How to ensure security on a compromised SecureAuth OTP App

Introduction

SecureAuth OATH OTP apps can be configured to wipe all provisioned data if the end-user supplies an invalid PIN the maximum set number of times. The app screen can be configured to automatically lock after a specified number of seconds.

Description / Definition

Failed Wipe	The app will automatically delete any user-specific provisioned data if someone enters an invalid PIN 'X number' of consecutive times – this number is configurable by the enterprise administrator
Screen Timeout	The app will automatically lock itself by presenting the PIN screen after 'X number' of seconds have elapsed – this number is configurable by the enterprise administrator

NOTE: Both features are only applicable if the PIN Lock screen feature is enabled

Applies to

SecureAuth IdP Version	SecureAuth OTP App
8.0+	All supported OTP apps (see Mobile Apps)

Prerequisites

1. Ensure the iOS or Android version is supported by checking **here**

2. Download and install the SecureAuth mobile app on the device(s) to be enrolled

   - **iOS**: https://itunes.apple.com/us/app/secureauth-otp/id615536686
   - **Android**: https://play.google.com/store/apps/details?id=secureauth.android.token

3. Configure the **OATH Provisioning Realm** / **App Enrollment Realm** in the SecureAuth IdP Web Admin for end-users to register their device(s) for OATH OTP / Multi-Factor App Enrollment

   - SecureAuth IdP 8.0 - OATH Seed Realm Configuration Steps
   - SecureAuth IdP 8.1 - OATH OTP Realm Configuration Steps
   - SecureAuth IdP 8.2 - SecureAuth App Enrollment Realm Configuration Steps
   - SecureAuth IdP 9.0.x - Multi-Factor App Enrollment (URL) Realm Configuration Steps
   - SecureAuth IdP 9.1+ - Multi-Factor App Enrollment (URL) Realm Configuration Steps

   NOTE: The name of the provisioning / enrollment realm has changed since the release of SecureAuth IdP version 8.0 – as of version 9.0.x, the realm is called **Multi-Factor App Enrollment Realm** which is the name used throughout this document

4. Configure SecureAuth IdP realm(s) in which OATH OTPs are used for Multi-Factor Authentication

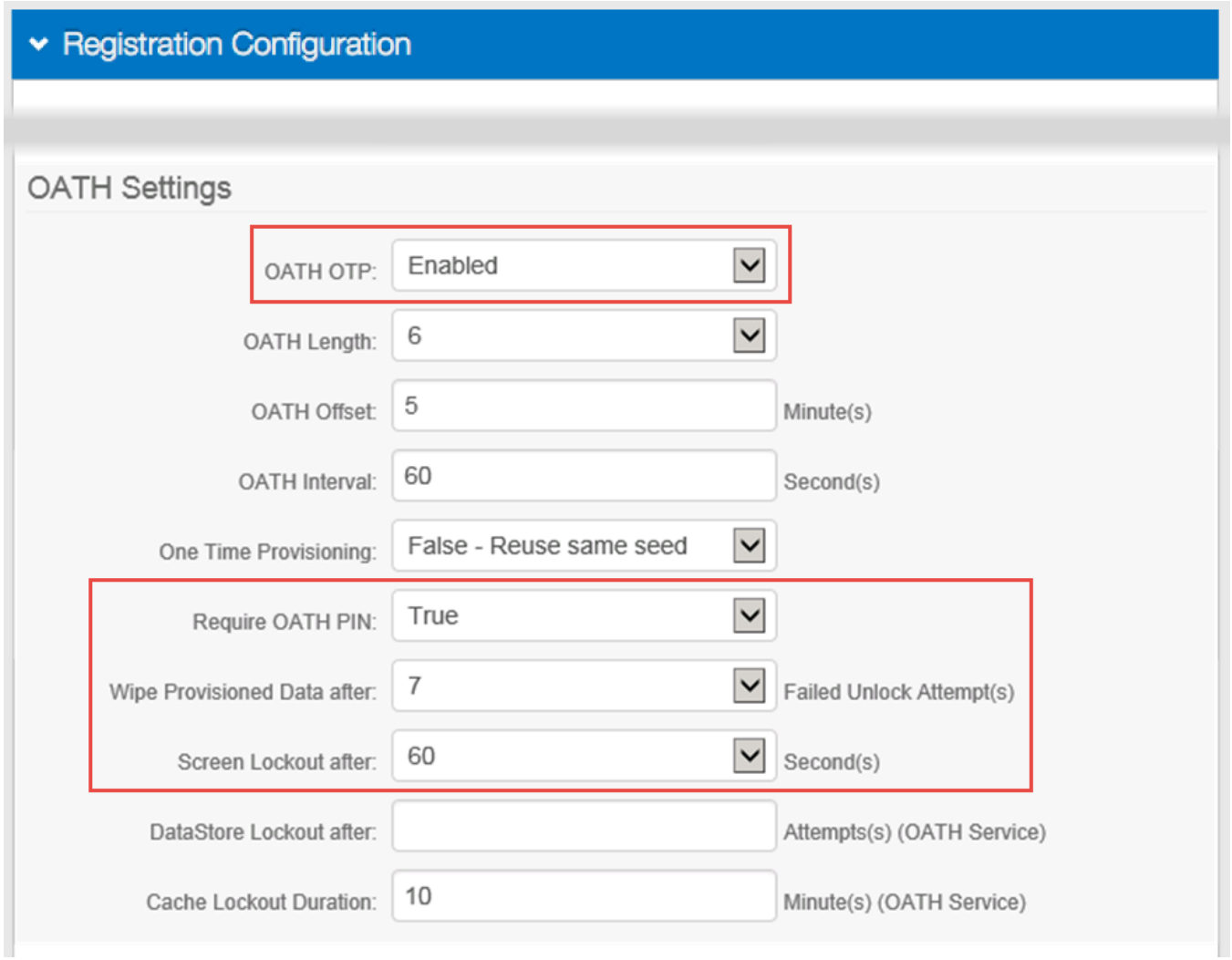
SecureAuth IdP Configuration Steps

1. If using SecureAuth IdP version 8.0, configure OATH settings starting on the **Registration Methods** tab

   If using SecureAuth IdP versions 8.1 to 9.x, configure OATH settings starting on the **Post Authentication** tab

Version 8.0

Registration Configuration



2. Scroll down to the OATH Settings section

3. If setting **Require OATH PIN** to **True**, optionally set values from the dropdowns for

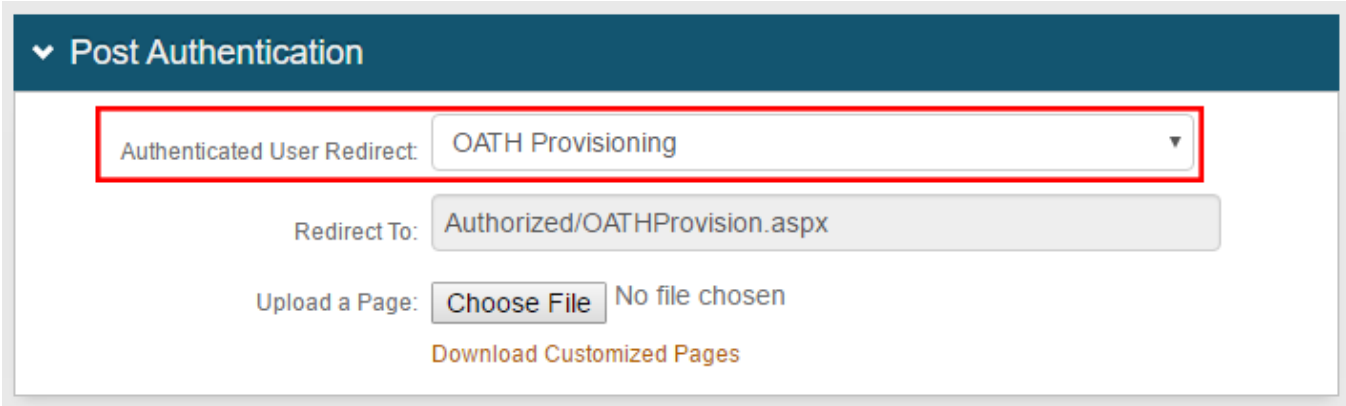
    a. **Wipe Provisioned Data after**: specify the maximum number of Failed Unlock Attempt(s) permitted, after which provisioned data will be wiped from the app

    b. **Screen Lockout after**: specify the number of Second(s) after which the app screen will lock out the end-user

Click **Save** once the configuration has been made before leaving the **Registration Methods** page to avoid losing changes

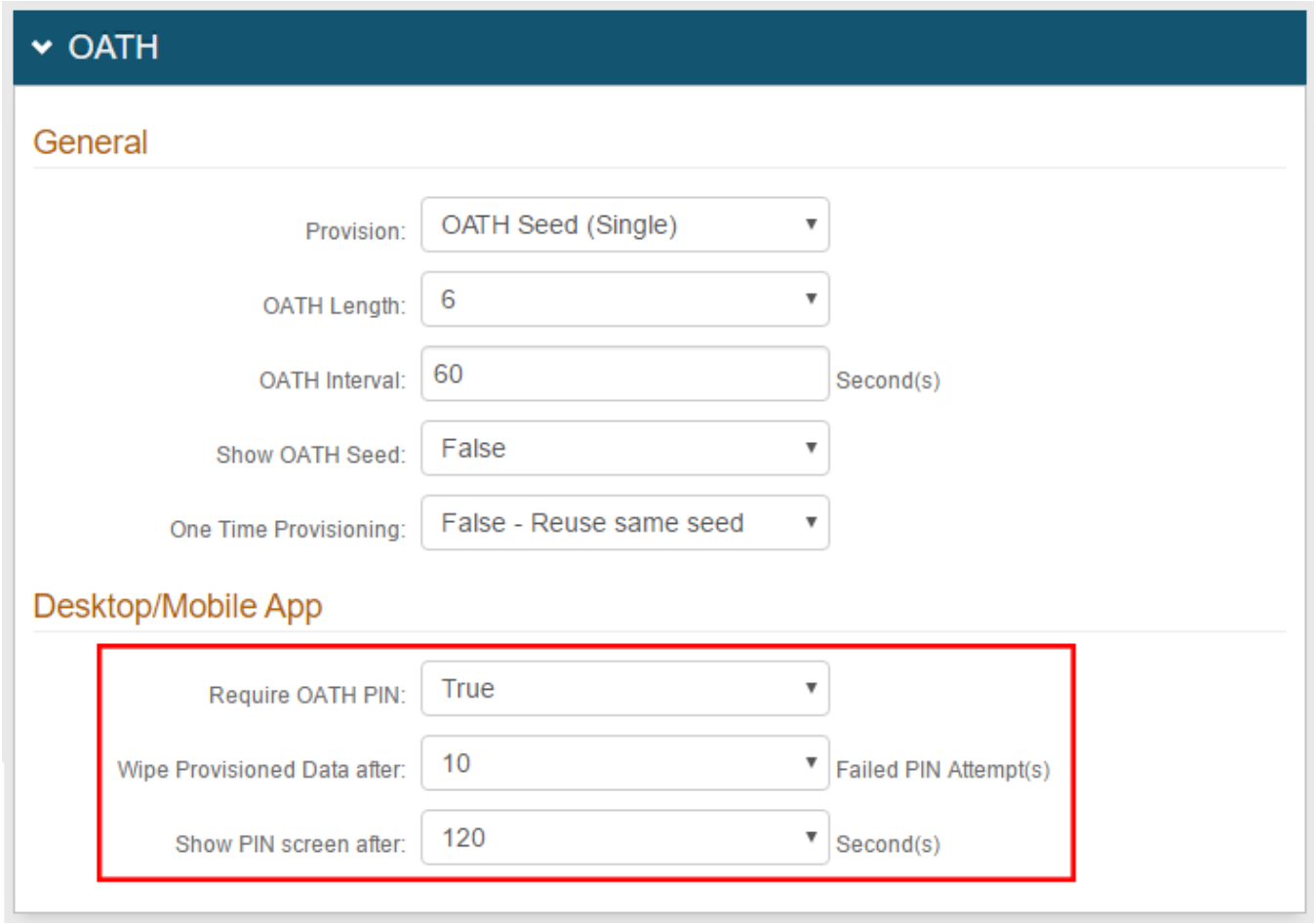
Version 8.1

Post Authentication



2. Select **OATH Provisioning** from the **Authenticated User Redirect** dropdown

OATH



3. In the **Desktop / Mobile App** section, if setting **Require OATH PIN** to **True**, optionally set values from the dropdowns for

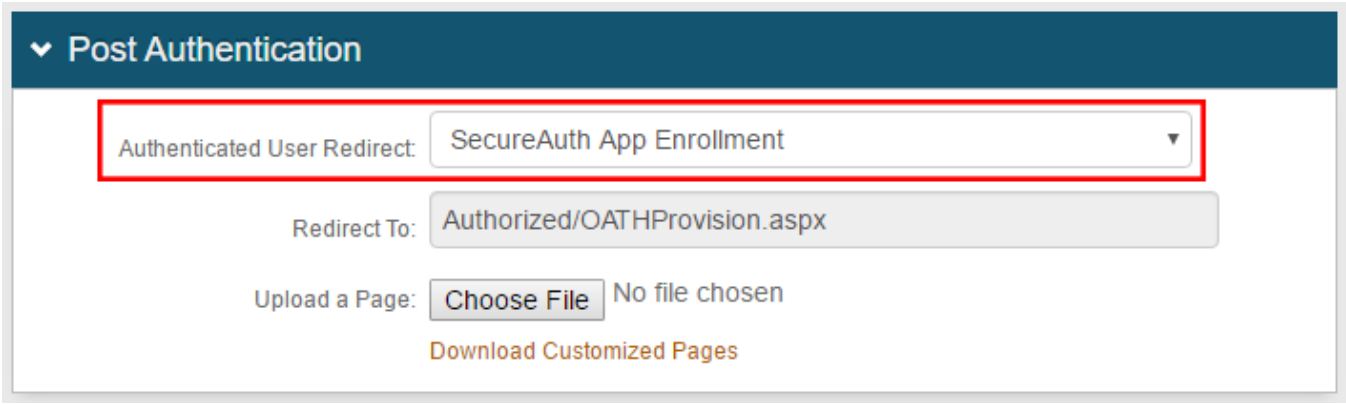
   a. **Wipe Provisioned Data after**: specify the maximum number of Failed PIN Attempt(s) permitted, after which provisioned data will be wiped from the app

   b. **Show PIN screen after**: specify the number of Second(s) after which the PIN screen will appear

Click **Save** once the configuration has been made before leaving the **Post Authentication** page to avoid losing changes

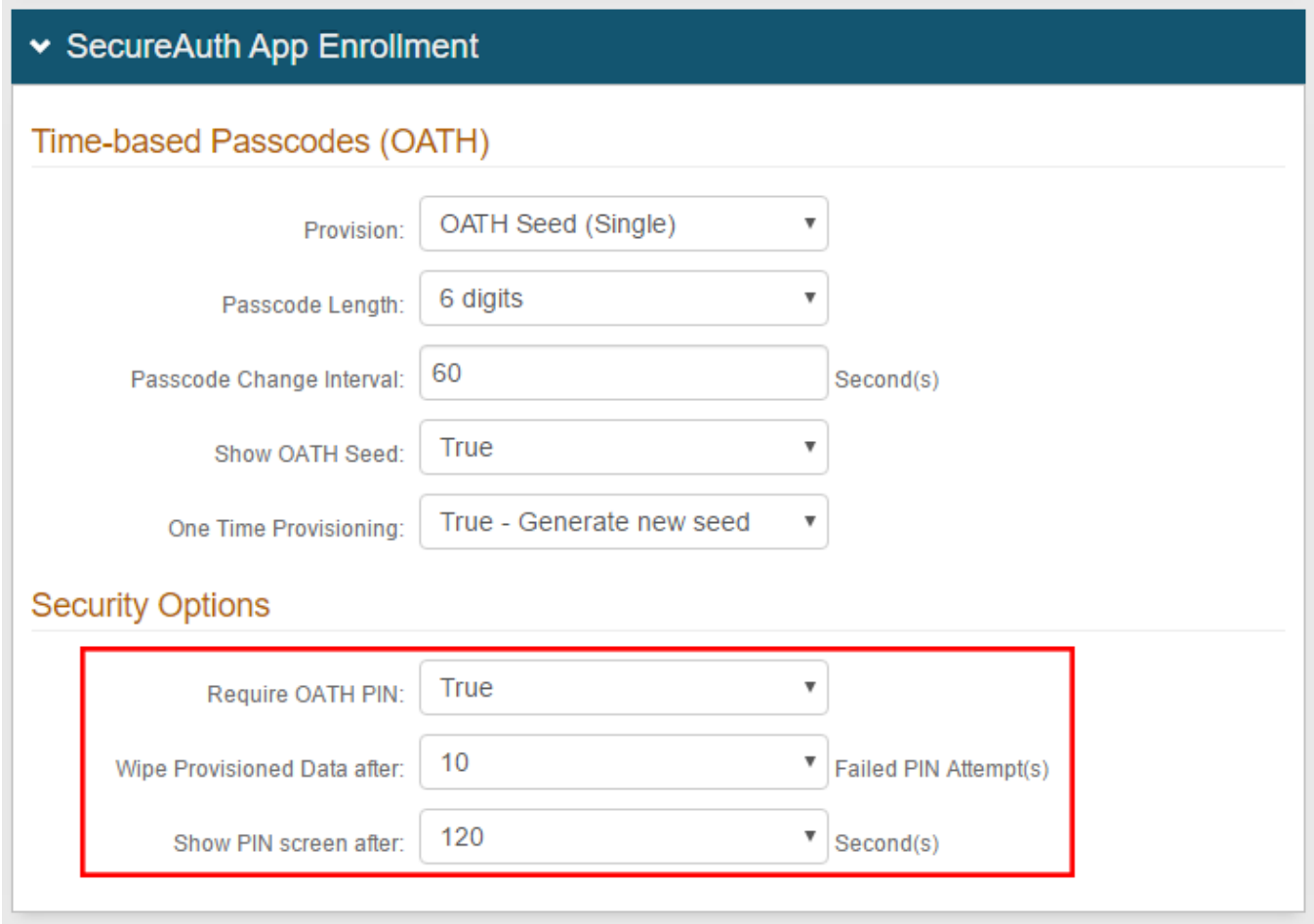
Version 8.2

Post Authentication



2. Select **SecureAuth App Enrollment** from the **Authenticated User Redirect** dropdown

SecureAuth App Enrollment



3. In the **Security Options** section, if setting **Require OATH PIN** to **True**, optionally set values from the dropdowns for

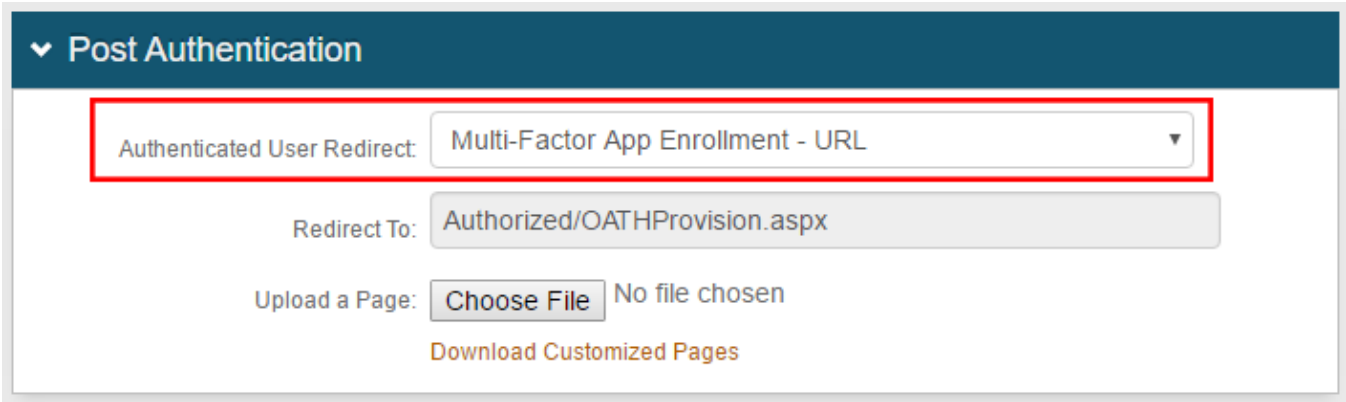
   a. **Wipe Provisioned Data after**: specify the maximum number of Failed PIN Attempt(s) permitted, after which provisioned data will be wiped from the app

   b. **Show PIN screen after**: specify the number of Second(s) after which the PIN screen will appear

Click **Save** once the configuration has been made before leaving the **Post Authentication** page to avoid losing changes

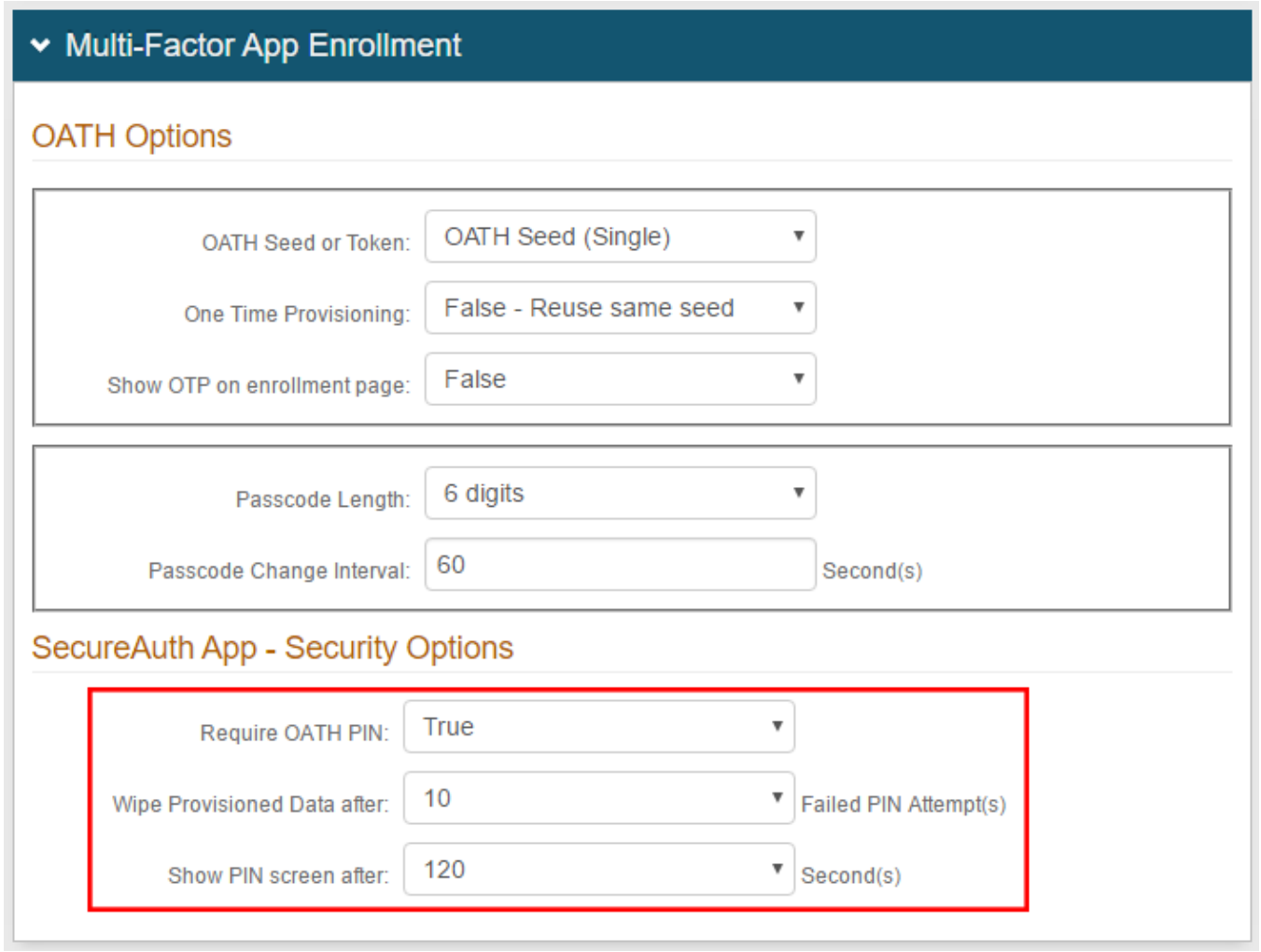
Version 9.x

Post Authentication



2. Select **Multi-Factor App Enrollment - URL** from the **Authenticated User Redirect** dropdown

Multi-Factor App Enrollment



3. In the **Security Options** section, if setting **Require OATH PIN** to **True**, optionally set values from the dropdowns for

a. **Wipe Provisioned Data after**: specify the maximum number of Failed PIN Attempt(s) permitted, after which provisioned data will be wiped from the app

b. **Show PIN screen after**: specify the number of Second(s) after which the PIN screen will appear

Click **Save** once the configuration has been made before leaving the **Post Authentication** page to avoid losing changes

Troubleshooting / Common Issues
Ensure the mobile app is the latest version from the app store
Ensure the device platform supports this functionality by checking **here**