Multifactor Authentication Toolkit

Table of Contents

MFA Client and Services Management

Click each title or page number to be taken to that section.

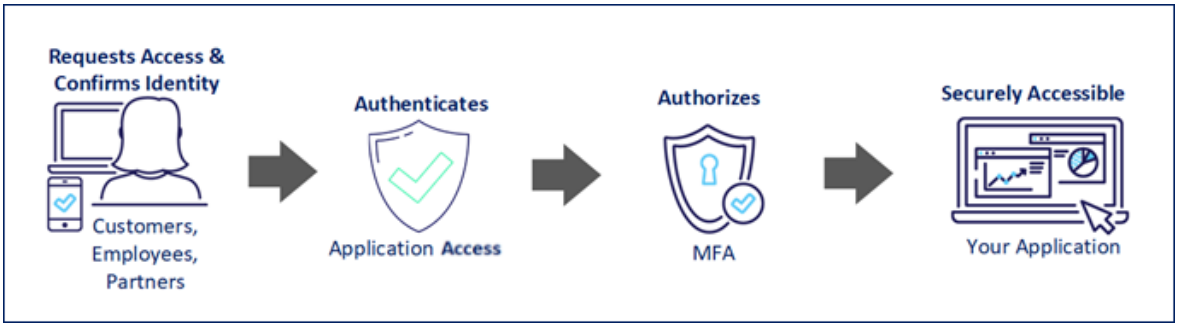
- Multifactor Authentication (MFA) Toolkit 2
- PingID MFA Quick Start 3
- MFA Authentication with PingID 6
- How to Modify an Existing Phone Number 8
- How to Add New or Additional Devices 10
- How to Pair a Device to an Additional Organization 14
- How to Unpair a Device 19
- How to Reset Your Desktop PIN Code 23
- How to Disable and Enable Passcodes for Apple Watch 25
- FAQs 26

For more information, click here to view the full guide on Installing and Configuring the PingID Client for Optum Multifactor Authentication (MFA)

Multifactor Authentication Toolkit

Knowledge for Success

Note: No action is necessary until prompted by your Optum application.
Multifactor authentication (MFA), sometimes referred to as “two-step verification”, adds a layer of protection to a website and/or application, by confirming a user’s identity when initially logging in. Utilizing your password and a one-time passcode (OTP) received via phone or additional desktop application, we’re able to confirm your identity.
To secure our applications, Optum has partnered with PingID to provide a strong MFA solution. PingID multifactor authentication (MFA) allows you to authenticate to your application using additional authentication methods, such as your mobile device, to enhance security and provide ease of access to those apps.



How does MFA work?

When you sign into your account, PingID sends an authentication notification to your PingID-configured device. You can authenticate using one of the following methods:

- Swipe, biometrics, or a push notification action via your device
- Entering a one-time passcode on your device when prompted
- Entering a one-time passcode into your web browser

  ** One-time passcodes can be received via SMS or voice*

What are the MFA-Supported Methods for Optum?

The following devices can be used to authenticate via the PingID application:

- Android Phone (Android 8.x or later)
- iPhone (iOS 12 or later)
- Desktop (MacOS and Windows)

Learn More

- PingID MFA Quick Start
- MFA Authentication with PingID
- MFA 2023 FAQs

PingID MFA Quick Start

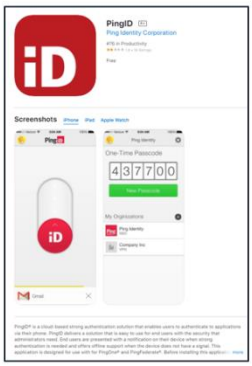
Product Tip

Summary

Optum has partnered with PingID to provide a Multifactor Authentication (MFA) solution to secure our applications. Utilizing your password and a one-time passcode (OTP) received via phone or additional desktop application, we are able to confirm your identity. Learn how to get started with PingID and register your device.

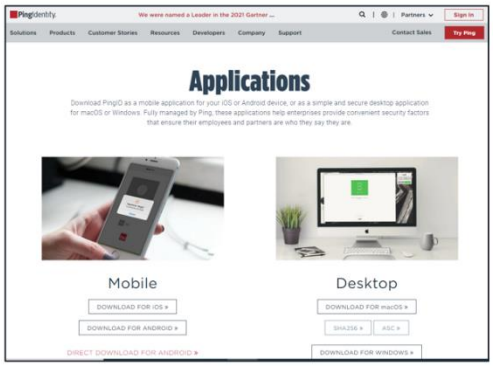
Get PingID

Download and Install PingID from your mobile device's app store or directly from the [PingID Website].



