

为UCS中心配置第三方证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[创建信任点](#)

[创建密钥环和CSR](#)

[应用密钥环](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍在思科统一计算系统中心软件（UCS中心）中配置第三方证书的最佳实践。

先决条件

要求

建议掌握下列主题的相关知识：

- 思科UCS中心
- 证书颁发机构 (CA)
- OpenSSL

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCS Central 2.0(1q)
- Microsoft Active Directory证书服务
- Windows 11专业版N
- OpenSSL 3.1.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

从证书颁发机构下载证书链。

1. 从证书颁发机构(CA)下载证书链。

Active Directory Certificate Services Documentation.' Under the heading 'Select a task:', there are three links: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'. A red arrow points to the third link." data-bbox="57 124 942 256"/>

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](#)

从CA下载证书链

2. 将编码设置为Base 64并下载CA证书链。

install this CA certificate.' Below that, it says: 'To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.' Under the heading 'CA certificate:', there is a dropdown menu showing 'Current []'. Under the heading 'Encoding method:', there are two radio buttons: 'DER' (unselected) and 'Base 64' (selected). Below that, there are five links: 'Install CA certificate', 'Download CA certificate', 'Download CA certificate chain', 'Download latest base CRL', and 'Download latest delta CRL'. A red arrow points to the third link." data-bbox="57 342 942 682"/>

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:

