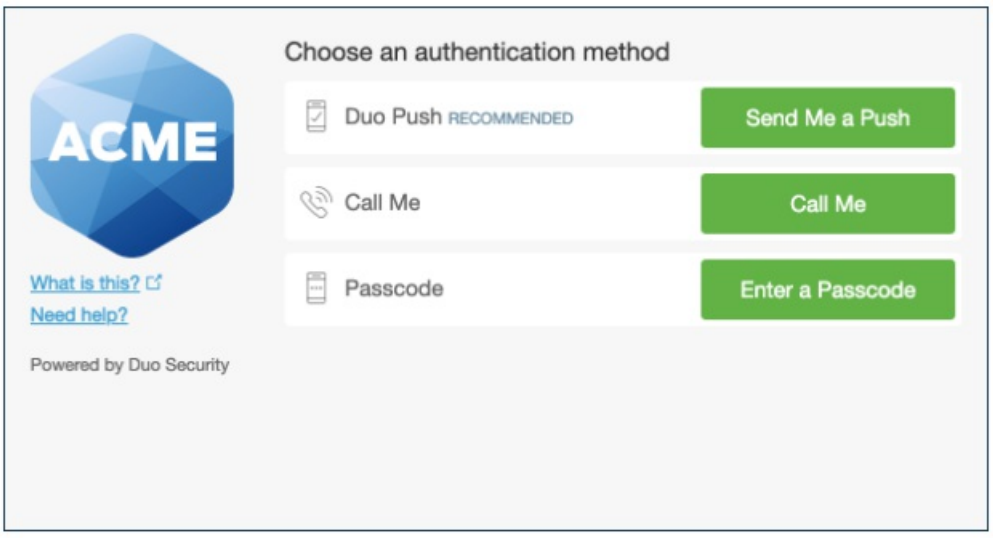
Using the Duo Prompt

Introduction

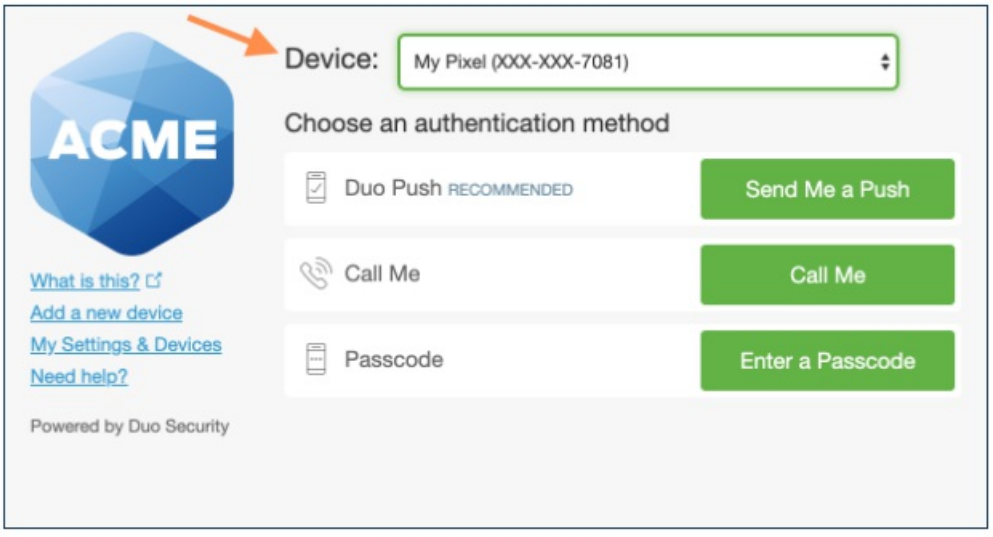
Page explains how to use the Duo prompt to authenticate to any Office 365 tools accessed outside of the Qualfon network.

Details

1. After completing Duo enrollment (or if your Duo administrator set you up to use Duo), you'll see the Duo Prompt the next time you perform a browser-based login to a web service or application protected with Duo.



