Setting Up HarvardKey Two-Step Verification

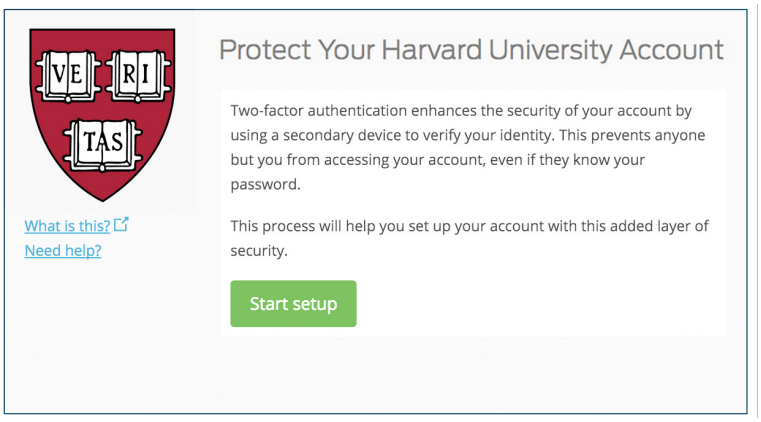
It's easy to set up two-step verification and add an extra layer of security to your HarvardKey account — all you need to do is register your phone, install the Duo Mobile app on your smartphone or tablet (if you have one), and activate two-step verification for your account.

These instructions depict installation of the Duo Mobile app for iOS, but the installation process for other mobile operating systems is very similar. If you're planning to use SMS or a phone call as your second factor for verification, follow the instructions below and choose the "landline" or "cell phone" options as appropriate. If you have any problems or need extra help, please contact the HUIT Service Desk at ithelp@harvard.edu or 617-495-7777.

1. Get Started

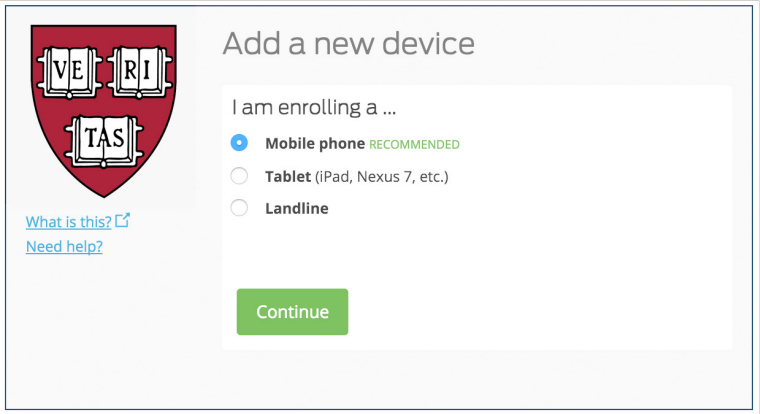
To set up two-step verification, log in to the HarvardKey self-service portal at **https://key.harvard.edu** and select the option for **Manage Your Account**. Then, click the option for **Manage Two-step Verification** and choose **Set Up Two-step Verification**. You'll be taken to a welcome screen that looks like the screen at the right.

Click **Start setup** to get started.



2. Choose Your Device

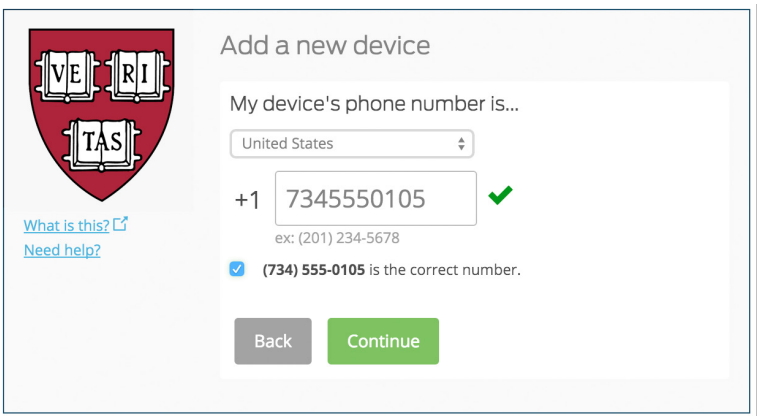
You can set up two-step verification for your HarvardKey account using a smartphone, SMS-capable mobile phone, wi-fi or cellular-enabled tablet, or a landline phone. However, using a smartphone is recommended for the best experience. Choose the device you plan to set up. When you're done, click **Continue**.



