Managing Crestron MTR Devices in Intune Without Breaking Teams Room Functionality

Your test failure was expected behavior—Microsoft explicitly warns that standard Windows policies will break Microsoft Teams Room (MTR) devices. The Teams Room application was removed because MTR devices require complete isolation from enterprise endpoint policies. This guide provides the exact configuration approach needed to safely enroll 50-60 Crestron devices alongside your 8,000+ standard endpoints.

Why standard Intune policies brick MTR devices

MTR devices run Windows 10/11 IoT Enterprise but function as purpose-built appliances, not general workstations. The **Teams Rooms application** receives updates exclusively through Windows Store and relies on a local "Skype" account for automatic sign-in. When standard enterprise policies target these devices, several critical failures occur:

- **App deployment policies** can remove or replace the pre-installed Teams Rooms application
- **Security baselines** contain settings explicitly incompatible with MTR operation
- **Password/compliance policies** break the local account auto-sign-in mechanism
- **Windows Store restrictions** prevent MTR app updates, causing version conflicts
- **Screen lock timeouts** create unusable meeting room experiences

Microsoft's documentation states definitively: *"Security baselines are **not supported**"* for Teams Rooms devices, and *"DO NOT install applications on to Teams Rooms on Windows devices. These should be treated like appliances."*

The isolation architecture your organization needs

Before enrolling a single Crestron device, establish complete policy isolation using this three-layer approach.

Layer 1: Dynamic Azure AD groups for device targeting

Create a dynamic device group that automatically captures all MTR devices based on naming convention:

Group Name	Dynamic Rule
MTR-Devices-All	`(device.displayName -startsWith "MTR-")`
MTR-Resource-Accounts	Static group for room mailbox accounts

Critical step: Establish a strict naming convention before enrollment. Use formats like `MTR-CRESTRON-{LOCATION}` or `MTR-%SER%` (serial number appended automatically via provisioning package).

Layer 2: Intune assignment filters for real-time exclusion

Assignment filters evaluate at device check-in, solving the dynamic group latency problem where policies apply before group membership calculates. Create this filter:

- **Name**: Exclude-MTR-Devices
- **Platform**: Windows 10 and later
- **Rule syntax**: `(device.deviceName -startsWith "MTR-") or (device.manufacturer -eq "Crestron")`

Apply this filter with "Exclude filtered devices" to every standard Windows policy targeting "All Devices."

Layer 3: Audit and modify all existing policies

Before enrollment, audit every Configuration Profile, Compliance Policy, Security Baseline, and App Deployment currently deployed. Add the MTR exclusion group to each policy's exclusion list. **This step is non-negotiable**—a single overlooked policy can brick devices.

Supported versus unsupported Intune policies for MTR

Microsoft provides explicit guidance on which policy types work with Teams Rooms.

Configuration profiles that are safe to deploy

Profile Type	Status	Notes
Administrative Templates	✅ Supported	For NTP, update settings
Certificates	✅ Supported	For network authentication
Delivery Optimization	✅ Supported	
Device Restrictions	✅ Supported	Minimal settings only

Profile Type	Status	Notes
Endpoint Protection	✅ Supported	Firewall, Defender
PowerShell Scripts	✅ Supported	Requires Azure AD join
Settings Catalog	✅ Supported	Most flexible option

Policy types that break MTR functionality

Profile Type	Status	Impact
Security Baselines	❌ **Not Supported**	Can remove Teams app, break functionality
Kiosk Profiles	❌ Not Supported	MTR has built-in kiosk mode
Shared Multi-user Device	❌ Not Supported	Conflicts with MTR architecture
Identity Protection	❌ Not Supported	MTR uses local account
Edition Upgrade	❌ Not Supported	Can corrupt image
Wi-Fi Profiles	❌ Not Recommended	MTR devices use wired LAN
VPN	❌ Not Recommended	Not applicable

Compliance settings that must be excluded from MTR

These settings will break Teams Room functionality:

- **All password policies** (prevents local Skype account auto-sign-in)
- **Maximum minutes of inactivity before password required** (disrupts meeting room experience)
- **Operating System version requirements** (can block sign-in after updates)
- **Microsoft Defender Anti-malware minimum version** (MTR auto-updates)

Configuration profiles for your specific management needs

Time synchronization via Settings Catalog

Navigate to Intune Admin Center → Devices → Configuration → Create Profile → Settings Catalog.

