HYPERSECU®

Using HyperFIDO™ with Google Accounts

11/13/2018

HSTE-NB0033.1-RV 1.2

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 Google Account.

NOTE: This document is up to date with Google Account procedures on the date of publication. However, Google 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 Google
- 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 2-step verification on your account.

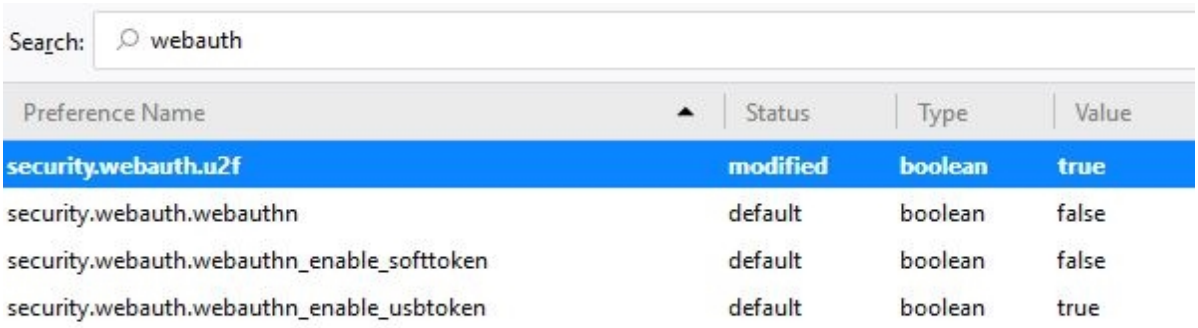
Setting Up FIDO U2F with Firefox

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.



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 2-Step Verification

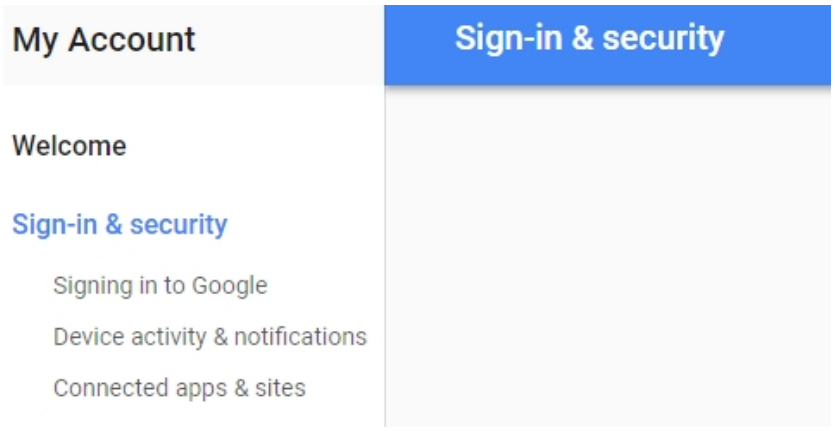
Before you register your HyperFIDO™ U2F security key, you must have 2-step verification enabled on your Google account.

If you already have 2-step verification enabled, you're ready to register your HyperFIDO security key. See *Registering Your HyperFIDO™ Security Key* on page 7..

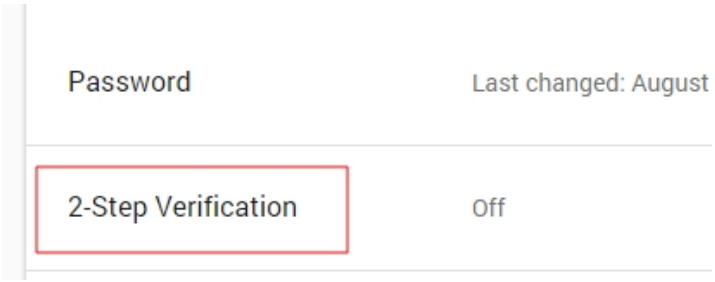
IMPORTANT: You must use a valid phone number when setting up 2-step verification. A valid phone number will allow you to access your account in the event your security key is lost.

---

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**.



