

GUIDE TO REMOTE WORK

STEP ONE: Enroll in MultiFactor Authentication (MFA) with DUO

At minimum, all users will need their Mednet username and password as well as DUO for multi-factor authentication in order to access any remote work options and tools.

In order to access the MFA Enrollment Portal you will need to be on the Mednet network. If you plan to use a mobile device (mobile phone, tablet, etc.), you will want to download the Duo Mobile application to the device prior to starting the enrollment process.



- [Download Duo Mobile App for iPhone](#)
- [Download Duo Mobile App for Android](#)

What are my options for remote work?

UCLA Health IT laptops/desktops: If you have been issued a laptop from UCLA Health IT, it is secure and ready for remote work.

Personal laptops/desktops:

Applications via the web

If you are using a personal computer, you can quickly connect to many applications on the web using just your Mednet login and DUO for multi-factor authentication.

DOES NOT REQUIRE VPN

- CareConnect Remote
- Mednet email and Office 365 Portal
- Box for UCLA Health
- Zoom web and video conferencing
- Outlook Web Application (OWA)
- HBS
- Human Resources WEB Site
- Campus Directory
- UCPATH

REQUIRES VPN

- REDCAP
- Shared Drives
- Remote Desktop
- Medhub
- Oncore
- PudMed
- UpToDate
- ...and More

Please work with your Division Administrator to request what you need.

For more information: <https://it.uclahealth.org/remote-work> or Call 310-267-CARE (2273)

GUIDE TO REMOTE WORK

What is VPN?

A VPN is a secured private network connection built on top of publicly accessible infrastructure. The Campus VPN service provides an alternative to using the proxy server for remote access to the UCLA Library and other campus resources. Campus VPN access is restricted to registered students and university employees with an active staff/faculty appointment.

Applications via Virtual Private Network (VPN)

If you have a personal laptop/desktop and use an application that requires direct connection to the Mednet network, you will need to access these resources through our Virtual Private Network (VPN). In order to get set up you will need to:

- [Request authorization for VPN access](#)
- [Install Global Protect VPN to connect to the Mednet network](#)
- [Encrypt your device](#)
- Install OnGuard to verify your encryption status
 - [OnGuard for Windows](#)
 - [OnGuard for Mac](#)

Requirements for VPN Access

- DUO Multi Factor Authentication Authenticating Using Multi-Factor Authentication on the Campus VPN
- Active Mednet Account
- VPN Access Request Submitted by DSA
- Computer must be encrypted (ClearPass OnGuard & Global protect VPN, per device. Self-encryption guide: https://mednet.uclahealth.org/device-security-toolkit/?utm_campaign=search)
- Compliant with Policy: Device and Removable Media Encryption, HS 9453-C <https://uclahealth.policystat.com/policy/4995278/latest/>

Remote Desktop

If you require remote access to applications or shared drives on a desktop issued by UCLA Health IT, you can remote into your desktop from any computer using Remote Desktop. In order to access this resource, you will need to [Submit a Ticket](#) with the following information:

- The computer name of the device you wish to access
- VPN (instructions listed above)

NOTE: If the computer was purchased either by an individual employee or by his/her local operating unit, encryption and password protection must be confirmed prior to activating VPN.

Please work with your Division Administrator to request what you need.

For more information: <https://it.uclahealth.org/remote-work> or Call 310-267-CARE (2273)