Be Connected day

collabdays

Intune Suite e AI: siamo già oltre il “Modern Device Management”?

Riccardo Corna

Microsoft MVP - IT Specialist - Microsys

Davide Salsi

User Endpoint Solution Architect - 4wardPRO | Microsoft MVP

30 . 5 . 2024

Milan

Sponsors

Endorsed by

Microsoft

Platinum sponsors

Cisco

EPOS

farnetworks green team

Insight

Gold sponsors

ACS Future at your side

ASC

audiocodes

ribbon

kramer

BLUDIS

FEITIAN

IE

4wardPRO

imagicle ZUCCHETTI

Inside Technologies

Lenovo

Ledestar

MAXHUB

neat.

OVERNET. upgrade your digital skills

SHURE

Q-SYS

spectralink

ALLNET.ITALIA

Silver sponsors

AVApvee

COMMED I A DIGITAL TRANSFORMATION

International Association of Microsoft Channel Partners

LOBRA

mida solutions

PIASYS

QUANTURE

ESPC

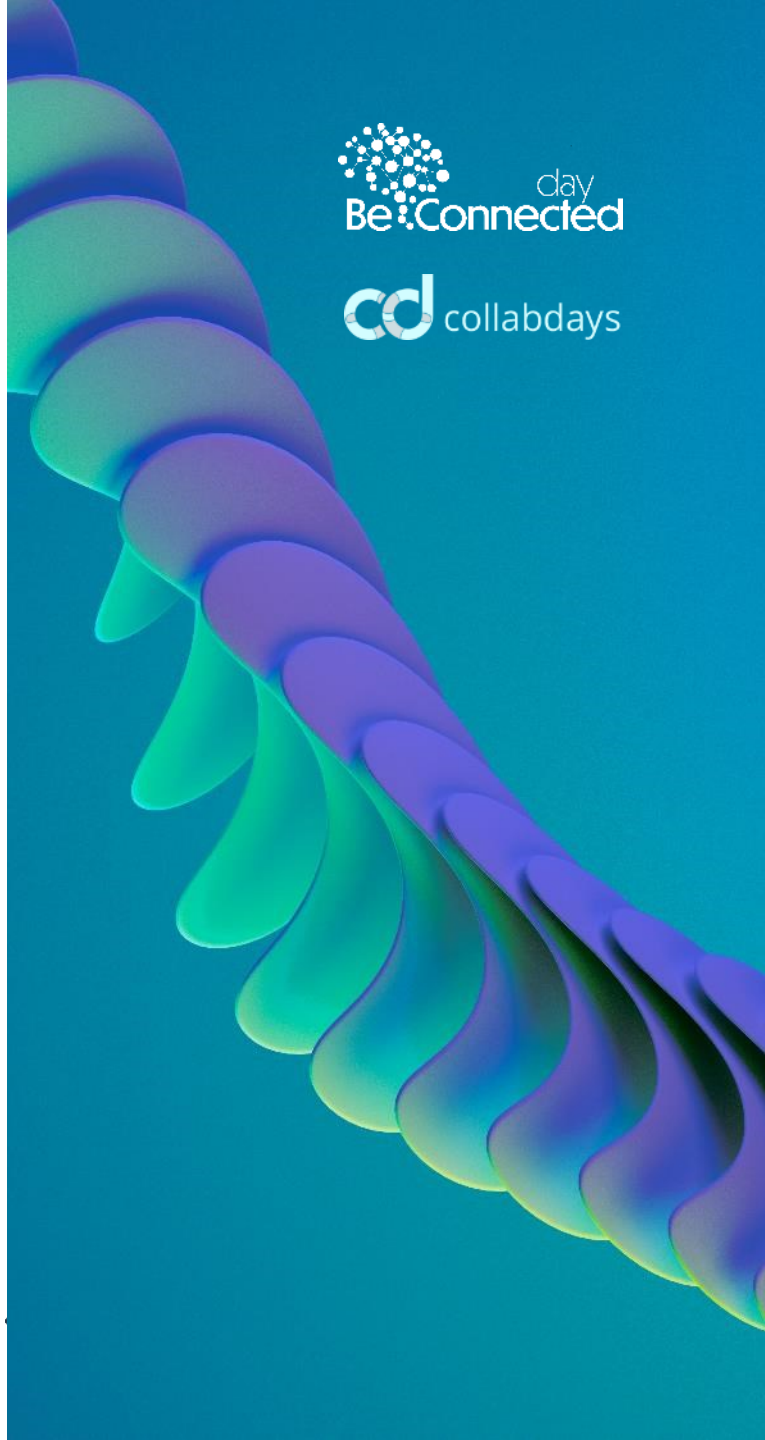
Tech partner

run events

Be Connected day

collabdays

TABLE OF CONTENTS



ABOUT ME

NICE TO SEE YOU

Davide Salsi

User Endpoint Solution Architect
@4wardPRO | Microsoft MVP

- USER ENDPOINT SOLUTION ARCHITECT @4WARDPRO
- MICROSOFT MVP
- CO-FOUNDER ITALIAN USER GROUP SU MICROSOFT INTUNE E CONFIGURATION MANAGER
- CO-AUTHOR CLOUDCOMMUNITY.IT E WINDOWSERVER.IT

ABOUT ME

NICE TO SEE YOU

Riccardo Corna

Senior Consultant @ Microsys
Microsoft MVP (Security)

- SENIOR CONSULTANT @ MICROSYS
- MICROSOFT MVP (SECURITY)
- CO-FOUNDER DEL MICROSOFT SECURITY ITALIAN USERS GROUP (LINKEDIN)
- MI PIACE CREARE CONTENUTI E CONDIVIDERLI
- BLOG: https://itspecialist.cloud

01

Riassunto puntate precedenti...


