

#POWERCON2023

Microsoft Intune: il braccio operativo della sicurezza sugli endpoint

Riccardo Corna

MVP Security – Senior Consultant

(Coautore: Davide Salsi – MVP Enterprise Mobility)



@itspecialcloud



/riccardocorna

83 %

Organizzazioni che hanno subito almeno 1 attacco negli ultimi 2 anni

25 %

Organizzazioni che hanno identificato l'accesso non autorizzato ai dati sensibili come una delle principali minacce alla sicurezza

90 %

di tutti gli attacchi ransomware riusciti hanno origine da dispositivi non gestiti

Rif: Microsoft Digital Defense Report – October 2023

Agenda

- Zero Trust
- Intune come un «Maestro» d'orchestra
- Perché "Maestro"?
- Band lineup
 - Endpoint Security
 - Threat Defense
 - Identità del device
 - Identità dell'utente
 - Privilegi minimi
- Q&A

Principi Zero Trust



Verifica esplicita

Autenticare e autorizzare sempre verificando l'identità e lo stato del device senza presupporre che questi siano attendibili



Assumere il breach

Segmentare gli accessi per prevenire movimenti laterali e protegge le comunicazioni attraverso la crittografia end-to-end



Privilegi minimi

Limitare l'accesso mediante: accessi "just-in-time" (JIT) e "just-enough-access" (JEA), policy adattive basate sul rischio e protezione dei dati

Microsoft Intune come un «Maestro» d'orchestra



Perché «Maestro» Microsoft Intune?

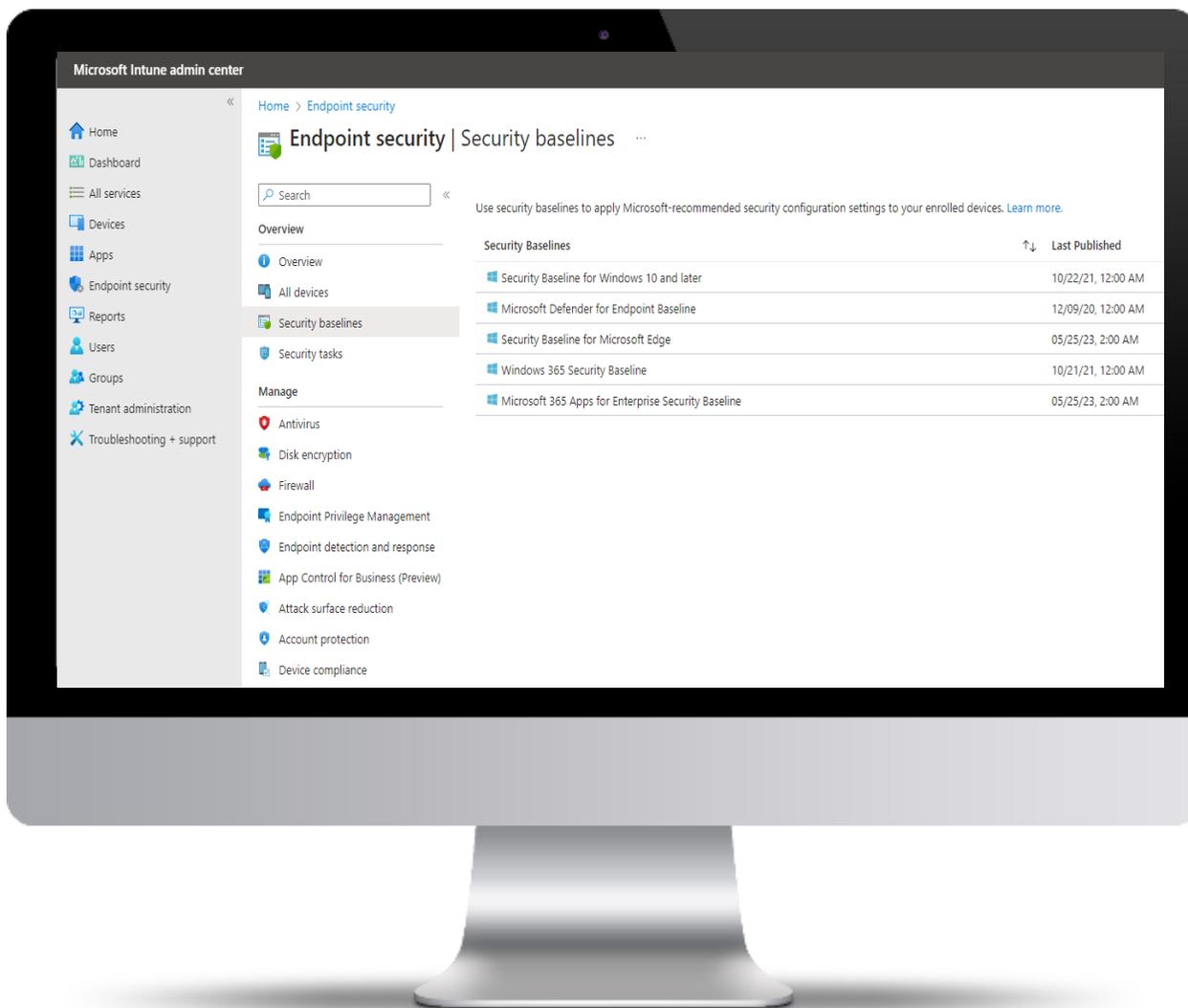
- Perché non serve solo a gestire dispositivi.
- Perché è il braccio operativo degli strumenti di sicurezza Microsoft per gli endpoint:
 - Cosa significa?
 - Molte delle configurazioni e delle informazioni che permettono di "calcolare" lo stato di salute e di sicurezza di un endpoint, sono veicolate da/attraverso Intune.



