

Duo Mobile - Authentication Methods

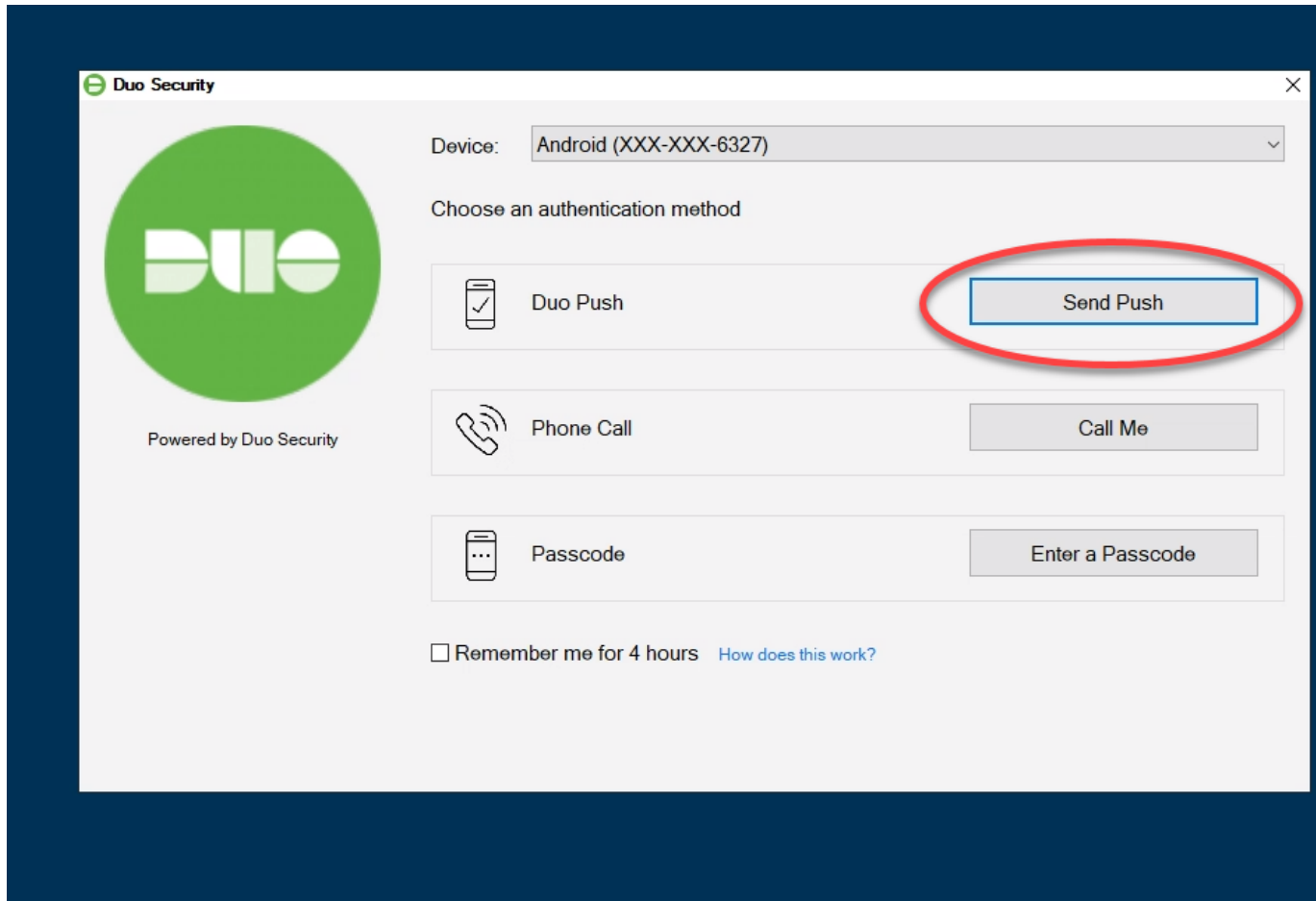
When accessing GCSC workstations or services such as myGCSC, Duo MFA provides users with various authentication options. The recommended and simplest method is **Duo Push**, where the Duo Mobile app sends a notification to the user's mobile device or watch*, allowing them to easily approve or deny the login with a single tap. Alternatively, users can choose to enter a passcode, also known as OTP (*One-Time Passcode*), which functions similarly to a traditional text message but is conveniently available within the Duo Mobile app, eliminating the need to wait for a text message. Although text and phone call authentication methods are also currently available, they are considered outdated and will eventually be phased out.

