

Configurer le certificat tiers pour UCS Central

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Créer le point de confiance](#)

[Création de Key Ring et CSR](#)

[Appliquer la sonnerie principale](#)

[Validation](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les meilleures pratiques pour configurer un certificat tiers dans le logiciel Cisco Unified Computing System Central (UCS Central).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Cisco UCS Central
- Autorité de certification (CA)
- OpenSSL

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- UCS Central 2.0(1q)
- Services de certificats Microsoft Active Directory
- Windows 11 Professionnel N
- OpenSSL 3.1.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Téléchargez la chaîne de certificats à partir de l'autorité de certification.

1. Téléchargez la chaîne de certificats à partir de l'autorité de certification (AC).

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](#) ←

Télécharger une chaîne de certificats à partir de CA

2. Définissez le codage sur Base 64 et téléchargez la chaîne de certificats CA.

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:

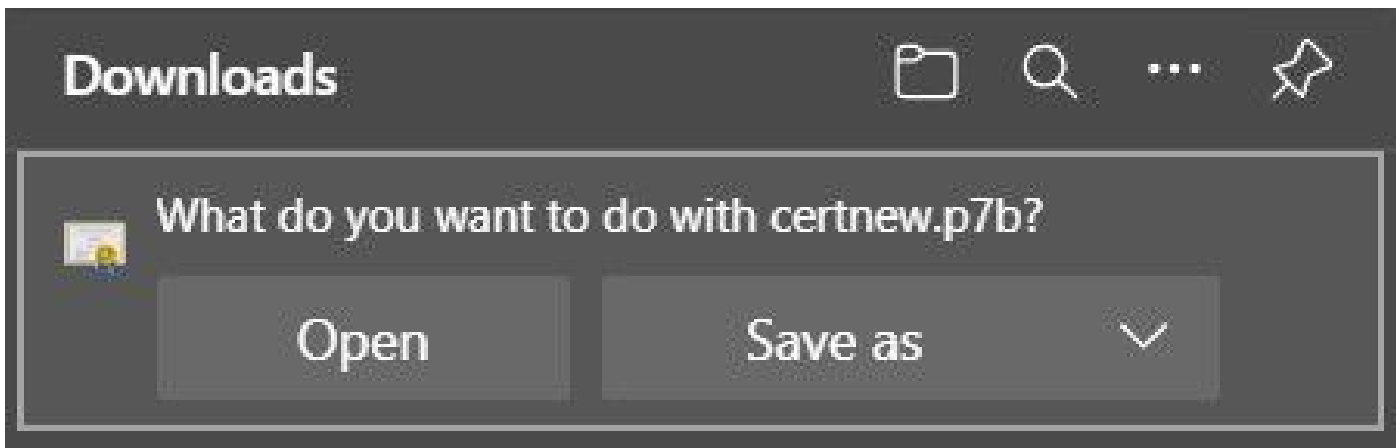
DER

Base 64

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

Définissez le codage sur Base 64 et téléchargez la chaîne de certificats CA

3. Notez que la chaîne de certificats de l'autorité de certification est au format PB7.



Le certificat est au format PB7

4. Le certificat doit être converti au format PEM avec l'outil OpenSSL. Pour vérifier si Open SSL est installé sous Windows, utilisez la commande 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)
```

Vérifier si OpenSSL est installé

 Remarque : l'installation d'OpenSSL sort du cadre de cet article.

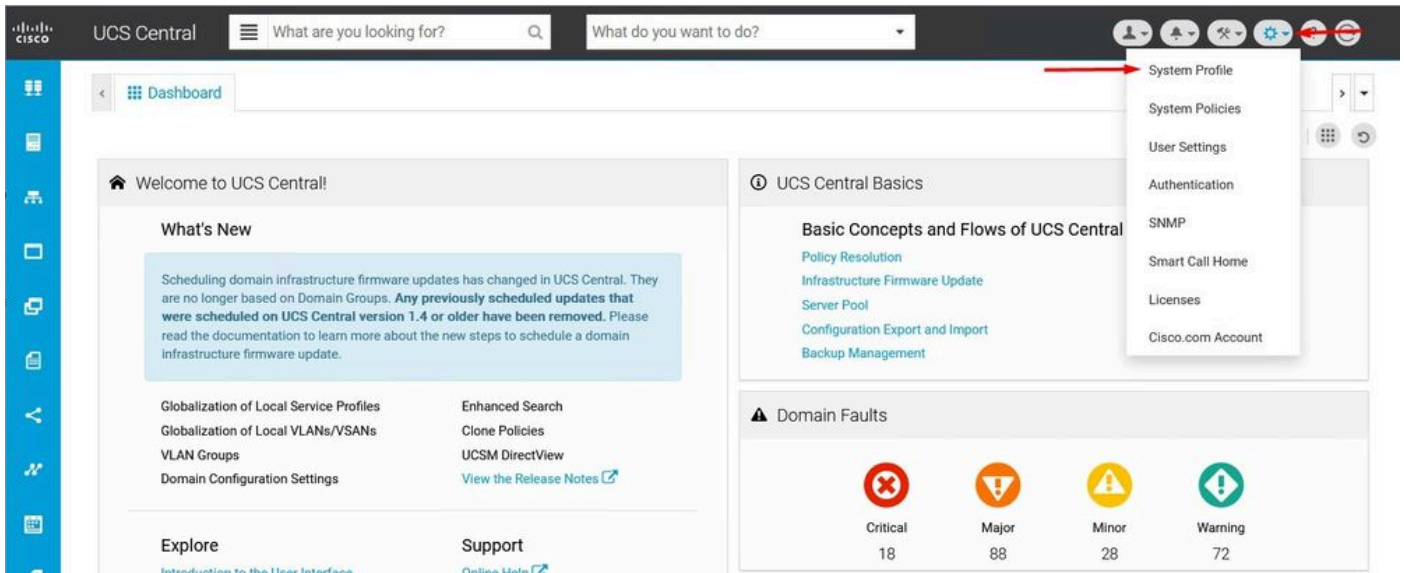
5. Si OpenSSL est installé, exécutez la commande `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` pour effectuer la conversion. Assurez-vous d'utiliser le chemin d'accès où le certificat est enregistré.

