

Konfigurieren eines Drittanbieterzertifikats für UCS Central

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Erstellen des vertrauenswürdigen Punkts](#)

[Erstellen von Keyring und CSR](#)

[Anwenden des Keyrings](#)

[Validierung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Best Practice für die Konfiguration eines Drittanbieterzertifikats in der Cisco Unified Computing System Central Software (UCS Central) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco UCS Central
- Zertifizierungsstelle
- OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

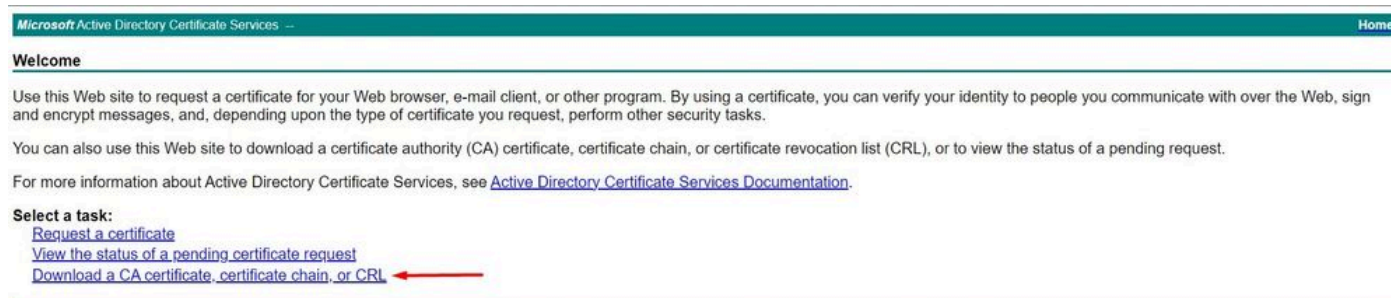
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Laden Sie die Zertifikatskette von der Zertifizierungsstelle herunter.

1. Laden Sie die Zertifikatskette von der Zertifizierungsstelle herunter.



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.

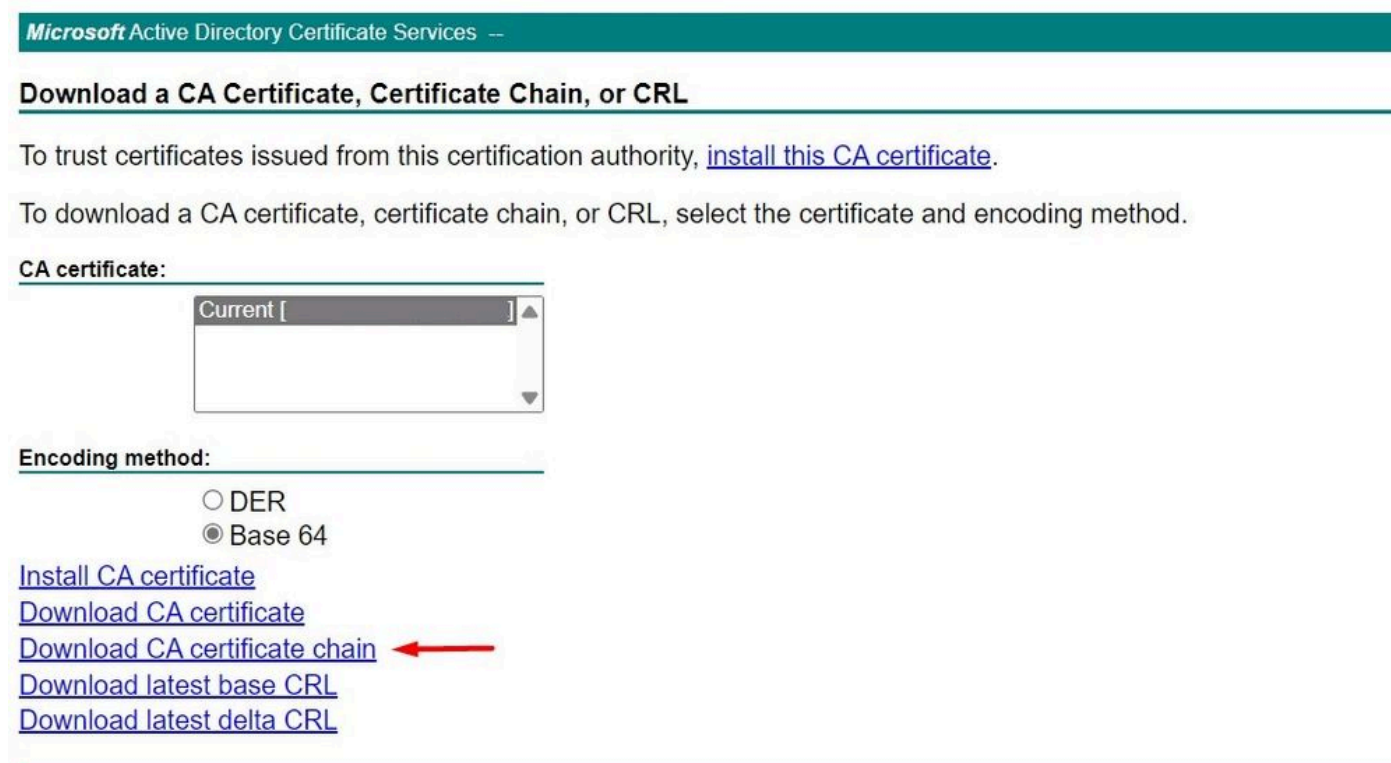
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

