Duo Universal Prompt

Universal Prompt will provide a simplified Duo 2-factor authentication experience helping you log in to your applications faster than before. The Duo login options will look different but will still support a wide range of login options.

Logging in with Verified Duo Push in the universal prompt.

New Universal Prompt

Enter Code on Your Device to Verify

More About Duo Universal Prompt Login Options

*Duo authentication methods listed from most to least secure*

Use the drop down items below to learn more

**Fingerprint Sensor**

Fingerprint authentication lets you use your device's fingerprint sensor for Duo login verification. Duo supports fingerprint verification with Touch ID on Apple MacBooks and Mac Magic Keyboards.

**Touch ID**

In order to use Touch ID with Duo, make sure you have the following:

- A MacBook Pro, MacBook Air or Magic Keyboard with a Touch ID button.
- A fingerprint enrolled in Touch ID (see how to do this at the Apple Support site).
- Chrome 70 or later. While Duo passwordless supports Touch ID in Safari, use of Touch ID for two-factor authentication in Safari and additional browsers on macOS is not available at this time.

Touch your Mac’s Touch ID sensor when prompted to log in to the application. If you aren’t able to access the Touch ID sensor (such as when you close and dock your laptop), then you can choose to type in your Mac login password instead to verify.
If you need to cancel a Touch ID authentication in progress, click or tap the cancel option shown by your browser, outside of the Duo Universal Prompt.

**Verified Duo Push**

Pushes a login request to your [iOS](https://www.apple.com) or [Android](https://play.google.com) phone or tablet if you have Duo Mobile installed and activated. Review the request on your phone or tablet, where you will receive a verification code. **Enter the code and tap Verify** to log in to the application from your mobile device. This is one of the easiest, fastest and most secure ways to verify Duo.
Note: If you did not prompt for a Duo push, click “I'm not logging in” to report this attempt to our Office of Information Security.
Log in using a passcode generated by a hardware token provided to you by your organization. Enter that passcode into the space provided and click or tap Verify to log in to the application.

Enter your passcode
Verify it's you by entering a passcode from your hardware token.

Passcode

Verify

Other options

Need help?
Secured by Duo

SMS or Text message passcodes
Log in using a passcode received from Duo in a text message. When you land on the text message page, it will show that a text message was just sent to you with a passcode. When you receive the message, enter that passcode into the space provided and click or tap Verify to log in to the application.

If you did not receive the text message from Duo, use the Send a new passcode link to try sending it again.

Passcodes received in a text message expire when used.
Enter your passcode
Verify it's you by entering a passcode from your hardware token.

Passcode

Verify

Other options

Need help?

Secured by Duo

Phone Call
Authenticate via phone callback. Answer the phone call from Duo and follow the voice instructions to log in to the application.

Answer the phone call
Verify it's you by pressing any key on your phone...

Calling "Office phone" (::::::-6297)

Other options

Need help?

Secured by Duo

Log In With the Duo Universal Prompt
After completing Duo enrollment, you'll see the Duo prompt the next time you perform a browser-based login to a web service or a campus application protected with Duo.
The first time you log in to an application with Duo using the Universal Prompt, Duo chooses one of your configured login options automatically, selecting the most-secure method from the ones you have available.

**What the options menu looks like:**

![Options Menu Image]

If you don’t want to use the method Duo automatically suggests for that application, cancel the Duo authentication in progress and click or tap *Other options*. Then, select the method you want from the list.

Future Universal Prompt logins to that application from the same device and browser will automatically use that same method. If you cancel the authentication in process and choose a different device, then the device you use becomes the first choice for that application.

Since Duo remembers the last-used authentication device for each application you access, the Universal Prompt should always display the previously used option for that application as the default.
Enter code in Duo Mobile

Verify it’s you by entering this verification code in the Duo Mobile app...

065

Sent to "iOS" (-------2613)

Other options

Need help? Secured by Duo

Remember my device

If you are logging into your device, you can click the option Yes, this is my device, to reduce number of time you must authenticate on your device. If you are using a public device or at device that is not yours, click No, other people use this device.
Successful login to your browser!

Success!
Logging you in...

Related Articles
- Duo - 2 Factor Authentication
- DUO 2-Factor Authentication
- Duo Enrollment
- Duo Prompt display issue on an iPhone or iPad
- Duo Two-Factor Authentication Enrollment for Faculty & Staff
• Duo Two-Factor Authentication for Incoming Students
• Duo: Manage Devices After Enrollment
• How to Activate Duo Push Notifications to your Smartphone
• Logging into AnyConnect VPN with a Duo Token
• New Phone-How to Reactivate Duo Mobile
• What is Duo 2-Factor Authentication (2FA)

Search Knowledge Base
Submit a Service Request