Upravljanje naprav z Microsoft 365

Slavko Kukrika
MVP in prijazen fant

#ntk19

Agenda

- Traditional vs. Modern management
- What is Microsoft 365?
- Enrolling, configuring and managing devices
- Controlling access to cloud apps and data
- Managing apps and deploying new devices

Traditional PC management

On-premises

On-premises Active Directory environment

Access to company resources from internal network only

PCs are running Windows operating system

All PCs are domain joined

PCs are managed by Group Policy (and Configuration Manager)

Using Win32 apps that are installed locally on PCs

Modern device management

Azure Active Directory (that can be synced with on-premises AD DS)

Devices are running different OSes (Windows, Android, iOS)

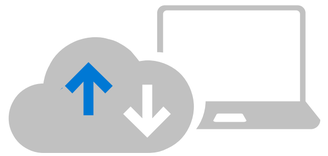
Many devices are not domain joined

Devices are managed by Mobile Device Management (MDM)

Accessing company resources from anywhere

- Conditional access policies control access to resources

Cloud apps, such as Office 365, are running from the cloud



Modern Workplace

Management powered by Microsoft 365 cloud

	On-premise (Traditional)	Cloud attached (Co-management)	Cloud managed (Modern)
Traditional OS Deployment	✓	✓	
Win32 app management	✓	✓	✓
Configuration and GPO	✓	✓	✓
Bitlocker Management	✓	✓	✓
Hardware and software inventory	✓	✓	✓
Update management	✓	✓	✓
Unified Endpoint Management – Windows, iOS, macOS, Android		✓	✓
Risk based access control – Compliance, Conditional Access		✓	✓
Autopilot provisioning – Autopilot, DEP, Zero Touch, KME		✓	✓
Advanced threat and security – Hello, Attestation, ATP, Secure Score		✓	✓
Telemetry driven policy – Security Baselines, Guided Deployments		✓	✓
Complete app management – Pro Plus, SaaS, Stores, CDN/D.O.		✓	✓
Integrated full stack M365 management – Analytics, Graph, RBAC, Audit		✓	✓

Microsoft 365

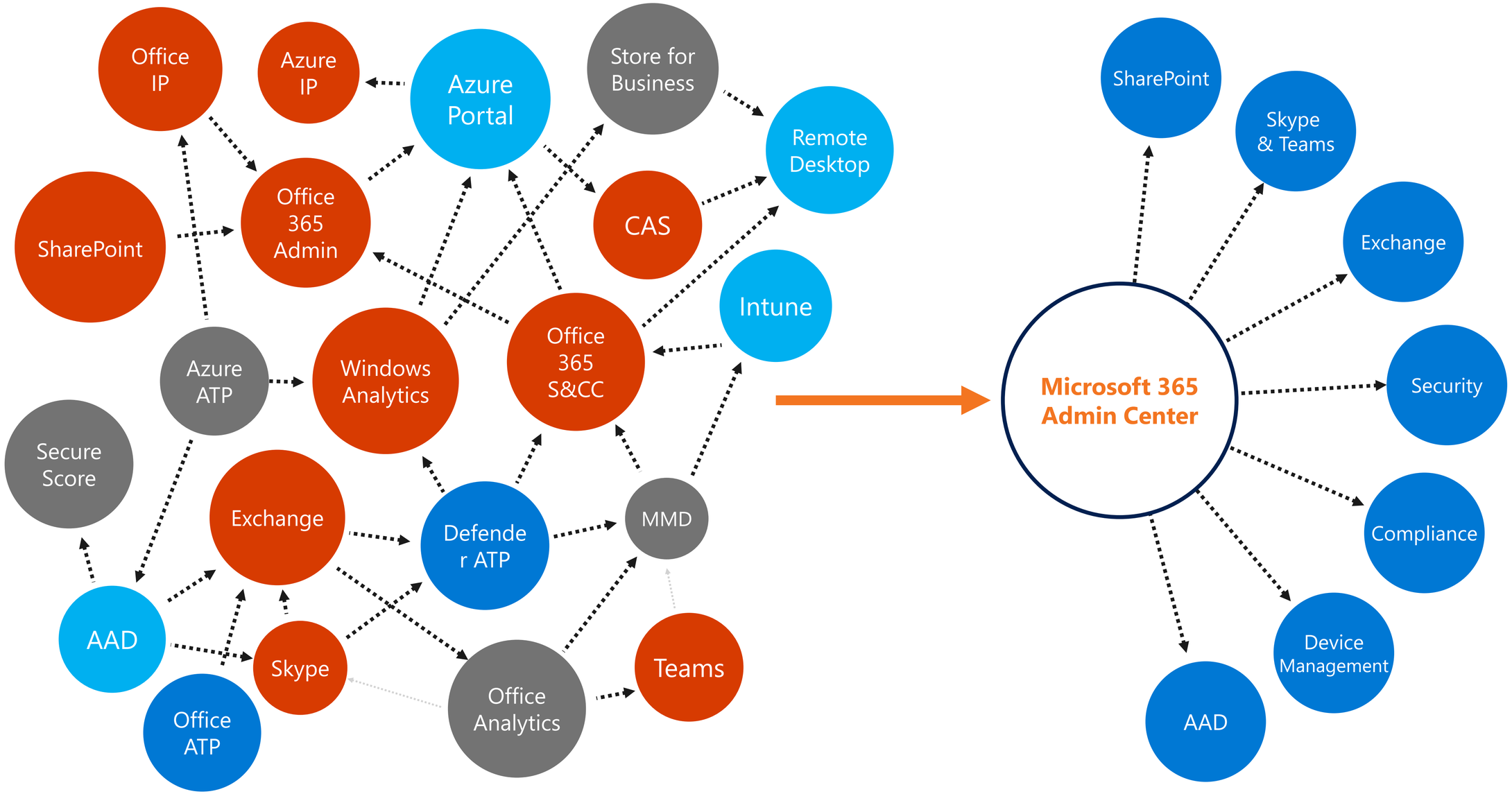
A complete, intelligent solution to empower employees to be creative and work together, securely.

