UDM Pro Network Expansion & Integration

Introduction

This guide covers the essential steps for expanding your network using a UniFi Dream Machine Pro (UDM Pro) and securing a Hikvision IP camera. We will detail how to add new Wi-Fi networks (SSIDs) and properly integrate a non-UniFi router to work as a seamless extension of your network, avoiding common conflicts.

Topic 1: How to Add a New Wi-Fi Network (SSID) in UDM Pro

Creating multiple SSIDs on your UDM Pro is ideal for segmenting your network for security and organization (e.g., creating separate Guest, IoT, or Work networks). The UDM Pro's controller pushes these settings to all connected UniFi Access Points.

Step-by-Step Guide to Creating an SSID:

1. **Access and Open UniFi Network:** Log into your UDM Pro and open the **Network** application.
2. **Navigate to WiFi Settings:** Click the **Settings** icon (gear) on the left menu, then select **WiFi**.
3. **Create New WiFi Network:** Click the "Create New" button.
4. **Configure Core Settings:**
    - **Name (SSID):** Enter the name you want your Wi-Fi network to broadcast.
    - **Password:** Set a strong password for the network.
    - **Network:** Assign this SSID to a specific network/VLAN. For a guest network, you must first create a new "Guest" network under `Settings > Networks` and then assign the SSID to it for proper isolation.
5. **Apply Changes:** Click "Add WiFi Network" to save. The UDM Pro will provision your access points with the new network.

Topic 2 & 3: Connecting the UDM Pro with an Additional Router and Using Them Together

You cannot manage a non-UniFi router's SSID from the UDM Pro. Instead, you must configure the second router to act as a simple Wi-Fi extender, a setup known as **Access Point (AP) Mode**.

The Core Principle: Avoiding "Double NAT"
Your UDM Pro must be the **only** device on your network acting as a router (managing traffic, assigning IPs via DHCP). If you connect a second router in its default "Router Mode," you create a **Double NAT** situation. This causes major issues, including:

- Devices on different routers being unable to communicate with each other.
- IP address conflicts and network instability.
- Poor performance for online gaming, video calls, and other services.
- Broken port forwarding.

The Correct Approach: Access Point (AP) Mode
By setting the second router to AP Mode, you disable its routing and DHCP functions. It becomes a simple bridge, converting the wired connection from the UDM Pro into a wireless signal. All devices, whether connected to the UDM Pro or the second router, will be on the same unified network, managed entirely by the UDM Pro.

Topic 4: How to Split Users Across Routers to Balance Internet Speed

This is achieved by **balancing the client load**, not by splitting internet bandwidth. The UDM Pro still manages all internet traffic. By strategically placing the second router (in AP Mode) in an area with weak Wi-Fi coverage, you provide a stronger connection point for devices in that area.

Benefits:

- **Reduces Congestion:** Prevents any single access point from becoming overloaded.
- **Improves Coverage:** Eliminates Wi-Fi dead zones.
- **Enhances Performance:** With fewer devices competing for airtime on each access point, every device gets a more stable and reliable connection.

Second Router Configuration & Hikvision Basics

Topic 5: Step-by-Step Configuration for Router 2 (in AP Mode)

Perform these steps **before** connecting the second router to your UDM Pro network.

1. **Isolate and Connect:** Factory reset the second router. Connect a computer directly to one of its **LAN ports** with an Ethernet cable.
2. **Log In to Admin Panel:** Open a web browser and enter the router's default IP address (e.g., `192.168.1.1`).
3. **Enable AP Mode (Easy Method):**
    - Look for an **"Operation Mode"** setting. If an **"Access Point (AP) Mode"** option exists, select it. The router will handle the configuration automatically.
4. **Manual Configuration (Universal Method):**
    - **Disable DHCP Server:** In the **LAN/Network settings**, find and **disable** the DHCP server. This is the most critical step.
    - **Set a Static IP Address:** Change the router's IP to one on the same network as your UDM Pro but *outside* its DHCP range.
        - *Example:* If your UDM Pro is `192.168.1.1` and its DHCP range is `192.168.1.100 - 192.168.1.200`, set this router's IP to `192.168.1.2`.
    - **Configure Wi-Fi:** Set up the SSID (Wi-Fi Name) and password.
5. **Save and Reboot:** Apply all changes.
6. **Connect to UDM Pro:** Run an Ethernet cable from a **LAN port** on your UDM Pro to a **LAN port** on the second router. **Never use the WAN/Internet port on the second router in this setup.**

