

# Configurar o portal de provisionamento de certificados ISE 2.0

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Limitações](#)

[Configurar](#)

[Verificar](#)

[Gerar certificado único sem solicitação de assinatura de certificado](#)

[Gerar certificado único com solicitação de assinatura de certificado](#)

[Gerar certificados em massa](#)

[Troubleshoot](#)

## Introduction

Este documento descreve a configuração e a funcionalidade do portal de provisionamento de certificados do Identity Services Engine (ISE).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- ISE
- Certificados e servidores de autoridade de certificação (AC).

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity Service Engine 2.0
- PC 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O portal de provisionamento de certificados é um novo recurso introduzido no ISE 2.0 que pode ser usado por dispositivos finais para registrar e baixar certificados de identidade do servidor. Emite certificados para dispositivos que não podem passar pelo fluxo de integração.

Por exemplo, dispositivos como terminais de ponto de venda não podem passar pelo fluxo. Traga seu próprio dispositivo (BYOD) e precisam receber certificados manualmente.

O Portal de Provisionamento de Certificados permite que um conjunto privilegiado de usuários carregue uma solicitação de certificado (CSR) para esses dispositivos; gere pares de chaves e faça o download do certificado.

No ISE, você pode criar modelos de certificado modificados e os usuários finais podem selecionar um modelo de certificado adequado para baixar um certificado. Para esses certificados, o ISE atua como um servidor de Autoridade de Certificação (CA) e podemos obter o certificado assinado pela CA interna do ISE.

O portal de provisionamento de certificados do ISE 2.0 suporta o download de certificados nestes formatos:

- Formato PKCS12 (incluindo a cadeia de certificados; um arquivo para a cadeia de certificados e a chave)
- Formato PKCS12 (um arquivo para certificado e chave)
- Certificado (incluindo cadeia) no formato Privacy Enhanced Electronic Mail (PEM), chave no formato PKCS8 PEM.
- Certificado no formato PEM, chave no formato PKCS8 PEM:

## Limitações

Atualmente, o ISE oferece suporte apenas a essas extensões em um CSR para assinar um certificado.

- subjectDirectoryAttributes
- nomeAlternativoassunto
- keyUsage
- identificadordeChaveassunto
- auditIdentity
- extendedKeyUsage
- CERT\_TEMPLATE\_OID (este é um OID personalizado para especificar o modelo que é usado geralmente no fluxo de BYOD)

**Note:** A CA interna do ISE foi projetada para suportar recursos que usam certificados como BYOD e, portanto, os recursos são limitados. O uso do ISE como uma CA corporativa não é recomendado pela Cisco.

## Configurar

Para usar o recurso de provisionamento de certificado na rede, o serviço CA interno do ISE deve ser habilitado e um portal de provisionamento de certificado deve ser configurado.

Etapa 1. Na GUI do ISE, navegue para **Administration > System > Certificate Authority > Internal CA** e, para habilitar as configurações internas da CA no nó do ISE, clique em **Enable 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...

Etapa 2. Crie modelos de certificado em **Administração > Sistema > Certificados > Modelos de Certificado > Adicionar**.

Insira os detalhes de acordo com o requisito e clique em **Submit (Enviar)**, conforme mostrado nesta imagem.

**Add Certificate Template**

\* Name: testcert  
Description: testing certificate

**Subject**

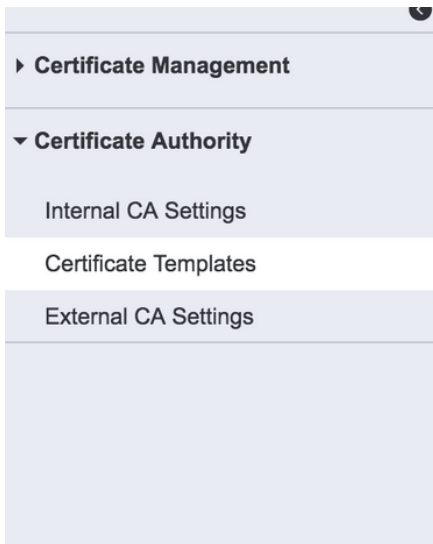
Common Name (CN): \$UserName\$ ⓘ  
Organizational Unit (OU):  
Organization (O):  
City (L):  
State (ST):  
Country (C):

