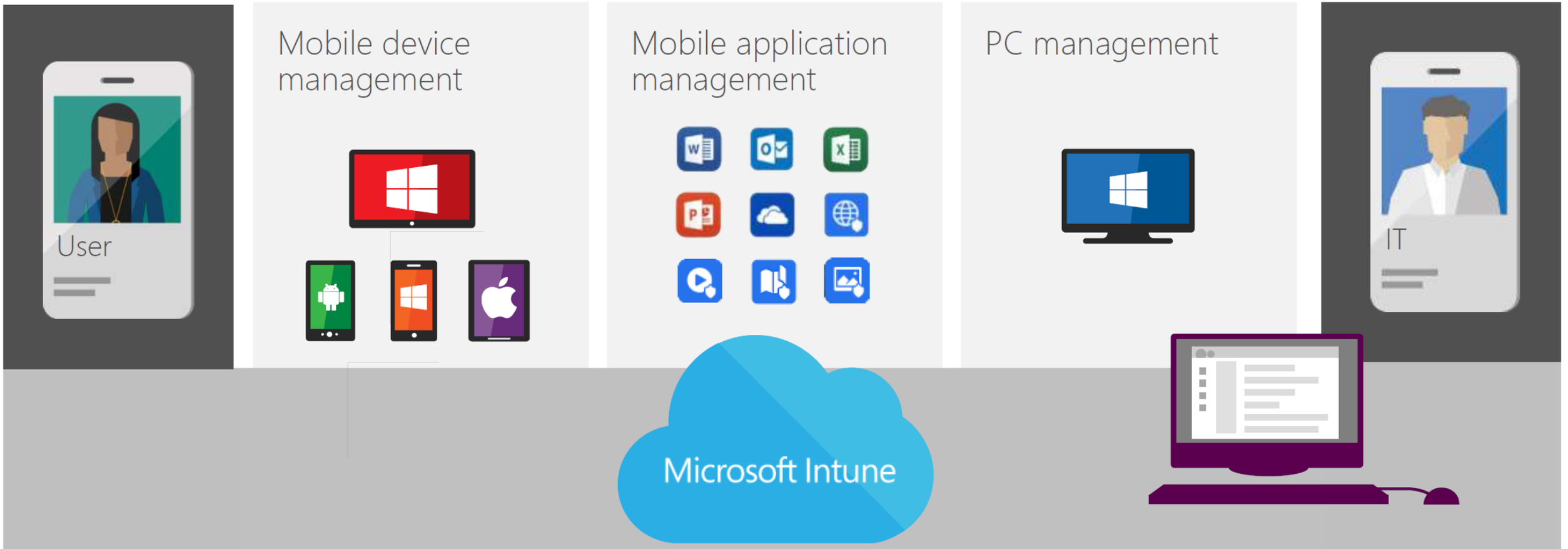
Microsoft

Mobile device and application management overview with Microsoft Intune

Sophie Chanialaki
Partner Technical Architect – Microsoft 365 Modern Desktop
Microsoft Central and Eastern Europe

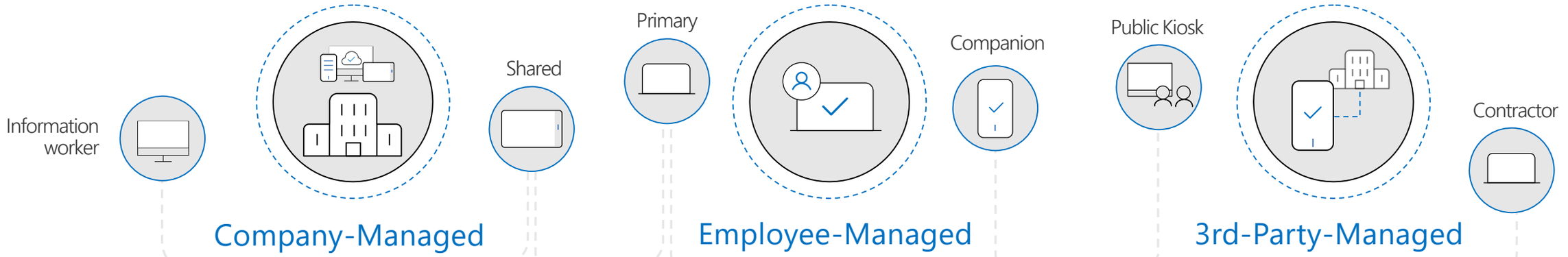
Enterprise mobility management with Intune



Intune helps organizations provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Unified endpoint management with Intune

Intune gives you the flexibility and control to secure your data on any device—even those you don't manage.



Secure your data on virtually **any** device with Intune

Mobile Device Management (MDM)

- Enroll devices for management
- Provision settings, certs, profiles
- Report & measure device compliance
- Remove company data from devices

Conditional Access: Restrict access to managed & compliant devices

Mobile Application Management (MAM)

- Publish mobile apps to users
- Configure and update apps
- Report app inventory & usage
- Secure & remove company data within mobile apps

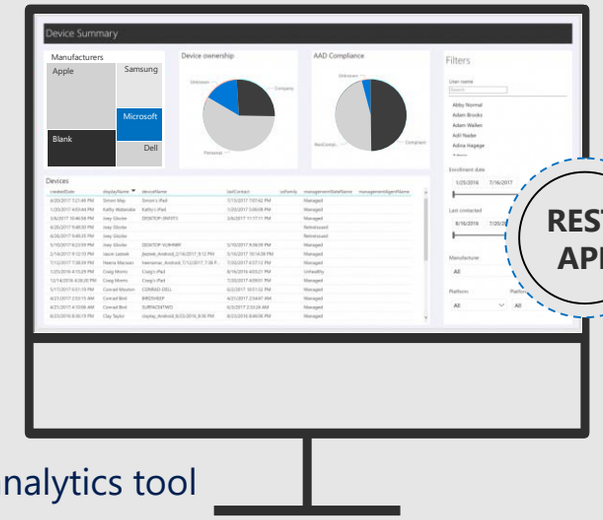
Conditional Access: Restrict which apps can be used to access email or files

Intune on Azure

Leverage Microsoft Graph API to access EMS and Office 365 data programmatically

Unified admin console

REST API



Favorite analytics tool

REST API

Users

Devices

Enterprise Mobility + Security

Apps

Data

REST API

Microsoft Graph API

Windows PowerShell

PS C: \> Manage and automate Intune, Azure AD, Office 365 and other Microsoft services with PowerShell, Python, and more.

Automate management workflows with other business and IT systems

Partners & resellers can integrate with Intune for their specific offerings

Built to meet the evolving needs of your enterprise

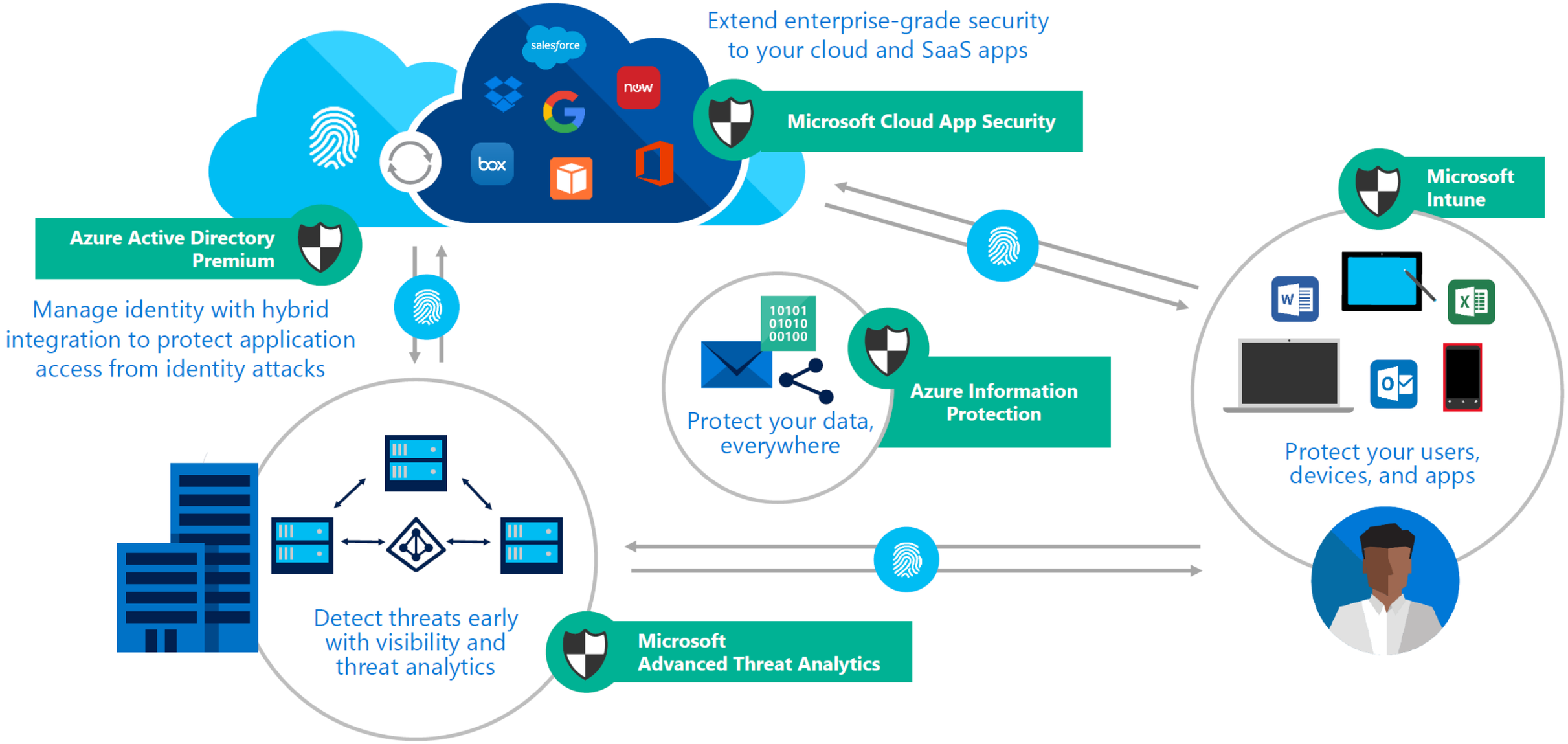
Redesigned architecture for scalability, resiliency, global availability, and security

