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

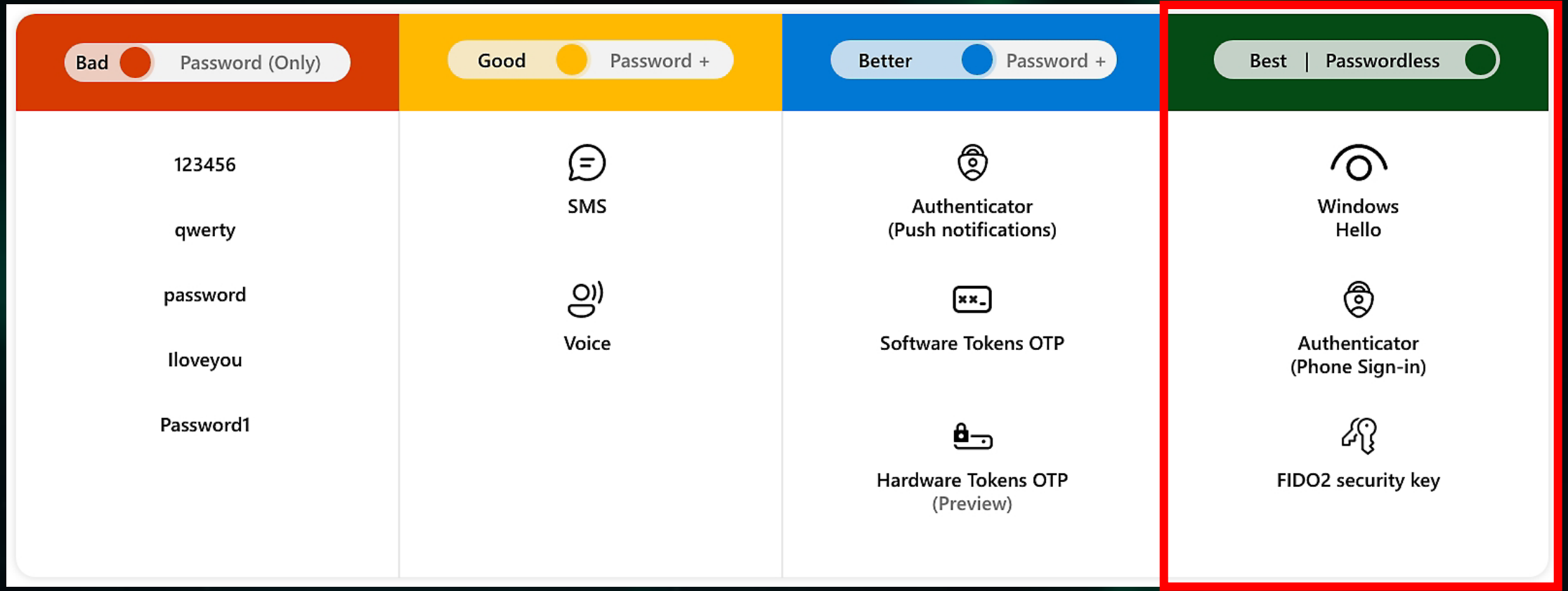
- Introduction to passwordless
- Basic setup
- Adoption of passwordless
- Enrollment Demos
- Conclusion

NORDIC
– VIRTUAL SUMMIT –

Introduction

Welcome to passwordless – you‘re here to stay

Where are you today?



