Using HyperFIDO™ with a GitHub Account or GitHub Enterprise Account

11/13/2018

HSTE-NB0033.2-RV 1.1

HYPERSECU INFORMATION SYSTEMS INC

#200-6191 Westminster Hwy, Richmond, BC V7C 4V4 Canada
1 (604) 279-2000| hypersecu.com

Table of Contents

What is HyperFIDO™?

The HyperFIDO™ U2F security key is designed to quickly and easily secure online accounts with any service compatible with FIDO, including GitHub, Facebook, Google Account services such as Gmail, and more.
FIDO promotes convenience while increasing protection by reducing reliance on vulnerable static passwords, meaning you are no longer required to create long complicated passwords. HyperFIDO does all the work for you with a single press of a button.

This document will demonstrate how to register and use your HyperFIDO U2F security key with a GitHub Account or GitHub Enterprise Account.

NOTE: This document is up to date with GitHub account procedures on the date of publication. However, GitHub reserves the right to make changes to their procedures and services at any time.

Requirements

Before you register your HyperFIDO security key, you will need:

- The latest version of any web browser compatible with FIDO U2F:
    - Google Chrome (recommended)
    - Opera
    - Mozilla Firefox Quantum (60.0 or above) with FIDO U2F enabled. See *Setting Up FIDO U2F with Firefox* on page 4.
- A valid account with GitHub
- HyperFIDO™ U2F security key

Getting Started

If you are using a Mac or Windows operating system with Google Chrome browser, no additional setup or configuration is required before you can begin registering and using your HyperFIDO security key.

If you are using Mozilla Firefox and/or a Linux operating system, some additional setup may be required.

- For Firefox, see *Setting Up FIDO U2F with Firefox* on page 4.
- For Linux operating systems, see *Setting Up FIDO U2F with Linux* on page 5.

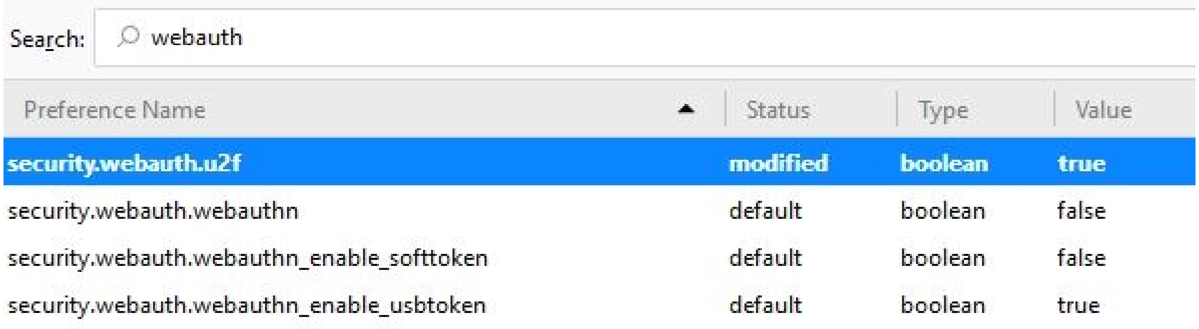
Once your browser and/or operating system is configured for FIDO U2F, you can begin by enabling two-factor authentication on your account.

Setting Up FIDO U2F with Firefox

To use HyperFIDO with Mozilla Firefox, you will need to enable `security.webauth.u2f` in the browser's configuration settings.

NOTE: You must be using Firefox Quantum (60.0) or higher. Enabling this feature requires accessing the configuration settings in the browser. Make sure you are familiar with this process before attempting to do so.

1. Open Firefox and type `about:config` into the browser's address bar.
2. In the search bar, search for *webauth* and locate **security.webauth.u2f** under Preference Name.
3. Double click on **security.webauth.u2f** to change the value from *false* to *true* in order to enable the feature.



Search: webauth

Preference Name	Status	Type	Value
security.webauth.u2f	**modified**	**boolean**	**true**
security.webauth.webauthn	default	boolean	false
security.webauth.webauthn_enable_softtoken	default	boolean	false
security.webauth.webauthn_enable_usbtoken	default	boolean	true

IMPORTANT: Mozilla Firefox may not support all services and web applications that use FIDO U2F. It is recommended you use Google Chrome web browser in order to have the most complete support for FIDO U2F.

