

Duo 2FA Frequently Asked Questions

Table of Contents

- [What is Duo 2FA?](#)
- [What email applications are supported with Duo 2FA?](#)
- [I don't want to use my personal phone with Duo 2FA. What other methods are available to me?](#)
- [Does the Duo mobile app work without cellular service or wireless internet connectivity?](#)
- [I am being prompted to authenticate with Duo 2FA every time I log in.](#)
- [I left my phone at home and I am now at work. What do I do?](#)
- [I lost my phone and I cannot log in.](#)
- [I got a new phone and my Duo 2FA push notifications are not working.](#)
- [Can I use Duo internationally?](#)

What is Duo 2FA?

Duo 2FA is a two-factor authentication method with Duo Security. Two-Factor authentication protects accounts against unauthorized logins by requiring a "2nd factor" in addition to a username and password. The 2nd factor is often a mobile app that is registered ahead of time or a passcode that is texted or called. With Duo 2FA, SPU accounts will be further protected against malicious logins that result from phishing attacks or other forms of cyber scams.

- [Learn more about Two-Factor Authentication \(2FA\).](#)
- [Learn more about why SPU is introducing 2FA](#)
- [Enroll your SPU account with Duo 2FA.](#)

What email applications are supported with Duo 2FA?

The only email clients that are compatible with Duo 2FA and are fully supported by CIS is Microsoft Outlook for Windows and Mac, and Outlook Mobile for iOS and Android.

[Click here for more information.](#)

I don't want to use my personal phone with Duo 2FA. What other methods are available to me?

While CIS *highly* recommends using a smartphone and the Duo mobile app for Duo 2FA, we understand that this option does not work for everyone. The following additional 2FA methods are available with Duo:

- Passcode via text. Duo will text a registered number a one-time use passcode.
- Verification via phone call. Duo will call a registered number and ask you to verify the login.
- Duo hardware token. A physical token can be registered to your Duo account, which can be used to generate passcodes as needed.

[Click here for more details on all the 2FA Device options.](#)

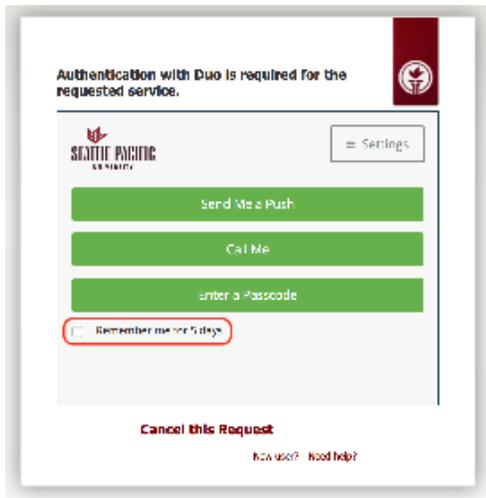
Does the Duo mobile app work without cellular service or wireless internet connectivity?

Yes! Even without connectivity, the mobile app can generate a passcode that you can use to authenticate.

1. Open the Duo mobile app
2. Tap the "Seattle Pacific University" entry to expand and see the passcode
3. In the Duo prompt at login, select "Enter a Passcode" to enter the passcode

I am being prompted to authenticate with Duo 2FA every time I log in.

When logging in with Duo 2FA, you have the option to remember the device and application you are logging in from. On the Duo 2FA screen during login, check the highlighted box before accepting the Duo 2FA prompt on your authenticated device. If you have already received an authentication prompt, you will need to cancel the prompt, check the box, and send a new prompt.



Duo 2FA will then remember the device and application for 5 days. This applies to the device + application combination, so you may need to check this box on several logins if you use multiple web browsers or devices. [Learn more about remembering devices in Duo 2FA here.](#)

I left my phone at home and I am now at work. What do I do?

Visit the CIS Help Desk in Lower Marston Hall or call at x2982 and we can provide you with a one-time 2FA passcode so you can log in and temporarily switch to a new 2FA device. [Click here for instructions on how to switch to a new 2FA device.](#)

I lost my phone and I cannot log in.

Visit the CIS Help Desk in Lower Marston Hall or call at x2982 and we can assist with deactivating your phone as an authorized 2FA device. We can also provide you with a one-time 2FA passcode so you can log in and switch to a new 2FA device. [Click here for instructions on how to switch to a new 2FA device.](#)

I got a new phone and my Duo 2FA push notifications are not working.

When a mobile app is registered with Duo 2FA as an authorized 2FA device, the registration is specific to the Duo app and the specific phone that is set up. If you purchase a new mobile phone, you will have to register the new phone with Duo 2FA and remove the old phone as an authorized device. [Click here for instructions on how to switch to a new 2FA device.](#)

If you require assistance or run into any issues, visit or call the CIS Help Desk in Lower Marston Hall or at x2982.

Can I use Duo internationally?

Yes. There are several options that may be useful:

1. Duo Mobile app - Even without internet connectivity, the Duo Mobile app can generate a passcode, which you can enter into the Passcode prompt in Duo.
2. Hardware token - A Duo hardware token can also generate a passcode, similar to the Duo Mobile app.
3. ByPass Code - Before you leave, CIS can provide you with a set of one-time use bypass codes to use during your trip
4. Normal Usage - If you have cellular service or a Wi-Fi connection, you can likely continue to use your typical method of authentication (Note: some countries may block the push notification because it is encrypted).

Related articles

- [Duo 2FA Device Management](#)
- [Application Requirements with Duo 2FA](#)
- [Duo 2FA Frequently Asked Questions](#)
- [Setting Up Duo 2FA](#)
- [Enrolling in Duo 2FA](#)
- [Login Process Changes with Duo 2FA](#)
- [Duo 2FA Device Options](#)