iOS

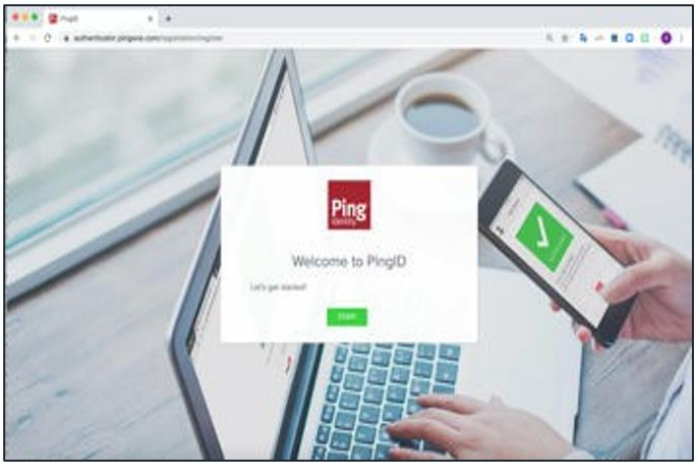
Google Play



PingID Website

Register with PingID

Sign in to your application, a registration window displays. Follow the on-screen instructions to add a new device to use with PingID.

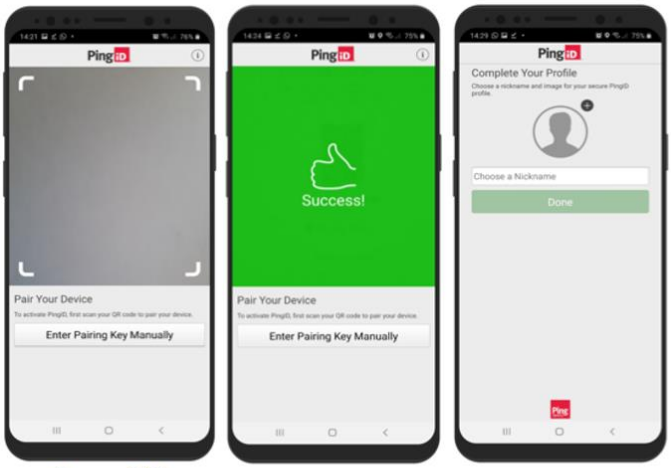


PingID MFA Quick Start

Product Tip

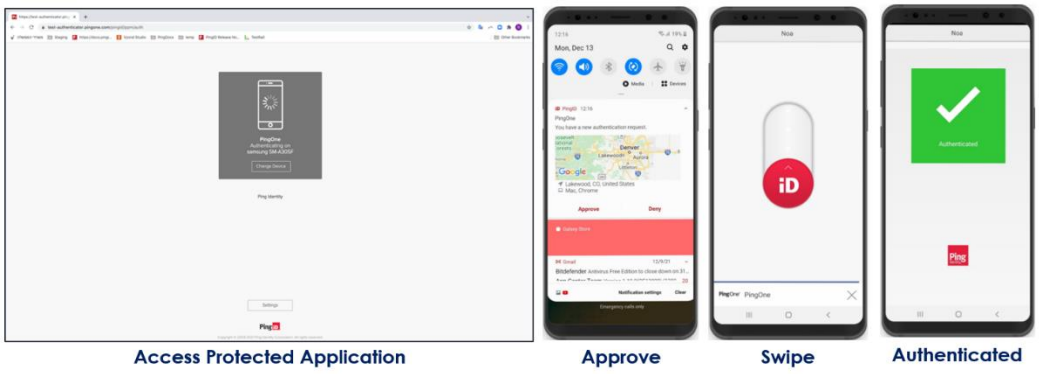
Configure PingID

Once registration is complete, follow the on-screen instructions in the PingID app to accept terms and permissions, and pair your device.



Authenticate with the PingID Mobile App

Now that your device is set up you can use PingID when you sign in to your Optum applications. After signing in, follow the steps that display to complete the MFA process. PingID displays a checkmark confirming successful authentication and you will be redirected to the application.



PingID MFA Quick Start

Product Tip

Authenticate with MacOS/Windows Desktop App

After signing in, follow the steps that display on the screen to complete the MFA process. PingID displays a checkmark confirming successful authentication and you will be redirected to the application.

Access protected account or application

Review PingID Prompt

Generate and copy a One-Time Passcode

Paste the One-Time Passcode & Sign-on

MFA Authentication with PingID

Product Tip

Summary

To secure our applications, Optum has partnered with PingID to provide a strong Multifactor Authentication (MFA) solution. PingID MFA allows you to authenticate to your application using additional authentication methods, such as your mobile device, to enhance security and provide ease of access to those apps. Learn how to Authenticate with PingID with after registering your device.

