User Accounts

University account, password, and authentication information.

- User Account Overview
  - Faculty/Staff user accounts
  - Student user accounts
- Password Information
- Two-Factor Authentication

User Account Overview

Information on user account provisioning, usage, and lifecycle.

Faculty/Staff user accounts

Your faculty/staff CU account is your single sign-on account for virtually all university related systems, including campus computers, Microsoft 365 resources including your email, Banner OneSIS, Brightspace, PASSHE Portal/Employee Self-Service, wireless connections, and remote access VPN service, as well as any other resources protected by university Single Sign-On.

Faculty/Staff account lifecycle

Employees will have a CU account automatically created once HR has the completed paperwork and completes the hiring action in SAP. The assigned username along with the initial password that can be used to logon to your computer and to access other university resources will be communicated directly to your supervisor or department secretary to be communicated to you.

Please understand that Faculty/Staff will not get to keep their account once they separate from employment with the university, therefore it is recommended that you do not use your work email account or storage for personal use.

Employees that have officially retired will get to keep their account for an additional 4 months after retirement date.

Separated employees that are granted emeritus status are able to request that they keep their email account indefinitely. Emeriti accounts only include email and will only remain in the system if they are accessed at least once every 90 days.

Password requirements and information

Certain password requirements must be followed when creating a new password. Please see the password information page for detailed requirements and information on changing or resetting your password.

Two-Factor Authentication (2FA)

Duo Two-Factor Authentication is required for all remote access. Faculty/Staff will be prompted to enroll when they sign in to a web resource. If you are not yet enrolled, it is recommended that you go to https://duo.commonwealthu.edu/ from your smartphone because this helps ensure you choose the correct app from the app store and it streamlines activating your account on the device.

Keep the office/phone up to date on your account

Employees should be sure to keep their campus office and phone number information up to date with HR and other systems including the Outlook address book and web directory. To set or update the information, log on to the PASSHE Portal/ESS, click on the "Employee Self-Service" tab, click on the "Personal Information" tab, click on "Address and Contact Information", then under "Campus Address", click on "Change Campus Address". Update your Office (Building & Room Number) and Work Phone (enter full number including area code), and click "Save Changes".

Keep your account secure

Please keep your password to yourself and do not provide it on an external website in response to a phishing email no matter how convincing an email request for your password looks. Do not ever enter it onto a Google Form or Microsoft Form. You should not click on questionable links or links that you know are phishing. Also do not provide Duo 2FA passcodes via text message or email or on external websites and also do not approve Duo Pushes you did not initiate. Please familiarize yourself with the official university policies, PRP 2510 - Information Security Policy and PRP 2550 - Acceptable Use of Technology Policy.

Student user accounts

Your student CU account is your single sign-on account for virtually all university related systems, including public computers across CU campuses in computer labs, Microsoft 365 resources including your student email, Banner OneSIS, Brightspace, wireless connections, Housing related systems, Print related services, Student Worker eTime, and any other resources protected by Single Sign-On.

Student account lifecycle

Undergraduate degree students will have a CU account automatically created after they pay their tuition deposit. They are given their username and initial password in the application portal.

Graduate degree students and non-degree undergraduate students (no tuition deposit required for these types of students) will have a CU account automatically created when they have at least one course scheduled. If you were a recent CU undergraduate student and your account has not yet become inactive, your active CU account and password remain the same. If your account did become inactive or you forget what your password was, you will need to reset your password to gain access to your account. If you are a brand new CU grad student, you will receive notice of your username and password from the graduate office. You may also reset your password to gain access to your account.

Your CU account will become inactive approximately 8-9 months after you last attend CU, typically shortly after two succeeding semesters conclude. At that time you will receive an email notification that your CU account will be deleted in 1 month, and during that time you will need to save any data from your M365 Email, OneDrive, and any campus network drives that you want to keep, since it will be deleted with your account, unless you re-enroll prior to deletion, which a separate email notification would confirm.

Password requirements and information

Certain password requirements must be followed when creating a new password. Please see the password information page for detailed requirements and information on changing or resetting your password.

Two-Factor Authentication (2FA)

Duo Two-Factor Authentication is required for all remote access. Students will be prompted to enroll when they sign in to a web resource. If you are not yet enrolled, it is recommended that you go to https://duo.commonwealthu.edu/ from your smartphone because this helps ensure you choose the correct app from the app store and it streamlines activating your account on the

device.

