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](#)
[トラブルシュート](#)

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。

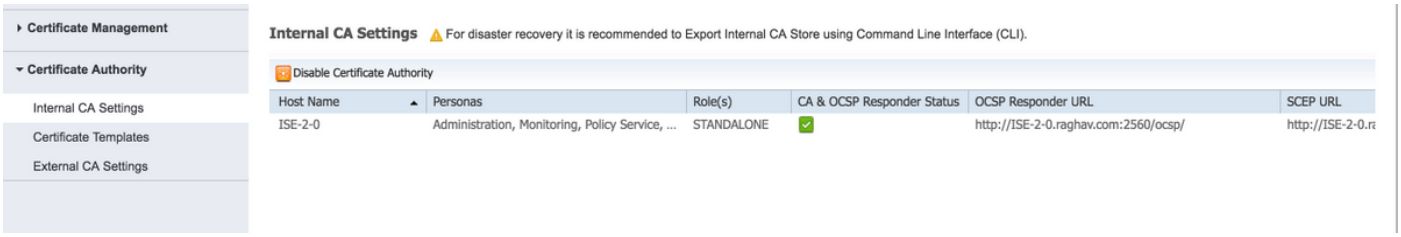
- subjectDirectoryAttributes
- subjectAlternativeName
- keyUsage
- subjectKeyIdentifier
- auditIdentity
- extendedKeyUsage
- CERT_TEMPLATE_OID（BYOD フローで通常使用されるテンプレートを指定するためのカスタム OID）

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

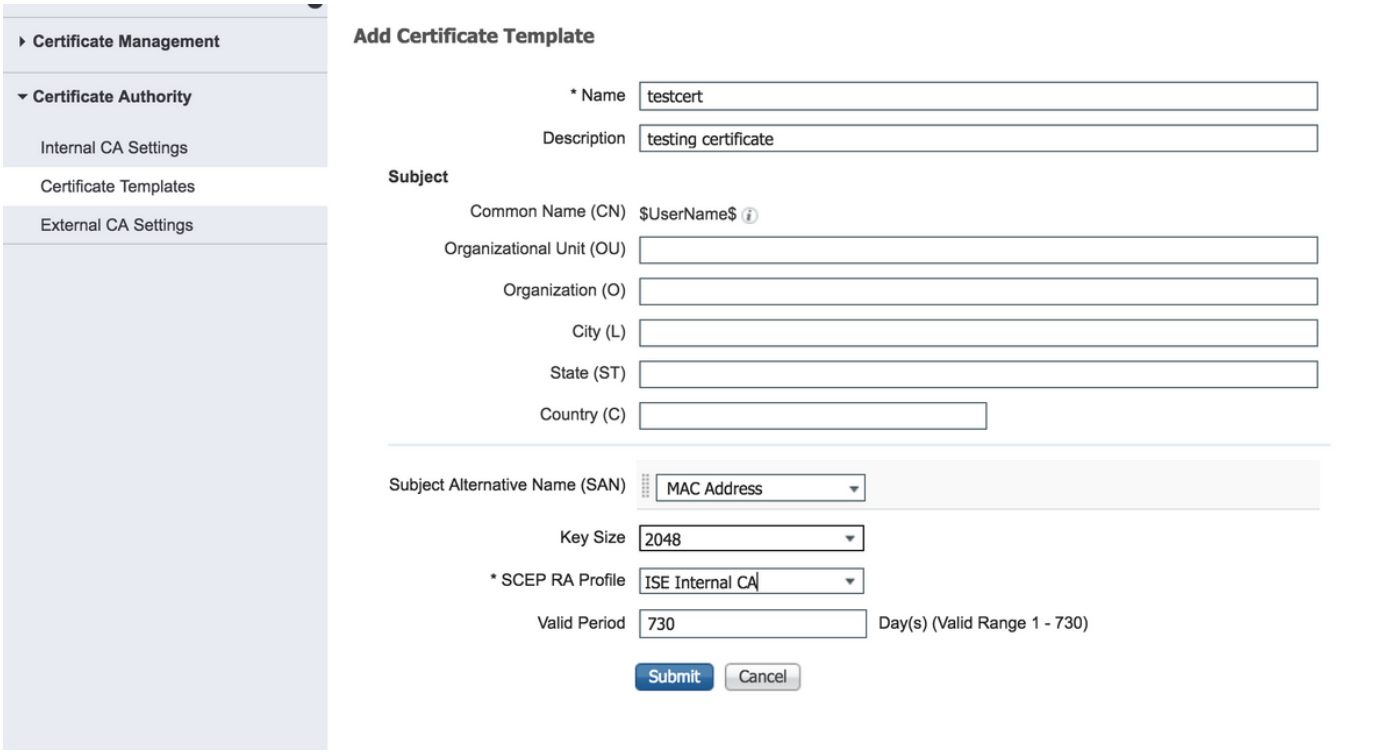
ネットワーク内で証明書プロビジョニングの機能を使用するには、ISE 内部 CA サービスを有効にして、証明書プロビジョニングポータルを設定する必要があります。

