よくある質問

# 証明書プロビジョニング ポータルに関する FAQ リリース 2.x

改訂：**April 27, 2017,**

# 証明書プロビジョニング ポータルに関する FAQ



### 証明書プロビジョニング ポータルの役割は何ですか。

証明書プロビジョニング ポータルは、オンボーディング フローを通過できないデバイスに証明書を発行します。たとえば、販売時点管理端末などのデバイスはBYODフローを通過できないため、証明書を手動で発行する必要があります。証明書プロビジョニング ポータルにより、一連の特権ユーザはこれらのデバイスの証明書要求をアップロードし、（必要に応じて）キー ペアを生成し、証明書をダウンロードすることができます。

### ログインできない理由は何ですか。

証明書プロビジョニング ポータルにログインするには、管理者が証明書プロビジョニング ポータル用に設定した特定の ID グループに属しているユーザ アカウントが必要です。管理者に問い合わせてください。

### パスワードを変更するにはどうすればよいですか。

Cisco ISE の内部ユーザのみ、証明書プロビジョニング ポータルでパスワードを変更できます（ユーザ情報が Cisco ISE 内部データベースに存在している必要があります）。パスワードを変更するには、次の手順を実行します。

1. クレデンシャルを使用して証明書プロビジョニング ポータルにログインします。
2. 右上隅の [アカウント（Account）] メニュー ドロップダウン リストをクリックします。
3. [パスワードの変更] をクリックします。
4. 画面の指示に従ってパスワードを変更します。

### 属性付きの証明書を 1 つ生成するにはどうすればよいですか。

属性付きの証明書を 1 つ生成するには、次の手順を実行します。

1. クレデンシャルを使用して証明書プロビジョニング ポータルにログインします。
2. [処理の選択（I want to）] ドロップダウン リストから、[単一の証明書の生成（証明書署名要求なし）（generate single certificate (no certificate signing request)）] を選択します。
3. [共通名（Common Name）] フィールドにユーザ名（証明書プロビジョニング ポータルへのログインに使用したユーザ名）を入力します。
4. [サブジェクト代替名（SAN）（Subject Alternative name (SAN)）] フィールドに、証明書を要求するデバイスの MAC アドレスを入力します。
5. 証明書テンプレートを選択します。
6. （任意）説明を入力します。
7. 証明書のダウンロード形式を選択します。
8. クライアント証明書を保護するためのパスワードを入力します。デバイスでこの証明書をインストールするときに、このパスワードを入力する必要があります。
9. [生成（Generate）] をクリックします。

システムにダウンロードできる証明書の zip ファイルが生成されます。

### 共通名（CN）とは何ですか。

認証サーバは、クライアント証明書の [共通名（Common Name）] フィールドに示された値を使用してユーザを認証します。[共通名（Common Name）] フィールドにユーザ名（証明書プロビジョニング ポータルへのログインに使用したユーザ名）を入力します。

### サブジェクト代替名（SAN）とは何ですか。サポートされる形式を教えてください。

サブジェクト代替名（SAN）とは、さまざまな値をセキュリティ証明書に関連付けられるようにする X.509 拡張です。Cisco ISE リリース 2.0 は MAC アドレスのみをサポートしています。したがって、[SAN/MACアドレス（SAN/MAC address）] フィールドには、デバイスの MAC アドレスを次のいずれかの形式で入力してください。

- 00-11-22-33-44-55
- 00:11:22:33:44:55
- 0011.2233.4455
- 001122-334455
- 001122334455

### 証明書テンプレートとは何ですか。

証明書テンプレートは、認証局（CA）がエンド エンティティに証明書を発行する際に使用されます。Cisco ISE 管理者が証明書テンプレートを作成し、要求の検証および証明書の発行時に CA が使用する一連のフィールドを定義します。[共通名（Common Name）]（CN）などのフィールドが要求の検証に使用されます（CN はユーザ名と一致する必要があります）。他のフィールドは、CA が証明書を発行する際に使用されます。