Endpoint Security

- Scenario:
 - Endpoint Security
- Piattaforme coinvolte:
 - Windows
 - macOS
 - iOS/iPadOS
 - Android
- Sezione:
 - Endpoint Security
 - Devices -> Configuration Profiles
- Strumento musicale:
 - Batteria





Security Baseline

- 01** Insieme di settings per Windows 10 che rappresentano le best practices di Microsoft per la sicurezza e la protezione del sistema operativo, di Edge, Defender for Endpoint, Microsoft 365 Apps e Windows 365
- 02** Vengono rilasciate periodicamente nuove versioni
- 03** Sono il risultato di un confronto da parte del team di security Microsoft con le raccomandazioni del Center for Internet Security (CIS) e di altre organizzazioni

Security Configuration Framework



Il Security Configuration Framework è una serie di raccomandazioni fornite da Microsoft per la configurazione e la conformità dei dispositivi:

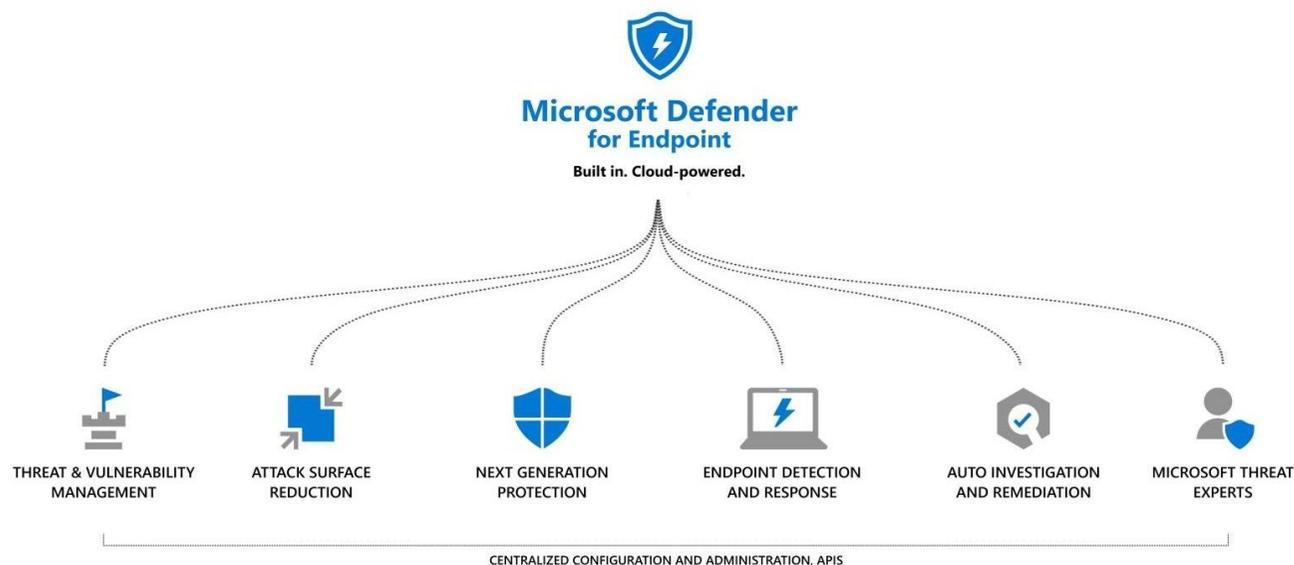
- iOS/iPadOS ([Personal](#) – [Supervised](#))
- Android ([Personal](#) – [Fully Managed](#))
- Suddivide i dispositivi in uno dei seguenti 3 livelli di sicurezza:
 - Basic (solo per device Corporate)
 - Enhanced
 - High

Threat Defense

- Scenario:
 - Threat Defense
- Piattaforme coinvolte:
 - Windows
 - macOS
 - iOS/iPadOS
 - Android
- Sezione:
 - Endpoint Security -> Antivirus
 - Devices -> Configuration Profiles
- Strumento musicale:
 - Chitarra (virtuoso)

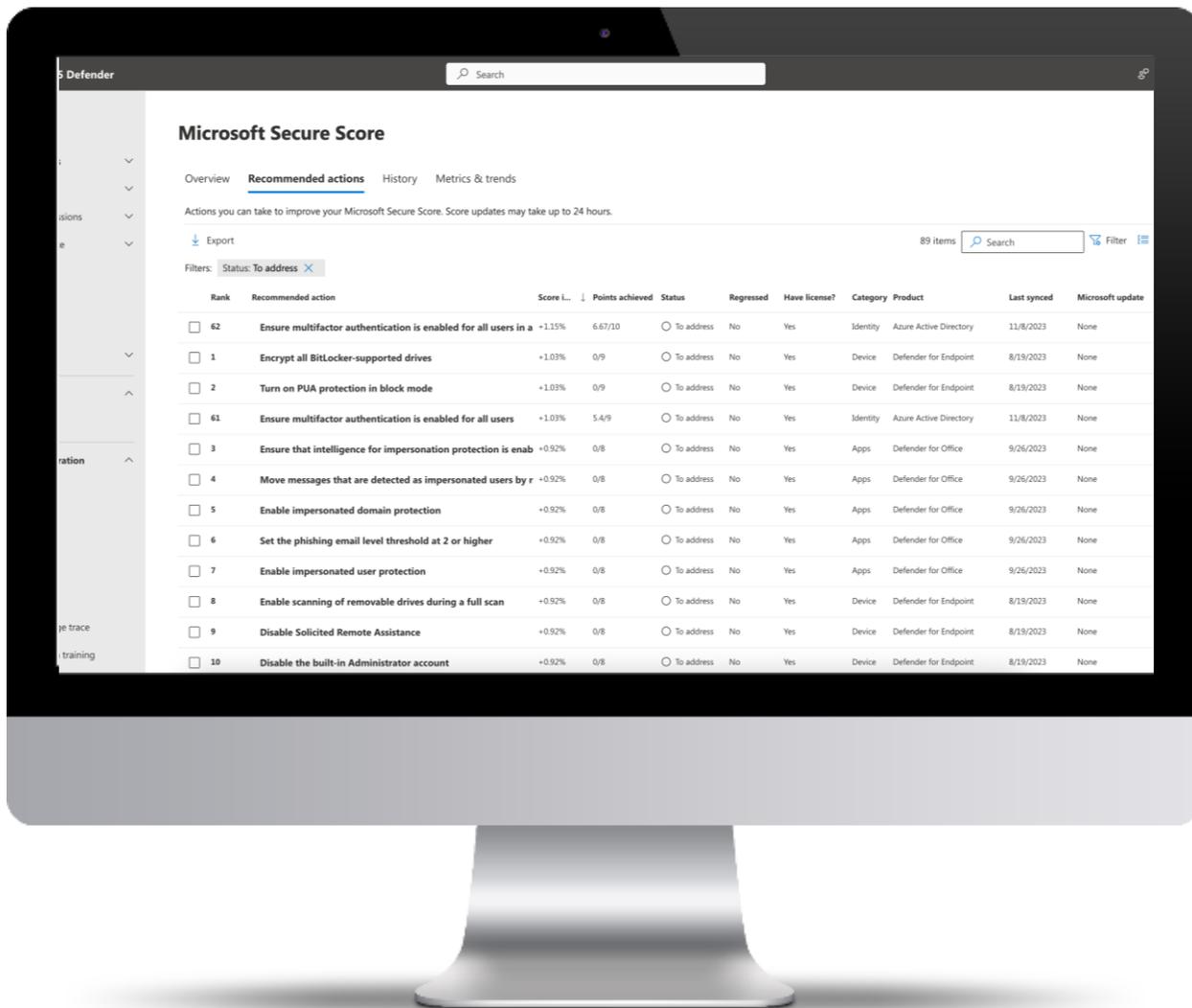


Microsoft Defender for Endpoint



Quali funzionalità e configurazioni di MDE vengono veicolate attraverso Intune?

