

Configurer le portail de provisionnement de certificat d'ISE 2.0

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Limites](#)

[Configuration](#)

[Vérification](#)

[Générer un certificat unique sans demande de signature de certificat](#)

[Générer un certificat unique avec une demande de signature de certificat](#)

[Générer des certificats en masse](#)

[Dépannage](#)

Introduction

Ce document décrit la configuration et la fonctionnalité du portail de provisionnement de certificat d'ISE.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Serveurs de certificats et d'autorité de certification (CA).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le portail d'approvisionnement de certificats est une nouvelle fonctionnalité introduite dans ISE 2.0 qui peut être utilisée par les périphériques finaux pour inscrire et télécharger des certificats d'identité à partir du serveur. Il émet des certificats aux périphériques qui ne peuvent pas passer par le flux d'intégration.

Par exemple, les appareils tels que les terminaux de point de vente ne peuvent pas suivre le flux BYOD (Bring Your Own Device) et doivent recevoir des certificats manuellement.

Le portail d'approvisionnement des certificats permet à un groupe privilégié d'utilisateurs de télécharger une demande de certificat (CSR) pour ces périphériques ; générez des paires de clés, puis téléchargez le certificat.

Sur ISE, vous pouvez créer des modèles de certificat modifiés et les utilisateurs finaux peuvent sélectionner un modèle de certificat approprié pour télécharger un certificat. Pour ces certificats, ISE agit en tant que serveur d'autorité de certification (AC) et nous pouvons obtenir le certificat signé par l'AC interne ISE.

Le portail d'approvisionnement de certificats ISE 2.0 prend en charge le téléchargement de certificats dans les formats suivants :

- format PKCS12 (y compris la chaîne de certificats); un fichier pour la chaîne de certificats et la clé)
- Format PKCS12 (un fichier pour le certificat et la clé)
- Certificat (chaîne comprise) au format PEM (Privacy Enhanced Electronic Mail), clé au format PEM PKCS8.
- Certificat au format PEM, clé au format PEM PKCS8 :

Limites

Actuellement, ISE ne prend en charge que ces extensions dans un CSR pour signer un certificat.

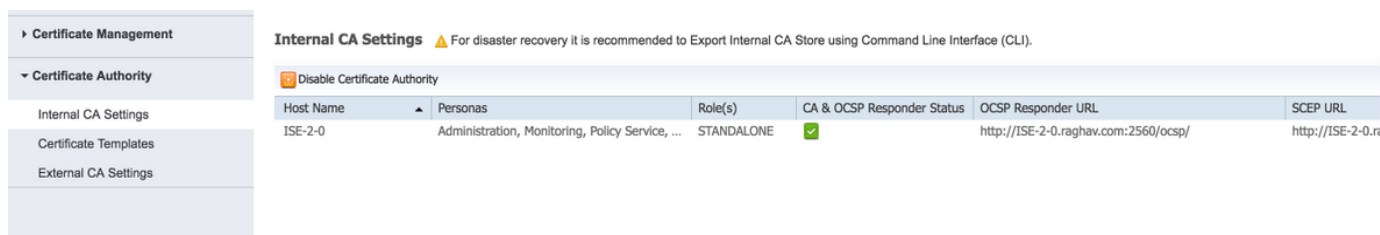
- subjectDirectoryAttributes
- subjectAlternativeName
- keyUsage
- subjectKeyIdentifier
- auditIdentity
- extendedKeyUsage
- CERT_TEMPLATE_OID (OID personnalisé pour spécifier le modèle généralement utilisé dans le flux BYOD)

Note: La CA interne ISE est conçue pour prendre en charge les fonctionnalités qui utilisent des certificats tels que le BYOD et donc les fonctionnalités sont limitées. L'utilisation d'ISE en tant que CA d'entreprise n'est pas recommandée par Cisco.

