

RESOL/E

by ErgonGroup

PRIMA DI INIZIARE



Controlla che l'audio del tuo microfono
e la videocamera siano disattivati



/ Digital

MASTERCLASS

Empowering Intune e Entra ID

MER 27/11 | 14:30-16:00

RESOL/E

/ RESOLVE

Siamo parte di ErgonGroup:

Nata nel 2006 come “**società del sapere**”, con gli anni e l’esperienza **ErgonGroup** ha sviluppato un know-how sempre più esteso in risposta alle esigenze di **persone, aziende, enti e istituzioni** che necessitano di crescere colmando gap, acquisendo tecnologie, sviluppando eccellenze individuali, di team e di organizzazione.

Oggi ci presentiamo come una **Holding che conta 3 brand**:
Resolve SB Srl, Upskill by ErgonGroup Srl, JObros Srl.

Upskill, Società **specializzata nella formazione e nei servizi formativi**. Grazie alla storia, all’esperienza e alla forza di ErgonGroup, da oltre 15 anni Upskill accompagna aziende, persone e istituzioni nello sviluppo di percorsi di alta **formazione manageriale**, fianco a fianco in tutte le fasi del processo formativo.

JObros, **Agenzia per il lavoro non convenzionale**. JObros accompagna persone e imprese nella loro crescita: affianca gli **HR** nella selezione, inserimento e creazione di talenti in azienda e supporta le **persone** nell’orientamento, nella ricerca del lavoro e nei percorsi di carriera.

Resolve nasce per colmare il gap tra il “dire” e il “fare”, affiancando imprenditori e manager, del settore pubblico e privato, nel delineare strategie e calarle in azienda e nel territorio, in modo semplice, tecnologico e sostenibile.

Dal 2023 è **Società Benefit**, a conferma dell’impegno sostanziale verso il mercato, le persone e i territori in cui opera.

RESOL/E
Consulenza strategica,
digitalizzazione e sostenibilità

UPSKILL
Formazione per le imprese
e le persone

JObros
Agenzia per il lavoro
non convenzionale

ergonGROUP
Più competenti. Più intelligenti. Più veloci.

Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

RESOL/E



/ CHI SIAMO

SPEAKER

VALENTINA VERTULLO

Sales Account Specialist di @RESOLVE

Sales Account di Resolve, Valentina è a capo del team Licensing IT. La sua mission è **colmare il gap tra le linee guida fornite da Microsoft (e brand correlati) e le esigenze delle aziende finali**, semplificando il mondo del licensing e diventando punto di riferimento per il cliente. Il suo obiettivo è fornire al cliente risposte che ne soddisfano i bisogni, senza mai perdere di vista standard di Sicurezza e Produttività.

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E



/ CHI SIAMO

SPEAKER

VINCENZO PAGANO

System Architect di @RESOLVE

System Architect di Resolve, Vincenzo si occupa di gestire progetti e infrastrutture IT principalmente su tecnologie Microsoft. Grande appassionato di Cloud Computing e di trasformazione digitale, affianca le aziende nel **sfruttare al meglio il potenziale del cloud per migliorare l'efficienza, la sicurezza, la scalabilità e l'innovazione.**

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E

/ AGENDA

1

ENTRA ID: GOVERNARE GLI ACCESSI

- *Migrazione dei metodi legacy ai metodi convergenti entro Settembre 2025*
- *Tipi di Join e spiegazioni tecniche sui processi*

2

INTUNE: RISORSA PREZIOSA ANCHE PER LA NIS2

- *Intune: le principali funzionalità*
- *Autopilot: distribuzione e fine ciclo vita device*
- *Definizione criteri ASR, Bitlocker e LAPS*

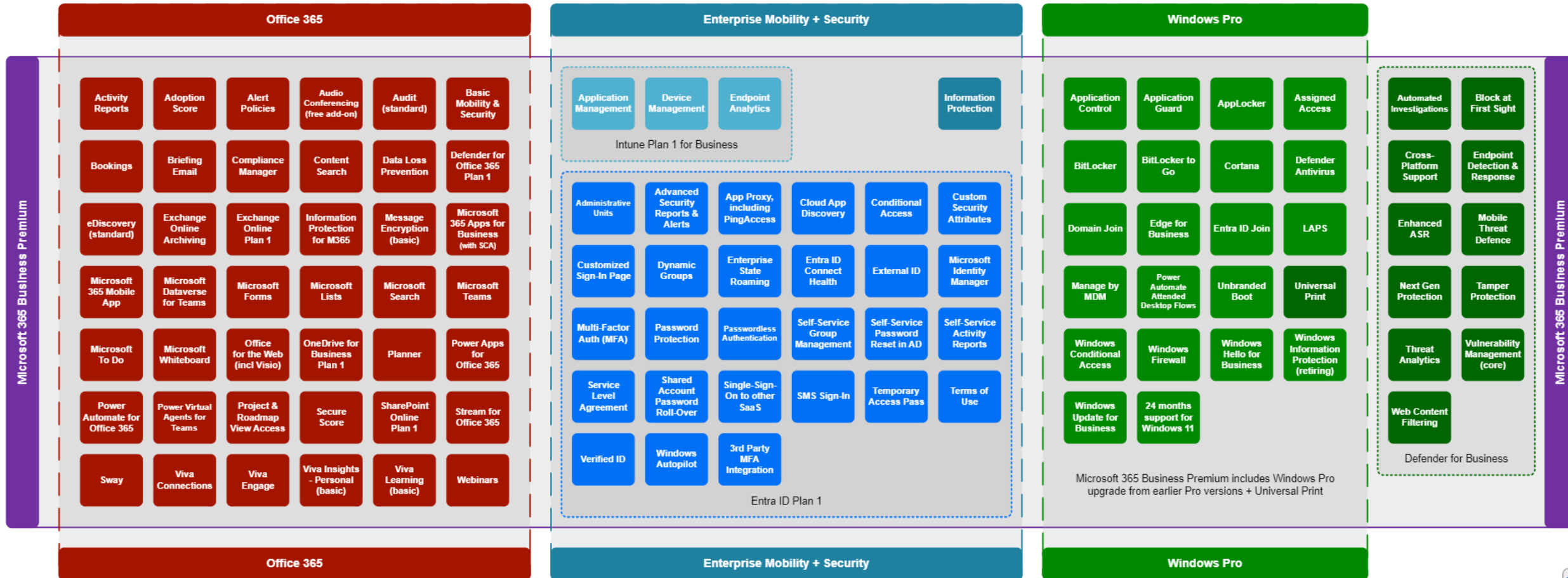
3

Q&A LIVE

MICROSOFT 365 BUSINESS PREMIUM

**UN UNICO PRODOTTO
PER GOVERNARE LE
PROCEDURE DI
SICUREZZA IN AZIENDA**

Microsoft 365 Business Premium



ENTRA ID: GOVERNARE GLI ACCESSI

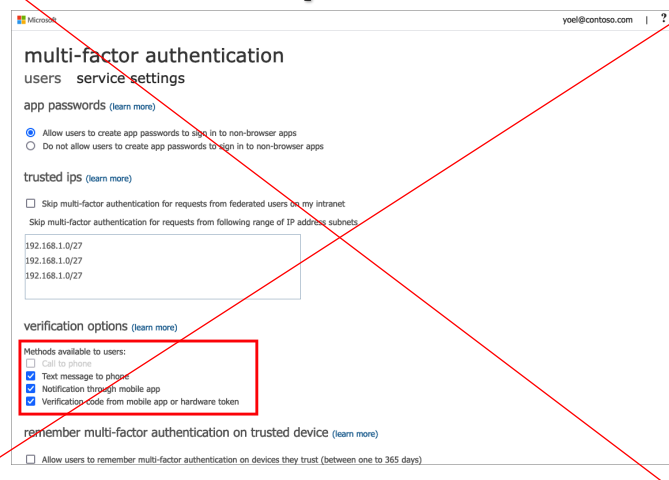
**MIGRAZIONE DEI METODI
LEGACY AI METODI
CONVERGENTI ENTRO
SETTEMBRE 2025**

/ Migrazione criteri legacy

Cosa comporta la migrazione?

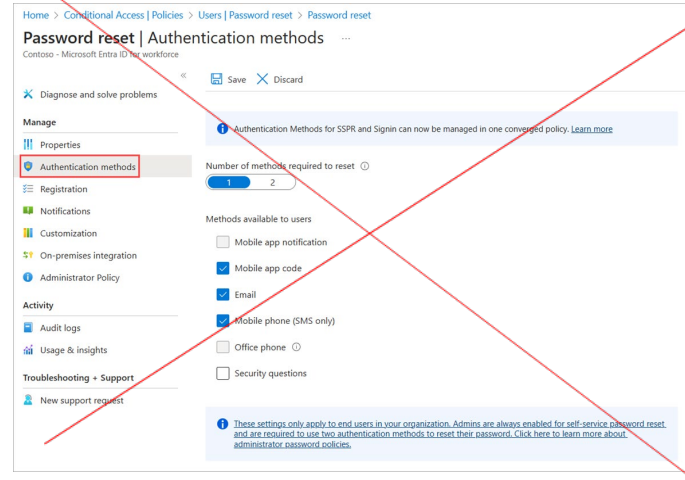
NO

MFA-perUser



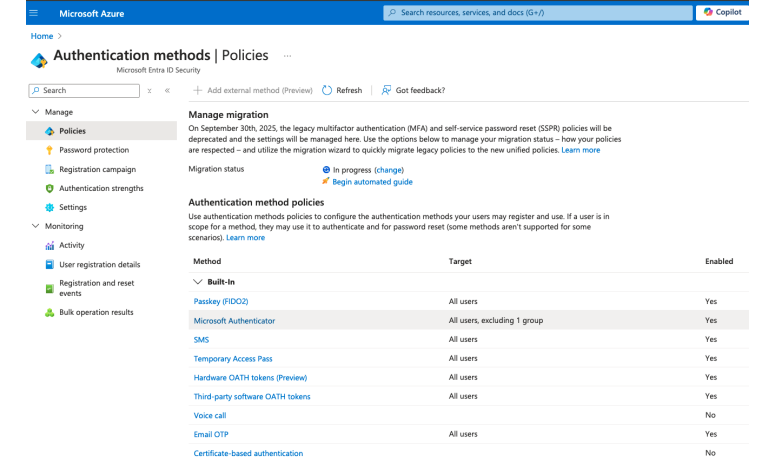
NO

ResetPassword AUTH



SI

Auth methods ENTRA



/ Criterio di MFA legacy

Per ogni metodo, tenere presente se è abilitato o meno per il tenant.

Criterio di autenticazione a più fattori	Criteri del metodo di autenticazione
Chiamata al telefono	Chiamate vocali
SMS al telefono	SMS
Notifica tramite app per dispositivi mobili	Microsoft Authenticator
Codice di verifica dall'app per dispositivi mobili o dal token hardware	Token OATH per software di terze parti Token OATH hardware Microsoft Authenticator

/ Criterio SSPR legacy

Per ogni metodo, tenere presente se è abilitato o meno per il tenant.