SIGNORI
E' STATO UN ONORE SUONARE CON VOI
imgflip.com

INTUNE SUITE

Intune Plan 1

Standard solution

Included in EMS E3, ME3, ME5, F1, F3, and Business Pro

Intune Plan 2

Add to Plan 1 to utilize these solutions:

Included

- Tunnel for Mobile App Management
- Specialty devices
- *Future advanced capabilities*

Prerequisite

- Intune Plan 1

Intune Suite

Add to Plan 1 to utilize these solutions

Included

- Remote help
- Endpoint Privilege Management
- Advanced Endpoint analytics
- Simplified app patching and packaging
- Cloud certificate management
- All Intune Plan 2 features

Prerequisite

- Intune Plan 1

02 Privilege Management

LEAST PRIVILEGE

Il secondo principio del modello Zero Trust è quello di assegnare i privilegi minimi necessari per svolgere le proprie attività adottando:

- accessi “just-in-time” (JIT) e “just-enough-access” (JEA)
- policy adattive basate sul rischio
- protezione dei dati

STATISTICHE LEAST PRIVILEGE

ROM	Issues found	% of customers with the issue
Higher		
15	No advanced MFA protection mechanisms enabled	37%
15	Poor user lifecycle management	21%
15	Lack of EDR coverage	13%
15	Lack of detection controls	10%
13	Resource exposed to public access	2%
12	Insufficient protections for local accounts	60%
12	Missing security barrier between cloud and on-premise	54%
12	Insecure Active Directory configuration	43%
12	Insufficient device security controls	8%
11	Legacy cloud authentication is still used	47%
11	No advanced password protection enabled	37%
11	Missing content based MFA protection mechanisms	24%
11	Insecure operating system configuration	3%
Medium		
8	Legacy and unsecure protocols	18%
7	Missing or inconsistent update management	43%
6	Missing cloud application management and monitoring	21%
6	No privileged identity management solution	8%
6	No MFA, or MFA not mandatory for privileged accounts	21%
6	Weak email protection against common threats	16%
6	Legacy or unsupported operating systems	14%
Lower		
4	No privilege separation	41%
4	No hardened workstations used for administration	23%
4	Missing data classification and sharing restrictions	5%
3	No vulnerability management	30%
2	No adherence to the Least Privilege Principle	63%

Rif: Report sulla difesa digitale Microsoft 2023

ENDPOINT PRIVILEGE MANAGEMENT

Microsoft Endpoint Privilege Management (EPM)

ha lo scopo di autorizzare l’esecuzione di determinati processi da parte di utenti che non detengono privilegi elevati; ciò avviene attraverso la definizione di policy di sicurezza che determinano chi può accedere a determinati privilegi e su quali processi.

ENDPOINT PRIVILEGE MANAGEMENT - PRO

1

Processo autorizzazione controllato

Le richieste di elevazione di privilegi vengono gestite in modo sicuro e tracciato, garantendo che solo gli utenti autorizzati possano eseguire determinate azioni.

2

Esecuzione specifici processi

E’ possibile consentire l'esecuzione di specifici processi con diritti elevati, senza esporre l'intero sistema operativo a rischi di sicurezza.

3

Ridotto coinvolgimento dell’IT

Il reparto IT viene coinvolto marginalmente nel processo di elevazione dei privilegi riducendo così tempi (e di conseguenza costi) legati ad attività non strategiche.

4

Integrato nel Sistema Operativo

Microsoft EPM è integrato direttamente nel sistema operativo, offrendo una soluzione nativa che non richiede software aggiuntivi.

ENDPOINT PRIVILEGE MANAGEMENT - CONTRO

1

Definizio

preve

re

Support Approved

app che
legi elevati per
reventivamente le
autorizzazione.

Demo time

Davide Salsi

Microsoft Intune admin center

admin@m365avengers....
AVENGERS

Avengers ...

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Get started with Copilot

Explore new ways to work smarter and faster using the power of AI.

Learn more about Copilot in Intune

Policy management

Get help with settings while creating a new configuration policy. Let Copilot analyze the potential security impact of a policy.

See how Copilot can help

Troubleshooting

Quickly analyze apps and policies assigned to a device to help determine issues affecting your users.