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

Zertifikatskette von CA herunterladen

2. Setzen Sie die Kodierung auf Basis 64 und laden Sie die Zertifizierungsstellen-Zertifikatskette herunter.



Microsoft Active Directory Certificate Services –

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:

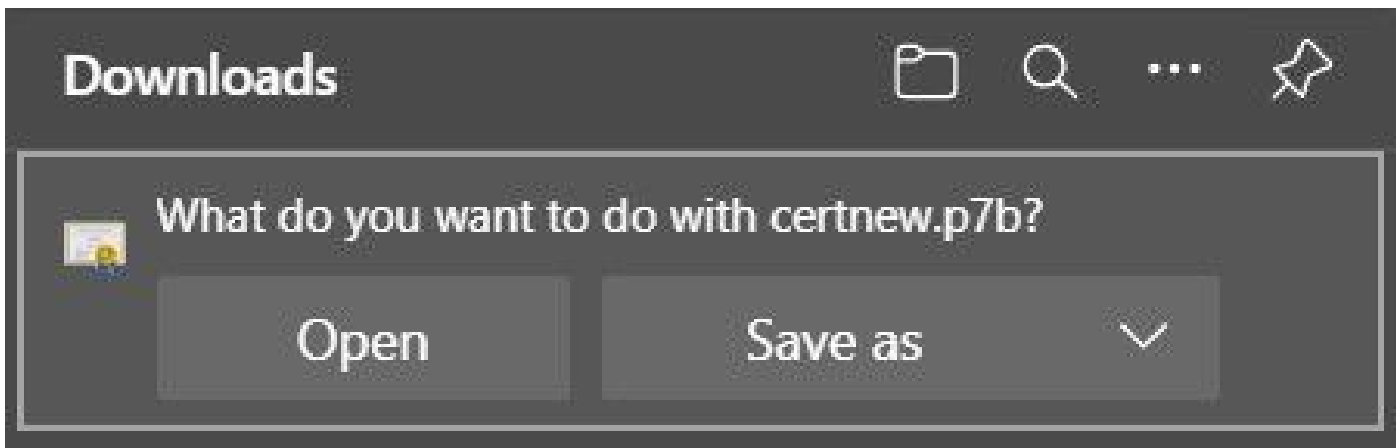
DER

Base 64

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

Legen Sie die Kodierung auf Basis 64 fest, und laden Sie die Zertifizierungsstellen-Zertifikatskette herunter.

3. Beachten Sie, dass die Zertifikatskette der Zertifizierungsstelle im PB7-Format vorliegt.




Das Zertifikat ist im PB7-Format.

