

# 配置 ISE 2.0 证书调配门户

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[限制](#)

[配置](#)

[验证](#)

[生成单个证书，无证书签名请求](#)

[使用证书签名请求生成单个证书](#)

[生成批量证书](#)

[故障排除](#)

## 简介

本文档介绍身份服务引擎 (ISE) 证书调配门户的配置和功能。

## 先决条件

### 要求

Cisco 建议您具有以下主题的基础知识：

- ISE
- 证书和证书颁发机构(CA)服务器。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎2.0
- Windows 7 PC

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。

## 背景信息

证书调配门户是ISE 2.0中引入的一项新功能，终端设备可以使用此功能从服务器注册和下载身份证书。它向无法通过自注册流程的设备颁发证书。

例如，销售点终端等设备无法通过自带设备(BYOD)流程，需要手动颁发证书。

证书调配门户允许特权用户组上传此类设备的证书请求(CSR);生成密钥对，然后下载证书。

在ISE上，您可以创建修改的证书模板，最终用户可以选择合适的证书模板下载证书。对于这些证书，ISE充当证书颁发机构(CA)服务器，我们可以获得由ISE内部CA签名的证书。

ISE 2.0证书调配门户支持以下格式的证书下载：

- PKCS12格式(包括证书链；证书链和密钥均为一个文件)
- PKCS12格式 (证书和密钥的一个文件)
- 隐私增强型电子邮件(PEM)格式的证书 (包括链)，PKCS8 PEM格式的密钥。
- PEM格式的证书，PKCS8 PEM格式的密钥：

## 限制

目前，ISE仅支持CSR中的这些扩展来签署证书。

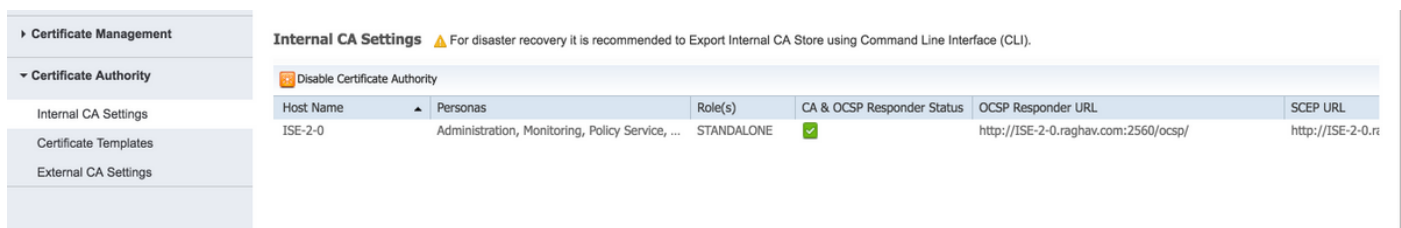
- subjectDirectoryAttributes
- subjectAlternativeName
- keyUsage
- subjectKeyIdentifier
- auditIdentity
- extendedKeyUsage
- CERT\_TEMPLATE\_OID (这是自定义的OID，用于指定通常在BYOD流中使用的模板)

**注意：**ISE内部CA旨在支持使用BYOD等证书的功能，因此功能有限。思科不建议将ISE用作企业CA。

## 配置

要在网络中使用证书调配功能，必须启用ISE内部CA服务，并配置证书调配门户。

第1步：在ISE GUI上，导航至**Administration > System > Certificates > Certificate Authority > Internal CA**，并要在ISE节点上启用内部CA设置，请点击**Enable Certificate Authority**。



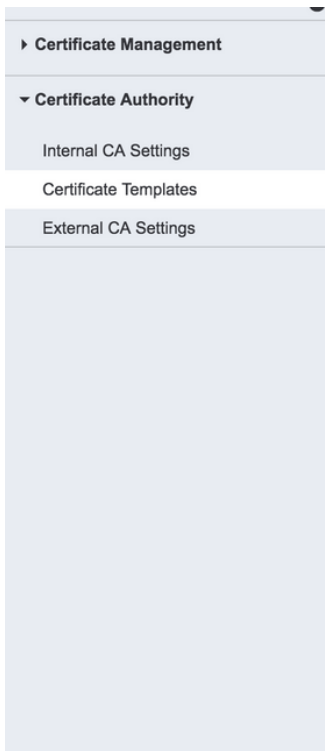
Internal CA Settings ▲ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

Disable Certificate Authority

Host Name	Personas	Role(s)	CA & OCSP Responder Status	OCSP Responder URL	SCEP URL
ISE-2-0	Administration, Monitoring, Policy Service, ...	STANDALONE	<input checked="" type="checkbox"/>	http://ISE-2-0.raghav.com:2560/ocsp/	http://ISE-2-0.r...

