Logging In with 2FA

Faculty, staff, and student employees who have enrolled in the two-factor authentication (2FA) service will be prompted to verify their identity a second time on 2FA protected services. Below is a description of the process.

1. Enter your NetID and Password in the login window.
2. Click Login.
3. You will receive a prompt for two-factor authentication.
   a. If your account has been set up to automatically send you a Push/Text/Call, you will receive a notification.
   b. Otherwise, manually select how you would like to verify your login.
4. Complete 2FA using your selected method.
5. Continue on to your service.

Remember my Device

Most people only have one or two devices that they use every day. 2FA at UConn allows users to remember their device(s) for 30 day intervals, which decreases the number of times you must use your second factor to log in. Once you enable this feature, you will not receive 2FA prompts for 30 days as long as you are using the same web browser on the same device. This improves end user convenience while still providing the security benefits of 2FA. To turn on this feature:

1. Navigate to any site that requires 2FA.
2. Login to the Single Sign On page with your NetID and NetID password.
3. Once you see the 2FA prompt, check: Remember me for 30 days. If your 2FA settings are configured to Automatically Send a Push, you must hit the blue Cancel button on the bottom of the 2FA box.
4. Complete 2FA login.

If you want the protection of 2FA but not the constant prompts to authenticate on your second factor, you can check a box on the Duo screen to Remember me for 30 days. As long as you are using the same browser and the same device, you will only receive one prompt every 30 days.

Related Articles

- Purchasing and Registering a Hardware Token for the 2FA Service
- Authenticating Using a Passcode
- Authenticating via Push Notification (Duo Mobile App)
- Setting Up a Backup Device for 2FA
- Setting Up a Tablet for 2FA