Delivered from the cloud and always up-to-date

Connect to PowerBI and other reporting platforms

Historical data with Intune Data Warehouse

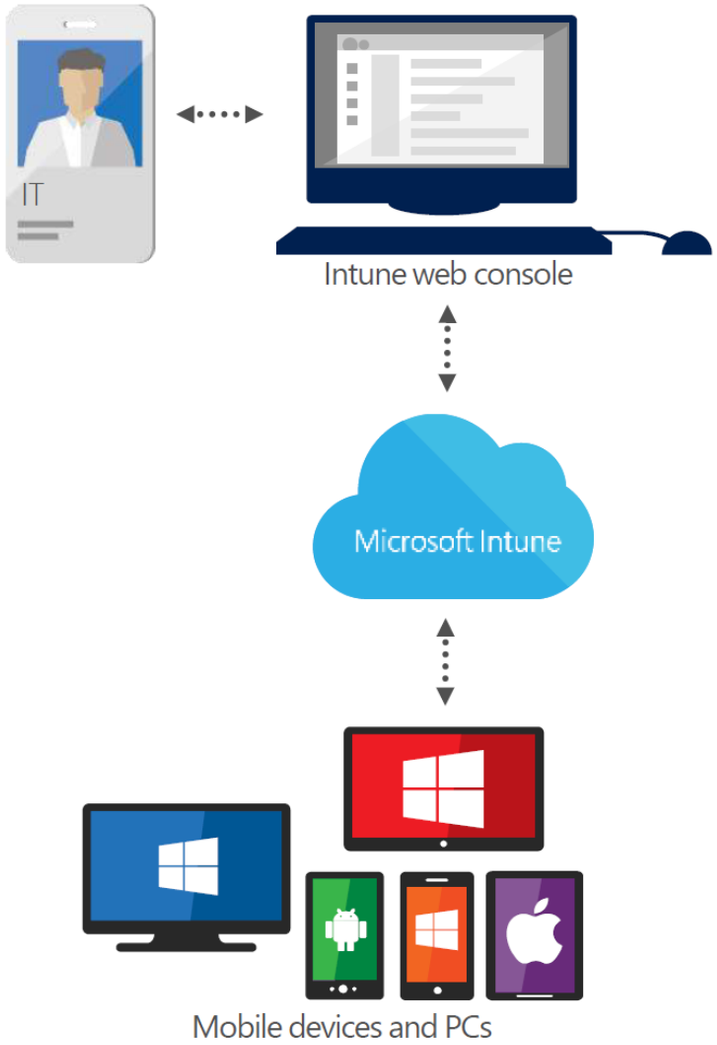
Enterprise Mobility +Security



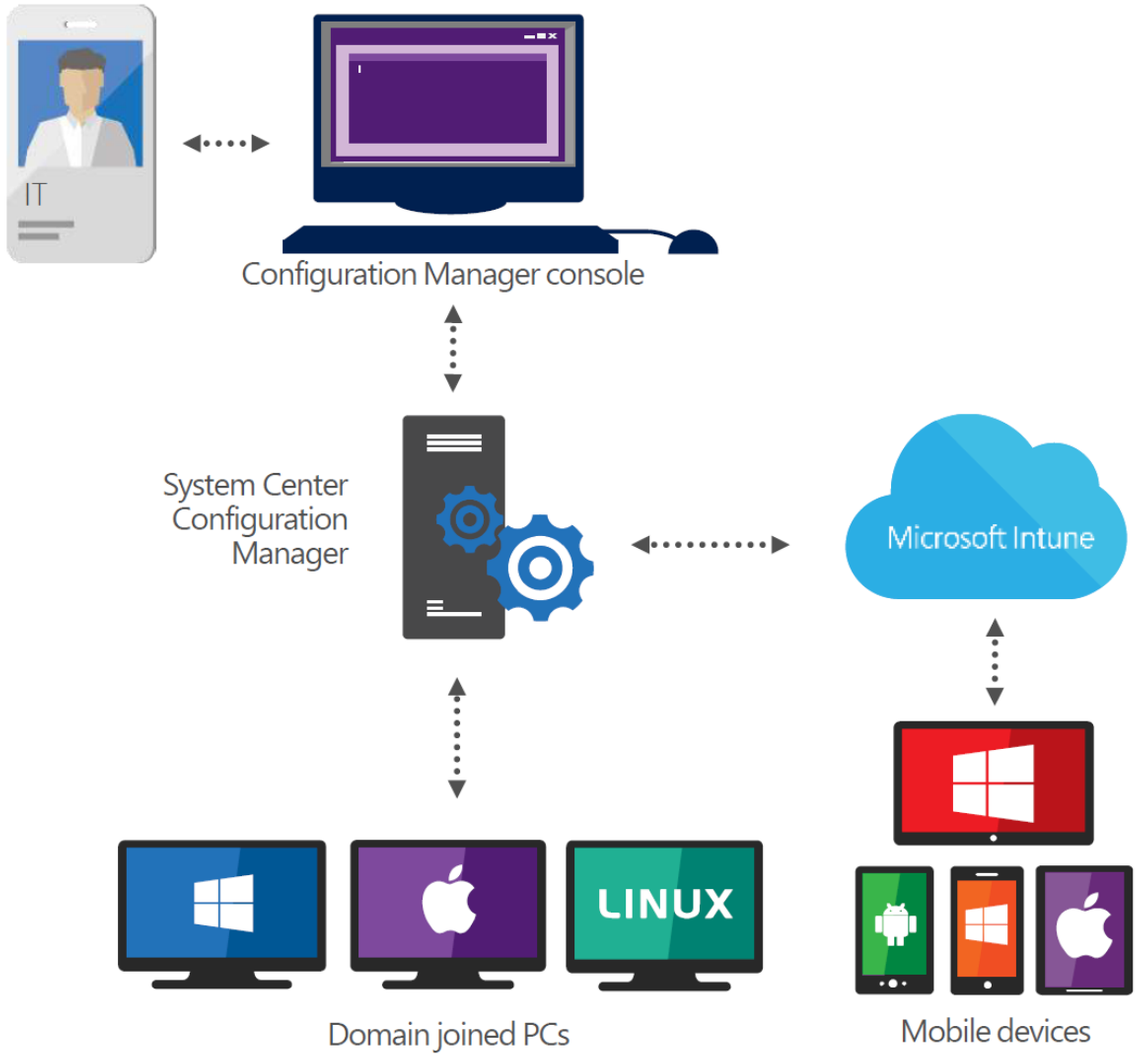
Deployment Scenarios

Deployment flexibility

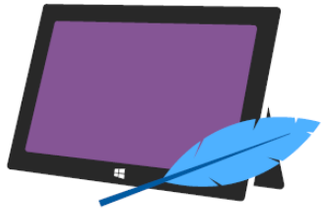
Intune standalone (cloud only)



Configuration Manager integrated with Intune (hybrid)

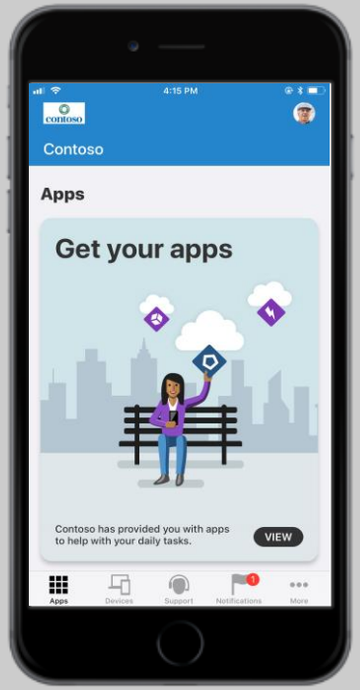


PC management

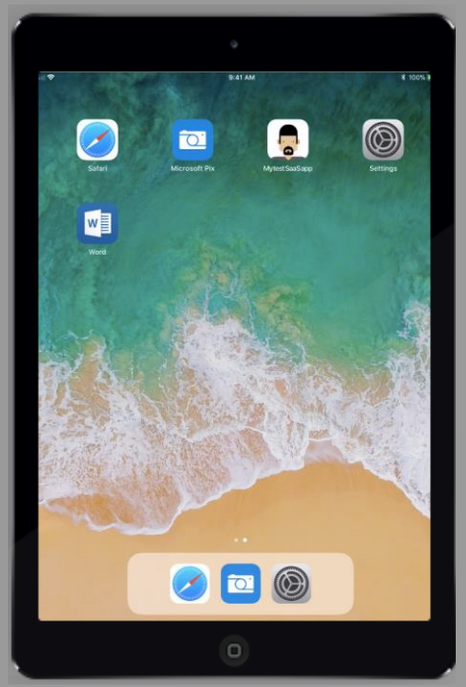


Intune standalone (cloud only)	Configuration Manager integrated with Intune (hybrid)
Lightweight, agentless OR agent-based management	Agent-based management only
PC protection from malware	PC protection from malware
PC software update management	PC software update management
Software distribution	Software distribution
Proactive monitoring and alerts	Proactive monitoring and alerts
Hardware and software inventory	Hardware and software inventory
Policies for Windows Firewall management	Policies for Windows Firewall management
	Operating system deployment
	PC, mobile device, Windows Server, Linux/Unix, Mac, and virtual desktop management
	Power management
	Custom reporting

iOS deployment scenarios



BYOD



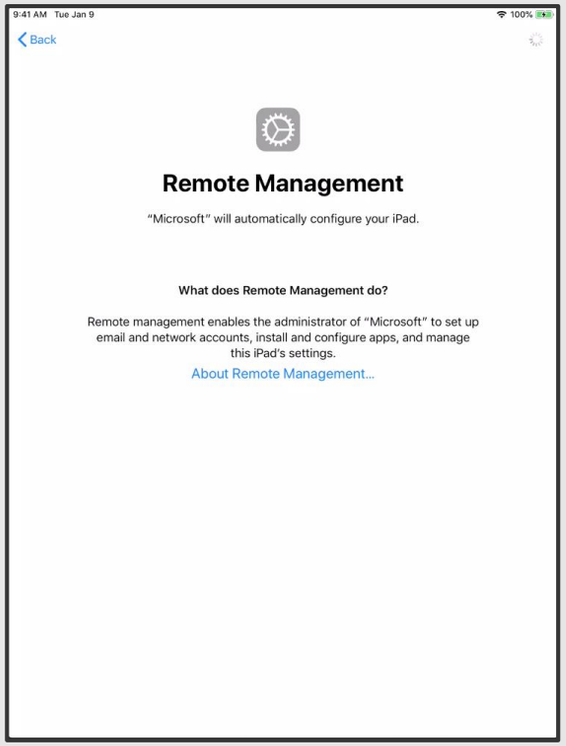
CORP OWNED

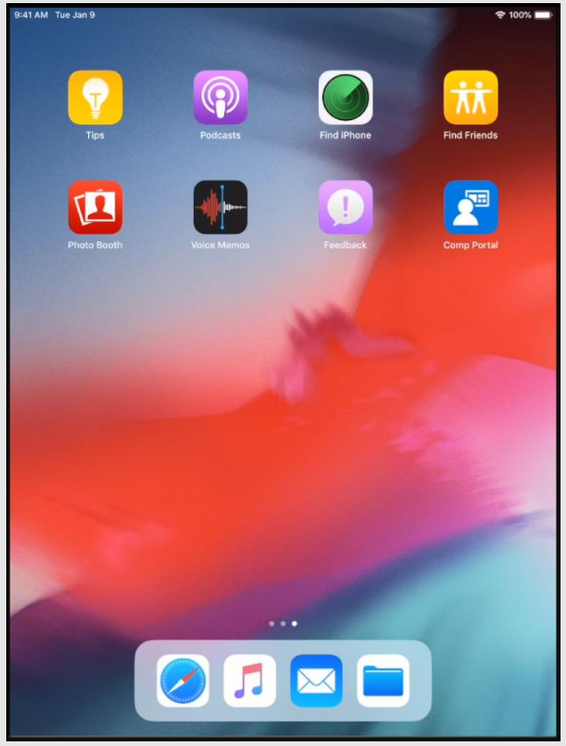
iOS app managed	iOS device managed	
• Data protection at the app level • App protection without full device management	• User-based enrollment via Company Portal • Push Apps and policies • Device based Compliance	• Apple Corporate programs like VPP, DEP, ASM • Supervised mode with for controls • Secure locked down devices: Kiosk, Classroom • Lock management profile to a device

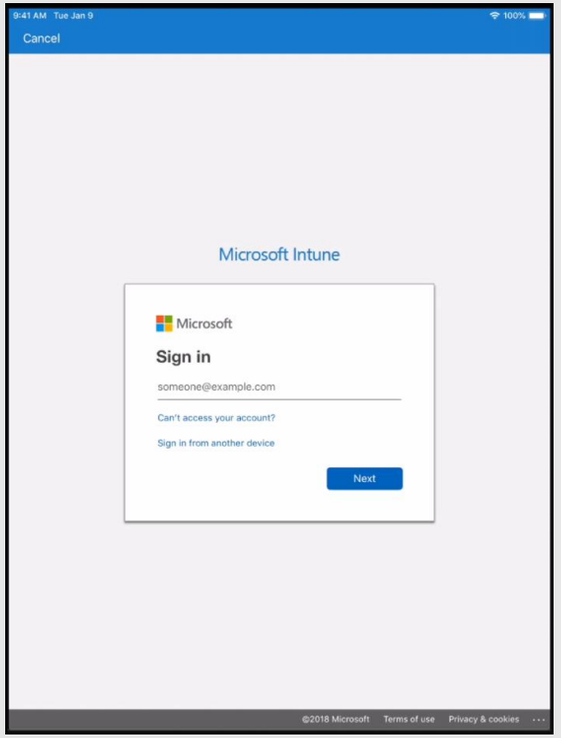
iOS DEP enrollment

User authentication via Company Portal

Setup Assistant → VPP → Company Portal downloads automatically → Single App Mode → User signs into Company Portal

