

Multi-Factor Authentication (MFA)

Frequently Asked Questions

1. What is MFA?

Multi-Factor Authentication (MFA) is a security tool that requires you to verify your identity in more than one way when logging into the College systems. When entering your College issued username and password, you will be prompted to confirm your identity with a code from the Microsoft Authenticator App, a text message, or a phone call.

Think of it as adding a deadbolt to your front door: your password is the key, but the second factor is the extra lock that keeps intruders out.

2. Why is the College requiring MFA?

Cybersecurity threats against higher education are growing rapidly. Colleges store valuable information such as:

- **For students:** grades, financial aid details, health information, housing records.
- **For faculty:** research data, course content, advising records, personal information.
- **For staff:** payroll data, HR files, institutional financial systems.

Hackers target colleges not only for sensitive information but also to disrupt teaching, learning, and operations. MFA dramatically reduces the risk of stolen accounts and keeps your personal information, academic work, and the College's reputation safe.

3. Who does this affect?

Everyone at the College: **faculty, staff, and students.**

- **Students** will use MFA when checking email, accessing cloud storage, registering for classes, applying for financial aid, and submitting assignments in the learning management system (LMS).
- **Faculty** will use MFA when accessing email, accessing cloud storage, grading in the LMS, submitting timesheets, and logging into research or advising tools.

- **Staff** will use MFA when accessing payroll, HR systems, budgets, and administrative applications.
-

4. How does MFA work day-to-day?

1. Log in with your College username and password.
2. Confirm your identity with **Microsoft Authenticator** (the College's required authentication app).
 - After downloading the free Microsoft Authenticator app to your phone, you'll receive either:
 - A **push notification** you simply approve, or
 - A **6-digit code** you type in.
3. If you do not have the app available, you may also use a text message or phone call as a backup.

It usually takes less than 10 seconds. If you check the "Remember me" option on your trusted device, you won't be prompted again for 30 days.

5. Do I have to use MFA every time I log in?

Not every time. You'll be asked for MFA if:

- You're logging in from a new device (such as a friend's computer).
- You clear your browser cache or cookies.
- You're using a public computer.
- OIT security policies require re-checking.

On your personal laptop or phone, once you've confirmed your identity through Microsoft Authenticator, you may not be asked again for 30 days.

6. What if I don't have my phone with me?

There are options:

- **Set up more than one verification method** (for example, add both the Microsoft Authenticator app and a backup phone number).
 - **Use text or phone call backup** to receive your login code.
 - If you're locked out, **call the OIT Helpdesk** and we can help you securely regain access.
-

7. What if I get a new phone or lose my old one?

Contact the OIT Helpdesk. We'll help you reset MFA and reconnect your new phone with the Microsoft Authenticator app. Be sure to reach out as soon as possible so you don't lose access to essential College systems.

8. Can I opt out of MFA?

No. MFA is required for all College accounts to ensure the protection of our community. This is part of our responsibility to safeguard sensitive academic, financial, and personal information, and to comply with state and federal cybersecurity requirements.

9. Which systems will require MFA?

- **Faculty & Staff:** Email, VPN/remote access, HR/payroll, Finance systems, advising tools, research databases, and other administrative systems.
 - **Students:** Email, learning management system (LMS), registration, financial aid, housing, library accounts, and student portal.
-


10. What if I get an MFA prompt I wasn't expecting?


If you receive an MFA notification in Microsoft Authenticator when you are **not** trying to log in, **deny the request immediately** and contact OIT. This could mean someone has stolen your password and is attempting to access your account. MFA helps stop them — but only if you don't approve the fraudulent request.

11. Who do I contact if I need help?

Reach out to the **Office of Information Technology (OIT) Helpdesk:**

 itsupport@smcm.edu

 240.895.4357

 Visit the OIT website for step-by-step guides and instructions.

💡 **Remember:** MFA with Microsoft Authenticator protects more than just your account — it protects your grades, your pay, your research, and the College's mission. A few extra seconds keep our entire community safe.
