Duo two-factor authentication

Frequently Asked Questions and Support

What is it and how does it affect me?

What is two-factor authentication?

Two-factor Authentication (2FA) adds an extra layer of security to your username and password process. It combines something you know (your username and password) with something you have (mobile phone, tablet, text message, landline phone) to verify your identity. This extra step adds significant security protection to your account and Uconn Health digital assets.

How does two-factor authentication affect me?

Chances are you are already using two-factor authentication to log into your financial institution or social media. This second layer of protection combines something you know (your username and password) with something you have (mobile phone, tablet, text message, landline), preventing anyone but you from logging into a system.

UConn Health uses Duo security to provide this service. You will now need to log in by:

1. Entering your username and password, and
2. Confirming your identity with the Duo app on your smartphone, tablet, or text message to your phone, or a call to a landline phone. ***IMPORTANT NOTE: Once a push notification is sent you have 60 seconds to approve the request.**

In summary, how does it work?

When you login to one of the following Duo protected services, you will be required to use Duo two-factor authentication:

- Outlook Web Access (OWA) to Web Based Email
- Pulse Secure VPN
- Citrix (remote.uchc.edu)
- Office 365 (portal.office.com)

You will enroll a device of your choice below that Duo will associate with your account. During login you will receive a Duo prompt and you will use that device to provide the additional two-factor part of authentication. You self-manage your device with Duo using the Duo Device Management Portal.

Smartphone/Tablet	Choose this method during enrollment to install the Duo Mobile App on your phone and during the login process you will select 'send me a push' which you will then use the App to 'Approve' your login. This is the easiest and preferred method.
Standard Mobile Phone	Older style phones or those with older IOS or Android versions if capable of receiving an SMS text message will receive a 'Passcode' you request during the Duo option prompt. You will then enter the 'Passcode' received on your phone into the Duo 'Passcode' prompt to authenticate.
Landline	Lastly you can enter a 'Landline' phone number and receive a call back during authentication. You must be near that phone during authentication.

To get your device enrolled, follow the instructions on the UConn Health Two-Factor Authentication site under the section titled "Enrolling and Activating Two Factor Authentication".

What data does Duo Mobile collect from my smartphone?

Duo Mobile cannot see your user data like your contacts, it cannot read your text messages, it cannot access your photos (but it can use your camera to scan a QR code if you explicitly allow that permission), it cannot access your files, it cannot erase your device, it cannot see information about other applications on your device. Duo Mobile cannot track your location. In general, the only personal data that Duo Mobile knows about you are the service accounts that you explicitly add to Duo Mobile. However, we do not track any personal data about these accounts–only the name of the service.

How do I enroll?

How do I setup two-factor authentication?

In order to use two-factor authentication, you must first download the Duo app on your device (e.g. smartphone, iPad) this is the preferred and primary method. The app will work anywhere in the world even without internet or cellular and you can access a 'passcode' from the app to authenticate with.

You can also enroll a standard mobile phone that has the capability to receive a text message. Note your cellular provider may charge for a text message. Additionally, you can enroll a landline phone to receive a call back. Follow the instructions on the UConn Health Two-Factor Authentication site under the section titled "Enrolling and Activating Two Factor Authentication" and choose "landline".

What is a passcode and how is it used?

A passcode is a six-digit code that you generate in the Duo app on your smartphone by pushing the down arrow of the right side of your screen. You enter the passcode after entering your username and password. You can generate a passcode on your smartphone, even if you do not have cellular or wireless (Wi-Fi) service anywhere in the world. **The passcode will appear in the Duo app on your smartphone, NOT in a text**!

Reminder: Access to your UConn Health email account on your personal mobile device is allowed only through the use of Outlook Web Access (OWA) or by installing MobileIron**.** Please refer to the Mobile Computing Device (MCD) Policy.

How do I remove an old device?

- If you have an old device that you are no longer using, you should remove it using My Settings and Devices in the Duo Device Management Portal.
- You'll need to have another device enrolled in Duo to authenticate to the Duo Device Management Portal in order to remove the old device.
- If you no longer have the old device or lost it, follow the section in this document for "I lost my phone or suspect that it's been stolen!"
- You manage your two-factor device on the UConn Health Two-Factor Authentication site under the section titled "Manage Your Device". Once authenticated you can click on Device Options and click on the Trash Can icon next to the old device you wish to remove.

My smartphone's operating system is older and I'm receiving a message "the Duo app is not compatible with my phone".

If you have an older smartphone operating system that is not up-to-date, the Duo mobile app may not be compatible with the older version. In that case you would to select "other (and Cell phones)" during mobile phone enrollment. During authentication you will receive a TEXT/SMS/PASSCODE sent to your mobile phone provided your phone is capable of receive text messages. Note there may be additional charges by your cellular carrier for receiving text messages.

I lost my phone or suspect that it's been stolen!

Contact the UConn Health Service Desk immediately if you lose your phone or suspect that it's been stolen! If you had previously enrolled a second authentication device you can Duo Device Management Portal to delete the device. If you are unable to delete the device, contact the UConn Health Service Desk to delete the device.

Troubleshooting Push Notifications on Android Devices:

https://help.duo.com/s/article/2050?language=en_US

Troubleshooting Push Notifications on iOS Devices:

https://help.duo.com/s/article/2051?language=en_US

Additional help with Common Issues:

https://guide.duo.com/common-issues#lost-phone

Where do I go to get help?

Important information about using Duo, enrolling and managing your device and additional information is located on the UConn Health Two-Factor Authentication site.

If you need help with an issue that isn't listed here, contact the UConn Health Service Desk.