yubico

# Securing Google Workspace with YubiKeys

© 2025 Yubico

yubico

# Workshop Agenda

| Topic | Estimated Duration |
|---|---|
| Welcome & Introductions | 0:05 |
| What is a YubiKey? | 0:05 |
| Concepts and Use Cases | 0:20 |
| YubiKey 101 | 0:15 |
| Google Administrator Configurations | 0:30 |
| User Registration and Authentication | 0:15 |
| Redeeming Pro Services Hours Post-Workshop | 0:10 |
| Questions and Wrap-Up | 0:15 |
| **Total** | **1:55** |

© 2025 Yubico

This document is the exclusive property of Yubico

# Yubico's Professional Services Team

## Deployment Advisors

Molly Babcock

Laura Eppley

Jeff Olives

## Engineers

Greg Whitney

Dante Melo

Mitchell Armenta

Kanchan Thakur

Scott Truger

© 2025 Yubico

This document is the exclusive property of Yubico

# What is a YubiKey?

© 2025 Yubico

yubico

# Technical Overview

## Easy, Fast, & Reliable Authentication

**YubiKey does not require a battery or network connection.**

FIDO2 CERTIFIED

**Waterproof** **Crush Resistant**

© 2025 Yubico

This document is the exclusive property of Yubico

# Concepts and Use Cases

© 2025 Yubico

yubico

# What is an Authentication Factor?

- Factors of authentication are something **you know** (knowledge), something **you have** (possession), and something **you are** (inherence)
- Something **you know** is most often a password or a PIN
- Something **you have** might be a bank card, OTP fob, or a YubiKey
- Something **you are** comprises biometric uniqueness, like your fingerprint or iris

© 2025 Yubico

This document is the exclusive property of Yubico

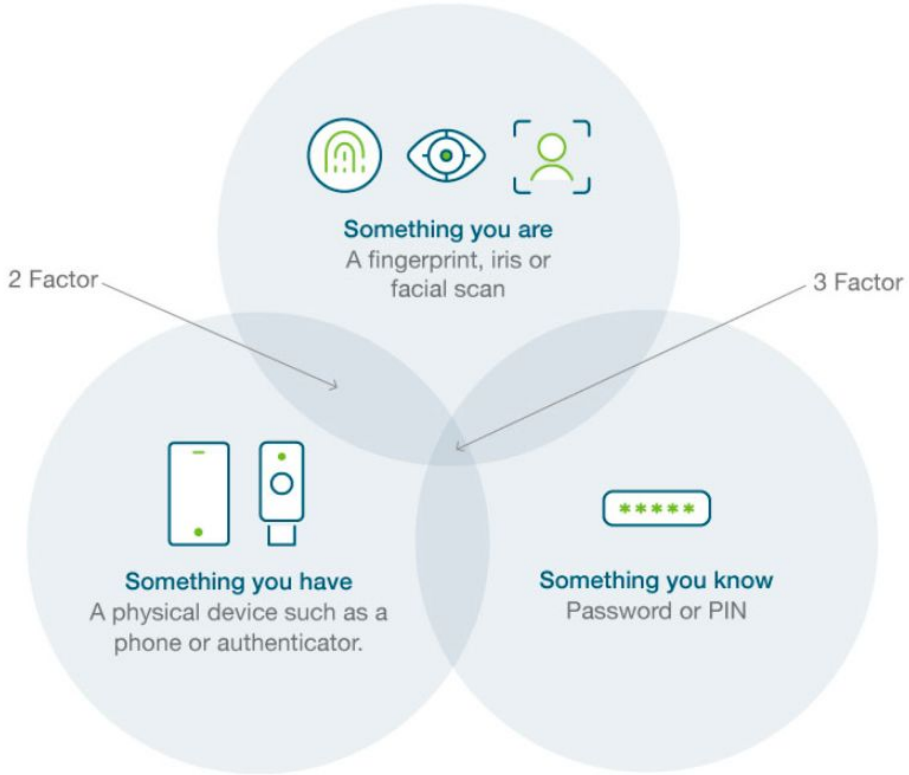
# What is Multi-Factor Authentication (MFA)?

- Multi-factor authentication is a process of identifying yourself (proving you are who you say you are) that involves multiple authentication factors
- Although username and password authentication involves two components (the username and password) it is **not** multi-factor authentication because both components are something you know. This is instead single-factor authentication
- Performing a cash withdrawal at an ATM using a bank card typically involves multi-factor authentication, as it involves something you have (the bank card), and something you know (the card's PIN)

© 2025 Yubico

This document is the exclusive property of Yubico

# Authentication Factors




© 2025 Yubico

This document is the exclusive property of Yubico

# What is Phishing?

- Phishing is attempting to trick people into revealing personal information like passwords
- Phishing often comes in the form of email or text message, often written with a sense of urgency (you will lose access, your account will be terminated, etc.)

© 2025 Yubico

This document is the exclusive property of Yubico

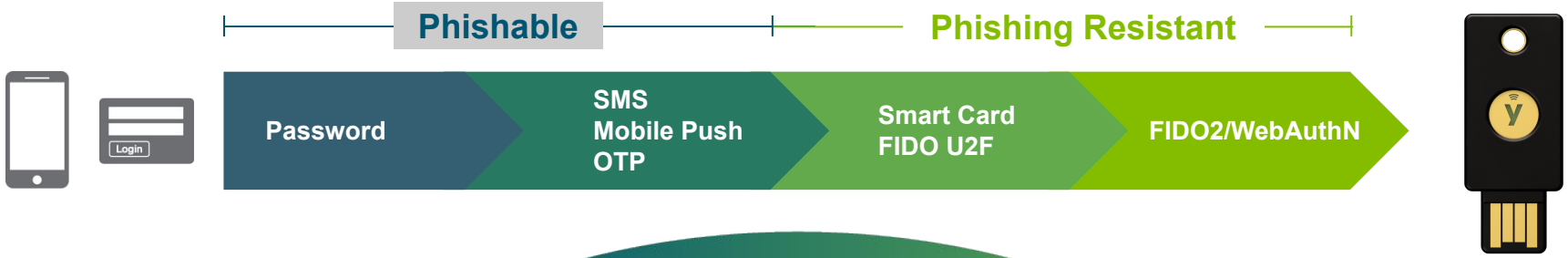
# What is Phishing-Resistant MFA?

- Phishing-resistant MFA is a category of multi-factor authentication that is designed to be less vulnerable to phishing attacks
- As an example, FIDO/WebAuthn includes the domain name (origin) of the service being registered with in the registration
    - As a result, a FIDO/WebAuthn authentication request will not be successful if the domain name does not match that established at the time of registration
    - This is passive phishing protection. Even if users do not realize they are being phished, FIDO will not allow them to complete authentication, because the domain name will not match, as is often the case with phishing attempts

© 2025 Yubico

This document is the exclusive property of Yubico

# Phishing-Resistant MFA Illustrated



© 2025 Yubico

This document is the exclusive property of Yubico

# Google Workspace MFA Methods

Source: F

| Factor Type | Security | Usability | Phishing Resistance |
|---|---|---|---|
| Security Keys | Strong | Easy | ✅ |
| Passkeys | Strong | Easy | ✅ |
| Google Prompt | Strong | Moderate | ⚠️ |
| Backup Codes | Moderate | Difficult | ⚠️ |
| Google Authenticator (Phone app OTP generator) | Moderate | Moderate | ❌ |
| Text Message | Weak | Moderate | ❌ |
| Phone Call | Weak | Moderate | ❌ |
| Passwords | Weak | Easy | ❌ |

© 2025 Yubico

This document is the exclusive property of Yubico

# What is FIDO2?

- FIDO stands for **F**ast **ID**entity **O**nline, and began as a standard developed by multiple companies, including Yubico, with the vision of bringing strong public key cryptography to the mass market
- Originally, FIDO was FIDO U2F, or Universal **2**nd **F**actor
- FIDO2 builds upon U2F, facilitating the possibility of passwordless multi-factor authentication
- Based on public key cryptography, FIDO2 offers strong, phishing resistant authentication that does not depend on a public key infrastructure or other on-premises resources
- In Google Workspace, FIDO2 registration is self service
- A FIDO2 credential is also known as a **Passkey**
- **Additional resources:**
  - WebAuthn Introduction and FIDO building blocks
  - What is FIDO2?
  - What is a Passkey?