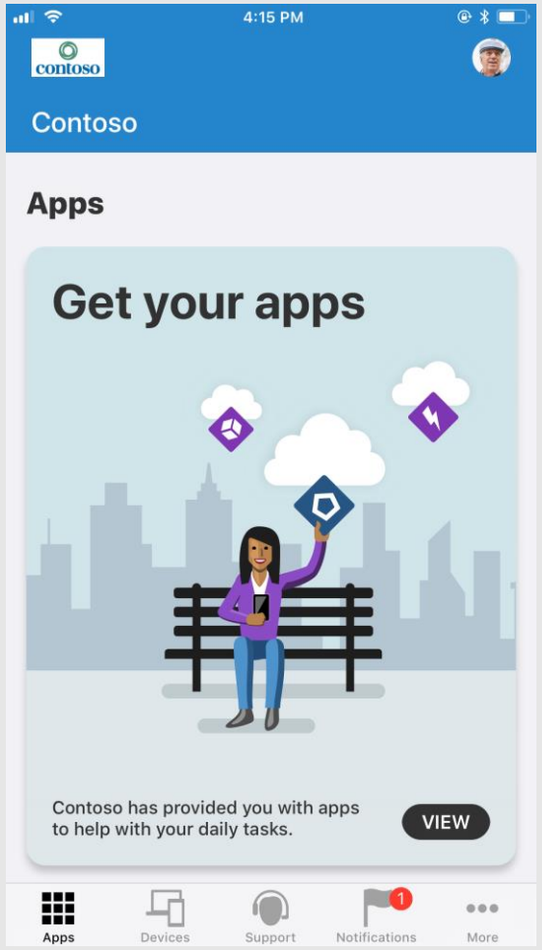


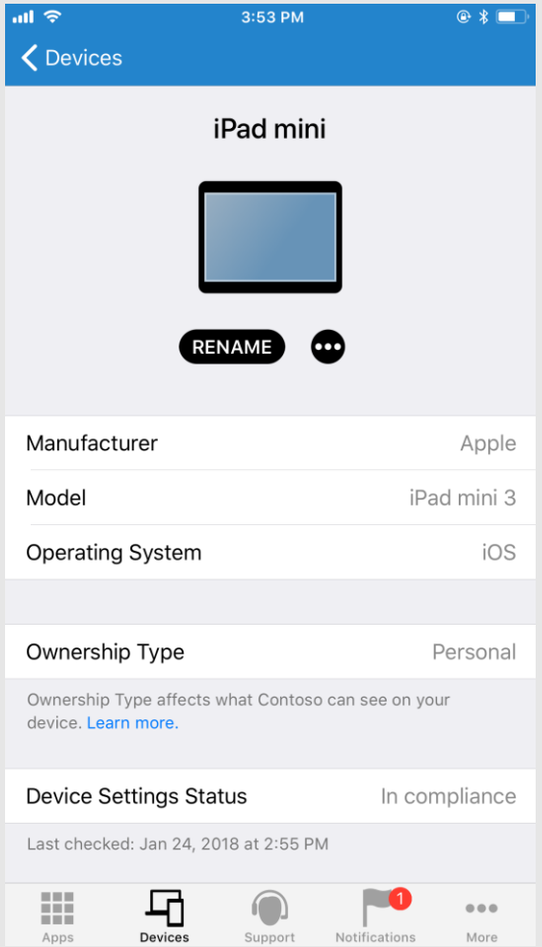


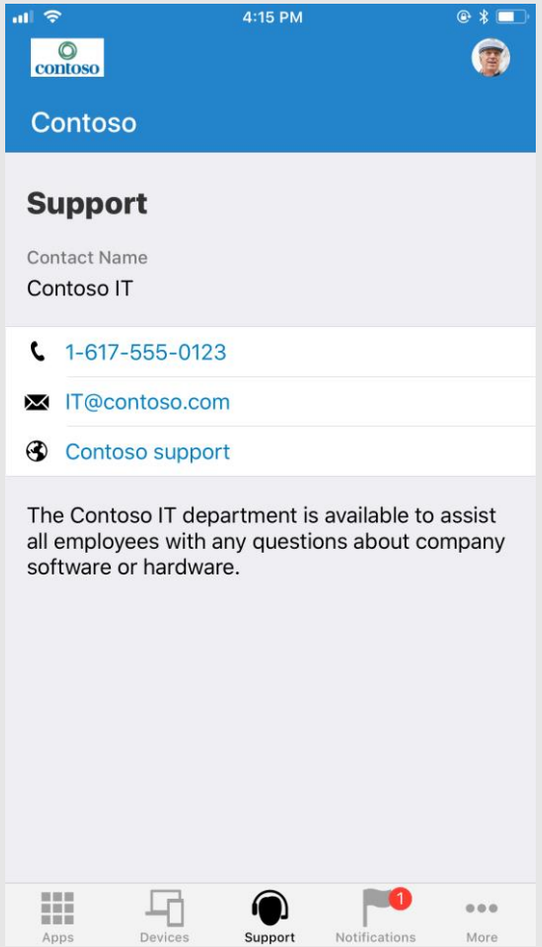


Company Portal

New End User Experience





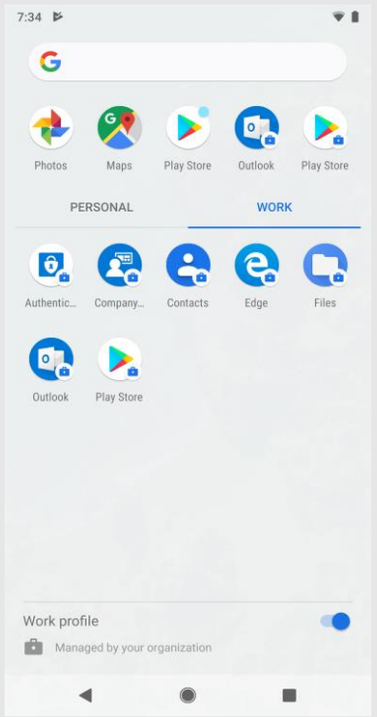


Android deployment scenarios

BYOD

Intune App Protection Without Enrollment

AE Work Profile



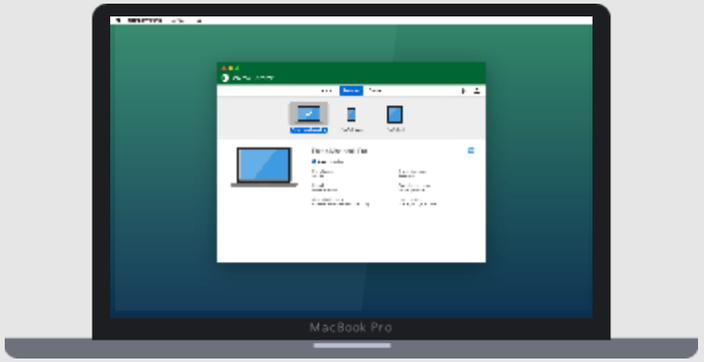
Corp Owned

AE Dedicated (kiosk)

Preview this year

AE Fully managed

macOS deployment scenarios



Intune managed

Basic platform MDM management. Ideal for:

- Scoped/modern management needs for corp owned devices
- Deploying certs, pw configuration, apps
- Limiting access to compliant Macs
- Protection with device wipe, encryption

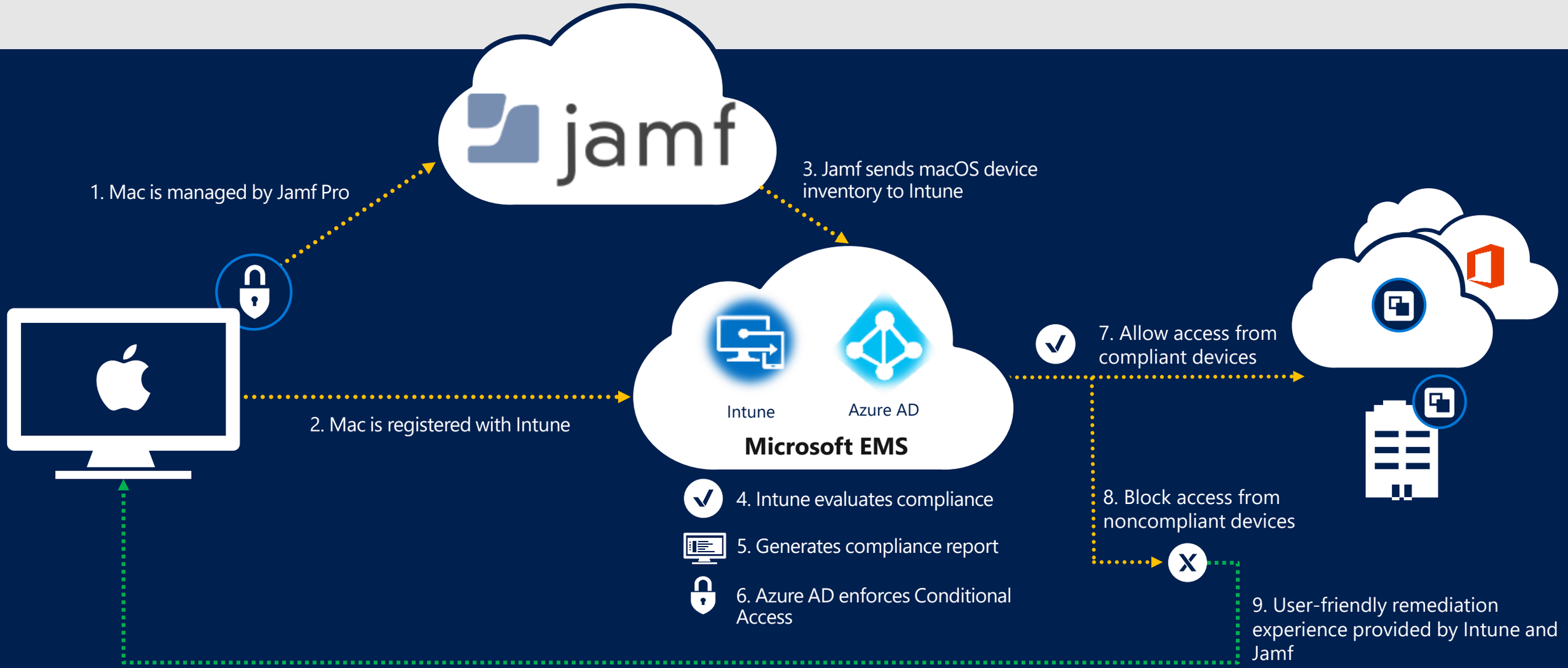
Jamf managed, Intune compliant

Advanced MDM management. Ideal for:

- Extensive inventory
- Depth of security controls
- Self Service app catalog & End user controls
- Limiting access to compliant Macs
- Scripting

EMS + Jamf

Intune device compliance for Jamf managed Macs



Demo

- Jamf Pro + Intune end user experience
- IT Pro: macOS management in Intune


QuickTime Player
File
Edit
View
Window
Help
Nicole
Company Portal

Intune’s role in Microsoft 365

Microsoft 365

Unlocks creativity

Built for teamwork

Integrated for simplicity

Intelligent security

Modernizing Windows 10 management

Modern management

Multiple Devices

User and Business Owned

Cloud Managed & SaaS Apps

Automated

Proactive

Self-Service

Better end user experience

Simpler management

More secure

Lower TCO

Paths to modern management

Cloud-first

A new organization starting with modern workplace

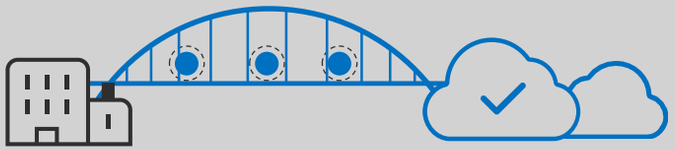
Big switch transition

Many workloads need to be modernized at the same time

Group by group transition

Doesn't address the needs of the full organization

Iterative (co-management)



