

yubico

Securing Google Workspace with YubiKeys

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

Yubico's Professional Services Team

Deployment Advisors



Molly Babcock



Laura Eppley



Jeff Olives

Engineers



Greg Whitney



Dante Melo



Mitchell Armenta



Kanchan Thakur



Scott Truger

What is a YubiKey?

Technical Overview

Easy, Fast, & Reliable Authentication

YubiKey does not require a battery or network connection.



Waterproof



Crush Resistant

yubico

Concepts and Use Cases

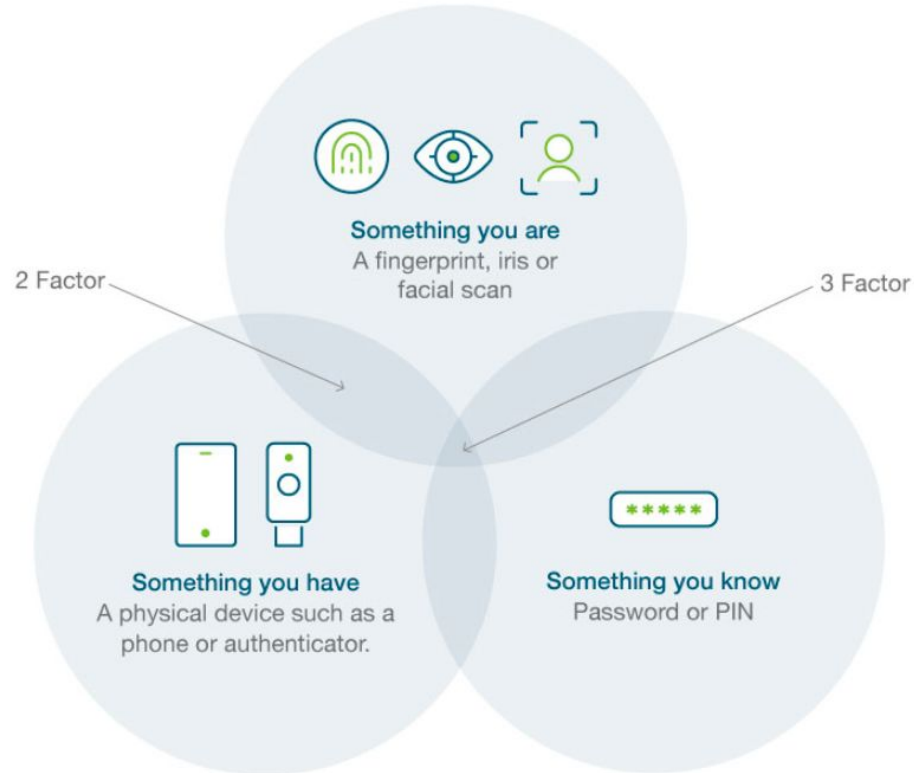
What is an Authentication Factor?

- 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

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)

Authentication Factors



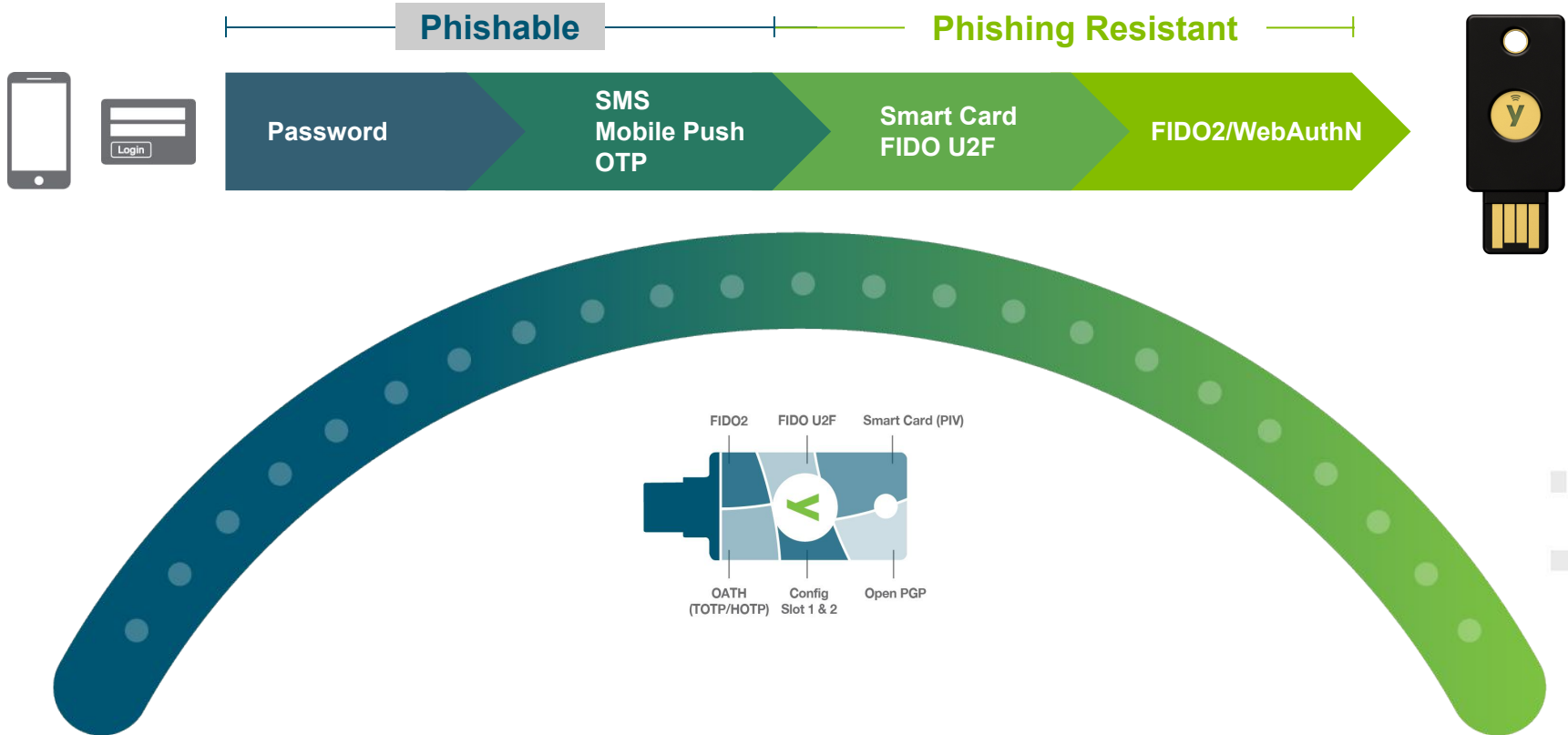
What is Phishing?