Configuration

Afin d'utiliser la fonctionnalité d'approvisionnement de certificats dans le réseau, le service d'autorité de certification interne ISE doit être activé et un portail d'approvisionnement de certificats doit être configuré.

Étape 1. Sur l'interface graphique de ISE, accédez à **Administration > System > Certificates > Certificate Authority > Internal CA** et pour activer les paramètres d'autorité de certification interne sur le noeud ISE, cliquez sur **Enable Certificate Authority**.



Étape 2. Créez des modèles de certificat sous **Administration > Système > Certificats > Modèles de certificat > Ajouter**.

Entrez les détails selon les besoins et cliquez sur **Soumettre**, comme indiqué dans cette image.

Add Certificate Template

* Name: testcert
Description: testing certificate

Subject

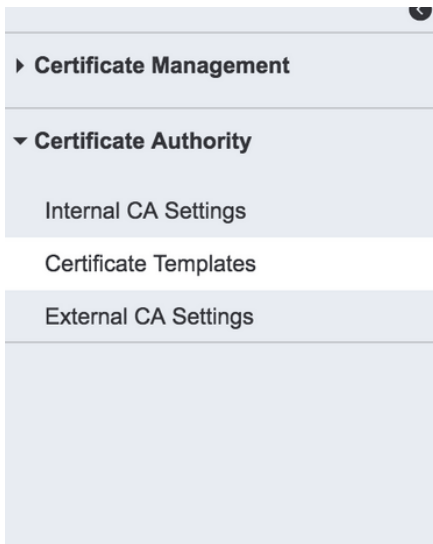
Common Name (CN): \$UserName\$ ⓘ
Organizational Unit (OU):
Organization (O):
City (L):
State (ST):
Country (C):

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

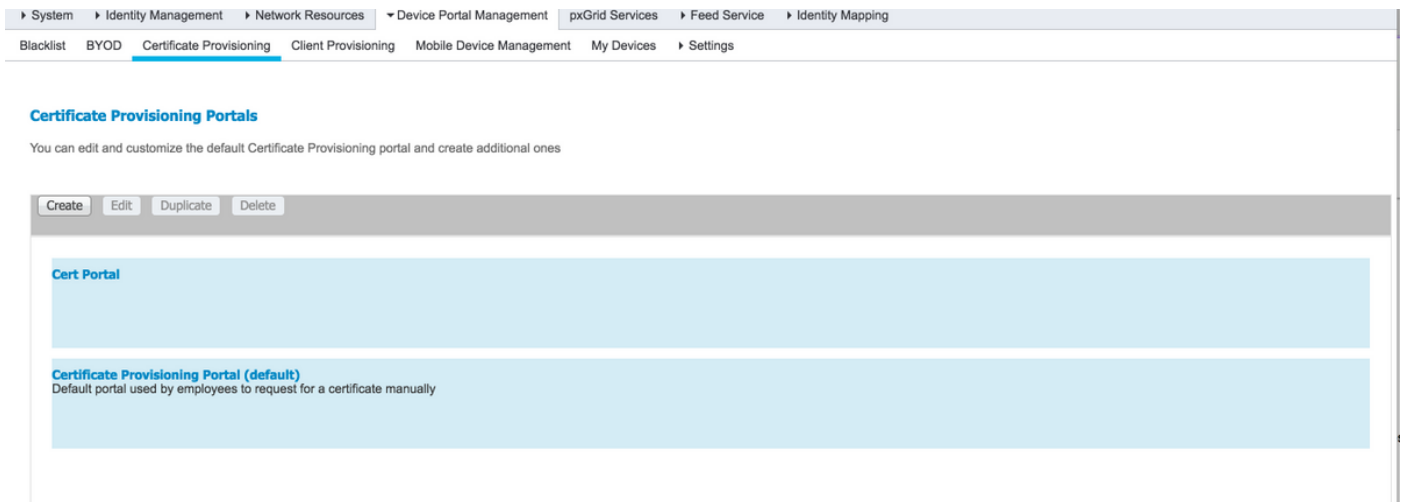
Note: Vous pouvez voir la liste des modèles de certificat créés sous **Administration > Système > Certificats > Modèles de certificat** comme indiqué dans cette image.



