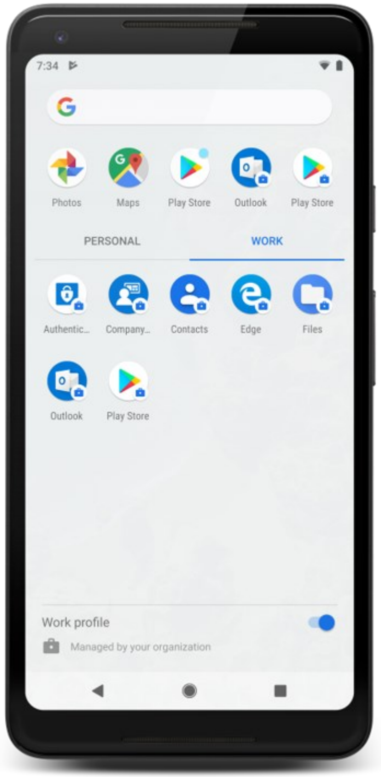
Microsoft

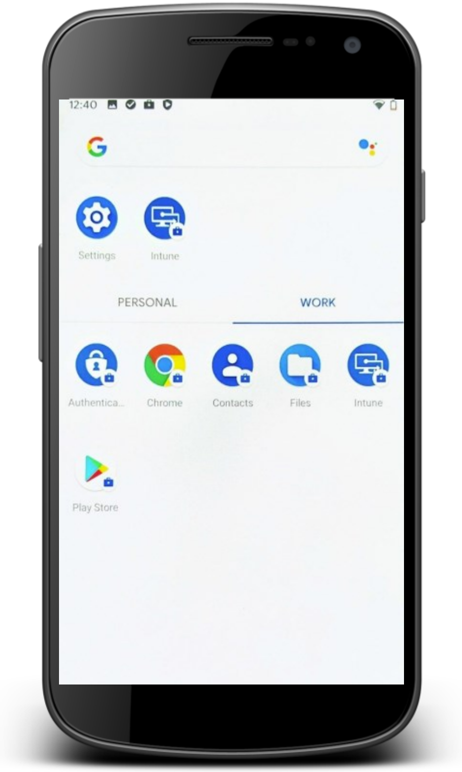
Shared Devices for Firstline Workers

Microsoft Endpoint Manager Customer Experience Engineering Team

Android deployment scenarios

Personally owned		Company owned		
Intune management	Intune management with Android Enterprise			
App protection policies	Work profile	Corp-owned with work profile PREVIEW	Fully managed	Dedicated