### 使用できる証明書形式を教えてください。

エンド エンティティ証明書は次のいずれかの形式でダウンロードできます。ここで使用する「エンド エンティティ」は、証明書が発行されるユーザまたはデバイスを指します。

- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンド エンティティの証明書と秘密キーを格納するバイナリ形式。
- PKCS12 形式（証明書とキーの両方で 1 ファイル）：1 つの暗号化ファイルにエンド エンティティ証明書と秘密キーを格納するバイナリ形式。
- プライバシー強化電子メール（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート CA 証明書、中間 CA 証明書、およびエンド エンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンド エンティティの秘密キーは PKCS8 PEM を使用して格納され、開始タグは「----------BEGIN ENCRYPTED PRIVATE KEY-----」、終了タグは「-----END ENCRYPTED PRIVATE KEY-----」です。
- PEM 形式の証明書、PKCS8 PEM 形式のキー：エンド エンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンド エンティティの秘密キーは PKCS8 PEM を使用して格納され、開始タグは「----------BEGIN ENCRYPTED PRIVATE KEY-----」、終了タグは「-----END ENCRYPTED PRIVATE KEY-----」です。

### 証明書パスワードはなぜ必要なのですか。従う必要があるパスワード規則はありますか。

証明書パスワードは証明書を保護するために必要です。証明書の内容を確認してデバイスに証明書をインポートするには、証明書パスワードを入力する必要があります。パスワードは、以下の規則に従う必要があります。

- パスワードには大文字、小文字、および数字を少なくとも 1 つずつ使用してください。
- パスワードの長さは 8 ～ 15 文字にする必要があります。
- 使用できる文字は、A ~ Z、a ~ z、0 ～ 9、_、# です。

### 証明書署名要求（CSR）とは何ですか。取得方法を教えてください。

証明書署名要求（CSR）とは、エンド エンティティ（ユーザまたはデバイス）から認証局（CA）に送信される証明書の要求です。CSR にはエンドエンティティを識別する重要な情報（共通名、サブジェクト代替名、部門名など）が含まれています。OpenSSL は CSR の生成に使用される最も一般的なツールの 1 つです。CSR の取得方法については管理者にお問い合わせください。

### CSR を含む証明書を 1 つ取得するにはどうすればよいですか。

CSR を含む属性付きの証明書を 1 つ生成するには、次の手順を実行します。

1. クレデンシャルを使用して証明書プロビジョニング ポータルにログインします。
2. [処理の選択（I want to）] ドロップダウン リストから、[単一の証明書の生成（証明書署名要求あり）（generate single certificate (with certificate signing request)）] を選択します。
3. CSR の詳細を入力します。
4. 証明書テンプレートを選択します。
5. （任意）説明を入力します。
6. 証明書のダウンロード形式を選択します。
7. クライアント証明書を保護するためのパスワードを入力します。デバイスでこの証明書をインストールするときに、このパスワードを入力する必要があります。
8. [生成（Generate）] をクリックします。