Below outlines an overview of each authentication method and how they work

DUO PUSH

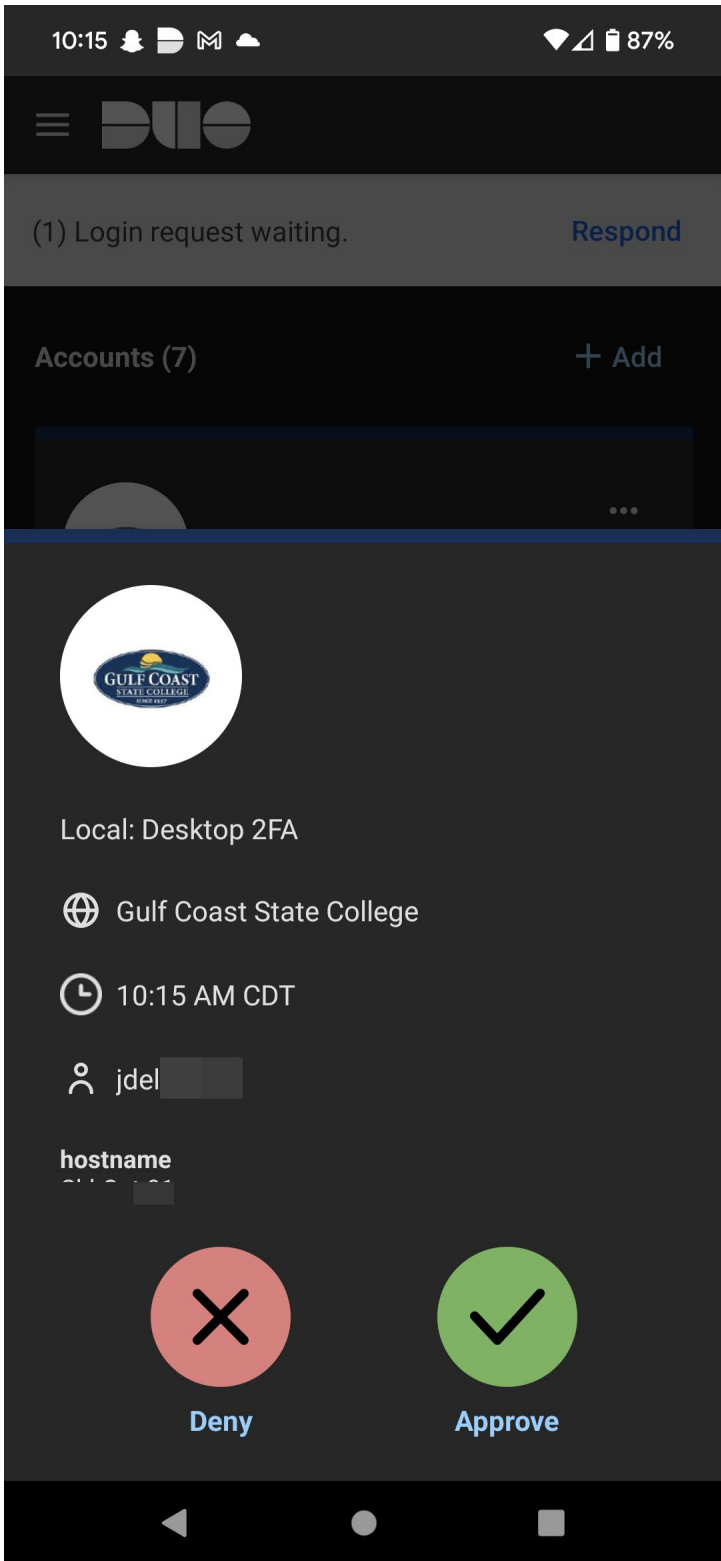
Duo Push based MFA will prompt the users to accept or deny login with a push notification to their device. The login flow would generally look like this,

1. User logs into a GCSC desktop with their GCSC ID and password
2. User selects **Send Push** for the authentication method



