SecureAuth Authenticate App for Android and iOS v5.x

**Introduction**

The SecureAuth Authenticate mobile app enables Multi-Factor Authentication during the login process. The Authenticate app must be connected to a user profile via a SecureAuth IdP mobile app enrollment realm or a Cloud Access account before it can be used.

The latest version of the app improves the end-user experience by eliminating the app PIN. Additionally, OATH seed storage security is increased by tying seed encryption to the screen lock. Users must enable the mobile device's screen lock for the app to function.

Refer to the NEW section and Release Notes for more information about the v5.x releases.

**Supported Features by App Version**

<table>
<thead>
<tr>
<th>Feature</th>
<th>App Version</th>
<th>SecureAuth IdP Versions</th>
<th>Cloud Access Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party app support on Android devices</td>
<td>v5.1</td>
<td>9.1+</td>
<td>All</td>
</tr>
<tr>
<td>Application Security, User Experience Enhancements</td>
<td>v5.0+</td>
<td>8.0+</td>
<td>All</td>
</tr>
<tr>
<td>Symbol-to-Accept</td>
<td>v5.0+</td>
<td>9.0+</td>
<td>All</td>
</tr>
<tr>
<td>Push-to-Accept notifications on Android Wear OS Smartwatch (Accept / Deny)</td>
<td>v4.6+</td>
<td>8.2+</td>
<td>--</td>
</tr>
<tr>
<td>Strong PIN enforcement</td>
<td>v4.5 - v4.7</td>
<td>8.0+</td>
<td>--</td>
</tr>
<tr>
<td>Biometric Unlock using Touch ID on iOS and Fingerprint Unlock on Android</td>
<td>v4.4 - v4.7</td>
<td>9.0+</td>
<td>--</td>
</tr>
<tr>
<td>QR Code mobile app enrollment</td>
<td>v4.3+</td>
<td>9.0+</td>
<td>--</td>
</tr>
<tr>
<td>Push-to-Accept notifications (Accept / Deny request)</td>
<td>v4.1+</td>
<td>8.2+</td>
<td>--</td>
</tr>
<tr>
<td>Push Notification alerts (OTP sent to home screen of mobile device)</td>
<td>v4.0+ and prior</td>
<td>8.0+</td>
<td>--</td>
</tr>
<tr>
<td>Time-based Passcodes (OATH OTP appears on app)</td>
<td>v4.0+ and prior</td>
<td>7.x+</td>
<td>--</td>
</tr>
</tbody>
</table>

**Prerequisites**

**SecureAuth IdP Web Admin Configuration Requirements**

**Configure Realm for App Enrollment**

Configure the OATH Provisioning Realm / App Enrollment Realm end-users will use to enroll the app on their device(s) for Push Notifications or OATH OTP

<table>
<thead>
<tr>
<th>Enrollment Method</th>
<th>SecureAuth IdP Version</th>
<th>Documentation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Mobile App Enrollment</td>
<td>9.0+</td>
<td>Multi-Factor App Enrollment (URL) Realm Configuration Guide</td>
<td>The name of the OATH provisioning / enrollment realm has changed since the release of SecureAuth IdP version 7.x.</td>
</tr>
<tr>
<td></td>
<td>8.2</td>
<td>SecureAuth App Enrollment Configuration Guide</td>
<td>As of version 9.0.1, the realm is called Multi-Factor App Enrollment Realm which is the name used throughout this document</td>
</tr>
<tr>
<td></td>
<td>8.1</td>
<td>OATH Provisioning Realm Configuration Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td>OATH Seed Realm Configuration Guide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7.x</td>
<td>Implementing OATH for Second Factor Authentication</td>
<td></td>
</tr>
<tr>
<td>QR Code Mobile App Enrollment</td>
<td>9.0+</td>
<td>Multi-Factor App Enrollment (QR Code) Realm Configuration Guide</td>
<td></td>
</tr>
</tbody>
</table>