4. Das Zertifikat muss mit OpenSSL in das PEM-Format konvertiert werden. Um zu überprüfen, ob Open SSL in Windows installiert ist, verwenden Sie den Befehl `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)
```

Überprüfen Sie, ob OpenSSL installiert ist

 Hinweis: Die OpenSSL-Installation wird in diesem Artikel nicht behandelt.

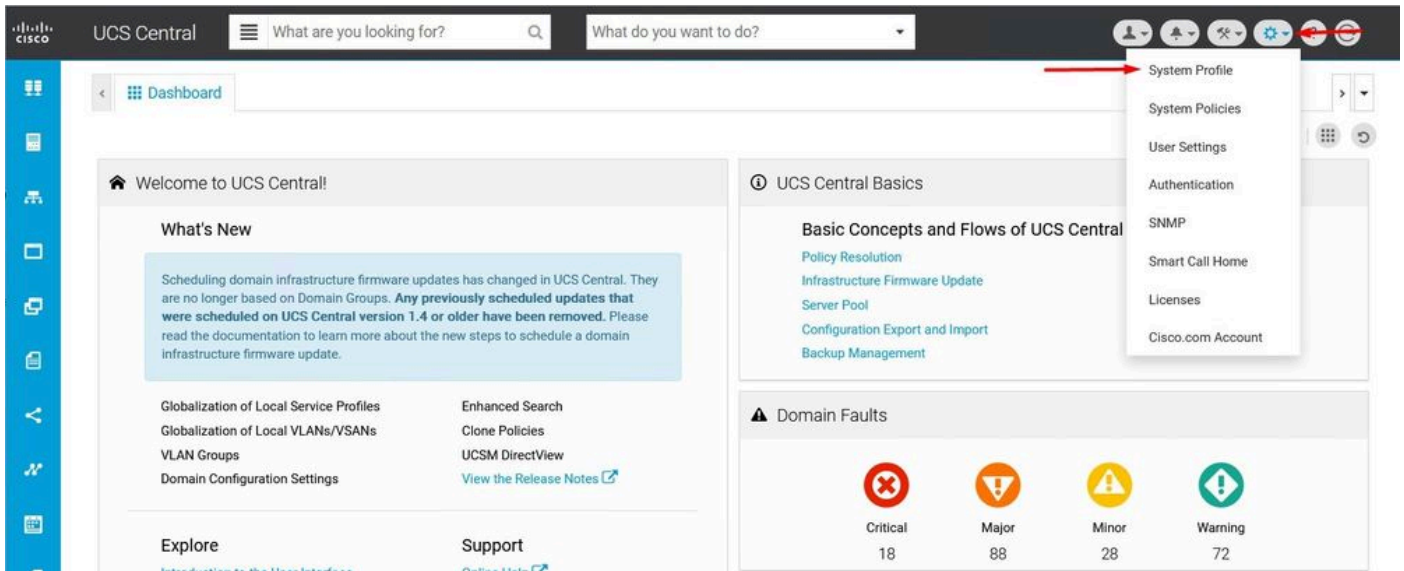
5. Wenn OpenSSL installiert ist, führen Sie den Befehl `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` aus, um die Konvertierung durchzuführen. Stellen Sie sicher, dass Sie den Pfad verwenden, unter dem das Zertifikat gespeichert ist.

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

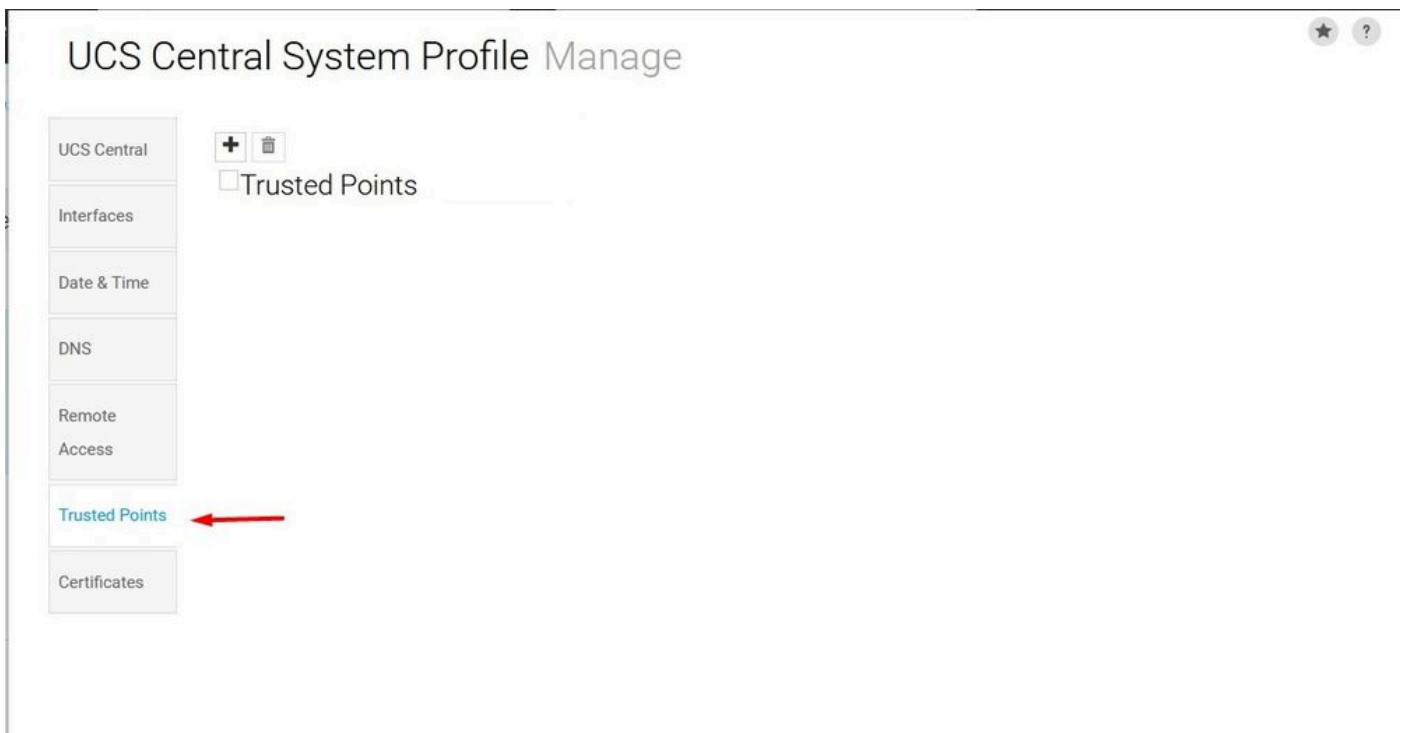
P7B-Zertifikat in PEM-Format konvertieren

Erstellen des vertrauenswürdigen Punkts

1. Klicken Sie auf das Symbol Systemkonfiguration > Systemprofil > Vertrauenswürdige Punkte.



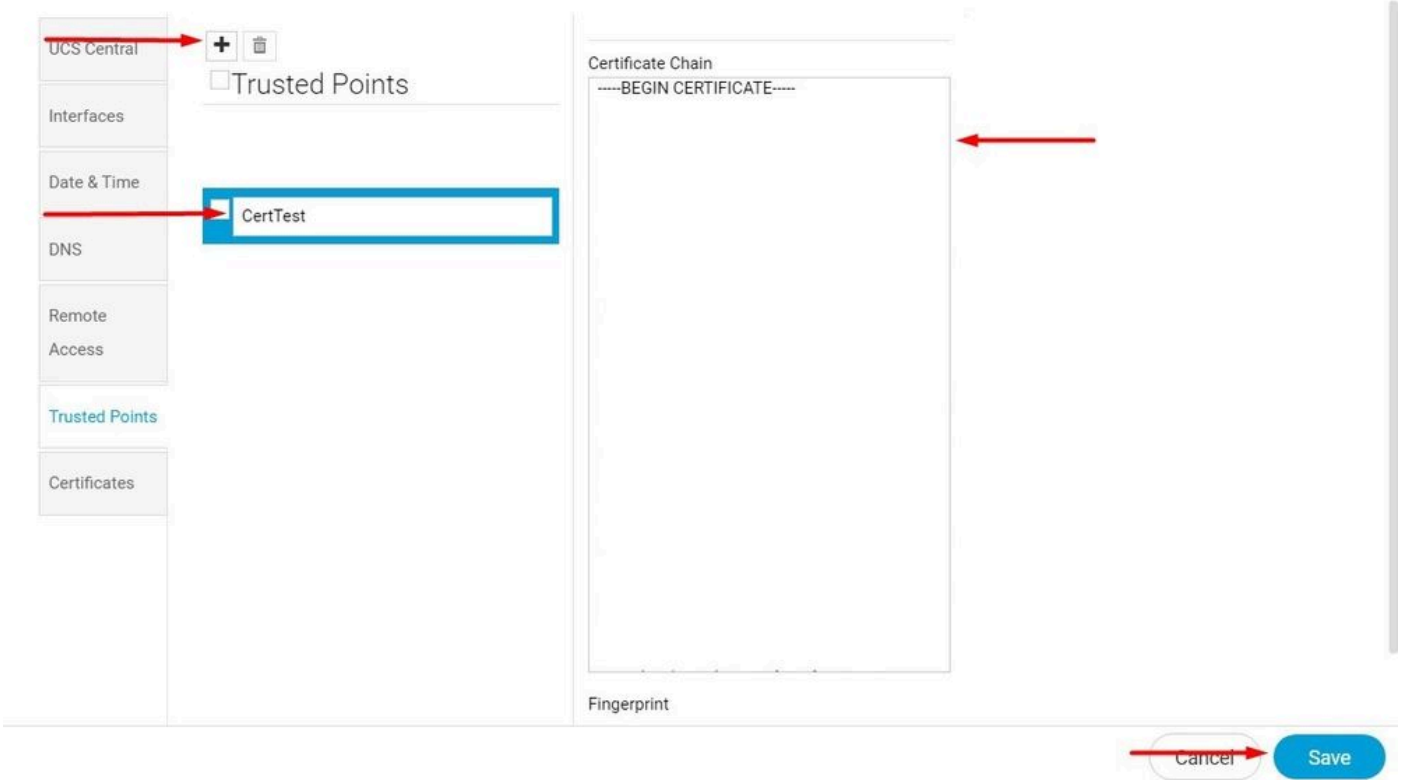
UCS Central-



SystemprofilUCS Central Trusted Points

2. Klicken Sie auf das Symbol + (Plus), um einen neuen Vertrauenswürdigen Punkt hinzuzufügen. Schreiben Sie einen Namen, und fügen Sie den Inhalt des PEM-Zertifikats ein. Klicken Sie auf Speichern, um die Änderungen zu übernehmen.

