Multifactor Authentication Registration Guide V9.2

Contents

Introduction

Multifactor authentication (MFA) is a method of logging into a system or application that requires an additional factor(s) (something other than your password) to log in. You've most likely used it when interacting with your financial institutions. Logging in will prompt you not only for your password, but also a special code or action (like swiping something on your smartphone or tablet). We have instituted MFA at the American Cancer Society and ACS CAN to protect you and the Society from malicious phishing attacks, which can compromise the security of our systems and data.

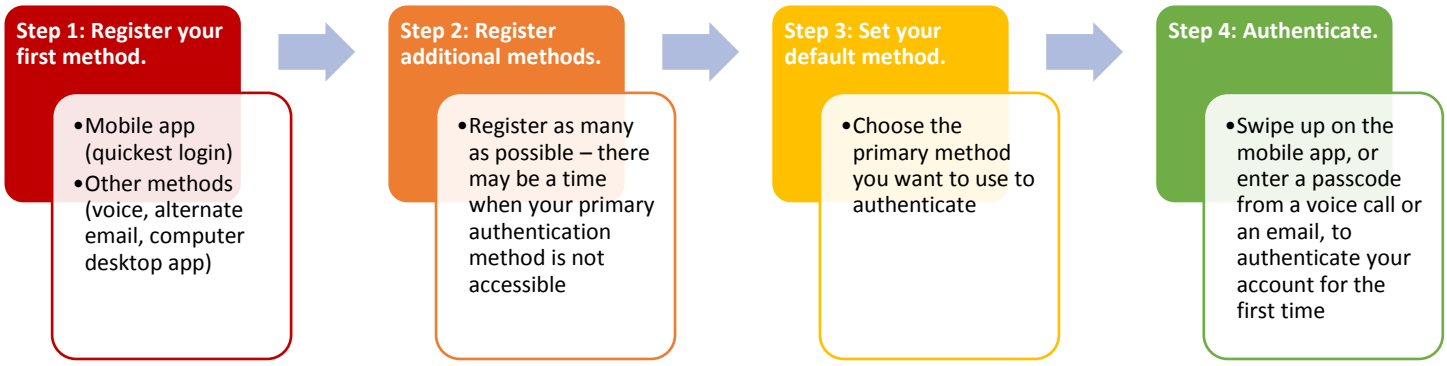
There are multiple 'devices,' or methods of authentication, you can use. The methods we use at ACS are:

- Mobile app installed on Android or iPhone (highly recommended, the fastest login).
- Phone call (must be a direct dial number that you have access to when you are using your computer, or a mobile device. Mobile app is recommended if you are a traveler).
- Email (an address you can access without being logged into your ACS computer or Office365 account).
- Desktop app already installed on your laptop/desktop (not available to volunteers).

Methods must be registered before they can be used for authentication. This guide walks you through the steps required to register both an initial method and additional methods. We recommend setting up as many methods as possible. This way, if you are unable to authenticate one way (perhaps your mobile device has lost its charge), you can authenticate another way.

You'll receive an email at your cancer.org email address each time you register a method. This is a security precaution designed to alert you to the fact that someone else may have obtained your username and password and registered a method with them. **If you receive this email but have not registered a method, open an urgent support ticket by using Ask Navi / Live Chat at helpme.cancer.org.** Be ready to provide the information contained in the registration email. If needed, one of our support personnel will follow up with you.

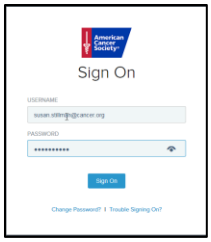
Below is a glance at the overall process to register for MFA:



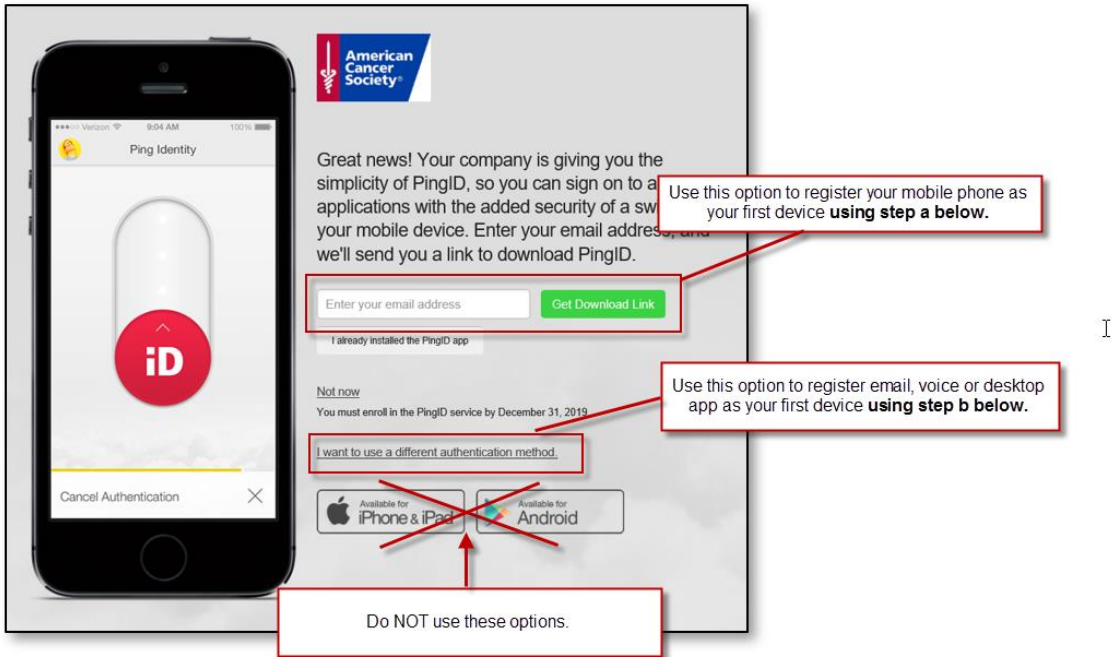
STEP 1: Register your First Authentication Method

Read all the steps in these instructions before you follow them

1. From your computer, follow this link https://sso.cancer.org:9031/idp/startSSO.ping?PartnerSpId=sso.cancer.org to the registration form.
2. Enter your ACS email address and password. Then select "Sign On".