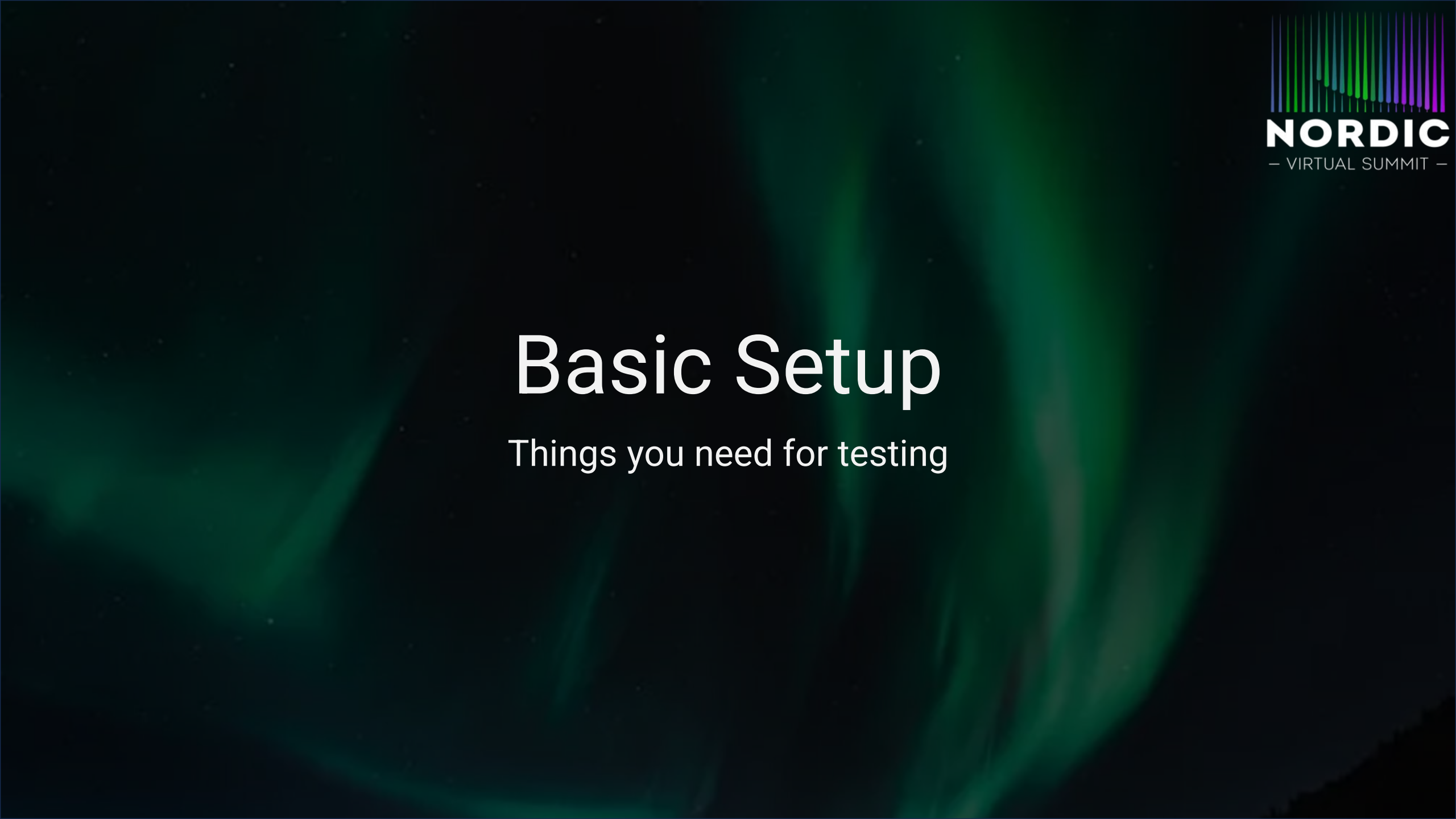
Passwordless

NORDIC
– VIRTUAL SUMMIT –

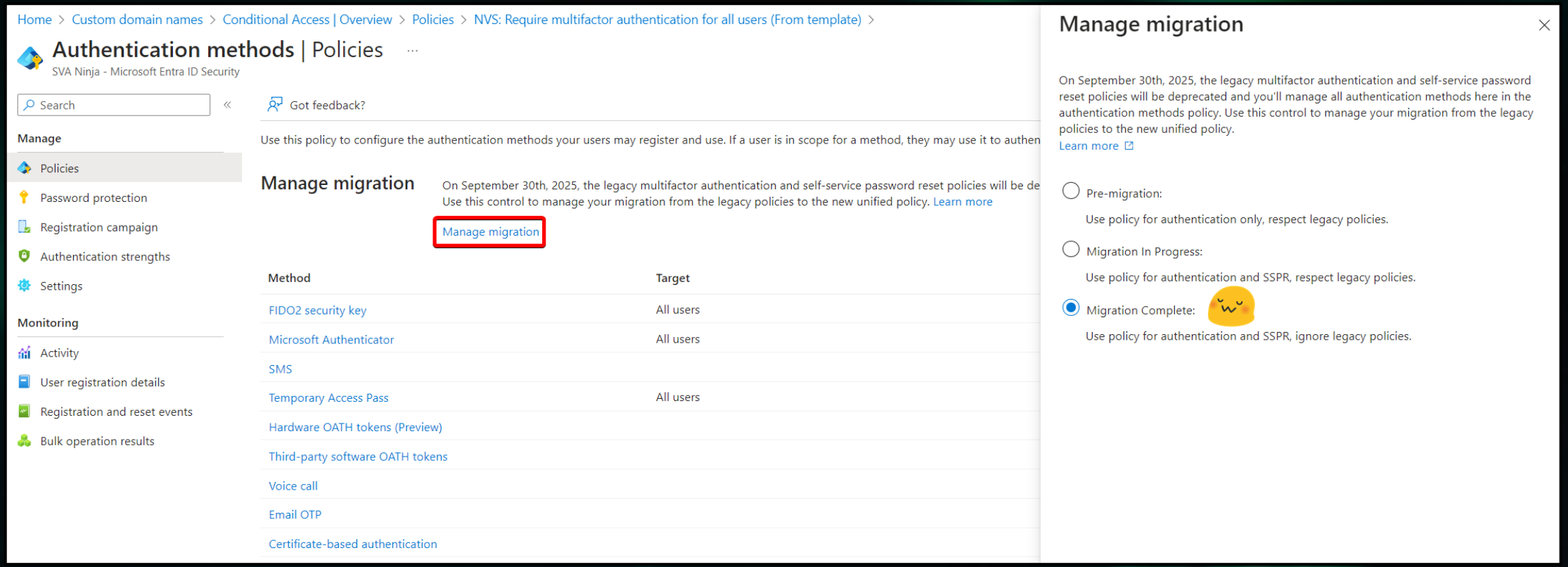
- Pros
  - Your users will love you
  - Management will love you
  - Security will love you
- Cons
  - Your users will also hate you (if you don’t prepare)
  - Exit-Strategy will kill user motivation
  - Security key might mean additional cost