See how Copilot can help

Status

Devices not in compliance
14

Configuration policies with error or conflict
0

Client app install failure
2

Connector errors
1

Service health
Healthy

Account status
Active

Spotlight

Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

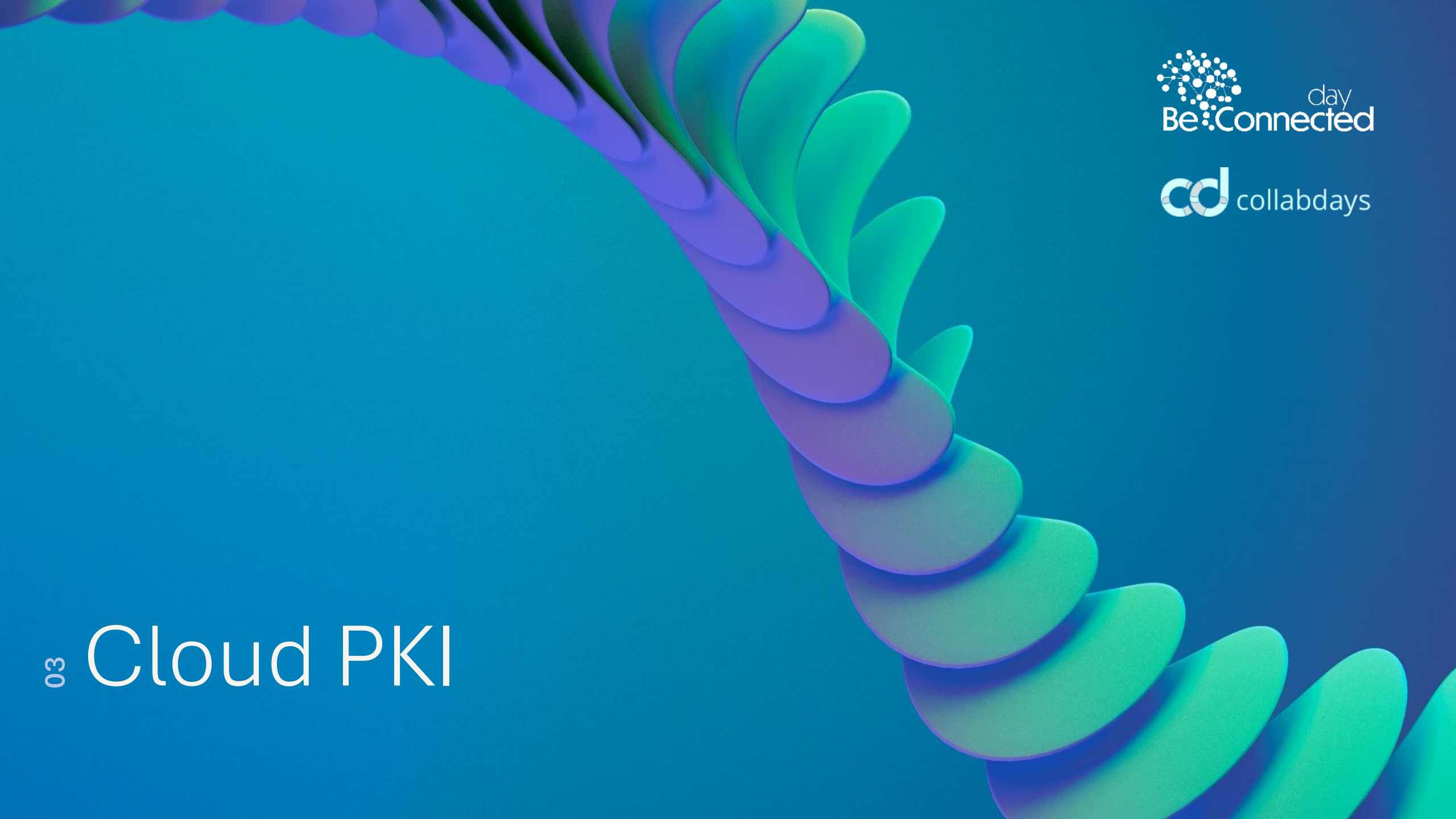
Explore

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

Get more out of Intune



03 Cloud PKI

MICROSOFT CLOUD PKI

Microsoft Cloud PKI è una soluzione gestita da Microsoft che fornisce servizi di infrastruttura a chiave pubblica (PKI) tramite il cloud.

La PKI è un insieme di ruoli, policy e procedure necessarie per creare, gestire, distribuire e revocare certificati digitali.

1 Rimozione server on-premise

Consente la rimozione dei server on-premise necessari al funzionamento dell'Infrastruttura PKI stessa.

2 Rimozione soluzioni di republishing

Consente la rimozione di soluzioni per il republishing della propria infrastuttura PKI verso l'esterno come Network Device Enrollment Service (NDES) e reverse proxy

3 Rilascio certificati multi-piattaforma

Consente di rilasciare in modo semplice e veloce certificati sulle piattaforme gestate da Intune: Windows – iOS – macOS – Android