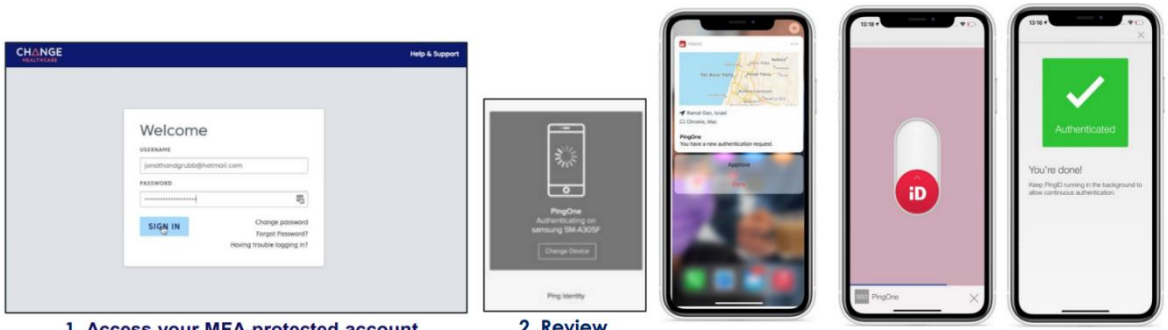
Authenticate with Android/iOS Mobile App

Sign in to your MFA-protected application to trigger a prompt to swipe to authenticate on your device:

Android

1. Access your MFA-protected account or application
2. Review PingID Prompt
3. Approve or Swipe
4. Authenticated

iOS



1. Access your MFA-protected account or application
2. Review PingID Prompt
3. Approve or Swipe
4. Authenticated

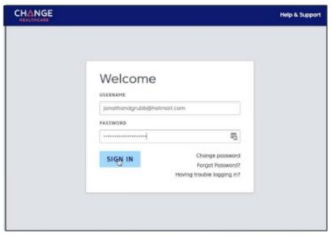
MFA Authentication with PingID

Product Tip

Authenticate with Voice or Text

When you sign in to your account or app, you receive:

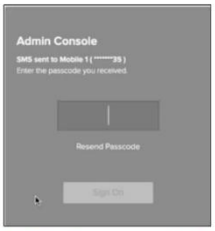
- A phone call with an automated recording of your passcode.
- An SMS with your passcode.



1. Access your MFA-protected account or application

2. Review PingID Prompt

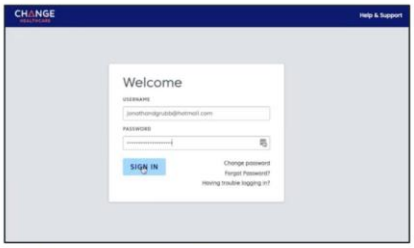
3. Receive a call or text that provides the passcode



4. Enter the passcode into the PingID prompt.

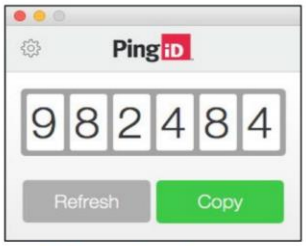
Authenticate with MacOS/Windows Desktop App

When you sign in to your account or app using a web browser, use PingID desktop app to authenticate:



1. Access your MFA-protected account or application

2. Review PingID Prompt



3. Generate and copy a One-Time Passcode

4. Paste the One-Time Passcode & Sign-on

Modifying an Existing Phone Number in MFA

Quick Reference Guide

Summary

Users can use Voice or Text to authenticate with MFA. There may be times when you need to update the phone number associated with your account. Learn how to update an existing phone number for MFA

1. Log in to your MFA-protected application.

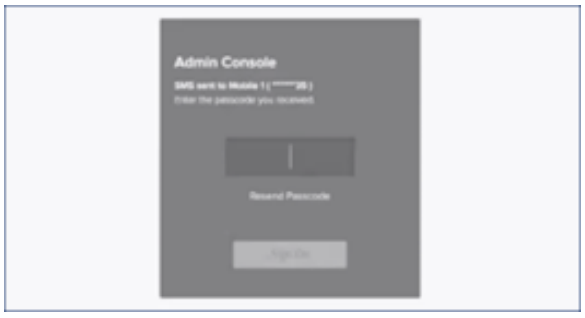
2. Click **Settings**.

3. Click the **Expand** icon on the My Devices screen.

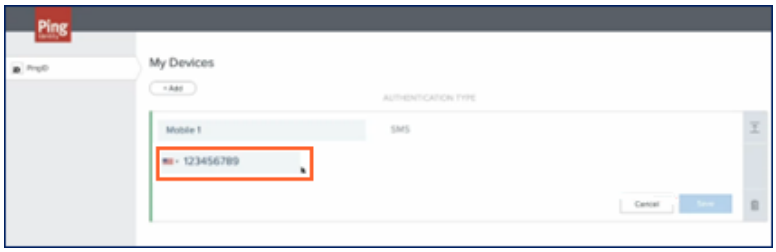
Modifying an Existing Phone Number in MFA

Quick Reference Guide

4. Enter the passcode and click **Sign On**. Upon verification, you are returned to the My Devices screen.



5. Edit the phone number and click **Save**.



Note: Click the **Delete** icon to delete the phone number instead of changing it.

6. Enter the passcode received via the new phone number and click **Verify**. Once verified, the phone number modification process is complete.

