



Device Deployment Playbook

Microsoft Teams Devices

Device deployment guidance

This playbook will assist you in delivering Microsoft Teams Devices inside your organization. Example scenarios can include Microsoft Teams Rooms (MTRs), Teams phones, Teams panels, and Surface Hub.

We have organized these resources by activity type, including device selection considerations, deployment activities, and ongoing management and operations. This real-world guidance is augmented by our technical product documentation which can be found at learn.microsoft.com.

For technical support, please open a support case or reach out to your Microsoft account team.



Table of contents

[Devices overview](#)

[Device selection](#)

[Important concepts](#)

[Configurations by device type](#)

[Security & network considerations](#)

[Conditional access / compliance policy examples](#)

[Maintenance & monitoring](#)

Got Feedback?

aka.ms/TeamsDevicePlaybookFeedback

NOTE: This playbook will focus on the most common & best practice methods for deploying/managing/monitoring Teams devices. Custom & complex environments should consult with their account team and/or a partner for support.

Devices overview



What are Teams Devices?

Teams makes it easy to get a portfolio of devices to meet your business needs. This includes plug and play solutions such as headsets, speakerphones, webcams, and monitors, where no extra configuration is required.

Note: This playbook will not address plug and play solutions. For more information, see the following:

<https://learn.microsoft.com/microsoftteams/devices/usb-devices>

Teams also supports a variety of purpose-built Teams enabled devices, such as phones, displays, rooms and panels, which can be deployed as personal devices or as shared devices, to meet the intended usage scenario.

Teams supports a portfolio of [desk phones](#) for users who require a traditional phone experience.






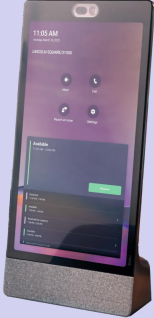
Teams [displays](#) are a category of all-in-one dedicated Teams devices.

Teams [rooms](#) transform meeting spaces ranging from small huddle areas to large conference rooms with a rich, collaborative Teams experiences.

Teams [panels](#) are dedicated Teams devices that display meeting details, typically mounted outside meeting rooms.



Teams devices

Teams Room on Windows	Teams Room on Android	Surface Hub	Panel	Phone	Displays
					
<ul style="list-style-type: none"> • Shared experience • Windows-based 	<ul style="list-style-type: none"> • Shared experience • Android-based 	<ul style="list-style-type: none"> • Personal and shared experience • Windows-based 	<ul style="list-style-type: none"> • Dedicated experience supporting a meeting room • Android-based 	<ul style="list-style-type: none"> • Personal or shared experiences • Android-based 	<ul style="list-style-type: none"> • Personal or shared experiences • Android-based

Tip: The use cases matter

With the broad selection of devices available for Teams, make sure to select an appropriate device to meet your identified business needs.

Personal | Shared



Personal devices experiences extend the features and functionality of Teams using a personal account. These include Teams Phones & Teams Displays.

Shared devices leverage a resource or common user account to deliver use cases leveraged by multiple users. These include Teams Rooms on Windows and Android, Teams Phones configured as common area phones, and Teams Displays configured for hotdesking scenarios.





Teams devices for shared spaces on Windows and Android

Core functionality is available on both platforms so end users can always have great audio and video experiences, use one-touch join to join meetings, and access inclusive features such as live captions and raise hand.

As Microsoft brings new features to Teams and to Teams Rooms, we strive to bring them to all platforms, but features may roll out at different times due to several factors, including things like technical feasibility and customer feedback for each platform. This means you may see some features rolling out on Windows before they come to the Android platform.

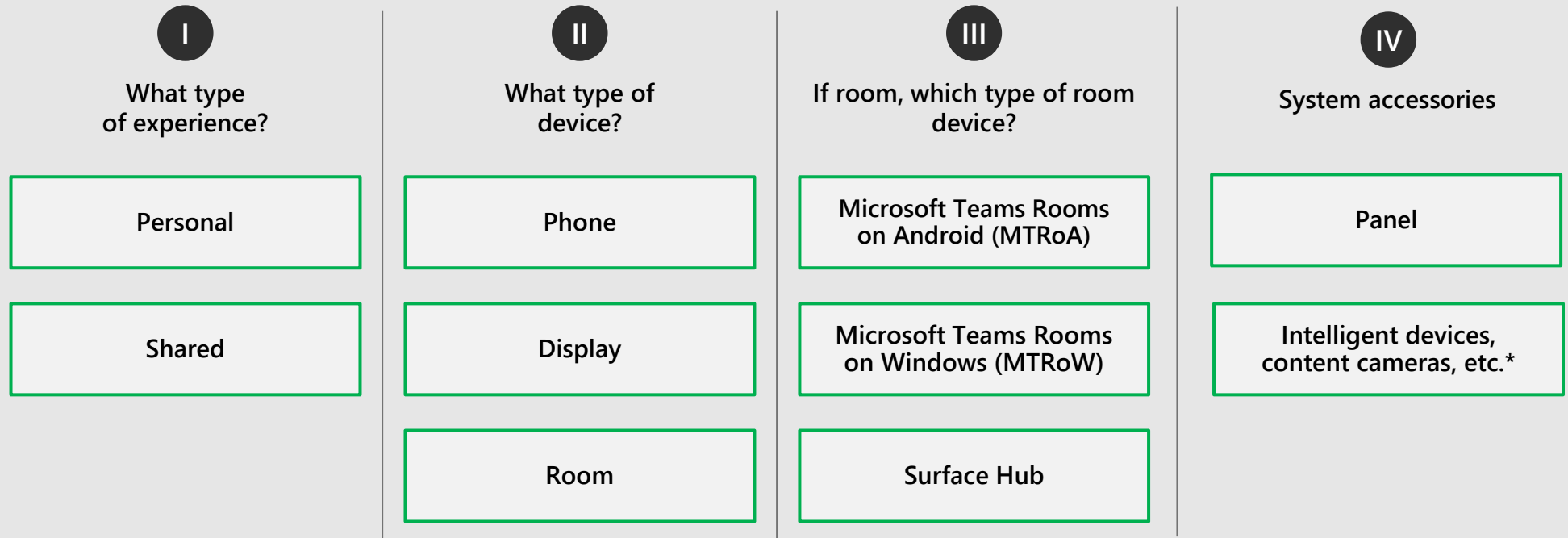
To help guide you as to what features are available on different platforms, you can refer to this [chart](#).

