Microsoft

Practical Teams Devices Rollout

Daryl Hunter
Principal Technical Program Manager
Global Customer Success

Who is this Daryl Hunter guy anyway?

Hi – I'm Daryl. You can call me DW. I've been breaking telephony systems as long as I can remember. In my technical strategy role at Microsoft I bring a competitive SME lens for all things Microsoft Teams Phone & Devices.

I have been married to Jenny for 20-something years, we have four kiddos in Middle School, High School and out and about adulting. We also have a dog – Ivy – she's a 6 year old Bernedoodle and unlike most really smart doodles, ours is full of dumbness.

I enjoy all things bourbon – it's a fascinating story for my home state of Kentucky. I also play competitive Chess & Backgammon. Let me know if you're up for a challenge!

Agenda

- Teams Academy – for IT Pro like you and me
- Intro Teams Device Deployment Playbook
- M365 Admin – Identities & Licensing
- Intune Admin – Enrollment & Compliance
- Entra Admin – Conditional Access
- Teams Admin – Validate Success
- Q&A + Wrap UP

Teams Academy & Device Deployment Playbook

Teams Academy – IT PRO Resources + Playbooks

- Teams Academy – For IT PRO like you and me
- https://aka.ms/teamsacademy
- You (and your customers) should bookmark this!

- Engineering Playbooks – Virtual Events, Teams Premium, Teams Places, VDI, SIP Gateway, Shared Calling, Teams Devices Deployment
- https://aka.ms/teams-devices-deployment-playbook

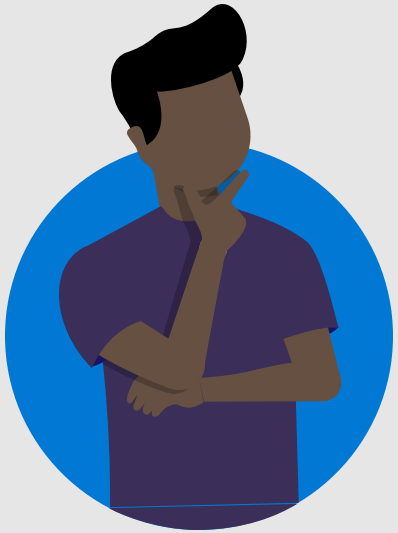
Microsoft Teams

Device Deployment Playbook

Microsoft Teams Devices

https://aka.ms/teams-devices-deployment-playbook

Selecting your device experience



I	II	III	IV
What type of experience?	What type of device?	If room, which type of room device?	System accessories
Personal	Phone	Microsoft Teams Rooms on Android (MTRoA)	Panel
Shared	Room	Microsoft Teams Rooms on Windows (MTRoW)	Intelligent devices, content cameras, etc.*

Device selection examples:

Personal phone: Provide traditional desk phone experiences to single user

Shared phone: Provide traditional desk phone experiences shared by multiple users

Shared room with Panel: Provide enhanced meeting experiences on Windows-based device dedicated to a meeting room, used by multiple users with panel displaying meeting room information mounted near the entry door.

Stay current with the growing list of certified Teams devices in the Teams devices marketplace.

* You can learn more about these devices here: Teams Intelligent Speaker & Content Camera

Teams Rooms on Windows

- ✓ Resource account created: Click Here
- ✓ Set resource account policies in Exchange: Click Here
- ✓ Password expiration disabled: Click Here
- ✓ Meeting room license assigned: Click Here
- ✓ Phone number assigned: Click Here
- ✓ Entra ID group created and all MTRW resource accounts are added to it (for assigning Intune configurations & conditional access policies): Click Here
- ✓ Conditional access configured (with IP restrictions & device compliance) and assigned to resource account group (and also excluded from existing policies): Click Here
- ✓ Entra ID dynamic group created for MTR devices to assign Intune compliance policies (matching to the devices display name: “MTR-”): Click Here
- ✓ Intune Compliance Policy created and assigned to the dynamic device group: Click Here
- ✓ Generate One Time Passcode: Click Here

Teams Rooms on Windows (cont.)

These items are intended to further secure your MTR deployment and speed up the deployment time:

- ✓ Ensure the Entra ID resource account group is in scope for Intune auto enrollment with Entra ID join: Click Here
- ✓ How to join to Entra ID & Intune: Click Here
- ✓ Set the system name (MTR-SerialNumber): Click Here
- ✓ Configure LAPS to manage the default local admin password: Click Here
- ✓ Create an Entra ID security group and add user accounts you want to have administrative access on your MTR: Click Here
- ✓ Configure an Intune CSP to deploy your new Entra ID admin group to all MTRs: Click Here
- ✓ Review and determine proxy configuration (if required): Click Here
- ✓ Deploy certificates (if required): Click Here

Teams Rooms on Android

- ✓ Resource account created: Click Here
- ✓ Set Exchange resource account policies: Click Here
- ✓ Password expiration disabled: Click Here
- ✓ Meeting room license assigned: Click Here
- ✓ Phone number assigned: Click Here
- ✓ Review authentication best practices for personal vs. shared: Click Here
- ✓ Android device administrator enabled: Click Here
- ✓ Entra ID security group created for Android MTRs, resource account added to it: Click Here
- ✓ Intune compliance policy created and assigned to Entra ID group: Click Here
- ✓ Conditional access configured (with IP restrictions & device compliance) and assigned to Entra ID group (exclude from other existing policies): Click Here

Teams Panel

Note: We recommend using existing Teams Room resource accounts unless no Room Device is in the space (first 4 bullets).