Search for "Windows Time Service" and configure:

Setting	Recommended Value
Enable Windows NTP Client	Enabled
NtpServer	`time.windows.com,0x9`
Type	NTP (not NT5DS for Entra-joined)
SpecialPollInterval	3600 (hourly sync)

Deploy a companion PowerShell script to ensure the time service starts automatically:

```powershell
Set-Service W32time -StartupType Automatic
Restart-Service W32time
```

Bluetooth management for Proximity Join

MTR devices require Bluetooth for **Proximity Join** features—the ability for users to join meetings from nearby devices. Do not disable Bluetooth.

CSP settings to configure (via Settings Catalog → Bluetooth):

Setting	Value	Rationale
AllowBluetooth	2 (Allow)	Required for Proximity Join
AllowAdvertising	1 (Allow)	Enables MTR beacon features
AllowDiscoverableMode	1 (Allow)	Required for room discovery
AllowPromptedProximalConnections	1 (Allow)	Required for Swift Pair

Windows Update for Business configuration

MTR devices have a built-in update scheduler that runs at 2 AM daily. Create a separate Update Ring specifically for MTR:

Navigate to: Devices → Windows → Update rings for Windows 10 and later

Setting	Recommended Value
Servicing channel	General Availability Channel (LTSC not supported)
Quality update deferral	7-14 days
Feature update deferral	0 (use Feature Updates policy instead)
Automatic update behavior	Auto install and restart at scheduled time
Active hours	7:00 AM – 11:00 PM
Deadline for quality updates	3 days

Critical: Only deploy Windows versions explicitly supported by MTR. Check Microsoft's Teams Rooms lifecycle support documentation before pushing feature updates.

For WSUS integration, configure via Settings Catalog:

- **Specify intranet Microsoft update service location**: Your WSUS URL
- Note: MTR app updates still come from Microsoft Store, not WSUS

Windows LAPS implementation

⚠️ **Crestron-specific warning**: Some Crestron peripherals (touch controllers, room schedulers) authenticate using local admin credentials. Password rotation may disconnect these devices. Contact Crestron support before implementing LAPS to understand the impact on your specific Flex models.

Enable LAPS in Entra ID: Navigate to entra.microsoft.com → Identity → Devices → Device Settings → Enable LAPS → Yes

Create LAPS policy: Endpoint Security → Account Protection → Create Policy

Setting	Recommended Value
Backup Directory	Azure AD only
Password Age Days	30
Administrator Account Name	**Admin** (match MTR default)
Password Complexity	Large + small letters + numbers + special characters
Password Length	14-20 characters
Post Authentication Actions	Reset password + Log off

Assign to your MTR device group only.

Crestron-specific guidance and documentation

Crestron provides official guidance for Intune management through several resources:

UC-ENGINE Security Reference Guide (Doc. 8726) confirms that Crestron UC-ENGINE devices are Microsoft Autopilot-ready and can be managed via Intune. The guide emphasizes: *"Tenant management and conditional access policies should be reviewed as part of a secure deployment."* Crestron

Key Crestron considerations:

1. **XiO Cloud integration**: Crestron recommends using XiO Cloud for hardware management (touch screens, audio devices) alongside Intune for Windows policies. XiO Cloud settings override local Crestron Settings app changes.
2. **Default account warning**: Per Crestron documentation: *"CAUTION: The password for the default Microsoft Teams account must not be changed. If changed, the device will require a reimage."*
3. **Supported documentation URLs**:
    - Flex MTR Systems Insider: support.crestron.com/app/answers/detail/a_id/1000471
    - UC-ENGINE Security Reference: crestron.com/getmedia/08d0bf30-a8d6-4346-b6b7-0ab1182fb8e5/mg_sr_uc-engine
    - MTR Configuration Guide: docs.crestron.com/en-us/9132/Content/Topics/Configuration-Teams.htm

---

Teams Room Pro versus Basic licensing for Intune

Your licensing choice significantly impacts management capabilities.