- Endpoint Detection and Response
- Antivirus
 - Pianificazione scansioni
 - Aggiornamento firme
 - Esclusioni
 - Tanto altro 😊
- Attack Surface Reduction (ASR) Rules
- Account protection
- Web Protection (iOS e Android)



Piano di hardening

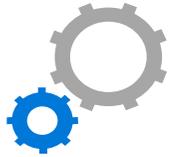
- 01** Il sensore di MDE analizza le configurazioni di macchina e l'ambiente circostante
- 02** I dati vengono analizzati dall'intelligenza del cloud Microsoft
- 03** Viene generato un elenco di azioni raccomandate per aumentare la postura di sicurezza
- 04** Si distribuiscono le configurazioni per implementare le remediation... con Intune!

Identità del device

- Scenario:
 - Identità del device
- Piattaforme coinvolte:
 - Windows
 - macOS
 - iOS/iPadOS
 - Android
- Sezione:
 - Devices -> Compliance Policies
 - Devices -> Conditional Access
 - Apps -> App protection policies
- Strumento musicale:
 - Chitarra (ritmica)

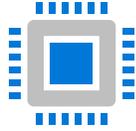


Compliance Policy



Configurazioni device

Esempio: richiesta PIN, encryption, ecc..



Caratteristiche OS

Esempio: versione min/max OS, integrità device, ecc...



Sicurezza app installate

Esempio: app installate da fonti sconosciute, ecc...



Livello di minaccia

Esempio: livello rischio determinato da MDE

- Regole e impostazioni che un dispositivo deve rispettare per essere considerato **conforme allo standard aziendale**
- Possono essere utilizzate per **monitorare e risolvere** le situazioni di difformità
- Possono essere sfruttate dal servizio di **Conditional Access**

Conditional Access

- Come interviene Intune nel Conditional Access oltre alla conformità?
- Filtri dispositivo
 - Possiamo definire dei filtri per includere o escludere dispositivi con specifiche proprietà
 - I filtri possono essere definiti anche tenant-wide dal menu

Tenant administration -> Filters

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure ⓘ

Yes No

Devices matching the rule:

Include filtered devices in policy

Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	<input type="text"/>	<input type="text"/>	<Pick a property and operator first>

+ Add express

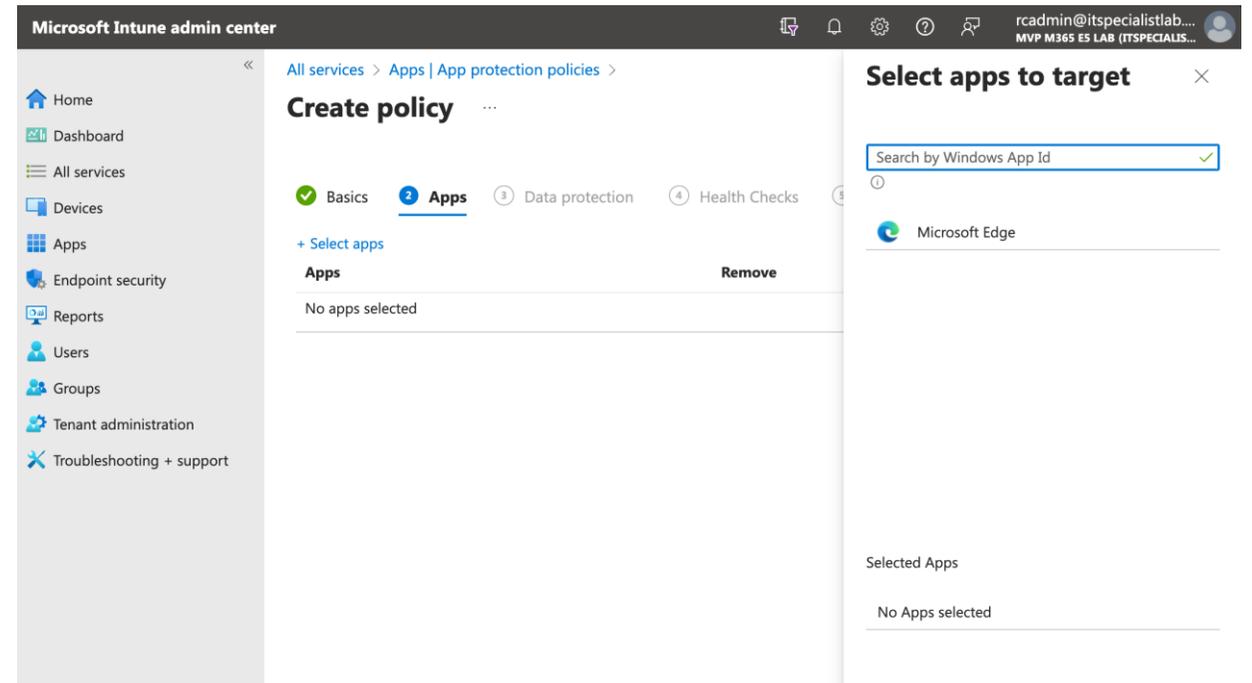
Rule syntax ⓘ

- DeviceId
- DisplayName
- DeviceOwnership
- EnrollmentProfileName
- IsCompliant
- Manufacturer
- MdmAppId
- Model
- OperatingSystem