Metodi di autenticazione reimpostazione della password self-service	Criteri del metodo di autenticazione
Notifica dell'app per dispositivi mobili	Microsoft Authenticator
Codice app per dispositivi mobili	Microsoft Authenticator Token OATH software
E-mail	OTP Email
Telefono cellulare	Chiamate vocali SMS
Telefono ufficio*	Chiamate vocali
Domande di sicurezza	Non ancora disponibile; copiare le domande per un uso successivo

/ EFFETTUARE LA MIGRAZIONE

Come procedere per completare la migrazione

CONDIVISIONE SCHERMO



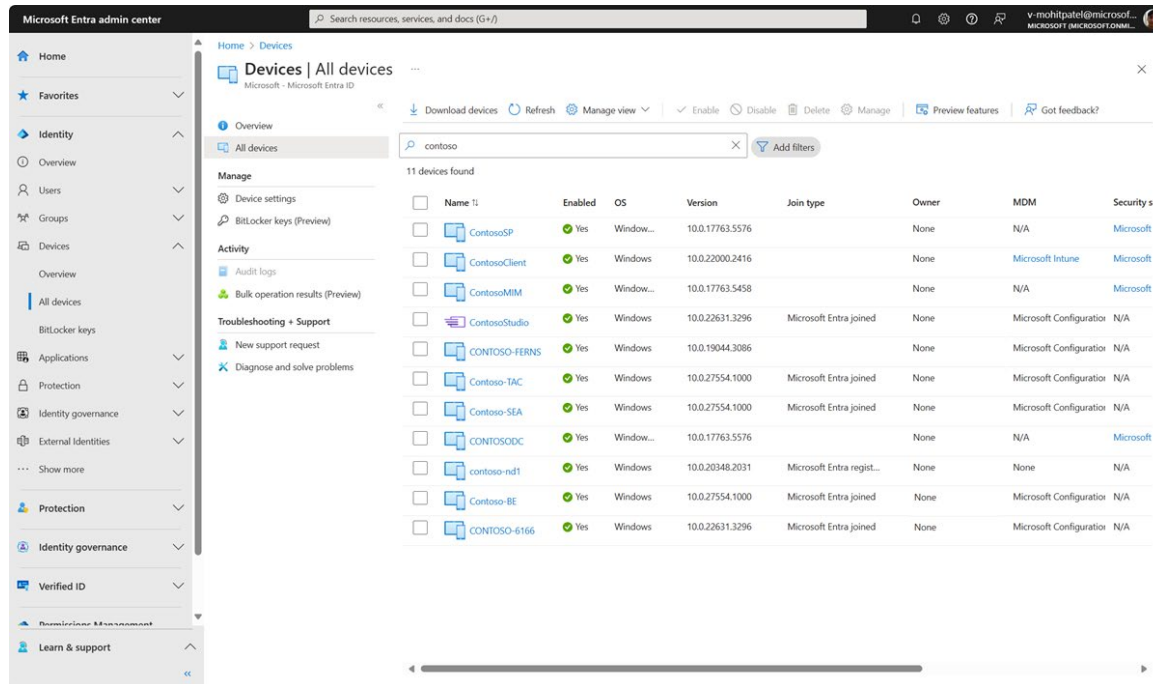
ENTRA ID: GOVERNARE GLI ACCESSI

TIPI DI JOIN E SPIEGAZIONI TECNICHE SUI PROCESSI

/ Informazioni sulle identità dei dispositivi

Dispositivi registrati in ENTRA ID

Un'identità del dispositivo è un oggetto in **Microsoft Entra ID**. Questo oggetto dispositivo è simile a utenti, gruppi o applicazioni. Un'identità del dispositivo fornisce agli amministratori informazioni utili per prendere decisioni relative all'accesso o alla configurazione.



Name	Enabled	OS	Version	Join type	Owner	MDM	Security s
ContosoSP	Yes	Window...	10.0.17763.5576		None	N/A	Microsoft
ContosoClient	Yes	Windows	10.0.22000.2416		None	Microsoft Intune	Microsoft
ContosoMIM	Yes	Window...	10.0.17763.5458		None	N/A	Microsoft
ContosoStudio	Yes	Windows	10.0.22631.3296	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSO-FERNS	Yes	Windows	10.0.19044.3086		None	Microsoft Configuration	N/A
Contoso-TAC	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
Contoso-SEA	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSODC	Yes	Window...	10.0.17763.5576		None	N/A	Microsoft
contoso-nd1	Yes	Windows	10.0.20348.2031	Microsoft Entra regist...	None	None	N/A
Contoso-BE	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSO-6166	Yes	Windows	10.0.22631.3296	Microsoft Entra joined	None	Microsoft Configuration	N/A

/ Conditional access policy

Le identità dei dispositivi sono un prerequisito per scenari come i criteri di accesso condizionale

Concedi



⚠ "Richiedi complessità dell'autenticazione" non può essere usato con "Richiedere l'autenticazione a più fattori" [Altre informazioni](#)

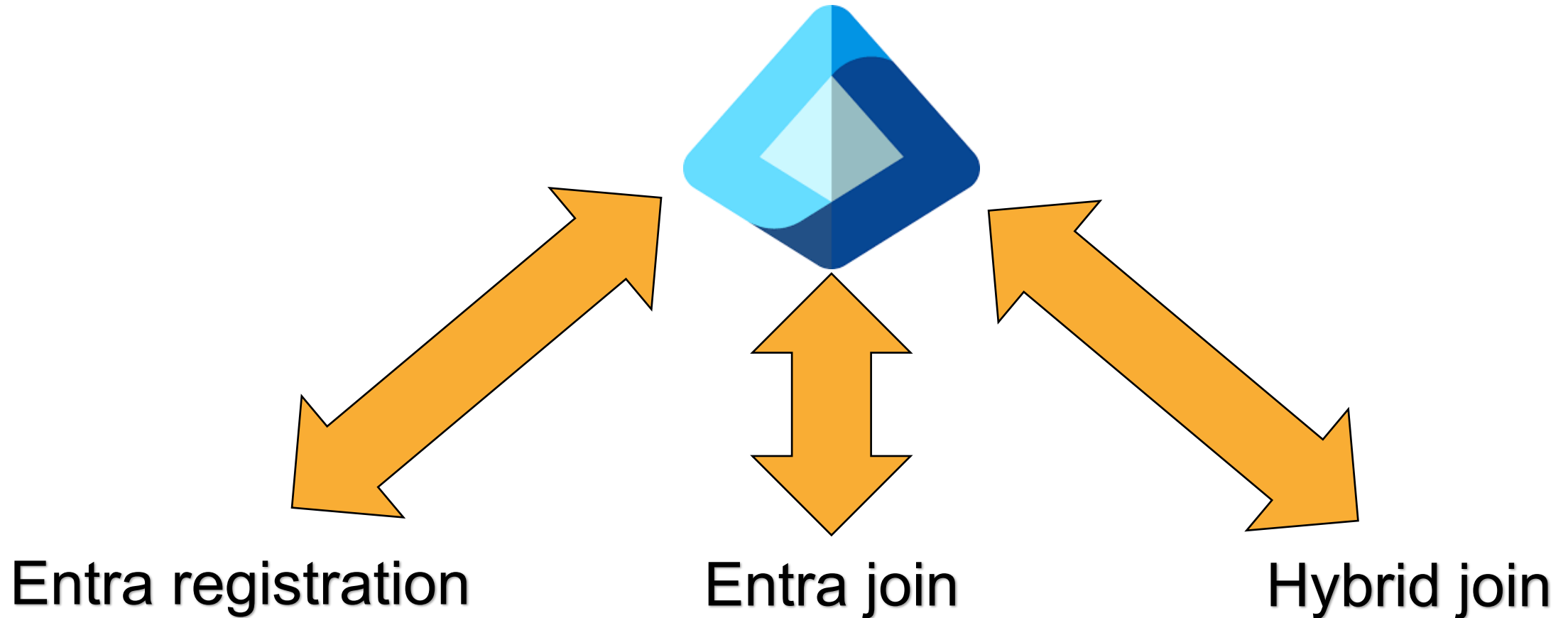
- ☐ Richiedi che i dispositivi siano contrassegnati come conformi ⓘ
- ☐ Richiedi dispositivo aggiunto a Microsoft Entra ibrido ⓘ
- ☐ Richiedi app client approvata ⓘ
[Visualizza l'elenco di app client approvate](#)
- ☐ Richiedi criteri di protezione dell'app ⓘ
[Visualizza l'elenco di app client protette da criteri](#)
- ☐ Richiedi modifica password ⓘ

Nel criteri di accesso condizionale nella sezione «Concedi», oltre a richiedere l'autenticazione a più fattori, possiamo richiedere che il dispositivo sia registrato.

Se non registrato, non si avrà accesso.

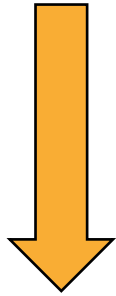
/ Ottenere un'identità del dispositivo

3 modi di effettuare il join



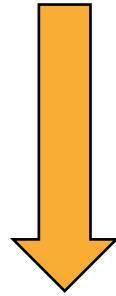
/ Scenario di dispositivo moderno

Lo scenario del dispositivo moderno è incentrato su due di questi metodi:



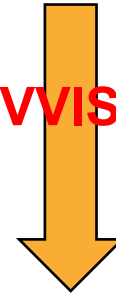
Entra registration

- Bring Your Own Device (BYOD)
- Dispositivo mobile (cellulare e tablet)



Entra join

Dispositivi Windows 11, Windows 10, Windows server di proprietà dell'organizzazione

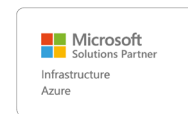
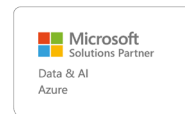


PROVVISORIO

Hybrid join

Considerato un passaggio provvisorio sulla strada per l'aggiunta a Microsoft Entra.

Tutti e tre gli scenari possono coesistere in una singola organizzazione.



/ Accesso alle risorse

Funzionalità SSO

La registrazione e l'aggiunta di dispositivi a Microsoft Entra ID offre agli utenti l'accesso Facile (SSO) alle risorse basate sul cloud.

Provisioning in corso

Manuale o gestito

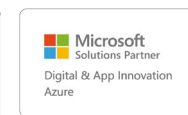
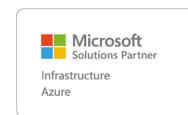
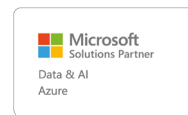
L'accesso dei dispositivi a Microsoft Entra ID può essere eseguito in modo self-service o in un processo controllato gestito dagli amministratori.



/ Dispositivi registrati di Microsoft Entra

In questi scenari, un utente può accedere alle risorse dell'organizzazione usando un dispositivo personale.

Registrato in Microsoft Entra	Descrizione
Definizione	Registrazione in Microsoft Entra ID senza richiedere l'account aziendale per accedere al dispositivo
Destinatari principali	•Applicabile a tutti gli utenti con i criteri seguenti:Bring Your Own Device •Dispositivi mobili
Proprietà del dispositivo	Utente o organizzazione
Sistemi operativi	•Windows 10 o successive macOS 10.15 iOS 15 Android Linux:Ubuntu 20.04/22.04 LTS •Red Hat Enterprise Linux 8/9 LTS



Provisioning	- Windows 10 o versione successiva – Impostazioni. iOS/Android - Portale aziendale o app Microsoft Authenticator - macOS - Portale aziendaleLinux - Agente di Intune
Opzioni di accesso del dispositivo	Credenziali locali dell'utente finale Password Windows Hello, PIN, Biometria o modello per altri dispositivi
Gestione dispositivi	Gestione di dispositivi mobili (esempio: Microsoft Intune)gestione di applicazioni mobili
Funzionalità principali	Accesso Single Sign-On (SSO) alle risorse cloud, accesso condizionale quando viene eseguita la registrazione in Intune, accesso condizionale tramite criteri di protezione delle app e consente l'accesso tramite telefono con l'app Microsoft Authenticator

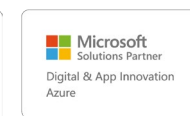
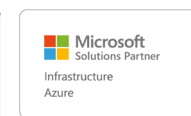
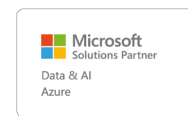
/ Dispositivi aggiunti a Microsoft Entra

In questi scenari, un utente può accedere alle risorse dell'organizzazione usando un dispositivo che richiede account aziendale.