- 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.)

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

Phishing-Resistant MFA Illustrated



yubico

Google Workspace MFA Methods

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	✗

Source: [Protect Your Business with 2-Step Verification](#)

What is FIDO2?

- FIDO stands for **F**ast **I**Dentity **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?](#)

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

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

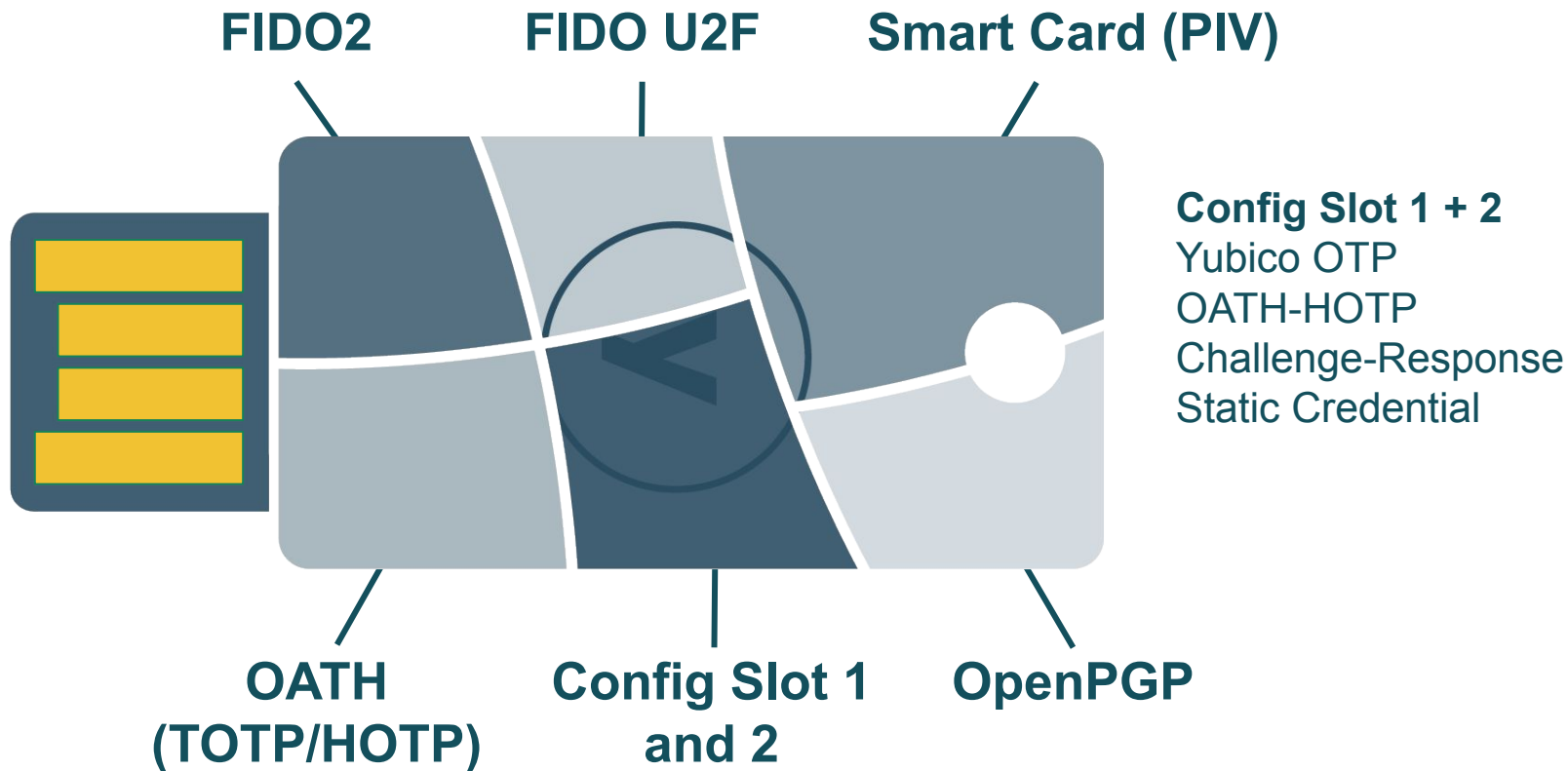
YubiKey 101

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

YubiKey Multiple Protocol Support



yubico

YubiKey interfaces

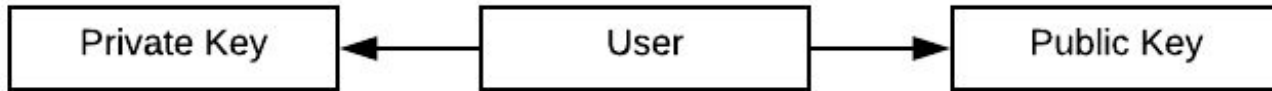
- **The YubiKey is a hardware device**
- **The physical interfaces are USB and NFC**
- **The USB interface provides 3 types of channels:**
 - **The OTP interface presents itself to the operating system as a USB keyboard**
 - **The FIDO interface presents itself as a generic human interface device (HID)**
 - **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)**