Note: Not all Teams Rooms features will be included on this list, so please continue to consult the [Microsoft 365 roadmap](#) and Microsoft sales representatives for additional details.

Device selection



Selecting your device experience



Device selection examples:

Personal phone: Provide traditional desk phone experiences to single user

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

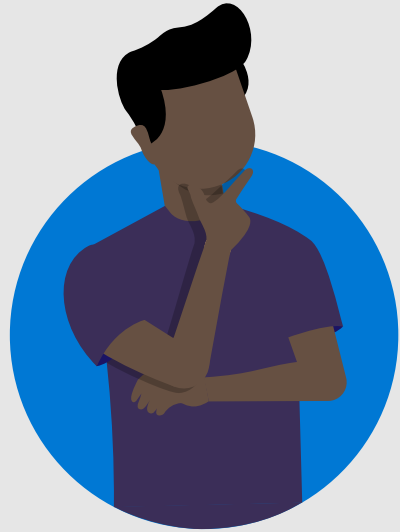
Shared room windows with Panel: Provide enhanced meeting experiences on Windows-based device dedicated to a meeting room, used by multiple users with panel displaying meeting room information mounted near the entry door.

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](#)

Selecting your device experience:

Teams Room on Windows



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

System accessories

Panel

Intelligent devices,
content cameras, etc.

How to
Deploy



Teams Rooms on Windows

- Overview of Teams Rooms on Windows [Click here](#)
- Set Teams account policies for Teams [Click here](#)
- Password expiration disabled [Click here](#)
- Meeting room license assigned [Click here](#)
- Room number assigned [Click here](#)
- AAD groups created and all MTRoW resource accounts are assigned [Click here](#)
- AAD dynamic group created for all devices matching to device name [Click here](#)
- Teams Compliance Policy created and assigned to dynamic device group [Click here](#)
- Conditional access configuration created for MTRoW devices [Click here](#)
- Ensure the AAD device account group is mapped for Teams into Microsoft with MTRoW [Click here](#)



Recommended:
**Teams Room
on Windows**

Provide best in class meeting room experiences

- Bring Teams meetings to any meeting space
- Provides inclusive and interactive meetings
- Flexible deployment options
- Secure by design
- Manageable via Teams Admin Center

Selecting your device experience:

Teams Room on Android



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

System accessories

Panel

Intelligent devices,
content cameras, etc.

How to
Deploy



Teams Rooms on Android

- ✓ Microsoft account enabled. [Click here](#)
- ✓ Set Exchange resource account policies. [Click here](#)
- ✓ Microsoft Exchange Online. [Click here](#)
- ✓ Meeting room license assigned. [Click here](#)
- ✓ Room monitor assigned. [Click here](#)
- ✓ Room authentication test passed. [Click here](#)
- ✓ Android device administrator enabled. [Click here](#)
- ✓ AAD security group created for associated SIs, resource accounts added. [Click here](#)
- ✓ Access compliance policy created and assigned to AAD Group. [Click here](#)
- ✓ Conditional access configured with IP restrictions & device compliance and assigned to AAD group. [Click here](#)

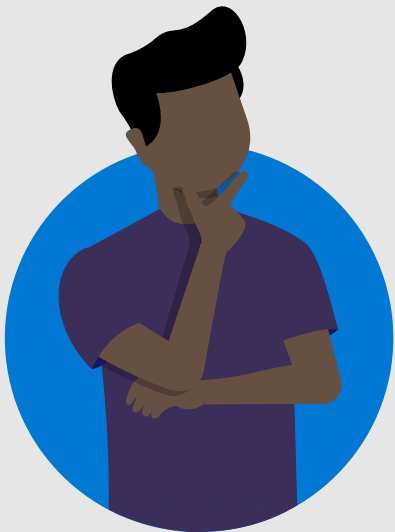


Recommended:
**Teams Room
on Android**

Provide best in class meeting room experiences

- Bring Teams meetings to any meeting space
- Provides inclusive and interactive meetings
- Flexible deployment options
- Secure by design
- Manageable via Teams Admin Center

Selecting your device experience: Surface Hub



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

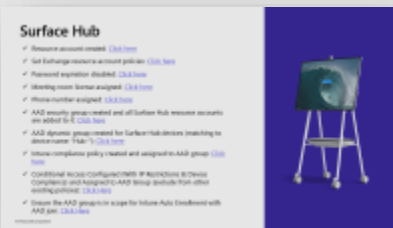
IV

System accessories

Panel

Intelligent devices

How to
Deploy

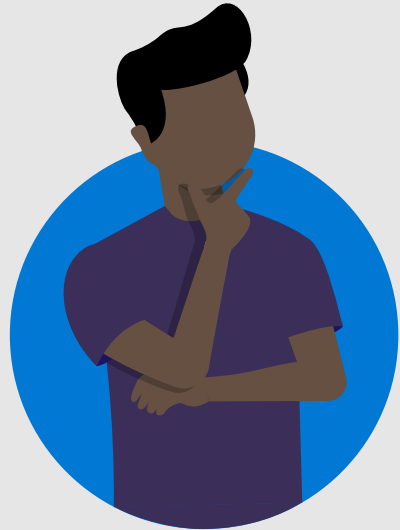


Recommended:
Surface Hub

Provide best in class whiteboard experiences

- Empower people to whiteboard together
- Provides inclusive and interactive meetings
- Makes any place teamwork space with mobile flexibility
- Secure by design
- Manageable via Teams Admin Center

Selecting your device experience: Teams Panel



I
What type
of experience?

