Security & Anti-Malware

Learn about how to keep your computer secure.

- Information Security Overview
- Password Checklist
- Recommended Anti-Malware Software
- Duo 2-Factor Authentication
    - Set Up Duo 2-Factor Authentication
    - Sign In with Duo 2-Factor Authentication
    - Recovering Duo 2-Factor Account
    - How to Access Duo Multi-Factor Authentication

Information Security Overview

Every day, it seems there is another news story about the latest data breach, ransomware attack, or other security related threat. ***Please*** take the time to read this page in full, and implement the advice contained here. Remember, the first defense against any malware attack or identity theft is **you**, the user.

Account Security	**Email-Related Threats**	**Identity Theft/Hacked Account**	**Password Managers**
Anti-Malware Software	**Adblock**	**Clear Web Browser Cache**	**Update Web Browser**

Identity and Data Security

Account Security

Q: How do I keep my accounts secure?

A: We recommend that you use a different password for every account you have. Each password should be unique and complex. A complex password contains a minimum of 8 characters. The key to a secure password is the longer the better. You can also include at least one lowercase letter, one uppercase letter, a number, and symbol. See Secure Password Management to learn where you can store all your passwords securely and in one place.

Email-Related Threats

Phishing

When reading your emails, always stay vigilant. If you receive an email—and something seems fishy about it—always listen to your gut. An email may look completely legit, but a corporation will never ask for you to email them things like your password or credit card information in plain text. Look at the URLs of the links in the email. Check the sender's email address. Never open a suspicious attachment. If something seems off, it probably is. The scam artists are getting much more sophisticated at seeming legitimate, but if you use a little bit of common sense, you should be able to catch when things don't feel right, and act accordingly. More information about how to detect phishing attempts and how to report phishing emails can be found in Google's Gmail Help Center.

Email attachments

Never open a suspicious attachment! And generally, do not open attachments that you were not expecting, or aren't from a trusted source. Gmail, and most webmail services have good malware scanning built in these days, but if the file is over 25MB, the scan won't run. Be careful, and stay vigilant. Again, practice common sense.

Phone-Related Threats

Scam Calls / Robocalls

If you receive a phone call that seems suspicious, whether it's a computer-generated voice on the other end or a person fishing for personal information: Don't follow any directions given by the caller. Just ***hang up the phone***. Following any prompts given by the caller may make them more likely to call again. ***Never give out any personal information*** to an unknown caller. Take down any information you remember and report the call to the FTC.

These calls often show up as being from a local phone number, spoofing of numbers is rampant among scam callers, to hide the call's origin and make the calls difficult to block.

Identity Theft/Hacked Account

Q: Help! My account has been compromised, what can I do?

A: The first and foremost thing you should do if you still have access to your account is to change all your passwords and security questions, along with anything associated with your account. Let your contacts know that your account has been compromised and to not open any suspicious

emails from you. After updating your passwords and security questions, check your email settings and make sure nothing has been changed. It is not uncommon for hackers to modify your recovery email address and automatically forward your emails to them. Scan your computer for malware and viruses (See our Anti-Malware Software section). For more information on securing your account:

- Secure an account that has suspicious activity (Google)
- Recover a hacked or hijacked account (Google)

Password Managers

Q: There are too many passwords to remember! What can I do?

A: LastPass is a password manager for all of your devices. LastPass is great for storing passwords for websites, web services, or just about anything else. It's more convenient and secure than your web browser's password manager, in that you can connect on all your devices. There is a LastPast Website and web add-on, a desktop application, and a mobile phone app. This means you only need to remember one password to have access to your passwords on all your devices.

You can download LastPass from here: https://lastpass.com/misc_download2.php

Q: How do I get started with LastPass?

A: Visit the LastPass User Support Page to learn how to make your profile secure and customize to your preferences.

There are some configuration settings you will want to get familiar with:

- Master Password - the one password you will need to remember to gain access into your LastPass account.
- Account Settings - add a recovery email or phone number, manage preferences, etc.
- Auto Logout - ensure LastPass logouts of your account when you are away from your device.

For a more detailed write-up on password management software, go here.

Anti-Malware Software

Q: How do I keep my computer secure?

A: We recommend downloading an antivirus and anti-malware software. To keep your computer secure, make sure that you keep your antivirus/anti-malware software up to date.

Windows 7 and **older**

- Microsoft Security Essentials - Unobtrusive, effective, and free.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Microsoft Security Essentials missed something, although it doesn't hurt to run it more often.

Windows 8 and **newer**

- **Windows Defender -** The successor to Microsoft Security Essentials, included with the operating system. You don't have to install any extra software.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Windows Defender missed something, although it doesn't hurt to run it more often.

Mac OS X

- ClamXAV - An antivirus software for Apple Macintosh provides full disk virus scans, scheduled scans and updates for times that suit you, automatic scanning of new downloads, quarantining infected files, and much more. Consider installing the free 30-day trial initially.
- Malwarebytes Anti-Malware - Has solid malware definitions in addition to an effective heuristics engine that will check your computer for software with suspicious behavior.

Network Security

Adblock

Q: What is an adblocker and which one should I use?

A: An adblocker is a web browser extension designed to prevent ads from appearing on a web page. Adblockers are useful on websites with questionable content where clicking on an ad may result in your computer downloading malware. We recommend uBlock Origin, which is available for Chrome, Firefox, and Edge.

Clear Web Browser Cache

Clearing your web browser's cache can help fix problems related to accessing web sites. If you are having problems accessing or otherwise using a website that you believe should be accessible and functioning normally, try clearing your browser's cache to fix the problem.

Q: How do I clear my browser cache?

Mozilla Firefox:

1. Click the menu icon (the three stacked horizontal lines near the top right of your browser window).
2. Click **History**, then choose the **Clear Recent History...** option.
3. Select the **Time Range** to clear (drop-down menu).
   - Select **Everything** to clear all cache.
4. Click **Details** to choose what history elements to clear.
   - e.g. Cache, Cookies, and Active Logins
   WARNING!: DO NOT check the Browsing & Download History or the Form & Search History boxes.
5. Click the **Clear Now** button.
6. Exit and re-launch the browser.

Google Chrome:

1. Click the menu icon (the three stacked horizontal lines near the top right of your browser window).
2. Hover your mouse cursor over the **History** menu option, then click **History** at the top of the expanded menu.
3. Click **Clear browsing data...**

4. Set the **Obliterate the following items** from drop-down menu to **the beginning of time**.
5. Check the **Cookies and other site and plugin data** and **Cached images and files** boxes ONLY. (Un-check all other check boxes)
6. Click the Clear browsing data button.
7. Exit and re-launch the browser.

Safari:

1. Open Safari.
2. Click on **Safari** in the upper toolbar and select **Clear History...**
3. Select **all history** from the drop-down list.
4. Click the **Clear History** button.
5. Quit and re-launch the browser.

Update Web Browser

Q: Why should I update my web browser?