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

Convertir le certificat P7B au format PEM

Créer le point de confiance

1. Cliquez sur l'icône System Configuration > System Profile > Trusted Points.



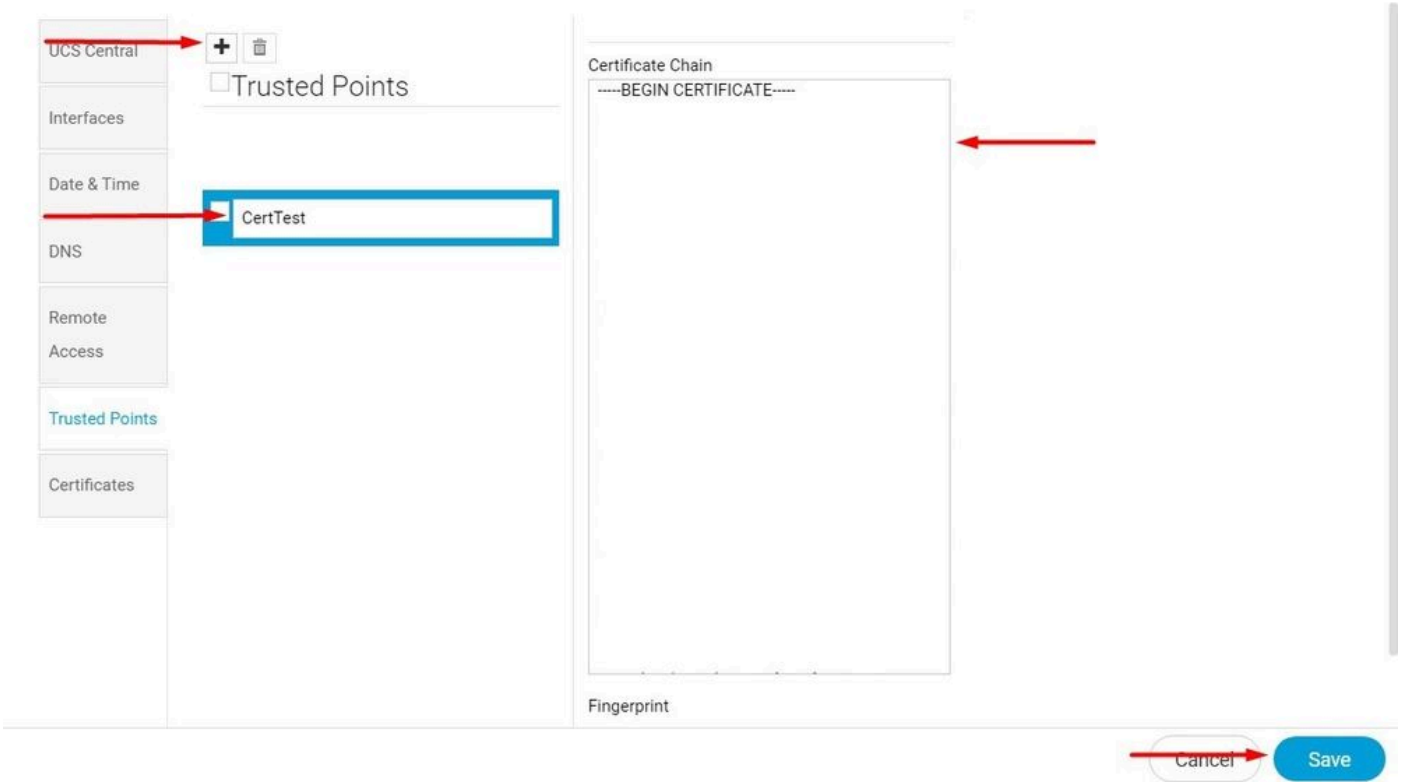
Profil



du système UCS Central
Points de confiance UCS Central

2. Cliquez sur l'icône + (plus) pour ajouter un nouveau point de confiance. Indiquez un nom et collez-le dans le contenu du certificat PEM. Cliquez sur Save pour appliquer les modifications.

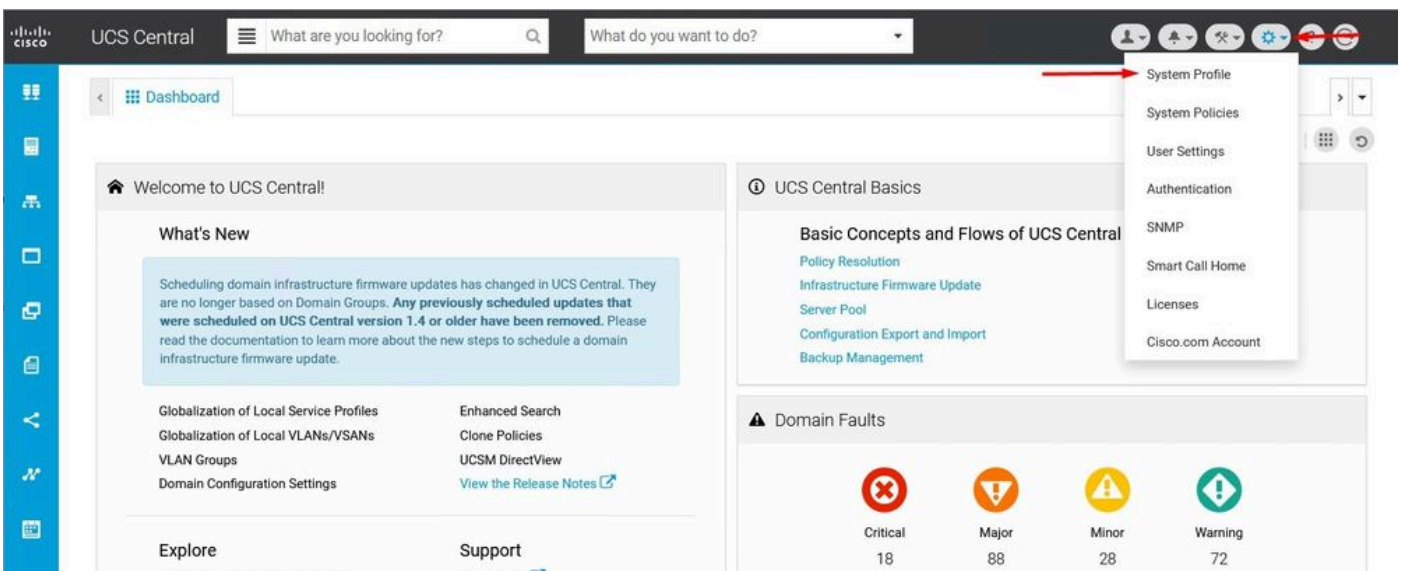
UCS Central System Profile Manage



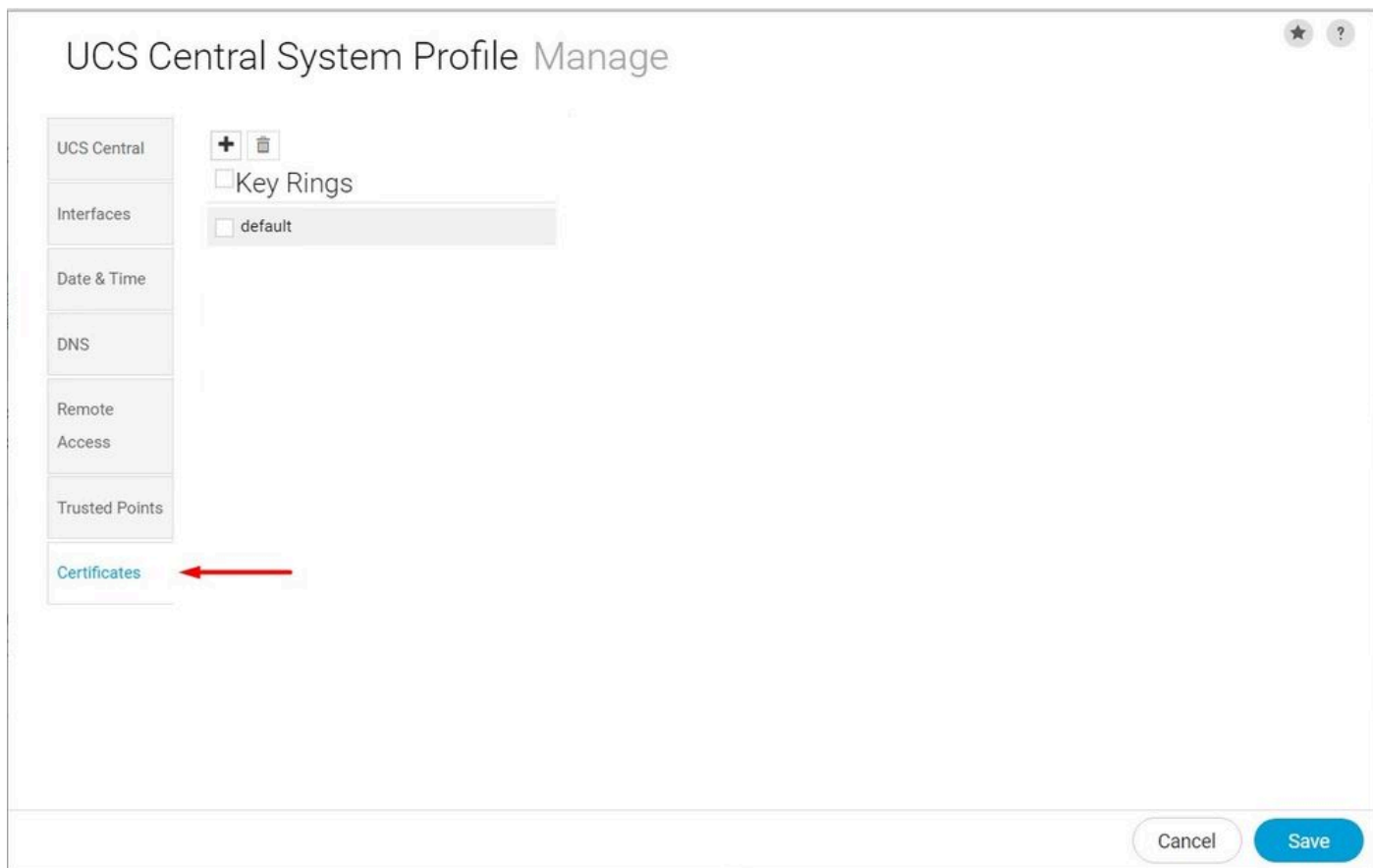
Copier la chaîne de certificats

Création de Key Ring et CSR

1. Cliquez sur l'icône Configuration du système > Profil du système > Certificats.



UCS Central System



ProfileCertificats UCS Central

2. Cliquez sur l'icône plus pour ajouter un nouveau Key Ring. Écrivez un nom, conservez le module avec la valeur par défaut (ou modifiez-le si nécessaire) et sélectionnez le point de confiance créé avant. Après avoir défini ces paramètres, passez à Demande de certificat.

