


What's new in MEM at Ignite



Panu Saukko
ProTrainIT
 @panusaukko
MVP



Sandy Zeng
Cloudway
 @sandy_tsang
MVP



Stefan Schörling
Onevinn
 @stefanschorling
MVP

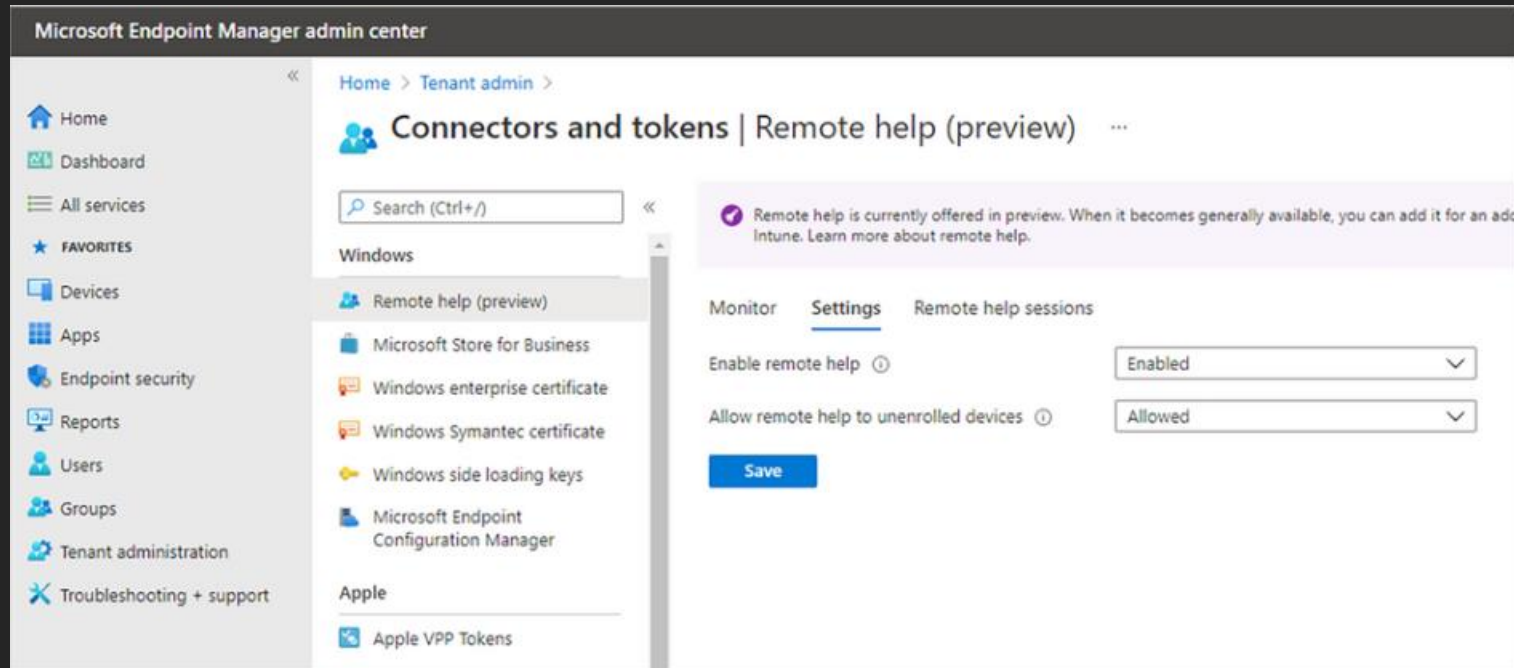
NORDIC

— VIRTUAL SUMMIT —

Remote help

Remote help

- New remote assistance tool
- Integrated with Intune






Remote session RBAC

- Own permissions

Microsoft Endpoint Manager admin center

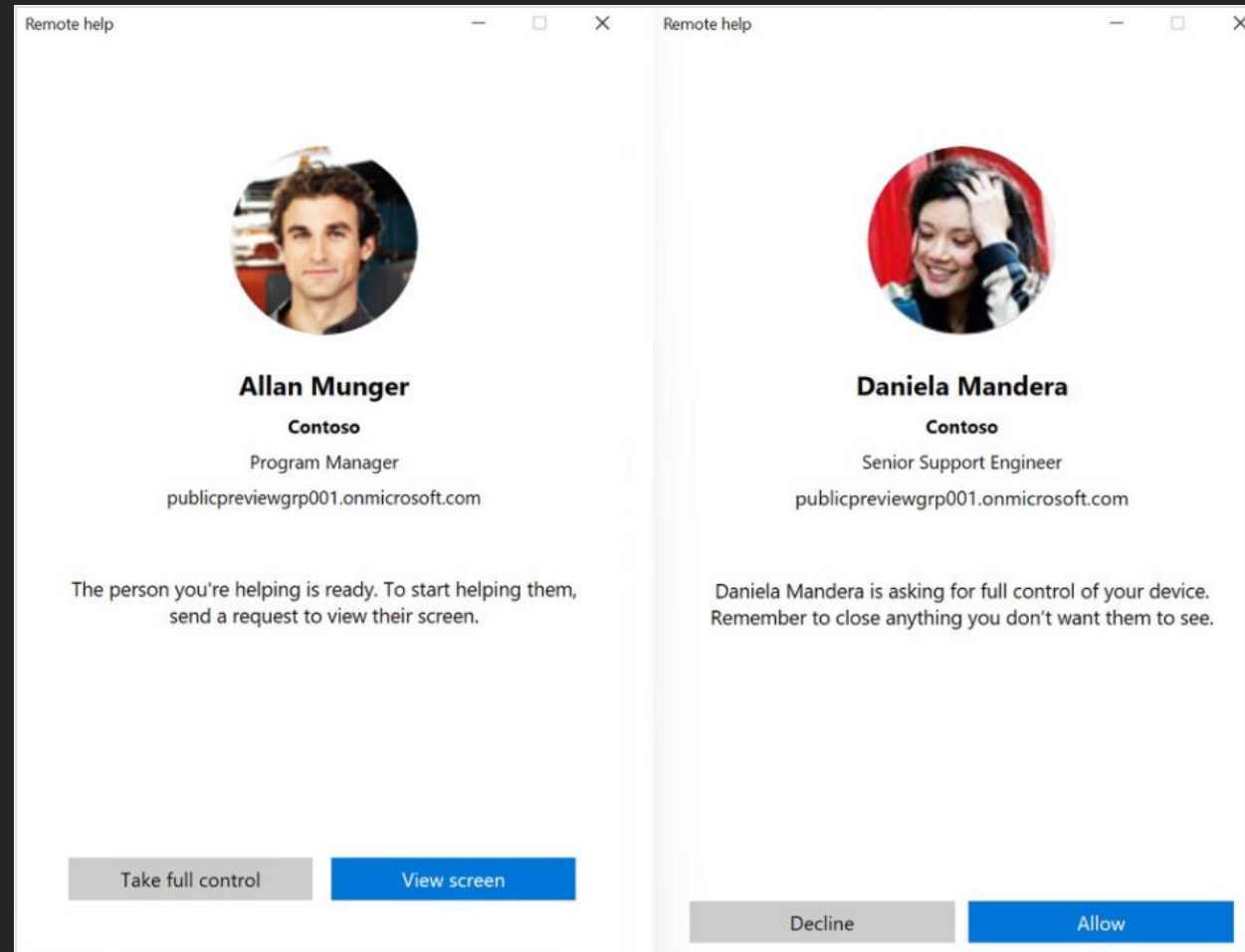
Home > Tenant admin > Endpoint Manager roles > Remote Help Operator Role >

Edit Custom Role

- Mobile apps
- Organization
- Partner Device Management
- Policy Sets
- Remote assistance connectors
- Remote help app
 - Take full control  ☐ No ☒ Yes
 - Elevation  ☒ No ☐ Yes
 - View screen  ☐ No ☒ Yes
- Remote tasks
- Roles
- Security baselines