Definizione	Aggiunto solo a Microsoft Entra ID che richiede l'account aziendale per accedere al dispositivo
Destinatari principali	Adatto a organizzazioni ibride e basate solo sul cloud. Applicabile a tutti gli utenti di un'organizzazione
Proprietà del dispositivo	Organizzazione
Sistemi operativi	Tutti i dispositivi Windows 11 e Windows 10 ad eccezione delle edizioni Home Windows server 2019 e successive (no core e su Azure)
Provisioning	• Self-service: Windows Out of Box Experience (Configurazione guidata) o Impostazioni • Registrazione in blocco • Windows Autopilot

Opzioni di accesso del dispositivo	Account aziendale che usa: • Password • Opzioni senza password come Windows Hello for Business, Platform Credential for macOS (anteprima pubblica) e chiavi di sicurezza FIDO2.0.
Gestione dispositivi	• Gestione di dispositivi mobili (esempio: Microsoft Intune) • Configuration Manager autonomo o co-gestione con Microsoft Intune
Funzionalità principali	• Accesso Single Sign-On (SSO) alle risorse cloud e locali • Accesso condizionale tramite la registrazione e la valutazione della conformità di gestione dei dispositivi mobili (MDM) • Reimpostazione della password self-service e reimpostazione del PIN di Windows Hello nella schermata di blocco

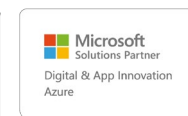
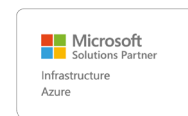
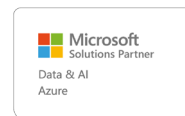
Con Intune e co-gestione è possibile richiedere la crittografia dell'archiviazione, complessità delle password, installazione del software e aggiornamenti software



/ Dispositivi ibridi aggiunti a Microsoft Entra

Le organizzazioni con implementazioni di Active Directory esistenti possono trarre vantaggio da alcune delle funzionalità fornite da Microsoft Entra ID implementando i dispositivi aggiunti all'ibrido Microsoft Entra. Questi dispositivi vengono aggiunti al Active Directory locale e registrati con Microsoft Entra ID.

Aggiunta a Microsoft Entra ibrido	Descrizione
Definizione	Aggiunto all'istanza locale di Microsoft Windows Server Active Directory e all'ID Microsoft Entra che richiede l'account aziendale per accedere al dispositivo
Destinatari principali	Adatto per le organizzazioni ibride con l'infrastruttura di Microsoft Windows Server Active Directory locale esistente
Proprietà del dispositivo	Organizzazione
Sistemi operativi	- Windows 11 o Windows 10 ad eccezione delle edizioni Home - Windows Server 2016, 2019, 2022, 2025



Provisioning	• Windows 11, Windows 10, Windows Server 2016/2019/2022/2025 • Aggiunta al dominio da parte dell'IT e della partecipazione automatica tramite Microsoft Entra Connessione • Aggiunta a un dominio da Windows Autopilot e accesso automatico tramite Microsoft Entra Connessione
Opzioni di accesso del dispositivo	• Password • Opzioni senza password come Windows Hello for Business e chiavi di sicurezza FIDO2.0.
Gestione dispositivi	Criteri di gruppo
Funzionalità principali	• Accesso Single Sign-On (SSO) alle risorse cloud e locali • Accesso condizionale tramite aggiunta a un dominio o Intune

/ Tipi di JOIN

Come controllare lo stato su ENTRA ID

CONDIVISIONE SCHERMO

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E

INTUNE: RISORSA PREZIOSA ANCHE PER LA NIS2

INTUNE: LE PRINCIPALI FUNZIONALITÀ

/ Microsoft Intune gestisce in modo sicuro le identità, le app e i dispositivi



/ MODERN MANAGEMENT

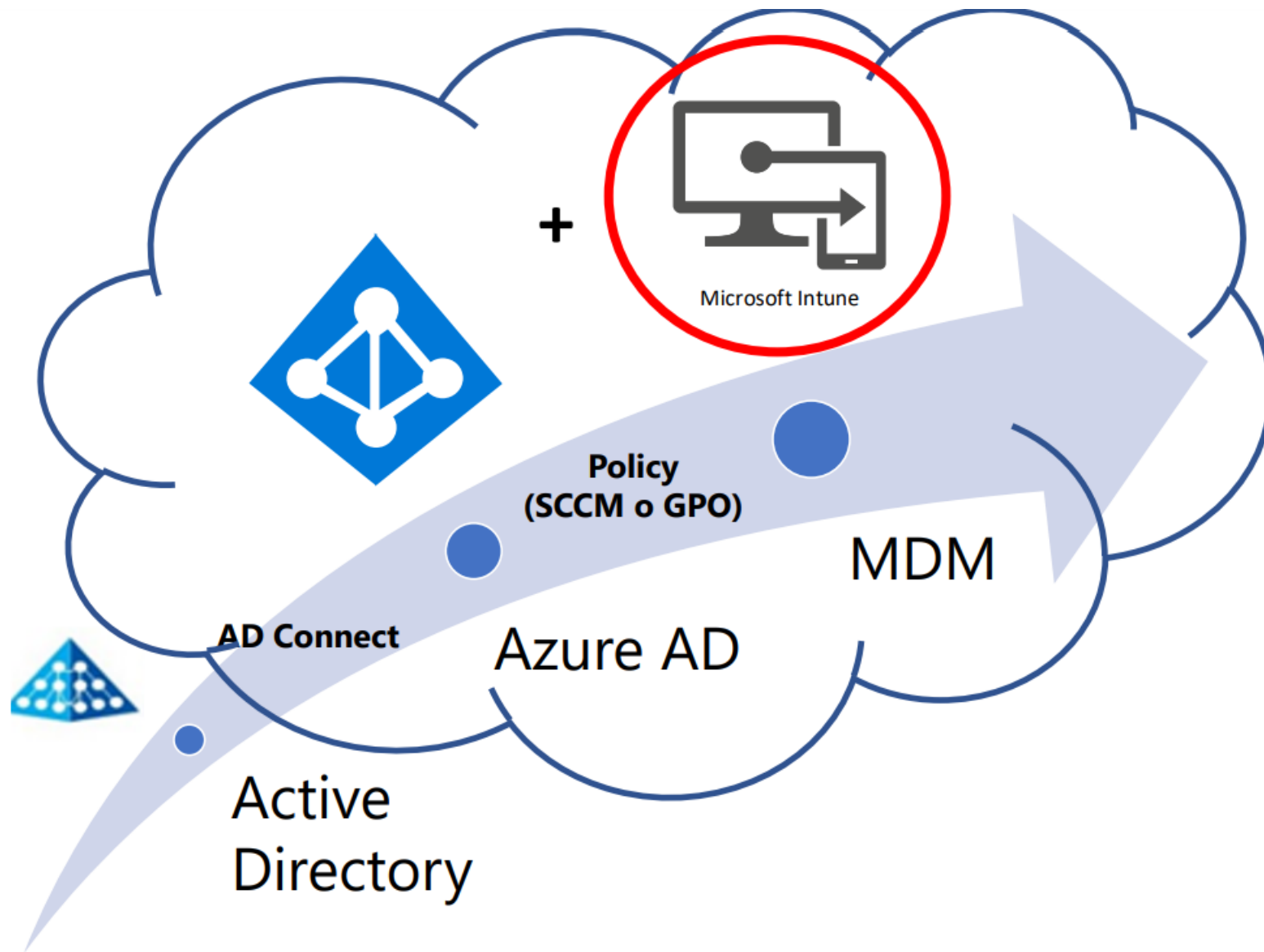
Cloud-based control

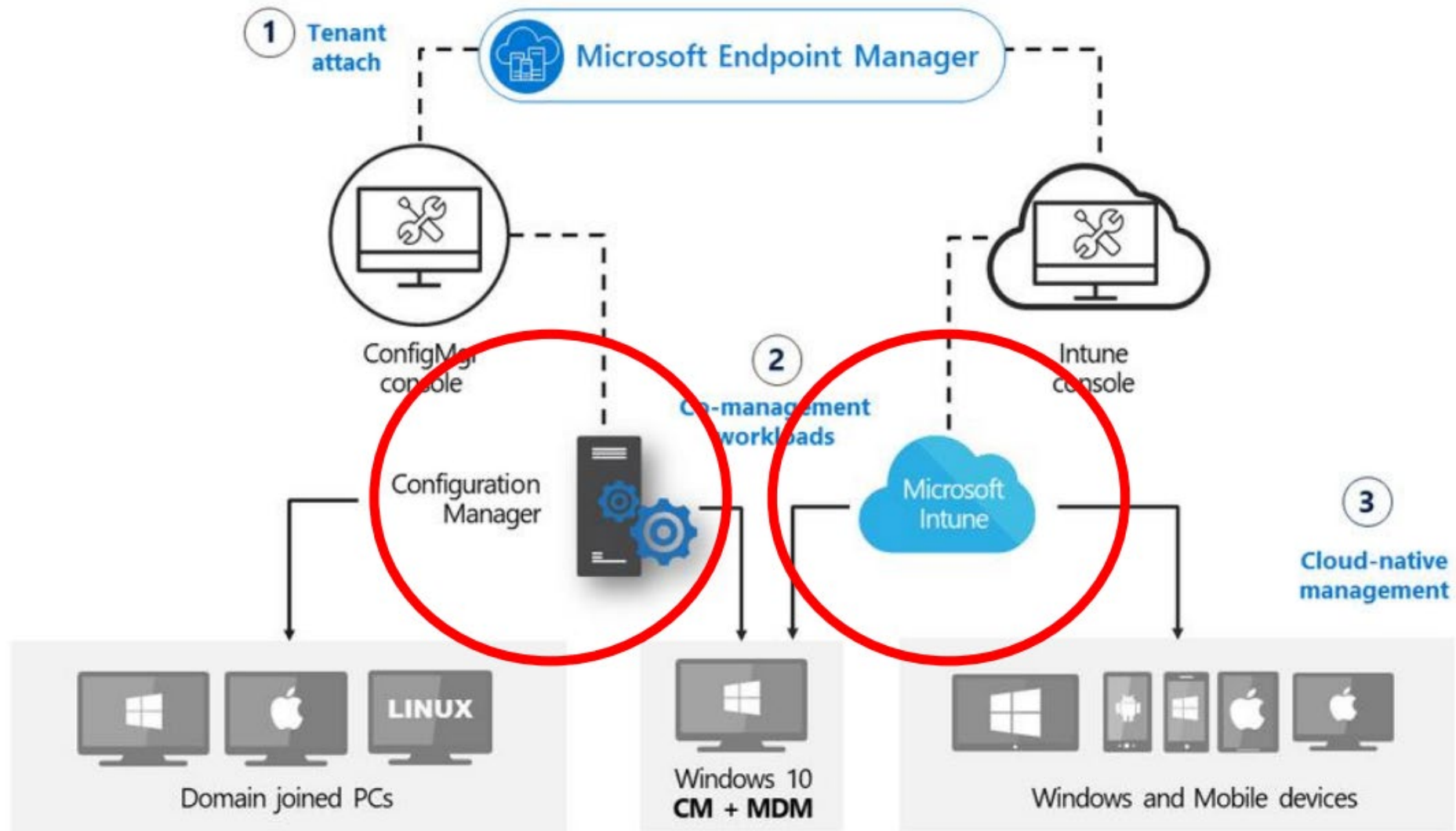
HTTPS SSL on 443

I client hanno bisogno soltanto di
Connessione internet

Non sono necessarie porte speciali
O altre configurazioni firewall







/ MICROSOFT INTUNE POLICIES

Profili di configurazione

Importazione ADMX

Security Baselines

Compliance policies

Proactive Remediations

Scripts



/ CONFIGURAZIONE PROFILI

Microsoft Intune

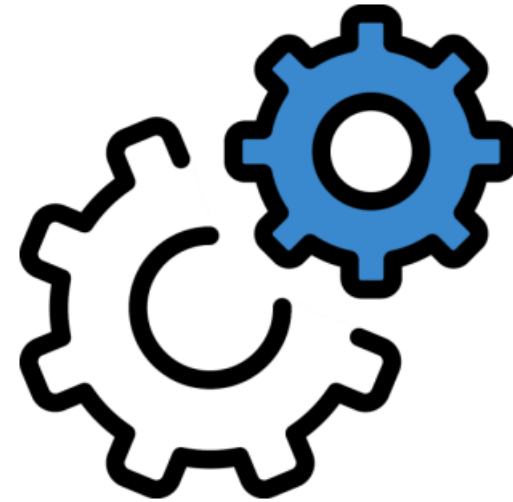
«Group policy» in stile impostazioni

Configuration Service Provider (CSP)

