



**Driving Modern Passwordless  
Authentication:**


**Citrix Workspace and Microsoft  
Azure Active Directory**



# Presenter:



## Jason Samuel




- Houston, TX
- Technical Solutions Management  
Security Architect, Alchemy Technology Group
- CTP
- Co-leader of the Houston CUGC
- Author of [jasonsamuel.com](http://jasonsamuel.com)
-  @\_JasonSamuel



# Why “Driving”?

**drive** [drahyv] [SHOW IPA](#) 

---

*verb (used with object), drove*  [drohv] or (*Archaic*) *drave*  [dreyv] , *driv·en*  [**driv-uhn**] , **driv·ing**.

- 1 to send, expel, or otherwise cause to move by force or compulsion:  
*to drive away the flies; to drive back an attacking army; to drive a person to desperation.*
- 2 to cause and guide the movement of (a vehicle, an animal, etc.):  
*to drive a car; to drive a mule.*

# Launch Control – your IT leadership controlling direction



# Shuttle on launchpad – a delivery mechanism we look after



# Astronauts - Citrix Engineers strapped in for the ride



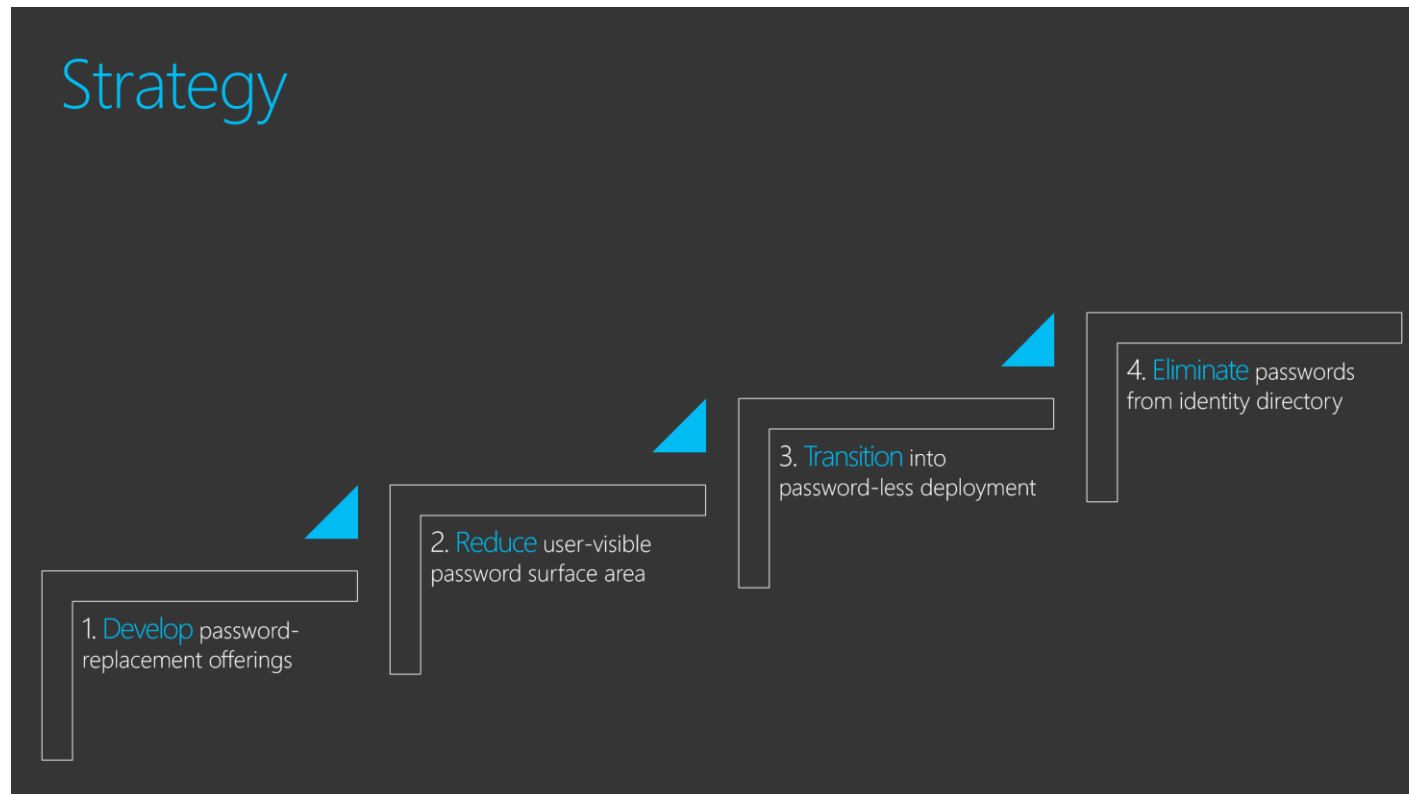
# Anyone feel like this some days?

- Body experiences 3 times the force of gravity
- 17,500 miles per hour
- For 8.5 minutes until orbit and main engine cutoff
- Think trying to breathe with a gorilla standing on your chest



# Passwordless Authentication Facts

- Passwordless authentication is not a fad. It is the now and the future.
- You will be asked to deploy it for your EUC environment at some point in the next few years.
- Your company may have already started down the path, and you don't know it.
- This is what Microsoft is telling your CISO right now:





# What passwords are today vs. what the business needs



# What your company's goal will be

- <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy>

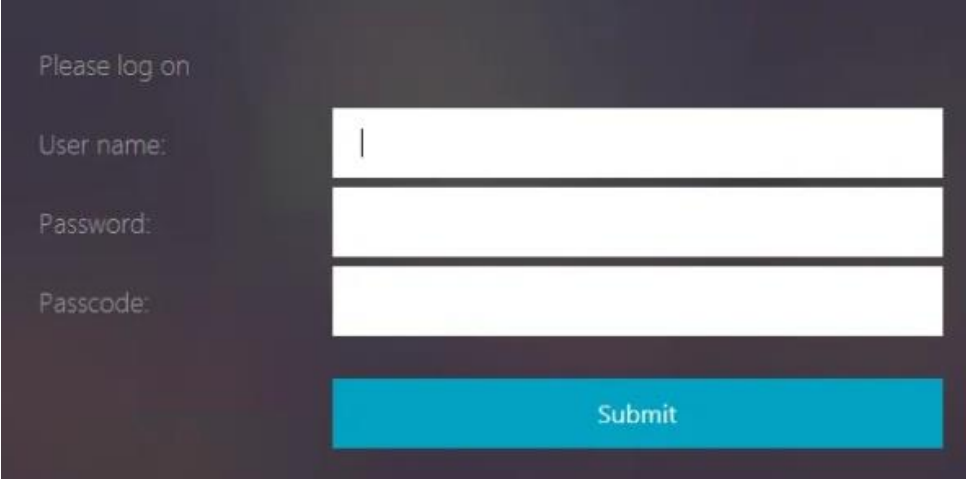
Once the user-visible password surface has been eliminated, your organization can begin to transition those users into a passwordless world. A world where:

- the users never type their password
- the users never change their password
- the users do not know their password

**Plus no more password lockouts  
and password resets!**

# Identity providers we've been told to use in the past with Citrix

- User ID + Password + MFA method as 2<sup>nd</sup> factor
  - Citrix ADC (NetScaler) + StoreFront
  - LDAP(S) bind straight to domain controllers
  - RADIUS, SAML , or OIDC to some backend server/service that often provides MFA capability (TOTP, push, SMS, phone call, security questions, etc.)
- Certificates (aka legacy passwordless authentication)
  - Citrix ADC (NetScaler) + StoreFront
  - x.509 client certificate deployed to endpoint computing device
  - x.509 client certificate on smart card or other external authenticator



Please log on

User name:

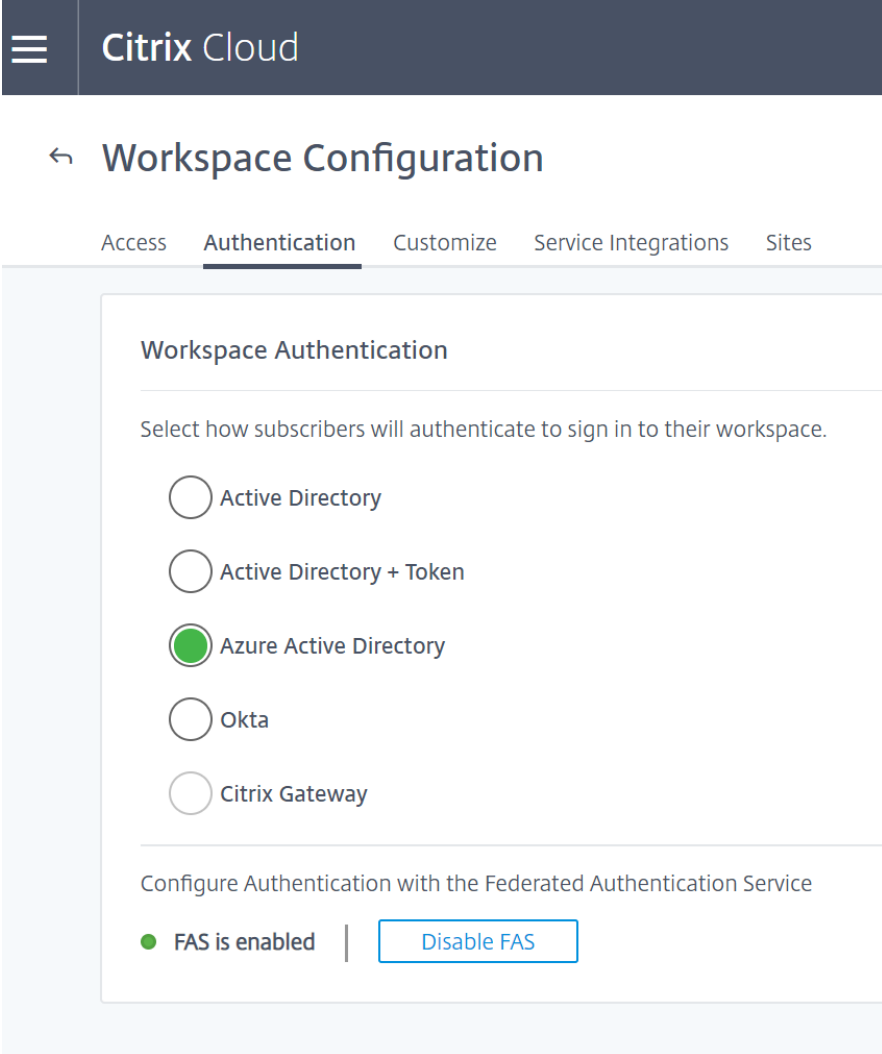
Password:

Passcode:

Submit

# What we can use with Citrix Workspace?

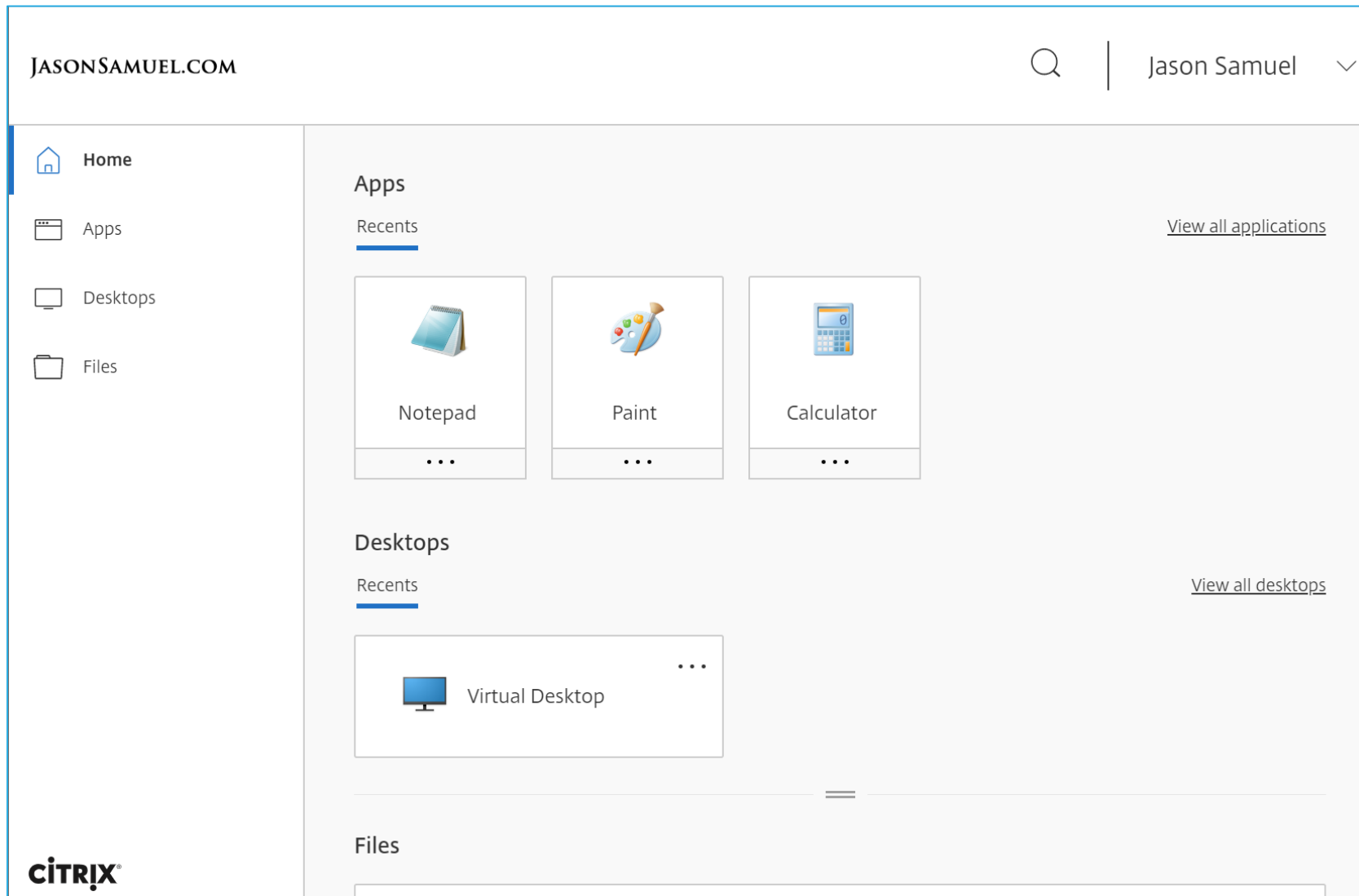
- Workspace + Gateway Service
  - AD password only
    - NO!!!!!!
  - AD password + Token
    - Free MFA from Citrix. Good for enterprises with no MFA solutions.
- Azure AD
  - Password + Azure MFA
  - Federation to whatever you like (like AD FS, Okta, Ping Federate, etc)
  - Modern password-less with Microsoft Authenticator
  - Modern password-less with FIDO2 hardware security key
- Okta (public tech preview)
- Citrix Gateway
  - Use your existing Citrix ADC (NetScaler) and any auth profiles created on it via an OAuth IDP Profile
  - So anything RADIUS, SAML, OAuth/OIDC can be used
- More options coming this year



The screenshot shows the Citrix Cloud interface for Workspace Configuration. The top navigation bar includes 'Citrix Cloud' and a hamburger menu. Below it, the 'Workspace Configuration' page is displayed with tabs for 'Access', 'Authentication', 'Customize', 'Service Integrations', and 'Sites'. The 'Authentication' tab is selected, showing 'Workspace Authentication' settings. The instruction reads: 'Select how subscribers will authenticate to sign in to their workspace.' There are five radio button options: 'Active Directory', 'Active Directory + Token', 'Azure Active Directory' (which is selected and highlighted with a green dot), 'Okta', and 'Citrix Gateway'. Below these options, there is a section for 'Configure Authentication with the Federated Authentication Service' (FAS), which shows 'FAS is enabled' with a green dot and a 'Disable FAS' button.

