Microsoft

Brownbag Session

Teams Devices with Conditional Access and Intune

Traci Herr
Sr. Escalation Engineer
Voice and Device SME, MCT
Traci.herr@microsoft.com
LinkedIn www.linkedin.com/in/traciherr/
Twitter @SkypeChick
Blog https://ucmess.wordpress.com

About Me – Traci Herr

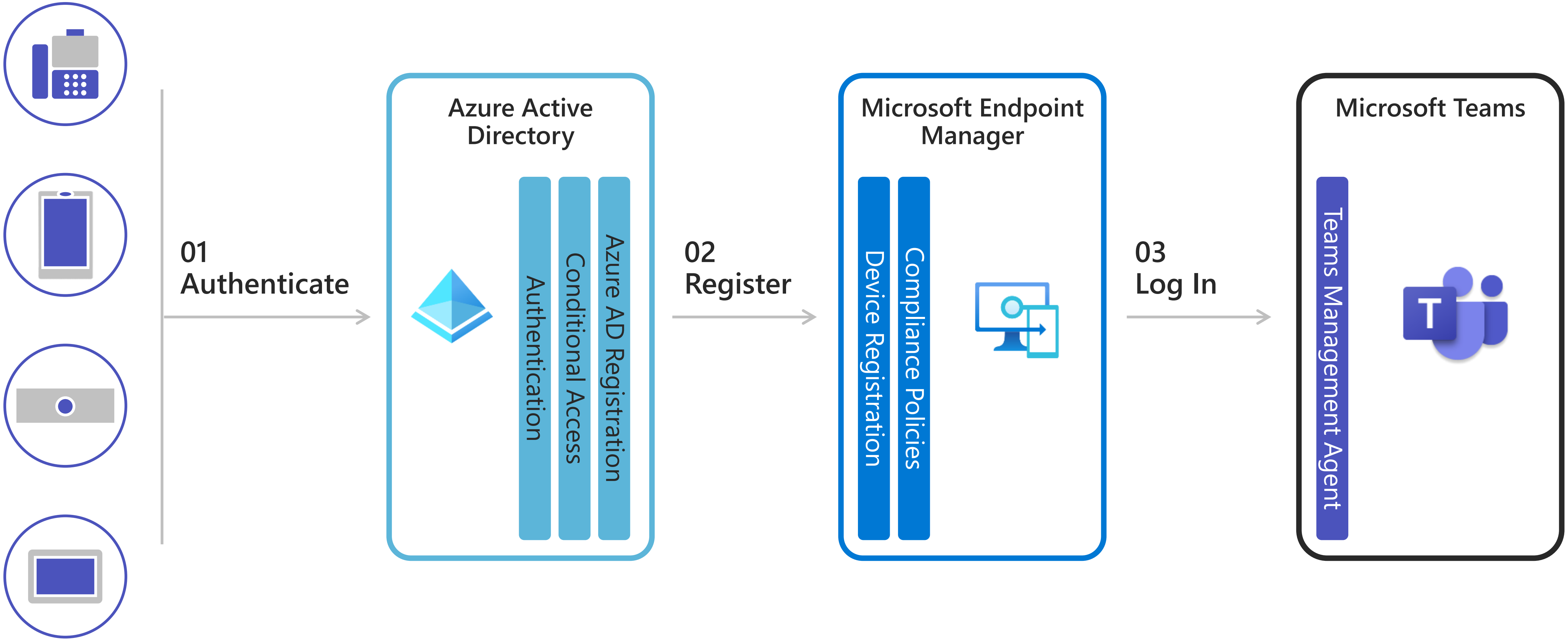
- Sr. Escalation Engineer
- Lead for North America Teams Device Escalation team
- Voice and Teams Device SME
- MSFT Certified Trainer (MCT)
- 20+ years with OCS, Lync, Skype, Teams & Telcom

Blog https://ucmess.wordpress.com

Twitter @skypechick

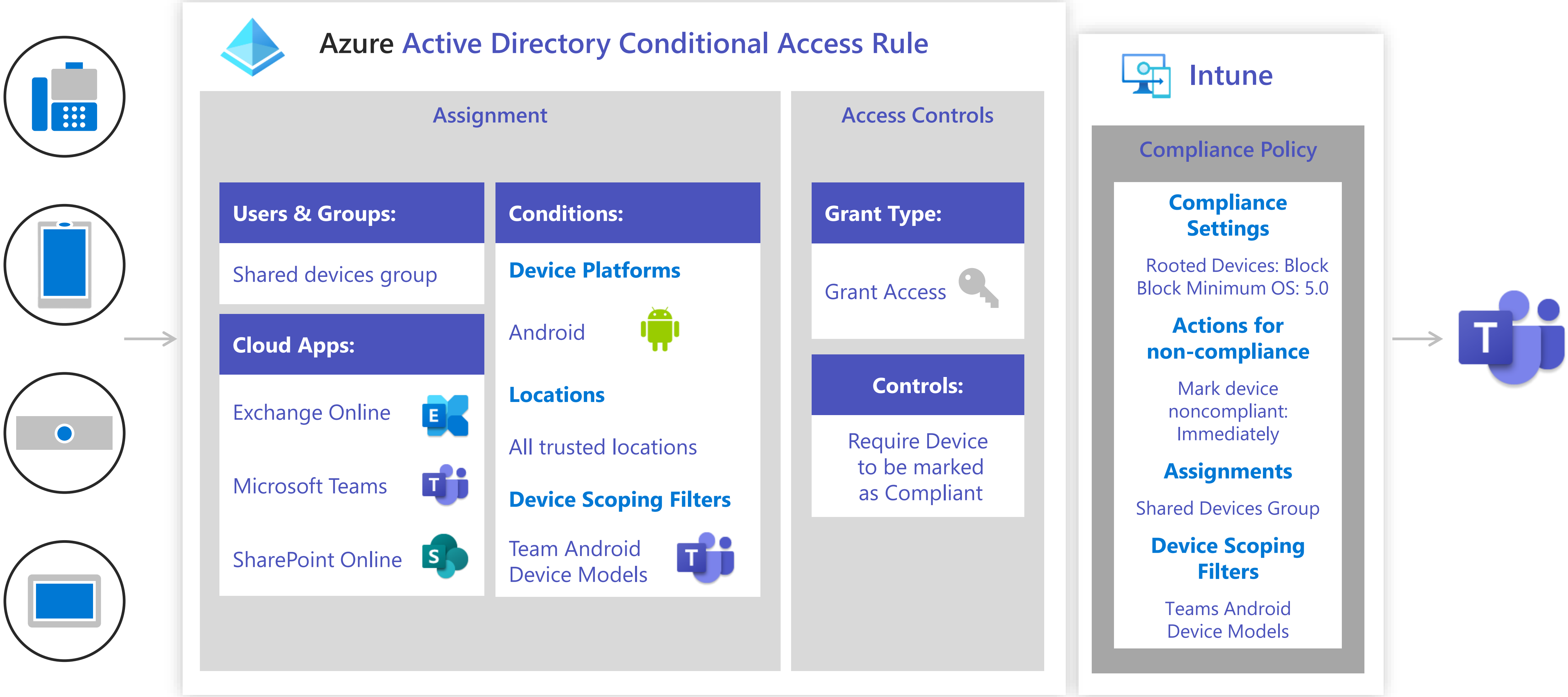
LinkedIn https://linkedin.com/in/traciherr

Sign-in and registration components



Shared devices conditional access

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: 5.0

Actions for non-compliance

Mark device noncompliant: Immediately

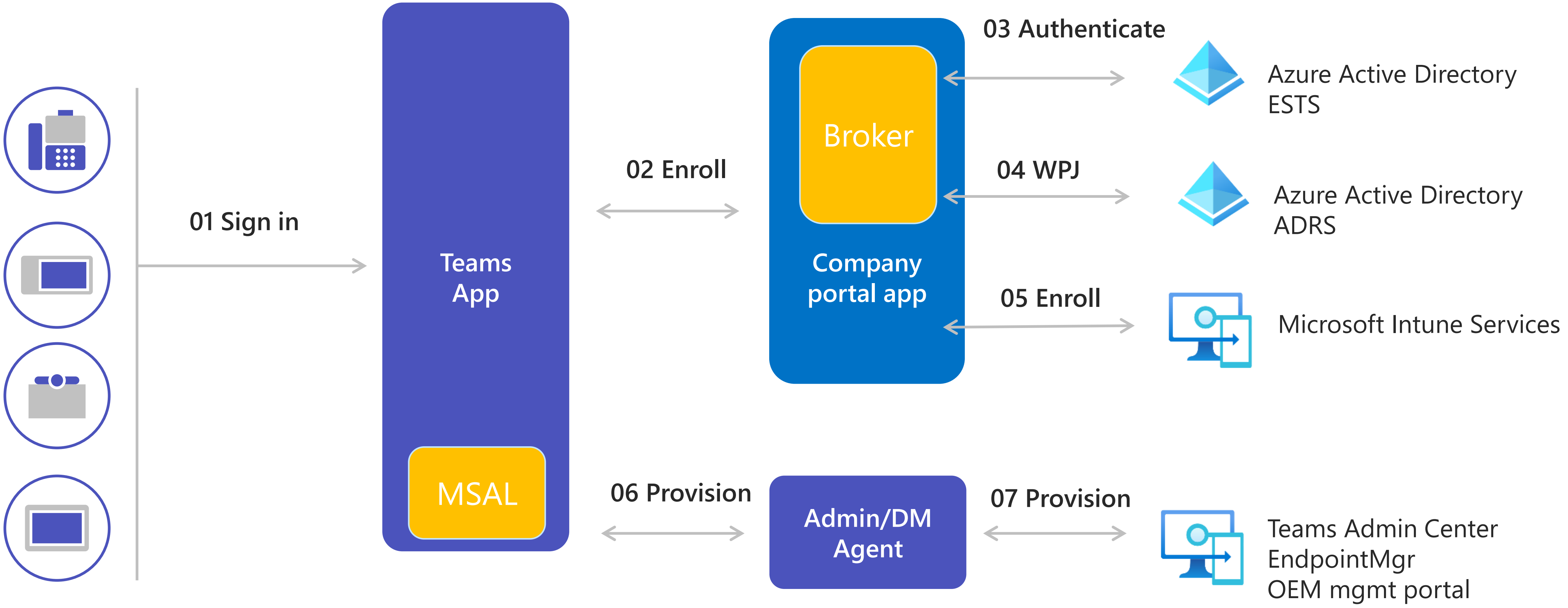
Assignments

Shared Devices Group

Device Scoping Filters

Teams Android Device Models

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



01 Sign in

Teams App

MSAL

02 Enroll

Broker

Company portal app

03 Authenticate

Azure Active Directory
ESTS

04 WPJ

Azure Active Directory
ADRS

05 Enroll

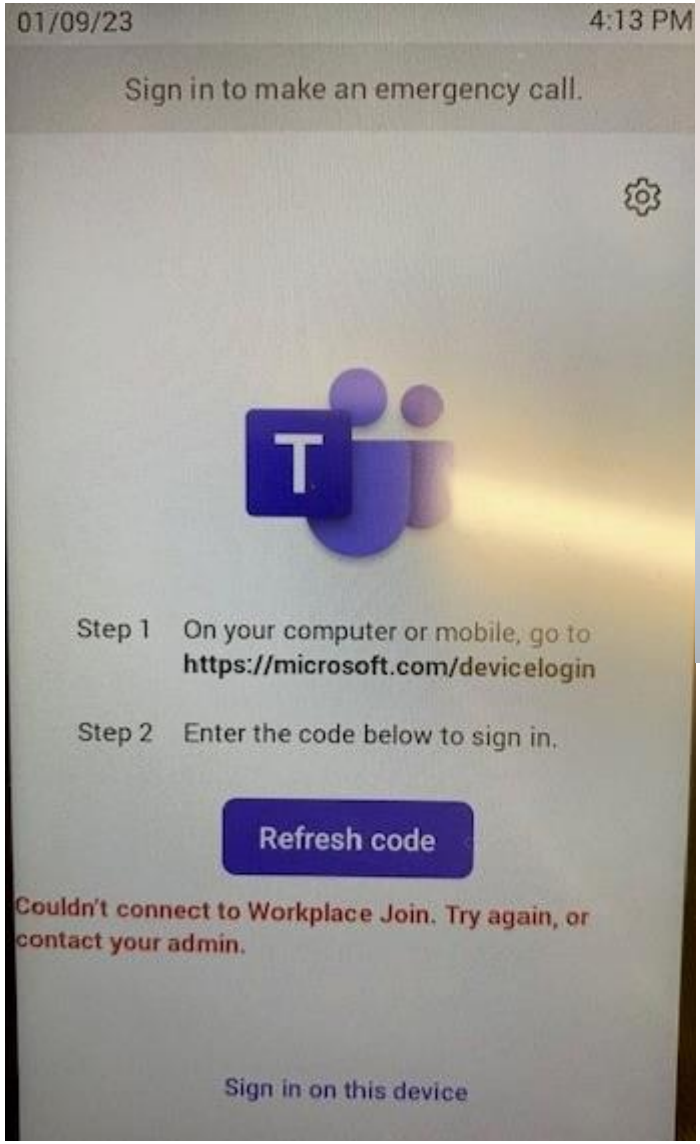
Microsoft Intune Services

06 Provision

Admin/DM Agent

07 Provision

Teams Admin Center
EndpointMgr
OEM mgmt portal



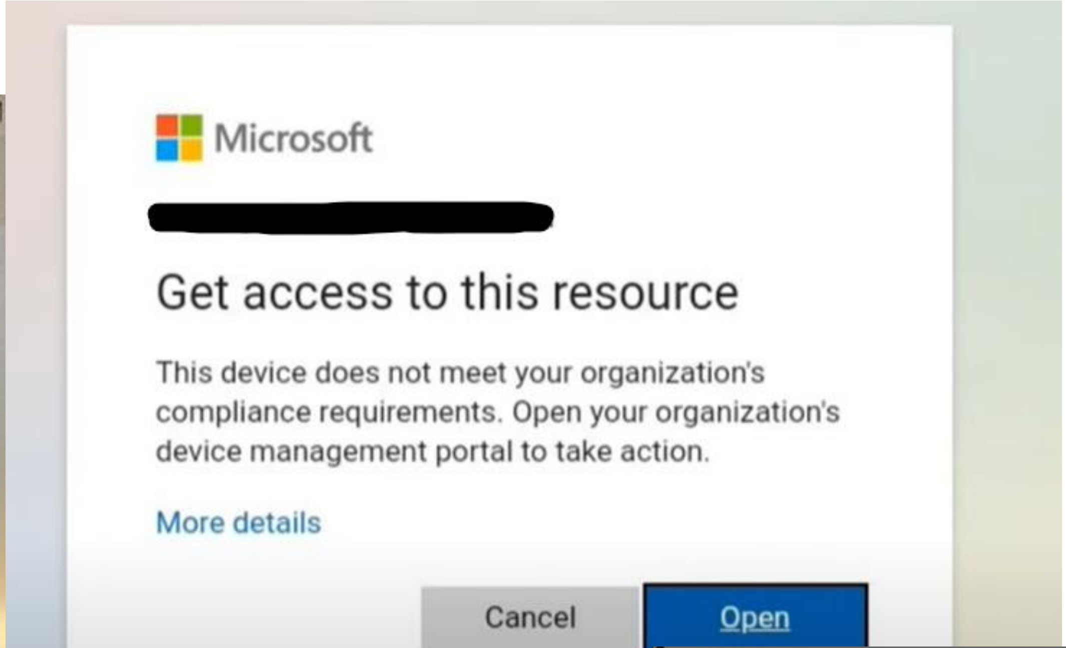
01/09/23 4:13 PM

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.

