ISE 2.0 certificaatprovisioningportal configureren

Inhoud

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)

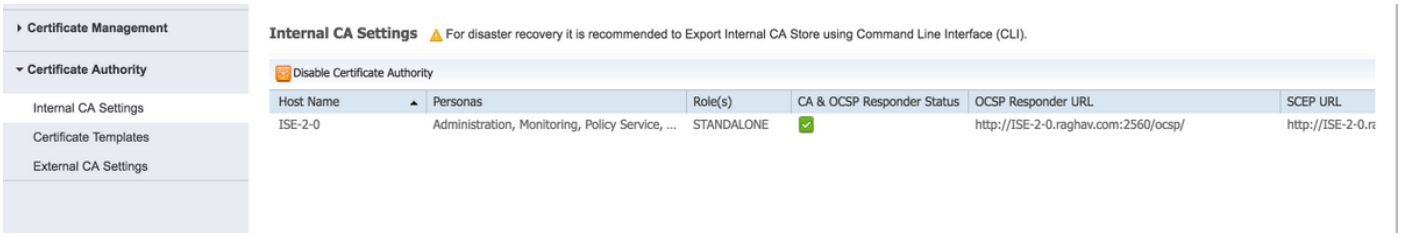
> Opmerking: ISE interne CA is ontworpen om functies te ondersteunen die certificaten zoals BYOD gebruiken en dus zijn de mogelijkheden beperkt. Het gebruik van ISE als Enterprise CA wordt niet aanbevolen door Cisco.

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.

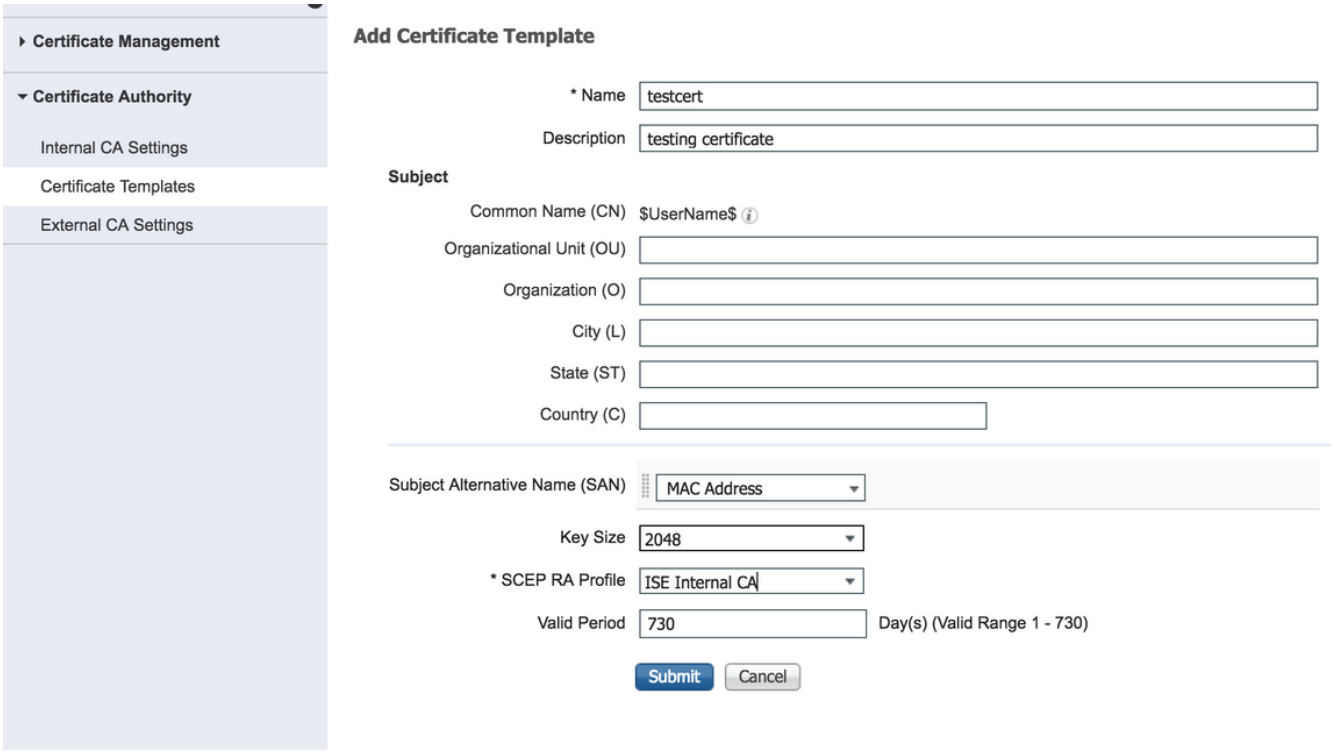
Stap 1.Op ISE GUI, navigeer naar **Administratie > Systeem > Certificaten > certificaatinstantie > Interne CA** en om de interne CA-instellingen op het ISE-knooppunt **in** te schakelen, klikt u op

certificaatinstantie inschakelen.

