SecureAuth 2FA end user set-up instructions

End-user experience

Updated April 30, 2021

The following sections describe the set-up steps that end users must complete to use two-factor authentication methods to log in.

The steps are starting points for SecureAuth administrators to customize for end users. Technically experienced end users might be able to set up their devices with the steps as shown, while technically inexperienced end users might need more guidance included in the steps.

We hope these steps, along with the email templates, help your team throughout the organization's onboarding journey.

Contents

Security code setup 2
  Password setup 3
  Set up for 2FA with phone, email, PIN, and security questions 4
Mobile app setup 5
  Connect with QR Code 5
  Connect with URL 8
  Paired Watch setup 12
Passwordless with FIDO2 WebAuthn device registration and management 13
Passwordless fingerprint setup 20
  Enroll a fingerprint 20
  Log onto Login for Windows after enrolling a fingerprint 21
<Different Primary Credential Provider> setup 23
YubiKey setup 24

Security code setup

Admins: Guide end users to set up the following options to obtain a security code (phone or email passcode, PIN, security answers) to use as a two-factor authentication method:

- Password setup
- Set up for 2FA with phone, email, PIN, and security questions

Only include steps for the 2FA methods you make available to your end users. Be sure to include sample guidance screenshots where mentioned in the following instructions. Notes to administrators begin with Admins; instructions and screenshots for admins to customize are highlighted in yellow.

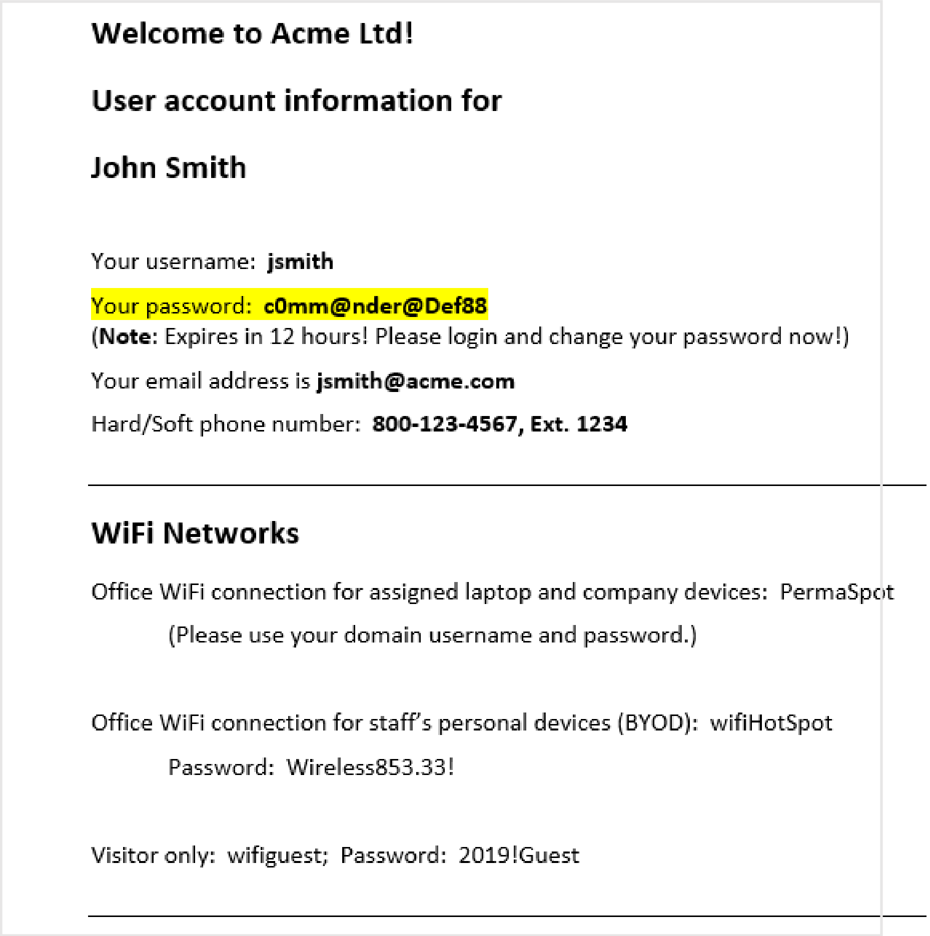
Password setup

Admins: If your organization uses passwordless login, skip this topic and proceed to Set up for 2FA with phone, email, PIN, and security questions.

If your organization uses passwords to log in, you will typically give new employees a temporary password to access the corporate network that is valid for a set amount of time. After first log in, employees must reset their password within the time expiration period. End users need a username and password to register for two-factor authentication (2FA).

If end users need to login when their machine is offline, they must choose an OATH-based method during the first login. After end users select a timed authentication option and enter their password, TOTP and HOTP passcode options will be available for them to use when logging on the machine offline.

The password is typically given to end users by administrators, the IT Support team, or Help Desk in a new employee welcome packet or hard copy sheet of paper, so end users can complete registration. The communication might look like this:



Welcome to Acme Ltd!

User account information for

John Smith

Your username: **jsmith**

Your password: **c0mm@nder@Def88**
(**Note:** Expires in 12 hours! Please login and change your password now!)

Your email address is **jsmith@acme.com**

Hard/Soft phone number: **800-123-4567, Ext. 1234**

WiFi Networks

Office WiFi connection for assigned laptop and company devices: PermaSpot

(Please use your domain username and password.)

Office WiFi connection for staff's personal devices (BYOD): wifiHotSpot

Password: Wireless853.33!

Visitor only: wifiguest; Password: 2019!Guest

Alternatively, if your organization allows end users to use their personal email address for registration, you will need to communicate that information to your end users.

Next, end users are ready to set up the 2FA method they will use to log into the corporate network.

Set up for 2FA with phone, email, PIN, and security questions

Admins: Copy and customize the steps before adding them to the SecureAuth email template. Remove steps for the methods you have not enabled.

If end users need to login when their machine is offline, they must choose an OATH-based method during the first login. After end users select a timed authentication option and enter their password, TOTP and HOTP passcode options will be available for them to use when logging on the machine offline.

The following information will be used for 2FA only. SecureAuth uses your contact information to send you a security code, which is used to verify your identity for access to your corporate network (such as email) and applications (such as Microsoft Office 365).

1. Open a browser and log into the following link to open the self-service portal:
   <Enter URL here>

2. Enter your phone number in the <insert label here> field.
   <Enter a screenshot of your self-service portal here. Highlight the phone field users need to fill out.>

3. Enter your email in the <insert label here> field.
   <Enter a screenshot of your self-service portal here. Highlight the email field users need to fill out.>

4. Enter a PIN with <x> digits.
   - PIN cannot contain consecutive, repeating digits; for example: 33333333 or 1111
   - PIN cannot be forward or backwards sequential; for example: 123456 or 87654321

   <Enter a screenshot of your self-service portal here. Highlight the PIN field users need to fill out.>

5. Provide answers to security questions. Keep in mind the following:
   - Answers are case insensitive, so if your answer is *Mustang*, you can also enter *mustang*.
   - Answers can be multiple words, such as *Main Street*.
   - Answers can be letters or numbers only.
   - Answers can be as short as two characters.

   <Enter a screenshot of your self-service portal here. Highlight the security questions users need to fill out.>

6. Review the information you entered and then save your changes.

Mobile app setup

Admins: Copy and customize the steps before adding them to the SecureAuth email template.