Keep your account secure

Please keep your password to yourself and do not provide it on an external website in response to a phishing email no matter how convincing an email request for your password looks. Do not ever enter it onto a Google Form or Microsoft Form. You should not click on questionable links or links that you know are phishing. Also do not provide Duo 2FA passcodes via text message or email or on external websites and also do not approve Duo Pushes you did not initiate. Please familiarize yourself with the official university policies, PRP 2510 - Information Security Policy and PRP 2550 - Acceptable Use of Technology Policy.

Password Information

Information on password requirements, lockout policies, and how to change or reset your password.

Password policy requirements

Faculty/Staff/Students must adhere to the following password requirements when changing their password:

- Your password must be at least **14 characters long** and not contain your first name, last name, or username (the portion of your email address before the "@").
- It must include characters from at least **three of the four categories** (UPPERCASE, lowercase, a numeric digit 0-9, a symbol such as !, $, %, etc.)
- It may not be identical to any of your previous passwords.

As part of the University's modernization efforts, we moved to **non-expiring passwords** to improve security and reduce password fatigue. Passwords no longer require routine changes, but may be reset if suspicious activity is detected.

Changing a known password

There are two options, make sure you choose "change". It is important to NOT choose a "forgot" or "reset" option as these options will reset your password to check the complexity and history requirement and if you do not enter a password that meets the current requirements, it will render your known password invalid so you will be locked out of your account until you succeed.

- From a PC computer on a CU campus, while logged in, press Ctrl+Alt+Del and choose the "**Change a password**" option.
- From off campus, you can change your password over the web by visiting https://password.commonwealthu.edu/ and choosing "**Change your expired/known password**".

Resetting a forgotten or non-working password

If your account gets locked out due to invalid password attempts, it will automatically unlock after 15 minutes. If you need to proceed to reset your password, there are two different ways to handle this situation:

- Utilize the Password Reset System over the web by visiting https://password.commonwealthu.edu/ and click "**Reset your forgotten/unknown password**".
- Click the "**Forgot My Password**" button on a campus PC computer login screen or on the Single Sign-On page.

Things to remember after setting a new password

Please remember to update the wireless settings and email settings on your personal laptop, smartphone, or tablet to include your new password.

If you are logged into any campus computers in which you did not directly change your password on (through either the Ctrl+Alt+Del method or expired password prompt), you will need to log off and log back on with the new password.

If any computers/devices attempt to authenticate with an outdated password, those computers/devices could cause your account to continually lock out until you update them with your new password. If this is happening to you, be sure to log off campus computers, forget the campus wireless network, and remove or update the outdated saved credentials in your windows credential manager or apple keychain.

About the password reset system

The password reset system will ask you three questions:

1. What is your 5-digit home Zip Code?

2. What is your birth date?

- It must be in the format: MM/DD/YYYY
- Make sure you enter the slashes, full year and leading zeros, Example: 01/02/1967

3. What is your personnel number? **(Faculty/Staff only)**

- This is your SAP employee ID number. Example: 123456
- If unsure of employee number, it is on ESS, payroll statements, and tax forms, or you could check with your department secretary.

3. What is your Banner OneSIS ID? **(Students only)**

- Example: P12345678

After answering the questions correctly, you may also have to provide a text message code for your protection to prove it is really you trying to reset your account's password.

The password reset system is only available for Students and Faculty/Staff with HR/SAP personnel numbers. At this time, auxiliary employees will still need to contact the help desk to have their password reset.

Invalid Login or Reset Attempts

After ten (10) invalid login attempts (i.e., entering the wrong password when logging onto a campus computer or a university web resource), an account will be locked for fifteen (15) minutes.

When using the password reset tool, if there are five (5) invalid attempts to reset a password (i.e. at least one invalid answer to the 3 questions 5 times in a row), the password reset system will unavailable for your account for one hour.

If you still need assistance after trying to reset your password, please contact the Help Desk at extension 4357 (HELP) or from off-campus at 877-435-7280.

Two-Factor Authentication

Duo two-factor authentication (2FA) is required for remote access from outside the CU trusted network.