How to prepare for passwordless

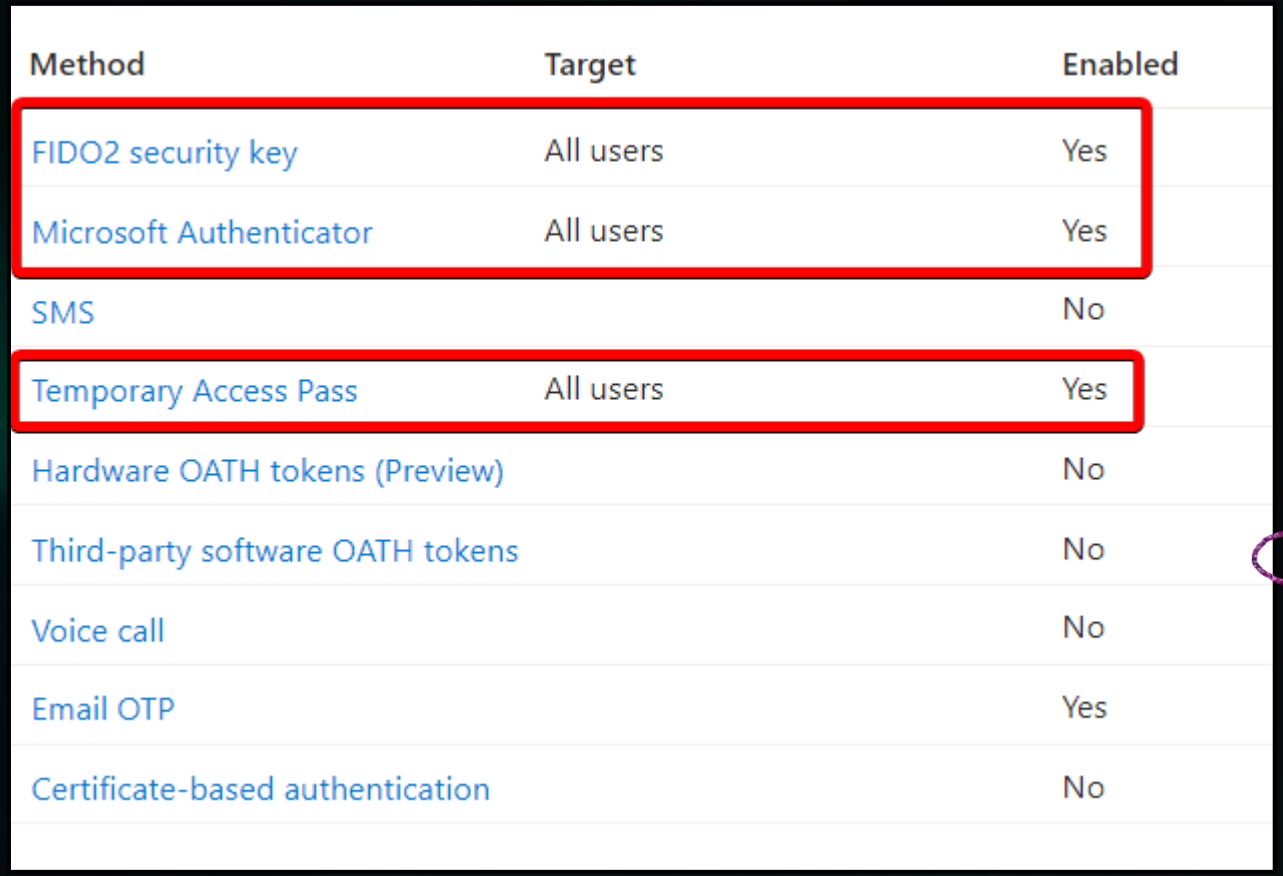
- Make Entra your primary IdP
- Inventory your (web-)applications
  - Authentication?
  - Authentication type?
  - Single sign-on?
- Test and verify – rinse and repeat


