



Edition

Implementing and building advanced Microsoft Entra ID Conditional Access scenarios

Kenneth van Surksum | Secure At Work

Workplace Ninja
Summit 2023





Agenda

www.wpninjas.eu
#WPNinjaS

Are you REALLY ready to go “Advanced” ?

Back to basics

Microsoft Defender for Cloud Apps

Conditional Access App Control

Authentication Context and Strength

Authentication Context, Authentication Strength

Filters

Filter for Devices, Filters for Apps and Workload Ids

Sensitivity Labels

Protect containers

Key takeaways:

- Understand integration with MDA
- What is Authentication Context and Authentication Strength and how can I use it?
- How to “trigger” Conditional Access in scenario’s where we are not authenticating
- Using filters to make CA dynamic
- Using Sensitivity Labels to control access to data hosted on SharePoint
- And much more..

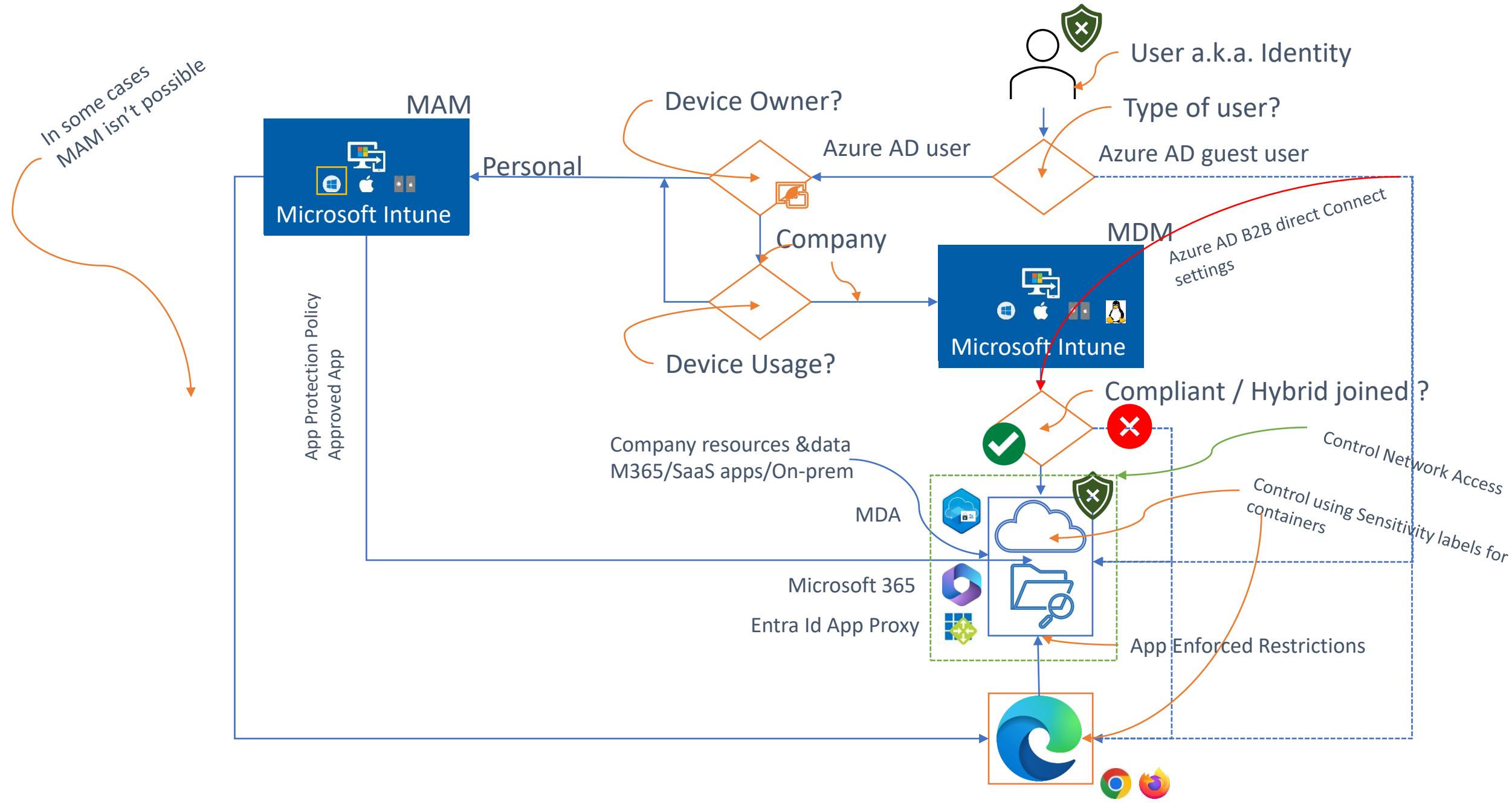
A close-up photograph of a man's torso and hands. He is wearing a bright red suit jacket over a white dress shirt with a visible collar and a gold-colored bow tie. His hands are clasped in front of him, wearing light blue gloves. A small blue pocket square is visible in his jacket's breast pocket.