Next, you will be asked to register a method to be used for your ACS account login and authentication. Below is the initial screen you will see on your computer when you start to register a method. **From this screen you can choose to register any method (not just mobile).** Registration of a mobile device as your first authentication method is highly recommended. You can also choose to register an email, voice line, or desktop method. Once an initial method is registered, you can use instructions in the section on p. 10 of this guide to register additional methods.



a. Register a Mobile Device (by installing the PingID Authenticator app)

Read all the steps in these instructions before you follow them

To register an alternate method, go to step b, *Alternate Authentication Options*, on p. 6.

You will **not** need to go to your app/play store for this.

1. Enter an email address you can access on your mobile device and select “Get Download Link”. It’s safe to use your personal email address.

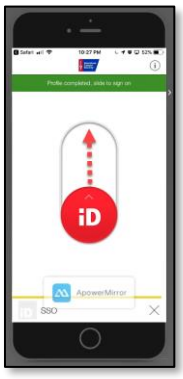
An image like the one below will display on your computer. Leave it on your desktop/laptop screen. You’ll return to it later.

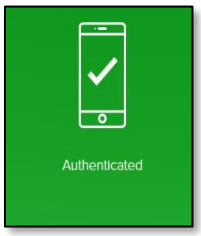
2. Open the email from your mobile device, select the appropriate download for your device and complete the app install.
3. Open the app on your mobile device, **accept the Terms of Service and all subsequent messages (required).**
4. After the install on your mobile device has completed, go back to your desktop and use your mobile device’s camera to scan the QR code (no QR scanner is needed).
    a. Your mobile device will also give you an option to enter a pairing key manually instead. Use the pairing key that appears next to the QR code. The one you see on your computer screen will differ from the example depicted above.
5. **Accept any subsequent messages (required).**
6. Enter a nickname (example: Susan ACS).
7. Wait while a pairing request is sent to your mobile device. You may see this displayed on your mobile device (the code you see will not match the code displayed below).

Pairing is complete when you see a red slider on your mobile device, depicted in the next step.

8. Swipe the red button up.

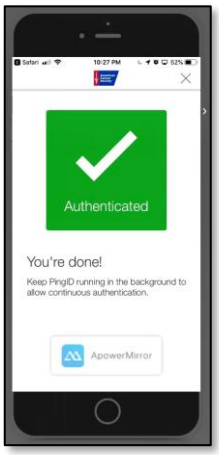
NOTE: If you use face or fingerprint recognition on your mobile device, you may not see this swipe action screen. Your face or fingerprint recognition replaces this step.





Next, PingID on your computer will send an MFA request to the PingID authenticator app on your mobile device.

Authentication will be verified. Your mobile device registration is complete.



At the same time, your computer browser will be redirected to the PingID registration "Success" page.

NOTE: You'll also receive an email advising that this mobile device has been registered.

9. **Proceed to the section on p. 10 of this guide to register additional methods (recommended).**

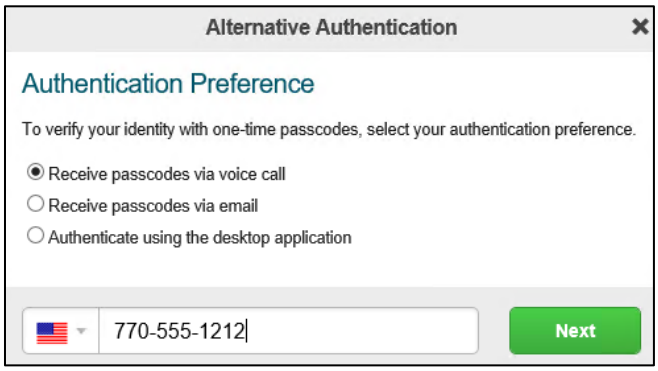
b. Alternate Authentication Options

Use these steps to register a voice, email, or desktop app method.

Read all the steps in these instructions before you follow them

1. *Receive passcodes via voice call.*
    a. Use this link https://sso.cancer.org:9031/idp/startSSO.ping?PartnerSpId=sso.cancer.org to go to the registration form, if you aren't already there.
    b. Sign on with your ACS email address and usual password.
    c. Select the "I want to use a different authentication method" option.
    d. Select the "Receive passcodes via voice call" option.
    e. Enter a phone number and select "Next".

    This must be a direct dial number or mobile device that you have access to when you are using your computer. Mobile is recommended if you are a traveler. Skype phones will NOT work for this since you must authenticate to log into Skype to use the phone.



    f. You'll receive a phone call and will be given a one-time passcode.
    g. Enter the passcode provided into the Phone Number Verification box that displays on your computer screen, then click "Verify".

h. Once Verified, your browser will be redirected to the PingID registration "Success" page.