CSR を含む証明書の zip ファイルが生成されます。ファイルをシステムにダウンロードします。

### バルク証明書要求を実行することはできますか。

はい。CSV ファイルを作成して証明書プロビジョニング ポータルにアップロードすることで、バルク証明書要求を行うことができます。

### バルク証明書要求の CSV ファイルを作成するにはどうすればよいですか。1 回の要求で取得できる証明書の数を教えてください。

バルク証明書要求の CSV ファイルを作成するには、次の手順を実行します。

1. クレデンシャルを使用して証明書プロビジョニング ポータルにログインします。
2. [処理の選択（I want to）] ドロップダウン リストから、[証明書の一括生成（generate bulk certificates）] を選択します。
3. [ここでCSVテンプレートをダウンロード（Download CSV template here）] をクリックします。CSV テンプレートがシステムにダウンロードされます。
4. ダウンロードしたファイルを MS Excel などのスプレッドシートで開きます。
5. デバイスの CN と SAN の値を各デバイスの行に入力します。
6. ファイルを保存します。
7. 証明書プロビジョニング ポータルで [アップロード（Upload）] をクリックします。
8. [参照（Browse）] をクリックして、システムから CSV ファイルを選択します。
9. 証明書テンプレートを選択します。
10. （任意）説明を入力します。
11. 証明書のダウンロード形式を選択します。
12. クライアント証明書を保護するためのパスワードを入力します。デバイスでこの証明書をインストールするときに、このパスワードを入力する必要があります。
13. [生成（Generate）] をクリックします。

すべての証明書を含む証明書の zip ファイルが生成されます。ファイルをシステムにダウンロードします。

1 回のバルク証明書要求で最大 500 の証明書を要求できます。

### 既存のバルク証明書要求をキャンセルするにはどうすればよいですか。

バルク証明書要求の処理中に、[証明書生成ステータス（Certificate Generation Status）] ページで [キャンセル（Cancel）] をクリックします。

### 複数のバルク証明書要求を送信できますか。

一度に送信できる要求は 1 つのみです。証明書が生成され、ダウンロードの完了を確認した後で別の要求を送信できます。

### バルク証明書要求の実行中にブラウザを閉じた場合はどうなりますか。

バルク証明書要求の処理中にブラウザを閉じたり、ログアウトしたりすると、[証明書生成ステータス（Certificate Generation Status）] ページに自動的にリダイレクトされます。このページで要求の進行状況を確認できます。証明書の生成が完了したら、概要を表示して生成された証明書をダウンロードできます。

### 他のユーザに代わって証明書を生成することはできますか。

他のユーザの証明書を生成できるのは、管理者権限（スーパー管理者権限または ERS 管理者権限）を持つユーザのみです。他のすべてのユーザは、自分の証明書以外を要求することはできません。

### 証明書の zip ファイルには何が含まれていますか。

選択した証明書のダウンロード形式に応じて、zip ファイルには次の内容が含まれています。

- エンドエンティティの証明書：指定した共通名やサブジェクト代替名などの情報が一致するエンドエンティティの証明書。たとえば Joe というユーザ名の要求者が、MAC アドレス（SAN）11-22-33-44-55-66 のデバイスについて要求を送信した場合、証明書ファイル名は Joe_11-22-33-44-55-66.cer です。
- 秘密キー（属性またはバルク証明書要求を使用する単一の証明書のみ）：エンドエンティティ証明書の秘密キー。Joe というユーザ名の要求者が、MAC アドレス（SAN）11-22-33-44-55-66 のデバイスについて要求を送信した場合、秘密キーのファイル名は Joe_11-22-33-44-55-66.key です。
- 証明書チェーン：Cisco ISE 内部 CA のルート CA までの証明書チェーンに含まれるすべての証明書。
- EAP-TLS 認証時に ISE サーバを信頼するエンドエンティティの場合、次のいずれかのファイルが zip ファイルに含まれています。
  - EAP 証明書チェーン（Cisco ISE サーバ証明書が外部 CA によって署名される場合）
  - Cisco ISE 自己署名証明書（ISE サーバがサーバ認証に自己署名証明書を使用する場合）

### 証明書を使用するにはどうすればよいですか。

ローカル システムに証明書の zip ファイルをダウンロードした後、次の手順を実行します。

1. クライアント デバイスのキー ストアに証明書をインポートします。バルク証明書要求を送信した場合は、関連する MAC アドレス（SAN に基づく）を持つデバイスに、関連するエンドエンティティ証明書と秘密キーをコピーします。
2. EAP-TLS ベースの認証を使用するように無線または有線の設定を変更し、エンドエンティティ証明書を選択します。
3. デバイスをネットワークに接続します。認証は成功するはずです。

