Multifactor Authentication Frequently Asked Questions

May 2019

What is Multifactor Authentication (MFA) and why are we using it?

Multifactor authentication 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 seen it when interacting with the financial institutions you use. Logging in will prompt you not only for your password, but also a special code or require you to perform a specific action (this is what's known as a second factor).

Starting in July 2019, multifactor authentication is the leading tool we will use to combat unauthorized access to user accounts which are often the result of phishing attacks, which may lead to stolen data, and which have the potential to cost the Society hundreds of thousands of dollars in fines, penalties, and proactive credit monitoring services – money which would otherwise have gone to supporting the mission of the Society. The use of multifactor authentication will result in fewer incidents and attacks, and provide better protection for our emails, chats, and files in OneDrive and SharePoint. Coupled with staff's diligence and critical thinking, MFA can help make security incidents a thing of the past.

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 do I authenticate?

First, you'll attempt to access an Office 365 application. As you do this, you'll be presented with a message that requires you to authenticate. What you do next depends on the "device" you have chosen to register. A device is the method by which you will take a specific action or receive the code to offer as authentication. Devices must be set up and registered for MFA before they can be used to provide authentication. The devices we will use at ACS are mobile phone/tablet, email, voice call, or desktop application.

Mobile device: Office 365 will ask you to authenticate. At the same time, it will detect your mobile device. Very quickly you'll see a red "slider" button appear on the screen of your mobile device. You'll swipe the button up and access will be granted. This is the easiest and fastest way to authenticate.

Email: This is the next fastest way to authenticate. The application you're accessing will request a code. Shortly you'll receive an email to the address you registered. Enter the code into the authentication box, and you're in. This requires you to register an email address you can access without having to log into Outlook (since you won't be able to get into Outlook until you authenticate.

Voice: When using this method, when you access the Office 365 application you want to use, you'll receive a phone call at the number you registered. You'll be given the authentication code, which you'll then enter into the box on your computer screen.

Desktop application: With this method, when asked to authenticate, you'll run a desktop authentication application, the icon for which you'll find on the desktop of your laptop/desktop. It will provide the code, which you'll enter in the authentication code box.

How often will I need to authenticate?

Once you have successfully authenticated, Office 365 issues your account a '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.).

How do I set up a device?

All existing staff, contractors, and volunteers with a Society Office 365 account (volunteer.cancer.org email address) will be required to take Multifactor Authentication training in June 2019. Staff will take the training via Society Pathways, and all other users will complete training via the Volunteer Learning Center. New staff, contractors, and volunteers with an Office 365 account will also be assigned MFA training upon their onboarding. Upon completion of the training, users will be directed to a soon-to-be-finalized Multifactor Authentication Registration Guide and Multifactor Authentication Registration form. The training will demonstrate setting up a device. You'll then use the Guide to set up your own device.

How many devices should I set up?

You may set up a maximum of five devices, and we recommend setting up as many devices as possible. This way, should you not be able to authenticate one way (perhaps your mobile device has lost its charge), you can authenticate another way.

How do I set up additional devices?

The soon-to-be-finalized Multifactor Authentication Registration Guide will provide a section on registering additional devices.

Can we change or add MFA options?

Yes.

Why do I get an email each time I register a device?

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 device with them. If you receive this email but have not registered a device, open an urgent ticket by using Ask Navi / Live Chat at helpme.cancer.org. Be ready to provide the information contained in the registration email. If needed, Service Desk personnel will follow up with you using the phone number we have on file.

I've received an email stating I've registered a device, but I haven't registered one.

This means that someone has obtained your username and password and registered a device for MFA. If you receive this email but have not registered a device, open an urgent 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 using the phone number we have on file.

What if I lose my instructions?

The soon-to-be-finalized Multifactor Authentication Registration Guide will be available via helpme.cancer.org. Please use the search bar at the top of the page and search for what you need.

How long will the training and registration take?

The training and registration can easily be completed within 30 minutes.

What platforms and applications will have multifactor enabled in the future?

There will be more information to come on this, but several of the Navigation Tools applications are in scope.

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.

Will ACS reimburse staff for data use on personal phones for multifactor authentication?

There are no plans to reimburse staff for using personal devices to perform multifactor authentication. Staff should check with their providers regarding costs for data usage. If they work in an office, they may use the guest Wi-Fi to mitigate data costs. And if they prefer, staff can use a different authentication, such as voice call (to generate a one-time passcode), non-ACS email (to generate a one-time passcode), or a computer desktop app.

Can an NCIC front-line specialist use the computer desktop app? A smartphone would be challenging for front-line staff given the frequency of their daily logging in and out.

If staff use the computer desktop app as their chosen method of additional authentication, they can simply launch the app and enter the generated passcode into the displayed authentication window.

What about areas where smartphones and tablets are not allowed due to security? There may be few desktop phones in those areas, as well.

If the mobile device app does not function, staff can use the computer desktop app, a voice call, or a non-ACS email address as their chosen method of additional authentication.

If my laptop is not refreshed until after MFA starts, will this affect my MFA registration on the new laptop?

You will only be affected if you have selected the computer desktop app as your authentication method. If you receive a new computer afterward, you will need to pair the new computer desktop app with your Ping ID account.

With so many independent user IDs and passcodes for different systems, is there some form of tips/tricks to remembering these?

We will continue encompassing many ACS systems into single sign-on to mitigate this issue.

A Salesforce session times out every 15 minutes. Will each timeout require a new authentication?

No, the MFA rollout to Salesforce will take session timeout intervals into account.

Will MobileIron (accessing ACS email on my smartphone) be included in MFA?

If you use MobileIron to access email on your mobile device, you will not have to authenticate using MFA at this time.

I use a shared computer. How should I authenticate with MFA?

If you work on a shared computer, we recommend you authenticate via a mobile device, voice line, or non-ACS email.