New remote help Windows app

- New app required



Remote help

- Preview coming soon!
- GA in early 2022
- Licensing not published yet:
 - “we intend to offer remote help as an advanced endpoint management solution at a premium above the existing price of licensing options that include Microsoft Endpoint Manager or Microsoft Intune”
- What will happen with Remote Tools over CMG?
- [Remote help: a new remote assistance tool from Microsoft - Microsoft Tech Community](#)

Windows updates and driver management

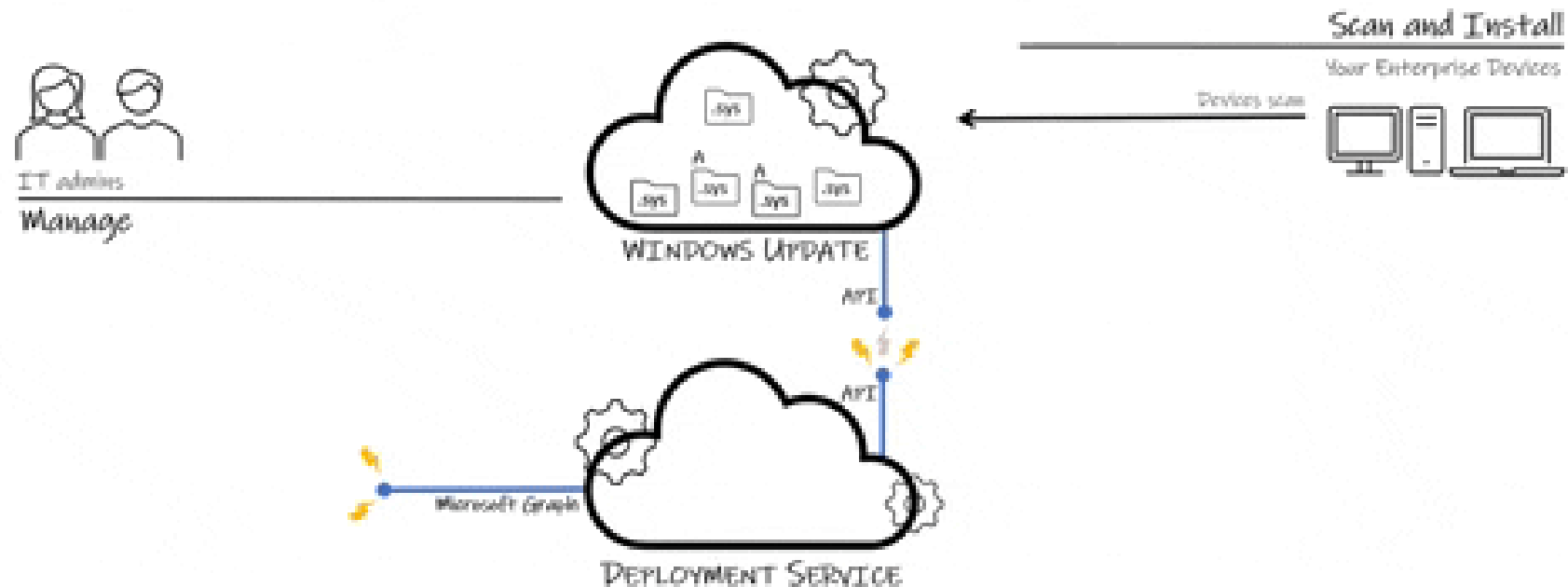
Deployment service for driver updates

<https://techcommunity.microsoft.com/t5/windows-it-pro-blog/deployment-service-for-driver-updates-public-preview-coming-soon/ba-p/2914212>

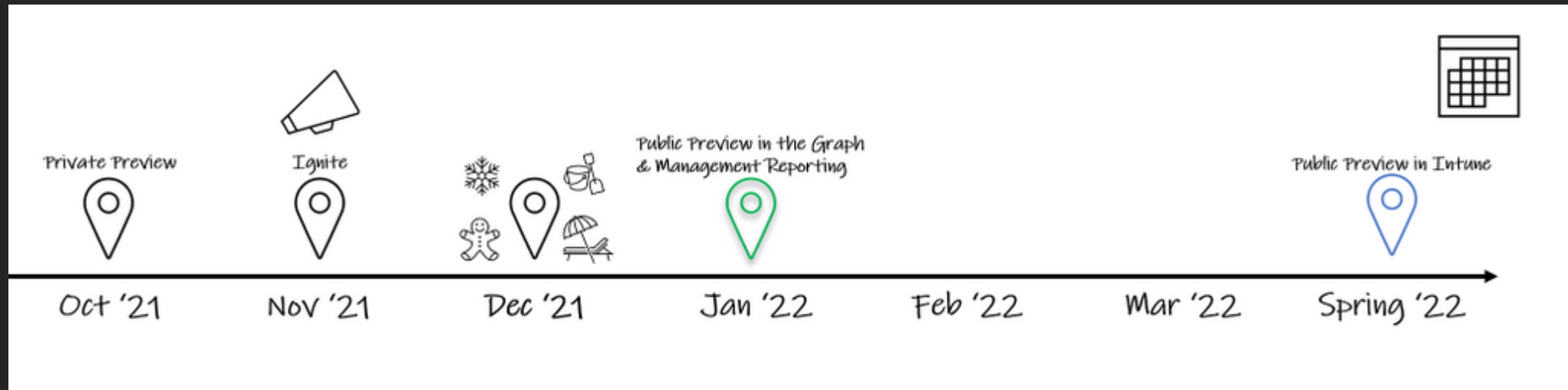
Deployment service for driver updates

- Approve driver/firmware updates

Driver & Firmware Servicing with the Graph



Deployment service for driver updates: Roadmap



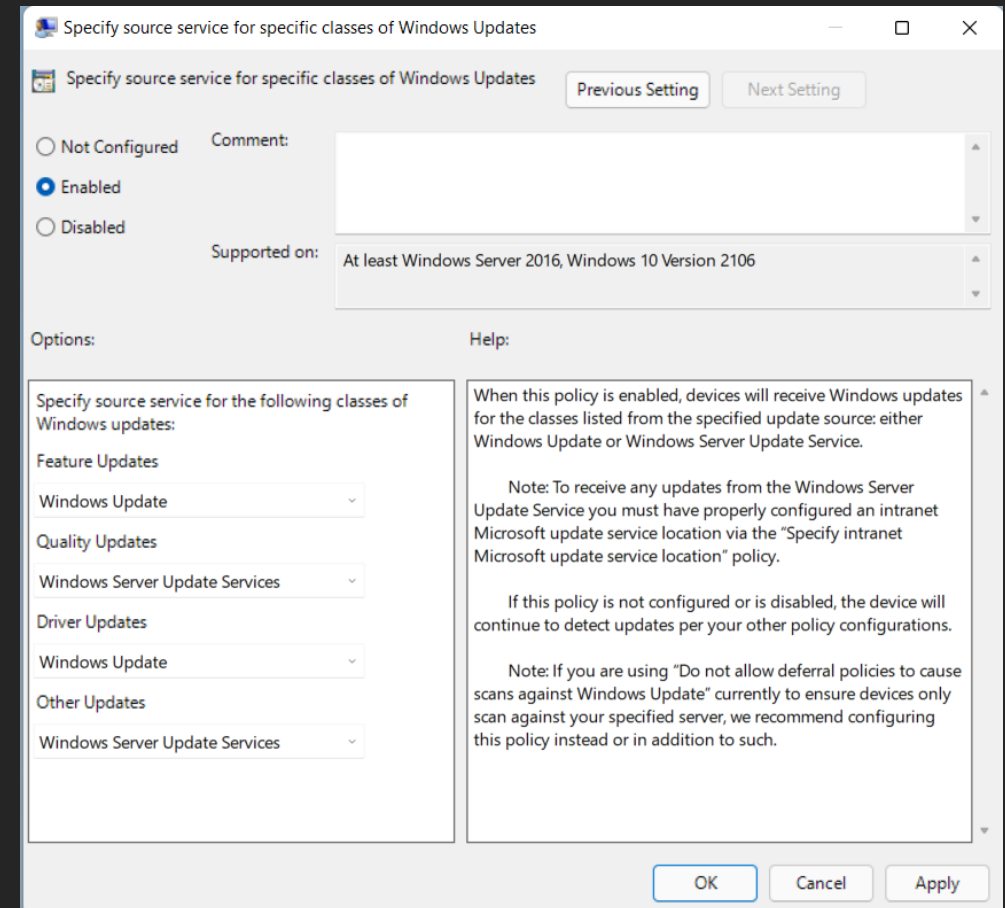
Update locations

- Get specific update contents from different locations
 - WSUS or Windows Update
- Windows 10 21H2 & Windows 11

More about updates:

See Julie's session: Wed 14.00 CET

Windows Updates, Why Modernize



The screenshot shows a Windows Group Policy dialog box titled "Specify source service for specific classes of Windows Updates". The dialog has a title bar with standard window controls. Below the title bar, there's a subtitle "Specify source service for specific classes of Windows Updates" and two buttons: "Previous Setting" and "Next Setting".