Personal

Shared

II
What type of
device?

Phone

Display

Room

III
If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV
System accessories

Panel

Intelligent devices,
content cameras, etc.

How to
Deploy



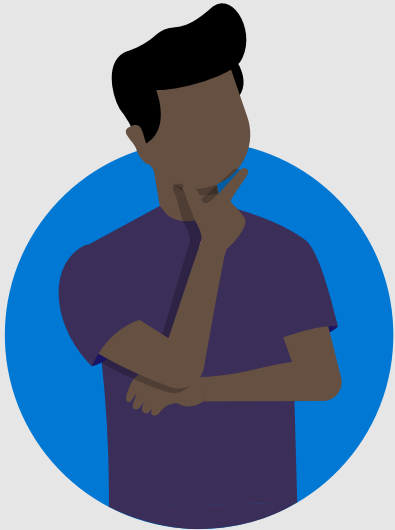

Recommended:
Teams Panel

Provide status information about meeting spaces

- Compact touchscreen device typically mounted outside conference rooms near the entrance
- Can leverage the same Teams Meeting Room account as the meeting space it is deployed for
- Provides a view of location and meeting details at a glance
- Allows reserving of meeting spaces for ad hoc meetings
- Capable of running Microsoft Teams apps and Line of Business (LOB) apps

Selecting your device experience:

Teams Phone (Common Area Phone (CAP) / shared)



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

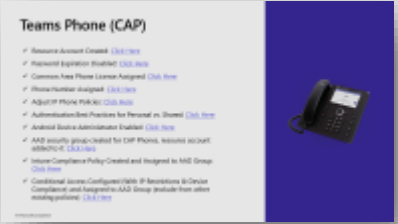
Device considerations

Touchscreen vs physical
buttons

Headset vs handset

Video

How to
Deploy



Recommended:
Teams Phone
(shared)

Provide traditional desk phone experiences for

- Common Area Phones (CAP) such as lobbies and breakrooms
- Shared use areas such as retail stores or manufacturing spaces
- Small huddle rooms that provide dedicated calling experiences
- Supports a wide range of calling features

Selecting your device experience:

Teams Phone (personal)



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

Device considerations

Touchscreen vs physical
buttons

Headset vs handset

Video

How to
Deploy



Teams Phone (Personal)

✓ Android Device Administrator Enabled [Click Here](#)
✓ Remote Access assigned to users that may utilize these devices to ensure compliance with Azure AD and future feature-related updates
✓ Remote Authentication/Shared Practices for Personal vs. Shared [Click Here](#)
✓ Intune Compliance Policy Created and Assigned to All Groups [Click Here](#)
✓ Conditional Access (without MFA) configured if applicable to ensure all devices are compliant with Intune [Click Here](#)



Recommended:
Teams Phone
(personal)

Provide traditional desk phone experiences for

- Users that prefer a physical form factor for voice focused scenarios
- User does not want to use a headset or speakerphone
- May be beneficial in high volume calling user personas
- Offload media to dedicated device separate from primary work device
- Supports a wide range of calling features

Selecting your device experience:

Teams Display (shared/hotdesking)



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

System accessories

Panel

Intelligent Devices,
Content Cameras, etc.

How to
Deploy



Teams Display (Hotdesking)

- ✓ Resource Account Created [\(Link Here\)](#)
- ✓ Set Exchange Resource Account Password [\(Link Here\)](#)
- ✓ Resource Experience Enabled [\(Link Here\)](#)
- ✓ Sharing Teams license assigned [\(Link Here\)](#)
- ✓ Resource Account assigned [\(Link Here\)](#)
- ✓ Android Device Administration Enabled [\(Link Here\)](#)
- ✓ Authentication/Authorization for Personal or Shared [\(Link Here\)](#)
- ✓ AAD security group created for display, resource account subject(s) [\(Link Here\)](#)
- ✓ Intune Compliance Policy Created and assigned to AAD Group [\(Link Here\)](#)
- ✓ Conditional Access Configured/Policy ID Re-evaluated and assigned to AAD Group (include them when existing policies) [\(Link Here\)](#)



Recommended:
Teams Display
(shared/hotdesking)

Provides all-in-one dedicated Teams device experience

- Users that prefer a physical form factor for video and content focused scenarios
- Allows users to reserve temporary workspaces in advance or on demand
- Offload media to dedicated device separate from primary work device
- Companion experience that allows seamless cross-device interaction

Selecting your device experience:

Teams Display (personal)



I

What type
of experience?

Personal

Shared

II

What type of
device?

Phone

Display

Room

III

If room, which type of room
device?

MTRoA

MTRoW

Surface Hub

IV

Device considerations

Touch screen, no
handset

How to
Deploy



Teams Display (Personal)

- ✓ Android Device Administration Enabled [Click Here](#)
- ✓ Mobile Network assigned to users that only utilize these devices to ensure compliance with secure app and phone features detailed below
- ✓ Remote Authentication Method Policy for Personal Use Enabled [Click Here](#)
- ✓ Network Compliance Policy Configured and Assigned to AAD Group [Click Here](#)
- ✓ Conditional Access without IP Restrictions if deployed outside office. In Device Compliance configured and assigned to AAD Group [Click Here](#)



Recommended:
Teams Display
(personal)

Provides all-in-one dedicated Teams device experience

- Users that prefer a physical form factor for video and content focused scenarios
- Join with microphone, camera, and speakers (or Bluetooth headset)
- Offload media to dedicated device separate from primary work device
- Companion experience that allows seamless cross-device interaction
- Hands-free Teams interactions using Cortana

Important concepts



What are Certified Devices?

