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)

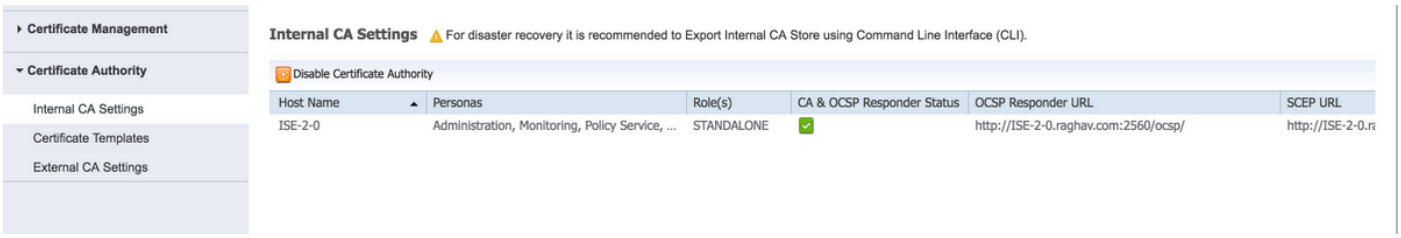
> **Nota:** La CA interna de ISE está diseñada para admitir funciones que utilizan certificados como BYOD y, por lo tanto, las capacidades son limitadas. Cisco no recomienda el uso de ISE como CA empresarial.

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.

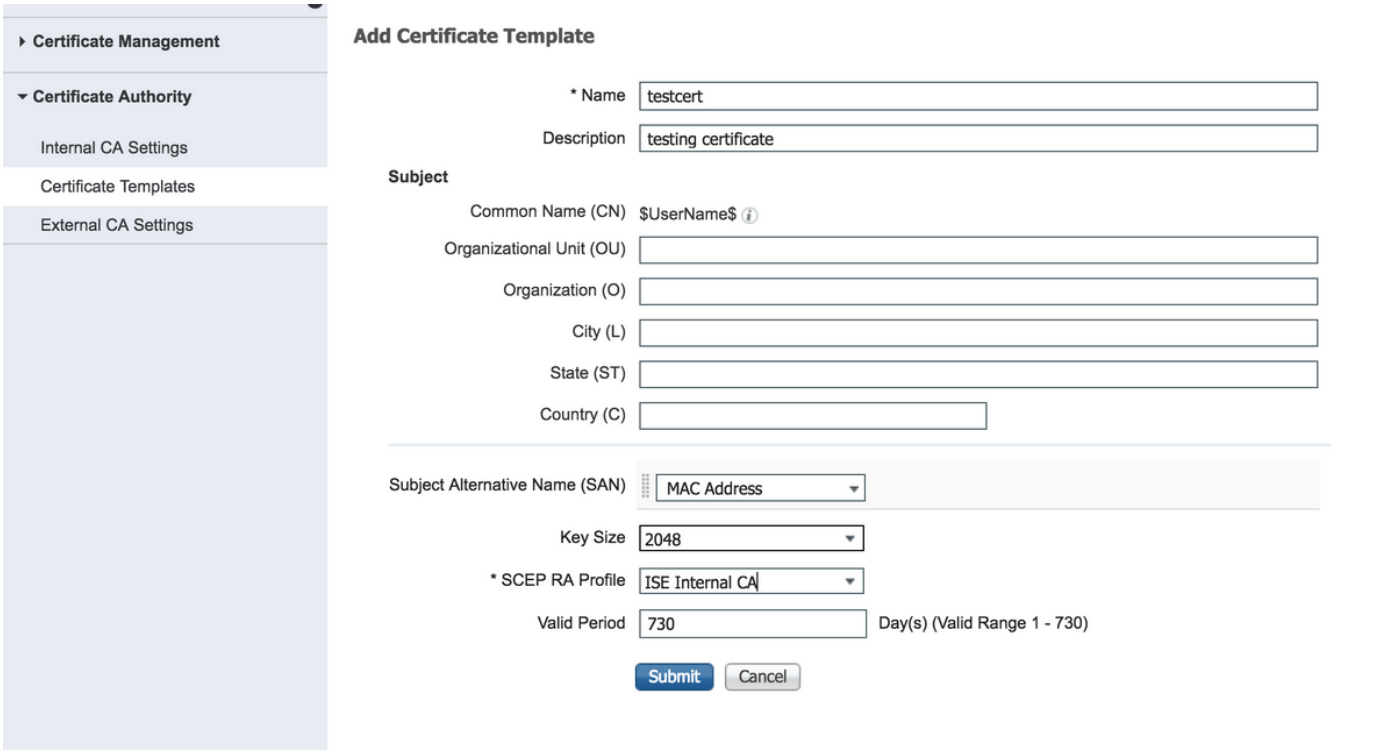
Paso 1.En la GUI de ISE, navegue hasta **Administration > System > Certificates > Certificate**

