

配置ISE 2.0證書調配門戶

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制](#)

[設定](#)

[驗證](#)

[生成沒有證書簽名請求的單個證書](#)

[使用證書簽名請求生成單個證書](#)

[生成批次證書](#)

[疑難排解](#)

簡介

本文檔介紹身份服務引擎(ISE)證書調配門戶的配置和功能。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- ISE
- 憑證和憑證授權單位(CA)伺服器。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎2.0
- Windows 7電腦

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。

背景資訊

證書調配門戶是ISE 2.0中引入的一項新功能，終端裝置可以使用它從伺服器註冊和下載身份證書。它會向無法通過自註冊流程的裝置頒發證書。

例如，銷售點終端等裝置無法通過「自帶裝置」(BYOD)流程，需要手動頒發證書。

憑證布建入口網站允許一組特殊使用者上傳此類裝置的憑證請求(CSR);生成金鑰對，然後下載證書。

在ISE上，您可以建立修改的證書模板，終端使用者可以選擇合適的證書模板來下載證書。對於這些證書，ISE充當證書頒發機構(CA)伺服器，我們可以獲得ISE內部CA簽名的證書。

ISE 2.0證書調配門戶支援以下格式的證書下載：

- PKCS12格式(包括憑證鏈結；一個檔案同時用於證書鏈和金鑰)
- PKCS12格式 (一個檔案用於證書和金鑰)
- 隱私增強型電子郵件(PEM)格式的證書 (包括鏈結)，PKCS8 PEM格式的金鑰。
- PEM格式的證書，PKCS8 PEM格式的金鑰：

限制

目前，ISE僅支援CSR中的這些擴展來簽署證書。

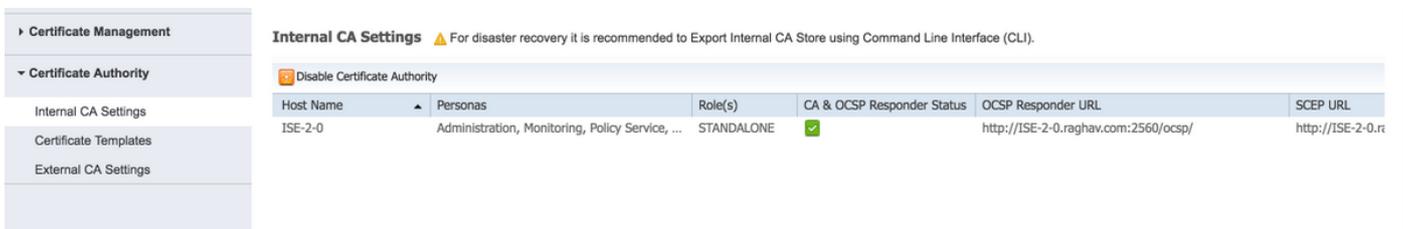
- 主題目錄屬性
- subjectAlternativeName
- 金鑰用法
- subjectKeyIdentifier
- auditIdentity
- extendedKeyUsage
- CERT_TEMPLATE_OID (這是一個定製的OID，用於指定通常用於BYOD流的模板)

附註：ISE內部CA旨在支援使用證書的功能(例如BYOD)，因此功能有限。思科不建議將ISE用作企業CA。

設定

要在網路中使用證書調配功能，必須啟用ISE內部CA服務並配置證書調配門戶。

步驟1.在ISE GUI上，導航到**Administration > System > Certificates > Certificate Authority > Internal CA**，要在ISE節點上啟用內部CA設定，請按一下**Enable Certificate Authority**。



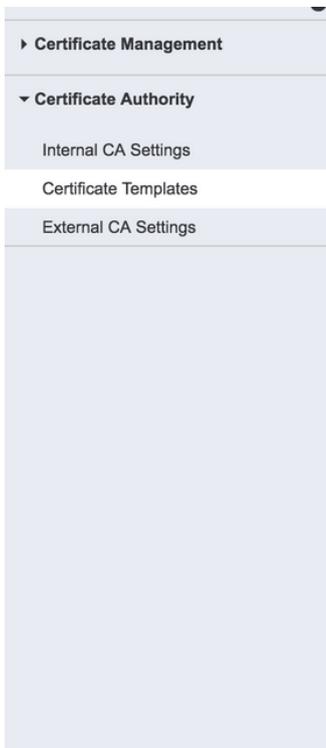
Internal CA Settings ⚠ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

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	✔	http://ISE-2-0.raghav.com:2560/ocsp/	http://ISE-2-0.r...