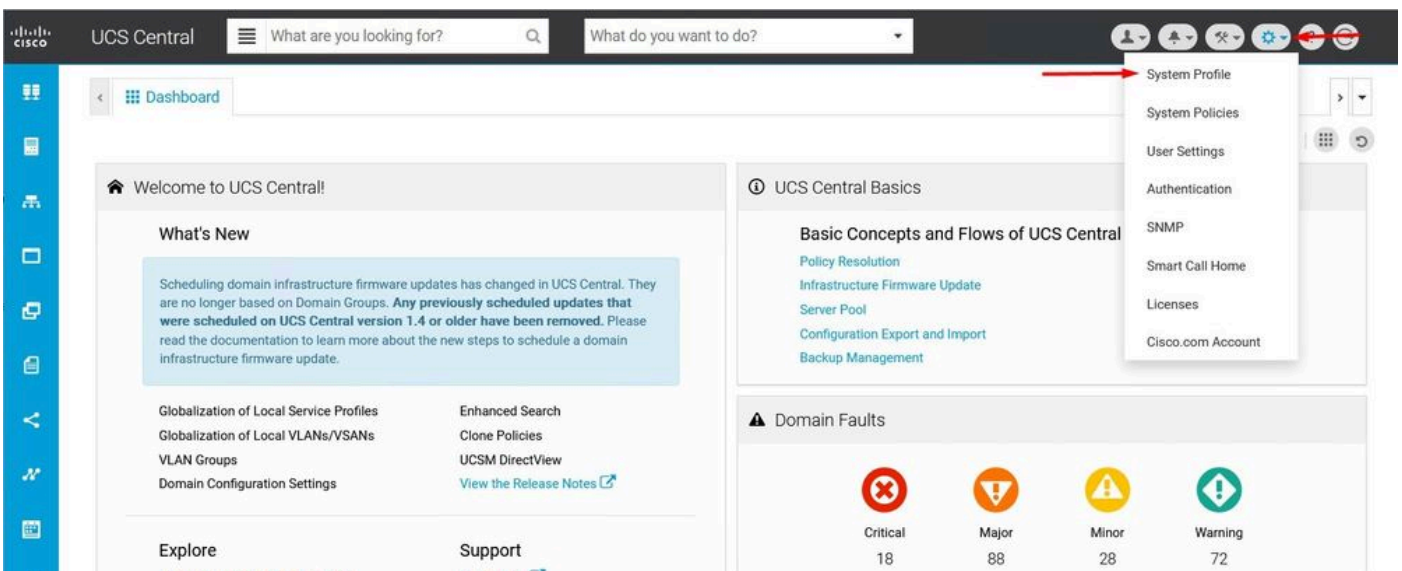
UCS Central System Profile Manage



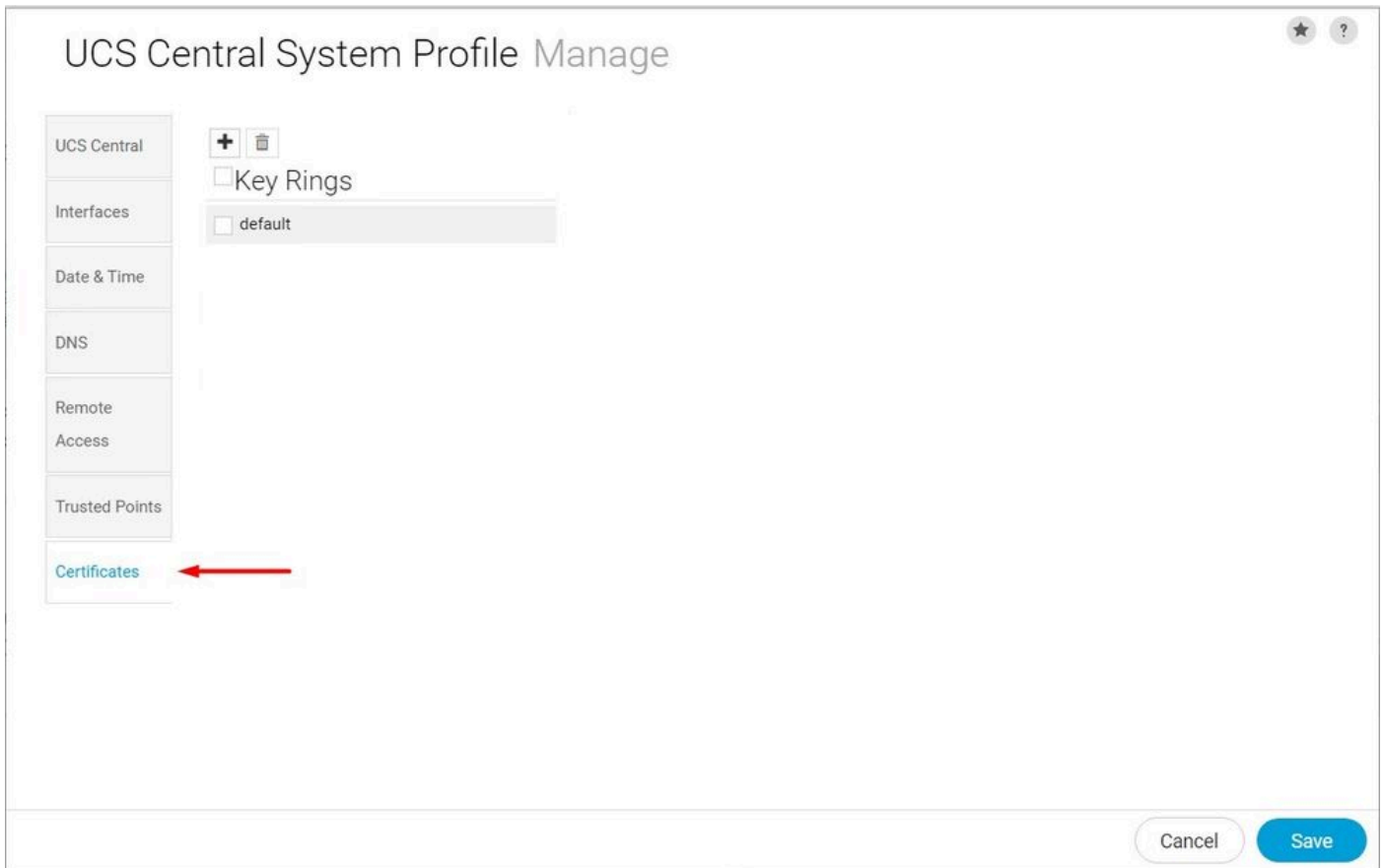
Zertifikatskette kopieren

Erstellen von Keyring und CSR

1. Klicken Sie auf das Symbol Systemkonfiguration > Systemprofil > Zertifikate.



UCS Central-



SystemprofilUCS Central-Zertifikate

2. Klicken Sie auf das Pluszeichen, um einen neuen Keyring hinzuzufügen. Schreiben Sie einen Namen, belassen Sie den Standardwert auf dem Modul (oder ändern Sie ihn ggf.), und wählen Sie den zuvor erstellten vertrauenswürdigen Punkt aus. Nach dem Festlegen dieser Parameter wechseln Sie zur Zertifikatanforderung.

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

Neuen Keyring erstellen

3. Geben Sie die erforderlichen Werte ein, um ein Zertifikat anzufordern, und klicken Sie auf Speichern.

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

Geben Sie die Details zum Erstellen eines Zertifikats ein.

4. Kehren Sie zum erstellten Keyring zurück, und kopieren Sie das generierte Zertifikat.

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 'Certificates', there are two options: 'Key Rings' (unchecked) and 'KeyRingTest' (checked). A red arrow points from the 'KeyRingTest' option to the