

HCC Student MFA FAQ

Category: Account Setup & Enrollment

Question: What is MFA and why do I need it?

Answer: Multi-Factor Authentication (MFA) adds an extra layer of security to your account by requiring something you know (your password) and something you have (like your phone). It helps protect your student account from unauthorized access.

Question: When will I be required to set up MFA?

Answer: You will be prompted to configure your devices for MFA between May 5th – May 17th. MFA authentication will be required starting May 18th.

Question: How do I start setting up MFA?

Answer: You will be prompted when you login to <https://portal.microsoft.com>, follow the on-screen instructions to register an authentication method such as Microsoft Authenticator or SMS. If you are not prompted on login, you can go to <https://aka.ms/mfasetup> to directly setup Microsoft MFA.

Question: Do I need a smartphone to use MFA?

Answer: No. If you don't have a smartphone, you can use any device that accepts SMS text messages.

Question: Can I skip MFA setup?

Answer: No. MFA is required under the HCC security policy to access the Microsoft online services and applications.

Category: Daily MFA Usage

Question: How often will I have to use MFA?

Answer: You will be prompted based on system requirements and security conditions when signing in. These conditions change based on various factors (for example, location when logging in, different devices, how often you login, etc).

Question: Do I have to use MFA when I log into Canvas or the Student Registration System?

Answer: No. At this time, MFA will only be required when accessing Microsoft online services and applications.

Question: Can I choose my default MFA method?

Answer: Yes. You can manage your preferred method in your security settings after setup.

Question: Can I use MFA on multiple devices?

Answer: Yes, depending on the method. For example, Authenticator can be installed on multiple devices.

Question: Can I log into multiple apps using MFA?

Answer: Yes. MFA applies when accessing supported HCC systems and Microsoft services.

Question: What if I am traveling internationally?

Answer: Ensure you have multiple MFA methods set up before traveling. Authenticator would be a preferred method to not incur international SMS charges.

Question: Can MFA work on shared computers?

Answer: Yes, but always log out and avoid saving credentials.

Category: Authentication Methods

Question: What MFA methods can I use?

Answer: You can use Microsoft Authenticator or SMS text messages.

Question: Can I use Google Authenticator (or some other non-Microsoft Authenticator) for MFA?

Answer: No. The HCC policy only allows Microsoft Authenticator.

Question: What is Microsoft Authenticator?

Answer: It is a mobile app that helps verify your identity using push notifications or verification codes.

Question: What is SMS authentication?

Answer: This method sends a one-time code to your phone via text message that you enter during login.

Category: Basic Troubleshooting

Question: I'm stuck during setup. What should I do?

Answer: Follow the instructions on <https://mfa.hccs.edu> or call 713-718-8800 (Select Option 6) for MFA assistance.

Question: I'm not receiving my MFA code. What should I do?

Answer: Try using another registered method if available. If the issue continues, call the HCC Service Desk at 713-718-8800.

Question: My phone doesn't get notifications from Authenticator. What can I do?

Answer: Ensure notifications are enabled for the app.

Question: I don't have my phone with me. Can I still log in?

Answer: If you do not have access to any MFA method, please contact IT Service Desk to get a temporary passcode for short-term login until you have access to your phone.

Question: What happens if I don't complete MFA setup?

Answer: You will not be able to access Microsoft online services or applications until MFA is configured.

Question: What happens if I lose access to my phone number?

Answer: Contact the HCC Service Desk at 713-718-8800 and someone will assist you with this issue.

Category: Device Changes & Recovery

Question: I upgraded my phone and now can't log in. What should I do?

Answer: Contact the HCC Service Desk at 713-718-8800 to reset your MFA so you can reconfigure it on your new phone.

Question: I lost my phone. How do I get back into my account?

Answer: Use another authentication method if available. Otherwise, contact support to reset your MFA settings.

Question: Can I transfer MFA to a new phone?

Answer: You must reconfigure MFA on the new device. Contact IT Service Desk for assistance with this change.

Question: Can I change my phone number for SMS MFA?

Answer: Yes, you can update it through your security info settings or contact support if needed.

Category: Troubleshooting & Access Issues

Question: My SMS codes are delayed. What should I do?

Answer: First reboot the mobile phone. If the issues still persists, try another MFA method or wait briefly and retry. If the issue persists, contact IT Service Desk.

Question: What if all my MFA methods fail?

Answer: Contact the HCC Service Desk immediately to reset your MFA.

Question: Where can I get more help or documentation?

Answer: Visit <https://mfa.hccs.edu> or call 713-718-8800 for support.

Category: Security Awareness

Question: I keep getting MFA prompts I didn't initiate.

Answer: **Do NOT approve those requests.** This could indicate a security issue. **HCC IT will never reach out to you and request the MFA code.** Change your password and contact IT Security immediately.

Question: Will MFA stop hackers completely?

Answer: MFA greatly reduces risk but does not eliminate all threats.

Question: Is my personal data visible to HCC through MFA?

Answer: MFA does not grant access to your personal data. It only verifies your identity.

Question: Why does MFA make my account more secure?

Answer: It prevents access even if your password is compromised.

Question: What is MFA fatigue?

Answer: It is when attackers repeatedly send MFA prompts hoping you approve one. If you are experiencing this issue, please contact IT Security.

Question: How should I respond to suspicious MFA requests?

Answer: Deny them and report the activity immediately to IT Security.