The Microsoft Teams Devices Certification Program ensures certified devices meet a high standard, with higher performance targets and quality metrics across the entire Teams experience (audio, video, user interface). Microsoft and Original Equipment Manufacturer (OEM) partners are actively working together to ensure devices meet all certification requirements, including security, audio and video quality, Teams experience, and accessibility.

For devices running Android: Certification end dates are based on the Android OS version running on the device when it enters the certification program. Our OEM partners are working to extend the lifetime of the certification by upgrading the Android OS version and re-certifying, or by releasing new models that are state-of-the-art. Beyond the certification period, Microsoft is committed to make efforts to support the most recent version of the Teams client on such devices for two years following the end of the certification period.

Device certification information:

- ✓ Certified Teams Room on Windows (and peripherals): [Click here](#)
- ✓ Certified Teams Rooms on Android: [Click here](#)
- ✓ Certified Surface Hub Accessories: [Click here](#)
- ✓ Certified Teams Panels: [Click here](#)
- ✓ Certified Teams Phones: [Click here](#)
- ✓ Certified Teams Displays: [Click here](#)

Teams Devices Management Portals

Microsoft 365
Admin Center

Teams Admin
Center

Microsoft
Endpoint
Manager
Portal

Azure Active
Directory
Portal

Exchange
Admin Center

OEM
Management
Portal (per OEM)

Microsoft Teams
Room Pro Portal
(Pro License)



Considerations at Scale

Design

- Create a set of standards for your deployment that use case requirements for each type of space.
- Leverage certified devices for all deployments for the best experience
- Understand dependencies, map any partner teams, and engage as required for a successful deployment

Implement

- Have processes understood and tested for implementation and problem resolution
- Engage on-site hands and plan resources to physically deploy as early as possible.

Monitor

- Create standard operating procedures for monitoring the performance of devices, using tools such as the Quality of Experience Report for Devices (aka.ms/qerpbitemplates)



Configurations by device type



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](#)
- ✓ AAD security group created and all MTRoW resource accounts are added to it: [Click here](#)
- ✓ AAD dynamic group created for MTR devices (matching to device name: "MTR-"): [Click here](#)
- ✓ Intune Compliance Policy Created and Assigned to dynamic device group: [Click here](#)
- ✓ Conditional access configured (with IP restrictions & device compliance) and assigned to resource account group (exclude from other existing policies): [Click here](#)
- ✓ Ensure the AAD resource account group is in scope for Intune auto enrollment with AAD join: [Click here](#)



Teams Rooms on Windows (cont.)

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

- ✓ How to join to Azure AD & Intune: [Click here](#)
- ✓ Set the system name (MTR-SerialNumber): [Click here](#)
- ✓ Configure PowerShell script to change the default local admin password: [Click here](#)
- ✓ Create an AAD 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 AAD admin group to all MTRs: [Click here](#)
- ✓ If using Managed Services, you can set the Teams Room Managed Service Installer & Key configured to deploy via Intune scoped to your device AAD group: [Click here](#)
- ✓ Set proxy settings: [Click here](#)
- ✓ Deploy certificates: [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](#)
- ✓ AAD security group created for Android MTRs, resource account added to it: [Click here](#)
- ✓ Intune compliance policy created and assigned to AAD Group: [Click here](#)
- ✓ Conditional access configured (with IP restrictions & device compliance) and assigned to AAD group (exclude from other existing policies): [Click here](#)



Surface Hub

- ✓ 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](#)
- ✓ AAD security group created and all Surface Hub resource accounts are added to it: [Click here](#)
- ✓ AAD dynamic group created for Surface Hub devices (matching to device name: "Hub-"): [Click here](#)
- ✓ Intune compliance policy created and assigned to AAD group: [Click here](#)
- ✓ Conditional Access Configured (With IP Restrictions & Device Compliance) and Assigned to AAD Group (exclude from other existing policies): [Click Here](#)
- ✓ Ensure the AAD group is in scope for Intune Auto Enrollment with AAD join: [Click Here](#)



Surface Hub (cont.)

These items are intended to further manage your Surface Hub deployment and speed up the deployment time:

- ✓ Create a device restriction profile: [Click Here](#)
- ✓ Create an AAD security group and add user accounts you want to have administrative access on your Surface Hubs: [Click Here](#)
- ✓ Add AAD security group as Admin on the Hubs: [Click Here](#)
- ✓ Set Surface Hub into Teams Only mode: [Click Here](#)
- ✓ Configure Teams Application Settings: [Click Here](#)
- ✓ Configure 802.1x network authentication: [Click Here](#)
- ✓ Install progressive web apps: [Click Here](#)
- ✓ Customize the start menu: [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](#)
- ✓ AAD group created for Teams Panels, resource account added to it: [Click Here](#)
- ✓ Intune Compliance Policy Created and Assigned to AAD Group: [Click Here](#)
- ✓ Conditional Access Configured (With IP Restrictions & Device Compliance) and Assigned to AAD 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](#)
- ✓ AAD security group created for CAP Phones, resource account added to it: [Click Here](#)
- ✓ Intune Compliance Policy Created and Assigned to AAD Group: [Click Here](#)
- ✓ Conditional Access Configured (With IP Restrictions & Device Compliance) and Assigned to AAD 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 Azure AD and Intune features detailed below.
- ✓ Review Authentication Best Practices for Personal vs. Shared: [Click Here](#)
- ✓ Intune Compliance Policy Created and Assigned to AAD Group: [Click Here](#)
- ✓ Conditional Access (without IP restrictions if deployed outside office) & Device Compliance configured and Assigned to AAD Group: [Click Here](#)



