User Guide: Adding a Device in Duo and Managing Settings

The Duo Mobile application provides an extra layer of security when it is incorporated into the login process for applications or web sites such as uab.box.com. In addition to using your BlazerID and strong password to log in, Duo Mobile leverages a personal device (a smartphone, a tablet, a token, etc.) to add a second authentication layer. That way, if your BlazerID strong password is ever compromised, the bad guys still would be unable to complete the login process because they would not have access to your personal device and the final authentication process provided by the Duo Mobile app.

It is highly recommended that you use a computer to add a device to your Duo account and to manage your settings. Be sure that you are using one of the following supported browsers:

- Chrome,
- Firefox,
- Safari,
- Internet Explorer 8 or later,
- Opera

For more information about using Duo Mobile two-factor authentication (2FA) at UAB, please visit http://www.uab.edu/it/home/2-factor. Duo’s “Guide to Two-Factor Authentication” (https://guide.duo.com/) also is an excellent resource for learning more about 2FA, Duo’s Mobile app, and how everything works.

**Note:** This document assumes that you already have created a Duo account and completed the initial enrollment of a device for use with Duo. It also assumes that now you want to add a second backup device. Instructions for managing devices also are provided below. If you do not have a Duo account and you haven’t enrolled an initial mobile device for use with Duo, please visit UAB’s 2-factor web page and use either the Quick Start Guide or click on the button for the specific type of device you want to use with Duo. Those instruction sets will guide you through the creation of a new Duo account and enrollment of your first mobile device to be used with Duo.

**Adding another device to your Duo account**

To set up a second backup device, please conduct the following steps:

1. Launch a browser and visit UAB’s 2FA Sign-Up page. Click the “Manage Devices” button and login to that site by typing your BlazerID and strong password.
2. Once you have authenticated, you will arrive at the Duo landing page. Underneath the UAB logo on the left, an “Add a new device” link will appear. Click it to begin the process of adding another device.
3. To add a device, you must first successfully complete 2FA to begin the process. On your computer screen, you will be asked to choose an authentication method (this will be sent to your primary authentication device and will leverage the typical method you use for 2FA).
   a. If your primary device is a smartphone that uses the Duo Mobile app, it is highly recommended that you use the Duo Push notification method. If you are using the mobile app and a smartphone, click the “Send me a Push” button.
   b. If your smartphone doesn’t have a signal and you can’t get a Duo push, open the Duo Mobile app on your phone, click the green key to generate a PIN, return to your computer and type the PIN in the passcode field, and then push the “Enter a Passcode” button.
   c. If you are using a cellphone with SMS texts or a hard token, use a PIN provided by the device, enter it into the passcode field, and click the “Enter a Passcode” button.

4. Once you have successfully authenticated with your primary device, you now will be asked what type of secondary device you want to add. From here, you can leverage the following documents to add a new device:
Figure 2: One a user kicks off the "Add a new device" workflow, he/she can follow the enrollment processes detailed below to add a second authentication device.

- **iPhone**: Begin with step 5 of the enrollment process detailed in the iPhone Duo self-enrollment guide.
- **Android phone**: Begin with step 5 of the enrollment process detailed in the Android phone Duo self-enrollment guide.
- **iPad**: Begin with step 5 of the enrollment process detailed in the iPad Duo self-enrollment guide.
- **Android tablet**: Begin with step 5 of the enrollment process detailed in the Android tablet Duo self-enrollment guide.
- **Cell phone and SMS texting**: Begin with step 5 of the enrollment process detailed in the cell phone and SMS texting Duo enrollment guide.
- **Hard token**: Hard tokens should only be used in the event that the Duo Mobile app cannot be used with a smartphone or tablet. In order to request a hard token, a user must first gain approval for the request from his/her supervisor and then submit a ServiceNow ticket to AskIT. Due to these factors, UAB does not recommend using a hard token as a secondary authentication device. It only should be used as a primary device in instances where a user cannot leverage a smartphone or tablet with the Duo Mobile app. For more on hard tokens, please visit UAB’s two-factor token page.

5. Once you have successfully completed the steps in the appropriate guide detailed in the previous step, enrollment and activation of your secondary authentication device will be complete. You will be returned to the “My Settings & Devices” page.

**Managing your Duo authentication devices**

The “My Settings & Devices” link allows you to manage your authentication device or devices. From here, you can change a device’s name, choose a primary device, add another device, choose a preferred authentication method for each device, or remove a device.
1. To manage your devices, launch a browser and visit UAB’s 2FA Sign-Up page. Click the “Manage Devices” button and login to that site by typing your BlazerID and strong password.