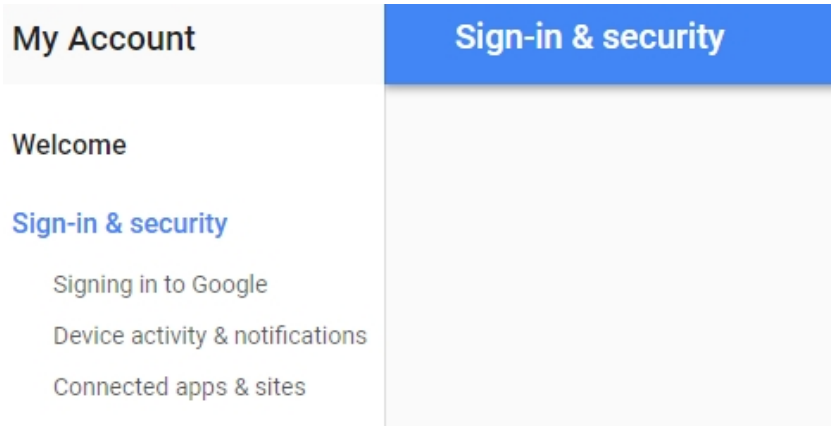
4. Follow the instructions provided on screen to finish setting up 2-step verification.

Registering Your HyperFIDO™ Security Key

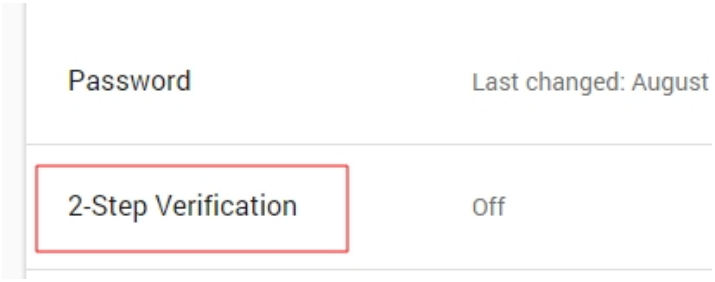
Before you register your HyperFIDO™ U2F security key, you must have 2-step verification enabled on your Google account. If you do not have 2-step verification enabled and are unsure of how to do so, see *Enabling 2-Step Verification* on page 5..

Once 2-step verification is enabled, you're ready to register your HyperFIDO security key.