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

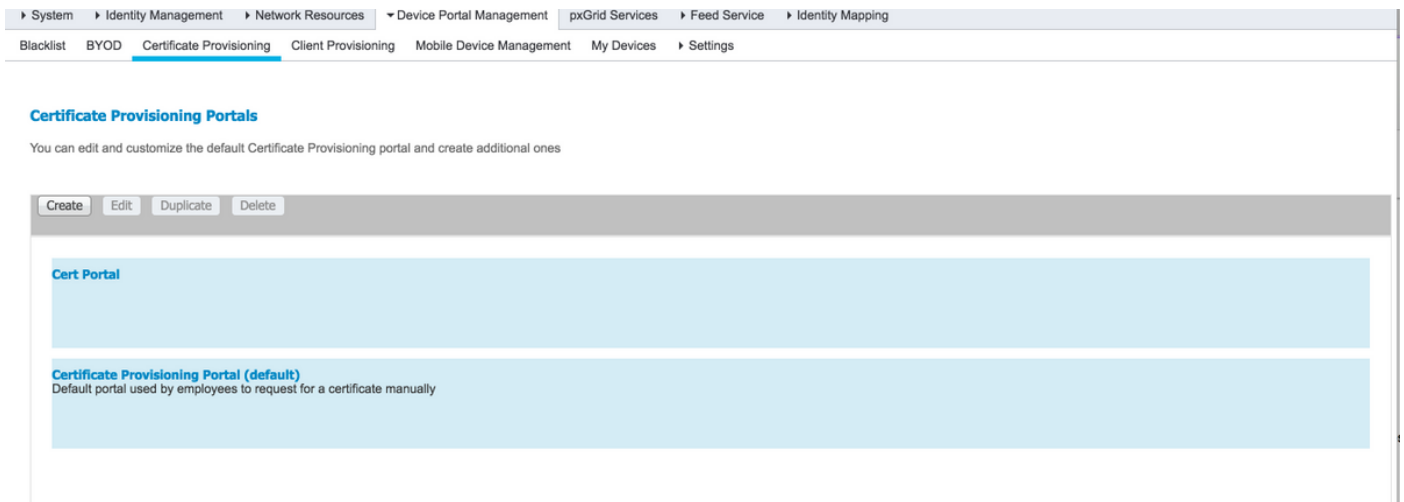
**Note:** Você pode ver a lista de modelos de certificado criados em **Administração > Sistema > Certificados > Modelos de Certificado** como mostrado nesta imagem.



## 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

Etapa 3. Para configurar o portal de provisionamento de certificados ISE, navegue para **Administração > Gerenciamento do portal do dispositivo > Provisionamento de certificado > Criar**, como mostrado na imagem:



Etapa 4. No novo portal de certificados, expanda as configurações do portal, conforme mostrado na imagem.

Portals Settings and Customization

Save Close

Portal Name: \*  Description:

Portal test URL  Language File



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

  
ALL\_ACCOUNTS (default)  
GROUP\_ACCOUNTS (default)  
OWN\_ACCOUNTS (default)

Chosen

Employee

Fully qualified domain name (FQDN):

Idle timeout:  1-30 (minutes)

porta HTTPS  
Interfaces permitidas

Porta que deve ser usada pelo portal de provisionamento  
As interfaces nas quais o ISE deve ouvir este portal.

Etiqueta de grupo de certificados  
método de autenticação  
Grupos autorizados  
Nome de domínio totalmente qualificado (FQDN)  
Tempo limite ocioso

A marca de certificado a ser usada para o portal de provisionamento.  
Selecione a sequência do repositório de identidades o qual o usuário pertence.  
O conjunto de usuários que podem acessar o portal de provisionamento.  
Você também pode fornecer FQDN específico a este portal de provisionamento.  
O valor define o timeout de ociosidade do portal.

**Note:** A configuração da origem da identidade pode ser verificada em **Administration > Identity Management > Identity Source Sequence**.

Etapa 5. Defina as configurações da página de login.

▼ **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

Etapa 6. Definir as configurações da 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)

Passo 7. Você também pode adicionar um banner de pós-login.

Etapa 8. Em Configurações do portal de Provisionamento de Certificado, especifique os modelos de certificado permitidos.