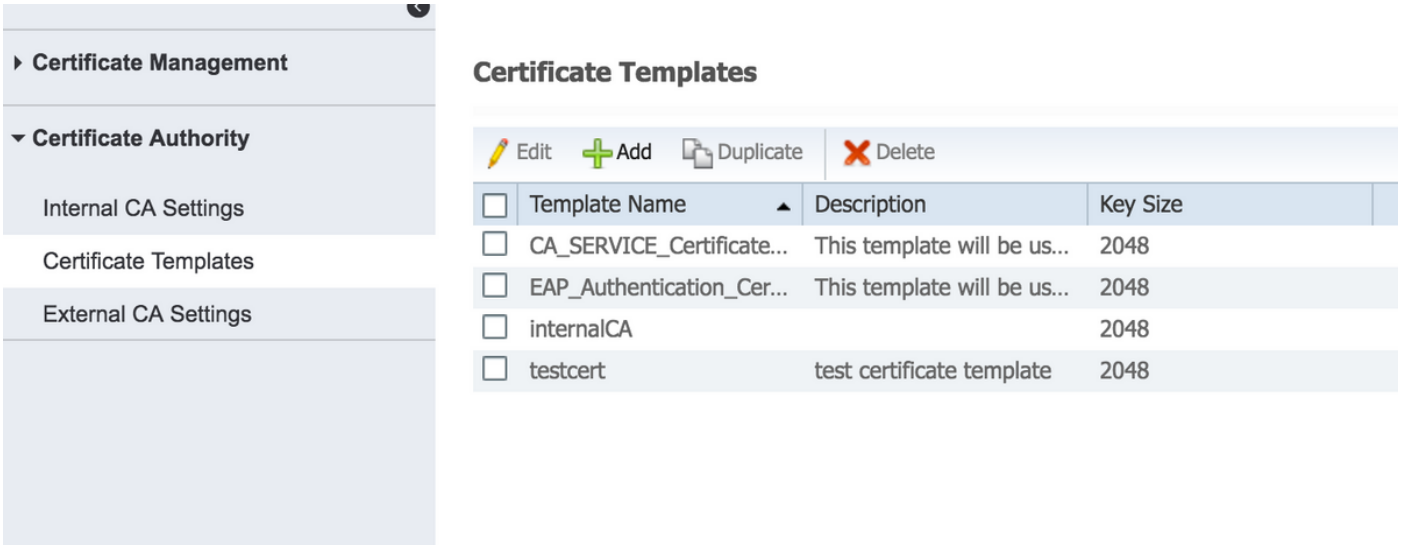


Stap 2. Maak certificaatsjablonen onder **Beheer > Systeem > Certificaten > certificaatsjablonen > Toevoegen**.

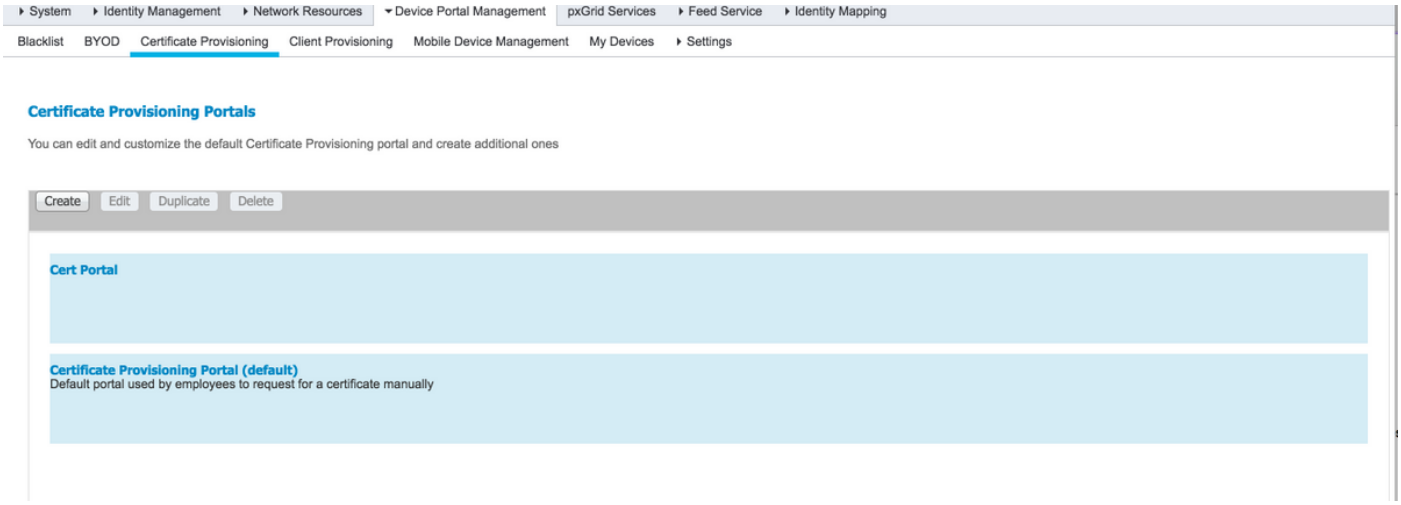
Voer de gegevens in volgens de vereisten en klik op **Indienen,** zoals in deze afbeelding wordt weergegeven.



