

Passwordless

No One Want's To Go Back

Martin Himken





- Senior Consultant Endpoint Management
- Intune experience: 5+ Years
- ConfiMgr experience: 12+ years

- Contact Info
- X/Twitter: MHimken
- GitHub: Mhimken
- Find me in the Winadmins Discord

Jóhannes Geir Kristjánsson

NORDIC - VIRTUAL SUMMIT -

- Enterprise Mobility MVP
- 12 years in IT

- Contact Info
- Winadmins Discord (WinAdmins.io)
- @jgkps



Agenda

- Introduction to passwordless
- Basic setup
- Adoption of passwordless
- Enrollment Demos
- Conclusion



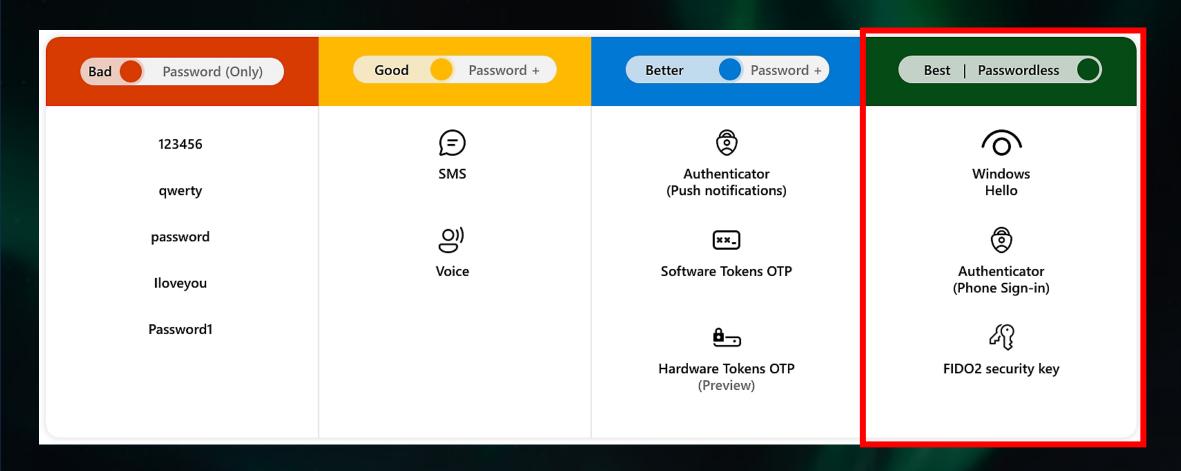


Introduction

Welcome to passwordless - you're here to stay

Where are you today?





Passwordless



Pros

- Your users will love you
- Management will love you
- Security will love you

Cons

- Your users will also hate you (if you don't prepare)
- Exit-Strategy will kill user motivation
- Security key might mean additional cost



How to prepare for passwordless





- Make Entra your primary IdP
- Inventory your (web-)applications
 - Authentication?
 - Authentication type?
 - Single sign-on?
- Test and verify rinse and repeat



Basic Setup

Things you need for testing

Prepare – Authentication methods



	· ·	icies > NVS: Require multifactor authentication for all users (From template) >	Manage migration ×	
Authentication methods SVA Ninja - Microsoft Entra ID Security	nods Policies ···		On September 30th, 2025, the legacy multifactor authentication and self-service password	
∠ Search «	Got feedback?		reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy	
Manage	Use this policy to configure the a	policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authen Learn more 🖸		
Policies	Manage migration	On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be de		
Password protection	Manage migration	Use this control to manage your migration from the legacy policies to the new unified policy. Learn more	Pre-migration:	
Registration campaign		Manage migration	Use policy for authentication only, respect legacy policies.	
Authentication strengths			Migration In Progress:	
Settings	Method	Target	Use policy for authentication and SSPR, respect legacy policies.	
Monitoring	FIDO2 security key	All users	Migration Complete:	
Activity	Microsoft Authenticator	All users	Use policy for authentication and SSPR, ignore legacy policies.	
User registration details	SMS			
Registration and reset events	Temporary Access Pass	All users		
Bulk operation results	Hardware OATH tokens (Preview)			
Bulk operation results	Third-party software OATH tok	ens		
	Voice call			
	Email OTP			
	Certificate-based authenticatio	n		