© 2025 Yubico

This document is the exclusive property of Yubico

# Identity Provider (IdP)

- An **Identity Provider (IdP)** is a system that stores users' information, verifies their identity, and provides that information to other applications or services
- **Benefits**
  - **Improved security** - IdPs often support advanced authentication methods like FIDO2 or passkeys, making it harder for hackers to gain access
  - **Single Sign-On (SSO)** - Users can access multiple applications with a single login, saving time and frustration
  - **Simplified User Management** - Administrators can easily manage user accounts, permissions, and access policies from a central location

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# Google Workspace Use Cases

- In-browser logon to applications that are federated with Google as their IdP
- Human Resource Information Systems (HRIS) with Google as the authoritative source
- Mobile devices in-browser logon
- Mobile devices native apps logon

© 2025 Yubico

This document is the exclusive property of Yubico

# YubiKey 101

© 2025 Yubico

yubico

# Authentication protocols

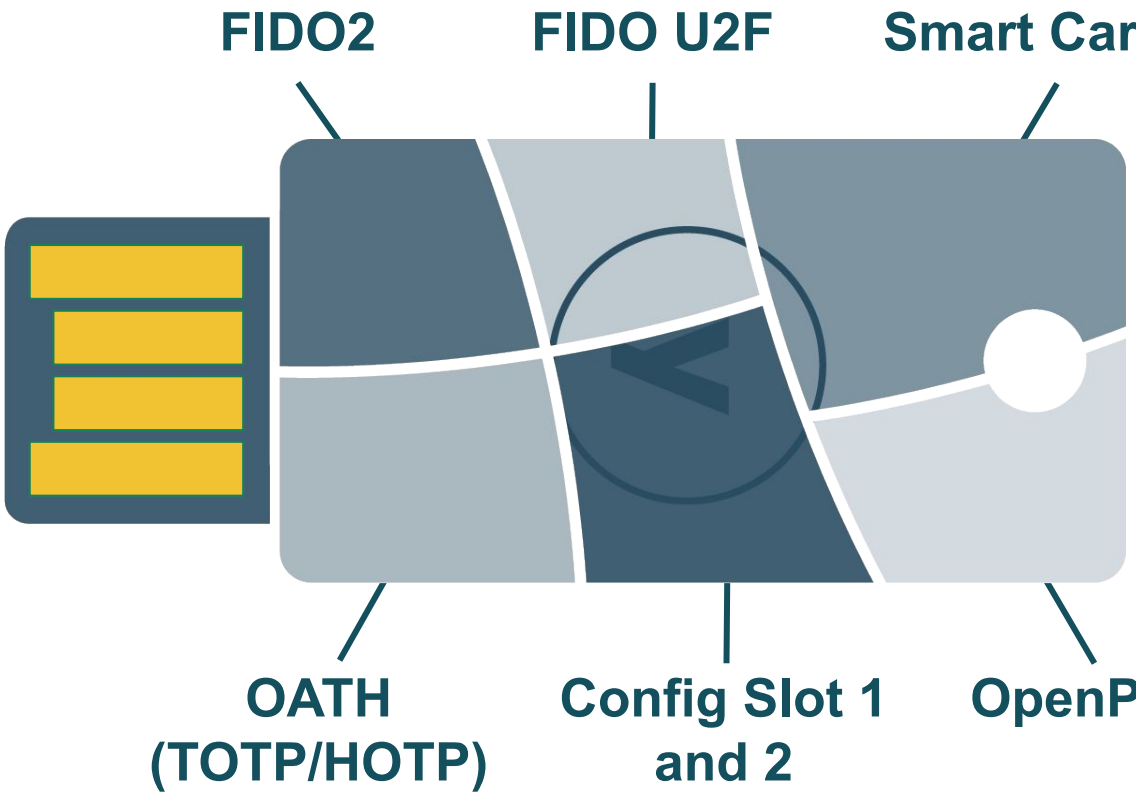
- The YubiKey is a hardware authenticator
- It supports several authentication protocols

| Shared secrets/symmetric crypto | Asymmetric crypto |
|---|---|
| Challenge-Response | OpenPGP |
| OATH TOTP, HOTP | PIV smart card |
| Yubico OTP | FIDO U2F, FIDO2 |

© 2025 Yubico

This document is the exclusive property of Yubico

# YubiKey Multiple Protocol Support




**Config Slot 1 + 2**
Yubico OTP
OATH-HOTP
Challenge-Response
Static Credential

© 2025 Yubico

This document is confidential to Yubico
CONFIDENTIAL - DO NOT SHARE

yubico

# YubiKey interfaces

- The YubiKey is a hardware device
- The physical interfaces are USB and NFC
- The USB interface provides 3 types of channels:
  - The OTP interface presents itself to the operating system as a USB keyboard
  - The FIDO interface presents itself as a generic human interface device (HID)
  - The CCID interface presents itself to the operating system as a USB smart card reader
- The NFC interface provides all applications (in a slightly different way, since an NFC reader is in the middle)

© 2025 Yubico

This document is the exclusive property of Yubico

# Symmetric Cryptography

- Symmetric cryptography: same key is used to encrypt and decrypt
- Both parties need to have a copy of the key
- This means both the user and the Credential Service must have a copy of the key

© 2025 Yubico

This document is the exclusive property of Yubico

# Public Key Cryptography

- Here the parties have key pairs (public, private)
- Also known as “asymmetric cryptography”
- It is not feasible to find the private key from the public key
- The user keeps the private key protected, and shares the public key with Relying Parties

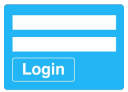
© 2025 Yubico

This document is the exclusive property of Yubico

# Authentication Progression

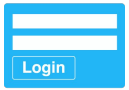
1960s — 2004 — 2014 — 2018

**Passwords**

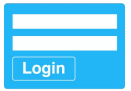



**Tokens & Smart Cards**

**FIDO U2F**



**FIDO2**



**FIDO2**

**FIDO2**

**FIDO (Fast Identity Online)**

- Strong two factor authentication
- One key to many services
- Strong phishing defense
- No client software, native support
- Deprecated 2022

Google yubico

yubico Microsoft Google

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# FIDO2 Summary

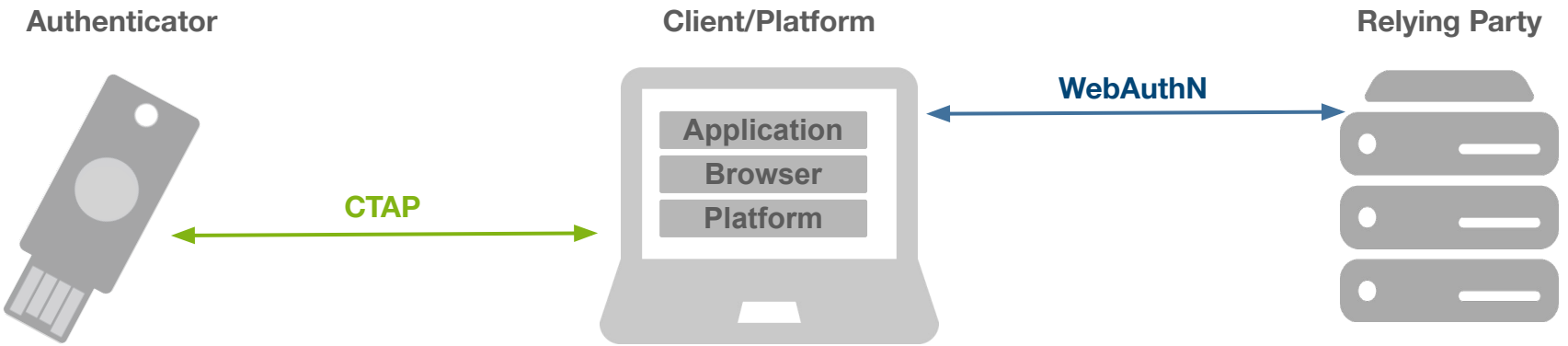
- Allows login securely without a password
  - Strong layered security multi-factor authentication
  - Strong defense against phishing and Man in the Middle(MitM) attacks
  - High usability with rapid login
- Built into widely adopted platforms (e.g. Windows) and on track for standardization via W3C, with support by all major browsers (e.g. Google, Mozilla, Edge, etc.)
- Includes the features of the original FIDO U2F

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# How FIDO2 Authentication Works



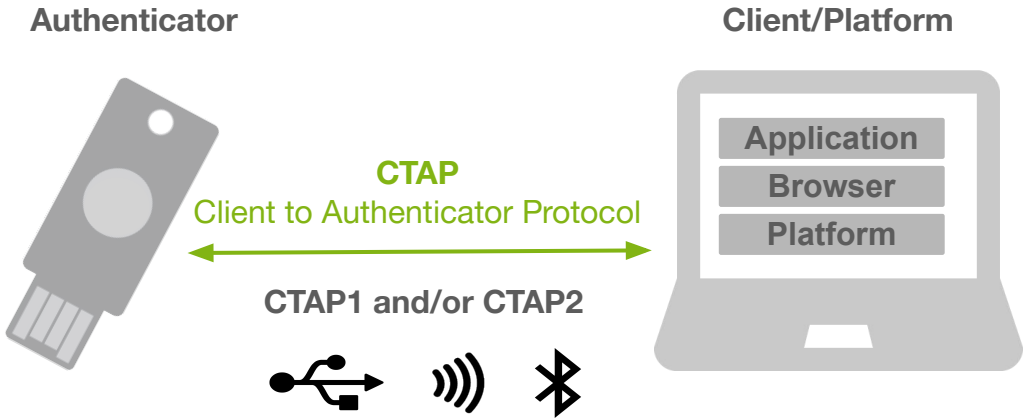

- **FIDO2 = CTAP + WebAuthn**
- A set of open standards utilizing public-key cryptography to enable strong first factor, second and multi-factor authentication

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# What is CTAP?




