Multi-Factor Authentication – FAQ

GENERAL QUESTIONS

Multi-Factor authentication

SAIT is deploying Multi-factor Authentication (MFA) to most applications for faculty, staff and students.

Currently, SAIT M365 accounts only require a username and password to gain access to applications. When the password is compromised, anyone using that username and password will have access to all the applications and data the rightful user is entitled to have.

What this will mean is that when SAIT end users access the Microsoft 365 suite of products through their SAIT credentials, individuals will be required to set up multi-factor authentication to confirm they are who they say they are.

This will include applications such as the following:

- Mail and Calendar applications including Microsoft Outlook,
- Outlook Web Access,
- Microsoft 365 applications: Word, Excel, PowerPoint Microsoft OneDrive for Business
- Microsoft Teams, SharePoint
- Other SAIT authorized Apps from the Microsoft portal

Informational Video: What is: Multifactor Authentication (microsoft.com)

What is Multi-Factor authentication (MFA)?

Multi-factor authentication (MFA) is a method of authentication that requires the end user to provide two methods of evidence to prove their identity to gain access to M365 products at SAIT. It works by requiring any two of the following verification methods:

- Your SAIT login credentials account and password used to log into your computer (i.e., for students: firstname.lastname.@edu.SAIT.ca or for employees/contractors: firstname.lastname.@sait.ca).
- A secondary authentication method (e.g., a verification code sent via text to your mobile phone, a phone call or an app on your smart phone)

Why is SAIT using Multi-Factor Authentication?

Implementing MFA has many benefits including enhancing SAIT's security. By requiring users to identify themselves by more than a username and password, we significantly reduce the risk of malicious attacks and cyber identity theft.

MFA reduces the risk of a security breach and sensitive data stays protected. It also ensures security for personal, institutional and research data. The reality is that with any organization including SAIT, employees do fall for phishing scams and do share passwords. If SAIT does not roll out MFA, we are wide open to attacks and one of the biggest security threats today is the risk of compromised credentials.

Who needs to set up MFA?

All faculty, staff, students, and contractors (or anyone using a SAIT email address) will be enrolled in MFA.

When wil new M365 end-users be added to MFA?

Once a stakeholder group (e.g., department, school, or group such as students) are added to MFA, new individuals starting at SAIT who are part of that stakeholder group will automatically be enrolled in MFA.

USING MFA

What are the methods for setting up MFA?

You can set-up MFA using one of four methods below:

- The Microsoft Authenticator mobile app, either using push notification or generating an authentication code
- Accept a call on your mobile phone
- Receive a text to your mobile phone, with an authentication code
- Accept a call to a desk phone (you will need access to this phone)

Be careful to only accept authentication requests when you are actively signing into your account (entering your password). Do not accept a request if you are not actively signing into your account.

What to expect?

When setting up MFA you will be prompted to set up your chosen authentication method. You will be asked to accept an authentication request (or provide a code) from your chosen method. Second factor authentication will also be required when logging in from a new device (or a different location) and may be required to access systems that are authenticated through Microsoft 365.

Set up includes 3 tasks:

- Task 1: Activate Multi-Factor Authentication (MFA)
- Task 2: Enroll in Multi-Factor Authentication
- Task 3: Receive digital code and input into pop-up screen
- Proceed to access M365 applications

What is the preferred method of verification to use?

SAIT recommends installing and using the **Microsoft Authenticator** mobile app, as it provides both online push notifications and offline authentication code options for sign-in, which is useful if you are travelling abroad without data. If you do not have a smartphone, then a call or text message to your mobile phone is the next best option.

The Microsoft Authenticator takes up very little space on your phone, cannot control your device, and you can choose to use the app without using your data plan.

Will MFA apply to shared mailboxes?

MFA will be applied to the individual users who access the shared mailbox, not the mailbox email itself.

What email and calendar applications support MFA?

Multi-factor authentication is supported with the following email and calendar apps:

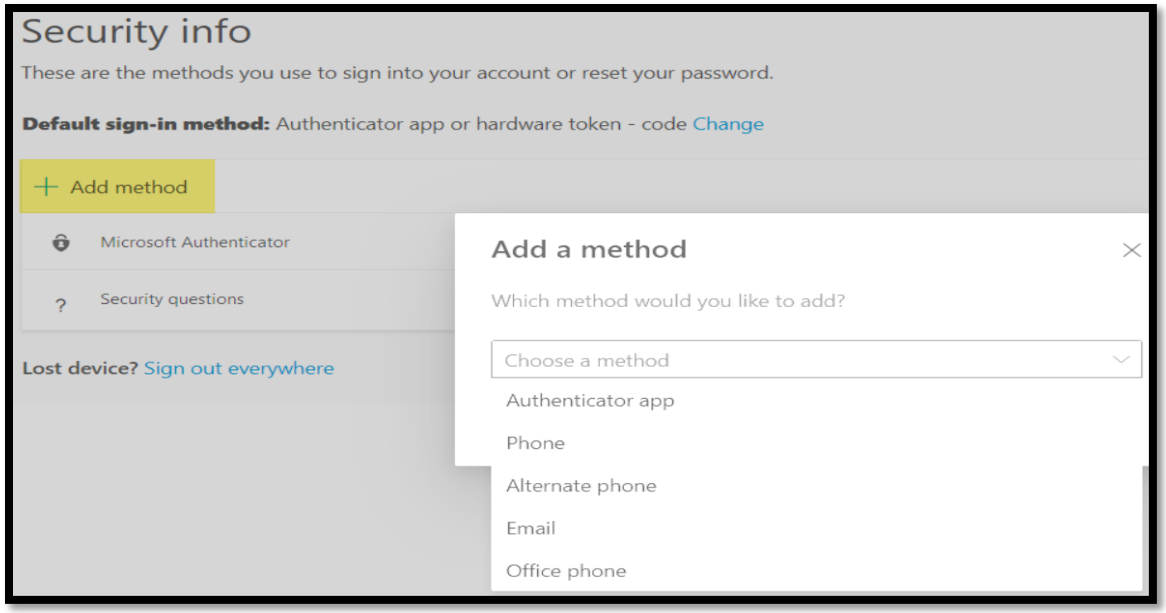
- Outlook 2016, 2019, and 365 for Windows and Mac
- Outlook for iPhone and iPad
- Outlook for Android phones and tablets
- Outlook Web Access
- Apple Mail and Calendar for iPhone (iOS 11 or later), iPad (iOS 11 or later, or iPadOS), and Mac (High Sierra or later) *
- Android Mail and GMail (Android 10 or later) *
- Mail for Windows 10

If your device does not support one of the above applications, consider, using Outlook Web Access instead.

* Using non-outlook apps may require you to remove and re-add your account to enable MFA, depending on how you set your device up.

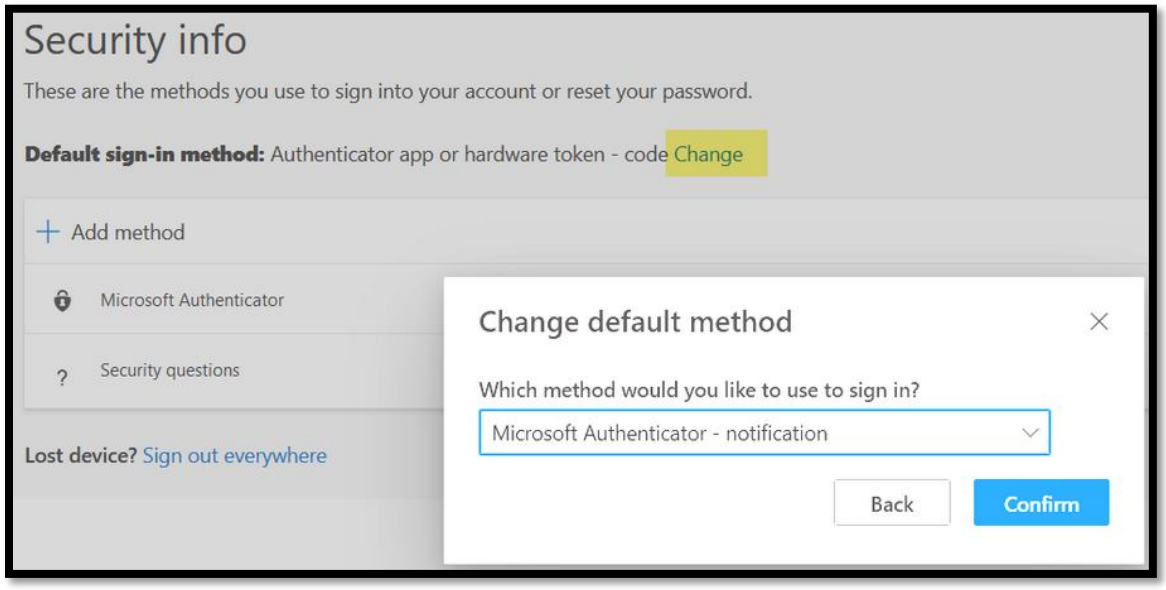
How do I add a second multi factor method?

- Please go to Microsoft Sign-ins security page
- Select **"Add method"** at the top of the options box.
- You can then choose from a selection of methods.
- see screen shot below for guidance



How do I change my current multi-factor authentication method?

- Please go to [Microsoft Sign-ins security page]
- Select **"Change"** next to **"Default sign-in method: Microsoft Authenticator - notification Change"**
- Change default method to **"Microsoft Authenticator - notification"**.
- See screen shot below for guidance:



HOW TO RESOLVE MFA CONCERNS

What issues could I run into when registering MFA?

