Daily Task (15-09-2025)

Part 1: Microsoft Intune Licensing and MDM

1. How Intune License Assignment Works if Applied Multiple Times

Applying an Intune license to a user multiple times (e.g., assigning it directly and also via a group membership) does not cause conflicts. The system is designed to be additive and idempotent.

- **Additive Nature:** A user's total service access is the sum of all licenses assigned to them. If Group A grants them "Office 365 E3" and Group B grants "Enterprise Mobility + Security E5" (which includes Intune), the user gets the services from both licenses.
- **Single Service, Multiple Licenses:** If a user is assigned a license that includes Intune both directly and through a group, the end result is simply that the user has one Intune license. The system recognizes the user is licensed for the service and doesn't assign it "twice." It simply ensures the entitlement is active.
- **Benefit:** This prevents accidental removal of a license. If you remove the user from a licensed group, but they still have a direct license assignment, they will retain access to Intune, preventing their devices from being unenrolled.

2. MDM User Scope Rules and Timing

The MDM (Mobile Device Management) user scope in Azure Active Directory determines which users are allowed to enroll their devices into Intune.

- **Rules:**
    - **None:** No users can enroll devices in Intune. This is effectively the "off" switch.
    - **Some:** Only users who are members of a specific Azure AD group that you select can enroll devices. This is the most common and recommended approach for phased rollouts.
    - **All:** All users (excluding guest users) in your Azure AD tenant are permitted to enroll their devices.
- **Timing:**
    - Changes to the MDM user scope are generally effective **within a few minutes**.
    - However, in large tenants or during periods of high load on Azure services, it can sometimes take **up to an hour** for the change to be fully propagated and effective for all users.
    - It is not instantaneous, so if a user tries to enroll immediately after being added to the scope group, it might fail. It's best to wait a short while.

3. How MDM Works in Intune

MDM in Intune is a framework for managing and securing mobile devices (laptops, phones, tablets). It works by establishing a trusted communication channel between the device and the Intune service.

1. **Enrollment:** A user enrolls their device. This process installs a management profile or registers the device with Intune. During enrollment, the device receives a certificate to securely communicate with the Intune service.
2. **Policy Delivery:** Once enrolled, Intune pushes "policies" to the device. These policies are rules you configure in the Intune admin center. Examples include:
    a. **Configuration Policies:** Set up Wi-Fi, VPN, or email profiles automatically.
    b. **Compliance Policies:** Enforce security requirements, like requiring a PIN/password, device encryption, or a minimum OS version.
    c. **Security Policies:** Configure Microsoft Defender for Endpoint, firewalls, and other security settings.
3. **Device Check-in:** The device periodically "checks in" with the Intune service to report its status (is it compliant?) and receive any new or updated policies. This check-in happens roughly every 8 hours, though it can be triggered manually.
4. **Enforcement:** If a device is found to be non-compliant (e.g., the user removes their PIN), Intune can take action. This can range from sending the user a notification to blocking their access to company resources like email (using Conditional Access) until the device is compliant again.

4. Troubleshooting Intune Users Not Showing After License Assignment

This is a common issue, usually related to synchronization delays.

- **Azure AD to Intune Sync:** Intune is a service that relies on Azure Active Directory (Azure AD). When you assign a license in Azure AD (or the Microsoft 365 admin center), it can take some time for that user's information to fully sync to the Intune service. This delay can be anywhere from **a few minutes to over an hour**.
- **Search Propagation:** Even after the user is in Intune, it can take additional time for them to appear in all search indexes across the portal.
- **Troubleshooting Steps:**
    - **Wait:** The first step is always to wait for at least 30-60 minutes.
    - **Verify License in Azure AD:** Go to Azure AD -> Users -> Select the user -> Licenses. Confirm that the Intune license is listed and in an "Active" state.
    - **Check Service Health:** Look at the Microsoft 365 Service Health dashboard to see if there are any ongoing issues with Intune or Azure AD.
    - **Use a Direct Link:** Try to access the user in Intune directly via a URL, if possible, rather than searching.
    - **Sign Out and Sign In:** Sign out of the Intune portal and sign back in to force a refresh of your session data.

5. How to Manually Assign Intune Licenses (Step by Step)

1. Log in to the **Microsoft Endpoint Manager admin center** (endpoint.microsoft.com) or the **Azure portal** (portal.azure.com). The steps below are for Azure AD.
2. Navigate to **Azure Active Directory**.
3. In the left-hand menu, click on **Users**.
4. Find and click on the user you want to assign the license to.
5. In the user's profile menu on the left, click on **Licenses**.
6. Click the **+ Assignments** button at the top.
7. A list of available licenses will appear. Find the license that includes Intune (e.g., "Enterprise Mobility + Security E3", "Microsoft 365 E5").
8. **Check the box** next to the desired license.
9. *(Optional but Recommended)* You can click on "Review license options" to turn specific services within that license on or off. Ensure "Microsoft Intune" is turned on.
10. Click the **Save** button at the bottom of the screen. The license is now assigned.

Part 2: Wi-Fi MAC Address Filtering

1. How to Block Phones from Wi-Fi Using Router MAC Filter

A MAC (Media Access Control) filter is a security feature on a router that allows you to create a list of devices that are either allowed or blocked from connecting to your network.

1. **Log in to Your Router:** Open a web browser and enter your router's IP address (commonly `192.168.1.1` or `192.168.0.1`). Log in with the administrator username and password.
2. **Find MAC Filtering Settings:** Look for a section named "MAC Filtering," "Access Control," "Network Filter," or similar, often under "Wireless" or "Security" settings.
3. **Enable the Feature:** Turn on the MAC filtering feature.
4. **Choose the Mode:**
    a. **Allow (Whitelist):** Only devices on your list can connect. This is more secure.
    b. **Block (Blacklist):** All devices can connect *except* for the ones on your list. This is what you would use to block specific phones.
5. **Add the Phone's MAC Address:** Find the MAC address of the phone you want to block (see instructions below) and add it to the blacklist. You will need to give it a name (e.g., "John's Phone") and enter the MAC address (e.g., `AA:BB:CC:11:22:33`).
6. **Save and Apply:** Save your settings. The router may need to reboot.

2. Why Blocked Phones Still Connect (Private/Random MAC Issue)

MAC filtering is an **outdated and unreliable security method** precisely because of MAC randomization, a privacy feature now standard on modern smartphones.

- **What it is:** To prevent tracking of your location across different Wi-Fi networks, both iOS and Android generate a **new, random MAC address** each time they connect to a new Wi-Fi network.
- **How it Defeats MAC Filtering:** When you block a phone's "real" hardware MAC address, the phone can simply generate a new, randomized MAC address the next time it connects. Your router sees this new MAC address as a completely different device, and since it's not on your block list, it allows the connection. The user can simply "forget" the network and reconnect to get a new MAC address and bypass the filter again.

3. How to Find the Real MAC Address and Disable Private MAC

To make MAC filtering work at all, you **must disable** this privacy feature on the target device.

For iPhone/iOS:

- **Find Real MAC Address:**
  - Go to **Settings** > **General** > **About**.
  - Scroll down to find "Wi-Fi Address." This is the device's true, permanent hardware MAC address.
- **Disable Private Wi-Fi Address (for a specific network):**
  - Go to **Settings** > **Wi-Fi**.
  - Tap the **"i" info icon** next to your Wi-Fi network name.
  - Toggle the **Private Wi-Fi Address** switch to **OFF**.
  - The phone will need to reconnect to the network, and it will now use its real MAC address.

For Android (steps can vary slightly by manufacturer):

- **Find Real MAC Address:**
  - Go to **Settings** > **About Phone** > **Status** (or similar path).
  - Look for "Wi-Fi MAC address." This is the device's permanent MAC address.
- **Disable Randomized MAC (for a specific network):**
  - Go to **Settings** > **Network & internet** > **Wi-Fi**.
  - Tap the **gear icon** or settings option next to your connected Wi-Fi network.
  - Tap on **Privacy** or **Advanced**.
  - You will see an option for "MAC address type." Change it from "Use randomized MAC (default)" to **"Use device MAC."**
  - The phone will reconnect using its real MAC address.

Part 3: UniFi Device Management

1. How to Reset a UniFi Device

This applies to devices like Access Points, Switches, and Security Gateways.

1. **Ensure the Device is Powered On.**
2. **Locate the Reset Button:** This is a small, recessed pinhole button on the device.
3. **Use a Paperclip:** Press and **hold the reset button for 10-15 seconds.**
4. **Observe the LED:** The device's LED light will flash and then change state (e.g., go from solid blue to blinking white).
5. **Release the Button:** Once the LED changes, release the button. The device will reboot to its factory default settings and will show up in your UniFi Network Controller as "Pending Adoption."

2. How to Reset a UniFi Password

For a modern UniFi OS Console (like a UDM Pro, UDM, or Cloud Key Gen2+), **resetting the password requires a full factory reset of the console.** There is no "Forgot Password" recovery option for security reasons.

The process is the same as the one above, but you perform it on the console itself:

1. **Ensure the Console is Powered On.**
2. **Locate the Reset Button:** Find the reset pinhole on the device.
3. **Press and Hold for 10+ Seconds:** Use a paperclip to press and hold the button.
4. **Observe Confirmation:** The device's front panel (if it has one, like the UDM Pro) will indicate it is resetting.
5. **Release and Wait:** Release the button and allow the console to reboot. This can take 5-10 minutes. It is now in a factory default state, ready for setup.

3. How to Use Common/Default Password in UniFi Devices

UniFi devices fresh out of the box or after a factory reset have default credentials.

- **Username:** `ubnt`
- **Password:** `ubnt`

Important: These credentials are ONLY used for two things:

1. Informing a UniFi Controller during the adoption process.
2. Directly SSHing into a device that is in a "factory default" state before it has been adopted. Once a device is adopted by a UniFi Network Controller, its credentials are automatically

changed to a complex, unique value managed by the controller, and the `ubnt/ubnt` login no longer works.

4. How UniFi OS Devices Create a New Admin Account After Factory Reset (Detailed)

After you factory reset a UniFi OS Console (like a UDM Pro), it erases everything and starts the initial setup wizard. This wizard is where you create the new owner account.

1. **Initial Connection:** After the reset, you connect to the console either:
    a. **Via Web Browser:** By plugging a computer into a LAN port and navigating to `192.168.1.1`.
    b. **Via Mobile App:** By using the UniFi Network app, which will discover the new console via Bluetooth.
2. **Start the Setup Wizard:** The wizard begins, asking you to name the console and configure its internet connection.
3. **The Administrator Account Screen:** You will reach a critical screen for setting up the owner account. Here, you are presented with two paths:
    a. Path A: Cloud-Connected Account (Default and Recommended)
        i. The wizard prompts you to **Sign In with your Ubiquiti (UI.com) Account**.
        ii. You enter your UI.com email and password.
        iii. The wizard then uses these cloud credentials to create the **Owner account** on the UDM Pro.
        iv. From this point on, your `ui.com` email and password are the new administrator credentials for this console. This automatically enables remote access via `unifi.ui.com`.
    b. Path B: Local-Only Administrator Account (Advanced)
        i. On the same screen that asks for your UI.com login, you must look for an option to bypass it. This is usually a small link labeled **"Advanced Setup"** or a checkbox to **"Disable Remote Access."**
        ii. When you select this, the UI.com login prompt is replaced with a form to create a **local account**.
        iii. You are required to enter a new **Username**, a new **Password**, and confirm the password.
        iv. This creates an administrator account that exists only on the UDM Pro itself. These new credentials are what you will use to log in locally. Remote access will be disabled by default.
4. **Finalization:** After the administrator account is created (via either path), the wizard finalizes the configuration, sets up a default Wi-Fi network, and reboots. Once it's back online, you can log in with the new credentials you just created.