

# Konfigurieren des ISE 2.0-Zertifikatsbereitstellungsportals

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Einschränkungen](#)

[Konfigurieren](#)

[Überprüfen](#)

[Generieren eines einzelnen Zertifikats ohne Zertifikatssignierungsanforderung](#)

[Generieren eines einzelnen Zertifikats mit Zertifikatssignierungsanforderung](#)

[Generieren von Massenzertifikaten](#)

[Fehlerbehebung](#)

## Einführung

Dieses Dokument beschreibt die Konfiguration und die Funktionen des ISE-Portals (Identity Services Engine) für die Zertifikatsbereitstellung.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- ISE
- Zertifizierungsstellen- und Zertifizierungsstellen-Server (Certificate Authority, CA).

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Identity Service Engine 2.0
- Windows 7 - PC

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Hintergrundinformationen

Das Portal für die Zertifikatsbereitstellung ist eine neue Funktion, die in ISE 2.0 eingeführt wurde und von Endgeräten zum Registrieren und Herunterladen von Identitätszertifikaten vom Server verwendet werden kann. Es werden Zertifikate für Geräte ausgegeben, die den Onboarding-Fluss nicht durchlaufen können.

Geräte wie Point-of-Sale-Terminals können beispielsweise nicht dem BYOD-Fluss (Bring Your Own Device) unterzogen werden und müssen manuell Zertifikate ausgestellt werden.

Über das Certificate Provisioning Portal können privilegierte Benutzer eine Zertifikatsanforderung (CSR) für diese Geräte hochladen. Generieren Sie Schlüsselpaare, und laden Sie dann das Zertifikat herunter.

Auf der ISE können Sie modifizierte Zertifikatsvorlagen erstellen, und Endbenutzer können eine geeignete Zertifikatsvorlage zum Herunterladen eines Zertifikats auswählen. Für diese Zertifikate fungiert die ISE als Zertifizierungsstellen-Server (Certificate Authority, CA), und das Zertifikat kann von der internen ISE-Zertifizierungsstelle signiert werden.

Das ISE 2.0-Portal für die Zertifikatsbereitstellung unterstützt den Zertifikatsdownload in folgenden Formaten:

- PKCS12-Format (einschließlich Zertifikatskette) eine Datei für Zertifikatskette und Schlüssel)
- PKCS12-Format (eine Datei für Zertifikat und Schlüssel)
- Zertifikat (einschließlich Kette) im Privacy Enhanced Electronic Mail (PEM)-Format, Schlüssel im PKCS8 PEM-Format.
- Zertifikat im PEM-Format, Schlüssel im PKCS8-PEM-Format:

## Einschränkungen

Derzeit unterstützt die ISE nur diese Erweiterungen in einem CSR, um ein Zertifikat zu signieren.

- subjectDirectoryAttributes
- subjectAlternativeName
- Schlüsselverwendung
- subjectKeyIdentifier
- AuditIdentity
- ExtendedKeyUsage
- CERT\_TEMPLATE\_OID (Dies ist eine benutzerdefinierte OID, mit der die Vorlage angegeben wird, die normalerweise im BYOD-Fluss verwendet wird)

**Hinweis:** Die interne Zertifizierungsstelle der ISE unterstützt Funktionen, die Zertifikate wie BYOD verwenden. Daher sind die Funktionen begrenzt. Die Verwendung der ISE als Enterprise CA wird von Cisco nicht empfohlen.

## Konfigurieren

Um die Funktion der Zertifikatsbereitstellung im Netzwerk nutzen zu können, muss der interne

ISE-Zertifizierungsstellen-Service aktiviert und ein Portal für die Zertifikatsbereitstellung konfiguriert werden.

Schritt 1: Navigieren Sie in der ISE-GUI zu **Administration > System > Certificates > Certificate Authority > Internal CA**, und aktivieren Sie die internen CA-Einstellungen auf dem ISE-Knoten, und klicken Sie auf **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	<input checked="" type="checkbox"/>	http://ISE-2-0.raghav.com:2560/ocsp/	http://ISE-2-0.r...

Schritt 2: Erstellen Sie Zertifikatsvorlagen unter **Administration > System > Certificates > Certificate Templates > Add**.

Geben Sie die Details gemäß den Anforderungen ein, und klicken Sie auf **Senden**, wie in diesem Bild gezeigt.