On the left, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a dropdown menu showing "At least Windows Server 2016, Windows 10 Version 2106".

Below the "Supported on:" section, there are two main sections: "Options:" and "Help:". The "Options:" section contains a list of update classes with dropdown menus for each: "Feature Updates" (set to "Windows Update"), "Quality Updates" (set to "Windows Update"), "Windows Server Update Services" (set to "Windows Server Update Services"), "Driver Updates" (set to "Windows Update"), and "Other Updates" (set to "Windows Server Update Services"). The "Help:" section contains a large text area with the following text:

When this policy is enabled, devices will receive Windows updates for the classes listed from the specified update source: either Windows Update or Windows Server Update Service.

Note: To receive any updates from the Windows Server Update Service you must have properly configured an intranet Microsoft update service location via the "Specify intranet Microsoft update service location" policy.

If this policy is not configured or is disabled, the device will continue to detect updates per your other policy configurations.

Note: If you are using "Do not allow deferral policies to cause scans against Windows Update" currently to ensure devices only scan against your specified server, we recommend configuring this policy instead or in addition to such.

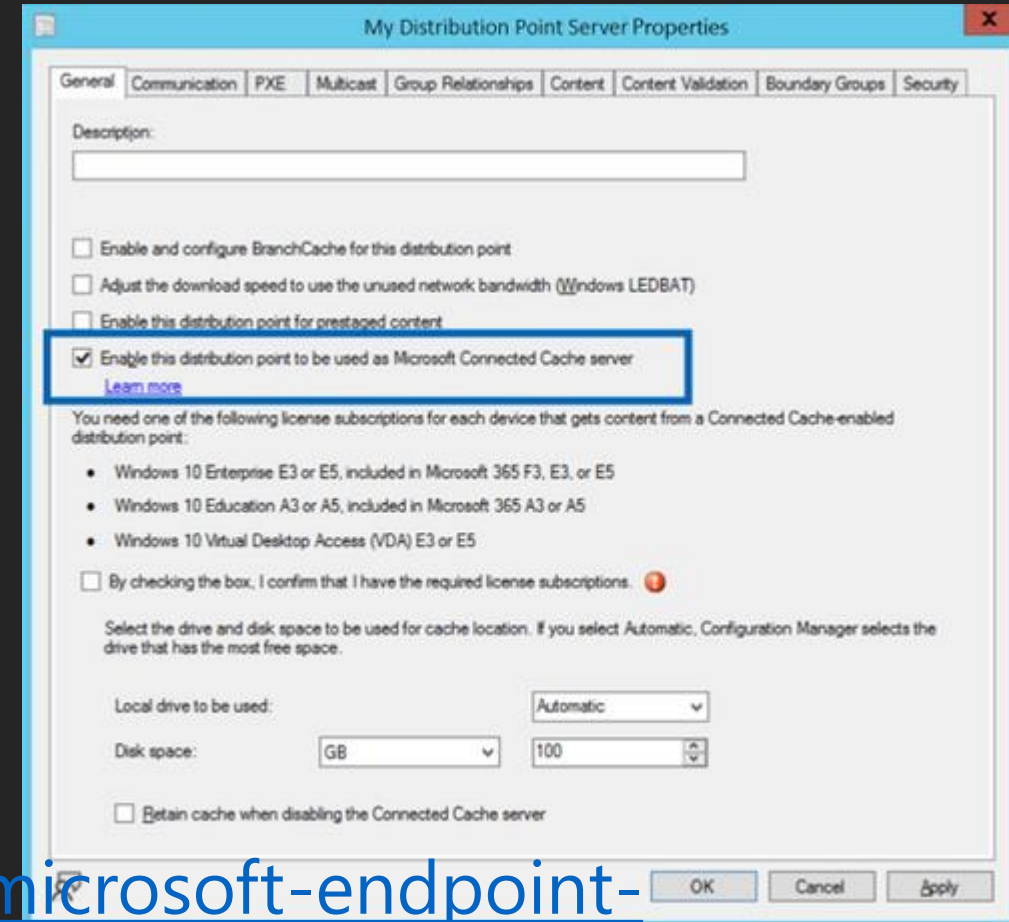
At the bottom right, there are three buttons: "OK", "Cancel", and "Apply".

Microsoft Connected Cache

<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-connected-cache-for-configuration-manager-generally/ba-p/2910802>

Microsoft Connected Cache in MEMCM

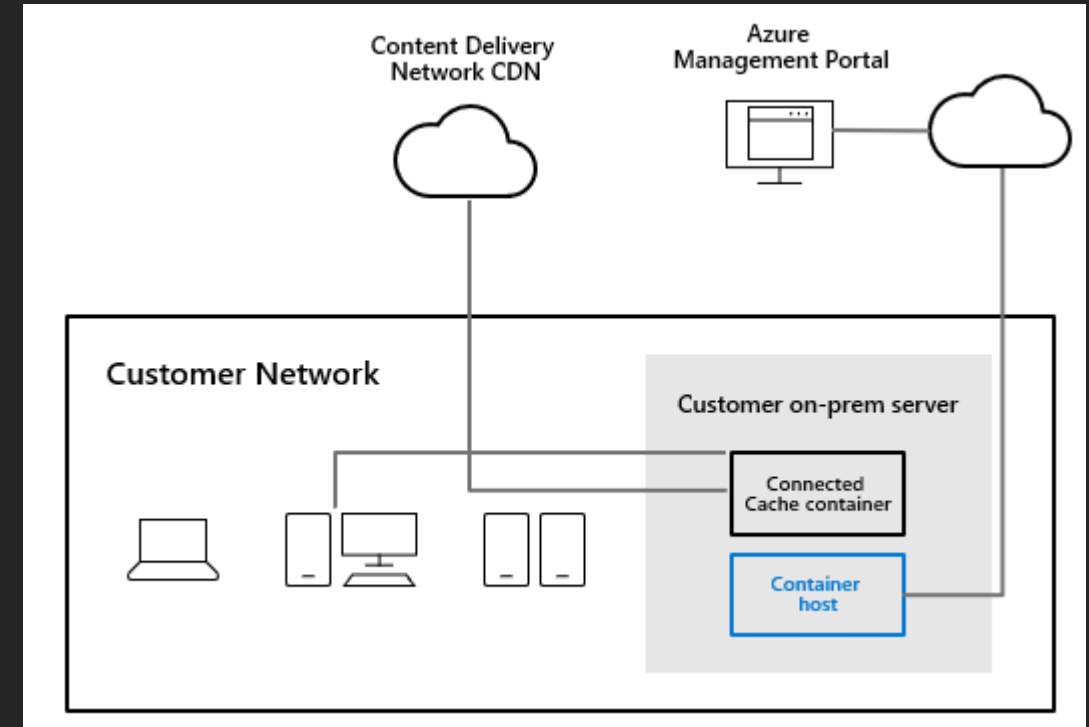
- Delivery optimization content server
 - Option on a ConfigMgr DP role
- Out of preview in ConfigMgr 2111
 - Preview started in ConfigMgr 1906
- Supports also non-ConfigMgr clients



<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-connected-cache-for-configuration-manager-generally/ba-p/2910802>

Microsoft Connected Cache managed in Azure

- Stand-alone local DO server
 - Windows/Linux
- Management from Azure
- Early preview published at Ignite 2019!



