

Configure el portal de aprovisionamiento de certificados ISE 2.0

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Limitaciones](#)

[Configurar](#)

[Verificación](#)

[Generar certificado único sin solicitud de firma de certificado](#)

[Generar certificado único con solicitud de firma de certificado](#)

[Generar certificados masivos](#)

[Troubleshoot](#)

Introducción

En este documento se describen la configuración y el funcionamiento del portal de aprovisionamiento de certificados de Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- ISE
- Certificados y servidores de autoridad certificadora (CA).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Service Engine 2.0
- PC con Windows 7

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El portal de aprovisionamiento de certificados es una nueva función introducida en ISE 2.0 que pueden utilizar los dispositivos finales para inscribirse y descargar certificados de identidad del servidor. Emite certificados a dispositivos que no pueden pasar por el flujo de incorporación.

Por ejemplo, los dispositivos como los terminales de punto de venta no pueden sufrir el flujo de la iniciativa "Trae tu propio dispositivo" (BYOD) y deben recibir certificados manualmente.

El portal de aprovisionamiento de certificados permite a un conjunto privilegiado de usuarios cargar una solicitud de certificado (CSR) para dichos dispositivos; genere pares de claves y, a continuación, descargue el certificado.

En ISE, puede crear plantillas de certificados modificadas y los usuarios finales pueden seleccionar una plantilla de certificado adecuada para descargar un certificado. Para estos certificados, ISE actúa como servidor de autoridad certificadora (CA) y podemos obtener el certificado firmado por la CA interna de ISE.

El portal de aprovisionamiento de certificados ISE 2.0 admite la descarga de certificados en estos formatos:

- Formato PKCS12 (incluida la cadena de certificados; un archivo para la cadena de certificados y la clave)
- Formato PKCS12 (un archivo para certificado y clave)
- Certificado (incluida la cadena) en formato de correo electrónico mejorado de privacidad (PEM), clave en formato PEM PKCS8.
- Certificado en formato PEM, clave en formato PKCS8 PEM:

Limitaciones

Actualmente, ISE sólo admite estas extensiones en un CSR para firmar un certificado.

- subjectDirectoryAttributes
- subjectAlternativeName
- KeyUsage
- subjectKeyIdentifier
- auditIdentity
- UsoClaveExtendida
- CERT_TEMPLATE_OID (se trata de un OID personalizado para especificar la plantilla que se utiliza normalmente en el flujo de BYOD)

Nota: La CA interna de ISE está diseñada para admitir funciones que utilizan certificados como BYOD y, por lo tanto, las capacidades son limitadas. Cisco no recomienda el uso de ISE como CA empresarial.

Configurar

Para utilizar la función de aprovisionamiento de certificados en la red, se debe habilitar el servicio de CA interna de ISE y configurar un portal de aprovisionamiento de certificados.

Paso 1. En la GUI de ISE, navegue hasta **Administration > System > Certificates > Certificate**

Authority > Internal CA y para habilitar la configuración interna de CA en el nodo ISE, haga clic en **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	Personnas	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...

Paso 2. Cree plantillas de certificado bajo **Administración > Sistema > Certificados > Plantillas de certificado > Agregar**.

Ingrese los detalles según el requisito y haga clic en **Enviar**, como se muestra en esta imagen.

Add Certificate Template

* Name: testcert
 Description: testing certificate

Subject

Common Name (CN): \$UserName\$ ⓘ
 Organizational Unit (OU):
 Organization (O):
 City (L):
 State (ST):
 Country (C):