main configuration area. The main area has two tabs: 'Basic' and 'Certificate Request'. The 'Certificate Request' tab is active, showing a 'Certificate Chain' section with a text area containing '-----BEGIN CERTIFICATE REQUEST-----'. Below this are input fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.


Das generierte Zertifikat kopieren

5. Wechseln Sie zur Zertifizierungsstelle, und fordern Sie ein Zertifikat an.

The screenshot shows the Microsoft Active Directory Certificate Services website. The header includes 'Microsoft Active Directory Certificate Services - mxslab-ADMXSV-CA' and a 'Home' link. The main content area has a 'Welcome' section with instructions on how to use the site to request a certificate, download a CA certificate, or view the status of a pending request. A 'Select a task:' section lists three options: 'Request a certificate' (with a red arrow pointing to it), 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

Zertifikat von CA anfordern

6. Fügen Sie das in UCS Central generierte Zertifikat ein, und wählen Sie in der Zertifizierungsstelle die Vorlage Webserver und Client aus. Klicken Sie auf Senden, um das Zertifikat zu generieren.

 **Hinweis:** Stellen Sie beim Generieren einer Zertifikatsanforderung in Cisco UCS Central sicher, dass das resultierende Zertifikat die Verwendung von SSL-Client- und SSL-Server-Authentifizierungsschlüsseln umfasst. Wenn Sie eine Microsoft Windows Enterprise-CA verwenden, verwenden Sie die Vorlage Computer oder eine andere geeignete Vorlage, die beide Schlüsselverwendungen enthält, falls die Vorlage Computer nicht verfügbar ist.

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 >

Zertifikat für den erstellten Schlüsselbund generieren

7. Konvertieren Sie das neue Zertifikat in PEM mit dem Befehl `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem`.

8. Kopieren Sie den Inhalt des PEM-Zertifikats, und gehen Sie zum erstellten Keyring, um den Inhalt einzufügen. Wählen Sie den erstellten vertrauenswürdigen Punkt, und speichern Sie die Konfiguration.

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

Fügen Sie das im Schlüsselbund angeforderte Zertifikat ein.

Anwenden des Keyrings

1. Navigieren Sie zu System Profile > Remote Access > Keyring, wählen Sie den erstellten

Keyring aus, und klicken Sie auf Save. UCS Central schließt die aktuelle Sitzung.

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

Erstellen des Keyrings auswählen