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

Créer un anneau de clés

3. Entrez les valeurs nécessaires pour demander un certificat et cliquez sur Enregistrer.

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

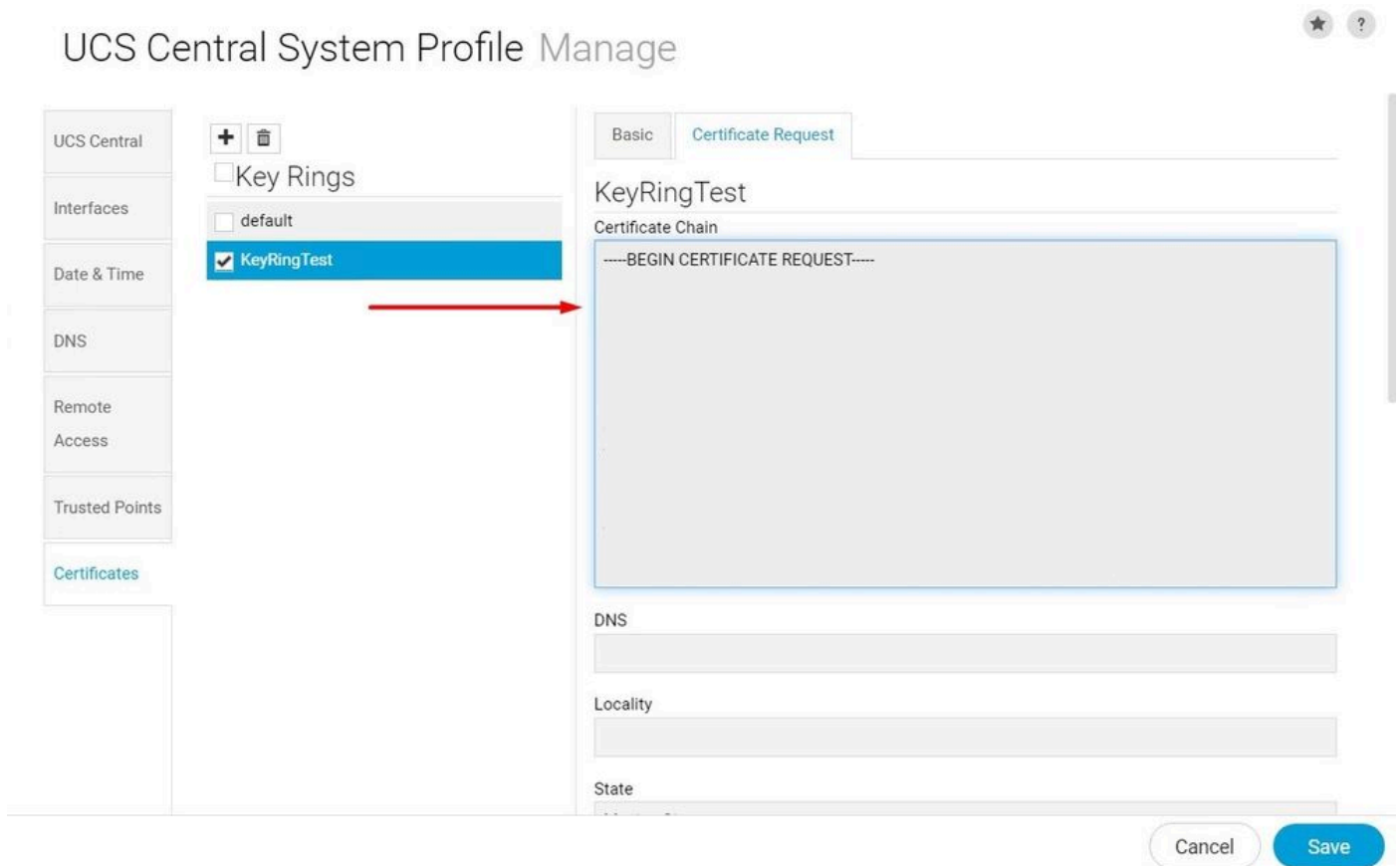
Email

Subject

Cancel Save

Entrez les détails pour générer un certificat

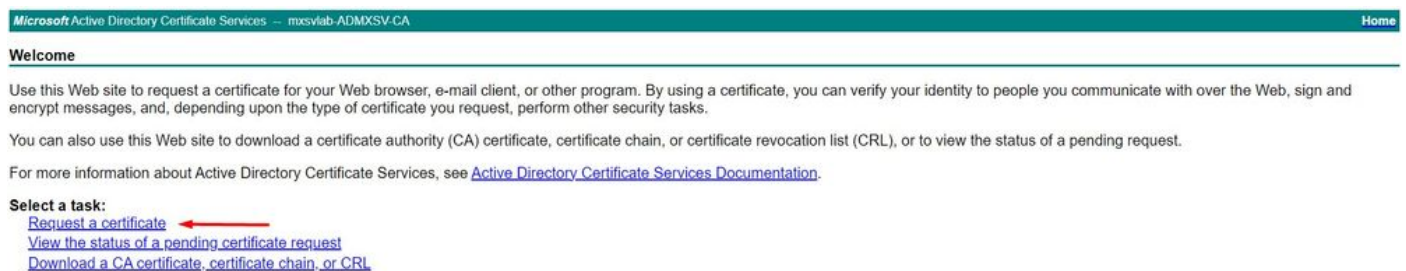
4. Retournez à la sonnerie de clé créée et copiez le certificat généré.



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 text area for the 'Certificate Chain' containing '-----BEGIN CERTIFICATE REQUEST-----'. Below this are input fields for 'DNS', 'Locality', and 'State'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Copier le certificat généré


5. Accédez à l'autorité de certification et demandez un certificat.



