SecureAuth Authenticate app for iOS and Android v5.2

Introduction

The SecureAuth Authenticate mobile app provides a Multi-Factor Authentication method for end-user validation during the login process.

The Authenticate app must first be installed on your mobile device and then connected to your user profile via a SecureAuth IdP mobile app enrollment realm before it can be used.

Once connected, the app can generate Time-based Passcodes (OATH TOTP), Push Notification One-time Passcodes (OTPs), and/or Push-to-Accept / Symbol-to-Accept login requests for you to use when authenticating to access a protected resource.

CONTENTS OF THIS DOCUMENT:

- What's new in SecureAuth Authenticate app v5.2
  - SecureAuth Authenticate app – iOS
  - Earlier versions of SecureAuth Authenticate App
- Prerequisites
  - Connect an account to your user profile
    - Choose the Connection Type
      - Connect with QR Code
      - Connect with URL
  - Login Requests from Push Notifications
    - Different ways to accept Login Requests
      - Accept request received on the app
      - Accept request from a notification on the app
      - Accept request on a paired watch
      - Accept symbol on a paired watch
  - App account management
    - Copy a passcode
    - Delete an account
    - Re-connect an account
    - Rename an account
  - PIN creation and management
    - Create a PIN
    - Create a new PIN
    - Change a PIN
    - Enter a PIN
- Release notes
- Related documentation

What's new in SecureAuth Authenticate app v5.2

- Rebranding.
- Minor bug fixes.
- For iOS: Support for customizable PIN to access a TOTP passcode from the app – see SecureAuth Authenticate app – iOS.

SecureAuth Authenticate app – iOS

A PIN entry (4, 6, 8, or 10 digits) may be required to view the TOTP on the app. This custom security option is configured on the QR code / URL app enrollment realm running on SecureAuth IdP version 9.3.
Tapping the settings cog – which replaces the question mark icon on the Accounts screen – opens the Settings screen with options to change the app PIN or to send a request to SecureAuth Support.
Earlier versions of SecureAuth Authenticate App

See SecureAuth Authenticate App for Android and iOS v5.x for information about features supported in earlier versions of this application.

Prerequisites

1. Ensure the version on the mobile device / paired watch is supported:
   - SecureAuth Compatibility Guide

2. Download and install SecureAuth Authenticate App:

3. Find out which SecureAuth IdP app enrollment realm (version 9.3) you should use to:
   - Enroll the app and provision it for Multi-Factor Authentication usage (if you do not have the app installed), or
   - Re-enroll the app for Multi-Factor Authentication usage if you are upgrading from version 5.0.x or 5.1.x to version 5.2.
   - IMPORTANT:
     - If the app enrollment realm requires you to use a QR code to connect, ensure the mobile device has a working camera.
     - If the app enrollment realm requires you to enter a URL to connect, get the web address of the app enrollment realm – see Connect with URL.

4. Follow the steps in Connect an account to your user profile below.

   NOTE: Push notifications must be enabled on the mobile device to use the login request feature on the app. Push notification enablement can be applied when the app is started or through the device’s setting.
Connect an account to your user profile

Choose the Connection Type

1. Start the app and tap the + icon.

2. Choose either Connect with URL or Connect with QR code and follow the workflow for that option.

Connect with URL

Connect with QR code

Ask your administrator for the URL or QR Code, then tap the “+” button to enroll the account.

Connect with QR Code

1. Use a device other than the one being provisioned – example: desktop, laptop – to access the login page of the QR code realm.

2. After successfully logging on the realm, use the app to scan the unique QR code on the page – this code is only valid for 10 minutes.

3. Create a PIN on the app if required – see Create a PIN.

4. If the account is successfully connected, a 6 or 8-digit passcode appears on the app.

5. Input that passcode in the Confirm box on the QR code realm page, and click Enable.

6. Tap Finished on the app.
Connect with URL

1. Enter the web address of the Multi-Factor Authentication app enrollment realm on the app.

   If the default URL realm SecureAuth998 is used, then you only need to enter the Fully Qualified Domain Name – example: secureauth.company.com

   If a different realm is used for Multi-Factor Authentication URL app enrollment, then the entire URL address that includes the realm name is required – example: https://secureauth.company.com/secureauth2

Enter Web Address

Enter web address provided by your administrator or enrollment page.

Web address

You will have to log in to connect your account.

Continue to Login
2. Select the Multi-Factor Authentication method to use for delivering the passcode you will use to connect your account.

3. After receiving the passcode and entering it on the app, you may be required to create a PIN – see Create a PIN.

4. Once the account is connected, it is listed on the Accounts screen and is available to use on the app.

Login Requests from Push Notifications

Different ways to accept Login Requests

Accept request received on the app

Tap Approve this request on the Login Request screen.
Accept request from a notification on the app

1. Swipe down on the Push Notification on the locked screen.
2. Tap to approve the request on the expanded notification on the screen.
Accept request on a paired watch

Tap Approve on the paired Apple Watch.
Accept symbol on a paired watch

1. When a symbol is presented on the Multi-Factor Authentication page, a Login Request is simultaneously dispatched to the enrolled account on the mobile device app and the paired watch.
2. Accept the correct symbol on the paired watch or on the mobile device app.

App account management

Copy a passcode
1. Tap the account to go to the Passcode screen.

2. Tap the passcode to copy it to the clipboard.

Delete an account

1. Use one of two methods:
   - Tap Edit, or
   - Swipe left on the account and tap Delete.
Re-connect an account

1. Swipe left on the account.
2. Tap Re-connect.
Rename an account

1. Tap Edit to go to the next screen.

2. Edit the account name and tap Done.
PIN creation and management

SecureAuth Authenticate app version 5.2 for iOS includes an optional security feature which, if configured on a SecureAuth IdP version 9.3 or later app enrollment realm, requires the setup and entry of a PIN to view the TOTP on the app.

PIN VALUE RESTRICTIONS:
- Cannot contain consecutive, repeating digits – example: 33333333 or 1111
- Cannot be forward or backwards sequential – example: 123456 or 87654321

PIN RULES:
- If upgrading from an earlier 5.x version of the app, then you are prompted to create a PIN and re-connect to your profile if the realm requires a PIN.
- An account on the app must be re-enrolled for Multi-Factor Authentication if the connected realm now requires a PIN entry.
- If accounts on the app use different PIN lengths, then the highest security setting (maximum 10 digits) is enforced to view the TOTP on the app.
- To apply the highest security setting to all accounts, you must re-enroll accounts that are not using the highest security setting.
- If multiple accounts exist on the app, you must create a new PIN whenever you:
  - Add an account that requires a higher security setting, or
  - Delete the account that used the highest security setting.

NOTE: Apple Watch and Android Wear OS watch integrations are not supported with the PIN-protected configuration in Authenticate App version 5.2.

Create a PIN

You are prompted to create a secure PIN with a specified number of digits (4, 6, 8, or 10) and to confirm the entry of that PIN during the app enrollment process.
Create a new PIN

You are prompted to create a secure PIN with a specified number of digits (4, 6, 8, or 10) when adding or deleting an account on the app.
Choose PIN

You must create a new PIN because you are adding or deleting an account.

PIN must not have repeating or sequential digits.

Change a PIN

1. Tap the settings cog on the Accounts screen.
2. Tap Change PIN on the next screen.
3. Go through the PIN creation workflow to create a new PIN.
Enter a PIN

Enter the PIN you created to unlock the app to use an account to validate yourself on a realm.
Release notes

Version 5.2 release date:

- 11/27/2018

What’s new:

- Rebranded user interface.
- Minor bug fixes.
- For iOS: Support for the optional security feature requiring a custom PIN (4, 6, 8, or 10 digits) to access a TOTP passcode from the app.

Known issue:

- Android 5 OS and earlier may not show the new logo rebranding.
- End users must accept notifications during Authenticate app installation on mobile devices; otherwise, device registration will fail.
This scenario occurs when a SecureAuth IdP 9.3 enrollment realm TOTP seed is set to Token mode. If SecureAuth IdP is configured for Seed mode, registration of mobile devices will succeed even if the user does not accept push notifications.

Related documentation

- Multi-Factor App Enrollment (QR Code) realm configuration
- Multi-Factor App Enrollment (URL) realm configuration
- Mobile Login Requests (Push Notifications) Registration Method for Multi-Factor Authentication
- Time-based Passcodes (OATH) Registration Method for Multi-Factor Authentication
- SecureAuth Authenticate App Troubleshooting
- How to Pair the SecureAuth Authenticate App on a Mobile Device and Watch
- SecureAuth Authenticate App for Android and iOS v5.x