

ISE 2.0 証明書プロビジョニングポータルの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[制限](#)

[設定](#)

[確認](#)

[単一の証明書を生成 \(証明書署名要求なし \)](#)

[単一の証明書を生成 \(証明書署名要求あり \)](#)

[証明書の一括生成](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Identity Services Engine (ISE) 証明書プロビジョニング ポータルの設定と機能について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE
- 証明書および認証局 (CA) サーバ。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Service Engine 2.0
- Windows 7 PC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

証明書プロビジョニング ポータルは、ISE 2.0 で導入された新機能であり、エンド デバイスが登

録したり ID 証明書をサーバからダウンロードしたりするために使用できます。これはオンボーディング フローを行うことができないデバイスに証明書を発行します。

たとえば、POS 端末などのデバイスは、Bring Your Own Device (BYOD; 個人所有デバイス持ち込み) フローを実行できず、証明書を手動で発行することが必要です。

証明書プロビジョニング ポータルでは、権限を持つ一連のユーザが、そのようなデバイスに証明書要求 (CSR) をアップロードできます。キーのペアを生成して、証明書をダウンロードします。

ISE では、ユーザは変更された証明書テンプレートを作成できます。エンドユーザは、適切な証明書テンプレートを選択して証明書をダウンロードできます。これらの証明書に対して、ISE は認証局 (CA) サーバとして機能し、ユーザは ISE 内部 CA によって署名された証明書を取得できます。

ISE 2.0 証明書プロビジョニング ポータルは、以下の形式での証明書ダウンロードをサポートします。

- PKCS12 形式 (証明書チェーンを含む。証明書チェーンとキーの両方のための 1 ファイル)
- PKCS12 形式 (証明書とキーの両方のための 1 ファイル)
- Privacy Enhanced Electronic Mail (PEM) 形式の証明書と、PKCS8 PEM 形式のキー。
- PEM 形式の証明書と、PKCS8 PEM 形式のキー。

制限

現在 ISE では、証明書の署名に対して CSR で以下の拡張機能のみをサポートしています。

- subjectDirectoryAttributes
- subjectAlternativeName
- keyUsage
- subjectKeyIdentifier
- auditIdentity
- extendedKeyUsage
- CERT_TEMPLATE_OID (BYOD フローで通常使用されるテンプレートを指定するためのカスタム OID)

注 : ISE 内部 CA は、証明書を使用する BYOD などの機能をサポートするように設計されているため、機能が制限されています。エンタープライズ CA として ISE を使用することは、シスコは推奨していません。

設定

ネットワーク内で証明書プロビジョニングの機能を使用するには、ISE 内部 CA サービスを有効にして、証明書プロビジョニングポータルを設定する必要があります。

ステップ 1 : ISE の GUI で、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [内部CA (Internal CA)] の順に移動し、[認証局の有効化 (Enable Certificate Authority)] をクリックして、ISE ノードで内部 CA 設定を有効にします。

Internal CA Settings ⚠ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

Disable 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...

ステップ 2 : [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書テンプレート (Certificate Templates)] > [追加 (Add)] で証明書テンプレートを作成します。

この図に示すように、要件に従って詳細を入力し、[送信 (Submit)] をクリックします。

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

注 : この図に示すように、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書テンプレート (Certificate Templates)] の順に移動して、作成された証明書テンプレートのリストを確認できます。

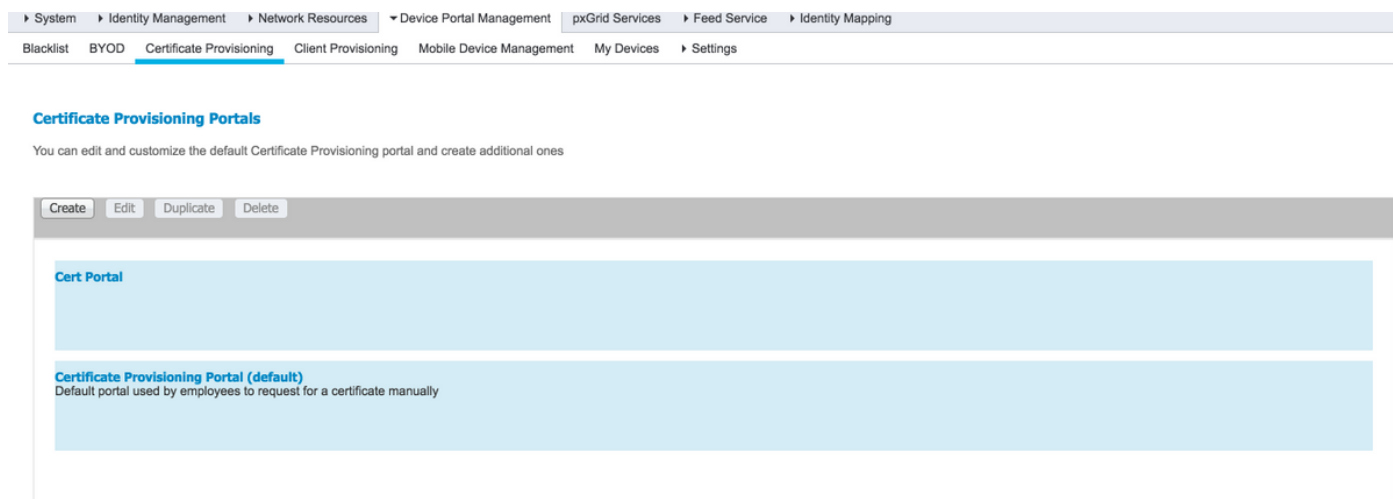
Certificate Templates

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

ステップ 3 : ISE 証明書プロビジョニングポータルを設定するには、図に示すように、[管理


(Administration)] > [デバイスポータル管理 (Device Portal Management)] > [証明書のプロビジョニング (Certificate Provisioning)] > [作成 (Create)] の順に移動します。



ステップ 4 : 図に示すように、新しい証明書ポータルでポータル設定を展開します。

Portals Settings and Customization

Portal Name: * Description:

 **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



```
graph TD; LOGIN[LOGIN] --> AUP[AUP]; AUP --> PostLoginBanner[Post Login Banner]; PostLoginBanner --> Next[ ];
```

▼ 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" value=""/> ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee

Fully qualified domain name (FQDN):

Idle timeout: 1-30 (minutes)

HTTPS ポート (HTTPS port)
 使用可能インターフェイス
 証明書グループ タグ
 認証メソッド
 承認されたグループ
 完全修飾ドメイン名 (FQDN)
 アイドル タイムアウト

HTTPS 用に証明書プロビジョニング ポータルが使用するポート。
 ISE がこのポータルをリスンするインターフェイス。
 証明書プロビジョニングポータルに使用する証明書タグ (このポータル
 このポータルへのログインを認証する ID ストアの順序を選択します。
 証明書プロビジョニングポータルにアクセスできる一連のユーザは、該
 特定の FQDN をこのポータルに付与することもできます。httpまたはh
 この値は、ポータルのアイドル タイムアウトを定義します。

注：ID ソースの設定は、[管理 (Administration)] > [ID管理 (Identity Management)] > [IDソース順序 (Identity Source Sequences)] で確認できます。

ステップ 5：ログインページを設定します。

▼ 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

ステップ 6 : AUP ページを設定します。

▼ 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)

ステップ 7 : ポストログインバナーを追加することもできます。

ステップ 8 : [証明書プロビジョニングポータルの設定 (Certificate Provisioning Portal Settings)] で、許可されている証明書テンプレートを指定します。

▼ Change Password Settings

Allow internal users to change their own passwords

▼ Certificate Provisioning Portal Settings

Certificate Templates: *

ステップ 9 : ページの上部にスクロールし、[保存 (Save)] をクリックして変更を保存します。

また、[ポータルページのカスタマイズ (Portal Page Customization)] タブに移動して、AUP のテキスト、ポストログインバナーのテキスト、およびその他のメッセージを必要に応じて変更することで、ポータルをさらにカスタマイズできます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ISE が証明書プロビジョニング用に正しく設定されていれば、次の手順を使用して ISE 証明書プロビジョニングポータルから証明書の要求やダウンロードを行うことができます。

ステップ 1 : ブラウザを開き、ポータルの認定するか証明書プロビジョニング テストURL (上記で設定したプロビジョニングを参照してください。この図のように、ポータルにリダイレクトされます。

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](#)

ステップ 2 : ユーザ名とパスワードを使用してログインします。

ステップ 3 : 認証に成功すると、AUP が承認され、証明書プロビジョニングページが表示されます。

ステップ 4 : 証明書プロビジョニングページでは、次の 3 つの方法で証明書をダウンロードできます。

- 単一の証明書 (証明書署名要求なし)
- 単一の証明書 (証明書署名要求あり)
- 証明書一括生成

単一の証明書を生成 (証明書署名要求なし)

- CSR なしで単一の証明書を生成するには、[単一の証明書を生成 (証明書署名要求なし) (Generate single certificate (without certificate signing request))] オプションを選択します。
- 共通名 (CN) を入力します。

注 : 特定の CN を要求者のユーザ名と一致させる必要があります。要求者は、ポータルへのログインに使用するユーザ名を参照します。admin ユーザのみが、別の CN の証明書を作成できます。

- 証明書を生成するデバイスの MAC アドレスを入力します。
- 適切な証明書テンプレートを選択します。
- ダウンロードする証明書の形式を選択します。
- 証明書のパスワードを入力し、[生成 (Generate)] をクリックします。
- 単一の証明書が正常に生成されて、ダウンロードされます。

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

単一の証明書を作成 (証明書署名要求あり)

- CSR なしで単一の証明書を作成するには、[単一の証明書を作成 (証明書署名要求あり) (Generate single certificate (with certificate signing request))] オプションを選択します。
- CSR の内容を、[Certificate Signing Request Details]の下のメモ帳ファイルからコピー アンドペーストします。
- 証明書を生成するデバイスの MAC アドレスを入力します。
- 適切な証明書テンプレートを選択します。
- ダウンロードする証明書の形式を選択します。
- 証明書のパスワードを入力し、[生成 (Generate)] をクリックします
- 単一の証明書が正常に生成されて、ダウンロードされます。

Certificate Provisioning

I want to: *

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: *

```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAAIQAQAwEDEOMAwGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUgySpKa465ecULygnjHG
NC7bPqz4+5
8vK723r23ghympvBNPw31K6qzUCmDYLOcTwp+ymbWY3rfYxQ
nde8NofbTL
CrIhcnbmn0+SD7UozaXYb1DmugD8YL9Ht0Vv//WBKie6B8jZKl
WwqjAKVJ
yqJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABjsSToasXW
kyEIQT,kK
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P5OK
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmlJ0wTEMMmwn7Wbn5AgMBAAGgZ
TBjBqkqkG9wOB
CQ4xVBUUAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYXKY
BwkwEwYDVR0BAwwCgYIKaYBBQUHAwEwEQYJYIZIAYb4QqEB
BAQDAgZAMA0GCSeG
Sib3DQEBQwIAA4IBAQCeZSHBMu71Pv?H9dQHTxY5v5WCyQ7
qNzOPUymVA3h+Z
Q1f72xulTIGEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALkXZWNyU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63/NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
JdypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ9K3hAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1f72xulTIGEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5hLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALkXZWNyU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63/NmZ9DH0dth20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
JdypRA7w5KoJGB0HLWBAZ3ckl7ymB6QMOC5OaCDwnUSEWZ6
54/YAQ9K3hAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

MAC Address:

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (O...

Certificate Password: *

Confirm Password: *

CN および MAC アドレス フィールドが含まれる CSV ファイルをアップロードすると、複数の MAC アドレス用の証明書を一括生成できます。

注：特定の CN を要求者のユーザ名と一致させる必要があります。要求者は、ポータルへのログインに使用するユーザ名を参照します。admin ユーザのみが、別の CN の証明書を作成できます。

- CSRを使用せずに単一の証明書を生成するには、[単一の証明書を生成する(証明書署名要求を使用)]オプションを選択します。
- 一括要求用に csv ファイルをアップロードします。
- 適切な証明書テンプレートを選択します。
- ダウンロードする証明書の形式を選択します。
- 証明書のパスワードを入力し、[生成 (Generate)] をクリックします
- 証明書 zip ファイルが一括生成されてダウンロードされます。



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](#)

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。