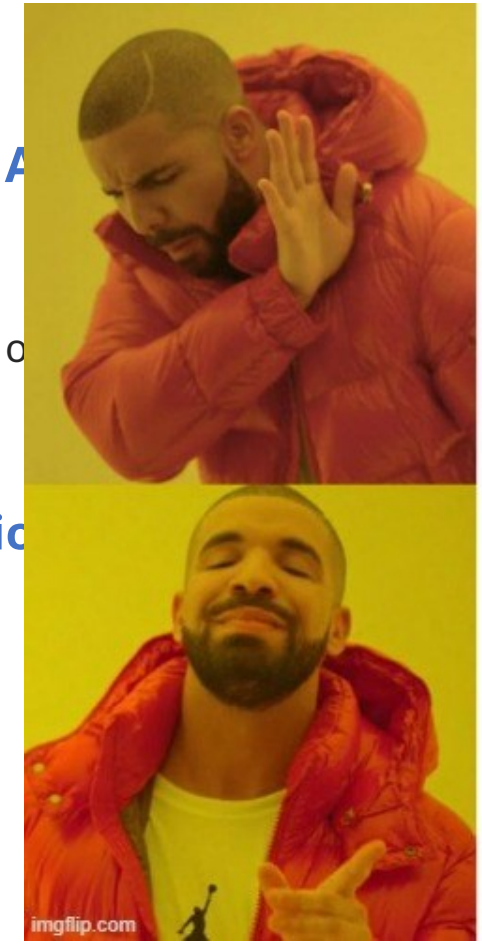
MICROSOFT CLOUD PKI - STEP

1. Creazione Certificate A

- Root CA
- Issuing CA (Intune – Bring your o

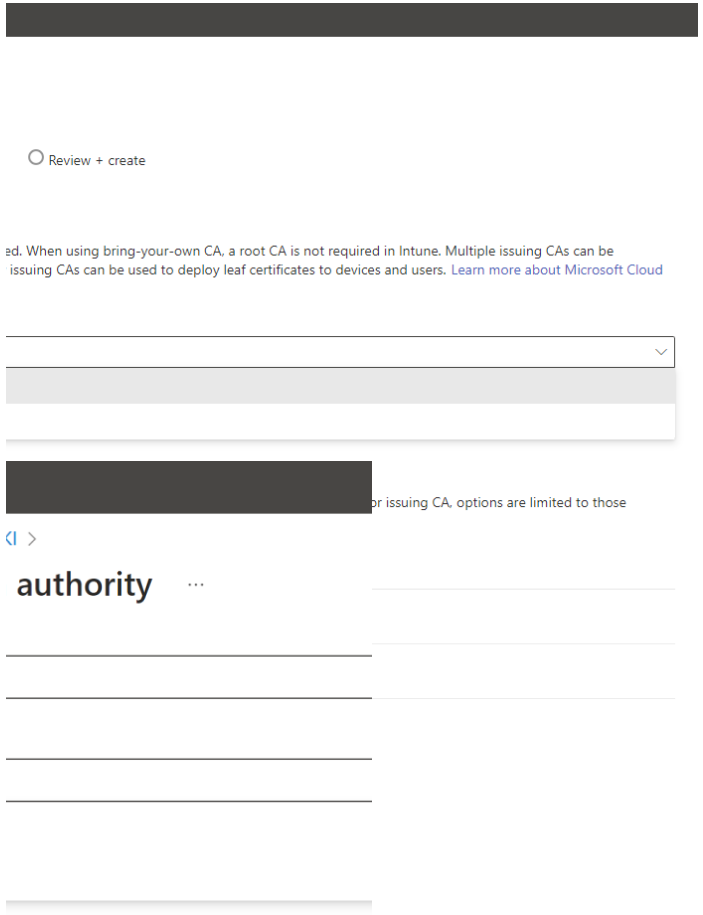
2. Deploy Trusted Certific

2. Deploy SCEP profile



PKI

CLOUD PKI



Demo time

Davide Salsi

Microsoft Intune admin center

admin@m365avengers....
AVENGERS

Avengers

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Get started with Copilot

Explore new ways to work smarter and faster using the power of AI.

Learn more about Copilot in Intune

Policy management

Get help with settings while creating a new configuration policy. Let Copilot analyze the potential security impact of a policy.

See how Copilot can help

Troubleshooting

Quickly analyze apps and policies assigned to a device to help determine issues affecting your users.

See how Copilot can help

Status

Devices not in compliance
14

Configuration policies with error or conflict
0

Client app install failure
2

Connector errors
1

Service health
Healthy

Account status
Active

Spotlight

Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

Explore

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

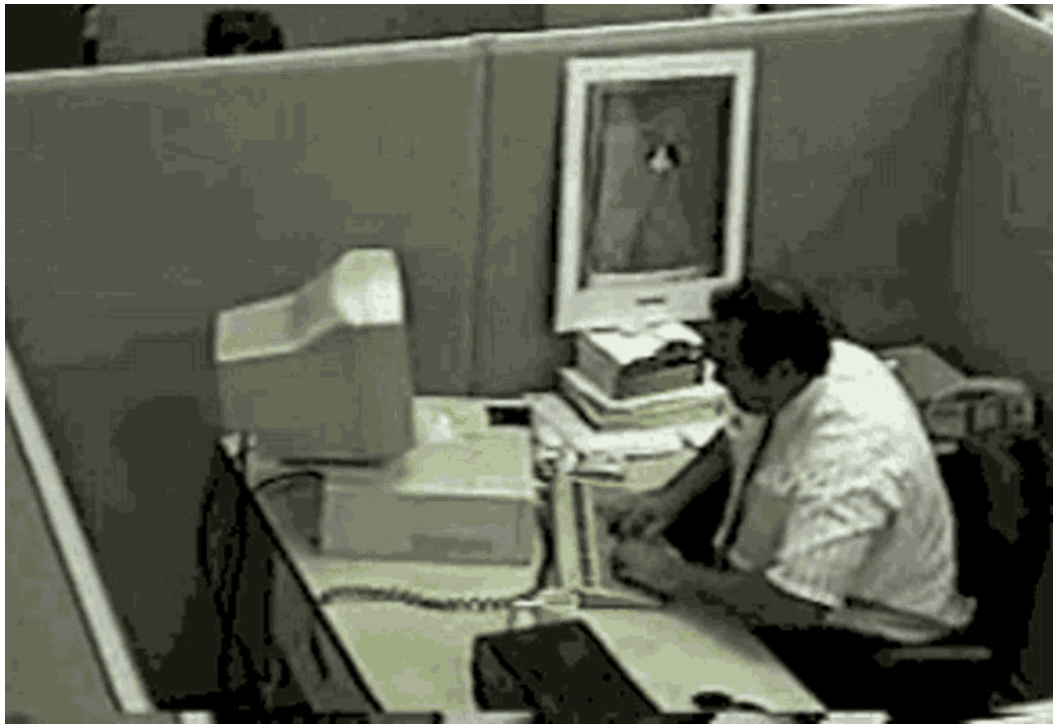
Explore

Get more out of Intune

04 Advanced Analytics

INTUNE ADVANCED ANALYTICS

Intune Advanced Analytics



- Battery health

INTUNE ADVANCED ANALYTICS - VANTAGGI

1

Miglioramento dell’esperienza utente

Identificare **criticità** che generano scarsa esperienza utente (**cattiva reputazione dell’IT**).

2

Informazioni dettagliate su device e app

Ottenere una **visione chiara** dello stato e dell'uso dei dispositivi, facilitando il monitoraggio delle prestazioni (es: Hardware obsoleto, configurazioni errate, BSOD).

3

Risoluzione proattiva delle anomalie

Identificare e risolvere **proattivamente** problemi specifici legati ai dispositivi o alle applicazioni in modo da ridurre significativamente i tempi di inattività.

4

Riduzione dei costi IT

Contribuire a un significativo **risparmio sui costi IT** attraverso ottimizzazioni e risoluzioni proattive.

Demo time

Davide Salsi

Microsoft Intune admin center

admin.salsid@4wardpro.it
4WARDPRO

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home >

Reports

Search

- Overview

Device management

- Device compliance
- Device configuration
- Group policy analytics
- Windows updates
- Cloud attached devices (preview)
- Cloud PC overview

Endpoint security

- Microsoft Defender Antivirus
- Firewall

Analytics

- Endpoint analytics

Intune data warehouse

- Data warehouse

Azure monitor

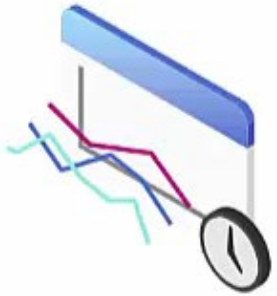
- Diagnostic settings
- Log analytics
- Workbooks

Monitor the health and activity of your endpoints

Use Intune reporting to monitor endpoint compliance, health, and trends in your organization.