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**

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



Authentication Progression

1960s

Passwords

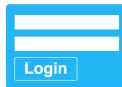


2004

Tokens & Smart Cards

2014

FIDO U2F



2018

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

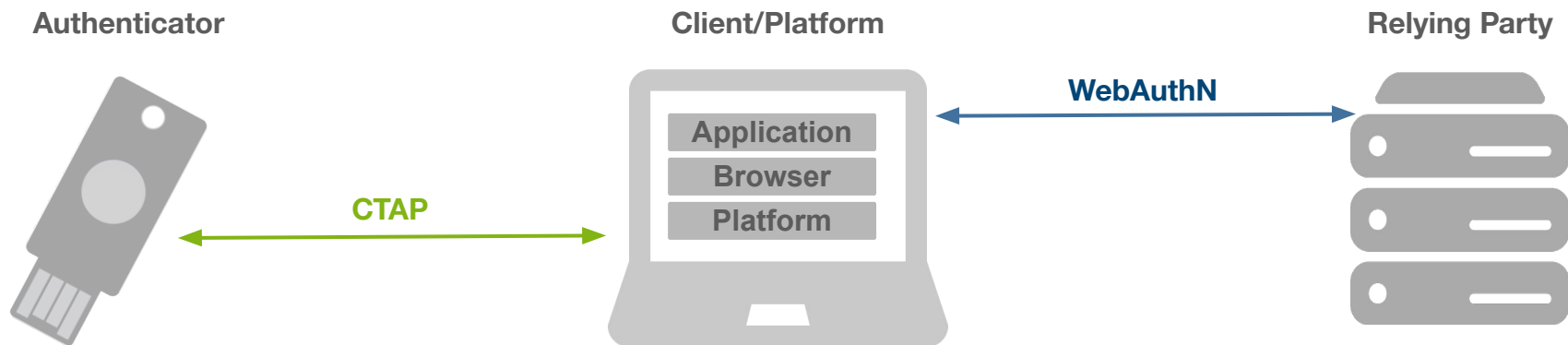
yubico
Microsoft Google

yubico

FIDO2 Summary

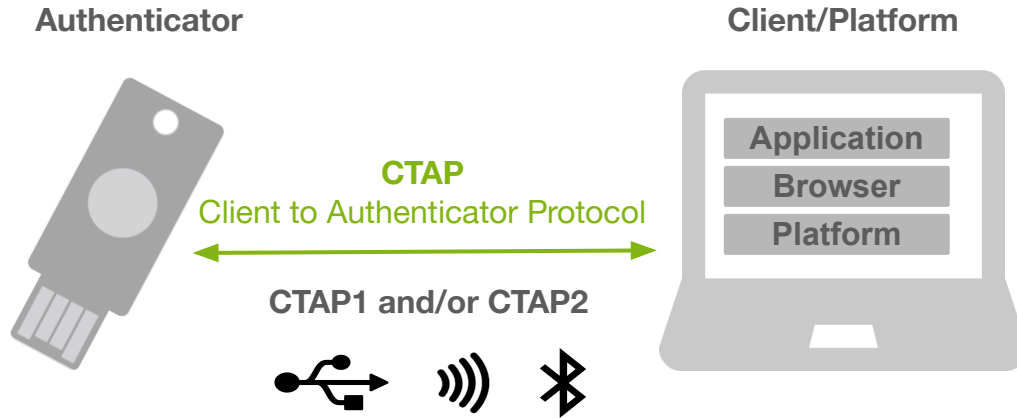
- Allows login securely without a password
 - Strong layered security multi-factor authentication
 - Strong defense against phishing and Man in the Middle(MitM) attacks
 - High usability with rapid login
- Built into widely adopted platforms (e.g. Windows) and on track for standardization via W3C, with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

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

What is CTAP?



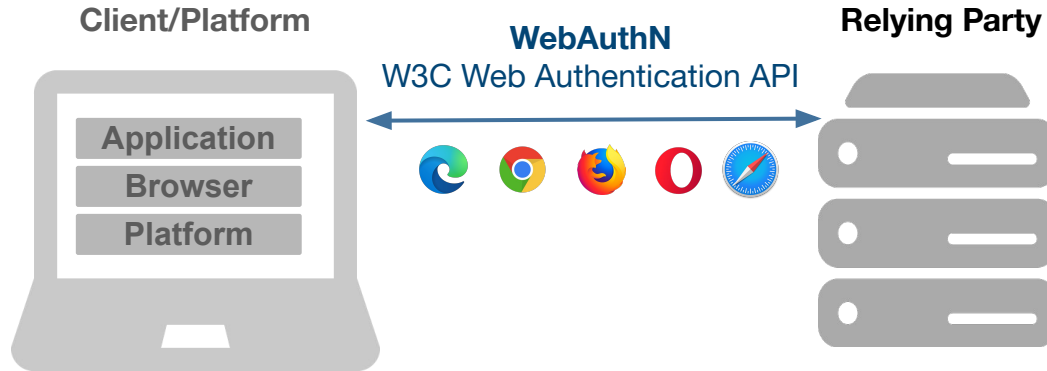
Application layer protocol used to communicate between an external authenticator (i.e. security key) and a client (desktop) or a platform (OS)

Authenticator generates and securely stores credentials

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

Communicates over USB, NFC, and Bluetooth

What is WebAuthn?