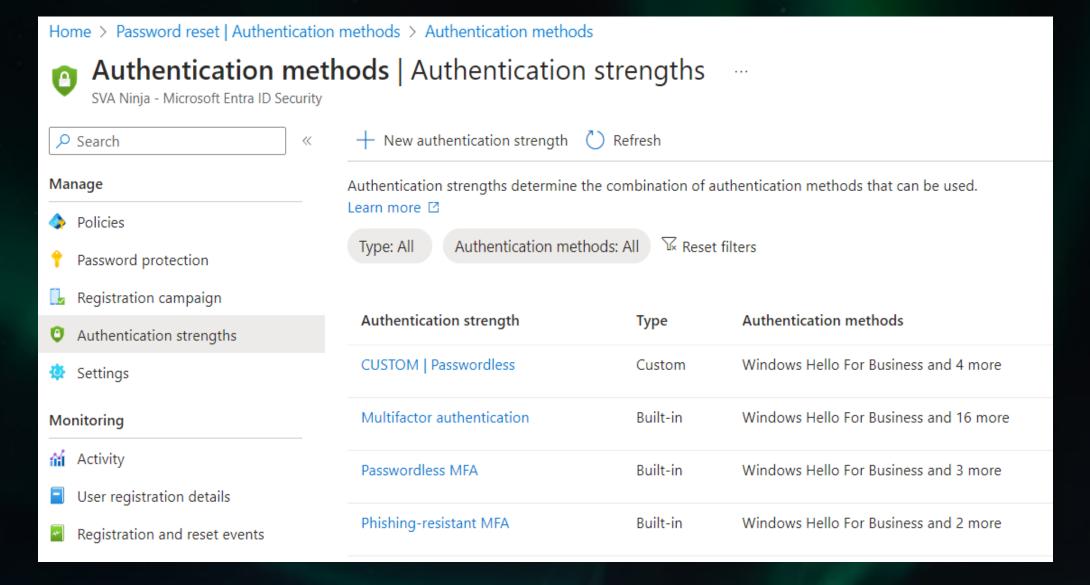
Prepare – Authentication methods



Method	Target	Enable	ed
FIDO2 security key	All users	Yes	
Microsoft Authenticator	All users	Yes	
SMS		No	
Temporary Access Pass	All users	Yes	
Hardware OATH tokens (Preview)		No	
Third-party software OATH tokens		No	
Voice call		No	
Email OTP		Yes	
Certificate-based authentication		No	

Temporary Access Pass settings Temporary Access Pass, or TAP, is a time-limited or limited-use pass TAP is issuable only by administrators, and is seen by the system as **Enable and Target** Configure **GENERAL** 1 hour Minimum lifetime: 1 day Maximum lifetime: 1 hour Default lifetime: No One-time: 8 characters Length: Edit

Prepare – Authentication strengths





Prepare – Authentication strengths



View Authentication Strength

Name Passwordless MFA

Type Built-in

Description High assurance authentication strength that

includes methods with Cryptographic keys, for

example Passkeys (FIDO2)

Authentication Flows Windows Hello For Business

OR

Passkeys (FIDO2)

OR

Certificate-based Authentication (Multifactor)

OR

Microsoft Authenticator (Phone Sign-in)

View Authentication Strength

Name CUSTOM | Passwordless

Type Custom

Description

Creation Date 11/19/2023, 11:38 PM

Modified Date 2/14/2024, 9:55 PM

Authentication Flows Windows Hello For Business

OR

Passkeys (FIDO2)

OR

Microsoft Authenticator (Phone Sign-in)

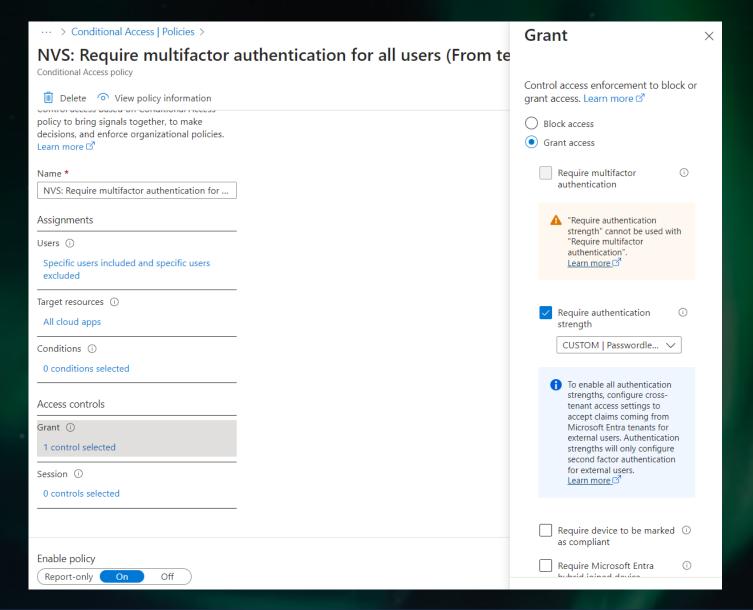
OR

Temporary Access Pass (One-time use)

OR

Temporary Access Pass (Multi-use)

