Multi-Factor Authentication FAQ

What is Multi-Factor Authentication?

A: Multi-Factor Authentication is a security system that requires you to provide 2 or more pieces of authentication when logging into an application. It is a security measure that prevents an unauthorized user, who may have acquired your username and password, to log in to your account.

Is Multi-Factor Authentication mandatory to set up?

A: Yes, you need to set up your multi-factor authentication options to protect your AHS email accounts.

How many authentication options do I need to set up?

A: We **strongly recommend** that everyone sets up at least 2 different authentication options. This way if you do not have access to your primary authentication option, or you change your phone number, you will still have an option for accessing your

When will I be prompted for Multi-Factor Authentication?

A: You will be prompted for multi-factor authentication when you attempt to login to your AHS email using the Outlook Web Access app either from a non-AHS network or using an AHS device that is logged in using a shared generic ID.

If you are connecting using NetMotion you will not be prompted for multi-factor authentication.

In the future, multi-factor authentication will be expanded to other AHS web-based applications and services. You will be told in advance when these changes will happen.

Multi-Factor Authentication FAQ

How does Multi-Factor Authentication work?

A: After logging in to Outlook Web Access with your username and password, if you are not on the AHS network, or you are logged in using a shared ID, you will be prompted to authenticate by one of several methods.

What are the methods available for authentication?

A: AHS has 3 methods of verification:

1. Microsoft Authenticator – A mobile app for iOS and Android devices that enables authentication by either allowing or denying through a notification or providing a one-time pin to be inputted.
2. Receive a phone call – Set up your mobile phone or landline to receive a phone call that will prompt you to allow or deny access.
3. Text message – Set up a mobile phone to receive text message with a code to authenticate with.

What is the recommended method of authentication?

A: The Microsoft Authenticator app is recommended as the primary method of authentication for those with access to a mobile device.

Can I use more than one method of authentication?

A: Yes! AHS recommends that you set up any of the available methods of authentication. You will select your primary authentication method that will automatically be contacted when you attempt to login. If your primary option is not available, you can choose to use any of the other authentication options you have set up at any time.

What happens if I don't have my primary authentication option available when I am logging in?

A: If you have set up multiple authentication methods you will be able to select a method that you do have access to. If you don't have access to any of your authentication methods, you will need to contact the Service Desk for assistance.

What happens if I change my phone number or mobile device?

A: You can change your authentication methods at any time by going to https://mysignins.microsoft.com/security-info here you can add or delete methods and change your primary authentication method at any time. You will need to be either logged in on the AHS network or have an existing authentication method available to make changes.

What if I don't have a phone line or mobile device I can use for authentication?

A: Multi-Factor Authentication is initially required for accessing your AHS email remotely. If you have business requirement to access your AHS email remotely and do not have a mobile device or phone line you can use, please talk to your manager to discuss other options.

Multi-Factor Authentication FAQ

Can I use the same phone number as my Office, Phone and Alternate phone methods?

A: The alternate phone number needs to be a different phone line than the one used to set up the Phone or Office Phone options. Only use a phone number once.

What happens if I get an authentication request and I am not trying to connect to my AHS email?

A: If you get an unexpected request to authenticate a login to your account **DO NOT** allow access. If you are notified through the authenticator app or receive a phone call use the options for denying access. Report the attempted to access your account to the Service Desk at the earliest opportunity.