Feature	Teams Rooms Basic	Teams Rooms Pro
Maximum licenses	25 per tenant	Unlimited
Intune included	❌ No	✅ Yes (Plan 1 & 2)
Entra ID P1 included	❌ No	✅ Yes
Conditional Access	❌ Not available	✅ Available
Defender for Endpoint P2	❌ No	✅ Yes
Teams Rooms Pro Management Portal	❌ No	✅ Full access
Remote device management	Limited	Full

For 50-60 devices requiring Intune management: Teams Rooms Pro (~$40/device/month) includes all necessary licensing. With Basic licenses, you must purchase separate Intune licenses and Entra ID P1.

Conditional Access note: MFA is not supported for MTR resource accounts—there's no second device to approve authentication. Use location-based controls and compliant device requirements instead. Exclude MTR resource accounts from all MFA policies.

Enrollment method for your Crestron fleet

Recommended: Bulk enrollment via provisioning package

Use Windows Configuration Designer to create a provisioning package that:

- Sets device naming convention (`MTR-CRESTRON-%RAND:4%`)
- Joins device to Azure AD
- Auto-enrolls in Intune
- **Critical setting**: "Configure devices for shared use" = **NO** (otherwise local sign-in fails)

Apply via USB during initial setup or remotely for existing devices.

Alternative: Device Enrollment Manager (DEM) account

For manual enrollment:

1. Create dedicated DEM account
2. Azure AD join from Settings → Accounts → Access work or school
3. **Important**: Remove primary user after enrollment (MTR is a shared device) Microsoft Community

DEM accounts support up to 1,000 devices; one account handles your 50-60 device deployment.

Implementation checklist

Complete these steps in order:

Before enrollment:

□ Establish naming convention (e.g., `MTR-CRESTRON-{ROOM}`)
□ Create dynamic Azure AD group with rule `(device.displayName -startsWith "MTR-")`
□ Create Intune assignment filter for MTR exclusion
□ Audit ALL existing policies—add MTR exclusion to each
□ Create MTR-specific compliance policy (Firewall, Defender only—no passwords)
□ Create MTR Update Ring (separate from standard endpoints)
□ Create LAPS policy with "Admin" account name
□ Test Crestron peripheral connectivity with LAPS before production deployment
□ Exclude MTR resource accounts from MFA Conditional Access policies

During enrollment:

□ Use provisioning package or DEM account
□ Verify device appears in MTR dynamic group
□ Remove primary user if using DEM enrollment
□ Confirm no standard policies apply to device

Post-enrollment verification:

□ Teams Room application launches correctly
□ Peripherals (touch controllers, cameras) function
□ Time synchronization working
□ Update ring assigned correctly
□ LAPS password visible in Entra portal

Conclusion

The core principle is **complete isolation**: MTR devices require separation from your standard 8,000+ device policy set. Microsoft explicitly documents that security baselines, password policies, and app deployment policies break Teams Rooms functionality. By implementing dynamic groups, assignment filters, and MTR-specific minimal policies before enrollment, your 50-60 Crestron devices will function reliably while gaining centralized management for time sync, Bluetooth, updates, and LAPS.

The most critical insight from community deployments: **create all exclusions before enrolling the first device**. The policy audit step is non-negotiable—one overlooked "All Devices" assignment can repeat the bricking incident. With proper isolation architecture, organizations successfully manage thousands of MTR devices alongside standard endpoints without conflicts.