# SecureAuth Passcode for Windows v2.0

**Introduction**

Use this guide to install and provision the **SecureAuth Passcode for Windows** application ("Passcode") for Multi-Factor Authentication on Windows desktop clients.

SecureAuth Passcode is a Windows desktop application that generates six- or eight-digit one-time passcodes (OTPs) that rotate based on the configured interval (e.g. every 60 seconds). The code can be used as an authentication option when logging into a resource protected by SecureAuth IdP.

Users can enroll one or more accounts with Passcode that can generate unique OTPs and can be edited or deleted through the interface.

The Passcode application supports optional PIN protection, which requires a user to enter a personal PIN to view the OTP.

Refer to **SecureAuth Passcode for Windows** for the latest version of the document for this application

**Prerequisites**

1. Minimum System Requirements:

- **Operating System**
  - Microsoft Windows 7 *(32-bit or 64-bit)*
  - Microsoft Windows 8.1 *(32-bit or 64-bit)*
  - Microsoft Windows 10 (*32-bit or 64-bit*)
  - Microsoft Windows Server 2008 R2 *(32-bit or 64-bit)*
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
- **Microsoft.Net**
  - Requires **Microsoft .NET Framework 4** or greater to be installed

2. Configure the **App Enrollment Realm / OATH Provisioning Realm** in the SecureAuth IdP Web Admin

- SecureAuth IdP 9.0 Configuration Steps
- SecureAuth IdP 8.2 Configuration Steps
- SecureAuth IdP 8.1 Configuration Steps
- SecureAuth IdP 8.0 Configuration Steps
- SecureAuth IdP pre-8.0 Configuration Steps

**Passcode** supports both **Single (OATH Seed)** and **Multi (OATH Token)** configurations for SecureAuth IdP versions 8.1+

**Passcode** supports **Roaming User Profiles** in Active Directory environments

When enabled, seed and PIN values are shared on all machines on which the Passcode application is installed. Any changes to seeds, PINs, and/or accounts are reflected on other machines once the Passcode application on the other machine is restarted.

**Requirements**:

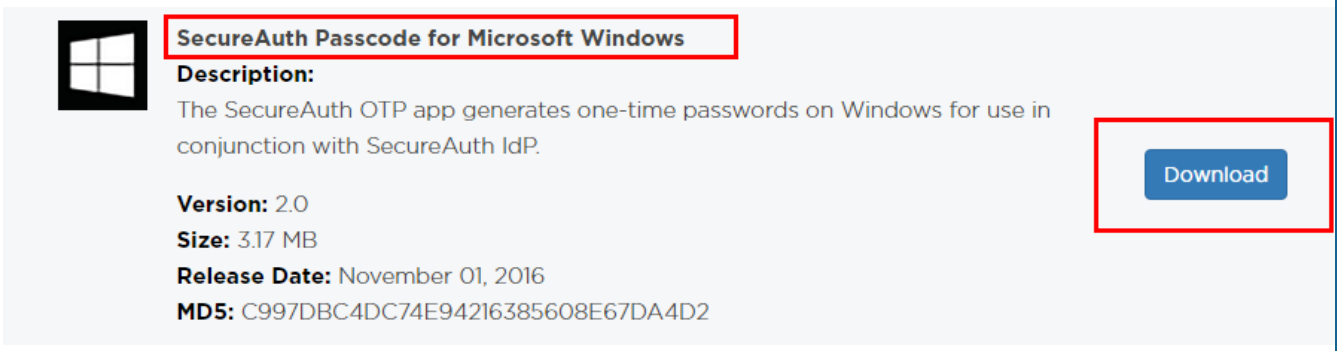
- The **Passcode** application must be installed on each machine used by the roaming profile
- A **Roaming User Profile GPO** must be enabled in Active Directory; for more information see the Microsoft Technet article on deploying Roaming Profiles

## Installation Steps

There are two methods of installing Passcode: **Wizard Install** and **Silent Install**

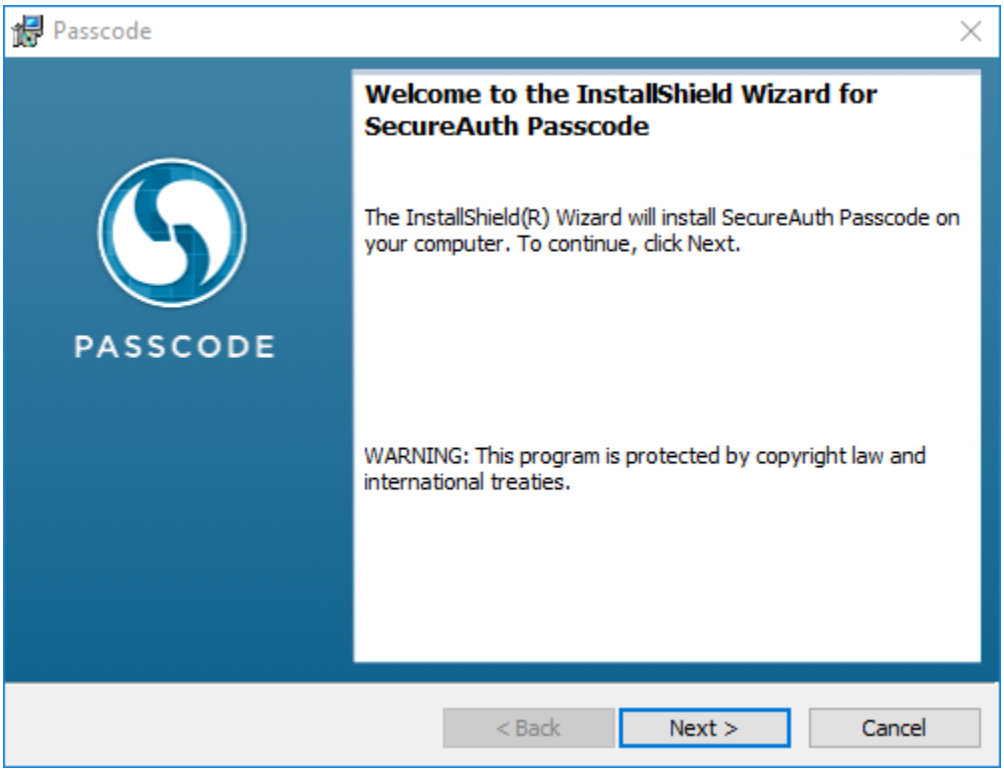
Follow the instructions of the preferred method *only*

