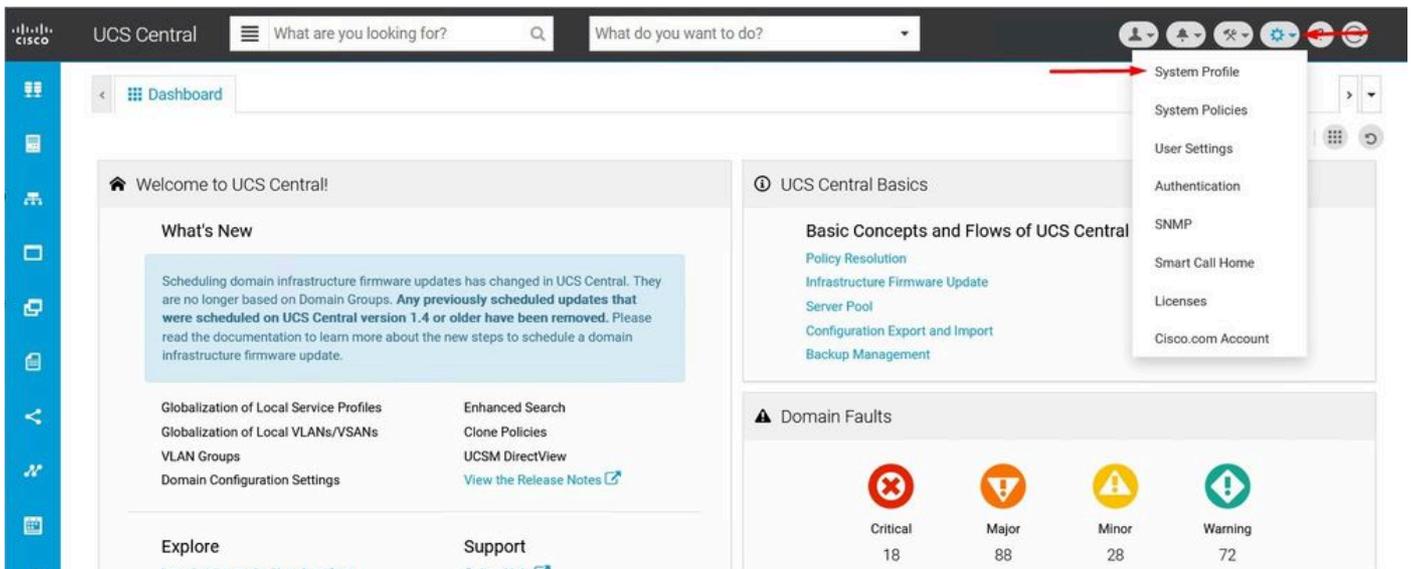
UCS Central System Profile Manage



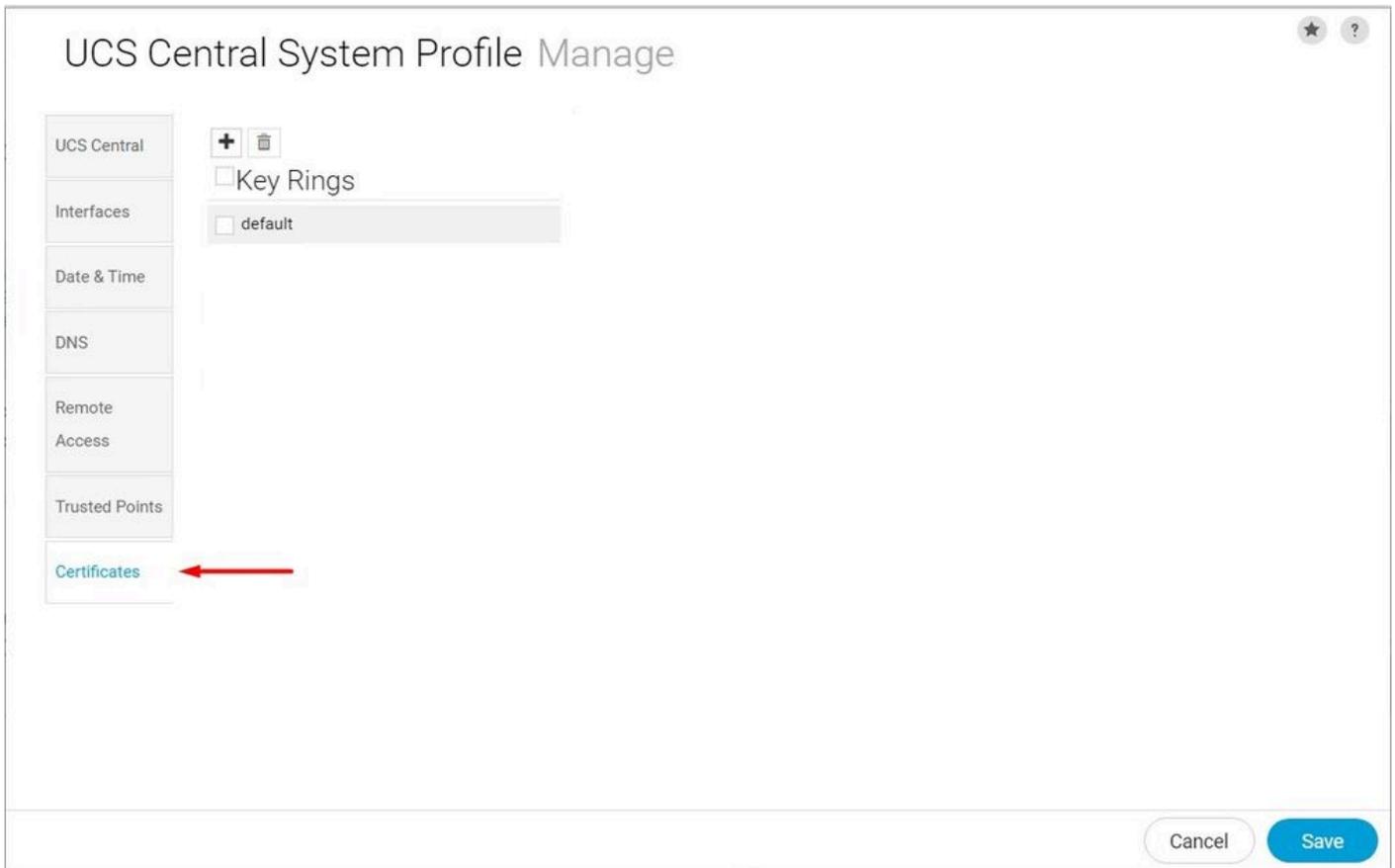