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

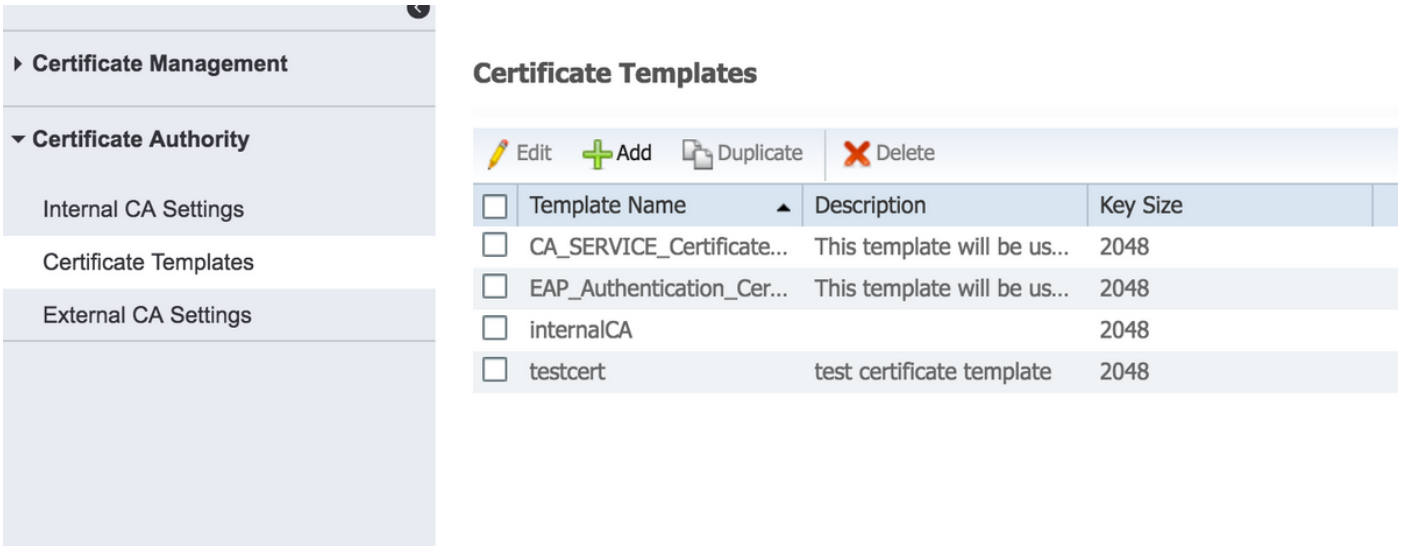


Paso 2. Cree plantillas de certificado bajo **Administración > Sistema > Certificados > Plantillas de certificado > Agregar**.

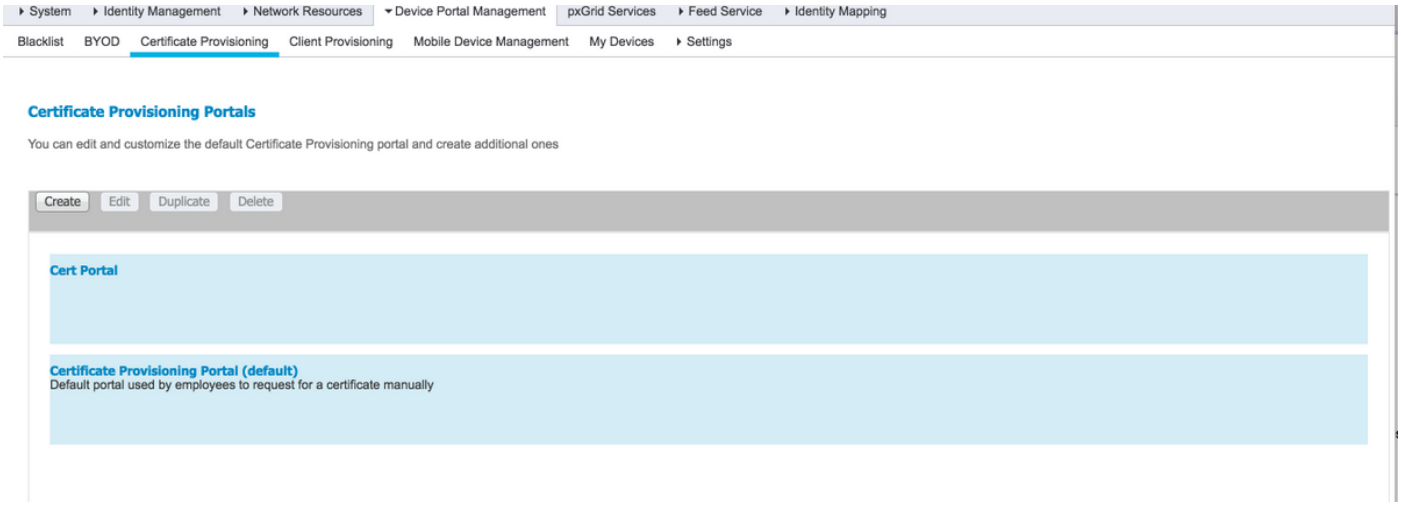
Ingrese los detalles según el requisito y haga clic en **Enviar,** como se muestra en esta imagen.



