Secure Login – Multi-Factor Authentication (MFA)

Strong passwords are essential, but they aren't enough. Phishing attacks and data breaches put your account at risk. Muti-Factor Authentication (MFA) provides extra security for your Geneseo Account. Some services and websites refer to this as two-step authentication, two-step verification, multi-factor authentication, or login verification.

With MFA, anyone trying to access your account must provide two forms of ID:

- Something you know, such as your password.
- Something you have, such as a passcode, a phone, or even a mobile app.

Enrollment

You are encouraged to self-enroll in MFA before April 1, 2020 when all accounts will be required to use multiple authentication methods. As an incentive, once you sign up for MFA you can change your password one last time and then keep it as long as you'd like. **No more mandatory annual password changes!**

Click the image to opt-in now!

Note that if you have already set up methods of authentication for Self Service Password Reset, you will simply be asked to provide authentication.

Resource: Microsoft Guide - Set up your Security info

Authentication Methods

There are several available options for authenticating with MFA - you can use your mobile device, your desk phone, or a security fob.

> ⚠ We suggest that you also configure your desktop work phone as a secondary MFA option to ensure access if you don't have access to your mobile device.

Authenticator App

The free Microsoft Authenticator app is our recommended way to authenticate. It is the fastest and easiest way to verify your identity. It is available for iOS and Android devices. This authentication method works by sending a "push" notification to your device to verify your login attempt. It also provides a rotating code you can type in if you are in an area you cannot receive push notifications or don't have wireless service.

Phone Verification

When you select phone calls as your verification method, you will get a call to the number you provided. Follow the instructions to provide authentication.

Text (SMS) Message

The text (SMS) message will contain a code that can be entered in the login window to provide authentication.

Web Browser Extension

If you do not have access to a mobile phone, you can install a web browser extension in Google Chrome or Firefox. The extension generates a code which you can then use to verify your identity. Please reference this wiki article on how to add the extension to your web browser Web Browser MFA Authenticator Extensions

Security Fob

If you do not have access to a mobile phone or desk phone, your department can purchase a security fob. The security fobs are small (about the size of a car key fob). Press the button on the fob to generate a number that can be typed in to the authentication screen to confirm your login. *Please note - hardware tokens must be purchased from CIT for $16. Third party hardware tokens are not supported.

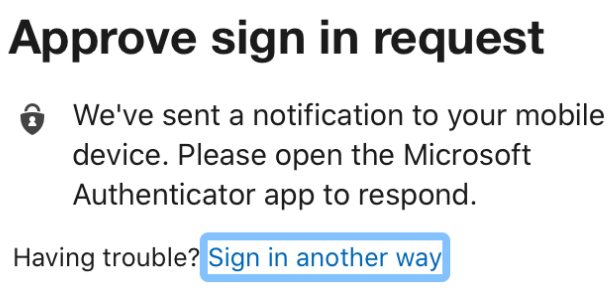
Troubleshooting and Questions

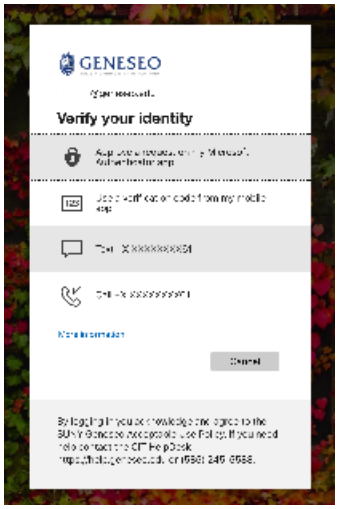
We are required to use MFA by new SUNY security guidelines. Our systems are under constant attack. The most common are password spray attacks where attackers send thousands of logins using usernames and passwords harvested from the web to phishing attacks where attackers attempt to get your username and password. Multi-factor Authentication stops all these attacks.

If you would like a detailed analysis of how MFA protects logins Your Pa$$word Doesn't Matter lays out Microsoft's research across millions of logins explaining why passwords are insecure and how MFA results in protecting against all but the most targeted attacks.

Logins to most Geneseo web based services and Microsoft's OneDrive and Office will require you to sign in and use MFA at least every 14 days. Sign in frequency varies between services based on security and vendor requirements.

When prompted to sign in, click on the **Sign in another way** button and select a new method.





You should notify the CIT HelpDesk as soon as possible if you lose your phone or authenticator.

Yes. Using a device for multi-factor login comes with the obligation to take reasonable precaution to protect it. Such precautions normally include the use of a password or a PIN to unlock the phone, as well as maintaining current versions of your device's operating system and Authenticator App.

Yes. Third-party apps such as 1Password, Authy, or Google Authenticator can be used as a software token to generate an OATH verification code. Users may have a combination of up to five OATH hardware tokens or authenticator applications such as the Microsoft Authenticator app configured for use at any time.

Follow our directions here How-To Manage your Multi-Factor Authentication Settings

Resource: https://docs.microsoft.com/en-us/azure/active-directory/user-help/security-info-setup-auth-app

You should report all messages that you did not generate. This may be a sign of someone attempting unauthorized access to your account, and your password may be compromised. Deny the notification and then confirm that it's a fraudulent attempt. You should change your Geneseo password if this occurs.

The Microsoft Authenticator needs access to your camera to take a picture of the QR code (the weird barcode looking square) on your screen. It does not use camera access for anything else.

The Microsoft authenticator does not track you and it does not log location data. The only push notifications it will ever send you are approval requests for logins to Geneseo systems. The Microsoft Authenticator does not give CIT or Microsoft access to any data or information on your device.

You may not think you have access to any information worth protecting, but all our faculty staff have access to some secure information of one kind or another, from your W-2 (which an attacker could use to commit fraud and receive your tax return) to student health data, FERPA protected student data, or college financial data.

If your Geneseo account is compromised, it also could be used to trick other Geneseo staff into responding to a phishing email. Your account can also allow an attacker to more easily access systems or compromise users that do have access to the data they are looking for.

Related articles

- Administering MFA and Azure Passwords
- How to Reset a Forgotten Password
- How-To Manage your Multi-Factor Authentication Settings
- Need Help Signing into Your Geneseo Account?
- Secure Login – Multi-Factor Authentication (MFA)

More Help

For questions, contact the CIT HelpDesk by calling (585) 245-5588, or visiting our online service desk.