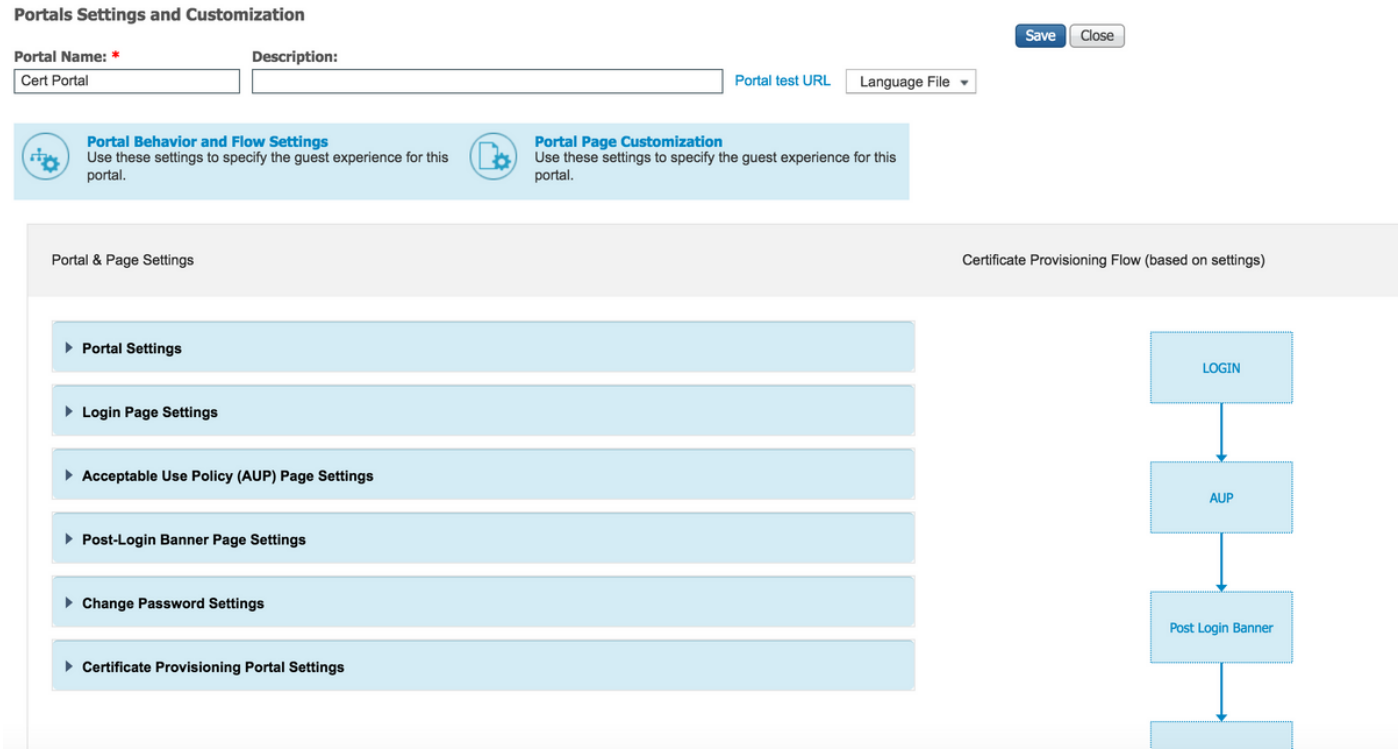
Opmerking: U kunt de lijst met gedefinieerde certificaatsjablonen zien onder **Beheer > Systeem > Certificaten > certificaatsjablonen** zoals in deze afbeelding weergegeven.