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。

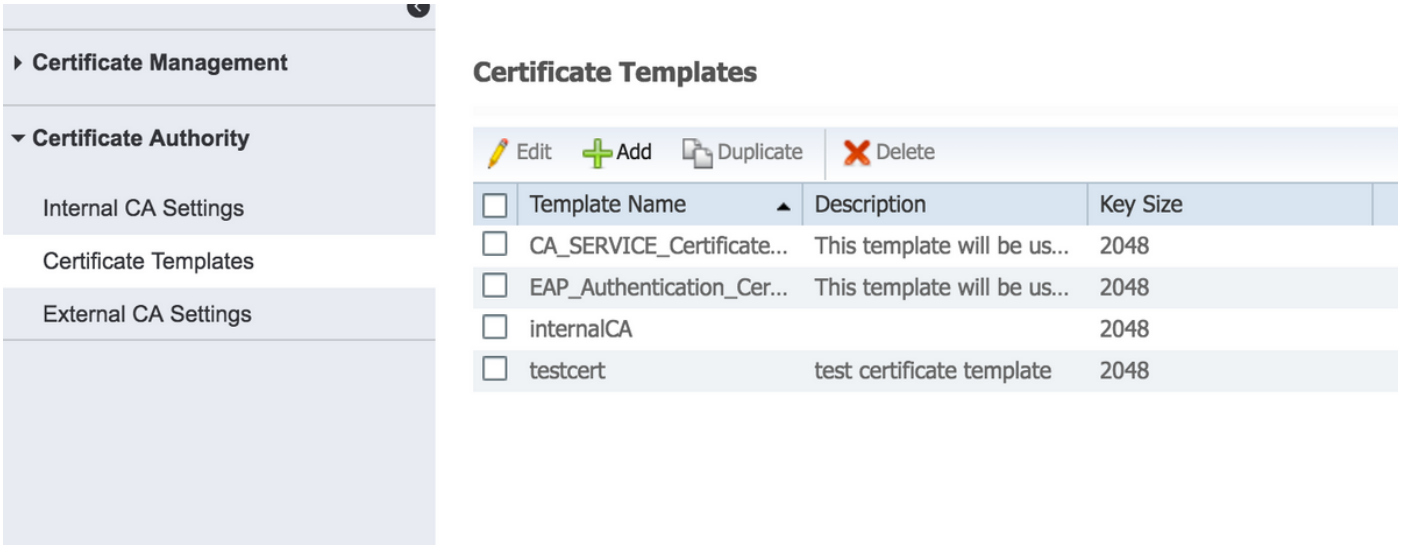


ステップ 2： [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書テンプレート（Certificate Templates）] > [追加（Add）] で証明書テンプレートを作成します。