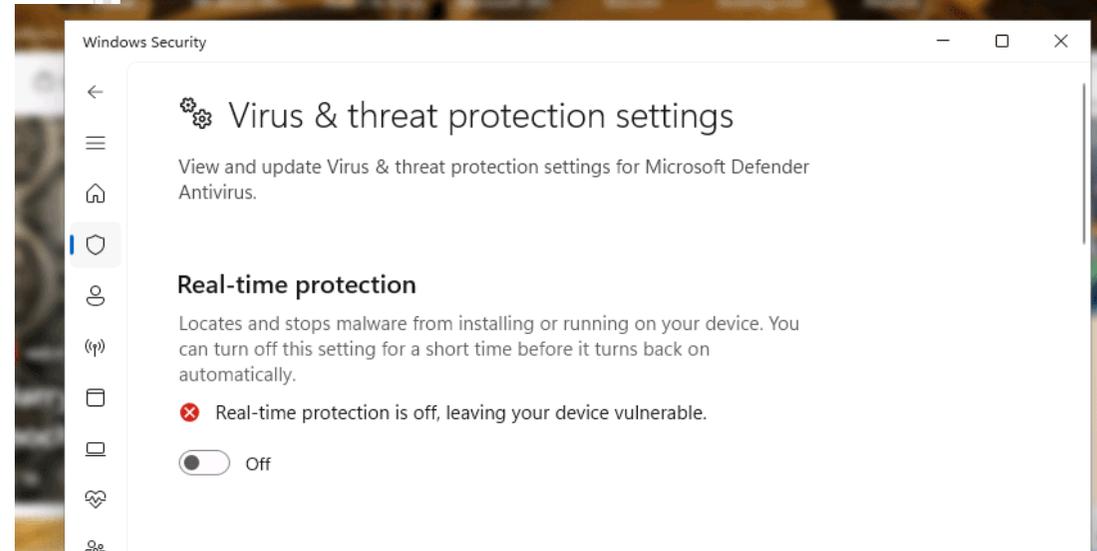
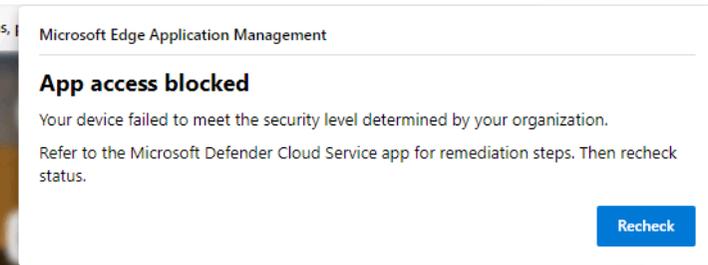
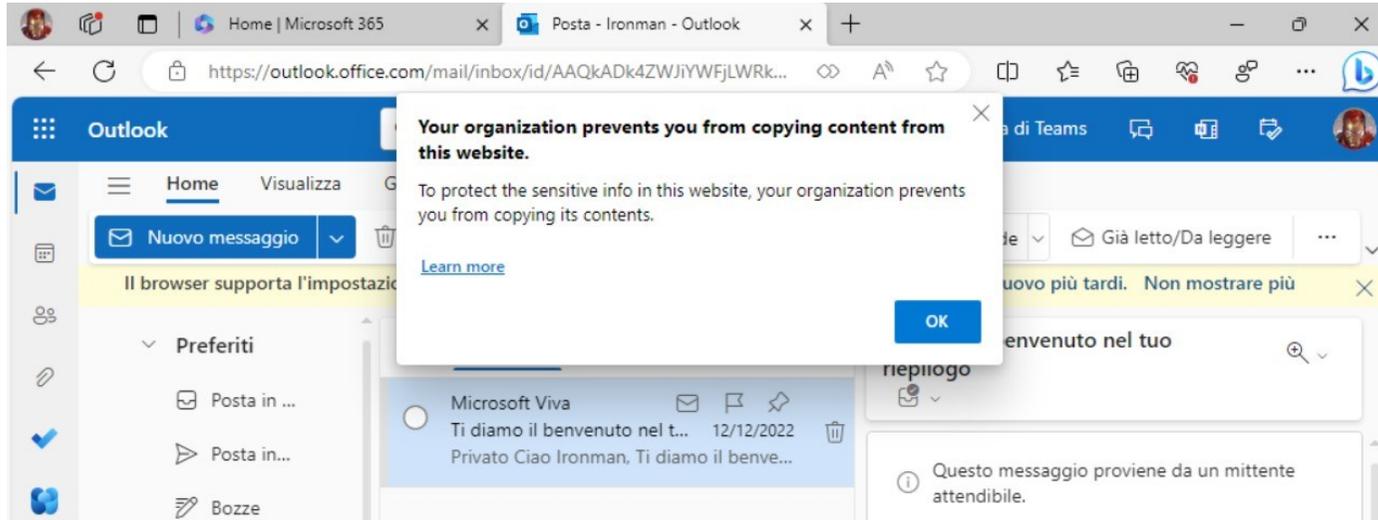
[Edit](#)

MAM per Windows

- Nuova funzionalità da poco in GA
- Supera alcuni limiti che aveva WIP
- Aiuta a separare in maniera chiara dati utente dai dati lavorativi
- Esperienza MAM simile a quella dei dispositivi mobile
- Il comportamento dell'app dipende esclusivamente dall'identità usata dall'utente



MAM per Windows



Identità dell'utente

- Scenario:
 - Identità dell'utente
- Piattaforme coinvolte:
 - Windows
- Sezione:
 - Devices -> Configuration Profiles
 - Endpoint Security -> Account Protection
- Strumento musicale:
 - Voce



Passwordless

- Quali funzionalità e impostazioni passano da Intune per un'esperienza passwordless?
- Windows Hello for Business
- Abilitazione Web Sign-In (+ TAP)
- Self Service Password Reset da login Windows
- NOVITÀ: Passwordless experience

