Our team is here to help.

If you are experiencing difficulty configuring or using DUO Security, it is best to discuss the issue with your local system administrator or IT representative. Departments may elect to use DUO Security in a variety of ways. Your local administrator can likely help solve your issue.

The URL below will provide a number of resources for your use. These resources include a self-enrollment guide, a list of frequently asked questions, and more.

Should your issues remain unresolved, please contact the UTS Service Desk (contact information below). Our service desk representatives are prepared to help you understand DUO, aid in troubleshooting the product, and escalate the issue as needed.

Contact Us

University Technology Services
University Information Security Office
1244 Blossom Street
Columbia, SC 29208
803-777-1800
servicedesk@sc.edu

www.sc.edu/multifactor

UNIVERSITY OF SOUTH CAROLINA

The University of South Carolina does not discriminate in educational or employment opportunities or decisions for qualified persons on the basis of race, color, religion, sex, national origin, age, disability, genetics, sexual orientation or veteran status.

University Technology Services
University Information Security Office
University of South Carolina

DUO Security

A guide to configuring, managing, and using Duo Security

UNIVERSITY OF SOUTH CAROLINA

Welcome to the future.

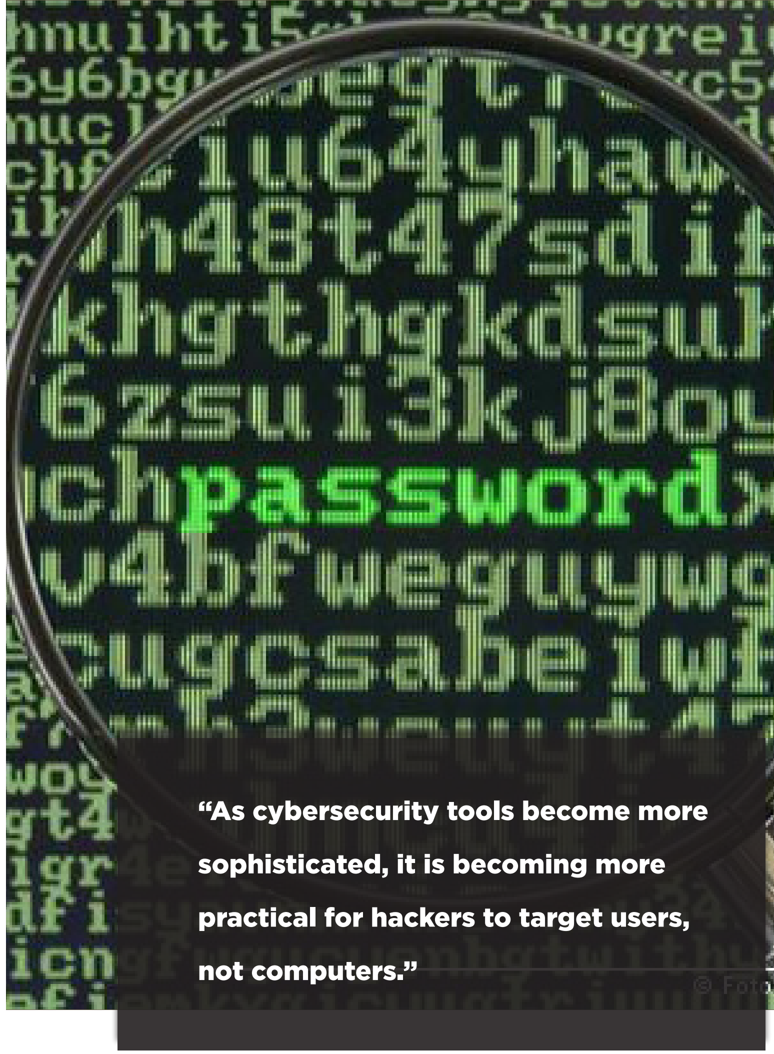
Multifactor authentication (MFA, also often referred to as two-step or two-factor authentication) is an overly technical sounding term for a very easy solution. Simply, it is a security tool that uses more than one verification technique to prove that a person attempting to access an account is really them. It is an important second layer of security for accounts and those who access data at the University of South Carolina.

The most common layer of security we are all familiar with is a password. We all deal with passwords each day. But, what happens if someone discovers or steals your passwords? Anyone could access your accounts!

That's where MFA comes in. Without MFA, anyone who discovers your password could gain access to any account protected by that password. However, if MFA has been enabled to protect an account, a password alone will not grant access.

Using MFA is similar to using your debit card at an ATM to get cash. To get cash, you must have your physical debit card, and you also have to know your PIN. Similarly, MFA combines something you know (your password) with something you have (your phone, a token, a code, or a key fob).

