

# ISE 2.0 certificaatprovisioningportal configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen](#)

[Configureren](#)

[Verifiëren](#)

[Enkelvoudig certificaat genereren zonder Aanvraag voor certificaatsignalering](#)

[Enkelvoudig certificaat genereren met certificaataanvraag](#)

[Bulkcertificaten genereren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft de configuratie en functionaliteit van het provisioningportal voor Identity Services Engine (ISE).

## Voorwaarden

### Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- ISE
- Certificaten en certificeringsinstanties (CA) servers.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine 2.0
- Windows 7 PC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

Het certificaatprovisioningportal is een nieuwe functie die in ISE 2.0 is geïntroduceerd en die door

end-apparaten kan worden gebruikt om identiteitsbewijzen van server in te schrijven en te downloaden. Het geeft certificaten af aan apparaten die niet door de instapstroom kunnen gaan.

Apparaten zoals verkooppunten kunnen bijvoorbeeld geen BYOD-stroom (Point-of-sale terminals) ondergaan en moeten handmatig worden afgegeven.

Met het certificaatprovisioningportal kunt u een bevoorrechte reeks gebruikers een certificaataanvraag (CSR) voor dergelijke apparaten uploaden; genereren van sleutelparen, en dan downloaden van het certificaat.

Op ISE kunt u aangepaste certificaatsjablonen maken en eindgebruikers kunnen een geschikte certificaatsjabloon selecteren om een certificaat te downloaden. Voor deze certificaten treedt ISE op als een CA-server (certificaatautoriteit) en we kunnen het certificaat laten ondertekenen door ISE interne CA.

ISE 2.0-portal voor provisioning van certificaten ondersteunt het downloaden van deze indelingen:

- PKCS12-formaat (met inbegrip van de certificeringsketen; één bestand voor zowel de certificeringsketen als de sleutel)
- PKCS12-formaat (één bestand voor zowel certificaat als sleutel)
- Certificaat (met inbegrip van keten) in Privacyuitgebreide Electronic Mail-formaat (PEM), sleutel in PKCS8 PEM-formaat.
- Certificaat in PEM-formaat, sleutel in PKCS8 PEM-formaat:

## Beperkingen

Momenteel ondersteunt ISE alleen deze uitbreidingen in een CSR om een certificaat te ondertekenen.

- subjectDirectoryAttributes
- onderworpenAlternativeName
- toetsGebruik
- subjectKeyIdentifier
- controleIdentity
- uitgebreidKeyGebruik
- CERT\_TEMPLATE\_OID (dit is een aangepaste OID die wordt gemaakt om de sjabloon te specificeren die doorgaans wordt gebruikt in BYOD-flow)

Opmerking: ISE interne CA is ontworpen om functies te ondersteunen die certificaten zoals BYOD gebruiken en dus zijn de mogelijkheden beperkt. Het gebruik van ISE als Enterprise CA wordt niet aanbevolen door Cisco.

## Configureren

Om de functie van certificatenvoorziening in netwerk te kunnen gebruiken, moet de interne CA-service van ISE ingeschakeld zijn en moet een provisioningportal ingesteld worden.

Stap 1. Op ISE GUI, navigeer naar **Administratie > Systeem > Certificaten > certificaatinstantie > Interne CA** en om de interne CA-instellingen op het ISE-knooppunt in te schakelen, klikt u op

## certificaatinstantie inschakelen.

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...

Stap 2. Maak certificaatsjablonen onder **Beheer > Systeem > Certificaten > certificaatsjablonen > Toevoegen**.

Voer de gegevens in volgens de vereisten en klik op **Indienen**, zoals in deze afbeelding wordt weergegeven.

