25-09-2025 Advanced Wi-Fi Security and User Control on the UDM Pro

1. How to Automatically Change the Wi-Fi Password Daily on a UDM Pro

The UDM Pro does not have a built-in graphical interface for scheduling automatic password changes. This functionality must be achieved using a custom script that interacts with the UniFi Controller's API.

- **Core Concept:** A script running on a separate computer (like a Raspberry Pi or any always-on PC) will automatically perform the steps you would manually: generate a new password and tell the UDM Pro to apply it to a specific Wi-Fi network.
- **Requirements:**
    - **A Host Machine:** A device that is always on and connected to the same network as your UDM Pro to run the script.
    - **A Script:** This is typically written in Python or as a shell script. Many community-developed examples are available on platforms like GitHub.
    - **A Scheduler:** A tool to run the script automatically every day. On Linux, this is a `cron` job. On Windows, it's the Task Scheduler.
- **Step-by-Step Process:**
    - **Create a Limited Admin Account:** On your UDM Pro, create a new local user with limited permissions (e.g., Hotspot Operator or a custom role) that the script can use to log in. This is more secure than using your main administrator account.
    - **Write or Adapt the Script:** The script needs to perform these functions:
        - Generate a new random password.
        - Authenticate with the UniFi Controller using the limited user's credentials.
        - Send an API command to modify the password (`wpa_pass`) of the target Wi-Fi network (SSID).
    - **Schedule the Script:** Set up a `cron` job or a Windows Scheduled Task to execute your script at a specific time every day (e.g., at 3:00 AM).

2. How to Create a Guest Wi-Fi User on a UDM Pro

Creating a guest network is a core feature of the UniFi platform, designed to give visitors internet access without exposing your main network.

- **Step 1: Create a Separate Guest Network:**

    - In the UniFi Controller, go to **Settings > Networks > Create New Network**.
    - Name it (e.g., "Guest LAN") and set its purpose to **"Guest Network"**. This automatically applies client isolation rules, preventing guest devices from seeing each other or your private devices.
- **Step 2: Create the Guest Wi-Fi SSID:**
    - Go to **Settings > WiFi > Create New WiFi Network**.
    - Give it a name (e.g., "MyBusiness Guest") and a password.
    - **Crucially**, under the **"Network"** dropdown, assign this Wi-Fi to the "Guest LAN" you created in Step 1.
- **Step 3: (Optional) Configure the Guest Portal:**
    - To create a splash page where users must agree to terms, enter a password, or use a voucher, go to **Settings > Profiles > Guest Hotspot**.
    - Enable the **"Hotspot Portal"** and choose an **Authentication method**:
        - **Password:** A single password for all guests on the portal.
        - **Vouchers:** Generate unique, time-limited codes for users. You can print these from the **Hotspot Manager**.
        - **Free Trial:** Allow access for a limited time after clicking a button.
    - Apply this Hotspot Profile to your Guest Wi-Fi under its advanced settings.

3. How to Block All Devices and Allow Only Specific Users on a UDM Pro Wi-Fi Network

The most secure and professional method to achieve this is by using WPA2/WPA3-Enterprise security, which requires each user to have a unique username and password.

- **Method: WPA2-Enterprise with a RADIUS Server**
    - **Enable the RADIUS Server:** Go to **Settings > Security > RADIUS > Server**. Toggle it **On** and set a strong "Secret" (this is for the system, not users).
    - **Create Users:** In the **Users** tab of the RADIUS settings, click **"Create New User"**. Create a unique username and password for every single device or person you want to allow.
    - **Create the Wi-Fi Network:**
        - Go to **Settings > WiFi > Create New WiFi Network**.
        - Under **Security**, select **"WPA2 Enterprise"** or **"WPA3 Enterprise"**.
        - The **RADIUS Profile** should be set to **"Default"**.

    - **Result:** Now, only a device that connects using one of the exact username/password combinations you created in the RADIUS server will be allowed on this network. All others are blocked by default.

4. Clarification on How the RADIUS Server Works for Blocking Devices

Enabling the RADIUS server itself does not block anyone. It's an authentication service that is dormant until a Wi-Fi network is told to use it.

- **Default State:** Your standard Wi-Fi network uses WPA2-Personal security, which checks if a device provided the one correct "pre-shared key" (your Wi-Fi password).
- **RADIUS-Enabled State:** A Wi-Fi network set to "WPA2-Enterprise" does not have a single password. When a device tries to connect, the UDM Pro forwards the device's username and password attempt to the RADIUS server.
- **The "Block":** The RADIUS server checks its list of users.
    - If the credentials match a user on the list, it sends an "Accept" message, and the device is allowed on the network.
    - If the credentials do not match any user, it sends a "Reject" message, and the device is denied access.
- Therefore, it acts as a "default-deny" bouncer for that specific network; you are blocked unless your name is on the list.

5. How to Enable BitLocker Encryption on Windows 11 Home

Windows 11 Home does not include the full "BitLocker" feature but has a nearly identical, more streamlined version called **"Device Encryption."**

- **Prerequisites:** Your device must have modern security hardware, specifically a **TPM 2.0 (Trusted Platform Module)** chip and **Secure Boot** enabled in the BIOS/UEFI. Most modern PCs that ship with Windows 11 meet these requirements.
- **Steps to Enable:**
    - First, check if your system supports it. Search for "System Information" in the Start Menu. Scroll to the bottom and find **"Device Encryption Support"**. It must say **"Meets prerequisites"**.
    - If it is supported, go to **Settings > Privacy & security > Device encryption**.
    - If it's off, you will see a toggle switch to turn it **On**.

- **CRITICAL STEP - Recovery Key:** Device Encryption automatically backs up its recovery key to the Microsoft account you used to sign in to Windows. You **must** verify this key is there in case you are ever locked out.
    - Log in to https://account.microsoft.com/devices/recoverykey to view and save your key. Store a copy in a safe place separate from the laptop.

6. How to Find the Permanent MAC Address on a Mobile Phone

Modern phones use MAC Randomization for privacy, showing a temporary MAC address to Wi-Fi networks. The permanent hardware address is found deep within the phone's general settings.

- **On Android:**
    - Go to **Settings > About phone**.
    - Tap on **Status** or **Status information**.
    - Look for **"Device Wi-Fi MAC address"**. This is the permanent address.
- **On iOS (iPhone):**
    - Go to **Settings > General**.
    - Tap on **About**.
    - Scroll down to find **"Wi-Fi Address"**. This is the permanent address.

7. How to Find the Exact Permanent MAC Address When It Changes Between Networks

The reason it changes is due to MAC Randomization. The method to find the permanent address is the same as above. However, if you want your phone to *use* its permanent address on a trusted network (like your home Wi-Fi), you must disable this feature on a per-network basis.

- **On Android:**
    - Connect to your Wi-Fi network.
    - Go to the network's settings (usually a gear icon next to the name).
    - Tap **Advanced** or **Privacy**.
    - Change "MAC address type" from "Randomized MAC" to **"Use phone MAC"**.
- **On iOS (iPhone):**
    - Connect to your Wi-Fi network.
    - Tap the **"i" icon** next to the network name.

- Turn the toggle for **"Private Wi-Fi Address" OFF**.

8. How to Recover Files After Deleting Them from a Laptop

Your chances of recovery depend on how the files were deleted and how quickly you act.

1. **Stop Using the Drive Immediately:** This prevents the deleted files' space from being overwritten by new data.
2. **Check the Recycle Bin:** The first and easiest place. If files are there, right-click and "Restore."
3. **Use Windows Backups:**
    a. **File History:** If you had it set up with an external drive, you can restore files from that backup.
    b. **Previous Versions:** Right-click the folder where the files were located, go to **Properties > Previous Versions**, and see if a version of the folder exists from before the deletion.
4. **Use Data Recovery Software:** If the above fails, use a dedicated program. **Important:** Install the program and save the recovered files to a *different* drive (e.g., an external USB drive).
5. **Contact Professional Data Recovery Services:** This is the expensive last resort for critically important data or physically damaged drives.

9. Suggestions for the Best Free Software for File Recovery

- **Best for Beginners: Recuva**
    - **Why:** It has a very simple wizard to guide you through recovery. It's effective for common situations like accidentally emptied Recycle Bins or deleted photos from a memory card.
    - **Features:** Standard and deep scan modes, portable version (can run from a USB stick without installation).
- **Most Powerful Free Option: PhotoRec & TestDisk**
    - **Why:** These are two utilities bundled together that can recover data from severely corrupted or formatted drives. PhotoRec is a file recovery beast, while TestDisk can recover entire lost partitions.
    - **Caveat:** It has no graphical interface and runs in a command-line window, making it challenging for non-technical users.
- **Best Interface (with limits): EaseUS Data Recovery Wizard Free**

- **Why:** It offers the power and clean interface of a premium product. It's great for quickly seeing if your files are recoverable.
- **Limitation:** The free version has a strict data cap (typically 2GB). It's perfect for a few essential documents but not for large-scale recovery.