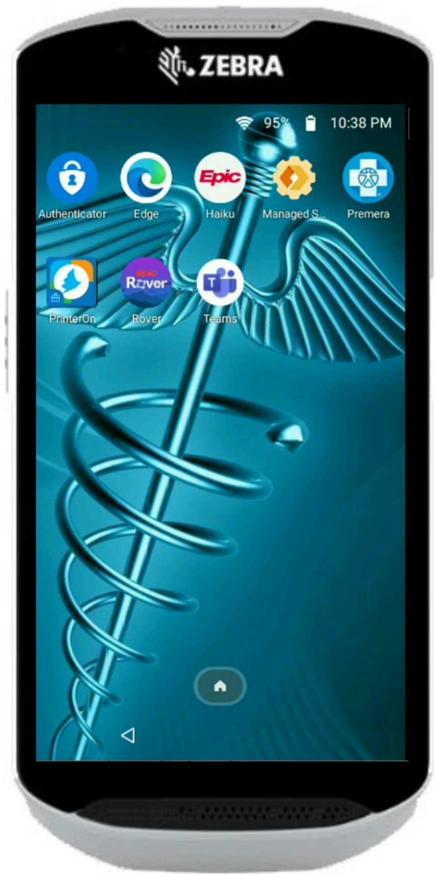


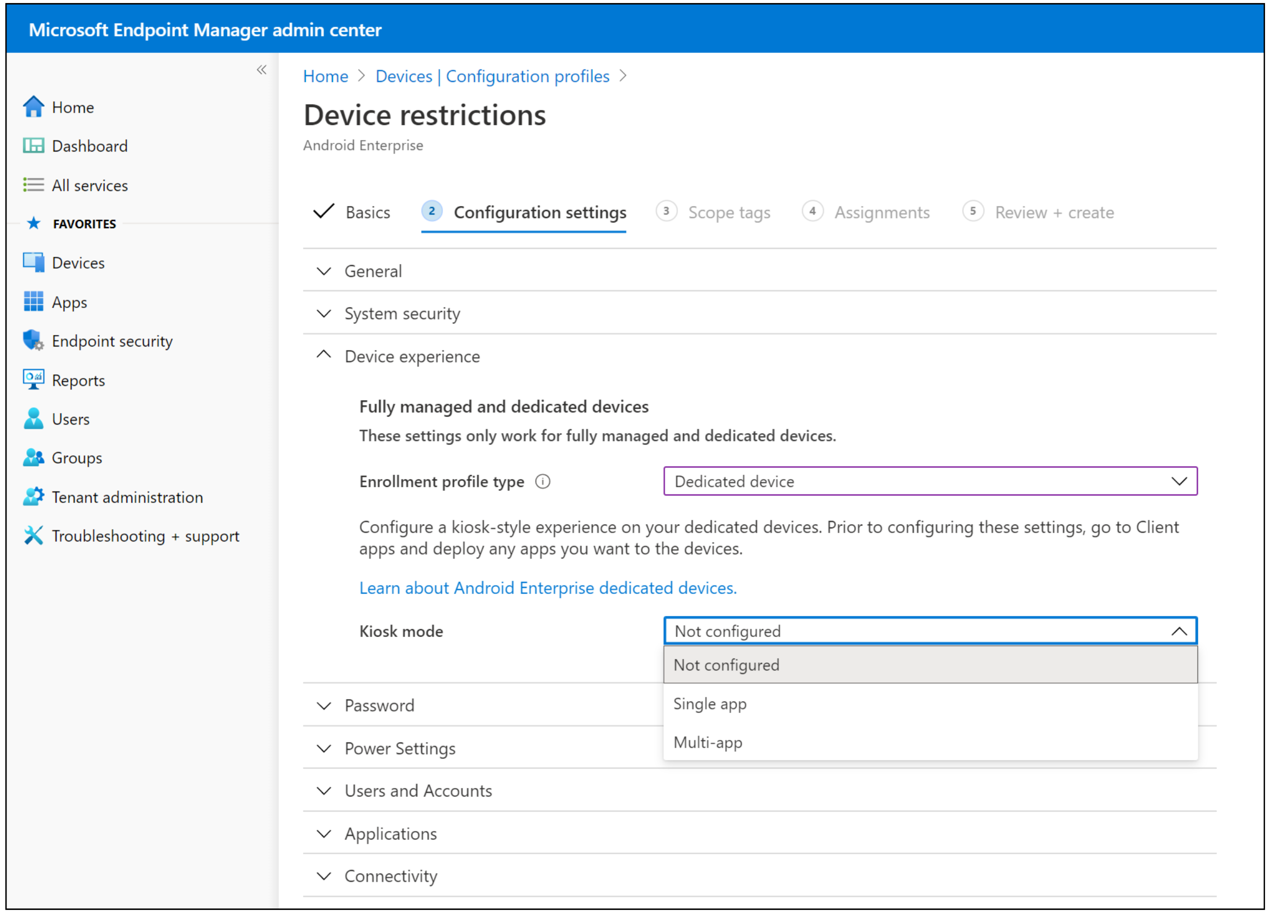


Dedicated Enrollment with Managed Home Screen

New config UI settings

- Folder icon
- App and folder icon size
- Screen orientation
- App notification badges
- Shortcut to settings menu
- Quick access to debug menu
- Quick access to device information
- Wi-fi allow-list




Microsoft Endpoint Manager admin center

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Home > Devices | Configuration profiles >

Device restrictions

Android Enterprise

✓ Basics · 2 Configuration settings · 3 Scope tags · 4 Assignments · 5 Review + create

General

System security

Device experience

Fully managed and dedicated devices

These settings only work for fully managed and dedicated devices.

Enrollment profile type: Dedicated device

Configure a kiosk-style experience on your dedicated devices. Prior to configuring these settings, go to Client apps and deploy any apps you want to the devices.

Learn about Android Enterprise dedicated devices.

Kiosk mode: Not configured

- Not configured
- Single app
- Multi-app

Password

Power Settings

Users and Accounts

Applications

Connectivity

Manage Android Enterprise devices with OEMConfig in Microsoft Intune

Support for rugged device OEMs with OEMConfig

BLUEBIRD

KYOCERA

DATALOGIC EMPOWER YOUR VISION

unitech because we care

Honeywell

SAMSUNG

spectralink

Archos

Ascom

ZEBRA

HMD

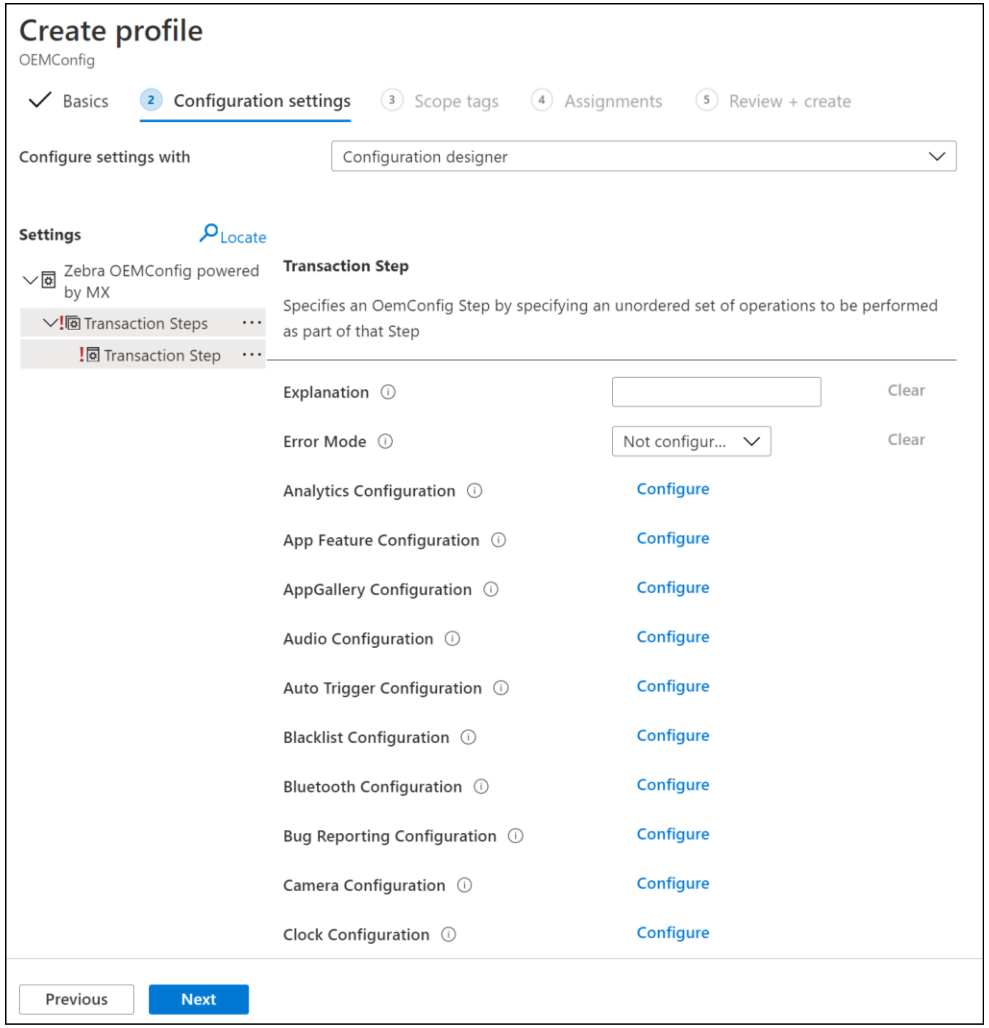
Seuic Mobile

Lenovo

LG

Point Mobile

Panasonic



Create profile
OEMConfig

✓ Basics · 2 Configuration settings · 3 Scope tags · 4 Assignments · 5 Review + create

Configure settings with: Configuration designer

Settings — Locate

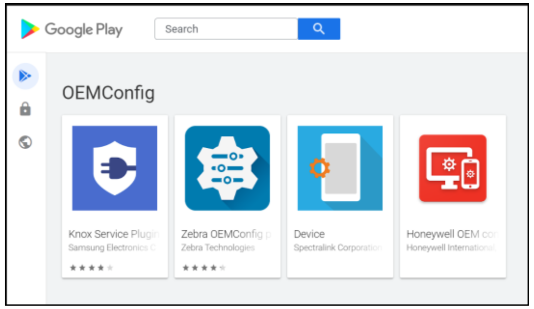
- Zebra OEMConfig powered by MX
  - Transaction Steps ...
    - Transaction Step ...