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

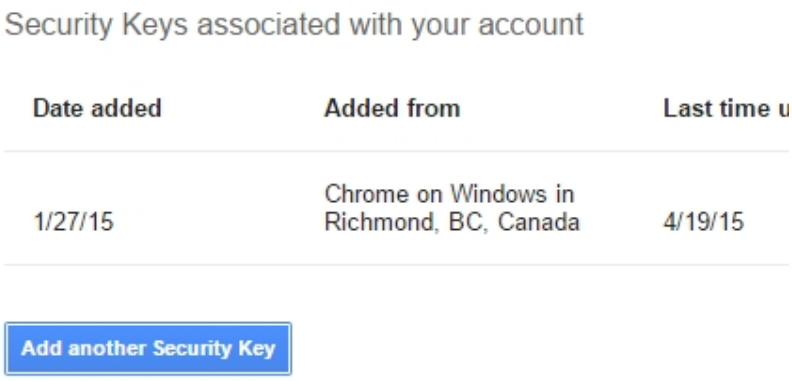


3. Click **2-Step Verification**.



4. Select the **Security Keys** tab and click **Manage**.

5. Click **Add another Security Key**, then follow the instructions on screen.



6. Once registration is complete, remove your HyperFIDO security key.

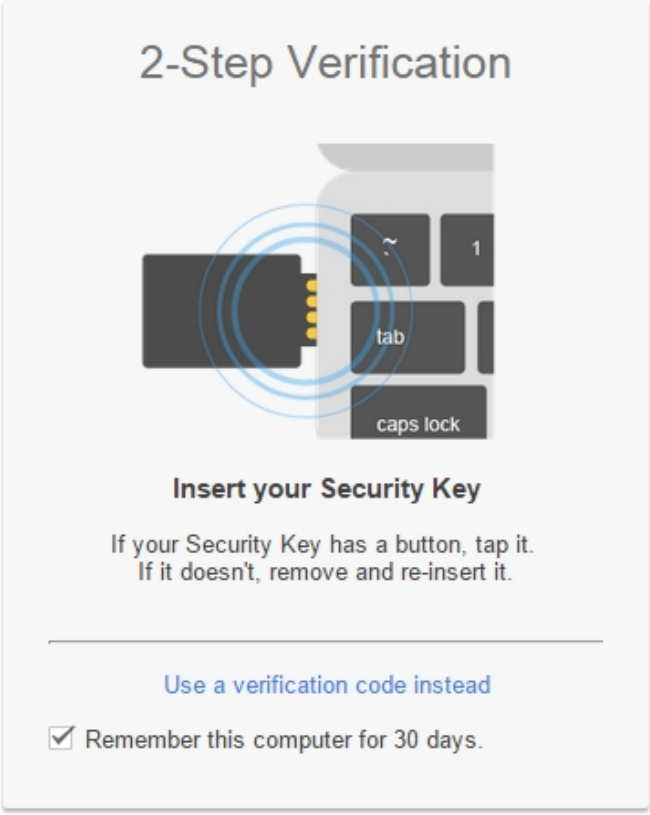
NOTE: Do not leave your HyperFIDO security key unattended inside your USB port. It's important to keep the device with you or stored safely away from your computer to ensure maximum security.

Using Your HyperFIDO™ Security Key

Once you've registered your HyperFIDO™ U2F security key, your Google 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 HyperFIDO on Desktop

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

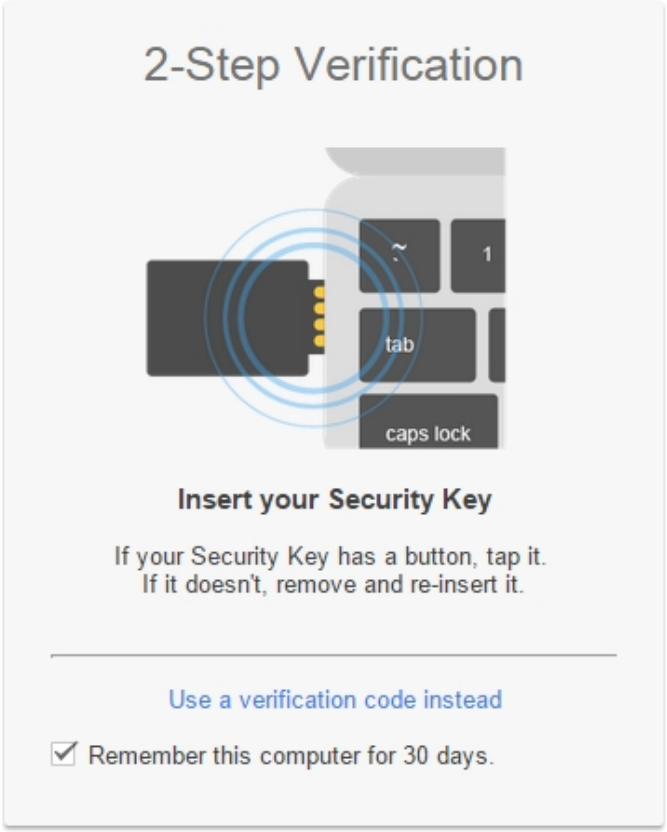


3. Press the button on your security key to finish signing in.

Enabling a Trusted Computer

You can choose to enable a specific computer as a trusted computer. This means you will not be asked for your security key for 30 days. Only private computers such as your home desktop should be marked as trusted.

To enable a trusted computer, simply check the **Remember this computer for 30 days** check box when signing in or registering your security key.



NOTE: The **Remember this computer for 30 days** check box is checked by default. Uncheck this box before performing the authentication if you don't want the computer to be remembered.

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 11.

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.

