NIC REBEL EDITION

10 Security Features you Must Configure in Windows 11

1

3

Windows 11: Secure by default

Our focused security work, driven by observing attacker patterns and behaviors, has resulted in a reported 62% drop in security incidents and a threefold reduction in firmware attacks and 2.9 times fewer instances of identity theft reported.[1]

Windows 11 Survey Report. Techaisle, September 2024. Windows 11 results are in comparison with Windows 10 devices.

NIC REBEL EDITION

4

WINDOWS 11

SECURITY FEATURES

MICROSOFT INTUNE

NIC REBEL EDITION

5

Nicklas Ahlberg

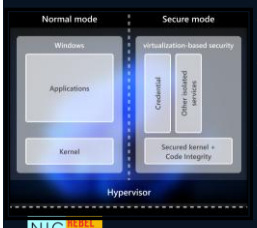
onevinn

NIC REBEL EDITION

6

8

#1 Virtualization-based security (VBS)



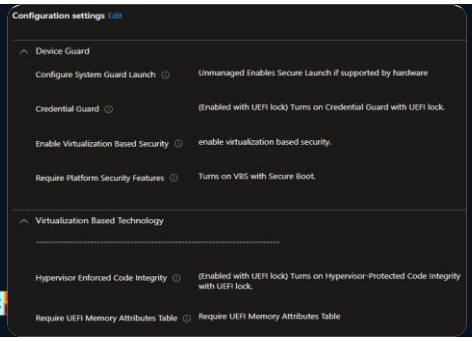
- **Crucial** for a good Windows security posture!
- Creates an isolated virtual environment for increased protection from vulnerabilities in the OS = the **root of trust** if the kernel has been compromised
- Protects security assets such as authenticated user credentials

9

Hardware requirements

- 64-bit CPU
- Second Level Address Translation (SLAT)
- IOMMUs or SMMUs (Intel VT-D, AMD-Vi, Arm64 SMMUs)
- Trusted Platform Module (TPM) 2.0
- Firmware support for SMM protection
- Unified Extensible Firmware Interface (UEFI) Memory Reporting
- Secure Memory Overwrite Request (MOR) revision 2
- Memory integrity-compatible drivers
- Secure Boot

10



11

#2 Windows Hello for Business: Multi-factor unlock

- Require another factor to sign in
- Shoulder surfing 👀
- Passwords and security keys will not require MFU
- Supports: PIN, Facial, Fingerprint and passive (connected to a specific network or Bluetooth device)

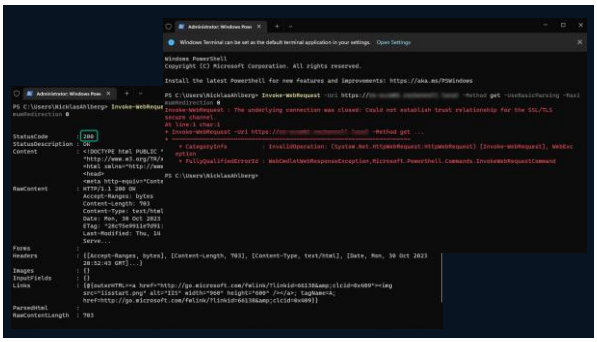
12

#3 Network List Manager

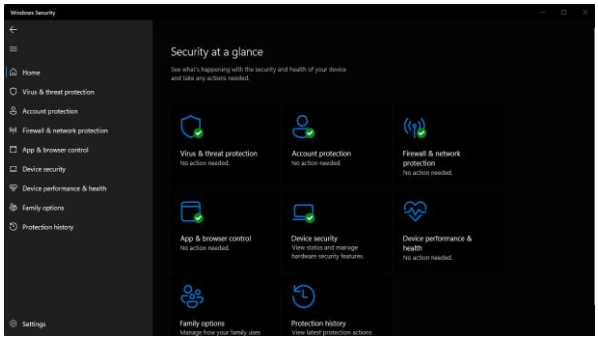
- Location awareness to properly apply Windows Firewall rules, Entra ID-joined devices!
- TLS 1.2 authentication
- Requires the "new" Defender Firewall template

```
$URL = "https://myhost.local"
Invoke-WebRequest -Uri $URL -Method GET -UseBasicParsing -MaximumRedirection 0
```