步骤2.在Administration > System > Certificates > Certificate Templates > Add下**创建证书模板**。

根据要求输入详细信息，然后点击**提交**，如下图所示。



### Add Certificate Template

\* Name

Description

**Subject**

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

---

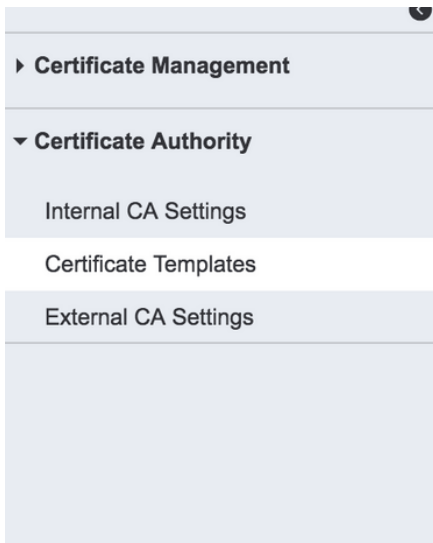
Subject Alternative Name (SAN)

Key Size

\* SCEP RA Profile

Valid Period  Day(s) (Valid Range 1 - 730)

**注意：**您可以在Administration > System > Certificates > Certificate Templates下看到已创建的证书模板的列表，如下图所示。



### Certificate Templates

Edit Add Duplicate Delete

<input type="checkbox"/>	Template Name	Description	Key Size
<input type="checkbox"/>	CA_SERVICE_Certificate...	This template will be us...	2048
<input type="checkbox"/>	EAP_Authentication_Cer...	This template will be us...	2048
<input type="checkbox"/>	internalCA		2048
<input type="checkbox"/>	testcert	test certificate template	2048

步骤3.要配置ISE证书调配门户，请导航至Administration > Device Portal Management > Certificate Provisioning > Create，如图所示：

### Certificate Provisioning Portals

You can edit and customize the default Certificate Provisioning portal and create additional ones

Create Edit Duplicate Delete

**Cert Portal**

**Certificate Provisioning Portal (default)**  
Default portal used by employees to request for a certificate manually

步骤4. 在新证书门户上，展开门户设置，如图所示。

#### Portals Settings and Customization

Save Close

Portal Name: \* Description: Portal test URL Language File

Cert Portal

**Portal Behavior and Flow Settings**  
Use these settings to specify the guest experience for this portal.

**Portal Page Customization**  
Use these settings to specify the guest experience for this portal.

Portal & Page Settings Certificate Provisioning Flow (based on settings)

- Portal Settings
- Login Page Settings
- Acceptable Use Policy (AUP) Page Settings
- Post-Login Banner Page Settings
- Change Password Settings
- Certificate Provisioning Portal Settings

```
graph TD; LOGIN[LOGIN] --> AUP[AUP]; AUP --> PostLogin[Post Login Banner]; PostLogin --> Empty[ ]
```

▼ Portal Settings

HTTPS port:\*  (8000 - 8999)

Allowed Interfaces:\*  Gigabit Ethernet 0  
 Gigabit Ethernet 1  
 Gigabit Ethernet 2  
 Gigabit Ethernet 3  
 Gigabit Ethernet 4  
 Gigabit Ethernet 5

Certificate group tag: \*    
Configure certificates at:  
**Administration > System > Certificates > System Certificates**

Authentication method: \*    
Configure authentication methods at:  
**Administration > Identity Management > Identity Source Sequences**

**Configure authorized groups**  
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
<input type="text"/> ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee

Fully qualified domain name (FQDN):

Idle timeout:  1-30 (minutes)

HTTPS端口  
 允许的接口  
 证书组标记  
 认证方法  
 授权组  
 完全限定域名(FQDN)  
 空闲超时

HTTPS证书调配门户应使用的端口。  
 ISE应侦听此门户的接口。  
 用于证书调配门户的证书标记，指示用于此门户的系统证书。  
 选择验证登录此门户的身份库序列。默认情况下，**证书请求**序列正在使用。  
 可通过将一组特定AD组和内部用户组移动到所选表来控制可访问证书调配门户的**用**  
 您还可以为此门户指定特定FQDN。使用http/https浏览到FQDN的用户将重定向到此  
 该值定义门户的空闲超时。

**注意：**可以在Administration > Identity Management > Identity Source Sequence下检查身份的**配置**。

步骤5.配置登录页设置。

▼ Login Page Settings

Maximum failed login attempts before rate limiting:  (1 - 999)

Time between login attempts when rate limiting:  (1 - 999)

Include an AUP

Require acceptance

Require scrolling to end of AUP

步骤6.配置AUP页面设置。

▼ Acceptable Use Policy (AUP) Page Settings

Include an AUP page

Require scrolling to end of AUP

On first login only

On every login

Every  days (starting at first login)

步骤7.您还可以添加登录后横幅。

步骤8.在Certificate Provisioning门户设置下，指定允许的证书模板。

▼ Change Password Settings

Allow internal users to change their own passwords

▼ Certificate Provisioning Portal Settings

Certificate Templates: \*

步骤9.滚动到页面顶部并单击“保存”以保存更改。

此外，可通过导航至门户页面自定义选项卡进一步自定义门户，在该选项卡中，AUP文本、登录后横幅文本和其他消息可根据要求进行更改。

## 验证

使用本部分可确认配置能否正常运行。

如果ISE已正确配置用于证书调配，则可通过以下步骤从ISE证书调配门户请求/下载证书。

步骤1.打开浏览器，浏览到如上所述配置的证书调配门户FQDN或证书调配测试URL。您被重定向到门户，如下图所示：

**CISCO** Certificate Provisioning Portal

**Sign On**  
Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username:

Password:

[Please read the terms and conditions.](#)

I agree to the terms and conditions

[Help](#)

步骤2.使用用户名和密码登录。

步骤3.身份验证成功后，接受AUP并进入证书调配页面。

步骤4.证书调配页面提供以下三种方式下载证书的功能：

- 单个证书 ( 无证书签名请求 )
- 单个证书 ( 带证书签名请求 )
- 批量证书

## 生成单个证书，无证书签名请求

- 要生成不带CSR的单个证书，请选择“生成单个证书 ( 不带证书签名请求 )”选项。
- 输入公用名(CN)。

**注意：**给定CN必须与请求者的用户名匹配。请求者是指用于登录门户的用户名。只有管理员用户可以为其他CN创建证书。

- 输入要为其生成证书的设备的MAC地址。
- 选择适当的证书模板。
- 选择应下载证书的所需格式。
- 输入证书密码并单击**G生成**。
- 成功生成并下载单个证书。

## Certificate Provisioning

I want to: \*

Generate a single certificate (without a certificat..

Common Name (CN): \*

test1

MAC Address: \*

11:35:65:AF:EC:12

Choose Certificate Template: \*

EAP\_Authentication\_Certificate\_Template

Description:

test certificate

Certificate Download Format: \*

PKCS12 format, including certificate chain (O... i

Certificate Password: \*

\*\*\*\*\*

Confirm Password: \*

\*\*\*\*\*|

Generate

Reset

## 使用证书签名请求生成单个证书

- 要生成不带CSR的单个证书，请选择“生成单个证书（带证书签名请求）”选项。
- 从记事本文件的“证书签名请求详细信息”下复制并粘贴CSR内容。
- 输入要为其生成证书的设备的MAC地址。
- 选择适当的证书模板。
- 选择应下载证书的所需格式。
- 输入证书密码并单击**Generate**。
- 将成功生成并下载单个证书。



## Certificate Provisioning

I want to: \*

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: \*

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuQCCAAIACAQAwEDEMwGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUgySpKa465ecULygnjHG
NC7bPqz4+5
8vK723r23ghympvBNPw31K6qzUCmDYLOcTwp+ymbWY3rfYxQ
nde8NofbTL
CrIhcnbmn0+SD7UozaXYb1DmugD8YL9Ht0Vv//WBKie6B8jZKl
WwqjAKVJ
yqJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABjslSToasXW
kyEIQT,8K5
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P50K
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0wTEMMmwn7Wbn5AgMBAAAGz
TBjBkqkG9wOB
CQ4xVBUAmAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYXKY
BwkwEwYDYR0BAwwCgYIKwYBBQUHAWAwEwEQYJYIZIAWY4QqEB
BAQDAgZAMA0GC9qG
Sib3DQEBQwUAA4IBAQCeZSHBMu71Pv?H9dQHTxY5v5WCyQ7
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLPXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/Wdu3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
lDypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ8K3HAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLPXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/Wdu3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
lDypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ8K3HAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

MAC Address:

Choose Certificate Template: \*

EAP\_Authentication\_Certificate\_Template

Description:

Certificate Download Format: \*

PKCS12 format, including certificate chain (O...

Certificate Password: \*

Confirm Password: \*

如果上传包含CN和MAC地址字段的CSV文件，则可以为多个MAC地址生成批量证书。

**注意：**给定CN必须与请求者的用户名匹配。请求者是指用于登录门户的用户名。只有管理员用户可以为其他CN创建证书。

- 要生成不带CSR的单个证书，请选择“生成单个证书（带证书签名请求）”选项。
- 上传csv文件以进行批量请求。
- 选择适当的证书模板。
- 选择应下载证书的所需格式。
- 输入证书密码并单击**Generate**。
- 生成并下载批量证书压缩文件。

The screenshot displays the 'Certificate Provisioning' interface. At the top left is the Cisco logo and the text 'Certificate Provisioning Portal'. The main form area is titled 'Certificate Provisioning' and contains the following fields and controls:

- I want to: \***: A dropdown menu with 'Generate bulk certificates' selected.
- Upload CSV File: \***: A file upload field containing 'maclist.csv' and a 'Choose File' button.
- If you don't have the CSV template, [download here](#)**: A link to download the CSV template.
- Choose Certificate Template: \***: A dropdown menu with 'EAP\_Authentication\_Certificate\_Template' selected.
- Description:**: A text input field containing 'test bulk certificate'.
- Certificate Download Format: \***: A dropdown menu with 'PKCS12 format, including certificate chain (O...)' selected, accompanied by an information icon.
- Certificate Password: \***: A password input field with masked characters '.....'.
- Confirm Password: \***: A confirm password input field with masked characters '.....|'.
- Generate**: A blue button to proceed with certificate generation.
- Reset**: A grey button to clear the form.

At the bottom center of the form area is a [Help](#) link.

## 故障排除

目前没有针对此配置的故障排除信息。