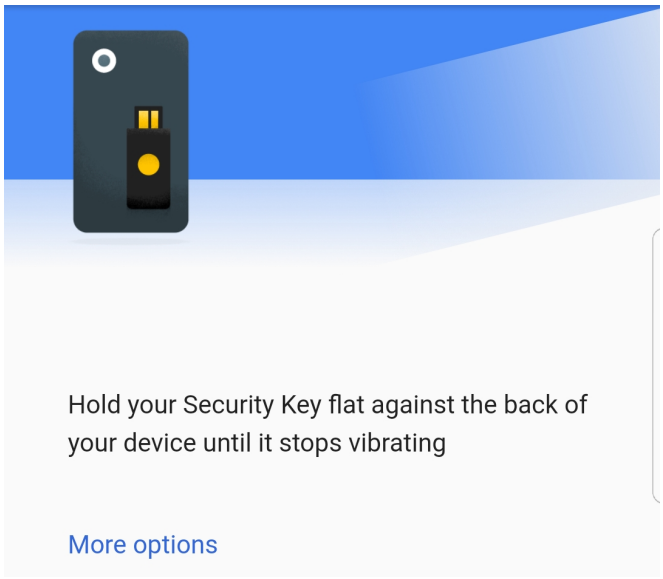
---

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.



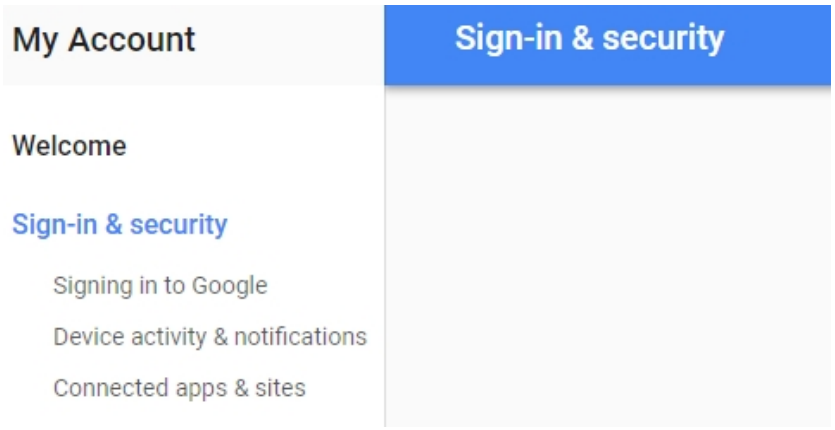
Accessing Your Account with Other Apps and Devices

If you've turned on 2-step verification, 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.

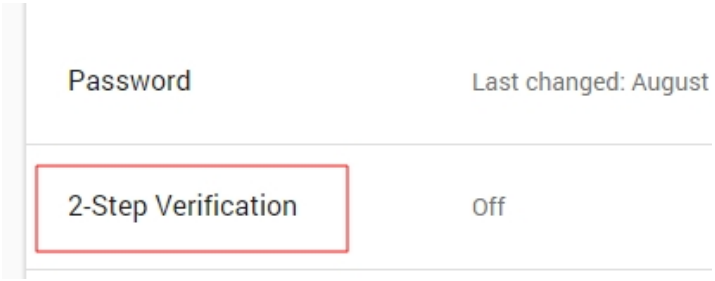
NOTE: If you are using our HyperFIDO NFC security key, you can skip this step and use the security key directly with your mobile device. See *Using HyperFIDO with Mobile Devices* on page 10..

---

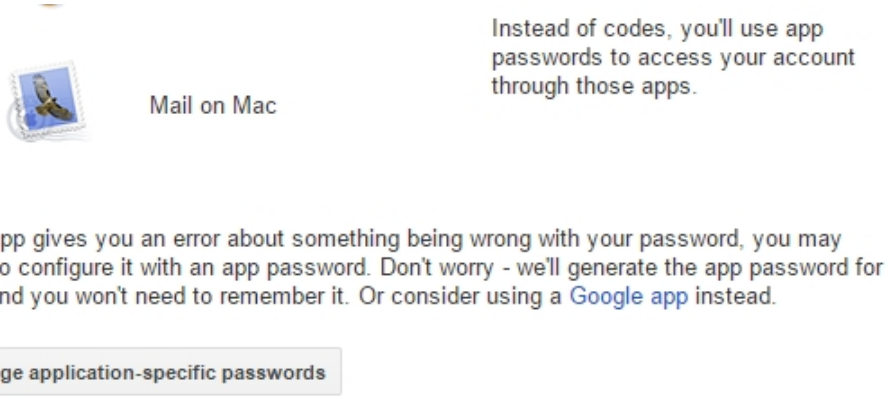
1. Sign in to your Google Account and go to My Account.
2. Under Sign-in & Security, click **Signing in to Google**.