Couldn't connect to Workplace Join. Try again, or contact your admin.

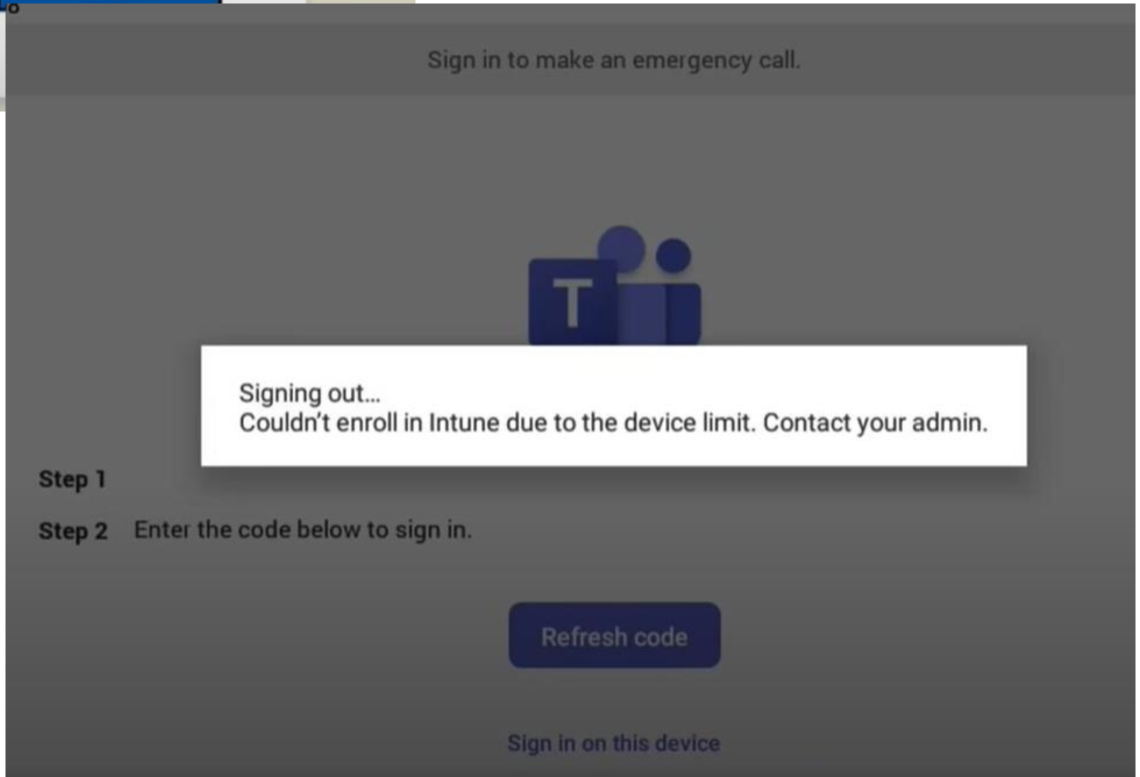


Microsoft

[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.



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.

Enrollment Flow

- User logs into the Teams device and authenticates to AAD
- License state of the user is checked, if licensed Intune enrollment flow starts
- Device registers in AAD
- Device registers with Intune and is provided with enrollment cert
  - Intune checks the enrollment restrictions of the user prior to enrolling
- Device checks-in to Intune and starts being provided with policy

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.

Enrolment Restrictions

Administrators can configure enrolment restrictions for users to limit the types of devices, versions and enrolment type

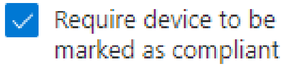
Because Android Device Administrator is being deprecated, many admins will have blocked this in Intune and this frequently causes a problem for Teams Device management

Office 365 MDM – aka MIfO

- There is a lightweight version of Intune produced for Office customers known as **Basic Mobility and Security for Office 365** or Microsoft Intune for Office (MIfO)
- It is possible to enrol Teams devices into MIfO but not recommended
- Officially we have never supported this scenario and may block it in future
- In general this is used by the SME community rather than large corporates.

Understanding Intune Enrollment Options

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



☑ Require device to be marked as compliant

- 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 enrolment?
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 enrolment 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 enrolment when an Intune licensed user attempts to logon?

Configuring Devices

- Intune has two types of policy for configuring devices

  Configuration Profile
  Compliance 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.

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*

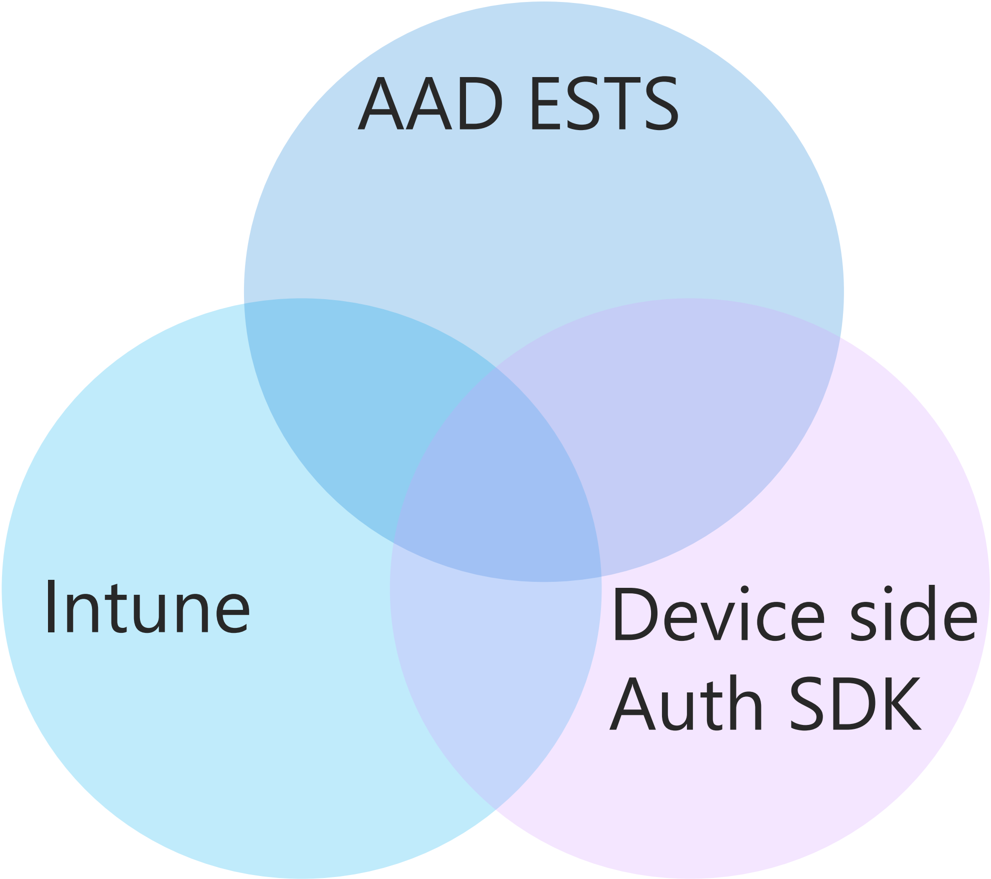
Understanding Conditional Access

- Conditional Access is an 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 AAD, Intune and device side auth code together to present the solution.



Conditional Access and Intune

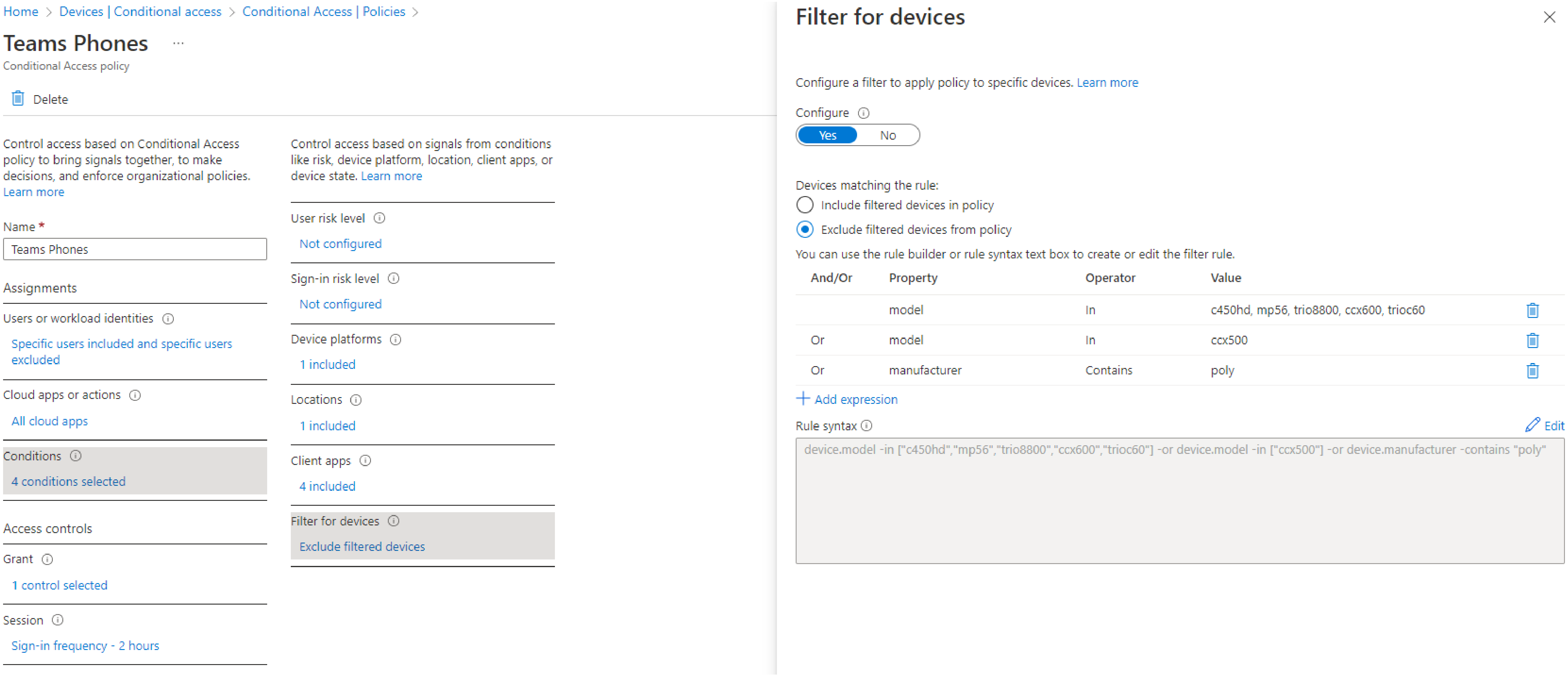
- Intune manages the setting of the 'IsCompliant' property on the AAD device object
- Only Intune can configure this property*
- When the user attempts to authenticate, the client sided auth code needs to hand up the AAD device id for the device at the same time. Device Code Flow (DCF)
- With this information, 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 AAD Device Objects only
- This will make your life better…I promise!



Home > Devices | Conditional access > Conditional Access | Policies >

Teams Phones ···

Conditional Access policy

Delete

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 or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

4 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 level ⓘ

Not configured

Sign-in risk level ⓘ

Not configured

Device platforms ⓘ

1 included

Locations ⓘ

1 included

Client apps ⓘ

4 included

Filter for devices ⓘ

Exclude filtered devices

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.

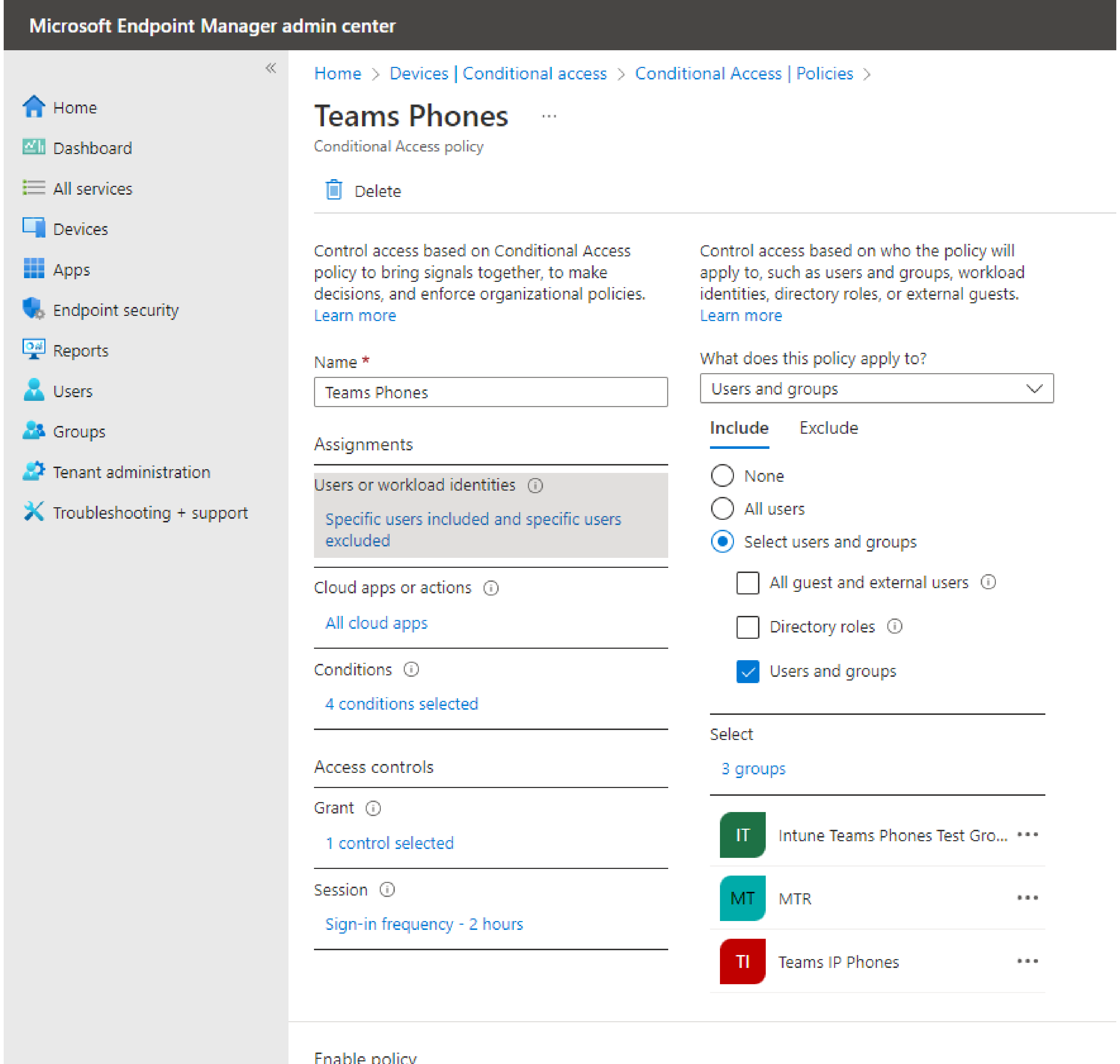
And/Or	Property	Operator	Value
	model	In	c450hd, mp56, trio8800, ccx600, trioc60
Or	model	In	ccx500
Or	manufacturer	Contains	poly

+ Add expression

Rule syntax ⓘ Edit

```
device.model -in ["c450hd","mp56","trio8800","ccx600","trioc60"] -or device.model -in ["ccx500"] -or device.manufacturer -contains "poly"
```

MAKE IT
REAL


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Conditional access > Conditional Access | Policies >
Delete

Teams Phones ...