Although it may seem like an inconvenience, two-factor authentication is a solution used to protect you from scammers accessing your information and to protect you from scammers impersonating you.

As more and more people become victim to advanced targeted phishing email campaigns and unknowingly give their password to scammers through an external website that looks like ours, as well as more and more external database exploits happen where people are using same or similar passwords, we have seen an ever-increasing amount of compromised accounts. With 2FA enforced, a scammer is unable to access protected resources and information by only knowing your password.

Duo 2FA Enrollment Info

Simply go to the Duo Management Portal at https://duo.commonwealthu.edu/ to enroll your device or manage your devices. You may also be prompted to enroll inline when you start using your new account.

If you have a smartphone, we highly recommend you enroll through the web browser on the device (i.e. Chrome, Safari, Firefox). This helps ensure you choose the correct app from the app store and streamlines activating your account on the device. When you need a second factor in order to log on remotely, using the "Duo Push" authentication method for the "Duo Mobile" app (by "Duo Security") on a smartphone is the most secure and user-friendly method.

If you do not have a smartphone, you may enroll a basic cell phone from a computer web browser.
If you do not ever access your CU account from outside the CU trusted network, then enrolling is not required.
If you do not have a mobile device, you may sign-out a small Duo hardware token for your keyring from the technology helpdesk at your campus, which will allow you to obtain passcodes.

How Duo 2FA changes your logon experience

2FA combines something you know (your password) with something you have (like your mobile phone).

When you log in to a Duo-protected application from outside the CU trusted network, you will still enter your password. Then you will be required to verify your identity, such as through a push notification on your smartphone or a text message passcode on a basic cell phone.

If your password becomes compromised and a scammer attempts to access your account remotely with your password through a Duo-protected application, they will not be able to successfully log in. If you did not trigger a Duo push notification by logging in to a Duo-protected app from outside the CU network, be sure NOT to approve the logon attempt. This will keep the scammer out of your account and alert Network Services that your password is compromised, at which time you should change your password immediately.

Video explanations of 2FA and Duo Push

- Please watch these short Duo videos to become familiar with Duo 2FA:

  Duo YouTube Video (1:59): What is Two-Factor Authentication?

  Duo YouTube Video (1:17): An Introduction to Duo 2FA

  Duo YouTube Video (0:20): 2FA with Duo Push
- Please watch the two videos associated with your campus for examples showing enrollment and Duo Push:

  CU IMS Video (1:35): **Bloomsburg** DEMO: Enroll your iPhone in Commonwealth University Duo Management Portal

  CU IMS Video (1:13): **Bloomsburg** DEMO: Accessing Microsoft 365 from off-campus using 2FA with Duo Push

  CU IMS Video (1:35): **Lock Haven** DEMO: Enroll your iPhone in Commonwealth University Duo Management Portal

  CU IMS Video (1:13): **Lock Haven** DEMO: Accessing Microsoft 365 from off-campus using 2FA with Duo Push

  CU IMS Video (1:35): **Mansfield** DEMO: Enroll your iPhone in Commonwealth University Duo Management Portal

  CU IMS Video (1:13): **Mansfield** DEMO: Accessing Microsoft 365 from off-campus using 2FA with Duo Push

Duo 2FA when traveling abroad

If you travel outside the country without the mobile device(s) you've enrolled into Duo, **you need to sign-out a Duo hardware token from your campus technology helpdesk prior to departure**. This duo hardware token fits on your keychain and allows you to obtain a passcode when you need one.

Information about other possible options using a device instead of the Duo hardware token:

- If you take your U.S. mobile device that you've enrolled and activated, you will be able to do a Duo Push when you have it connected via Wi-Fi or foreign mobile data service.
- If you take your U.S. mobile device that you've enrolled and activated, while you do not have Wi-Fi or foreign mobile data service, you can still open the "Duo Mobile" app to obtain a valid passcode (even though it's not connected to the Internet).

- If you take your U.S. mobile device and will have foreign mobile service and can still receive text messages at your existing number, you will be able to obtain a text message passcode (although in this case, a Duo Push should be preferred via activated Duo Mobile app).
- If you will instead have a separate foreign mobile device and already know what your foreign cell phone number will be, you can enroll it as an additional device/number in the Duo Device Management Portal before you leave while you still have access to your U.S. mobile device to pass 2FA.