Embedded on Windows 10/11

Templates / Settings Catalog

Policy per W10/11, Office ed Edge



/ CONFIGURAZIONE PROFILI

Microsoft Intune

OMA-DM

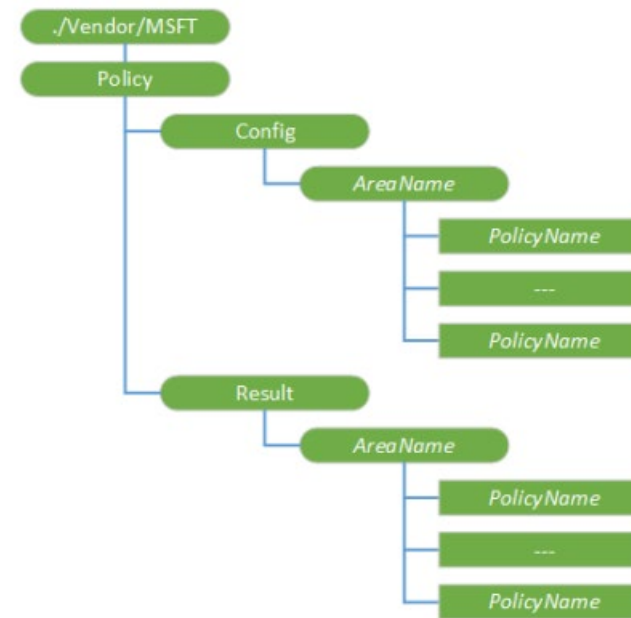
Open Mobile Alliance
Device Management

OMA-URI

Open mobile Alliance
Uniform Resource Identifier

CPS

Configuration Service Provider



/ CONFIGURAZIONE PROFILI

Microsoft Intune

Home > Devices | Windows > Windows

Windows | Configuration profiles

Search

+ Create profile Columns Refresh Export Filter

Search by name

Profile name
BSLABS - Client Certificate
BSLABS - Root Certificate
DigiCert Global Root CA
Intune data collection policy
MDM Wins Over GP
NDES-ClientCertificate
W10_DomainJoin_HybridJoin

Create a profile

Platform: Windows 10 and later

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. [Learn more](#)

Search

Template name

- Administrative Templates
- Custom
- Delivery Optimization
- Device Firmware Configuration Interface
- Device restrictions
- Device restrictions (Windows 10 Team)
- Domain Join
- Edition upgrade and mode switch
- Email

/ IMPORTAZIONE ADMX

Microsoft Intune

20 ADMX + ADML files

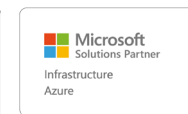
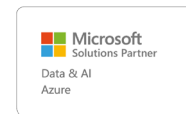
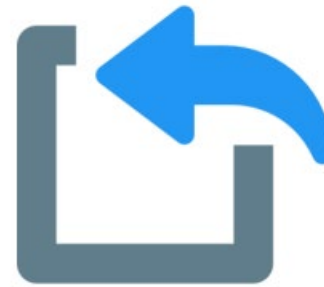
Possono essere caricati

Ogni file deve essere di 1 MB o inferiore

Per ogni file ADMX, è possibile caricare
un solo file ADML

Attualmente sono supportati solo
file ADML in en-us

Third-party/partner



RESOL/E

/ IMPORTAZIONE ADMX

Microsoft Intune

Profiles **Import ADMX**

+ Import Refresh Export Columns

Template Name ↑	Version	Status
google.admx	1.0	✓ Available
chrome.admx	1.0	✓ Available

✓ Basics **2 Configuration settings** 3 Scope tags 4 Assignments 5 Review + create

All Settings

Computer Configuration

Google

Google Chrome

User Configuration

Google Chrome

Computer Configuration/Google/Google Chrome

Search to filter items...

Setting name	State	Setting type	Path
Allow or deny screen capture			
Content settings			
Default search provider			
Deprecated policies			
Extensions			
Google Cast			
HTTP authentication			
Legacy Browser Support			
Native Messaging			
Other			

/ COME MIGRARE I CRITERI DI GRUPPO

Group Policy Analytics tool

Analyzes your on-premises GPOs

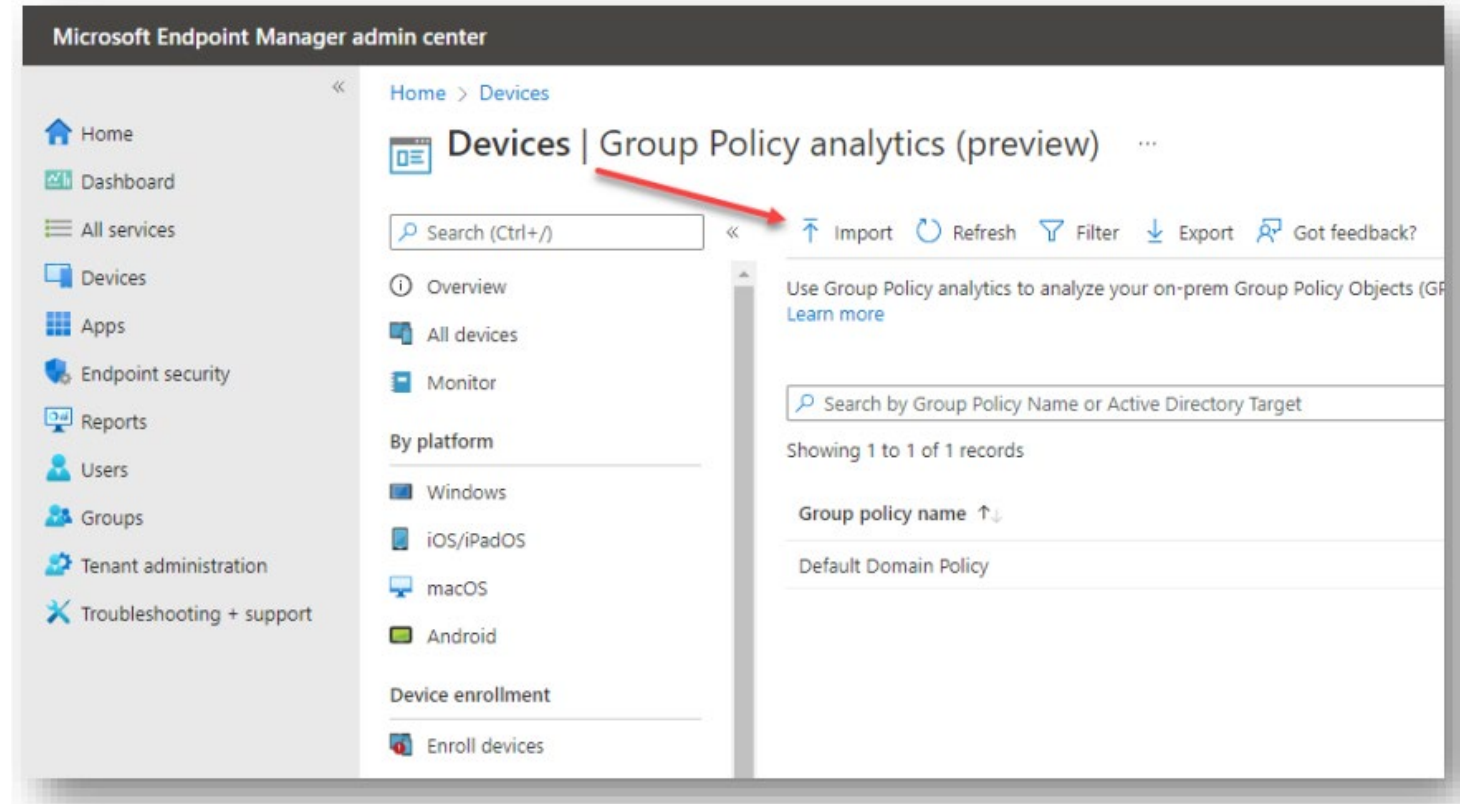
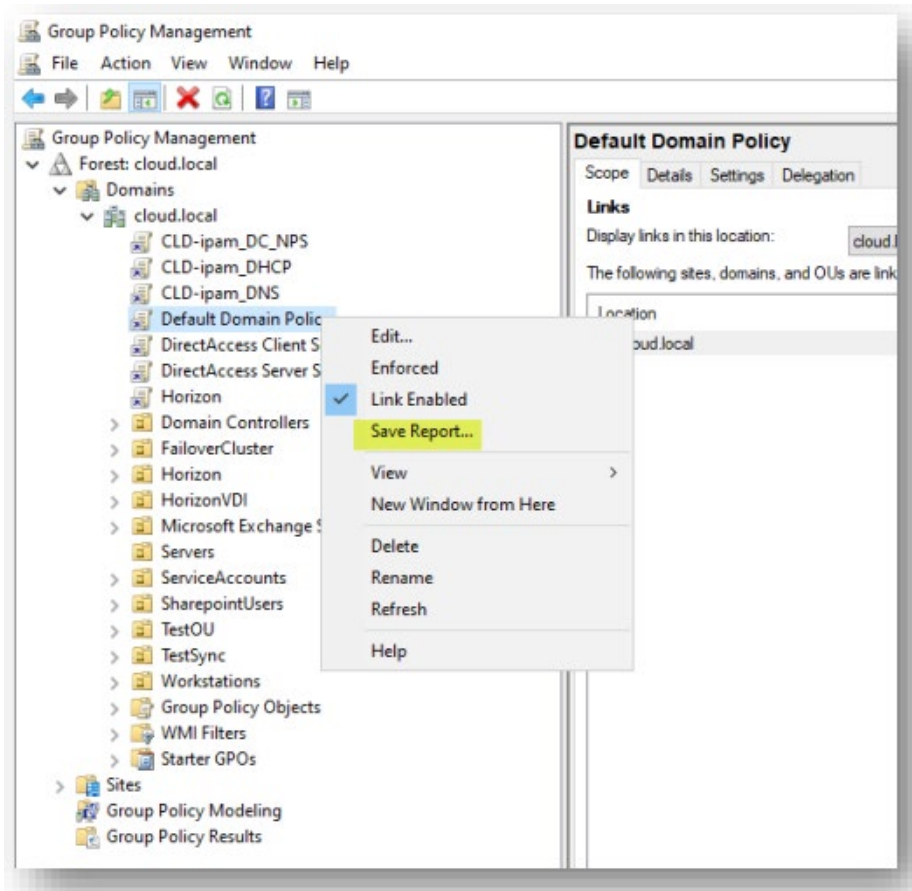
Group Policy Analytics tool

Translates GPOs
to the cloud-based settings

Shows which settings are supported
in Microsoft Intune



/ COME MIGRARE I CRITERI DI GRUPPO



Microsoft Endpoint Manager admin center

Home > Devices >

Default Domain Policy

Group Policy analytics (preview)

Refresh Filter Export Got feedback? Back

Search by Setting Name

Setting Name ↑↓	Group Policy Setting... ↑↓	MDM Support ↑↓	Value ↑↓	Min OS Version ↑↓	CSP Name ↑↓	CSP Mapping ↑↓
ForceLogoffWhenHourEx...	N/A	⚠ No	0	0		
LockoutBadCount	N/A	✅ Yes	5	15063	Policy	./Device/Vendor/MSFT...
LockoutDuration	N/A	⚠ No	30	0		
LSAAnonymousNameLoo...	N/A	⚠ No	0	0		
MaxClockSkew	N/A	⚠ No	5	0		
MaximumPasswordAge	N/A	✅ Yes	42	15063	Policy	./Device/Vendor/MSFT...
MaxRenewAge	N/A	⚠ No	7	0		
MaxServiceAge	N/A	⚠ No	600	0		
MaxTicketAge	N/A	⚠ No	10	0		
MinimumPasswordAge	N/A	✅ Yes	30	17130	Policy	./Device/Vendor/MSFT...
Network security: Do not ...	N/A	✅ Yes	true	18362	Policy	./Device/Vendor/MSFT...
PasswordComplexity	N/A	✅ Yes	true	15063	Policy	./Device/Vendor/MSFT...
ResetLockoutCount	N/A	⚠ No	30	0		
TicketValidateClient	N/A	⚠ No	true	0		

Showing 1 to 14 of 14 records

< Previous Page 1 of 1 Next >

+ Select all ↑ Import Refresh Filter Export **→ Migrate** Got feedback?