3. Add Your Phone Number

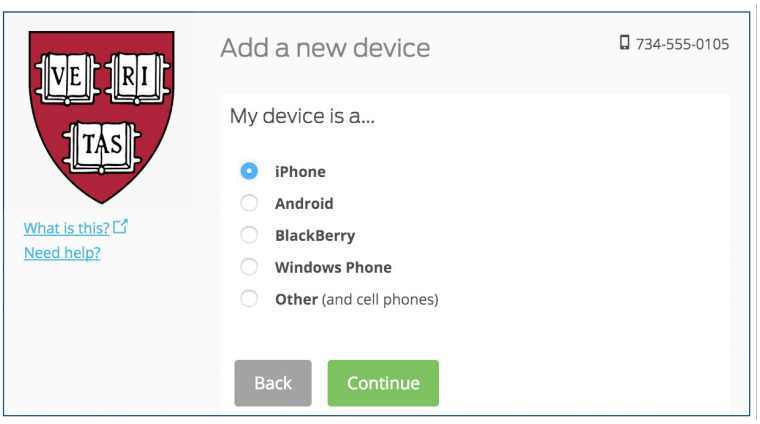
Next, select your country and enter your phone number. Use the number of the smartphone, cell phone, or landline that you'll have with you when you're logging in. If you chose "Landline" in the previous step, you can also enter an extension.

Verify that number, check the box, and click **Continue**.



4. Choose Platform

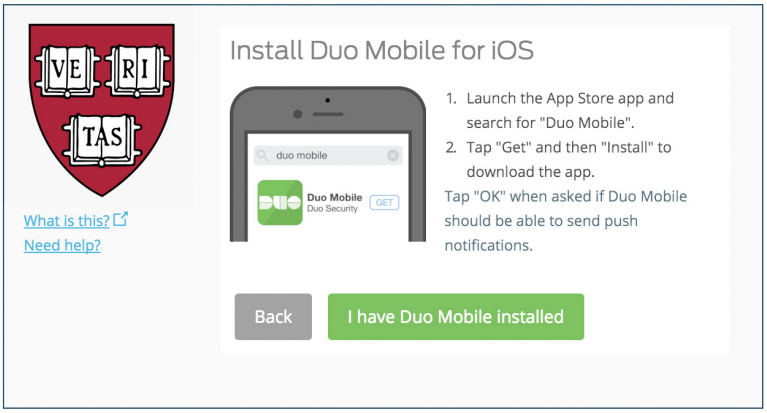
Next, choose your device's operating system. Duo Mobile supports most common operating systems, but if yours isn't listed, choose the option for "Other". When you're done, click **Continue**.



5. Install Duo Mobile

If you're using a smartphone or tablet for your second factor, you'll need to install the Duo Mobile app. It's fast and easy, it works in any country, and it doesn't require a cellular or wi-fi connection. If you don't have the app, you'll still be able to log in using a phone call or text message, but it's strongly recommended that you use the app to authenticate. (Duo Mobile supports as minimum versions Android 2.3.3, iOS 6.0, BlackBerry 10 and BBOS 4.5.0, and Windows Mobile 6.5.3.)

Follow the platform-specific instructions on the screen to install Duo Mobile. When you're done, click **I have Duo Mobile Installed**.

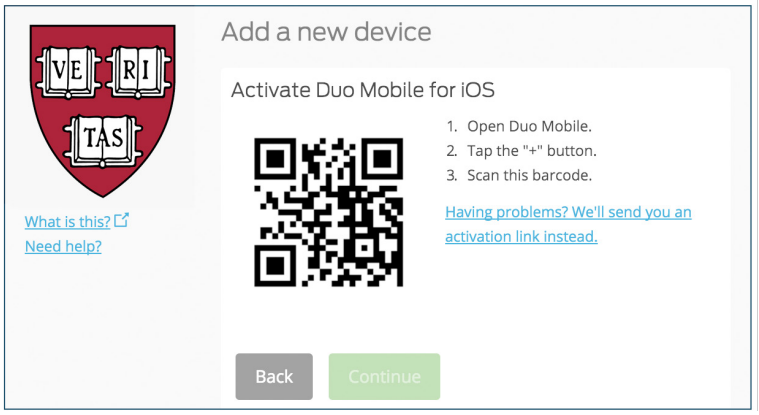


6. Activate on Your Device

Activating the Duo Mobile app will link it to your HarvardKey account so you can use it to log in.

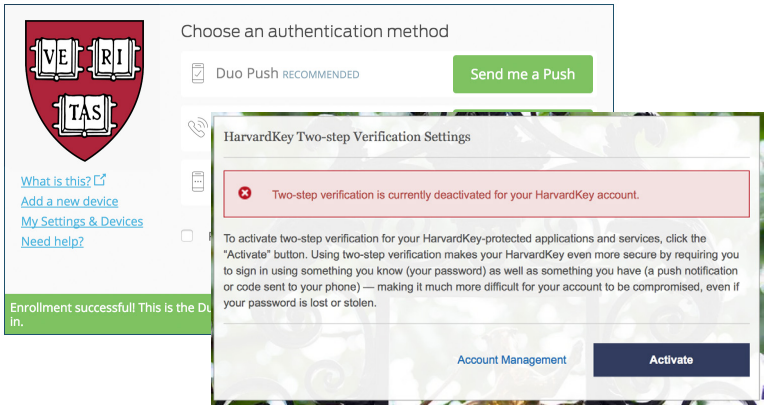
On iPhone, Android, Windows Phone, and BlackBerry 10, activate Duo Mobile by scanning the barcode with the app's built-in barcode scanner. You'll see a window that looks like the one at the right; after you scan the barcode, you'll be able to click the **Continue** button.