3. User receives a notification on their phone requesting to approve the login.

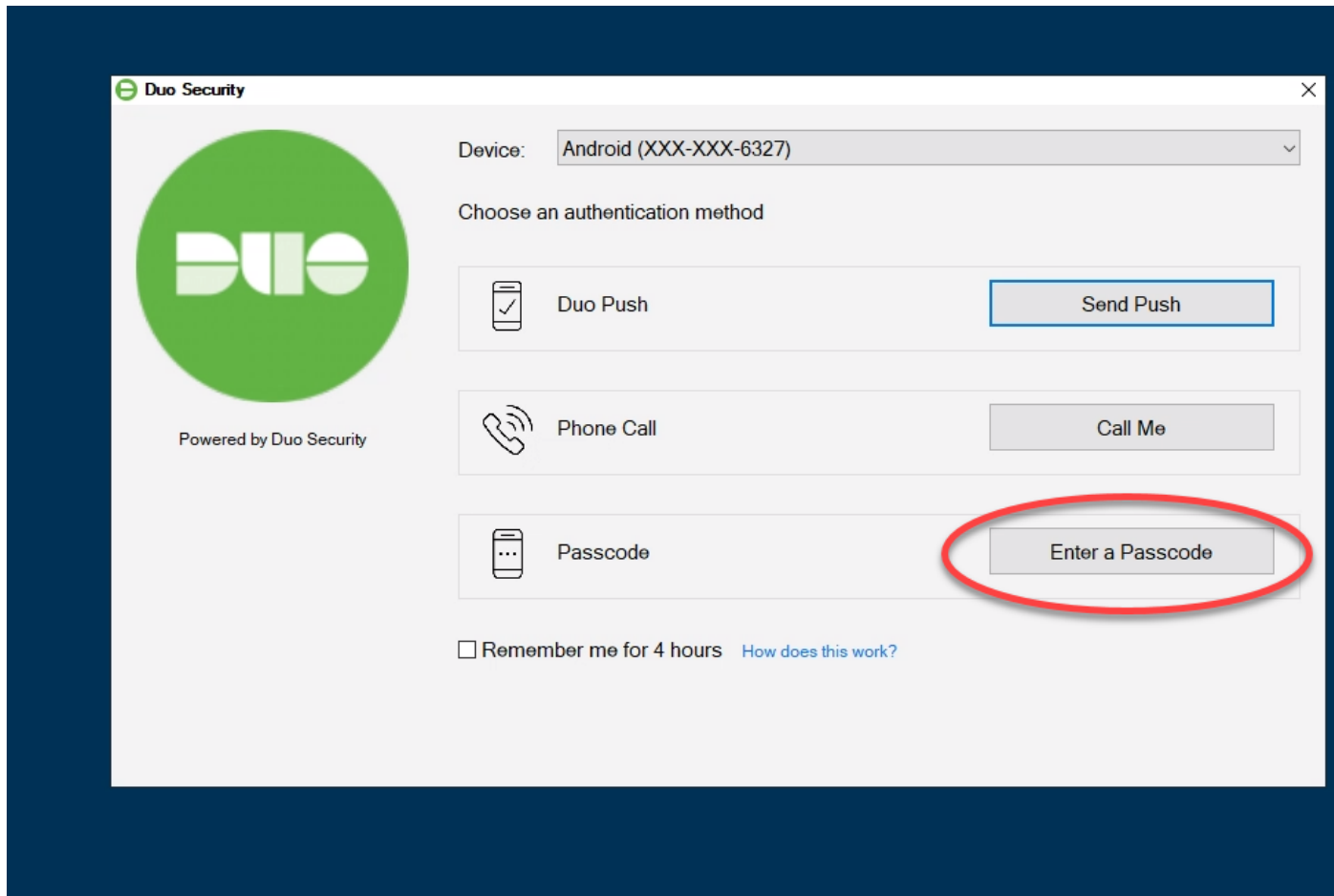
**If the user has a supported watch with the Duo Mobile app installed, this same tap approval can be done via their watch instead.*