**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

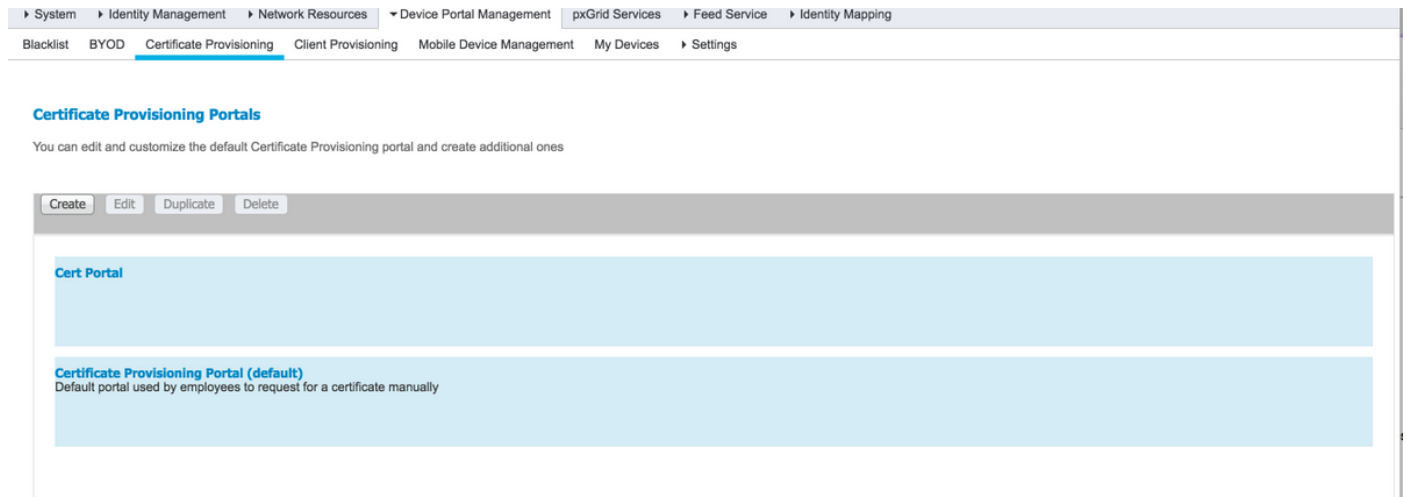
Opmerking: U kunt de lijst met gedefinieerde certificaatsjablonen zien onder **Beheer > Systeem > Certificaten > certificaatsjablonen** zoals in deze afbeelding weergegeven.