NORDIC
– VIRTUAL SUMMIT –
Basic Setup
Things you need for testing

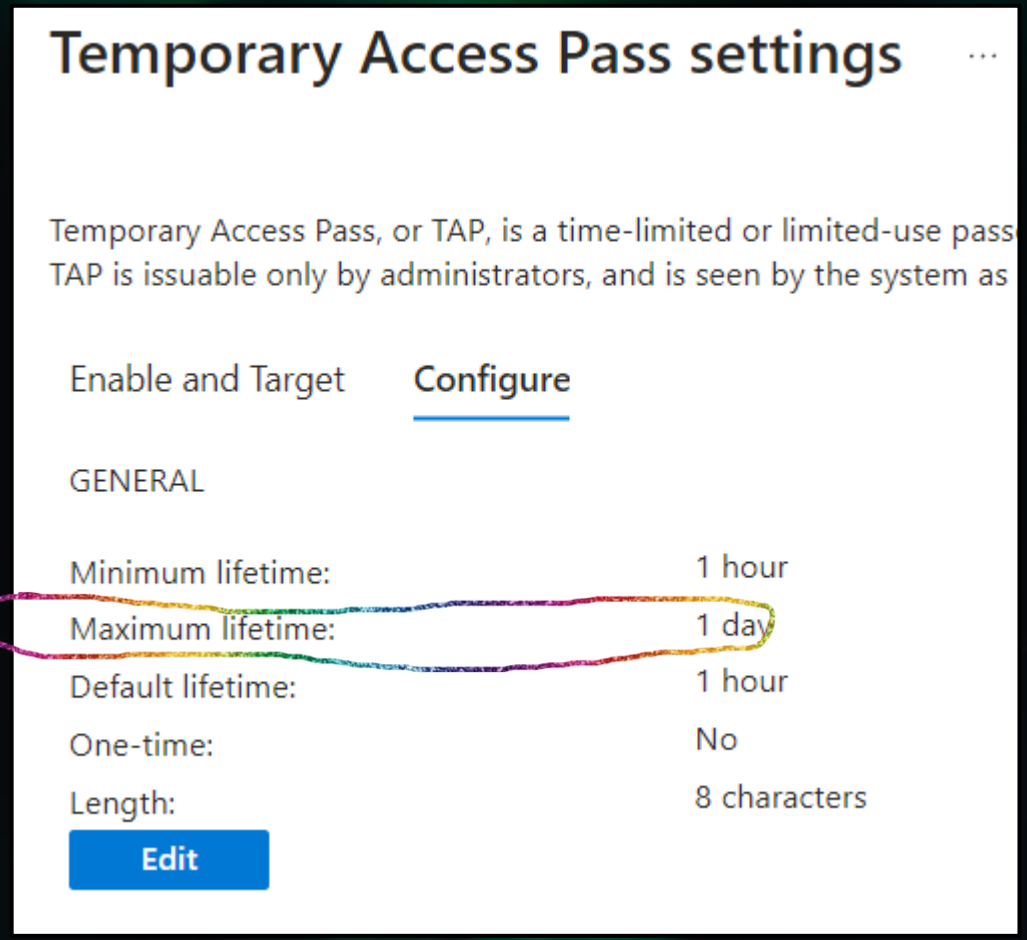
Prepare – Authentication methods



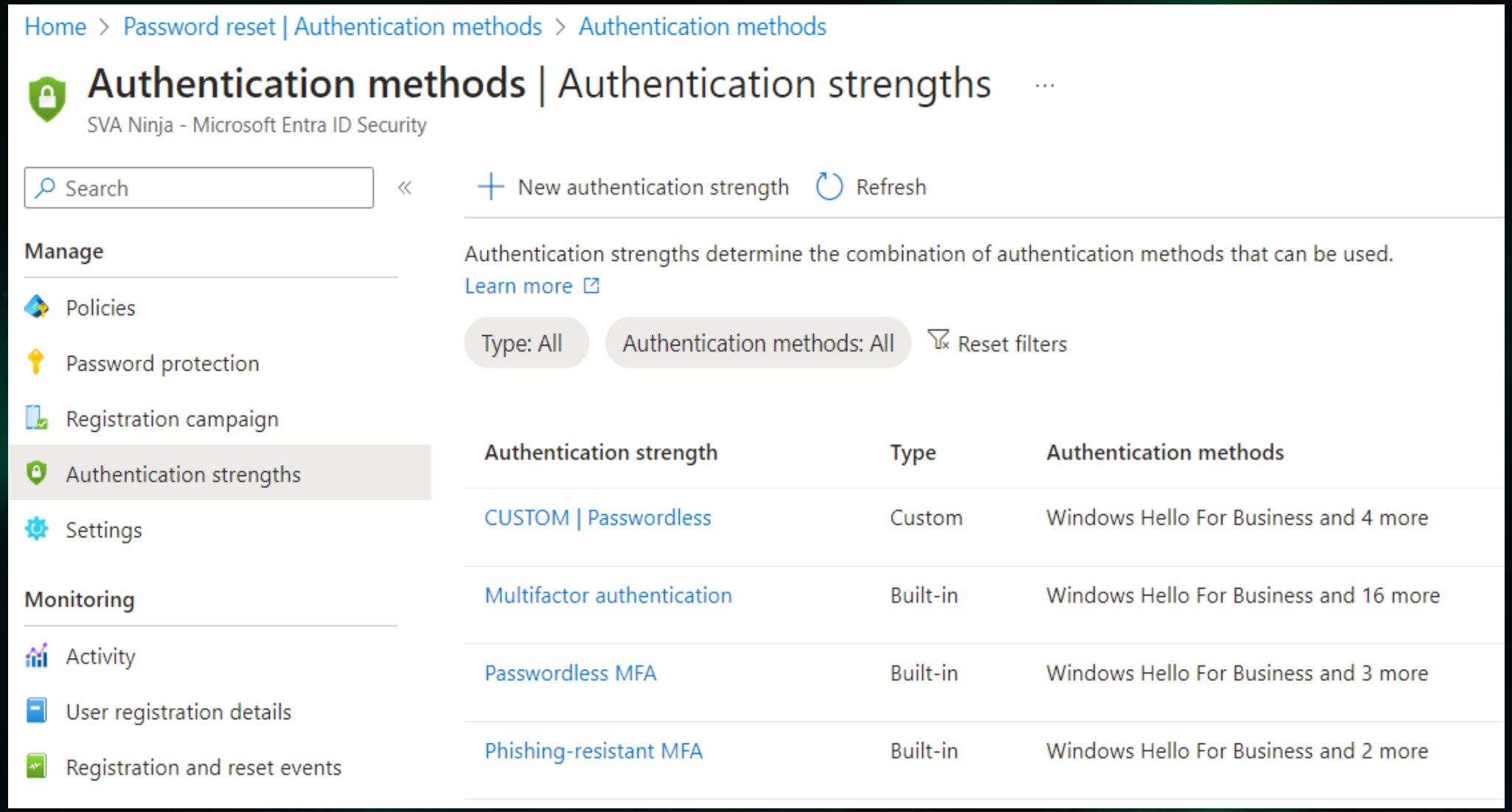
Prepare – Authentication methods



Method	Target	Enabled
