

Webinar: Azure Readiness – EMS - Sicherheit, 19.2.2020.



Vorstellung



Michael Stachowski

Business Development Manager Microsoft Security

Microsoft Partner Technical Solutions Professional (P-TSP)

Community Lead Microsoft Surface Community Deutschland

Seit Juni 2018 bei Bechtle am Standort Köln

- Microsoft Competence Center
- Schwerpunkt Modern Workplace Solutions mit Microsoft 365
- Microsoft AutoPilot

Seit Oktober 2019 bei Bechtle Logistik & Service

- Microsoft Software Solutions Team
- Schwerpunkt Microsoft Security

Agenda

1. Trends – wieso muss ich meine mobilen Geräte überhaupt absichern?
2. Microsoft Intune: alle Services im Überblick
3. Mobile Security
4. Datensicherheit (Mobile Device)
5. Lizenzierung
6. Roadmap
7. Beantwortung von Fragen

- Trends – Wieso muss ich meine (mobilen) Geräte überhaupt absichern?
- Microsoft Endpoint Manager – alle Services im Überblick
- Mobile Security (MAM)
- Lizenzierung
- Roadmap
- Q&A



Agenda

Wieso muss ich meine (mobilen) Geräte überhaupt absichern?



Geschäftsverlust

\$2,9 Millionen

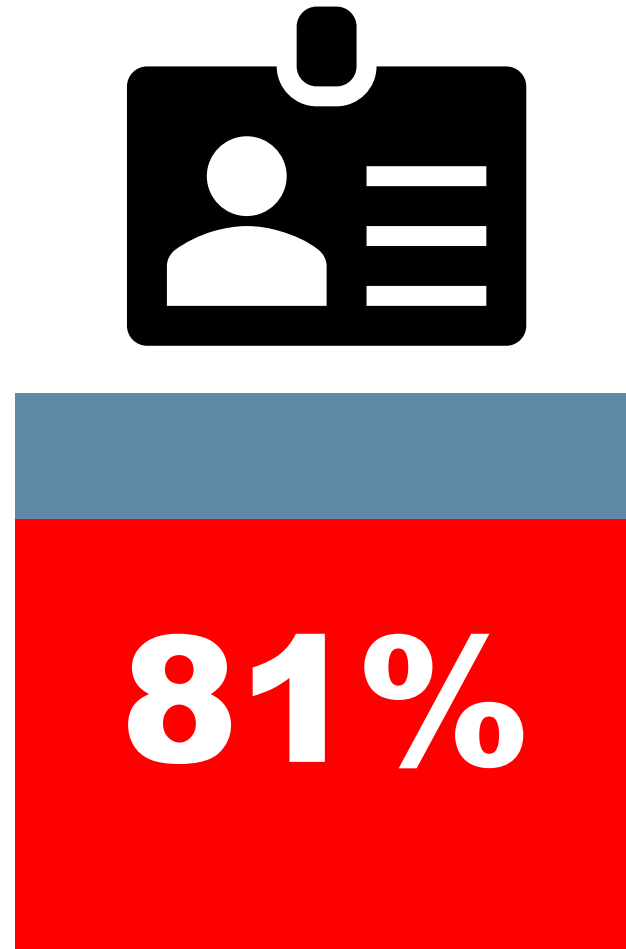
pro Minute durch Cyberkriminalität in 2019

Geschäftsverlust

\$1.500.000.000.000

pro Jahr durch Cyberkriminalität in 2019

Was ist der Haupteinfallswinkel bei heutigen Attacken?



Hacker ♥ Passwörter

Beliebte Passwörter in 2018

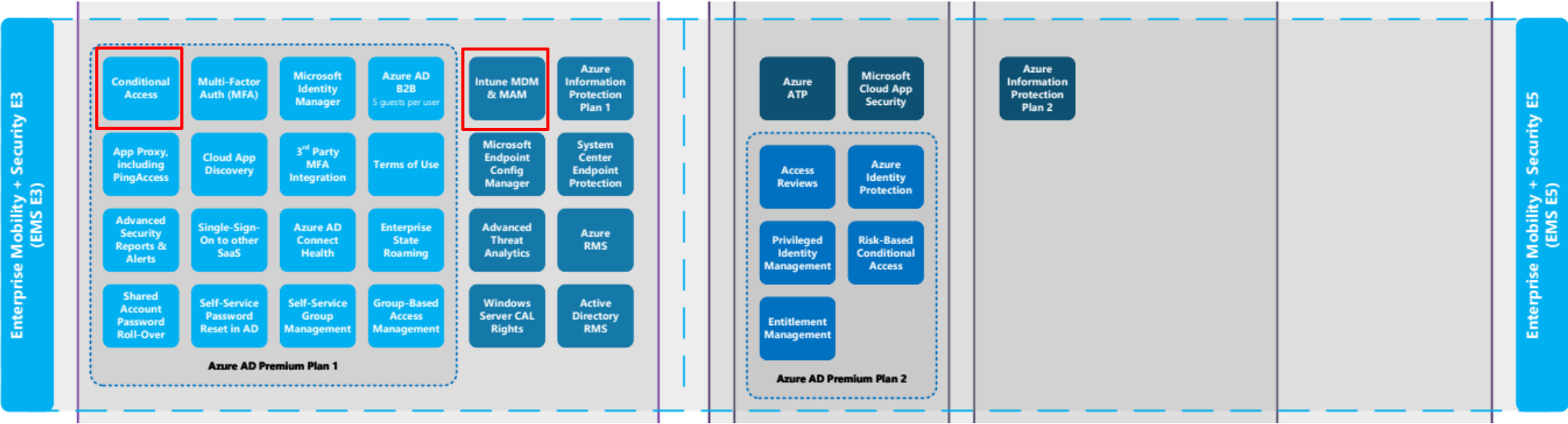
1	123456	6	hallo123
2	12345	7	hallo
3	123456789	8	123
4	ficken	9	passwort
5	12345678	10	master

Beliebte Passwörter in 2019

1	123456	6	111111
2	123456789	7	1234567890
3	12345678	8	123123
4	1234567	9	000000
5	password	10	abc123

Quelle: <https://hpi.de/pressemitteilungen/2019/die-beliebtesten-deutschen-passwoerter-2019.html>