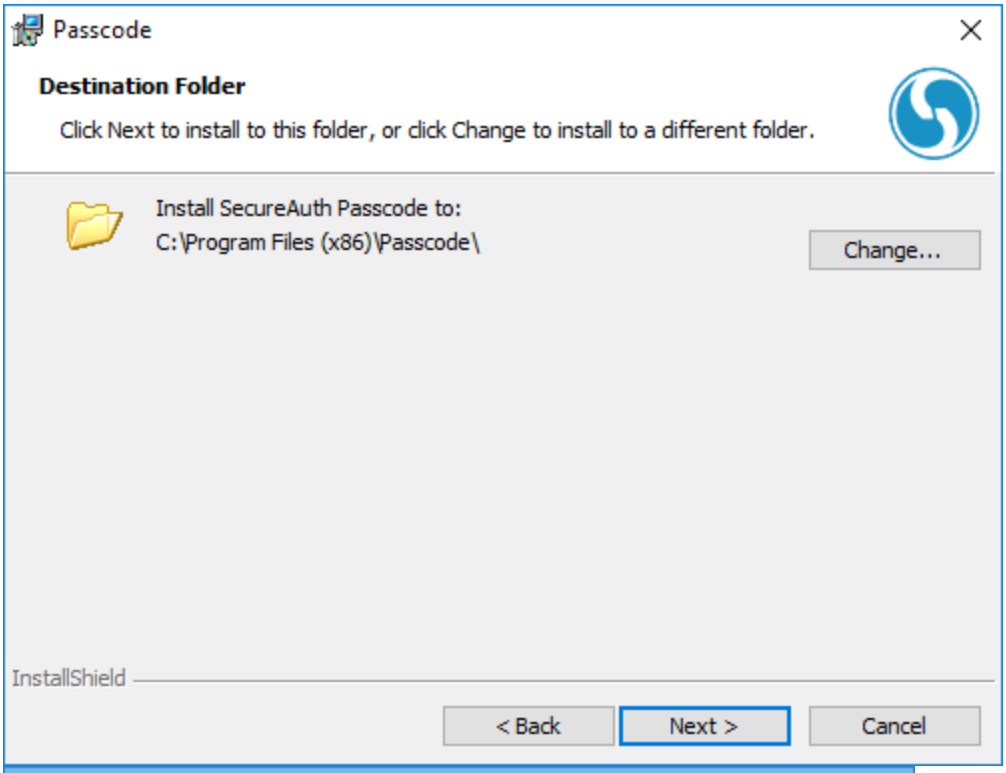
### Wizard Install

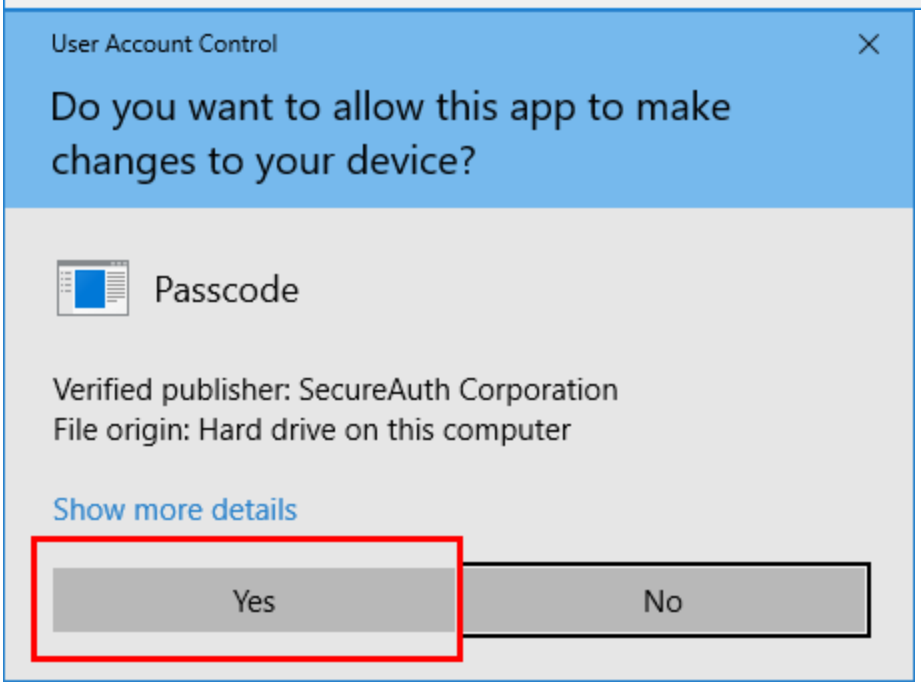


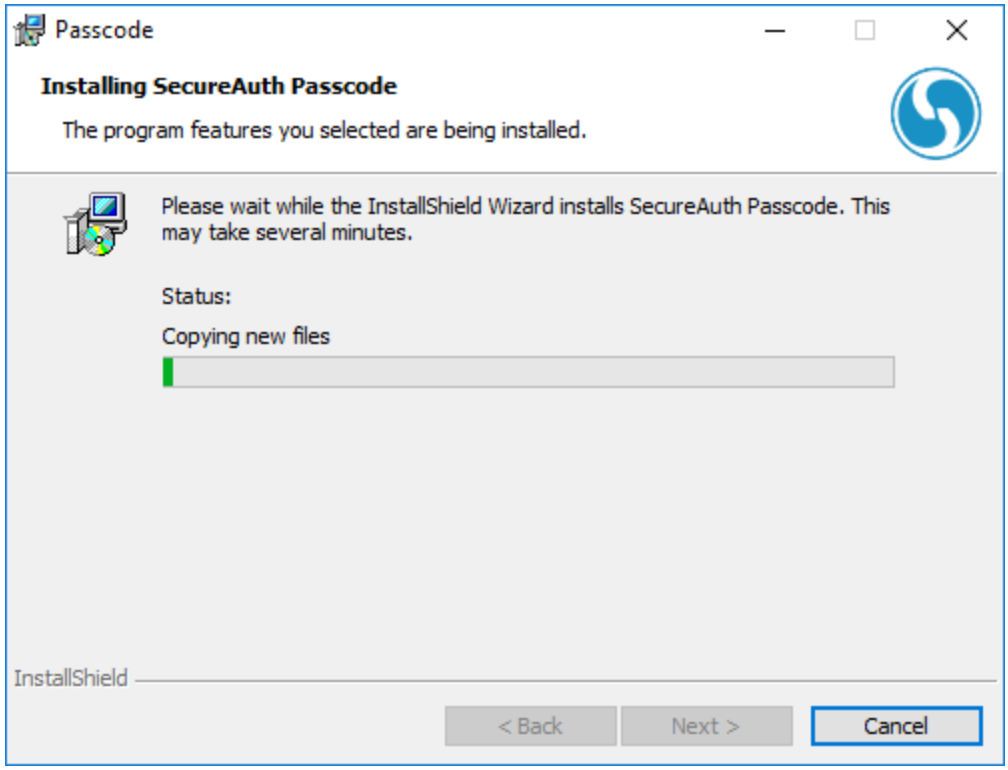

1. Download the **Passcode** client application from the **SecureAuth Downloads** page
2. Open the **Passcode_2.0.msi** file