複製憑證鏈結

建立金鑰環和CSR

1. 按一下System Configuration icon > System Profile > Certificates。

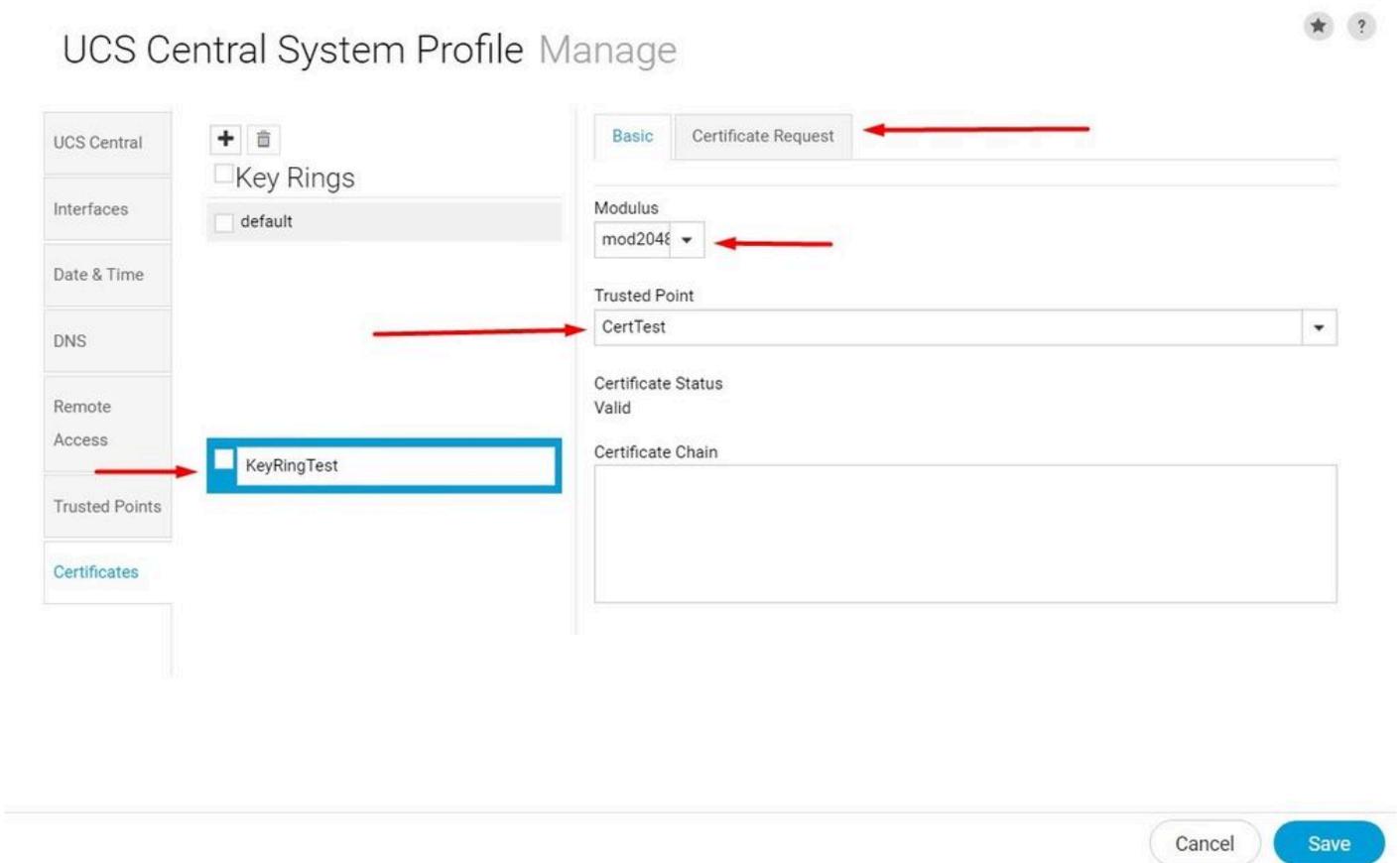


UCS中心系統



配置檔案UCS中心證書

2. 按一下加號圖示增加新的金鑰環。寫入名稱，將係數保留為預設值（或視需要修改），然後選取之前建立的「信任點」。設定好這些引數後，請轉到Certificate Request。