**Application layer protocol used to communicate between an external authenticator (i.e. security key) and a client (desktop) or a platform (OS)**

Authenticator generates and securely stores credentials

Private keys, PINs, and biometric information never leave the authenticator

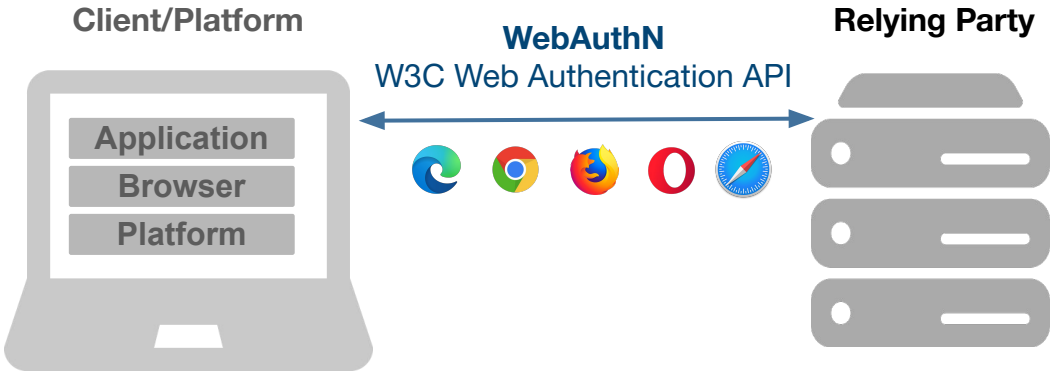
Communicates over USB, NFC, and Bluetooth

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# What is WebAuthn?




**Specification that enables the creation and use of strong public key-based credentials by web applications**

Strongly authenticate users

Major browsers are on track to implement full Web Authentication APIs

Includes FIDO2, allowing backwards compatibility of FIDO U2F with capable authenticators

© 2025 Yubico

This document is the exclusive property of Yubico

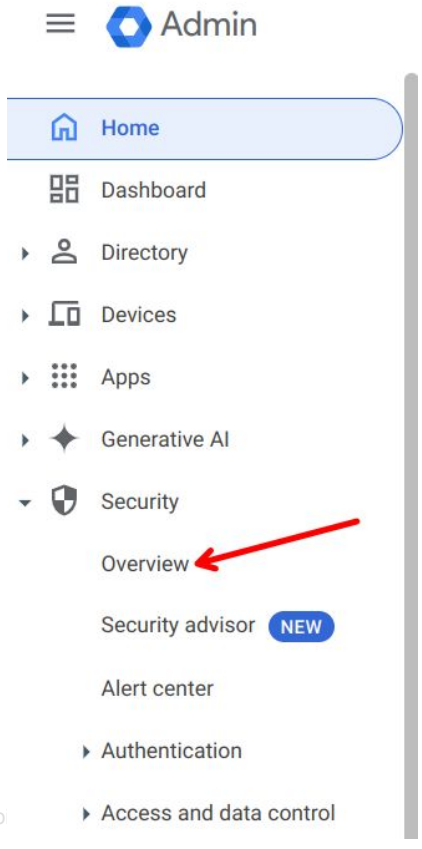
yubico

# Administrators

© 2025 Yubico

# How to enable YubiKeys as an Admin

1. Log into https://admin.google.com/ as a Google Workspace Administrator
2. Expand **Security** on the left side
3. Select **Overview**