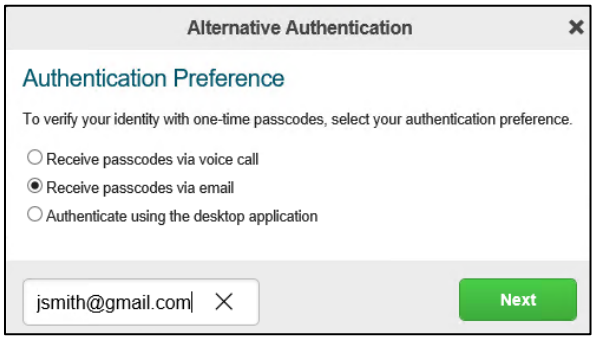
NOTE: You'll also receive an email saying that this method has been registered.

i. Proceed to the section on p. 10 of this guide to register additional methods (recommended).

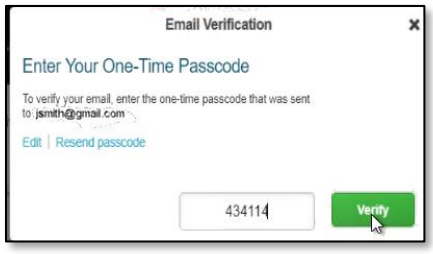
2. *Receive passcodes via email*

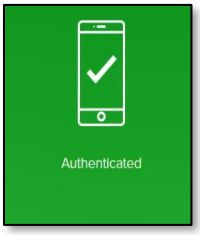
Read all the steps in these instructions before you follow them

a. Use this link https://sso.cancer.org:9031/idp/startSSO.ping?PartnerSpId=sso.cancer.org to go to the registration form, if you aren't already there.
b. Sign on with your ACS email address and usual password.
c. Select the "I want to use a different authentication method" option.
d. Select the "Receive passcodes via email" option.
e. Enter a valid email address and click "Next". (**NOTE:** Do not use your cancer.org email address. Use an email address you can get to from your mobile device or through a web browser).



f. You'll receive a "Welcome to PingID" email containing a one-time passcode. Enter the passcode into the Email Verification box on your computer screen, then click "Verify".





g. Once the passcode is authenticated, your browser will be redirected to the PingID registration "Success" page.

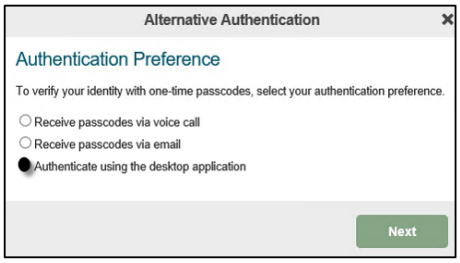
NOTE: You'll also receive an email saying that this method has been registered.

h. Proceed to the section on p. 10 of this guide to register additional methods (recommended).

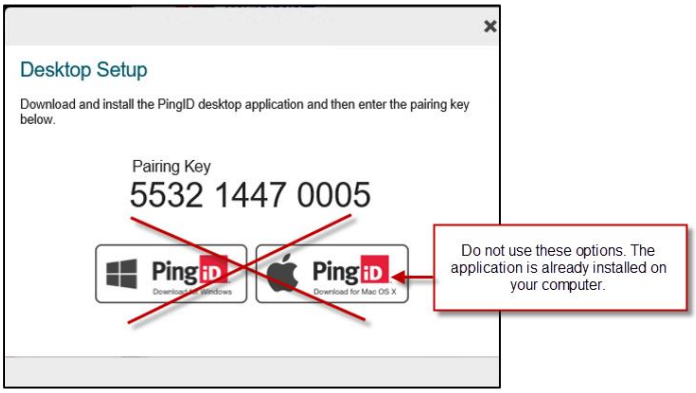
3. Authenticate using the desktop application:

Read all the steps in these instructions before you follow them

a. Use this link https://sso.cancer.org:9031/idp/startSSO.ping?PartnerSpId=sso.cancer.org to go to the registration form, if you aren't already there.
b. Sign on with your ACS email address and usual password.
c. Select the "I want to use a different authentication method" option.
d. Choose the "Authenticate using the desktop application" option and click "Next".



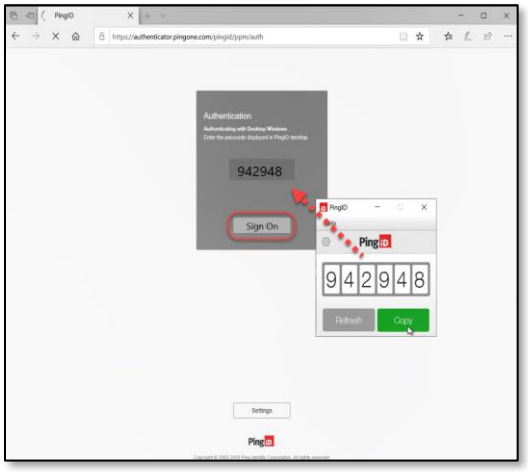
e. Copy the Paring Key provided on your computer screen.

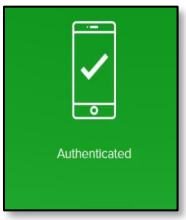


f. Open the PingID desktop application on the desktop of your computer.

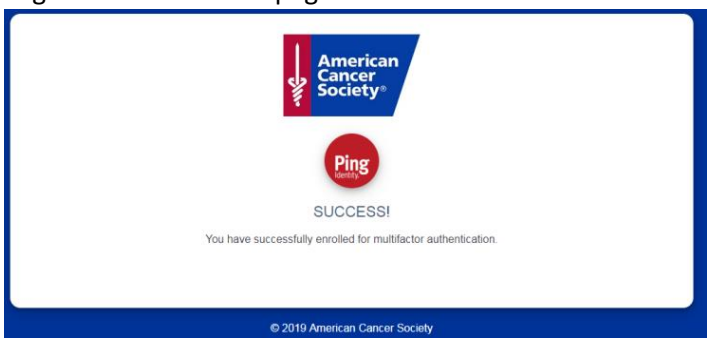
g. Enter or paste the pairing key into the available field and click “Pair”.

h. Once the app has been paired with your account, your browser will prompt for you to provide a one-time passcode. At the same time, the one-time passcode will be presented within the PingID desktop application. Click “Copy” and paste the code into your browser.





i. Once the passcode is authenticated, your browser will be redirected to the PingID registration "Success" page.



