

Using HyperFIDO™ with Facebook

11/13/2018

HSTE-NB0033.4-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™?	3
Introduction	3
Requirements	3
Getting Started	4
Setting Up FIDO U2F with Firefox	4
Setting Up FIDO U2F with Linux	5
Automatically Download and Install the Rules File	5
Manually Download and Install the Rules File	5
Enabling Two-Factor Authentication	5
Registering Your HyperFIDO™ Security Key	6
Using Your HyperFIDO™ Security Key	8
Troubleshooting	9
Security Key Won't Authorize	9
Accessing Your Account Without Your Security Key	9
Deleting a Security Key	9

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.

Introduction

This document will demonstrate how to register and use your HyperFIDOU2F security key with a Facebook Account.

NOTE: This document is up to date with Facebook Account procedures on the date of publication. However, Facebook 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 Facebook
- 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.

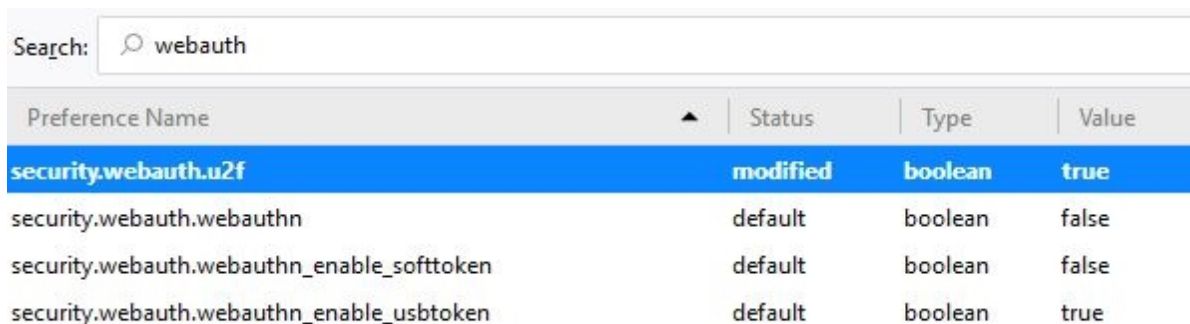
Once your browser and/or operating system is configured for FIDO U2F, you can begin by enabling two-factor authentication on your account.

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.



The screenshot shows the Firefox about:config search interface. A search bar at the top contains the text 'webauth'. Below the search bar is a table of search results. The first row is highlighted in blue and shows the preference 'security.webauth.u2f' with a status of 'modified', a type of 'boolean', and a value of 'true'. The other three rows show 'security.webauth.webauthn' (default, boolean, false), 'security.webauth.webauthn_enable_softtoken' (default, boolean, false), and 'security.webauth.webauthn_enable_usbtokens' (default, boolean, true).

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_usbtokens	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

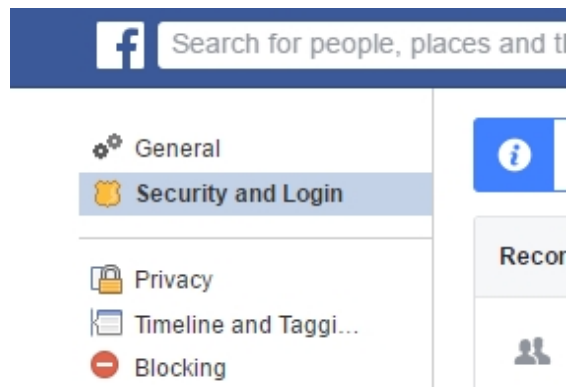
Before you register your HyperFIDO™ U2F security key, you must have two-factor authentication enabled on your Facebook account.

To enable two-factor authentication on your Facebook account, follow the procedure described by Facebook's help topic located here: facebook.com/help/148233965247823.

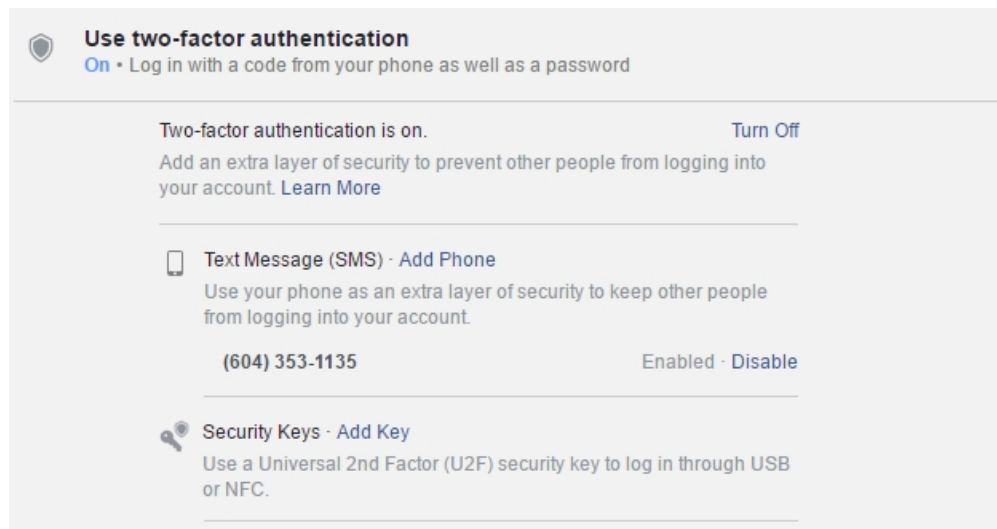
Registering Your HyperFIDO™ Security Key

Once you've enabled two-factor authentication on your Facebook account, you can proceed to register your HyperFIDO™ security key.

