PingID End User Guide

June 4, 2025

Table of Contents

Secure authentication with PingID

What do you want to do?

Pair › Authenticate › You're in!

I forgot my device | My device was stolen

- Pair a device with PingID

  Register your device to start using PingID

- Authenticate with PingID

  Securely authenticate with PingID.

- Verify your identity

  Verify your identity with PingID

- Manage and share Creds

  Pair, receive, and share your digital credentials (Creds)

- Understand PingID

  Understand PingID basics and pairing a device

- Manage your devices

  Add and change devices and manage your settings

Getting started

Introducing PingID

PingID multi-factor authentication (MFA) is a strong authentication solution that allows you to authenticate to your app, application portal, or desktop machine using additional authentication methods, such as your mobile device, to enhance security and provide ease of access to your apps.

Use PingID to pair your account details with a device, such as PingID mobile app, a mobile device with biometrics, a security key, an email address, or a hard token, so you can securely authenticate to access your account, app, or device. For more information, see also What is pairing?

If you pair your account with PingID mobile app, you can also verify your identity using the app. See Verify your identity with PingID.

When you sign on to your account, PingID sends an authentication notification to your device. Authenticate on your device when prompted or enter the OTP into your web browser.

PingID can authenticate your access using the following methods:

- PingID mobile app on your iOS or Android device: Authenticate using the PingID mobile app with swipe, biometrics authentication, Apple Watch, or an OTP generated by the app.
- PingID Desktop app: Open the app on your Windows PC or Mac and generate an OTP.
- Windows Hello: If your Windows Hello device supports FIDO2 biometrics, use it to access your account or apps through a web browser using PingID authentication.
- Apple Mac Touch ID: If your Apple Mac machine supports FIDO2 platform biometrics, use it to access your account or apps through a web browser using PingID authentication.
- iOS biometrics: If your iPhone or iPad supports FIDO2 biometrics, use Touch ID or Face ID to access your account or apps through a web browser using PingID authentication.
- Android biometrics: If your Android device supports FIDO2 biometrics, use it to access your account or apps through a web browser using PingID authentication.
- Security key: Use your FIDO2-compliant security key to authenticate using PingID mobile app.
- Authenticator app: Generate an OTP using an authenticator app, such as Google Authenticator.
- YubiKey: Connect your YubiKey to your Windows PC or Mac and then tap to generate an OTP.
- SMS or voice: Receive an OTP by SMS or voice call.
- Email: Receive an OTP by email.
- Hardware token: Generate an OTP using your hardware token

PingID can be used to securely access the following resources:

- Web: Access your account or app using a web browser.
- VPN: Access your company's VPN.
- Windows login: Access your Windows login machine.
- Mac login: Access your Mac machine.

> **Note**
>
> The authentication methods available to you, as well as the types of resources you can access are defined by your organization's policy.

The 'what and why' of pairing your device with PingID

Set up your device for secure authentication with PingID by pairing it with your account, and learn what to do if your device is lost, stolen, or you want to change the device you are using to authenticate.

PingID supports the use of many different authentication device types. When you have selected the device and method you want, pair it to your account, so you can use it to authenticate with PingID.

What is pairing and why do I need to do it?

PingID lets you register, or 'set up' a device or authentication method by pairing it with your account, so you can sign on to your company services and applications with the added security of multi-factor authentication (MFA). Pairing creates a trust between the authentication method you want to use and your account, so you can use that authentication method to authenticate during the sign on process. Depending on your organization's configuration, you can pair several devices to use for secure authentication with PingID. However you must pair or connect each device or authentication method separately in order to be able to use it authenticate with PingID.

The pairing process varies depending on the type of device you want to use. For example, when pairing the PingID mobile app, your company will give you a QR code or pairing key that you can scan or enter into the PingID mobile app to complete the pairing process. If you're pairing a device that uses biometrics, you might be asked to scan your face or fingerprint.

There are many devices that you can pair, and the options available will vary according to the resources you want to access, and the options your company allows. See Pairing a device with PingID for a full list of devices that can be paired with PingID and instructions of how to do so.

After your device is paired, you can use it to authenticate to any service that your company protects using PingID and access your resources securely. See Authenticating securely with PingID for instructions about how to authenticate with a device Authenticating securely with PingID.

1. The PingID mobile app receives the notification sent by the mobile notification server.
2. The PingID mobile app sends the PingID server a test request in order to test the established trust components, enabling a security handshake between the app and the server. If all trust components are valid and the device meets the organization's requirements, the server updates the user's profile.
3. The PingID server finalizes the pairing process with a success server response message that the device is paired. The PingID mobile app then shows the one-time passcode (OTP) screen to the user.
4. The PingID server triggers a first authentication request that is sent to the user's mobile device as part of the authentication flow.

Which devices or authentication methods can I pair with PingID?

You can pair various devices, such as the PingID mobile app, an authenticator app like Google Authenticator, or a security key, with PingID.

You can see a list of authentication methods that can be paired with PingID here.

The authentication methods available to you are defined by your company, so some of the methods listed might not be available to you. If you want to know the full list available for your organization, contact your organization's help desk.

Pairing a device - when I already have a device paired with PingID

If you have more than one device paired with PingID, and your organization allows it, you can pair additional devices from your Devices page. For information, see I want to pair an additional device or add an authentication method.

You might also be able to pair a device in the following situations, without needing to contact your help desk:

- My device was lost or stolen
- I forgot my device or left it at home
- I want to transfer the PingID mobile app from my old mobile to a new device

I want to pair a device or authentication method for the first time

Your company decides which devices you can pair with your account, and which resources you can access. Select the device you want to pair, and then select the tab with instructions that fit the resource you want to access (accessing an account or app through a web browser, your VPN, your Windows machine, or your Mac machine).

For a list of devices and how to pair them see Pairing a device with PingID.

> **Note**
>
> The authentication methods available to you as well as the types of resources you can access are defined by your organization's policy. For more information, contact your organization's administrator.

PingID authentication for the web

There are many authentication methods that your company can enable to allow you to securely authenticate with PingID.

To access your account or app using a web browser, you can authenticate using the following authentication methods:

- PingID mobile app: Authenticate using the PingID app on your Android or iOS mobile device with swipe, biometrics authentication, Apple Watch, or a one-time passcode (OTP). PingID mobile app can also be used to authenticate manually when offline.
- Desktop app: If you pair desktop app through the web, you can use it to generate a one-time passcode (OTP) to authenticate securely to access your account or app.
- Authenticator app: Generate a one-time passcode using an authenticator app, such as Google Authenticator.
- Windows Hello: If your Windows Hello device supports FIDO2 biometrics, use it to access your account and/or apps via a web browser, using PingID authentication.
- Apple Mac Touch ID: If your Mac machine supports FIDO2 platform biometrics, use it to access your account or apps through a web browser using PingID authentication.
- iOS or iPadOS biometrics: If your iOS device supports FIDO2 biometrics, use Face ID or Touch ID to access your account and/or apps via a web browser, using PingID authentication.

- Android biometrics: If your Android device supports FIDO2 biometrics, you can use it to access your account and/or apps via a web browser, using PingID authentication.
- Security key: Connect your security key to your machine and then tap to authenticate. You can also use your security key to authenticate manually when offline.
- Authenticator app: Generate a one-time passcode using an authenticator app, such as Google Authenticator.
- YubiKey: Connect your YubiKey to your machine and then tap to generate a one-time passcode.
- SMS or voice: You receive a one-time passcode (OTP) by SMS or by voice call.
- Email: You receive an OTP by email.
- Hardware token: You are asked for an OTP, which you copy from your hardware token.

To benefit from secure, multi-factor authentication using PingID, first you must pair or connect your device with your account.

PingID authentication for Windows login

Pair your device with PingID, using one of the supported devices, and then you can use PingID to authenticate to your Windows machine.

Authentication varies depending on your organization's configuration. There are two main flows:

- Passwordless authentication: Authenticate with PingID only, without entering a password.

> **Note**
>
> Windows login passwordless authentication is currently supported when using PingID mobile app, that has already been paired with your account.

- Second factor authentication: Enter your username and password and then authenticate using PingID.

You can benefit from secure authentication with PingID whether you are signing on to Windows locally, or remotely with Remote Desktop Protocol (RDP).

You can authenticate using:

- PingID mobile app: Authenticate using the PingID app on your Android or iOS mobile device with swipe, biometrics authentication, Apple Watch, or a one-time passcode (OTP). PingID mobile app can also be used to authenticate manually when offline.
- Security key: Connect your security key to your machine and then tap to authenticate. You can also use your security key to authenticate manually when offline.
- YubiKey: Connect your YubiKey to your machine and then tap to generate a one-time passcode.
- SMS or voice: You receive a one-time passcode (OTP) by SMS or by voice call.
- Email: You receive an OTP by email.
- Hardware token: You are asked for an OTP, which you copy from your hardware token.

To benefit from secure, multi-factor authentication using PingID, first you must pair or connect your device with your account.

PingID authentication for VPN

There are many authentication methods that your company can enable to allow you to securely authenticate with PingID as a second factor of authentication when accessing your VPN or any remote access clients that support the RADIUS protocol.

To access a VPN, you can authenticate using:

- PingID mobile app: Authenticate using the PingID app on your Android or iOS mobile device with swipe, biometrics authentication, Apple Watch, or a one-time passcode (OTP). PingID mobile app can also be used to authenticate manually when offline.
- Desktop app: If you pair desktop app through the web, you can use it to generate a one-time passcode (OTP) to authenticate securely to access your VPN.
- Authenticator app: Generate a one-time passcode using an authenticator app, such as Google Authenticator.
- YubiKey: Connect your YubiKey to your machine and then tap to generate a one-time passcode.
- SMS or voice: You receive a one-time passcode (OTP) by SMS or by voice call.

- Email: You receive an OTP by email.
- Hardware token: You are asked for an OTP, which you copy from your hardware token.

To benefit from secure, multi-factor authentication using PingID, first you must pair or connect your device with your account.

PingID authentication for Mac login

You can use PingID to authenticate with your Mac.

PingID can be used as a second factor of authentication when signing on to your Apple Mac machine.

When you sign on to your Mac laptop or desktop machine, you'll be asked to authenticate.

You can authenticate using:

- Your iOS or Android device: Authenticate using the PingID app on your mobile device with swipe, fingerprint authentication, Apple Watch, or a one-time passcode. You can also use the PingID mobile app to authenticate manually when offline.
- Authenticator app: Generate a one-time passcode using an authenticator app, such as Google Authenticator.
- YubiKey: Connect your YubiKey to your machine and then tap to generate a one-time passcode.
- SMS or voice: You'll be sent a one-time passcode (OTP) by SMS or by voice call.
- Email: You'll be sent a one-time passcode by email.
- Hardware token: You are asked for a one-time passcode, which you copy from your hardware token.

> **Note**
>
> To benefit from secure, multi-factor authentication using PingID, first you need to pair (connect) your device with your account.

Pairing a device with PingID

Which device do you want to pair with PingID?

Pair › Authenticate › You're in!

I forgot my device | My device was stolen

- PingID mobile app
- Apple Mac Touch ID
- Security Key
- PingID desktop
- Windows Hello
- YubiKey
- Authenticator app
- Android Biometrics
- Email
- SMS or Voice call
- iOS and iPad OS
- Hardware token

- Verifying your identity
- What is pairing?
- Managing your devices

Using PingID mobile app authentication

PingID allows you to download an app to your mobile device and use it to sign on to your company services and applications with the added security of multi-factor authentication (MFA).

To set up PingID mobile app authentication, first install PingID mobile app on your device, and then register or "pair" it with your account. Pairing creates a trust between the app and your account so that you can use the app to authenticate. After you've paired your device, each time that you sign on to your account you'll receive a push notification to your mobile device asking you to authenticate using an approval request, biometrics, number matching, or a one-time passcode (OTP). The method you use depends on your company and device configuration.

> **Note**
>
> If you are running an older version of the mobile app (1.x), go to the legacy documentation for information.

- Pair PingID mobile app

  Register your device for secure authentication with PingID mobile app.

- What is PingID mobile app?

  An introduction to PingID mobile app and how it works.

- Manage your devices

  Add and change devices and manage your settings.

- Legacy documentation

  View documentation for previous versions of PingID mobile app.

Pairing PingID mobile app (using a QR code or pairing key)

To start using PingID mobile app for secure authentication, identity verification, or sharing your digital credentials (Creds), you'll need to install PingID mobile app on your mobile device, and then register or "pair" it with your account.

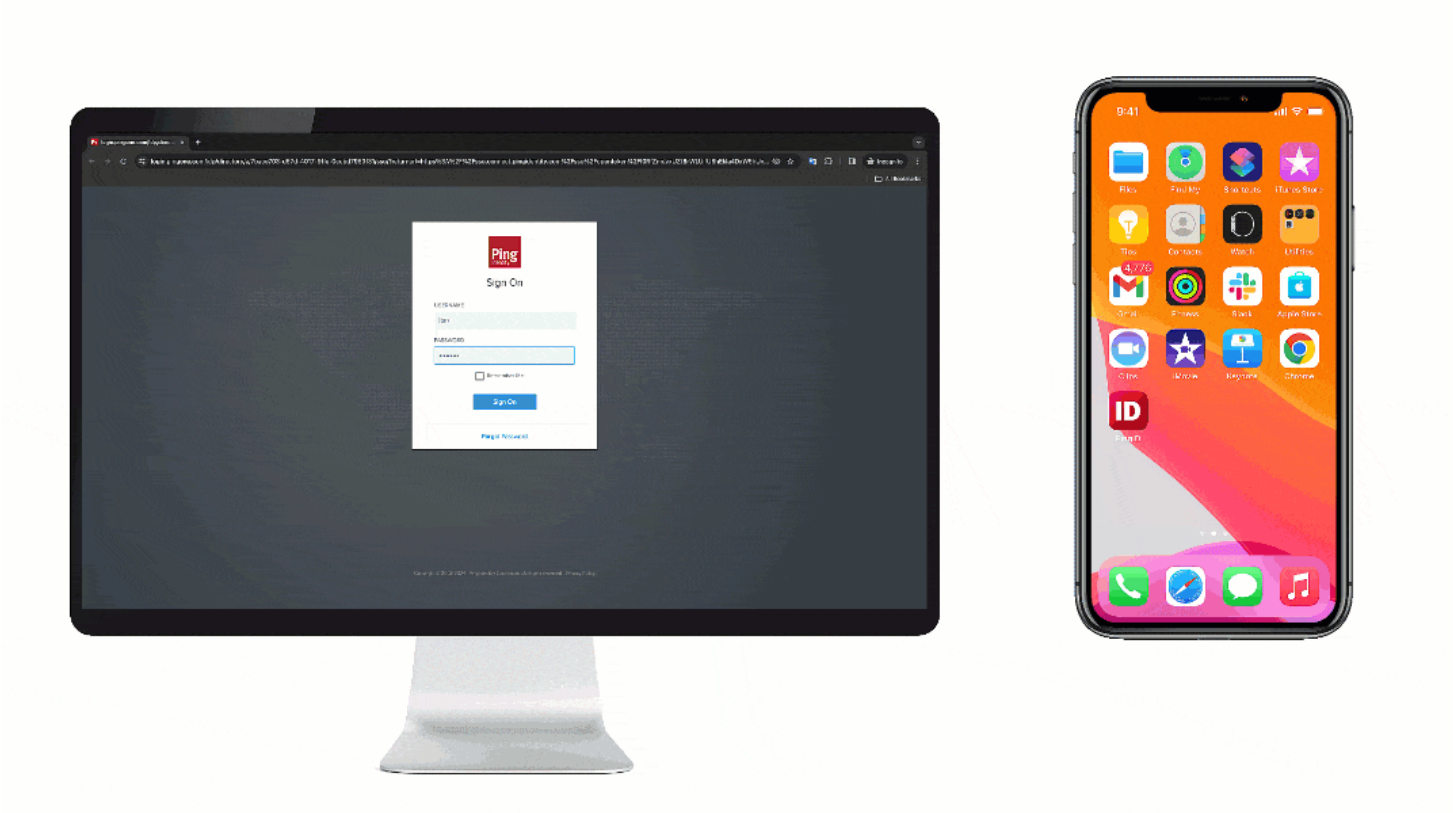
Before you begin

1. Install PingID mobile app on your device from the relevant app store:
   - iOS
   - Android

   You can also download the app from the PingID downloads page.
2. Get your QR code and display it on a different device. You might see it on your screen when you sign on to your account or app, or your organization might send it to you by email. You'll need to display it on your computer screen so that you can scan it using your mobile device during the pairing process.
3. If your organization requires it, you'll need to set up biometrics (such as fingerprint or face recognition) on your mobile device.

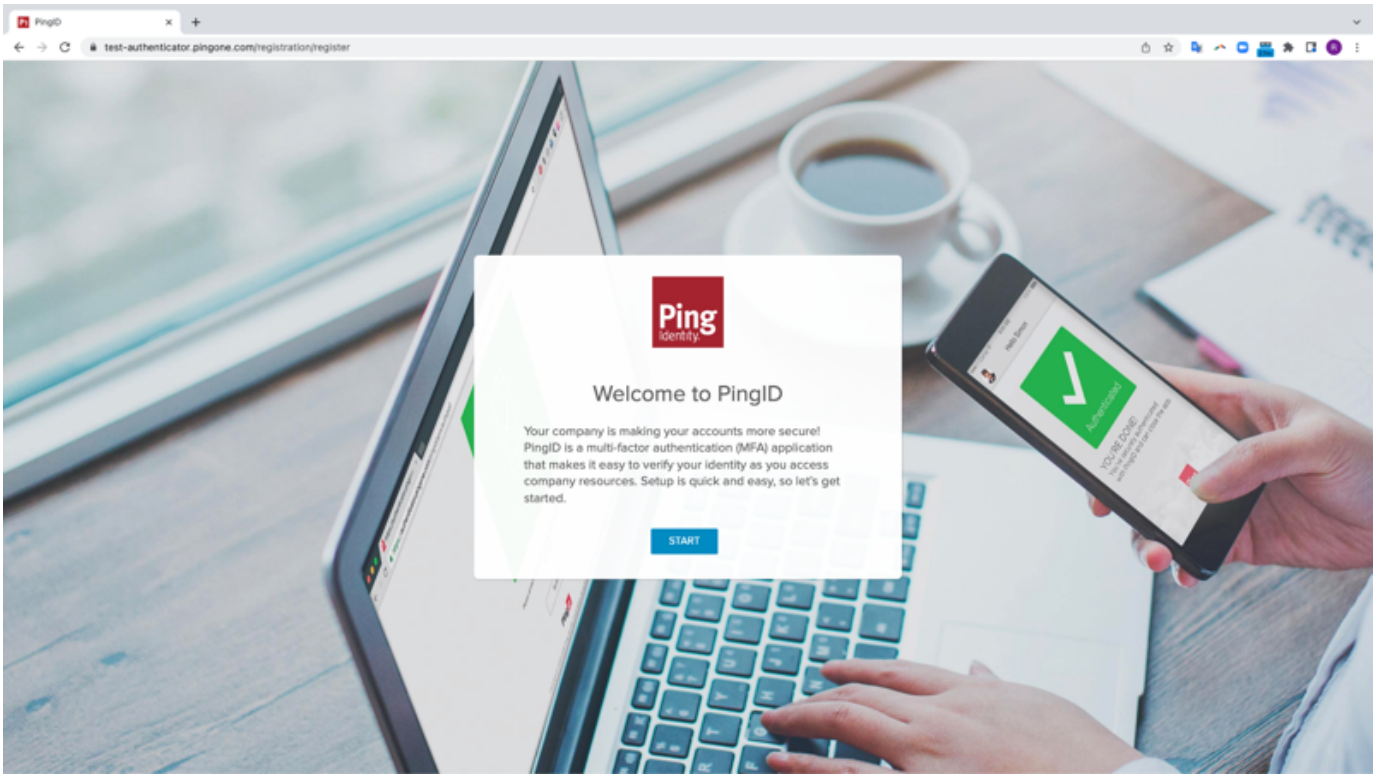
About this task

> **Note**
>
> After you've paired your device and authenticated successfully, you can also use it to authenticate for Windows login, or Mac login, if required.



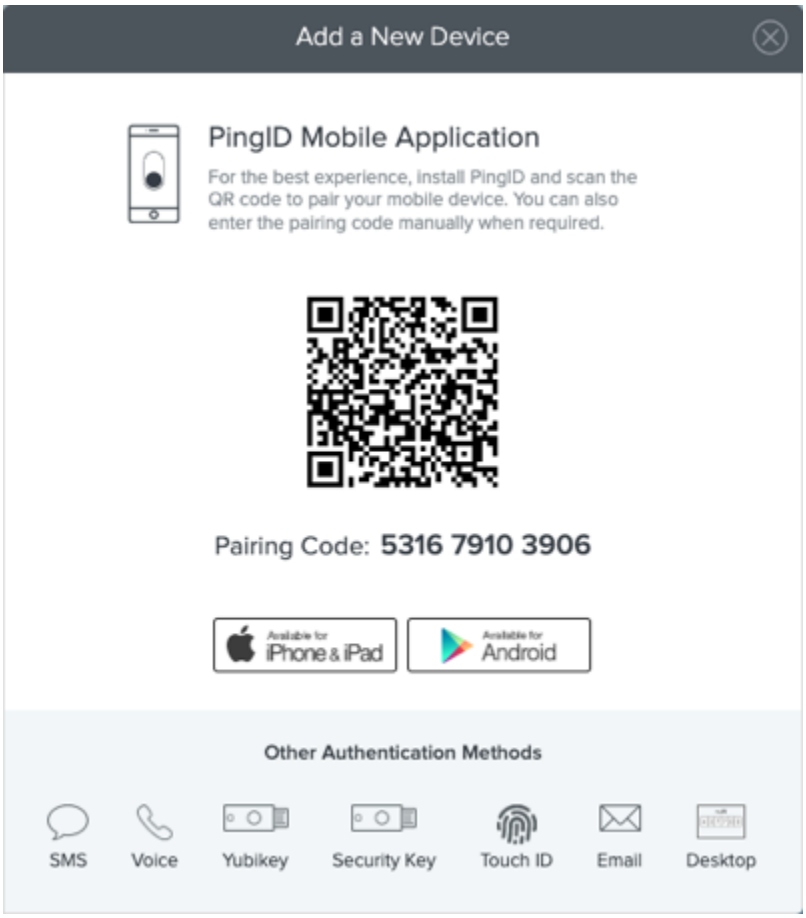
Steps

1. Sign on to your account or app, and when you see the registration window click **Start**.



Result:

You'll see the **Add a New Device** window showing the QR code.

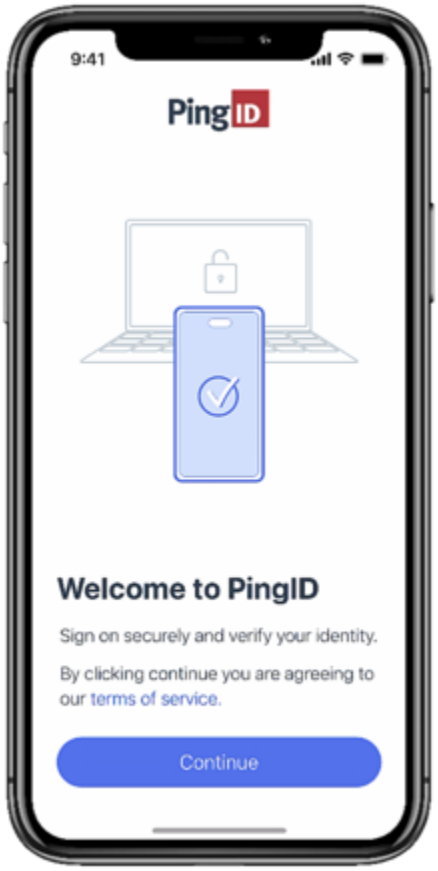


> **Note**
>
> Your organization should provide you with a QR code. You might see it on your screen when you sign on to your account or app, or your company might send it to you by email.
> Before moving to the next step, make sure you have the QR code clearly visible on a *different device* from the one you are using to pair PingID mobile app (for example, on your laptop).

2. Open the PingID mobile app.

   Result:

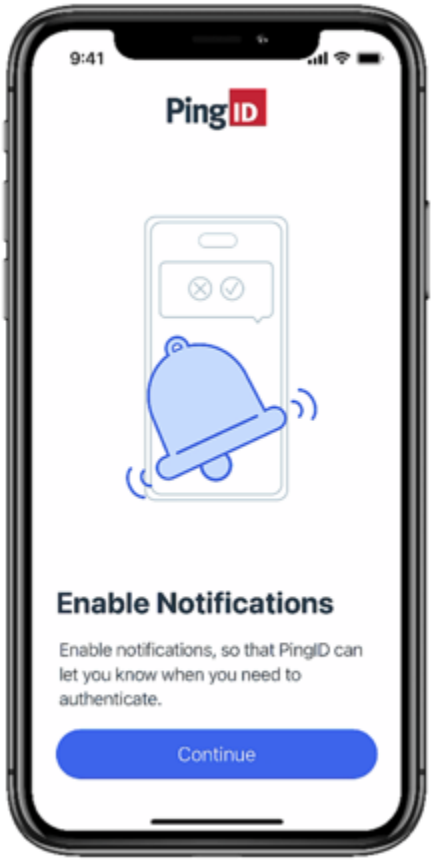
   You'll see the welcome screen with a link to the terms of service.



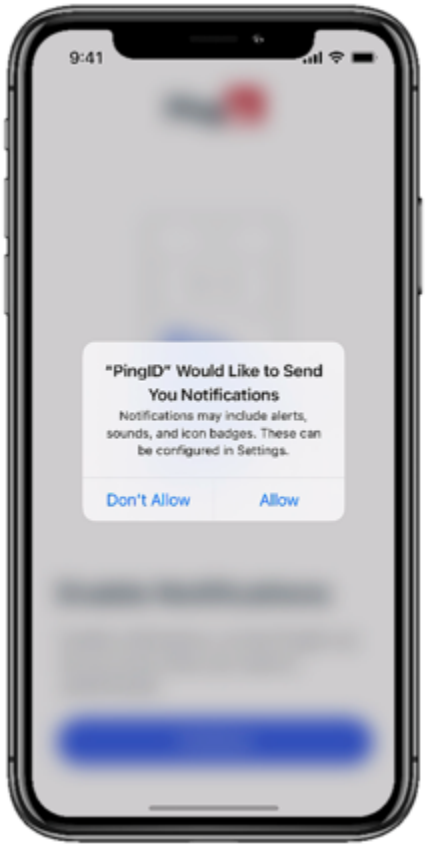
3. Review the terms of service and tap **Continue**.

   Result:

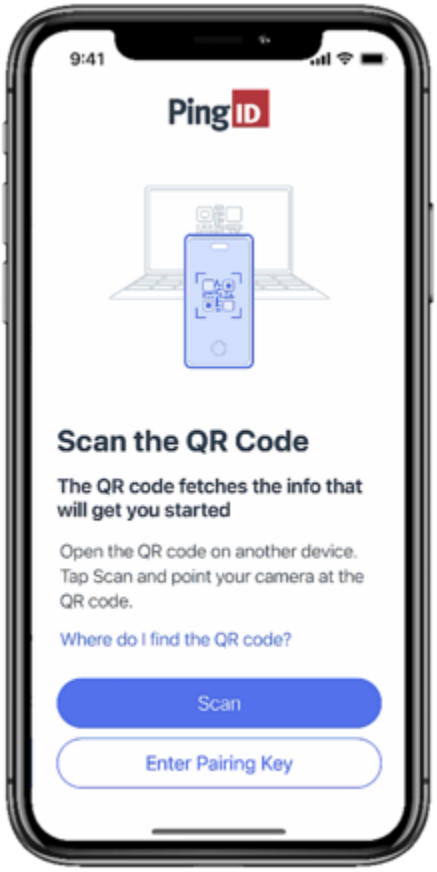
   You'll be asked to enable notifications on your mobile device. PingID sends notifications to your device to let you know when you need to authenticate, verify your identity, or receive or share Creds.



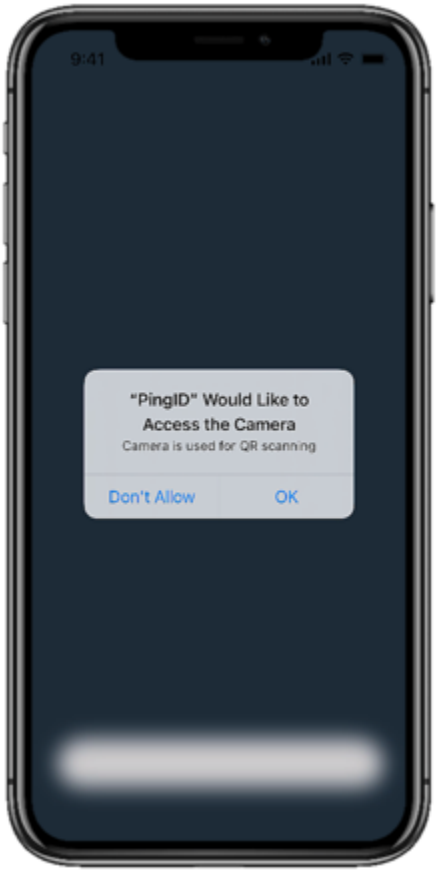
4. Tap **Continue** to enable notifications, and then on the confirmation popup, tap **Allow**.



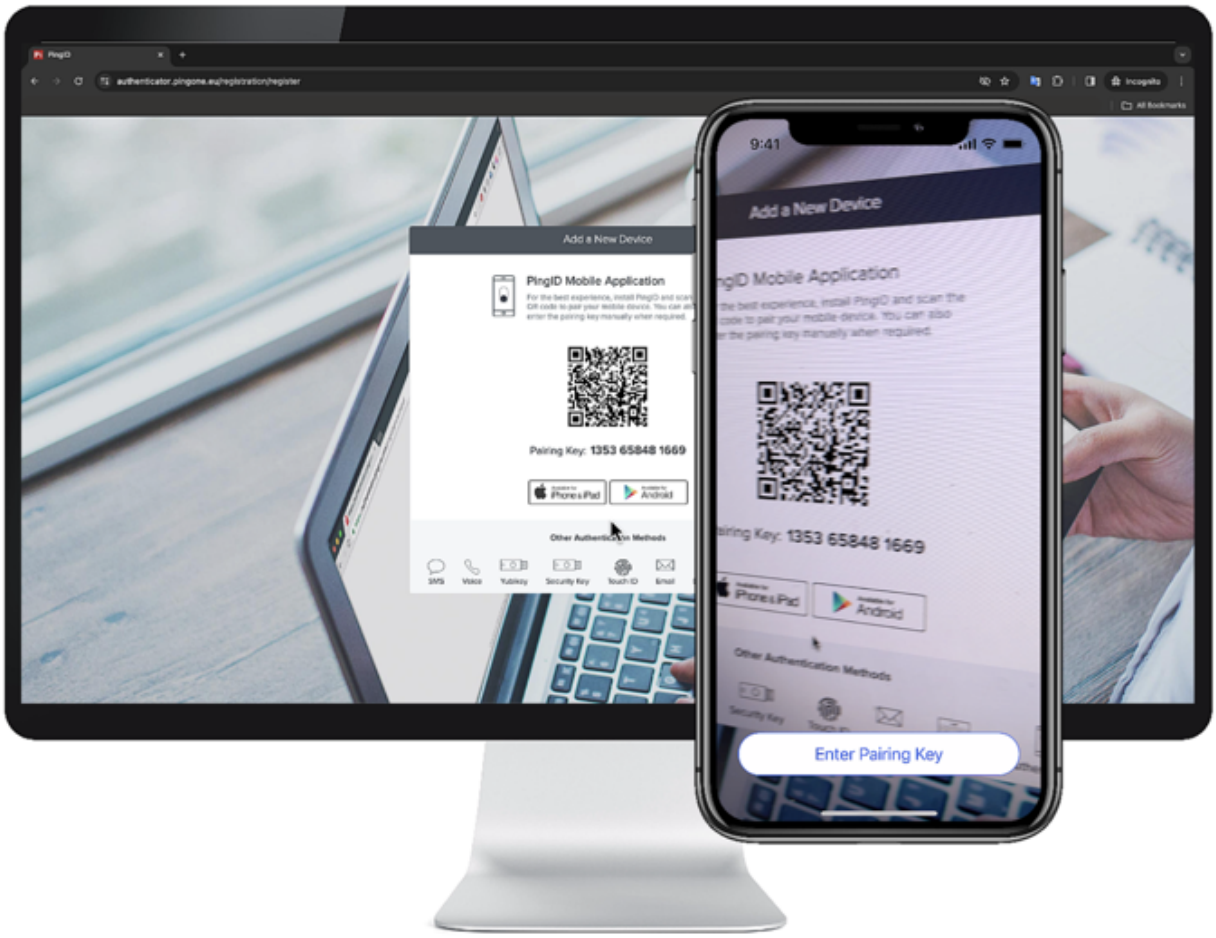
5. Make sure that the QR code provided by your company is displayed on a different device, tap **Scan**, and then scan the QR code with your mobile device.



6. You'll be asked to allow PingID to access your camera.

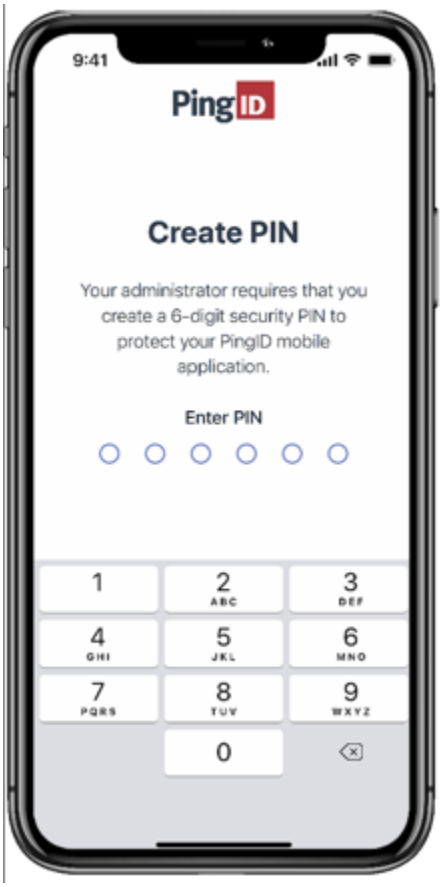


7. Tap **OK**, and then point your camera at the QR code.



> **Tip**
>
> If you can't scan the QR code, on your mobile device, tap **Enter Pairing Key** and enter the pairingkey (long numerical code) that is displayed below the QR code.

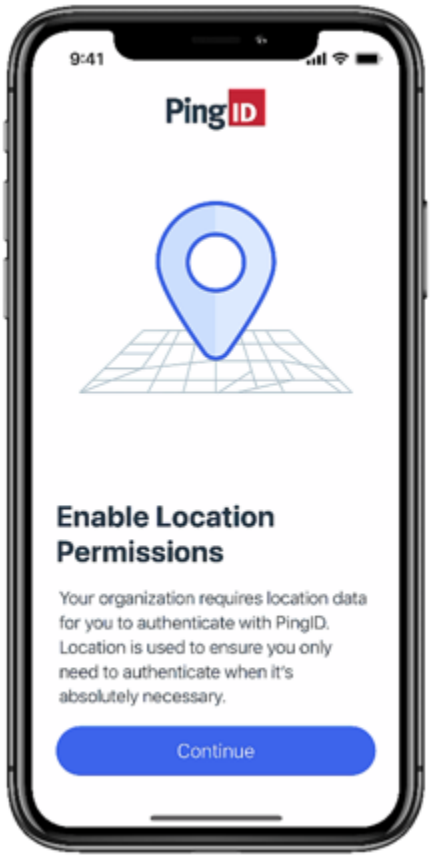
8. If your admin requires you to add a PIN code, you'll be asked to create your own unique 4 or 6-digit PIN.



Note

- If you are required to create a PIN code, you'll need to enter it every time you authenticate with PingID mobile app.
- Your PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively, and you can't choose digits that are in ascending or descending sequence, such as 1234.

9. If your company security policy requires them to know your device location, you'll be asked to allow PingID mobile app to access your location. Tap **Continue**, and then select the relevant location permissions.

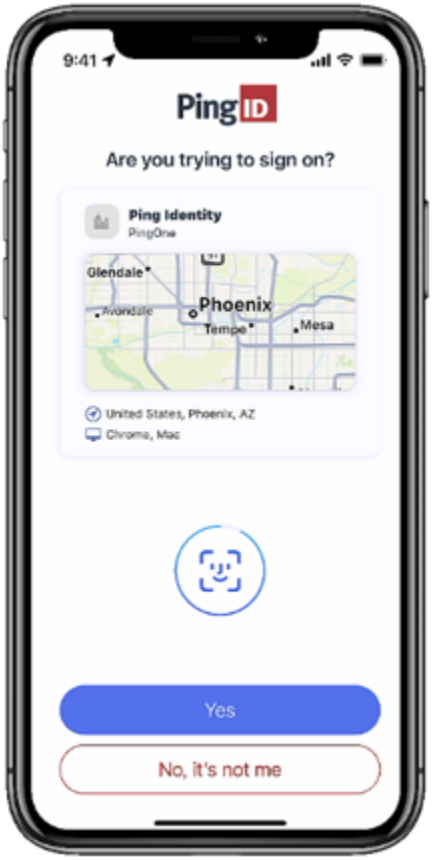


> **Note**
>
> Location options might differ slightly depending on the mobile device you are using. Because your company's security policy might require you to allow access to your device location even when PingID mobile app is closed, it is recommended that you choose the most permissive options:
>
> - Android users: Select **Precise** and **When using the app**.
> - iOS users: Select **Always Allow**.

Result:

You'll see the PingID mobile app screen showing the one-time passcode (OTP) number, and an authentication request is generated immediately. You'll see a message asking if you are trying to sign on.

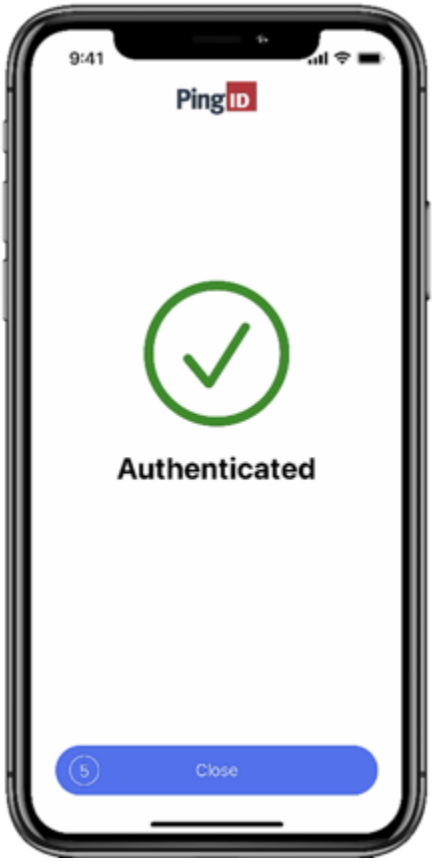
10. When prompted, tap **Yes** to approve the authentication or authenticate using biometrics. You have a limited amount of time to approve the request.



> **Note**
>
> If you are authenticating with biometrics, you might be asked to confirm you allow PingID to scan your biometrics. For more details about authentication methods and how to authenticate, see Authenticating using PingID mobile app.

Result:

You'll see a green check mark confirming authentication is successful and you are granted access to the service or app that you wanted to access.



The next time you sign on to your account or application, you'll be able to use PingID mobile app to authenticate or to verify you identity. Learn more in:

- Authenticating using PingID mobile app
- Verify your identity with PingID
- Pairing and sharing your Creds

Related links

- Troubleshooting PingID authentication

What is PingID mobile app and how does it work?

PingID allows you to download an app to your mobile device and use it to sign on to your company services and applications with the added security of multi-factor authentication (MFA). You can also use it to verify your identity to your employer.

To set up PingID mobile app authentication, first download PingID mobile app to your device, and then register or "pair" it with your account. Pairing creates a trust between the app and your account so you can use the app to authenticate.

After you've paired your device, each time that you sign on to your account you'll receive a push notification to your mobile device asking you to authenticate using an approval request, biometrics, number matching, or a one-time passcode (OTP). The method you use depends on your company and device configuration. You'll also be able to respond to a request to verify your identity (learn more in Verify your identity with PingID).

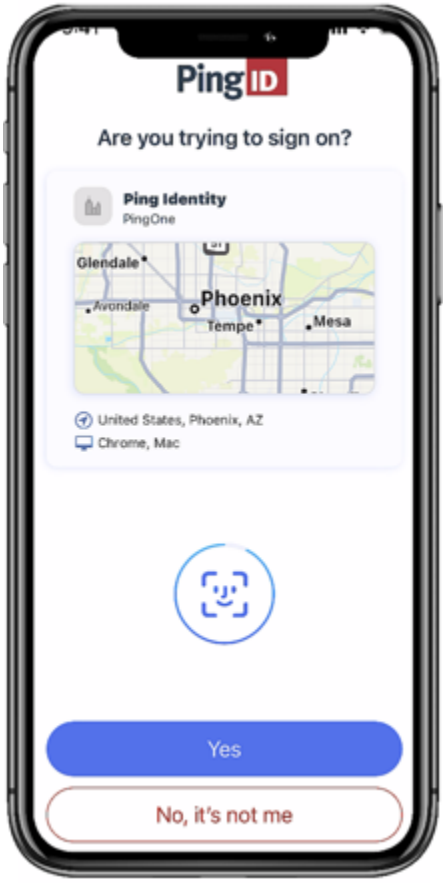
For details of how to pair PingID mobile app, see Pairing PingID mobile app (using a QR code or pairing key).

You can use PingID mobile app to access your account from a web browser, your company VPN, or to access your Windows login or Mac login machine. For details of how to authenticate with PingID mobile app, see Authenticating using PingID mobile app.

Note

The PingID mobile app using biometrics (fingerprint, face, or iris authentication) and iOS or Android biometrics authentication are different methods of authentication:

- PingID mobile app using biometrics: Allows you to authenticate when accessing your account from various different devices. Requires you to define biometrics on your mobile device face or fingerprints), install PingID mobile app on your mobile device, and pair PingID mobile app with your account.
- iOS or Android biometrics: Allows you to authenticate using your mobile device's built-in biometrics (face or fingerprint) when signing on to your account using a web browser. It doesn't require PingID mobile app, however, you can only sign on to your account from the same device with which you want to authenticate. Biometrics authentication is available when using supported Windows Hello, Mac Touch ID, iOS or iPadOS, and Android devices.

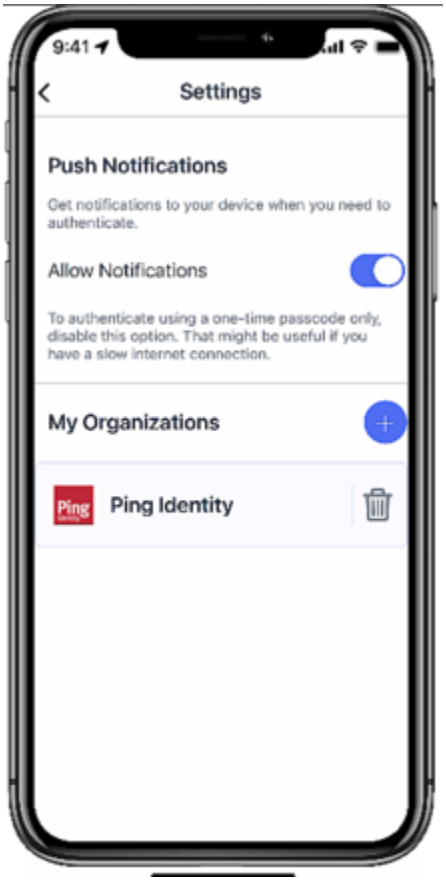


You do not need to launch the PingID mobile app each time you want to authenticate. As long as it is running in the background, a push notification automatically appears on your screen or lock screen prompting you to authenticate.

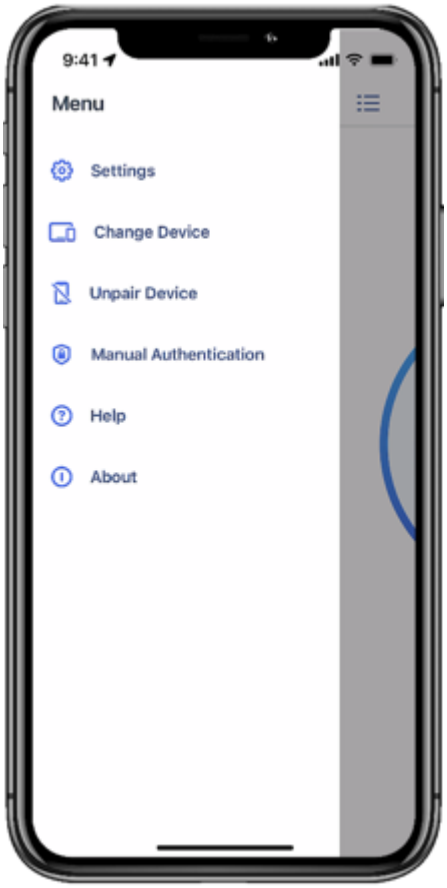
What else can I do with PingID app?

Open the PingID mobile app to access additional options:

- Change your device: To move PingID authentication to a new device.
- Add an organization: If you want to use the PingID mobile app to authenticate against accounts in more than one organization.



- Change your mobile app PIN
- Report fraud
- Disable push notifications
- Get an OTP that you can use to authenticate. This is useful when your mobile device is offline and you do not have data or Wi-Fi access. (If you're offline, your mobile device will not receive the push notifications that tell you that you need to authenticate with PingID.)
- Send event logs: Send a log of your activity to customer support for help when troubleshooting issues.



Learn more in PingID mobile app management.

Using PingID mobile app authentication (legacy)

PingID allows you to use your mobile device to sign on to your company services and applications with the added security of multi-factor authentication (MFA).

> **Note**
>
> This is legacy documentation. If you are running PingID mobile app 2.0 or later, see Using PingID mobile app authentication.

The PingID mobile app enables you to authenticate from your mobile device in a variety of ways, including swipe, biometrics, number matching, or a one-time passcode (OTP) depending on your company and device configuration. You might also be able to authenticate manually when offline. Use the PingID mobile app to authenticate when accessing your account or app from any device.

Depending on your organization's configuration, you can use PingID mobile app to access your account or app using a Web browser, your company's VPN, a Windows login machine, or a Mac machine.

To get started, you'll need to download the app to your mobile device, and pair (connect) your device with your account. After you've paired your device, each time you sign on to your account, you will receive a push notification to your mobile device asking you to authenticate.

For more general information about PingID mobile app, see What is PingID mobile app and how does it work?.

If you have a new mobile device and want to transfer PingID mobile app from your old device to your new device, see Transfer PingID mobile app authentication to a different device.

Select the instructions relevant to the resources you want to access.

Web

UsePingID mobile app to access your account or app using a web browser.

iOS

- Set up your iPhone for PingID authentication
- Authenticate using your iPhone
- Authenticate manually if you're offline

Android

- Set up your Android for PingID authentication
- Authenticate using your Android
- Authenticate manually if you're offline

VPN

Use PingID mobile app to access your company's VPN.

iOS

- Set up your iPhone for PingID authentication (VPN)
- Authenticate using your iPhone (VPN)
- Authenticate manually if you're offline (VPN)

Android

- Set up your Android for PingID authentication (VPN)
- Authenticate using your Android (VPN)
- Authenticate manually if you're offline (VPN)

Windows login

Use PingID mobile app to access your Windows login machine. Register using a web browser, and then authenticate when signing on to your Windows login machine either locally or using a remote desktop machine (RDP).

iOS

- Set up your iPhone for PingID authentication (Web)
- Authenticate using your iPhone (Windows login)
- Authenticate manually if you're offline

Android

- Set up your Android for PingID authentication (Web)
- Authenticate using your Android
- Authenticate manually if you're offline

Use PingID mobile app to access a remote desktop machine through the Windows RDP client

Mac login

Use PingID mobile app to access your Mac machine.

iOS

- Set up your iPhone for PingID authentication (Web)
- Authenticate using your iPhone (Mac login)
- Authenticate manually if you're offline (Mac login)

Android

- Set up your Android for PingID authentication (Web)
- Authenticate using your Android (Mac login)
- Authenticate manually if you're offline (Mac login)

Managing your devices and getting help

- Authenticate using a backup device
- Manage your devices
- Manage PingID mobile app
- Transfer PingID mobile app authentication to a different device
- Troubleshoot PingID authentication

(legacy) Pairing PingID mobile app for Android (using a QR code or pairing code)

To set up PingID mobile app for secure authentication, you need to download the app to your Android device, and then register or 'pair' PingID mobile app with your account.

Before you begin

If you want to use your Android device biometrics to authenticate with PingID mobile app or your organization requires it, you must first configure biometrics, such as fingerprint, face, or iris, on your device.

> **Note**
>
> Not all Android devices support all types of Biometric authentication with PingID. Fingerprint authentication is supported on all devices from Android 6.x and later. For more information, see Troubleshooting PingID authentication.

About this task

Setting up PingID to authenticate using your mobile device typically involves the following steps:

- Download PingID from your app store, or through the email link you receive from your organization.
- Pair your device. Pairing a device creates a trust between your device and your account.

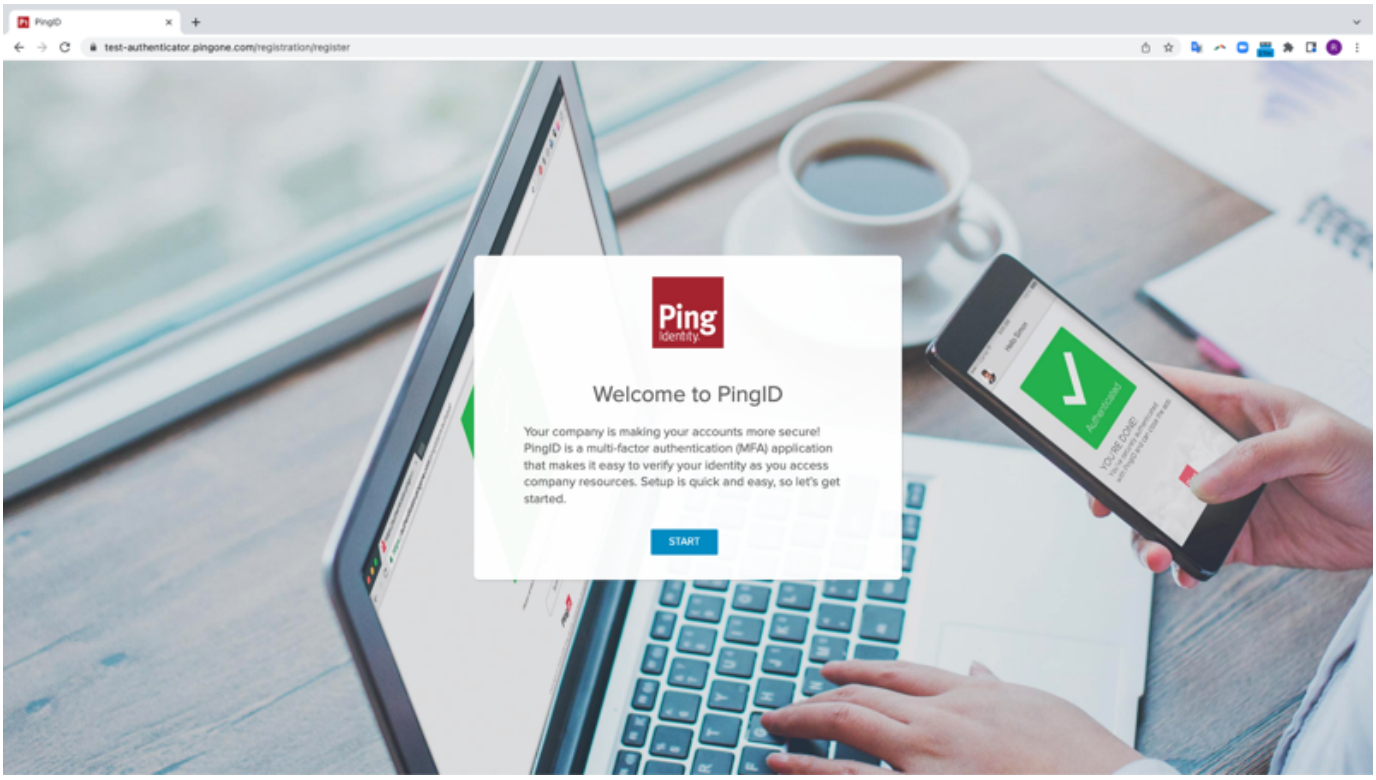
> **Note**
>
> After you have paired your device and authenticated successfully, you can also use it to authenticate for Windows login, or Mac login, if required.

{{{ Video removed }}}

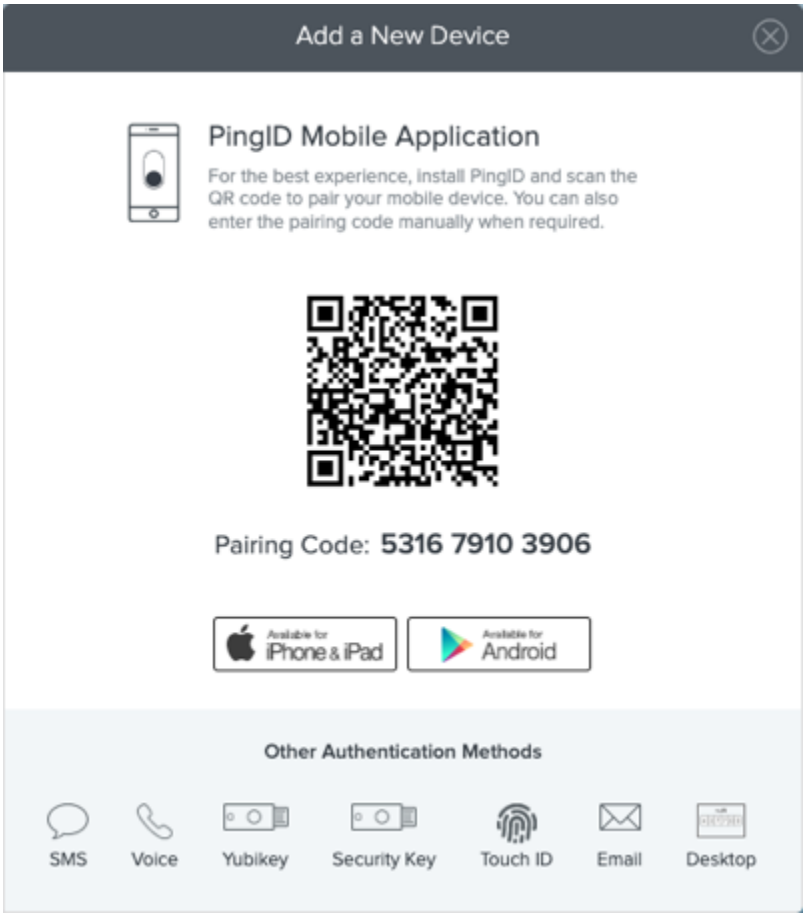
> **Note**
>
> Setting up PingID might vary slightly depending on the device model you are using. Also, the windows you see might vary from the ones shown below.

Steps

1. Sign on to your account or app and when you see the registration window and click **Start**.



You'll see the **Add a New Device** window, showing the QR code.



2. Download and install the PingID app using one of the following options:

   Choose from:

   - **From Google Play App Store**: On your mobile device, open Google Play Apps Store, and tap **Install**.
   - **Using the Google Play link**: On the PingID registration screen, search for PingID, tap the **Available for Android** button, and from the Google Play store site, install the app remotely on your Google-registered mobile device.

   > **Note**
   >
   > If you have antivirus software installed, you may receive a message that PingID is seeking root access to your device. If so, select **Yes**, or **Trust**.

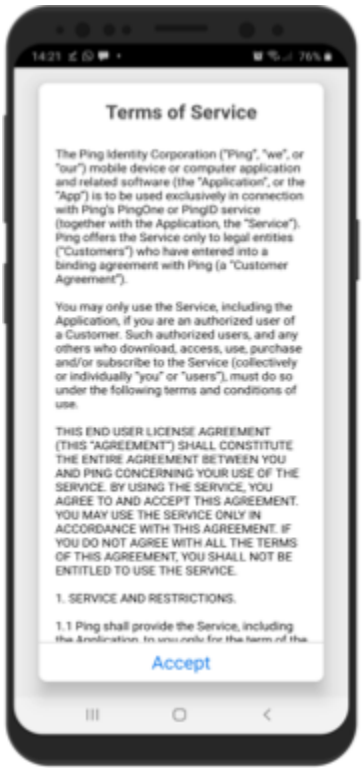
3. Details of your pairing key and QR code are displayed on your web browser. If you are using the Legacy Registration Window, on the PingID registration window, click the **I already installed the PingID app** button (I already installed the PingID app) to view the QR code.

4. After the PingID app is installed, on your mobile device, tap **Open**.

   Result:

   The PingID mobile app opens.

5. The first time you access PingID mobile app, you'll be asked to accept the terms of service. Tap **Accept**.

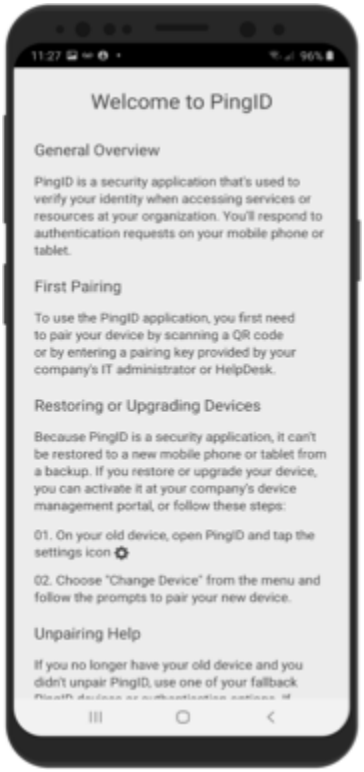


   A message opens telling you to accept all PingID permission requests, including notification requests, and camera permissions when prompted to do so.

6. Tap **I Understand**.

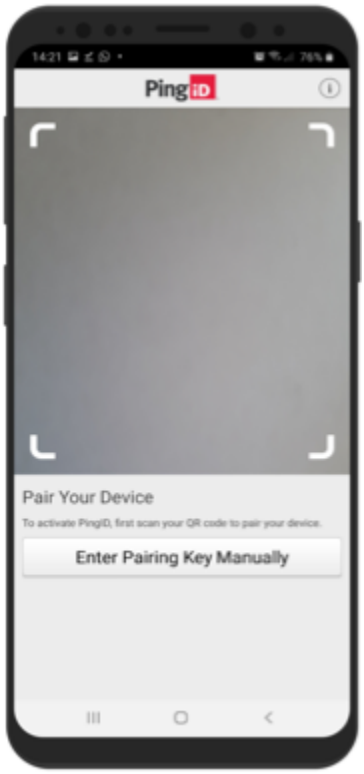
Result:

The **Welcome to PingID** information window opens, giving you an introduction to PingID mobile app and how it works.



7. Tap **Continue**, and then tap **Allow** and **OK** to accept all camera and location permission requests from PingID.

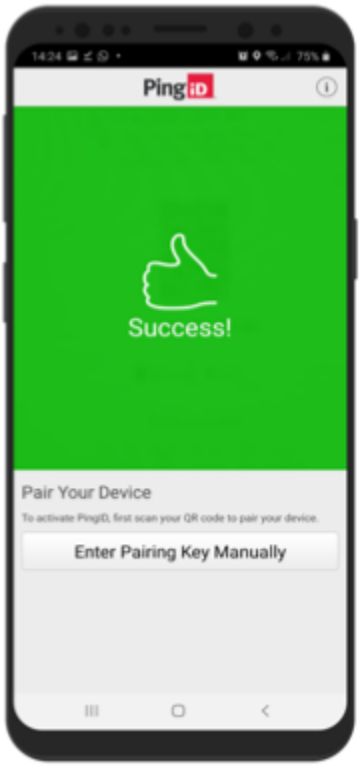
8. From the PingID app on your device, point your device at the QR code on your browser to scan it.



If you are unable to scan the QR code, on your mobile device tap **Enter Pairing Key Manually** and enter the pairing key as shown on the registration page.

Result:

You'll see a green checkmark indicating the pairing request is successful, and the **Complete Your Profile** window opens automatically.



9. If your admin requires you to add a PIN code, you'll be asked to create your own unique 4 or 6 digit PIN.

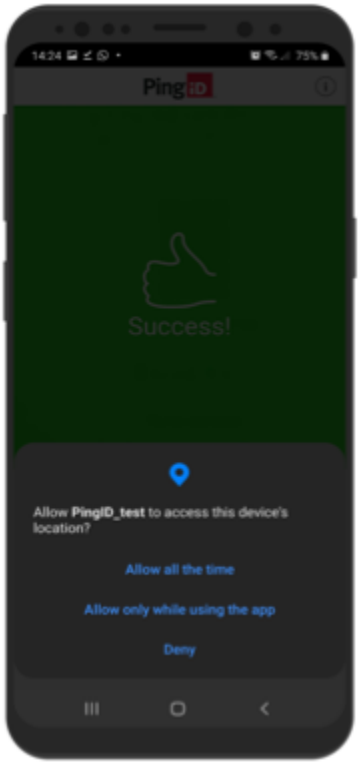
> **Note**
>
> - If you are required to create a PIN code, you'll need to enter it every time you authenticate with PingID mobile app.
> - Your PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively, and you can't choose digits that are in ascending or descending sequence, such as 1234.

10. If you have not already enabled location settings, a popup appears, asking you to allow PingID to use your location. Choose from the following options:

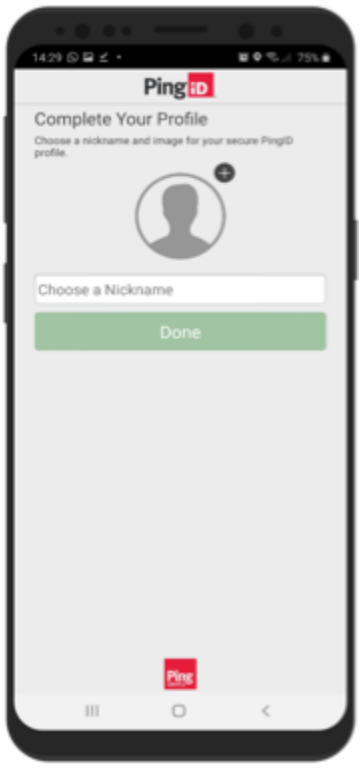
    Choose from:

    - (Recommended) **Allow all the time**: Always allow PingID to access location. Your company's security policy may require you to allow access to location to authenticate, even when PingID mobile app is closed, so this option is recommended.
    - **Allow only while using this app**: Only allow PingID to access your location when using PingID mobile app.
    - **Only this time**: Allow PingID to access your location for this authentication request only.
    - **Deny**: Do not allow PingID mobile app to access your location.

    > **Note**
    >
    > The options and the number of popups that appear may differ slightly depending on the Android version your device is running.

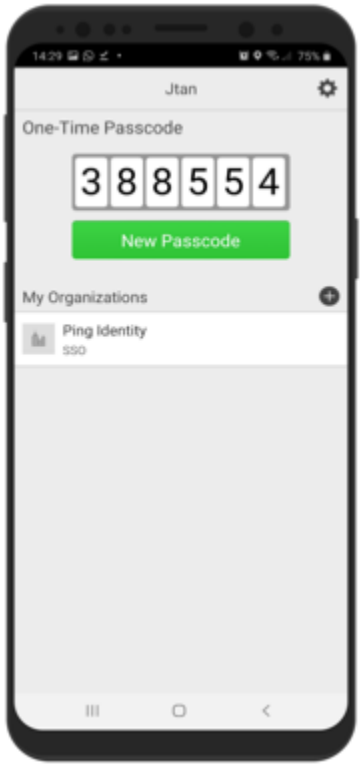


11. Enter a nickname for your profile, optionally add a picture, and then tap **Done**. Your profile picture appears on the authentication screen when you receive a push notification, and indicates that the push notification is authentic.



Result:

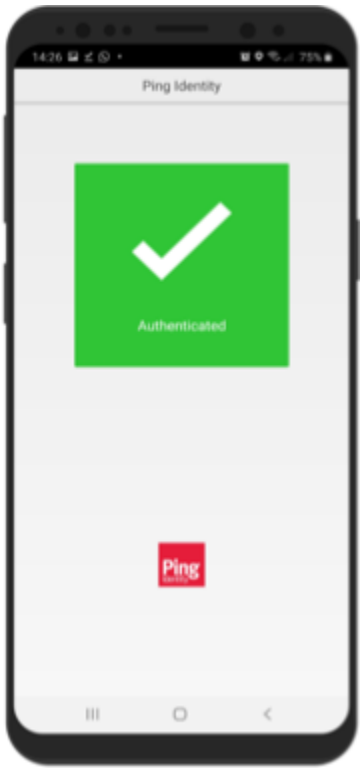
You'll see the PingID mobile app screen showing the one-time passcode number and your organization name in the organization list, and an authentication request is generated immediately.



12. Authenticate using your mobile device.

Result:

After you successfully authenticate, you'll see a green checkmark confirming authentication, and you are redirected to the company protected browser based service or app that you wanted to access.



> **Note**
>
> If you have not already allowed PingID to access location data all the time, you may be prompted to allow location data. Select **Allow all the time**, when prompted.

For information regarding troubleshooting, see Troubleshooting.

Related links

- Using PingID mobile app authentication (legacy)

(legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code)

To set up PingID mobile app for secure authentication, you need to download the app to your iOS device, and then register or 'pair' PingID mobile app with your account.

About this task

Setting up PingID to authenticate using your mobile device typically involves the following steps:

- Download PingID from your app store or with the email link you receive from your organization.
- Pair your device. Pairing a device creates a trust relationship between your device and your account.

> **Note**
>
> After you have paired your device, and authenticated successfully, you can also use it to authenticate for Windows login, or Mac login, if required.

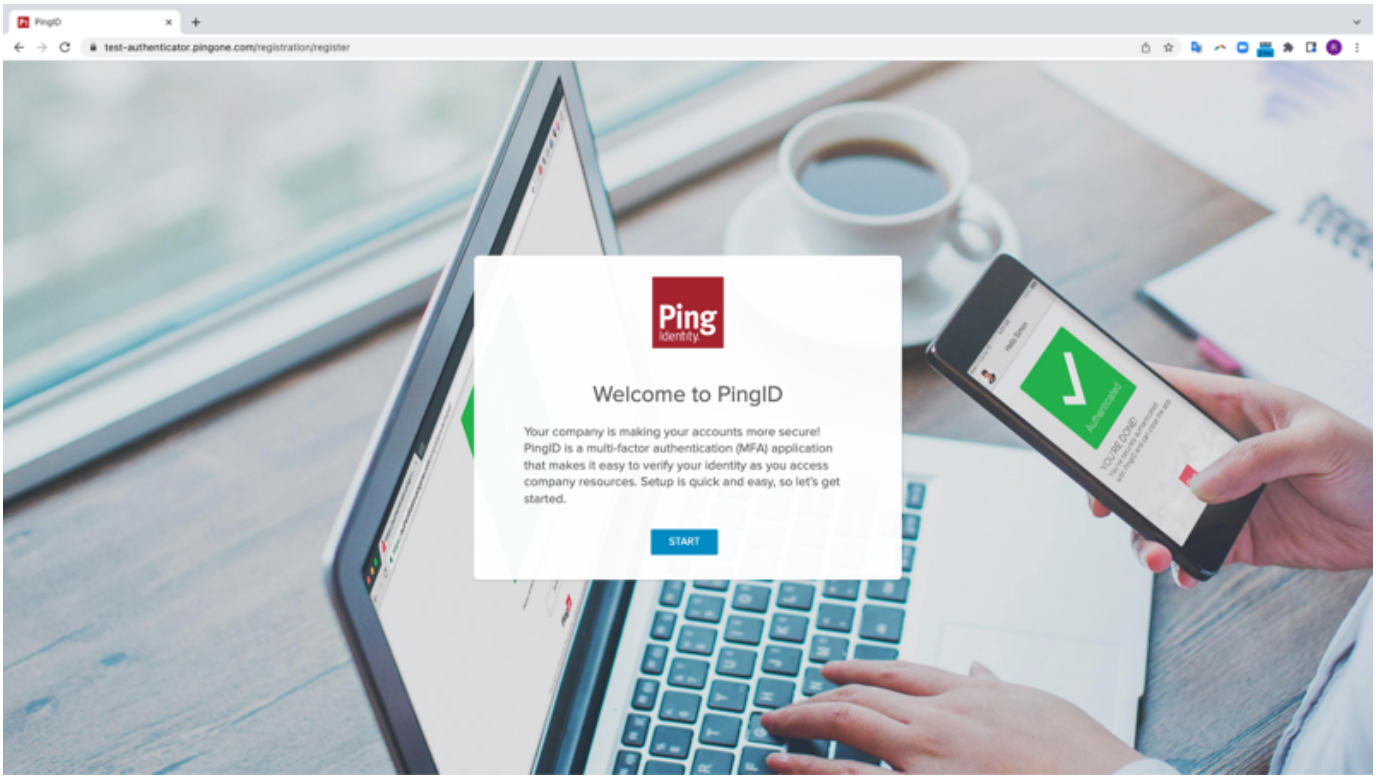
{{{ Video removed }}}

> **Note**
>
> Setting up PingID might vary slightly depending on the device model you are using, and the screens you see might vary from the ones shown here.

> **Important**
>
> If your organization requires authentication by biometrics, you'll need to set up biometrics (such as fingerprint authentication) on your device.

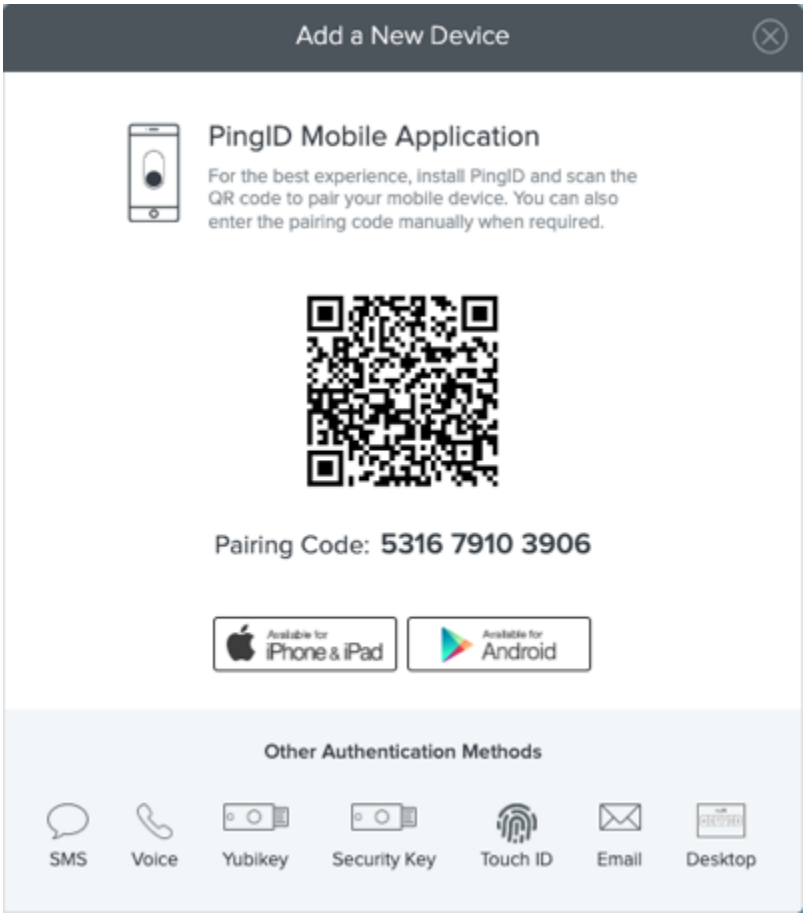
Steps

1. Sign on to your account or app, and when you see the registration window, click **Start**.



Result:

You'll see the **Add a New Device** window, showing the QR code.



2. Download and install the PingID app using one of the following options:

   Choose from:

   - **From the App Store**: On your mobile device, open the iPhone App Store, search for PingID, and tap **Install**.
   - **Using the Apple Store link**: On the PingID Registration window, click **Available for iPhone and iPad**, and from the Apple store site, install the app remotely on your iPhone or iPad.
   - **Generate an email link**: On the PingID Registration window, enter your email address and click **Get Download Link**. After you receive an email with a link to download the app, click the link and follow the instructions to install the app.

3. If you are using the Legacy Registration window, after you've installed PingID mobile app, in the PingID Registration window, click **I already installed the PingID app** to view the QR code.

   Result:

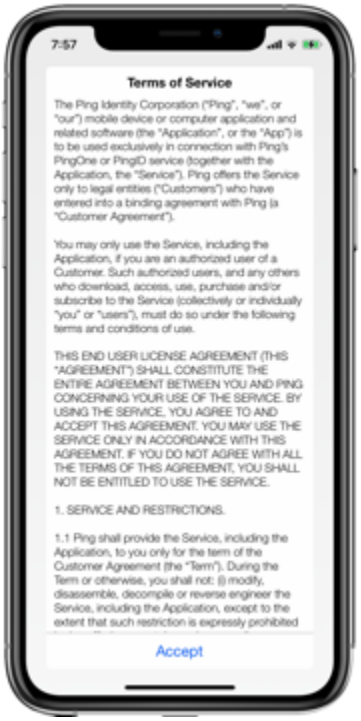
   Details of your pairing key and QR code are displayed in your web browser.

4. After the PingID app is installed, on your mobile device, tap **Open**.

   Result:

   The PingID app opens.

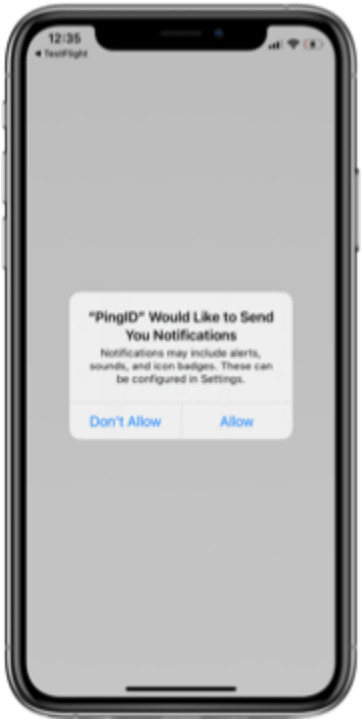
5. The first time you access PingID, you'll be asked to accept the terms of service. Tap **Accept**.



Result:

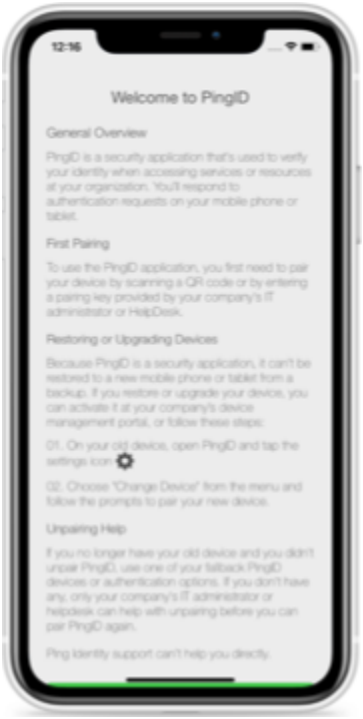
A message opens telling you to accept all PingID permission requests, including notification requests, and camera permissions when prompted to do so.

6. Tap **I Understand** and accept the notification request.

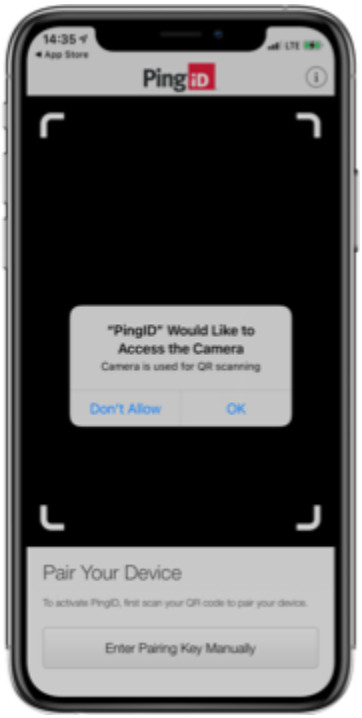


Result:

The **Welcome to PingID** information window opens, giving you an introduction to the PingID mobile app and some basic tasks.



7. Tap **Continue**, and tap **Allow** or **OK** to accept all PingID permission requests, including notification requests and camera permissions.



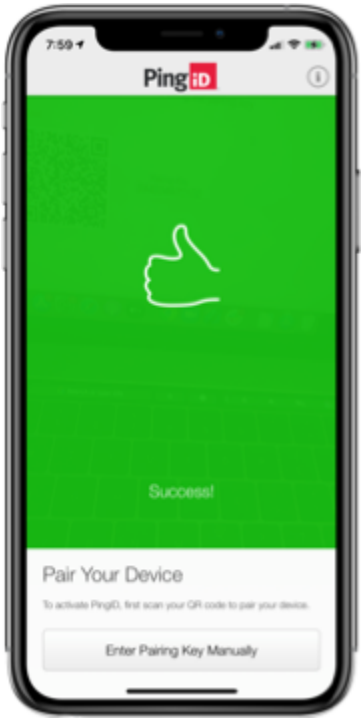
8. To pair your device with the QR code, from the PingID app on your device, point your device at the QR code in your browser.

Tip

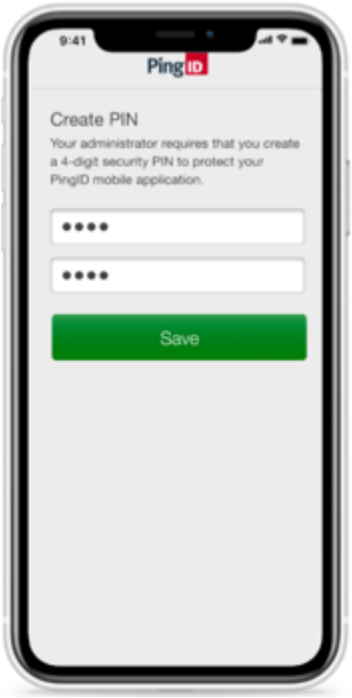
If you are unable to scan the QR code, on your mobile device, tap **Enter Pairing Key Manually** and enter the pairing key as shown on the registration page.

Result:

The green **Success!** message with a check mark displays, indicating the pairing request is successful, and the **Complete Your Profile** page opens automatically.

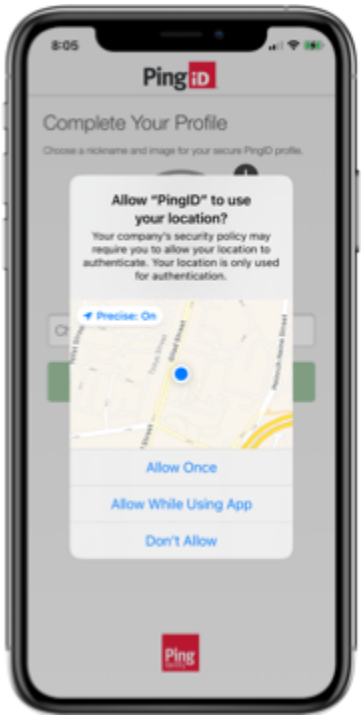


9. If your admin requires you to add a PIN code, you'll be asked to create your own unique 4 or 6 digit PIN.



> **Note**
>
> - If you are required to create a PIN code, you'll need to enter it every time you authenticate with the PingID mobile app.
> - Your PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively, and you can't choose digits that are in ascending or descending sequence, such as 1234.

10. If you have not already enabled location settings, when prompted to allow PingID to use your location, complete the following steps:



1. Tap **Allow While Using the App** (recommended), or **Allow Once**.

   Result:

   You receive another popup requesting the ability to keep location available in the background.

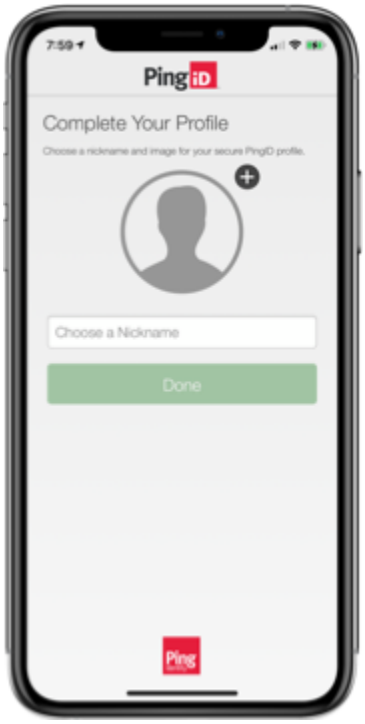
2. When prompted to always allow PingID to use your location, even when you are not using the app, tap **Change to Always Allow**.

> **Note**
>
> This option does not appear if you select **Allow Once** in the previous step.

Your company's security policy might require you to allow access to location to authenticate, even when PingID mobile app is closed, so this option is recommended.

11. In the **Choose a Nickname** field, enter a nickname for your profile and optionally add a picture. Tap **Done**.

    Your profile adds a layer of security. Your profile picture appears on all swipe or biometrics authentication requests, showing that the authentication request is intended for you.

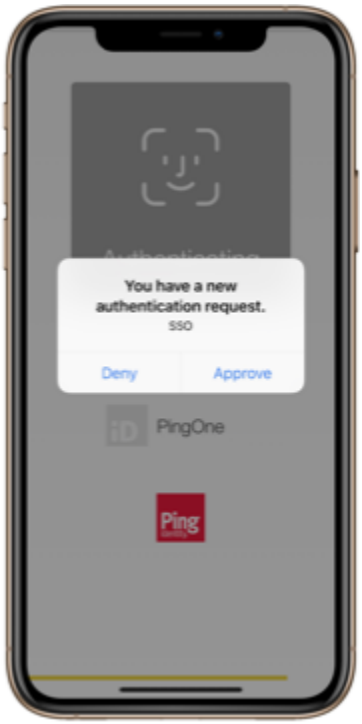


Result:

The PingID app screen displays, showing the one-time passcode number and your organization name in the organization list.

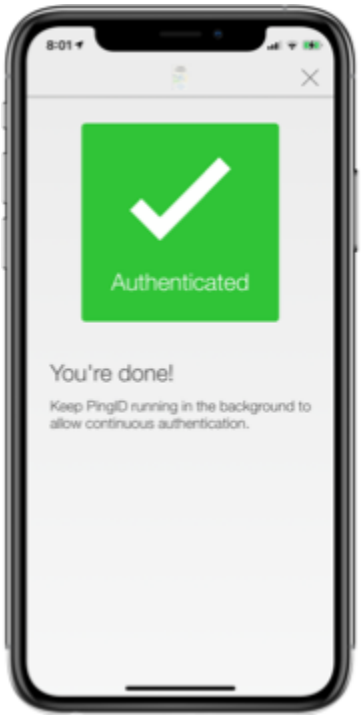
An authentication request is generated immediately, and you are prompted to authenticate on your device according to the authentication method set by your administrator, such as Face ID or Touch ID.

12. Authenticate using your mobile device.



Result:

After you have authenticated, a green check mark displays confirming authentication, and you are redirected to the company protected browser-based service or app that you wanted to access.



Next steps

For troubleshooting help for your mobile device, see Troubleshooting.

Related links

- Using PingID mobile app authentication (legacy)

(legacy) Pairing PingID mobile app for authenticating to your company's VPN

To set up PingID mobile app for secure authentication when accessing your company VPN, you need to download the app to your iOS device, and then register or 'pair' PingID mobile app with your account.

About this task

> **Note**
>
> Setting up MFA might vary slightly depending on the device you are using.
> If your organization requires authentication by biometrics, you must set up biometrics recognition on your device.

Steps

1. From your web browser or application, sign on to your VPN with your username and password.

   Result:

   A message appears, asking you to install the PingID app and displays your pairing key. You need the pairing key for step 4.

2. From your mobile device:

   1. Go to the **App Store**.

2. Search for PingID.
3. Tap **Install**.

   Result:

   If you have antivirus software installed, you might receive a message that PingID is seeking root access to your device. If so, select **Yes** or **Trust**.

3. After the installation is complete, on your device, tap **Open**.
   1. The first time you access PingID, to accept the **Terms of Service**, tap **Accept**. A message opens telling you to accept all PingID permission requests, including notification requests, and camera permissions when prompted to do so.
   2. Tap **I understand**. The **Welcome to PingID** information window opens, giving you an introduction to the PingID mobile app and how it works.
   3. Tap **Continue**, and then tap **Allow** and **OK** to accept all camera and location permission requests from PingID.
4. Tap **Enter Pairing Key Manually** and enter the pairing key. Tap **Pair Device**.

   Result:

   The **Complete Your Profile** screen opens on your device.
5. If your admin requires you to add a PIN code, you'll be asked to create your own unique 4- or 6-digit PIN.

   > **Note**
   > - If you are required to create a PIN code, you'll need to enter it every time you authenticate with the PingID mobile app.
   > - Your PIN code must include at least 3 or 4 different digits for PIN lengths of 4 and 6 digits, respectively, and you can't choose digits that are in ascending or descending sequence, such as 1234.
6. If you have not already enabled location settings, a popup appears, asking you to allow PingID to use your location. Choose from the following options:

   > **Note**
   > The exact wording of the message, and the number of popups presented may differ depending on the OS version that your device is running.

   Choose from:

   - (Recommended) **Allow all the time**: Always allow PingID to access location. Your company's security policy may require you to allow access to location to authenticate, even when the PingID mobile app is closed, so this option is recommended.
   - **Allow only while using this app**: Only allow PingID to access your location when using the PingID mobile app.
   - **Only this time**: Allow PingID to access your location for this authentication request only.
   - **Deny**: Do not allow the PingID mobile app to access your location.
7. Enter a nickname for your device, optionally add a picture, and then tap **Done**.

Result:

Your device is paired and a one-time passcode (OTP) is displayed on your device.

8. After your device is paired, on the VPN sign-on page, type `OK`.

   Result:

   A push notification is sent to your mobile device.

9. When prompted, authenticate on your mobile device.

   Result:

   The pairing process is complete. The next time you sign on to your VPN with your username and password, you are prompted to authenticate on your device. For help with troubleshooting issues, see Troubleshooting PingID authentication.

Related links

- Using PingID mobile app authentication (legacy)

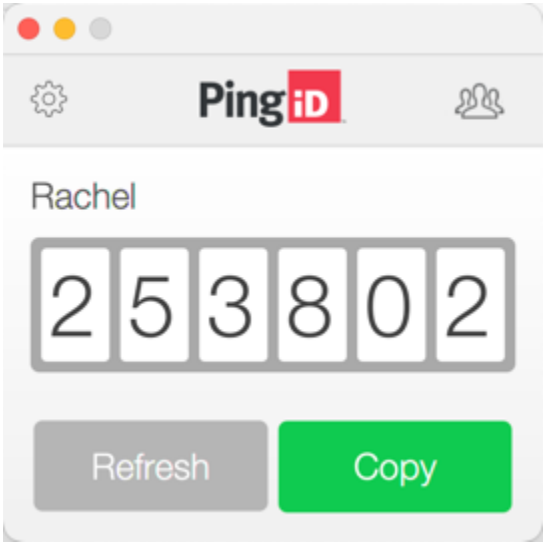
Using PingID desktop app authentication

Use PingID desktop app to authenticate using an app on your computer (PC or Mac) for a secure sign-on experience.

To set up PingID desktop app authentication, you need to download PingID desktop app to your computer, and then register or 'pair' it with your account. Pairing creates a trust between the desktop app and your account so that you can use the app to authenticate.

After pairing your device with your account, each time you sign on to your account, launch the PingID desktop app to generate a one-time passcode (OTP) you can use to authenticate.

After you have paired your device and authenticated successfully, you can use the app to authenticate when accessing your account using a web browser, to access your company VPN, or to access a Windows login machine using Remote Desktop Protocol (RDP), if your company configuration allows it.



You can find information on managing your PingID desktop app, including software updates, changing your PIN, adding an organization, and sending log in PingID desktop app management.

> **Note**
>
> The option to pair your account with this device type is defined by your company policy.

PingID desktop app for remote access for Windows login

If you want to use PingID desktop app for remote access for Windows login, you need to download and install the PingID desktop app to a different laptop or desktop from the one that you are trying to access remotely and pair (connect) that machine with your account. Then, you can receive a one-time passcode (OTP) from the local PingID desktop app to authenticate and sign on to your Windows machine remotely using RDP.

Pair desktop app

Pairing your PingID desktop app

To set up PingID desktop app for secure authentication, you need to register or 'pair' PingID desktop app with your account.

Before you begin

- Install the PingID desktop app. This is often done by your administrator. For instructions on how to install it yourself, see the relevant tab in this section for Mac or Windows.

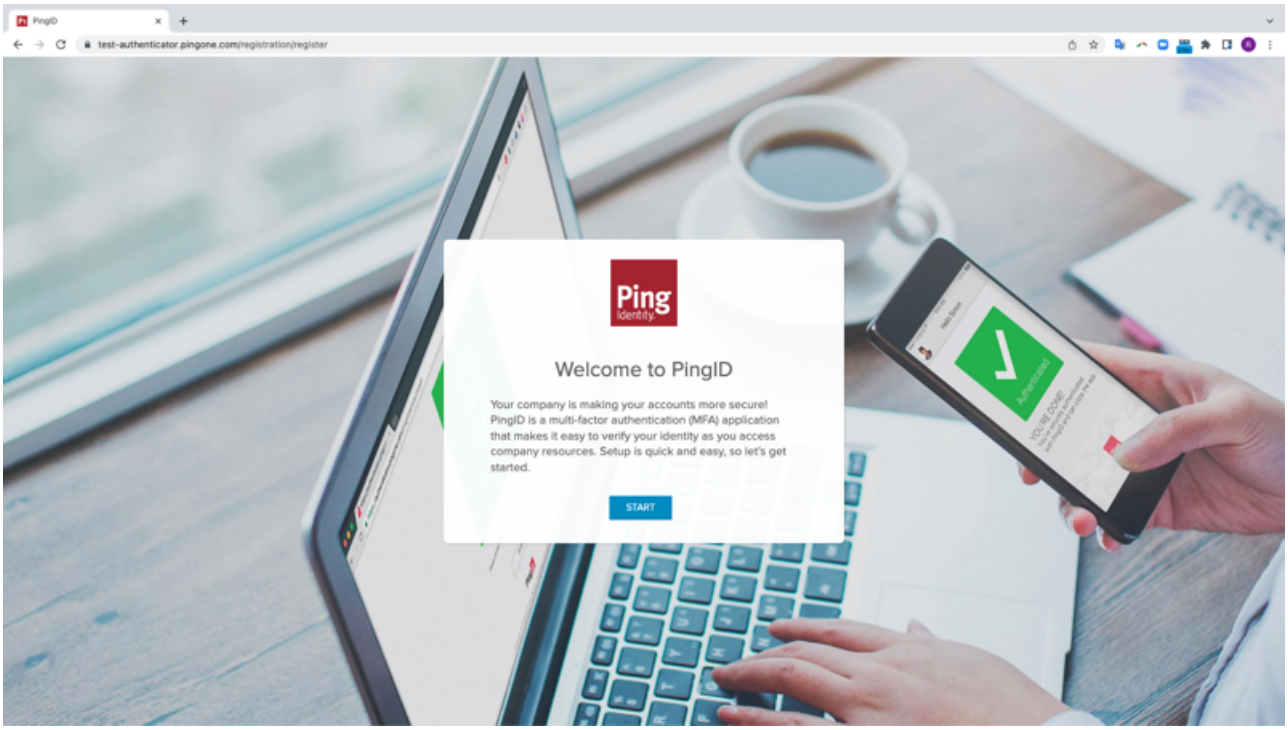
About this task

After you have paired your device and authenticated successfully, you can also use the app to authenticate when accessing your VPN, or a Windows login machine using Remote Desktop Protocol (RDP), if required.

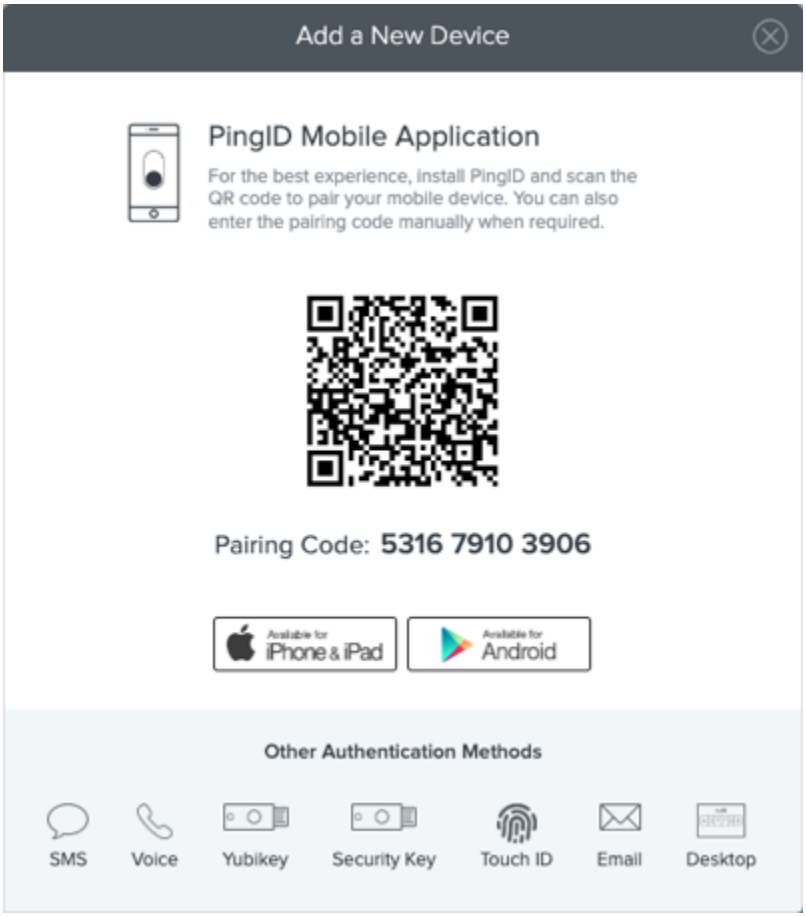
> **Note**
>
> If you already have a device paired with your account and your organization allows you to pair more than one device, you can add the PingID desktop app as an authentication method in the **My Devices** page. For more information, see Adding and reordering devices.

Steps

1. Sign on to your account or app and when you see the registration window, click **Start**.



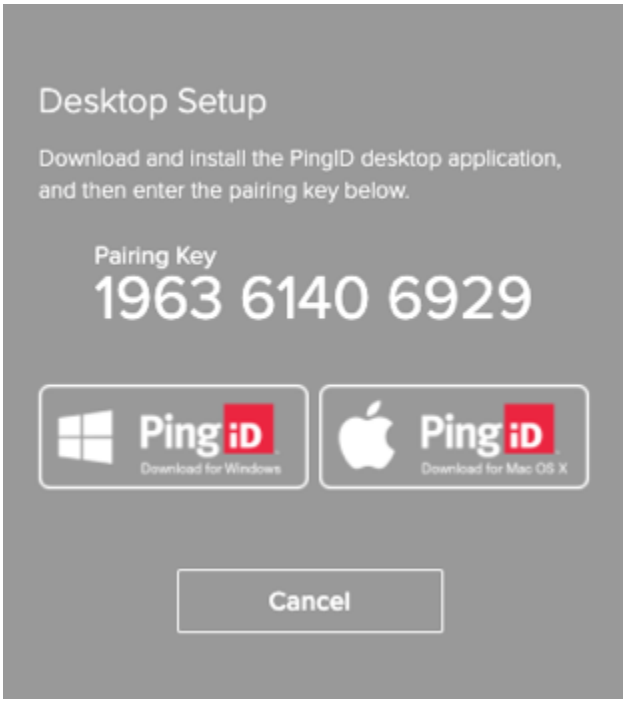
You'll see the **Add a New Device** window, showing the QR code.



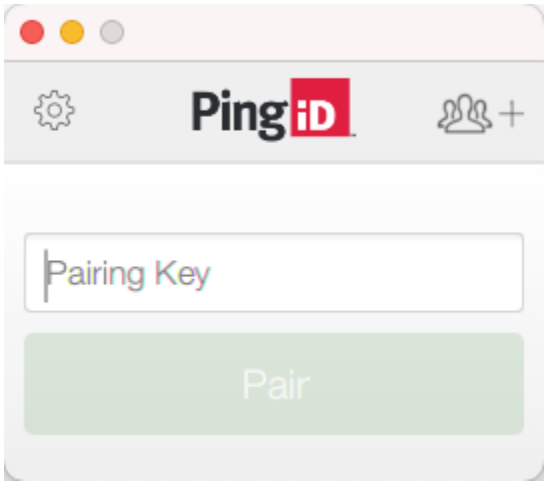
2. In the **Add a New Device** window, click **Desktop**.

   Result:

   The **Desktop Setup** window opens, displaying a **Pairing Key**.



3. Launch the PingID desktop application, and in the **Pairing Key** field enter the pairing key from step 2 and then click **Pair**.



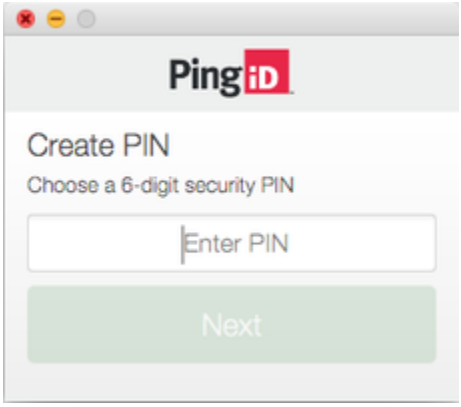
4. (Optional) If you want to create a user profile, before you enter the pairing key, click  , enter a name for the profile, and then click **Create**. The Desktop app shows the name of the profile and the **Pairing Key** field.

   Result:

   A one-time passcode (OTP) generates. If you are prompted to create a PIN code, see step 4.

5. If your organization requires you to create a PIN code:

   1. In the **Enter PIN** field, enter a PIN code. Click **Next**.

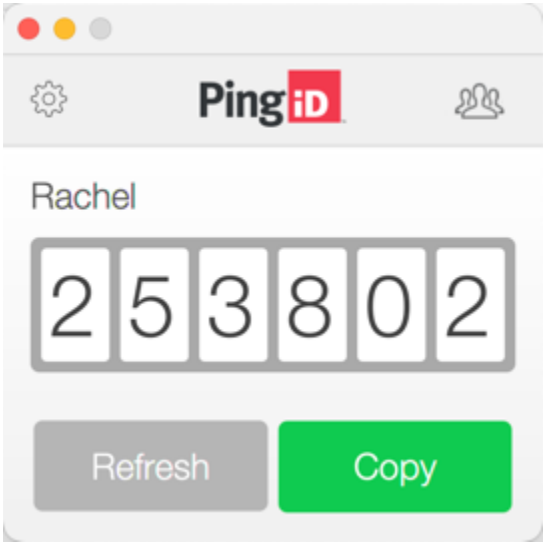


> **Note**
>
> The PIN code must be either 4 or 6 digits, as specified, and include more than 2 different digits if the PIN length is 4 digits, or 3 different digits if the PIN length is 6 digits. Digits must not be in ascending or descending sequence. For example, 1111, 123321, 8787, and 765432 are not allowed.

2. Re-enter the PIN code when prompted. Click **Done**.

   Result:

   An OTP is generated.



6. The next time you sign on to your account or app using a web browser, use the PingID desktop app to authenticate:

   1. Launch the PingID desktop app to generate an OTP.
   2. Copy the OTP.
   3. Paste the OTP into the **Authentication** field in your browser.
   4. Click **Sign On**.

Result:

The green checkmark appears indicating your successful authentication. Your browser redirects to the portal or app you need to access.

Related links

- Authenticating using PingID desktop app

Install on Mac

Installing PingID desktop authentication on a Mac

Install desktop authentication on your Apple Mac machine so that you can pair it for secure authentication.

Before you begin

- Ensure you have administrator privileges on your machine

About this task

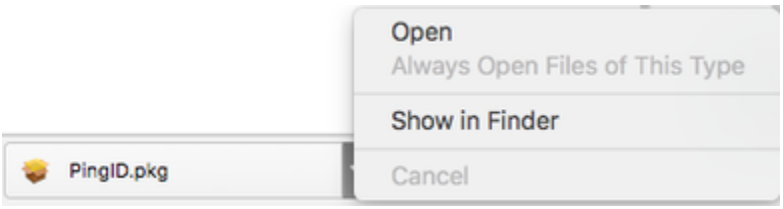
To start using PingID desktop app, you need to:

1. Download and install PingID desktop app.
2. Pair PingID desktop app with your account.

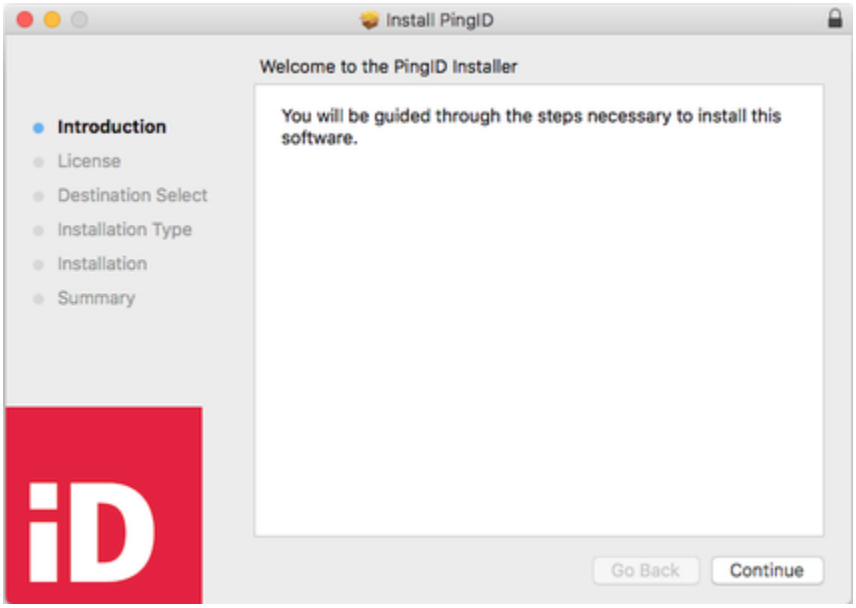
After you have installed and paired your device, you can use PingID desktop app to authenticate when access your account using a web browser, your VPN, or your Windows login machine using RDP.

Steps

1. Download PingID desktop app for Mac, and click **Save**.

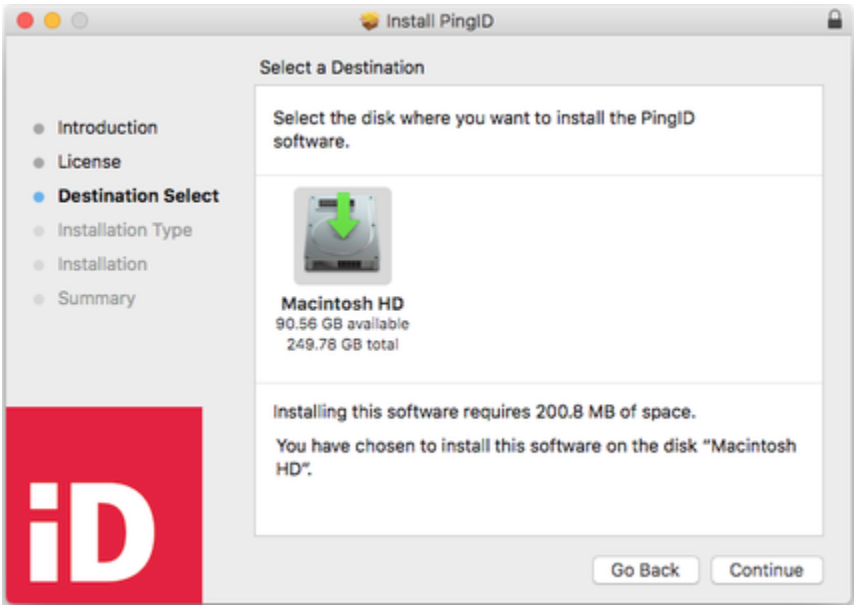


2. Install the PingID desktop app:
    1. To launch the PingID desktop app installer, click the `PingID.pkg` download file. Click **Continue**.

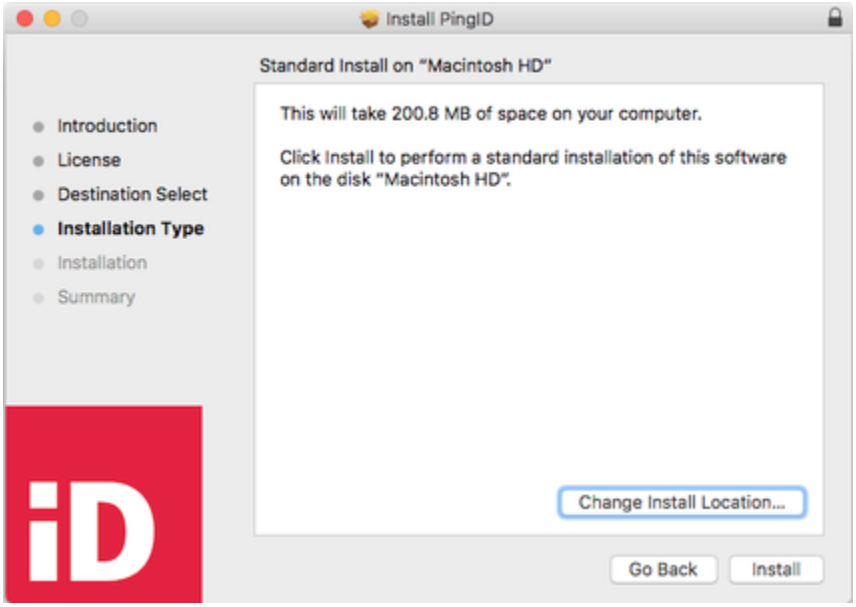


    2. Review the **Software License Agreement** and click **Continue**. Click **Agree**.

3. In the **Select a Destination** window, in the **Destination Select** section, select the disk where you want to install PingID for Desktop. Click **Continue**.