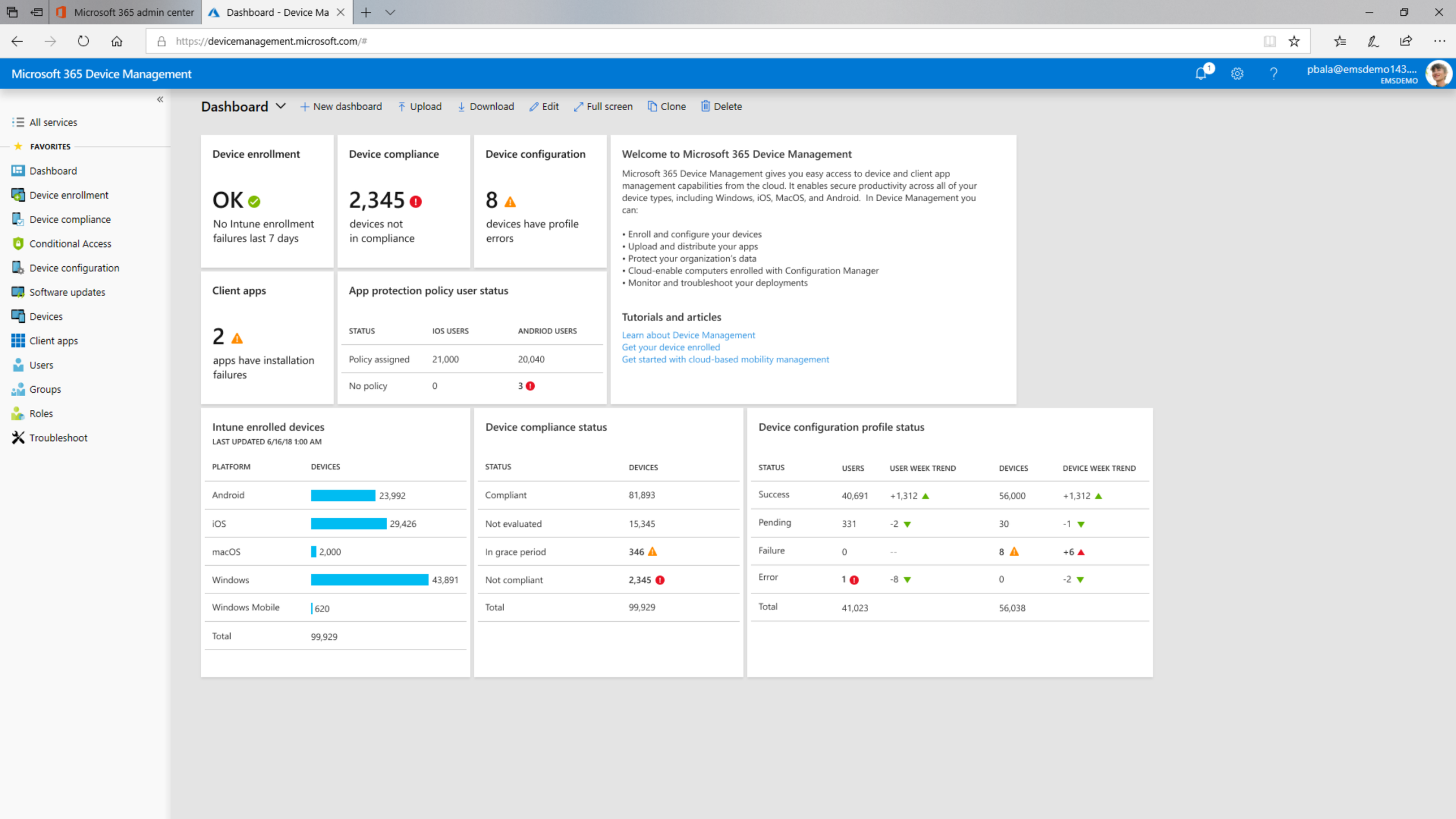
Office 365

Windows 10

Enterprise Mobility + Security

Microsoft 365 admin center




Microsoft 365 admin center
Dashboard - Device Ma
https://devicemanagement.microsoft.com/#
Microsoft 365 Device Management
pbala@emsdemo143....
EMSDEMO
All services
FAVORITES
Dashboard
Device enrollment
Device compliance
Conditional Access
Device configuration
Software updates
Devices
Client apps
Users
Groups
Roles
Troubleshoot
Dashboard
New dashboard
Upload
Download
Edit
Full screen
Clone
Delete
Device enrollment
OK
No Intune enrollment failures last 7 days
Device compliance
2,345
devices not in compliance
Device configuration
8
devices have profile errors
Welcome to Microsoft 365 Device Management
Microsoft 365 Device Management gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, MacOS, and Android. In Device Management you can:
• Enroll and configure your devices
• Upload and distribute your apps
• Protect your organization's data
• Cloud-enable computers enrolled with Configuration Manager
• Monitor and troubleshoot your deployments
Tutorials and articles
Learn about Device Management
Get your device enrolled
Get started with cloud-based mobility management
Client apps
2
apps have installation failures
App protection policy user status
STATUS
IOS USERS
ANDRIOD USERS
Policy assigned
21,000
20,040
No policy
0
3
Intune enrolled devices
LAST UPDATED 6/16/18 1:00 AM
PLATFORM
DEVICES
Android
23,992
iOS
29,426
macOS
2,000
Windows
43,891
Windows Mobile
620
Total
99,929
Device compliance status
STATUS
DEVICES
Compliant
81,893
Not evaluated
15,345
In grace period
346
Not compliant
2,345
Total
99,929
Device configuration profile status
STATUS
USERS
USER WEEK TREND
DEVICES
DEVICE WEEK TREND
Success
40,691
+1,312
56,000
+1,312
Pending
331
-2
30
-1
Failure
0
--
8
+6
Error
1
-8
0
-2
Total
41,023
56,038