- ✓ Resource Account Created: Click Here
- ✓ Set Exchange Resource Account Policies: Click Here
- ✓ Password Expiration Disabled: Click Here
- ✓ Meeting Room License Assigned: Click Here
- ✓ Android Device Administrator Enabled: Click Here
- ✓ Entra ID group created for Teams Panels, resource account added to it: Click Here
- ✓ Intune Compliance Policy Created and Assigned to Entra ID Group: Click Here
- ✓ Conditional Access Configured (With IP Restrictions & Device Compliance) and Assigned to Entra ID Group (exclude from other existing policies): Click Here
- ✓ Optional: Add line of business (LOB) apps: Click Here

Teams Phone (CAP)

- ✓ Resource Account Created: Click Here
- ✓ Password Expiration Disabled: Click Here
- ✓ Common Area Phone License Assigned: Click Here
- ✓ Phone Number Assigned: Click Here
- ✓ Adjust IP Phone Policies: Click Here
- ✓ Authentication Best Practices for Personal vs. Shared: Click Here
- ✓ Android Device Administrator Enabled: Click Here
- ✓ Entra ID security group created for CAP Phones, resource account added to it: Click Here
- ✓ Intune Compliance Policy Created and Assigned to Entra ID Group: Click Here
- ✓ Conditional Access Configured (With IP Restrictions & Device Compliance) and Assigned to Entra ID Group (exclude from other existing policies): Click Here

Teams Phone (Personal)

- ✓ Android Device Administrator Enabled: Click Here
- ✓ Review licenses assigned to users that may utilize these devices to ensure compliance with Entra ID and Intune features detailed below.
- ✓ Review Authentication Best Practices for Personal vs. Shared: Click Here
- ✓ Intune Compliance Policy Created and Assigned to Entra ID Group: Click Here
- ✓ Conditional Access (without IP restrictions if deployed outside office) & Device Compliance configured and Assigned to Entra ID Group: Click Here

Microsoft Teams

Security & Network Considerations

Microsoft Teams

Conditional Access / Compliance Policy Examples

Microsoft Teams

Maintenance & Monitoring

M365 Admin
Identities & Licensing

M365 Admin – Identities & Licensing

Personal Devices

- End-user identity
- End-user licensing + any add-ons – Teams Phone, Calling Plan, Intune, Entra

Shared Devices

- Common Area Phones – end-user-based Resource Account identity
- Common Area Phones - Shared Device License – includes Intune, Entra + any add-ons
- Playbook - Resource Account Created: Click Here
- Playbook - Common Area Phone License Assigned: Click Here

- Teams Rooms – Rooms-based Resource Account identity
- Teams Rooms Pro License – includes Intune, Entra - + any add-ons
- Teams Rooms Basic License – does not include anything else + add-ons
- Playbook - Resource account created: Click Here
- Playbook - Meeting room license assigned: Click Here

Intune Admin
Enrollment & Compliance

Intune Admin – Enrollment & Compliance

Android

- Compliance targets an identity
- Playbook - Android device administrator enabled: Click Here
- AOSP - Full Migration Guide: Click Here
- AOSP – AOSP Device Management for Teams Devices FAQ: Click Here

Windows

- Compliance targets the device account
- Playbook - Entra ID group created and all MTRW resource accounts are added to it (for assigning Intune configurations & conditional access policies): Click Here
- Playbook - Entra ID dynamic group created for MTR devices to assign Intune compliance policies (matching to the devices display name: “MTR-”): Click Here
- Playbook - Intune Compliance Policy created and assigned to the dynamic device group: Click Here

Intune Admin
Enrollment & Compliance

Understanding Intune Enrollment

Android enrollment

- Company Portal client built into the firmware enrolls using Device Administrator profile at time of login.
- Controlled by the assignment of the Intune license to the resource account the device signs into.
- Intune enrollment is recommended for all Teams Android devices

Windows enrollment

- Leverages existing Windows enrollment process
- Devices can be enrolled into Intune with two methods:
  - Using the Teams resource account
  - Using a DEM account for bulk enrolment which allows the device to be setup in shared device mode (Recommended)
- Can be automated using a provisioning package.