DUO PASSCODE

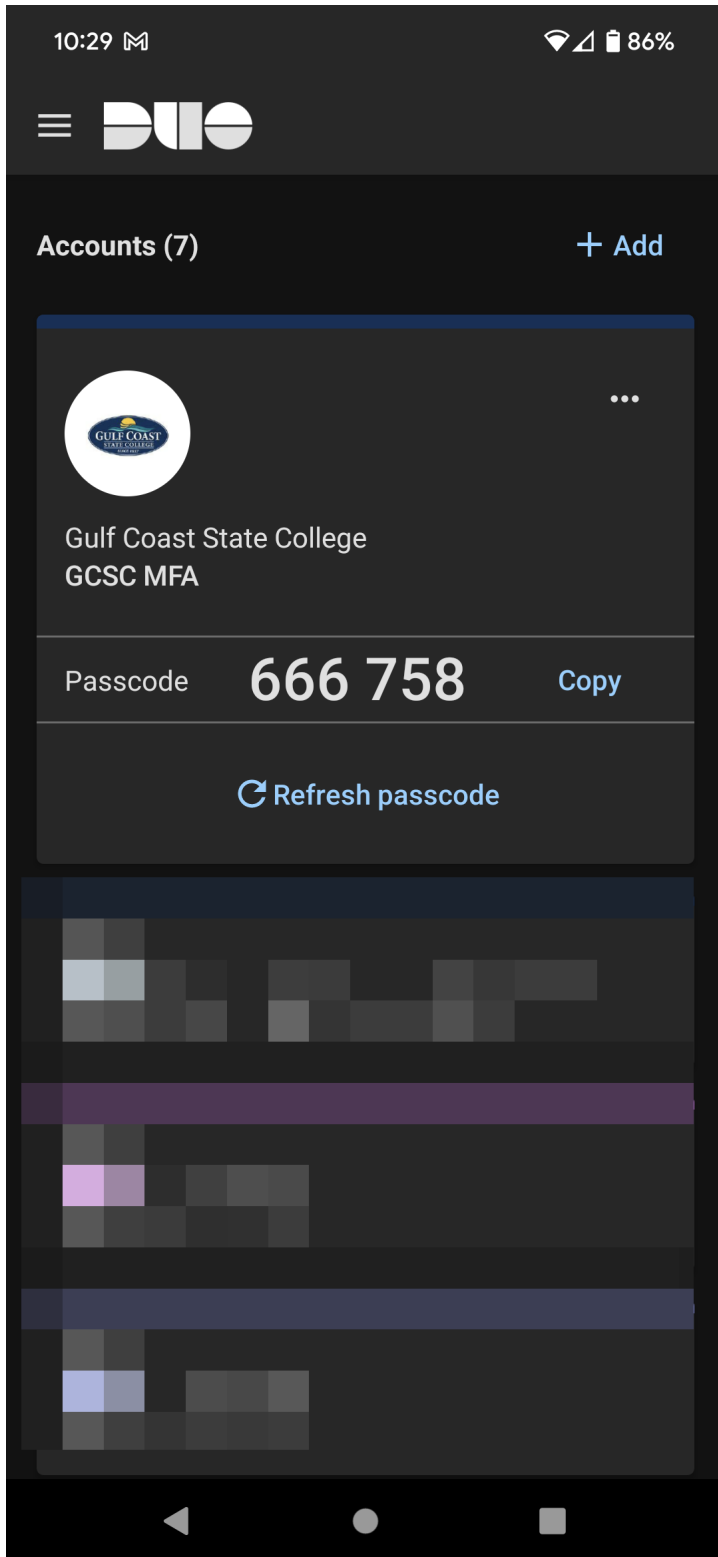
Duo Passcode based MFA will accept the 6-digit passcode from within the app. The login flow would generally look like this,

1. User logs into a GCSC desktop with their GCSC ID and password
2. User selects **Enter a Passcode** for the authentication method