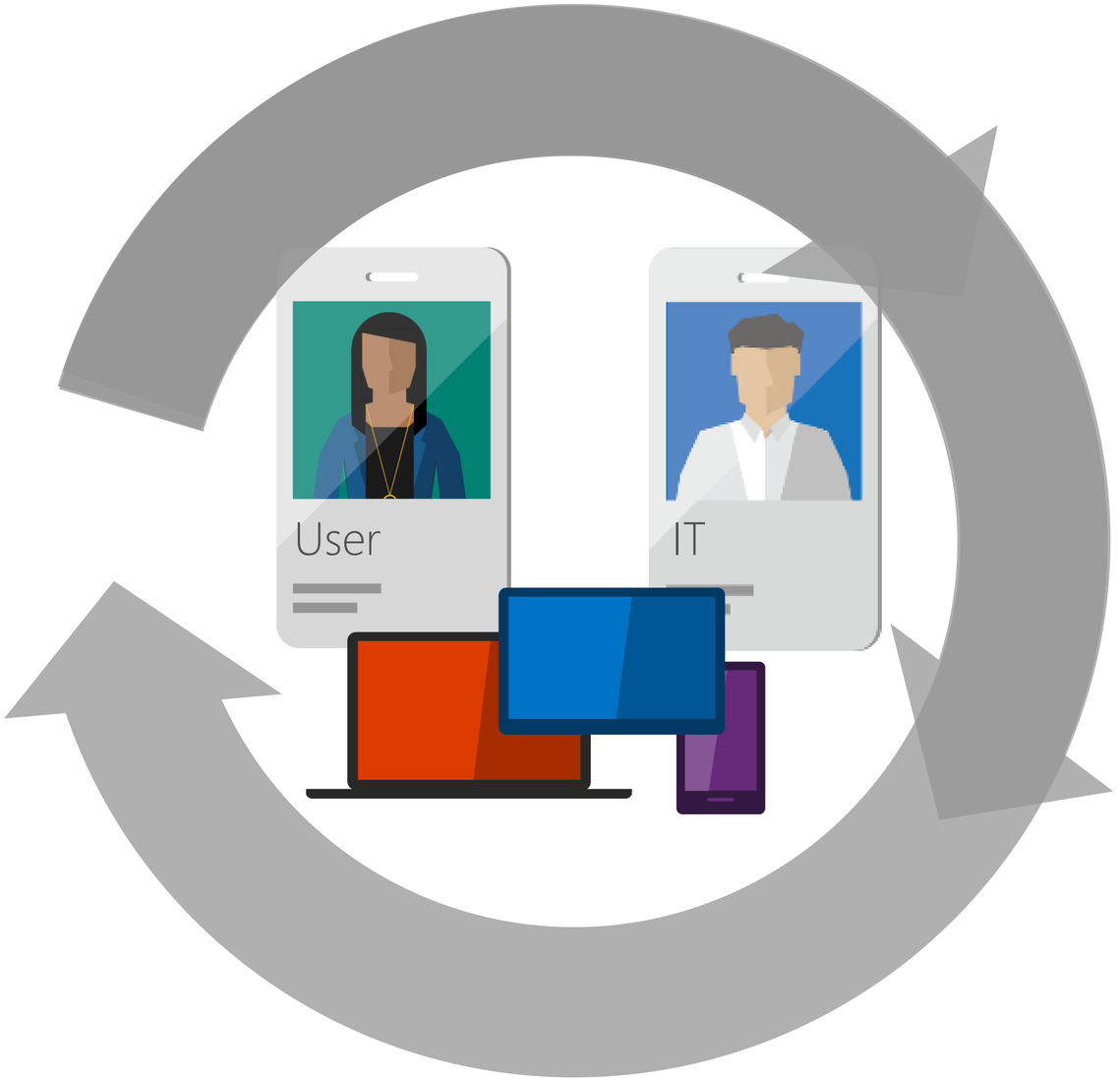
Device lifecycle management

Enroll

- Provide a self-service Company Portal for users to enroll devices
- Deliver custom terms and conditions at enrollment
- Bulk enroll devices using Apple Configurator or service account
- Restrict access to resources if a device is not enrolled

Provision

- Deploy certificates, email, VPN, and WiFi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy app restriction policies
- Deploy data protection policies



Retire

- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices

Manage and Protect

- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy, cut, paste, and save as between Intune-managed apps and personal apps
- Report on device and app compliance

Enrolling devices to management

Device enrollment

Device must be first enrolled to MDM (Intune)

- Windows 10 devices can be enrolled automatically
- Push certificate required for iOS devices