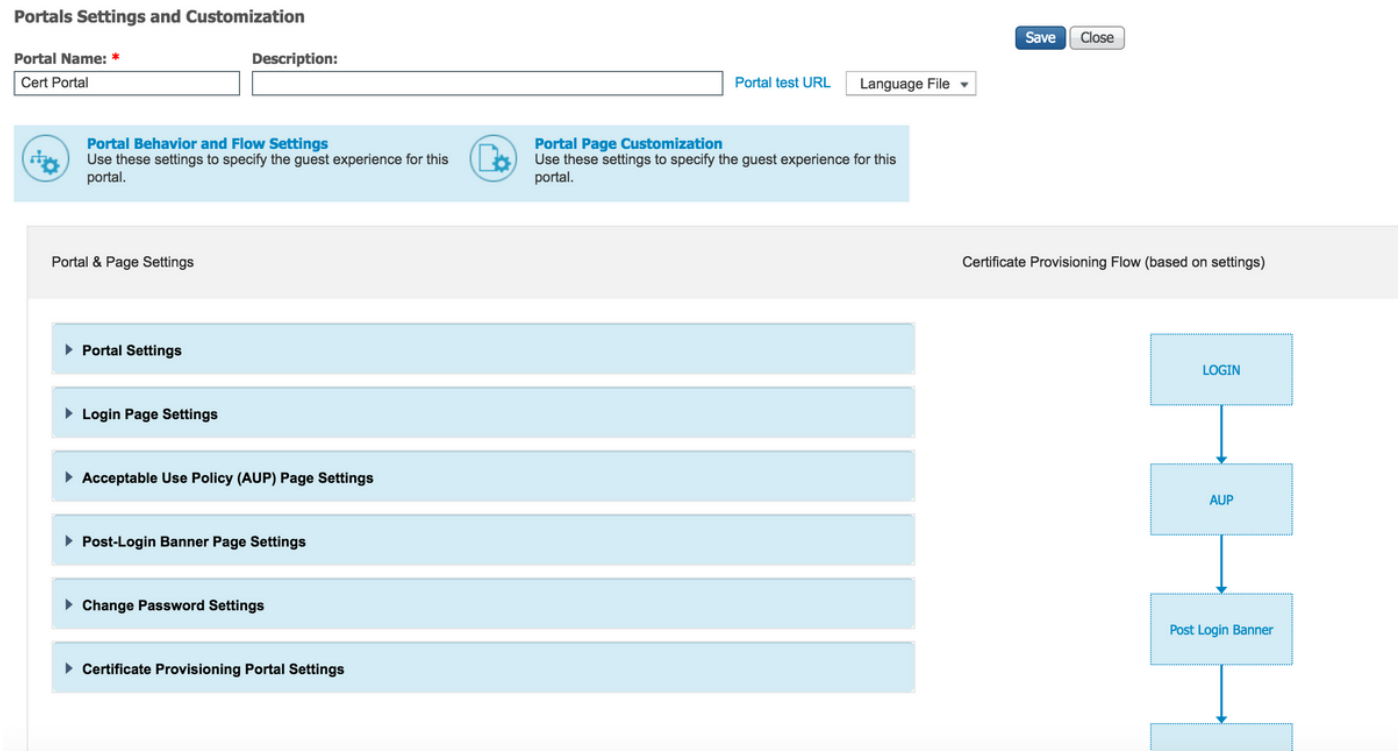
Nota: Puede ver la lista de plantillas de certificados creadas en **Administration > System > Certificates > Certificate Templates** como se muestra en esta imagen.