---



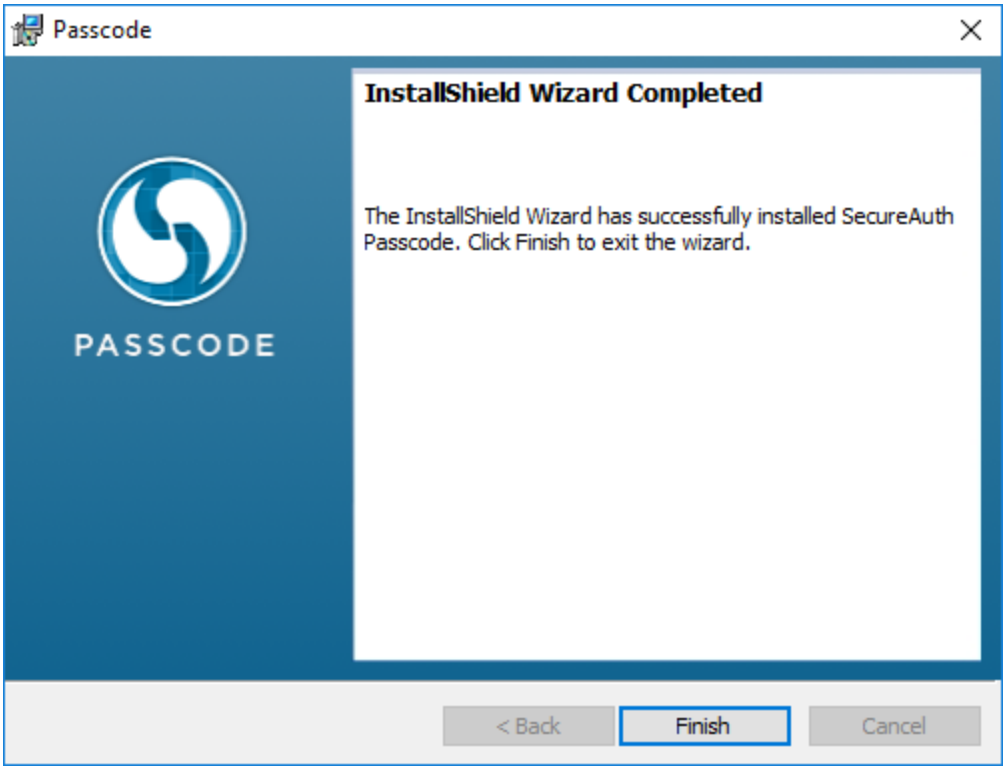

Passcode
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install SecureAuth Passcode to:
C:\Program Files (x86)\Passcode\
Change...
InstallShield
< Back
Next >
Cancel


User Account Control
Do you want to allow this app to make changes to your device?
Passcode
Verified publisher: SecureAuth Corporation
File origin: Hard drive on this computer
Show more details
Yes
No




The InstallShield Wizard window opens

3. Click **Next** to continue
4. Review the current settings, then click **Next**
5. If a User Account Control (UAC) confirmation appears, then click **Yes** to begin the installation
6. Wait for the InstallShield Wizard to install the client application to the device




7. Click **Finish** once the installation is complete

## Silent Install

**Passcode** supports a silent install option (no user interaction required) via the Windows Command Line Interface. To perform a silent install, follow these steps:

1. Download the **Passcode** client application from the **SecureAuth Downloads** page

2. Open an elevated command prompt (Run as administrator)

3. Use the following syntax to perform a silent install:

| | |
|---|---|
| **Syntax:** | `<installerPath>\Passcode2_0.msi /quiet INSTALLDIR=<installDirectoryPath> ENROLLMENTURL=<enrollmentURLpath>` |
| **Example:** | `C:\users\admin\Downloads\Passcode2_0.msi /quiet INSTALLDIR="C:\SecureAuth Files\Passcode" ENROLLMENTURL=secureauth.company.com` |

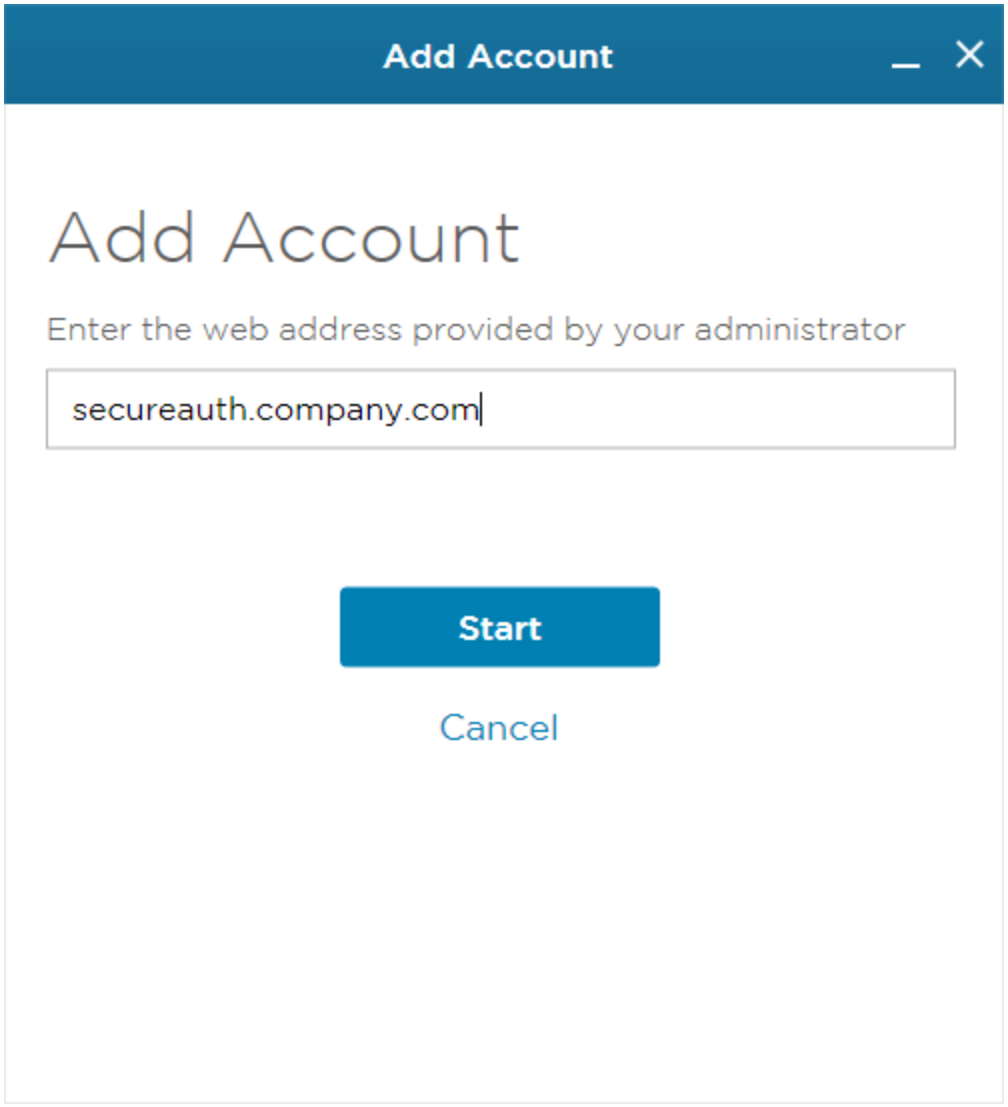
### The **INSTALLDIR** and **ENROLLMENTURL** attributes are **OPTIONAL**