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

Strongly authenticate users

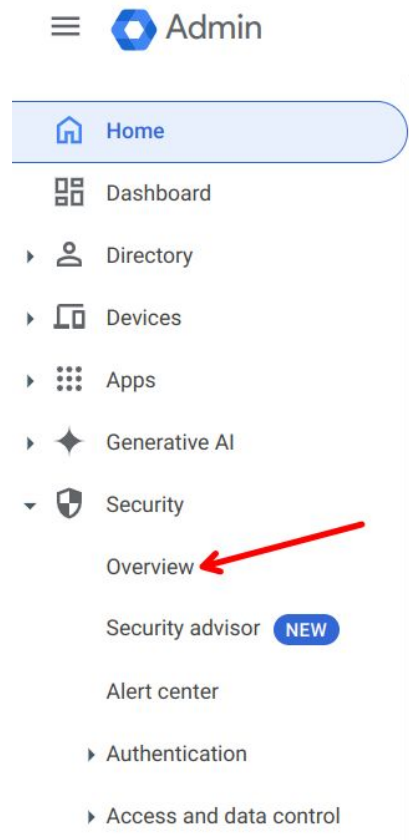
Major browsers are on track to implement full Web Authentication APIs

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

Administrators

How to enable YubiKeys as an Admin

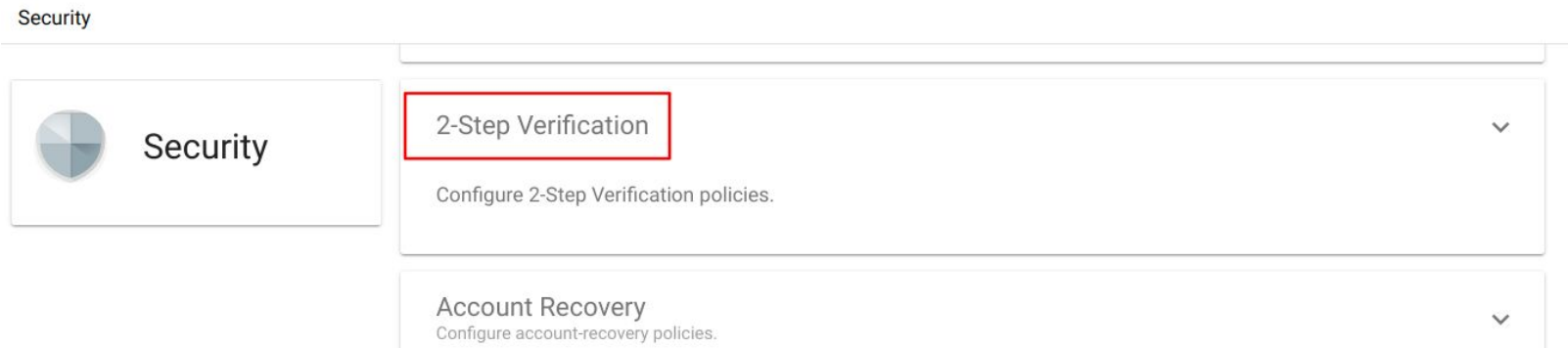
1. Log into <https://admin.google.com/> as a Google Workspace Administrator
2. Expand **Security** on the left side
3. Select **Overview**






How to enable YubiKeys as an Admin (cont.)

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

Security



The screenshot shows a sidebar with a 'Security' icon and label. The main content area has a scrollable list of security options. The '2-Step Verification' option is highlighted with a red rectangular border. Below it is the 'Account Recovery' option. Both options include a description and a downward-pointing chevron icon.

 Security	2-Step Verification  Configure 2-Step Verification policies.
	Account Recovery  Configure account-recovery policies.

How to enable YubiKeys as an Admin (cont.)

4. Choose and enable the approved Methods

2-Step Verification

Authentication
Locally applied


Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. [Learn more](#)

Allow users to turn on 2-Step Verification

Enforcement

Off

On

On from 

New user enrollment period
Allows new users some time to enroll before enforcement is applied

None ▾

Frequency
Users can avoid repeated 2-Step Verification on their trusted devices. [Learn more](#)

Allow user to trust the device

Methods
Select the method to enforce. [Learn more](#)

Any

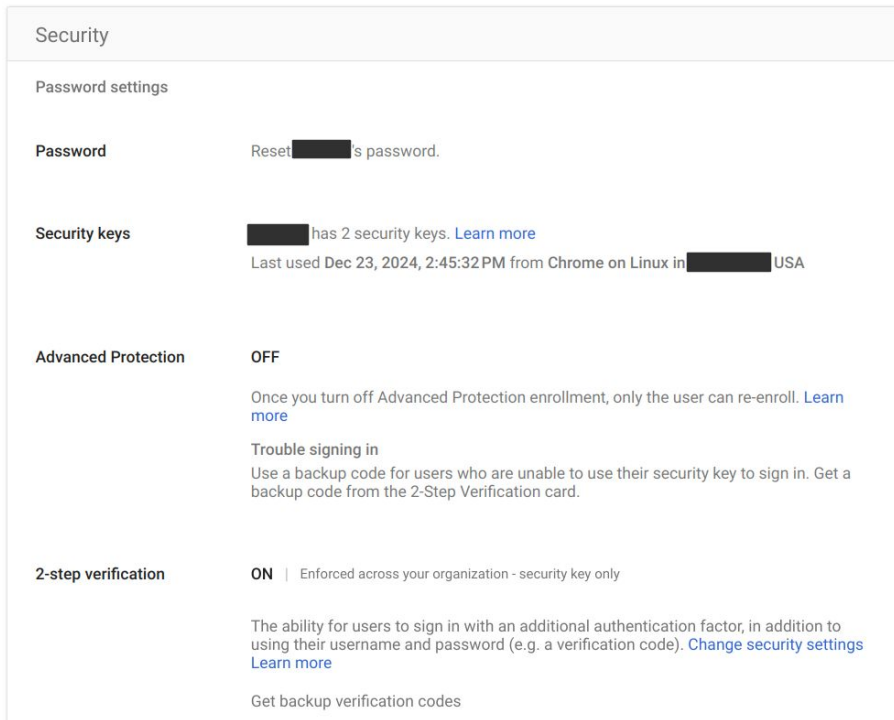
Any except verification codes via text, phone call

Only security key

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



The screenshot shows the 'Security' settings page for a user in the Google Admin console. The page is organized into sections: Password settings, Security keys, Advanced Protection, and 2-step verification. The 'Password' section shows a 'Reset' button. The 'Security keys' section indicates the user has 2 security keys and shows the last used key details. The 'Advanced Protection' section is currently 'OFF'. The '2-step verification' section is 'ON' and enforced across the organization.