Oh, look! FAS is enabled! 😊

# Citrix Workspace (post-authentication)



# What if you're using on-prem Citrix VAD?

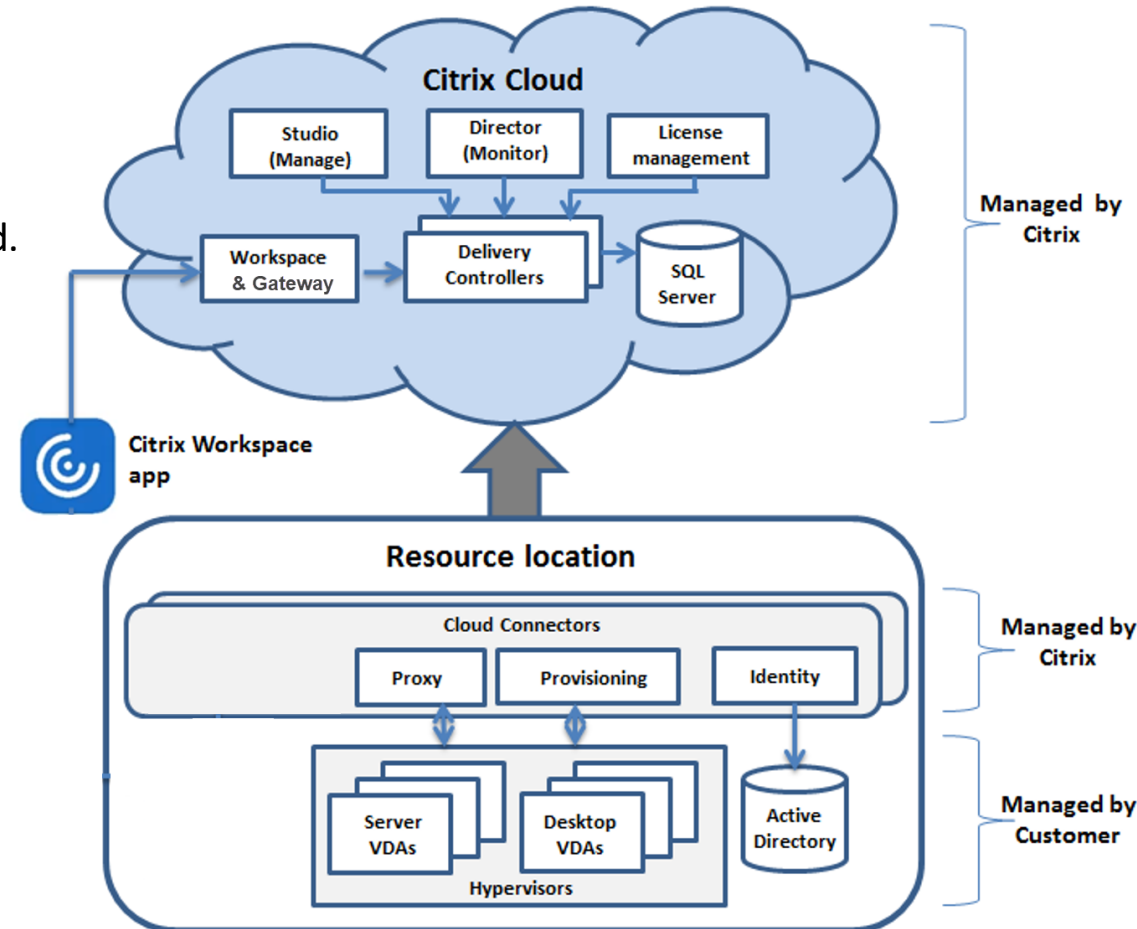
- Yes, Azure AD works with your on-prem Citrix ADC (NetScaler) and StoreFront just fine.
- Everything I will show you today with password-less auth works with on-prem CVAD too.



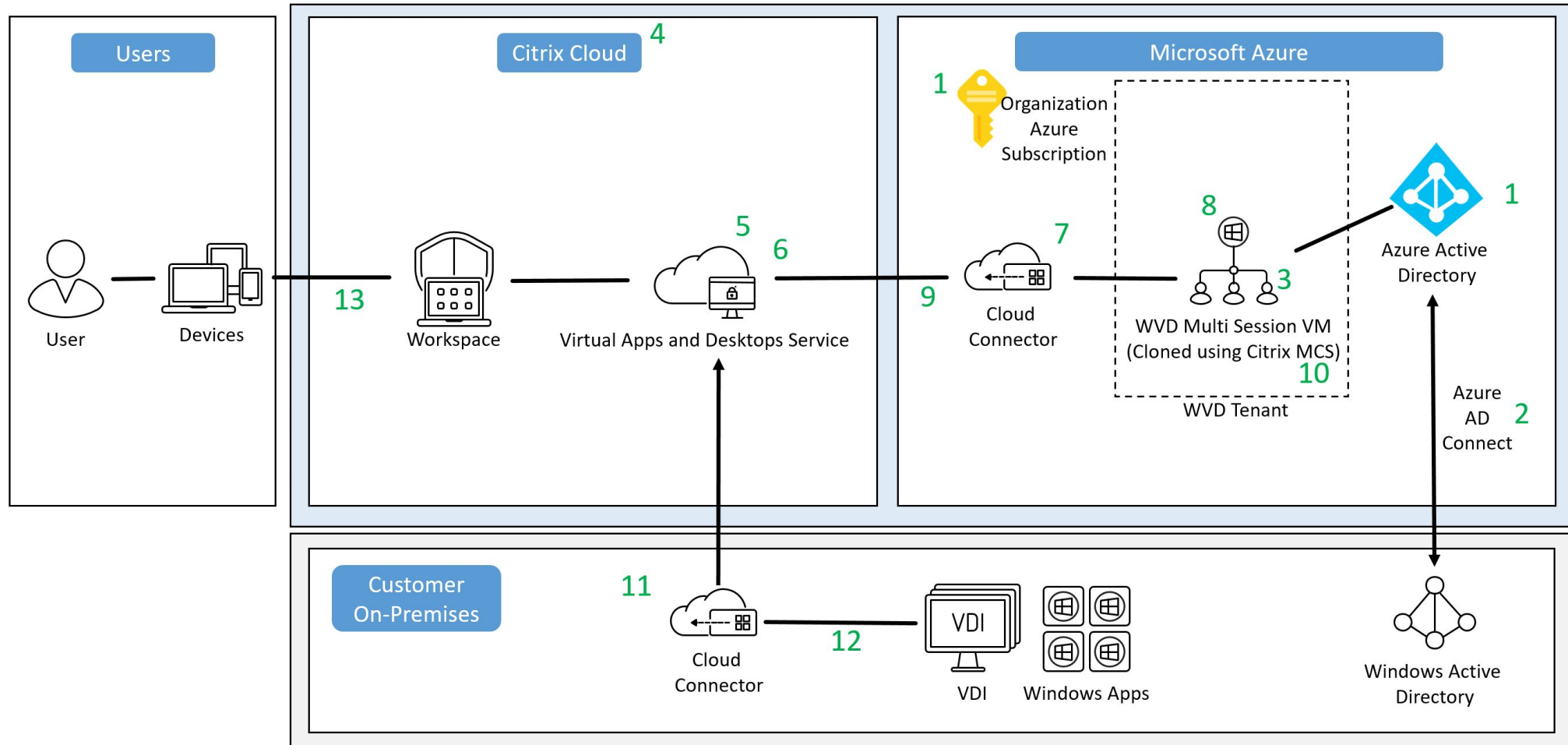
- Citrix Cloud and the Citrix VAD Service is the now and the future.
- Even if you haven't deployed it today, you need to start learning it now because you WILL eventually at your company or maybe another company you may work at some day. Learn now so one day you don't feel like an astronaut with a gorilla standing on your chest all of a sudden.
- Your resume will look 100x better with new technology on it. Your experience with MetaFrame is not valuable to employers. Employers are not looking for that skill in 2020. Saying you are an "on-prem expert" is not the buzz word recruiters are looking for. They look for someone capable of deploying, integrating, & managing new technology. They look for "cloud experts".
- Every company is using some form of cloud service today whether you are aware of it or not.
- If you have a CIO that says "We're not doing cloud" in 2020, you will have a new CIO soon.

# Citrix Cloud explained...

- A control plane running in Microsoft Azure (in Citrix's tenant, not yours)
- CVAD Service = Citrix Virtual Apps and Desktop as a PaaS subscription service you pay Citrix for
  - DDCs = it's just there and globally available, no more DR needed site needed. Citrix monitors and scales it.
  - Studio = same
  - Director = same
  - SQL "aka the reason for many Citrix performance issues because no one maintains it properly" = same
  - License Server = no more licenses because it's a subscription...but you can view usage and assignments
- Citrix Workspace = replaces StoreFront...like StoreFront replaced Web Interface....and so on...you've been through this
- Citrix Gateway Service = the new Citrix Gateway...no more firmware updates and instant HA and GSLB
- VDAs = can be in your on-prem datacenters or in Azure, AWS, GCP. They talk to Cloud Connectors in each datacenter (Citrix calls it a Resource Location) which act as a proxy up to the CVAD Service DDCs.



# Citrix Cloud + Microsoft Azure is extremely flexible for hybrid cloud...and you can use WVD only Windows 10 multi-session, NVIDIA backed VMs, AutoScale, etc.