If end users need to login when their machine is offline, they must choose an OATH-based method during the first login. After end users select a timed authentication option and enter their password, TOTP and HOTP passcode options will be available for them to use when logging on the machine offline.

Use these steps to download and set up the SecureAuth Authenticate mobile app for iOS or Android devices. After setting up the mobile app, use it to log in with one of the following methods:

<Delete the methods you have not enabled for your organization.>

- Login confirmation: Notifications that will ask you to accept or deny a login attempt.
- Notification passcode: Passcodes delivered to your device through app notification.
- Timed passcode: Passcodes that live in and are generated from the app. Use a timed passcode to log in when you are offline.
- Face or fingerprint recognition: Notifications that will ask you to use your mobile device's face or fingerprint recognition.

In addition to iOS and Android devices, you can also set up and use SecureAuth Authenticate on a Chromebook, which is viewed as an Android device. Although the following screens do not show a Chromebook user interface, the Android screen examples are the same as what you will see on a Chromebook.

IMPORTANT:

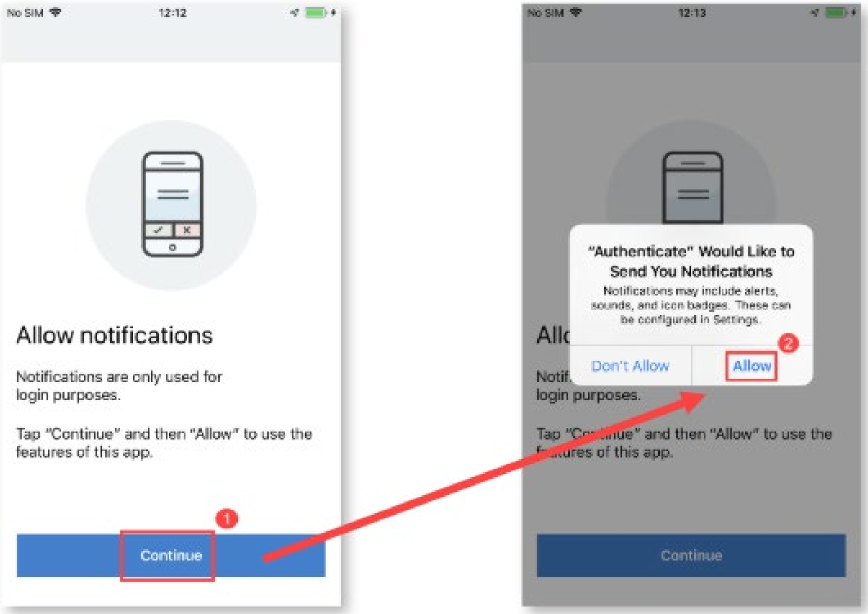
- If using a Chromebook, ensure it has a working webcam.
- <If end users will enter a URL to connect, give them the web address of the SecureAuth IdP app enrollment realm. See Connect with URL.>

Connect with QR Code

1. Download and install the SecureAuth Authenticate mobile app.
   iOS: https://itunes.apple.com/us/app/secureauth-otp/id615536686
   Android: https://play.google.com/store/apps/details?id=secureauth.android.token&hl=en_US

2. Log in to the following webpage **on your desktop computer:**
   <Enter the QR code enrollment realm URL here.>

3. After successfully logging in, open the mobile app. iOS users will see a message requesting that you enable push notifications on your mobile device. (Push notifications are enabled by default for Android users.) This is required for you to use the login request feature on the app.



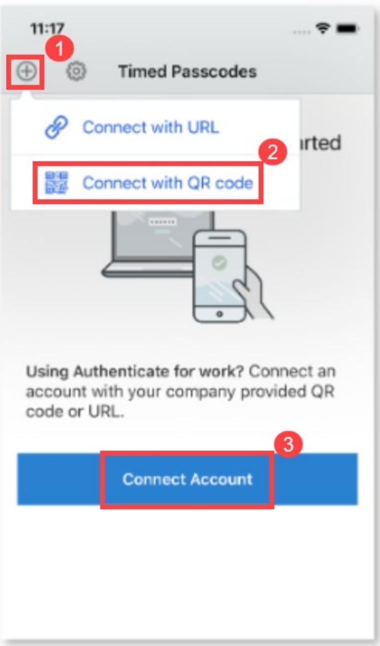
Allow notifications

Notifications are only used for login purposes.

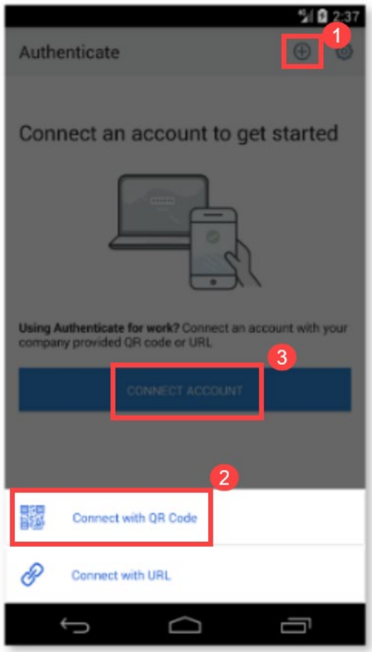
Tap "Continue" and then "Allow" to use the features of this app.

"Authenticate" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

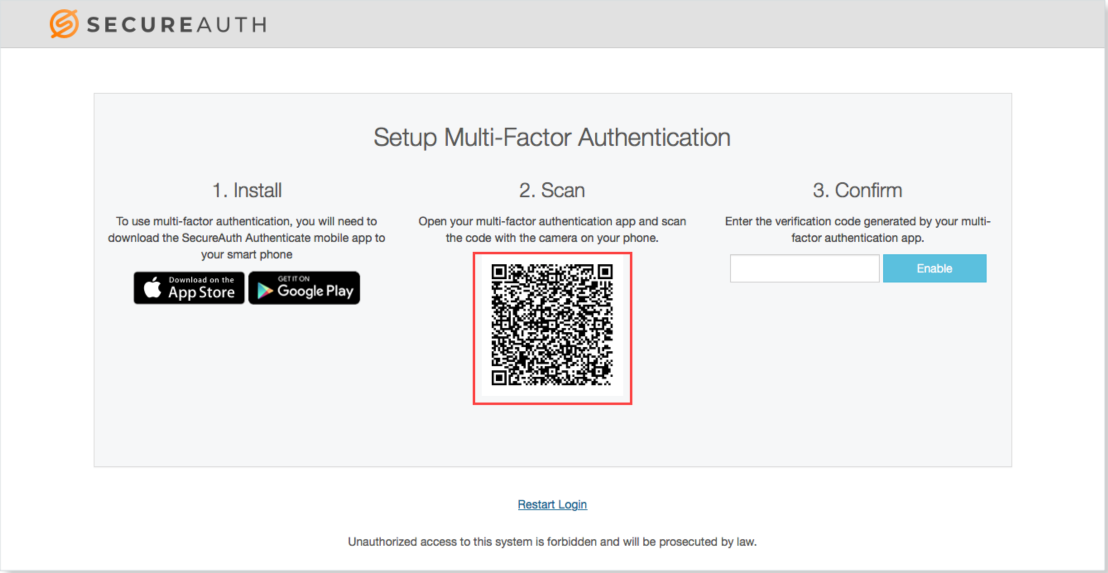


Using Authenticate for work? Connect an account with your company provided QR code or URL.



Connect an account to get started

Using Authenticate for work? Connect an account with your company provided QR code or URL.