Validierung

1. Warten Sie, bis auf UCS Central zugegriffen werden kann, und klicken Sie auf das Schloss neben https://. Die Website ist sicher.

https:// /ui/faces/Login.xhtml

About

Connection is secure

Permissions for this site

Cookies (1 cookies in use)

UCS Central ist sicher

Fehlerbehebung

Überprüfen Sie, ob das generierte Zertifikat die Verwendung von SSL-Client- und Server-Authentifizierungsschlüsseln enthält.

Wenn das für CA angeforderte Zertifikat nicht den SSL-Client- und Server-Authentifizierungsschlüssel enthält, wird ein Fehler mit der Meldung "Invalid certificate. Dieses Zertifikat kann nicht für die TLS-Serverauthentifizierung verwendet werden. Check key usage extensions" wird angezeigt.

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

Fehler bei TLS-Serverautorisierungsschlüsseln

Mit dem Befehl `openssl x509 -in <my_cert>.pem -text -noout` können Sie überprüfen, ob das Zertifikat im PEM-Format, das mit der in der Zertifizierungsstelle ausgewählten Vorlage erstellt wurde, über den richtigen Schlüssel für die Serverauthentifizierung verfügt. Sie müssen Webserverauthentifizierung und Webclientauthentifizierung im Abschnitt zur erweiterten Schlüsselverwendung sehen.