Setting Up FIDO U2F with Linux

Depending on your Linux operating system, you may be required to add a rules file in order to use your HyperFIDO security key. You can either automatically download and install the rules file or manually install it.

Automatically Download and Install the Rules File

1. From your terminal, execute:

```
$ sudo curl
https://hypersecu.com/downloads/files/configurations/70-u2f.rules
> /etc/udev/rules.d/70-u2f.rules
$ sh -c /etc/udev/rules.d/70-u2f.rules
```

2. Restart your computer.

Manually Download and Install the Rules File

If you are unable to execute the commands, you can manually download and install the rules file.

1. Download the rules file from hypersecu.com/downloads/70-u2f.rules
2. Copy the file to `/etc/udev/rules.d/`
3. Restart your computer.

NOTE: If you already have the rules file from another U2F vendor, add the following into the current rules file and restart your computer:

```
# HyperSecu HyperFIDO
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", ATTRS
{idVendor}=="096e|2ccf", ATTRS{idProduct}=="0880", TAG+="uaccess"
```

Enabling Two-Factor Authentication

Before you register your HyperFIDO™ U2F security key, you must have two-factor authentication enabled on your GitHub account.

In addition to enabling two-factor authentication for your personal account, organization owners can also require organization members and project collaborators to enable two-factor authentication for their accounts before they are able to access repositories.

- **To enable two-factor authentication for your personal account**, follow the procedures provided by GitHub at the following link: help.github.com/articles/configuring-two-factor-authentication-via-a-totp-mobile-app

- **To require organization members to have two-factor authentication enabled**, follow the procedures provided by GitHub at the following link: help.github.com/articles/requiring-two-factor-authentication-in-your-organization

If you already have two-factor authentication enabled, you're ready to register your HyperFIDO security key. See *Registering Your HyperFIDO™ Security Key* on page 7..

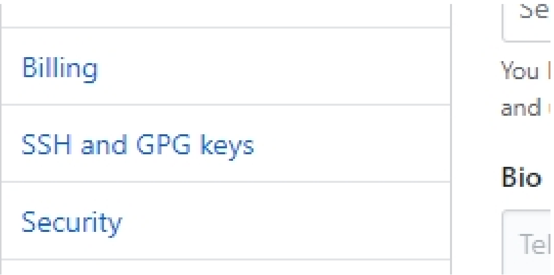
IMPORTANT: Store the recovery codes provided to you somewhere safe after enabling two-factor authentication. The recovery codes will allow you to get back into your account should you lose access.

Registering Your HyperFIDO™ Security Key

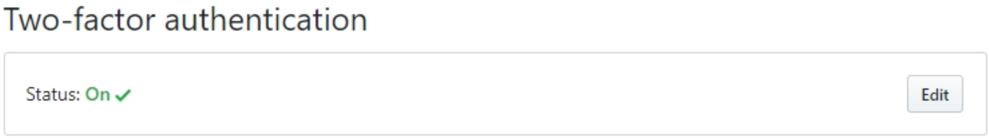
Before you register your HyperFIDO™ U2F security key, you must have two-factor authentication enabled on your GitHub account. If you do not have two-factor authentication enabled and are unsure of how to do so, see *Enabling Two-Factor Authentication* on page 5..

Once two-factor authentication is enabled, you're ready to register your HyperFIDO security key.

1. Sign in to your GitHub account.
2. Click your profile photo, then click **Settings**.
3. In the Personal settings sidebar, click **Security**.



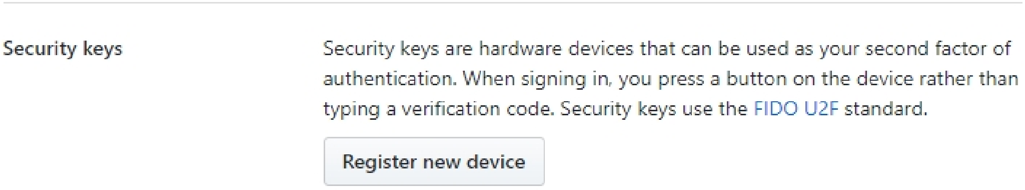
4. Under Two-factor authentication, click **Edit**.



Two-factor authentication

Status: On ✓

5. Scroll down to Security keys, then click **Register new device**.



Security keys

Security keys are hardware devices that can be used as your second factor of authentication. When signing in, you press a button on the device rather than typing a verification code. Security keys use the FIDO U2F standard.