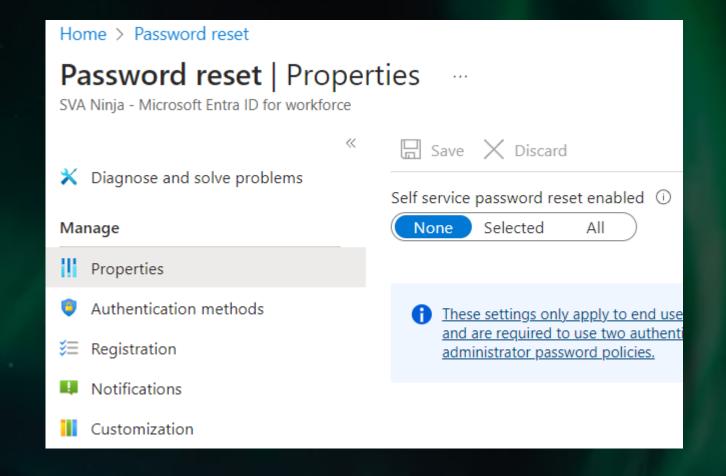
Prepare - Conditional Access





Prepare – Password reset





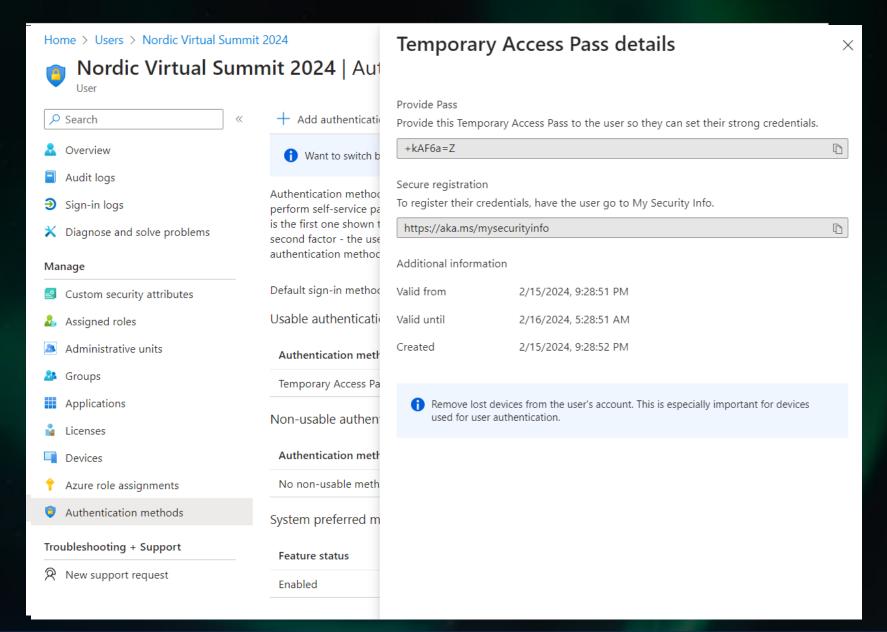
Prepare - Create the user



- Use the admin portal (yes!)
- Create a user with a very long (40+) complex password
- Don't require user to change password

eset password VS@sva.ninja	
Automatically create a password	
Passwords must be between 8 and 256 characters and use a combin three of the following: uppercase letters, lowercase letters, numbers,	
Password *	
	0
Require this user to change their password when they first sign in]
Email the sign-in info to me	•

Prepare – Create the TAP







Adoption of passwordless

Phases of Adoption

- Password reign supreme
 - Limited SSO

- Transitionary phase
 - Mix of both
 - Functionally password-less
- Completely Password-less
 - SSO Everywhere
 - Phishing Resistant



What are passkeys?

- Passkeys are WebAuthn credentials bound to a device
- The 'pass' may be used remotely
- Used to replace most or all passwords
- Security keys are physical, passkeys are not





Why is it 'phishing resistant'?



- Two factors are always required
- Simple phishing sites don't work - remember 'there is no password!'





Demo

New Employee Procedure – Phone first

New Employee Procedure – Phone first

- When you should do the phone first
 - Enables onboard of everything else
 - Other phone apps
 - Laptops
 - Tablets
 - etc
 - Verify the TAP, must be Typable by the user
 - More resilient to scheduling mistakes
 - Gives them something to do while the computer Autopilot



Authenticator Setup with TAP







Demo

New Employee Procedure – Computer first

New Employee Procedure – Computer first

NORDIC

- Users with no smartphone access
- Make Autopilot as short and reliable as possible
- Requirements for the user:
 - Stable internet connection
 - Keyboard layout should match the TAP layout

The virtual machine 'W11_SVN_MEJ' is turned off

To start the virtual machine, select 'Start' from the Action menu

Star

Status: Off



Conclusion

Some pitfalls – many benefits

Do's and Don'ts

- Do's
 - Use one-time TAP whenever possible
 - Encourage the use of the Authenticator app
 - Allow the use of WHFB sooner than later

• Don'ts

- Use a TAP to enroll devices on behalf of users
- Use a TAP to sign in as VIPs to assist them
- Allow passwordless users to reset their password



Gotchas



- Removing the account from the authenticator might remove the registered device from Entra
- Let your setup 'cook' for 24 hrs
- Disable Self-Service-Password-Reset (SSPR)

Conclusion

- Use Entra as your IdP
- 'Enlighten' legacy web-apps
- Make passwordless options available to existing users and required for new hires
- Inventory and Test
- Your users are already familiar with passwordless

Passwordless is





Helpful content

Advanced Deployment Guide by MS: https://admin.microsoft.com/Adminportal/Home?Q=Search#/modernonboarding/passwordlesssetup



Services that support passkeys https://passkeys.directory/



Terminology explained https://passkeys.dev/



