UT Southwestern Medical Center | My UTSW

Two-Factor Authentication

In order to protect the sensitive information of our patients, faculty, staff and students, an additional layer of security is required for off-campus access to sensitive Information Resources. In most cases, the use of “Duo” two-factor authentication provides this layer of protection.

What is “Two-Factor Authentication”?
Even tech savvy employees have fallen for cyber-attacks that trick them out of their passwords using a technique called phishing. The bad guys can then use your stolen password to log into systems such as PeopleSoft and re-route your paycheck to the criminal’s bank account, steal your identity using your tax statements also available in PeopleSoft, or access information in your email account and Epic.

Two-factor authentication ensures that even when your password is stolen, the bad guys cannot access sensitive information. When remotely logging into UT Southwestern information resources from a new computer, you will be asked to verify your identity in one of four ways:

What is Duo?
This is the name of the product UT Southwestern has selected for implementing two-factor authentication.

What if I don’t have a phone or don’t want to use my phone for two-factor authentication?
The use of your phone for two-factor authentication is not mandatory. If you would like to remotely access or systems without the use of a phone, a keychain token can be provided to you by contacting the IR Service Desk. This key is less secure than the other methods of authentication so use of a phone is preferred.

How do I setup/register my phone?
The first time that you login to an information resource with Duo two-factor authentication enabled, you will be prompted to register. You will only need to register once, even if you access multiple types of information resources.

Most common options follow:

- Duo Mobile App
- Text Messages
- Voice Calls

Do I need to use Duo every time I login?
No, if you are on a trusted device such as your home computer, you can "trust" the device for 60 days. All devices on the UT Southwestern, Parkland and Children's network are automatically trusted and will not ask for you to perform two-factor authentication.

What information resources require two-factor authentication?
All information resources with sensitive information used by employees, faculty, staff and students will require two-factor authentication. This will be implemented for all systems over the course of the next couple years. Given the great amount of IT resources required to open the Clements University Hospital in November, there is a break in implementation around this November.

1. Juniper VPN Network Access (November)
2. Outlook Web Access (January)
3. Citrix (February)
4. PeopleSoft (February)
5. Other (TBD)

I received a login request message that I did not make, what do I do?
Immediately change your password as it is likely that someone has stolen your password and is trying to use it maliciously. If you are using the Duo App, pressing the red "deny" button will alert Information Security. If you are not using the Duo App, you should contact the Service Desk to let them know of the incident.

What if I get a new phone number or have no access to my old number?
You can enroll additional phones or tablets at any time. However, to prevent the malicious registration of unauthorized devices, you will need to have access to at least one of your registered devices. If you do not have access to one of your registered devices, you may contact the IR Service Desk to have your device registration reset.

I need to change the phone number registered to my account. How do I do that?
If you have multiple devices registered (such as your desk phone), you can visit http://utswra.swmed.edu from outside of the network (or https://vpninstall.swmed.edu/ from inside of the network), log in with your username and password, then click "Manage Devices" to add or remove a new device. If you do not have multiple devices, for security reasons you will need to contact the Information Resources Service Desk to have your account reset.

What if I use the Juniper Pulse client to login to VPN?
For information about using the Juniper Pulse client, you can visit http://guide.duosecurity.com/pulse. To do the initial one-time Duo Two Factor registration, you will need to visit https://utswra.swmed.edu from your off-site location or https://vpninstall.swmed.edu from inside the network.

Can I register for two-factor while on campus?
While VPN services are only available from outside of the network, Information Resources has setup a website at https://vpninstall.swmed.edu/ that will allow you to register for two factor authentication while on the UT Southwestern network.

Juniper Pulse is requesting a Secondary Password. What do I type in the box? There are multiple types of secondary passwords you choose from based on your preferences. For information about which option best works for you, please visit http://guide.duosecurity.com/pulse. Please note, you will need to register for two-factor authentication before you can login with the Juniper Pulse by visiting https://utswra.swmed.edu from your off-site location or https://vpninstall.swmed.edu from inside the network. You only need to perform this registration once.

Can't you just block access from outside of the United States?
Since UT Southwestern is an international organization, there are many legitimate users outside of the United States who daily need to connect to our sensitive information resources. Additionally, attackers are using infected computers in the Unites States to carry out their cyber-attacks against UT Southwestern.

Can I use the Duo mobile app to protect other accounts with Two Factor, such as Gmail and Facebook?
Yes. For more information, please visit http://guide.duosecurity.com/third-party-accounts. Please note that the use of Duo

mobile for these personal accounts is not supported by the Information Resources Service Desk.

The computer is repeatedly asking for me to download and install Junos Pulse. What do I do?
Often this is caused by having both “Network Connect” and “Junos Pulse” software installed at the same time. Removing the old “Network Connect” software often resolved this issue.

I am receiving Java issues when trying to upgrade the Juniper Pulse software. What do I do?
Ensure the old “Network Connect” software is no longer installed. If you are still experiencing an issue, uninstalling and re-installing the Juniper Pulse software will likely correct the issue.

I am traveling internationally. Will my device need to have international voice, texting, or data to authenticate? No, you can still use the Duo Mobile app or a physical keychain fob to authenticate. By opening up the Duo Mobile app, you can press the “key” icon which will generate your 6-digit login code. Alternatively, pressing the button on the keychain will present the 6-digit login code.

Is the Duo Mobile app trustworthy to install on my personal device? The Duo Mobile app is highly rated in both the Android and Apple stores. Additionally, this app has been reviewed and approved by the Information Security department to ensure appropriate levels of security and privacy. The app does not have the ability to access data on your phone such as pictures, messages or contacts.

My username and password does not have access to anything confidential. Why do I still need two-factor protection? Most attackers are interested in using your username and password to break into the secure internal network so that they can look for vulnerabilities on the thousands of sensitive internal systems on campus. Alternately, attackers will login to a user’s email account and send out hundreds or thousands of phishing messages to other faculty, staff and students in an attempt to compromise their computers and\or get access to sensitive information.

Do I need to install software on my laptop or home computer to do two-factor authentication? No, two-factor authentication is integrated into the various login pages, so additional software is not required.