Conditional Access policy

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 or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

4 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Sign-in frequency - 2 hours

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

What does this policy apply to?

Users and groups

Include Exclude

○ None

○ All users

● Select users and groups

□ All guest and external users ⓘ

□ Directory roles ⓘ

☑ Users and groups

Select

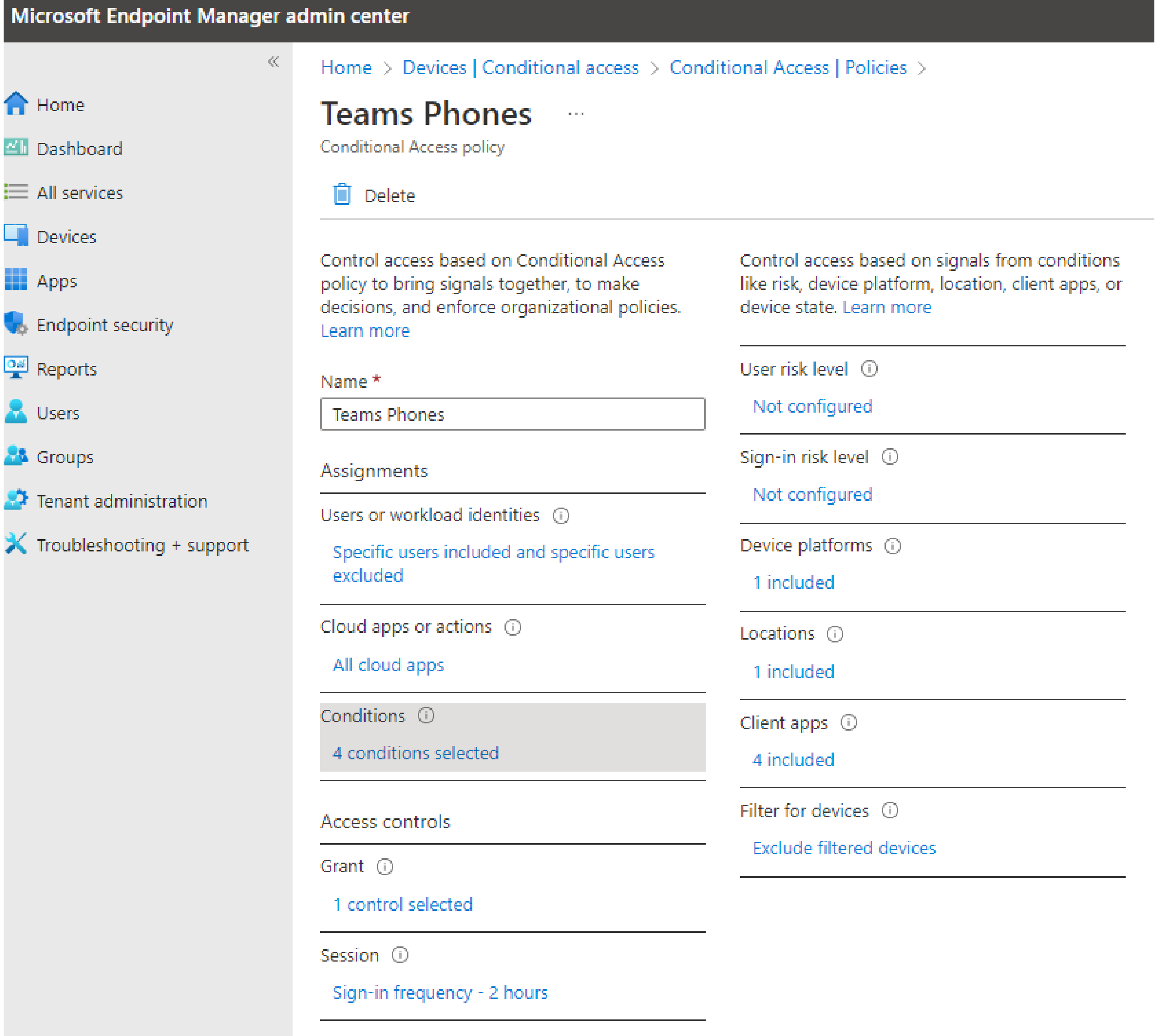
3 groups

IT Intune Teams Phones Test Gro... •••

MT MTR •••

TI Teams IP Phones •••

Enable policy


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Conditional access > Conditional Access | Policies >
Delete

Teams Phones

Conditional Access policy

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 or workload identities

Specific users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

4 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 level

Not configured

Sign-in risk level

Not configured

Device platforms

1 included

Locations

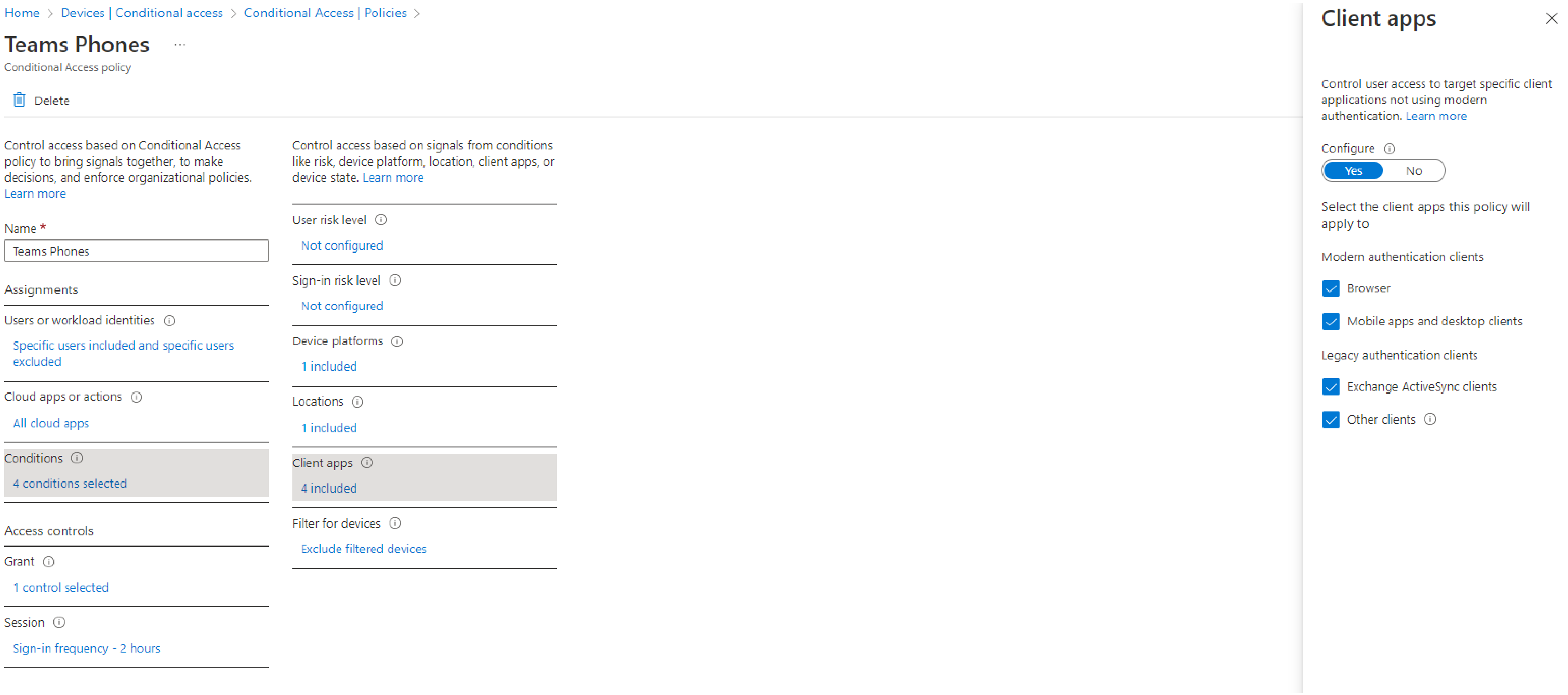
1 included

Client apps

4 included

Filter for devices

Exclude filtered devices



Home > Devices | Conditional access > Conditional Access | Policies >

Teams Phones

Conditional Access policy

Delete

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 or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

4 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 level ⓘ

Not configured

Sign-in risk level ⓘ

Not configured

Device platforms ⓘ

1 included

Locations ⓘ

1 included

Client apps ⓘ

4 included

Filter for devices ⓘ

Exclude filtered devices

Client apps

Control user access to target specific client applications not using modern authentication. Learn more

Configure ⓘ

[✓ Yes] No

Select the client apps this policy will apply to

Modern authentication clients

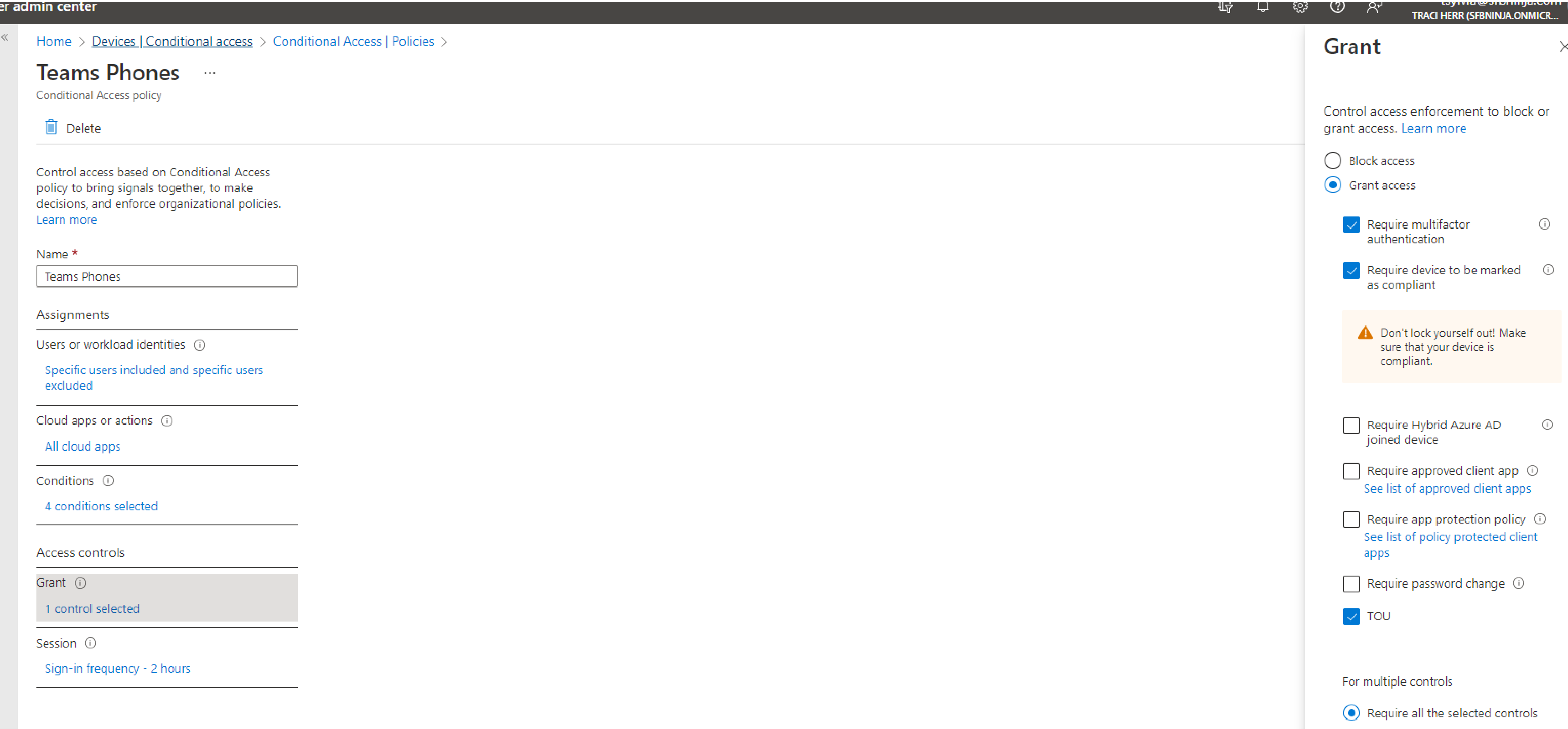
☑ Browser

☑ Mobile apps and desktop clients

Legacy authentication clients

☑ Exchange ActiveSync clients

☑ Other clients ⓘ



er admin center

TRACI HERR (SFBNINJA.ONMICR...

Home > Devices | Conditional access > Conditional Access | Policies >

Teams Phones ···

Conditional Access policy

Delete

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 or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

4 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Sign-in frequency - 2 hours

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication ⓘ

☑ Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant.

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

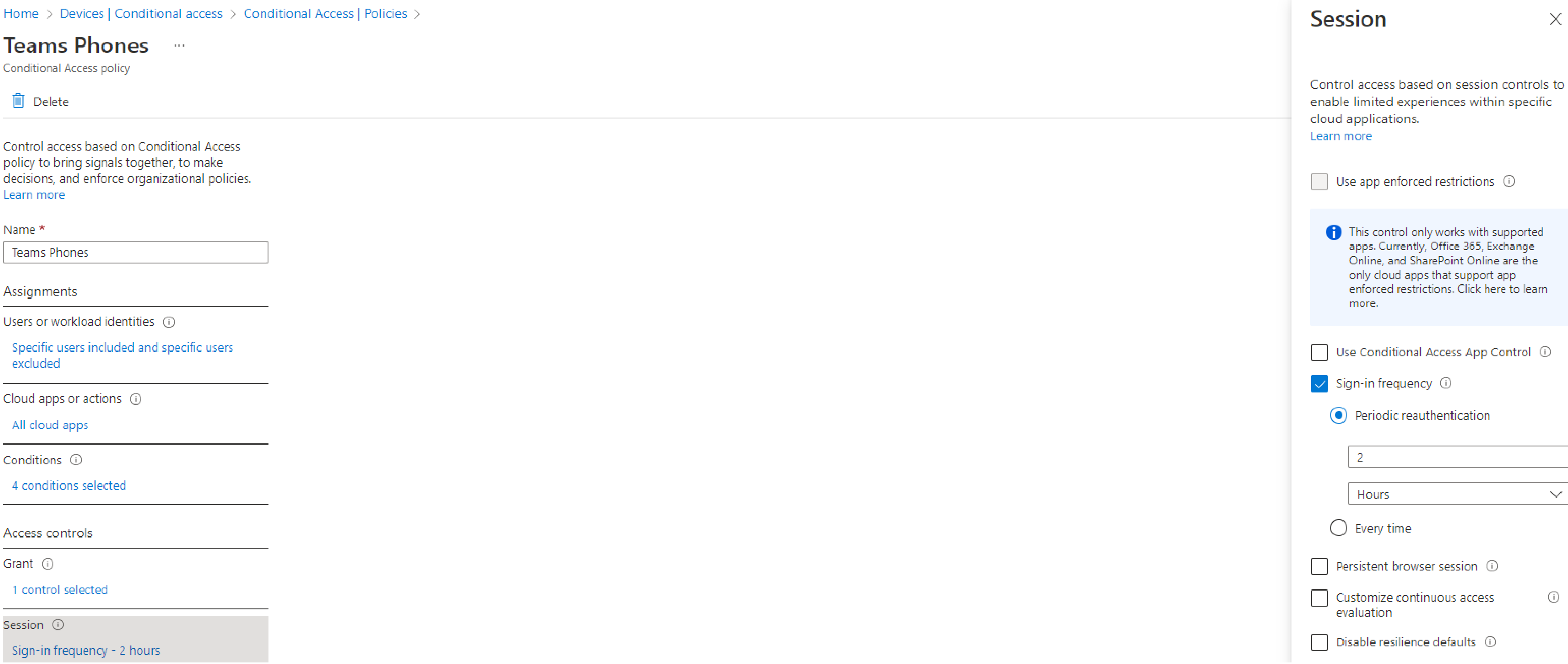
□ Require app protection policy ⓘ
See list of policy protected client apps

□ Require password change ⓘ

☑ TOU

For multiple controls

● Require all the selected controls



Home > Devices | Conditional access > Conditional Access | Policies >

Teams Phones ···

Conditional Access policy

Delete

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 or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

4 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Sign-in frequency - 2 hours

Session ✕

Control access based on session controls to enable limited experiences within specific cloud applications.

Learn more

□ Use app enforced restrictions ⓘ

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

□ Use Conditional Access App Control ⓘ

☑ Sign-in frequency ⓘ

● Periodic reauthentication

2

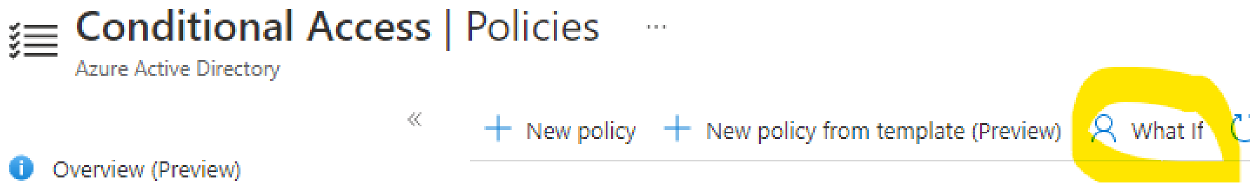
Hours

○ Every time

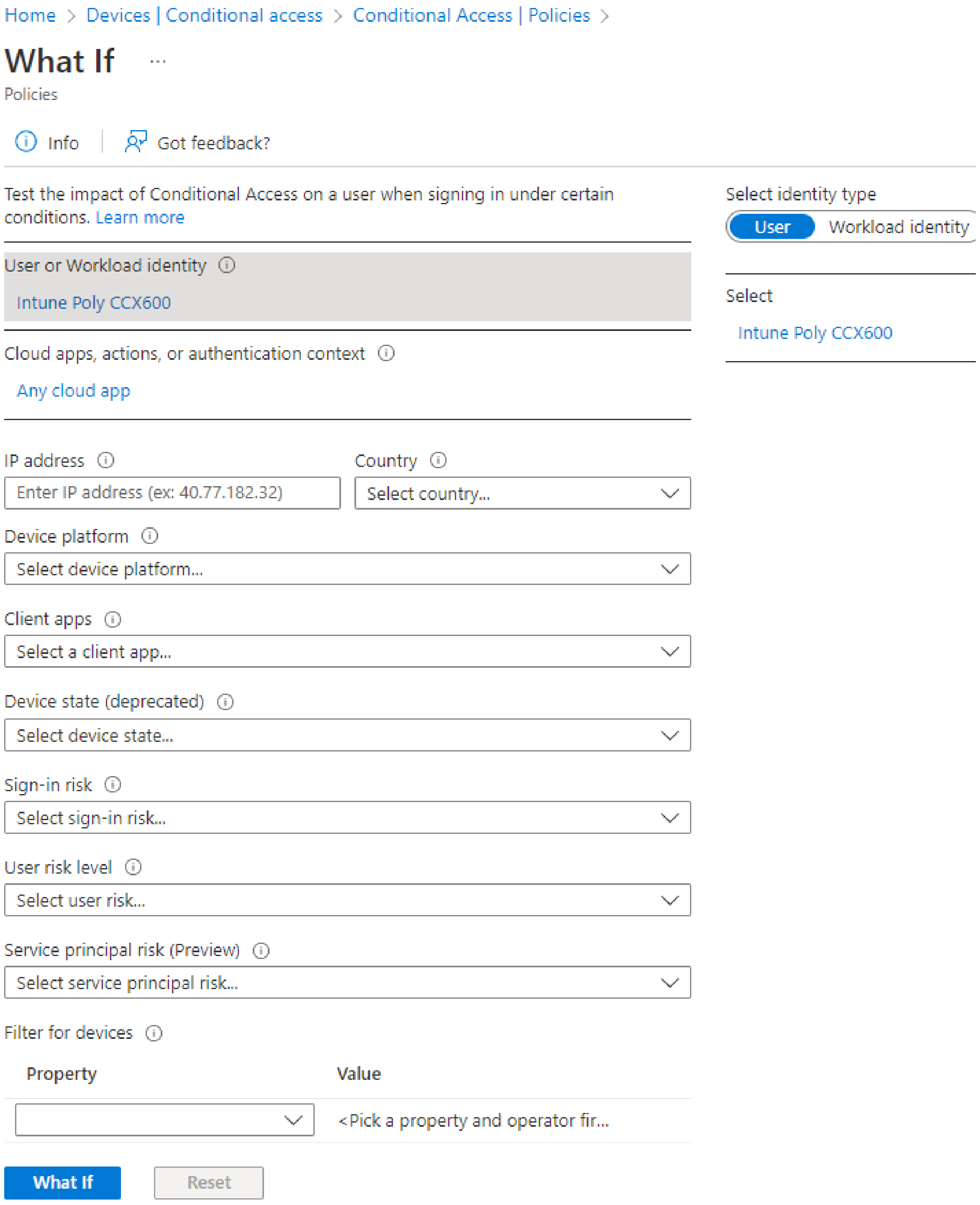
□ Persistent browser session ⓘ

□ Customize continuous access evaluation ⓘ

□ Disable resilience defaults ⓘ



Conditional Access | Policies
Azure Active Directory
Overview (Preview)
New policy
New policy from template (Preview)
What If



Home > Devices | Conditional access > Conditional Access | Policies >
What If
Policies
Info
Got feedback?

Test the impact of Conditional Access on a user when signing in under certain conditions. Learn more

Select identity type: User | Workload identity

User or Workload identity: Intune Poly CCX600

Select: Intune Poly CCX600

Cloud apps, actions, or authentication context: Any cloud app

IP address: Enter IP address (ex: 40.77.182.32)

Country: Select country...

Device platform: Select device platform...

Client apps: Select a client app...

Device state (deprecated): Select device state...

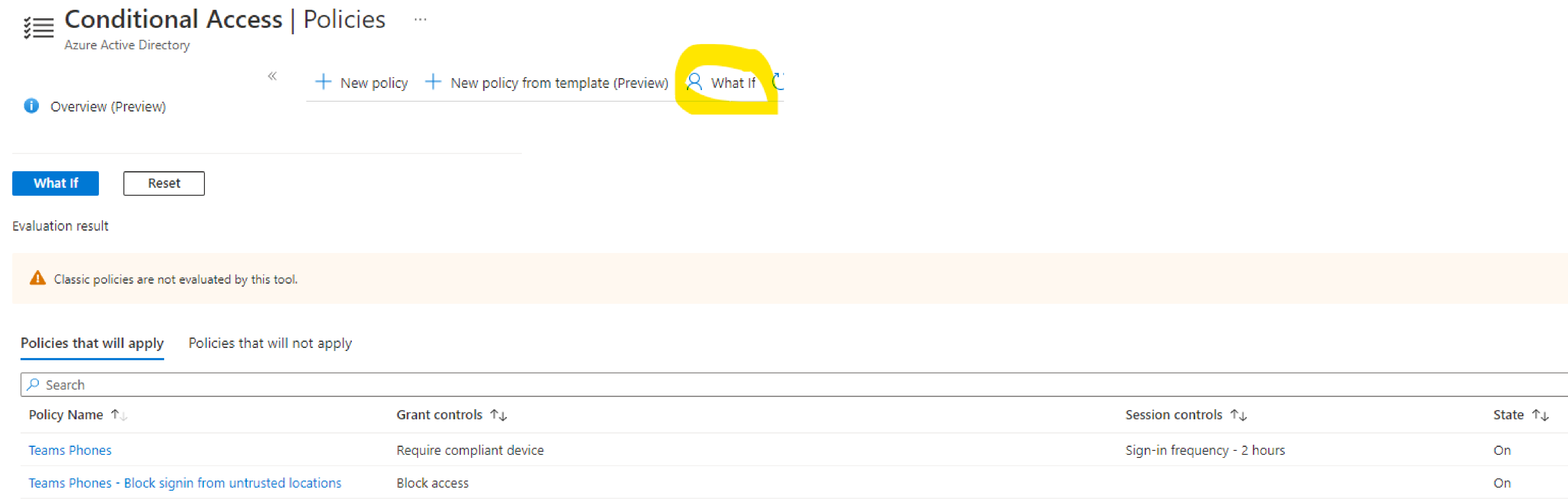
Sign-in risk: Select sign-in risk...

User risk level: Select user risk...

Service principal risk (Preview): Select service principal risk...

Filter for devices

Property	Value
	<Pick a property and operator fir...

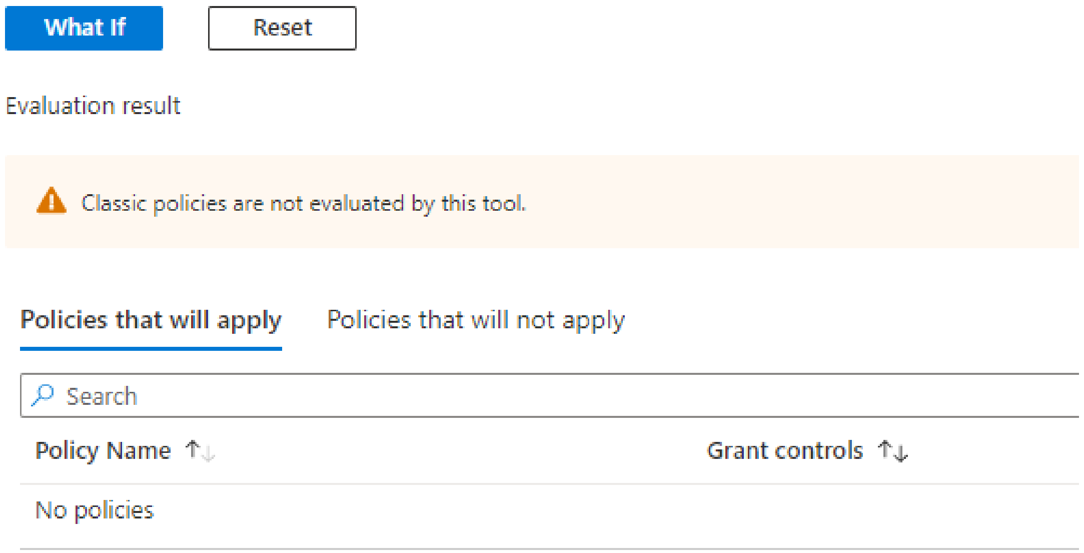


Evaluation result

Classic policies are not evaluated by this tool.

Policies that will apply | Policies that will not apply

Policy Name	Grant controls	Session controls	State
Teams Phones	Require compliant device	Sign-in frequency - 2 hours	On
Teams Phones - Block signin from untrusted locations	Block access		On

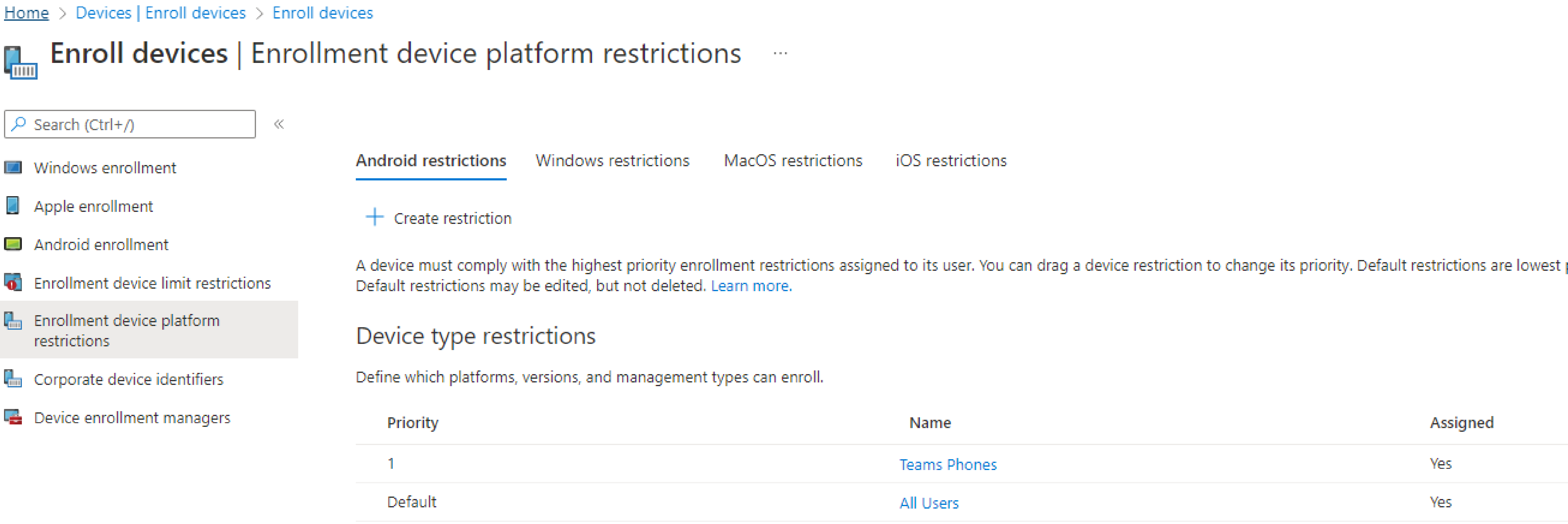


Evaluation result

Classic policies are not evaluated by this tool.

Policies that will apply | Policies that will not apply

Policy Name	Grant controls
No policies	



Home > Devices | Enroll devices > Enroll devices
Search (Ctrl+/)
Windows enrollment
Apple enrollment
Android enrollment
Enrollment device limit restrictions
Enrollment device platform restrictions
Corporate device identifiers
Device enrollment managers
Android restrictions
Windows restrictions
MacOS restrictions
iOS restrictions
+ Create restriction

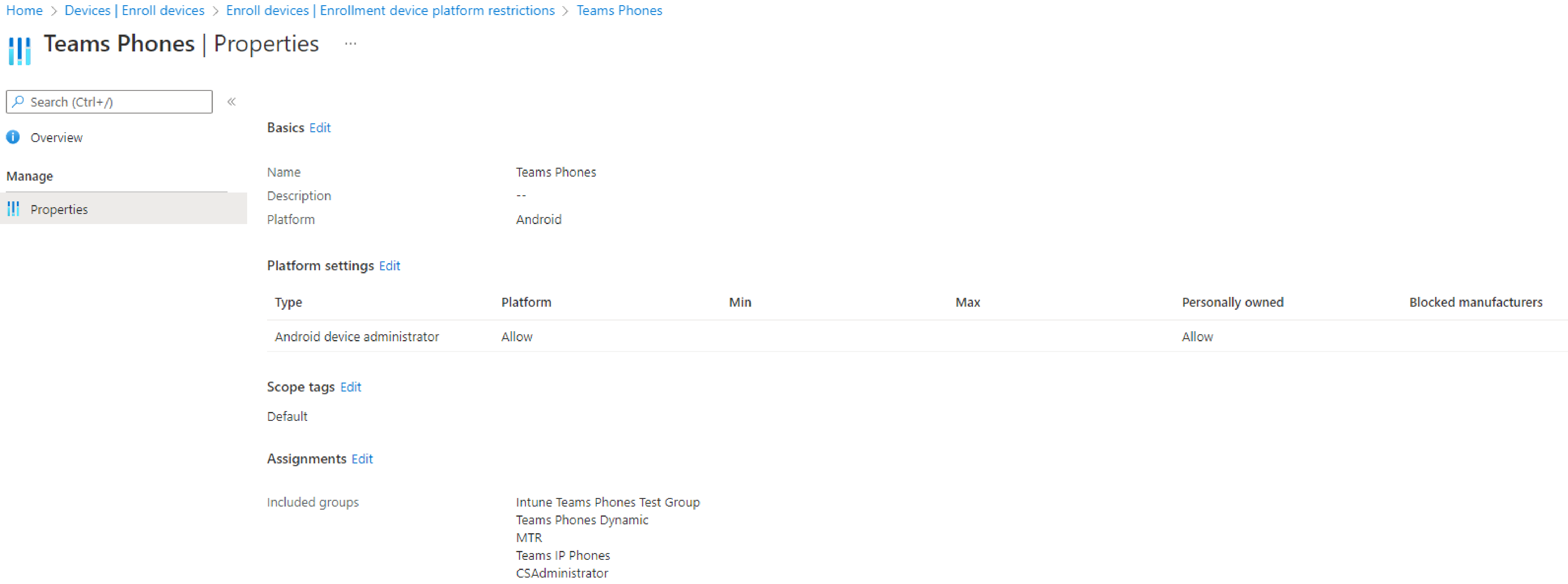
Enroll devices | Enrollment device platform restrictions ...

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest p
Default restrictions may be edited, but not deleted. Learn more.

Device type restrictions

Define which platforms, versions, and management types can enroll.

Priority	Name	Assigned
1	Teams Phones	Yes
Default	All Users	Yes



Home > Devices | Enroll devices > Enroll devices | Enrollment device platform restrictions > Teams Phones

Teams Phones | Properties

...
Search (Ctrl+/)
«
Overview
Manage
Properties

Basics Edit

Name	Teams Phones
Description	--
Platform	Android

Platform settings Edit

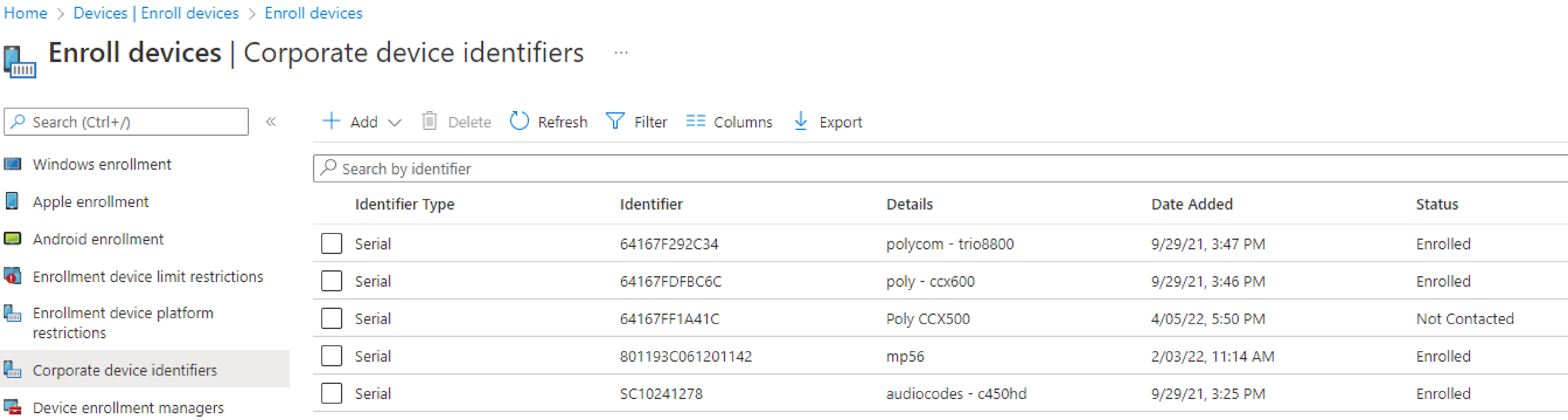
Type	Platform	Min	Max	Personally owned	Blocked manufacturers
Android device administrator	Allow			Allow	

Scope tags Edit

Default

Assignments Edit

Included groups	Intune Teams Phones Test Group Teams Phones Dynamic MTR Teams IP Phones CSAdministrator

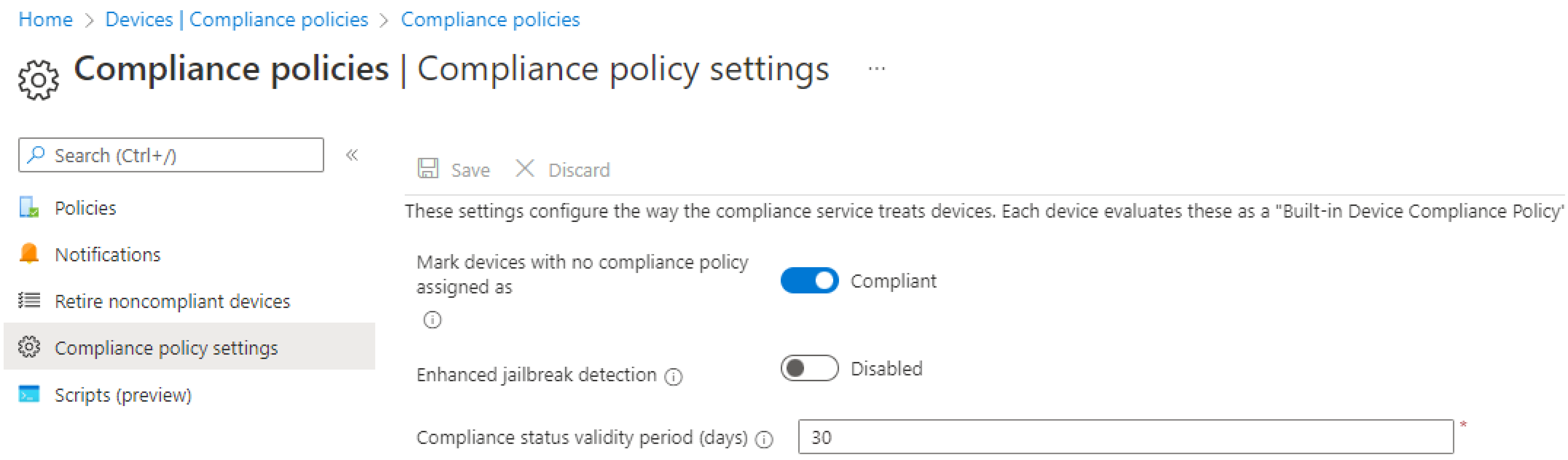


Home > Devices | Enroll devices > Enroll devices

Enroll devices | Corporate device identifiers ...

Search (Ctrl+/)
«
Windows enrollment
Apple enrollment
Android enrollment
Enrollment device limit restrictions
Enrollment device platform restrictions
Corporate device identifiers
Device enrollment managers
+ Add
Delete
Refresh
Filter
Columns
Export
Search by identifier

	Identifier Type	Identifier	Details	Date Added	Status
□	Serial	64167F292C34	polycom - trio8800	9/29/21, 3:47 PM	Enrolled
□	Serial	64167FDFBC6C	poly - ccx600	9/29/21, 3:46 PM	Enrolled
□	Serial	64167FF1A41C	Poly CCX500	4/05/22, 5:50 PM	Not Contacted
□	Serial	801193C061201142	mp56	2/03/22, 11:14 AM	Enrolled
□	Serial	SC10241278	audiocodes - c450hd	9/29/21, 3:25 PM	Enrolled



Home > Devices | Compliance policies > Compliance policies

Compliance policies | Compliance policy settings

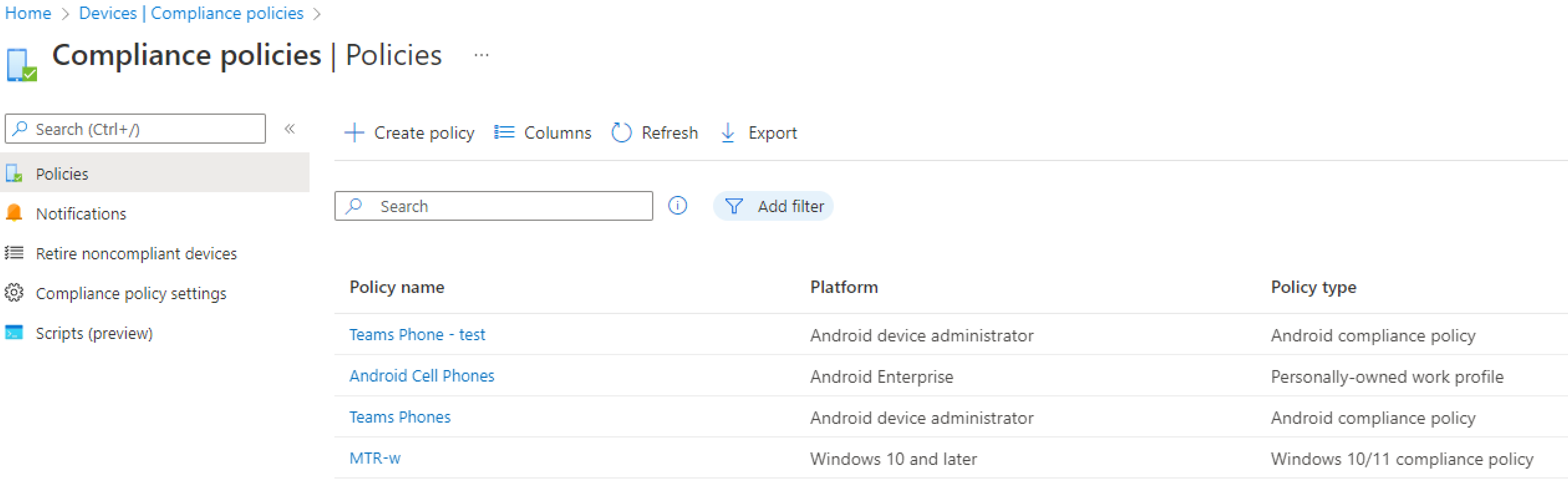
...
Search (Ctrl+/)
«
Policies
Notifications
Retire noncompliant devices
Compliance policy settings
Scripts (preview)
Save
Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy'

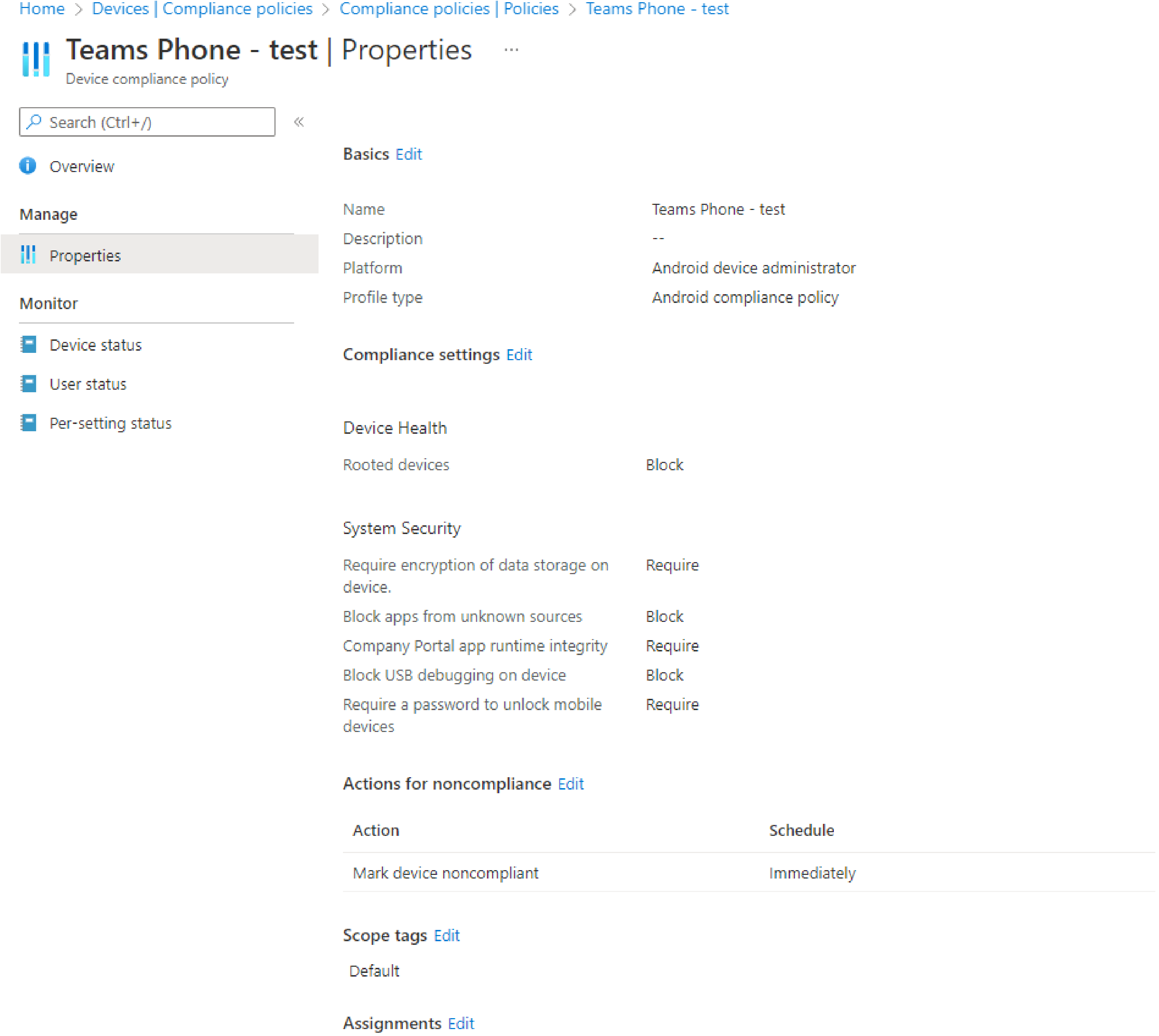
Mark devices with no compliance policy assigned as ⓘ Compliant

Enhanced jailbreak detection ⓘ Disabled

Compliance status validity period (days) ⓘ 30 *


Home > Devices | Compliance policies >
Compliance policies | Policies ...
Search (Ctrl+/)
Policies
Notifications
Retire noncompliant devices
Compliance policy settings
Scripts (preview)
+ Create policy
Columns
Refresh
Export
Search
Add filter

Policy name	Platform	Policy type
Teams Phone - test	Android device administrator	Android compliance policy
Android Cell Phones	Android Enterprise	Personally-owned work profile
Teams Phones	Android device administrator	Android compliance policy
MTR-w	Windows 10 and later	Windows 10/11 compliance policy



Teams Phone - test | Properties

Device compliance policy

Basics Edit

Name	Teams Phone - test
Description	--
Platform	Android device administrator
Profile type	Android compliance policy

Compliance settings Edit

Device Health

Rooted devices	Block

System Security

Require encryption of data storage on device.	Require
Block apps from unknown sources	Block
Company Portal app runtime integrity	Require
Block USB debugging on device	Block
Require a password to unlock mobile devices	Require

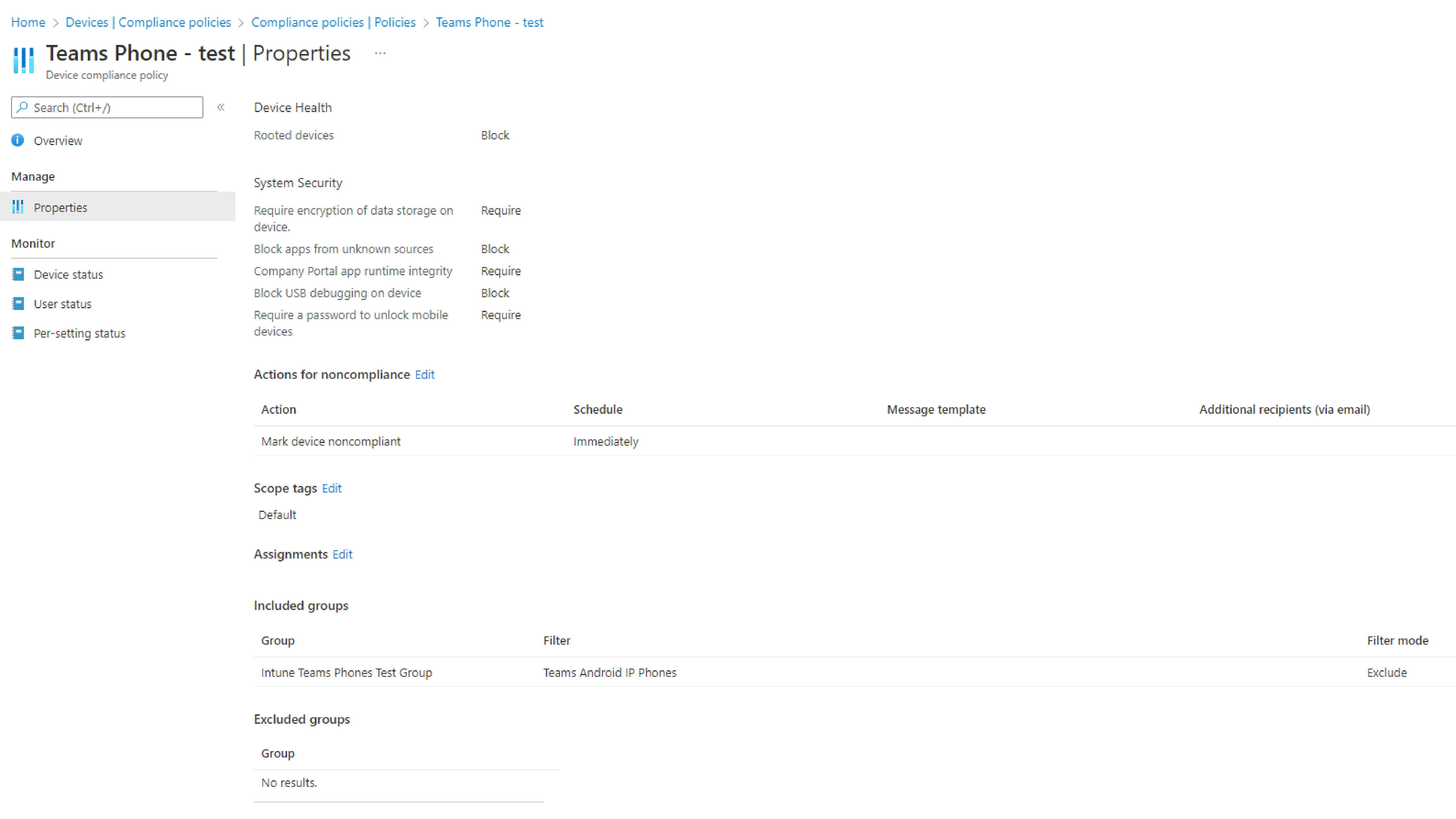
Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately

Scope tags Edit

Default

Assignments Edit



Home > Devices | Compliance policies > Compliance policies | Policies > Teams Phone - test
Search (Ctrl+/)
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status

Teams Phone - test | Properties

Device compliance policy

Device Health

Rooted devices	Block

System Security

Require encryption of data storage on device.	Require
Block apps from unknown sources	Block
Company Portal app runtime integrity	Require
Block USB debugging on device	Block
Require a password to unlock mobile devices	Require

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags Edit

Default

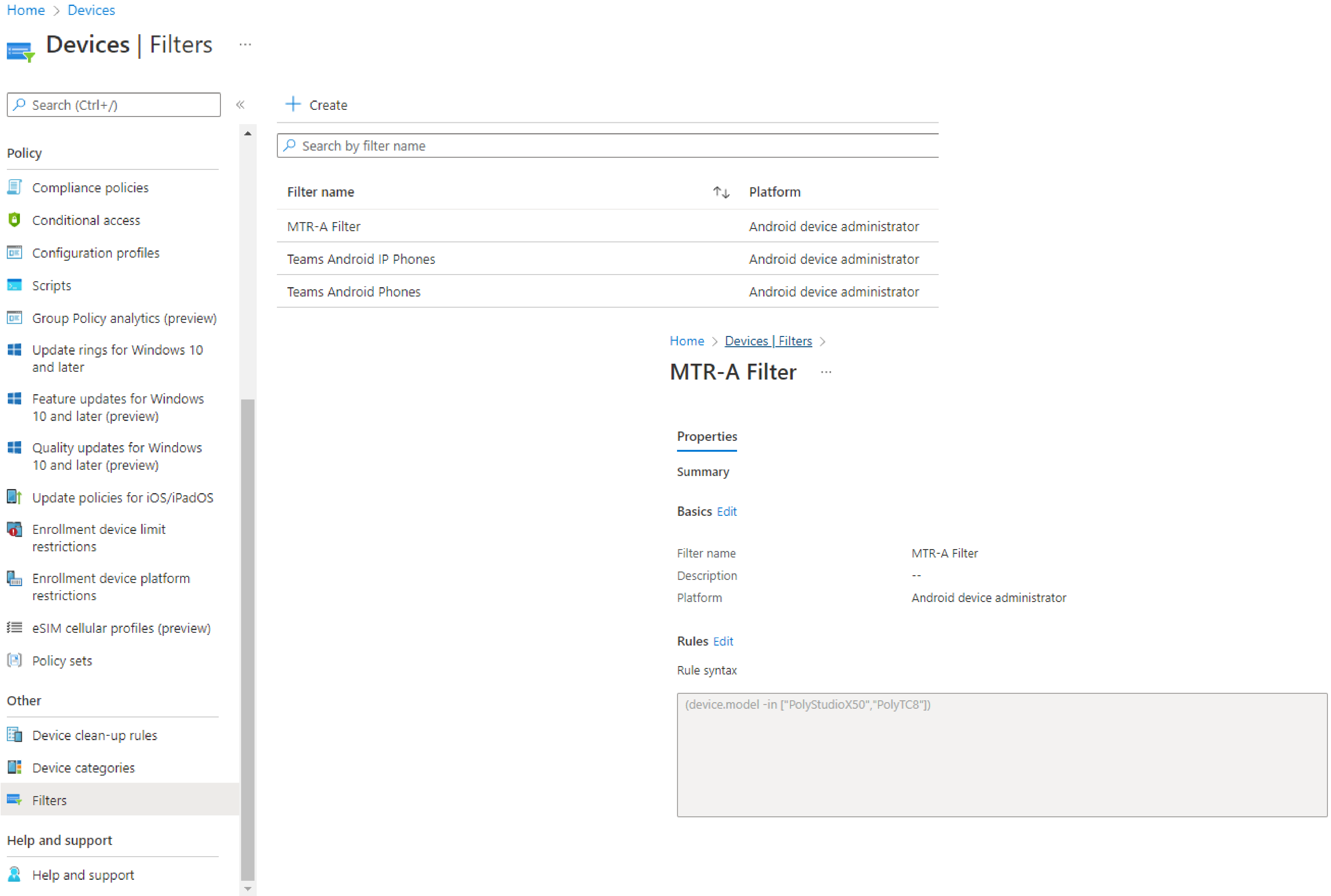
Assignments Edit

Included groups

Group	Filter	Filter mode
Intune Teams Phones Test Group	Teams Android IP Phones	Exclude

Excluded groups

Group
No results.



Home > Devices
Devices | Filters
Search (Ctrl+/)
Policy
Compliance policies
Conditional access
Configuration profiles
Scripts
Group Policy analytics (preview)
Update rings for Windows 10 and later
Feature updates for Windows 10 and later (preview)
Quality updates for Windows 10 and later (preview)
Update policies for iOS/iPadOS
Enrollment device limit restrictions
Enrollment device platform restrictions
eSIM cellular profiles (preview)
Policy sets
Other
Device clean-up rules
Device categories
Filters
Help and support
Help and support
+ Create
Search by filter name

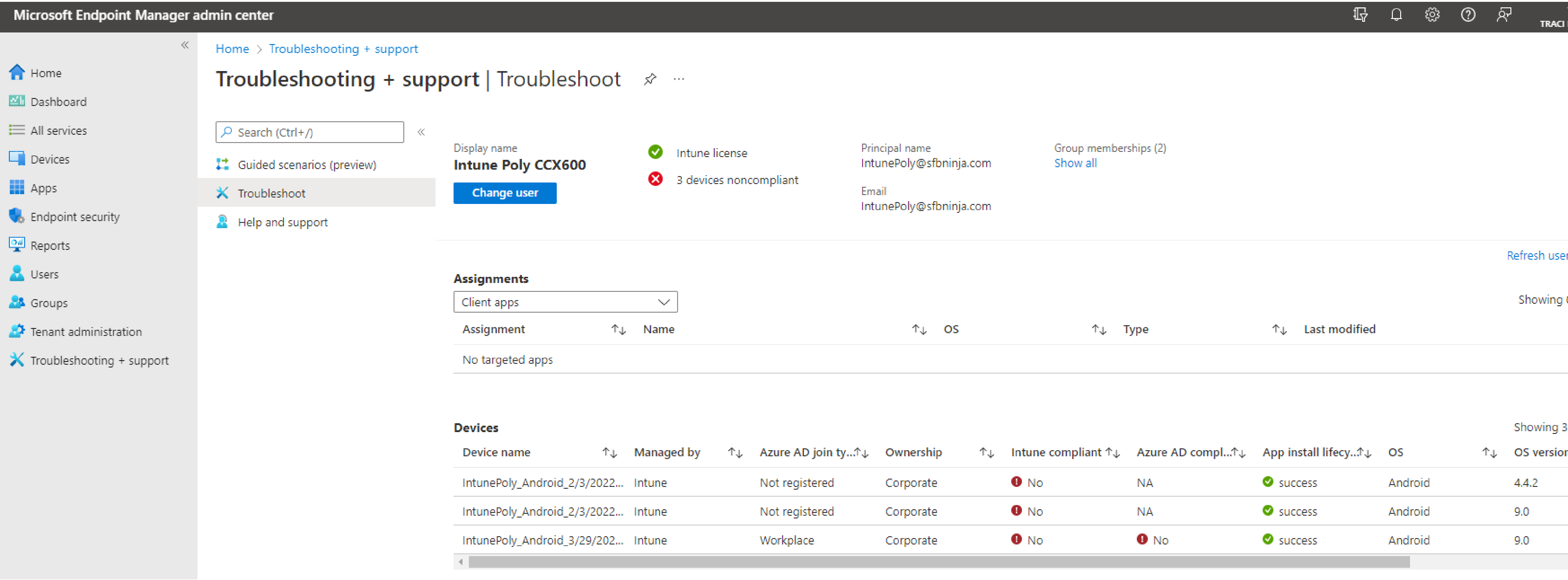
Filter name	Platform
MTR-A Filter	Android device administrator
Teams Android IP Phones	Android device administrator
Teams Android Phones	Android device administrator

Home > Devices | Filters >
MTR-A Filter
Properties
Summary
Basics Edit

Filter name: MTR-A Filter
Description: --
Platform: Android device administrator

Rule syntax

```
(device.model -in ["PolyStudioX50","PolyTC8"])
```



Troubleshooting + support | Troubleshoot

Display name
Intune Poly CCX600

✓ Intune license

✗ 3 devices noncompliant

Principal name
IntunePoly@sfbninja.com

Email
IntunePoly@sfbninja.com

Group memberships (2)

Assignments

Client apps

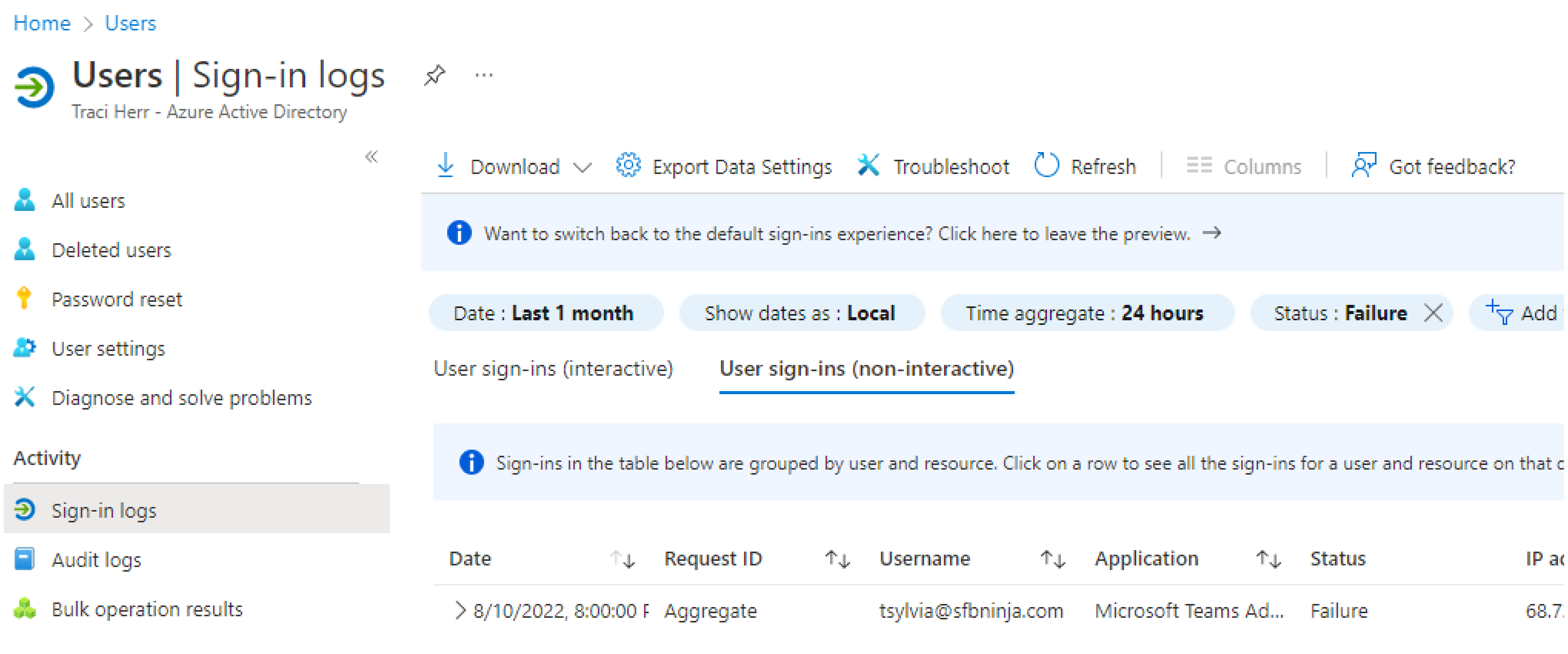
Showing

Assignment	Name	OS	Type	Last modified
No targeted apps				

Devices

Showing 3

Device name	Managed by	Azure AD join ty...	Ownership	Intune compliant	Azure AD compl...	App install lifecy...	OS	OS versio
IntunePoly_Android_2/3/2022...	Intune	Not registered	Corporate	❗ No	NA	✓ success	Android	4.4.2
IntunePoly_Android_2/3/2022...	Intune	Not registered	Corporate	❗ No	NA	✓ success	Android	9.0
IntunePoly_Android_3/29/202...	Intune	Workplace	Corporate	❗ No	❗ No	✓ success	Android	9.0

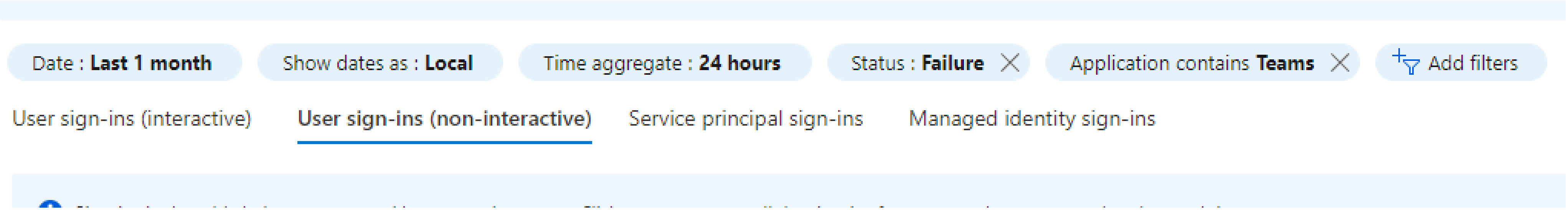


Want to switch back to the default sign-ins experience? Click here to leave the preview. →

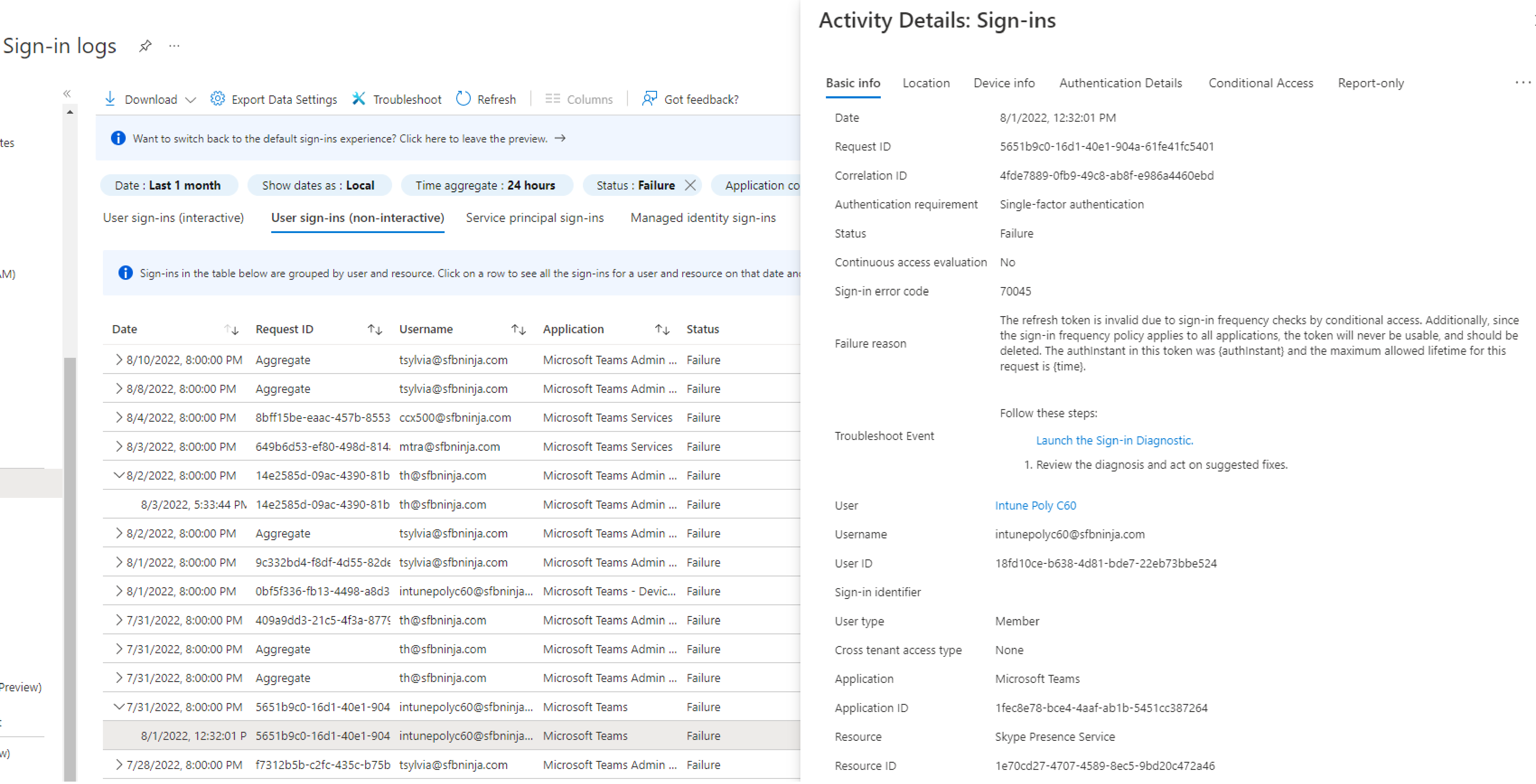
Date : **Last 1 month** | Show dates as : **Local** | Time aggregate : **24 hours** | Status : **Failure**

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.


Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

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



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

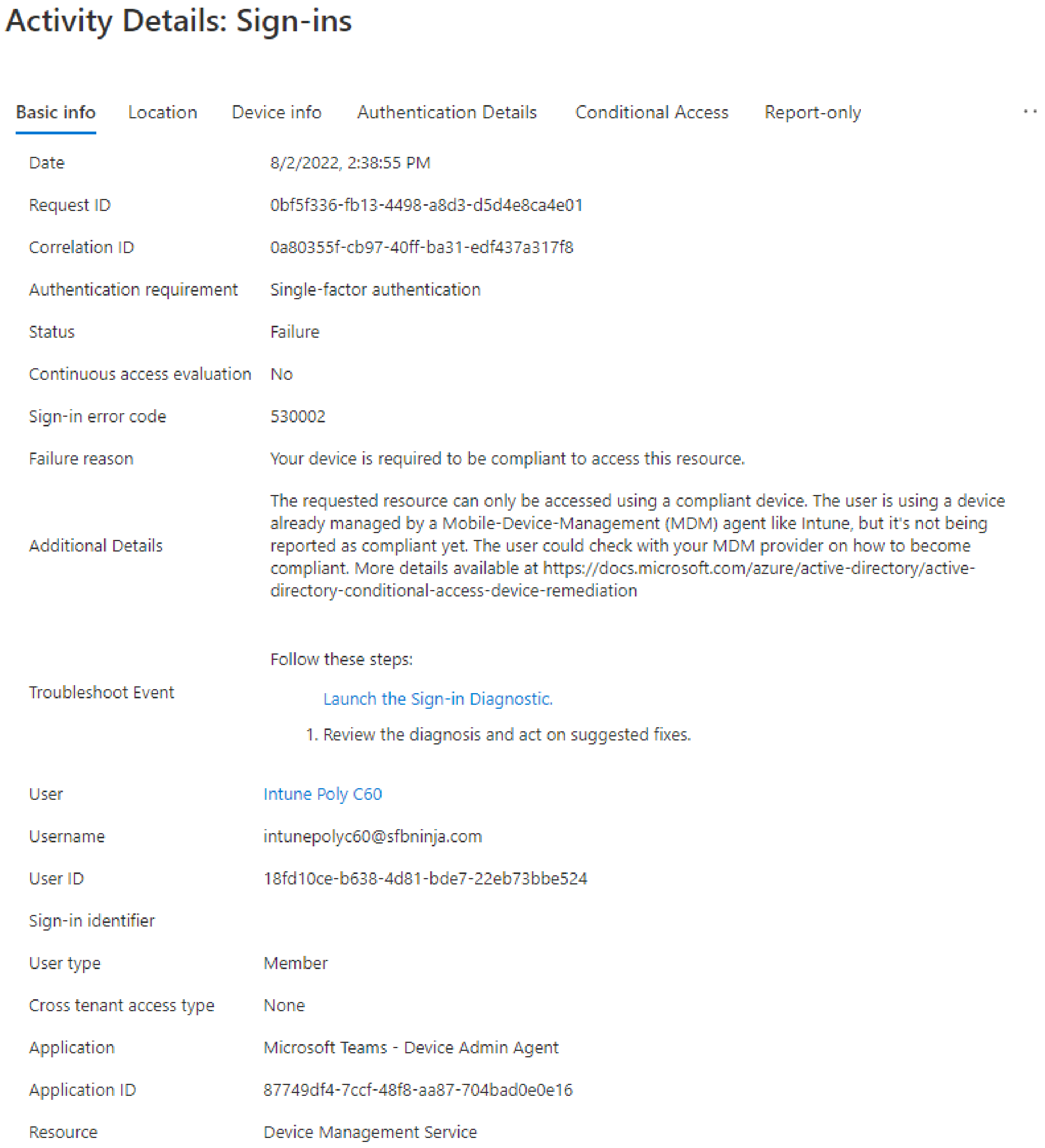
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

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 anc

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 PN	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

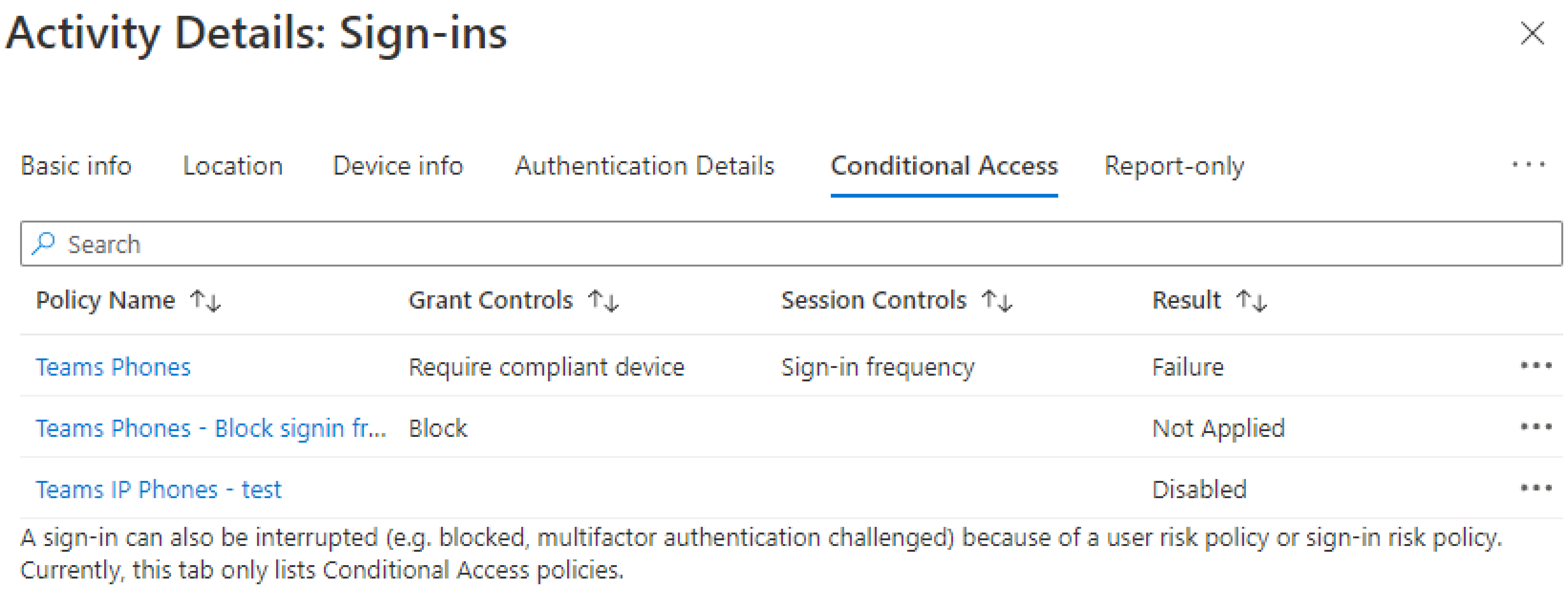
Activity Details: Sign-ins

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

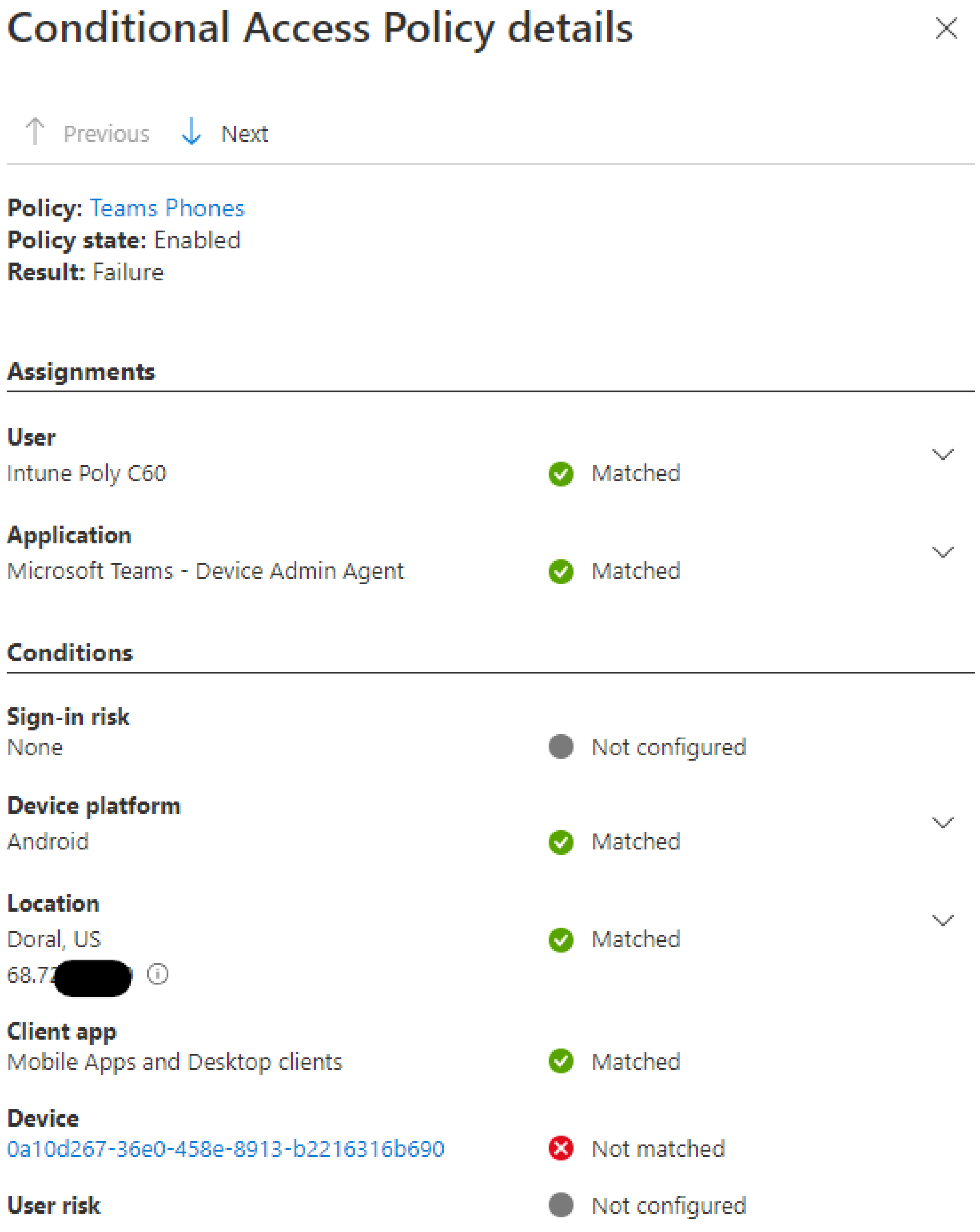
Date	8/2/2022, 2:38:55 PM
Request ID	0bf5f336-fb13-4498-a8d3-d5d4e8ca4e01
Correlation ID	0a80355f-cb97-40ff-ba31-edf437a317f8
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	530002
Failure reason	Your device is required to be compliant 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

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

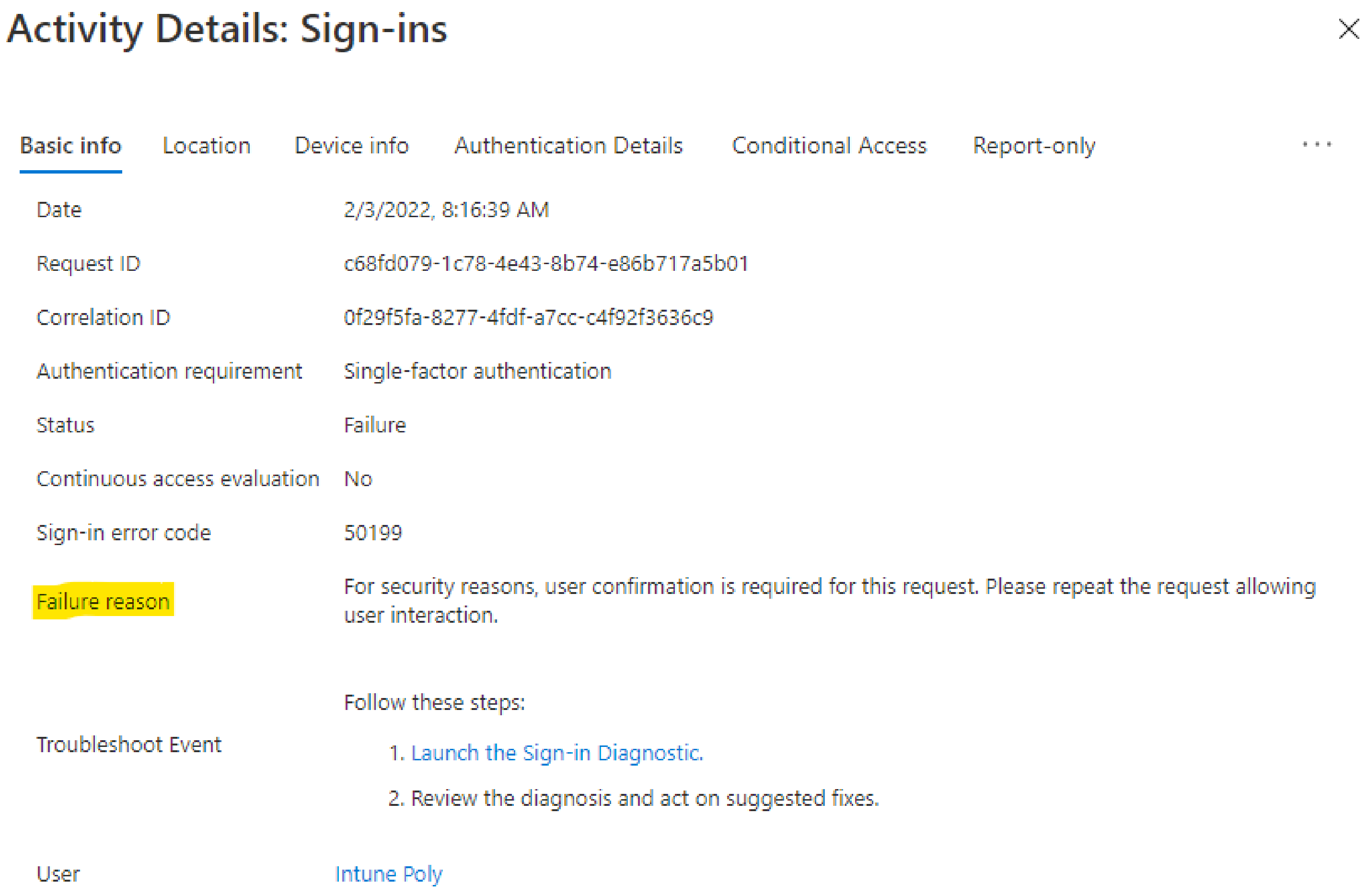
Policy: Teams Phones
Policy state: Enabled
Result: Failure

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 68.7[redacted] ⓘ	✓ Matched
Client app Mobile Apps and Desktop clients	✓ Matched
Device 0a10d267-36e0-458e-8913-b2216316b690	✗ Not matched
User risk	● Not configured



Activity Details: Sign-ins

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

Teams Rooms, Phones, Panels and Displays Best Practices and Supportability Docs (not NDA)

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

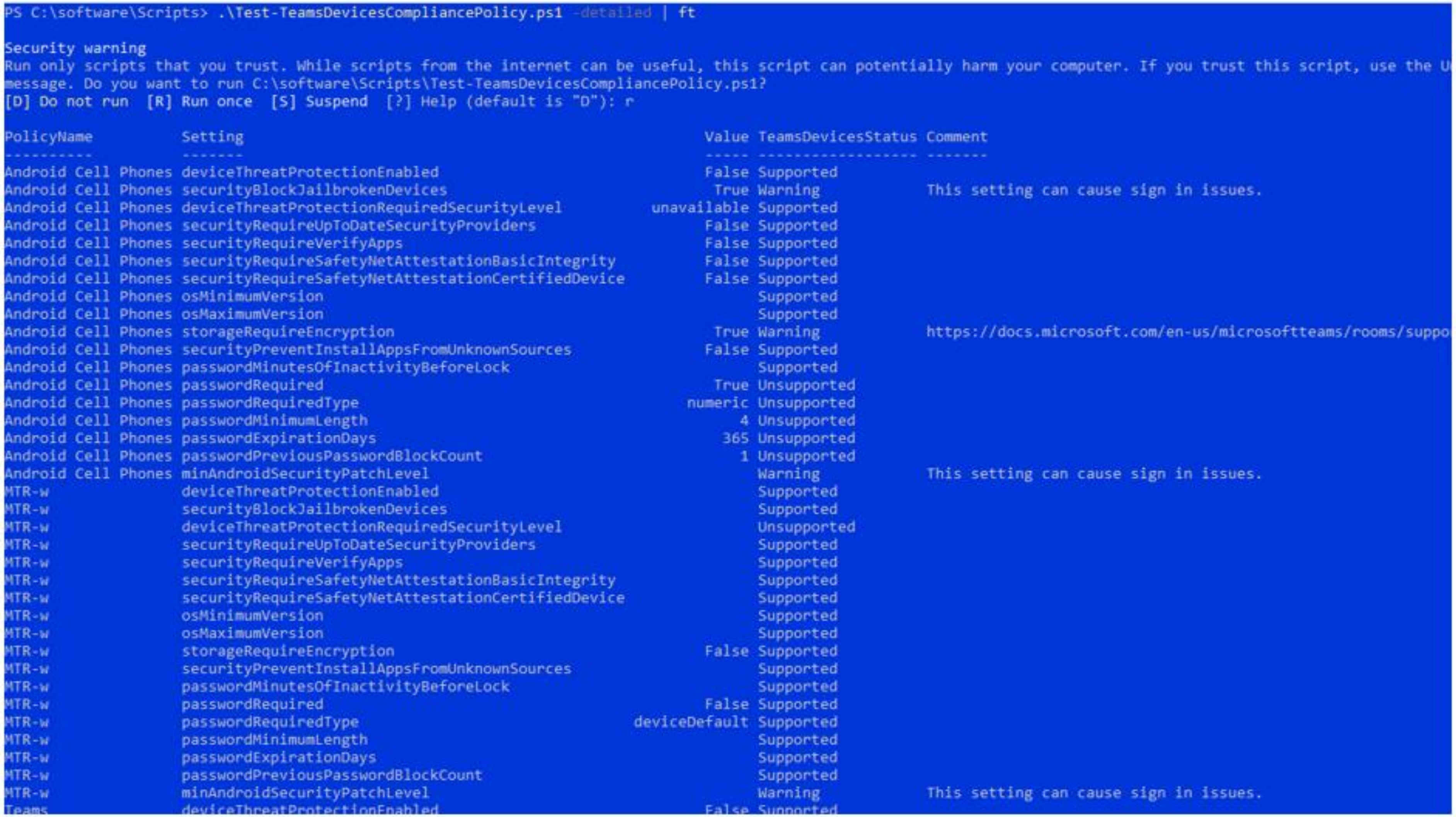
Intune

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/

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
```

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

Questions?