Iteratively move workloads to modern

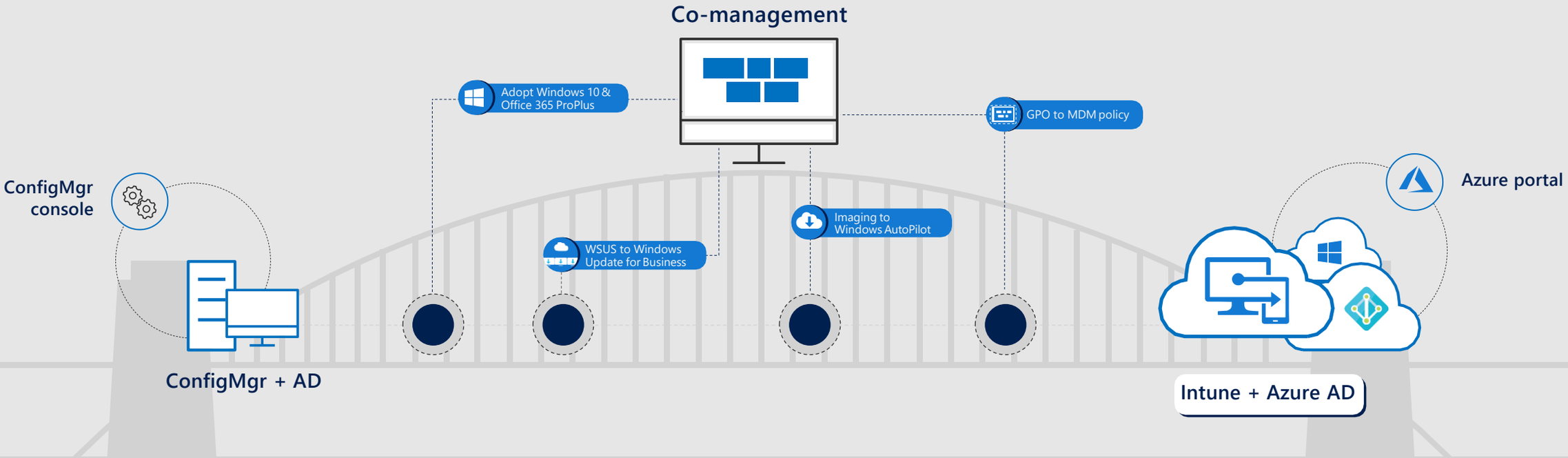
Start a practical move to modern Windows 10 management with EMS

With co-management, transition to modern management in a controlled, iterative way

Manage Windows 10 devices with ConfigMgr and Intune at the same time

Gradually move specific workloads to Intune in small, manageable steps

Transitioning from traditional to modern management is a simple experience for IT Pros and nondisruptive for end users



Benefits of co-management

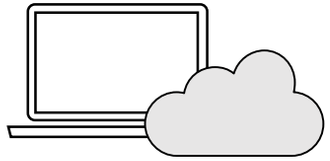
- A practical way to migrate over time
- Minimized risk during transition
- An integrated solution; simple to implement
- Nondisruptive for end users

Mobile Application Management (APP)

What does APP do for customers?

- Helps honest users from mistakenly leaking **corporate data**
- Provides both mobile **app configuration** and **management**
- **Enforce** use of **Managed Browser**
- **Checks** device **health** and **compliance**
- Works with 3rd **party MDM** and **without enrolment**

Mobile app management recap



Windows AutoPilot leads the way

To modern management

To the cloud

To Microsoft 365:

- Windows 10 Enterprise
- Office 365 ProPlus
- EMS

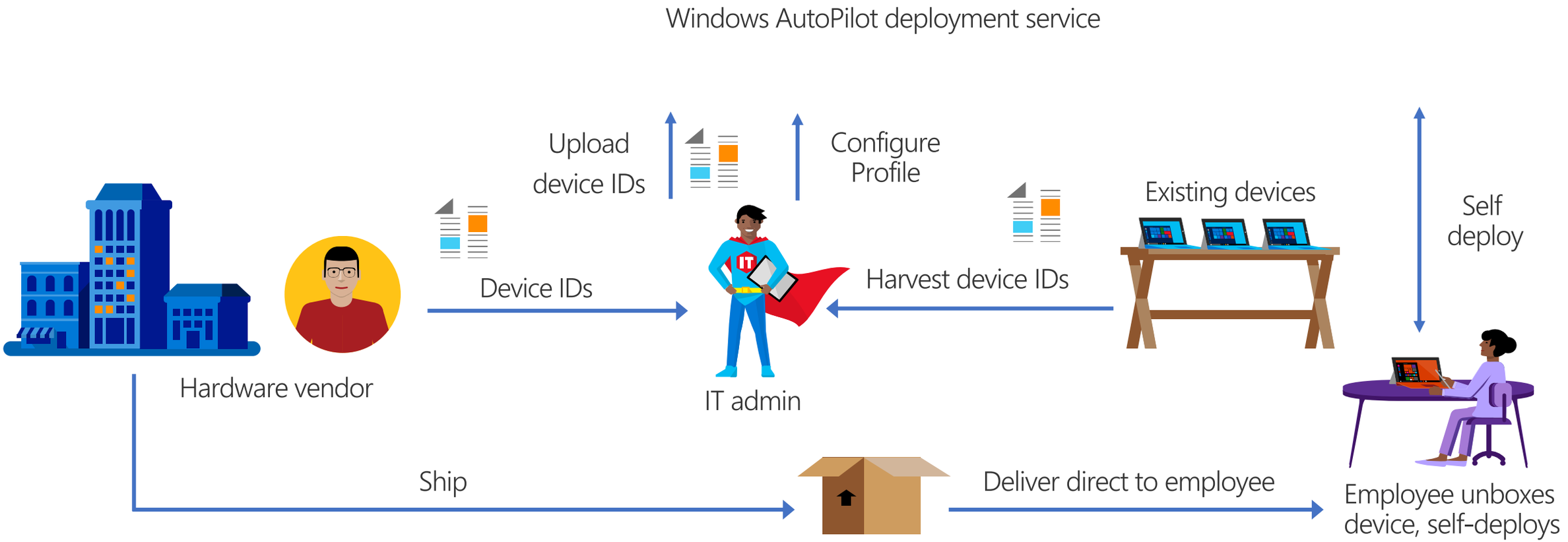
Simple for users and IT

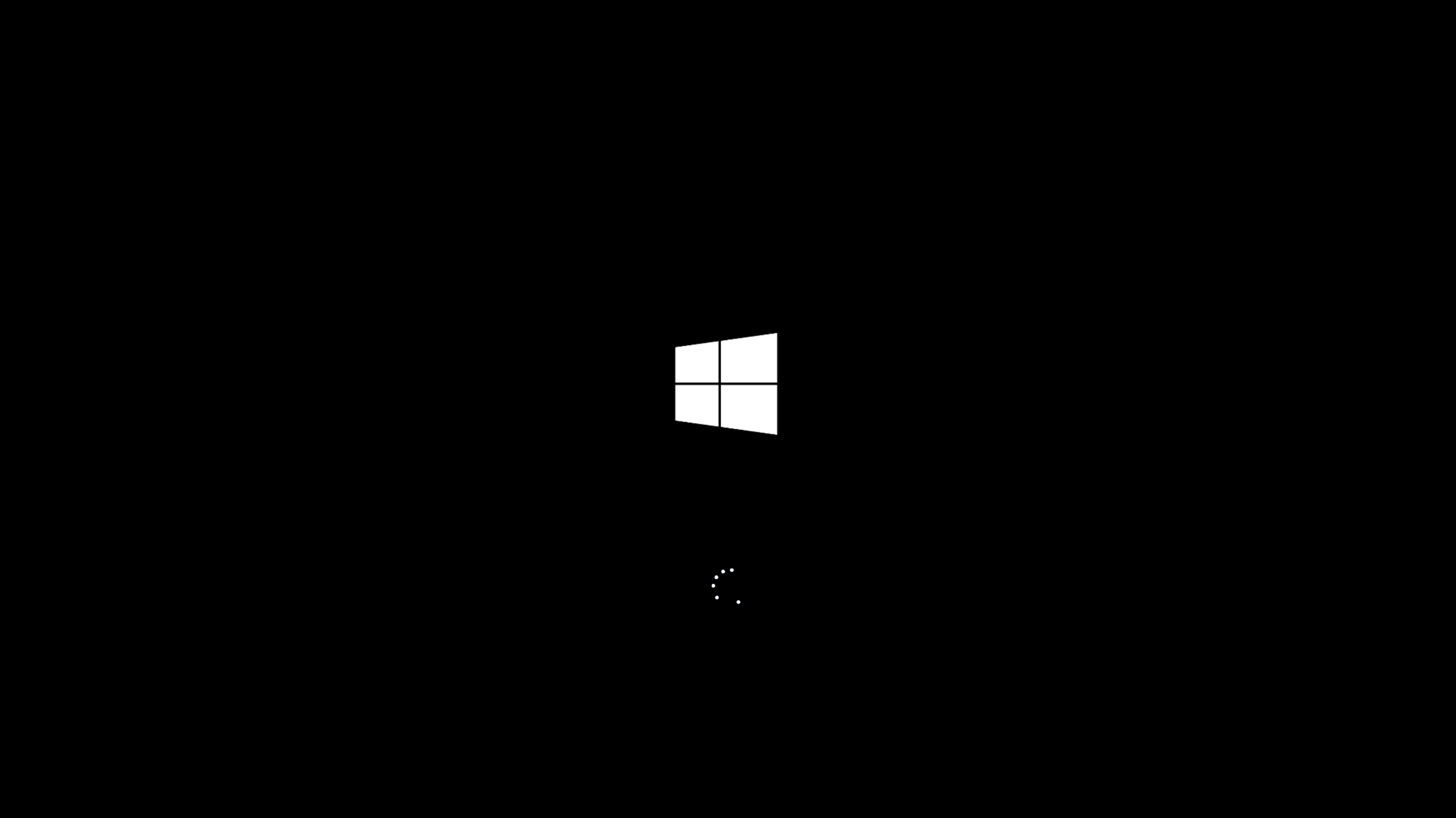
No more images

Lower TCO

Better experience

Introducing Windows AutoPilot





Now we can go look for any updates...

Alright, you're connected. Now we can go look for any updates...

Network

Welcome to Contoso!
Let’s get you set up for work…

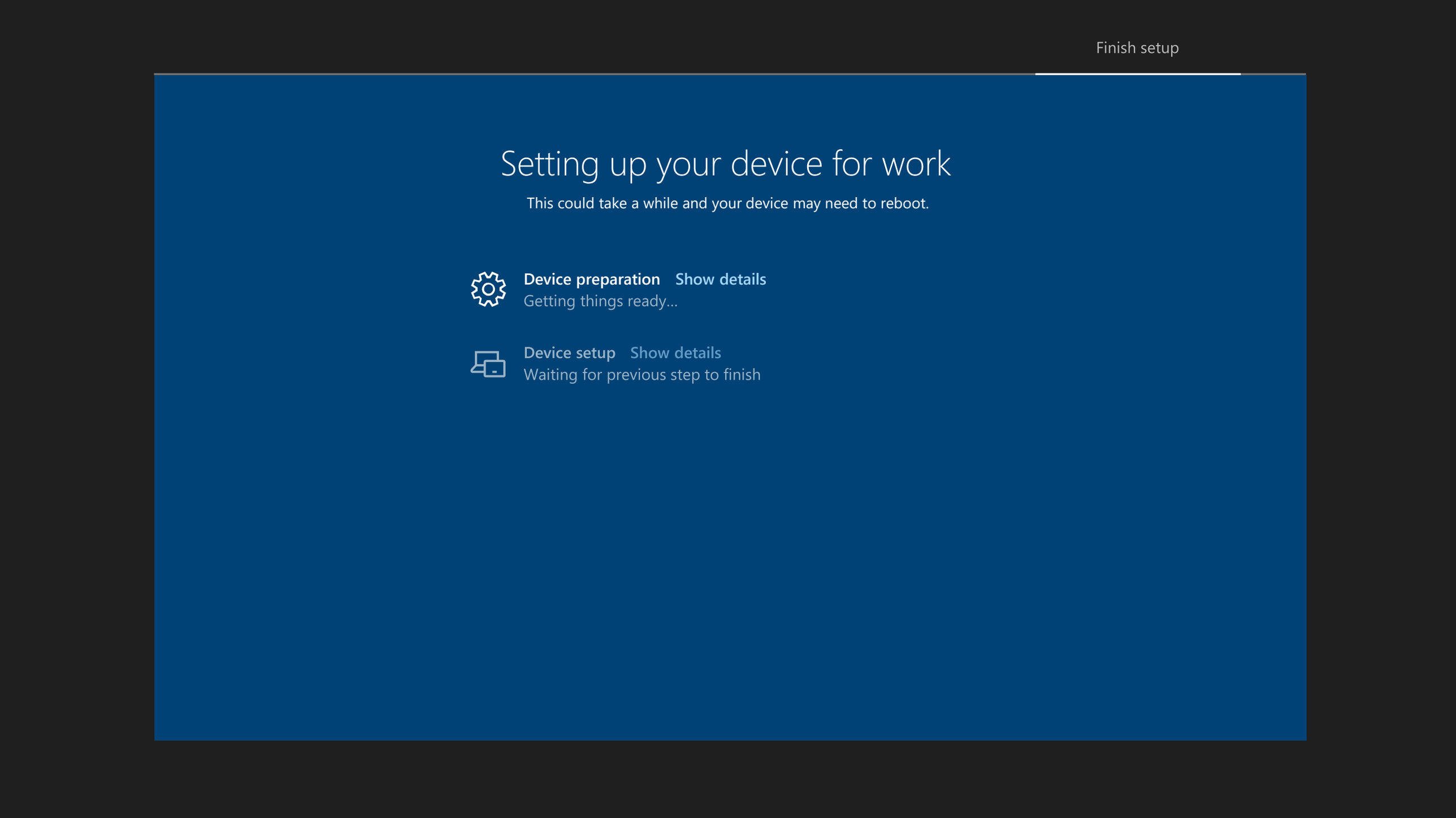
Account

Welcome to Contoso! We'll take it from here.