4. To change the location where PingID is installed, in the **Installation Type** section, click **Change Install Location** and browse to the new location.



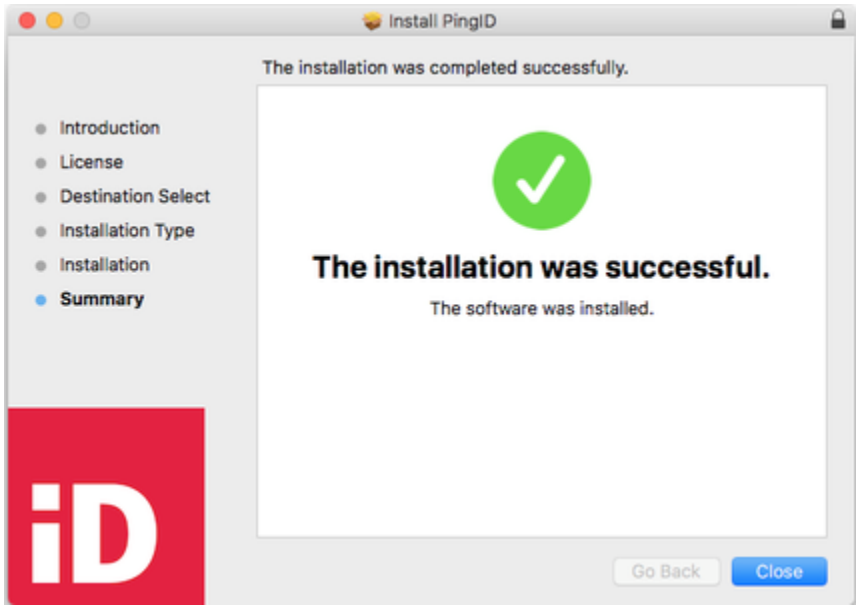
5. Click **Install**.

> **Note**
>
> By default, the PingID desktop app installs in the **Applications** folder.

6. If prompted, enter your system password.

   Result:

   The PingID desktop app installer window displays the **The installation was successful** message with a green check mark. PingID is added to the **Applications** list on your Mac.



7. Click **Close**.

Next steps

Pair PingID desktop app with your account. For information, see Pairing your PingID desktop app.

Install on Windows

Installing PingID desktop authentication on Windows

Install the PingID desktop app on your Windows machine so that you can pair it for secure authentication.

About this task

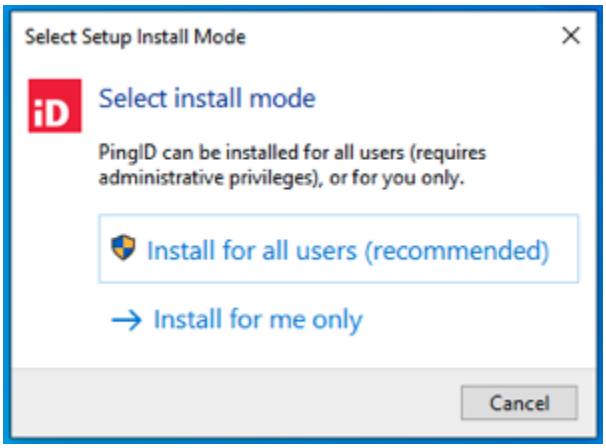
To start using PingID desktop app on your Windows machine, you need to:

1. Download and install PingID desktop app.
2. Pair PingID desktop app with your account.

After you have installed and paired your device, you can use PingID desktop app to authenticate when access your account using a web browser, your VPN, or a different Windows login machine remotely, using RDP.

Steps

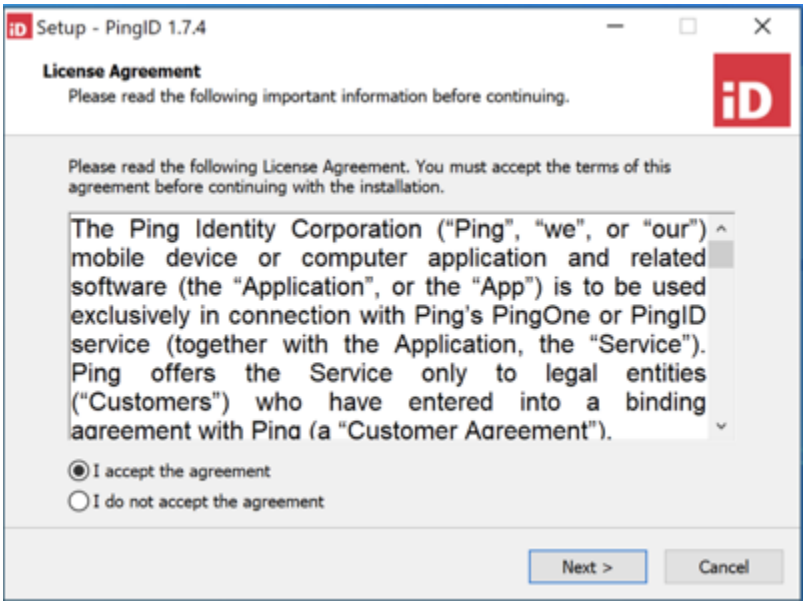
1. Download PingID desktop app for Windows, and click **Save**.
2. To install the PingID desktop app:
    1. Click the `pingID.exe` download file to launch the PingID desktop app installer.
    2. In the **Select install mode** window, choose the relevant option:
        - **Install for me only**: install the desktop app on your local machine.
        - **Install for all users**: For administrators only. Allows administrators to install the desktop app on multiple machines concurrently.



Result:

The **PingID Setup** wizard opens.

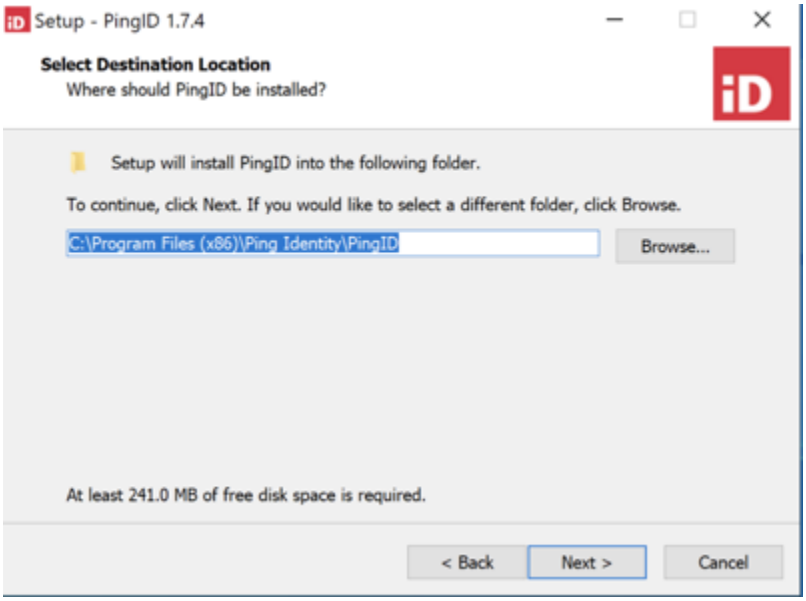
3. Review the Software License Agreement and select **I accept the agreement**. Click **Next**.



Result:

The **License Agreement** window opens.

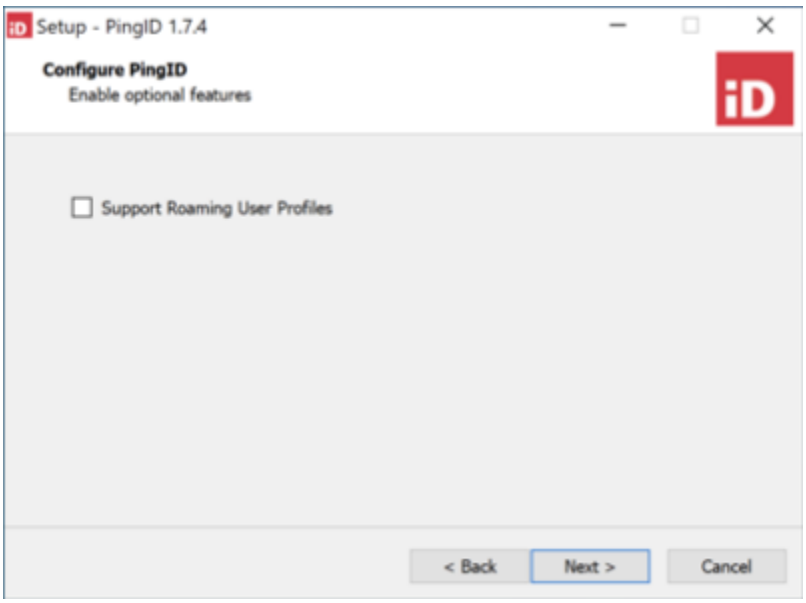
4. Click **Browse** and select the folder in which you want to install PingID and then click **Next**.



Result:

The **Configure PingID** window opens.

5. To synchronize the settings in the domain roaming folder, select the **Support Roaming User Profiles** check box.



> **Note**
>
> During a manual update or reinstall over an existing installation, the **Configure**PingID**Enable optional features** window does not display. The previous installation setup is maintained.

6. To add the **Support Roaming User Profiles** setting to an existing configuration when it was not previously enabled:
    1. Unpair your Windows desktop app.
    2. Uninstall the desktop app, reinstall, and select the **Support Roaming User Profiles** check box to allow the use of roaming user profiles.
7. Click **Next**.

    Result:

The files are extracted and the PingID desktop app launches.

Next steps

Pair PingID desktop app with your account. For information, see Pairing your PingID desktop app.

Using Windows Hello for authentication with PingID

If your Windows Hello device supports FIDO2 biometrics, you can use it to authenticate with PingID for a secure sign-on experience. To set up your Windows Hello device for secure authentication with PingID, you need to register or 'pair' it with your account.

Pairing creates a trust between your Windows Hello device and your account so that you can use it to authenticate during the sign-on process. You can use Windows Hello biometrics to access your account and apps using a web browser.

Note

PingID Mobile app using biometrics (fingerprint, face or, iris authentication) and Biometric web authentication with Windows Hello are different methods of authentication:

- PingID mobile app: Allows you to authenticate when accessing your account from various different devices. Requires you to install PingID mobile app on your mobile device, and to pair it with your account.
- Biometrics authentication: Allows you to authenticate using your Windows Hello device's built-in biometrics, when signing on to your account, without downloading an app. You can only sign on to your account from the same device with which you want to authenticate.

Web only

Pairing your Windows Hello device

To set up Windows Hello authentication on your Windows machine for secure authentication with PingID, you need to register or 'pair' your Windows Hello device with your account.

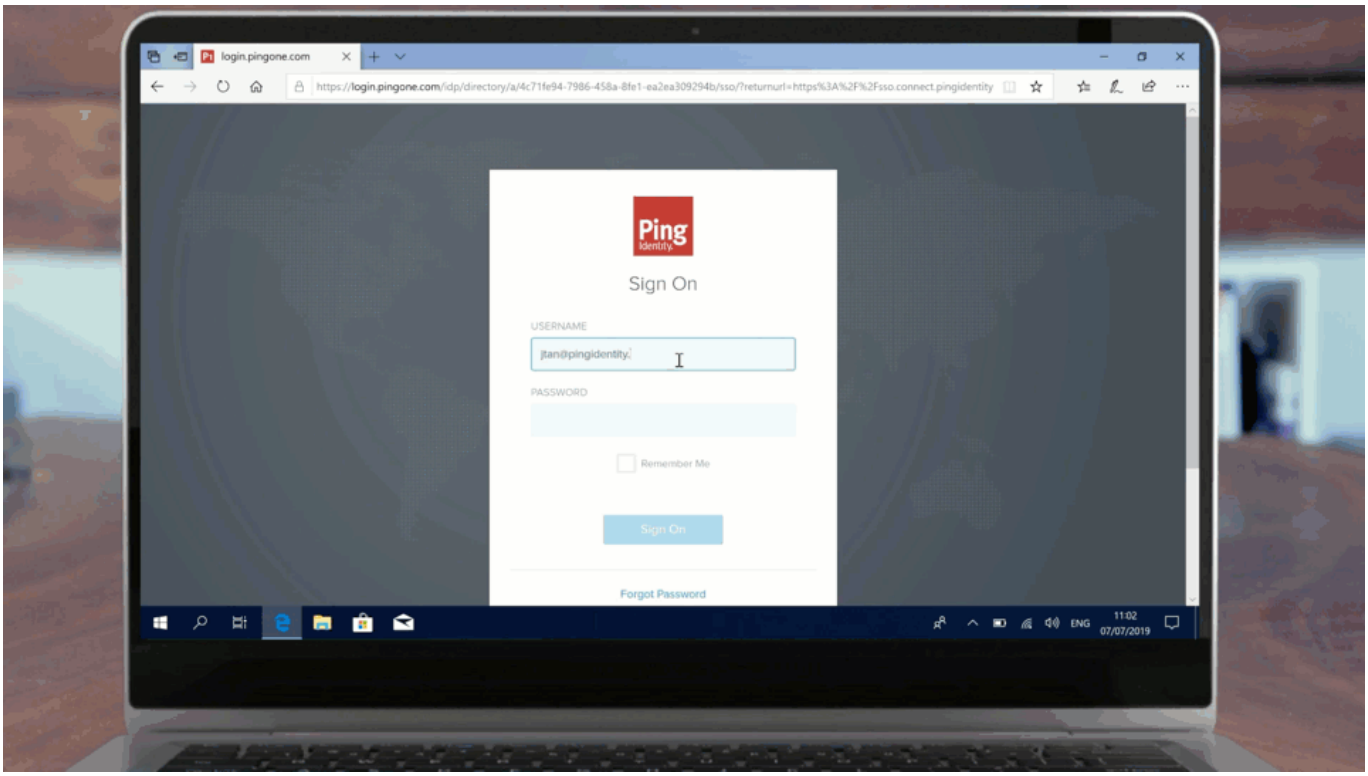
Before you begin

Ensure your Windows Hello device supports FIDO2 biometrics and that you are using:

- Windows 10, OS Build 1809 or later.
- A browser that supports the use of FIDO2 biometrics, such as Windows Edge v44.17763 or later.
- Set up Windows Hello biometrics sign in on your machine, such as registering your fingerprints or face. Follow the manufacturer's guidelines to do so.

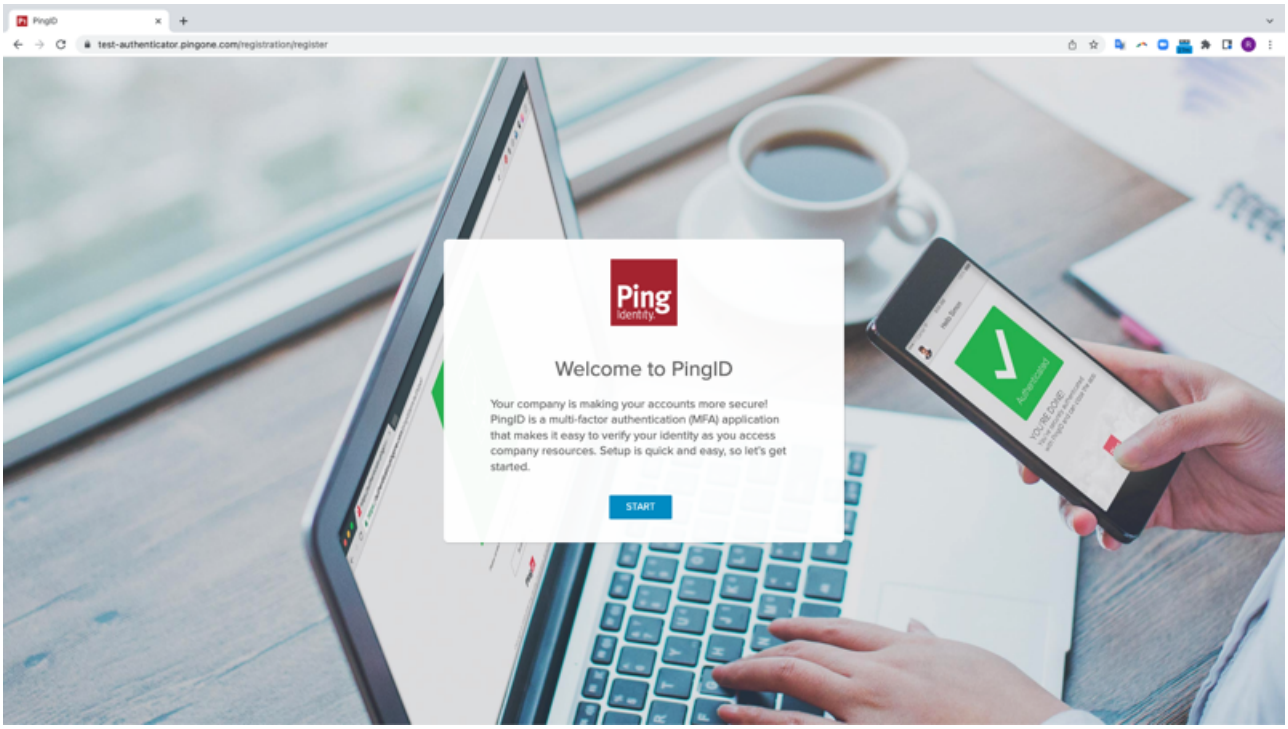
About this task

> **Note**
>
> After registering, use your Windows Hello device to authenticate with PingID for both second factor or passwordless authentication flows depending on your organization's configuration. For more information, see Authenticating with PingID using Windows Hello.

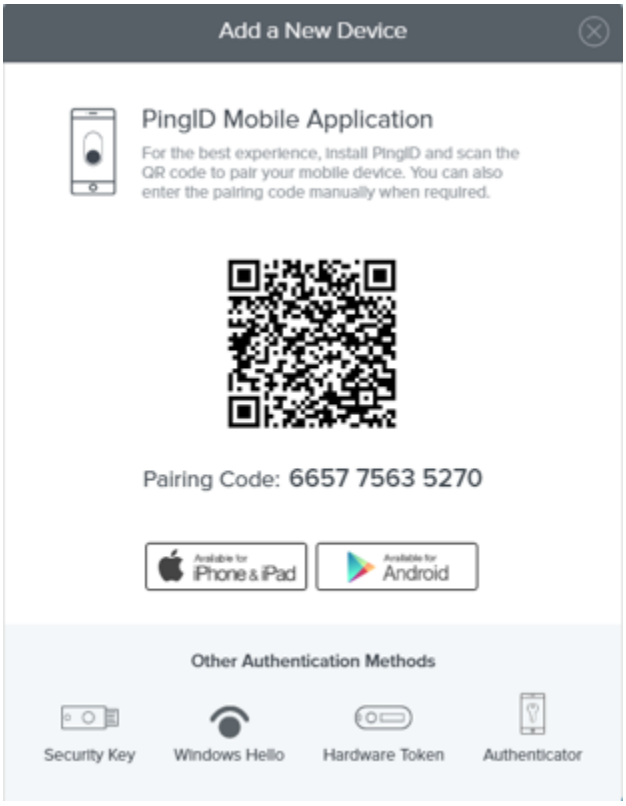


Steps

1. From your Windows Hello machine, sign on to your account or app and when you see the registration window, click **Start**.



You'll see the **Add a New Device** window, showing the Windows Hello icon.



2. In the **Add a New Device** window, click **Windows Hello**.

> **Note**
>
> If the **Authenticate using Windows Hello** option does not appear in the list, see [pid_ug_setting_up_windows_hello_auth.dita].

Result:

Your application prompts you to authenticate.

3. Use your Windows Hello device to validate your identity, for example, using your fingerprint.

> **Note**
>
> Ensure the **Alternative Authentication** browser window is the active window.
> If you see a message asking if you permit your device to communicate with the biometrics device, select **Allow** or **Yes** to continue. The message can differ depending on the browser you are using.

Result:

A green check mark appears with an **Authenticated** message, indicating authentication is successful. You are automatically signed on to your account or app.

Result

To sign on to your account or application, authentication requests prompt you to use your biometrics device. For more information, see Authenticating with PingID using Windows Hello.

For troubleshooting, see Troubleshooting FIDO2 biometrics.

Related links

- Authenticating with PingID using Apple Mac Touch ID

Using Apple Mac Touch ID for authentication with PingID

You can use your Apple Mac device with Touch ID for secure access your account and apps when using a web browser with PingID authentication. To set up your Apple Mac Touch ID device for secure authentication with PingID, you need to register or 'pair' your device with your account.

If your Mac machine supports FIDO2 platform biometrics, after pairing it with your account you can use it to access your account or apps through a web browser.

Note

Do not confuse biometric web authentication for Mac with the PingID mobile app, which also uses fingerprint or face authentication.

- PingID mobile app: Use PingID mobile app to authenticate when you access your account from various devices. Requires you to install PingID mobile app on your mobile device, and to pair it with your account.
- Apple Mac Touch ID: Authenticate using your Mac device's built-in biometrics, when signing on to your account, without downloading an app. You can only sign on to your account from the same device with which you want to authenticate.

You can use biometric web authentication through Touch ID only to authenticate your account from the same Touch ID device you use to access your account.

Web only

Pairing your Mac Touch ID device

To set up your Apple Mac machine for secure authentication, you need to register or 'pair' your Mac Touch ID device with PingID.

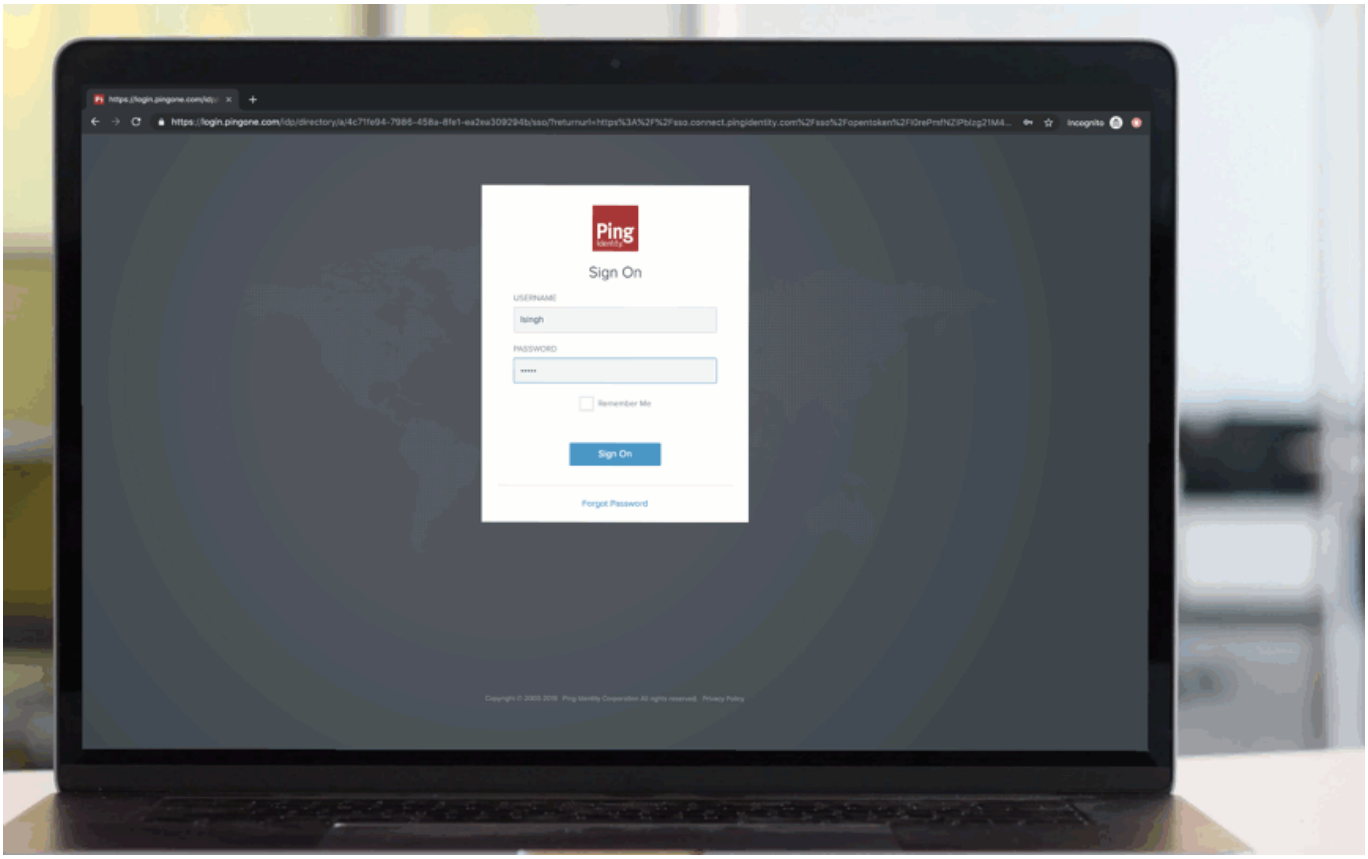
Before you begin

- Ensure that your Mac device has Touch ID and supports FIDO2 platform biometrics.
- Set up Touch ID biometrics sign on for your machine, such as registering your fingerprints. Follow the manufacturer's guidelines to do so.
- Ensure you are using a browser that supports the use of FIDO2 platform biometrics, such as Google Chrome or Safari, and that you have the latest version of the browser.

> **Note**
>
> Safari browser for Touch ID authentication requires MacOS Big Sur or later.

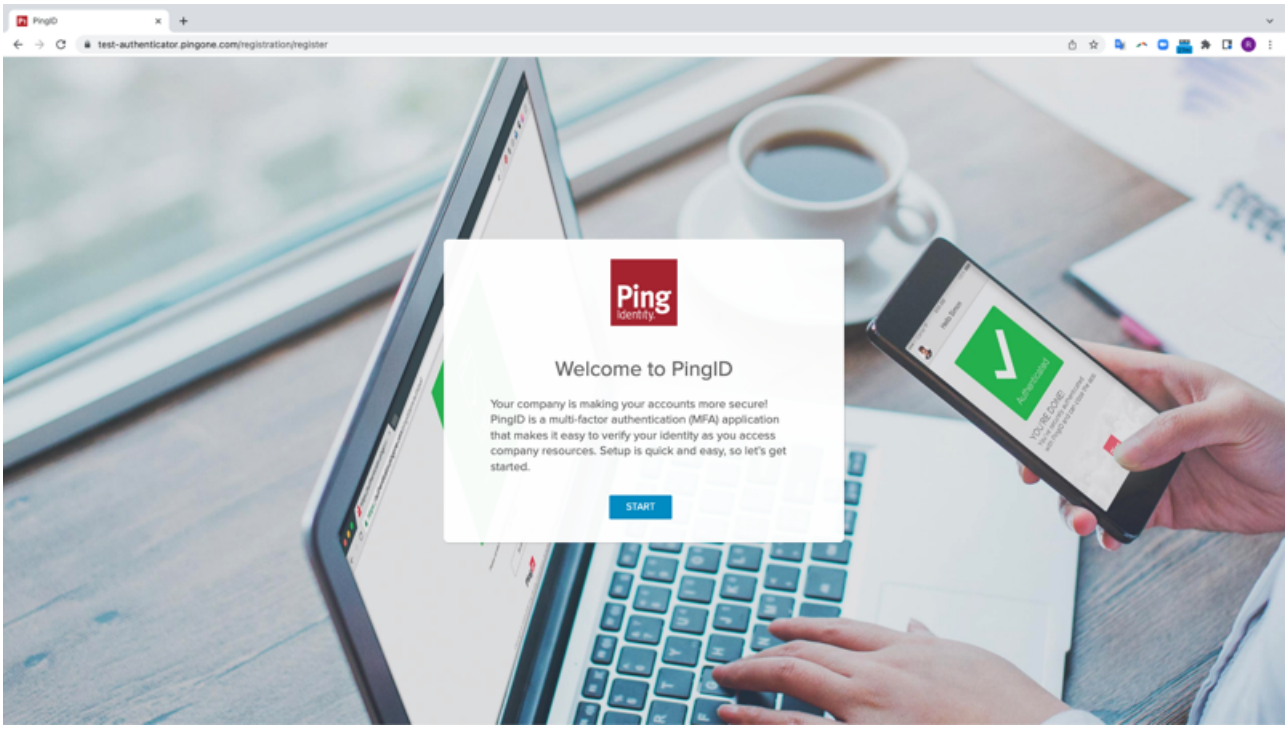
- Touch ID FIDO2 authentication is currently browser-specific. The browser that you use to set up your device must be the same browser you use to authenticate. For example, if you set up your Touch ID FIDO2 device using a Safari browser, you will only be able to authenticate with that Touch ID FIDO2 device on a Safari browser. If you want the option to authenticate using a different browser, you must pair the device through the browser separately.

About this task

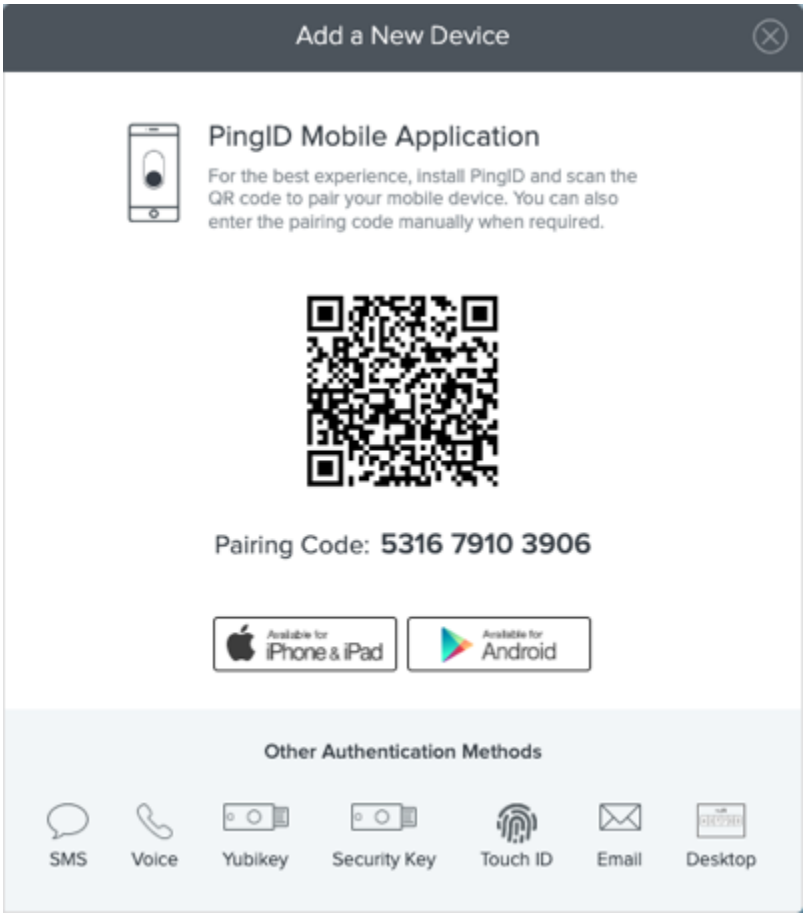


Steps

1. From your Mac machine, sign on to your account, and when you see the registration window, click **Start**.



You'll see the **Add a New Device** window, showing the Touch ID icon.

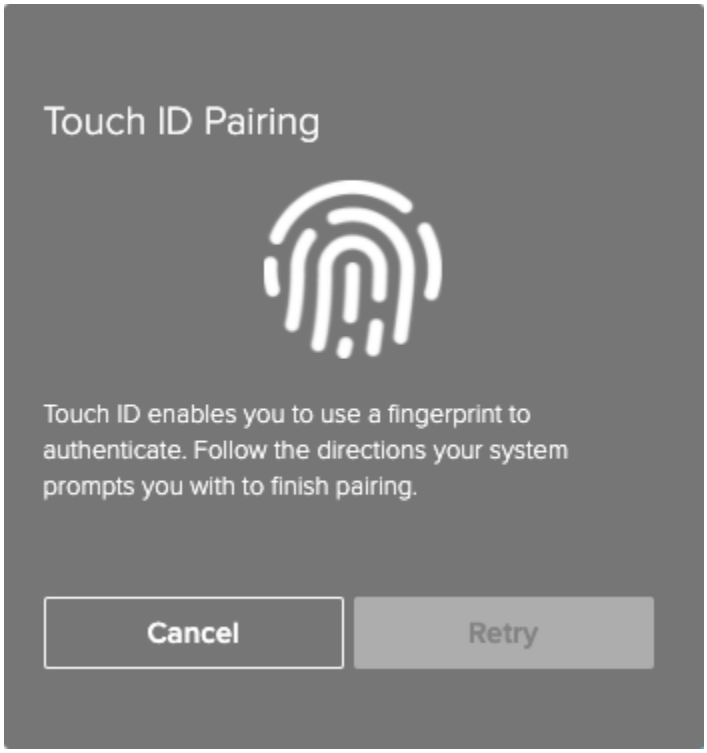


2. In the **Add a New Device** window, click **Touch ID**.

> **Note**
>
> If the **Authenticate using Windows Hello** option does not appear in the list, see Troubleshooting FIDO2 biometrics.

Result:

You are prompted to authenticate.



3. Use your Mac device to validate your identity, such as using your fingerprint.

> **Note**
>
> - Make sure the **Alternative Authentication** browser window is the active window.
> - If you see a message asking if you permit your device to communicate with the biometrics device, select **Allow** or **Yes** to continue. The message might differ depending on the browser you are using.

Result:

A green **Authenticated** message with a check mark appears, indicating your device pairing is successful, and you are automatically signed on to your account or app.

Next steps

The next time you sign on to your account or application, follow the prompt to authenticate using your biometrics device. For information, see Authenticating with PingID using Apple Mac Touch ID.

Related links

- Troubleshooting FIDO2 biometrics

Related links

- Authenticating with PingID using Apple Mac Touch ID

Using iOS or iPadOS biometrics for authentication with PingID

If your iOS device supports FIDO2 biometrics, you can use the built-in biometrics in your device (Face ID or Touch ID) to authenticate with PingID for a secure sign-on experience. To set up your iOS device for secure authentication with PingID, you need to register or 'pair' it with your account.

You can use your iOS device (iPhone or iPad) to access your account or apps using a web browser.

> **Note**
>
> PingID mobile app using biometrics and iOS biometric authentication are different methods of authentication:
>
> - PingID mobile app: Allows you to authenticate when accessing your account from various different devices. Requires you to install PingID mobile app on your mobile device, and to pair it with your account.
> - iOS biometrics authentication: Allows you to authenticate when accessing your account from a specific iOS device, using that device's built-in biometrics, through Touch ID or Face ID. You can only sign on to your account from the same device with which you want to authenticate.

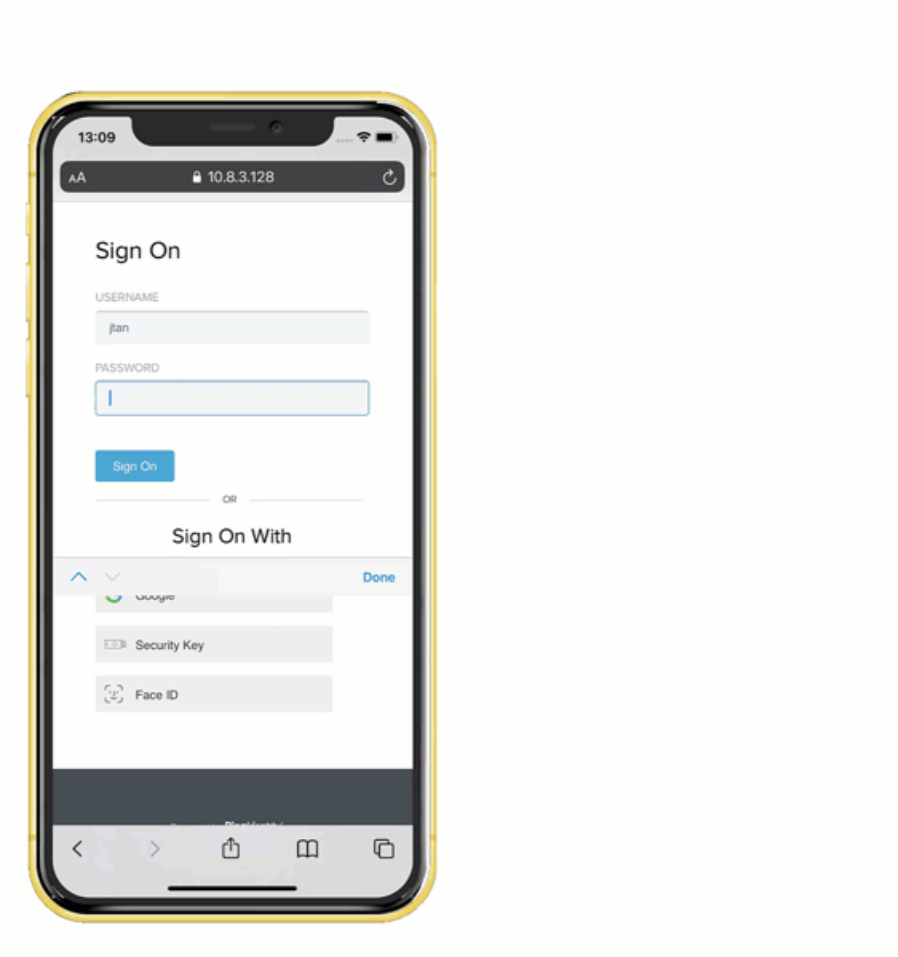
Web only

Pairing your iOS or iPadOS biometrics device

Pair your iOS or iPadOS device so that you can use it to authenticate with PingID.

Before you begin

- Ensure your device supports FIDO2 biometrics and is running iOS 14 or later or iPadOS 14 or later.
- Set up biometric authentication on your accessing device, such as registering your face or fingerprints. Follow the manufacturer's guidelines to do so.
- Ensure you are using a browser that supports the use of FIDO2 biometrics, such as Safari, and that you have the latest version of the browser.

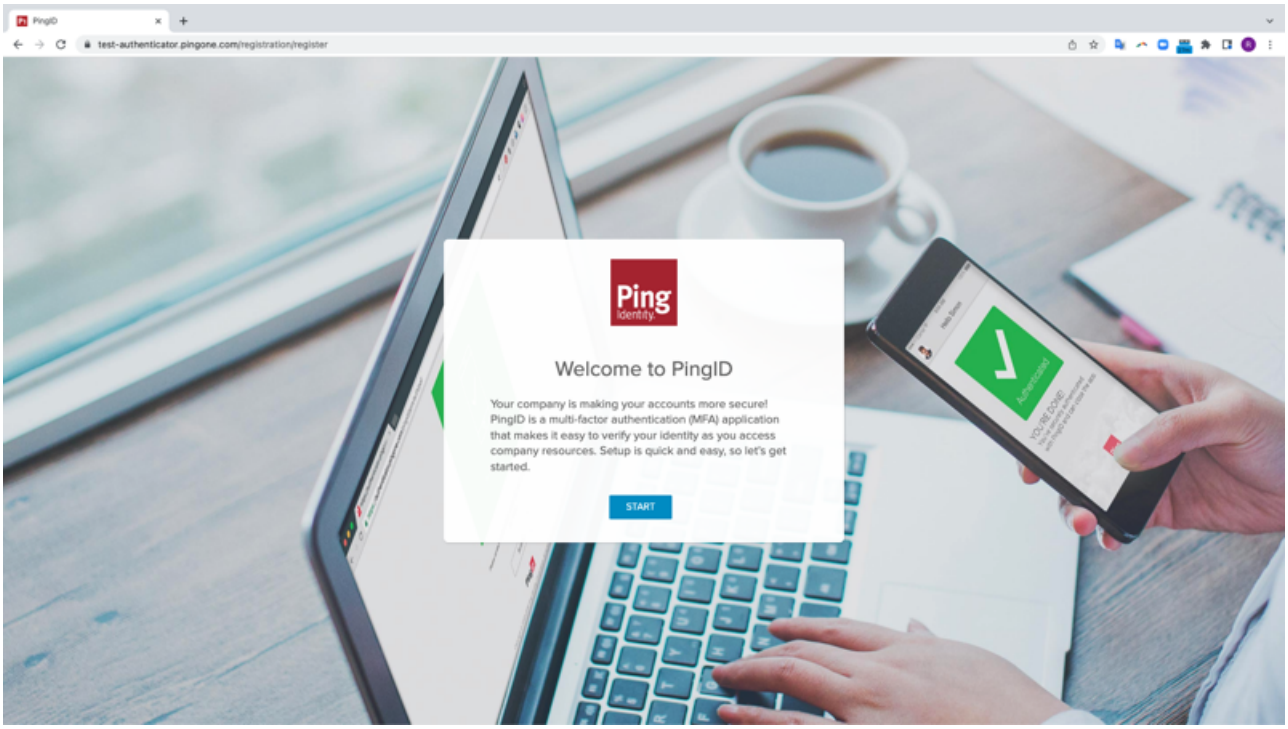


About this task

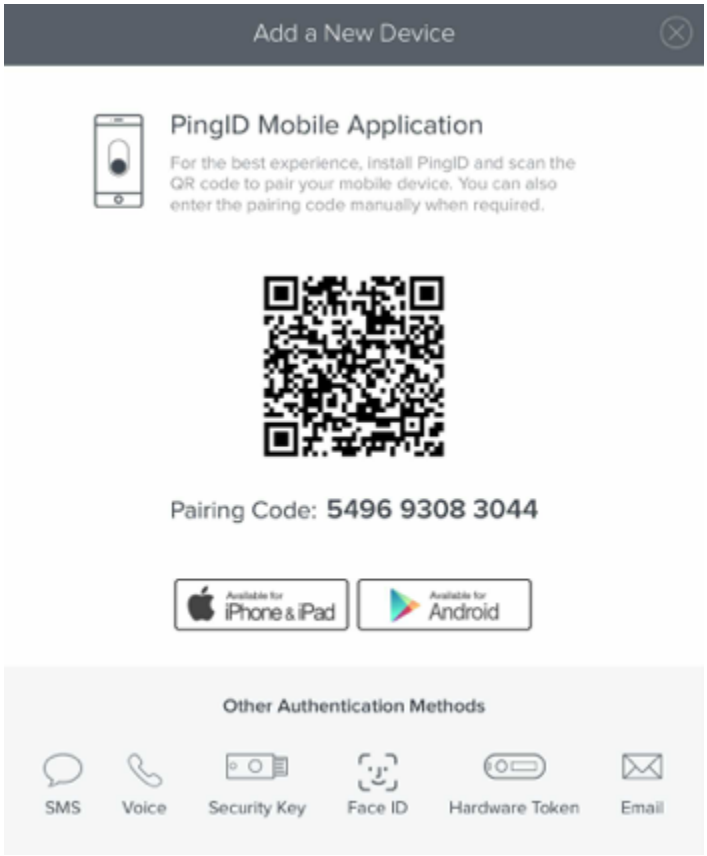
Follow the instructions below to set up biometrics authentication on your device. The following example shows the process on an iPad device.

Steps

1. From the registration window, click **Start**.



You'll see the **Add a New Device** window, showing the Face ID icon.

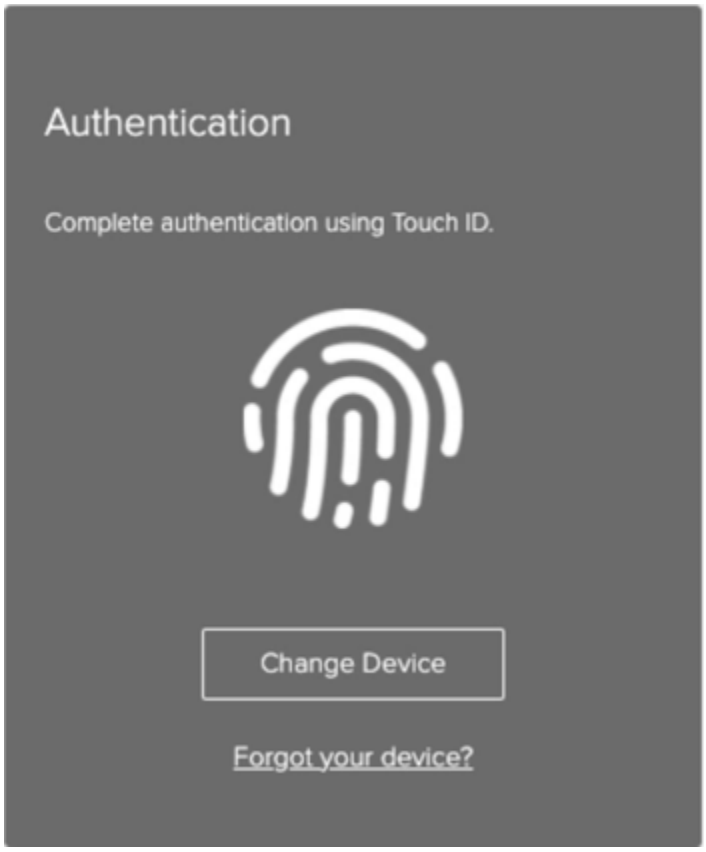


2. In the **Add a New Device** window, click **Face ID**.

> **Tip**
>
> Tap **Authenticate using Face ID**, even if your device only supports fingerprint authentication. You will be able to authenticate using your fingerprint.

Result:

A window appears prompting you to authenticate using your biometrics device.



3. Use your device to validate your identity with fingerprint or Face ID.

> **Note**
>
> Make sure that the **Alternative Authentication** window is the active window.
> If a message appears asking you to allow your device to communicate with the biometrics device, select **Allow** or **Yes** to continue. The message might differ depending on your browser.

Result:

A green **Authenticated** message with a check mark appears, indicating your device pairing is successful, and you are automatically signed on to your account or app.

4. The next time you want to sign on to your account or application, follow the prompt to authenticate using your biometrics device.

   For more information, see Authenticating with PingID using iOS or iPadOS biometrics.

Related links

- Troubleshooting FIDO2 biometrics

Related links

- Authenticating with PingID using iOS or iPadOS biometrics

Using Android biometrics for authentication with PingID

If your Android device supports FIDO2 biometrics, you can use the built-in biometrics in your Android to authenticate with PingID for a secure sign-on experience. To set up your Android device for secure authentication with PingID, you need to register or 'pair' it with your account.

You can use Android biometrics to access your account or apps using a web browser.

Note

PingID mobile app using biometrics (fingerprint, face, or iris authentication) and Biometric web authentication for Android are different methods of authentication:

- PingID mobile app: Allows you to authenticate when accessing your account from various different devices. Requires you to install PingID mobile app on your mobile device and to pair it with your account.
- Biometrics authentication: Allows you to authenticate using your Android device's built-in biometrics, when signing on to your account without downloading an app. You can only sign on to your account from the same device with which you want to authenticate.

Web only

Pairing your Android biometrics device

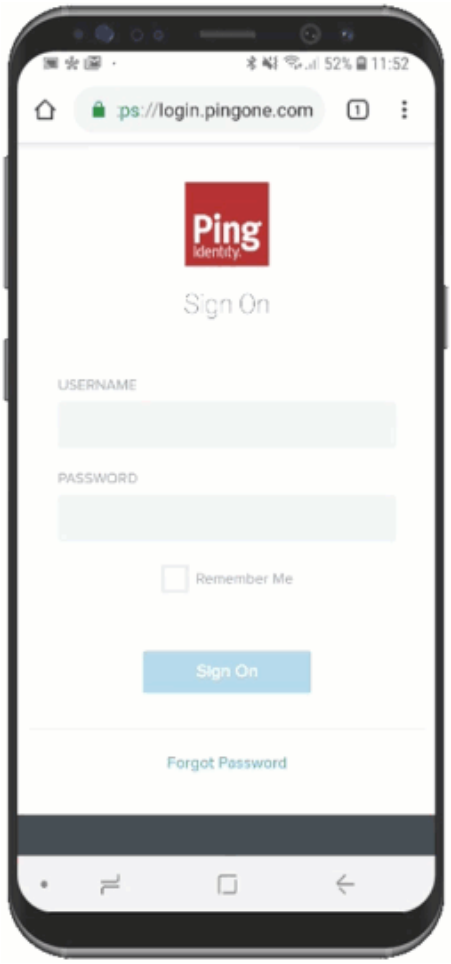
To set up biometrics authentication on your Android, you need to register or 'pair' your device with PingID.

Before you begin

You'll need to:

- Make sure your device supports FIDO2 biometrics.
- Set up biometric authentication on your accessing device (such as registering your fingerprints). Follow the manufacturer's guidelines to do so.
- Ensure you are using a browser that supports the use of FIDO2 biometrics, such as Google Chrome or Microsoft Edge, and that you have the latest version of the browser.

Follow the instructions below to set up biometrics authentication on your device. The following example is for Android devices.

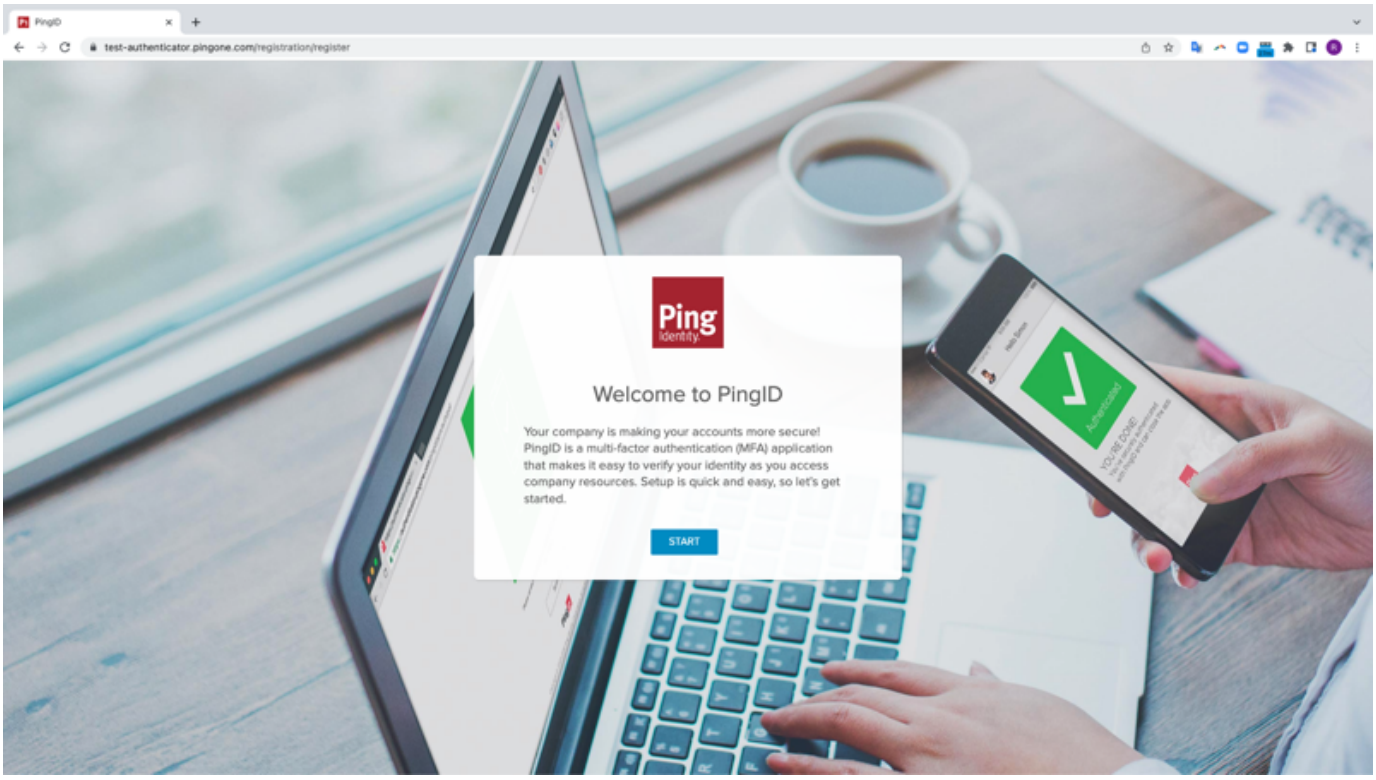


About this task

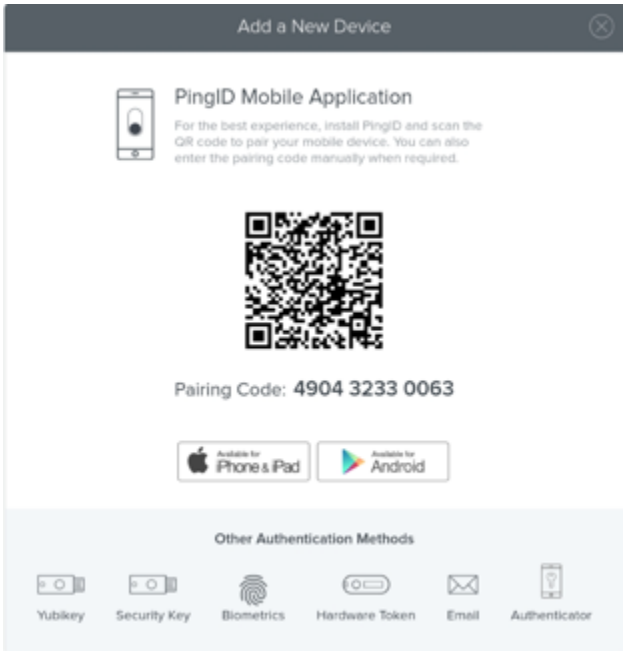
To set up biometrics authentication on your device:

Steps

1. From your Android biometrics device, sign on to your account or app, and when you see the registration window, click **Start**.



You'll see the **Add a New Device** window showing the biometrics icon.

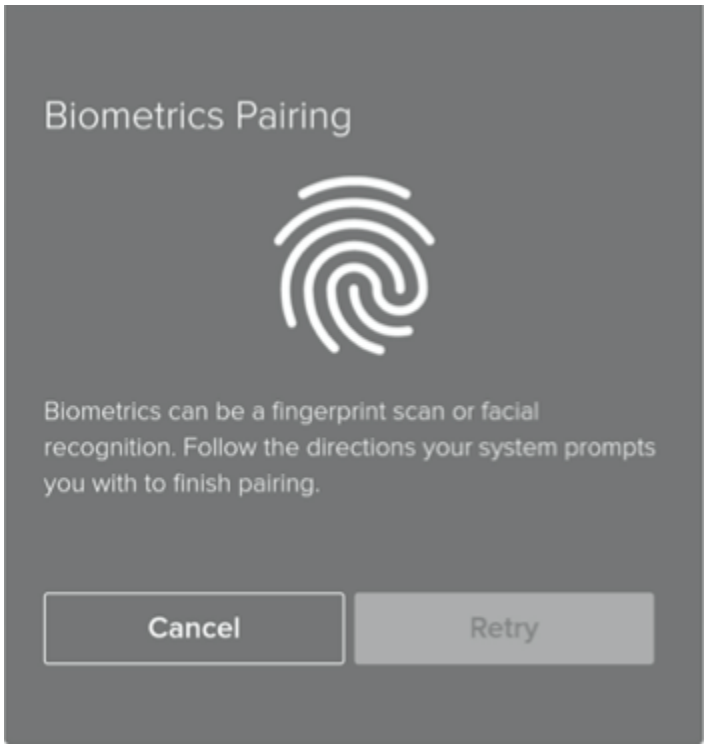


2. In the **Add a New Device** window, click **Biometrics**.

> **Tip**
>
> Tap **Authenticate using Face ID**, even if your device only supports fingerprint authentication. You will be able to authenticate using your fingerprint.

Result:

You'll see a window prompting you to authenticate using your biometrics device.



3. In the **Alternative Authentication** popup window, select **Authenticate using biometrics** (for Android/other devices). You are prompted to authenticate using your biometrics device.
4. Use your biometrics device to validate your identity (fingerprint or Face ID).

> **Note**
>
> - Make sure the **Alternative Authentication** browser window is the active window.
> - If you see a popup message asking if you permit your device to communicate with the biometrics device, select **Allow** or **Yes** to continue. The popup message may differ depending on the browser you are using.

Result:

You'll see a green checkmark indicating your device has been paired successfully, and you are automatically signed on to your account or app.

5. The next time you want to sign on to your account or application, follow the prompt to authenticate using your biometrics device.

For more information, see Authenticating with PingID using an Android biometrics.

Related links

- Troubleshooting FIDO2 biometrics for Android

Related links

- Authenticating with PingID using an Android biometrics

Using a security key (FIDO2) for authentication with PingID

You can use a FIDO2 security key for secure authentication with PingID. To set up your security key for secure authentication with PingID, you need to register or 'pair' it with your account.

Pairing creates a trust between the security key and your account, so you can use it to authenticate during the sign-on process.

After you have paired your account successfully, you can use a security key to access your account using a Web browser or to access a Windows login machine. If you do not have internet access or a network connection when accessing through Windows login, if you have authenticated successfully online at least once, you can also use a security key to authenticate manually when offline.

Web or Windows login

Pairing your security key

Register or 'pair' your security key so that you can use it to authenticate with PingID.

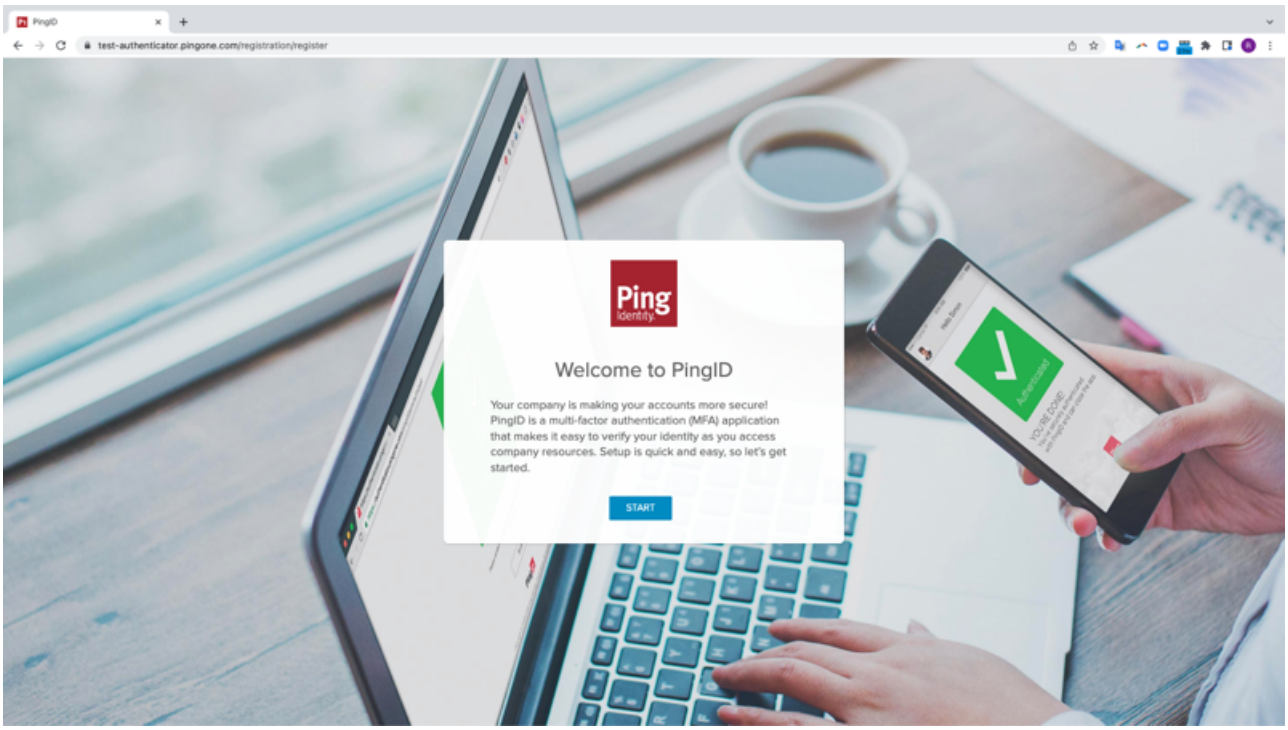
Before you begin

- Ensure you are using a browser that supports the use of a security key, such as Google Chrome or Firefox, and that you have the latest version of the browser.
- If you are pairing the security key using a mobile device, the mobile device must be running either:
  - Android devices: Android 7 or later
  - iOS devices: iOS 13.3 or later
- If your security key uses biometrics, such as your fingerprint to authenticate, set it up according to the security key manufacturer's guidelines.
- If you are using a virtual machine (VM) to connect to your accessing device and want to pair your security key, ensure your VM is configured to recognize a USB device.

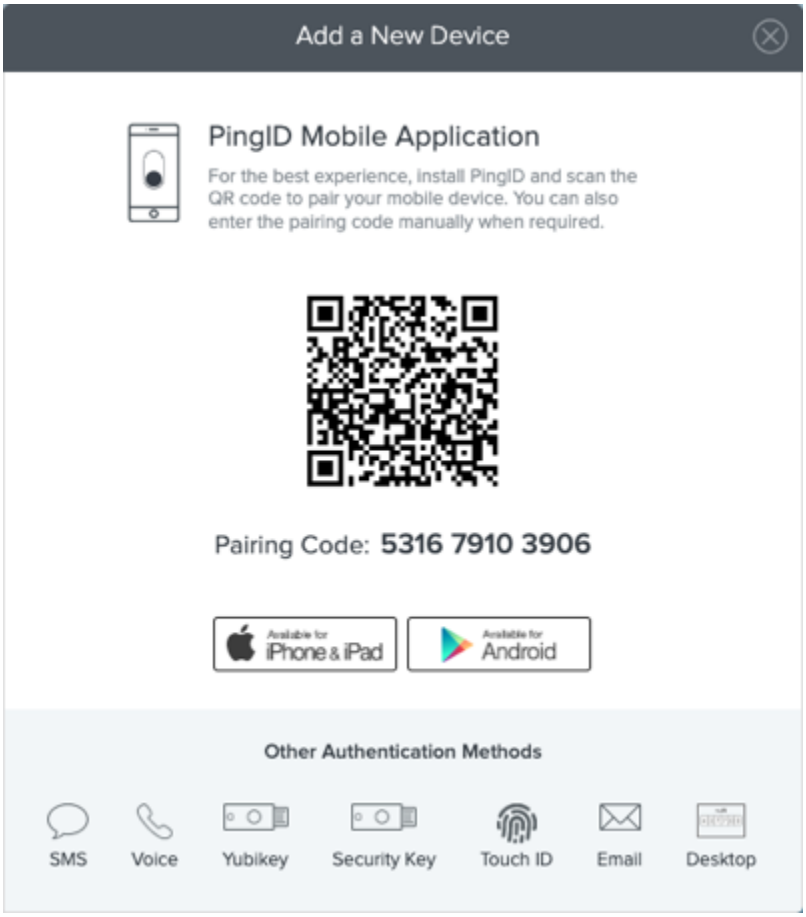
> **Note**
>
> After you have paired your device, and authenticated successfully, you can also use it to authenticate for Windows login, if required.

Steps

1. Sign on to your account or app and when you see the registration window, click **Start**.



You'll see the **Add a New Device** window, showing the security key icon.

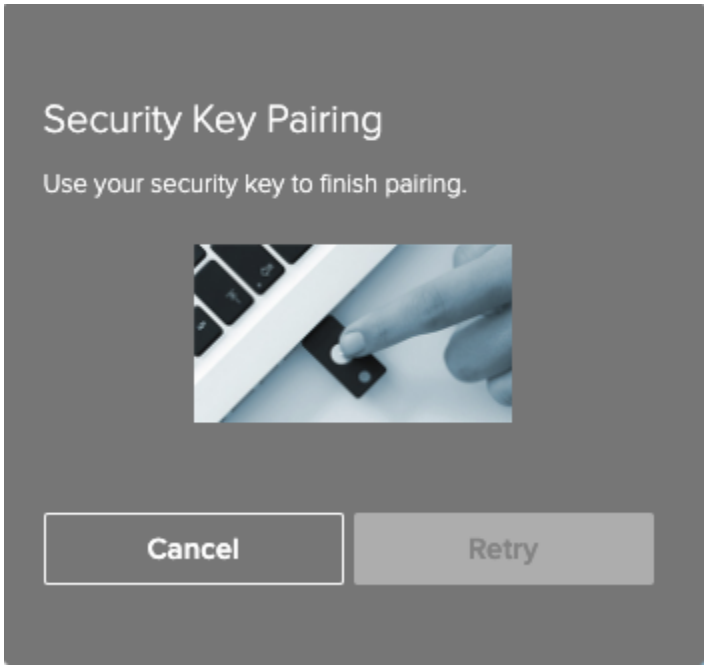


2. In the **Add a New Device** window, click **Security Key**.

> **Tip**
>
> Tap **Authenticate using Face ID**, even if your device only supports fingerprint authentication. You will be able to authenticate using your fingerprint.

Result:

A window appears and prompts you to authenticate with your security key.



3. Use your security key to authenticate.

   > **Note**
   >
   > - Make sure the **Alternative Authentication** browser window is the active window.
   > - If you see a message asking if you permit your device to communicate with the security key, select **Allow** or **Yes** to continue. The message might vary depending on your browser.

   Result:

   A green **Authenticated** message with a check mark appears, indicating your device has been paired successfully, and you are automatically signed into your account or app.

4. The next time you sign on to your account or application, follow the prompt to authenticate using your biometrics device.

   For more information, see Authenticating with PingID using a security key.

Using an authenticator app for authentication with PingID

PingID allows you to use an external authenticator app of your choice, such as the Google authenticator app or the Microsoft authenticator app, to access your account with the added security of multi-factor authentication. To set up your authenticator app for secure authentication with PingID, you need to download the authenticator app and then register or 'pair' it with your account.

Pairing creates a trust between your authenticator app and your account so that you can use it to authenticate during the sign-on process. This section describes how to pair your authenticator app with PingID.

You can use an authenticator app to access your account using a Web browser, to access your company's VPN, or to access a Mac login machine.

Web or Mac

Pairing your authenticator app

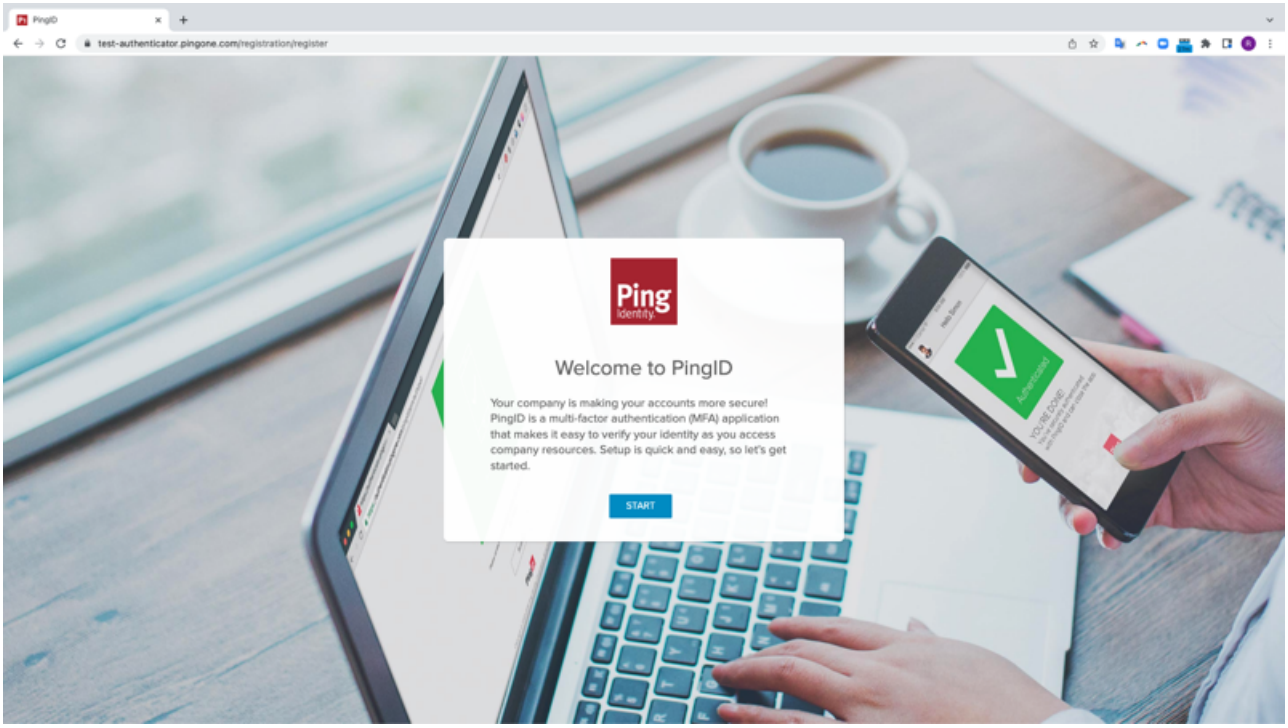
Download an authenticator app and then register or 'pair' it with your account so that you can use it to authenticate with PingID.

Before you begin

Download and install the authenticator app that you want to use, such as Google Authenticator.

Steps

1. On your mobile device, download and install the authenticator app that you want to use, such as Google Authenticator.
2. Sign on to your account or app and when you see the registration window, click **Start**.



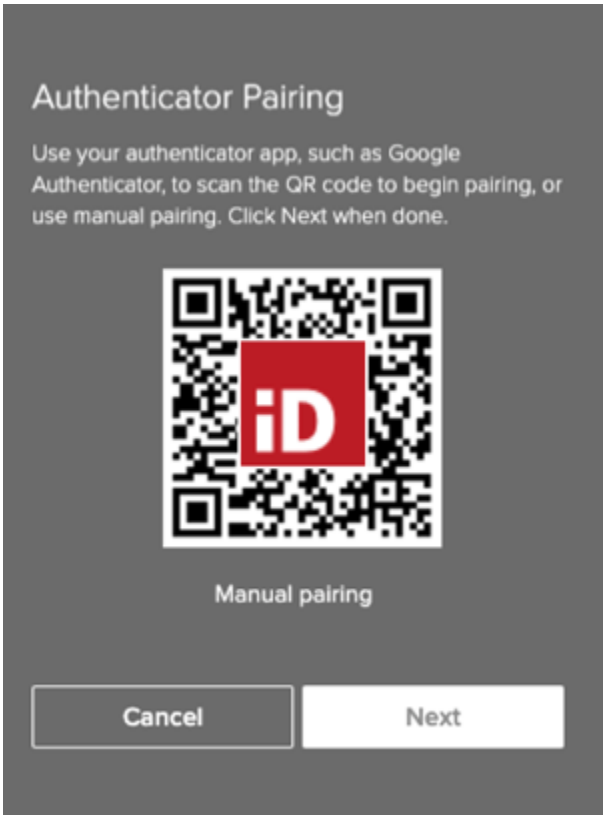
You'll see the **Add a New Device** window showing the **Authenticator** icon.

3. In the **Add a New Device** window, click **Authenticator**.

> **Tip**
>
> Tap **Authenticate using Face ID**, even if your device only supports fingerprint authentication. You will be able to authenticate using your fingerprint.

Result:

The **Authenticator Pairing** window appears, showing the QR **Pairing Code**.



4. Open the authenticator app:

> **Note**
>
> The steps might vary depending on the authenticator app you choose.

   1. Create or add a new account.
   2. Accept all permissions, if prompted, such as permission for the app to access your camera. Check the help files for your specific authenticator if needed.
   3. From the authenticator app on your device, point your device at the QR code on your browser and scan it.

      > **Note**
      >
      > If you are unable to scan the QR code, on your mobile device tap **Manual Pairing**, referred to as a code or provided key, and enter the pairing key shown on the registration page.

      Result:

      A confirmation message appears on your authenticator app telling you that your account was added successfully and displays a new entry showing your account name and a one-time passcode (OTP).

5. In your browser, click **Next**, enter the OTP displayed on your authenticator app, and click **Verify**.

> **Note**
>
> The passcode updates approximately every 30 seconds, and you can use it only one time.
> A screen capture of the Verification window for the user to enter the OTP.

Result:

After you authenticate, a green check mark appears confirming authentication, and you are redirected to the company protected browser-based service or app that you need to access.

6. The next time you sign on to your account or app, authenticate using the OTP generated by your authentication app.

Next steps

For information about how to authenticate with your authenticator app, see Authenticating with PingID using an authenticator app.

VPN

Pairing your authentication app (VPN)

Download an authenticator app and then register or 'pair' it with your account so that you can use it to securely access your VPN with PingID.

Before you begin

Download and install the authenticator app that you want to use, such as Google Authenticator.

Steps

1. From your web browser or application:
    1. Sign on to your VPN with your username and password.
    2. When prompted, install the PingID app.
    3. In the **Response** field, enter `other`. Click **Sign In**.
    4. To set up your authenticator app, in the **Response** field, enter `authenticator`. Click **Sign In**.

    Result:

    A pairing key generates and displays on-screen.
2. Open your authenticator app.

    > **Note**
    >
    > Depending on the authenticator app you choose, the steps might vary.

    1. Create a new account and accept all permissions, if prompted.
    2. Tap the option to enter a manual code, also called a code or provided key.
    3. Enter the pairing key provided in step 1.

    Result:

    A confirmation message displays on your authenticator app confirming your account is added successfully. A new entry appears showing your account name and a one-time passcode (OTP).
3. On your web browser or application, in the **Response** field, enter the OTP. Click **Sign In**.

    Result:

    Pairing and authentication are complete, and you are signed on to your VPN.

Next steps

For more information about how to authenticate with your authenticator app, see Authenticating with PingID using an authenticator app.

Related links

- Authenticating with PingID using an authenticator app

Using a YubiKey (OTP) for authentication with PingID

You can use a YubiKey for secure authentication with PingID. To set up your YubiKey, you need to register or 'pair' it with your account.

> **Note**
>
> The option to pair your account with this device type is defined by your company policy.

Before you can start using your YubiKey to authenticate, you need to register or 'pair' it with your account. Pairing creates a trust between the YubiKey and your account so that you can use the YubiKey to authenticate during the sign-on process.

You can use a YubiKey to access your account using a web browser, to access your company's VPN, or to access a Windows login or Mac login machine. For Mac login, you must register your YubiKey through the web to use it to access your Mac Login machine.

> **Note**
>
> - This section details how to use your YubiKey OTP for authentication with PingID. It is also possible to pair some types of YubiKey as a security key for the added security benefits of FIDO2 authentication. If you're not sure whether to pair your device as a YubiKey or a security key, then check with your organization's helpdesk representative before you pair it.
> - See https://www.yubico.com/products/yubikey-hardware/compare-yubikeys/ for a list compatible YubiKey models.

Web

Pairing your YubiKey

Register or 'pair' your YubiKey hardware token, so you can use it to authenticate with PingID.

Before you begin

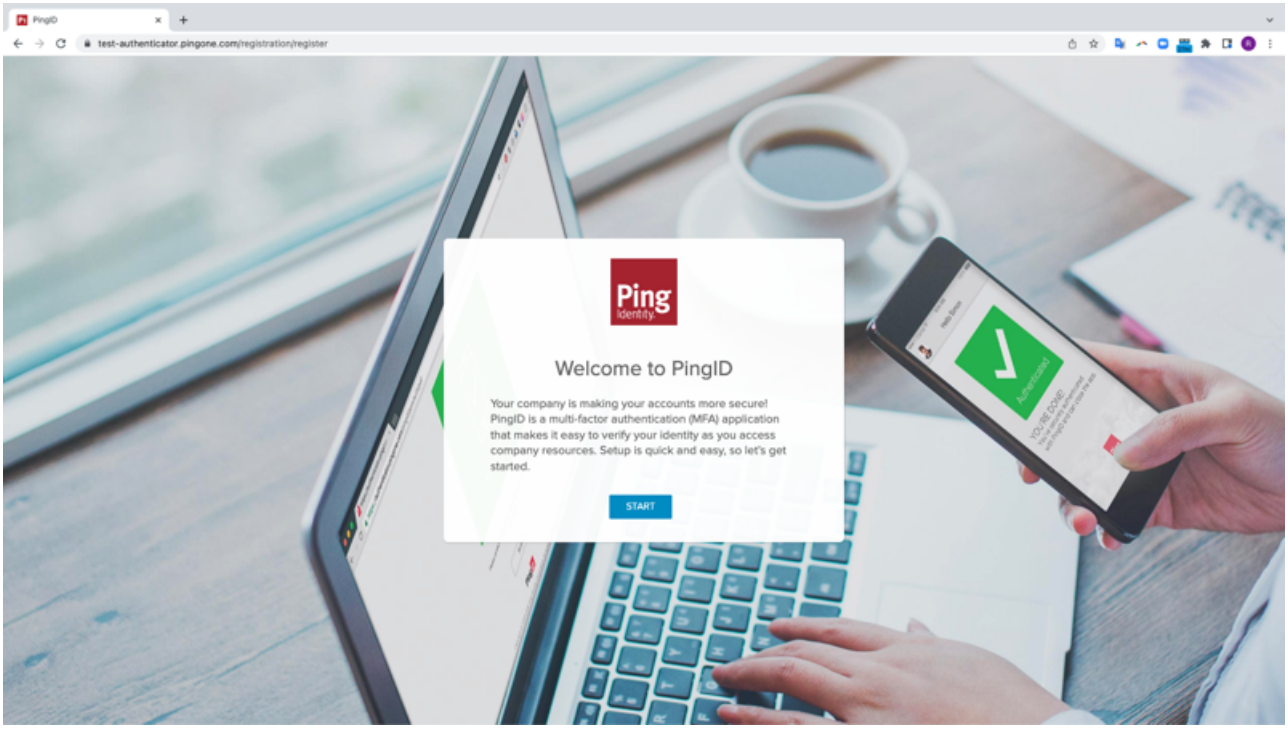
If you are using a virtual machine (VM) to connect to your accessing device, and you need to pair your YubiKey, configure your VM to recognize a USB device.

About this task

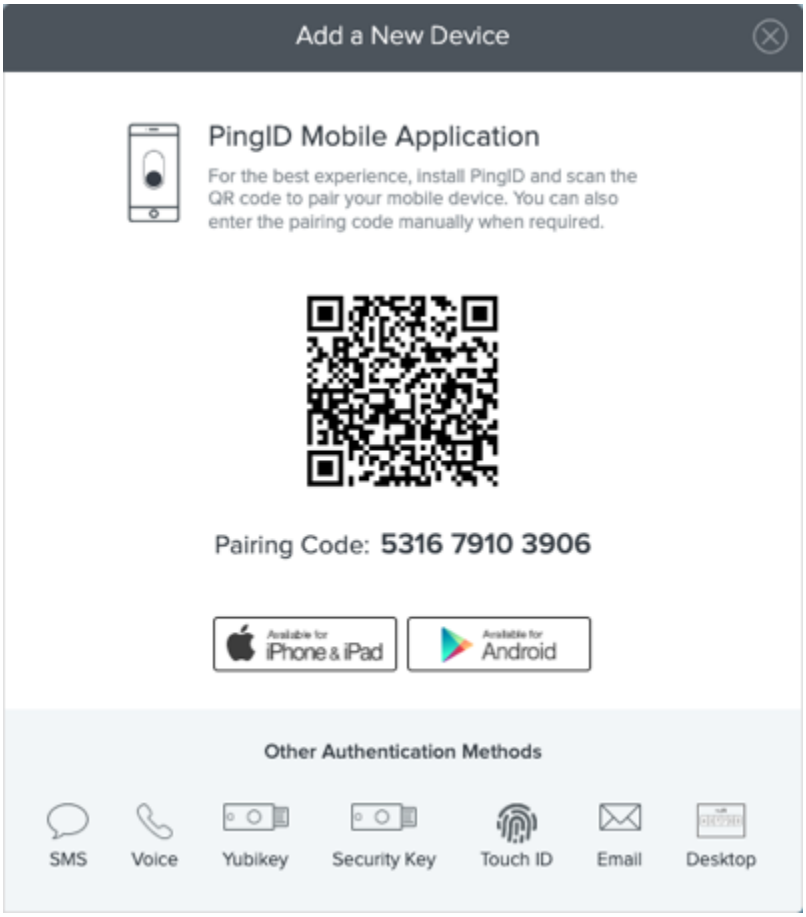
> **Note**
>
> After you have paired your device and authenticated successfully, you can also use it to authenticate for Windows login or Mac login, if required.

Steps

1. Sign on to your account or app, and when you see the registration window, click **Start**.



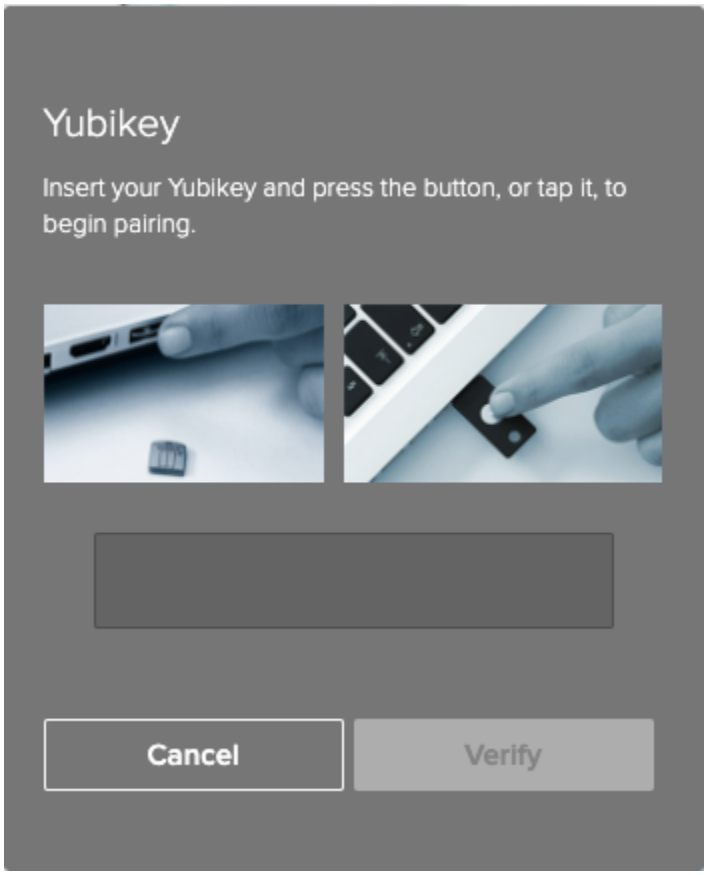
You'll see the **Add a New Device** window, showing the YubiKey icon.



2. In the **Add a New Device** window, click **YubiKey**.

   Result:

   You are prompted to authenticate with your YubiKey.



3. Insert the YubiKey into your computer USB port, make sure the **Alternative Authentication** window is the active window on your machine, and then tap the YubiKey.

> **Note**
>
> If you are using a YubiKey Neo and need to register using a browser on your mobile device through NFC, the process is different. To complete the registration process:
>
> 1. Download the YubiClip application to your mobile device and enable NFC.
> 2. Place the YubiKey next to your mobile device. The verification code is copied to the device clipboard.
> 3. Paste the code into the YubiKey authentication field in your browser, and tap **Verify**.

Result:

A one-time passcode (OTP) automatically generates and enters into the **YubiKey Setup** window. **Verify** is selected automatically, and a green check mark appears, indicating the pairing request is successful. You are automatically signed on to your account or app.

Next steps

The next time you sign on to your account or application, you'll be able to use your YubiKey to authenticate. For more information, see Authenticating with PingID using a YubiKey.

VPN

Pairing your YubiKey (VPN)

Register or 'pair' your YubiKey hardware token so that you can use it to securely access your company's VPN with PingID.

About this task

To set up your YubiKey on your VPN:

Steps

1. From your web browser or application, sign on to your VPN and enter your username and password.
2. Enter `other`. Click **Sign In**.
3. In the blank field, enter `YubiKey`. Click **Sign In**.
4. Insert your YubiKey into the USB port on your machine.
5. Click the **text** field to ensure your mouse cursor is placed in the field. Tap the YubiKey.

   Result:

   The YubiKey one-time passcode (OTP) is automatically entered into the text entry field.
6. Click **Sign In**.

Next steps

The next time you sign on to your account or application, you'll be able to use your YubiKey to authenticate. For more information, see Authenticating with PingID using a YubiKey.

Windows login

Pairing your YubiKey (Windows login)

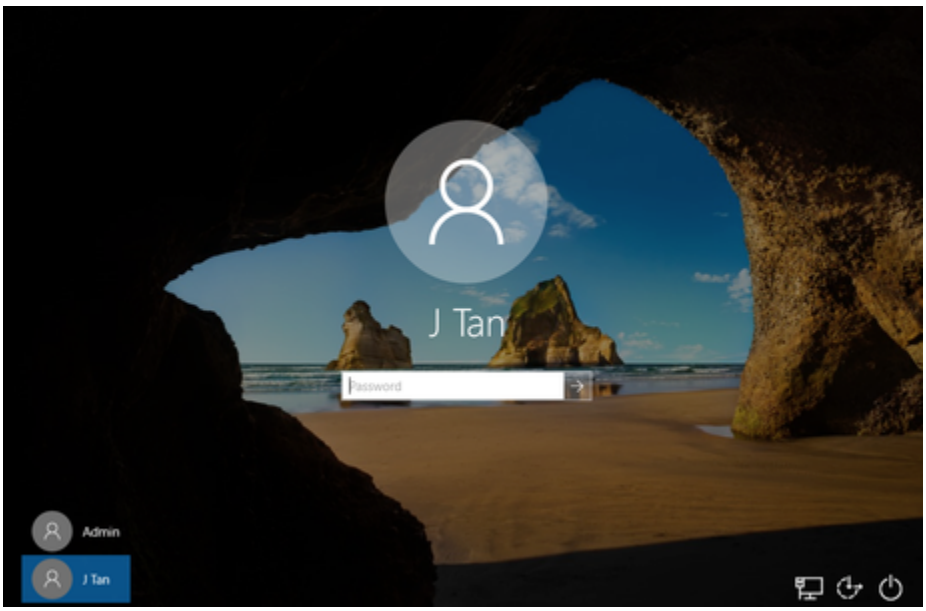
Register or 'pair' your YubiKey hardware token so that you can use it to access your Windows login machine securely with PingID.

About this task

> **Note**
>
> If you are accessing Windows login through a virtual machine (VM), before pairing your YubiKey, make sure your VM is configured to recognize a USB device.

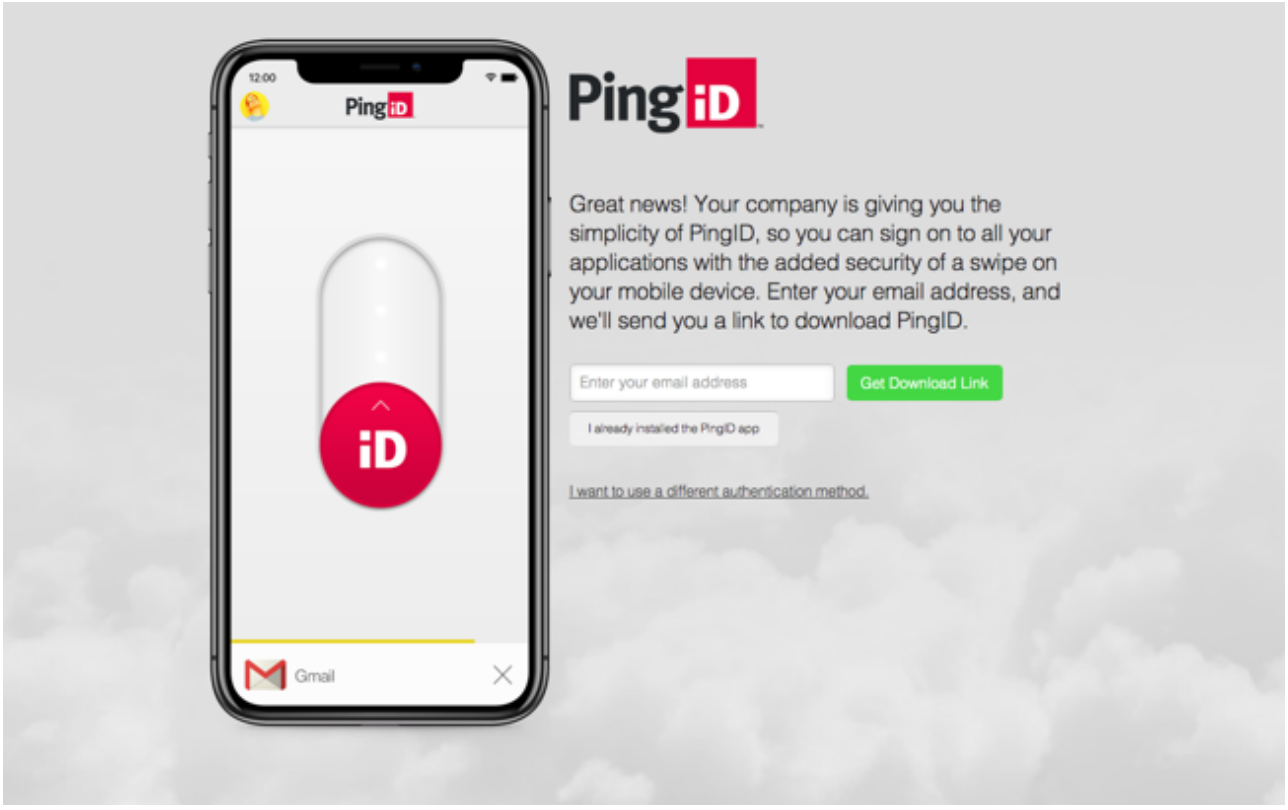
Steps

1. Sign on to your Windows machine.



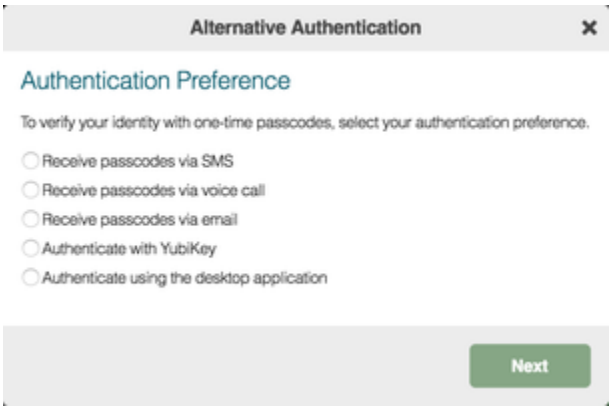
Result:

The PingID registration window displays.



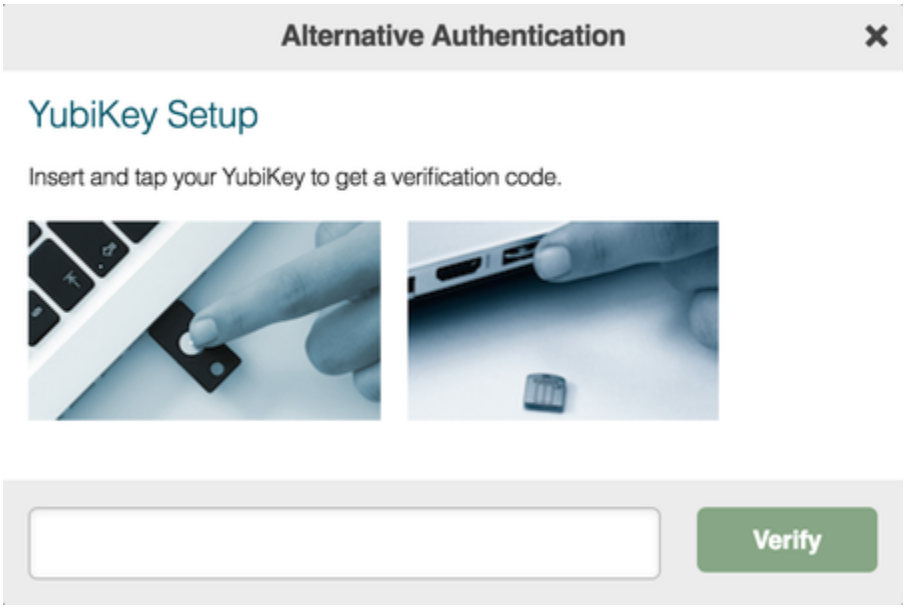
> **Note**
>
> Until you have successfully completed the registration process, you cannot minimize the PingID registration window. If you close the window, you are automatically redirected back to the sign-on page.

2. Click **I want to use a different authentication method**.
3. In the**Alternative Authentication** window, select **Authenticate with YubiKey**. Click **Next**.



Result:

The **Alternative Authentication** window displays, prompting your **YubiKey Setup** and verification.



4. Insert the YubiKey into your computer USB port. Tap the YubiKey.

> **Note**
>
> Make sure that the **Alternative Authentication** window is the active window on your machine.

Result:

A one-time passcode (OTP) is automatically generated and inserted into the **YubiKey Setup** window, and **Verify** is selected automatically.

5. The next time you sign on to your Windows machine, account, or app:
    1. Enter a YubiKey OTP.
    2. Press your YubiKey button to generate the OTP.
    3. Click **Sign On** to authenticate and sign on.

Result

The green **Authenticated** message appears with a check mark, indicating that authentication is successful. You are signed on to your Windows machine.

Next steps

The next time you sign on to your account or application, you'll be able to use your YubiKey to authenticate. For more information, see Authenticating with PingID using a YubiKey.

Related links

- Authenticating with PingID using a YubiKey

Using SMS or voice authentication with PingID

You need to register or 'pair' your mobile device with your account so that you can receive a one-time passcode (OTP) to your device by SMS or voice call, and use it to authenticate securely with PingID.

Pairing a device creates a trust between your device and your account so that you can use your device to authenticate during the sign-on process. After you have paired your device, each time you sign on to your account or application, you receive a one-time passcode (OTP) through SMS or voice call with which to authenticate.

You can use SMS or voice calls to access your account using a Web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Note

The option to pair your account with this device type is defined by your company policy.

Web or Mac

Pairing your mobile device for SMS or voice authentication with PingID

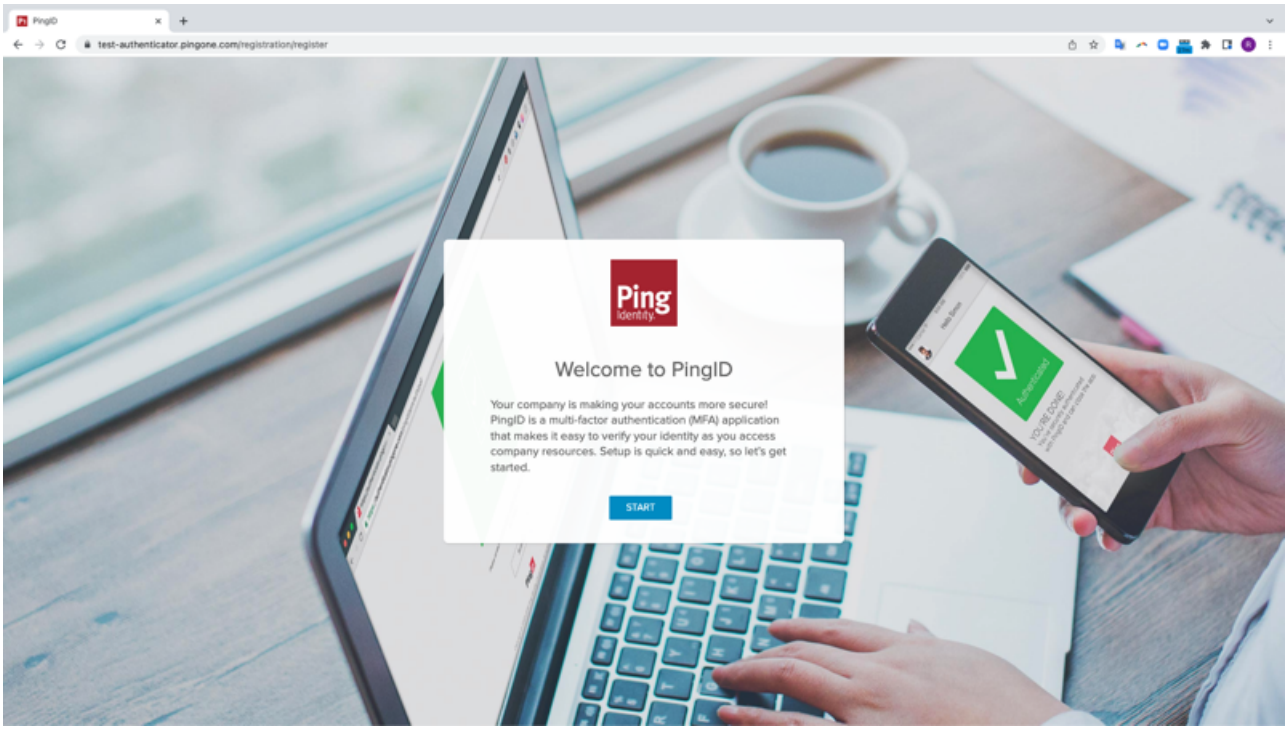
Register or 'pair' your mobile device so that you can receive a one-time passcode (OTP) by SMS or voice call and use it to authenticate securely with PingID.

About this task

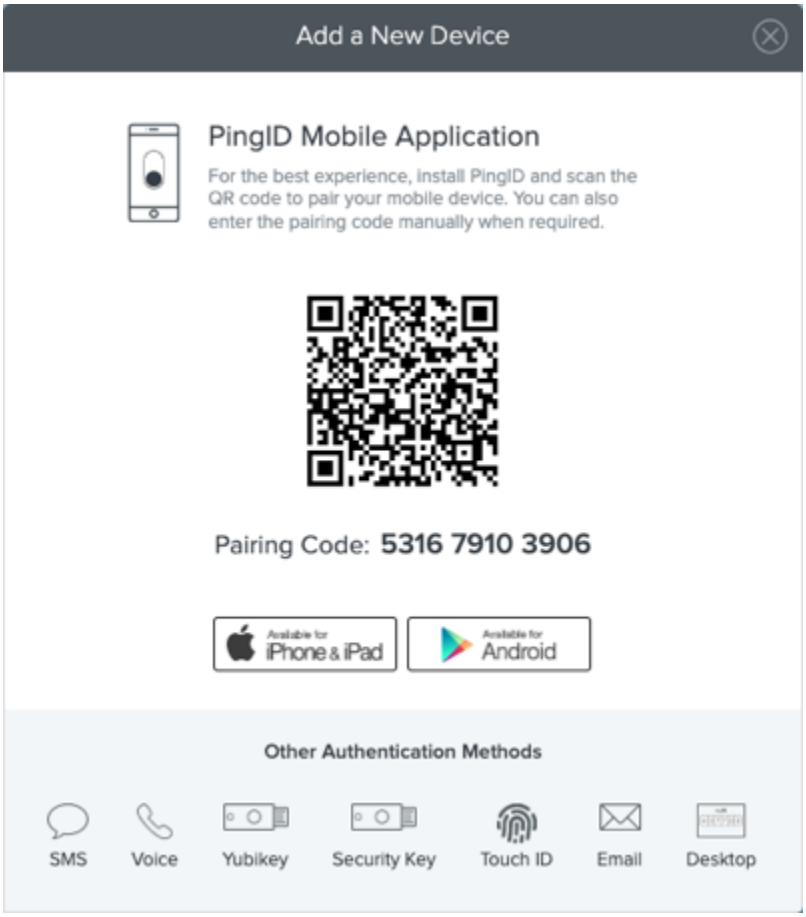
> **Note**
>
> After you have paired your device, and authenticated successfully, you can also use it to authenticate for Windows login or Mac login, if required.

Steps

1. Sign on to your account or app and when you see the registration window, click **Start**.

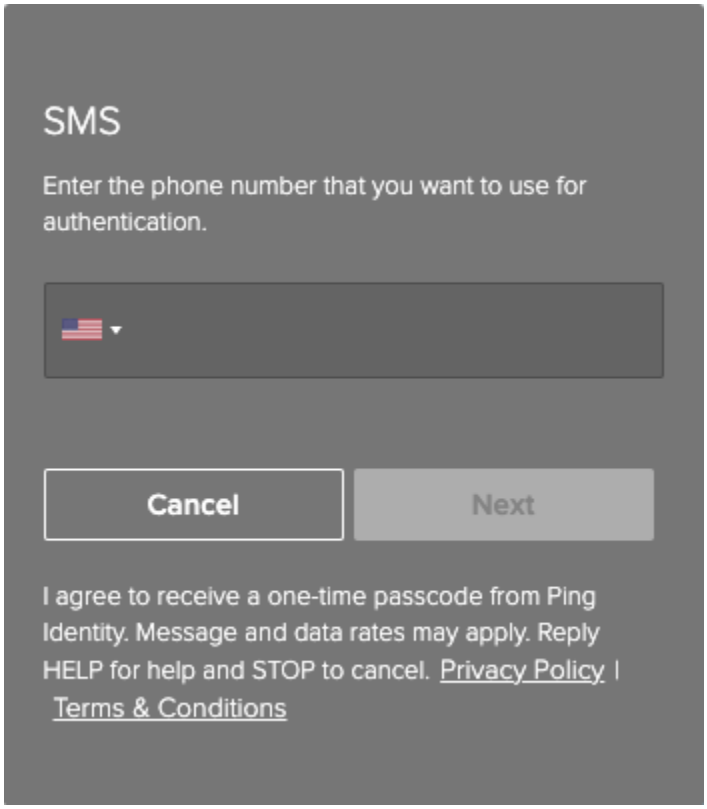


You'll see the **Add a New Device** window, showing the **SMS** and **Voice** icons.



2. In the **Add a New Device** window, click either **SMS** or **Voice**.

3. In the **SMS** window, in the **international country code** list, select your international country code and enter your phone number you want to use to authenticate. Click **Next**.



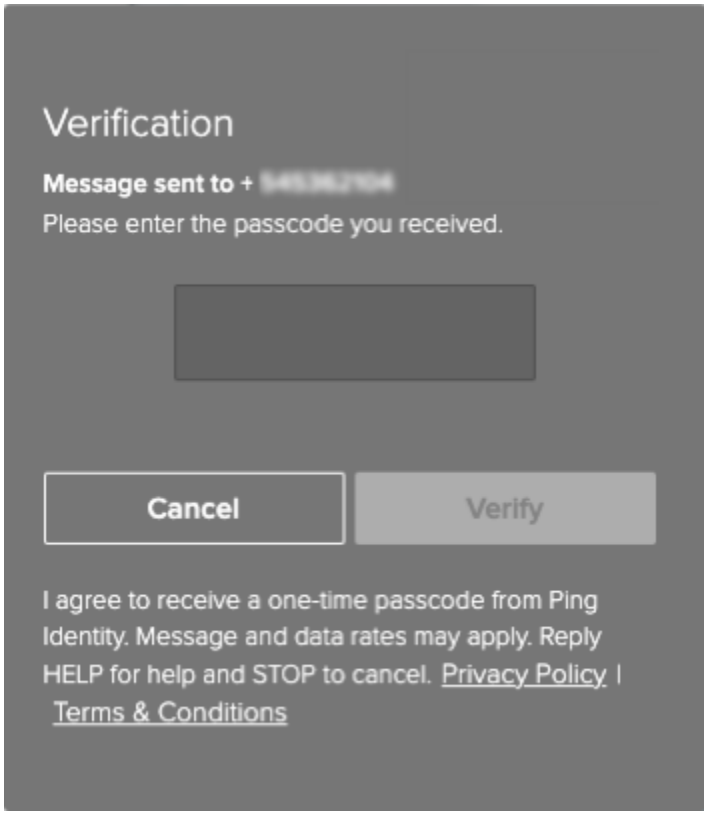
Note

To support voice calls using phone numbers with extensions, enter the phone number followed by a comma and the extension number. Examples include:

- The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
- The extension can include the # or * characters. For example: +12025550123,#2992 or +12025550123,2992#.
- If there is more than one extension, then a comma should separate the extension and the nested extension. For example: +12025550123,#2992,#2991.
- Each comma generates a 2-second pause. After the call is answered, the extension is dialed after two seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional 2-second pause. For example, three commas for a 6-second pause before the nested extension: +12025550123,#2992,,,#2991.

Result:

PingID sends a one-time passcode (OTP) to your mobile through SMS or voice call.



4. In the **Authentication** window, enter the OTP. Click **Verify**.

   Result:

   When successfully verified, the green **Authenticated** message appears, and you are automatically signed on to your account or app.

Next steps

The next time you sign on to your organization dock or application:

1. PingID sends an OTP to your mobile device.
2. In the **Authentication** window, enter the OTP.
3. Click **Sign On** to complete the authentication.

   For information, see Authenticating with PingID using SMS or voice.

VPN

Pairing your mobile device for SMS or voice authentication (VPN)

Register or 'pair' your mobile device so that you can receive a one-time passcode (OTP) by SMS or voice call and use it to access your company's VPN securely with PingID. Pairing a device creates trust between your device and your account so that you can use your device to authenticate during the sign-on process.

About this task

To set up SMS or voice authentication for your VPN:

Steps

1. From your web browser or application, sign on to your VPN with your username and password.
2. Enter `other`. Click **Sign In**.
3. In the text entry field, enter the phone number that you want to use to authenticate:

   Choose from:

   - For SMS: Enter `sms` followed by the country code and your mobile number in the format **sms: 1-4155555555**. Click **Sign In**.
   - For voice: Enter `voice` followed by the country code and your mobile number in the format **voice: 1-4155555555**. Click **Sign In**.

     > **Note**
     >
     > Phone numbers with extensions are supported for voice calls where the phone number is followed by a comma and the extension number. Examples include:
     > - The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
     > - The extension can include the # or * characters. For example: +12025550123, #2992 or +12025550123,2992#.
     > - If there is more than one extension, a comma should separate the extension and the nested extension. For example: +12025550123,#2992,#2991.
     > - Each comma generates a 2-second pause. After the call is answered, the extension is dialed after 2 seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional 2-second pause. For example, three commas for a 6-second pause before the nested extension: +12025550123,#2992,,,#2991.

   Result:

   You receive a one-time passcode (OTP) to your device through either SMS or voice call.
4. In the text entry field, enter the OTP from step 3 and then click **Sign In**.

   Result:

   Your device is paired and authentication complete.

Next steps

The next time you sign on to your VPN, an OTP is sent to your device and in the VPN entry field, you'll be asked to enter the OTP to authenticate. For information, see Authenticating with PingID using SMS or voice.