Subject Alternative Name (SAN): MAC Address

Key Size: 2048

* SCEP RA Profile: ISE Internal CA

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

Submit Cancel

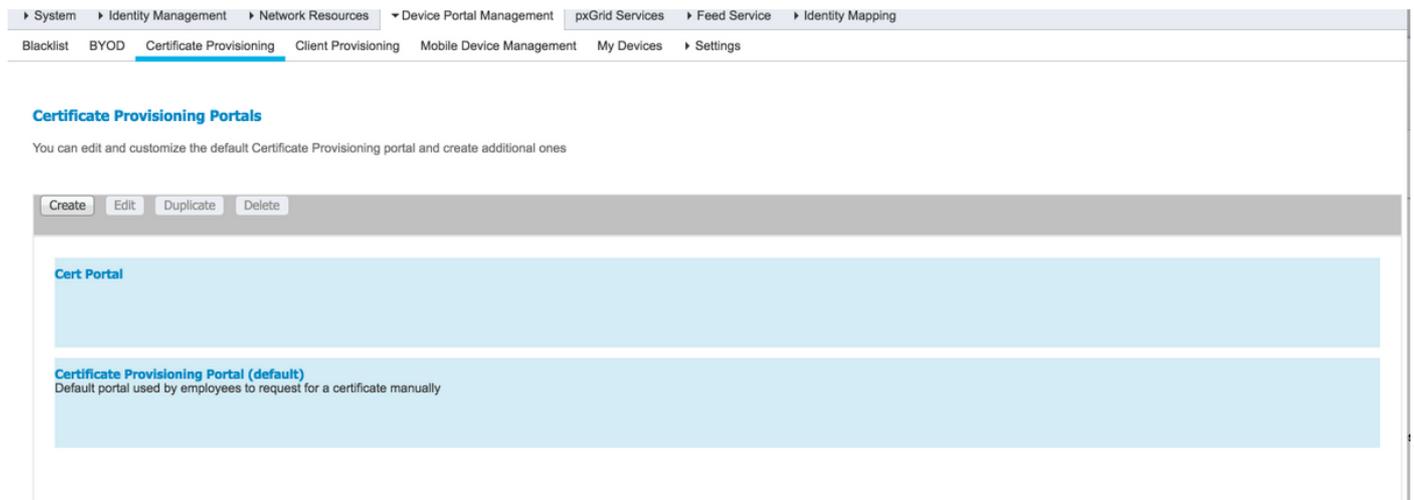
Nota: Puede ver la lista de plantillas de certificados creadas en **Administration > System > Certificates > Certificate Templates** como se muestra en esta imagen.