Getting you set up for work may take a while, but leave everything to us.
Please don't turn off this device.

Not a Contoso device?

Next


Finish setup
Setting up your device for work
This could take a while and your device may need to reboot.
Device preparation
Show details
Getting things ready...
Device setup
Show details
Waiting for previous step to finish

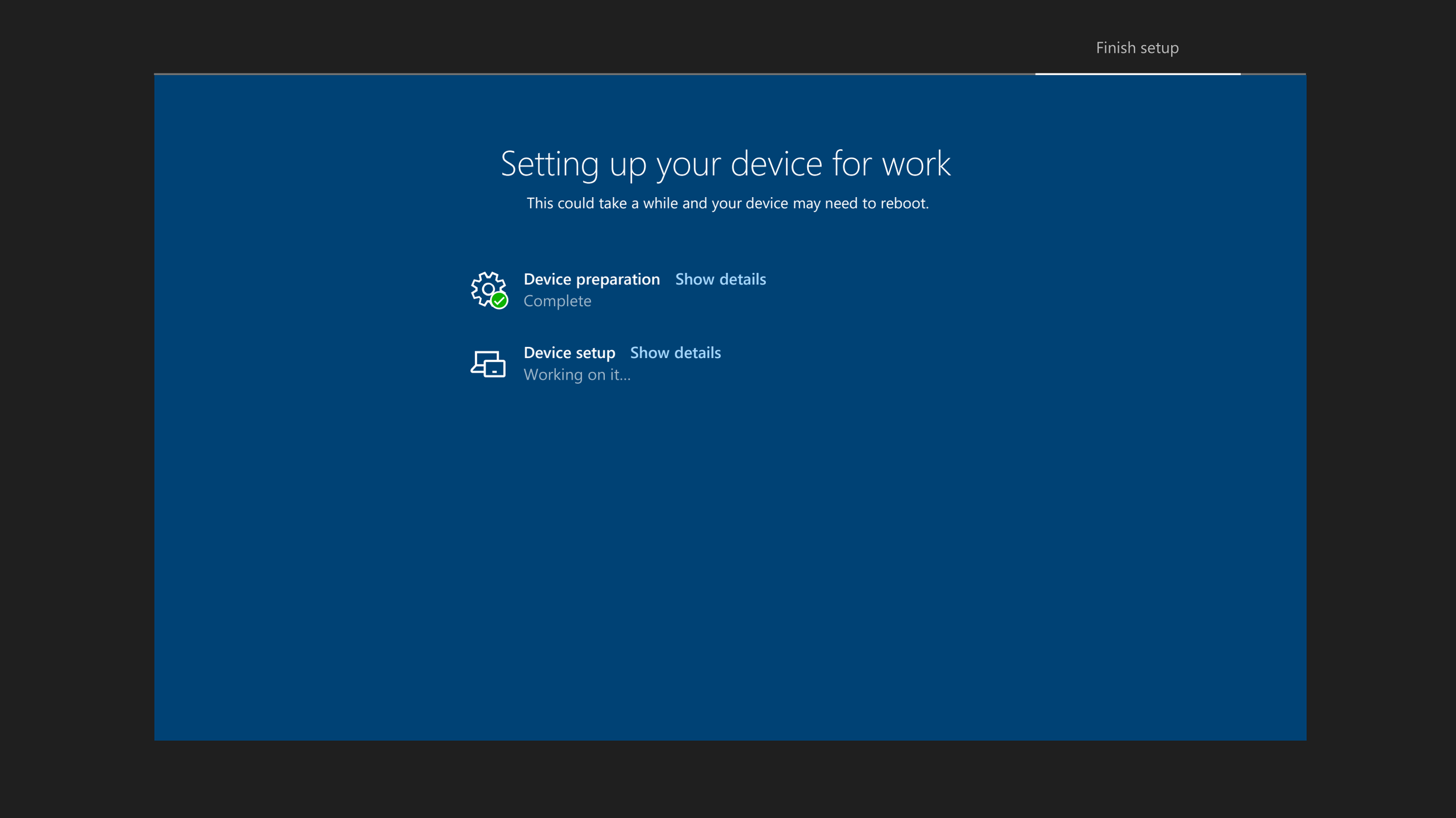
Finish setup

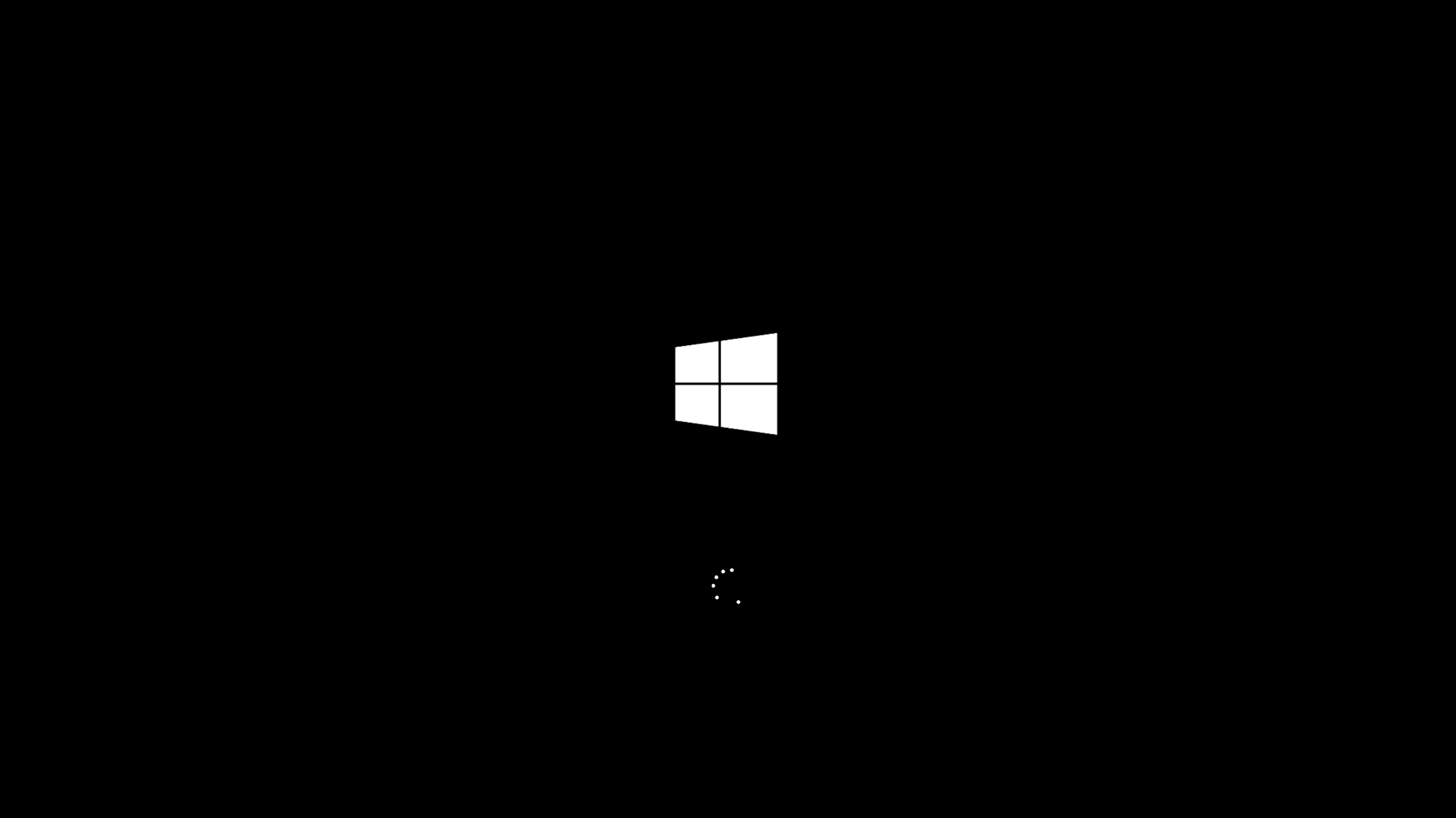
Setting up your device for work

This could take a while and your device may need to reboot.

Device preparation Show details
Complete

Device setup Show details
Getting things ready...


Finish setup
Setting up your device for work
This could take a while and your device may need to reboot.
Device preparation
Show details
Complete
Device setup
Show details
Working on it...



Finish setup

Setting up your device for work

This could take a while and your device may need to reboot.

Device preparation Show details
Complete

Device setup Show details
Still working on it...

Finish setup

Setting up your device for work

This could take a while and your device may need to reboot.