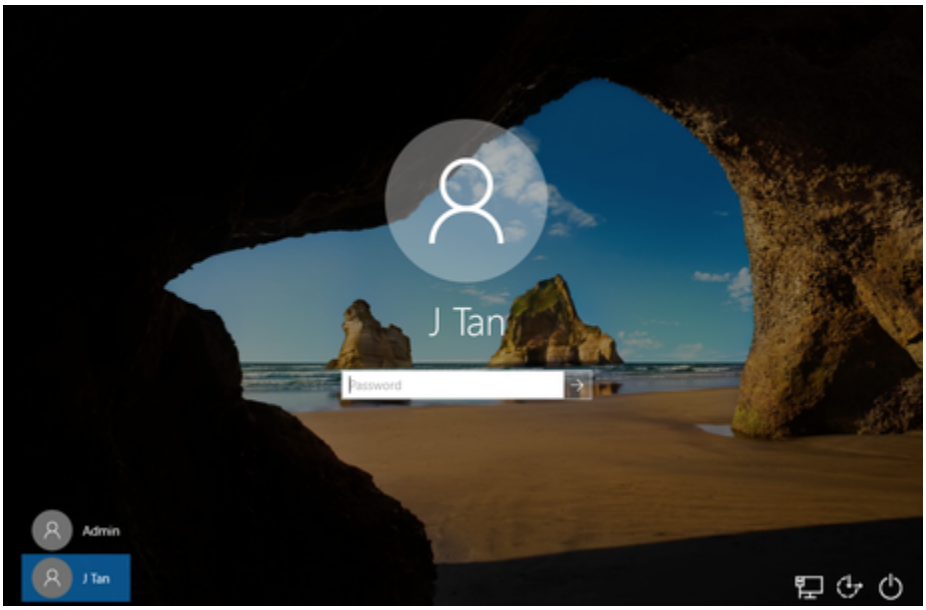
Windows login

Pairing your mobile device for SMS or voice authentication (Windows login)

Register or 'pair' your mobile device so that you can receive a one-time passcode (OTP) by SMS or voice call and use it to access your Windows login machine securely with PingID.

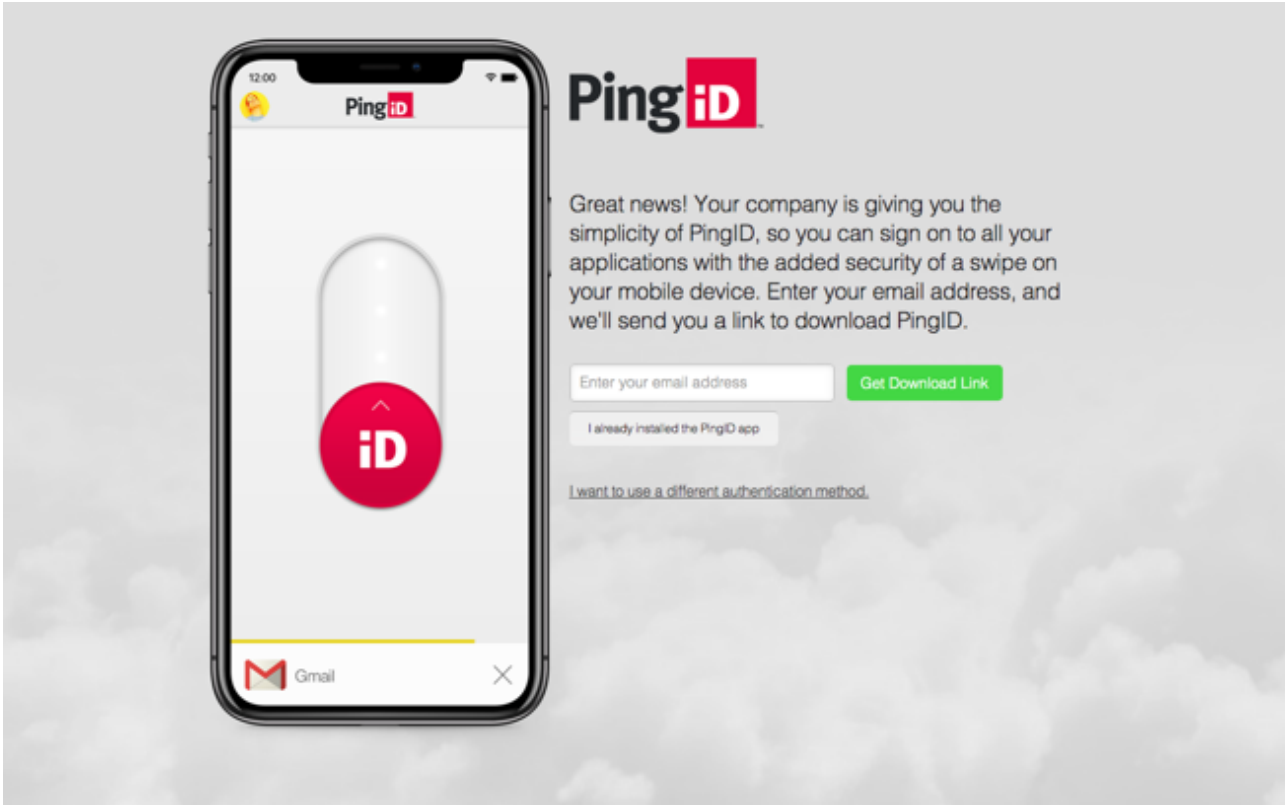
Steps

1. Sign on to your Windows machine.



Result:

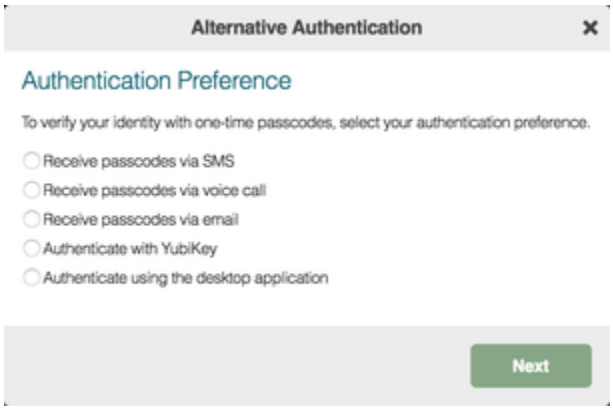
The PingID registration window displays.



> **Note**
>
> Until you successfully complete the registration process, you cannot minimize the PingID registration window. If you close the window, you are automatically redirected back to the Windows login page.

2. Click **I want to use a different authentication method**.
3. In the **Alternative Authentication** window:
    1. Enter your authentication preference, select either **Receive passcodes via SMS** or **Receive passcodes via voice call**.
    2. From the country code list, select the country code.
    3. Enter the phone number that you want to use to authenticate.
    4. Click **Next**.

> **Note**
>
> Phone numbers with extensions are supported for voice calls when the phone number is followed by a comma and the extension number. Examples include:
>
> - The phone number +12025550123 with the extension 2992 is entered as +12025550123,2992.
> - The extension can include the # or * characters. For example: +12025550123,#2992 or +12025550123,2992#.
> - If there is more than one extension, then a comma should separate the extension and the nested extension. For example: +12025550123,#2992,#2991.
> - Each comma generates a 2-second pause. After the call is answered, the extension is dialed after 2 seconds. If a pause is required for longer than 2 seconds, add an additional comma for each additional two-second pause. For example, three commas for a 6-second pause before the nested extension: +12025550123,#2992,,,#2991.



Result:

A one-time passcode (OTP) is sent to your mobile through a SMS or voice call.

4. In the **Authentication** window, enter the passcode into passcode field. Click **Verify**.
5. The next time you sign on to your Windows machine or application:
    1. An OTP sends to your mobile prompting you to enter it in your browser.
    2. Enter the passcode in the **Authentication** window in your browser.
    3. Click **Sign On** to complete the authentication.

Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful. You are signed on to your Windows machine.

Next steps

Next time you sign on to your Windows machine, you'll be able to authenticate using the OTP sent to your mobile device using SMS or Voice. For information, see Authenticating with PingID using SMS or voice.

Related links

- Authenticating with PingID using SMS or voice

Using email for authentication with PingID

Register or 'pair' your email address, so you can receive a one-time passcode (OTP) to your email, and use it to authenticate securely with PingID.

Pairing creates a trust between your email address and your account.

If your company configuration allows it, you can use email to access your account using a Web browser, to access your company's VPN, or to access a Windows login, or Mac login machine.

Note

The option to pair your account with this device type is defined by your company policy.

Web or VPN or Mac

Pairing your email

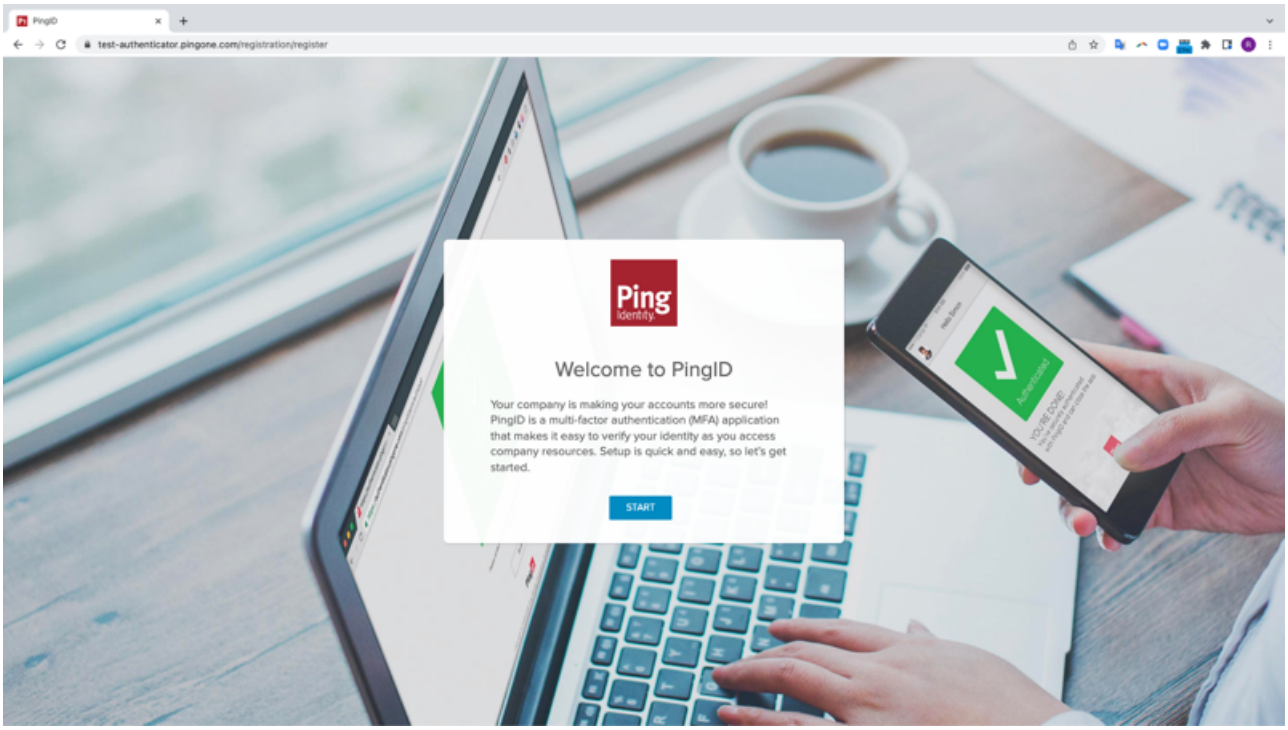
Register or 'pair' your email address from a web browser, so you can receive a one-time passcode (OTP) to your email, and use it to authenticate securely with PingID.

About this task

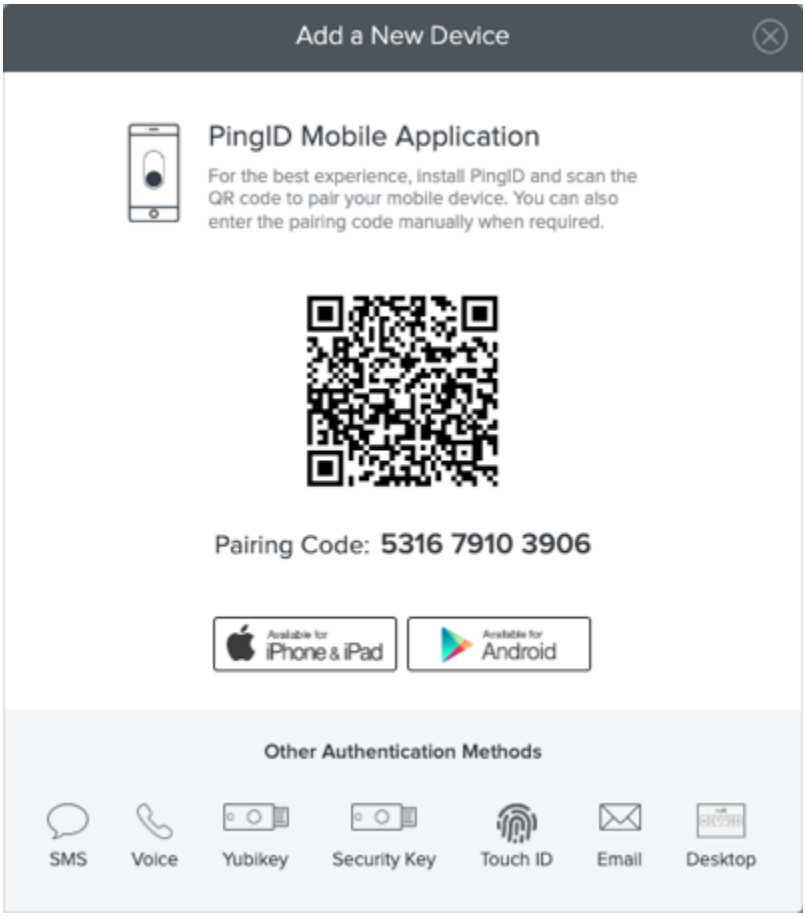
> **Note**
>
> After you have paired your device and authenticated successfully using a web browser, you can also use it to authenticate when accessing your VPN or Mac login machine, if your company allows you to do so.

Steps

1. Sign on to your account or app and when you see the registration window, click **Start**.



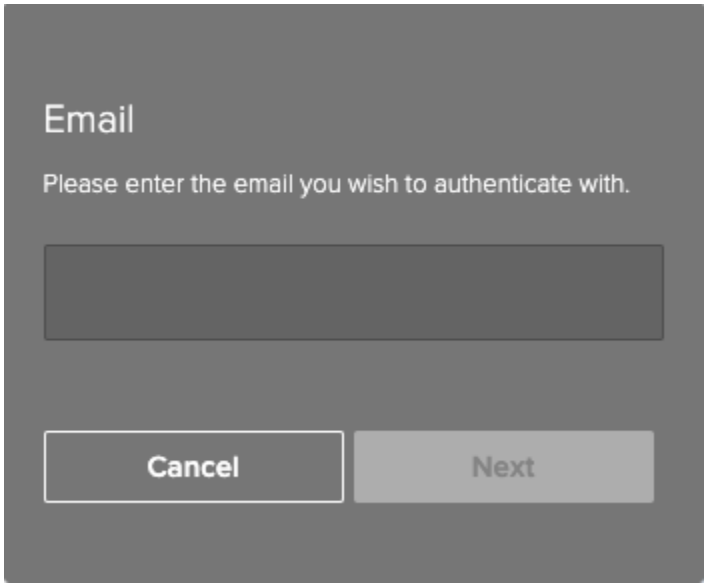
You'll see the **Add a New Device** window, showing the **Email** icon.



2. In the **Add a New Device** window, click **Email**.

   Result:

   You'll see a pop-up window in which you can enter your email address.

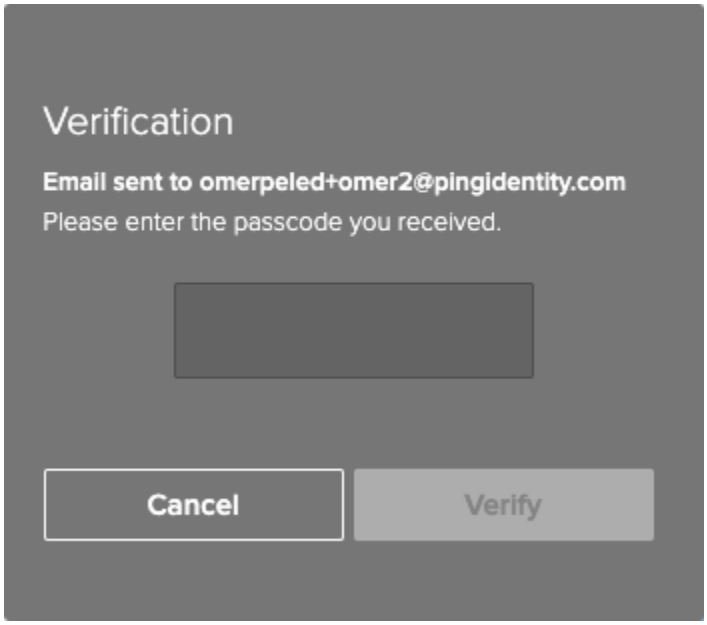


3. Enter your email address, and then click **Next**.

Result:

A one-time passcode (OTP) is sent to the email address you specified.

4. Copy the OTP you received in the PingID email. In your browser, in the **Enter passcode** field, paste or enter the OTP. Click **Verify**.



Result:

After you successfully authenticate, the green **Authenticated** message with a check mark appears. You are automatically signed on to your organization's dock or app.

Result

The next time you sign on to your account or app:

1. You receive an OTP through your email.

2. Enter the OTP.

3. Click **Sign On** to complete the authentication.

Windows login

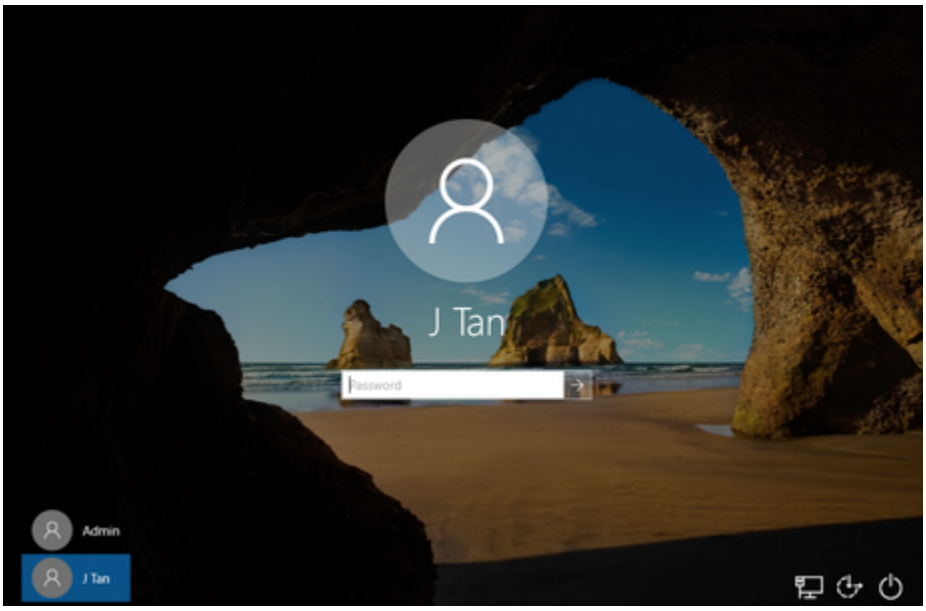
Pairing your email (Windows login)

Register or 'pair' your email address, so you can receive a one-time passcode (OTP) to your email, and use it to securely access your Windows login machine with PingID.

About this task

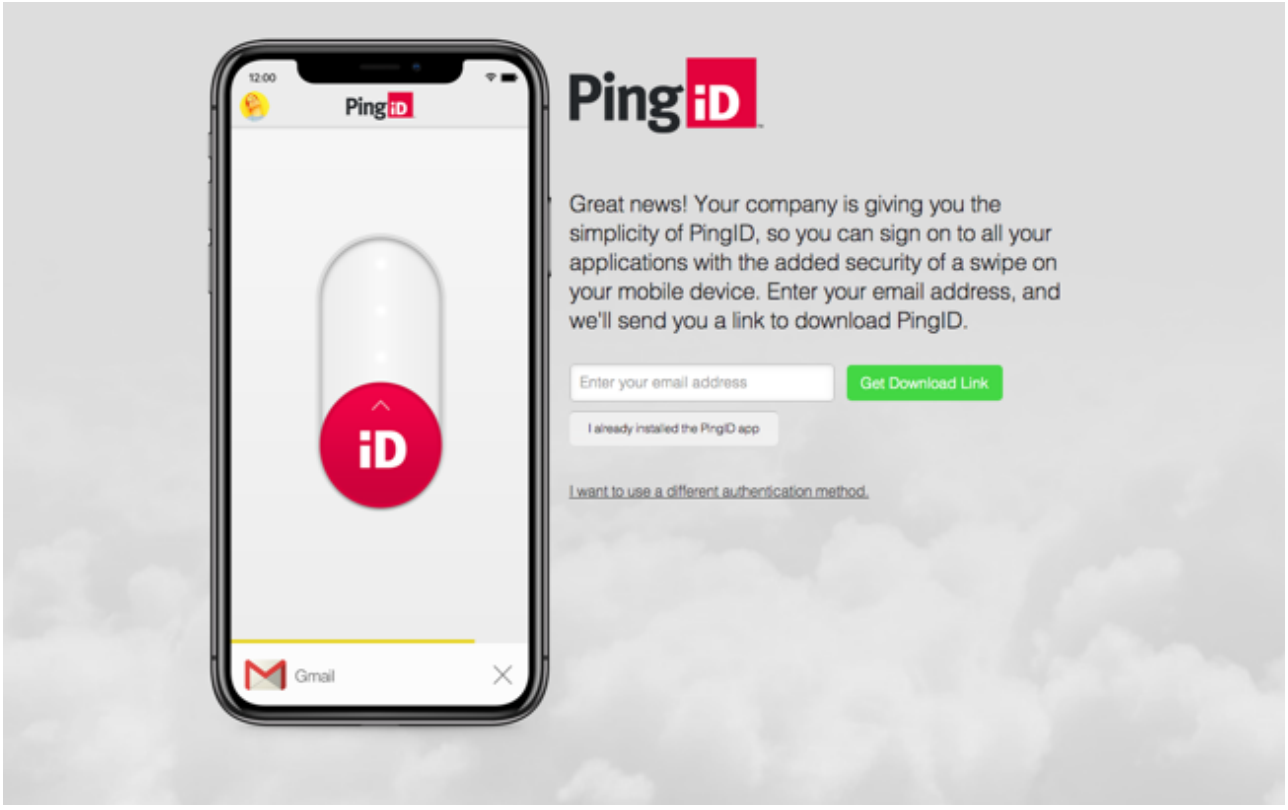
Steps

1. Sign on to your Windows machine.



Result:

The PingID registration window displays.

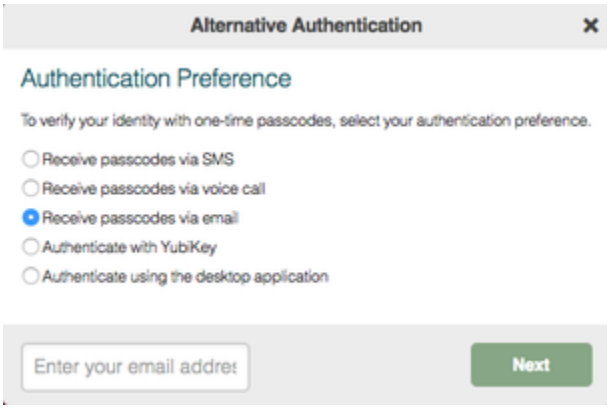


> **Note**
>
> Until you successfully complete the registration process, you cannot minimize the PingID registration window. If you close the window, you are automatically redirected back to the login page.

2. Click **I want to use a different authentication method**.

   Result:

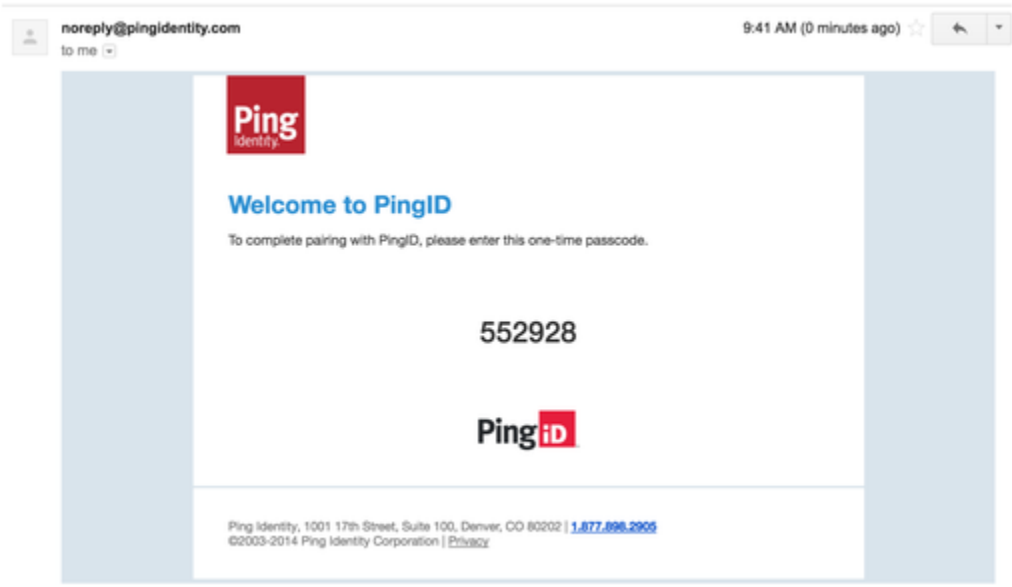
   The **Alternative Authentication** window appears.



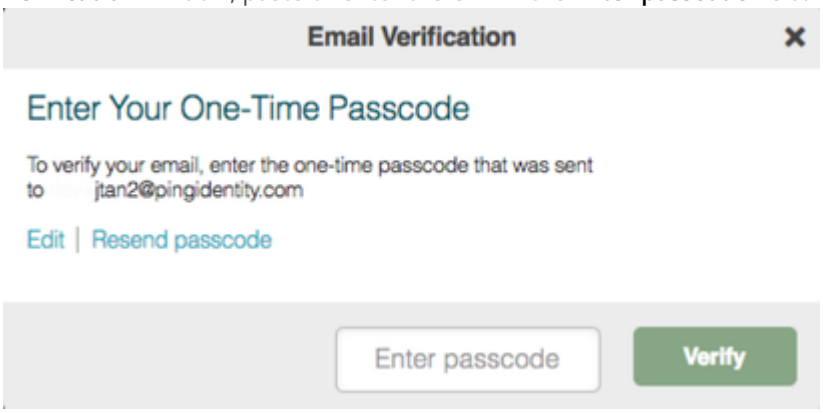
3. Click **Receive passcodes via email** and enter your email address in the **email address** field. Click **Next**.

   Result:

   PingID sends a one-time passcode (OTP) to your specified email address.



4. On a different device, open your email account and copy the OTP from the PingID email. In the Windows **Email Verification** window, paste or enter the OTP in the **Enter passcode** field. Click **Verify**.



Result:

A green **Authenticated** message with a check mark appears, indicating successful authentication. You are automatically signed on to your Windows machine.

5. The next time you sign on to Windows:
    1. You receive a OTP through your email.
    2. Enter the OTP.
    3. Click **Sign On** to authenticate and sign on.

Next steps

You can now authenticate using your email to access your Windows login machine. For information, see Authenticating using email (Windows login).

Related links

- Authenticating with PingID using email

Using a hardware token (OTP) for authentication with PingID

You can use your hardware token to get a one-time passcode (OTP) that you can use for secure authentication with PingID. To set up your hardware token, you need to register or 'pair' it with your account.

Pairing creates a trust between the hardware token and your account so that you can use it to authenticate during the sign on process.

You can use a hardware token to access your account using a Web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Web or Mac

Pairing your hardware token (web)

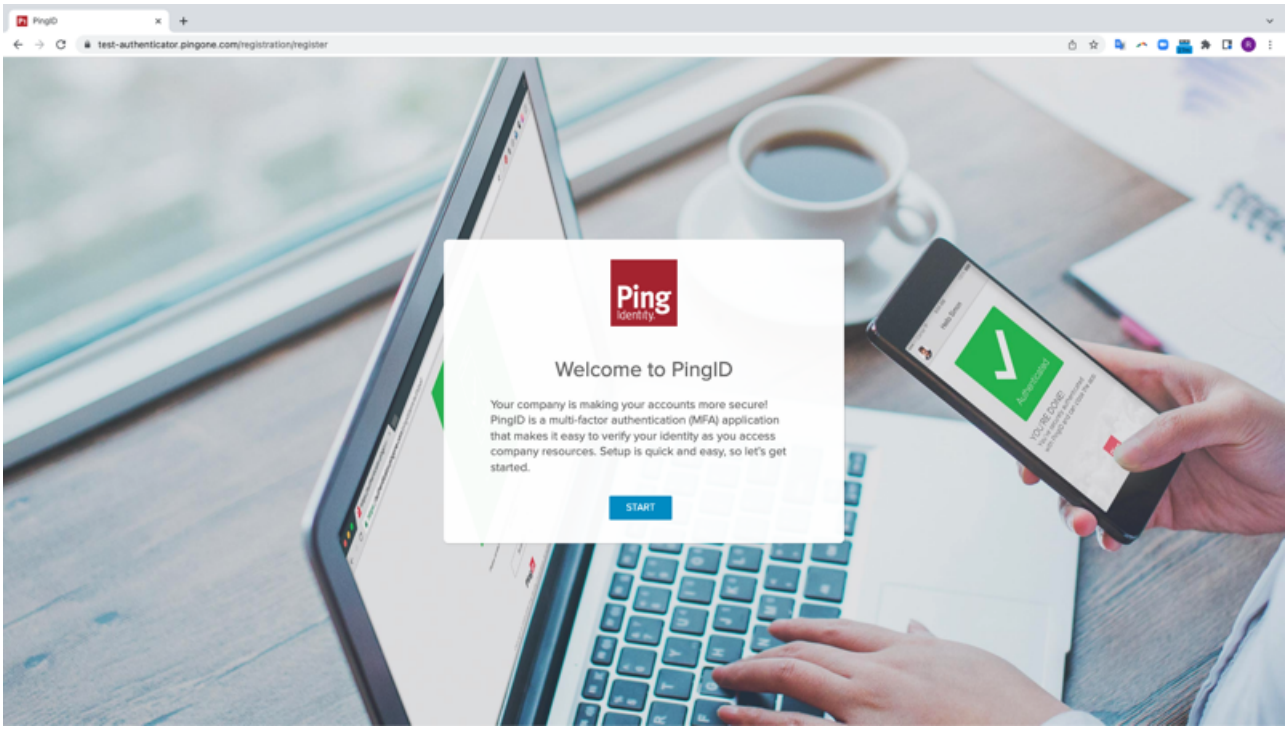
Register or 'pair' your hardware token so that you can generate a one-time passcode (OTP) and use it to authenticate securely with PingID when accessing your account or app from a web browser.

About this task

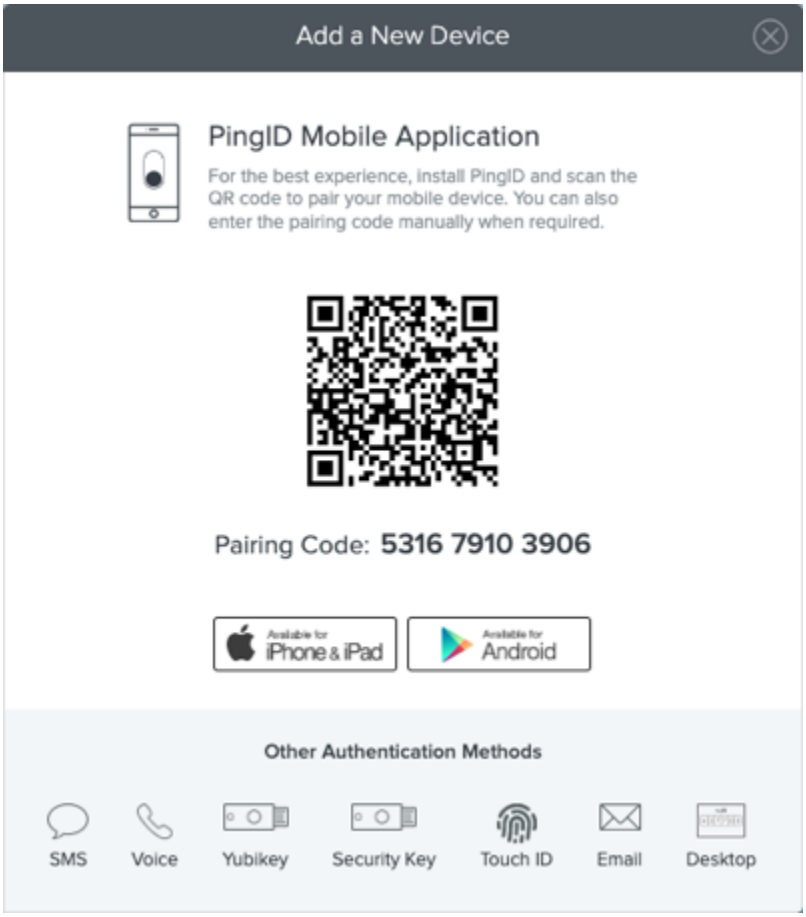
> **Note**
>
> After you have paired your device and authenticated successfully, you can also use it to authenticate for Windows login or Mac login, if required.

Steps

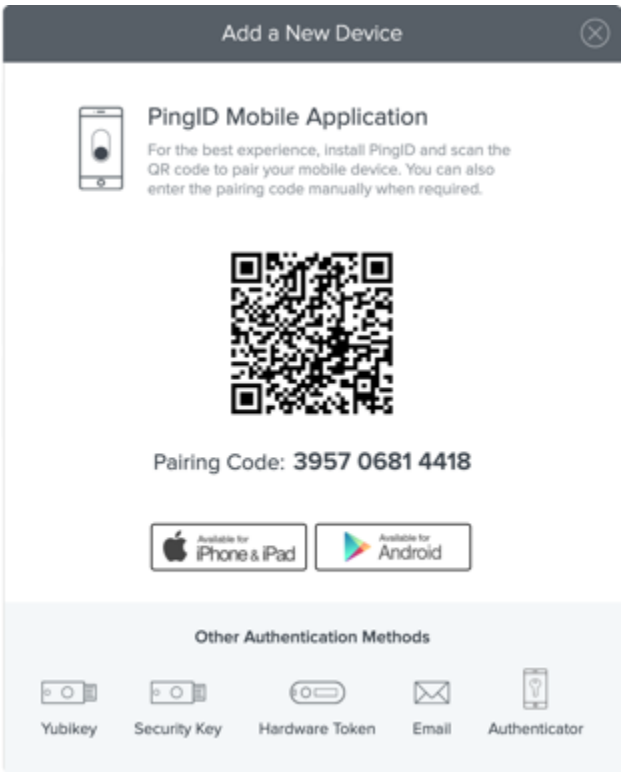
1. Sign on to your account or app and when you see the registration window, click **Start**.



You'll see the **Add a New Device** window, showing the QR code.

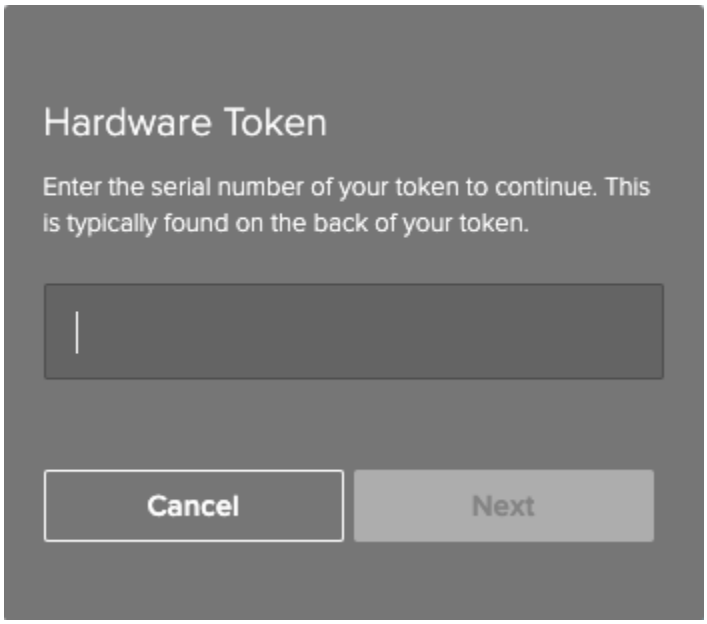


2. In the **Add a New Device** window, click **Hardware Token**.



Result:

The **Hardware Token Pairing** window displays.

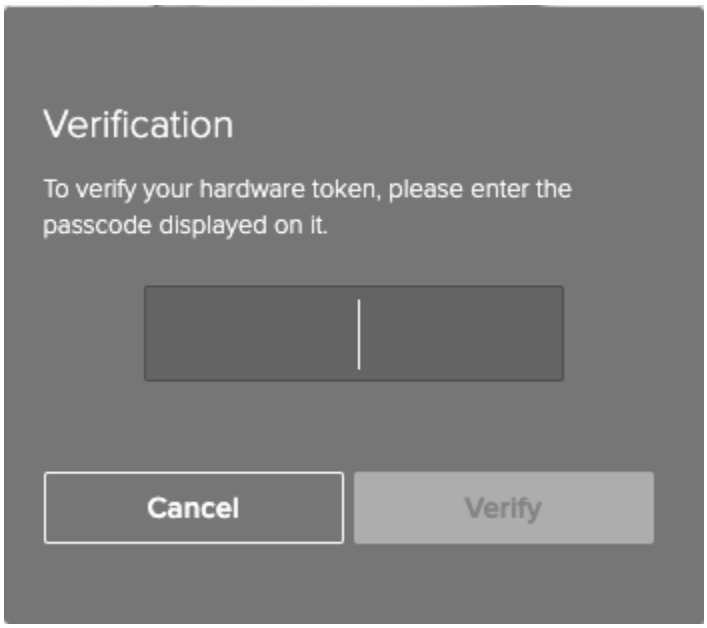


3. Enter your token serial number. Click **Next**.

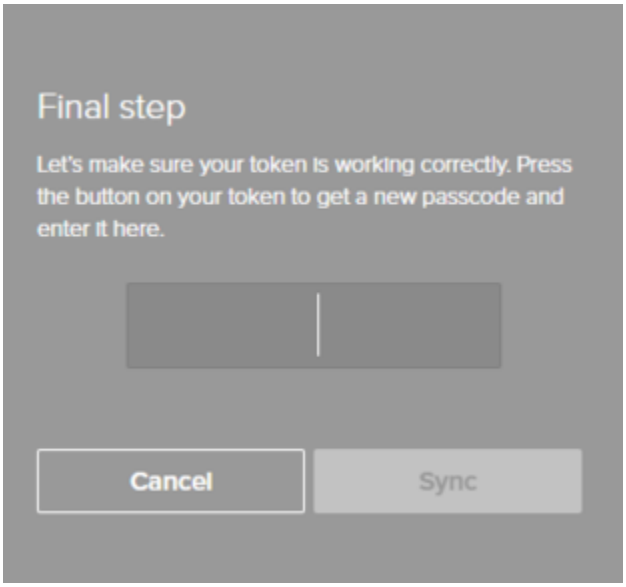
> **Note**
>
> The serial number is usually printed on the back of your token.

Result:

The **Verification** window displays.



You might see the **Final Step** window. It indicates that you token needs to be resynchronized, if so, follow the instructions and then click **Sync**.



4. Enter the passcode from your hardware token. Click **Verify**.

   Result:

   A green check mark appears, indicating your device is paired successfully. You are automatically signed on to your account or app.

5. The next time you sign on to your account or application, you need to authenticate using your hardware token.

   For more information, see Authenticating using a hardware token (Web).

VPN

Pairing your hardware token (VPN)

Register or 'pair' your hardware token so that you can generate a one-time passcode (OTP) and use it to authenticate securely with PingID when accessing your VPN.

Steps

1. From your web browser or app, sign on to your VPN and enter your username and password.
2. You will be asked to choose between several pairing devices. Enter `other`.
3. Click **Sign in**.
4. In the next text entry field, enter `token` followed by a space and then the serial number of your hardware token. (The serial number is usually printed on the back of the token. For example, `token 12345678`.)
5. In the OTP text entry field, enter the passcode on your hardware token.
6. Click **Sign in**.

   Result:

   Your hardware token is paired and authentication completed. You are signed into your VPN.

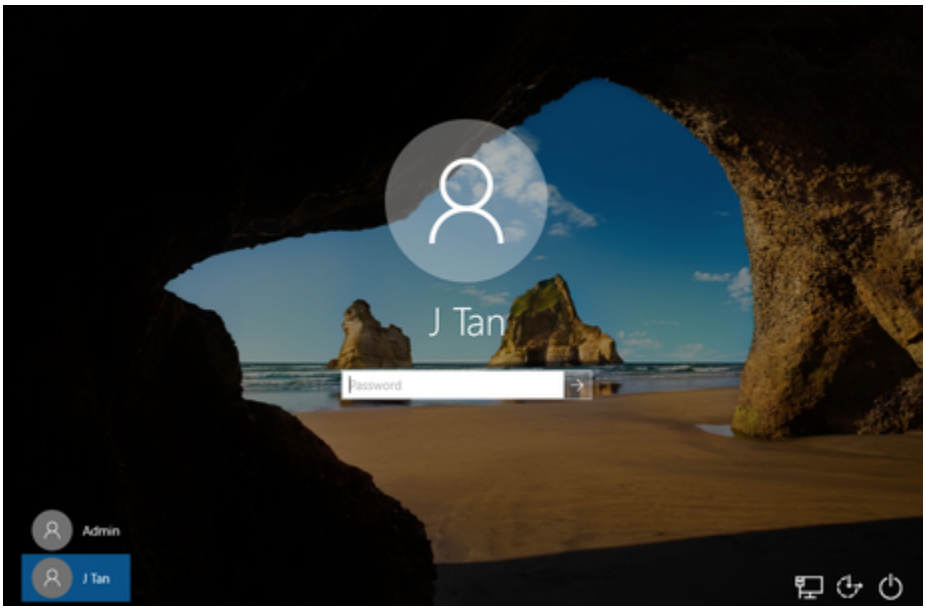
Windows login

Pairing your hardware token (Windows login)

Register or 'pair' your hardware token so that you can generate a one-time passcode (OTP) and use it to authenticate securely with PingID when accessing your Windows login machine.

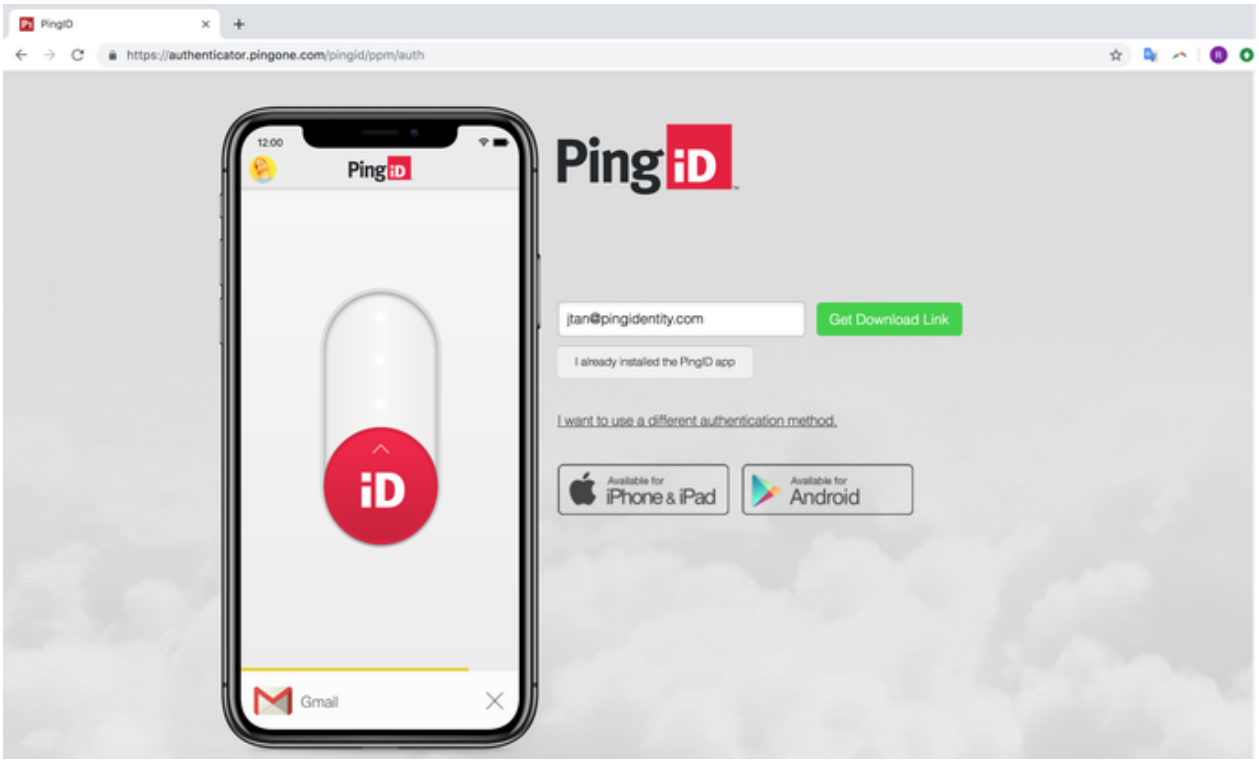
Steps

1. Sign on to your Windows machine.



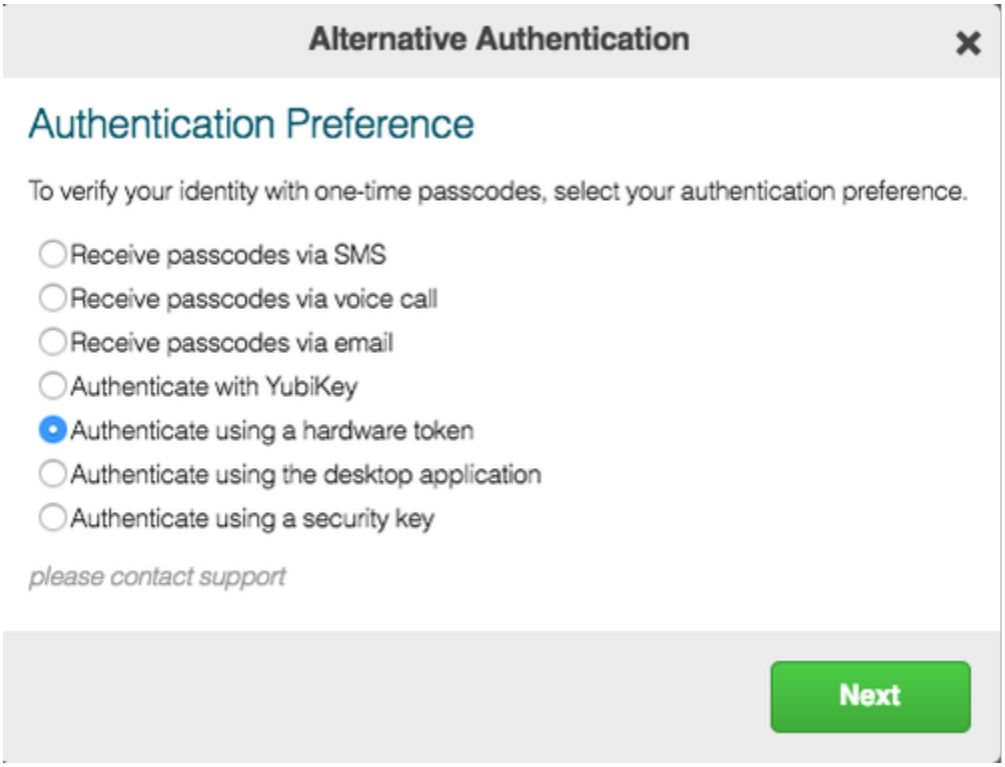
Result:

The PingID registration window displays.



> **Note**
>
> Until you successfully complete the registration process, you cannot minimize the PingID registration window. If you close the window, you are automatically redirected back to the Windows login window.

2. Click **I want to use a different authentication method**.
3. In the **Alternative Authentication** window, in the **Authentication Preference** section, click **Authentication using a hardware token**. Click **Next**.



+

Result:

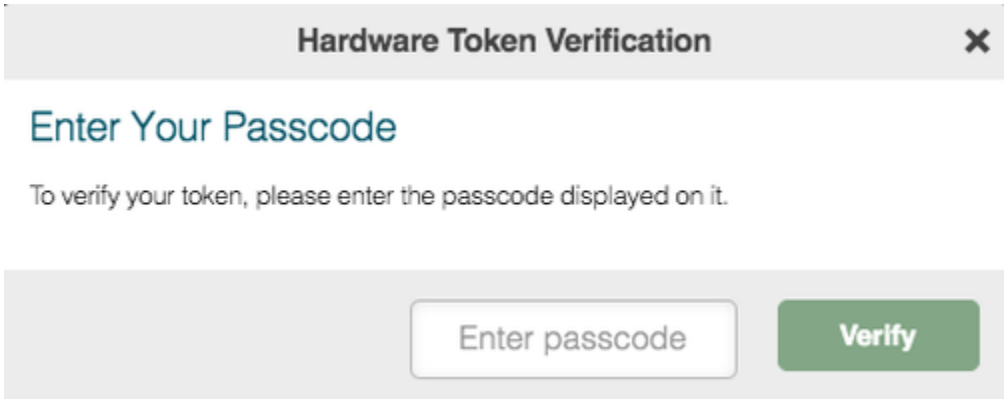
+ The **Hardware Token Pairing** window appears requesting the **Serial number** of your token.

+ image::mbn1564021291180.png[alt="A screen capture of the Hardware Token Pairing window."]

1. In the **Serial number** field, enter your token serial number. Click **Next**.

> **Note**
>
> The serial number is usually printed on the back of your token.

Result:



The OTP entry window is displayed

2. Enter the OTP from your token. Click **Verify**.

+

Result:

+ You are signed on to your Windows machine.

1. The next time you sign on to your Windows machine:
    1. You receive a OTP through your hardware token.
    2. Enter the hardware token OTP in the **Hardware Token Verification** window.
    3. Click **Sign On** to authenticate and sign on.

Related links

- Authenticating with PingID using a hardware token

Authenticating securely with PingID

How are you authenticating with PingID?

Pair › Authenticate › You're in!

I forgot my device | How do I pair a device? | I lost my device

- PingID mobile app
- Apple Mac Touch ID
- Security Key
- PingID desktop app
- Windows Hello
- YubiKey
- Authenticator app
- Android Biometrics
- Email
- SMS or Voice call
- iOS and iPad OS
- Hardware token

- Backup device

- Verifying your identity
- Managing your devices

Authenticating using PingID mobile app

Use the PingID mobile app to authenticate when accessing your account or app from any device.

After you've paired your device, each time you need to authenticate, you'll receive a push notification to your device which asking you to authenticate using PingID mobile app by approving a notification request, biometrics, number matching, or a one-time passcode (OTP). The method you use depends on your company and device configuration. You might also be able to authenticate manually when offline. Tap the relevant option for more details.

Depending on your organization's configuration, you can use PingID mobile app to access your account or app using a Web browser, your company's VPN, a Windows machine, or a Mac machine.

If you are running an older version of the mobile app (1.x), go to the legacy documentation for information.

- Approve a notification

  Approve a notification message sent to your device.

- Mobile app biometrics

  Use your device biometrics to authenticate with PingID mobile app.

- Number Matching

  Authenticate by number matching.

- One-time passcode (OTP)

  Use an OTP from PingID mobile app to authenticate.

- Smart watch

  Approve notifications from your smart watch.

- Manual authentication

  Authenticate when offline or when accessing a VPN.

- Legacy documentation

  View documentation for previous versions of PingID mobile app.

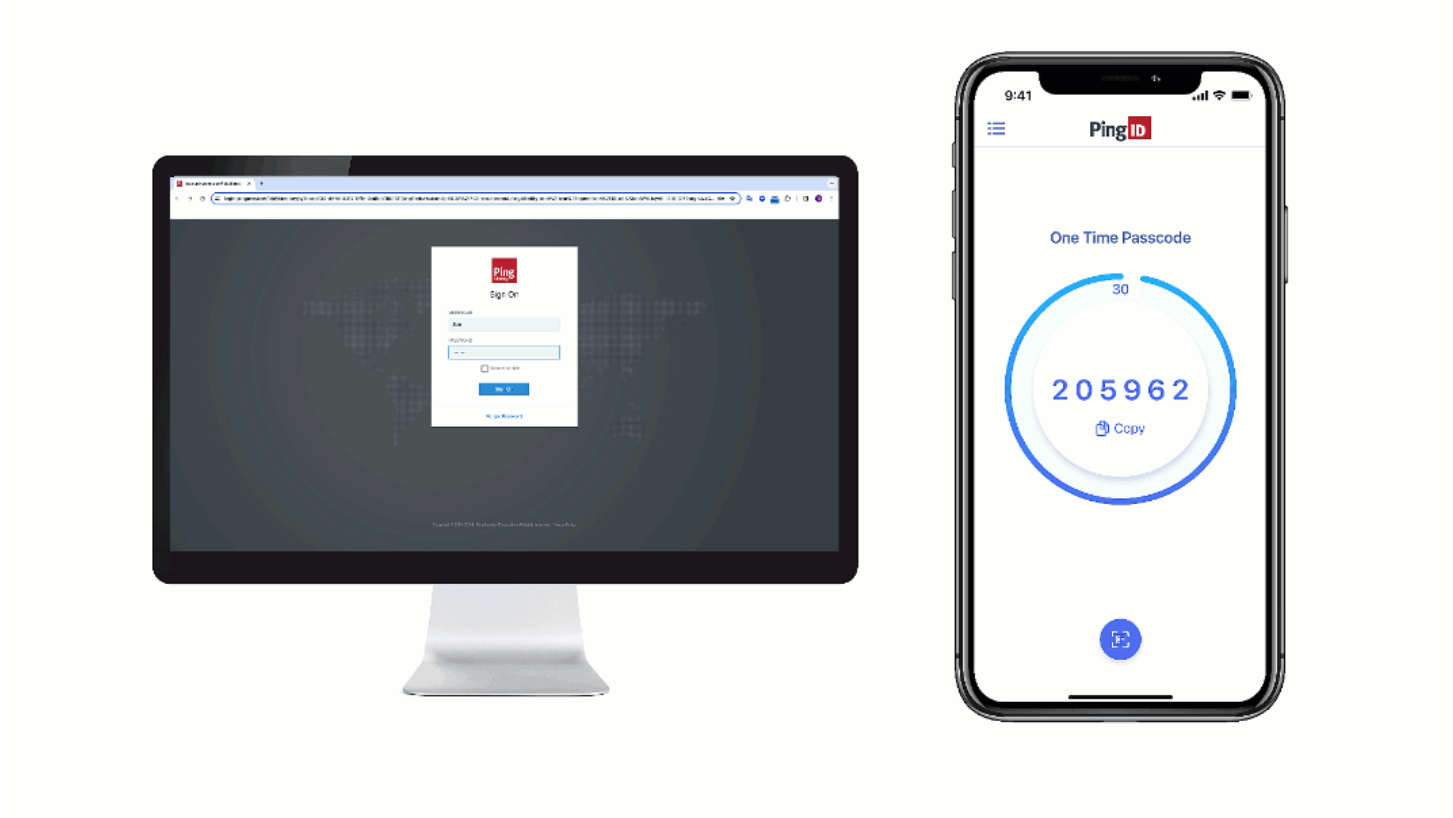
Approving a notification message

If you have the PingID mobile app running on your mobile device, you might be asked to approve a notification message that is sent to you mobile device so that you can securely access your resources.

Before you begin

Pair your mobile device with PingID mobile app. Learn more in Pairing PingID mobile app (using a QR code or pairing key).

About this task



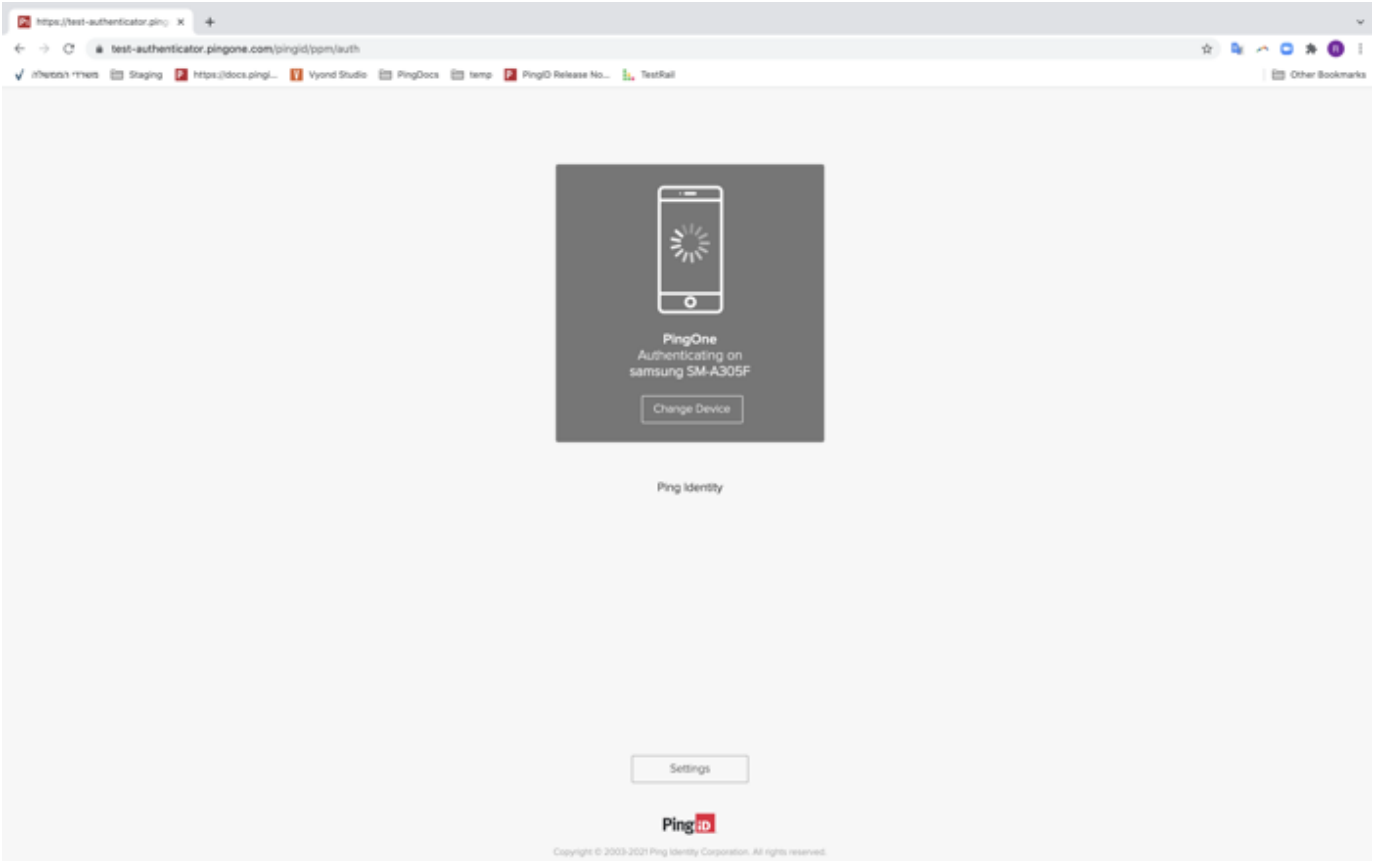
> **Note**
>
> The authentication process might vary slightly depending on your organization's configuration, as well as your mobile device operating system (OS) version and notification settings. Some devices might give you the option to approve a notification from the lock screen.

Steps

1. Sign on to your account or device or access the application that requires authentication.

   Result:

   You'll see the **Authenticating** window and an authentication notification request is sent to your mobile device.

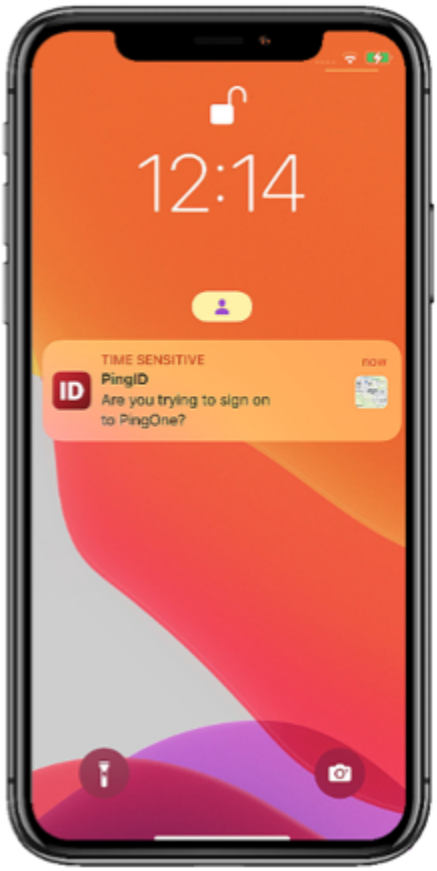


2. On your mobile device, approve the authentication notification message that asks if you are trying to sign on:

   Choose from:

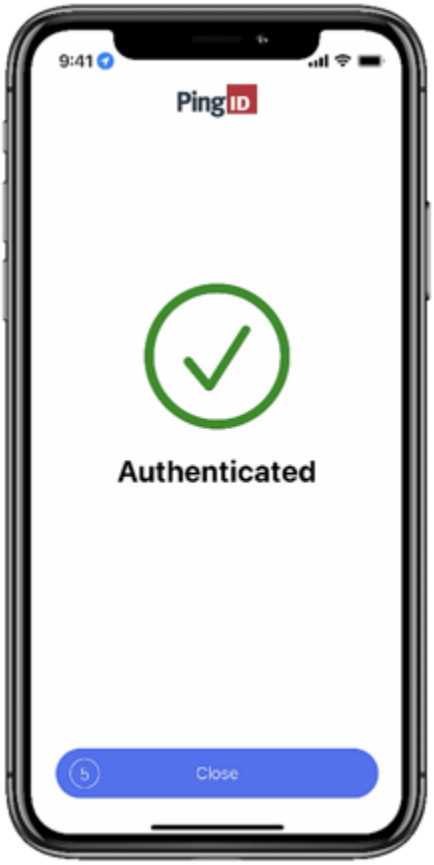
   - If PingID mobile app is open, tap **Yes**.

- If your phone is locked or PingID mobile app is closed, you might be able to authenticate from the lock screen. Long-tap the notification or swipe down, and then tap **Yes**.



Result:

You'll see the green check mark in PingID mobile app indicating that your access is approved.



Authenticating using biometrics

If you have the PingID mobile app running on your mobile device, you can authenticate using device biometrics, such as fingerprint or facial recognition, to securely access your resources.

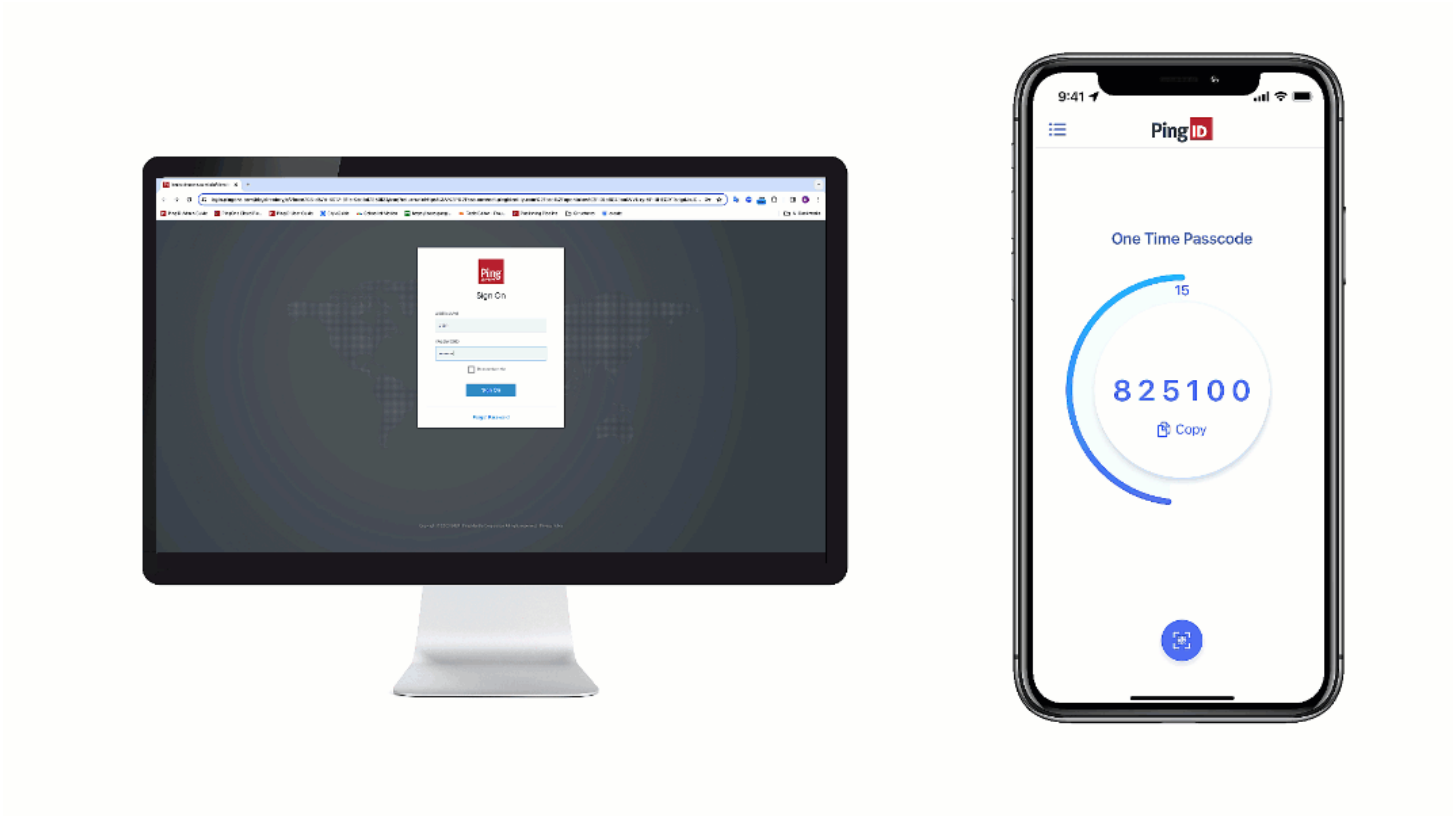
Before you begin

Register biometrics on your mobile device, and then pair your mobile device with PingID mobile app. Learn more in Pairing PingID mobile app (using a QR code or pairing key).

About this task

Note

- Biometrics authentication is only available if the option is enabled by your organization.
- Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when sending the authentication request.

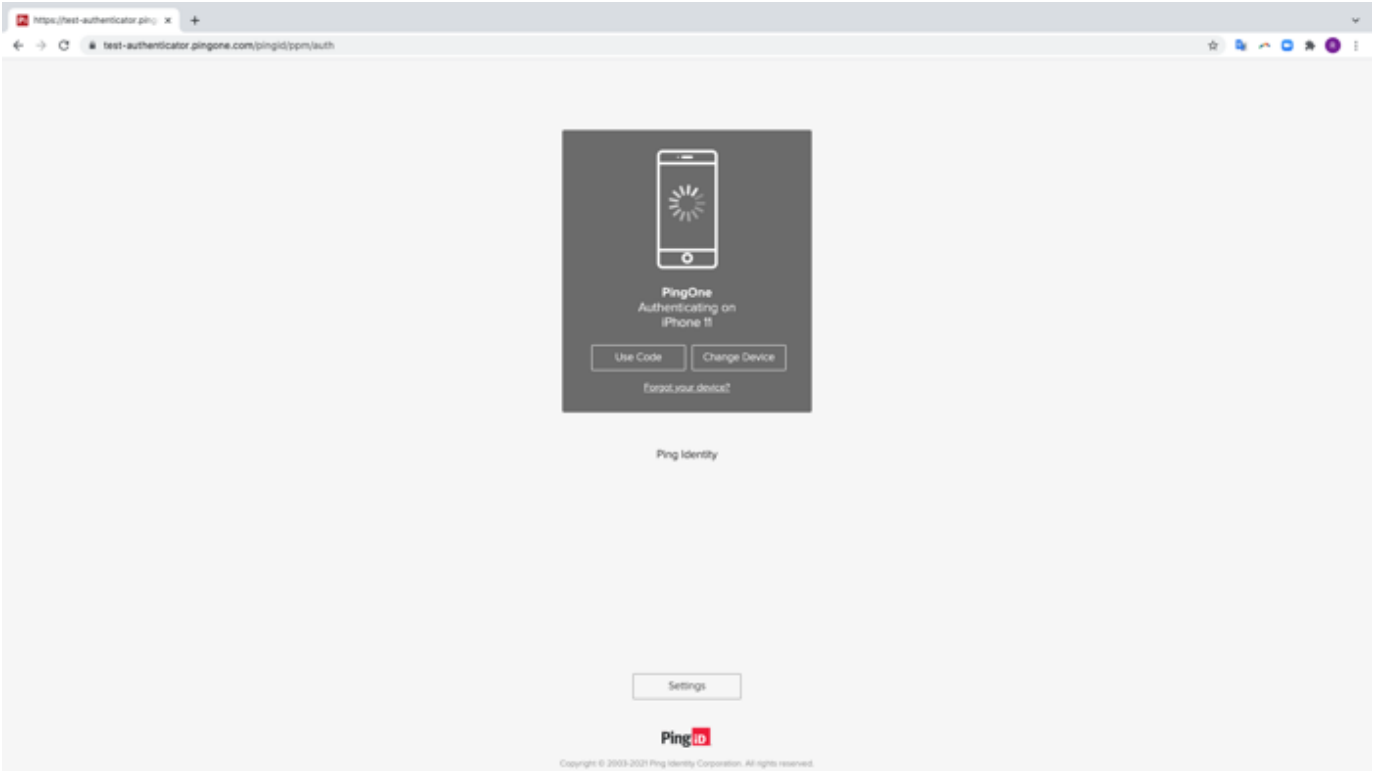


Steps

1. Sign on to your account or device, or access the application that requires authentication.

   Result:

   You'll see the **Authenticating** window and an authentication notification request is sent to your mobile device.



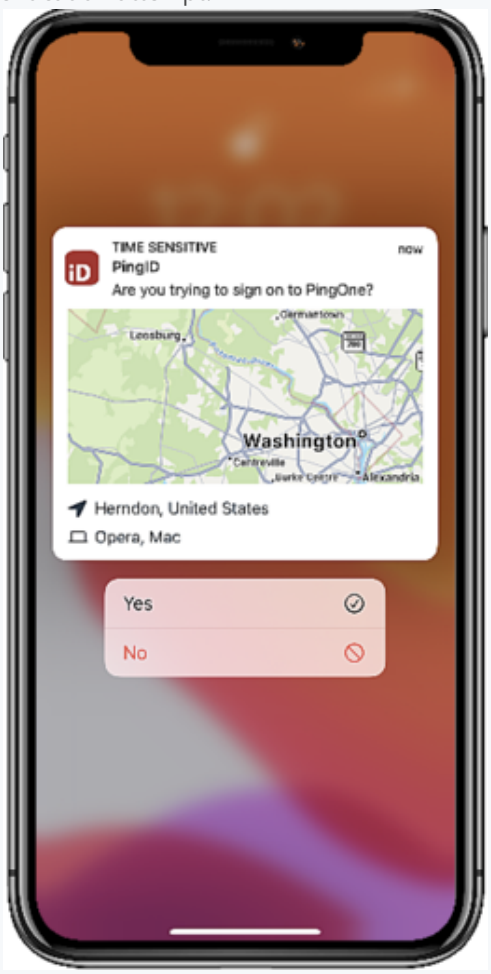
2. Accept the authentication notification message that asks if you are trying to sign on:

   Choose from:

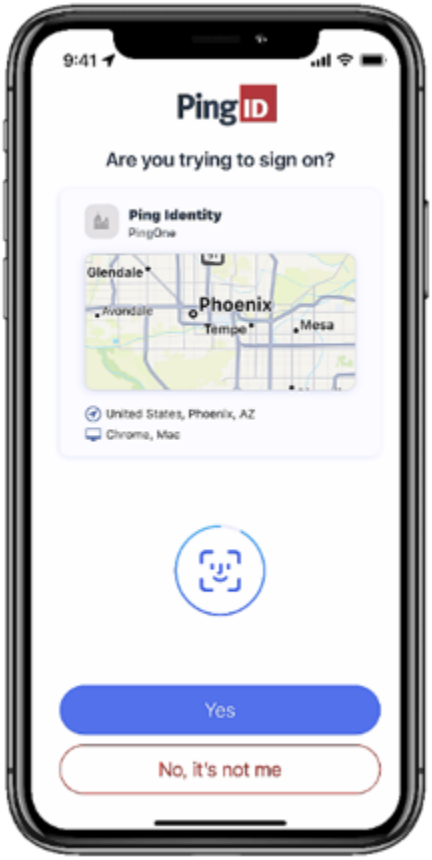
   - If your device is locked, long press or swipe the notification until it shows the option to approve or deny the request, and then tap **Yes**.
   - If your device is unlocked, on the notification, tap **Yes** or long-press the notification until it shows the option to approve or deny the request, and then tap **Yes**.

Note

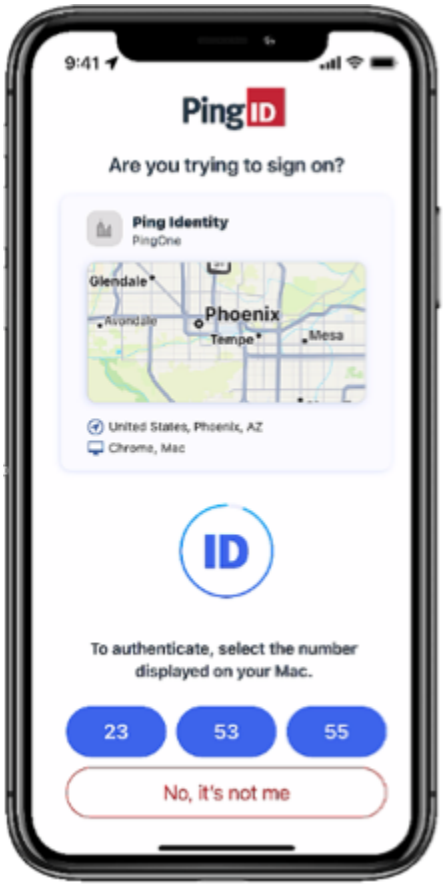
If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.



- If your mobile phone is unlocked and PingID is open, you'll be asked to authenticate with your biometrics.

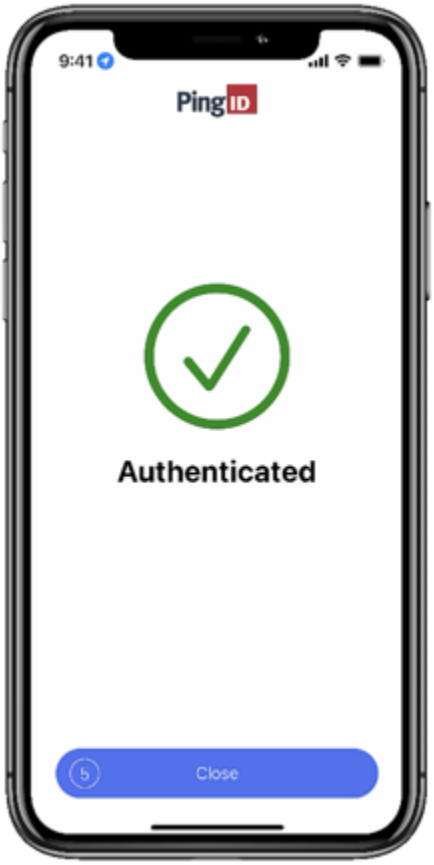


3. You might be asked to authenticate by number matching. If so, PingID mobile app opens and displays a number-matching screen. Select the same number that appears on the **Authentication** screen or enter it manually if required, and then authenticate with your biometrics.



Result

An **Authenticated** message with a checkmark appears, indicating successful authentication, and your access is approved. You are automatically signed on to your application.



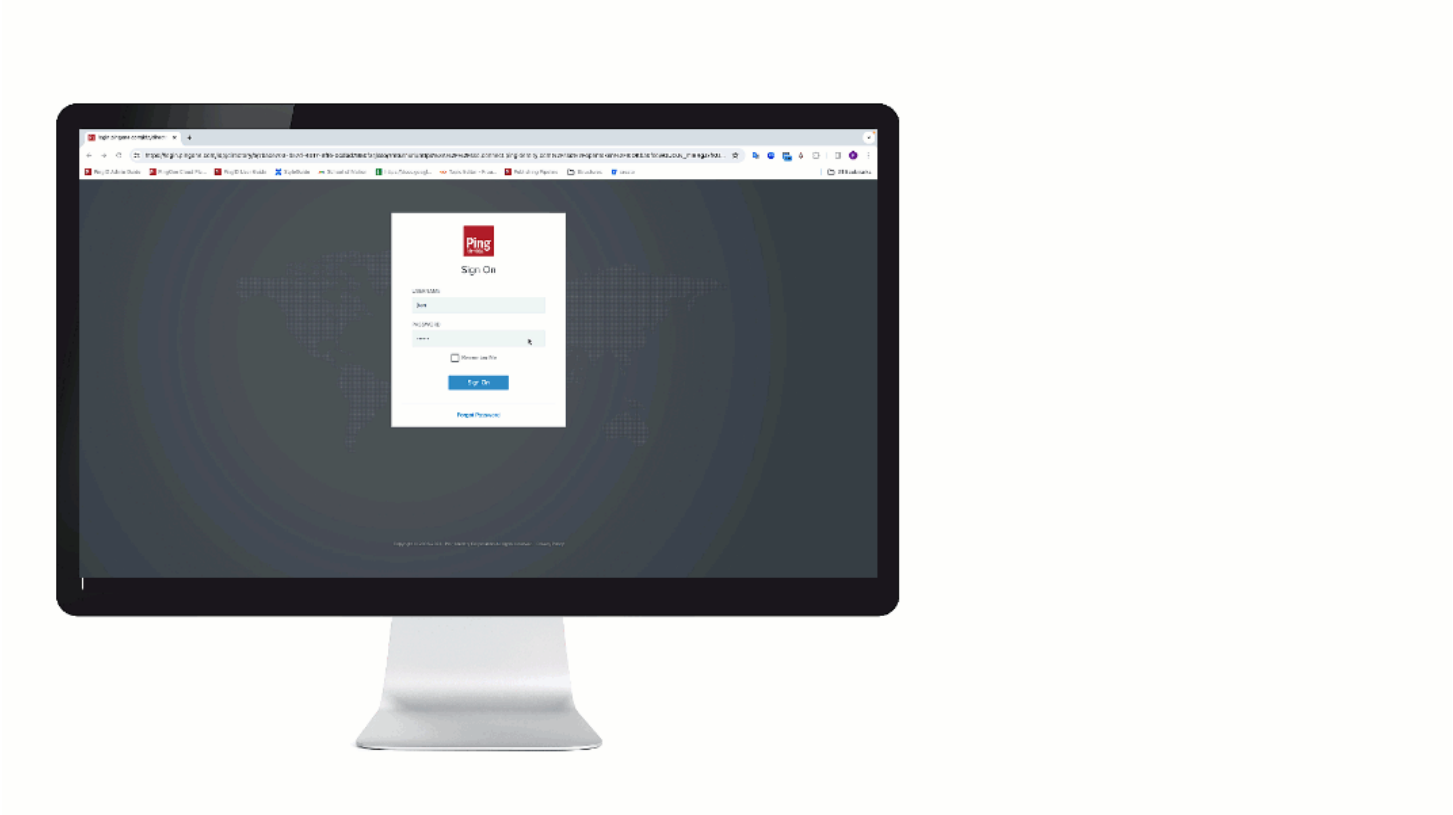
Authenticating using number matching

You might be asked to authenticate by selecting the number in PingID mobile app that matches the number displayed on the authenticating screen.

Before you begin

Pair your mobile device with PingID mobile app. Learn more in Pairing PingID mobile app (using a QR code or pairing key).

About this task

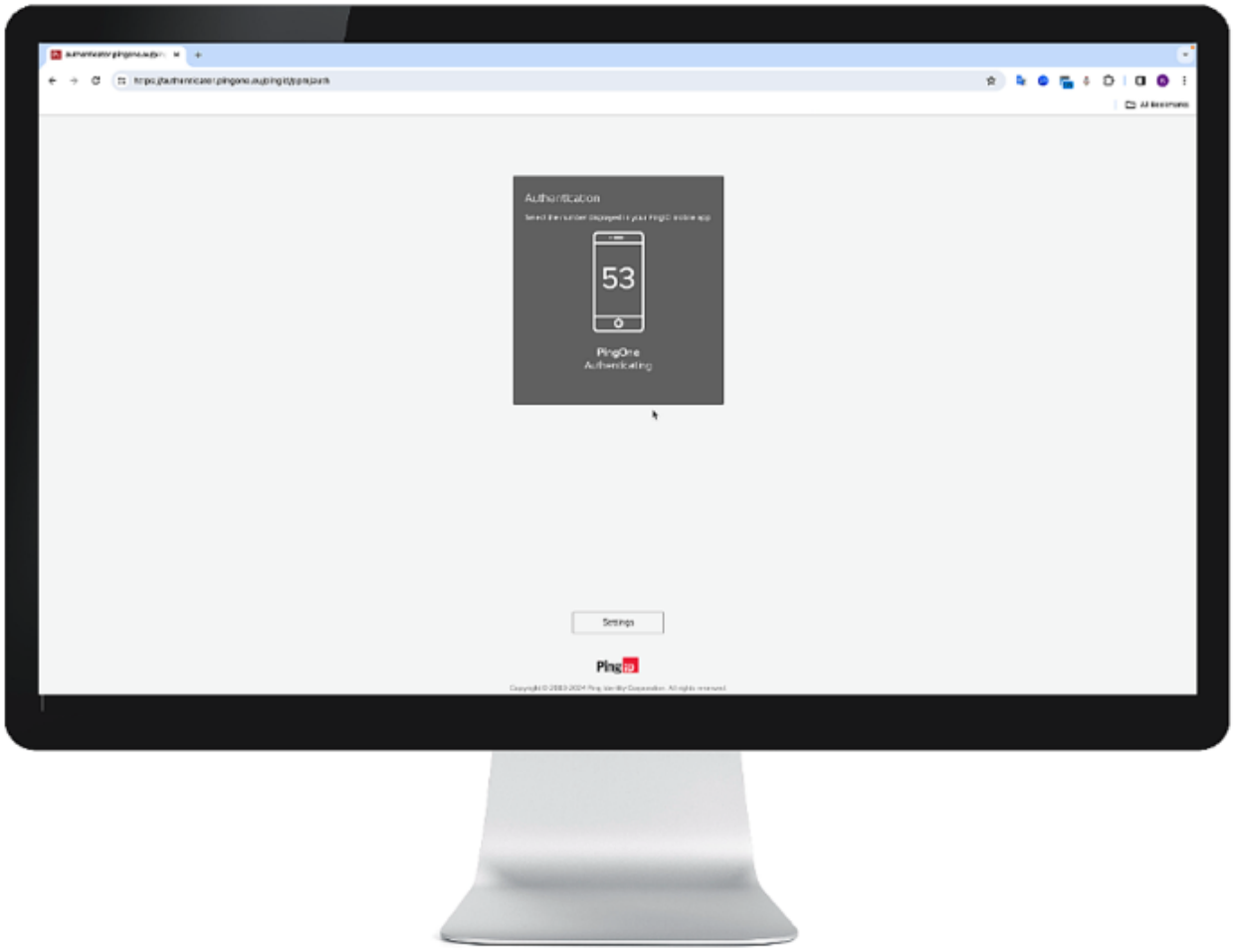


Steps

1. Sign on to your account or device, or access the application that requires authentication.

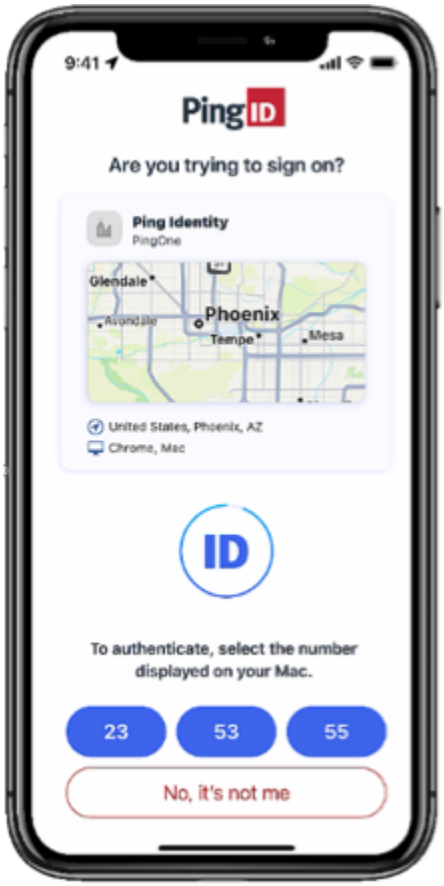
   Result:

   The **Authentication** window displays a number and a message asking you to select the same number in PingID mobile app.



2. Open PingID mobile app and select the number that matches the number shown on the **Authentication** screen or enter it manually if asked to do so.

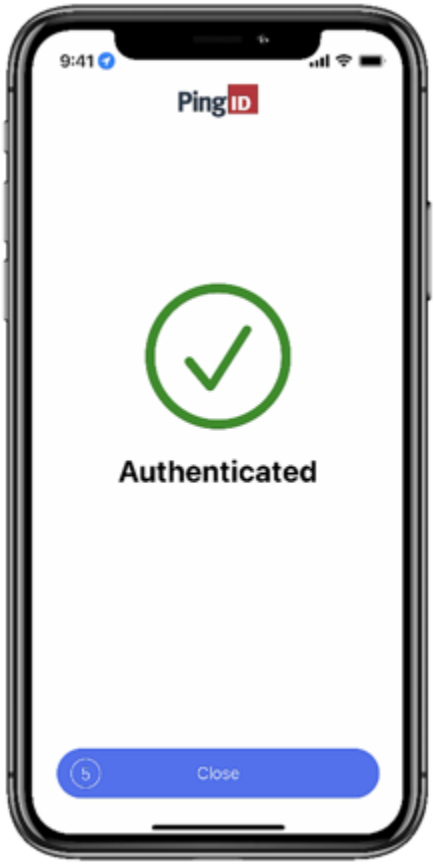
   You might also be asked to authenticate with your biometrics.



> **Note**
>
> Number matching support when using a smart watch depends on your organization's configuration and the type of smart watch you use.
>
> - Apple smart watch users can select the number from their smart watch.
> - Number matching isn't supported on Android watches.
> - It is not possible to manually enter a number on a smart watch.

Result

A checkmark appears indicating successful authentication and your access is approved. You are automatically signed on to your application.



Authenticating using a one-time passcode

If you cannot authenticate online using the PingID mobile app, or you are unable to receive push notifications to your mobile device, you can still authenticate by using a one-time passcode (OTP) from the app.

Before you begin

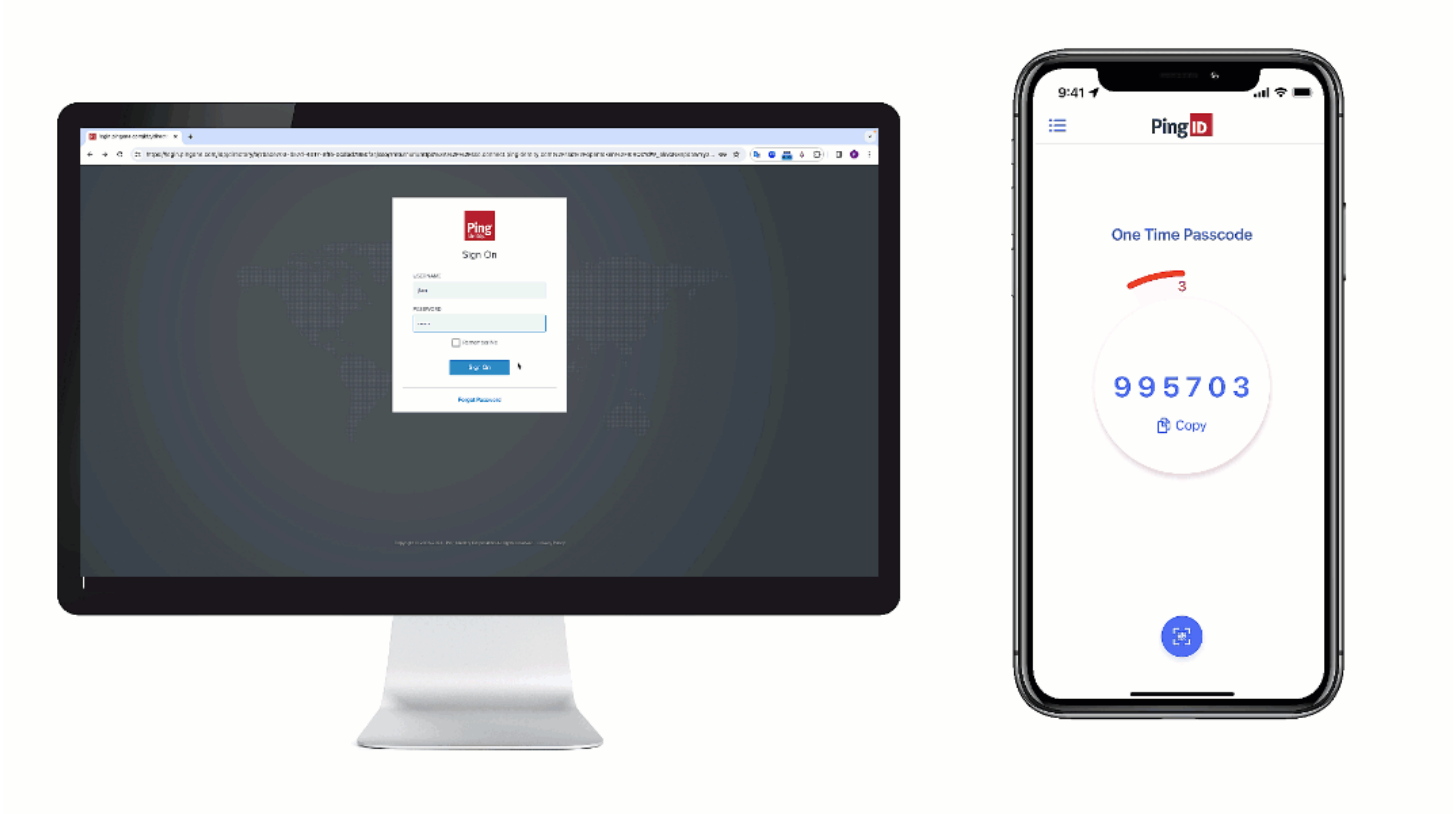
To authenticate using an OTP, you need to pair your mobile device with the PingID mobile app. If your mobile device is offline, you can only use an OTP to authenticate if you have authenticated successfully online at least once. Learn more in Pairing PingID mobile app (using a QR code or pairing key).

About this task

When you open the PingID app, it generates a new 6-digit OTP and displays a countdown timer showing when the current OTP is due to expire. Each OTP is unique, is valid for a limited time period, and can only be used once.

Note

- The OTP is refreshed at regular time intervals. Always use the current OTP displayed on PingID mobile app.
- If your organization's policy requires it, you might need to wait until the push notification sent to your mobile device times out before you can enter the OTP in the authentication window.

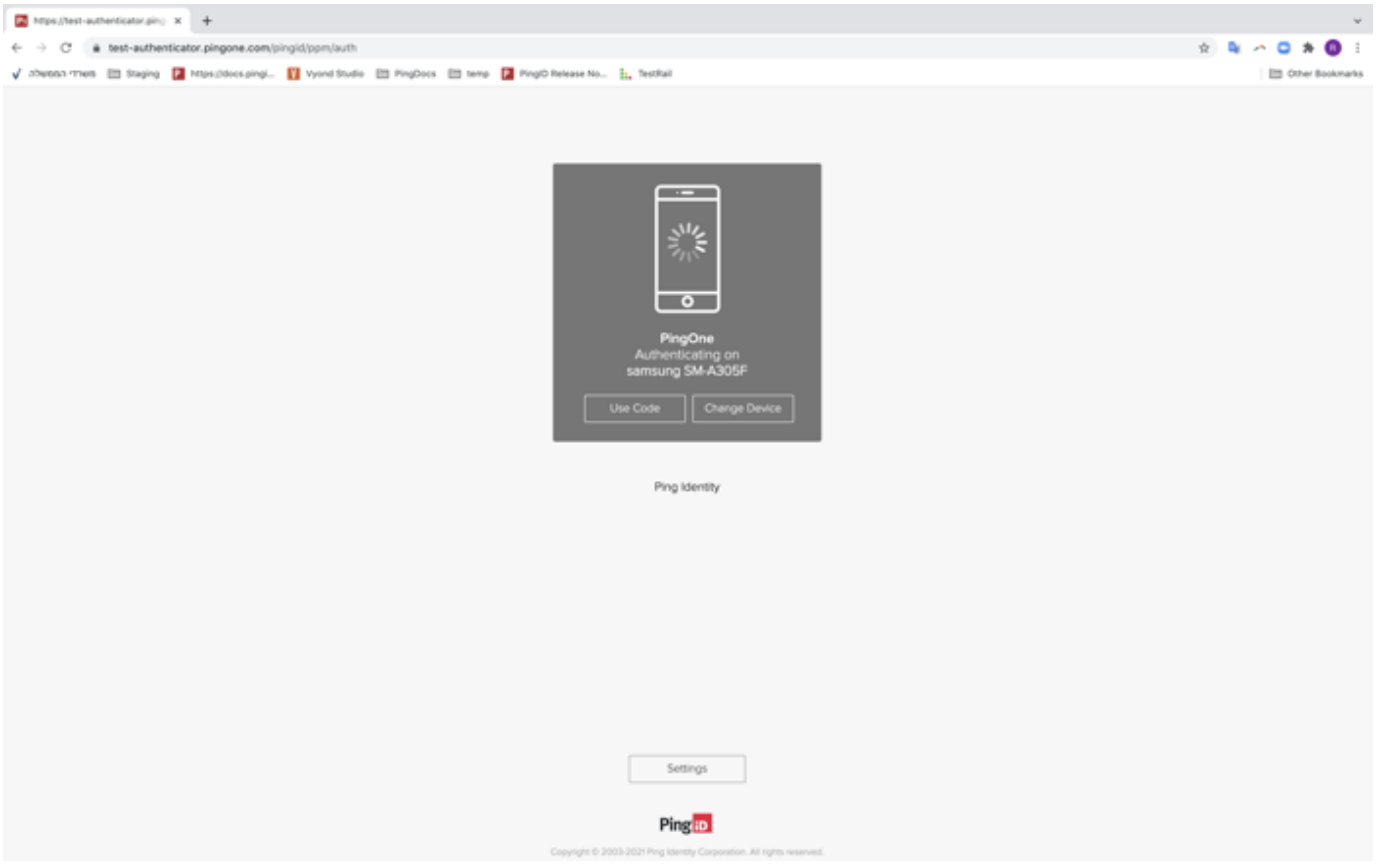


Steps

1. Sign on to your account or device, or access the application that requires authentication.

   Result:

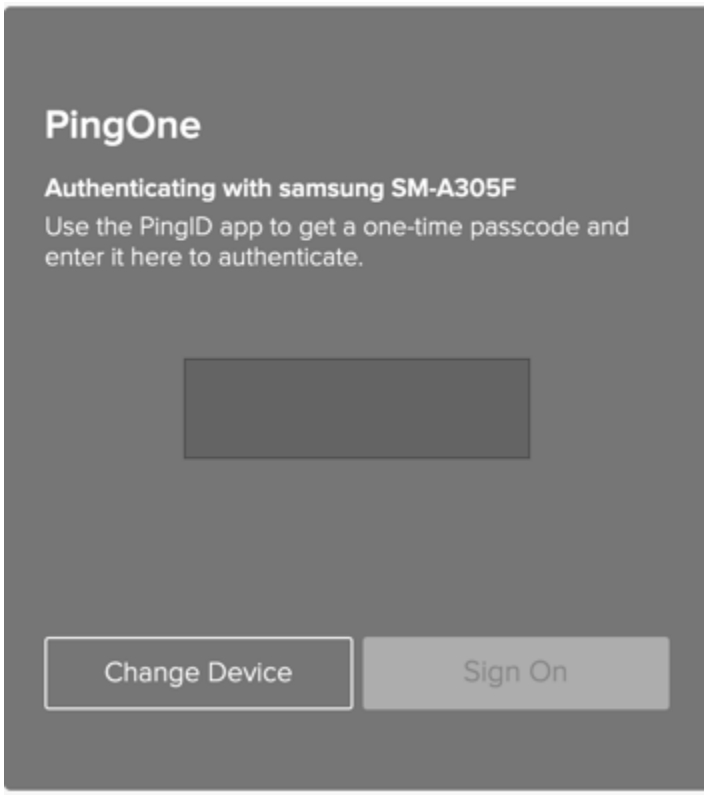
   You'll see the **Authenticating** window.



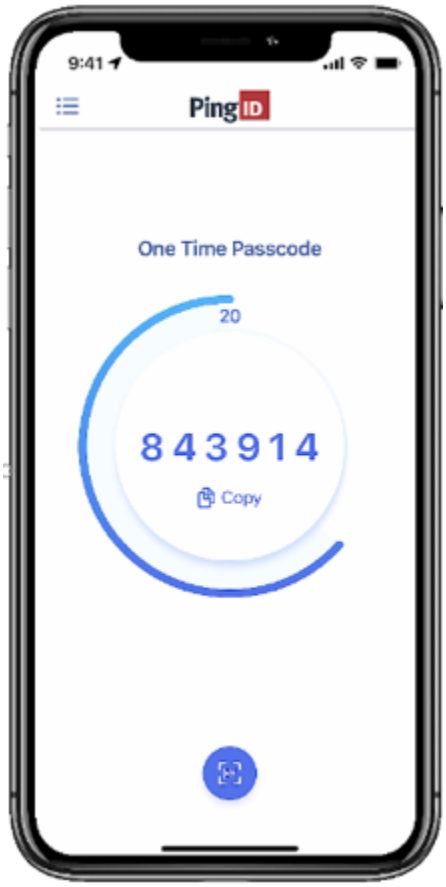
2. In the **Authentication** window, if you don't receive a push notification telling you to authenticate, either click **Use Code**or wait until the push notification timeout occurs on your mobile device.

   Result:

   You are asked to enter an OTP.



3. On your mobile device, open the PingID mobile app to view the current OTP. The OTP refreshes at regular intervals.



4. In the **Authentication** window, enter the current OTP into the field and then click **Sign On**.

> **Note**
>
> If you receive a push notification on your mobile device before signing on using the OTP, you can still approve the notification.

Result

A green **Authenticated** message with a check mark appears, indicating authentication is successful and your access is approved.

Authenticating using a smart watch

You can authenticate with PingID mobile app using your smart watch.

About this task

If you have a smart watch paired with your mobile device, with the PingID mobile app installed,you can receive authentication notifications to your smart watch, in parallel with your mobile device. You can then authenticate without taking your mobile device out of your pocket.

If you're using an Apple Watch, download the app to your smart watch so that you can access an OTP (one-time passcode) from your Apple Watch

> **Note**
>
> The ability to authenticate using a smart watch varies according to your device model and configuration. Android smart watches do not support authenticating using number matching. Android users must select a number from their mobile devices to authenticate. Learn more in Authenticating using number matching.

Steps

1. If your mobile device is locked or inactive and you have a smart watch, when you sign on, a notification appears on your smart watch, as well as your mobile device. Swipe up to view the message, and then tap **Yes**.

1. If you see three numbers displayed on your smart watch, your organization also requires you to authenticate by number matching. To complete authentication, select the number on your smart watch that matches the number displayed on the **Authentication** screen.

Result

You'll see the green check mark, indicating authentication is successful and you're signed in to your account.

Enabling and disabling passcodes on your Apple Watch

Enable the use of one-time passcodes (OTPs) on your Apple Watch.

About this task

If you have installed the PingID mobile app on your device, on most models of the Apple Watch, thePingID mobile app is installed on the watch automatically. You should receiving notifications to your watch fromPingID and can also open the PingID mobile app on your watch to receive a one-time passcode (OTP). If the Apple Watch app is disabled, you will not be able to access an OTP from your watch.

> **Note**
>
> Your Apple Watch only receives notifications when your mobile device is locked and the mobile device screen is in sleep mode.

Steps

1. On your iPhone, tap the Watch app, and then tap **PingID**.
2. To enable or disable the app on your Apple watch, tap **Show App on Apple Watch**.

   Result:

   The PingID mobile app is installed on your Apple Watch, and the PingID icon appears.
3. To view the current OTP, on your Apple Watch, tap the PingID icon.

4. **Optional:** To get a new passcode, tap **Refresh**.

Authenticating manually with PingID mobile app

In some situations, such as if you are signing on to your company VPN or if you do not have internet access, you might be asked to authenticate manually through the PingID mobile app.

Authenticating manually is slightly different than the normal sign-on process. It also varies depending on whether you want to:

- Access resources on your computer and authenticate through your mobile device.
- Access resources on your mobile device and authenticate using that same mobile device.

Access resources on a computer

Authenticating manually to access resources on your computer

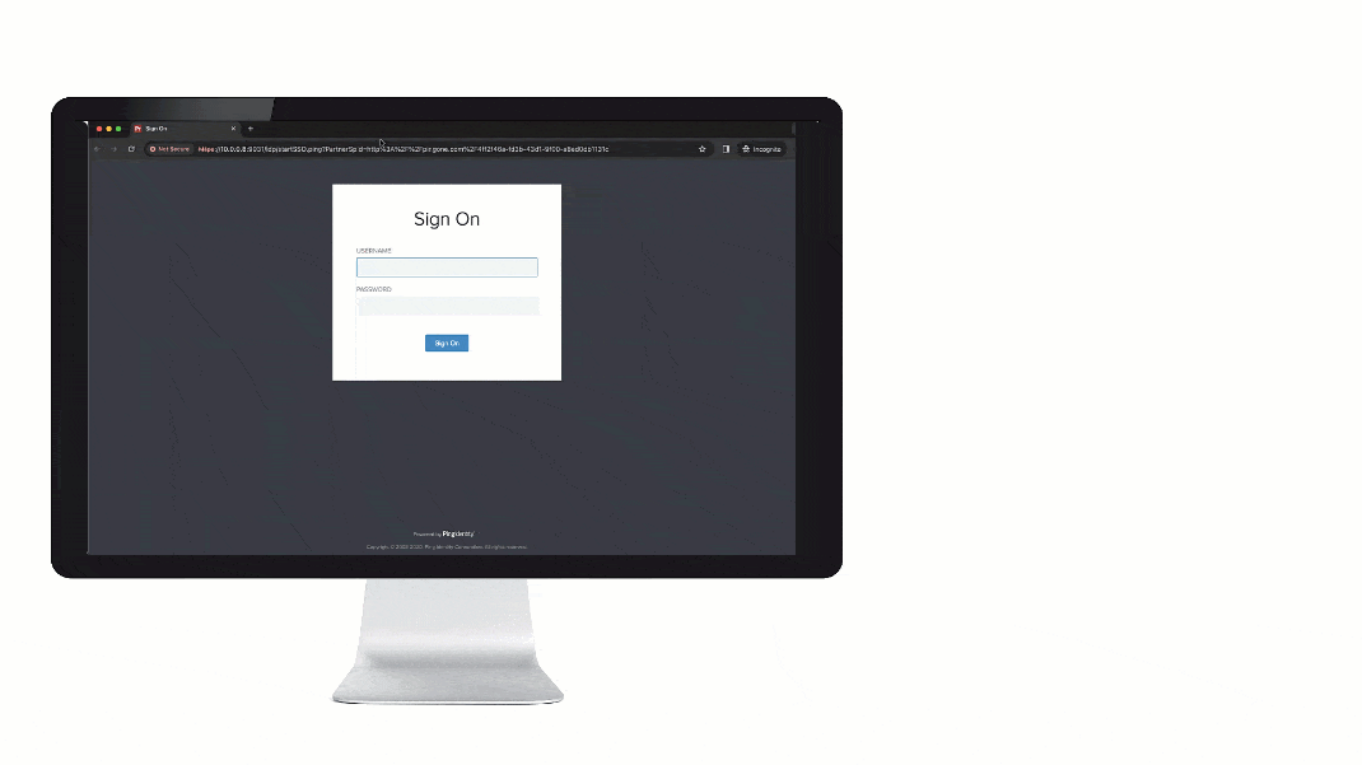
When you sign on to your account, device, or VPN, you might be asked to authenticate manually through the PingID mobile app.

Before you begin

To authenticate manually to access resources on your computer or any device other than the one with PingID mobile app installed, you need:

- A mobile device with PingID mobile app installed and paired with your account, and with which you have successfully authenticated online at least once.
- A working camera on the mobile device with the PingID mobile app camera permissions set to **Approve**. Learn more in PingID mobile app management.

About this task



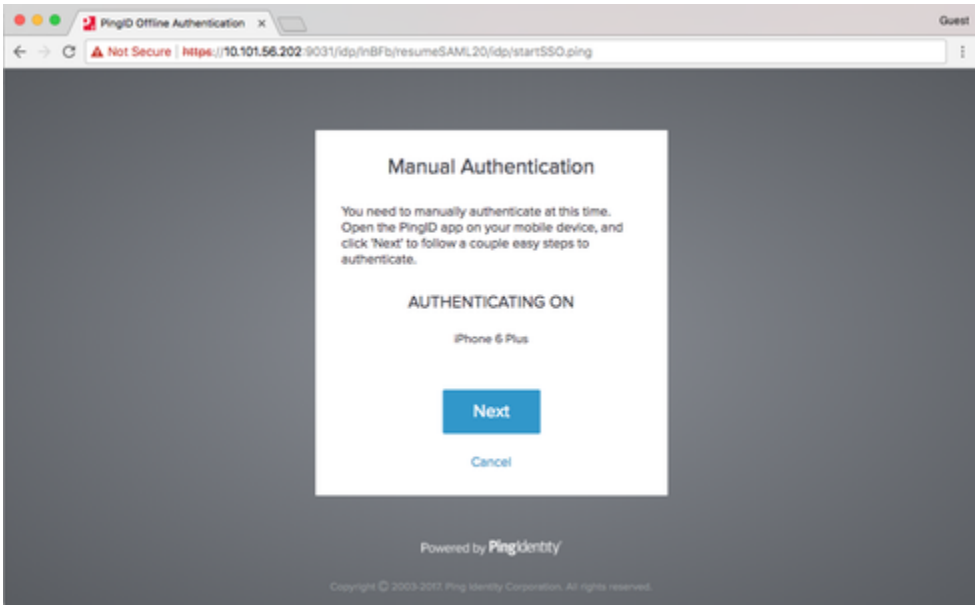
Steps

1. Sign on to your account or device or access the application that requires authentication.

   If you have more than one device paired with your account, you'll see a list of your devices. Select the device you want to use to authenticate.