Duo 2FA options in detail

You are able to enroll smartphones, basic cell phones, and tablets. If you have none of these, you will be able to obtain a small duo hardware token for your keyring from your campus technology helpdesk.

The second factor available depends on your enrolled devices. You can do Duo Push (Internet-connected smartphone or tablet with activated Duo Mobile app), text message passcode (basic cell phone or smartphone), Duo Mobile passcode (Duo Mobile app on an offline/online smartphone or tablet), hardware token passcode (Duo hardware token), or platform authenticators (like Touch ID, Face ID, Windows Hello, or Android biometrics) and roaming authenticators (like security keys). We always recommend enrolling your smartphone using the Duo Mobile app so that you always have your second factor with you as an option to help you authenticate from anywhere. To add or edit your devices, during authentication, choose "Other Options" and then choose "Manage Devices".

When you are logging on to a standard web resource, the prompt will choose the best method for you, which would be a Duo Push if you have an activated Duo Mobile app or potentially a platform authenticator like MacOS TouchID or Windows Hello, but you could always choose "Other Options" to choose your authentication method, such as "Duo Push", "Text message passcode", or "Duo Mobile passcode". If you have typical browser settings, you should be able to choose a "Remember me" option during logon to prevent future second-factor challenges in that browser for a time. You may also get asked if you are on a shared computer or not, which will also help determine if it should remember you on that browser/computer.

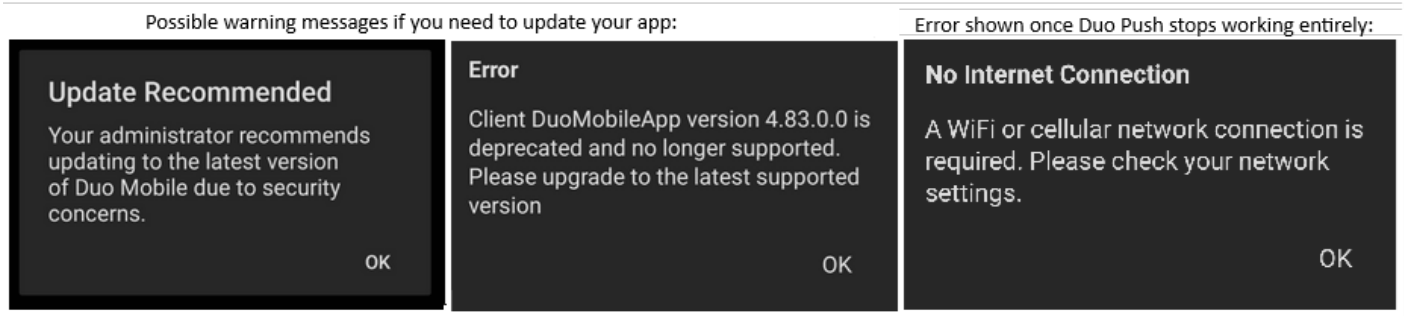
Troubleshooting

If you do not have the convenient Duo Push option or it stopped working, it is because you do not currently have the Duo Mobile app activated. You should [Re]activate Duo Mobile if you did not fully complete the enrollment process, you wiped your mobile device, you fully uninstalled the Duo Mobile app, or you replaced your smartphone and have the same phone number. Log in to the Duo Management Portal (which in this case would require you to request a text message passcode to pass 2FA) and look for the "[Re]activate Duo Mobile" button to activate the app. If you don’t have the option, be sure your phone number is configured correctly as either Apple or Android and look for the link to the app store and download and install the "Duo Mobile" app. If the phone number and platform is correct and you have Duo Mobile installed, choosing "[Re]activate Duo Mobile" should give you the steps to enable the Duo Push option for future authentications.

Update Duo Mobile to 4.85.0 or newer by 4/15/26 to continue using Duo Push

Duo Mobile in App Store (Apple) | **Duo Mobile in Play Store (Android)**

Throughout the Spring 2026 semester, you will no longer be able to receive Duo Pushes reliably if you are running a Duo Mobile app version below 4.85.0, which was released about a year earlier, due to outdated encryption certificates. Beginning 4/15/26 or shortly thereafter, Duo Push on those outdated app versions will stop working entirely. The exact timing is dependent on when expected browser and operating system encryption certificate updates take place.