**End-user Setup Requirements**

1. Ensure Android or iOS Version on Mobile Device / Paired Watch is Supported
### For Authenticate App v5.x

<table>
<thead>
<tr>
<th>OS</th>
<th>Mobile Device Version (App Version)</th>
<th>Paired Wearable Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>• 4.4+ (v5.0+)</td>
<td>W1+</td>
<td>Refer to the SecureAuth Compatibility Guide for additional information about supported mobile devices and paired smartwatches</td>
</tr>
<tr>
<td>iOS</td>
<td>• 8+ (v5.0) • 10+ (v5.0+)</td>
<td>Series 1+</td>
<td>For the v5.1 app on an Apple Watch, only watchOS 4 is supported</td>
</tr>
</tbody>
</table>

### For Authenticate App v4.x

<table>
<thead>
<tr>
<th>OS</th>
<th>Mobile Device Version</th>
<th>Paired Wearable Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>4.0+</td>
<td>4.0.1+</td>
<td>Refer to the SecureAuth Compatibility Guide for additional information about supported mobile devices and paired smartwatches</td>
</tr>
<tr>
<td>iOS</td>
<td>5.1.1+</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### 2. Download and Install SecureAuth Authenticate App

a. Download the app from the mobile store

<table>
<thead>
<tr>
<th>Device</th>
<th>Store</th>
<th>Download URL</th>
</tr>
</thead>
</table>

b. If this is a first time installation of the app on the mobile device, proceed with the installation process

**NOTE:** If this is an upgrade of the app from Version 4.x to Version 5.x on iOS, see the important message below
Upgrade the App on iOS from Version 4.x to Version 5.x

A. If a PIN is used to unlock v4.x of the app, enter that PIN to migrate accounts to v5.x of the app

B. Any existing account appears on the app, and thereafter, the app PIN is no longer used
3. Connect the Mobile App to a User Profile for Multi-Factor Authentication

Connect the Authenticate app to an end-user profile by starting the app and then selecting a Multi-Factor Authentication enrollment method – enter the enrollment URL or scan the QR code from a SecureAuth IdP or Cloud Access mobile app enrollment page.

For Authenticate App v5.x

For Authenticate App v4.x

See Connect Account to User Profile for v5.x

See First-Time Provisioning for v4.x

NOTE: See App Account Management for information on how to use features in the app for v5.x or v4.6 (and earlier)

NOTE: Push notifications must be enabled on the mobile device in order to use the Push Notification feature on the app. Push notification enablement can be applied when the app is started or through the device’s setting.

NEW SecureAuth Authentication App v5.x

What's New in v5.1

- Symbol-to-Accept support for Apple Series Paired Watches
- Third party apps supported on Android devices – The app running on an Android device can scan the QR code from a third party site such as Google and Facebook to enroll the app for generating timed passcodes for 2-Factor Authentication to that site.
Point Camera at QR Code

Log in to a QR code enabled enrollment portal or get a QR code from the security settings associated with your user profile.

Place a barcode inside the viewfinder rectangle to scan it.
What's New in v5.0

- **Complete re-design** – The app has been re-designed to offer the user:
  - Simplified steps to accept Login Requests on the app as a second authentication factor
  - Symbol-to-Accept authentication method to thwart phishing attempts
  - Android Wear OS and Apple Watch support for login requests
- **Improved OATH seed security** – The seed’s security is protected via an encryption key tied to the device’s screen lock – this makes it difficult to extract the seed, and virtually impossible on devices using hardware encryption
- **Greater ease of use** – Streamlined workflows provide a more user-friendly experience when enrolling accounts, managing accounts, and using the app to supply a second authentication factor
- **New user interface** – Both Android and iOS user interfaces are now built with native components specific to each platform
Accounts page
Re-Connect Account

If your account stops working, you may need to re-connect it.

If you enrolled via QR code, you will need to login to the site that originally provided the QR code from your desktop computer.

