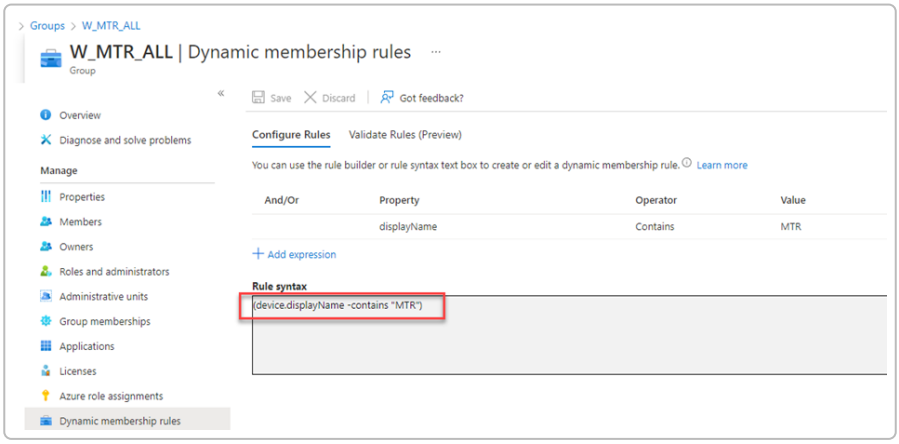
ChatGPT

Intune Management Plan for Teams Rooms (Crestron) Devices

1. **Isolate Teams Rooms Devices in Intune and Exclude from Standard Policies:**



Dynamic Azure AD group using naming to target Teams Rooms. We will create a dedicated dynamic device group (e.g. devices with names starting with "MTR") to manage all Teams Rooms systems [1]. This ensures these 50–60 Crestron Teams Room devices are handled separately and **excluded** from the normal Intune policies applied to end-user laptops/desktops [2]. Treat Teams Rooms as special-purpose **appliance** devices, not typical user workstations [3]. In practice, this means we will **not** assign standard Windows configuration baselines or user-targeted policies to them – applying regular end-user policies *"will break things"* on an MTR [4]. For example, **password policies** or login requirements must be avoided, since **Teams Rooms auto-sign-in with a passwordless local "Skype" account** [5]. (Microsoft explicitly notes that enforcing password policies can prevent the Skype account from signing in automatically [6].) By isolating these devices in their own Intune group and filtering them out of general profiles, we prevent any base policy from unintentionally removing the Teams app or altering the device's specialized setup.

2. **Use a Bulk Enrollment Method (or Script) to Intune-Enroll without Disrupting Autologin:** To onboard the existing standalone (workgroup) Teams Rooms into Intune, we will use a **scripted or bulk enrollment** approach rather than interactive user enrollment. Microsoft's recommended method is creating a **provisioning package** via Windows Configuration Designer for bulk Azure AD join and Intune enrollment [7], which can be applied to each device (this avoids manually logging in with a user account on the device). This approach preserves the device's auto-login configuration. If a provisioning package is not feasible, an alternative is a PowerShell-driven enrollment using a **Device Enrollment Manager (DEM) account** or the room's resource account credentials. For example, we can run a PowerShell script (locally or via RMM) that calls the MDM enrollment API with the Intune enrollment URL and credentials (as documented in community guides). The key is to **enroll the device in Intune (and Azure AD join it)** without permanently switching the console's login to an admin user. We will ensure any tech doing this uses the local Admin account (default password "sfb") when needed and then returns the device to the Skype user session. *This prevents breaking the automatic Skype user login.* (In other words, we won't join

with a normal user account in the UI, since that can disable the autologon and leave the device stuck at a Windows login screen – a known issue if enrollment is done incorrectly.)