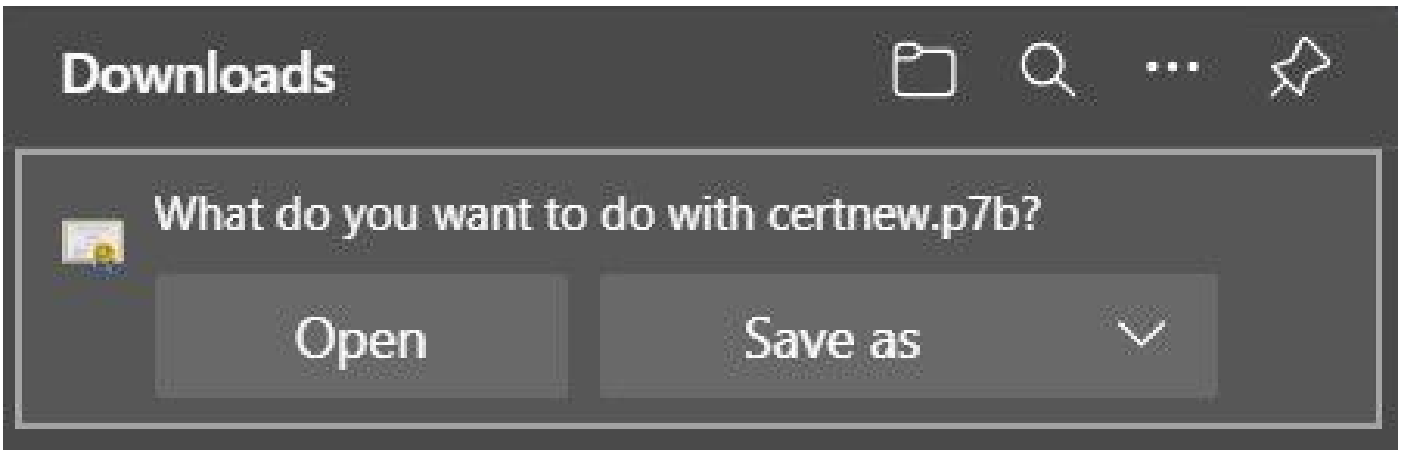
DER

Base 64

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

将编码设置为Base 64并下载CA证书链

3. 请注意，CA证书链为PB7格式。




证书采用PB7格式

4. 必须使用OpenSSL工具将证书转换为PEM格式。要检查Windows中是否安装了Open SSL，请使用命令`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)
```

检查是否已安装OpenSSL

 注意：OpenSSL安装不在本文讨论范围之内。

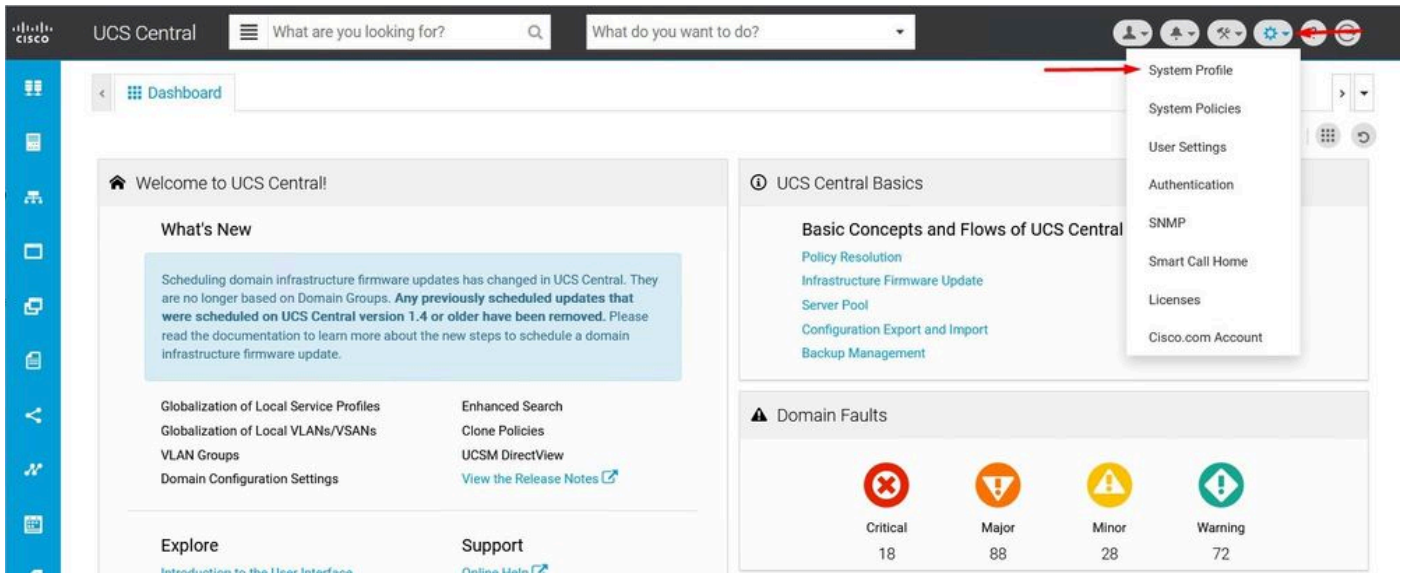
5. 如果安装了OpenSSL，请运行`openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` 命令以执行转换。确保使用保存证书时的路径。

