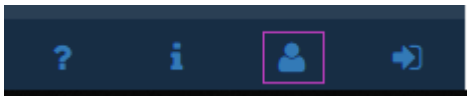
ユーザープロフィール

User profileでは、ユーザーが自身のアカウントに関する詳細を編集したり、パスワードを変更したりすることができます。

User profileにアクセスするには、管理インターフェイスの左下の**Profile**アイコンを選択します。 **Edit profile**と**Change password**の2つのセクションがあります。



> **備考**
>
> すべてのユーザーは自分のユーザープロフィールを管理できます。

プロフィールを編集

ユーザーのアカウント詳細には以下が含まれます：

- **Username (必須)** - 管理インターフェイスにログインするのに使用される名前。
- **First name (必須)** - ユーザーの名前。
- **Last name (必須)** - ユーザーの名字。
- **Email (必須)** - ユーザーの完全修飾電子メールアドレス。**このアドレスは、パスワードリセットやその他のシステム通知を送信するのに使用されます。**
- **Time zone** - 管理ダッシュボード上において表示される日時のローカル・タイムゾーン。
- **Two factor login status (required)** - 現在のユーザーについて2FAの**enable**（有効）または**disable**（無効）を切り替えます。無効化された状態から有効に切り替えると、ユーザーは、画面に表示される手順に従ってGoogle認証システムを使用して2FAをセットアップするように要求されます。
- **Enabled** - ユーザーはログイン時にこのアカウントに関連付けられた認証コードを入力するよう求められます。そうしないとログインが失敗します。
- **Disabled** - 2FAが無効化され、ログイン時に2FAが必要なくなります。

> **重要**
>
> インスタンスで強制2要素認証が有効な場合、ユーザーは2FAを無効化できなくなります。

管理APIクライアント証明書

- **Certificate Algorithm** - AES256 は、新しい暗号化規格を使用してより強固なセキュリティを提供します。LEGACY は、旧来の暗号化規格を使用してより広い互換性を提供します。
- **Tracker** - 有効化すると、証明書がダウンロードされる度にその有効期限が追跡されます。証明書の有効期限まで90日以内になると、 `Business Admin` 及び `System Admin` のロールを持つユーザーへEメール通知が送信されます。
- **Download** - 管理APIリクエストに使用する**.p12**形式の3DSリクエスタークライアント証明書と `metadata.txt` ファイルを圧縮した `zip` ファイルをダウンロードできます。
  `metadata.txt` ファイルには次の情報が含まれています。

  - `P12-Filename` - P12ファイルのファイル名。例：cert-b1cdf956-a4f4-4ce4-ade6-cd84d68e59f2.p12

  - `P12-Password` - 生成されたP12ファイルの安全なランダムパスワード。長さ：16文字

  - `Created-Date` - P12ファイルが生成されたUTC単位の日付と時刻。形式： `yyyy-MM-dd'T'HH:mm:ss` 例：2023-12-12T10:01:15

  - `Expiry-Date` - クライアント証明書ファイルの有効期限が切れるUTC単位の日付と時刻。クライアント証明書ファイルは有効期限が切れると無効になります。有効期限が切れる前に新しいファイルを再ダウンロードしてください。形式： `yyyy-MM-dd'T'HH:mm:ss` 例：2025-12-12T10:01:15

  > **クライアント証明書の有効期限切れ**
  >
  > ダウンロードされたクライアント証明書には、セキュリティ上の理由から、ダウンロード日から**2年間の有効期限**があります。すべての証明書がこの有効期限の前に更新されていることを確認してください。**有効期限が切れてしまった場合、APIリクエストはエラー**になり認証は拒否されます。

この機能の詳細については、APIドキュメントの概要を参照してください。

- **Revoke** - セキュリティが侵害された場合、現在のクライアント証明書を失効させ、新しいIDで証明書を再発行します。

> **警告**
>
> **Revoke**した場合過去に発行されたクライアント証明書は失効され、新しいクライアント証明書をダウンロードするまではAPIリクエストができなくなります。