Use Group Policy analytics to analyze your on-prem Group Policy Objects (GPO) and determine your level of modern management support. [Learn more](#)

Search by Group Policy Name or Active Directory Target

Showing 1 to 3 of 3 records

< Previous Page 1 of 1 Next >

Migrate ↑↓	Group policy name ↑↓	Active directory target ↑↓	MDM support ↑↓	Unknown settings ↑↓
☒	BS - FIREWALL	BS_FIREWALL	✅ 100%	View
☐	BSL - Restricted Group - Local Admins	BSL_Restricted_Group_Local_Admins	✅ No settings in pol...	View

/ COMPLIANCE POLICIES

Microsoft Intune

Richiedere a utenti e dispositivi
di rispettare i prerequisiti aziendali

Criteri e impostazioni

Combinazioni con
Accesso condizionale



/ ESITO COMPLIANCE

Positivo o negativo

Custom Compliance

Custom compliance ⓘ Require Not configured

Select your discovery script [Click to select](#)

Upload and validate the JSON file with your custom compliance settings Select a file

Device Health

Windows Health Attestation Service evaluation rules

Require BitLocker ⓘ Require Not configured

Require Secure Boot to be enabled on the device ⓘ Require Not configured

Require code integrity ⓘ Require Not configured

Device Properties

Configuration Manager Compliance

System Security

Microsoft Defender for Endpoint





Tipi di Enrollments, File ADMX, Configurazioni e Compliance

CONDIVISIONE SCHERMO