NOTE: You'll also receive an email saying that the desktop application has been registered.

j. **Proceed to the section on p. 10 of this guide to register additional methods (recommended).**

STEP 2: Register an Additional Method

Mobile Device

Skip this section if you have already registered your mobile device using the instructions in step a in the *Register Your First Authentication Method* section.

Read all the steps in these instructions before you follow them

Installation Overview

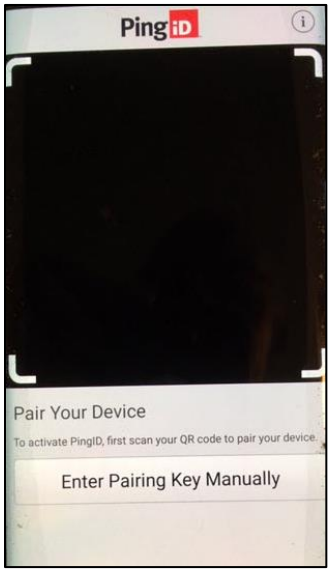
The steps you'll use to do this appear below. Here is a high-level explanation of what happens when you follow the steps.

PingID is the app that we use to enable mobile devices for multifactor authentication. In these steps you'll go to your mobile device's app store and download the PingID app. You'll install and open the app on your mobile device. Then you'll follow a link in the instructions below to the PingOne Portal (where the addition/deletion of methods takes place).

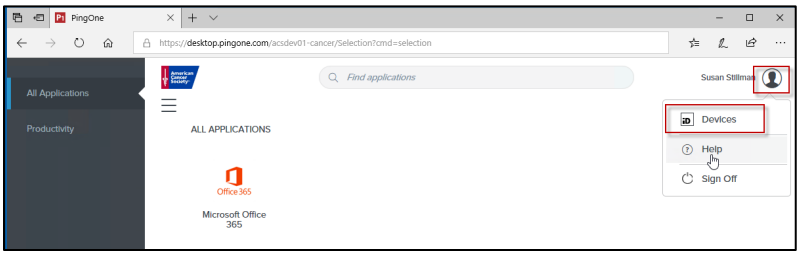
You'll tell the portal you want to add a device. It will present a QR code that you'll scan with the camera of your mobile device (no QR scanning app is needed) to enable the setup. Your mobile device will pair with the PingID app via the PingOne portal, after which you'll be able to use your mobile device to authenticate.

1. On your mobile device, go to the App or Google Play store and search for the PingID app.
2. Tap Install.
3. Tap Open (once installation is complete).
4. Accept Terms of Service and subsequent messages.

5. Set your mobile device, aside a moment. Leave it at this screen.

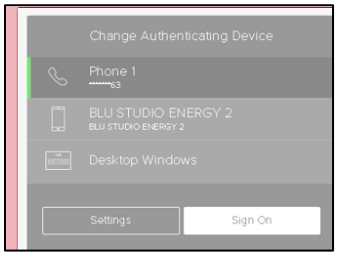


6. Follow this link https://desktop.pingone.com/ACS-Portal/ to the PingOne Portal.
7. Sign on with your usual ACS email address and password.
8. Click your profile icon, then click “Devices”.



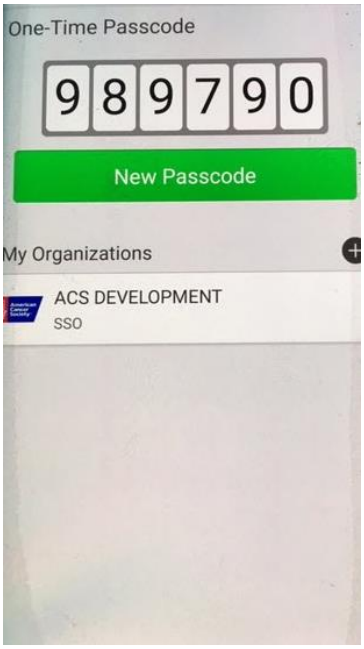
9. Click the “Add” button.

10. Authenticate when prompted.
    a. If you have not yet registered an additional method, authenticate, then go to step b. If you have already registered more than one method, you’ll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



11. Use the camera on your mobile device to scan the QR code that appears in the center of the image (depicted below) that appears on your desktop (no QR scanning app is needed).
    a. You may also enter the pairing code manually instead. Use the one displayed on your screen. The one displayed below is an example.

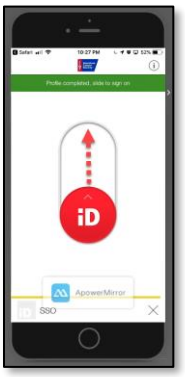
12. Accept any messages that appear.
13. Enter a nickname (example: Susan ACS).
14. Wait while a pairing request is sent to your mobile device via the PingID app. You may see this while you wait (the code you see will not match the code displayed below).

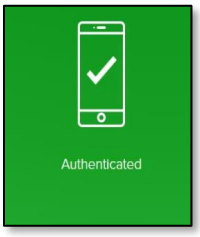


Pairing is complete when you see a red slider on your mobile device, depicted in the next step.

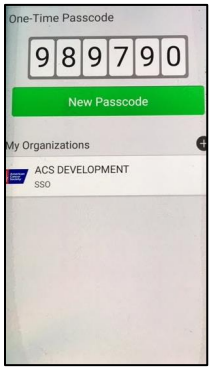
15. Swipe the red button up.