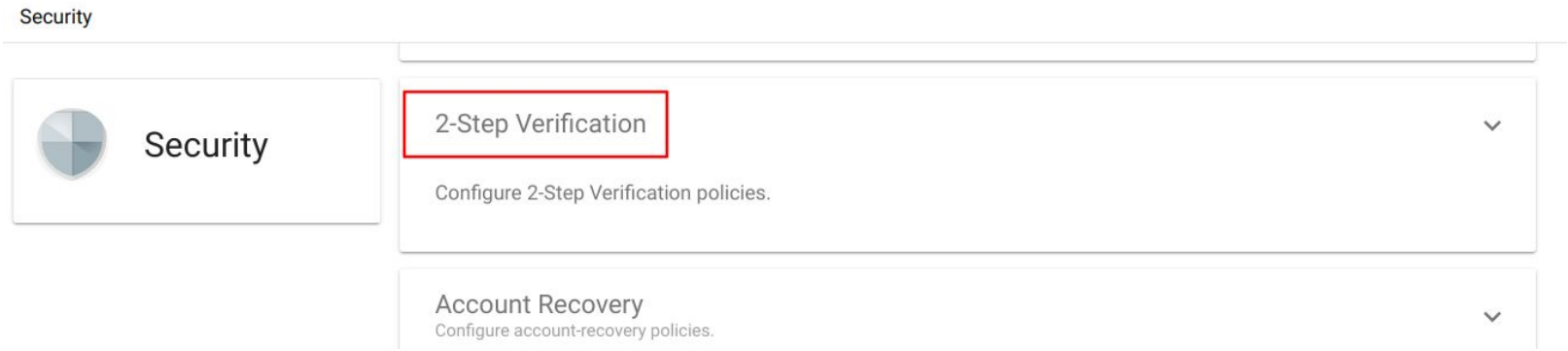

© 2025 Yubico

This document is the exclusive property of Yub

yubico

# How to enable YubiKeys as an Admin (cont.)

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

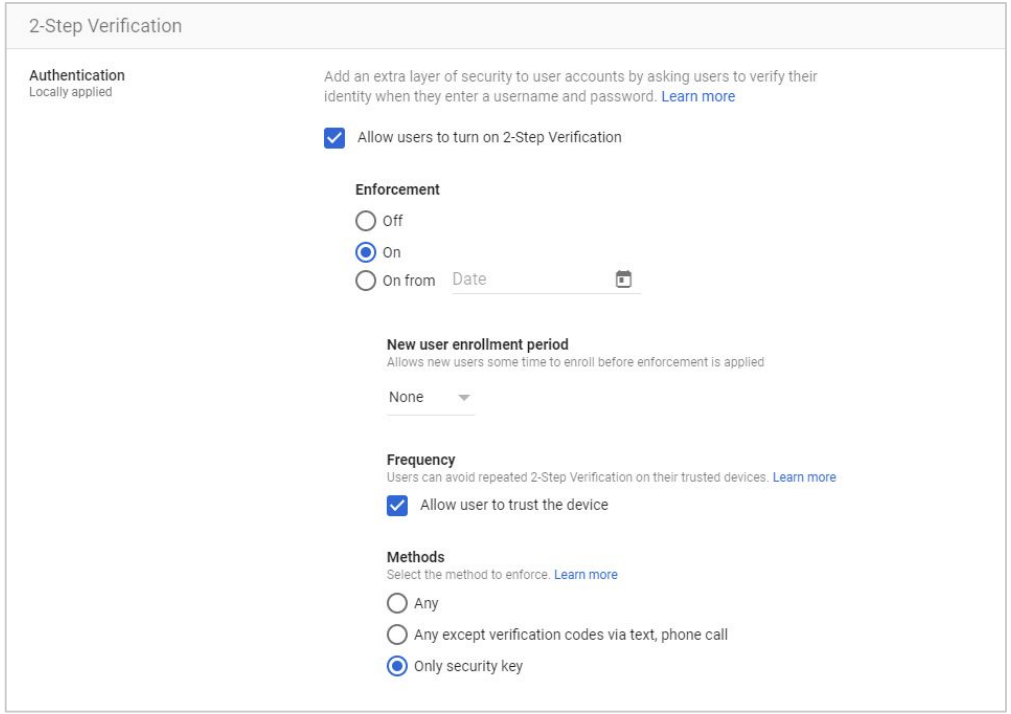



© 2025 Yubico

This document is the exclusive property of Yubico

# How to enable YubiKeys as an Admin (cont.)

4. Choose and enable the approved Methods



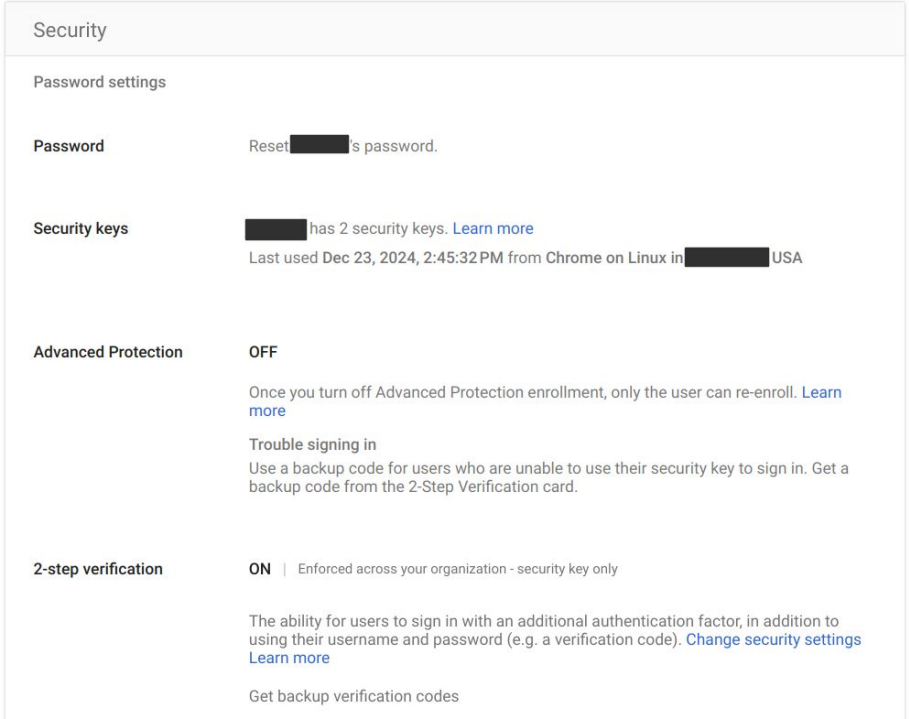

© 2025 Yubico

This document is the exclusive property of Yubico

# Manage a user's security settings

## Open user security settings

1. In your Google Admin console (at admin.google.com)
2. Expand **Directory** on the left side
3. Select **Users**
4. Scroll in the Users list, find the user
   Tip: To find a user, you can also type the user's name or email address in the search box at the top of your Admin console. If you need help, see Find a user account
5. Click the user's name to open their account page
6. Click the **Security** tab




© 2025 Yubico

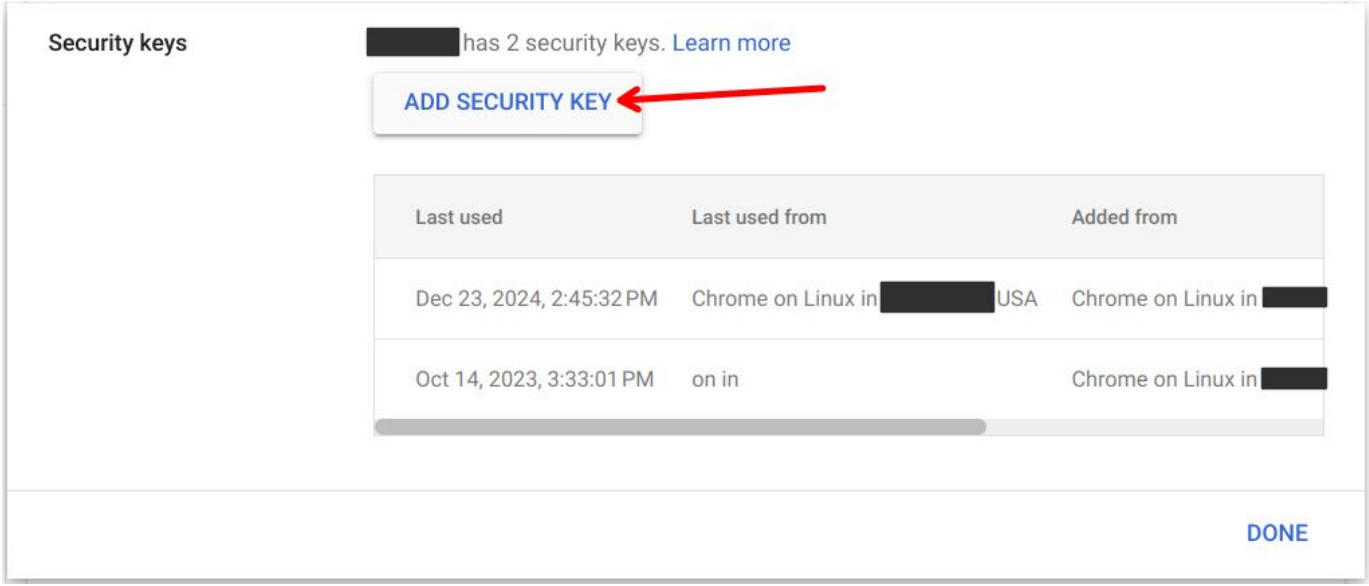
This document is the exclusive property of Yubico

# View and add a YubiKey

Admins can add a YubiKey for a user, or the user can add their own YubiKey.

To add a key for a user:

1. Click on **Security keys** to display the add button
2. Click **Add Security Key**



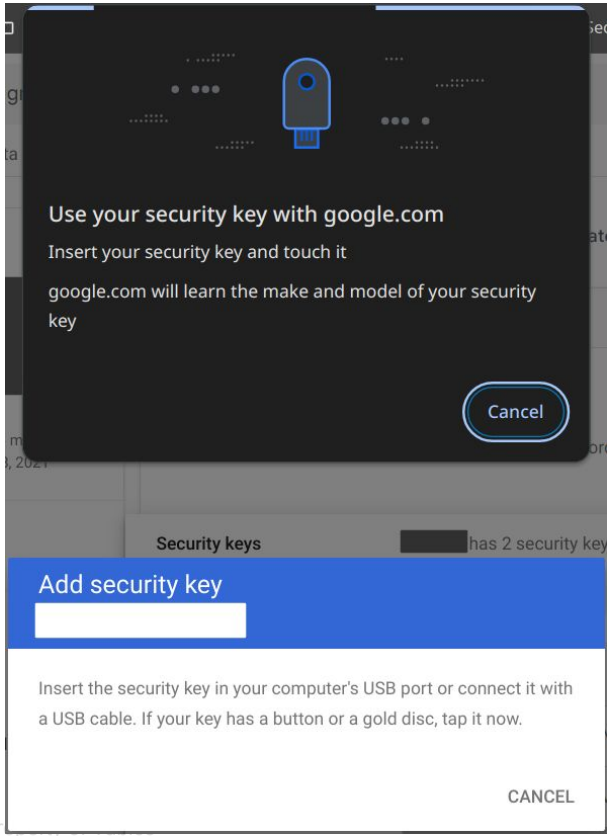

© 2025 Yubico

yubico

# View and add a YubiKey (cont.)

3. Follow the on-screen instructions
4. You will be prompted to insert the key, then tap the capacitive sensor

**Note**: Users can add their own keys by following the instructions in Add a security key to your Google Account.




© 2025 Yubico

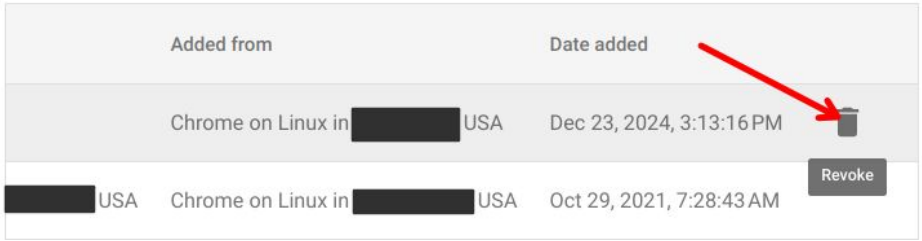
This document is the exclusive pr

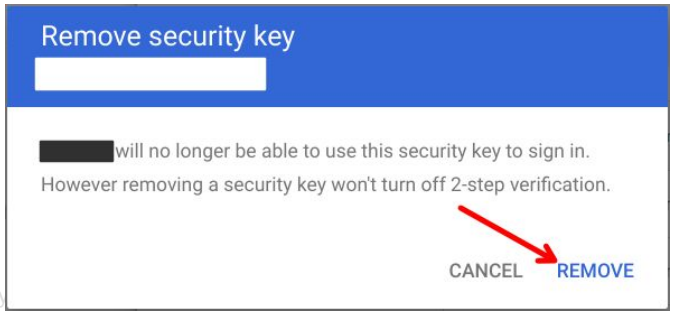
# Remove a YubiKey

A YubiKey should only be removed from a user's account when it is lost. If the YubiKey is temporarily unavailable, an Admin can generate backup security codes as a temporary workaround. See Get backup verification codes for a user below.