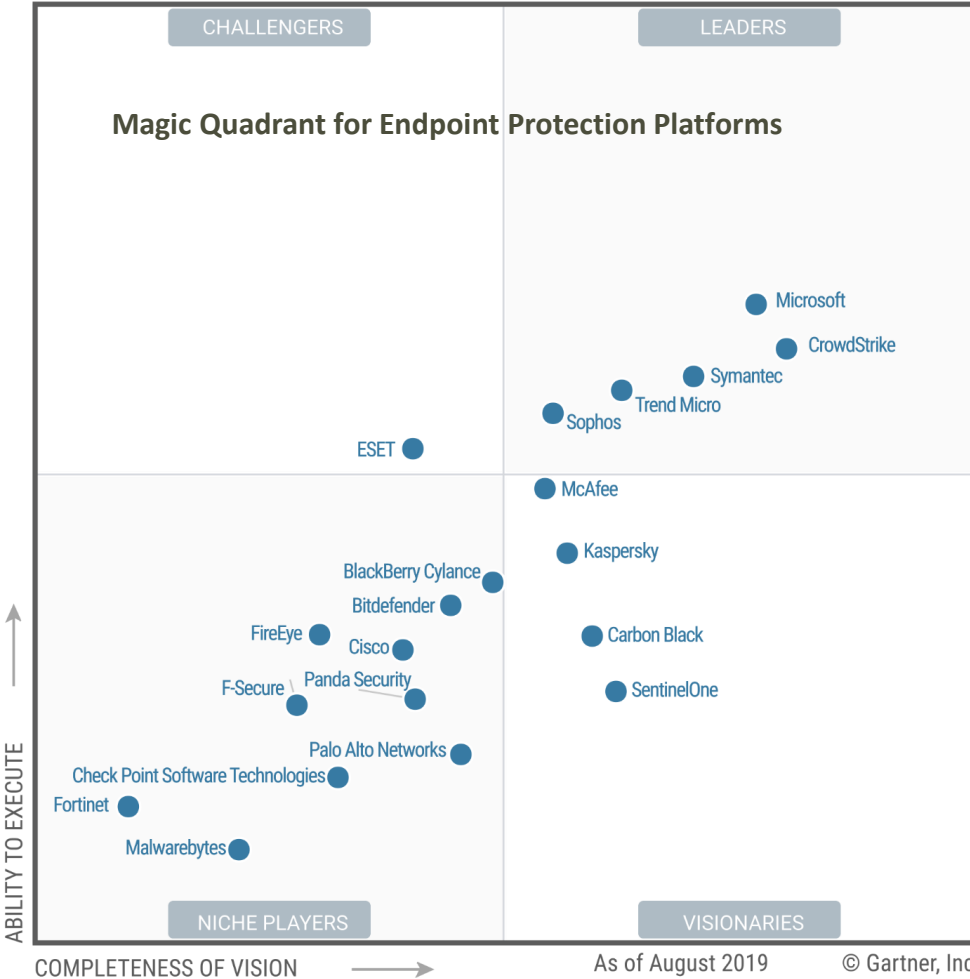
Überblick Enterprise & Mobility Suite



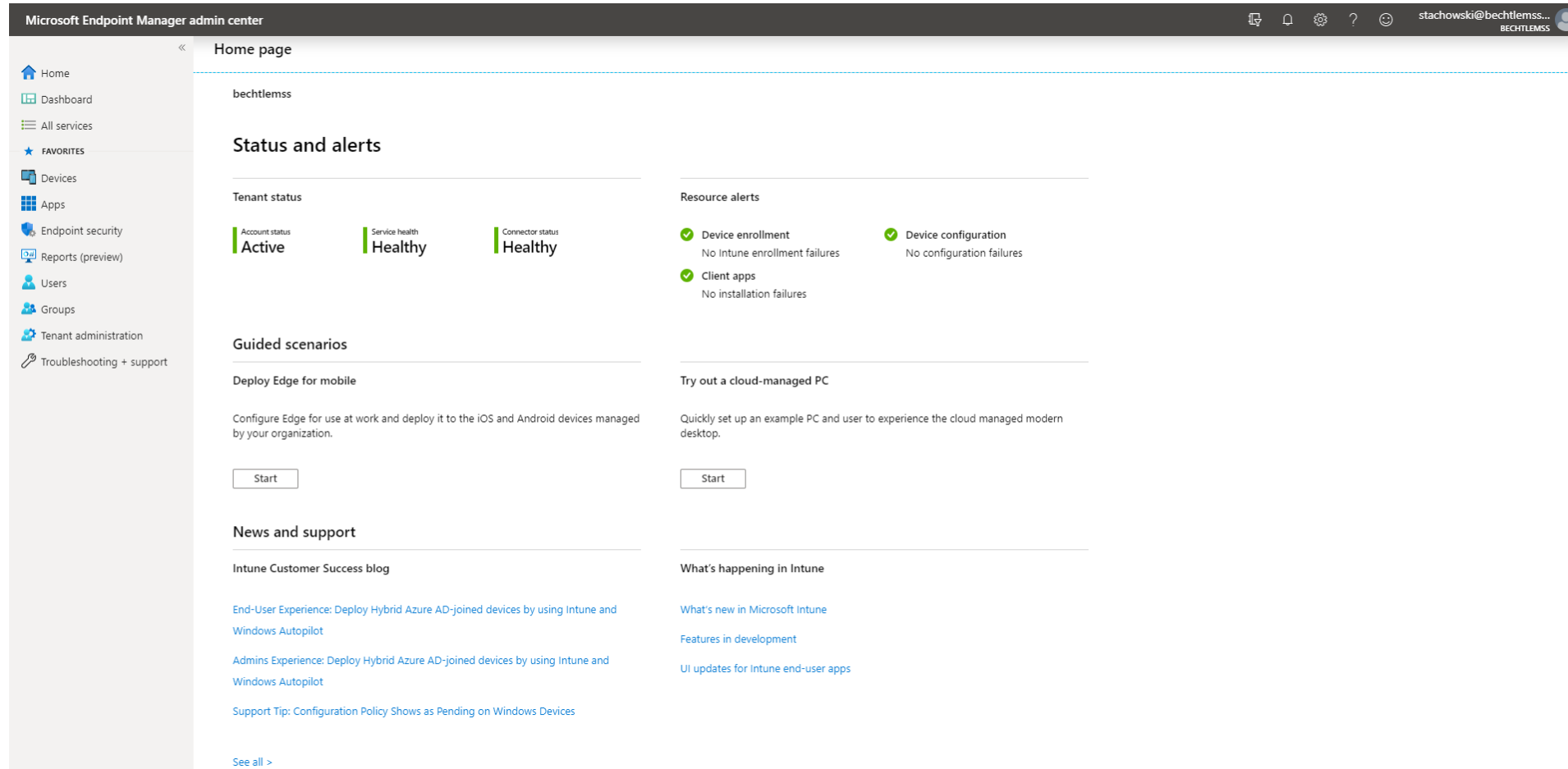
Microsoft Endpoint Manager - alle Services im Überblick



Gartner Magic Quadrant



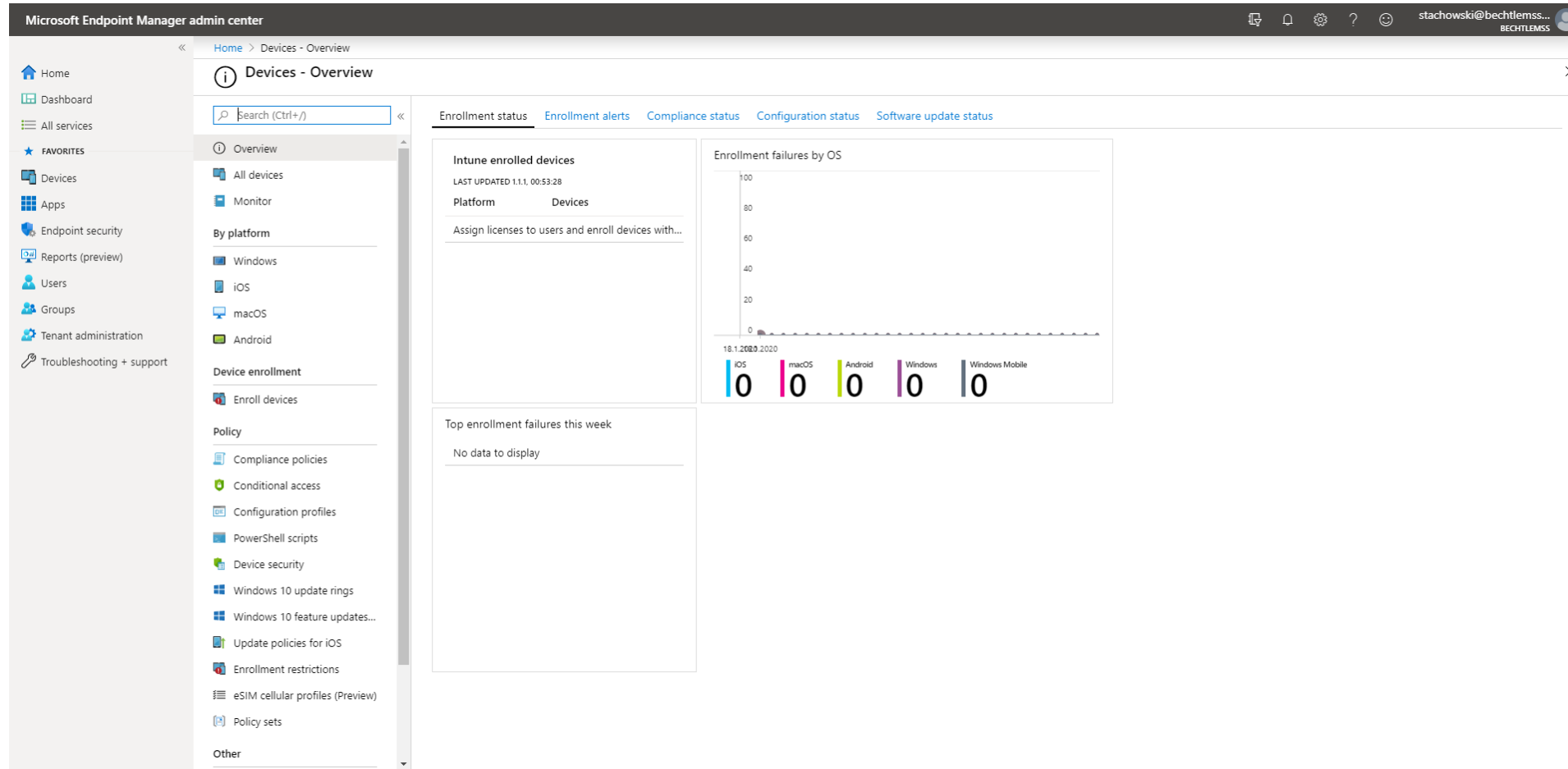
Microsoft Endpoint Manager – Dashboard



The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar includes the title 'Microsoft Endpoint Manager admin center', user information 'stachowski@bechtlemss... BECHTLEMSS', and icons for help, settings, and notifications. The left sidebar lists navigation options: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports (preview), Users, Groups, Tenant administration, and Troubleshooting + support.