SECUREAUTH

Setup Multi-Factor Authentication

1. Install

To use multi-factor authentication, you will need to download the SecureAuth Authenticate mobile app to your smart phone

2. Scan

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

3. Confirm

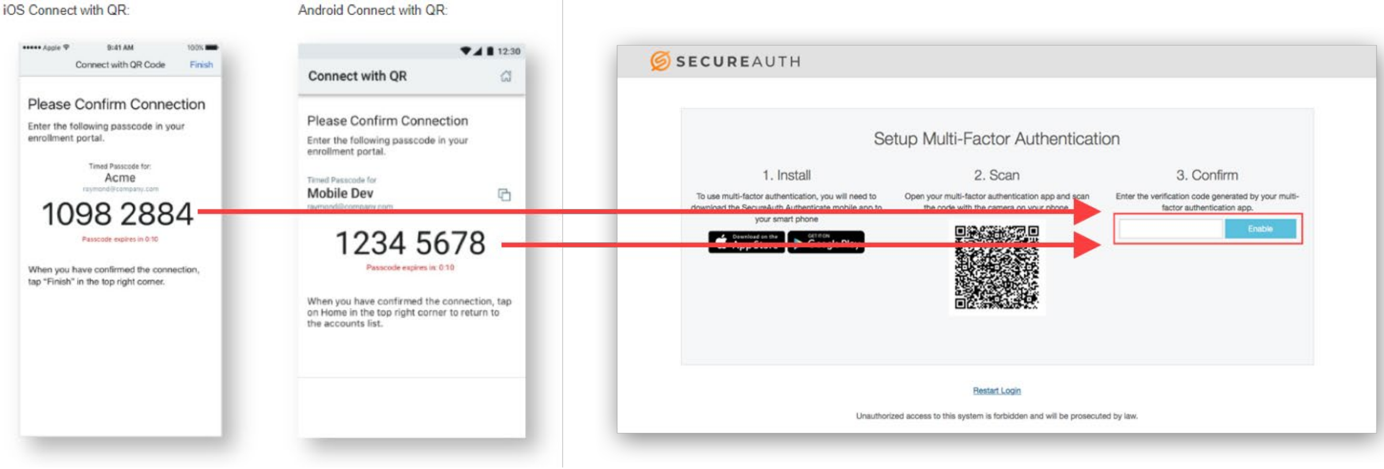
Enter the verification code generated by your multi-factor authentication app.

Unauthorized access to this system is forbidden and will be prosecuted by law.

The QR code is valid for 10 minutes, by default. <Optionally, change the time length in SecureAuth® Identity Platform. See "Change the QR code scan availability time length" in Multi-Factor App Enrollment (QR Code) realm configuration.>

If using a Chromebook, take a picture of the unique QR code on the page and hold the code (on a phone or printout) up to the webcam to scan it in.

6. Follow directions to create an account PIN. <Remove this step if you have not enabled a PIN.>


iOS Connect with QR:

Please Confirm Connection

Enter the following passcode in your enrollment portal.

Timed Passcode for:
Acme
raymond@company.com

1098 2884

Passcode expires in 0:10

When you have confirmed the connection, tap "Finish" in the top right corner.

Android Connect with QR:

Please Confirm Connection

Enter the following passcode in your enrollment portal.

Timed Passcode for
Mobile Dev
raymond@company.com

1234 5678

Passcode expires in: 0:10

When you have confirmed the connection, tap on Home in the top right corner to return to the accounts list.

SECUREAUTH

Setup Multi-Factor Authentication

1. Install

2. Scan

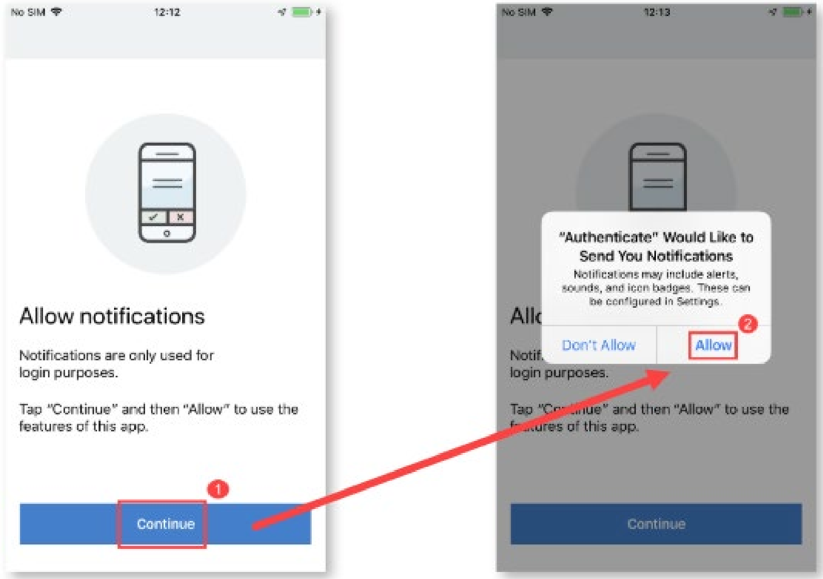
3. Confirm

Unauthorized access to this system is forbidden and will be prosecuted by law.

8. On the mobile app, tap **Finished** or the home icon.

Connect with URL

1. Download and install the SecureAuth Authenticate mobile app.
   iOS: https://itunes.apple.com/us/app/secureauth-otp/id615536686
   Android:
   https://play.google.com/store/apps/details?id=secureauth.android.token&hl=en_US



Allow notifications

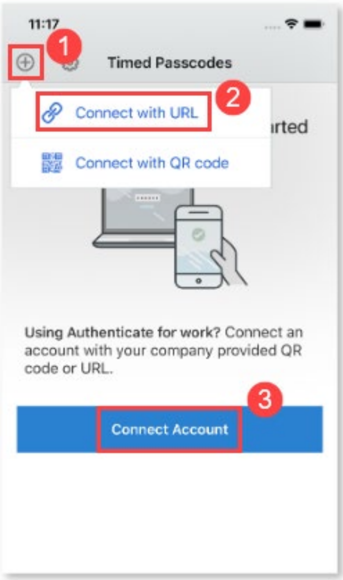
Notifications are only used for login purposes.

Tap "Continue" and then "Allow" to use the features of this app.

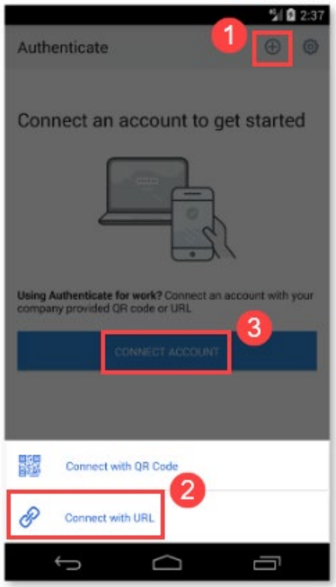
"Authenticate" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

3. Tap the plus sign (+) to add an account. Select **Connect with URL**.



Using Authenticate for work? Connect an account with your company provided QR code or URL.



Connect an account to get started

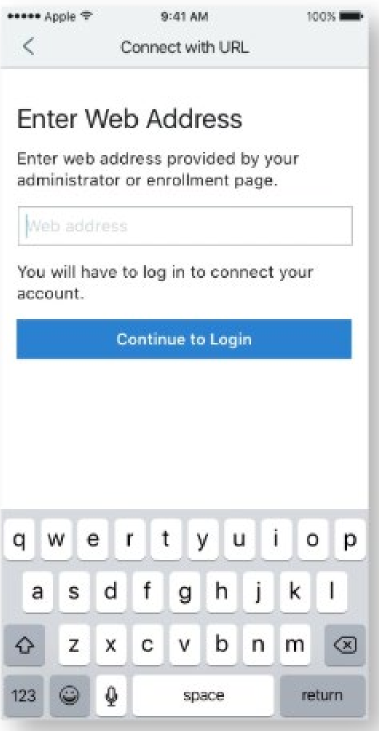
Using Authenticate for work? Connect an account with your company provided QR code or URL.