To remove a YubiKey from a user's account:

1. Click on **Security keys** to display the key information table.
2. Scroll the table all the way to the right.
3. Hover over the table line for the key you want to remove and select the **Revoke** icon
4. A new window will pop up, click **Remove**

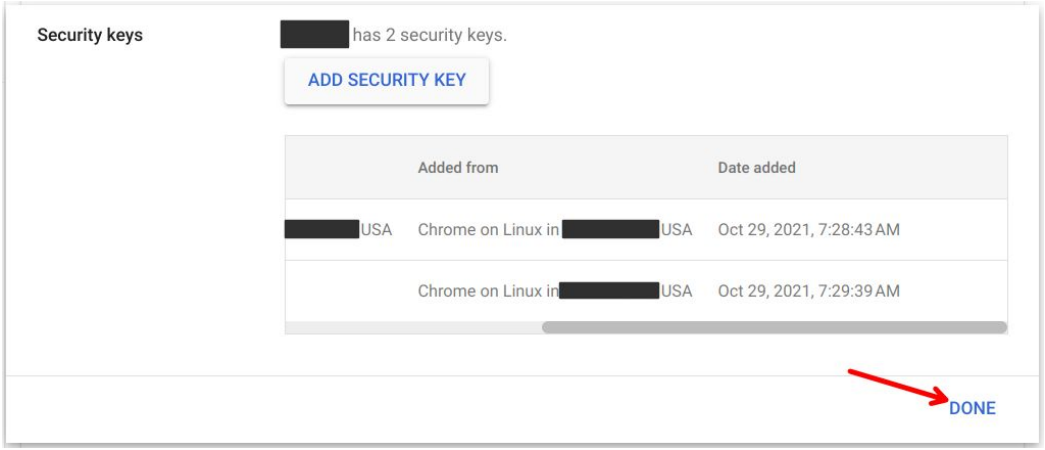



© 2025 Yubico
This document is the exclusive property
yubico

# Remove a YubiKey (cont.)

5. Click **Done**




**Note**: The Admin audit log adds an entry each time you revoke a security key.

| Date ↓ | Event | Description | Actor |
|---|---|---|---|
| 2024-12-23T15:17:55-07:00 | Security Key Revoke | A security key enrolled for user [redacted] | [redacted] |

© 2025 Yubico

This document is the exclusive property of Yubico

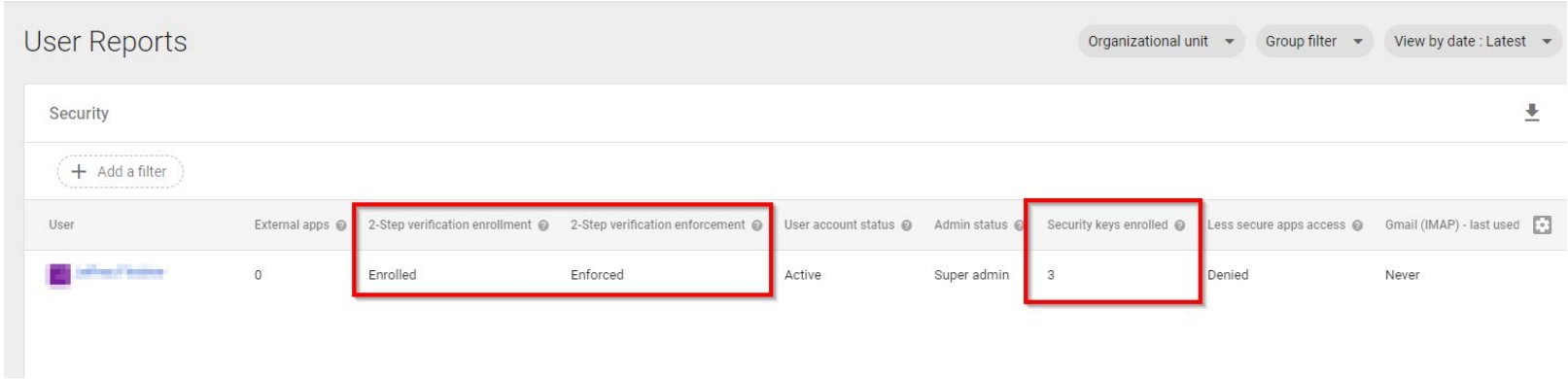
yubico

# User Reporting

Admins can access data on their users and their 2-Step Verification status in Reporting

**Note:** The default lag time for these reports is 1 - 3 days [per Google]

**Reporting > User Reports > Security**

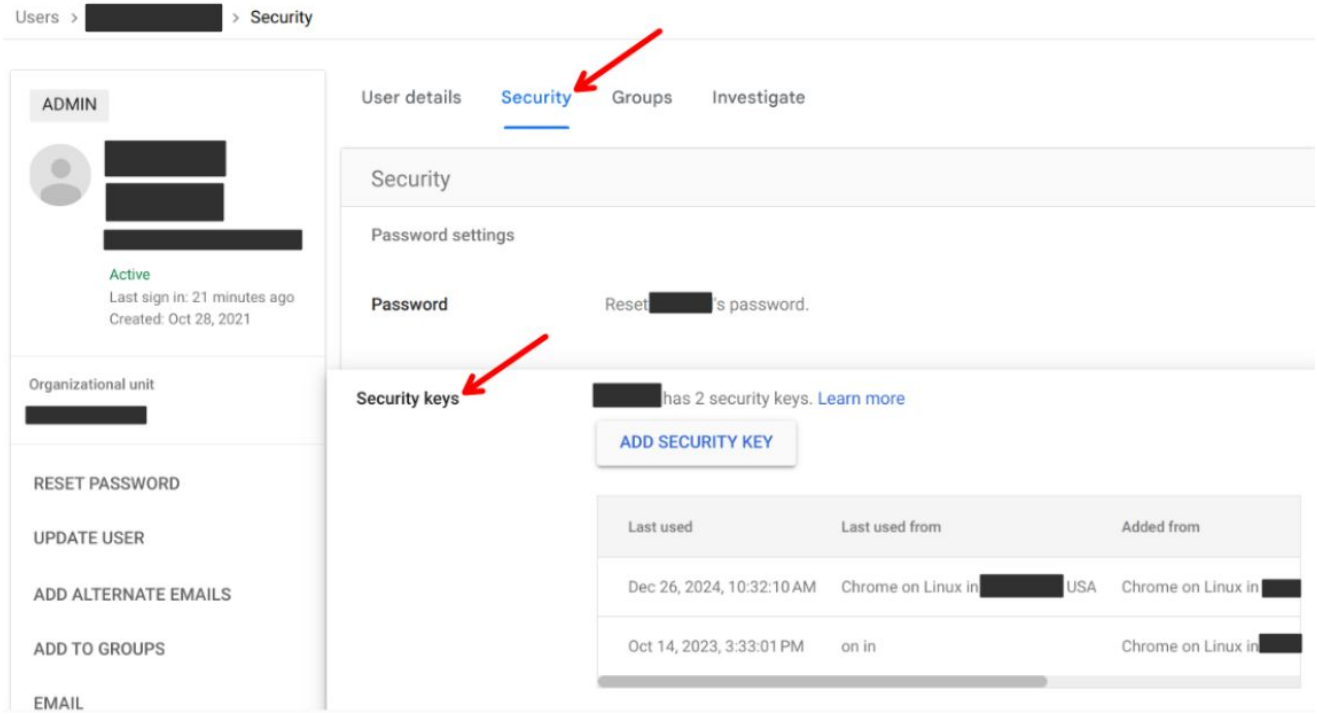



© 2025 Yubico

This document is the exclusive property of Yubico

# User Reporting (cont.)

Once an Admin clicks on the user name, he/she can access data on their YubiKeys by clicking on **Security > Security keys**




