2-Step Verification with Duo FAQ's

How it works

What is Two-Step Verification with Duo?

Two-Step verification with Duo also known as "multi-factor authentication," provides an extra layer of security in addition to passwords. This additional step ensures that your University information, transactions or online work is safer from unauthorized access by requiring a second method to verify your identity – such as a phone, code, token, or other registered device. Even if someone obtains your password, they cannot access your account without having your registered Two-Step device. You can set up two or more verification options through Duo (see Multi-Factor Options below).

Who needs to use Two-Step Verification with Duo?

Two-Step Verification is currently optional (available by request) for Sacramento staff, but will be required for staff and faculty who use PeopleSoft CMS and CFS, and those with access to Level One Data. Ultimately, the goal is to have full campus participation to ensure increased network security.

What are the benefits of using Two-Step Verification with Duo?

Two-Step Verification with Duo provides extra protection for the sensitive University information our systems contain in case you are a victim of phishing or hacking. If someone steals your credentials and tries to access your account, your user name and password will not be sufficient to log in. The thief will also need to have access to your device to complete the login process. If someone else tries to log in to your account and attempts to send a push, you will be notified on your device, and you can deny them access.

Which University services or systems require 2-Step Verification with Duo for login?

After you enroll in 2-Step verification with Duo, you will receive a Duo log-in notification when you sign into participating Sac State applications.
Setup

How do I enroll?

You can request enrollment in 2-Step Verification with Duo through the IRT Service Desk. Within 1 business day, you will receive a text message with information to register your phone. If you chose a token, you will receive an email letting you know when your token is ready to be picked up at the IRT Service Desk in AIRC 2005.

1. If you choose to use the Duo mobile app (recommended, not required), download it from the Apple or Android app store prior to enrolling.
2. When you enroll, you’ll need to select a secondary method (hardware token, desk phone, etc.) so that you won’t get locked out.

How does the 2-Step Verification with Duo mobile application work?

Two-Step Verification with Duo uses mobile technology to send an authentication request to your registered device. When you log into My Sac State and participating SacState applications, click Send Push at the Duo prompt, and a request will be sent to your smartphone, or other registered device. You simply tap to approve it, or enter a code.

How do I set up automatic Duo Push/Call notifications?

If you enable automatic Duo Push/Call, the system will automatically send an authentication request as either a push notification to your Duo Mobile app, or a phone call to your device (depending on which you’ve selected). To enable this feature:

1. In the Duo Control Settings panel, click "My Settings & Devices" and authenticate using your chosen device.
2. Scroll down to "Default Device" and select the device you’ll use with automatic Duo Push/Call.
3. Click the drop-down menu under "When I log in" and select either “Automatically send this device a Duo Push” or “Automatically call this device.”
4. Click Save.
How do I set up Duo to require one log-in per day (Remember me for 12 hours)?

To avoid being prompted by Two-Step Verification with Duo multiple times a day, select the checkbox next to Remember me for 12 hours during log-in.

Limitations on Remember Me for 12 hours:
* It won't carry over between different computers, or switching web browsers (from Chrome to Firefox, for example).
* Due to some technical limitations, it isn’t available for all services. It also may not carry over between different services, or if you block cookies, or are using incognito mode.

I don't have my 2-Step Verification with Duo device (or my backup) with me. What can I do?

No problem! Contact the IRT Service Desk Team at 916.278.7337, servicedesk@csus.edu, or drop in to AIRC 2005.

Multi-factor Options

What options can I choose for my 2-Step Verification with Duo?
When you enroll, you’ll select two verification methods to prevent you from being locked out of your account. **Note:** you are not required to use your personal smart phone.

**Most common**
- Mobile device/smart phone (with Duo mobile app)
- Sacramento State campus desk phone
  **Alternatives** If you prefer not to use your smart phone
- Duo Hardware Token (keychain fob)
- U2F Yubikey token (plugs into your device USB port)

Can I enroll more devices in 2-Step Verification with Duo?
You can register multiple devices to your account, so you can always access your account even if one device is temporarily unavailable. After you enroll, you can add additional devices such as hardware tokens and tablets.

How do Hardware Tokens Work?
Duo tokens work with any browser and do not require a USB port. Duo tokens display a passcode at the touch of a button, which you type into the open Duo prompt.
How does my campus desk phone work with 2-Step Verification with Duo?
On the Duo prompt, you'll click the “Call Me” button, and Duo will call your desk phone.
Answer the call and listen to the instructions to authenticate: the recorded voice will ask you
to press any key on your phone to log in.

Devices & Data

What devices does the Duo mobile application support?

The Duo mobile app works on most current smart phones and devices, including:

- iOS devices (iPhone, iPad, iPod)
- Android devices (phone, tablet)
- Blackberry
- Windows Phone 7
- Windows Mobile

Learn more about other Duo supported devices/OS versions.

What if I don't have/don't want to use a mobile device?

Although use of the Duo Push app on a mobile device is recommended, Duo supports
multiple device options including using your campus phone extension, or hardware tokens.
(See Multi-Factor Options section.)

My mobile device is on an older OS, and I'm unable to
install the Duo mobile application from the App Store. What
do I do?

You may need to upgrade to a newer iOS or Android version to install the Duo mobile app,
or choose a different combination of multi-factor options, such as a Duo Hardware Token
(keychain fob) paired with your campus desk phone, or a U2F Yubikey token that plugs into
your device USB port. (See Multifactor Options section.)

How do I manage or edit my 2-Step Verification devices?

The next time you receive the Duo login prompt, click the "My Settings & Devices " link in
the menu on the left. Complete the Duo authentication on your second device. Then select
"Devices" to manage/add a new device.
Can I use the app on my smart phone without affecting my data plan?

Yes! To use the Duo app with no impact on your data plan, connect to a wireless network, open the Duo Mobile app, and tap the green key icon. Rather than a push notification (which uses data on your plan), a passcode (set of numbers) will appear. You'll use this passcode to log into the system.

How do I authenticate with the Duo Mobile app if I don't have cell signal, data, or Wi-Fi connection?

If you cannot use a “Push” or “Call,” use a “Passcode.” You can generate a passcode by opening the Duo app and touching the "California State University" option. You will receive a 6-digit passcode which you can enter on the Duo prompt window to authenticate.

If you chose a token as one of your Duo authentication options, you can also generate a passcode using your token.

I replaced the phone that I had registered for my 2-Step Verification with Duo. What should I do?

If you use the Duo Mobile app, you will need to access your 2-Step Verification settings and re-enroll your mobile phone by adding it as a new device.

- If you have an alternate/backup device (such as your desk phone or token) enrolled in Duo 2-Step Verification handy:
  - Go to My Sac State and log in. When you get a Duo screen, DO NOT SEND A PUSH, select the “Duo Settings” button.
  - From the Device drop-down menu, select your alternate/backup device, then click “Manage Devices” to authenticate using Duo.
  - Use the “Actions” drop-down menu to delete your old phone, then click “Enroll another device” to enroll your new phone. (See the Device Management Guide for detailed tutorials)
- Don’t have an alternate/back-up device with you? Contact the IRT Service Desk Team at 916.278.7337 or servicedesk@csus.edu.
I lost my device I use to authenticate using 2-Step with Duo. What should I do?

If you lose your phone or suspect it has been stolen, contact the IRT Service Desk Team at 916.278.7337 immediately. The team can disable your phone from being able to authenticate with 2-Step Verification, and can assist you with logging in with another method.

Troubleshooting

My account is locked out. What should I do?

The most common reason why your account is locked is because you have entered an incorrect password for your My Sac State account, or the 2-Step Verification has failed at least 10 times. Please contact the IRT Service Desk Team at 916.278.7337 or servicedesk@csus.edu.

What if I receive a 2-Step Verification push notification on my device that I didn't request?

Important: If you receive a push notification from the Duo app that you did not request, it means someone is trying to log in using your account, and your My Sac State account may have been compromised. Tap the Deny button in your Duo app, and contact the IRT Service Desk Team at 916.278.7337 or servicedesk@csus.edu for assistance.

Why have I stopped receiving push notifications on the Duo Mobile app?

You may have trouble receiving push requests if there are Wi-Fi issues between your mobile device and Duo Security. Many mobile phones have trouble determining whether to use the Wi-Fi or cellular data when checking for push requests. Simply turning the phone to airplane mode and back to normal operating mode again often resolves these issues, or connecting to a reliable Internet connection. Similarly, the issue may be resolved by turning off the Wi-Fi connection on your device and using the cellular data connection. If these two methods do not resolve the issue, contact the IRT Service Desk Team at 916.278.7337 or servicedesk@csus.edu.