▼ **Change Password Settings**

Allow internal users to change their own passwords

▼ **Certificate Provisioning Portal Settings**

Certificate Templates: \*

**Etapa 9.** Role até o topo da página e clique em **Salvar** para salvar as alterações.

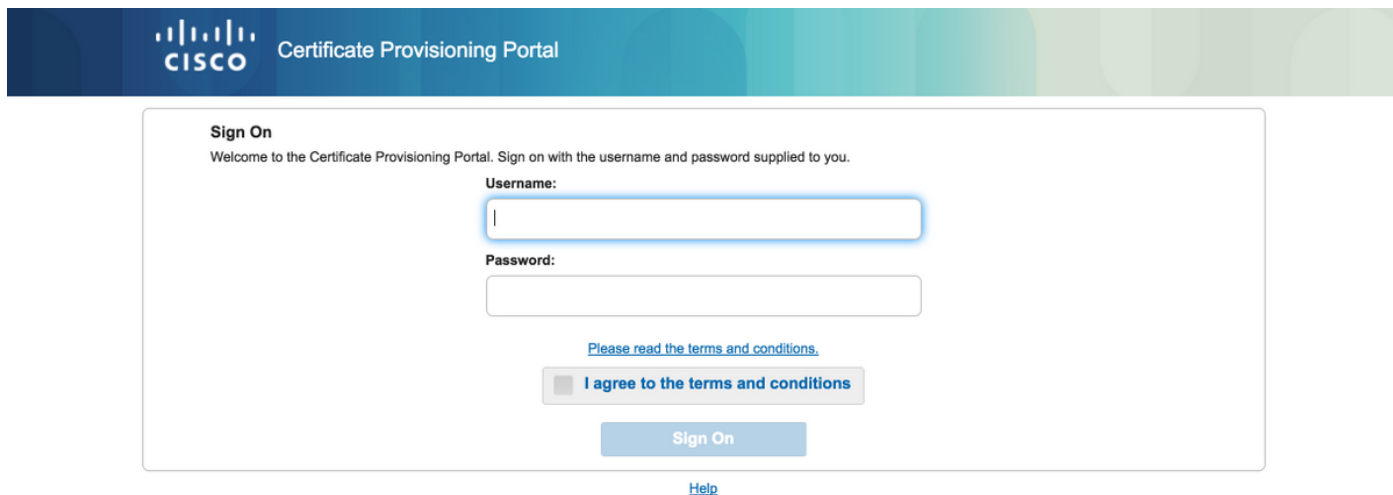
Além disso, o portal pode ser mais personalizado navegando até a guia **Personalização da página do portal**, onde o texto AUP, o texto do banner de pós-login e outras mensagens podem ser alterados conforme os requisitos.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Se o ISE estiver configurado corretamente para provisionamento de certificado, um certificado poderá ser solicitado/baixado do portal de provisionamento de certificado do ISE com estas etapas.

Etapa 1. Abra o navegador e navegue até o portal de provisionamento de certificados FQDN conforme configurado acima ou o URL do teste de provisionamento de certificados. Você é redirecionado para o portal, como mostrado nesta imagem:



The screenshot shows the Cisco Certificate Provisioning Portal Sign On page. At the top, there is a blue header with the Cisco logo and the text "Certificate Provisioning Portal". Below the header, the page title is "Sign On" and the subtitle is "Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you." The main content area contains a "Username:" label followed by a text input field, a "Password:" label followed by a password input field, a link "Please read the terms and conditions.", a checkbox labeled "I agree to the terms and conditions", and a "Sign On" button. At the bottom of the form area, there is a "Help" link.

Etapa 2. Faça login com o nome de usuário e a senha.

Etapa 3. Após a autenticação bem-sucedida, aceite o AUP e ele chega à página de provisionamento de certificado.

Etapa 4. A página de provisionamento de certificado fornece a funcionalidade para fazer o download de certificados de três maneiras:

- Certificado único (sem solicitação de assinatura de certificado)
- Certificado único (com solicitação de assinatura de certificado)
- Certificados em massa

## Gerar certificado único sem solicitação de assinatura de certificado

- Para gerar um único certificado sem CSR, selecione a opção **Gerar certificado único (sem solicitação de assinatura de certificado)**.
- Digite o nome comum (CN).

**Note:** O CN fornecido deve corresponder ao nome de usuário do solicitante. O solicitante refere-se ao nome de usuário usado para fazer login no portal. Somente usuários Admin podem criar um certificado para um CN diferente.

- Insira o endereço MAC do dispositivo para o qual o certificado está sendo gerado.

- Escolha o modelo de certificado apropriado.
- Escolha o formato desejado no qual o certificado deve ser baixado.
- Digite uma senha de certificado e clique em **GGerar**.
- Um único certificado é gerado e baixado com êxito.

