YubiKey & OATH-TOTP Verification

May 7, 2015

Introduction

Yubico is the leading provider of simple, open online identity protection. The company's flagship product, the YubiKey®, uniquely combines driverless USB hardware with open source software. More than a million users in 100 countries rely on YubiKey strong two-factor authentication for securing access to computers, mobile devices, networks and online services. Customers range from individual Internet users to e-governments and Fortune 500 companies. Founded in 2007, Yubico is privately held with offices in California, Sweden and UK.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Trademarks

Yubico and YubiKey are trademarks of Yubico Inc.

Contact Information

Yubico Inc
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
USA
info@yubico.com

1 Setting up the YubiKey for OATH-TOTP

All YubiKey hardware can support the OATH-TOTP standard authentication method, used by services such as Microsoft Cloud accounts, Google Apps, Dropbox, EverNote and GitHub.

This method utilizes one of the two configuration slots for a single site; no more than 2 sites or services can be supported on a single YubiKey. If there is a need to support additional sites or services, Yubico recommends the YubiKey NEO used with the YubiKey Desktop Authenticator and YubiOATH Android app.

To setup your YubiKey for OATH-TOTP 2-step verification, you will need:

- Access to the account to be secured with OATH-TOTP
- The YubiTOTP application
- A YubiKey version 2.2 (or later) with an empty configuration slot

The YubiTOTP application above can be found in the Yubico webpage:

http://www.yubico.com/applications/internet-services/gmail/

Caution: YubiKeys normally come shipped with the first configuration slot Pre-configured with either a Yubico OTP or a Symantec VIP credential. Be extra careful about overwriting this. This guide assumes that you decide to use the second configuration slot, which is empty by default.

The procedure adds a Challenge/Response configuration to the YubiKey in HMAC- SHA1 mode using the shared OATH secret from the site or service to be secured. The helper app (YubiTOTP) passes the current system time as a challenge to the YubiKey and processes the response as per the OATH specification to generate a 6 or 8 digit OATH-TOTP code. The helper app is triggered by double clicking the icon in the system tray. The OATH-TOTP 6 or 8 digit response is automatically typed into the text field the cursor is currently in.

2 Configuring a YubiKey for TOTP on a Secured Site

When setting up a YubiKey to work with a site protected with OATH-TOTP, the process will be to take the secret key provided by that site and configure it directly into one of the slots on the YubiKey.

While each site will have a different process to present the secret key slightly differently, the process should have some similar steps:

1. **Log into your Account** – Before 2-Factor verification can be applied to any account, you will first need to be able to log into the account.

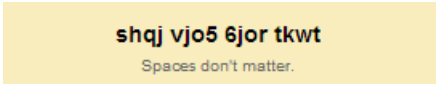
2. **Access Security / 2nd Factor Verification Settings** – Most sites or services will have the settings for 2-Factor verification in the Security section of the user account settings. Some sites will require verification of a backup device, like an SMS/text message capable mobile phone, before permitting users to set up a 2nd Factor Verification device.

3. **Select Mobile Application** – When setting up your YubiKey, you will want to choose the option to set up a Mobile Application for verification; the process for configuring the YubiKey uses the same secret key as used by less secure mobile authentication apps. For ease of use, Yubico recommends selecting “Android” as the device type if prompted.

4. **Look for the QR code** – Most sites or services first present the secret key as a QR Code (see example below). When a QR code is presented, there should be a link or option to present the secret key as plain text as well, such as an option if the QR code cannot be scanned

Example of a QR code image

5. **Display the Secret Key as text** – Clicking on the link or option to display the secret key should display the key as text. The secret key is often displayed in blocks of no more than 4 characters apiece.

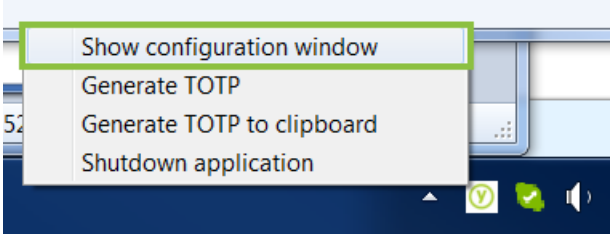


Example of a Secret Key

6. **Copy the Secret Key** – Copy the Secret Key to the clipboard. It is HIGHLY recommend to also save the secret key to a secure location or to print it out and file it with other records. With a copy of the secret key, a backup YubiKey can be configured to gain access to the secured account in the event your primary YubiKey is unavailable.