2. Once you have authenticated, you will arrive at the Duo landing page. Underneath the UAB logo on the left, a “My Settings & Devices” link will appear. Click it to manage your Duo-enrolled device or devices.

3. To manage your devices, you must first successfully complete 2FA to begin the process. On your computer screen, you will be asked to choose an authentication method (this will be sent to your primary authentication device and will leverage the typical method you use for 2FA).
   
   a. If your primary device is a smartphone that uses the Duo Mobile app, it is highly recommended that you use the Duo Push notification method. If you are using the mobile app and a smartphone, click the “Send me a Push” button.
   
   b. If your smartphone doesn’t have a signal and you can’t get a Duo push, open the Duo Mobile app on your phone, click the green key to generate a PIN, type the PIN in the passcode field, and then push the “Enter a Passcode” button.
   
   c. If you are using a cellphone with SMS texts or a hard token, use a PIN provided by the device, enter it into the passcode field, and click the “Enter a Passcode” button.

4. The “My Settings & Devices” page will display all of your enrolled devices and the actions that you can take to manage them. From here, you can perform the following:
Figure 4: On the "My Settings & Devices" page, you can manage an existing mobile device, add another device for use with Duo, and set a specific device as the default for all Duo-related actions.

**a. Change the device’s name:**

i. If you want to change the name for your device, click the “Device Options” button to the right of the device.

ii. Once you click that button, a number of other buttons appear. Click the “Change Device Name” button.
iii. You now will be able to change your device’s display name by typing the name in the display field. **Note:** Hard tokens’ display names cannot be changed.

iv. Once you have typed in the new display name, click the green “Save” button at the right.

v. At this point, your device name will be changed. For example, if you are using an iPhone, your device name before was likely iOS and your phone number (iOS 555-555-1234). If you changed the display name to “Tom’s iPhone,” the display name should now be “Tom’s iPhone 555-555-1234.

b. **Select the primary device used for 2FA:**

i. If you have multiple Duo authentication devices, you can choose which one is the primary device to be used by 2FA.
Figure 7: If you have multiple mobile devices enrolled in Duo, you can choose a primary device for Duo to use for 2FA. Simply click the pull-down menu next to "Default Device," select your primary device, and then click the green "Save" button.

ii. On the “My Settings & Devices” page, locate the “Default Device” pull-down menu.

iii. By clicking on the pull-down menu, you can select your primary authentication device. A check mark is displayed next to the device that currently is being used as your primary authentication device.

iv. Select your primary device and click the green “Save” button at the bottom.

c. Select the method used for 2FA:

i. You can change the 2FA method used to login.

ii. On the “My Settings & Devices” page, locate the “When I log in” pull-down menu.

Figure 8: The “When I log in” pull-down menu allows users to specify the 2FA authentication method Duo will use.

iii. By clicking on the pull-down menu, you can select your 2FA notification method. A check mark is displayed next to the method that currently is being used for the 2FA process. **Note:** Choosing “Ask me to choose an authentication method”
allows the user to select either the Duo Push method or the “Enter a Passcode” option when authenticating with Duo. This is the recommended setting.

iv. Select your 2FA notification method and click the “Save” button.

d. Remove a device:

i. Important note: If you delete a device before adding a new device as a primary, you might be unable to complete the 2FA process and could be locked out of any applications or sites that use Duo Mobile 2FA. That would require contacting AskIT for assistance. Therefore, it is HIGHLY recommended that you **DO NOT DELETE** a device until you can enroll a second device for 2FA, elevate it to the primary device, and confirm that it works. Once you have confirmed that the new device works as your primary 2FA method, then remove the old device.

![My Settings & Devices](image)

ii. If you are adding a new authentication device and want to delete an old one, be sure to first add the new device and make it the primary 2FA device using the steps detailed above in this document.

iii. Once you have added a new device, made it the primary, and confirmed that you can use it for 2FA, locate the old device on the “My Settings & Devices” page and click the “Device Options” button next to it.

iv. A number of other buttons appear for the device that you selected, including a red trash can icon. Click the icon.
v. A final confirmation asking whether you want to remove the device will appear. Click the “Remove” button to complete the process, or “Cancel” if desired.

If you encounter any problems with the authentication process, please contact AskIT by calling 996-5555 or visiting uab.edu/techhelp.