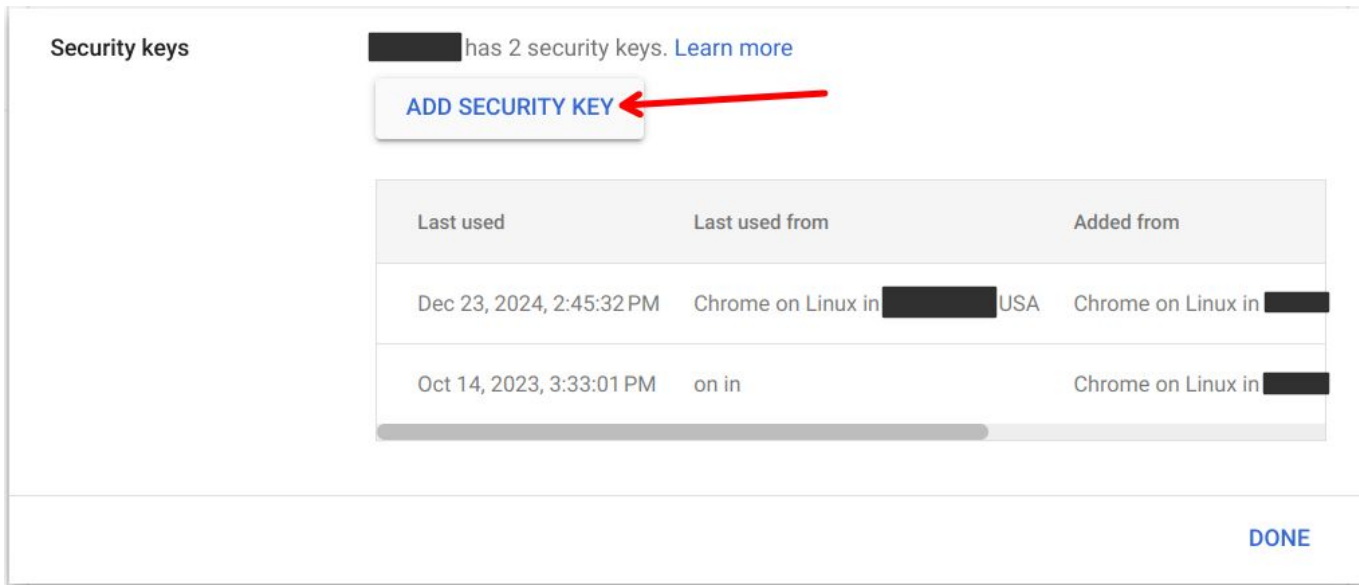
Security	
Password settings	
Password	Reset [redacted]'s password.
Security keys	[redacted] has 2 security keys. Learn more Last used Dec 23, 2024, 2:45:32 PM from Chrome on Linux in [redacted] USA
Advanced Protection	OFF Once you turn off Advanced Protection enrollment, only the user can re-enroll. Learn more Trouble signing in Use a backup code for users who are unable to use their security key to sign in. Get a backup code from the 2-Step Verification card.
2-step verification	ON Enforced across your organization - security key only The ability for users to sign in with an additional authentication factor, in addition to using their username and password (e.g. a verification code). Change security settings Learn more Get backup verification codes

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**



Security keys

██████ has 2 security keys. [Learn more](#)

ADD SECURITY KEY

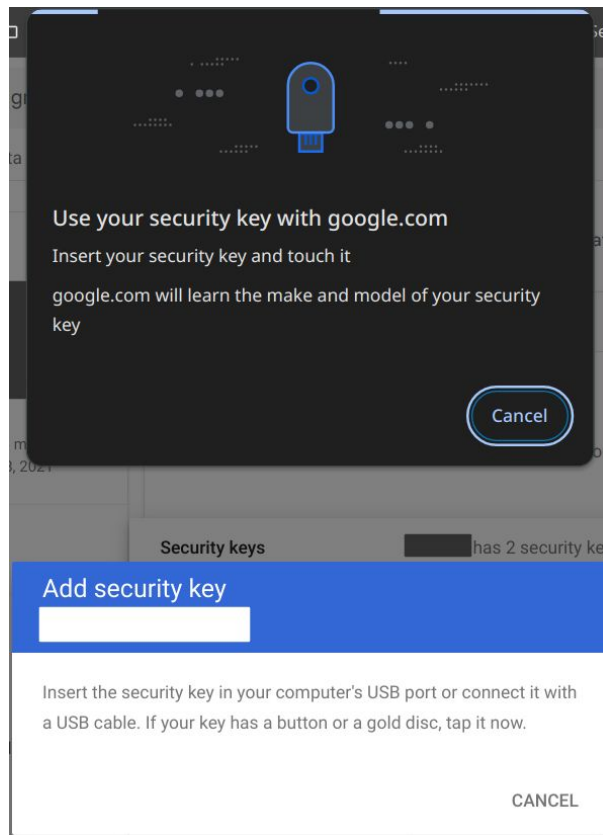
Last used	Last used from	Added from
Dec 23, 2024, 2:45:32 PM	Chrome on Linux in ██████ USA	Chrome on Linux in ██████
Oct 14, 2023, 3:33:01 PM	on in	Chrome on Linux in ██████

DONE

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](#).