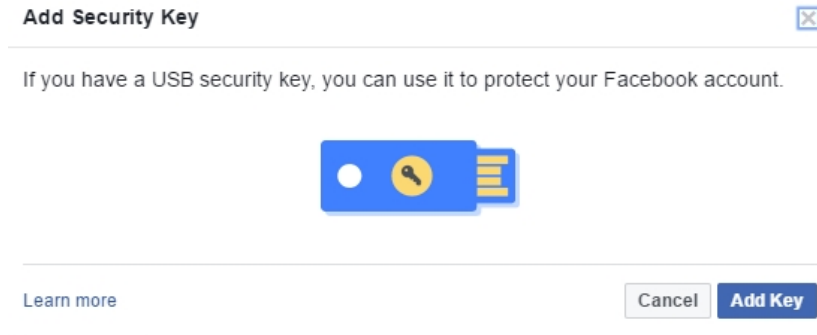
1. Navigate to **Settings** and click **Security and Login**.



2. Under Setting Up Extra Security, click **Use two-factor authentication** to expand the menu, then click **Add Key**.



3. In the Add Security Key window, click **Add Key** again.



4. Insert the HyperFIDO U2F security key into an available USB port.
5. Wait for the security key to blink, then press the button or tap the gold disk.



6. Enter a name for your security key.
7. Click **Done**.

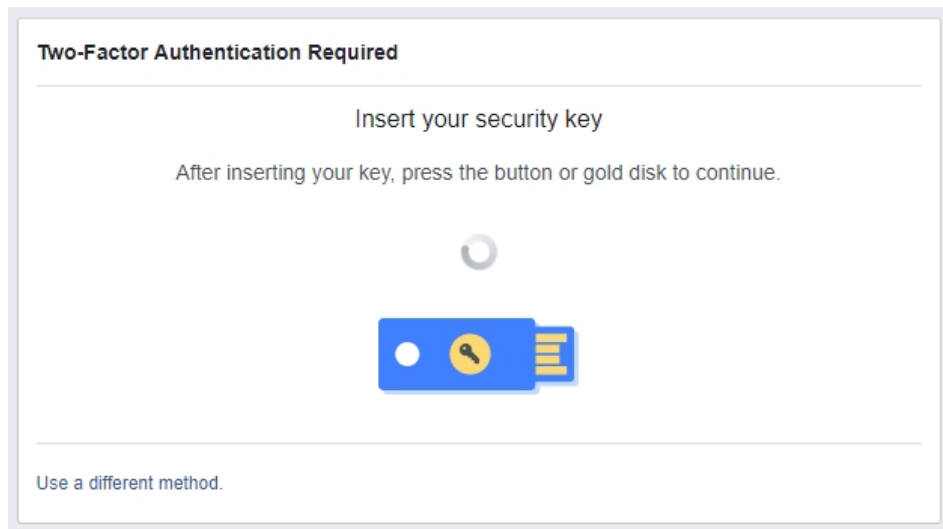
NOTE: You can add multiple security keys to your account. To do so, simply repeat the steps above until you have completed adding all your security keys.

Using Your HyperFIDO™ Security Key

Once you've registered your HyperFIDO™ U2F security key, your Facebook 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 Facebook account with your regular username and password.
2. When prompted, insert your HyperFIDOsecurity key into a USB port.



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

NOTE: If you are on a trusted computer such as a personal laptop, you can choose **Save Browser** to avoid having to use your security key again. Do not choose this option when using a public or otherwise unsecure computer.

Troubleshooting

Hypersecu Information Systems Inc is not responsible for any errors related to Facebook services and operations. Please contact the support team for Facebook 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 Facebook account.

1. Sign in with your username and password as usual
2. When the prompt to insert your security key appears, click **Use a different method**.
 - Use your Facebook Code Generator or a 3rd party code generator and enter the 6-digit code, then click **Continue**.
 - If you do not have access to a code generator, click **Need another way to authenticate?** and click **Text me a login code**, then enter the code sent to you via SMS and click **Continue**.

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

Deleting a Security Key

If you want to delete your security key, you can do so at any time.

1. In the **Security and Login** tab under **Settings**, navigate to Setting Up Extra Security and click **Use Two Factor Authentication**.
2. Locate the name of the security key you want to delete and click **Delete**.



3. Click **Delete Key** to confirm you want to delete the security key.

IMPORTANT: Deleting all of your security keys will cause Facebook to use an alternate authentication method the next time you sign in, such as text messaging. Ensure that you have a valid alternate authentication method set up before removing all security keys.