If you received a personalized email notification message from IT about your device or if your Duo Mobile app is showing an "Update Recommended" or "Please upgrade" message, or a "No Internet Connection" message even when you are connected, your version of the app *is* affected, and you should go to the App Store (Apple) or Play Store (Android) to update your Duo Mobile app:

Fix: Update your Duo Mobile app to continue using Duo Push

1. On the device you need to update, tap the appropriate link to show the Duo Mobile app in the proper app store:
   Duo Mobile in App Store (Apple)
   Duo Mobile in Play Store (Android)
2. Tap "**Update**" (the "Update" option is only visible if an update is available, otherwise the option says "Open")

If that does not work on your device or you are not reading this on the device, follow these steps on the device:

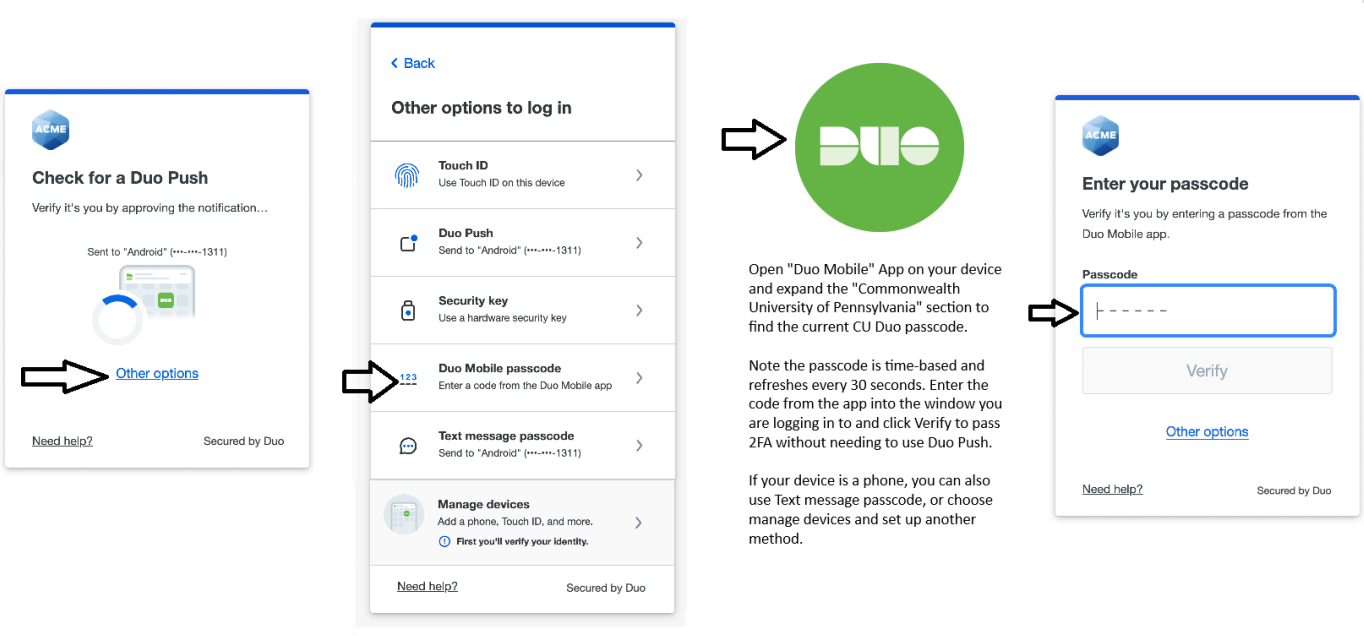
1. Open the App Store or Play Store
2. Search for "Duo Mobile"
3. Tap "Update" (the "Update" option is only visible if an update is available, otherwise the option says "Open")

If you are unable to update the Duo Mobile app, you will no longer be able to use Duo Push for 2FA, but you will still be able to use passcodes found in the Duo Mobile app or obtained via text message by choosing "Other Options" during Duo 2FA:

Workaround: Use outdated Duo Mobile app passcode to pass 2FA without using Duo Push

1. When prompted to check for a Duo Push that never comes through, choose "Other options"
2. Choose "Duo Mobile passcode"
3. Open the "Duo Mobile" app on your device, expand the "Commonwealth University of Pennsylvania" account and obtain the current CU Duo passcode
4. Promptly enter the CU Duo passcode into the passcode prompt where you are logging in and choose "Verify" - Done!