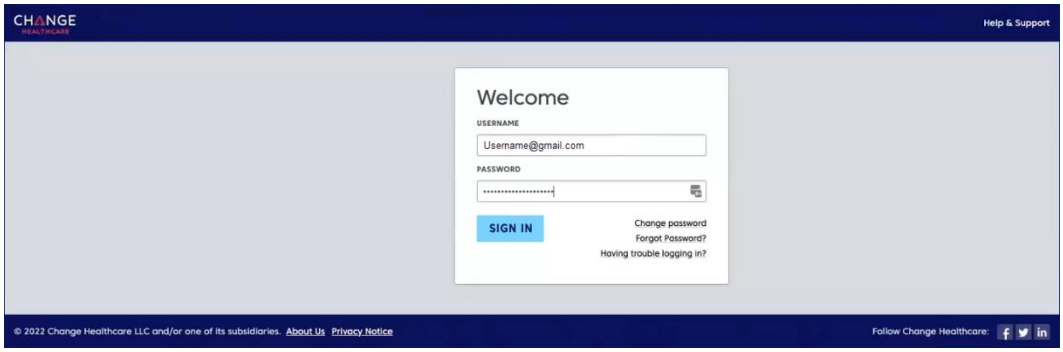
Adding New or Additional Devices for MFA

Quick Reference Guide

Summary

Adding more authentication devices is useful if your preferred device is unavailable. When you are prompted to authenticate, you can select a different device. Learn how to add additional devices for MFA.

1. Log in to your MFA-protected application.



2. Click **Settings**.

3. Click **Add** on the My Devices window.

Note:

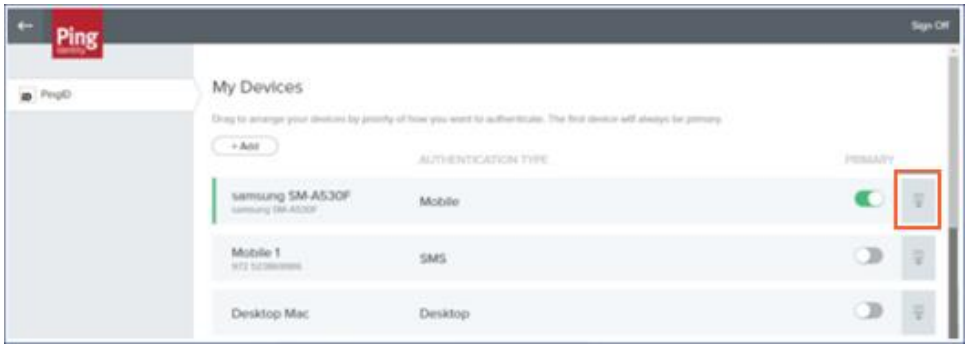
- Existing Authentication Device May Be Required
- You may be prompted to authenticate using an existing authentication device.

4. Click the new authentication method to add.

Note:

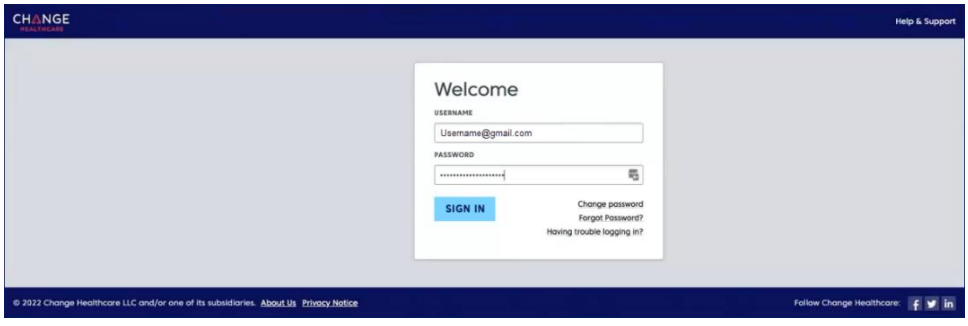
- Authentication methods may vary
- Each authentication method prompts you with its own set of instructions. Follow the instructions, download the relevant software, if required, and complete the registration and pairing of your newly added device. When the system has completed pairing your device, you are redirected back to the My Devices page, displaying the new device as the last row in the listing with its default nickname.

5. Click the **Expand** icon to view and edit details of a device, including:
   - **Device nickname:** Name of the device as it displays when you are prompted to authenticate. The marketing name of the device (e.g., iPhone X) or the authentication method (e.g., SMS) displays by default.
   - **Device details:** Details that identify the authenticating device (e.g., your phone number). If you choose to edit the details, you are prompted to authenticate and must make sure the details are valid (e.g., valid phone number in the correct format). To protect your privacy, this information may display as masked if you have not recently authenticated.
   - **Authentication type:** Type of authentication method (e.g., SMS). You cannot edit this information.