If using your desktop or laptop, it is recommended that you close all apps, browsers and tabs when initially setting up MFA to avoid being prompted to authenticate for each Microsoft 365 session that is open.

If using a mobile device as your second authentication, and you are being asked to MFA multiple times, close the application on your mobile device and relaunch the application to re-initialize MFA.

Why was I not prompted to authenticate?

If you are working on SAIT Campus on the day of an MFA rollout, you will NOT be prompted to authenticate. Once you log in from a non-SAIT IP address, you will be prompted to complete the authentication process.

What should I do when I get a verification request, I don't recognize?

If you receive approval requests for access to your MFA applications and you are not actively signing in (entering your password), then **deny the access.** If this occurs frequently, your account password may be compromised.

In this case, please contact the ITS Service Desk at https://sait.ca/ITS, by email at ITS.ServiceDesk@sait.ca or by phone at 403.774.5200.

Can password sharing occur with MFA?

The fundamental rule to keep our data secure is not to share your passwords.

If you do share your password, keep in mind that with MFA, an authorization attempt will be sent to your personal device which only you will have access to. This means that the person who is also using your login credentials will be unable to access your account.

If you are sharing your password for the purposes of enabling someone to assist you in managing your email and calendar, it is advisable to use alternative methods such as:

- Sharing your calendar in Outlook properties
- Sharing your email in Outlook properties
- Setting up a delegate in systems

What if my phone is lost or stolen?

If your phone is lost/stolen or access to the application is lost, users can receive a recovery key from the Service Desk.

Can MFA control my phone and monitor me?

Simply put, the answer is "No". The Microsoft Authenticator app is not owned by SAIT. SAIT is not granted any information from it, and the app is not able to collect information about the phone to send to Microsoft. It also does not have a Mobile Device Management (MDM) component, so it will not attempt to manage the phone.

Who will my information be shared with?

The Microsoft Authenticator app is not owned by SAIT. SAIT is not granted any information from the app, and the app is not able to collect information about the phone to send to Microsoft. The application retains the email address for verification and sends a digital code for the second verification.

Will I have to enter a 2nd MFA every time I access SAIT MFA based applications?

No. When you sign in with a new device (e.g., phone or another computer) you will be asked to verify who you are and enter the digital code.

If you log off and log back in or if you lose your internet connection, you will need to reauthenticate by entering the digital code.

You may be required to reauthenticate if SAIT deems necessary.

If the MFA system deems the login to be questionable, such as impossible travel – log into a device in Calgary, and then log into another device somewhere else around the world, you will be required to reauthenticate by entering the digital code.

Is MFA required when on Campus?

MFA will NOT be required if the user is on Campus and is using an internal IP address. Users will only be required to authenticate with MFA from an external IP address.

I'm using an unsupported email client, what should I do after enabling MFA?

Email software clients such as Mozilla, Thunderbird, Apple Mail, Outlook 2010 and older, Outlook 2011 for Mac, and Android Mail (Android 9 and older) do not support Office 365/Exchange and require IMAP connection to the O365 server to retrieve emails.

What do I do if my emails do not sync with my mobile app after MFA is launched?

Some users may not be able to sync their apple or android mail emails on a native mail app after MFA is enabled. In this case, deleting and re-adding the email account should work.

If that still doesn't work, use the Microsoft Outlook app to sync emails on your phone. It creates a much more secure connection.

What if I am traveling internationally?

If you have an international mobile plan, the Microsoft Authenticator app will work. Otherwise, when you are prompted for MFA, click on Sign in another way. From there, select Use a verification code from my mobile app, you will then be prompted to enter a code. Open the Microsoft Authenticator app and enter the 6-digit code into your login screen.

DELEGATE ACCESS FAQ's

How do I setup Delegate Access?

Delegator - Person delegating access to another:

- Go to outlook
- Click the file tab
- Click Account settings and then click delegate access
- Click Add
- Type the name of the person whom you want to designate as your delegate
- Click Add and then click OK
- In the Delegate Permissions dialog box, accept the default permission settings or select custom access levels as desired
- To notify the delegate of the changed permissions, select the "Automatically send a message to delegate summarizing these permissions check box.

This setting affects ALL exchange folders. This includes all Mail, Contacts, Calendar, tasks, notes and journal folders.

- Click OK
- Select Add and select the employee you want to grant access. Add permission access.

Delegate - Person who is delegated access:

- Go to outlook
- Click the file tab
- Click Account settings and then double click on email address
- Click on more settings and then choose advanced
- Under open additional mailbox, please enter the leader's email you are receiving access to

See link for setup:
Allow someone else to manage your mail and calendar (microsoft.com)

For additional technical support, please contact the ITS Service Desk at https://sait.ca/ITS, by email at ITS.Support@sait.ca or by phone at 403.774.5200 to reset your MFA method.