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**

Added from	Date added	
Chrome on Linux in [redacted] USA	Dec 23, 2024, 3:13:16 PM	
[redacted] USA	Chrome on Linux in [redacted] USA	Oct 29, 2021, 7:28:43 AM

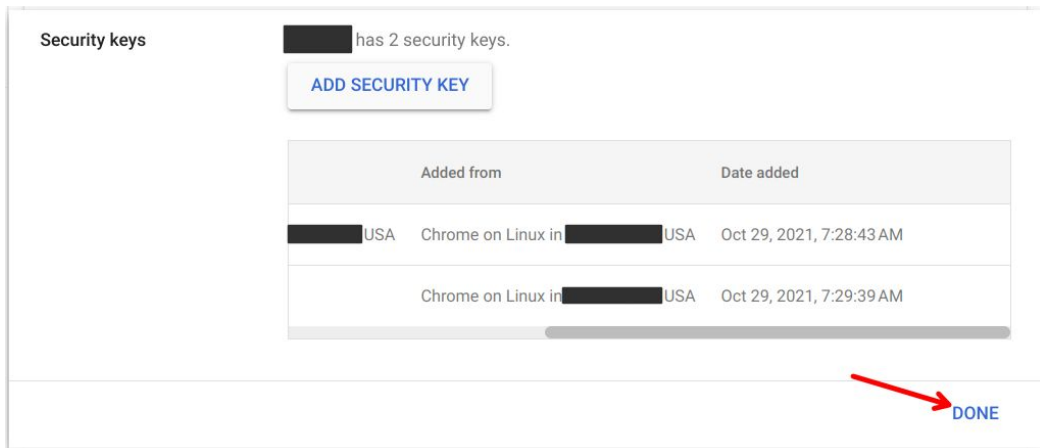
Remove security key

[redacted] will no longer be able to use this security key to sign in.
However removing a security key won't turn off 2-step verification.

[CANCEL](#) [REMOVE](#)

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	

User Reporting

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

Reporting > User Reports > Security

User Reports

Organizational unit Group filter View by date : Latest

Security

+ Add a filter

User	External apps	2-Step verification enrollment	2-Step verification enforcement	User account status	Admin status	Security keys enrolled	Less secure apps access	Gmail (IMAP) - last used
	0	Enrolled	Enforced	Active	Super admin	3	Denied	Never

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**

The screenshot shows the Microsoft Entra ID user management interface. The breadcrumb navigation is "Users > [redacted] > Security". The user profile on the left is for an "ADMIN" user, who is "Active" and last signed in 21 minutes ago. The "Security" tab is selected in the top navigation, and the "Security keys" section is highlighted with a red arrow. The "Security keys" section shows that the user has 2 security keys and includes an "ADD SECURITY KEY" button. A table below lists the security keys with columns for "Last used", "Last used from", and "Added from".

Users > [redacted] > Security

ADMIN

[redacted]

Active
Last sign in: 21 minutes ago
Created: Oct 28, 2021

Organizational unit
[redacted]

RESET PASSWORD

UPDATE USER

ADD ALTERNATE EMAILS

ADD TO GROUPS

EMAIL

User details **Security** Groups Investigate

Security

Password settings

Password Reset [redacted]'s password.

Security keys [redacted] has 2 security keys. [Learn more](#)

[ADD SECURITY KEY](#)

Last used	Last used from	Added from
Dec 26, 2024, 10:32:10 AM	Chrome on Linux in [redacted] USA	Chrome on Linux in [redacted]
Oct 14, 2023, 3:33:01 PM	on in	Chrome on Linux in [redacted]

Users

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

Google Account

Search Google Account

Home

Personal info

Data & privacy

Security

People & sharing

Payments & subscriptions

About

Security

Settings and recommendations to help you keep your account secure

Your account is protected

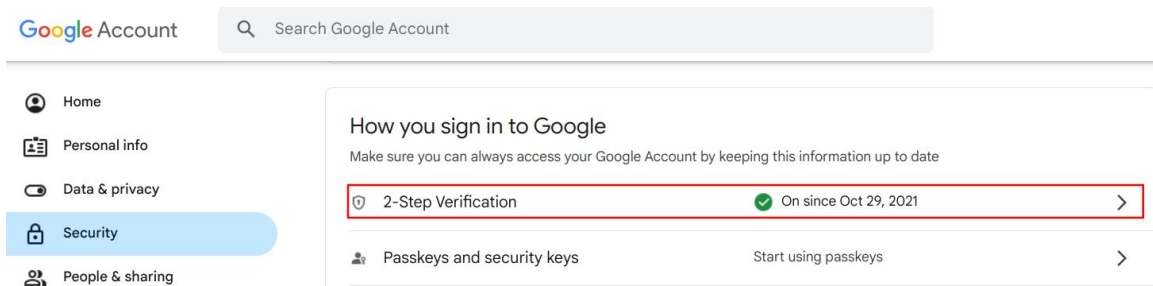
The Security Checkup checked your account and found no recommended actions

[See details](#)

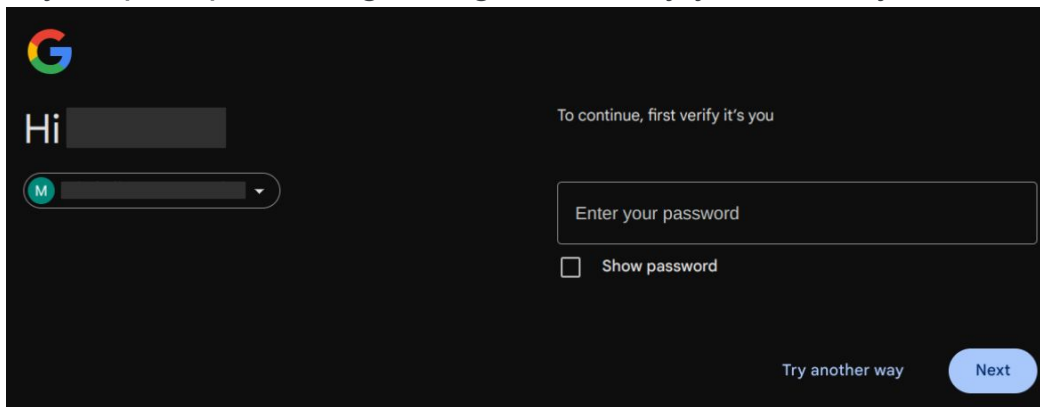
Recent security activity

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




Enrolling your YubiKey (cont.)