CISCO Certificate Provisioning Portal

**Certificate Provisioning**

I want to: \*

Generate a single certificate (without a certificat... ▼

Common Name (CN): \*

MAC Address: \*

Choose Certificate Template: \*

EAP\_Authentication\_Certificate\_Template ▼

Description:

Certificate Download Format: \*

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

Certificate Password: \*

Confirm Password: \*

Generate
Reset

## Gerar certificado único com solicitação de assinatura de certificado

- Para gerar um único certificado sem CSR, selecione a opção **Gerar certificado único (com solicitação de assinatura de certificado)**.
- Copie e cole o conteúdo do CSR do arquivo notepad em **Certificate Signing Request Details**.
- Insira o endereço MAC do dispositivo para o qual o certificado está sendo gerado.
- Escolha o modelo de certificado apropriado.
- Escolha o formato desejado no qual o certificado deve ser baixado.
- Digite uma senha de certificado e clique em **Gerar**.
- Um único certificado será gerado e baixado com êxito.



Certificate Provisioning

I want to: \*

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: \*

```

-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaIQAQAwEDEOMAwGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUjySpKa465ecULygnjHG
NC7bPq4+5
8vK723r23ghympvBNPw31K6qzUcMdyL0cTwpP+xbWY3rfY5Q
nde8NofbTL
Crlhznbnm0+SD7lUozpXYa1DmugD8YLSHT0VV/WBKie6B8jZKl
WwqgAKVJ
ysJC55eBZ/yYBRB2xARvhlTon1/SyhHNnlRHw6L5ARolSToasXW
kyEIQT_RK
8DmkucOm3h46NulhrWgRfO9H6uGry8vz7FvqSDsX4na0f6P50K
6y4YumKNzSJE
qKowamNaGLdHcNkKa8nmlJ0wTEMMmwn7Wbn5AgMBAAGz
TBjBqzkkiG9wOB
CQ4xVjBUMAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQUZimj75r5w
DyYp/vWAYKCY
BwkwEwYDVR0BAwwCgYIKwYBBQUHAWEwEQYJYIZIAyM4QqEB
BAQDAgZAMA0GCSqG
Sib3DQEBCwUAA4IBAQCsZSHBMu71Pv?H9dQHTsY5v5WcyQ7
qNzOPUynVA3h+Z
Q1f72xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoo1mF7ALkKZWNYU9oAUeLdn9P?W0u3mfQICUPWPh8OzB
KA90V4uzY8Gif
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJpJyXN8fmS
n2f0M6CDMH
J0ynsRA7w5K0JGB0HLWBAZ3ckl7ymB6QMOC5OzCDwnIUSEWZ6
54/YAQ8KsHAx0+
xp2BY1uLY5EY5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
    
```

```

qNzOPUynVA3h+Z
Q1f72xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoo1mF7ALkKZWNYU9oAUeLdn9P?W0u3mfQICUPWPh8OzB
KA90V4uzY8Gif
tKDCq63NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJpJyXN8fmS
n2f0M6CDMH
J0ynsRA7w5K0JGB0HLWBAZ3ckl7ymB6QMOC5OzCDwnIUSEWZ6
54/YAQ8KsHAx0+
xp2BY1uLY5EY5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----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: \*

\*\*\*\*\*

Generate

Reset

## Gerar certificados em massa

Você pode gerar certificados em massa para vários endereços MAC se carregar arquivos CSV que contenham campos de endereços CN e MAC.

**Note:** O CN fornecido deve corresponder ao nome de usuário do solicitante. O solicitante refere-se ao nome de usuário usado para fazer login no portal. Somente usuários Admin podem criar um certificado para um CN diferente.

- Para gerar um único certificado sem CSR, selecione a opção **Gerar certificado único (com solicitação de assinatura de certificado)**.
- Carregue o arquivo csv para solicitação em massa.
- Escolha o modelo de certificado apropriado.
- Escolha o formato desejado no qual o certificado deve ser baixado.
- Digite uma senha de certificado e clique em **Gerar**.
- Um arquivo zip de certificado em massa é gerado e baixado.

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

- I want to: \***: A dropdown menu with the selected option 'Generate bulk certificates'.
- Upload CSV File: \***: A file upload field with a 'Choose File' button and the filename 'maclist.csv'.
- If you don't have the CSV template, [download here](#)**: A link to download a template.
- 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...'. A blue information icon is visible to the right of the dropdown.
- Certificate Password: \***: A password input field with masked characters '.....'.
- Confirm Password: \***: A second password input field with masked characters '.....|'.
- Generate**: A blue button to submit the form.
- Reset**: A grey button to clear the form.

At the bottom center of the page, there is a [Help](#) link.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.