Organizational reports

Generate a summarized report of the latest, overall state of your endpoints and apply filters to refine your data.



Trends reports

Create a report from historical data to help you identify patterns and trends over time.

Advanced reports

Create custom queries and visualizations from raw data with the help of Log Analytics and Azure monitor workbooks.

05

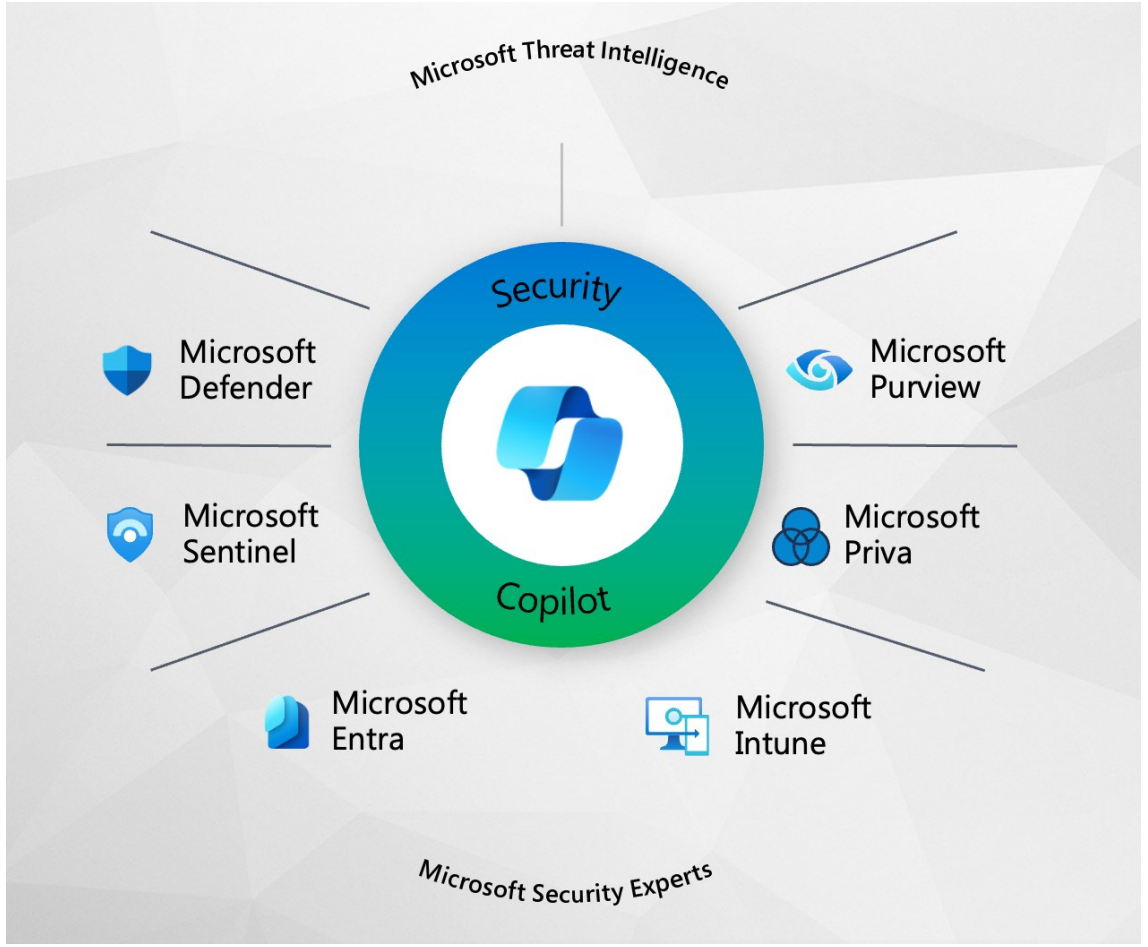
Copilot for Security

MICROSOFT COPILOT FOR SECURITY: COS'È, ESPERIENZE, INTERAZIONI

Microsoft Copilot for Security è uno strumento di analisi della sicurezza basato su intelligenza artificiale generativa. Esistono due modi per sfruttare la sinergia tra Copilot for Security e Intune:

- **Microsoft Copilot in Intune:** detta «embedded experience». Copilot è integrato nel portale di Microsoft Intune. I suggerimenti di Copilot e i loro output sono direttamente contestualizzati nell'ambito di Intune.

- **Microsoft Copilot for Security:** detta anche «stand-alone experience», è il vero e proprio portale di Copilot for Security. Da qui è possibile ottenere informazioni su tutti i prodotti, oltre che Intune.



COSA CI SERVE PER INIZIARE?

SOTTOSCRIZIONE AZURE

Copilot in Intune è incluso una volta attivato Copilot for Security. Non ci sono altri requisiti di licenza o licenze specifiche di Intune per utilizzare Copilot in Intune.

SECURITY COMPUTE UNITS (SCUS)

Le SCU sono le unità di risorse necessarie per garantire l'operatività computazionale di Copilot for Security.
Viene fatturato il consumo Azure su base oraria in un modello di capacità predefinita.
Le SCU possono essere aumentate/diminuite.

CAPACITY

La capacità, nel contesto di Copilot for Security, è una risorsa di Azure che contiene le SCU. Le SCU sono fornite per Copilot for Security.

Set up your security capacity

Security copilot is a generative AI-first platform with asset mapping, tiered storage, policy services, integration services, and more. It powers all workloads of the security platform.

Azure Subscription

Resource group

Create a new one

Capacity name

CopilotForSecurityCapacity

Prompt evaluation location

United States

If this location has too much traffic, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region

US East

Select the number of units

Security compute units provide the computing power that drives the Copilot for Security experience (USD 4 per unit).

Security compute units

3

Read more about security compute units and the recommended number based on your organization's size and probable usage.