# Why Azure AD is a common cloud identity provider



Active Directory



Azure  
Active Directory

# Azure AD flavors

	FREE	OFFICE 365 APPS	PREMIUM P1	PREMIUM P2
<b>Core Identity and Access Management</b>				
Directory Objects <sup>1</sup>	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
Single Sign-On (SSO) <sup>2</sup>	up to 10 apps	up to 10 apps	unlimited	unlimited
User provisioning	✓	✓	✓	✓
Federated Authentication (ADFS or 3rd party IDP)	✓	✓	✓	✓
User and group management (add/update/delete)	✓	✓	✓	✓
Device registration	✓	✓	✓	✓
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	✓	✓	✓	✓
Azure AD Connect sync (extend on-premises directories to Azure AD)	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Azure AD Join: desktop SSO & administrator bitlocker recovery	✓	✓	✓	✓
Password Protection (global banned password)	✓	✓	✓	✓
Multi-Factor Authentication <sup>3</sup>	✓	✓	✓	✓
Basic security and usage reports	✓	✓	✓	✓
<b>Business to Business Collaboration</b>				
Azure AD features for guest users <sup>4</sup>	✓	✓	✓	✓
<b>Identity &amp; Access Management for Office 365 apps</b>				

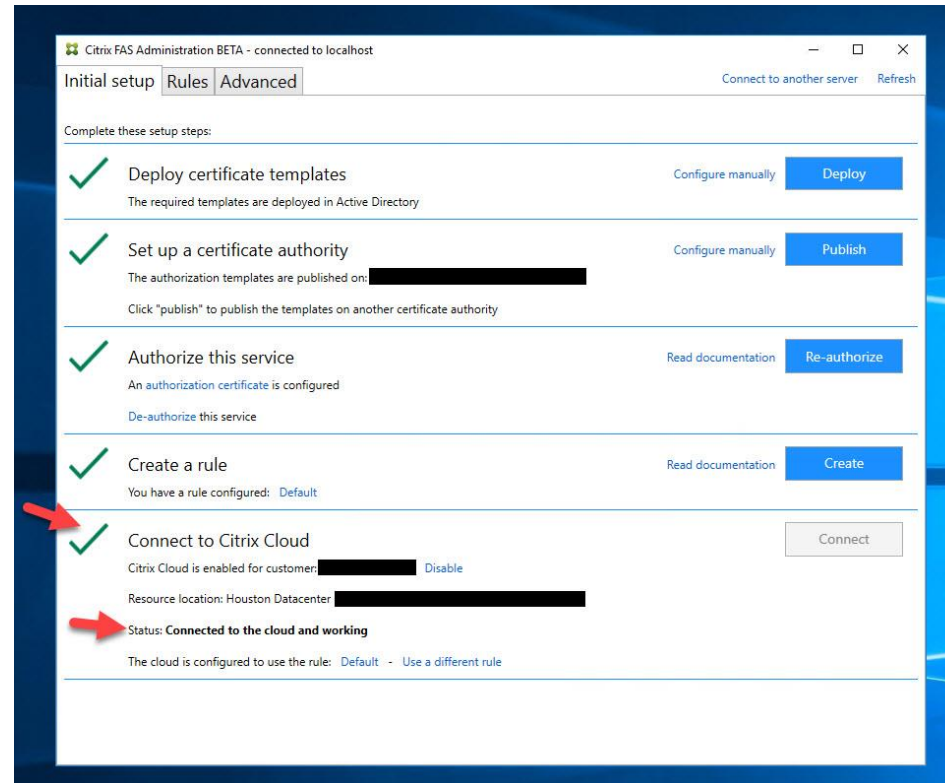
# Azure AD is more than just authentication...

- **Azure AD Conditional Access** – after authenticating, it kicks in and can do IFTTT type logic. “If coming from external IP then do not allow using this highly sensitive app”.
- **Azure AD Identity Protection** - risk-based policies that automatically respond to risky behaviors (example: impossible traveler)
- **Azure AD Password Protection** – dynamically ban passwords and force resets from global banned password list sourced from real password spray attacks and custom ones like “CompanyProduct123!”. Yes it protects your on-prem Active Directory too.
- **Azure AD Self Service Password Reset (SSPR)** – hope you move to password-less soon but if you use passwords now, then you should use this so the Service Desk can take a break.
- **Azure AD Smart Lockout** – intelligent lockout of attackers using brute force password attacks without impacting the targeted user
- **Azure Advanced Threat Protection (Azure ATP)** – there are several “ATP” services...this one is to identify, detect, & investigate advanced threats, compromised identities, & malicious insider actions back on your on-prem DCs
- **Microsoft Cyber Defense Operations Center (CDOC)** – security analysts, forensics, data scientists using ML, BA, automation, look sign-in logs sent to Intelligent Security Graph. Big picture, contain, coordinate remediation.
- **Microsoft Threat Intelligence Center (MSTIC)** – automated systems, security intelligence feeds, and actual human SOC analysts watching the Internet as a whole classifying threats and protecting you in real-time.

**Plus about 15 more bullets I can't fit on this slide.**

# Passwordless over a remoting protocol requires Citrix FAS

- Citrix FAS acts as a middleman that takes modern web auth like Azure AD and converts it into something the Windows OS understands (a certificate) to complete SSO.
- Citrix FAS now works CVAD Service in Citrix Cloud. You can use the same servers for CVAD on-prem. It's just an update, you don't need to build new servers:



# Listen for these things from your Security team...

- Can we get rid of that RADIUS server in the corner your NetScalers are using? You're one of the last teams using it.
- We're deploying <fill in the blank from below> with our physical machines this year. Does Citrix work with these?
  - Windows Hello for Business
  - Microsoft Authenticator passwordless phone sign-in
  - FIDO2 hardware security keys
- The Service Desk is getting too many password reset requests after users lock themselves out on your NetScaler Gateways.
- We detected your NetScalers are getting login attempts from <insert VIP username> every few days with an incorrect password. The user says it's not them. We think someone is validating passwords against your box without triggering a password lockout.



# Windows Hello for Business



TRUST: Device itself + Localized Biometric (finger or face)

(PIN can be used but biometric has higher identity assurance and better user experience)

- Passwordless authentication for Hybrid Azure AD Joined (HAADJ) or Azure AD Joined (AADJ) physical Windows 10 Enterprise laptops or desktops
- A form of trusting the device itself + using localized biometric (finger or face) or PIN code
- Private key is stored on the device and unlocked using the biometric or PIN code
- Requires IR camera or fingerprint reader to use biometrics – so newer devices
- May require Microsoft Certificate Authorities and AD FS depending on your configuration
- **CANNOT** be used with non-persistent VMs and remoting protocols right now. Not designed for that.

# Microsoft Authenticator phone sign-in



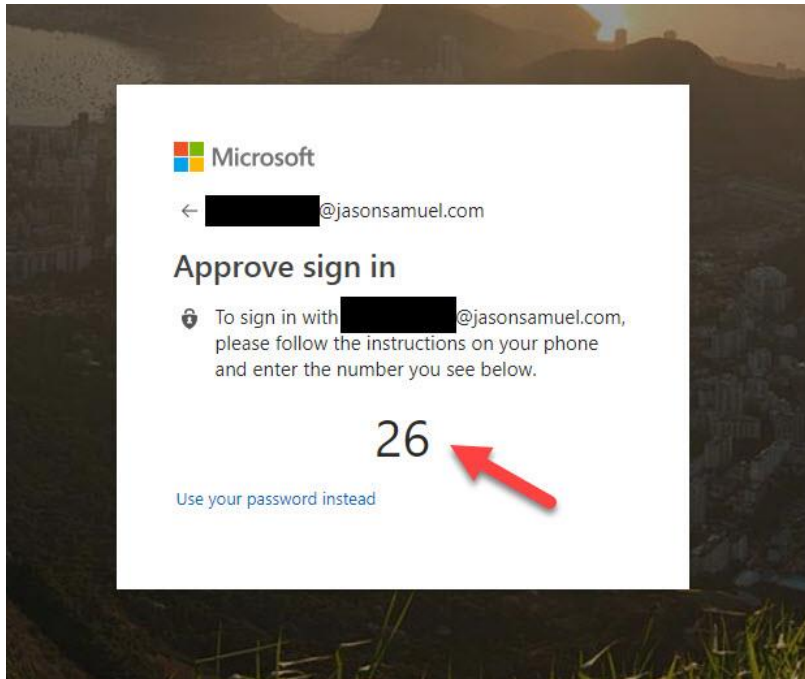
TRUST: Mobile phone with Microsoft Authenticator app + Localized Biometric (finger or face)

(PIN can be used but biometric has higher identity assurance and better user experience)