Certificate Templates

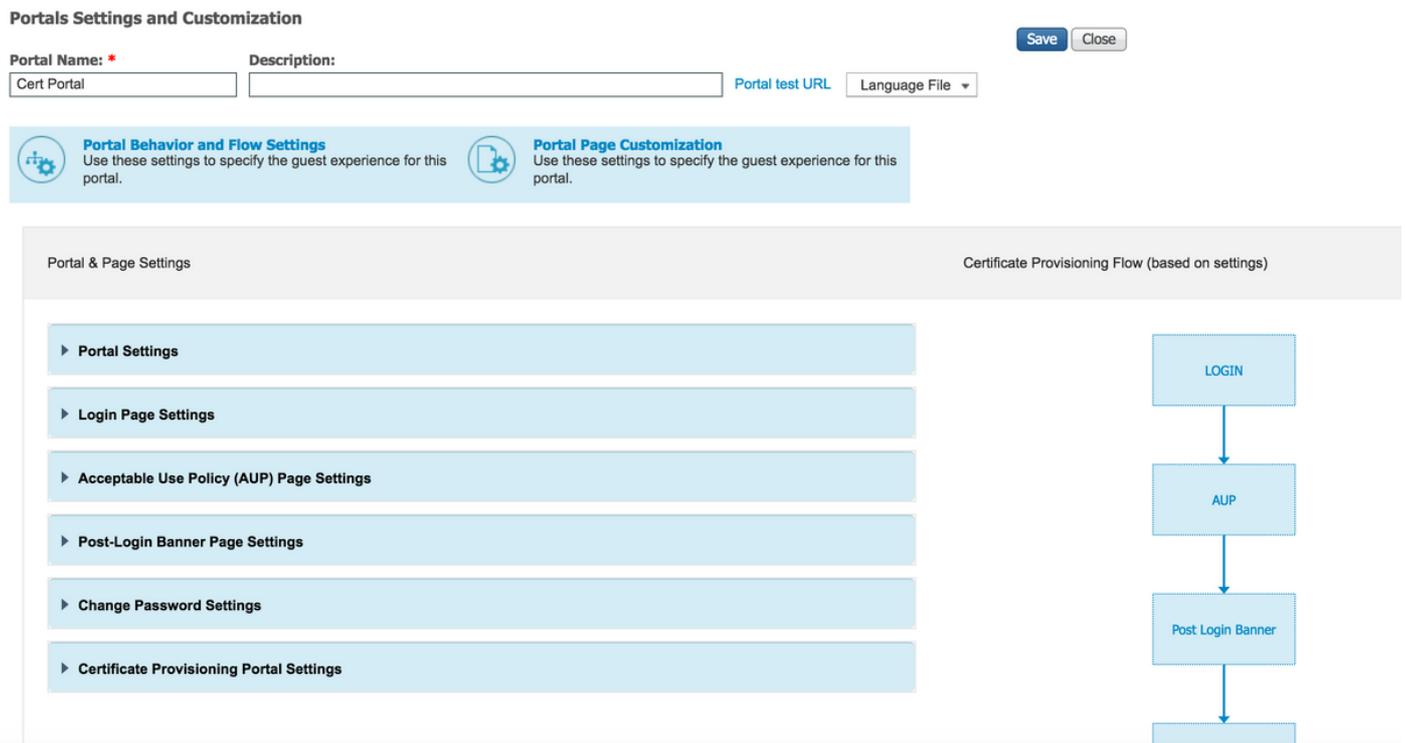
Edit Add Duplicate Delete

Template Name	Description	Key Size
CA_SERVICE_Certificate...	This template will be us...	2048
EAP_Authentication_Cer...	This template will be us...	2048
internalCA		2048
testcert	test certificate template	2048

Paso 3. Para configurar el portal de aprovisionamiento de certificados ISE, navegue hasta **Administración > Administración del portal de dispositivos > Aprovisionamiento de certificados > Crear**, como se muestra en la imagen:



Paso 4. En el nuevo portal de certificados, expanda la configuración del portal, como se muestra en la imagen.



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)

puerto HTTPS
 Interfaces permitidas
 Etiqueta del grupo de certificados
 método de autenticación
 Grupos autorizados
 Nombre de dominio completamente calificado (FQDN)
 Tiempo de espera inactivo

Puerto que debe utilizar el portal de aprovisionamiento.
 Las interfaces en las que ISE debería escuchar e intentar establecer una conexión.
 La etiqueta de certificado que se utilizará para el grupo de usuarios.
 Seleccione la secuencia del almacén de identidad que se utilizará para autenticar a los usuarios.
 El conjunto de usuarios que pueden acceder al portal.
 También puede asignar un FQDN específico a este grupo de usuarios.
 El valor define el tiempo de espera inactivo para un usuario inactivo.

Nota: La configuración del origen de identidad se puede comprobar en **Administration > Identity Management > Identity Source Sequence**.

Paso 5. Configure los parámetros de la página de inicio de sesión.

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

Paso 6. Configuración de los parámetros de la página AUP.

▼ **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)

Paso 7. También puede agregar un banner de inicio de sesión posterior.

Paso 8. En Configuración del portal de aprovisionamiento de certificados, especifique las plantillas de certificados permitidas.

▼ **Change Password Settings**

Allow internal users to change their own passwords

▼ **Certificate Provisioning Portal Settings**

Certificate Templates: *

Paso 9. Desplácese hasta la parte superior de la página y haga clic en **Guardar** para guardar los cambios.

Además, el portal se puede personalizar aún más navegando a la pestaña **Personalización de la página del portal** donde el texto de la PUA, el texto del banner de inicio de sesión y otros mensajes se pueden cambiar según los requisitos.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Si ISE se configura correctamente para el aprovisionamiento de certificados, se puede solicitar/descargar un certificado del portal de aprovisionamiento de certificados ISE con estos pasos.

Paso 1. Abra el explorador y vaya al FQDN del portal de aprovisionamiento de certificados tal y como se configuró anteriormente o a la URL de prueba de aprovisionamiento de certificados. Se le redirige al portal, como se muestra en esta imagen:

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](#)

Paso 2. Inicie sesión con el nombre de usuario y la contraseña.

Paso 3. Después de una autenticación exitosa, acepte AUP y éste se desplaza a la página de aprovisionamiento de certificados.

Paso 4. La página de aprovisionamiento de certificados proporciona la funcionalidad necesaria para descargar los certificados de tres maneras:

- Certificado único (sin solicitud de firma de certificado)
- Certificado único (con solicitud de firma de certificado)
- Certificados masivos

Generar certificado único sin solicitud de firma de certificado

- Para generar un solo certificado sin CSR, seleccione la opción **Generar un solo certificado (sin solicitud de firma de certificado)**.
- Introduzca un nombre común (CN).

