Module 7

Managing Teams Rooms

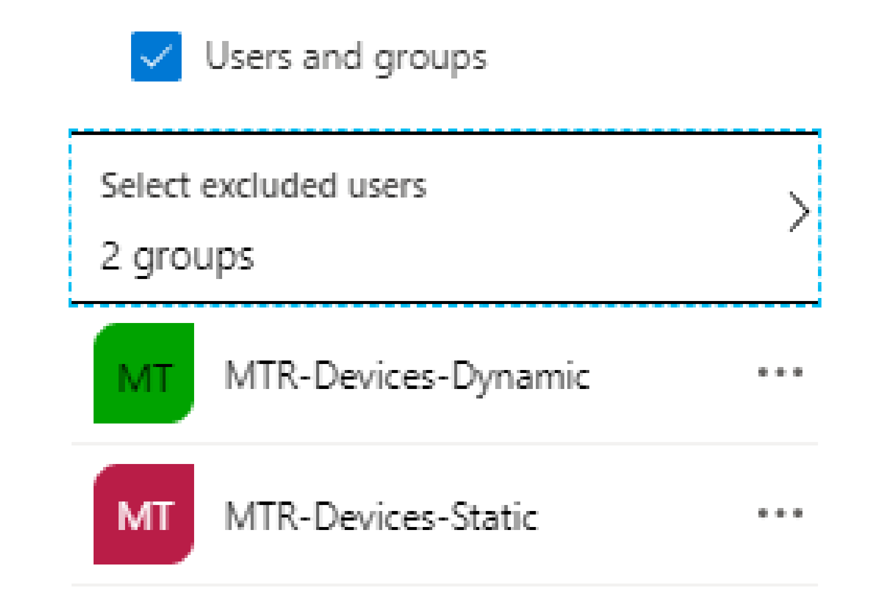
Managing Windows

THIS IS NOT JUST ANOTHER COMPUTER!

Supported Management methods

Supported Management methods

- Active Directory
- Azure Active Directory
- Intune
- Microsoft Endpoint Manager
- Group Policies



☑ Users and groups

Select excluded users

2 groups

MT MTR-Devices-Dynamic

MT MTR-Devices-Static

GPOs / Intune / AAD Considerations

Create dedicated

- OU for the accounts and Teams Rooms devices
- AAD Security Groups for accounts and Teams Rooms devices
- Intune Device Configuration policies
- Conditional Access Policies

Block inheritance on OUs for Teams Rooms accounts and devices, exclude from

- Conditional Access Policies
- MDM Device Configuration policies
- Multi-Factor Authentication policies

Windows security measures

Require Secure Boot and DMA protection.

Lock down all non-administrative users through system policies.

Prevent all standard users but Skype from logging on locally.

Prevent all but administrators access to the device from the network.

Disable insecure guest logons.

Deploy a keyboard filter for allow/block list.

Setup custom key blocking.

Set the default behavior for AutoRun to be Do not Execute.

Prohibit connection to non-domain networks when connected to domain authenticated network.

Turn off WiFi Sense.

Require secure RPC communication.

Delete all windows installed per-user run values under Skype Account.

Hypervisor enforced Code Integrity (HVCI) enabled

Windows security measures

✓

Additional device security information

Lock down policies are continually assessed and tested during the product lifecycle.

✓

Additional details on lockdown policies, account provisioning, and other security measures can be found by inspecting configuration files on the device at c:\users\skype\ScriptLaunchCache\

Examples include:

- Config.cmd
- Registry.pol.txt
- SkypeRoomSystem.reg
- SkypeUser.reg

✓

Another method to review the appropriate files is the following

- Download the SRS Deployment Kit
- Extract the Appx package from the MSI file.
- Unzip the Appx package.
- Review appropriate files located in the \Scripts folder.

Azure Active Directory

What is Microsoft Azure Active Directory?

A subscription-based part of the Microsoft cloud platform

Improves efficiency and simplifies administration with no infrastructure required

Cloud-based identity and access management service

Enrollment

Azure AD joining devices can be achieved several ways

Azure AD join the device from Settings

Windows Configuration Designer can be used to create a Provisioning Package

Hybrid Azure AD join

Management

Consider:

Naming devices with a prefix allows grouping dynamically

- TR-Serial
- TR-Location

Device renaming via Intune

- Not supported for hybrid AAD join

Dynamic AAD* groups allow easy exclusion and inclusion of policies in Intune

*Dynamic Groups requires AAD P1

Microsoft Endpoint Manager

Microsoft Endpoint Manager

The secure, integrated management solution

Cloud-powered intelligence

Optimized for the Microsoft 365 stack

Fully integrated security and identity

Endpoint detection and remediation

Streamlined updates

Any device and any app

Microsoft Endpoint Configuration Manager

What is Microsoft Endpoint Configuration Manager

Configuration Manager helps you deliver more effective IT services by enabling:

Secure and scalable deployment of applications, software updates, and operating systems.

Cloud-powered analytics and management for on-premises and internet-based devices.

Real-time actions on managed devices.

Compliance settings management.

Comprehensive management of servers, desktops, and laptops.

Configuration Manager

Use Configuration Manager to:

- Inventory Teams Rooms
- Deploy new Teams Rooms images
- Configure endpoint protection (firewall, Microsoft Defender, etc.)

Intune

What is Microsoft Intune?