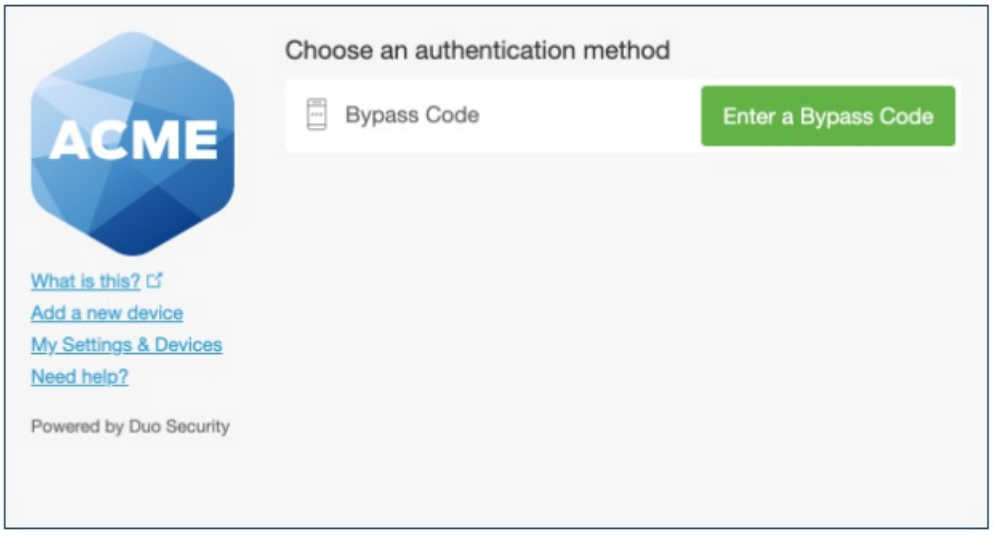
2. If you have more than one device enrolled, like a mobile phone and a hardware token, you'll see a device selector.



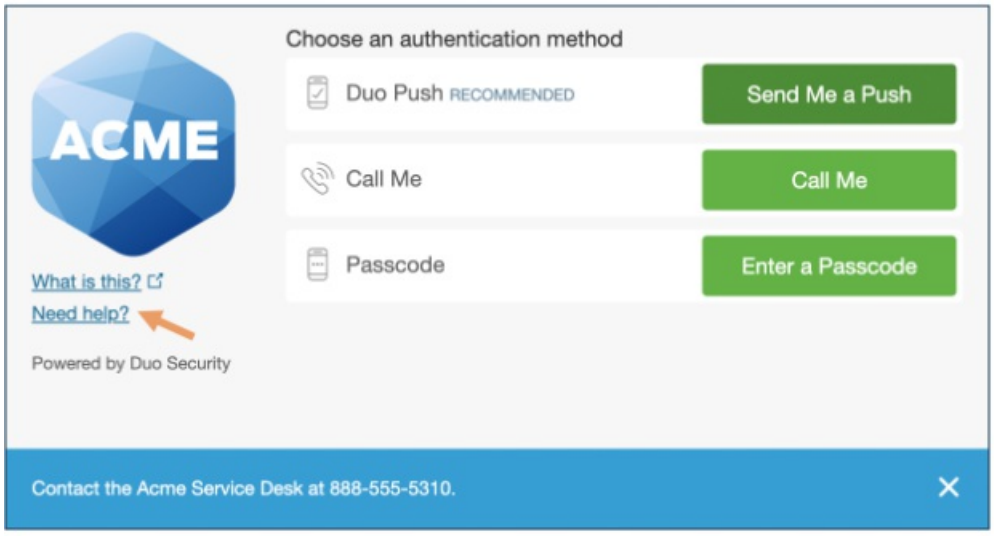
3. Select the device you want to use and then choose your authentication method.

- **Duo Push:** Pushes a login request to your phone or tablet (if you have Duo Mobile installed and activated on your iOS, Android, or Windows Phone device). Just review the request and tap Approve to log in.
- **Call Me**: Authenticate via phone callback.
- **Enter a Passcode**: Log in using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator. Click Send codes to get a new batch of passcodes texted to your phone.