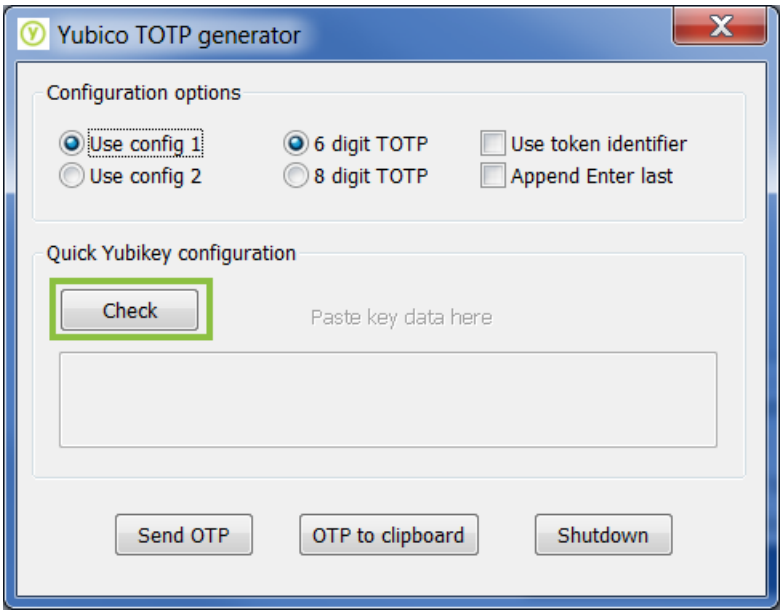
7. **Plug in your YubiKey & Launch the YubiTOTP app** – The YubiTOTP app will automatically configure the YubiKey when the secret code is provided. When running, the YubiTOTP app should appear in the icon tray on the task bar (icon may be hidden at first). The YubiTOTP app will also need to be running to generate the Verification codes once the YubiKey is configured.

8. **Open the YubiTOTP Configuration Window** – Open the configuration window by right clicking the YubiTOTP app taskbar icon. In the Right click context menu, select "Show configuration window"

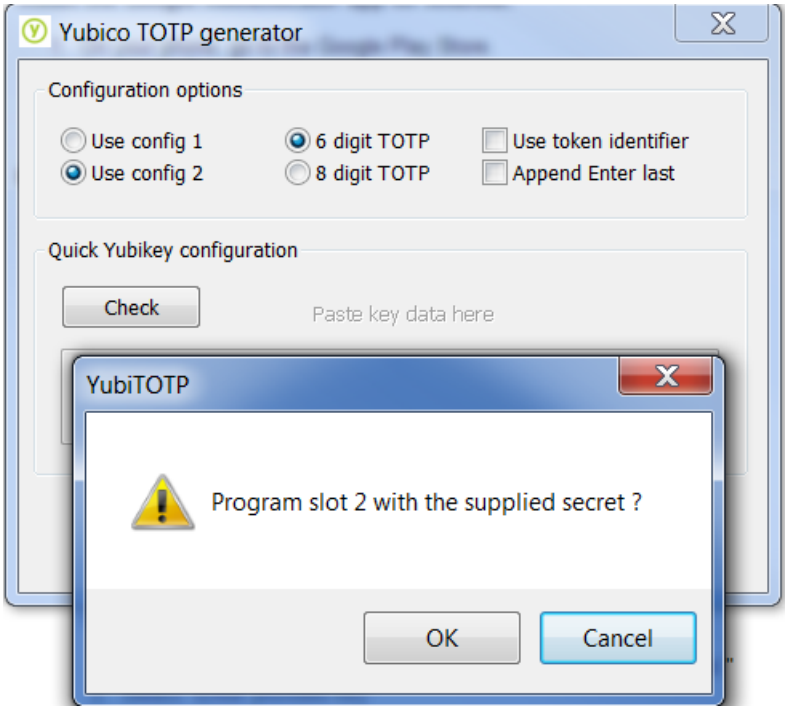


9. **Configure the OATH-TOTP Settings** – Check with the service for the OATH-TOTP verification settings. If settings are not explicitly stated by the site or service, use the "6 digit TOTP" option and ensure the "Use token identifier" and "Append Enter last" options are not checked.