6. Select **Passkeys and security keys**

Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

 **Passkeys and security keys** ✓ 2 security keys >

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

+ Create a passkey + Use a security key

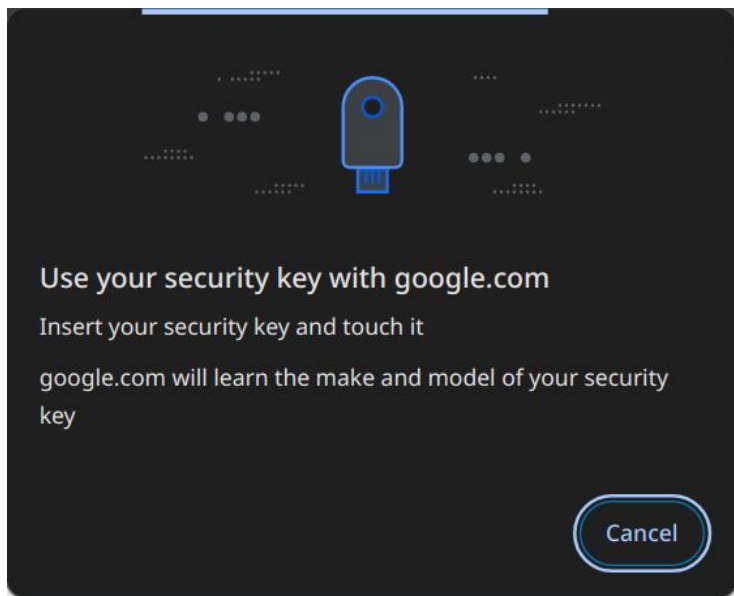
Passkeys

Create passkeys on your devices, or you can create a passkey on your security key. [Learn more](#) ⓘ

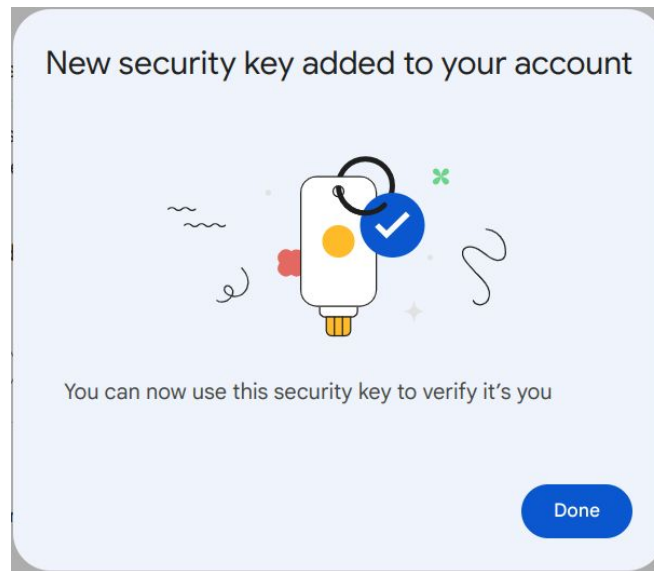
YOUR DEVICES

Enrolling your YubiKey (cont.)

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

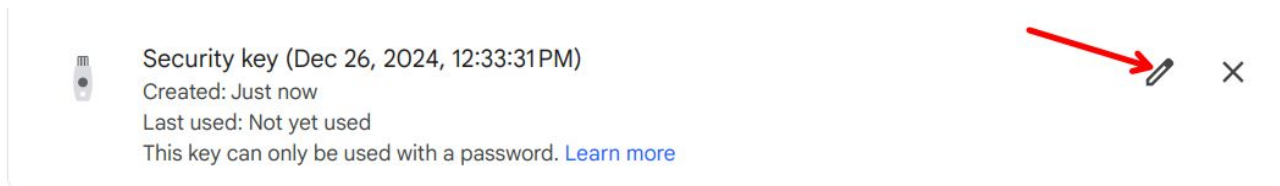


6. Click **Done**

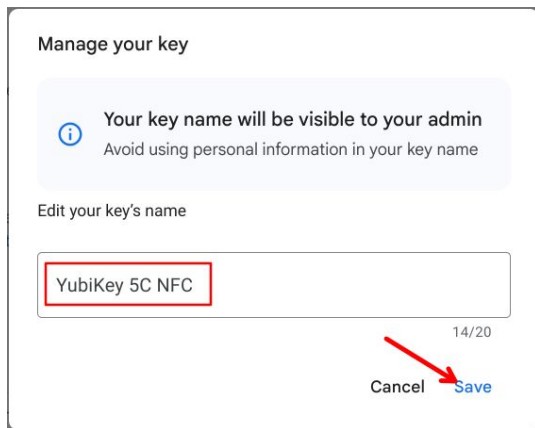


Enrolling your YubiKey (cont.)