Topic 6 & 7: Hikvision DS-2DE2A404IW Management & Reset Methods

Key Device Information:

- **Official Website:** Use the official Hikvision website for datasheets, manuals, and firmware.
- **Login Page:** Access by entering the camera's IP address (find with SADP tool, default is often `192.168.1.64`) into a web browser.
- **User Management:** Log in as `admin`, go to **Configuration > System > User Management** to add or remove users.
- **GUID File:** This is a password reset key. You must export it from the User Management menu *before* you forget your password and save it in a safe place.

Understanding Restore vs. Default on a Hikvision Device:
It is crucial to know the difference between the two options found under **Configuration > Maintenance**.

Feature	Simple Restore	Default (Factory Reset)
Effect	Resets device configurations (e.g., image, events) to default.	Wipes **all** settings, users, and logs.
What it KEEPS	**Keeps the IP address and all user accounts (usernames/passwords).**	**Nothing.** The device returns to an inactive, out-of-the-box state.
Use Case	Fix a configuration mistake without getting locked out.	Securely wipe the device for resale or recover from a lost password.

Advanced Hikvision Security & Unbinding

Topic 8: Troubleshooting Unauthorized Access to a Hikvision Device

If you have changed the `admin` password but still suspect unauthorized access, the issue is almost always one of three things, as the `admin` password only controls direct local access.

1. **Saved Credentials in Apps:**
    - **Problem:** Apps like Hik-Connect or iVMS-4200 have the *old password* saved and continue to use it.
    - **Solution:** Manually edit the device profile in **every app** on every phone and computer and update the password.
2. **ONVIF User Accounts:**
    - **Problem:** The camera can have separate ONVIF users (for third-party system integration) that are not visible in the main user list and may have a weak password.

- **Solution:** Go to **Configuration > Network > Advanced Settings > Integration Protocol**. Check for ONVIF users, disable the protocol if unused, or change the passwords for any existing users.

3. **Linked Hik-Connect Cloud Account:**
    - **Problem:** The device is linked to someone's Hik-Connect cloud account (likely the installer). This gives them remote access that completely bypasses the local admin password.
    - **Solution:** The device **must be unbound** from their account.

Topic 9 & 10: Step-by-Step Guide to Unbinding a Hikvision Device from Hik-Connect

This is the only way to revoke cloud-based remote access for a previous user. The method depends on your camera's firmware version.

Method 1: Unbinding via Web Interface (Older Firmware)

1. Log in to the camera's web interface and navigate to **Configuration > Network > Advanced Settings > Platform Access**.
2. Confirm the **Registration Status** is **"Online."**
3. If a button is visible, click **"Unbind"** or **"Unlink."**
4. Enter the `admin` password and the 6-character **Verification Code** from the camera's sticker to confirm. The status should now show as "Offline."

Method 2: Unbinding via the App (Modern Firmware - No "Unbind" Button)
On newer firmware, the "Unbind" button is removed for security. The action must be performed by the person whose account currently holds the device.

1. **Contact the Account Owner:** You must contact the person (e.g., the original installer) whose Hik-Connect account the device is linked to.
2. **Provide Them These Instructions:** Ask them to open their Hik-Connect app and follow these steps:
    - Select the device from their list.
    - Go to its **Settings** (usually a `...` or gear icon).
    - Scroll to the bottom and tap **"Delete Device."**
    - Confirm the deletion.
3. **What if the Owner is Unreachable?**
    - You must contact **Hikvision official support.**
    - Provide them with **proof of ownership** (a photo of the camera's serial number sticker).
    - They will manually unbind the device from the old account after verifying your ownership.