A subscription-based part of the Microsoft cloud platform

Improves efficiency and simplifies administration with no infrastructure required

Manages Internet-connected computers and mobile devices in one place

Deploys corporate applications to managed mobile devices and computers

Helps to protect corporate assets with configuration policies and remote wipe scenarios

Integrates with existing System Center Configuration Manager deployments as required

aka.ms/intunemtr

MDM capabilities with Microsoft Intune

Helps provide device security and configuration for settings such as password complexity, roaming settings, VPN, encryption, and wireless communication

Deploys business applications

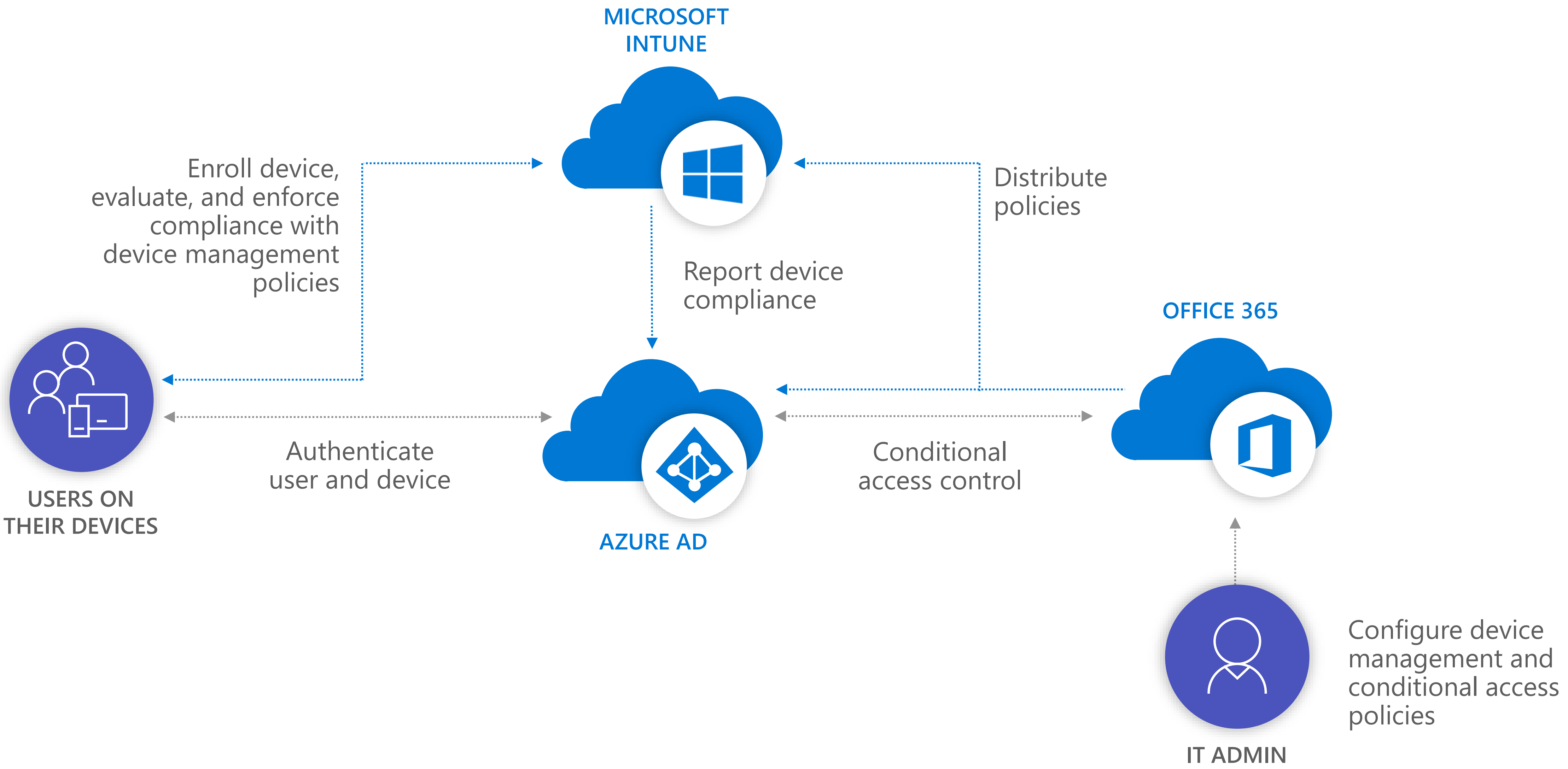
Deploys store applications

Provides access to company resources

Enables inventory and reporting

Provides the ability to retire and wipe mobile devices

Office 365 MDM



MICROSOFT INTUNE

Enroll device, evaluate, and enforce compliance with device management policies

Distribute policies

Report device compliance

OFFICE 365

USERS ON THEIR DEVICES

Authenticate user and device

AZURE AD

Conditional access control

Configure device management and conditional access policies

IT ADMIN

Enrollment

Automatic MDM enrollment is recommended

Only device targeted policies apply

Teams Rooms sign in with a local user account (Not an AAD user account) and do not request any user-assigned policies during Intune synchronization

Intune

Device Configuration Profiles

Administrative Templates (Avoid if possible)

Certificates (Skype for Business)