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。

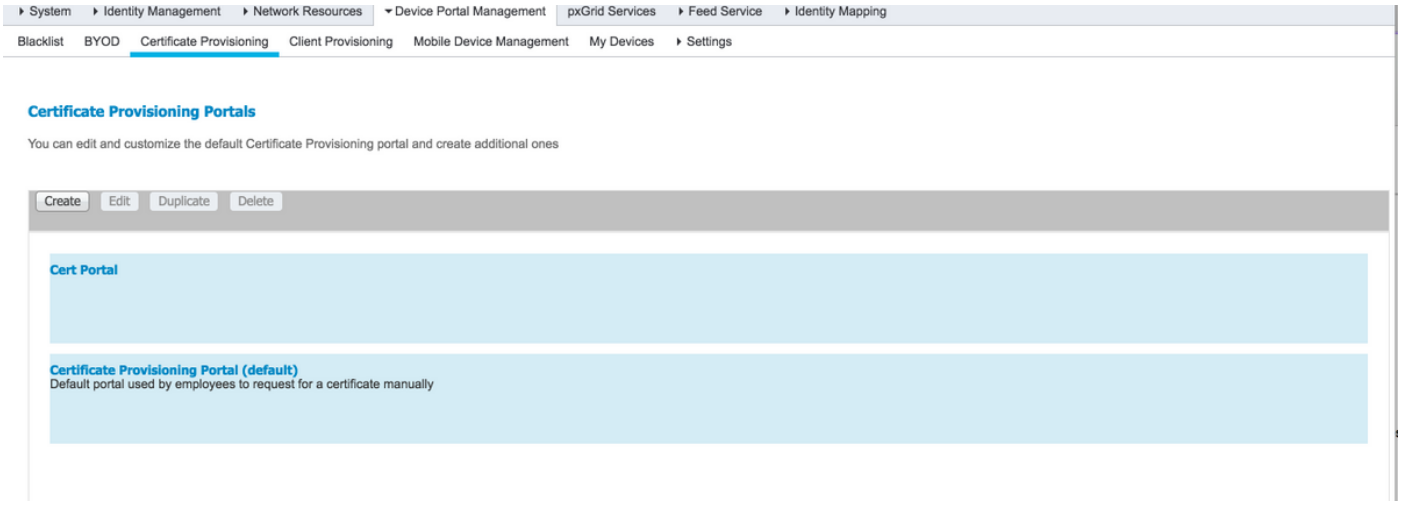


注：この図に示すように、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書テンプレート（Certificate Templates）] の順に移動して、作成された証明書テンプレートのリストを確認できます。