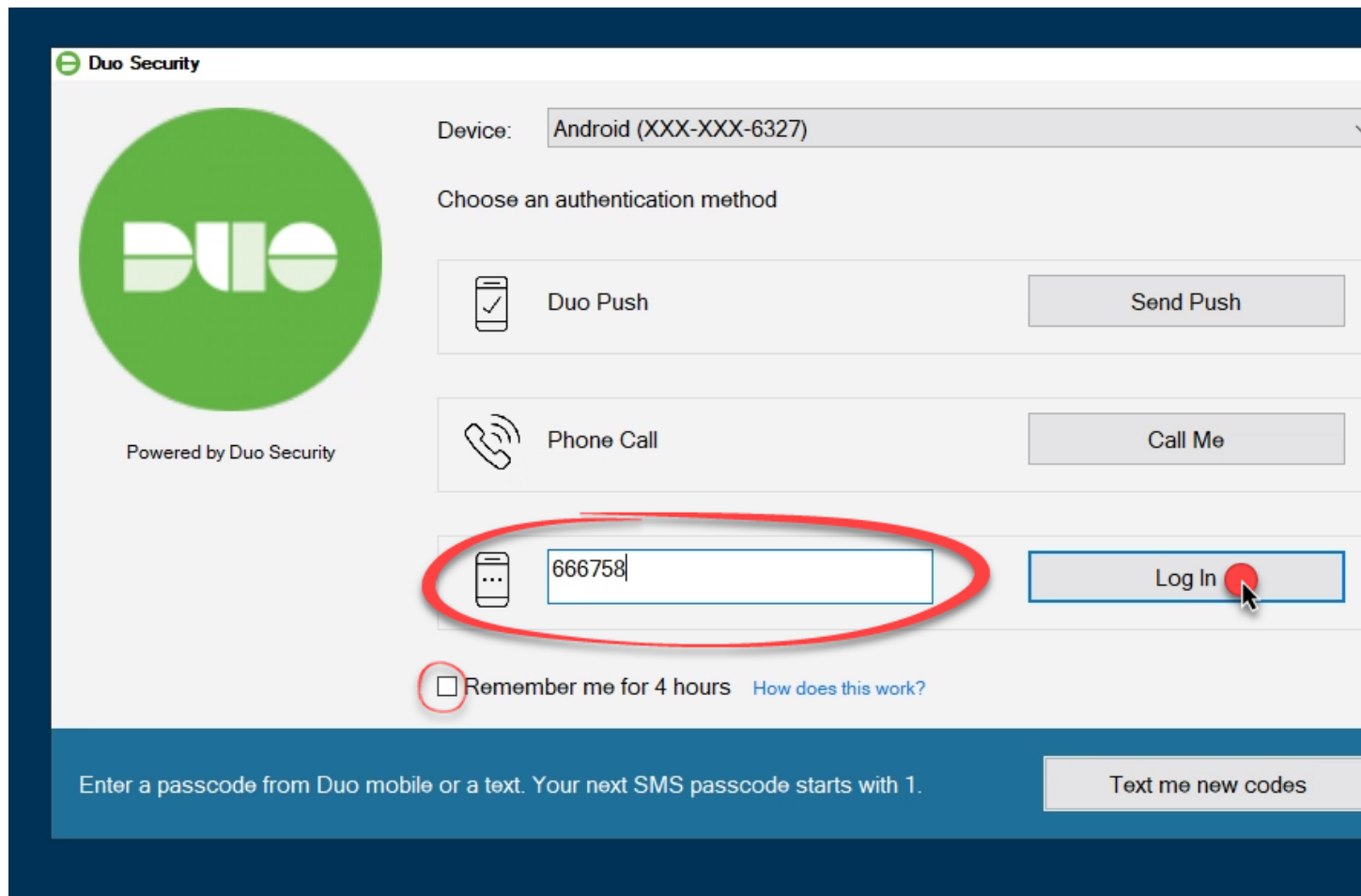
3. User opens the Duo Mobile app on their mobile device, taps the 'Gulf Coast State College' entry which exposes the passcode

** It is advised to tap on the "Refresh passcode" option each time you utilize this method in order to ensure the use of a valid code and prevent any potential issues.*



4. User inputs the passcode into the passcode field on the computer and clicks **Log In**

** If you wish to be remembered on the computer to reduce MFA requests, be sure to check the box to 'Remember me for 4 hours'*



Duo Security

Device: Android (XXX-XXX-6327)

Choose an authentication method

Duo Push Send Push

Phone Call Call Me

Log In

Remember me for 4 hours [How does this work?](#)

Enter a passcode from Duo mobile or a text. Your next SMS passcode starts with 1. Text me new codes

TEXT MSG

- Optionally, clicking the 'Text me new codes' will send the user a text message to their mobile device to input into the passcode field

PHONE CALL

Duo Phone Call based MFA will call the registered phone number. The login flow would generally look like this,

1. User logs into a GCSC desktop with their GCSC ID and password

2. User selects **Call Me** for the authentication method

3. User receives a voice phone call from a undetermined number, an automated voice announces itself as Duo and requests the user to '**Press any key to login**'

Why will text and phone calls be eventually phased out?

While a phone call or text message for second factor authentication provides an additional layer of security, it is important to note that these methods have certain vulnerabilities. They lack encryption, which means that the information transmitted during the authentication process is not protected against potential interception. Additionally, these methods are considered outdated and attackers have become adept at exploiting their weaknesses. The rapid progress of technology has made it increasingly easier for attackers to intercept, manipulate, spoof, and impersonate text messages and phone calls. This makes them less secure and more susceptible to malicious activity. As a result, these vulnerabilities will eventually render these methods obsolete, prompting the need for more secure alternatives.