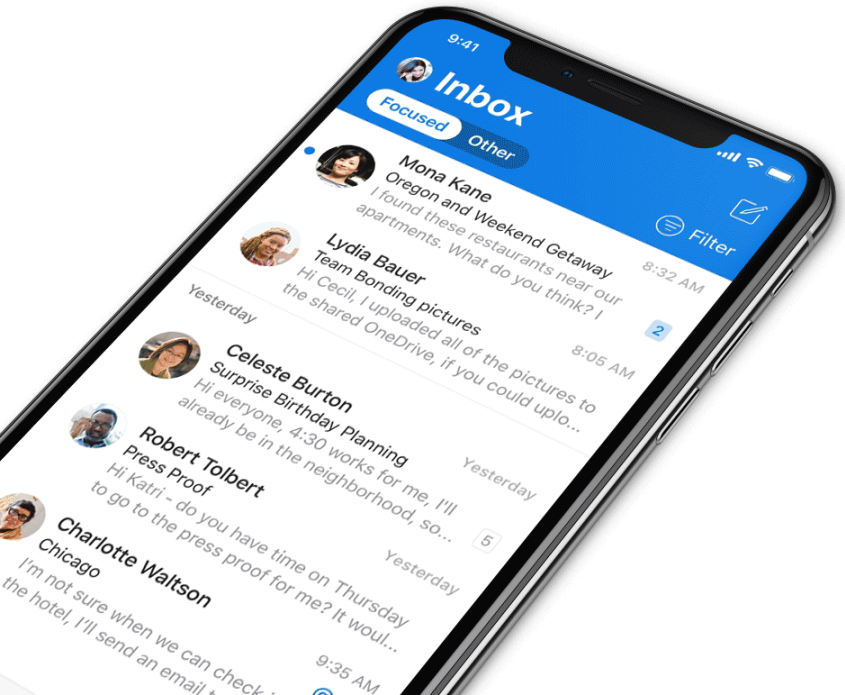
Microsoft Teams Phone Summit - Day 2 am

Using Intune when Deploying Teams Phone Devices

Traci Herr

Digital Event Code of Conduct for Microsoft Webinars:



Microsoft's mission is to **empower every person and every organization on the planet to achieve more**. This includes all Microsoft events and gatherings, including on digital platforms, where we seek to create a respectful, friendly, fun and inclusive experience for all participants.

- We expect all digital event participants to uphold the principles of this Code of Conduct, which covers the main digital event and all related activities. We do not tolerate disruptive or disrespectful behavior, messages, images, or interactions by any party participant, in any form, at any aspect of the program including business and social activities, regardless of location.

- Microsoft will not tolerate harassment or discrimination based on age, ancestry, color, gender identity or expression, national origin, physical or mental disability, religion, sexual orientation, or any other characteristic protected by applicable local laws, regulations, and ordinances.

We encourage everyone to assist in creating a welcoming and safe environment.

We will mute your microphone for the session

Ask your questions via chat, we will get to all of them, live or after. Common questions will get addressed out loud.

We will be posting all recordings to the Microsoft CommUnity Connection YouTube channel approximately 2-3 days after the session has finished. Subscribe here to get updates
https://www.youtube.com/@TeamsPhoneCommUnity

Teams Phone Summit Schedule

Tuesday, March 5th	Wednesday, March 6	Thursday, March 7
10:00am – 11am EST Teams Reporting and Analytics	**10:00am – 11am EST** Using Intune when Deploying Teams Phone Devices	**10:00am – 11am EST** Exploring AI Innovation in Teams Phone with Copilot and Teams Premium
1:00pm – 2:00pm EST Adoption Change Management with Teams Phone Deployment	**1:00pm – 2:00pm EST** Teams Phone Roadmap	**1:00pm – 2:00pm EST** Teams Phone Devices for your Organization

aka.ms/TeamsPhoneSummitReg

Using Intune when Deploying Teams Phone Devices

Traci Herr – Sr Support Escalation Engineer at Microsoft

Wednesday March 6th, 10 am EST

About Me – Traci Herr

- Sr. Escalation Engineer
- Lead for North America Teams Device Escalation team
- Voice and Teams Device SME
- MSFT Certified Trainer (MCT)
- 20+ years with OCS, Lync, Skype, Teams & Telcom