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



Prepare – Authentication strengths



Prepare – Authentication strengths

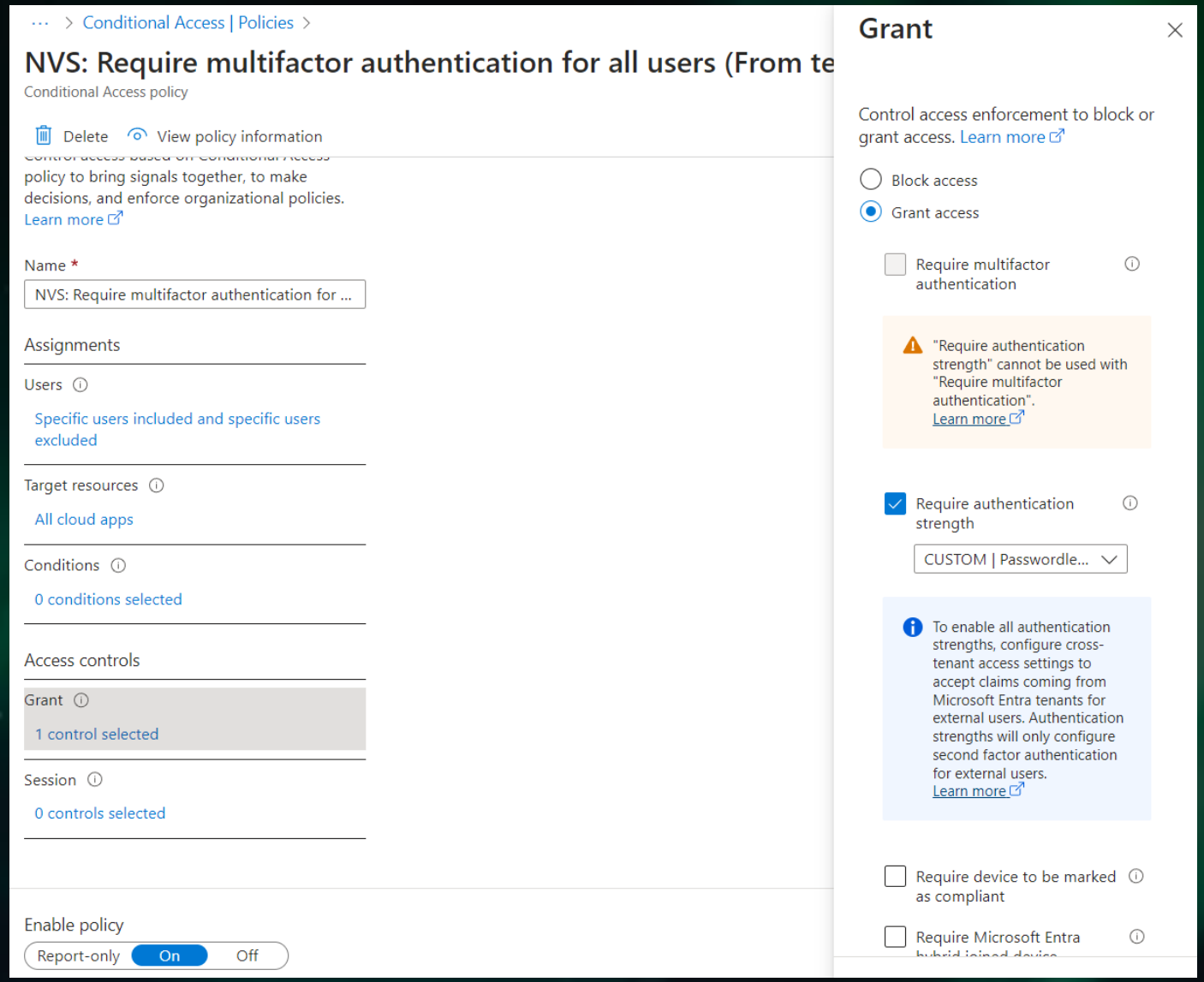
View Authentication Strength

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)