4. Enter the following web address: <Enter the URL enrollment realm URL here.>

   <Tell end users which of the following to use in your instructions.>
   If you are using the default SecureAuth998 URL realm, you can enter the Fully Qualified Domain Name, for example, secureauth.company.com.

   If you are using a different realm for Multi-Factor Authentication URL app enrollment, then you must enter the entire URL address that includes the realm name, for example, https://secureauth.company.com/secureauth2.

iOS Connect with URL screen:

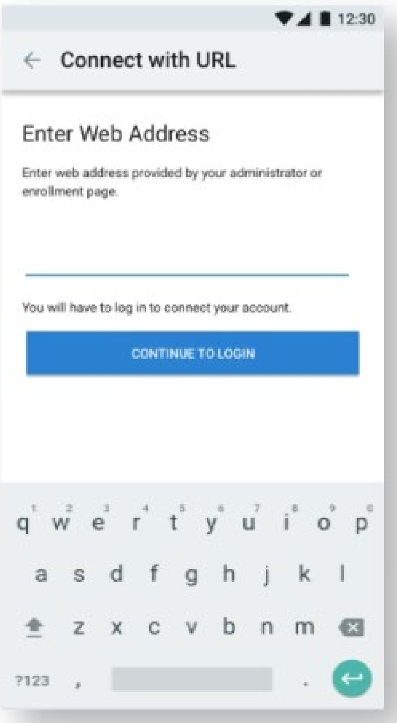


Enter Web Address

Enter web address provided by your administrator or enrollment page.

You will have to log in to connect your account.

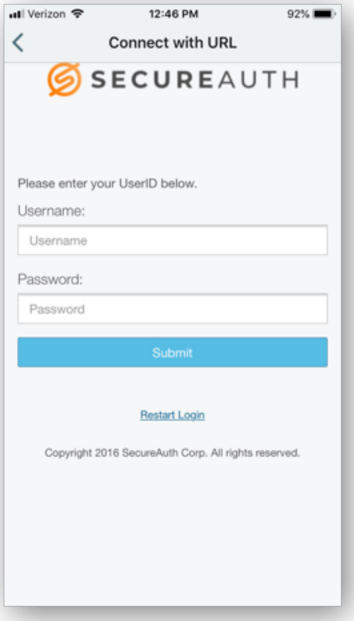
Android Connect with URL screen:



Enter Web Address

Enter web address provided by your administrator or enrollment page.

You will have to log in to connect your account.



Please enter your UserID below.

Username:

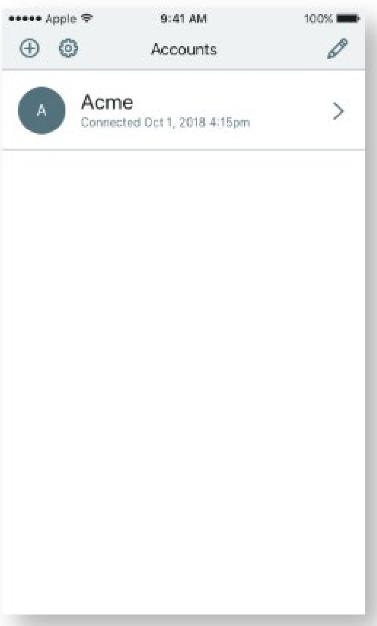
Password:

Copyright 2016 SecureAuth Corp. All rights reserved.

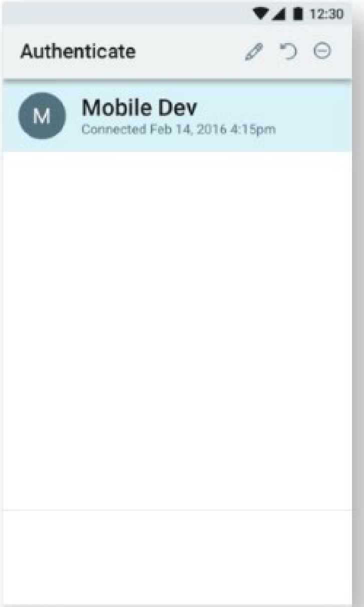
6. Follow the directions to create an account PIN. <Remove this step if you have not enabled a PIN.>

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

iOS Accounts screen:



Android Accounts screen:



Admins:

- If you have enabled biometric ID use for end users, tell them it is available. Explain the following: To use face or fingerprint recognition as a second factor, turn on face or fingerprint recognition on your mobile device now, **before** setup.
- If end users' mobile phones are set up for face or fingerprint recognition before setup, then the features will work automatically with the SecureAuth mobile app after setup.
- If end users want to use face or fingerprint recognition after setup, but didn't turn on the features before setup, they must turn on face or fingerprint recognition on their mobile device, then setup the SecureAuth mobile app again.
- Ensure that push notifications are enabled on end users' mobile device to log in with face or fingerprint recognition on the app. Guide end users to set push notifications when they start the app or in the device's settings.

Paired Watch setup

Admins: Copy and customize the steps before adding them to the SecureAuth email template.

You can use an Apple Watch or Android Wear watch paired to your mobile device to receive notification passcodes, login confirmations, and view your timed passcodes.

The paired watch does not require any set up, but you must complete Mobile app setup for the watch your device is paired with.

Passwordless with FIDO2 WebAuthn device registration and management

Admins: Copy and customize the steps before adding them to the SecureAuth email template. Passwordless authentication using FIDO2 WebAuthn is supported with the following criteria:

- SecureAuth® Identity Platform version 20.06 or later
- Available to sites running the Prevent package
- If your end users are new to FIDO2 WebAuthn, see How SecureAuth FIDO2 WebAuth works.

IMPORTANT:

- <Admins: End users must register their FIDO2-enabled devices. Give them the FIDO Enrollment URL to connect to the registration page. Find the URL in the Identity Platform > Multi-Factor Methods page > click FIDO2 (WebAuthn) edit icon > FIDO Enrollment URL. Alternatively, if end users will use your company portal, send the appropriate URL.>
- If you set device restrictions for roaming authenticators when setting up MFA options in the Identity Platform, you must tell your end users to provide verification (for example, PIN) for enrollment and authentication when using a roaming device. Learn more about PIN support for roaming devices in Admin troubleshooting PIN support for FIDO2 WebAuthn.
- If you restricted the number of devices end users can register to use for authentication, include the number in your instructions to end users so they don't receive an error message when attempting to register more than the maximum allowed. You can also specify whether end users can replace a device with a new device when they reach the maximum limit. Additionally, you can specify whether end users can remove their own devices from the enrollment page. Learn more in FIDO2 WebAuthn global MFA settings. Be sure to tell end users the actions they can and cannot perform.
- If your company is new to using passwordless, see Passwordless secure login. This short topic addresses some common concerns end users often have about security when moving to passwordless. It also contains a one-minute video with a simple, visual explanation of risk checks.

Using FIDO2 WebAuthn replaces the traditional password with strong passwordless log-in options, such as fingerprint recognition and security keys. Although entering a password sometimes makes people feel secure, using a passwordless option is much more secure because of the added security checks that occur in the background. With a passwordless log-in option, you can easily use a registered device to securely log in to company applications.