Users can enroll their devices

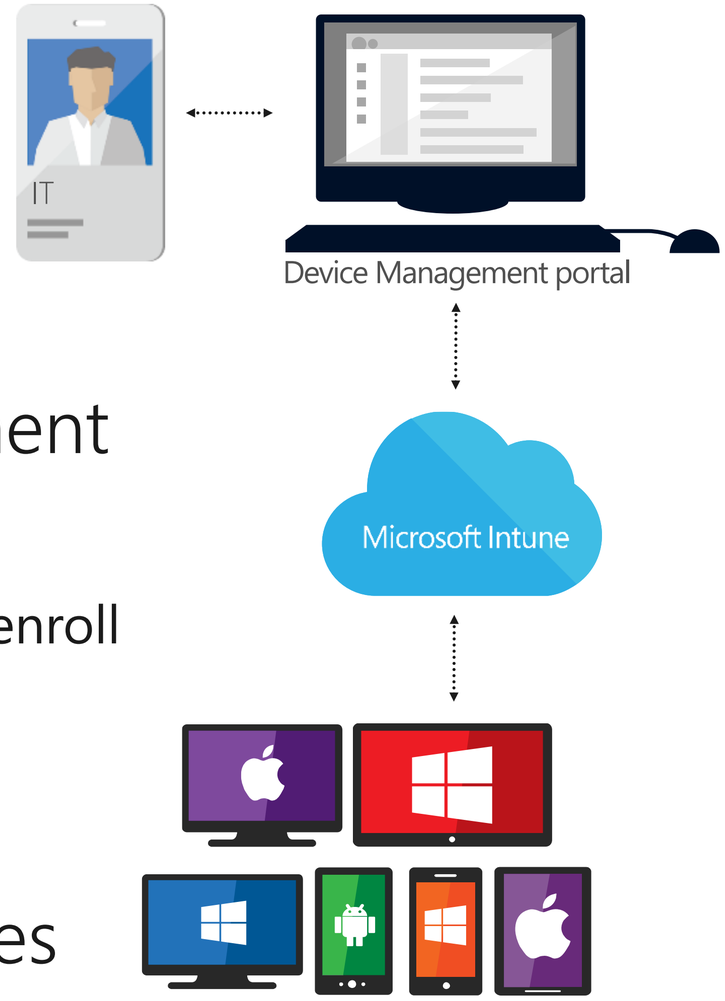
Enrollment status page can be shown during enrollment

Enrollment restrictions

- Which device types can be enrolled, number of devices that user can enroll

Data Enrollment Manager

Prevent access to resources from non-enrolled devices



Device Management requires Azure Active Directory

Users must have Intune license to enroll device to management

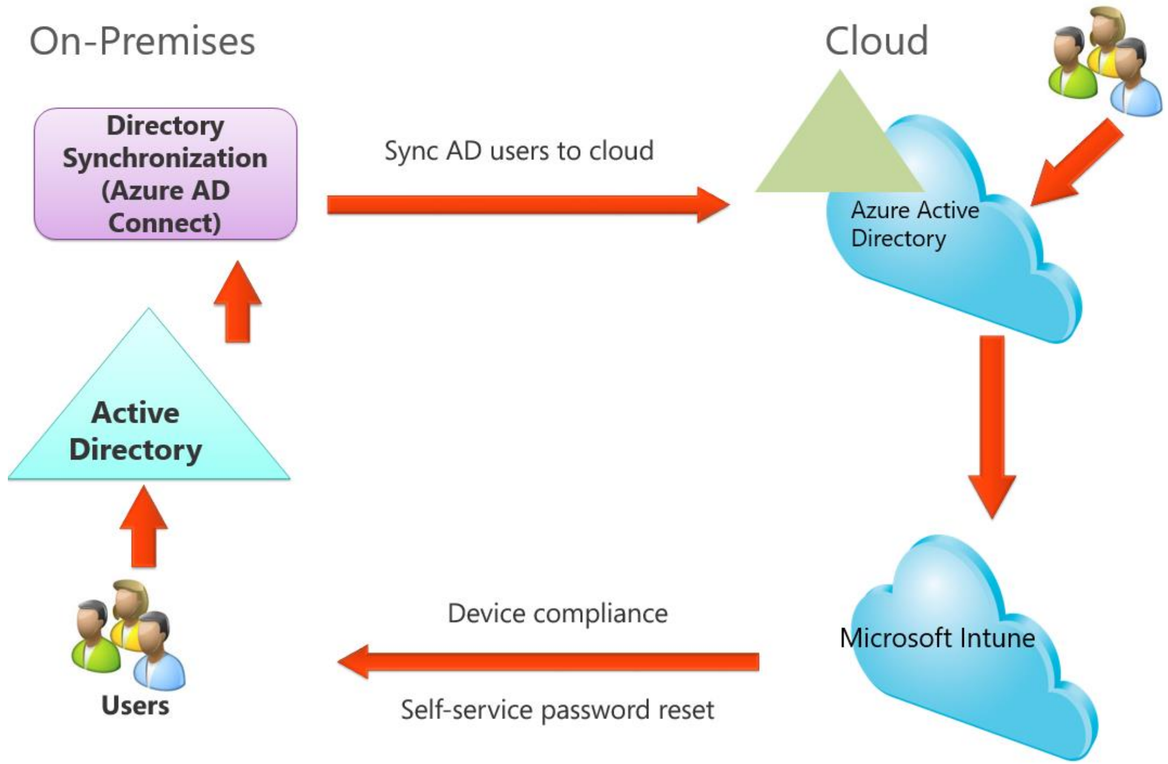
Devices and their properties are stored in Azure Active Directory