Delivery Optimization

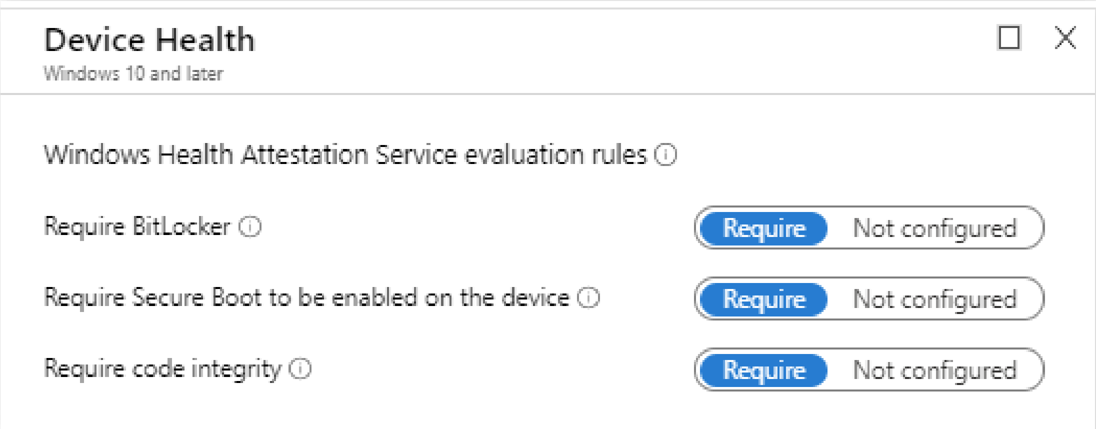
Device Restrictions

Endpoint Protection

Intune Device Compliance Policies

Device Health

Require Secure Boot
Require code integrity



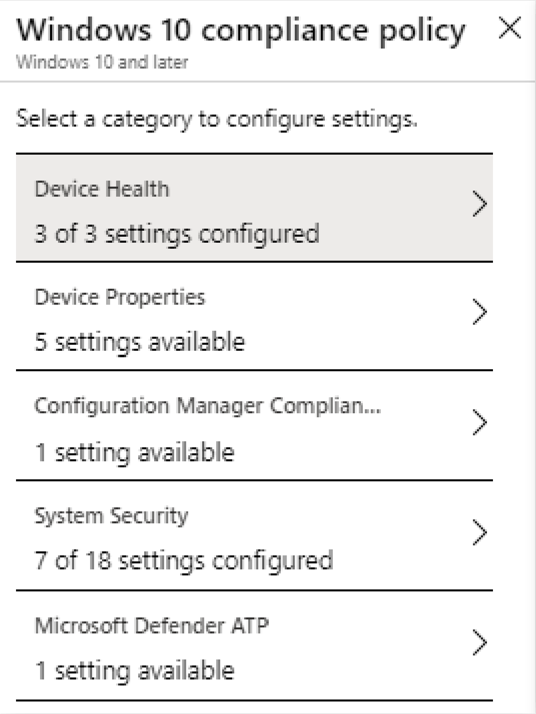
Device Health
Windows 10 and later

Windows Health Attestation Service evaluation rules ⓘ

Require BitLocker ⓘ [✓ Require] Not configured

Require Secure Boot to be enabled on the device ⓘ [✓ Require] Not configured

Require code integrity ⓘ [✓ Require] Not configured



Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health
3 of 3 settings configured

Device Properties
5 settings available

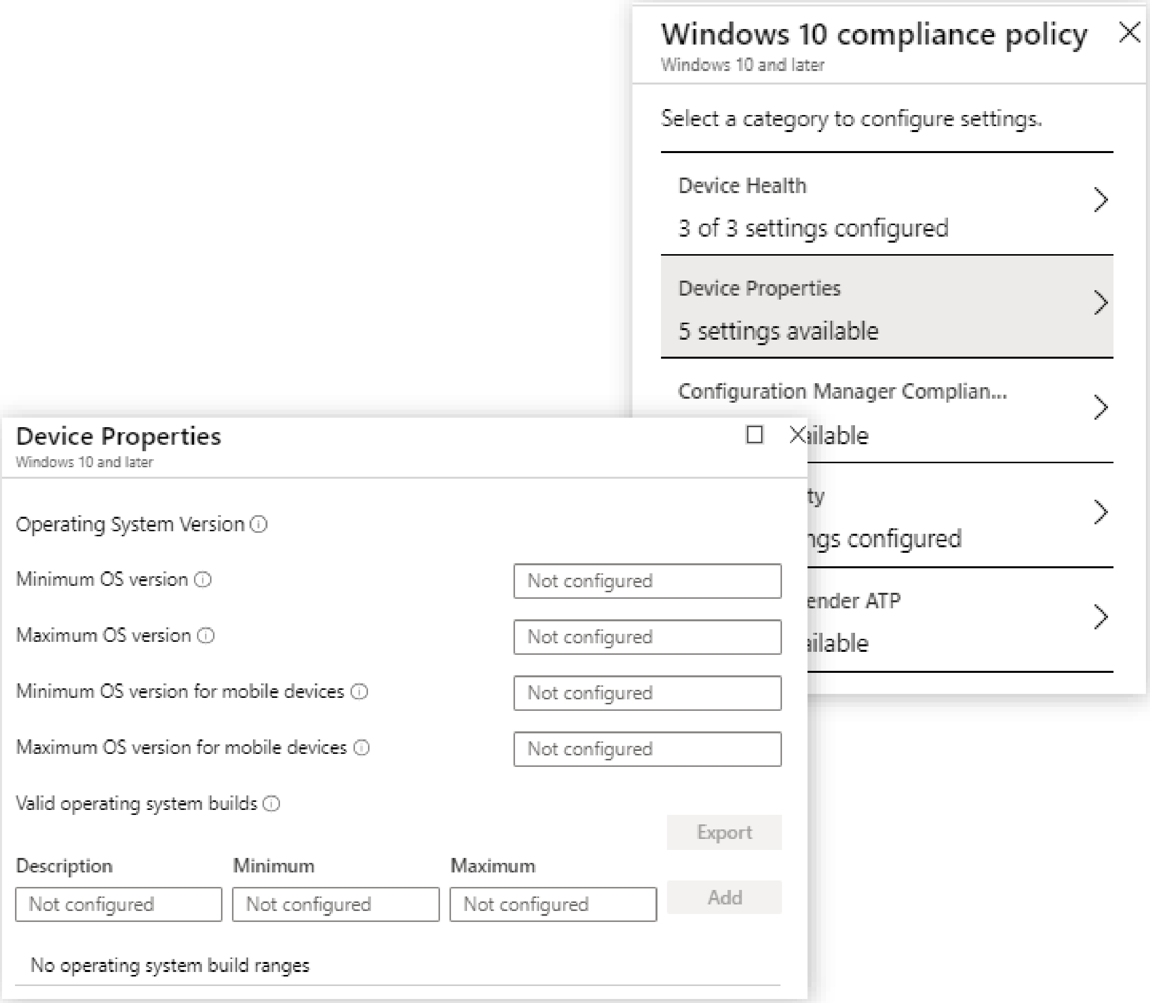
Configuration Manager Complian...
1 setting available

System Security
7 of 18 settings configured

Microsoft Defender ATP
1 setting available

Intune Device Compliance Policies

OS Version compliance should not be the same compliance check as other computers as Teams Rooms is on a delayed cycle to validate functionality with new Windows 10 releases.



Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health
3 of 3 settings configured

Device Properties
5 settings available

Configuration Manager Complian...
ailable

ty
ngs configured

ender ATP
ilable

Device Properties
Windows 10 and later

Operating System Version

Minimum OS version	Not configured
Maximum OS version	Not configured
Minimum OS version for mobile devices	Not configured
Maximum OS version for mobile devices	Not configured

Valid operating system builds

Description	Minimum	Maximum
Not configured	Not configured	Not configured

No operating system build ranges

Intune Device Compliance Policies

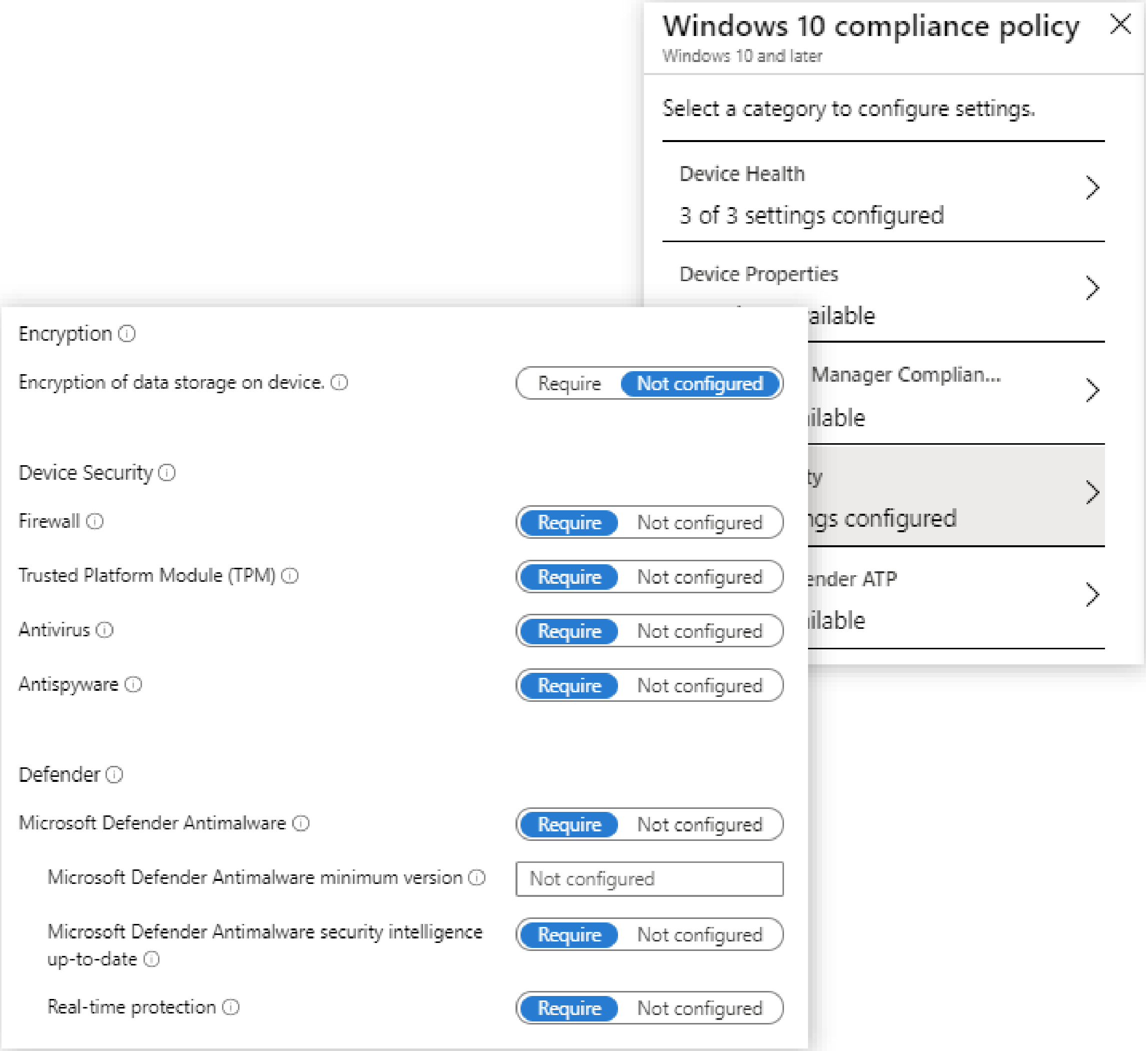
System Security

Password – **Don’t use**

Encryption of data storage – optional

Device Security – Recommended (Firewall, TPM, Antivirus, Antispyware)

Defender - Optional



Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health
3 of 3 settings configured

Device Properties
ailable

Manager Complian...
ilable

ty
gs configured

ender ATP
ilable

Encryption

Encryption of data storage on device. Require [✓ Not configured]

Device Security

Firewall [✓ Require] Not configured

Trusted Platform Module (TPM) [✓ Require] Not configured

Antivirus [✓ Require] Not configured

Antispyware [✓ Require] Not configured

Defender

Microsoft Defender Antimalware [✓ Require] Not configured

Microsoft Defender Antimalware minimum version: Not configured

Microsoft Defender Antimalware security intelligence up-to-date [✓ Require] Not configured

Real-time protection [✓ Require] Not configured

Admin Templates

Do not set the following using Admin Templates:

- Timeout of logon sessions (auto lockout)
- Power management related policies
- Requiring additional authentication steps
- Denying access to local drives
- Prompting users for slow network connections
- Start a certain program at logon
- Push Windows Update to Teams Room System
- Password requirements

Intune

Add Local Admins

https://docs.microsoft.com/en-us/windows/client-management/mdm/accounts-csp

Group Policy

What is Group Policy?