If you will use a laptop, desktop, mobile phone, or tablet as your FIDO2 device, they must be supported by at least one of the following operating systems (OS):

- Windows OS
- Mac OS
- Android OS

Use one or more of the following devices for passwordless with FIDO2 login:

<Delete the methods unavailable to your end users.>

- Security key, such as YubiKey; use as an external device
- Bluetooth security key, such as Titan; use as an external device
- Fingerprint recognition; use as a built-in or attached device on laptop or desktop
- Android device; use as a built-in device with the device's screen lock (fingerprint recognition, PIN, or pattern)
- Personal identification number (PIN); use as a built-in device on laptop or desktop

1. In a Google Chrome, Firefox, Microsoft Edge, or Apple Safari browser, enter the URL to the [SecureAuth FIDO2 | company portal] registration page sent by your administrator.

   Log in using your username, password, and available two-factor authentication method.

   <Admin: add HTTPS URL from FIDO2 (WebAuthn) page; remove if sending link to company portal>

   <Admin: The FIDO2 registration and authentication web page for your end users requires HTTPS in the URL.>

   Example: https://example.secureauth.com/SecureAuth7

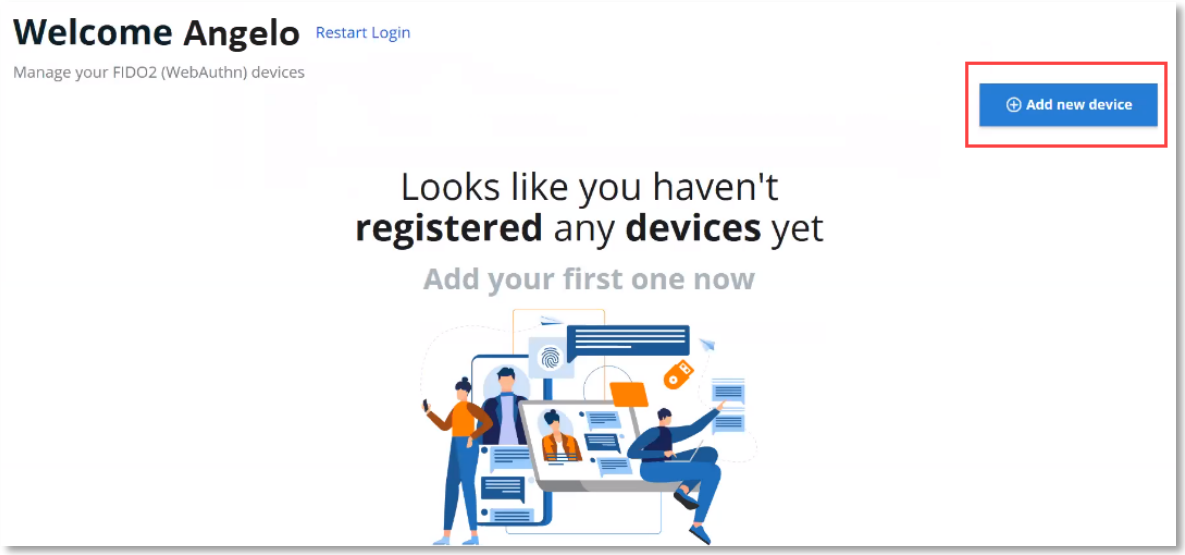
   <Admin: add link to company portal; remove if sending URL from FIDO2 (WebAuthn) page>
   Example: https://portal.example.com/SecureAuth7/SecurePortal.aspx

   [If using a company portal, add a screenshot of the portal, highlighting the FIDO2 tile. Instruct end users to click the tile.]

   Keep this link handy because you will use it whenever you need to register another device (such as a new security key or phone) or manage a registered device (remove or edit a device).

   If you are not sure if your device is FIDO2-compliant, check the device serial number on the device website to ensure FIDO2 compliance.

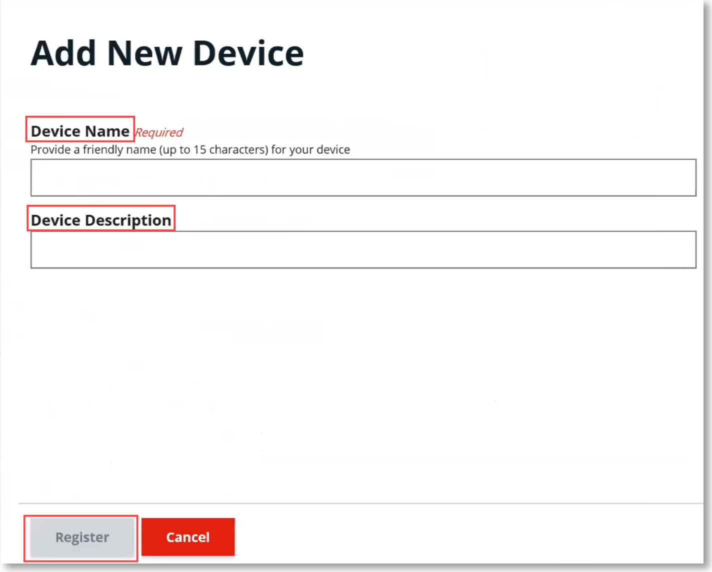
2. On the registration page, click **Add new device** at the top right.


Welcome Angelo
Restart Login
Manage your FIDO2 (WebAuthn) devices
Add new device
Looks like you haven't registered any devices yet
Add your first one now

3. In the **Add New Device** page, enter a device name and device description.

   Example of device name: Galaxy S20 or YubiKey5

   Example of description: Asha's Samsung or Juan's YubiKey NFC

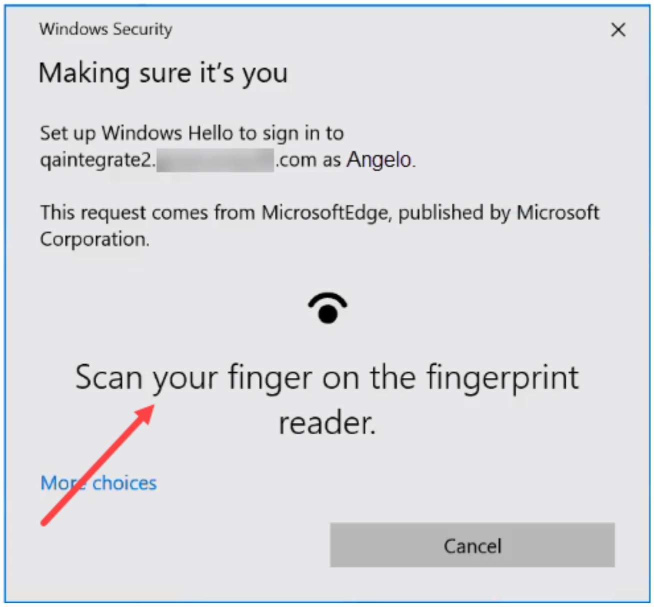


5. Click **Register**.

   <Admin: The following paragraphs describe the WebAuthn browser behavior. If your users are technical, you can delete the paragraphs; if not, read the content carefully to decide the level of information that will guide your users to success.>

   The browser and OS (Windows OS, Mac OS, etc.) you are using control the registration screens and login options you see.

   For example, you have set up Windows Hello for fingerprint identification and now are setting up a Titan security key. You set the device name and description, then click **Register**. You might see a message like the following from the Microsoft Edge browser, requesting you to sign in with a fingerprint, even though you are now setting up a Titan security key.