Blog https://ucmess.wordpress.com

Twitter @skypechick

LinkedIn https://linkedin.com/in/traciherr

Agenda

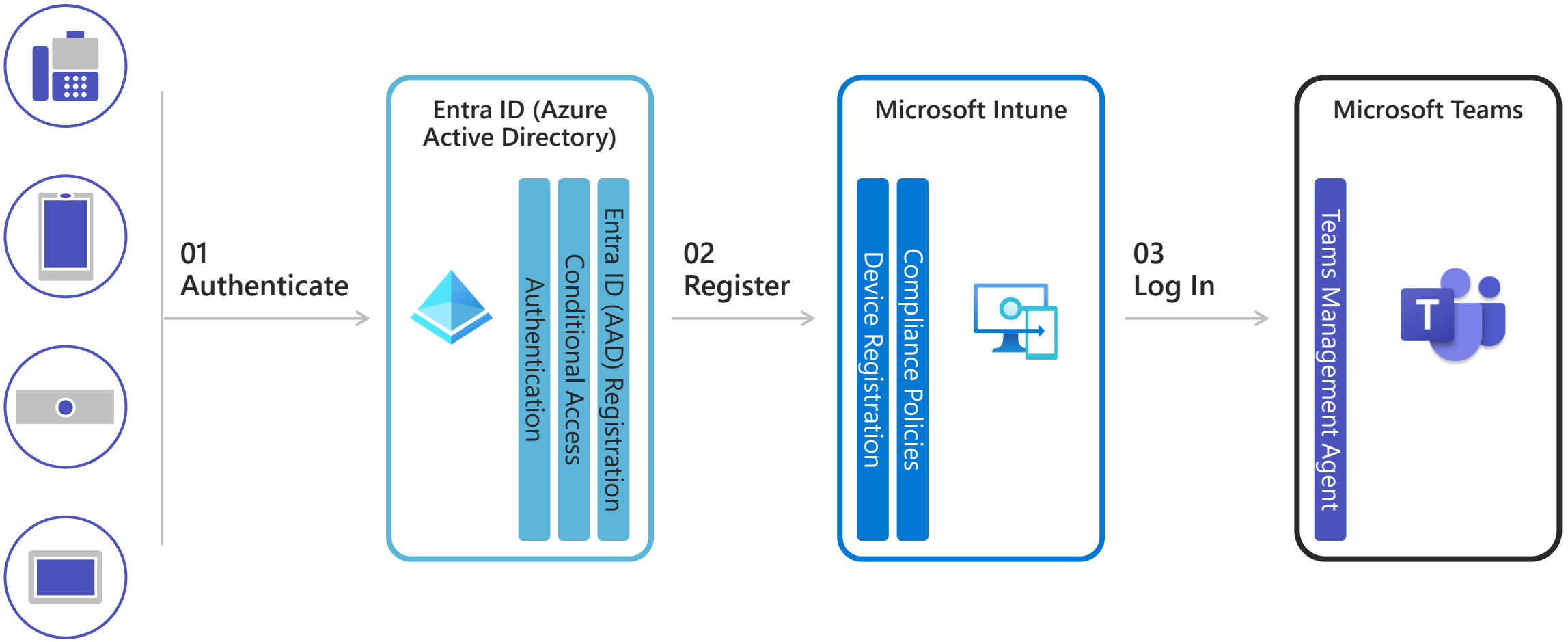
Teams Android devices Sign-in

AAD Authentication and Conditional Access

Intune with Teams Android Devices

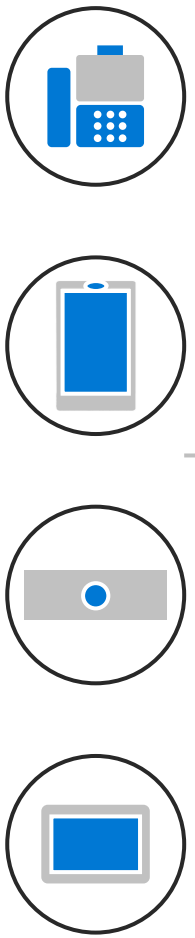
How to Troubleshoot

Sign-in and registration components



Shared devices conditional access

Intune compliance + Device filters



Entra ID (Azure AD) 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: 5.0

Actions for non-compliance

Mark device noncompliant: Immediately

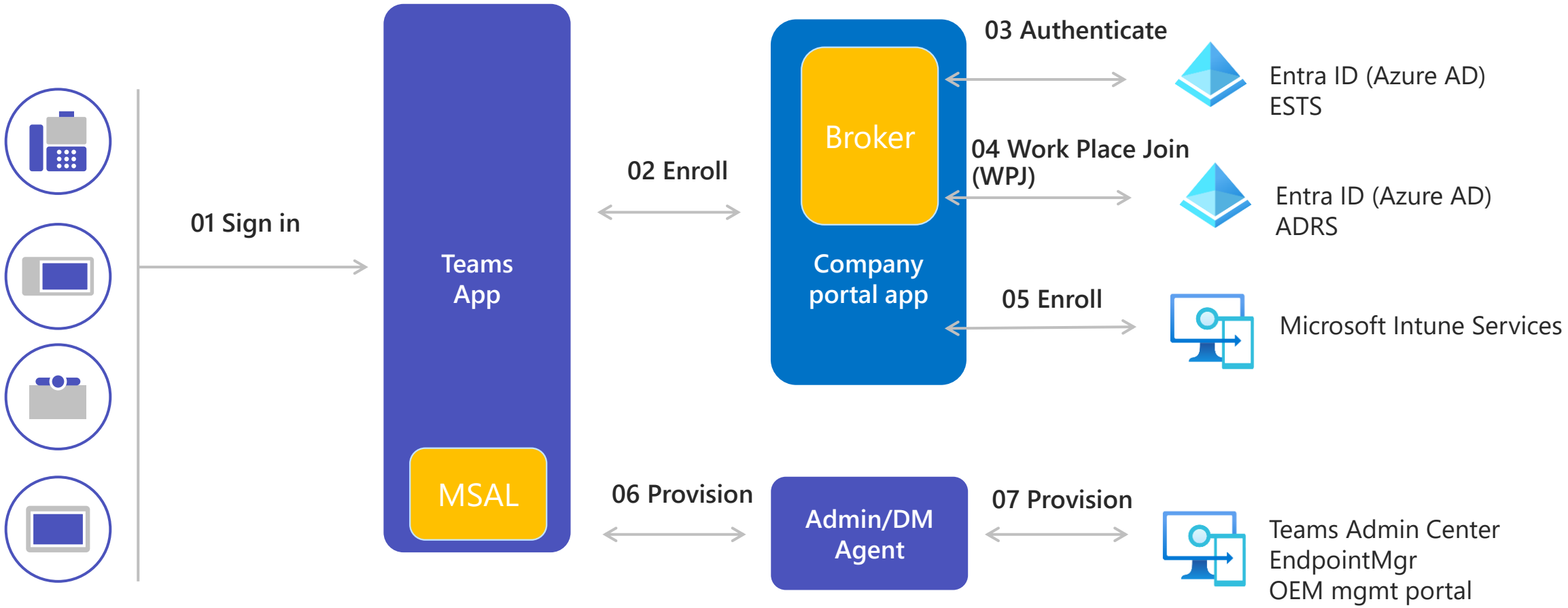
Assignments

Shared Devices Group

Device Scoping Filters

Teams Android Device Models

Inside your Phone or MTR
Sign in and registration flow with username/password



Intune

Android Fundamentals

- There are two basic models of management of an Android device.

  Android Device Administrator – this is 'legacy' but applies to nearly every device. Provides a very basic level of management of a device.

  Because this is the legacy method, general guidance to customers is to migrate away from it. This causes some confusion because it is the way we will manage Teams devices.

  Android Enterprise – this is the modern approach, but requires OEMs to bundle some Google services with their devices.

  There are many different types of management model under the Android Enterprise heading.

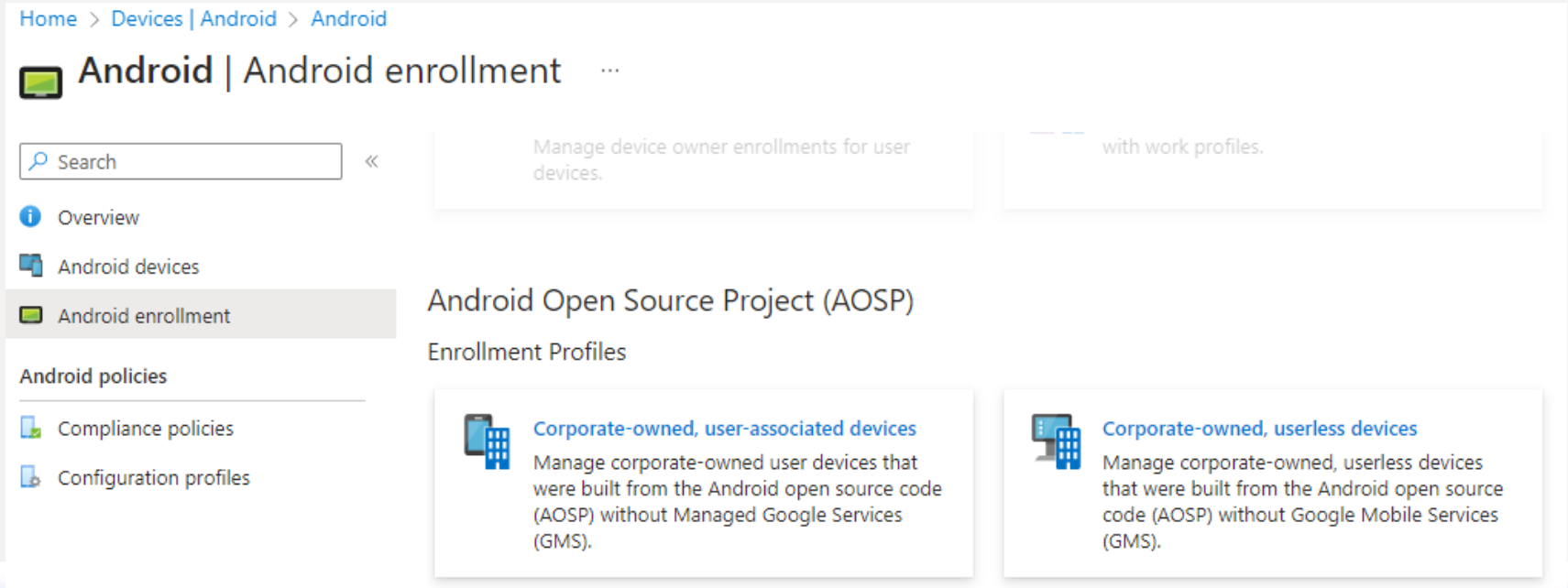
  Teams devices don't support Android Enterprise so we won't go into more detail – but – customers may use terms like COPE (Corporate-Owned, Personally Enabled), Fully Managed, COBO (corporate-owned, business-only) – these are all variants of Android Enterprise management.