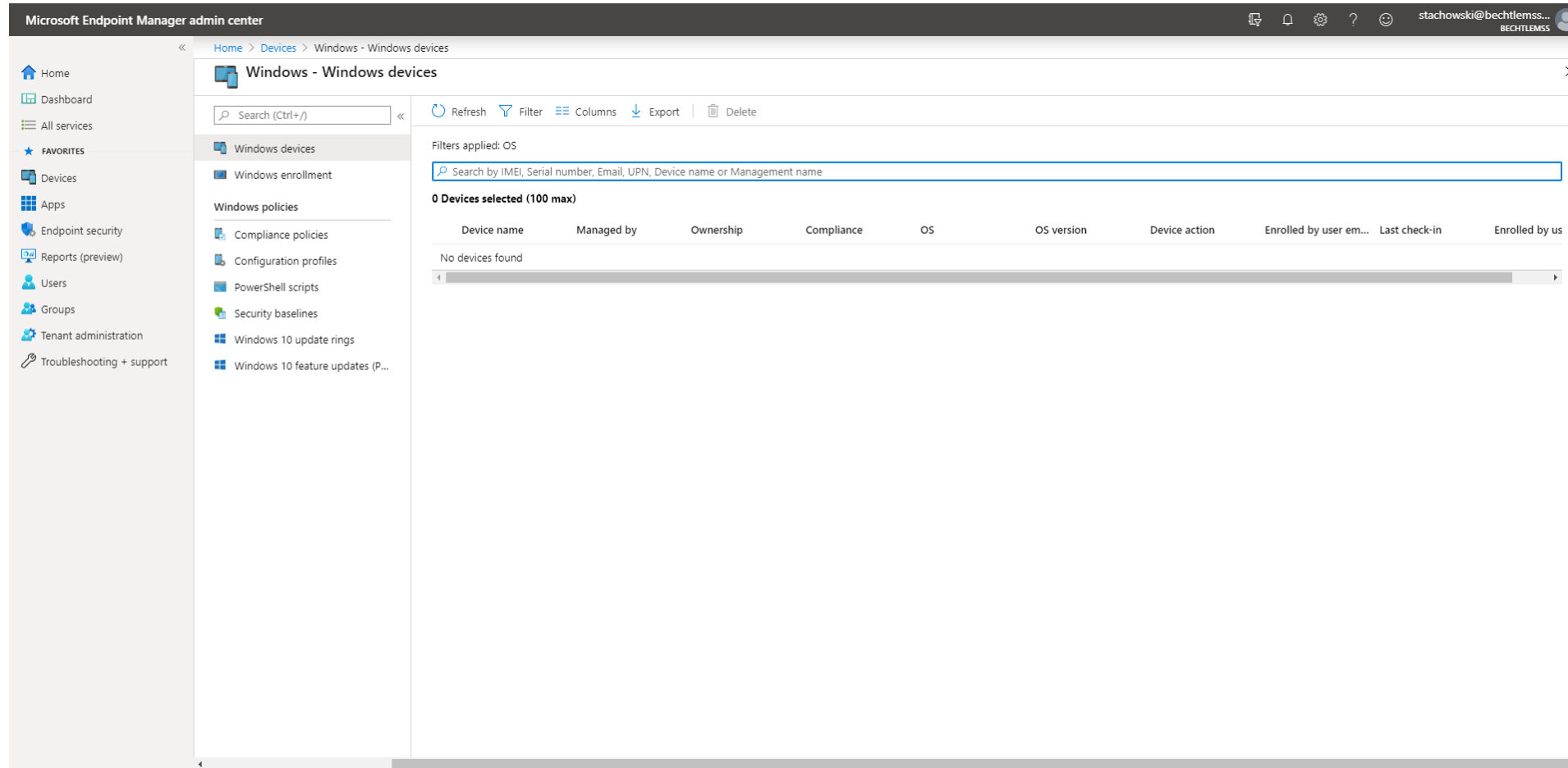
The main content area, titled 'Home page', shows the tenant 'bechtlemss' and a 'Status and alerts' section. This section includes 'Tenant status' with three indicators: Account status (Active), Service health (Healthy), and Connector status (Healthy). It also features 'Resource alerts' with two items: 'Device enrollment' (No intune enrollment failures) and 'Device configuration' (No configuration failures), both marked with green checkmarks. Below this, there are 'Guided scenarios' for 'Deploy Edge for mobile' and 'Try out a cloud-managed PC', each with a 'Start' button. The 'News and support' section includes links to the 'Intune Customer Success blog' and 'What's happening in Intune'.

Microsoft Endpoint Manager – Devices



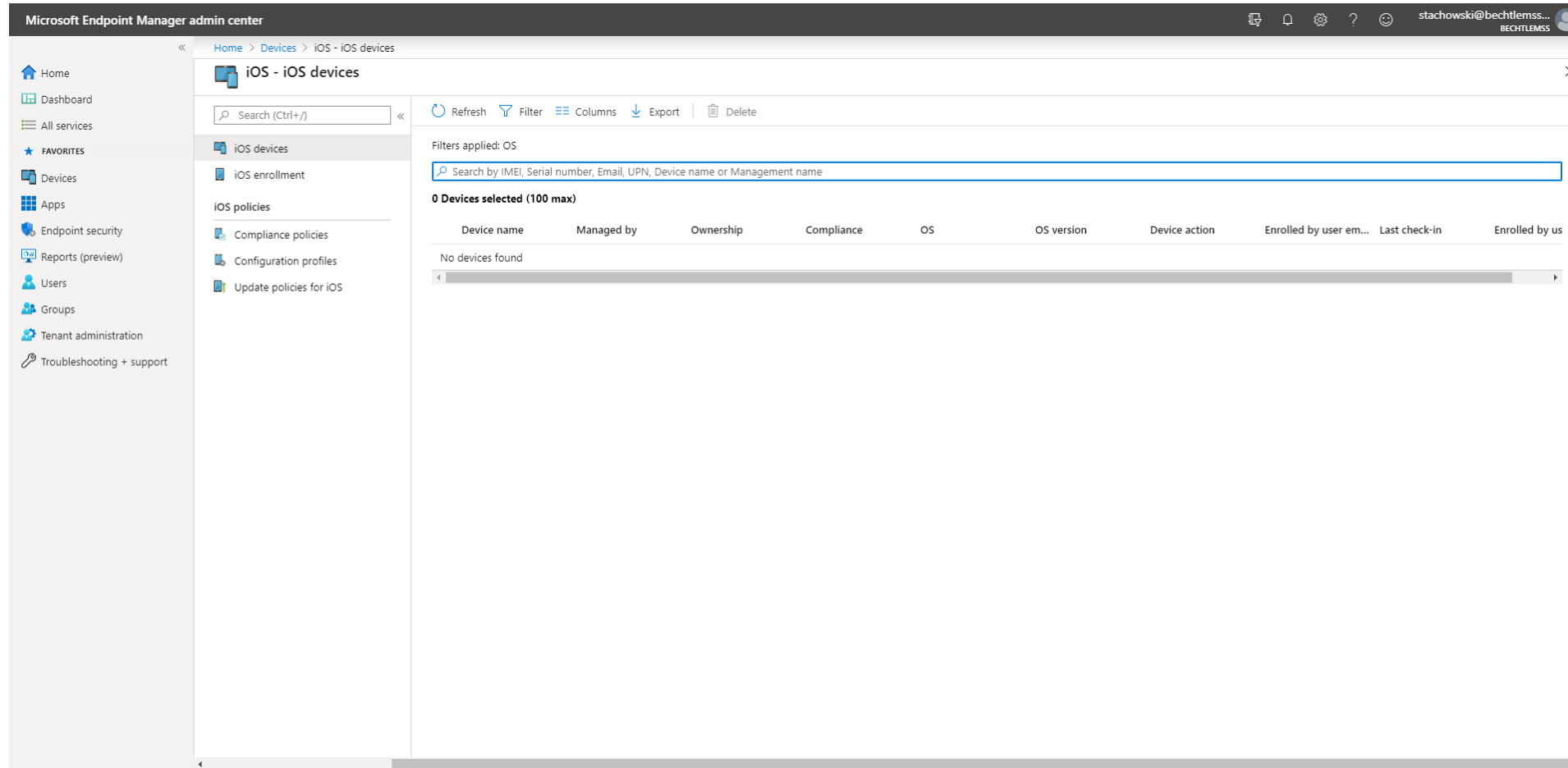
The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar shows the user 'stachowski@bechtle...' and the 'BECHTLEMSS' organization. The left sidebar contains a navigation menu with sections like 'Home', 'All services', 'FAVORITES', and 'Devices'. The main content area is titled 'Devices - Overview' and includes a search bar, a list of navigation links (Overview, All devices, Monitor, By platform), and a list of device enrollment and policy options. The 'By platform' section lists Windows, iOS, macOS, and Android. The 'Device enrollment' section includes 'Enroll devices'. The 'Policy' section lists various policies like Compliance policies, Conditional access, Configuration profiles, PowerShell scripts, Device security, Windows 10 update rings, Windows 10 feature updates, Update policies for iOS, Enrollment restrictions, eSIM cellular profiles (Preview), and Policy sets. The 'Other' section is also visible. The main content area displays 'Intune enrolled devices' with a table showing 'Platform' and 'Devices'. Below this, there is a section for 'Enrollment failures by OS' with a bar chart showing zero failures for iOS, macOS, Android, Windows, and Windows Mobile. The chart is dated 18.1.2020. Below the chart, there is a section for 'Top enrollment failures this week' which shows 'No data to display'.