次のエラーが表示された場合はどのように対処すればいいですか。

- **無効な要求 - 指定されたCSRのCNが入力されたユーザ名と一致せず、該当ユーザにはERS管理者権限がありません（Invalid request - The given CSR has a CN that doesn't match the provided username, and that user doesn't have ERS Admin）**
  要求の共通名（CN）の値が要求者のユーザ名と一致しないため、このエラー メッセージが表示されます。CN は証明書を要求しているユーザのユーザ名と一致する必要があります。このチェックにより、本人以外が証明書を要求することを防ぎます。ただし、ERS 管理者グループに属するユーザ（管理者ユーザ）は他のユーザに代わって証明書を要求でき、CN が管理者ユーザのユーザ名に一致する必要はありません。

  **回避策**：[共通名（Common Name）] フィールドにユーザ名を入力して要求を再送信します。

- **指定されたCNが無効です。[] " : ; | = , + * ? < >を使用することはできません（The given CN is invalid. Cannot contain [] " : ; | = , + * ? < > characters）**
  このエラー メッセージは、CN に無効な文字が使用されている場合に表示されます。無効な文字には、[ ] " : ; | = , + * ? < > が含まれます。これらの文字は Active Directory ユーザ名で許可されていないため、CN に使用できません。

  **回避策**：有効な CN の要求を再送信します。

- **無効なMACアドレス（Invalid MAC address）**
  MAC アドレスが無効なため、このエラーが表示されます。MAC アドレスの形式は 11-11-11-11-11-11、11:11:11:11:11:11、1111.1111.1111、111111.111111、111111111111 にする必要があります。デリミタの「-」、「,」、「:」、および「.」を除き、MAC アドレスには 0 ～ 9 の数字と A ～ F の文字のみを使用できます。

  **回避策**：サポートされる形式で MAC アドレスを指定し、要求を再送信します。

- **CAサーバエラー - 内部CAへの証明書要求がCNに失敗しました（CA server error - Certificate request to internal CA failed CN）**
  このエラーは Cisco ISE 内部 CA の一般的な障害を示しています。

  **回避策**：要求を再送信します。引き続き要求が失敗する場合は、管理者に問い合わせてください。

- **ISEサーバエラー - 指定されたCSRテキストの形式が誤っています（ISE server error - The given CSR text is malformed）**
  CSR が有効な PEM 形式ではないため、このエラー メッセージが表示されます。

  **回避策**：有効な PEM 形式で CSR を指定します。

- **無効な要求 - 指定されたCSRのOU RDNが、指定の証明書テンプレートに定義された内容と一致しません（Invalid request - The given CSR has an OU RDN that doesn't match what's defined in the provided Certificate Template）**
  OU RDN（またはエラー メッセージに示されている RDN）が証明書テンプレートの内容と一致しないため、このエラー メッセージが表示されます。

  **回避策**：管理者に問い合わせて、CSR で使用する RDN 値を確認してください。

- **このCSVには許容される最大数を超えるエントリが含まれています。最大数は500です（There are more than the max allowed entries in this CSV. Max is 500）**
  提供した CSV ファイルに 500 を超えるエントリが含まれているため、このエラー メッセージが表示されます。

  **回避策**：各ファイルのエントリが 500 以下になるように、複数の CSV ファイルに分割します。バルク証明

書要求の CSV ファイルを 1 つずつ送信します。1 つの要求が完了してから次の要求に進みます。

- **CSVファイルの列が欠落しているか余分な列があります。テンプレートに従ってください（There are either missing or extra columns in the CSV file. Please stick to the template**）
  CSV ファイルの形式が正しくないため、このエラー メッセージが表示されます。

  **回避策**：各エントリにそれぞれ 2 つのフィールドの値（CN と SAN）が指定されていることを確認します。SAN は MAC アドレスである必要があります。要求を再送信します。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。


この資料の記載内容は2016年5月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp