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.

A Visual User Change

Here's a visual comparison of logging in with Duo Push in the new universal prompt vs. the previously traditional prompt:

![New Universal Prompt](image1)
![Previous Traditional Prompt](image2)

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 78 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.

**Duo Push**

Pushes a login request to your **iOS** or **Android** phone or tablet if you have Duo Mobile installed and activated. Review the request on your phone or tablet and tap **Approve** to log in to the application. This is one of the easiest ways to verify Duo.
Log in using a passcode generated by the Duo Mobile app installed and activated on your Android or iOS device. Open Duo Mobile and locate your organization's account in the accounts list, and tap **Show** to generate a six-digit passcode. 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**

**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

[masked 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.
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:
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 right default option for that application.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duo Push</td>
<td>Send to iPad (iOS)</td>
</tr>
<tr>
<td>Duo Mobile passcode</td>
<td>Enter a code from the Duo Mobile app</td>
</tr>
<tr>
<td>Hardware token</td>
<td>Enter a code from your hardware token</td>
</tr>
<tr>
<td>Text message passcode</td>
<td>Send to “iPhone” (-2548)</td>
</tr>
<tr>
<td>Phone call</td>
<td>Call “iPhone” (-2548)</td>
</tr>
<tr>
<td>Bypass code</td>
<td>Enter a code from your IT help desk</td>
</tr>
<tr>
<td>Manage devices</td>
<td>Add a phone, Touch ID, and more.</td>
</tr>
<tr>
<td></td>
<td>⚠ First you’ll verify your identity.</td>
</tr>
</tbody>
</table>

**Need help?**

Secured by Duo
Remember me for 14 days

This will look different, but will still be an option for each browser you have logged into. When asked to trust this browser, select "Yes, trust this browser" to remember you for 14 days.

Trust this browser?

You won't need to log in as often from this browser.

Yes, trust browser

No, do not trust browser

Successful login to your browser!
Success!

Logging you in...

Related Articles

- 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 Ivanti with Duo Token
- New Phone-How to Reactivate Duo Mobile
- What is Duo 2-Factor Authentication (2FA)

We value your feedback! Click HERE to suggest updates to an existing article, request a new article, or submit an idea.

Search Knowledge Base

Submit a Service Request