**Add Certificate Template**

\* Name

Description

**Subject**

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

---

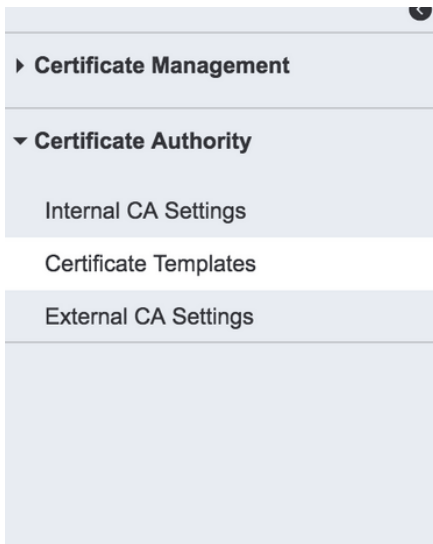
Subject Alternative Name (SAN)

Key Size

\* SCEP RA Profile

Valid Period  Day(s) (Valid Range 1 - 730)

**Hinweis:** Sie können die Liste der erstellten Zertifikatsvorlagen unter **Administration > System > Certificates > Certificate Templates (Verwaltung > System > Zertifikate > Zertifikatsvorlagen)** anzeigen, wie in diesem Bild gezeigt.

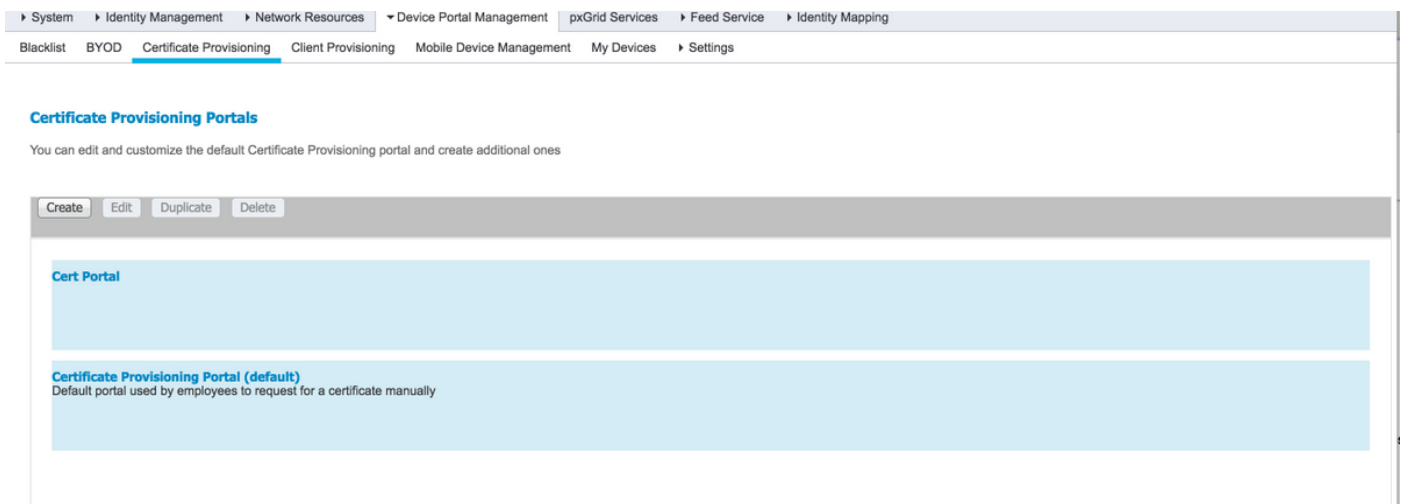


## Certificate Templates

✎ Edit   + Add   📄 Duplicate   ✖ Delete

<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

Schritt 3: Um das ISE-Portal für die Zertifikatsbereitstellung zu konfigurieren, gehen Sie zu **Administration > Device Portal Management > Certificate Provisioning > Create (Verwaltung > Geräteportal-Management > Zertifikatsbereitstellung > Erstellen)**, wie im folgenden Bild gezeigt:



Schritt 4: Erweitern Sie im neuen Zertifikatsportal die Portaleinstellungen, wie im Bild gezeigt.

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)

HTTPS-Port  
Zugelassene Schnittstellen

Port, der vom Portal für die Zertifikatsbereitstellung für HTTPS v  
Die Schnittstellen, auf denen die ISE auf dieses Portal hören so

Zertifikatgruppen-Tag	Das Zertifikat-Tag, das für das Zertifikatsbereitstellungsportal v
Authentifizierungsmethode	Wählen Sie die Identitätsspeichersequenz aus, die die Anmelde
Autorisierte Gruppen	Die Anzahl der Benutzer, die auf das Portal für die Zertifikatsbe
Vollqualifizierter Domänenname (FQDN)	Sie können diesem Portal auch einen bestimmten FQDN zuwei
Leerlaufzeitüberschreitung	Der Wert definiert das Leerlaufzeitlimit für das Portal.