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

Étape 3. Afin de configurer le portail de mise en service des certificats ISE, accédez à **Administration > Device Portal Management > Certificate Provisioning > Create**, comme indiqué dans l'image :



Étape 4. Sur le nouveau portail de certificats, développez les paramètres du portail, comme illustré dans l'image.

Portals Settings and Customization

Save Close

Portal Name: *

Description:

Cert Portal

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

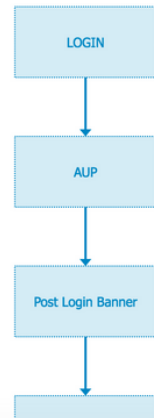
▶ Login Page Settings

▶ 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
<input type="text"/>
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Chosen
Employee



➔ Choose all

✗ Clear all

Fully qualified domain name (FQDN):

Idle timeout:

1-30 (minutes)

Port HTTPS
Interfaces autorisées

Port qui doit être utilisé par le portail d'approvisionnement des certificats
Les interfaces sur lesquelles ISE doit écouter ce portail.

Balise de groupe de certificats

Méthode d'authentification

Groupes autorisés

Nom de domaine complet (FQDN)

Délai d'inactivité

Balise de certificat à utiliser pour le portail d'approvisionnement de ce

Sélectionnez la séquence de magasin d'identités qui authentifie la co

L'ensemble des utilisateurs qui peuvent accéder au portail d'approvisi

Vous pouvez également attribuer un nom de domaine complet spécifi

La valeur définit le délai d'inactivité du portail.

Note: La configuration de la source d'identité peut être vérifiée sous **Administration > Identity Management > Identity Source Sequence**.

Étape 5. Configurez les paramètres de la page de connexion.

▼ **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

Étape 6. Configurez les paramètres de la page 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)

Étape 7. Vous pouvez également ajouter une bannière de post-connexion.

Étape 8. Sous Certificate Provisioning portal settings, spécifiez les modèles de certificat autorisés.

▼ **Change Password Settings**

Allow internal users to change their own passwords

▼ **Certificate Provisioning Portal Settings**

Certificate Templates: *

Étape 9. Faites défiler la page jusqu'en haut et cliquez sur **Enregistrer** pour enregistrer les modifications.

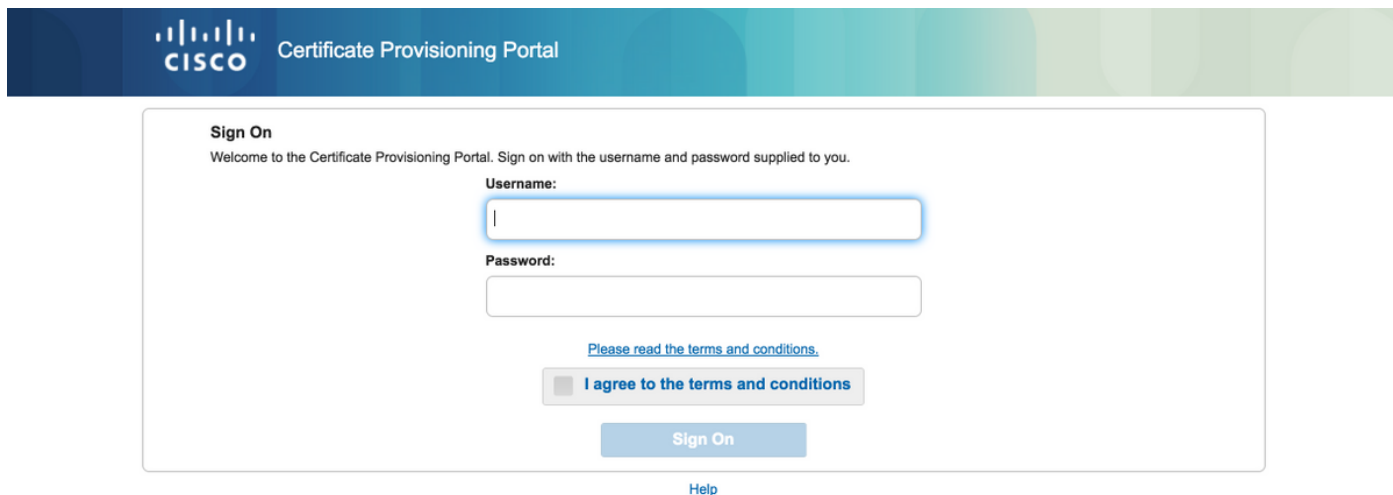
En outre, le portail peut être personnalisé en accédant à l'onglet **Personnalisation de la page du portail** où le texte AUP, le texte de la bannière de post-connexion et d'autres messages peuvent être modifiés selon les besoins.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Si ISE est configuré correctement pour le provisionnement des certificats, un certificat peut être demandé/téléchargé à partir du portail de provisionnement des certificats ISE en procédant comme suit.