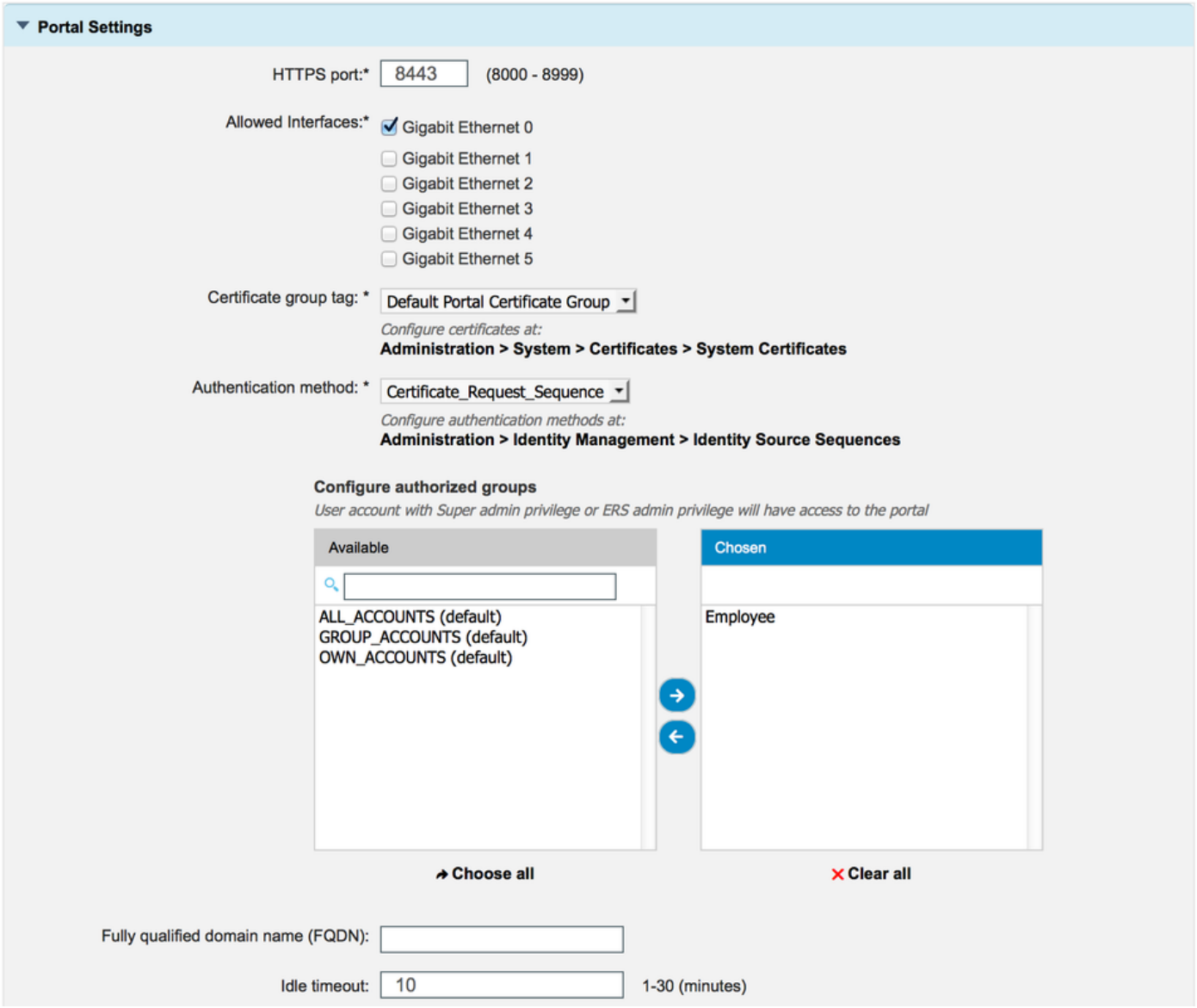


Paso 3. Para configurar el portal de aprovisionamiento de certificados ISE, navegue hasta **Administración > Administración del portal de dispositivos > Aprovisionamiento de certificados > Crear**, como se muestra en la imagen:



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

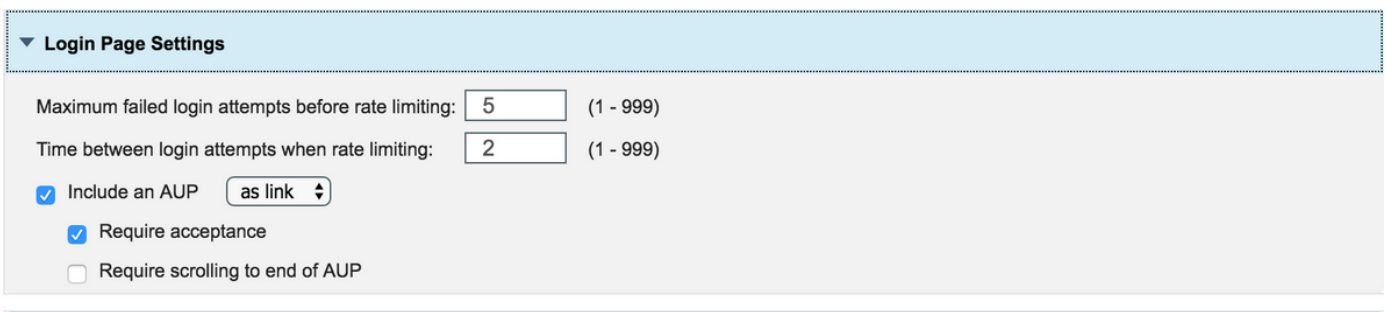




puerto HTTPS	Puerto que debe utilizar el portal de aprovisionam
Interfaces permitidas	Las interfaces en las que ISE debería escuchar e
Etiqueta del grupo de certificados	La etiqueta de certificado que se utilizará para el
método de autentificación	Seleccione la secuencia del almacén de identida
Grupos autorizados	El conjunto de usuarios que pueden acceder al p
Nombre de dominio completamente calificado (FQDN)	También puede asignar un FQDN específico a es
Tiempo de espera inactivo	El valor define el tiempo de espera inactivo para

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

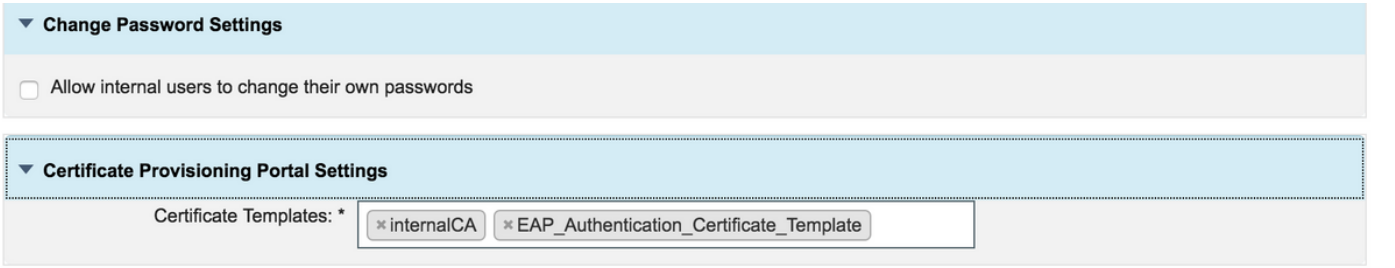
Paso 5. Configure los parámetros de la página de inicio de sesión.



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

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.