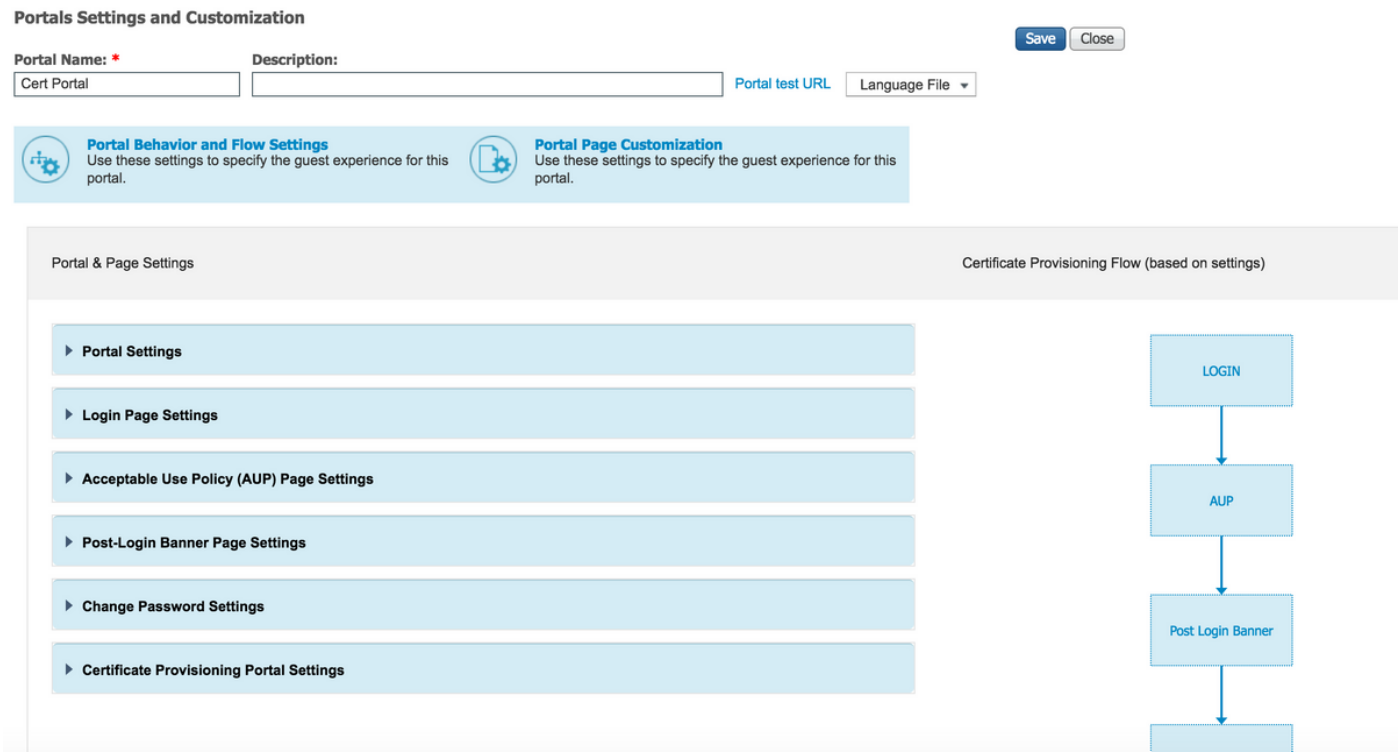


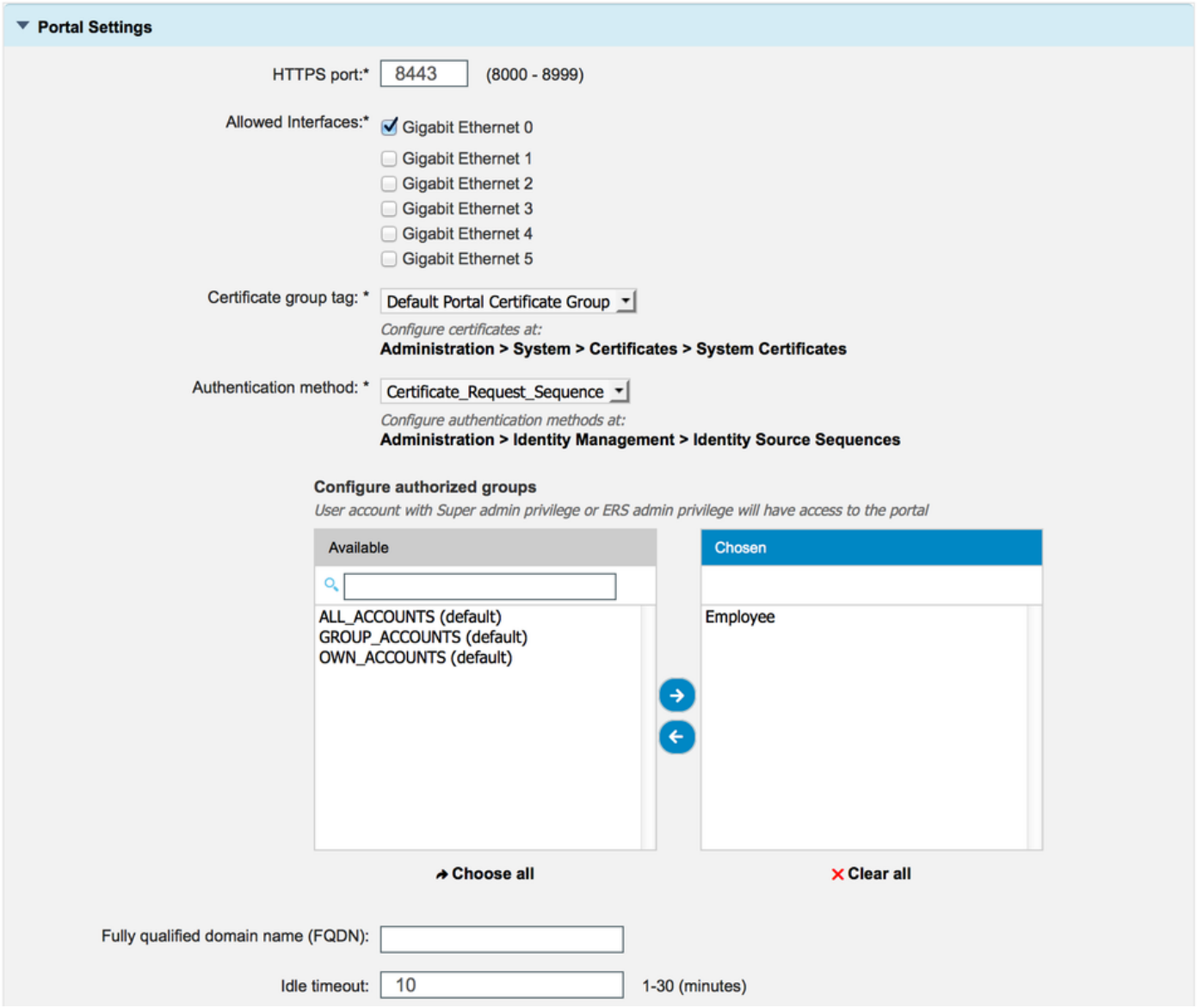
ステップ 3：ISE 証明書プロビジョニングポータルを設定するには、図に示すように、[管理

（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。

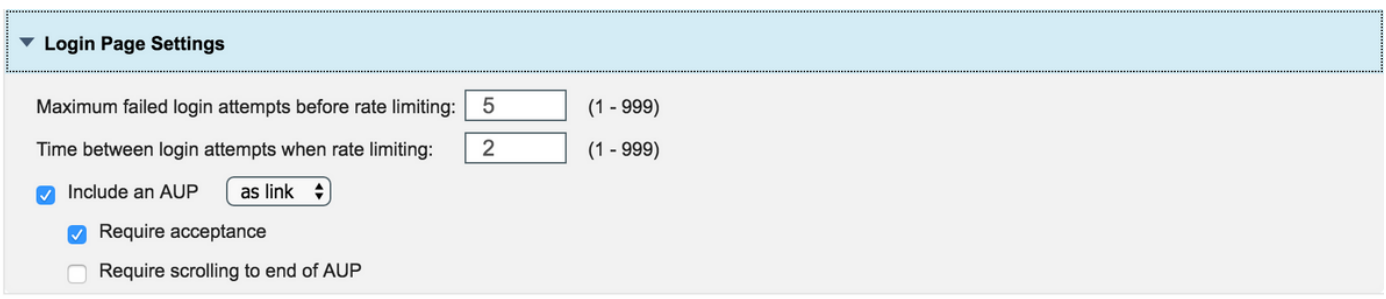




HTTPS ポート（HTTPS port）	HTTPS 用に証明書プロビジョニング ポータルが使用するポート。
使用可能インターフェイス	ISE がこのポータルをリッスンするインターフェイス。
証明書グループ タグ	証明書プロビジョニングポータルに使用する証明書タグ（このポータル
認証メソッド	このポータルへのログインを認証する ID ストアの順序を選択します。
承認されたグループ	証明書プロビジョニングポータルにアクセスできる一連のユーザは、該
完全修飾ドメイン名（FQDN）	特定の FQDN をこのポータルに付与することもできます。http または h
アイドル タイムアウト	この値は、ポータルのアイドル 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。