© 2025 Yubico

yubico

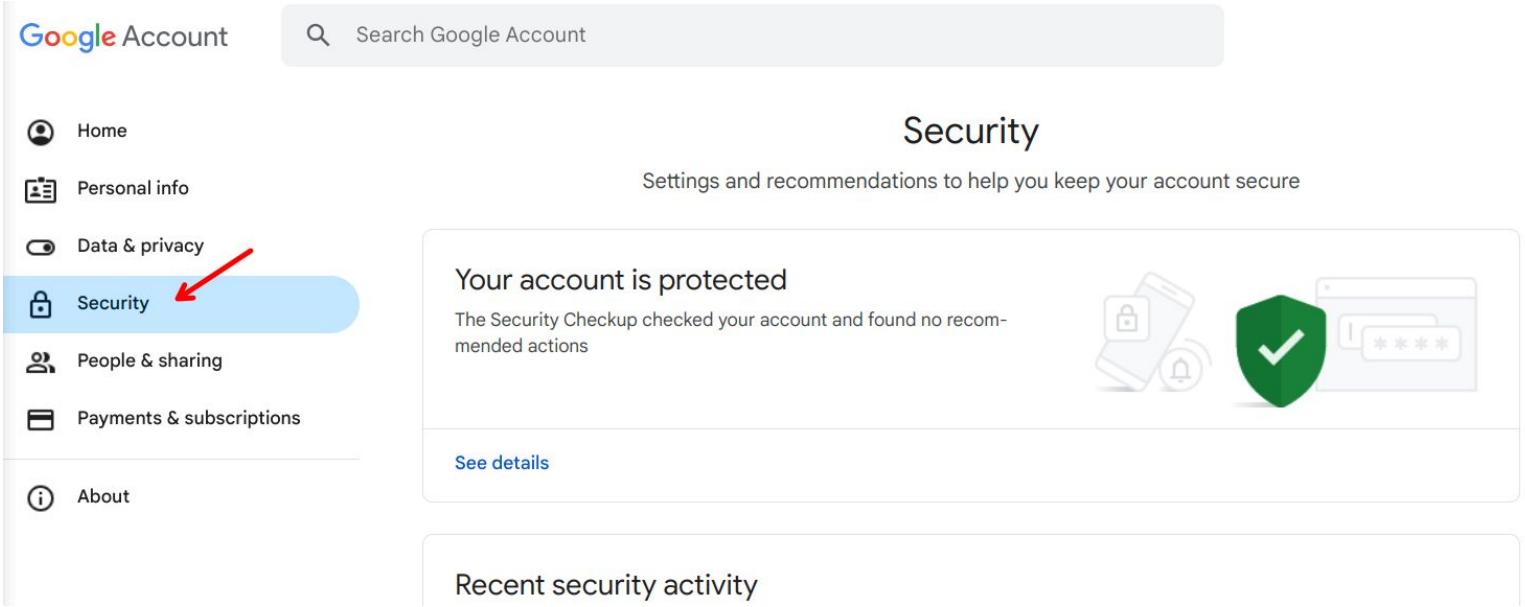
# Users

© 2025 Yubico

yubico

# Enrolling your YubiKey

1. Open a compatible browser like Chrome, FireFox, Edge, or Safari
2. Navigate to myaccount.google.com
3. Click on **Security** in the far left panel

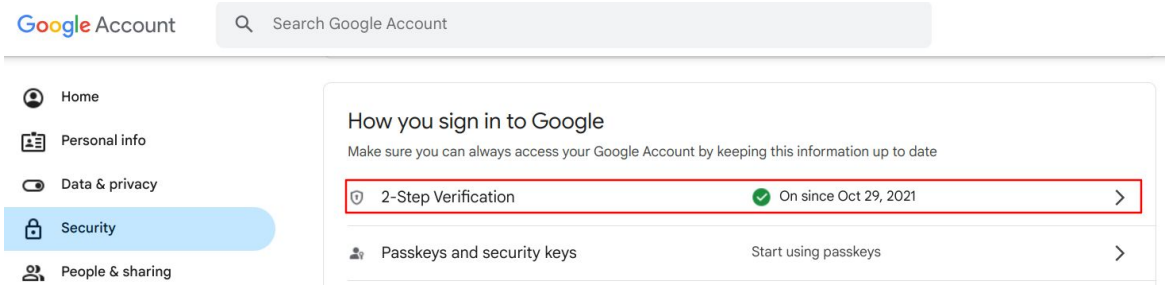



© 2025 Yubico

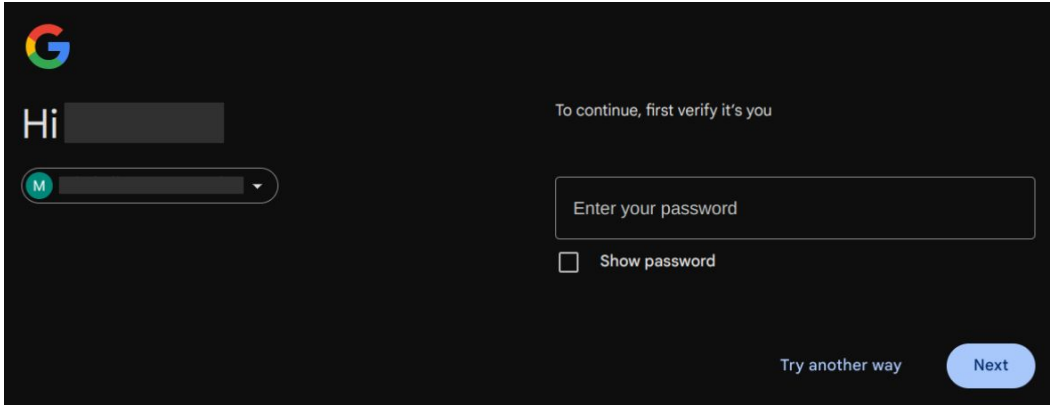
This document is the exclusive property of Yubico

