Multi-Factor Authentication

Columbus State University will **NEVER** ask for your password or MFA information. **Do not** provide this information to anyone.

Be aware of phishing attempts asking for this information. Columbus State University will never ask you to verify or cancel account changes through an external form or suspicious links. **Please do not click any links or respond to these message.** Common phishing attempts to gain access to this information include threats of account termination/deletion or prompts to click a link to provide this information.

Columbus State University utilizes Multi-Factor Authentication (MFA) while logging into CSU services, such as MyCSU, CougarVIEW, and more. To provide an extra layer of security, the University System of Georgia requires that all students, faculty, and staff use MFA when authenticating to campus applications and services.

Users will be required to provide additional verification when signing in to any MFA-protected application through the use of the Microsoft Authenticator mobile application, by receiving a phone call, or by receiving a text message with an authorization passcode.

Register for MFA

Please see our frequently asked questions section below if you have any questions about using MFA at CSU, or contact the CSU HelpDesk at 706-507-8199 or at helpdesk@columbusstate.edu if you have any issues.

Please Note: The CSU HelpDesk only assists with MFA issues from Monday to Friday, 8 AM to 5 PM.

Download the Microsoft Authenticator App

Download the Microsoft Authenticator app from the Google Play and Apple App Store.

MFA Enrollment Process

Enrolling your device in MFA is extremely easy. You can view our instructions below.

- Setting up the Microsoft Authenticator app
- Setting up a mobile device
- Setting up an office phone

Managing Your Authentication Devices

Adding or removing devices from your account is simple.

- Change your two-factor verification method and settings

Frequently Asked Questions

Why is CSU using MFA?
Multi-factor authentication is required and actively used by the University System of Georgia and member institutions. It adds a second layer of security, keeping your account secure even if your password is compromised. With MFA, you'll be alerted right away via the application if someone is trying to log in to your account.

Can I opt-out of using MFA at CSU?

No. The use of the service is mandated by the University System of Georgia. All students, faculty, and staff are required to use multi-factor authentication to authenticate to campus applications and services (MyCSU, CougarVIEW, OneUSG Connect, and more). Enrolling in MFA helps protect your account as well as university and personal data.

What authentication methods are available through MFA?
MFA offers several methods of providing two-factor authentication based on your device:

Smartphones

- Push Notification (via Microsoft Authenticator app) - Recommended
- Passcodes
- Phone Call

Traditional Cellphone/"Feature Phones"

- Passcodes (Only via SMS)
- Phone Call

Tablets

- Push Notification (via Microsoft Authenticator app) - Recommended
- Passcodes

Landline Phones

- Phone Call

What devices are compatible with the Microsoft Authenticator app?
The Microsoft Authenticator app is currently compatible with the following devices:

Apple Devices:

- iPhone - Requires iOS 11.0 or later.
- iPad - Requires iPad OS 11.0 or later.
- iPod touch - Requires iOS 11.0 or later.

Android Devices:

- Requires Android 6.0 and up

Can I use my office phone?
You can use a landline phone, such as your office phone, but please be aware that you will need access to this device in order to authenticate to MFA-protected applications. We recommend that you have an alternative device, such as a cell phone or tablet, to ensure that you can access MFA-protected applications while out of the office, such as at home or on trips.

I got a new mobile phone/tablet. How do I authenticate to my account?
If you have registered an alternate authentication method, such as a landline phone, you can use that method to authenticate to Microsoft's authentication setup page and add your new device. If you do not have an alternate authentication method, please contact the CSU Help Desk at 706-507-8199 or helpdesk@columbusstate.edu for assistance adding your new device as a new authentication method.

What if I lose my phone/tablet or my device is stolen?
Please contact the CSU HelpDesk at 706-507-8199 or helpdesk@columbusstate.edu. The CSU HelpDesk can provide a temporary bypass or create an alternate authentication method. If your device is stolen, please contact the CSU HelpDesk

as soon as possible to prevent unauthorized access to your account. We highly recommend having an additional device on your account to ensure that you maintain access to your account even if your primary device is lost or stolen.

What should I do if I get an authentication request and I am not trying to log in?
Deny the request and report the incident to the CSU HelpDesk immediately by calling the CSU Help Desk at 706-507-8199.

How do I enroll more than one device in MFA?
It is important to enroll more than one device (such as a smartphone and desk phone) in MFA to avoid difficulties authenticating if you lose or do not have your only enrolled device with you. To add multiple devices:

- Log into Microsoft's additional security verification page and authenticate with your current device.
- Update your settings under "how would you like to respond?" and click on "Save."

Will MFA ask for my password?
MFA will never ask for your user ID and password. If you receive such a request, do not respond.

What if I am in a location that does not have cellular or WiFi service?
The Microsoft Authenticator app can be used without cellular or WiFi service by generating passcodes within the app. Simply choose the Enter a Passcode option when you get the MFA authentication prompt. To generate the passcode, open the Microsoft Authenticator app on your phone and tap on your account in the list. If you do not have access to the Microsoft Authenticator app, please contact the CSU Help Desk at 706-507-8199 or helpdesk@columbusstate.edu to receive a unique, temporary bypass code.

Will the CSU Help Desk ever ask for my Microsoft Authenticator passcode?
No. The CSU HelpDesk will never ask for your password nor your Microsoft Authenticator passcode provided by the Microsoft Authenticator app or via SMS. If you receive such a request, please do not respond as this request may not be legitimate and may possibly be an attempt to gain unauthorized access to your account.

The CSU HelpDesk may send a legitimate Microsoft Authenticator prompt to your phone when you are requesting assistance as a way to verify your identity. This prompt will contain a support request message and a confirmation code that the CSU HelpDesk may ask for when verifying your identity.

What data is collected/retained by MFA and the Microsoft Authenticator app?
The Microsoft Authenticator app collects three types of information:

- Account info you provide when you add your account. This data can be removed by removing your account.
- Diagnostic log data that stays only in the app until you Send feedback in the app's#top menu to send logs to Microsoft. These logs can contain personal data such as email addresses, server addresses, or IP addresses. They also can contain device data such as device name and operating system version. Any personal data collected is limited to info needed to help troubleshoot app issues. You can browse these log files in the app at any time to see the info being gathered. If you send your log files, Authentication app engineers will use them only to troubleshoot customer-reported issues.
- Non-personally identifiable usage data, such "started add account flow/successfully added account," or "notification approved." This data is an integral part of our engineering decisions. Your usage helps us determine where we can improve the apps in ways that are important to you. You see a notification of this data collection when you use the app for the first time. It informs you that it can be turned off on the app's#Settings#page. You can turn this setting on or off at any time.

I already use the Microsoft Authenticator app for another university/business. Do I have to install it again?
You can have multiple accounts registered to the same Microsoft Authenticator app without any problems. Simply follow the directions on the MFA enrollment process to add your Columbus State University account to your existing Microsoft Authenticator app.