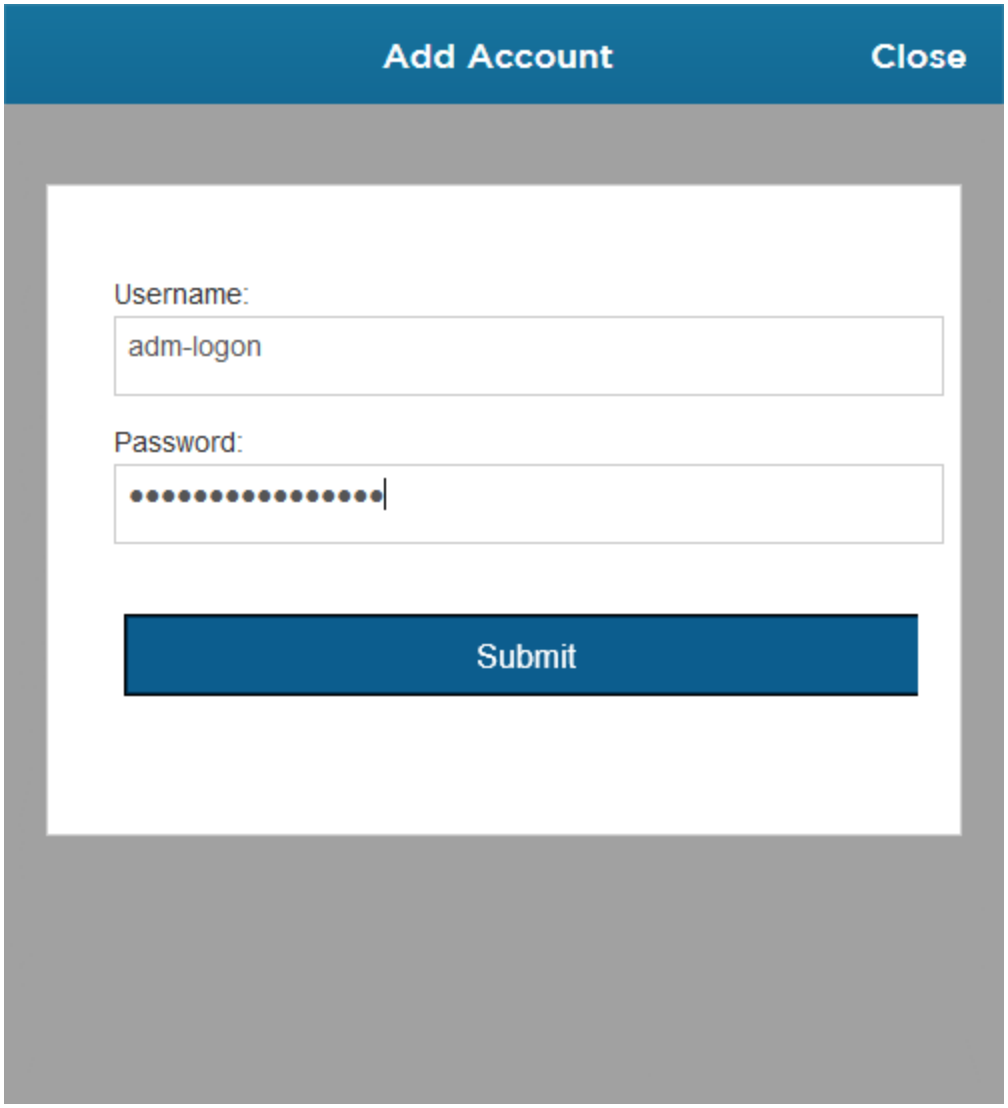
- The INSTALLDIR attribute is only required if installing Passcode to a non-default location; the default location is C:\Program Files (x86)\Passcode
- The ENROLLMENTURL attribute pre-fills the Add Account page with the URL when the end-user opens the application for the first time
    - The Add Account screen will display a notice to alert the end-user that "A web address has been provided by your administrator"; the end-user is able to modify this pre-filled URL if desired
    - If the administrator chooses to specify an account Enrollment URL in the command line syntax, then any existing provisioned accounts on the end-user's machine will be deleted
    - If using **SecureAuth998** as the app enrollment realm, then only the domain name is required for the ENROLLMENTURL attribute (e.g. secureauth.company.com); if using a different realm for app enrollment, then the entire URL and realm name are required (e.g. https://secureauth.company.com/secureauth2)

## Provisioning Steps


1. Open the **Passcode** client application from the Windows Start menu

The Passcode splash screen appears


Add Account
Add Account
Enter the web address provided by your administrator
secureauth.company.com
Start
Cancel