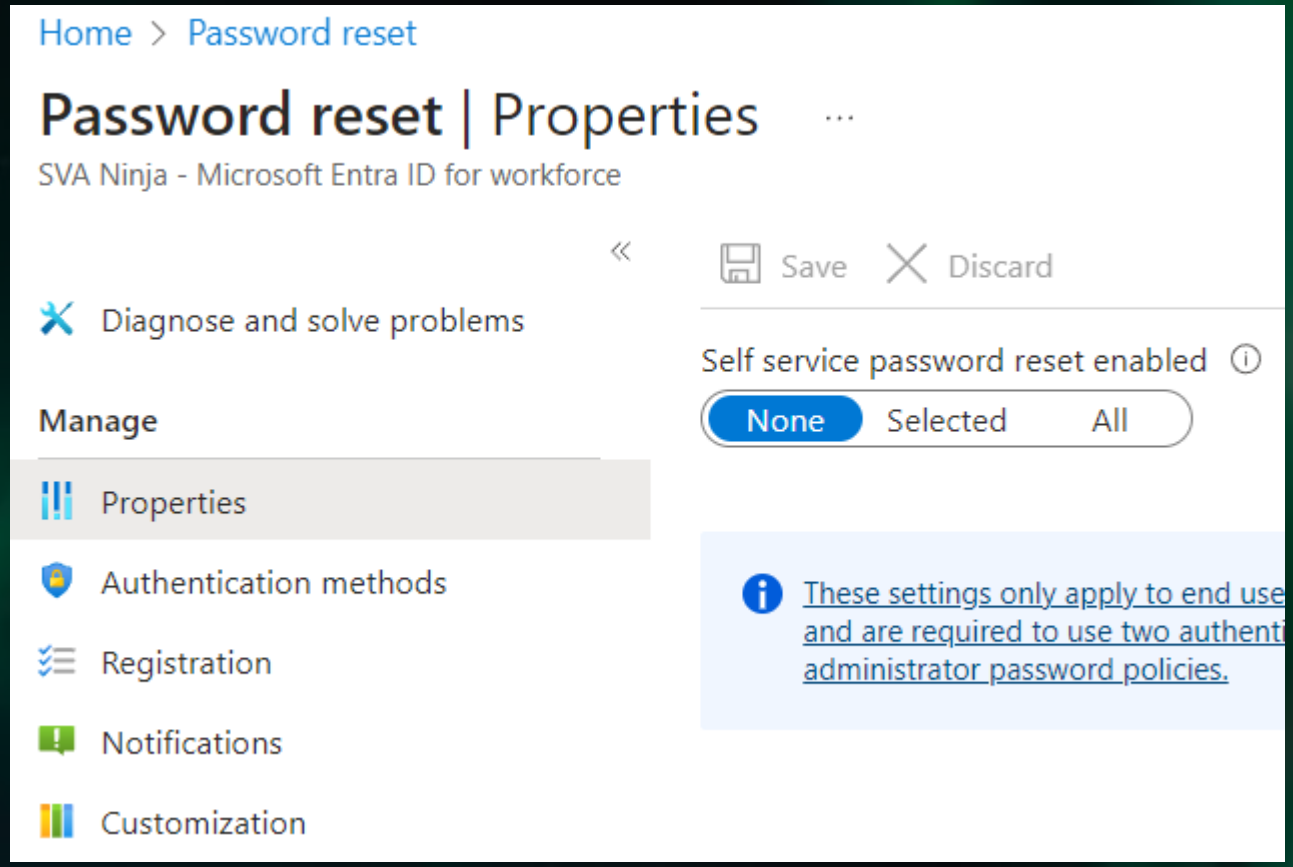
View Authentication Strength

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

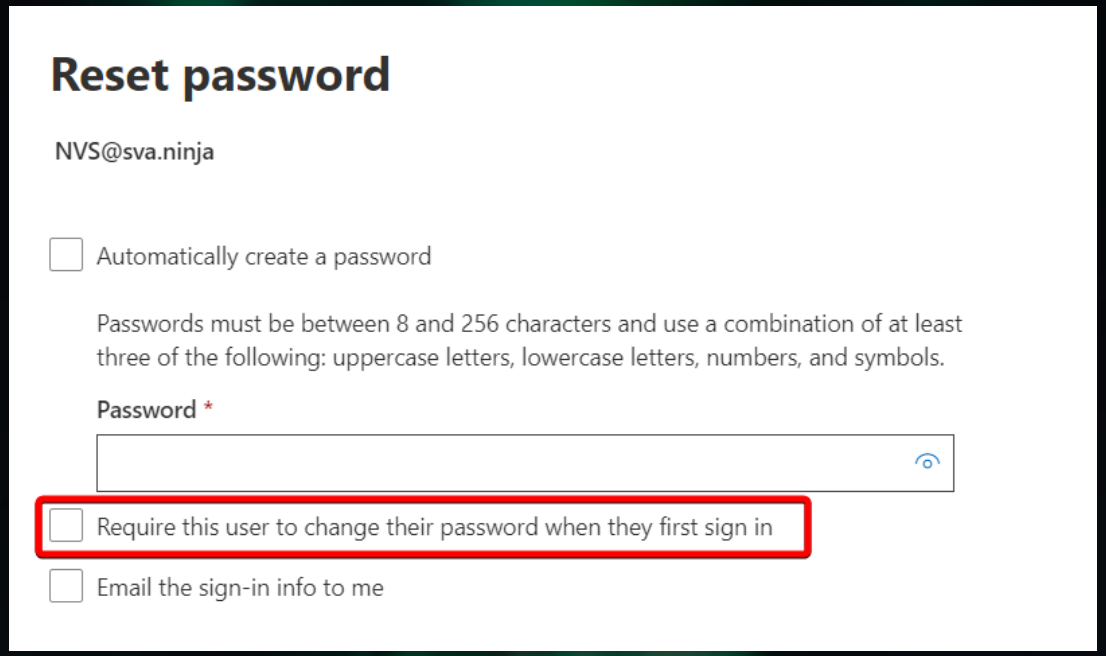


Prepare – Password reset

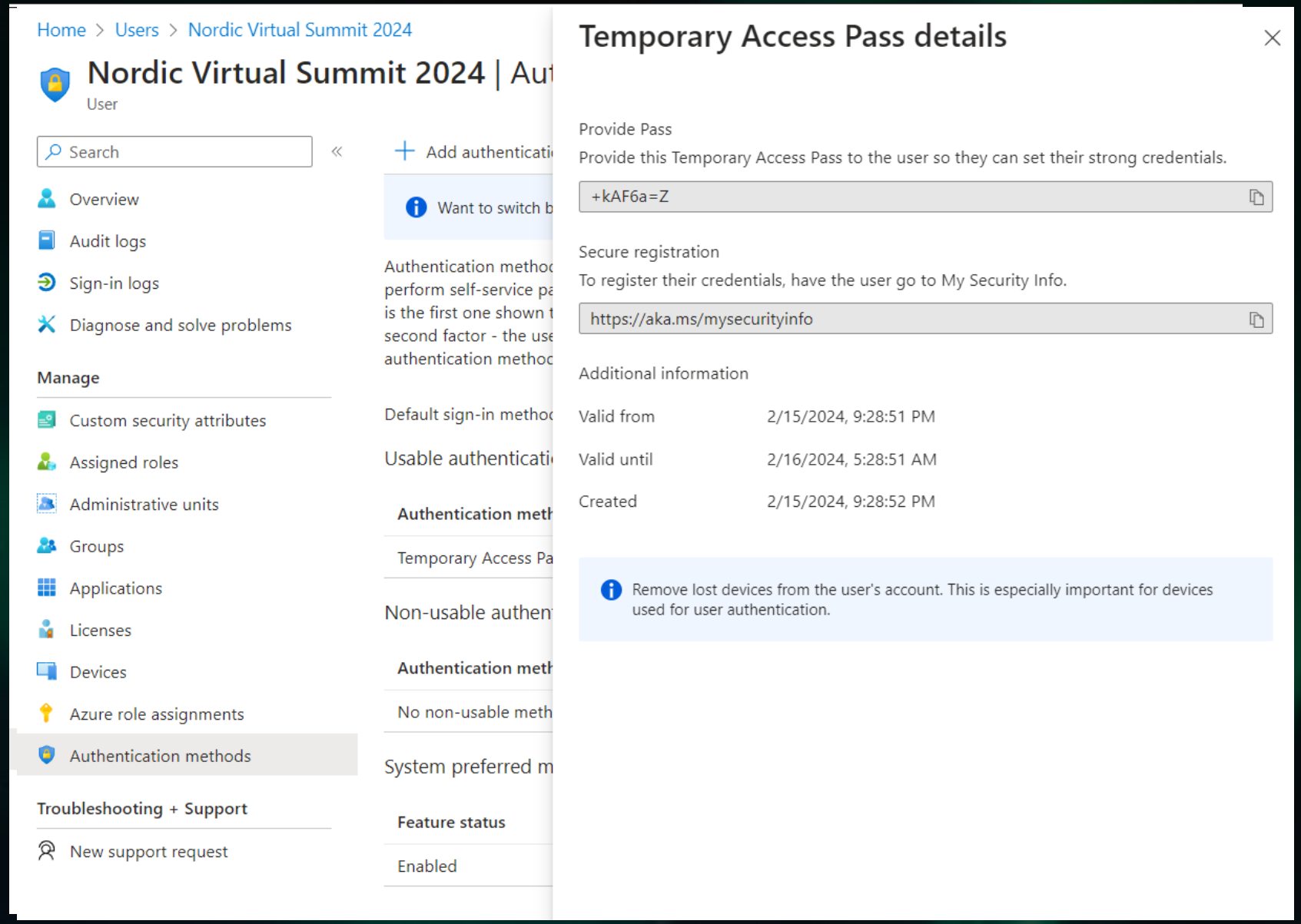


Prepare – Create the user

- Use the admin portal (yes!)
