D-Link

Nuclias Unity User Manual

Version 1.00

2026 | Cloud Network Management

nuclias unity

Table of Contents

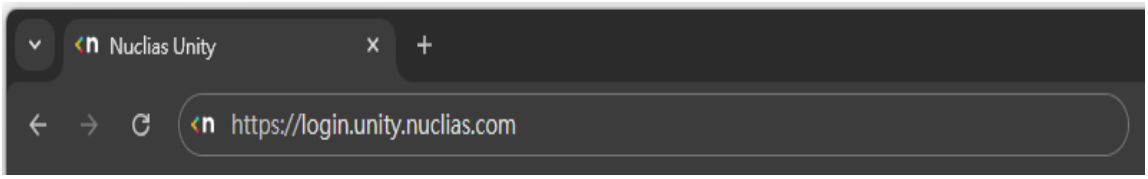
Introduction

Nuclias Unity is a centralized cloud network management platform designed to simplify the deployment, configuration, and monitoring of switches and access points across multiple sites.

This guide provides clear, step-by-step instructions to help you set up and manage your Nuclias Unity deployment. Whether installing a single device or multiple access points and switches, follow the procedures in order to ensure a smooth setup and reliable network operation.

Nuclias Unity is a cloud-managed platform accessible through Google Chrome or Microsoft Edge web browsers. Before accessing Nuclias Unity, ensure you have an active internet connection, then open your web browser and enter the required URL to begin.

Given URL: https://login.unity.nuclias.com/



Before you begin managing your network through Nuclias Unity, please complete the following two critical steps to ensure successful device adoption and management. All compatible devices must be running a firmware version that supports Nuclias Unity cloud management. Please check the D-Link support website for your specific device model and install the minimum required firmware version as indicated in the compatibility document.
Ensure your D-Link switches and access points are listed on the official Compatible Device List for Nuclias Unity. Refer to the PDF available at the link below:

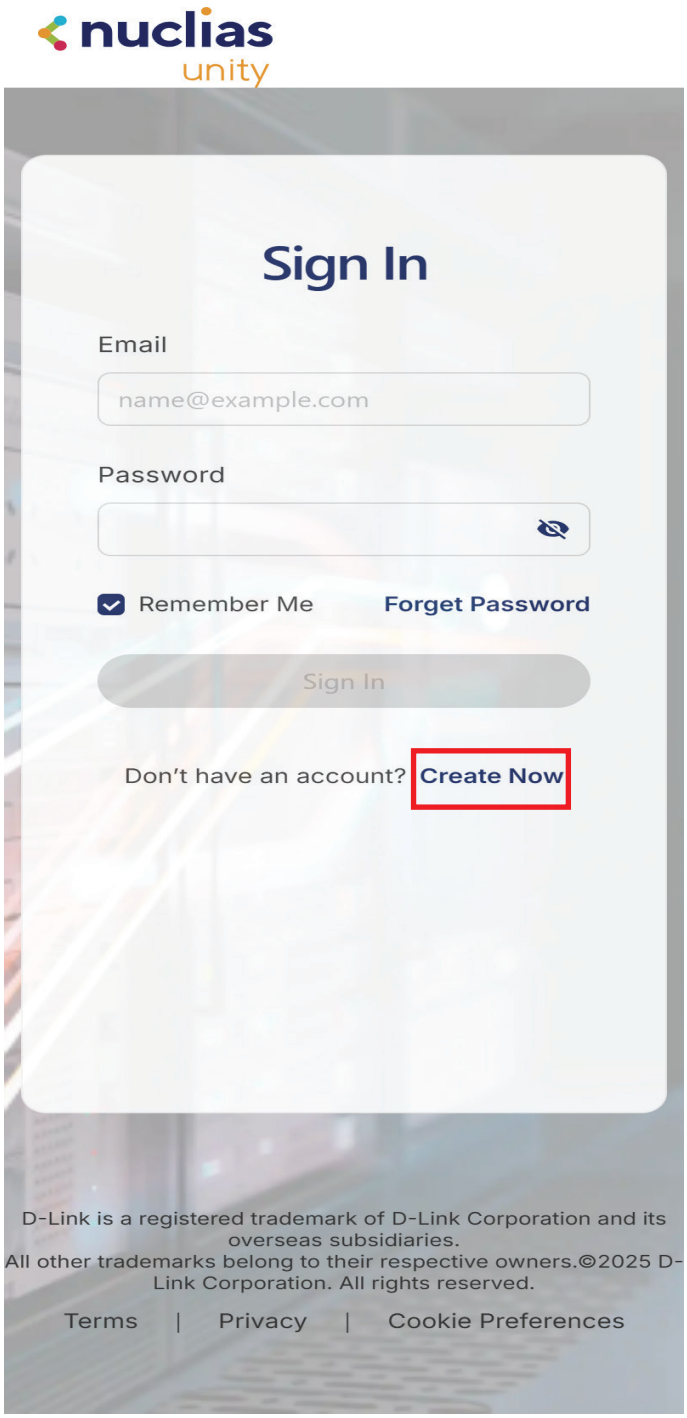
Given URL: https://www.dlink.com/tw/zh/-/media/product-pages/nuclias/nuclias-unity/compatible-products-for-nuclias-unity-solutionv16.pdf

Creating an Account

To access Nuclias Unity, you need a valid email address and password. Before signing in, you must first register your email address to activate your Nuclias Unity account.

Enter your email and password, then click Sign In to access Nuclias Unity.

You haven't registered your email account for Sign In. Please click '**Create Now**' to register your name and email address for Nuclias Unity.



Getting Started with Nuclias Unity Create Account

To create your Nuclias Unity account using the web browser, enter your Name and a valid Email address, as a six-digit verification code will be sent to it.
Create a strong password for the Organization, Site, and connected Devices. Make sure the password follows the rules listed below.

Password Rules (Important and Must Follow):

• Length: The password must be 8–30 characters long to ensure sufficient security.

Composition: Must contain ALL of the following:

• Must include at least one uppercase letter (A–Z), one lowercase letter (a–z), and one number (0–9).

• Allowed at least one Special Characters: ~ ! @ # $ ^ & * { } [ ] ( ) _ - + = . | : ; “ ‘ < , > / \

Security Restrictions:

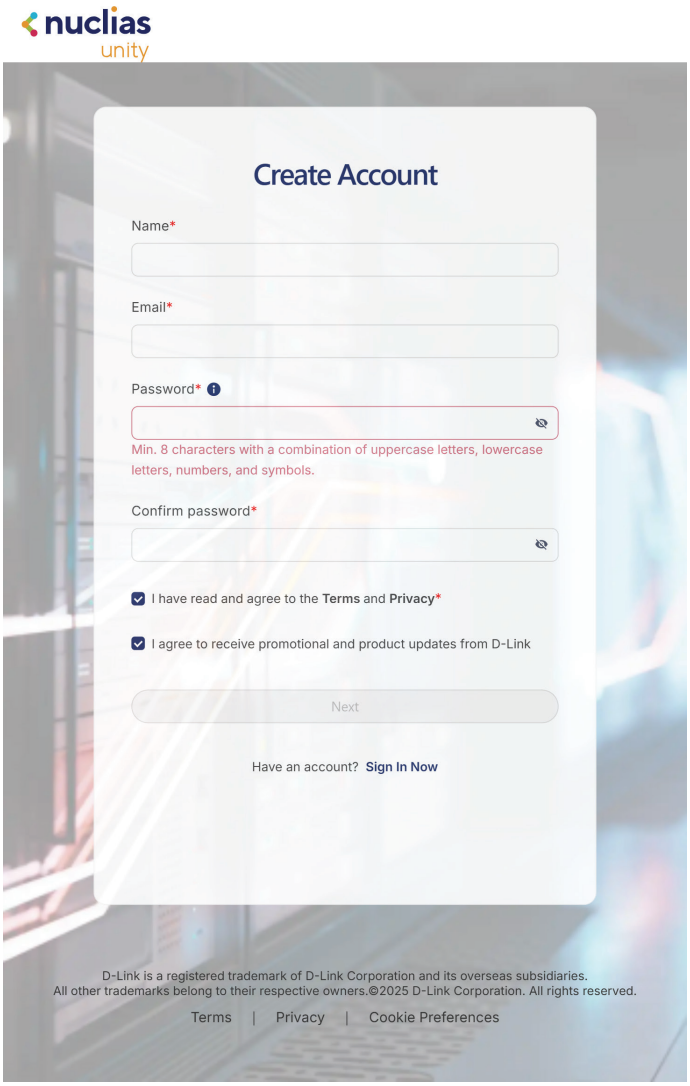
• Cannot be the same as the user name.

• Cannot be the same as default login accounts (e.g., “admin”) or default IP addresses.

• Must be non-consecutive characters (e.g., “1111”, “aaaa” are not allowed).

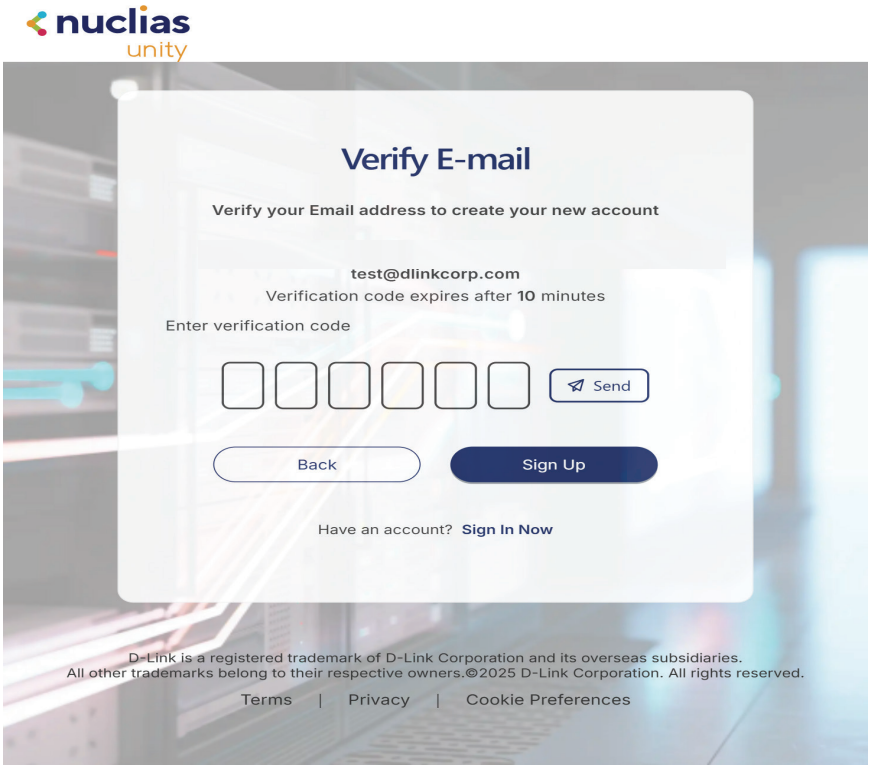
Note: If a non-compliant password is set, the device may reboot and cause abnormal operation.

Enter your password following the rules, then enter it again in the Confirm Password field. Review and agree to the Terms and Conditions, then click **Next** to continue.



Getting Started with Nuclias Unity Verify E-Mail

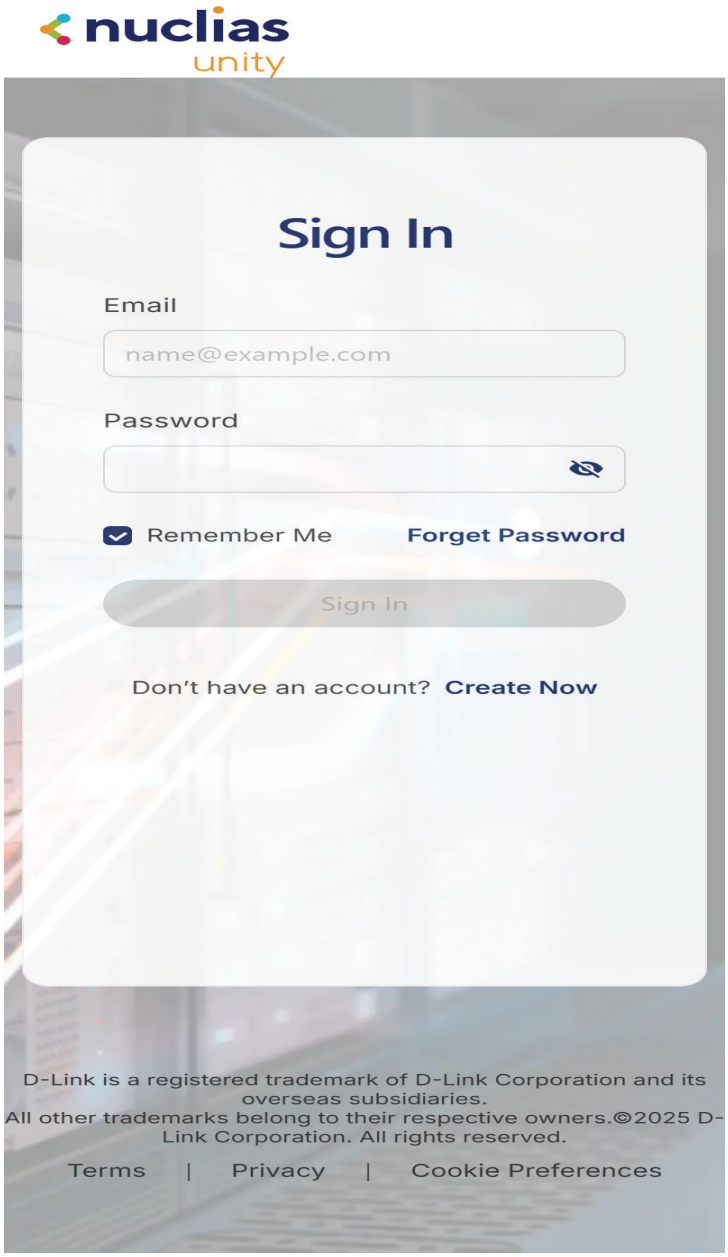
Click Send the verification code to your registered Email account, when you receive six-digit verification code fill into the verification code box.



If you have not received the email, wait a few more seconds for the verification code to arrive before completing your account registration.

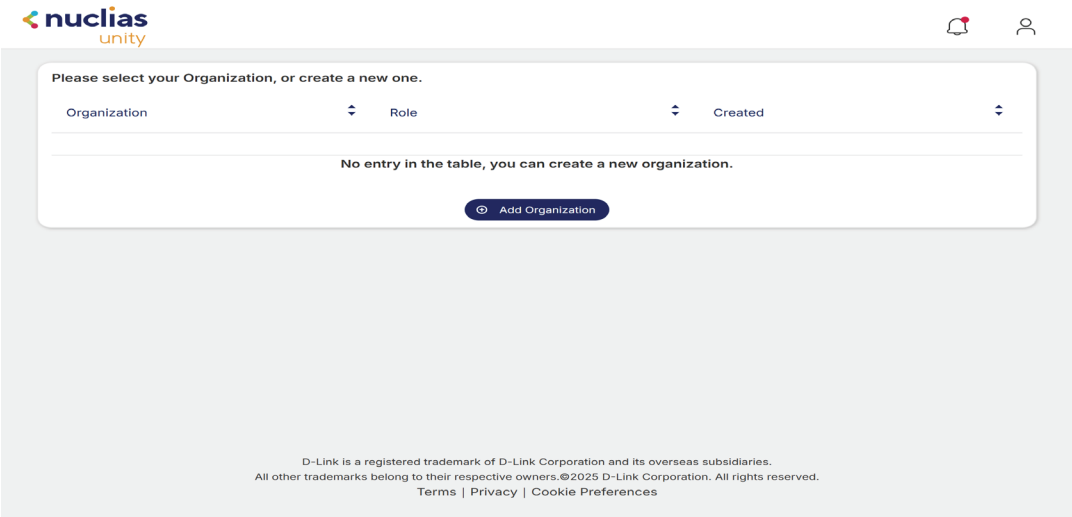
Getting Started with Nuclias Unity Logging in to Nuclias Unity

After creating your user account, open a supported web browser and enter the Nuclias Unity URL in the address bar.
On the login page, enter your registered email address and password, then click Sign In to access the platform. Once logged in, you can begin configuring your organization, sites, and devices.



Getting Started with Nuclias Unity Add Organization

Once you have successfully logged in, you will be prompted to create an **Organization** name, followed by a **Site** name.
The Organization and Site structure forms the foundation for managing your network, devices, and configurations within the Nuclias Unity platform. Enter the required information and proceed to continue the setup process.

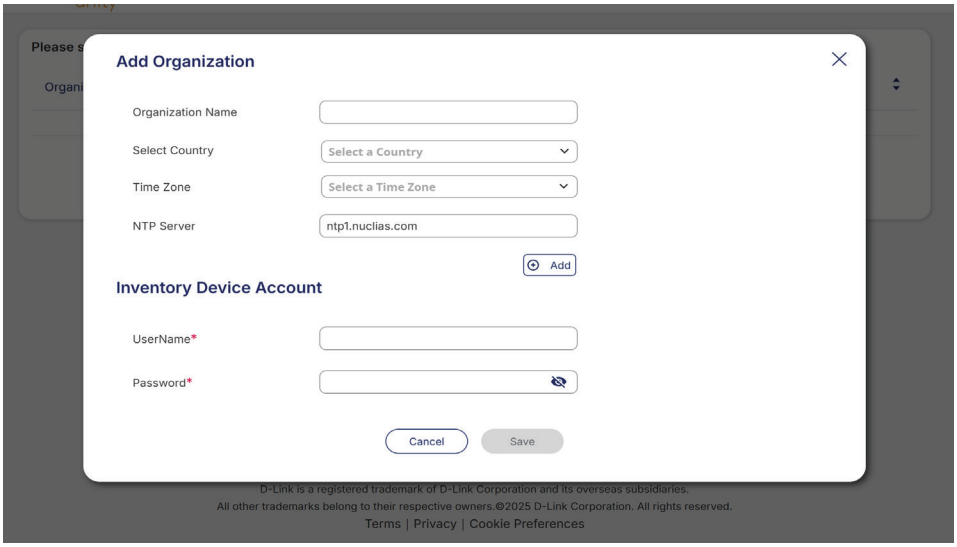


Enter the required organization details in the configuration page:

- **Name** – Enter a name to identify your Organization.
- **Country** – Select the country where the network is deployed.
- **Time Zone** – Choose the appropriate time zone for accurate scheduling and logs
- **NTP Server** – Specify the Network Time Protocol (NTP) server to synchronize system time.
- **Inventory Device Account** – Enter Username and Password for connected devices.

Please set a username and a password that comply with the specified requirements.

After completing all required fields, click **Save** to apply the settings and proceed.

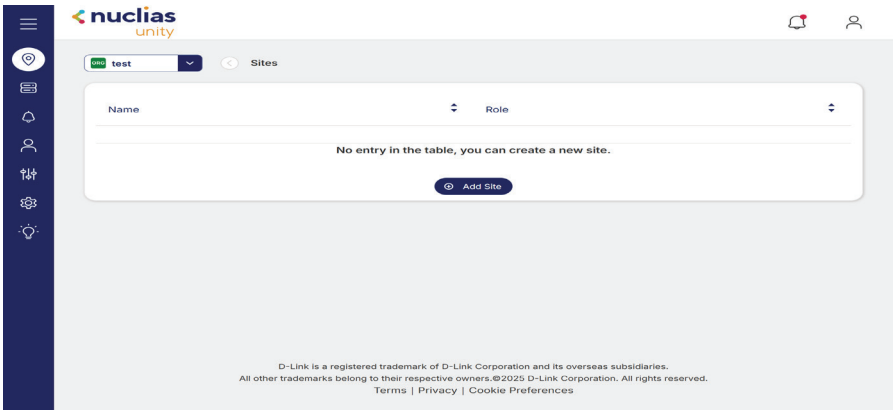


An Inventory Device Account is maintained at the organizational level to manage devices before they are deployed to specific sites. It provides centralized control over procurement, staging, and distribution, ensuring consistent oversight at the management level.

Gettting Started with Nuclias Unity Add New Site

After successfully creating your Organization Name, the system will automatically proceed to the next step, where you will create a new Site for your organization.

On the Site configuration page, locate and click Add Site, as shown in the image below. This will open the site setup page, allowing you to enter the necessary site details and complete the creation process.

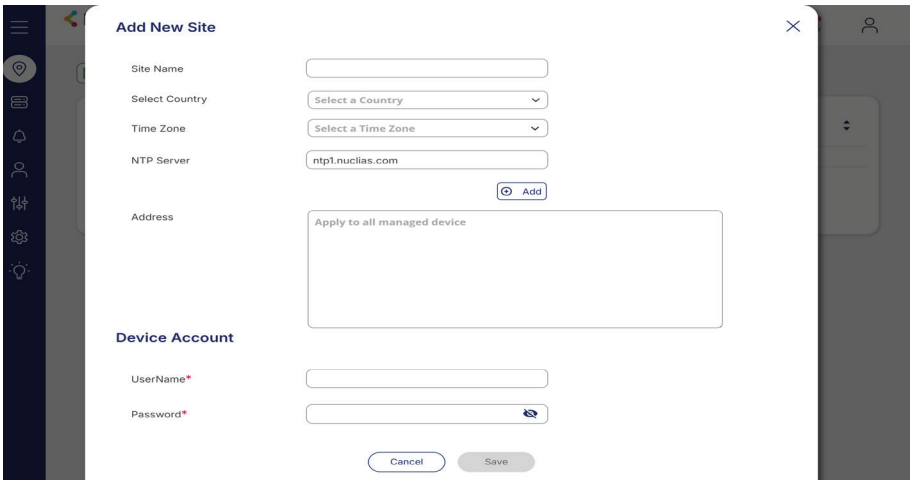


Enter the required site details in the configuration page:

- **Name** – Enter a name to identify your site.
- **Country** – Select the country where the network is deployed.
- **Time Zone** – Choose the appropriate time zone for accurate scheduling and logs
- **NTP Server** – Specify the Network Time Protocol (NTP) server to synchronize system time.
- **Site Username and Password** – Enter the organization-level login credentials.

Please set a username and a password that comply with the specified requirements.

After completing all required fields, click **Save** to apply the settings and proceed.



Each site has a dedicated Device Account with a common password shared by all devices assigned to that site. This provides site-level credential management, enabling users to access any device within their location (e.g., all 10 devices at a site would share one password).

Device Configuration

Device Configuration

To begin configuring your switches, you need to know the device's default IP address, username, and password. Follow the step-by-step instructions below to initiate switch configuration.

1. Basic Information Required Before Configuration

Parameter	Default Value
Default Switch IP Address	10.90.90.90
Default Switch Username	admin
Default Switch Password	admin

Note: If the device default IP address is not 10.90.90.90, reset the device to its default settings before proceeding.

2. Network Requirements for Accessing the Web-Based GUI

To access the switch's web-based interface, the PC must be on the same subnet as the switch.

If the switch has the default IP 10.90.90.90:

- The PC IP must be set to: 10.90.90.X
- Where X = 1–89 or 91–254 (e.g., 10.90.90.100)
- Subnet Mask: 255.0.0.0

3. Requirements for Nuclias Unity Cloud Device Discovery

For the switch to be discovered by the Nuclias Unity cloud platform:

- D-Link Discovery Protocol (DDP) must be enabled.
- DDP is disabled by default and must be manually enabled to allow cloud discovery.

4. Default IP Mode of D-Link Switches

- Default Mode: Static IP
- To obtain an IP address automatically, enable DHCP on the switch.

Once the switch is properly configured with the correct IP settings and DDP is enabled, it can be discovered and managed through the Nuclias Unity cloud management platform.

Device Configuration Device Setup

Connecting to the Switch

Ensure your PC is connected to the switch using an Ethernet cable. Before accessing the switch's web-based interface, you must configure your PC with an IP address and subnet mask that are compatible with the switch's default IP settings.

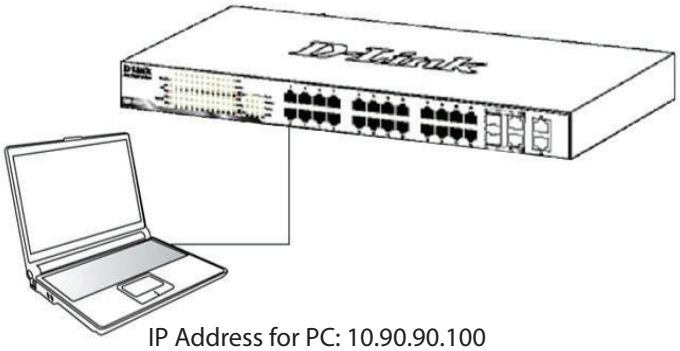
If the switch has the default IP address 10.90.90.90, configure your PC with the following settings:

- IP Address: 10.90.90.X (where X is 1–89 or 91–254, for example, 10.90.90.100)
- Subnet Mask: 255.0.0.0

Refer to the picture below for an example of how to configure your PC IP address and subnet mask.

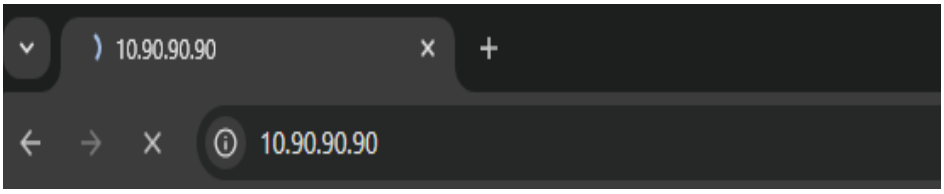
Note: Proper IP configuration is required to establish communication between your PC and the switch before accessing the web-based GUI or enabling cloud discovery.

IP Address for Switch: 10.90.90.90
Subnet: 255.0.0.0



IP Address for PC: 10.90.90.100
Subnet: 255.0.0.0

Now enter your switch IP address (10.90.90.90) into your web browser, as shown in the picture below.