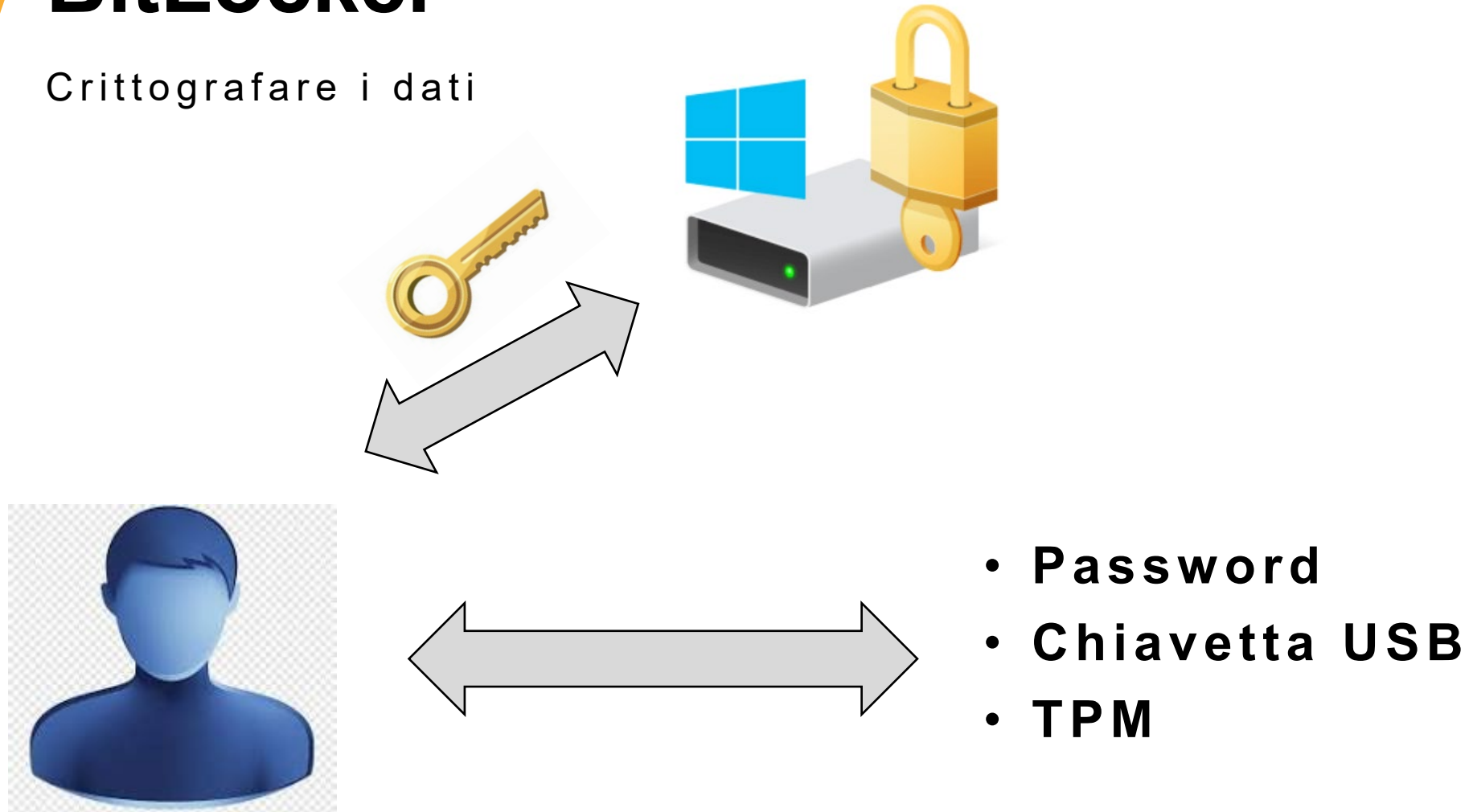


INTUNE: RISORSA PREZIOSA ANCHE PER LA NIS2

DEFINIZIONE CRITERI ASR, BITLOCKER E LAPS

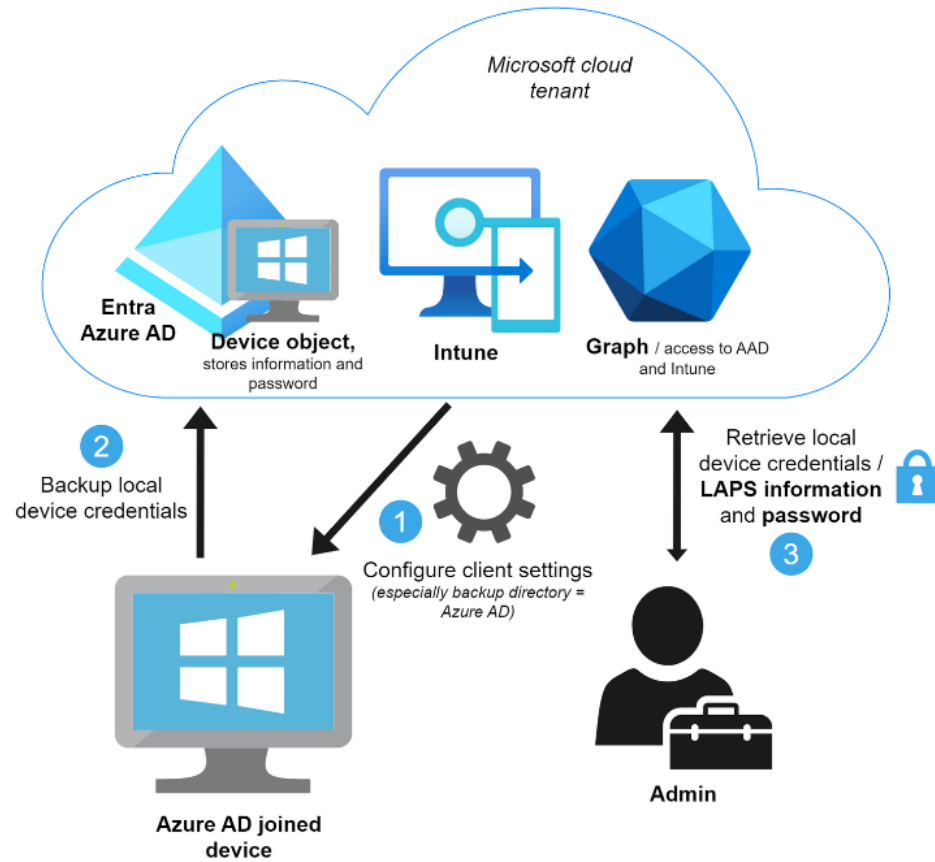
/ BitLocker

Crittografare i dati



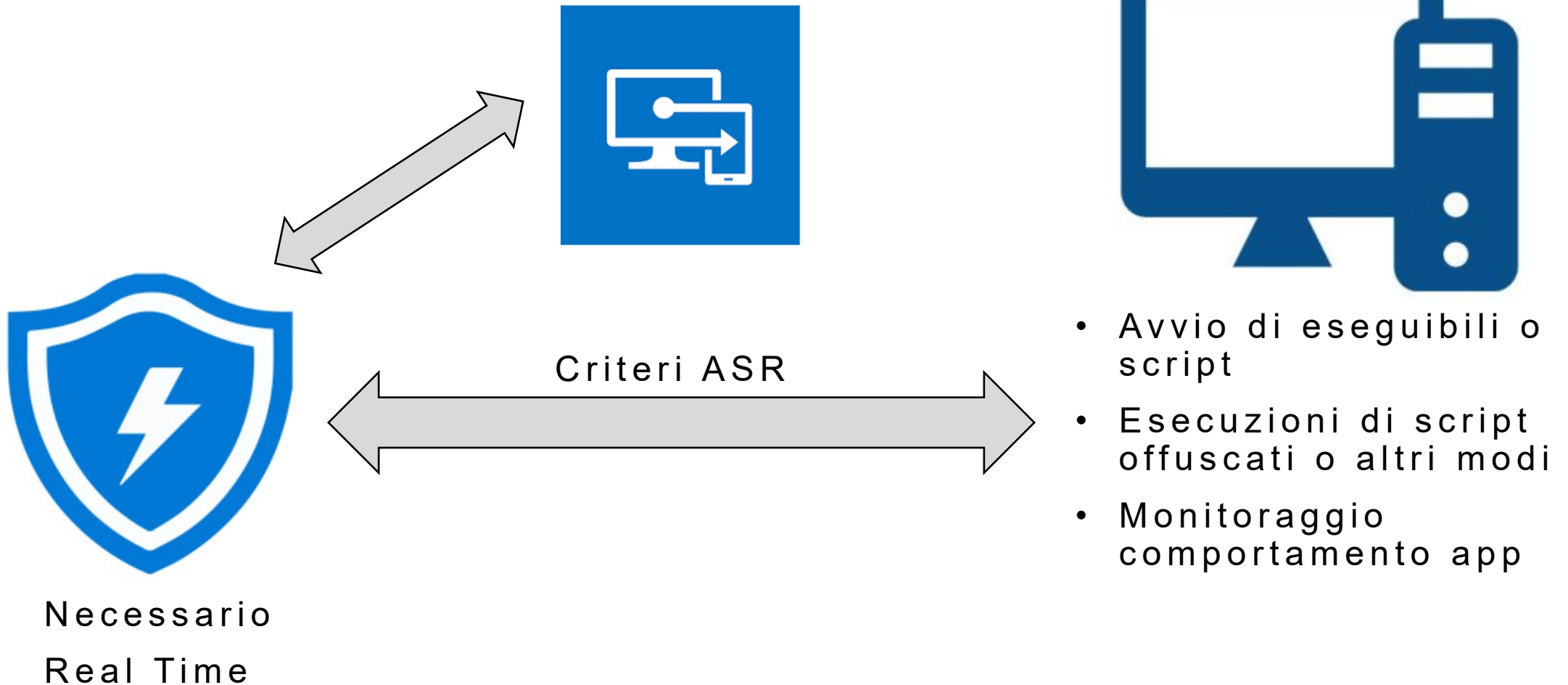
/ WINDOWS LAPS

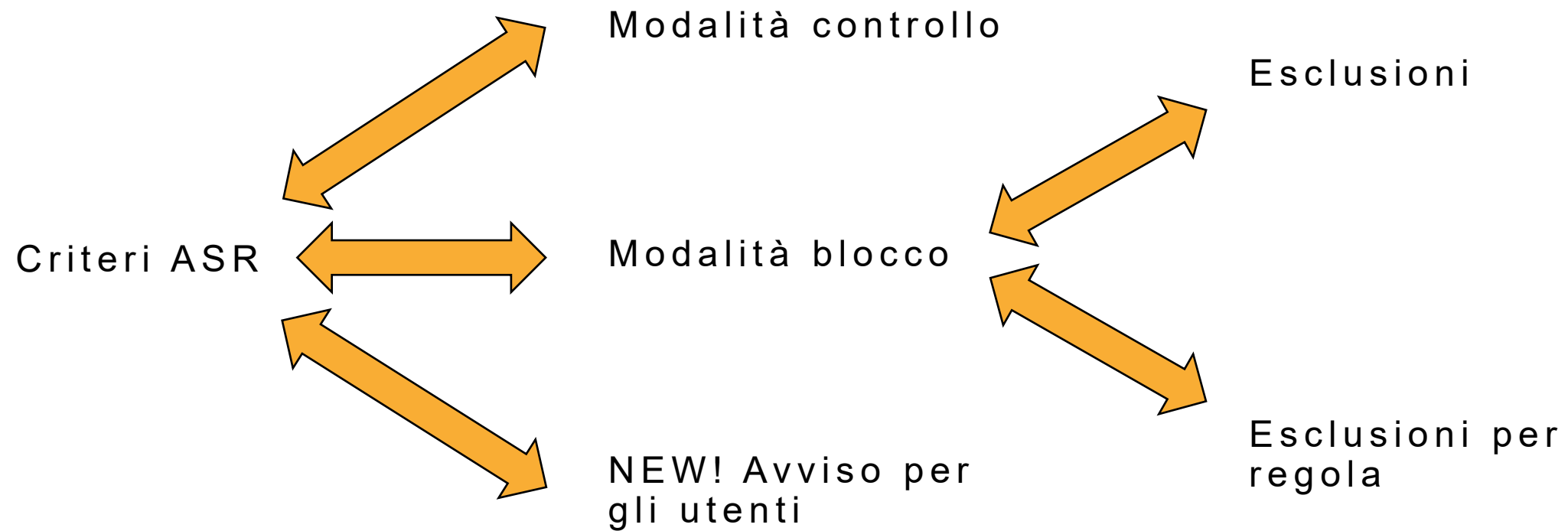
Password admin locale



/ REGOLE ASR

Ridurre la superficie di attacco





/ PROCESSO DI APPLICAZIONE

Test regole ASR

Testare e valutare le regole ASR





Regole ASR, LAPS e Bitlocker

CONDIVISIONE SCHERMO

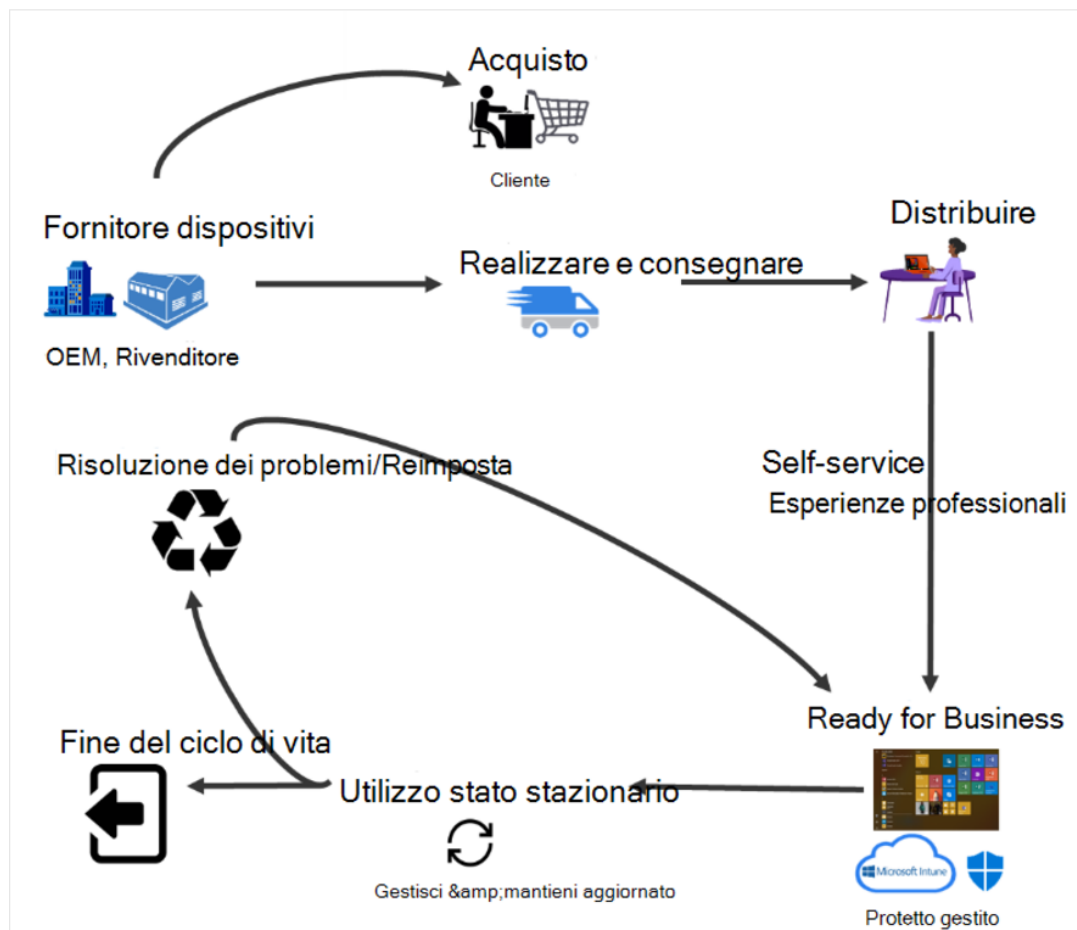


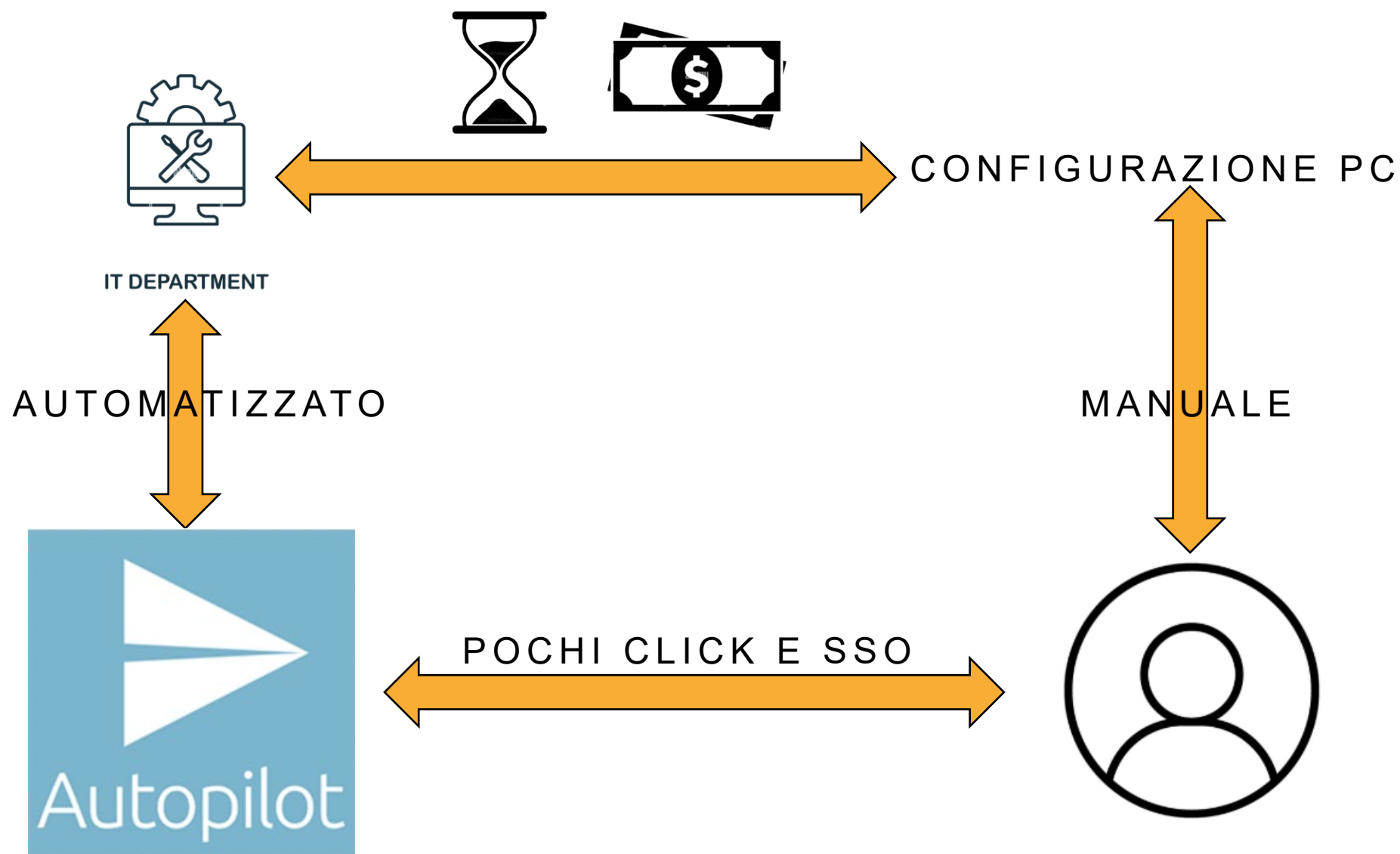
INTUNE: RISORSA PREZIOSA ANCHE PER LA NIS2

AUTOPILOT: DISTRIBUZIONE E FINE CICLO VITA DEVICE

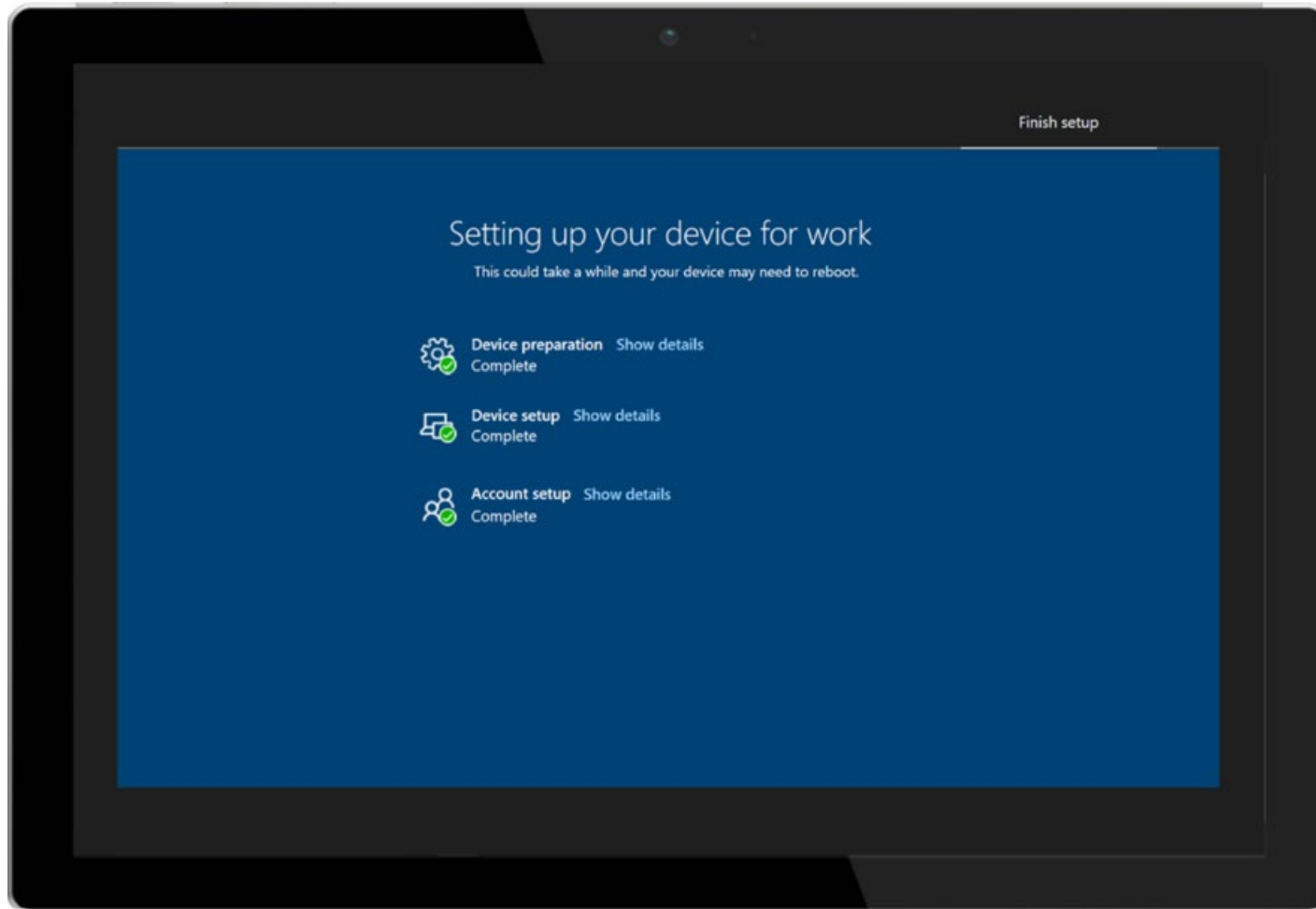
/ AUTOPILOT

FLUSSO DI GESTIONE

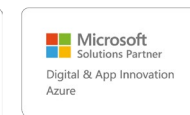
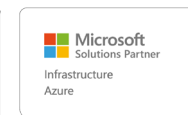
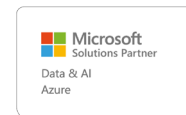




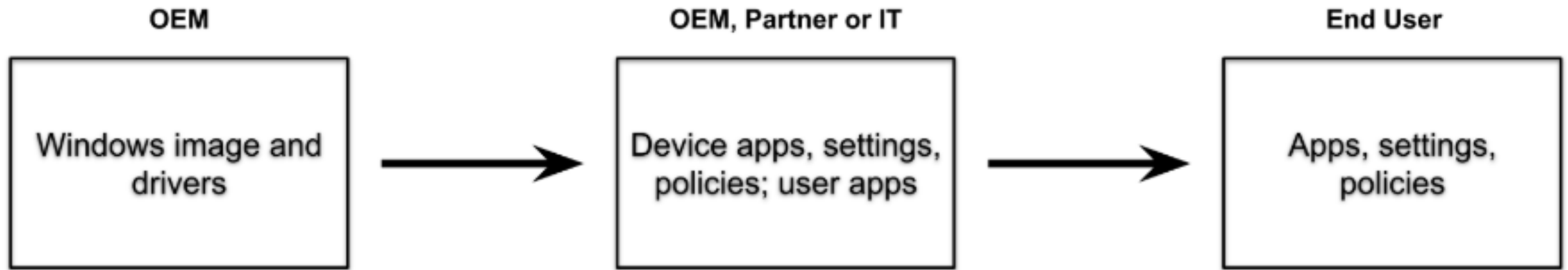
/ ESEMPIO DI CONFIGURAZIONE UTENTE



/ FUNZIONALITA' ABILITATE AUTOPILOT



/ PROVISIONING



/ REGISTRAZIONE DEL DISPOSITIVO

PRIMA

HASH HARDWARE

DEVICE ID TENANT

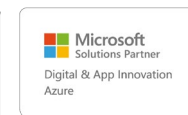
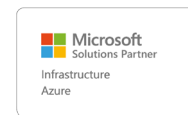
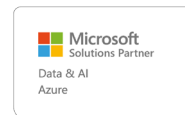
- Registrazione OEM
- Registrazione di rivenditori, server di distribuzione o partner
- Registrazione automatica
- Registrazione manuale