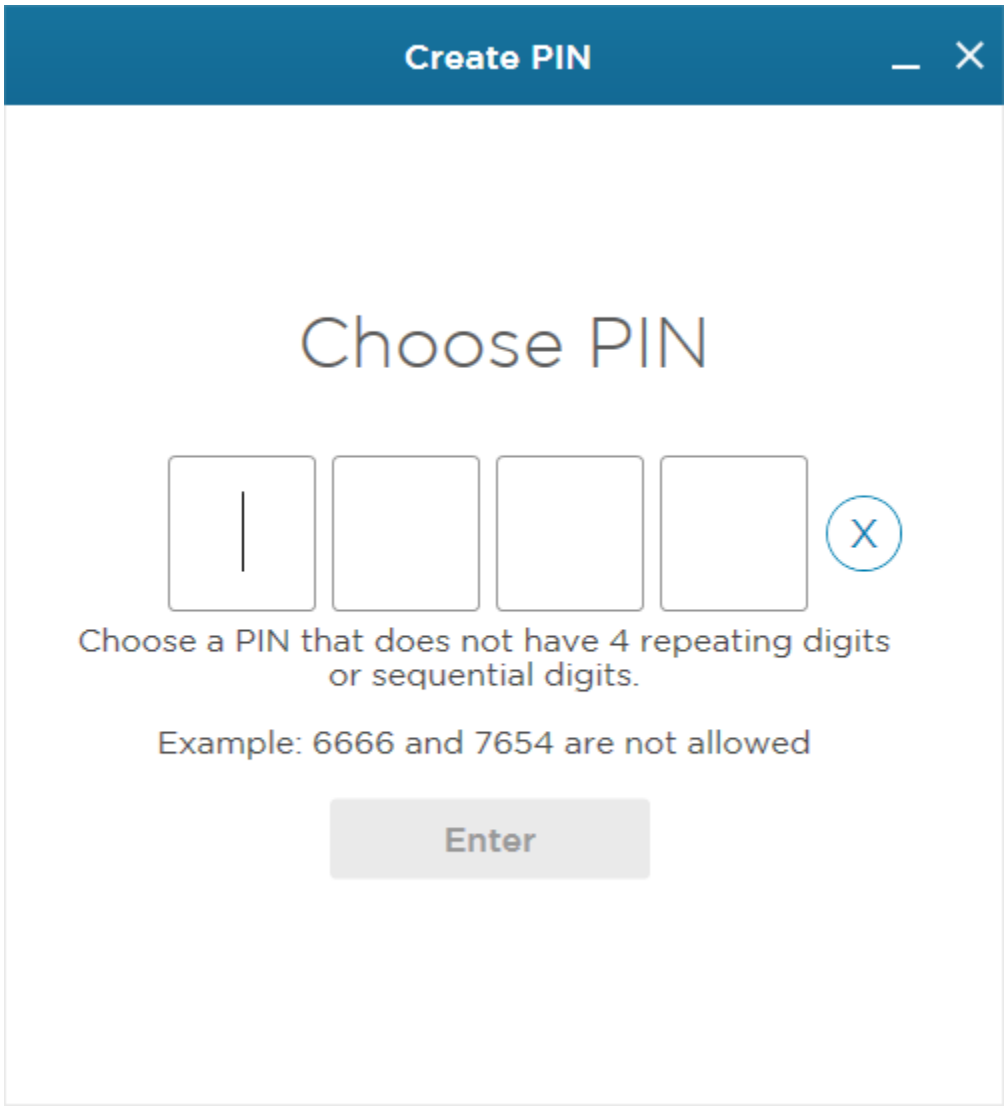

If this is a fresh install, then the **Add Account** window opens

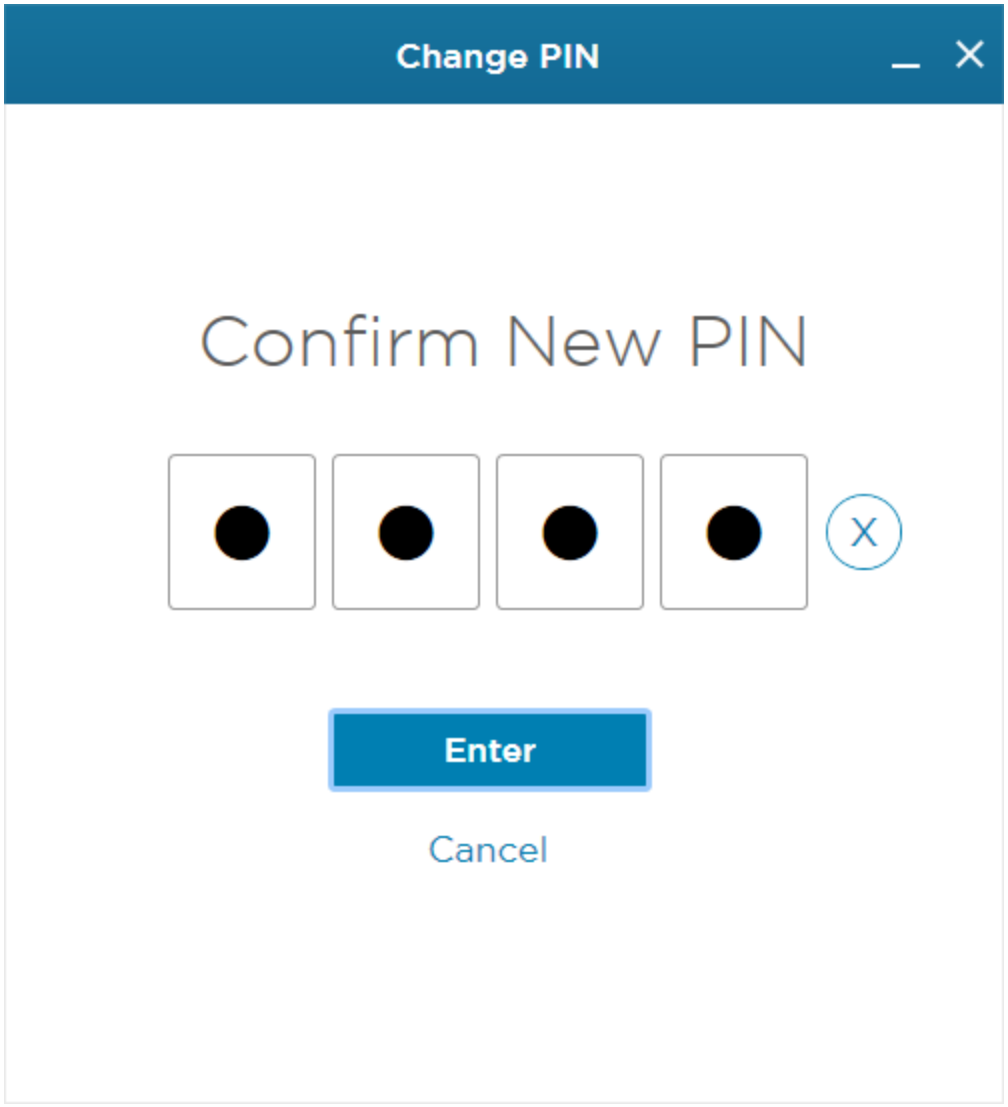
2. Provide the **Server URL**, which is the SecureAuth IdP App Enrollment /OATH Provisioning realm