[Enrolling Microsoft Teams Rooms on Windows devices with Microsoft Endpoint Manager - Microsoft Tech Community]

Entra Admin Conditional Access

Entra Admin – Conditional Access

Android

- Playbook - Conditional access configured (with IP restrictions & device compliance) and assigned to Entra ID group (exclude from other existing policies): Click Here

Windows

- Playbook - Entra ID group created and all MTRW resource accounts are added to it (for assigning Intune configurations & conditional access policies): Click Here
- Playbook - Conditional access configured (with IP restrictions & device compliance) and assigned to resource account group (and also excluded from existing policies): Click Here

Conditional Access with Teams Devices

Teams Devices support integration with Conditional Access in Entra ID

Planning your access strategy around both the account being used, and the device type. The importance of this is reflected both in the conditional access policies assigned to the account, but also the capabilities of the device against those policies.

Examples include:

- Shared Android Devices vs Android Mobile Phones
- Use of Filters for Devices to configure granular policies
- Use of Multi Factor Authentication

Tip: Use the "What If" tool within Microsoft Entra Admin Center to view what policies are being applied to the accounts your devices will sign-in with.

Tip: Check what policies are supported, per device type here
Tip: Check out our best practices for Conditional Access and Intune compliance here

Shared devices conditional access (Windows Devices)

Intune compliance + Trusted location

Entra ID Conditional Access Rule

Assignment

Users & Groups:

Shared devices group

Cloud Apps:

Exchange Online

Microsoft Teams

SharePoint Online

Conditions:

Device Platforms

Windows

Locations

All trusted locations

Access Controls

Grant Type:

Grant Access

Controls:

Require Device to be marked as Compliant

Intune

Compliance Policy

Compliance Settings

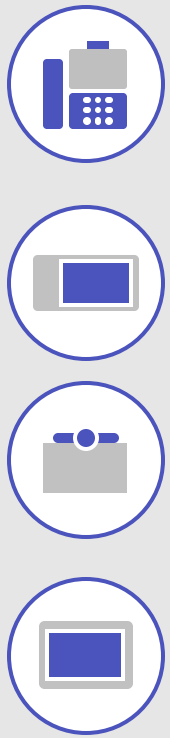
Firewall: Enabled
Defender: Enabled

Actions for non-compliance

Mark device noncompliant: Immediately

Shared devices conditional access (Shared Android Devices)

Intune compliance + Device filters



Entra ID Conditional Access Rule

Assignment

Users & Groups:

Shared devices group

Cloud Apps:

Exchange Online

Microsoft Teams

SharePoint Online

Conditions:

Device Platforms

Android

Locations

All trusted locations

Device Scoping Filters

Team Android Device Models

Access Controls

Grant Type:

Grant Access

Controls:

Require Device to be marked as Compliant

Intune

Compliance Policy

Compliance Settings

Rooted Devices: Block
Block Minimum OS: 8.0

Actions for non-compliance

Mark device noncompliant: Immediately

Assignments

Shared Devices Group

Device Scoping Filters

Teams Android Device Models

Teams Admin Validate Success

Teams Admin – Validate Success

Company Portal

Software health

Software type	Current version	Health status
Teams Admin Agent	1.0.0.202407050618.product	Up to date
Firmware	NFA1.20241113.0515	Up to date
Company Portal	5.0.6152.0	Up to date
OEM Agent	1	Up to date
Teams	1449/1.0.97.2024122401	Up to date

AOSP

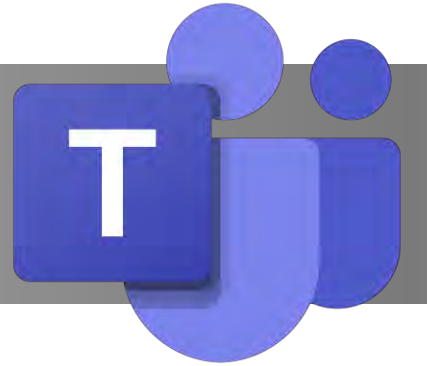
Software health

Software type	Current version	Health status
Teams Admin Agent	1.0.0.202407050618.product	Up to date
Firmware	2.3.480	Up to date
OEM Agent	1.0.160	Up to date
Teams	1449/1.0.94.2024122303	Up to date
Authenticator	6.2410.7268	Up to date
Microsoft Intune	24.09.1	Up to date

Let’s Make It Real!

Drop to Screen Share

Required Teams Device Updates



Action required!

Device AOSP Firmware Change

- Blog and FAQ
- Step-by-step guidance
- Video

AOSP Triggered MFA Change

- Blog and FAQ – Local Login or Adjust CA
- CA Policies – Use Device or Location Filters

Auto Upgrade Begins May 15th

Action required!

Exclude Identities from DCF policy

- Blog
- Step-by-step guidance

Device Teams App Update (by June 2025)

- Phones: 1449/1.0.94.2025020301
- MTRA: 1449/1.0.96.2025020302
- Panels: 1449/1.0.97.2025020502 / 2025021101

Rolling Out Now

Microsoft

Wrap Up!

Questions? Answers? Tomatoes?

Thank you!