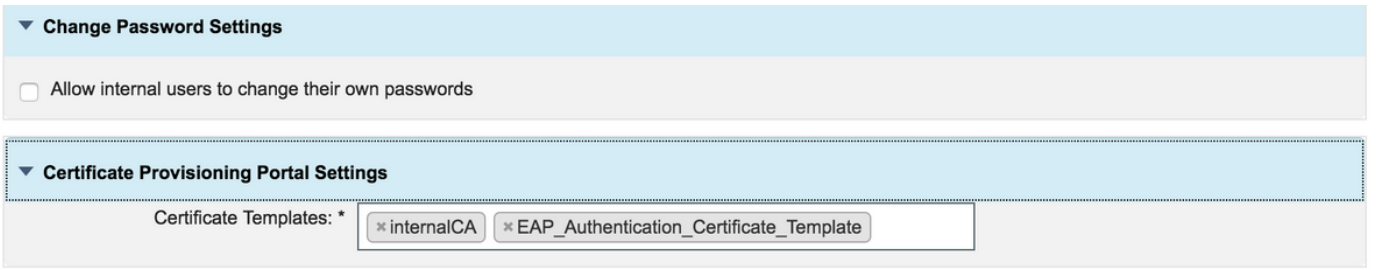
ステップ 5：ログインページを設定します。



ステップ 6：AUP ページを設定します。

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。



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。

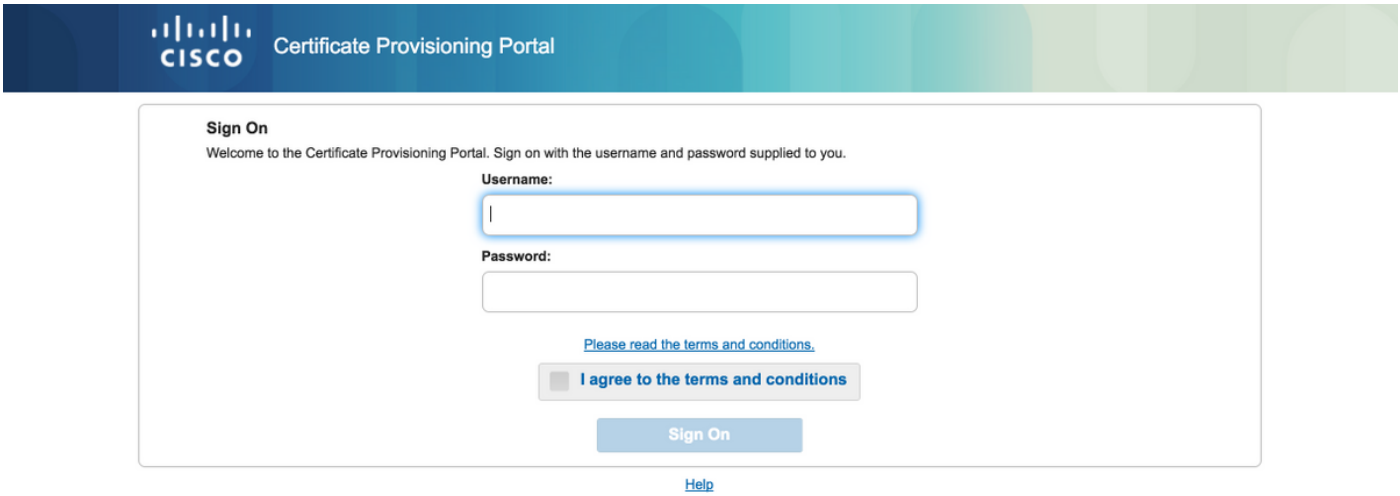
また、[ポータルページのカスタマイズ（Portal Page Customization）] タブに移動して、AUP のテキスト、ポストログインバナーのテキスト、およびその他のメッセージを必要に応じて変更することで、ポータルをさらにカスタマイズできます。