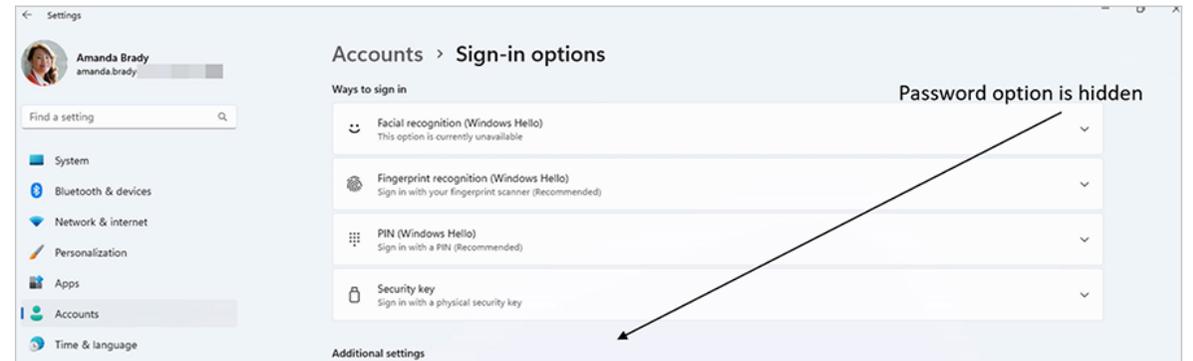
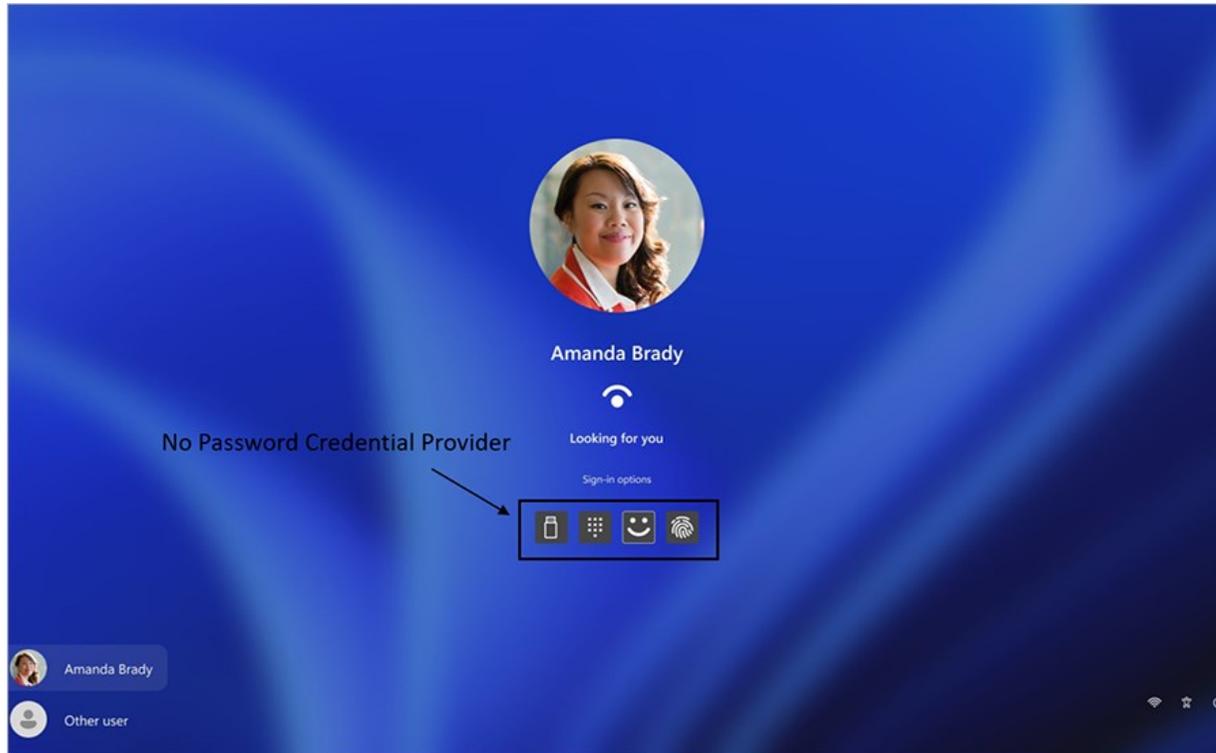


Passwordless Experience

- Gli utenti che accedono con WHfB o una chiave FIDO2:
 - Non possono utilizzare la password sulla schermata di blocco di Windows.
 - Non vengono sollecitati a utilizzare una password durante autenticazioni in sessione (elevazione UAC, gestore password nel browser, ecc.).
 - Non hanno l'opzione "Account > Cambia password" nelle Impostazioni.
- Non impatta account locali
 - Utile se l'admin locale sotto LAPS deve fare help-desk
- È comunque permesso ad un utente di accedere con password quando utilizza l'opzione *Altro utente* nella schermata di blocco.
- Il provider di credenziali della password è nascosto solo per l'ultimo utente che ha effettuato l'accesso con WHfB o una chiave FIDO2
- La Passwordless Experience di Windows non mira a impedire agli utenti di usare le password, ma piuttosto a guidarli ed educarli nel ridurre il suo utilizzo

The screenshot shows the Windows Settings application in the 'Create profile' section, specifically the 'Configuration settings' tab. The 'Authentication' category is expanded, showing a notification that 9 of 10 settings are not configured. The 'Enable Passwordless Experience (Windows Insiders only)' setting is selected, and a dropdown menu is open, displaying four options: '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', and 'Disabled. The Passwordless experience will not be enabled on Windows'. On the right side, the 'Settings picker' is visible, showing a search bar and a list of categories including 'Authentication', which is currently selected. Below the categories, a list of 10 settings in the 'Authentication' category is shown, with 'Enable Passwordless Experience (Windows Insiders only)' checked.

Passwordless Experience



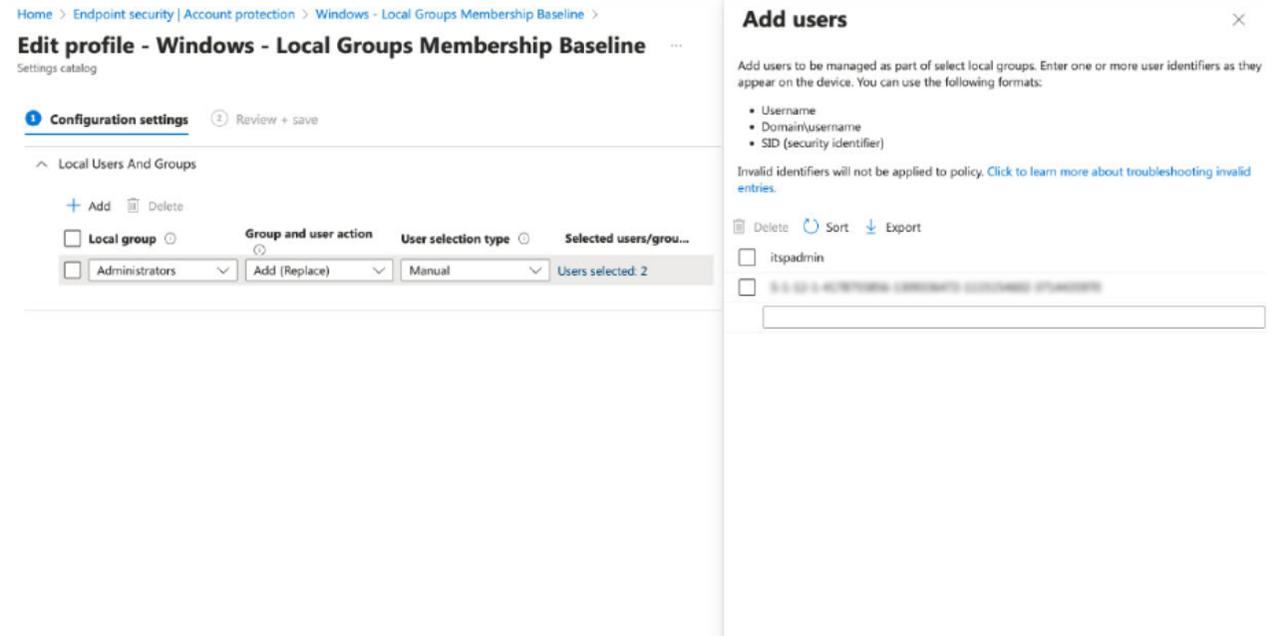
Privilegi Minimi

- Scenario:
 - Privilegi Minimi
- Piattaforme coinvolte:
 - Windows
- Sezione:
 - Endpoint Security -> Account protection
 - Endpoint Security -> Endpoint Privilege Management
- Strumento musicale:
 - Basso



Local User Group Policy

- Un utente che joina manualmente il proprio client ad Entra ID, diventa amministratore di macchina
- Inoltre, chi ha ruolo Global Admin o di Entra Joined Device Local Administrator, è amministratore
- Con le Local User Group Policy possiamo aggiungere, rimuovere o aggiornare le membership dei gruppi locali di macchina!