    NOTE: If you use face or fingerprint recognition on your mobile device, you may not see this swipe action screen. Your face or fingerprint recognition replaces this step.

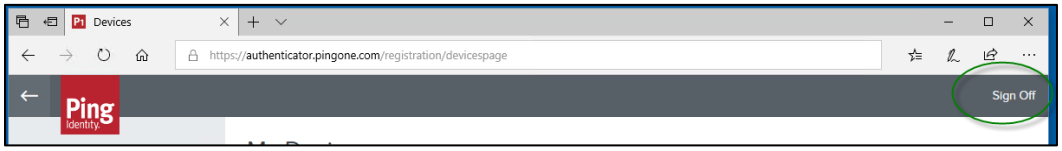




16. PingID may return to this screen. This code is not necessary. Dismiss it.



17. Sign off.

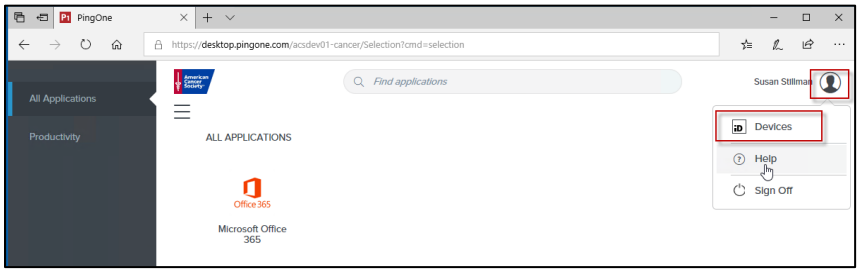


Voice

Read all the steps in these instructions before you follow them

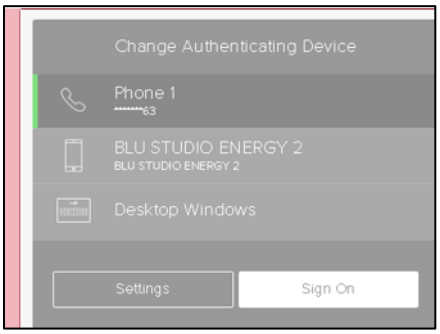
1. Follow this link https://desktop.pingone.com/ACS-Portal/ to the PingOne Portal.
2. Sign on with your usual ACS email address and password.

3. Click your profile icon, then click “Devices”.

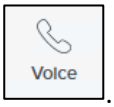


4. Click the “Add” button.

5. Authenticate.
    a. If you have not yet registered an additional method, authenticate, then go to step b. If you have already registered more than one method, you’ll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



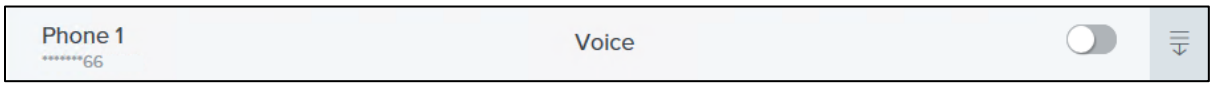
    b. This screen will appear.

6. Select 

.

7. Enter a phone number.
    a. This must be a direct dial number or mobile device that you have access to when you are using your computer. Mobile is recommended if you are a traveler. Skype phones will NOT work for this since you must authenticate to log into Skype to use the phone.
8. Wait for a call, then enter code provided.

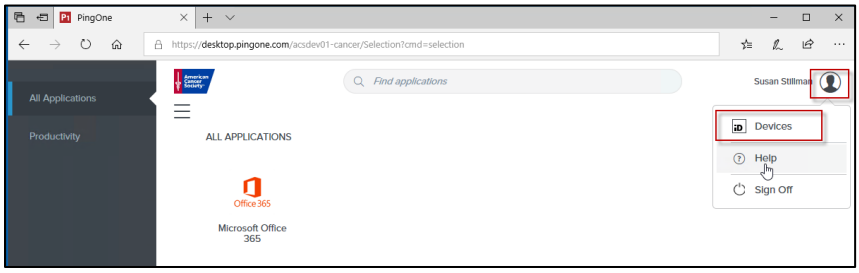
The method will be added to the device list.



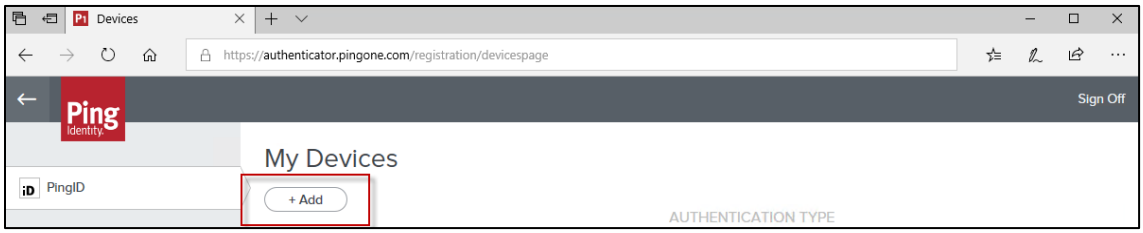
Email

Read all the steps in these instructions before you follow them

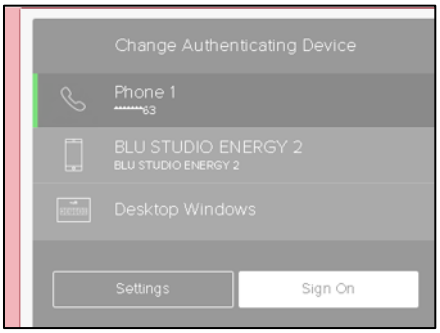
1. Follow this link https://desktop.pingone.com/ACS-Portal/ to the PingOne Portal.
2. Sign on with your usual ACS email address and password.
3. Click your profile icon, then click “Devices”.