6. Enter a name or description for the security key and click **Add**.

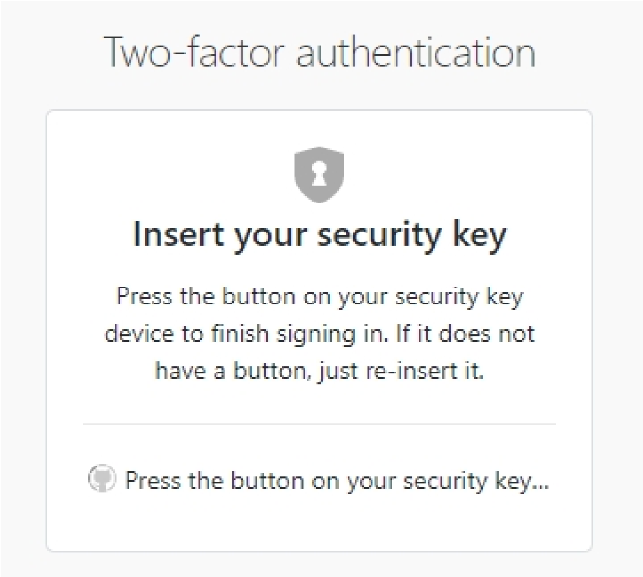
7. When prompted, press the button on your security key to register.

Using Your HyperFIDO™ Security Key

Once you've registered your HyperFIDO™ U2F security key, your GitHub account will no longer be accessible when signing in without first inserting your security key, keeping it secure from remote hackers and other malicious attacks.

Using your HyperFIDOsecurity key is simple. To use your key:

1. Sign in to your GitHub account with your regular username and password.
2. When prompted, insert your HyperFIDOsecurity key into a USB port.



Two-factor authentication

Insert your security key

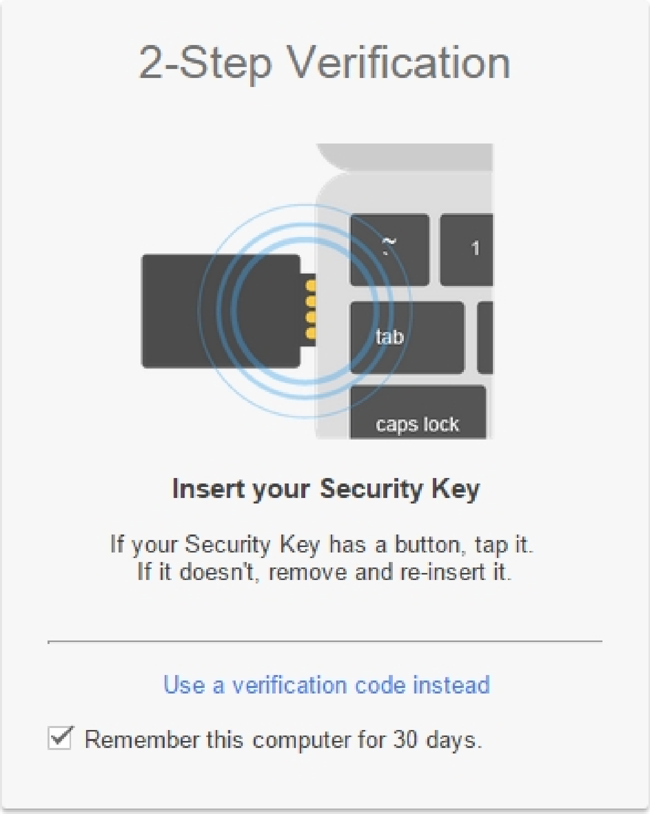
Press the button on your security key device to finish signing in. If it does not have a button, just re-insert it.

Press the button on your security key...

3. Press the button on your security key to finish signing in.

Using HyperFIDO on Desktop

1. Sign in to your GitHub account with your regular username and password.
2. When prompted, insert your HyperFIDOsecurity key into a USB port.



2-Step Verification

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

Use a verification code instead

☑ Remember this computer for 30 days.

3. Press the button on your security key to finish signing in.

Using HyperFIDO with Mobile Devices

If you are using a standard HyperFIDO security key without NFC capabilities, you will need to grant access using Google's App Passwords feature. To do so, follow the procedures described in *Accessing Your Account with Other Apps and Devices* on page 10.