Windows LAPS

The screenshot shows the Microsoft Endpoint Security console. On the left, the navigation pane is visible with 'Account protection' selected. The main area shows a search for profiles with 'No results'. A 'Create a profile' dialog box is open, showing the following configuration:

- Platform: Windows 10 and later
- Profile: Select a profile
- Local user group membership: Local admin password solution (Windows LAPS) (highlighted with a red box)
- Account protection (Preview)

- Soluzione di Just in Time (JIT) local admin password
- Le password sono quindi:
 - Uniche per ogni sistema
 - Generate casualmente
 - Memorizzate in Entra ID o in Active Directory
- Architettura basata su:
 - Group Policy Client Extension (AD)
 - Endpoint Security Policy (Intune)

Windows LAPS - configurazione

- Backup password:
 - Azure AD
 - Active Directory
- Complessità password
- Lunghezza password
- Azioni post-autenticazione
 - Reset password
 - Reset password + Logoff
 - Reset password + Reboot

The screenshot displays the 'Create profile' configuration page for Windows LAPS, specifically the 'Configuration settings' step. The breadcrumb trail is 'Home > Endpoint security | Account protection > Create profile ...'. Below the title, it says 'Local admin password solution (Windows LAPS)'. The progress bar shows five steps: 1. Basics (checked), 2. Configuration settings (active), 3. Scope tags, 4. Assignments, and 5. Review + create.

The 'LAPS' section is expanded, showing several configuration options:

- Backup Directory**: A dropdown menu currently set to 'Not configured'. The options are: 'Not configured', 'Disabled (password will not be backed up)', 'Backup the password to Azure AD only', and 'Backup the password to Active Directory only'.
- Administrator Account Name**: A text input field.
- Password Complexity**: A dropdown menu currently set to 'Not configured'. The options are: 'Not configured', 'Large letters', 'Large letters + small letters', 'Large letters + small letters + numbers', and 'Large letters + small letters + numbers + special characters'.
- Password Length**: A text input field with a red asterisk indicating a required field.
- Post Authentication Actions**: A dropdown menu currently set to 'Not configured'. The options are: 'Not configured', 'Reset password: upon expiry of the grace period, the managed account password will be reset.', 'Reset the password and logoff the managed account: upon expiry of the grace period, the managed ...', 'Reset the password and reboot: upon expiry of the grace period, the managed account password will ...', and 'Not configured'.
- Post Authentication Reset Delay**: A text input field with a red asterisk indicating a required field.

Privilegi minimi - Use Case

Applicazione legacy installata sul device che richiede privilegi elevati per scrittura su folder e/o chiavi di registry di sistema



Privilegi minimi (Soluzioni disponibili)

- Local Admin



Local Admin

PRO:

- Massima (troppa) autonomia agli utenti



CONTRO:

- Elevata esposizione a compromissioni
- Possibilità di modifiche a basso livello
- Installazione/esecuzione di software autorizzato



Privilegi minimi (Soluzioni disponibili)

- Local Admin
- Windows LAPS



Windows LAPS

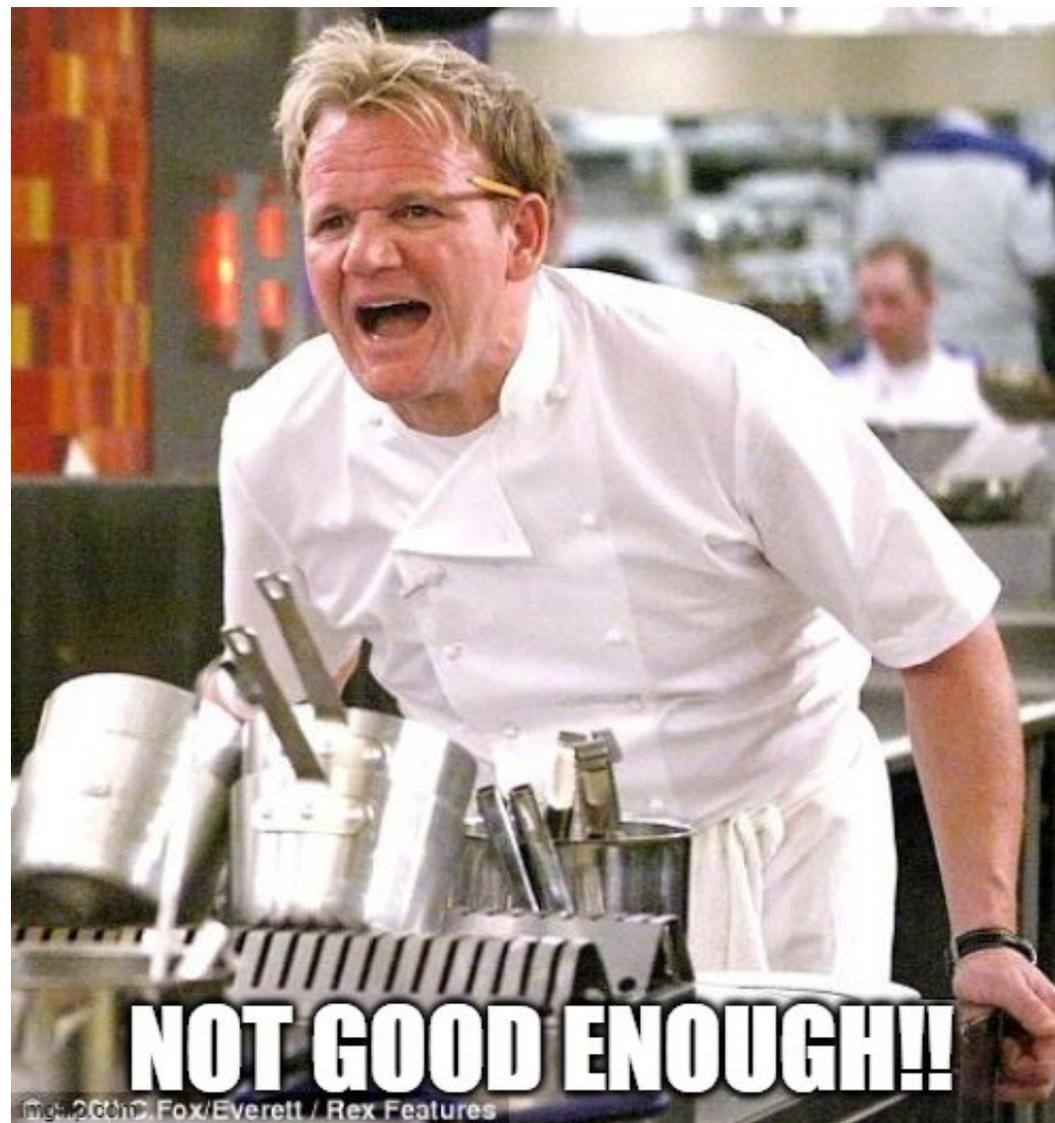
PRO:

- Processo di autorizzazione controllato
- Rotazione della password admin locale



CONTRO:

- Necessario un gruppo di lavoro IT
- Possibilità di esecuzione di qualsiasi processo
- Effort di implementazione su AD *



Privilegi minimi (Soluzioni disponibili)

- Local Admin
- Windows LAPS
- Endpoint Privilege Management



Endpoint Privilege Management

PRO:

- Processo di autorizzazione controllato
- Possibilità di eseguire di specifici processi con privilegi
- Ridotto consumo di RAM per l'esecuzione
- "Integrato" nel sistema operativo



CONTRO:

- Definizione preventiva delle regole



What's New Ignite 2023

The graphic features a vibrant, abstract background with flowing, wavy lines in shades of yellow, orange, red, and purple. The text 'Microsoft Ignite' is centered on the left side of this graphic.

**Microsoft
Ignite**

Microsoft Cloud PKI

- Cloud-based Public key infrastructure (PKI)
- Permette di semplificare la gestione dei certificati:
 - Rimozione dei server on-premise
 - Possibilità di rilascio certificati su multi-piattaforma (Windows, iOS, macOS, Android)
 - Riduzione costi legati a servizi come Network Device Enrollment Service (NDES) e reverse proxy

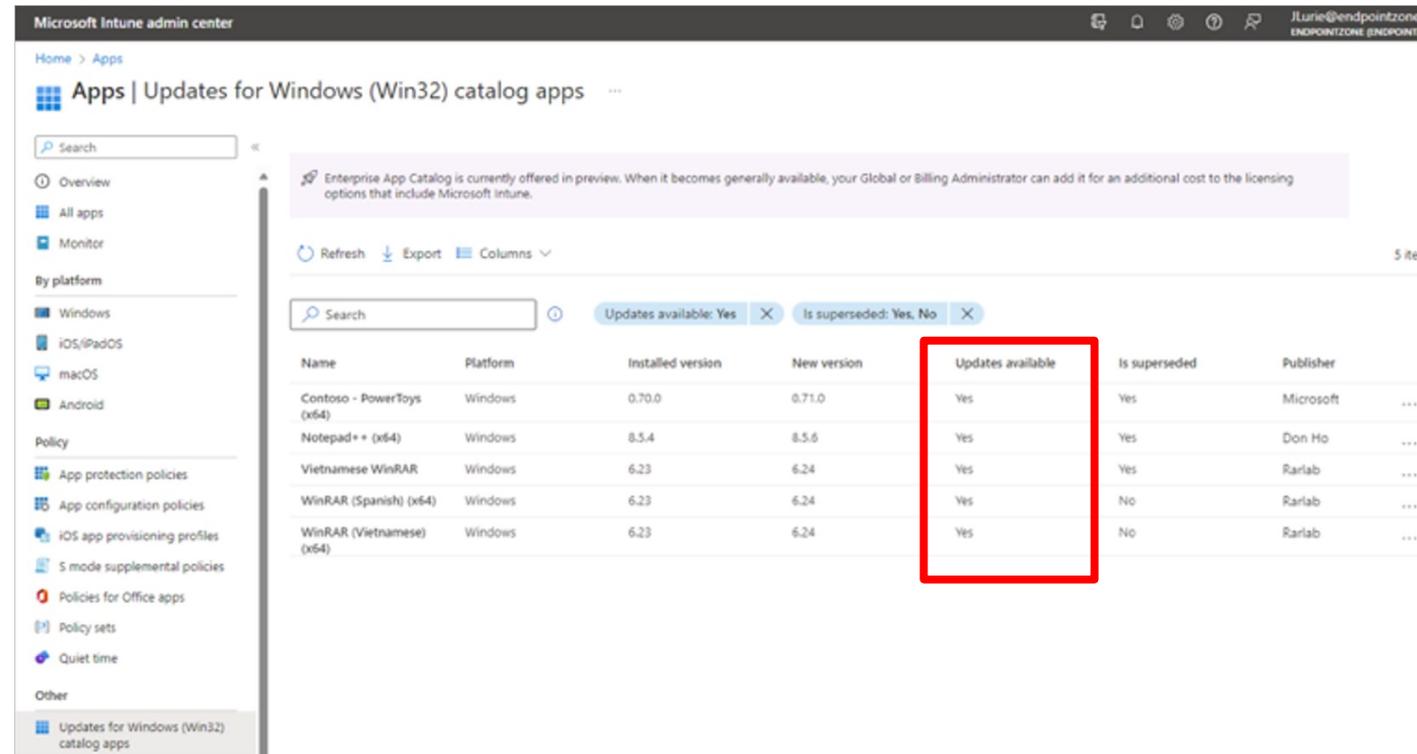
The screenshot shows the 'Create certification authority' page in the Microsoft Intune admin center. The page is divided into three tabs: 'Basics', 'Configuration settings', and 'Review + create'. The 'Configuration settings' tab is active. The page includes a navigation sidebar on the left with options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create certification authority' and contains the following fields and sections:

- About root and issuing certificate authorities (CAs):** A note stating that a root CA must be created before an issuing CA can be created, and that multiple issuing CAs can be contained by a root CA.
- CA type:** A dropdown menu set to 'Issuing CA'.
- Root CA:** A dropdown menu showing 'Contoso Corp Root CA' with a close button (X).
- Common name (CN):** 'Contoso Corp Root CA'.
- Status:** 'active'.
- Validity period:** A dropdown menu set to '10 years'.
- Subject attributes:** A section for providing details to help identify the certification authority.
 - Common name (CN):** 'Contoso corp Issuing CA'.
 - Organization (O):** 'Contoso corporation'.
 - Organizational unit (OU):** 'IT'.
 - Country (C):** 'United States'.
 - State or province (ST):** 'New York'.
 - Locality (L):** 'NY'.
- Encryption:** A section for key size and algorithm, with a dropdown menu set to 'RSA-4096 and SHA-512'.