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

将P7B证书转换为PEM格式

创建信任点

1. 单击System Configuration icon > System Profile > Trusted Points。



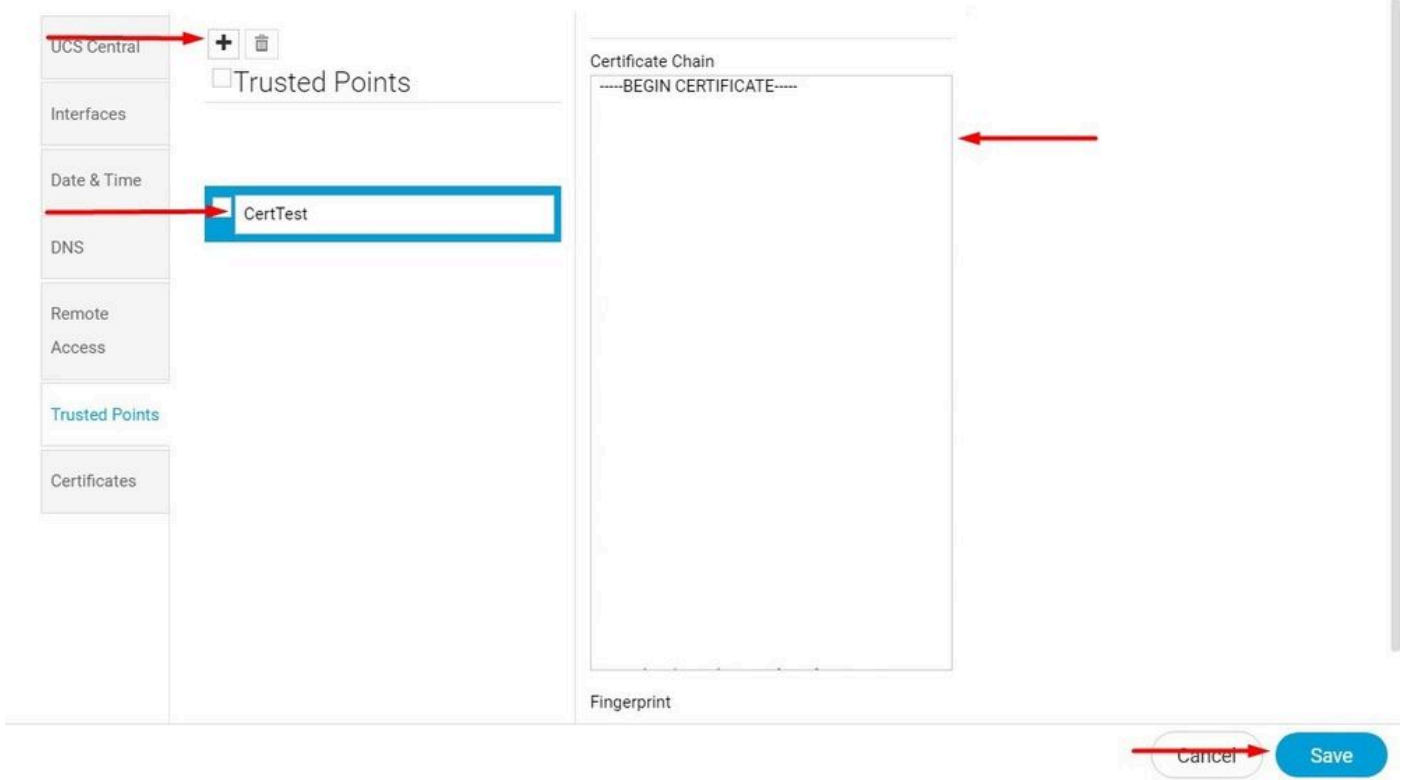
UCS中心系统



配置文件UCS中心受信任点

2. 单击+ (加号) 图标添加新的信任点。写下名称并粘贴到PEM证书的内容中。单击Save以应用更改。

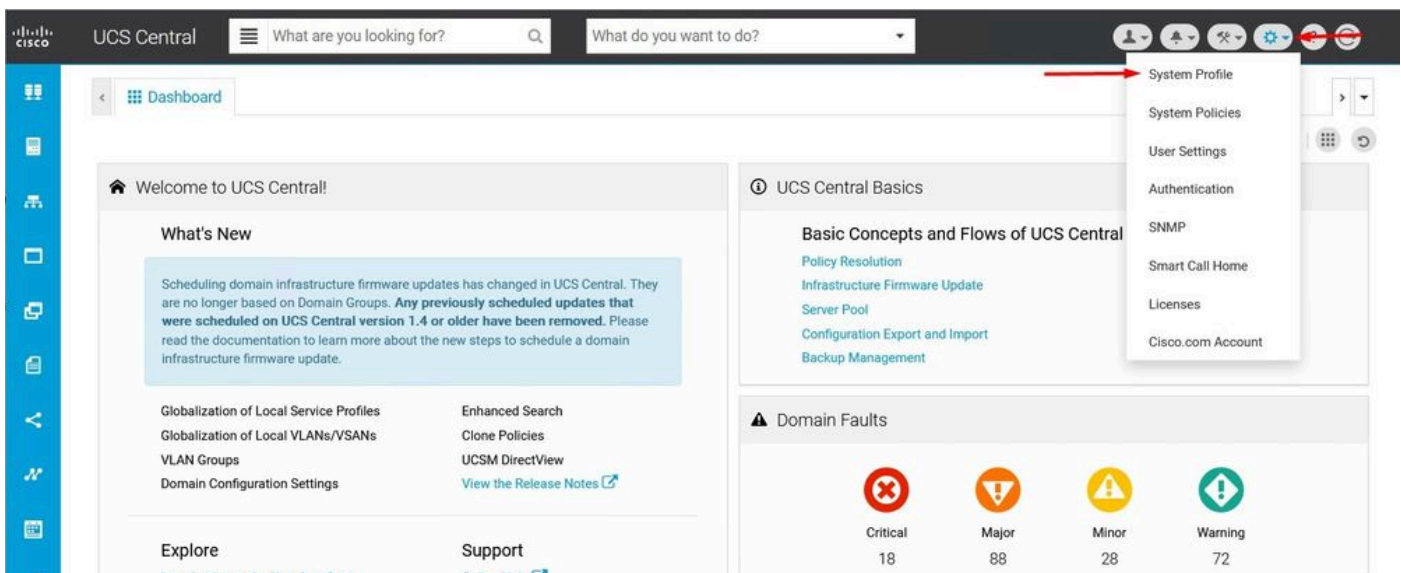
UCS Central System Profile Manage



复制证书链

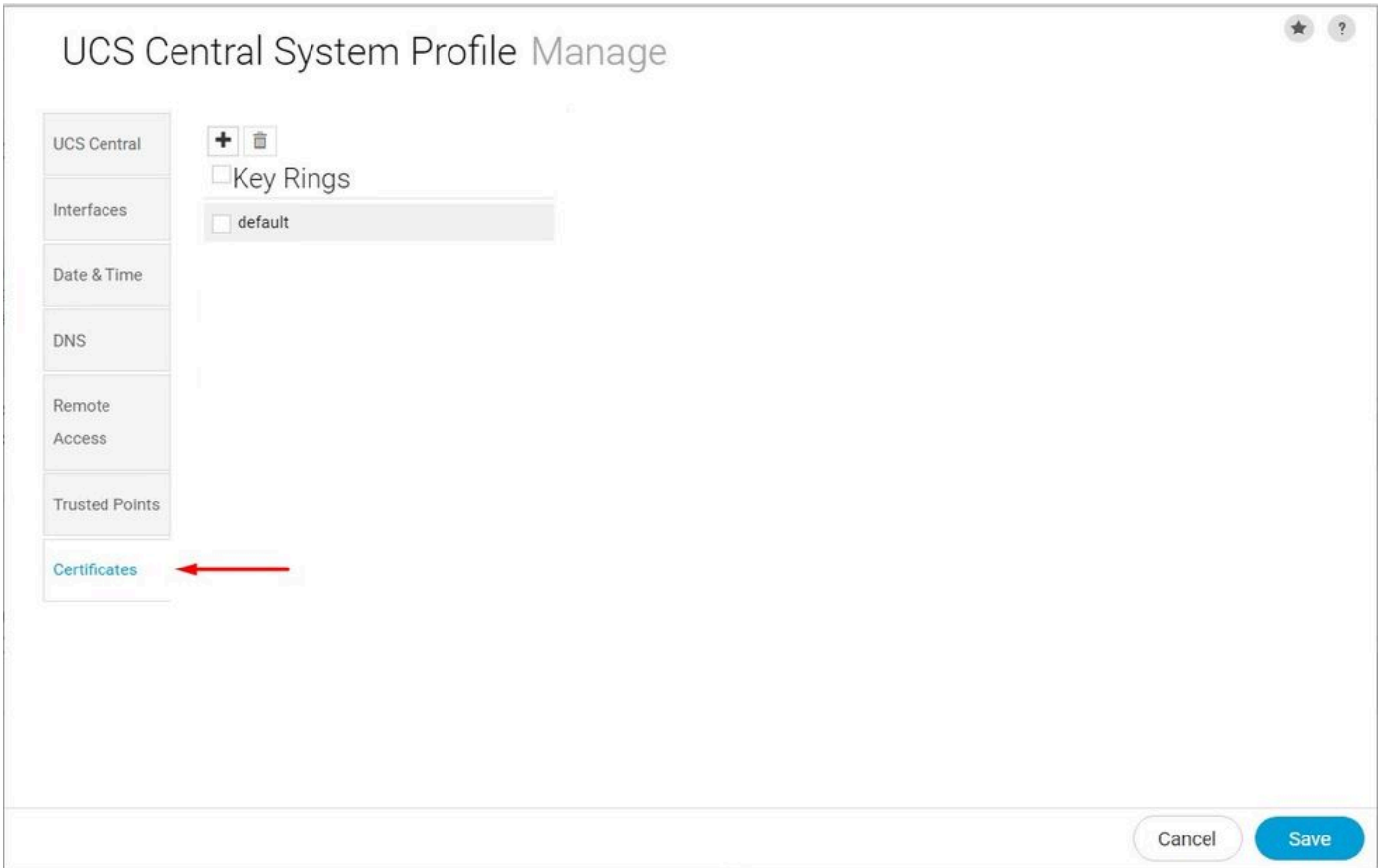
