Enabling Google 2-Step Verification

Brad Christ - 2025-04-01 - Comments (0) - Multi-factor Authentication

In addition to enabling Okta multi-factor authentication, you may also enable Google 2-Step Verification for additional account security. Some Google apps and services, such as Drive/Drive File Stream and Chrome, bypass the normal SOU login page. To protect those apps, you must also enable Google 2-Step Verification. To learn more about Google 2-Step, visit their guide.

Set up 2-Step Verification

1. Go to the Google 2-Step Enrollment page. You might have to sign in to your SOU Google Account again.
2. Select "**Get started"**.
3. Follow the step-by-step setup process.
4. Once you're finished, you'll be taken to the 2-Step Verification settings page. Review your settings and add multiple verification methods. The next time you login, you'll prompted to use a second factor.

Google supports the following authentication methods:

- Phone Call: Receive a code via a phone call to your landline or mobile phone.
- Text Message: Receive a code via text message on your mobile device.
- Google Prompt: Enroll in Prompt to allow push notifications to your device. Just one tap allows you to approve authentication requests. Note: users of iOS devices will need to download the "Google Search" app to enable Prompt. All users: Prompt and tokens cannot be enabled simultaneously.
- Authenticator Apps: Authenticator apps give you the ability to generate a code, even without data service or Wi-Fi.
    - Google Authenticator: Available for iOS or Android devices.
    - Duo Authenticator: Available for iOS and Android devices. Can generate codes for both Duo and Google!
- Token: You can purchase and register a USB token. For more information about tokens, see this knowledgebase article.
- Backup Codes: Print a paper copy of the single-use backup codes. If your mobile device isn't available, you can use one of those codes.

Add and Manage your Devices

Go to the Google 2-Step Settings page. You might have to sign in to your SOU Google Account again.

Scroll down to “Set up alternative second step.” You can also access this page by visiting “My Account” when logged into SOU email account.

Some devices require an app password to connect (or stay connected) to your Google account:

- Devices running Android 2.3.x or older
- Mail app on Apple devices not running iOS 8.3 or greater on your iPhone or OSX 10.10.3 on your Mac
- Email clients (e.g., Thunderbird, Outlook, Mac Mail)
- Instant messengers (e.g., Pidgin, Adium)

Troubleshooting

If you are encountering issues with Google 2-Step verification, review Google's documentation or contract your IT Computing Coordinator or the Help Desk for assistance.