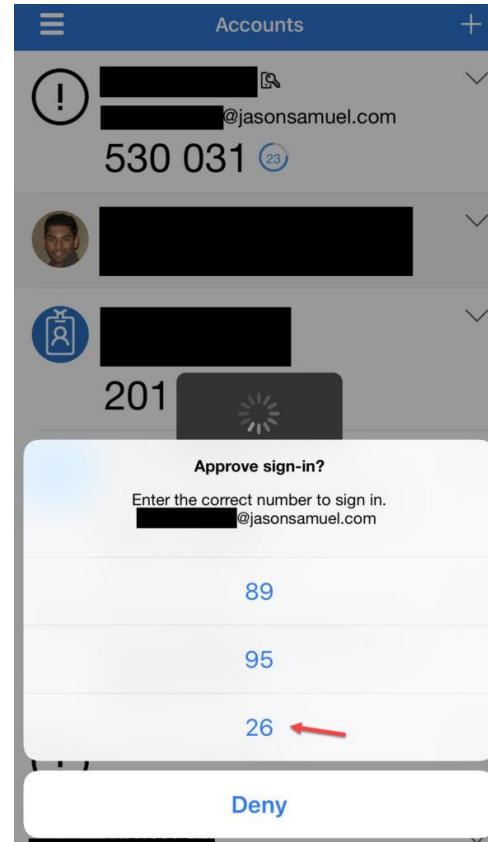
- This is not the same as Azure MFA using Microsoft Authenticator for 2<sup>nd</sup> factor
- Same app, but handles both 1<sup>st</sup> and 2<sup>nd</sup> factor so completely passwordless.
- Trust is created by AAD being aware of your phone through a device registration process.  
NO, THIS IS NOT MDM ENROLLMENT WITH INTUNE (MEM)! Two completely different things.
- Extremely convenient and fast user login experience

# Passwordless login with Citrix Workspace + Authenticator

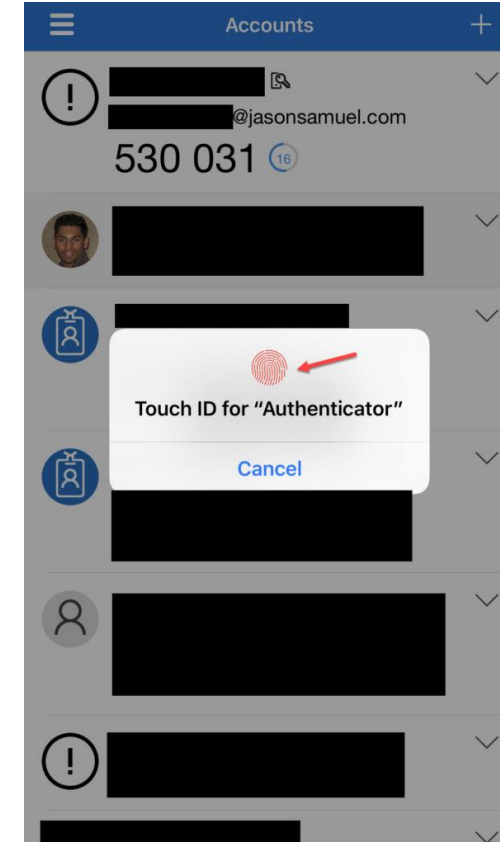
1. Citrix Workspace takes you to AAD and after entering your email address, you will get a random number on your screen



2. Microsoft Authenticator on your phone pops up like this and you click the number that matches your screen



3. Microsoft Authenticator forces you to use a 2<sup>nd</sup> factor to prove its really you. Biometric (Touch ID/Face ID) or PIN code.





# FIDO2 hardware security key

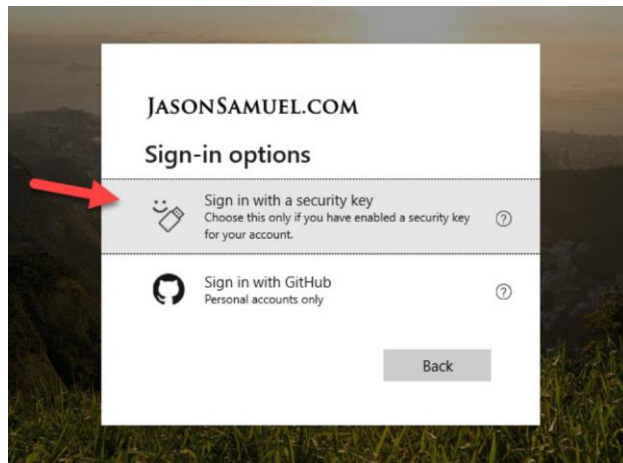


TRUST: FIDO2 security key (USB, NFC, BLE) + Localized Biometric (finger)  
(PIN can be used but biometric has higher identity assurance and better user experience)

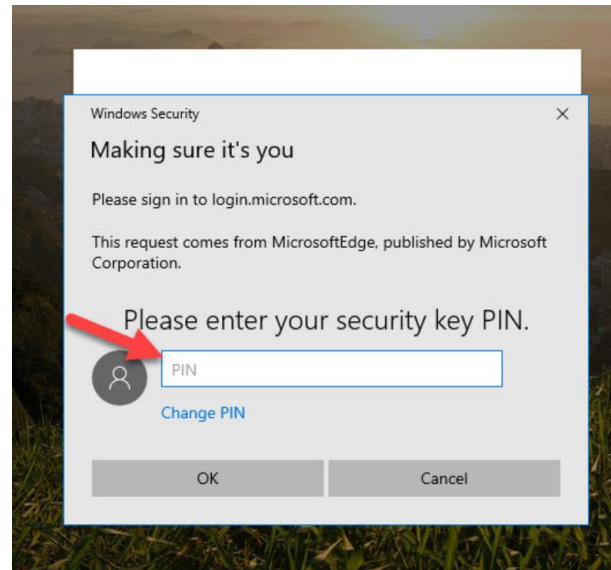
- Open standard for passwordless web authentication, still very young but huge industry momentum
- External authenticator that stores the private key, unphishable
- Can use PIN code or biometric to unlock it
- Can be used for both physical and virtual Windows OS logins
- Can be used for both personal and enterprise needs, better security all around
- Don't confuse your old FIDO U2F key with FIDO2. U2F keys are for 2<sup>nd</sup> factor and can't do passwordless. FIDO2 keys are the successor to FIDO U2F keys.
- Can be used concurrently with Microsoft Authenticator (user forgets or loses phone, battery dead, no cell service, etc)

# Passwordless login with Citrix Workspace + FIDO2

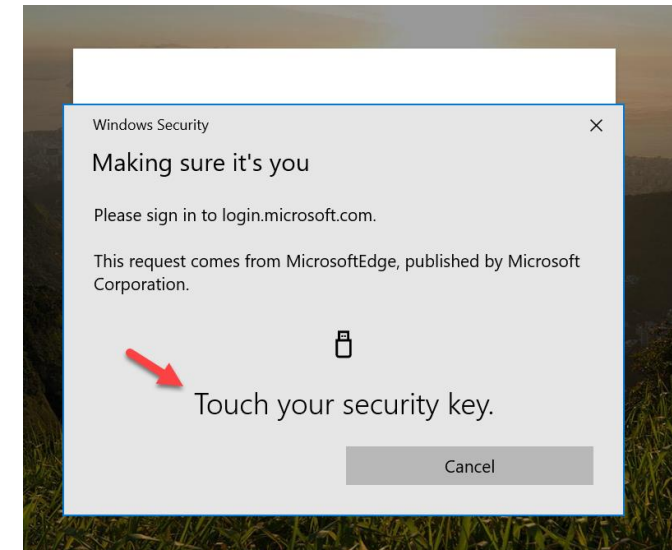
1. Citrix Workspace takes you to AAD and you don't even type in your user name. Just click this option. It's both username-less and password-less. 😊



2. Put your thumb on the key to read your fingerprint and unlock the key. Or use your PIN code.



3. You only have to touch the key again if you used PIN. With biometric you see this screen first and it takes care of both biometric + gesture in one go.



# FIDO Alliance created the FIDO2 open standard

- 260 member companies - <https://fidoalliance.org/members/>



- 40 are Board Level Members, recognize any you trust with your data already?


**February 11, 2020 (2 weeks ago)...**



NIST is a member...

