

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Deep dive on Cisco Microsoft Teams Rooms

Darren Henwood

BRKCOL-2688

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

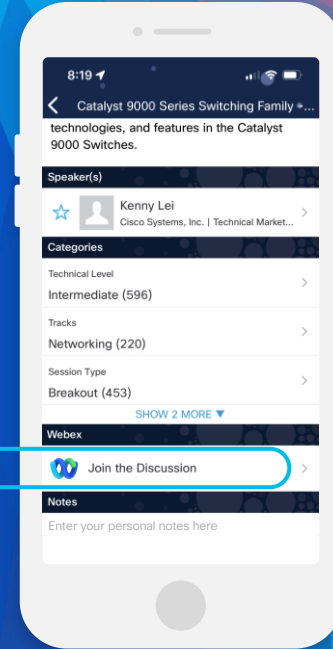
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://cislive.ciscoevents.com/cislivebot/#BRKCOL-2688>

Interoperability (Google, Microsoft, Zoom, Google, etc)

Licensing Implications

User Experience (consistency)

Webex Calling

Extensibility

SIP Calling



- VIMT (CVI – SIP)
- VIMT (WebRTC)
- MTR
- USB Passthrough

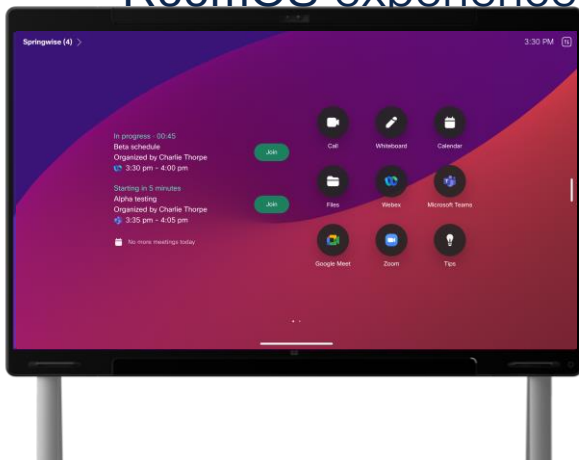
Agenda

- Introduction
- Architecture & Licensing
- Deployment
- Management
- Troubleshooting

Flexibility and Choice



RoomOS experience

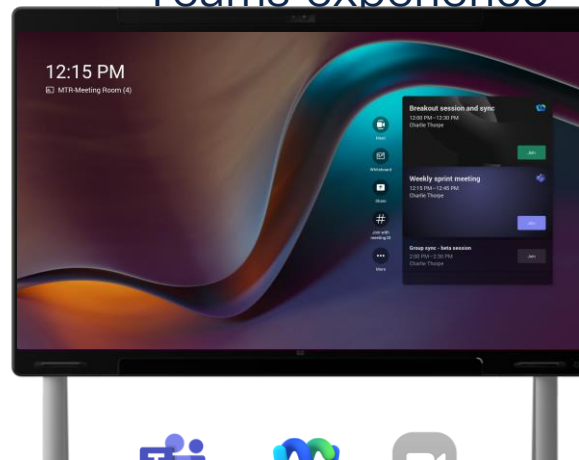


Includes native Webex Meetings and Events
with interop support for Microsoft Teams, Google, and Zoom

OR



Teams experience



Includes native Microsoft Teams
and Webex Meetings and Events

Same device, powered by Cisco RoomOS

Cisco devices for Microsoft Teams Rooms



Room Bar

Integrated video bar appliance designed for simple, flexible and cost-effective video-enablement of **small workspaces**



Room Bar Pro

Bringing together the best of both worlds with easy-to-deploy, AI-powered meetings scaled to the **medium workspace**



Room Kit EQ

Powerful room kit with the Quad Camera, AI-powered Codec EQ, and smart room peripherals for **medium to large workspaces**



Room Kit Pro

Advanced room kit with the Quad Camera, the powerful Codec Pro, and smart peripheral options for **very large workspaces** and specialist AV environments



Desk Pro

All-in-one video conferencing and digital whiteboarding for **jump rooms and huddle spaces**



Board Pro

All-in-one video conferencing and digital whiteboarding for **small to medium workspaces and ideation spaces**



Other devices (roadmap)

Microsoft Teams Display



Desk Pro

All-in-one video conferencing and digital whiteboarding for [Personal workspaces](#), [Hotdesking](#) and [Focus Spaces](#)

Expected early
2024

Microsoft Teams Panel

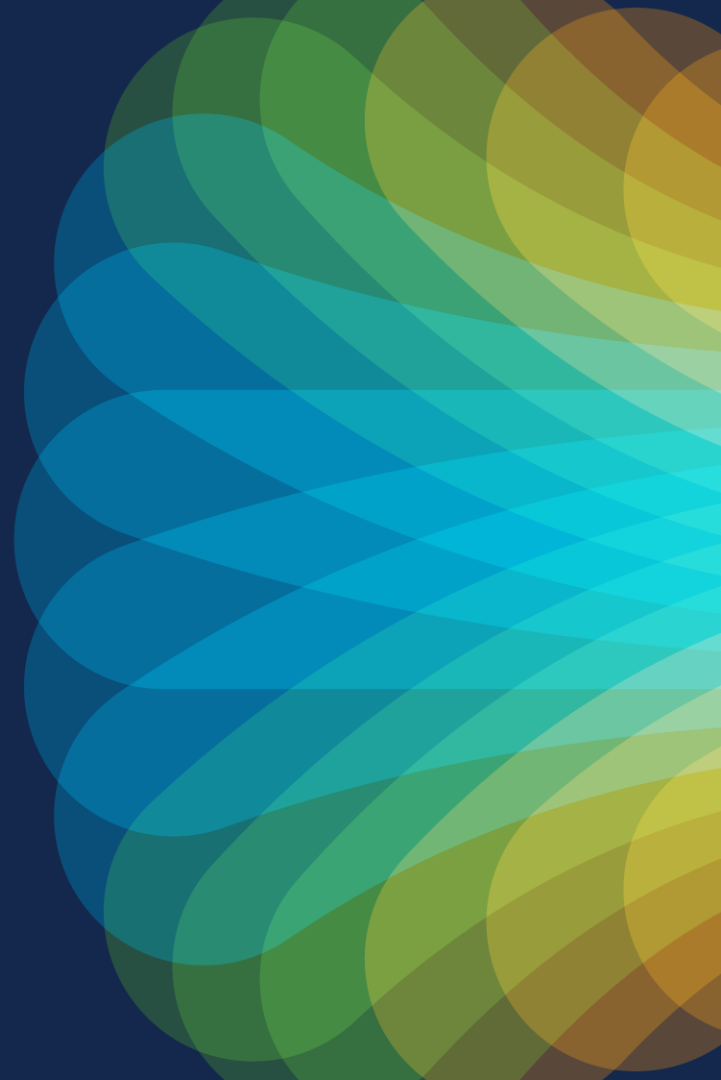


Room Navigator

Room booking panel for [workspaces](#)

2024

Architecture & Licensing



Teams Devices Management Portals

Microsoft 365
Admin Center

Teams Admin
Center

Microsoft Endpoint
Manager Portal

Azure Active
Directory Portal

Exchange Admin
Center

OEM Management
Portal (per OEM)

Microsoft Teams
Room Pro
Management Portal
(license required)

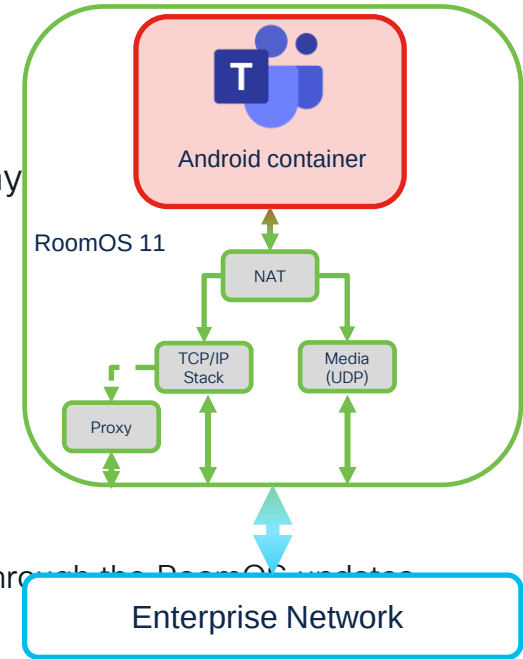
MTR Operating System



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

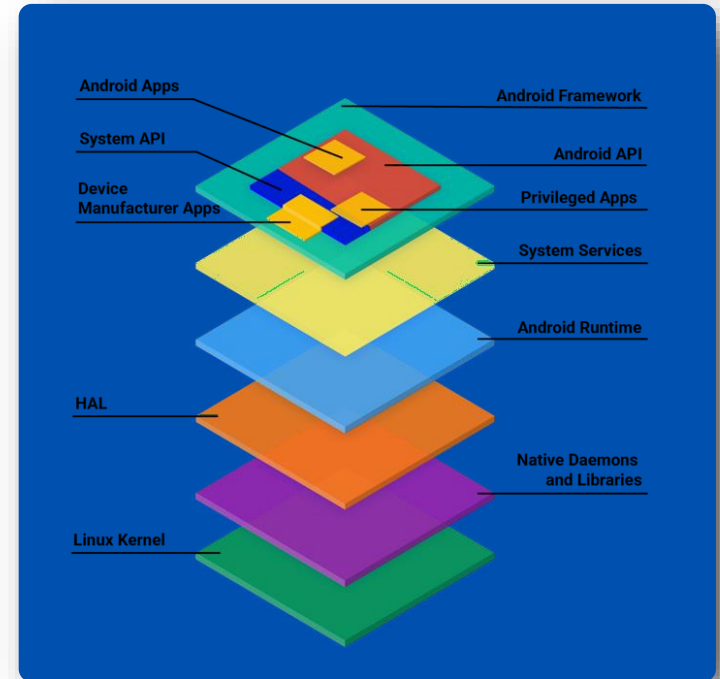
Cisco Devices Certified for Microsoft Teams Rooms

- Secure RoomOS environment
 - RoomOS is the OS running on Cisco Collaboration devices.
 - Purpose built for real-time collaboration and security
 - Microsoft Teams Rooms on Android is not visible to the network layer
 - Android 11/Android 12 is containerized on top of RoomOS
 - Network traffic is handled by RoomOS
 - Single IP Stack to network (RoomOS)
 - Single MAC address per device (RoomOS)
 - Single wireless configuration (RoomOS)
 - RoomOS updates include updates to the secure Android container
 - Updating of Android is not a customer commitment as this is taken care of through the RoomOS updates



Security Considerations

- Microsoft Teams Rooms on Android
- Android Container
 - Built on Android AOSP
 - Android is an open source operating system for mobile devices and a corresponding open source project led by Google. This site and the Android Open Source Project (AOSP) repository offer the information and source code needed to create custom variants of the Android OS, port devices and accessories to the Android platform, and ensure devices meet the compatibility requirements that keep the Android ecosystem a healthy and stable environment for millions of users.
 - RoomOS updates and Android updates will always be 1:1 – Meaning they will be released together. We sign all RoomOS builds today and will also be signing the Android release so that only approved apps can be installed.
 - Microsoft apps can be updated by Microsoft or Cisco. This is because we build in the Microsoft Applications to our release and the signing key from these apps are unique to Microsoft so that only they are able to update their apps directly.
 - We remove all applications not relevant or required for operation and no other applications are allowed to be installed.
 - Our existing PSIRT process requires us to be open about any known vulnerabilities including those discovered in Android. We will be patching those as they arise.
 - No current documentation on our builds or patches due to being a Cisco developed Android build.



Microsoft Teams Rooms licensing

	Microsoft Teams Rooms Basic	Microsoft Teams Rooms Pro
Maximum number of licenses	25	Unlimited
Microsoft Teams	✓	✓
Microsoft Teams Rooms Pro Management		✓
Audio Conferencing ¹	✓	✓
Whiteboard	✓	✓
Teams Phone Standard		✓
Microsoft Intune ²		✓
Microsoft Entra ID P1		✓
Microsoft Defender for Endpoint Plan 2		✓
Skype for Business Plan 2 ³		✓
Geographic availability	Worldwide	Worldwide
Segment availability	Commercial, Worldwide Public Sector, Education, Charity, GCC	Commercial, Worldwide Public Sector, Education, Charity, GCC, GCC-High
Channel availability	Web Direct, New commerce experience (NCE) - Customer led ⁴	EA, EAS, EES, CSP, Web Direct, NCE - Customer led, NCE - Partner led

Full list: <https://learn.microsoft.com/en-us/microsoftteams/rooms/rooms-licensing>

Meeting Join

	Microsoft Teams Rooms Basic	Microsoft Teams Rooms Pro
Join Teams meetings with 1-touch, proximity, and meeting ID	✓	✓
Start ad hoc meetings from the room	✓	✓
Direct Guest Join for Zoom and Webex meetings	✓	✓
Join meetings across Teams clouds		✓
Room check-in with Teams Panel		✓
Coordinated meeting		✓

Full list: <https://learn.microsoft.com/en-us/microsoftteams/rooms/rooms-licensing>

License support

- The following licensing options are available.
- Microsoft Teams Rooms – applicable to Cisco Desk Pro, Board Pro, Room Bar, Room Kit Pro and Room Kit EQ
 - Basic
 - Pro
- Microsoft Teams Display – Applicable to Cisco Desk Pro *
 - Microsoft Teams Shared Device – Applicable to Cisco Desk Pro if configured as Hot desk
 - Microsoft Office 365 E1/E3/E5 – Applicable to user that the Cisco Desk Pro is configured for.
- Microsoft Teams Panel – applicable to Cisco Room Navigator (stand alone) *
 - Microsoft Teams Shared Device

Control Hub Registration Concept...



Teams Admin Center

Control Hub

Management Capabilities

Microsoft Teams Admin Center and Webex Control Hub

	MTR on Android (no Control Hub registration)	MTR on Android (<u>with</u> Control Hub registration)
Device Inventory	Limited	✓
Device Configuration	Limited	✓
Software Upgrade	Limited	✓
Device Alerts	✗	✓
Meeting Metrics & Analytics	Teams Admin Center only	Teams Admin Center and Control Hub
Macros	✗	Partial
UI Extensions	✗	Beta October 2023
API Integrations	✗	✓
Device Metrics & Analytics	✗	✓
Room Metrics & Analytics	✗	✓
Native Webex Meetings	✗	✓
Environmental Metrics	✗	✓
Thousand Eyes	✗ X	

Managing Devices via Teams Admin Center

Contoso Electronics | Microsoft Teams admin center

Search

✓ Device diagnostics queued. This operation will be canceled if it can't start within 7 days of submission.

Pymble MTR Pro

cisco deskpro

PM

Download device logs

Update software

Restart

Refresh details

Health status: **Healthy**

Offline since: --

Device name: **cisco-deskpro foc2503nvu5**

Username: **pymblemtr@moderncomms.**

Peripherals | Health | Details | Activity | **History**

History

Action	Status	Scheduled at	Modified
DeviceRestart	Queued ⓘ	-	Nov 2
ConfigUpdate			Nov 2

This operation will be canceled if it can't start within 7 days of submission.

Ordering CH

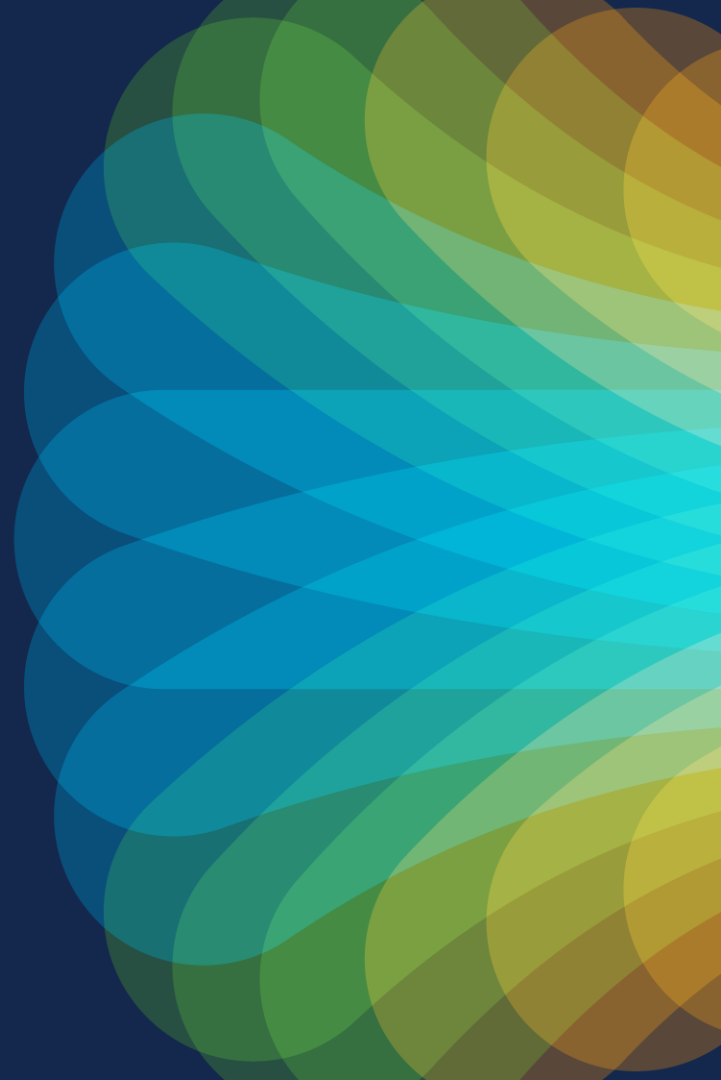
Need to have rough idea on cost of CH for MTR

*Is this best SKU?
What is discount*

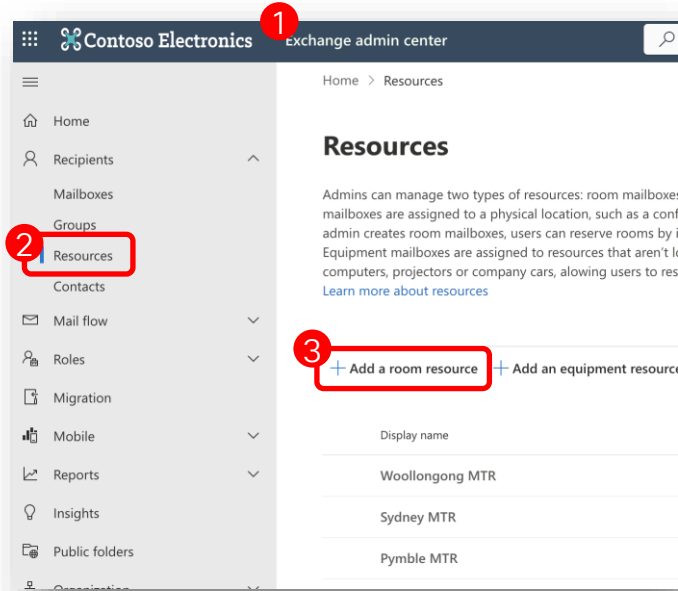
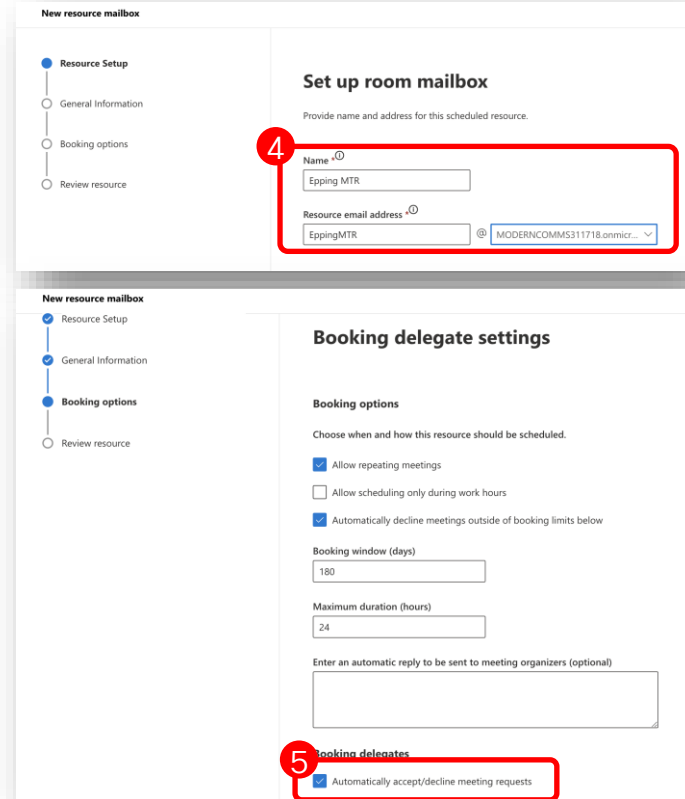
The product discounts are cascaded to subscription items, however subscription items may only be eligible for lower discounts. To apply the proper discount to subscription items, click on "MORE" and then, "Apply Discount".

	Lead Time	(AUD)		Filter By	All Items		Price (AUD)	(%)	Price (AUD)
☐ 1.0 CS-DESKPRO-K9 more	21 days	20,412.07	1				8,164.83	60.00	8,164.83
Cisco Desk Pro Success Track: COLLABORATION Valid as of 19-Nov-2023 02:37:49 PST Edit Options Select Service/Subscription Validate Recommended Content Add Note More Actions Add Subtotal									
☐ 2.0 A-DEVICE-PACKAGE more	Not Applicable	0.00	1				0.00	60	0.00
Device Package Support Subscription Valid as of 19-Nov-2023 02:41:41 PST Requested Start Date 22-Nov-2023 Requested For Initial Term 12 Months From 22-Nov-2023 To 21-Nov-2024 Automatically Renews For 12 Months From 22-Nov-2024 Billing Frequency Monthly Billing Linked Hardware Items View Details Edit Options Validate Recommended Content Add Note More Actions Add Subtotal									
2.1 A-CD-DESKPRO more	3 days	112.13 Per User /Month	1 User				112.13 Per User /Month	0.00	1,345.56
Control Hub, Adv Analytics & Cloud Updates with ESS 8x5xNBD									
2.2 SVS-DESKPRO-ECDN more	3 days	0.00 Per Each/ 12 Months	1 Each				0.00 Per Each/ 12 Months	0.00	0.00
Cisco Desk Pro Support ESS WITH 8X5XNBD									
Estimate Total All Prices Shown in AUD									
Average Product Discount	60.00 %	Product Total	8,164.83						
Average Service Discount	0.00 %	Service Total	0.00						
Average Subscription Discount	0.00 %	Subscription Total	1,345.56						
		Total Price	9,510.39						

Setup



Create Room Resource



Hide Room (optional)

The screenshot shows the Exchange Admin Center interface for Contoso Electronics. The left sidebar contains navigation links: Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, Settings, and Other features. The main content area is titled 'Resources' and includes a description of resource types and a table of resources. The 'Epping MTR' resource is selected. A right-hand pane shows details for 'Epping MTR', including its name, email address, department, company, and capacity. A red box with the number '4' highlights the 'Hide from global address list (GAL)' option under the 'Resource contact information' section.

Exchange admin center

Home > Resources

Resources

Admins can manage two types of resources: room mailboxes and equipment mailboxes. Room mailboxes are assigned to a physical location, such as a conference room or auditorium. After an admin creates room mailboxes, users can reserve rooms by including them in meeting requests. Equipment mailboxes are assigned to resources that aren't location specific, such as a portable computers, projectors or company cars, allowing users to reserve them in meeting requests. [Learn more about resources](#)

Delete Refresh Export resources

Display name ↑	Email address
Dundee MTR	dundeemtr@MODERNCOMMS311718.onmicrosoft.com
Edinburgh MTR	edinburghmtr@MODERNCOMMS311718.onmicrosoft.com
☒ Epping MTR	EppingMTR@MODERNCOMMS311718.onmicrosoft.com
Glasgow MTR	glasgowmtr@MODERNCOMMS311718.onmicrosoft.com
Newcastle MTR	newcastletr@MODERNCOMMS311718.onmicrosoft.com
Parramatta MTR	parramattamtr@MODERNCOMMS311718.onmicrosoft.com

Epping MTR

Room Mailbox

Delete Resource

General Booking Delegation Others

Room Name
Epping MTR

Email address
EppingMTR@MODERNCOMMS311718.onmicrosoft.com

Department

Capacity

Company

Address book policy
[No Policy]

[Manage resource details](#)

[Additional information](#)

Resource contact information

[Manage resource contact information](#)

Hide from global address list (GAL)
No
[Manage hide from GAL](#)

Configure Account

The screenshot displays the Microsoft 365 admin center interface for Contoso Electronics. The left navigation pane shows the 'Active users' link highlighted with a red box and a red circle labeled '2'. The main content area shows the 'Active users' list with the 'Epping MTR' user selected, also highlighted with a red box and a red circle labeled '4'. A red circle labeled '3' points to the edit icon (pencil) next to the 'Epping MTR' user. The right-hand pane shows the user's profile for 'Epping MTR', with the 'Licenses and apps' tab selected, highlighted with a red box and a red circle labeled '5'. In the 'Licenses' section, the 'Microsoft Teams Rooms Pro' license is selected with a checkmark, highlighted with a red box and a red circle labeled '6'. Other visible licenses include 'Advanced Communications', 'Microsoft Teams Shared Devices', and 'Office 365 E3'. The top navigation bar shows the 'Home' link highlighted with a red circle labeled '1'.

Contoso Electronics Microsoft 365 admin center

Home > Active users

Active users

Add a user Multi-factor authentication Refresh Delete user

☐	Display name ↑	Username
☐	Dundee MTR	dundeemtr@MODERNCOM
☐	Edinburgh MTR	edinburghmtr@MODERNCOM
☒	Epping MTR	EppingMTR@MODERNCOM
☐	Glasgow MTR	GlasgowMTR@MODERNCOM
☐	Microsoft Service Account	ms-serviceaccount@MODE
☐	MOD Administrator	admin@MODERNCOMMS
☐	Newcastle MTR	newcastletr@MODERNCOM
☐	Parramatta MTR	parramattamtr@MODERNCOM
☐	Pymble MTR	pymbletr@moderncomm

Epping MTR

Reset password Block sign-in Delete user

Account Devices **Licenses and apps** Mail OneDrive

Select location *

United States

Licenses (1)

- ☐ **Advanced Communications**
13 of 15 licenses available
- ☒ **Microsoft Teams Rooms Pro**
0 of 10 licenses available
- ☐ **Microsoft Teams Shared Devices**
9 of 10 licenses available
- ☐ **Office 365 E3**
9 of 10 licenses available

Multi-Factor Authentication (disable)

1

2

multi-factor authentication users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Sign-in allowed users Multi-Factor Auth status: Any

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
Dundee MTR	dundeembr@MODERNCOMMS311718.onmicrosoft.com	Disabled
Epping MTR	EppingMTR@MODERNCOMMS311718.onmicrosoft.com	Disabled
Glasgow MTR	glasgowmtr@MODERNCOMMS311718.onmicrosoft.com	Disabled
Microsoft Service Account	ms-serviceaccount@MODERNCOMMS311718.OnMicrosoft.com	Disabled

Epping MTR

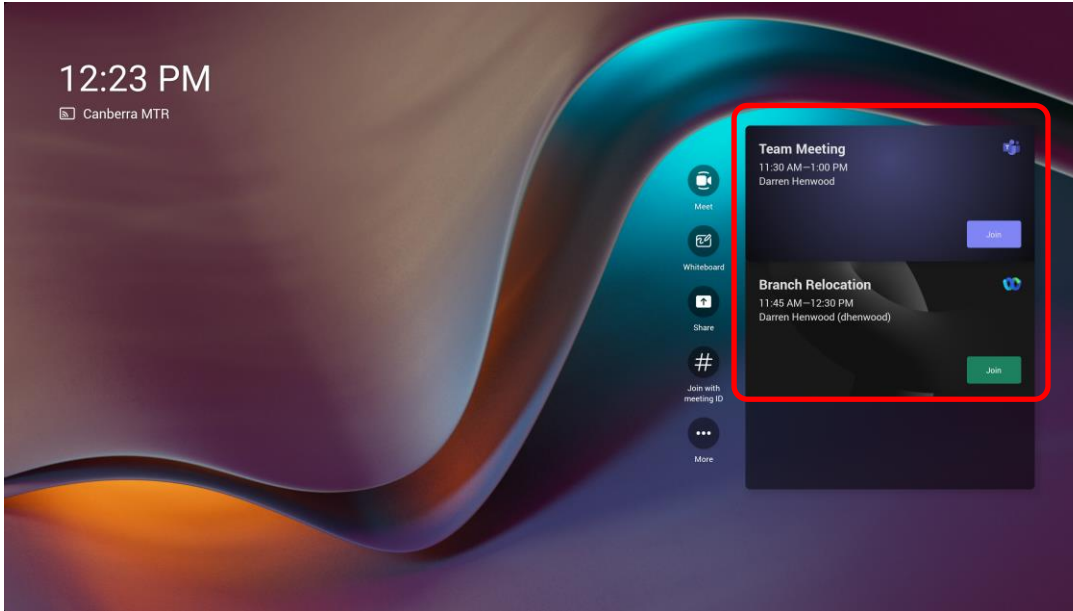
quick steps

Enable

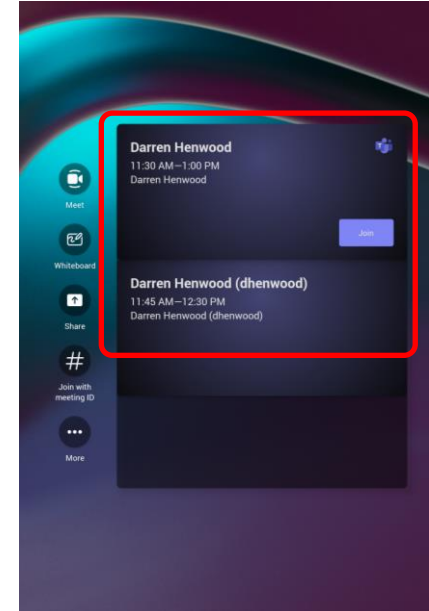
Manage user settings

"It's important to note that Microsoft Teams Rooms resource accounts shouldn't be configured to use multifactor authentication (MFA), smart card authentication, or client certificate-based authentication (which are all available for end users)". [Details](#)

Optimizing User Experience



Desired Appearance 😊



Default Appearance 😞

Exchange PowerShell

Install-module ExchangeOnlineManagement

\$Credentials = Get-Credential

Connect-ExchangeOnline -Credential \$Credentials

Set the UPN for the account (ensure email domain matches O365 domain)

\$DisplayName = "Epping MTR"

Set room resource password to not expire

Set-MsolUser -UserPrincipalName \$TeamsVariable -PasswordNeverExpires \$true

Set processing to be correctly processed

Set-CalendarProcessing -Identity \$DisplayName -DeleteSubject \$false -AddOrganizerToSubject \$false -DeleteComments \$false -AutomateProcessing AutoAccept

- Consideration needs to be given to the resource mailbox properties that will be assigned to the Microsoft Teams Room.
- AutomateProcessing
 - Mailbox should be set to AutoAccept to ensure that the meeting organizer receives the room reservation Accept/Decline.
- AddOrganizerToSubject
 - This can be set to \$false so that the meeting organizer is not added to the subject of the meeting request.
- DeleteComments
 - This should be set to \$false to ensure that text in the message body of the incoming meeting request is not deleted. This is a requirement to process external Teams and third-party meetings to provide the One Touch Join experience.
- DeleteSubject
 - This should be set to \$false to keep the subject of the meeting request
- ProcessExternalMeetingMessages
 - This must be set to \$true to process meeting requests that originate outside of the Exchange organization. This is a requirement to process external Teams meetings and third-party meetings.

-ProcessExternalMeetingMessages \$true -AllowConflicts \$true

PowerShell Commands

```
# Set processing to be correctly processed
PS C:\> Set-CalendarProcessing -Identity $DisplayName -AutomateProcessing AutoAccept
-AddOrganizerToSubject $false -DeleteComments $false -DeleteSubject $false
-ProcessExternalMeetingMessages $true -RemovePrivateProperty $false
```

Consideration needs to be given to the resource mailbox properties that will be assigned to the Microsoft Teams Room.

- *AutomateProcessing - Mailbox should be set to AutoAccept to ensure that the meeting organizer receives the room reservation Accept/Decline.*
- *AddOrganizerToSubject - This can be set to \$false so that the meeting organizer is not added to the subject of the meeting request.*
- *DeleteComments - This should be set to \$false to ensure that text in the message body of the incoming meeting request is not deleted. This is a requirement to process external Teams and third-party meetings to provide the One Touch Join experience.*
- *DeleteSubject - This should be set to \$false to keep the subject of the meeting request*
- *ProcessExternalMeetingMessages - This must be set to \$true to process meeting requests that originate outside of the Exchange organization. This is a requirement to process external Teams meetings and third-party meetings.*

Create Device in Control Hub

webex Control Hub

Search

1

2

3

Devices

Find devices by status, type, and more

156 devices

Filter by: Online (57) Expired (2) Offline (67) Issues (27) Activating (2) Status unavailable (1)

Select one or more devices for bulk actions

Type	Product	Status	Platform	Belongs to
Rooms & Desks	Cisco Room Bar	Offline		Crescendo Room Bar
Rooms & Desks	Cisco Room Kit Pro	Issues		Crescendo Roomkit Pro
Rooms & Desks	Cisco Desk Pro	Online		Darren Henwood

Add device

What are you setting up for?

4

Personal usage

Assign a single personal device to a user

Shared usage

Add shared device and services to a workspace

Multiple Cisco IP phones

Bulk activate devices using a CSV file

Add device

Workspaces represent a physical space in your organization. It may contain one device. Workspace details show usage, settings, and environmental status for that physical space and cost of your space.

Name *

5

Epping MTR

Type ⓘ

What type best describes the Workspace?

Huddle

Add device

Activation Code

password. Share this code with the person setting up the device belonging to the device. Once the device has been successfully activated, you will be able to use the device.

6

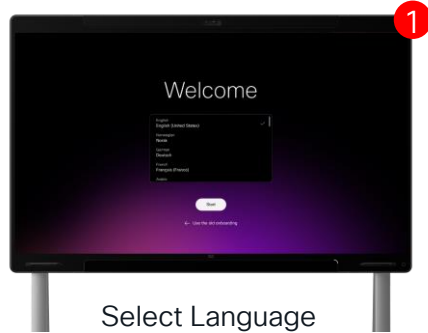
7996-9490

Expires November 28, 2023 10:53 AM (AEST)

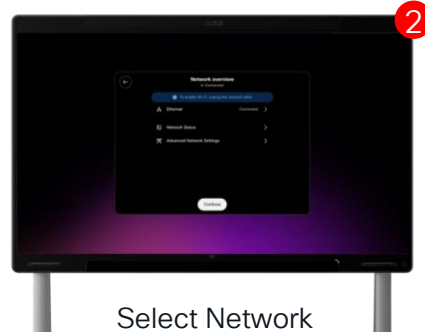
This code cannot be used to activate Cisco IP Phones

Copy Email Print

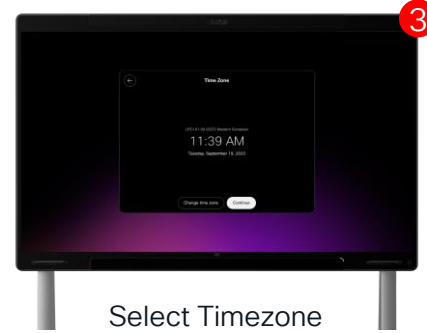
Device Registration Process



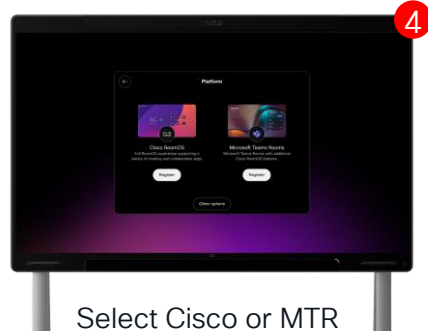
Select Language



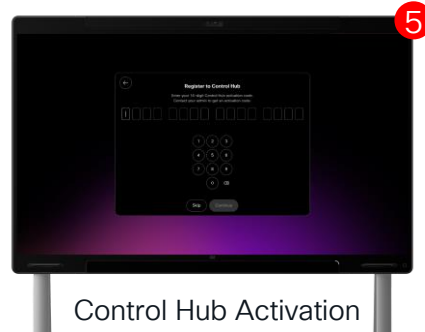
Select Network



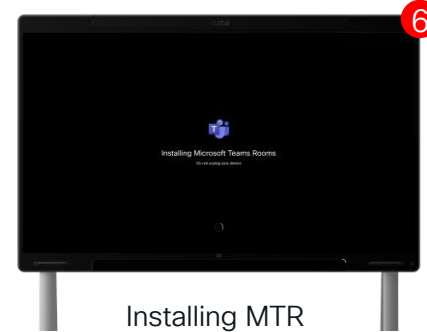
Select Timezone



Select Cisco or MTR

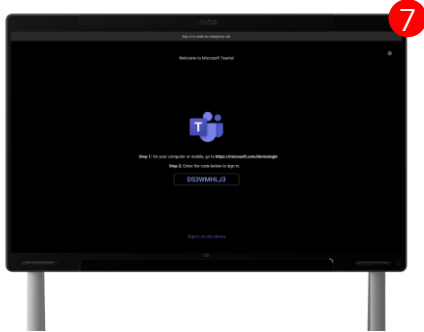
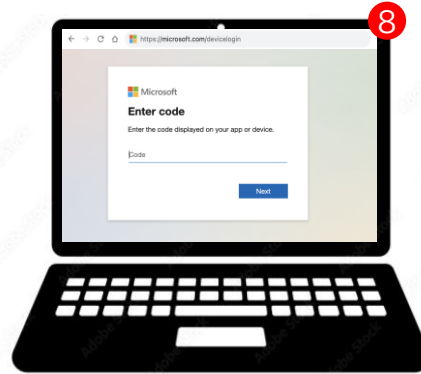


Control Hub Activation
Code



Installing MTR

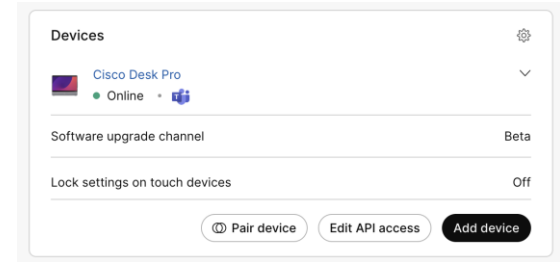
Device Registration Process



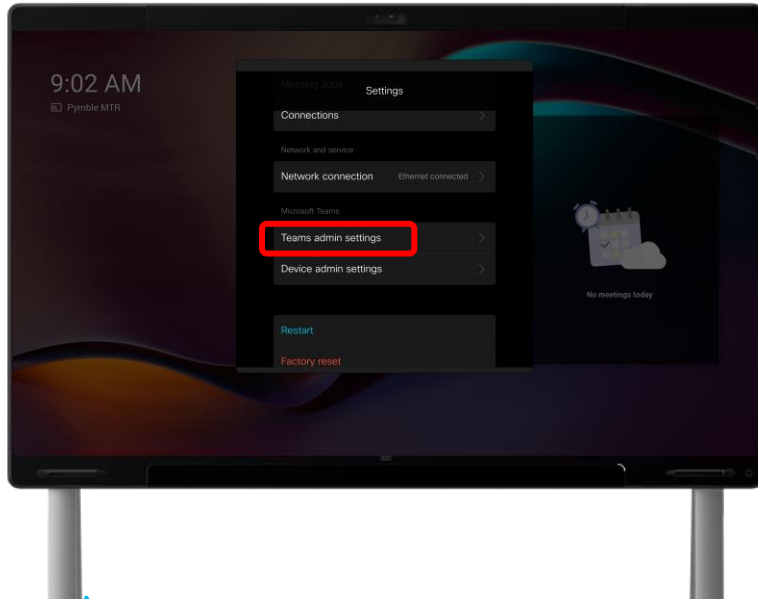
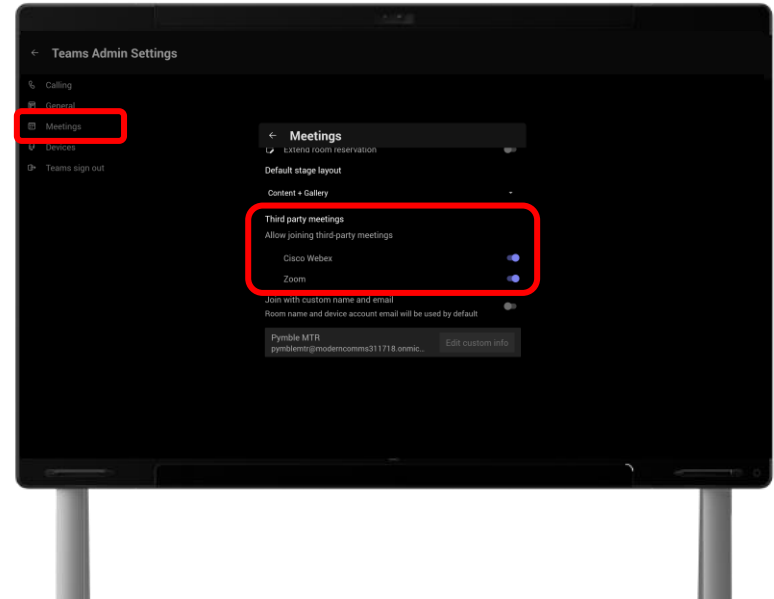
Enable Webex Join

xconfiguration UserInterface SettingsMenu Mode: Unlocked

OR



THEN



PowerShell Commands

Install required modules

PS C:\> Install-Module AzureAD

PS C:\> Install-Module MSOnline

PS C:\> Install-Module ExchangeOnlineManagement

PS C:\> Install-Module Microsoft.Graph -Scope AllUsers

Login using a Microsoft 365 Admin account

PS C:\> \$Credentials = Get-Credential

PS C:\> Connect-MsolService -Credential \$Credentials

PS C:\> Connect-ExchangeOnline -Credential \$Credentials -ShowProgress \$true

PS C:\> Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All

Set the UPN for the account (ensure email domain matches O365 domain)

PS C:\> \$UpnVariable = "eppingmtr@moderncomms311718.onmicrosoft.com"

PS C:\> \$DisplayName = "Epping MTR"

Next Page...

PowerShell Commands

Create Room Resource

```
PS C:\> New-Mailbox -Name $DisplayName -Room
```

Set processing to be correctly processed

```
PS C:\> Set-CalendarProcessing -Identity $DisplayName -AutomateProcessing AutoAccept  
-AddOrganizerToSubject $false -DeleteComments $false -DeleteSubject $false  
-ProcessExternalMeetingMessages $true -RemovePrivateProperty $false
```

Next Page...

PowerShell Commands

Set room resource password to not expire

```
PS C:\> Set-MsolUser -UserPrincipalName $UpnVariable -PasswordNeverExpires $true
```

Set the usage location of the O365 tenancy

```
PS C:\> Set-MsolUser -UserPrincipalName $UpnVariable -UsageLocation (Get-MsolCompanyInformation).CountryLetterCode
```

Obtain the Microsoft Teams Pro license

```
PS C:\> $TeamsProLicense = Get-MgSubscribedSku | where {$_.SkuPartNumber -like $("*Pro")}
```

Apply the Pro license to the account

```
PS C:\> Set-MgUserLicense -UserId $UpnVariable -AddLicenses @{Skuld = $TeamsProLicense.Skuld} -RemoveLicenses @()
```

Create Control Hub Activation Code

REST API Call

POST

<https://webexapis.com/v1/devices/activationCode?orgId=Y2lzY29zcGFyYXZvLjY2MjhlODQ>

HEADER

Authorization: Bearer <Token>
Content-Type: application/json

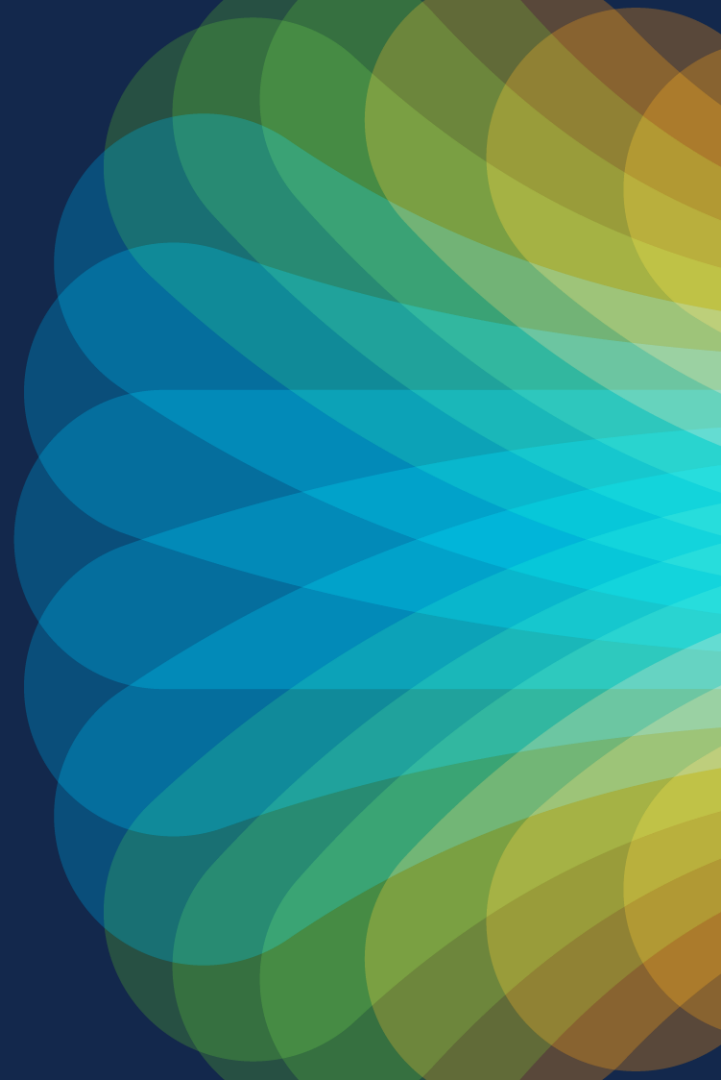
BODY

```
{  
  "workspaceId": "Y2lzY29zcGFyYXZvLjY2MjhlODQ",  
  "model": "Cisco Room Bar"  
}
```

RESPONSE

```
{  
  "code": "5414011256173816",  
  "expiryTime": "2023-11-21T23:38:03.215Z"  
}
```

Network Requirements



Network Requirements

Domains, IP, ports: <https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

Note that open connectivity to TCP ports 80 and 443, and to UDP ports 3478 (STUN), 3479 (Audio), 3480 (Video), and 3481 (sharing/VBSS) are required.

Microsoft Teams Rooms does not support proxy authentication as it may interfere with regular operations of the room. Ensure that Microsoft Teams Rooms have been exempted from proxy authentication before going into production. [Reference](#)

Be sure to use a network connection with enough bandwidth (we recommend 10 mbps up/down per Teams Room) to ensure your meetings perform well. [Reference](#)

Microsoft – Network Requirements

- Microsoft Office 365 and Microsoft Teams has several network requirements. The links below detail these requirements further. Please note that if the Cisco collaboration device is also registered to Control Hub, there are additional network considerations that are detailed on the following slides.

Teams Rooms on Android	
Microsoft Teams	<u>Required</u>
Microsoft Office 365	<u>Required</u>
Microsoft Intune	<u>Optional</u>
Pro Management Portal	<u>Optional</u>
Unauthenticated Proxy	<u>Optional</u> *
QoS	<u>Optional</u>
802.1x	<u>Optional</u> *
Bandwidth Policy	<u>10 Mbps</u>

Cisco Network Requirements

- The following requirements need to be taken into consideration when the Cisco collaboration device is registered to Control Hub. These requirements are in addition to the Microsoft network requirements as detailed in the previous slide.

Destination port	Protocol	Description
443	TLS	Webex HTTPS signaling – session establishment to Webex services are based on URLs rather than IP addresses
5004 and 9000	SRTP over UDP	Encrypted audio, video and content sharing for when Cisco collaboration device is joining a Native Webex meeting experience
5004	SRTP over TCP	TCP also serves as fallback for encrypted audio, video and content if UDP cannot be used.
443	SRTP over TLS	Fallback transport protocol for encrypted audio, video and content sharing if UDP and TCP cannot be used. Media over TLS is not recommended in production environments

⁽¹⁾ If you are using DNS services within your enterprise network, then ports 53 and 123 do not need to be opened through your firewall

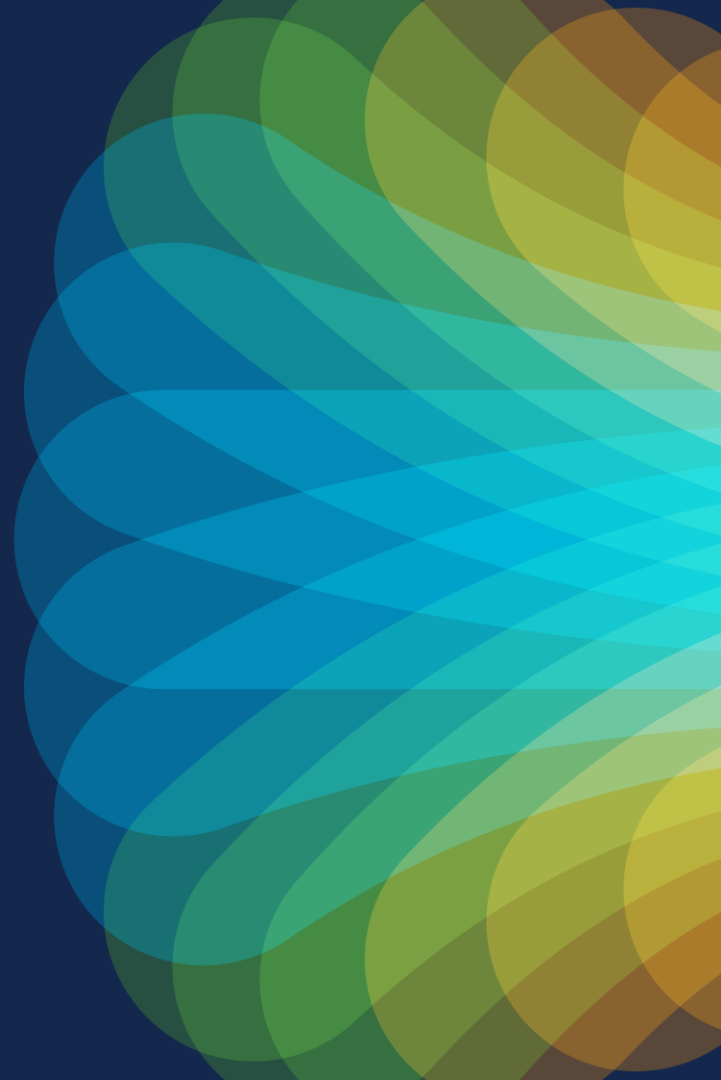
Cisco Network Requirements

- The following requirements need to be taken into consideration when the Cisco collaboration device is registered to Control Hub. These requirements are in addition to the Microsoft network requirements as detailed in the previous slides.
- Configure your firewall to allow access to these destinations Webex IP subnets and transport protocol ports for media streams from Webex apps and devices. UDP is Cisco's preferred transport protocol for media and we strongly recommend using only UDP to transport media. Webex apps and devices also support TCP and TLS as transport protocols for media, but these are not recommended in production environments as the connection-orientated nature of these protocols can seriously affect media quality over lossy networks.

Note: The IP subnets listed below are for Webex media services. Filtering Webex signaling traffic by IP address is not supported as the IP addresses used by Webex are dynamic and may change at any time. HTTP signaling traffic to Webex services can be filtered by URL/domain in your Enterprise Proxy server, before being forwarded to your firewall.

- For a full and current list of IP subnets for media services, please see
- https://help.webex.com/en-us/article/WBX000028782/Network-Requirements-for-Webex-Services#id_135011

Teams Admin Center & Control Hub



Navigating Teams Admin Center (TAC)

The screenshot displays the Microsoft Teams Admin Center (TAC) interface for Contoso Electronics. The left sidebar shows the navigation menu with 'Teams Rooms on Android' selected. The main content area is titled 'Teams Rooms on Android' and includes a description: 'Control and manage your Teams certified Teams Rooms on Android devices across your organization, create and upload configuration profiles to make changes, [set up alert rules](#), and apply updates for each device. [Learn more](#)'. Below this, there are three summary cards: 'Devices summary' (8 Total, 2 Online, 6 Offline), 'Health summary' (2 Healthy, 0 Non-urgent, 0 Critical), and 'License summary' (a bar chart showing 8 Pro licenses). There are also sections for 'Browse Teams certified devices' with a 'Shop devices' button and 'Software auto-updates' showing 0 updates. At the bottom, there are tabs for 'Teams Rooms on Android', 'Touch consoles', and 'Configuration profiles'. The 'Teams Rooms on Android' tab is active, showing a table of devices with columns: Display name, Username, Device name, License, Health status, Automatic updates, and Manufacturer. The table contains one item: 'Pymble MTR' with username 'pymblemtr@modernco...', device name 'cisco-deskpro foc2503n...', license 'Pro', health status 'Healthy', automatic updates 'General', and manufacturer 'cisco'.

Teams Rooms on Android

Control and manage your Teams certified Teams Rooms on Android devices across your organization, create and upload configuration profiles to make changes, [set up alert rules](#), and apply updates for each device. [Learn more](#)

Devices summary

8 Total, 2 Online, 6 Offline

Health summary

2 Healthy, 0 Non-urgent, 0 Critical

License summary

8 Pro

Browse Teams certified devices

[Shop devices](#)

Software auto-updates

0 Automatic updates are underway.

Teams Rooms on Android | Touch consoles | Configuration profiles

Edit | Assign configuration | Manage tags | Update | Restart | Remove | 8 items

✓	Display name	Username	Device name ⓘ	License ⓘ	Health status ⓘ	Automatic updates	Manufacturer
	Pymble MTR	pymblemtr@modernco...	cisco-deskpro foc2503n...	Pro	Healthy	General	cisco

Configuration Templates

The screenshot displays the Microsoft Teams admin center interface. The top navigation bar includes the 'Microsoft Teams admin center' title, a search bar, and several utility icons. The left-hand navigation pane lists various administrative sections, with 'Teams Rooms on Android' currently selected. The main content area is titled 'Melbourne Devices' and shows the 'Default Template for Melbourne'. Under the 'General' tab, several configuration settings are visible: 'Device lock' is turned 'On', 'Timeout' is set to '30 seconds', 'Device lock PIN' is '123456', 'Language' is 'English (United States)', 'Timezone' is '(UTC-12:00) International Date Line West', 'Date format' is 'DD/MM/YYYY', and 'Time format' is '12 Hours (AM/PM)'.

Microsoft Teams admin center

Search

Teams Rooms on Android \ Configuration profiles \ Melbourne Devices

Melbourne Devices

Default Template for Melbourne

General

Device lock	☒ On
Timeout	30 seconds
Device lock PIN	123456
Language	English (United States)
Timezone	(UTC-12:00) International Date Line West
Date format	DD/MM/YYYY
Time format	12 Hours (AM/PM)

Introduction to Microsoft Pro Management Platform

- The Microsoft Teams Rooms Pro Management service (aka Pro Portal), is similar to Webex Control Hub in terms of it being a cloud-based management solution.
- Pro Portal allows for proactive monitoring and updating of Microsoft Teams Rooms devices and their peripherals.
- The solution is aimed at organizations looking to optimize the meeting room experience for end users and rapidly scale footprint by real-time monitoring and management for Microsoft Teams Rooms devices.
- There are three key aspects to the service:
 - Intelligent operations
 - Update management
 - Enhanced insights

What exactly can Pro Portal do?

- Management Capabilities
- Room planning and rollout
- Monitoring
- Troubleshooting and remediation
- Update management
- Insights and recommendations
- Compliance and certifications
- Supported devices
- Supported clouds
- Supported regions
- Integrations

Accessing the Pro Management Portal

- Access to the portal is governed through the use of a Roles Based Access Control (RBAC).
- For someone who needs to be able to access the portal, they will need to be assigned the correct role.
- This will need to be assigned by an administrator in the Microsoft 365 Admin Center.
- The type of role that is assigned is called a Managed Service Administrator.
- This can be found under:
- portal.rooms.microsoft.com>Settings>Roles>Managed Service Administrator and select Assignments and then Add.
- Users who are assigned this role are responsible for the day-to-day management and monitoring of Teams Rooms

Welcome to the Pro Management Portal

Navigation

Microsoft Teams Rooms Pro Management

Home

Incidents

Rooms

Reports

Updates

Planning

Settings

General

Roles

Groups

Partners

ServiceNow

Hi, Charlie!

Portal information

Check out [our docs](#) to learn more about how to use this portal.

Open Office Hours

Every Wednesday from 9:00 to 10:00 Pacific Time

An open forum to learn more about the Teams Rooms Pro Management program with the experts.

Topics Include:

- Room health and how to escalate
- What's coming next
- Microsoft's role in managing your rooms
- How to get help through the Microsoft Service Operation Center
- Live questions

Find the meeting join information in the help panel.

Known Issues

This link lists the known issues for the Microsoft Teams Rooms app when it's used on Windows and Android devices: [Known Issues in Teams Rooms and devices](#)

What's new?

Date

Wednesday, October 25th 2023

Additional signals for Teams Rooms on Windows

We are excited to announce new signals that enhance monitoring of your MTRoWs:

Wi-Fi signal strength - Teams Rooms device is connected to Wi-Fi with a signal strength of less than or equal to 70%. Call quality and user experience could be impacted.

CPU performance limited - The maximum processor state is configured below 100% and may impact performance. This may be defined by the active Power Plan on the Teams Room. For additional information please refer to: <https://aka.ms/mitro/CPUlimitation>

Auto-remediation available. Will adjust configuration to optimal value.

Sleep Timer - A 'Sleep after' timer is set under Windows power plan configuration on this device. This can impact the monitoring, maintenance and the wake response of the Teams Room. For more information about sleep timer settings for MTR devices, refer to: <https://aka.ms/mitro/sleeptimer>

Auto-remediation available. Will adjust configuration to optimal value.

Windows Update Components Need Reset - The device has not received Windows updates in the last 35 days and one of the following is true: The device has rolled back to a previous version, Windows update services are failing or There is a significant amount of errors in the Windows Update logs.

Workspace Insights Survey

Date

Tuesday, October 3rd 2023

We are evaluating a product concept to bring in more Workspace Insights for our IT Admin customers and want to better understand which types of insights are the most valuable to you and your organization. Please complete the survey at this [link](#).

Thank you for taking time to complete this survey to help shape our product offerings.

Nightly Reboot alerts

Date

Friday, September 29th 2023

Some MTRW systems got affected by an issue that triggered Nightly Reboot alerts. PMP team is currently mitigating the issue for all systems above OS build 19045, but still have some systems on older versions still affected by this symptom.

Beginning of next week we will extend the fix to MTRW devices on OS build above 10.0.19044.

There are no actions that needs to be executed by customers at this time and problem should be resolved for majority of rooms as soon as the fix is rolled out.

MTR App 4.18.44 unpaused on some tenants

Portal Overview

Incidents

Microsoft Teams Rooms Pro Management

Home

Incidents

Rooms

Reports

Updates

Planning

Settings

General

Roles

Groups

Partners

ServiceNow

Incidents

Review incidents affecting your rooms

8 ACTIVE

8 NEED ACTION

0 SYSTEM INVESTIGATING

Record an issue

Active Resolved

>	Problem	Ticket	Room	Type	Status	Severity	Impact	Unread	Last message
▼	Connectivity	8 active	8 affected rooms		8 need action			6 unread	
	Offline	MSEWN2-SAPIUW	MTR-Meeting Room	MTR Android	Needs action	Critical			5 months ago
	Offline	MSEWN2-8PATPW	MTR-Meeting Room	Touch Console	Needs action	Critical			4 months ago
	Offline	MSEWN2-F0YKIH	cisco-roomnavigatc	Touch Console	Needs action	Critical			2 months ago
	Offline	MSEWN2-3FEYOU	cisco-roomnavigatc	Touch Console	Needs action	Critical			2 months ago
	Offline	MSEWN2-BEH42P	MTR Board Room ('	Touch Console	Needs action	Critical			1 month ago
	Offline	MSEWN2-DREHNY	WX1 AR/PR MTR Bc	MTR Android	Needs action	Critical			9 days ago
	Offline	MSEWN2-H9JRAD	WX1-BarPro	MTR Android	Needs action	Critical			8 days ago
	Offline	MSEWN2-WC4SS4	WX1-BarPro	Touch Console	Needs action	Critical			8 days ago

Rooms

- Overview of the health of the room(s) being monitored by the Pro Management platform.
- MTR Pro License is needed to provide coverage for monitoring.
- MTR Basic whilst showing, also show error as not supported

The screenshot displays the 'Microsoft Teams Rooms Pro Management' dashboard. At the top, a summary bar shows 13 MANAGED rooms, with 3 HEALTHY, 0 UNHEALTHY, 8 UNMONITORED, 2 SUPPRESSED, 0 ONBOARDING, 0 SLEEPING, and 6 UNLICENSED. Below this is a table listing 13 items, each with columns for Name, Hostname, State, Type, Suppressed, Onboarding, Needs action, Tags, Groups, and License type. Two callout boxes are present:

- Callout 1:** Points to a row with 'License type' 'Unlicensed'. The text states: 'This meeting room device does not have a valid Microsoft Teams Rooms Pro or Premium license. The license is currently expired, and you have 14 days remaining to continue benefiting from the Teams Rooms Pro device management capabilities. Please ensure the appropriate license is assigned within this timeframe. Learn more about licensing [here](#), find devices with unsupported licenses [here](#), and manage your Teams licenses at [M365 Admin Center](#).'
- Callout 2:** Points to a row with 'License type' 'Basic'. The text states: 'This meeting room device does not have a valid Microsoft Teams Rooms Pro or Premium license. The license is currently expired, and you have 3 days remaining to continue benefiting from the Teams Rooms Pro device management capabilities. Please ensure the appropriate license is assigned within this timeframe. Learn more about licensing [here](#), find devices with unsupported licenses [here](#), and manage your Teams licenses at [M365 Admin Center](#).'

Rooms – healthy device

- Ticket status (and resolved tickets)
- Settings tab allows view of Teams apps and device detail
 - Allows for a configuration profile to be applied
 - This needs to have been created in Teams Admin Center first
 - Profile has limited impact upon RoomOS config on Cisco device – aimed at MTR components

 **MTR Board Room (10)**

cisco-roomkiteq foc2726h8t1 | mtrboardroom@tmedemo.com

Status

SettingsActivityActionsGroupsCall History

This room is online with all signals enabled and active.

Active tickets

Show all signals

🗑️ Suppress

▼	Problem	Ticket	Status	Action	Severity
	Recorded		✓ Healthy		
▼	Connectivity	1 recently resolved	✓ Healthy		
	Offline	MSEWN2-Y7TVI3	✓ Healthy	Resolved	Critical
	Hardware and peripherals		✓ Healthy		
	Other		✓ Healthy		

Record an issue

Suppress room

Unenroll

📄 Collect logs

Rooms – unhealthy device

- Automatic ticket generation including category and severity
 - Audio
 - Display
 - Peripherals
 - Connectivity
 - Versioning

 **MTR Board Room (10)**
cisco-roomnavigator foc2718h6xv | mtrboardroom@tmedemo.com

[Status](#) [Settings](#) [Activity](#) [Actions](#) [Groups](#)

The monitoring agent in this room appears to be disconnected.

Active tickets

Show all signals

Suppression

>	Problem	Ticket	Status	Action	Severity
	Recorded		Unmonitored		
▼	Connectivity	1 active	Unhealthy	1 needs action	
	Offline	MSEWN2-MCWYOM	Unhealthy	Needs action	Critical
	Other		Unmonitored		

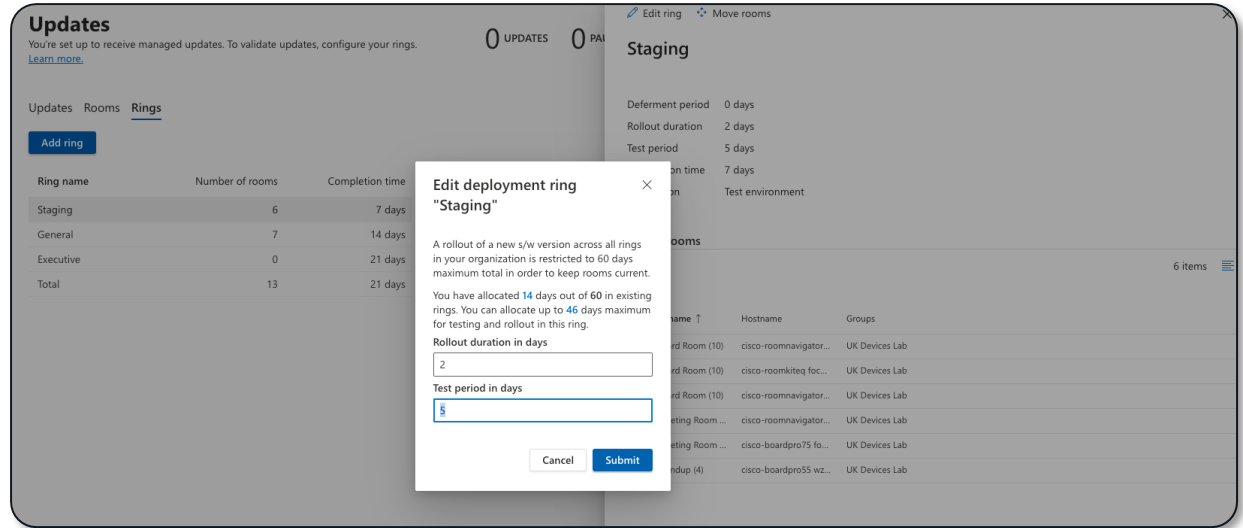
Record an issue

Suppress room

Collect logs

Updates

- Managed Updates:
- Automatically managed
 - No action needed from IT team
 - Only Microsoft validated software can be automatically managed
- Ring validated
 - Staging/Validation
 - General
 - Executive/Final



Simple answer

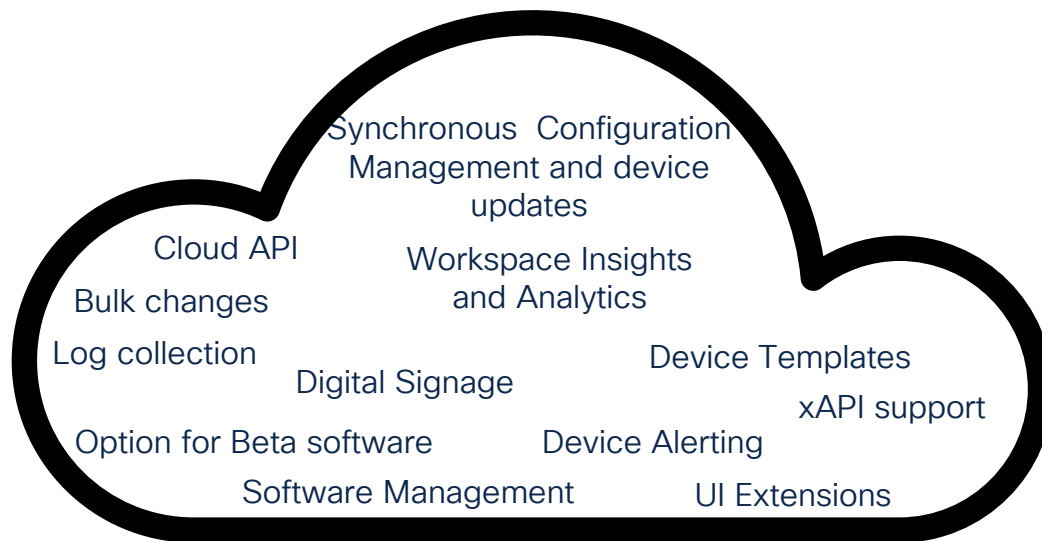
- Currently....not a lot!
- Today, many of the capabilities seen in Pro Portal seem to offer limited coverage for Microsoft Teams Rooms on Android with much more of the focus based on Microsoft Teams Rooms on Windows.
- Actions in Pro Portal are queued. For example, requesting a restart of a device will queue and will action at some point.
- Pro Portal also links out to a number of the other Microsoft admin centers. For example, if assigning a template to a device, it has to be created in Teams Admin Center first.
- Health reporting also limited.

So, do we still need Control Hub?



Control Hub compliments Microsoft Admin centers

- Control Hub offers many advantages over and above the capabilities available from the various Microsoft Admin centers.



Control Hub registration



Device inventory,
management,
and monitoring in
Control Hub



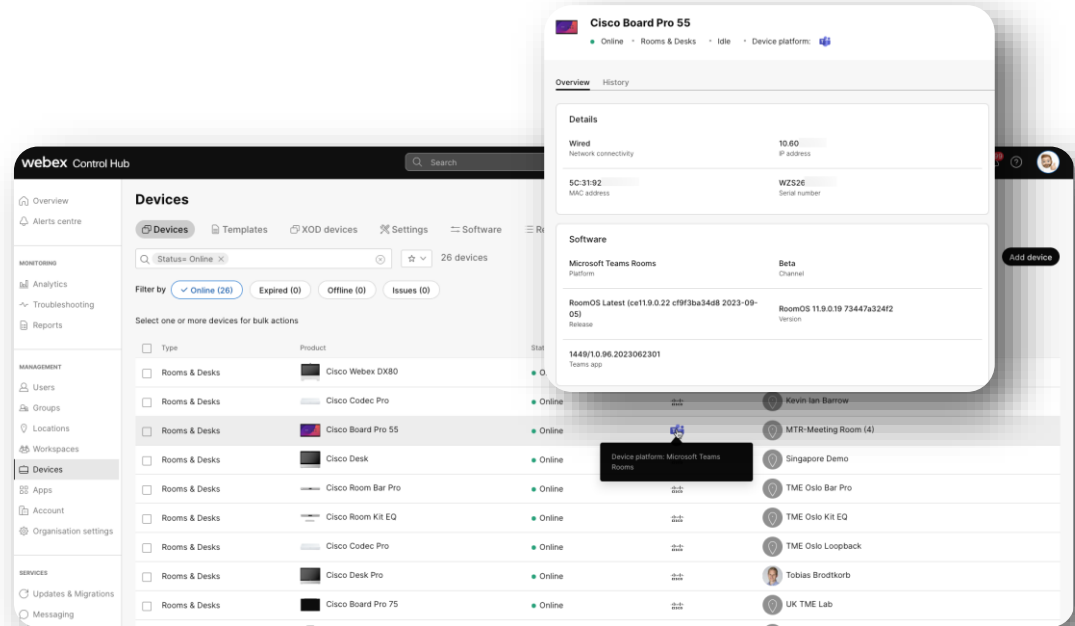
Access to the full
value of Control Hub
alongside Microsoft
Teams Admin Center



Workspace
environmental and
occupancy metrics

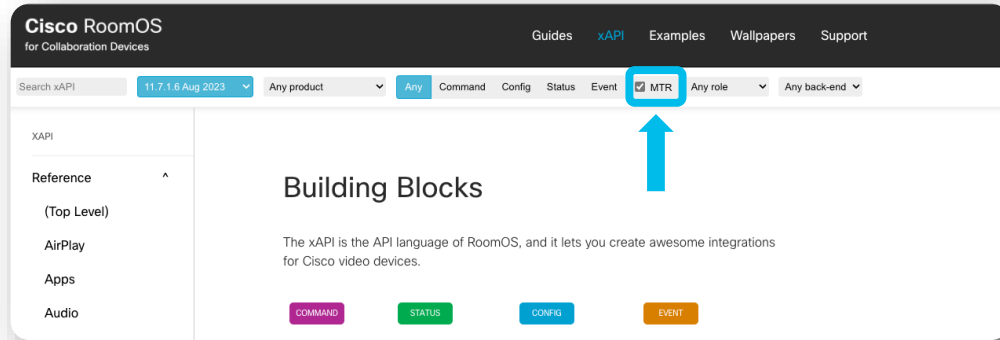


Macros, UI
extensions and
Cloud API access



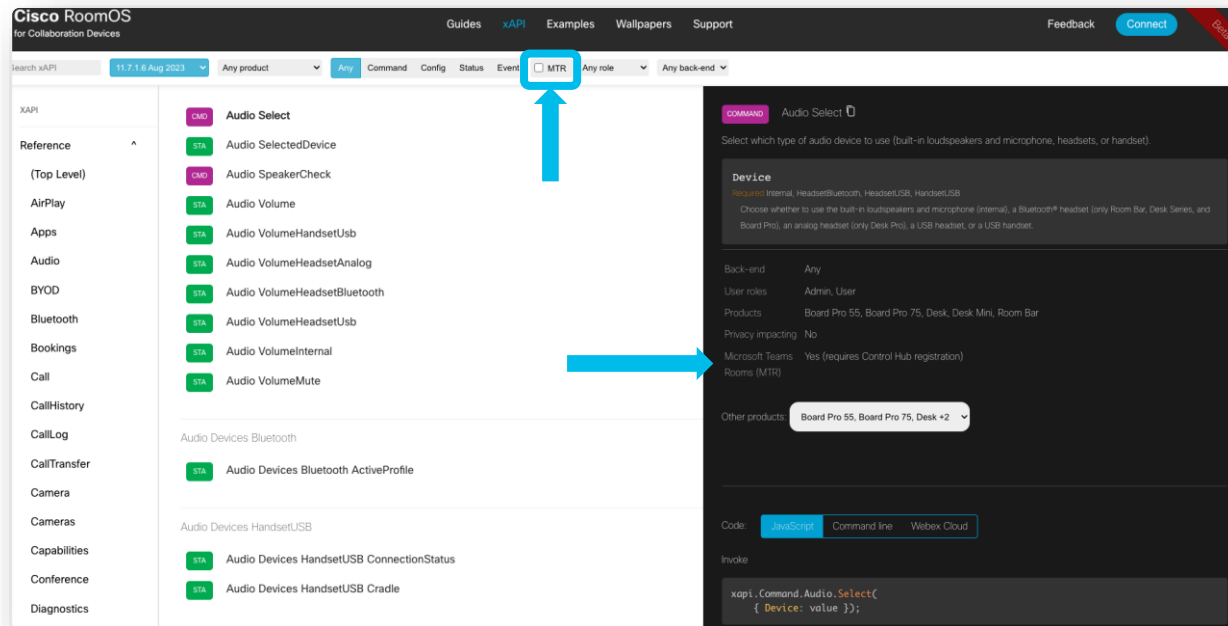
Macros

- Support is there in RoomOS today
 - Not every xAPI is supported when running Microsoft Teams Rooms
 - Event based macros supported
 - Requires Control Hub registration
- <https://roomos.cisco.com>
 - MTR filter available to show xAPI's that are applicable when supporting Microsoft Teams Rooms



RoomOS xAPI Availability

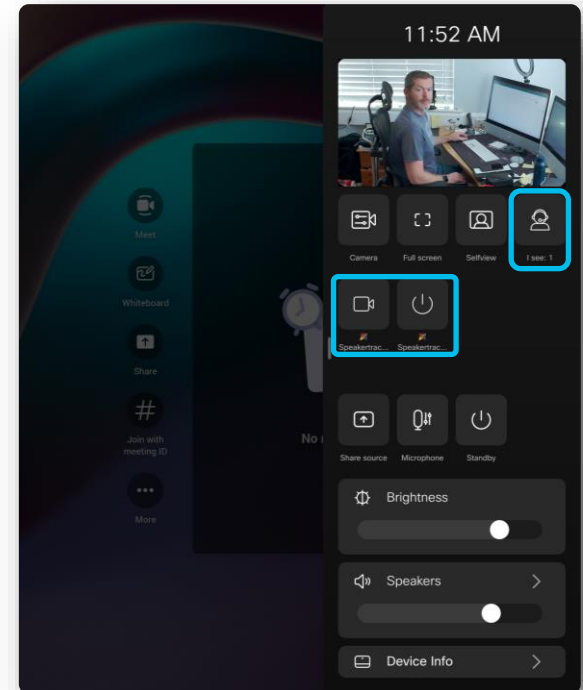
- When reviewing roomos.cisco.com API's, only those xAPI's that have Microsoft Teams Rooms (MTR): Yes status will be visible when MTR filter is applied.
- Please note that you do need to be Control Hub registered to be able to use xAPIs



UI Extensions

Screenshot of full-page UI

- User Interface Extensions (aka UI Extensions) has just reached beta status
- Allows for the end user to be able to invoke and action (for example, close the shades or turn on the light)
- UI Extension will be limited to being visible within the Control Panel of the device.
 - Control Panel is visible by swiping in from the right hand side of the main screen on the Desk Pro and Board Pro and swiping in from the right-hand side of the Room Navigator paired with the Room Bar/Room Bar Pro/Room Kit EQ/Room Kit Pro



Management Capabilities

Microsoft Teams Admin Center and Webex Control Hub

	MTR on Android (no Control Hub registration)	MTR on Android (<u>with</u> Control Hub registration)
Device Inventory	Limited	✓
Device Configuration	Limited	✓
Software Upgrade	Limited	✓
Device Alerts	✗	✓
Meeting Metrics & Analytics	Teams Admin Center only	Teams Admin Center and Control Hub
Macros	✗	Partial
UI Extensions	✗	Beta October 2023
API Integrations	✗	✓
Device Metrics & Analytics	✗	✓
Room Metrics & Analytics	✗	✓
Native Webex Meetings	✗	✓
Environmental Metrics	✗	✓

Device Inventory

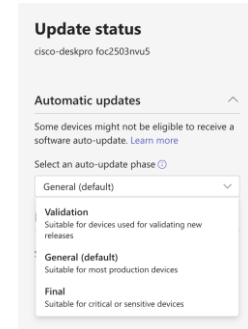
- Control Hub would provide you with:
- Cisco collaboration device and its connected peripherals:
 - Room Navigator
 - Cisco Table Mic Pro
 - Cisco camera (for those platforms with external or multiple camera sources)
 - Attached non-Cisco peripherals
 - Screens
- Teams Admin Center would provide you with:
- Cisco collaboration device
- Room Navigator that is registered with the same resource account as the codec
- If MTR Pro licensed, Teams Admin Center will show you from the main codec view that it has a Navigator attached.

Device Configuration

- Control Hub would provide you with:
- Near real-time configuration of RoomOS on the Cisco collaboration device.
- Allow for device templates to be created and deployed to allow for simpler configuration steps
- The ability to run and execute an xCommand configuration directly from Control Hub to make a change to the device (for example requesting and executing an immediate reboot)
- Teams Admin Center would provide you with:
- The ability to make some small changes to the Teams app
 - Change background image
 - Change time zone and time display
 - Create templates that can be deployed to devices as they register (again only affecting the Teams app on the device)
 - Request a device to reboot which will go into a queue to be executed at some point

Software Upgrade

- Control Hub would provide you with:
- Monthly release of RoomOS software
- Advanced Software Control options to delay deployment of software to certain workspaces
- Preview channel builds
- Option of Beta channel builds (need to be part of the beta program for this channel)
- Not all software releases in Control Hub will be certified by Microsoft
- Teams Admin Center would provide you with:
- Only Microsoft Certified software is available
- Slower release cycle so customer may need to wait longer for a particular fix or feature
- Manual software or automatic upgrade depending on license type assigned



How fast does the rollout happen? Eligible devices receive updates in weekly cycles based on the update phase they are in. For example, devices in General phase start receiving updates only after 15/30 days have elapsed since the new version was published. To ensure a stable rollout, the devices are updated gradually for a tenant and not all at once. Overall, the rollout of each new version takes a few weeks after the start of each update phase. [Details](#)

Device Alerts

- Control Hub would provide you with:
 - Online/Offline status displays in Control Hub
 - Issues detected and resolved. For example:
 - Navigator disconnected
 - Microphone missing
 - Camera disconnected
 - Options for delivery channel
 - Email
 - Webhooks
- Teams Admin Center does not provide for pro-active alerts.
- You will however see online/offline status in Teams Admin Center for the Cisco collaboration device and also Room Navigator
- MTR basic will show separate
- MTR Pro will show linked Navigator
- Microsoft Teams Pro Portal however can generate tickets based on certain aspects (such as online/offline).
- Pro Portal also has a basic integration into Service Now to raise tickets into ticketing platform.

Meeting Metrics and Analytics

- Control Hub would provide you with:
 - Real-time troubleshooting information when the device is in a native Webex meeting.
 - Historical troubleshooting information from when the device has attended a native Webex meeting.
- Teams Admin Center would provide you with:
 - Information for when the device has been in a Microsoft Teams meeting

Macro support

- Control Hub would provide you with:
- The ability to support a macro script leveraging the devices RoomOS API's
 - This is a limited set of API's
 - Macros could run based on events happening

Point to note:

Some features of RoomOS run based on Macros. One example of this would be Audio Console on the Codec EQ and Codec Pro

- Teams Admin Center would provide you with:
- Macros are not supported without a Control Hub registration

UI Extensions

- Control Hub would provide you with:
 - The ability to create a macro script and place a User Interface within the Control Panel of the device that will allow the end user to interact with the device or invoke a service
 - For example it could be a Service Now integration that would allow someone to report that the workspace needs to be serviced or that perhaps the last call was great/not so great.
 - The UI extension would overlay over the top of the MTR UI to allow you to interact
- Teams Admin Center would provide you with:
 - No access to UI extensions

Workspace Metrics and Analytics

- Control Hub would provide you with:
 - Near real-time views of number of people within the workspace
 - Near real-time view as to whether the device is online or idle (Control Hub will show when it is in a MTR, Webex or WebRTC call)
 - Near real-time details on:
 - Temperature
 - Humidity
 - Noise levels
 - Air Quality (when Room Navigator is present)
 - Historical analytics going back up to 30 days
 - Workspace insights
- Teams Admin Center would provide you with:
 - No access to Workspace metrics and analytics.

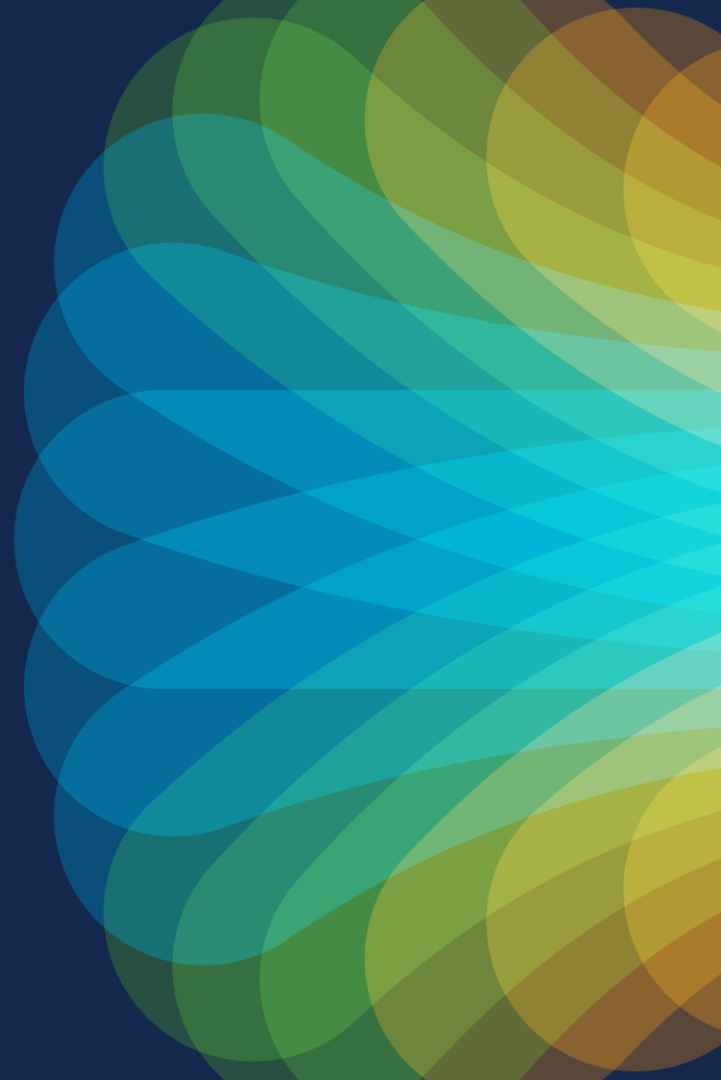
Native Webex meetings

- If registered to both Control Hub and Teams Admin Center, you would have:
 - Native Microsoft Teams Rooms join
 - Native Webex join
 - Direct Guest Join to Zoom via WebRTC
- If only Teams Admin Center registered, you would have:
 - Native Microsoft Teams Rooms join
 - Direct Guest Join to Webex via WebRTC
 - Direct Guest Join to Zoom via WebTRC

Software Upgrade

- Control Hub would provide you with:
 - Monthly software upgrade with the option of Advanced Software Control
 - Stable build software
 - Verification channel (also Stable build software)
 - Stable and Verification channel supported by Cisco TAC
 - Preview channel
 - Beta channel (requires customer is enrolled)
- Teams Admin Center would provide you with:
 - Microsoft Teams certified release software
 - All software based on a Stable RoomOS release
 - Depending on MTR licenses will allow for different phases for update
 - No concept of Preview or Beta

Microsoft Entra and Intune



Microsoft Azure Entra

Microsoft Entra ID, prepare a Microsoft Entra group with dynamic membership to hold all of the Teams Rooms resource accounts. This will simplify future management, such as applying Conditional Access policies. In order to most easily leverage Microsoft Entra dynamic groups, determine a naming convention that will uniquely identify your Teams Rooms resource accounts.

Check statement for MTR Basic...not having Intune license



Microsoft Azure Entra

Characteristics

Can deliver Identity Management and User attributes.

Can manage group of users.

Users can have different characteristics:

- Microsoft Azure tenant Users

- On-premise Users

- Microsoft Free Users

- Guest from another tenant

- Guest created in Microsoft Free tenant



A powerful IdP with many different authentication mechanisms including latest mechanisms like FIDO devices and Passwordless

Support OIDC and SAML protocols for SSO



Microsoft Entra

Conditional Access (CA)



Enforce access controls with adaptive policies

Bring together real-time signals such as [user context](#), [device](#), [location](#), and [session risk](#) information to determine when to allow, block, or limit access, or require additional verification steps.



Help protect data inside applications

[Monitor and control sessions](#), [application access](#), and [sensitive data across your organization](#) in real time based on user behaviour in apps, both on-premises and in the cloud.



Restrict access for vulnerable and compromised devices

Use conditional access policies to check the [device health and security posture of registered devices](#) and ensure only healthy and trusted devices can access your corporate resources.



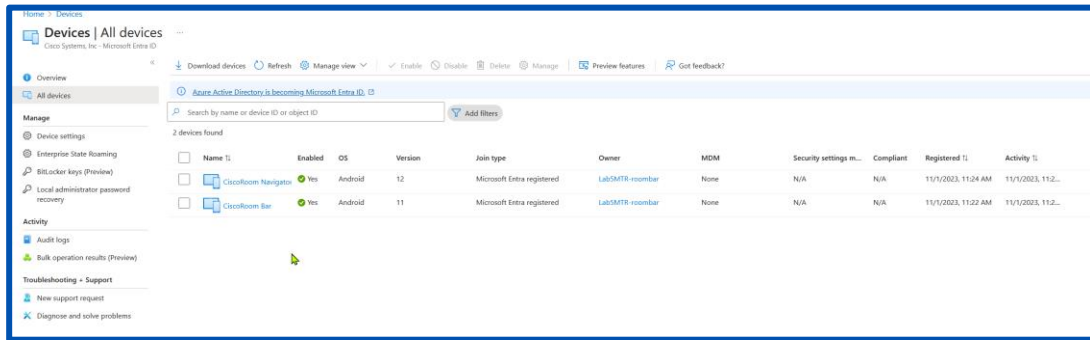
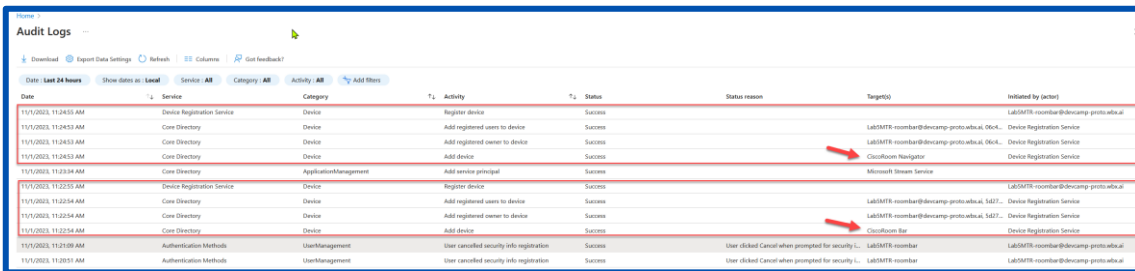
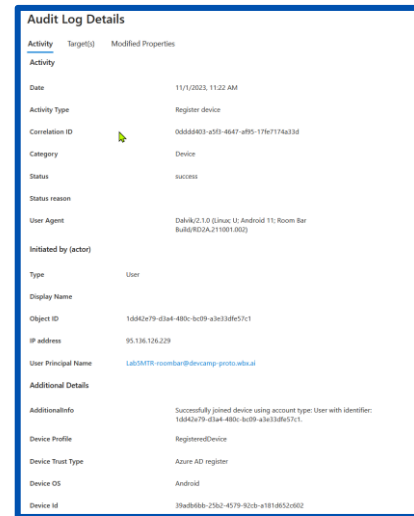
Microsoft Entra

Device monitoring

When registering a Cisco video device as an MTR it is going to appear in the devices of Entra

You will notice the two registrations one for the Webex Room Bar and one for the Webex Navigator

You can see the registrations messages in the audit log





Microsoft Entra

Device monitoring

Even without intune, the regular MTR registration in Entra, doesn't stop the customer to configure Entra Conditional Access (CA).

We can exclude the MTR devices from the CA policies, by filtering for devices and exclude them from CA

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
	displayName	Contains	CiscoRoom

[+ Add expression](#)

Rule syntax ☐

```
device.displayName -contains "CiscoRoom"
```

Activity Details: Sign-ins

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

Date: 11/1/2023, 7:45:05 PM

Request ID: f5c052f-2840-4311-b2b6-26b295a05000

Correlation ID: 2240794b-c257-49ff-ac83-70338b0446ee

Authentication requirement: Single-factor authentication

Status: Failure

Continuous access evaluation: No

Original transfer method: None

Sign-in error code: 530003

Failure reason: Your device is required to be managed to access this resource.

The requested resource can only be accessed using a compliant device. The user is either using a device not managed by a Mobile Device Management (MDM) agent like Intune, or it's using an application that doesn't support device authentication. The user could enroll their devices with an approved MDM provider, or use a different app to sign in, or find the app vendor and ask them to update their app. More details available at <https://docs.microsoft.com/en-us/active-directory/active-directory-conditional-access-device-remediation>

Additional Details:

Follow these steps:

Troubleshoot Event: Launch the [Sign-in Diagnostic](#).

1. Review the diagnosis and act on suggested fixes.

User: LAb5MTR-roombae

Username: LAb5MTR-roombae@devcamp-proto.wbaui

User ID: 1d442e79-d3a1-480c-bc09-abc33d8d57c1

Sign-in identifier:

User type: Member

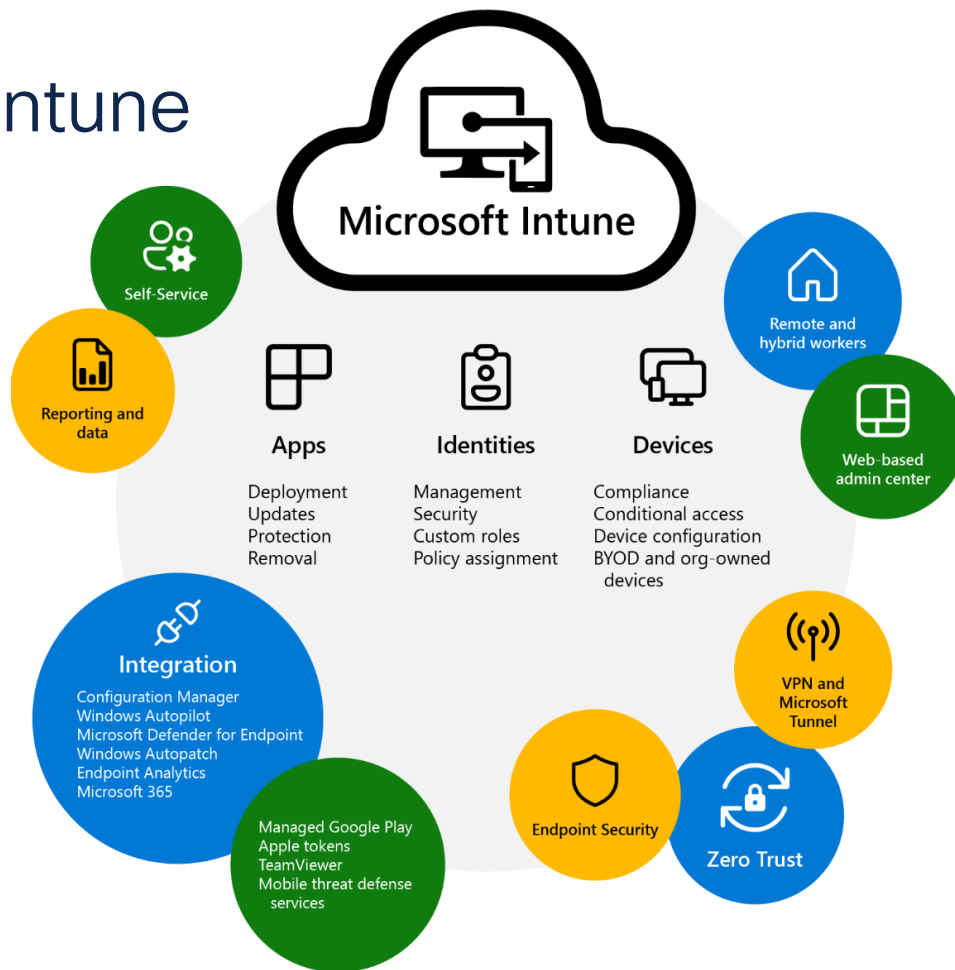
Cross-tenant access type: None

If Cisco room Devices are not excluded, then Entra CA will block the login/registration



Microsoft Intune

What it does ?





Microsoft Intune

Enterprise Mobility Manager (EMM) – Endpoint Security



MDM (Mobile Device Manager)

Deployment of a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure, for the purpose of simplifying and enhancing the IT management of end user devices.

Typically used to manage devices that are owned by the company.



MAM (Mobility Application Manager)

Mobile application management provides granular controls at the application level which enable system administrators to manage and secure application or 'app' data.

Typically used to manage application, when the device is normally owned by the employee, it requires a “Portal” application that controls all the other application under the device that will be managed by the company.



Intune SDK

A piece of software that will be add to the application and allows Intune to deliver policies without the requirement of any other management application.

Typically used by customer that don't have/want an Mobily software deployment platform and deliver device policies to protect the company data in way that does minimum change to a device that is not own by the company

(<https://learn.microsoft.com/en-us/mem/intune/developer/app-sdk>)



Microsoft Intune

MAM (Mobily Application Manager)

Application can be deployed in two ways :

Using Intune validated applications from Mobile App Stores

Applications that are available in the Apple/Android store and have been validate to work with Intune for policies deployment.

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps>



Deployment of IPA/APK/PKG/MSI and wrapping it

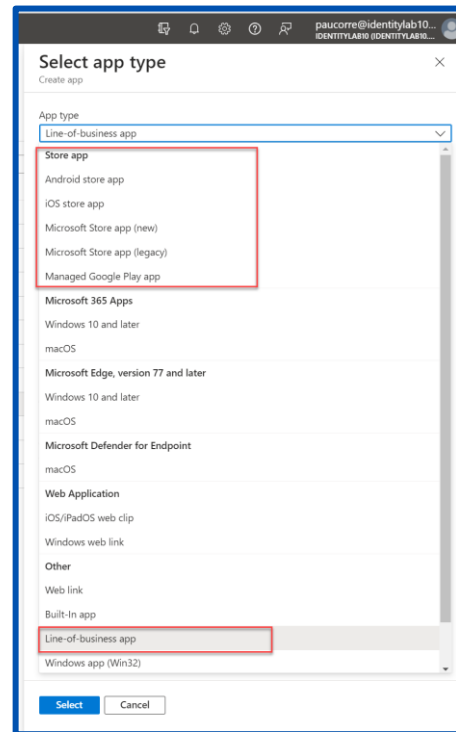
In this mode application vendor provided the un-sign application and after wrapping it, will be deployed through the Company Portal Application with the company policies.

In Intune this deployment is done with Line-of-business App.

To request access to the un-sign version of Webex please read

<https://help.webex.com/en-us/article/n4b78j9/Mobile-application-management-license-agreement>

In iOS and Android, we can also use appConfig to deliver security features to the application <https://help.webex.com/en-us/article/alsshfb/Webex-App-%7C-Secure-mobile-devices>





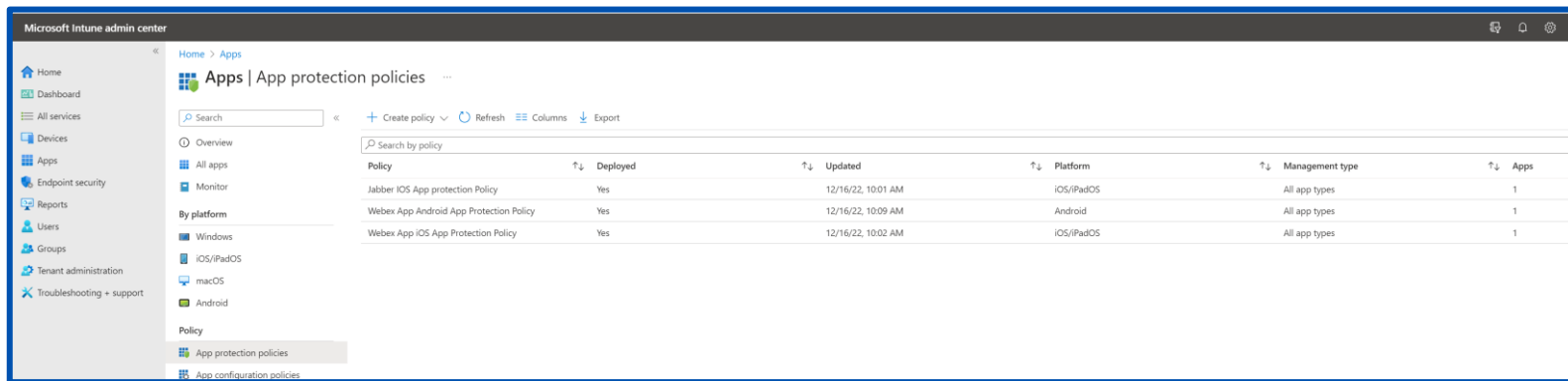
Microsoft Intune

Intune SDK

In Intune, you require that the App Protection Policies to be configured for the Webex App

No other Device or Application configuration is needed in Intune

Customer that has Microsoft Intune, **don't necessarily need** to deploy the Webex App for Intune





Microsoft Intune

Enterprise Mobility Manager (EMM) – Endpoint Security



MDM

normally means

Company own device



MAM

normally means

Employee own device (Higher IT department engagement)



SDK

normally means

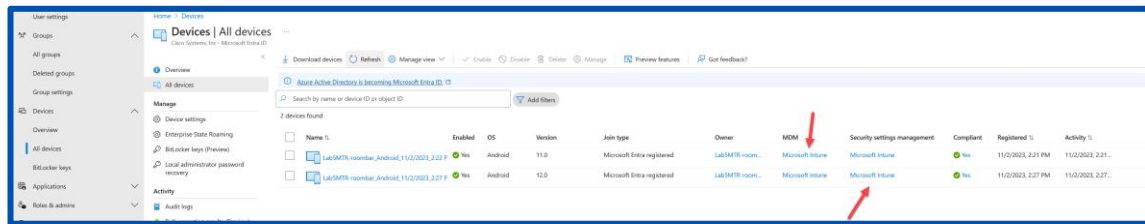
Employee own device (Lower IT department engagement)



Microsoft Intune

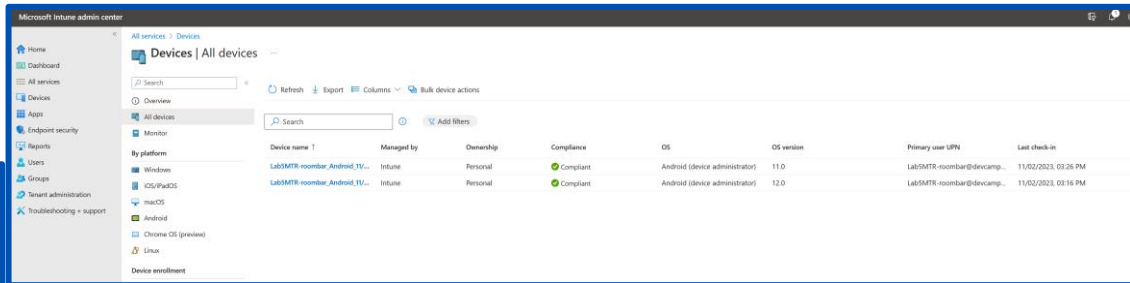
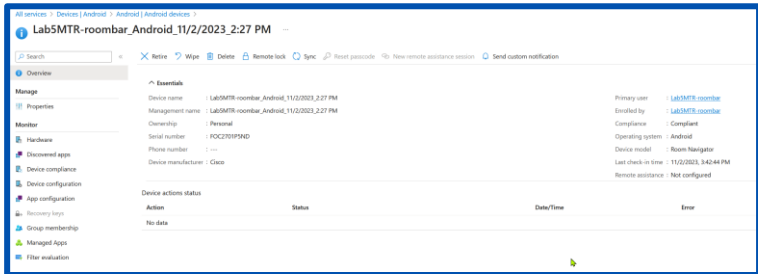
Register MTR in Intune

For the MTR device to be register in Intune in addition to the Entra device an Intune License will need to be assign to the user created for the room



If the user has the Intune License it will appear as using the MDM from Intune and follow the Security Settings Management from Intune in Entra device information

You will also be able to see it in Intune device and see its compliance status





Microsoft Intune

Intune Compliance policy and Entra CA

Typically, our customer will create an Entra CA policy that requires that the device be marked as compliant to allow to grant access

Supported Intune device compliance policies for Android MTR devices :

- Rooted Devices
- Operating System Version (minimum, maximum)
- Require encryption of data storage on device.
- Company Portal app runtime integrity
- Block USB debugging on device

All services > Endpoint security | Device compliance > Compliance policies | Policies >

Android compliance policy

Android device administrator

Basics **Compliance settings** Actions for noncompliance Assignments Review + create

- Microsoft Defender for Endpoint
- Device Health
- Device Properties
 - Operating System Version
 - Minimum OS version 12.0 ✓
 - Maximum OS version Not configured
- System Security

Grant

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

☐ Block access

☒ Grant access

- ☐ Require multifactor authentication
- ☐ Require authentication strength
- ☒ Require device to be marked as compliant
- ☒ Require Microsoft Entra hybrid joined device
- ☐ Require approved client app
- ☐ Require app protection policy
- ☐ Require password change

[Don't lock yourself out! Make sure that your device is compliant. Learn more](#)

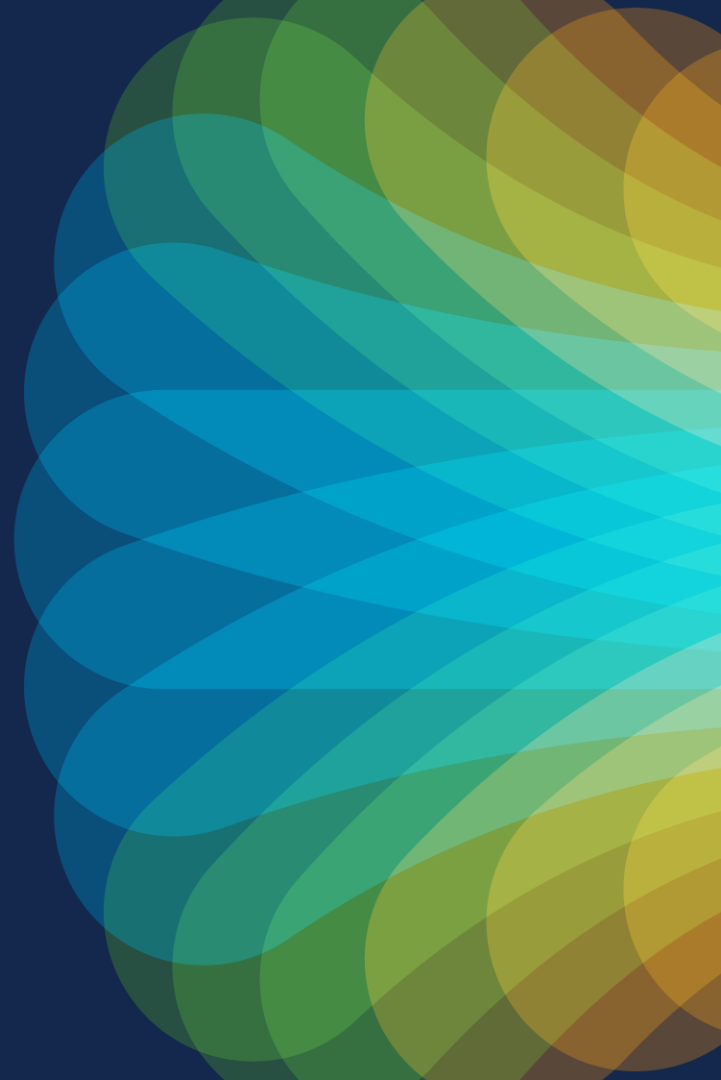
[Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. Learn more](#)

[See list of approved client apps](#)

[See list of policy protected client apps](#)

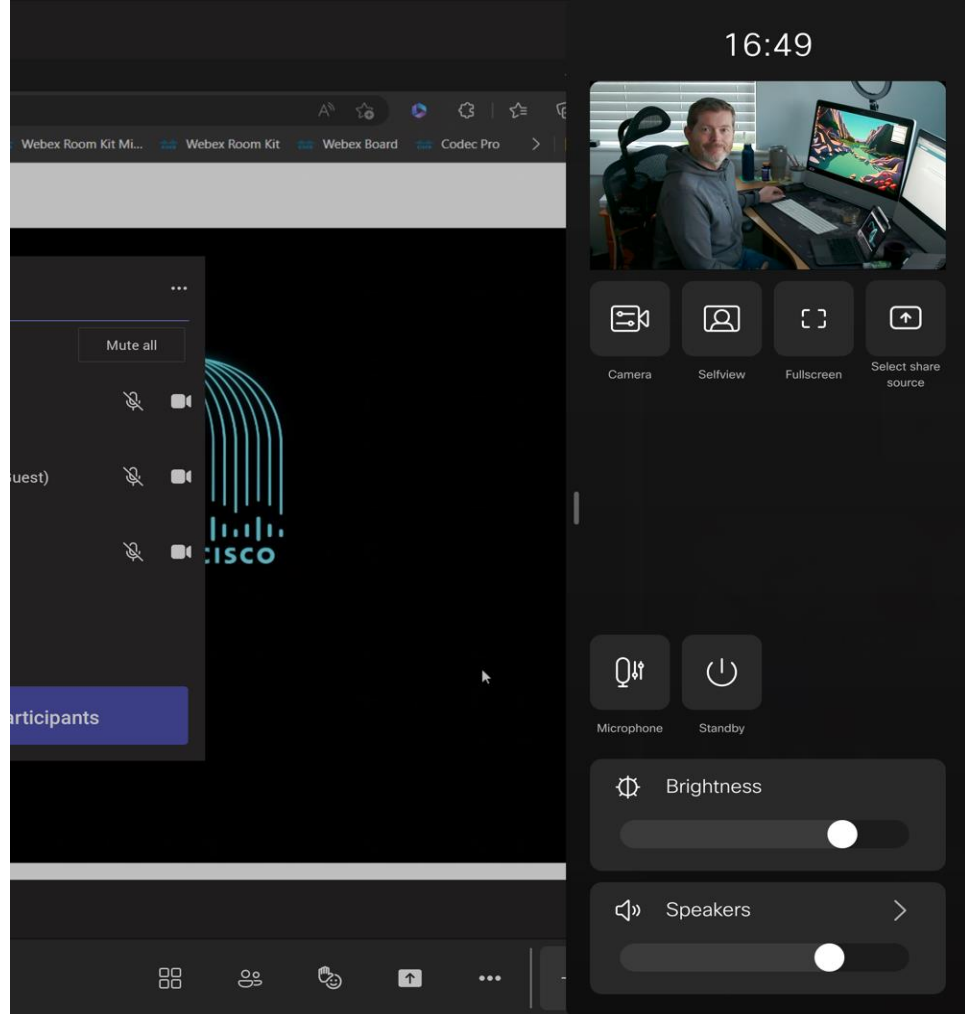
Select

Core RoomOS 11 features supported with Microsoft Teams experience



Access to RoomOS 11 Camera and Audio settings

- Access to RoomOS 11 AI features
- Camera Intelligence
- Audio Intelligence
- Background Replacement (Cisco Desk Pro only)
- When in a
 - Microsoft Teams meeting
 - Webex meeting
 - Zoom meeting
 - BYOD meeting (USB Passthrough)

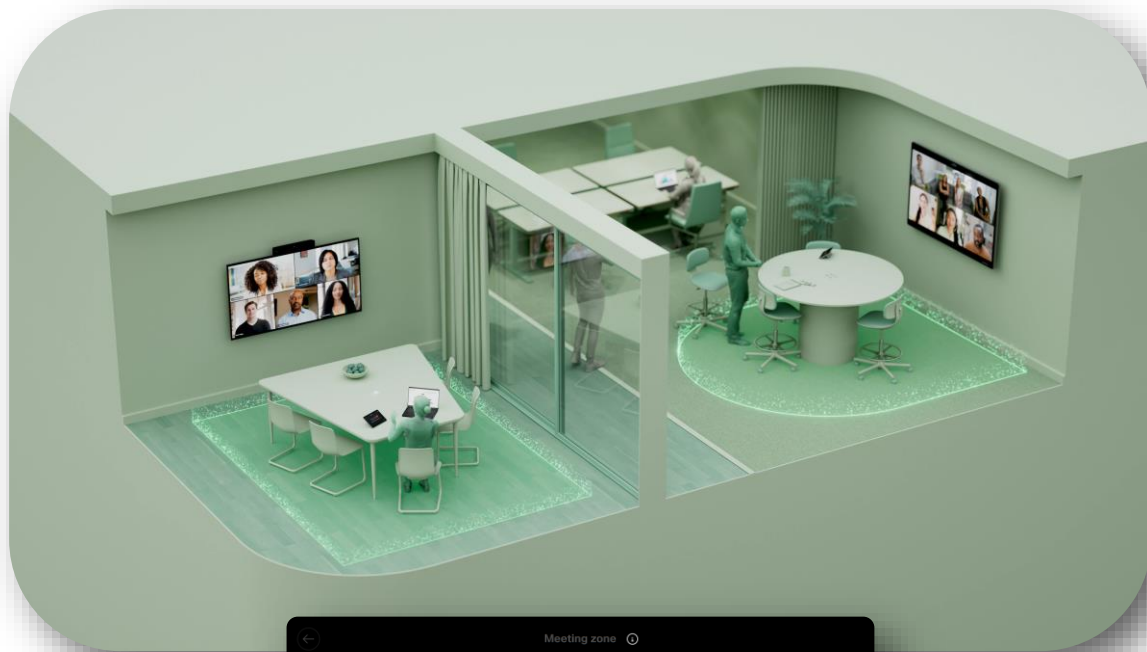
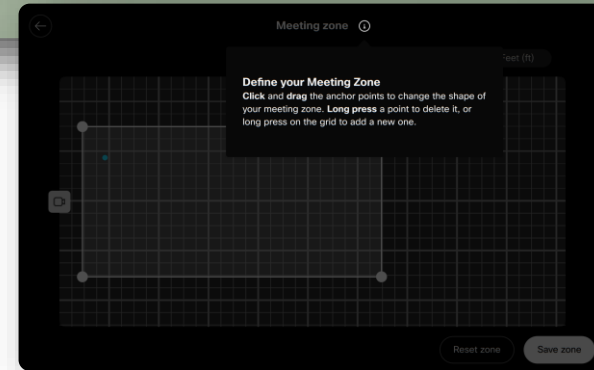


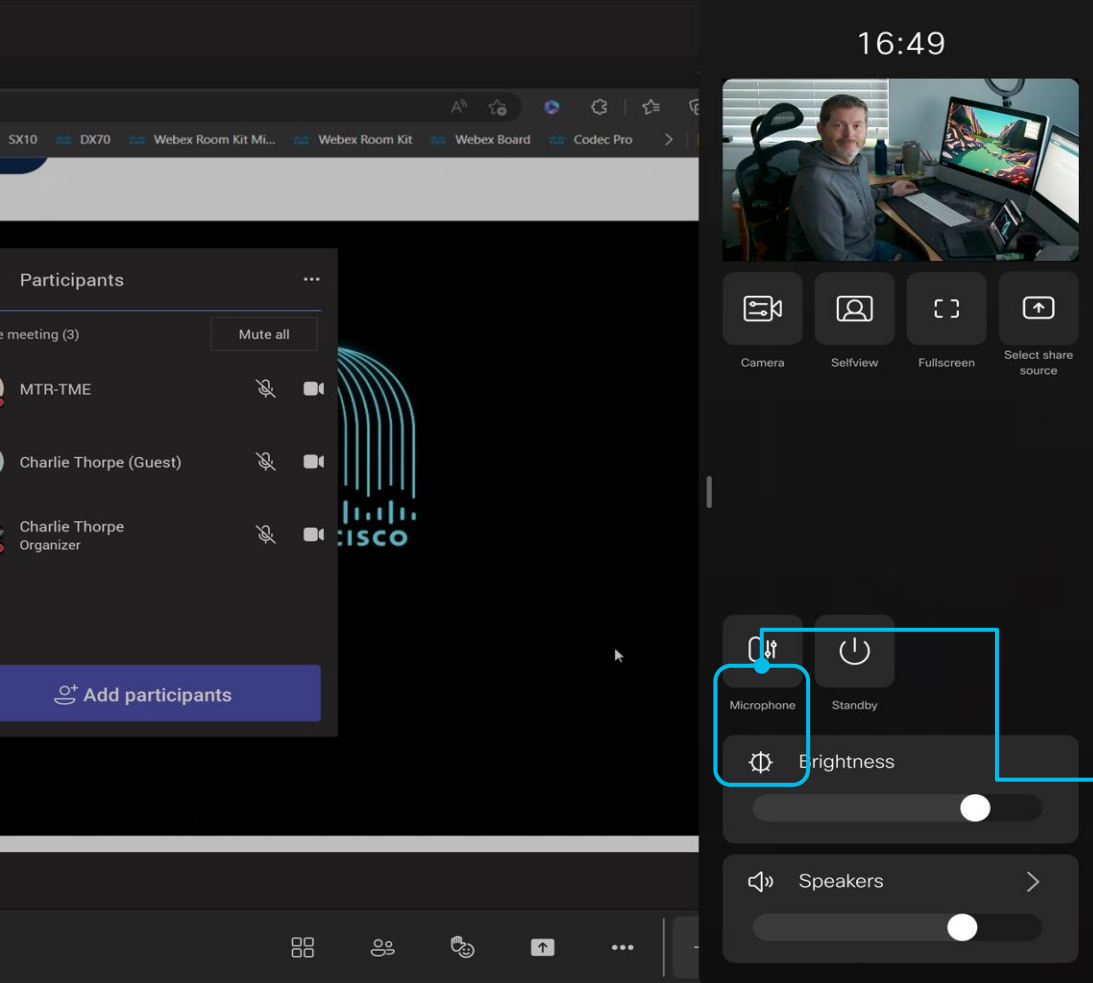
Camera Intelligence

- Cisco Desk Pro
- Best View
- Cisco Board Pro, Room Bar, Room Bar Pro, Room Kit EQ and Room Kit Pro
- Group
- Frames
- SpeakerTrack
- All of the above
- Meeting Zone
- Manual mode
- PTZ controls on local camera
- Multiple cameras

Meeting Zone

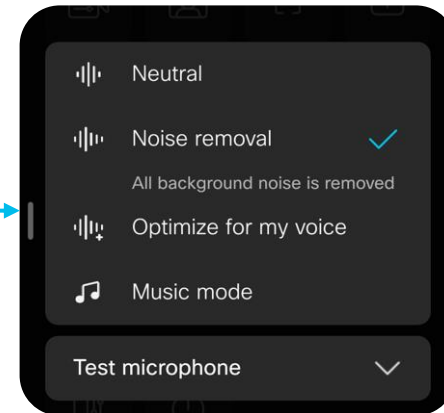
- Enable efficient, distraction-free meetings in open spaces and glass-walled meeting rooms by only framing and tracking people in the meeting.
- Manually set boundaries via the underlying RoomOS UI





Noise removal

Noise removal settings can be accessed from the audio device settings



Content Sharing

Make content sharing simple with a wide range of wired and wireless options:

- USB-C*
- HDMI
- Microsoft Teams Cast
- Miracast®

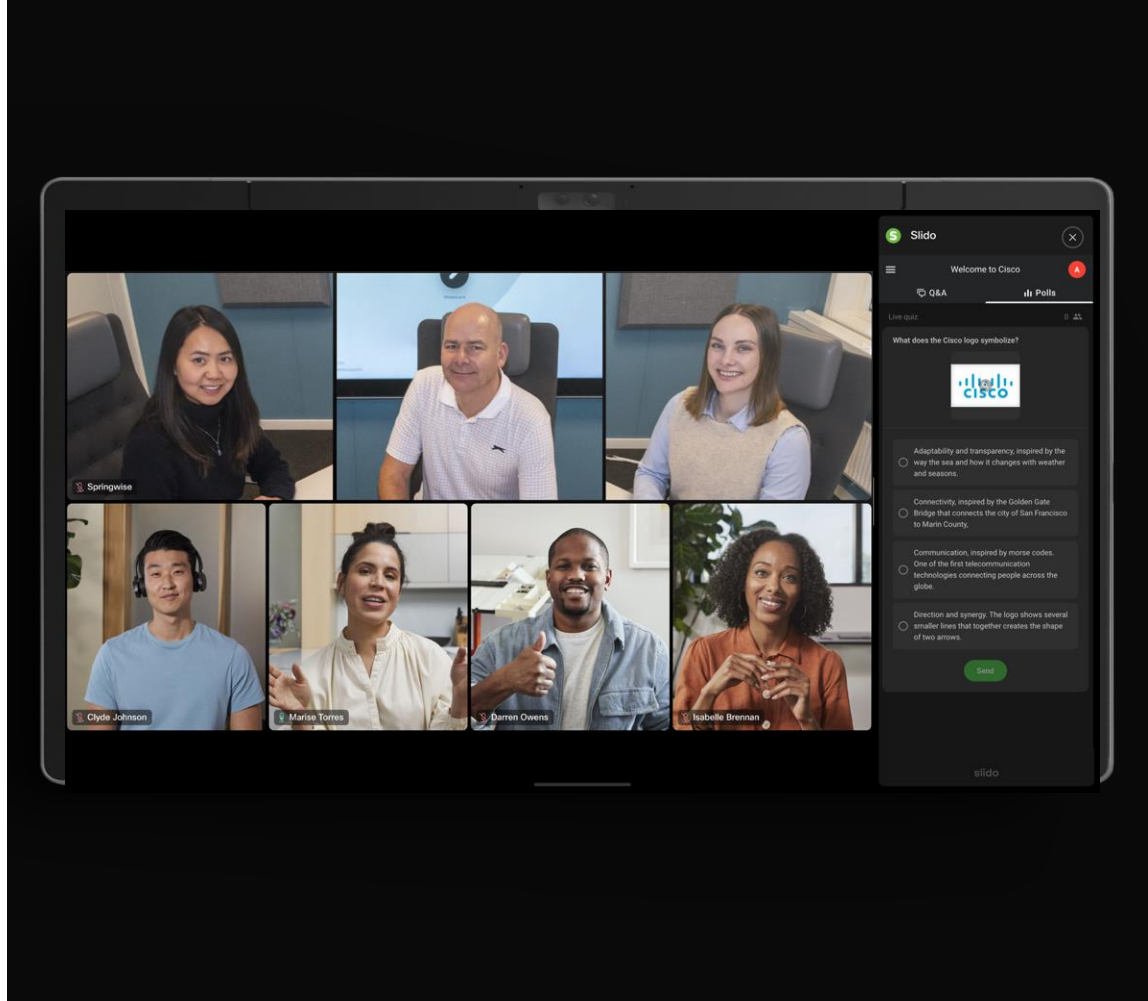
*USB-C sharing is not available with the Room Kit Pro



Fully featured Webex meetings

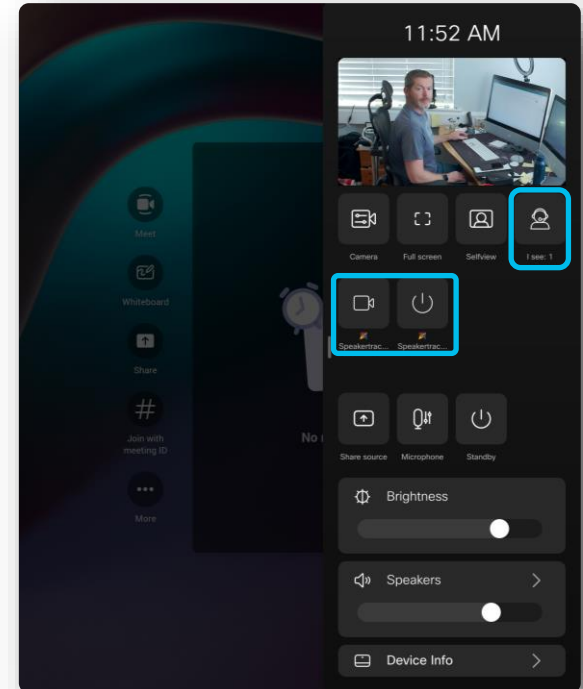
Including:

- Flexible layouts
- People Focus
- Breakouts
- Whiteboarding
- Webinars
- Polling
- Assistant
- Embedded apps

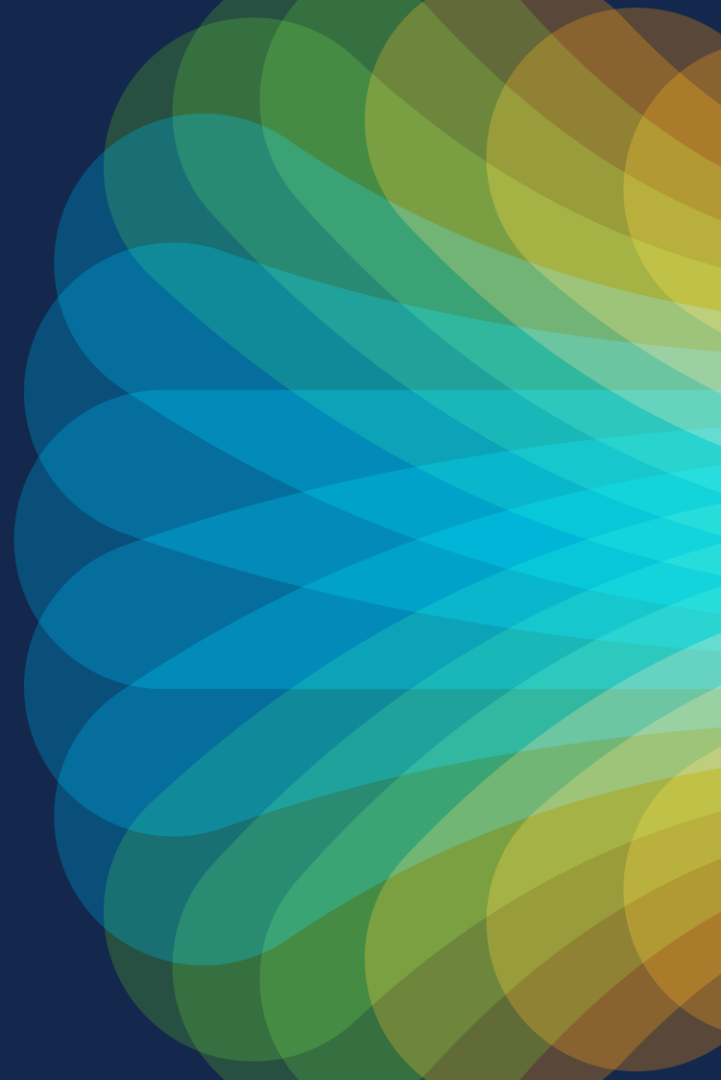


UI Extensions

- User Interface Extensions (aka UI Extensions) has just reached beta status
- Allows for the end user to be able to invoke and action (for example, close the shades or turn on the light)
- UI Extension will be limited to being visible within the Control Panel of the device.
 - Control Panel is visible by swiping in from the right hand side of the main screen on the Desk Pro and Board Pro and swiping in from the right-hand side of the Room Navigator paired with the Room Bar/Room Bar Pro/Room Kit EQ/Room Kit Pro



Troubleshooting



Capture Cisco Logs

The screenshot displays the Cisco Webex Control Hub interface. A modal window titled "Manage Logs" is open in the center. The modal contains the following content:

Generate new logs

Logs generated by the Cisco Webex Cloud are also made available to the Cisco technical support organization. If opening a support case, please provide a feedback ID to the technical support representative so that they may locate the applicable log files.

Uploading new logs might take five minutes or more. You may close this window while waiting for a log upload to finish, and then check back later.

+ Generate Log All Logs Refresh

Time	Type	Feedback ID	Action
11/26/2023 3:24 PM	Full Log	2be45827-8fce-acd3-2341-59f5c7090702	Download

Close

The background interface shows the "webex Control Hub" header with a search bar and user profile. The left sidebar includes navigation links for Overview, Alerts center, MONITORING (Analytics, Troubleshooting, Reports, Customer Journey Data), and MANAGEMENT (Users, Groups, Locations, Workspaces, **Devices**, Apps, Account, Collaboration Australia). The main content area shows "Software" (Beta Channel) and "Alerts" sections.

Common pitfalls and issues

Account setup and creation

- Incorrect Account Creation
 - It's crucial you follow the MTR account creation instructions
 - Do NOT create or use a User Account for MTR
 - Create a Room Resource and run the proper PowerShell Commands
 - Confusion often around where to assign a license / reset password – This is done via PowerShell or in the *Users* section in O365 Admin.
- No Webex meetings show up / No Join button
 - Often caused by incorrect Exchange Calendar Processing rules
 - Same as above – related often to incorrect account creation
 - Ensure the 3rd Party Interop is enabled
 - This has to be done on every single device individually today. Unlock the Device Settings and go to Teams Admin Settings > Meetings > Enable the Webex 3rd party interop

Common pitfalls and issues

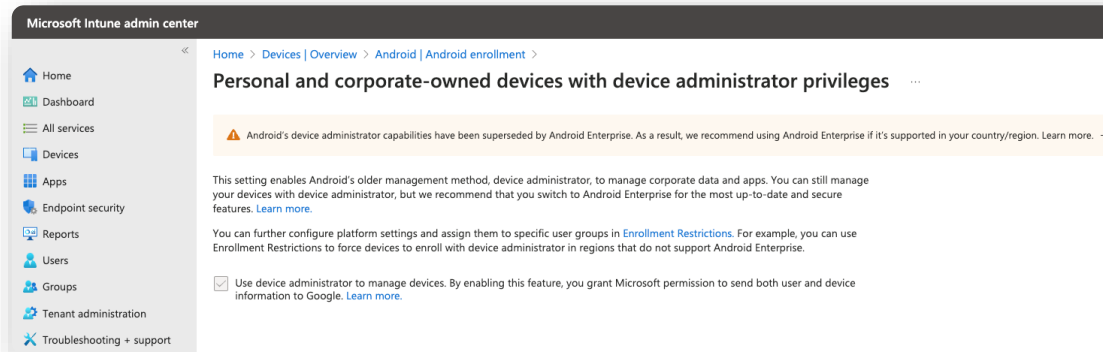
Account setup and creation

- Teams Meeting or Webex Meeting Join button Does not Activate
 - This is not typically an issue but more a difference of design from Microsoft.
 - Microsoft does not “light up” the Join button until the meeting starts.
 - You can join early by simply pressing the Join button even if it’s not “active”

Microsoft Intune

Android Device Administration and Enrollment

- Intune needs to be setup correctly to manage Android based Microsoft Teams Rooms devices.
- As of today, Microsoft only support the legacy Android Device Administrator Management for MTRoA devices. This uses an older and depreciated set of Android API's for device management.
- Microsoft is moving to a Next Gen Management platform using Android Open Source Project (AOSP) Enrollment Profiles. This is not yet available (expected 1st half of 2024)



Common pitfalls and issues

Conditional Access Policies

- Conditional Access Policies allow a set of conditions to be met prior to allowing a device to sign-in. This can be a challenge for some users today, especially in Beta because not all of our devices might meet the conditions set up or required by a company.
- If a device is failing due to a conditional access policy, you can troubleshoot by looking at the device account sign-in logs.
- Go to the Entra Sign-In portal and find User sign-ins tab
- Search for the user account or filter by Teams application and Status: Failure
- Please note: If a Conditional Access policy with Sign-in frequency is configured, this will make all Teams Android devices periodically sign out. This is expected behavior.

Assignment	Teams Rooms on Windows	Teams Rooms on Android and panels	Teams phones and displays
User or workload identities	Supported	Supported	Supported
Cloud apps or actions	Supported Teams Rooms needs to access the following three Cloud apps when in Teams only mode: Office 365 Exchange Online, Office 365 SharePoint Online, and Microsoft Teams	Supported Teams Rooms needs to access the following three Cloud apps when in Teams only mode: Office 365 Exchange Online, Office 365 SharePoint Online, and Microsoft Teams	Supported Teams Android devices need to access the following three Cloud apps: Office 365 Exchange Online, Office 365 SharePoint Online, and Microsoft Teams
Conditions	---	---	---
User risk	Supported	Supported	Supported
Sign-in risk	Supported	Supported	Supported
Device platforms	Supported	Supported	Supported
Locations	Supported	Supported	Supported
Client apps	Not supported	Not supported	Not supported
Filter for devices	Supported	Supported	Supported
Grant	---	---	---
Block access	Supported	Supported	Supported
Grant access	Supported	Supported	Supported
Require multi-factor authentication	Not supported	Not supported	Supported
Require authentication strength	Not supported	Not Supported	Not supported
Require device to be marked as compliant	Supported	Supported	Supported
Require Microsoft Entra hybrid joined device	Not supported	Not supported	Not supported
Require approved client app	Not supported	Not supported	Not supported
Require app protection policy	Not supported	Not supported	Not supported
Require password change	Not supported	Not supported	Not supported
Sessions	---	---	---
Use app enforced restrictions	Not supported	Not supported	Not Supported
Use Conditional Access App Control	Not supported	Not Supported	Not supported
Sign-in frequency	Supported	Supported	Supported
Persistent browser session	Not supported	Not supported	Not supported

Common pitfalls and issues

Supported device Compliance Policies

- Microsoft Teams Rooms on Android has a limited set of Compliance Policies that can be applied.

Teams Rooms on WindowsTeams Rooms on AndroidTeams phones and displaysTeams panels

Below is a table of device compliance settings and recommendations for their use with Teams Rooms.

Policy	Availability	Notes
Microsoft Defender for Endpoint	--	--
Require the device to be at or under the machine risk score	Not supported	
Device Health	--	--
Device managed with device administrator	Required	Teams Android devices management requires device administrator to be enabled.
Rooted devices	Supported	
Require the device to be at or under the device threat level	Not supported	
Google Play Protect	--	--
Google Play Services is configured	Not supported	Google play isn't installed on Teams Android devices.
Up-to-date security provider	Not supported	Google play isn't installed on Teams Android devices.
Threat scan on apps	Not supported	Google play isn't installed on Teams Android devices.
SafetyNet device attestation	Not supported	Google play isn't installed on Teams Android devices.
Device properties	--	--
Operating System Version (minimum, maximum)	Supported	
System security	--	--
Require encryption of data storage on device.	Supported	
Device security	--	--
Block apps from unknown sources	Not supported	Only Teams admins install apps or OEM tools
Company Portal app runtime integrity	Supported	
Restricted apps	Not supported	
Block USB debugging on device	Supported	
*All Android devices	--	--
Maximum minutes of inactivity before password are required	Not supported	
Require a password to unlock mobile devices	Not supported	
Android 10 and later	--	--
Android 9 and earlier or Samsung Knox	--	--
Required password type	Not supported	

Resources

- [Known issues in Teams Rooms and devices - Microsoft Teams | Microsoft Learn](#)

Filter by title

Teams Troubleshooting

> Administration

> Authentication

> Channels

> Conferencing

> Exchange integration

> Files

> Forms

> IM and Presence

> Meetings

> Mobile

> OneNote Integration

> Phone System

> Provisioning

> Sign-in

> Sites

> Tabs

> Teams Rooms and devices

Collect Android Teams device logs

Conditional Access-related issues on Teams Android devices

Known issues

On-screen keyboard size is reduced on some devices

Signed out of Teams Android devices

Teams Rooms app doesn't start automatically after updates

Teams Rooms devices can't fetch calendar

> Teams Rooms Pro Management

> Teams on Linux

> Teams on Mac

> Teams on Windows

> Third-party programs

Teams Rooms and devices on Android

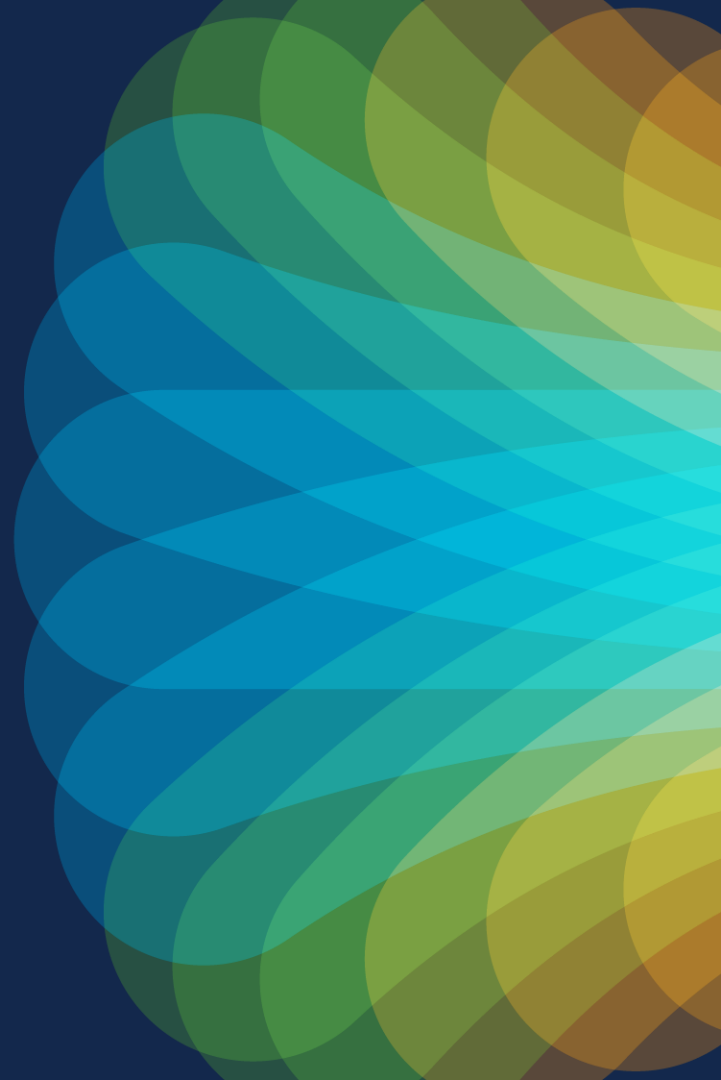
Issues affecting multiple devices

Issue	Description	Workaround
The Report an issue option in Teams Rooms on Android devices doesn't work	In Teams Rooms on Android devices, Teams phones, Teams panels and Teams displays, the Report an issue option under Settings is unavailable.	The option to report issues from Teams Rooms on Android devices is being enhanced. The Report an issue option will be unavailable until the updated experience is released. If you were using the Report an issue option to collect device logs to troubleshoot issues, use the Microsoft Teams admin center instead. See Collect Android Teams device logs for detailed instructions.
Teams phones and Teams panels sign out automatically, and Teams Rooms on Android devices become unpaired	Some models of Teams phones and Teams panels that are running version 5.0.5882.0 of the Company Portal app sign out automatically. Also, Teams Rooms on Android devices that are running the Teams Rooms app version 1449/1.0.96.2023090601 and Company portal app version 5.0.5954.0 might sign out automatically and the touch console on the devices becomes unpaired.	Microsoft is investigating this issue. No workaround is available at this time.

Issues with meeting room devices

Issue	Description	Workaround
Laser pointer and drawing tools in PowerPoint Live don't display for in-room participants	In-room meeting participants in a Teams meeting who are using Teams Rooms on Android devices aren't able to see the following features during a PowerPoint Live presentation: Laser pointer, pen, highlighter, and eraser.	Join the meeting on your personal device to see the laser pointer and drawing tools in PowerPoint Live.
Teams Admin Settings unavailable on Teams Rooms on Android devices with Teams Rooms Basic license.	The Teams Admin Settings option under Device Settings is unavailable on devices that have the Teams Rooms Basic license for Teams Rooms on Android CY22 U3 app (version 1449/1.0.96.2022120503).	Admins can either assign a Teams Rooms Pro license to the same device or downgrade the device to use Teams Rooms on Android CY22 U2B app (version: 1449/1.0.96.2022090606) instead.
Video issues in some	On some Logitech devices that run Teams Rooms on	

One final thing...



ThousandEyes – RoomOS Agents

Get Hop by Hop visibility for your Webex Meetings

- ThousandEyes Endpoint agent is natively incorporated into **RoomOS devices** that will provide **hop-by-hop network path** visibility when these devices are part of the **meetings**.
- It uses the same integration with the control hub that is provided for Windows and Mac clients, so a familiar troubleshooting experience is available to admins. These agents are part of RoomOS but need to be activated explicitly using the Webex control hub and are licenced through ThousandEyes.

Roadmap on MTR
Q1CY24



CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic. On the left, there are overlapping, wavy shapes in shades of red, orange, and yellow, resembling a stylized cloud or a series of overlapping circles. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect. The overall color palette is a rainbow spectrum.

cisco *Live!*

Let's go

#CiscoLiveAPJC