- Create a user with a very long (40+) complex password
- Don‘t require user to change password



Prepare – Create the TAP



NORDIC
– VIRTUAL SUMMIT –

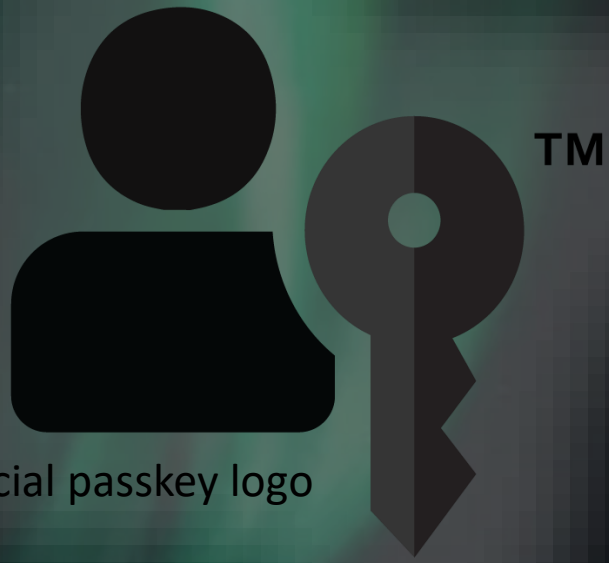
Adoption of passwordless

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



Official passkey logo

Why is it ‘phishing resistant’?