The screenshot shows the 'Microsoft Active Directory Certificate Services' website. The page has a green header with the text 'Microsoft Active Directory Certificate Services - mxslab-ADMXSV-CA' and a 'Home' link. Below the header is a 'Welcome' section with 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](#).' Below this is a 'Select a task:' section with three links: 'Request a certificate' (highlighted with a red arrow), 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

Demander un certificat à l'AC

6. Collez le certificat généré dans UCS Central et, dans l'autorité de certification, sélectionnez le modèle Serveur Web et Client. Cliquez sur Submit pour générer le certificat.

 **Remarque :** lors de la génération d'une demande de certificat dans Cisco UCS Central, assurez-vous que le certificat obtenu inclut les utilisations de clé d'authentification client et serveur SSL. Si vous utilisez une autorité de certification Microsoft Windows Enterprise, utilisez le modèle Ordinateur ou un autre modèle approprié qui inclut les deux utilisations des clés, si le modèle Ordinateur n'est pas disponible.

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 >

Générer un certificat à utiliser dans l'anneau de clés créé

7. Convertissez le nouveau certificat en PEM à l'aide de la commande `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem`.

8. Copiez le contenu du certificat PEM et accédez à la sonnerie de clé créée pour coller le contenu. Sélectionnez le point de confiance créé et enregistrez la configuration.

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

Collez le certificat demandé dans le porte-clés

Appliquer la sonnerie principale

1. Accédez à System Profile > Remote Access > Keyring, sélectionnez l'anneau Key créé, puis cliquez sur Save. UCS Central ferme la session en cours.

UCS Central System Profile Manage



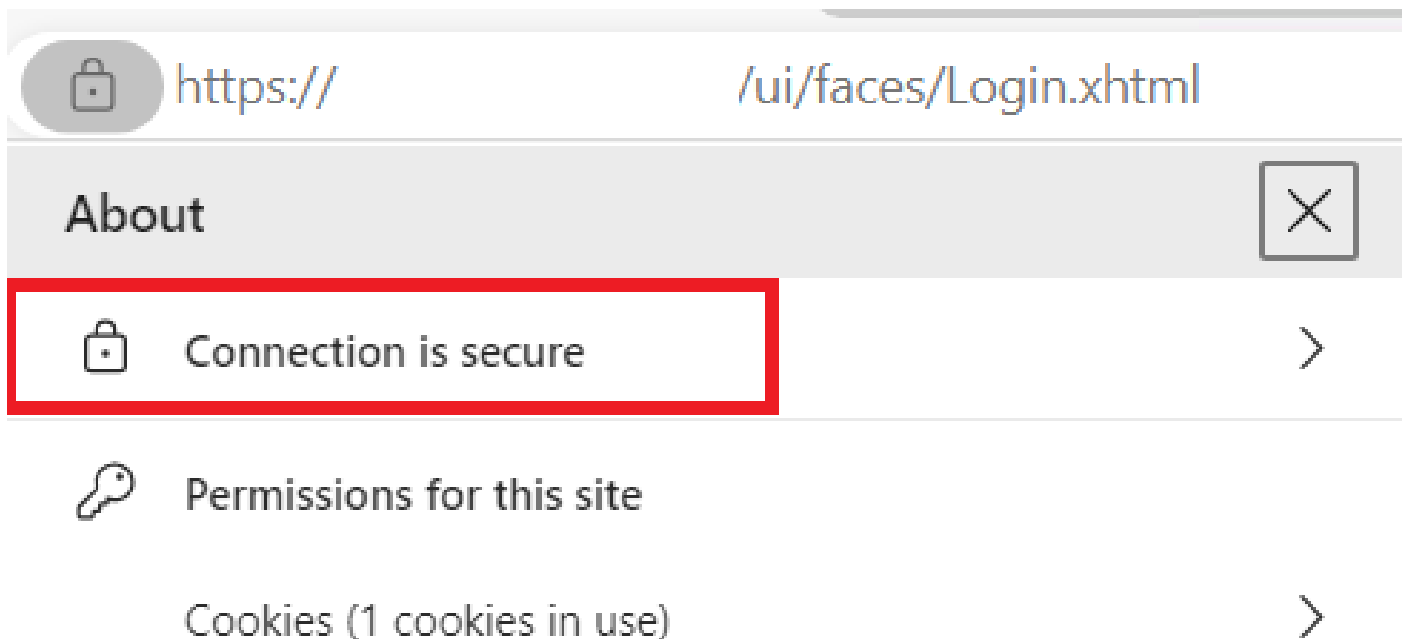
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

Cancel Save

Sélectionnez l'anneau clé créé

Validation

1. Attendez qu'UCS Central soit accessible et cliquez sur le verrou en regard de https://. Le site est sécurisé.



UCS Central est sécurisé

Dépannage

Vérifiez si le certificat généré inclut les utilisations de clé d'authentification du serveur et du client SSL.

Lorsque le certificat demandé à l'autorité de certification n'inclut pas la clé d'authentification du client et du serveur SSL, une erreur indiquant « Certificat non valide. Ce certificat ne peut pas être utilisé pour l'authentification du serveur TLS. Vérifiez les extensions d'utilisation de la clé.

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

Erreur sur les clés d'autorisation du serveur TLS

Pour vérifier si le certificat au format PEM créé à partir du modèle sélectionné dans l'autorité de certification a les utilisations de clé d'authentification du serveur correctes, vous pouvez utiliser la commande `openssl x509 -in <my_cert>.pem -text -noout`. Vous devez voir Authentification du serveur Web et Authentification du client Web sous la section Utilisation de clé étendue .

