UC SANTA BARBARA

THE Current

July 16, 2021

Harrison Tasoff

Multi-factor Authentication Q&A

UC Santa Barbara will roll out multi-factor authentication (MFA) for VPN access this summer, with plans to use the protocol for a number of other applications over the course of the next year. The goal is to apply the best security practices to ensure the integrity of campus networks, data and user accounts. The University of California has chosen Duo Security as its MFA provider, and UC Santa Barbara has already implemented Duo for several of its IT services.

Multi-factor authentication secures information using not only what you know, but also what you have. A familiar example is withdrawing money from an ATM: What you know is your PIN, and what you have is your bank card.

When logging into an account, what you know is your password, and what you have is a device, like a smartphone. Together these grant you access.

Sam Horowitz, the campus's chief information security officer answered questions about the new protocol.

Who will this affect?

This change will affect everyone that uses the campus Pulse Secure virtual private network (VPN) service.

What services will be affected?

Multi-factor authentication was required to access UC Path as of late 2020. Recently several financial system applications were added to the list of those requiring MFA. Now, VPN will be added. This will be followed by other services in the fall.

If you're a Power BI user on campus, you will also need MFA to access that service. You will need it to access a departmental network via the campus virtual private network (VPN). However, for now, you will still be able to access the general campus network with the VPN without multi-factor authentication.

IT staff with administrator functions may also require Duo for multi-factor authentication.

Beginning later in 2021, MFA will be required for nearly everything that currently requires a single sign-on, including timekeeping in Kronos and the campus VPN.

Why does the university need multi-factor authentication?

Multi-factor authentication is recognized as a best practice for protecting accounts. It has been effectively used in industry for decades and many service companies either offer or require it of their customers.

As a matter of course, the campus security operations center receives notifications of compromised accounts from multiple sources almost every day. The criminals with access to these compromised usernames and passwords can't use them when MFA is in place.

Will things just switch over, or do I need to sign up for something?

Faculty and staff will need to enroll in multi-factor authentication with Duo Security. The fastest and simplest method is to use your cellphone.

What are the options for authentication?

The best option is to use the Duo app. Download and enrollment instructions can be found at it.ucsb.edu/mfa. Authentication can also be established via text message or using a small token device.

With Duo, you can set multiple devices to act as authenticators, for example, a second smartphone or a tablet.

How do I enroll?

To enroll, go to it.ucsb.edu/mfa and click the big blue button that says “Enroll in MFA now!” This will take you to a page with step-by-step instructions on how to enroll.

If you need to get a token, call 805-893-5000 and request one, though we hope you’ll use your smartphone. It is the fastest, easiest way to use multi-factor authentication.

Can I use multi-factor authentication for my personal accounts?

Absolutely. If you set up MFA, no one can access your accounts even if they have your password because they need the additional factor as well. For more info on multi-factor authentication visit twofactorauth.org.

What is the process for people who do not have smartphones?

Those who don’t have or want to use their smartphones will need to use text messaging or the tokens. That said, using the token is as easy as pushing a button and typing six digits.

What happens if my phone is stolen or compromised?

Multi-factor authentication is what you have AND what you know. So even if they have your phone, a criminal would still need to know your password to access your accounts. It takes two to tango.

What options do I have if my phone is lost, broken, or outside the service area?

If you are out of service area, you can always generate the six-digit code with the Duo application itself. It will appear even if you are outside of cellphone range.

Otherwise, call 805-893-5000 and they will set you up so you can log in without MFA for a few days until you’re able to enroll another device, at which point MFA will work again as normal.

What information will I need to provide to reset my multi-factor authentication?

The service desk will follow the same process to reset your MFA as if you had lost your password.

What happens when I get a new phone?

In Duo, you just select “enroll a new phone.”

Can I use a tablet without cell service?

Absolutely. Just download the Duo app. Multi-factor authentication can be done over Wi-Fi.

Are there any complications if I’m trying to login with multi-factor authentication from out of state or abroad?

You shouldn’t encounter any major issues with MFA while out of state or abroad. In rare cases with satellite phones, there may be enough lag that push authentication may not work, and you will need to use a code generated from the app or a token to log in.

How long do I need to keep the Duo app on my phone?

You will need to keep the Duo app installed on your device as long as you’re using MFA. So essentially as long as you’re employed at the university.

If I already have Duo installed, will it work for UCSB requirements?

Absolutely. You don’t need to do it again.

Will there be any conflict between multi-factor authentication I set up on my own and those required by UCSB and other institutions?

No.

Will Duo have a separate entry for each account and service?

It will not.

You can create multiple entries for other services and accounts you wish to use Duo for without any conflict. Duo can also allow multiple devices to serve as authenticators with the app.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.