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。



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。

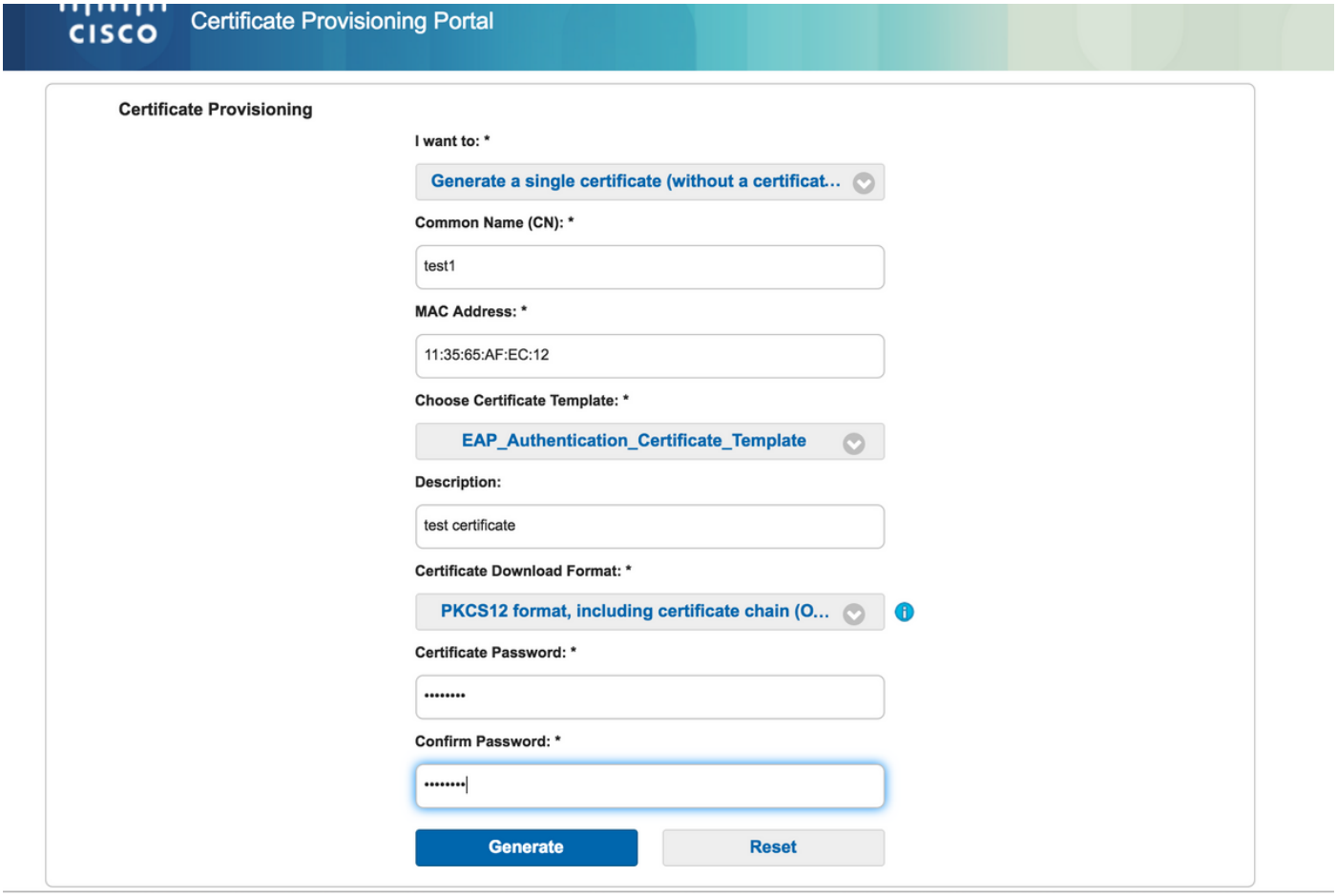
- 単一の証明書（証明書署名要求なし）
- 単一の証明書（証明書署名要求あり）
- 証明書一括生成