Device preparation Show details
Complete

Device setup Show details
Complete

We’re getting everything ready for you

Don’t turn off your PC

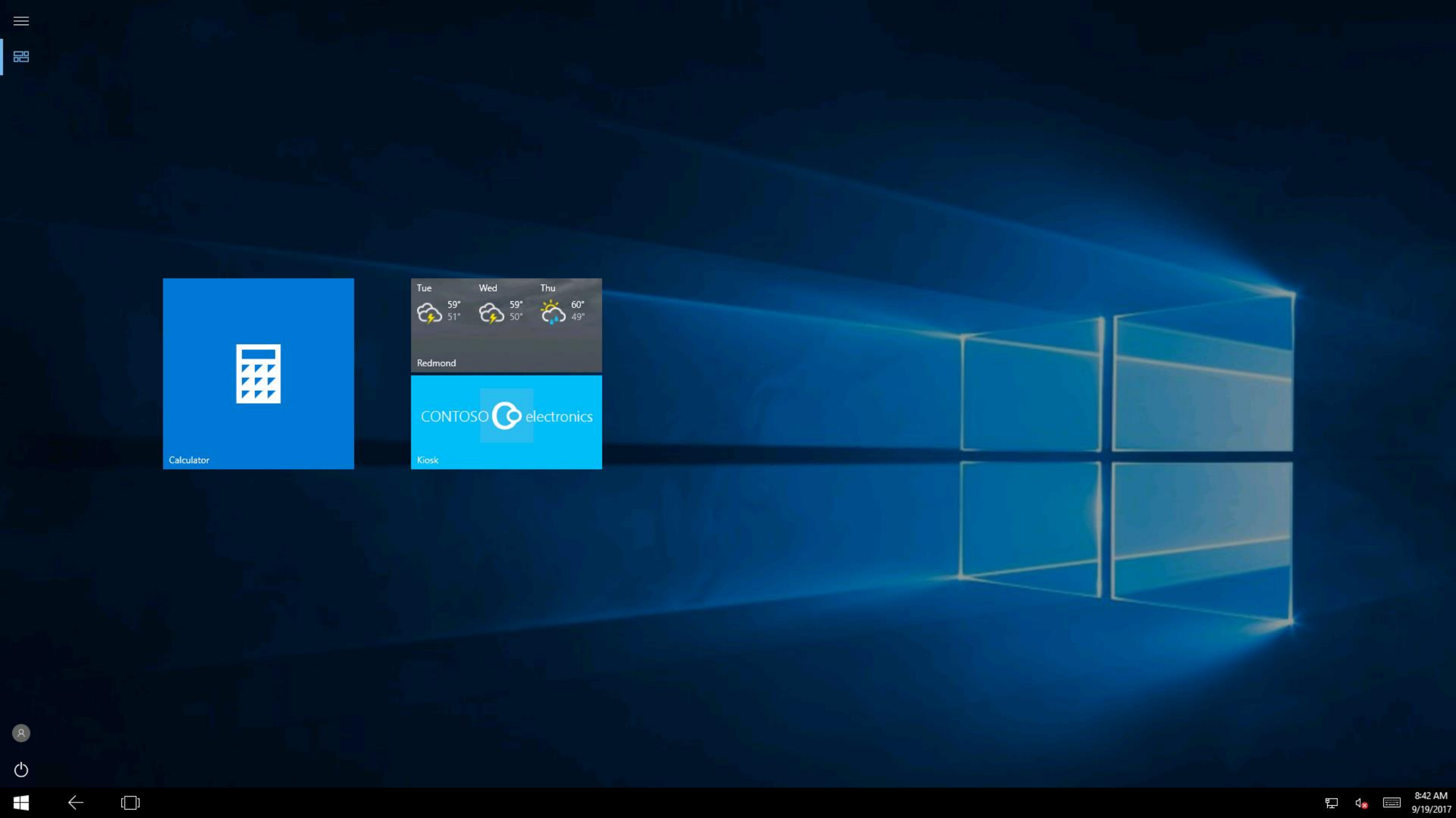
This will just take a moment

Don’t turn off your PC

Leave everything to us

Don’t turn off your PC

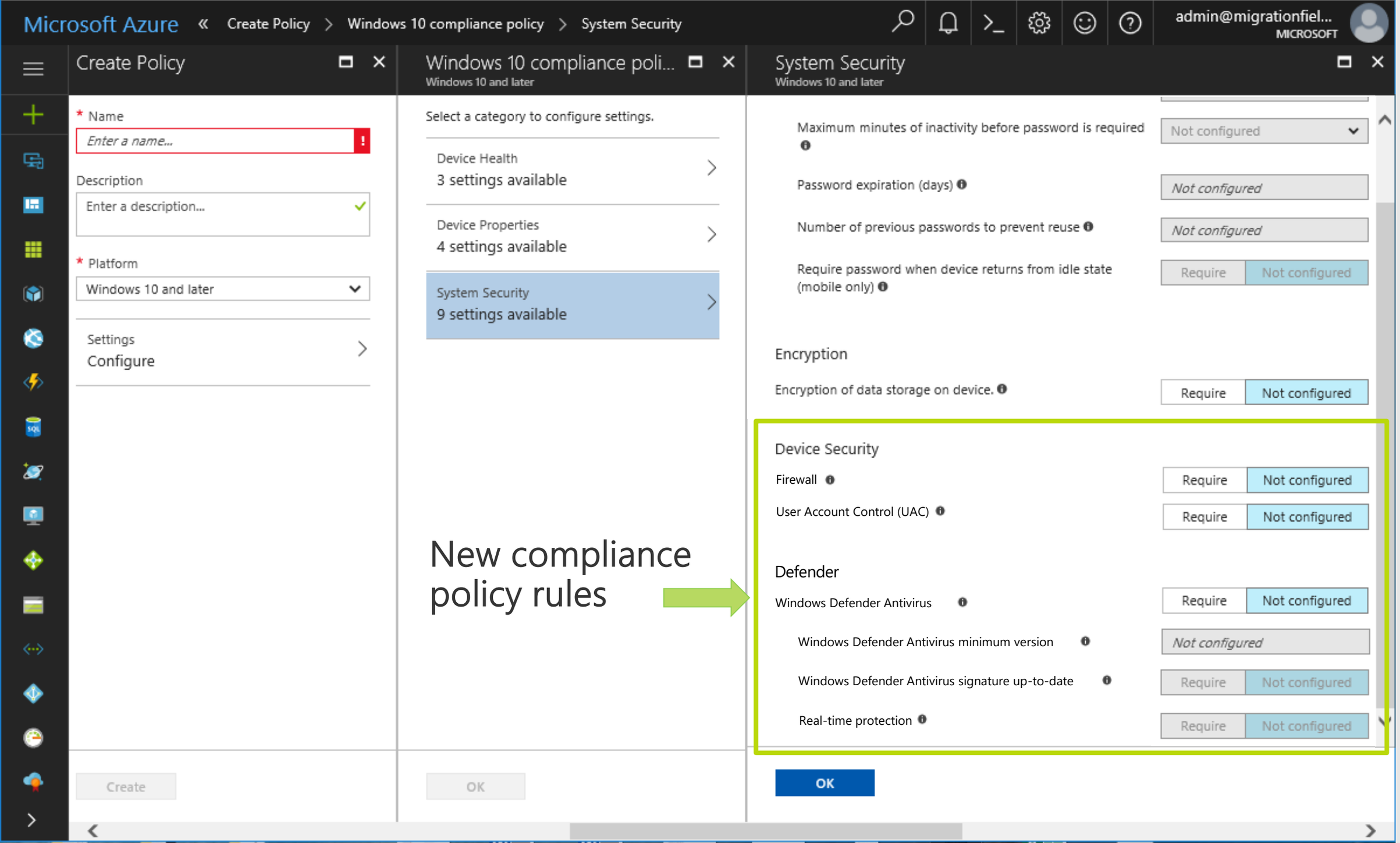
Almost there


Calculator
Tue
59°
51°
Wed
59°
50°
Thu
60°
49°
Redmond
CONTOSO electronics
Kiosk
8:42 AM
9/19/2017

Demo

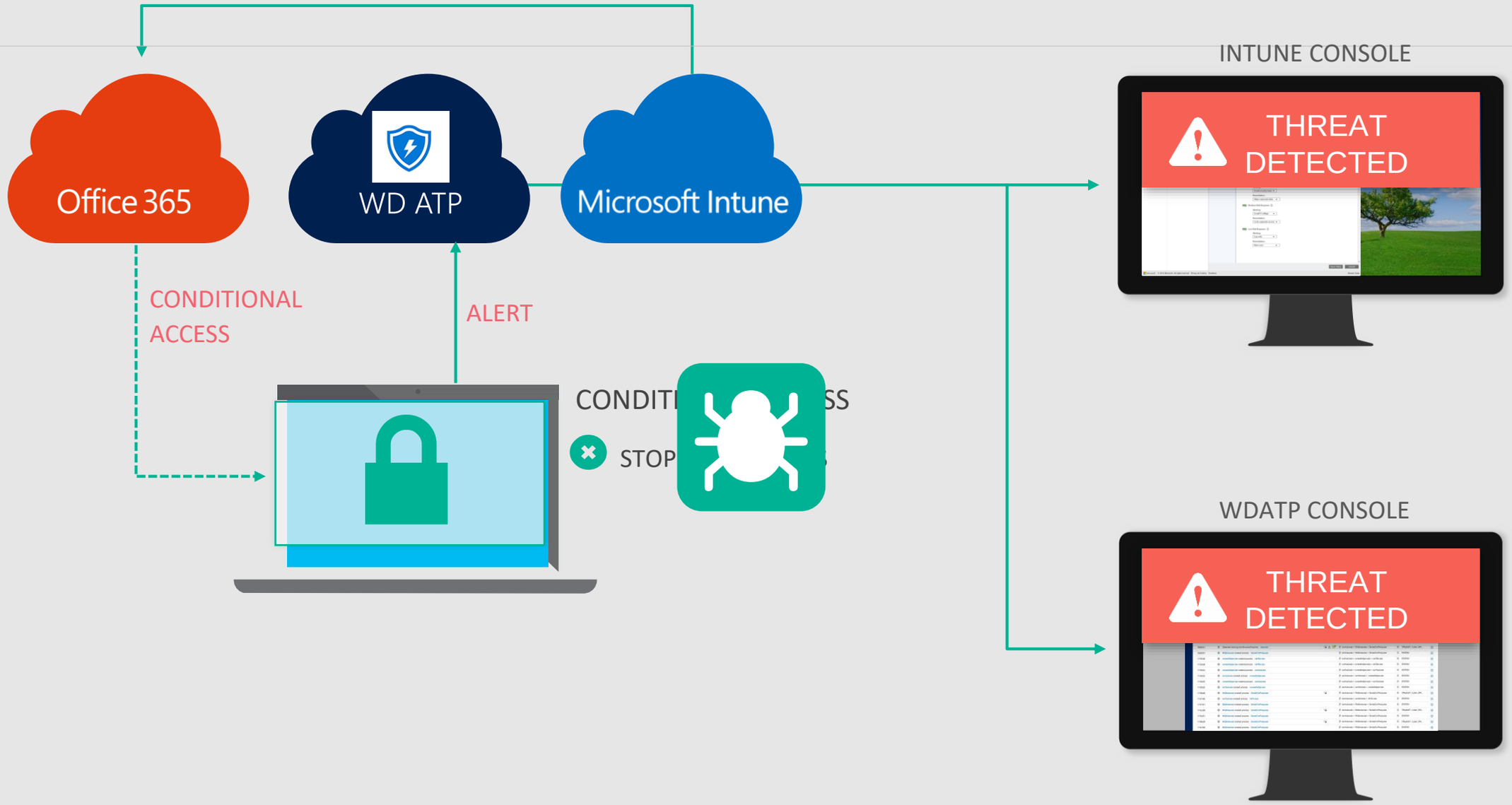
Demo – Securing Win10 devices with Intune