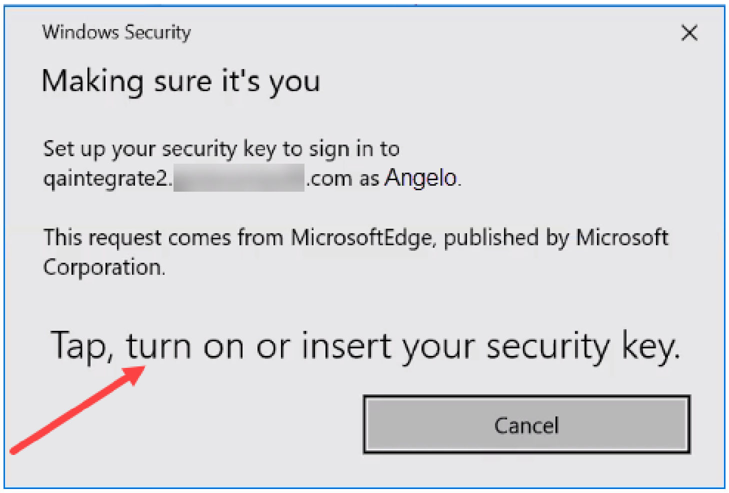
Making sure it's you

Set up Windows Hello to sign in to qaintegrate2.[redacted].com as Angelo.

This request comes from MicrosoftEdge, published by Microsoft Corporation.

Scan your finger on the fingerprint reader.

You can cancel out of that message and then you will see another message from the Microsoft Edge browser requesting you to sign in with your security key.



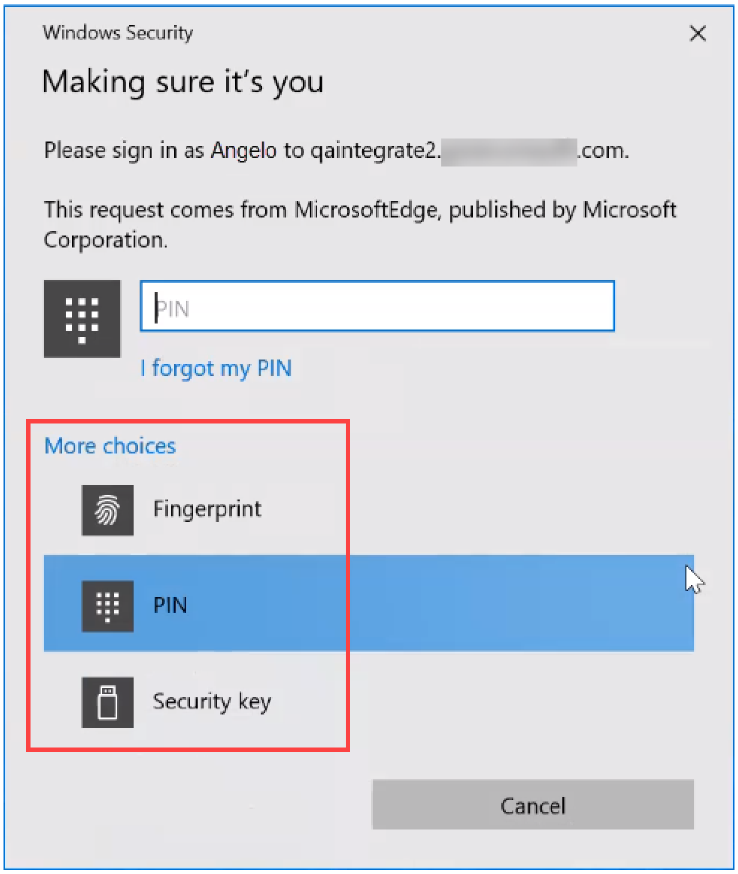
Making sure it's you

Set up your security key to sign in to qaintegrate2.[redacted].com as Angelo.

This request comes from MicrosoftEdge, published by Microsoft Corporation.

Tap, turn on or insert your security key.

After registration, when you select FIDO2 from your company's login choices, you might see several choices to log in because the browser tracks all the ways you have set up to register. For example, if you previously set up a PIN as a login method, then the Microsoft Edge browser will show a Windows Hello PIN choice along with the fingerprint and security key methods you set up.



Windows Security

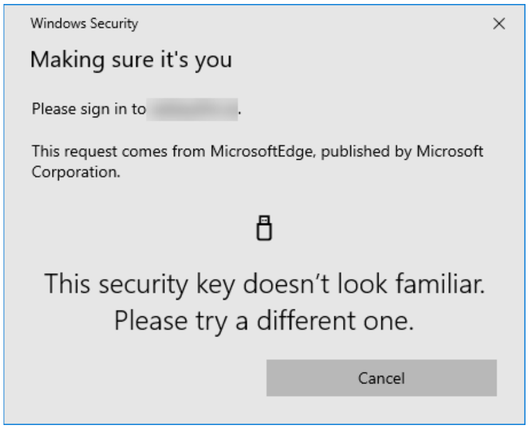
Making sure it's you

Please sign in as Angelo to qaintegrate2.[redacted].com.

This request comes from MicrosoftEdge, published by Microsoft Corporation.

Note that you must use the device you register to log in to a resource, such as Office 365; otherwise, the following will happen:

In this scenario, you have two FIDO2-compliant YubiKey security keys. You register one, log in, and then place the key on the desk next to the other YubiKey. The next time you log in, you use the YubiKey that is not registered. You will see a browser message like the following:



Windows Security

Making sure it's you

Please sign in to [redacted].

This request comes from MicrosoftEdge, published by Microsoft Corporation.

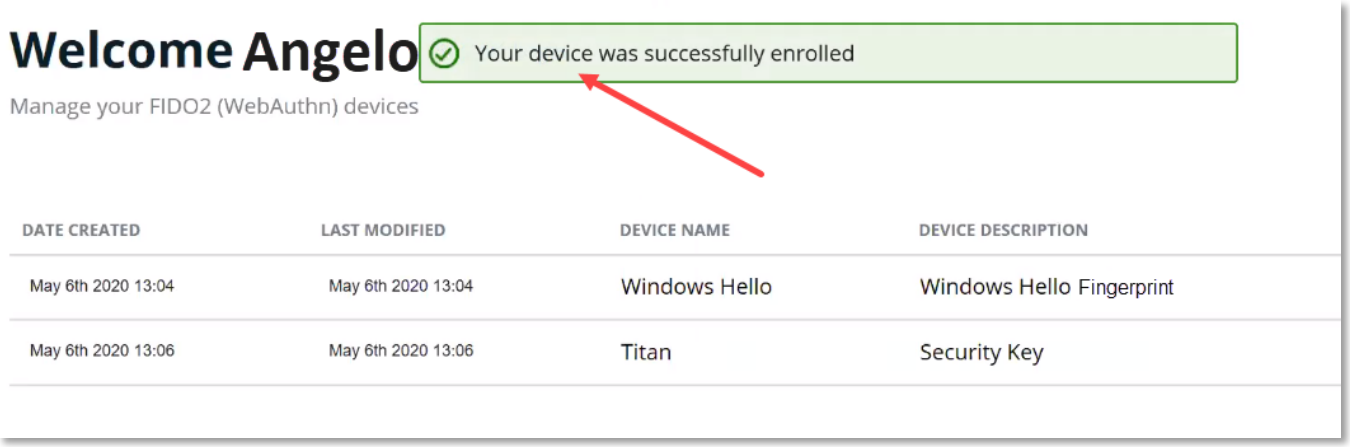
This security key doesn't look familiar. Please try a different one.