# Enrolling your YubiKey (cont.)

4. Scroll down to **How you sign in to Google** and click on **2-step verification**




5. You may be prompted to sign in again to verify your identity

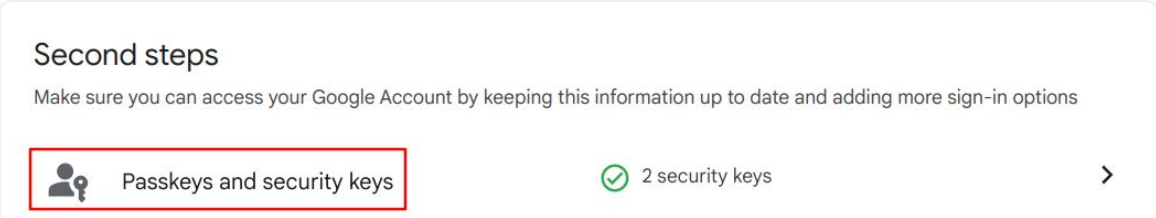



© 2025 Yubico

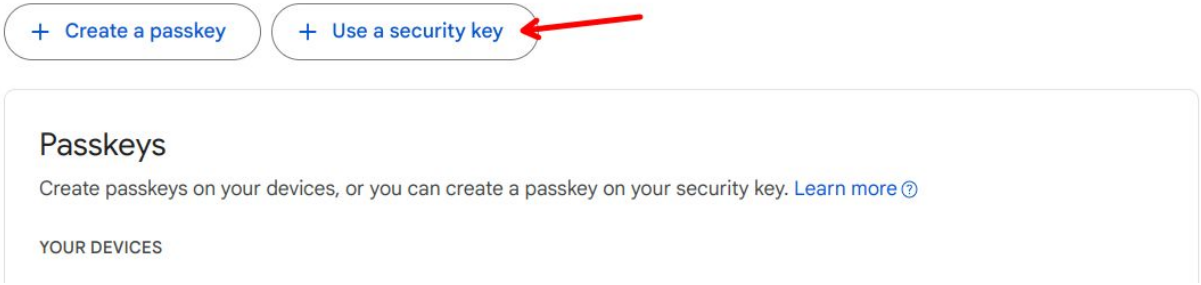
yubico

# Enrolling your YubiKey (cont.)

6. Select **Passkeys and security keys**




7. Click **+ Use a security key**

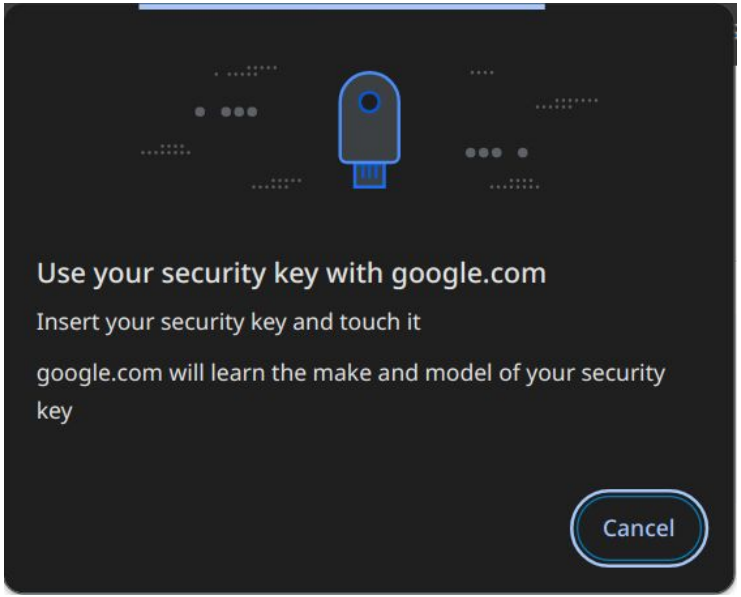



© 2025 Yubico

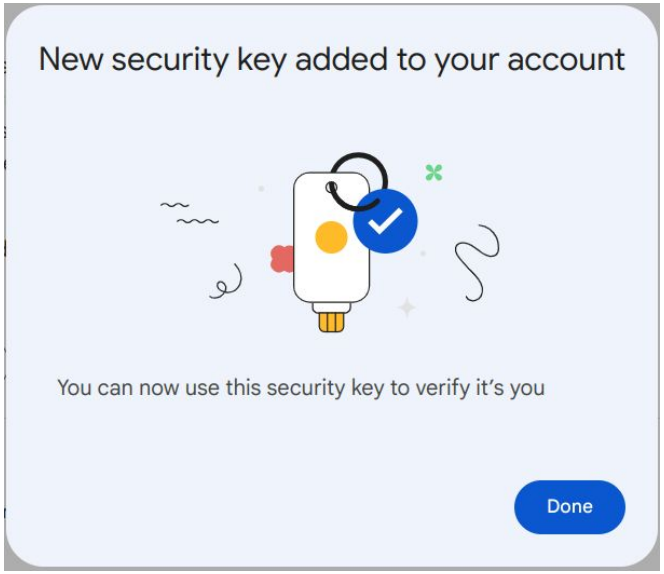
This document is the exclusive property of Yubico

# Enrolling your YubiKey (cont.)

5. You will be prompted to insert your YubiKey and touch the capacitive sensor to register it




6. Click **Done**

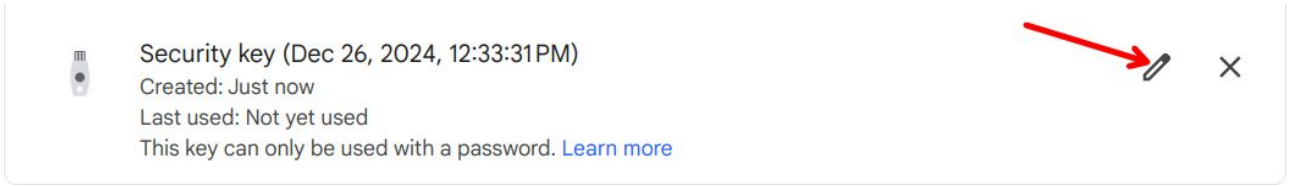



© 2025 Yubico

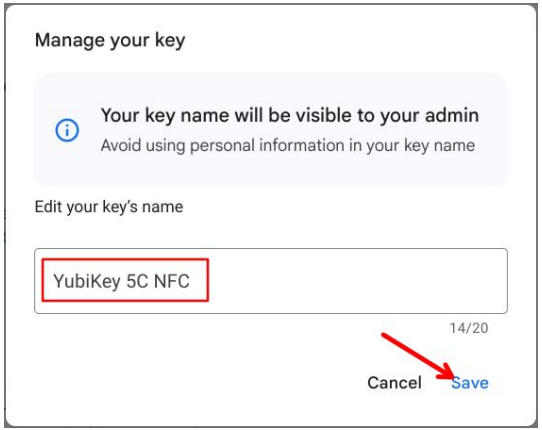
This document is the exclusive property of Yubico

# Enrolling your YubiKey (cont.)

7. To name your YubiKey, select the edit pencil next to the newly registered security key




8. Enter a name, then select **Save**

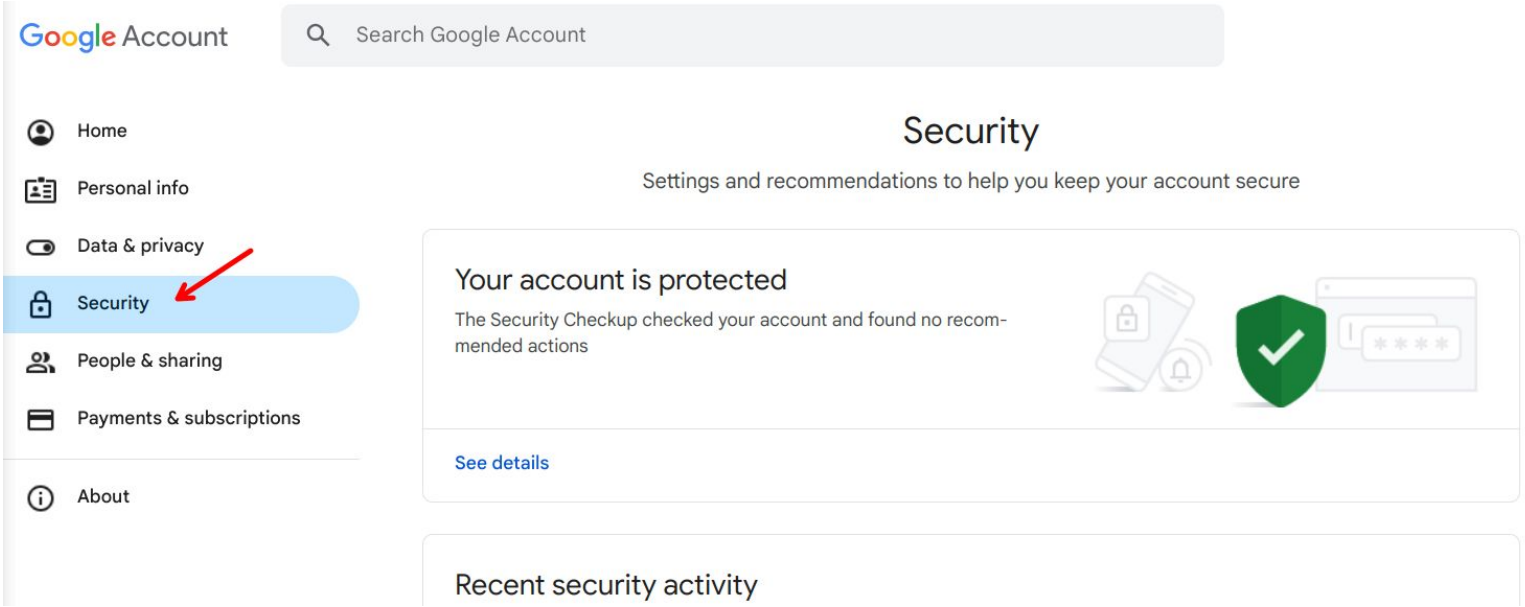



© 2025 Yubico

This document is the exclusive property of Yubico

# Viewing your enrolled YubiKeys

1. Open a compatible browser like Chrome, FireFox, Edge, or Safari
2. Navigate to myaccount.google.com
3. Click on **Security** in the far left panel