创建密钥环和CSR

1. 单击System Configuration icon > System Profile > Certificates。



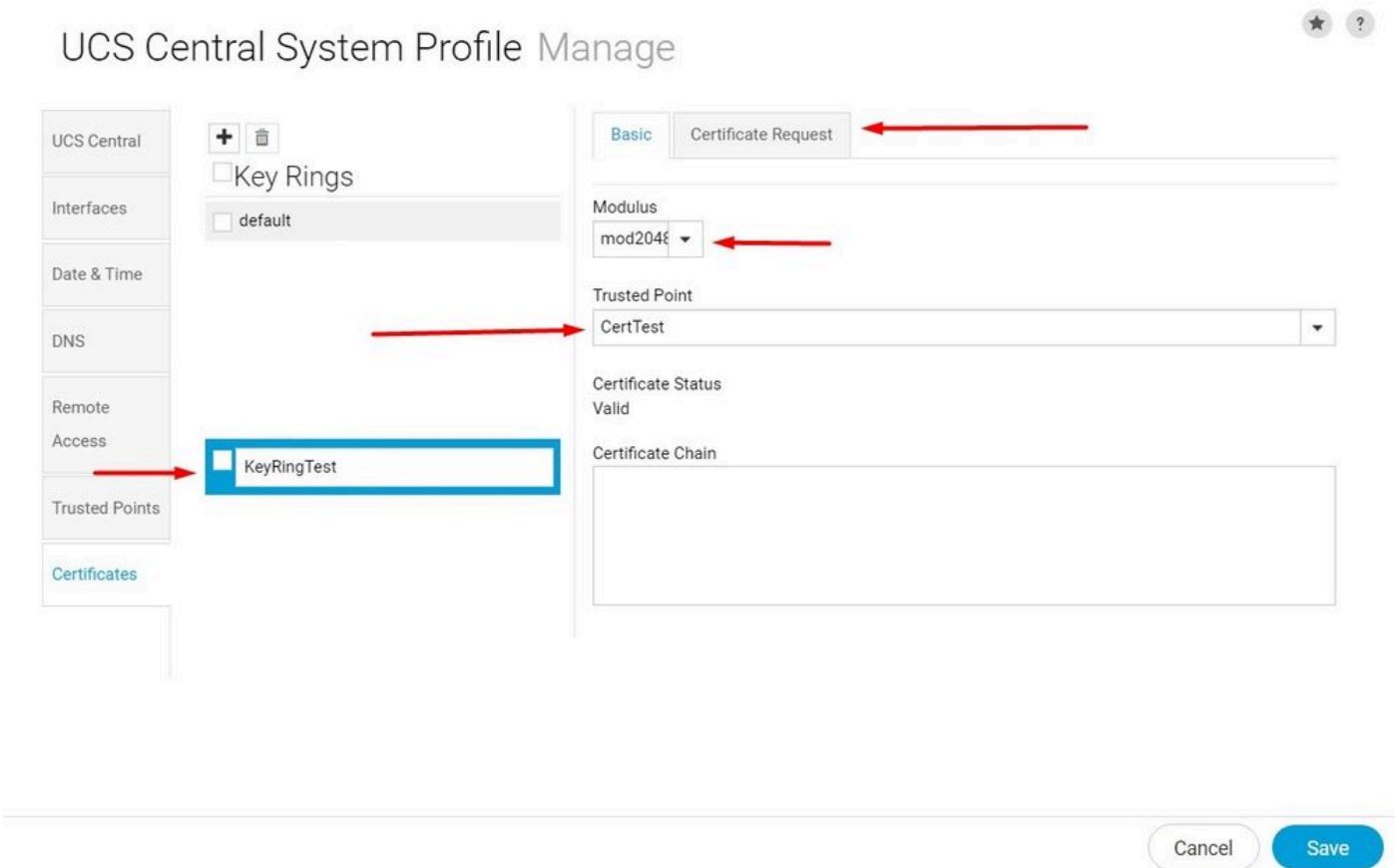
UCS中心系统

配



置文件UCS中心证书

2. 单击加号图标添加新密钥环。写下名称，将系数保留为默认值（或根据需要修改），并选择之前创建的信任点。设置这些参数后，移至证书请求。



创建新密钥环

3. 输入申请证书所需的值，然后单击保存。

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

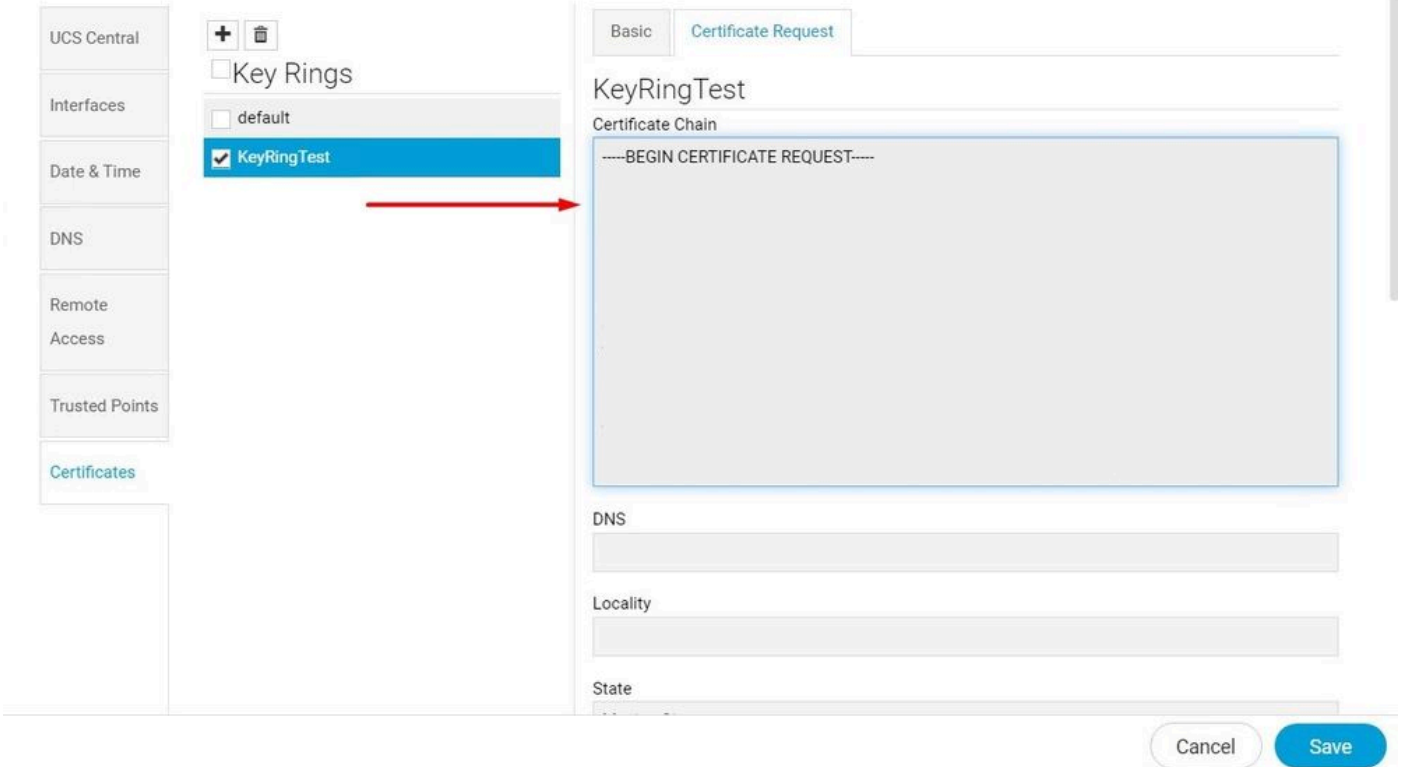
Email

Subject

Cancel Save

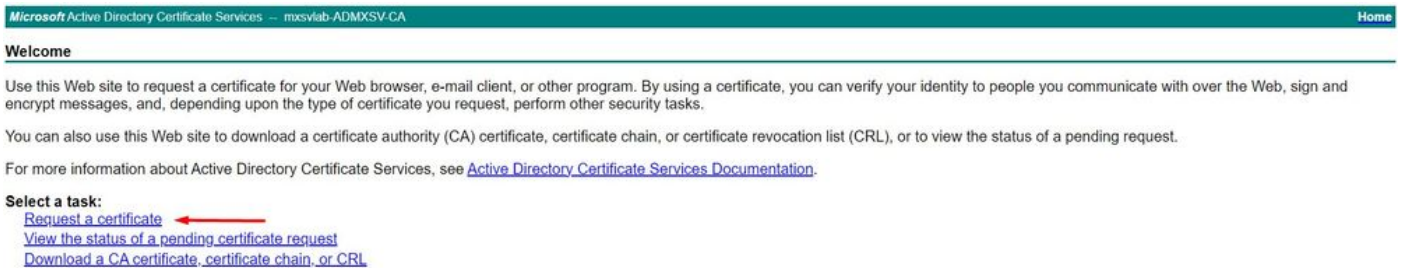