I acknowledge that I have read, understood, and agree to the Terms and Conditions

Continue

Microsoft Copilot for Security (preview)

Microsoft

Microsoft Copilot for Security (preview)

Add to Favorites

Microsoft | Azure Service

Plan

Microsoft Copilot for Security

Create

Overview Plans Usage Information + Support Ratings + Reviews

Provision capacity in Security Compute Units (SCU) to run Copilot for Security workloads. These workloads provide insights, evaluate prompts, run promptbooks and automate them in both the standalone product and embedded experiences across Microsoft Security.

- Flexibly provision compute units to meet your organization needs.
- Easily manage costs with in-product dashboard.

More products from Microsoft See All

Active Directory Health Check
Microsoft
Azure Service
Assess the risk and health of Active Directory environments.
Create

AD Replication Status
Microsoft
Azure Service
Identify Active Directory replication issues in your environment.
Create

Device Update for IoT Hub
Microsoft
Azure Service
Securely and Reliably update your devices with Device Update for IoT Hub.
Create

Front Door and CDN profiles
Microsoft
Azure Service
Azure Front Door and CDN profiles is security led, modern cloud CDN that provides static and dynamic content acceleration, global load balancing and enhanced security for your apps,
Create

Set up your Copilot capacity

Basics | Review + Create

This capacity will provide the computing power that drives the Microsoft Copilot for Security experience.

Project Details

Subscription * [redacted]

Resource group * [redacted]

Create new

Capacity details

Name your capacity and select a location

Capacity name * Enter a name

This name must be unique, use at least 3 characters, and contain no symbols except a hyphen.

Prompt evaluation location * United States (US)

This selection will affect where your prompts are evaluated and how your usage is priced.

☐ If this location is busy, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Azure resource region US East

Security compute units

Security compute units provide the computing power that drives the Security Copilot experience ($4 per unit). Read more about security capacity units and the recommended number based on your organization's size and probable usage.

Number of units * 1

Estimated monthly cost $2880/month

☐ I acknowledge that I have read, understood, and agreed to the Terms and Conditions

Previous Next Review + create

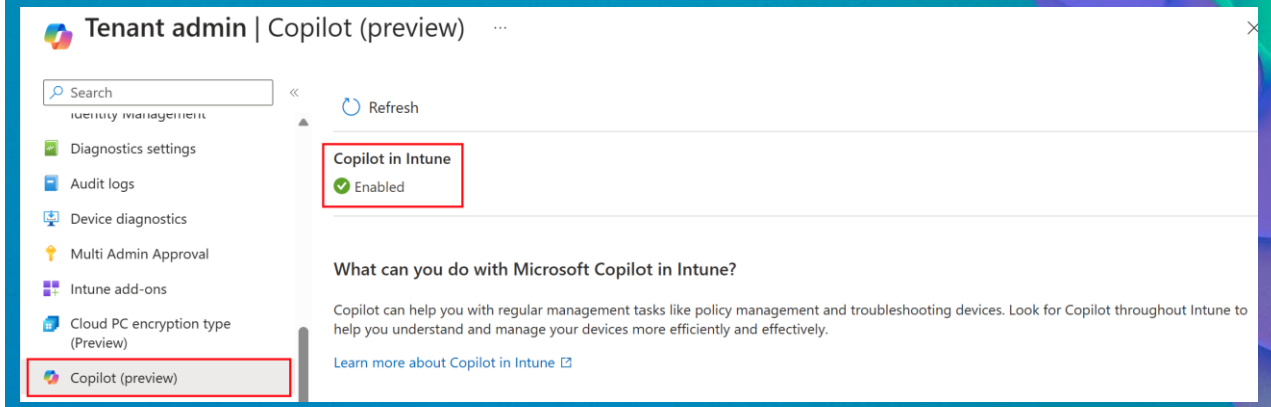
Give feedback

CONFIGURAZIONE DI COPILOT

Prima di poter utilizzare le funzionalità di Copilot in Intune, è necessario configurare Microsoft Copilot for Security e completare la prima esecuzione nell'apposito portale di Microsoft Copilot for Security.

È possibile verificare lo stato di attivazione ne portale amministrativo di Intune:

Intune > **Tenant Administration** > **Copilot**



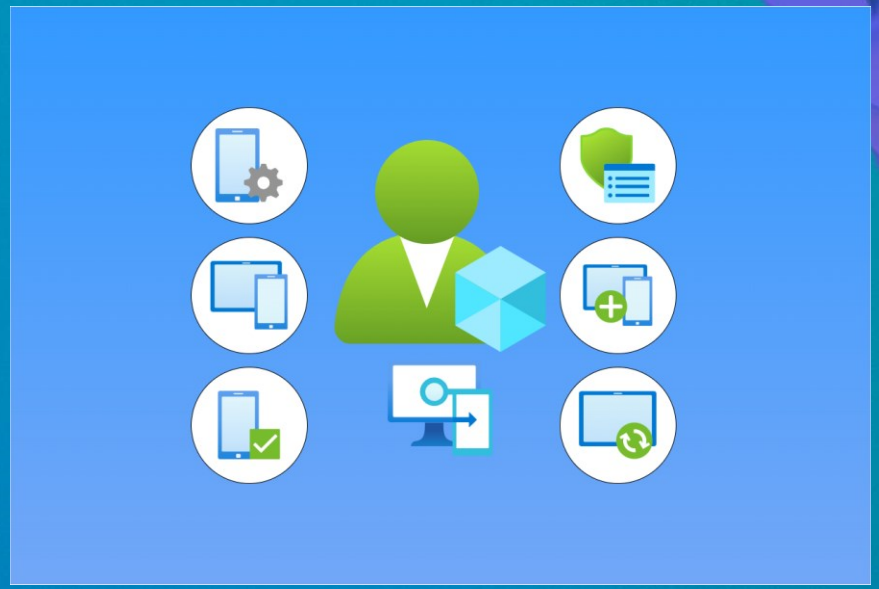
CONFIGURAZIONE DEI RUOLI (RBAC)

L’accesso a Copilot in Intune è gestito tramite Copilot for Security o Microsoft Entra ID.