Teams Phone Devices Updates

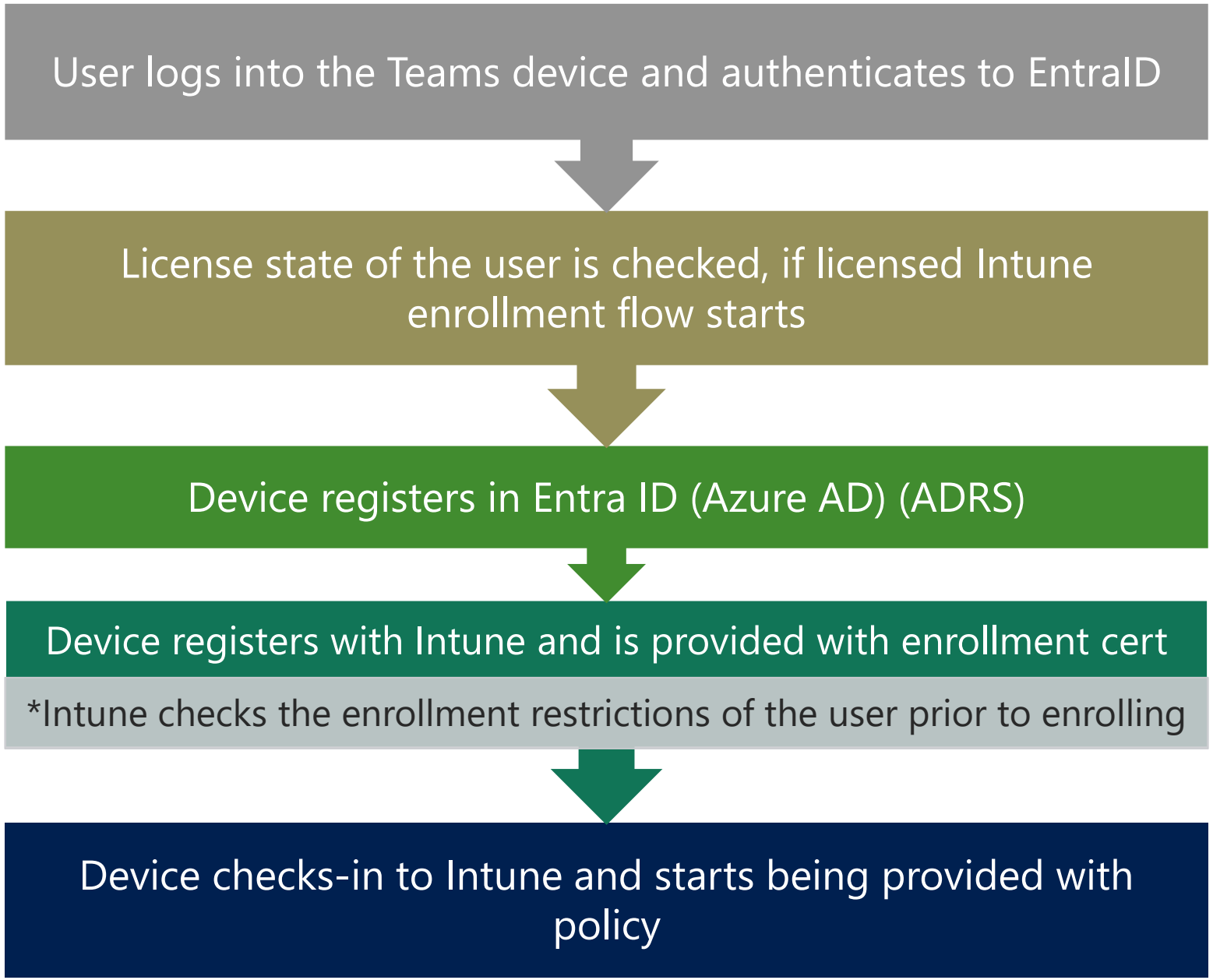
COMING SOON

Device Management via Intune AOSP

Intune's latest Android (AOSP) management solution for Teams Devices will be available later this year.



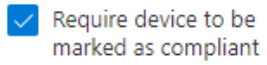
Enrollment Flow



Understanding Intune Enrollment Options

- Customers can enforce enrollment of devices generally via Conditional Access policy

- Secondary to this for Teams devices, if the user is licensed for Intune and they attempt to login to a Teams device, they will be *forced* to enroll
  - *If the enrollment fails, the user is pushed back to the login prompt and the device will be unusable until they are able to enroll*



- There is no option on this – some admins may not wish to enroll but the only way to achieve that is to remove the user license which impacts all their devices

Check your understanding…

- Why might an administrator have blocked Device Administrator enrollment?
- Which firewall ports need to be opened for a device to communicate with Intune?
- How could you check a user's license status?
- How could you troubleshoot a device enrollment failure?
- If you receive a Device Cap Limit reached error what has happened?
- How does a device authenticate to the Intune service?
- What happens if a teams device fails enrollment when an Intune licensed user attempts to logon?

Configuring Devices

- Intune has two types of policy for configuring devices
  Configuration Profile
  Compliance Policy
  App Protection Policy
- Teams devices can consume both but we are primarily interested in Compliance Policy because this drives how Conditional Access is evaluated on a device
- Intune Configuration Profiles are not recommended to be used with Teams devices.
- App Protection Policies are not supported with Teams devices and will break them if in conjunction with CA.

Using Assignment Filters with Intune Policy

- Not all devices support all compliance settings – for Teams devices particularly, encryption can be troublesome.
- Admins have the control to add Assignment Filters on each policy that contains unsupported settings for Teams devices.
- An assignment filter allows the admin to determine applicability of a policy at the point of device check-in. This means you can do compound targeting e.g. apply this policy to this user *when using this device*