> If using **SecureAuth998** as the app enrollment realm, then only the domain name is required (e.g. secureauth.company.com); if using a different realm for app enrollment, then the entire URL and realm name are required (e.g. https://secureauth.company.com/secureauth2)

3. Click **Start**
4. Follow the configured workflow, which may include Multi-Factor Authentication

> Shown in the image is **Username + Password Only (on 1st page)**


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




5. Set the **PIN** (if required in the App Enrollment Realm configuration) and click **Enter**

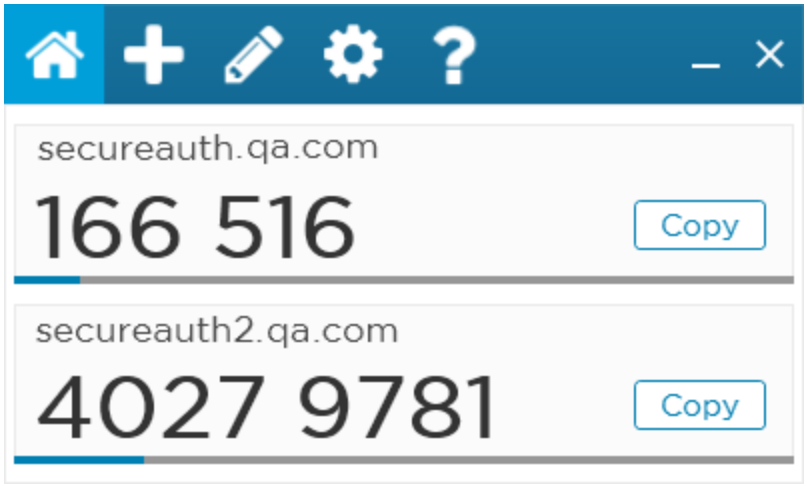
PIN values contain the following restrictions:

- Must not contain 4 repeating digits (e.g. '6666')
- Must not be forward or backwards sequential ( e.g. '4567' or '7654')

6. Confirm the PIN, and click **Enter** again

The **OTP Panel** appears and the client application displays the one-time password (OTP) that can be used for Multi-Factor Authentication

**Application Usage**



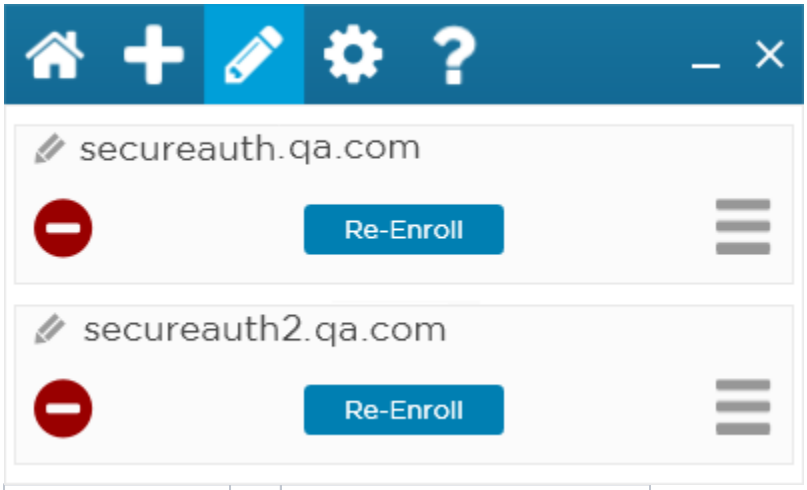

When the application is opened, the **OTP panel** appears (after PIN entry, if required)

- The **OTP** is either 6 or 8 digits in length, depending on admin configuration
- The blue bar under the OTP digits indicates how much time remains to use the OTP for login (configured by admin)
    - The bar turns red when there are ten (10) seconds remaining; when the time is elapsed, a new OTP displays
- Click the **Copy** button to the right of the OTP to copy the OTP to clipboard for easy input into the login page

**Toolbar**

| | | |
|---|---|---|
|  | **Home** | Displays the **OTP panel**, which shows the OTPs for all accounts on domains that have been provisioned |
|  | **Add Account** | Opens the **Add Account** screen, allowing the user to provision an additional domain |
|  | **Edit Accounts** | Opens the **Edit Accounts** screen. From here, the user can **rename**, **re-enroll**, **reorder**, and **delete** accounts |
|  | **Change PIN** | Opens the **PIN Selection** screen, allowing the user to change the registered PIN |
|  | **About** | Opens the **About** screen, which displays the **Passcode** version number |
|  | **Minimize and Quit** | Minimizes the application window or exits the application |