13



14



15

#4 Credential Guard

Protects against credential theft, such as pass-the-hash

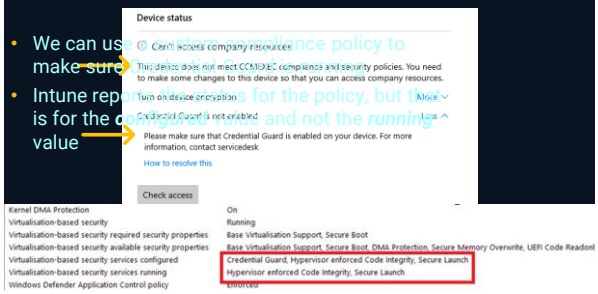
- **New installations:** Enabled by default on W11 (without UEFI lock)
- **Existing installations:** No change when updating to W11
- **Controls:** Security baseline, CSP, Settings Catalog, Account protection
- **UEFI lock:** Block remote disablement (Intune/script/GPO)
- **Hardware requirements:** FW, TPM (1.2 & 2.0), VBS, Secure Boot

Note

While Credential Guard is a powerful mitigation, persistent threat attacks will likely shift to new attack techniques, and you should also incorporate other security strategies and architectures.

16

- We can use a device compliance policy to make sure
- Intune reports on this for the policy, but this is for the configuration and not the *running* value



17

#5 Windows Hello for Business:
Enhanced Sign-in Security

- ESS isolates the biometric data to trusted hardware or memory regions.
- Tamper protection!
- "Impossible" for malware to exploit the bio data to simulate a sign-in
- Utilizes VBS, so don't skip the W11 HW requirements 😁

NIC REBEL EDITION

18

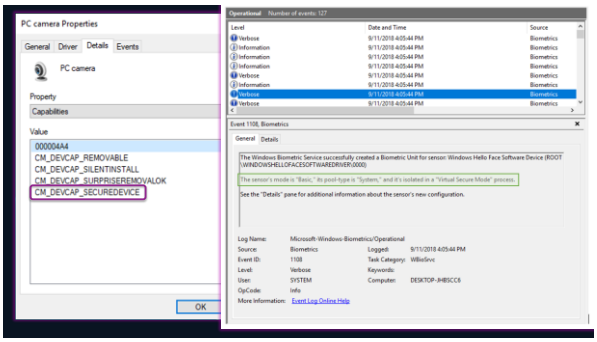
#5 Windows Hello for Business
Enhanced Sign-in Security

Prerequisites

- ❗ All the Windows 11 hardware requirements
- 📷 Internal camera with ESS support
- 👆 Internal fingerprint sensor with ESS support
- 📄 BIOS with ESS support
- 💻 It is clear that our OEM's own the pre-reqs!

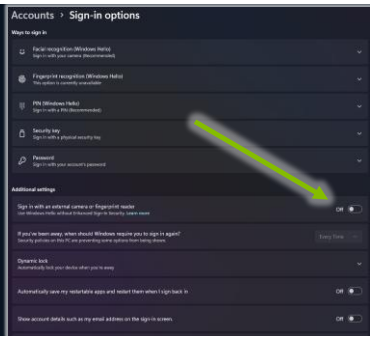
NIC REBEL EDITION

19

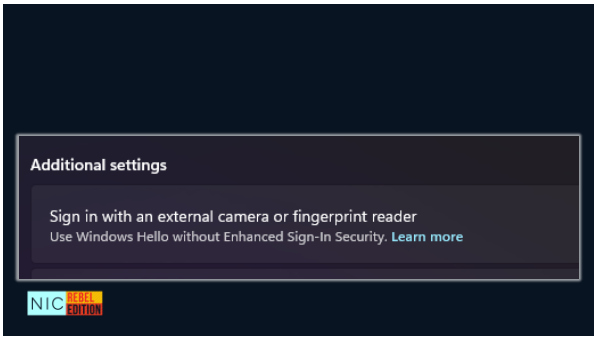


20

- Settings ->
- Accounts ->
- Sign-in options

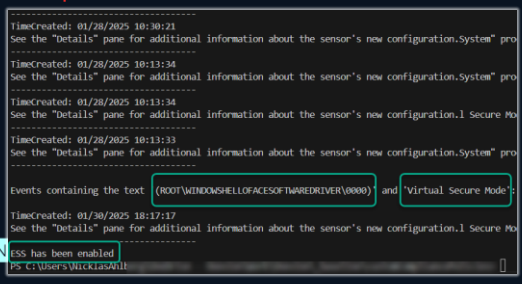


21



22

https://rockenroll.tech



23

Windows ~~Hello~~

Researchers Reveal "Windows Hell No" Vulnerability in Windows Hello Biometric System

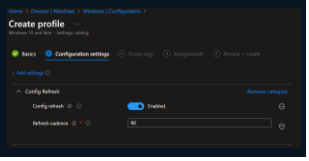
August 8, 2025

Enhanced Sign in Security to the rescue!