   Result:

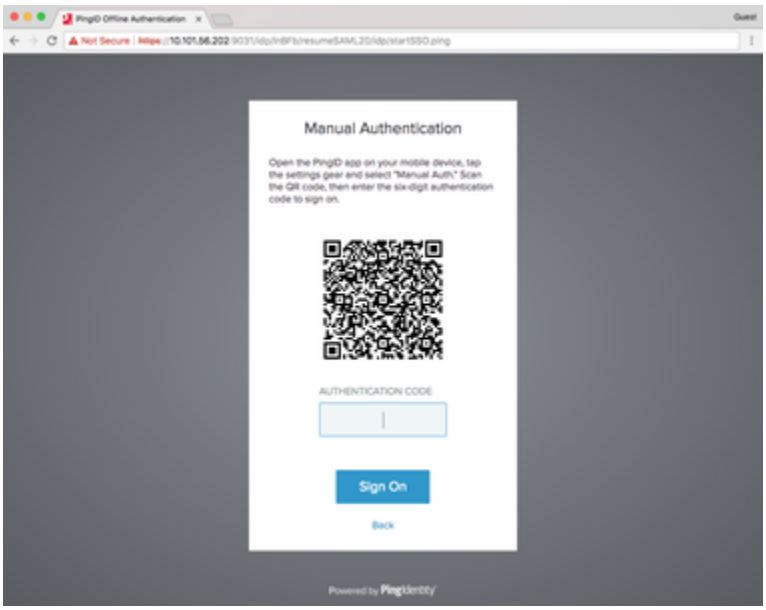
   A **Manual Authentication** message appears, requesting that you manually authenticate.



2. Click **Next**.

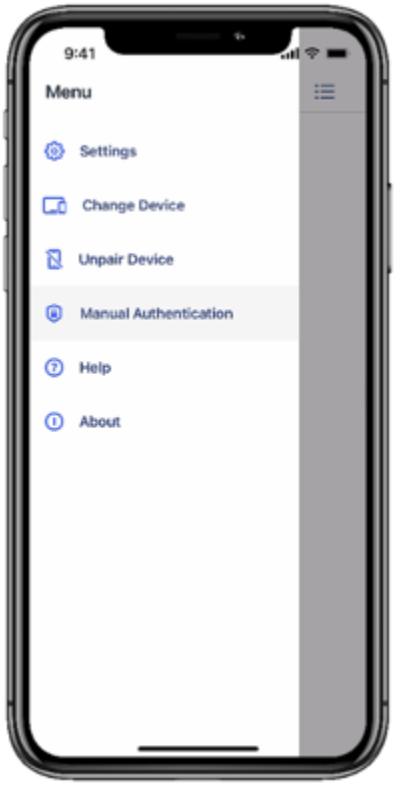
   Result:

   A **Manual Authentication** message appears, displaying a QR code or an authentication key, requesting that you authenticate manually.

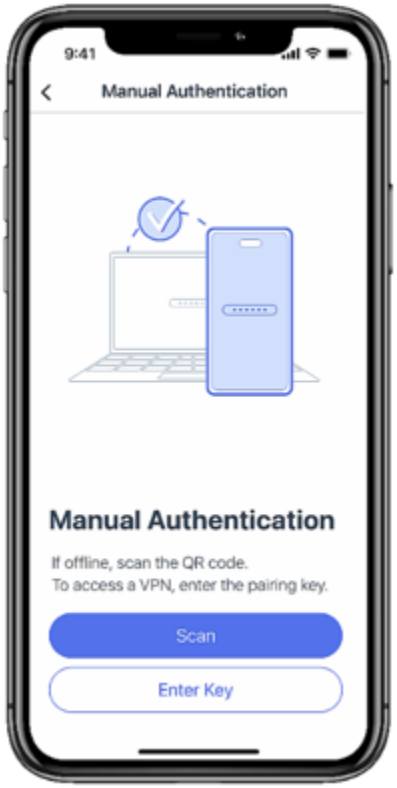


3. From your mobile device, open the PingID mobile app.

4. Tap the **Menu** icon ( ) and select **Manual Authentication**.



Result:



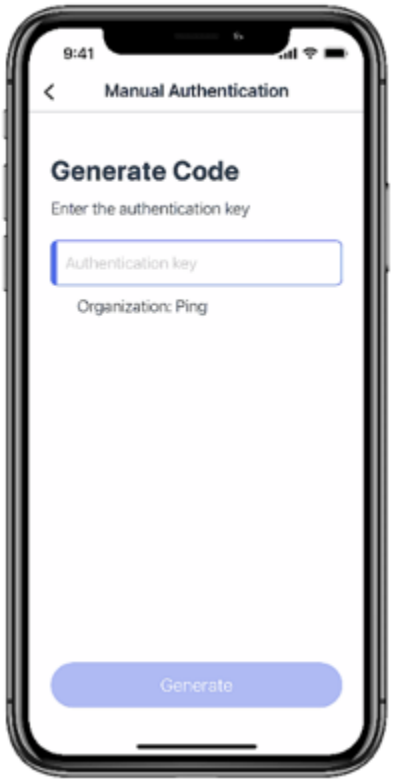
5. Do either:

Choose from:

- If your computer displays a QR code: In PingID mobile app, tap **Scan** and use your mobile device to scan the QR code.

> **Tip**
>
> You can scan the QR code directly from your device camera without opening the mobile app.

- If your computer displays an authentication key or you are trying to access your VPN: Tap **Enter Key** and then, on the **Generate Code** screen, enter the pairing key (long numerical code) that is displayed on your computer.

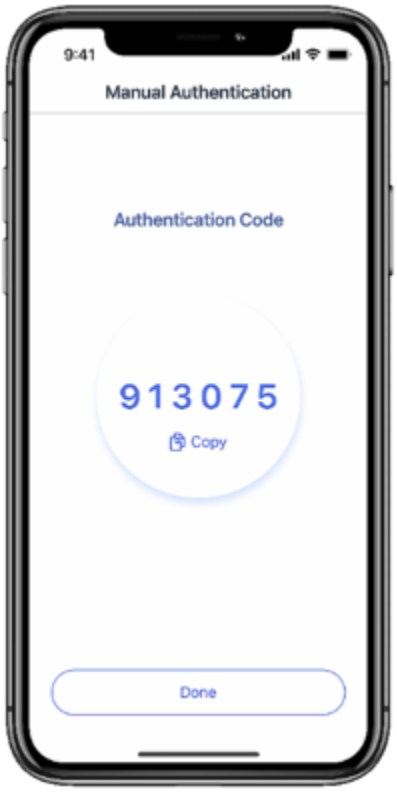


> **Note**
>
> You might also be asked to authenticate using your device biometrics.

> **Tip**
>
> + If PingID is paired with more than one organization, on the**Generate Code** screen, make sure that the correct organization is selected. Tap**Change Organization** to change the default organization, if needed.

Result:

You receive an **Authentication Code** in the PingID mobile app.



6. On your computer, enter the **Authentication Code** into your web browser, and click **Sign on**.

Result

You are successfully authenticated and automatically signed on to your account.

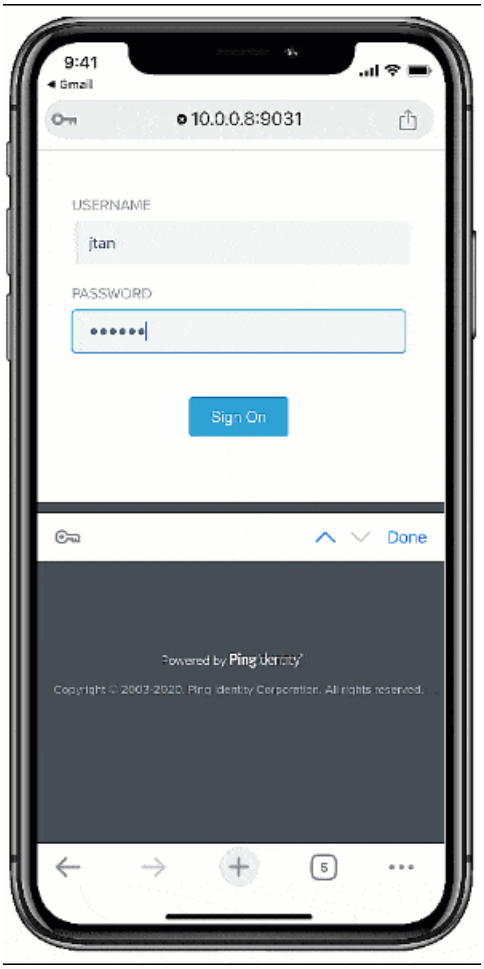
Access resources on a mobile device

Authenticating manually to access resources on your mobile device

When you sign on to your account using a web browser on your mobile device, if you are asked to authenticate manually and have the PingID mobile app paired to that device, follow these instructions to authenticate manually from the same device.

Before you begin

To authenticate manually from your mobile device to access resources on the same mobile device, you need a device that is already paired with your account and with which you have successfully authenticated online at least once.



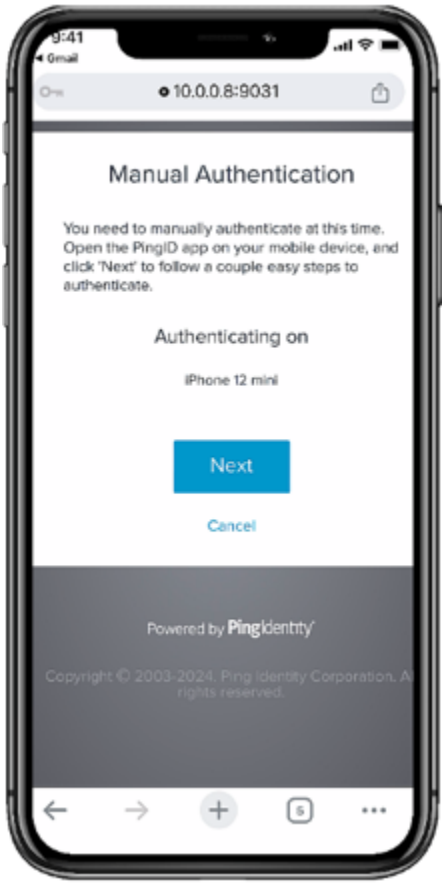
Steps

1. From a mobile device that is paired with PingID mobile app, open a browser window and sign on to your account or access the application that requires authentication.

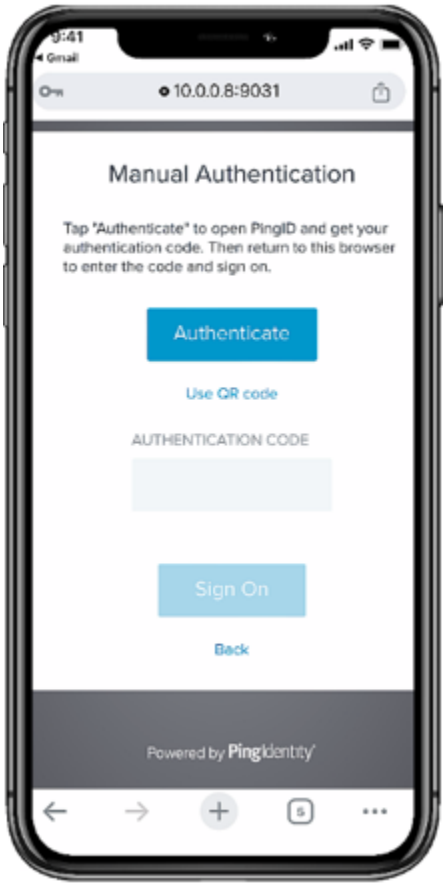
   If you have more than one device paired with your account, a list of all your currently paired devices appears. Select the device you want to use to authenticate.

   Result:

   A **Manual Authentication** message appears with the **Authenticating On** section and the **Next** option.



2. Click **Next**.



> **Note**
>
> If you are trying to access resources on a device that is not your authenticating device, such as a different mobile device or an iPad that is not paired with PingID, click **Use QR Code**, and follow the steps outlined in Authenticating manually to access resources on your computer.

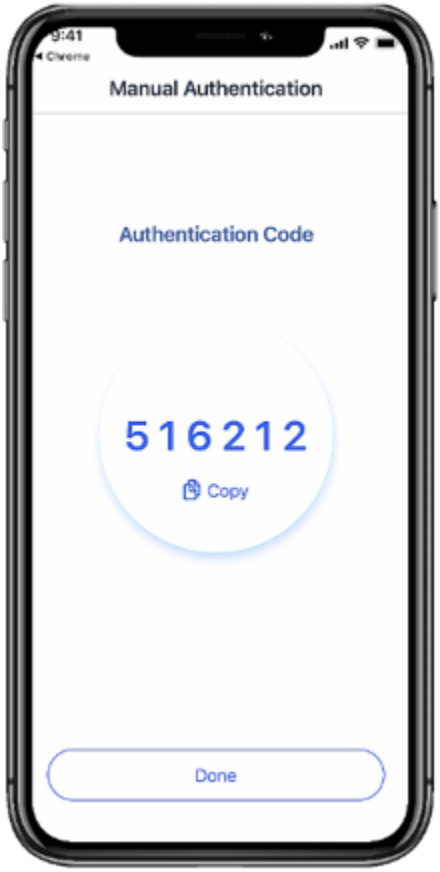
Result:

A **Manual Authentication** message appears.

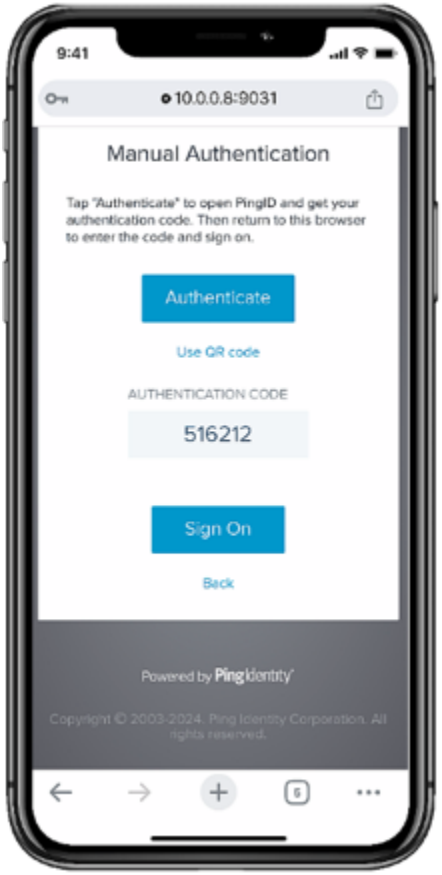
3. Tap **Authenticate**, and authenticate with your device biometrics, if required.

   Result:

   PingID mobile app opens automatically, and you receive an **Authentication Code**.



4. Tap **Copy** to copy the authentication code, then return to your web browser.
5. In the web browser, tap the **Authentication Code** field and paste the authentication code into the field. Click **Sign on**.



Result

You are successfully authenticated and signed on to your account or app.

Using PingID mobile app authentication (legacy)

PingID allows you to use your mobile device to sign on to your company services and applications with the added security of multi-factor authentication (MFA).

> **Note**
>
> This is legacy documentation. If you are running PingID mobile app 2.0 or later, see Using PingID mobile app authentication.

The PingID mobile app enables you to authenticate from your mobile device in a variety of ways, including swipe, biometrics, number matching, or a one-time passcode (OTP) depending on your company and device configuration. You might also be able to authenticate manually when offline. Use the PingID mobile app to authenticate when accessing your account or app from any device.

Depending on your organization's configuration, you can use PingID mobile app to access your account or app using a Web browser, your company's VPN, a Windows login machine, or a Mac machine.

To get started, you'll need to download the app to your mobile device, and pair (connect) your device with your account. After you've paired your device, each time you sign on to your account, you will receive a push notification to your mobile device asking you to authenticate.

For more general information about PingID mobile app, see What is PingID mobile app and how does it work?.

If you have a new mobile device and want to transfer PingID mobile app from your old device to your new device, see Transfer PingID mobile app authentication to a different device.

Select the instructions relevant to the resources you want to access.

Web

UsePingID mobile app to access your account or app using a web browser.

iOS

- Set up your iPhone for PingID authentication
- Authenticate using your iPhone
- Authenticate manually if you're offline

Android

- Set up your Android for PingID authentication
- Authenticate using your Android
- Authenticate manually if you're offline

VPN

Use PingID mobile app to access your company's VPN.

iOS

- Set up your iPhone for PingID authentication (VPN)
- Authenticate using your iPhone (VPN)
- Authenticate manually if you're offline (VPN)

Android

- Set up your Android for PingID authentication (VPN)
- Authenticate using your Android (VPN)
- Authenticate manually if you're offline (VPN)

Windows login

Use PingID mobile app to access your Windows login machine. Register using a web browser, and then authenticate when signing on to your Windows login machine either locally or using a remote desktop machine (RDP).

iOS

- Set up your iPhone for PingID authentication (Web)
- Authenticate using your iPhone (Windows login)
- Authenticate manually if you're offline

Android

- Set up your Android for PingID authentication (Web)
- Authenticate using your Android
- Authenticate manually if you're offline

Use PingID mobile app to access a remote desktop machine through the Windows RDP client

Mac login

Use PingID mobile app to access your Mac machine.

iOS

- Set up your iPhone for PingID authentication (Web)
- Authenticate using your iPhone (Mac login)
- Authenticate manually if you're offline (Mac login)

Android

- Set up your Android for PingID authentication (Web)
- Authenticate using your Android (Mac login)
- Authenticate manually if you're offline (Mac login)

Managing your devices and getting help

- Authenticate using a backup device
- Manage your devices
- Manage PingID mobile app
- Transfer PingID mobile app authentication to a different device
- Troubleshoot PingID authentication

Authenticating using your iPhone (Web) (legacy)

This section covers the options available for authenticating using your iPhone, when accessing your account or app using a web browser.

You can authenticate using the following options:

- Using swipe authentication for iPhone
- Using biometrics authentication for iPhone
- Authenticating with PingID using a one-time passcode
- Authenticating using your Apple Watch

If you have not yet paired PingID mobile app with your account, see Set up your iPhone for PingID authentication (Web).

If your organization allows you to authenticate using more than one device type, you can add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

Contact your organization for the defined policy and the options available to you.

Using swipe authentication for iPhone (legacy)

If you have the PingID app running on your mobile device and your organization is using swipe authentication, swipe for authentication to sign on to your resources.

About this task

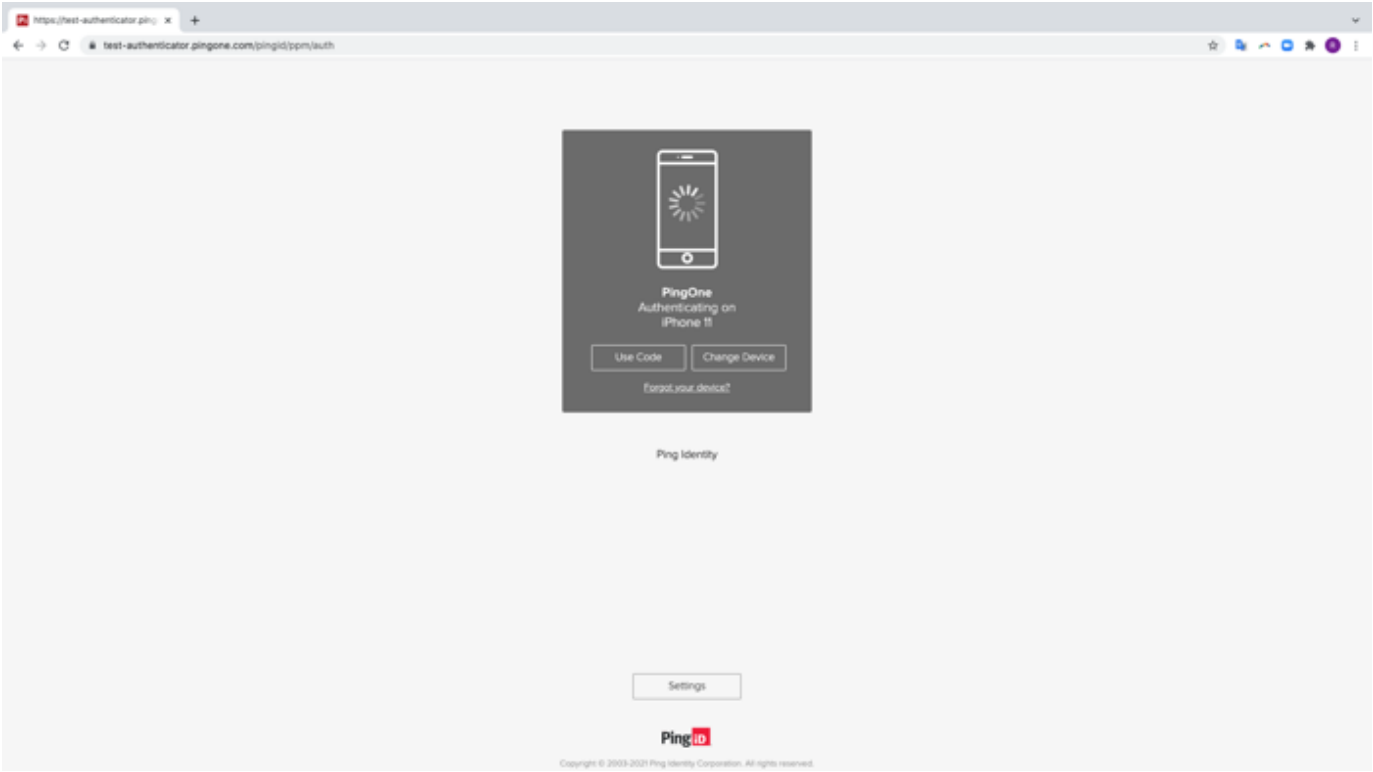
{{{ Video removed }}}

Steps

1. Sign on to your account or access an application that requires authentication.

   Result:

   The **Authenticating** window appears and an authentication notification request is sent to your device.

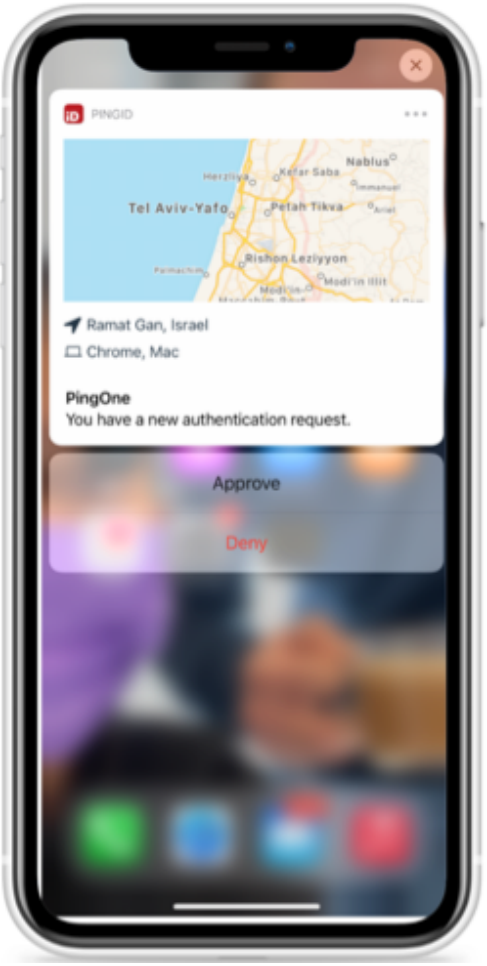


2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

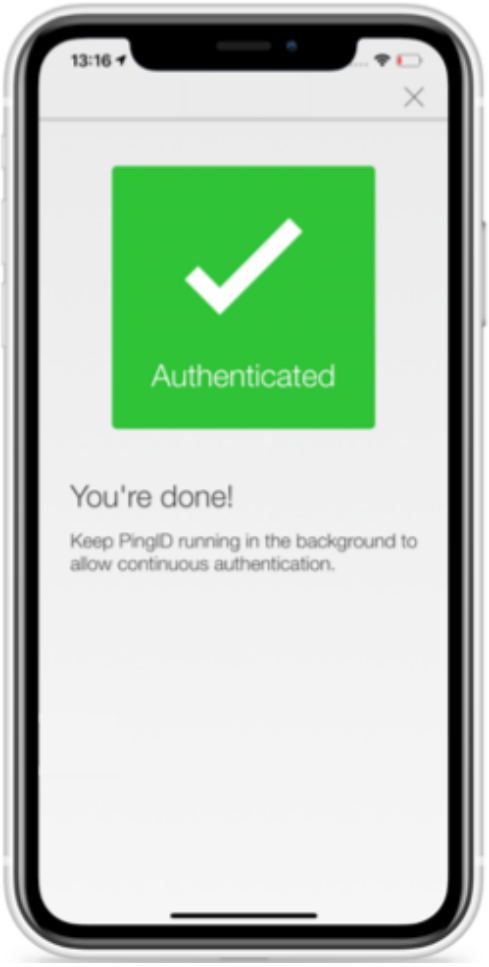
   > **Note**
   >
   > If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.



- If your mobile phone is unlocked and PingID is open, swipe to authenticate.

Result:

A green check mark appears indicating successful authentication and your access is approved. You are automatically signed on to your application.



Using biometrics authentication for iPhone (legacy)

Authenticate using your device biometrics, such as fingerprint or Face ID, with the PingIDmobile app. Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when sending the authentication request.

Before you begin

- Register your biometrics on your device, such as fingerprints or Face ID.
- Set up your iPhone for PingIDauthentication to authenticate using your device biometrics with PingID mobile app. For more information, see (legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code).

About this task

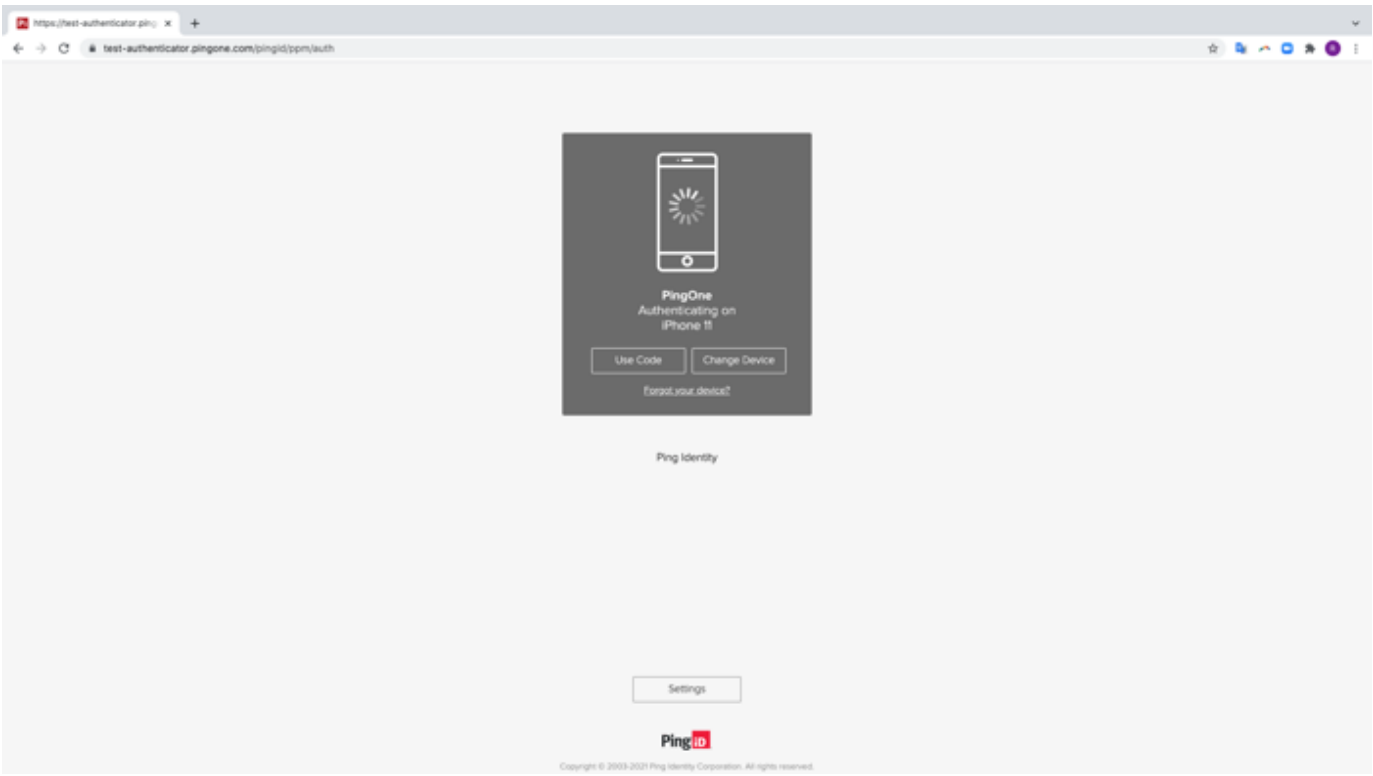
> **Note**
>
> Biometrics authentication is only available if the option is enabled by your organization.

Steps

1. Sign on to your account or access the application that requires authentication.

   Result:

The **Authenticating** window appears and an authentication notification request is sent to your device.



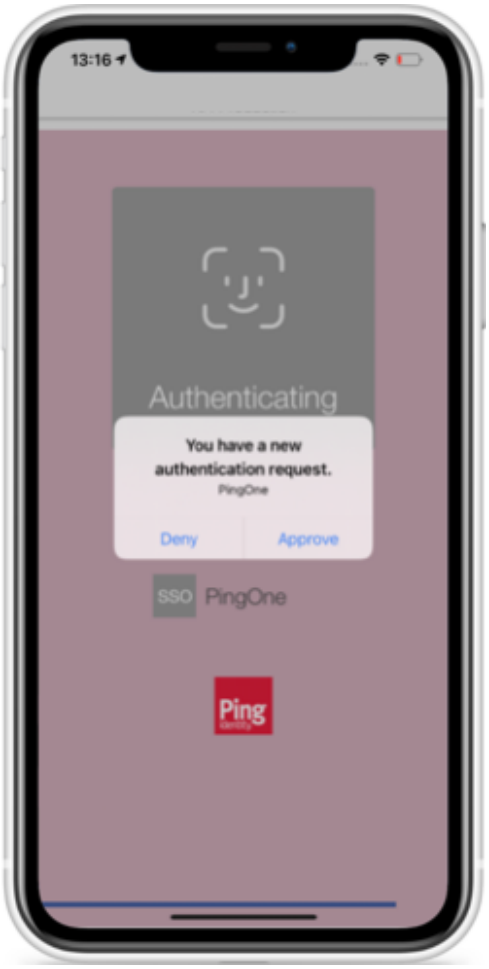
2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

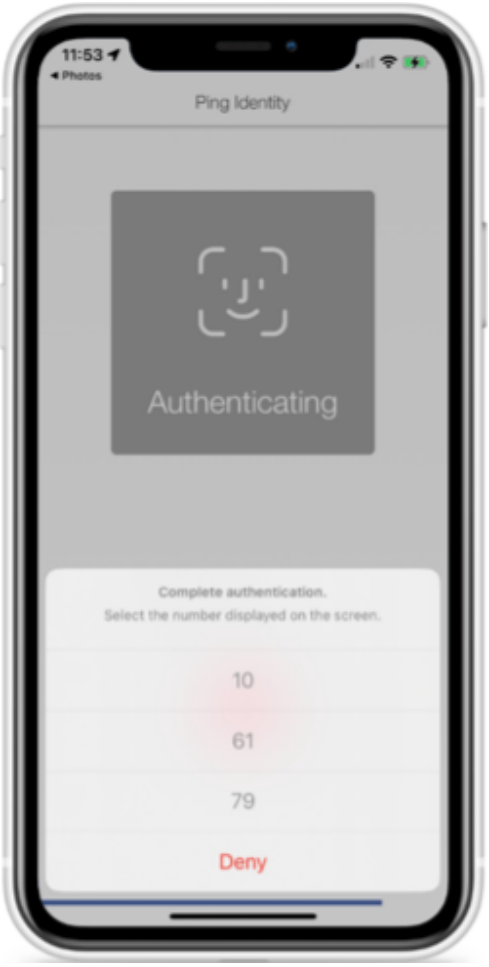
   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

     > **Note**
     >
     > If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.

   - If your mobile phone is unlocked and PingID is open, you'll be prompted to authenticate with your biometrics.
   - Face ID: Tap the message asking you to authorize scanning with Face ID, if prompted, or your face is scanned automatically.
   - Fingerprint: To scan your fingerprint, touch the Home button lightly.

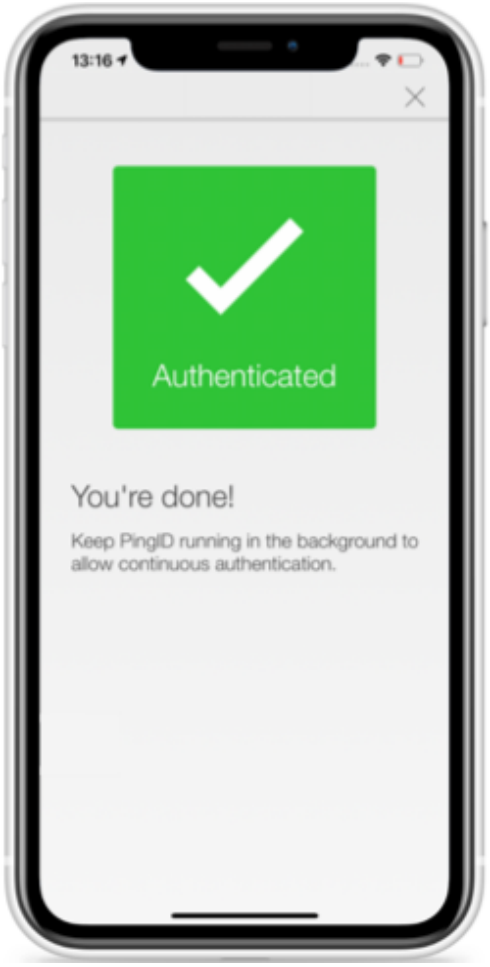


3. You might be asked to authenticate by number matching. If so, you'll see a number on the **Authentication** screen and you'll need to open PingID mobile app, and select the same number. If you don't see the option, skip this step.



Result

A green **Authenticated** message with a check mark appears, indicating successful authentication and your access is approved. You are automatically signed on to your application.



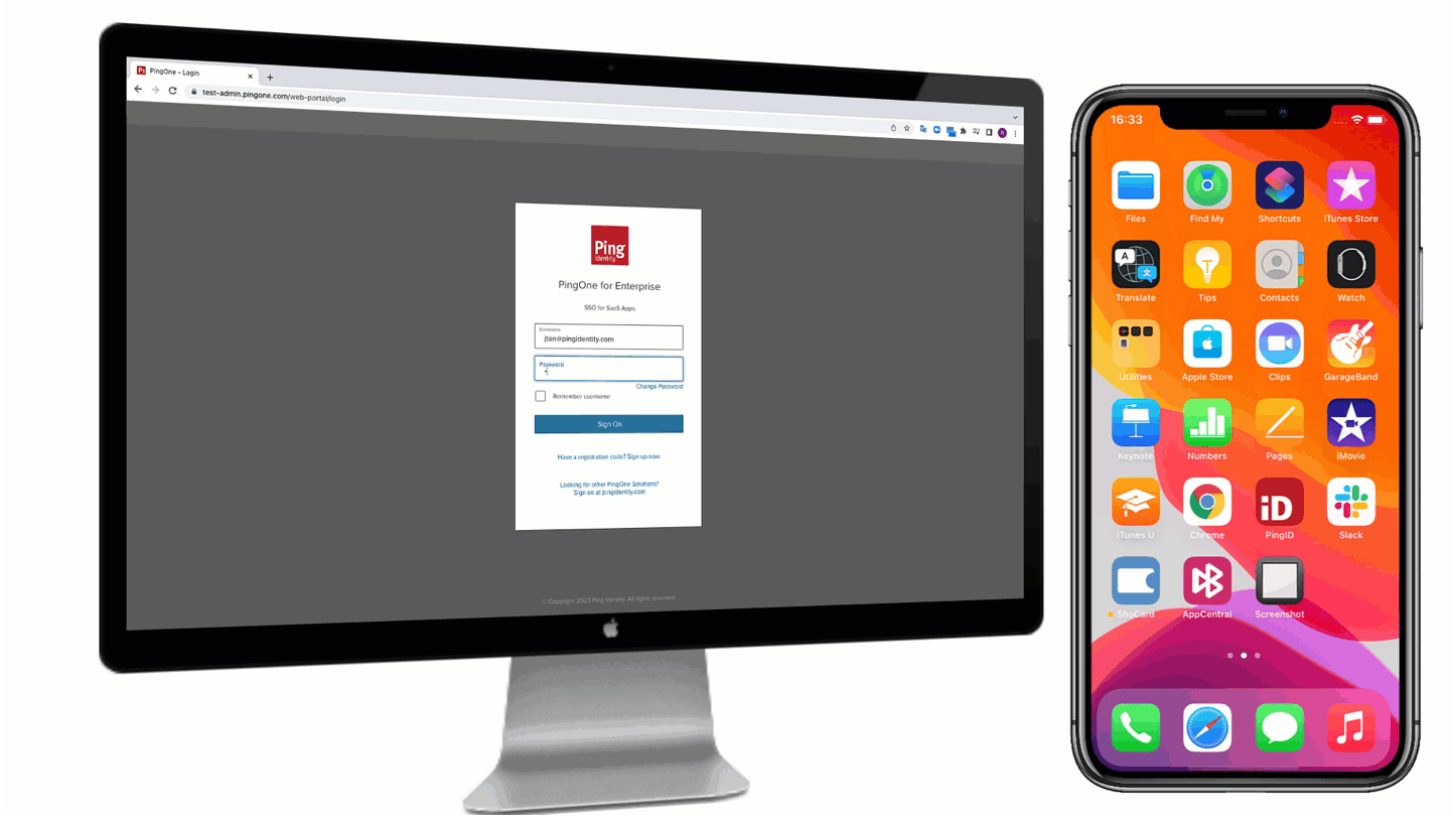
Authenticating by number matching (legacy)

You might be asked to authenticate by selecting the number in PingID mobile app that matches the number displayed on the authenticating screen.

Before you begin

- To authenticate using number matching, you need PingID mobile app 1.34 or later.

About this task



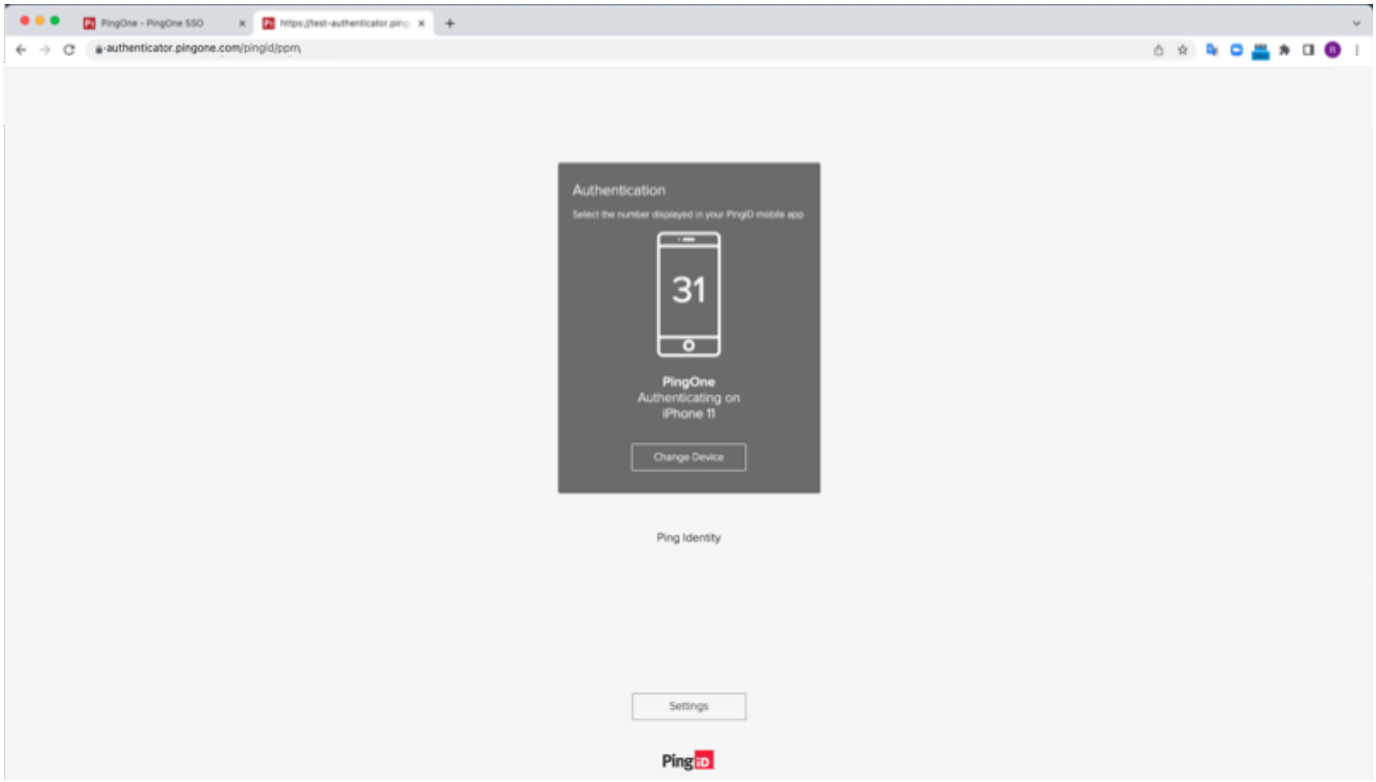
Steps

1. Sign in to your account, or access the application that requires authentication.

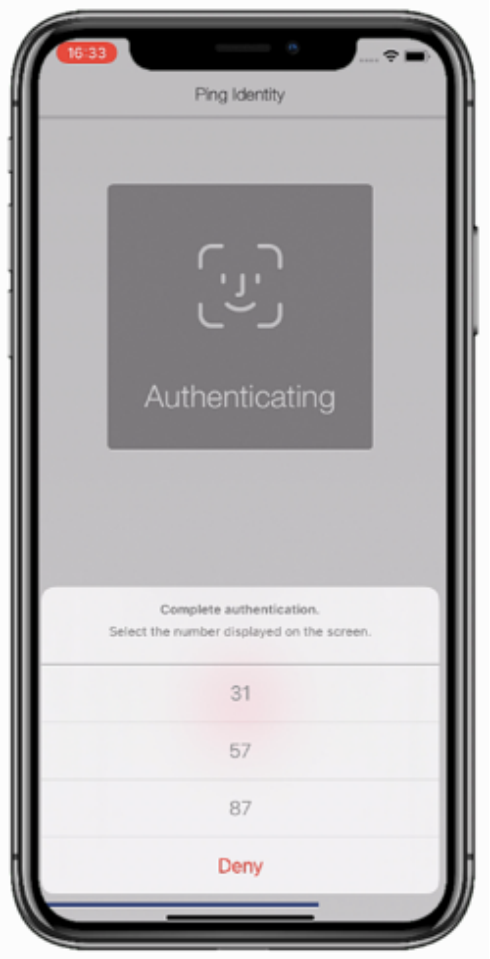
> **Note**
>
> If your device supports biometrics authentication, you might be asked to authenticate using your biometrics before you are asked to authenticate by number matching.

Result:

The Authentication window displays a number, and a message asking you to select the same number in PingID mobile app.

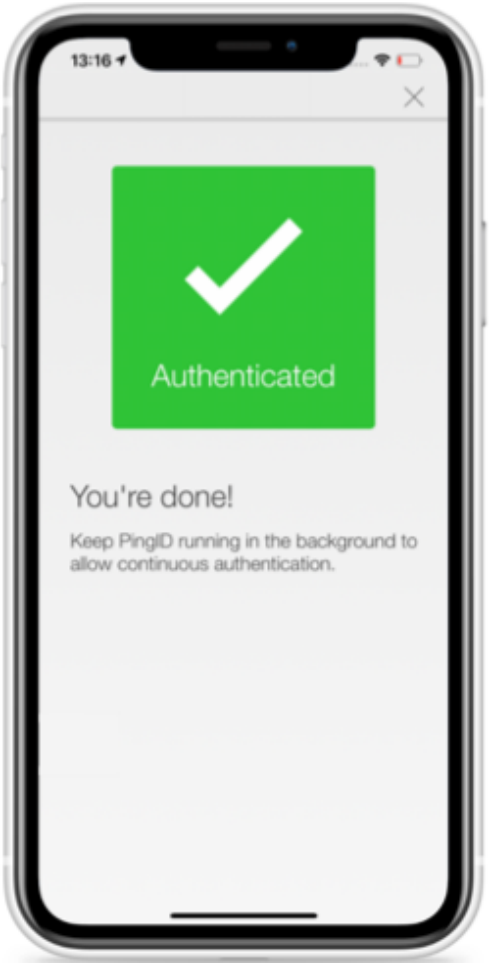


2. Open PingID mobile app and select the number that matches the number shown on the **Authentication** screen.



Result:

A green check mark appears indicating successful authentication and your access is approved. You are automatically signed on to your application.



Authenticating with PingID using a one-time passcode (legacy)

If you do not have internet access and cannot authenticate online, use the PingID mobile app to generate a one-time passcode (OTP) for you to authenticate with to access your account and applications.

About this task

Depending on your organization policy, you can either authenticate immediately using an OTP, or you need to wait for the push notification request to timeout before you are able to enter the OTP.

Each time you launch the PingID app, PingID generates a new passcode. Each passcode is unique and can only be used one time. For authentication, use the OTP that appears on your device at the time you are signing on to your account.

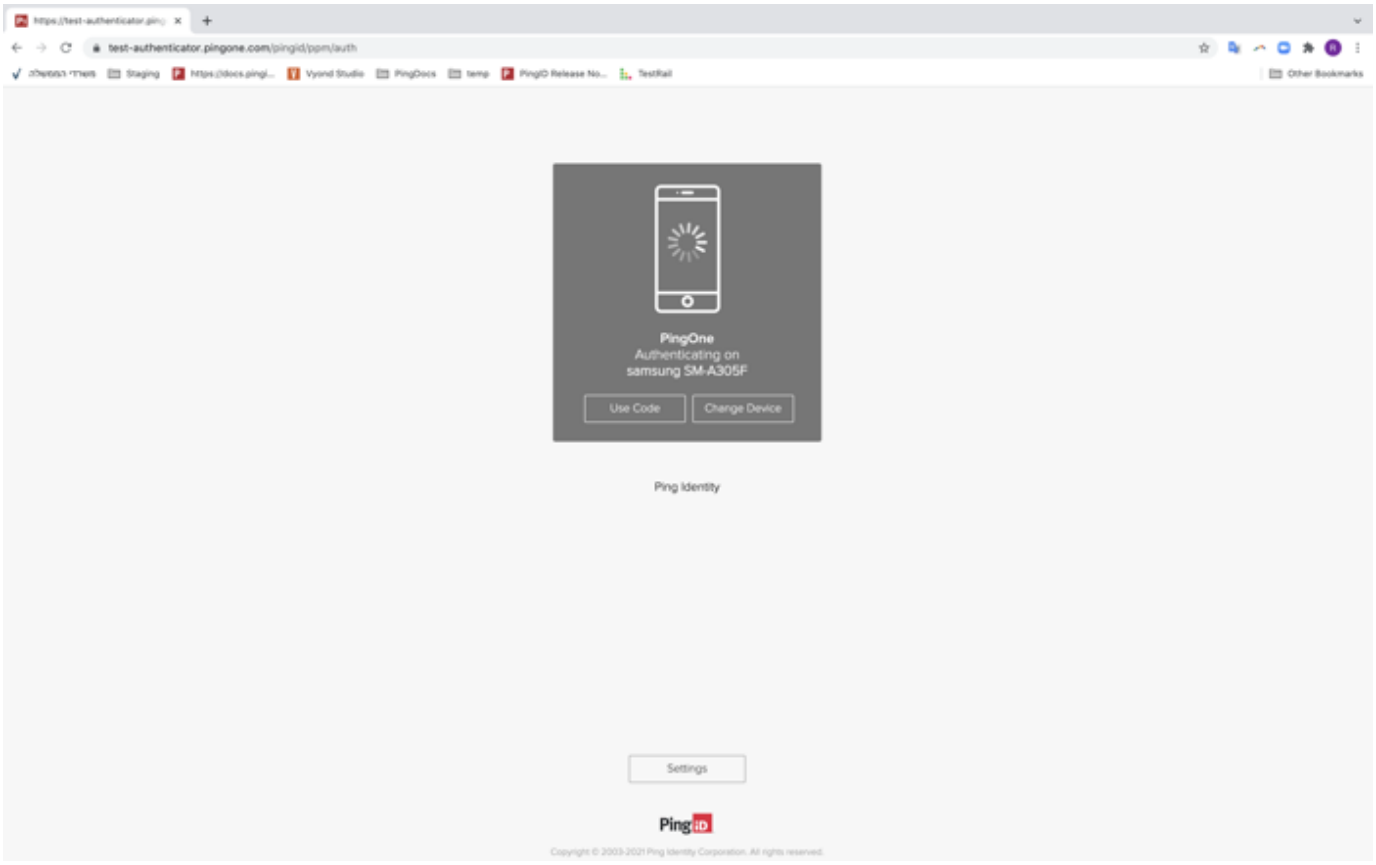
> **Note**
>
> You can only view and use the OTP if it is enabled by your organization.

Steps

1. Sign on to your account or app.

   Result:

   The **Authenticating on...** window appears.



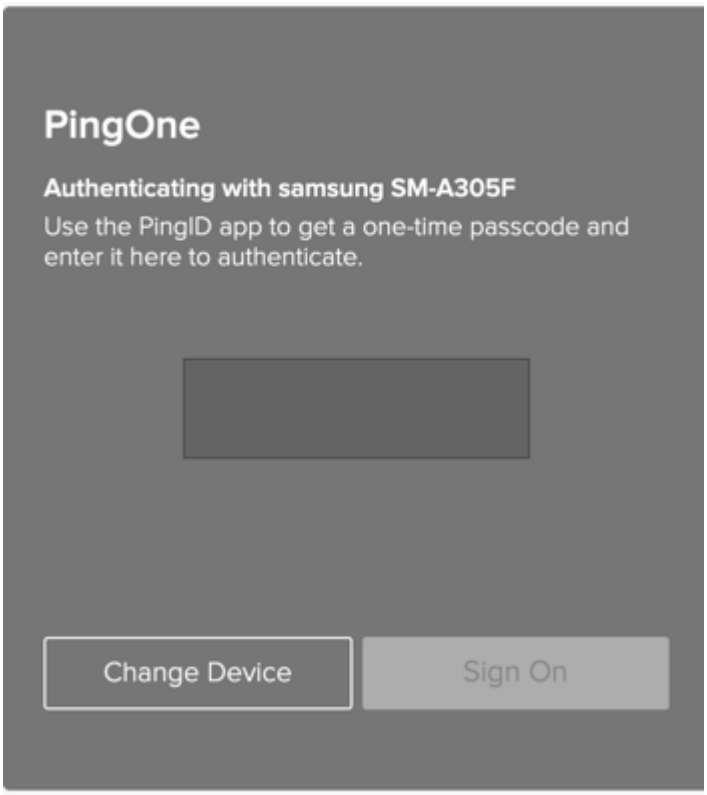
2. In the **Authentication** window either:

   Choose from:

   - Click **Use Code**
   - Wait until the push notification timeout occurs.

     Result:

     You are prompted to enter an OTP.



3. On your mobile device, open the PingID app to view the current OTP.

> **Note**
>
> - The OTP refreshes each time you open the PingID app. To generate a new one-time passcode, tap **New Passcode**.
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

4. In the **Authentication** window, enter the OTP into the passcode field. Click **Sign On**.

> **Note**
>
> If you receive a push notification on your mobile device before signing on using the OTP, you can still approve the authentication request using swipe or biometrics.

Result

A green **Authenticated** message with a check mark appears, indicating authentication is successful and your access is approved.

Authenticating using your Apple Watch (legacy)

You can authenticate with PingID mobile app using your Apple watch. For current content, see Authenticating using a smart watch.

About this task

If you have an Apple Watch paired with your iPhone, the PingID mobile app automatically presents the **Approve** or **Deny** authentication notification on the Apple Watch, in parallel with your iPhone, so you can authenticate without taking your iPhone out of your pocket.

> **Note**
>
> You do not need to install the PingID app on your Apple watch to receive notifications. However, if you do install the app on your watch, you can also access a one-time passcode (OTP) from the app on your Apple watch.

Steps

1. If your mobile device is inactive and your Apple Watch is on your wrist, when you sign on, a notification appears on your Apple Watch, as well as your mobile device.Swipe up to view the message, and then tap **Approve**.

2. If you see three numbers displayed on your Apple Watch, your company also requires you to authenticate by number matching. If so, to complete authentication, select the number on your Apple watch that matches the number displayed on the **Authentication** screen.

Result

You'll see the green checkmark, indicating authentication is successful and you're signed in to your account.

Enabling and disabling passcodes on your Apple watch

Enable the use of PingID one-time passcodes (OTPs) on your Apple watch.

About this task

If you have installed the PingID app on your device, the PingID Apple Watch app is automatically installed on your watch and you will start receiving notifications to your watch. You can also open the PingID app on your watch to receive a one-time passcode (OTP). If the Apple watch app is disabled, you will not be able to access a one-time passcode from your watch.

> **Note**
>
> The Apple watch only receives notifications when your mobile device is locked, and the mobile device screen is in sleep mode.

Steps

1. On your iPhone, tap the Watch app, and then tap **PingID**.
2. To enable or disable the app on your Apple watch, tap **Show App on Apple Watch**.

   Result:

   The PingID app is installed on your Apple watch, and the PingID icon appears.
3. To view the current one-time passcode, on your Apple watch, tap the PingID icon.

4. (Optional) To get a new passcode, tap **Refresh**.

Authenticating with PingID manually (legacy)

When you sign on to your account using a web browser, you might be asked to authenticate manually through the PingID mobile app.

You will not be asked to authenticate manually often, but be aware that authenticating manually is different than the normal sign on process.

- If you want to access resources on your computer and authenticate through your mobile device, see Authenticating manually to access resources on your computer (legacy).
- If you want to access resources on your mobile device and also authenticate using that same device, see Authenticating manually to access resources on your mobile device (legacy).

Authenticating manually to access resources on your computer (legacy)

When you sign on to your account using a web browser, you might be asked to authenticate manually through the PingID mobile app.

Before you begin

To authenticate manually to access resources on your computer, you need:

- A device with the PingID mobile app 1.8 or later that is already paired with your account and with which you have successfully authenticated at least once.
- A working camera on your device with the PingID mobile app camera permissions set to **Approve**. See PingID mobile app management.

About this task

You will not be asked to do this very often, but be aware that authenticating manually differs from the normal sign on process.
brightcove::2DBsmx9[start='34s', autoplay=true, accountID="771836189001", width=768, height=432]

> **Note**
>
> You cannot sign on to your account from a web browser that is located on the same device that you use to authenticate, unless it is a mobile device that is paired with the PingID mobile app. If you are trying to access resources on your mobile device, see Authenticating manually to access resources on your mobile device (legacy).

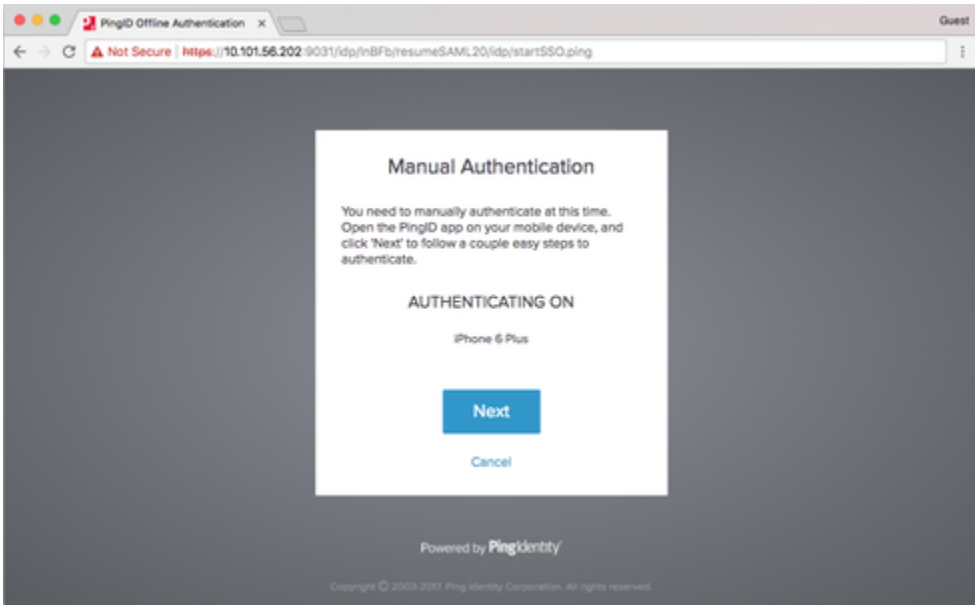
Steps

1. Sign on to your account, or access the application that requires authentication.

   If you have more than one device paired with your account, you'll see a list of your devices. Select the device you want to use to authenticate.

   Result:

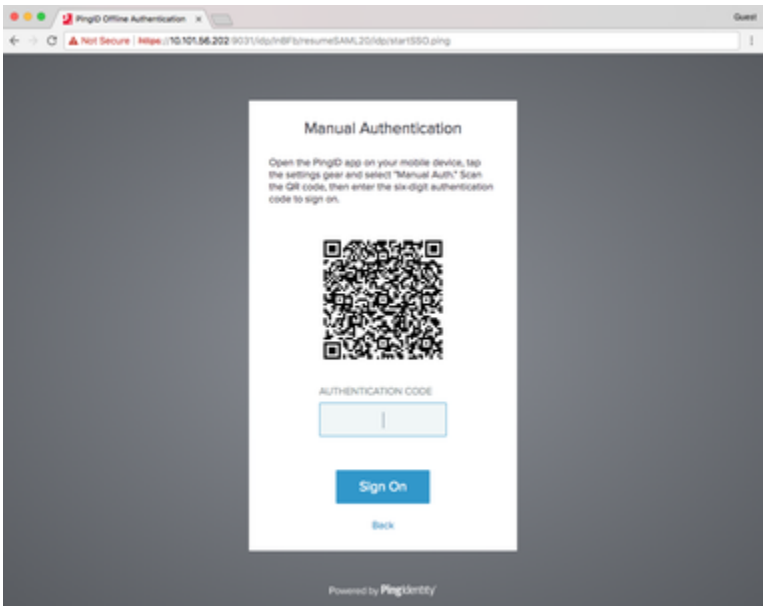
   A **Manual Authentication** message appears, requesting that you manually authenticate.



2. Click **Next**.

   Result:

   A **Manual Authentication** message appears, displays a QR code, and requests that you authenticate manually.



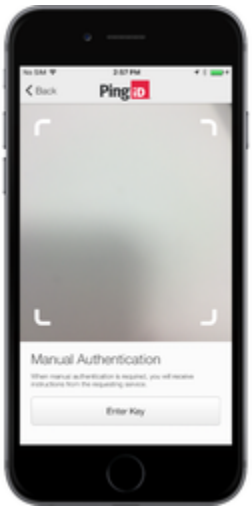
3. From your mobile device, open the PingID app.

4. Tap the **Gear** icon ( ) and select **Manual Auth**.

Result:

If required, authenticate with your device biometrics. The QR code scanner for manual authentication opens.

5. Use your mobile to scan the QR code displayed on the **Manual Authentication** screen.



Result:

You receive an **Authentication Code**.

6. Enter the **Authentication Code** into your web browser. Click **Sign on**.

Result

You are successfully authenticated and automatically signed on to your account.

Authenticating manually to access resources on your mobile device (legacy)

When you sign on to your account using a web browser, you might be asked to authenticate manually using the PingID mobile app.

Before you begin

To authenticate manually from your mobile device to access resources on the same device, you need:

- A device with PingID mobile app 1.8.4 or later, that is already paired with your account and with which you have successfully authenticated at least once.

About this task

You will not be asked to authenticate manually often, but be aware that authenticating manually is slightly different than the normal sign on process.

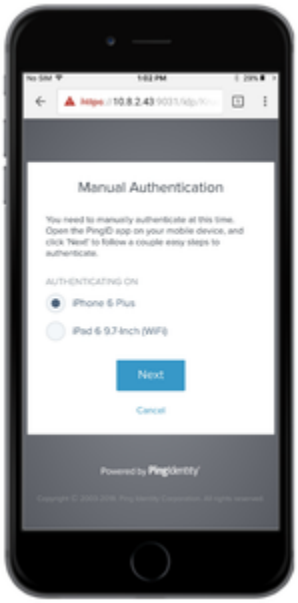
Steps

1. From a mobile device that is paired with PingID, open a browser window and sign on to your account, or access the application that requires authentication.

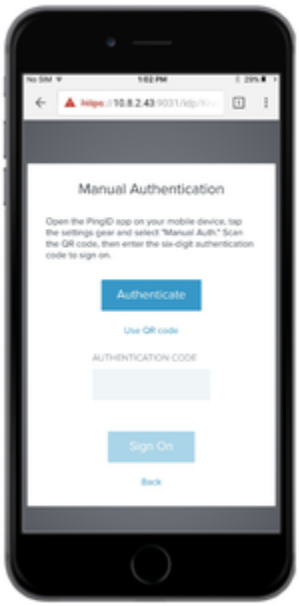
   If you have more than one device paired with your account, a list of all your currently paired devices appears. Select the device you want to use to authenticate.

   Result:

   A **Manual Authentication** message appears with the **Authenticating On** section and the **Next** option.



2. Click **Next**.



> **Note**
>
> If you are trying to access resources on a device that is not your authenticating device, such as a different mobile device or an iPad that is not paired with PingID, click **Use QR Code**, and follow the steps outlined in Authenticating manually to access resources on your computer (legacy).

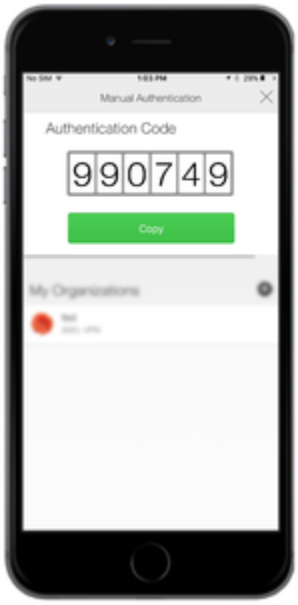
Result:

A **Manual Authentication** message appears.

3. Tap **Authenticate**, and authenticate with your device biometrics, if required.

Result:

PingID mobile app opens automatically, and you receive an **Authentication Code**.



4. Tap **Copy**, and then return to your web browser.

5. In the web browser, tap the **Authentication Code** field and paste the code into the field. Click **Sign on**.

Result

You are successfully authenticated and signed on to your account or app.

Authenticating using your Android (Web) (legacy)

This section covers the options available for authenticating using your Android when accessing your account or app using a web browser.

Depending on your organization's configuration, you can usePingID mobile app to authenticate using the following options:

- Using swipe authentication for Android

- Using biometrics authentication for Android
- Authenticating by number matching
- Authenticating using a one-time passcode
- Authenticating using your Android watch
- Authenticating manually

If you have not yet paired PingID mobile app with your account, see Set up your Android for PingID authentication (Web).

If your organization allows you to authenticate using more than one device type, you can also add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

> **Note**
>
> The options available to you are defined by your organization's policy.

Using swipe authentication for Android (legacy)

If you have the PingID app running on your mobile device and your organization is using swipe authentication, swipe for authentication to sign on to your resources.

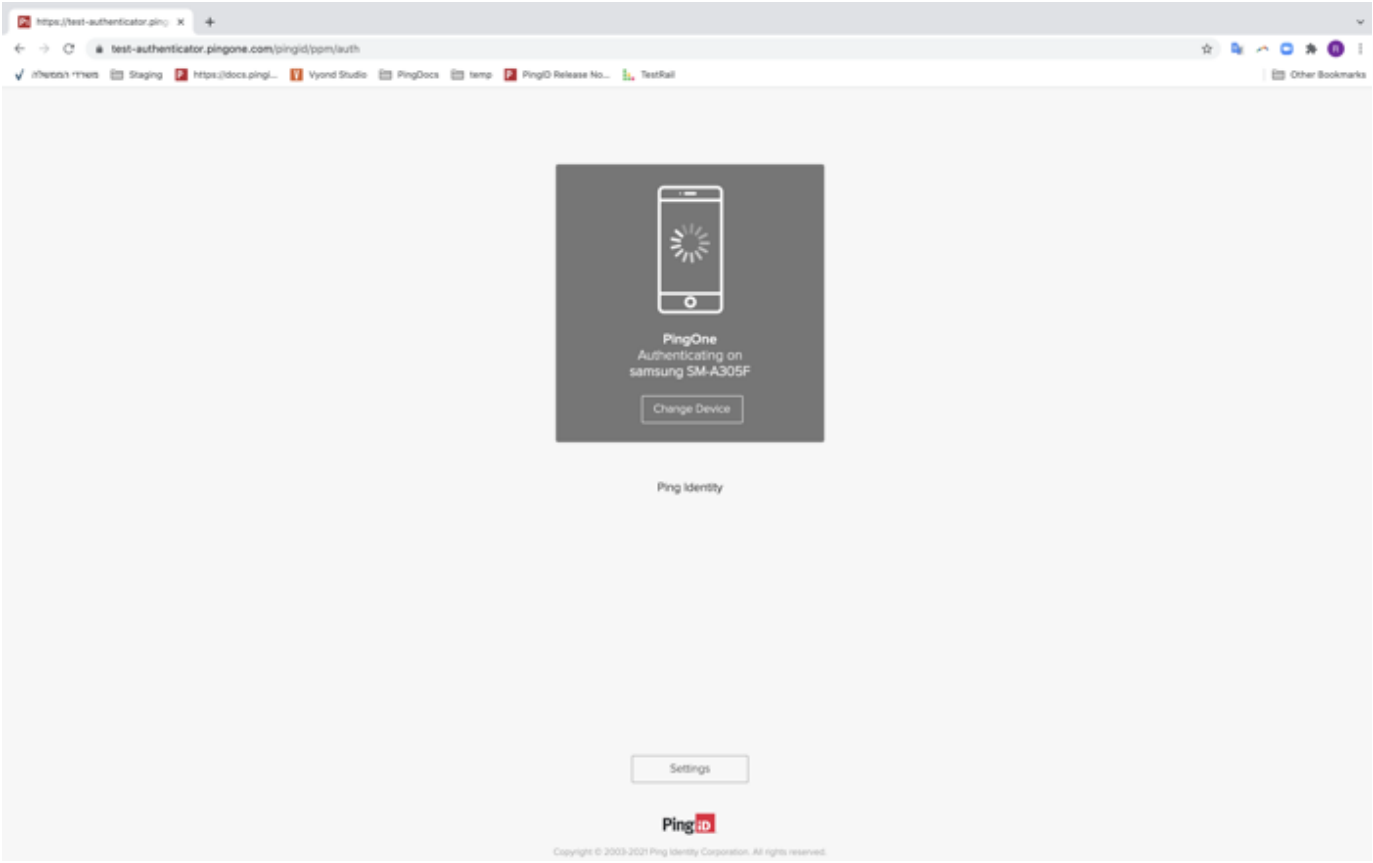
About this task

If you have the PingID app running on your mobile device, and your organization is using swipe authentication, when logging in to your resources, you'll be prompted to swipe to authenticate.

> **Note**
>
> The authentication process may vary slightly depending on the Android version and the notification settings on your device. Some Android versions may give you the option to approve the push notification from the lock screen.

Steps

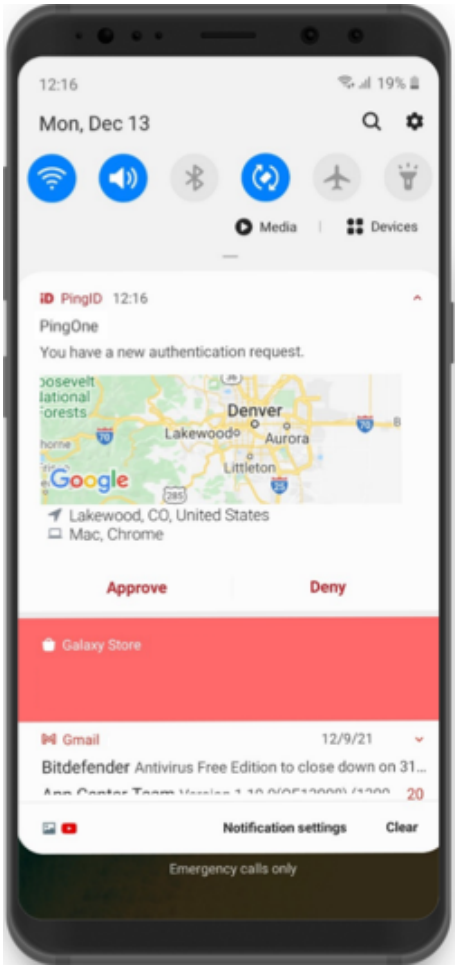
1. Sign on to your account, or access the application that requires authentication. You'll see the **Authenticating** screen, and an authentication notification request is sent to your device.



2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.



Note

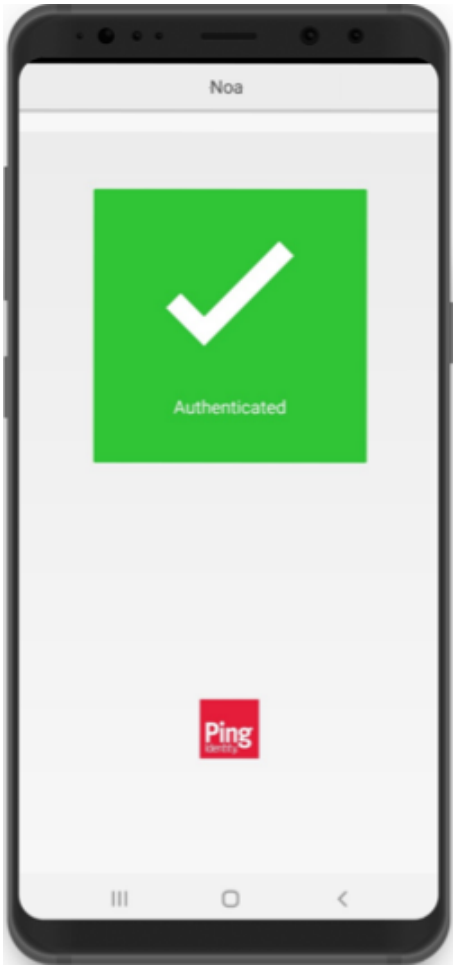
- If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.
- For Android version 10 and later, you must unlock your device to authenticate.

◦ If PingID mobile app opens showing the swipe screen, swipe up to authenticate.

> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

You'll see the green check mark on your mobile indicating your access is approved, and PingID closes.



Using biometrics authentication for Android (legacy)

Authenticate using your device biometrics, such as fingerprint or Face recognition, with the PingIDmobile app. Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when sending the authentication request.

Before you begin

You'll need to register your biometrics on your device and then pair your Android device so you can authenticate using biometrics.

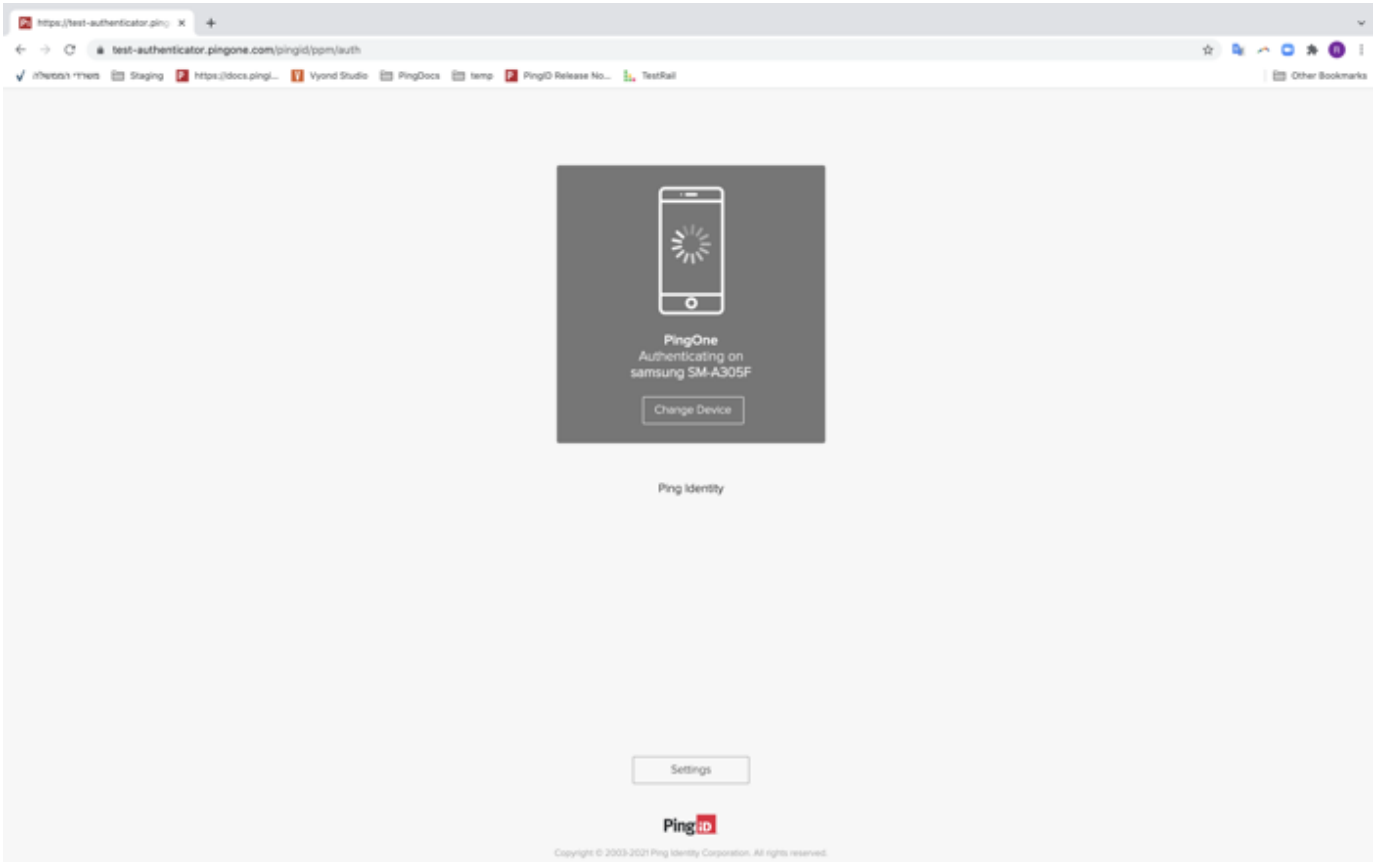
About this task

Note

- Biometrics authentication is only available if the option is enabled by your organization.
- The authentication process may vary slightly depending on the Android version and the notification settings on your device. (The images shown here relate to a Samsung device. Actual implementation may vary according to device model.)
- Some Android devices do not support face or iris authentication with PingID. If you are not able to authenticate with face or iris authentication, we recommend using fingerprint authentication (see also Troubleshooting PingID authentication).

Steps

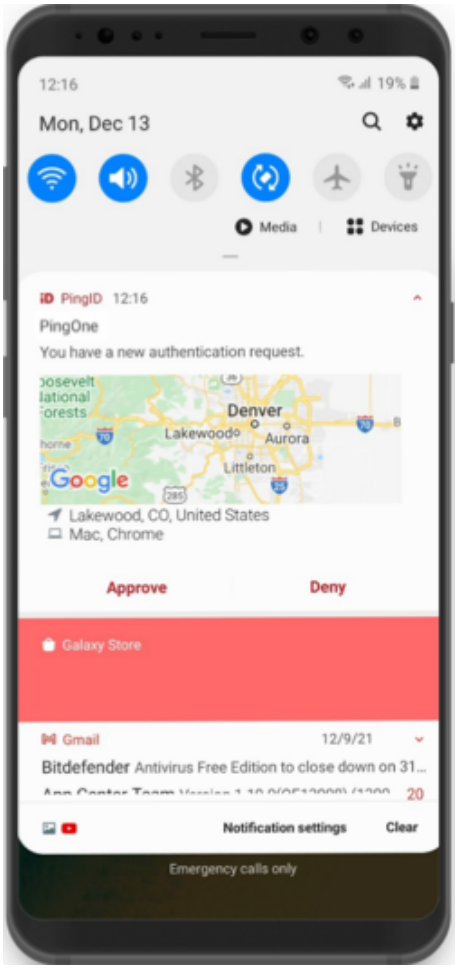
1. Sign in to your account, or access the application that requires authentication. You'll see the **Authenticating** screen, and an authentication notification request is sent to your device.



2. Accept the authentication notification, depending on your mobile's notification settings:

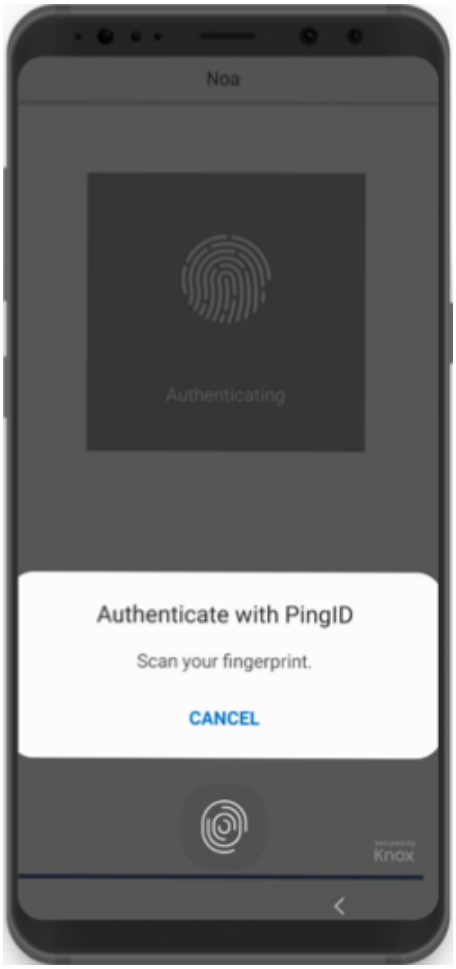
   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.



> **Note**
>
> - If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.
> - For Android version 10 and higher, you must unlock your device to authenticate.

- If PingID mobile app opens, authenticate using your biometrics.

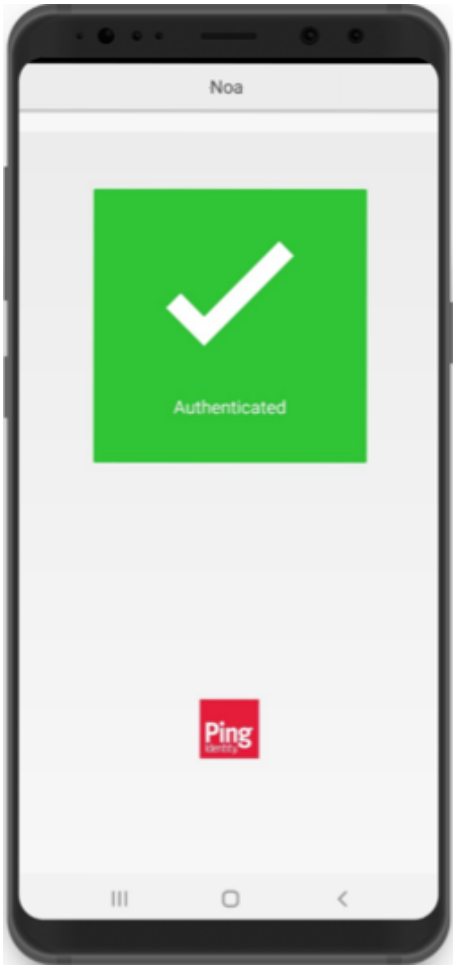


> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

3. You might be asked to authenticate by number matching. If so, you'll see a number on the **Authentication** screen and you'll need to open PingID mobile app, and select the same number. If you don't see the option, skip this step.

Result

You'll see the green checkmark on your mobile indicating your access is approved, and PingID closes.



Authenticating with PingID using a one-time passcode (legacy)

If you do not have internet access and cannot authenticate online, use the PingID mobile app to generate a one-time passcode (OTP) for you to authenticate with to access your account and applications.

About this task

Depending on your organization policy, you can either authenticate immediately using an OTP, or you need to wait for the push notification request to timeout before you are able to enter the OTP.

Each time you launch the PingID app, PingID generates a new passcode. Each passcode is unique and can only be used one time. For authentication, use the OTP that appears on your device at the time you are signing on to your account.

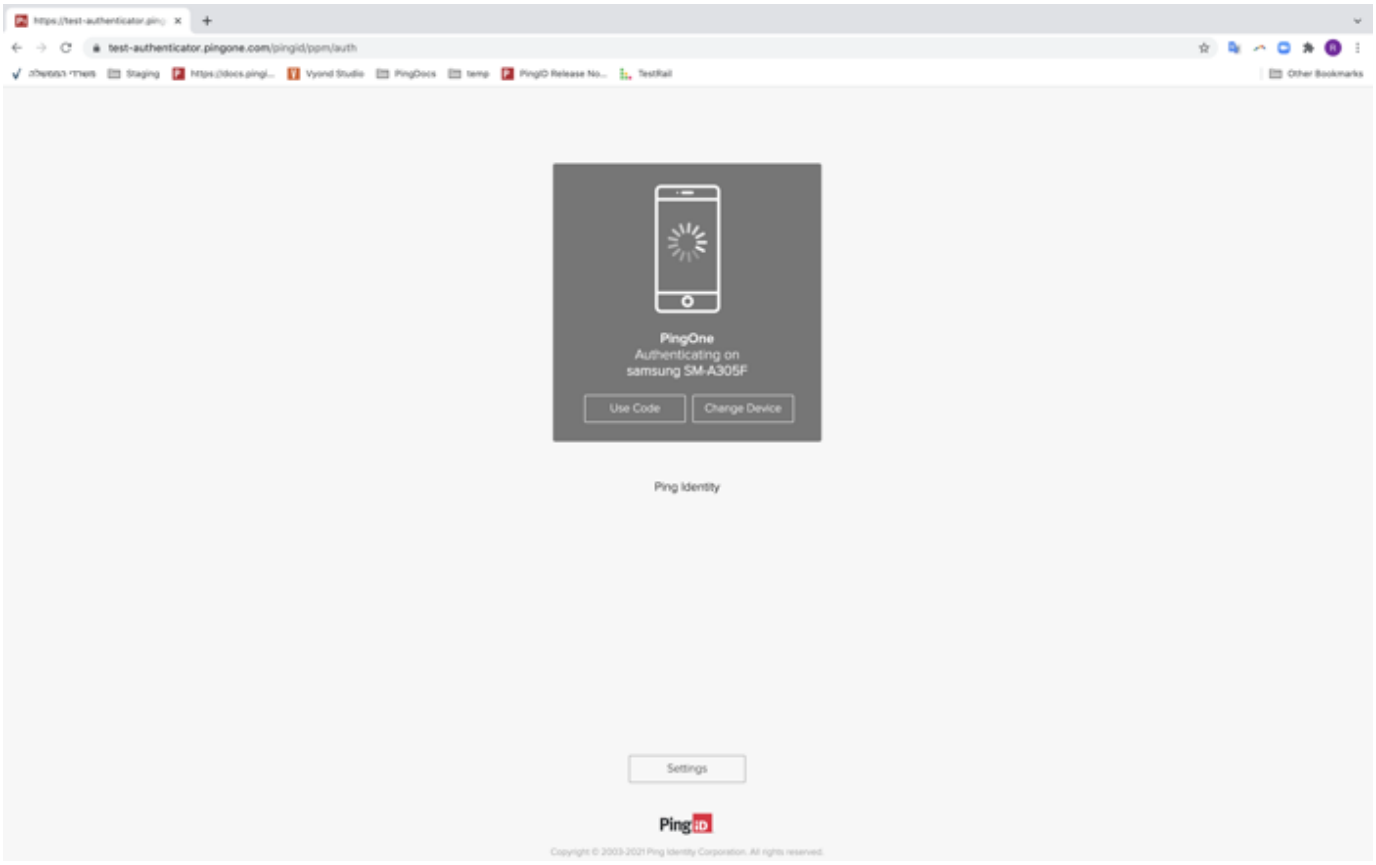
> **Note**
>
> You can only view and use the OTP if it is enabled by your organization.

Steps

1. Sign on to your account or app.

   Result:

   The **Authenticating on...** window appears.



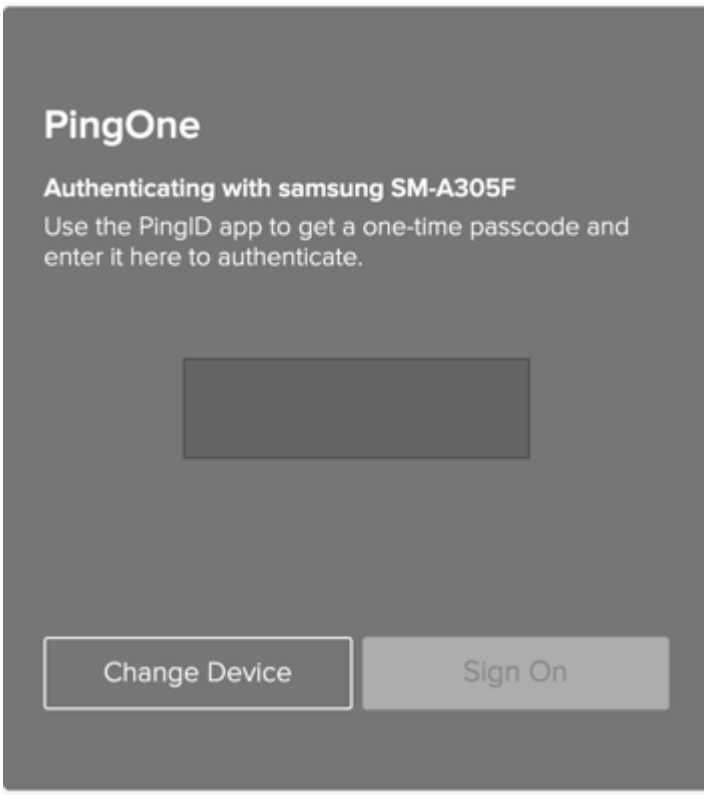
2. In the **Authentication** window either:

   Choose from:

   - Click **Use Code**
   - Wait until the push notification timeout occurs.

     Result:

     You are prompted to enter an OTP.



3. On your mobile device, open the PingID app to view the current OTP.

> **Note**
>
> - The OTP refreshes each time you open the PingID app. To generate a new one-time passcode, tap **New Passcode**.
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

4. In the **Authentication** window, enter the OTP into the passcode field. Click **Sign On**.

> **Note**
>
> If you receive a push notification on your mobile device before signing on using the OTP, you can still approve the authentication request using swipe or biometrics.

Result

A green **Authenticated** message with a check mark appears, indicating authentication is successful and your access is approved.

Authenticating using your Android watch (legacy)

You can authenticate with PingID mobile app using your Android watch.

For current content, see Authenticating using a smart watch.

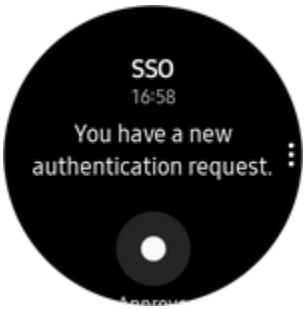
About this task

Some Android models automatically allow you to authenticate using your Android watch. If the PingID mobile app is installed on your phone, and if your Android watch model and configuration are compatible with the PingID mobile app, you'll automatically start receiving push notifications to your Android watch when your phone is locked.

> **Note**
>
> The ability to authenticate using an Android watch varies according to Android model and configuration.

Steps

1. If your Android device and configuration supports the use of Android watch for notifications, when your phone is locked, you will receive a notification to your watch automatically.



2. Swipe to authenticate.

Authenticating using your Android (VPN) (legacy)

You can authenticate to your VPN with your Android device in a variety of ways.

Use any of the following options:

- Swipe authentication for Android
- Fingerprint authentication for Android
- Authenticate using your Android watch
- Authenticate using a one-time passcode
- Authenticate manually

> **Note**
>
> The options available to you are defined by your organization's policy.

If your organization allows you to authenticate using more than one device type, you can also add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

Using swipe authentication for Android (VPN)

If you have the PingID app running on your mobile device and fingerprint authentication is not enabled, swipe to authenticate for your Android device.

About this task

> **Note**
>
> The authentication process might vary slightly depending on the Android version and the notification settings on your device. Some Android versions give you the option to approve the push notification from the lock screen.

Steps

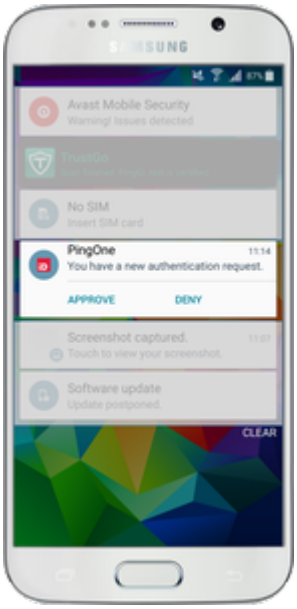
1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.

    If you have more than one device paired with your account, a message appears, displaying a list of all your currently paired devices.

    1. For multiple devices only: enter the number of the device you want to use to authenticate.
    2. Click **Sign In**.

        Result:

        An authentication notification is sent to your device.
2. On your device, either:
    - If a PingID notification is shown, approve the notification.

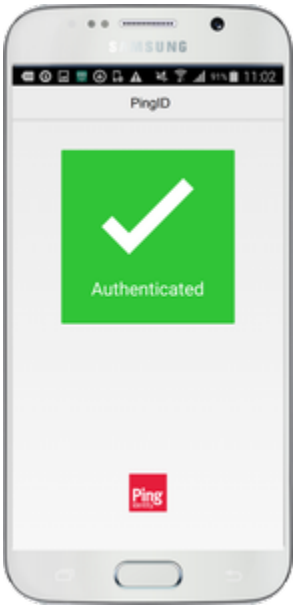


- If the PingID mobile app opens, swipe up when prompted to do so.

> **Note**
>
> - For Android version 10 and earlier, you must unlock your device to authenticate.
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

A green **Authenticated** message with a check mark appears, indicating successful authentication and PingID closes. You are automatically signed on to your VPN.



Using biometrics authentication for Android (VPN)

Biometrics authentication is simple using a mobile device. Authentication varies slightly depending on your settings and whether your device is locked or unlocked when the authentication request sends.

Before you begin

- Register your biometrics on your device.
- Set up your mobile device for VPN authentication. See (legacy) Pairing PingID mobile app for authenticating to your company's VPN.

About this task

> **Note**
>
> Biometrics authentication is only available if your organization enables the option.
> The authentication process might vary slightly depending on the Android version and the notification settings on your device.
> The images shown here relate to a Samsung device. Actual implementation might vary according to device model.

Steps

1. From your web browser or application:
    1. Sign on to your VPN with your username and password.
    2. Click **Sign In**.

       Result:

       If you have more than one device and your organization policy allows it, a message appears showing all of your devices in a numbered list.
    3. For multiple devices only: enter the number of the device you want to use to authenticate and click **Sign In**.

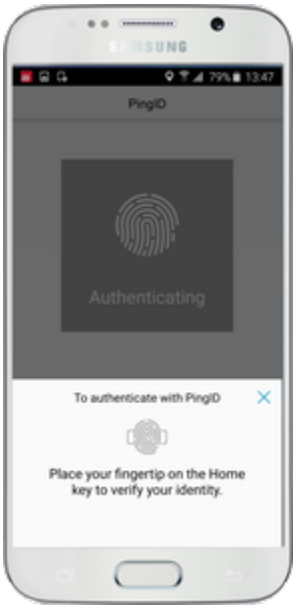
Result:

A message displays requesting that you authenticate, and an authentication notification is sent to your device.

2. On your device, if a PingID notification is shown, approve the notification.

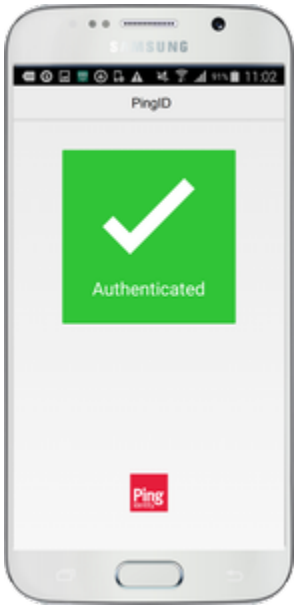
> **Note**
>
> - For Android version 10 and earlier, you must unlock your device to authenticate.
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

3. Scan your biometrics when prompted to do so.



Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful. You are signed on to your VPN.



Authenticating using a one-time passcode (VPN)

If you do not have internet access temporarily, you can still authenticate using the PingID mobile app by generating a one-time passcode (OTP).

About this task

The OTP is unique and can only be used once. Only the OTP that appears on your device at the time that you sign on to your account is valid for authentication.

> **Note**
>
> If permitted by your organization's policy, you can view and use the OTP.

Steps

1. From your web browser or application:
    1. Sign on to your VPN with your username and password.

        > **Note**
        >
        > If you have more than one device, and your organization policy allows it, a message displays showing all of your devices in a numbered list.

    2. For multiple devices only: enter the number of the device you want to use to authenticate.
    3. Click **Sign In**.
2. On your mobile device, open the PingID app to view the current OTP.

    > **Note**
    >
    > When you open PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

The OTP refreshes each time you open the PingID app. To generate a new OTP, tap **New Passcode**.

3. Enter the OTP into the text field. Click **Sign In**.

Result

After you have successfully authenticated, you are signed on to your VPN.

Authenticating manually (VPN)

When you sign on to your VPN, you might be asked to authenticate manually using the PingID mobile app.

Before you begin

To authenticate manually you need the following:

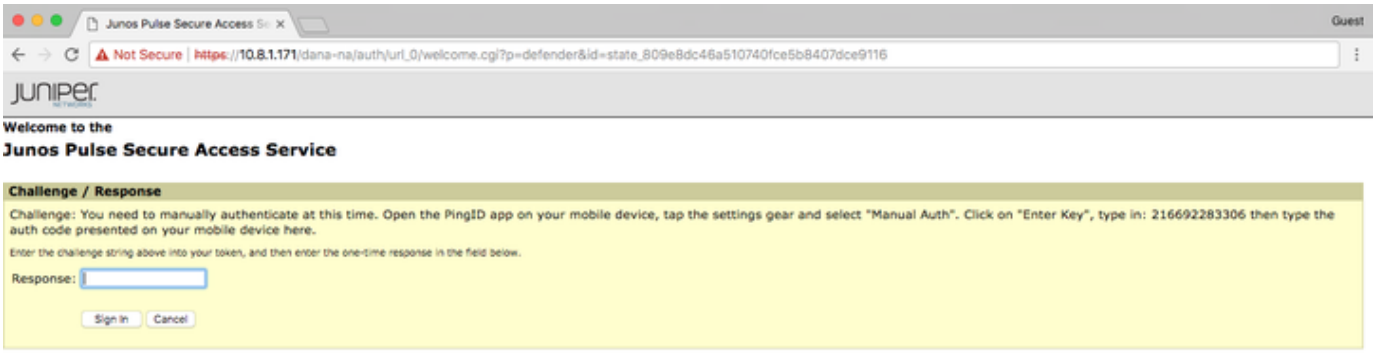
A device with the PingID mobile app 1.8 or later that is already paired with your account and with which you have successfully authenticated at least once.

About this task

You will not be asked to authenticate manually often, but be aware that authenticating manually is different than the normal sign on process.

Steps

1. Sign on to your VPN.



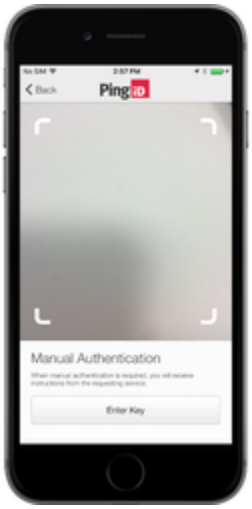
Result:

A **Manual Authentication** message appears, displaying a 12-digit key, and requests that you authenticate manually.

2. From your mobile device, open the PingID mobile app.
3. Tap the **Gear** icon ( ) and select **Manual Auth**. Authenticate with your device biometrics, if required.

Result:

The **Manual Authentication** screen opens.



4. Tap **Enter Key**.
5. In the **Security Key** field, enter the 12-digit key displayed on the VPN sign on page, and tap **Verify**.

Result:

You receive an authentication code.

6. In the VPN **Response** field, enter the **Authentication Code**. Click **Sign In**.

   Result:

   You are successfully authenticated and signed on to your VPN.

Authenticating using your iPhone (VPN) (legacy)

This section covers the options available for authenticating to your VPN using your iPhone.

You can authenticate using the following options:

- Swipe authentication for iPhone
- Fingerprint authentication for iPhone
- Authenticate using your Apple watch
- Authenticate using a one-time passcode

- Authenticate manually

If your organization allows you to authenticate using more than one device type, you can also add a device and decide which device you want to use as your primary (default) authentication method. See Managing your devices.

The options available to you are defined by your organization's policy.

Using swipe authentication for iPhone (VPN)

If you have the PingID app running on your mobile device and biometrics authentication is not enabled, you are prompted to swipe to authenticate.

Steps

1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.

    If you have more than one device and your organization policy allows, a message appears showing all of your devices in a numbered list.

    1. For multiple devices only: enter the number of the device you want to use to authenticate.
    2. Click **Sign In**.

        Result:

        A message displays requesting that you authenticate, and an authentication notification is sent to your device.

        > **Note**
        >
        > When you open PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

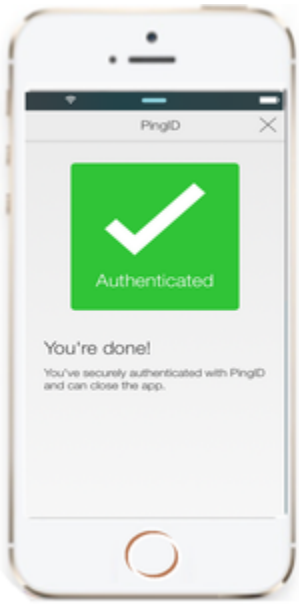
2. Depending on your notification settings, swipe to authenticate:

    Choose from:

    - If your device is unlocked:
        1. Tap the notification
        2. Swipe to authenticate
    - If your device is locked:
        1. Swipe left to open the authentication notification and unlock the screen.
        2. Swipe to authenticate.

Result

Thee green **Authenticated** message with a check mark appears, indicating authentication is successful, and you are signed on to your VPN.



Using biometrics authentication for iPhone (VPN)

Authenticate with your device biometrics using the PingID mobile app.

Before you begin

- Register biometrics on your device, such as fingerprints or Face ID.
- Set up your mobile device for VPN authentication to authenticate using your device biometrics.

For more information, see (legacy) Pairing PingID mobile app for authenticating to your company's VPN.

About this task

The authentication process might vary depending on whether your device is locked or unlocked when the authentication request is sent.

> **Note**
>
> Biometrics authentication is only available if the option is enabled by your organization.

Steps

1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.

    If you have more than one device and your organization's policy allows, a message appears showing all of your devices in a numbered list.

    1. For multiple devices only: enter the number of the device you want to use to authenticate.
    2. Click **Sign In**.

        Result:

        A message displays requesting that you authenticate and an authentication notification is sent to your device.

        > **Note**
        >
        > When you open PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

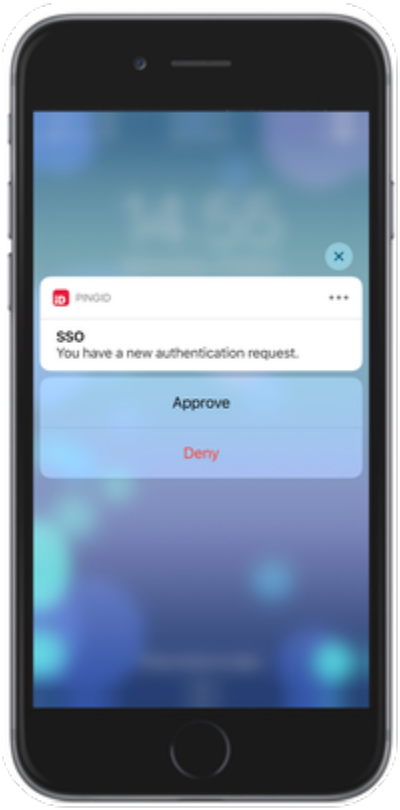
2. Depending on your notification settings, approve the authentication notification:

    Choose from:

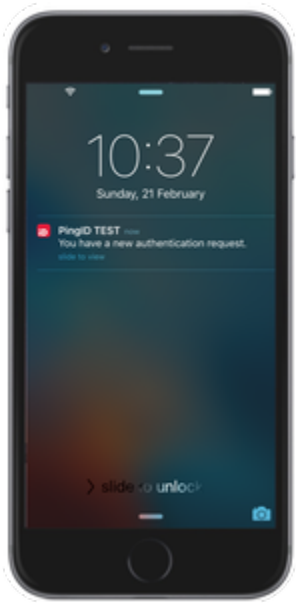
    - If your phone is unlocked:
        1. Tap the notification banner, or tap **Approve**.

- If your phone is locked:

  1. Slide the message to the left and tap **Approve**.

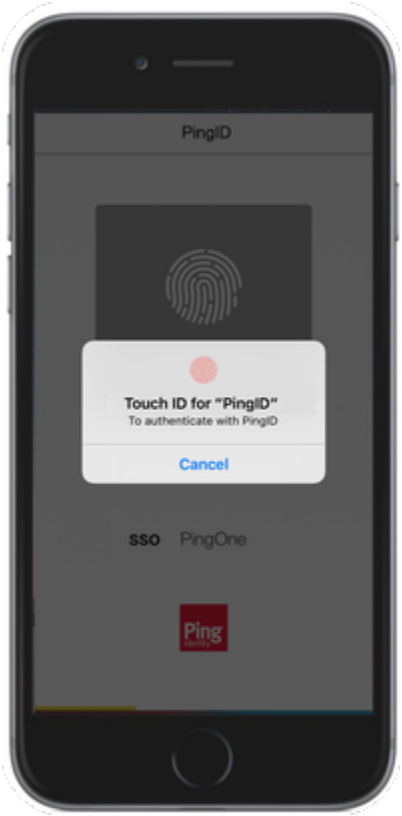


  2. If you do not have the **slide to view** option, swipe right to unlock the device.



Result:

The biometrics scan is activated and a message appears on your device prompting you to authenticate using your device biometrics.



3. Authenticate using your device biometrics:

   Choose from:

   - Face ID: Tap the popup asking you to authorize scanning with Face ID, if prompted, and otherwise your face is scanned automatically.

- Fingerprint: Touch the Home button lightly to scan your fingerprint.

> **Note**
>
> Do not press hard on the Home button, as it can cancel the authentication action, rather than approve it.

Result:

The green **Authenticated** message appears with a check mark, indicating authentication is successful, and you are signed on to your VPN.

Enabling and disabling passcodes on your Apple watch

Enable the use of PingID one-time passcodes (OTPs) on your Apple watch.

About this task

If you have installed the PingID app on your device, the PingID Apple Watch app is automatically installed on your watch and you will start receiving notifications to your watch. You can also open the PingID app on your watch to receive a one-time passcode (OTP). If the Apple watch app is disabled, you will not be able to access a one-time passcode from your watch.

> **Note**
>
> The Apple watch only receives notifications when your mobile device is locked, and the mobile device screen is in sleep mode.

Steps

1. On your iPhone, tap the Watch app, and then tap **PingID**.
2. To enable or disable the app on your Apple watch, tap **Show App on Apple Watch**.

   Result:

   The PingID app is installed on your Apple watch, and the PingID icon appears.
3. To view the current one-time passcode, on your Apple watch, tap the PingID icon.

4. (Optional) To get a new passcode, tap **Refresh**.

Authenticating using a one-time passcode (VPN)

If you do not have internet access temporarily, you can still authenticate using the PingID mobile app by generating a one-time passcode (OTP).

About this task

The OTP is unique and can only be used once. Only the OTP that appears on your device at the time that you sign on to your account is valid for authentication.

> **Note**
>
> If permitted by your organization's policy, you can view and use the OTP.

Steps

1. From your web browser or application:
    1. Sign on to your VPN with your username and password.

        > **Note**
        >
        > If you have more than one device, and your organization policy allows it, a message displays showing all of your devices in a numbered list.

    2. For multiple devices only: enter the number of the device you want to use to authenticate.
    3. Click **Sign In**.
2. On your mobile device, open the PingID app to view the current OTP.

    > **Note**
    >
    > When you open PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

    The OTP refreshes each time you open the PingID app. To generate a new OTP, tap **New Passcode**.
3. Enter the OTP into the text field. Click **Sign In**.

Result

After you have successfully authenticated, you are signed on to your VPN.

Authenticating manually (VPN)

When you sign on to your VPN, you might be asked to authenticate manually using the PingID mobile app.