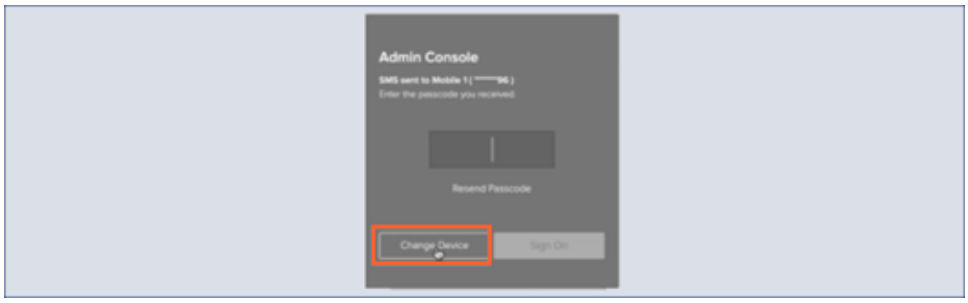


6. Click the **slider** to On (green) in the **Primary** column to make a device the primary (default) device. The toggled device moves to the top of the list.

7. Return to your application and log in.



8. Once the new device is added, the MFA prompt allows you to select how to authenticate. Click **Change Device**.



9. Click the **device** to authenticate with. Click **Sign On** and authenticate with the new device.

Pairing and Adding an Additional Organization to PingID

Quick Reference Guide

Summary

With PingID, you can use the same device to authenticate for more than one organization. Learn how to pair a mobile device to an additional organization.

Pair a Mobile Device to an Additional Organization

1. Sign in to the account or service of the new organization to display the Authentication window with the QR code and pairing key.

2. Open PingID on your device to view My Organizations Click the **plus** icon.

Pairing and Adding an Additional Organization to PingID

Quick Reference Guide

3. Scan the QR code or click **Enter Pairing Key Manually**. Enter the **pairing key** and then tap **Add Service**.

4. The organization is added to your My Organizations list. **Authenticate** on your device when prompted.

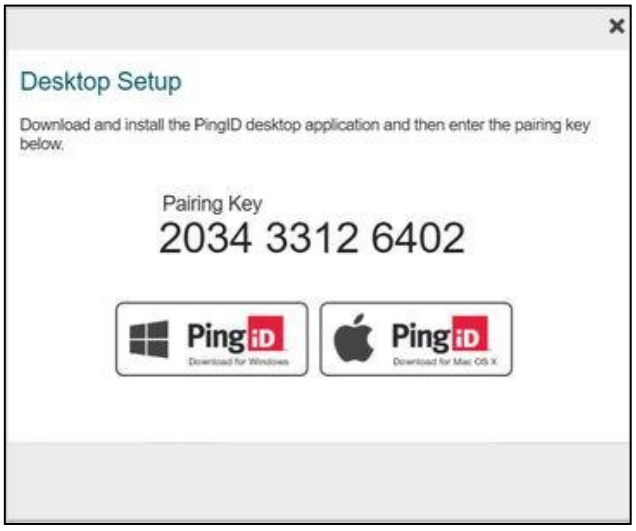
Pairing and Adding an Additional Organization to PingID

Quick Reference Guide

Pair a Desktop Device to an Additional Organization

1. Sign in to the account or service of the new organization and click **Desktop**.

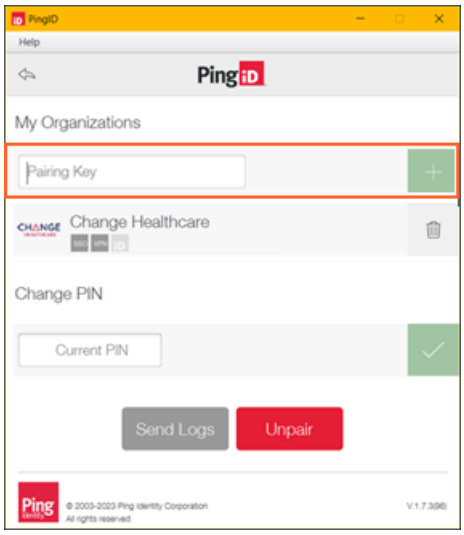
2. The Desktop Setup window displays the pairing key needed for step 4.



Pairing and Adding an Additional Organization to PingID

3. Open the PingID desktop application and click the **Gear** icon.

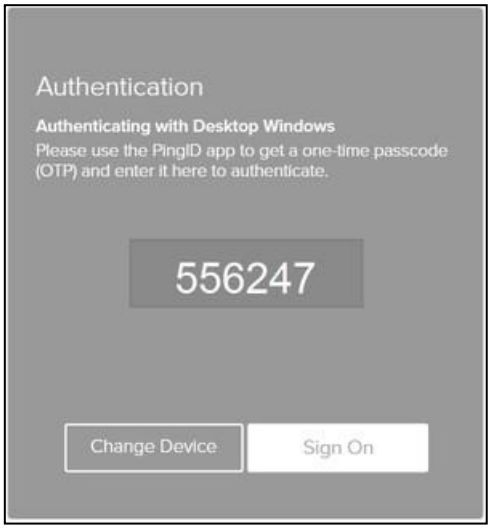
4. Copy and paste the **pairing key** from Step 2 into the Pairing Key field. Click the **plus** icon.



