DUO 2FA FAQ

Overview:

Brandeis continues to strengthen its IT environment through the use of two-factor authentication using Duo Security (Duo). As part of these efforts, Duo is being integrated into the Brandeis suite of applications.

By default, when you want to log into your Brandeis Account using a browser for the first time in a day, you will also be prompted via Duo to confirm the login. This is generally once per login. This default behavior is the most secure option available.

For users desiring greater convenience, the Duo login page has a “Remember this device for 30 days” checkbox. If this option is checked, the device and web browser (e.g. Chrome, Firefox, Safari) combination will be remembered. (Using another browser on the same device or using another device will prompt for 2FA).

Please note: you may not see the “Remember me for 30 days” checkbox until you’ve successfully enrolled and logged into Duo at least once. To enable this, deny the prompt from your second factor to log in, and the checkbox should be available shortly.

See your question right away? Click the link below to scroll to the answer!

What services require Duo for login?
Do I need a smartphone with a data plan?
How do I register a smartphone for Duo Two-Factor Authentication?
How do I get a hardware token?
What should I do if I forgot my smartphone or hardware token?
What should I do if I have a new cell phone or new phone number?
What do I do if my hardware token stops working?
What if I lose my hardware token?
I use another 2FA app like Google Authenticator, LastPass Authenticator, or Google 2-Step, how does this affect me?
What if I already use DUO for another employer?
What do I do if I'm traveling abroad with no cell phone service and my phone is my 2nd factor? How will I access my account?
My computer won’t let “Remember me for 30 days” - now what?

Related articles

What services require Duo for login?
Most Brandeis websites that require a login will eventually require DUO for login.
Some services that require DUO 2FA are listed on the main DUO - Two-Factor Authentication webpage.

Do I need a smartphone with a data plan?
It is not necessary to have a smartphone to use Duo. You can use a tablet, desk phone, or hardware token for your second factor instead. A data plan is not required for your device. If you have the Duo app on your phone, you can click the key icon next to your account to get a one-time passcode to log in, which doesn't require any data usage.

How do I register a smartphone for Duo Two-Factor Authentication?
Devices must be enrolled in Brandeis' portal for DUO device management.
See Enrollment Instructions on Duo's website for a detailed guide.
How do I get a hardware token?

They are available upon request at the Technology Help Desk. It will need to be activated by a Technology Help Desk staff member before leaving the Help Desk area.

What should I do if I forgot my smartphone or hardware token?

Contact the Technology Help Desk for a one-time use passcode. The Technology Help Desk will have to verify your identity.

What should I do if I have a new cell phone or new phone number?

If you have the same phone number, but a new phone, go to https://identity.brandeis.edu/identity-manage/duo_device and log in using a different 2nd factor. Once logged in, select the Device Options button next to the cell phone you wish to update and click “Reactivate Duo Mobile”. The webpage will have you scan a QR code again.

If you have the same phone, but a new number, go to https://identity.brandeis.edu/identity-manage/duo_device and log in using a different 2nd factor. Once logged in, select the Device Options button next to the cell phone you wish to update and click the trash button to delete it. Add and activate your cell phone as if it were a new device.

What do I do if my hardware token stops working?

Please call or come to the Technology Help Desk as the token will need to be reset by a staff member.

What if I lose my hardware token?

Contact the Technology Help Desk ASAP. We will replace it for you, and can assist with deactivating the lost one.

I use another 2FA app like Google Authenticator, LastPass Authenticator, or Google 2-Step, how does this affect me?

DUO is not currently compatible with Google Authenticator or LastPass Authenticator.

If you have Google 2-Step enabled on your Brandeis account, Duo is intended as a replacement. You may use both, both you will be prompted twice for a 2nd factor (by both Duo and Google).

What if I already use DUO for another employer?

If you use the DUO mobile app, you can still register your smartphone as your second factor. The mobile app will create a Brandeis profile alongside your existing profile. If you currently use a hardware token, you will need to obtain a second hardware token from the Technology Help Desk.

What do I do if I'm traveling abroad with no cell phone service and my phone is my 2nd factor? How will I access my account?

If you're traveling without cell service and your cell phone is your usual second factor. You have two options:

1. Have DUO send a list of 10 passcodes to your phone before you leave. You'd select “text me new codes” in the screenshot below.
   a. You arrive at this screen by clicking the ‘Enter a Passcode’ button.
Get a hardware token from the Help Desk.

My computer won't let "Remember me for 30 days" - now what?

If the 'Remember me' tool is greyed out and "You need to enable cookies in order to remember this device." has appeared in the blue message bar, you likely have the cookie settings pictured below.

To resolve the issue, change 'From visited' to 'Always' in the field next to 'Accept third-party cookies and site data' and save your changes however the browser updates (clicking 'OK', 'Save', etc.)

*image is from the web browser Firefox. Other browsers, such as Chrome and Safari will have their settings displayed differently.

Or, if you want to keep third-party cookies blocked, enable an exception for the Duo cookies via this Duo FAQ "Can Duo's Remembered Devices feature work if third-party cookies are blocked?"

Get Help:

For additional assistance with Duo, troubleshooting, lost/stolen devices, or any other Duo issues, please Contact the Technology Help Desk

Additional documentation:

Can be found on DUO Security's website

Related articles

- Setting up DUO
- DUO - Two-Factor Authentication
• DUO 2FA FAQ