Enabling an MFA service adds the additional layer of protection to accounts and the data you access through them. Think of MFA as a brand-new deadbolt lock for your account. Because MFA requires something only you have, if your password gets stolen, it will be much more difficult for someone to access your accounts and subsequently compromise university data.



"As cybersecurity tools become more sophisticated, it is becoming more practical for hackers to target users, not computers."

You are a target, too!

As cybersecurity tools become more sophisticated, it is becoming more practical for hackers to target users, not computers. With today's detection technology, one mistake can sound the alarm to security professionals. Because of that, many would-be hackers are choosing to target the people who use computers. If a hacker can discover an authorized user's account credentials, they're far less likely to sound the alarms that will get them caught.

MFA is an efficient and effective way for the University of South Carolina to help reduce the risk of account takeover.

Getting Started with DUO Security

"DUO Push" Initial Set Up

1. If you haven't done so, set up your VIP ID security questions by visiting **https://my.sc.edu/vipid/claim**. Here you will fill in the fields with the requested information. Once your security questions are configured, you may visit **https://my.sc.edu/multifactor**. Log in using your USC Network Username and password.
2. Answer one of your VIP ID security questions.
3. Press the submit button.
4. Enter the phone number of the device you wish to configure, then select whether it is a land line or mobile phone.
5. If it is a mobile phone, select your smartphone's operating system from the dropdown menu.
6. Click "**Add Phone**."
7. Select "**Activate.**" If you have enrolled a smartphone, a QR Code will be displayed.
8. Search "DUO Mobile" in the Apple App Store, or Google Play Store.
9. Install the App, then open it and tap the **+** button at the top of the screen.
10. Scan the QR Code from step 8, then select "**Continue.**"
11. Select "**Test authentication**," then enter your USC Network Username and password.
12. Select your configured device from the dropdown menu and select "DUO Push" and click "**Log in**."

Authenticating with DUO "Push"

DUO "Push" is the recommended way to authenticate using DUO Security. Once your device has been configured to work with DUO, the DUO "Push" technique is mostly hands off. When you attempt to access a service that is protected by DUO Security, you will enter your USC Network ID and password. Within seconds, you will receive a notification on your mobile phone that someone is attempting to access your account. Simply approve the log in from your phone to verify your identity.

Enter your Network username and password, as usual.
Use your phone to verify your identity.
Securely logged in

Authenticating with voice calls

While using the DUO Security Mobile App in conjunction with "DUO Push" is the recommended authentication method, it is also possible to authenticate using a voice call. To do this, it is necessary to repeat the steps from the previous column. When prompted to enter the phone number, provide the phone number for the device you wish to receive DUO calls. It may be a mobile phone, or your office landline.

When you are ready to test your configuration, select "**Test Authentication**," then enter your USC Network Username and password. Choose your desired device from the dropdown menu, then select the bubble beside "**Phone call**." Within moments, you should receive a voice call from DUO. Simply press 1 on the telephone keypad to verify your identity.

Authenticating with SMS Text Messages

DUO Security also allows users to authenticate via text message. If your mobile device has not been previously configured to work with DUO, you will need to complete the steps from the previous column.

When you are ready to test your configuration, select "**Test Authentication,**" then enter your USC Network Username and password. On the next page, select the appropriate device from the dropdown menu, select the bubble for "**Passcode,**" then click "**Send SMS passcodes.**" That link will change to text and read "*Next SMS passcode starts with 1.*" You should have received an SMS message to your phone. Locate the passcode in the message that begins with 1 (or the appropriate number). Enter that passcode in the DUO passcode field and your authenication is complete.

Hardware Tokens and Key Fobs

DUO Security supports hardware tokens and key fobs . The implementation of this technology will require a procurement and incur additional cost to the department.

While more costly than other authentication methods, hardware tokens and key fobs can be a trustworthy way for users to present their second authentication factor. These devices may be useful for those who travel internationally or work remotely. To learn more about hardware tokens, including information on supported devices, place a service ticket with the UTS Service Desk by calling (803)777-8823.

Using your mobile phone to authenticate using DUO "Push", voice calls, or SMS text messaging will result in mild data and/or service useage and is subject to billing,as defined by your contract with a service carrier. **The university will not reimburse for expenses.**

What if I forget my phone?

Sooner or later, most of us will forget our mobile phone. Don't worry, DUO Security provides ways for you to access the accounts you need, even without your mobile phone.

You can also visit the DUO self-service portal at **https://my.sc.edu/multifactor**. From this portal, you can generate a one time passcode that will allow access the appropriate system. You could also ask DUO to call your desk phone. If your device was lost or stolen, this portal will also allow you to delete the device from your DUO account, insuring no one can use it to access accounts in your name. It may also be possible to speak with your local system administrator or IT representative about procuring a hardware token or key fob for your use, at the department's expense.

DUO Security offers an effective way for the university to implement multifactor authentication (MFA) without crippling the business process.