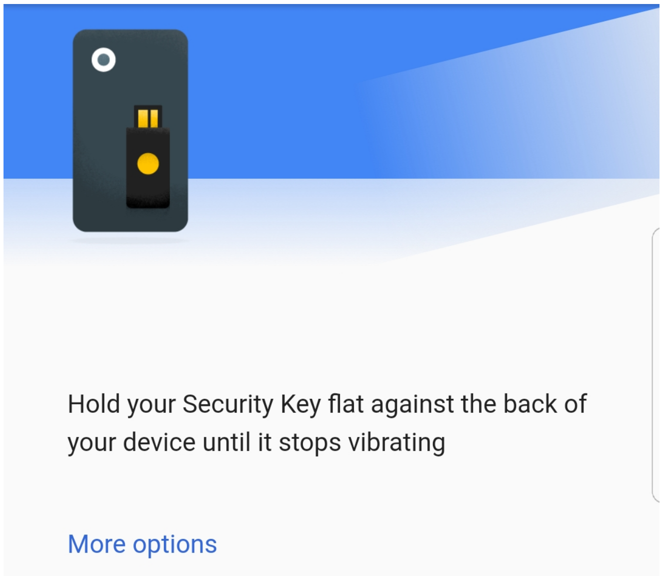
If you are using a HyperFIDO NFC device, you can authenticate your device directly using your security key.

IMPORTANT: HyperFIDO NFC is compatible only with Android devices.

1. Ensure that all Google Account-related applications are updated.

IMPORTANT: If you're using a third party application that **does not** use Google Identity Platform APIs, you must have the Google Authenticator application installed, as well.

2. Go to **Settings** on your device and add your Google Account.
3. Enter the name of the account you wish to add and the password.
4. When prompted, tap the security key to the NFC sensor on your mobile device to finish signing in.



Hold your Security Key flat against the back of your device until it stops vibrating

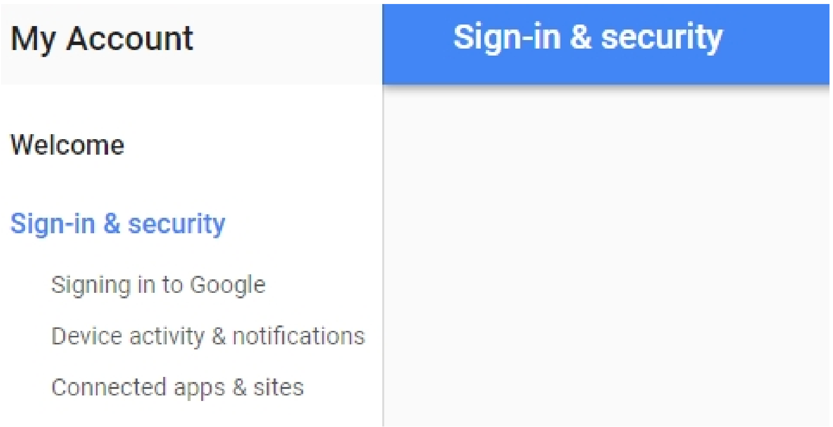
Accessing Your Account with Other Apps and Devices

If you've turned on two-factor authentication, but still want to access your account through applications like Microsoft Outlook or mobile email applications, you can do so through Google's App Passwords feature.

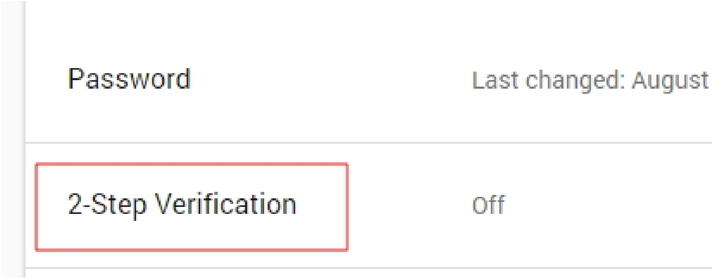
NOTE: If you are using our HyperFIDO NFC security key, you can skip this step and use the security key directly with your mobile device. See *Using HyperFIDO with Mobile Devices* on page 9..