A: It is important to always run the most updated version of your web browser. Using an outdated web browser can compromise the security of your computer and any networks to which it is connected. Web browser developers are constantly searching for security vulnerabilities and when they find them they fix them and update the software. Therefore, if you are running a later version of a browser you are leaving yourself vulnerable to malicious websites.

Do not use browsers that no longer have updates or are being retired (e.g. Safari for PCs, Internet Explorer).

Q: How do I update my web browser?

A: It is highly recommended to set up your browser to automatically update. For update instructions and how to set up automatic update follow the link for instructions for your specific browser:

- Google Chrome: this browser's default is to automatically update
- Firefox: this browser's default is to automatically update
- Safari: this browser updates with macOS updates
- Edge: this browser's default is to automatically update

NOTE: If the instructions outlined here do not match the menus and options in the web browser you are using, please check to be sure that you are using the most recent version of the web browser. Using an outdated web browser can compromise the security of your computer and any networks to which it is connected.

Password Checklist

*For information about **User Accounts**, including SJSU and CSUMB accounts, see the **User Accounts page** on the IT Website.*

Keep in mind that your Gmail password is not necessarily the same as your MLML password.

Password Checklist

A strong and unique password will keep your account safe.
Here is a checklist for creating secure passwords for all of your accounts:

- Your password should be easy for you to remember without being obvious for someone else to guess.
- The **longer and more complex** the password, the stronger it is.
  - Include a variety of characters, such as punctuation marks, numbers, and mix capital and lowercase letters.
  - Don't choose a dictionary word as your password.
- Have a **recovery email** or **phone number** set up with your account to be able to recover it in case you lose access.
  - Here are the Google Account Recovery instructions.
  - If you ever have a situation where your account is compromised, check to see that the recovery email or phone number hasn't been changed.
- **Never use the same password** on multiple accounts. A **password manager** can help you keep track of your passwords (and generate very strong passwords).
- **Use multi-factor authentication**. This adds an extra layer of security by having you approve a login with your smartphone or entering a code sent to your smartphone or from a physical token.
  - Gmail 2-Step Verification instructions.
  - All SJSU employees must use Duo 2-Factor Authentication to access SJSUOne services. For instructions, see our Guide to set up Duo 2-Factor Authentication.
- **Never tell anyone your password**.
- **Never write down your password**. Use a **password manager** instead!
- Periodically **change your password**.
- Make sure you have strong passwords on all of your accounts.

Recommended Anti-Malware Software

We recommend downloading an antivirus and anti-malware program. To keep your computer secure, make sure that you keep your antivirus/anti-malware software up to date.

Windows 7 and **older**

- Microsoft Security Essentials - Unobtrusive, effective, and free.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Microsoft Security Essentials missed something, although it doesn't hurt to run it more often.

Windows 8 and **newer**

- **Windows Defender -** The successor to Microsoft Security Essentials, included with the operating system. You don't have to install any extra software.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Windows Defender missed something, although it doesn't hurt to run it more often.

macOS

- ClamXAV - An antivirus software for Apple Macintosh provides full disk virus scans, scheduled scans and updates for times that suit you, automatic scanning of new downloads, quarantining infected files, and much more. Consider installing the free 30-day trial initially.
- Malwarebytes Anti-Malware - Has solid malware definitions in addition to an effective heuristics engine that will check your computer for software with suspicious behavior.

Duo 2-Factor Authentication

Set Up Duo 2-Factor Authentication

****Did you get a new phone and not setup Duo Restore beforehand? Visit our Recovering Duo 2-Factor Account page to learn how to setup Duo 2-Factor Authentication on a new device.****

What is Two-Factor Authentication?

Two-Factor Authentication (2FA) adds a second layer of security to your SJSUOne account. By verifying your identity using a second factor (such as your mobile device or a key fob), 2FA prevents anyone else from logging into your account, even if they know your password.

Duo 2FA only effects your SJSUOne account. Once it is set up, you must use Duo 2FA to sign-in to this account and its associated services (SJSU Email, PeopleSoft, CFS, FTS, etc). It does not apply to your MLML-specific credentials.

Currently, it is available to all SJSU/Foundation Staff, Faculty, and Student Employees.

To setup Duo 2-Factor Authentication:

- **Start with First Steps**
- **Proceed to Installation**
- **Continue to either SmartPhone (recommended) or Key Fob**
- **Finish by Enabling Third-Party Accounts for easy recovery**

First Steps:

- Go to the SJSU Duo Page
- Scroll down to **Register for Duo 2FA - SJSU Employees Only**
- Select the **Smartphone App** option in the **Duo Method** section of the form.
  - *Please Note:* Only select the **Key Fob** option if you *do not own a smartphone* or *absolutely refuse* to install the Duo App on your phone. A key fob is a small physical device that displays a continuously updating passcode. Please submit an IT Helpdesk Ticket to request a key fob.
- Enter your information and then **Submit** the form. Select "**College of Science**" in the **Division or College** section:

SJSU-Duo-Registration.png

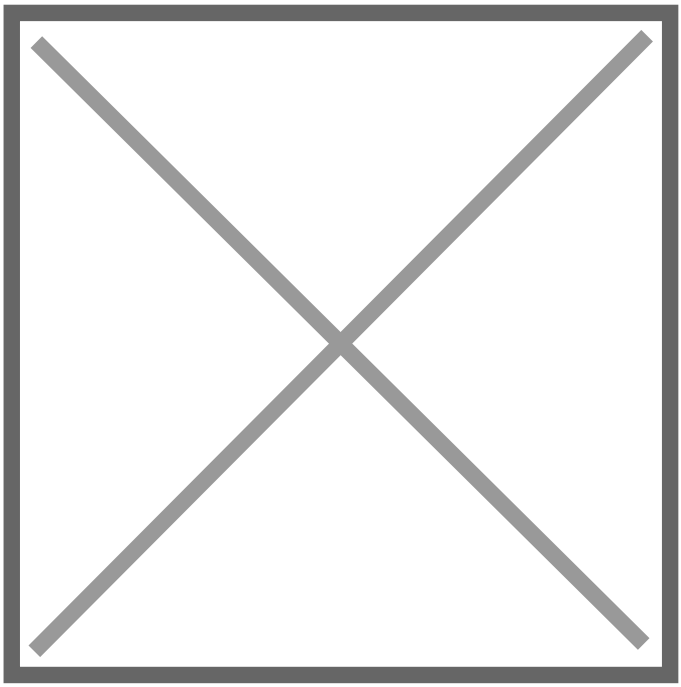
- Wait to receive an email from SJSU IT enabling Duo on your account
- Once you receive the email with setup instructions, it may take 1-2 hours for the change to sync to your account

Install Instructions:

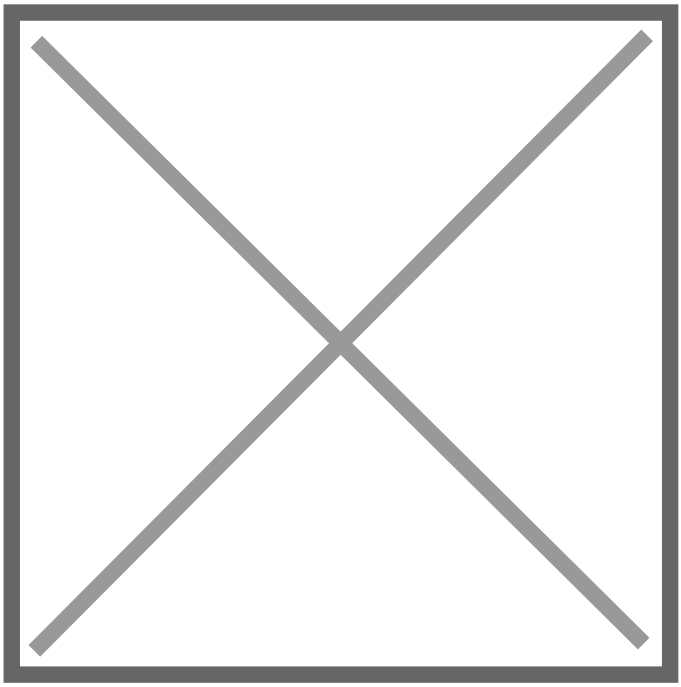
- Navigate to the **SJSUOne** page, or any other page where you use your SJSU login credentials (eg. SJSU Email):

SJSUOne-Sign-In.png

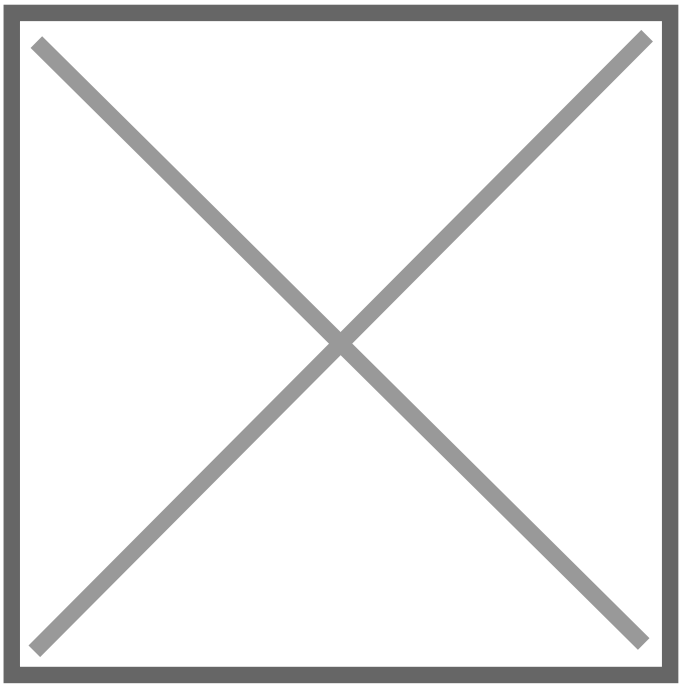
- **Sign In**:
  - Note: If you are already logged in, you may want to use your browser's incognito/private mode so that you do not have to log out and back in again.



- Click **Setup**:



- Scroll down and click **Start Setup**:



If you are using a Key Fob:

- Press **Enter a Passcode**, and press the single **Button** on your **Duo Key Fob**:

Duo-Fob-Select-Passcode.png

Duo-Fob.jpg

- Enter your **One Time Password** from the Key Fob into the passcode field and press **Log In**:
  - You have about 15 seconds to enter the passcode.

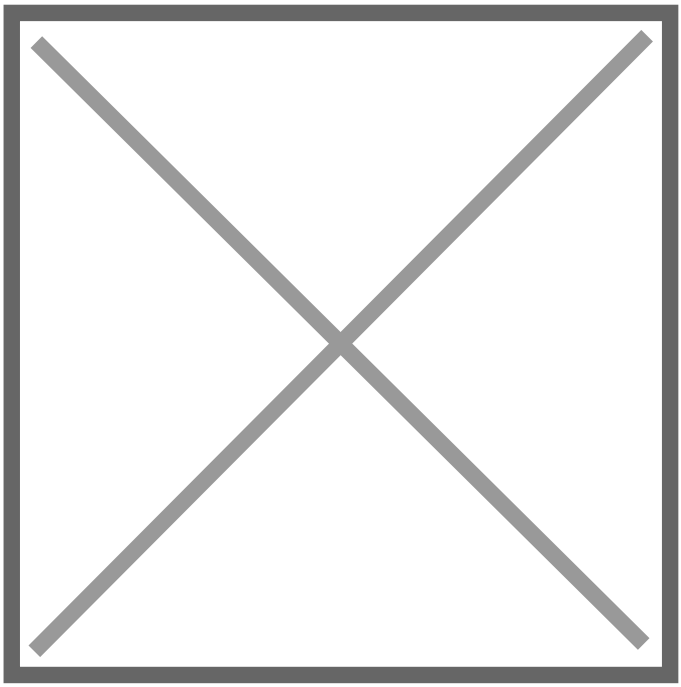
Duo-Fob-OTP.jpg

Duo-Fob-Login.png

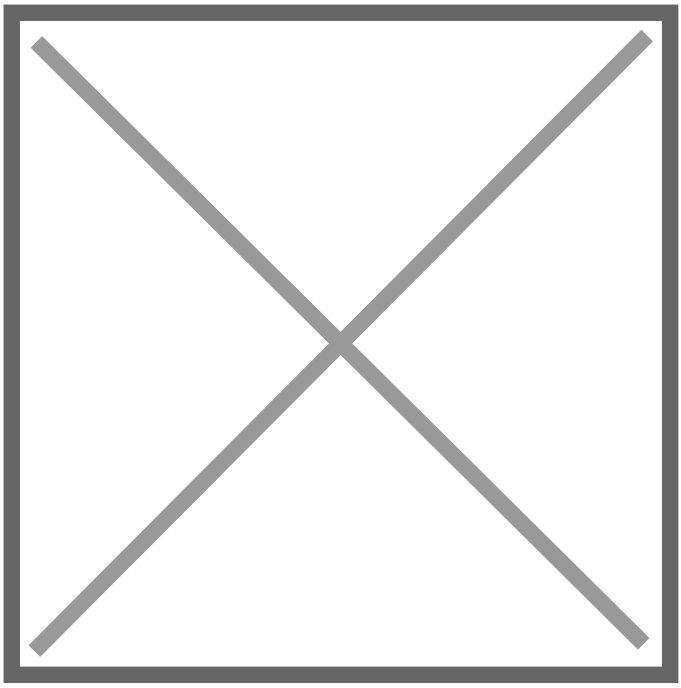
Congratulations, Duo 2-Factor Authentication should now be set up for use with your Key Fob!