NORDIC
– VIRTUAL SUMMIT –

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

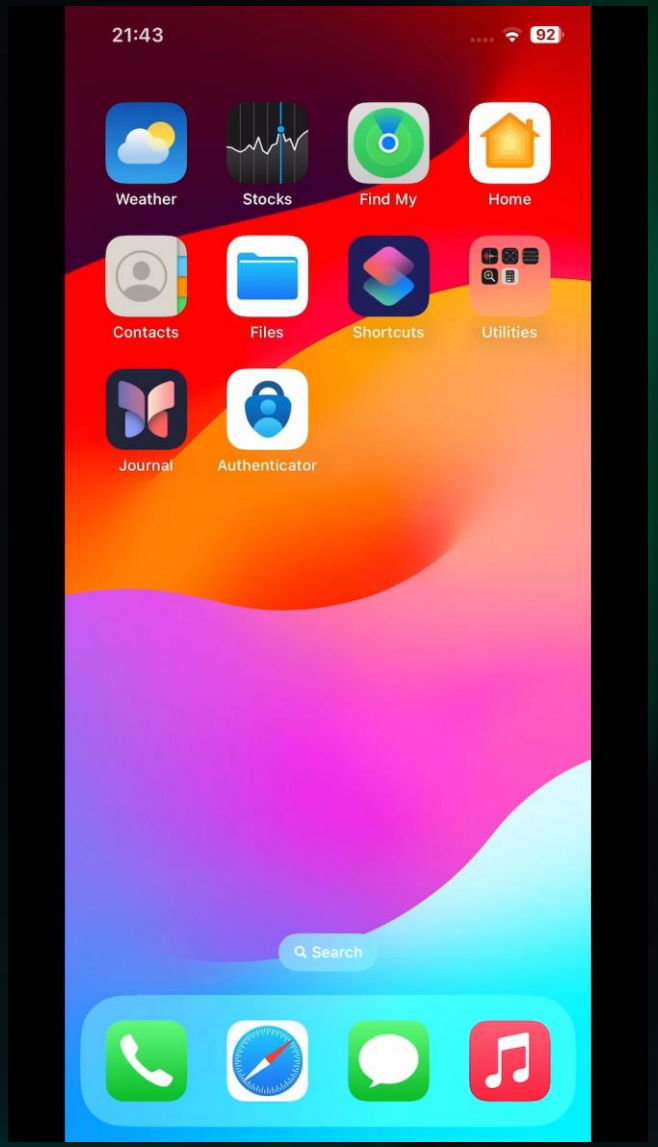
Demo

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

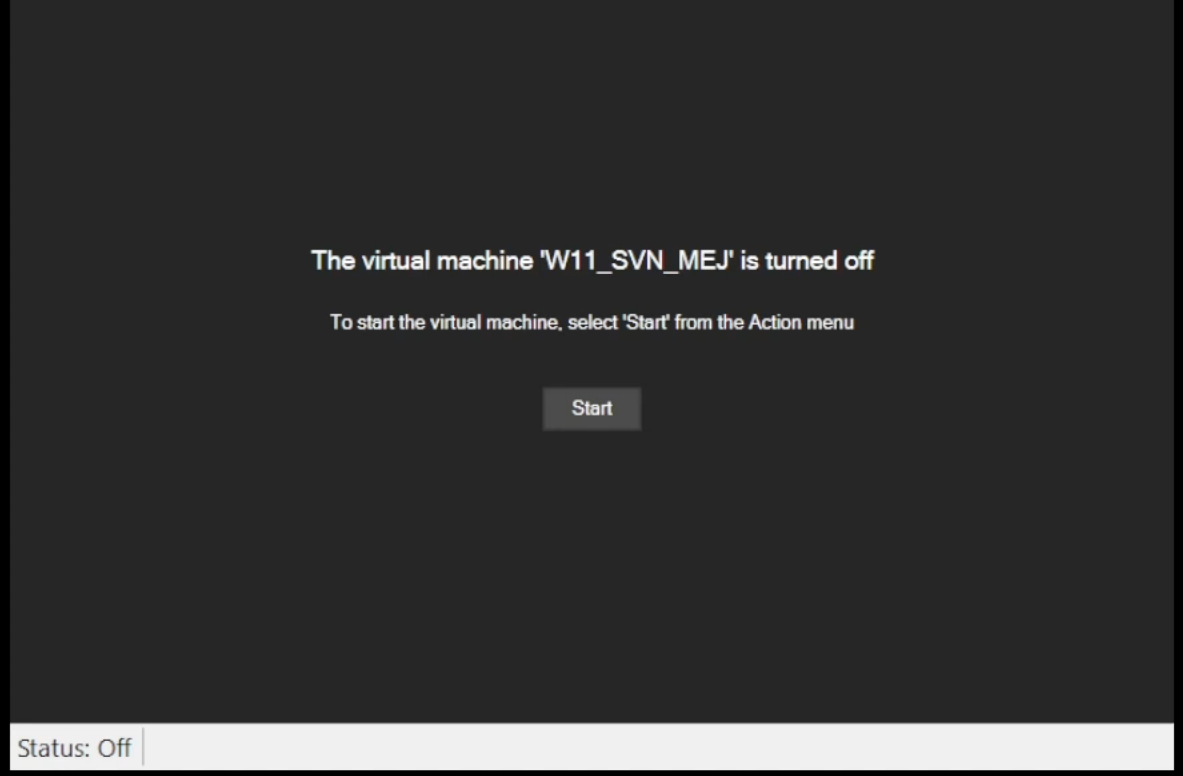


Demo

New Employee Procedure – Computer first

New Employee Procedure – Computer first

- 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
Start
Status: Off

NORDIC
– VIRTUAL SUMMIT –

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/

NORDIC
– VIRTUAL SUMMIT –