```
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:

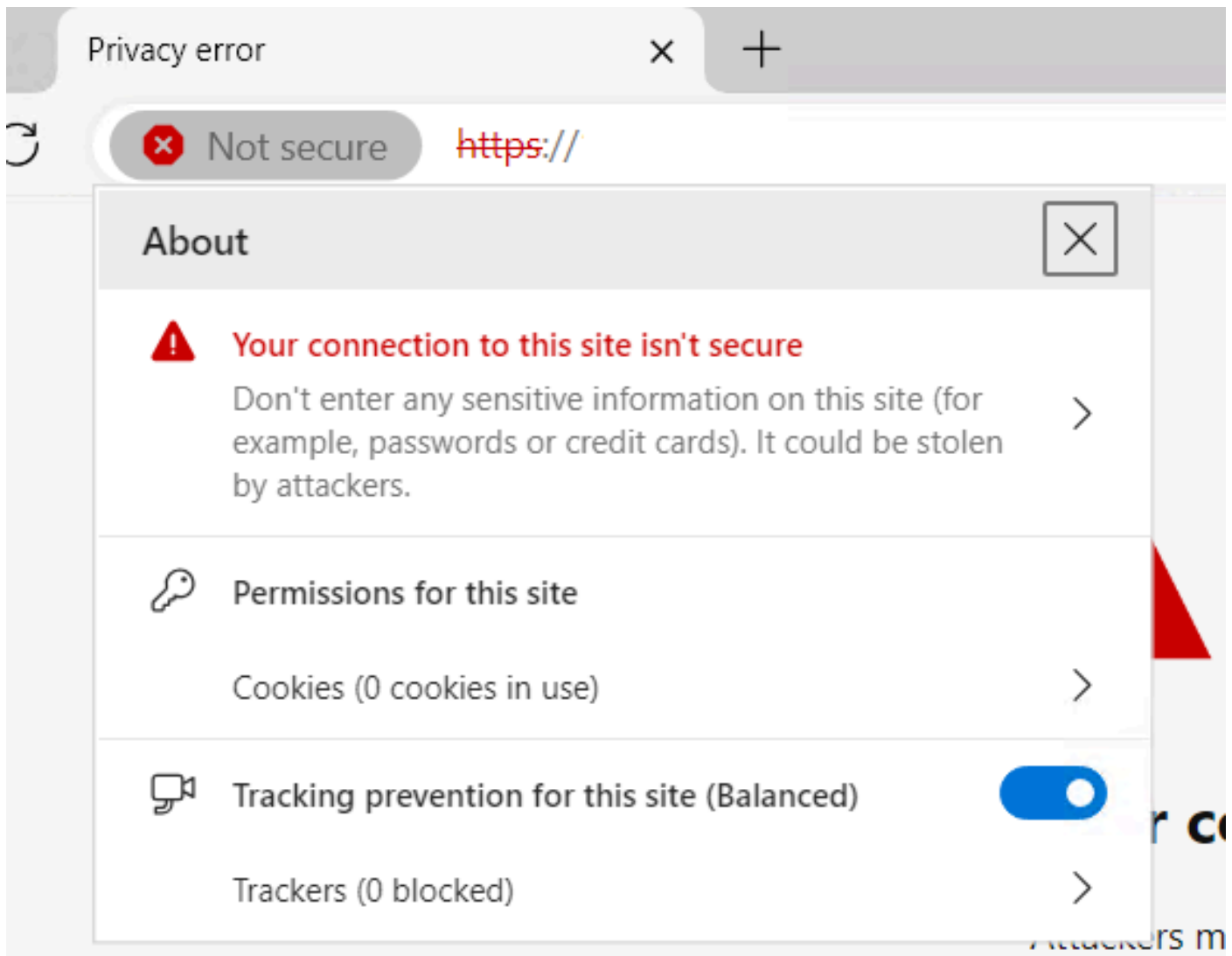
    X509v3 CRL Distribution Points:
        Full Name:

    Authority Information Access:
```

Webserver und Webclient-Autorisierungsschlüssel in Zertifikat angefordert

UCS Central wird immer noch als unsicherer Standort markiert.

Manchmal wird die Verbindung nach der Konfiguration des Drittanbieterzertifikats noch vom Browser markiert.



UCS Central ist noch immer ein unsicherer Standort

Um zu überprüfen, ob das Zertifikat ordnungsgemäß angewendet wird, stellen Sie sicher, dass das Gerät der Zertifizierungsstelle vertraut.

Zugehörige Informationen

- [Cisco UCS Central Administration Guide, Version 2.0](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.