**Are you REALLY ready to go
“Advanced” ?**

Goals



Protect company data hosted in Microsoft 365 and protect identity and network location of users



Compliant

or

Hybrid Microsoft Entra Joined

Non-compliant

*Can be managed
Or unmanaged*



Azure AD Conditional Access Whitepaper version 1.4

December 2022 edition, 140 pages of Conditional Access goodness. Written by: Kenneth van Surksum

Now also available to download and import from Github
Available at: <https://www.vansurksum.com>

White paper

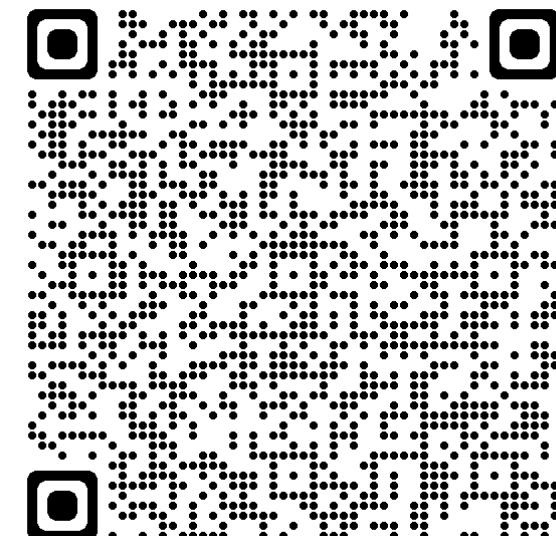
Latest release: The December 2022 update of the Conditional Access demystified whitepaper.

- Major release (from 95 to 140 pages)
- Includes updated workflow cheat sheet
- Much more information added



Download the paper from my blog at:

<https://www.vansurksum.com/2022/12/15/december-2022-update-of-the-conditional-access-demystified-whitepaper-and-workflow-cheat-sheet/>



About “Kenneth van Surksum”

Focus

Modern Workplace Consultant, Microsoft Certified Trainer, Co-founder and organizer at Workplace Ninja User Group Netherlands