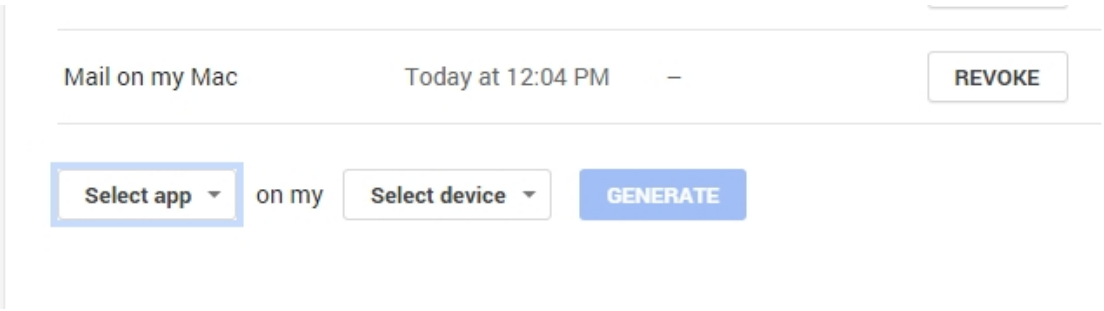
3. Click **2-Step Verification**.



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



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



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 Google services and operations. Please contact the support team for Google 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.

Security Key Not Recognized

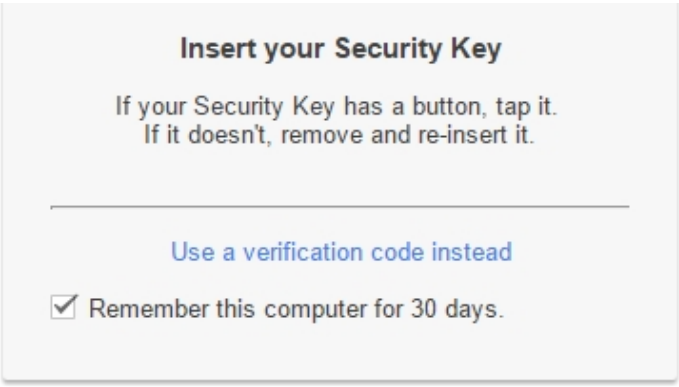
If your HyperFIDO™ security key is not recognized by your device, try the following options:

- If the security key is a HyperFIDO NFC security key, ensure that NFC is enabled on your mobile device.
- Remove your security key and try the registration or sign in process again.
- Restart your device and try the registration or sign in process again.

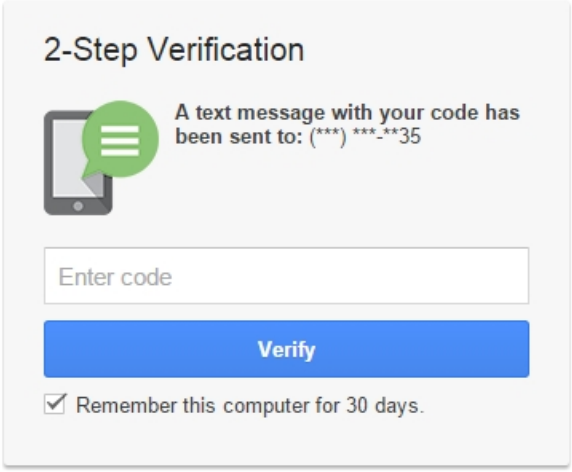
Accessing Your Account Without Your Security Key

If you're unable to use your security key, you can still access your account provided you have attached a valid phone number to your account.

1. Sign in to your Google Account with your regular username and password.
2. When prompted to enter your security key, click **Use a verification code instead**.



