

2024

Secure Data on Personally-Owned Devices

Security Concerns with Employee Devices

Lost or stolen devices

Intentional/Unintentional
Data Theft

Employee Attrition/Offboarding



Microsoft Intune app protection policies

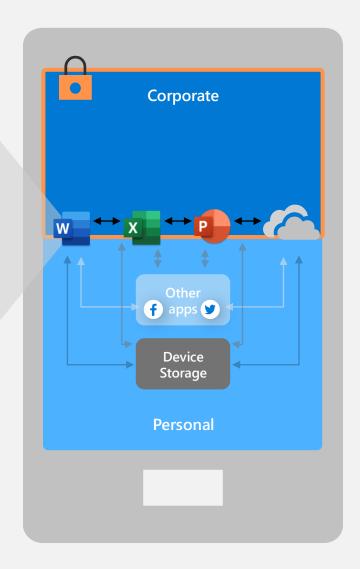
Microsoft Intune provides app protection policies (APP), which are app-level rules that can manage and protect your organization's corporate data

App protection policies can be applied to

iOS/iPadOS devices (iPhones, iPads, iPods)*

Android devices





^{*} For simplicity, later in this slide deck they all will be referred to as iOS devices.

Also, we will use [iOS] and [Android] tags to mark items specific to these device types.

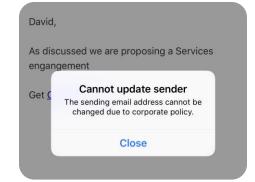
What do app protection policies provide?



Multi-identity awareness

Targets protection ONLY to corporate account

Personal and unmanaged accounts aren't affected





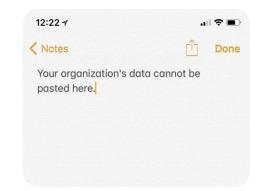
Data protection

Encrypts corporate data

Controls data transfer mechanisms between managed and unmanaged apps

Controls transfer of web content

Selective wipe of corporate data – whether it be admin, user, or offline initiated

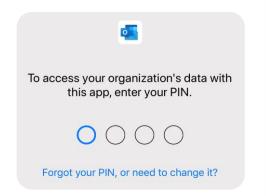




Access requirements

Controls access to corporate data via PIN, biometrics, or credentials

Provides inactivity timers





Conditional launch

Validates device health: Jailbreak/Rootkit, mobile threat defense

Validates OS variables like OS version, Android patch version

Validates app variables like app version or SDK version

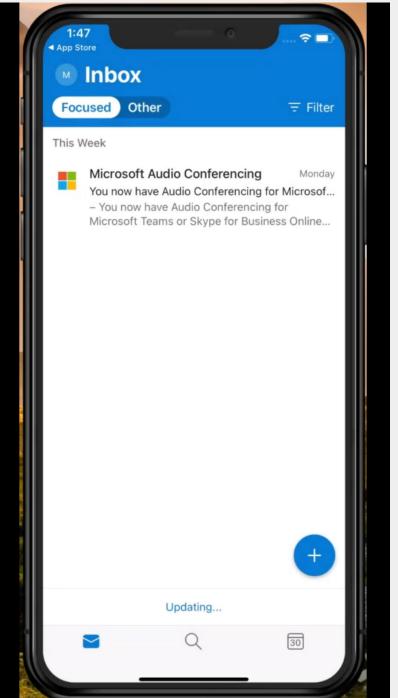
Validates device model or manufacturer



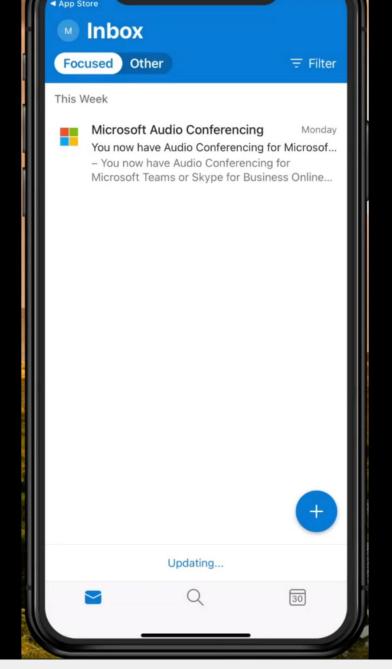


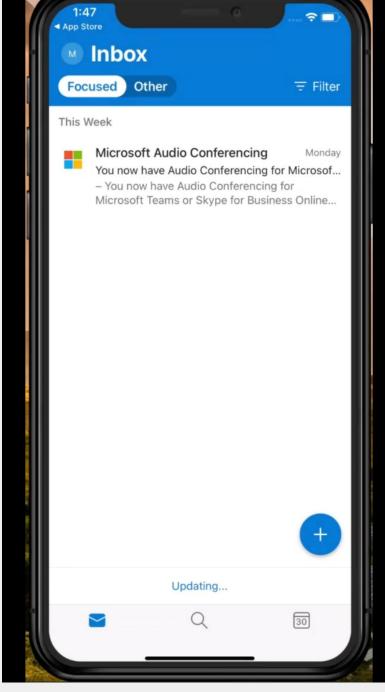
















How do we get started?



Project-based professional services for deploying Microsoft Intune Mobile Application Management



Microsoft Intune Licensing



AHEAD

Thank You

Accelerate Your Impact ahead.com