Étape 1. Ouvrez le navigateur et accédez au nom de domaine complet du portail d'approvisionnement des certificats tel que configuré ci-dessus ou à l'URL du test d'approvisionnement des certificats. Vous êtes redirigé vers le portail, comme l'illustre cette image :



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 page, there is a "Help" link.

Étape 2. Connectez-vous avec le nom d'utilisateur et le mot de passe.

Étape 3. Une fois l'authentification réussie, acceptez AUP et elle s'affiche sur la page d'approvisionnement des certificats.

Étape 4. La page d'approvisionnement des certificats fournit la fonctionnalité de téléchargement des certificats de trois manières :

- Certificat unique (sans demande de signature de certificat)
- Certificat unique (avec demande de signature de certificat)
- Certificats en bloc

Générer un certificat unique sans demande de signature de certificat

- Afin de générer un certificat unique sans CSR, sélectionnez l'option **Générer un certificat unique (sans demande de signature de certificat)**.
- Saisissez Common Name (CN).

Note: Le CN donné doit correspondre au nom d'utilisateur du demandeur. Le demandeur fait référence au nom d'utilisateur utilisé pour se connecter au portail. Seuls les utilisateurs Admin peuvent créer un certificat pour un autre CN.

- Saisissez l'adresse MAC du périphérique pour lequel le certificat est généré.

- Sélectionnez le modèle de certificat approprié.
- Choisissez le format souhaité pour le téléchargement du certificat.
- Entrez un mot de passe de certificat et cliquez sur **Ggénérer**.
- Un seul certificat est généré et téléchargé avec succès.

CISCO Certificate Provisioning Portal

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

Générer un certificat unique avec une demande de signature de certificat

- Afin de générer un certificat unique sans CSR, sélectionnez l'option **Générer un certificat unique (avec demande de signature de certificat)**.
- Copiez et collez le contenu CSR à partir du fichier bloc-notes sous **Détails de la demande de signature de certificat**.
- Saisissez l'adresse MAC du périphérique pour lequel le certificat est généré.
- Sélectionnez le modèle de certificat approprié.
- Choisissez le format souhaité pour le téléchargement du certificat.
- Entrez un mot de passe de certificat et cliquez sur **Generate**.

- Un seul certificat sera généré et téléchargé avec succès.