Device Configuration Device Login

Logging Into the Switch

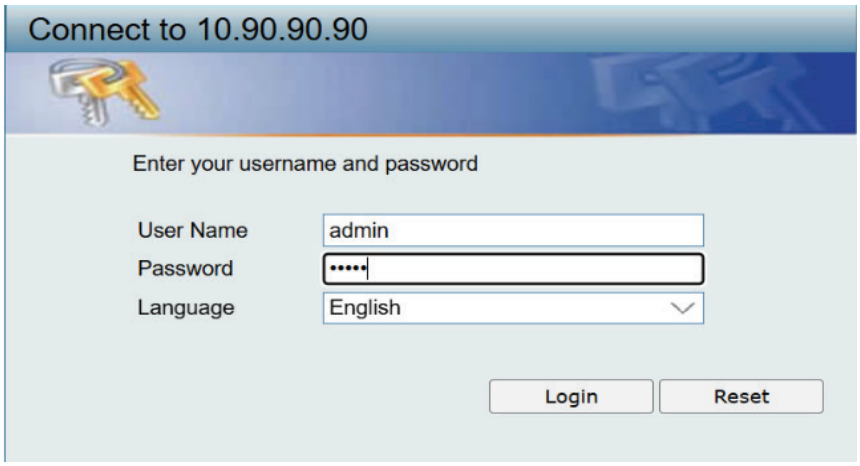
After you enter the switch's IP address in your web browser, a login dialog box will appear. Enter the following default credentials to access the switch's web-based interface:

Username: admin

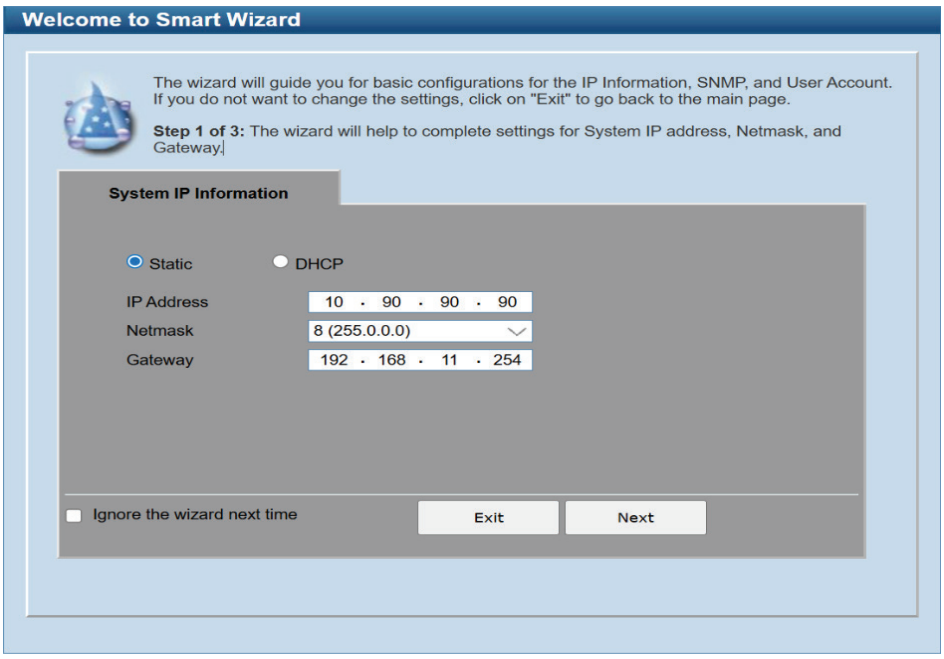
Password: admin

Before proceeding, you may also select your preferred language from the available options to navigate the interface more comfortably.

Note: It is recommended to change the default password after your first login to ensure network security.

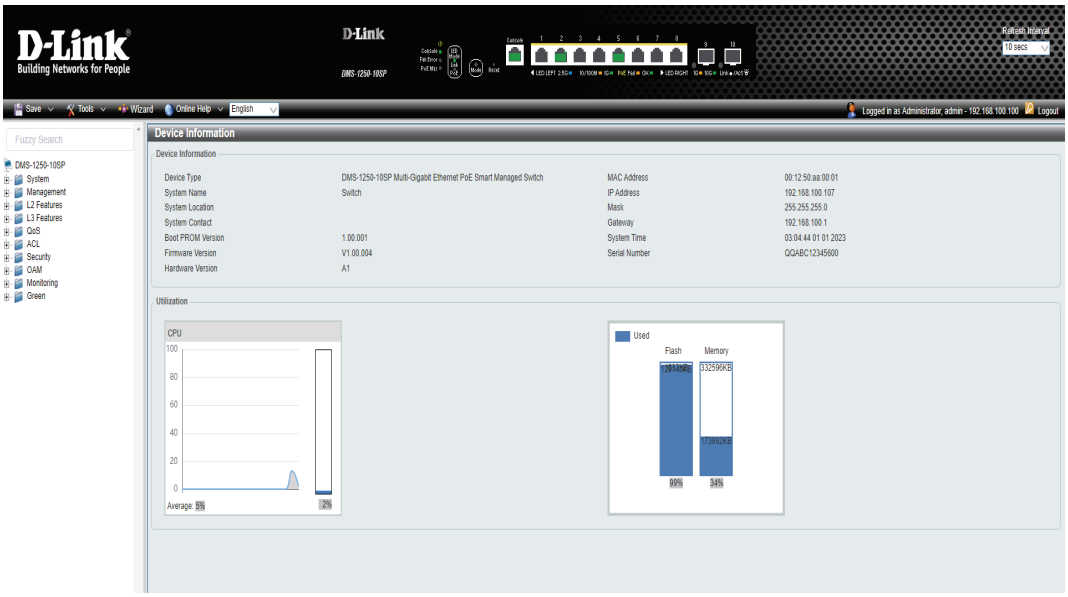


After entering your username and password, the Smart Wizard page will appear. **Do not select DHCP mode** at this stage, as it will break the connection between your PC and the switch. Simply click **Exit,** as shown in the picture below, to proceed to the main dashboard for further configuration.

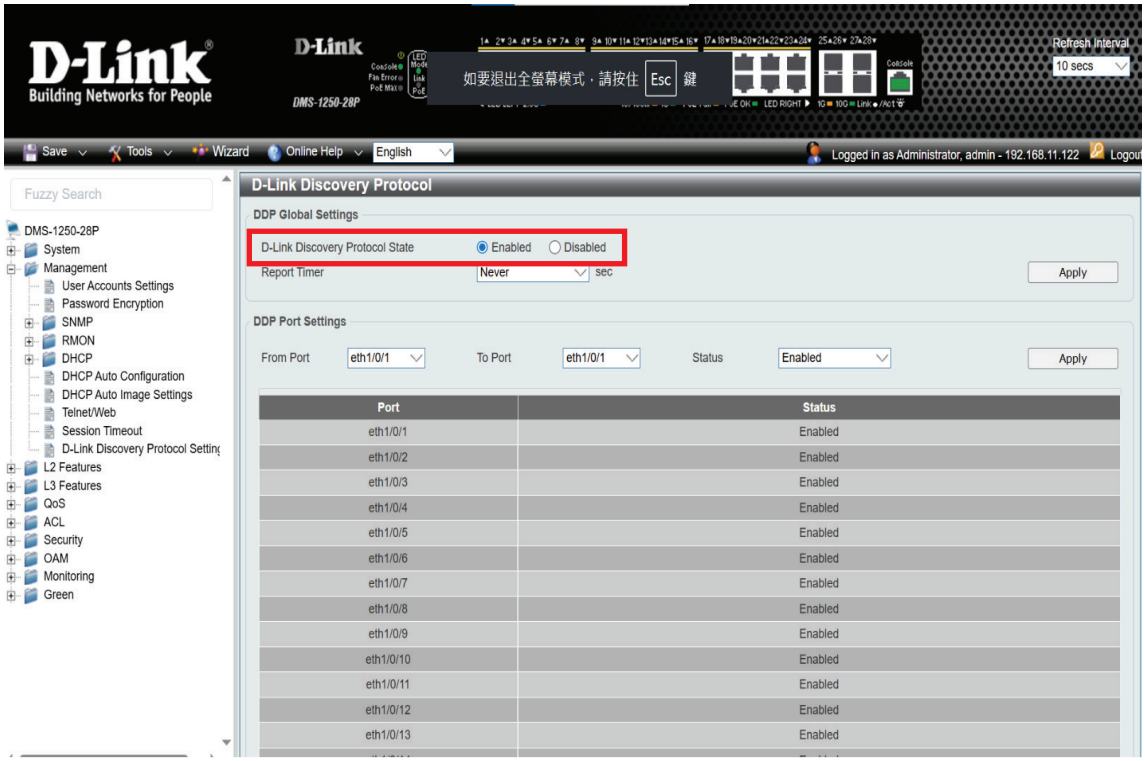


Device Configuration DDP Enable

When you click Exit in the Setup Wizard, the switch dashboard will appear as shown below.



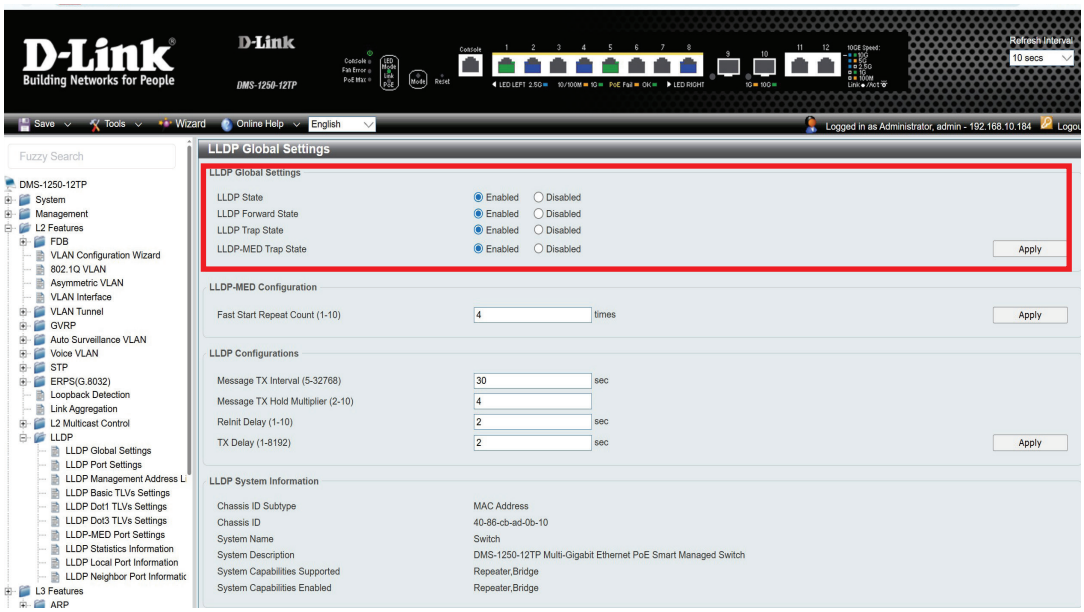
Click **Management** from the drop-down menu on the left side. Then select **DHCP** and choose **D-Link Discovery Protocol** Settings. By default, it is disabled, so enable it and click **Apply** to save the changes.



Device Configuration DHCP Enable

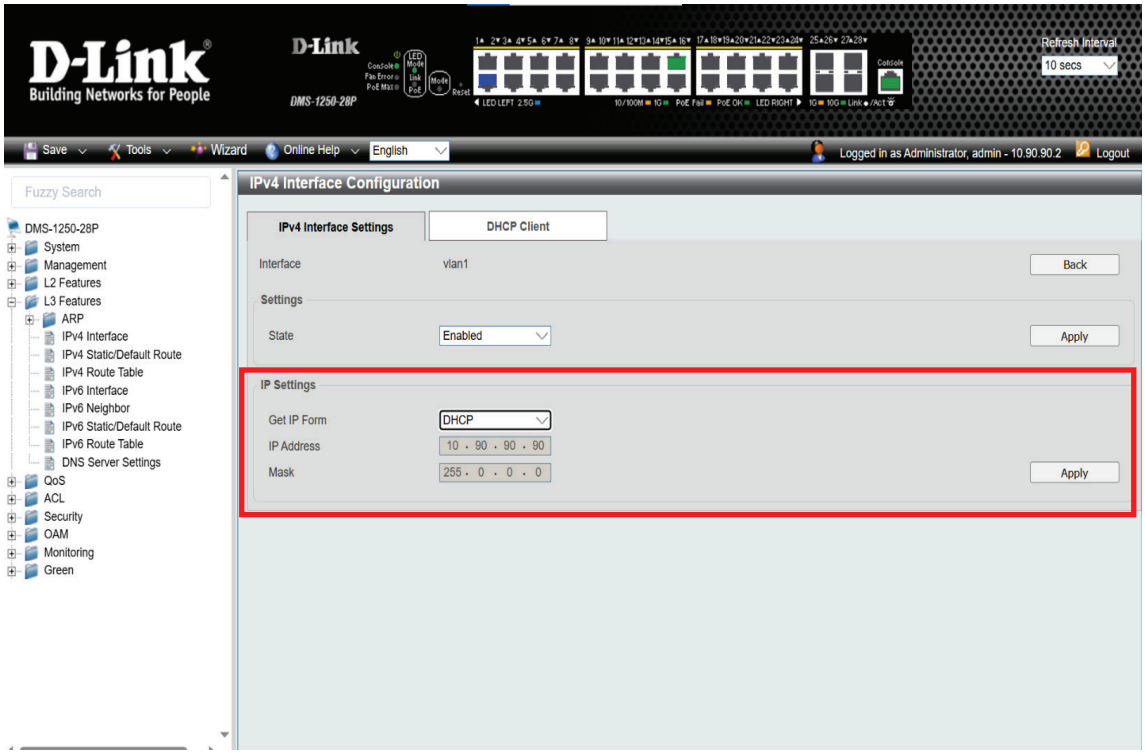
After enabling DDP, you also need to enable LLDP to ensure proper device discovery and communication.

Now, Go to **L2 Features** from the top-left drop-down menu, select **LLDP Global Settings**, and enable LLDP State, LLDP Forward State, LLDP Trap Status, and LLDP-MED Trap State. Then click **Apply**, as shown in the image below.



After enabling LLDP, you also need to enable DHCP so the switch can obtain an IP address automatically when the switch connected to the internet.

Now, go to **L3 Features** in the drop-down menu at the top-left corner, click **IPv4 Interface**, select **DHCP** under **IP Settings**, and click **Apply**, as shown in the picture below.



Device Configuration Device Connectivity

At this stage, your PC will be disconnected from the switch, and the switch is now ready to connect to the internet to obtain an IP address automatically.

Before continuing, make sure your setup is connected to the internet. You may use a D-Link router or a USB dongle to provide internet access. Confirm that your PC, switch, access point, and mobile phone are all connected to the same network. This ensures that all devices can communicate properly during configuration.

Now use your web browser on the PC to log in to Nuclias Unity. Ensure the PC is connected to the internet, and verify that your Organization and Site Name are displayed.

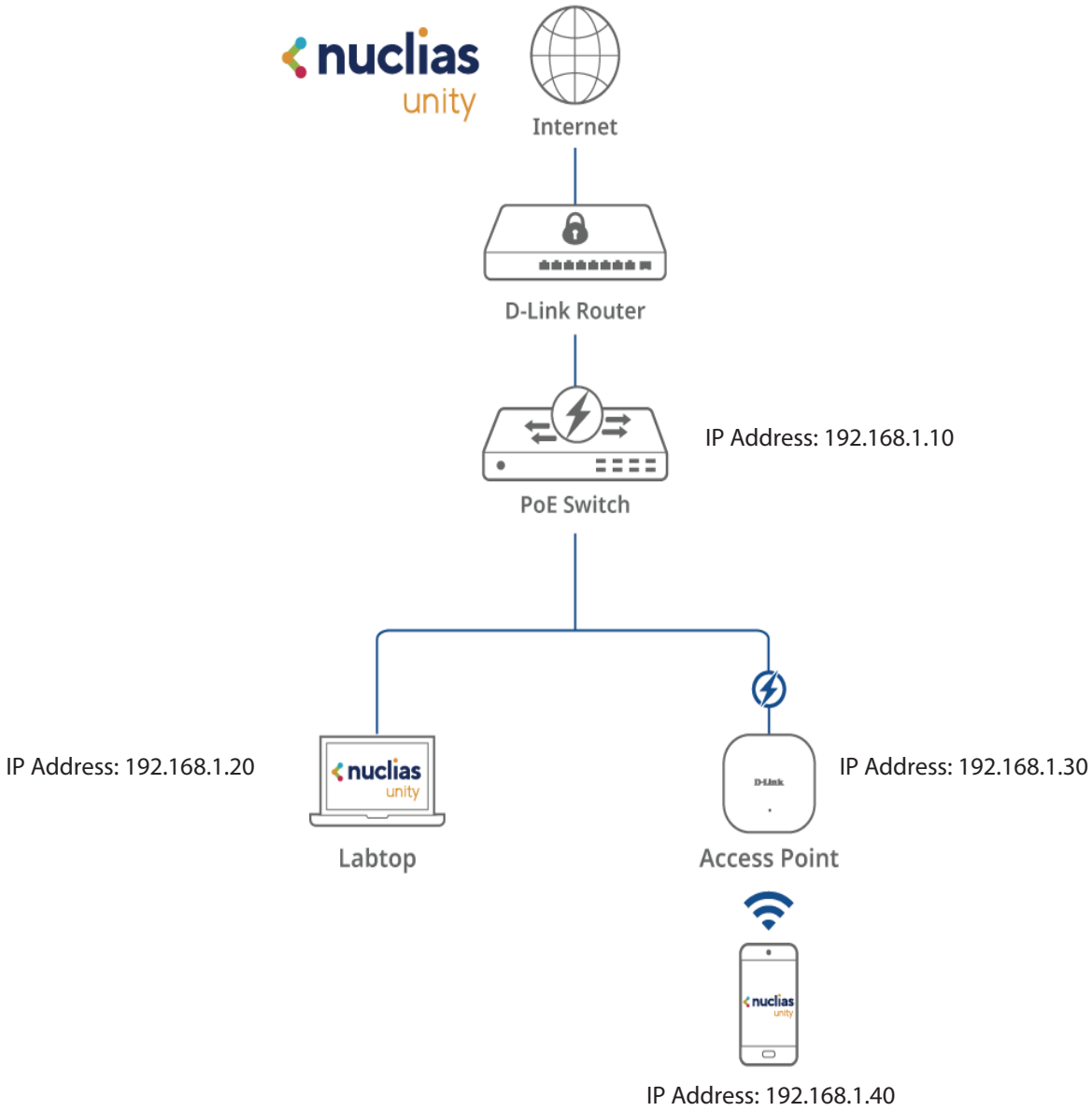
Note: By default, DHCP should be enabled on the access point. If it is not enabled, please log in to your access point and enable DHCP.

Next, launch the Nuclias Unity app and ensure your Android or iOS mobile device is connected to the internet.

Below is a simple environment setup featuring a PoE switch and an Access Point, which will be discovered and managed through Nuclias Unity.

The diagram also shows how your existing network connects to the internet.

Ensure that all devices are connected to the same network, as illustrated in the connection diagram below.



Software Installation

Nuclias Unity App

Download the Nuclias Unity app from the QR code for download application or use the Google Play Store (Android) or the Apple App Store (iOS), and ensure that you install the recommended or latest supported version.

Before launching the app, confirm that you have already created your Organization and Site Name through the Nuclias Unity web browser interface.

Ensure your mobile device is connected to the internet. For device discovery and management, your mobile phone must be connected to the same network environment as your switches and access points, with active internet access.

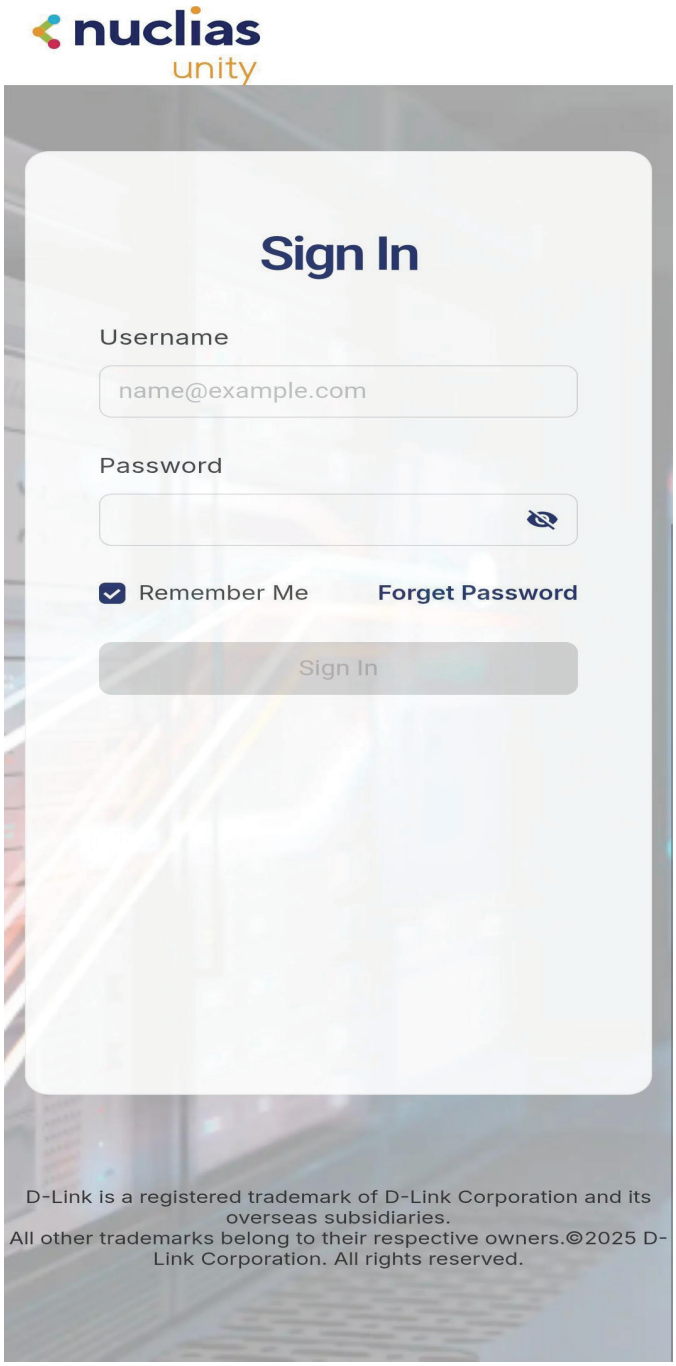
Once these requirements are met, open the Nuclias Unity app and log in using your registered Email Address and Password.

Note: If your mobile device is not connected to the same network as the target devices, the Nuclias Unity app will not be able to detect or discover them.

Download QR Code:

Software Installation Device Setup

Log in to the Nuclias Unity app using your registered email address and password. Ensure that the credentials match the account you created earlier. Once logged in, the app will connect to your Nuclias Unity organization and allow you to begin discovering and managing your devices.

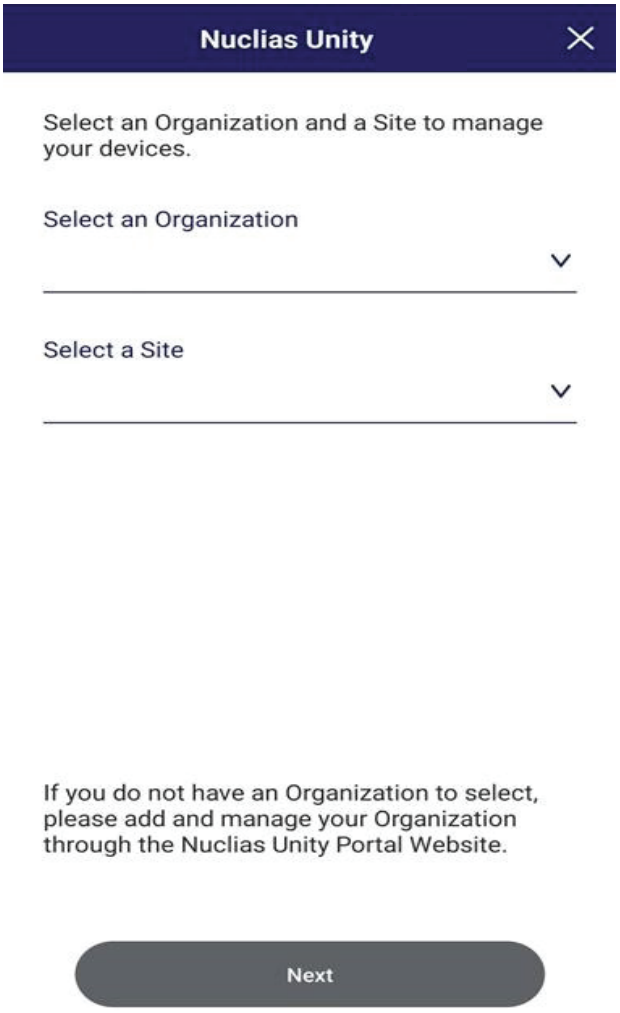


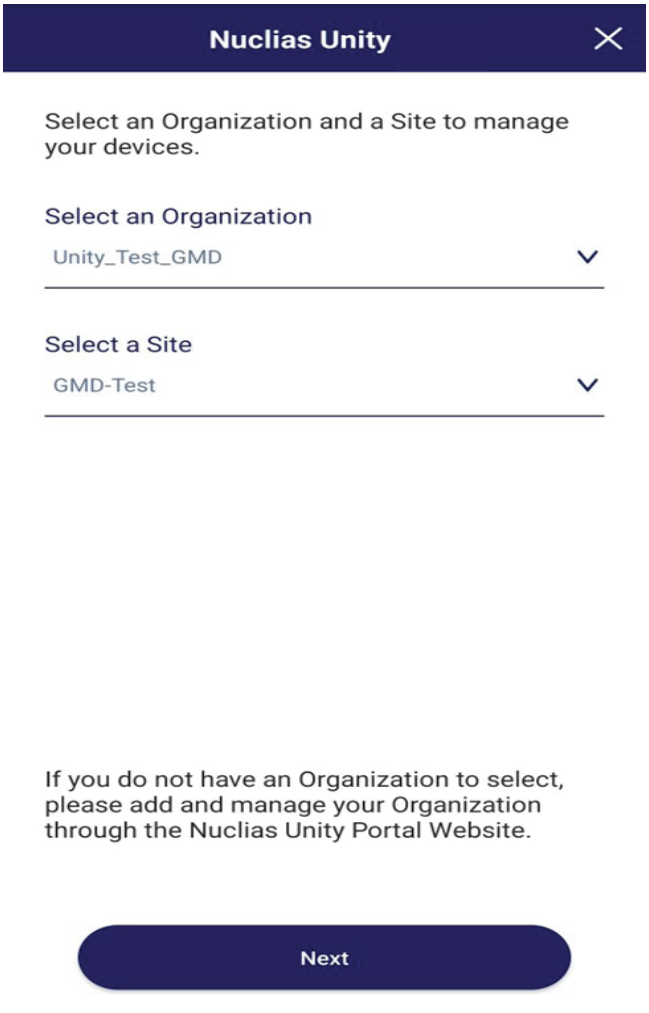
Software Installation Sign In - Nuclias Unity App

After successfully logging in to the Nuclias Unity app, the system will prompt you to select your **Organization** and **Site Name**, as shown in the image below.