---

1. Sign in to your Google Account and go to My Account.
2. Under Sign-in & Security, click **Signing in to Google**.



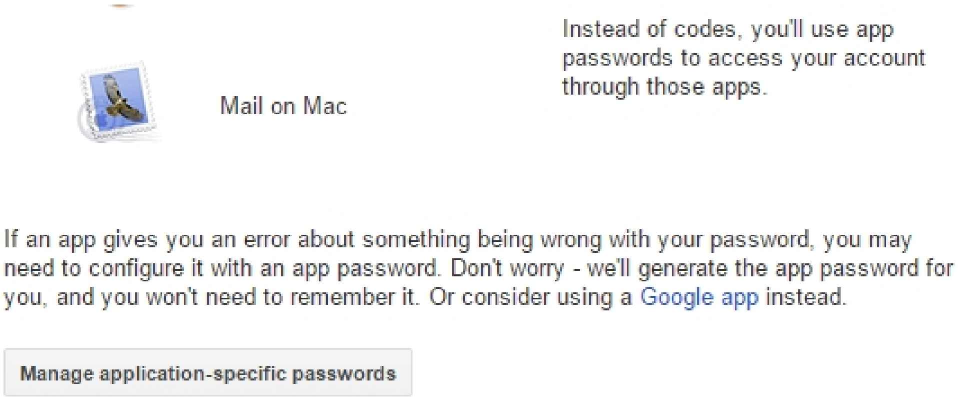
3. Click **2-Step Verification**.



Password Last changed: August

2-Step Verification Off

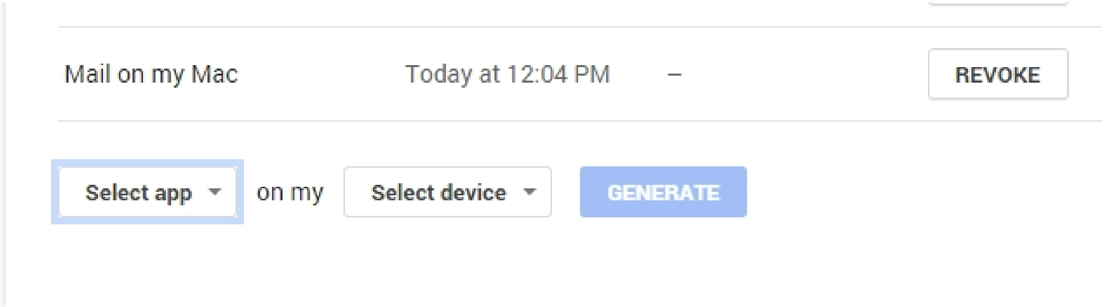
4. Select the **App-specific passwords tab** and click **Manage application-specific passwords**.



Instead of codes, you'll use app passwords to access your account through those apps.

If an app gives you an error about something being wrong with your password, you may need to configure it with an app password. Don't worry - we'll generate the app password for you, and you won't need to remember it. Or consider using a Google app instead.

5. From the Select app drop-down menu, select the appropriate option.
6. From the Select device drop-down menu, select the appropriate option.



Mail on my Mac Today at 12:04 PM –

7. Click **Generate** and follow the instructions on-screen, then click **Done**.

NOTE: You can revoke access from any of these applications or devices from the same screen by clicking **Revoke** next to the application or device you want to remove.

Troubleshooting

Hypersecu Information Systems Inc is not responsible for any errors related to GitHub services and operations. Please contact the support team for GitHub in such cases.

Security Key Won't Authorize

If your HyperFIDO™ security key will not authorize your sign in attempt, try the following options:

- Remove the security key and try the sign in process again. Ensure that the security key is not plugged in before you are prompted to authenticate by pressing the button.
- Ensure the security key you're using has been registered.
- Delete the security key and register it again.

Accessing Your Account Without Your Security Key

If you're unable to use your security key, you can still access your GitHub account.

1. Sign in with your username and password as usual
2. Choose one of the following options:
   - Click **Enter a two-factor code from your phone** to receive an text message with a verification code
   - Click **Enter a recovery code** to use one of your recovery codes if you no longer have access to your mobile device
3. Click **Verify**.

NOTE: If you are unable to recover your account using the methods above, contact GitHub Support for further assistance.

Sudden Loss of Repository Access

If you are suddenly unable to access repositories you previously had access to, you may have deactivated two-factor authentication from your personal account while belonging to an organization that requires its members and collaborators to have two-factor authentication enabled.

To regain access, re-enable two-factor authentication and contact the organization owner to reinstate your access privileges.