DOPO

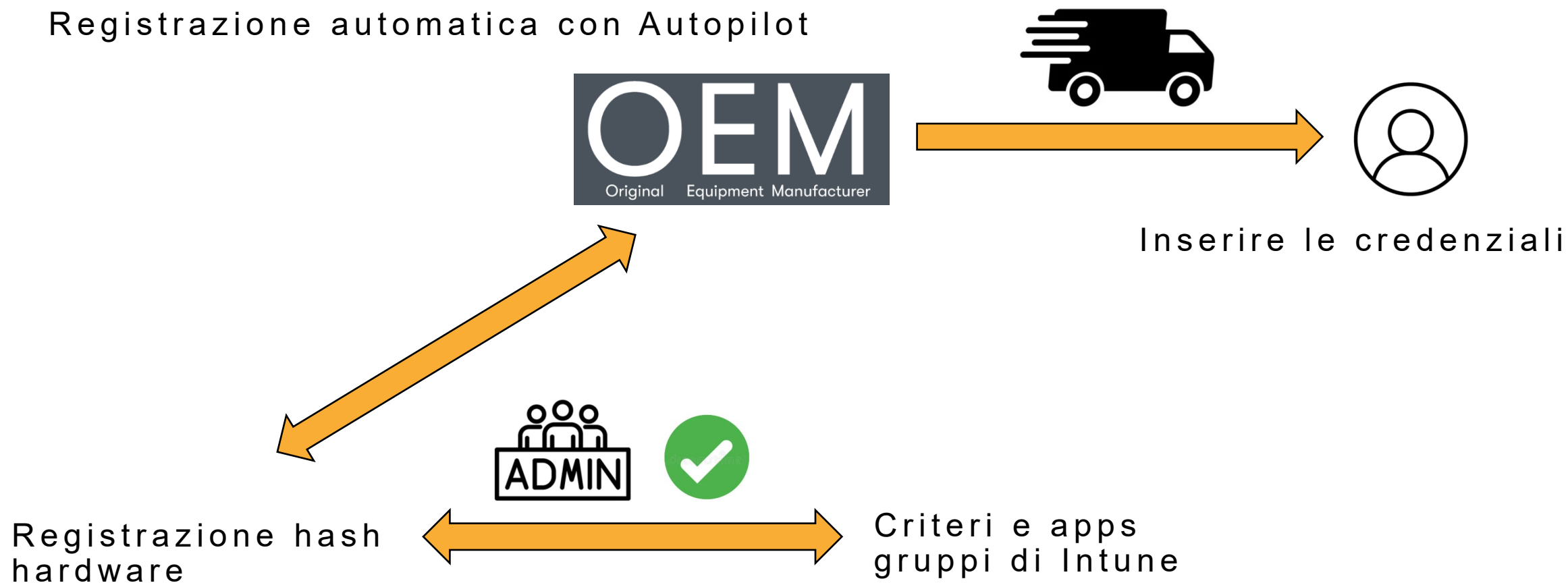
DISTRIBUZIONE

- Policy
- Compliance
- Security
- Apps



/ REGISTRAZIONE OEM

Registrazione automatica con Autopilot

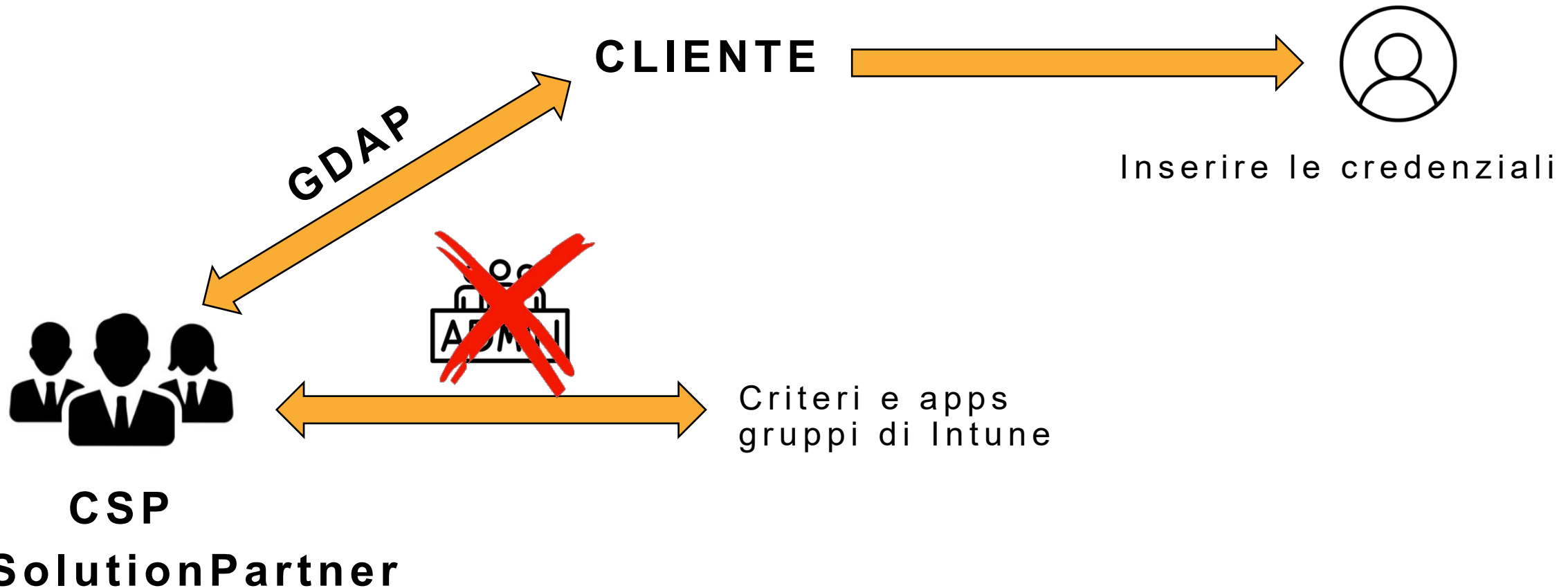


Produttori di dispositivi coinvolti

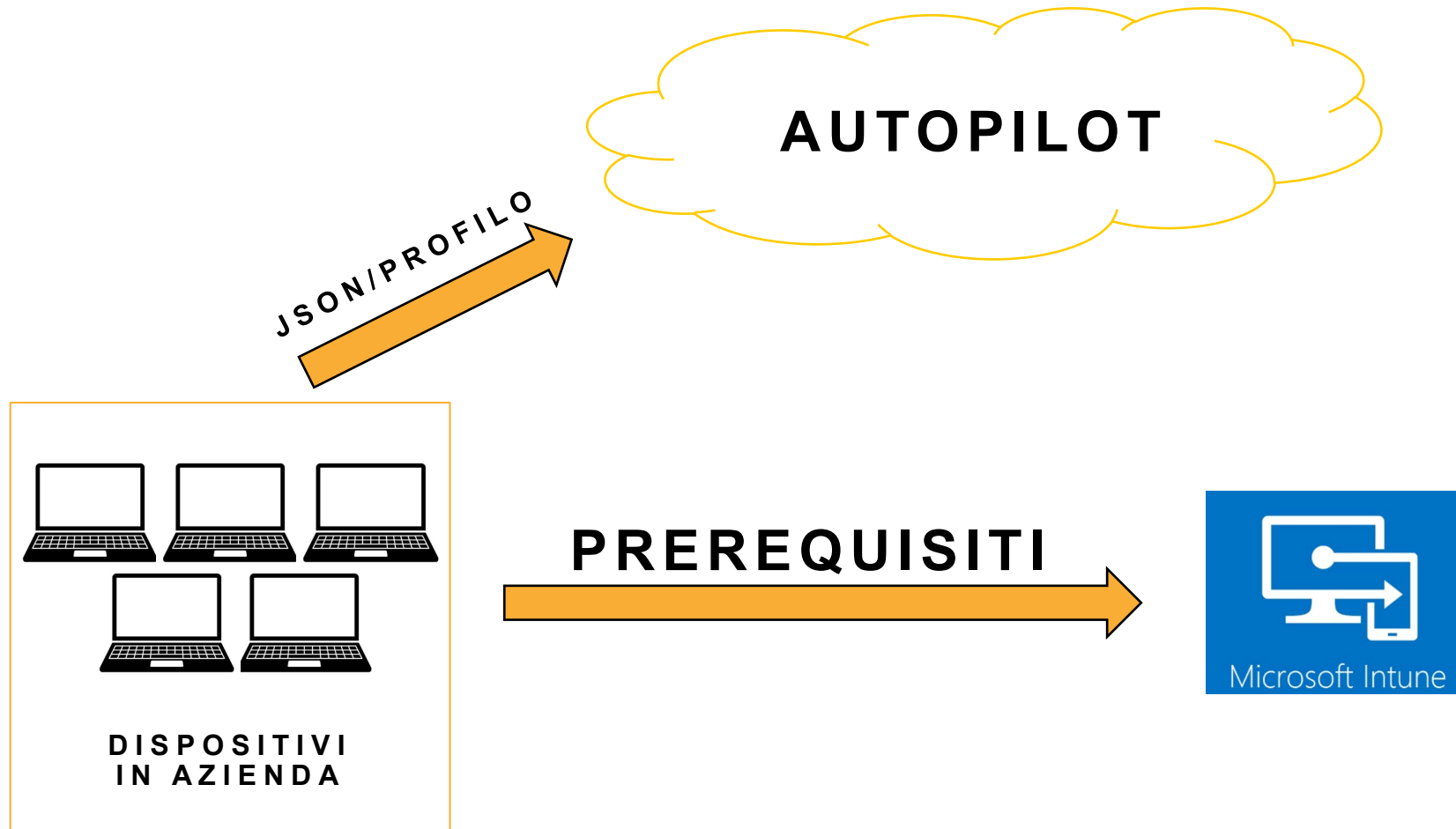
Questi marchi spediscono dispositivi con Windows Autopilot. I dipendenti riceveranno i dispositivi acquistati già pronti per l'utilizzo: basterà eseguire l'accesso senza l'intervento del personale IT.



/ Registrazione di rivenditori, server di distribuzione o partner



/ Registrazione automatica dei dispositivi esistenti



/ PROFILO

Microsoft Endpoint Manager admin center

<< Home > Devices > Windows > Windows Autopilot deployment profiles >

Create profile

Windows PC

1 Basics 2 Out-of-box experience (OOBE) 3 Assignments 4 Review + create

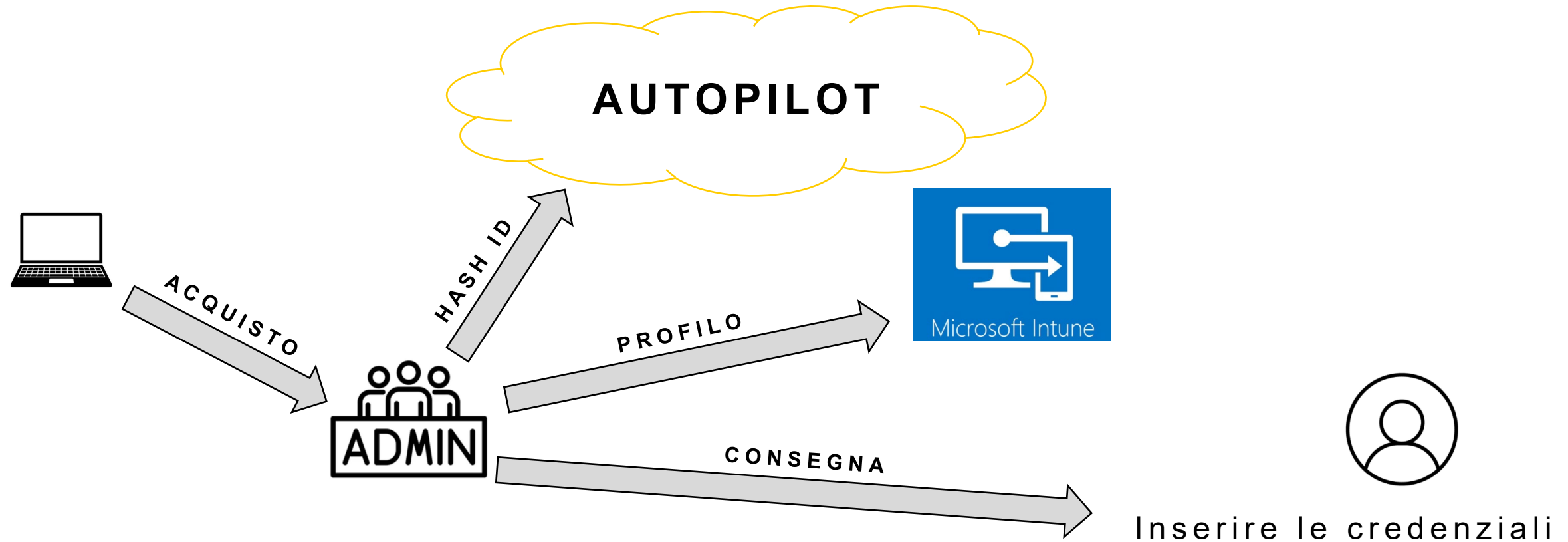
Name *

Description

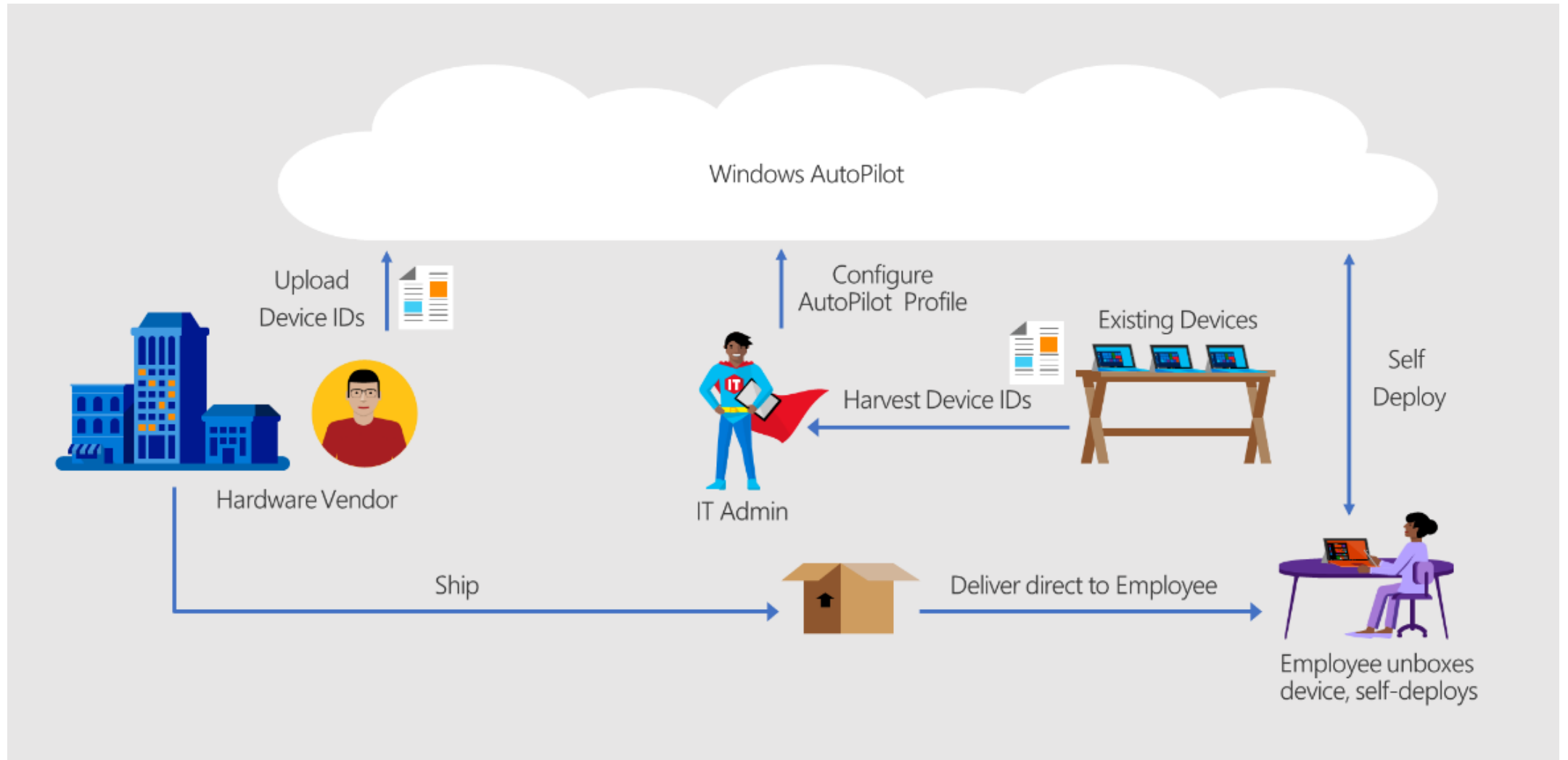
i By default, this profile can only be applied to Autopilot devices synced from the Autopilot service.[Learn more](#)

Convert all targeted devices to Autopilot ① ☐ No ☒ Yes

/ REGISTRAZIONE MANUALE



/ DIFFERENZA AUTO-MANUALE



MICROSOFT 365 BUSINESS PREMIUM

SPUNTI DI RIFLESSIONE