Conditional Access

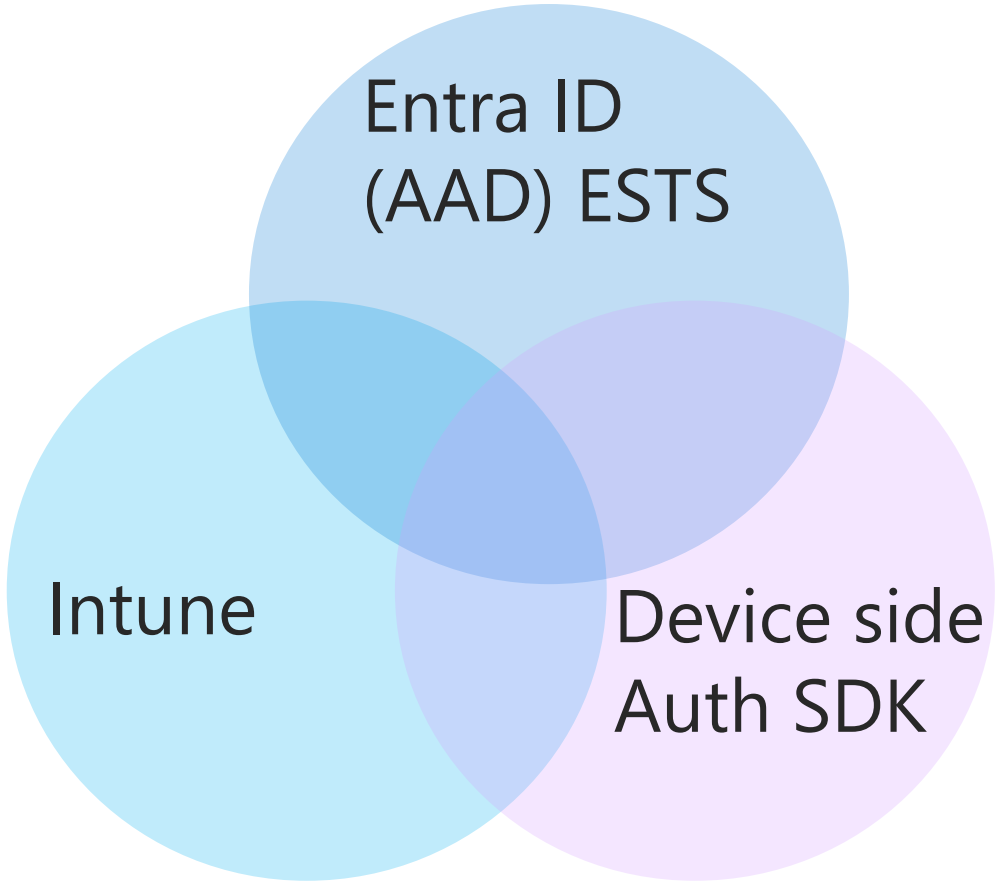
Understanding Conditional Access

- Conditional Access is an Entra ID (AAD) feature that allows authentication to be granted to a resource assuming certain conditions are met
- One of these options is to require the user to be using a managed, compliant device

  This is attractive to admins because it means they can ensure that corporate data is only being accessed on a device that (e.g.) is encrypted or has a passcode set
- There are many other CA options that can be set which are entirely independent of Intune (e.g. require MFA)

Understanding Conditional Access

Conditional access works by bringing Entra ID (AAD), Intune and device side auth code together to present the solution.



Conditional Access and Intune

- Intune manages the setting of the ‘IsCompliant’ property on the Entra ID (AAD) device object
- Only Intune can configure this property*
- When the user attempts to authenticate, the client sided auth code needs to hand up the Entra ID (AAD) device id for the device at the same time. Device Code Flow (DCF)
- With this information, ESTS can check to see if the device is marked ‘IsManaged’==True and ‘IsCompliant’==True
- Validation of these properties happens at the point of authentication only – if the device is granted an auth token the next evaluation will be when a new token is requested

Conditional Access and Enrollment

- There is a built-in exception to the ‘require compliant device’ requirement in CA on Intune device enrollment
- This is designed to prevent the chicken-and-egg scenario of not being able to enrol to become compliant because you aren’t compliant.

Conditional Access Filter for Devices

- **Use it on every existing policy** that has unsupported settings for the Teams Android Devices
- Affects Entra ID (AAD) Device Objects only
- This will make your life better…I promise!

Teams Phones

Conditional Access policy

Delete | View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Teams Phones

Assignments

Users

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

3 conditions selected

Access controls

Grant

1 control selected

Session

Sign-in frequency - 2 hours

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

Not configured

Sign-in risk

Not configured

Device platforms

1 included and 1 excluded

Locations

2 included

Client apps

Not configured

Filter for devices

Exclude filtered devices

Enable policy

Report-only | On | Off

Save

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure

Yes | No

Devices matching the rule:

- ○ Include filtered devices in policy
- ◉ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	model	In	c450hd, mp56, trio8800, ccx600, trioc60, polytc8
Or	model	In	ccx500, polystudiox50
Or	manufacturer	Contains	poly
Or	model	Contains	lenovocd-18781y
Or	manufacturer	Contains	logi
Or	manufacturer	Contains	Neatframe
Or	displayName	Starts with	Poly
Or	displayName	Starts with	Lenovo
Or	displayName	Starts with	AudioCodes
Or	displayName	Starts with	Yealink

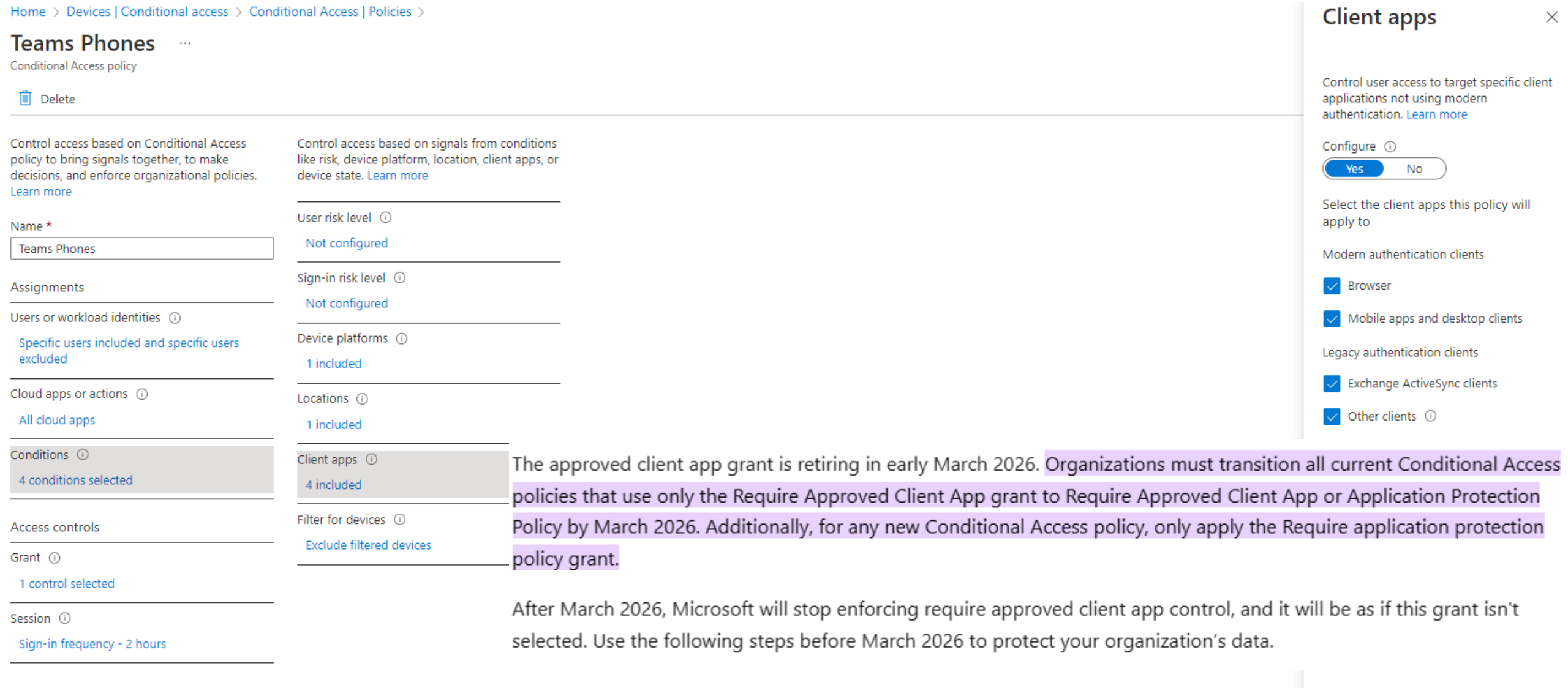
+ Add expression

Rule syntax

Edit

```
device.model -in ["c450hd","mp56","trio8800","ccx600","trioc60","polytc8"] -or device.model -in ["ccx500","polystudiox50"] -or device.manufacturer -contains "poly" -or device.model -contains "lenovocd-18781y" -or device.manufacturer -contains "logi" -or device.manufacturer -contains "Neatframe" -or device.displayName -startsWith "Poly" -or device.displayName -startsWith "Lenovo" -or device.displayName -startsWith "AudioCodes" -or device.displayName -startsWith "Yealink"
```

Done



The approved client app grant is retiring in early March 2026. Organizations must transition all current Conditional Access policies that use only the Require Approved Client App grant to Require Approved Client App or Application Protection Policy by March 2026. Additionally, for any new Conditional Access policy, only apply the Require application protection policy grant.