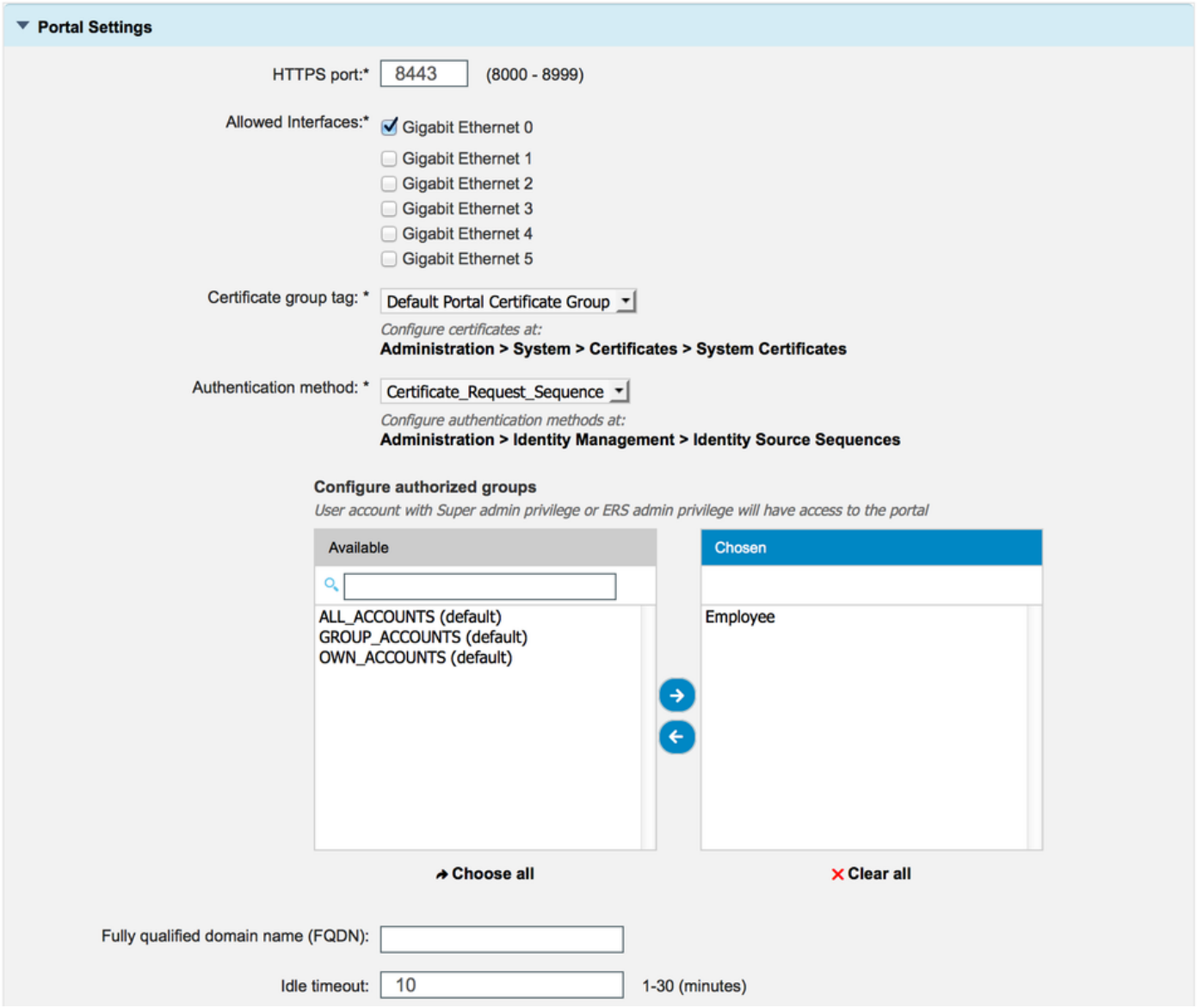


Stap 3. Om het ISE-provisioningportal te configureren **kunt u** navigeren naar **Beheer > Apparaatportal > certificaatprovisioning >** Aanmaken zoals in de afbeelding:



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

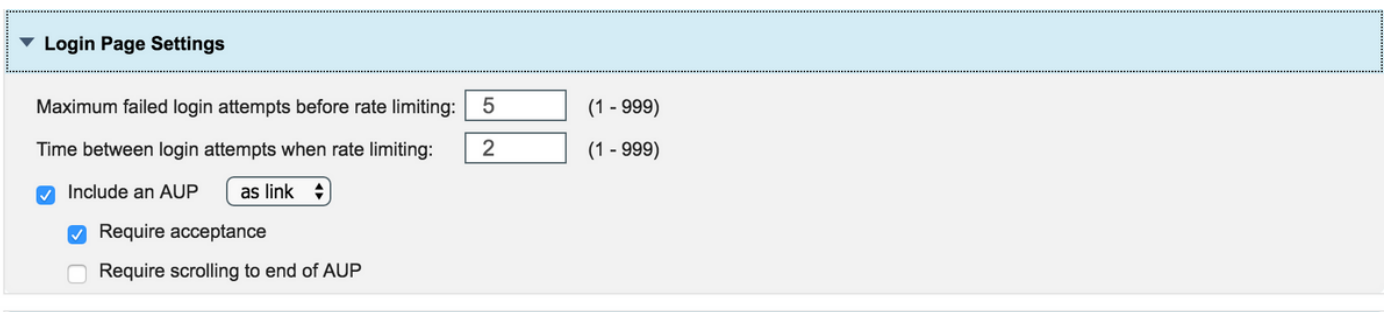




HTTPS-poort	Poorten die moeten worden gebruikt door het
Toegestane interfaces	De interfaces waarop ISE naar dit portaal mo
certificaatgroep	Het certificaatlabel dat wordt gebruikt voor he
Verificatiemethode	Selecteer de reeks van de identiteitsopslag d
Goedgekeurde groepen	De gebruikersgroepen die toegang kunnen kr
Volledig gekwalificeerde naam van de woonplaats (FQDN)	U kunt ook specifieke FQDN aan dit portaal g
Inactiviteitstimer	De waarde definieert de ongebruikte tijdslimie

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

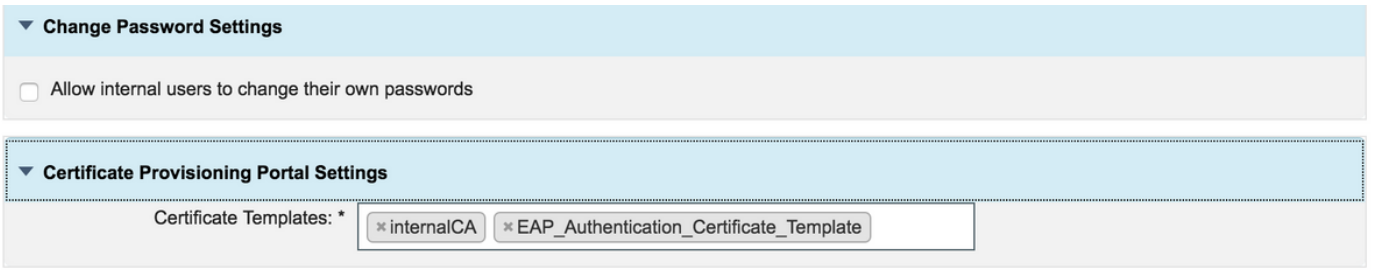
Stap 5. Configuratie van de logpagina-instellingen.



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

Stap 7. U kunt ook post-inlogscanner toevoegen.