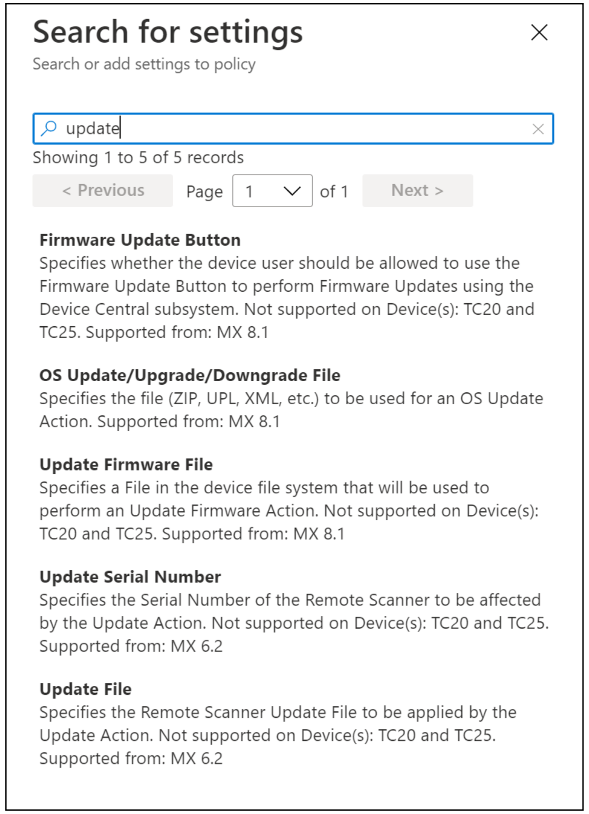
Transaction Step

Specifies an OemConfig Step by specifying an unordered set of operations to be performed as part of that Step

Explanation ⓘ		Clear
Error Mode ⓘ	Not configur...	Clear
Analytics Configuration ⓘ	Configure	
App Feature Configuration ⓘ	Configure	
AppGallery Configuration ⓘ	Configure	
Audio Configuration ⓘ	Configure	
Auto Trigger Configuration ⓘ	Configure	
Blacklist Configuration ⓘ	Configure	
Bluetooth Configuration ⓘ	Configure	
Bug Reporting Configuration ⓘ	Configure	
Camera Configuration ⓘ	Configure	
Clock Configuration ⓘ	Configure	

Previous · Next





Search for settings
Search or add settings to policy

update

Showing 1 to 5 of 5 records

< Previous · Page 1 of 1 · Next >

Firmware Update Button
Specifies whether the device user should be allowed to use the Firmware Update Button to perform Firmware Updates using the Device Central subsystem. Not supported on Device(s): TC20 and TC25. Supported from: MX 8.1

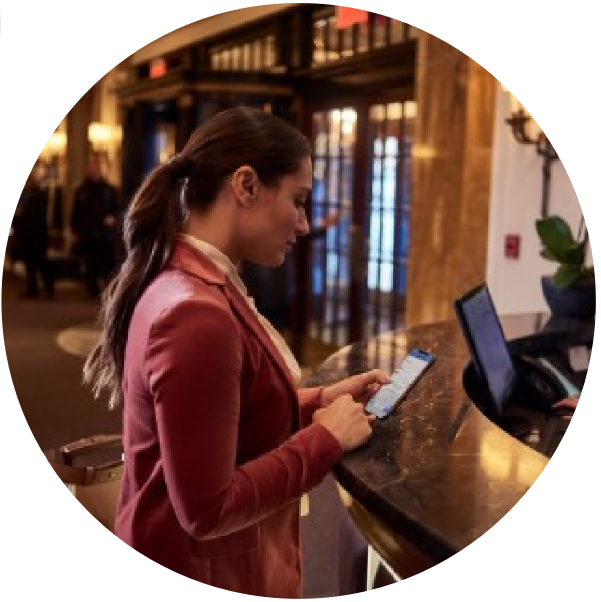
OS Update/Upgrade/Downgrade File
Specifies the file (ZIP, UPL, XML, etc.) to be used for an OS Update Action. Supported from: MX 8.1

Update Firmware File
Specifies a File in the device file system that will be used to perform an Update Firmware Action. Not supported on Device(s): TC20 and TC25. Supported from: MX 8.1

Update Serial Number
Specifies the Serial Number of the Remote Scanner to be affected by the Update Action. Not supported on Device(s): TC20 and TC25. Supported from: MX 6.2

Update File
Specifies the Remote Scanner Update File to be applied by the Update Action. Not supported on Device(s): TC20 and TC25. Supported from: MX 6.2

Enabling firstline workers with Intune & Android



Deploy shared devices at scale

- Automatically configure devices in AAD Shared Device mode
- Easy Intune enrollment using Google Zero-touch or QR code
- Azure AD Conditional Access support

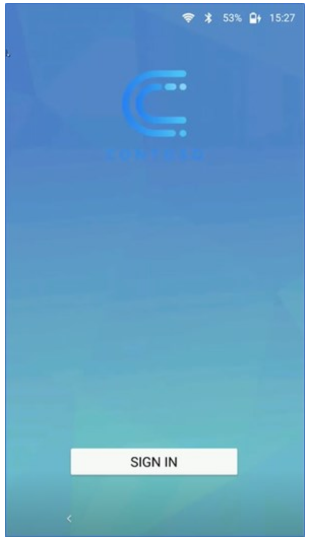
Configurable experience for shared devices

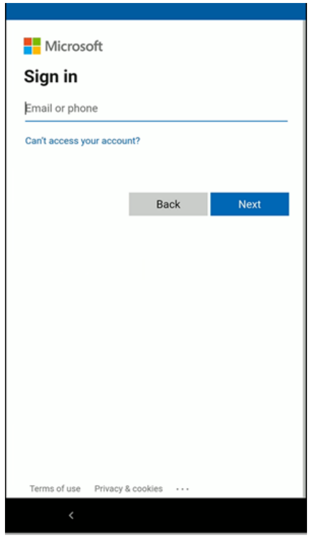
- Lock down shared devices to a certain set of apps for firstline workers
- Configure corporate branding
- Custom session-based PIN