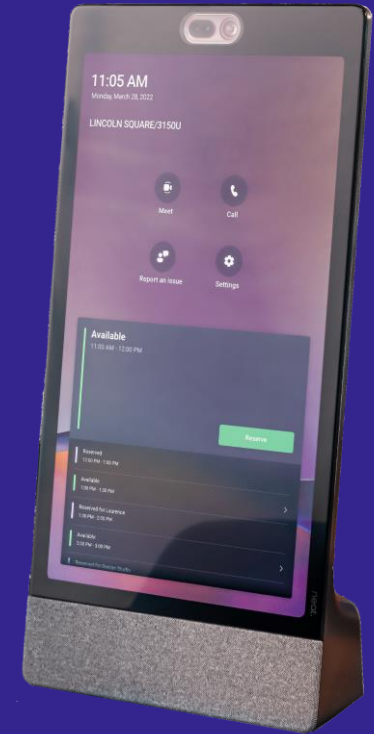
Teams Display (Hotdesking)

- ✓ 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](#)
- ✓ Android Device Administrator Enabled: [Click Here](#)
- ✓ Authentication Best Practices for Personal vs. Shared: [Click Here](#)
- ✓ AAD security group created for displays, resource account added to it: [Click Here](#)
- ✓ Intune Compliance Policy Created and Assigned to AAD Group: [Click Here](#)
- ✓ Conditional Access Configured (With IP Restrictions) and Assigned to AAD Group (exclude from other existing policies): [Click Here](#) & [Click Here](#)



Teams Display (Personal)

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



Security & Network Considerations



Security Considerations

- Resource Accounts:
 - Do not enforce password expiration
 - Do not enforce multi-factor authentication through another device (push notification, text, phone call, etc), instead leverage known location and/or device compliance as the second factor to secure accounts
- Conditional Access:
 - Resource accounts should be excluded from user CA policies and have unique policies created to ensure the resource accounts are locked down appropriately
 - Consider device filters to apply your CA policies
- Local Device Security:
 - Ensure all local administrative passwords are changed during setup
 - Teams Rooms performance is tested with Microsoft Defender. Disabling this or adding other endpoint security software is not supported as it can lead to unpredictable results and potential system degradation
- Administrative Portals:
 - Only grant those who need access to manage devices access to the Teams Admin Center & Managed Service portals and scope those permissions to specific devices.

Network Connectivity Requirements & Considerations

	Teams Room on Windows	Teams Room on Android	Surface Hub	Teams Panels	Teams Phone	Teams Display
Microsoft Teams	Required	Required	Required	Required	Required	Required
Microsoft Office 365	Required	Required	Required	Required	Required	Required
Microsoft Intune	Required	Required	Required	Required	Required	Required
Microsoft Store	Required	N/A	Required	N/A	N/A	N/A
Windows Update	Required	N/A	Required	N/A	N/A	N/A
Pro Portal	Optional	Optional	Optional	N/A	N/A	N/A
Azure Monitor	Optional	N/A	Optional	N/A	N/A	N/A
Unauthenticated Proxy	Optional	Optional *	Optional	Optional *	Optional *	Optional *
Authenticated Proxy	N/A	N/A	N/A	N/A	N/A	N/A
QoS	Optional	Optional	Optional	Optional	Optional	Optional
802.1x	Optional	Optional *	Optional	Optional *	Optional *	Optional *
Bandwidth Policy	10 mbps	10 mbps	10 mbps			

Conditional Access / Compliance Policy Examples



Conditional Access with Teams Devices

Teams Devices support integration with Conditional Access in Azure Active Directory.

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:

- Personal versus Shared Android Devices
- 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](#)