/ Sicurezza non integrata

ManageEngine



Kaspersky
Anti-Virus

CITRIX®
XenMobile



MobileIron



Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

RESOL/E

/ Costi/benefici a confronto

PRODOTTO		FEATURES
COLLAB	Exchange Online Plan 1 (50 GB) Exchange Online Archiving for Exchange Online (1,5 TB) Suite Office completa (15 installazioni per licenza) Ms Teams OneDrive SharePoint Planner Forms	
	Microsoft Defender for Office 365 P1 (filtro antiphishing e antispam avanzato) Intune Mmd (5 device per licenza) Entra ID Plan 1	Patch management Software Distribution Conditional Access Autopilot Azure Information Protection Upgrade Sistema Operativo Threat Analytics Vulnerability Management Secure Score
SECURITY	Windows Pro Defender for Business	

EMPOWERING INTUNE E ENTRA ID

/ DOMANDE

Chiedete in chat le vostre curiosità

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E

EMPOWERING INTUNE E ENTRA ID

/ CONTATTI

Resolve è la società di consulenza di ErgonGroup

CONTATTI

✉ info@resolve-consulenza.it

🌐 www.resolve-consulenza.it

☎ +39 049 636 5600

Sede legale

Viale Dell'Industria, 21
35129 – Padova (PD)

Sedi operative

Friuli Venezia Giulia, Veneto,
Lombardia, Toscana



RESOL/E

RESOL/E

by ErgonGroup