Troubleshooting tip: If you receive an error message stating that your device was not registered, try the following workarounds:

- Device is already registered. Verify the device registration by opening the registration page at the address your administrator sent you, in step 1.
- Device is iOS. SecureAuth currently does not support FIDO2 on iOS devices, so you cannot use an iPhone, iPad, or iPad mini for passwordless log in. (Several other options for passwordless login are available. Refer to the information above step 1.)
- Device is not FIDO2- or Universal two-factor (U2F)-compliant. Register a different device that is FIDO2-compliant. Alternatively, you can use the device to log in, but you will have to provide a password.
- Web browser lost connection. Refresh the browser and try registering the device again.

<Admin: During registration, SecureAuth makes a call to the FIDO alliance to obtain information about the device's attestation certificate. The end user device data must match the FIDO device data, or the end user will see the following message: "We can't register your device because it doesn't meet our FIDO2 requirements. Try registering with a different device. If this doesn't work, contact your administrator.">

6. On the [SecureAuth FIDO2 registration page | your company portal], you will see the device name and description that you specified.



Welcome Angelo

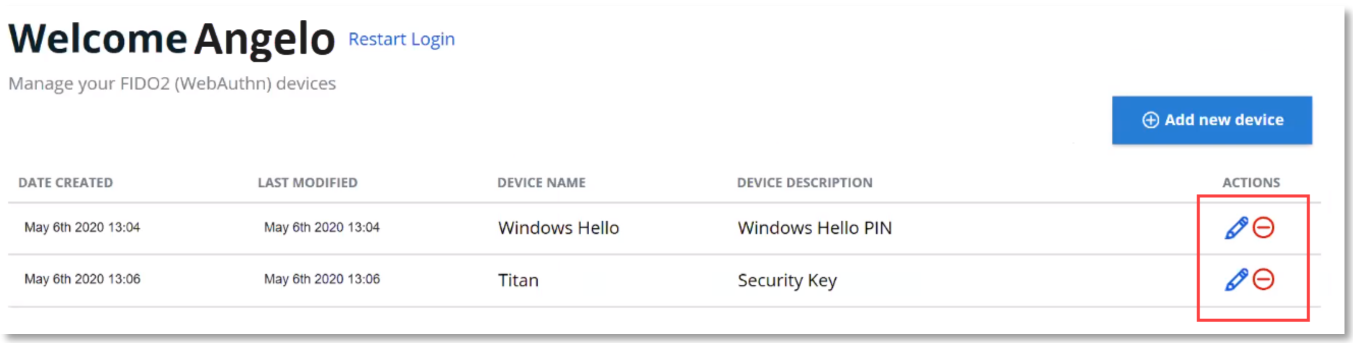
Your device was successfully enrolled

Manage your FIDO2 (WebAuthn) devices

DATE CREATED	LAST MODIFIED	DEVICE NAME	DEVICE DESCRIPTION
May 6th 2020 13:04	May 6th 2020 13:04	Windows Hello	Windows Hello Fingerprint
May 6th 2020 13:06	May 6th 2020 13:06	Titan	Security Key

<Admin: For company portal, change screenshot to show successful registration.>

7. Repeat steps 2 - 7 to set up another device. Think about the devices (mobile phone, desktop, laptop, security key, tablet) you will use to access a company app and register the device, so it is ready for use.
8. Edit a device by clicking the pencil icon to the right of the device name.
9. Delete a device by clicking the red minus icon to the right of the device name.



Welcome Angelo

Manage your FIDO2 (WebAuthn) devices

DATE CREATED	LAST MODIFIED	DEVICE NAME	DEVICE DESCRIPTION	ACTIONS
May 6th 2020 13:04	May 6th 2020 13:04	Windows Hello	Windows Hello PIN	✎ ⊖
May 6th 2020 13:06	May 6th 2020 13:06	Titan	Security Key	✎ ⊖

Passwordless fingerprint setup

Admins: Copy and customize the steps before adding them to the SecureAuth email template. Fingerprint recognition without a password is supported with the following criteria:

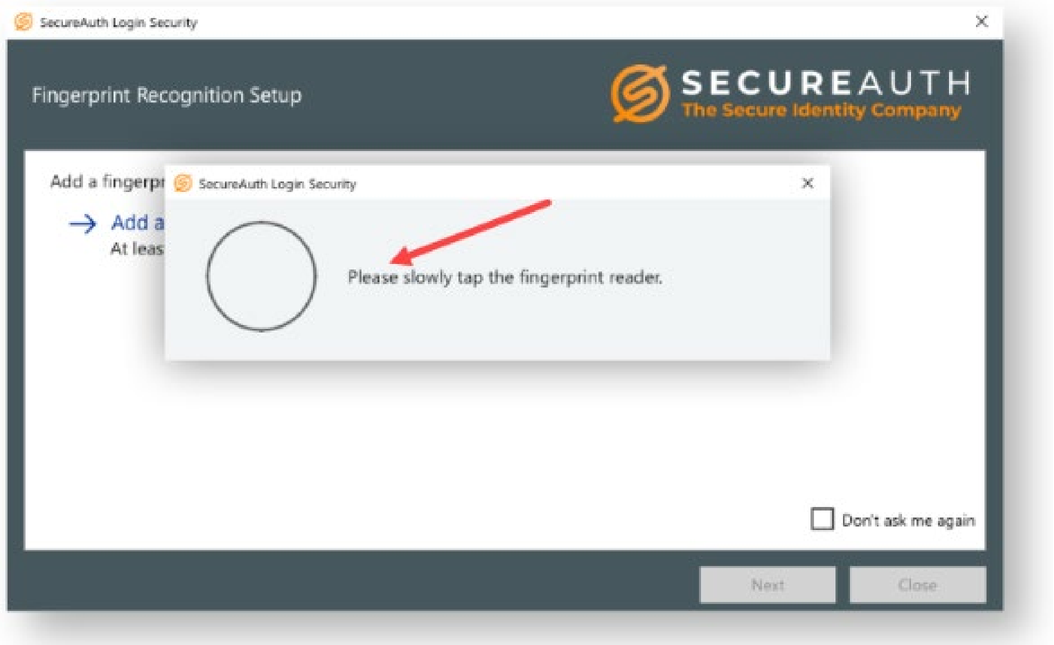
- SecureAuth IdP 9.2 or later running on Windows 10 version 1607 or later OR
- SecureAuth® Identity Platform version 19.07 or later running on Windows 10 version 1607 or later
- Available to sites running the Prevent package

Use these steps to set up one or more fingerprints to use as a passwordless method to log in:

Enroll a fingerprint

1. Connect the fingerprint reader to your Windows machine, if necessary.
2. Log onto Login for Windows with your Windows password.

   If offline, choose an OATH-based method, such as <admin fill in what is set up for end users>, which you used when online.
3. The SecureAuth Fingerprint Recognition Setup screen opens. Click **Add a Fingerprint**.
4. Follow the onscreen directions to add at least one fingerprint to use to log in without a password. (You can add as many fingerprints as you want.)


SecureAuth Login Security
Fingerprint Recognition Setup
SECUREAUTH
The Secure Identity Company
Add a fingerpr
Add a
At leas
SecureAuth Login Security
Don't ask me again
Next
Close

Please slowly tap the fingerprint reader.