Before you begin

To authenticate manually you need the following:

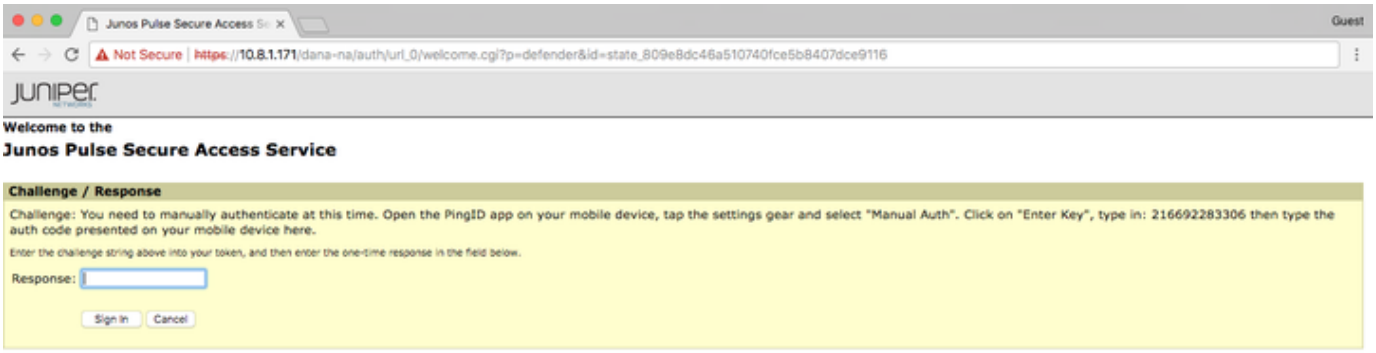
A device with the PingID mobile app 1.8 or later that is already paired with your account and with which you have successfully authenticated at least once.

About this task

You will not be asked to authenticate manually often, but be aware that authenticating manually is different than the normal sign on process.

Steps

1. Sign on to your VPN.



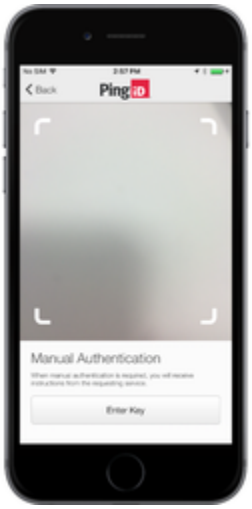
Result:

A **Manual Authentication** message appears, displaying a 12-digit key, and requests that you authenticate manually.

2. From your mobile device, open the PingID mobile app.
3. Tap the **Gear** icon ( ) and select **Manual Auth**. Authenticate with your device biometrics, if required.

Result:

The **Manual Authentication** screen opens.



4. Tap **Enter Key**.
5. In the **Security Key** field, enter the 12-digit key displayed on the VPN sign on page, and tap **Verify**.

Result:

You receive an authentication code.

6. In the VPN **Response** field, enter the **Authentication Code**. Click **Sign In**.

Result:

You are successfully authenticated and signed on to your VPN.

Authenticating using your Android (Windows login) (legacy)

You can authenticate to Windows login with your Android device in a variety of ways.

Use any of the following options:

- Swipe authentication
- Biometrics authentication
- One-time passcode
- Android watch
- Manual authentication when offline.

If your organization allows you to authenticate using more than one device type, you can also add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

The options available to you are defined by your organization's policy.

Using swipe authentication for Android (Windows login)

If you have the PingID app running on your mobile device and your organization is using swipe authentication, sign on to your Windows desktop or laptop machine using swipe to authenticate.

Before you begin

Pair your device with PingID mobile app to enable authentication. For more information, see (legacy) Pairing PingID mobile app for Android (using a QR code or pairing code) or Adding and reordering devices.

About this task

> **Note**
>
> The authentication process might vary slightly depending on the Android version and the notification settings on your device. Some Android versions might give you the option to approve the push notification from the lock screen.

Steps

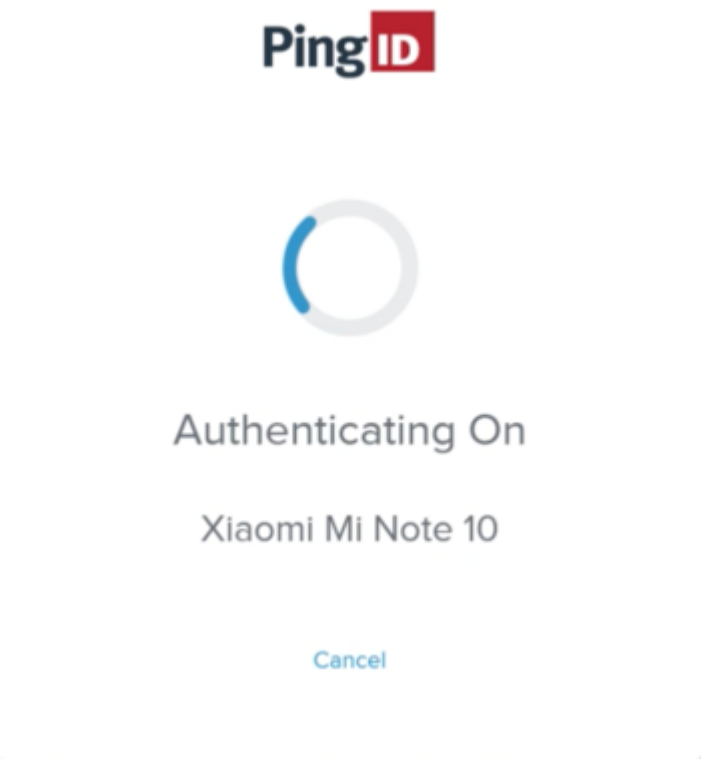
1. Sign on to your Windows laptop or desktop machine.

   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

   Result:

   The **Authenticating on...** window appears, and an authentication notification request is sent to your mobile device.

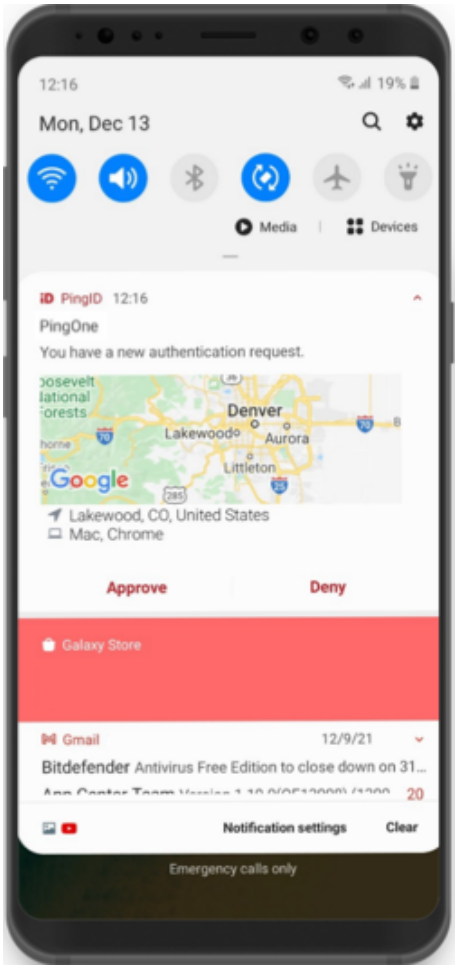


> **Note**
>
> If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.

2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.



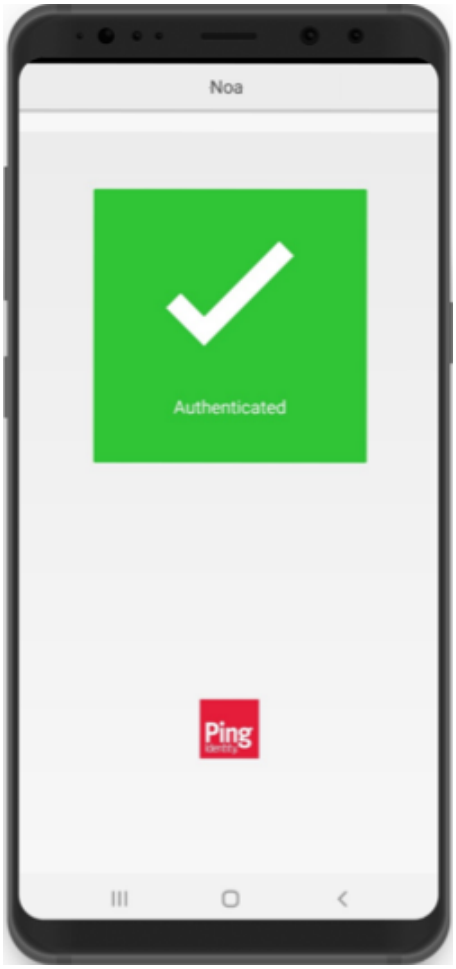
> **Note**
>
> For Android version 10 and higher, you must unlock your device to authenticate.

◦ If PingID mobile app opens showing the swipe screen, swipe up to authenticate.

> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

You'll see the green checkmark on your mobile indicating your access is approved, and PingID closes.



Result

You are signed on to your Windows machine.

Using biometrics authentication for Android (Windows login)

Use your Android mobile device to scan your biometrics to authenticate and verify your identity.

Before you begin

Register your biometrics on your device and then pair your device in order to authenticate using your biometrics. For more information, see (legacy) Pairing PingID mobile app for Android (using a QR code or pairing code).

About this task

Authentication might vary depending on your phone model, phone settings, and whether your device is locked or unlocked when the authentication request is sent.

The following animation shows an example of a passwordless authentication flow using biometrics.

> **Note**
>
> You might need to enter your password, depending on your organization's configuration.

> **Note**
>
> Biometrics authentication is only available if the option is enabled by your organization.
> The authentication process might vary slightly depending on the Android version and the notification settings on your device. The images shown here relate to a Samsung device. Actual implementation might vary according to device model.

Steps

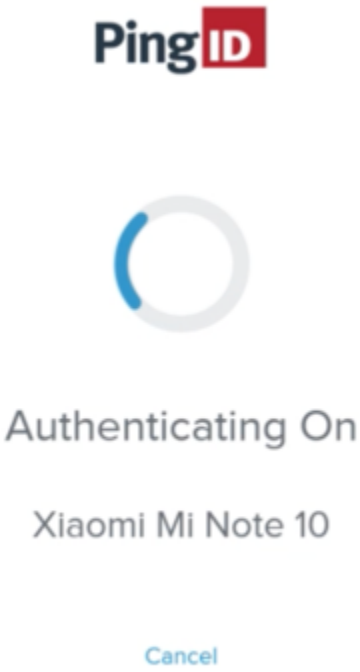
1. Sign on to your Windows laptop or desktop machine.

   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

The **Authenticating** window appears, and an authentication notification request is sent to your device.

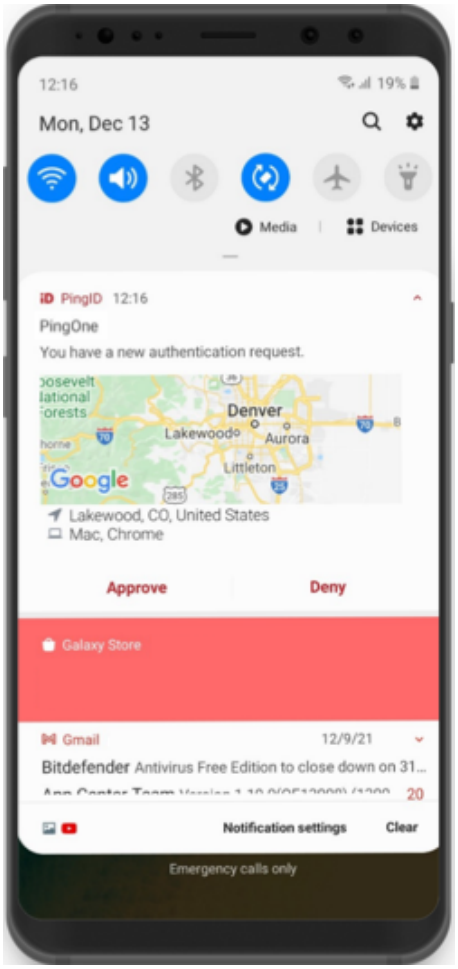


> **Note**
>
> If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.

2. Accept the authentication notification, depending on your mobile's notification settings:

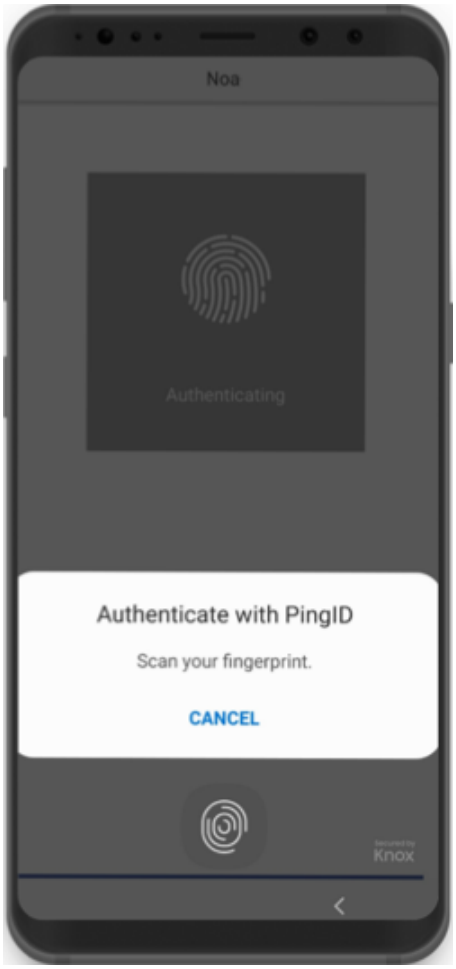
   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.



> **Note**
>
> For Android version 10 and higher, you must unlock your device to authenticate.

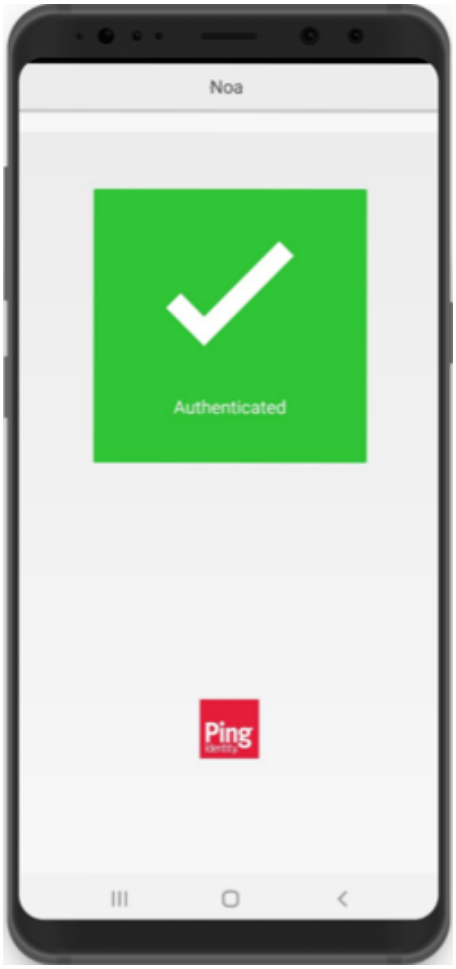
◦ If PingID mobile app opens, authenticate using your biometrics.



> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

You'll see the green checkmark on your mobile indicating your access is approved, and PingID closes.



You are automatically signed on to your Windows machine.

Authenticating using a one-time passcode (Windows login)

One of the authentication methods that administrators can allow is the use of a generated one-time passcode (OTP).

Before you begin

Pair your device with PingID mobile app to enable authentication. For more information, see (legacy) Pairing PingID mobile app for Android (using a QR code or pairing code) or Adding and reordering devices.

Steps

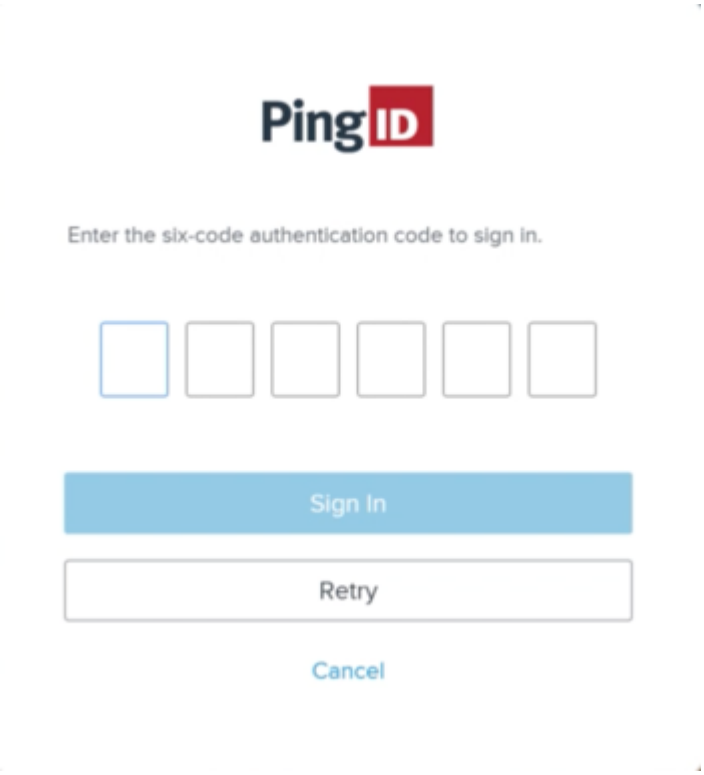
1. Sign on to your Windows laptop or desktop machine.

   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

The **Authenticating on...** window appears. This is where you will enter the OTP after it has been generated in the app.



2. On the device you use for MFA, open the PingID app, and get the one-time passcode that is displayed.

> **Note**
>
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.
> - The one-time passcode refreshes each time you open the PingID app. If you need to generate a new one-time passcode, tap **New Passcode**.

3. Return to the **Authentication** window on your Windows computer, enter the passcode, and click **Sign In**.

Result:

MFA is complete, and you are signed on to your Windows computer.

Authenticating using your Android watch (Windows Login)

You can authenticate with PingID mobile app using your Android watch.

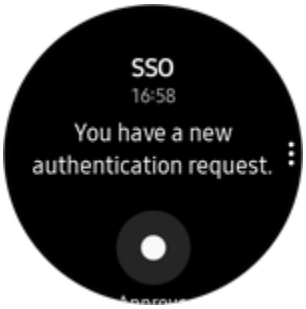
About this task

Some Android models automatically allow you to authenticate using your Android watch. If the PingID mobile app is installed on your phone, and if your Android watch model and configuration are compatible with the PingID mobile app, you'll automatically start receiving push notifications to your Android watch when your phone is locked.

> **Note**
>
> The ability to authenticate using an Android watch varies according to Android model and configuration.

Steps

1. If your Android device and configuration supports the use of Android watch for notifications, when your phone is locked, you will receive a notification to your watch automatically.



2. Swipe to authenticate.

Authenticating manually with the PingID mobile app (Windows Login)

If you sign on to your Windows laptop or desktop machine without having a network connection, such as airplane mode or without Wi-Fi connection, you can authenticate manually using the PingID mobile app.

Before you begin

To authenticate manually with PingID you must first pair your device with PingID and authenticate online at least once. For more information see (legacy) Pairing PingID mobile app for Android (using a QR code or pairing code) or Adding and reordering devices.

About this task

The process to authenticate manually is different than the way you usually sign on.

To authenticate manually:

- PingID mobile app must be installed on your device, paired with your account. Minimum requirements for manual authentication is PingID mobile app 1.18. For windows passwordless authentication, PingID mobile app 2.15 or later is required.
- You need to successfully authenticate to the specific Windows machine you are trying to access online at least one time before you can authenticate manually.
- Your device must have a working camera, with the PingID Mobile app camera permissions set to **Approve**. For more information, see PingID mobile app management (legacy).

Steps

1. Sign on to your Windows laptop or desktop machine.
    - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
    - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

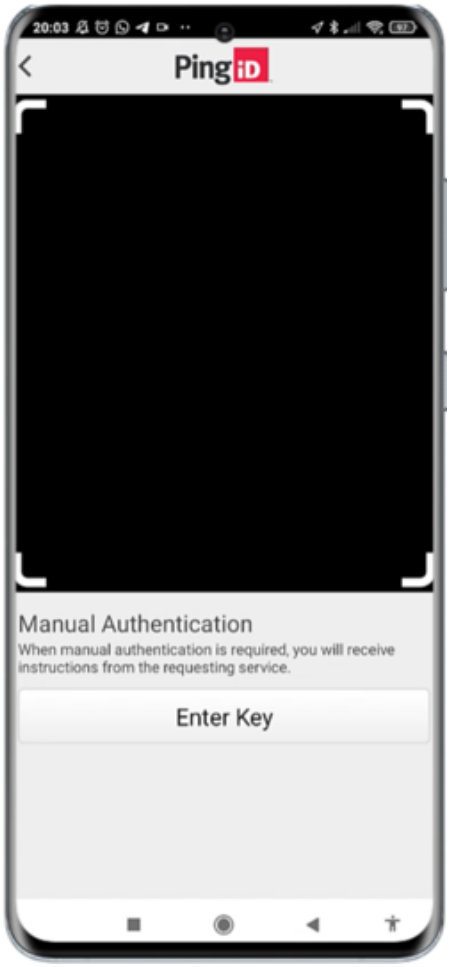
A Manual Authentication message appears, displaying a QR code requesting that you authenticate manually.

> **Note**
>
> If you have more than one mobile device paired with your account, you'll need to select the device you want to use to authenticate before the Manual Authentication message appears.

2. On your mobile device, open the PingID mobile app:
    1. Tap the **Gear** icon ()
    2. Select **Manual Auth**.
    3. Authenticate using your device biometrics, if required.

       Result:

       The QR code scanner for manual authentication opens.



3. Using your mobile device, scan the QR code displaying in the **Manual Authentication** window.

   Result:

   You receive an **Authentication Code**.

4. Enter the **Authentication Code** into the **Manual Authentication** window. Click **Sign In**.

   Result

You are signed on to your Windows machine.

Authenticating using your iPhone (Windows login) (legacy)

This section describes the various ways you can authenticate to Windows login using your iPhone.

You can use any of the following methods to authenticate:

- Swipe
- Biometrics
- Apple Watch
- One-time passcode
- Authenticate manually with PingID mobile app
- Authenticate manually with the PingID mobile app

If your organization allows you to authenticate using more than one device type, you can add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

The options available to you are defined by your organization's policy.

Using swipe authentication for iPhone (Windows login)

If you have the PingID app running on your mobile device and your organization is using swipe authentication, sign on to your Windows desktop or laptop machine using swipe to authenticate.

Before you begin

Pair your device with PingID mobile app to enable authentication. For more information, see (legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code) or Adding and reordering devices.

About this task
Steps

1. Sign on to your Windows laptop or desktop machine.

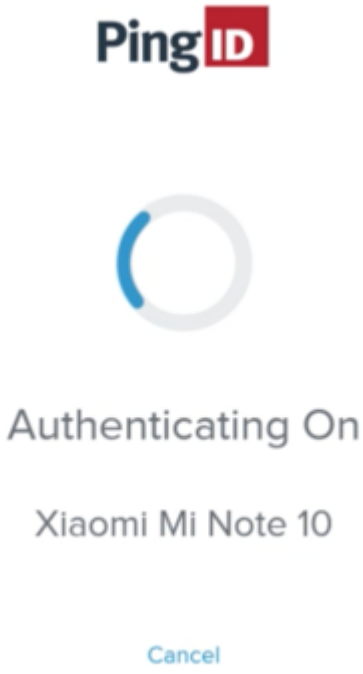
   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

+

Result:

+ The **Authenticating on...** window appears, and an authentication notification request is sent to your mobile device.



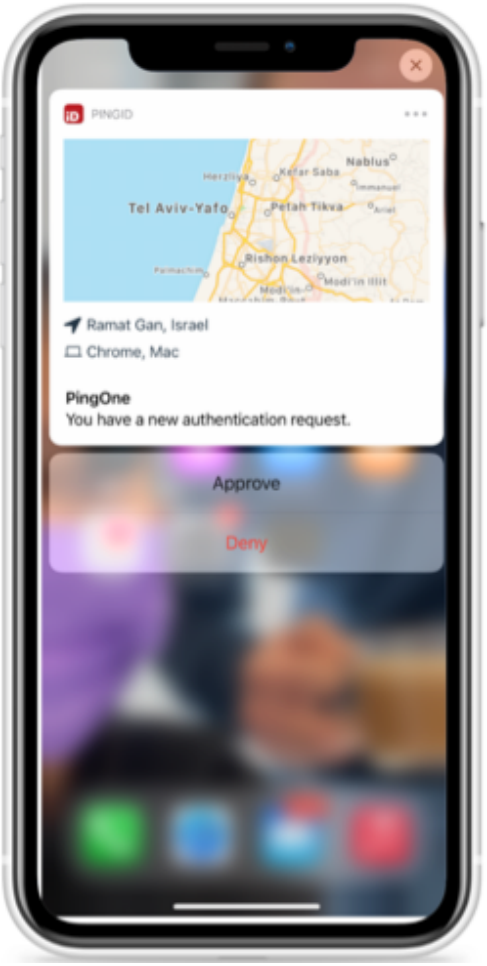
+

1. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

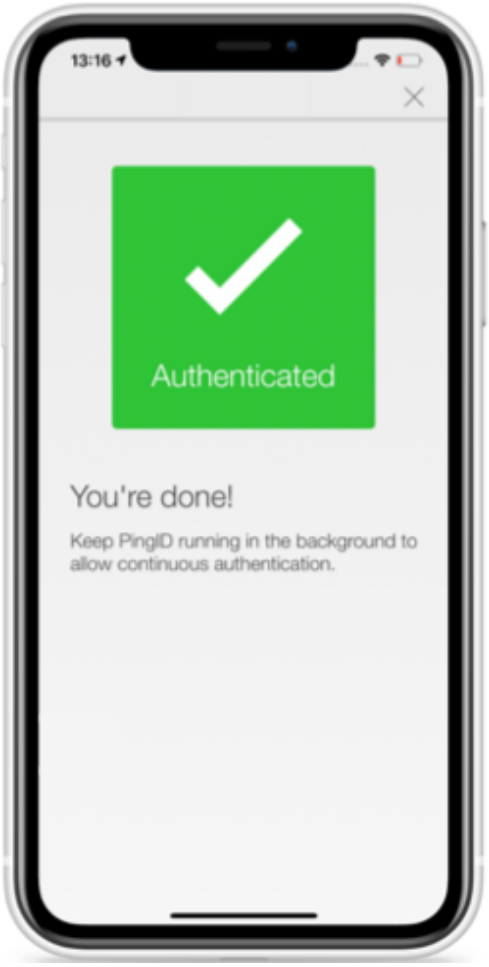
   > **Note**
   >
   > If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.



- If your mobile phone is unlocked and PingID is open, swipe to authenticate.

Result:

The green **Authenticated** screen appears with a check mark, indicating successful authentication.



Result

You are signed on to your Windows machine.

Using biometrics authentication for iPhone (Windows login)

Authenticate with your device biometrics using PingID mobile app.

Before you begin

- Register biometrics on your device, such as fingerprints or Face ID.
- Pair your iPhone to use biometrics to authenticate. See (legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code).

About this task

Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when the authentication request sends.

The following animation shows an example of a passwordless authentication flow using biometrics. NOTE: You might need to enter your password, depending on your organization's configuration.

> **Note**
>
> Biometrics authentication is only available to you if the option is enabled by your organization.

Steps

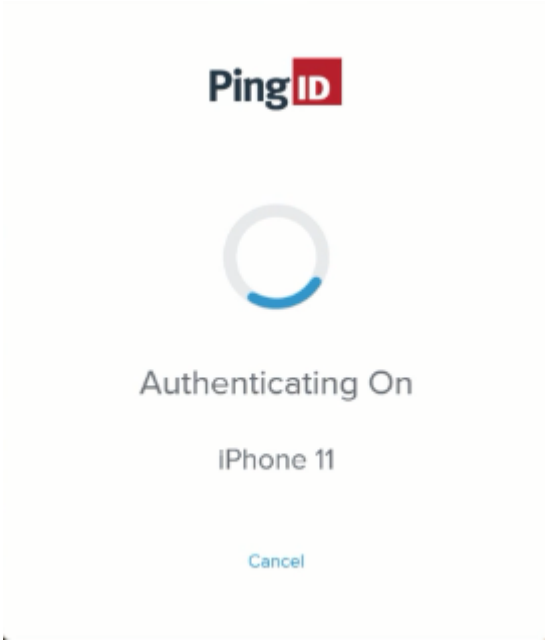
1. Sign on to your Windows laptop or desktop machine.

   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

The **Authenticating on...** window appears, and an authentication notification request is sent to your mobile device.



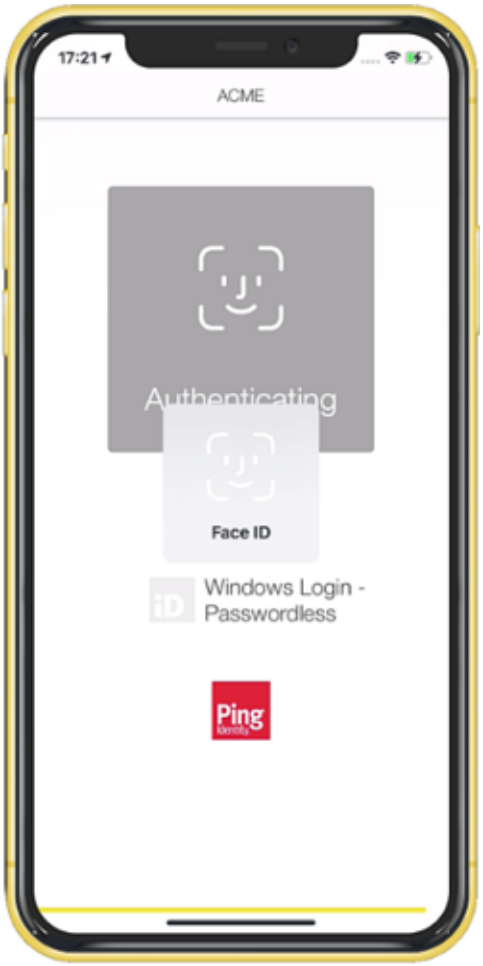
2. Accept the authentication notification:

   Choose from:

   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

     > **Note**
     >
     > If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.

   - If your mobile phone is unlocked and PingID is open, you'll be prompted to authenticate with your biometrics.
   - Face ID: Tap the message asking you to authorize scanning with Face ID, if prompted, or your face is scanned automatically.



- Fingerprint: To scan your fingerprint, touch the Home button lightly.

  Result:

  The green **Authenticated** screen appears with a check mark, indicating successful authentication.

  Result

  You are signed on to your Windows machine.

Enabling and disabling passcodes on your Apple watch (Windows login)

Enable the use of PingID one-time passcodes (OTPs) on your Apple watch.

About this task

If you have installed the PingID app on your device, the PingID Apple Watch app is automatically installed on your watch and you will start receiving notifications to your watch. You can also open the PingID app on your watch to receive a one-time passcode (OTP). If the Apple watch app is disabled, you will not be able to access a one-time passcode from your watch.

> **Note**
>
> The Apple watch only receives notifications when your mobile device is locked, and the mobile device screen is in sleep mode.

Steps

1. On your iPhone, tap the Watch app, and then tap **PingID**.
2. To enable or disable the app on your Apple watch, tap **Show App on Apple Watch**.

   Result:

   The PingID app is installed on your Apple watch, and the PingID icon appears.

3. To view the current one-time passcode, on your Apple watch, tap the PingID icon.

4. (Optional) To get a new passcode, tap **Refresh**.

Authenticating using a one-time passcode (Windows login)

One of the authentication methods that administrators can allow is the use of a generated one-time passcode (OTP).

Before you begin

Pair your device with PingID mobile app to enable authentication. For more information, see (legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code) or Adding and reordering devices.

Steps

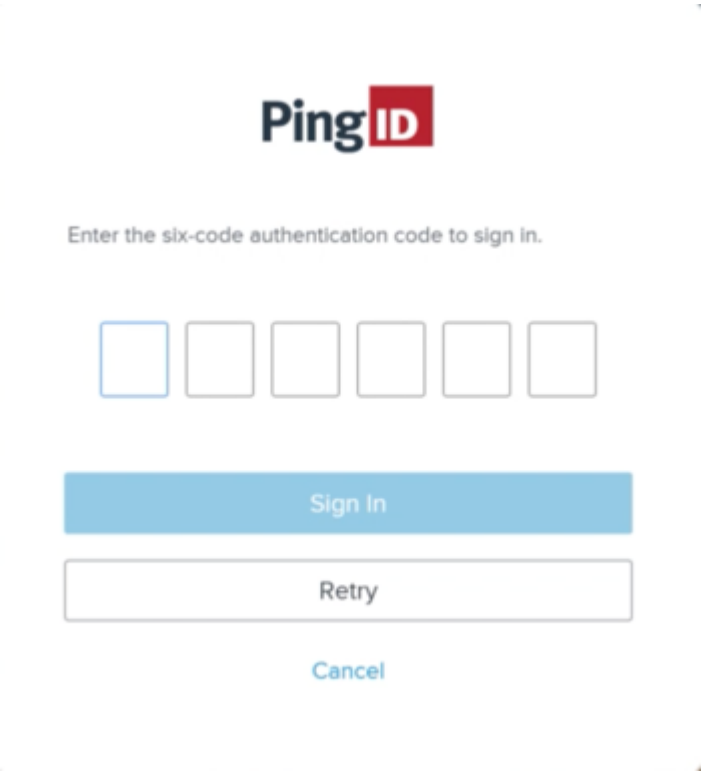
1. Sign on to your Windows laptop or desktop machine.

   Choose from:

   - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
   - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

The **Authenticating on...** window appears. This is where you enter the OTP after it has been generated in the app.



2. On the device you use for MFA, open the PingID app, and get the one-time passcode that is displayed.

> **Note**
>
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.
> - The one-time passcode refreshes each time you open the PingID app. If you need to generate a new one-time passcode, tap **New Passcode**.

3. Return to the **Authentication** window on your Windows computer, enter the passcode, and click **Sign In**.

Result:

MFA is complete, and you are signed on to your Windows computer.

Authenticating manually with the PingID mobile app (Windows Login)

If you sign on to your Windows laptop or desktop machine without having a network connection, such as airplane mode or without Wi-Fi connection, you can authenticate manually using the PingID mobile app.

Before you begin

To authenticate manually with PingID you must first pair your device with PingID and authenticate online at least once. For more information see (legacy) Pairing PingID mobile app for iPhone (using a QR code or pairing code) or Adding and reordering devices.

About this task

The process to authenticate manually is different than the way you usually sign in.

To authenticate manually:

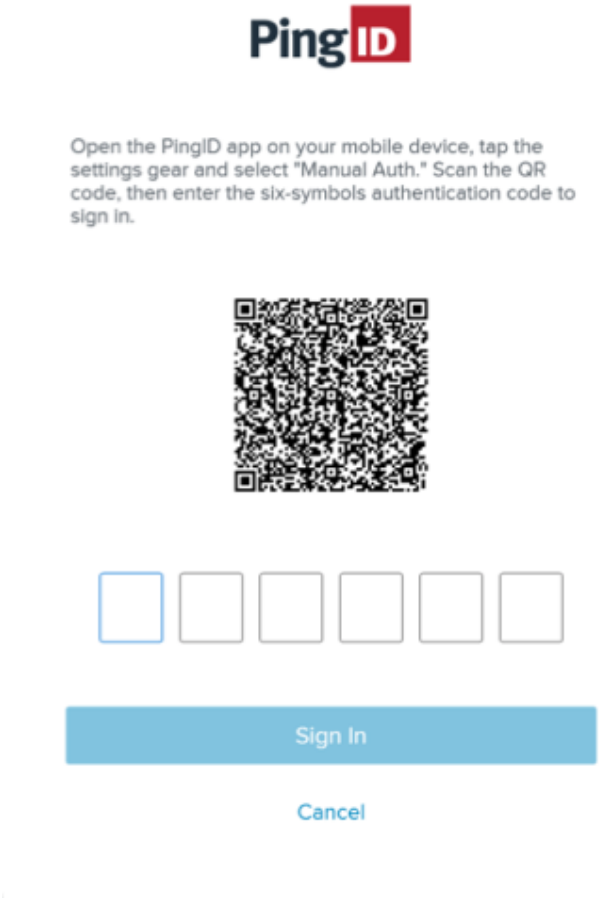
- PingID mobile app must be installed on your device, paired with your account. Minimum requirements for manual authentication is PingID mobile app 1.18. For windows passwordless authentication, PingID mobile app 2.15 or later is required.
- You need to successfully authenticate to the specific Windows machine you are trying to access online at least one time before you can authenticate manually.
- Your device must have a working camera, with the PingID Mobile app camera permissions set to **Approve**. For more information, see PingID mobile app management (legacy).

Steps

1. Sign on to your Windows laptop or desktop machine.
    - If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon, and then click the arrow.
    - If your organization requires a username and password: Under **Sign-in options**, click the key icon and enter your username and password and then click the arrow key.

Result:

A Manual Authentication message appears, displaying a QR code requesting that you authenticate manually.



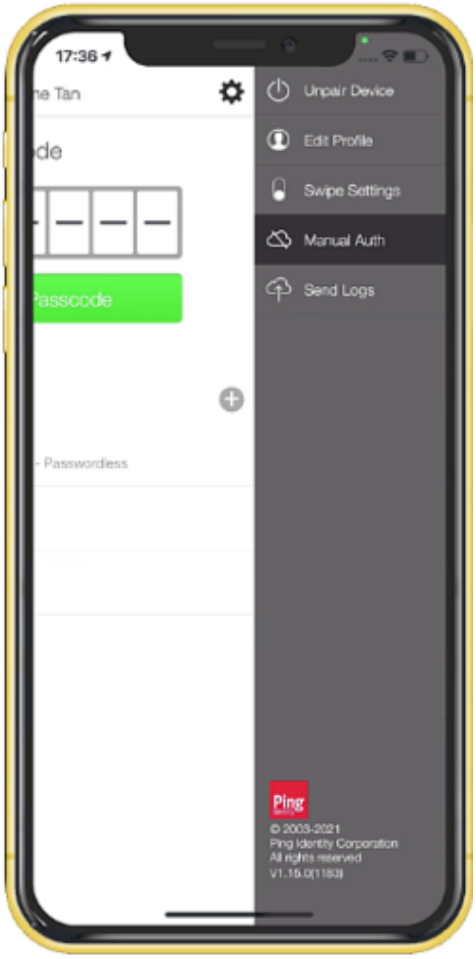
> **Note**
>
> If you have more than one mobile device paired with your account, you'll need to select the device you want to use to authenticate before the Manual Authentication message appears.

2. On your mobile device, open the PingID mobile app:

    1. Tap the **Gear** icon ( ) .

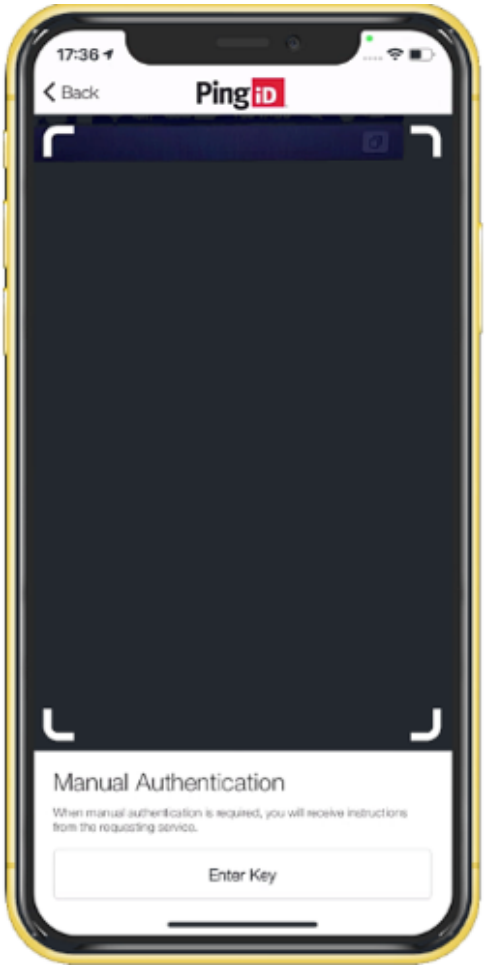
    2. Select **Manual Auth**.

    3. Authenticate using your device biometrics, if required.



Result:

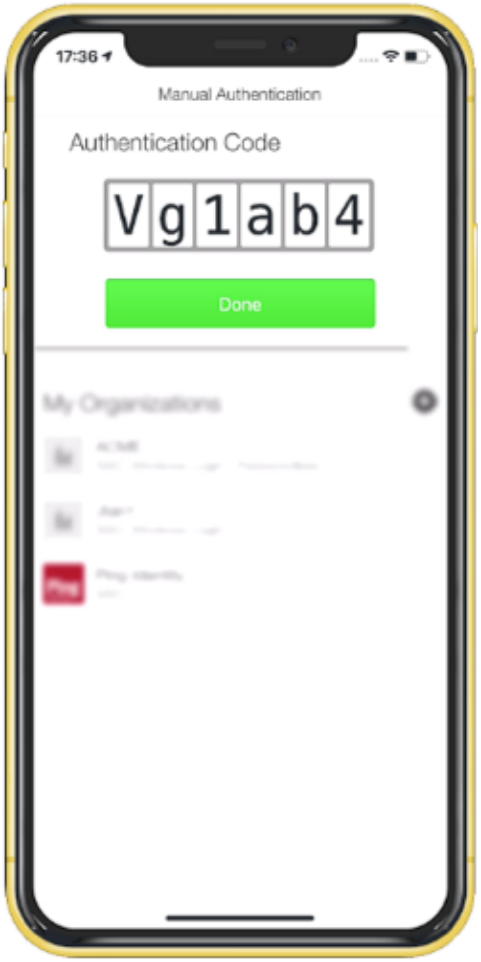
The QR code scanner for manual authentication opens.



3. Using your mobile device, scan the QR code displaying in the **Manual Authentication** window.

   Result:

   You receive an **Authentication Code**.



4. Enter the **Authentication Code** into the **Manual Authentication** window. Click **Sign In**.

Result

You are signed on to your Windows machine.

Using PingID mobile app for RDP authentication

You can use PingID to access a remote desktop machine through the Windows RDP client, and enjoy a passwordless experience.

Before you begin

- Ensure the Windows login passwordless client is installed on the relevant local and remote desktop machine.
- Pair your device to authenticate with PingID and authenticate at least once.

About this task

You won't need to enter your password, but you will need to authenticate twice using PingID - when accessing the RDP and the second time when signing on to the remote Windows machine. Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when sending the authentication request.

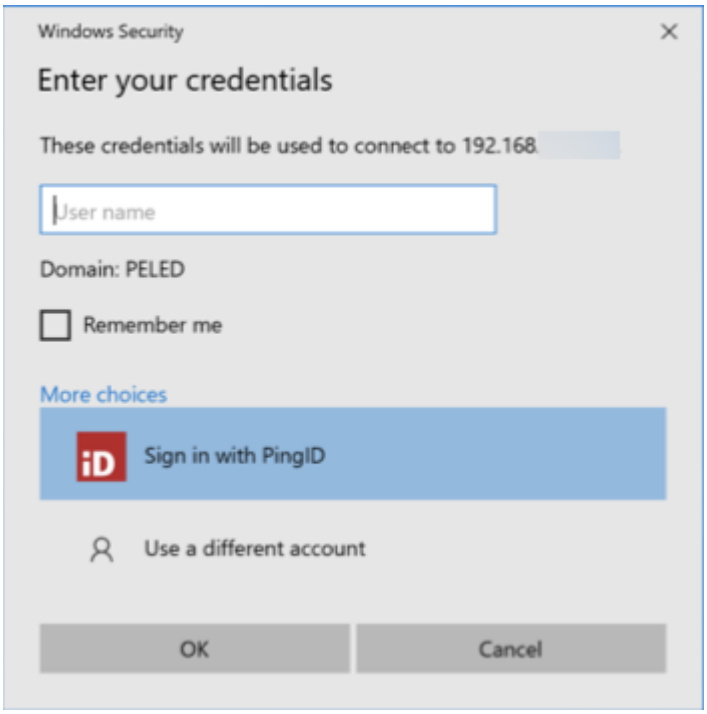
Steps

1. Open your RDP window.

```
mstsc -v <ipaddress>
```

Result:

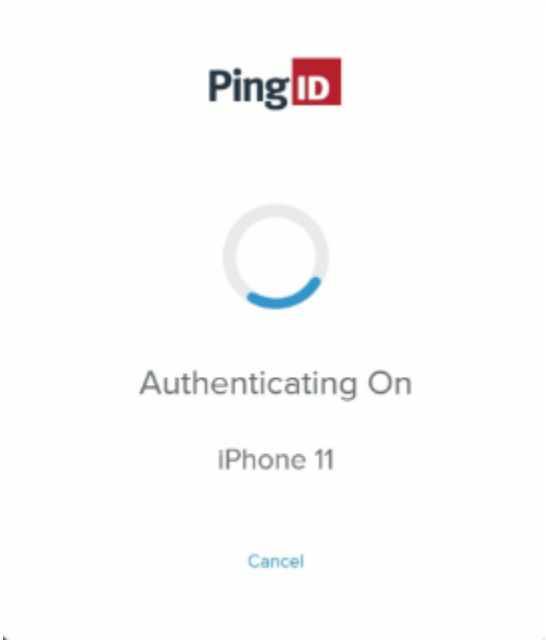
The Enter Your Credentials window opens.



2. Enter your username, and then click **Sign In with PingID**.

Result:

The **Authenticating on...** window appears, and an authentication notification request is sent to your mobile device.



3. Authenticate with PingID mobile app.

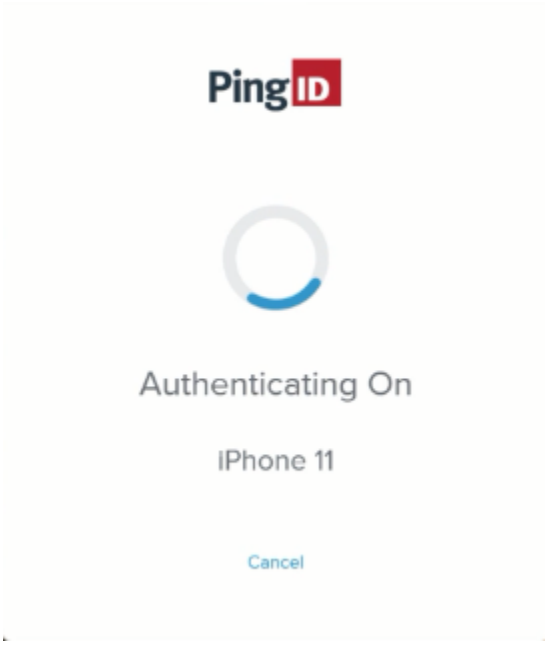
Result:

The remote desktop sign on window opens.

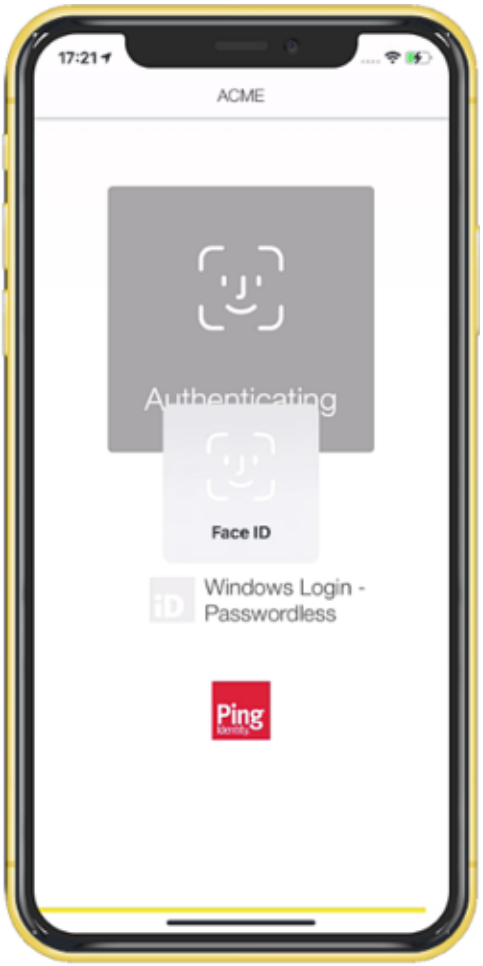
4. Under **Sign-in options**, click the PingID icon, and then click the arrow.

   Result:

   The **Authenticating on...** window appears, and an authentication notification request is sent to your mobile device.



5. Authenticate using PingID.



> **Note**
>
> The example here shows face authentication. The exact configuration might vary according to your preferences and your organization's configuration.

Result:

The green **Authenticated** screen appears with a check mark, indicating successful authentication.

Result

You are signed on to your Windows machine.

Authenticating using your Android (Mac Login) (legacy)

Methods of authenticating using PingID Mobile app to access your Apple Mac machine.

You can authenticate using the following options:

- Swipe authentication for Android
- Biometrics authentication for Android
- Authenticating using your Android watch (legacy)

- Authenticate using a one-time passcode
- Authenticate manually

If your organization allows you to authenticate using more than one device type, you can also add a device and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

The options available to you are defined by your organization's policy.

Using swipe authentication for Android (Mac Login)

Using PingID mobile app swipe authentication on your Android so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- You have paired your Android device.

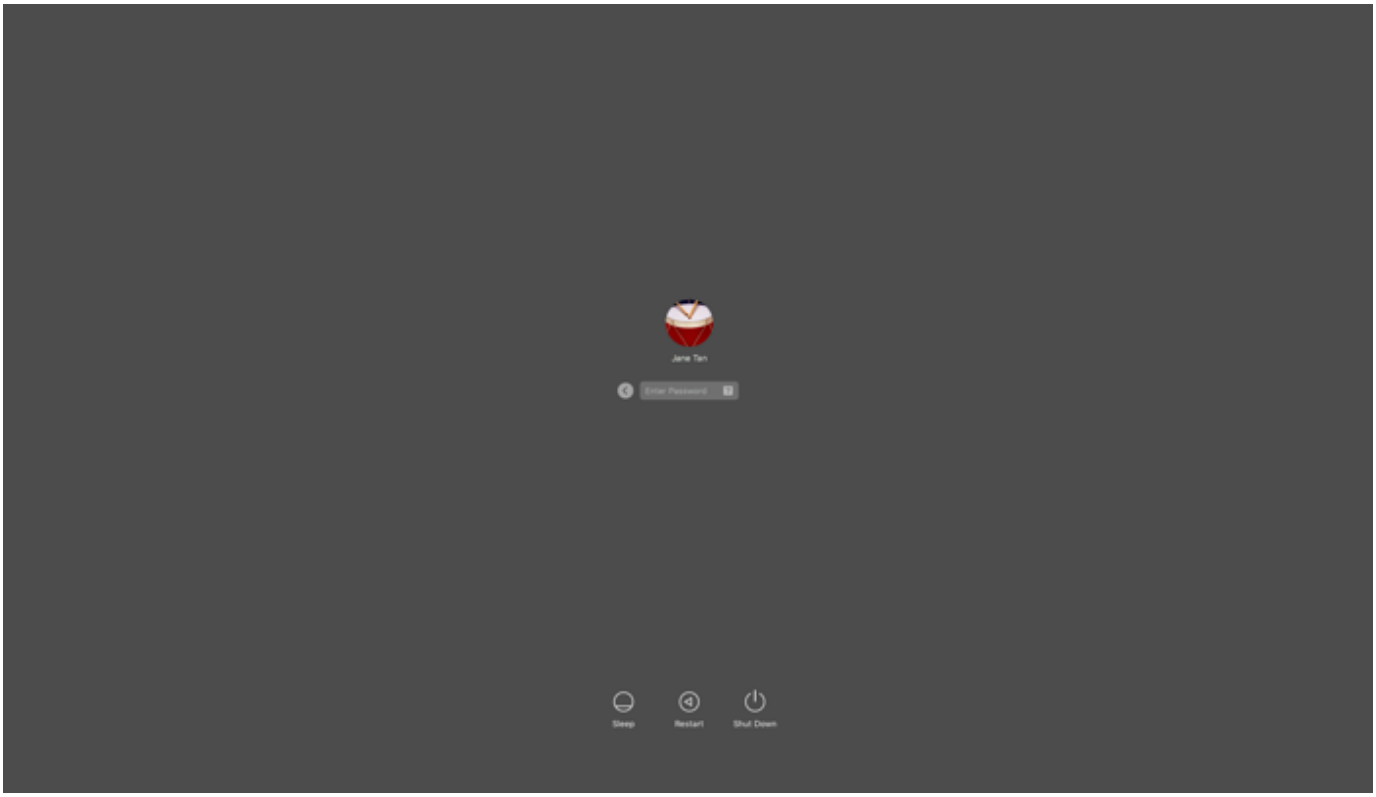
About this task

If you have the PingID app running on your mobile device, and your organization is using swipe authentication, when signing on to your Mac machine, you'll be prompted to swipe to authenticate.

> **Note**
>
> The authentication process might vary slightly depending on the Android version and the notification settings on your device. Some Android versions might give you the option to approve the push notification from the lock screen.

Steps

1. Sign on to your Mac machine.



Result:

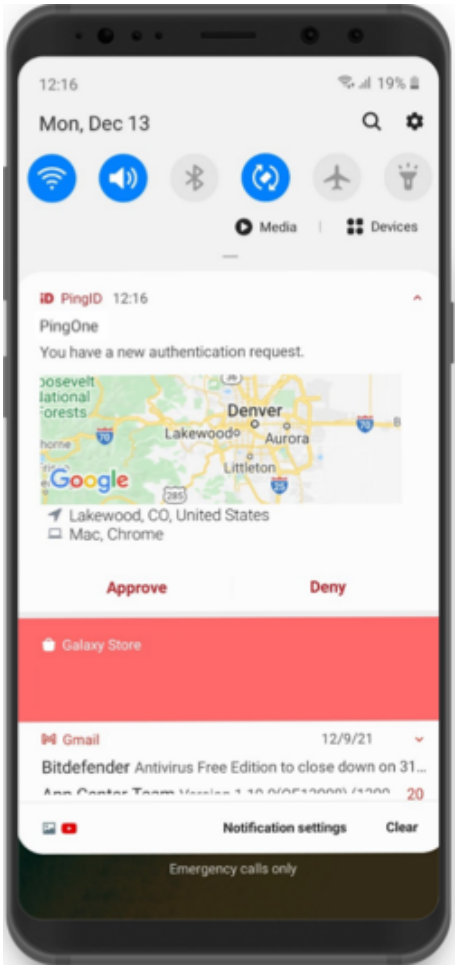
The **Authenticating** window opens, and an authentication notification request is sent to your mobile device.

2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.

> **Note**
>
> If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.



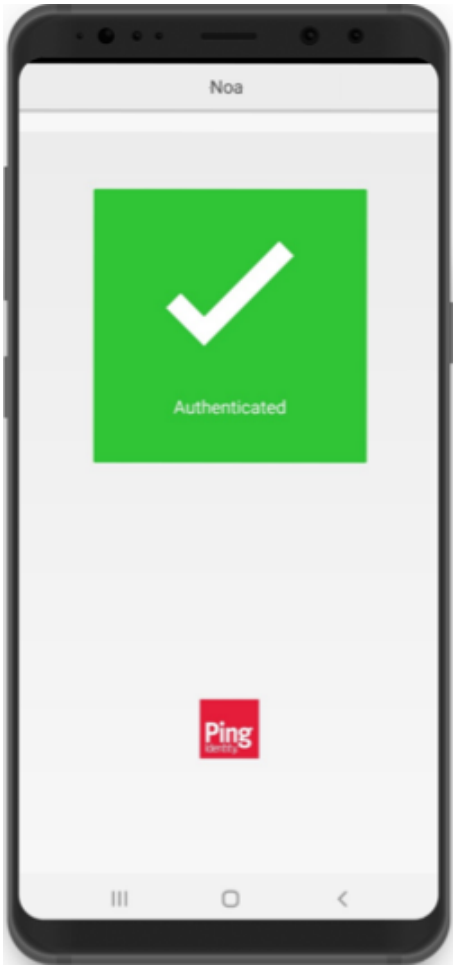
+ NOTE: For Android version 10 and higher, you must unlock your device to authenticate.

    ◦ If PingID mobile app opens showing the swipe screen, swipe up to authenticate.

> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

You'll see the green checkmark on your mobile indicating your access is approved, and PingID closes.



You're signed on to your Mac machine.

Using biometrics authentication for Android (Mac Login)

Using PingID mobile app biometrics authentication on your Android so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS 10.13 or later.
- You have registered your biometrics on your Android device.
- You have paired your Android device.

About this task

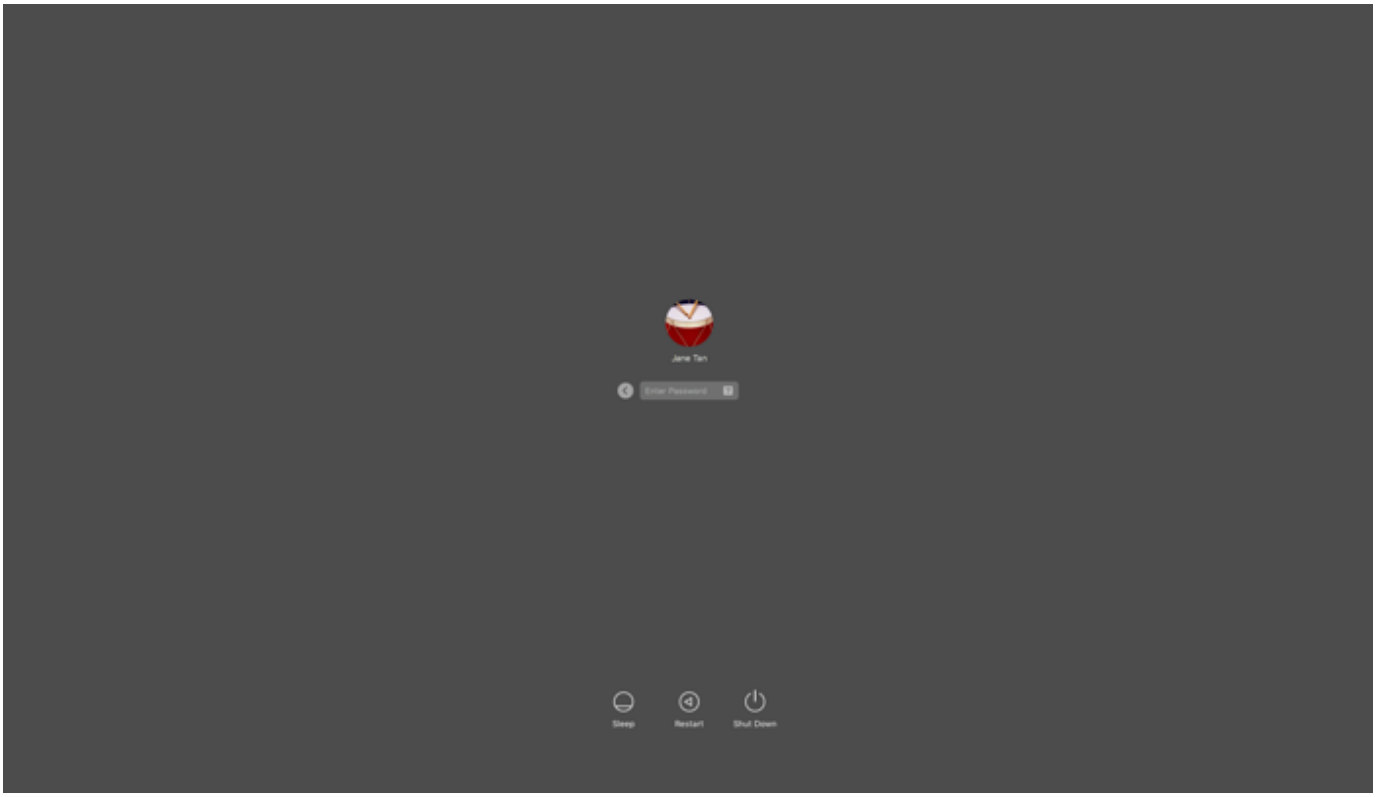
Biometrics authentication is simple using a mobile device. Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when the authentication request is sent.

Note

- Biometrics authentication is only available if the option is enabled by your organization.
- The authentication process may vary slightly depending on the Android version and the notification settings on your device. (The images shown here relate to a Samsung device. Actual implementation may vary according to device model.)
- Some Android devices do not support face or iris authentication with PingID. If you are not able to authenticate with face or iris authentication, we recommend using fingerprint authentication.

Steps

1. Sign on to your Mac machine.



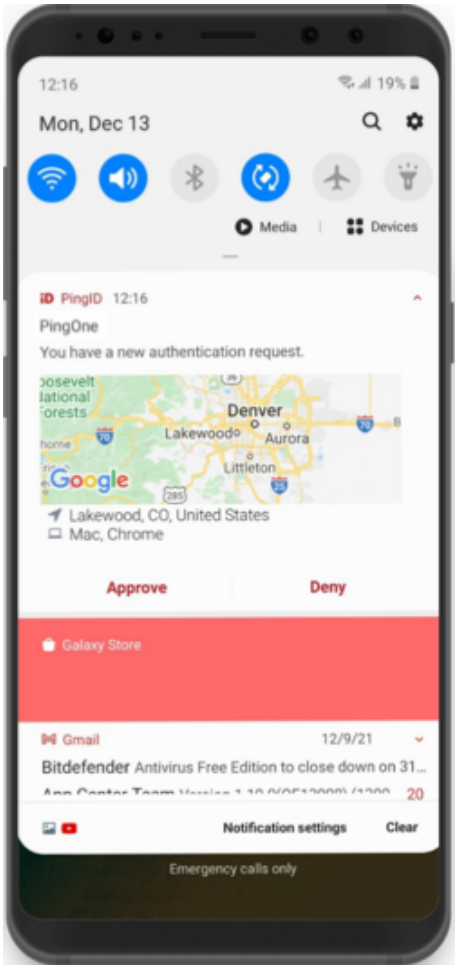
Result:

The **Authenticating** window opens, and an authentication notification request is sent to your device.

2. Accept the authentication notification, depending on your mobile's notification settings:

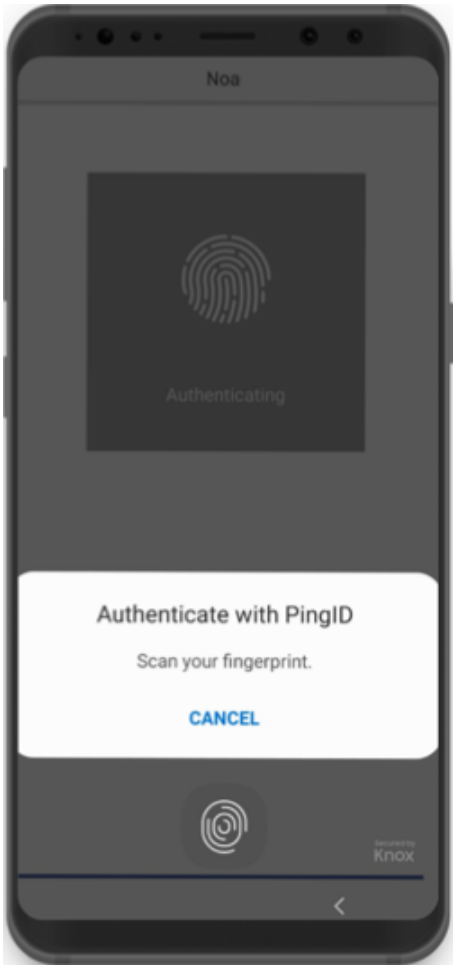
   Choose from:

   - If you see the notification screen appears, slide the notification down until you see the option to approve or deny the request, and then tap **Approve**.



> **Note**
>
> For Android version 10 and higher, you must unlock your device to authenticate.

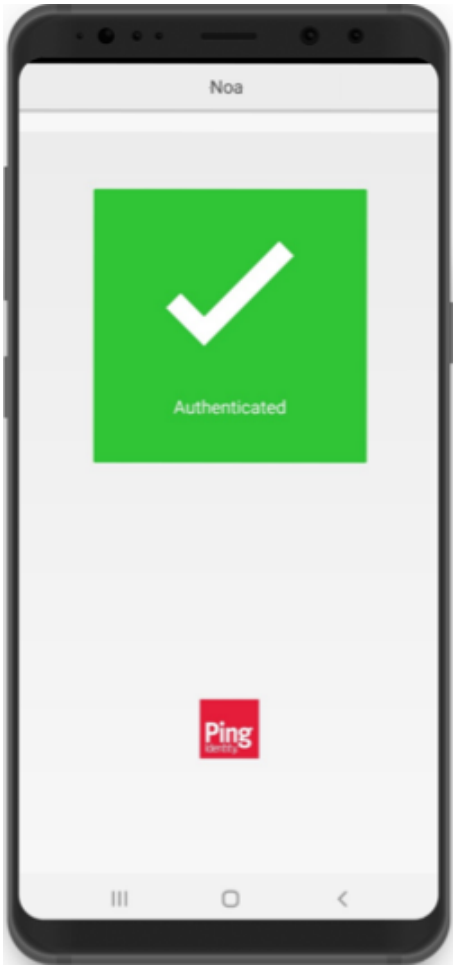
- If PingID mobile app opens, authenticate using your biometrics.



> **Note**
>
> When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.

Result:

You'll see the green checkmark on your mobile indicating your access is approved, and PingID closes.



You're signed on to your Mac machine.

Authenticating using your Android watch (legacy)

You can authenticate with PingID mobile app using your Android watch.

For current content, see Authenticating using a smart watch.

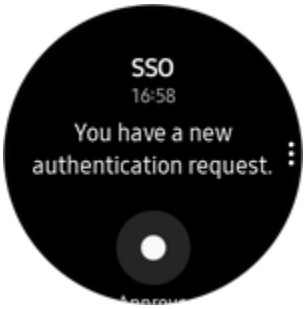
About this task

Some Android models automatically allow you to authenticate using your Android watch. If the PingID mobile app is installed on your phone, and if your Android watch model and configuration are compatible with the PingID mobile app, you'll automatically start receiving push notifications to your Android watch when your phone is locked.

> **Note**
>
> The ability to authenticate using an Android watch varies according to Android model and configuration.

Steps

1. If your Android device and configuration supports the use of Android watch for notifications, when your phone is locked, you will receive a notification to your watch automatically.



2. Swipe to authenticate.

Authenticating using a one-time passcode (Mac Login)

Using PingID mobile app on your Android to get a one-time passcode with which to authenticate, so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- You have paired your mobile device (Android or iOS).

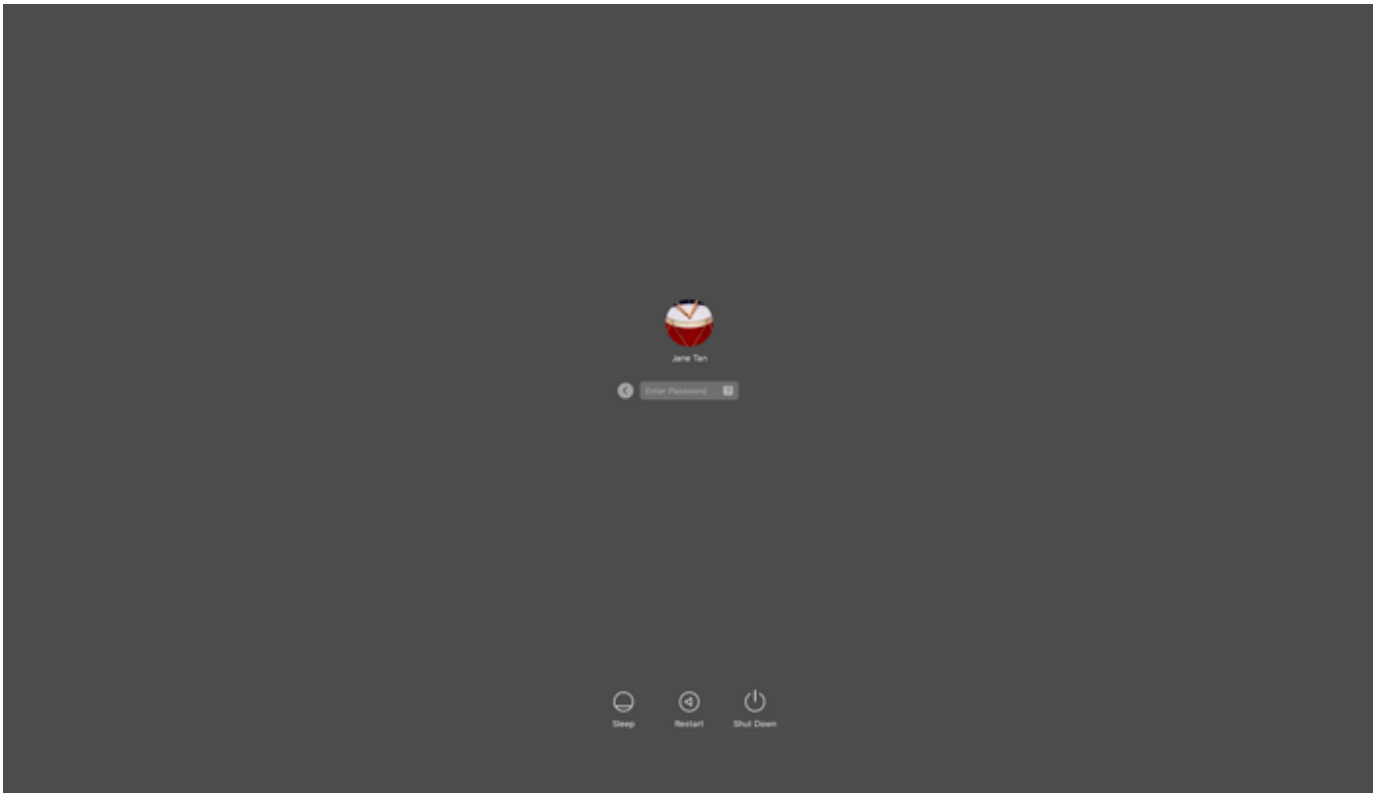
About this task

If you don't have internet access from your mobile device temporarily, you can still authenticate using PingID mobile app by generating a one-time passcode (OTP). The one-time passcode is unique, and can only be used once. Only the one-time passcode that appears on your device at the time that you sign on to your account is valid for authentication.

> **Note**
>
> You'll only be able to view and use the one-time passcode if permitted by your organization's policy.

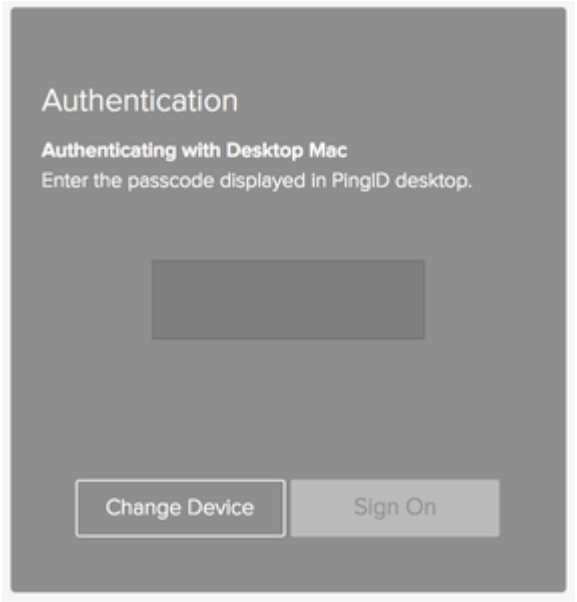
Steps

1. Sign on to your Mac machine.



Result:

The **Authenticating** window opens, and an authentication notification request is sent to your mobile device.



2. On your mobile device, open the PingID mobile app and enter the one-time passcode into the passcode field on the authentication screen. Press Enter.

> **Note**
>
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.
> - The one-time passcode refreshes each time you open the PingID app. To generate a new one-time passcode, tap **New Passcode**.

Result:

You're signed on to your Mac machine.

Authenticating manually with PingID mobile app (Mac Login)

Authenticate using PingID mobile app when your

Before you begin

To authenticate manually using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- Your device has PingID mobile app V1.8 or higher paired with your account.
- You have paired your device and authenticated online with PingID at least once to the Mac machine that you are trying to access.
- You have a working camera on your device, with PingID mobile app camera permissions set to **Approve**. For more information, see PingID mobile app management (legacy).

About this task

If you try to sign on to your Mac machine without having a network connection (e.g., in airplane mode, or when without Wi-Fi connection), you might be asked to authenticate manually using the PingID mobile app. Authenticating manually is slightly different than the way you usually sign on.

> **Note**
>
> If you have paired a security key for offline authentication, you also see the option to choose your security key to authenticate.

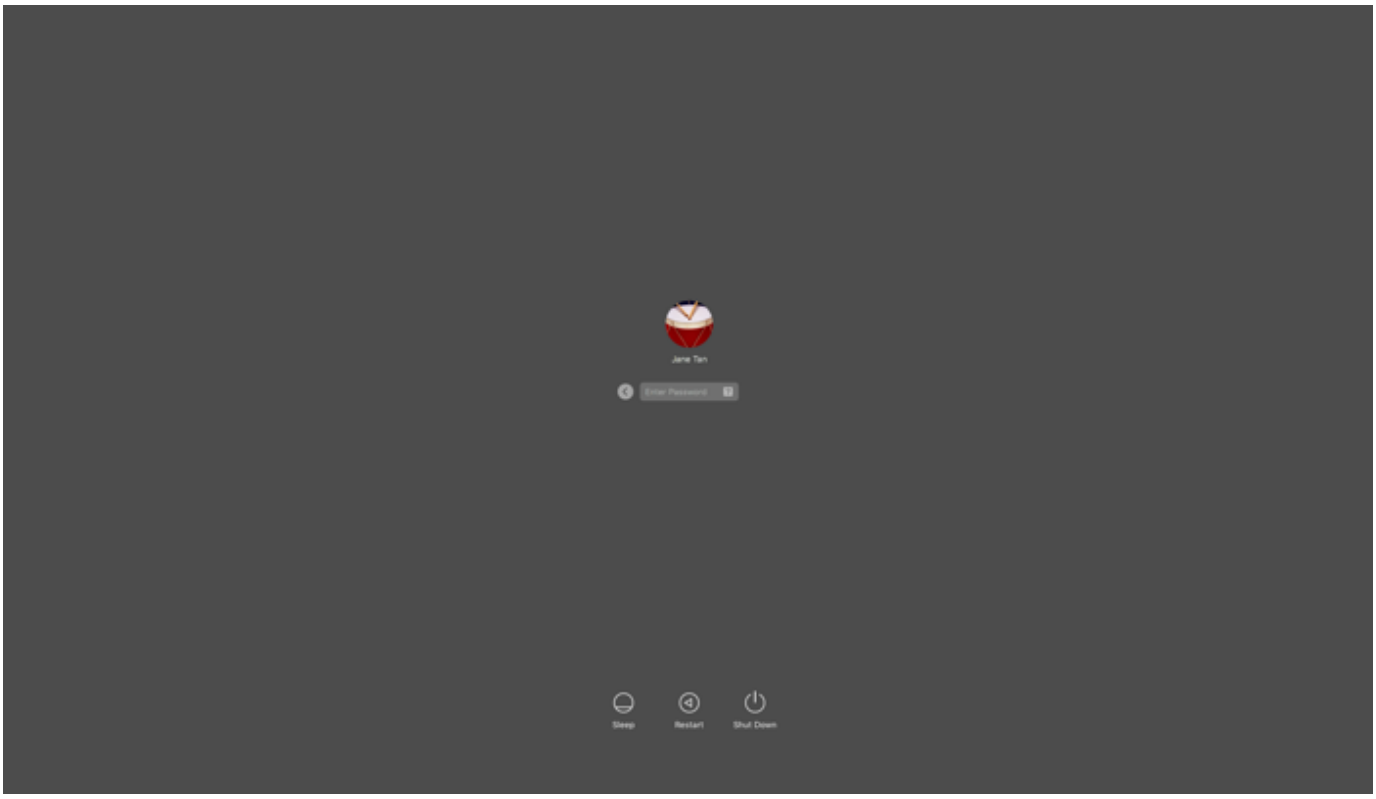
{{{ Video removed }}}

Steps

1. Sign on to your Mac machine.

   Result:

   You'll see a notice telling you that you need to manually authenticate.

   > **Note**
   >
   > If you have more than one device paired with your account, you'll see a list of your devices. Select the device you want to use to authenticate.

2. Click **Next**.

   Result:

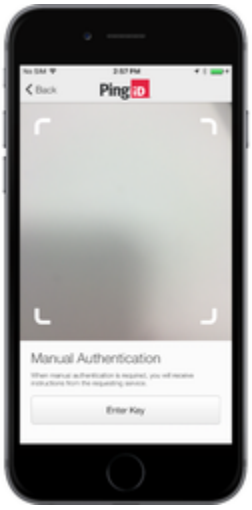
   You'll see a Manual Authentication message, displaying a QR code, requesting that you authenticate manually.

3. On your mobile device, open PingID mobile app.
4. Tap 

   and select **Manual Auth**. Authenticate with your device biometrics, if required.

Result:

The QR code scanner for manual authentication opens.



5. Use your mobile device to scan the QR code displayed on the **Manual Authentication** window.

   Result:

   You'll receive an authentication code.

6. Enter the authentication code into the **Manual Authentication** window, and click **Sign on**.

   Result:

   You're signed on to your machine.

Authenticating using your iPhone (Mac Login) (legacy)

You can authenticate using the following options:

- Swipe authentication for iPhone
- Biometrics authentication for iPhone
- Authenticate using your Apple watch

- Enable/Disable passcodes on your Apple watch
- Authenticate using a one-time passcode
- Authenticate manually with PingID mobile app

If your organization allows you to authenticate using more than one device type, you can also add a device, and decide which device you want to use as your primary (default) authentication method. For more information, see Managing your devices.

The options available to you are defined by your organization's policy.

Authenticating using swipe authentication for iOS (Mac Login)

Using PingID mobile app swipe authentication so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

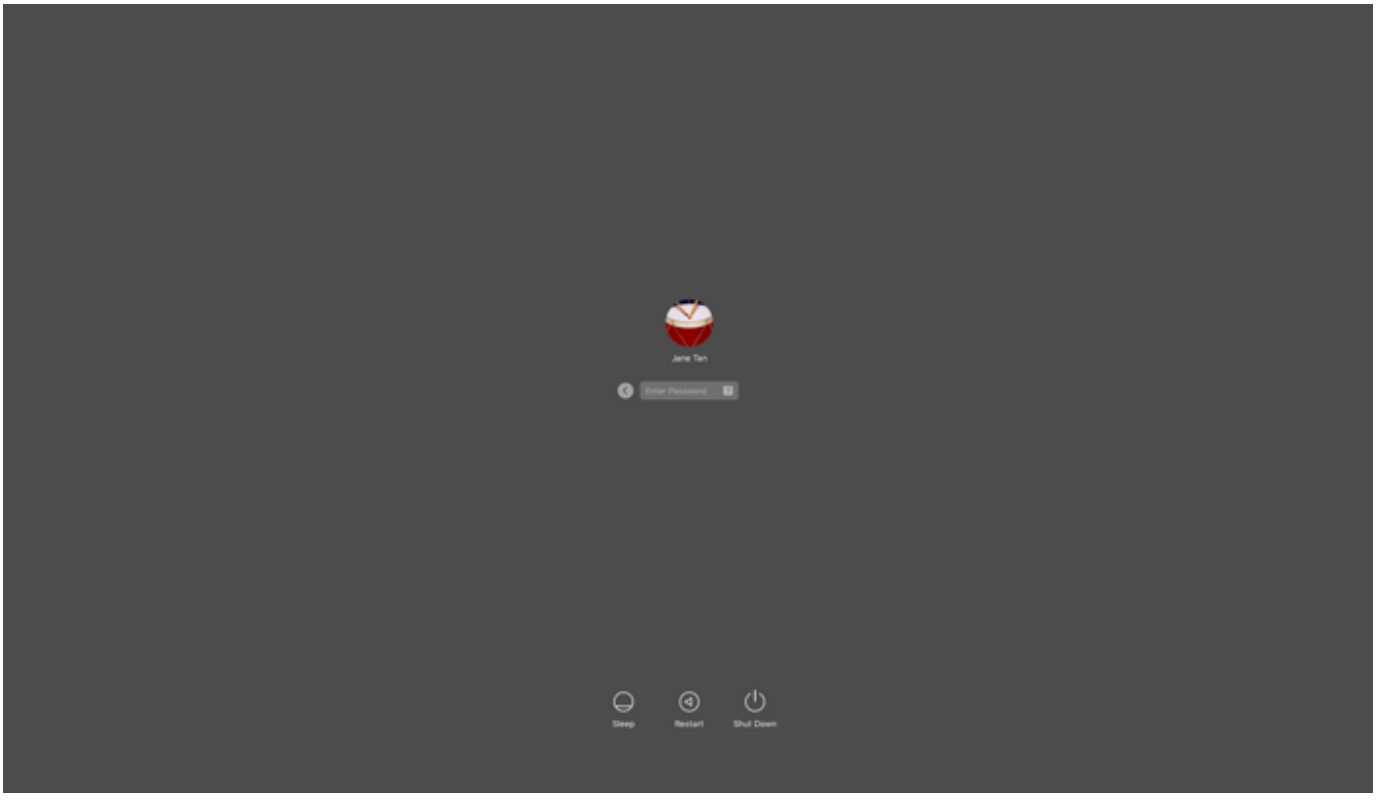
- Your Apple Mac is running Mac OS v10.13 or later.
- You have paired your iOS device (iPhone, or iPad).

About this task

If you have the PingID app running on your mobile device, and your organization is using swipe authentication, when signing on to your resources, you are prompted to swipe to authenticate.

Steps

1. Sign on to your Mac machine.



Result:

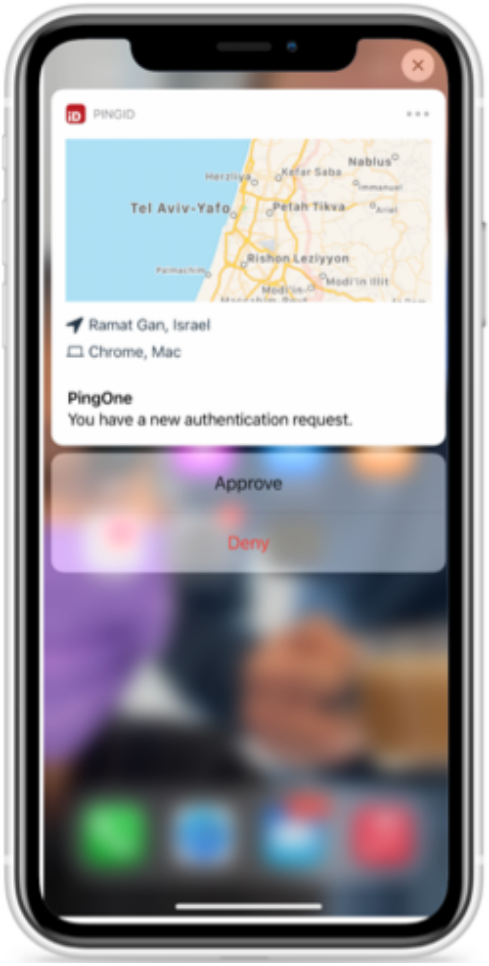
The **Authenticating** window opens, and an authentication notification request is sent to your mobile device.

2. Accept the authentication notification, depending on your mobile's notification settings:

   Choose from:

   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

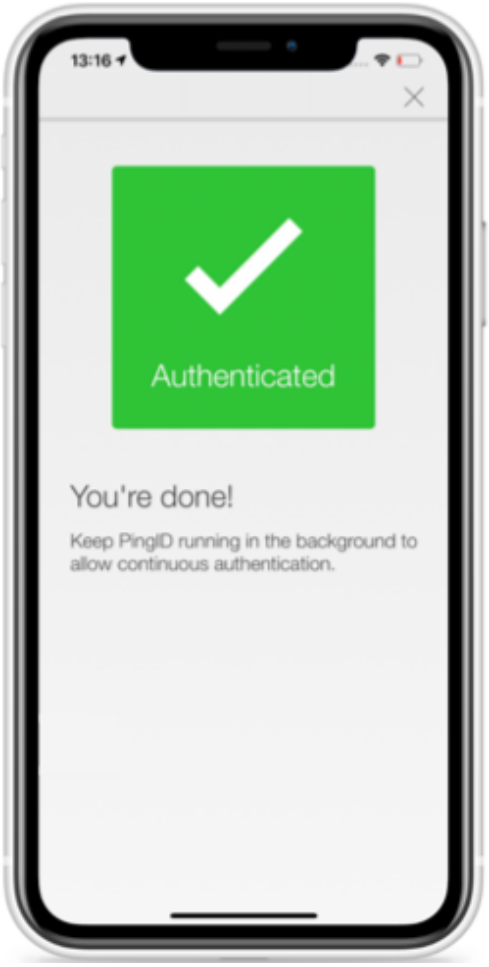
   > **Note**
   >
   > If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.



◦ If your mobile phone is unlocked and PingID is open, swipe to authenticate.

Result:

You'll see the green checkmark indicating authentication is successful.



Result

You're signed on to your Mac machine.

Authenticating using biometrics authentication for iPhone (Mac Login)

Using PingID mobile app biometrics authentication on your iOS device so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- You have registered biometrics on your iPhone, such as fingerprints or FaceID.
- You have paired your iOS device (iPhone, or iPad) from a browser on a different machine (not your Mac).

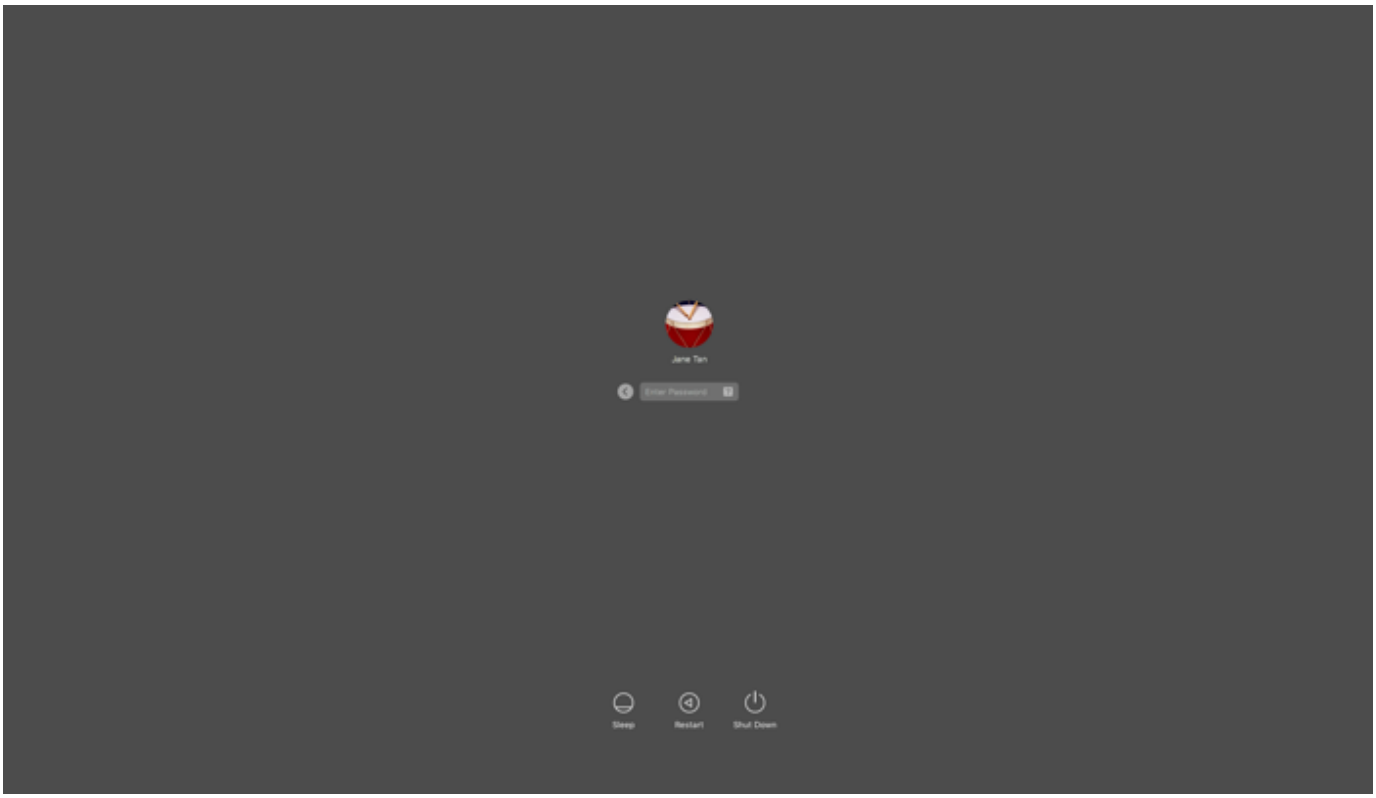
About this task

Authenticating using your device biometrics is simple using PingID mobile app. Authentication varies slightly depending on your phone model, phone settings, and whether your device is locked or unlocked when the authentication request is sent.

> **Note**
>
> Biometrics authentication is only available if the option is enabled by your organization.

Steps

1. Sign on to your Mac machine.



Result:

The **Authenticating** window opens, and an authentication notification request is sent to your mobile device.

2. Accept the authentication notification, depending on your mobile's notification settings:

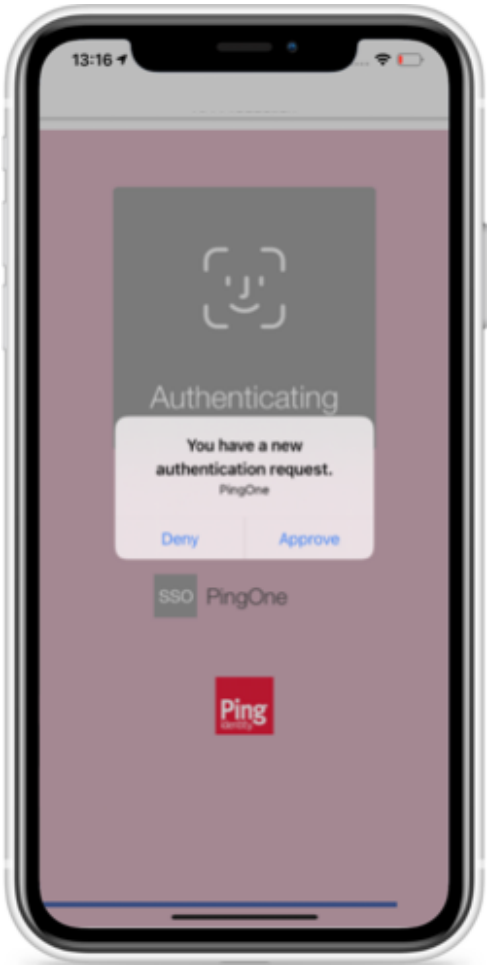
   Choose from:

   - If your device is locked, long press the notification until it shows the option to approve or deny the request, and then tap **Approve**.
   - If your device is unlocked, pull down the notification until it shows the option to Approve or Deny the request, and then tap **Approve**.

Note

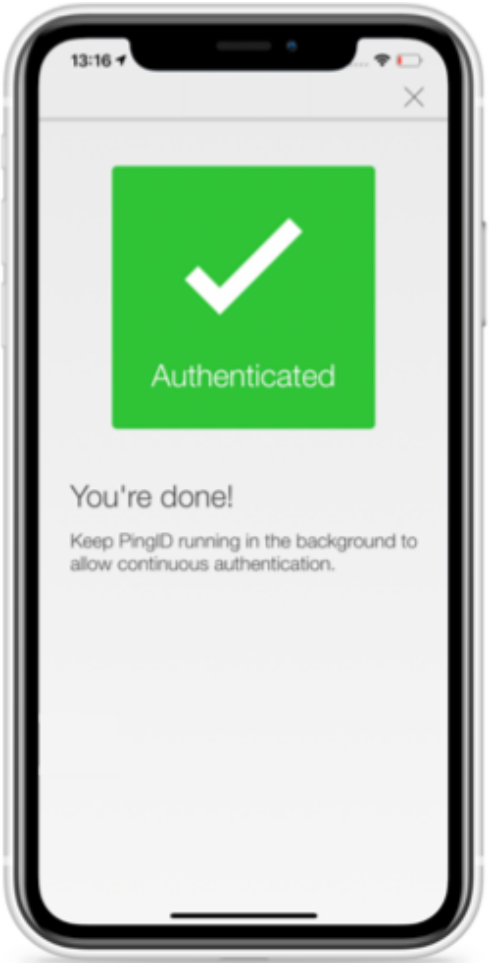
If configured by your organization, you'll see a map on the notification screen, showing the location, device type, and browser used by the device attempting to accessing your account or app. This can help you identify a fraudulent authentication attempt.

- If your mobile phone is unlocked and PingID is open, you'll be prompted to authenticate with your biometrics.
- Face ID: Tap the message asking you to authorize scanning with Face ID, if prompted, or your face is scanned automatically.
- Fingerprint: To scan your fingerprint, touch the Home button lightly.



Result:

The green **Authenticated** screen appears with a check mark, indicating successful authentication.



Result

You're signed on to your Mac machine.

Authenticating using your Apple Watch (legacy)

You can authenticate with PingID mobile app using your Apple watch. For current content, see Authenticating using a smart watch.

About this task

If you have an Apple Watch paired with your iPhone, the PingID mobile app automatically presents the **Approve** or **Deny** authentication notification on the Apple Watch, in parallel with your iPhone, so you can authenticate without taking your iPhone out of your pocket.

> **Note**
>
> You do not need to install the PingID app on your Apple watch to receive notifications. However, if you do install the app on your watch, you can also access a one-time passcode (OTP) from the app on your Apple watch.

Steps

1. If your mobile device is inactive and your Apple Watch is on your wrist, when you sign on, a notification appears on your Apple Watch, as well as your mobile device.Swipe up to view the message, and then tap **Approve**.

2. If you see three numbers displayed on your Apple Watch, your company also requires you to authenticate by number matching. If so, to complete authentication, select the number on your Apple watch that matches the number displayed on the **Authentication** screen.

Result

You'll see the green checkmark, indicating authentication is successful and you're signed in to your account.

Enabling and disabling passcodes on your Apple watch

Enable the use of PingID one-time passcodes (OTPs) on your Apple watch.

About this task

If you have installed the PingID app on your device, the PingID Apple Watch app is automatically installed on your watch and you will start receiving notifications to your watch. You can also open the PingID app on your watch to receive a one-time passcode (OTP). If the Apple watch app is disabled, you will not be able to access a one-time passcode from your watch.

> **Note**
>
> The Apple watch only receives notifications when your mobile device is locked, and the mobile device screen is in sleep mode.

Steps

1. On your iPhone, tap the Watch app, and then tap **PingID**.
2. To enable or disable the app on your Apple watch, tap **Show App on Apple Watch**.

   Result:

   The PingID app is installed on your Apple watch, and the PingID icon appears.
3. To view the current one-time passcode, on your Apple watch, tap the PingID icon.

4. (Optional) To get a new passcode, tap **Refresh**.

Authenticating using a one-time passcode (Mac Login)

Using PingID mobile app on your Android to get a one-time passcode with which to authenticate, so you can access your Apple Mac machine.

Before you begin

To authenticate using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- You have paired your mobile device (Android or iOS).

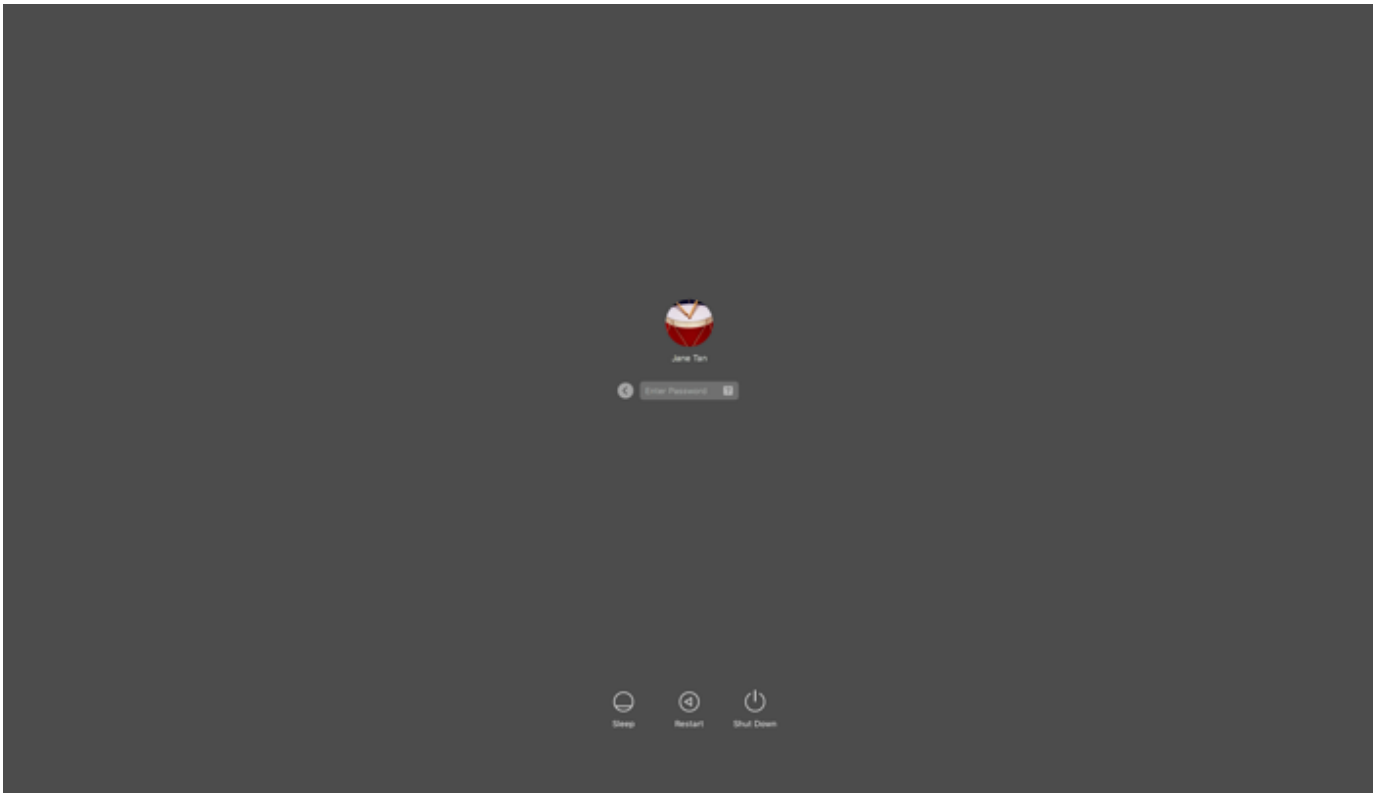
About this task

If you don't have internet access from your mobile device temporarily, you can still authenticate using PingID mobile app by generating a one-time passcode (OTP). The one-time passcode is unique, and can only be used once. Only the one-time passcode that appears on your device at the time that you sign on to your account is valid for authentication.

> **Note**
>
> You'll only be able to view and use the one-time passcode if permitted by your organization's policy.

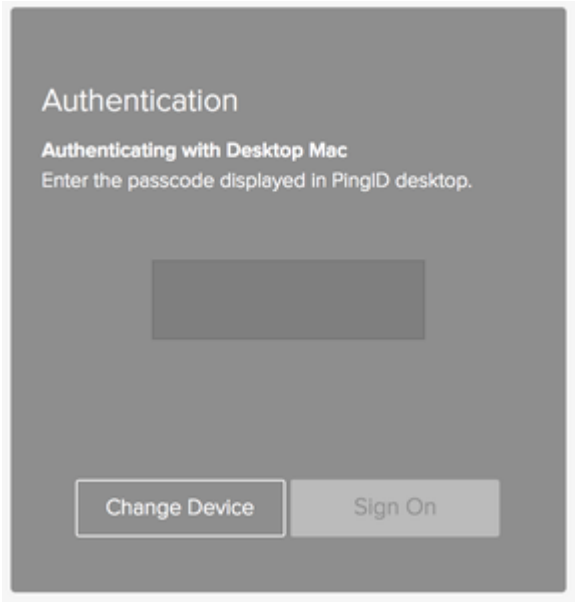
Steps

1. Sign on to your Mac machine.



Result:

The **Authenticating** window opens, and an authentication notification request is sent to your mobile device.



2. On your mobile device, open the PingID mobile app and enter the one-time passcode into the passcode field on the authentication screen. Press Enter.

> **Note**
>
> - When opening PingID mobile app, update your location permissions to **Allow all the time**, if prompted to do so.
> - The one-time passcode refreshes each time you open the PingID app. To generate a new one-time passcode, tap **New Passcode**.

Result:

You're signed on to your Mac machine.

Authenticating manually with PingID mobile app (Mac Login)

Authenticate using PingID mobile app when your

Before you begin

To authenticate manually using PingID mobile app, make sure:

- Your Apple Mac is running Mac OS v10.13 or later.
- Your device has PingID mobile app V1.8 or higher paired with your account.
- You have paired your device and authenticated online with PingID at least once to the Mac machine that you are trying to access.
- You have a working camera on your device, with PingID mobile app camera permissions set to **Approve**. For more information, see PingID mobile app management (legacy).

About this task

If you try to sign on to your Mac machine without having a network connection (e.g., in airplane mode, or when without Wi-Fi connection), you might be asked to authenticate manually using the PingID mobile app. Authenticating manually is slightly different than the way you usually sign on.

> **Note**
>
> If you have paired a security key for offline authentication, you also see the option to choose your security key to authenticate.

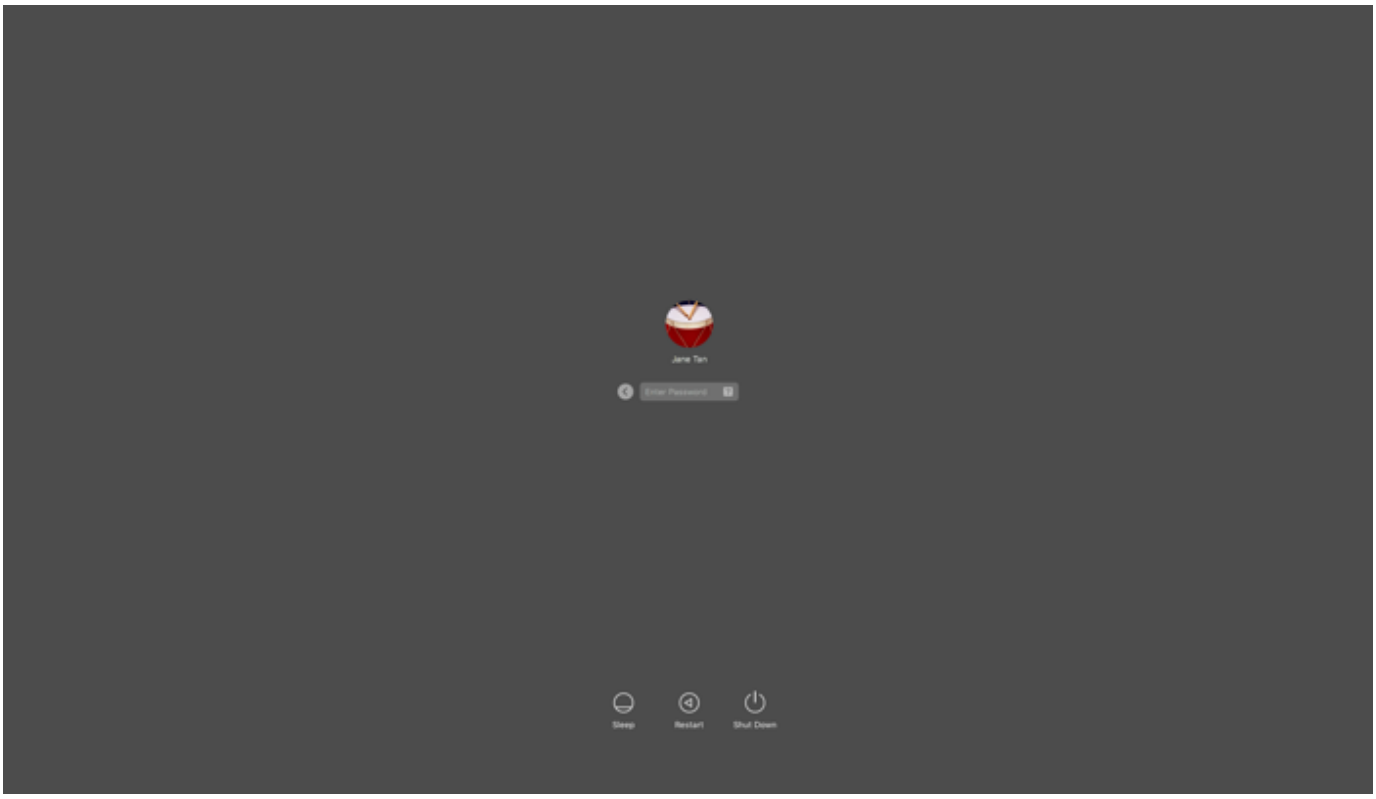
{{{ Video removed }}}

Steps

1. Sign on to your Mac machine.

   Result:

   You'll see a notice telling you that you need to manually authenticate.

   > **Note**
   >
   > If you have more than one device paired with your account, you'll see a list of your devices. Select the device you want to use to authenticate.

2. Click **Next**.

   Result:

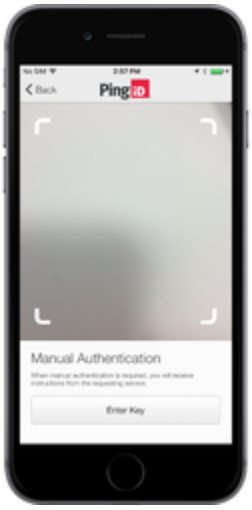
   You'll see a Manual Authentication message, displaying a QR code, requesting that you authenticate manually.

3. On your mobile device, open PingID mobile app.
4. Tap 

   and select **Manual Auth**. Authenticate with your device biometrics, if required.

Result:

The QR code scanner for manual authentication opens.



5. Use your mobile device to scan the QR code displayed on the **Manual Authentication** window.

   Result:

   You'll receive an authentication code.