Understanding Intune Enrollment

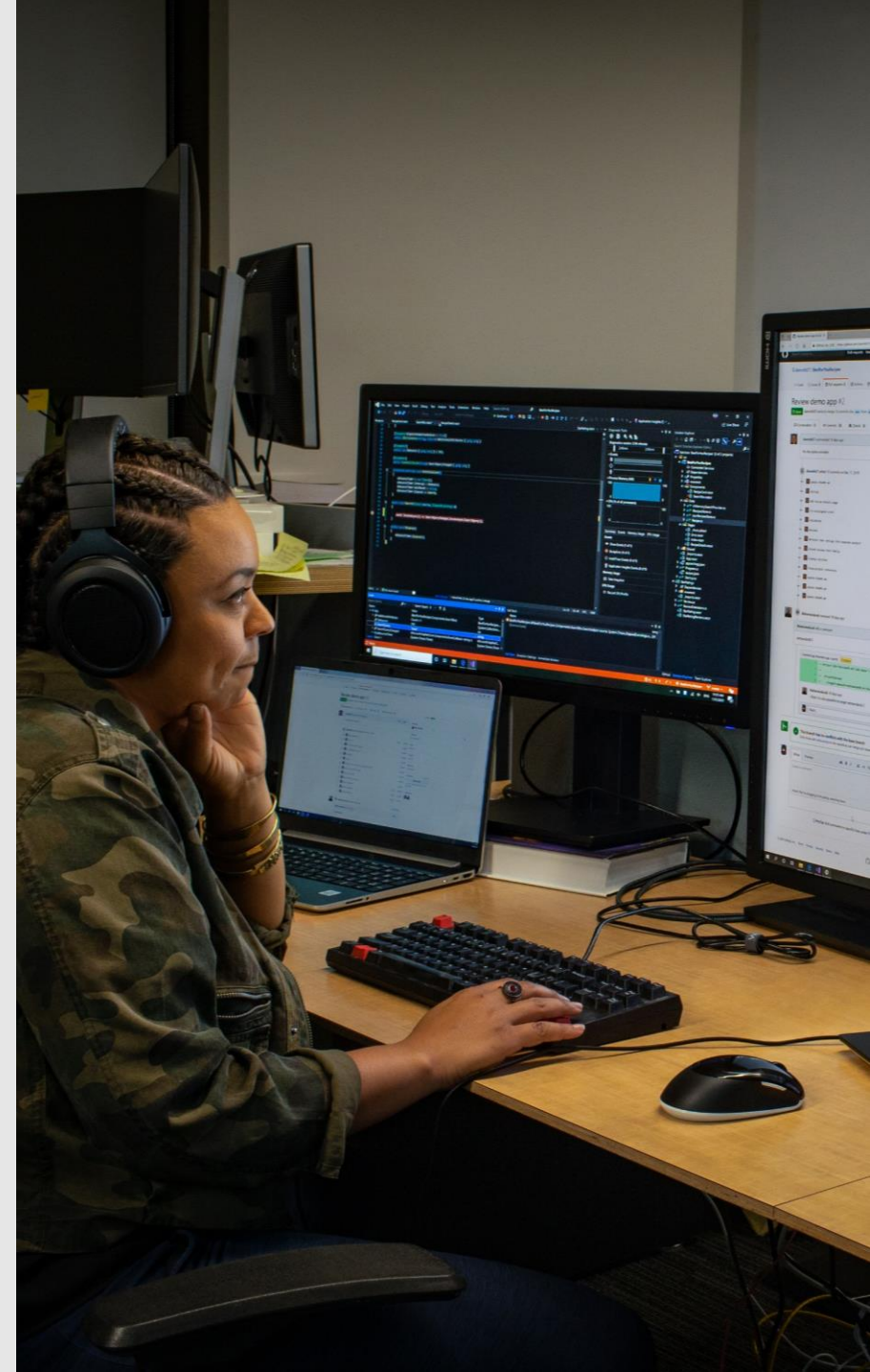
Android enrollment

- 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

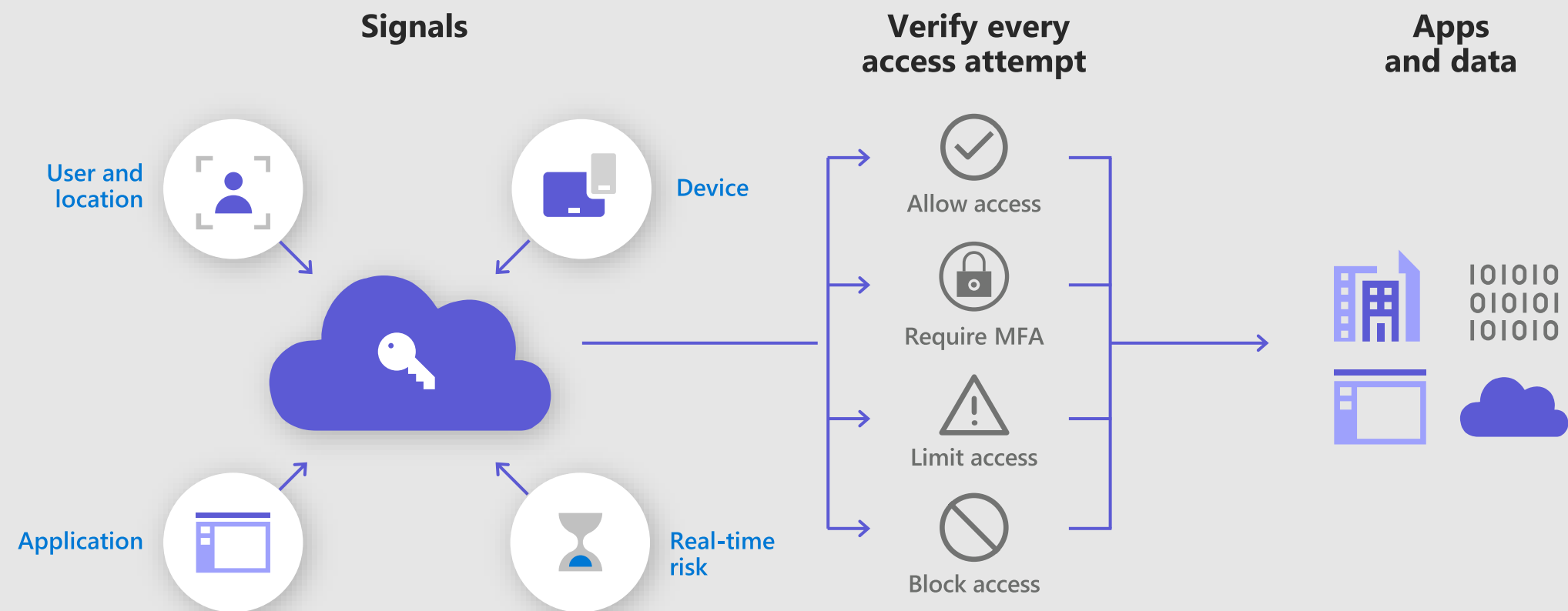
Windows enrollment

- Leverages existing Windows 10 IoT 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](#)

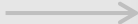



Illustrating Conditional Access with Teams Devices



Shared devices conditional access (Windows Devices)