CANCEL  RE-CONNECT
Time-Based Passcode for:
Work Portal

116 386

Passcode expires in 0:09
New Features

Device Screen Lock and Seed Security

OATH PIN Enablement Not Required on SecureAuth IdP

The Require OATH PIN security option setting does not need to be made on the SecureAuth IdP Web Admin, since the device screen lock is used instead of the app PIN; this security feature cannot be disabled by the administrator.
1. On the **Web Admin**, click the **Post Authentication** tab and select either **Multi-Factor App Enrollment - URL** or **Multi-Factor App Enrollment - QR Code** from the **Authenticated User Redirect** dropdown.

Select either the **Version 9.0.0** or **Versions 9.0.1+** tab for the next configuration step.
2. In the Multi-Factor Enrollment section, under SecureAuth App - Security Options, the selection of False from the Require OATH PIN dropdown is required for app security only in versions 4.x of the Authenticate App.
2. In the Multi-Factor Enrollment section, under SecureAuth App - Security Options, the selection of False from the Require OATH PIN dropdown is required for app security only in versions 4.x of the Authenticate App.
Device Screen Lock Must Be Enabled

- Enforcement of the device screen lock replaces the app-PIN from earlier versions of the app
- Disabling the screen lock disables the app and shows the screen lock required page
- If the screen lock is re-enabled, the accounts must be re-connected
- Tapping the icon starts the re-enrollment process
- For account enrollment via QR code, the same page from which the QR code was scanned must be used for login access

Re-enroll Accounts if OATH Seed is Lost

- Tapping the icon starts the re-enrollment process
- For account enrollment via QR code, the same page from which the QR code was scanned must be used for login access
This app requires you to enable the device screen lock.

SCREEN LOCK SETTINGS
This app requires you to enable a passcode on your device.

To enable a passcode:

Go to Settings on your iPhone

Navigate to:

Touch ID & Passcode

Click “Turn Passcode On” and create a passcode for this device.
Login Requests from Push Notifications

Different Ways to Accept Login Requests
Accept request from the app...

Tap Approve / Deny on the Login Request page

Accept request from notification...

1. Swipe down on the Push Notification on the locked screen

2. Tap Approve / Deny on the expanded notification on the screen
Login request. Tap to see request in app.
Accept request on a paired watch...

On Android Wear OS, tap **Approve** / **Deny**

On Apple Watch, tap **Accept** / **Deny**
Login request from:
Work Portal
Bob Barker
38.88.249.178
LOS ANGELES, US

Deny
Approve
Login request. Tap to see request in app.

Accept

Deny
Accept symbol on a paired watch...

Refer to Mobile Login Requests (Push Notifications) Registration Method for Multi-Factor Authentication for information on configuring Symbol-to-Accept

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

![SecureAuth Login Request Image]

Please respond to the login request sent to your mobile device.

Please click here to use an alternate verification method.
Login request from:

**Work Portal**

- Realm 43
- jsmith
- 192.169.9.73

DENY THIS REQUEST
Connect an Account (v5.x)

Connect Account to User Profile

The enrollment workflow varies based on the configurations set on the Multi-Factor App Enrollment Realm

Shown below is the Username + Password, + 2-Factor Authentication workflow on an iOS device
Connect an account to get started.

Ask your administrator for the URL or QR Code, then tap the "+" button.
1. Start the app on the iOS or Android mobile device
2. Tap + to open the menu
3. Tap Connect with URL or Connect with QR code

Ask your administrator for the URL or QR Code, then tap the "+" button.
For the Web Address entry, if using **SecureAuth998** as the **Multi-Factor App Enrollment realm**, then only the Fully Qualified Domain Name (FQDN) is required – e.g. **secureauth.company.com**

If using a different realm for the **Multi-Factor App Enrollment**, then the entire URL address which includes the realm name is required – e.g. **https://secureauth.company.com/secureauth2**

1. Set the **Web address** to the Domain Name (DN) of the SecureAuth IdP appliance, e.g. **secureauth.company.com**
2. Select the Multi-Factor Authentication method to use for receiving the code to connect the account
3. After entering the code that was delivered, the connected account appears on the **Accounts** page
Enter Web Address

Enter the web address given to you by your account administrator.