输入详细信息以生成证书

4. 返回到创建的密钥环，然后复制生成的证书。



复制生成的证书

5. 转到CA并请求证书。



Microsoft Active Directory Certificate Services – mxslab-ADMXSV-CA 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](#)

从CA请求证书

6. 将生成的证书粘贴到UCS中心并在CA中选择Web Server and Client模板。单击Submit以生成证书。

 **注意：**在思科UCS中心生成证书请求时，请确保生成的证书包含SSL客户端和服务端身份验证密钥用法。如果使用Microsoft Windows Enterprise CA，请利用“计算机”模板，或者在“计算机”模板不可用时利用同时包括密钥用法的另一个相应模板。

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 >

生成要在创建的密钥环中使用的证书

7. 使用命令 `openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem` 将新证书转换为 PEM。

8. 复制 PEM 证书的内容并转到创建的密钥环以粘贴内容。选择已创建的受信任点并保存配置。

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

粘贴密钥环中请求的证书

应用密钥环

1. 导航到系统配置文件>远程访问>密钥环，选择创建的密钥环，然后单击保存。UCS中心关闭当前会话。

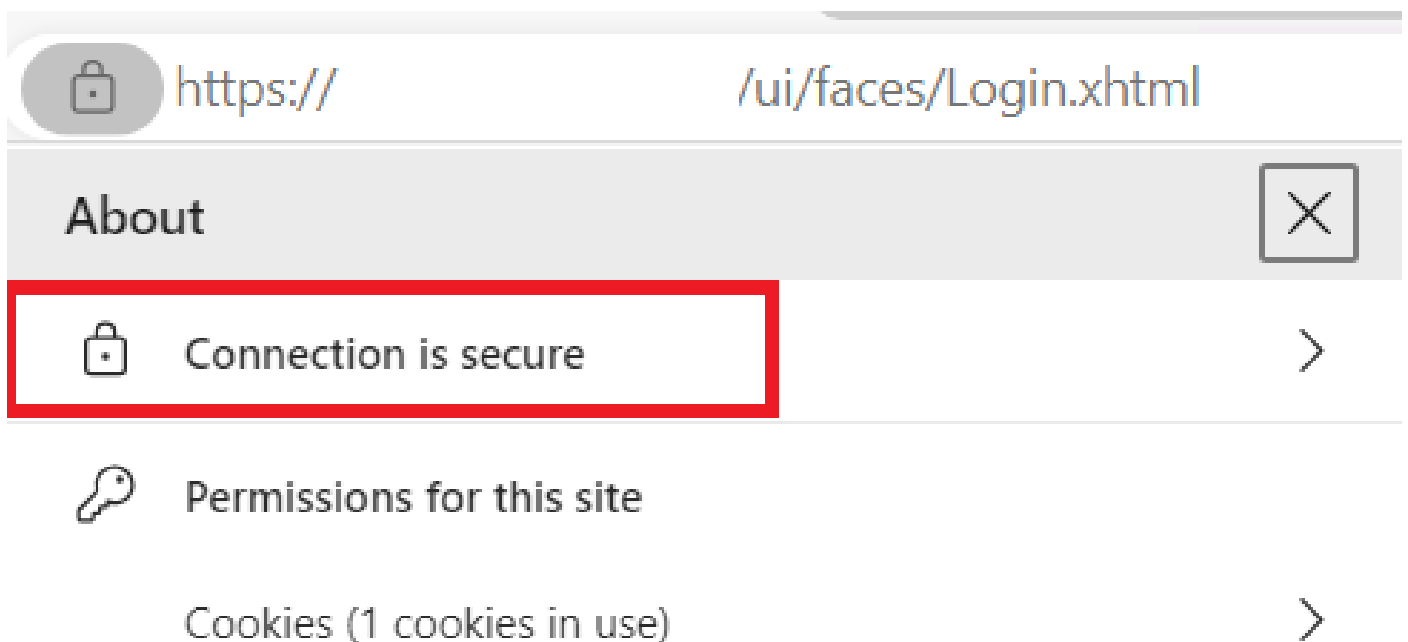
UCS Central	HTTPS Enabled
Interfaces	HTTPS Port 443
Date & Time	