Pairing and Adding an Additional Organization to PingID

Quick Reference Guide

5. The organization is added to the My Organizations list. **Authenticate** with your desktop when prompted.



Unpairing a Device from your PingID

Quick Reference Guide

Summary

You can unpair devices from your account portal, My Devices page or with the mobile app. PingID prompts you to pair a new device the next time you sign in if you remove all your paired devices. Learn how to unpair your devices.

Unpair a Device via the Account Portal

1. Access your My Devices page by one of the following options:
    - During authentication: Click **Settings** when the Authentication window opens.
    - From your organization portal: Sign in to your account and in the **Avatar** menu, click **Devices**.
    - **VPN only**: From the Devices link that appears on your VPN landing page or that you received from your organization.

    The My Devices window opens and lists the devices and their Authentication Type paired with your account. The primary device has a green highlight with the **Primary** switch toggled to the on position.

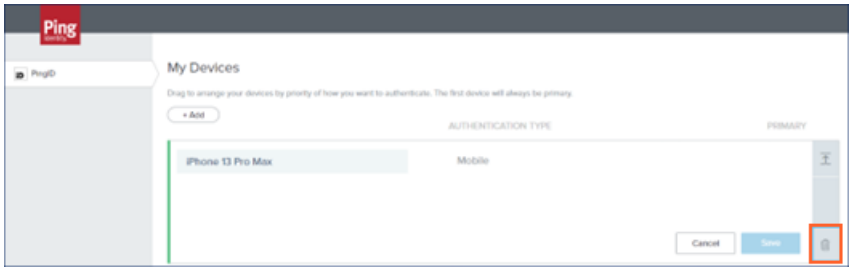
2. Click the **Expand** icon next to the device you want to remove.

Note: You might be prompted to authenticate with your primary (default) authentication device.

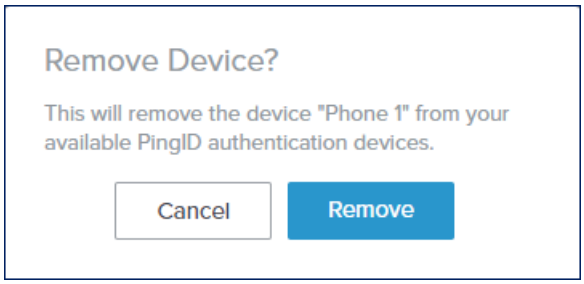
Unpairing a Device from your PingID

Quick Reference Guide

3. Click the **Delete** icon.



4. Click **Remove**. The device is removed and no longer displays in the My Devices list.



Note: The next device displayed in the My Devices list is assigned as the primary device by default if the device was defined as your primary device.

Unpairing a Device from your PingID

Quick Reference Guide

Unpair via a Mobile Device

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.

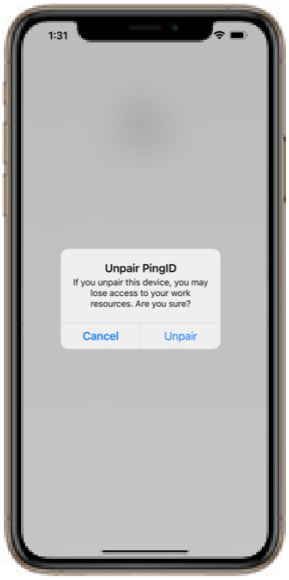
3. In the menu, tap **Unpair Device**.

Unpairing a Device from your PingID

Quick Reference Guide

4. A message displays asking you to confirm your request to unpair your device from the PingID app. Tap **Unpair** to confirm your changes or tap **Cancel** to stop your unpairing request.

5. Tap **Unpair** and tap **Ok**. The device is unpaired, and you cannot use it to authenticate.



Product Tip

Resetting Your Desktop PingID Pin Code

Summary

With PingID desktop app, you can reset your desktop PIN code if you lose or forget it. Learn how to reset your desktop PIN code for PingID.

Reset a Lost or Forgotten PIN Code

1. Uninstall and reinstall the PingID desktop app.
2. Re-pair the desktop app to your PingID account.

Reset a PIN Code You Know

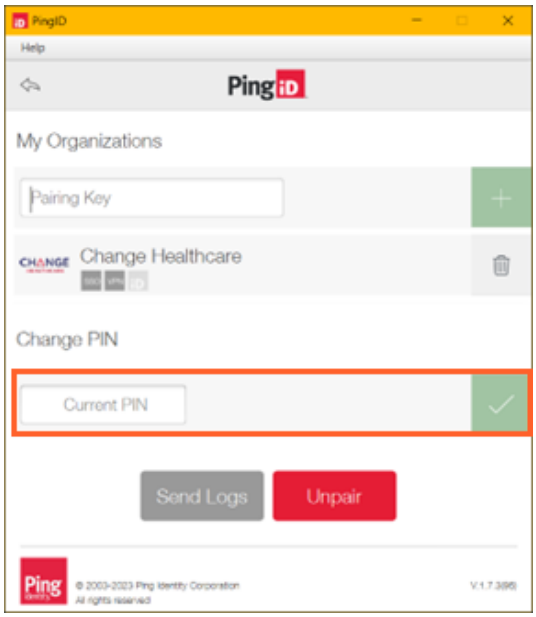
1. Open the PingID desktop app and enter your **PIN code** and click **Next**.