Can't scan the barcode? Click the prompt for the activation link and then follow the instructions.



7. Turn On Two-step Verification

Once you've activated the app, you'll see the screen at right. (It's also the prompt that you'll see when you log in to a HarvardKey-protected system and you have two-step verification turned on.) **Now you simply need to turn on two-step verification for your HarvardKey login.** To do this, go to the account management area of the HarvardKey self-service portal at https://key.harvard.edu and select **Manage Two-Step Verification**. From there, choose **Manage Your Two-Step Verification Settings** and follow the prompts to turn on two-step verification whenever you access a protected application or service. (You can turn off two-step verification here, too.)



Frequently Asked Questions

What devices can I use for two-step verification? What if I don't have a smartphone?

You can use two-step verification on a variety of devices. The simplest method is to download and set up the Duo Mobile app for your iOS or Android smartphone — then, in order to log in, just tap on the push notification you receive when you authenticate to a protected resource. If you don't have or prefer not to use a smartphone, you can also use two-step verification on a tablet, a mobile phone capable of receiving SMS text messages, or even a landline phone. See the table below for more information about what authentication methods are available for the device of your choice.

Device	Two-step Options	Platforms
Smartphone	• Duo Mobile push notification • Duo Mobile passcode • Text message • Phone call	• iOS • Android
Tablet	• Duo Mobile push notification • Duo Mobile passcode	• iOS • Android • Windows Mobile
Mobile Phone	• Text message • Phone call	• Any mobile phone capable of receiving SMS text messages
Landline	• Phone call	• All phones

What can I expect after I set up two-step verification?

After you set up and activate two-step verification, when you go to log in to a resource protected by HarvardKey, you'll be prompted to verify your login using the secondary method of your choice. In some of these instances, you'll see an extra page displayed after the regular HarvardKey login screen asking you to enter the code you receive. This works as follows:

- **If you use push notifications**, you'll see a push notification on your device; tap "Approve" to complete your login. (You need a wi-fi or cellular data connection to use this option.)
- **If you use a Duo Mobile passcode**, launch the Duo Mobile app to see your current authentication code; enter this code on the screen where you're logging in to a protected resource. (You do not need a wi-fi or cellular data connection for this option, because the app runs on your device.)
- **If you use a text message**, you'll receive a text containing the authentication code; enter this code on the screen where you're logging in to a protected resource.
- **If you use a phone call**, you'll receive an automated phone call asking you to press any key on your phone to authenticate.

Keep in mind that the frequency with which you're asked to log in using two-step verification varies depending on factors such as the sites or resources you try to use (some resources always require two-step verification), your individual browser and cookie settings, and others. To learn more about how "single sign-on" works in HarvardKey, see the HarvardKey FAQs at http://reference.iam.harvard.edu/faq.

I frequently travel internationally. How does this affect two-step verification?

If you travel internationally and need access to resources protected by HarvardKey, you may wish to set your two-step verification method (under "Manage Two-step Verification" in the HarvardKey self-service portal at https://key.harvard.edu) to Duo Mobile Passcode. Using Duo Mobile Passcode (available for smartphone or tablet), you can generate authentication codes even if you don't have an Internet, wi-fi, or cellular connection.

Please note that if you're traveling internationally (or have an international phone number) and are using text messages as your method of two-step verification, you may be subject to your carrier's roaming charges for SMS messages.

I lost my phone or got a new one. What do I do about two-step verification?

If you lose your phone, or suspect that it's been stolen, please contact the HUIT Service Desk immediately at ithelp@harvard.edu or 617-495-7777 so your phone can be disabled for authentication and we can help you log in using another phone or device. Note that even though it's important that you contact the HUIT Service Desk if your phone is lost or stolen, remember that your password will still protect your HarvardKey account.

If you get a new smartphone or mobile device, you'll need to re-activate the Duo Mobile app in order for it to work on the new device. You can do this yourself by visiting the HarvardKey self-service portal at https://key.harvard.edu and choosing "Manage Two-Step Verification" under "Manage Your HarvardKey Account." If you have any questions, don't hesitate to contact the HUIT Service Desk for help.

I no longer receive push notifications for two-step verification.

If you're having trouble receiving push notifications when you try to log in to HarvardKey, this may be because there are network issues between your phone and the Duo service — particularly if you're moving between buildings on Harvard's campus, as many phones can have trouble determining whether to use the wi-fi or cellular data channel when checking for push requests. You may be able to troubleshoot this problem easily simply by turning your phone to "airplane mode" and then back to regular operating mode again, or turning off your device's wi-fi connection and forcing it to use its cellular data connection.

If that doesn't work, check the time and date on your phone and make sure they are correct. If your date and time are manually set, try changing your device's configuration to automatically sync date/time with the network.

If you're still having troubles, log in to the HarvardKey self-service portal at https://key.harvard.edu with a passcode generated by the Duo Mobile app and then send a new activation link to your phone. You can do this under "Manage Two-step Verification" in the "Manage Your HarvardKey Account" section of the portal.