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。

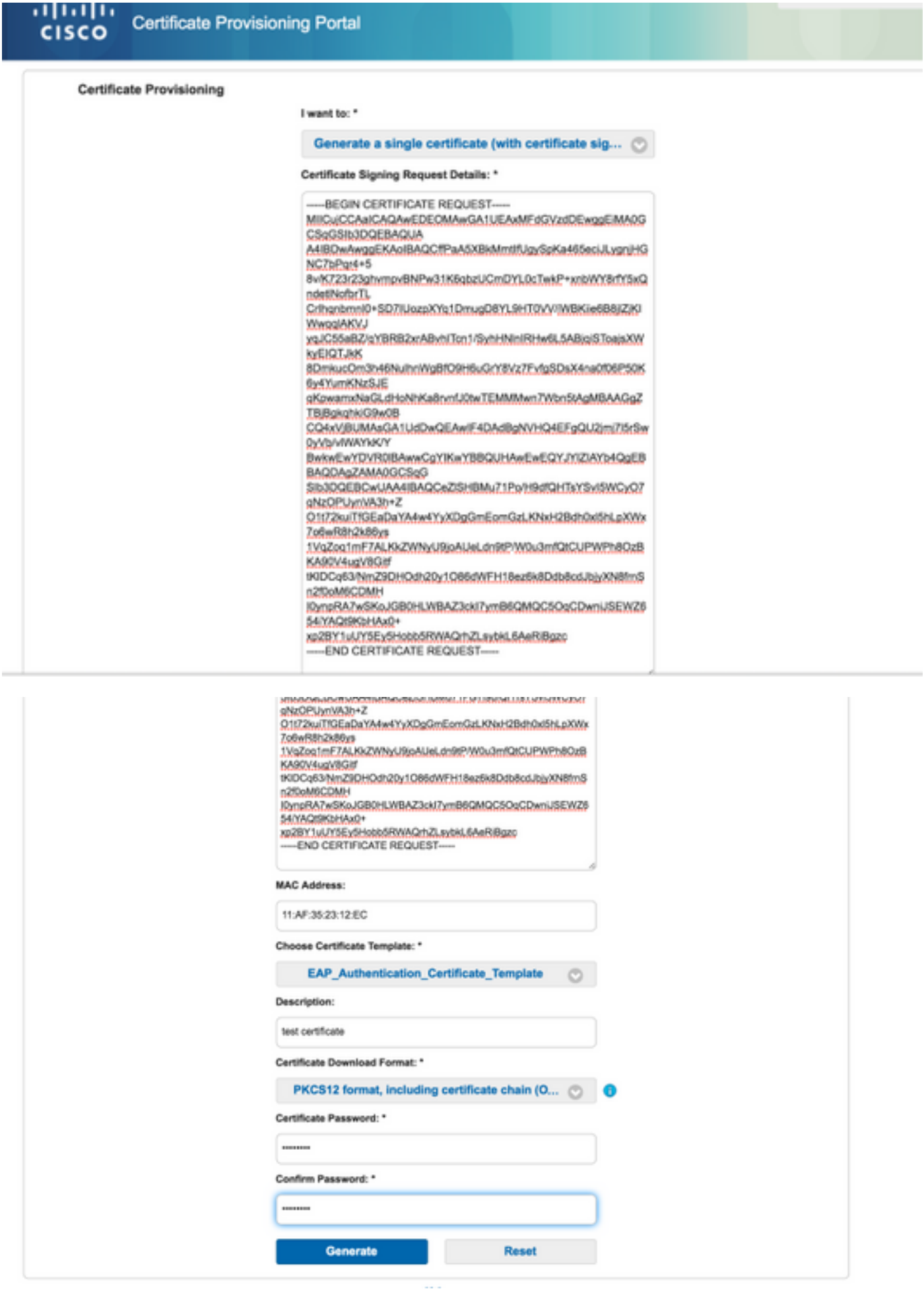
  注：特定の CN を要求者のユーザ名と一致させる必要があります。要求者は、ポータルへのログインに使用するユーザ名を参照します。admin ユーザのみが、別の CN の証明書を作成できます。