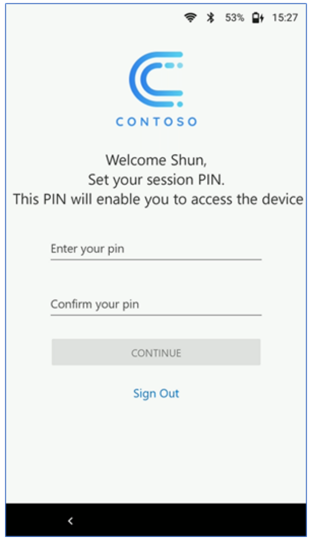
Azure AD shared device mode with Managed Home Screen

Sign in/sign out experience

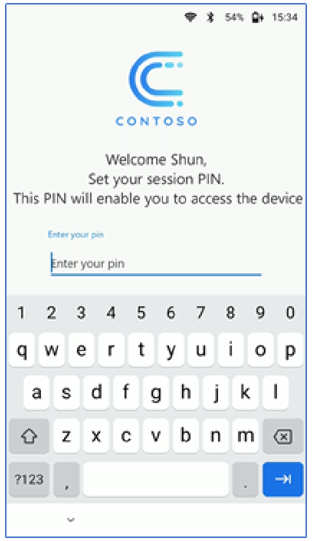
Session PIN for easy unlock while in use







Welcome Shun,
Set your session PIN.
This PIN will enable you to access the device

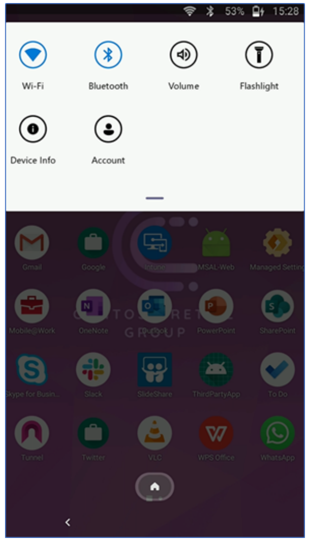


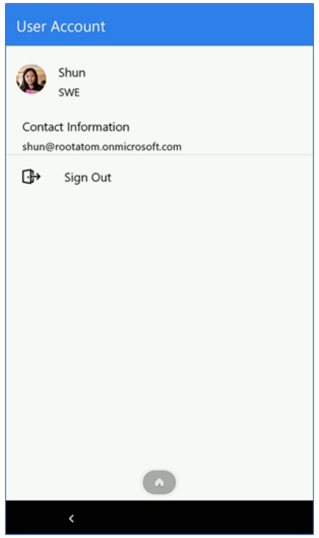
Welcome Shun,
Set your session PIN.
This PIN will enable you to access the device

Customize assigned home screen icons

Define corporate branding

Configure access to Wi-Fi, Bluetooth controls, etc.





Shun
SWE

Contact Information
shun@rootatom.onmicrosoft.com

https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-shared-devices

Requirements to support Azure AD shared device mode

- Apps must adopt MSAL to support Shared Device mode
- No user data saved between sessions
- “Single role” (i.e. apps/policies remain the same from sign-on to sign-on)
- Android devices must support Google Mobile Services
- Device Owner enrollment supported i.e. Dedicated