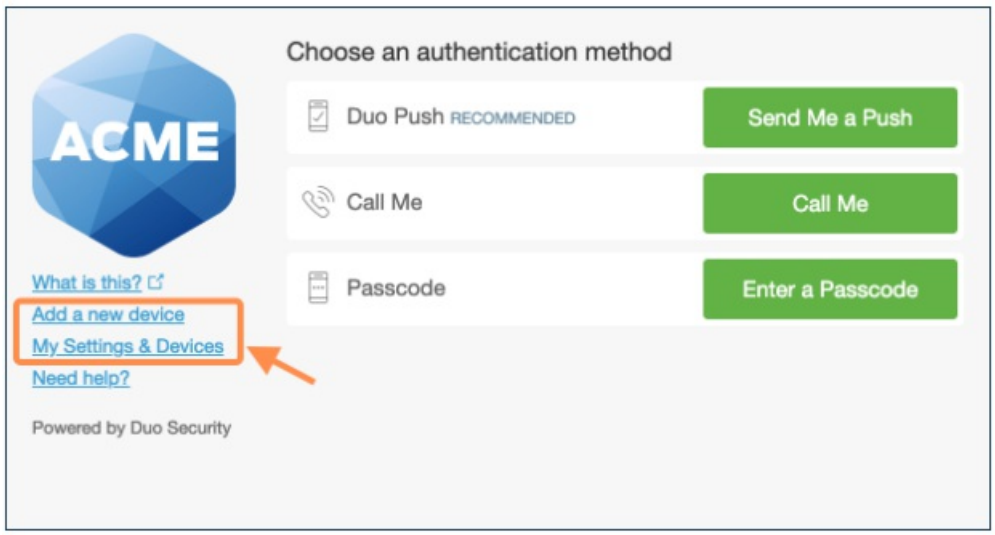
4. Your Duo administrator may have limited which authentication methods you can use to log in. If this is the case, then the Duo prompt shows only the allowed methods. So, if your organization disallows phone call for Duo logins, the prompt may only show the "Send Me a Push" and "Enter a Passcode" options.
5. In the event that your organization restricts use of the authentication methods attached to your account, you'll see a message indicating this, with the option to enter a Duo bypass code.



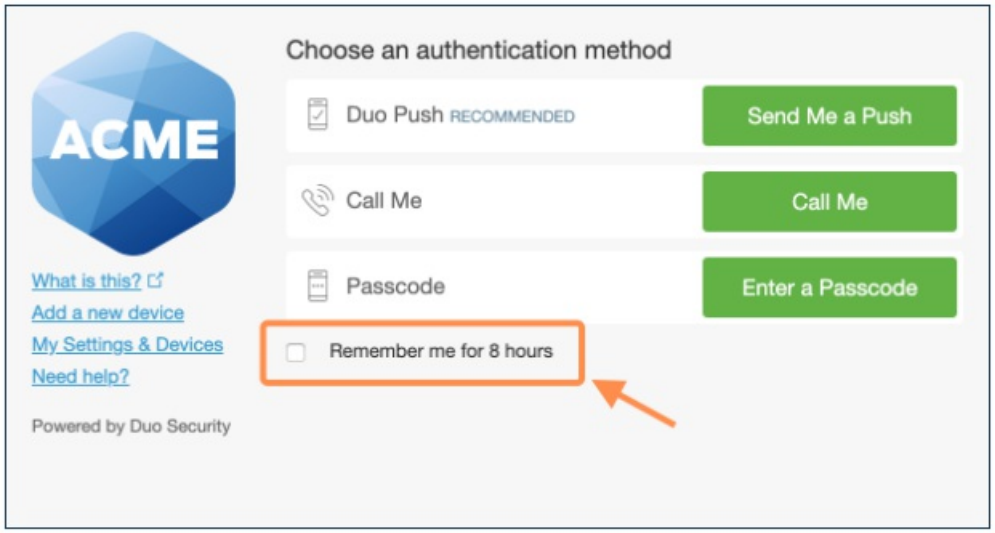
6. If you can't authenticate or aren't sure what to do, click Need help? on the left side of the Duo prompt. Your administrator may have customized the help text with additional instructions or contact information.



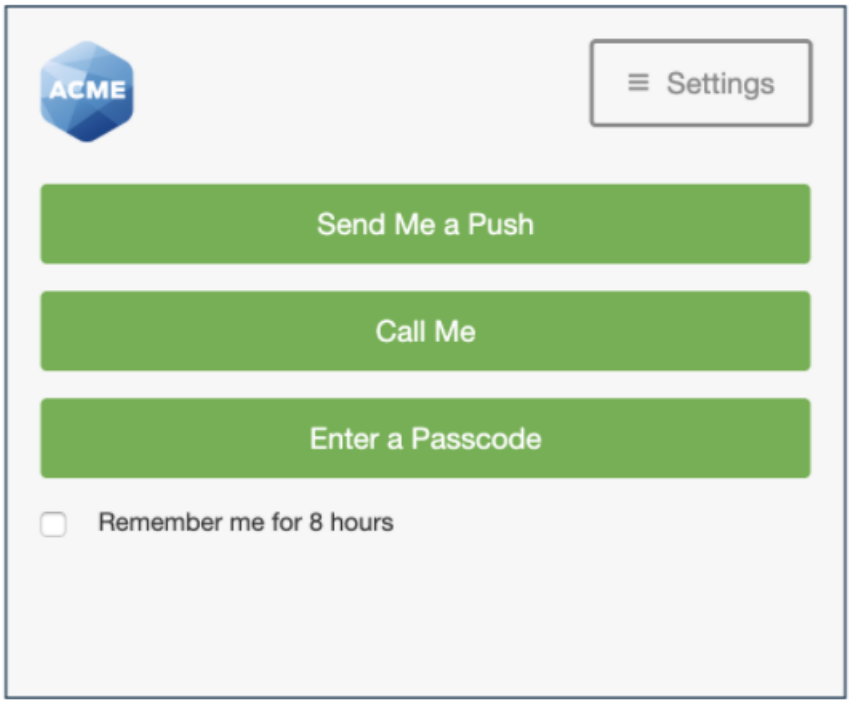
7. Additional Information:
    - **Self-Service Options**
        1. If your organization has enabled self-service you can add an additional authentication device by clicking the Add a new device link, or update your setting and remove authentication methods by clicking My Settings & Devices.