<https://techcommunity.microsoft.com/t5/windows-it-pro-blog/introducing-microsoft-connected-cache-microsoft-s-cloud-managed/ba-p/963898>

Windows 11 compatibility data

Desktop Analytics

Desktop Analytics doesn't support Windows 11. For information about Windows 11 hardware readiness, Microsoft recommends that you enable tenant attach and [Endpoint analytics](#).

📘 Important

The recent shift to hybrid and remote work is changing the way organizations manage enterprise devices. Many organizations are moving to modern cloud management solutions. Microsoft is making new features available in Microsoft Endpoint Manager to better facilitate and support this change as you begin your transition to Windows 11 devices.

To align investments with this shift, **Desktop Analytics will be retired on November 30, 2022.** Over the next year, the types of insights currently found in Desktop Analytics will be incorporated directly into the Microsoft Endpoint Manager admin center.

For more information, see [A data-driven approach to managing devices in your organization](#) [↗].

[What's new in Desktop Analytics - Configuration Manager | Microsoft Docs](#)

Windows 11 Compat: Endpoint Analytics

Home > Reports > Endpoint analytics

Endpoint analytics | Work from anywhere (preview) ...

Search (Ctrl+/)

Overview

Settings

Reports

- Startup performance
- Proactive remediations
- Recommended software
- Application reliability
- Work from anywhere (preview)

Overview

Windows

Cloud identity

Cloud management

Cloud provisioning

This report will replace Recommended software soon. We've improved insights and scores to help you better understand your organization's readiness for Windows 11.

The ability for your employees to work from anywhere and be productive is essential in today's world. This report offers insights on how prepared your workforce is to be productive from anywhere. Review your organization's score and compares to the selected baseline. Refer to the insights and recommendations to learn how to improve your organization's readiness for Windows 11. [Learn more about the Work from anywhere report.](#)

Baseline ⓘ All organizations (median)

Filter All Devices

Work from anywhere score ⓘ

Work from anywhere score

73

Baseline ⓘ

51

Score categories

Capability	Score
Windows ⓘ	<div></div>
Cloud identity ⓘ	<div></div>
Cloud management ⓘ	<div></div>

Windows

Capabilities that enable users to work from anywhere

Review insights and metrics related to how many devices in your organization are running older versions of Windows. [Learn more about the Windows score category.](#)

Insights and recommendations ⓘ

We don't have anything to share with you right now.

Windows version	Number of devices
Older versions	<div></div> 0

72% of your Windows devices meet the hardware requirements for Windows 11. Windows 11 provides a refreshed UI and a new set of features. [Learn more.](#)

Device status	Number of devices
Meets hardware requirements	<div></div> 5069

Windows 11 hardware readiness insights do not impact your Work from anywhere score.

Top hardware blockers	Percent of non-upgraded devices that do not ...
CPU family	<div></div> 27.88
TPM	<div></div> 6.02
System firmware	<div></div> 1.66
RAM	<div></div> 0.01

Windows 11 Compat: Update compliance

WaaSUUpdateInsights (3)

Windows 11 Readiness Sta...

Safeguard Holds

WaaSUUpdateInsights

Diagnose and solve problems

Summary

Settings

Locks

Update Compliance Settings

General

Workbooks

Log Analytics Workspace

Properties

Workspace Data Sources

Virtual machines

Azure Activity log

Automation

Workbooks | Windows 11 Readiness ...

Edit Save Refresh Alerts Share Feedback ? Help Auto refresh: Off

Compliance - Windows 11 Readiness Status

This workbook utilizes data from **Update Compliance** to provide a report on which devices in your environment meet the **hardware requirements** for Windows 11.

Capability Status ⓘ

All ▼

Windows 11 Readiness Status



Status	Count
NotCapable	9
NotStarted	4
Capable	2

Upcoming improvements



New Reports in Microsoft Endpoint Manager admin center

In the coming months, we'll be releasing device-level upgrade and update readiness insights directly in the Reports node of the Microsoft Endpoint Manager admin center, giving you insights for all your Endpoint Manager-managed devices. These reports will tell you if any of your Windows devices have application or driver compatibility risks or Safeguard holds that will prevent an upgrade from Windows 10 to Windows 11 – or a feature update from one version of Windows to another. We will also show you the top compatibility risks across your organization making it easy to see which impact the largest number of devices so that you can prioritize fixes effectively.

[A data-driven approach to managing devices in your organization - Microsoft Tech Community](#)

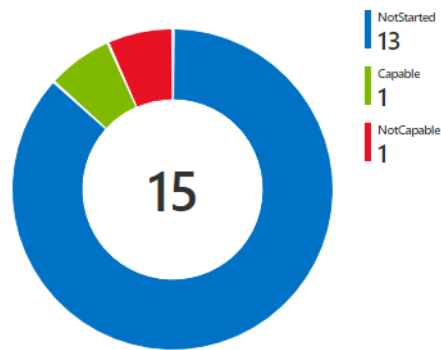
Make your own report?

Windows 11 Readiness Status

This report provide on which devices in your environment meet the [hardware requiriement](#) for Windows 11

TimeRange: Last 3 days
Current Build: All
Target Build: 10.0.22000.194

Windows 11 readiness Status



Windows 11 Readines Scan Status by Manufacturer

Manufacturer	↑↓	Capable ↑↓	NotCapable ↑↓	NotStarted ↑↓
Microsoft Corporation		1	0	2
Dell Inc.		0	0	1
HP		0	0	4
System manufacturer		0	0	1
LENOVO		0	1	1
Gigabyte Technology Co., Ltd.		0	0	1
Alienware		0	0	1
ASUS		0	0	1
Intel(R) Client Systems		0	0	1

Windows 11 NotCapable Reasons by Manufacturer

ReadinessReason ↑↓ LENOVO...↑↓

CpuFms 1

Speakers (Lenovo Audio): 57%

Schedule Windows 11 Updates

Create feature update deployment ...

Feature update deployments

1 Deployment settings 2 Scope tags 3 Assignments 4 Review + create

i Enable Windows health monitoring and select Windows Update scope to get detailed device states and errors. [Learn more](#)

Name *

Description

Feature deployment settings

Feature update to deploy ⓘ

Windows 11



i By selecting this Feature update to deploy you are agreeing that when applying this operating system to a device either (1) the applicable Windows license was purchased through volume licensing, or (2) that you are authorized to bind your organization and are accepting on its behalf the relevant Microsoft Software License Terms to be found here <https://go.microsoft.com/fwlink/?linkid=2171206>.

Rollout options *

- ☒ Make update available as soon as possible
- ☐ Make update available on a specific date
- ☐ Make update available gradually