Group Policy is a feature of Microsoft Windows that controls the working environment of user accounts and computer accounts.

Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

Group Policy only applies to domain-joined workstation

Quality of Service via Group Policy

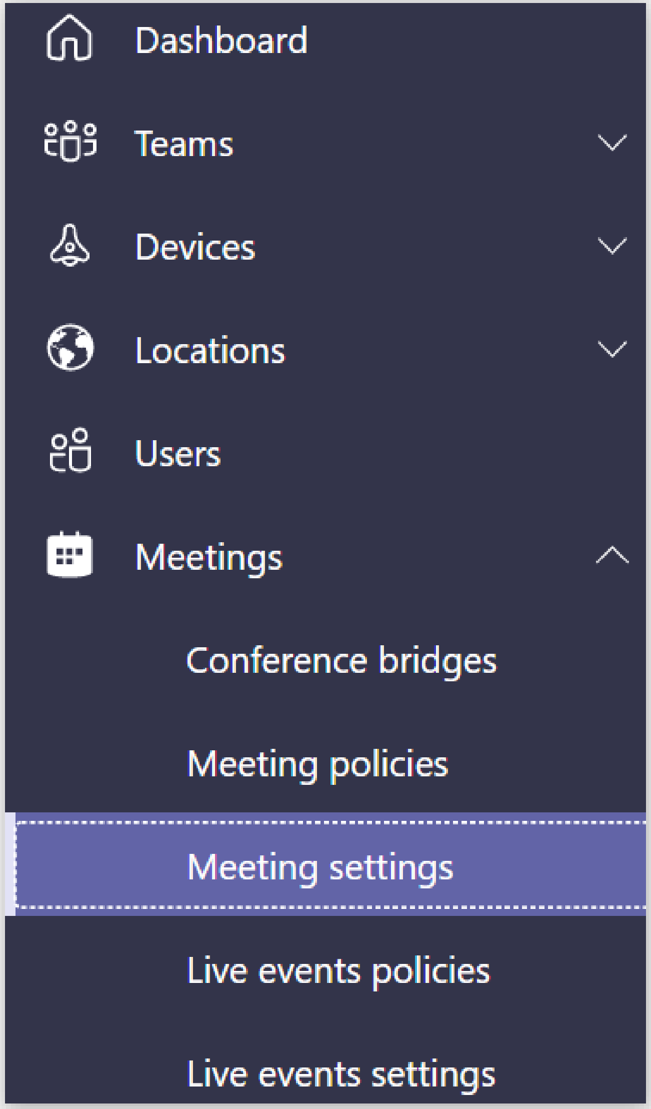
For quality, reliable media, it is highly encouraged to enable Quality of Service throughout the entire network.

A comprehensive design should be undertaken which includes endpoints, switches, and routers.

QoS settings can be configured on Windows servers and PC's via Group Policy

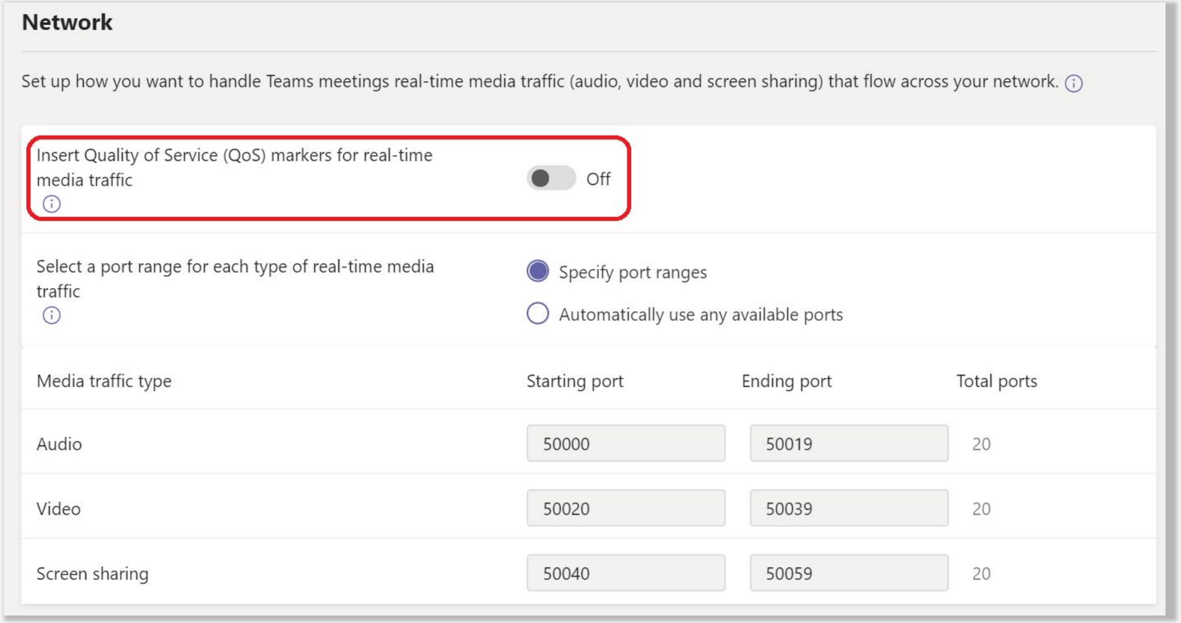
Enable QoS for Microsoft Teams Clients

Navigate to the Microsoft Teams Admin Center
Select Meetings and then Meeting settings



Enable QoS for Microsoft Teams Clients

Scroll down to Network and enable Insert Quality of Service (QoS) markers for real-time media traffic



Network

Set up how you want to handle Teams meetings real-time media traffic (audio, video and screen sharing) that flow across your network.