On the selection screen, choose the appropriate **Organization Name** from the list. Then, select the corresponding **Site Name** associated with that organization.

After confirming your selections, tap **Next** to proceed to the next step and continue with device discovery and management.





Software Installation Adding Devices into Nuclias Unity App

To discover connected devices using the Nuclias Unity app, ensure that the **Scan (Multicast)** option is enabled. This option is enabled by default and allows the app to automatically detect devices within the same network environment.

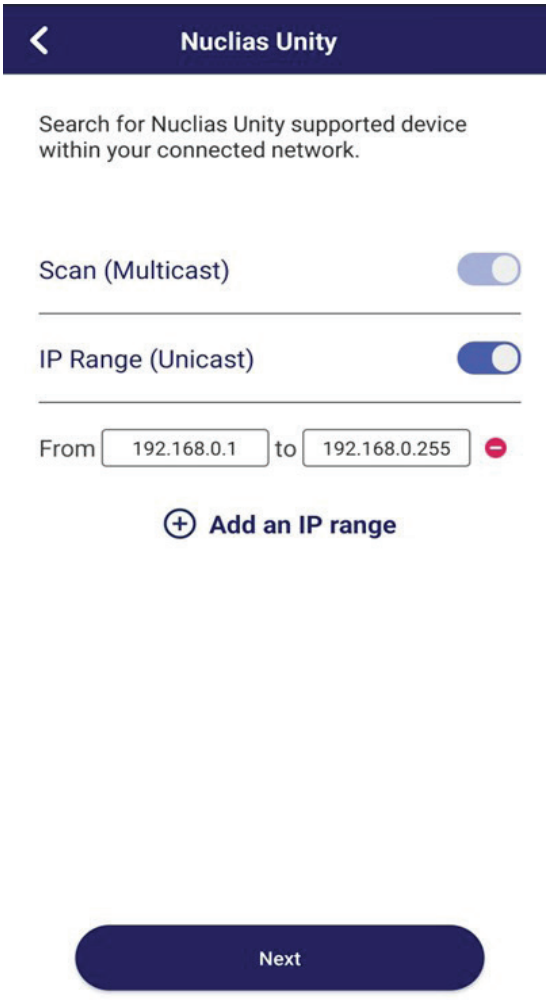
If you want to scan a specific IP range, enable the **IP Range (Unicast)** option and manually configure the required IP address range. When using Unicast scanning, you must enter the correct IP range that corresponds to the subnet where your devices are located. If you are unsure of the correct IP range, consult your IT administrator for assistance.

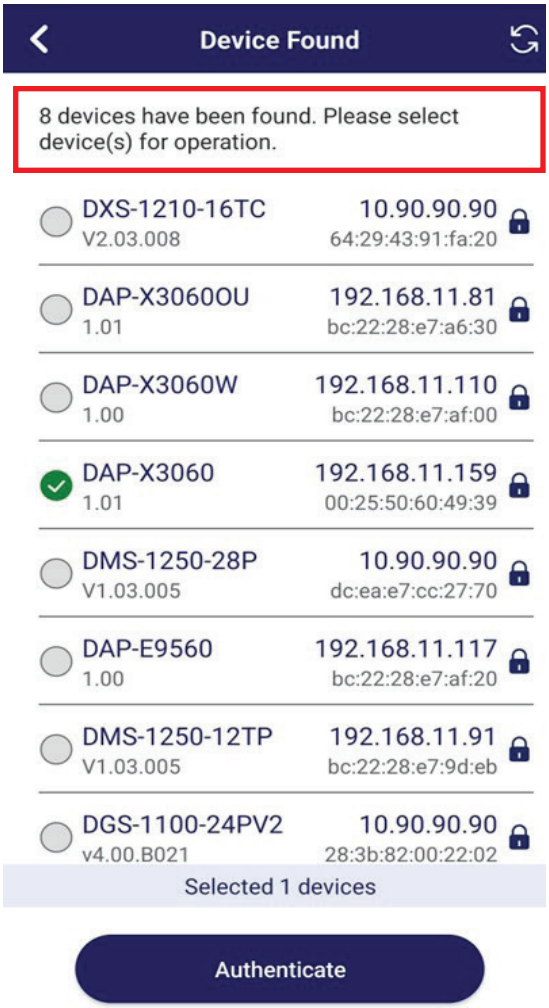
To configure the IP address range, enter the starting and ending IP addresses as shown in the example below. For instance, you may define a range from **192.168.0.1 to 192.168.0.255**.

If additional IP ranges are required, click **Add an IP Range** and enter the necessary details. After completing the configuration, click Next to proceed to the next step.

After configuring the IP address range, the app will scan the network and display the discovered devices, as shown in the image below.

From the list of detected devices, select the device you wish to manage through Nuclias Unity. Then, click **Authenticate** to begin the adoption process and proceed to the next step.





Software Installation Adding Devices intoNuclias Unity

During the authentication process, enter the device's **username** and **password** in the required fields.

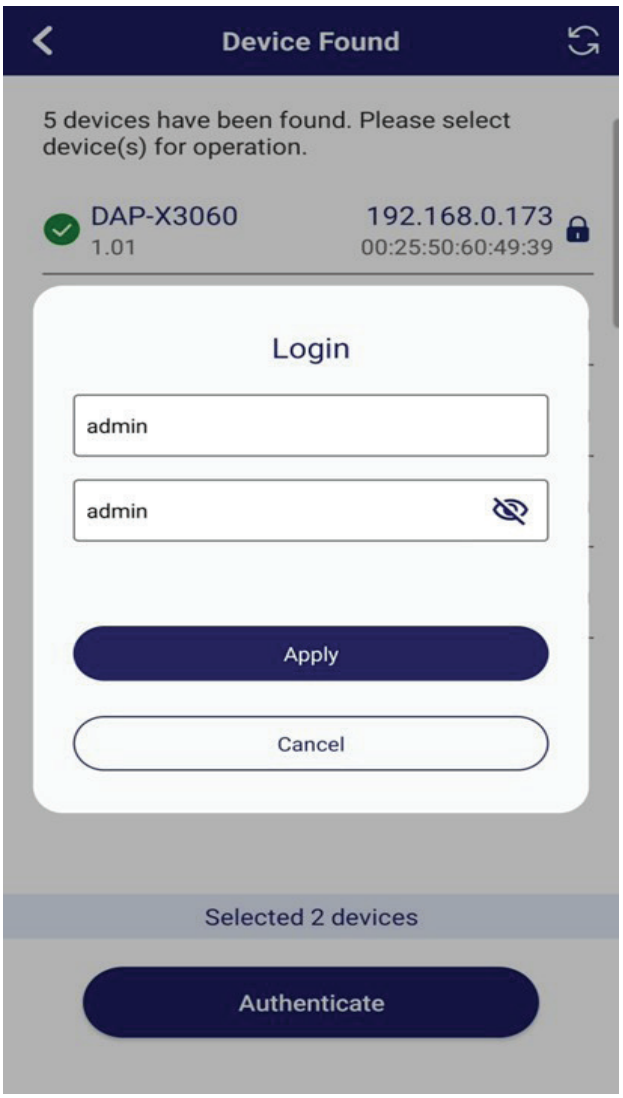
If authentication fails, it may indicate that the device credentials have been changed from the default settings. In this case, perform a hardware reset on the device to restore the factory default settings, and then repeat the adoption process.

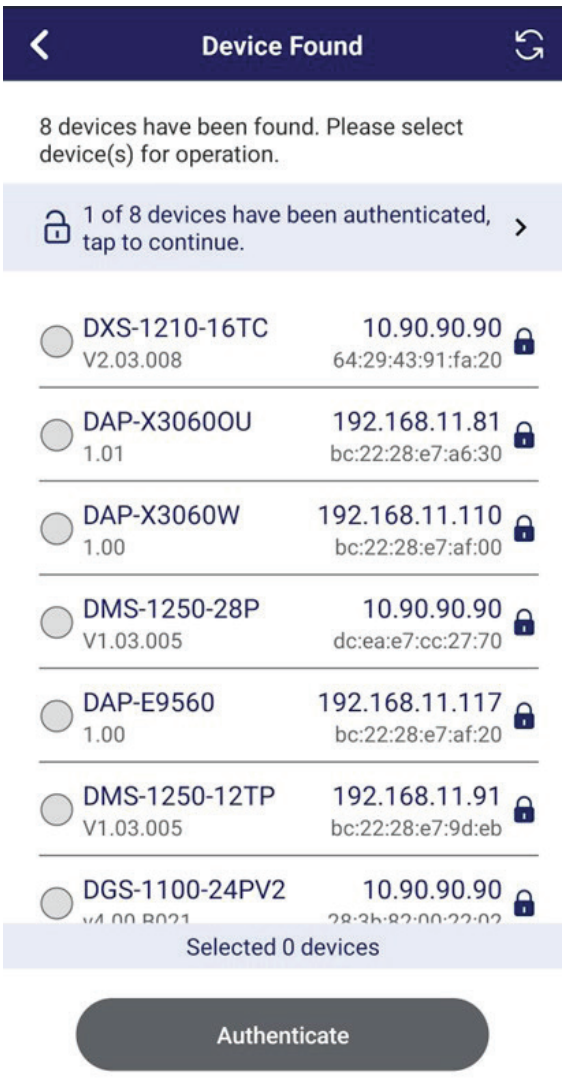
By default, both the username and password are set to "**admin**."You may also configure a new username and password according to your security requirements.

After entering the correct credentials, click **Apply** to authenticate and adopt the device into Nuclias Unity.

After successfully authenticating the device, a notification will appear at the top of the screen indicating the number of devices ready to be managed through Nuclias Unity.

Tap the notification to review the authenticated devices, then proceed with the adoption process to add them into your Nuclias Unity network for centralized management.





Software Installation Adding Devices into Nuclias Unity App

After authentication, select the desired device from the list of authenticated devices.

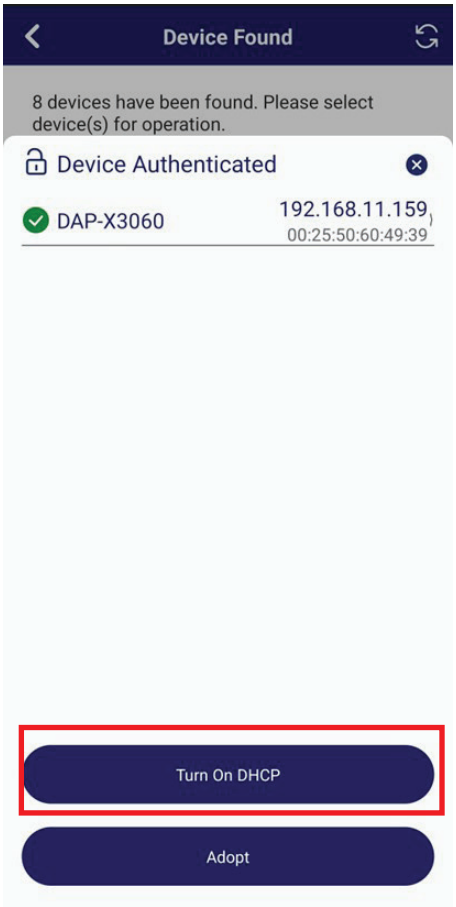
Before proceeding with adoption, click **Turn On DHCP**, as shown in the image below. This step enables DHCP on the device, allowing it to automatically obtain an IP address from the network's DHCP server. Ensure that your network has an active DHCP server available.

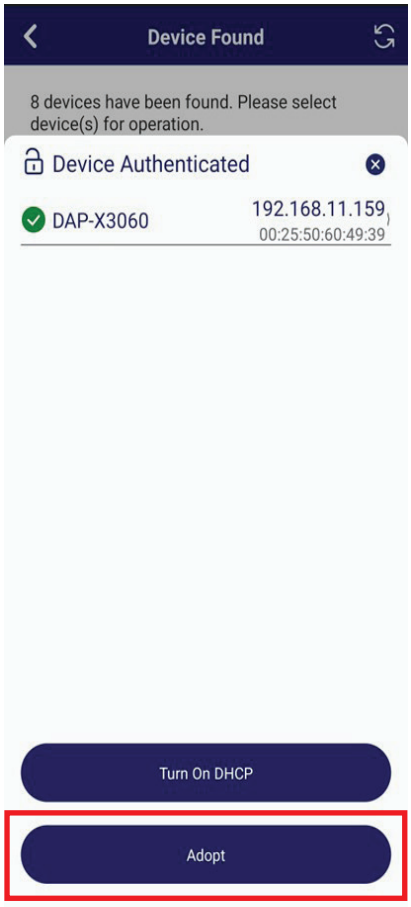
Once DHCP is enabled, click **Adopt** to add the device to your Nuclias Unity Organization and Site.

After clicking **Adopt**, a success notification will appear confirming that the device has been successfully adopted. The adopted device will then be associated with your selected **Organization and Site Name**.

Click **Done** to complete the process. If you need to adopt additional devices, repeat the same steps for each device.

To verify that the devices are online and properly managed, log in to Nuclias Unity through a web browser and check the device status under your Organization and Site.





Nuclias Unity Configuration Nuclias Proxy

Nuclias Unity Proxy is a dedicated software appliance designed to act as an intermediary bridge between the Nuclias Unity cloud platform and specific high-end on-premises network devices.

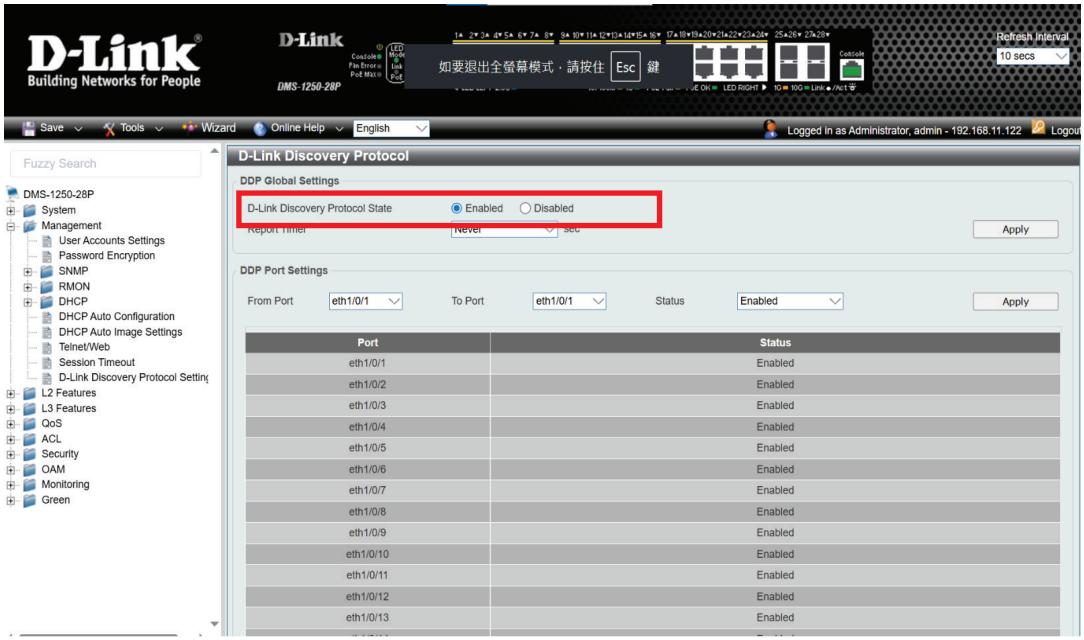
Here are the key details about Unity Proxy based on the provided documents:

Software-Based Solution: It is not a hardware controller. The Unity Proxy software must be installed on a PC running **Windows 10 or a later version (64-bit)**.

The supported device of Unity Proxy will be more and more in the future. Suggest to put “Resource Center” URL let user can download Unity Proxy and also can check Compatible Products.

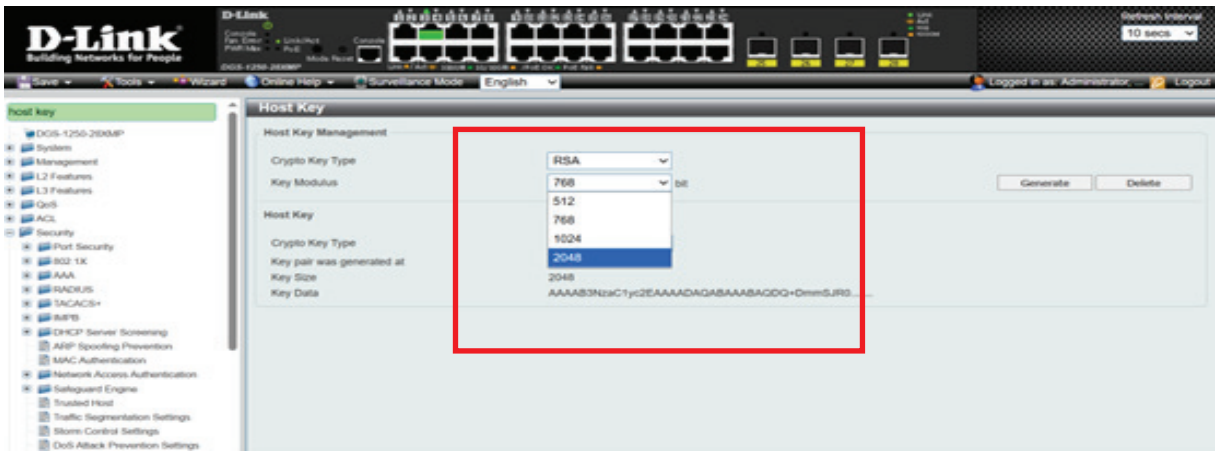
Pre-configuration Requirements: switches managed via Unity Proxy require manual pre-configuration before they can be adopted. This includes enabling the D-Link Discovery Protocol (DDP), enabling the IP SSH Server State, generating an RSA Host Key (e.g., 2048-bit), and setting the IPv4 interface to DHCP. It also requires a third-party component called Npcap (version 1.86 or higher) to function properly.

DDP Enable – Enables the D-Link Discovery Protocol (DDP), allowing the device to be automatically discovered and managed by compatible network management systems.



SSH Global Setting: Enable – Enables Secure Shell (SSH) access, allowing secure remote management of the device through an encrypted command-line connection.

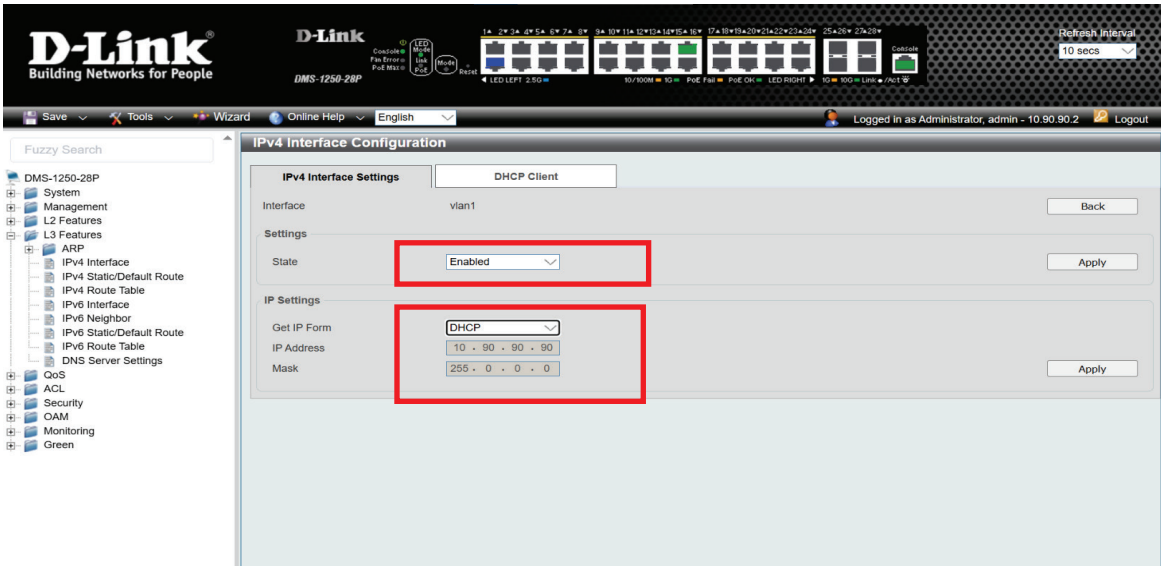
Generate Host Key – Select the Key Modulus with the maximum bit (2048) value for stronger security, then click Generate to create the key data.



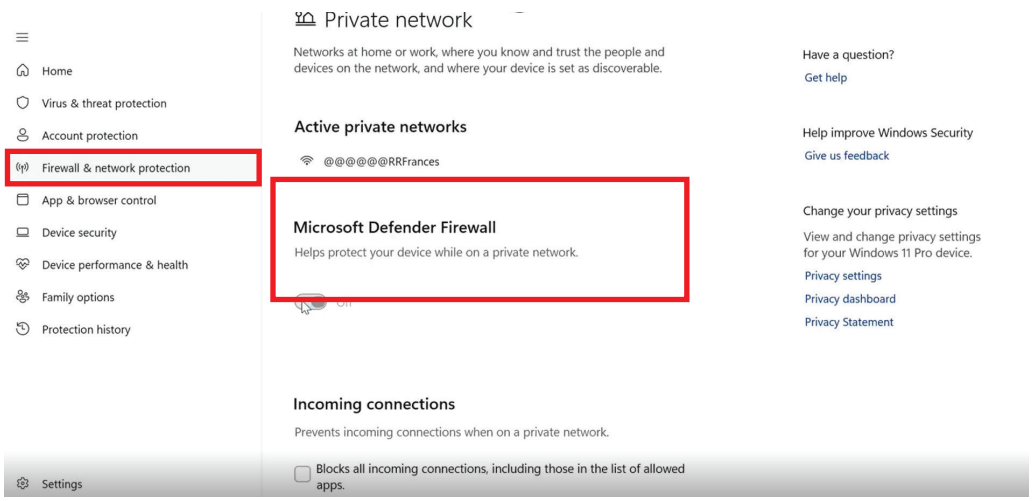
Click Generate, then a Success message will appear.

After generation, the key data will be displayed.

Enable DHCP Mode – Allows the router to automatically assign an IP address to the device.

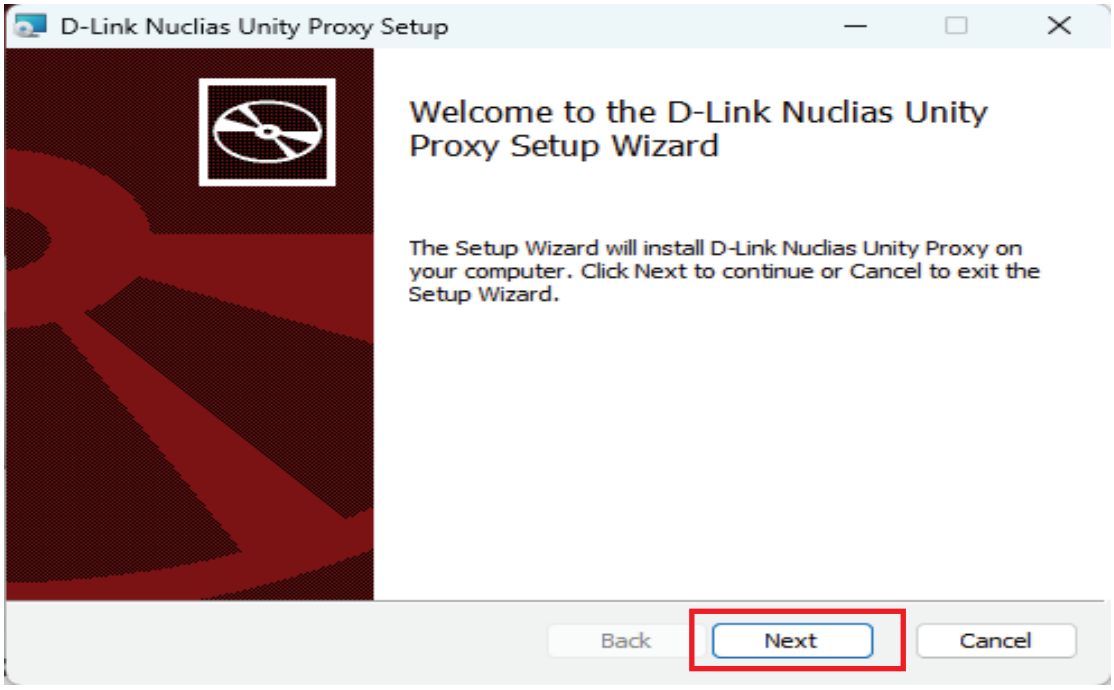


Before install and use Nuclias Unity Proxy, you need to turn off the firewall on your Windows PC. Navigate to **Firewall & Network Protection** on your Windows PC, then **Turn Off** the Microsoft Defender Firewall.