Microsoft Endpoint Manager – Windows Devices



The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar shows the user's name 'stachowski@bechtle...' and the company 'BECHTLEMSS'. The left sidebar contains a navigation menu with options like Home, Dashboard, All services, and a FAVORITES section. The main content area is titled 'Windows - Windows devices' and includes a search bar, a list of filters (Refresh, Filter, Columns, Export, Delete), and a table of devices. The table has columns for Device name, Managed by, Ownership, Compliance, OS, OS version, Device action, Enrolled by user em..., Last check-in, and Enrolled by us. The table currently shows '0 Devices selected (100 max)' and 'No devices found'.

Microsoft Endpoint Manager – iOS Devices



Microsoft Endpoint Manager admin center

Home > Devices > iOS - iOS devices

Home

Dashboard

All services

FAVORITES

Devices

Apps

Endpoint security

Reports (preview)

Users

Groups

Tenant administration

Troubleshooting + support

iOS - iOS devices

Search (Ctrl+/)

Refresh Filter Columns Export Delete

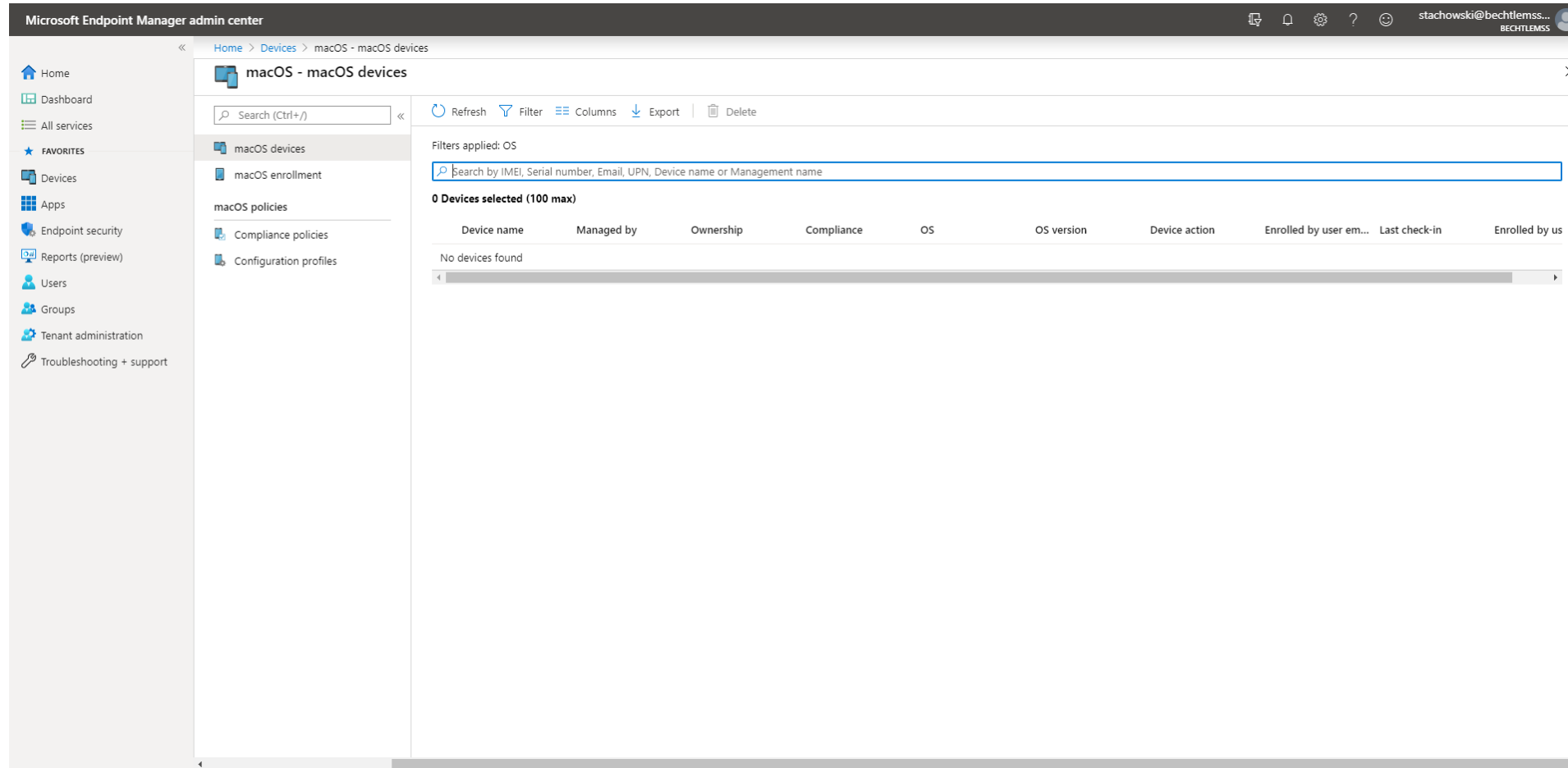
Filters applied: OS

Search by IMEI, Serial number, Email, UPN, Device name or Management name

0 Devices selected (100 max)

Device name	Managed by	Ownership	Compliance	OS	OS version	Device action	Enrolled by user em...	Last check-in	Enrolled by us
No devices found									

Microsoft Endpoint Manager – MacOS Devices



The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar shows the user 'stachowski@bechtlemss...' and the 'BECHTLEMSS' organization. The left sidebar contains a navigation menu with options like Home, Dashboard, All services, and various management tools. The main content area is titled 'macOS - macOS devices' and includes a search bar, filters, and a table of devices. The table is currently empty, showing '0 Devices selected (100 max)' and 'No devices found'.

Microsoft Endpoint Manager admin center

Home > Devices > macOS - macOS devices

macOS - macOS devices

Search (Ctrl+/)

Refresh Filter Columns Export Delete

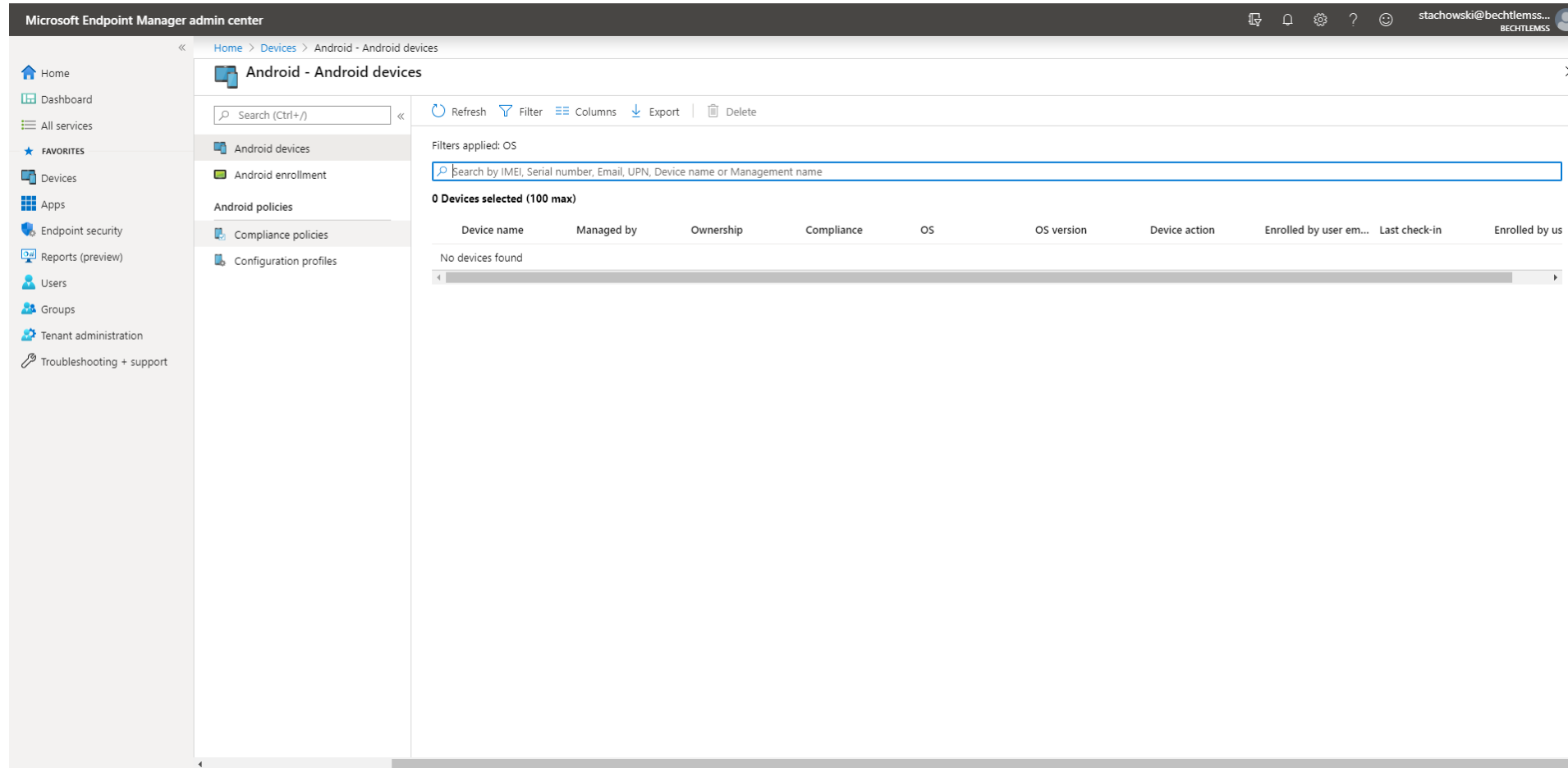
Filters applied: OS

Search by IMEI, Serial number, Email, UPN, Device name or Management name

0 Devices selected (100 max)

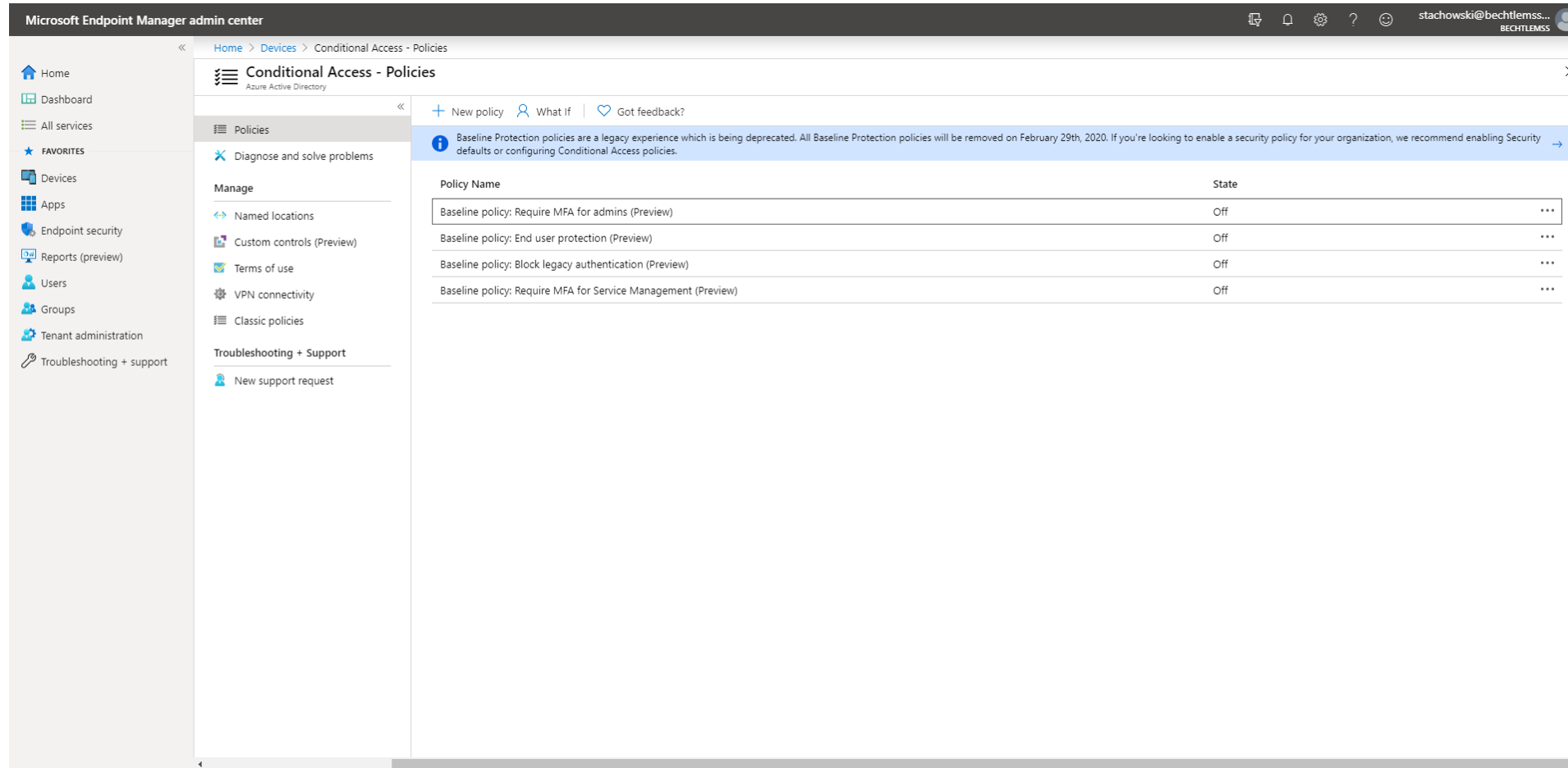
Device name	Managed by	Ownership	Compliance	OS	OS version	Device action	Enrolled by user em...	Last check-in	Enrolled by us
No devices found									

Microsoft Endpoint Manager – Android Devices



The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar shows the user's name 'stachowski@bechtlemss...' and the 'BECHTLEMSS' organization. The left sidebar contains a navigation menu with options like Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports (preview), Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Android - Android devices' and includes a search bar, a list of filters (Refresh, Filter, Columns, Export, Delete), and a table of devices. The table has columns for Device name, Managed by, Ownership, Compliance, OS, OS version, Device action, Enrolled by user em..., Last check-in, and Enrolled by us. The table currently shows '0 Devices selected (100 max)' and 'No devices found'.

Microsoft Endpoint Manager – Conditional Access



Microsoft Endpoint Manager admin center

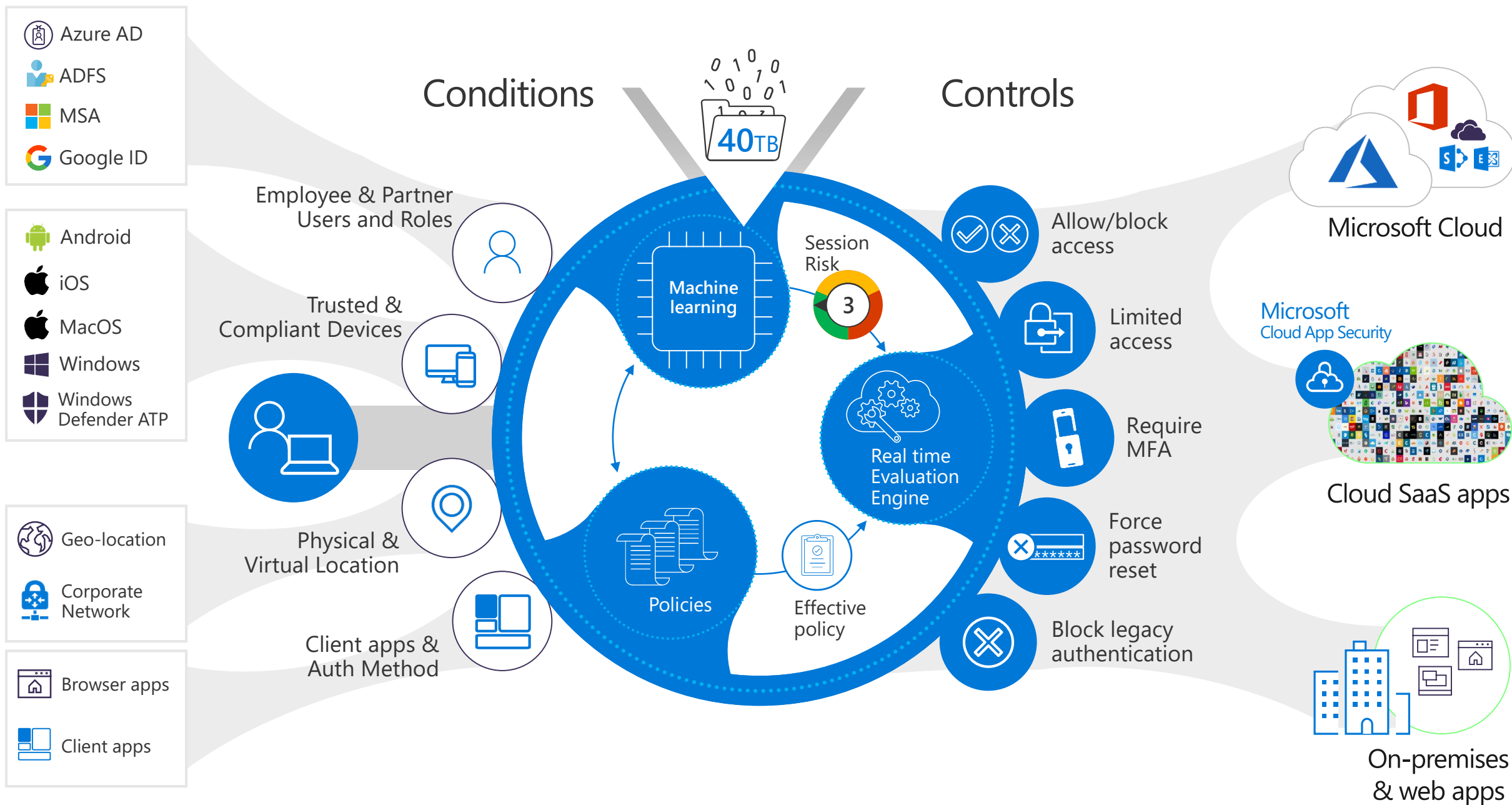
Home > Devices > Conditional Access - Policies

Conditional Access - Policies

Baseline Protection policies are a legacy experience which is being deprecated. All Baseline Protection policies will be removed on February 29th, 2020. If you're looking to enable a security policy for your organization, we recommend enabling Security defaults or configuring Conditional Access policies.

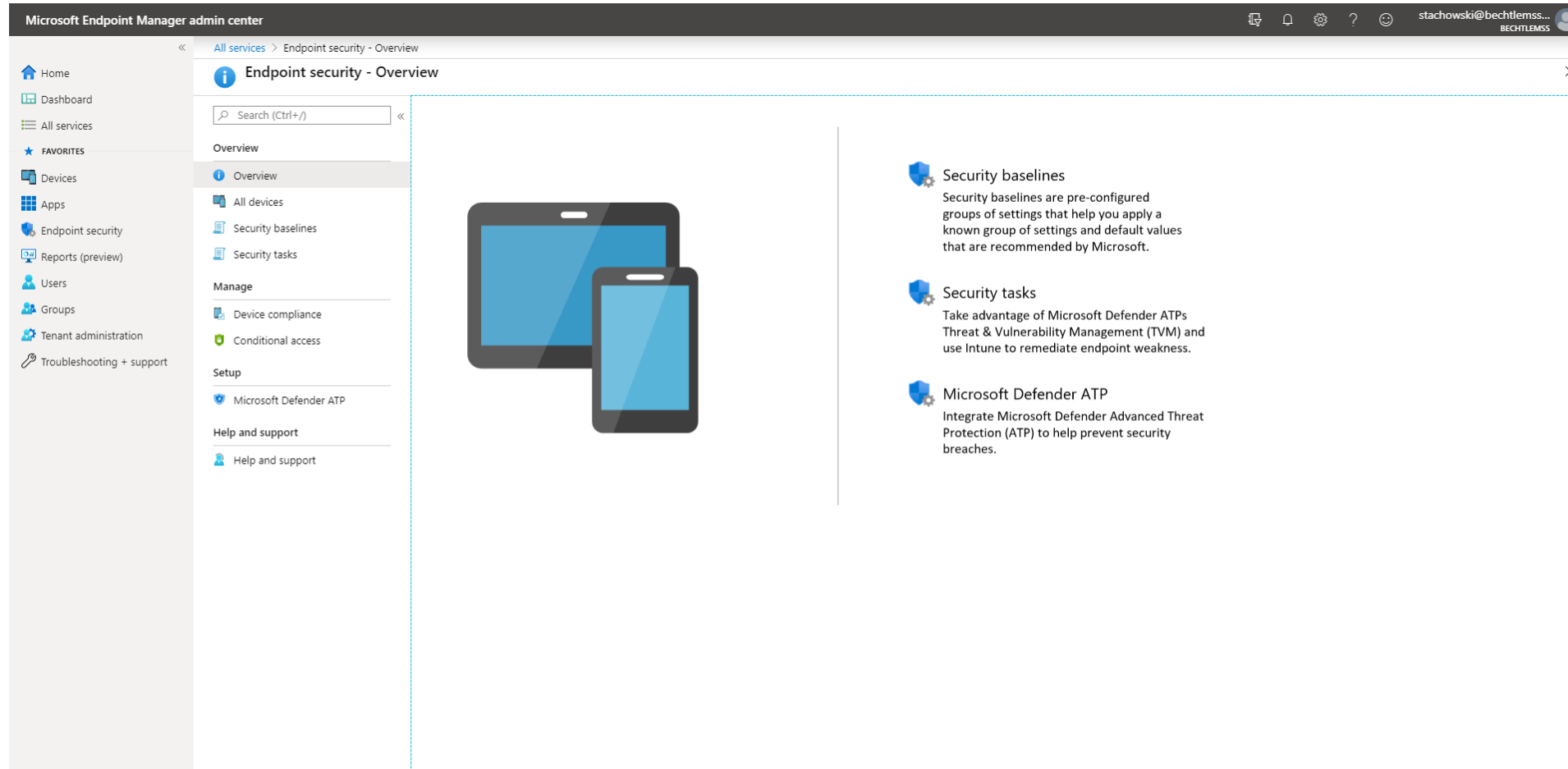
Policy Name	State
Baseline policy: Require MFA for admins (Preview)	Off
Baseline policy: End user protection (Preview)	Off
Baseline policy: Block legacy authentication (Preview)	Off
Baseline policy: Require MFA for Service Management (Preview)	Off

Conditional Access





Microsoft Endpoint Manager – Endpoint Protection



The screenshot displays the Microsoft Endpoint Manager admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports (preview), Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Endpoint security - Overview" and includes a search bar. Below the search bar, there are sections for Overview, Manage, Setup, and Help and support. The Overview section is currently selected, showing a list of items: All devices, Security baselines, and Security tasks. The Manage section includes Device compliance and Conditional access. The Setup section includes Microsoft Defender ATP. The Help and support section includes Help and support. The main content area also features a large illustration of a tablet and a smartphone, and three key features are highlighted: Security baselines, Security tasks, and Microsoft Defender ATP.

Endpoint security - Overview

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Device compliance
- Conditional access

Setup

- Microsoft Defender ATP

Help and support

- Help and support

Security baselines
Security baselines are pre-configured groups of settings that help you apply a known group of settings and default values that are recommended by Microsoft.

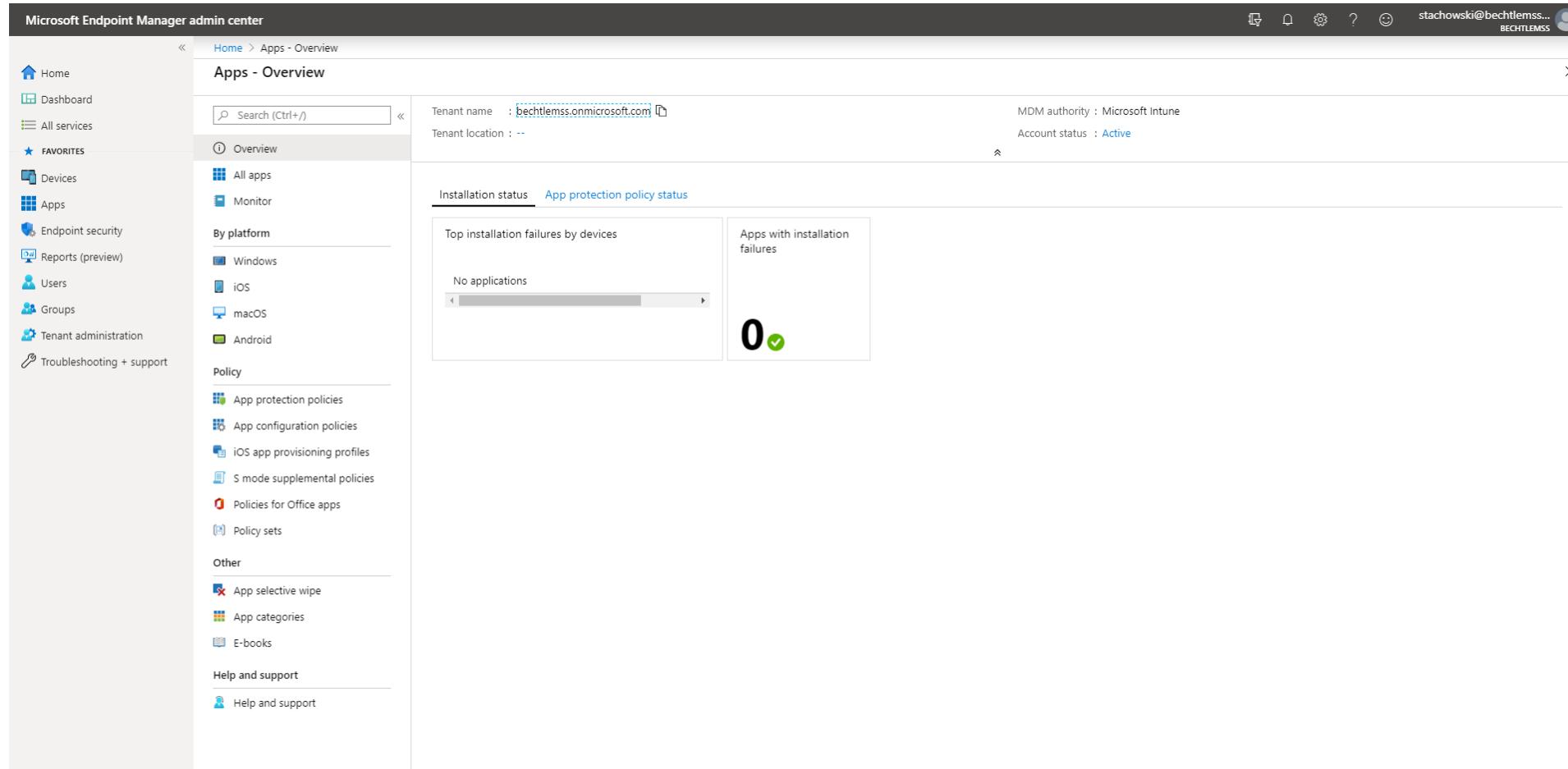
Security tasks
Take advantage of Microsoft Defender ATPs Threat & Vulnerability Management (TVM) and use Intune to remediate endpoint weakness.

Microsoft Defender ATP
Integrate Microsoft Defender Advanced Threat Protection (ATP) to help prevent security breaches.

Mobile Security - MAM Richtlinien

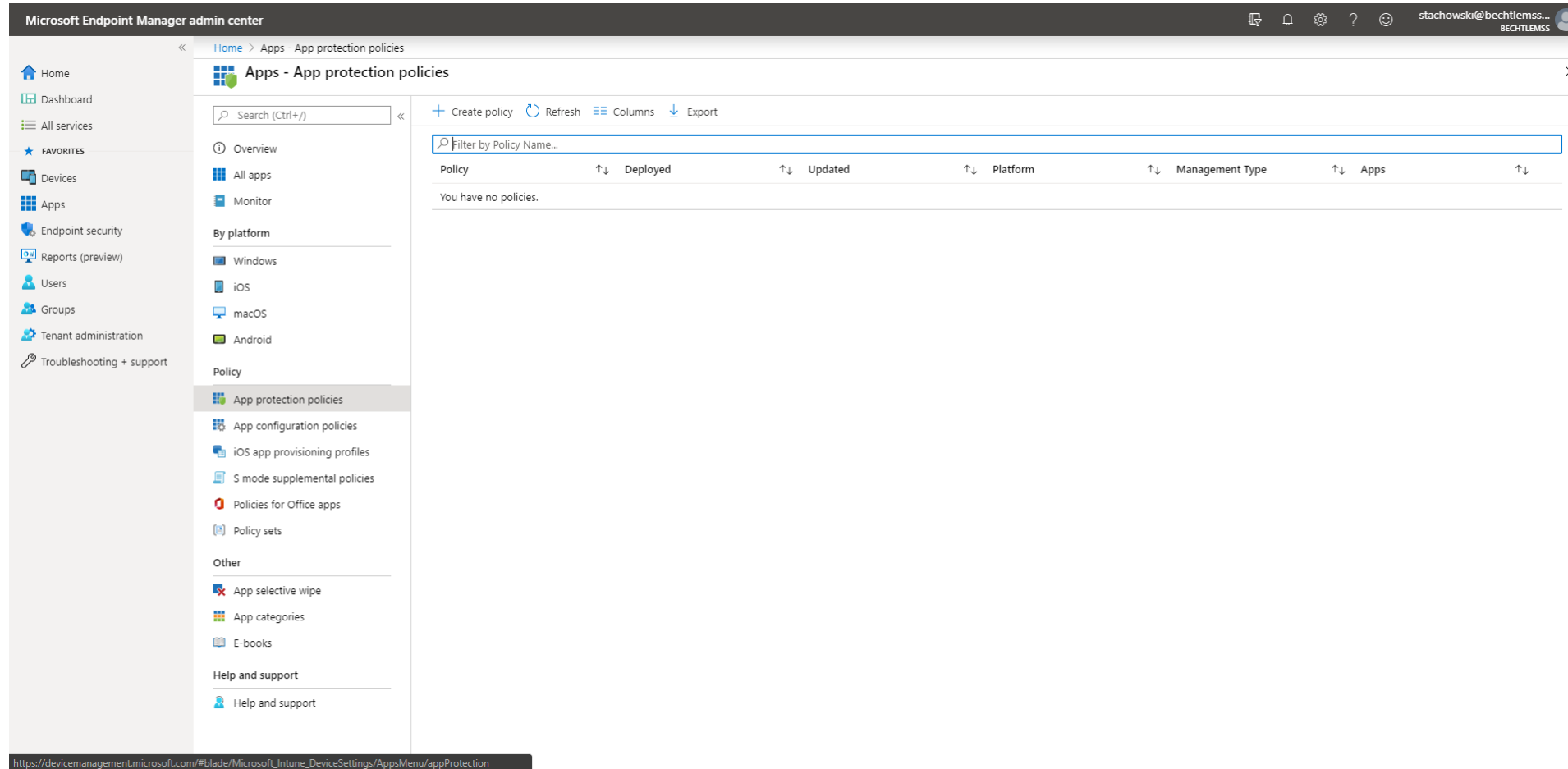


Microsoft Endpoint Manager – App Verwaltung (MAM)



The screenshot displays the Microsoft Endpoint Manager admin center interface. The top navigation bar shows the user 'stachowski@bechtlems...' and the tenant 'BECHTLEMSS'. The left sidebar contains a navigation menu with categories like 'Home', 'All services', 'FAVORITES', 'Devices', 'Apps', 'Endpoint security', 'Reports (preview)', 'Users', 'Groups', 'Tenant administration', and 'Troubleshooting + support'. The main content area is titled 'Apps - Overview' and includes a search bar, tenant information (Tenant name: bechtlems.onmicrosoft.com, MDM authority: Microsoft Intune, Account status: Active), and two tabs: 'Installation status' and 'App protection policy status'. The 'Installation status' tab shows 'Top installation failures by devices' with 'No applications' and 'Apps with installation failures' with a count of '0' and a green checkmark.

Microsoft Endpoint Manager – App Verwaltung (MAM)



Microsoft Endpoint Manager admin center

Home > Apps > App protection policies

Apps - App protection policies

Search (Ctrl+/)

Filter by Policy Name...

Policy	↑↓ Deployed	↑↓ Updated	↑↓ Platform	↑↓ Management Type	↑↓ Apps
You have no policies.					

By platform

- Windows
- iOS
- macOS
- Android

Policy

- App protection policies
- App configuration policies
- iOS app provisioning profiles
- S mode supplemental policies
- Policies for Office apps
- Policy sets

Other

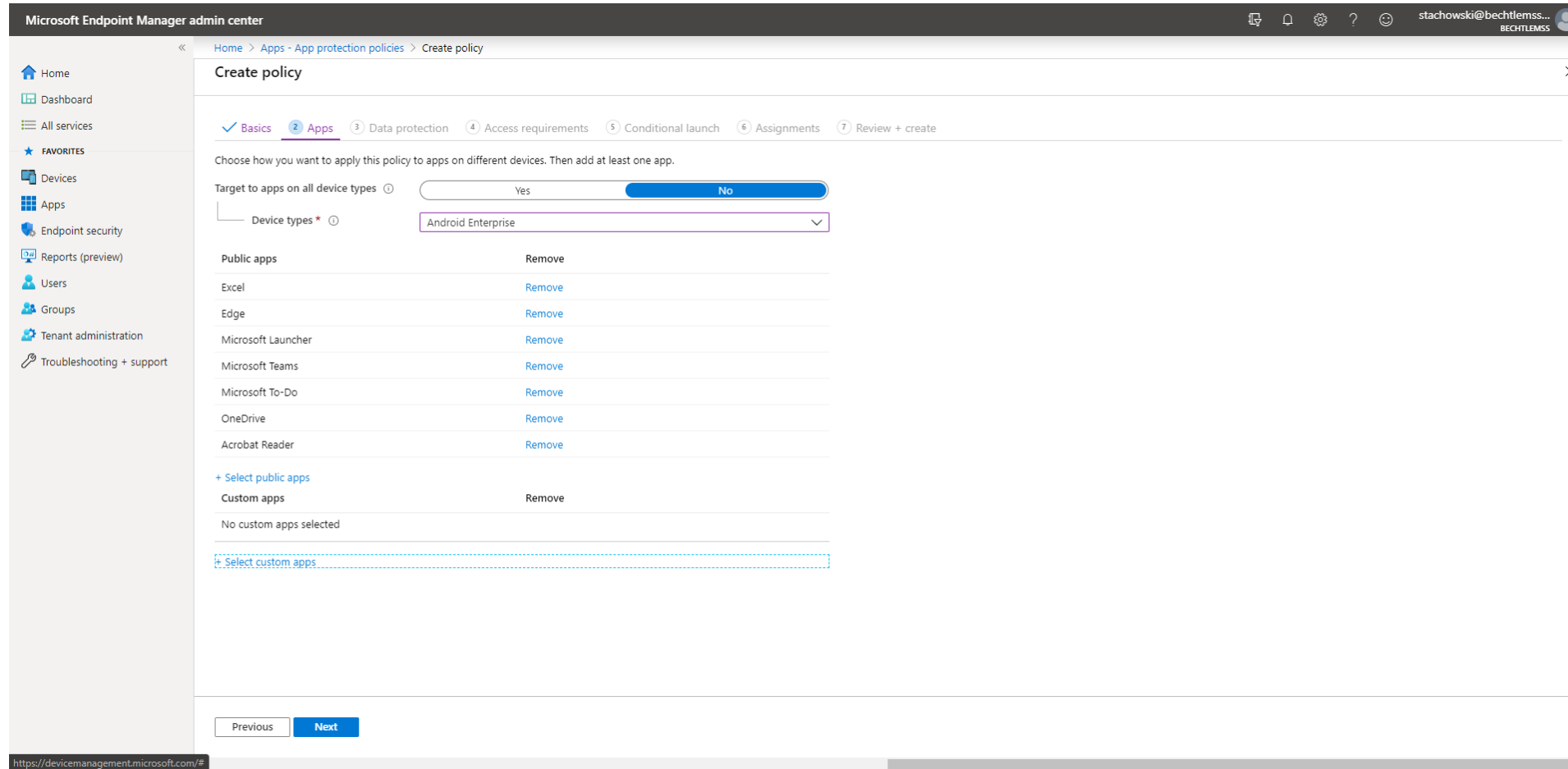
- App selective wipe
- App categories
- E-books