Web address

You will be asked to login before you can connect your account.
Please choose the delivery method for your Passcode.

- Send login request to SAMSUNG-DEV
- Time-based Passcode - SecureAuth OTP Mobile App
- Email xxxxx@secureauth.com
- Voice: xxx-xxx-2975

Submit
1. Use a device other than the one being provisioned – e.g. desktop, laptop – to log on the QR code realm.

2. Upon successful authentication, start the app and scan the unique QR code which is valid for 10 minutes.

3. Note the 6- to 8-digit code that appears, and then tap Finished.
Setup Two-Factor Authentication

1. Install
   To use two-factor authentication, you will need to
download the SecureAuth mobile app to your smart
phone

2. Scan
   Open your two-factor authentication app and scan
the code with the camera on your phone.

3. Confirm
   Enter the verification code generated by your two-
   factor authentication app.

Restart Login

Copyright 2016 SecureAuth Corp. All rights reserved.
Almost Finished

Finish connecting your account by entering the following passcode on the page where you scanned the QR code.

854 980

Finished
4. In the Confirm box, enter the 6- or 8-digit code from the app, and click Enable.
**ANDROID**

1. Press the account to go to the passcode screen
2. Tap the double-square icon to copy the passcode to the clipboard

**iOS**

1. Tap the account to go to the passcode screen
2. Tap the passcode to copy it to the clipboard

**ANDROID**

1. Tap the account
2. Tap the trash can icon

**iOS**

1. Use one of two methods
   - Tap **Edit** or
   - Swipe left on the account and tap **Delete**
Time-Based Passcode for:
Work Portal

116 386

Passcode expires in 0:09
Time-Based Passcode for:

Work Portal

705 596

Copied to clipboard.
Re-connect an Account
Rename an Account
**ANDROID**

1. Press the account and tap the reconnect icon

2. Tap **RE-CONNECT**

**iOS**

1. Swipe left on the account, tap **Edit**

2. Tap **Re-connect**

**ANDROID**

1. Press the account and tap the pencil icon

2. Edit the account name and tap **SAVE**

**iOS**

1. Tap **Edit** to go to the next screen

2. Edit the account name and tap **Done**
Work Portal  
Connected Mar 13, 2017 7:57 AM

VPN  
Connected Mar 13, 2017 9:15 AM

Push-To-Accept48  
Connected Mar 13, 2017 10:35 AM
Accounts

Work Portal
Connected Feb 17, 2017 12:10 PM

VPN
Connected Feb 17, 2017 2:10 PM

Delete Re-Connect
Work Portal
Connected Mar 13, 2017 7:57 AM

VPN
Connected Mar 13, 2017 9:15 AM

Push-To-Accept48
Connected Mar 13, 2017 10:35 AM
The enrollment workflow varies based on the configurations set on the Multi-Factor App Enrollment Realm

Shown below is the Username + Password, + 2-Factor Authentication workflow

Steps 9 and 10 are only applicable if a required PIN code is configured
Three ways to provide login verification:

1. Use time-based passcodes

2. Authorize login requests

3. Receive notification passcodes
Add Account

Enter the web address provided by your administrator

e.g. https://idp.company.com

Enroll
1. Start the app on the iOS or Android mobile device

2. Tap Begin Setup

3. Set the web address to the Domain Name (DN) of the SecureAuth IdP appliance, e.g. secureauth.company.com

   If using SecureAuth998 as the Multi-Factor App Enrollment Realm, then only the Fully Qualified Domain Name (FQDN) is required – e.g. secureauth.company.com

   If using a different realm for Multi-Factor App Enrollment, then the entire URL address which includes the realm name is required – e.g. http://secureauth.company.com

4. Tap Enroll
5. Provide the **Username** and **Password**, and tap **Submit**.

6. Select the Multi-Factor Authentication method, and tap **Submit**.

7. Enter the enrollment code received via the method selected in step 6, and tap **Submit**.

8. Tap **OK** once the app on the device is successfully enrolled.
Please choose the delivery method for your Registration Code.

