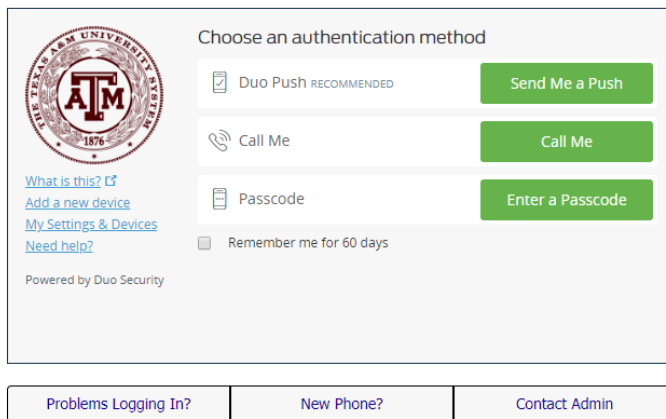


Two Factor Authentication in SSO

Two Factor Authentication is a security technique that supplements your SSO password – **something you know** – with a second, tangible identification factor – such as your phone, which is **something you have**.

SSO's two-factor process is implemented in partnership with [Duo Security](#). Using Two Factor Authentication in SSO means you will be prompted by Duo to acknowledge your login requests with your chosen method:

Current business rules require you to use [Two Factor Authentication](#) to help secure your account.



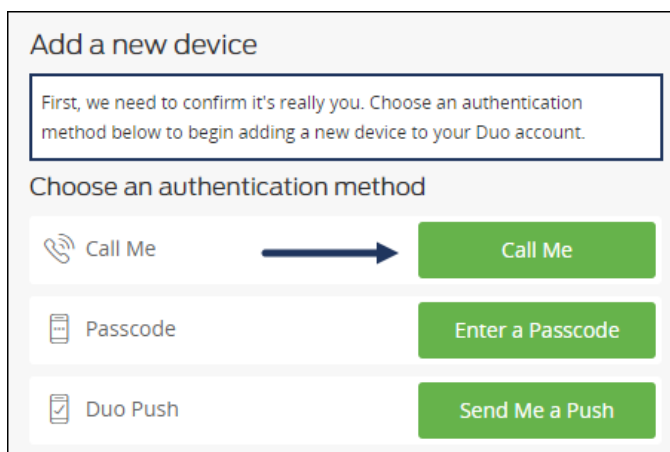
The screenshot shows the Duo Security authentication interface for TAMU. On the left is the TAMU logo. The main heading is "Choose an authentication method". There are three options: "Duo Push RECOMMENDED" with a "Send Me a Push" button, "Call Me" with a "Call Me" button, and "Passcode" with an "Enter a Passcode" button. Below these is a checkbox for "Remember me for 60 days". On the left side, there are links for "What is this?", "Add a new device", "My Settings & Devices", and "Need help?". At the bottom, there are three buttons: "Problems Logging In?", "New Phone?", and "Contact Admin".

Remember me for 60 days

Note that you can choose to have your **computer** remember your two-factor login for 60 days. This means you will not have to utilize the Duo prompt for this time period. You can select this option multiple times.

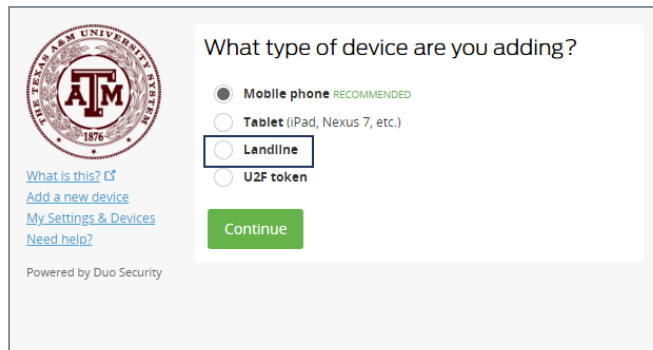
First Time Users

Click **Add a new device** and follow the instructions provided. You will be asked to verify your identity. It is recommended to provide your landline phone number for this initial verification process.



The screenshot shows the "Add a new device" verification screen. At the top, it says "Add a new device". Below that, a message box states: "First, we need to confirm it's really you. Choose an authentication method below to begin adding a new device to your Duo account." Underneath, the heading "Choose an authentication method" is followed by three options: "Call Me" with a "Call Me" button, "Passcode" with an "Enter a Passcode" button, and "Duo Push" with a "Send Me a Push" button. A blue arrow points from the "Call Me" option to its button.

Next you will be prompted to select a device to add as your default method. You can add additional devices later and remove as needed.



The screenshot shows a web interface for adding a device. On the left is the TAMU logo with the text 'THE TEXAS A&M UNIVERSITY SYSTEM' and '1876'. Below the logo are links: 'What is this?', 'Add a new device', 'My Settings & Devices', and 'Need help?'. At the bottom left, it says 'Powered by Duo Security'. The main content area is titled 'What type of device are you adding?' and contains four radio button options: 'Mobile phone RECOMMENDED', 'Tablet (iPad, Nexus 7, etc.)', 'Landline', and 'U2F token'. The 'Landline' option is selected and highlighted with a blue border. A green 'Continue' button is at the bottom.

Select the option you prefer. You can enroll multiple devices and types of devices. Typically users will use their office phone (landline) first and then their mobile phone.

- **Mobile phone** – Uses the free Duo app* to send you a notification (push) or phone call for identity verification
- **Tablet** – Uses the Duo app* to send you a notification (push) for identity verification
- **Landline** – Uses a phone call to your landline for identify verification
- **U2F token** – Uses a special hardware device (not currently available)

*Searchable using the app store on your Smart device

Follow the directions provided for the type of device you selected.

[Click here to learn about using Two Factor Authentication.](#)

Is Two Factor Authentication Required?

While it is not required for all employees to use Two Factor Authentication, it is recommended that it be used as an additional security measure for all SSO account holders.

Some users will be **required** to implement Two Factor Authentication.

Alternate Logins and SSO Two Factor Authentication

It is worth noting that the initial implementation of SSO's Two Factor Authentication only applies when logging into SSO using your UIN. The [alternate login applications](#) that can be used with SSO will not:

- use your SSO two-factor enrollment selection
- access your two-factor device(s) registered with Duo on behalf of SSO

Here are two links that will help you with Two Factor Authentication in SSO:

<http://it.tamus.edu/sso/?s=duo>

<http://it.tamus.edu/sso/help-system/key-concepts/security/two-factor-authentication-in-sso/>

<http://it.tamus.edu/sso/help-system/key-concepts/employee-navigation/profile/using-two-factor-authentication/managing-devices/>