Previous

Next

Windows 365

Windows 365 – What is it

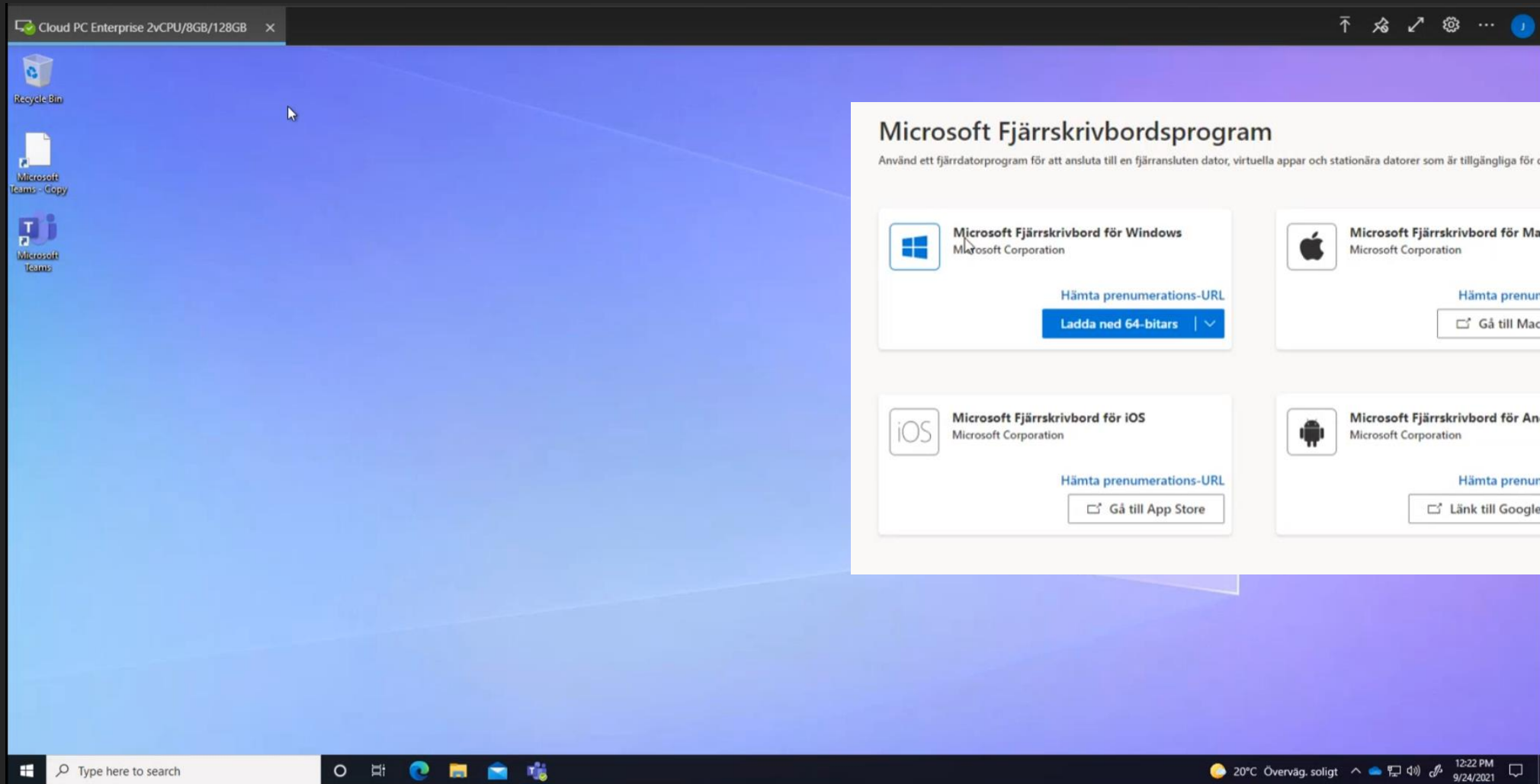
- PC in the Cloud
- Accessible from any device
- License based = Fixed Price
- License = Size and type of VM
- Hosted in Microsoft Subscription
- Connectivity is hosted by Microsoft

See Petter's session: Wed 10.00 CET
Windows 365: Why? When? When not?

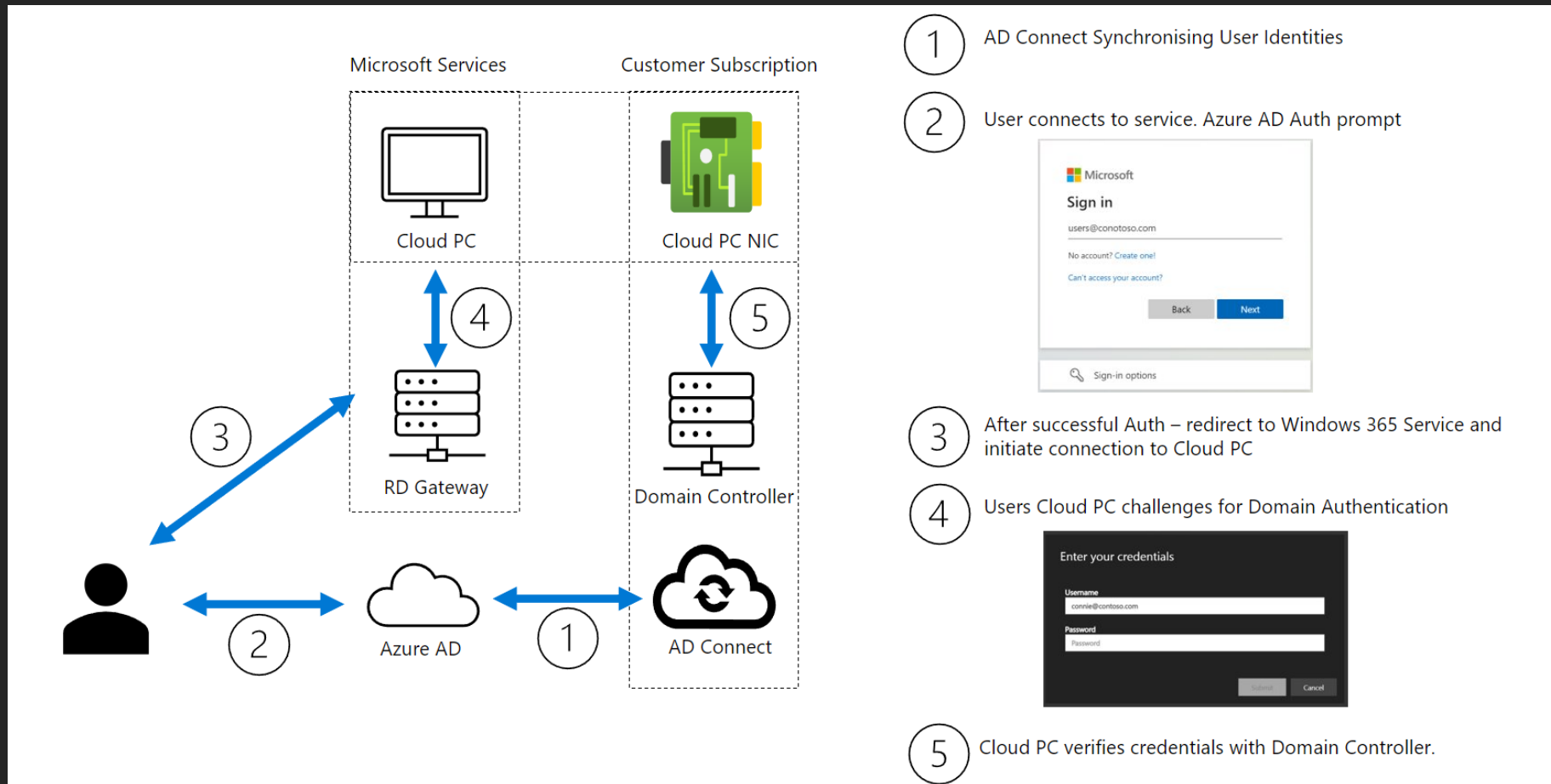


Business Enterprise		
Basic	Standard	Premium
Run light productivity tools and web browsers.	Run a full range of productivity tools and line-of-business apps.	Run high-performance workloads and heavier data processing.
\$31.00 user/month Subscription automatically renews ¹	\$41.00 user/month Subscription automatically renews ¹	\$66.00 user/month Subscription automatically renews ¹
2 vCPU 4 GB RAM 128 GB Storage	2 vCPU 8 GB RAM 128 GB Storage	4 vCPU 16 GB RAM 128 GB Storage
<ul style="list-style-type: none">✓ Integrated with Microsoft Endpoint Manager for advanced threat protection, and PC and mobile device management✓ Supports the desktop versions of Office apps, Outlook, and OneDrive✓ Supports the desktop version of Microsoft Teams (chat and audio calls only)✓ Unlimited users	<ul style="list-style-type: none">✓ Integrated with Microsoft Endpoint Manager for advanced threat protection, and PC and mobile device management✓ Supports the desktop versions of Office apps, Outlook, and OneDrive✓ Supports the desktop version of Microsoft Teams✓ Unlimited users	<ul style="list-style-type: none">✓ Integrated with Microsoft Endpoint Manager for advanced threat protection, and PC and mobile device management✓ Supports the desktop versions of Office apps, Outlook, and OneDrive✓ Supports the desktop version of Microsoft Teams✓ Supports Microsoft Visual Studio, Power BI, and Dynamics 365✓ Unlimited users