- 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。



単一の証明書を生成（証明書署名要求あり）

- 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。

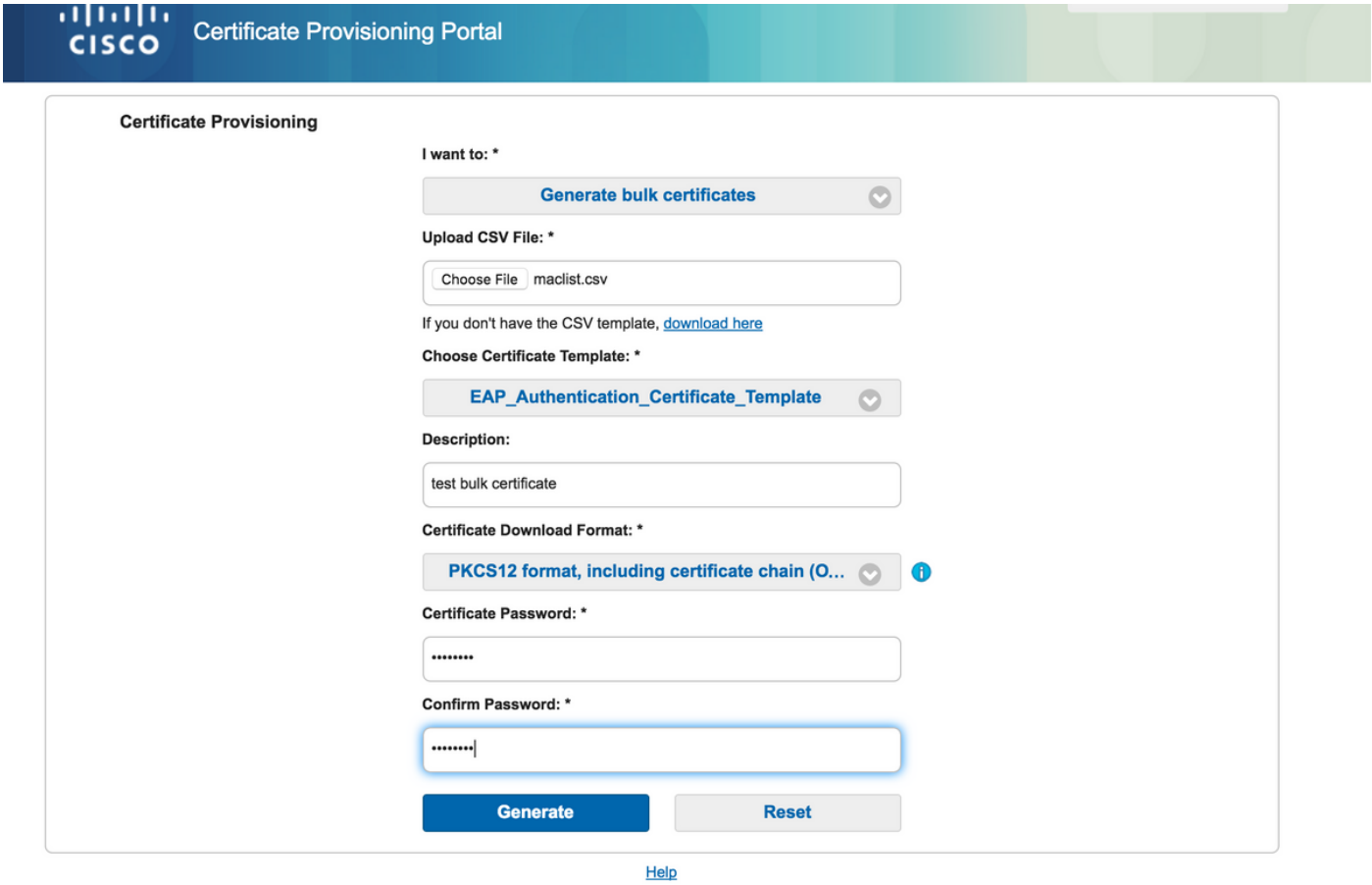

Certificate Provisioning Portal
Certificate Provisioning
I want to: *
Generate a single certificate (with certificate sig...
Certificate Signing Request Details: *
-----BEGIN CERTIFICATE REQUEST-----
MIIClCCAaICAQAwEDEOMAwGA1UEAxMFdGVzdDEwggEiMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCffPaA5XBkMmtlfUgySpKa465eciJLygnjHG
NC7bPgc4+5
8vK723r23ghvmpvBNPw31K6qbzUCmDYL0cTwkP+xnbWY8rfY5xQ
ndetlNofbrTL
CrlhqnbmnI0+SD7lUozpXYq1DmugD8YL9HT0VV/lWBKie6B8jZKI
WwqqlAKVJ
yqJC55aBZ/aYBRB2xrABvhlTcn1/SyhHNlnIRHw6L5ABjqiSToajsXW
kyEIQTJkK
8DmkucOm3h46NulhriWgBfO9H6uGrY8Vz7FvfgSDsX4na0f06P50K
6y4YumKNzSJE
qKpwamxNaGLdHoNhKa8rvnfJ0twTEMMMwn7Wbn5tAgMBAAGgZ
TBJBgkqhkiG9w0B
CQ4xVjBUMAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw
0yVb/vlWAYkK/Y
BwkwEwYDVR0lBAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB
BAQDAgZAMA0GCSqG
SIb3DQEBCwUAA4IBAQCeZtSHBMu71Po/Hl9dfQHTsYSvl5WCyO7
qNzOlPUynVA3h+Z
O1t72kuiTfGEaDaYA4w4YyXDgGmEomGzLKNxH2Bdh0xl5hLpXWx
7o6wR8h2k86ys
1VqZoq1mF7ALKkZWNyU9joAUeLdn9tP/W0u3mfQtCUPWPh8OzB
KA90V4ugV8Gtf
tK0DCq63/NmZ9DHOdh20y1Q86dWFH18ez6k8Ddb8cdJbjyXN8fmS
n2f0oM6CDMH
l0ynpRA7wSKoJGB0HLWBAZ3ckI7ymB6QMQC5OqCDwniJSEWZ6
54/YAQt9KbHAx0+
xp2BY1uUY5Ey5Hobb5RWAQrhZLsybkL6AeRiBgzc
-----END CERTIFICATE REQUEST-----
MAC Address:
11:AF:35:23:12:EC
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

証明書の一括生成

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。



トラブルシュート

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。