Quando un amministratore invia un prompt, Copilot può accedere solo ai dati per cui l'amministratore ha i permessi, verificando i ruoli RBAC e gli scope tag.

Per accedere a tutti i dati di Intune in Copilot for Security, utilizza uno dei seguenti ruoli in Microsoft Entra ID:
- Global Administrator
- Intune administrator

Se non admin, specificatamente nell’ambito del RBAC di Intune, è necessario avere come minimo **l’Endpoint Security Manager**.



COPILOT FOR SECURITY

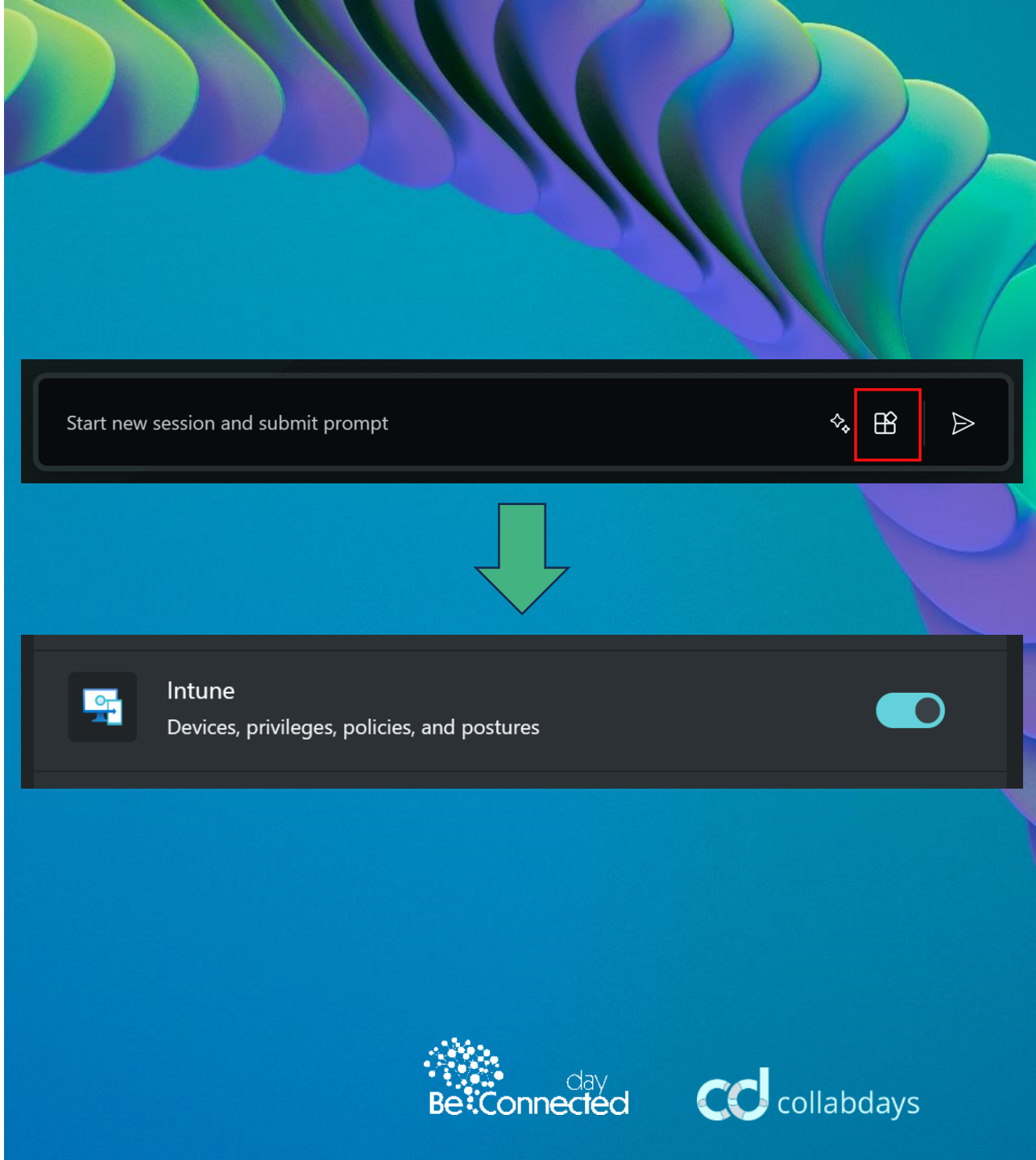
ATTIVAZIONE PLUGIN DI INTUNE

Per utilizzare Copilot in Intune, è necessario abilitare il plug-in Intune in Copilot for Security.

Questo plug-in consente di accedere ai dati di Intune e di utilizzare Copilot nel portale.

Per attivare:

Sources (barra dei prompt > angolo destro).



COME POSSIAMO USARLO?

1

Per saperne di più su singole impostazioni, il loro impatto e i valori consigliati