10. **Check your YubiKey** – Ensure the correct YubiKey is plugged in click the "Check" button on the YubiTOTP configuration window.



11. **Paste the Secret Key in the YubiTOTP app** – From the Clipboard, paste the secret key into the text field in the YubiTOTP app. This will automatically start the process to program the YubiKey to work with the YubiTOTP app for the OATH-TOTP verification. When prompted to program the selected Configuration slot, select “Yes” to proceed.



12. **Congratulations, your YubiKey has been successfully configured!** When the site or service prompts you for the Verification Code, put the cursor in the indicated field, select (or double click) the Yubico icon in the system tray then select "Verify". You may want to configure your system tray so the YubiTOTP icon is always visible "show icon and notifications".

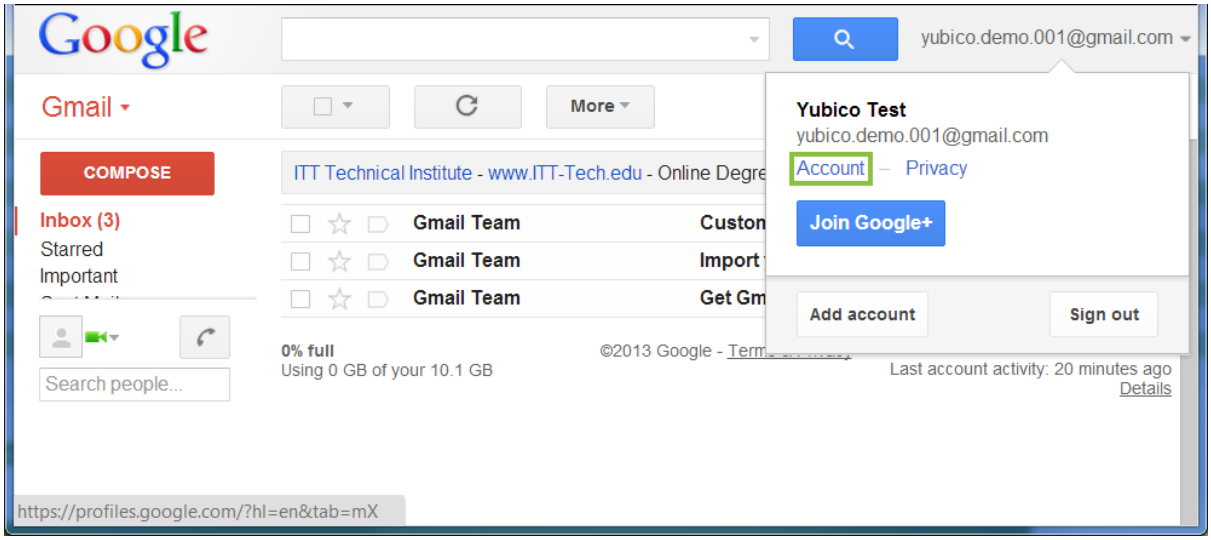
13. **Using the YubiTOTP app** – When asked for a TOTP code from the secured site, make sure the YubiTOTP app is launched. With your configured YubiKey plugged in, click inside the field indicated for the TOTP code, then double click the YubiTOTP icon. The code will be entered automatically.

14. **Create a back-up YubiKey** – A backup YubiKey can be created at any time using the YubiTOTP app and the secret key acquired from the site. Simply follow the previous steps with the new YubiKey, but use your existing secret key instead of requesting a new one from the site or service. Requesting a new secret key from an OATH-TOTP secured site will result in your original YubiKey to no longer be valid for that site or service.