建立新的金鑰環

3. 輸入請求證書所需的值，然後按一下儲存。

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

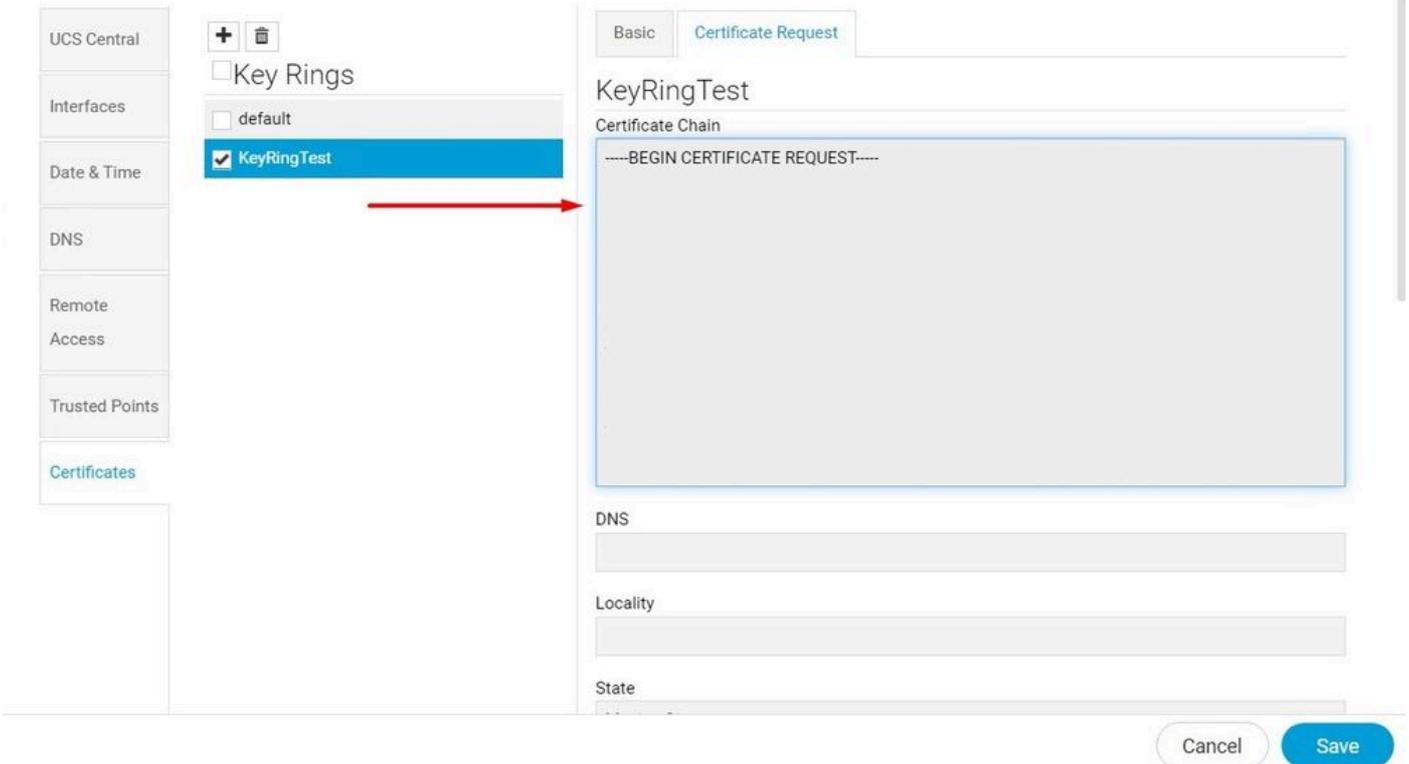
Email

Subject

Cancel Save

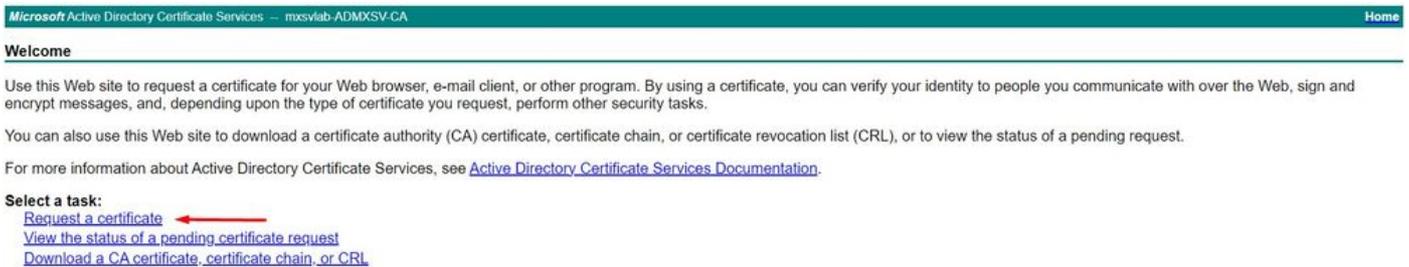
輸入詳細資訊以生成證書

4. 返回建立的金鑰環，並複製生成的證書。



複製產生的憑證

5. 轉到CA並請求證書。



向CA請求證書

6. 貼上在UCS Central中生成的證書，並在CA中選擇Web Server and Client模板。按一下Submit以生成證書。

 **注意：**在Cisco UCS Central中生成證書請求時，請確保生成的證書包含SSL客戶端和伺服器身份驗證金鑰用法。如果使用Microsoft Windows Enterprise CA，請利用Computer範本，或包含兩種主要用法的另一個適當範本（如果Computer範本無法使用）。