**NIST**

**National Institute of Standards and Technology**  
Technology Administration, U.S. Department of Commerce

# FIDO2 security key form factors

- Physical ports

- USB-A
- USB-C
- Lightning port

- Contactless

- NFC (Near-Field Communication)
- BLE (Bluetooth Low Energy)



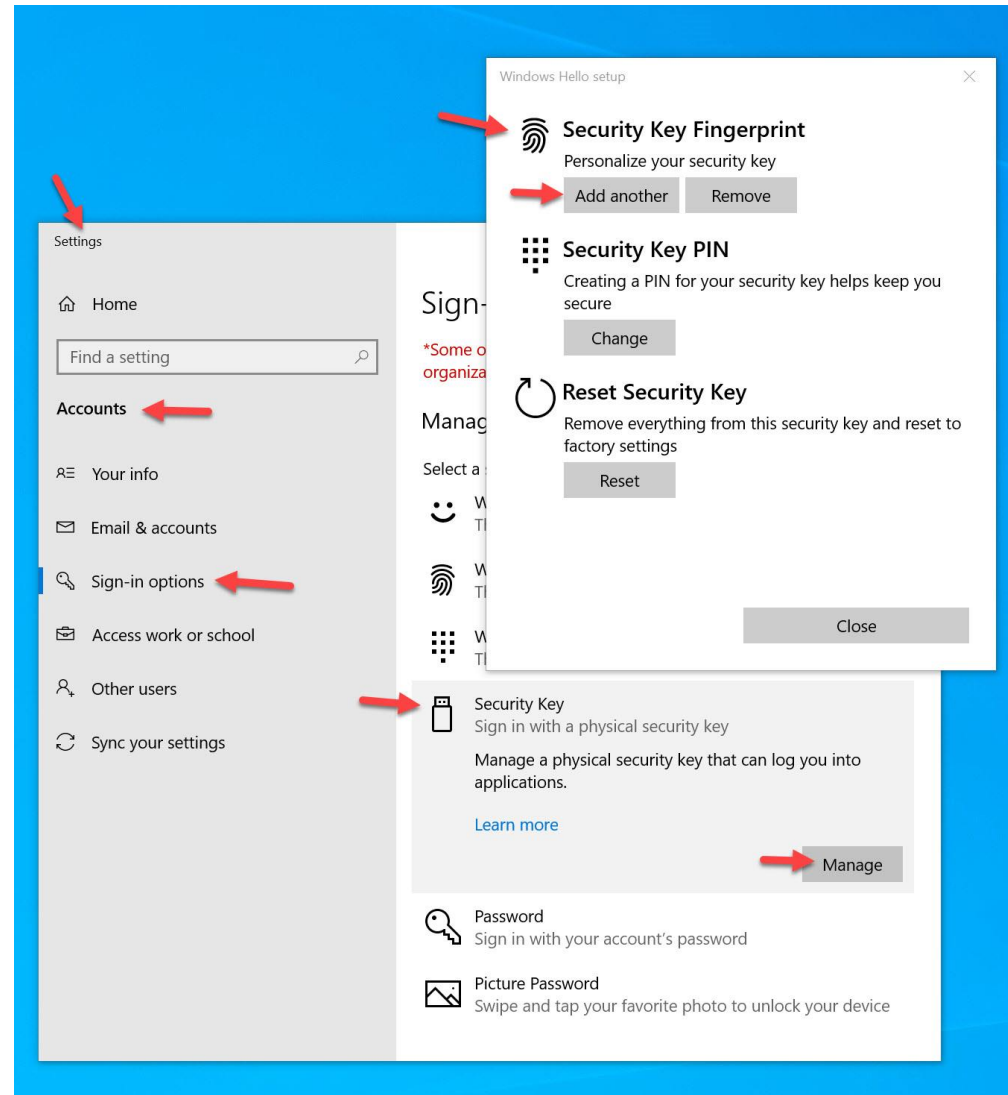
Some keys can do multiple form factors in one!

- Windows 10 build 1903 and newer

- Windows Hello has become a certified FIDO2 authenticator
- Not a security key, but can be used to manage security keys including enrolling fingerprints, PIN, reset key, etc.

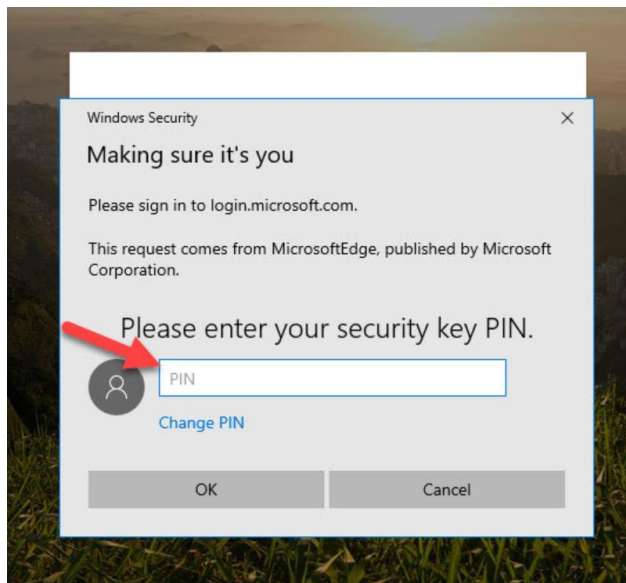


# Windows 10 1903 from May 2019 or newer...even Home...try it yourself

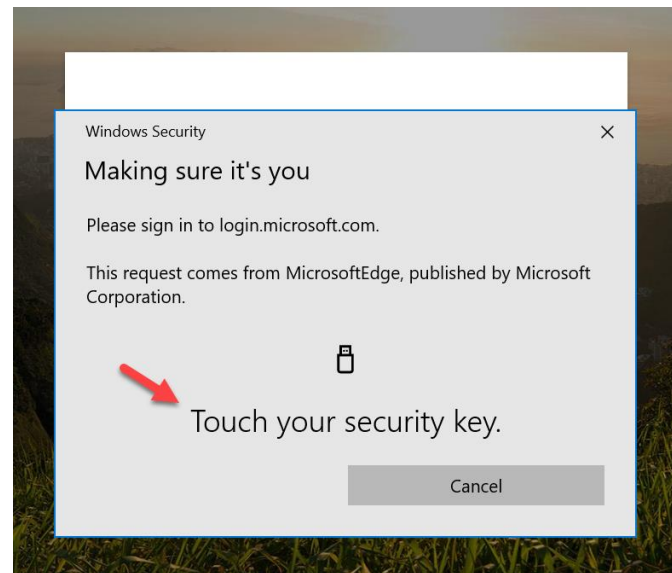


# User experience for users varies based on key form factor

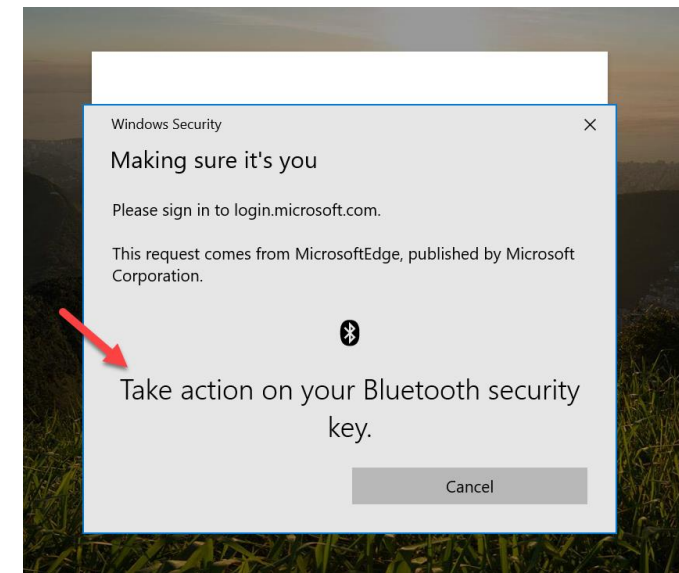
- PIN code only
- Biometric (fingerprint)
- Biometric (fingerprint) as primary + PIN code as secondary if scan fails – the standard for Azure AD



**VS.**



**(physical biometric prompt)**



**(BLE biometric prompt)**



# All shapes and sizes...



# Get the key that fits your needs

- FIDO2 key models I've personally tested with Citrix Workspace + Azure AD
  - Yubico YubiKey 5 NFC
  - Yubico YubiKey 5Ci
  - Feitian BioPass K27
  - Feitian BioPass K26
  - Feitian All-In-Pass K33
  - Ensurity ThinC-AUTH
  - eWBM Goldengate G310
  - HID Global Crescendo Key
  - ...any key that conforms to FIDO2 will work
- Some of these companies make older FIDO U2F keys too.
- Make sure you are purchasing a FIDO2 key and not FIDO U2F!