24

#6 Config Refresh

- Only Policy CSP!
- Configure a cadence that makes sense
- Offline functionality!
- Ability to pause Config Refresh for troubleshooting purposes



25

26

Yay! Safe from local admin tampering…

🤨 hmm no you are **not**

Config refresh is designed to work with MDM policies managed by the Policy CSP.

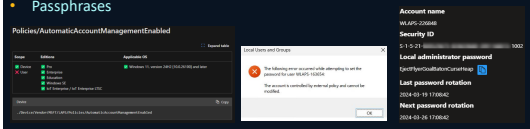
Policies like:

- Firewall
- Applocker
- Personal Device Encryption (PDE)
- Local administrative password solution (LAPS)
- Is not part of drift control

27

#7 Windows LAPS: What's new

- ⭐Automatic account management mode
- Account tampering protection
- Passphrases



28

Policies/AutomaticAccountManagementEnabled

Expand table

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ Windows SE ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 11, version 24H2 [10.0.26100] and later

Device — Copy

```
./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementEnabled
```

29

Policies/AutomaticAccountManagementTarget

Expand table

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ Windows SE ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 11, version 24H2 [10.0.26100] and later

Device — Copy

```
./Device/Vendor/MSFT/LAPS/Policies/AutomaticAccountManagementTarget
```

Use this setting to configure which account is automatically managed.

The allowable settings are:

0=The builtin administrator account will be managed.

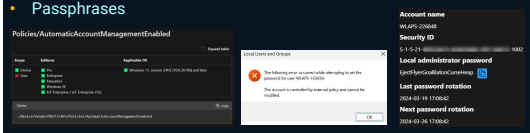
1=A new account created by Windows LAPS will be managed.

If not specified, this setting will default to 1.

30

Windows LAPS: What's new

- Automatic account management mode
- ⭐Account tampering protection
- Passphrases

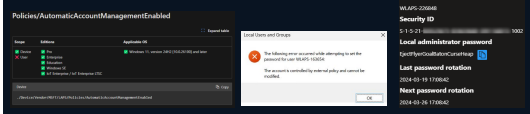


31

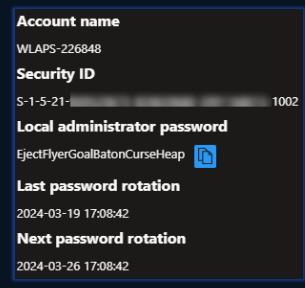
32

Windows LAPS: What's new

- Automatic account management mode
- Account tampering protection
- ⭐Passphrases



33



34

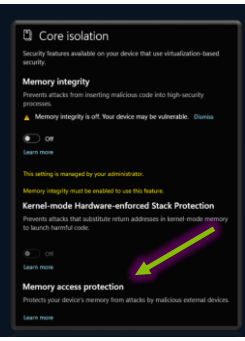
#8 BitLocker PIN

- Protects against DMA port attacks before Windows has booted
- We see more and more customers using BitLocker PIN
- Setting a PIN after Windows provisioning is challenging
- PIN is part of the bitpixie mitigations strategy

35

(Bonus) Kernel DMA Protection

- Protects against DMA attacks, **after** Windows has booted
- Drive-by DMA attacks
- Requires the device/driver to support DMA-remapping (isolated space within memory)
- Enabled by default, if **UEFI** has been configured correctly

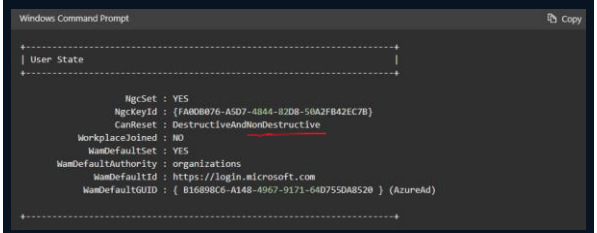


36

#9 Personal Data Encryption Shared computers, sensitive users

- Adds an extra protection layer on personal data(AES-CBC with a 256-bit key.
- Requires Windows Hello for Business (no FIDO support)
- No support for RDP
- Backup needed! – OneDrive!?
  - TPM Reset = data is lost
  - Destructive PIN reset = data is lost