DNS	Key Ring KeyRingTest
Remote Access	
Trusted Points	
Certificates	

选择创建的密钥环

验证

1. 等待可访问UCS中心并单击https://旁边的锁定。网站是安全的。



UCS中心是安全的

故障排除

检查生成的证书是否包括SSL客户端和服务端身份验证密钥用法。

当向CA请求的证书不包含SSL客户端和服务端身份验证密钥用法时，错误提示“证书无效”(Invalid certificate)。此证书无法用于TLS服务端身份验证，显示check key usage extensions”。

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

TLS服务端授权密钥错误

要验证从CA中选择的模板创建的PEM格式的证书是否具有正确的服务端身份验证密钥用法，您可以使用命令openssl x509 -in <my_cert>.pem -text -noout。您必须在Extended Key Usage 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:

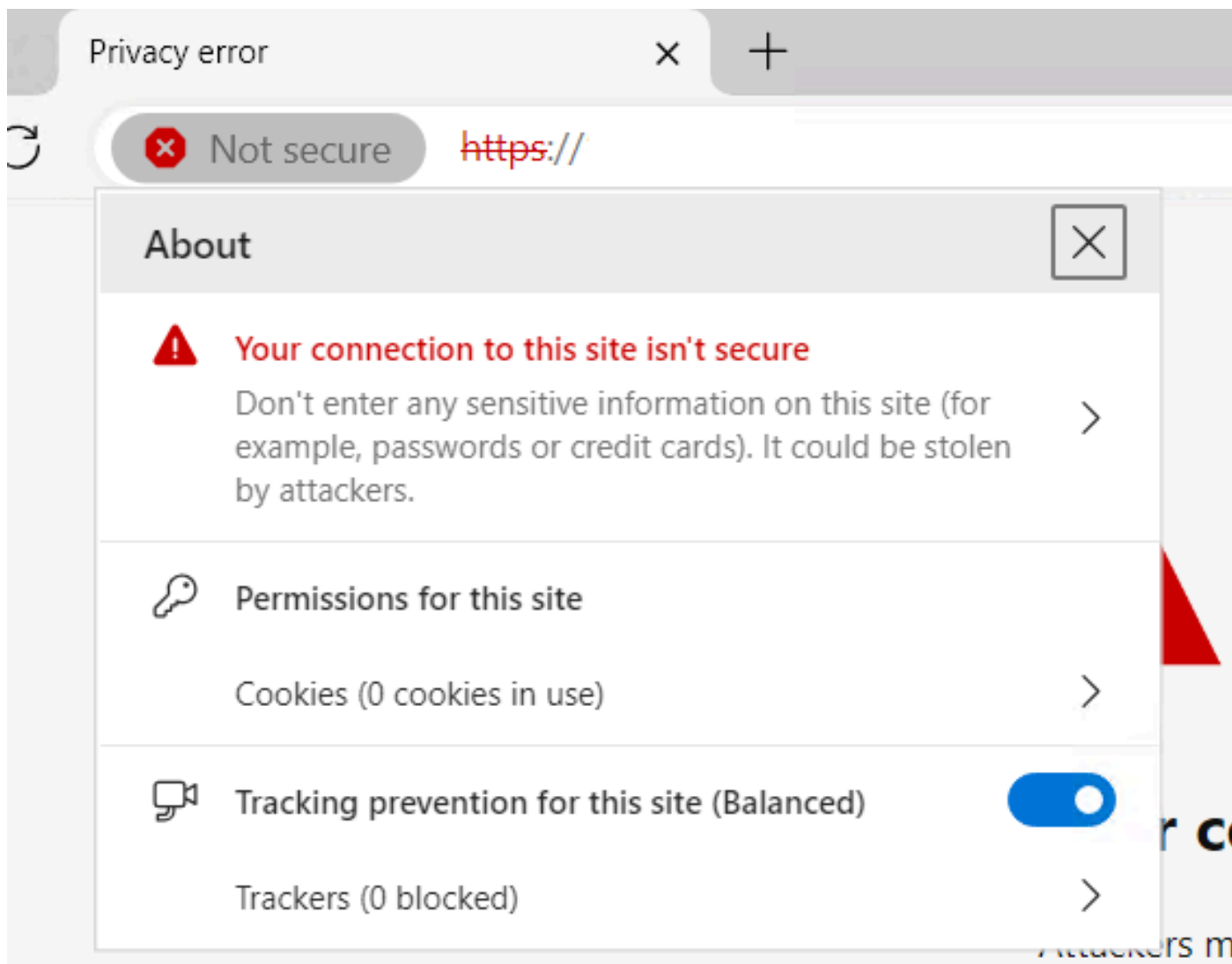
    X509v3 CRL Distribution Points:
    Full Name:

    Authority Information Access:
```

请求的证书中的Web服务器和Web客户端授权密钥

UCS中心仍标记为不安全站点。

有时，在配置第三方证书后，浏览器仍会标记连接。



UCS中心仍是一个不安全的站点

要验证证书是否正确应用，请确保设备信任证书颁发机构。

相关信息

- [Cisco UCS中心管理指南2.0版](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。