3. **Apply a Limited Intune Configuration Baseline Tailored for Teams Rooms:** Once enrolled, each Teams Room will receive a minimal set of Intune configuration profiles designed **not** to interfere with Teams functionality. We will **avoid overly restrictive device configuration profiles** – for instance, we will **not apply** any blanket "Device Restrictions" template or Endpoint Security profile that isn't explicitly verified for MTR use [8] [9]. (Microsoft's Intune team advises that many settings like custom Shell, multi-user kiosk, etc., are **unsupported** on Teams Rooms [10].) Instead, we will focus on a few safe, **supported** configurations:

4. **BitLocker Drive Encryption:** Enable BitLocker on the MTR local drive to protect data at rest [11]. Teams Rooms meet the hardware requirements (TPM 2.0, UEFI) for BitLocker, so we will deploy an **Endpoint Protection** profile turning on BitLocker with AES encryption and store recovery keys in Azure AD/Intune [12] [13]. This will secure the devices without affecting the Teams application. BitLocker can be enforced as a compliance requirement too (only after enabling it) [14] [6].
5. **Windows Defender and Firewall:** Ensure Microsoft Defender Antivirus and the firewall are active (these are enabled by default on Teams Rooms and are actually required by Microsoft) [15]. We will verify via Intune compliance policy that **Defender AV is running and up-to-date, firewall enabled**, etc., which aligns with Teams Rooms security baselines (these settings are usually already on by default in the OEM image) [15]. No third-party AV will be installed to avoid conflicts [16].

6. **Critical Security Updates Only:** Avoid configuring features that are not meant for Teams Rooms (for example, **no** screensaver or lock timeout policy – we want the room display to show meeting info continually). We also won't use Intune's **"Shared PC" mode** or **Kiosk mode** profiles on these devices [10] because Teams Rooms already runs its own kiosk shell. In summary, our configuration baseline will be as lightweight as possible: only what's needed for security and management, and nothing that would modify the user experience of the Teams app.

7. **Implement Windows Update Management with a Maintenance Window:** We will create a custom **Windows Update Ring** in Intune specifically for the Teams Rooms group to control OS updates without disrupting meetings. This policy will use the **Semi-Annual Channel** for stability [17]. We'll configure **automatic installation and reboot** to occur during an overnight maintenance window – e.g. set active hours from 7 AM to 7 PM (so updates install outside of 7AM-7PM) with automatic install and restart allowed at, say, 3 AM [18]. In our test profile (named "MTR_Updates"), we plan to **set deferral periods to 0** days (no delay) so that quality updates apply as soon as possible, but only during the scheduled time [17]. Feature updates for Windows will be pinned to a supported version – for example, if the devices are on Windows 10 21H2, we might freeze feature updates at 21H2 using Intune **Feature Update** policy [19]. This ensures the OS doesn't jump to a new version that hasn't been validated for Teams Rooms (preventing an incompatibility) [20]. We will also enable **Quality Update** policies to enforce important hotfixes and allow a quick grace period (e.g. auto-restart within 1 day of install) [21]. Intune will be set to *Allow* driver updates to be downloaded for these devices [22], but by default Intune will place device firmware updates as **optional** – we will review those in Intune before approving, since a bad firmware auto-install could potentially brick a device [23] [24]. (Drivers that the OEM publishes to Windows Update will appear in the device's Optional Updates; we'll apply them during maintenance windows after testing.) **Crucially, we will not block the Microsoft Store** on these devices, because the Teams Rooms app itself updates via the Store mechanism. (The Teams Rooms app updates are delivered through Microsoft Store for Business by default [25], so

if we had any Intune policy disabling the Store or removing UWP apps, we must remove that for MTRs. Our Intune baseline will leave the Store enabled to allow Teams client auto-updates.)

8. **Enable Windows LAPS for Local Admin Password Management:** To improve security and meet compliance, we will deploy the new **Windows LAPS** (Local Administrator Password Solution) via Intune on all Teams Rooms. Each MTR device has a local Administrator account (often the username is "Admin" with a default password "sfb"). We will use Intune's *Endpoint Security* > *Account Protection* policy for **Windows LAPS** [26]. In that profile, we'll configure LAPS to **manage the built-in Admin account's password**, rotating it on a schedule and storing the encrypted password in Intune/Azure AD [27]. We will target this policy to our MTR device group [28]. This way, even though all these devices started with the same default admin password, Intune will periodically set each one to a unique random password that we can retrieve securely from the Intune portal [29]. This addresses the goal of implementing LAPS for the conference room PCs. After enabling LAPS, we'll validate on a test device that the password rotates and can be read by an authorized admin in Intune (under **Devices > [Device] > Local admin password**) [30]. This policy greatly reduces the risk of someone using the default "sfb" password to compromise a device, without affecting the operation of the Teams app (the Skype user account is separate and unaffected by LAPS).