Insert Quality of Service (QoS) markers for real-time media traffic — Off

Select a port range for each type of real-time media traffic

● Specify port ranges

○ Automatically use any available ports

Media traffic type	Starting port	Ending port	Total ports
Audio	50000	50019	20
Video	50020	50039	20
Screen sharing	50040	50059	20

Turning on Insert Quality of Service (QoS) markers for real-time media traffic will also enable communication to the Transport Relay with UDP ports 3479 (Audio), 3480 (Video) and 3481 (Sharing).

Recommended Port Ranges for Microsoft Teams

Media traffic type	Client source port range	Protocol	DSCP value	DSCP class
Audio	50,000–50,019	TCP/UDP	46	Expedited Forwarding (EF)
Video	50,020–50,039	TCP/UDP	34	Assured Forwarding (AF41)
Application/ Screen Sharing	50,040–50,059	TCP/UDP	18	Assured Forwarding (AF21)

Applying QoS to clients

Create a Group Policy Object that applies QoS markers for Teams media.

Full instructions can be found here.

To apply QoS to non-Windows device types, consider applying QoS at the network layer (e.g. network switch, WiFi access point).

http://aka.ms/qosinteams

Update Management

Update Management

Device reboots nightly at 2:30AM

This helps with:

- ✓ Optimizing app resource utilizations
- ✓ Install pending updates
- ✓ Both Teams Rooms app updates and Windows updates
- ✓ Clears cache and other Windows resources

Updating Windows

- New Windows releases become available after the release has been certified to work properly with Teams Rooms

- Windows patches (for example, security) are deployed and installed as they are made available

Resetting Microsoft Teams Rooms

Reset/Repair Teams Rooms

If the system is not running well, you may need to perform a factory reset.

The Teams Rooms app could also be "out of date" and unable to update to a current version.

There is a "Microsoft Teams Rooms recovery tool" to assist with repairing or resetting the device.

https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/recovery-tool

Steps to Repair Out-of-Date system

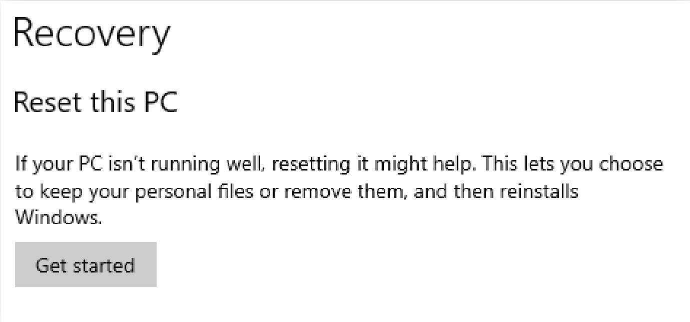
1. Download Microsoft Teams Rooms **installation package** and extract to a USB Stick

2. Run RecoveryTool.ps1 and select **repair**

3. System is now up to date

Reset (Factory Restore)

1 Download Microsoft Teams Rooms **installation package** and extract to a USB Stick

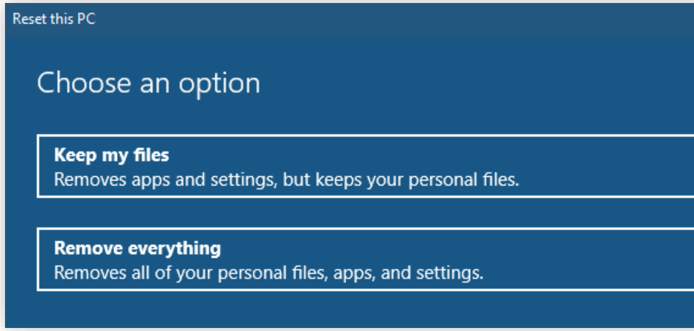


Recovery

Reset this PC

If your PC isn't running well, resetting it might help. This lets you choose to keep your personal files or remove them, and then reinstalls Windows.

2 Run **RecoveryTool.ps1** and select reset (option 2)



Reset this PC

Choose an option

Keep my files
Removes apps and settings, but keeps your personal files.

Remove everything
Removes all of your personal files, apps, and settings.

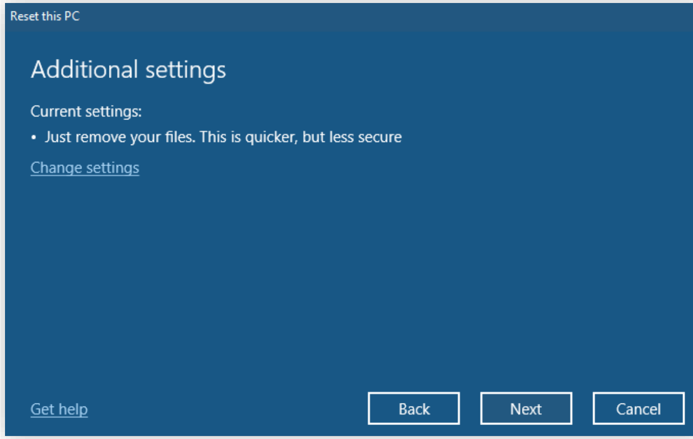
3 You are then asked to perform a Windows Reset
Select "**Remove everything**"

Reset (Factory Restore)

4

Keep the "Just remove your files…." option and **click Next**

You may be notified about not being able to revert to a previous version of Windows after resetting.



