

# User profile

The **User profile** allows users to edit details relating to their own account and change their passwords.

Select the **Profile** icon in the bottom left hand corner of the administration interface to access your **User profile**. There are two sections, **edit profile** and **change password**.



## Note

All users are able to manage their own user profile.

## Edit profile

Contains the account details for the user:


- **Username (required)** - name used to login to the administration interface.
- **First name (required)** - first name of the user.
- **Last name (required)** - last name of the user.
- **Email (required)** - fully qualified email address of the user. **This address will be used to send password reset and other system notifications.**
- **Time zone** - local timezone for all time and dates to be displayed in on the administration interface.
- **Two factor login status (required)** - toggle to **enable** or **disable** 2FA for the current user. Toggling from disabled to enabled will prompt the user to setup 2FA using Google Authenticator by following the steps displayed on screen.
- **Enabled** - prompts the user on login to enter the authenticator code associated with this account, otherwise login will fail.
- **Disabled** - 2FA is disabled and not required on login.

 **Important**

If the instance has [Force two factor login](#) enabled, the user will not be able to disable 2FA.

## Admin API client certificate

- **Certificate Algorithm** - AES256 provides stronger security using modern encryption standards. LEGACY provides broader compatibility using older encryption standards.
- **Tracker** - When enabled, the expiry date is tracked each time a certificate is downloaded. Business Admins and System Admins will receive an email notification when the certificate is 90 days or less away from expiring.
- **Download** - allows the download of the client certificate for the user, to be used in Admin API requests. The downloaded zip file contains a `metadata.txt` file with the following information:
  - **P12-Filename** - The filename of the P12 file. Example: cert-b1cdf956-a4f4-4ce4-ade6-cd84d68e59f2.p12
  - **P12-Password** - The generated secure random password of the P12 file. Length: 16 characters
  - **Created-Date** - The date and time in UTC which the P12 file was generated. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2023-12-12T10:01:15
  - **Expiry-Date** - The date and time in UTC which the client certificate file will be expired. The client certificate file will be invalid after the expiry date, please re-download a new one before the expiry date. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2025-12-12T10:01:15

 **Client certificate expiry**

Downloaded client certificates have a **2 year expiry** from date of download for security reasons. Ensure that all certificates are renewed before this expiry date, **otherwise API requests will be rejected due to an expired certificate error.**

For more information on this functionality, see the [API document overview](#).

- **Revoke** - revokes the current client certificate if the security has been compromised and re-issues a certificate with new ID.

 **Warning**

**Revoking** a client certificate will invalidate all instances of the certificate, and you will not be able to initiate API requests until the replacement certificate is downloaded.

## Master Auth API client certificate

**ActiveServer** uses X.509 authentication to authorise users using the auth API, described [here](#). If the user is a PSP that connects to **ActiveServer** on behalf of merchants, they may wish to avoid storing multiple client certificates for all merchants users. The **Master Auth API client certificate** can be used in combination with a [Merchant token](#) to authenticate a **Business Admin user** on behalf of a merchant. For information on using the master certificate with the merchant token, refer [here](#).

 **Important**

Only a **Business admin** can manage this certificate. As it can be used to authenticate on behalf of all merchants, special care should be taken in order to protect its security.

 **Attention**

**Deleting** a user with a Master Auth API client certificate, will invalidate the certificate linked to that user. You must apply a new certificate before deleting the user, or all the transactions will fail.

- **Certificate Algorithm** - AES256 provides stronger security using modern encryption standards. LEGACY provides broader compatibility using older encryption standards.
- **Tracker** - When enabled, the expiry date is tracked each time a certificate is downloaded. Business Admins and System Admins will receive an email notification when the certificate is 90 days or less away from expiring.
- **Download** - allows the download of the client certificate for the user, to be used for Authentication API requests for all merchants. The downloaded zip file contains a `metadata.txt` file with the following information:
  - **P12-Filename** - The filename of the P12 file. Example: cert-ba-b1cdf956-a4f4-4ce4-ade6-cd84d68e59f2.p12

- **P12-Password** - The generated secure random password of the P12 file. Length: 16 characters
- **Created-Date** - The date and time in UTC which the P12 file was generated. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2023-12-12T10:01:15
- **Expiry-Date** - The date and time in UTC which the client certificate file will be expired. The client certificate file will be invalid after the expiry date, please re-download a new one before the expiry date. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2025-12-12T10:01:15

#### Client certificate expiry

Downloaded client certificates have a **2 year expiry** from date of download for security reasons. Ensure that all certificates are renewed before this expiry date, **otherwise API requests will be rejected due to an expired certificate error.**

For more information on this functionality, see the [API document overview](#).

- **Revoke** - revokes the current client certificate if the security has been compromised and re-issues a certificate with new ID.

#### Warning

**Revoking** a client certificate will invalidate all instances of the certificate, and you will not be able to initiate API requests until the replacement certificate is downloaded.

## CA certificates

- **Download** - allows the download of the servers CA certificates, to be used in Admin API requests. For more information on this functionality, see the [API document overview](#).

#### Tip

**Admin API client certificate** and **CA certificate** management is only available once the instance has been [activated](#).

 **Version 1.0.3**

Certificate download was added in the version 1.0.3 release.

## Change password

Allows the user to change their password by filling in the following fields:

- **Current password (required)** - current password for the user, must be correct or password change will fail.
- **New password (required)** - new password for the user, must conform to the [Password history check](#) rules.
  - **Requirements** - *Between 8 and 100 characters, must contain at least one letter and one number.*
- **Confirm new password** - new password for the user, must match **New password** field.