Duo FAQ

Article Number: 488 | Last Updated: Wed, Apr 6, 2022 at 10:15 AM

What Two-factor authentication requires something you know (your Clemson password) and something you have (like a mobile phone, tablet, or a smartphone app) as an added layer of security to prevent anyone else from accessing your account. Two-factor authentication is the most effective method of account takeover prevention, helping to protect both you and the Clemson community. **Why** Passwords are essential for security and privacy, but they are often not enough.Â They can often be stolen, guessed, and hacked -- you might not even know who else has your password and is accessing your account. Two-factor authentication adds a second layer of security to your account to make sure that it stays safe, even if someone else knows your password, by using your phone or other device to verify your identity. You will be alerted right away (on yourÂ mobile phoneÂ or tablet) if someone tries to log in using your password. This prevents anyone but you from accessing your accounts. **Who** All Clemson students, faculty, and staff will be required to enroll in Duo in order access 2FA protected applications. **How** Duo's self-enrollment process makes it easy to register your cell phone or tablet and install the application on your device. You can complete your enrollment atÂ https://www.clemson.edu/2fa . We suggest doing thisÂ on a device other than the one you plan to register.Â After completing the process, you can test the authentication process by visiting https://www.clemson.edu/2fa/check .Â **FAQs and Tips** **What if I do not have a mobile phone?** You can use a tablet. Duo also lets you link multiple devices to your account, so you can use your mobile phone or tablet. In fact, we suggest that you enroll more than one device for redundancy in the event a device is lost. **What if I lose my mobile phone or it is stolen?** Contact the Help Desk via email (ITHelp@clemson.edu) or call 864-656-3494 immediately if you lose your phone or suspect that it has been stolen. The device will be disabled for authentication and you will be assisted in enrolling another phone/device. While it is important that you contact the Help Desk if you lose your phone, remember that your password will still protect your account. **What if I get a new mobile phone or wipe my existing phone? (Reactivating Duo Mobile)** If you get a new phone you will need to re-activate Duo Mobile. This can be done through our Device Management Portal at https://2fa.clemson.edu/. When accessing the portal, you will need to complete the two-factor authentication process. If you have a second device, you can use it to authorize. Otherwise, you will need to choose the option to have Duo call or send passcodes via text to your phone before you can re-activate Duo mobile. Once you have authenticated, under the Device Management tab, if you click **Device OptionsÂ** for the device that needs to be reactivated, you should see the option appear below. Once you have clicked on that, it will give you a new QR code to scan with your device. **What if I don't have a cell phone or a tablet for a secondary device?** The CCIT Support Center will have Duo D-100 hardware tokens available for $20. These devices are the preferred alternative to a mobile device or phone because they will work for any situation or application. In the event an employee does not have a suitable mobile device, it is our suggestion that the department purchase this token for their employee. If the employee later leaves, the token and be returned to the department and assigned to another user. Alternatively, you are welcome to purchase a personal YubiKey to be used for 2FA. A list of model prices and feature comparisons can be found on the vendor's website here: https://www.yubico.com/products/yubikey-hardware/. Please be aware the U2F version of the YubiKey only functions in Chrome or Opera web browsers. Native applications like Cisco AnyConnect will not work with the U2F YubiKey. If you purchase another model that supports event-based HOTP, a Duo admin will need to enroll the device for you. This can be done in the CCIT Support Center. **Does Duo work with Texts?** Yes, you can send a SMS Text Message to the Duo Mobile app on your smartphone that you acknowledge to confirm your identity. **How many chances will I get to authenticate?** You will have five chances to authenticate a request. After the fifth chance, your two-factor authentication will be deactivated and you will not be able to access the system you are attempting to log into. **What should I do if I get an authentication message and I am not trying to log in?** Deny the request and report the incident to the Help Desk immediately via email (ITHelp@clemson.edu) or by calling 864-656-3494. **I am getting a message that I am locked out. What do I do?** Your account will lock when there are too many failed attempts to authenticate. The lockout should clear automatically in 15 minutes, so you can either wait, or

contact the Help Desk at 864-656-3494 for assistance with your account. **Can I opt out of Duo?** No. Two-factor authentication adds a second layer of security to our online accounts. In an effort to keep your personal account information secure, we are requiring two-factor authentication on selected services. **I frequently travel internationally. How does this affect two-step verification?** If you travel internationally and need access to resources protected by Duo,Â you have two choices. You can continue to use Duo Push through your cell phone or purchase a hardware token to use with Duo. **How do I enroll more than one device in 2FA?** Please keep in mind it is important to enroll more than one device (such as a smartphone and tablet) in 2FA to avoid difficulties authenticating if you lose or don't have your only enrolled device with you. To add multiple devices: Please log intoÂ 2fa.clemson.edu and authenticate with your current device. Then, under the **Manage Devices**Â tab,Â under your current device there should be a plus symbol that says **Add Another Device**.

You will need to click that and go through the steps to set up an additional device. Once you have another device enrolled, you should now see a drop down under menu that says **Default Device**.

If you have your settings to automatically send you a push, the device you select here will be the one it will go to.

If you use devices interchangeably, it is best to set your **When I log in**Â preference to **Ask me to choose an authentication method**. Then when you log in to a system that requires Duo, you will see a dropdown to choose which device to authenticate with.Â You will be able to choose the appropriate device, and thenÂ select any appropriate applicable method . **Will Duo ask for my password?** Duo, Clemson's partner in 2FA, will never ask for your user ID and password. If you receive such a request, do not respond. **What if I only have one device registered and it's not available to access my account?** We recommend that you have two devices registered with Duo in case one device is unavailable. Â In the event that you can't access your account due to your device(s) being unavailable, please contact the CCIT Support Center at 864-656-3494 for a temporary bypass code to allow access to your accounts.

Posted - Wed, Jan 25, 2017 at 8:55 AM.
Online URL: https://hdkb.clemson.edu/phpkb/article.php?id=488