2. Click the **Gear** icon.

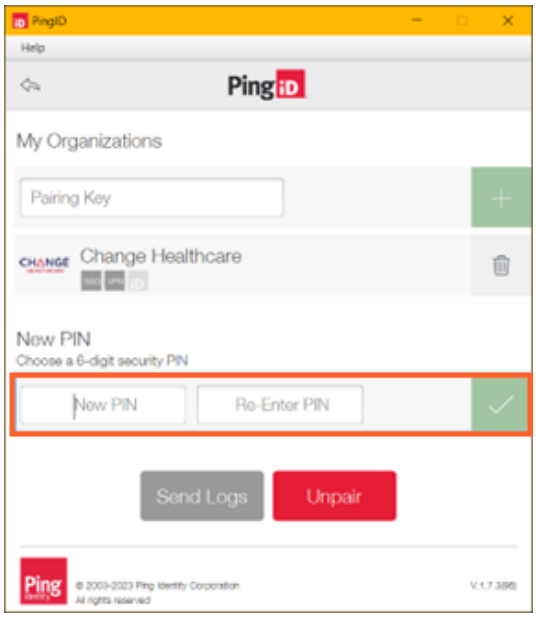
Resetting Your Desktop PingID Pin Code

Product Tip

3. Enter your **PIN code** in the Current PIN field and click the **green checkmark**.



4. Enter the **new PIN** in the New PIN and RE-Enter PIN fields. Click the **green checkmark.**



Enabling or Disabling PingID MFA Passcodes on Apple Watch

Quick Reference Guide

Summary

The PingID Apple Watch app is automatically installed on your watch, and you will start receiving notifications to your watch when you install PingID on your iPhone. Learn how to disable or enable the passcodes on your Apple watch.

1. Tap the **Watch** app on your iPhone, then tap **PingID**.

2. Tap **Show App on Apple Watch** to enable or disable the app on your Apple Watch. The PingID app is installed on your Apple Watch, and the PingID icon displays.

   Note:

   - The Apple Watch only receives notifications when your mobile device is locked and in sleep mode.
   - If the Apple Watch app is disabled, you will not be able to access a one-time passcode from your watch.

3. To view the current one-time passcode on your Apple Watch, tap the **PingID** icon. Tap **Refresh** for a new passcode.

Multifactor Authentication (MFA) with PingID

Frequently Asked Questions

Last updated: June 2, 2023

The following questions and answers have been compiled to help answer frequently asked questions we have received regarding multifactor authentication with PingID. Please note that this document will continue to be updated as we receive new questions and/or updates to any answers provided.

General information

What is MFA?

Multifactor Authentication (MFA) is a virtual security feature that uses two or more factors or "methods" to identify and authenticate users to ensure only approved individuals can access information in a virtual environment, network, or website.

How does MFA work?

With MFA, you must verify your identity with separate methods to ensure proper access, such as:

- What you know (e.g., a password)
- What you have (e.g., something only an approved user would have such as your personal cell phone).
- Something you are (e.g., biometrics such as facial recognition and fingerprint).

By using two different methods to authenticate access to Optum networks, we can keep all information secure and safe.

My company currently uses CIAM. What is the difference between this and MFA? Why do I need to use both?

CIAM is the centralized authority for identity/authentication within the domain of the Optum platform; this includes all customer facing applications and users of those applications. CIAM MFA (PingID) adds a layer of protection to the CIAM sign-in process by requiring you to not only enter your password, but also a specific code received by phone or an additional desktop application.

In short, CIAM authenticates who you are by your User Id and Password and CIAM MFA authorizes access based on what you have, to prove your identity by authentication with cell phone, biometrics, or one-time use passcode.

Multifactor Authentication (MFA) with PingID

Frequently Asked Questions

Do I have to use a cell phone?

No. Optum supports the following PingID MFA methods:

- Authentication via an Android Phone app (Android 8.x or later)
- Authentication via an iPhone app (iOS 12 or later)
- Authentication via the Desktop app (MacOS and Windows)
- One-time Passcode via SMS or Voice

What if I am already using PingID for MFA for other applications?

You can use your existing devices and enroll additional devices to your identity as needed.

What if I am already using a different MFA client for other applications?

Currently, Optum only supports PingID for MFA authentication. Therefore, PingID is required to access Optum applications.

Can I select which Optum applications use MFA?

No. Once MFA is enabled for your organization, it applies to all your protected applications.

When do I have to start using MFA with PingID?

MFA will be automatically enabled between May 3 and June 30. Once enabled, all users in your organization are required to use MFA, which requires the successful pass of an MFA challenge on initial login.

What if I am on leave during this transition?

If you are on leave when MFA is enabled for your organization, you will be enrolled automatically and will be able to register new devices when you return from leave.