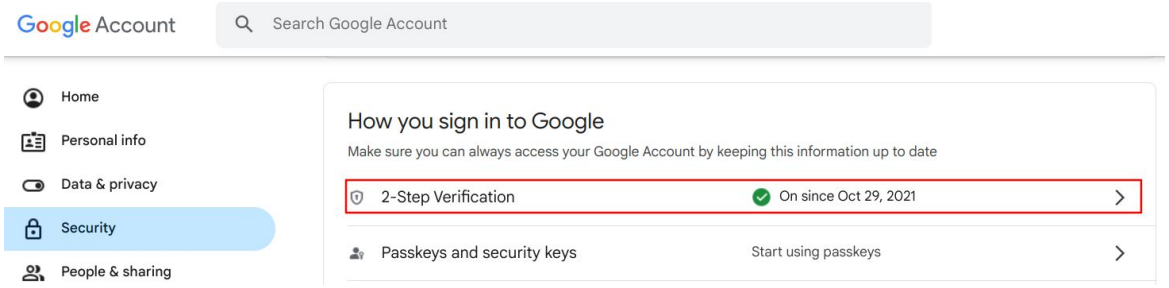



© 2025 Yubico

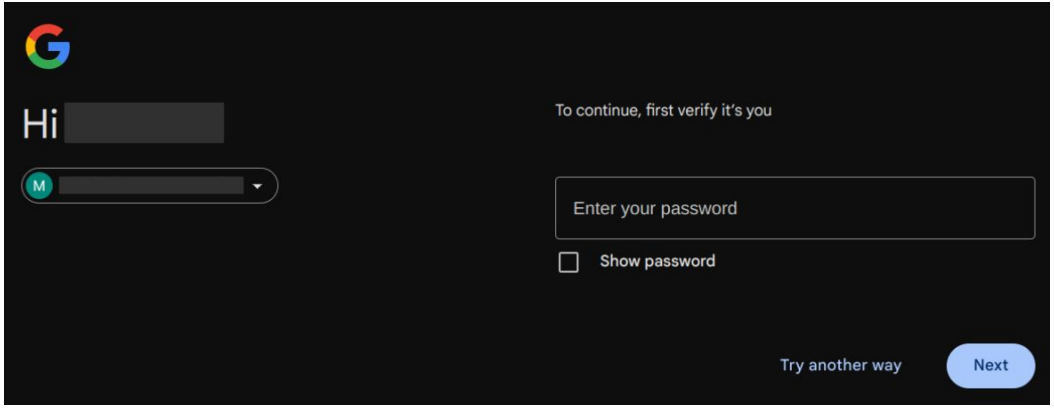
This document is the exclusive property of Yubico

# Viewing your enrolled YubiKeys (cont.)

4. Scroll down to **How you sign in to Google** and click on **2-step verification**




5. You may be prompted to sign in again to verify your identity

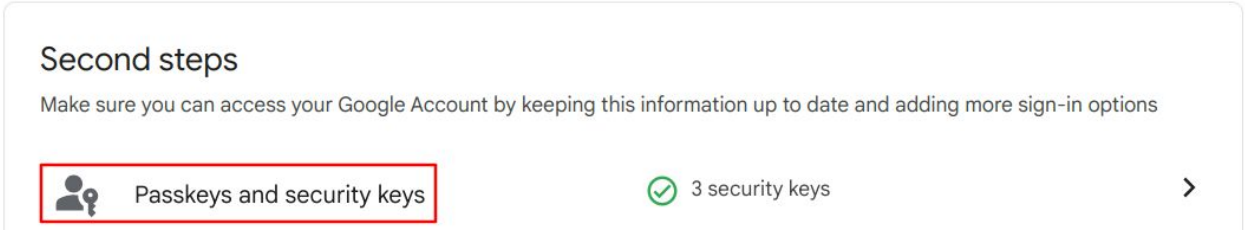



© 2025 Yubico

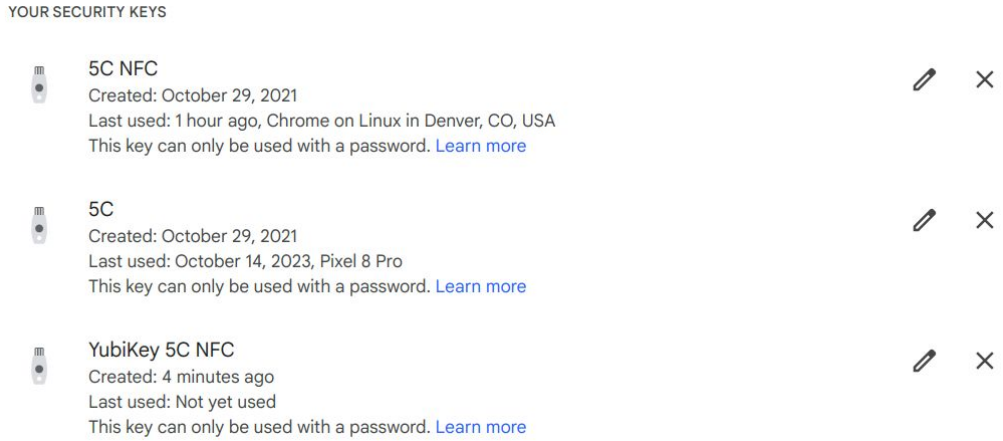
yubico

# Viewing your enrolled YubiKeys (cont.)

6. Select **Passkeys and security keys**




7. Scroll down to **Your Security Keys**



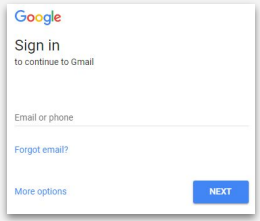

© 2025 Yubico

# Signing in with your YubiKey

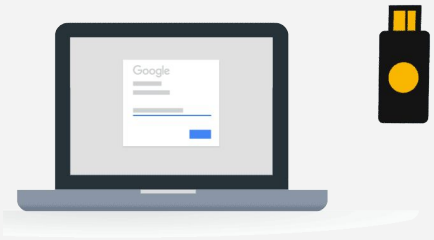
## Computer

If you have Security keys set up as second step in logging in, it’s easy to do:

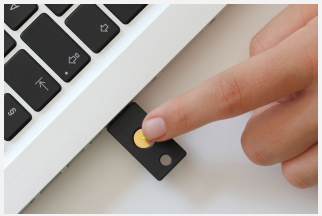
**1 Enter pw or PIN**




**2 Insert key**




**3 Touch key**



© 2025 Yubico

This document is the exclusive property of Yubico

# Signing in with your YubiKey

## Mobile devices

**Android**

1 Enter pw or PIN

2 Tap or insert key

**IOS**

1 Enter pw or PIN

2 Tap or insert key

© 2025 Yubico

This document is the exclusive property of Yubico

yubico

# What’s Next?

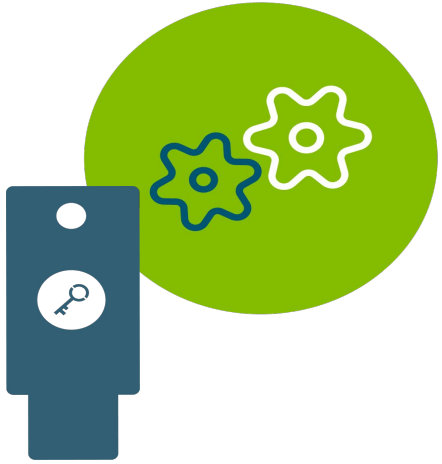
© 2025 Yubico

# Deployment Best Practices Workshop

## Planning for the operational aspects of a YubiKey deployment

**The workshop will cover…**

- Project readiness & planning
- Distributing YubiKeys
- Preparing and training end users
- YubiKey lifecycle management
- Successful user communications
- Customer deployment stories
- Available resources and materials



© 2025 Yubico

This document is the exclusive property of Yubico

# YubiKey Deployment Office Hours

Join us for open sessions to answer your questions, troubleshoot, provide consultation and discuss YubiKeys

| Tuesdays at 1 PM | Fridays at 10 AM |
| --- | --- |
| Join Microsoft Teams Meeting | Join Microsoft Teams Meeting |
| ID: 243436492249 | ID: 215605564804 |
| Passcode: mQ6KU3ZC | Passcode: wi6CL3Ln |

© 2025 Yubico

This document is the exclusive property of Yubico

# Professional Services Hours

## Features

### On-demand consulting

Provides technical and operational guidance when you need it

### Flexible hours

Not tied to a specific engagement timeline.  Hours can be used over 12 month period

### Multiple methods of assistance

Can be used to schedule virtual meetings or email with PS engineers and advisors

## How to communicate with Professional Services

1. Open a support case online (**https://yubi.co/support**). This is the preferred contact method for most scenarios as your support case will be logged for future reference
2. Email us at **professional-services@yubico.com**

© 2025 Yubico

This document is the exclusive property of Yubico

# Questions and Wrap-Up

© 2025 Yubico

yubico

# Questions

© 2025 Yubico

This document is the exclusive property of Yubico

© 2025 Yubico