Demo

ALPINE SKI

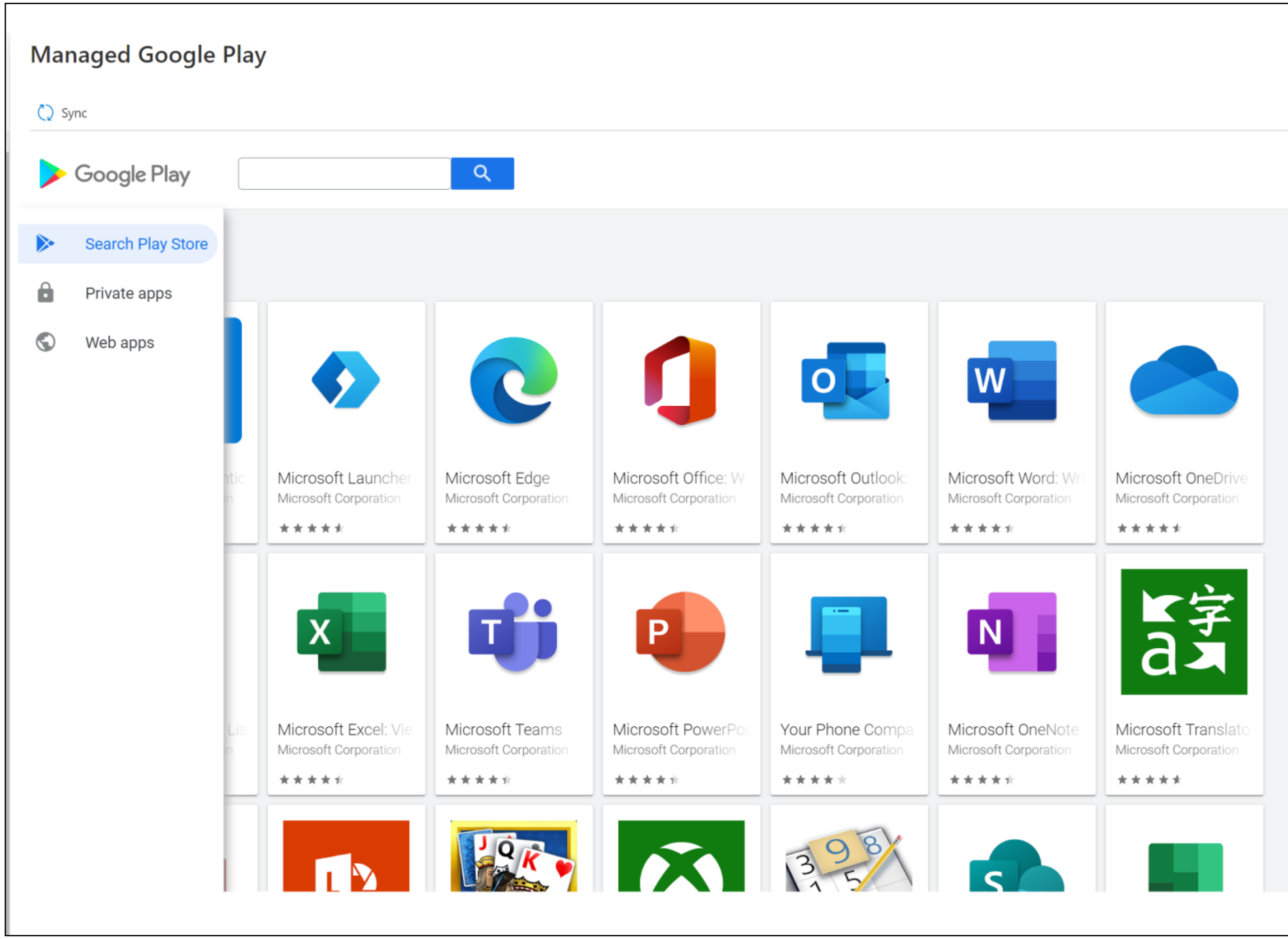
Android Enterprise Enrollment

MHS JSON example

```
 {
          "key": "wallpaper",
          "valueString": "https://wallpapercave.com/wp/PhAOqMZ.jpg"
      },
                                             {
                                                                   "key": "enable_auto_signout",
                                                                   "valueBool": true
                                             },
                                             {
                                                                   "key": "inactive_time_to_signout",
                                                                   "valueInteger": 900
                                             },
                                             {
                                                                   "key": "auto_signout_time_to_give_user_notice",
                                                                   "valueInteger": 600
                                             },
                                             {
                                                                   "key": "enable_session_PIN",
                                                                   "valueBool": true
                                             },
                                             {
                                                                   "key": "session_PIN_complexity",
                                                                   "valueString": "simple"
                                             },
                                             {
                                                                   "key": "enable_mhs_signin",
                                                                   "valueBool": true
                                             }
    ]
}
```

Managed Google Play (MGP)

- **Enterprise version** of Google Play
- **Distribution channel** for mobile applications (Public and Business) on Android Enterprise
- **Web app support**
- **Google Play release tracks**
- **MGP benefits**
  - App allow list
  - Silent provisioning of apps
  - No need to use personal Google accounts
  - App config
  - App security scanning
- **App publishing**
  - Managed Play iFrame
  - Google Play developer console
  - Custom App Publishing API



Managed Google Play Store in Intune

What’s New in Intune’s Android support

Work Profile

- Flow to move to WP from device administrator
- UX guidance to get apps in managed Google Play
- Block face and iris unlock

Corporate-owned with a work profile (preview)

- Enrollment support
- Device configuration settings
- Device compliance settings
- Conditional access support
- App management capabilities
- Remote action support
- Resources access (Certs, Wi-Fi, and VPN)
- MTD support

Fully Managed & Microsoft Launcher

- PFX certificate support
- Manage S/MIME settings for Outlook
- Set Microsoft Launcher as default launcher
- Microsoft Launcher config for wallpaper, dock, and more
- Derived credentials support

Managed Home Screen

- Customize icons, change the screen orientation , and show app notifications on badge icons
- Hide the Managed Settings shortcut
- Easier access to the debug menu
- Create an allowed list of Wi-Fi networks
- Easier access to the device information

Rugged

- New schema settings, and search for existing schema settings using OEMConfig on Android Enterprise
- New device OEM onboarding supporting OEMConfig

Firstline worker

- Azure AD shared device mode with Managed Home Screen

Managed Google Play

- Pre-release testing for Managed Google Play app

Device Security

- Use Microsoft Defender ATP in compliance policies for Android
- Configure Defender ATP web protection for Android devices

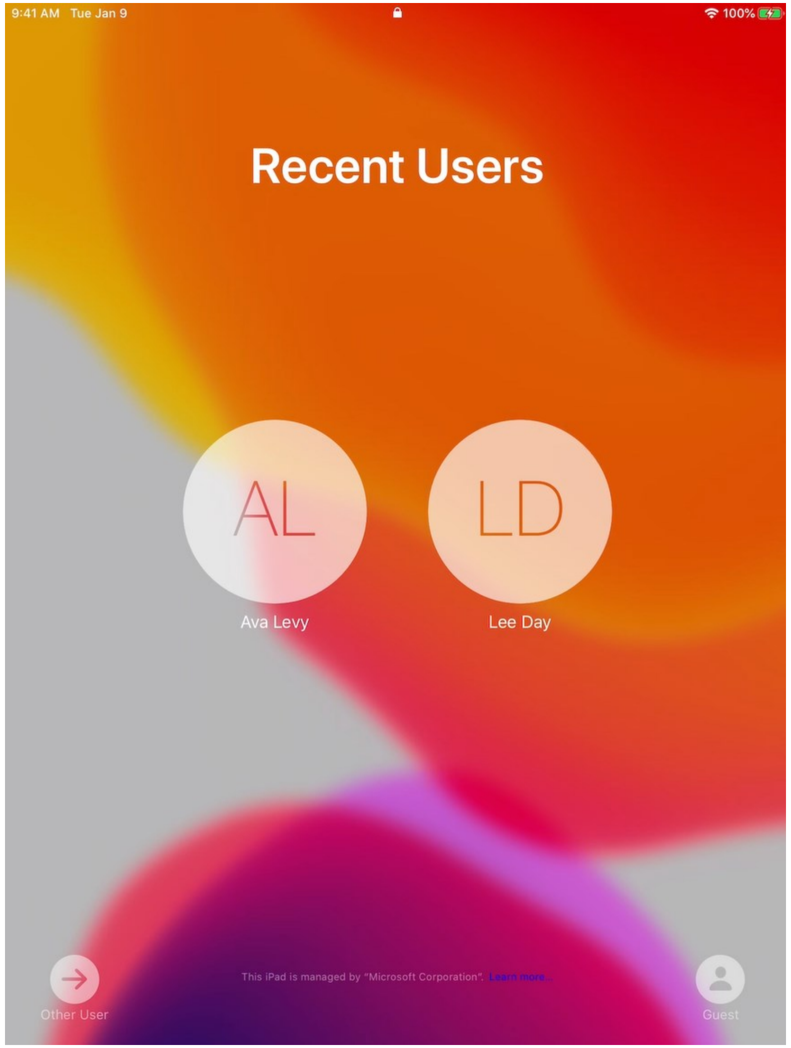
Troubleshooting

- Intune diagnostic tool with Microsoft Edge for Android ("about:intunehelp")

Shared iPad

What is a Shared iPad?

- Supports Multiple Users
- Each user has their own login
- Deployed via Apple Device Enrollment



Recent Users

This iPad is managed by "Microsoft Corporation". Learn more...