- Email xxxxx@xxxxxxx.com
- Voice : xxx-xxx-xxxx
- SMS/Text : xxx-xxx-xxxx

Submit
Enter the code that you just received by email.

624792

Submit
What is this?

This number is a one-time passcode used when you select the "Leave taken" button.

Enrollment success!

You can use this method to authenticate when your device doesn't have internet access.

Don't show this again
9. Create a 4-digit PIN code for use to unlock the app
10. Confirm the 4-digit PIN code that was just entered
11. Tap the **three lines button** located on the upper left (or swipe) to open the drawer menu; the **three dots button** on the upper right opens the account management page (see App Account Management below)

Tap **Change PIN** to change the 4-digit PIN code

Tap **Send Feedback** to send an email to SecureAuth regarding the application
Choose a PIN that does not have 4 repeating digits or sequential digits.

Example: 6666 and 7654 are not allowed.
<table>
<thead>
<tr>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>PQRS</td>
<td>TUV</td>
<td>WXY</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>PQRS</td>
<td>TUV</td>
<td>WXY</td>
</tr>
<tr>
<td>0</td>
<td><img src="image" alt="Close button" /></td>
<td></td>
</tr>
</tbody>
</table>
QR Code Enrollment

Using QR Code mobile app enrollment, the end-user is delivered a QR code by a specialized SecureAuth IdP realm, and this QR code is captured using the mobile device's camera and then read by the app.

The QR Enrollment Realm also supports the use of Google Authenticator to perform the same function (for OTP only) by manually entering the alphanumeric value associated with the QR code.

The QR Code Enrollment feature is supported by SecureAuth IdP versions 9.0+ only.

The interface shown below is from the iOS application – the Android application interface is the same, with minor UI distinctions.
Setup Two-Factor Authentication

1. Install
To use two-factor authentication, you will need to download the SecureAuth mobile app to your smartphone.

2. Scan
Open your two-factor authentication app and scan the code with the camera on your phone.

3. Confirm
Enter the verification code generated by the two-factor authentication app.

1. Log on the Multi-Factor App Enrollment (QR Code) realm from a device other than the one being provisioned (e.g. desktop, laptop).

2. Upon successful authentication, start the app

Each unique QR code is valid for 10 minutes

Application Workflow
3. Tap **Begin Setup**

4. Tap **Enroll with QR Code**

5. Point the mobile device's camera at QR Code to scan

6. Create a 4-digit PIN (if required in the configuration)

7. Note the Time-based Passcode in the application
Choose Enrollment Method

Enroll with QR Code

https://enroll.mycompany.com
Enroll with URL
Enroll with QR Code

Point camera at QR Code

Setup Two-Factor Authentication

2. Scan

Open your two-factor authentication app and scan the code with the camera on your phone.

© 2016 SecureAuth Corp. All rights reserved.
Choose PIN

Choose a PIN that does not have
4 repeating digits or sequential digits.
Example: 6666 and 7654 are not allowed
Almost Finished

Complete confirmation of this device by entering the "soft token" or "time-based passcode" of the newly added account into Step 3 of the Setup web page.

OK

You can use this method to authenticate when your device doesn't have internet access.

Don't show this again
8. Enter the numeric 6- or 8-digit Time-based Passcode from the mobile device app into the Confirm field on the browser, then click Enable.

If the code is correct, then the Setup Complete screen appears, and the mobile device app is now successfully enrolled and can be used for Multi-Factor Authentication.
Tap the pencil icon next to the name – or the name itself – to edit the account name; tap the red circle on the upper left to delete the account; tap the + on the upper right to add another account.

The name of the account can be changed at any time. Tap Delete to confirm the action.