37



38

Personal Data Encryption (PDE)
Requirements

- Windows 11 22H2 or later (known folder encryption 24H2)
- Hybrid Joined or Entra Joined
- Windows editions: Education/Enterprise (Pro is not supported).
- Does not replace BitLocker

39

#10 Enhanced phishing protection

- Ensure that enterprise credentials are not used for malicious or unintended purposes.
  - Notify malicious
  - Notify password reuse
  - Notify unsafe app

💡Use advanced hunting to find related events and educate your users.

```
DeviceEvents
| where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
| extend TriggerReason = parse_json(AdditionalFields).Experience
```

40

Security Baselines / STIGs

Security Baselines

- Security Baseline for Windows 10 and later
- Microsoft Defender for Endpoint Baseline
- Security Baseline for Microsoft Edge
- Windows 365 Security Baseline
- Microsoft 365 Apps for Enterprise Security Baseline

41

- Virtualization Based Security
- Multi Factor Unlock
- Network List Manager
- Credential Guard
- Enhanced sign-in security
- Config Refresh
- Windows LAPS
- BitLocker PIN
- Personal Data Encryption
- Enhanced Phishing Protection

42

Thank you so much for attending!

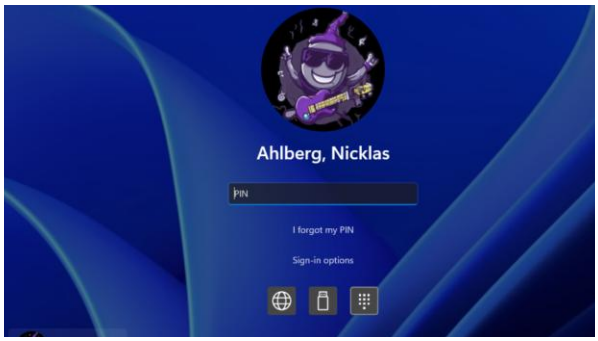
43

#11 Passwordless & Web sign-in

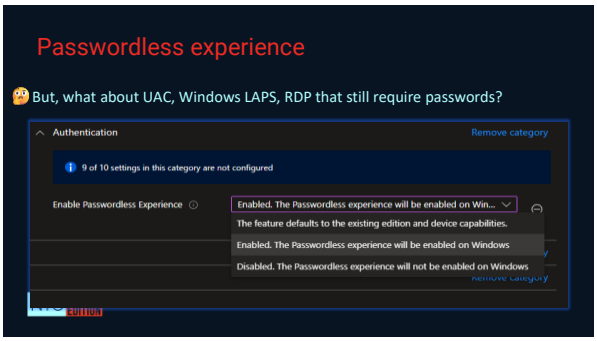
- Windows 11, version 22H2 with **KB5030310** and later
- Supports sign-in using **TAP**
- Windows 11: Sign in with auth app
- Supports **Entra ID-join** only

- 💡More and more customers ask f passwordless!

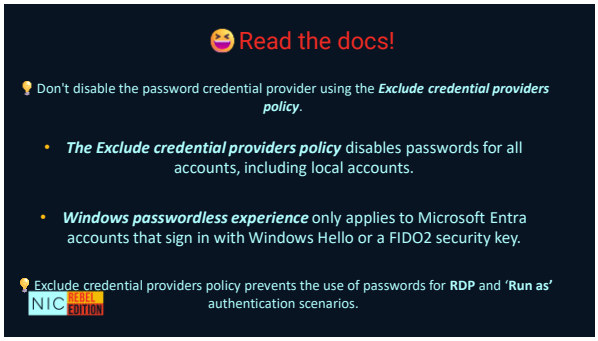
44


Ahlberg, Nicklas
PIN
I forgot my PIN
Sign-in options

45


Passwordless experience
But, what about UAC, Windows LAPS, RDP that still require passwords?
Authentication
Remove category
9 of 10 settings in this category are not configured
Enable Passwordless Experience
Enabled. The Passwordless experience will be enabled on Win...
The feature defaults to the existing edition and device capabilities.
Enabled. The Passwordless experience will be enabled on Windows
Disabled. The Passwordless experience will not be enabled on Windows

46


Read the docs!
Don't disable the password credential provider using the Exclude credential providers policy.
The Exclude credential providers policy disables passwords for all accounts, including local accounts.
Windows passwordless experience only applies to Microsoft Entra accounts that sign in with Windows Hello or a FIDO2 security key.
Exclude credential providers policy prevents the use of passwords for RDP and 'Run as' authentication scenarios.
NIC REBEL EDITION

47