4. Click the “Add” button.



5. Authenticate.
    a. If you have not yet registered an additional method, authenticate, then go to step b. If you have already registered more than one method, you’ll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



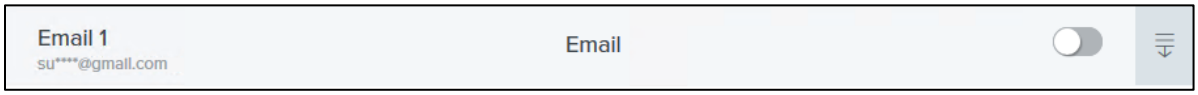
b. This screen will appear.

6. Select 

.

7. Enter the email address you wish to use for authentication.
    a. Do not use your cancer.org email address. Use an email address you can get to from your mobile device or a web browser.
8. Wait for an email, then enter the code provided.

    The method will be added to the device list.



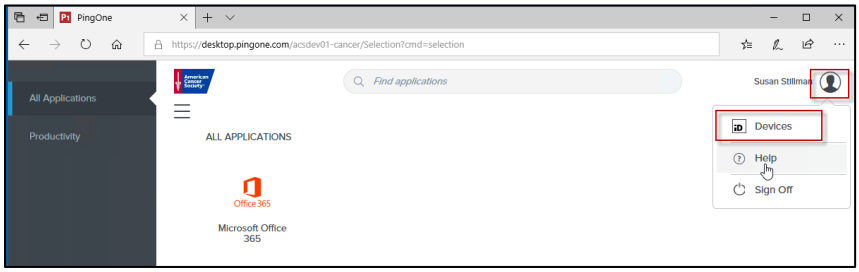
9. Sign off.

Desktop Application

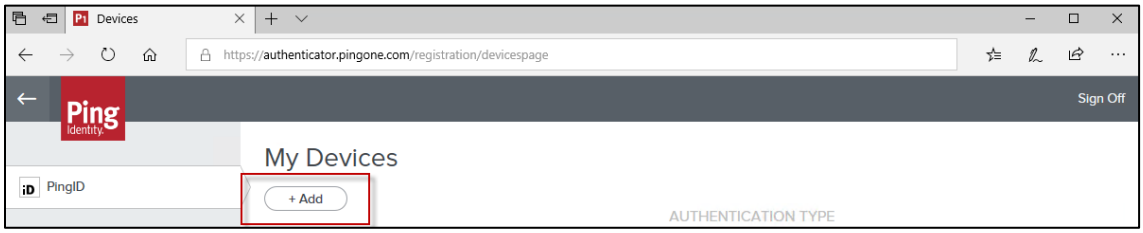
NOTE: This option is not available to volunteers.

Read all the steps in these instructions before you follow them

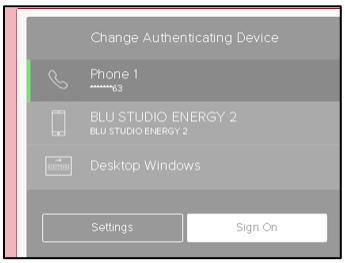
1. Follow this link https://desktop.pingone.com/ACS-Portal/ to the PingOne Portal.
2. Sign on with your usual ACS email address and password.
3. Click your profile icon, then click “Devices”.



4. Click the “Add” button.



5. Authenticate.
    a. If you have not yet registered an additional method, authenticate, then go to step b. If you have already registered more than one method, you’ll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



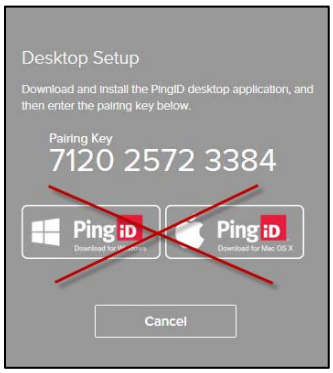
    b. This screen will appear.

6. Select 

.

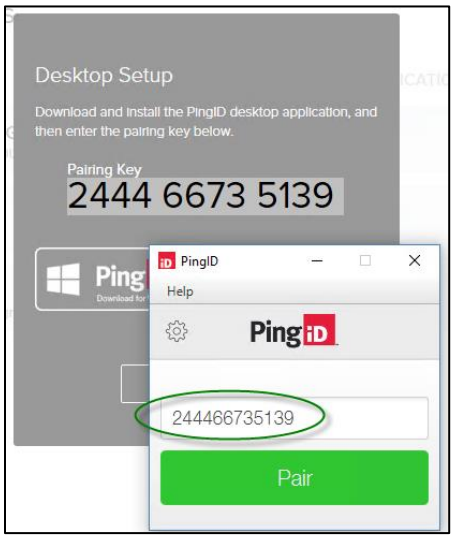
7. Copy the pairing key that appears on your screen. The pairing code on your screen will differ from the example below.

   Do **NOT** select either of the download options.

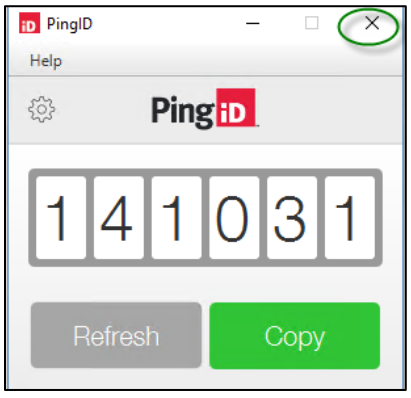


8. Open the PingID desktop app  from your desktop.

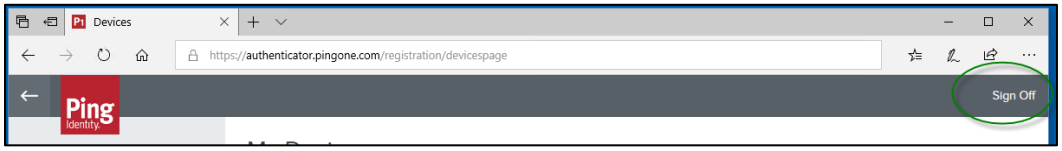
9. Paste the pairing code into the box that appears.