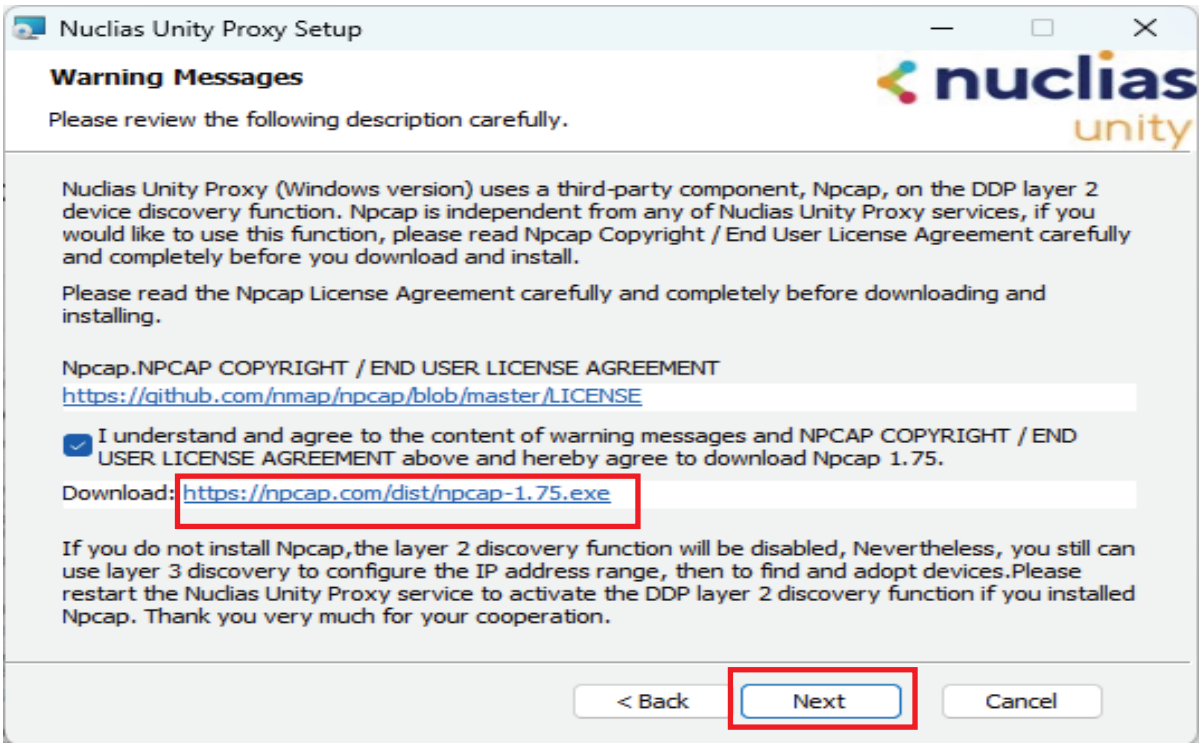
Nuclias Unity Nuclias Proxy Proxy Installation

Install Nuclias Unity Proxy on your computer to connect the local network with the Nuclias Unity cloud platform.

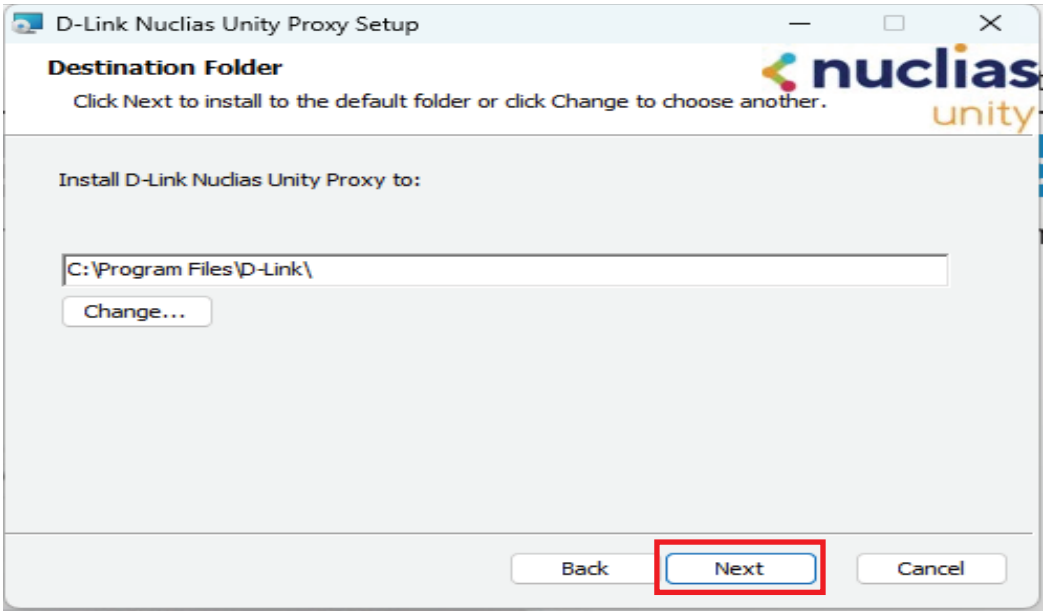


Agree to the Terms and Conditions, then click **Download** to install and redirect to **NCAP** install page.

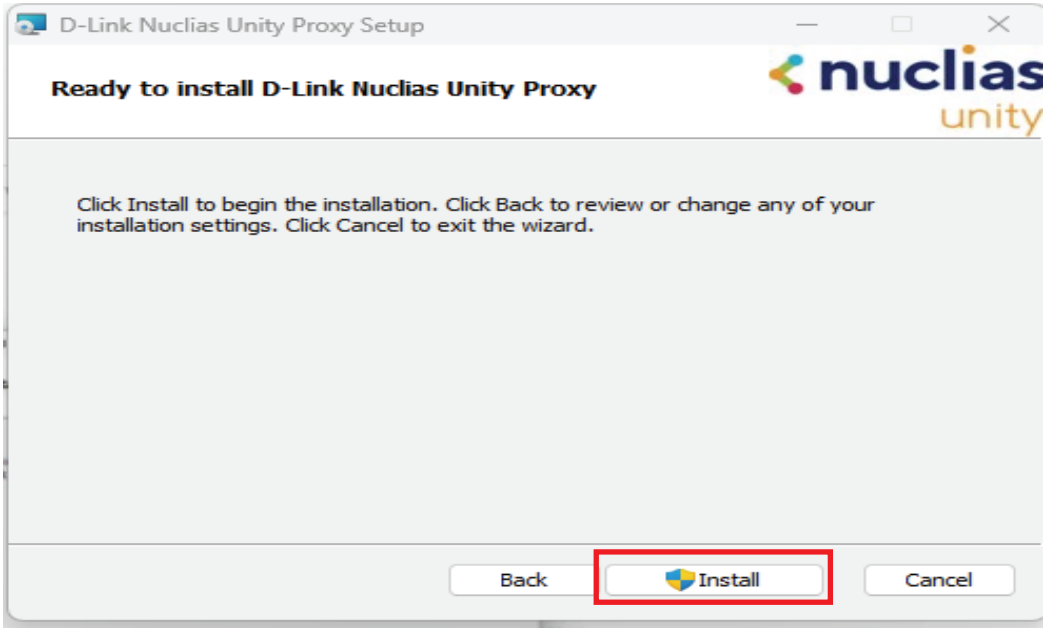
NOTE: Before launching the Nuclias Unity Proxy software, you must first agree to the Terms and Conditions, then click the URL to download the NCAP file and install the NCAP driver. This must be done before finishing the proxy installation; if the proxy installation is already complete, ensure the NCAP driver is installed prior to launching the software.



The installer will suggest a default path, such as C:\Program Files\NCAP Driver. We recommend using this location. To change it, click Browse, select your desired folder, and click OK. When ready, click Next to continue.

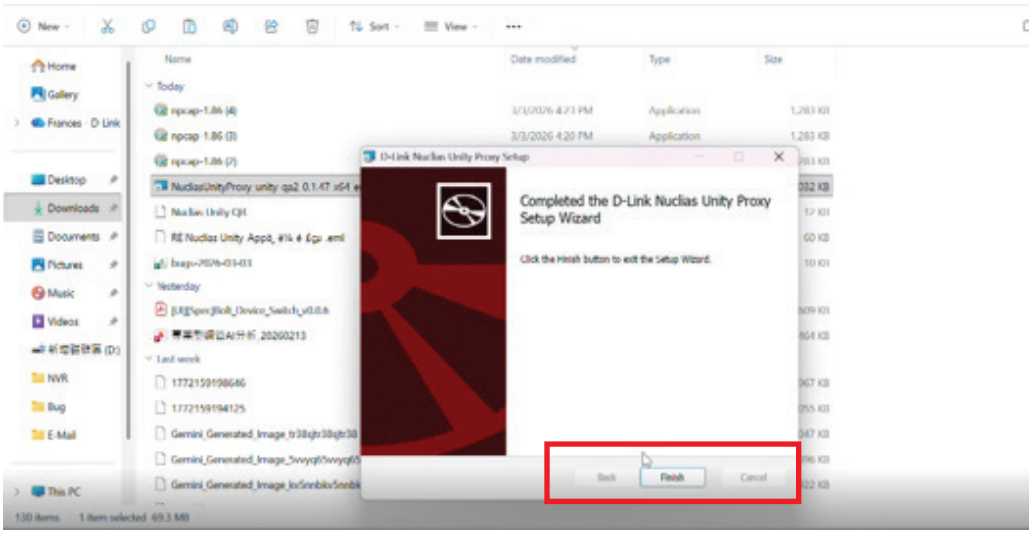


Click Install to begin installing the Nuclias Unity Proxy. The installation progress will be displayed on screen. This process may take a few minutes. Please wait for it to complete.

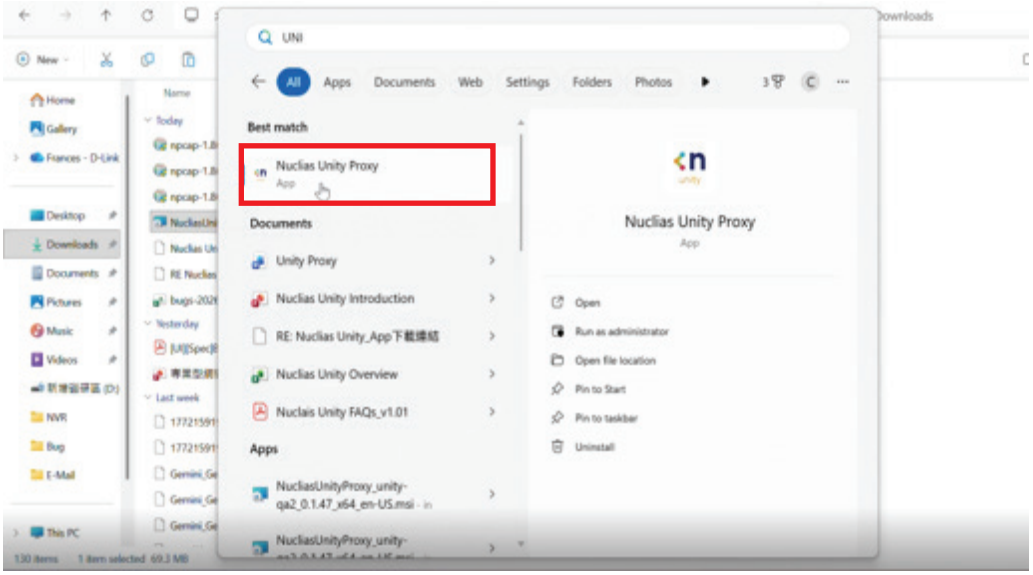


Nuclias Unity Nuclias Proxy Proxy Installation

Once the installation is complete, click Finish to exit the setup wizard. The Nuclias Unity Proxy is now installed on your system.

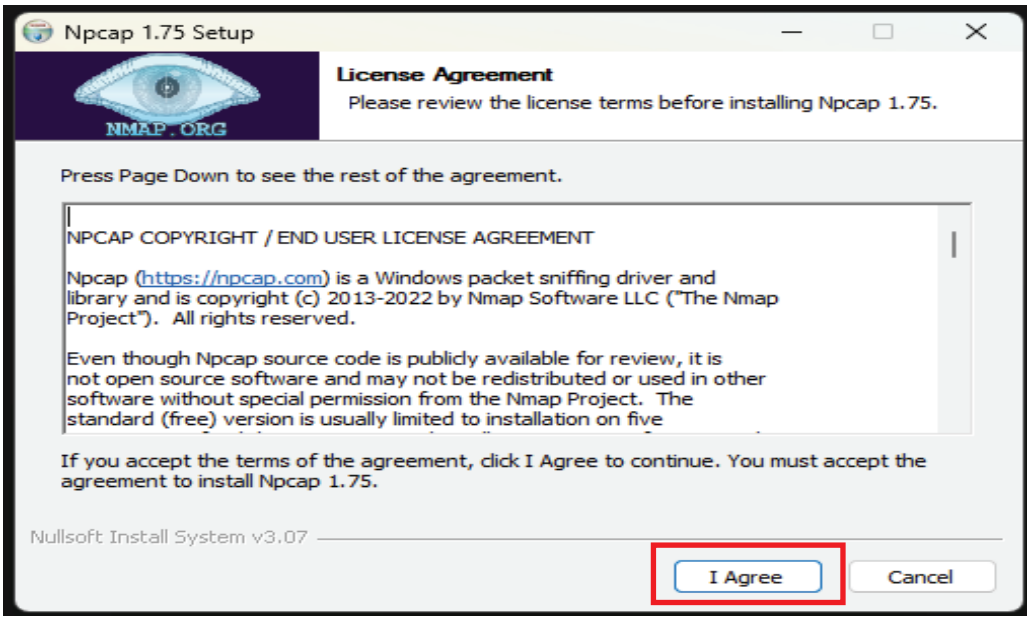


To confirm the software was installed successfully, go to the search bar on your taskbar and type Nuclias Unity Proxy. If the application appears in the search results, the installation is complete and ready to use.

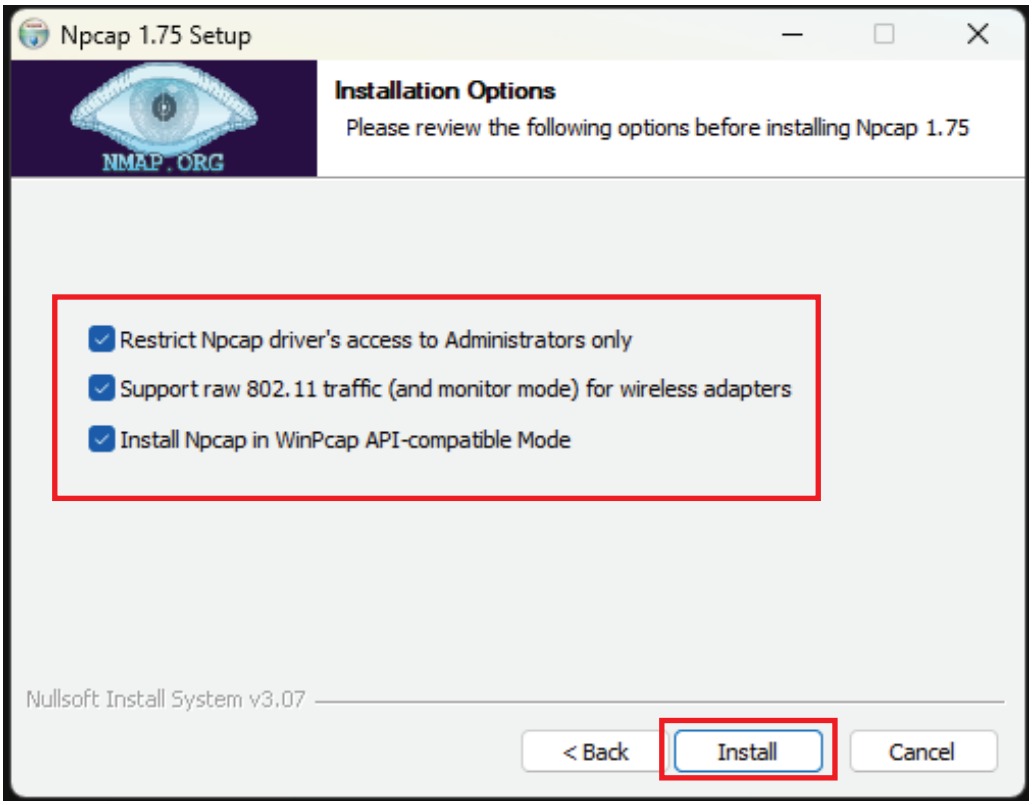


Nuclias Unity Nuclias Proxy **NCAP Installation**

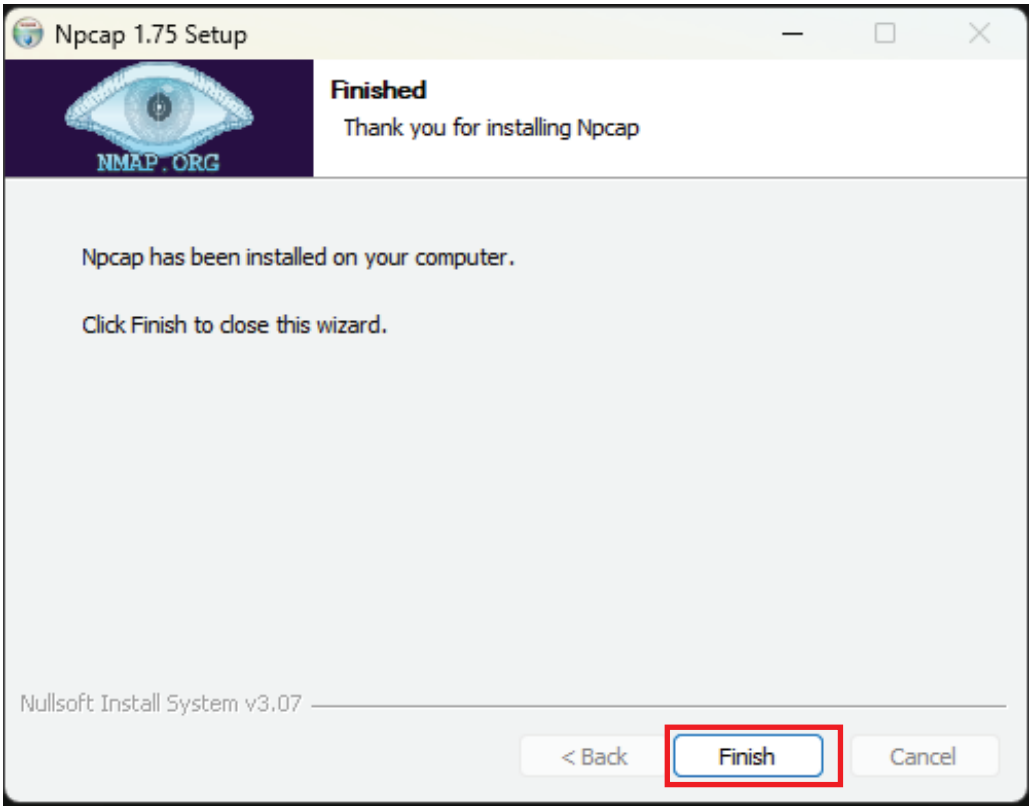
Navigate to the location where you downloaded the NCAP driver file. Double-click the file to begin the installation process.



Select and enable all required options as needed, then click Install to begin installing the NCAP driver. Wait for the installation process to complete.



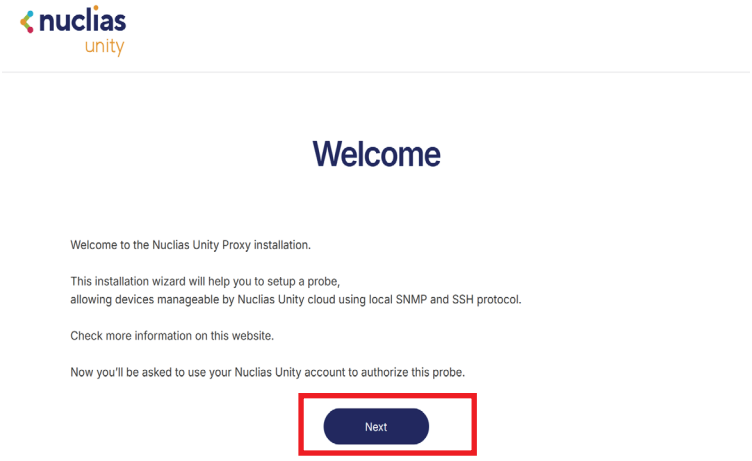
Once the installation is complete, click Finish to exit the setup wizard. The NCAP driver is now installed on your system.



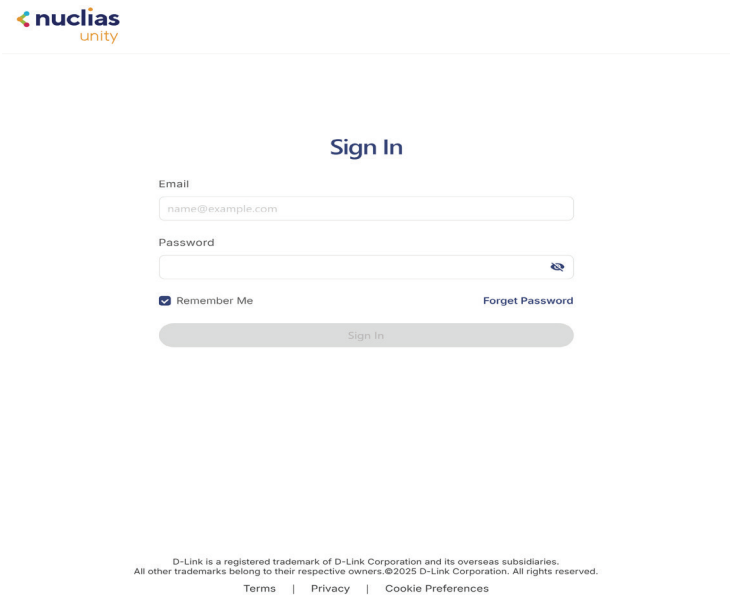
Nuclias Unity Nuclias Proxy **Launch Proxy**

Go to the search bar on your taskbar and type Nuclias Unity Proxy. Select the application from the search results to launch it. Ensure you have a valid account to log in. Enter your credentials, then click Next to proceed.

Note: Before launching the Nuclias Unity Proxy software, you must first agree to the Terms and Conditions, then click the URL to download the NCAP file and install the NCAP driver. This must be done before finishing the proxy installation; if the proxy installation is already complete, ensure the NCAP driver is installed prior to launching the software.

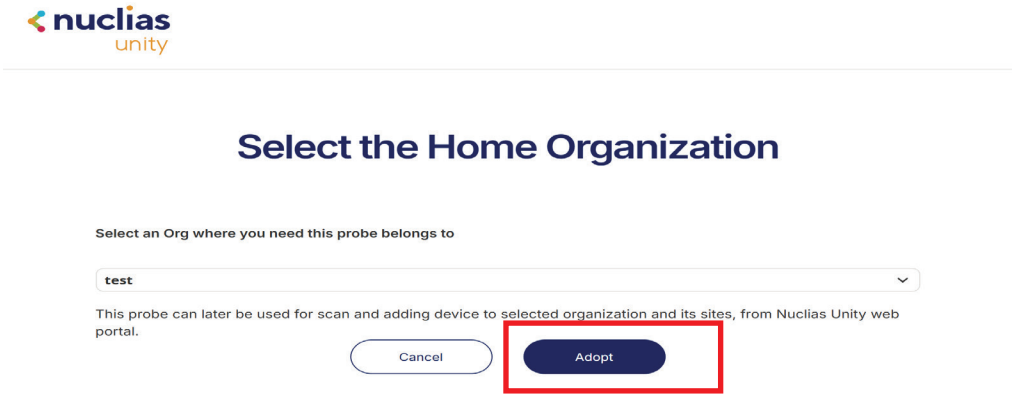


Log in to your Nuclias Unity cloud platform and verify that you have created an Organization and a Site. These are required before proceeding.



Nuclias Unity Nuclias Proxy **Launch Proxy**

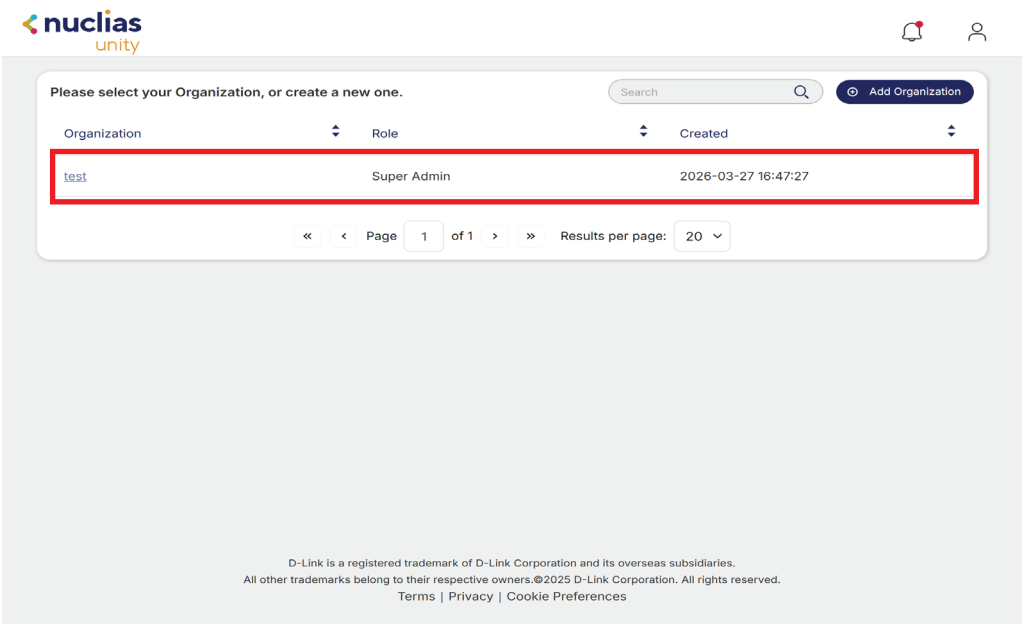
In the Nuclias Unity Proxy window, select the appropriate Organization from the dropdown menu. Create a new Unity Proxy or select an existing one from the list, then click Adopt to continue.