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

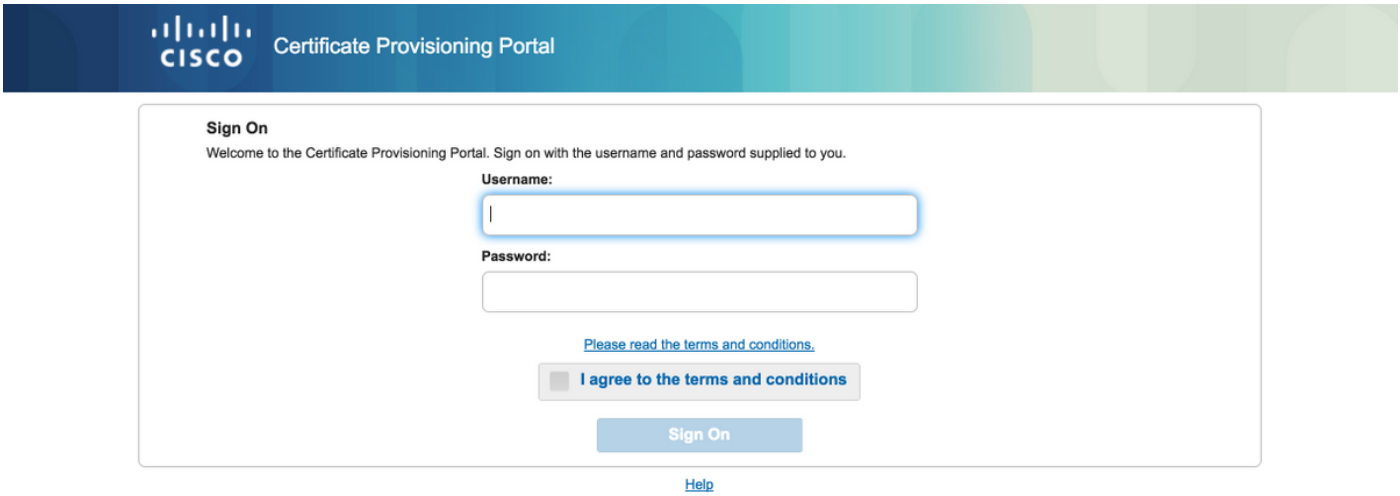
Además, el portal se puede personalizar aún más navegando a la pestaña **Personalización de la página del portal** donde el texto de la PUA, el texto del banner de inicio de sesión y otros mensajes se pueden cambiar según los requisitos.

Verificación

Utilize 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:



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:

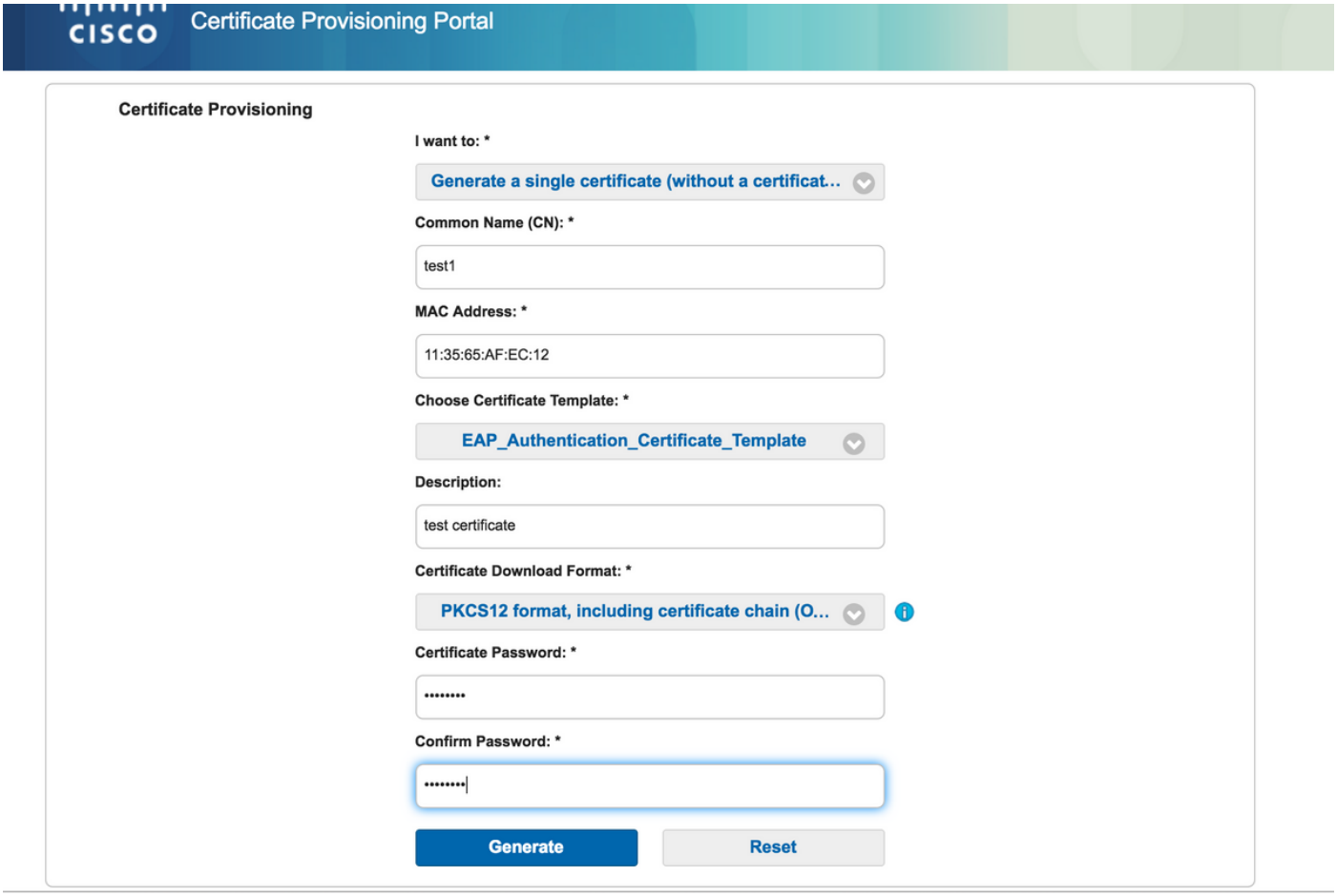
- Certificado único (sin solicitud de firma de certificado)
- Certificado único (con solicitud de firma de certificado)
- Certificados masivos