9. **Manage Bluetooth Settings without Breaking Proximity Features:** We will use Intune to ensure Bluetooth is handled in a way that suits our meeting room needs. Many Teams Rooms rely on Bluetooth Low Energy beacons for the **Proximity Join** and **Casting** features (allowing users to detect the room system from their phone or laptop) [31] [32]. Therefore, we **must not disable the Bluetooth radio** via policy if we want those features to work. Our plan is to **allow Bluetooth** on these devices and even enforce that the Bluetooth radio is on during meeting hours. By default, the Teams Room app has a setting to enable Bluetooth beaconing – we will verify it's enabled in the Teams admin settings (on the device). In Intune, we will not apply any device restriction that globally turns off Bluetooth or prevents user from toggling it. If anything, we might use a Settings Catalog policy to *enable* Bluetooth connectivity if it's ever turned off. (If security policy in some conference rooms requires no Bluetooth, we would disable Proximity Join accordingly – but given the request to manage Bluetooth, we assume we want it on.) Additionally, we'll monitor Intune's device compliance or configuration reports to ensure no other policy inadvertently blocks Bluetooth. If we encounter any Intune compliance setting related to Bluetooth (e.g. "Bluetooth allowed" setting in Device Restrictions), we will set it to **Allowed** for these Teams Rooms. In summary, Bluetooth will be left **enabled** and managed to support meeting functionality.

10. **Ensure Accurate Time Configuration on Devices:** Maintaining correct system time is important for scheduling meetings and joining conferences. All Teams Rooms will be configured to sync time automatically. Since they are Azure AD joined (not on-prem domain), they will use Windows' internet time sync by default. We will double-check that the Windows Time service is running and can reach time servers. If needed, we can enforce time settings via Intune. For example, Intune's **Settings Catalog** has a *Time and Language* section where we can set a specific time zone or enable automatic time zone adjustment [33] [34]. Our plan is to use a configuration profile to ensure each device is in the correct **time zone** (particularly if our organization spans multiple regions). We can either set the time zone explicitly for each group of devices (e.g. "GMT Standard Time" for London offices, "Pacific Standard Time" for West Coast, etc.) [35], or allow "Set time zone automatically" if the devices have location services enabled. Enabling *automatic time zone* would require also allowing location services on the device [36]. In a controlled meeting room environment, it might be easier to just statically set the known time zone for each room via Intune policy. We will also ensure the option "Set time automatically" is on (so the clock syncs

with internet NTP servers). In testing, we'll verify that after enrollment the device's clock is correct and stays accurate. If any issues arise (for example, if the device is offline and can't sync), we might use a PowerShell script deployed via Intune to set a reliable NTP server or correct time. Overall, time will be centrally managed so all rooms show the correct meeting times.

11. **Preserve Teams Rooms Application and Configurations:** Finally, we will double-check that none of our Intune policies remove or conflict with the core Teams Rooms software. The Intune configurations chosen above align with Microsoft's supported policies for Teams Rooms, so we expect no interference with the Teams app. We will **avoid any Intune app removal or app deployment policy** that might uninstall the "Microsoft Teams Rooms" app (which is a UWP app packaged as `Microsoft.SkypeRoomSystem_8wekyb3d8bbwe`). In our initial test, a base policy accidentally removed the Teams app – to prevent that, we are not including any such "uninstall" actions in the new baseline. We also ensure the **Microsoft Store remains enabled** for these devices because the Teams Rooms app uses the store to get updates [25]. Additionally, we won't push software that isn't supported on MTR; Microsoft advises against installing additional software on Teams Rooms beyond what's provided [37]. No Office apps, no user productivity apps – these devices will be kept as dedicated meeting appliances. We also heed Microsoft's guidance to **leave the default Skype user account untouched** (we won't set any policy to rename it, add a password, or change its group membership) [5]. This local account must stay as is for the automatic login to the MTR app to work. In summary, our Intune management will improve security and compliance (updates, encryption, password management) **without altering the Teams meeting functionality or the underlying appliance configuration**. We will thoroughly test these policies on a pilot room system before rolling out to all 50-60 devices to ensure that Teams still launches and operates normally (e.g. the devices sign into their room accounts and can join meetings). Once confirmed, we'll have all our Teams Room devices enrolled in Intune, managed in a safe manner that meets our goals (controlling time settings, Bluetooth, updates, and local admin passwords) **without breaking any Teams or Crestron functionality**.