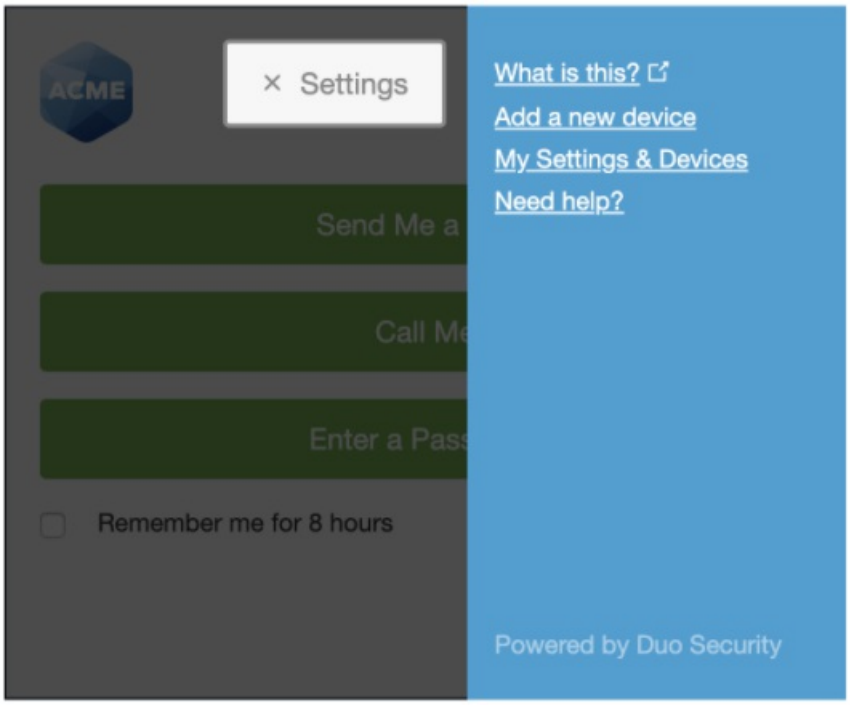
    - **Trusted Devices**
        1. You'll also see a Remember me for... option if your administrator enabled Duo's trusted devices feature. If you check this box when authenticating you won't need to perform Duo second-factor authentication again for the duration specified on the prompt.



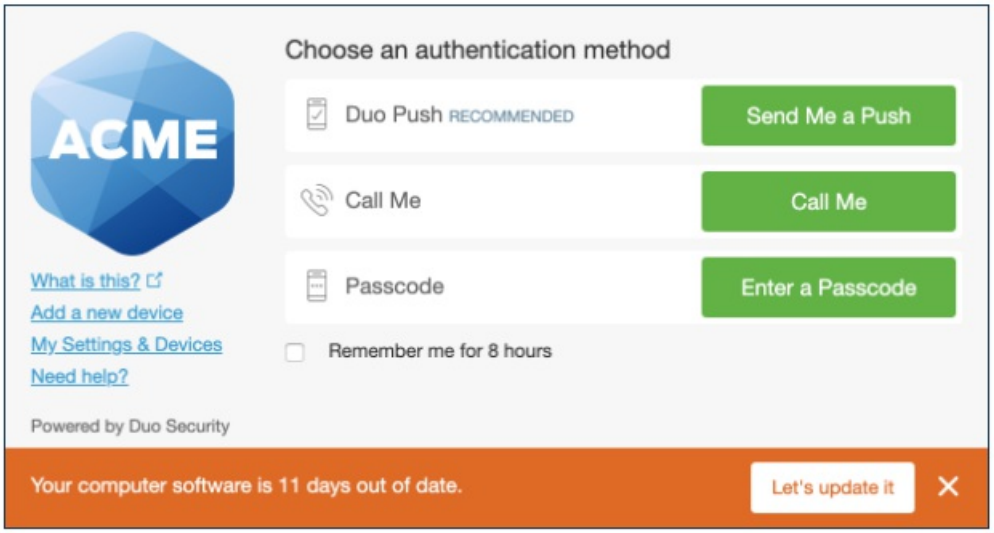
- **Authenticating from Smaller Screens**
  1. If you're logging in with Duo from a device with a smaller screen (like a tablet) or small browser window then your Duo Prompt may look slightly different. Don't worry! All the devices and options shown in the full-size prompt are available for use, and you can enroll and manage devices by following the same steps.