Intune compliance + Trusted location









Azure Active Directory 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






Azure Active Directory 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

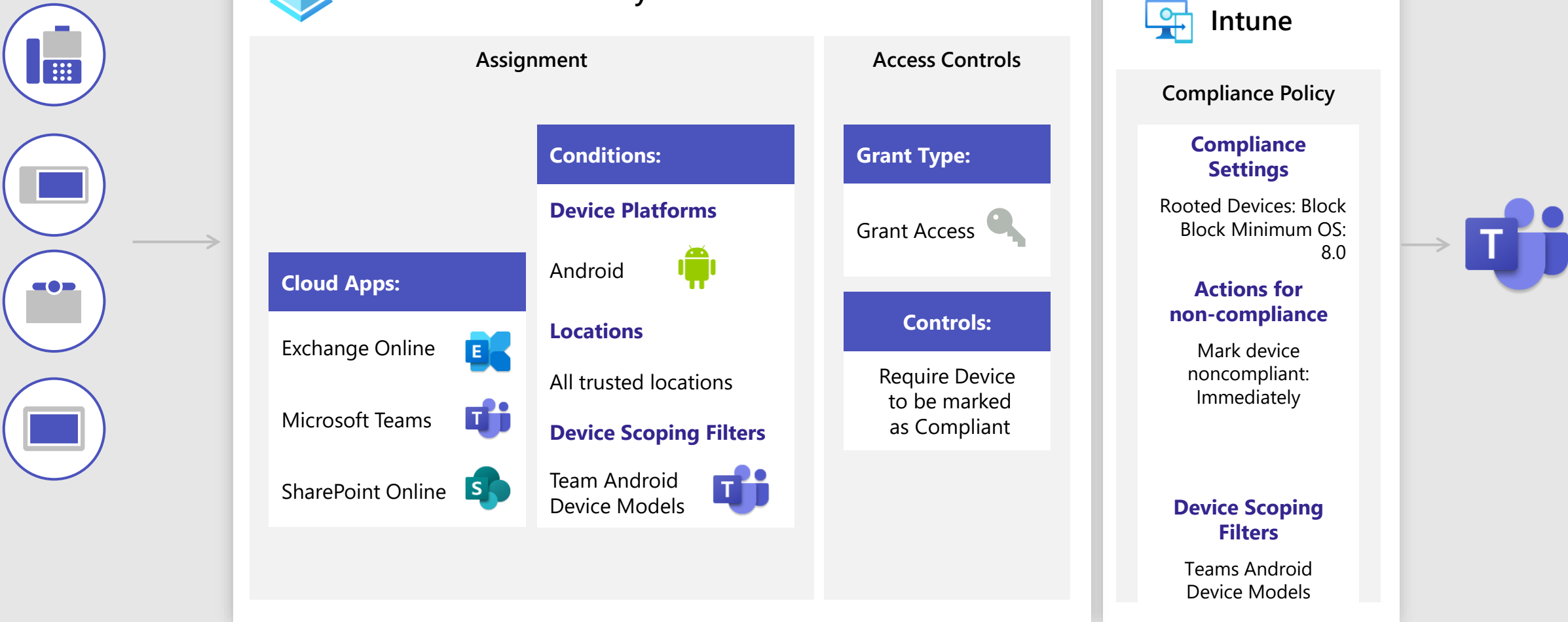
Device Scoping Filters

Teams Android Device Models



Shared devices conditional access (Personal Android Devices)

Intune compliance + Device filters



Maintenance & Monitoring



Monitoring Teams Devices

I	II	III	IV	V	VI
Teams Room on Windows	Teams Room on Android	Surface Hub	Teams Panel	Teams Phone	Teams Display
Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center
Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal
Azure Monitor	Azure Monitor	Azure Monitor	Azure Monitor	Azure Monitor	Azure Monitor
3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools



Recommended:
Teams Admin Center
& Pro Portal

Monitor & Ensure Stability of Your Devices

- Ensure you are always running the latest certified Teams device software & firmware
- Know when your devices are online or offline
- Monitor connected peripherals
- Proactive solutions to resolve issues with your devices
- Role based access control to ensure the right people monitor the right devices

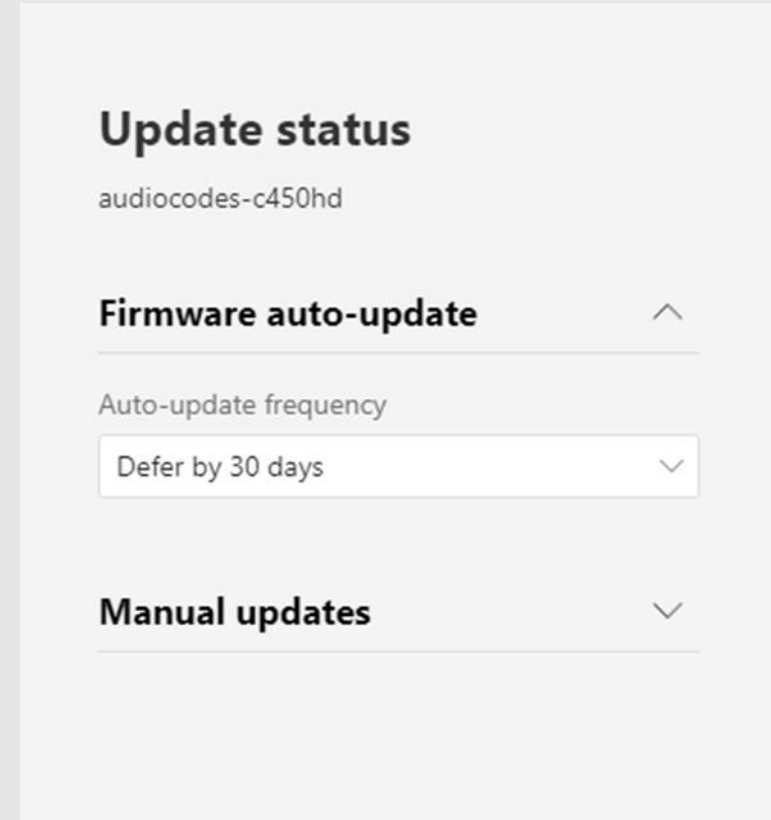
Available
Coming Soon
Not Available

Managing Teams Devices

I	II	III	IV	V	VI
Teams Room on Windows	Teams Room on Android	Surface Hub	Teams Panel	Teams Phone	Teams Display
Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center	Teams Admin Center
Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal	Teams Rooms Pro Portal
Configuration Files	Configuration Files	Configuration Files	Configuration Files	Configuration Files	Configuration Files
Intune	Intune	Intune	Intune	Intune	Intune
Group Policy	Group Policy	Group Policy	Group Policy	Group Policy	Group Policy
AD / AAD	AAD	AD / AAD	AAD	AAD	AAD
SCCM	SCCM	SCCM	SCCM	SCCM	SCCM
3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools	3rd Party Tools
	Recommended	Available	Coming Soon	Not Available	