Nota: El CN dado debe coincidir con el nombre de usuario del solicitante. El solicitante se refiere al nombre de usuario utilizado para iniciar sesión en el portal. Sólo los usuarios administradores pueden crear un certificado para un CN diferente.

- Introduzca la dirección MAC del dispositivo para el que se genera el certificado.
- Elija la plantilla de certificado adecuada.
- Elija el formato deseado en el que se debe descargar el certificado.
- Introduzca una contraseña de certificado y haga clic en **Ggenerar**.
- Se genera un solo certificado y se descarga correctamente.

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

Generar certificado único con solicitud de firma de certificado

- Para generar un solo certificado sin CSR, seleccione la opción Generar un solo certificado (sin solicitud de firma de certificado).
- Copie y pegue el contenido CSR del archivo de bloc de notas en **Detalles de solicitud de firma de certificado**.
- Introduzca la dirección MAC del dispositivo para el que se genera el certificado.
- Elija la plantilla de certificado adecuada.
- Elija el formato deseado en el que se debe descargar el certificado.
- Ingrese una contraseña de certificado y haga clic en **Generar**.
- Se generará y descargará un solo certificado correctamente.

Certificate Provisioning

I want to: *

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: *

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuQCCAAICAQAwEDEMGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUgySpKa465ecULygnjHG
NC7bPqz4+5
8vK723r23ghympvBNPw31K6qzUCmDYLOcTwp+ymbWY3rfYxQ
nde8NofbTL
CrHbnbnj0+SD7UlozoXYb1DmugD8YL9Ht0Vv//WBKie6B8jZKl
WwoqAKVJ
ysJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABjsSToasXW
kyEIQT,8K5
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P50K
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0wTEMMmwn7Wbn5AgMBAAGgZ
TBjBkqkqkG9wOB
CQ4xVBUUAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYXKCY
BwkwEwYDYR0BAwwCgYIKaYBBQUHAwEwEQYJYIZIAyB4QqEB
BAQDAgZAMA0GCSqG
Sib3DQEBCwUAA4IBAQCeZSHBMu71Pv?H9dQHTxY3v5WCyQ7
qNzOPUymVA3h+Z
Q1f72xulTfGEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/W0u3mfQcUPWPh8OzB
KA90V4uzV8Gif
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2f0M6CDMH
J0ypRA7w5K0JGB0HLWBAZ3ckl7ymB6QMOC5OqCDwnUSEWZ6
54/YAQ9K3hAx0+
xp2BY1uUYSEySHobb5RWAQhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1f72xulTfGEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/W0u3mfQcUPWPh8OzB
KA90V4uzV8Gif
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2f0M6CDMH
J0ypRA7w5K0JGB0HLWBAZ3ckl7ymB6QMOC5OqCDwnUSEWZ6
54/YAQ9K3hAx0+
xp2BY1uUYSEySHobb5RWAQhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

MAC Address:

11:AF:35:23:12:EC

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

test certificate

Certificate Download Format: *

PKCS12 format, including certificate chain (O...

Certificate Password: *

Confirm Password: *

Generar certificados masivos

Puede generar certificados masivos para varias direcciones MAC si carga archivos CSV que contienen los campos de dirección CN y MAC.

Nota: El CN dado debe coincidir con el nombre de usuario del solicitante. El solicitante se refiere al nombre de usuario utilizado para iniciar sesión en el portal. Sólo los usuarios administradores pueden crear un certificado para un CN diferente.

- Para generar un solo certificado sin CSR, seleccione la opción **Generar un solo certificado (con solicitud de firma de certificado)**.
- Cargue el archivo csv para solicitud masiva.
- Elija la plantilla de certificado adecuada.
- Elija el formato deseado en el que se debe descargar el certificado.
- Ingrese una contraseña de certificado y haga clic en **Generar**.
- Se genera y descarga un archivo zip de certificado masivo.



Certificate Provisioning

I want to: *

Generate bulk certificates

Upload CSV File: *

Choose File maclist.csv

If you don't have the CSV template, [download here](#)

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

test bulk certificate

Certificate Download Format: *

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

Certificate Password: *

.....

Confirm Password: *

.....|

Generate Reset

[Help](#)

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.