What's new in Win10 Conditional access

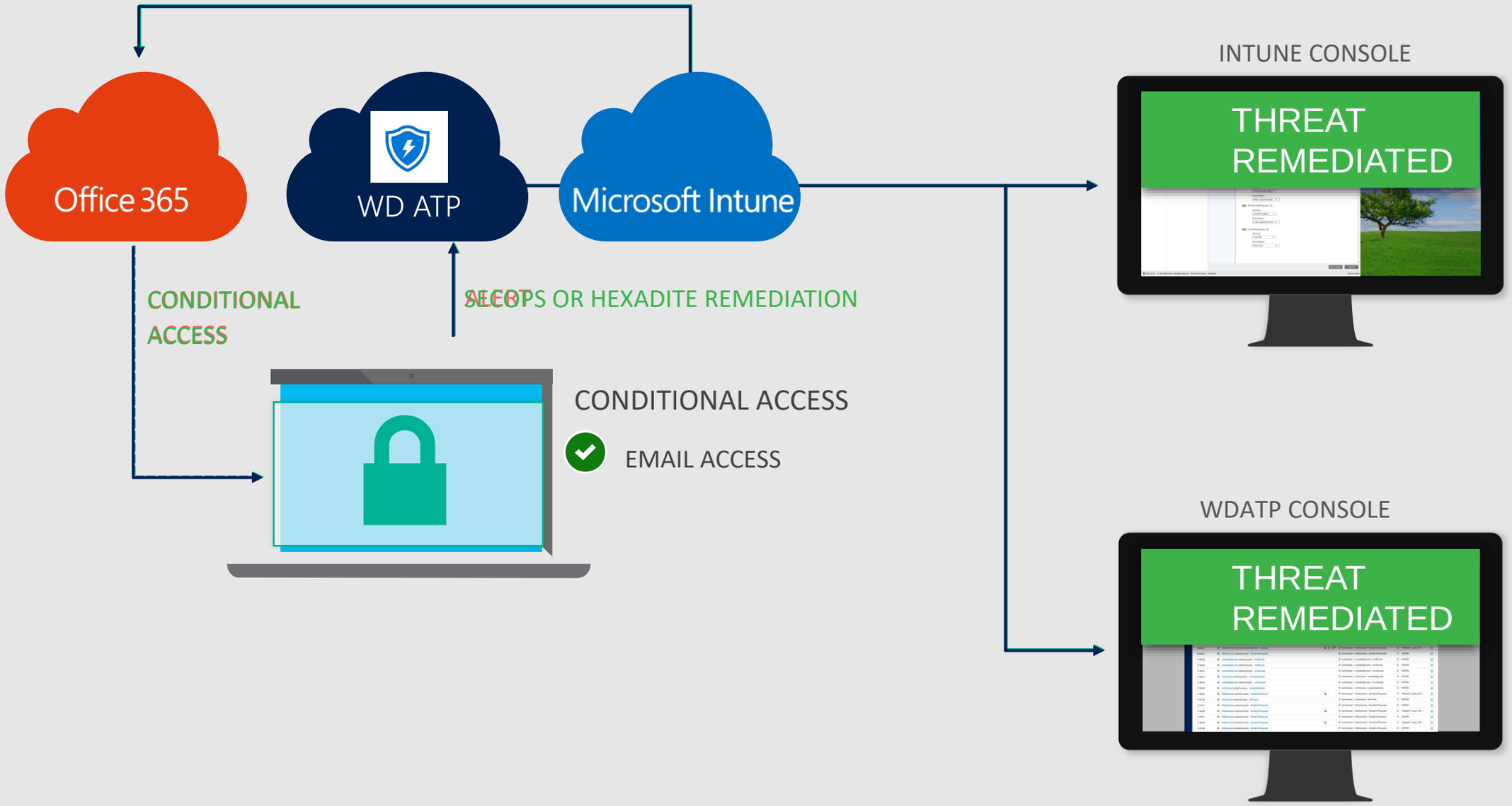

Microsoft Azure
Create Policy
Windows 10 compliance policy
System Security
admin@migrationfiel...
MICROSOFT
Create Policy
* Name
Enter a name...
Description
Enter a description...
* Platform
Windows 10 and later
Settings
Configure
Create
Windows 10 compliance poli...
Windows 10 and later
Select a category to configure settings.
Device Health
3 settings available
Device Properties
4 settings available
System Security
9 settings available
OK
System Security
Windows 10 and later
Maximum minutes of inactivity before password is required
Not configured
Password expiration (days)
Not configured
Number of previous passwords to prevent reuse
Not configured
Require password when device returns from idle state (mobile only)
Require
Not configured
Encryption
Encryption of data storage on device.
Require
Not configured
Device Security
Firewall
Require
Not configured
User Account Control (UAC)
Require
Not configured
Defender
Windows Defender Antivirus
Require
Not configured
Windows Defender Antivirus minimum version
Not configured
Windows Defender Antivirus signature up-to-date
Require
Not configured
Real-time protection
Require
Not configured
OK
New compliance policy rules

New Scenario:
Conditional Access based on Device Risk signals from Defender ATP

Goal: Ensure only trusted and secure Win10 devices have access to corporate data.



Goal: Ensure only trusted and secure Win10 devices have access to corporate data.



Risk reflection in WDATP

Machines list

Data period: 30 days | Tags: All | Risk level: All | Malware category alerts: All | Health: All | Group: All | OS platform: All | Tags: All | Export

Machine name	Tags	Risk level	Active alerts	Health	Group	Domain	OS platform	Internal IP	Last seen
sthunte-pc		High	14	Impaired communication, ...	Machine's group	redmond.corp.microsoft.com	Windows 10	192.168.1.4	12.22.2017
sqrrl		High	11	No sensor data	Machine's group	europe.corp.microsoft.com	Windows 10	10.190.99.45	12.24.2017
minint-dywndh		Medium	10	Active	Machine's group	AAD joined	Windows 10	10.80.170.12	12.22.2017
dakapl-devsec1		Low	9	Inactive	Machine's group	NTDEV.corp.microsoft.com	Windows 10	10.170.88.197	10.07.2017
amrmpfe-pc		Low	6	Requires attention	Machine's group	redmond.corp.microsoft.com	Windows 10	192.168.8.100	12.22.2017
johndoe-lap		No risk found	0	Impaired communication	Machine's group	redmond.corp.microsoft.com	Windows 10	10.190.99.45	12.23.2017

sthunte-pc

sthunte-pc

Actions

Domain: redmond.corp.microsoft.com
OS: Windows10 64-bit (Build 16299)
Group: #Machine group#
Tags: Tag-1 Tag-1 Tag-1
Machine IP addresses
Investigation package collection is available 12/24/17 | 08:32

Logged on users (last 30 days)

3 see all users

Most frequent: Stas Hunter (Local admin)
Least frequent: Gregg Mensch (standard user)

Machine risk - High

Active alerts:

6	4	4	0
High	Medium	Low	Informational

2 Azure ATP Alerts

Machine health - Misconfigured

Impaired communication, No sensor data

First seen: 6 months ago
Last seen: 16 days ago

600/1000 Windows secure score
Machine security state requires attention

Alerts related to this machine

1-8 of 31

Last activity	Title	User	Severity	Status	Investigation State	Assigned to
12.22.2017 | 18:59:06	Windows Defender AV detected active 'Bluether' high-severity malware Malware		High	New	Disabled	Not assigned
12.22.2017 | 18:33:43	Windows Defender AV detected 'Bluether' high-severity malware Malware	europe\sthunte	High	New	Disabled	Not assigned
12.22.2017 | 18:16:10	Windows Defender AV detected an active 'CVE-2017-11882' exploit malware Exploit		Medium	New	Disabled	Not assigned
12.22.2017 | 18:05:23	Windows Defender AV detected 'CVE-2017-11882' exploit malware Exploit	europe\sthunte	Low	New	Disabled	Not assigned
12.22.2017 | 16:54:55	Windows Defender AV detected 'ShellCode' exploit malware Exploit	europe\sthunte	Low	New	Disabled	Not assigned
12.22.2017 | 16:28:42	Windows Defender AV detected an active 'CVE-2017-11826' exploit malware Exploit		Medium	New	Benign	Not assigned
12.22.2017 | 16:28:42	Malicious document detected Exploit		High	New	Disabled	Not assigned
12.22.2017 | 16:23:44	FinFisher Detected Backdoor		High	New	Disabled	Not assigned

Machine timeline

Value: Search in machine timeline
Information level: All
Event type: All
User account: All
Remove all filters

12.22.2017 | 19:24

Jul 2017 Aug 2017 Sep 2017 Oct 2017 Nov 2017 Dec 2017 Today

Define compliance policy

New
Dashboard
Intune
Azure Active Directory
Azure AD Identity Protect...
All resources
Resource groups
App Services
SQL databases
SQL data warehouses
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
More services

Microsoft Intune

Search (Ctrl+/)
Overview
Quick start
MANAGE
Device enrollment
Device compliance
Device configuration
Devices
Mobile apps
eBooks
Conditional access
On-premises access
Users
Groups
Intune roles
Software updates
HELP AND SUPPORT
Help and support
Troubleshoot

Device compliance - Policies

Microsoft Intune

Search (Ctrl+/)
Overview
MANAGE
Policies
Notifications
MONITOR
Device compliance
Devices without compliance pol...
Setting compliance
Policy compliance
SETUP
Compliance policy settings
Mobile Threat Defense
HELP AND SUPPORT
Help and support

Create Policy | Columns | Filter | Refresh | Export

Search by name

POLICY NAME	PLATFORM	POLICY TYPE	ASSIGNED	LAST MODIFIED
Android 5+ MTD Medium	Android	Android compliance policy	No	5/16/17, 2:13 AM
Android Compliance Policy	Android	Android compliance policy	No	4/06/17, 4:38 PM
Android Compliance Policy	Android	Android compliance policy	No	3/31/17, 5:24 AM
Block Jailbroken Android	Android	Android compliance policy	Yes	3/31/17, 5:14 AM
Block Jailbroken iOS	iOS	iOS compliance policy	No	1/20/17, 7:31 AM
CDAC compliance	Windows 10 a...	Windows 10 compliance poli...	No	6/15/17, 8:43 AM
Demo	iOS	iOS compliance policy	No	7/17/17, 7:26 AM
Device Compliance - Graph	iOS	iOS compliance policy	No	4/04/17, 9:41 PM
iOS Compliance - Becky	iOS	iOS compliance policy	Yes	7/28/17, 10:52 AM
iOS Compliance - Conrad	iOS	iOS compliance policy	Yes	6/05/17, 2:55 PM
iOS Compliance Policy	iOS	iOS compliance policy	No	4/06/17, 4:38 PM
iOS Compliance Policy	iOS	iOS compliance policy	No	3/31/17, 5:24 AM
iOS trusted device	iOS	iOS compliance policy	No	6/29/17, 2:21 PM
MTD Android (heenamac)	Android	Android compliance policy	Yes	7/21/17, 11:52 AM
MTD iOS demo (heenamac)	iOS	iOS compliance policy	Yes	7/21/17, 9:54 AM
no jail broken	Android	Android compliance policy	No	7/27/17, 2:46 PM
no jail broken android	Android	Android compliance policy	No	7/27/17, 2:37 PM
no jailbroken	Android	Android compliance policy	No	7/27/17, 2:11 PM
no rooted	Android	Android compliance policy	No	7/27/17, 1:53 PM
No Rooted Devices	Android	Android compliance policy	No	7/27/17, 1:02 PM
Require compliant PIN	iOS	iOS compliance policy	Yes	6/14/17, 8:10 PM
Security baselines	iOS	iOS compliance policy	No	7/17/17, 9:38 AM
Security demo	iOS	iOS compliance policy	No	7/17/17, 2:05 PM
Simmay Require corporate email profile	iOS	iOS compliance policy	Yes	11/01/17, 2:03 PM
test	iOS	iOS compliance policy	No	6/29/17, 1:35 PM

New
Dashboard
Intune
Azure Active Directory
Azure AD Identity Protect...
All resources
Resource groups
App Services
SQL databases
SQL data warehouses
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
More services >

Create Policy

* Name

Enter a name...

Description

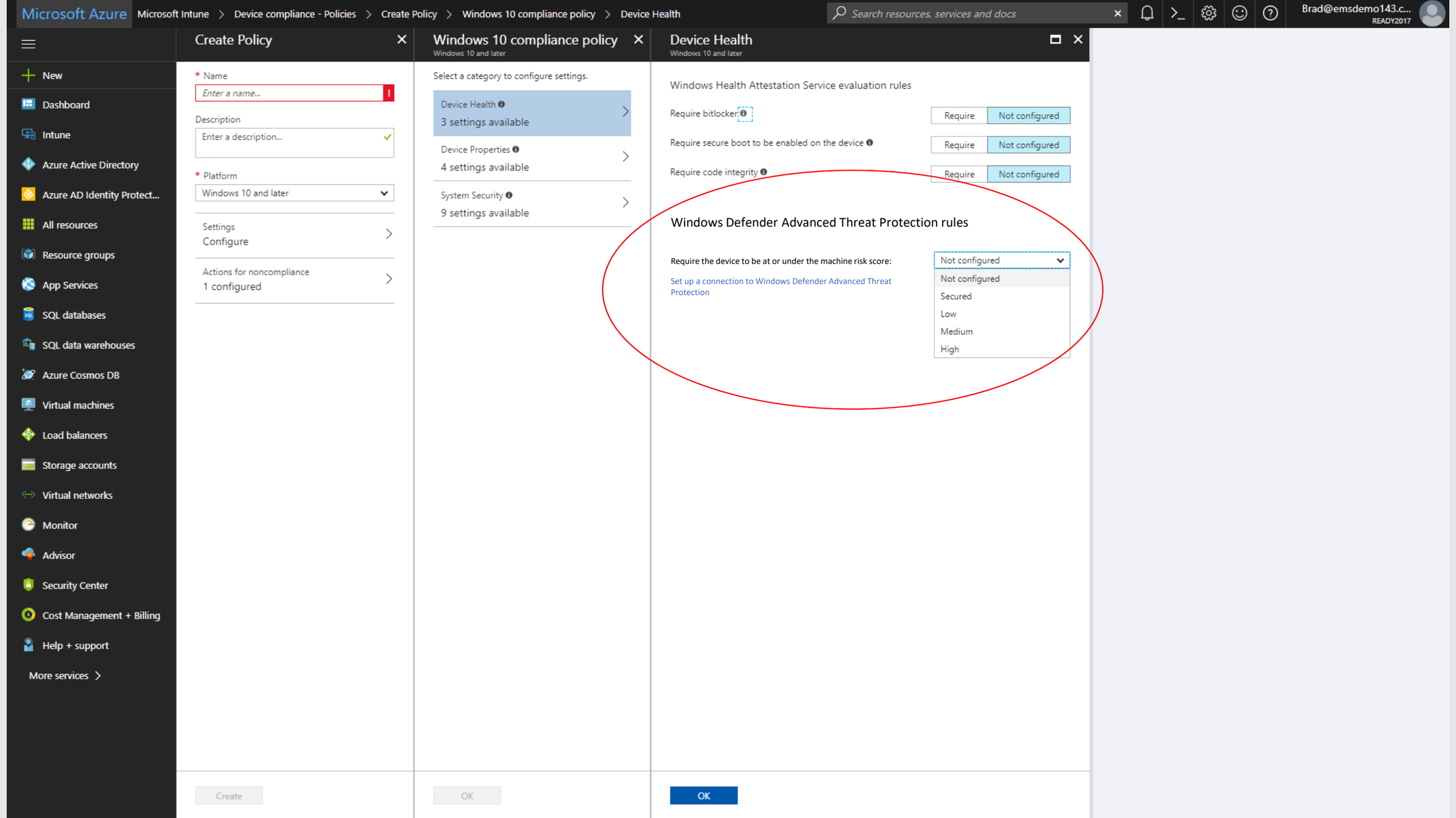
Enter a description...