Keeping Teams Devices Up to Date

- Teams Room on Windows Devices:
 - The MTR will automatically pull Teams Room app updates from the Microsoft Store
 - The MTR will automatically download Windows Updates
 - Updates will be applied during maintenance cycle (2:30AM Local Time Zone)
- Teams Android Devices
 - Teams Admin Center will automatically push Android firmware N-1 once released
 - Immediate / 30 Day / 90 Day options
 - Teams app updates must be manually installed if they are deployed separately from firmware
- Surface Hub
 - The Surface Hub will automatically pull Teams Room app updates
 - The Surface Hub will automatically download Windows Update



The screenshot shows the 'Update status' page for a device named 'audiocodes-c450hd'. It features a section for 'Firmware auto-update' with an expandable dropdown menu. The dropdown is currently open, showing the 'Auto-update frequency' setting, which is set to 'Defer by 30 days'. Below this, there is a section for 'Manual updates', also with an expandable dropdown menu.

Update status
audiocodes-c450hd

Firmware auto-update ^

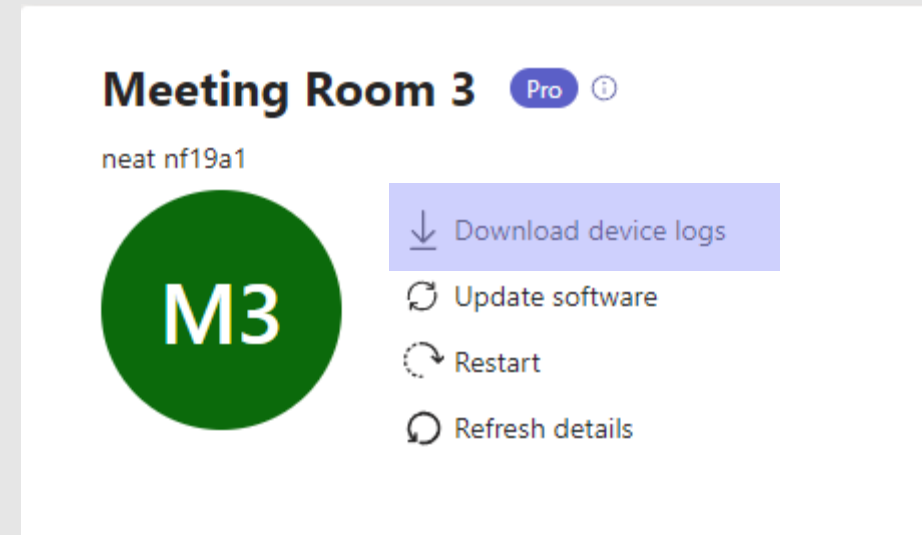
Auto-update frequency

Defer by 30 days v

Manual updates v

Investigating Issues

- Open Support Case
- Provide logs from device to support engineer
- To download logs from Teams Devices
 - Use Teams Admin Center to download device logs
 - Use Teams Rooms Pro Portal to download device logs
 - Use PowerShell script to collect device logs on MTRoW
 - USB drive to collect logs from Surface Hub



Teams Admin Center or Teams Rooms Pro Portal

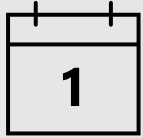
Teams Admin Center

- View all Teams Devices in a single location
- Monitor online/offline status of devices
- Device alert policies
- Set device configuration settings
- Restart devices remotely
- Download device log files
- Manage updates for Android devices
- Group multiple devices together for management
- View real-time call analytics
- View meeting activity and usage details

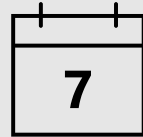
Teams Rooms Pro Portal

- Supports MTRoW (Surface Hub & MTRoA coming soon)
- Room planning to understand inventory & make decisions
- Controlled update rings
- Restart devices remotely
- Set device configuration settings
- Threat protection with Windows Defender for Endpoint
- Orchestrated security updates
- Service Now integration
- Health, reliability, and utilization insights
- Role-based Access Control

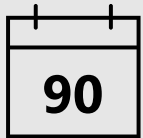
Day in the Life of a Teams Device Admin



- Monitor for configured Device State Alerts from Teams Admin Center
- Monitor for *Actions Required* from the Teams Room Pro Portal
- As needed, onboard new Teams devices



- Ensure you have [installed](#) the latest version of the QER MTR Power BI template
- Review QER MTR Power BI for MTR health and user experience issues and remediate
- Sign on to the Teams Room Pro Portal and confirm updates are applying successfully and no issues need to be addressed
- Sign on to Teams Admin Center and confirm devices are updated and no issues need to be addressed
- Review new Teams Room software releases for [MTRoW](#) and [MTRoA](#)
- Review [What's New In Teams Devices](#) for a complete list of updates
- Review the [Microsoft 365 Roadmap](#) for planned and released MTR features
- Review the [Teams blog](#) for insights into new and upcoming features and announcements for Teams, including MTR



- Proactive Physical Inspection of Devices



Thank you

Got Feedback?

aka.ms/TeamsDevicePlaybookFeedback