Groups are used for management (assigning policies and profiles)

- Assigned
- Dynamic User
- Dynamic Device

Users and groups can be synced

- Azure AD Connect



Configuring devices

- Device configuration profile
- Platform and Profile type controls what can be configured
- Assign to group
  - Exclusion
- After assignment Intune starts notifying devices
  - Typically takes less than five minutes
  - If device is not available, it gets policy during next refresh (refresh cycle is 6 or 8 hours)
- Group Policy wins over MDM policy
- Scope (tag) controls who can manage it
- PowerShell scripts for Windows 10 devices

Are devices compliant?

Device compliance policy

- Define the rules and settings that users and devices must meet to be compliant
- Device type specific

Assigned to groups, can configure exclusion

If multiple policies apply, most restrictive result wins

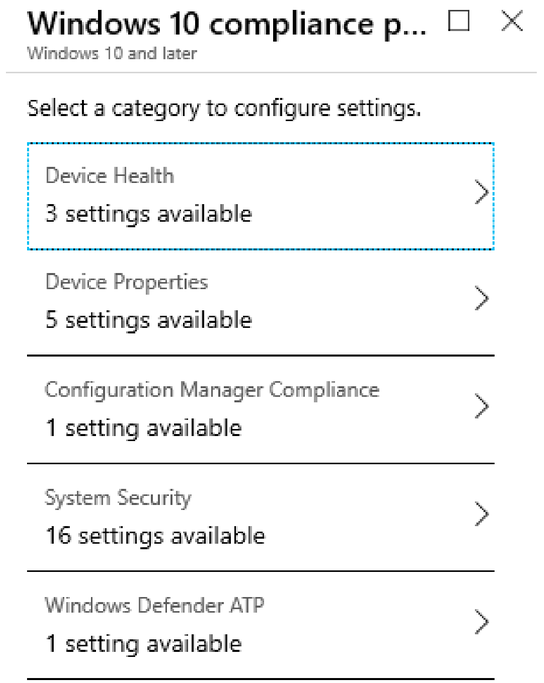
Actions for noncompliance

Compliance status written in Azure AD

- Can be synced to on-premises Active Directory

Compliance often used with Conditional Access Policies

- Or for compliance reporting



Controlling Access

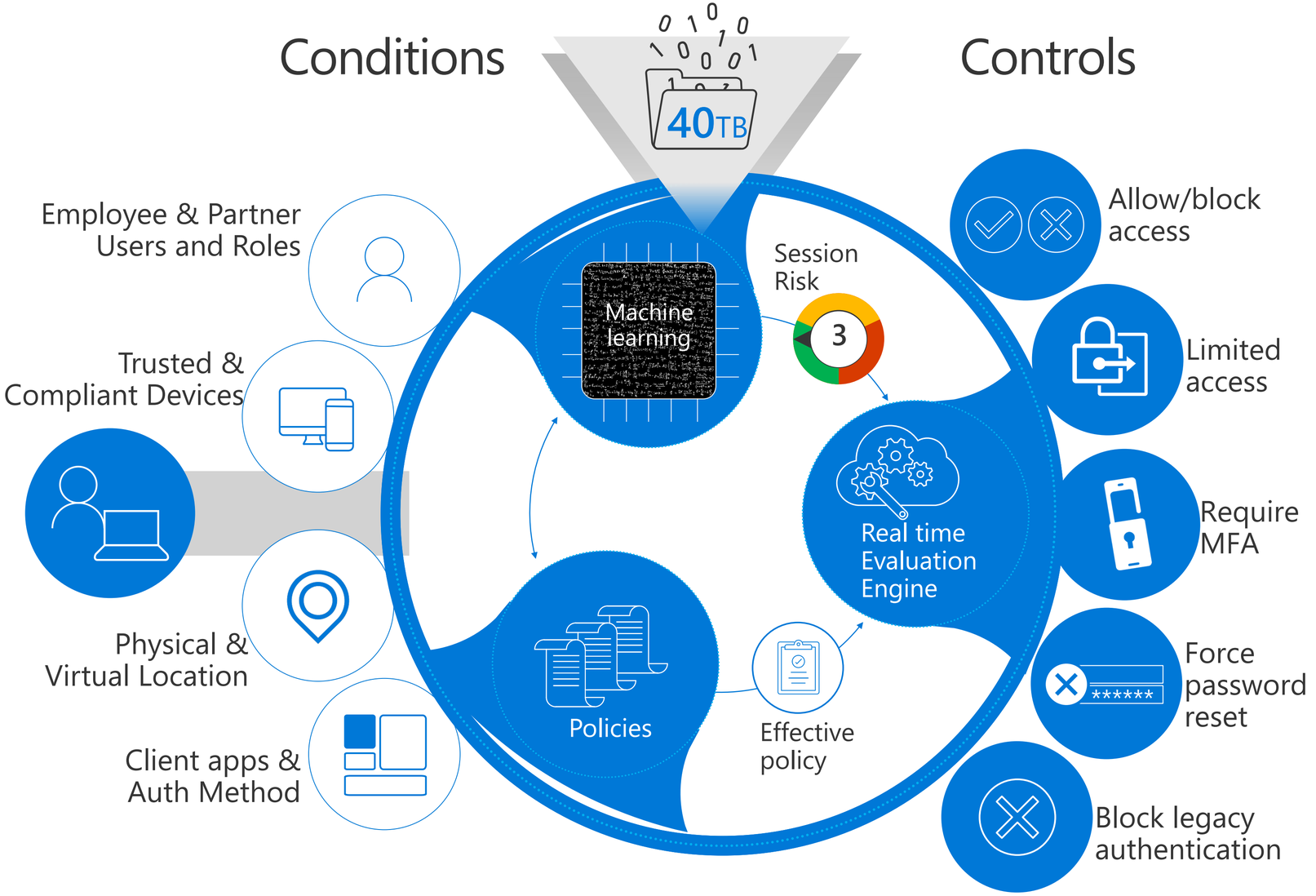
Conditional Access

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps



Microsoft Cloud

Microsoft
Cloud App Security

Cloud SaaS apps

On-premises apps

Deploying and managing apps

Client apps

Different app types can be deployed

- Store apps, Office 365, web link, built-in, LOB and Win32 apps

After installation apps are updated automatically (except LOB apps)