10. Click “Pair”.
11. Close the final box that appears.



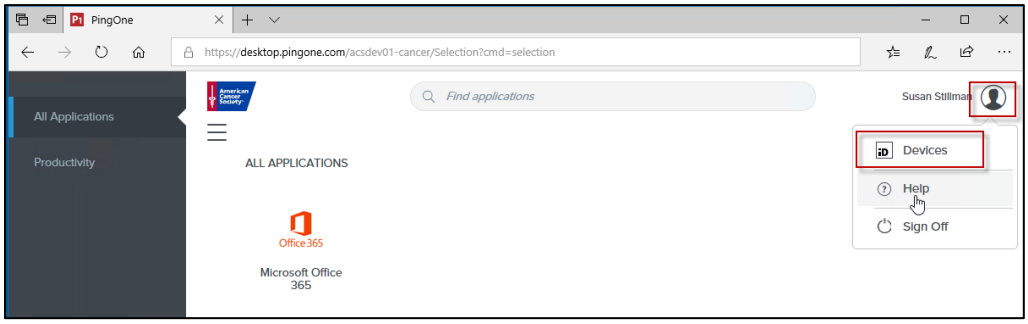
12. Sign off.



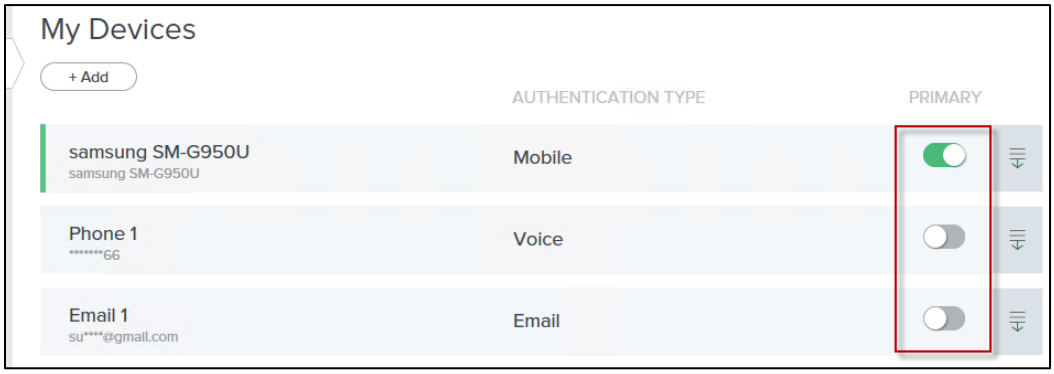
STEP 3: Set a Default Authentication Method

You must have registered at least two methods before you can perform this step. It only needs to be done if you wish to change your primary authentication method.

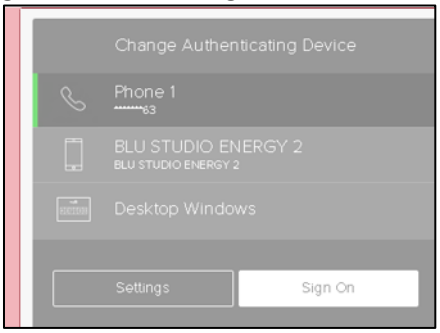
1. Follow this link https://desktop.pingone.com/ACS-Portal/ to the PingOne Portal.
2. Sign on with your usual ACS email address and password.
3. Click your profile icon, then click “Devices”.



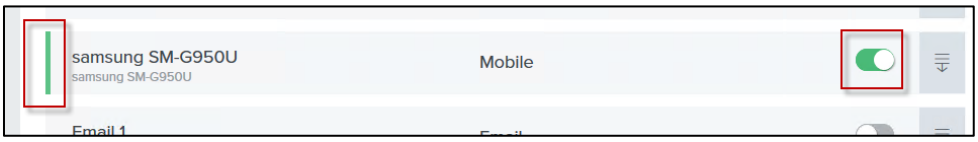
4. Click to the right of the slider for the method you wish to make primary.



5. Authenticate as directed.
   a. You’ll be asked which one you wish to use for authentication. Your default method will be preceded by a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



b. You'll return to this screen. The new default method will have a green edge to its left and the slider button background to the right will be green.



6. Sign off.

STEP 4: Authenticate

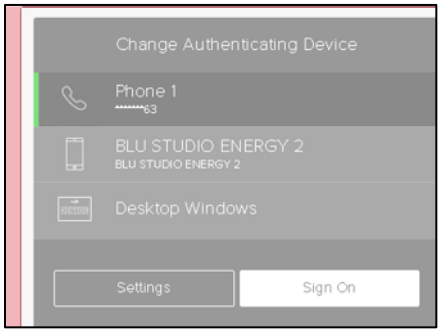
This is not a step you'll be prompted for immediately after registering your authentication methods. You may be asked to authenticate the next day, but you also may not. Microsoft can remember who you are and what computer you use. If it remembers you, you may not have to authenticate until your next password change (which happens every 90 days).

Right now, authentication applies to any Office 365 application, including Outlook, Word, Excel, PowerPoint, OneDrive, Skype for Business, OneNote, and Yammer. It applies to the applications on your computer and to the applications available online at office.com. As you attempt to access these applications, you may be presented with a message that requires you to authenticate. What you do next depends on the method you choose to authenticate with.