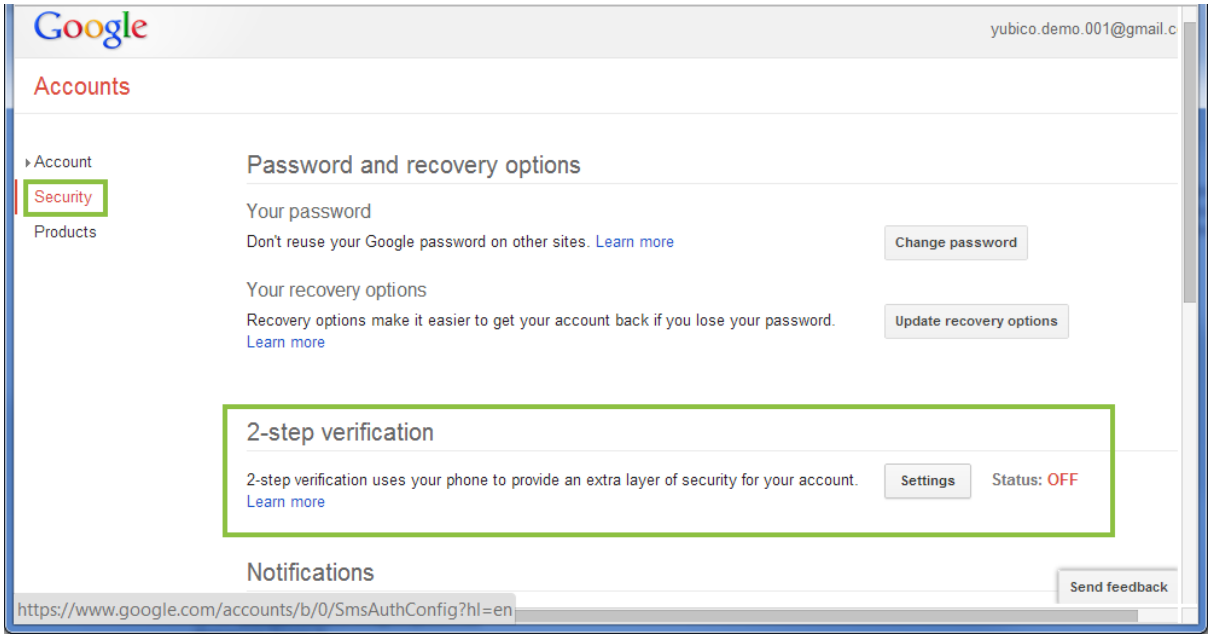
3 Setting up Google Apps

As an example, below are the steps required to set up a Google Apps account's OATH-TOTP 2-factor verification with a YubiKey and the YubiTOTP app.

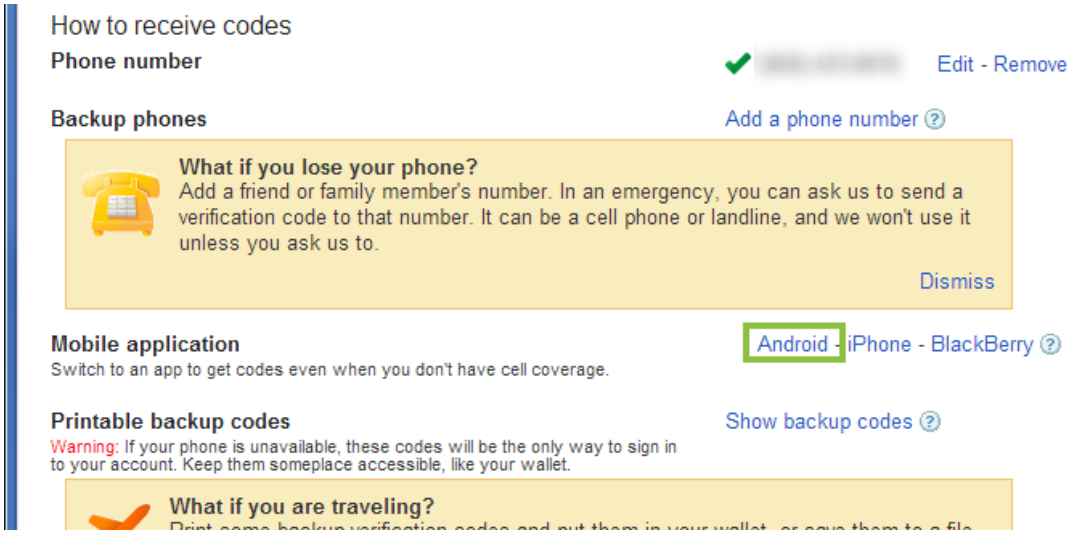
1. Log in to your Gmail Account and choose "Account".