**Certificate Templates**

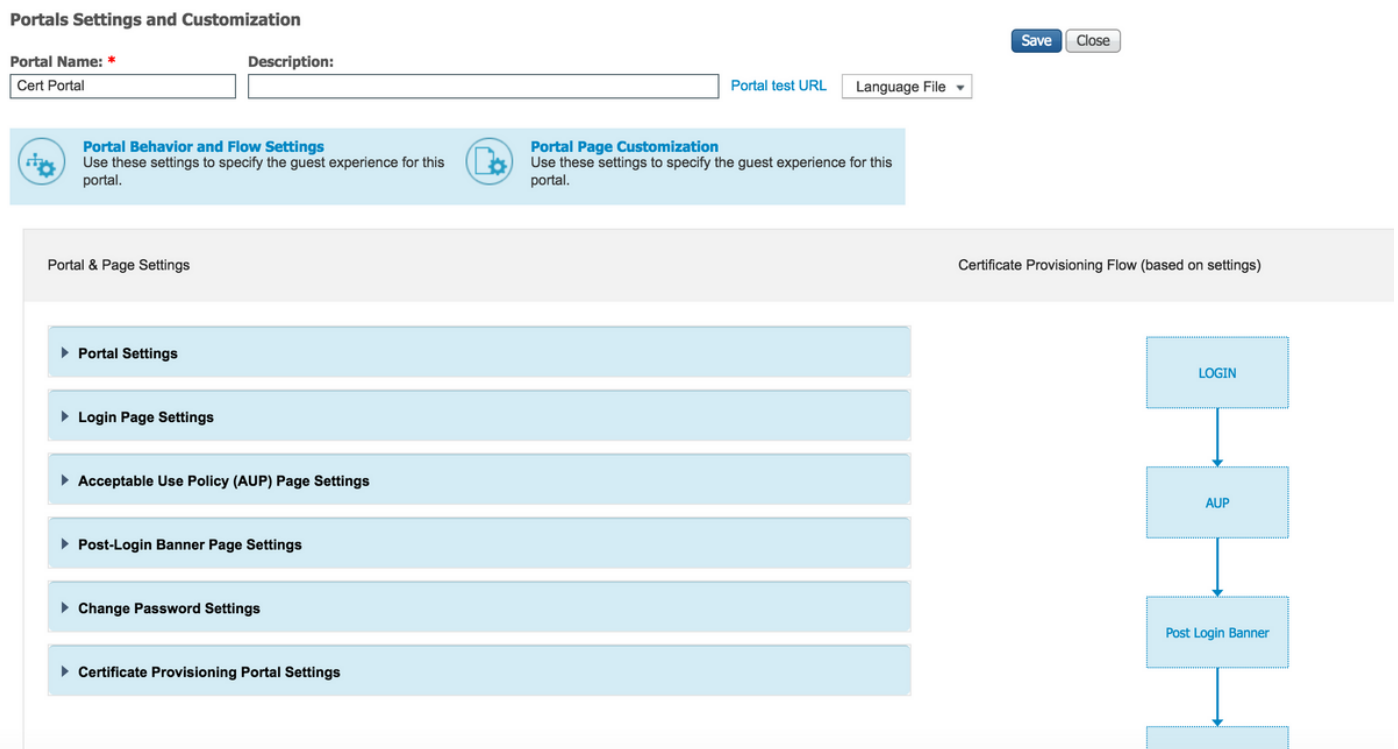
Edit Add Duplicate Delete

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

Stap 3. Om het ISE-provisioningportal te configureren kunt u navigeren naar **Beheer > Apparaatportal > certificaatprovisioning > Aanmaken** zoals in de afbeelding:



Stap 4. Sluit de portal-instellingen aan op het nieuwe poort op een certificaat, zoals in de afbeelding.



**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-poort

Toegestane interfaces

certificaatgroep

Verificatiemethode

Goedgekeurde groepen

Volledig gekwalificeerde naam van de woonplaats (FQDN)

Inactiviteitstimer

Poorten die moeten worden gebruikt door het

De interfaces waarop ISE naar dit portaal mo

Het certificaatlabel dat wordt gebruikt voor he

Selecteer de reeks van de identiteitsopslag o

De gebruikersgroepen die toegang kunnen k

U kunt ook specifieke FQDN aan dit portaal g

De waarde definieert de ongebruikte tijdslimi

Opmerking: De configuratie van de identiteitsbron kan worden gecontroleerd onder **Beheer > Identity Management > Identity Bron Sequence**.

Stap 5. Configuratie van de logpagina-instellingen.

**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

Stap 6. Configuratie van de AUP-pagina-instellingen.

▼ 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)

Stap 7. U kunt ook post-inlogscanner toevoegen.

Stap 8. Specificeer onder Instellingen voor certificaatprovisioningportal de certificaatsjablonen die zijn toegestaan.

▼ Change Password Settings

Allow internal users to change their own passwords

▼ Certificate Provisioning Portal Settings

Certificate Templates: \*

Stap 9. Scrollt naar de bovenkant van de pagina en klik op **Opslaan** om de wijzigingen op te slaan.

Bovendien kan de portal verder worden aangepast door naar het **tabblad Portal pagina** te navigeren, waar de AUP-tekst, de post-inlogtekst en andere berichten naar wens kunnen worden gewijzigd.

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Als ISE correct is ingesteld voor het provisioneren van certificaten, kan een certificaat worden aangevraagd/gedownload van het ISE-provisioningportal met deze stappen.

Stap 1. Open de browser en blader naar een certificaatprovisioningportal FQDN zoals hierboven ingesteld of naar de URL van de certificatenprovisioningtest. U wordt naar het portaal terugverwezen, zoals in deze afbeelding wordt getoond:

**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](#)

Stap 2 . Meld u aan bij de gebruikersnaam en het wachtwoord.

Stap 3. Na succesvolle authenticatie accepteert u de AUP en wordt het verzonden naar de pagina met bepalingen voor certificaten.