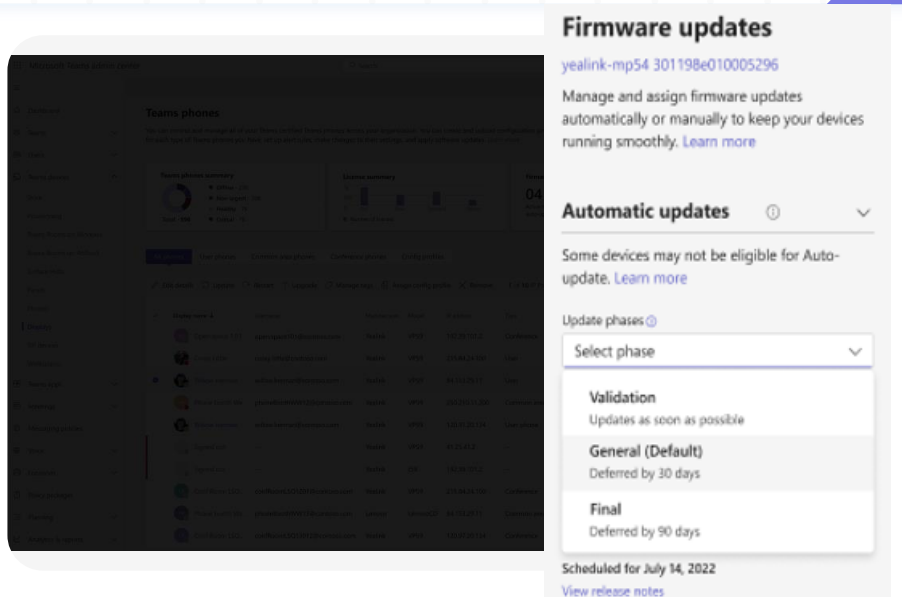
After March 2026, Microsoft will stop enforcing require approved client app control, and it will be as if this grant isn't selected. Use the following steps before March 2026 to protect your organization's data.


MAKE IT
REAL

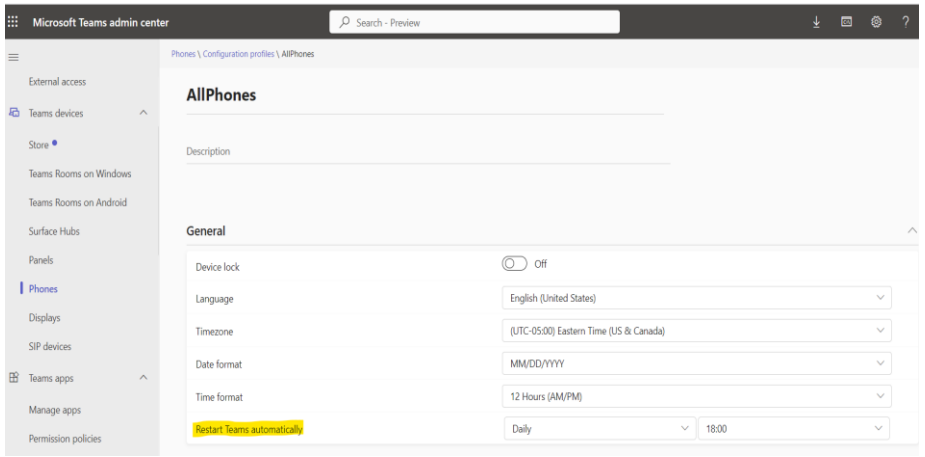
Troubleshooting

Teams Phone Devices Best Practices

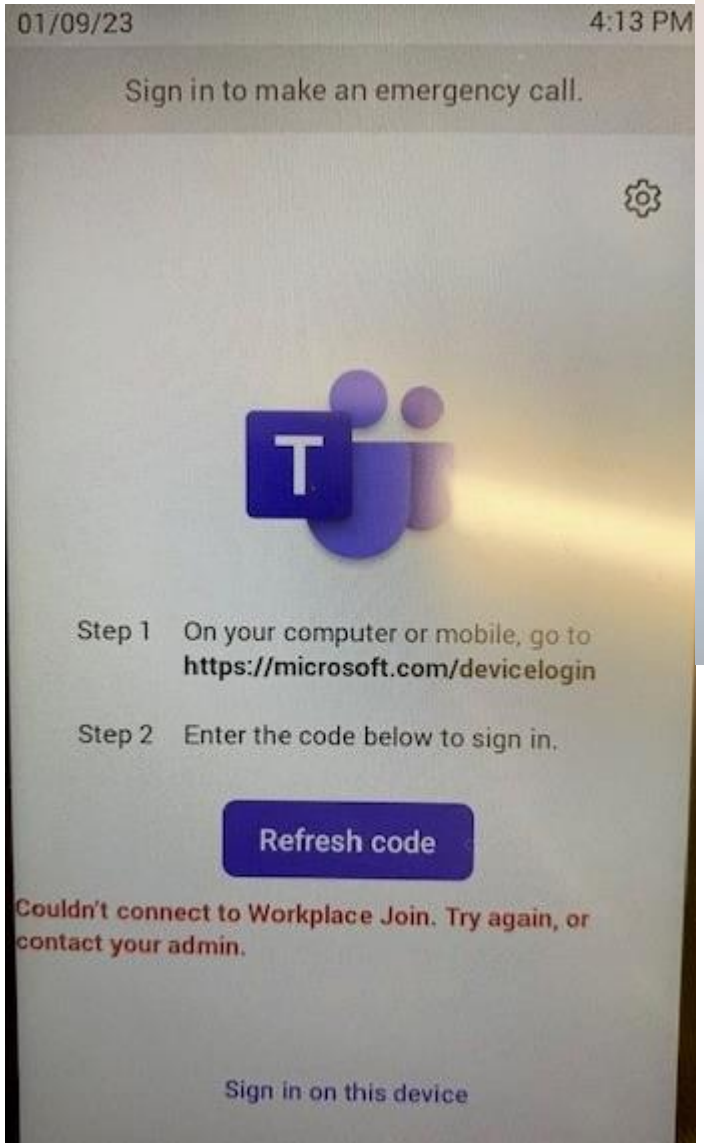
- Use configuration profile to apply settings in bulk
- Enable Daily App restart for optimal phone performance
  - Option: Daily, When Needed, Never
- Setup automated firmware updates on Teams Admin Center
  - Validation (Update as soon as possible)
  - General (Deferred by 30 days) - Default
  - Final (Deferred by 90 days)
- Roll out updates to your devices in phases