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 >

生成要在建立的金鑰環中使用的證書

7. 使用命令 `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` 將新證書轉換為 PEM。

8. 複製 PEM 證書的內容並轉到建立的金鑰環以貼上內容。選擇建立的信任點並儲存配置。

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

貼上金鑰環中要求的憑證

套用金鑰環

1. 導航到系統配置檔案>遠端訪問>金鑰環，選擇已建立的金鑰環，然後按一下儲存。UCS Central關閉當前會話。

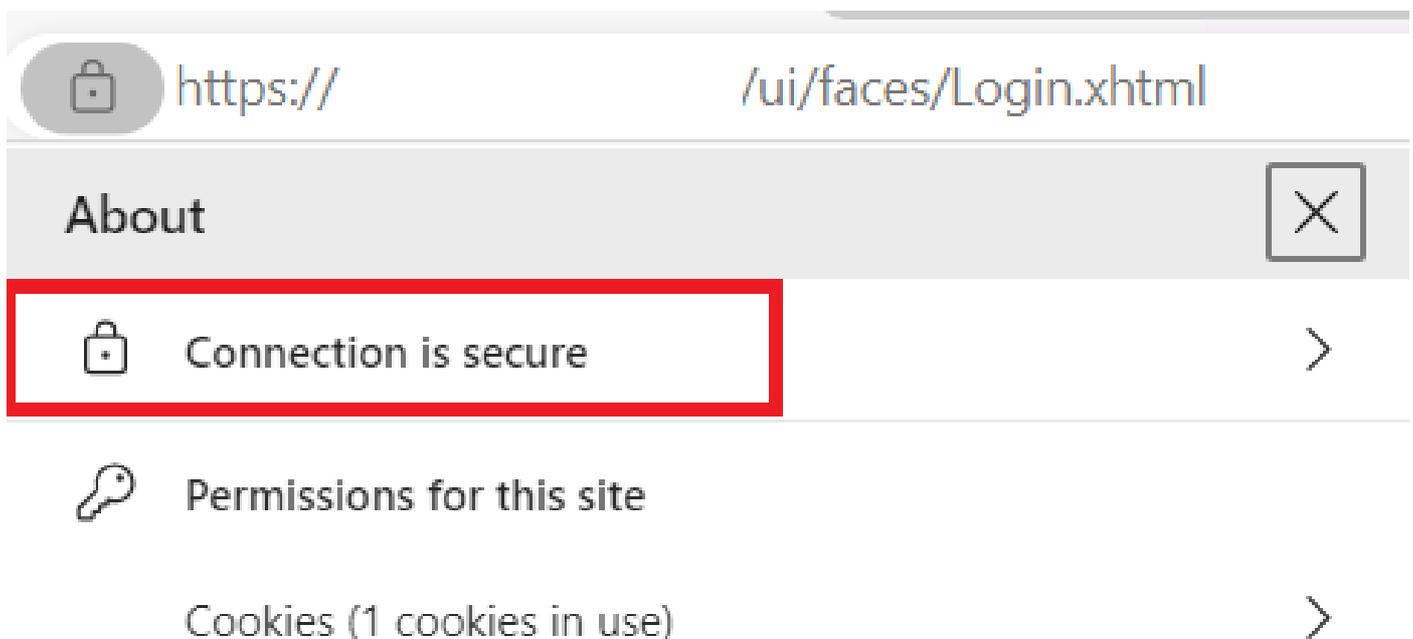
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

