DUO Security – Frequently Asked Questions (FAQ)

1. Do I have to use DUO every time I check my e-mail, or log on to a university service?
   a. While we do anticipate the university’s use of multi-factor authorization and DUO Security will increase in the coming years, as of now we have not scheduled an e-mail integration of DUO. If your department has opted to implement DUO to protect a specific service, you will need to authenticate using DUO in order to access that service.

2. Can I set up DUO on more than one phone?
   a. Yes, the self-service portal will allow users to configure multiple phones/mobile devices for DUO use.

3. I have a new phone and the DUO app stopped working, what should I do?
   a. You should use the self-service portal to enroll your new device. While inside the portal, you can also elect to delete old devices.

4. Can I use the DUO app internationally?
   a. Yes. The DUO Security mobile app is designed to work internationally, even providing authentication methods requiring no access to data or Wi-Fi networks.

5. What if I forget my phone at home?
   a. Users are encouraged to configure multiple devices and authentication methods within the self-service portal. This will allow users to have many ways to authenticate. If multiple devices have not been configured, it is easy to visit the self-service portal and have DUO call your desk or generate a single-use passcode, allowing authentication.
6. Do I need a smartphone to use DUO?
   a. No, DUO allows users to authenticate using a smartphone, cellphone, landline, tablet, or hardware token. We do recommend that users who have a smartphone elect to use DUO Push via the mobile app.

7. What if my phone is lost or stolen?
   a. If a phone or device that is configured for DUO use has been lost or stolen, you should, as quickly as feasible, visit the self-service portal on my.sc.edu to delete the missing device from your DUO account.
   b. If you are unable to access the self-service portal, you may also contact the UTS Service Desk at (803)777-1800 or servicedesk@sc.edu. This will allow the University Information Security Office to disable your DUO account temporarily to avoid fraudulent access to university data.

8. What if I do not have a cell phone, or do not wish to use my cell phone?
   a. DUO Security does not require that you have a cell phone or smartphone. Perhaps you should use the self-service portal to configure DUO to call your office landline? By working with your local system administrator, it may be possible to issue a hardware token, or key fob, at the department’s cost and discretion.

9. What if I do not have a data plan on my phone?
   a. If you have access to a Wi-Fi connection, DUO Push will still work.
   b. The DUO Security mobile app provides options that work without a connection, if necessary. The app can generate the required code without the need for an Internet or data connection.
   c. DUO Security does not require that you have a cell phone or smartphone at all! Perhaps you should use the self-service portal to configure DUO to call your office landline? By working with your local system administrator, it may be possible to issue a hardware token or key fob, at the department’s cost and discretion.
10. What if I do not have a data or Wi-Fi connection?
   a. The DUO Security mobile app provides options that work without a connection, if necessary. The app can generate the required code without the need for an Internet or data connection.

11. Am I required to use multi-factor authorization?
   a. Multi-factor authentication is required to protect applications/services that house or transmit restricted data. Multi-factor authentication is recommended for all other applications and services. DUO Security is a multi-factor authentication solution provided by UTS through the University Information Security Office.

   If a service you use at work has been onboarded to DUO, you will need to use the service to access that service.

12. Whom should I contact if I have questions or concerns about DUO?
   a. If you have questions or concerns about DUO Security, your local system administrator or SLA contact is the best place to start. If your question is still unresolved, put in a ServiceNow ticket by contacting the UTS Service Desk at (803)777-1800 or servicedesk@sc.edu. They can further answer your questions, and further escalate the matter, if appropriate.

13. I have an application that could/should leverage DUO. How can I start using/requiring it?
   a. If you are prepared to implement DUO Security as a multi-factor authentication solution, please reference the “DUO Security Onboarding Process” document. This document is available for viewing and downloading at sc.edu/multifactor.

14. How are accessibility issues handled?
   a. Due to the variety of authentication options available, we expect there is a way for DUO Security to accommodate every user.
15. Does DUO Security see or record my password?
   a. No. The university’s authentication systems verify your password internally. DUO only provides the second authentication factor, “something you have”.

16. Who is eligible to use DUO?
   a. The university’s implementation of DUO is licensed to include all faculty, staff, student employees, and university affiliates, with the capacity for discretionary additions on a case-by-case basis.

17. Does it cost me money to use DUO?
   a. It depends on how you set it up. DUO “Push” authentication through the mobile app will consume a very small amount of Internet data traffic to function (a few kilobytes per login). This difference likely is not noticeable. Text messages and voice calls to phone are only sent when you request them, and will be billed by your carrier like any other text message or inbound voice call.

   The university will not reimburse users for any expenses incurred. If you are concerned that you could incur significant expense by using DUO on a device, you should choose another authentication method. The self-service portal will allow you to configure DUO to call your desk landline. You could also talk to your local system administrator about hardware token technology.