**Hinweis:** Die Konfiguration der Identitätsquelle kann unter **Administration > Identity Management > Identity Source Sequence** überprüft werden.

### Schritt 5: Konfigurieren der Einstellungen für die Anmeldeseite

**▼ 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

### Schritt 6: Konfigurieren der Einstellungen für die AUP-Seite

**▼ 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)

### Schritt 7: Sie können auch Banner nach der Anmeldung hinzufügen.

### Schritt 8: Geben Sie unter Einstellungen für das Zertifikatsbereitstellungsportal die zulässigen Zertifikatsvorlagen an.

**▼ Change Password Settings**

Allow internal users to change their own passwords

**▼ Certificate Provisioning Portal Settings**

Certificate Templates: \*

### Schritt 9: Navigieren Sie zum oberen Seitenrand, und klicken Sie auf **Speichern**, um die Änderungen zu speichern.

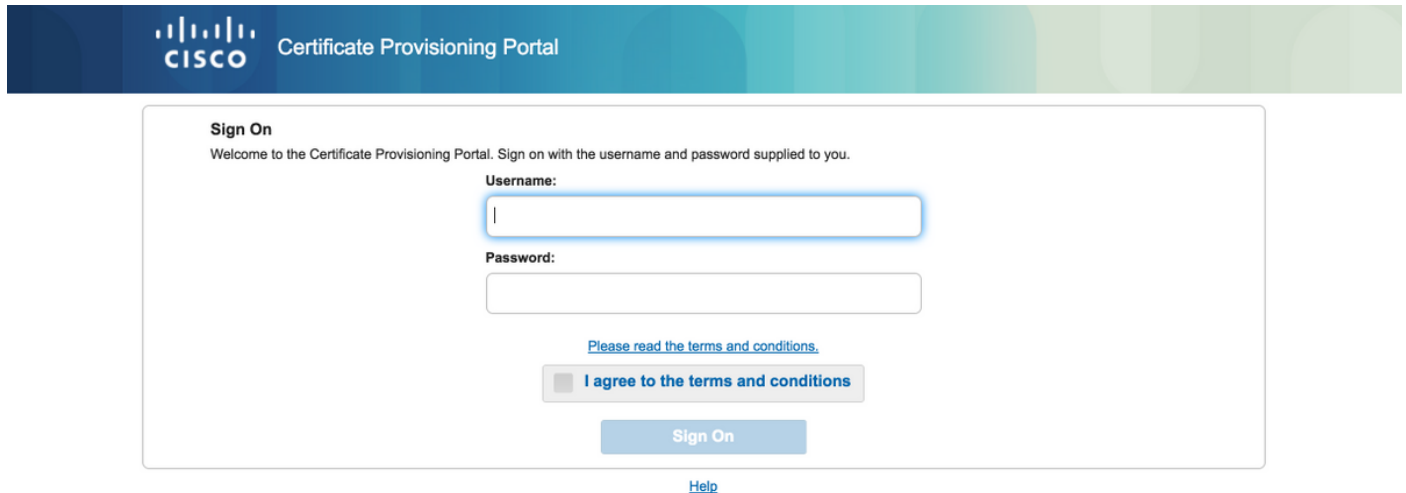
Zusätzlich kann das Portal durch Navigieren zur Registerkarte **für die Anpassung der Portalseite** weiter angepasst werden, auf der der AUP-Text, der Text des Anmeldebanners und andere Nachrichten entsprechend den Anforderungen geändert werden können.

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn die ISE für die Zertifikatsbereitstellung korrekt konfiguriert ist, kann ein Zertifikat mit diesen Schritten vom ISE-Zertifikatsbereitstellungsportal angefordert/heruntergeladen werden.

Schritt 1: Öffnen Sie den Browser, und rufen Sie das Portal für die Zertifikatsbereitstellung FQDN (wie oben konfiguriert) oder die URL für den Test zur Zertifikatsbereitstellung auf. Sie werden zum Portal umgeleitet, wie in diesem Bild gezeigt:



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 is titled "Sign On" and includes a welcome message: "Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you." There are two input fields: "Username:" and "Password:". Below the password field, there is a link "Please read the terms and conditions." and a checkbox labeled "I agree to the terms and conditions". A "Sign On" button is located at the bottom of the form. A "Help" link is positioned below the "Sign On" button.