```
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:

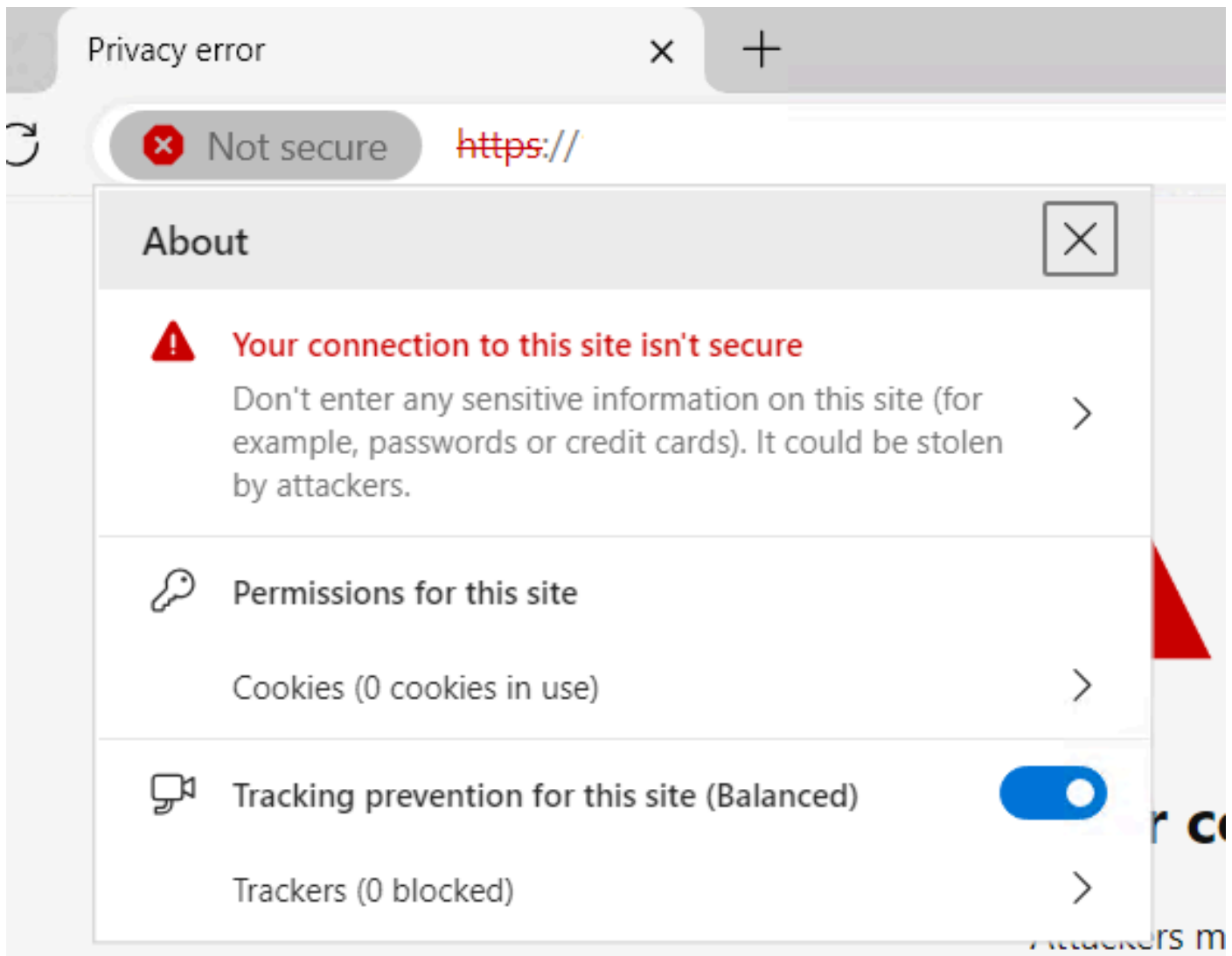
    X509v3 CRL Distribution Points:
    Full Name:

    Authority Information Access:
```

Clé d'autorisation du serveur Web et du client Web dans le certificat demandé

UCS Central est toujours marqué comme site non sécurisé.

Parfois, après la configuration du certificat tiers, la connexion est toujours marquée par le navigateur.



UCS Central est toujours un site non sécurisé

Pour vérifier si le certificat est appliqué correctement, assurez-vous que le périphérique fait confiance à l'autorité de certification.

Informations connexes

- [Guide d'administration centrale de Cisco UCS, version 2.0](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.