The enrollment process initiates again to add new accounts.
Add Account

Enter the web address provided by your administrator

e.g. https://idp.company.com

Enroll
Accounts

❚ Appliance 1 Directory 1

— Re-enroll

❚ Appliance 1 Directory 2

— Re-enroll
<table>
<thead>
<tr>
<th>Appliance 1 Directory 2</th>
<th>4173 7172</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance 1 Directory 1</td>
<td>394 740</td>
</tr>
</tbody>
</table>
Tap and hold the three lines on the account and drag to reorganize the accounts.

The accounts will reorganize on the account management page and on the home page.

SecureAuth Authenticate App End-User Experiences (v4.x)

Strong PIN Enforcement (v4.5 - v4.7)
Create PIN

Choose PIN

Choose a PIN that does not have 4 repeating digits or sequential digits.

Example: 6666 and 7654 are not allowed

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ABC</td>
<td>DEF</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GHI</td>
<td>JKL</td>
<td>MNO</td>
</tr>
</tbody>
</table>
Strong PIN enforcement, which is available in v4.5 - v4.7

- utilizes complexity rules such as non-sequential, non-repeating formats
- disallows a PIN using 4 repeating digits such as 1111
- disallows a PIN using 4 sequential digits such as 1234

Only end-users downloading and installing these versions of the app for the first time are impacted

End-users upgrading to this version do not have to change their PIN

Biometric Unlock (v4.4 - v4.7)

The Biometric Unlock feature, which is available in v4.4 - v4.7, enables a fingerprint scanned on a registered mobile device – using Touch ID on iOS and Fingerprint Unlock on Android – to be used instead of a PIN to unlock the app

The mobile device must have Touch ID (on iOS) / Fingerprint Unlock (on Android) integrated within the operating system in order to use the Biometric Unlock feature

<table>
<thead>
<tr>
<th>iOS - Touch ID Platform Support</th>
<th>Android - Fingerprint Unlock Platform Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 5s+</td>
<td>Google Android 6.0 device with fingerprint sensor (Google FP API) including Samsung S7</td>
</tr>
<tr>
<td>iPad Pro</td>
<td>Samsung proprietary API: S5 and S6</td>
</tr>
<tr>
<td>iPad Air 2</td>
<td></td>
</tr>
<tr>
<td>iPad Mini 3+</td>
<td></td>
</tr>
<tr>
<td>Biometric Unlock Enrollment Steps</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>The interface shown below is from the iOS application – the Android application interface is the same, with minor UI distinctions</td>
<td></td>
</tr>
</tbody>
</table>

1. Start the app; the splash screen appears
2. Tap **Begin Setup** on the onboarding screen
3. Select the enrollment option to use with Touch ID / Fingerprint Unlock and proceed with the workflow for that selection
SecureAuth Authenticate

Three ways to provide login verification:

1. Use time-based passcodes

   0804 1282

2. Authorize login requests

   Accept  Deny

3. Receive notification passcodes

   87563

   Begin Setup
Choose Enrollment Method

- 4. Create a 4-digit PIN
- 5. Confirm the 4-digit PIN
- 6. Touch the sensor on the mobile device to register the fingerprint for Biometric Unlock
- 7. Tap Close

Enroll with QR Code

https://enroll.mycompany.com

Enroll with URL
Create PIN

Choose PIN

Choose a PIN that does not have
4 repeating digits or sequential digits.
Example: 6666 and 7654 are not allowed

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ABC</td>
<td>DEF</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GHI</td>
<td>JKL</td>
<td>MNO</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>PQRS</td>
<td>TUV</td>
<td>WXYZ</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use Biometric Unlock / PIN Options

Confirm PIN

Confirm 4-digit PIN

Touch ID for “Authenticate”
Touch your finger to the fingerprint sensor to enable Touch ID as an alternative to entering a PIN.