* Platform

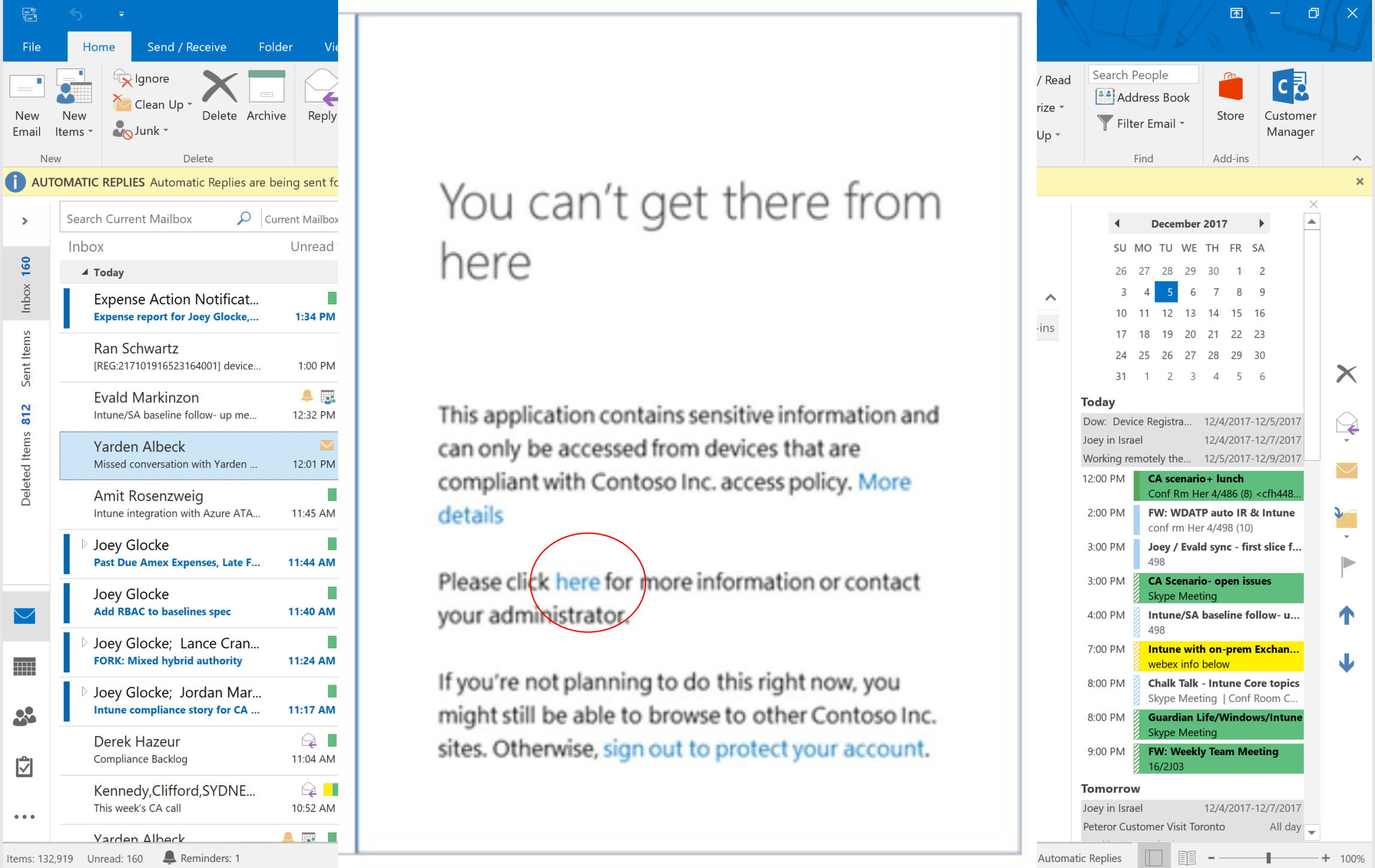
Windows 10 and later

Select a platform
Android
Android for Work
iOS
macOS
Windows Phone 8.1
Windows 8.1 and later
Windows 10 and later

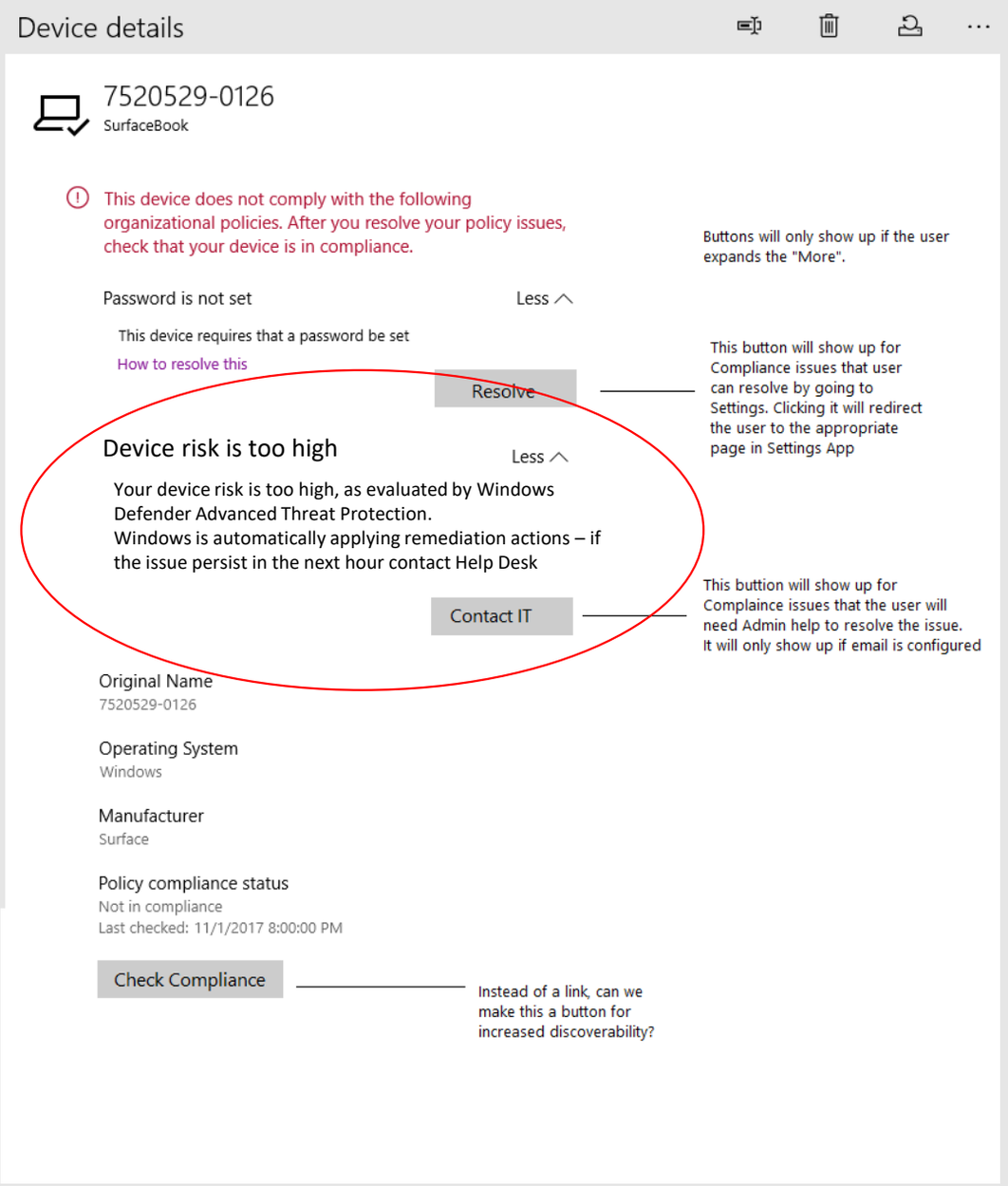
Create


Microsoft Azure
Microsoft Intune > Device compliance - Policies > Create Policy > Windows 10 compliance policy > Device Health
Search resources, services and docs
Brad@emsdemo143.c...
READY2017
New
Dashboard
Intune
Azure Active Directory
Azure AD Identity Protect...
All resources
Resource groups
App Services
SQL databases
SQL data warehouses
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
More services
Create Policy
* Name
Enter a name...
Description
Enter a description...
* Platform
Windows 10 and later
Settings
Configure
Actions for noncompliance
1 configured
Create
Windows 10 compliance policy
Windows 10 and later
Select a category to configure settings.
Device Health
3 settings available
Device Properties
4 settings available
System Security
9 settings available
OK
Device Health
Windows 10 and later
Windows Health Attestation Service evaluation rules
Require bitlocker
Require secure boot to be enabled on the device
Require code integrity
Require
Not configured
Windows Defender Advanced Threat Protection rules
Require the device to be at or under the machine risk score:
Not configured
Secured
Low
Medium
High
Set up a connection to Windows Defender Advanced Threat Protection
OK

End user experience


File
Home
Send / Receive
Folder
New Email
New Items
Ignore
Clean Up
Junk
Delete
Archive
Reply
New
Delete
AUTOMATIC REPLIES Automatic Replies are being sent fc
Search Current Mailbox
Current Mailbox
Inbox
Unread
Inbox 160
Sent Items
Deleted Items 812
Today
Expense Action Notificat...
Expense report for Joey Glocke,...
1:34 PM
Ran Schwartz
[REG:217101916523164001] device...
1:00 PM
Evald Markinzon
Intune/SA baseline follow- up me...
12:32 PM
Yarden Albeck
Missed conversation with Yarden ...
12:01 PM
Amit Rosenzweig
Intune integration with Azure ATA...
11:45 AM
Joey Glocke
Past Due Amex Expenses, Late F...
11:44 AM
Joey Glocke
Add RBAC to baselines spec
11:40 AM
Joey Glocke; Lance Cran...
FORK: Mixed hybrid authority
11:24 AM
Joey Glocke; Jordan Mar...
Intune compliance story for CA ...
11:17 AM
Derek Hazeur
Compliance Backlog
11:04 AM
Kennedy,Clifford,SYDNE...
This week's CA call
10:52 AM
Items: 132,919
Unread: 160
Reminders: 1
You can't get there from here
This application contains sensitive information and can only be accessed from devices that are compliant with Contoso Inc. access policy. More details
Please click here for more information or contact your administrator.
If you're not planning to do this right now, you might still be able to browse to other Contoso Inc. sites. Otherwise, sign out to protect your account.
Search People
Address Book
Filter Email
Store
Customer Manager
Find
Add-ins
December 2017
SU MO TU WE TH FR SA
Today
Dow: Device Registra... 12/4/2017-12/5/2017
Joey in Israel 12/4/2017-12/7/2017
Working remotely the... 12/5/2017-12/9/2017
12:00 PM CA scenario+ lunch
Conf Rm Her 4/486 (8) <cfh448...
2:00 PM FW: WDATP auto IR & Intune
conf rm Her 4/498 (10)
3:00 PM Joey / Evald sync - first slice f...
498
3:00 PM CA Scenario- open issues
Skype Meeting
4:00 PM Intune/SA baseline follow- u...
498
7:00 PM Intune with on-prem Exchan...
webex info below
8:00 PM Chalk Talk - Intune Core topics
Skype Meeting | Conf Room C...
8:00 PM Guardian Life/Windows/Intune
Skype Meeting
9:00 PM FW: Weekly Team Meeting
16/2J03
Tomorrow
Joey in Israel 12/4/2017-12/7/2017
Peteror Customer Visit Toronto All day
Automatic Replies
100%

Company Portal Experience



Microsoft