- The passcode in your app is time-based and refreshes every 30 seconds
- If your device is a phone, you can use the "Text message passcode" option instead if that is more convenient to you
- You can also use the "Manage devices" option to add/remove/modify your two-factor options
- Phishing warning: Do not provide Duo passcodes to anyone via text message, email, or on web forms



See below for more details on hardware and software version compatibility with the Duo Mobile app:

Info for Apple iPhone/iPad iOS devices (as of January 2026)

- If you are running iOS 16 (released 9/12/22) or newer, you will be able to update the Duo Mobile app in the App Store.

- The following devices can support iOS 16 or later, but may require that you run a system update:
  iPhone 8 through iPhone 13
  iPad 6th Gen through 9th Gen
  iPad Mini 5th Gen through 6th Gen
  iPad Air 3rd Gen through 5th Gen
  iPad Pro 1st Gen through 5th Gen

- The following devices cannot support iOS 16 and therefore cannot update the Duo Mobile app:
  iPhone 7 and older
  iPad 5th Gen and older
  iPad Mini 4th Gen and older
  iPad Air 2nd Gen and older
  iPod Touch 7th Gen and older (No iPod Touch is supported)

- The following devices shipped with iOS 16 or later and therefore natively support updating the Duo Mobile app:
  iPhone 14 and newer
  iPad 10th Gen and newer
  iPad Mini 7th Gen and newer
  iPad Air 6th Gen and newer
  iPad Pro 6th Gen and newer

Info for Samsung Galaxy Android devices (as of January 2026)

- If you are running Android 11 (released for Samsung Galaxy Android devices in 2022) or newer, you will be able to update the Duo Mobile app in the Play Store.

- The following devices can support Android 11 or later, but may require that you run a system update:
  Samsung Galaxy S10 through S20
  Samsung Galaxy Note 10 through Note 20
  Samsung Galaxy Tab S6 through Tab S7
  Samsung Galaxy Z Fold 1 through Fold 2
  Samsung Galaxy Z Flip 1 through Flip 2
  Samsung Galaxy A series or M series released in approximately mid-2020 to mid-2021

- The following devices cannot support Android 11 and therefore cannot update the Duo Mobile app:
  Samsung Galaxy S9 and older
  Samsung Galaxy Note 9 and older

Samsung Galaxy Tab S5 and older
Samsung Galaxy A series or M series released before approximately mid-2020

- The following devices shipped with Android 11 or later and therefore natively support updating the Duo Mobile app:
  Samsung Galaxy S21 and newer
  Samsung Galaxy Tab S8 and newer
  Samsung Galaxy Tab S7 FE (NOT other S7 series Tabs)
  Samsung Galaxy Z Fold 3 and newer
  Samsung Galaxy Z Flip 3 and newer
  Samsung Galaxy A series or M series released in approximately mid-2021 or later

Info for Google Pixel Android devices (as of January 2026)

- If you are running Android 11 (released for Google Android devices on 10/19/21) or newer, you will be able to update the Duo Mobile app in the Play Store.
- Google Pixel 2 through Google Pixel 4 can support Android 11 or later, but may require that you run a system update.
- Google Pixel 1 cannot support Android 11 and therefore cannot update the Duo Mobile app.
- The following devices shipped with Android 11 or later and therefore natively support updating the Duo Mobile app:
  Google Pixel 5 and newer
  Google Pixel Tablet 1 and newer

Info for Duo Mobile app, including checking your version

To check your Duo Mobile app version:

1. Launch Duo Mobile app on the mobile device.
2. Open the side navigation drawer in the Duo app by tapping the three-line menu icon in the upper-left corner of the screen.
3. The app version will be displayed at the bottom of the navigation drawer.

Check the version carefully; Note that the latest version as of January 2026 is v4.104.0, which is newer than v4.85.0

- Beginning around the end of April 2026, Duo Mobile in the App/Play Store will only support iOS 17+ and Android 12+

- Duo provides help articles that show the most current info regarding iOS and Android versions that Duo Mobile supports.
- It is good practice to allow apps on your device to auto-update so that they receive the latest security fixes. Learn more about how to update Apple iOS apps and how to update Android apps.