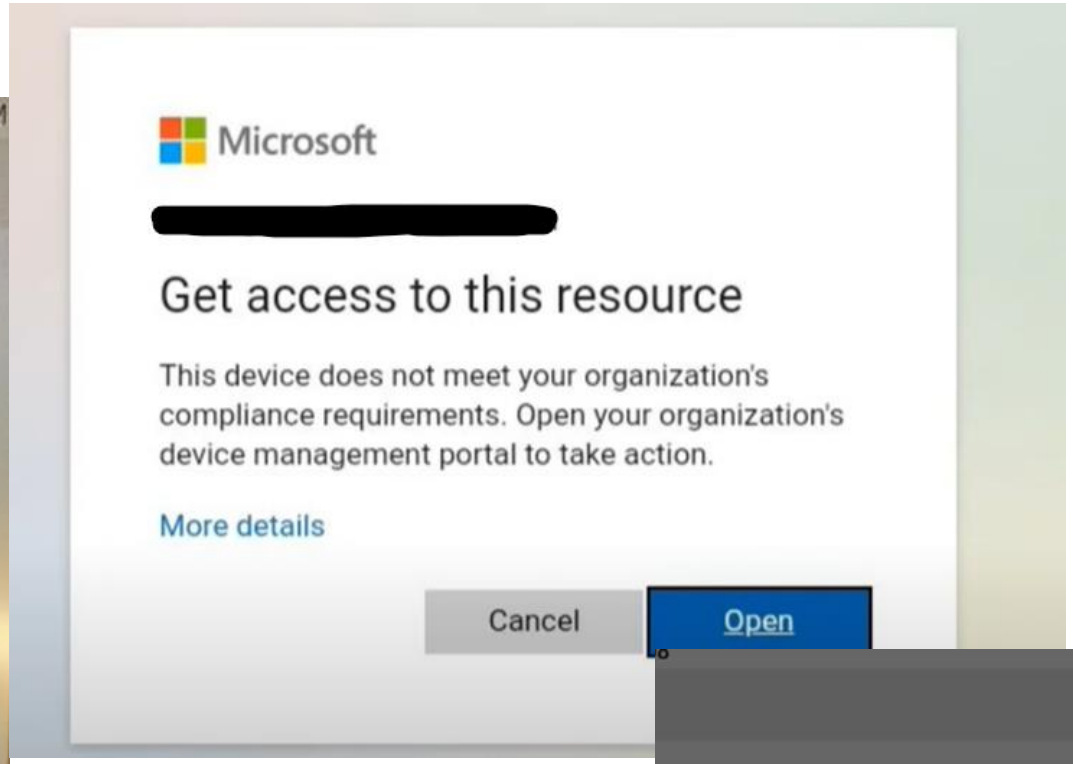


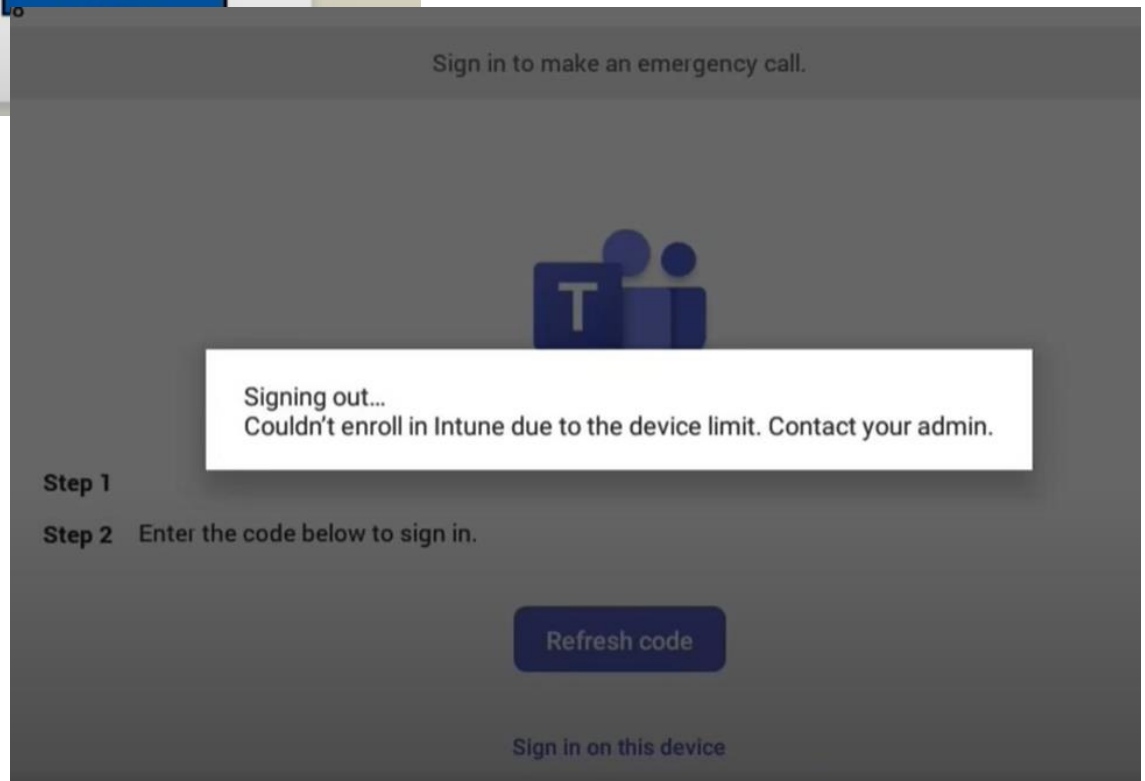
Manage firmware updates



Schedule app restart


01/09/23
4:13 PM
Sign in to make an emergency call.
Step 1 On your computer or mobile, go to https://microsoft.com/devicelogin
Step 2 Enter the code below to sign in.
Refresh code
Couldn't connect to Workplace Join. Try again, or contact your admin.
Sign in on this device


Microsoft
[redacted]
Get access to this resource
This device does not meet your organization's compliance requirements. Open your organization's device management portal to take action.
More details
Cancel
Open


Sign in to make an emergency call.
Signing out...
Couldn't enroll in Intune due to the device limit. Contact your admin.
Step 1
Step 2 Enter the code below to sign in.
Refresh code
Sign in on this device

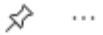
Troubleshooting Tools (Live Demo)

- WhatIf - Conditional Access
- Troubleshooting + Support – Intune & CA
- EntraID (AAD) Signin Logs
- EntraID (AAD) Audit Logs

Home > Users

Users | Sign-in logs

Traci Herr - Azure Active Directory



- All users
- Deleted users
- Password reset
- User settings
- Diagnose and solve problems

Activity

- Sign-in logs
- Audit logs
- Bulk operation results

Download | Export Data Settings | Troubleshoot | Refresh | Columns | Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 1 month** | Show dates as : **Local** | Time aggregate : **24 hours** | Status : **Failure** | Add

User sign-ins (interactive) | **User sign-ins (non-interactive)**

Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that c

Date	Request ID	Username	Application	Status	IP ac
> 8/10/2022, 8:00:00 F	Aggregate	tsylvia@sfbninja.com	Microsoft Teams Ad...	Failure	68.7

Date : **Last 1 month** | Show dates as : **Local** | Time aggregate : **24 hours** | Status : **Failure** | Application contains **Teams** | Add filters

User sign-ins (interactive) | **User sign-ins (non-interactive)** | Service principal sign-ins | Managed identity sign-ins

Sign-in logs

Download | Export Data Settings | Troubleshoot | Refresh | Columns | Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 1 month** | Show dates as : **Local** | Time aggregate : **24 hours** | Status : **Failure** | Application co

User sign-ins (interactive) | **User sign-ins (non-interactive)** | Service principal sign-ins | Managed identity sign-ins

Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date an

Date	Request ID	Username	Application	Status
8/10/2022, 8:00:00 PM	Aggregate	tsylvia@sfbninja.com	Microsoft Teams Admin ...	Failure
8/8/2022, 8:00:00 PM	Aggregate	tsylvia@sfbninja.com	Microsoft Teams Admin ...	Failure
8/4/2022, 8:00:00 PM	8bff15be-eaac-457b-8553	ccx500@sfbninja.com	Microsoft Teams Services	Failure
8/3/2022, 8:00:00 PM	649b6d53-ef80-498d-814	mtra@sfbninja.com	Microsoft Teams Services	Failure
8/2/2022, 8:00:00 PM	14e2585d-09ac-4390-81b	th@sfbninja.com	Microsoft Teams Admin ...	Failure
8/3/2022, 5:33:44 PM	14e2585d-09ac-4390-81b	th@sfbninja.com	Microsoft Teams Admin ...	Failure
8/2/2022, 8:00:00 PM	Aggregate	tsylvia@sfbninja.com	Microsoft Teams Admin ...	Failure
8/1/2022, 8:00:00 PM	9c332bd4-f8df-4d55-82de	tsylvia@sfbninja.com	Microsoft Teams Admin ...	Failure
8/1/2022, 8:00:00 PM	0bf5f336-fb13-4498-a8d3	intunepolyc60@sfbninja...	Microsoft Teams - Devic...	Failure
7/31/2022, 8:00:00 PM	409a9dd3-21c5-4f3a-877	th@sfbninja.com	Microsoft Teams Admin ...	Failure
7/31/2022, 8:00:00 PM	Aggregate	th@sfbninja.com	Microsoft Teams Admin ...	Failure
7/31/2022, 8:00:00 PM	Aggregate	th@sfbninja.com	Microsoft Teams Admin ...	Failure
7/31/2022, 8:00:00 PM	5651b9c0-16d1-40e1-904	intunepolyc60@sfbninja...	Microsoft Teams	Failure
8/1/2022, 12:32:01 P	5651b9c0-16d1-40e1-904	intunepolyc60@sfbninja...	Microsoft Teams	Failure
7/28/2022, 8:00:00 PM	f7312b5b-c2fc-435c-b75b	tsylvia@sfbninja.com	Microsoft Teams Admin ...	Failure

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	8/1/2022, 12:32:01 PM
Request ID	5651b9c0-16d1-40e1-904a-61fe41fc5401
Correlation ID	4fde7889-0fb9-49c8-ab8f-e986a4460ebd
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	70045
Failure reason	The refresh token is invalid due to sign-in frequency checks by conditional access. Additionally, since the sign-in frequency policy applies to all applications, the token will never be usable, and should be deleted. The authInstant in this token was {authInstant} and the maximum allowed lifetime for this request is {time}.
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	Intune Poly C60
Username	intunepolyc60@sfbninja.com
User ID	18fd10ce-b638-4d81-bde7-22eb73bbe524
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Microsoft Teams
Application ID	1fec8e78-bce4-4aaf-ab1b-5451cc387264
Resource	Skype Presence Service
Resource ID	1e70cd27-4707-4589-8ec5-9bd20c472a46

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	8/2/2022, 2:38:55 PM
Request ID	0bf5f336-fb13-4498-a8d3-d5d4e8ca4e01
Correlation ID	0a80355f-cb97-40ff-ba31-edf437a317f8
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	530002
Failure reason	Your device is required to be compliant to access this resource.
Additional Details	The requested resource can only be accessed using a compliant device. The user is using a device already managed by a Mobile-Device-Management (MDM) agent like Intune, but it's not being reported as compliant yet. The user could check with your MDM provider on how to become compliant. More details available at https://docs.microsoft.com/azure/active-directory/active-directory-conditional-access-device-remediation
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	Intune Poly C60
Username	intunepolyc60@sfbninja.com
User ID	18fd10ce-b638-4d81-bde7-22eb73bbe524
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Microsoft Teams - Device Admin Agent
Application ID	87749df4-7ccf-48f8-aa87-704bad0e0e16
Resource	Device Management Service

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | **Conditional Access** | Report-only | ...

Search

Policy Name	Grant Controls	Session Controls	Result	
Teams Phones	Require compliant device	Sign-in frequency	Failure	...
Teams Phones - Block signin fr...	Block		Not Applied	...
Teams IP Phones - test			Disabled	...

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

Conditional Access Policy details

Previous Next

Policy: Teams Phones
Policy state: Enabled
Result: Failure

Assignments

User
Intune Poly C60 — Matched

Application
Microsoft Teams - Device Admin Agent — Matched

Conditions

Sign-in risk
None — Not configured

Device platform
Android — Matched

Location
Doral, US — Matched
68.7[redacted]

Client app
Mobile Apps and Desktop clients — Matched

Device
0a10d267-36e0-458e-8913-b2216316b690 — Not matched

User risk — Not configured

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only | ...

Date	2/3/2022, 8:16:39 AM
Request ID	c68fd079-1c78-4e43-8b74-e86b717a5b01
Correlation ID	0f29f5fa-8277-4fdf-a7cc-c4f92f3636c9
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	50199
Failure reason	For security reasons, user confirmation is required for this request. Please repeat the request allowing user interaction.
Troubleshoot Event	Follow these steps: 1. Launch the Sign-in Diagnostic. 2. Review the diagnosis and act on suggested fixes.
User	Intune Poly

Script that will check for Unsupported Settings in your Policies

```
PS C:\software\Scripts> .\Test-TeamsDevicesCompliancePolicy.ps1 -detailed | ft

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the U
message. Do you want to run C:\software\Scripts\Test-TeamsDevicesCompliancePolicy.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): r

PolicyName          Setting                                          Value TeamsDevicesStatus Comment
----------          -------                                          ----- ----------------- -------
Android Cell Phones deviceThreatProtectionEnabled                    False Supported
Android Cell Phones securityBlockJailbrokenDevices                    True Warning           This setting can cause sign in issues.
Android Cell Phones deviceThreatProtectionRequiredSecurityLevel unavailable Supported
Android Cell Phones securityRequireUpToDateSecurityProviders         False Supported
Android Cell Phones securityRequireVerifyApps                        False Supported
Android Cell Phones securityRequireSafetyNetAttestationBasicIntegrity False Supported
Android Cell Phones securityRequireSafetyNetAttestationCertifiedDevice False Supported
Android Cell Phones osMinimumVersion                                       Supported
Android Cell Phones osMaximumVersion                                       Supported
Android Cell Phones storageRequireEncryption                          True Warning           https://docs.microsoft.com/en-us/microsoftteams/rooms/suppo
Android Cell Phones securityPreventInstallAppsFromUnknownSources     False Supported
Android Cell Phones passwordMinutesOfInactivityBeforeLock                  Supported
Android Cell Phones passwordRequired                                  True Unsupported
Android Cell Phones passwordRequiredType                           numeric Unsupported
Android Cell Phones passwordMinimumLength                                4 Unsupported
Android Cell Phones passwordExpirationDays                             365 Unsupported
Android Cell Phones passwordPreviousPasswordBlockCount                   1 Unsupported
Android Cell Phones minAndroidSecurityPatchLevel                           Warning           This setting can cause sign in issues.
MTR-w               deviceThreatProtectionEnabled                          Supported
MTR-w               securityBlockJailbrokenDevices                         Supported
MTR-w               deviceThreatProtectionRequiredSecurityLevel            Unsupported
MTR-w               securityRequireUpToDateSecurityProviders               Supported
MTR-w               securityRequireVerifyApps                              Supported
MTR-w               securityRequireSafetyNetAttestationBasicIntegrity      Supported
MTR-w               securityRequireSafetyNetAttestationCertifiedDevice     Supported
MTR-w               osMinimumVersion                                       Supported
MTR-w               osMaximumVersion                                       Supported
MTR-w               storageRequireEncryption                         False Supported
MTR-w               securityPreventInstallAppsFromUnknownSources           Supported
MTR-w               passwordMinutesOfInactivityBeforeLock                  Supported
MTR-w               passwordRequired                                 False Supported
MTR-w               passwordRequiredType                       deviceDefault Supported
MTR-w               passwordMinimumLength                                  Supported
MTR-w               passwordExpirationDays                                 Supported
MTR-w               passwordPreviousPasswordBlockCount                     Supported
MTR-w               minAndroidSecurityPatchLevel                           Warning           This setting can cause sign in issues.
Teams               deviceThreatProtectionEnabled                    False Supported
```