Help and support

- Help and support

https://devicemanagement.microsoft.com/#blade/Microsoft_Intune_DeviceSettings/AppsMenu/appProtection

Microsoft Endpoint Manager – App Verwaltung (MAM)



The screenshot shows the 'Create policy' page in the Microsoft Endpoint Manager admin center. The breadcrumb trail is: Home > Apps - App protection policies > Create policy. The page has a sidebar with navigation links: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports (preview), Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create policy' and includes a progress bar with steps: Basics (checked), Apps (active), Data protection, Access requirements, Conditional launch, Assignments, and Review + create. Below the progress bar, there is a section 'Choose how you want to apply this policy to apps on different devices. Then add at least one app.' This section contains a toggle for 'Target to apps on all device types' set to 'No', a dropdown for 'Device types' set to 'Android Enterprise', and a list of 'Public apps' with 'Remove' links for each: Excel, Edge, Microsoft Launcher, Microsoft Teams, Microsoft To-Do, OneDrive, and Acrobat Reader. There is also a '+ Select public apps' link. Below this is a section for 'Custom apps' with a 'Remove' link and the text 'No custom apps selected'. At the bottom, there is a '+ Select custom apps' link. The page footer shows the URL 'https://devicemanagement.microsoft.com/#' and navigation buttons 'Previous' and 'Next'.

Microsoft Endpoint Manager – App Verwaltung (MAM)

Microsoft Endpoint Manager admin center

Home > Apps > App protection policies > Create policy

Create policy

✓ Basics ✓ Apps **3 Data protection** 4 Access requirements 5 Conditional launch 6 Assignments 7 Review + create

This group includes the data loss prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer

Backup org data to Android backup services ☒ Allow ☐ Block

Send org data to other apps

Select apps to exempt

Save copies of org data ☐ Allow ☐ Block

Allow user to save copies to selected services

Receive data from other apps

Restrict cut, copy, and paste between other apps

Cut and copy character limit for any app

Screen capture and Google Assistant ☒ Allow ☐ Block

Approved keyboards ☐ Require ☒ Not required

Select keyboards to approve

Encryption

Encrypt org data ☒ Require ☐ Not required

Encrypt org data on enrolled devices ☒ Require ☐ Not required

Microsoft Endpoint Manager – App Verwaltung (MAM)

Microsoft Endpoint Manager admin center

Home > Apps - App protection policies > Create policy

Create policy

✓ Basics ✓ Apps ✓ Data protection **4 Access requirements** 5 Conditional launch 6 Assignments 7 Review + create

Configure the PIN and credential requirements that users must meet to access apps in a work context.

PIN for access ☒ Require ☐ Not required

PIN type ☒ Numeric ☐ Passcode

Simple PIN ☒ Allow ☐ Block

Select minimum PIN length

Fingerprint instead of PIN for access (Android 6.0+) ☒ Allow ☐ Block

Override fingerprint with PIN after timeout ☒ Require ☐ Not required

Timeout (minutes of inactivity)

PIN reset after number of days ☐ Yes ☒ No

Number of days

Select number of previous PIN values to maintain

App PIN when device PIN is set ☒ Require ☐ Not required

Work or school account credentials for access ☐ Require ☒ Not required

Recheck the access requirements after (minutes of inactivity)

Previous Next

Microsoft Endpoint Manager – App Verwaltung (MAM)

Microsoft Endpoint Manager admin center

Home > Apps - App protection policies > Create policy

Create policy

[✓ Basics](#)
[✓ Apps](#)
[✓ Data protection](#)
[✓ Access requirements](#)
[5 Conditional launch](#)
[6 Assignments](#)
[7 Review + create](#)

Set the sign-in security requirements for your access protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company app. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. [Learn more about conditional launch actions.](#)

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN ...
Offline grace period	720	Block access (minutes) ...
Offline grace period	90	Wipe data (days) ...

Select one

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. [Learn more about configuring device compliance settings for enrolled devices.](#)

Setting	Value	Action
Jailbroken/rooted devices		Block access ...

Select one

Previous Next

Lizenzierung



Lizenzierung

	Enterprise Mobility + Security E3	Enterprise Mobility + Security E5
Einfachere Zugriffsverwaltung und Sicherheit	✓	✓
Mehrstufige Authentifizierung	✓	✓
Bedingter Zugriff	✓	✓
Risikobasierter bedingter Zugriff		✓
Erweiterte Sicherheitsberichte	✓	✓
Privileged Identity Management		✓
Windows Server-Clientzugriffslizenz (Client Access License, CAL)*	✓	✓

M365 on a Page



Roadmap



Roadmap

App Verwaltung

- Anzeigen von Benachrichtigungen für die Unternehmensportal-App unter Windows
- Anzeigen von Installationsstatusmeldungen für die Unternehmensportal-App
- Festlegen von Microsoft Edge als Zielbrowser für Webclips auf iOS-Geräten
- Verbesserungen an den Funktionen des macOS-Unternehmensportals
- App für Microsoft Defender Advanced Threat Protection (ATP) für macOS

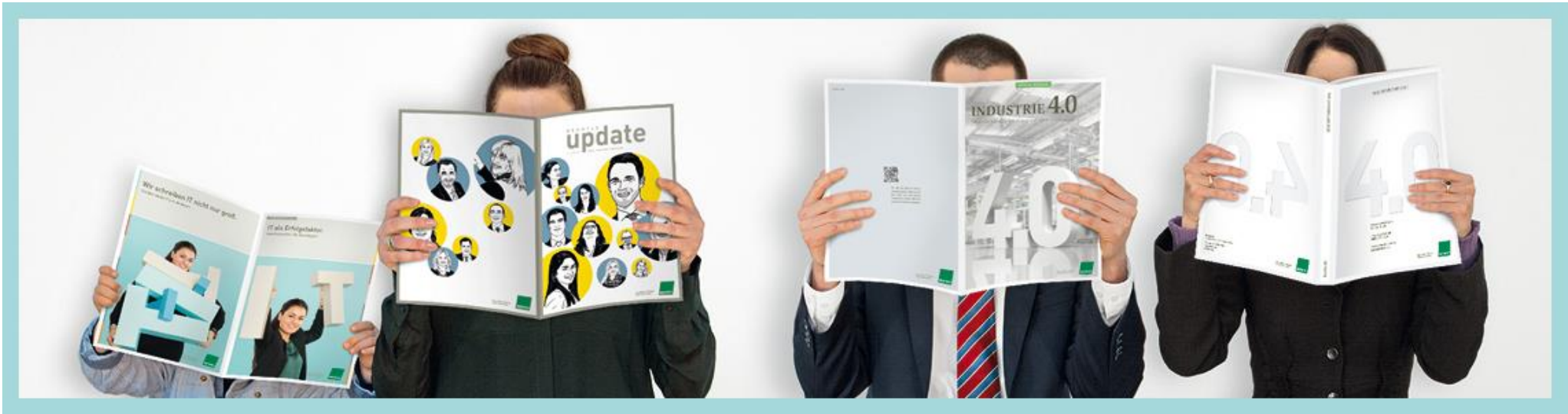
Gerätekonfiguration & Geräteverwaltung

- Verbesserte Benutzeroberfläche für das Erstellen von Konfigurationsprofilen auf iOS- und macOS-Geräten
- Ändern des primären Benutzers für Windows-Geräte
- Auswählen, welche iOS/iPadOS-Updates an registrierte Geräte gepusht werden sollen

Besten Dank! Stellen Sie uns Ihre Fragen.



Vorschau.



20.02.2020 Webinar: Citrix Summit 2020 Update

Mehr Infos unter bechtle.com/ch/ueber-bechtle/events

Handeln Sie jetzt. Kontaktieren Sie uns.

Bechtle Schweiz AG

Tel. +41 848 820 420

bechtle.ch/kontakt

Michael Stachowski

Michael Stachowski, Business Development Manager Microsoft Security,

Bechtle Logistik & Service, Neckarsulm

michael.stachowski@bechtle.com