# Where can you use FIDO2 besides AAD?

- <https://www.dongleauth.info/>



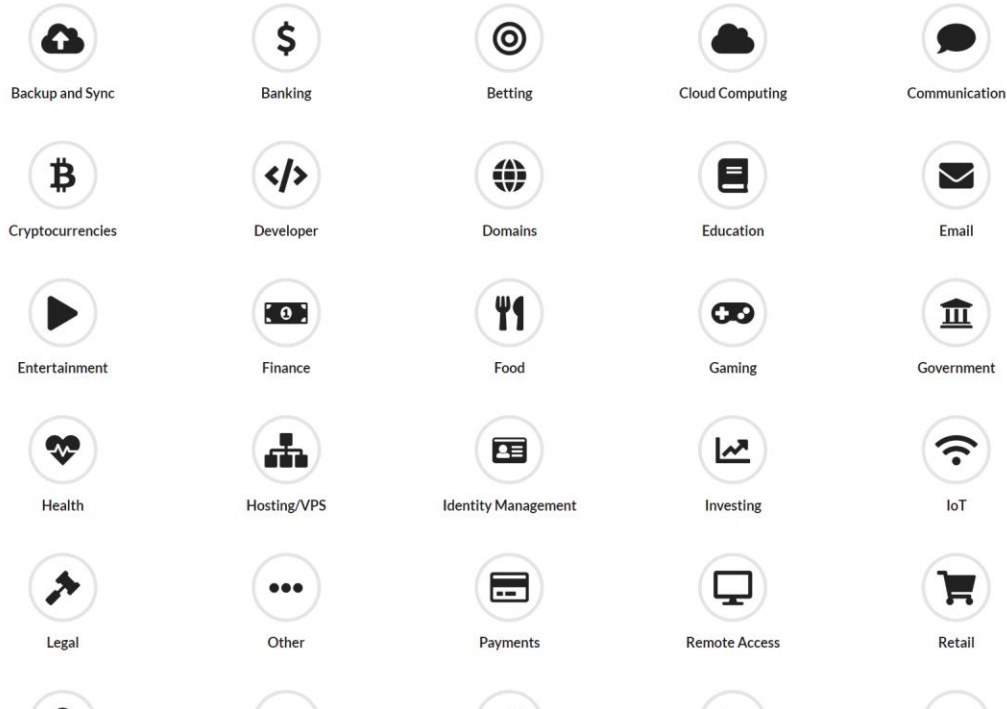
## USB-Dongle Authentication

List of websites and whether or not they support [One Time Passwords \(OTP\)](#) or [Web Authentication \(WebAuthn\)](#) respectively FIDO2, U2F.

Also see the list of [dongles](#) and the protocol they support.

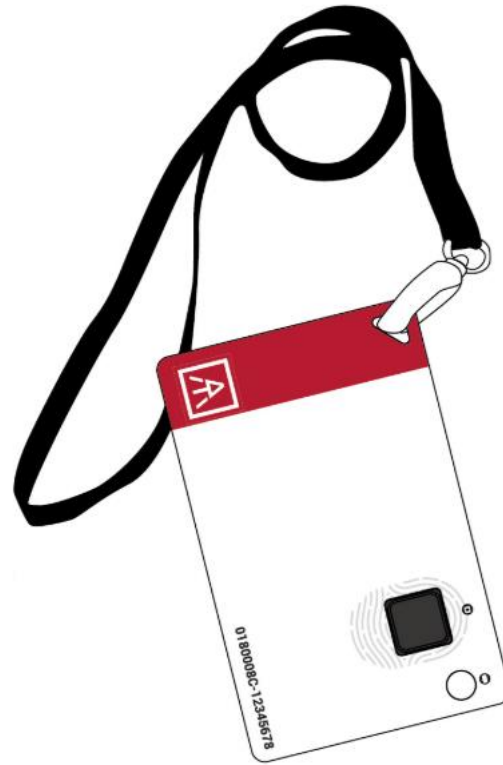
Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Q Search websites



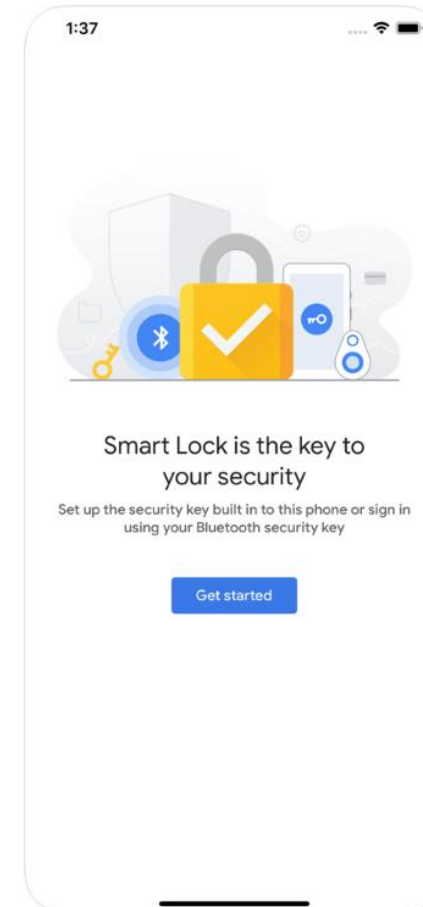
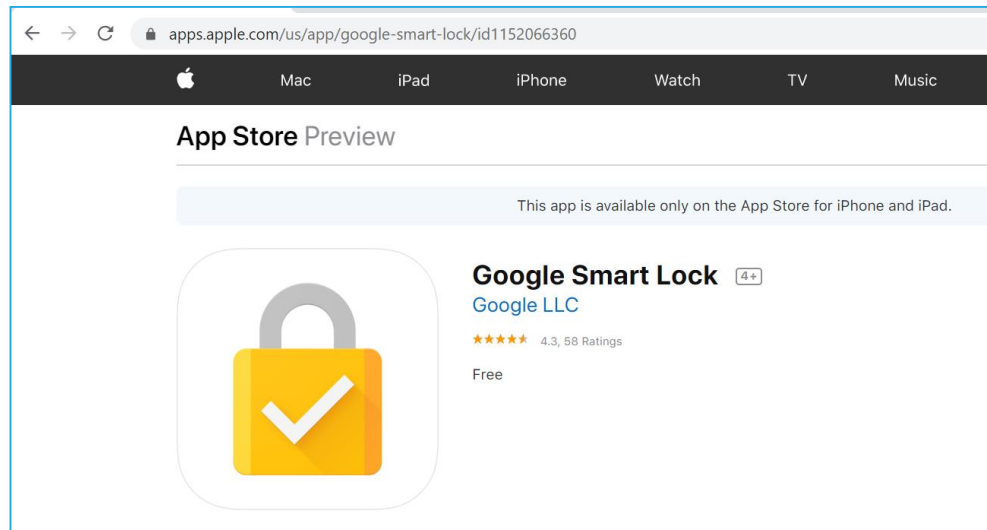
# Other FIDO2 form factors?

- Employee badge?



# Other FIDO2 form factors?

- In software using your iOS or Android phone's secure hardware?
  - **April 10, 2019** - Google Android 7+ Phone Is Now a FIDO2 Security Key
  - **January 13, 2020** – Google Smart Lock app for Google accounts – “With this new update, you can now set up your phone's built-in security key” using the iPhone's Secure Enclave

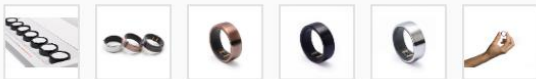


# Other FIDO2 form factors?

- Wearables?

## 24/7 Smart Ring

Motiv Ring now delivers even more convenience and information to you 24 hours of your day, 7 days a week.