選擇建立的金鑰環

驗證

1. 請等待，直到可以訪問UCS Central，然後按一下https://旁邊的鎖。場地是安全的。



UCS Central是安全的

疑難排解

檢查生成的證書是否包含SSL客戶端和伺服器身份驗證金鑰用法。

當向CA請求的證書不包含SSL客戶端和伺服器身份驗證金鑰使用時，錯誤顯示「證書無效」。此憑證無法用於TLS伺服器驗證，檢查金鑰使用延伸」出現。

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

TLS伺服器授權金鑰相關錯誤

要驗證從CA中選擇的模板建立的PEM格式證書是否具有正確的伺服器身份驗證金鑰用法，可以使用命令 `openssl x509 -in <my_cert>.pem -text -noout`。您必須在擴展金鑰用法部分下看到Web Server Authentication和Web Client Authentication。

```
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:

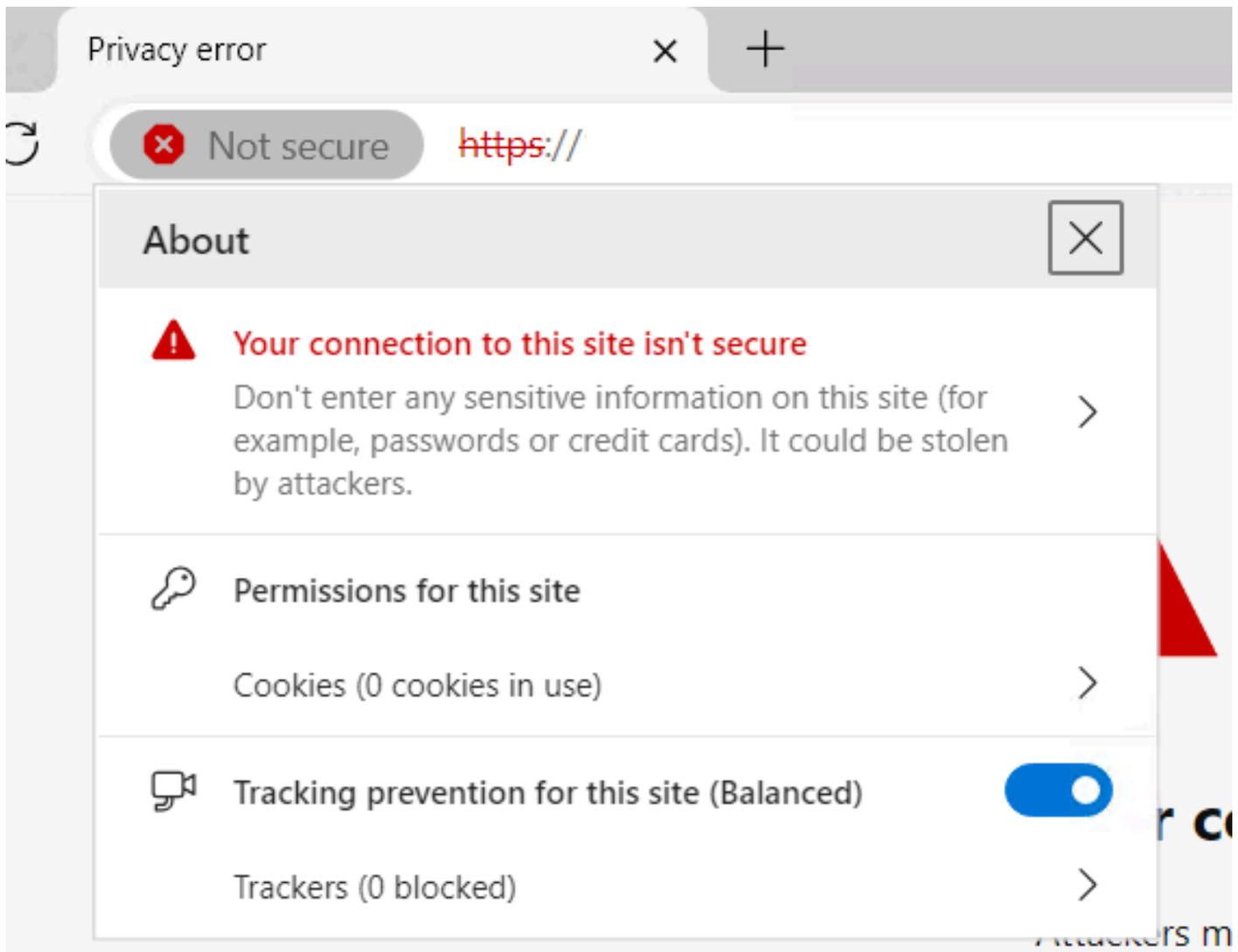
    X509v3 CRL Distribution Points:
    Full Name:

    Authority Information Access:
```

已請求證書中的Web伺服器和Web客戶端授權金鑰

UCS中心仍標籤為不安全站點。

有時，在配置第三方證書後，瀏覽器仍會標籤連線。



UCS Central仍是一個不安全的站點

要驗證是否正確應用了證書，請確保裝置信任證書頒發機構。

相關資訊

- [Cisco UCS中心管理指南2.0版](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。