Reset this PC

Additional settings

Current settings:

- Just remove your files. This is quicker, but less secure

5

Click Reset

6

The PC will reboot several times. The whole process takes about 2.5 hours

Catastrophic Recovery

Should the device be completely unable to boot Windows, you will need to contact the device manufacturer and they will provide you with the tools to factory image the device.

The vendor-supplied image assures that the proper drivers and tools are installed to correctly work with their hardware.

Work with the vendor for instructions on how to install the recovery image

Microsoft Teams Rooms Premium

Expert management to empower your IT team

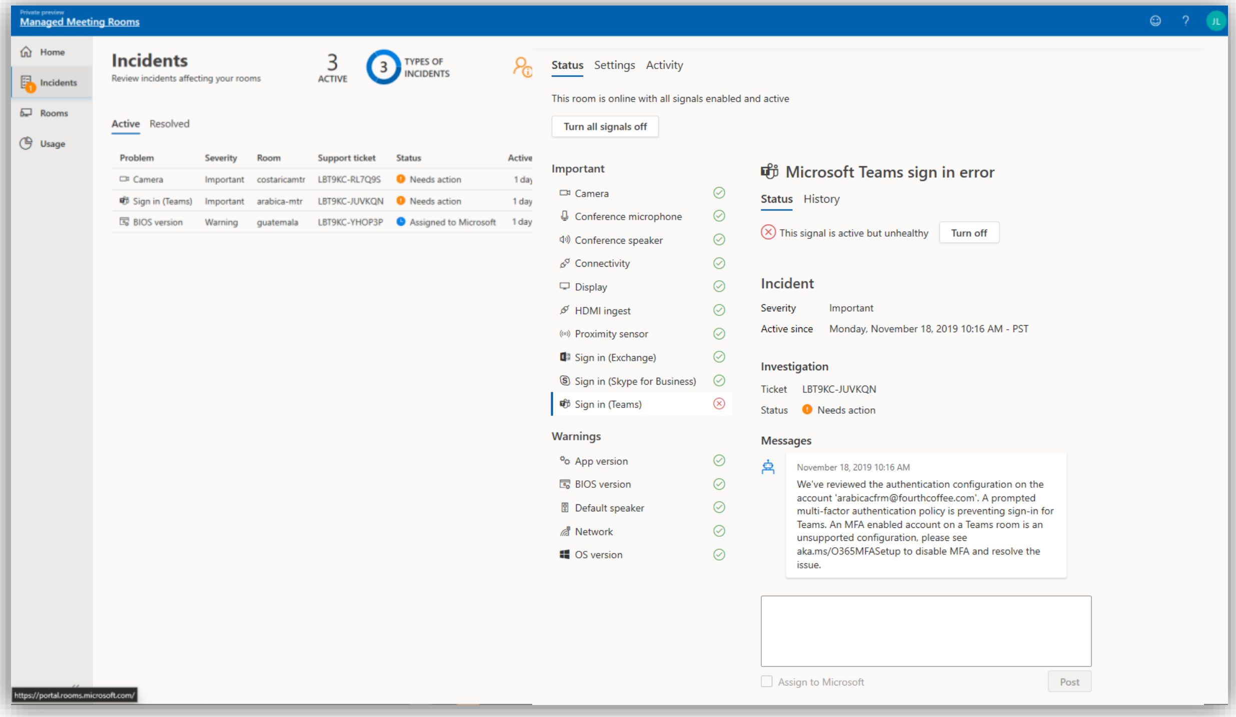
24x7x365 monitoring, alerting, incident management and resolution

Room planning and inventory management

Global service availability and elasticity

Microsoft Endpoint Management integration

Teams Rooms Standard



Incidents

Review incidents affecting your rooms

3 ACTIVE

3 TYPES OF INCIDENTS

Problem	Severity	Room	Support ticket	Status	Active
Camera	Important	costaricamtr	LBT9KC-RL7Q9S	Needs action	1 day
Sign in (Teams)	Important	arabica-mtr	LBT9KC-JUVKQN	Needs action	1 day
BIOS version	Warning	guatemala	LBT9KC-YHOP3P	Assigned to Microsoft	1 day

This room is online with all signals enabled and active

Important

Camera	✓
Conference microphone	✓
Conference speaker	✓
Connectivity	✓
Display	✓
HDMI ingest	✓
Proximity sensor	✓
Sign in (Exchange)	✓
Sign in (Skype for Business)	✓
Sign in (Teams)	✗

Warnings

App version	✓
BIOS version	✓
Default speaker	✓
Network	✓
OS version	✓

Microsoft Teams sign in error

This signal is active but unhealthy

Incident

Severity Important

Active since Monday, November 18, 2019 10:16 AM - PST

Investigation

Ticket LBT9KC-JUVKQN

Status Needs action

Messages

November 18, 2019 10:16 AM

We've reviewed the authentication configuration on the account 'arabicacfrm@fourthcoffee.com'. A prompted multi-factor authentication policy is preventing sign-in for Teams. An MFA enabled account on a Teams room is an unsupported configuration, please see aka.ms/O365MFASetup to disable MFA and resolve the issue.

Proactive security ensures peace of mind from threats

Optimized security, protection, and policies

Software and firmware update maintenance

Enhanced insights grounded in learnings from many customers

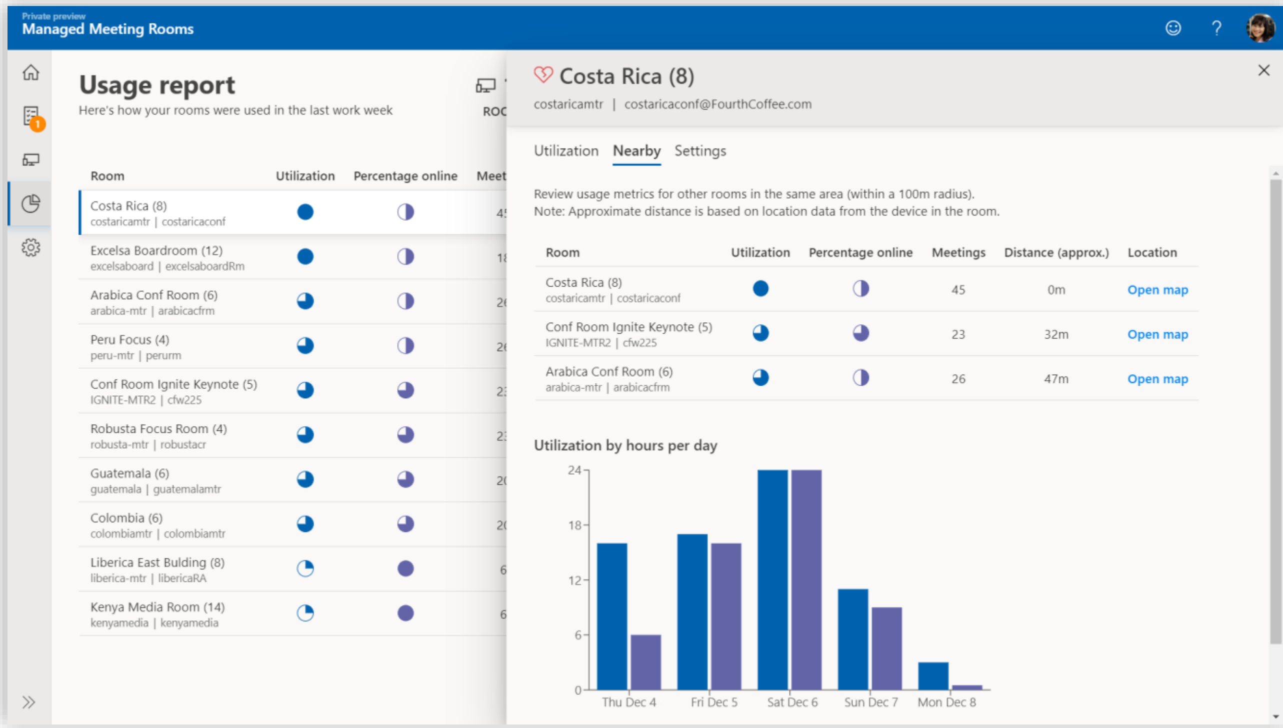
Inventory, health, and compliance reporting

Insights, analytics, and recommendations

Recommendations built from many customers

Recommendations across tenants

Preventive and proactive actions



Usage report

Here's how your rooms were used in the last work week

Room	Utilization	Percentage online	Meet
Costa Rica (8) costaricamtr | costaricaconf	●	◑	4
Excelsa Boardroom (12) excelsaboard | excelsaboardRm	●	◑	1
Arabica Conf Room (6) arabica-mtr | arabicacfrm	◕	◑	2
Peru Focus (4) peru-mtr | perurm	◕	◑	2
Conf Room Ignite Keynote (5) IGNITE-MTR2 | cfw225	◕	◕	2
Robusta Focus Room (4) robusta-mtr | robustacr	◕	◕	2
Guatemala (6) guatemala | guatemalamtr	◕	◕	2
Colombia (6) colombiamtr | colombiamtr	◕	◕	2
Liberica East Bulding (8) liberica-mtr | libericaRA	◔	●	6
Kenya Media Room (14) kenyamedia | kenyamedia	◔	●	6

Costa Rica (8)

costaricamtr | costaricaconf@FourthCoffee.com

Review usage metrics for other rooms in the same area (within a 100m radius).
Note: Approximate distance is based on location data from the device in the room.

Room	Utilization	Percentage online	Meetings	Distance (approx.)	Location
Costa Rica (8) costaricamtr | costaricaconf	●	◑	45	0m	Open map
Conf Room Ignite Keynote (5) IGNITE-MTR2 | cfw225	◕	◕	23	32m	Open map
Arabica Conf Room (6) arabica-mtr | arabicacfrm	◕	◑	26	47m	Open map

Utilization by hours per day

Trusted partners for additional support

Best of breed certified hardware recommendations

Reference on-site service partners for installation and support

Partner value added services available

Remote management

The Technology will manage the device with actions such as:

1 Update software and firmware

2 Mitigate issues through reboots, resetting USB connections & states

3 Collect specific logs to help diagnose issues.

The Technology does not monitor or record audio, video, media, or meeting content.

Network requirements

Protocol	Port
AMQP over WebSockets	443
HTTPS	443

Personally Identifiable Information (PII)

Category	PII	Reason for Query
Ongoing Data Collection & Management	IP Address, Identity of the Room Account (Exchange, Skype for Business and/or Teams), User Activity/Identity from the Room user logged in log file along with Diagnostics information*, Location Coordinates, Emails and communication within Portal with Microsoft or software	Identify and Connect to the System Under Management; Identify, Diagnose, and Mitigate failures; Track Usage, Analytics, and Insights; Query & Repair Connectivity Status

*Sensitive PII in the Device Activity log is redacted out locally (not collected by the Technology):

1. Meeting Subject & Body
2. Contact Card information for Meeting Attendees (such as Title, Phone Number, etc.)
3. In Meeting IM Message Content

Other collected data

Category	Reason for Query
Event log information	Identify, Diagnose, and Mitigate failures and for Usage, Analytics, and Insights
Windows System Queries Examples: List of USB devices, power state, etc.	Identify, Diagnose, and Mitigate failures

Data collected will be processed by Microsoft in accordance with the Microsoft Privacy Statement, available at http://aka.ms/privacy.

Thank you!

Questions?

Microsoft