Windows 365 - Overview



Windows 365 - Authentication

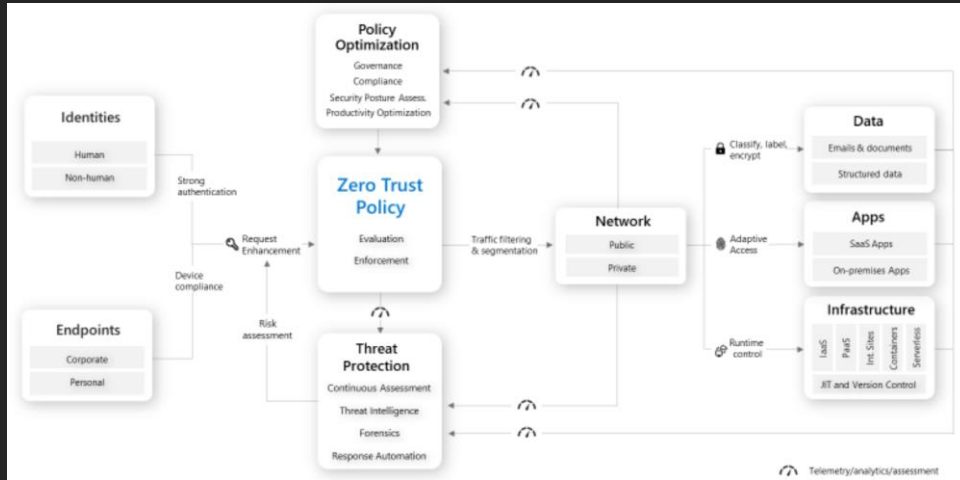


Windows 365 – Ignite



- Performance Improvements
- Native Azure AD Join Support
 - No Domain Controller Required
 - No VNET or Azure Subscription Required
 - SSO Support
 - Windows Hello

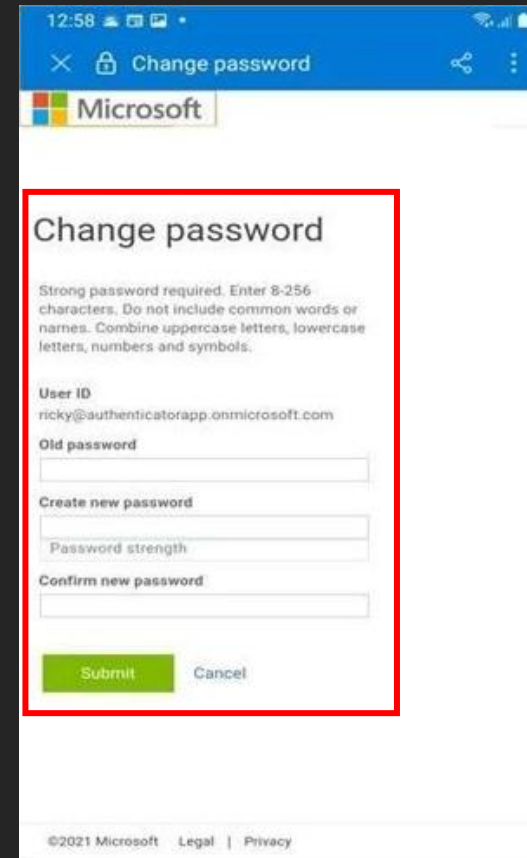
<https://techcommunity.microsoft.com/t5/windows-it-pro-blog/what-s-happening-windows-365-at-microsoft-ignite/ba-p/2912555>



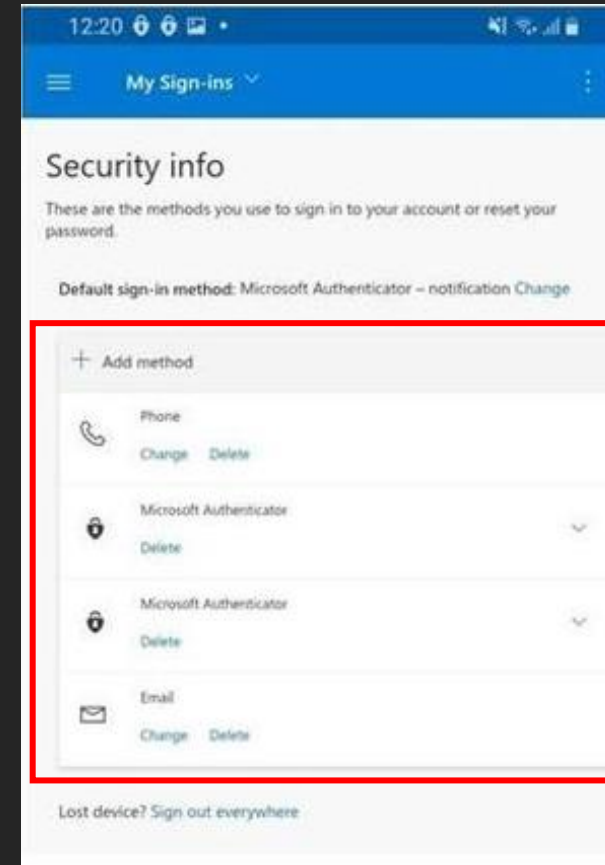
Zero Trust Updates

aka.ms/ztamodel

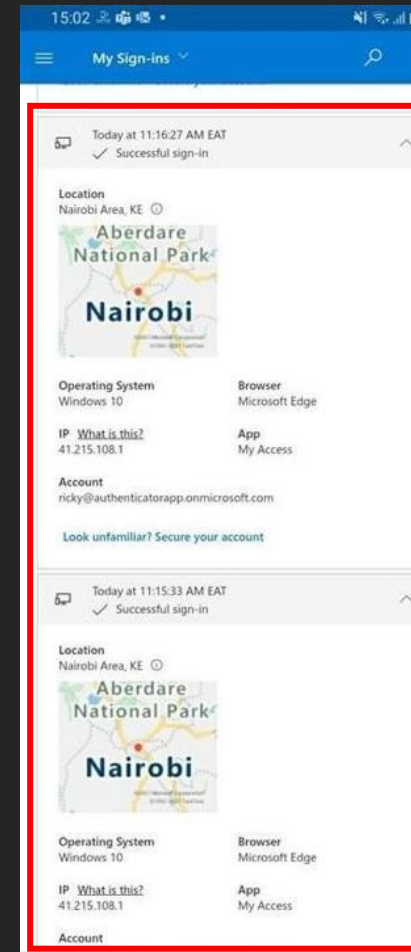
Authenticator App – PW Change



Authenticator App – Security Info



Authenticator App – Review Signins



Conditional Access – Custom Compliance

Home > Devices > Compliance policies >

Create custom script ...

1 Basics 2 Settings 3 Review + create

Detection script *

```
1 $exclusions = Get-MpPreference | Select-Object -Property  
2  
3 $ExclusionsSet = 0  
4 $ControlledFolderAccessEnabled = $false  
5  
6 if ($exclusions -ne $null -and $exclusions.ExclusionPath  
7 {  
8     $ExclusionsSet = $exclusions.ExclusionPath.Count  
9 }  
10
```

Run this script using the logged on credentials ☒ Yes ☐ No

Enforce script signature check ☒ Yes ☐ No

Run script in 64 bit PowerShell Host ☒ Yes ☐ No

<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-endpoint-manager-adds-management-and-compliance-checks/ba-p/2902346#WindowsCustomCompliance>

Conditional Access – Device Filters

- Condition based on Devices
- Example PAW Scenario

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	
	displayName	Equals	PAW-0001	

+ Add expression

Rule syntax ⓘ

Edit

device.displayName -eq "PAW-0001"

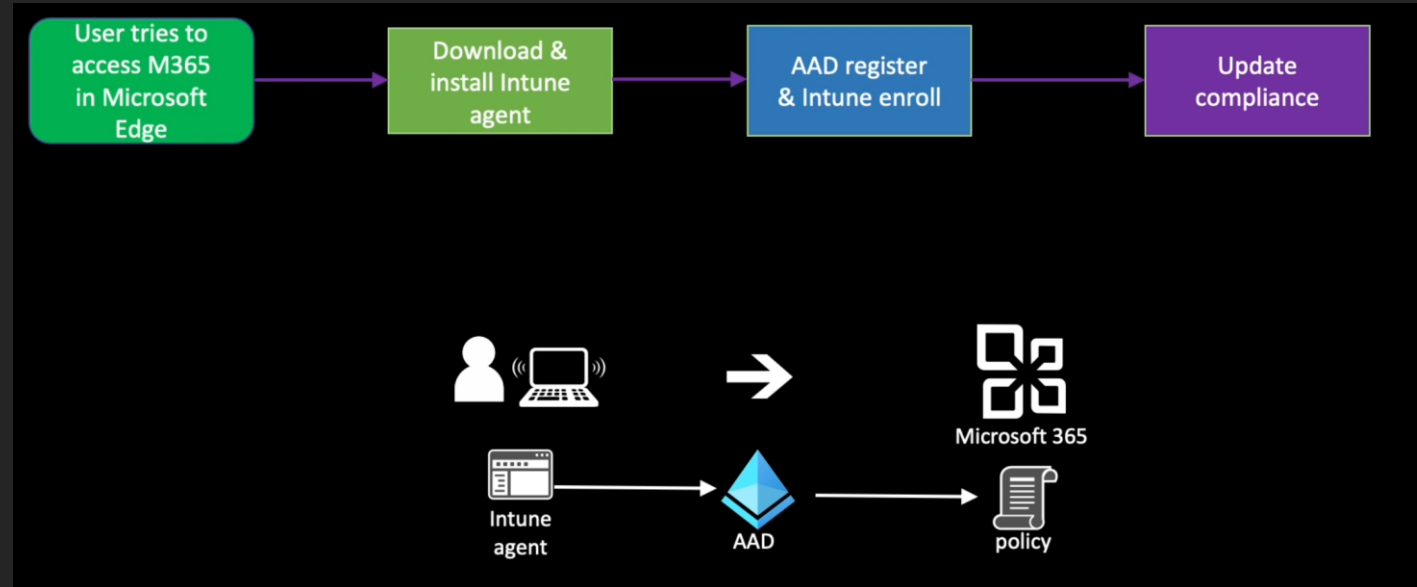
MEM – Linux

- *Preview Early 2022*
- Enroll Linux Desktops with MEM and AAD
- Target Compliance Policies
 - Require Distro type and version
 - Password Complexity
 - Encryption
- Reporting in MEM
- Ensure AV is Enabled
- Deploy Custom Scripts
- Apply Wi-Fi Profiles and Certificates

<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-endpoint-manager-adds-management-and-compliance-checks/ba-p/2902346>

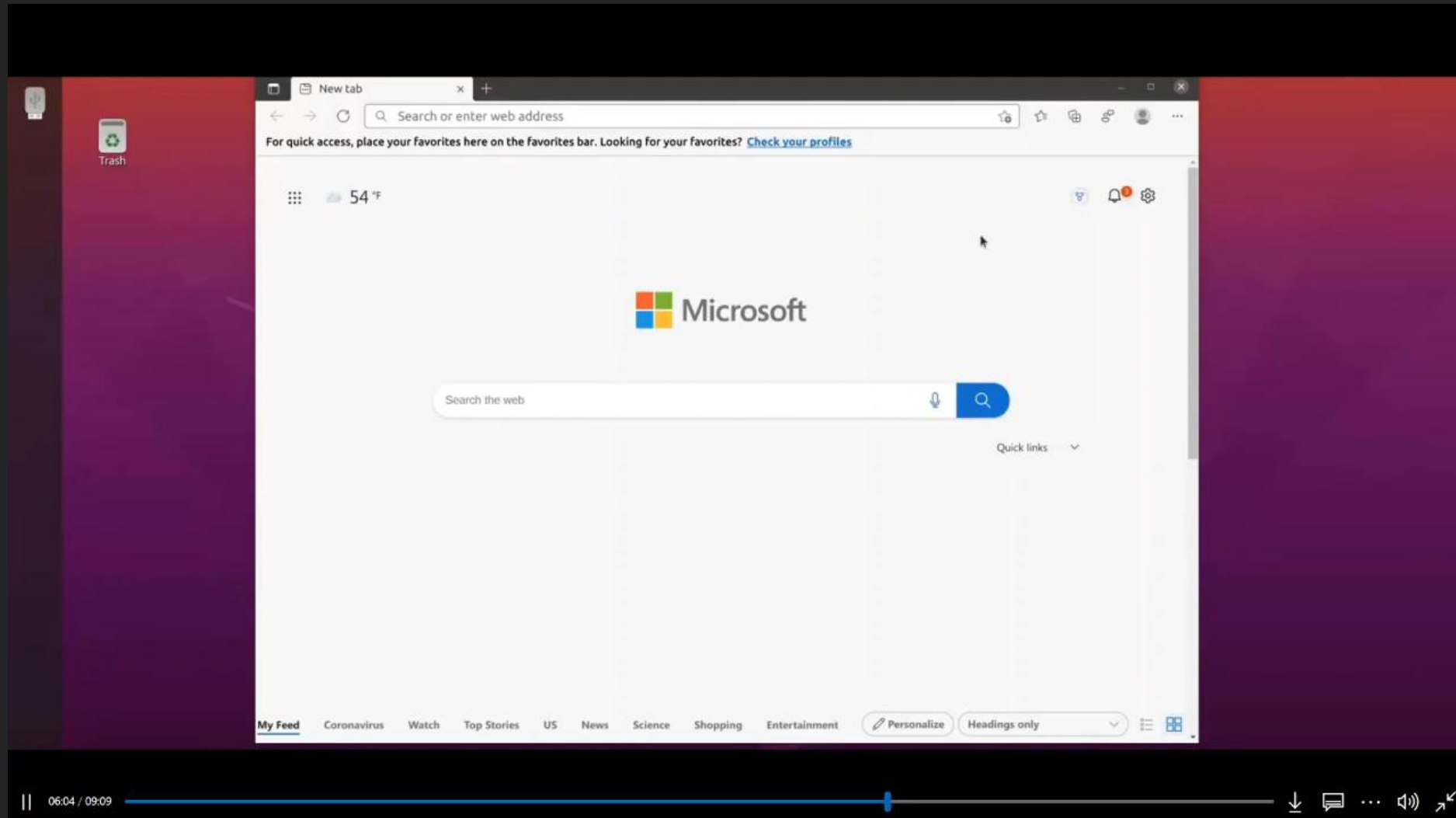
Conditional Access – Linux

- Use Conditional Access to Grant web app usage based on device compliance



<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-endpoint-manager-adds-management-and-compliance-checks/ba-p/2902346>