If you are using a Smartphone:

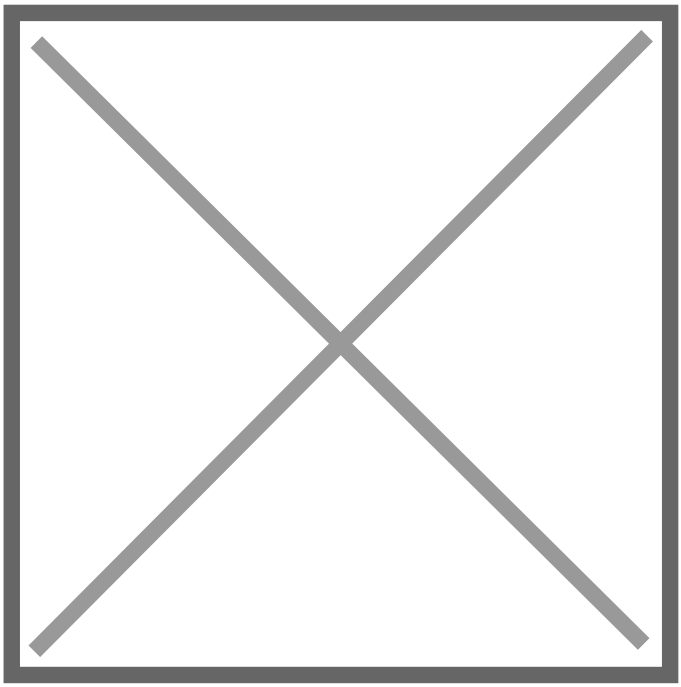
- Select **Mobile phone** and click **Continue**:



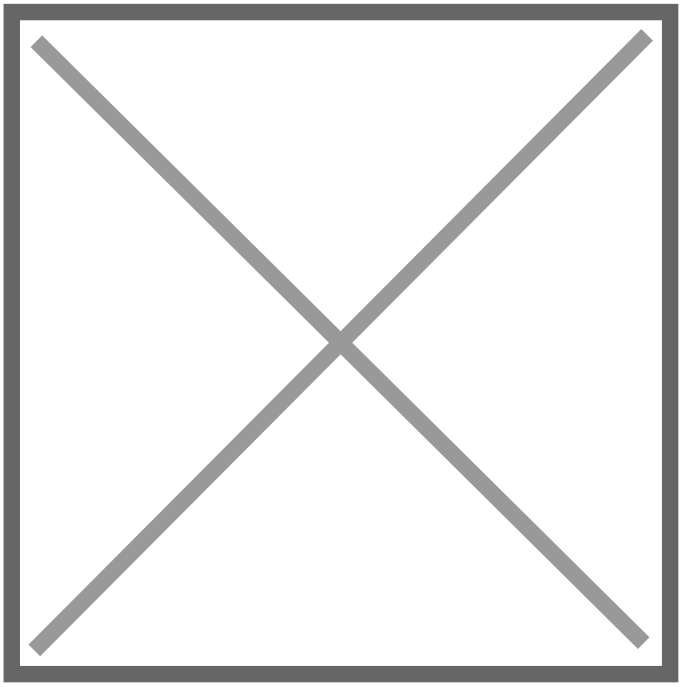
- Enter your **phone number** and click **Continue**:



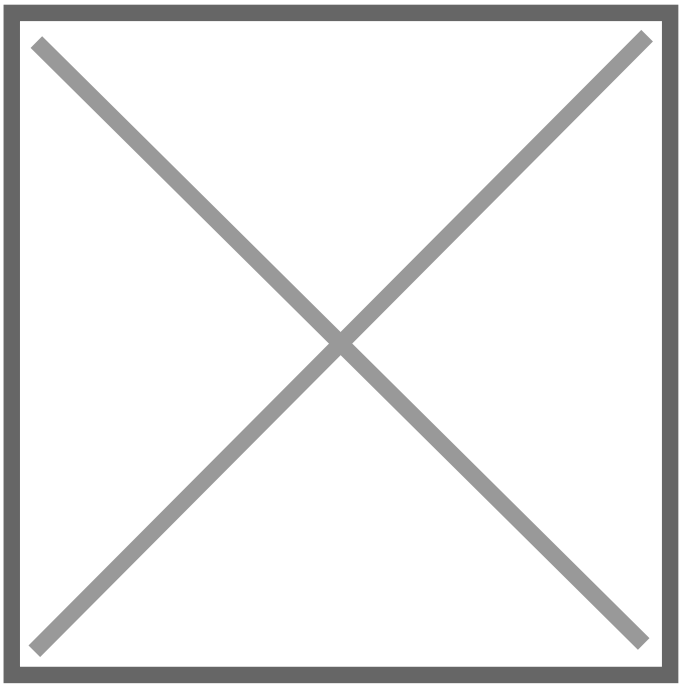
- Select the **type of phone** and click **Continue**:



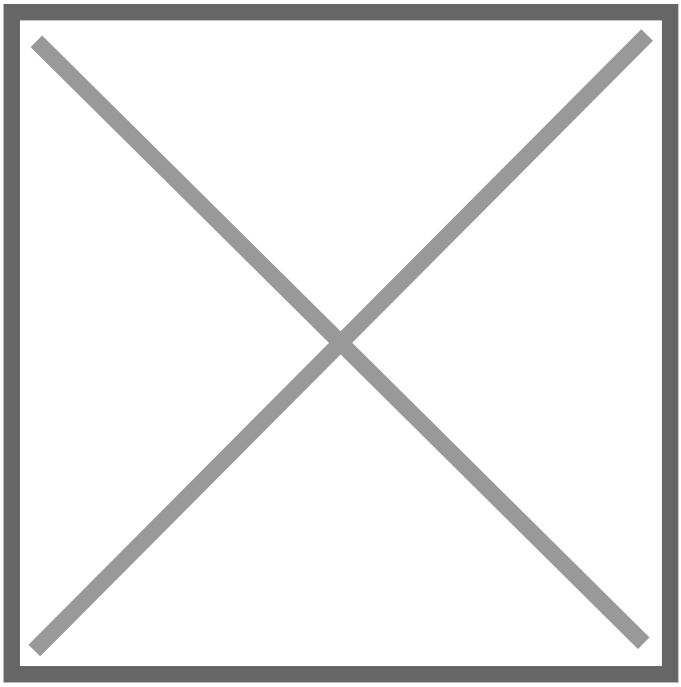
- Search and install “**Duo mobile**” from your app store onto your device:
  - Apple **App Store** for iOS
  - Google **Play Store** for Android
- Once downloaded, go back to setup screen and click **I have Duo Mobile** :

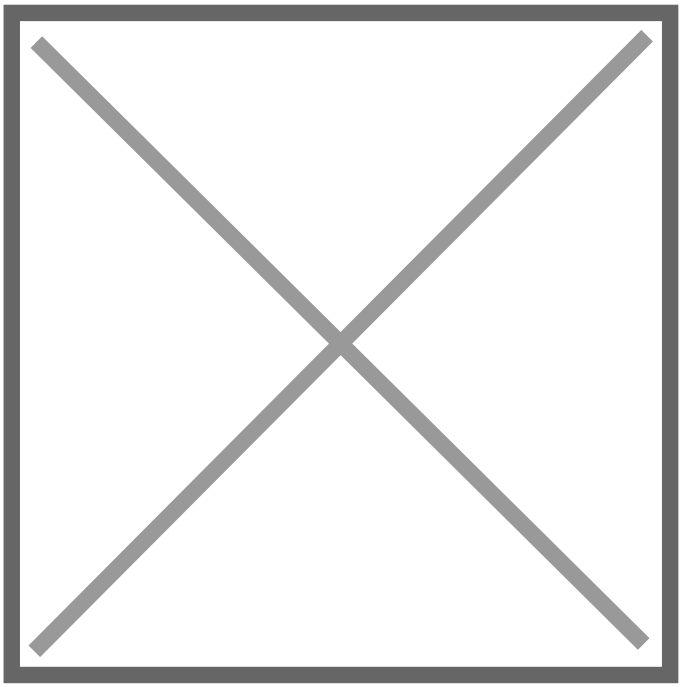


- Open the Duo Mobile app and tap **Get Started** or **Add Account**:

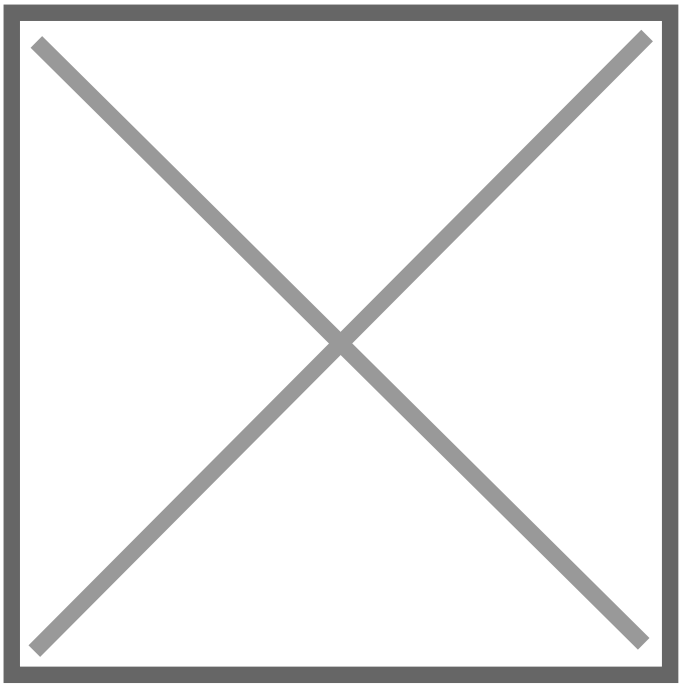


- **Allow camera permissions** on your device if you have not already, and **scan the QR code** that appears on the setup screen:

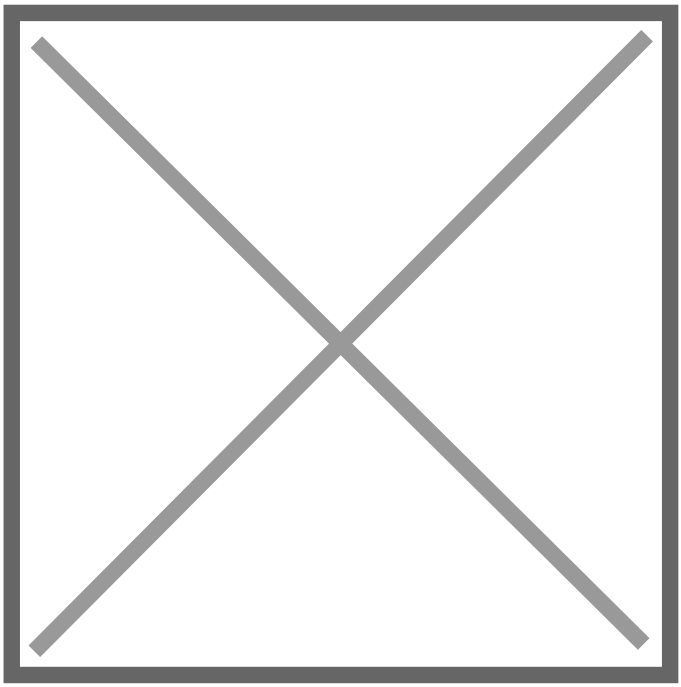




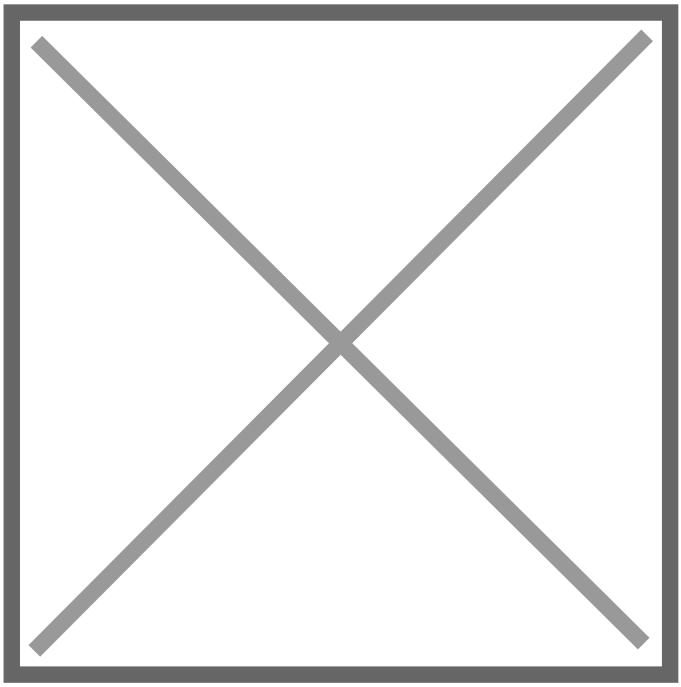
- Once you have scanned the QR code, scroll down and click **Continue** on the setup screen:



- Check/set device settings for Duo and click **Continue to Login**:

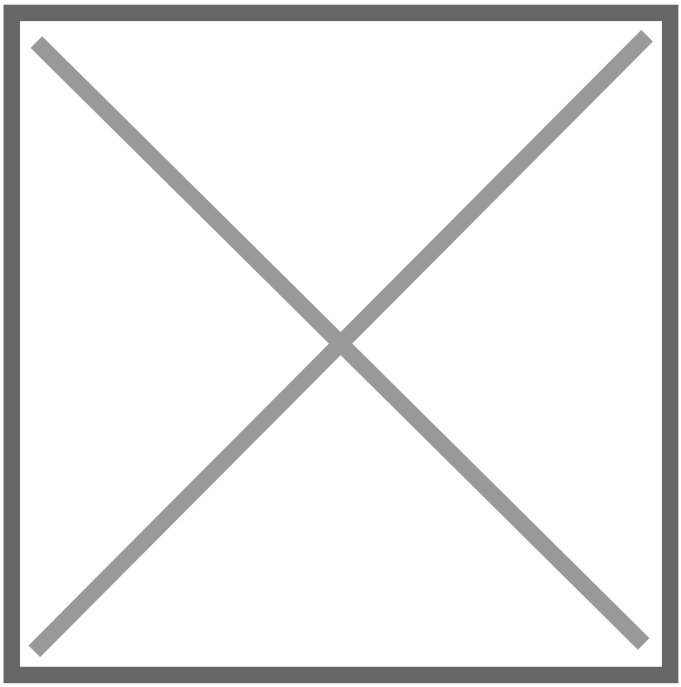


- Congratulations, Duo 2-Factor Authentication should now be set up for use with your smartphone!