Mobile App

1. Access the desired Office 365 application (Outlook, Word, Excel, Skype, etc.).

   You'll be prompted to authenticate. If you have not yet registered an additional method, go to step 2. If you have already registered more than one method, you'll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click "Sign On" to use it or click another method then click "Sign On".

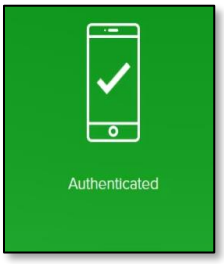


2. Go to your mobile device. The authentication app will open and display red swipe button.

3. Swipe up.

   NOTE: If you use face or fingerprint recognition on your mobile device, you may not see this swipe action screen. Your face or fingerprint recognition replaces this step.

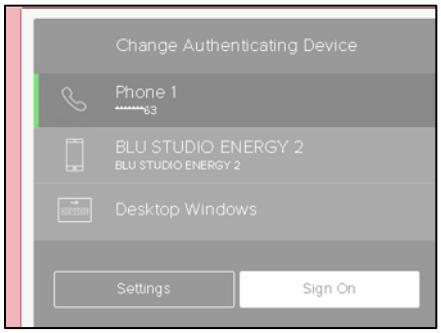
   You'll see a green success message.



Voice

1. Access the desired Office 365 application (Outlook, Word, Excel, Skype, etc.).

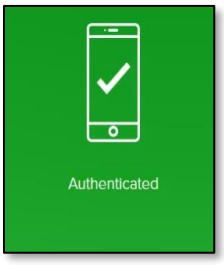
   You'll be prompted to authenticate. If you have not yet registered an additional method, go to step 2. If you have already registered more than one method, you'll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click "Sign On" to use it or click another method then click "Sign On".



2. The phone you registered will ring.
3. When answered, you'll be given the authentication code.

4. Enter the code, then click “Next”.

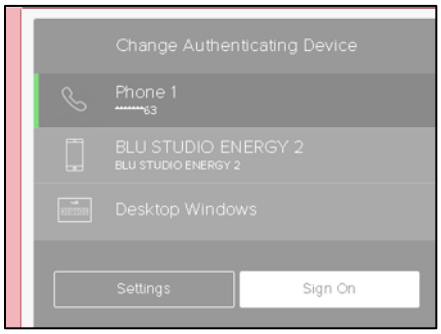
   You’ll see a green success message.



Email

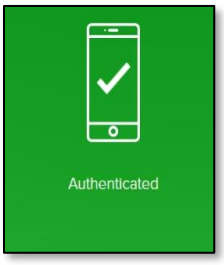
1. Access the desired Office 365 application (Outlook, Word, Excel, Skype, etc.).

   You’ll be prompted to authenticate. If you have not yet registered an additional method, go to step 2. If you have already registered more than one method, you’ll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click “Sign On” to use it or click another method then click “Sign On”.



2. Check the email address you registered.
3. Open the email that contains the authentication code.
4. Return to the window that is prompting for the code.
5. Enter the code, then click “Next”.

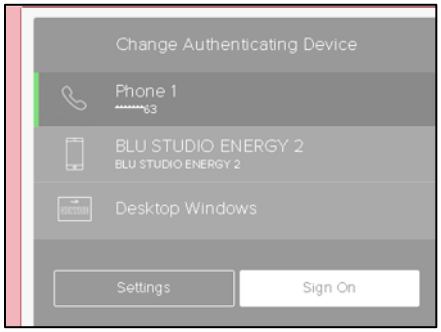
   A green success message will appear.



Desktop Application

1. Access the desired Office 365 application (Outlook, Word, Excel, Skype, etc.).

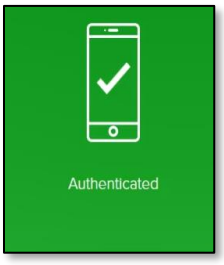
   You'll be prompted to authenticate. If you have not yet registered an additional method, go to step 2. If you have already registered more than one method, you'll be asked which one you wish to use for authentication. Your default method will be identified with a green bar. Click "Sign On" to use it or click another method then click "Sign On".



2. Open the PingID desktop application 

.
3. Click the "Copy" button.
4. Return to the window that is prompting for the code.
5. Paste the code, then click "Sign On".

   A green success message will appear.



Resources & Frequently Asked Questions

A full FAQ is available on Society Source (https://www.societysource.org/) for staff and via helpme.cancer.org for volunteers.

What if I have trouble?
As with any software or process, you can go to helpme.cancer.org and use the search bar at the top of the page to search for what you need. If you cannot find answers with search, you can try to Ask Navi, the chatbot assistant, or initiate a Live Chat with the Service Desk

What applications will require multifactor authentication?
Starting in July 2019, all Office 365 applications will require multifactor authentication. These applications are Outlook, Word, Excel, PowerPoint, OneDrive, Skype for Business, OneNote, and Yammer. This applies to the applications that are on your computer and to the applications available online at office.com.

How often will I need to authenticate?
Once you have successfully authenticated, Office 365 issues your account a digital 'token' and grants access. The typical authentication is good for 90 days, unless your security profile changes. Following are examples of changes to your security profile that will prompt you to reauthenticate: The current token expires (every 90 days), you reset your password, you start a new Office 365 session on a separate device, you start a new Office 365 session in a different web browser on the same device. Please note: the authentication period may differ for future applications added into MFA.

Once I authenticate in one application, will that authenticate me for all of them?
Yes, for most applications and roles. As noted above, logging in from another country may trigger more authentications, and some staff may need to authenticate more often than others (e.g., if you have access to highly sensitive information, etc.).

Do I have to be on the VPN to register for MFA?
No, being on the VPN is not a requirement.