Linux Demo



Microsoft Defender for Endpoint

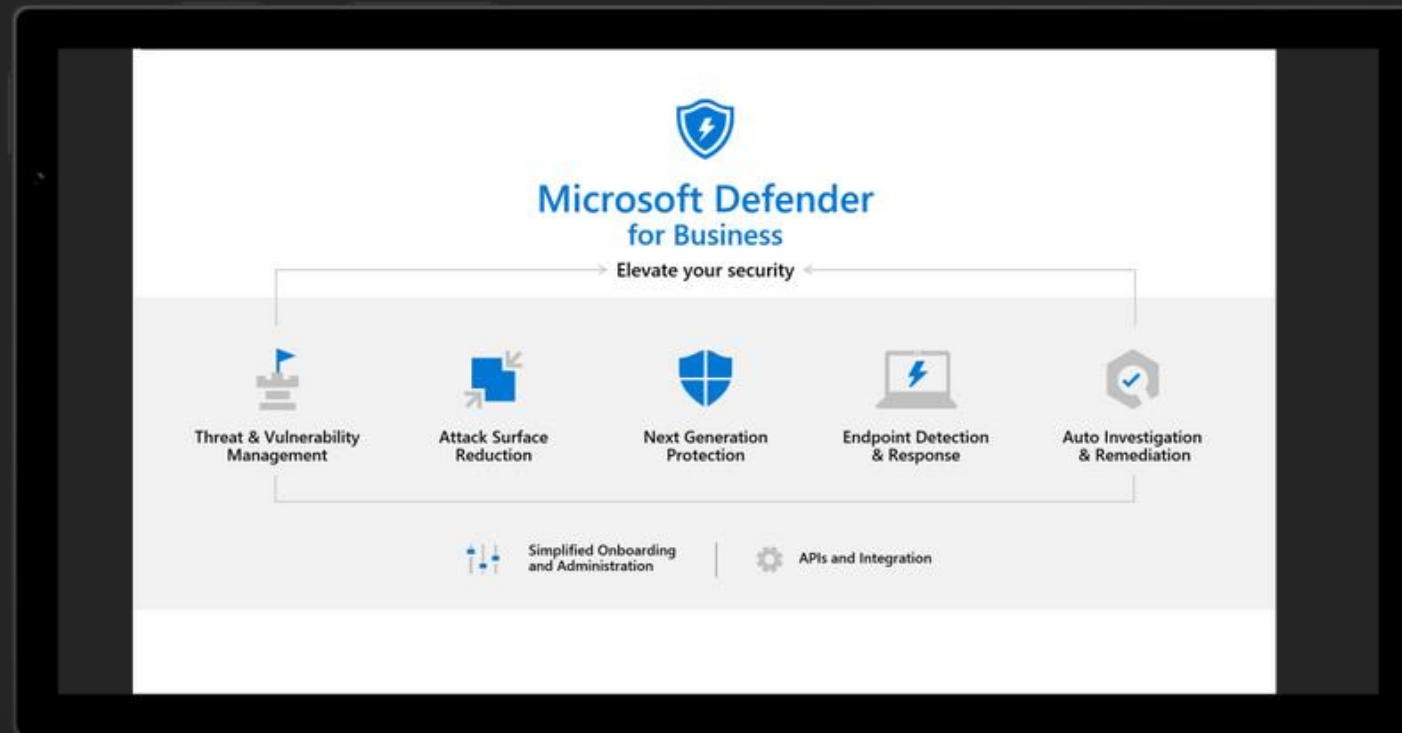
What's new in MDE



- Microsoft Defender for Business
- Microsoft Defender P1
- Unified Down-level Agent in Preview for WS 2012 R2 and 2016
- Preview of new Policy Management Channel
- Linux Agent Enhancements
 - Linux Live Response (Private Preview)
 - TVM Preview for Debian
 - New Distribution Support (Amazon Linux 2 and Fedora 33+ and Preview of RHEL6.7+ CentOS 6.7+)
 - Behavior Monitoring is GA (Memory Scanning, Ransomware)
<https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/endpoint-security-for-unenrolled-defender-for-endpoint-devices/ba-p/2822656>

Microsoft Defender for Business

- Small Business Offer up to 300 Seats
 - As a standalone offering, priced at \$3 per user per month.
 - Included as part of Microsoft 365 Business Premium

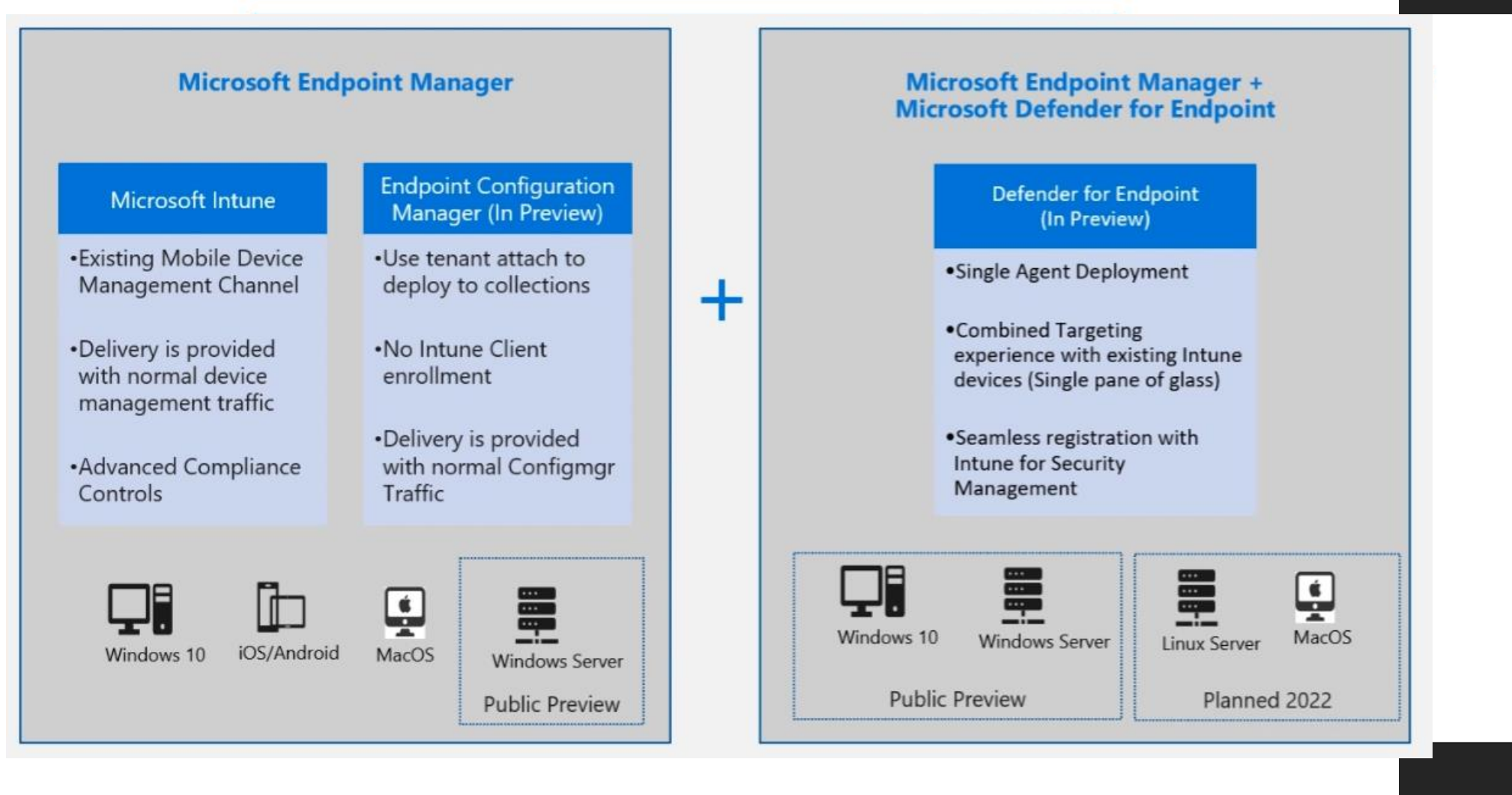


Microsoft Defender for Endpoint P1

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts **		✓

If you have Microsoft 365 E3 or A3 but not Microsoft 365 E5 or A5 <https://aka.ms/mdep1trial>

MDE Policy Management



Other new announcements

- <https://techcommunity.microsoft.com/t5/microsoft-365-blog/announcing-ga-of-servicing-profiles-for-microsoft-365-apps/ba-p/2910765>
- <https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/microsoft-adds-android-open-source-project-device-management/ba-p/2792318>
- <https://techcommunity.microsoft.com/t5/video-hub/managing-macos-devices-with-microsoft-endpoint-manager/ba-p/2911282>

MEM related sessions at Ignite



- [Managing Windows updates in the cloud \(The Blueprint Files\)](#)
- [Manage Windows updates in the Cloud](#)
- [Endpoint Management for hybrid work](#)
- [Interpreting Data in Microsoft Endpoint Manager](#)
- [Endpoint security management with Microsoft Endpoint Manager](#)
- [Cloud native Windows Endpoints \(microsoft.com\)](#)

What's missing?

- No new announcements/sessions about upcoming Microsoft Store and MEM integration
 - One Q & A session about apps management, no recording available
 - [Delivering apps in the enterprise](#)

Summary

- Zero trust enhancements
- Data driven insights (Endpoint analytics)
- Tools for Windows 11 enterprise deployment
- Windows 365/Azure Virtual Desktop
- Support for non-Windows platforms