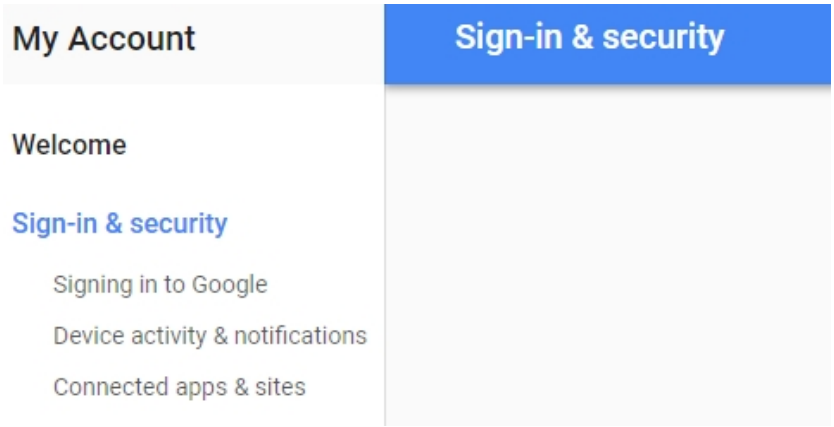
3. Once you've received a text message on your phone with the verification code, enter the code and click **Verify** to sign in.



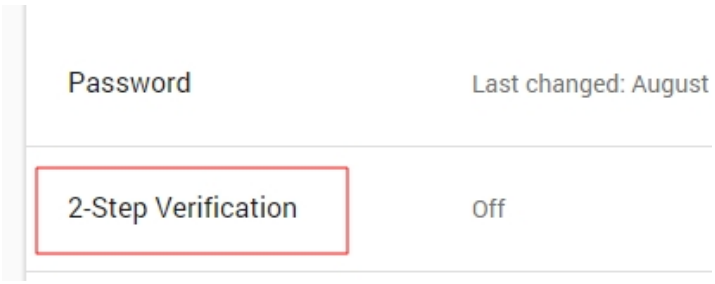
Removing a Trusted Computer

If you wish to remove a trusted a computer before 30 days have expired, you can do so manually.

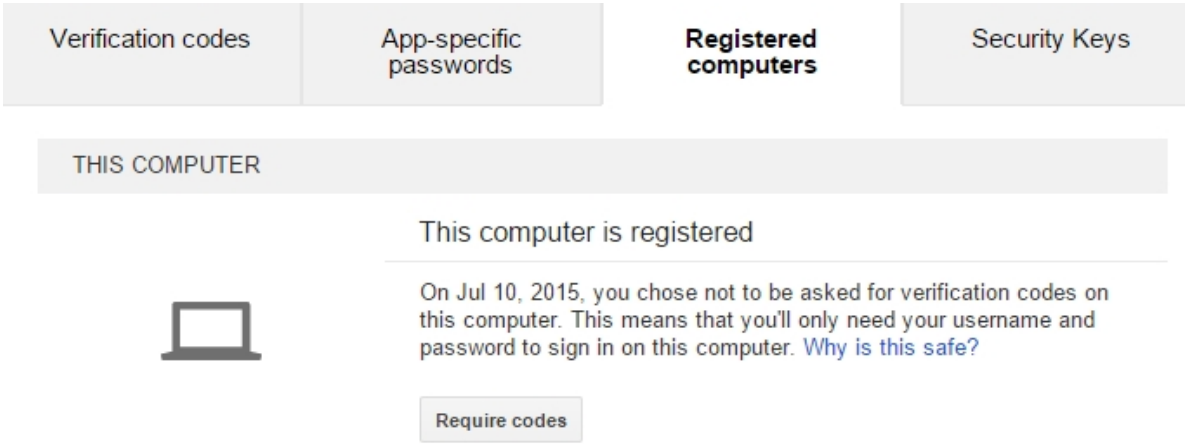
1. Sign in to your Google Account and go to My Account.
2. Under Sign-in & Security, click **Signing in to Google**.



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



4. Select the **Registered computers** tab and perform one of the following actions:
   a. If you are currently using the computer you want to remove as trusted, click **Require codes** under This Computer.



   b. If you want to remove all other previously registered computers and devices except for the one you are currently using, click **Change setting** under Other Computers and Devices, then click **Require codes**.