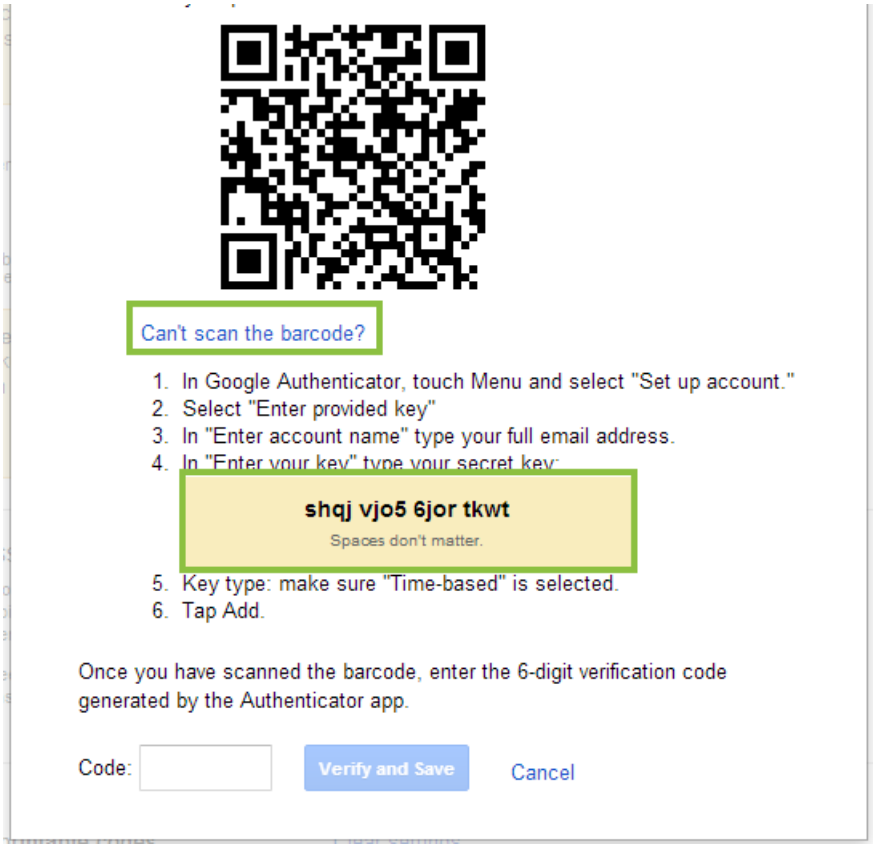
2. In the Account page, select "Security" and locate the "2-step verification" section. Click the button labelled settings, and proceed to register for 2-step verification by registering a telephone number to the Google Account.



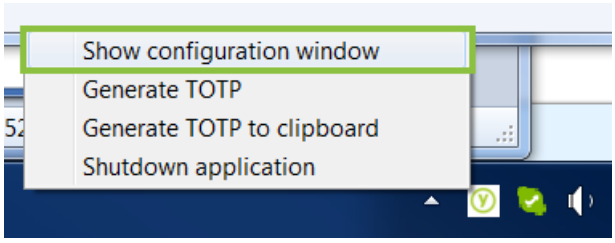
3. Once 2-step verification is enabled, locate the “Mobile Application” section and select the Android option. The actual screen layout may be a bit different based on your region.



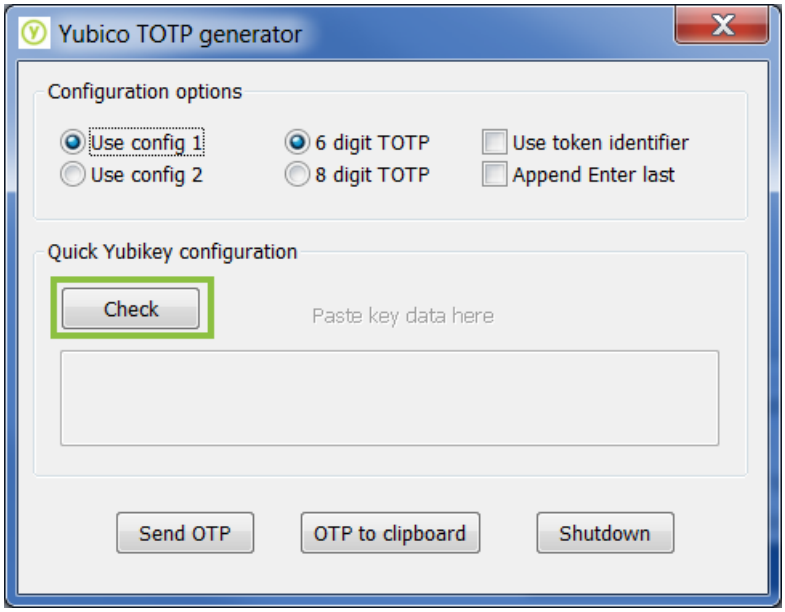
4. In the dialog that opens, click the “Can’t scan the barcode?” link under the image and copy the 20 digit key provided.