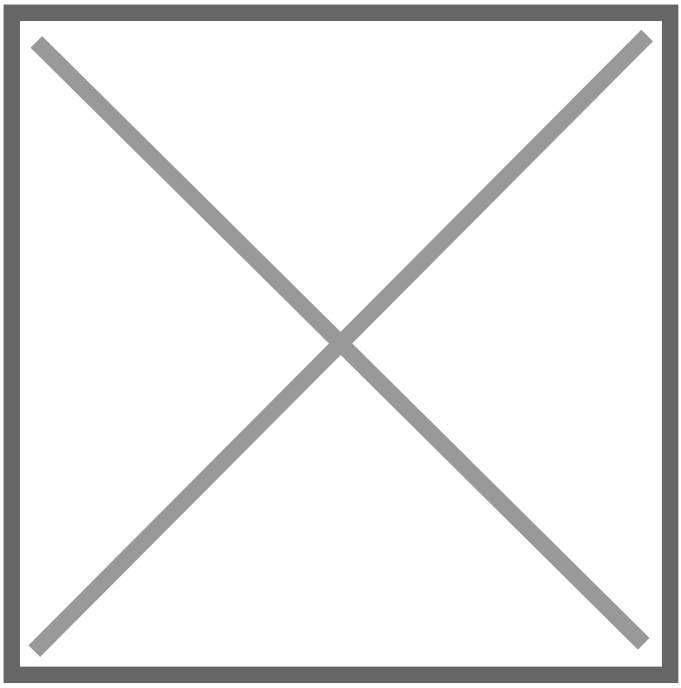


Signing In:

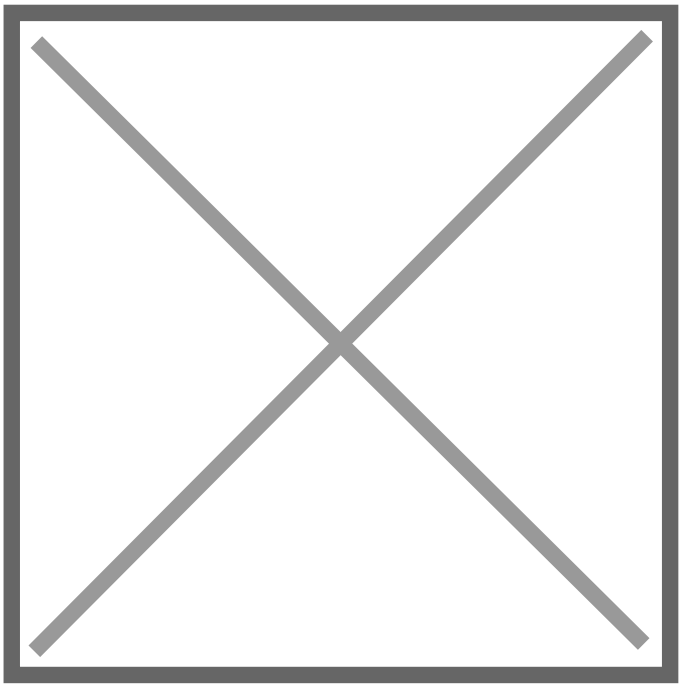
- To sign in with Duo 2FA from your computer or other device, click **Send Me a Push**:



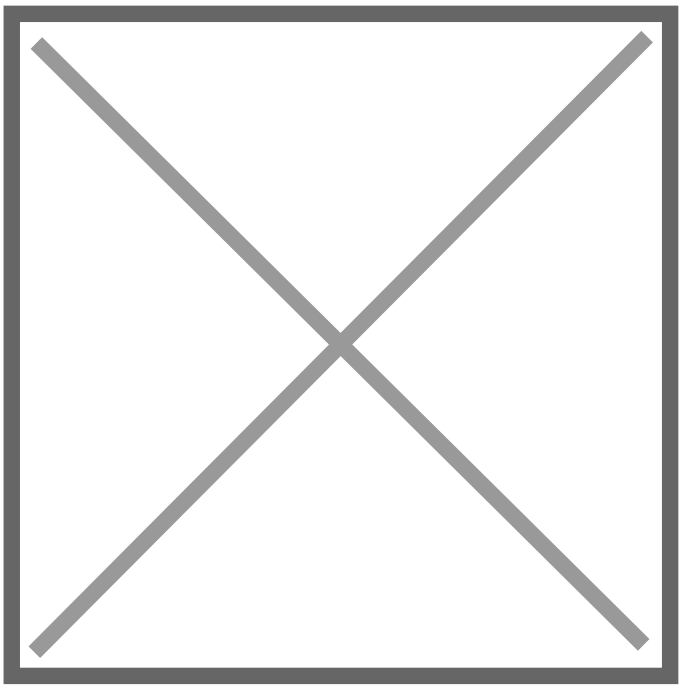
- Press **Approve** on your phone:

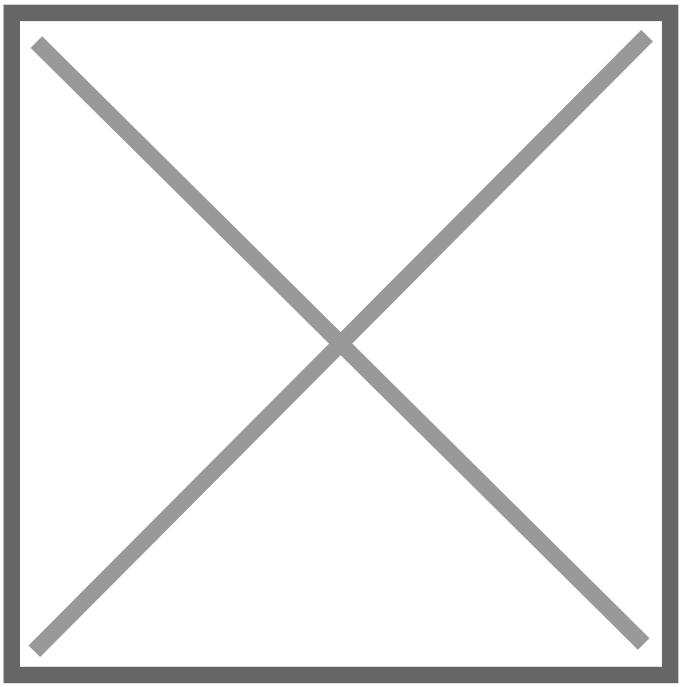


- Alternatively, click **Enter Passcode:**
    - Entering a passcode may be helpful in situations where the push notification won't get through, for instance when your computer has a connection to the internet but you have no data service (cell or WiFi) on your phone.



- Enter the **passcode** from Duo on your phone into the field on the device you are signing in with:





Enable Easy Account Recovery:

Recovering your account on a new device can be made simple by setting up Duo Restore NOW - before you get a new device. It backups your account and uses a recovery password that you can enter on your new device to register that new account. If you do not do this, you will have to unregister your old device, then register your new device with SJSU IT (even if it is the same number).