From

The Netherlands

My Blog

<https://www.vansurksum.com>



Certifications

Microsoft 365 Certified Enterprise Administrator



Microsoft Certified Azure Solutions Architect



Hobbies

Cooking on my Kamado Joe & Sports



Contact

kenneth@vansurksum.com

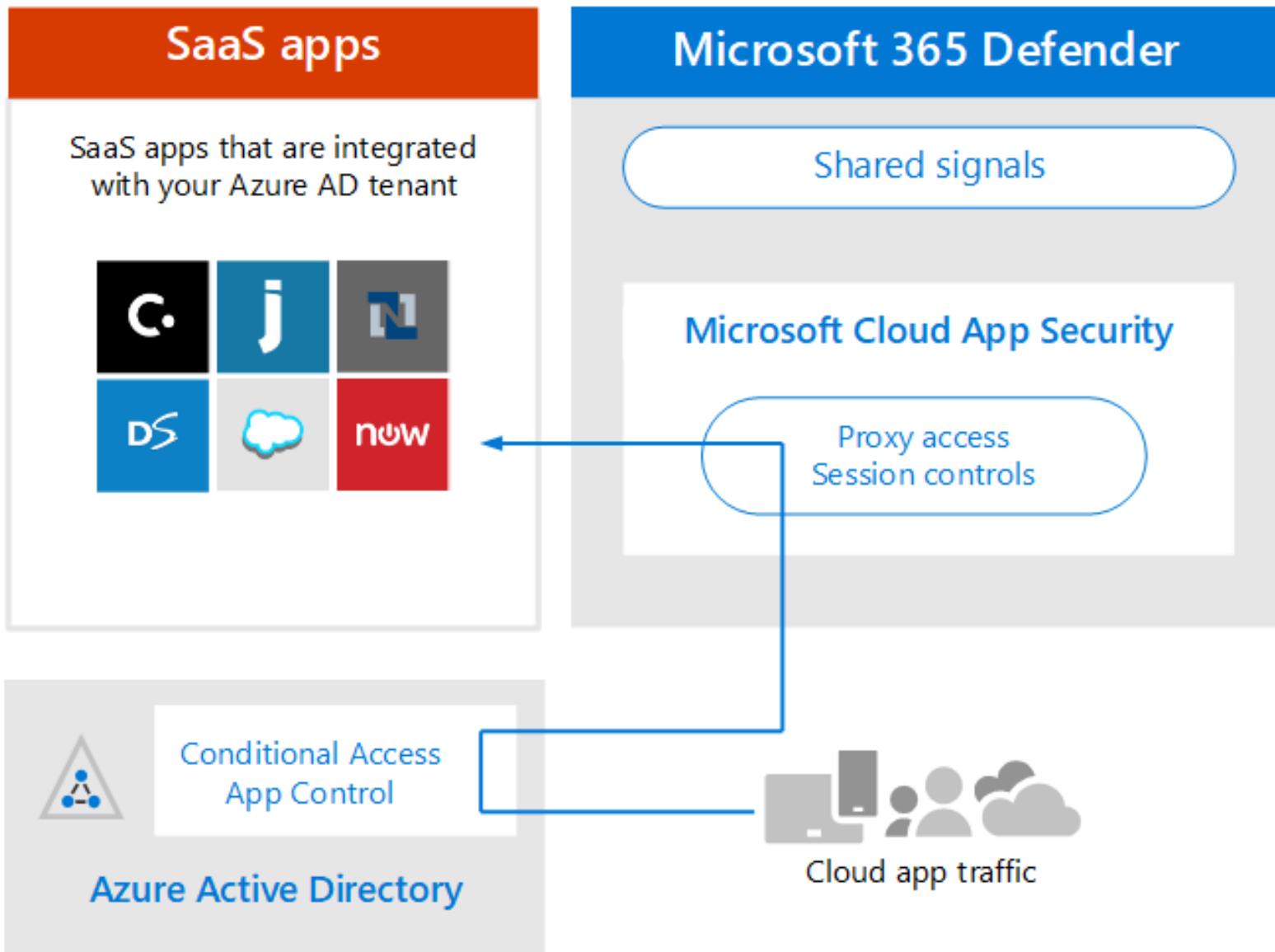


<https://twitter.com/kennethvs>

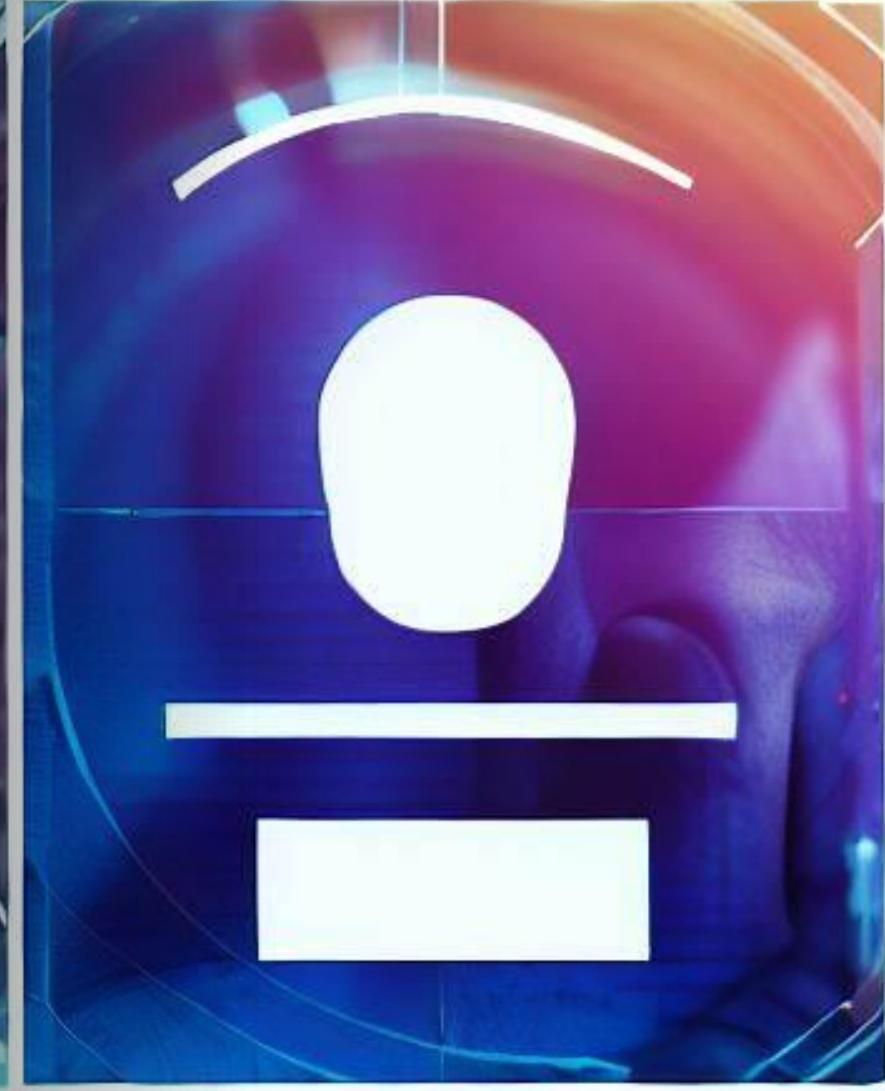
<https://www.linkedin.com/in/kennethvansurksum>



Microsoft Defender for Cloud Apps (MDA)



Authentication Context





What is an Authentication Context?

*Defined label used
outside of
Conditional Access,
which **triggers** a
Conditional Access
policy*

*Where can
Authentication
Context be
used?*

Protected Actions

Privileged Identity Management

Sensitivity Labels

Microsoft Defender for Cloud Apps

Possible Scenarios'

- Only allow protected actions to be performed from Hybrid joined/Compliant devices
- Require step-up authentication when performing protected action
- Only allow PIM activation from a Privileged Access Workstation (PAW)
- Trigger step-up authentication when elevating to a privileged role using PIM
- Require phishing resistant MFA when accessing highly sensitive SharePoint site
- Trigger TOC agreement when accessing files classified with sensitive label
- Much more.....



*Demonstration: Microsoft Defender for
Cloud Apps & Authentication Context*



Authentication Strength

Authentication Strength



Grant X

Control access enforcement to block or grant access. [Learn more](#)

Block access
 Grant access

Require multifactor authentication ⓘ

Require authentication strength (Preview) ⓘ

Multi-factor authentic... ▾

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication"

ⓘ To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Azure AD tenants for external users. Authentication strengths will only configure second factor authentication for external users.

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password and...



SMS



Voice

Better: Password and...



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)



Authenticator
(Phone Sign-in)