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



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

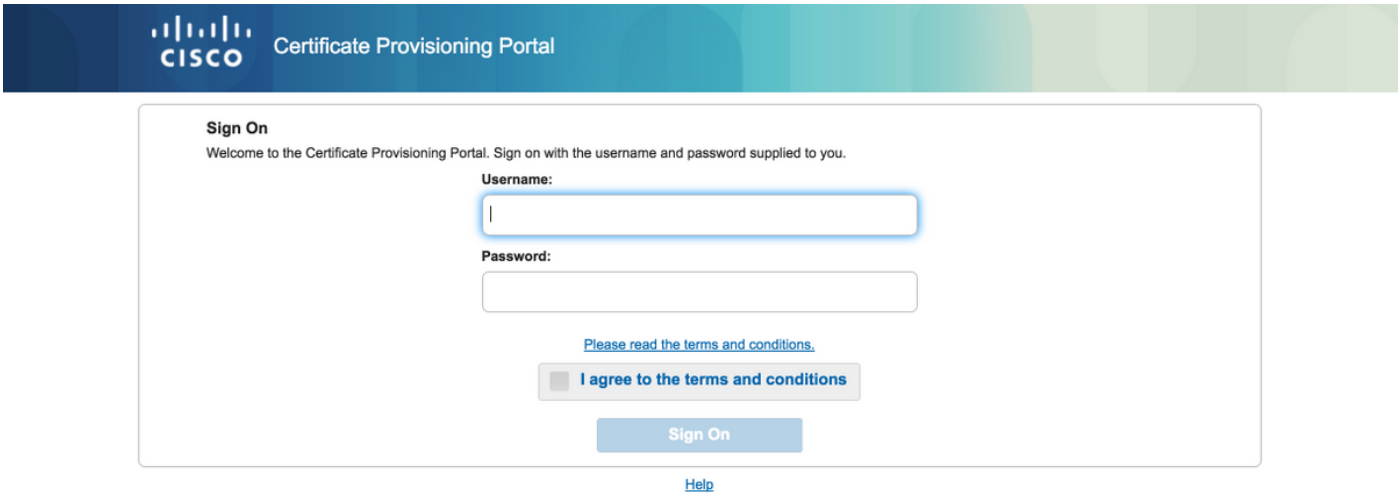
Bovendien kan de portal verder worden aangepast door naar het **tabblad** Portal **pagina** te navigeren, waar de AUP-tekst, de post-inlogtekst en andere berichten naar wens kunnen worden gewijzigd.

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:



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.

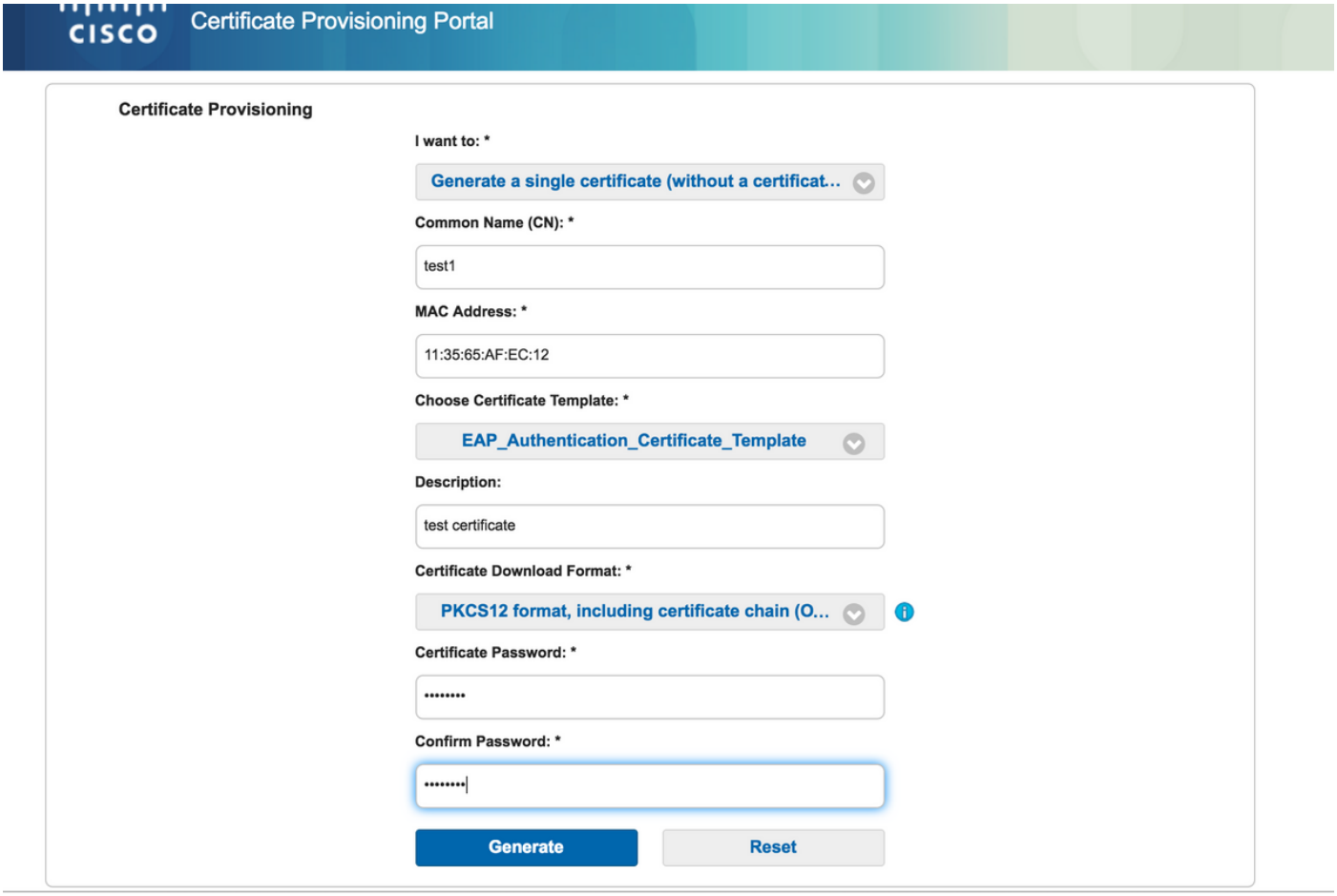
- Voer het MAC-adres in van het apparaat waarvoor het certificaat wordt gegenereerd.