Sources: The plan above is based on Microsoft's best practice recommendations for managing Teams Rooms via Intune and real-world case studies. Microsoft documentation emphasizes treating Teams Rooms as specialized devices and excluding them from standard user device policies [4] [3]. The Intune Support Team's guidance on enrolling Teams Rooms was followed for choosing an appropriate enrollment method [7]. We also incorporated advice from community experts on which Intune configuration profiles are supported or recommended for Teams Rooms (e.g. enabling BitLocker, avoiding unsupported settings) [9] [11]. The importance of not disabling the Teams app or its updates was noted in an Intune deployment blog [25]. Additionally, Microsoft's Teams Rooms documentation and tech community posts highlight that password or lock policies can interfere with the room system's auto-login mechanism [6] – hence we have avoided those. By adhering to these sources and lessons learned from our initial test (which inadvertently removed Teams), this plan ensures we manage the devices in Intune's modern framework while keeping the meeting rooms running smoothly [2] [31]. The combination of Intune's device grouping, targeted profiles, and careful policy selection achieves our goal of full management (updates, security, settings) with zero impact on the critical Teams Rooms functionality. [4] [27]

---

[1] [26] [27] [28] [29] [30] How to enable LAPS on the MTR Admin account via Intune
https://maxime.hiez.ca/en/blog/2025-02-17-intune-how-to-enable-laps-mtr

[2] MTR on Windows received policies - how to remove? - Microsoft Q&A
https://learn.microsoft.com/en-us/answers/questions/1616010/mtr-on-windows-received-policies-how-to-remove

3 5 16 37 Microsoft Teams Rooms on Windows and Teams Android device security - Microsoft Teams | Microsoft Learn
https://learn.microsoft.com/en-us/microsoftteams/rooms/security

4 8 9 10 11 12 13 Managing a Microsoft Teams Room (MTR) Device with Intune – Part 3 – Configuration Profiles – Blog – Chiffers.com
https://blog.chiffers.com/managing-a-microsoft-teams-room-mtr-device-with-intune-part-3-configuration-profiles/

6 14 15 20 Supported Conditional Access and Intune device compliance policies for Microsoft Teams Rooms - Microsoft Teams | Microsoft Learn
https://learn.microsoft.com/en-us/microsoftteams/rooms/supported-ca-and-compliance-policies

7 Enrolling Microsoft Teams Rooms on Windows devices with Microsoft Endpoint Manager | Microsoft Community Hub
https://techcommunity.microsoft.com/blog/intunecustomersuccess/enrolling-microsoft-teams-rooms-on-windows-devices-with-microsoft-endpoint-manag/3246986

17 18 19 21 22 23 24 25 Managing a Microsoft Teams Room (MTR) Device with Intune – Part 2 – Updates – Blog – Chiffers.com
https://blog.chiffers.com/managing-a-microsoft-teams-room-mtr-device-with-intune-part-2-updates/

31 32 5 Tips on getting Teams Room Proximity Join and Casting to work - UCPrimer
https://www.ucprimer.com/ucprimer/5-tips-on-getting-teams-room-proximity-join-and-casting-to-work

33 34 35 View Blog
https://www.mdmandgpanswers.com/blogs/view-blog/how-to-set-time-zones-using-intune

36 Set time zone to automatic in Intune - Microsoft Q&A
https://learn.microsoft.com/en-us/answers/questions/2085344/set-time-zone-to-automatic-in-intune