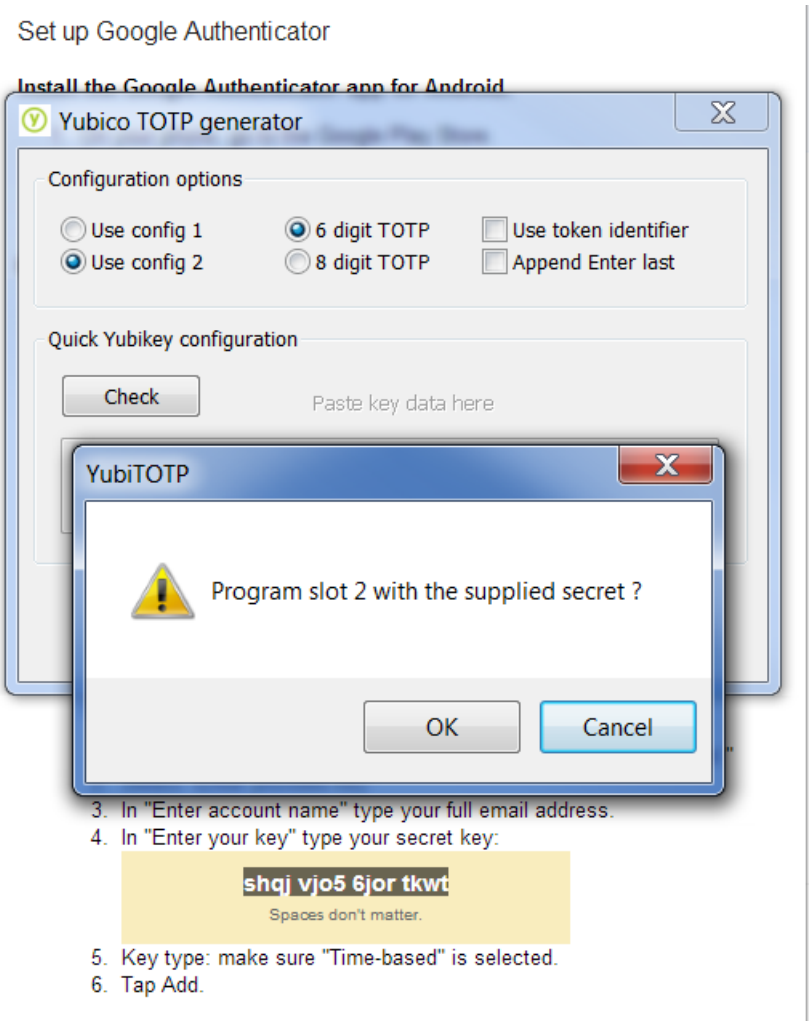
5. Launch the YubiTOTP app and right click its taskbar icon. In the Right click context menu, select “Show configuration window”



6. Plug in your YubiKey and click the “Check” button on the YubiTOTP configuration window. Make sure the “Use token identifier” and “Append Enter last” options are not checked.



7. Paste the Google Application key into the text field in the YubiTOTP app. This will automatically program the YubiKey to work with the YubiTOTP app for the Google Authenticator.



8. Congratulations, your YubiKey has been successfully configured! When Google prompts you for the Verification Code, put the cursor in the box, select (double click) the Yubico icon in the system tray then select "Verify". You may want to configure your system tray so the YubiTOTP icon is always visible "show icon and notifications".

4 Troubleshooting

If your YubiKey is not generating valid codes, check the following:

- Make sure the correct YubiKey is inserted.
- Make sure only a single YubiKey is inserted in the computer.
- Attempt to enter another code – TOTP codes have a limited lifespan, and are often not valid after 30 seconds or less. If a TOTP code is not entered soon enough, it may expire and a new code will need to be generated.
- Make sure the system time on the host computer is correct – if the system time is off, the time-dependent codes will not be valid. Make sure the host computer is set to the correct time, or automatically syncing its internal clock to a valid timekeeping site.
- Make sure your YubiKey is plugged in securely and in the correct orientation with the USB slot. If the LED on the YubiKey is not on, it is not inserted correctly.