6. Enter the authentication code into the **Manual Authentication** window, and click **Sign on**.

   Result:

   You're signed on to your machine.

Authenticating using PingID desktop app

Use PingID desktop app to generate a one-time passcode (OTP) that you can use to authenticate securely to access your account, app, VPN, or Windows login machine through Remote Desktop Protocol (RDP).

Before you begin

- Download PingID desktop app and then pair your device with your account to enable authentication (see Using PingID desktop app authentication).

About this task

If your organization allows it, you can authenticate PingID desktop app to access your account using a web browser, to access your company's VPN, or to access a Windows login machine using RDP.

Web

Authenticating using the PingID desktop app (Web)

Authenticate using the PingID desktop app.

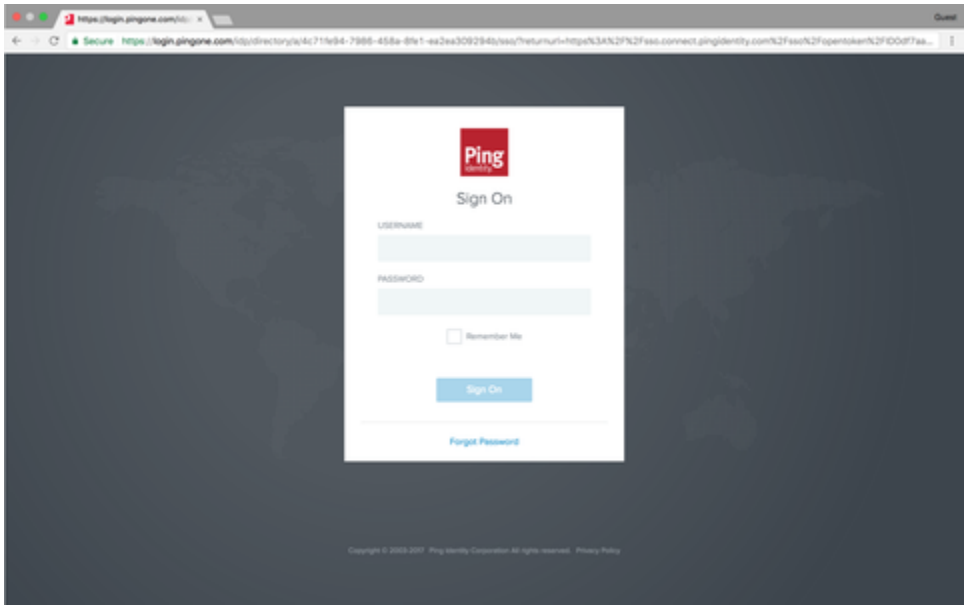
Before you begin

You must pair the PingID desktop app with your account. For more information, see:

- Pairing your PingID desktop app

Steps

1. Sign on to your account or access an application that requires authentication.



Result:

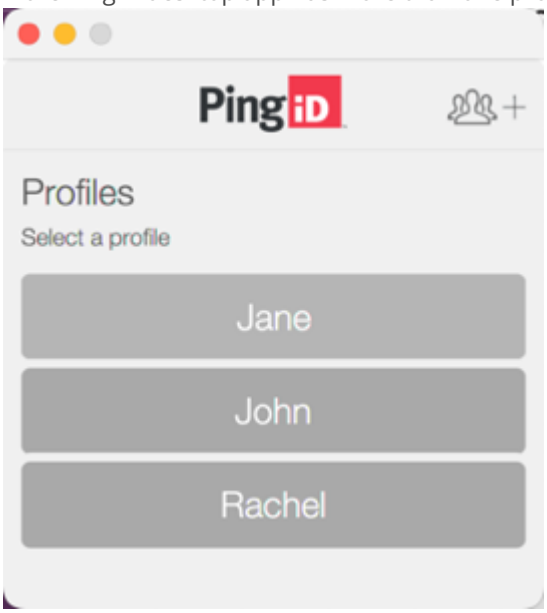
The **Authentication** window opens, prompting you to enter a OTP.

2. In the **Authentication** window, enter the OTP that displays in your PingID desktop app. Click **Sign On** to launch the PingID desktop app.

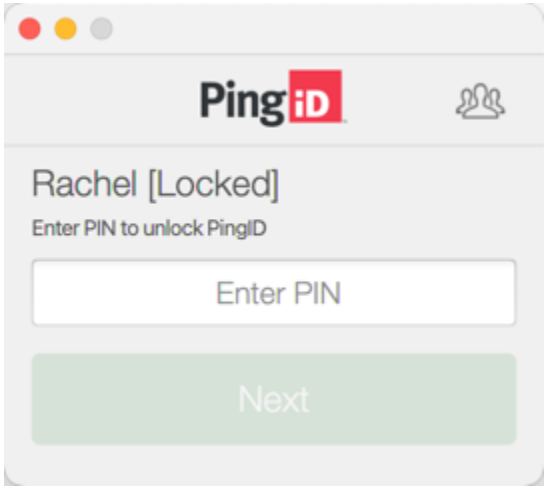
   Result:

   If more than one profile exists on PingID desktop app, all profiles are displayed. If your organization requires you to enter a PIN code, the **Locked** window displays, prompting you to enter a PIN.

3. If the PingID desktop app has more than one profile, select your profile, otherwise skip this step.



4. If the **Locked** window displays and you are prompted to enter a PIN code, enter the PIN code and then click **Next**, otherwise skip this step.

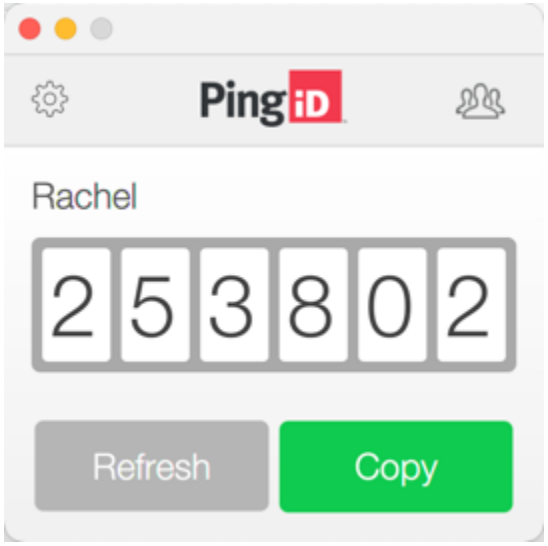


Result:

The PingID desktop app displays an OTP.

5. Click **Copy** to copy the OTP and paste it into the **Authentication** window.

> **Note**
>
> Ensure the browser window is the active window when pasting the OTP. You can only use an OTP once. Click **Refresh** to generate a new OTP, if required.



6. Click **Sign On**.

Result:

The green **Authenticated** message with a checkmark appears, indicating your authentication is successful, and your access is approved.

VPN

Authenticating using the desktop app (VPN)

After you setup the PingID desktop app authentication for web, use the desktop app to generate a OTP to use to authenticate with a VPN.

About this task

Use the PingID desktop app to authenticate for web with a VPN.

Steps

1. From your web browser or application sign on to your VPN:
    1. Enter your username and password.
    2. Click **Sign In**.

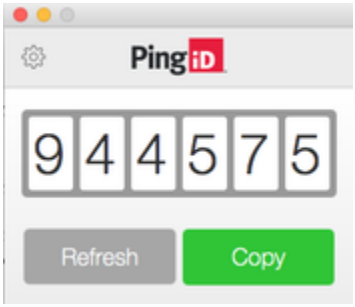
    Result:

    For multiple devices only: a message displays all of your devices in a numbered list.

    1. Enter the number for the PingID desktop app and then click **Sign In**.
2. Launch the PingID desktop app.

    Result:

    A passcode generates.

3. In the blank field, enter the OTP and then click **Sign In**.

    Result:

    After you successfully authenticate, your browser is redirected to your VPN.

Windows login using RDP

Authenticating using the desktop app (Windows login)

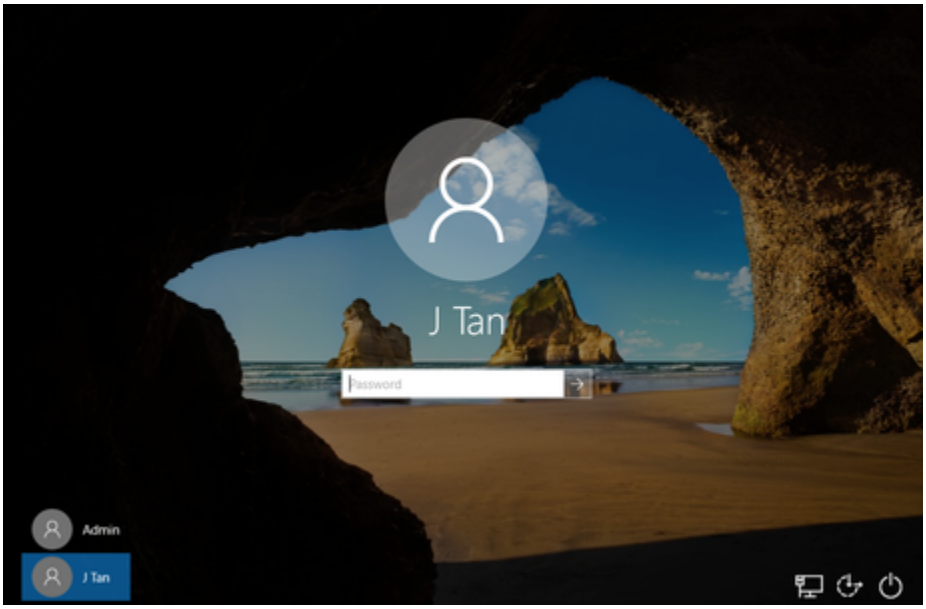
Authenticate using the PingID desktop app to access a Windows machine that requires PingID multi-factor authentication (MFA).

About this task

> **Important**
>
> To authenticate for your Windows machine, set up the PingID desktop app on a different machine from the Windows machine you are accessing.

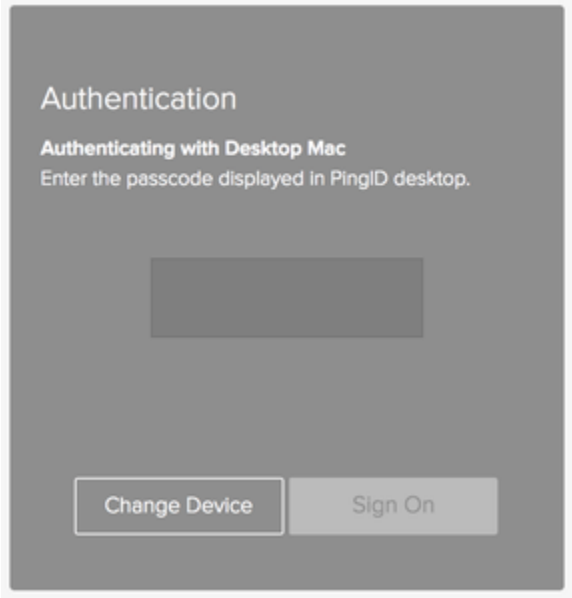
Steps

1. Sign on to your Windows machine either locally or remotely using an RDP.

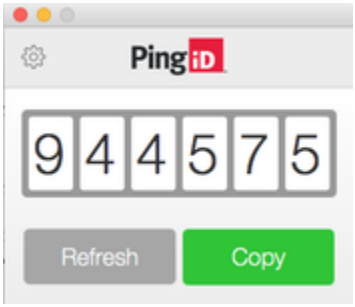


Result:

The **Authentication** window appears, prompting you to enter a passcode.



2. Launch the PingID desktop app from a local machine.



Result:

The PingID app generates a passcode.

3. On the Windows machine, in the **Authentication** window, enter the passcode. Click **Sign On**.

Result:

The green check mark appears, indicating successful authentication. You are signed on to your Windows machine.

Authenticating with PingID using Windows Hello

Authenticate using Windows Hello through PingID to access your account or app through a web browser.

Before you begin

To authenticate using the built-in biometrics in your Windows Hello machine, ensure the following:

- You've paired your Windows Hello device with PingID. See Pairing your Windows Hello device.
- You are using a browser that supports FIDO2 biometrics, such as Microsoft Edge, and that you have the latest version of the browser.

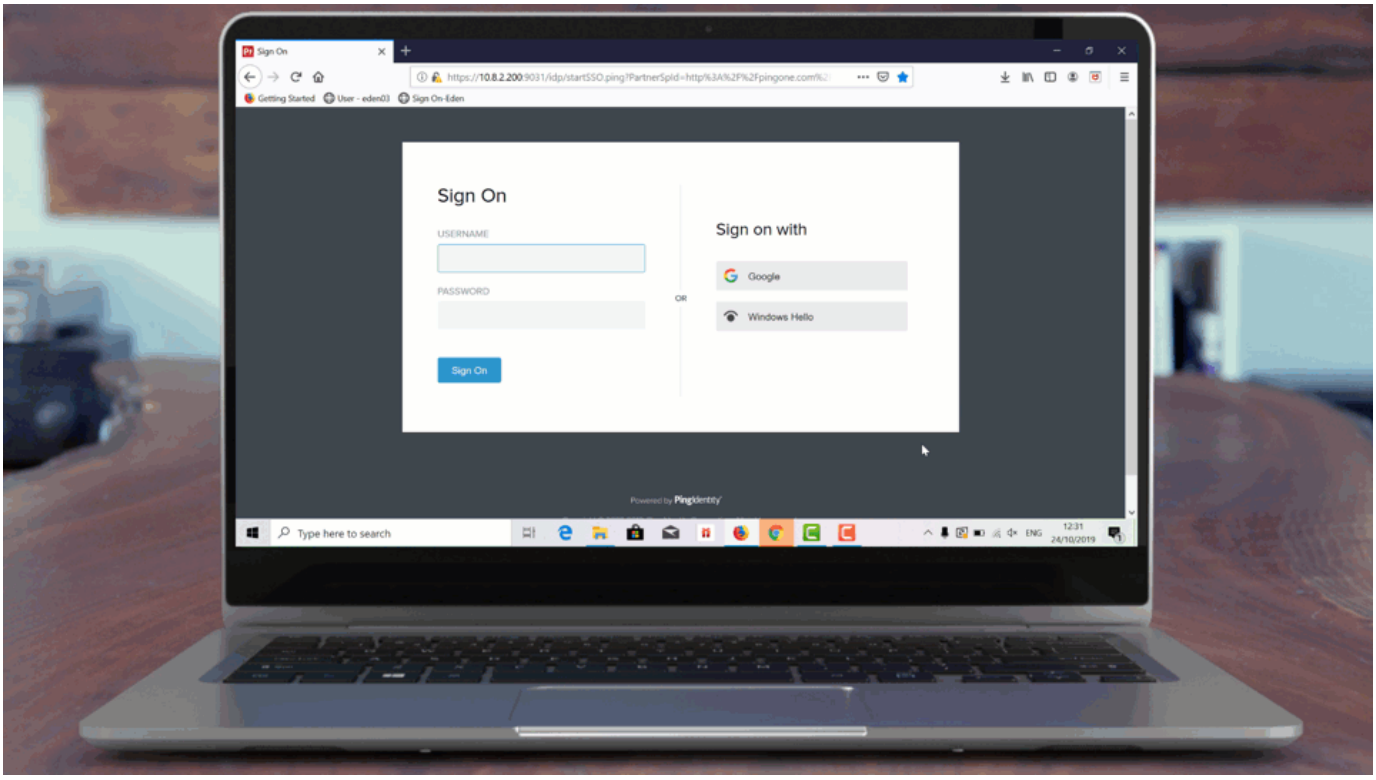
> **Note**
>
> You can only use Windows Hello to authenticate when you are accessing your account or resources from your Windows Hello machine.

About this task

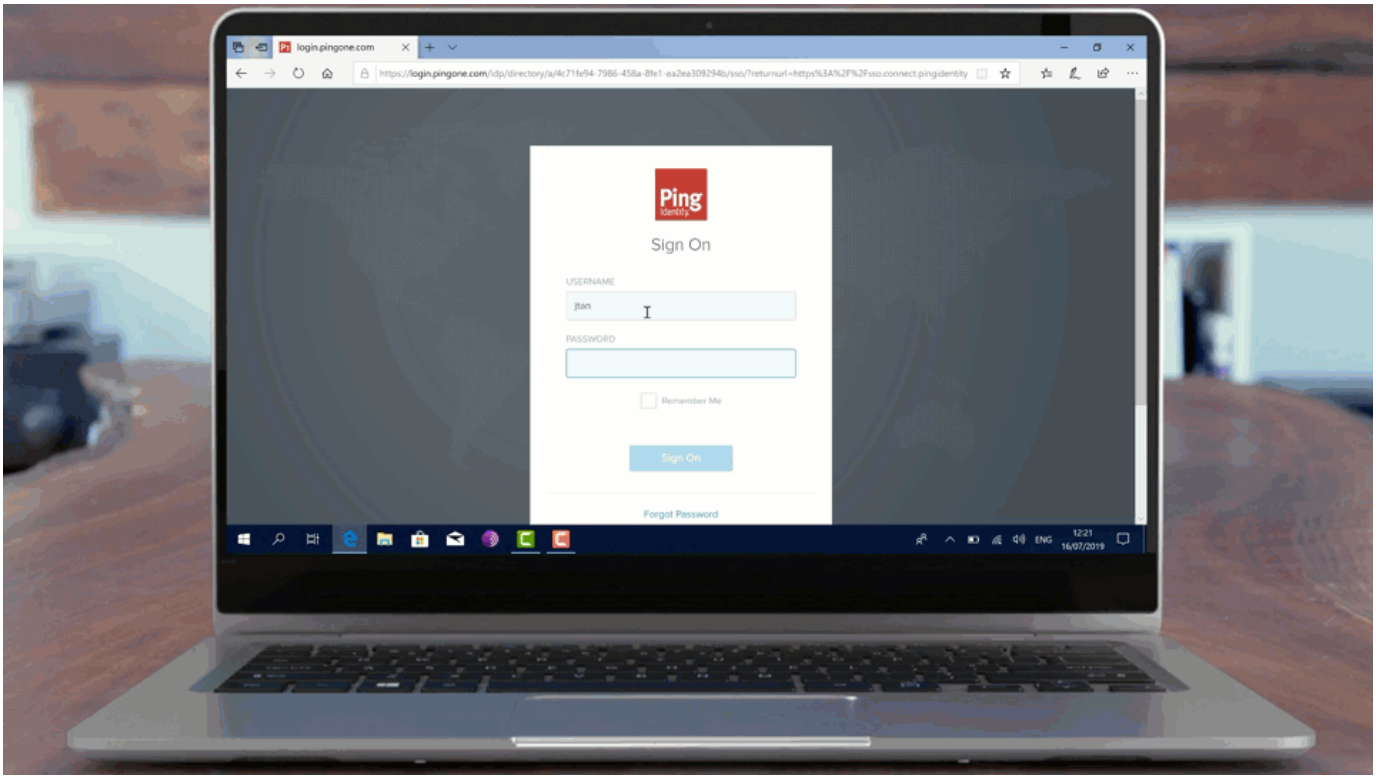
The authentication process varies slightly depending on your browser and your organization's implementation.

The following animations demonstrate the two most common implementations of biometrics authentication with PingID for Windows Hello:

- **Passwordless authentication**: No username or password required.



- **Second factor authentication**: Enter your username and password, and then authenticate with Windows Hello for a more secure sign on.



Steps

1. Sign on to your Windows Hello machine:

   Choose from:

   - Open a browser window and sign on to your account.
   - Access an application that requires authentication.

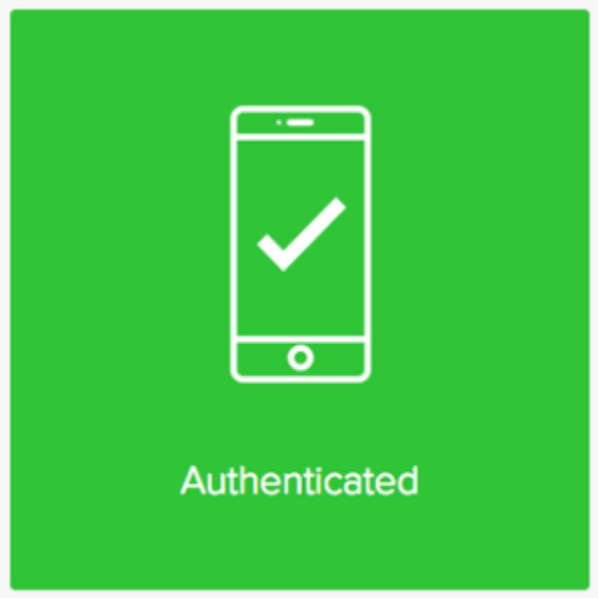
   > **Note**
   >
   > You might see an additional window in your browser prompting you to authenticate. The actual appearance of this window varies depending on your browser.

2. In the **Authentication** window, authenticate using the built-in biometrics on your Windows Hello machine, for example using your fingerprint.

   > **Tip**
   >
   > Ensure the browser window is the active window.

Result

A green **Authenticated** message with a check mark appears, indicating authentication is successful. You are redirected to your account or app.



Related links

- Troubleshooting FIDO2 biometrics

Authenticating with PingID using Apple Mac Touch ID

Using the built-in biometrics in your Apple Mac machine to authenticate securely with PingID when accessing your account or app using a web browser.

Before you begin

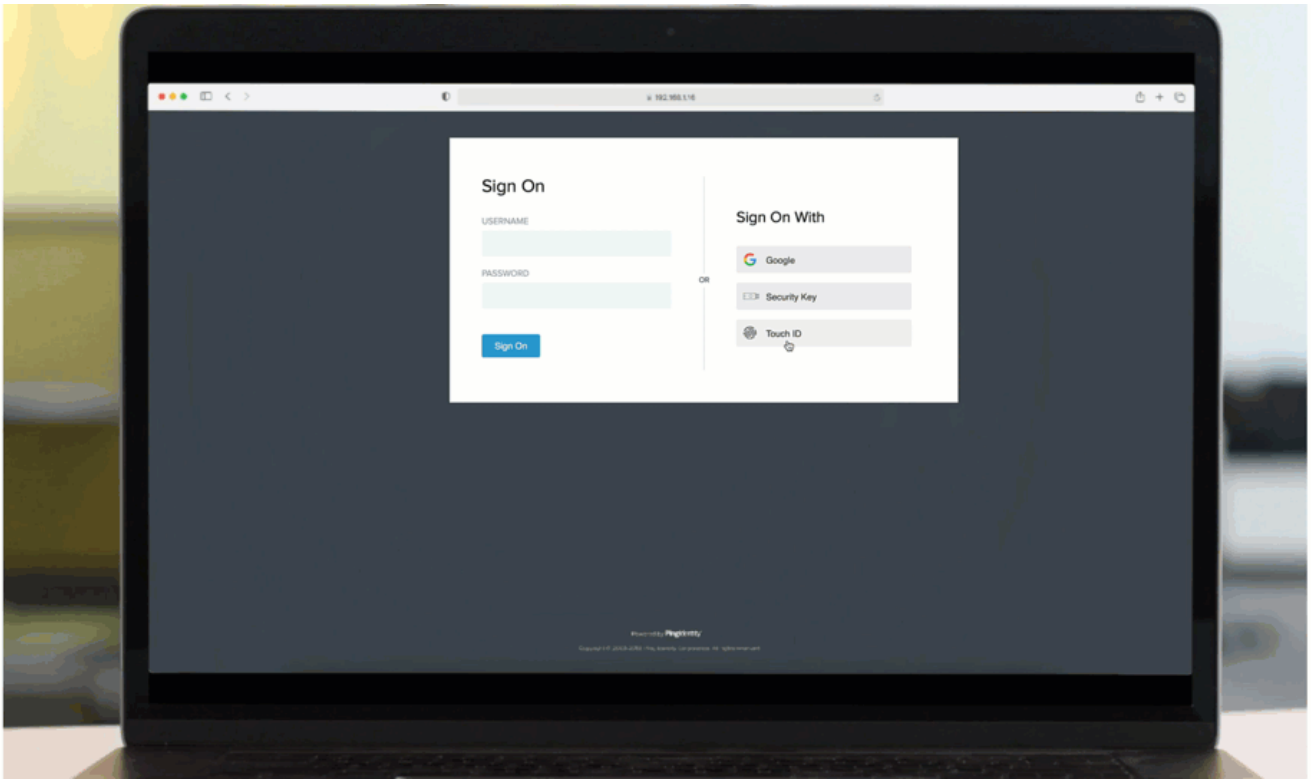
- Ensure your Mac device is paired with PingID. For more information, see Pairing your Mac Touch ID device.
- Use a browser that supports FIDO2 biometrics, such as Google Chrome or Safari, and that you have the latest version of the browser.

About this task

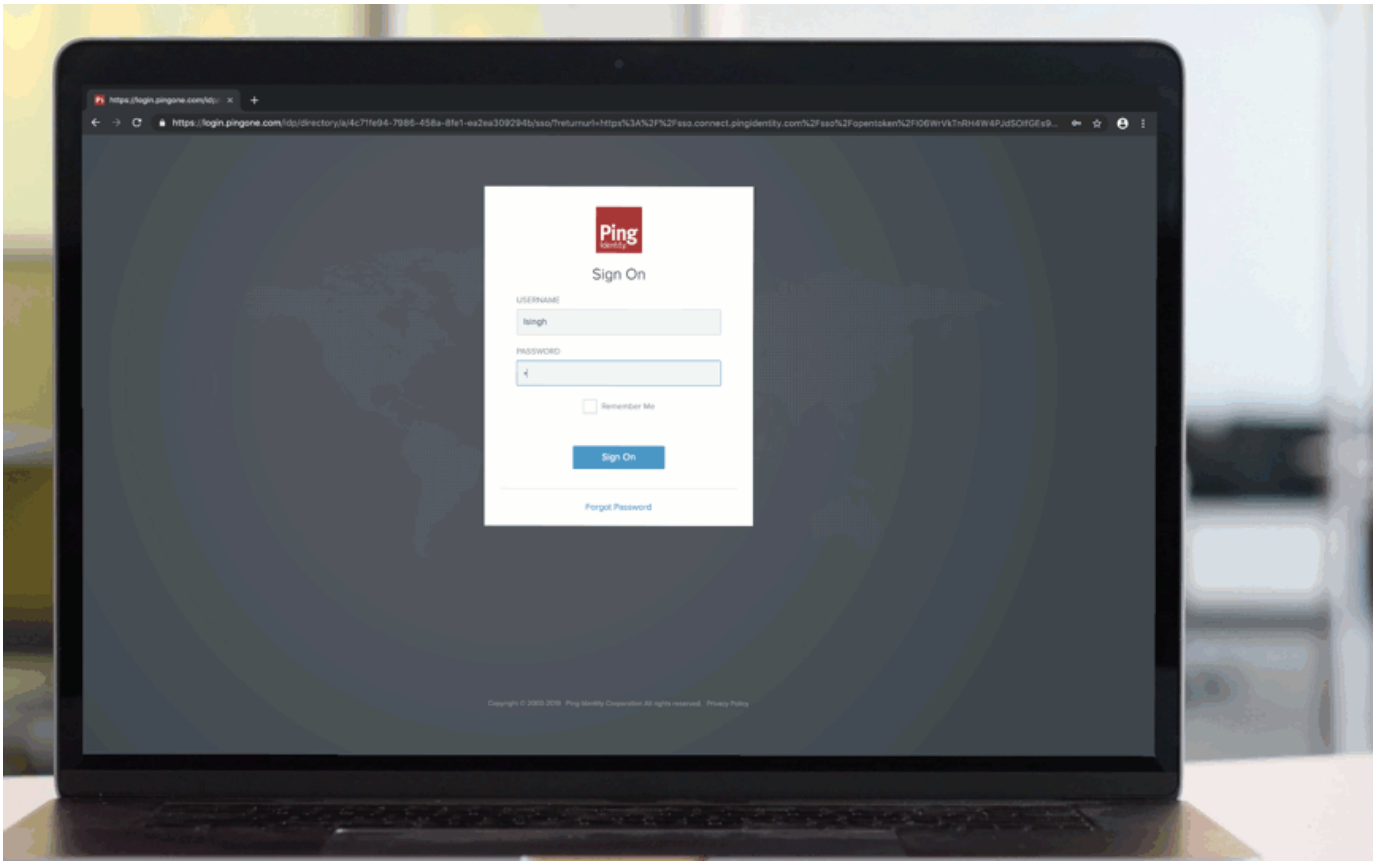
The authentication process varies slightly depending on your browser and your organization's implementation.

The following animations demonstrate the two most common implementations of biometrics authentication with PingID for Mac:

- **Passwordless authentication**: No username or password required.



- **Second factor authentication**: Enter your username and password, and then authenticate with Mac Touch ID for a more secure sign on.



Steps

1. On your Mac machine, open a browser window and sign on to your account or access an application that requires authentication.

   > **Note**
   >
   > Depending on the browser that you are using, an additional window might appear in your browser prompting you to authenticate.

   Result:

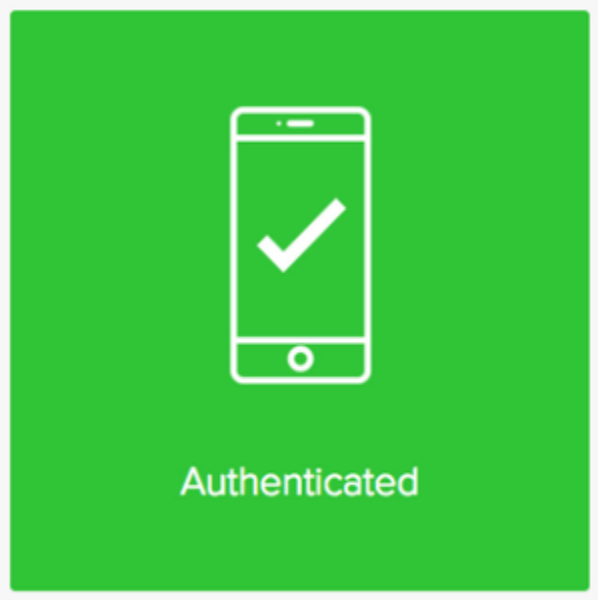
   An **Authentication** window appears, prompting you to authenticate.

2. Use your Mac device to validate your identity, such as using your fingerprint.

   > **Note**
   >
   > Ensure the **Authentication** window is selected as the active window before you authenticate.

Result

A green **Authenticated** check mark appears, indicating your device pairing is successful, and you are automatically signed on to your account or app.



Related links

- Troubleshooting FIDO2 biometrics

Authenticating with PingID using iOS or iPadOS biometrics

Authenticate using the built-in biometrics on your iPhone or iPad device with PingID, when accessing your account or app using a web browser.

Before you begin

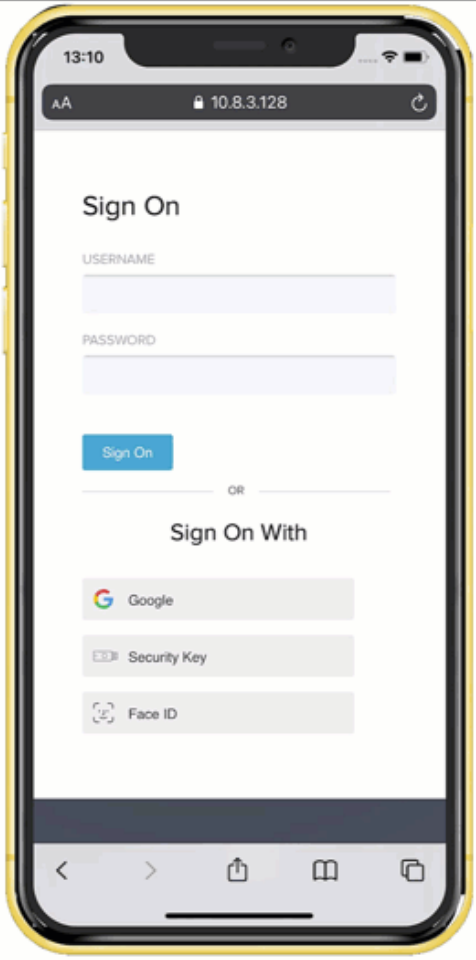
- Ensure that you paired your iOS or iPadOS biometrics device with PingID. For information, see Pairing your iOS or iPadOS biometrics device.
- Use a browser that supports FIDO2 biometrics, such as Safari 14 or later, and make sure that you have the latest version of the browser.
- Ensure that you are using a device with iOS or iPadOS 14 or later, and have biometrics set up on your device (such as Face ID or fingerprint).

About this task

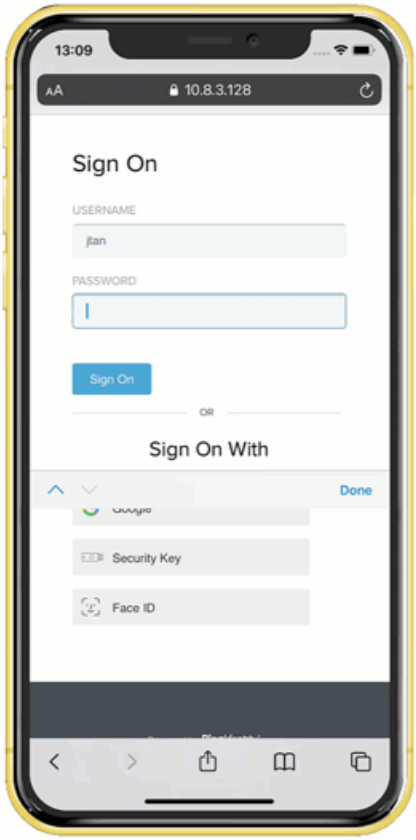
The authentication process varies slightly depending on your browser and your organization's implementation.

The following animations demonstrate the two most common implementations of biometrics authentication with PingID for iOS:

- **Passwordless authentication**: Authenticate using your biometrics, without entering a username or password.



- **Second factor authentication**: Enter your username and password, and then authenticate with your biometrics device.



Steps

1. On your iPhone or iPad, open a browser window and sign on to your account or access an application that requires authentication.

   > **Note**
   >
   > Depending on your browser, an additional window might appear in your browser prompting you to authenticate.

   Result:

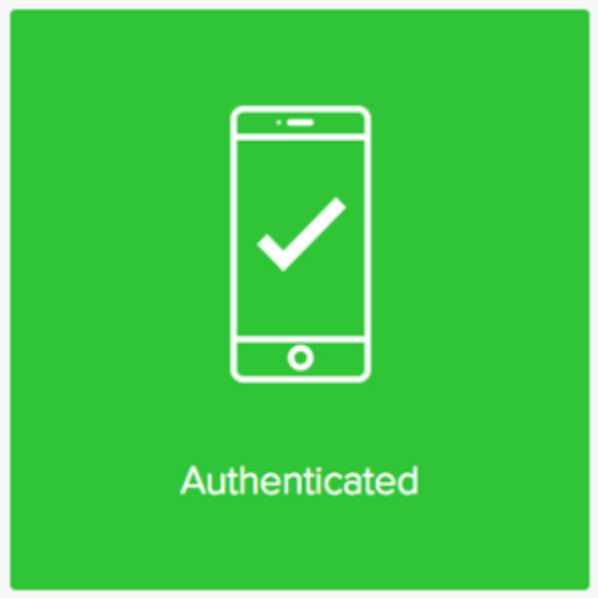
   An **Authentication** window appears.

2. Tap **Continue** and then authenticate using the fingerprint or face sensor on your device.

   > **Note**
   >
   > If you have more than one account associated with your device, you'll see a list of accounts. Select the account you want to access and then tap **Continue**.

Result

A green **Authenticated** message with a check mark appears indicating your device pairing is successful, and you are automatically signed on to your account or app.



Related links

- Troubleshooting FIDO2 biometrics

Authenticating with PingID using an Android biometrics

Authenticate using the built-in biometrics on your Android device with PingID when accessing your account or app using a web browser.

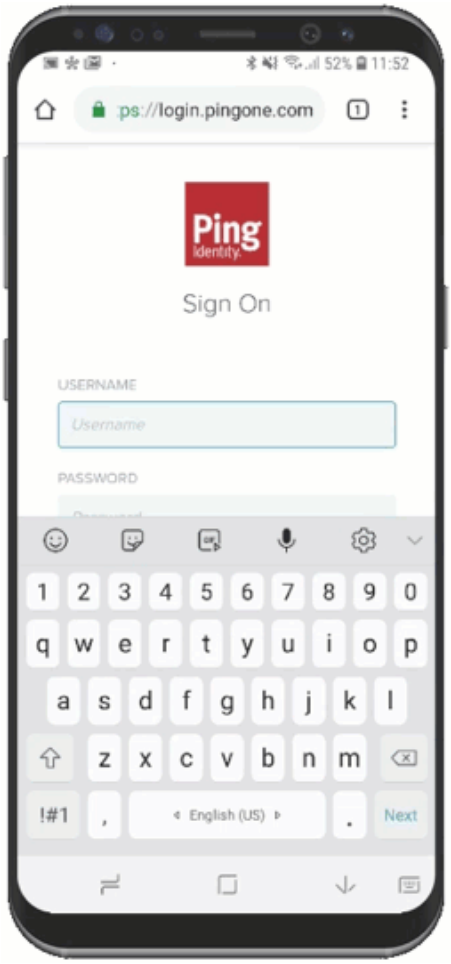
Before you begin

- Ensure you paired your Android biometrics device with PingID. See Pairing your Android biometrics device.
- Use a browser that supports FIDO2 biometrics, such as Google Chrome or Microsoft Edge, and that you have the latest version of the browser.
- If you are authenticating with a mobile device, ensure you are using a device with Android v7 or later. iPhone and iPad devices do not currently support FIDO2 biometrics.

About this task

The authentication process might vary depending on your browser.

The following example shows biometrics authentication on an Android device.



Steps

1. On your Android biometrics accessing device, open a browser window and sign on to your account or access an application that requires authentication.

   > **Note**
   >
   > Depending on your browser, an additional window might appear in your browser prompting you to authenticate.

   Result:

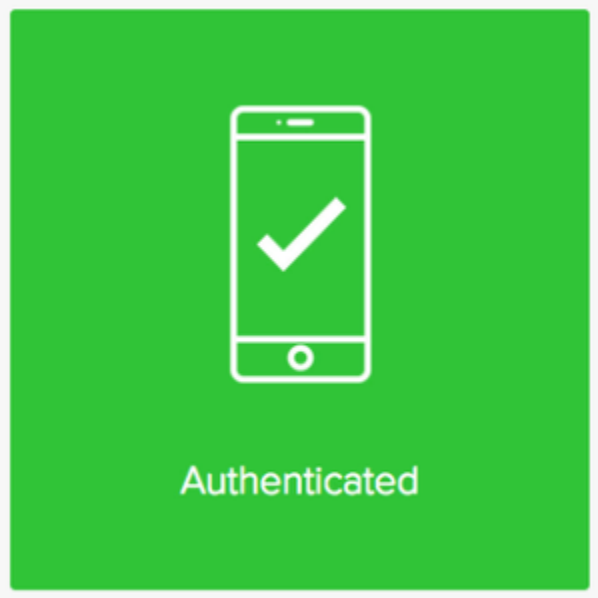
   An **Authentication** window appears, prompting you to authenticate.

2. Authenticate using the fingerprint or face sensor on your device.

   > **Note**
   >
   > Ensure the **Authentication** browser window is selected as the active screen before you authenticate.

Result

A green **Authenticated** message with a check mark appears indicating your device pairing is successful, and you are automatically signed on to your account or app.



Related links

- Troubleshooting FIDO2 biometrics for Android

Authenticating with PingID using a security key

You can authenticate using a security key access your account or app securely with PingID.

Before you begin

- Pair your security key with your account to enable authentication. For information, see Setting up a security key or Managing your devices.
- Ensure you are using a browser that supports the use of a security key, such as Google Chrome or Microsoft Edge, and that you have the latest version of the browser. The authentication process might vary slightly depending on the browser that you are using.
- To authenticate with a mobile device, the mobile device must be running either:
  - Android devices: Android 7 or later
  - iOS devices: iOS 13.3 or later
- If you are using a virtual machine (VM) to connect to your accessing device and want to authenticate using your security key, ensure that your VM is configured to recognize a USB device.

About this task

You can use a security key to access your account using a web browser or to access a Windows login machine.

> **Note**
>
> - The authentication process might vary slightly depending on the browser that you are using and your organization's implementation.

Authenticating using a security key

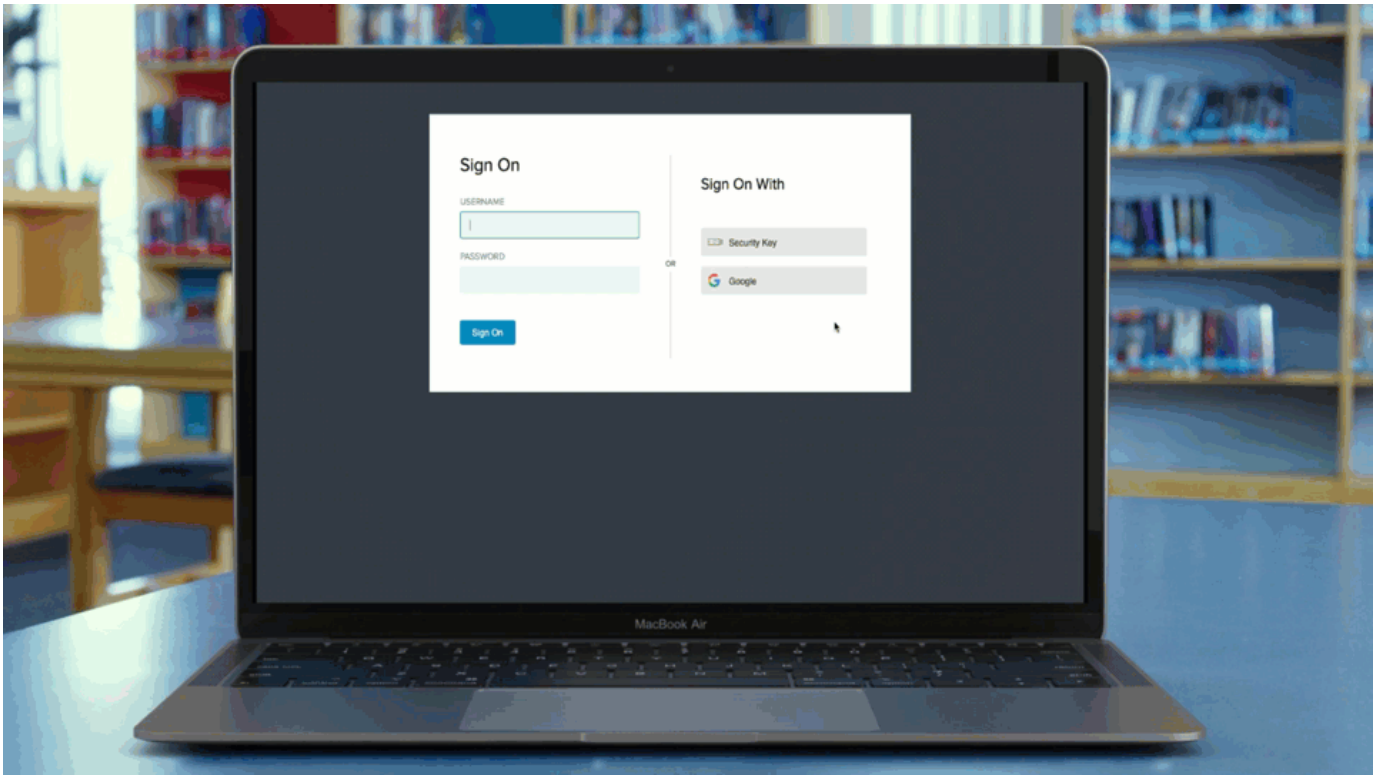
Authenticate using a security key to securely access your account or app using a web browser.

About this task

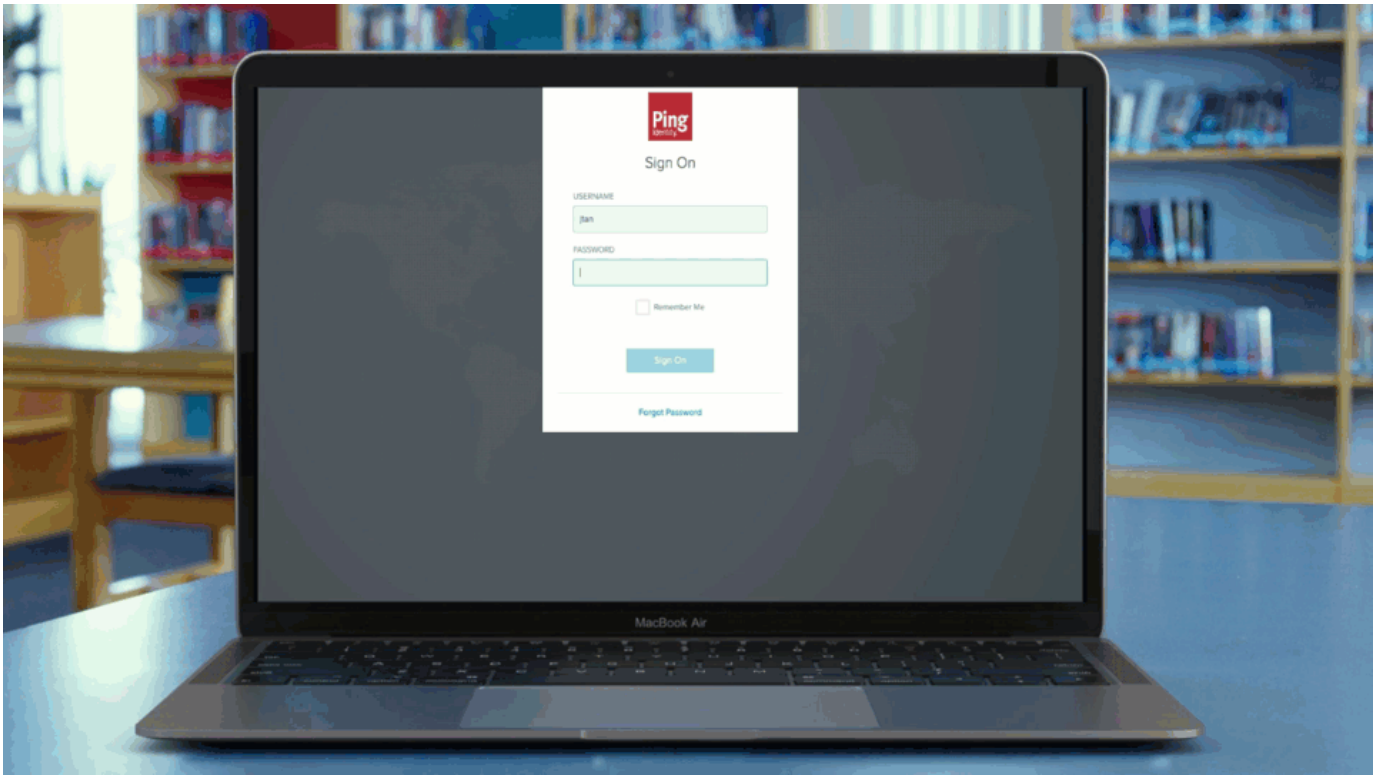
The authentication process might vary slightly depending on the browser that you are using and your organization's implementation.

The following animations demonstrate the two most common implementations of security key authentication with PingID:

- **Passwordless authentication**: No username or password required.



- **Second factor authentication**: Enter username and password, and then authenticate with your security key for a more secure sign-on.



> **Note**
>
> Your security key must be paired with your account to enable authentication. For more information, see Pairing your security key.

Steps

1. Connect your security key.

   Choose from:

   - Connect through a USB cable.
   - If your security key model supports it, connect through NFC or Bluetooth, and make sure it is set to **ON**.

2. Open a browser window and sign on to your account or access an application that requires authentication.

> **Note**
>
> - Depending on your browser, an additional window in your browser might appear prompting you to authenticate with a security key.
> - If you are using iOS or macOS, you might be presented with an additional dialog where you must press **Continue** before authenticating with the key.

Result:

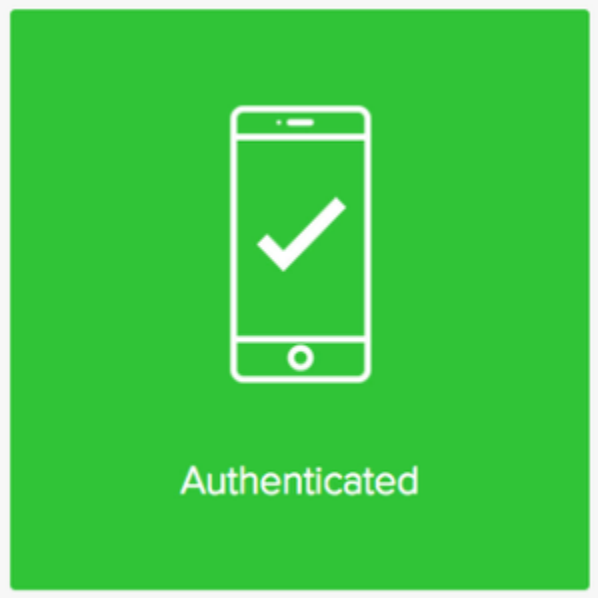
The **Authentication** window appears, prompting you to authenticate using your security key.

3. Use your security key to authenticate.

> **Tip**
>
> Select the **Authentication** browser window as the active window before you press the security key button.

Result

The green **Authenticated** message with a check mark appears, indicating successful authentication, and you are redirected to your account or app.



Authenticating using a security key (Windows login)

Use your security key to authenticate for a successful sign-on to your Windows device.

Before you begin

- The minimum version of Windows login you need depends on the following:
  - If your organization requires you to enter a password to authenticate, you'll need PingID for Windows login 2.3 or later.
  - If your organization has eliminated passwords, you'll need PingID for Windows Passwordless login 1.2 or later.

  If you're not sure, check with your organization's administrator.

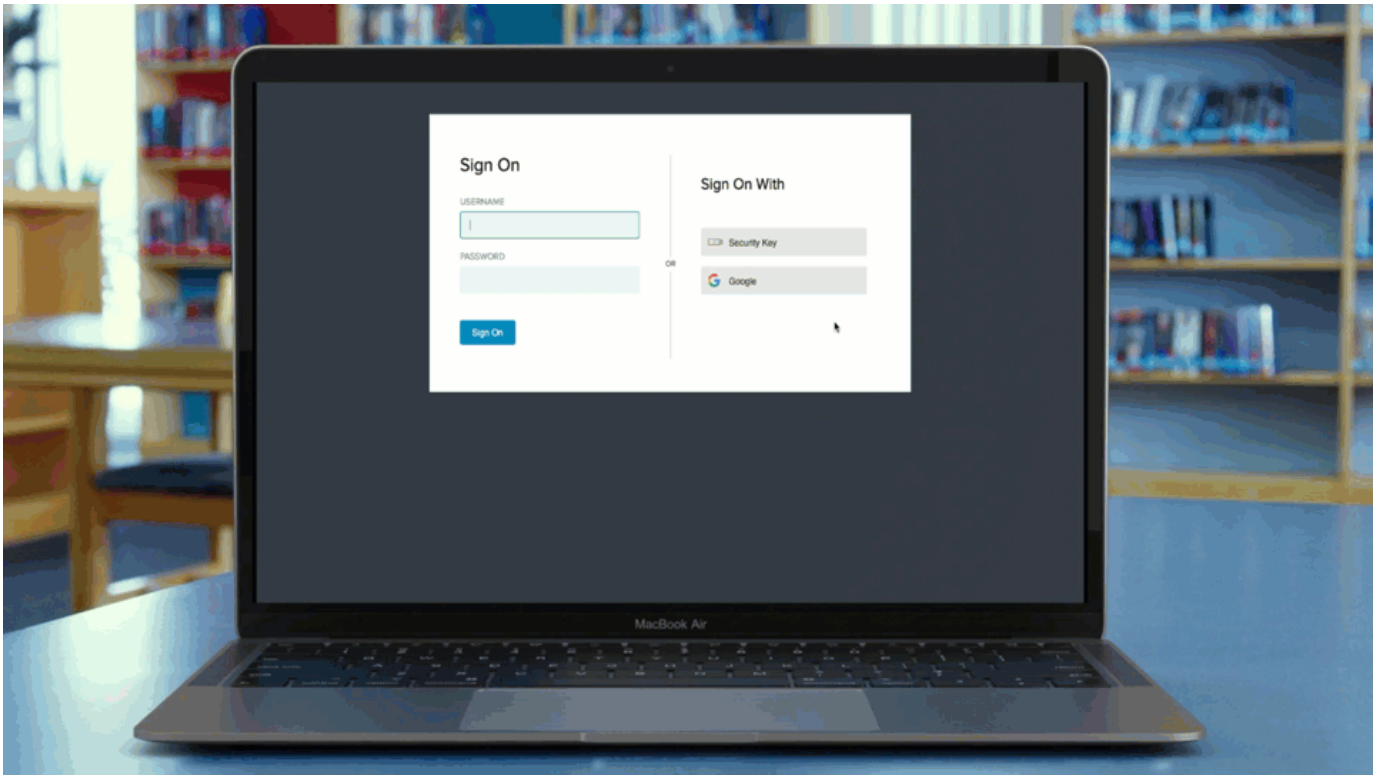
Note

- If your organization requires you to enter a password when you sign on, it is not possible to use a FIDO2 security key to authenticate when accessing your Windows login account through RDP. If your organization has eliminated passwords, you can do so.
- To use your security key to authenticate when you are offline, you must authenticate successfully at least once when online. For more information, see Authenticating using a security key for manual authentication.

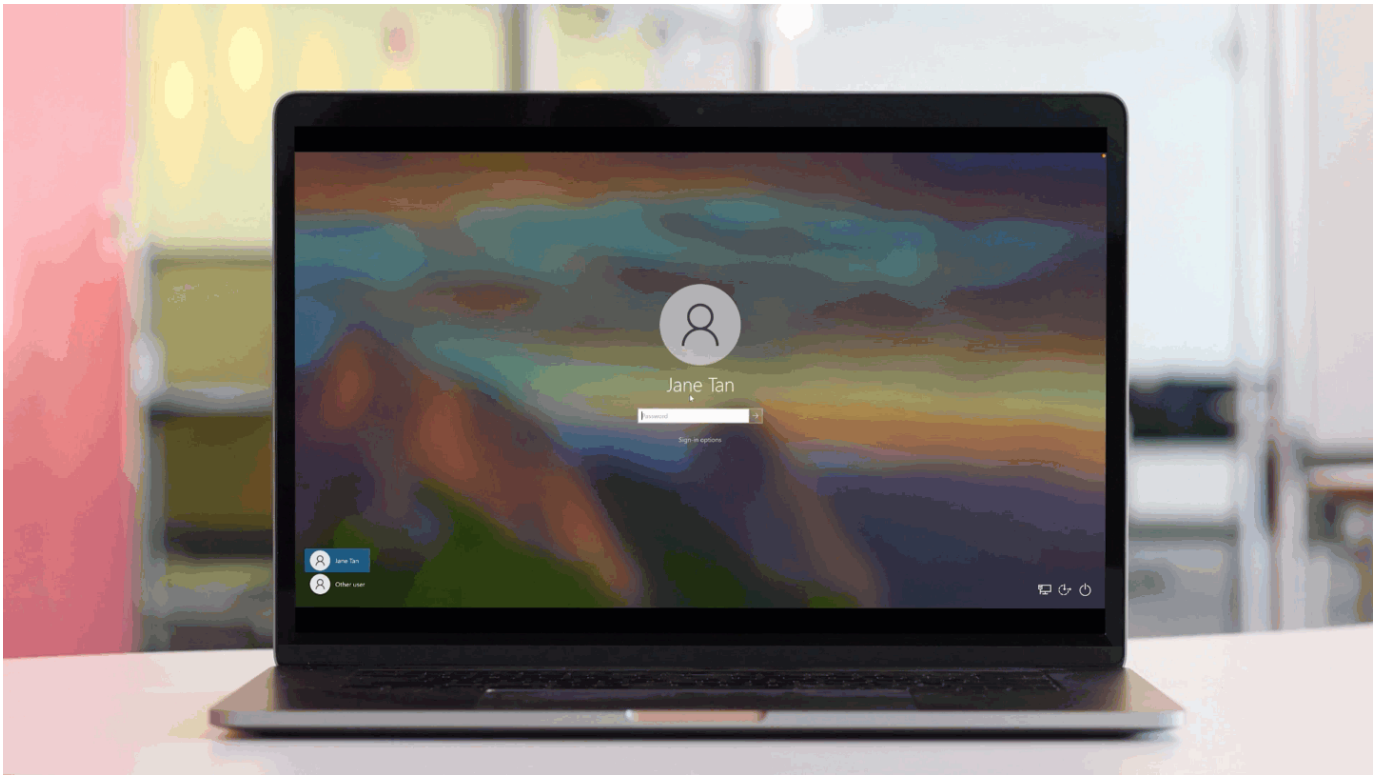
About this task

The authentication flow varies slightly according to your organization's configuration policy.

- Passwordless authentication



- Authentication with a password



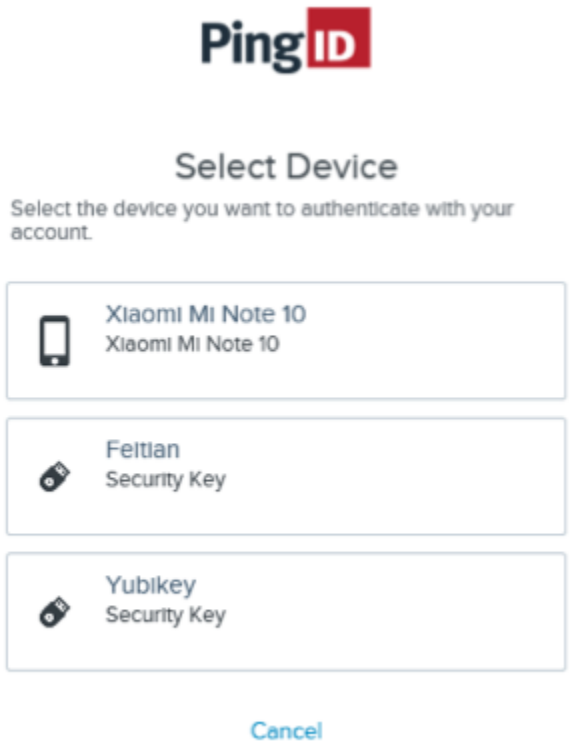
Steps

1. Sign on to your Windows laptop or desktop machine.

Choose from:

- If your organization has eliminated passwords: Under **Sign-in options**, click the PingID icon ( ), and then click the arrow.
- If your organization requires a username and password: Under **Sign-in options**, click the key icon ( ) , enter your username and password, and then click the arrow key.

2. (Windows passwordless users only) If you have more than one device paired with your account, you'll see a list of your paired devices. Select the security key that you want to use to authenticate.



3. When you see a window asking you to authenticate with your security key, connect your security key, either physically through a USB cable or, if applicable, ensure NFC or Bluetooth are set to **ON**. If you have a biometrics security key, tap it with your fingerprint to authenticate, otherwise enter your PIN code, if prompted to do so.

> **Note**
>
> You might see a message indicating that you are using one or more deprecated security key. If so, you should delete all deprecated devices (deprecated devices show the **Delete** option). Before you delete a device, make sure you have at least one alternative device paired with your account.

Result:

You are redirected to your Windows account.

Authenticating using a security key for manual authentication (Windows login)

You are only prompted to authenticate manually if you are signing on to your Windows machine without a network connection or Wi-Fi.

Before you begin

- To use your security key to authenticate when you are offline, you must authenticate successfully at least once when online. For information, see Authenticating using a security key (Windows login).
- The minimum version of Windows login you need depends on the following:
  - If your organization requires you to enter a password to authenticate, you'll need PingID for Windows login 2.3 or later.

- If your organization has eliminated passwords, you'll need PingID for Windows Passwordless login 1.2 or later.

If you're not sure, check with your organization's administrator.

- If your organization requires you to enter a password when you sign on, it is not possible to use a FIDO2 security key to authenticate when accessing your Windows login account through RDP. If your organization has eliminated passwords, you can do so.
- If you are using a U2F security key, offline authentication is only supported when using PingID for Windows login 2.3 - 2.7.x.

About this task

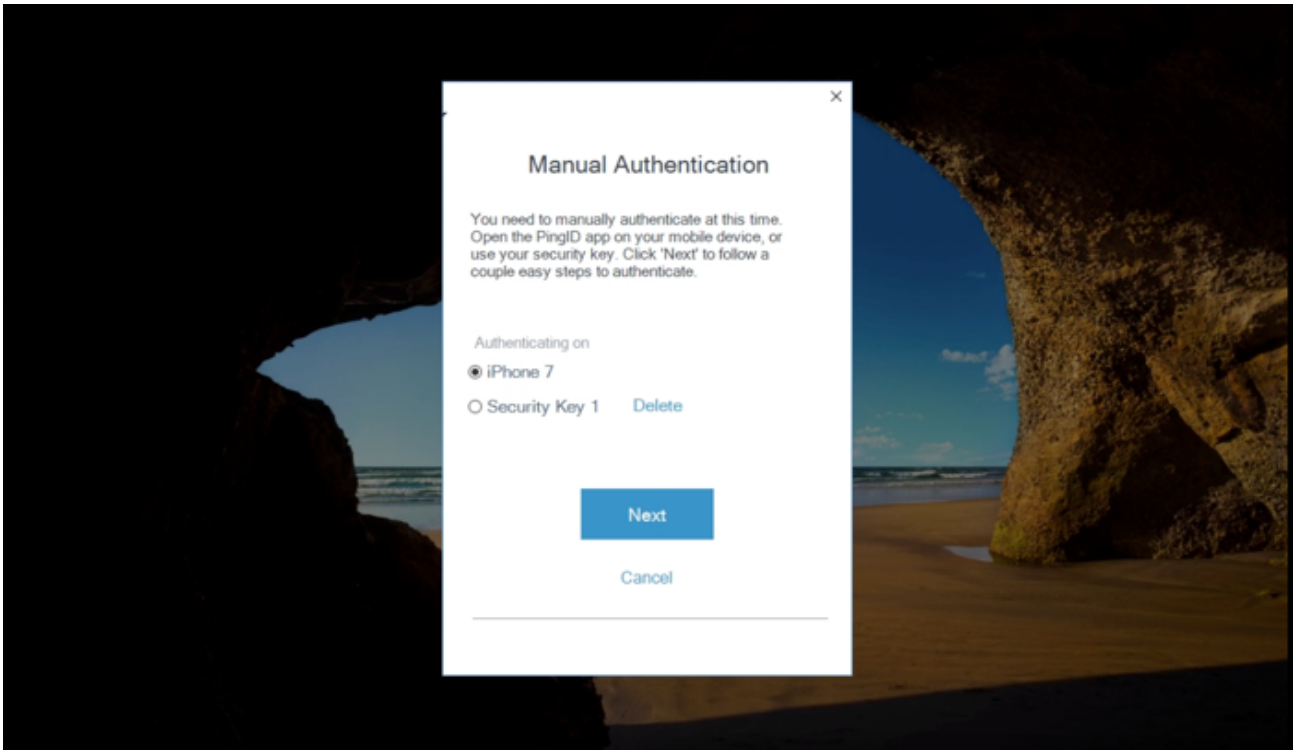
Manual authentication with a security key is only possible if:

- Your company policy and configuration allow the use of a security key to authenticate when offline.
- You have already paired a security key and authenticated successfully at least once when online.

> **Note**
>
> From PingID for Windows login 2.8 and later, you can use any security key that is paired to your account as long as you have successfully authenticated with it at least once online using the specific Windows machine that you want to sign on from. For version 2.7 and lower, you need to pair a security key specifically for manual authentication.

Steps

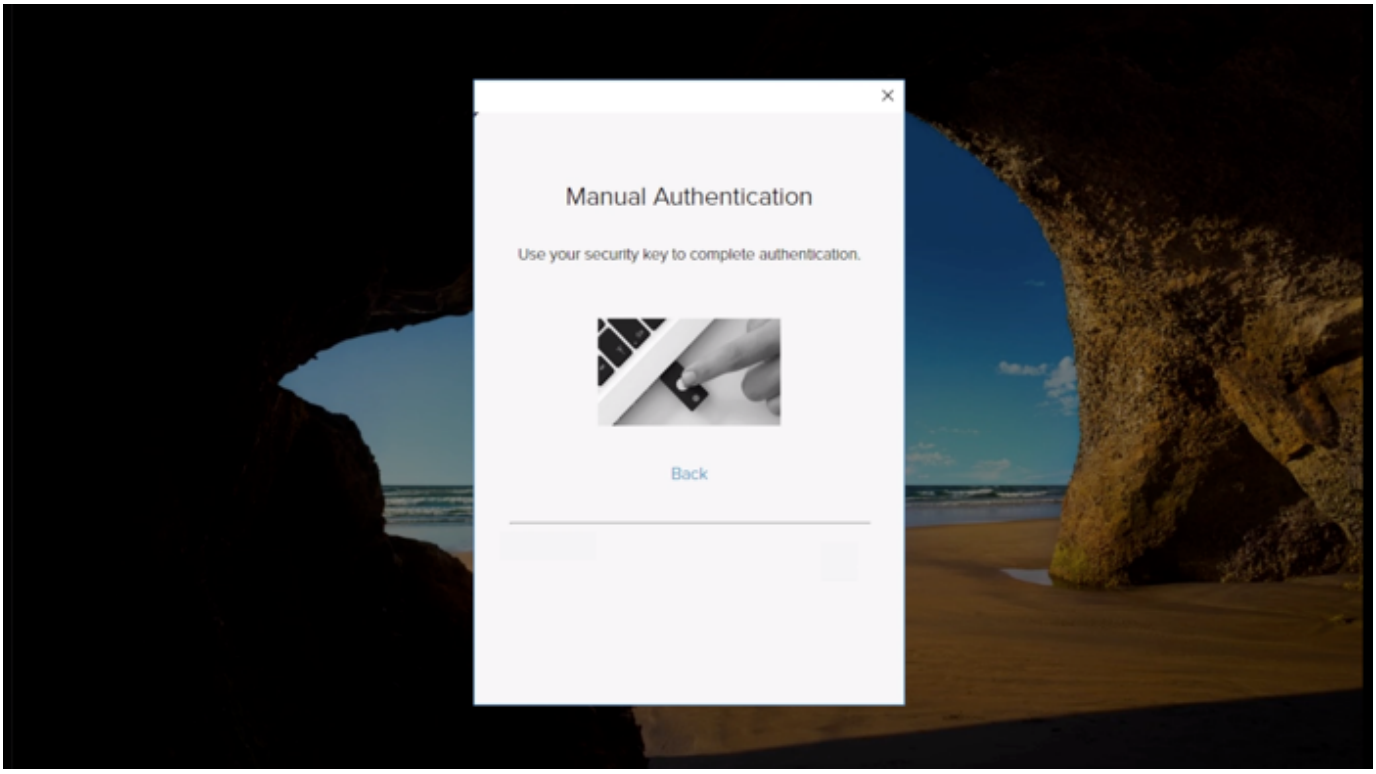
1. Connect your security key either physically through a USB cable or, if applicable, ensure NFC or Bluetooth are set to **ON**.
2. Sign on to your Windows machine.
    1. If you are offline and do not have an internet connection, in the **Manual Authentication** window, follow the prompting to authenticate manually.



> **Note**
>
> If you enrolled a security key for manual authentication in Windows login 2.7 or lower, and then upgraded to Windows login 2.8 or higher, you may see the same security key listed but with a different nickname. You should delete the deprecated duplicate device (deprecated devices show the **Delete** option). Before you delete a device, make sure you have at least one alternative device paired with your account.

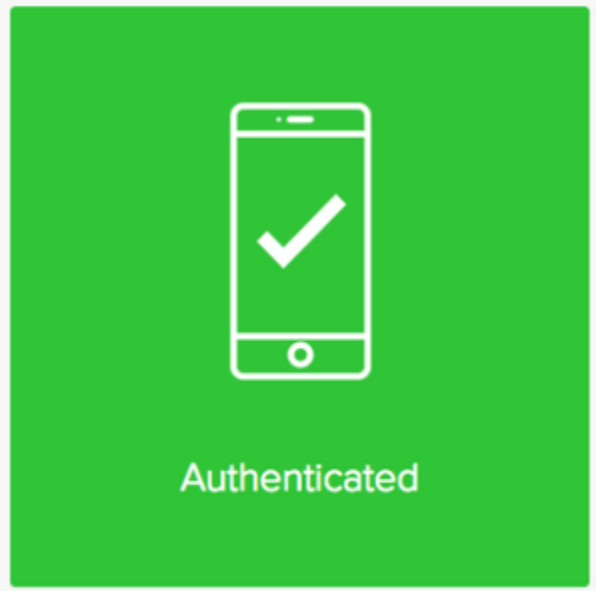
2. If you have more than one authentication method paired with your account, in the **Authenticating on** section, select **Security Key**.
3. Click **Next**.

3. Use your security key to authenticate.



Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful. You are redirected and signed on to your account or app.



Related links

- Troubleshooting a security key authentication

Authenticating with PingID using an authenticator app

You can authenticate using your authenticator app, such as Google Authenticator or Microsoft Authenticator, to generate a passcode to use to authenticate with PingID.

Before you begin

Pair your authenticator app with your account to enable authentication. For more information, see Using an authenticator app for authentication with PingID.

About this task

When using your authenticator app to get a passcode:

- If you have more than one account paired with your authenticator app, make sure you select the passcode that corresponds to the account you are trying to access.
- The passcode changes approximately every 30 seconds. When prompted to authenticate, enter the most recent passcode.
- You can only use a passcode one time.

> **Note**
>
> You must pair your authenticator app with your account to enable authentication. For more information, see Setting up your authenticator app for PingID authentication.

You can use an authenticator app to access your account using a web browser, to access your company's VPN, or to access a Mac login machine.

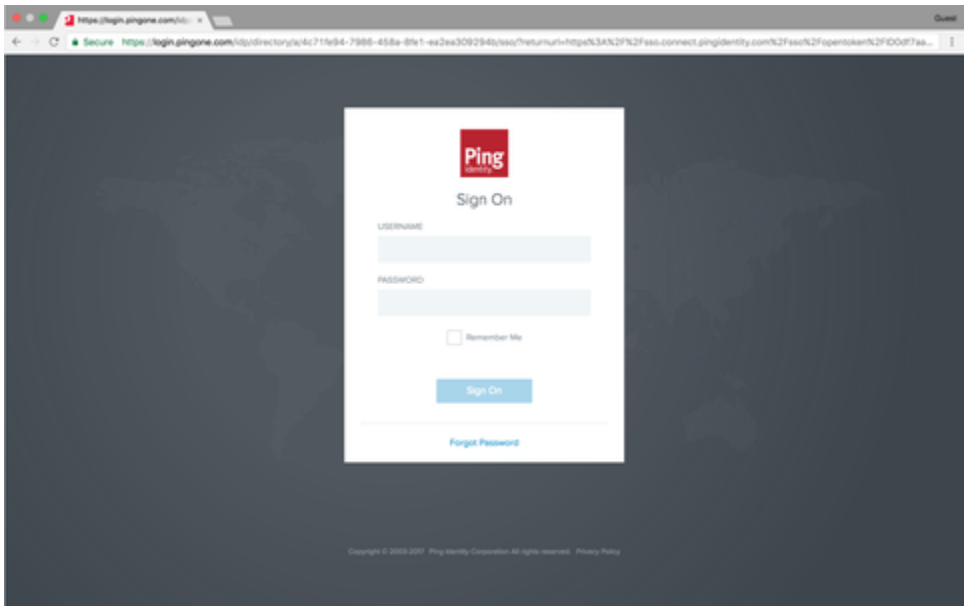
Web

Authenticating using an authenticator app

Authenticate using your authenticator app, such as Google Authenticator or Microsoft Authenticator, to generate a passcode to use to authenticate with PingID.

Steps

1. Sign on to your account or access an application that requires authentication.



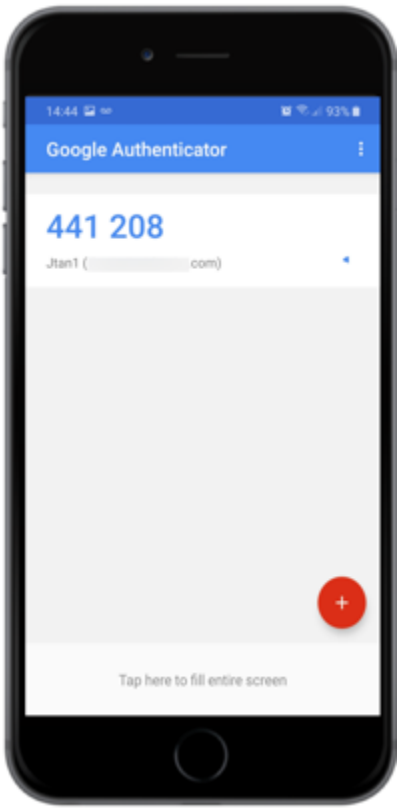
Result:

The **Authentication** window appears, prompting you to enter a passcode.

2. Launch your authenticator app.

   Result:

   The authenticator app displays a one-time passcode (OTP) for your account.



> **Note**
>
> This example shows the Google Authenticator.

3. In your browser, in the **Authentication** window, enter the passcode. Click **Sign On**.

   Result:

   A green check mark appears, indicating authentication is successful and your access is approved.

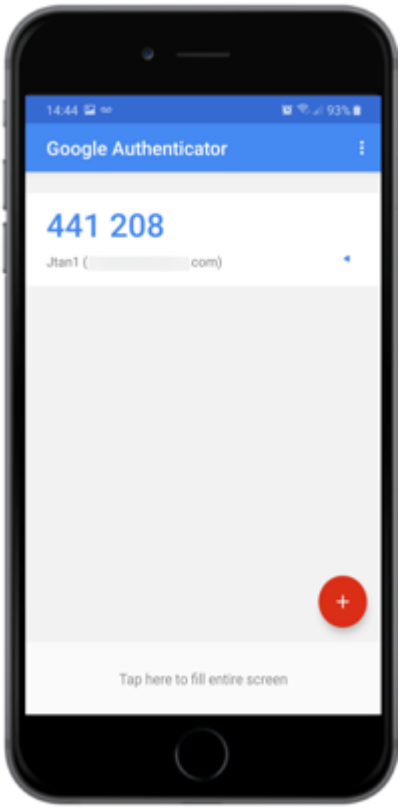
VPN

Authenticating using your authenticator app (VPN)

Authenticate with your authenticator app, such as Google Authenticator or Microsoft Authenticator, to generate a passcode to use to authenticate with PingID.

Steps

1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.
    2. For multiple devices only: a message displays showing a numbered list of all your devices. Enter the number for authentication app.
    3. Click **Sign In**.
2. Launch the authentication app. The authenticator app displays a OTP for your account.



> **Note**
>
> This example shows the Google Authenticator.

3. In the blank field, enter the OTP. Click **Sign In**.

Tip

To sign on and authenticate in one step:

1. On the sign-on page, in the **Password** field, when you sign on, add the OTP to the end of your password. The syntax requirements are as follows:
   - `<password><OTP>` (no spaces permitted)
   - `<password>,<OTP>` (use of spaces permitted when entering the OTP)
2. Click **Sign In**.

Result:

After successful authentication, your browser redirects you to your VPN.

Mac login

Authenticating using an authenticator app (Mac Login)

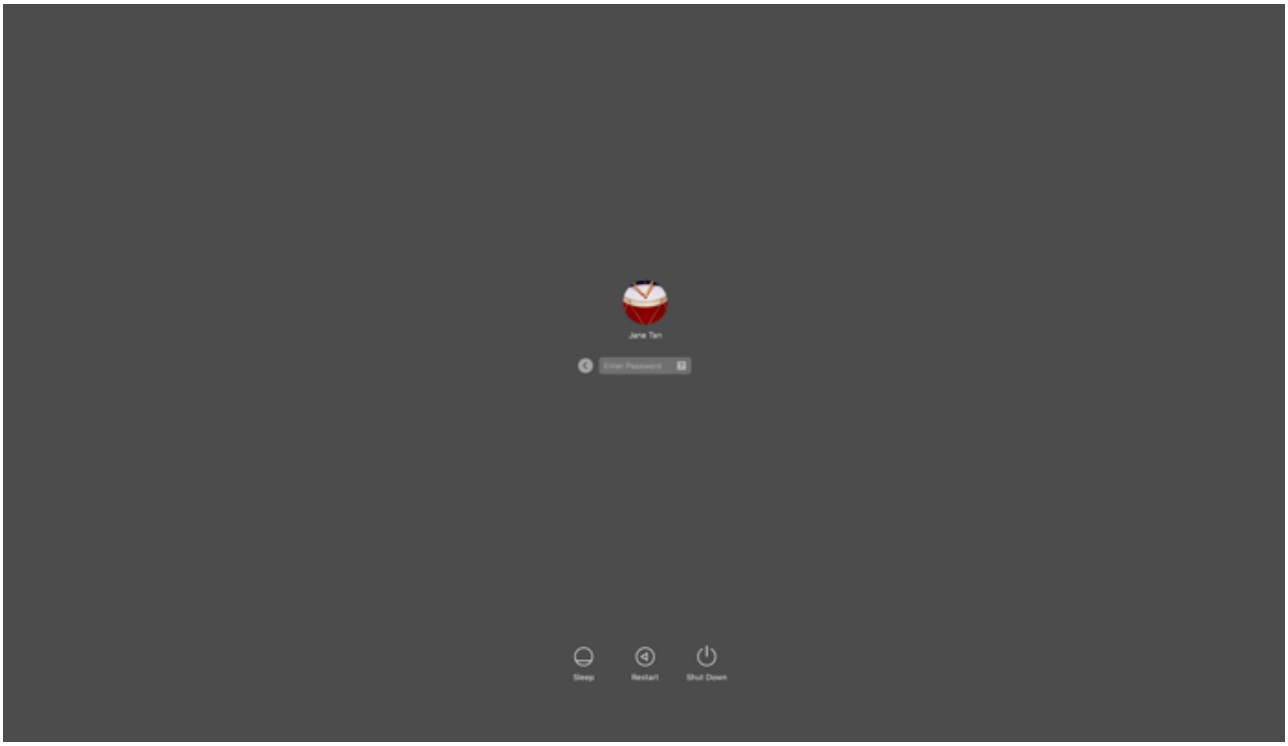
You can authenticate using your authenticator app, such as the Google Authenticator or the Microsoft Authenticator, to generate a passcode that you can use to authenticate with PingID.

Before you begin

Make sure your Apple Mac is running Mac OS v10.13 or later.

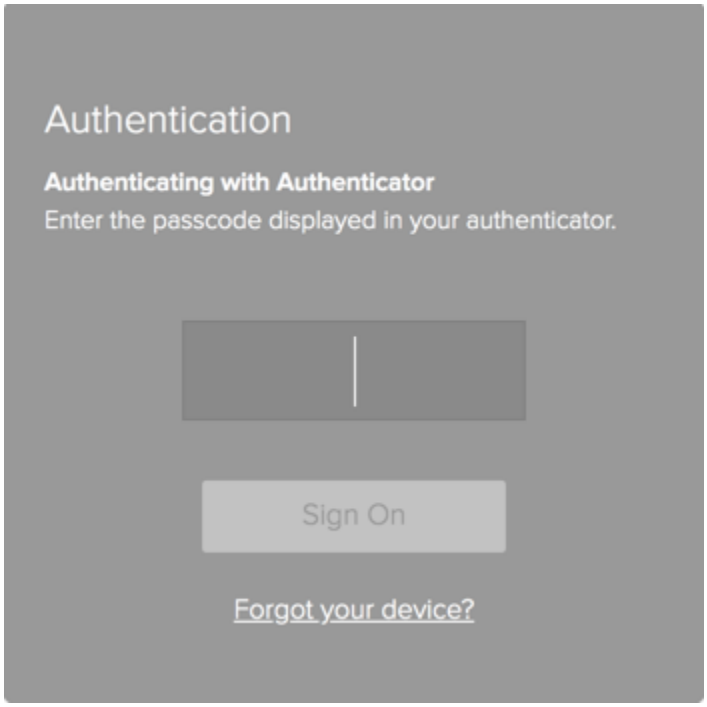
Steps

1. Sign on to your Mac machine.



Result:

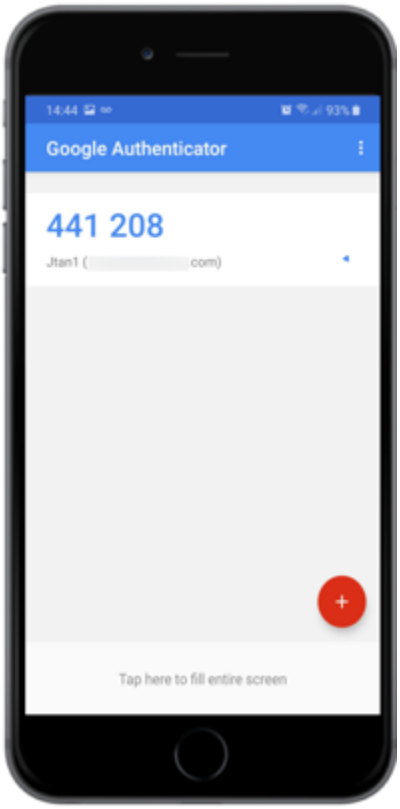
You'll see the **Authentication** window, prompting you to enter a passcode.



2. Launch your authenticator app.

   Result:

   The authenticator app displays a one-time passcode for your account.



> **Note**
>
> This example shows the Google Authenticator.

3. Enter the passcode into the **Authentication** window, and then click **Sign On**.

   Result:

   You'll see the green check mark indicating authentication is successful and you are signed on to your machine.

Authenticating with PingID using a YubiKey

You can use a YubiKey to access your account using a web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Before you begin

Pair your YubiKey with your account to enable authentication. For more information, see Using a YubiKey (OTP) for authentication with PingID.

About this task

If you are using a virtual machine (VM) to connect to your accessing device and to authenticate with your YubiKey, configure your VM to recognize a USB device.

Web

Authenticating using a YubiKey

Authenticate using your YubiKey hardware token.

About this task

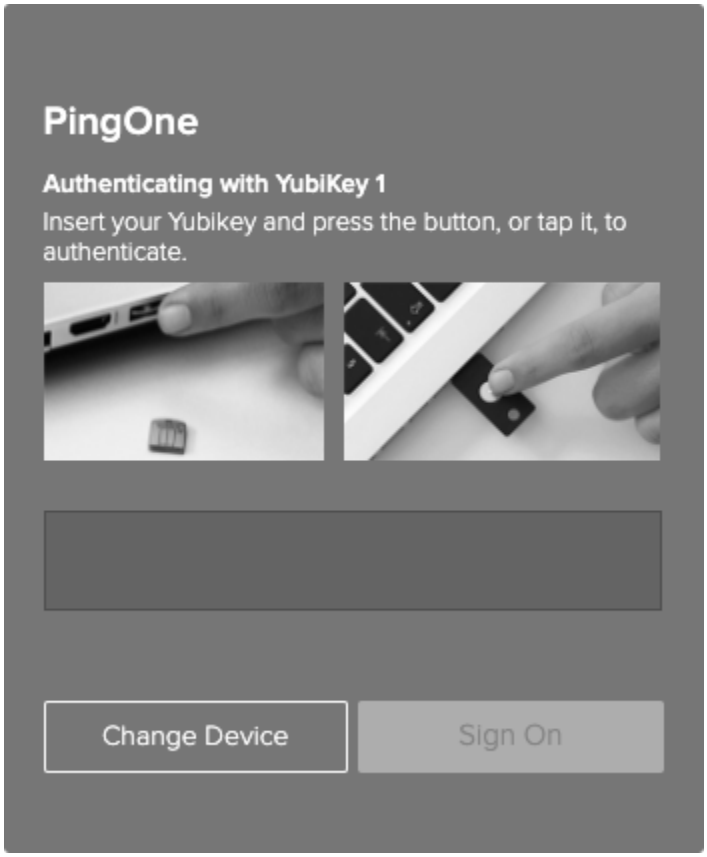
In a browser, sign on to your account and then use your YubiKey hardware token to authenticate.

Steps

1. Sign on to your account or access an application that requires authentication.

   Result:

   The **YubiKey Authentication** window appears, prompting you to enter a YubiKey passcode.



2. Insert the YubiKey into your computer USB port. Press the YubiKey button.

   > **Note**
   >
   > Make sure the **YubiKey Authentication** window is selected as the active screen before you press the YubiKey button.

   Result:

   A one-time passcode (OTP) automatically generates and enters into the **YubiKey Authentication** window.

> **Note**
>
> If you are using a YubiKey Neo and need to register using a browser on your mobile device through NFC, the process is different. To complete the registration process:
>
> 1. Download the YubiClip application to your mobile device and enable NFC.
> 2. Place the YubiKey next to your mobile device. The verification code is copied to the device clipboard.
> 3. Paste the code into the **YubiKey Authentication** field in your browser. Tap **Verify**.

3. Click **Sign On**.

   Result:

   A green check mark appears, indicating authentication is successful and your access is approved.

VPN

Authenticating using a YubiKey (VPN)

Use your YubiKey hardware token to authenticate.

About this task

In a browser, sign on to your account to use your YubiKey hardware token to authenticate.

Steps

1. From your web browser or application, sign on to your VPN with your username and password and then:
   1. Enter your username and password.
   2. For multiple devices only: A message displays showing a numbered list of all your devices. Enter the number for YubiKey.
   3. Click **Sign In**.

      Result:

   The text entry field displays.
2. Insert your YubiKey into the USB port on your computer, and tap your YubiKey.

   Place your mouse cursor in the text entry field to ensure the OTP is entered into the field automatically.

   Result:

   An OTP populates the text field.
3. Click **Sign In**.

   Result:

   After you have authenticated successfully, you are signed on to your VPN.

Windows login

Authenticating using a YubiKey (Windows login)

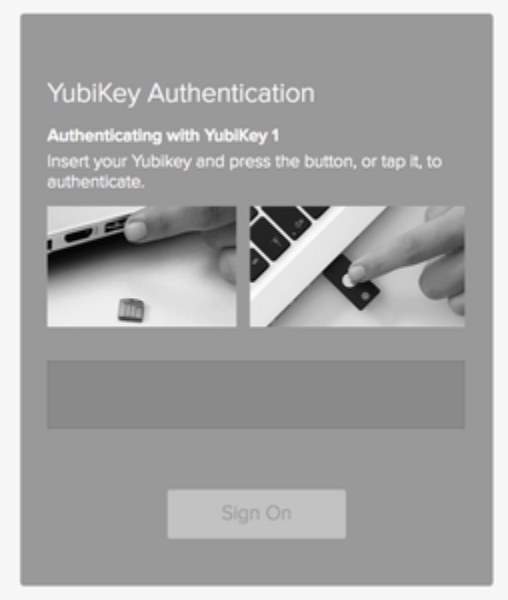
Use your YubiKey hardware token to authenticate to sign on to your Windows machine.

Steps

1. Sign on to your Windows machine.

   Result:

   The **YubiKey Authentication** window appears, prompting you to enter a YubiKey passcode.



2. Insert the YubiKey into your computer USB port and press the YubiKey button.

   > **Note**
   >
   > Make sure the **YubiKey Authentication** window is selected as the active window before you press the YubiKey button.

   Result:

   A OTP is automatically generated and inserted into the **YubiKey Authentication** window.

3. Click **Sign On**.

Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful. You are signed on to your Windows machine.

Mac login

Authenticating using a YubiKey (Mac Login)

Use your YubiKey hardware token to authenticate when you sign on to your Mac machine.

About this task

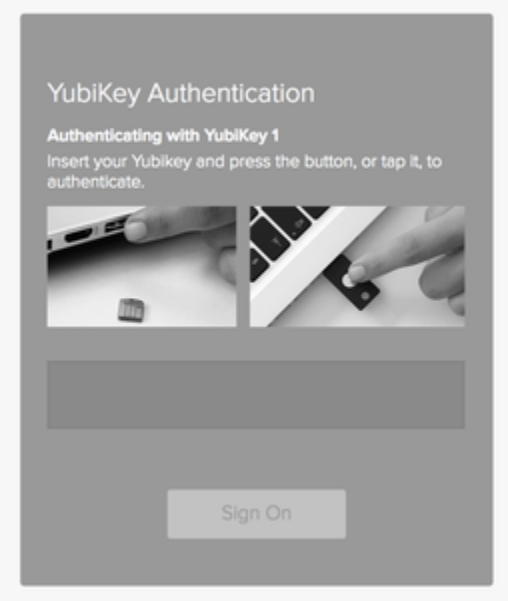
Make sure your Apple Mac is running Mac OS 10.13 or later.

Steps

1. Sign on to your Mac machine.

   Result:

   You'll see the **YubiKey Authentication** window, prompting you to enter a YubiKey passcode.



2. Insert the YubiKey into your computer USB port, and then press the YubiKey button.

   > **Note**
   >
   > window is selected as the active window before you press the YubiKey button.

   Result:

   A OTP is automatically generated and inserted into the **YubiKey Authentication** window.

3. Click **Sign On**.

   Result:

   You'll see the green check mark indicating authentication is successful, and you'll be signed on to your machine.

Authenticating with PingID using SMS or voice

Get a one-time passcode (OTP) by SMS or voice call and use it to authenticate securely with PingID.

Before you begin

- Pair your device with your account to enable authentication. For more information, see Using SMS or voice authentication with PingID.

About this task

If your organization allows it, you can use SMS and voice calls to access your account using a Web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Web

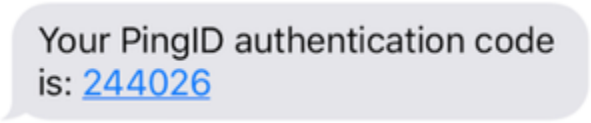
Authenticating using an SMS or voice passcode

After you set up authentication by SMS or voice, when you sign on to your account or app, you receive a passcode to use to authenticate.

About this task

Use a voice call or SMS to receive an authentication passcode from PingID.

- Voice call: You receive a phone call with an automated recording of your passcode.
- SMS: You receive an SMS with details of your passcode.



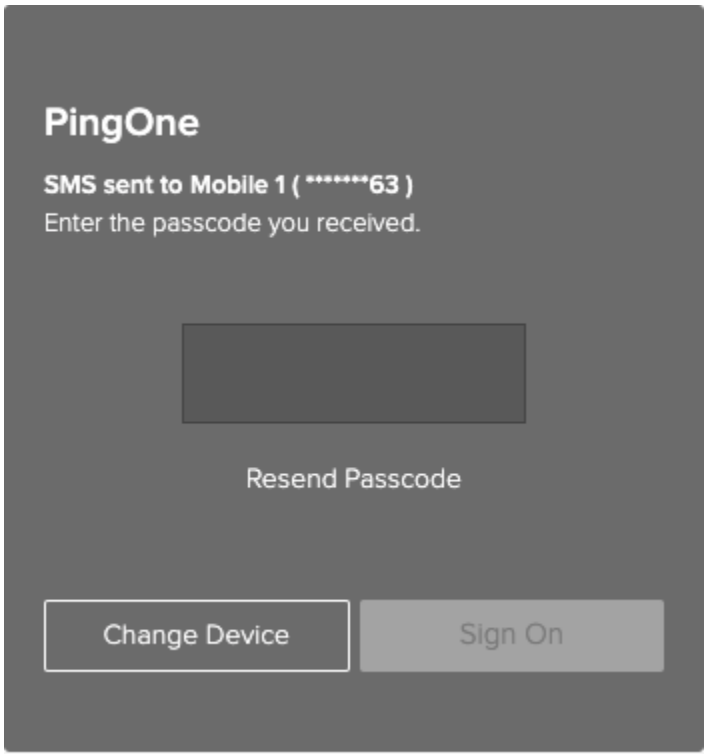
Steps

1. Sign on to your account or an application that requires authentication.

   Result:

   In the **Authenticating** window, you receive an SMS or voice message with the authentication passcode.

2. In the **Authenticating** window, enter the passcode. Click **Sign On**.



> **Note**
>
> If you didn't receive a passcode by SMS or voice call, click **Resend Passcode**.

Result

You see a green **Authenticated** message with a check mark, indicating authentication is successful and your access is approved.

> **Important**
>
> If you are using voice authentication, consider protecting your secure voice codes. You can protect them in one of two ways:
>
> - Change your voicemail password from the device default.
> - Disable voicemail.

VPN

Authenticating using an SMS or voice passcode (VPN)

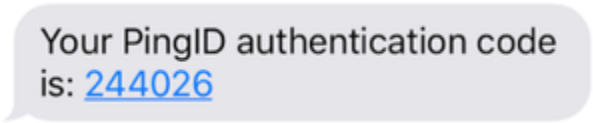
To authenticate using SMS or voice, sign on to your account and receive a OTP to use to authenticate.

Steps

1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.
    2. For multiple devices only: A message displays showing a numbered list of all your devices. Enter the number for SMS or voice.
    3. Click **Sign In**.

       Result:

       You receive a OTP through SMS or voice call.

2. Enter the OTP from step 1 into the **text** field. Click **Sign In**.

   Result:

   After you successfully authenticate, you are signed on to your VPN.

Windows login

Authenticating using an SMS or voice passcode (Windows Login)

After you set up authentication by SMS or voice, to sign on to your Windows machine, you receive a passcode to use to authenticate.

About this task

Use a voice call or SMS to receive an authentication passcode from PingID.

- Voice call: You receive a phone call with an automated recording of your passcode.
- SMS: You receive an SMS with details of your passcode.

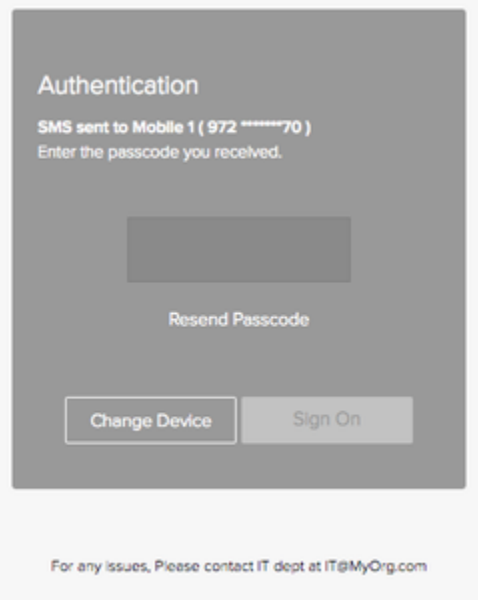
Steps

1. Sign on to your Windows laptop or desktop machine.

   Result:

   The **Authenticating** window appears. You receive an SMS or voice message on your mobile device showing the OTP.

2. In the **Authentication** window, enter the passcode. Click **Sign On**.



> **Note**
>
> If you didn't receive a passcode by SMS or voice call, click **Resend Passcode**.

Result:

You see a green **Authenticated** message with a check mark indicating that authentication is successful, and your access is approved.

Mac login

Authenticating using an SMS or voice passcode (Mac Login)

Use SMS or voice to authenticate when you sign on to your Mac machine.

Before you begin

Make sure:

- Your Apple Mac is running Mac OS 10.13 or later.
- You have paired your mobile device for SMS or voice authentication.

About this task

If you have set up authentication by SMS or voice, when you attempt to sign on to your Mac machine, you receive a passcode with which to authenticate.

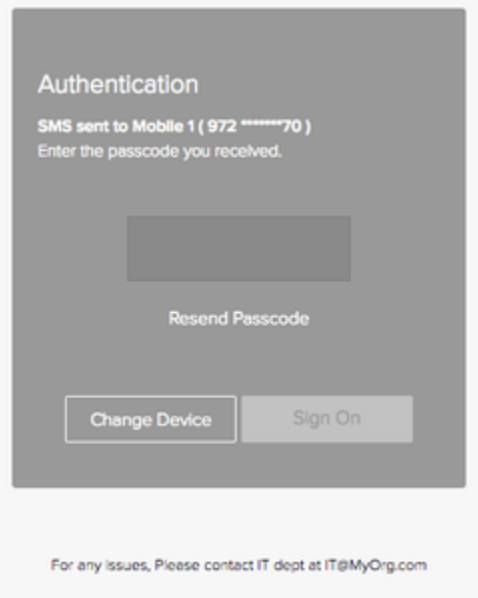
- Voice call: You receive a phone call with an automated recording of your passcode.
- SMS: You receive an SMS with details of your passcode.

Steps

1. Sign on to your Mac machine.

   Result:

   You'll see the **Authenticating** window. You'll receive an SMS or voice message to your mobile device, showing the OTP.



> **Note**
>
> If you didn't receive a passcode by SMS or voice call, click **Resend Passcode**.

2. In the **Authenticating** window, enter the passcode and click **Sign On**.

Result:

You'll see the green check mark indicating authentication is successful, and you're signed on to your Mac machine.

Authenticating with PingID using email

Get an email with a one-time passcode (OTP) that you can use to authenticate securely with PingID.

Before you begin

- Pair your device with your account to enable authentication. For more information, see Using email for authentication with PingID.

About this task

If your organization allows it, you can use a hardware token to access your account using a web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Web

Authenticating using email

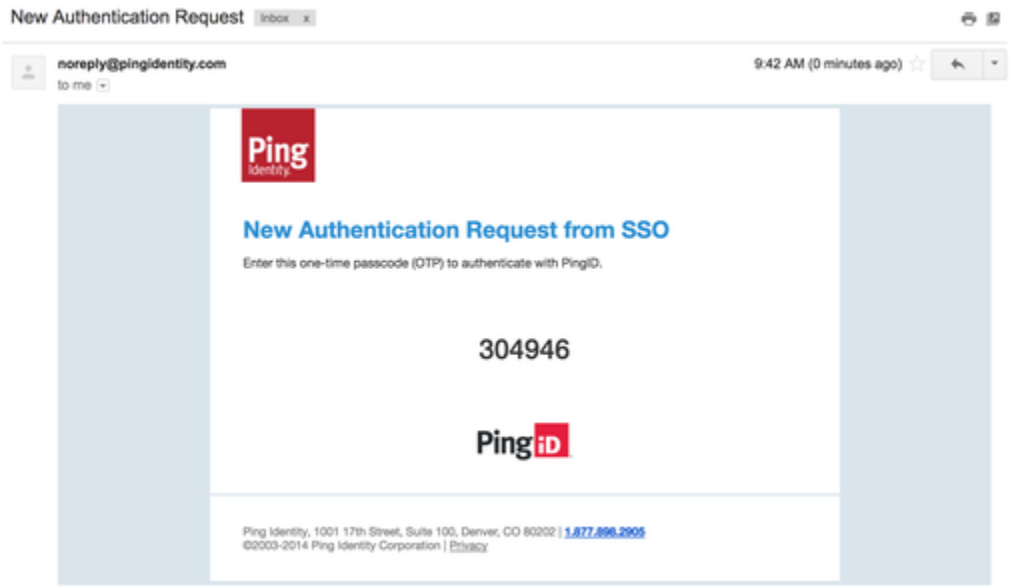
Authenticate for your account or app through your email.

Steps

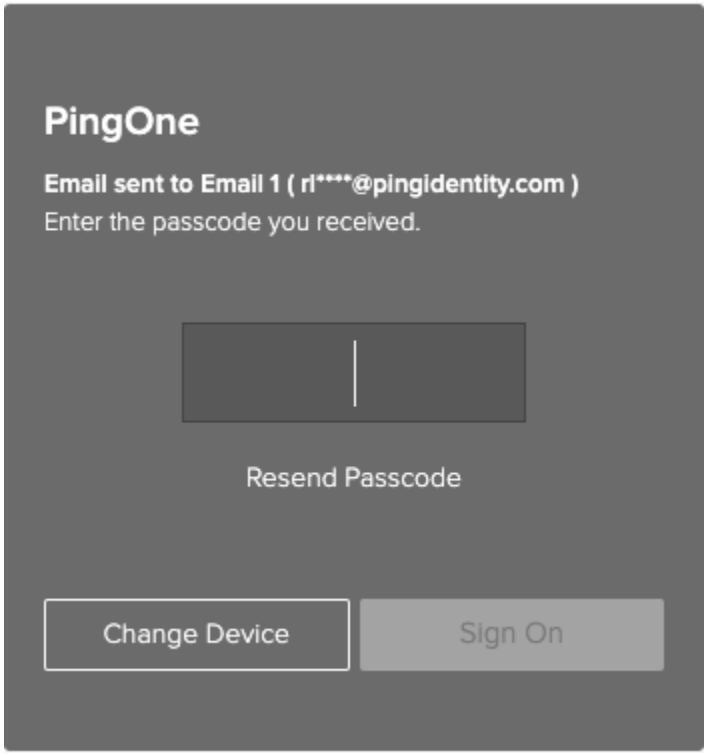
1. Sign on to your account or an application that requires authentication.

   Result:

   The **Authenticating** window appears. You receive an authentication passcode by email.



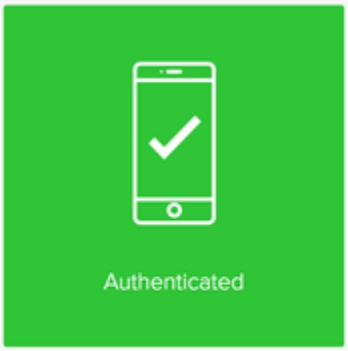
2. In the **Authentication** window, enter the passcode. Click **Sign On**.



> **Note**
>
> If you need to generate a new passcode, click **Resend Passcode**.

Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful, and your access is approved.



VPN

Authenticating using email (VPN)

After you set up email authentication for web, you receive a OTP through email to use to authenticate to your VPN.

About this task

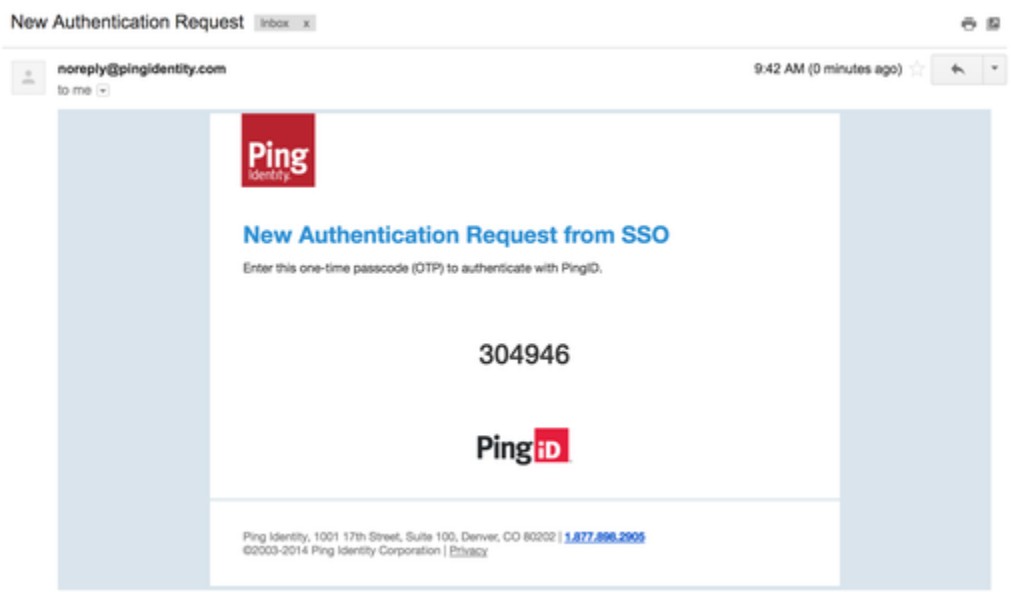
Use your email to receive an OTP to authenticate to your VPN.

Steps

1. From your web browser or application, sign on to your VPN:
    1. Enter your username and password.
    2. For multiple devices only: A message displays showing a numbered list of all your devices. Enter the number for email.
    3. Click **Sign In**.

       Result:

       You receive an email with your OTP.



2. In the text entry field, enter the OTP from step 1. Click **Sign In**.

   Result:

   After your authentication is successful, you are signed on to your VPN.

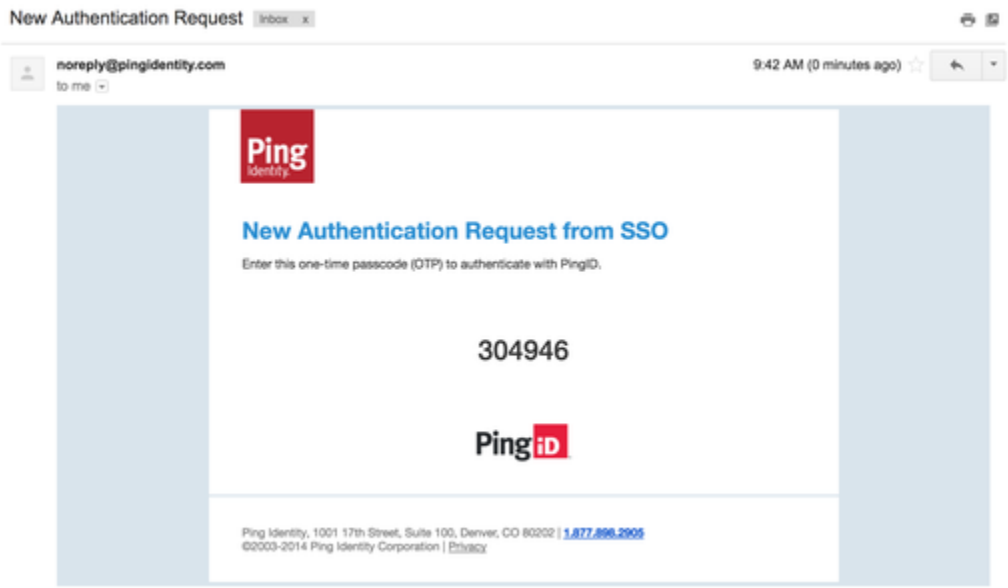
Windows login

Authenticating using email (Windows login)

After you set up email authentication for Windows login, you can receive a OTP through email to use to authenticate.

Steps

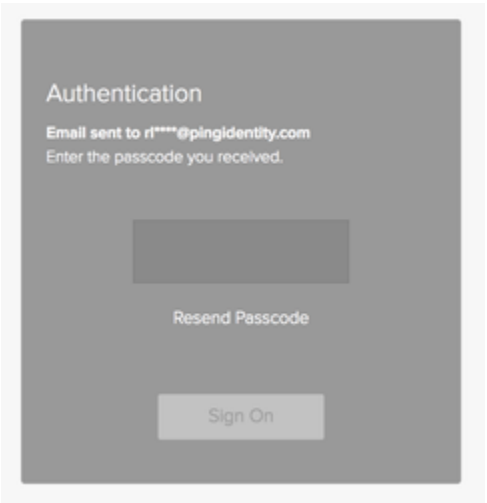
1. Sign on to your Windows machine.



