

2-Step Verification and Microsoft

To help secure your personal data, combat the threat of identity theft and other cybercrimes, and to comply with institutional and government regulations, Hartwick will begin enforcing 2-Step Verification for all user accounts in Microsoft Azure AD. Hartwick utilizes Microsoft Azure AD to provide secure, cloud-based, single-sign-on (SSO) authentication to a growing list of Hartwick applications. Single-Sign-On will provide a uniform login experience across disparate applications and 2-Step Verification, combined with Microsoft's industry leading security, will help to ensure a safe and secure online experience.


Microsoft Azure AD compliant Hartwick Applications:

Barnes & Noble Hartwick College Bookstore	EAB Navigate	Ellucian CRM Advance
Forticlient VPN	Hartwick Handshake	Chrome River
Maxient	True Blue Connect	StarRez
Pathway Planner	Transact Mobile Ordering	Office 365

Note: with SSO, once you've authenticated to one of the above applications, you're automatically authenticated to any others to which you have access.

This policy will go into effect 11/15/2022 and will be strictly enforced. As of 11/15/2022, the next time you log in to a Microsoft Azure AD application, you will be prompted to provide a second authentication method such as a cell number to receive texts or the Microsoft Authenticator App on your phone for more convenient access. The screenshots to follow provide an example of what to expect when enabling 2-Step Verification.

At the login prompt, enter your Hartwick e-mail address: [username]@hartwick.edu




Sign in


[username]@hartwick.edu

[Can't access your account?](#)


Next

 Sign-in options

If prompted, be sure to indicate that you are using a work or school account:




It looks like this email is used with more than one account from Microsoft. Which one do you want to use?



Work or school account

Created by your IT department

telecom@hartwick.edu



Personal account


Created by you

telecom@hartwick.edu

Tired of seeing this? [Rename your personal Microsoft account.](#)

Back

Enter your network password:



← telecom@hartwick.edu


Enter password

password

[Forgot my password](#)

Sign in

You will now be prompted to enter additional information to enroll in 2-Step Verification as follows:



telecom@hartwick.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

Upon clicking “Next,” Microsoft will prompt you to install the Microsoft Authenticator App on your cell phone. However, you may opt to receive a code via text (SMS) message or phone call if you prefer.

If you prefer to receive a code, click the link “I want to set up a different method.”

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose “Next”.

[I want to use a different authenticator app](#)

Next

[I want to set up a different method](#)

Enter your phone number and choose whether to receive a text message or voice call:

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1) ▼

Enter phone number

☒ Text me a code

☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next


[I want to set up a different method](#)

Click next and follow the instructions to finalize your enrollment in 2-Step Verification. Note that you will only have to complete this enrollment process once.

The next time you log in, you will be prompted to approve your sign-in request via the method you selected during the previous steps.

If you are using a personal device, feel free to check the box allowing you to trust the device for 90 days. Selecting this box will still require you to sign in using your username and password. However, you will not be prompted for 2-step verification during the 90-day period. Do not select this option if you are using a public or shared device.

Approve sign in request


 Open your Microsoft Authenticator app and approve the request to sign in.

☒ Don't ask again for 90 days

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)

Additionally, you may opt to remain signed in. By default, you will be automatically signed out after 15 minutes of inactivity or when closing your web browser. Clicking “Yes” will allow you to remain signed in for 4 hours and will keep your session active even in the event that you close your browser window.

 **HARTWICK
COLLEGE**
1863

donoj@hartwick.edu

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No

Yes

If at any point you wish to change your sign-in method or add an additional method you may do so via <https://myaccount.microsoft.com/>

Click “Security Info” on the side menu and then add or delete sign-in methods as needed.

HARTWICK COLLEGE

My Sign-Ins

Overview

Security info

Organizations

Devices






Privacy

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification [Change](#)

+ Add sign-in method

	Phone	[REDACTED]	Change	Delete
	Office phone	[REDACTED]	Change	Delete
	Microsoft Authenticator (in Authenticator)	[REDACTED]		Delete
	Microsoft Authenticator	[REDACTED]		Delete
	Email	[REDACTED]	Change	Delete

Lost device? [Sign out everywhere](#)