App configuration policies for configuring apps

- Android and iOS only

Intune-enlightened apps provide the best control

With or without enrollment

Protecting app data

App protection policies

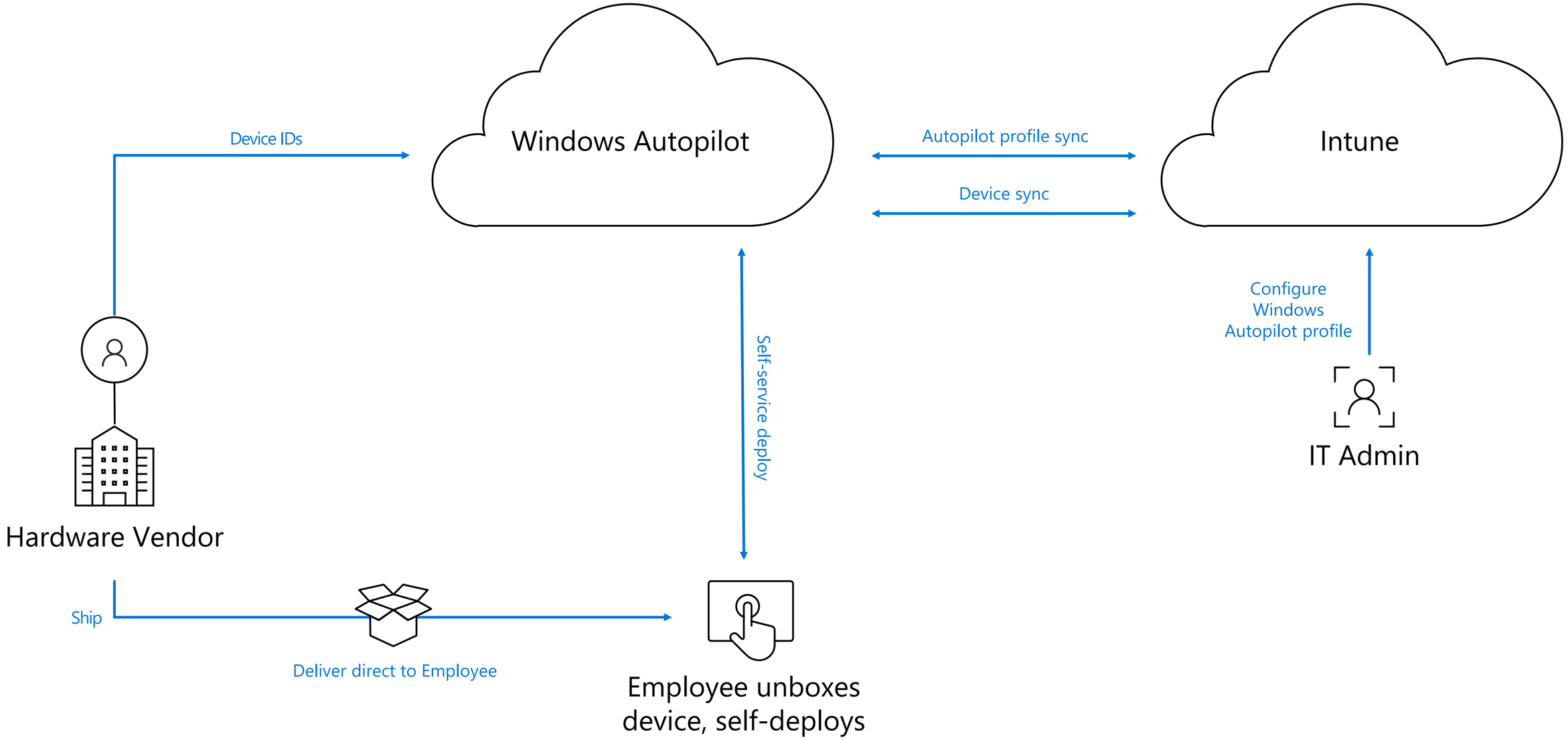
Separates personal and corporate apps

- Corporate data is encrypted
- Control interaction between app types

Can require corporate app for access

Selective wipe removes corporate data

Deploying new devices – Windows Autopilot



Monitoring and reporting on devices

Basic monitoring in Microsoft 365 Device Management

- Data can be exported

Intune Data Warehouse for custom reports from your Intune data

- Can be analyzed by using Power BI

Delegating permissions

- Device Management (Intune) includes granular permission delegation
  - Role Based Access Control (RBAC)
- Several built-in roles
  - Can create own roles
  - Granular permissions can be assigned
- Scope (tag) for every role and for every Intune resource

Summary

- Microsoft 365 brings modern device management
  - It is often synced with on-premises Active Directory
  - Co-management for coexistence with traditional management
- Device Management is provided by Intune
  - Microsoft 365 Device Management admin center
  - Azure portal
- Devices must be enrolled to management first
  - Use conditional access policy to enforce enrollment
- Configure devices, gather compliance data, deploy apps
- Conditional access policies control access to apps

Additional information

What is device management?
https://docs.microsoft.com/en-us/intune/what-is-device-management

Managing devices with Microsoft Intune: What's new and what's next
https://myignite.techcommunity.microsoft.com/sessions/64592

What is Microsoft Intune?
https://docs.microsoft.com/en-us/intune/what-is-intune

Compliance Overview
https://docs.microsoft.com/en-us/intune/device-compliance-get-started

What is conditional access in Azure Active Directory?
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview