



BeConnected *day*

Microsoft Teams Device Universe



Roberto Ferazzi

Business & Technical Advisor @ FAR Networks



Fabrizio Volpe

Solution Architect @ Symity



Luca Vitali

Cloud Collaboration & Security PM @ Centro Computer



Teamwork across spaces and devices



United by Microsoft Teams



Individual workspaces

Individual office or dedicated workspace
On the go or in transit at home



Group workspaces

Small, medium and large meeting rooms
huddle/focus spaces and touchdown spaces
collaboration workspaces



Personal devices



Audio & video peripherals

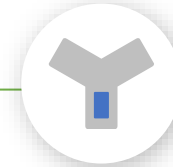


PCs and Mobile

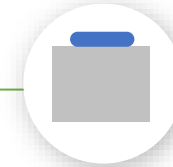


Phones

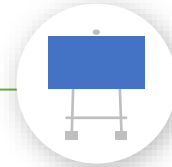
Shared devices



Conference phones



Teams Rooms

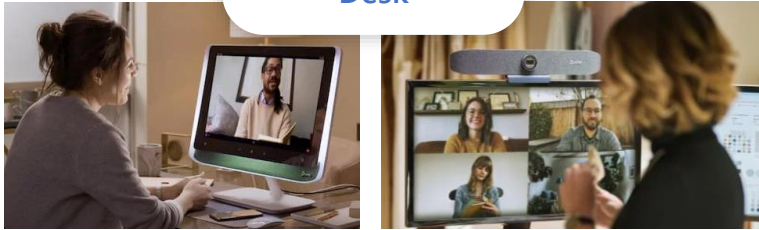


Surface Hub

Una soluzione per ogni spazio



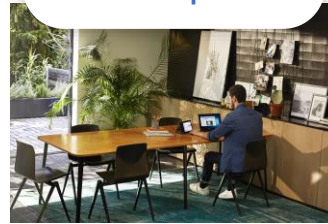
Desk



Headsets and speakers

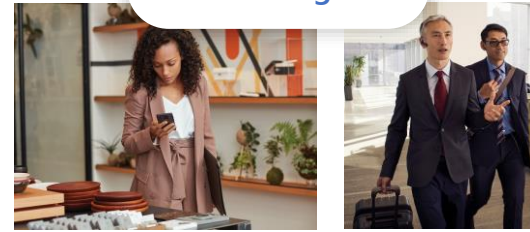
Webcams

Third space



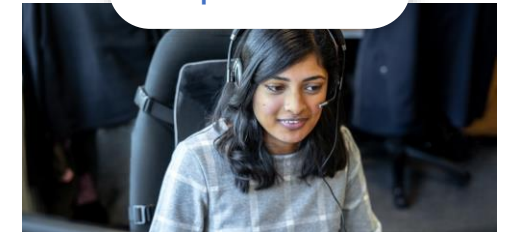
Monitors

On the go



Phones

Open office



Displays



Microsoft Teams personal space devices

Microsoft Teams peripherals



SENNHEISER



EPDS



logitech



Jabra



poly

Microsoft Teams phones



poly



audiocodes



Microsoft Teams displays New category



Lenovo

Browse full selection at Devices Showcase office.com/teamsdevices

25 Novembre 2021

<https://www.beconnectedday.it>

#BCD25Nov21

Teams Phone



Touch phones



Audiocodes C448 HD



Audiocodes C470 HD



Poly CCX400/500



Audiocodes C450 HD



Poly CCX 600

Non-Touch phones

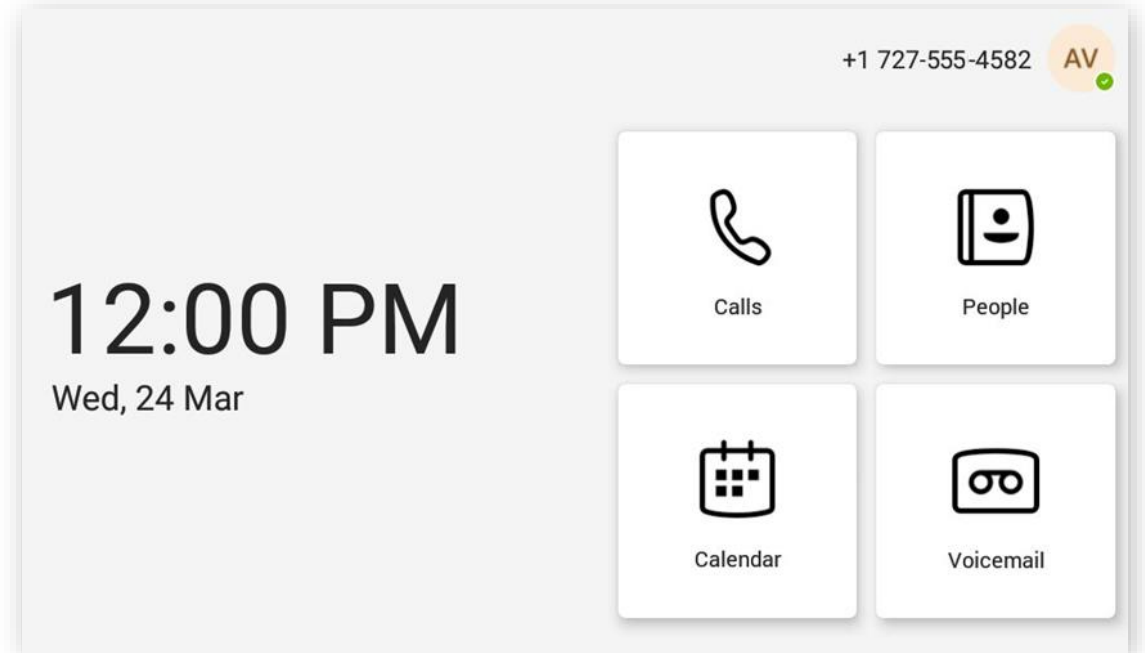
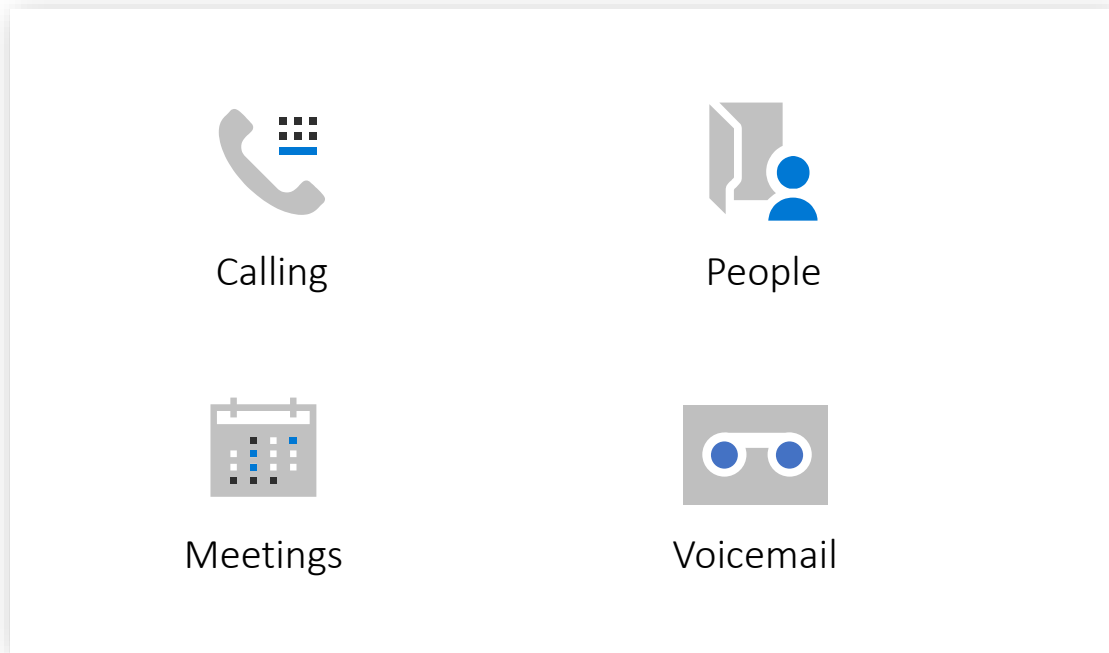


AudioCodes C435



Poly Trio C60

Teams Phone experience



SIP Gateway (coming soon)



Leverage your existing SIP phone investments

User authentication

Core calling features

Inbound / outbound calls to Teams or PSTN (hold/resume with music, mute/unmute, DTMF)

Call transfer (single step/blind, consulted transfer)

Dial in/out from a meeting (audio conferencing)

Device-only “do not disturb”

Voicemail and message waiting indicator

Integrated into Teams routing policies/regulations

Device inventory management in Teams admin center

Static emergency calling, static emergency location support with security desk notifications

Compatible SIP phones



Cisco IP Phones with MPP firmware (6821, 6901, 7800 series, 8800 series)



Polycom SIP phones (VVX series 100, 200, 300, 400, 500, 600 etc.)



Yealink (T20 series, T30 series, T40 series, T50 series)

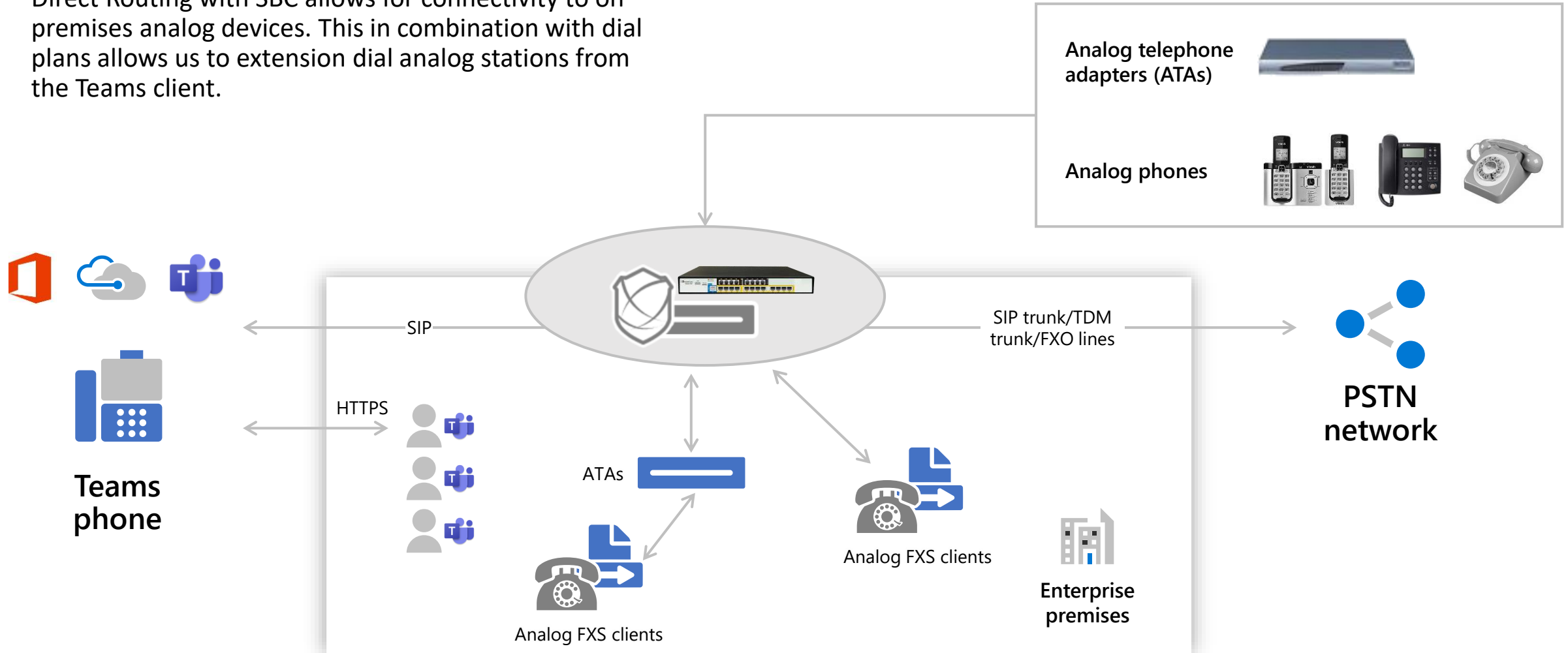


AudioCodes 400 HD series

Analog Device Interop certification



Direct Routing with SBC allows for connectivity to on premises analog devices. This in combination with dial plans allows us to extension dial analog stations from the Teams client.



Microsoft Teams Room Systems



Microsoft Teams Room



Microsoft Teams Room (MTR o MTRoW)



Logitech Tap

Poly Studio MTR Solutions

Microsoft Teams Room on Android (MTRoA)

Logitech Rally Bar e Rally Bar Mini



Poly Studio X30, X50 e X70



MTR vs MTR on Android



Principali Funzionalità	MTR on Windows	MTR on Android
Display Support	Single or Dual HDMI displays with optional touch support	Single or Dual HDMI displays with optional touch support
Support for external cameras, room audio systems	SI	NO
Transmit video resolution	Fino a 1080p	Fino a 1080p
Support zoom and WebEx	SI	NO
HDMI Input	SI	SI
Pin e Spotlight participant	SI	NO
Content camera	SI	NO
Coordinated meetings with Surface Hub	SI	NO

Teams devices for shared spaces feature comparison between Windows and Android

<https://docs.microsoft.com/en-us/microsoftteams/rooms/teams-devices-feature-comparison>

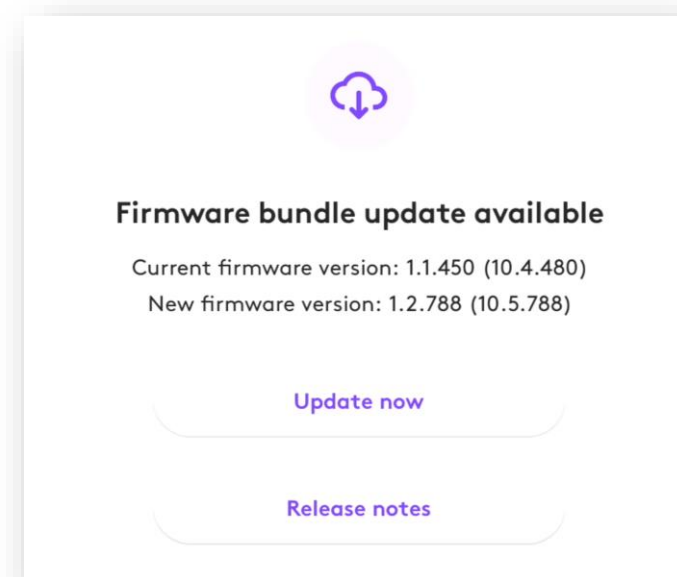
MTRoA: principali differenze



Anche se MS sta portando le soluzioni MTRoA verso la parità di funzioni con le tradizionali MTRoW, ci sono alcune differenze intrinseche:

i device basati su Android assomigliano molto ai tradizionali Codec da sala, con hw proprietario e fw monolitici.

Questo li rende molto più semplici da gestire ed aggiornare rispetto alle soluzioni basate su Windows



MTRoA: principali differenze



- il fw è blindato, rendendoli molto difficili da attaccare (quasi impossibile?). Sempre più Aziende propendono verso queste soluzioni per via degli aspetti legati alla sicurezza.



MTRoA: principali differenze



- i controller touch da tavolo sono stati pensati fin dall'inizio con connessione di rete lan in Cat5e POE, rendendo l'installazione molto più semplice
- l'HDMI Injection (content sharing) è previsto sul device, non tramite Touch da tavolo, rendendo anche in questo caso l'installazione più semplice



MTRoW

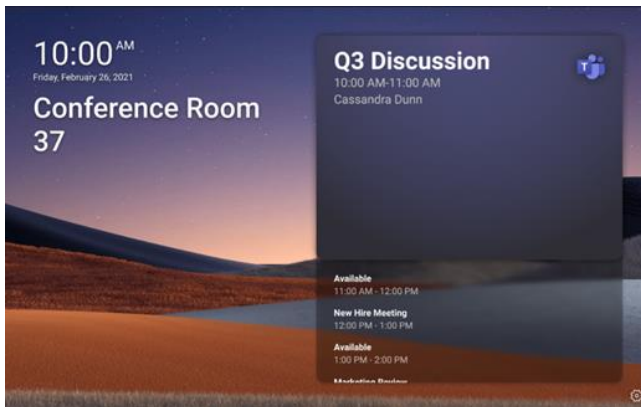
Gestione dei Teams Device



Gestione dei device: Overview



- I dispositivi certificati che possono essere registrati in Microsoft Teams includono: Collaboration bars, Conference phones, Desk phones, Microsoft Teams Rooms, Teams displays and Teams panels
- Sebbene alcune attività di gestione di base siano disponibili nell'interfaccia di amministrazione di Teams, un modo più completo per gestire i dispositivi richiede l'uso di Azure Active Directory, Intune e Microsoft Mobile Device Management



Gestione dei device: Teams Admin Center

- Monitoraggio di base delle Meeting Rooms

The image illustrates the navigation and monitoring process in the Teams Admin Center. On the left, a dark navigation pane shows 'Teams devices' expanded to 'Teams Rooms on Windows'. The main content area displays the 'Teams Rooms on Windows' overview, which includes a 'Devices summary' table and a 'Health summary' table.

Devices summary		
32	32	0
Total	Online	Offline

Health summary		
31	0	1
Healthy	Non-urgent	Critical

Below the overview, a list of devices is shown, with 'logitech-tap G6B' highlighted as 'Critical'. An arrow points from this device to a detailed 'Health status' panel on the right. This panel shows the device name 'logitech-tap G6B' and a notification: 'You can now configure how the status of each peripheral will impact the health status of their parent device.' Below this, a 'Critical issues (1)' section contains a message: 'Your Display 2 is disconnected. Check the device's physical connection and power source. Nov 23, 2021, 4:41 PM'.

Gestione dei device: Teams Admin Center



- Monitoraggio di base delle Meeting Rooms

Peripheral health

Manage health impact | 8 peripherals

Peripheral	Name	Offline since	Health status	Health impact
✓ HDMI ingest	Crestron Flex	--	Connected	Critical
Compute	Crestron Electronics UC-Engine	--	Connected	Critical
Room camera	N/A	Nov 19, 2021, 6:10 PM	Disconnected	Critical
Content camera	Logi Rally Camera	--	Connected	Critical
Speaker	Shure P300 Echo Cancelling Speakerphone (Shure Intelli...	--	Connected	Critical
Conferencing speaker	Shure P300 Echo Cancelling Speakerphone (Shure Intelli...	--	Connected	Critical
Microphone	Shure P300 Echo Cancelling Speakerphone (Shure Intelli...	--	Connected	Critical
Display 1	Display 1	--	Connected	Critical

Connectivity health

Connectivity indicator	Health problem reason	Offline since	Health status
✓ Network		--	Connected
Sign in (Exchange)		Nov 19, 2021, 6:10 PM	Disconnected
Sign in (Skype for Business)		Nov 19, 2021, 6:10 PM	Disconnected
Sign in (Microsoft Teams)		--	Connected

Gestione dei device: Teams Admin Center



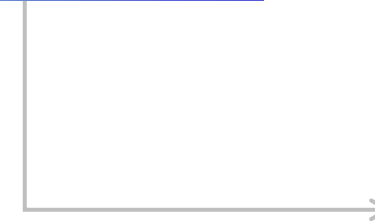
- Gestione di base dei desk phones

✓	Display name	Username	Device name	Health status	Manufacturer	Model	IP address	Tags	Configuration profile
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	--
			poly-ccx400 6416	Offline	poly	ccx400		--	--
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	--
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	--
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	Polycom
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	--
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	Polycom
			poly-ccx400 6416	Offline	poly	ccx400		--	Polycom
			poly-ccx400 6416	Non-urgent	poly	ccx400		--	--
			yealink-t55a 3151	Offline	yealink	t55a		--	--
			audiocodes-c450	Offline	audiocodes	c450hd		--	--

Conditional Access



- Conditional Access è una funzionalità di Azure Active Directory (Azure AD) che consente di garantire che i dispositivi che accedono alle risorse di Office 365 siano gestiti correttamente e siano sicuri
- Se si applicano Conditional Access condizionale al servizio Teams, i dispositivi Android (inclusi telefoni Teams, display Teams e Microsoft Teams Rooms in Android) che accedono a Teams devono essere registrati in Intune e le relative impostazioni devono essere conformi ai criteri
- Se il dispositivo non è registrato in Intune o se è registrato ma le sue impostazioni non sono conformi ai criteri, Conditional Access impedirà a un utente di accedere o usare l'app Teams nel dispositivo.



Grant ×

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

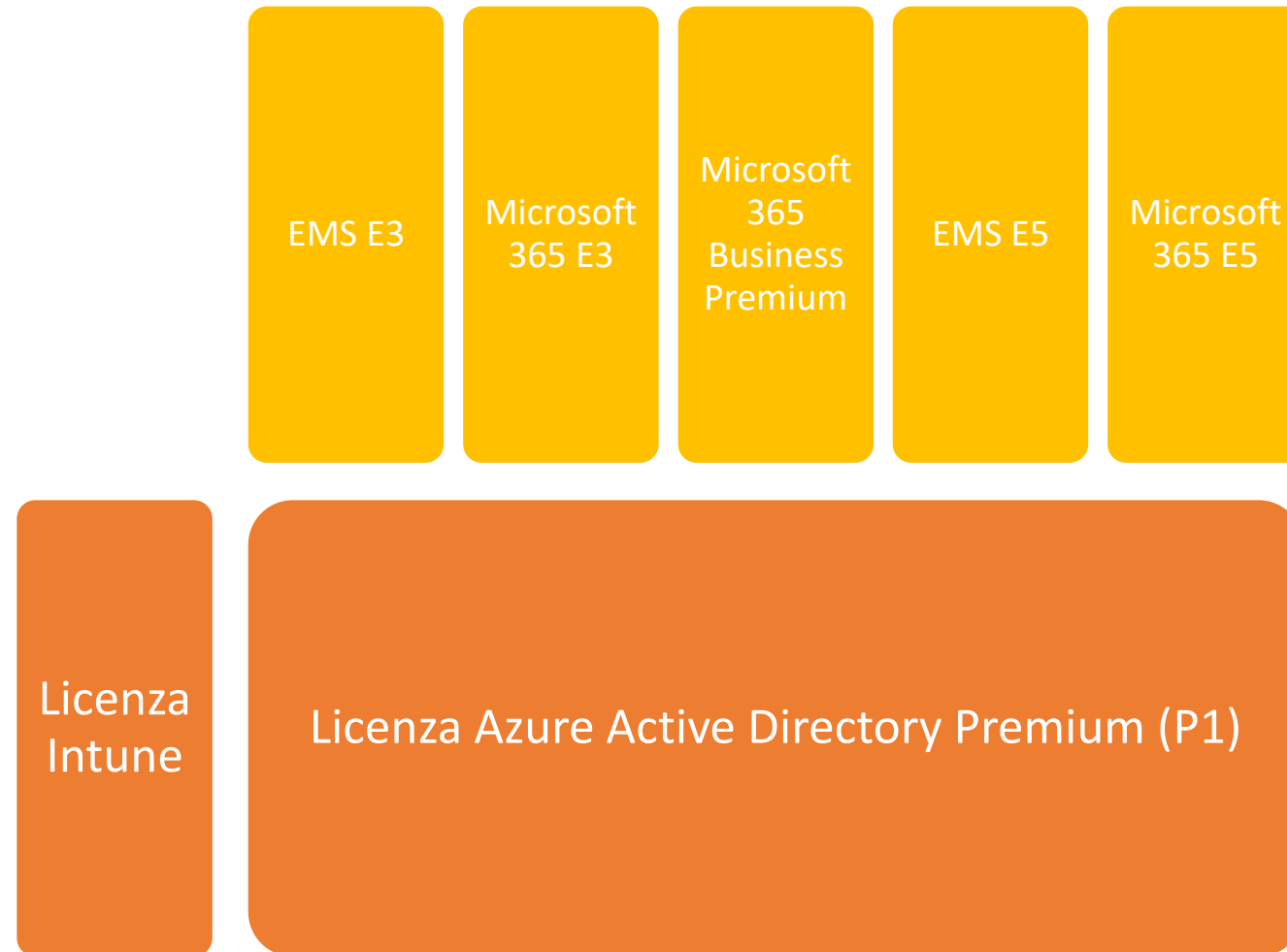
Require app protection policy ⓘ
[See list of policy protected client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

Conditional Access - Licenze



Conditional Access – Azure AD (ed in MEM)

Azure Active Directory admin center

Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications

All services

All

General

Identity

Security

Hybrid

General (1)

Help + support

Identity (19)

- Azure Active Directory
- Azure AD Connect Health
- Azure AD Conditional Access**

Home >

Devices | Overview

Search (Ctrl+/)

Overview

All devices

Monitor

By platform

- Windows
- iOS/iPadOS
- macOS
- Android

Device enrollment

- Enroll devices

Provisioning

- Windows 365

Policy

- Compliance policies
- Conditional access**

Conditional Access – Azure AD



All services > Conditional Access >

New ...

Conditional Access policy

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

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

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

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

- None
- All cloud apps
- Select apps


Select

- None
- Select at least one app.

Select

Cloud apps

teams

 Microsoft Teams
cc15fd57-2c6c-4117-a88c-83b1d56b4bbe

Conditional Access – Azure AD



All services > Conditional Access >

New ...

Conditional Access policy

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

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

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

Device platforms ⓘ

Not configured

Locations ⓘ

0 included

✘ With "Selected locations" you must choose at least one location.

Client apps ⓘ

Not configured

Device state (Preview) ⓘ

Not configured

Filter for devices ⓘ

Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

- Any location
- All trusted locations
- Selected locations

Select

None

✘ Choose at least one location

Select

Locations

Location type : All types

Trusted type : All types

Search names

Name	Location type	Trusted
<input type="checkbox"/> MFA Trusted IPs	IP ranges	Yes
<input type="checkbox"/> Internal IPs	IP ranges	Yes
<input type="checkbox"/> Public IP Deskphone	IP ranges	Yes

Conditional Access – Azure AD Dynamic Groups

Azure Active Directory admin center

All services > Contoso > Groups > TeamsDeskPhones

Overview

TeamsDeskPhones
Teams Users Desk Phones

Membership type: Dynamic

Source: Cloud

Type: Security

Object Id: 8ee97f80-7f20-4a5f-9e09-f46e4b971e97

Creation date: 9/9/2021, 11:31:48 AM

Membership processing status: Update complete

Membership last updated: 9/9/2021, 1:53:49 PM

Direct members

- 3 Total
- 0 User(s)
- 0 Group(s)
- 3 Device(s)
- 0 Other(s)

Group memberships: 0

Owners: 0

Total members: 3

General settings

Group name *

Group description

Group type: Security

Membership type *

Object Id: 8ee97f80-7f20-4a5f-9e09-f46e4b971e97

Azure AD roles can be assigned to the group

TeamsDeskPhones | Dynamic membership rules

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.

And/Or	Property	Operator	Value
Or	displayName	Starts With	Johanna
Or	displayName	Starts With	Poly

Rule syntax: `(device.displayName -startsWith "Johanna") or (device.displayName -startsWith "Poly")`

Microsoft Endpoint Manager (MEM)



Microsoft Endpoint Manager admin center

Home > **Devices | Overview**

Search (Ctrl+/)

Enrollment status | Enrollment alerts | Compliance status | Configuration status | Software update status

Intune enrolled devices
LAST UPDATED 11/24/21, 9:32 AM

Platform	Devices
Android	1
Windows	1
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	2

Enrollment failures by OS

OS	Failures
iOS	0
macOS	0
Android	0
Windows	0
Windows Mobile	0

Top enrollment failures this week

Failures	Count
No data to display	

Android | Android devices

Search (Ctrl+/) Refresh Filter Columns Export Bulk Device Actions

Filters applied: OS

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufacturer

Showing 1 to 1 of 1 records

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Primary user UPN
Johanna_Android_9/9/20...	Intune	Personal	Not Compliant	Android (device administra...	9.0	9/9/2021, 12:38:16 PM	JohannaL@M365B194434...

MEM: Teams Desk Phones

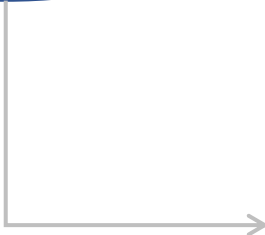
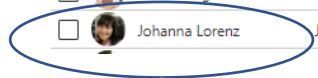


Home > **Users** | All users (Preview) ...
Contoso - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Preview info Got feedback?

This page includes previews available for your evaluation. View previews →

	Name	UPN	Member	Mobile	Phone	Account type	Account ID
<input type="checkbox"/>	Debra Berger	DebraB@M365B194434.OnMi...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Diego Siciliani	DiegoS@M365B194434.OnMi...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Emily Braun	EmilyB@M365B194434.OnMic...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Enrico Cattaneo	EnricoC@M365B194434.OnMi...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Federico	Federico@M365B194434.onm...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Grady Archie	GradyA@M365B194434.OnMi...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	HeatherW	HeatherW@m365b194434.on...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Henrietta Mueller	HenriettaM@M365B194434.O...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Irvin Sayers	IrvinS@M365B194434.OnMicr...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Isaiah Langer	IsaiahL@M365B194434.OnMic...	Member	No	Yes	Member	M365B194434.onmicrosoft.com
<input type="checkbox"/>	Johanna Lorenz	JohannaL@M365B194434.On...	Member	No	Yes	Member	M365B194434.onmicrosoft.com



Johanna Lorenz | Devices ...
User

Diagnose and solve problems Manage Profile Custom security attributes (preview) Assigned roles Administrative units Groups Applications Licenses **Devices** Azure role assignments Authentication methods

Enable Disable Delete Manage Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more ☞

Didn't find your device? View All devices
Search by name or device ID or object ID

3 devices found

	Name	Enabled	OS	Version	Join Type	MDM	Compliant	Registered	Activity
<input type="checkbox"/>	JohannaL_Android_9/9...	Yes	Android	9.0	Azure AD registered	Microsoft Intune	No	9/9/2021, 12:37:27 PM	9/9/2021, 12:37:27 PM
<input type="checkbox"/>	JohannaL_Android_9/9...	Yes	Android	9.0	Azure AD registered	Microsoft Intune	No	9/9/2021, 12:19:42 PM	9/9/2021, 12:19:42 PM
<input type="checkbox"/>	JohannaL_Android_9/9...	Yes	Android	9.0	Azure AD registered	Microsoft Intune	No	9/9/2021, 12:32:43 PM	9/9/2021, 12:32:43 PM

View devices syncing settings and app data

MEM: Device Compliance Policy



TeamsDeskPhonesCompliance | Properties ...
Device compliance policy

Search (Ctrl+/) <<

Overview

Manage

Properties

Monitor

- Device status
- User status
- Per-setting status

Properties

Name: teamsdeskphonescompliance
Description: Teams Desk Phones Compliance
Platform: Android device administrator
Profile type: Android compliance policy

Compliance settings Edit

Device Health

Rooted devices: Block

Device Properties

Minimum OS version: 10

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Send push notification to end user	Immediately
Remotely lock the noncompliant device	1 days

Scope tags Edit

Default

Assignments Edit

Included groups

Group	Filter (preview)
TeamsDeskPhones	IncludeCCX400

Excluded groups

Group

No results.

Devices | All devices ...

Search (Ctrl+/) <<

Refresh Filter Columns Export Bulk Device Actions

Overview

All devices

Monitor

By platform

- Windows
- iOS/iPadOS

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufacturer

Showing 1 to 2 of 2 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓
JohannaL_Android_9/9/2021_1...	Intune	Personal	Not Compliant
MWP-UK-47774	Intune	Corporate	Not Compliant

Domande?




BeConnected *day*



@ucugit



<https://www.linkedin.com/company/ucugit/>



<https://www.youtube.com/channel/UC-mC2XVA3gl9qpCvtOI5P1g>