2

Per riassumere i profili di configurazione e I loro settaggi

3

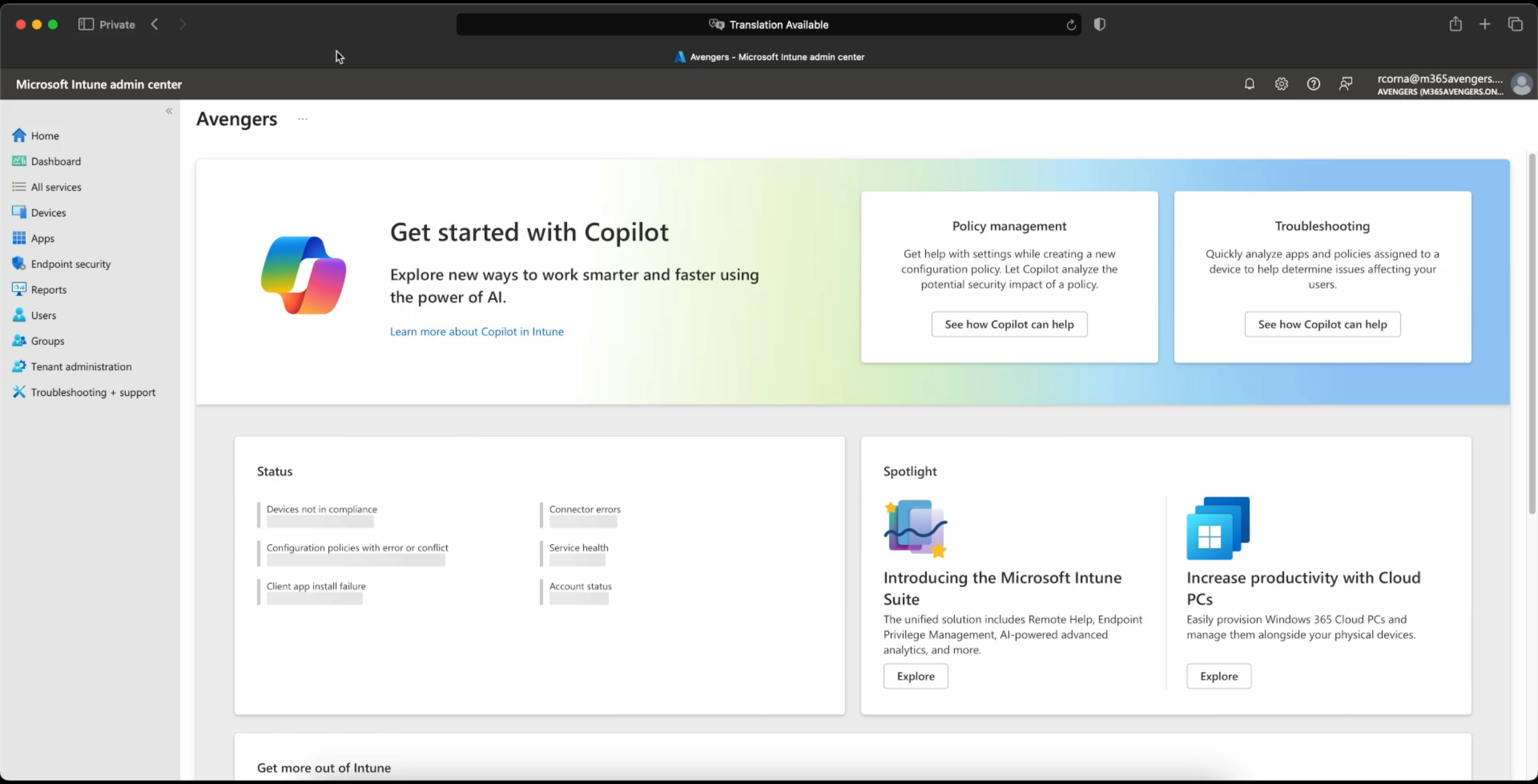
Per avere informazioni dettagliate e correlate sui dispositivi

4

Per fare troubleshooting

Demo time

Riccardo Corna


Private
Translation Available
Avengers - Microsoft Intune admin center
Microsoft Intune admin center
rcorna@m365avengers....
AVENGERS (M365AVENGERS.ON...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Avengers
Get started with Copilot
Explore new ways to work smarter and faster using the power of AI.
Learn more about Copilot in Intune
Policy management
Get help with settings while creating a new configuration policy. Let Copilot analyze the potential security impact of a policy.
See how Copilot can help
Troubleshooting
Quickly analyze apps and policies assigned to a device to help determine issues affecting your users.
See how Copilot can help
Status
Devices not in compliance
Connector errors
Configuration policies with error or conflict
Service health
Client app install failure
Account status
Spotlight
Introducing the Microsoft Intune Suite
The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.
Explore
Increase productivity with Cloud PCs
Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.
Explore
Get more out of Intune

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Avengers

Get started with Copilot

Explore new ways to work smarter and faster using the power of AI.

Learn more about Copilot in Intune

Policy management

Get help with settings while creating a new configuration policy. Let Copilot analyze the potential security impact of a policy.

See how Copilot can help

Troubleshooting

Quickly analyze apps and policies assigned to a device to help determine issues affecting your users.

See how Copilot can help

Status

Devices not in compliance
19

Configuration policies with error or conflict
0

Client app install failure
2

Connector errors
1

Service health
Healthy

Account status
Active

Spotlight

Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

Explore

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

IDEE DI PROMPT

1

INFORMAZIONI GENERALI

- What apps are added to Intune?
- What Intune apps are assigned the most?
- How many devices were enrolled in Intune in the last 24 hours?
- Tell me about Intune devices for Jon Smith.

2

DESTINATARI DELLE POLICY

- How many users is ContosoApp assigned to?
- Which groups are ContosoApp assigned to?
- How many apps are assigned to the device ID Enter the device ID in Intune?
- Why is the "Allow Microsoft Store App to auto update" policy applying to DeviceA?

3

DISPOSITIVI

- What devices are used by UserA@contoso.com?
- What groups is DeviceA in?
- Tell me about DeviceA.
- Who is the primary user for DeviceA?
- Is ContosoApp installed on DeviceA?

4

SIMILITUDINI E DIFFERENZE

- What is the hardware configuration difference between the DeviceA and DeviceB devices?
- What are the similarities in compliance policies between the DeviceA and DeviceB devices?


Q&A

Microsoft Security Italian User Group

Microsoft Intune Italian User Group

AVD & W365 Italian User Group

ITSpecialist.cloud

emmblog.com

We care about your feedback

Please take a moment to tell us your opinion using the run.events app.

Be Connected day

collabdays

Grazie!

30 . 5 . 2024
Milan

Riccardo Corna
Microsoft MVP - IT Specialist - Microsys

Davide Salsi
User Endpoint Solution Architect - 4wardPRO | Microsoft MVP, Security