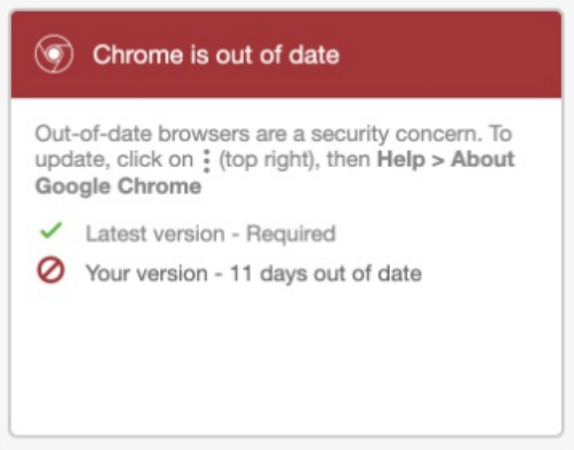
  2. Access Add a New Device or My Settings & Devices by clicking the Settings button at the top. Click the X on the Settings button to return to the Duo Prompt.



- **Software Updates**
  1. You may be prompted to update outdated browser or plugin software when authenticating if your organization enabled this feature. You can take a few minutes to update your web browser, Flash, or Java version to the most recent before authenticating, or choose to update later and continue on to the protected resource.

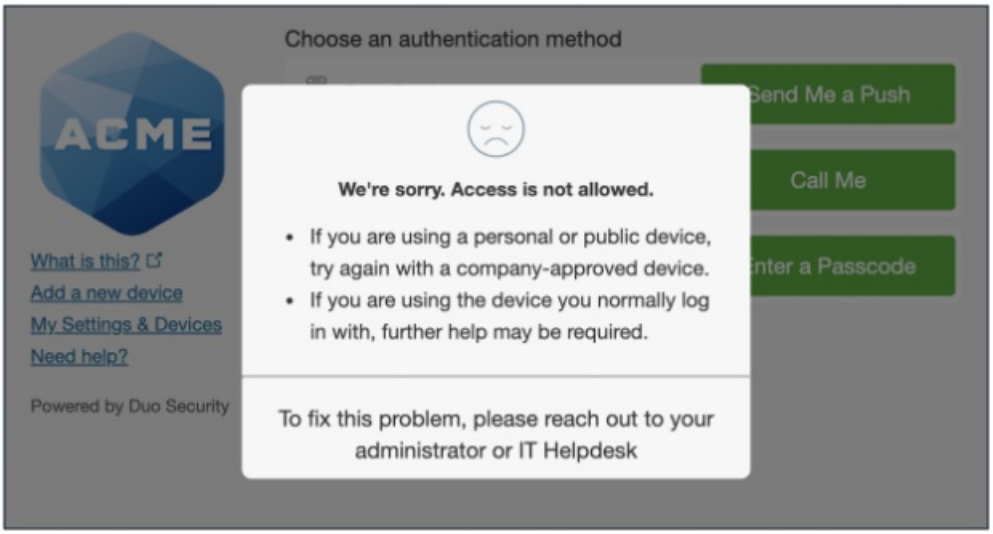


  2. If your organization blocks access to Duo-protected resources from devices with outdated browsers or plugins, then you may not complete two-factor authentication until you update your software.



3. Your administrator may also choose to block access from certain computer and mobile operating systems. In this case, you must upgrade your OS to an allowed version or switch to a different device.

- **Personal Devices**
  1. Your organization may choose to block access to applications from devices not managed by the organization. If this policy is enforced then you won't be able to complete Duo authentication from your personal device.



Related Articles

Revision History

Date Created: 12/09/2020 10:29 am EST
Last Modified: 12/09/2020 10:29 am EST