Result:

The **Authenticating** window appears. You receive an authentication passcode by email.

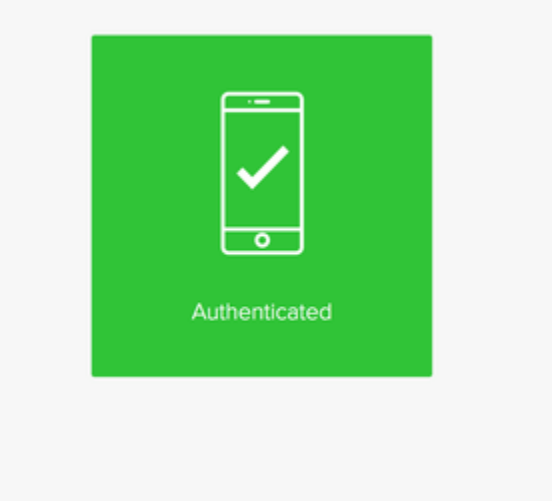
2. In the **Authentication** window, enter the passcode. Click **Sign On**.



> **Note**
>
> If you need to generate a new passcode, click **Resend Passcode**.

Result

The green **Authenticated** message appears with a check mark, indicating authentication is successful, and your access is approved. You are signed on to your Windows machine.



Mac login

Authenticating using email (Mac Login)

Use an email passcode to authenticate when you sign on to your Mac machine.

Before you begin

Make sure:

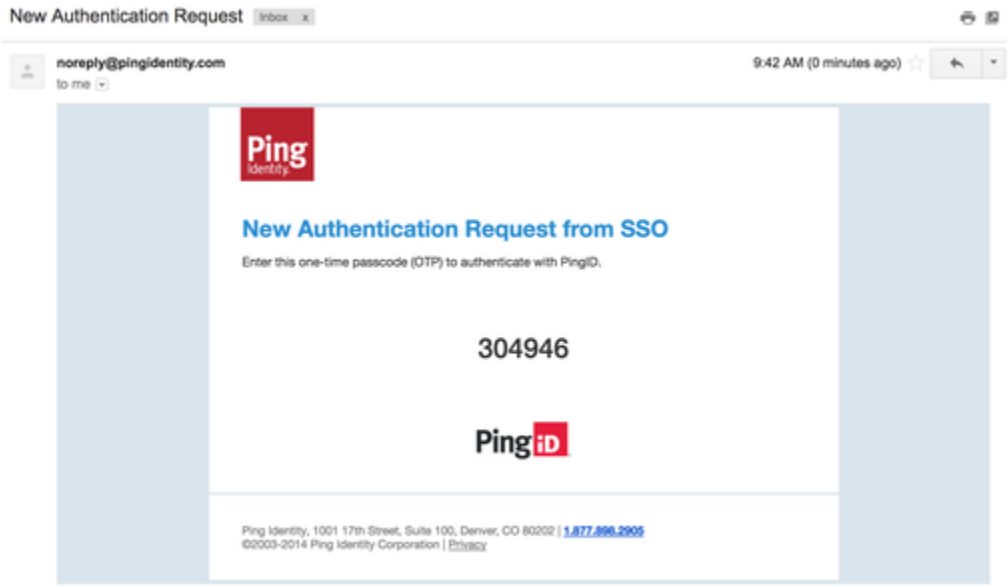
- Your Apple Mac is running Mac OS 10.13 or later.
- You have paired your email.

Steps

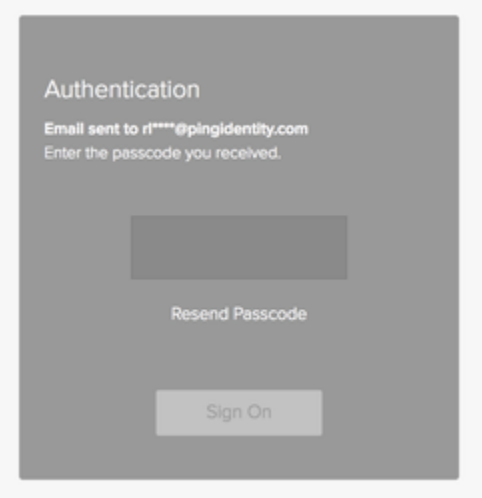
1. Sign on to your Mac machine.

   Result:

   You'll see the **Authenticating** window and you'll receive a passcode by email.



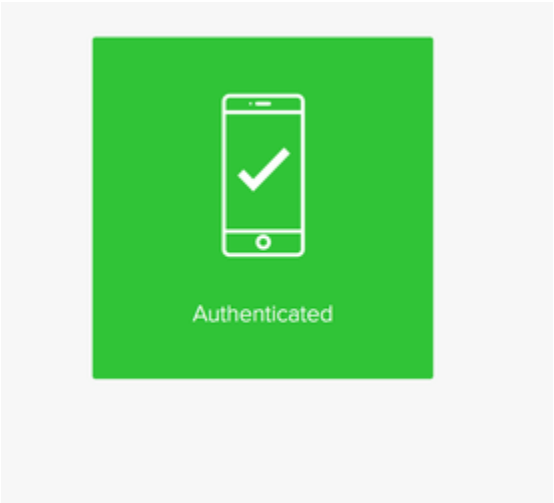
2. In the **Authenticating** window, enter the passcode and click **Sign On**.



> **Note**
>
> If you need to generate a new passcode, click **Resend Passcode**.

Result:

You'll see the green check mark indicating authentication is successful.



Result

You're signed on to your Mac machine.

Authenticating with PingID using a hardware token

Use a one-time passcode (OTP) from your hardware token to authenticate securely with PingID.

Before you begin

- Pair your device with your account to enable authentication. For more information, see Using a hardware token (OTP) for authentication with PingID.
- You might also need to resynchronize your hardware token, if required.

About this task

If your organization allows it, you can use a hardware token to access your account using a web browser, to access your company's VPN, or to access a Windows login or Mac login machine.

Web or Mac

Authenticating using a hardware token (Web)

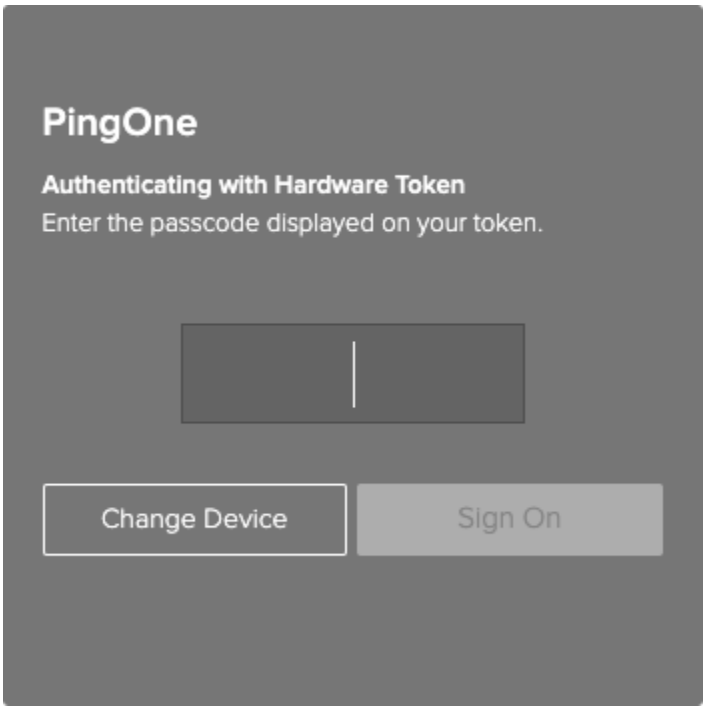
Use a OTP from your hardware token to authenticate securely with PingID when accessing your account or app through a web browser.

Steps

1. Sign on to your account or access an application that requires authentication.

Result:

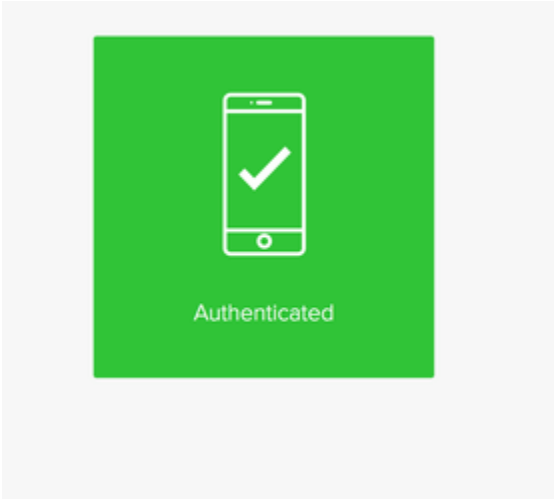
The **Authentication** window appears requesting your passcode.



2. Enter the OTP from your hardware token. Click **Verify**.

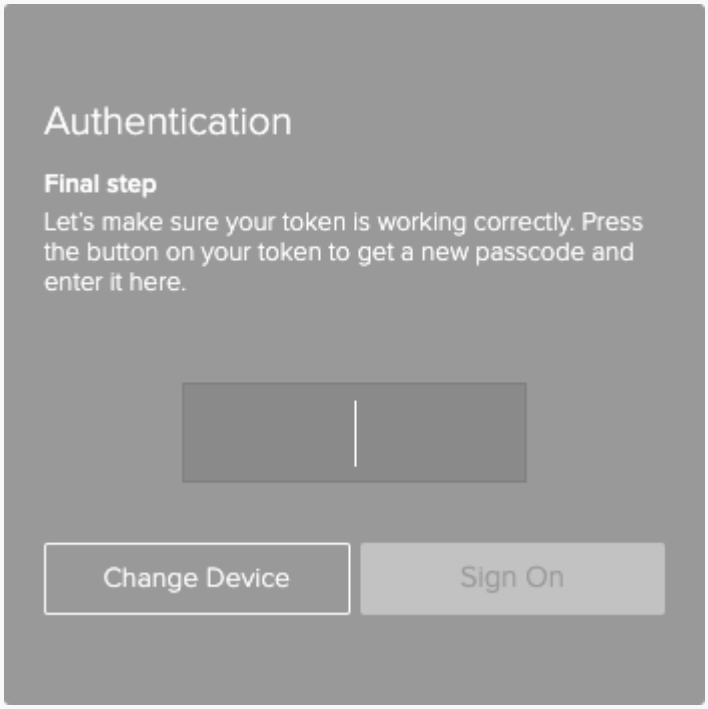
Result:

A green check mark appears, indicating your successful authentication and access. You are automatically signed on to your application.



Note

If you did not get the green check mark, your hardware token might be out of sync. You see a further authentication window.



Enter the OTP from your hardware token. Click **Sign On**. You should see the green check mark shown above.

VPN

Authenticating using a hardware token (VPN)

Use a OTP from your hardware token to authenticate securely with PingID when accessing your VPN.

Steps

1. From your web browser or app, sign on to your VPN with your username and password.

   Result:

   You are offered a text entry field for an OTP.

2. In the text entry field, enter the OTP displayed on your hardware token to authenticate to your VPN.
3. Click **Sign in**.

   Result:

   After you are authenticated, you are signed on to your VPN.

Windows login

Authenticating using a hardware token (Windows login)

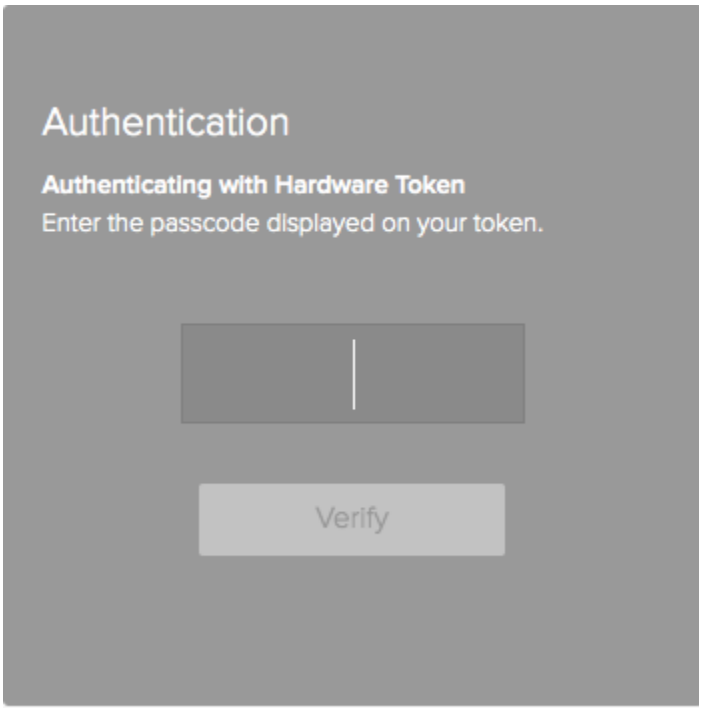
Use a OTP from your hardware token to authenticate securely with PingID when accessing your Windows machine.

Steps

1. Sign on to your Windows machine.

   Result:

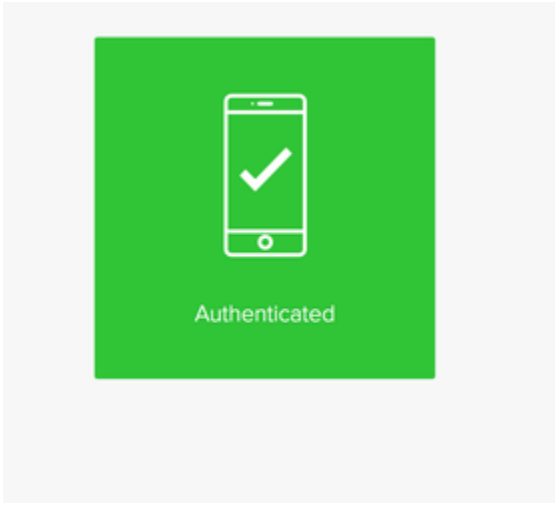
   The **Authentication** window appears requesting the OTP displayed on your hardware token.



2. Enter the OTP from your hardware token. Click **Verify**.

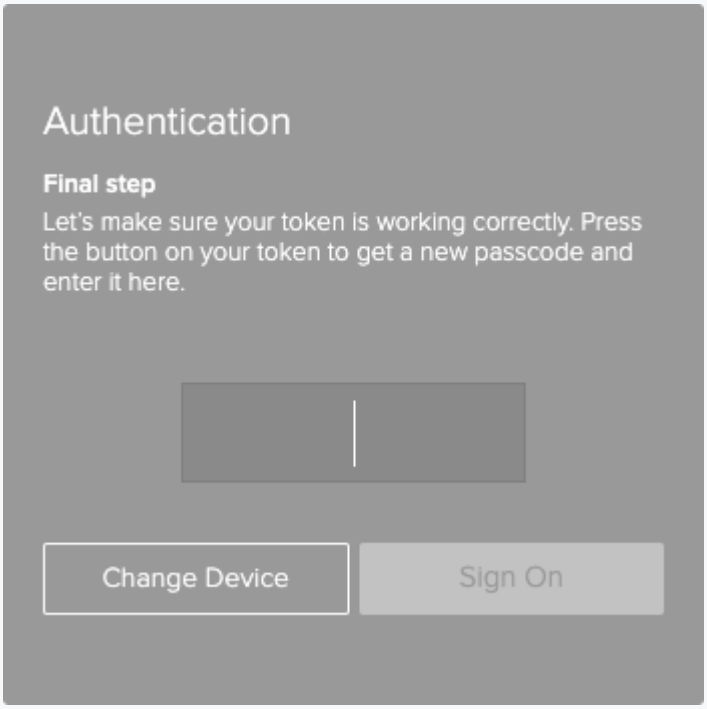
Result

The green **Authenticated** message with a check mark appears, indicating authentication is successful and your access is approved. After a few moments, you are signed on to Windows.



Note

If you did not get the green check mark, your hardware token might be out of sync. You will see a further authentication window.



Enter the OTP from your hardware token. Click **Sign On**. You should see the green check mark shown above.

Mac login

Authenticating using a hardware token (Mac login)

Use a OTP from your hardware token to authenticate securely with PingID when accessing your Mac machine.

Before you begin

Make sure:

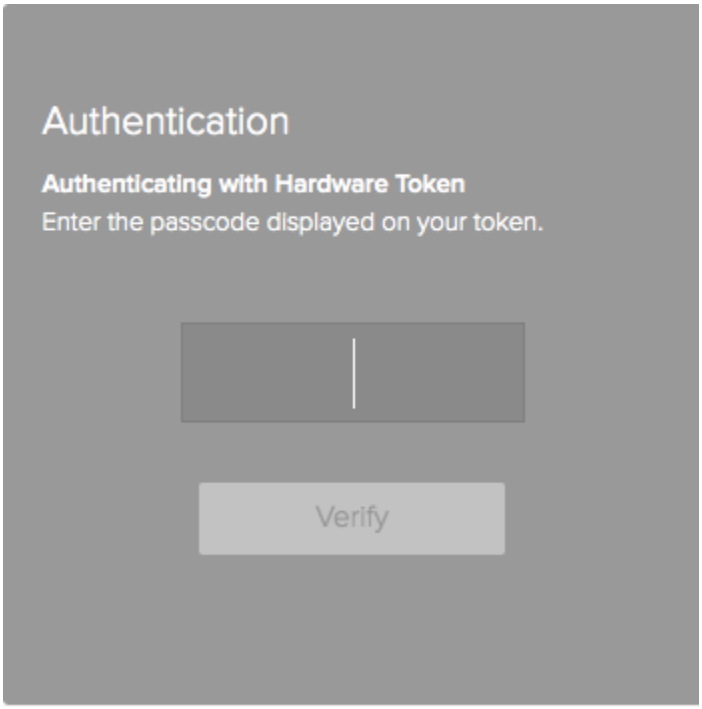
- Your Apple Mac is running Mac OS 10.13 or later.
- You have paired your hardware token.

Steps

1. Sign on to your Mac machine.

   Result:

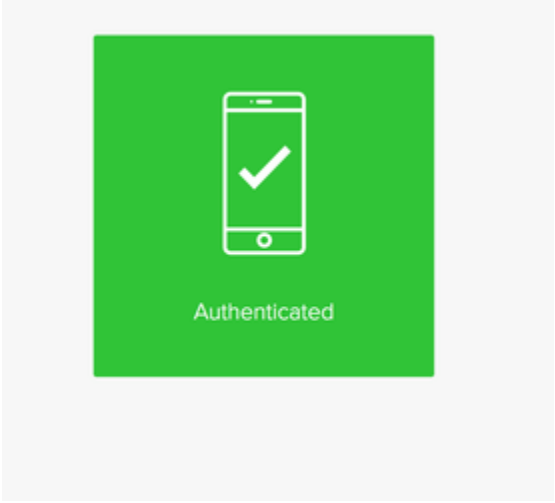
   You'll see the **Authenticating** window, prompting you to enter a passcode.



2. Generate an OTP using your hardware token.
3. In the **Authentication** window, enter the OTP and click **Verify**.

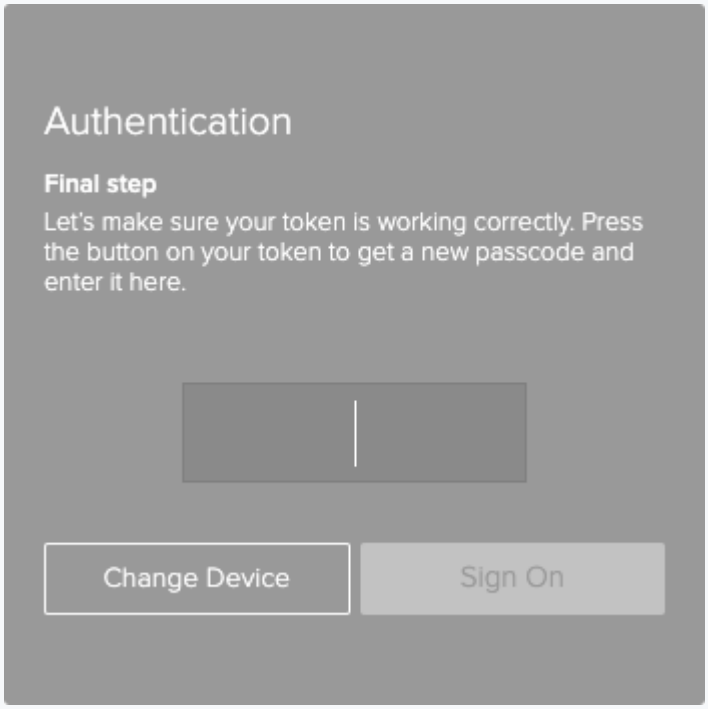
   Result:

   The green check mark indicates authentication is successful and your access is approved.



Note

If you did not get the green check mark, your hardware token might be out of sync. You will see a further authentication window.



Enter the OTP from your hardware token. Click **Sign On**. You should see the green check mark shown above.

Result

You're signed on to your Mac machine.

Resync a hardware token

Resynchronizing a hardware token

About this task

Hardware tokens need to maintain time synchronization.

To resync your token if you receive an error:

Steps

1. Access the **Devices** page, do one of the following.

   Choose from:

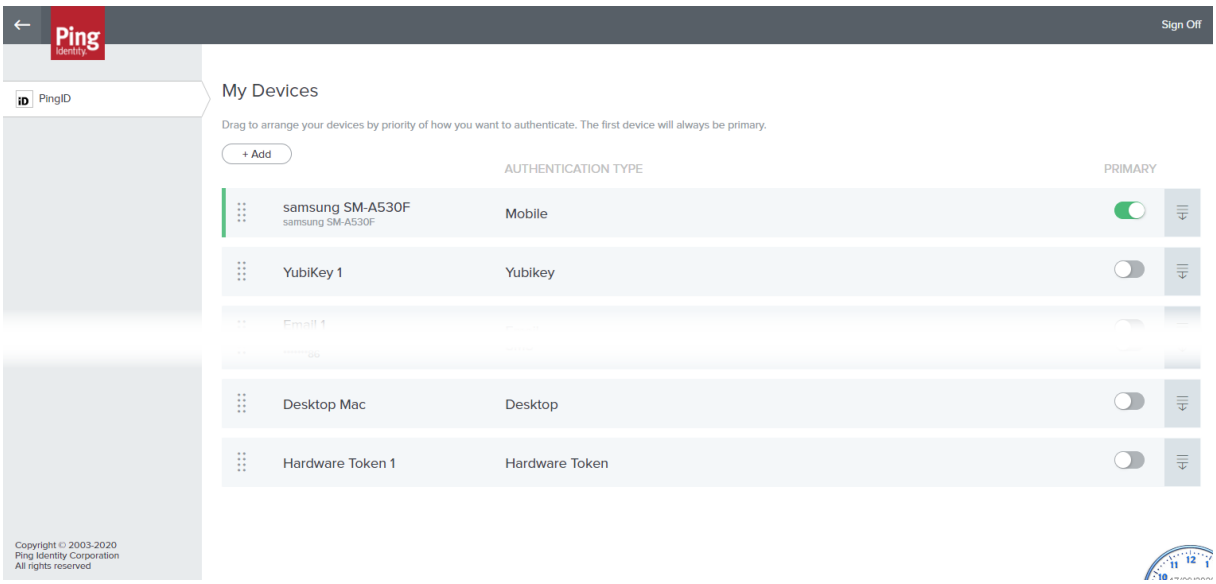
   - During authentication: When the **Authentication** screen opens, click **Settings**.

     > **Note**
     >
     > To resync an out-of-sync hardware token, you must first authenticate using an alternative method, such as email. That is the situation assumed in the example below.

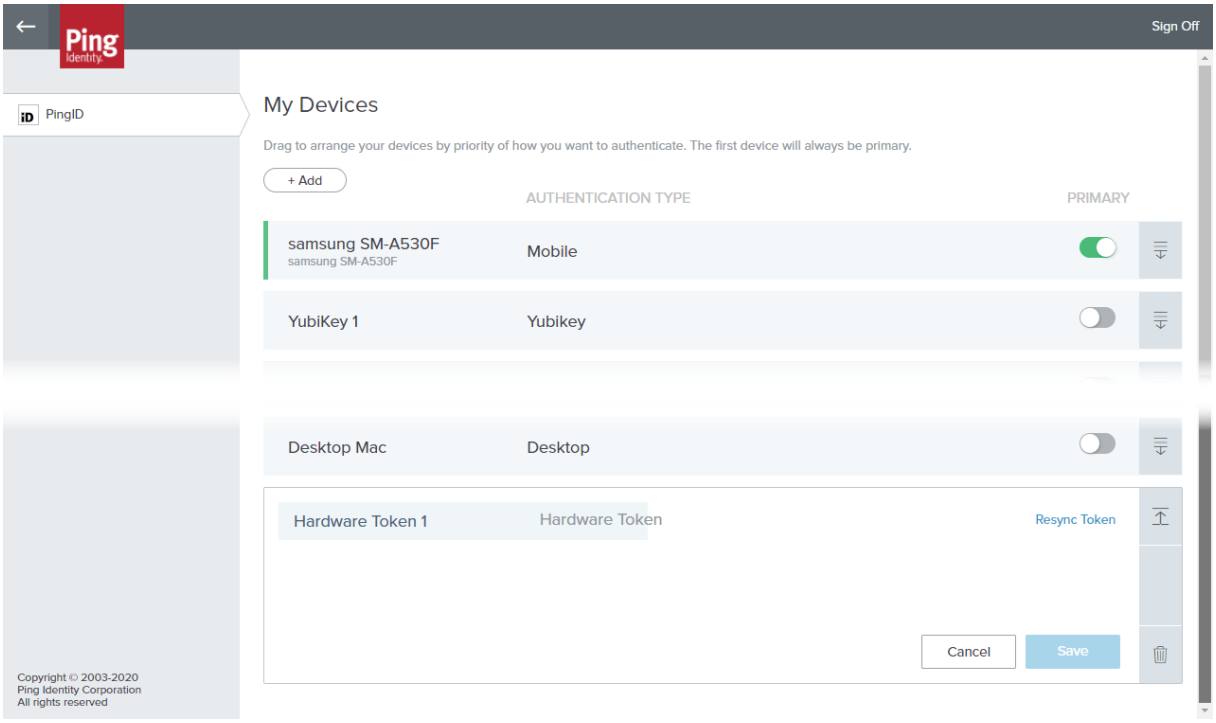
   - From your organization dock: Click the **Account** icon ( ) and then click **Devices**.
   - From a link provided by your IT department.

   Result:

   The **Devices** page opens, showing the devices you currently have paired with your account. The primary device is shown in green.

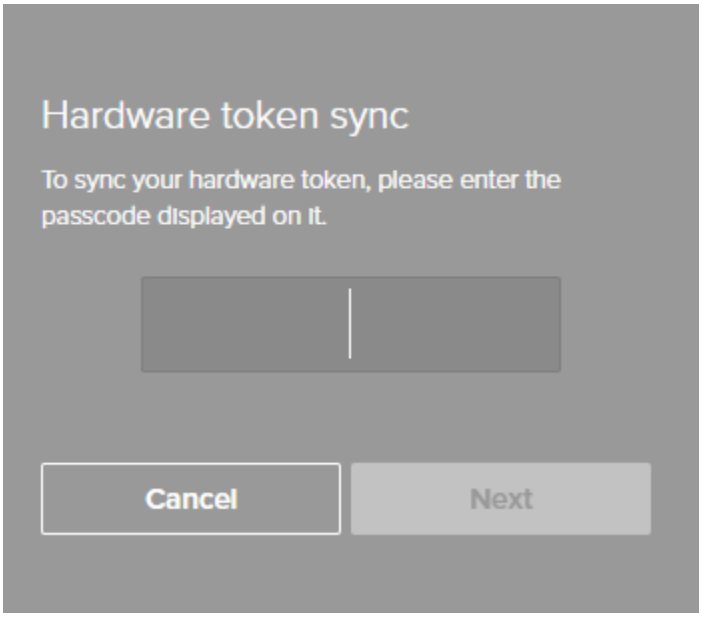


Click the **Expand** icon ( ) to view details of a device.



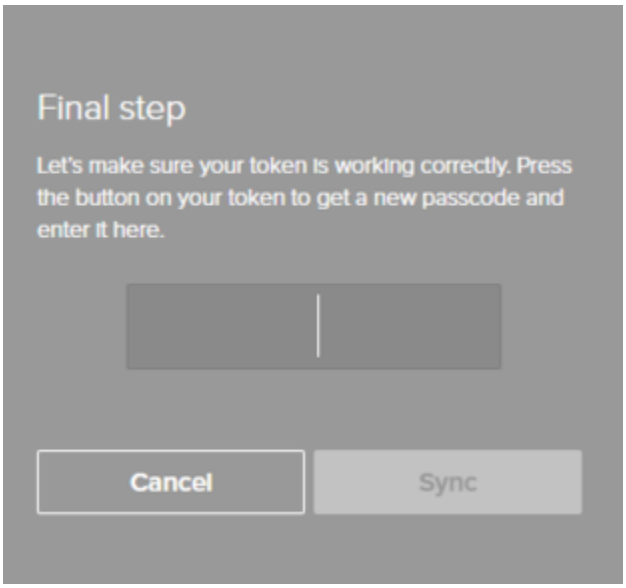
2. Click the **Resync Token** option.

The **Hardware token sync** window is displayed:



1. Enter the passcode displayed on the token.

The **Final step** window is displayed.



1. Wait for a new passcode on your token and enter it.
2. Click **Sync** to complete the resync.

   Result:

   Your token is now resynced and should be available for authentications.

Authenticating with PingID using a backup device

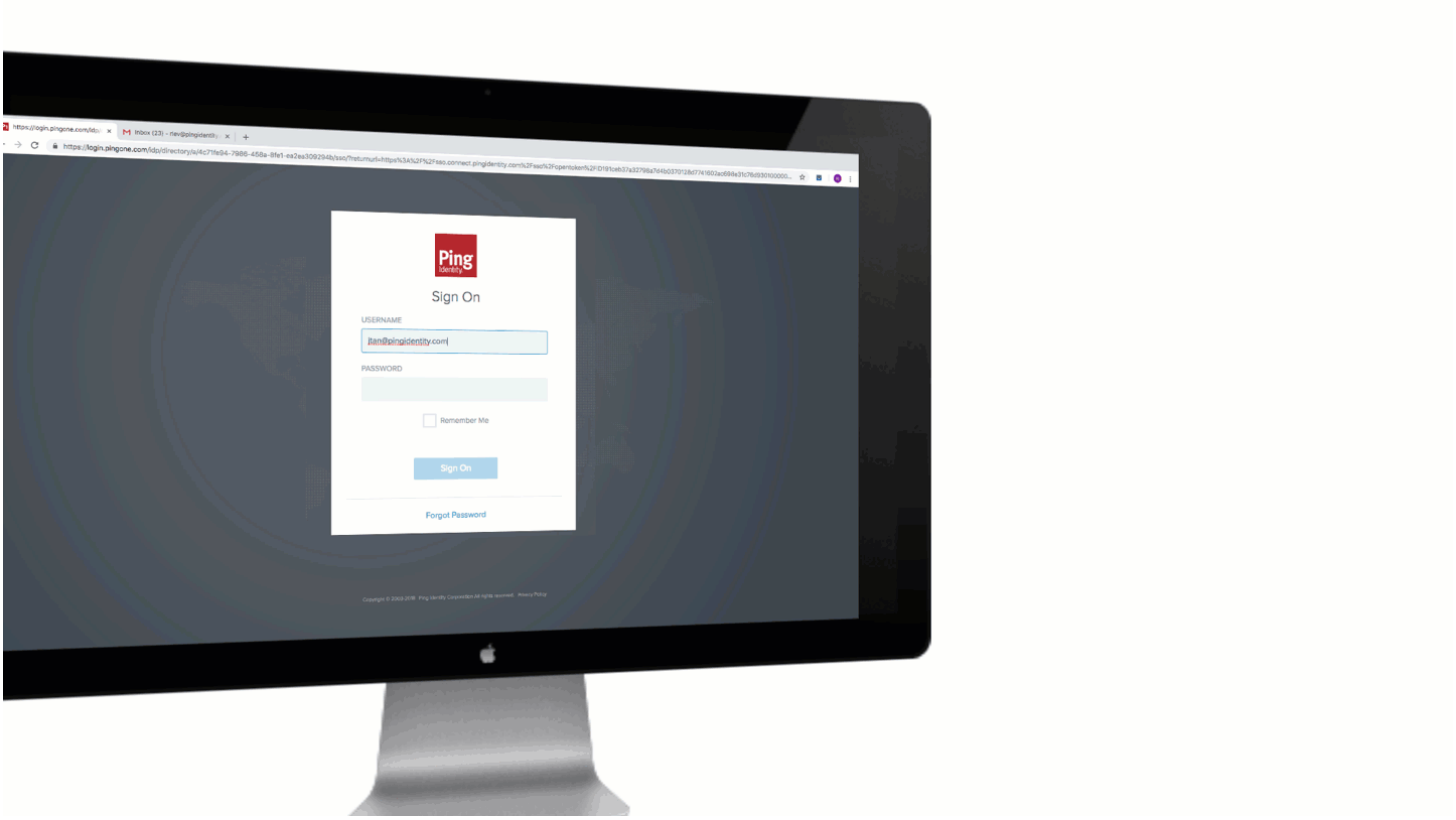
If you forgot or lost your paired device or it is stolen, you might be able to authenticate using a backup device.

About this task

Use the **Forgot your device?** link to get a one-time passcode (OTP) to use to authenticate through email, SMS, or voice message.

If you are unable to access one of your paired devices, click **Forgot your device?** to see the backup devices available to you. The devices you can use depend on the information available in your organization's directory and can include your personal email or an alternative phone number.

> **Important**
>
> The **Forgot your device?** link is only available if your organization has enabled this feature and there is a valid backup device for your account.

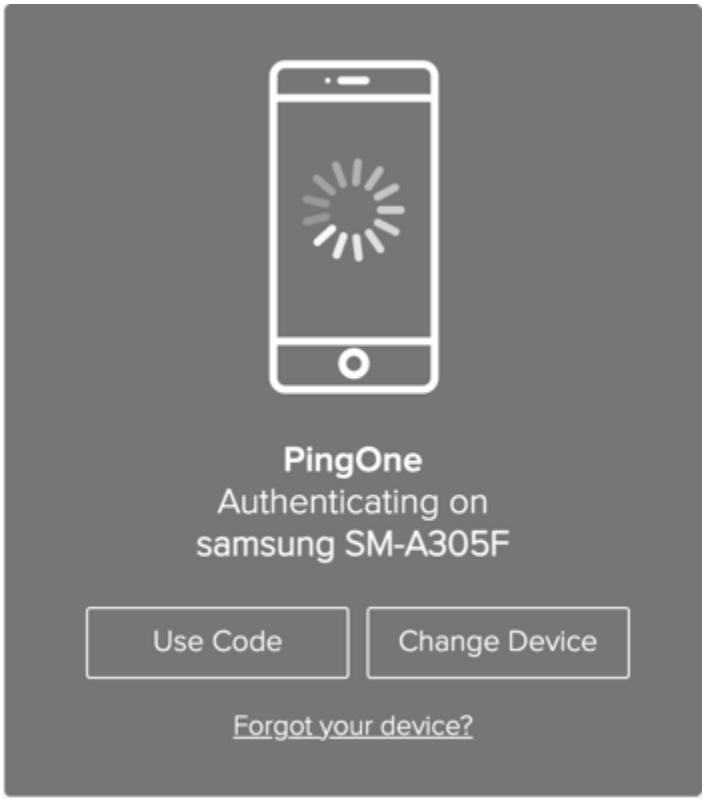


Steps

1. Sign on to your account or app.

   Result:

   The **Authenticating on...** window appears displaying the **Forgot your device?** link.

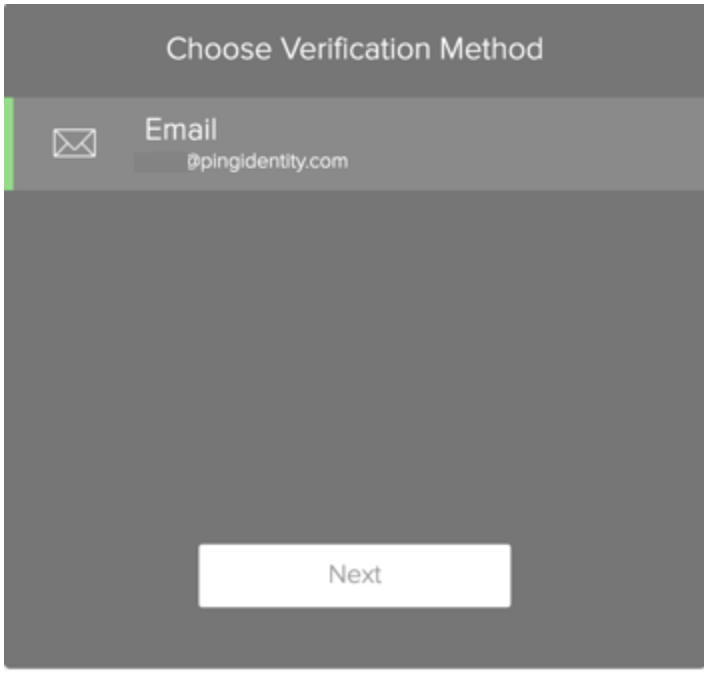


> **Note**
>
> If the **Forgot your device** link is not available, contact your helpdesk to access your account.

2. Click **Forgot your device?**.

   Result:

   The **Choose Verification Method** window displays a list of the backup devices available to you.



> **Note**
>
> The list of devices available to you depends on the configuration options defined by your organization.

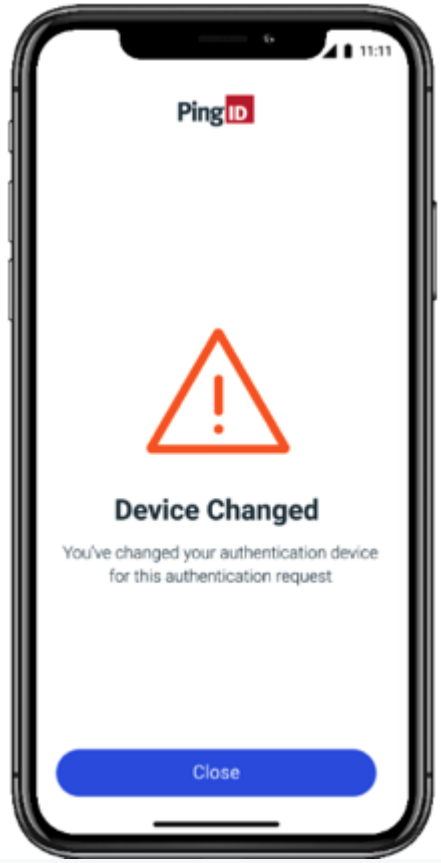
3. From the **Choose Verification Method** list, select the device or method you want to use to authenticate. Click **Next**.

   Result:

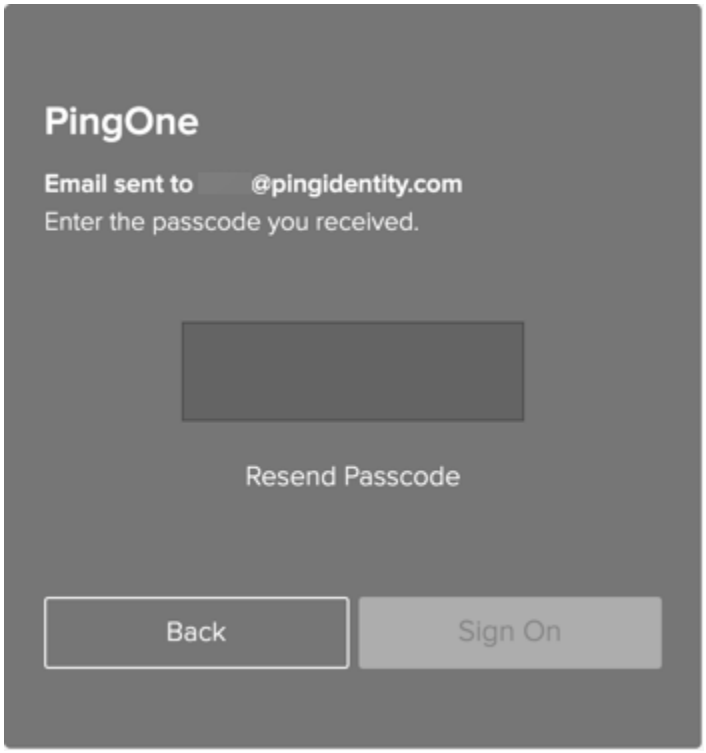
   You receive an OTP to the device that you selected.

Note

If a push notification is sent to your primary device, the push notification cancels, and a **Device Change** notification displays on your primary device.

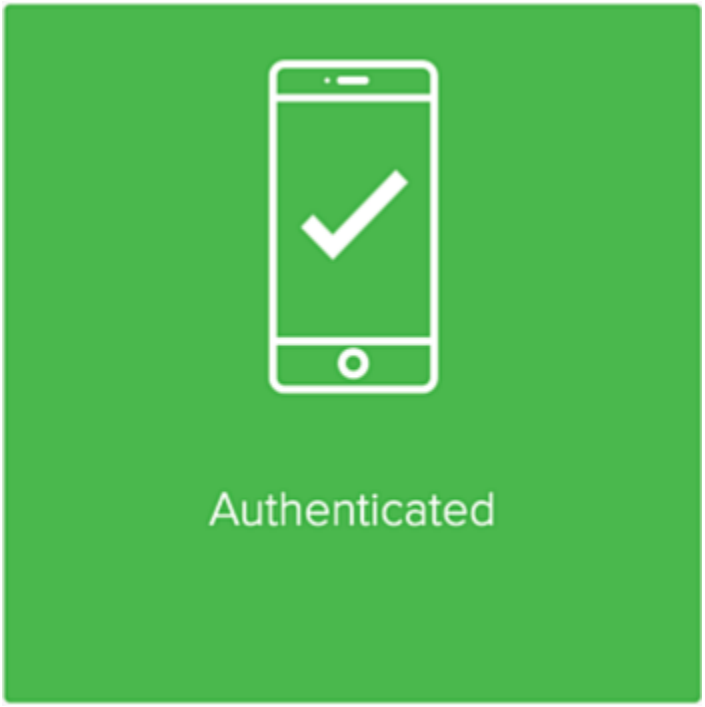


4. In the **Authentication** window, enter the OTP into the passcode field. Click **Sign On**.



Result:

You see a green check mark, indicating successful authentication, and your access is approved. You are automatically signed on to your application.



Verify your identity with PingID

Verify your identity to your employer

Pairing my device | Authenticating with PingID

- How to verify your identity

  How to verify your identity with PingID

- What is identity verification

  An introduction to identity verification PingID

- Troubleshooting verification

  Answers to common issues when verifying your identity

How to verify your identity

You can verify your identity using PingID, without needing to be physically present at the employer.

Before you begin

1. Install PingID mobile app to your mobile device from the relevant app store:
   - iOS
   - Android

   You can also download the app from the PingID downloads page.
2. Get the QR code from your employer (usually by email, or SMS) and display it on a different device. You'll either find the QR code:
   - On the employer's website, when they ask you to verify your identity.
   - Sent to you by email or SMS.
3. Make sure that you have your government-issued ID with you.

About this task

When asked to verify your identity, you will be asked to do one or more of the following:

- Take a live selfie to confirm it's you.
- Scan the front and back of your valid ID.
- Provide a phone number or email address so that you can receive a code to confirm it's you.

The organization making the request defines which of these actions you'll be asked to do.

Steps

1. Tap 

and scan the QR code that you received from the organization that's asking you to verify your identity. You'll be asked to do one or more of the following steps.

1. If you are asked to match a code, check that the code on the app matches the code on your phone, and tap **Begin Verification**.
2. If you are asked to enter your phone number, select the correct country code and enter your phone number (without the 0 prefix), and tap **Continue**.
3. When you are asked to capture your ID, make sure you have an ID with you (for example, passport, ID card, or driver license), tap **Continue**, and then:
    1. Allow all camera permissions for your browser or the PingID mobile app.
    2. Scan the front of your ID.
    3. Scan the back of your ID.

    > **Tip**
    >
    > Make sure that you are in a place with good lighting and that all of the details on the ID and any barcode is clearly visible in the camera.
    > If you are using a web browser, you can also upload a photo of your ID.
4. If you are asked to verify you email, enter your email address, and tap **Enter**.

Result

You'll see a confirmation message telling you that you've completed the steps required to submit your verification check.

Verification might take a few seconds or a few minutes and depends on the organization's requirements. Some documents might require more detailed checking. If you are unable to proceed after several minutes, contact the organization requesting the verification check for further guidance.

What is identity verification?

Identity verification enables you to prove your identity digitally by sharing verifiable information, such as a live selfie and a government-issued ID.

An organization might ask you to verify your identity as part of their employee onboarding process. You might also be asked to verify your identity if you forgot your password or as part of the account recovery process if your authenticating device was lost or stolen.

Using a series of verification steps, PingID enables you to prove your identity to your employer, so you don't need to be physically present to present your proof of identity.

Typically, the employer that's asking you to verify your identity will give you a QR code to scan with your mobile device or to access from an SMS message. They'll ask you to download PingID mobile app to scan the QR code or enter the SMS code.

When you scan the QR code, you'll need to do one or more of the following from within PingID mobile app:

- Verify your phone number or email address. A code is sent to the phone number or email address that you provide.
- Provide a live selfie.
- Scan your ID, such as a passport, government-issued ID card, or driver license.
- Provide a recording of your voice.

The use of a live selfie and other security verification checks prevents anyone that might attempt to obtain your details fraudulently from being able to do so.

The tasks you are asked to do vary depending on the organization making the verification request.

Which IDs are valid?

Many types of IDs from locations across the world are acceptable forms of identification. Typically, these include any government-issued identity document with a photo such as:

- ID cards
- Passports or passport cards
- Driver licenses
- Residence permits or visas

If your ID is not on this list, you can check with the employer making the verification request to see if they can accept it.

How do you secure my personal information?

Verification establishes a chain of trust between you and your employer. When this trust relationship is established, it reduces the likelihood of unauthorized individuals accessing your personal account or impersonating your digital identity.

During the verification process, your personal identifiable information (PII) is securely stored by Ping Identity for a limited time period of no more than 30 minutes, and information is only shared with your employer if they are permitted to access it. After the verification is completed, Ping Identity only stores the status of the verification request, and all PII used in the verification request is deleted.

What information is shared with my employer during the verification process?

Any of the information that appears on your ID and details of your phone number, email address, and voice sample will be shared with your employer if requested for verification purposes.

How do I start verifying my identity?

When an employer wants you to verify your identity, they will show you a QR Code or send you one by email or SMS.

From your mobile device, you'll need to download the PingID mobile app and use it to scan the QR code.

To enroll and verify your ID, see How to verify your identity

Troubleshooting PingID authentication issues

Find solutions to common PingID authentication issues.

Troubleshooting PingID authentication

The following use cases provide solutions to common PingID authentication issues that end users might encounter.

After entering the wrong password a number of times, I am told that I am locked out

Solution

After three incorrect password attempts, you are locked out for two minutes. Try again after the two minutes have passed.

I'm trying to pair or authenticate with PingID mobile app using Face or Iris biometric authentication on my Android device. I am unable to complete the process as I get an error message 'Canceled'

Because of Android biometrics security limitations, Face and Iris recognition aren't supported for use with the PingID mobile app on some devices.

Solution

1. Make sure you have defined biometrics on your device.
2. If you are trying to use Face or Iris recognition, and your device doesn't appear to be supported, try the following additional configuration steps:
    1. Configure Fingerprint authentication. On some devices, Face or Iris recognition only appears when Fingerprint recognition is also configured on the Android device.
    2. Make sure you are using the latest version of Android OS on your device. Some devices require the latest version of Android OS to support Face or Iris authentication with PingID mobile app.

If you still can't authenticate using Face or Iris recognition, then your device doesn't support face or iris authentication with PingID mobile app.

> **Tip**
>
> If you can't authenticate with Face or Iris recognition, use Fingerprint authentication.

I have defined both Face and Fingerprint on my Android device, but when I authenticate with PingID mobile app, I don't have the option to choose between them

Solution

- Some Android devices don't give the option to choose between different biometrics authentication methods when authenticating with PingID mobile app. In such cases, set the primary method you want to use to authenticate in your device settings.
- Because of Android biometrics security limitations, Face and Iris recognition aren't supported for use with the PingID mobile app on some devices.

I received a message that my device is jailbroken, but I don't think that my device is jailbroken.

If your company implements a policy that doesn't allow the use of a jailbroken device, you receive this error if your device is jailbroken. You might also see this error in the following instances:

- Scenario A: Your device has applications that contain code that appears the same as a jailbroken application, such as the Cydia app. If so, your device appears as jailbroken to PingID mobile app, preventing you from authenticating.
- Scenario B: If you backup and restore to your current device using a backup that originates from a previous device that was jailbroken, it flags your current device as jailbroken even though the jailbreak activity wasn't performed on your current device.

Solution

Scenario A: Check whether you have any apps with the Cydia scheme and then uninstall them:

1. On your device, open the Safari browser and in the address field, enter the following:

```
cydia://
```

If you have an app that appears to PingID as a jailbroken app, a window displays asking you to `Open this page in <problematic app name>`.

1. Uninstall any problematic apps that are listed in the alert.

Scenario B: If you want to use PingID mobile app on this device, you must erase all contents and settings and then reinstall PingID mobile app.

> ⚠ **Warning**
>
> Erasing all content and settings deletes all of the apps, data, and personal settings from your device. Your device will reset to the factory defaults.

1. On your device, go to **Settings → General** and tap **Erase all content and settings**.
2. If you want to restore a backup, make sure the device from which the backup restores doesn't originate from a device that was jailbroken in the past.

Authentication error message

If you have an authentication error, you receive an error message that varies depending on your device:

- iOS::

`You must have Touch ID enabled to authenticate with PingID.`

- Android::

`You must have fingerprint enabled to authenticate with PingID.`

If these messages display, then your organization defined Fingerprint authentication as a requirement for signing on to services protected by PingID mobile app.

Solution

To authenticate, enable Touch ID or Fingerprint recognition on your mobile device.

Troubleshooting PingID mobile app notifications (iOS)

You need to be able to receive notification to your device when authenticating with PingID mobile app. If you are experiencing delays receiving notifications to your device, the following use cases provide solutions to common issues that iPhone users report with delays receiving notifications to their devices.

Turn off scheduled notification summary

When the notification summary feature is enabled, it prevents your iPhone from sending notifications straight away. Instead, it schedules them to appear at a specific time during the day. Disable notification summary so that you receive notifications immediately.

Solution

1. On your iPhone device, go to **Settings → Notifications**.
2. Tap **Scheduled Summary** and then make sure it is turned off.

Turn off Focus Mode or add PingID to the allowed notifications list

Focus mode (Do Not Disturb) silences calls, notifications, and alerts during designated times, so you can focus on other things without being disturbed.

Solution

Disable Focus Mode, or add PingID mobile app to the Focus Mode allowed list, so that you continue to receive notifications even when Focus Mode is on. .

1. On your iPhone device, go to **Settings → Focus → Do Not Disturb**.
2. Do either:
    - Allow notifications from PingID mobile app: Tap **Allowed Notifications → Apps → Add App** and select PingID mobile app.
    - Turn off**Do Not Disturb** to disable Focus Mode completely.
3. Make sure Focus Mode is not configured to turn on automatically: Go to **Turn On Automatically** and make sure that **Schedule** is disabled.

Allow Notifications for PingID mobile app

Make sure that your iPhone is set to allow notifications for PingID mobile app.

Solution

1. On your iPhone device, go to **Settings → PingID mobile app → Notifications**.
2. Make sure **Allow Notifications** is enabled, and **Time Sensitive Notifications** is enabled.
3. On the same screen, allow PingID mobile app to send alerts on the Lock Screen, Notification Center, and Banners.

Disable Low Data Mode

If your iPhone is set to enable Data Savings, it can prevent PingID mobile app from using data in the background, causing delays to your receiving notifications.

Solution

Disable Low Data Mode if you are using Wi-Fi:

1. On your iPhone device, go to **Settings → Wi-Fi**.
2. Tap the Info icon next to the Wi-Fi network to which you are connected and make sure that **Low Data Mode** is disabled.

Disable Low Data Mode if you are using Mobile Data:

1. On your iPhone device, go to **Settings → Mobile Data → Mobile Data Options**.
2. Make sure that **Low Data Mode** is disabled.

Disable Low Power Mode

If your iPhone battery saver is enabled, it can prevent PingID mobile app from running in the background, causing delays to your receiving notifications on time.

Solution

Disable Low Power Mode:

- On your iPhone device, go to **Settings → Battery** and make sure **Low Power Mode** is disabled.

Update PingID mobile app

Make sure you are running the latest version of PingID mobile app. See Updating the PingID mobile app.

Update your iPhone

Updating your iPhone to the latest version ensures you benefit from the latests bug fixes and improvements, to help you with any issues you might be experiencing with your iPhone, and notifications.

Solution

Check for and install any pending updates.

- On your iPhone device, go to **Settings → General → Software Update** and download and install any pending updates.

Reset your iPhone

If you still experience issues with delayed notifications, your last option is to reset your iPhone. This process resets all of your iPhone settings to the factory default, and should only be attempted if all of the other solutions presented do not fix your issue. If your personal files are backed up, they will not be affected.

Solution

To reset your iPhone:

1. On your iPhone device, go to **Settings → General → Transfer or Reset iPhone**.
2. Tap **Reset** and then select **Reset All Settings**.

Troubleshooting device management

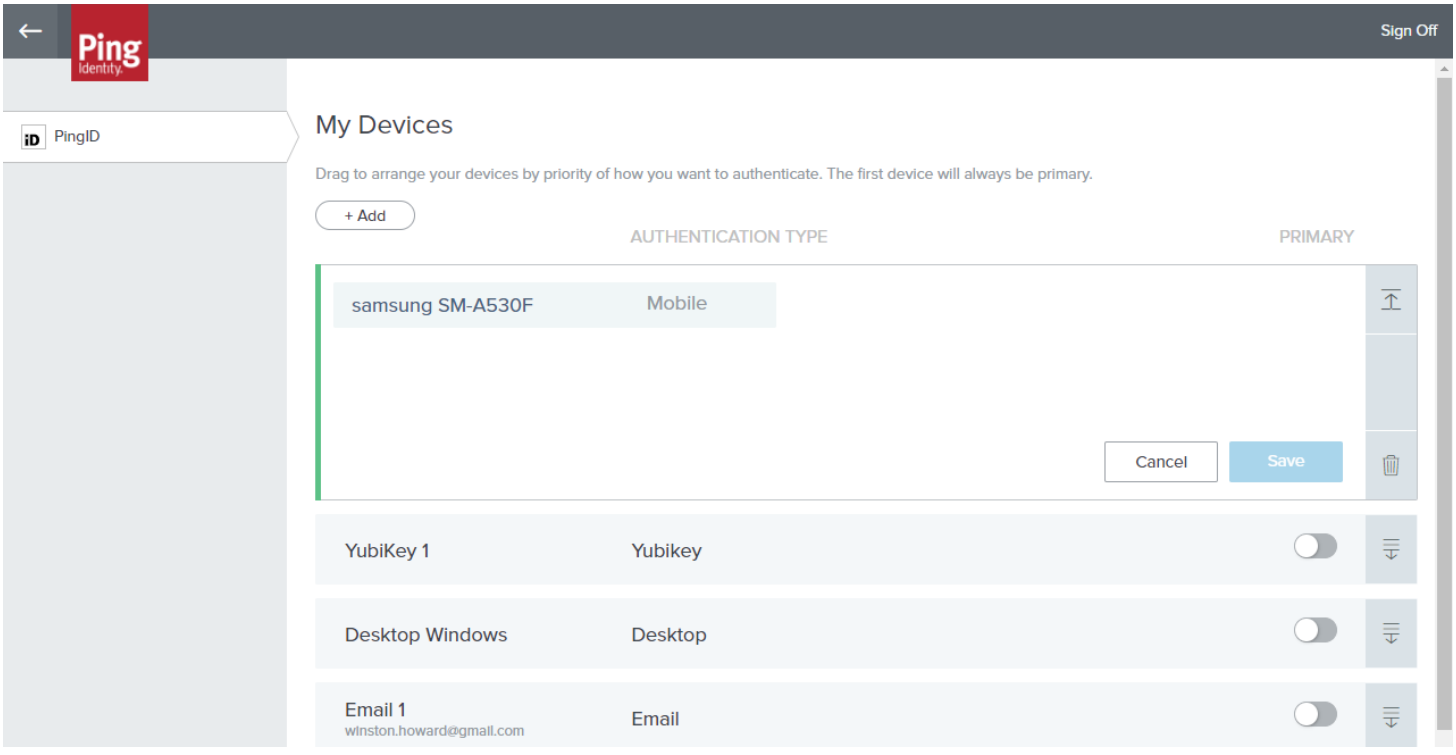
This section lists issues that you might encounter if you have more than one device paired with your account.

I'm trying to add a device. I'm being prompted to authenticate using FIDO2 biometrics, even though my accessing device is not paired with PingID.

If you only have FIDO2 biometrics devices paired with your account and your current accessing device is not paired with your account, you cannot manage your devices from the **My Devices** page.

Access the **My Devices** page from a FIDO2 biometrics device that is paired with your account and add an additional device, such as email, SMS, or Security Key. When accessing the **My Devices** page from your non-paired biometrics device, you can authenticate using the additional device and can then pair the new FIDO2 biometrics device to your account (recommended).

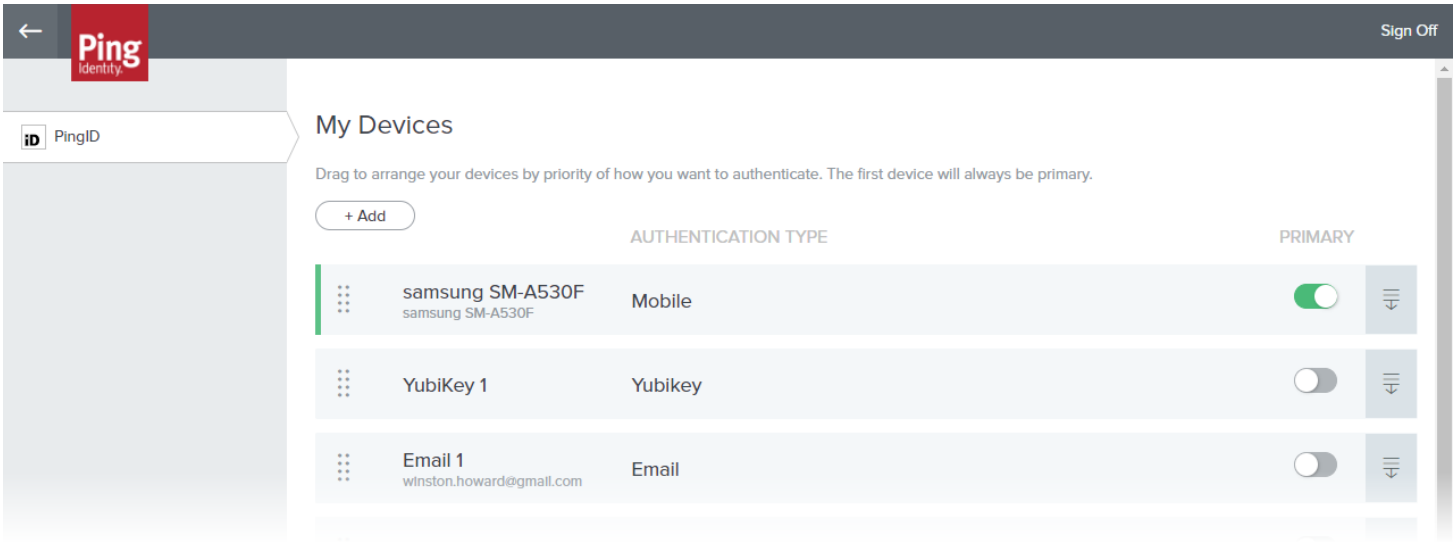
I cannot edit the mobile device details on My Devices page



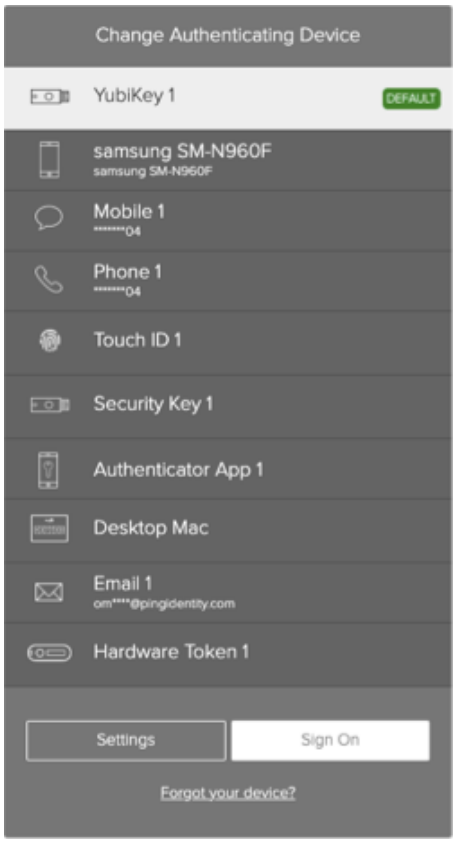
When I click the **Expand** icon ( ) next to one of the devices listed on the **My Devices** page, the details are not displayed and I cannot edit them.

The reason is that you can only change the device details for email, SMS, and voice authentication types. However, you can edit the description or device nickname for all authentication types.

My personal details are visible for one of my devices even when the screen is masked or locked



For your security, the **My Devices** page automatically masks or locks your personally identifiable information (PII) after a few minutes of inactivity and prompts you to authenticate if you want to make changes.
Only information in the **Device Detail**s field is masked automatically. Information in your device **Nickname** field is not automatically masked. Remove any personal information from the device **nickname** field. For more information, see Adding and reordering devices.



When I click the Settings button nothing happens, and I'm unable to access the My Devices page

When you click **Settings** from the **Authentication** or **Change Authenticating Device** page, the system generates a new authentication request. You'll need to authenticate again to access the **My Devices** page.

> **Note**
>
> If your primary authentication device is email, SMS, or voice, it generates a one-time passcode (OTP) with which to authenticate. When you click **Settings**, a new OTP will be sent to your device, so make sure to check it. You must use the new OTP to access the **My Devices** page because any previously issued passcodes are no longer valid.

When I enter my one-time passcode, I see the message 'invalid passcode'

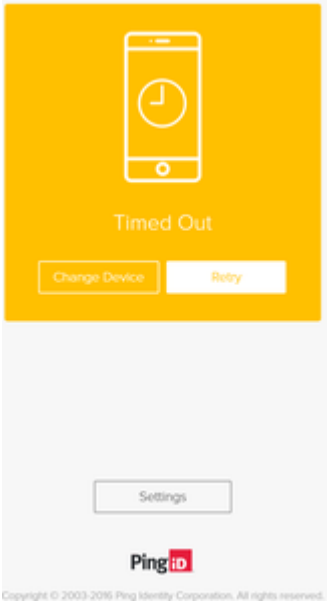
If you entered the wrong passcode or an old passcode that is no longer valid, you receive the message **Invalid passcode**. To generate a new passcode choose from the following actions:

- Click **Resend Passcode**. A new passcode is sent to the same device.
- Click **Change Device**, and select a different device with which to authenticate.

When trying to authenticate, I see the message 'Timed Out'

When prompted to authenticate, you have a limited timeframe in which to authenticate. This timeframe is defined by your organization. If you wait longer than the time defined, you see the **Timed Out** message. To try again, choose from the following actions:

- Click **Retry**.
- Click **Change Device**, and select a different device with which to authenticate.



Troubleshooting FIDO2 biometrics

This section lists common issues that end users may encounter when using FIDO2 biometrics authentication.

I am trying to sign on to my account using Safari and I see the error 'Found no credentials on this device', even though my device is paired with PingID

if you recently accessed the Safari settings on your iOS or Mac device, and selected Clear history and website data from Safari, your PingID credentials are also deleted.

Solution

- If you have more than one device paired with your account:
    1. Sign on to your account and then access your Devices page.
    2. Unpair your iOS or Mac device. For more information, see Unpairing a device
    3. Pair your iOS or Mac device again. For information see Pairing your Mac Touch ID device or Pairing your iOS or iPadOS biometrics device.
- If this is the only device that is paired with your account:
    1. Contact your organization's helpdesk and ask them to unpair your device.
    2. When you receive confirmation that your device is unpaired, pair your iOS or Mac device again. For information see Pairing your Mac Touch ID device or Pairing your iOS or iPadOS biometrics device.

I paired my Mac and can authenticate in one browser, but when I switch to a different browser, I can't authenticate

Mac Touch ID FIDO2 authentication is browser specific, so although it is supported by both Safari and Chrome browsers, when you pair your device, you can only authenticate using the same browser that you used to pair your account.

Solution

To authenticate from more than one browser, you need to pair your device with the second browser separately.

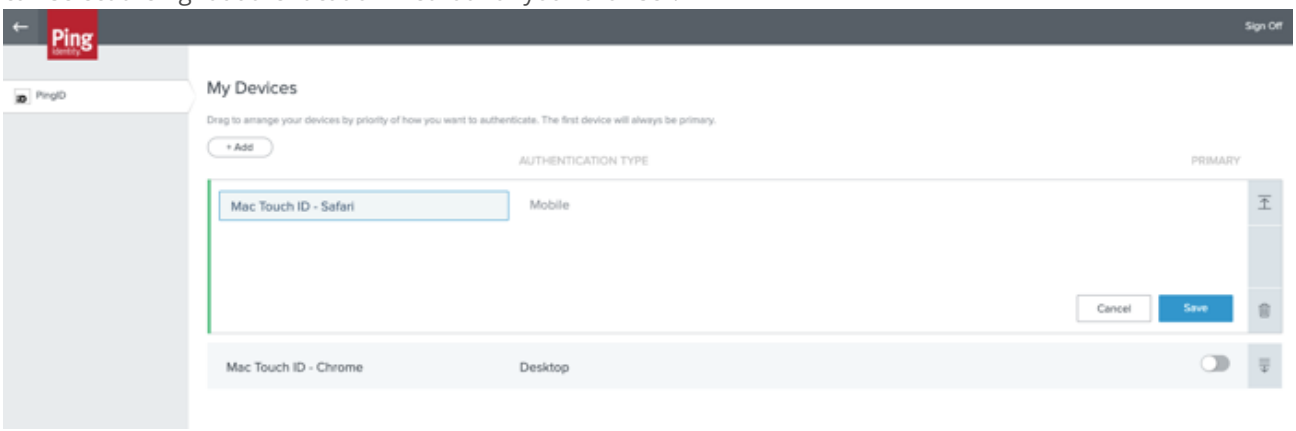
1. Pair your Mac Touch ID device with a browser. In this example, we'll use Safari. For information, see Pairing your Mac Touch ID device.
2. From that browser - in this example, Safari - go to your Devices page, and add another authentication device, such as a security key. For information, see: Adding and reordering devices.
3. Go to the second browser that you want to use - in this example, Chrome.
4. From Chrome, sign on to your account and authenticate with the second device - in this example, a security key.

> **Note**
>
> If your Mac Touch ID device is your primary authentication method, you'll need to click Change Device and select the Security Key specifically.

5. In Chrome, go to your Devices page and click Add. You may be prompted to authenticate with your security key.

6. In the Add a New Device window, click Touch ID and then follow the instructions to pair your Touch ID device from the new browser. For information, see Pairing your Mac Touch ID device.

7. When you have completed pairing your device, expand the entry and rename the new Mac device entry, to specify which browser it can be used to access. Do this for your existing entry too. That way, when you authenticate, you can select the right authentication method for your browser.



I am trying to pair my FIDO2 biometrics device and I don't see it as an option in the list of authentication methods

Solution

- Check that the device you are using supports FIDO2 platform biometrics.
- Check that the browser you are using supports FIDO2 platform biometrics (e.g. the latest version of Chrome or Microsoft Edge).
- Ensure you have configured biometrics (e.g. your fingerprint or face) on your FIDO2 device.
- Ensure you are accessing your account from the biometrics device you want to pair (for example, access your account from Windows Hello machine if you want to pair a Windows Hello machine). This applies even when adding the device via the **Devices** page.

I am prompted to authenticate using one of the existing biometrics devices paired with my account, although I am trying to pair with my new device.

I have at least one biometrics device already paired with my account (Windows Hello, Apple Mac Touch ID, iOS, iPadOS or Android biometrics).

Solution

Log on to your Devices page using one of your paired biometrics device, and then pair an additional (non-FIDO2 biometrics) device with your account, such as YubiKey or authentication app. You can then log on to your Devices page from your new biometrics device, and add your biometrics device via the Devices page. Here's an example of how to do that.

I am prompted to authenticate with FIDO2 biometrics even though my device is not paired as FIDO2 biometrics

Solution

Do one of the following:

- Pair your FIDO2 biometrics device. After pairing, you can authenticate using the device the next time you are prompted to do so. To pair your device, see Pairing your Mac Touch ID device.
- Change your authentication device. When prompted to authenticate, click **Change Device** and authenticate with one of your paired devices.

I want to authenticate using my biometrics device, but I am prompted to authenticate with a Security Key. I cannot authenticate with either device.

This could occur if you are logging on to your account using a device that supports biometrics and either:

- Biometrics (e.g., fingerprint or face) are not defined on your device, or have been deleted from your device.
- Biometrics authentication was not successful (e.g., your face is defined but was not recognized by your device).

Solution

- Check all biometrics are defined correctly on your device, and that you are using the latest version of a browser that supports FIDO2 platform biometrics.

- If you have another device paired with your account, in the browser window:
    1. Cancel the security key request.
    2. Select **Change Device**, if available and select an alternative device to authenticate.

It is recommended that you pair your biometrics device with PingID so you can benefit from FIDO2 biometrics authentication on that device as well in the future.

I want to authenticate using my biometrics device, but I am prompted to authenticate with a Security Key even though I do not have one paired with my account

This could occur if you are logging on to your account using a device that supports biometrics and either:

- Biometrics (e.g., fingerprint or face) are not defined on your device, or have been deleted from your device.
- Biometrics authentication was not successful (e.g., your face is defined but was not recognized by your device).

Solution

- Check all biometrics are defined correctly on your device, and that you are using the latest version of a browser that supports FIDO2 platform biometrics.
- If you have another device paired with your account, in the browser window:
    1. Cancel the security key request.
    2. Select Change Device, if available and select an alternative device to authenticate.

It is recommended that you pair your biometrics device with PingID so you can benefit from FIDO2 biometrics authentication on that device as well in the future.

I registered my Windows Hello device but is does not appear as an option when trying to log in or authenticate

Solution

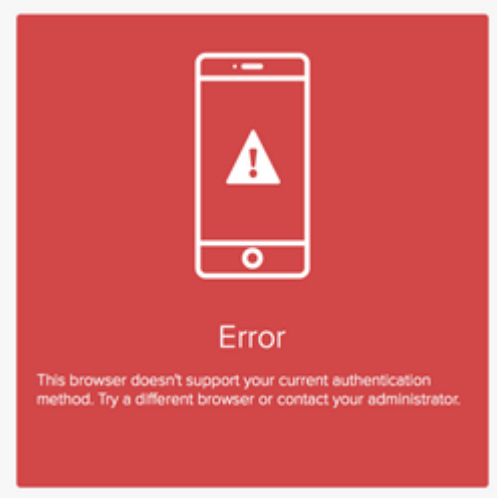
- Check all biometrics are defined correctly on your device.
- Ensure you are using an operating system that supports FIDO2 platform biometrics
- Ensure you are using the latest version of a browser that supports FIDO2 platform biometrics.

Troubleshooting a security key authentication

This section lists common issues that you may encounter when pairing and authenticating with a security key.

Error message when I try to authenticate

I try to log on and see the following error message:



Solution:

- The browser you are using does not support the use of a security key, or you are not using the latest version of the browser.
- Open a browser that supports use of security key, such as Google Chrome, and make sure you have the most up-to-date browser version installed on your device.

Security key doesn’t respond when I tap itI enter my username and password and then tap the security key when prompted, but nothing happens.

Solution:

- Make sure the browser window is the active window before you tap the security key. You can do this by clicking anywhere in the browser window.
- Make sure your security key is connected appropriately - either physically via a USB cable, or ensure NFC, or Bluetooth are set to 'ON'.

I am not given the option to authenticate using my security key, and must authenticate with a different device

I enter my username and password and I am prompted to authenticate using a different device. This happens even if my device is the primary device, or I have the option to choose a different device.

Solution:

- The browser you are using may not support the use of a security key, or you are not using the latest version of the browser.
- Open a browser that supports use of security key, such as Google Chrome, and make sure you have the most up-to-date browser version installed on your device.
- Make sure your security key is connected appropriately - either physically via a USB cable, or ensure NFC, or Bluetooth are set to 'ON'.

I want to authenticate using my biometrics device, but I am prompted to authenticate with a Security Key. I cannot authenticate with either device.

This could occur if you are logging on to your account using a device that supports biometrics and either:

- Biometrics (e.g., fingerprint or face) are not defined on your device, or have been deleted from your device.
- Biometrics authentication was not successful (e.g., your face is defined but was not recognized by your device).

Solution:

- Check all biometrics are defined correctly on your device, and that you are using the latest version of a browser that supports FIDO2 platform biometrics.
- If you have another device paired with your account, in the browser window:
    1. Cancel the security key request.
    2. Select **Change Device**, if available and select an alternative device to authenticate.

It is recommended that you pair your biometrics device with PingID so you can benefit from FIDO2 biometrics authentication on that device as well in the future.

I want to authenticate using my biometrics device, but I am prompted to authenticate with a Security Key, even though I do not have one paired with my account.

This could occur if you are logging on to your account using a device that supports biometrics and either:

- Biometrics (e.g., fingerprint or face) are not defined on your device, or have been deleted from your device.
- Biometrics authentication was not successful (e.g., your face is defined but was not recognized by your device).

Solution:

- Check all biometrics are defined correctly on your device, and that you are using the latest version of a browser that supports FIDO2 platform biometrics.
- If you have another device paired with your account, in the browser window:
    1. Cancel the security key request.
    2. Select **Change Device**, if available, and select an alternative device to authenticate.

It is recommended that you pair your biometrics device with PingID so you can benefit from FIDO2 biometrics authentication on that device as well in the future.

I am trying to pair my security key while using a virtual machine (VM), and I'm getting a message that it's already paired

I've never paired this security key with my account before.

Solution: The VM may not be recognizing your security key.

- If you are using a virtual machine (VM), and want to pair your security key, check your VM configuration, and make sure the security key that you are trying to pair is recognized by your VM.

Troubleshooting identity verification

The following use cases provide solutions to common identity verification issue.

I cannot take a selfie

Solution

If you're having trouble taking a selfie, in PingID mobile app, try the following:

- Move to an environment with good lighting.
- Make sure there's nothing blocking your face.
- Position the camera directly in front of your face.
- Move the camera farther from or closer to frame to:
  - Position your face in the **center** of the oval.
  - Make sure all of your face appears **inside** the oval.
- Make sure your camera doesn't move while you are taking the selfie.

If you're still unable to take a selfie, contact your employer's support team.

I cannot capture my ID

Solution

Place the ID on a flat surface and hold the camera horizontally over the ID, and then make sure that:

- All four corners of the ID are visible by the camera, and in focus.
- The camera is steady when taking the picture.
- You're in an environment with good lighting.
- There's no glare on the ID.
- Nothing is blocking the ID, including your fingers.
- Make sure you are using a permitted ID. You can use a government-issued identity document with a photo to verify your ID, such as an:
  - ID card
  - Passport or passport card
  - Driver license
  - Residence permit or visa

If your ID is not on this list, you can check with the employerorganization making the verification request to see if they can accept it.

Why did my ID verification fail?

Solution

There are various reasons that verification may fail, including:

- The ID type that you presented is not accepted by the employer or is not a supported ID type.
- The image quality is too poor for the selfie or ID captured.
- The ID document is not readable, the ID is damaged, or the ID barcode is damaged.
- Some employers do not accept expired IDs.

The criteria for verification can vary between employers. For more specific information, contact the employer that is making the verification request.

How do I know if my verification request was successful?

Solution

The next steps after completing identity verification vary depending on the employer and the action you're trying to complete. If you are unsure how to proceed, contact the employer for more guidance.

Manage and share Creds

How to pair, receive, manage, and share digital credentials (Creds)

Pairing a device for authentication | Authenticating with PingID | Verifying your identity

- What are Creds?

  Learn what Creds are and why to use them

- Getting started with Creds

  Learn the steps needed to start using Creds

- Pairing and sharing Creds

  How to start receiving and sharing your Creds

- Troubleshooting Creds

  Get answers to common issues when using Creds

All you wanted to know about using Creds

What are Creds?

Creds are digital versions of your credentials (such as an employee ID, membership card, or proof of certification) that represent your identity, affiliation, or eligibility. They're issued by trusted organizations to your PingID mobile app, and can be used to easily verify your identity or securely authorize transactions in a single step.

For example, as an employee, you might need Creds to gain access to your office. Your employer could issue you with a digital employee badge credential containing verifiable information such as your:

- Full name
- Employee ID
- Job title and department
- Access level clearances
- Photo

Physical IDs can be lost, stolen, or forged. Digital Creds are stored in your PingID mobile app. They're more secure because they're cryptographically signed by your employer and bound to your specific mobile device. When you need to prove your identity, you can present the necessary Creds through your app.

Imagine arriving at work and using your Creds to:

- Access your building without your physical key card
- Access specific floors or office areas based on your security clearance level
- Sign on to company systems and applications

- Sign internal documents digitally
- Prove your employment status to third parties when needed.

Creds are always accessible on your mobile device and are stored securely in your PingID app. You can view, manage, and share your Creds whenever you need, putting you in control of your digital identity.

Why use Creds?

Creds revolutionize the way you receive and share verifiable credentials and information. You no longer need to carry around access cards you might need for work or your work credentials.

With Creds, you can prove you are who you say you are and share limited credentials (Creds) with interested parties straight from your mobile device using PingID mobile app.

Unlike traditional physical cards with which you have to share all of the information that appears on the card at once, the parties requesting information from you can allow you to choose which details you share with them, so you can leave out 'optional' fields and share only the information that's needed.

Benefits include:

Easy access: Access everything you need right from your mobile device with no physical wallet required.

Secure and safe: Your Creds are protected with advanced technology, ensuring your information stays secure and unchangeable.

Sharable: Creds can be shared with many different verifiers, not only the organization that issued them. This gives you the flexibility to use them in many different situations.

Who can issue Creds?

Creds are typically issued by trusted organizations (issuers) that can validate your information, such as:

- Employers
- Banks
- Universities or education platforms
- Healthcare providers
- Government agencies The Creds issued to your app are backed by the trusted reputation of the organization that issues them, ensuring the authenticity and security of the Creds.

What is an "issuer"?

An issuer is an authority, such as an employer, university, or any trusted organization that can issue a digital credential directly to your PingID mobile app.

For example, your employer can create and issue Employee ID Creds to give you access to their resources, or gym membership Creds (known as **'Creds'**) directly to your PingID mobile app, so you can store those Creds securely and share them directly from the app.

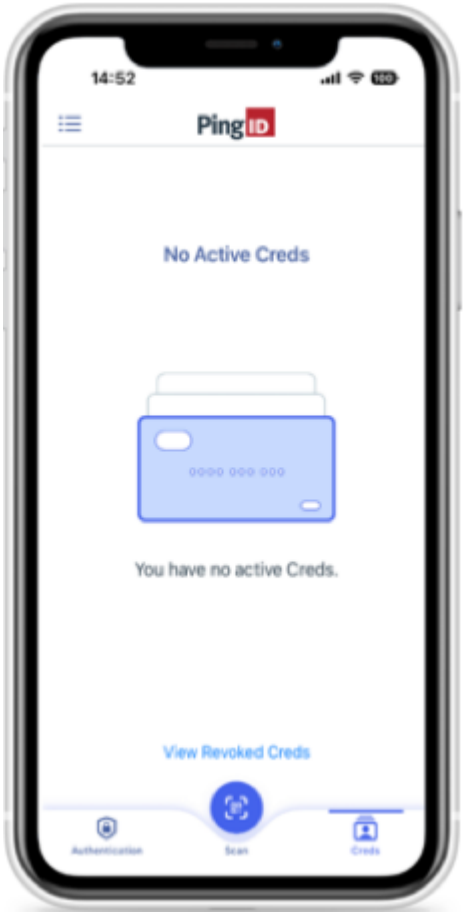
Getting started with Creds

Use this basic workflow to get you set up so you can start using Creds.

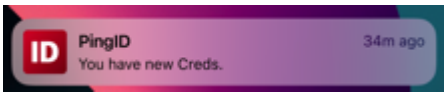
1. If you don't already have it installed on your mobile device, download PingID mobile app from your app store.

   Learn more: Pairing PingID mobile app (using a QR code or pairing key)

2. Pair PingID mobile app with the organization that's issuing your Creds.

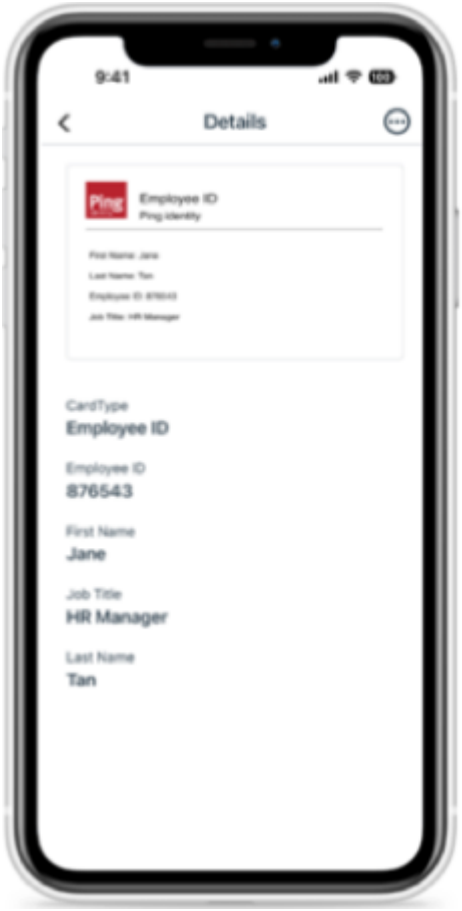


3. When the issuer sends you Creds, you'll get a notification on your mobile device. Tap the notification or open the app to view your Creds.

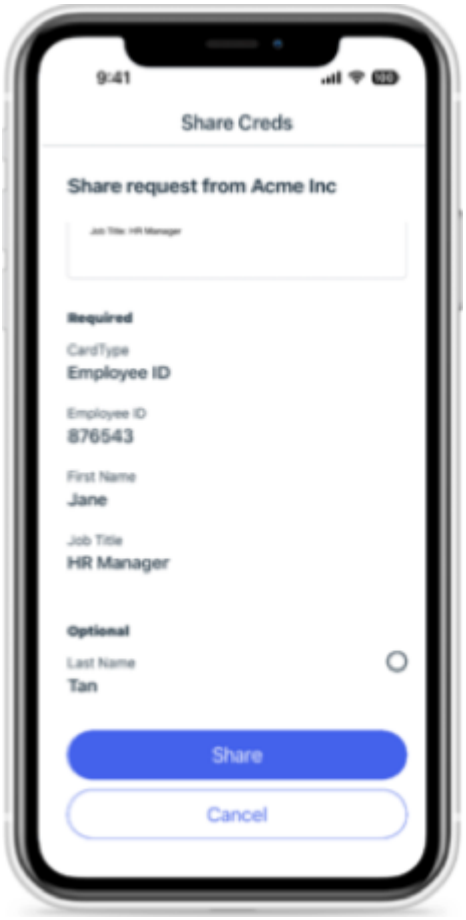


You can see your Creds on the PingID mobile app **Creds** tab.

4. Tap the Creds entry to view the details.



5. To share your Creds, you'll use PingID mobile app to scan a QR code that you'll receive from the organization that's requesting your information. You'll be able to see details of the Creds they want you to share, and approve the request from the app.



Learn more in Pairing and sharing your Creds

Pairing and sharing your Creds

How do I pair Creds?

To start receiving Creds, you first need to pair your PingID mobile app with an issuer (for example, your employer). To receive Creds from more than one issuer, you must pair your app with each issuer separately.

Before you begin

Before pairing, make sure you have:

- A biometrics lock, such as face or fingerprint ID, or a PIN defined on your mobile device.
- A QR code or link from the issuing organization.

Steps

To pair Creds:

1. In PingID mobile app, tap **Scan**.
2. Scan the QR code provided by the issuer.

3. Accept all the permissions requested. They allow PingID to send notifications and use the camera to scan QR codes for receiving and sharing Creds.
4. Enter your mobile device PIN or biometrics to complete the pairing process.

How do I receive Creds?

You'll be notified on your mobile device whenever you receive new Creds from an issuer.

Before you begin

To receive Creds, you must first pair your mobile device with the issuer of those Creds.

Steps

1. To see your new Creds, navigate to the **Creds** tab.
2. To view Creds details, tap the Creds that you want to view.

   New Creds are labeled 'New' for the first 24 hours, or until they are opened.

How do I share my Creds?

Steps

1. If you're asked to share your Creds the requester issuer will display a QR code. Open PingID mobile app, tap **Scan**, and scan the QR code.
2. Review the Creds details.
   - Required fields are pre-selected and can't be removed.
   - Optional fields are listed under an **Optional** heading. Select the checkbox next to any optional field that you want to include when sharing the Creds.
3. To send the selected information to the requesting organization, tap **Share**.

Can I backup or move my Creds to a new device?

Creds are stored securely on a single device and cannot be backed up or transferred manually. If you need to move your Creds to a new device or reinstall the PingID mobile app, you'll need to have your Creds reissued.

To do that, contact the issuer's support team. They can help you pair your new device and reissue Creds to that device.

Troubleshooting Creds

The following use cases provide solutions to common issues with receiving or sharing your Creds.

Why don't I see any Creds?

If you don't see any Creds in your PingID mobile app **Creds** tab, the following reasons might apply:

- **Your Creds aren't paired**:

  You need to pair your device with the organization that will be issuing your Creds (the issuer). The issuer should provide you with a QR code you can scan to pair your device.

  ### *Solution*

  Open PingID mobile app, tap **Scan**, and then scan the QR code you received from the issuer. Follow the instructions on the screen to pair your device.

  Learn more in Pairing and sharing your Creds

- **The Creds weren't issued yet**

  If you don't see the Creds you expect to see listed in the **Creds** tab in PingID mobile app, your Creds might not have been issued yet.

  ### *Solution*

  Contact the organization that are due to issue your Creds to check when you should expect to receive them.

- **The Creds were revoked**

  Some Creds might be issued for a limited time period, or the issuer might have reason to revoke them.

  ### *Solution*

  If you suspect your Creds were revoked by the Issuer in error, contact the issuer's support team to confirm this or request that they reissue them.

- **You moved PingID mobile app to a different device**

  If you paired PingID mobile app on one device and then move PingID to a new device, your Creds do not transfer automatically. You'll need to contact your issuer to help you unpair and reissue your Creds.

> **Tip**
>
> If you think you should have Creds, but you're not seeing them, contact your organization's customer support team for assistance.

How do I move my Creds to a new device?

Creds are securely stored on a single device and cannot be backed up or transferred manually.

Solution

If you need to move your Creds to a new device or reinstall the PingID app, contact the support team of the organization that issued your Creds and ask them to reissue your Creds. They can help you pair your new device and reissue Creds to that device.

How do I unpair an issuer from my PingID mobile app?

To receive Creds, you pair your PingID app with each issuer from which you want to receive Creds. However you cannot unpair an issuer directly.

Solution

Delete all the Creds related to the issuer you want to remove.

To do that:

1. On the PingID mobile app **Creds** tab, tap a Creds entry to view its details and confirm the issuer.
2. For each Creds entry that you want to delete, swipe left to reveal the **Delete** button, and then tap **Delete**.
3. Repeat the previous steps for each Creds entry you want to delete.

What happens if an issuer revokes my Creds?

If your Creds were revoked, you'll won't be able to use them or share them with others.

Solution

If you think your Creds were revoked in error, or you would like to request that they are reissued, contact the issuer's support team.

Managing your devices

Add, remove, or edit the devices that you use to authenticate depending on your needs. Choose from a list of devices when you authenticate. Manage your PingID mobile app (including transferring the app to a new device), manage PingID desktop app, and find out what to do if your device is lost or stolen.

Throughout this section, we will use the term "device" and "authentication device" to include "authentication method" as well unless there is a specific difference.

Adding and authenticating with multiple devices

If you have more than one device paired with your account, you can select an alternative device to authenticate with during the sign-on process. This is useful when you leave your phone at home, find yourself temporarily without an internet connection, or need to authenticate manually.

- Add and reorder devices
- Rename a device
- Select a device during authentication
- Select a device during authentication (VPN)
- Unpair a device
- Handling a lost, broken, or stolen device situation

Managing PingID mobile app

You can manage many of your PingID settings from the PingID mobile app, including:

- Move PingID app to a different phone (Change Device)
- View, pair or remove additional organizations
- Change your mobile app PIN
- Disable push notifications
- Report fraud
- Send an event log to your support team
- View supported operating systems
- Manage your Android device settings forPingID
- Manage your iPhone device settings for PingID
- Update PingID mobile app
- Unpair PingID mobile app
- View legacy documentation

Managing PingID desktop app

You can manage many of your PingID settings from within the PingID desktop app, including:

- Pair your desktop app to an additional organization
- Manually update the desktop app (Mac)
- Manually update the desktop app (Windows)
- Change or reset your desktop app PIN code
- Disable your proxy for PingID desktop app
- Send an event log to customer support.
- Unpair PingID desktop app.

Handling a lost, broken, or stolen device situation

If your device is lost or stolen, unpair it immediately to ensure that no one else can use it to access to your account. It is also recommended to report it to your IT department for security reasons.

Even if your device is lost, broken, or stolen, it will still be paired to your account and you should take steps to unpair it immediately. Unpairing a device depends on your organization set up and whether you have another device paired with your account. To unpair your device, do one of the following:

I have another device paired with my account

If you have another device paired with your account, in addition to the device that was lost or stolen, you can unpair your device yourself. Sign on to your account, go to your **Devices** page, and unpair your device. For information, see Unpairing a device.

I have a backup device I can use to access my account

If you have a backup device, you can unpair your device yourself.

1. Sign on to your account using your backup authentication device. For information, see Authenticating with PingID using a backup device.
2. Go to your **Devices** page, and unpair your device. For information, see Unpairing a device.

The lost, broken, or stolen device was the only device paired with my account

If the device was the only device paired with your account, and you do not have a backup device, or you do not have access to your **Devices** page, contact your organization's customer support representative and ask them to unpair the device for you.

Related links

- Moving PingID mobile app authentication to a new device (change device)

Adding and reordering devices

About this task

This task covers the following activities related to your devices list at authentication time:

- Adding a device
- Editing device details
- Choosing a primary (default) device
- Reordering your devices list

This section is relevant if your organization allows you to authenticate using more than one device. Adding more authentication devices is useful if your preferred device is unavailable (for example, if you left your mobile device at home). When prompted to authenticate, you'll be able to select a different device.

Furthermore, you can reorder your list of devices to reflect your priority. The device at the top of the list will always be used for authentication, by default.

> **Note**
>
> The options available for adding a device are defined by your organization. When adding a FIDO2 biometrics device, or security key, the browser used to access the **My Devices** page must support WebAuthn platform or WebAuthn respectively.

Steps

1. Access the **Devices** page either:

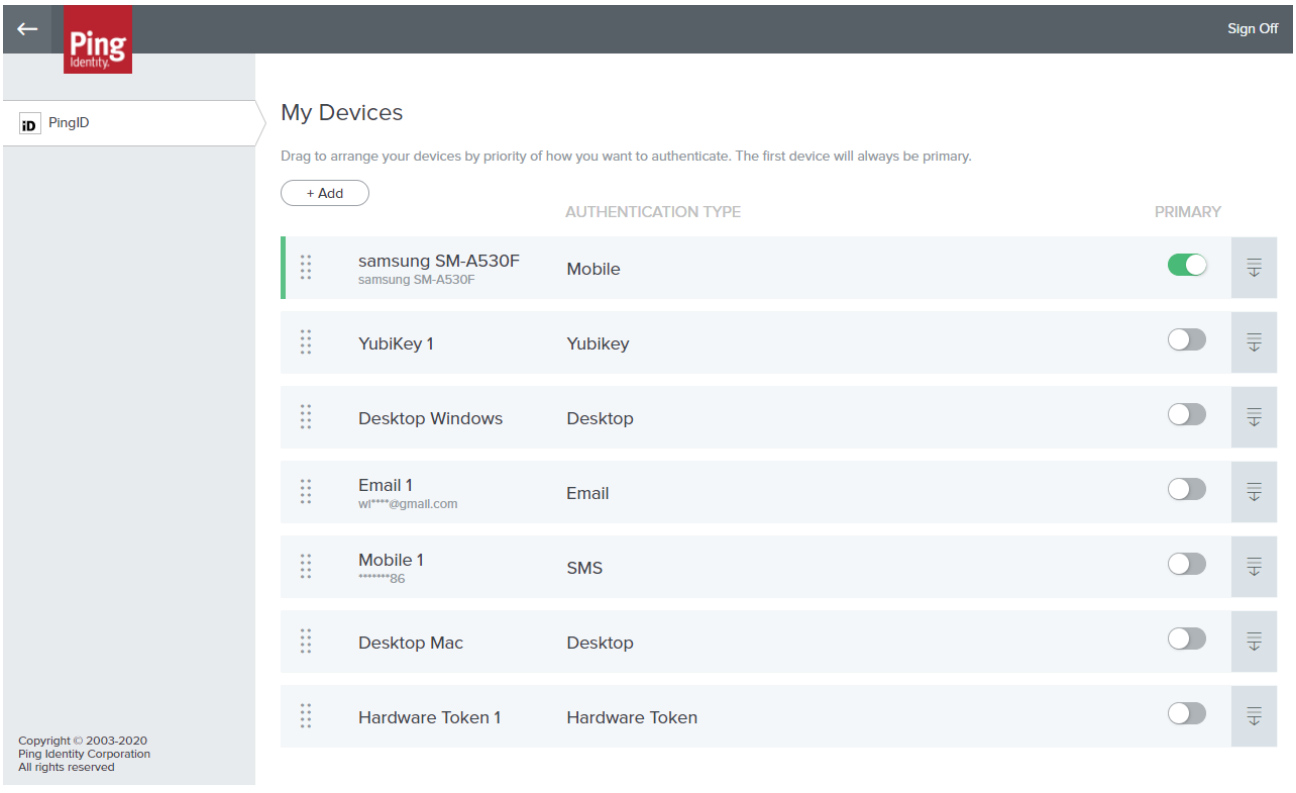
   Choose from:

   - During authentication: When the **Authentication** screen opens, click **Settings**.
   - From your organization dock: Click the **Account** icon ( ) and then click **Devices**.
   - From a link provided by your IT department.

   > **Note**
   >
   > When adding a FIDO2 biometrics device (including Windows Hello or Touch ID), you must access the **My Devices** page from the device that you want to add.

   Result:

   The **My Devices** page opens, showing the devices you currently have paired with your account. The primary device is first in the list.



2. Click **+Add**. You might be asked to authenticate using an existing authentication device.

   Result:

   The **Add New Device** window opens.

> **Note**
>
> The actual list of options available is defined by your organization.

3. Select the new authentication method to add, and follow the relevant instructions (see Pairing a device with PingID.

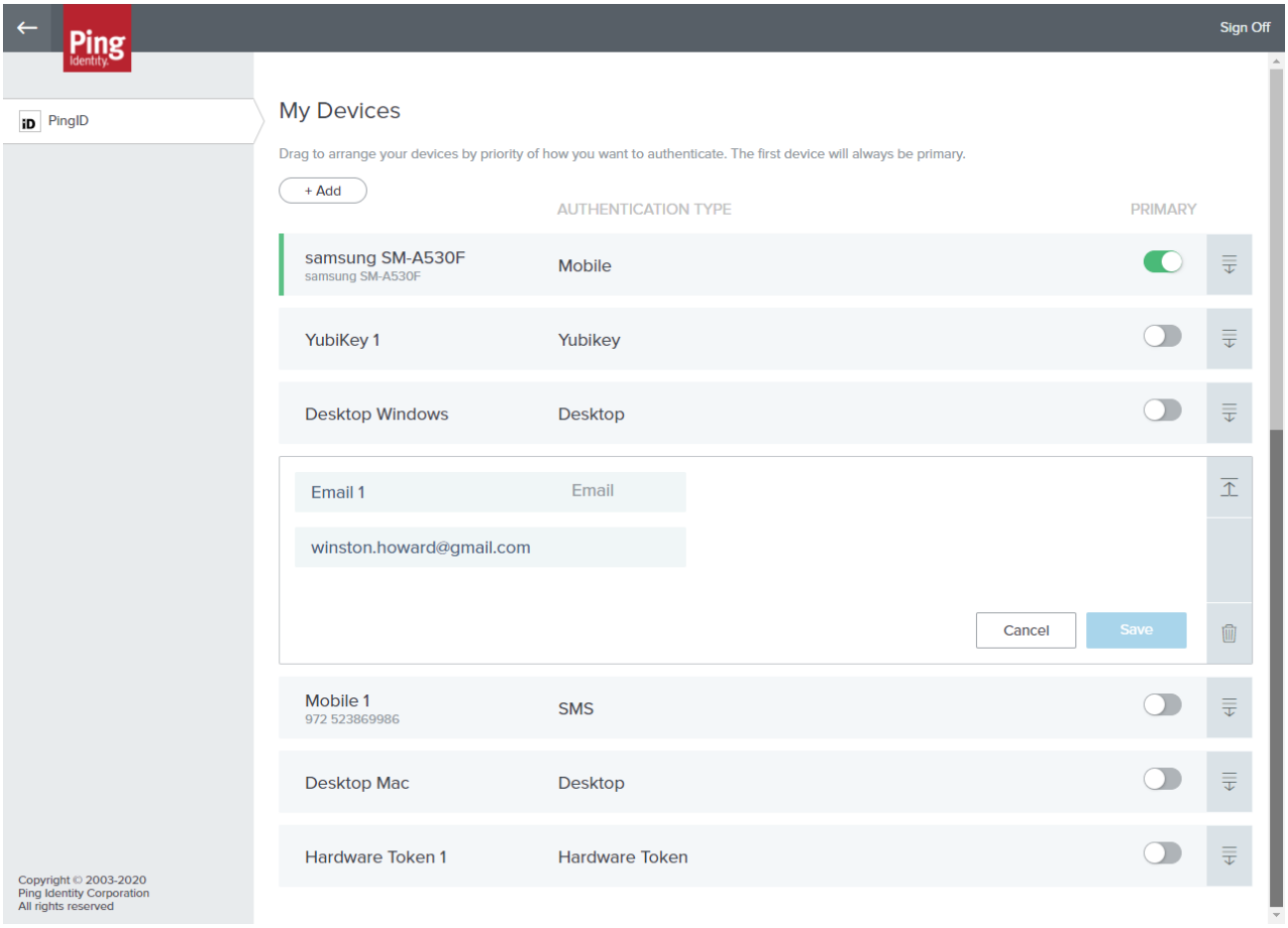
   Result:

   Each authentication method has its own set of instructions. Follow the instructions, download the relevant software, if required, and complete the registration and pairing of your newly added alternate authentication device.

   When the system has completed pairing your new authentication device, you are redirected back to the **My Devices** page, displaying the new device as the last row in the listing, with its default nickname.

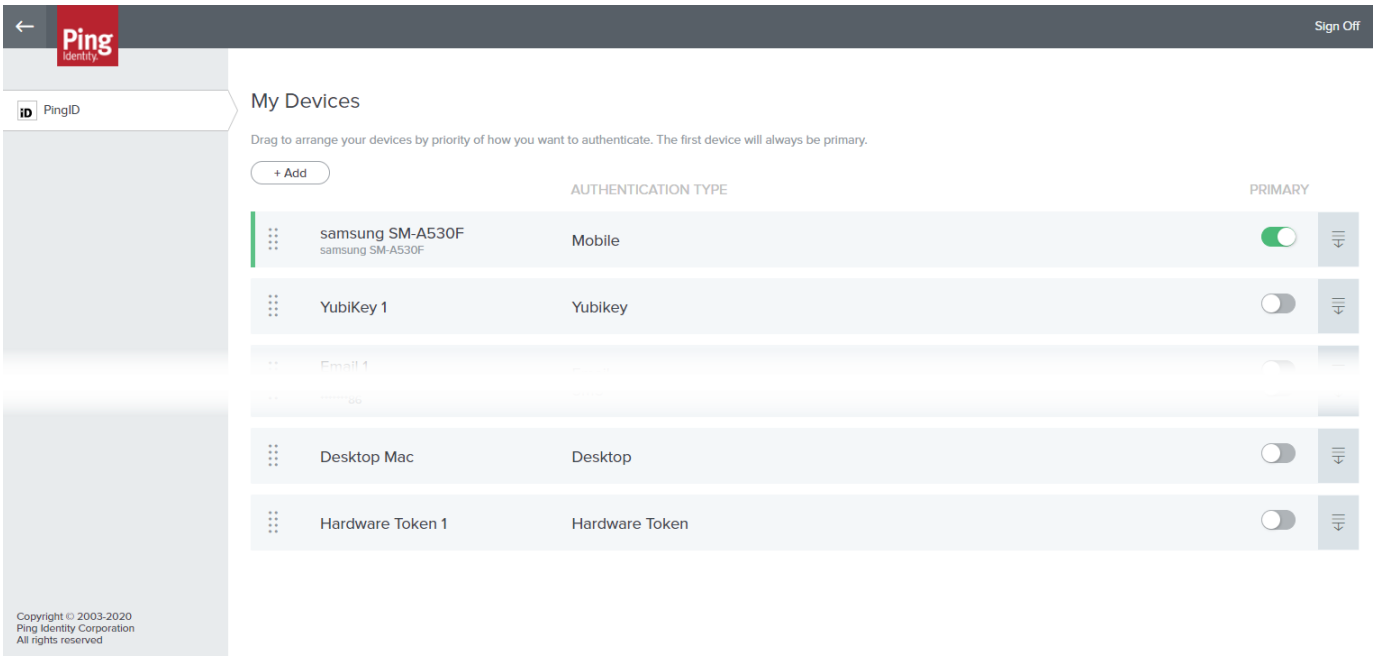
4. In the **My Devices** list, to view and edit details of a device, in the relevant row, click the **Expand** icon ( ) , and edit the following details:

   - Device nickname: This is the name of the device as it will appear when you are prompted to authenticate. The marketing name of the device (for example, iPhone X) or the authentication method (for example, email) is displayed by default.
   - Device details: Details that identify the authenticating device (for example, your email address or phone number). If you choose to edit the details, you are prompted to authenticate and must make sure the new details are valid (for example, valid phone number in the correct format). To protect your privacy, this information may appear masked if you have not recently authenticated.
   - Authentication type: Type of authentication method (for example, email, SMS, or YubiKey). This information is not editable.

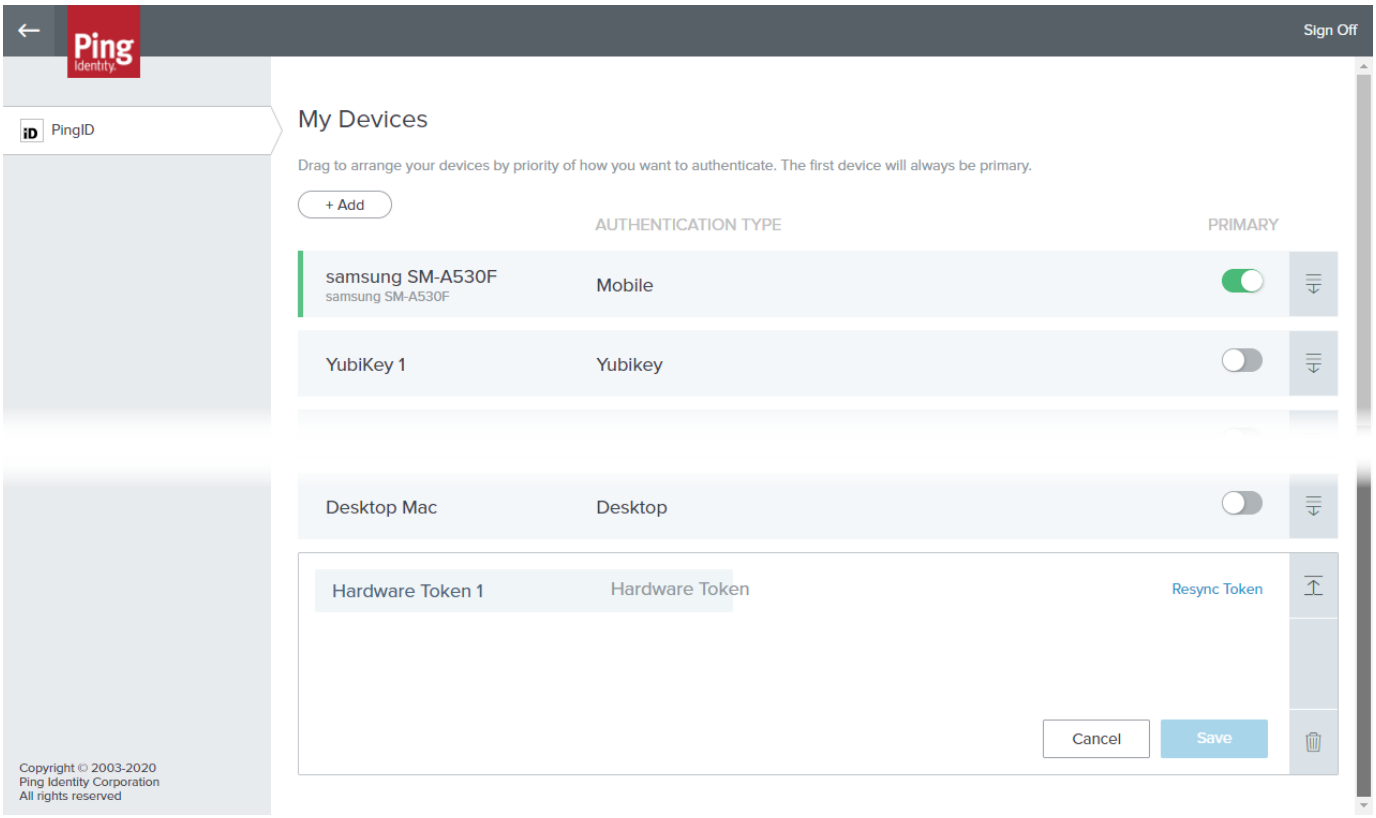


5. To make your new device (or any other) the primary (default) device, move the slider to **on** (green) in the **Primary** column. The toggled device will be moved to the top of the list.