Schritt 2: Melden Sie sich mit Benutzernamen und Kennwort an.

Schritt 3: Akzeptieren Sie nach erfolgreicher Authentifizierung AUP, und es wird die Seite für die Zertifikatsbereitstellung angezeigt.

Schritt 4: Auf der Seite für die Zertifikatsbereitstellung stehen drei Möglichkeiten zum Herunterladen von Zertifikaten zur Verfügung:

- Einzelzertifikat (ohne Anforderung zur Signierung des Zertifikats)
- Einzelnes Zertifikat (mit Anforderung für Zertifikatssignierung)
- Massenzertifikate

## Generieren eines einzelnen Zertifikats ohne Zertifikatssignierungsanforderung

- Um ein einzelnes Zertifikat ohne CSR zu generieren, wählen Sie die Option **Einzelzertifikat generieren (ohne Zertifikatssignierungsanfrage)** aus.
- Geben Sie den allgemeinen Namen (CN) ein.

**Hinweis:** Die angegebene CN muss mit dem Benutzernamen des Antragstellers übereinstimmen. Der Antragsteller bezieht sich auf den Benutzernamen, der für die Anmeldung beim Portal verwendet wird. Nur Admin-Benutzer können ein Zertifikat für einen anderen CN erstellen.

- Geben Sie die MAC-Adresse des Geräts ein, für das das Zertifikat generiert wird.

- Wählen Sie die entsprechende Zertifikatsvorlage aus.
- Wählen Sie das gewünschte Format aus, in dem das Zertifikat heruntergeladen werden soll.
- Geben Sie ein Zertifikatskennwort ein, und klicken Sie auf **G.Generieren**.
- Es wird ein einzelnes Zertifikat erstellt und erfolgreich heruntergeladen.

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

## Generieren eines einzelnen Zertifikats mit Zertifikatssignierungsanforderung

- Um ein einzelnes Zertifikat ohne CSR zu generieren, wählen Sie die Option **Einzelzertifikat (mit Zertifikatssignierungsanfrage)** erstellen.
- Kopieren Sie den CSR-Inhalt aus der Notizblock-Datei unter **Details** der **Zertifikatsanforderung**.
- Geben Sie die MAC-Adresse des Geräts ein, für das das Zertifikat generiert wird.
- Wählen Sie die entsprechende Zertifikatsvorlage aus.
- Wählen Sie das gewünschte Format aus, in dem das Zertifikat heruntergeladen werden soll.
- Geben Sie ein Zertifikatskennwort ein, und klicken Sie auf **Generate (Generieren)**.



- Es wird ein einziges Zertifikat erstellt und erfolgreich heruntergeladen.

**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
NC7bPqz4+5
8vK723r23qhympvBNPw31K6qzUCmDYLOcTwp+xnbWY8rfY5xQ
ndetNofbrTL
CrIhrnbmJ0+SD7IUozpXYe1DmugD8YL9HT0VVW/BKie6B8JZKI
WwqgAKYJ
yqJC55eBZ/yYBRB2rAbvhlTon1/SyHNeIRHw6L5ABqjSToasXW
kyEIQT,JkK
8DmkucOm3h46NulhrWpBfD9H6uGrY8Yz7FvqSDsX4na0f6P5OK
6y4YmKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0twTEMMWnTWbn5AgMBAAGz
TBJBqkqhkG9wOB
CO4xVBUmAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jm7i5rSw
dyYb/vWAYKQY
BwkwEwYDVR0BAwwCoYIKwYBBQUHAWEwE/QYJYIZIAYb4QgEB
BAQDAgZAMA0GC5qG
Sib3DQEBCwUAA4IBAQCeZShiBMu71PwH9dQHtsYSvi5WCyO7
qNzOPUynWA3h+Z
Q1i72kuTIGeAaDaYA4w4YyXDGmEomGzLKNxH2Bdh0x5LpXWx
7o6wR8h2k88ys
1VoZoc1mF7ALkkZWYyU9pAUkLdn9P/Wdu3mfQcUPWPh8QzB
KA90V4ugV8Qif
KDCq63NmZ9DHOdh20y1Q86dWFH16ez6k8Ddb6cdJbyXN8fmS
n2f0m6CDMH
lQynpRA7wSKoJGB0HLWBAZ3ckl7ymB6QMOC5OqCDwnUSEWZ6
54YAQ69GhAx0+
xp2BY1uUY5EyShobb5RWaQhZLaytkL6AeR/Bgzo
-----END CERTIFICATE REQUEST-----
```



## 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](#)

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.