- Kies de juiste certificaatsjabloon.

- Kies de gewenste bestandsindeling waarin het certificaat moet worden gedownload.

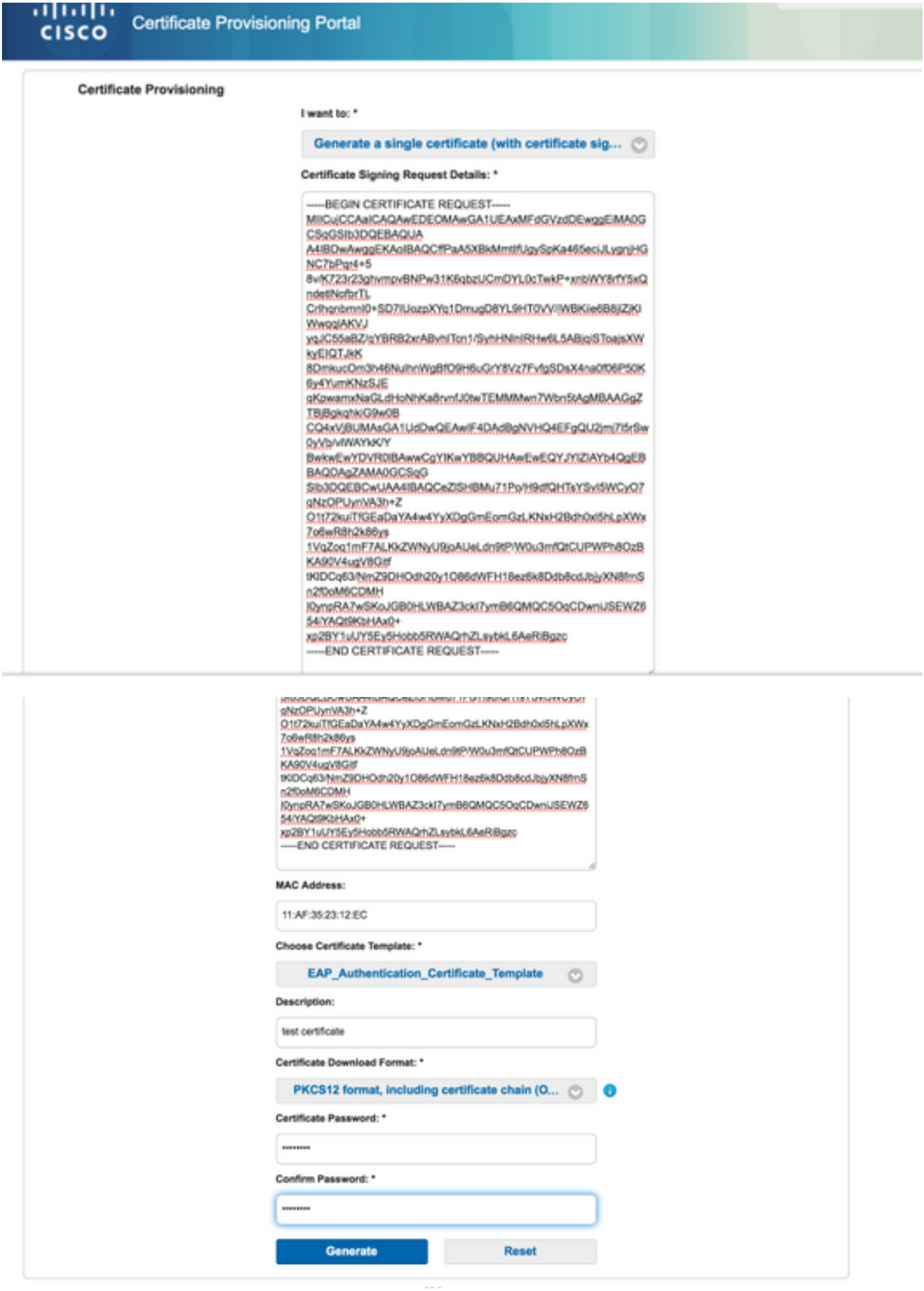
- Voer een certificaatwachtwoord in en klik op **Gopwekken.**

- Er wordt één certificaat gegenereerd en gedownload.