Window
Hello



FIDO2 security key



Certificates

Best: Passwordless

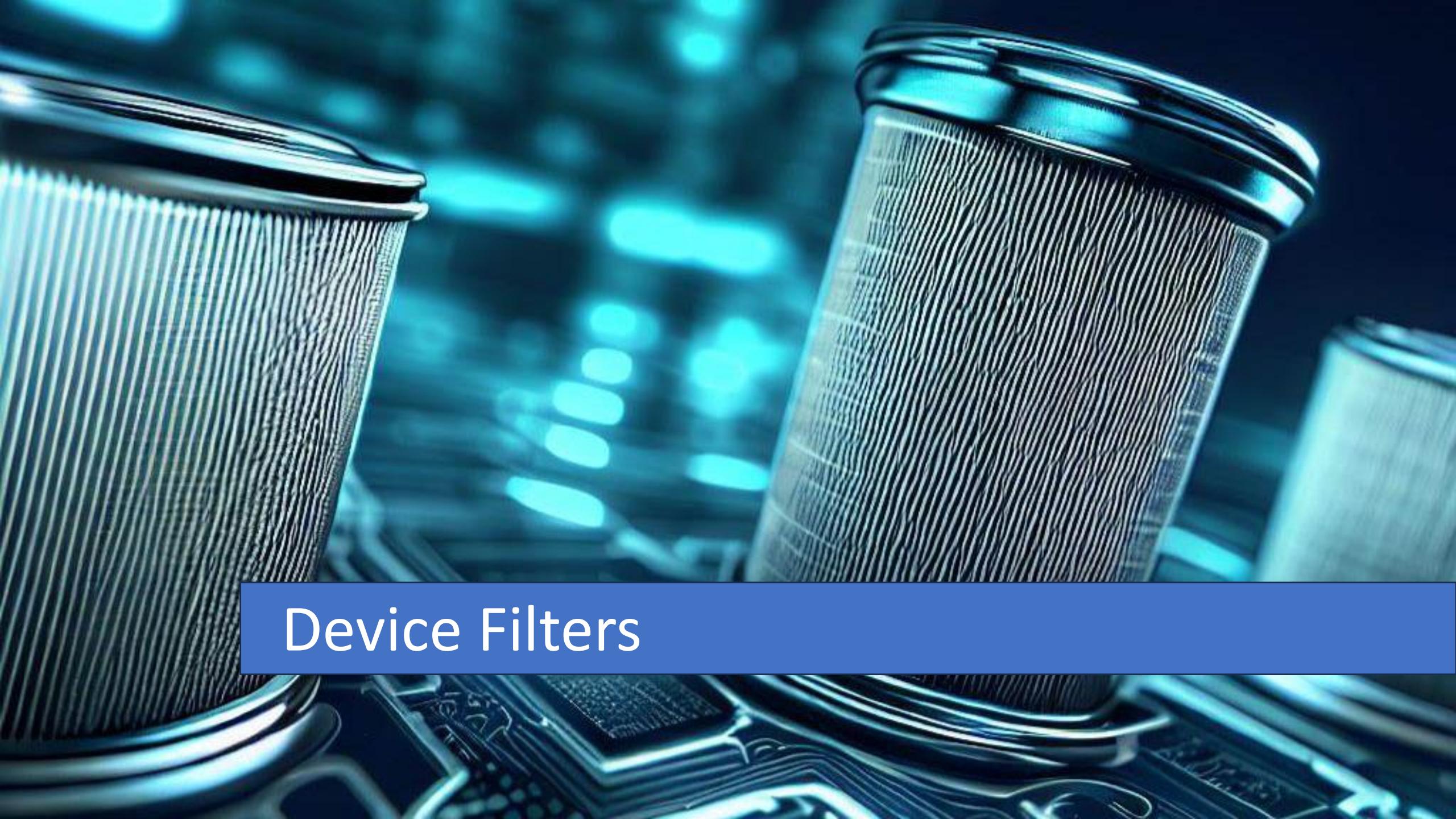
A photograph of a laboratory scene. In the foreground, a person wearing a white lab coat and blue nitrile gloves holds a clear glass Erlenmeyer flask containing a bright blue liquid. The background is slightly blurred, showing a black microscope on a stand, several clear glass test tubes in a rack, and a green glass bottle. The lighting is bright and clinical.

Demonstration: Authentication Strength in Action

A scene from Toy Story featuring Woody and Buzz Lightyear. Woody, on the left, has a neutral expression and is looking towards the right. Buzz, on the right, is in a dynamic pose with his arms raised, wearing his signature green space ranger suit. The background shows a room with a chalkboard and some shelves.

FILTERS.

FILTERS EVERYWHERE.



Device Filters

Device Filters

Device state (deprecated)

Control user access when the device the user is signing-in from is not "Hybrid Azure AD joined" or "marked as compliant". This has been deprecated. Use 'Filter for devices' instead. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

Select the device state condition used to exclude devices from policy.