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).

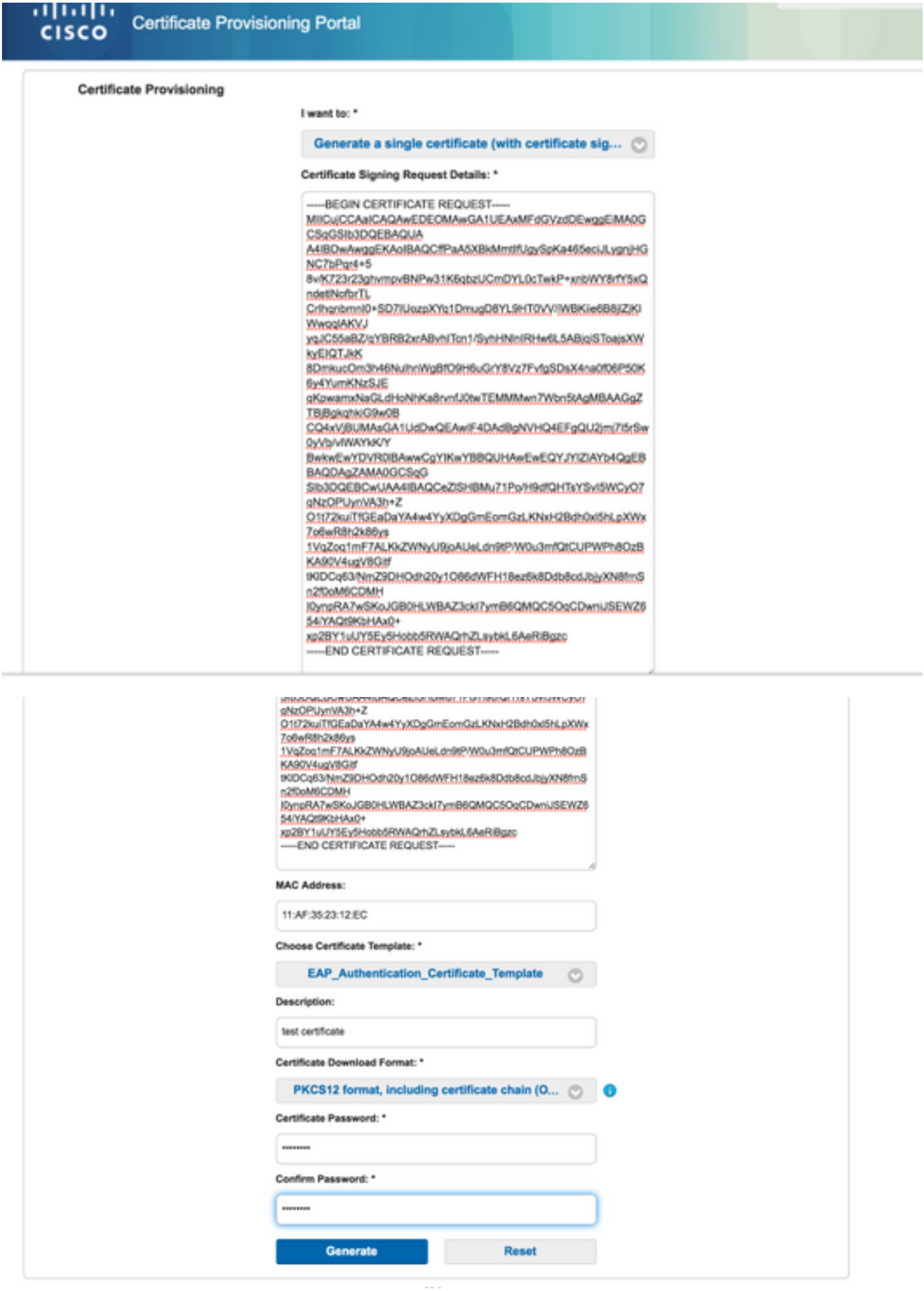
  Nota: El CN dado debe coincidir con el nombre de usuario del solicitante. El solicitante se refiere al nombre de usuario utilizado para iniciar sesión en el portal. Sólo los usuarios administradores pueden crear un certificado para un CN diferente.