   If you added a hardware token, you will see it in a window similar to this:



Click the **Expand** icon ( ) to view details of a device:



The only available edit are changing the token name and **Resync**. You do not need to resync unless your token goes out of sync with the OTP server. See Resynchronizing a hardware token for further details.

6.

To reorder the device list, drag the devices one at a time to their new position, using the Position icon ( ) to the left of each item in the list. You may be asked to authenticate first. Having done so, you may make multiple moves. Note you can change the primary device in this way.

> **Note**
>
> The left hand Position control ( ) icons are unavailable in edit mode.

PingID mobile app management

You can manage many of your PingID settings from the PingID mobile app.

You can also manage your phone settings to ensure you're providing the necessary permissions to the PingID mobile app.

Note

PingID mobile app uses the same language as the language defined in your phone mobile OS settings. If it's not one of the supported languages, it displays in English by default.

Managing PingID mobile app

Use the PingID mobile app to:

- Transfer your PingID authentication to a different phone.
- View, pair, or remove additional organizations.
- Change your PingID mobile app PIN
- Report authentication attempts that might be fraudulent
- Disable push notifications and authenticate with a one-time passcode (OTP) only.
- Send the event log to your support team
- Unpair the PingID mobile app.

Managing your device settings

Manage device settings related to PingID mobile app.

- Managing your device settings for iOS
- Managing your device settings for Android

Legacy documentation

View legacy PingID mobile app documentation.

Supported operating systems

The PingID mobile app can be used on the following operating systems.

Android

PingID is supported on any device running Android 9.x or later.

> **Note**
>
> Beginning with version 1.13 of the PingID Mobile App for Android, the app uses the Google camera API for scanning of QR codes and for taking a picture for the user profile. Therefore, these functions will not be available if you do not have Google Play Services installed or if you did not grant permission to the Google camera app.

iOS

PingID is supported on any Apple device running iOS 15 or later.

Moving PingID mobile app authentication to a new device (change device)

If you get a new mobile device, you can move PingID mobile app authentication from your old device to your new device in one action - without having to unpair and then re-pair it.

Before you begin

Before you begin, note the following:

- You should not use the backup and restore feature on your mobile device to move the PingID application to your new device. Although it will transfer the app to your new device, your account will remain paired to your old device, so you won't be able to authenticate from either device.
- To create a QR code your old device must be connected to the internet.

In some situations, you might not be able to transfer PingID to your new device directly, such as:

- If this feature is disabled by your organization.
- If you don't have access to your old phone, or do not start the transfer from within the PingID mobile app of your old phone.

- If you're not planning to use the PingID mobile app on your new device, but want to use a different authentication method, such as the device's built-in biometrics.
- If your old device is paired to more multiple organizations located in different data centers.

In these cases, you must manually unpair PingID from your old device and then manually pair PingID with your new device.

If you are unable to access your old device or your device is damaged, lost, or stolen, see A lost or stolen device situation.

About this task

This topic shows you how to transfer PingID mobile app authentication from your old phone to a new one using a QR code found within the app.

Steps

1. On your new device, download and install the PingID mobile app.
2. On the device you want to unpair (your old device), open the PingID mobile app, tap the **Menu** icon ( ), and then tap **Change Device**( ).

   > **Note**
   >
   > If your admin has disabled the option, the **Change Device** option will not be visible in the menu.

   Result:

   Your old device displays a QR code and pairing key.
3. On your new device, open the PingID mobile app and scan the QR code or enter the pairing key.

Result:

The pairing of your new device is complete, your old device is unpaired, and your organization is added to PingID. To view the organization, tap the **Menu** icon ( ), and then tap Settings.

Result

The next time you sign on to your account or app, you are prompted to authenticate from your new device.

> **Note**
>
> After you transfer PingID authentication to your new device, you are no longer able to authenticate on your old device.

Managing organizations

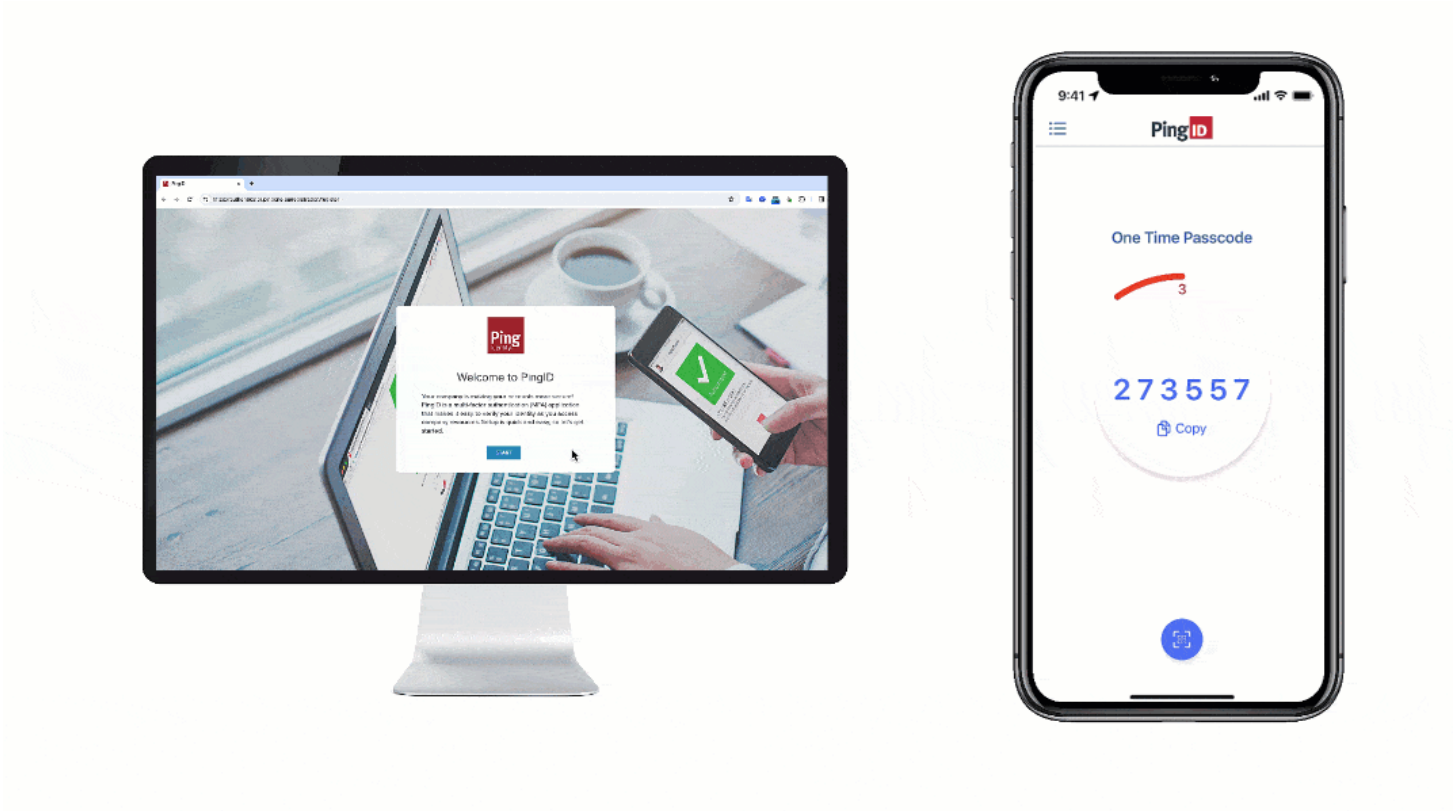
Use the PingID mobile app to view, pair, or remove additional organizations.

Before you begin

Ensure you have installed the PingID mobile app and paired it to your device.

About this task

You can use the PingID mobile app to authenticate to any organization that is paired to the mobile app.



Steps

1. Sign on to the account or service of the new organization.

Result:

The **Authentication** window appears, displaying the QR code and pairing key.

2. Open PingID on your mobile device and tap the **Menu** icon ( ).
3. Tap **Settings**( ).

   You'll see a list of your organizations.
4. To add a new organization:

   1. Click the **Plus**icon ( ).

      Result:

   The **Add Organization** screen opens, showing the QR code scanner.

      1. Scan the QR code or click **Enter Pairing Key** to enter the pairing key manually, and then tap **Pair**.

         Result:

         The organization is added to your **My Organizations** list, and you can use the PingID mobile app to authenticate when accessing your account in that organization.
5. To delete an organization, click the **Delete** icon ( ) next to the organization that you want to delete, and then confirm your choice.

   Result:

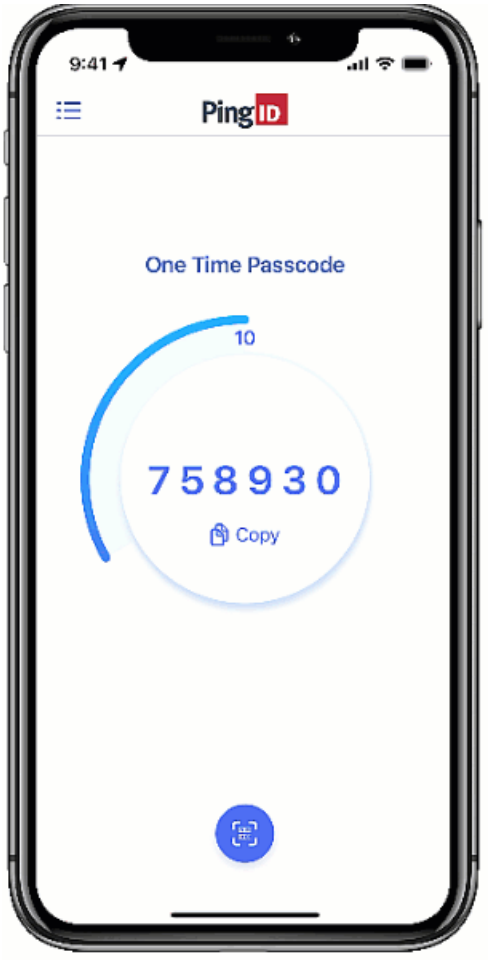
   PingID mobile app is unpaired and you can no longer use it to authenticate to that organization.

Changing your PingID mobile app PIN

If you have to enter a PIN code each time you open or user the PingID mobile app, you can change it from within the app.

About this task

Your PIN code must include at least 3 or 4 different digits for 4 and 6-digit PIN lengths, respectively, and you can't choose digits that are in ascending or descending sequence, such as 1234.



Important

If you forget your PIN, you cannot reset it. You'll need to unpair PingID mobile app and then pair it again.

Steps

1. On your device, open the PingID mobile app.
2. Tap the **Menu** icon ( ), and then tap**Change PIN**( ).
3. Enter your current PIN code, and then enter a new PIN code.

   Result:

   You'll see a message telling you that your PIN is successfully changed, and the next time you open the app or authenticate with PingID, you'll be asked to enter the new PIN.

Reporting fraudulent authentication attempts

If you receive an authentication request that you didn't initiate, you can report it as fraud.

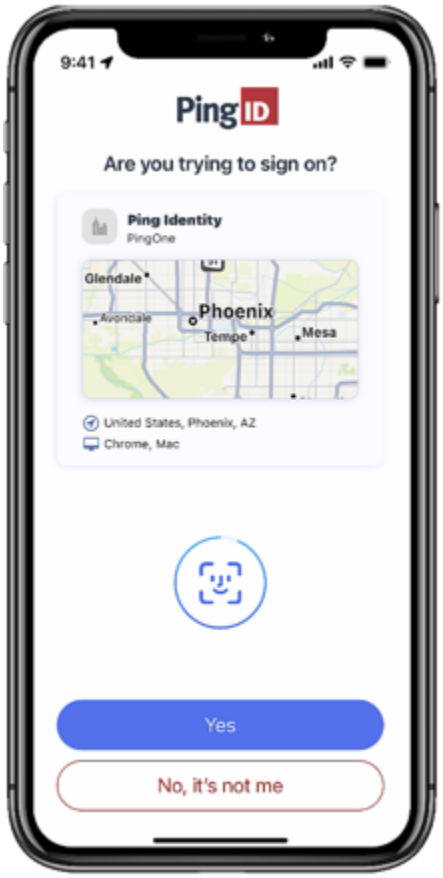
About this task

If you receive an authentication request, but you don't know why, the request could be fraudulent. It is important not approve an authentication request that you did not initiate or one that you did not expect to receive.

If you are in any doubt, you should deny the request and report it as fraudulent using the PingID mobile app.

Steps

1. If you suspect an authentication request is fraudulent, open the PingID mobile app and, when asked to authenticate, tap **No, it's not me**.



> **Tip**
>
> If the authentication request appears on a notification banner, tap any blank space on the notification banner to open the PingID mobile app.

Result:

After you cancel the authentication request, you see the Authentication request **Denied** screen showing the **Report Fraud** button at the bottom of the screen.

image::uyv1707224212437.png[alt="Image of the Authentication request denied screen, showing the Report Fraud button at the bottom of the screen"

2. Tap **Report Fraud**.

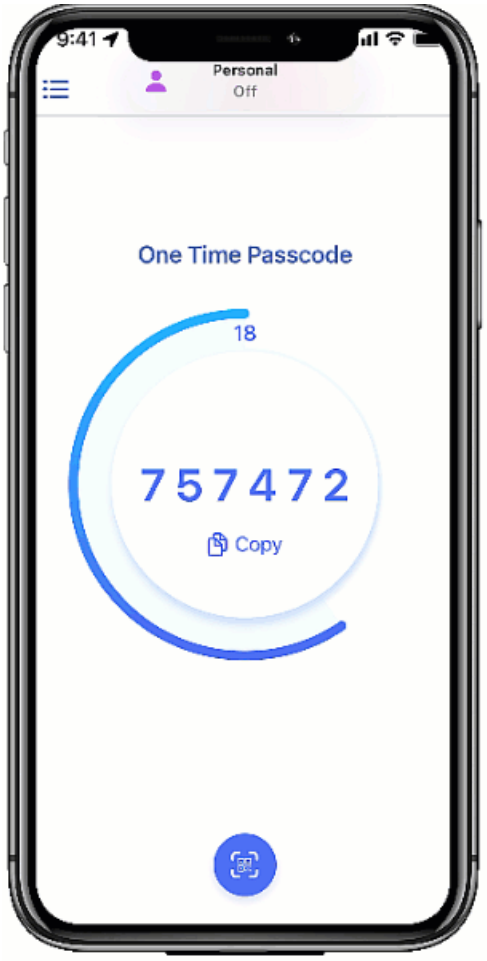
Result:

Details of the authentication request are marked as possible fraud and are logged accordingly.

Disabling push notifications

If you experience slow internet speeds, or prefer to authenticate using a one-time passcode (OTP) only, you can disable push notifications to PingID mobile app.

About this task



Steps

1. Open PingID on your mobile device and tap the Menu icon ( ).
2. Tap **Settings** ( ).

   You'll see a list of your organizations.
3. To disable notifications, tap **Allow Notifications** until the slider turns gray.

Result

The settings are updated immediately. The next time you need to authenticate, enter the latest passcode that appears in the PingID mobile app.

Updating the PingID mobile app

If you enable automatic updates on your mobile device you'll automatically get the latest version of the PingID mobile app. You can also manually download the latest updates to the PingID mobile app by going to your app store.

Steps

1. From your mobile device, go to your app store (for iOS users) or Google Play (for Android users), and search for PingID.

   Result:

   If there is an update available, you'll see the **Update** button. If you only see the **Open** button, this indicates that you are running the latest version and no update is required.

2. If an update is available, tap **Update**.

   Result:

   The progress bar displays and the app store prompts you to open the app when the update is complete.

3. To launch PingID when the update install is complete, tap **Open**.

Sending the event log

Send event logs to customer support.

About this task

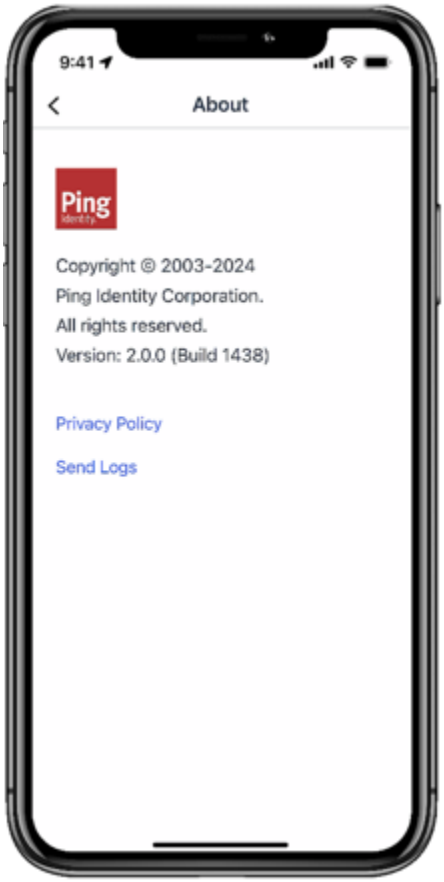
Sending event logs to customer support helps them troubleshoot issues.

Steps

1. In the PingID mobile app, tap the **Menu** icon (), and then tap **About**.

   Result:

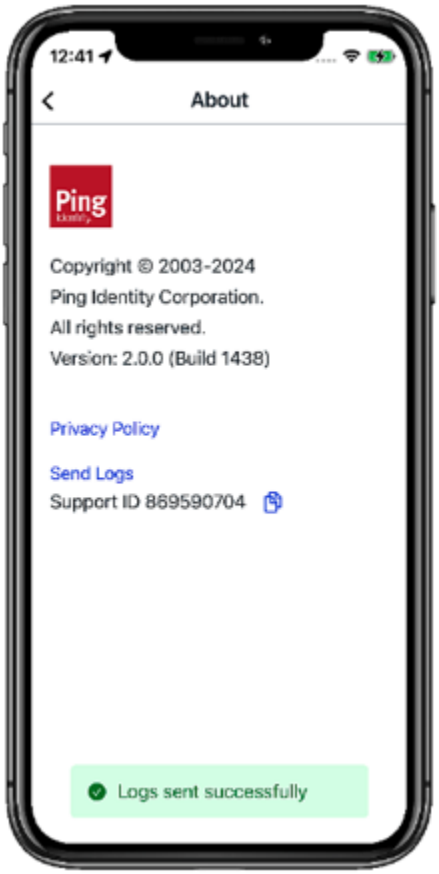
   The **About** screen opens, showing the **Privacy Policy** and **Send Logs** links.



2. Tap the **Send Logs** link.

   Result:

   A confirmation message appears, telling you that the logs have been successfully sent to customer support. The Support ID appears below the **Send Logs** link.



Managing your device settings for Android

Manage your mobile app using recommended device settings.

When installing PingID mobile app, you will be asked to allow to access device settings, such as your device camera. You might also be asked to share your location if required by your organization's policy. The settings requested are needed for PingID mobile app to work correctly.

> **Note**
>
> - We recommend you accept the default settings when installing PingID mobile app.
> - The PingID mobile app uses the language that's defined in your device's mobile OS settings unless it is not one of the supported languages. If the defined language is not supported, the app defaults to English.

For more information, see the following topics:

- Enabling or disabling PingID notification settings for Android
- Enabling mobile app app permissions for Android

Enabling or disabling PingID notification settings for Android

Enable notifications to ensure PingID notifies you when you need to authenticate.

About this task

You can choose to enable notifications from PingID mobile app when the **Do Not Disturb** settings on your mobile device are set to **Priority Only**. If you need to temporarily disable notifications, do so from your PingID mobile app settings.

> **Note**
> These settings apply to Android 6.x and later.

Steps

1. On your Android device, go to **Settings → Notifications**, and then tap **PingID**.
2. If required, select from the following notification options:

Option	Description
Block all	Never show notifications from this app. If selected, you will not be notified when you are required to authenticate. **Note** If selected, you can't choose another option.
Show silently	If selected, your device will not make a sound, vibrate, or peek notifications into view when a notification is received.
On the lock screen	Choose what happens on the lock screen if your device is locked when a notification is received. Tap to select from: ***Show all notification content*** Show all notifications and their content on the lock screen. ***Hide sensitive notification content*** Show a notification has arrived, but hide the content. ***Don't show notifications at all*** Hide all notifications.
Override Do Not Disturb	Select if you want to show PingID mobile app notifications and allow notification interruptions, even when you set your Do Not Disturb settings to **Priority Only**.

Enabling mobile app app permissions for Android

If you didn't enable the relevant permissions when installing PingID mobile app, you can enable them manually from your phone settings.

About this task

We recommend enabling all PingID mobile app permissions. If you accept all pop-up requests when you install PingID mobile app, all PingID mobile app permissions are enabled by default. If you need to enable them at a later date, you can do so through the PingID mobile app settings on your device.

Steps

1. On your Android device, go to **Settings → Apps → PingID → Permissions**.
2. Enable the following permissions:

Option	Description
Camera	Enables PingID mobile app to access your camera so you can pair your device using the QR code.
Location	Enables PingID mobile app to access and incorporate location-based information to enhance security.
Telephone	Enables PingID mobile app to use your phone settings so you can authenticate more securely from your mobile device.

Managing your PingID settings for iPhone

Manage your PingID mobile app using recommended device settings.

When installing PingID mobile app, you will be asked to allow PingID to access device settings, such as your device camera. You might also be asked to share your location if required by your organization's policy. The settings requested are needed for PingID to work correctly. The name and location of settings might vary slightly depending on your version of iOS.

> **Note**
>
> - We recommend that you accept the default settings when installing PingID.
> - The PingID mobile app uses the language that's defined in your device's mobile OS settings unless it is not one of the supported languages. If the defined language is not supported, the app defaults to English.

Enabling PingID notification settings for iPhone

Enable pop-ups and notifications to ensure PingID mobile app notifies you when you need to authenticate.

About this task

You can choose to enable notifications from PingID mobile app even when the Do Not Disturb settings are set to **Priority Only** on your device. If you need to temporarily disable pop-ups, you can do so from your PingID mobile app settings.

Steps

1. On your iOS device, go to **Settings → PingID → Notifications**.
2. To enable notifications, tap **Allow Notifications**.

3. Enable any of the following notification options:

Option	Description
Show in Notification Center	Tap to display all PingID mobile app notifications in the Notification Center.
Sounds	Tap to enable a sound to be heard when a PingID mobile app notification is received.
Badge App Icon	Tap to display a marker on the PingID mobile app icon if it has a notification for you.
Show on Lock Screen	Tap to show a PingID notification on your lock screen, if the screen is locked when the notification is received.
Alert Style When Unlocked	Defines how notifications are displayed when your phone is unlocked. **Banners** is recommended.

Enabling PingID mobile app permissions for iPhone

We recommend enabling all PingID mobile app permissions.

About this task

If you accept all pop-up requests when you install PingID mobile app, all required permissions are enabled by default. If you need to enable them at a later date, you can do so through the PingID mobile app settings on your device.

Steps

1. On your device, go to **Settings → PingID**.

   Result:

   The PingID mobile app settings are shown.

2. Tap the relevant slider to **On** to enable any of the following settings:

Option	Description
Tap Location, then select While Using the App	Enable PingID mobile app to access your location information, to enhance security, and enable you to bypass sign on when in authorized locations if enabled by your organization settings.
Camera	Allow PingID mobile app to access your camera, so you can scan the QR code when pairing your device.
Background App Refresh	Enable PingID mobile app to check for new information in the background in an intelligent and controlled manner.

Option	Description
Cellular Data	Enable PingID mobile app swipe or fingerprint authentication to use your phone data when not connected to a Wi-Fi network.

Enabling time-sensitive notifications in Focus Mode

Make sure you receive push notifications from PingID, even when your device is in Focus Mode.

About this task

Time-sensitive notifications are notifications that need your immediate response - such as those you receive from PingID. To ensure you always receive notifications from PingID even when your device is in focus mode, enable time-sensitive notifications on your iOS device.

Steps

1. On your device, tap **Settings → Focus** and select the relevant Focus Group.
2. Under **Allowed Notifications**, select **Apps**, and toggle **Time Sensitive** to **On**.

Unpairing the PingID mobile app

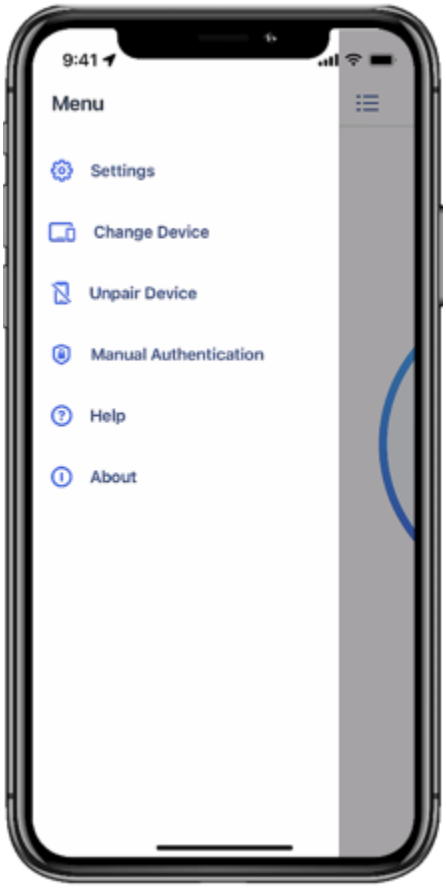
If you no longer use the PingID mobile app to authenticate, you can unpair your device.

Steps

1. Open the PingID app on the device that you want to unpair.

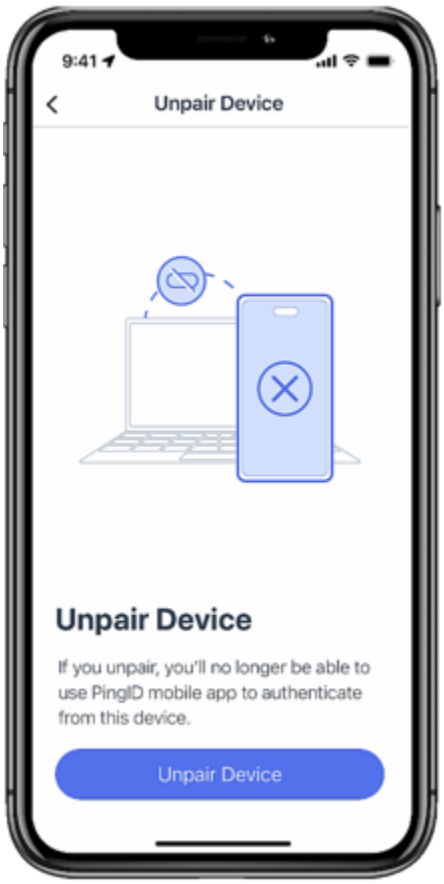
> **Important**
>
> Ensure your device has access and is connected to the internet before unpairing your device.

2. Tap the **Menu** icon ( ) and then tap **Unpair Device**( ).



Result:

You'll see the **Unpair Device** screen, warning you that if you unpair your device, you'll no longer be able to use the app to authenticate from this device.



3. Tap **Unpair Device**.

   Result:

   You'll see a confirmation message.

4. Tap **Unpair** to confirm the request.

Result

The device is unpaired, and you can no longer use it to authenticate.

PingID mobile app management (legacy)

You can manage many of your PingID settings from the PingID mobile app.

This section includes documentation for the previous version of PingID mobile app. For the latest version, see PingID mobile app management.

Use PingID mobile app to:

- Transfer your PingID authentication to a different phone (legacy).
- Pair your device to an additional organization (legacy).
- Enable use of a one-time passcode (OTP) to authenticate rather than swipe or fingerprint (legacy).

- Report authentication attempts that might be fraudulent (legacy).
- Send an event log to customer support (legacy).
- View the PingID mobile app version (legacy).
- Update the PingID mobile app manually (legacy).
- Unpair or uninstall the PingID mobile app (legacy).

You can also manage your phone settings to ensure you're providing the necessary permissions to the PingID mobile app.

> **Note**
>
> PingID mobile app uses the same language as the language defined in your phone mobile OS settings. If it's not one of the supported languages, it displays in English by default.

Transferring PingID mobile app authentication to a different device using a QR code (legacy)

If you are using the PingID mobile app and want to change or upgrade to a new device, transfer PingID authentication from your old device to your new device using a QR code in the PingID mobile app.

About this task

This topic shows you how to transfer PingID mobile app authentication from your old phone to a new one using a QR code.

> **Note**
>
> In some situations, you might not be able to transfer PingID to your new device directly, such as:
>
> - If this feature is disabled by your organization.
> - If you don't have access to your old phone, or do not start the transfer from within the PingID mobile app of your old phone.
> - If you're not planning to use the PingID mobile app on your new device, but want to use a different authentication method, such as the device's built-in biometrics.
> - If your old device is paired to more than one data center.
>
> In these cases, you must manually unpair PingID from your old device and then manually pair PingID with your new device.

If you are unable to access your old device or your device is damaged, lost, or stolen, you can learn more in A lost or stolen device situation.

Steps

1. On your new device, go to the apps store to download and install the PingID mobile app.

   > **Note**
   >
   > If you use the backup and restore feature on your mobile device to move apps to your new device, the PingID application is transferred to your new phone, but the connection to your user account will be lost and you won't be able to authenticate. Therefore, you must download the PingID mobile app to your new phone, and then transfer the PingID service to your new device using the instructions described here.

2. On the device you want to unpair (your "old" device), open the PingID mobile app, tap the **Gear** icon ( ), and then tap **Change Device**.

   > **Note**
   >
   > If your admin has disabled the option, the **Change Device** option will not be visible in the menu.

   Result:

   Your old device displays a QR code and pairing key.

3. On your new device, open the PingID mobile app and scan the QR code or enter the pairing key.

   Result:

   Your new device displays a green **Authenticated** message with a check mark, confirming the pairing of your new device is complete, your old device is unpaired, and your organization is added to PingID.

Result

The next time you sign on to your account or app, you are prompted to authenticate on your new device.

> **Note**
>
> After you transfer PingID authentication to your new device, you are no longer able to authenticate on your old device.

Pairing your mobile device to an additional organization

Using the PingID mobile app, use the same device to authenticate for more than one organization.

Before you begin

Ensure you have downloaded the PingID mobile app and paired it to your device.

About this task

Use the PingID mobile app to:

- Pair your device to an additional organization.
- View the organizations paired with your device.
- Unpair one or more organizations.

Steps

1. Sign on to the account or service of the new organization.

   Result:

   The **Authentication** window appears, displaying the QR code and pairing key.
2. To see your list of organizations, open PingID on your device and go to the **My Organizations** section.
3. To add a new organization, click the **Plus**icon ( ) .

   Result:

   The **Add New Service** screen opens, showing the QR code scanner.
4. Scan the QR code or click **Enter Pairing Key Manually**. Enter the pairing key and then tap **Add Service**.

   Result:

   The organization is added to your **My Organizations** list.
5. When prompted, authenticate on your device.

Result

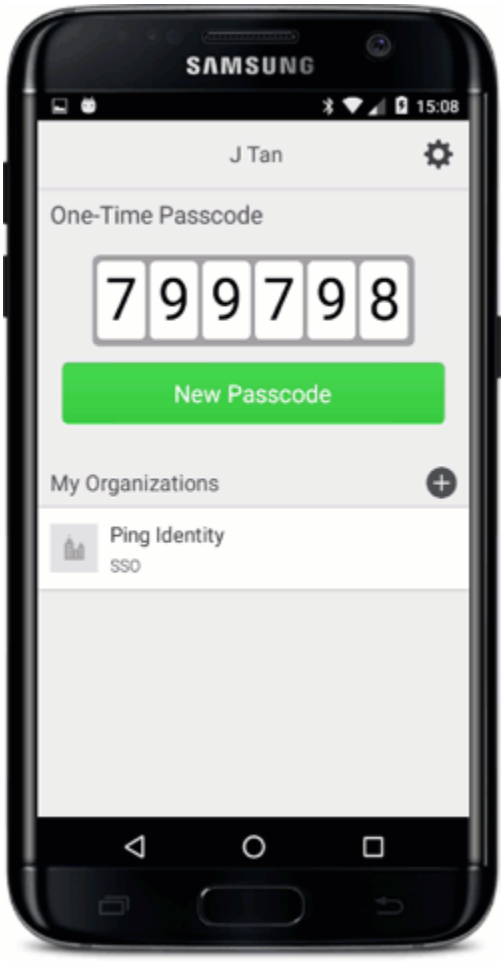
Access services and authenticate to all organizations from your device.

Editing your profile (legacy)

Add your picture to your profile to provide another layer of security for authentication requests.

About this task

Your profile picture appears on all swipe or fingerprint authentication requests. Your profile adds a layer of security by showing that an authentication request is intended for you.

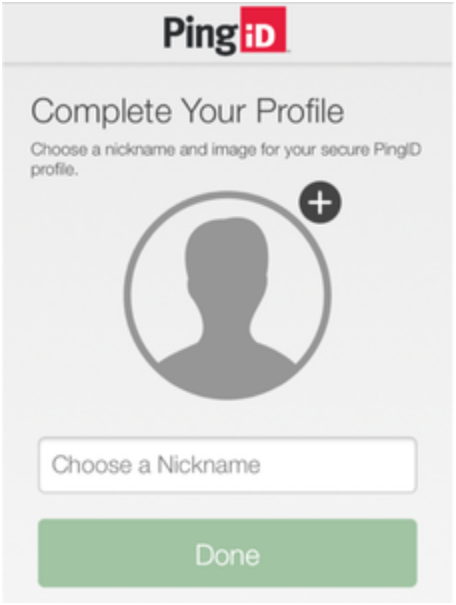


Steps

1. On your device, open the PingID application.
2. Tap the **Gear** icon ( ), and then tap **Edit Profile**.

   Result:

   The **Complete Your Profile** screen opens.



3. To add a profile picture, tap the **Plus** icon ( ), and then tap either:

   Choose from:

   - **Take Photo**: Take a photo with your camera, crop the picture as required, and then tap the check mark to add the photo to your profile.
   - **Choose Existing**: Select the picture you want to use, crop the picture as required, and tap **Done**.

4. Edit your profile name.
5. Tap **Save Changes**.

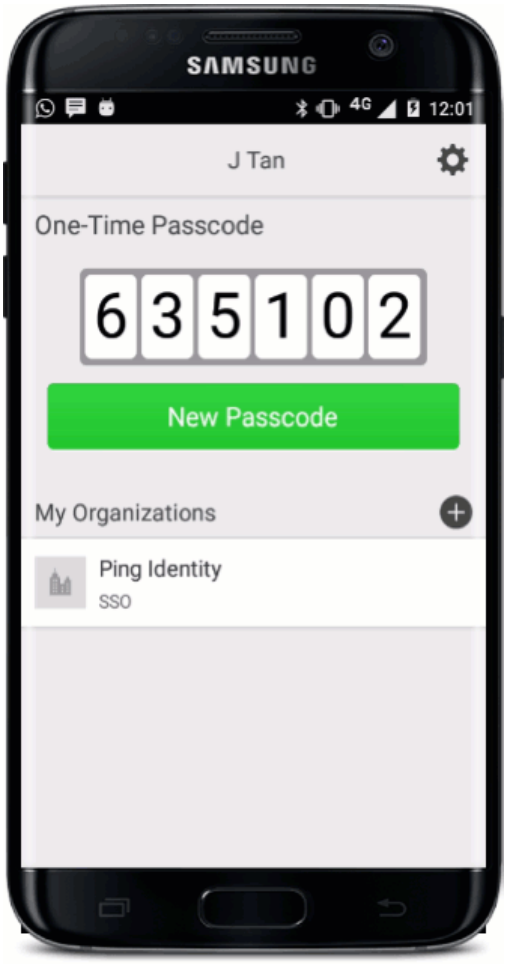
   Result:

   Your profile is updated immediately.

(Legacy) Enabling or disabling swipe and biometrics authentication

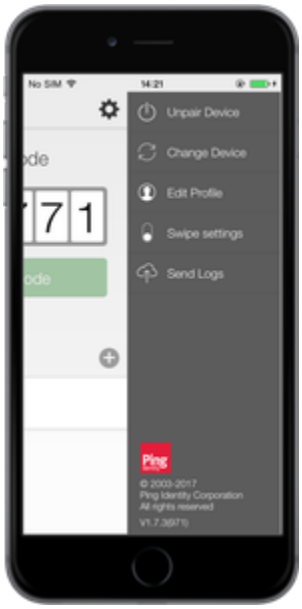
If you experience slow internet speeds, or prefer to authenticate using a one-time passcode (OTP) only, you can disable swipe or biometrics authentication.

About this task



Steps

1. On your device, open the PingID application.



2. Tap the **Gear** icon (), and then select **Swipe settings**.

3. To disable swipe authentication, tap **Enable Swipe** until the slider moves to the left (disabled).

Result

The settings are updated immediately. If swipe is disabled, the next time you are prompted to authenticate, enter the passcode generated on your mobile device by PingID.

Reporting fraudulent authentication attempts (legacy)

If you receive an authentication request that you didn't initiate, you can report it as fraud.

About this task

If you receive an authentication request but you don't know why, the request could be fraudulent. You should deny the request and report it as fraudulent from within the PingIDmobile app.

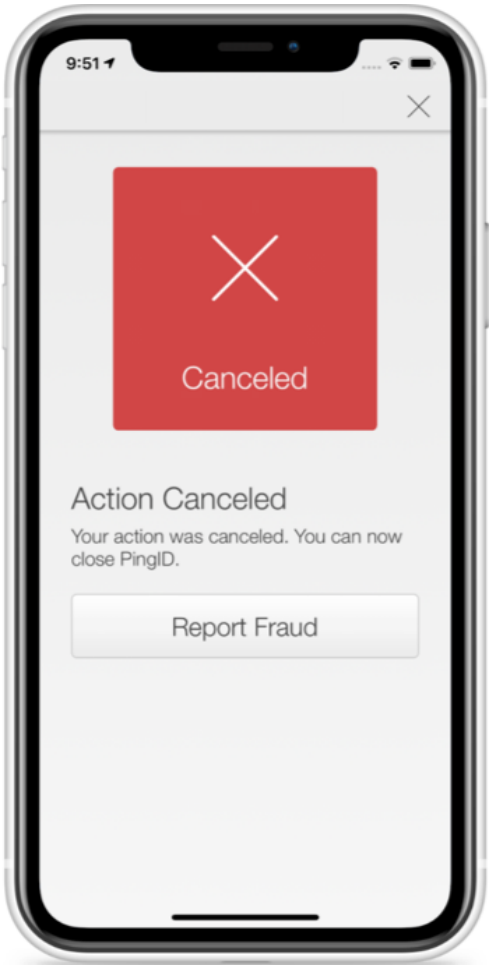
Steps

1. If you suspect an authentication request is fraudulent, open the PingIDmobile app and tap **Cancel**.

   > **Tip**
   >
   > If the authentication request appears on a notification banner, tap any blank space on the notification banner to open the PingIDmobile app.

   Result:

   After you cancel the authentication request, you see the **Authentication request denied** screen with a red X and the **Report Fraud** button at the bottom of the screen.



2. Tap **Report Fraud**.

   Result:

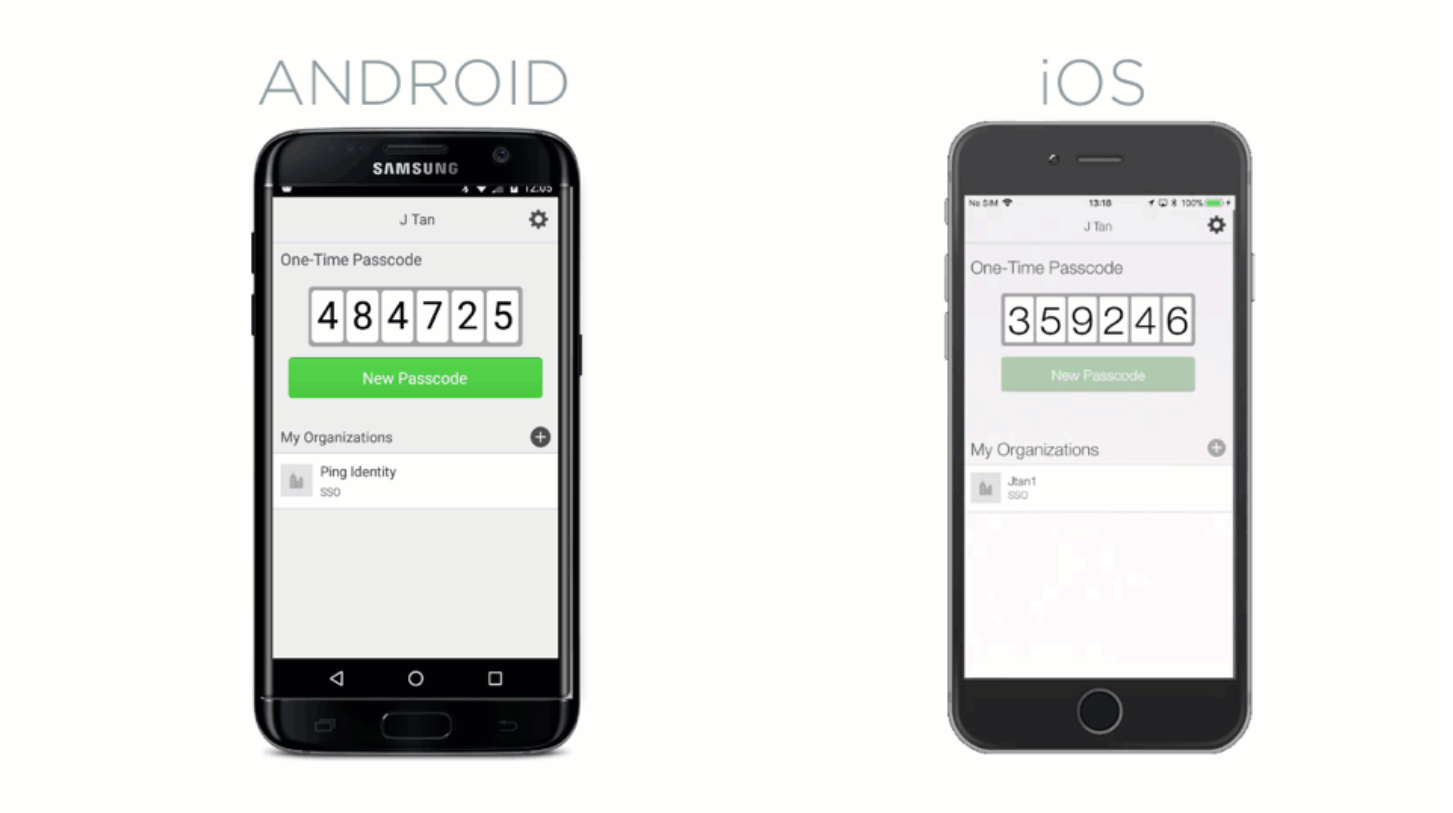
   Details of the authentication request are marked as possible fraud and are logged accordingly.

Sending the event log (legacy)

Send event logs to customer support.

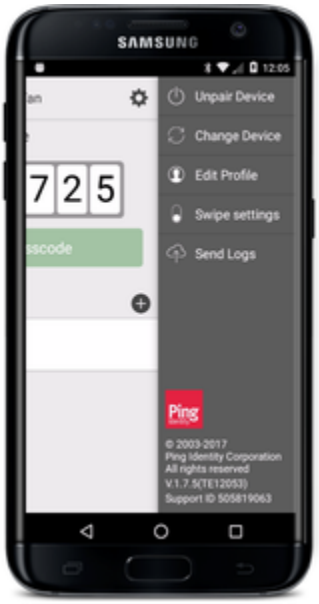
About this task

Sending event logs to customer support helps them troubleshoot issues.



Steps

1. On your mobile device, open the PingID application.
2. Tap the **Gear** icon, and then tap **Send Logs**.



Result:

A confirmation message appears, telling you that the logs have been successfully sent to customer support.

3. If you are asked to supply your PingID support ID, after sending the log file, tap the **Gear** icon .

Result:

The support ID is displayed at the bottom of the PingID mobile app menu.

Viewing the PingID mobile app version (legacy)

View your version of the PingID mobile application.

About this task

Check the version of PingID running on your mobile device.

Steps

1. On your mobile device, open the PingID application.
2. Tap the **Gear** icon.

Result

The version is displayed in the bottom right corner of the screen.

Updating the PingID mobile app (legacy)

If youPingID enable automatic updates on your mobile device you'll automatically get the latest version of the PingID mobile app. You can also manually download the latest updates to the PingID mobilePingID app by going to your app store.

Steps

1. From your mobile device, go to your app store, and search for PingID.

   Result:

   If there is an update available, you'll see the **Update** button. If you only see the **Open** button, this indicates that you are running the latest version and no update is required.

2. If an update is available, tap **Update**.

   Result:

   The progress bar displays and the app store prompts you to open the app when the update is complete.

3. To launch PingID when the update install is complete, tap **Open**.

Unpairing an organization from the PingID mobile app

If your device is paired with more than one organization, use the app to unpair a single organization without unpairing your device completely.

About this task

> **Note**
>
> If you have only a single organization paired to your device and you unpair the organization, your device unpairs automatically.

Steps

1. Open the **PingID** app on your mobile device.

   Result:

   In the **My Organizations** section, a list populates the organizations paired with your device.

2. Tap the organization that you want to remove.

   Result:

   A message showing the name of the organization opens, asking if you want to remove the organization.

3. Tap **Remove Organization**.

   Result:

   The organization is removed, and you cannot use your device to authenticate the account associated with that organization.

Unpairing the PingID mobile app (legacy)

To no longer use your mobile device to authenticate using the PingID mobile app, unpair your device.

About this task

On your mobile device, unpair your device from the PingID app.

Steps

1. Open the **PingID** app on the device that you want to unpair.

   Ensure your device has access and is connected to the internet before unpairing your device.

2. Tap the **Gear** icon in the top right corner of the app.

   Result:

   The PingID authentication screen moves left to reveal the PingID mobile app menu.

3. In the menu, tap **Unpair Device**.

   Result:

   A message appears asking you to confirm your request to unpair your device from the PingID app.

4. Confirm or cancel your changes:

   Choose from:

   - To confirm your changes, tap **Unpair**.
   - To stop your unpairing request, tap **Cancel**.

5. Tap **Unpair**. Tap **Ok**.

Result:

The device is unpaired, and you cannot use it to authenticate.

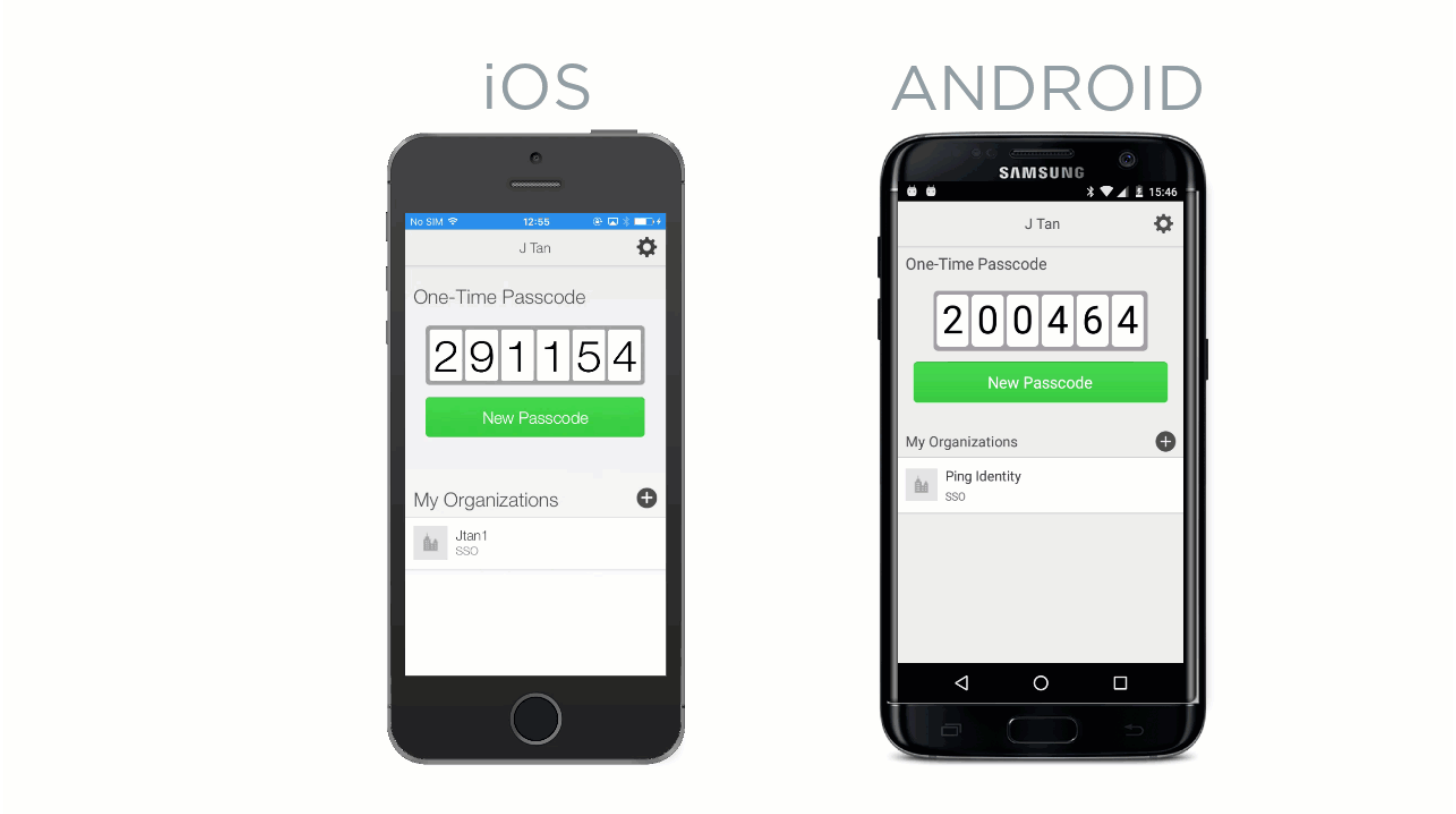
Uninstalling the PingIDmobile app (legacy)

Uninstall the PingID mobile app from a single device.

About this task

If you want to keep the PingID mobile app after you uninstall it from one device, you can transfer PingID to a different device in one simple procedure. For more information, see Transferring PingID mobile app to a different device using a QR code.

> **Note**
>
> After uninstalling the mobile app, the device remains paired to the PingID server but cannot be used. Administrators can unpair the device from the PingID server.



Steps

1. Unpair the PingID app from all organizations.

> **Caution**
>
> If you do not unpair the app before uninstalling, you might experience problems pairing other devices. Contact your helpdesk for support.

2. Uninstall the PingID app on an Android or iOS device:

   Choose from:

   - Android:

     1. On your device, press and hold the **PingID** application icon and then drag it to the **Uninstall** icon at the top right hand corner of your screen.

   - iOS:

     1. On your device, press and hold the **PingID** application icon until all icons appear with an **x** on the top left.
     2. On the PingID app, tap **x**.
     3. Tap **Delete** to confirm your request.

3. Click **Delete**.

   Result:

   The PingID app is deleted and all associated data is removed.

Managing your device settings

Manage your mobile app using recommended device settings.

When installingPingID mobile app, you will be asked to allow to access device settings, such as your device camera. You might also be asked to share your location if required by your organization's policy. The settings requested are needed for to work correctly. The name and location of settings might vary slightly depending on your device and OS version.

> **Note**
>
> - The mobile app uses the same language as that defined in your device's mobile OS settings unless it is not one of the supported languages. If the defined language is not supported, the app defaults to English.

We recommend you accept the default settings when installing PingID mobile app. However if you need to enable or change a setting, see the relevant section:

- Managing your PingID settings for iPhone
- Managing your device settings for Android

PingID desktop app management

You can manage many of your PingID settings from within the PingID desktop app.

Use the PingID desktop app to:

- Pair your desktop app to an additional organization.

- Update the PingID desktop app manually or automatically:
  - On a Mac
  - On a Windows machine.
- Change or reset your desktop app PIN code (if your organization enforces the use of a PIN code).
- Manage user profiles
- Disable your proxy for PingID desktop app.
- Send an event log to customer support.
- Unpair PingID desktop app.

> **Note**
>
> You can download the PingID desktop app from the pingid} download page.

Pairing the desktop app to an additional organization

Use a single device to authenticate against more than one organization, using the PingID desktop app.

Before you begin

Download the PingID desktop application and pair it to your device.

About this task

Use the application to:

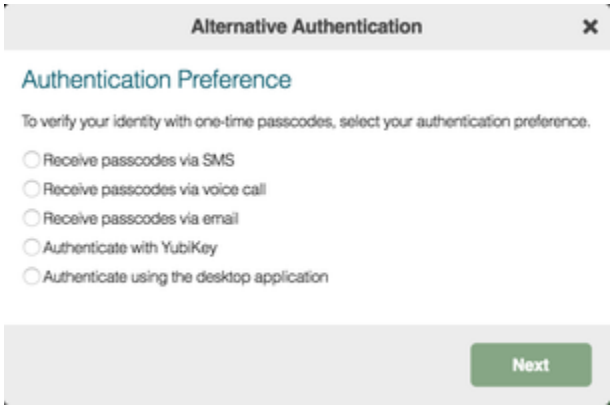
- Pair your device to an additional organization.
- View the organizations paired with your device.
- Unpair one or more organizations.

Steps

1. Sign on to the account (service) of the new organization.

   Result:

   The registration window displays.
2. Click **I want to use a different authentication method**.
3. In the **Alternative Authentication** window, select **Authenticate using the desktop application**, and then click **Next**.



Result:

The **Desktop Setup** window shows the pairing key that you need in step 5.

4. Open the **PingID** desktop application and click the **Gear** icon.
5. On the **Registration** window, copy the pairing key and paste it into the **Pairing Key** field.
    1. To add the pairing key, click the **Plus** icon.

        Result:

        The organization is added to the **My Organizations** list.
6. Click the **Back** icon.
    1. Copy the passcode.
    2. When prompted to authenticate, enter the passcode into your organization's **Authentication** window.

Result

You can access services and authenticate to all of your organizations from the desktop application.

Managing the PingID desktop app on a Mac

Updating the desktop app on a Mac

Keep PingID desktop up-to-date to ensure you have access to the latest features, security features, and fixes.

About this task

When you launch the desktop app it checks if there's a new version available of the software. If you enable the automatic update feature, your app updates automatically. If you do not enable the automatic update feature, you can check for updates manually, be notified when an update is available, and decide when to download and install the update.

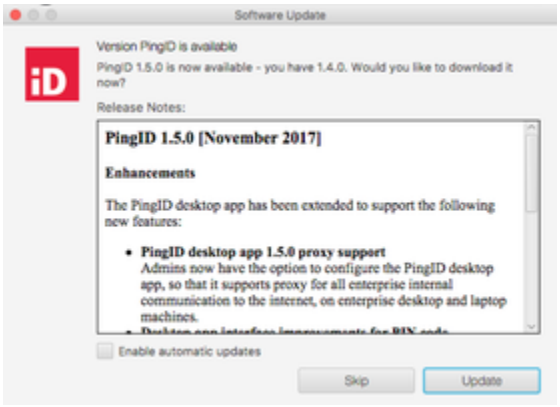
> **Note**
>
> If your organization's policy allows it, you can choose for updates to install manually or automatically. If your organization does not allow you to choose, this menu option is disabled and is not visible to you.

Steps

1. To check for updates in the menu bar, go to **PingID → Check for Updates...**.

   Result:

   A progress bar displays. If an update is available, the **Software Update** window shows you the software version number and the release notes detailing any changes and new features.



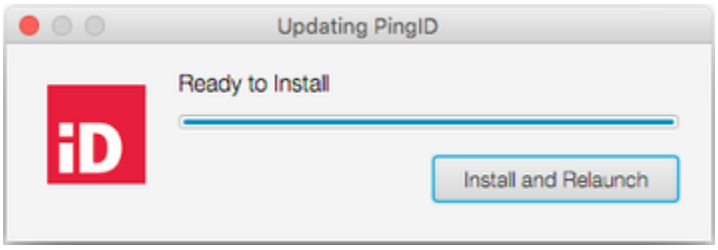
2. Select an update option:

   Choose from:

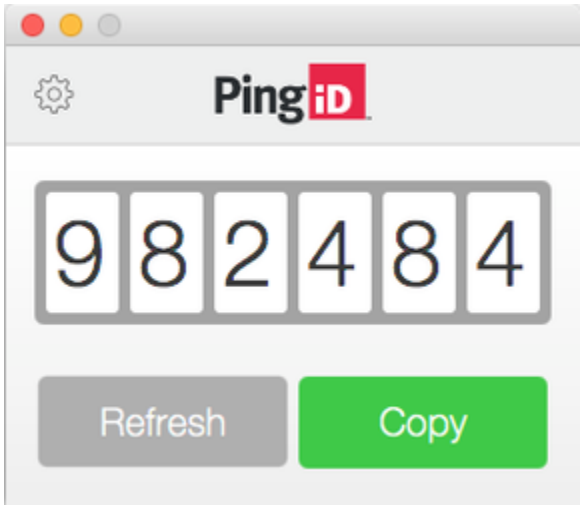
   - **Update**: To start downloading and installing the update.
   - **Skip**: To skip the update.
   - **Enable automatic updates** (optional): Select the check box to automatically check for updates in the future.

   > **Note**
   >
   > If enabled, when an update is available, it downloads automatically and proceeds to the **Install and Relaunch** window described in the following step.

3. After the update downloads, click **Install and Relaunch**.



4. Enter the password to your computer if prompted to do so.



> **Important**
>
> Depending on the changes to your company security policy, you might be required to create a PIN code after a desktop app update and then enter it each time you access the app to secure your desktop app.

Result

When the update is complete, the old PingID desktop app version closes and the updated version of the app opens automatically.

Enabling or disabling automatic updates on a Mac

Enable or disable automatic updates that activate whenever you open PingID using a Mac.

About this task

Whenever you launch the PingID desktop application, it checks if there's a new version of the software available. If automatic updates are enabled, your app is automatically updated as soon as a new version of the software becomes available.

Steps

- Launch the **PingID** desktop app.

  Choose from:

  - To enable automatic updates, from the **Menu** bar, go to **PingID → Automatic Updates** and select the **Automatic Updates** check box.

    For changes to take effect, you must close and restart the desktop application.

  - To disable automatic updates, from the **Menu** bar, go to **PingID → Automatic Updates** and clear the **Automatic Updates** check box.

  The check mark next to **Automatic Updates** is removed, and PingID is no longer updated automatically.

Uninstalling the desktop app on a Mac

Uninstall the PingID desktop application using a Mac computer.

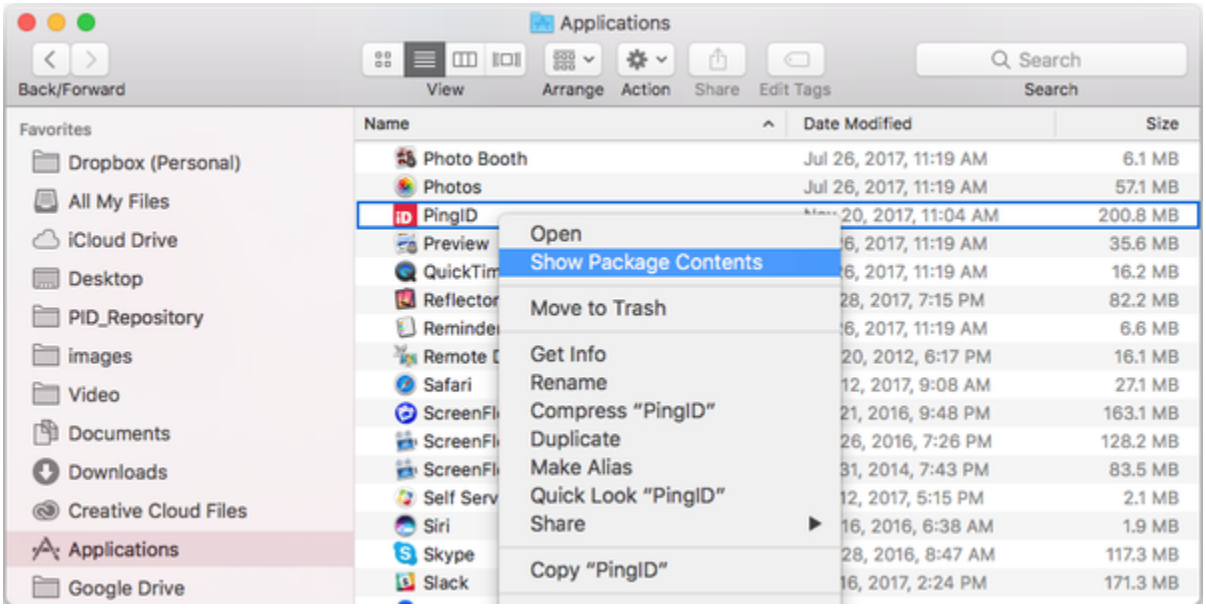
Before you begin

You must unpair your account from the desktop app before uninstalling the app from your Mac. For more information, see Unpairing the desktop app.

About this task

Steps

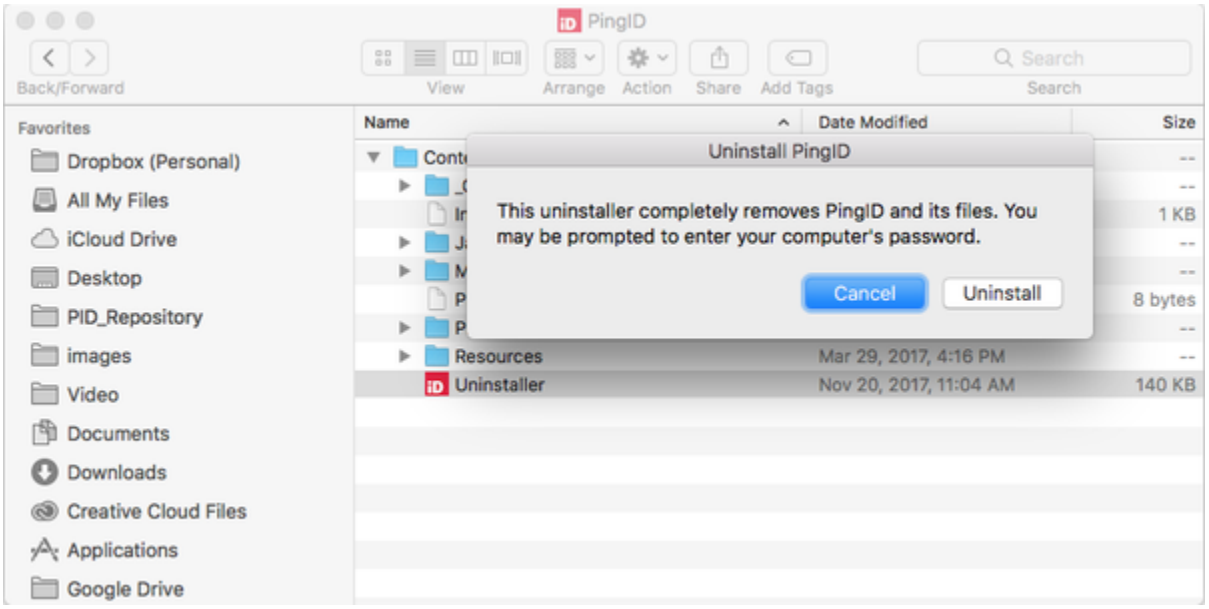
1. On your Mac, open **Finder** and in the **Applications** folder right-click **PingID**.
   - Click **Show Package Contents**.



2. From the **Contents** folder, select **Uninstaller**.

   Result:

   A confirmation message is displayed.



3. Click **Uninstall**, and enter your computer password if prompted.

Result:

The app is uninstalled, and all PingID desktop files are removed from your Mac.

Managing the PingID desktop app on Windows

Manage operations for the PingID desktop application on a Windows machine.

Updating the desktop app on Windows

Update the PingID desktop application on a Windows machine.

Before you begin

You must have administrator privileges to install PingID desktop updates on your Windows machine.

About this task

Keep the PingID desktop application updated to ensure you have access to the latest updates, security features, and fixes. When you launch the desktop application, it checks if there's a new version of the software available. If automatic updates are enabled, your application is updated automatically. If automatic updates are not enabled, you can check for updates manually, or you will be notified that an update is available when you want to download and install the update.

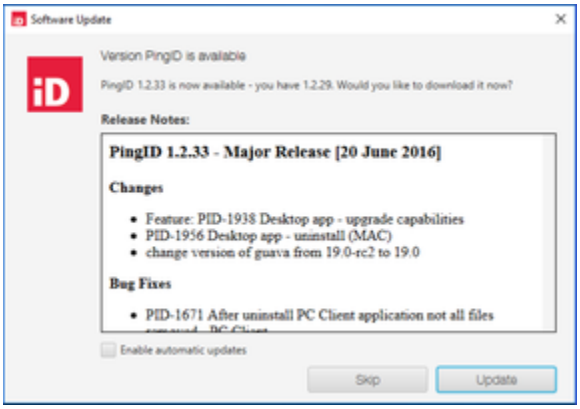
> **Note**
>
> If your organization's policy allows it, you can choose whether updates are installed manually or automatically, otherwise the option is disabled and will not be visible to you. To activate automatic updates, launch the desktop application, and go to **Help → Automatic Updates**.

Steps

1. Launch the **PingID** desktop application.

   The application automatically checks for updates.

2. To manually check for updates, go to **Menu → Help → Check for Updates...**



Result:

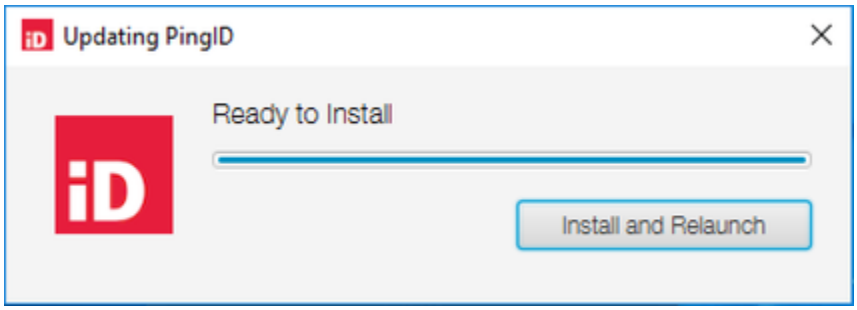
If an update is available, the **Software Update** window shows you the software version number and the release notes, describing details of changes and new features.

3. From the **Software Update** window, select from the following options.

   Choose from:

   - **Update**: Download the update
   - **Skip**: Skip the update
   - **Enable automatic updates** (optional): Select to automatically scan for updates in the future. When an update is available, it is downloaded automatically and proceeds to the **Install and Relaunch** window.

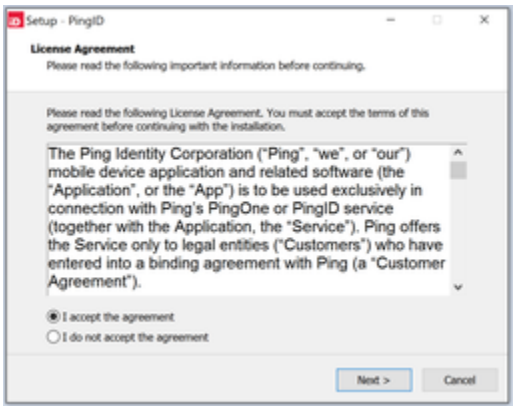
4. Once the update is downloaded, click **Install and Relaunch**.



Result:

The old version of PingID desktop app closes, and the PingID setup wizard opens.

5. In the **License Agreement** window, select **I accept the agreement** and click **Next**.



Result:

A bar displays the installation progress. When the installation is complete, the desktop application reopens automatically, showing the current one-time passcode.

> **Important**
>
> After a desktop application update, you might be required to create a PIN code to secure your desktop application and then enter it each time you access the application.

Enabling or disabling automatic updates on Windows

Enable or disable automatic updates on your Windows machine to determine whether PingID automatically updates to newer versions.

About this task

Whenever you launch the PingID desktop application, the application automatically checks to see if there's a new version of the software available. If you enable automatic updates, then your application is automatically updated as soon as a new version of the software becomes available.

Steps

1. Launch the **PingID** desktop application.
2. Go to **Help → Automatic Updates**.

   Choose from:

   - To enable automatic updates, select the **Automatic Updates** check box.
   - To disable automatic updates, clear the **Automatic Updates** check box.

Uninstalling the desktop app on Windows

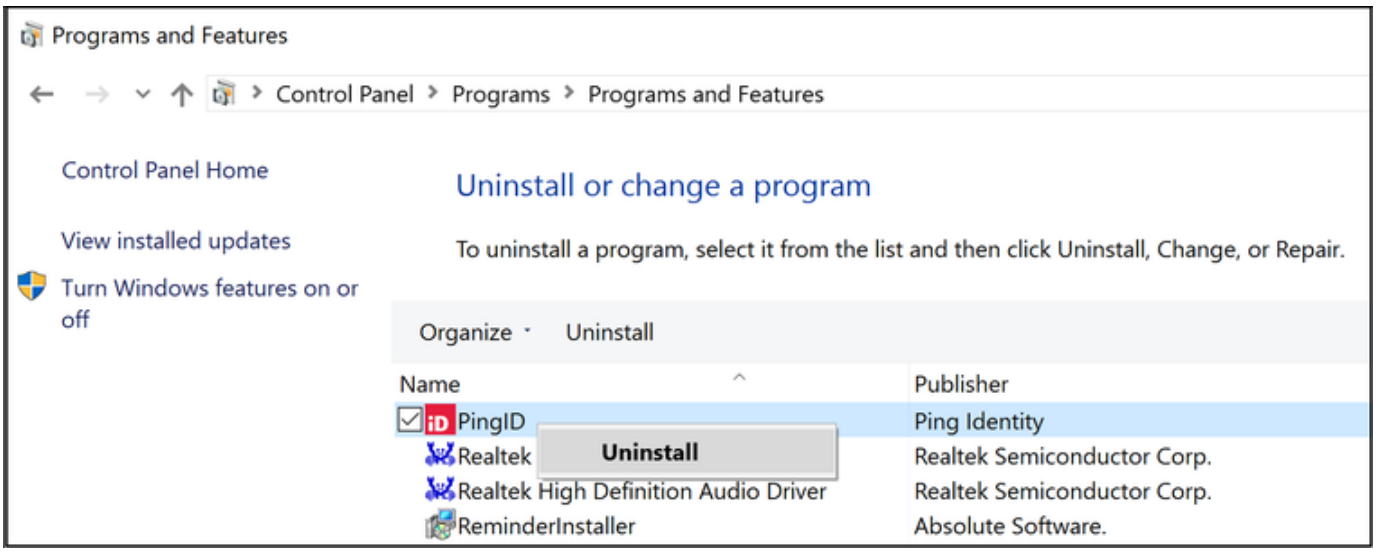
Uninstall the PingID desktop application on a Windows machine.

Before you begin

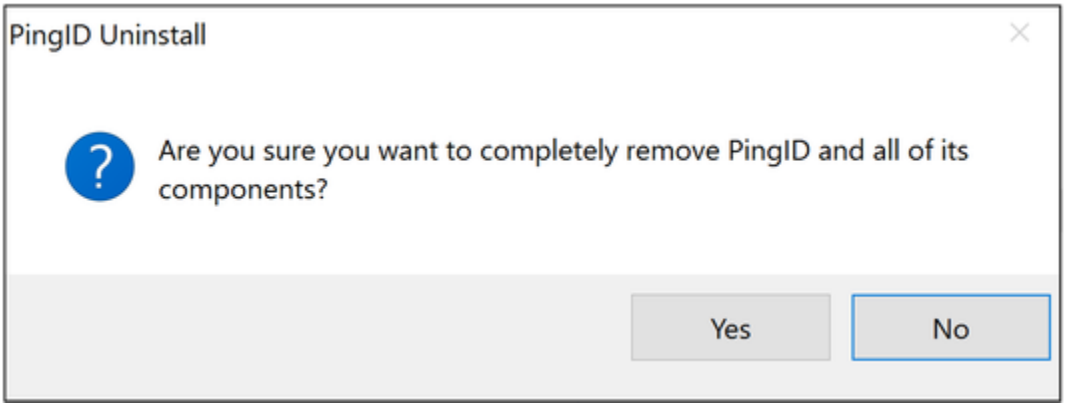
You must unpair your account from the PingID desktop application before uninstalling the application from your Windows machine. For more information, see Unpairing the desktop app.

Steps

1. Go to **Control Panel → Programs → Programs and Features**.
2. Select the **PingID** check box, and then click **Uninstall**.



3. To confirm your selection., click **Yes**.



Result

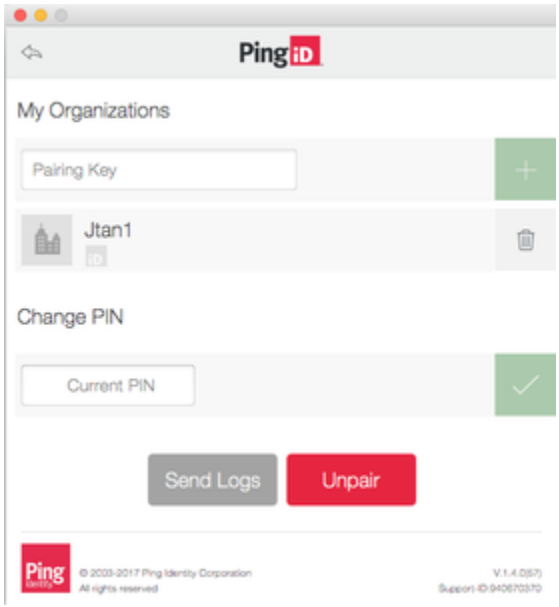
A progress bar displays as PingID begins uninstalling. When the uninstall is complete, a confirmation message will display saying that PingID was successfully removed from your computer.

Changing your desktop PIN code

Change your PIN code from the PingID desktop application.

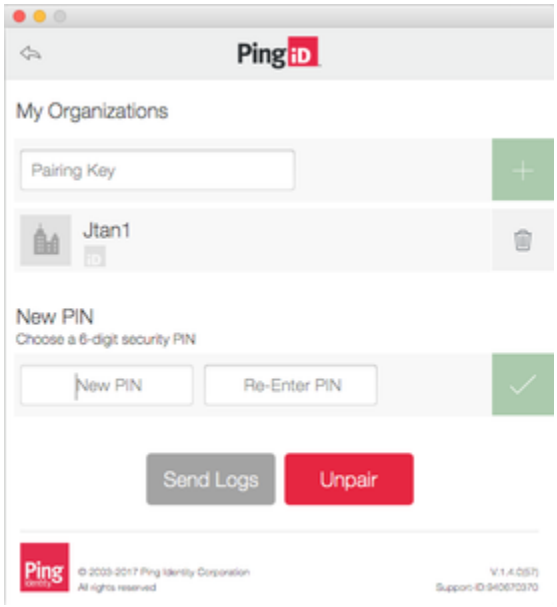
Steps

1. Launch the PingID desktop app and click the **Gear** icon..



1. In the **Change PIN** field, enter your current PIN. Click the green check mark.
2. In the **New PIN** field, enter your new PIN and re-enter it in the second field. Click the green check mark.

> **Note**
>
> The PIN code should include at least 3 or 4 different digits, depending on the PIN length, and consecutive numbers must not be in an ascending (such as 1234) or descending (such as 4321) sequence.



Result

The PingID PIN number is changed.

Managing PingID desktop app profiles

Use multiple user profiles to pair PingID desktop app to various accounts and generate OTPs separately for each account. User profiles also enable PingID desktop app to store desktop app settings and preferences per profile.

You can add or delete one or more user profiles in your PingID Desktop app instance.

To create a user profile:

1. Launch PingID desktop app and then click .
2. Enter a name for the profile, and then click **Create**.

   The Desktop app shows the name of the profile and the **Pairing Key** field. You can then pair the profile to your account. Learn more in Pairing your PingID desktop app.

To rename a user profile:

1. In PingID desktop app, select the profile you want to rename and enter a PIN code if required.
2. Click the settings icon and, in the **Profile Name** field, update the name, and then click the green checkmark.

> **Note**
>
> If the current profile is locked with a PIN code you do not need to know the code to switch to a different profile.

To switch to a different profile:

- In the PingID desktop app menu, click **PingID > Profiles**, and select your profile.

> **Note**
>
> Deleting your user profile doesn't unpair PingID desktop app from your account. You'll also need to unpair the device separately. Learn more in Unpairing the desktop app.

To delete a user profile:

1. On PingID desktop app, click  , and then select the user profile that you want to delete.
2. Click **PingID > Profiles > Delete current profile**.

   The user profile is deleted and the **Profiles** page displays all other profiles.

Resetting your desktop app PIN code

Details of what to do if you forget the PIN code that you use with your PingID desktop app.

About this task

If you've forgotten the PIN code you use to access the desktop app, you'll need to contact your organization's support representative and ask them to unpair the desktop app. You'll need to uninstall the app, and then pair it again. You can create a new PIN code during the pairing process.

Steps

1. Uninstall PingID desktop app.
2. Contact your organization's support representative and ask them to unpair the desktop app.
3. Install PingID desktop app again, and pair it with your account. During the pairing process follow the instructions to create a new PIN code.

Unpairing an organization from PingID desktop app

If your device is paired with more than one organization, use the application to unpair a single organization without unpairing your device completely.

About this task

> **Note**
>
> If you have only a single organization paired to your device and then you unpair the organization, your device is automatically unpaired. If this is the only device paired with your account, you must register a new PingID device to access your account again.

Steps

1. Open the PingID desktop application and click the **Gear** icon.

   Result:

   In the **My Organizations** section, you'll see a list of the organizations paired with your device.

2. For the organization you want to remove, click the **Delete** icon.
3. To confirm your selection, click **Remove**.

Result

The organization is removed and you can't use your device to authenticate when accessing the account associated with that organization anymore.

Enabling or disabling your proxy for PingID desktop

If your admin has run the script that enables proxy use for the PingID desktop app, you can use a menu option to disable proxy use or re-enable it. These menu options are visible only if the admin has run the proxy enablement script.

About this task

Some organizations use a proxy to communicate between the PingID desktop application configured on enterprise desktops and laptops and the PingID server. If this is the case in your organization, you must ensure your proxy is enabled. You might need to disable your proxy sometimes, for example, if you're signing on to PingID from outside your company network.

> **Note**
>
> If you see the error 'no network connection' when you launch the desktop application, there might be a problem with your proxy. Contact customer support for further assistance.

Steps

1. To enable or disable communication by proxy, open the PingID application menu.

   Choose from:

   - Mac: click **PingID**, and then select or clear **Proxy**.
   - Windows: click **Help**, and then select or clear **Proxy**.

2. Sign on to your account and enter the PingID passcode when prompted.

Unpairing the desktop app

Unpair the PingID desktop application from your machine.

About this task

To unpair your desktop application, complete the following processes:

1. Unpair the local desktop app on your machine.
2. Unpair the desktop app service linked to your account.

Important

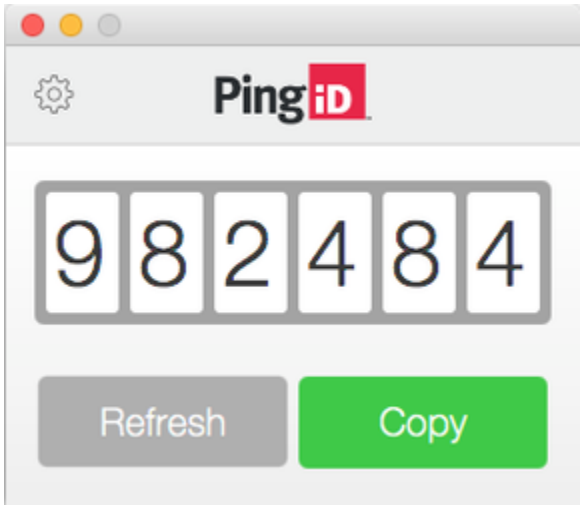
If you unpair while online (connected to the internet), steps 1 and 2 are done at the same time. If you are offline, you need to unpair the desktop application service separately. If you have more than one device paired to your account, you can do this from your **Devices** page, otherwise contact your customer support, who will do it for you.

Note

If you have more than one organization paired to the desktop application and you want to unpair a single organization, see Unpairing an organization from PingID desktop app.

Steps

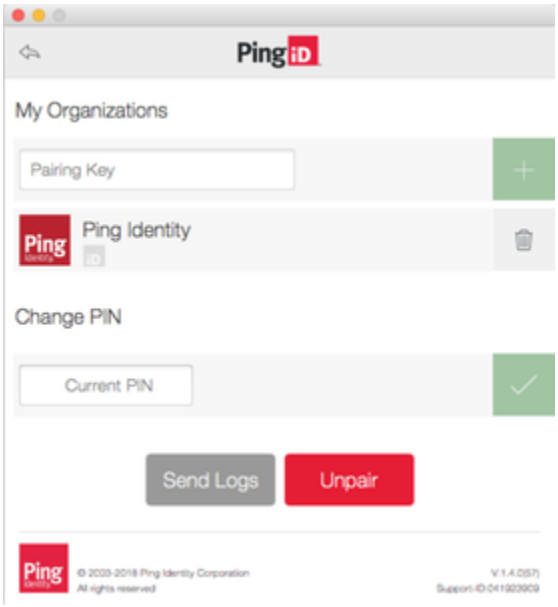
1. Open the desktop application and, if prompted, enter your PIN.



Note

If you forget your PIN code, see Resetting your desktop app PIN code.

2. Click the **Gear**( ) icon.



Result:

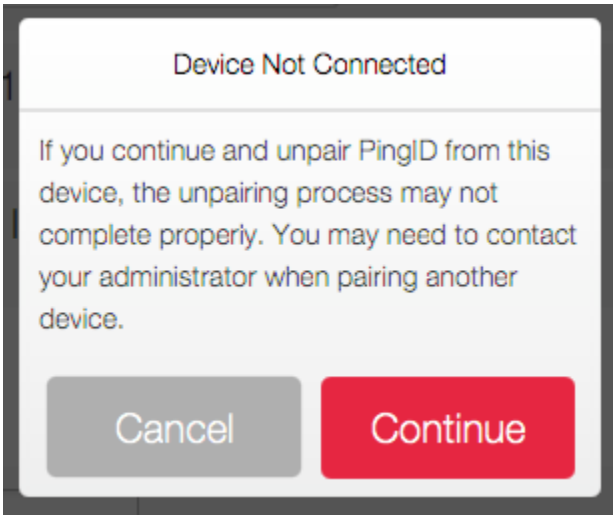
A list of the organizations paired with the desktop app displays.

3. Click **Unpair**.
4. To confirm your selection, click **Unpair**.

   Result:

   If your machine is online, all organizations associated with your account are unpaired and the process is complete.

   If your machine is offline, the following message is displayed, and you need to complete the next step to complete the unpairing process.



5. If you are unpairing the desktop application while offline, choose from the following options:

   Choose from:

   - If you are able to connect to the network, or access a WiFi connection, click **Cancel**, connect, and then start the unpairing process again.

- If you have more than one device paired with your account, go to your **Devices** page and unpair the PingID desktop service. For more information, see Unpairing a device.
- If you do not have more than one device paired with your account, contact customer support to unpair the desktop application from your list of paired PingID devices.

Sending log information

Send PingID desktop application event logs to customer support for troubleshooting.

About this task

You might have to send PingID desktop application event logs to your customer support team to assist them in troubleshooting issues.

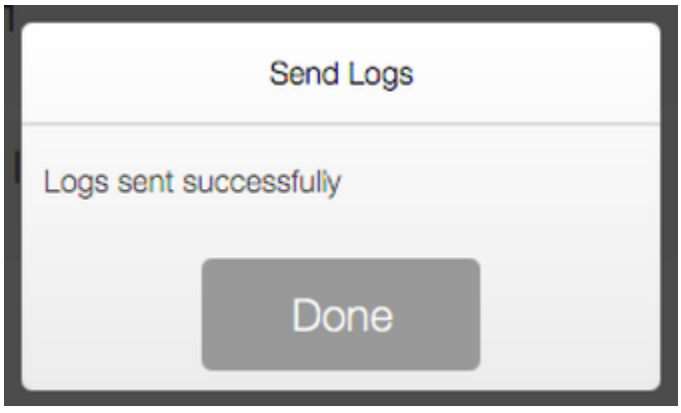
> **Important**
>
> If you unpair your device, all log information is deleted.

Steps

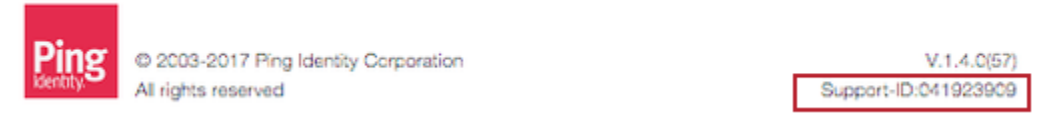
1. Launch the PingID desktop application and enter your PIN code if required.
2. Click the **Gear** icon.
3. Click **Send Logs**.

   Result:

   A confirmation message shows the logs have been sent successfully.



> **Note**
>
> If you are asked for your PingID Support ID, it's in the lower right corner of the PingID desktop application after you send the log file.



Choosing a different device for authentication (Web/Windows)

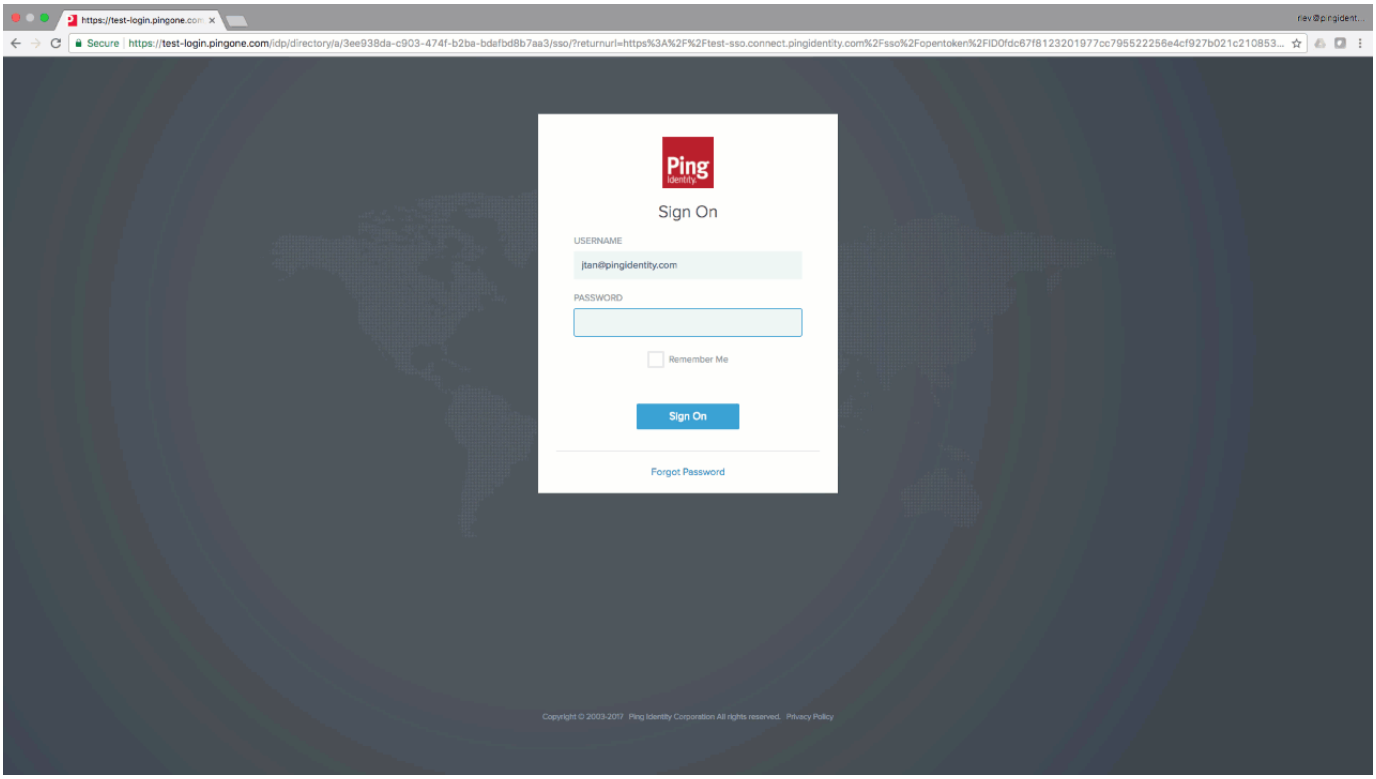
About this task

If you have more than one device paired with your account, you can choose a different device to use to authenticate.

> **Note**
>
> The ability to pair more than one type of device and the type of device you can use to authenticate is defined by your organization.

Steps

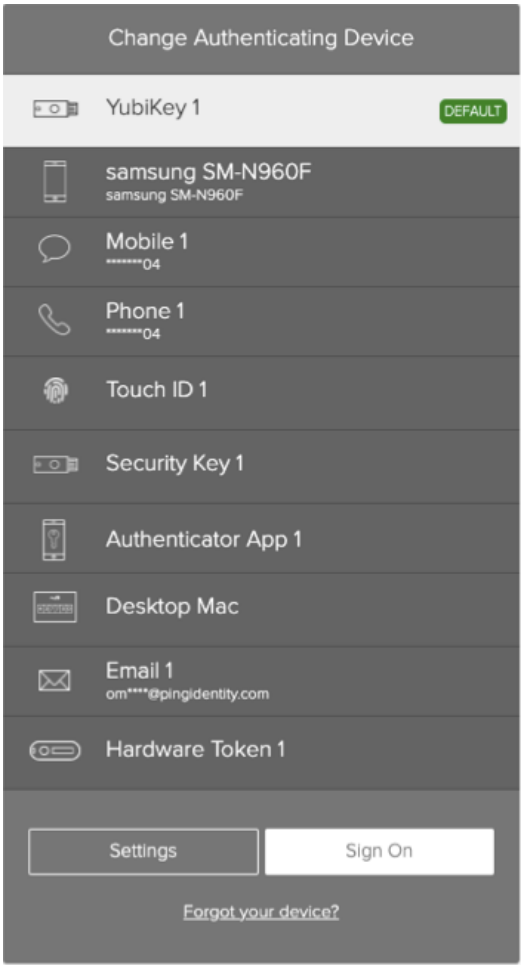
1. Start a multi-factor authentication (MFA) process.



Result:

If your organization's configuration is set to **Prompt User to Select**, the **Change Authenticating Device** window appears with a list of all your available devices. Otherwise, you will see the authentication page and will be able to click the **Change Device** option, in order to get to the **Change Authenticating Device** window with a list of all your available devices.

2. In the **Change Authenticating Device** window, from the list of available devices, select the device you want to use. Select **Sign On**.



Result:

You are prompted to authenticate through the method you selected.

Choosing a different device for authenticating (VPN)

About this task

If you have more than one device paired with your account, choose the device you want to use to authenticate.

> **Note**
>
> The ability to pair more than one type of device, and the type of device you can use to authenticate is defined by your organization.

Steps

1. Sign on to your VPN.
    1. In a web browser, enter your VPN sign on URL.
    2. Enter your username and password.

       If you have more than one device, a message appears detailing each device in a numbered list.

3. For multiple devices only: Enter the number of the device you want to use to authenticate.
4. Click **Sign In**.

   Result:

   A message appears requesting that you authenticate, and an authentication notification is sent to your device.

2. Authenticate using your selected device.

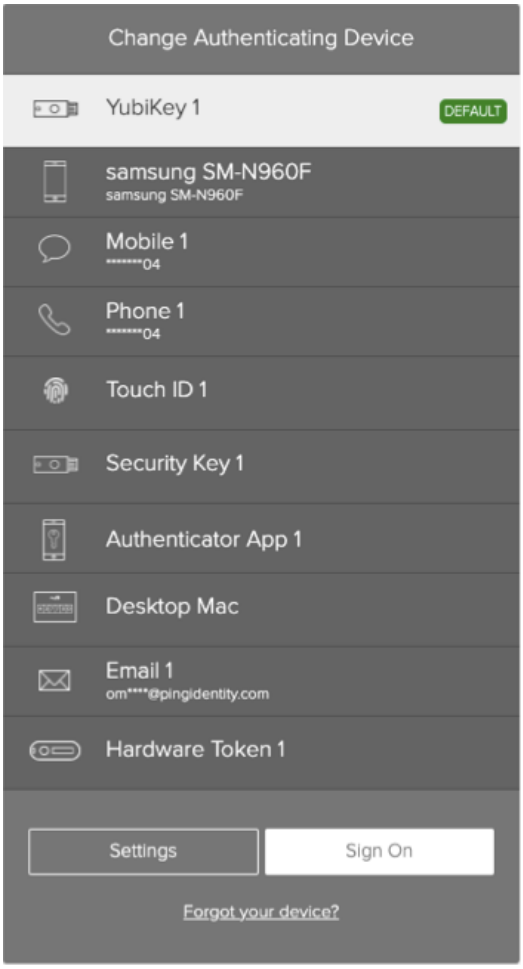
   The authentication can be a request for swipe, fingerprint authentication, or a passcode, depending on your device.

3. Click **Sign In**.

Renaming a device

About this task

If you have more than one device paired with your account, rename each device so that you can more easily identify it in the list of devices that appear when you authenticate. You can change the name of any device that appears in the list from your **Devices** page.



Steps

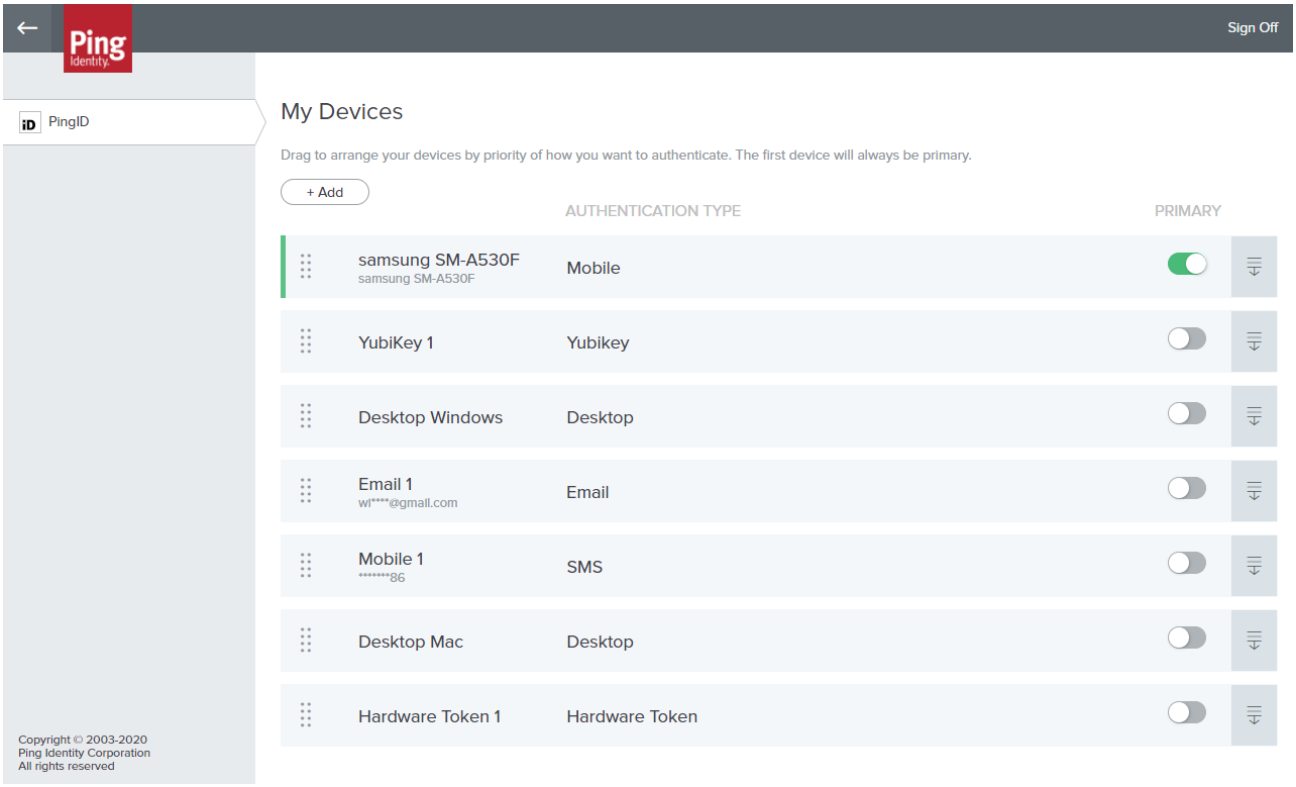
1. Access the **Devices** page either:

   Choose from:

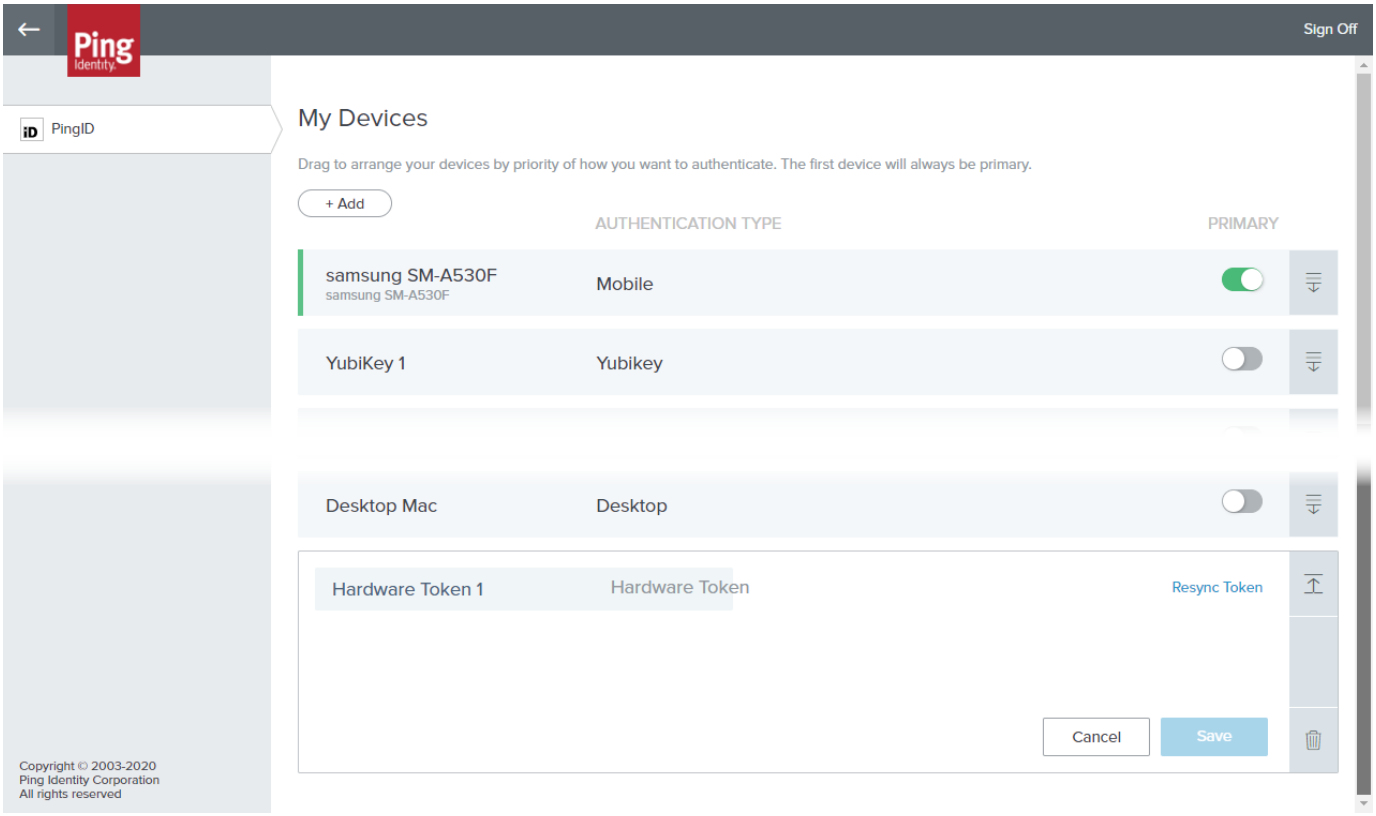
   - During authentication: When the **Authentication** screen opens, click **Settings**.
   - From your organization dock: Click the **Account** icon ( ) and then click **Devices**.
   - From a link provided by your IT department.

   Result:

   The **Devices** page opens, showing the devices you currently have paired with your account. The primary device is shown in green.



2. Click the **Expand** icon ( ) to expand the entry next to the device you want to rename. You may be prompted to authenticate with your primary (default) authentication device.



3. Click the name field, delete the current text, enter the new name, and then click **Save**.

Unpairing a device

If you no longer want to use a device to authenticate with PingID, you need to unpair it.

Before you begin

If you do not have access to manage your devices from the **My Devices** page, contact your organization's helpdesk to ask your administrator to help you to unpair the device.

If your device is lost, broken, or stolen, and you do not have another device paired with your account, see Handling a lost, broken, or stolen device situation.

About this task

You can unpair devices from your account portal **My Devices** page.

> **Caution**
>
> If you remove all your paired devices, you might be blocked the next time you try to sign on (unless your organization's configuration allows users to register a new device during authentication).

Steps

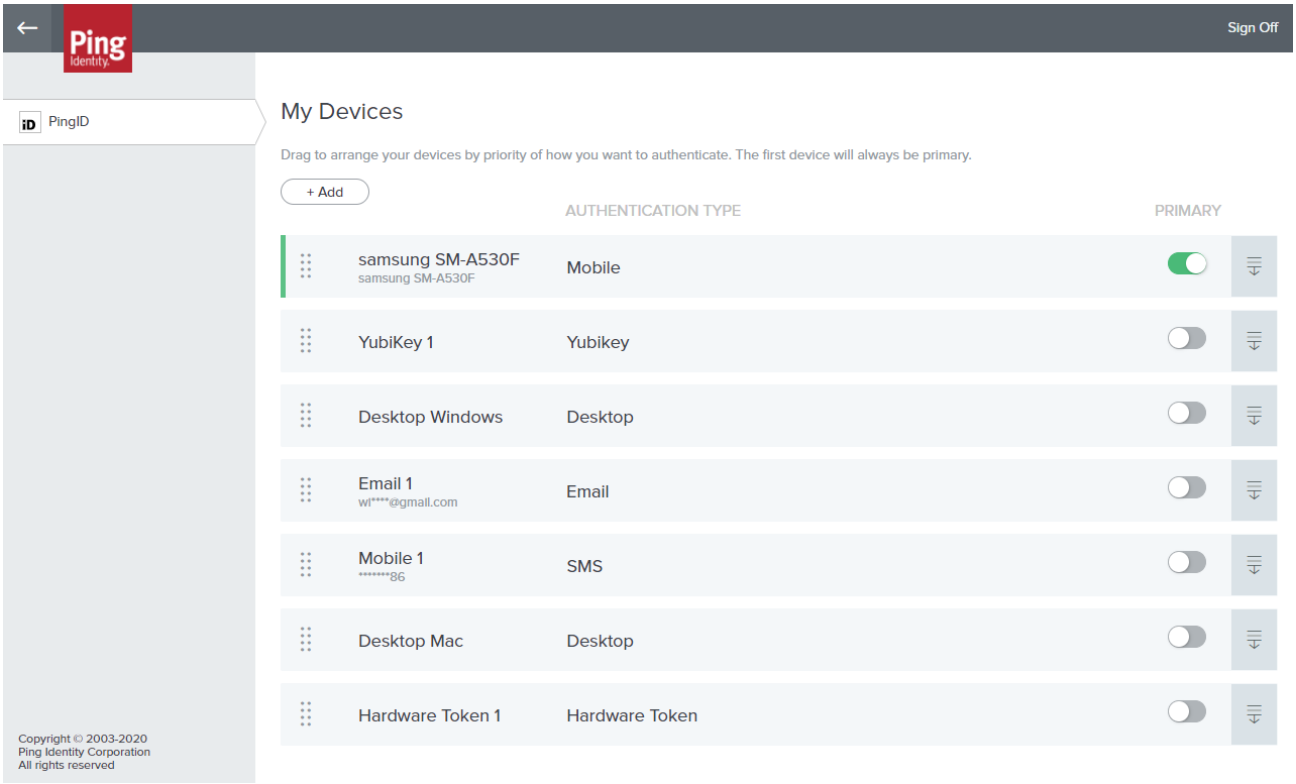
1. Access your **My Devices** page:

Choose from:

- During authentication: When the **Authentication** window opens, click **Settings**.
- From your organization portal: Sign on to your account and in the Avatar menu, click **Devices**.
- From a link provided by your IT department.
- (VPN only): From the **Devices** link that appears on your VPN landing page or that you received from your organization.

Result:

The **My Devices** window opens and lists the devices and their **Authentication Type** paired with your account. The primary device has a green highlight and the **Primary** switch is toggled to the on position.



2. Click the **Expand** icon ( ) next to the device you want to remove.

   A message asking you to authenticate with your primary (default) authentication device might appear.

3. Click the **Delete** icon.

   Result:

   A dialog appears asking to confirm your removal request.

4. To confirm the removal, click the **Remove** button.

   Result:

   The device is removed and no longer appears in the **My Devices** list. If the device was defined as your primary device, the next device appearing in the **My Devices** list is assigned as the primary device by default.

5. Repeat steps 1 to 4 for each device you want to unpair.

> **Note**
>
> If you are unable to unpair a device, contact your administrator.