

Configurazione del portale di provisioning dei certificati ISE 2.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Limitazioni](#)

[Configurazione](#)

[Verifica](#)

[Genera certificato singolo senza richiesta di firma certificato](#)

[Genera certificato singolo con richiesta di firma certificato](#)

[Genera certificati in blocco](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento vengono descritte la configurazione e la funzionalità del portale di provisioning dei certificati di Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- ISE
- Server Certificati e Autorità di certificazione (CA).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Identity Service Engine 2.0
- PC con Windows 7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il portale di provisioning dei certificati è una nuova funzionalità introdotta in ISE 2.0 che può essere utilizzata dai dispositivi terminali per registrare e scaricare certificati di identità dal server. e rilascia certificati ai dispositivi che non possono passare attraverso il flusso di caricamento.

Ad esempio, i dispositivi come i terminali POS non possono essere sottoposti al flusso BYOD (Bring Your Own Device) e devono ricevere certificati manualmente.

Il portale di provisioning dei certificati consente a un gruppo privilegiato di utenti di caricare una richiesta di certificato (CSR) per tali dispositivi; generare una coppia di chiavi e quindi scaricare il certificato.

Con ISE, è possibile creare modelli di certificato modificati e gli utenti finali possono selezionare un modello di certificato adatto per scaricare un certificato. Per questi certificati, ISE opera come server CA (Certification Authority) e possiamo ottenere il certificato firmato dalla CA interna ISE.

Il portale per il provisioning dei certificati ISE 2.0 supporta il download dei certificati nei seguenti formati:

- formato PKCS12 (compresa la catena di certificati; un file per la catena di certificati e la chiave)
- Formato PKCS12 (un file per certificato e chiave)
- Certificato (catena inclusa) in formato PEM (Privacy Enhanced Electronic Mail), chiave in formato PEM PKCS8.
- Certificato in formato PEM, chiave in formato PEM PKCS8:

Limitazioni

Attualmente ISE supporta solo queste estensioni in un CSR per firmare un certificato.

- AttributiDirectoryOggetto
- NomeAlternativoSoggetto
- utilizzoChiave
- identificatoreChiaveOggetto
- identitàcontrollo
- sintassiChiaveEstesa
- CERT_TEMPLATE_OID (OID personalizzato per specificare il modello utilizzato in genere nel flusso BYOD)

Nota: La CA interna di ISE è progettata per supportare funzionalità che utilizzano certificati come BYOD, pertanto le funzionalità sono limitate. Cisco sconsiglia di usare ISE come CA aziendale.

Configurazione

Per utilizzare la funzionalità di provisioning dei certificati nella rete, è necessario abilitare il servizio CA interno ISE e configurare un portale per il provisioning dei certificati.

Passaggio 1. Sulla GUI ISE, selezionare **Amministrazione > Sistema > Certificati > Autorità di certificazione > CA interna** e per abilitare le impostazioni della CA interna sul nodo ISE, fare clic su **Abilita Autorità di certificazione**.

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...

Passaggio 2. Creare i modelli di certificato in **Amministrazione > Sistema > Certificati > Modelli di certificato > Aggiungi**.

Immettere i dettagli in base al requisito e fare clic su **Invia**, come mostrato in questa immagine.

Add Certificate Template

* Name: testcert
Description: testing certificate

Subject

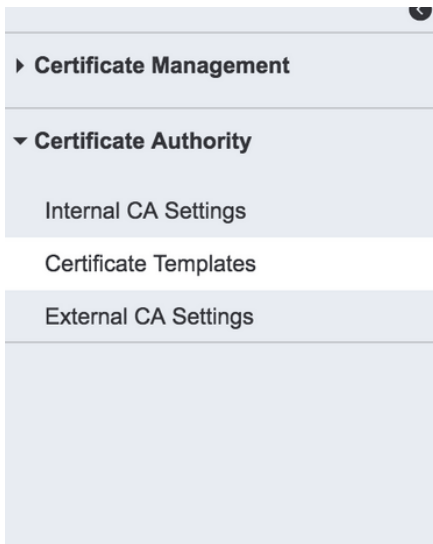
Common Name (CN): \$UserName\$ ⓘ
Organizational Unit (OU):
Organization (O):
City (L):
State (ST):
Country (C):

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

Nota: È possibile visualizzare l'elenco dei modelli di certificato creati in **Amministrazione > Sistema > Certificati > Modelli di certificato**, come illustrato in questa immagine.

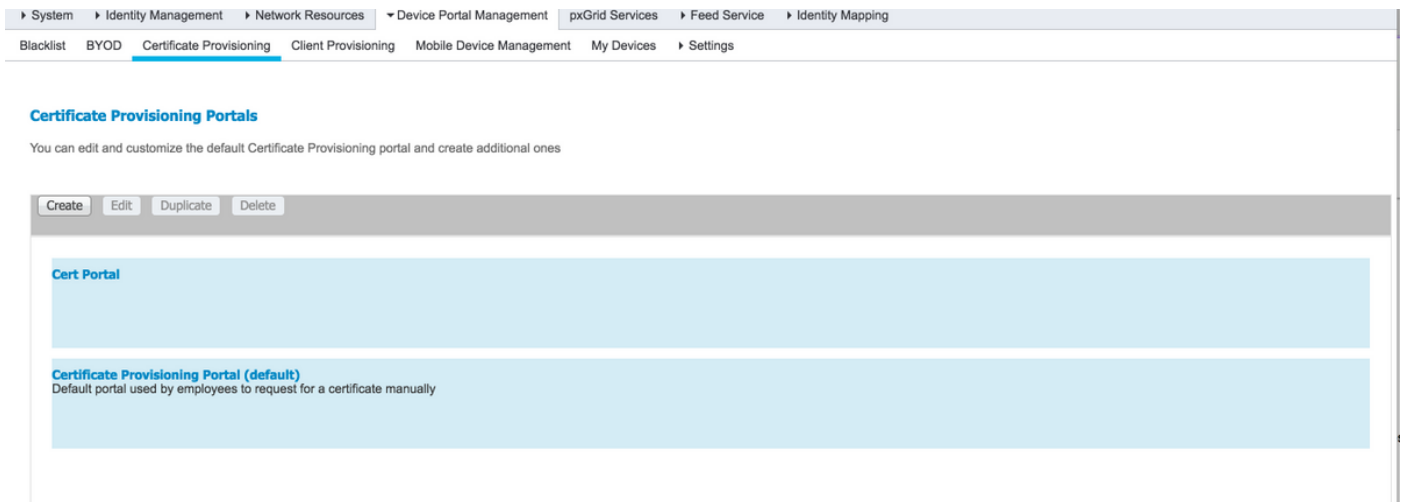


Certificate Templates

✎ 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

Passaggio 3. Per configurare il portale di provisioning dei certificati ISE, selezionare **Amministrazione > Gestione portale dispositivi > Provisioning certificati > Crea**, come mostrato nell'immagine:



Passaggio 4. Nel nuovo portale certificati espandere le impostazioni del portale, come illustrato nell'immagine.

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

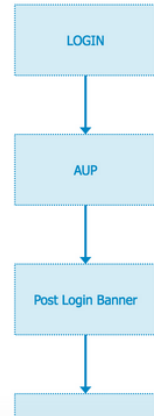
▶ Login Page Settings

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

→ ←

➔ Choose all

✗ Clear all

Fully qualified domain name (FQDN):

Idle timeout: 1-30 (minutes)

porta HTTPS
Interfacce consentite

Porta che deve essere utilizzata dal portale di provisioning dei certifi
Le interfacce su cui ISE deve eseguire l'ascolto per questo portale.

Tag gruppo di certificati
Metodo di autenticazione
Gruppi autorizzati
Nome di dominio completo (FQDN)
Timeout di inattività

Tag del certificato da utilizzare per il portale di provisioning dei certificati
Selezionare la sequenza di archiviazione delle identità che autenticano
È possibile controllare l'insieme di utenti che possono accedere al portale.
È inoltre possibile assegnare un FQDN specifico a questo portale. Gli
Il valore definisce il timeout di inattività per il portale.

Nota: La configurazione dell'origine identità può essere verificata in **Amministrazione > Gestione identità > Sequenza origine identità**.

Passaggio 5. Configurare le impostazioni della pagina di accesso.

▼ **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

Passaggio 6. Configurare le impostazioni della pagina 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)

Passaggio 7. È anche possibile aggiungere il banner di accesso al post.

Passaggio 8. In Impostazioni portale di provisioning dei certificati specificare i modelli di certificato consentiti.

▼ **Change Password Settings**

Allow internal users to change their own passwords

▼ **Certificate Provisioning Portal Settings**

Certificate Templates: *

Passaggio 9. Scorrere fino all'inizio della pagina e fare clic su **Salva** per salvare le modifiche.

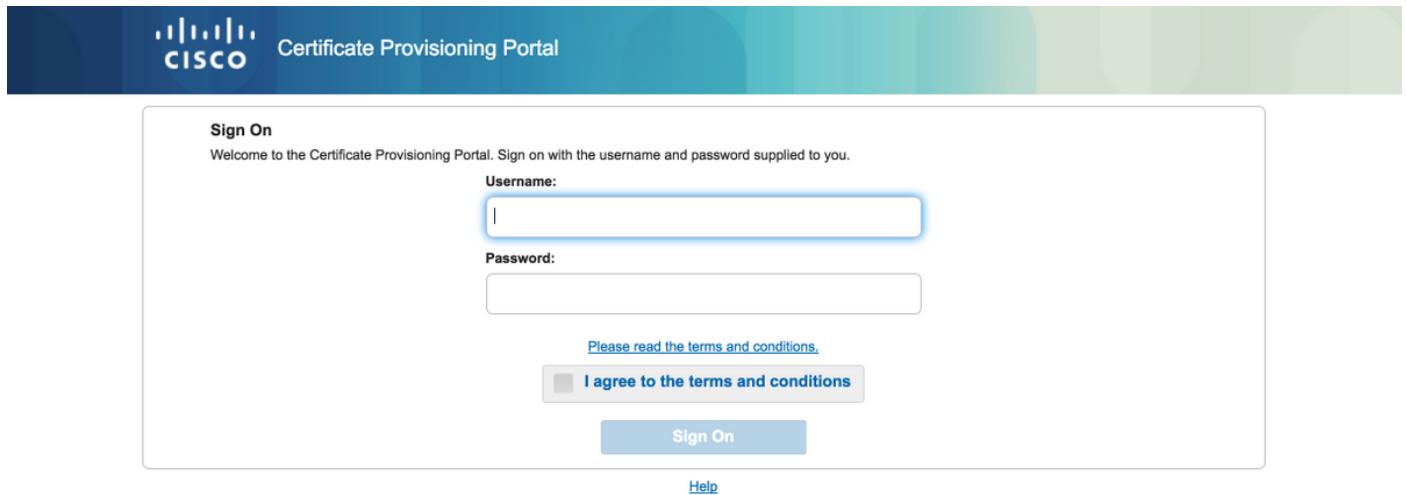
Inoltre, il portale può essere ulteriormente personalizzato passando alla scheda di **personalizzazione della pagina del portale**, in cui è possibile modificare il testo AUP, il banner di accesso post e altri messaggi in base ai requisiti.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Se ISE è configurato correttamente per il provisioning dei certificati, è possibile richiedere/scaricare un certificato dal portale di provisioning dei certificati ISE seguendo questi passaggi.

Passaggio 1. Aprire il browser e passare all'FQDN del portale di provisioning dei certificati configurato in precedenza o all'URL del test di provisioning dei certificati. L'utente viene reindirizzato al portale, come mostrato nell'immagine seguente:



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, there is a "Help" link.

Passaggio 2. Accedere con nome utente e password.

Passaggio 3. Dopo aver completato l'autenticazione, accettare l'autenticazione automatica e viene visualizzata la pagina di provisioning del certificato.

Passaggio 4. La pagina di provisioning dei certificati fornisce la funzionalità per scaricare i certificati in tre modi:

- Certificato singolo (senza richiesta di firma del certificato)
- Certificato singolo (con richiesta di firma del certificato)
- Certificati in blocco

Genera certificato singolo senza richiesta di firma certificato

- Per generare un singolo certificato senza CSR, selezionare l'opzione **Genera singolo certificato (senza richiesta di firma del certificato)**.
- Inserire il nome comune (CN).

Nota: Il CN specificato deve corrispondere al nome utente del richiedente. Il richiedente fa riferimento al nome utente utilizzato per accedere al portale. Solo gli utenti amministratori possono creare un certificato per un CN diverso.

- Immettere l'indirizzo MAC del dispositivo per il quale viene generato il certificato.

- Scegliere il modello di certificato appropriato.
- Scegliere il formato desiderato per il download del certificato.
- Immettere una password per il certificato e fare clic su **Ggenerare**.
- Viene generato e scaricato un singolo certificato.

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

Genera certificato singolo con richiesta di firma certificato

- Per generare un singolo certificato senza CSR, selezionare l'opzione **Genera singolo certificato (con richiesta di firma del certificato)**.
- Copiare e incollare il contenuto CSR dal file del Blocco note in **Dettagli richiesta firma certificato**.
- Immettere l'indirizzo MAC del dispositivo per il quale viene generato il certificato.
- Scegliere il modello di certificato appropriato.
- Scegliere il formato desiderato per il download del certificato.
- Immettere una password per il certificato e fare clic su **Genera**.

- Verrà generato e scaricato un singolo certificato.

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
CSqGSIb3DQEBAQUA
AAIBDwAwggEKAoIBAQCfPaA5XBkMmrfUjz/SrKa465ecULygnHG
NC7bPq4+5
8vK723r23qhympvBNPw31K6qzUCmDYLOcTwp+xbWY8rfY5xQ
ndetNofbrTL
Crlhrnbnj0+SD7IUozpXYe1DmugD8YL9HT0Vv//WBKie6B8JZKI
WwqgAKYJ
yqJC55eBZ/yYBRB2rAbvhlTon1/SyHNeIRHw6L5ABqjSToasXW
kyEIQT,JkK
8DmkucOm3h46NulhrWpBfD9H6uGrY8Yz7FvqSDsX4na0f6P50K
6y4YmKNzSJE
qKowamxNaGLdHcNhKa8nmfJ0twTEMMWnTWbn5AgMBAAGz
TBJBqkqhkG9wOB
CO4xVBUmAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2im7i5rSw
dyYb/vWAYKQY
BwkwEwYDVR0BAwwCoYIKwYBBQUHAwEwE/QYJYIZIAyb4QqEB
BAQDAgZAMA0GC5qG
Sib3DQEBCwUAA4IBAQCeZShiBMu71PwH9dQHtsYSvISWcyO7
qNzOPUynWA3t+Z
Q1i72kuTIGeEaDaYA4w4YyXDGmEomGzLKNxH2Bdh0x5HLeXWx
7o6wR8h2k88ys
1VoZoc1mF7ALkkZWYyU9pAUkLdn9P/W0u3mfQcUPWPh8QzB
KA90V4ugV8Qif
KDCq63NmZ9DHOdh20y1Q86dWFH16ez6k8Ddb6cdJbyXN8fmS
n2f0m6CDMH
lQynpRA7wSKoJGB0HLWBAZ3ckl7ymB6QMOC5OqCDwnUSEWZ6
54YAQ69GhAx0+
xp2BY1uUYSEyShobb5RWaQhZLaytkL6AeR/Bgzo
-----END CERTIFICATE REQUEST-----
```

-----BEGIN CERTIFICATE REQUEST-----
 gNzCPJynVA3h+Z
 Q1f72kuITIGEaDaYAfw4YyXDqGmEomGzLKNdH2BdhOx5HLPXWk
 Zo6wR8hZk86ys
 1VsZoa1mF7ALkKzWNYU9oAUel,dn9P^W0uGmQtCUPWPh8OzB
 KA90V4ugV9GIf
 tK0Cq63NmZjDHOdh20y1O86dWFH18ezPk8Ddt8cod,byXN8fmS
 n26oM9CDMH
 J0ypRA7w5KoJGB0HLWBAZ3ckJ7ymB6QMQCSOzCDwniJSEWZ6
 54/YAQ9KzHAxQ+
 xpZBY1uJZYSEyHobb6RWAQrhZLsytkL6AeRBozc
 -----END CERTIFICATE REQUEST-----

MAC Address:

Choose Certificate Template: *

Description:

Certificate Download Format: *

Certificate Password: *

Confirm Password: *

Genera certificati in blocco

È possibile generare certificati collettivi per più indirizzi MAC se si caricano file CSV che contengono i campi CN e indirizzo MAC.

Nota: Il CN specificato deve corrispondere al nome utente del richiedente. Il richiedente fa riferimento al nome utente utilizzato per accedere al portale. Solo gli utenti amministratori possono creare un certificato per un CN diverso.

- Per generare un singolo certificato senza CSR, selezionare l'opzione **Genera singolo certificato (con richiesta di firma del certificato)**.
- Caricare il file CSV per la richiesta in blocco.
- Scegliere il modello di certificato appropriato.
- Scegliere il formato desiderato per il download del certificato.
- Immettere una password per il certificato e fare clic su **Genera**.
- Viene generato e scaricato un file zip di certificati in blocco.

Certificate Provisioning

I want to: *

Generate bulk certificates ▼

Upload CSV File: *

Choose File

If you don't have the CSV template, [download here](#)

Choose Certificate Template: *

EAP_Authentication_Certificate_Template ▼

Description:

Certificate Download Format: *

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

Certificate Password: *

Confirm Password: *

Generate **Reset**

[Help](#)

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.