- Device Hybrid Azure AD joined ⓘ
- Device marked as compliant ⓘ

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
	isCompliant	Equals	True
Or	trustType	Equals	Hybrid Microsoft Entra joined

+ Add expression

Rule syntax ⓘ

```
device.isCompliant -eq True -or device.trustType -eq "ServerAD"
```

×



deviceId, displayName, manufacturer,
mdmApplId, model, operatingSystem,
operatingSystemVersion, physicalIds,
profileType, systemLabels, trustType
and extensionAttributes

Beware!

For a device that is **unregistered** with Azure AD,
all device properties are
considered as null values

- Make properties available

Condition “Device Platform”
depends on User Agent
String

- Can easily be mimicked

Possible Scenario's

- Give access to Azure Management for privileged users only, coming from privileged or secure admin workstations
- Block access from devices running non supported Windows versions (like Windows 7, 8.1)
- Do not require MFA for specific account (traditional AD service accounts) when used on specific devices, like Teams phones or Surface Hub devices



Filters for Apps & Workload Identities

Role	↑↓	Description
<input type="checkbox"/>  Attribute Assignment Administrator 		Assign custom security attribute keys and values to supported Azure AD objects.
<input type="checkbox"/>  Attribute Assignment Reader 		Read custom security attribute keys and values for supported Azure AD objects.
<input type="checkbox"/>  Attribute Definition Administrator 		Define and manage the definition of custom security attributes.
<input type="checkbox"/>  Attribute Definition Reader 		Read the definition of custom security attributes.



Security and identity

Security comes as standard with all Microsoft products and technologies. No matter the size of your organisation, use these practical resources to get secure today and protect against threats in the future. Protect your data and block attacks with built-in security.

Workload Identities Premium

This per-workload identity licensed offer enables customers to detect and respond to compromised workload identities and helps simplify lifecycle management.

From €2.80 licenses/month

[Details](#)

[Compare](#)

Workload Identities Premium (Month to Month)

YOU OWN THIS

This per-workload identity licensed offer enables customers to detect and respond to compromised workload identities and helps simplify lifecycle management.

From €3.40 licenses/month

[Details](#)

[Compare](#)

Possible Scenario's

- Create a specific Conditional Access policy for all Apps which are tagged with a tag UsedByDepartment and value Finance
- Create a specific Conditional Access policy only allowing “tagged” workload identities to be used from trusted locations
- Create a specific Conditional Access policy, which blocks medium and high “Service Principal risk” for “tagged” workload identities

A close-up photograph of a pile of colorful dog tags. The tags are various colors including yellow, red, blue, green, and orange, and are stacked in a somewhat disorganized manner. They have a standard military-style hole punch on the left side.

Sensitivity Labels

Content can be shared with:

SharePoint OneDrive

Most permissive	Least permissive
<input type="radio"/>	<input type="radio"/>
Anyone Users can share files and folders using links that don't require sign-in.	
	New and existing guests Guests must sign in or provide a verification code.
	Existing guests Only guests already in your organization's directory.
	Only people in your organization No external sharing allowed.



Unmanaged devices

The setting you select here will apply to all users in your organization.

[Learn more about controlling access from unmanaged devices.](#)

To customize conditional access policies, save your selection and go to the [Azure AD admin center](#).

- Allow full access from desktop apps, mobile apps, and the web
- Allow limited, web-only access
- Block access

If you don't want to limit or block access organization-wide, you can do so for specific sites.

[Learn how to control access to specific sites by using Microsoft PowerShell](#)

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings.

Content can be shared with

- Anyone ①
Users can share files and folders using links that don't require sign-in.
- New and existing guests ①
Guests must sign in or provide a verification code.
- Existing guests ①
Only guests in your organization's directory.
- Only people in your organization
No external sharing allowed.

Use Azure AD Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context.

- Determine whether users can access SharePoint sites from unmanaged devices (which Intune).
 - ① For this setting to work, you must also configure the SharePoint feature that blocks or limits access from unmanaged devices.

- Allow full access from desktop apps, mobile apps, and the web
- Allow limited, web-only access ①
- Block access ①
- Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access rule.
[Learn more about authentication context](#)
 - High Authentication Context - Requires compliant device, TOU, or MFA



Demonstration: Granular SharePoint access on Unmanaged devices using Sensitivity Labels



Thank you