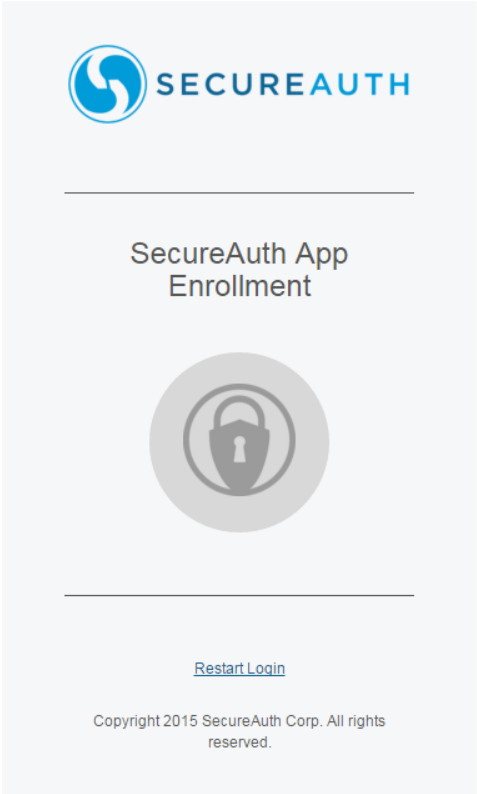
**Edit Accounts Screen**

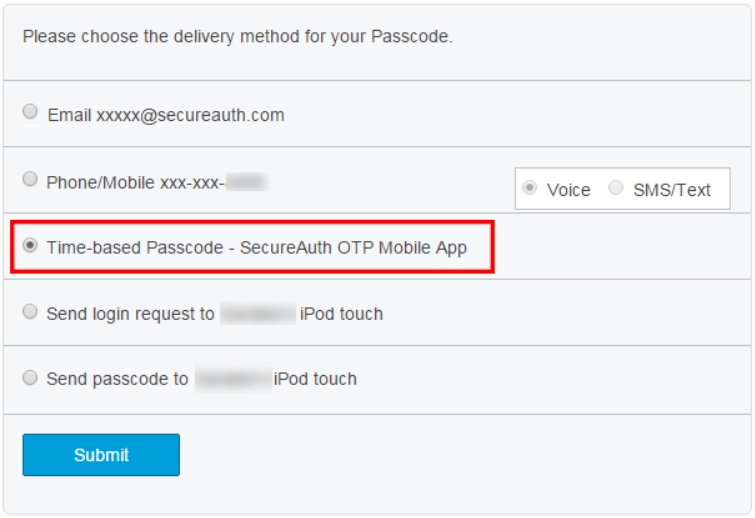



| | | |
|---|---|---|
|  | **Rename** | Renames the provisioned account |
|  | **Re-enroll** | Clears out the provisioning data for the account and restarts the **Provisioning** process |
|  | **Reorder** | Drag the 3 bars to reorder the accounts listed on the OTP panel |
|  | **Delete** | Click to delete the provisioned account |

## End-user Experience

In **SecureAuth IdP 9.0.2+**, when the end-user is presented the page of Multi-Factor Authentication methods from which to choose, the Multi-Factor Authentication method that was last selected and used in a successful login attempt persists as the default method for the next login in each device / browser




1. Initiate the login process on a realm that enables OATH OTPs as a second-factor option (configured on the **Registration Methods** tab of the realm)

2. Follow the configured workflow

3. Once on the Multi-Factor Authentication methods page, select **Time-based Passcode** from the list of options, and click **Submit**

⚠ By default, the listing for the **Time-based Passcode** option is followed by the text "**SecureAuth OTP Mobile App**"

However, this listing applies to all devices and browsers provisioned for Single (OATH Seed) mode – e.g. mobile apps, desktop apps, etc.

In environments that support more than one type of OTP app, the end-user may not know this option also applies to desktop OTP apps

For these scenarios, SecureAuth recommends replacing the **SecureAuth OTP Mobile App** label with a more generic name – e.g. **SecureAuth OTP App** – to improve the end-user experience and to minimize confusion

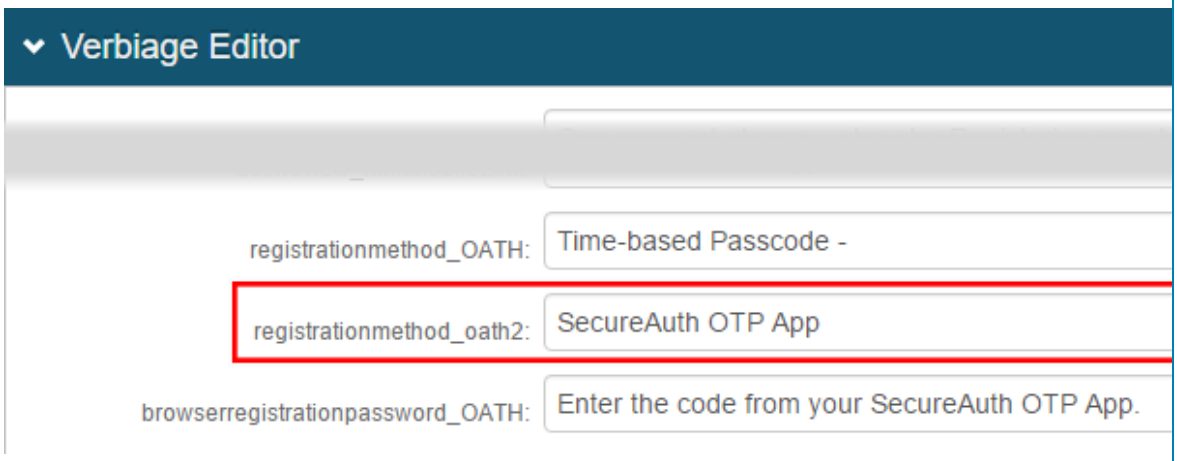
These configuration steps can be applied to any Passcode app provisioned for OATH Seed (Single) mode (based on Multi-Factor App Enrollment Realm configurations)

SecureAuth recommends making these modifications ***before*** end-users enroll their browsers / devices to avoid any caching issues on the client-side pages