步驟2.在**Administration > System > Certificates > Certificate Templates > Add**下建立證書模板。

根據要求輸入詳細資訊並按一下**Submit**，如下圖所示。



Add Certificate Template

* Name

Description

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

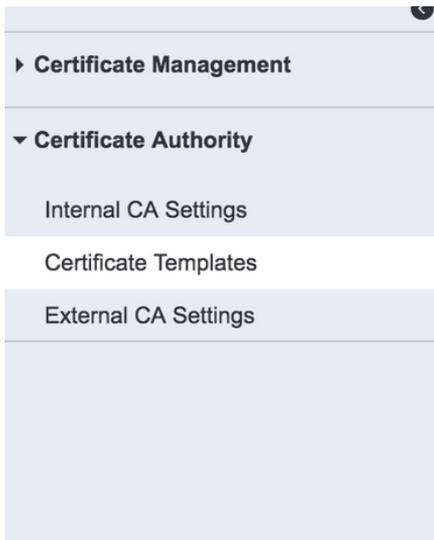
Subject Alternative Name (SAN)

Key Size

* SCEP RA Profile

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

附註：您可以在Administration > System > Certificates > Certificate Templates下看到已建立的證書模板清單，如下圖所示。



Certificate Templates

<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

步驟3。若要設定ISE憑證布建入口網站，請導覽至管理>裝置入口網站管理>憑證布建>建立，如下圖所示：

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

步驟4. 在新證書門戶上，展開門戶設定，如下圖所示。

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.

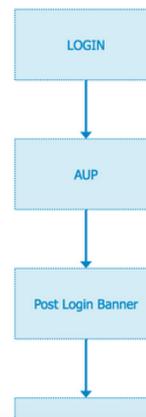


Portal Page Customization
Use these settings to specify the guest experience for this portal.

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



▼ **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
→ Choose all	✗ Clear all

Fully qualified domain name (FQDN):

Idle timeout: 1-30 (minutes)

HTTPS埠
 允許的介面
 證書組標籤
 驗證方法
 授權組
 完全限定的域名稱(FQDN)
 空閒超時

證書調配門戶應用於HTTPS的埠。
 ISE應偵聽此門戶的介面。
 要用於證書設定門戶的證書標籤，指示要用於此門戶的系統證書。
 選擇驗證登入到此門戶的身份庫序列。預設情況下，**certificate_request_sequ**
 可以通過將一組特定的AD組和內部使用者組移到所選表來控制可以訪問證書調
 您還可以為此門戶指定特定FQDN。使用http/https瀏覽到FQDN的使用者將重定
 該值定義入口的空閒超時。

附註：可以在**管理>身份管理>身份源序列**下檢查身份源的配置。

步驟5.設定登入頁面設定。

▼ **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

步驟6.配置AUP頁面設定。

▼ 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)

步驟7.您還可以新增登入後橫幅。

步驟8.在證書調配門戶設定下，指定允許的證書模板。

▼ Change Password Settings

- Allow internal users to change their own passwords

▼ Certificate Provisioning Portal Settings

Certificate Templates: *

步驟9.滾動至頁面頂部，然後按一下**Save**以儲存變更。

此外，通過導航到**Portal page customization**頁籤，可以進一步自定義門戶，在該頁籤中，可以根據需要更改AUP文本、登入後標題文本和其他消息。

驗證

使用本節內容，確認您的組態是否正常運作。

如果ISE已正確配置證書調配，則可以通過以下步驟從ISE證書調配門戶請求/下載證書。

步驟1.開啟瀏覽器並瀏覽到如上配置的證書調配門戶FQDN或證書調配測試URL。系統會將您重新導向至入口網站，如下圖所示：

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

Sign On

[Help](#)