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.

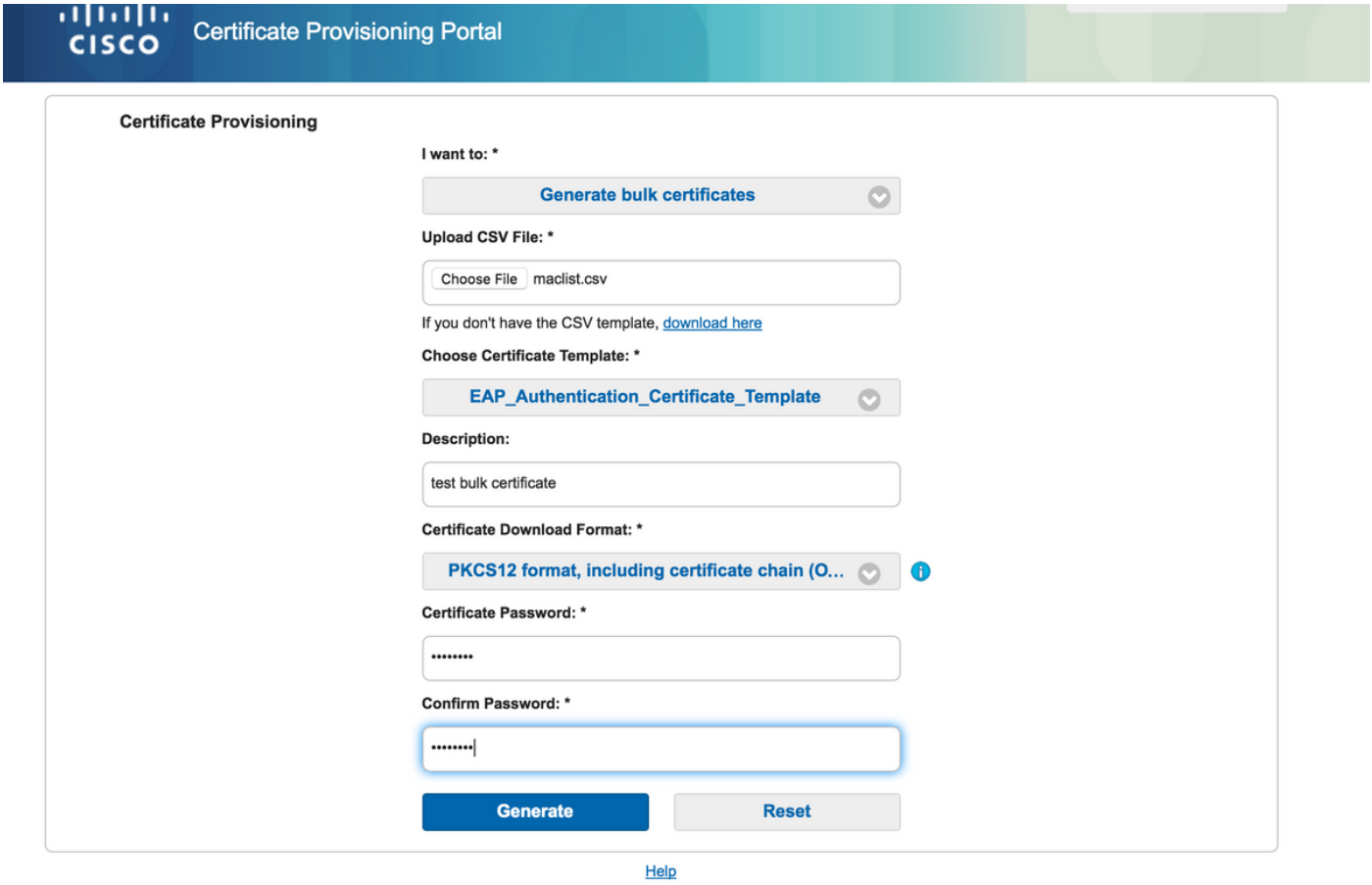


Bulkcertificaten genereren

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.



Problemen oplossen

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