## Overview


1. In the **Advanced Settings** section, click **Content and Localization**

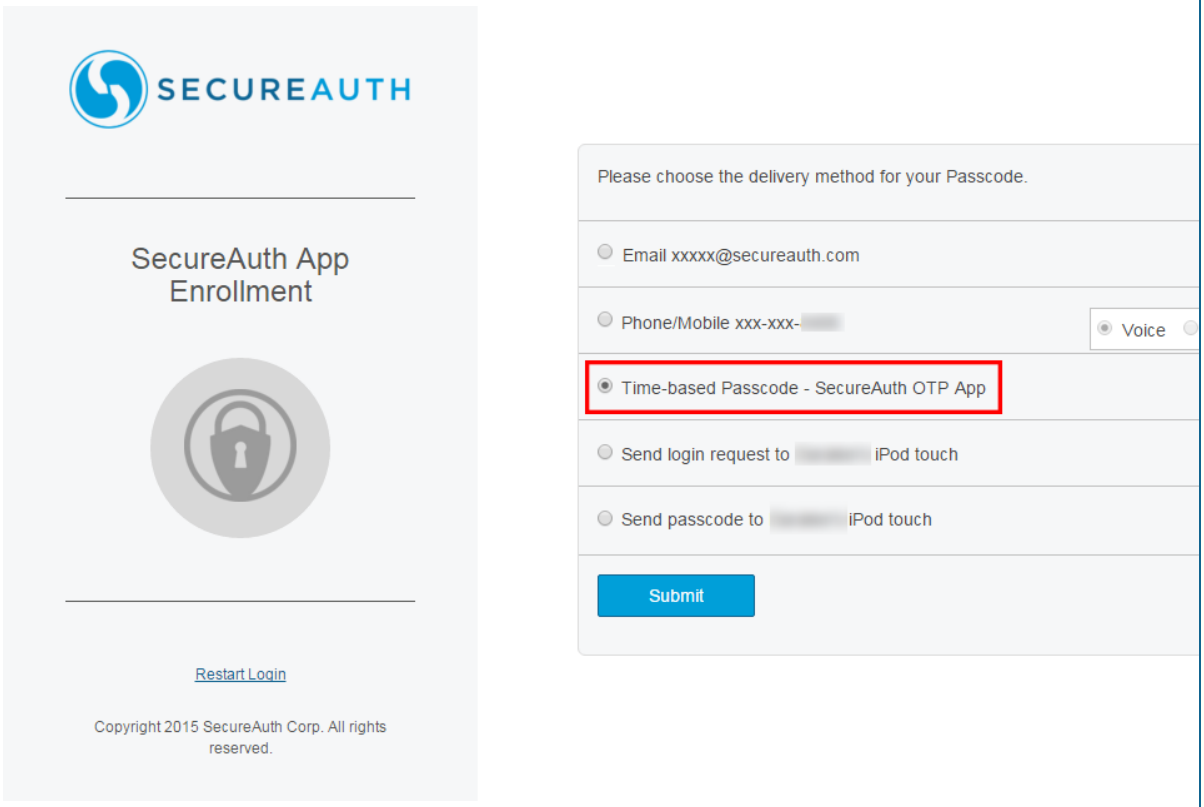
### Verbiage Editor




2. Search for the **registrationmethod_oath2** field and alter the content, e.g. **SecureAuth OTP App**

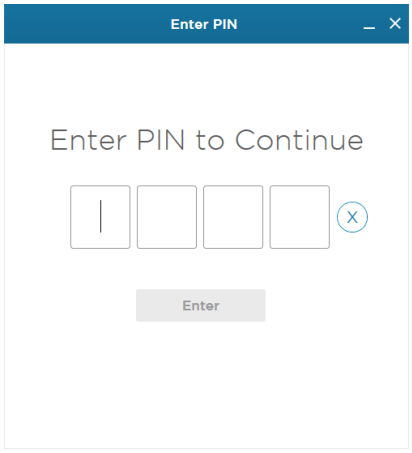
Click **Save** once the configurations have been completed and before leaving the **Content and Localization** page to avoid losing changes

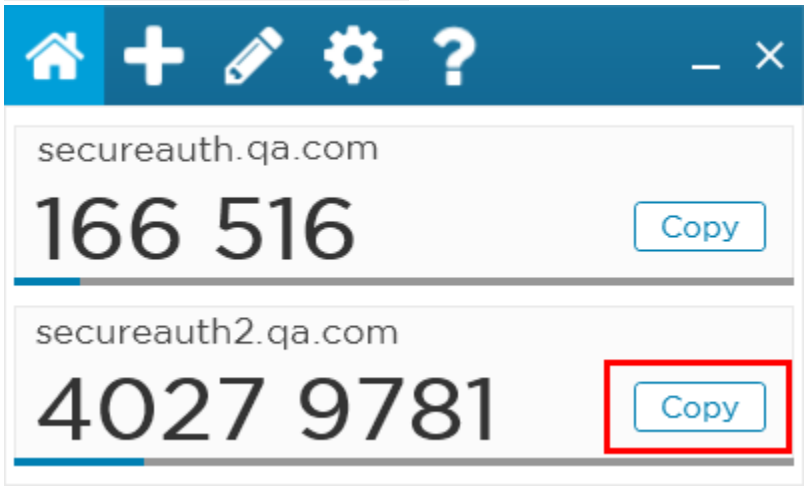
**Example Output**




On the **Registration Methods** page, the option now displays as **Time-based Passcode - SecureAuth OTP App**

The **Time-based Passcode - SecureAuth OTP Mobile App** option is for ***all*** devices and browsers that are provisioned for **OATH Seed (Single)** mode; therefore, if using more than one OTP app (mobile apps, desktop apps, etc.), then a generic name is recommended, e.g. **SecureAuth OTP App**

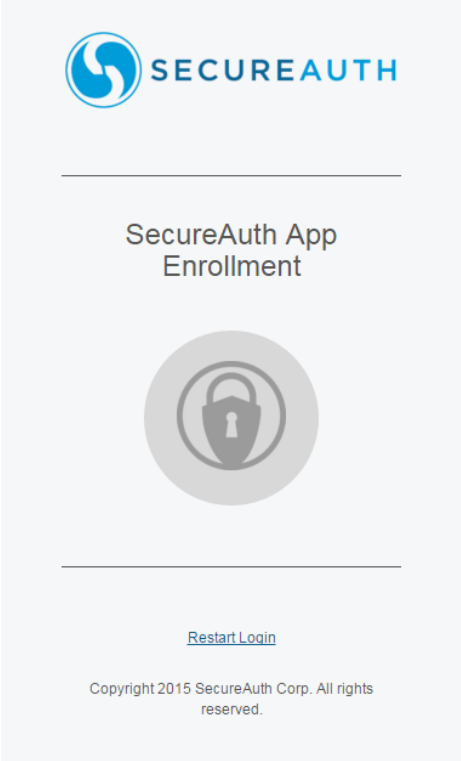


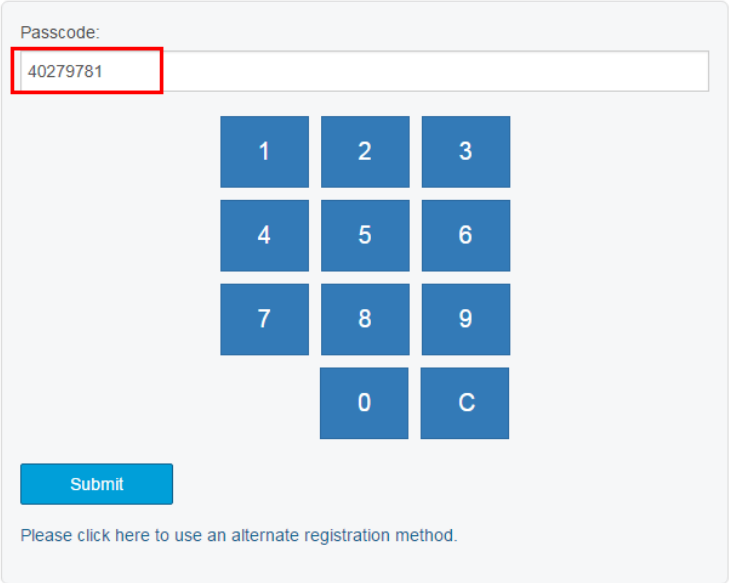




4. Start the **Passcode** app

5. If a PIN is required to unlock the app, input the **PIN** and click **Enter**

6. On the account tile, click **Copy** to grab the passcode




7. Paste the passcode from the app onto the login page, and click **Submit** to gain access to the realm

## Release Notes

### Version 2.0

**Released on November 1, 2016**

| New Features |
| --- |
| Multiple account support |
| New UI and Branding (formerly SecureAuth Windows Desktop OTP Client) |
| Weak PIN protection |
| PIN brute force protection |
| Roaming profile support (Windows only) |
| Application hardening |
| **Resolved Issues** |
| Installation path defaults to Windows standards |
| Security and stability improvements |