步驟2.使用使用者名稱和密碼登入。

步驟3.成功驗證後，接受AUP並轉到證書調配頁面。

步驟4.憑證布建頁面提供以下三種方式下載憑證的功能：

- 單個證書 (無證書簽名請求)
- 單個證書 (帶證書簽名請求)
- 批次證書

生成沒有證書簽名請求的單個證書

- 若要產生不含CSR的單一憑證，請選擇**產生單一憑證 (不含憑證簽署請求)**選項。
- 輸入公用名(CN)。

附註：給定的CN必須與請求者的使用者名稱匹配。請求者引用用於登入門戶的使用者名稱。只有Admin使用者可以為不同的CN建立證書。

- 輸入為其生成證書的裝置的MAC地址。
- 選擇適當的證書模板。
- 選擇應下載證書的所需格式。
- 輸入證書密碼並按一下**G生成**。
- 生成並成功下載單個證書。

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... 

Certificate Password: *

.....

Confirm Password: *

.....|

Generate

Reset

使用證書簽名請求生成單個證書

- 若要產生不含CSR的單一憑證，請選擇**Generate single certificate(with certificate signing request)**選項。
- 從**憑證簽署請求詳細資訊**下的記事本檔案中複製和貼上CSR內容。
- 輸入為其生成證書的裝置的MAC地址。
- 選擇適當的證書模板。
- 選擇應下載證書的所需格式。
- 輸入證書密碼並按一下**Generate**。
- 將成功生成和下載單個證書。

Certificate Provisioning

I want to: *

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: *

```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAAIACAQAwEDEOMAwGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUgySpKa465ecULygnjHG
NC7bPqz4+5
8vK723r23ghympvBNPw31K6qzUCmDYLOcTwp+ymbWY3rfYxQ
nde8NofbTL
CrIhcnbmn0+SD7UozaXYb1DmugD8YL9Ht0Vv//WBKie6B8jZKl
WwqjAKVJ
yqJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABjsSToasXW
kyEIQT,8K5
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P50K
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0wTEMMmwn7Wbn5AgMBAAAGz
TBjBkqkqG9wOB
CQ4xVjBUAmAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYwXKY
BwkwEwYDVR0BAwwCgYIKaYBBQUHAwEwEQYJYIZIAW4QqEB
BAQDAgZAMA0GCSeG
Sib3DQEBQwUAA4IBAQCeZSHBMu71Pv?H9dQHTxY3v5WCyQ7
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALkXZWNyU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
JdypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ9K3hAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALkXZWNyU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
JdypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ9K3hAx0+
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: *

如果上傳包含CN和MAC地址欄位的CSV檔案，則可以生成多個MAC地址的批次證書。

附註：給定的CN必須與請求者的使用者名稱匹配。請求者引用用於登入門戶的使用者名稱。只有Admin使用者可以為不同的CN建立證書。

- 若要產生不含CSR的單一憑證，請選擇**Generate single certificate(with certificate signing request)** 選項。
- 上傳批次請求的csv檔案。
- 選擇適當的證書模板。
- 選擇應下載證書的所需格式。
- 輸入證書密碼並按一下**Generate**。
- 生成並下載批次證書zip檔案。

The screenshot shows the Cisco Certificate Provisioning Portal interface. At the top, there is a header with the Cisco logo and the text "Certificate Provisioning Portal". Below the header, the main content area is titled "Certificate Provisioning".

The form contains the following fields and options:

- I want to: ***: A dropdown menu with the selected option "Generate bulk certificates".
- Upload CSV File: ***: A file upload field with the text "Choose File" and the filename "maclist.csv". Below this field, there is a link: "If you don't have the CSV template, [download here](#)".
- Choose Certificate Template: ***: A dropdown menu with the selected option "EAP_Authentication_Certificate_Template".
- Description:**: A text input field containing "test bulk certificate".
- Certificate Download Format: ***: A dropdown menu with the selected option "PKCS12 format, including certificate chain (O...)". An information icon (i) is visible to the right of this dropdown.
- Certificate Password: ***: A password input field with masked characters "*****".
- Confirm Password: ***: A confirm password input field with masked characters "*****".

At the bottom of the form, there are two buttons: "Generate" (highlighted in blue) and "Reset".

Below the form, there is a [Help](#) link.

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。