Stap 4. De pagina voorzieningen voor certificaten biedt de functionaliteit om certificaten op drie manieren te downloaden:

- Enkelvoudig certificaat (zonder verzoek tot ondertekening van het certificaat)
- Enkelvoudig certificaat (met aanvraag voor ondertekening van certificaat)
- Bulkcertificaten

## Enkelvoudig certificaat genereren zonder Aanvraag voor certificaatsignalering

- Als u één certificaat zonder CSR wilt genereren, selecteert u de optie **Enkelvoudig certificaat genereren (zonder certificaataanvraag te ondertekenen)**.
- Voer een gemeenschappelijke naam in (CN).

Opmerking: De opgegeven GN moet overeenkomen met de gebruikersnaam van de aanvrager. De aanvrager verwijst naar de gebruikersnaam die gebruikt wordt om in te loggen naar het portal. Alleen gebruikers van Admin kunnen een certificaat maken voor een andere GN.

- Voer het MAC-adres in van het apparaat waarvoor het certificaat wordt gegenereerd.
- Kies de juiste certificaatsjabloon.
- Kies de gewenste bestandsindeling waarin het certificaat moet worden gedownload.
- Voer een certificaatwachtwoord in en klik op **Gopwekken**.
- Er wordt één certificaat gegenereerd en gedownload.

## 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

## Enkelvoudig certificaat genereren met certificaataanvraag

- Als u één certificaat zonder CSR wilt genereren, selecteert u de optie **Enkelvoudig certificaat genereren (zonder certificaataanvraag)**.
- Kopieer en plak de CSR-inhoud van het notebookbestand onder **Gegevens over certificaataanvraag**.
- Voer het MAC-adres in van het apparaat waarvoor het certificaat wordt gegenereerd.
- Kies de juiste certificaatsjabloon.
- Kies de gewenste bestandsindeling waarin het certificaat moet worden gedownload.
- Voer een certificaatwachtwoord in en klik op **Generate**.
- Er wordt één certificaat gegenereerd en gedownload.



### 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
WwoqAKVJ
yqJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABjsSToasXW
kyEIQT,8K5
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P50K
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0wTEMMmwn7Wbn5AgMBAAGgZ
TBjBqkqkG9wOB
CQ4xVBUUAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYXKY
BwkwEwYDYR0BAwwCgYIKwYBBQUHAWAwEwEQYJYIZIAyM4QqEB
BAQDAgZAMA0GCSqG
Sib3DQEBCwUAA4IBAQCeZSHBMu71Pv?H9dQHTxY5v5WCyQ7
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/Wdu3mfQICUPWPh8OzB
KA90V4uzV8Gif
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbjXN8fmS
n2foM6CDMH
J0ynRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ8K3HAx0+
xp2BY1uUYSEySHobb5RWAQhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1172xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/Wdu3mfQICUPWPh8OzB
KA90V4uzV8Gif
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbjXN8fmS
n2foM6CDMH
J0ynRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ8K3HAx0+
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: \*

\*\*\*\*\*

Generate

Reset

U kunt bulkcertificaten voor meerdere MAC-adressen genereren als u CSV-bestanden uploadt die GN- en MAC-adresveld bevatten.

Opmerking: De opgegeven GN moet overeenkomen met de gebruikersnaam van de aanvrager. De aanvrager verwijst naar de gebruikersnaam die gebruikt wordt om in te loggen naar het portal. Alleen gebruikers van Admin kunnen een certificaat maken voor een andere GN.

- Als u één certificaat zonder CSR wilt genereren, selecteert u de optie **Enkelvoudig certificaat genereren (met aanvraag voor certificaten ondertekenen)**.
- Upload het CSV-bestand voor bulkaanvraag.
- Kies de juiste certificaatsjabloon.
- Kies de gewenste bestandsindeling waarin het certificaat moet worden gedownload.
- Voer een certificaatwachtwoord in en klik op **Generate**.
- Een zip-bestand met certificaat wordt gegenereerd en gedownload.

The screenshot shows 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 the selected option 'Generate bulk certificates'.
- Upload CSV File: \***: A file upload field with a 'Choose File' button and the filename 'maclist.csv'. Below it 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...)' and an information icon.
- Certificate Password: \***: A password input field with masked characters '.....'.
- Confirm Password: \***: A password input field with masked characters '.....|'.
- At the bottom of the form are two buttons: 'Generate' (highlighted in blue) and 'Reset'.

Below the form is a small blue link labeled 'Help'.

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.