Close

1 ABC
2
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
1. Start the app

2. To unlock the app, engage the fingerprint identity sensor until a response message appears

3a. If the fingerprint is recognized, the success message appears and the app is unlocked

3b. If the fingerprint is not recognized at step 2, a screen appears with the option to Use PIN Instead

4b. Tap Cancel to attempt using the fingerprint identity option again – or tap Use PIN Instead to go through the PIN entry workflow

5b. If the fingerprint identity option was used at step 4b and fingerprint recognition fails for the maximum number of attempts set by the device, the Unlock App Failed screen appears and the PIN entry workflow must be used to unlock the app
Unlock App Failed

We were unable to verify your fingerprint. Please unlock the app with your PIN instead.

OK
The Biometric Unlock option is disabled / re-enabled by first opening the drawer menu – see step 11 in Navigate the App – and then tapping the toggle switch.

Result of end-user tapping the Touch ID / Fingerprint Unlock toggle switch to disable the option.

Result of end-user tapping the Touch ID / Fingerprint Unlock toggle switch to re-enable the option.
Push-to-Accept, which is one of two (2) Push options for Multi-Factor Authentication, lets the end-user Accept or Deny a login request as a second authentication factor on an enrolled mobile device app.

Push-to-Accept Notifications (Accept / Deny Login Request) (v4.1+)
The other Push option is Push Notification, which sends an OTP alert message to the home screen of an end-user’s mobile device app.

Push-to-Accept is supported by SecureAuth IdP versions 8.2+

1. Access a realm configured for Mobile Login Requests - Accept / Deny by initiating the login process

2. Follow the configured workflow

3. On the Multi-Factor Authentication methods page, select Send login request from the list of the options

4. Click Submit

5. A Push-to-Accept request is delivered to the enrolled device app, ready for the end-user to tap Accept or Deny on the app
Authenticate now
Login request. Tap to see request in app.
slide to view
Login Request

SA QA
User SelfService

Admin55
11:00:08 at 11/24/2015
When the login request is submitted, the app on the mobile device must be minimized or closed in order for the **Accept / Deny** screen to appear on the mobile device

6. Tap (or swipe) to access the **Accept** and **Deny** options on the next screen

7. Tap **Accept** to enable secure access to the realm (or **Deny** to refuse access)

8. The application displays the result to the end-user (see below)

---

Result of end-user’s **acceptance** of access

Result of end-user’s **denial** of access

Result of Push-to-Accept login request **timeout**
Login Request

Accepted!
Close
Login Request

Denied!
Close
Login Request

The request has expired
Push-to-Accept lets the end-user Accept or Deny a login request as a second authentication factor on an enrolled mobile device app.

When an Android Wear OS smartwatch is successfully paired with an Android mobile device app enrolled for Push-to-Accept, the smartwatch receives Login Request notifications simultaneously with the app on the mobile device.

Issues may arise if the smartwatch is paired with the mobile device after the app is installed.

In this scenario, SecureAuth recommends uninstalling or reinstalling the app after the Android Wear (Wear OS) watch is successfully paired with the Android mobile device.
"Ok Google"
moto

SecureAuth

Login Request
When the login request is submitted, the app on the mobile device must be minimized or closed in order for the **Accept / Deny** screen to appear on the smartwatch.

1. The notification alert appears on the smartwatch.

2. Swipe up to view the **Login Request** notification screen.

3. Swipe left to access the **Open** screen.
4. Tap Open to access the Accept and Deny options on the next screen.

5. Tap Accept (green circle with check mark) to enable secure access to the realm or Deny (red circle with X) to refuse access.

6. The application displays the result to the end-user (see below).

Result of end-user's acceptance of access
Result of end-user's denial of access
There is no timeout screen that appears on the smartwatch to notify the end-user that the login request has expired.
Push Notification Alerts (OTP Sent to Device Home Screen) (v4.x and prior)

Push Notification, which is one of two (2) Push options for Multi-Factor Authentication, sends an OTP alert message to the home screen of an end-user’s mobile device.

The other Push option is Push-to-Accept, which lets the end-user Accept or Deny a login request as a second authentication factor on an enrolled mobile device app.