CISCO Certificate Provisioning Portal

Certificate Provisioning

I want to: *

[Generate a single certificate \(with certificate sig...](#)

Certificate Signing Request Details: *

```
-----BEGIN CERTIFICATE REQUEST-----
MII/CuCCAa/CAQAwEDEOMAwwGA1UEAwMFdGVzdDEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfPaA5XBkMmrfUjz/SrKa465ecULygnHG
NC7bPqt4+5
8vIK723r23qhympvBNPw31K6qzUCmDYLOcTwp+xbWY8rfY5xQ
ndetNofbrTL
Crlhrnbnj0+SD7IUozpXYe1DmugD8YL9HT0Vv//WBKie6B8jZKI
WwqgAKYJ
yqJC55eBZ/yYBRB2rAbvhlTon1/SyHNeIRHw6L5ABqjSToasXW
kyEIQT,jKk
8DmkucOm3h46NulhrWpBfD9H6uGrY8Yz7FvqSDsX4na0f6P5OK
6y4YmKNzSJE
qKowamxNaGLdHcNhKa8nmfJ0twTEMMWnTWbn5AgMBAAGz
TBJBqkqhkG9wOB
CO4xVBUmAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2im7i5rSw
dyYb/vWAYKQY
BwkwEwYDVR0BAwwCoYIKwYBBQUHAwEwE/QYJYIZIAyb4QqEB
BAQDAgZAMA0GC5qG
Sib3DQEBCwUAA4IBAQCeZShiBMu71PwH9dQHtsYSvISWcyO7
qNzOPUynWA3t+Z
Q1172kuITIGeEaDaYA4w4YyXDGmEomGzLKNxH2Bdh0x5HLpXWx
7o6wR8h2k88ys
1VoZoc1mF7ALKkZWYyU9pAUkLdn9P/Wdu3mfQcUPWPh8QzB
KA90V4ugV8Qif
KDCq63NnmZ9DHOdh20y1Q86dWFH16ez6k8Ddb6cdJbyXN8fmS
n2f0m6CDMH
lQynpRA7wSKoJGB0HLWBAZ3ckl7ymB6QMOC5OqCDwnUSEWZ6
54YAQ69GhAx0+
xp2BY1uUYSEyShobb5RWaQhZLaytkL6AeR/Bgzo
-----END CERTIFICATE REQUEST-----
```

-----BEGIN CERTIFICATE REQUEST-----
gNzCPJynVA3h+Z
Q1f72kuITIGEaDaYAfw4YyXDqGmEomGzLKNdH2BdhOx5HLPXWk
ZofwR8hZk86ys
1VsZoa1mF7ALkKzWNYU9oAUel,dn9P*W0uJmQtCUPWPh8OzB
KA90V4uqV9Gif
tK0Cq63NmZjDHOdh20y1O86dWFH18ezFk8Ddt8codJbyXN8mS
n26oM9CDMH
J0ypRA7w5KoJGB0HLWBAZ3ckJ7ymB6QMQCSOzCDwniJSEWZ6
54/YAQ9KzHAxQ+
xpZ8Y1uJZYSEyHobb6RWAQrhZLsytkL6AeRBozc
-----END CERTIFICATE REQUEST-----

MAC Address:

Choose Certificate Template: *

Description:

Certificate Download Format: *

Certificate Password: *

Confirm Password: *

Générer des certificats en masse

Vous pouvez générer des certificats en bloc pour plusieurs adresses MAC si vous téléchargez des fichiers CSV qui contiennent des champs d'adresse CN et MAC.

Note: Le CN donné doit correspondre au nom d'utilisateur du demandeur. Le demandeur fait référence au nom d'utilisateur utilisé pour se connecter au portail. Seuls les utilisateurs Admin peuvent créer un certificat pour un autre CN.

- Afin de générer un certificat unique sans CSR, sélectionnez l'option **Générer un certificat unique (avec demande de signature de certificat)**.
- Téléchargez le fichier csv pour une demande en bloc.
- Sélectionnez le modèle de certificat approprié.
- Choisissez le format souhaité pour le téléchargement du certificat.
- Entrez un mot de passe de certificat et cliquez sur **Generate**.
- Un fichier zip de certificat en bloc est généré et téléchargé.

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](#)

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.