- Stylish, minimalist design for 24/7 wearability
- Waterproof to 165 feet; lightweight titanium
- 3-day battery life; quick 90-minute charge
- Tracks fitness, sleep + heart rate
- Available in [7 Motiv Ring sizes](#)
- Available on iOS + Android, [check compatibility](#)
- **FREE priority shipping**
- **1-year warranty, 45-day guarantee**

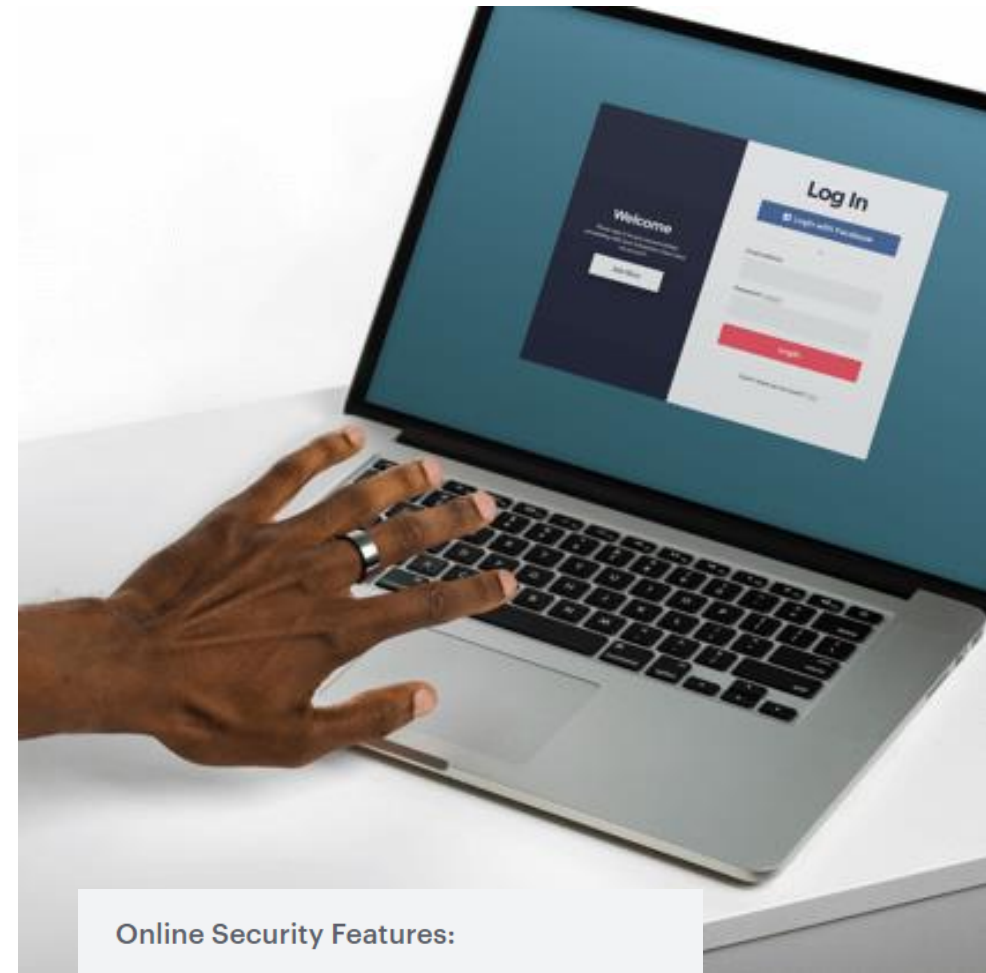
**\$199.99**

*Due to high demand we're currently shipping backorders.  
Will accept new orders in 6-8 weeks*

MyMotiv.com only ships to the US.

[Click here](#) to find out if Motiv Ring is available in your country and where you can purchase it.

To allow you to soon take advantage of password-free login, Motiv Ring has officially been named FIDO Certified™ by the FIDO Alliance – among the first FIDO2-certified devices.




### Online Security Features:

- 2-Step Verification (2FA)
- Passwordless Login (coming soon)
- Facial recognition (iOS; coming soon on Android)
- Fingerprint Identity (iOS; coming soon on Android)

# Breaking News from Monday, Feb 24...

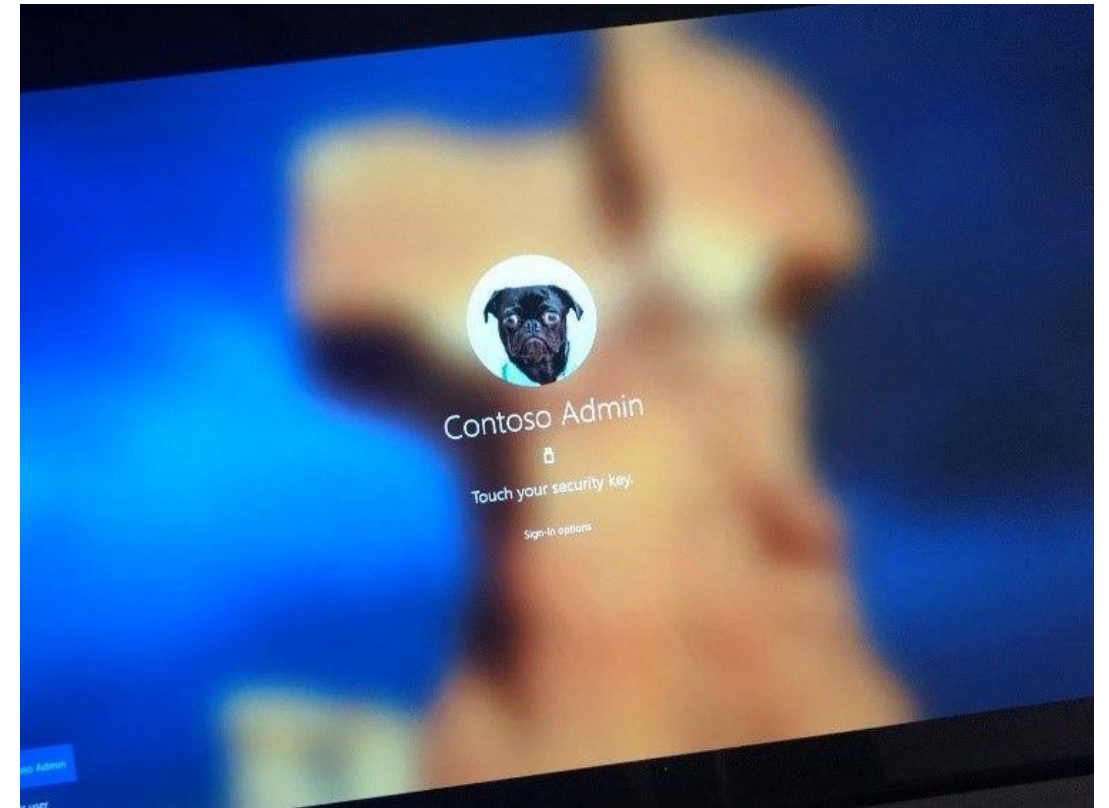
☰ 🔍 Microsoft Sign In 👤

 Alex Simons (AZURE) Microsoft

Public preview of Azure AD support for FIDO2 security keys in hybrid environments

6 hours ago

I'm excited to announce the public preview of Azure AD support for FIDO2 security keys in hybrid environments. Users can now use FIDO2 security keys to sign in to their Hybrid Azure AD joined Windows 10 devices and get seamless sign-in to their on-premises and cloud resources. Since



1. Windows Server patch for Domain controllers (Server [2016](#)/Server [2019](#)).
2. Windows Insider Builds 18945 or later for PCs.
3. Version 1.4.32.0 or later of [Azure AD Connect](#).

<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/public-preview-of-azure-ad-support-for-fido2-security-keys-in/ba-p/1187929>

# AAD User Self-Service Registration of Passwordless Authentication Methods

The screenshot displays the 'My Sign-Ins' page in a Microsoft account interface. The left sidebar contains navigation options: Overview, Security info (highlighted with a red arrow), Organizations, Devices, and Privacy. The main content area is titled 'Security info' and includes a description: 'These are the methods you use to sign into your account or reset your password.' Below this, it states the 'Default sign-in method: Authenticator app or hardware token - code' with a 'Change' link. An 'Add method' button is present, with a red arrow pointing to it. A list of registered methods follows, with a red box highlighting the 'Microsoft Authenticator' and 'Security key' entries. Red arrows point to these entries with the labels 'Your phone' and 'Your FIDO2 keys' respectively. Each method entry includes an icon, a name, a masked value, and a 'Delete' link. The 'Security key' entries also include a dropdown arrow.

Method	Name	Value	Action
Phone		[Redacted]	Change, Delete
Office phone		[Redacted]	Enable two-step verifi
Microsoft Authenticator		[Redacted]	Delete
Security key	eWBM Goldengate G310		Delete
Security key	eWBM Goldengate G310 - blue		Delete
Security key	YubiKey 5 NFC - Blue		Delete
Security key	HID Global Crescendo Key		Delete
Security key	Ensurity ThinC-AUTH - blue		Delete
Security key	Ensurity ThinC-AUTH		Delete
Security key	Feitian K33 AllinPass		Delete
Security key	Feitian USB		Delete
Security key	YubiKey 5 NFC JSC		Delete



# Questions?



# Round Table Discussions at 3 PM Today

- Cover any questions on authentication, identity, & access management specific to your environment. And some giveaways to get you started with passwordless. 😊
- Live Demos
  - Workspace + Azure AD + Microsoft Authenticator passwordless login + FAS + virtual desktop launch with full Windows SSO
  - Workspace + Azure AD + FIDO2 security key passwordless login + FAS + virtual desktop launch with full Windows SSO