- 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.



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.

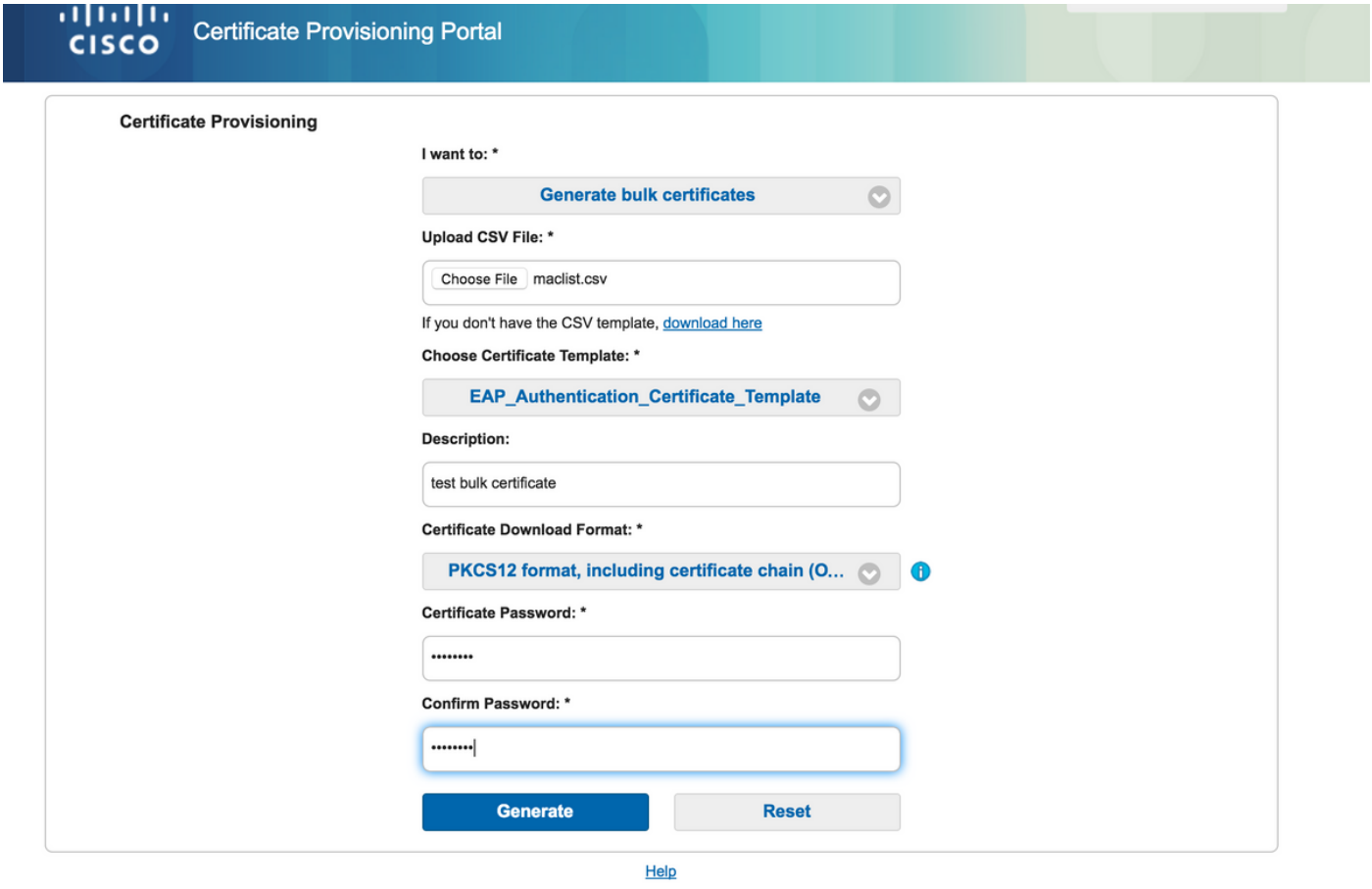


Generar certificados masivos

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.



Troubleshoot

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