Teams Rooms, Phones, Panels and Displays Best Practices and Supportability Docs

Conditional Access

https://learn.microsoft.com/en-us/microsoftteams/rooms/supported-ca-and-compliance-policies?tabs=phones
https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-rooms-and-devices/teams-android-devices-conditional-access-issues
https://learn.microsoft.com/en-us/MicrosoftTeams/devices/authentication-best-practices-for-android-devices#using-filters-for-devices

Intune

https://learn.microsoft.com/en-us/microsoftteams/rooms/supported-ca-and-compliance-policies?tabs=phones
https://learn.microsoft.com/en-us/microsoftteams/devices/phones-displays-deploy#configure-intune-to-enroll-teams-android-based-devices
https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy#microsoft-teams-android-devices
https://learn.microsoft.com/en-us/microsoftteams/rooms/conditional-access-and-compliance-for-devices
https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-rooms-and-devices/rooms-known-issues#teams-phone-devices
https://learn.microsoft.com/en-us/microsoftteams/rooms/security-android

Traci's Personal Blog

https://ucmess.wordpress.com/2022/06/30/teams-android-device-phone-mtr-panel-display-error-the-company-portal-has-been-inactive-for-some-time-you-may-need-to-sign-in-again/
https://ucmess.wordpress.com/2022/03/14/teams-ip-phone-mtr-sign-in-loop/
https://ucmess.wordpress.com/2022/08/22/protect-your-teams-devices-from-conditional-access/
https://ucmess.wordpress.com/2022/10/24/checking-intune-compliance-policies-for-unsupported-settings/

Additional Learning videos and Micro-Learnings

Teams devices for IT Pros 1: Intune Compliance & Conditional Access with Teams Rooms on Android
Teams devices for IT Pros 2: Intune Compliance & Conditional Access with Teams Android devices

Micro-Learning (5-15 min. videos) Troubleshooting Teams Devices hosted by Michael Tressler & Traci Herr
Teams devices for IT Pros 3: Can You Stump Herr? Episode 1
Teams devices for IT Pros 4: Can You Stump Herr? Episode 2
Teams devices for IT Pros 5: Can You Stump Herr? Episode 3
Teams devices for IT Pros 6: Can you Stump Herr? Episode 4

Microsoft Teams

Q&A

Event Giveaway

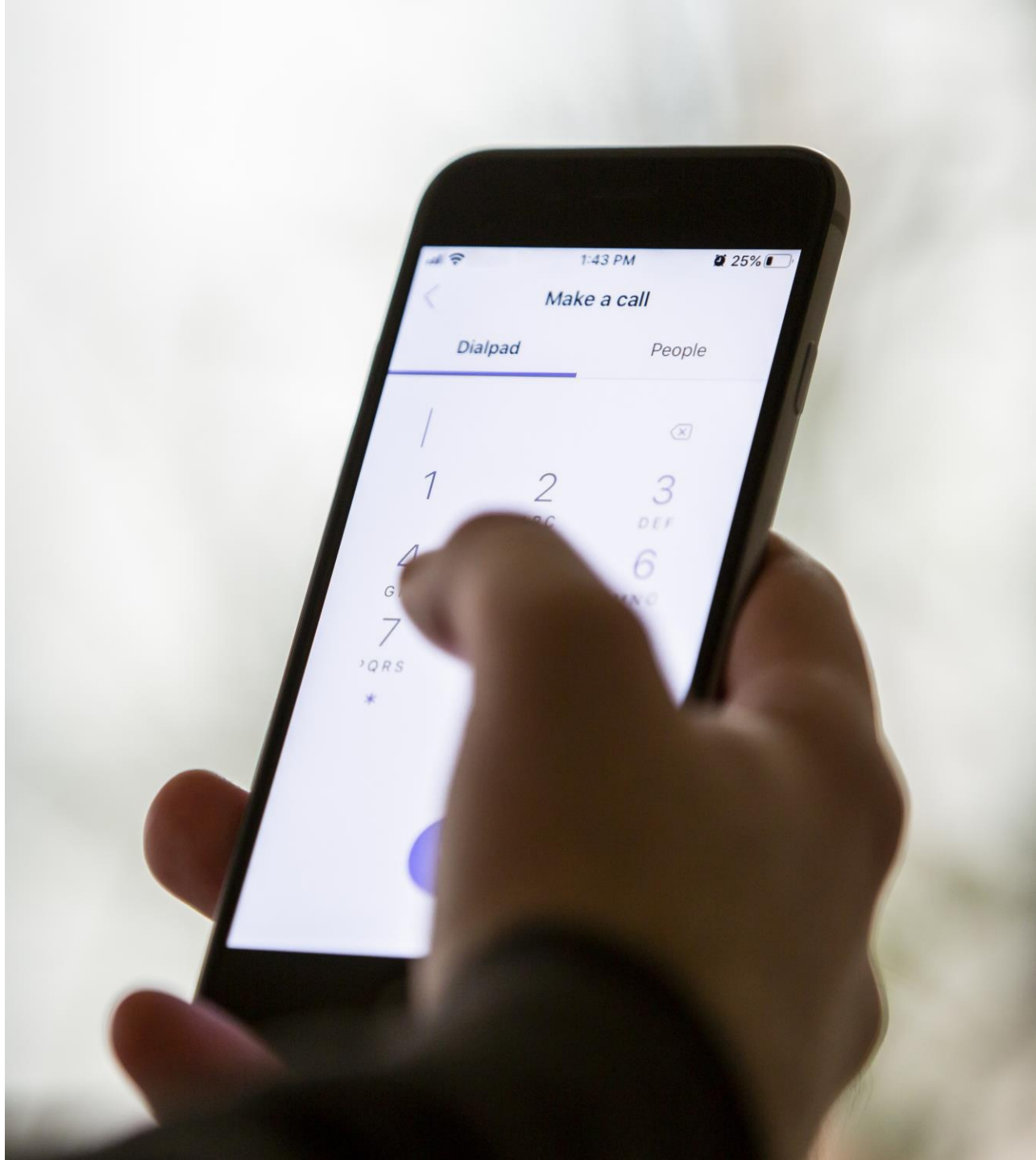
Giving away a prize pack for each session. Fill out a survey to be entered.

We will reach out after the Teams Phone Summit to the winners!

If you are a government employee, please fill out the survey and indicate you are not eligible to participate.

Call to Action

- Need a more technical conversation on Teams Phone?
  - Set up a meeting with your Microsoft Account Teams or partner
- Teams Phone POC/Pilot
  - Let's talk about how we can help you with a POC and/or Pilot
- Interested in reducing your IT spend, simply administration and support your users
  - Let's talk about how Shared Calling is the right solution for you
- Let's get started - https://aka.ms/TeamsPhoneSummitDay2AM



We want your Feedback!

- Let us know how we did
- Do you need any help with Teams Phone?
- Register for the giveaway

https://aka.ms/TeamsPhoneSummitDay2AM

Thank you for attending!!

Using Intune when Deploying Teams Phone Devices