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



- Enter a name, then select **Save**



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

Google Account

Search Google Account

Home

Personal info

Data & privacy

Security

People & sharing

Payments & subscriptions

About

Security

Settings and recommendations to help you keep your account secure

Your account is protected

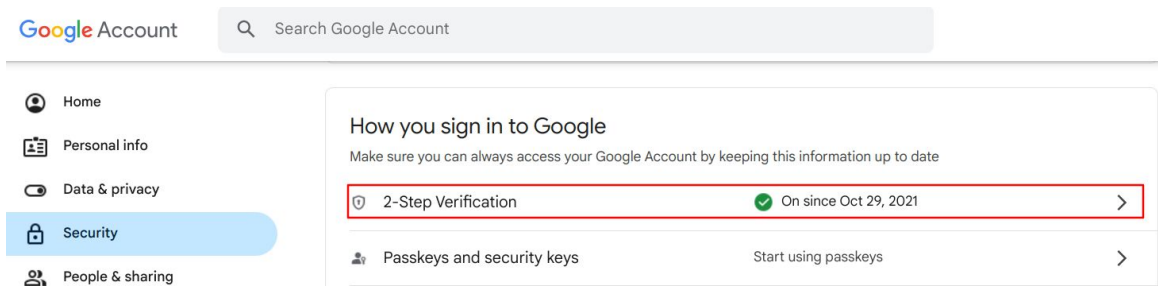
The Security Checkup checked your account and found no recommended actions

[See details](#)

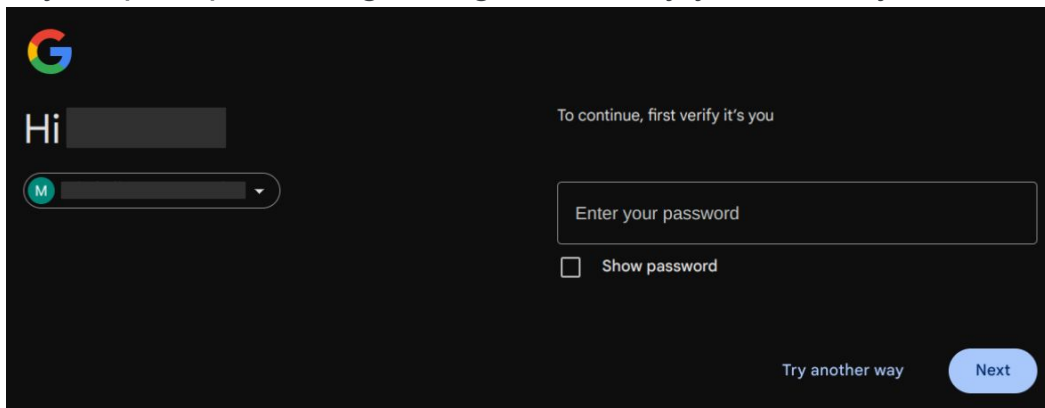
Recent security activity

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




Viewing your enrolled YubiKeys (cont.)

6. Select **Passkeys and security keys**










Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

 **Passkeys and security keys** 3 security keys >

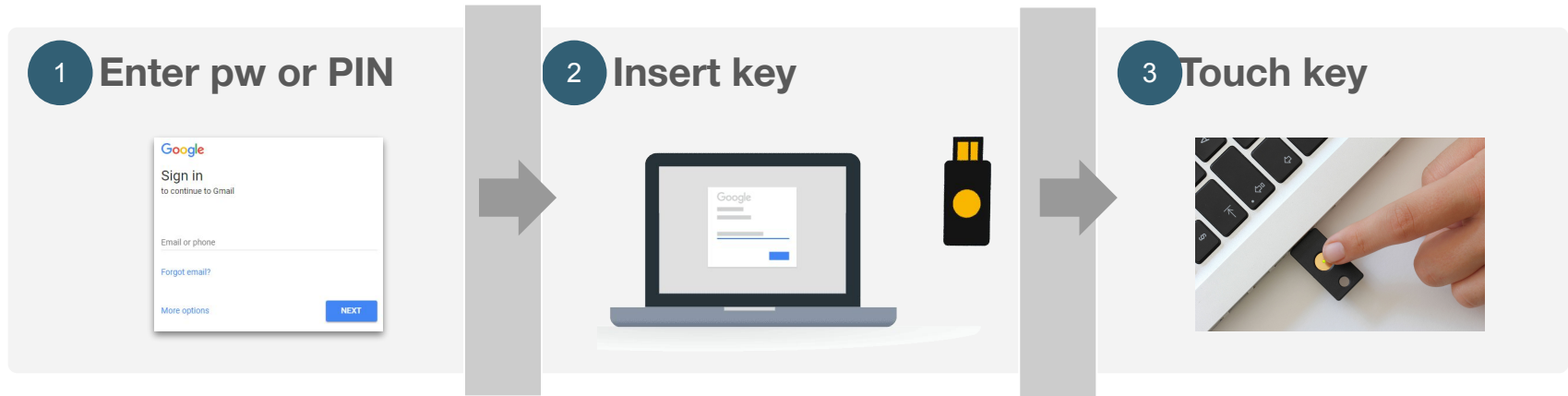
7. Scroll down to **Your Security Keys**

YOUR SECURITY KEYS

	5C NFC Created: October 29, 2021 Last used: 1 hour ago, Chrome on Linux in Denver, CO, USA This key can only be used with a password. Learn more	 
	5C Created: October 29, 2021 Last used: October 14, 2023, Pixel 8 Pro This key can only be used with a password. Learn more	 
	YubiKey 5C NFC Created: 4 minutes ago Last used: Not yet used This key can only be used with a password. Learn more	 

Signing in with your YubiKey Computer

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



Signing in with your YubiKey

Mobile devices

Android

1 Enter pw or PIN



2 Tap or insert key

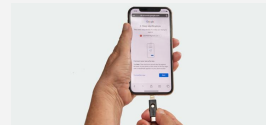


IOS

1 Enter pw or PIN



2 Tap or insert key



yubico

Redeeming PS Hours Post-Workshop

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 redeem PS Hours

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 enterprise@yubico.com

Questions and Wrap-Up

Questions