Shared iPad – The Basics

- Released in Apple School Manager with iOS 9.3
- Released in Apple Business Manager with iPadOS 13.4
- Requires Managed Apple IDs
- Requires the devices be supervised and enrolled
- Does not require Microsoft Authenticator Shared Devices Mode

What are managed Apple IDs?

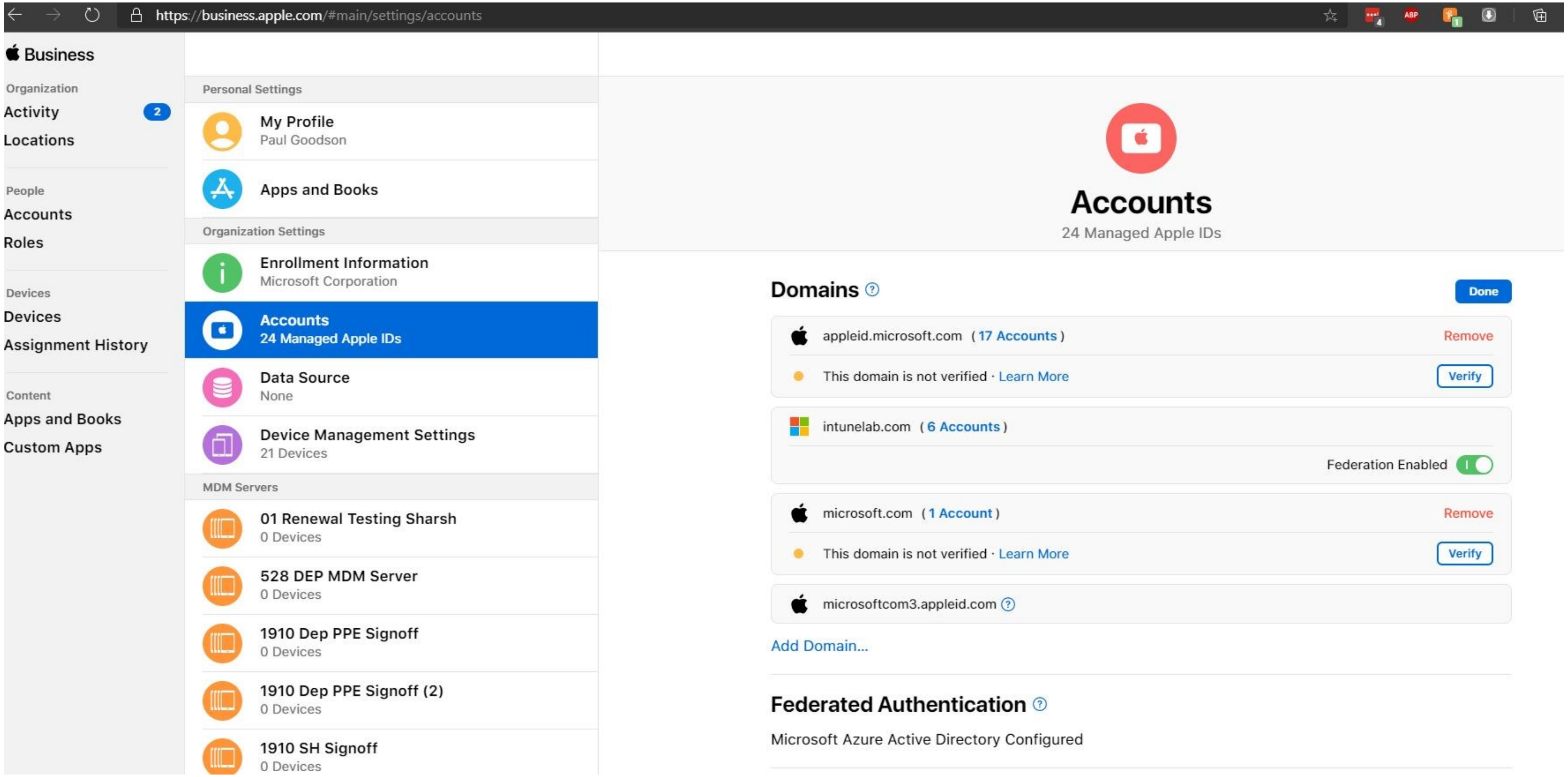
- Managed by IT
- Created either manually in Apple Business Manager or automatically with Federation
  - We strongly recommend creating automatically by federating AAD to Apple
- Used to sign in to Shared iPad and access Apple services
- Allows for an easy end user provisioning experience
- No App Store
- No Apple Pay
- No “Find My” functionality
- No Apple Books

Apple Documentation - What are Managed Apple IDs in Apple Business Manager?

Azure AD to Apple Federation

- Benefits
  - Users can leverage their corporate AAD accounts as Managed Apple IDs
  - Managed Apple IDs are created automatically after signing in with Corporate AAD credentials
- Requirements
  - iOS 11.3+, iPadOS 13.1+, macOS 10.13.4+
  - UPN and SMTP must match
  - Only one organization can verify/federate a domain
- Most Common Issue
  - User has already created a non-managed Apple ID using their corporate email/UPN

ABM Federation



My Profile
Paul Goodson

Apps and Books

Enrollment Information
Microsoft Corporation

Accounts
24 Managed Apple IDs

Data Source
None

Device Management Settings
21 Devices

01 Renewal Testing Sharsh
0 Devices

528 DEP MDM Server
0 Devices

1910 Dep PPE Signoff
0 Devices

1910 Dep PPE Signoff (2)
0 Devices

1910 SH Signoff
0 Devices

Accounts
24 Managed Apple IDs

Domains

appleid.microsoft.com (17 Accounts) Remove
This domain is not verified · Learn More Verify