At the bottom of the page, there are 'Back' and 'Next' buttons.

Enterprise App Management

- Il ritardo nell'applicazione delle patch e nell'aggiornamento delle applicazioni è una delle principali vulnerabilità a cui sono esposte le aziende
- Semplifica il ciclo di vita della gestione delle applicazioni
- Riduce l'effort da parte degli IT Admin nella creazione e nell'aggiornamento delle app



Microsoft Intune admin center

Home > Apps

Apps | Updates for Windows (Win32) catalog apps

Enterprise App Catalog is currently offered in preview. When it becomes generally available, your Global or Billing Administrator can add it for an additional cost to the licensing options that include Microsoft Intune.

Refresh Export Columns

Search

Updates available: Yes Is superseded: Yes, No

Name	Platform	Installed version	New version	Updates available	Is superseded	Publisher
Contoso - PowerToys (x64)	Windows	0.70.0	0.71.0	Yes	Yes	Microsoft
Notepad++ (x64)	Windows	8.5.4	8.5.6	Yes	Yes	Don Ho
Vietnamese WinRAR	Windows	6.23	6.24	Yes	Yes	Rarlab
WinRAR (Spanish) (x64)	Windows	6.23	6.24	Yes	No	Rarlab
WinRAR (Vietnamese) (x64)	Windows	6.23	6.24	Yes	No	Rarlab

Security Copilot + Intune

- Security Copilot è una piattaforma basata su cloud AI che offre un'esperienza basata su linguaggio naturale
- Può aiutare i professionisti della sicurezza in diversi scenari: incident response, threat hunting e raccolta di informazioni
- Come funzionerà insieme ad Intune?
 - Prompt specifici innescheranno la cooperazione con Intune
 - Nelle prossima slide alcuni esempi



Security Copilot + Intune (Policy)

The screenshot displays the Microsoft Intune management console. The left sidebar contains navigation options: Home, Dashboard, Devices (selected), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Devices | Configuration' and shows a list of policies under the 'Policies' tab. The table below lists these policies.

Policy name ↑	Platform	Policy type	Scope tags
Amit Work Laptop	Intune	Personal	Windows
Brooklyn-Office	Co-managed	Corporate	Windows
Bart-Office	Intune	Personal	Windows
Brooklyn-Office	Co-managed	Corporate	Windows
Cameron-Work	Intune	Personal	Windows
david_AndroidForWork	Intune	Corporate	Windows
DESKTOP-D86AGTG	Intune	Personal	Windows
DESKTOP-OMM7MAH	Intune	Personal	Windows
DESKTOP-V60FCT9	Intune	Personal	Windows
Doyle-Work	Intune	Corporate	Windows
Esther-Main	Intune	Personal	Windows
FISH-21H1-G2-1	Intune	Personal	Windows
FISH-21H1-G2-3	Intune	Personal	Windows
HOLELENS-9VQCE2	Intune	Corporate	Windows
Jacob-Work	Intune	Corporate	Windows

On the right, a 'Security Copilot' panel shows a generated policy: 'Create a policy that blocks users from using any removable storage devices on Windows 11 laptops'. The generated policy configuration is as follows:

- Setting: All Removeable Storage classes: Deny...

Below the configuration, there is a 'Create policy' button and a note: 'AI-generated content may be incorrect'. At the bottom of the panel, there is a text input field 'Ask about policies ...' with a search icon.

Security Copilot + Intune (Policy)

The screenshot displays the Microsoft Intune Security Copilot interface. The main content area shows the configuration for a policy named "Removable drive policy [new]". The policy description is "Block users from using any removable storage devices on Windows11 laptops" and it is targeted at "Windows 10 or later".

Configuration settings:

- Administrative Templates: System > Removable Storage Access
- Allow removable storage device *: Disabled

Scope tags:

- Selected tags: Default

Assignments:

Included Groups:

Groups	Group members	Filter	Filter mode
NorAm HQ	468 devices, 218 users	None	None

Excluded Groups:

- Groups: No results

Security Copilot Overview:

This policy is designed to block users from using any removable storage devices on Windows11 laptops, and will effectively block access to removable storage devices for the targeted devices.

Conflicts:

A policy conflict has been detected. You already have a policy for these devices that may conflict with this policy. Please review before deploying.

Policy ↑	Value
Removable drive policy [new]	Disabled
Marketing removable drive override policy	Enabled

User impact:

- Limited Flexibility
- Potential Workflow Disruptions

Security impact:

- Enhanced Security
- Compliance

Buttons: Previous, Review + create, Give feedback, Summarize this policy, Share report, Ask about this policy ...

Security Copilot + Intune (Remediation)

The screenshot displays the Microsoft Intune web interface. The left sidebar contains navigation options: Home, Dashboard, Devices (selected), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Devices | Configuration' and shows the 'Policies' tab. A table lists 128 policies, with the following data visible:

Policy name	Platform	Policy type	Scope tags
Amit Work Laptop	Intune	Personal	Windows
Brooklyn-Office	Co-managed	Corporate	Windows
Bart-Office	Intune	Personal	Windows
Brooklyn-Office	Co-managed	Corporate	Windows
Cameron-Work	Intune	Personal	Windows
david_AndroidForWork	Intune	Corporate	Windows
DESKTOP-D86AGTG	Intune	Personal	Windows
DESKTOP-OMM7MAH	Intune	Personal	Windows
DESKTOP-V60FCT9	Intune	Personal	Windows
Doyle-Work	Intune	Corporate	Windows
Esther-Main	Intune	Personal	Windows
FISH-21H1-G2-1	Intune	Personal	Windows
FISH-21H1-G2-3	Intune	Personal	Windows

On the right, the 'Security Copilot' panel is active, showing suggestions for policy remediation as of November 15, 3:55 PM. The suggestions include:

- "Summarize the policy Contoso Windows 10 security."
- "Which existing Windows 10 configuration policies contain encryption related settings?"
- "Which Intune settings are available to hide the shutdown button on the start menu?"
- "Which Intune settings are available to hide the shutdown button on the start menu?"
- "Generate a policy that hides the shutdown button on the start menu."

SIGNORI



E' STATO UN ONORE SUONARE CON VOI

Seguiteci!

**Microsoft
Security
Italian User
Group**



**Microsoft Intune
Italian User
Group**



**AVD & W365
Italian User
Group**



ITSpecialist.cloud



Grazie

Riccardo Corna

MVP Security – Senior Consultant



@riccardocorna



/riccardocorna