   Tap your finger slowly over the reader so all whorls are added. Continue to tap until you receive the message that the fingerprint was successfully created.
5. The fingerprint is called Fingerprint 1 by default. You can rename the fingerprint to something more memorable, such as Fore, Middle, Ring, Pinkie, or Thumb. Later, you might want to add or delete fingerprints; meaningful names help you identify the fingerprints you have saved.

6. Optionally, click **Add another fingerprint** and follow the onscreen directions. To add fingerprints later, go to: **Start** menu > **SecureAuth** > **Fingerprint Recognition**
7. Now your fingerprints are saved. You can use any enrolled fingerprint but remember which fingers you enrolled because **only** the enrolled fingerprints will work.
8. Log out from Login for Windows.

Log onto Login for Windows after enrolling a fingerprint

Before you can authenticate with a password only, you must pass an initial security check to verify that you are who you say you are. This entails logging on with your password for verification, then logging out, and logging in with an enrolled fingerprint.

1. Log onto Login for Windows with your Windows password. (This completes the check.)
2. Log out from Login for Windows.
3. Use an enrolled fingerprint to log onto Login for Windows.

In subsequent logins, you can use an enrolled fingerprint (without a password) to authenticate.

Note that there are a few gotchas if you disconnect an external fingerprint reader after fingerprint enrollment.

- If you use an external fingerprint reader, do not disconnect the reader from your computer before logging out; doing so will cause an error to be displayed: **Fingerprint data not found**. The fingerprint data will be found when you connect the reader to the same computer.
- If you connect the **same** external fingerprint reader, you can use the fingerprints you enrolled for authentication, instead of entering a password.
- If you connect a **different** external fingerprint reader, the new fingerprint reader might not read the enrolled fingerprint. You might need to enroll the fingerprint again, by following the instructions above, in “Enroll a fingerprint” and then verifying your identity in “Log onto Login for Windows after enrolling a fingerprint.”

Admins:

- If an end user’s password is changed from a different site, for example, from Active Directory, the fingerprint login will not work for their account until they log in again and use the new password. (Logging in again using Login for Windows will associate the new password with the enrolled fingerprints.)
- If the fingerprint reader is disconnected when end users log in with Login for Windows, consider the following scenarios:
    - If end users enroll a fingerprint using an external fingerprint reader and then disconnect it, they must enter their password the next time they log in. If they connect the **same** external fingerprint reader, they can use the fingerprints they enrolled for authentication, instead of entering a password.
    - If end users enroll a fingerprint using an external fingerprint reader and then disconnect it, they must enter their password the next time they log in. If they connect

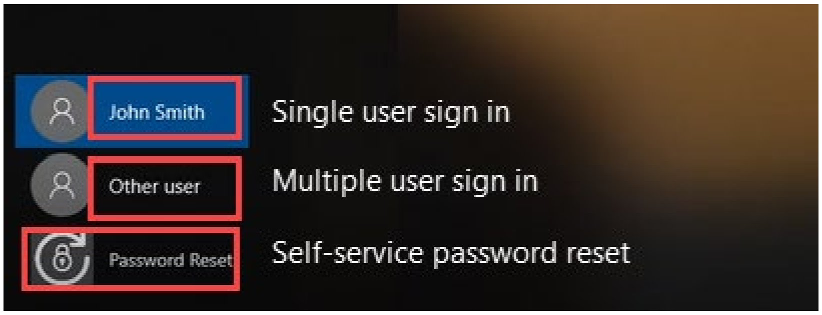
a **different** external fingerprint reader, the new fingerprint reader might not read the enrolled fingerprint. The end user might need to enroll the fingerprint again, by following the instructions above, starting with step 2.

<Different Primary Credential Provider> setup

Admins: Copy and customize the steps before adding them to the SecureAuth email template.

Use these steps to sign in by using <a different primary credential provider> on a Windows computer.

<Delete the sign-in choices you have not enabled for your organization.>



- Single user: You can sign in as yourself. The image above shows John Smith as the single user, which is where your name will be displayed. If you have different ways to log in (for example, a key and a smart card), they will be displayed for you to select.
- Multiple user: You can sign in as “Other user.” You must first specify who you are before signing in. If you have different ways to sign in (for example, a key and a smart card), they will be displayed for you to select.
- Password reset: You can reset your password. This is useful if it is time to change your password to ensure the security of your computer, are locked out by too many incorrect attempts, or any other reason. Your computer must be online (connected to the company network) to reset your password.

1. Log onto your computer.

   <You can log in in while your computer is online or offline.>

2. Sign in.

   <Enter a screenshot of credential provider login screen here. Highlight the field that end users need to use.>

   The image shows <two sign-in options/one sign-in option>, a <Microsoft> credential provider (the key icon) and a <Microsoft Smart Card> credential provider (the card icon). To sign in, click the <appropriate> icon.

   If you can sign in as "Other user", you must first specify who you are by entering your user name. Click the <sign-in options> link to choose the appropriate icon to sign in, for example, a <Microsoft> credential provider (the key icon) or a <Microsoft Smart Card> credential provider (the card icon).

3. You are now logged in.
4. Notice the placement of the Password Reset icon on the lower left. To update your password, click the icon. Your computer must be online to reset your password.

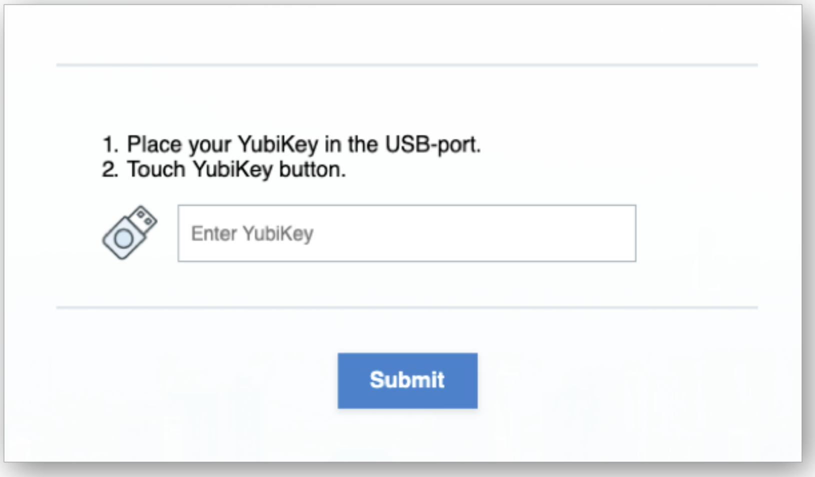
YubiKey setup

Admins: These instructions apply only if you require end users to self-provision. If you have provisioned the YubiKey for them, they do not need this setup instruction. Be sure to copy and customize the steps before adding them to the SecureAuth email template.

If end users need to login when their machine is offline, they must choose an OATH-based method during the first login. After end users select a timed authentication option and enter their password, TOTP and HOTP passcode options will be available for them to use when logging on the machine offline.

Use these steps to set up a YubiKey that provides a passcode to use as a two-factor authentication (2FA) method to log in.

1. Open a browser and log in to the following link to open the self-service portal: <Enter URL here>



1. Place your YubiKey in the USB-port.
2. Touch YubiKey button.

3. You can now use your YubiKey to log in.

   <Admins: Give the correct guidance to end users about how to use the YubiKey (press/tap), depending on how you set up the YubiKey in the SecureAuth IdP enrollment realm.>

Copyright Information

For information on support, contact your SecureAuth support or sales representative:

Email: support@secureauth.com
inside-sales@secureauth.com

Phone: +1-949-777-6959 or +1-866-859-1526

Website: https://www.secureauth.com/support
https://www.secureauth.com/contact