認証APIマスタークライアント証明書

ActiveServerは、ここで説明されているように認証APIではX.509認証を使用してユーザーを認証します。決済代行会社等が加盟店に代わって**ActiveServer**に接続する必要がある場合、すべての加盟店ユーザーの複数のクライアント証明書の保存を避けたい場合に重宝されます。 **認証APIマスタークライアント証明書**をマーチャントトークンと組み合わせて使用して、加盟店に代わって**ビジネス管理者ユーザー**を認証できます。マーチャントトークンでマスター証明書を使用する方法については、こちらを参照してください。

> **重要**
>
> **ビジネス管理者**のみこの証明書を管理できます。すべての加盟店に代わって認証に使用できるため注意が必要です。安全な場所に保管しましょう。

> **注意**
>
> 認証APIマスタークライアント証明書をダウンロードした際のユーザーを**削除**した場合、 そのユーザーに紐づく証明書は無効化されてしまいます。別のユーザーでダウンロードした新しい証明書を適用せずにユーザーを削除してしまった場合、取引がすべて失敗してしまう恐れがあります。

- **Certificate Algorithm** - AES256 は、新しい暗号化規格を使用してより強固なセキュリティを提供します。LEGACY は、旧来の暗号化規格を使用してより広い互換性を提供します。
- **Tracker** - 有効化すると、証明書がダウンロードされる度にその有効期限が追跡されます。証明書の有効期限まで90日以内になると、 `Business Admin` 及び `System Admin` のロールを持つユーザーへEメール通知が送信されます。
- **Download** - 全ての加盟店の代わりに認証APIリクエストを実行できる、**.p12**形式の3DSリクエスターマスタークライアント証明書と `metadata.txt` ファイルを圧縮した `zip` ファイルをダウンロードできます。 `metadata.txt` ファイルには次の情報が含まれています。

  - `P12-Filename` - P12ファイルのファイル名。例：cert-b1cdf956-a4f4-4ce4-ade6-cd84d68e59f2.p12

- `P12-Password` - 生成されたP12ファイルの安全なランダムパスワード。長さ：16文字

- `Created-Date` - P12ファイルが生成されたUTC単位の日付と時刻。形式： `yyyy-MM-dd'T'HH:mm:ss` 例：2023-12-12T10:01:15

- `Expiry-Date` - クライアント証明書ファイルの有効期限が切れるUTC単位の日付と時刻。クライアント証明書ファイルは有効期限が切れると無効になります。有効期限が切れる前に新しいファイルを再ダウンロードしてください。形式： `yyyy-MM-dd'T'HH:mm:ss` 例：2025-12-12T10:01:15

> **クライアント証明書の有効期限切れ**
>
> ダウンロードされたクライアント証明書には、セキュリティ上の理由から、ダウンロード日から**2年間の有効期限**があります。すべての証明書がこの有効期限の前に更新されていることを確認してください。**有効期限が切れてしまった場合、APIリクエストはエラー**になり認証は拒否されます。

この機能の詳細については、APIドキュメントの概要を参照してください。

- **Revoke** - セキュリティが侵害された場合、現在のクライアント証明書を失効させ、新しいIDで証明書を再発行します。

> **警告**
>
> **Revoke**した場合過去に発行されたクライアント証明書は失効され、新しいクライアント証明書をダウンロードするまではAPIリクエストができなくなります。

CA証明書

- **Download** - 管理APIにリクエストを送信する際に必要なサーバーCA証明書をダウンロードします。この機能の詳細については、APIドキュメント概要を参照してください。

> **Tip**
>
> **管理APIクライアント証明書**と**CA証明書**の機能はアクティブ化されたインスタンスでのみご利用可能です。

> **バージョン1.0.3**
>
> 証明書のダウンロードはバージョン1.0.3で追加されました。

パスワード変更

ユーザーは以下のフィールドを入力することでパスワードを変更できます。

- **Current password (必須)** - ユーザーの現在のパスワード。正しくない場合は、パスワードの変更が失敗します。
- **New password (必須)** - ユーザーの新しいパスワード。パスワード履歴チェックルールを確認する必要があります。
    - *Requirements - 8～100文字で、少なくとも1つの文字と1つの数字を含む必要があります。*
- **Confirm new password** - ユーザーの新しいパスワード。**New password**フィールドと一致する必要があります。