1. Access a realm configured for **Mobile Login Requests - Passcode (OTP)** by initiating the login process.

2. Follow the configured workflow.

3. On the Multi-Factor Authentication methods page, select **Send passcode to iPod touch** from the list of options.

4. Click **Submit**.
Authenticate now
Your one time password is 1039,
Doraiswamy Ota.
slide to view
5. A passcode Push Notification is delivered to the enrolled device app and appears on the home screen, along with the OTP.

6. Enter the Passcode received from the Push Notification and click Submit.

Time-based Passcodes (OATH OTP) (v4.x and prior)

When the app on a mobile device is enrolled to use time-based passcodes as a second authentication factor, a passcode appears on the app for a configured amount of seconds before it is replaced by a new passcode.
The current passcode that appears on the app must be entered in the user interface of login screen as part of the authentication workflow.

1. Access a realm configured for **Time-based Passcodes (OATH)** by initiating the login process.

2. Follow the configured workflow.

3. On the Multi-Factor Authentication methods page, select **Time-based Passcode** from the list of the options.

   If the device is provisioned on a **Single (OATH Seed) Multi-Factor App Enrollment Realm**, then select **Time-based Passcode - SecureAuth OTP Mobile App**.

   If the device is provisioned on a **Multi (OATH Token) Multi-Factor App Enrollment Realm**, then select the appropriate app, e.g. **Time-based Passcode - iPhone**.

4. Click **Submit**.
Copied to clipboard.
5. Start the app and use the appropriate Time-based Passcode (if more than one account is activated)

   If accessing the realm on a mobile browser, tap the Passcode account to copy the code, which can then be pasted into the **Passcode** field on the login page.

6. Enter the OTP into the **Passcode** field and click **Submit**.
## Release Notes

### Version 5.1

**iOS Version Release Date:** January 31, 2018

<table>
<thead>
<tr>
<th>What's New in iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Watch support for timed passcodes and login requests</td>
</tr>
<tr>
<td>Two-factor authentication support on sites that use timed passcodes, such as Facebook and Google – requires availability of QR code enrollment method</td>
</tr>
<tr>
<td>Usability improvements and bug fixes</td>
</tr>
</tbody>
</table>

**Known Issue**

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.

**Android Version Release Date:** October 30, 2017

<table>
<thead>
<tr>
<th>What's New in Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-Factor Authentication supported on sites that use timed passcodes, such as Facebook and Google – requires availability of QR code enrollment method</td>
</tr>
<tr>
<td>Usability enhancements</td>
</tr>
<tr>
<td>Performance improvements and bug fixes</td>
</tr>
</tbody>
</table>

### Version 5.0

**Release Date:** June 6, 2017

<table>
<thead>
<tr>
<th>What's New in Android</th>
<th>What's New in iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device lock enforcement</td>
<td>Device lock enforcement</td>
</tr>
<tr>
<td>Phishing-resistant login requests (Symbol-to-Accept)</td>
<td>Ability to approve login requests from notifications</td>
</tr>
<tr>
<td>Android Wear OS support for notifications</td>
<td>Ability to approve login requests from Apple Watch notifications</td>
</tr>
<tr>
<td>Performance, security, usability, and stability improvements</td>
<td>Performance, security, usability, and stability improvements</td>
</tr>
<tr>
<td>Related Documentation</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>Multi-Factor App Enrollment (QR Code) Realm Configuration Guide</td>
<td></td>
</tr>
<tr>
<td>Multi-Factor App Enrollment (URL) Realm Configuration Guide</td>
<td></td>
</tr>
<tr>
<td>Time-based Passcodes (OATH) Registration Method for Multi-Factor Authentication</td>
<td></td>
</tr>
<tr>
<td>Mobile Login Requests (Push Notifications) Registration Method for Multi-Factor Authentication</td>
<td></td>
</tr>
<tr>
<td>SecureAuth Authenticate App Troubleshooting</td>
<td></td>
</tr>
<tr>
<td>How to Pair the SecureAuth Authenticate App on a Mobile Device and Watch</td>
<td></td>
</tr>
</tbody>
</table>