intunelab.com (6 Accounts)
Federation Enabled

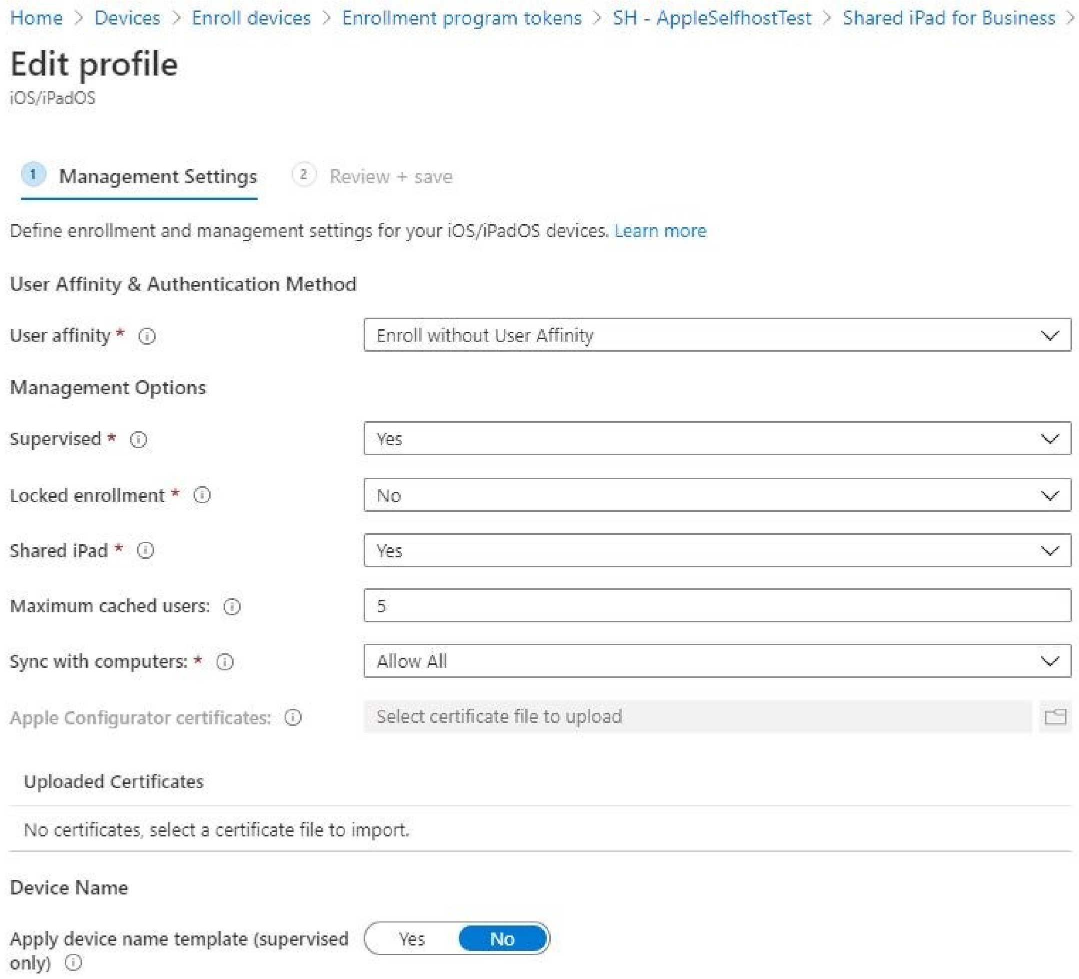
microsoft.com (1 Account) Remove
This domain is not verified · Learn More Verify

microsoftcom3.appleid.com

Federated Authentication

Microsoft Azure Active Directory Configured

How do you deploy a Shared iPad in Intune?



Home > Devices > Enroll devices > Enrollment program tokens > SH - AppleSelfhostTest > Shared iPad for Business >

Edit profile

iOS/iPadOS

Define enrollment and management settings for your iOS/iPadOS devices. Learn more