To learn how to setup Duo Restore for your iOS or Android follow the instructions on this page.

For more information:

- SJSU Duo Page
- Duo End-User Guide

Sign In with Duo 2-Factor Authentication

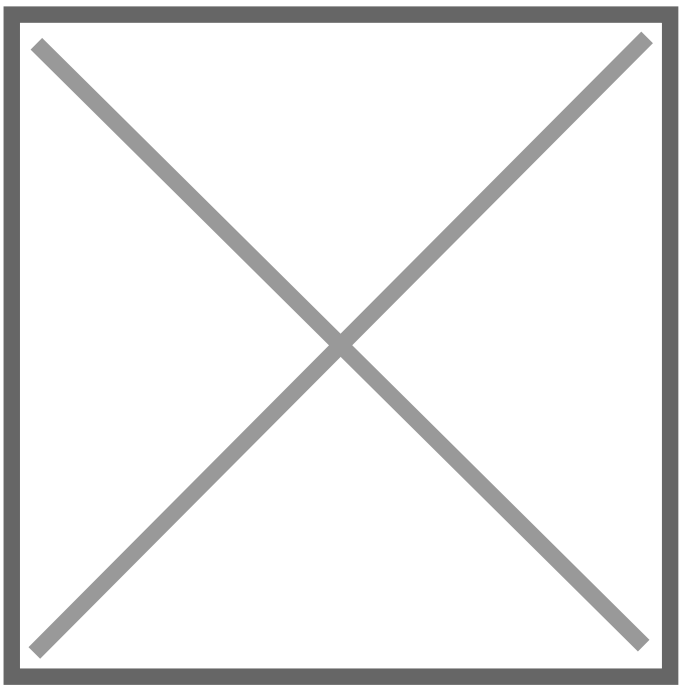
This page assumes you have **previously set up** Duo 2-Factor Authentication with your **smartphone** or a **key fob**. If you have not, please see our Duo Set Up Guide.

First, sign in to SJSU Normally:

- Navigate to the **SJSUOne** page, or any other page where you use your SJSU login credentials (eg. SJSU Email):

SJSUOne-Sign-In.png

- **Sign In** with your SJSU ID Number or SJSU Email Address and Password:
- ◦ Note: If you are already logged in, you may want to use your browser's incognito/private mode so that you do not have to log out and back in again.

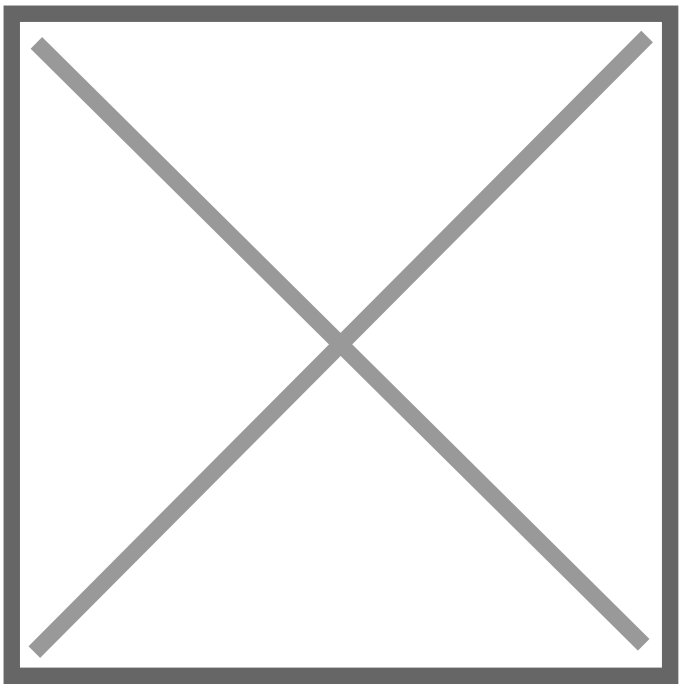


Your browser will now bring up the Duo 2-Factor Authentication page, the method you use to sign in with Duo 2-FA will vary based on which option you select and whether you are using a smartphone or a key fob.

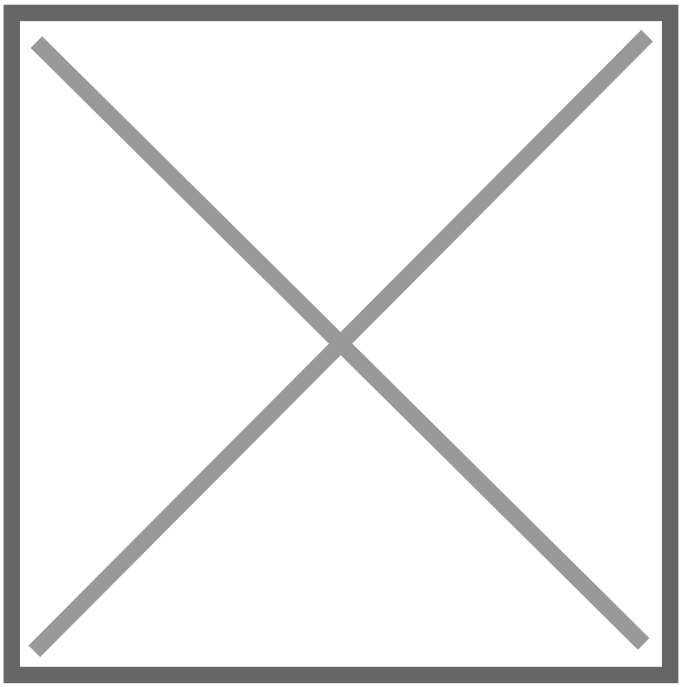
These methods are outlined below.

Sign In with a Push Notification:

- To sign in with 2-factor Authentication from your computer or other device you are signing in with, click **Send Me a Push**:

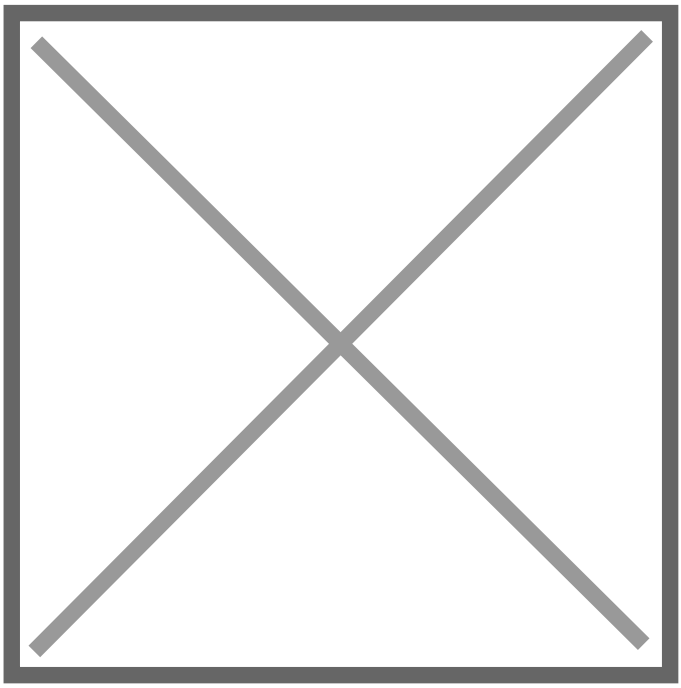


- Press **Approve** on your phone:

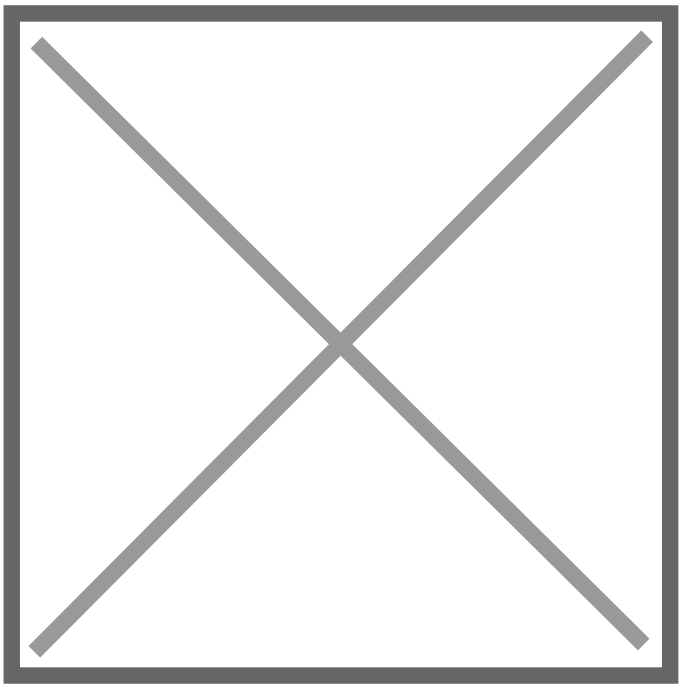


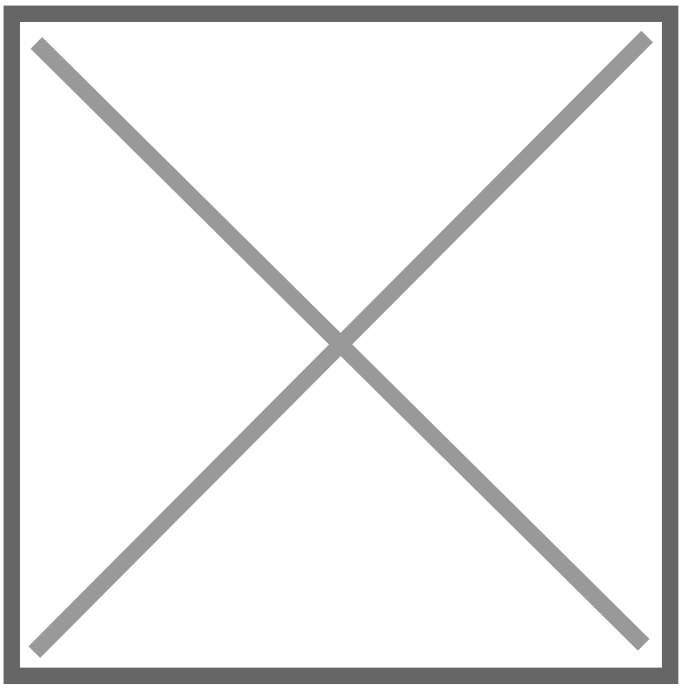
Sign In with a Passcode:

- Alternatively, click **Enter Passcode:**
  - Entering a passcode may be helpful in situations where the push notification won’t get through, for instance when your computer has a connection to the internet but you have no data service (cell or WiFi) on your phone.



- Enter the **passcode** from Duo on your phone into the field on the device you are signing in with:





Sign in with a Key Fob Passcode:

- On the Duo **Sign in** page, where it says **Device**, make sure the device selected is **Token**:

Duo-Devices.jpg

- Press **Enter a Passcode**, and press the single **Button** on your **Duo Key Fob**:

Duo-Devices-Passcode-highlight.jpeg

Duo-Fob.jpg

- Enter your **One Time Password** from the Key Fob into the passcode field and press **Log In**:
  - You have about 15 seconds to enter the passcode.

Duo-Fob-OTP.jpg

Duo-Token-Passcode-Login-highlighted.jpeg

Recovering Duo 2-Factor Account

When you setup your Duo 2-Factor Account, it's important to setup Duo Restore to ensure easy account recovery if you get a new device or your account is deleted off your original device. However, if you did not enable Duo Restore before getting a new device do not fear, you can still recover your account by contacting the SJSU IT Help Desk. Follow the instructions below:

1. File an IT Ticket and include your name, and your SJSU email address and ID number.
2. When your request is processed, you will be sent a temporary bypass code.
    1. Visit the SJSU Duo MFA Settings page: https://sjsu.okta.com/signin/verify/duo/web
    2. Enter this code when prompted for a Duo code: image-1634258396430.png
    3. Follow the directions on the SJSU Duo setup page to add your new device as a Duo authentication device: https://www.sjsu.edu/it/services/computer-security/duo/

How to Access Duo Multi-Factor Authentication

What is Duo?

Two-Factor Authentication (MFA) adds a second layer of security to your SJSUOne account. By verifying your identity using a second factor (such as your mobile device or a key fob), MFA prevents anyone else from logging into your account, even if they know your password

Who should use Duo?

Students should set up Duo MFA to protect their account and private information from being hacked. As of September 2020, it is available to all SJSU staff and students

How does Duo work?

Two-Factor Authentication combines something you know (your username and password) with something you carry (your Apple or Android smartphone, or a Hardware Token / Key-Fob), to ensure that only you can log in to your SJSUOne account. After entering your username and password you will be prompted to confirm your login, using your device

Cost

- Using the smartphone app factor is covered by the CSU master license
- Hardware tokens (key fobs) are purchased by SJSU and provided to you. Replacements are available for broken or lost fobs

How do I set up Duo for my account?

Using a smartphone

1. Download the Duo mobile app
   - Apple Devices
   - Android Devices
2. Register for SJSU Duo
   - After you register, Duo should be enabled for your account within one hour

- At your next login, a series of prompts will guide you through the self service Duo Mobile enrollment process. The initial enrollment should be completed by logging in from a web browser on a computer, and having your phone with you

3. Secure login
    - Once your enrollment is complete, every time your SJSU ID and Password is requested, you will also get a notification pushed to your mobile device. Acknowledge this notification to complete the login process

Using a key FOB

The current procedures for student access to Duo are only for smart phones, so please contact the IT Service Desk for assistance by calling 408-924-1530 or by submitting a help desk ticket. Because Duo MFA is a security service, the IT Service Desk must confirm your identity before providing assistance.

More Resources:

SJSU's Duo for Students page

Duo's Guide to MFA's

Duo's YouTube channel