I authenticate using my company's authentication process to access Optum products; do I also need to authenticate using a Optum method?

No. If your company is currently federated with Optum, your process to log into Optum products will not change.

Multifactor Authentication (MFA) with PingID

Frequently Asked Questions

What is federated access?

Federated access is when a customer uses their own identity management systems and already leverages other SaaS applications to authenticate the user's identity against their internal identity system.

Does two-step verification occur each time the users log in?

Yes, users will need to complete the two-step verification each time they log in.

Will I need to reauthenticate if I have the product open in the background?

Yes, users will need to reauthenticate after 60 minutes of inactivity.

Does MFA impact remote users or onsite users?

This impacts both remote and onsite users.

What should I do if my company does not allow PingID to be installed on my workstation?

PingID does not require users to install any applications on their mobile phone or desktop. You can choose between the SMS and call options and provide your mobile phone number to receive the code via text or a phone call. These options are listed at the bottom of the prompt screen.

My company does not allow individual users to download applications. Is there a way to install PingID on all our company issued devices; laptops/desktops/ tablets/etc.?

To deploy the PingID MFA desktop application across an entire organization instead of on a per user basis, download the desktop application from the PingID Downloads page, then have your system administrator follow your organization's software management policy for deploying software packages.

I have downloaded the app, however it is asking me pair my device with either a QR code or enter the pairing key manually; where do I find the QR code or Pairing Key?
After MFA is activated for your organization the QR code and Pairing key display when you log in to a MFA protected application. No action is necessary until prompted by your Optum application.

Multifactor Authentication (MFA) with PingID

Frequently Asked Questions

Can more than one user share one CIAM account but use their own PingID app (Mobile or Desktop) for MFA challenge?

This is allowed and possible, however this kind of use case is typically not recommended due to recommended security practices.

What are the differences between a critical, major, and minor issue for CIAM issue?

The CIAM Engineering team has defined the SLAs for completing each type of Support Request:

- Critical: 1 working day
- Major: 3 working days
- Minor: 5 working days

Is there a cost to download the PingID app?

No, the PingID app is free to download.

Timeline

Will I be required to login using multifactor authentication after a certain date, or can the user continue to login as regular?

Users will be required to use MFA once it has been implemented for their organization. Implementation dates vary by organization.

Troubleshooting

I received a message saying I'm locked out. What should I do?

After three incorrect password attempts, you are locked out for two minutes. You can try logging in again after two minutes have passed.

What should I do if I have gone through all of the steps, but have not received a verification code?

Contact Optum via your support portal or by calling 1-866-371-9066.

What do I do if an authentication error message displays when authenticating with PingID?

Frequently Asked Questions

iOS: You must have Touch ID enabled to authenticate with PingID.

Android: You must have fingerprint enabled to authenticate with PingID.

If one of these messages display, then your organization defined fingerprint authentication as a requirement for signing on to services protected by PingID mobile app.

To authenticate, enable Touch ID or Fingerprint recognition on your mobile device.

Why does the fingerprint notification not display on my mobile device when authenticating with PingID?

If your organization's policy enables fingerprint authentication notifications, set the mobile device's general notification and the PingID mobile app-related notification settings to ON.

What do I do if the fingerprint scan fails when authenticating with PingID?

After several attempts, the device might lock for a predefined number of seconds. When it unlocks, you can retry the authentication process.

You might receive instructions to enter your mobile's backup password, an error screen, or a canceled screen. Follow the instructions displayed on your screen, check the Fingerprint configuration on your device, and consider recapturing clearer scans of your fingerprints.

iPhone Troubleshooting

Why does the iPhone interactive notification not display when authenticating with PingID?

Interactive notifications may not display because your organization disabled the interactive notification actions according to its security policies, your mobile's iOS is earlier than version 8, or your PingID mobile app is earlier than version 1.4.

Ensure your iOS and the PingID mobile app are updated to the latest versions.

Android Troubleshooting

Why does a fingerprint notification display on my Android device instead of a swipe screen?

Fingerprint authentication has been configured for your organization. If your Android device supports it, use fingerprint authentication instead of the swipe screen.

Multifactor Authentication (MFA) with PingID

Frequently Asked Questions

Why am I getting a "Canceled" error message when using face or iris biometric authentication with PingID mobile app on my Android device?

Face and iris recognition are not supported for use with the PingID mobile app on some devices. Try the following configuration steps to verify if your device supports face and iris recognition.

- Verify you have defined biometrics on your device.
- Configure fingerprint authentication.
- Make sure you are using the latest version of Android OS on your device.

If you still cannot authenticate using face or iris recognition, then your device does not support face or iris authentication with PingID mobile app. Try to use fingerprint authentication instead.

Why is there not an option to choose between face and fingerprint when authenticating with PingID when I have both defined on my Android device?

Some Android devices do not give the option to choose between different biometrics authentication methods when authenticating with PingID mobile app.

Attempt to set the primary authentication method for your device but face and fingerprint recognition may not be supported for use with PingID mobile app on some Android devices.