User Affinity & Authentication Method

User affinity * ⓘ: Enroll without User Affinity

Management Options

Supervised * ⓘ: Yes

Locked enrollment * ⓘ: No

Shared iPad * ⓘ: Yes

Maximum cached users: ⓘ 5

Sync with computers: * ⓘ Allow All

Apple Configurator certificates: ⓘ Select certificate file to upload

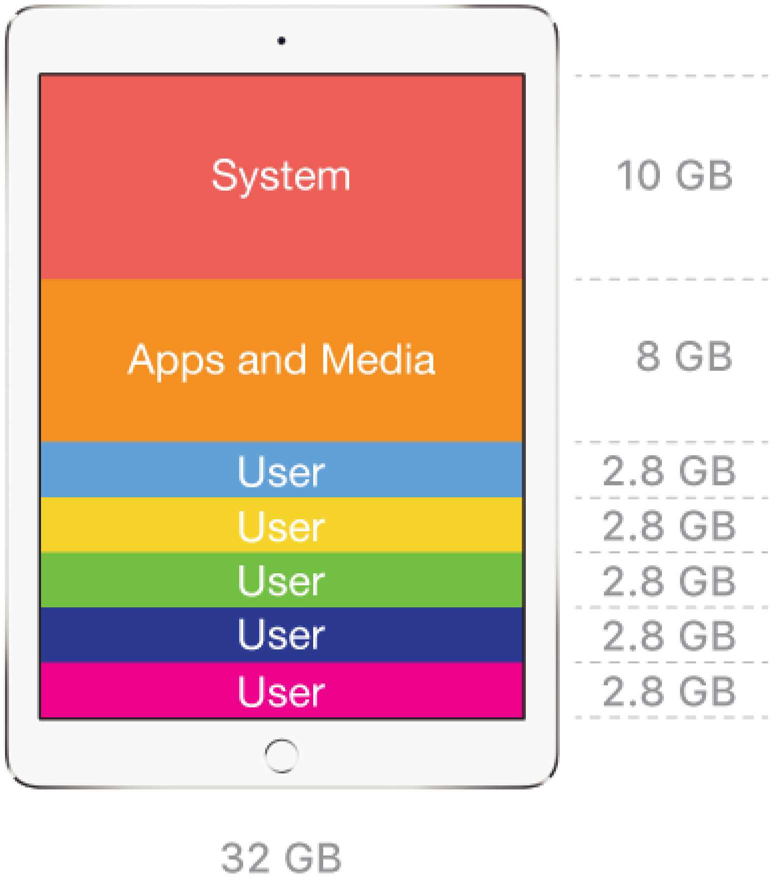
Uploaded Certificates

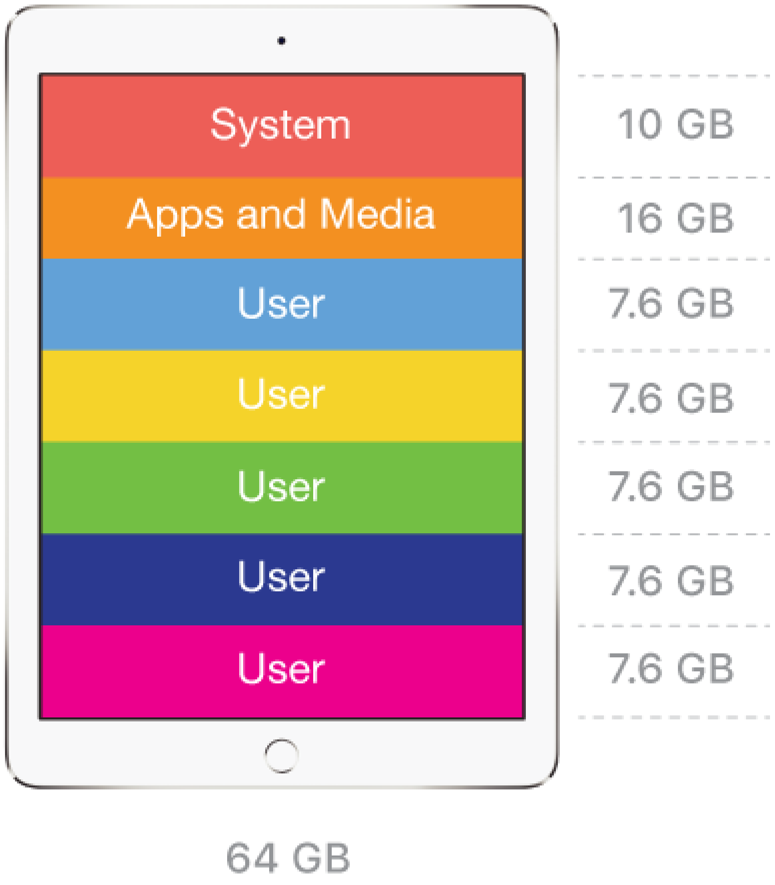
No certificates, select a certificate file to import.

Device Name

Apply device name template (supervised only) ⓘ: Yes [✓ No]

Maximum Cached Users?



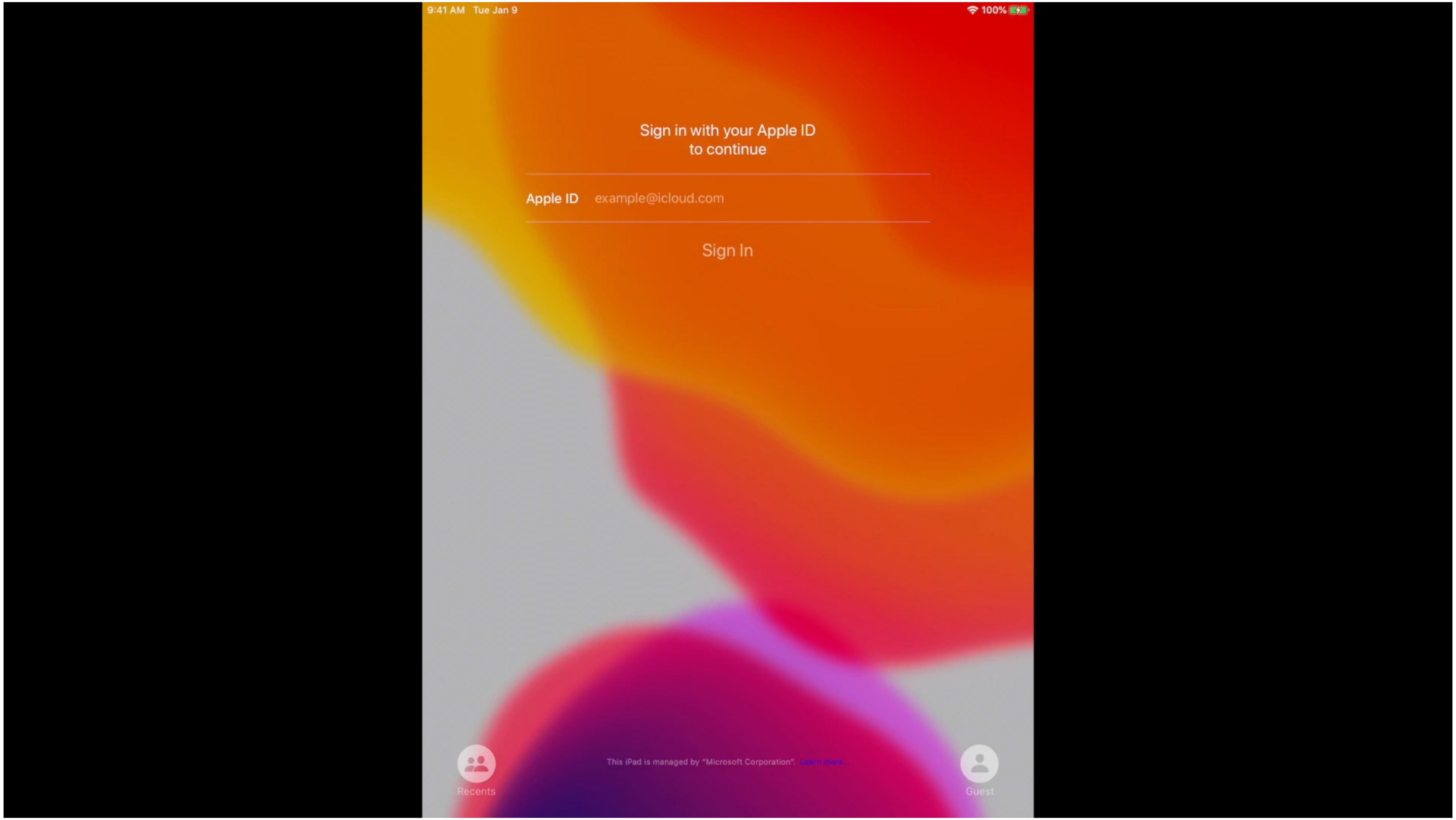


Use Shared iPad - Deployment Guide

A few things to know…

- Use VPP apps targeted to devices as required installs with device licensing
- Targeting policy to users is coming
- Passcode requirements are controlled by Apple
  - Apple Business Manager always requires a complex passcode
  - Apple School Manager allows for complex and non-complex passcodes

Demo



Sign in with your Apple ID
to continue

Apple ID example@icloud.com

This iPad is managed by "Microsoft Corporation". Learn more...

Resources

Intune UserVoice

https://microsoftintune.uservoice.com/

Intune features in development

https://docs.microsoft.com/en-us/mem/intune/fundamentals/in-development

Microsoft