Check the Summary section to confirm the status shows Online and that the proxy is successfully linked to your Organization. Before proceeding, ensure that the **Organization Name** and the **last five digits of the Unity Proxy ID** are correctly displayed and match your records.

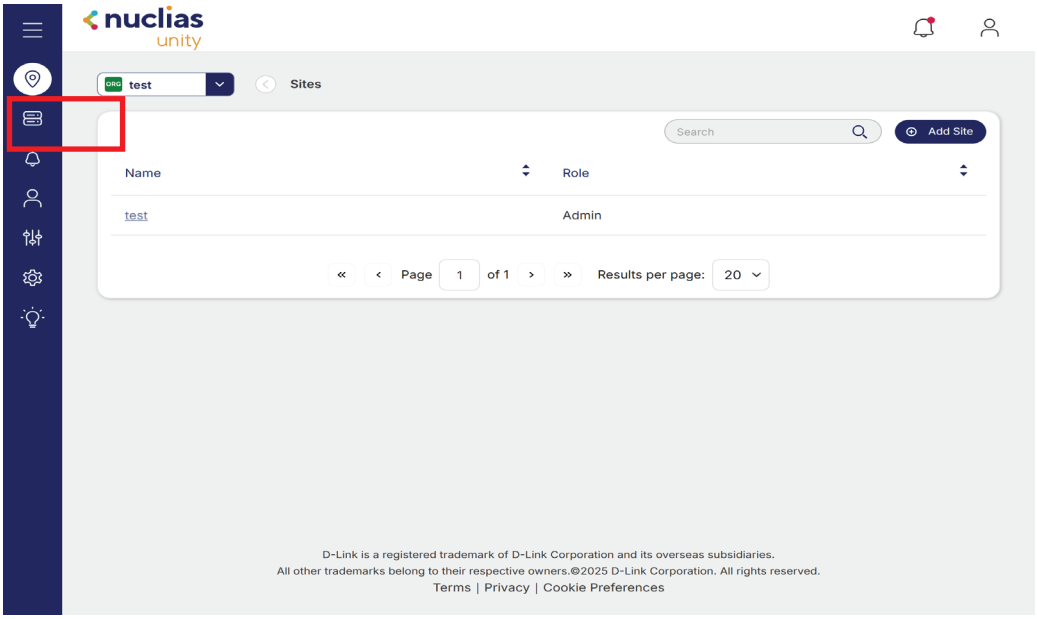
Nuclias Unity Nuclias Proxy **Add Device**

Go to the Nuclias Unity cloud platform and select the appropriate **Organization** from the menu.

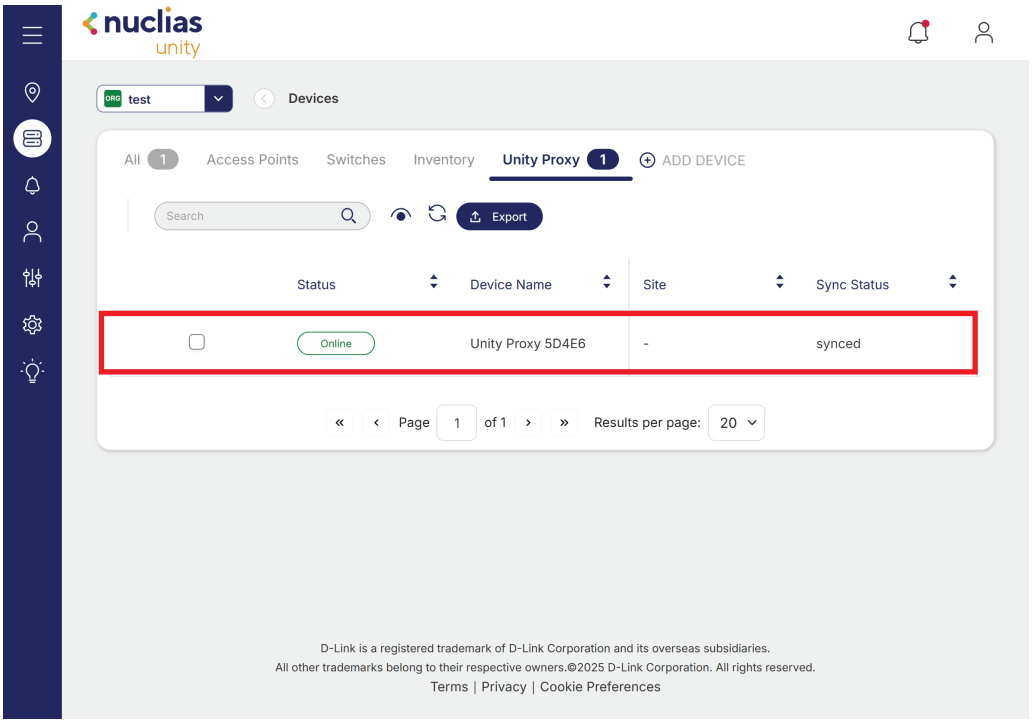


Nuclias Unity Nuclias Proxy **Add Device**

From the left-side menu bar, navigate to Devices.

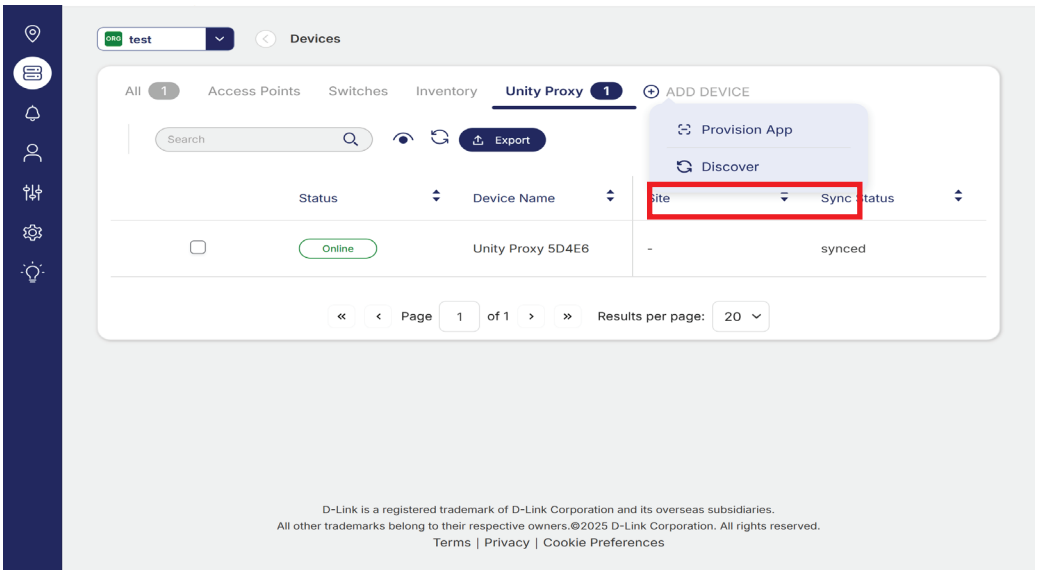


In the Device session, ensure the device name appears along with the last five digits of the **Proxy ID**, and confirm the status is **Online**.

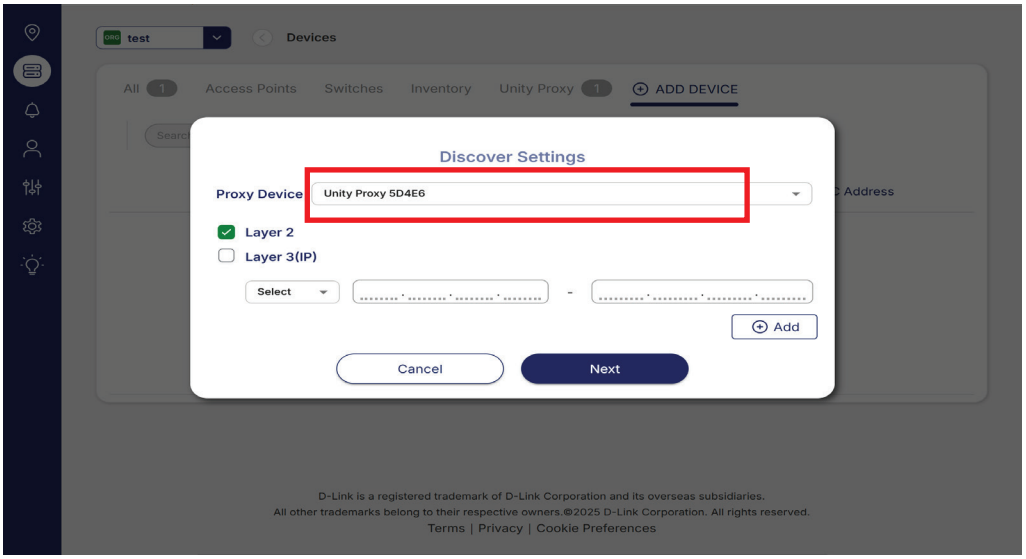


Nuclias Unity Nuclias Proxy **Add Device**

Click Add Device, then select Discover to begin searching for available devices.

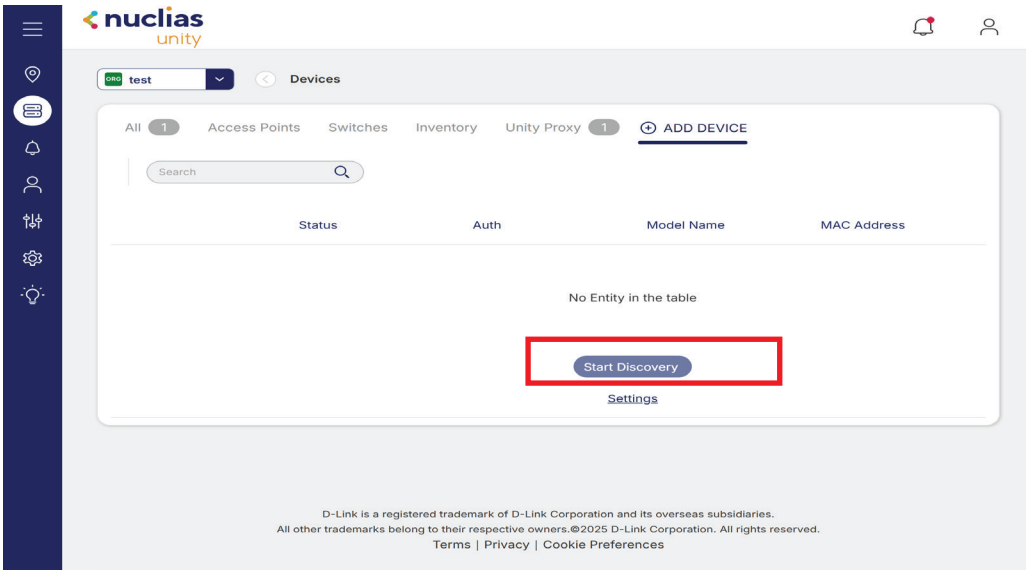


In the Proxy Device list, locate and select the Unity Proxy using the last five digits of its Unity Proxy ID for identification.

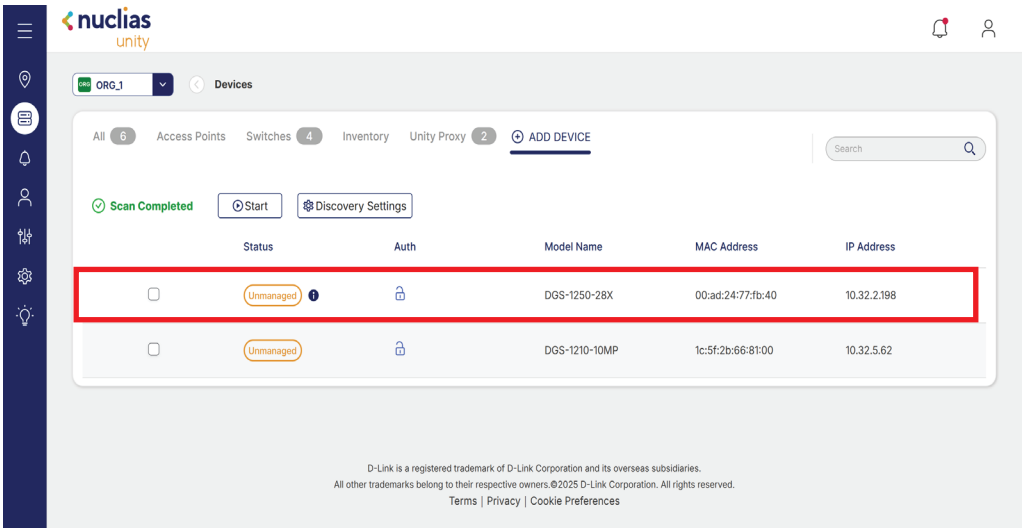


Nuclias Unity Nuclias Proxy **Add Device**

Click Start Discover to begin searching for available devices in Nuclias Unity.

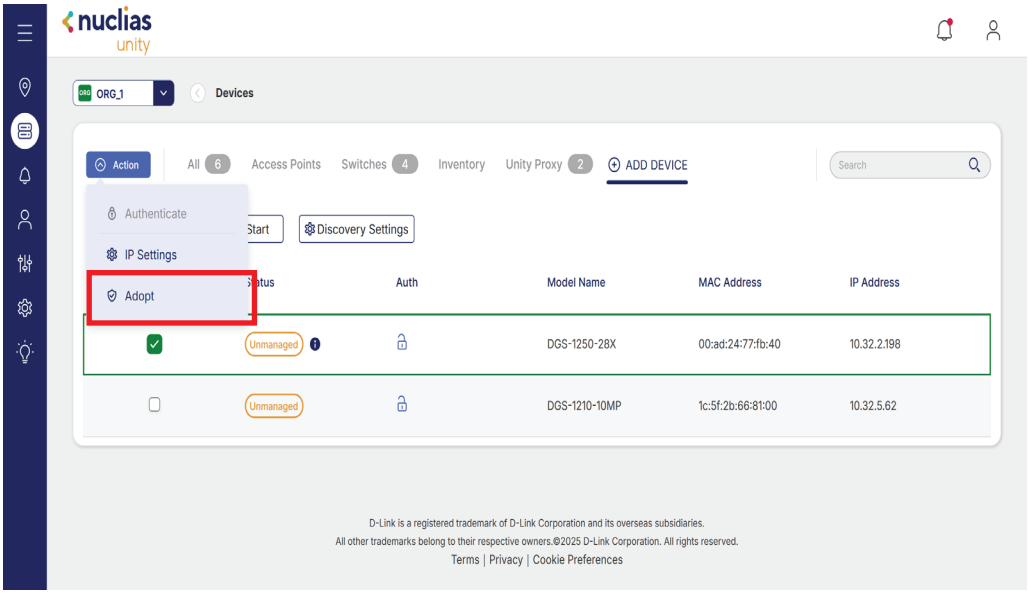


Once discovery is complete, the connected devices will appear in the list. Their initial status will show as Unmanaged.

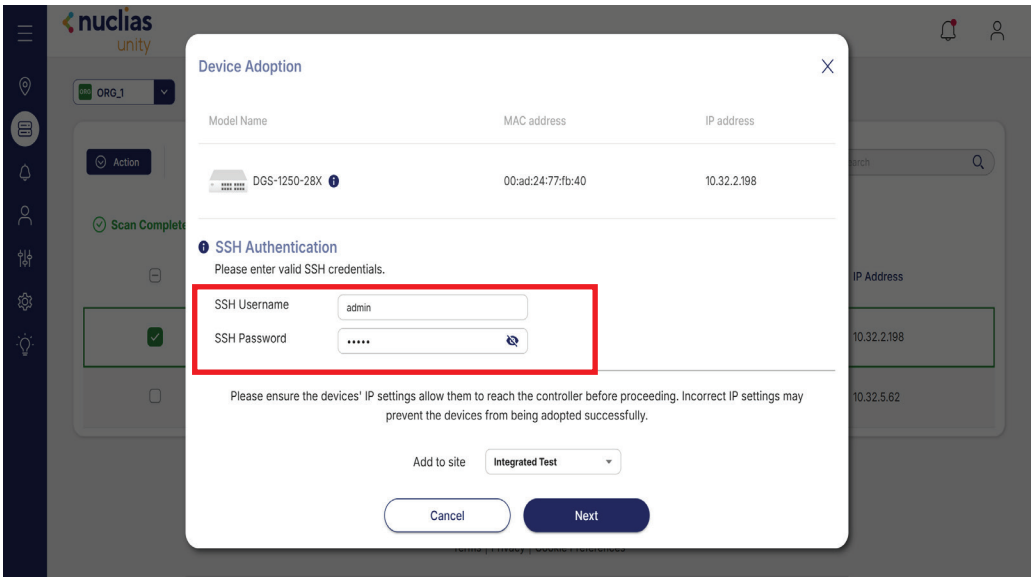


Nuclias Unity Nuclias Proxy Add Device

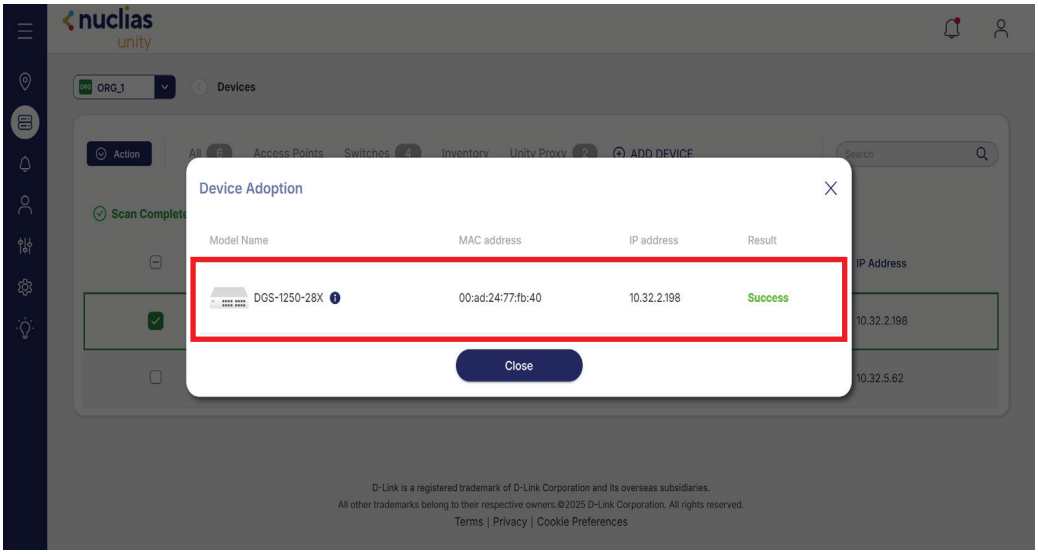
Select the device, go to the Action menu, and choose Adopt to begin managing it in Nuclias Unity.



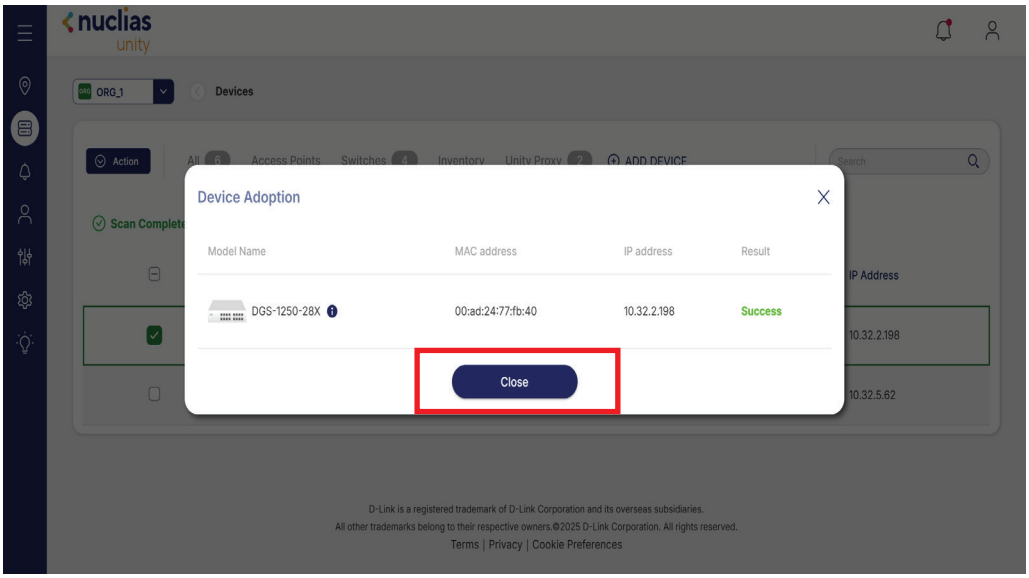
Enter a username and password for the adopted device, then click Next to continue.



The adopted devices will now display a Success status.

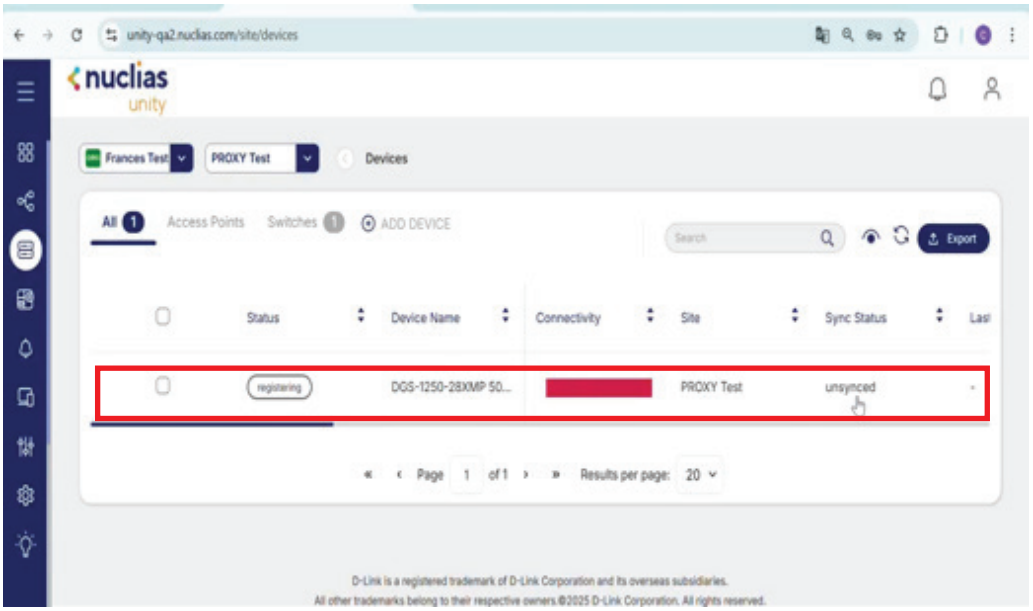


Confirming they have been successfully added and are being managed by Nuclias Unity.

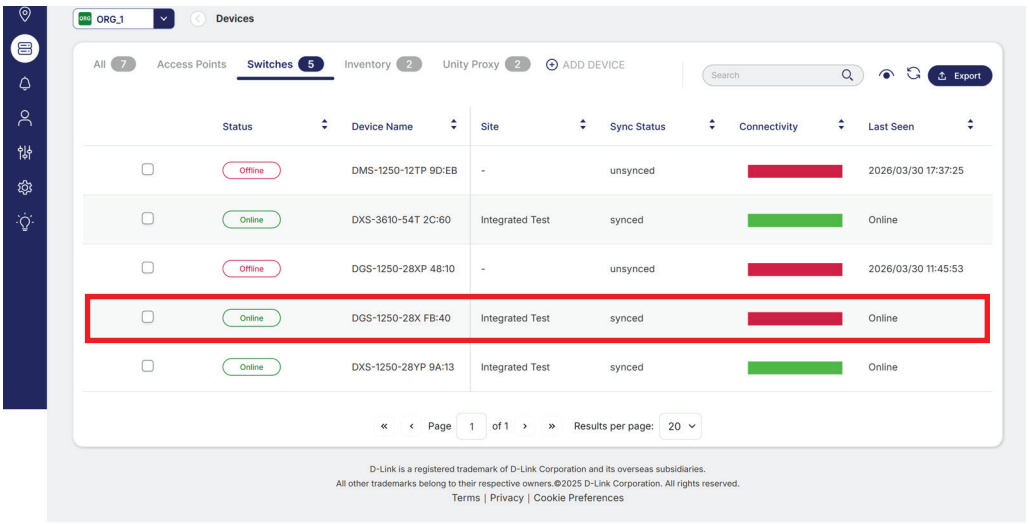


Nuclias Unity Nuclias Proxy **Add Device**

If the device status still shows Registering or Unsynced, wait a few minutes or refresh your browser to allow time for the connection to update.



After a few minutes or refreshing the page, the device status will update to Online and Syncing, indicating it is now properly connected and synchronizing with Nuclias Unity.



Portal Overview

The D-Link Nuclias Unity portal is a centralized, cloud-based network management platform designed to simplify the deployment, monitoring, and configuration of switches and access points across multiple sites. The intuitive web interface allows administrators to manage their entire network infrastructure from a single location

Platform Structure

Nuclias Unity uses a hierarchical management structure consisting of Organization, Site, and Devices. The Organization serves as the top-level structure, Sites represent individual physical locations or branches, and devices such as switches and access points are assigned within each Site. This design enables scalable and efficient multi-site network management.

User Interface Layout

The portal interface is organized into three main areas: the Top Navigation Bar, the Left Navigation Menu, and the Main Workspace Panel. The top navigation bar allows you to select the Organization and Site, view notifications, and access user profile settings. The left navigation menu provides quick access to key management sections such as Dashboard, Topology, Devices,Wi-Fi Planner, Events, Clients, Firmwar Managements, Settings, and Resource Center. The main workspace panel displays configuration pages, monitoring data, and device management controls.

Dashboard Overview

The Dashboard provides a real-time summary of your network status. It displays the number of connected switches and access points, their online or offline status, traffic statistics, top devices and SSIDs by usage, wireless uplink and downlink activity, as well as alerts and notifications for quick monitoring and troubleshooting.

Device Management

The Devices section allows administrators to view and manage all adopted devices within a Site. From this page, you can monitor device status, check CPU and memory usage, review PoE power consumption, and access configuration options for individual switches and access points.

Topology View

The Topology section provides a visual representation of the network layout. It shows how devices are interconnected through wired and wireless links, displays device names or MAC addresses, indicates online or offline status, and offers zoom and filtering tools for easier navigation and troubleshooting.

Configuration and Profiles

The Settings and Profiles sections allow administrators to configure wireless SSIDs, wired network settings, port profiles, and captive portal options. These centralized configuration tools ensure consistent policy deployment and simplified network management across all managed Sites.

Nuclias Unity Interface Overview

Organization and Site Overview

Nuclias Unity uses a hierarchical structure based on Organization and Site to simplify multi-location network management.

Organization

An Organization is the highest-level management entity within Nuclias Unity. It represents your entire business, institution, or network environment. All Sites, devices, configurations, and administrative settings are managed under an Organization.

The Organization level allows you to:

- Define global administrative credentials
- Manage multiple Sites under one structure
- Maintain centralized control and visibilit
- Apply consistent policies across locations

Each deployment must have at least one Organization.

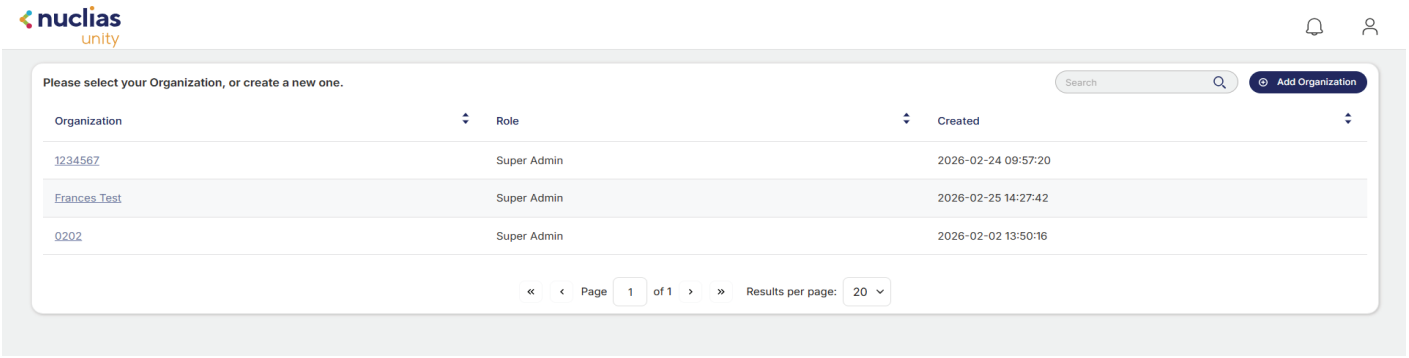
Site

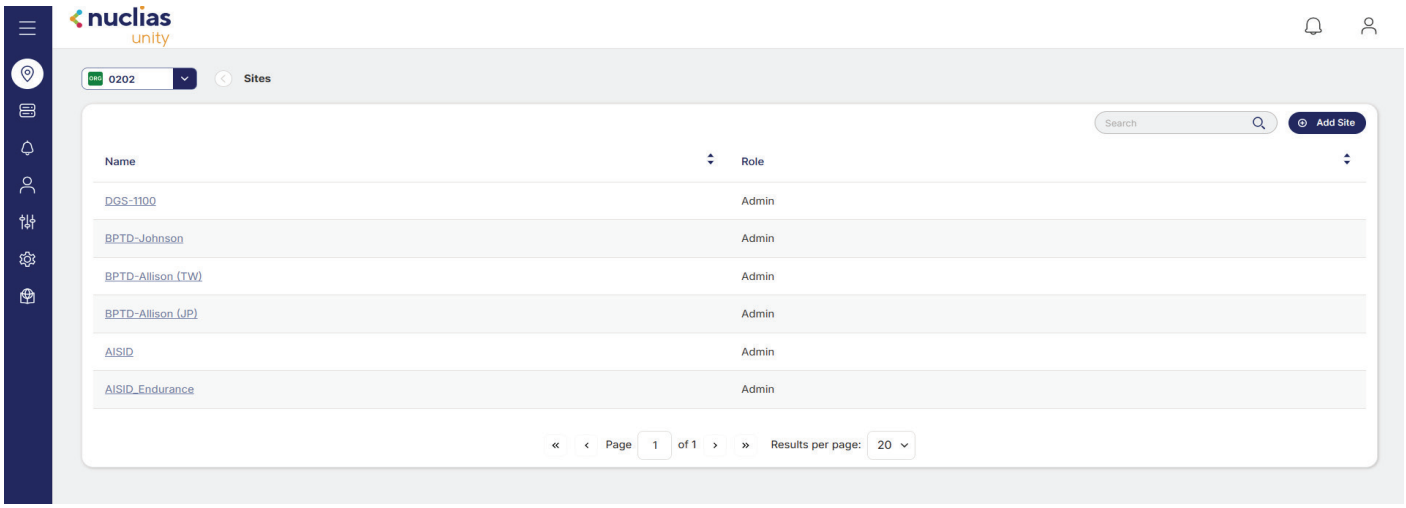
A Site represents a specific physical location or branch within the Organization, such as a headquarters, campus building, retail store, or remote office. Devices such as switches and access points are assigned to a Site. Network settings, monitoring data, and configurations are managed at the Site level.

The Site structure allows you to:

- Separate networks by location
- Manage devices independently per branch
- Monitor traffic and performance per Site
- Apply location-specific configurations

This Organization and Site structure ensures scalable, flexible, and efficient management for single-site and multi-site deployments.

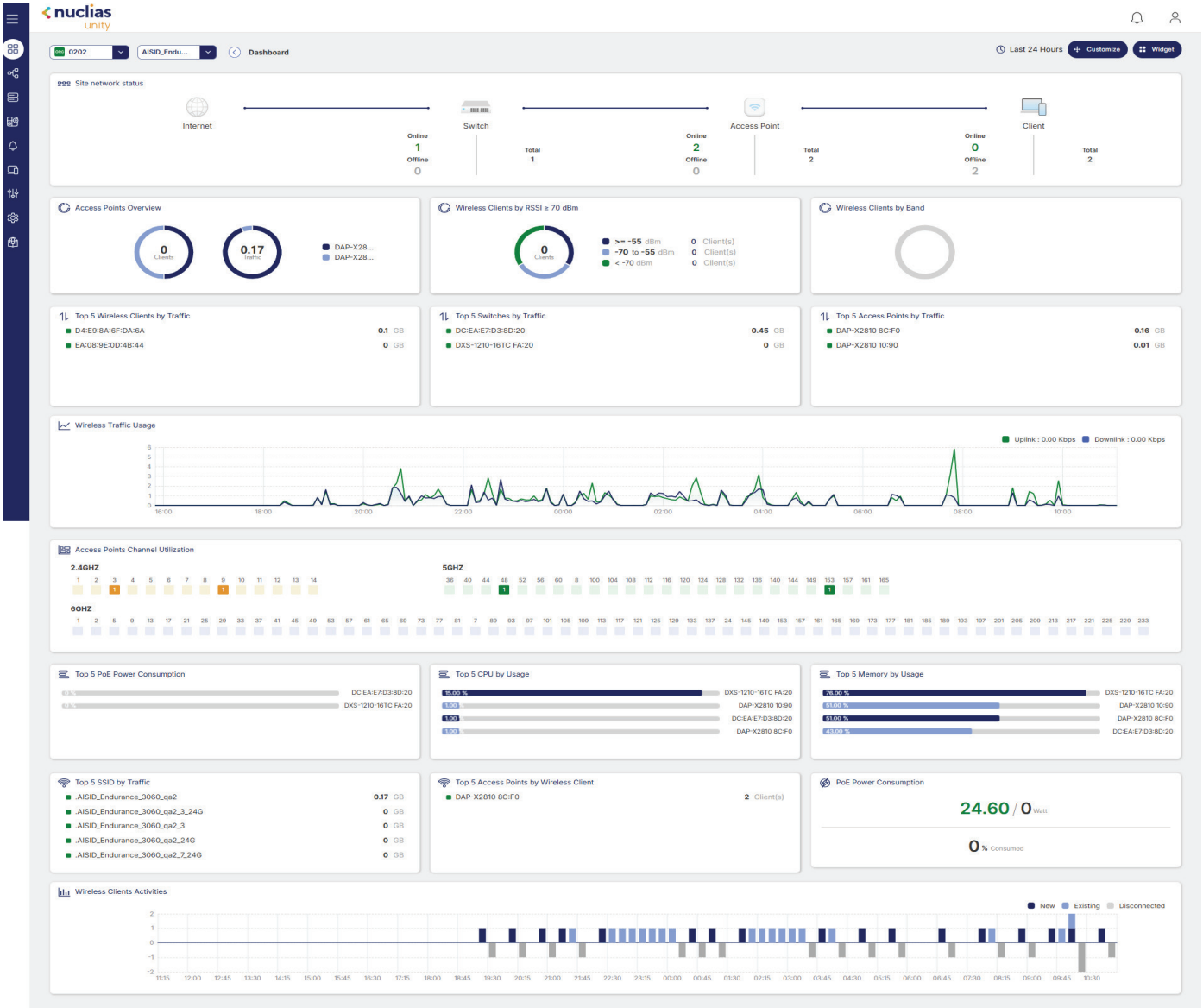




Nuclias Unity Dasboard

The Dashboard provides a centralized, real-time view of your network within the selected Organization and Site. It displays device status, traffic usage, topology, and key performance indicators, with customizable widgets for monitoring selected network performance metrics.

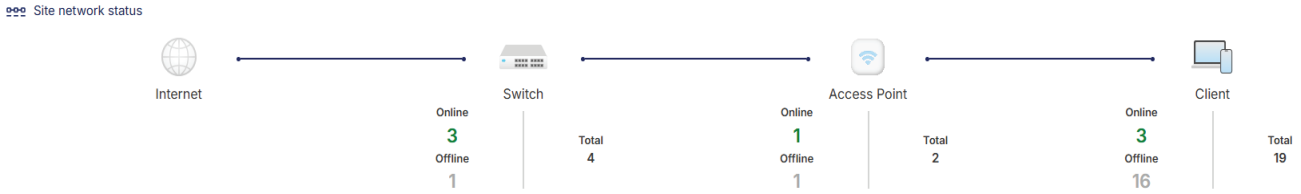
This section enables administrators to monitor switches, access points, and overall network health, quickly identify issues, and ensure stable network operation.



Nuclias Unity Dashboard Network

The Site Network Status section provides a real-time overview of device and client activity within the selected Site. It displays the total number of switches and access points, along with their current Online and Offline status for quick health monitoring.

This section also shows the total number of connected clients across the network, allowing administrators to monitor user activity and overall network load. By consolidating device and client information in one view, the Site Network Status helps ensure efficient monitoring and faster troubleshooting.



Nuclias Connect Dashboard **Network**

The Access Point Overview provides a summary of client connections and traffic activity across all managed access points within the selected Site. It displays the total number of connected wireless clients and the overall traffic usage, including uplink and downlink data.

This overview helps administrators monitor wireless network utilization, evaluate client distribution, and ensure optimal performance across access points.

Wireless Clients by RSSI ≥ -70 dBm

This section displays the number of wireless clients with an RSSI value greater than or equal to -70 dBm, indicating strong signal strength and stable connection quality. Monitoring RSSI levels helps administrators assess wireless coverage performance and identify potential signal or placement issues.

Wireless Clients by Band

This section displays the distribution of wireless clients across different frequency bands, such as 2.4 GHz, 5 GHz, and 6 GHz. It helps administrators understand band utilization, optimize load balancing, and ensure efficient wireless performance.

Top 5 Wireless Clients and Access Points by Traffic

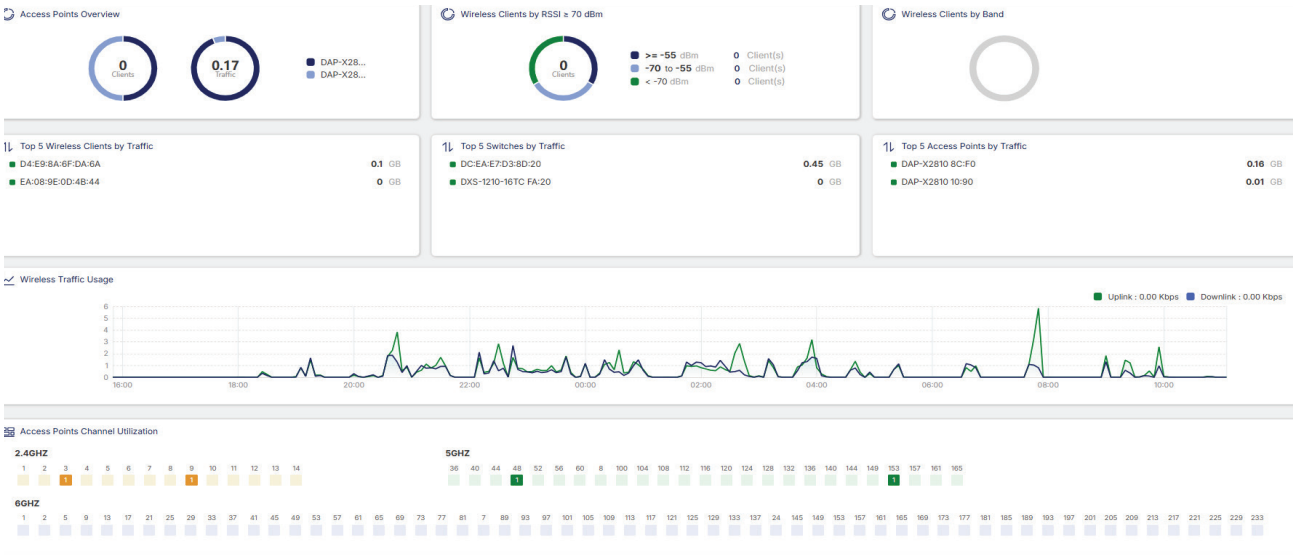
This section displays the top five wireless clients and access points ranked by traffic usage. It helps administrators identify high-bandwidth users and heavily utilized access points for better monitoring and performance optimization.

Wireless Traffic Usage

This section provides an overview of total wireless traffic across the selected Site, including uplink and downlink data. It enables administrators to monitor bandwidth consumption, analyze usage trends, and ensure efficient wireless network performance.

Access Point Channel Utilization

This section shows how access points are using available channels across the 2.4 GHz, 5 GHz, and 6 GHz bands. It helps administrators monitor channel congestion, optimize channel allocation, and improve overall wireless network performance.



Nuclias Unity Dashboard Clients

This section provides a summary of each SSID's performance, including total traffic usage, number of connected wireless clients, and client activity. It enables administrators to monitor usage patterns, evaluate network load per SSID, and optimize wireless performance and user experience.

Top 5 SSID by Traffic

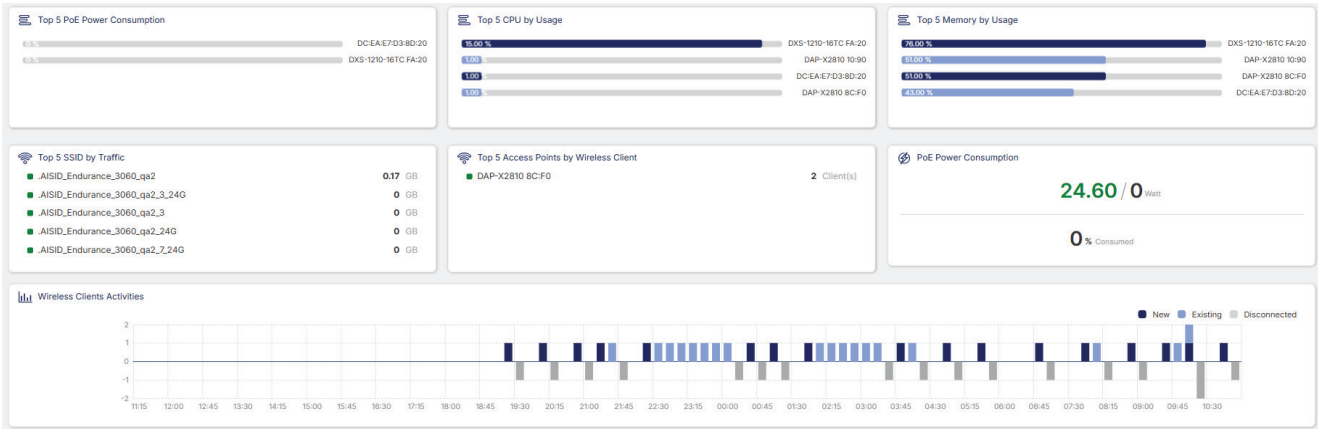
This section displays the top five SSIDs ranked by total traffic usage. It helps administrators identify the most heavily utilized wireless networks and monitor bandwidth distribution across SSIDs.

Top 5 Access Points by Wireless Clients

This section displays the top five access points with the highest number of connected wireless clients. It helps administrators monitor client distribution, identify heavily loaded access points, and optimize wireless capacity planning.

Wireless Client Activities

This section provides insights into wireless client behavior, including connection duration, traffic usage, and activity trends. It helps administrators monitor user activity, identify unusual patterns, and ensure optimal wireless network performance.



The detailed information about each managed switch includes CPU usage, memory usage, and PoE power consumption. Monitoring these metrics helps administrators assess device performance, detect potential overloads, and ensure stable and efficient network operation.

Top 5 PoE Power Consumption

This section displays the top five switches consuming the most PoE (Power over Ethernet) power. It helps administrators monitor power usage, manage PoE resources efficiently, and identify devices that may require attention due to high power consumption.

Top 5 CPU by Usage

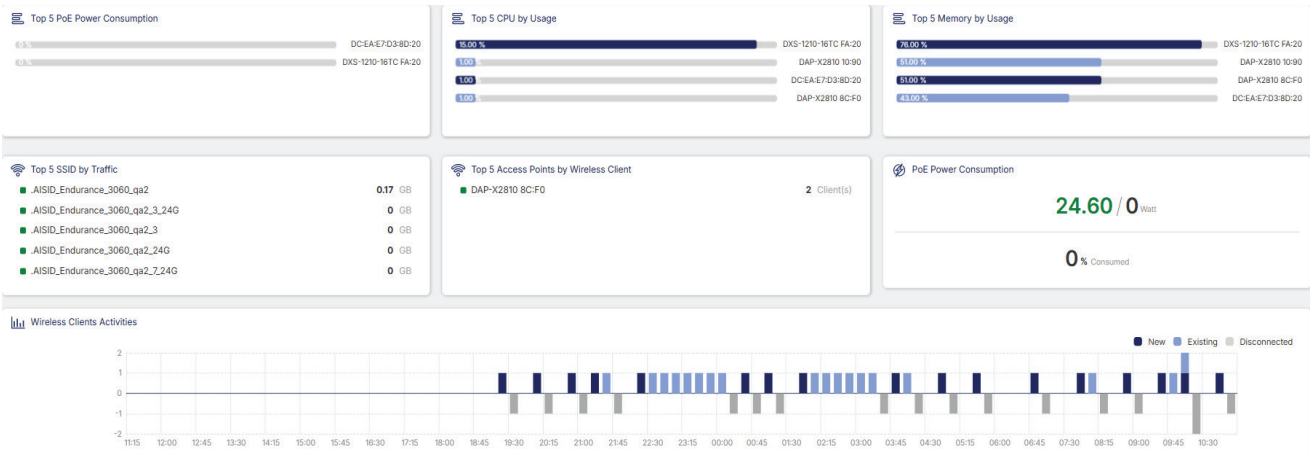
This section shows the top five switches or devices with the highest CPU usage. It helps administrators identify devices under heavy processing load, monitor performance trends, and take proactive measures to prevent network issues.

Top 5 Memory by Usage

This section displays the top five switches or devices with the highest memory usage. Monitoring memory utilization helps administrators identify devices under heavy load, optimize performance, and prevent potential network slowdowns or failures.

PoE Power Consumption

This section shows the total PoE power being consumed by all connected devices, measured in watts. It helps administrators monitor power usage, ensure sufficient PoE capacity, and manage energy distribution efficiently across the network.

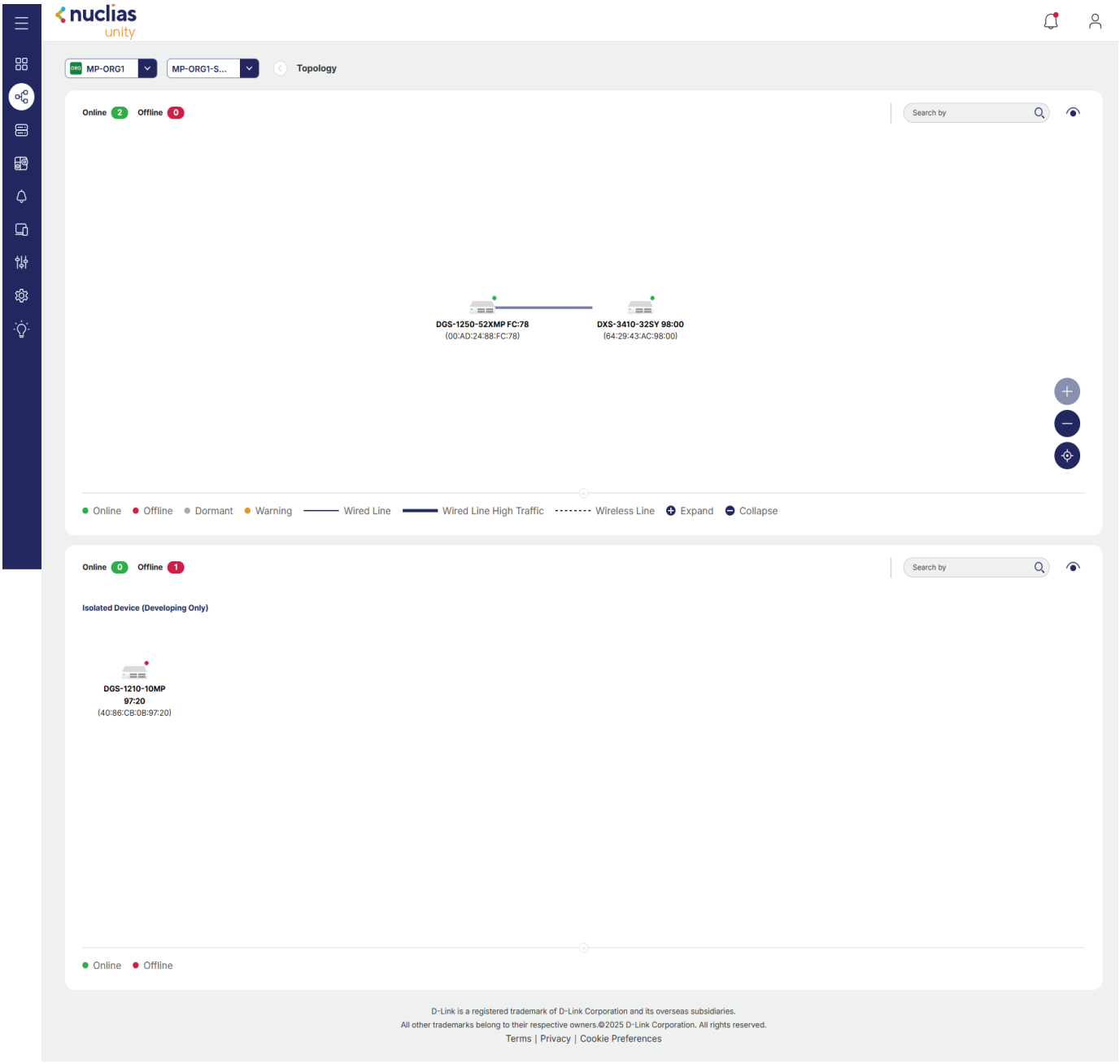


Nuclias Unity Topology

The Topology section in Nuclias Unity provides a graphical representation of your network infrastructure within the selected Site. It visually displays how switches, access points, and connected devices are interconnected through wired and wireless links.

The topology shows device names or MAC addresses, indicates online and offline status, and allows administrators to zoom, search, and filter devices for easier navigation. This visual layout helps simplify network monitoring, troubleshooting, and overall infrastructure management.

To access the Topology view after logging in, click Topology from the left-side menu bar. This will open the graphical network overview for the selected Organization and Site.



Nuclias Unity Topology

The topology diagram displays all discovered and connected network devices, including **Access Points, Switches,** and other managed devices within the selected Organization and Site. Each device is clearly indicated along with its current status, showing whether it is **Online** or **Offline**, helping administrators quickly identify connectivity issues or inactive equipment.

Device relationships can manually mapped to illustrate how network components communicate with each other. This graphical overview simplifies troubleshooting by enabling users to trace connections and identify potential problem points within the network infrastructure.

At the bottom of the topology page, users can choose how connections are displayed by selecting either:

Wired Links — Shows physical Ethernet connections between switches and other wired devices.

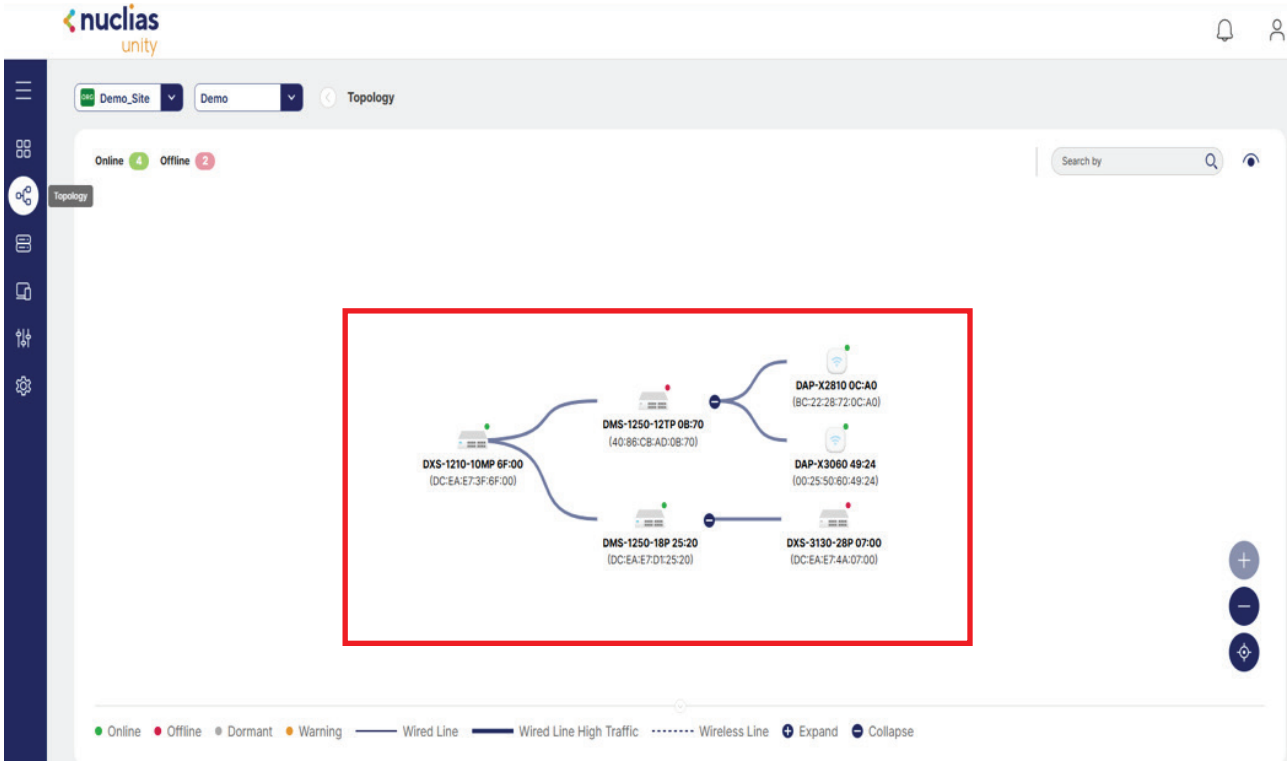
Switching between these options allows administrators to generate a connection diagram tailored to either the wired or wireless network environment for easier analysis and monitoring.

If you want, I can also make a short version, step-by-step procedural version, or a UI tooltip version depending on how formal your manual needs to be.

Nuclias Unity Topology

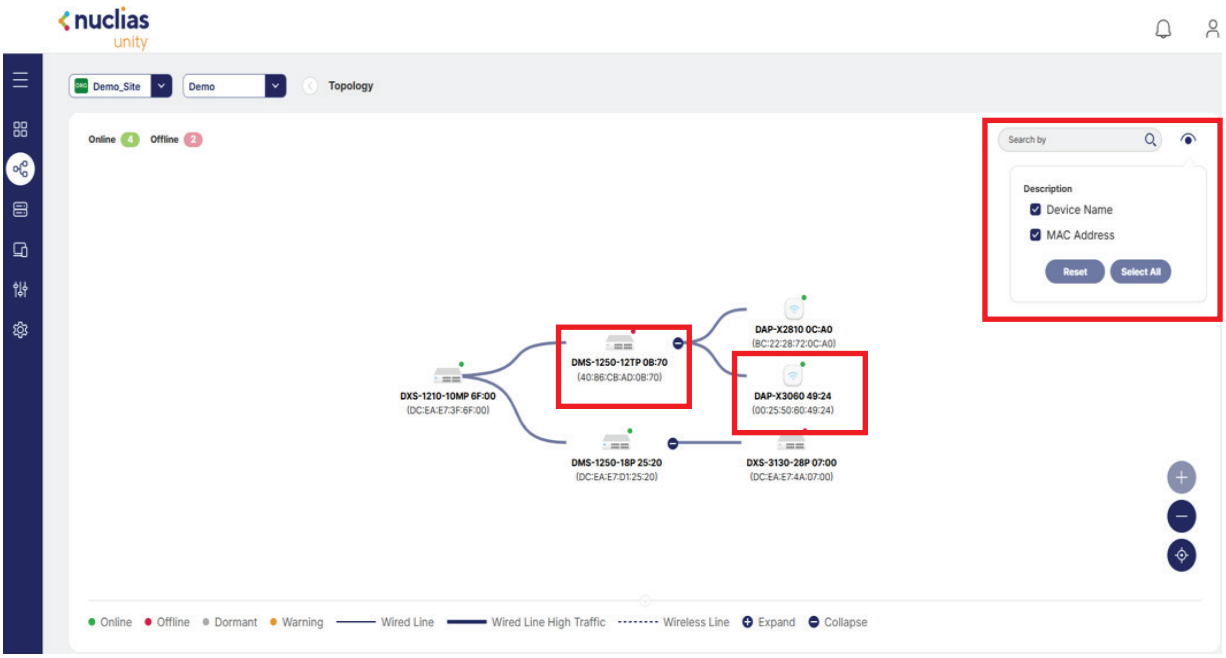
In the Topology, you can visually see how network devices are connected to one another within the network infrastructure. Each device is displayed with key information, including its **Connection Relationships, Online** or **Offline Status**, **Device Name,** and **MAC Address**, allowing administrators to quickly identify and verify devices.

This visual layout helps users understand network structure at a glance, making it easier to monitor device availability, confirm connectivity, and troubleshoot potential network issues.



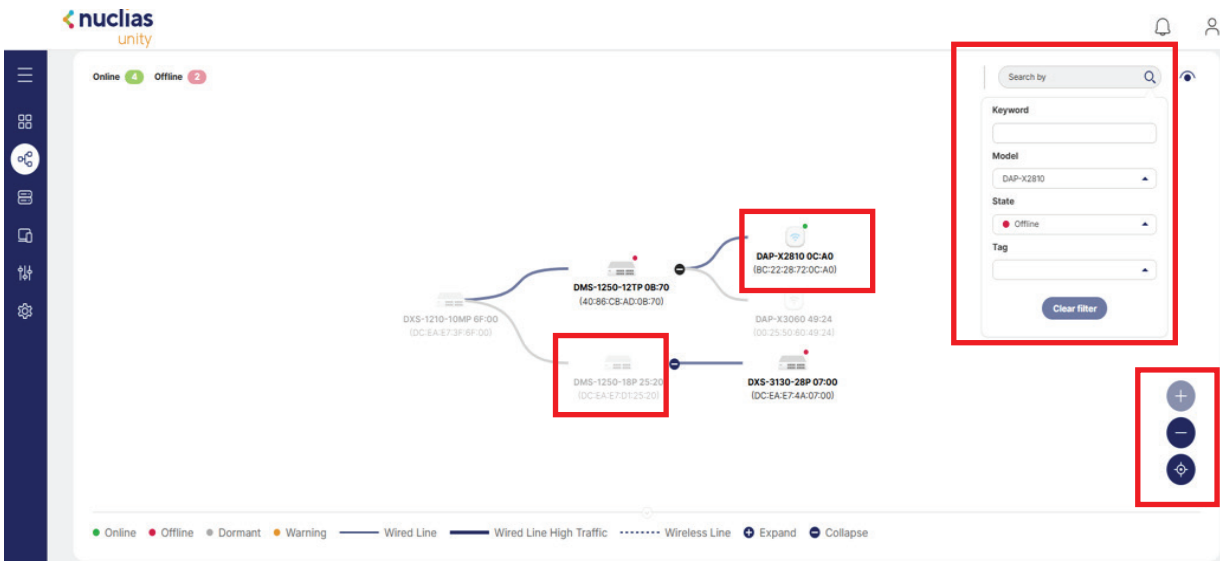
Nuclias Unity Topology

In the **top-right corner,** click the **Eye** icon to select how device information is displayed in the connection diagram. You can choose to show either **Device Names** or **MAC Addresses**, allowing you to customize the topology based on your monitoring or troubleshooting needs.



In the **top-right corner**, use the search bar to filter devices by specific models. You can also apply filters to display only **Online** or **Offline Devices**, allowing you to quickly check device status within the topology.

Click the plus (+) or minus (–) icons to **Zoom In or Out** of the topology, allowing you to either see all connected devices at a glance or focus on specific devices and connections in greater detail.



Nuclias Unity Topology

In the **Topology** section, select any connected device to view detailed information about its status and performance. A panel will appear displaying the following options:

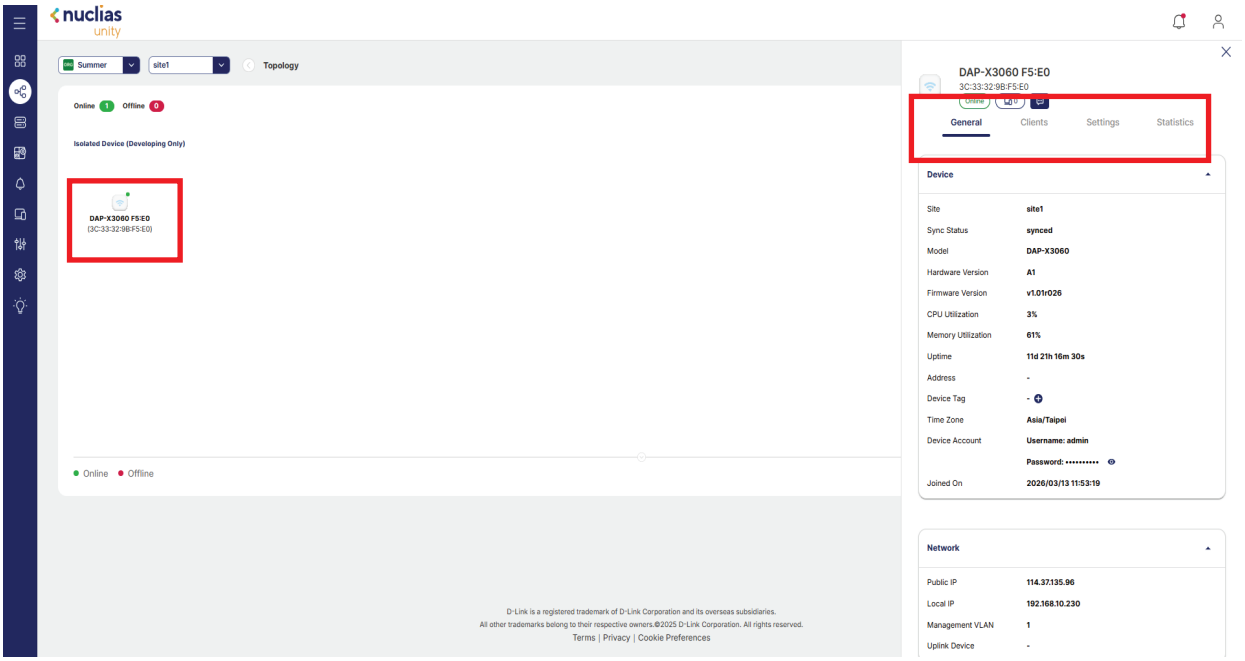
General: View basic device information such as device name, model, IP address, firmware version, and operational status.

Clients: Access information about connected clients, including client name, MAC address, IP address, connection type, and signal strength for wireless devices.

Settings: Modify device settings directly from the topology view, allowing quick configuration changes such as port settings, VLAN assignments, or wireless parameters without navigating away from the visual map.

Statistics: Monitor traffic statistics for the selected device, including Tx/Rx traffic volume, packet counts, and bandwidth utilization to assess performance and identify potential network issues.

This integrated view enables network administrators to efficiently manage devices, monitor connected clients, adjust configurations, and analyze traffic patterns directly from the network topology interface.



Nuclias Unity Devices

The Devices page provides centralized management and monitoring for all network devices adopted into Nuclias Unity, including switches and access points. From this section, administrators can view device status, configure settings, and monitor performance across the selected Organization and Site.

Device Overview

The Devices page displays a complete list of all managed devices within the selected site. Each device entry provides key perational information, allowing administrators to quickly understand network status and device health.

Displayed information typically includes:

- Device name and model
- Device type (Switch or Access Point)
- Online or offline status
- IP address and MAC address
- Firmware version
- Device uptime
- Connected client count
- Current operational status

This overview enables administrators to quickly identify devices that require attention or troubleshooting.

Device Status Monitoring

Administrators can monitor real-time device conditions directly from the Devices page. Status indicators help quickly determine whether devices are functioning normally.

Common status indicators include:

- Online — Device is connected and operating normally.
- Offline — Device is unreachable or disconnected from the network.
- Provisioning — Configuration is being applied.
- Updating — Firmware upgrade is in progress.

These visual indicators allow fast identification of network issues.

Device Management

Selecting a device opens its detailed management panel, where administrators can perform configuration and monitoring tasks such as:

- Viewing device information and statistics
- Managing network settings
- Monitoring traffic usage
- Checking connected clients
- Rebooting devices remotely
- Updating firmware
- Editing device name or location

Changes applied through Nuclias Unity are automatically synchronized with the selected device.

Search and Filter Options

To simplify device management in large deployments, the Devices page includes search and filtering tools.

Administrators can:

- Search devices by name or model
- Filter devices by status (Online or Offline)
- View devices by type (Switches or Access Points)
- Quickly locate specific devices within the network

These tools help improve operational efficiency when managing multiple devices.

Device Adoption Status

Devices must be authenticated and adopted before they can be managed through Nuclias Unity. Once adopted:

- Devices appear under the selected Organization and Site.
- Configuration settings can be applied remotely.
- Monitoring and analytics become available.

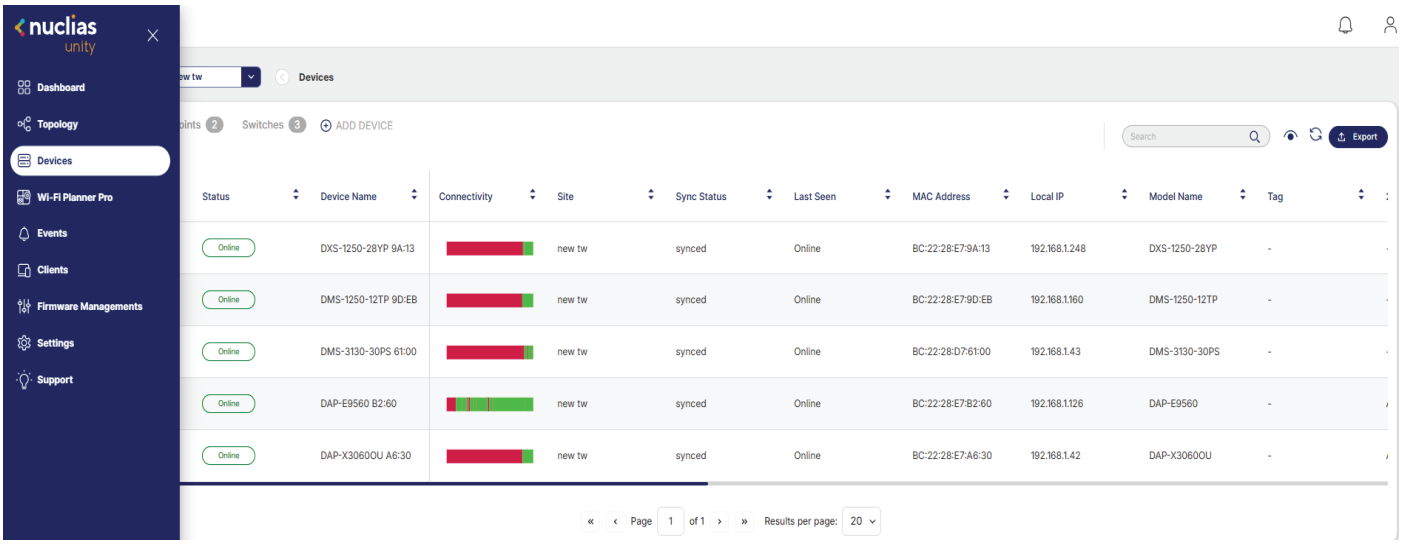
If a device appears offline after adoption, verify network connectivity and device configuration.

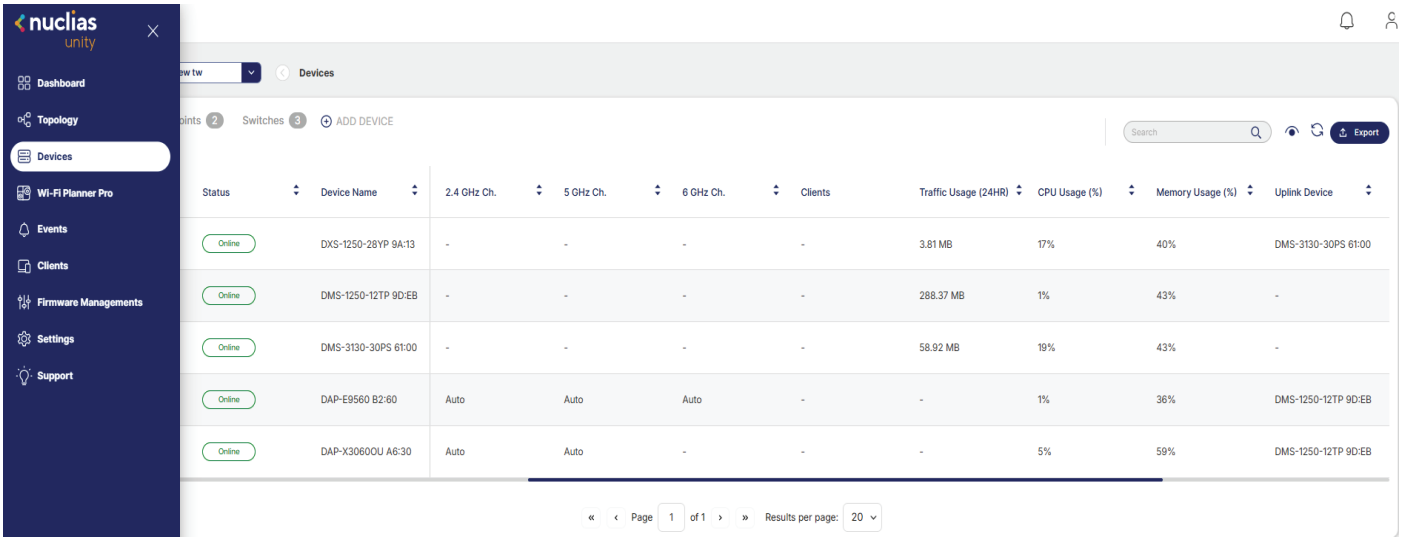
Device Actions

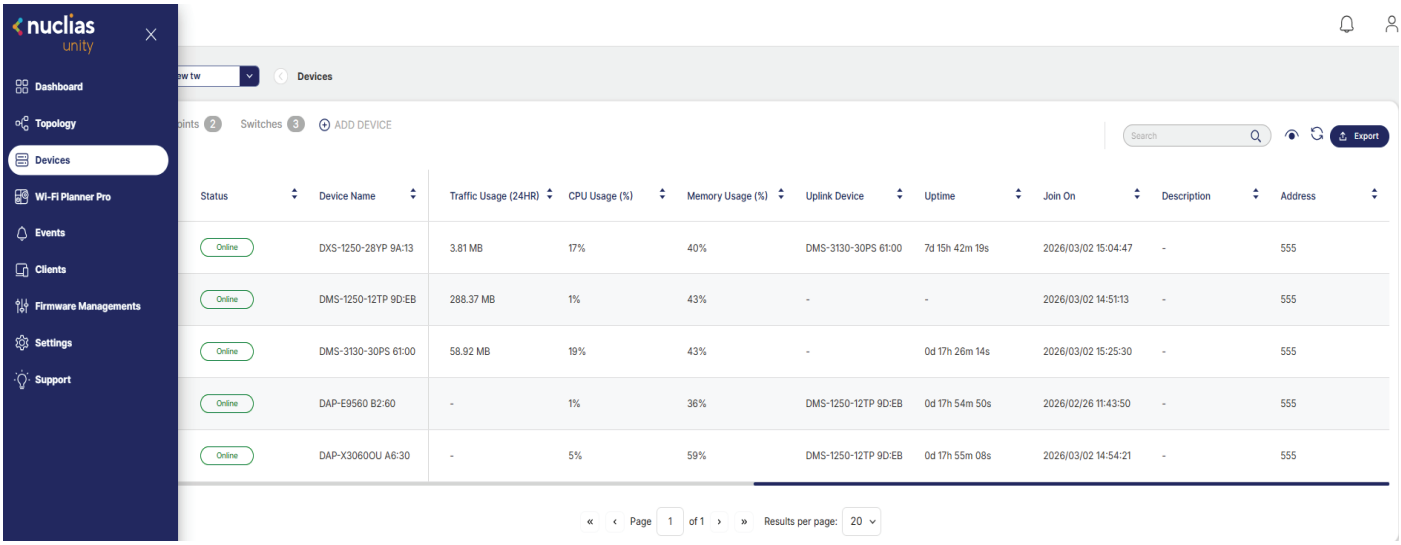
Administrators can perform bulk or individual actions directly from the Devices page, including:

- Adopt devices
- Reboot devices
- Upgrade firmware
- Remove devices from management
- Refresh device status

These actions allow efficient centralized control without accessing devices locally.


nuclias unity
Dashboard
Topology
Devices
Wi-Fi Planner Pro
Events
Clients
Firmware Managements
Settings
Support
Devices
Switches 3
ADD DEVICE
Search
Export
Status
Device Name
Connectivity
Site
Sync Status
Last Seen
MAC Address
Local IP
Model Name
Tag
Online
DXS-1250-28YP 9A:13
new tw
synced
Online
BC:22:28:E7:9A:13
192.168.1.248
DXS-1250-28YP
DMS-1250-12TP 9D:EB
BC:22:28:E7:9D:EB
192.168.1.160
DMS-1250-12TP
DMS-3130-30PS 61:00
BC:22:28:D7:61:00
192.168.1.43
DMS-3130-30PS
DAP-E9560 B2:60
BC:22:28:E7:B2:60
192.168.1.126
DAP-E9560
DAP-X3060OU A6:30
BC:22:28:E7:A6:30
192.168.1.42
DAP-X3060OU
Page 1 of 1
Results per page: 20


nuclias unity
Dashboard
Topology
Devices
Wi-Fi Planner Pro
Events
Clients
Firmware Managements
Settings
Support
Devices
Switches 3
ADD DEVICE
Search
Export
Status
Device Name
2.4 GHz Ch.
5 GHz Ch.
6 GHz Ch.
Clients
Traffic Usage (24HR)
CPU Usage (%)
Memory Usage (%)
Uplink Device
Online
DXS-1250-28YP 9A:13
3.81 MB
17%
40%
DMS-3130-30PS 61:00
DMS-1250-12TP 9D:EB
288.37 MB
1%
43%
DMS-3130-30PS 61:00
58.92 MB
19%
43%
DAP-E9560 B2:60
Auto
36%
DMS-1250-12TP 9D:EB
DAP-X3060OU A6:30
5%
59%
Page 1 of 1
Results per page: 20

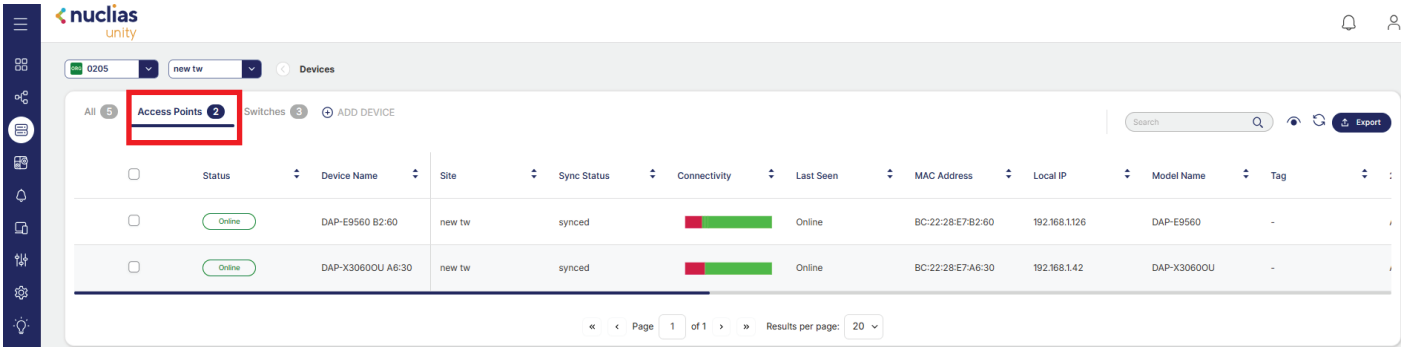

nuclias unity
Dashboard
Topology
Devices
Wi-Fi Planner Pro
Events
Clients
Firmware Managements
Settings
Support
Devices
Switches 3
ADD DEVICE
Search
Export
Status
Device Name
Traffic Usage (24HR)
CPU Usage (%)
Memory Usage (%)
Uplink Device
Uptime
Join On
Description
Address
Online
DXS-1250-28YP 9A:13
3.81 MB
17%
40%
DMS-3130-30PS 61:00
7d 15h 42m 19s
2026/03/02 15:04:47
555
DMS-1250-12TP 9D:EB
288.37 MB
1%
43%
2026/03/02 14:51:13
DMS-3130-30PS 61:00
58.92 MB
19%
43%
0d 17h 26m 14s
2026/03/02 15:25:30
DAP-E9560 B2:60
1%
36%
DMS-1250-12TP 9D:EB
0d 17h 54m 50s
2026/02/26 11:43:50
DAP-X3060OU A6:30
5%
59%
0d 17h 55m 08s
2026/03/02 14:54:21
Page 1 of 1
Results per page: 20

Nuclias Unity Devices

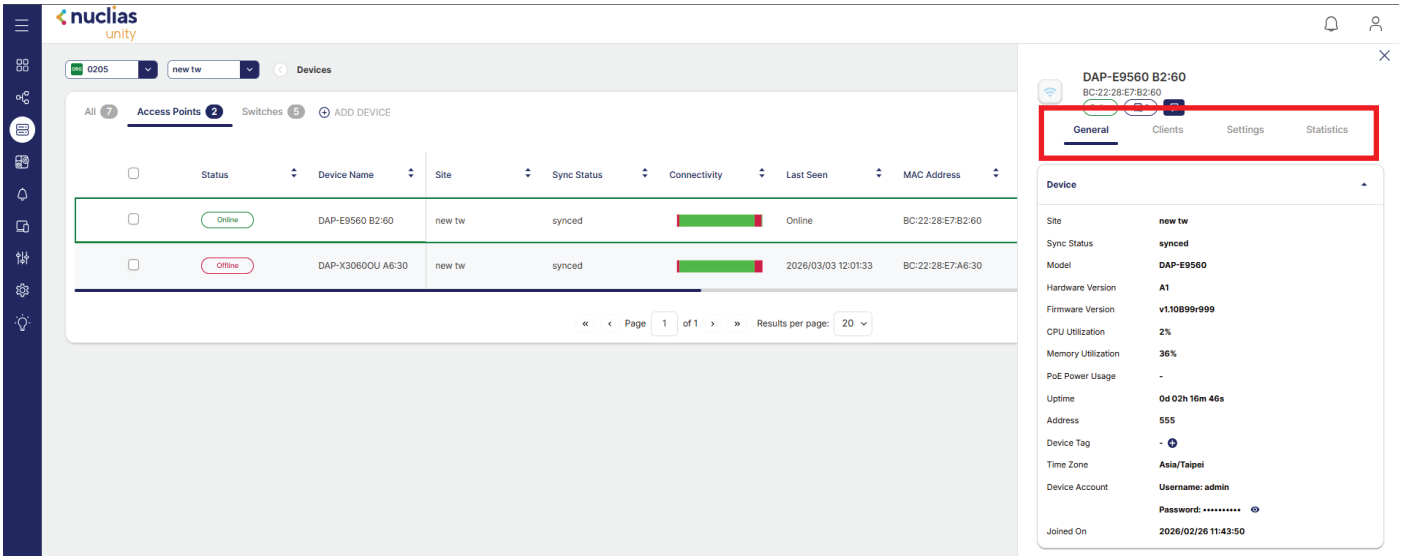
Field	Description
Status	Displays the current operational state of the device, indicating whether it is online or offline.
Device Name	The assigned name used to identify the device within Nuclias Unity.
Connectivity	Shows the device's connection type and current network connection status.
Site	Indicates the Site where the device is deployed and managed.
Sync Status	Displays whether the device configuration is synchronized with the Nuclias Unity platform.
Last Seen	Shows the most recent time the device communicated with the management platform.
MAC Address	The unique hardware identifier assigned to the device's network interface.
Local IP	The IP address assigned to the device within the local network.
Model Name	Identifies the specific model of the device.
Tag	A customizable label used to group or organize devices for easier management.
2.4 GHz Ch	Displays the wireless channel currently used by the 2.4 GHz radio.
5 GHz Ch	Displays the wireless channel currently used by the 5 GHz radio.
6 GHz Ch	Displays the wireless channel currently used by the 6 GHz radio (if supported).
Clients	Shows the number of connected clients currently associated with the device.
Traffic Usage (24HR)	Displays the total network traffic transmitted and received by the device over the past 24 hours.
CPU Usage (%)	Indicates the current processor utilization of the device.
Memory Usage (%)	Shows the percentage of memory currently being used by the device.
Uplink Devices	Identifies the upstream device providing network connectivity.
Uptime	Displays how long the device has been running since its last restart.
Join On	Shows the date and time when the device was adopted into Nuclias Unity.
Description	A customizable field for adding notes or additional information about the device.
Address	Displays the physical location or installation address assigned to the device.

Nuclias Unity Devices Access Points

The Devices option provides detailed information for both Access Points and Switches, allowing you to monitor status, performance, and connectivity from a centralized view. It also displays the number of connected devices, helping administrators quickly monitor network activity and client connections. From the **left-side menu**, go to **Devices** and select **Access Points** to view and manage your access points.

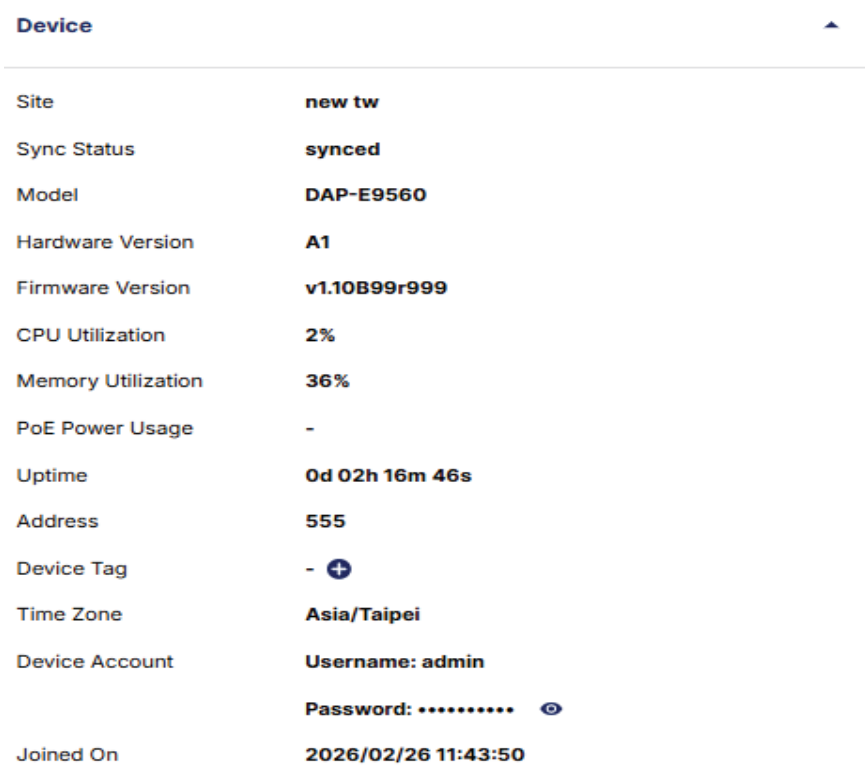


Select any Access Point from the list to view detailed information and configuration settings for the selected device. It provides detailed information under the **General, Clients, Settings, and Statistics sections** for the connected Access Point.



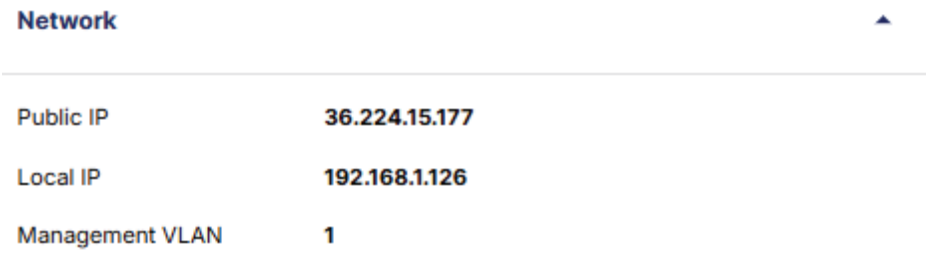
Nuclias Unity Devices Access Points **General**

The General section contains information about the **Device** details, **Network** settings, **Wireless SSIDs**, and **Radio** configuration.

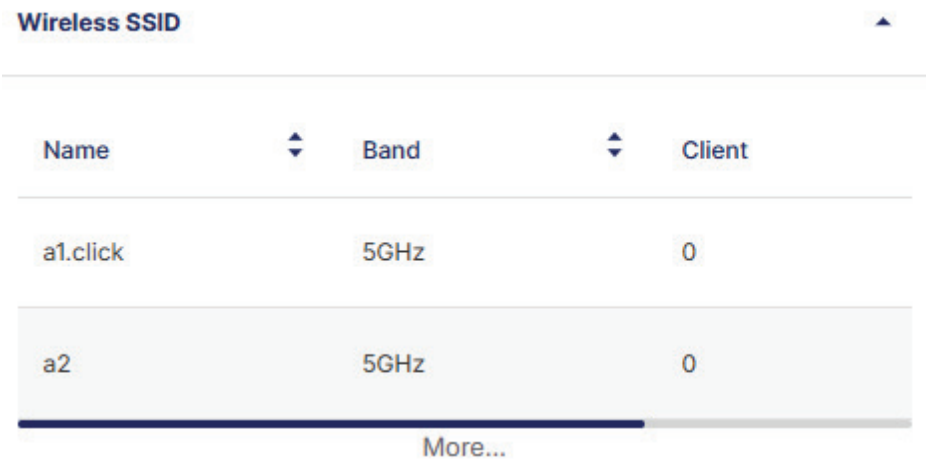


Parameter	Description
Site	Displays the site where the device is currently assigned.
Sync Status	Indicates whether the device configuration is synchronized with Nuclias Unity.
Model	Shows the device model name.
Hardware version	Displays the hardware revision of the device.
Firmware version	Indicates the current firmware running on the device.
CPU Utilization	Shows the current percentage of CPU usage.
Memory Utilization	Displays the percentage of memory currently in use.
PoE Power Usage	Indicates the amount of Power over Ethernet (PoE) power being consumed.
Uptime	Shows how long the device has been operating since the last reboot.
Address	Displays the configured physical location or address of the device.
Device Tag	Shows the assigned tag used for device identification or grouping.
Time Zone	Indicates the time zone configured for the device.
Device Accout	• Username – Shows the login username configured for the device. • Password – Indicates the password associated with the device account (hidden for security purposes).
Joined On	Shows the date and time when the device was added to Nuclias Unity.

Nuclias Unity Devices Access Points

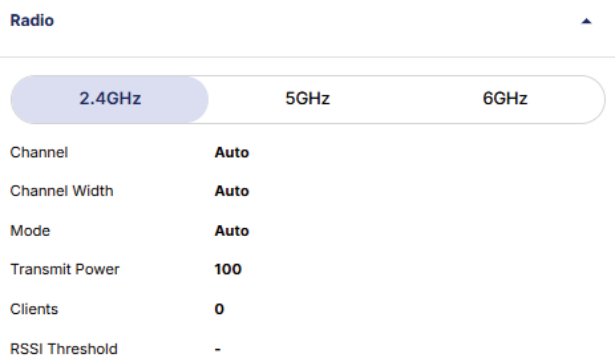


Parameter	Description
Public IP	Enter the administrative username that is used to access the configuration settings for all access points in the network.
Local IP	Enter the administrative password that is used to access the configuration settings for to all access points in the network.
Management VLAN	Check the box to enable the console function.



Parameter	Description
Name	Displays the SSID (wireless network name) broadcast by the Access Point.
Band	Indicates the wireless frequency band used by the SSID (2.4 GHz, 5 GHz, or 6 GHz).
Client	Shows the number of wireless clients currently connected to the SSID.
Action	Provides available management options for the SSID, such as viewing details or modifying settings.

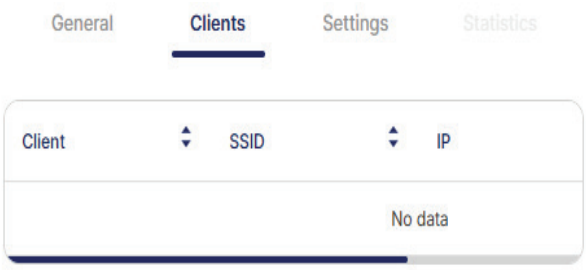
Nuclias Unity Devices Access Points



Parameter	Description
Channel	Displays the wireless channel currently used by the radio.
Channel Width	Indicates the channel bandwidth (e.g., 20 MHz, 40 MHz, 80 MHz or 160MHz).
Mode	Shows the radio operation mode (e.g., 802.11a/b/g/n/ac/ax/be).
Transmit Power	Displays the current transmission power of the radio.
Clients	Shows the number of clients connected to this radio.
RSSI Threshhold	Indicates the minimum signal strength (RSSI) required for clients to maintain a stable connection.

Nuclias Unity Devices Access Points **Clients**

The Clients section provides detailed information about each wireless client connected to the Access Point. It includes the following fields:

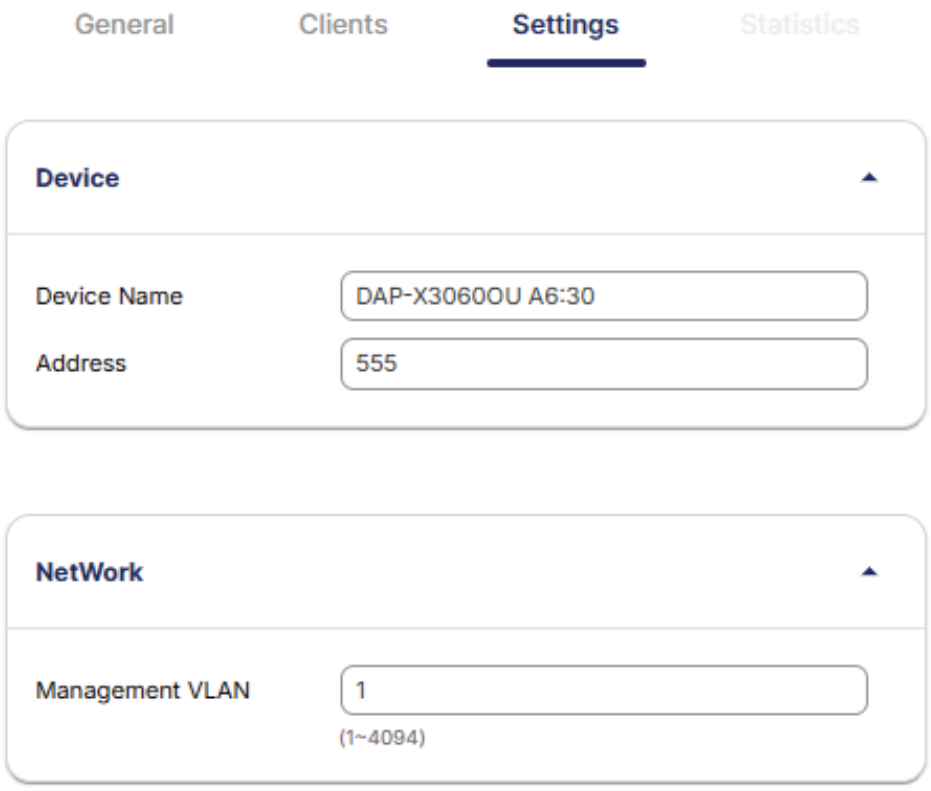


Parameter	Description
Client	Displays the name or identifier of the connected device.
SSID	Shows the wireless network (SSID) the client is connected to.
IP	Displays the IP address assigned to the client.
Signal	Indicates the signal strength (RSSI) of the client's connection to the Access Point.

Nuclias Unity Devices Access Points **Settings**

The Settings section contains configuration details for the connected Access Point, organized into the following categories:

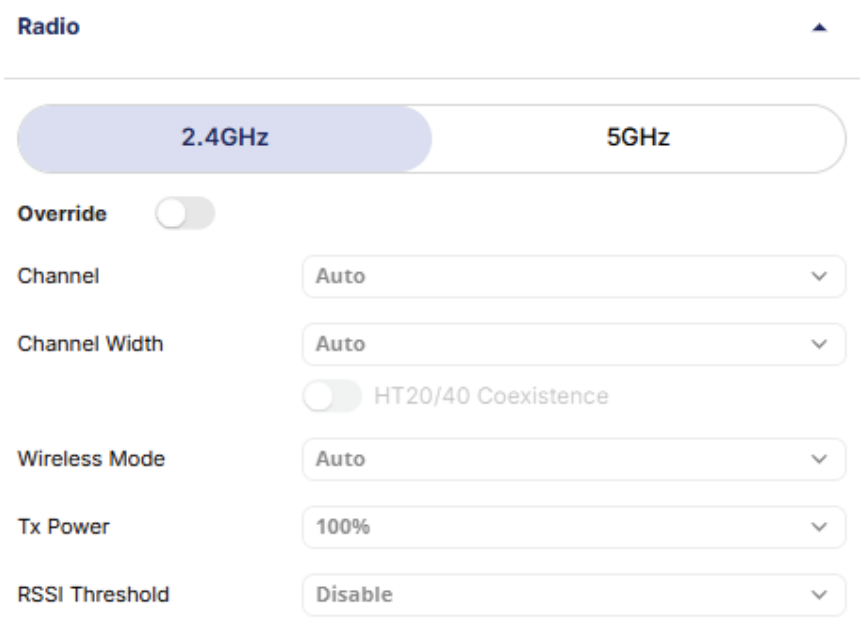
- Device – Provides device-related configuration options and basic system settings.
- Network – Displays and allows configuration of network parameters and connectivity settings
- Radio – Includes wireless radio configuration settings for the 2.4 GHz, 5 GHz, and 6 GHz bands.
- Management – Contains management and administrative settings used for device control and access.



Parameter	Description
Device Name	Displays the assigned name of the device for identification and management purposes.
Address	Shows the physical location or configured address of the device within the network deployment.
Management VLAN	Indicates the VLAN ID used for device management traffic and administrative access.

Nuclias Unity Devices Access Points

The Wireless Resource function in Nuclias Connect helps provides real-time RF management of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the 2.4GHz or 5GHz tab to view existing settings.



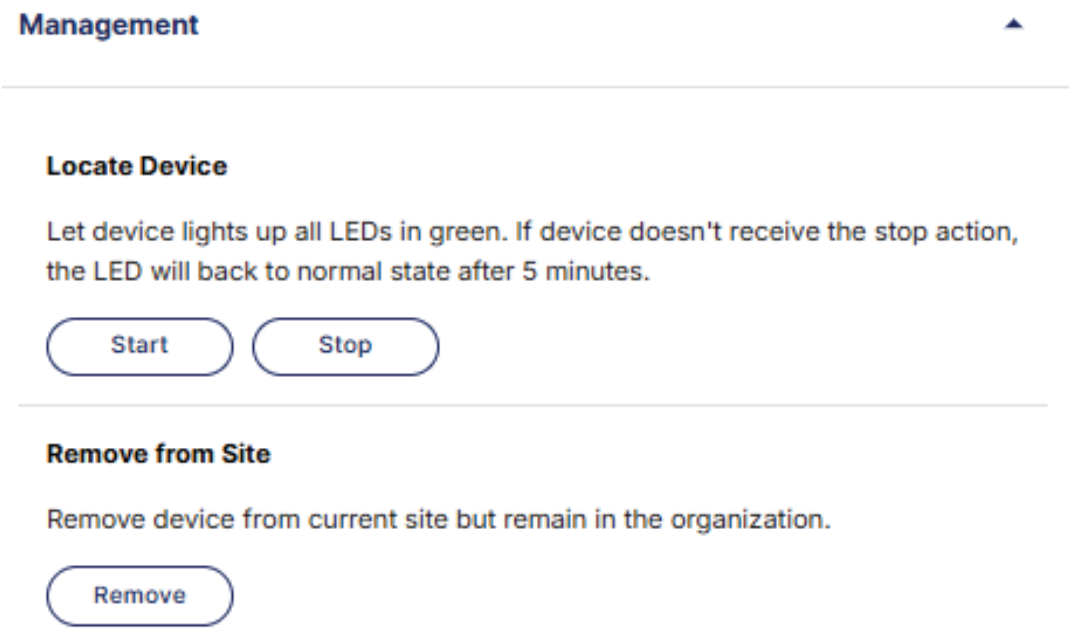
Parameter	Description
Channel	Displays the wireless channel currently used by the radio.
Channel Width	Indicates the bandwidth of the wireless channel (e.g., 20 MHz, 40 MHz, 80 MHz, or 160 MHz).
Wireless Mode	Shows the wireless standard supported by the radio (e.g., 802.11b/g/n/ax for 2.4 GHz, 802.11a/n/ac/ax for 5 GHz, or 802.11ax for 6 GHz).
Tx Power	Displays the transmission power level used by the radio to broadcast wireless signals.
RSSI Threshold	Defines the minimum signal strength required for clients to maintain a stable wireless connection.

Nuclias Unity Devices Access Points

The Management section provides administrative controls used to manage and maintain the device within the network. It allows administrators to perform device-level actions such as locating the device physically and removing it from the current Site when required.

Locate Device – Activates the device identification feature (such as LED blinking) to help physically locate the device within the deployment area.

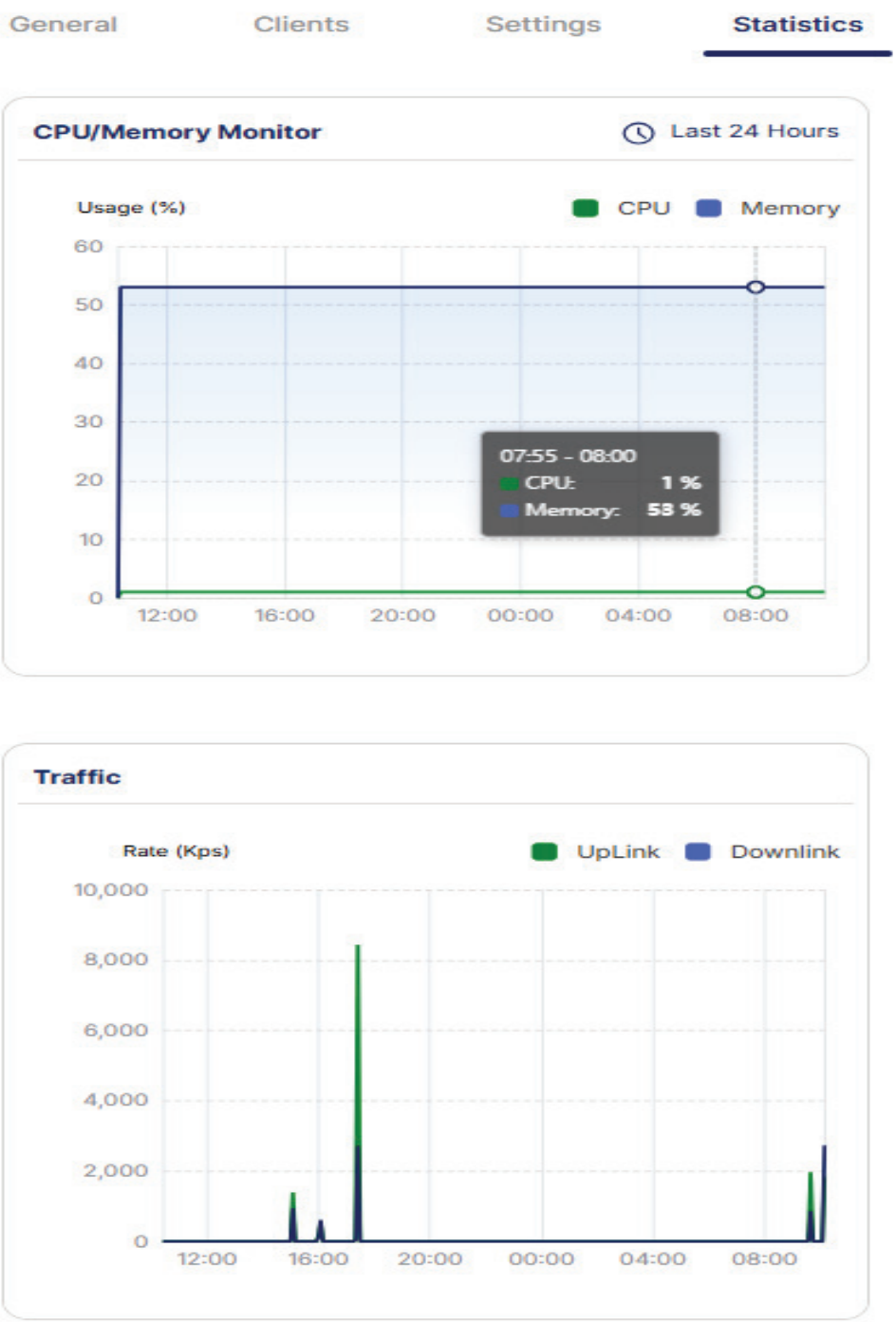
Remove from Site – Removes the device from the current Site, stopping centralized management under the selected Site but not from the Organization.



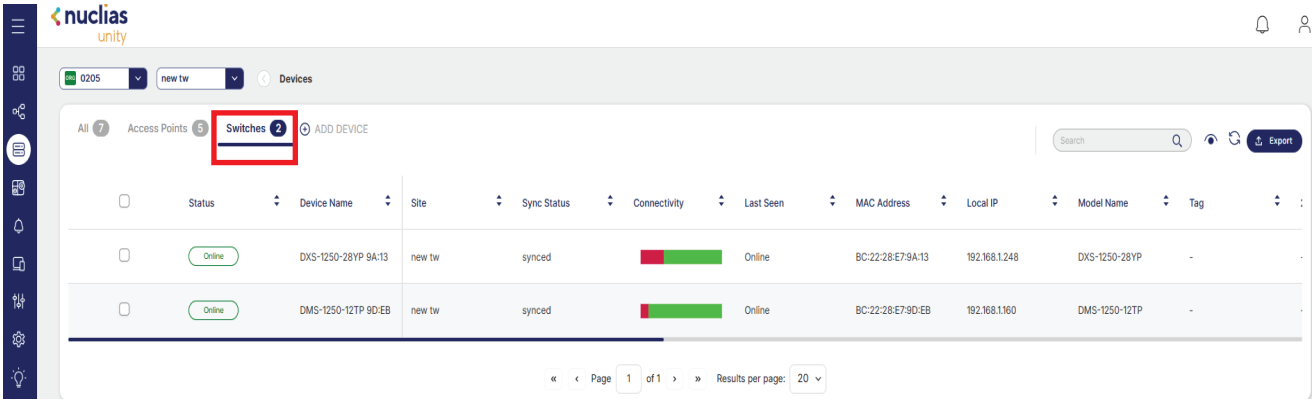
The Statistics section provides performance and traffic monitoring information for the device. It includes real-time and historical data related to CPU usage, memory utilization, and network traffic.

- CPU Monitor – Displays the current processor utilization of the device, helping administrators evaluate system performance.
- Memory Monitor – Shows memory usage to ensure sufficient resources are available for stable operation.
- Uplink Traffic – Indicates the amount of data transmitted from the device to the network or internet.
- Downlink Traffic – Displays the amount of data received by the device from the network or internet.

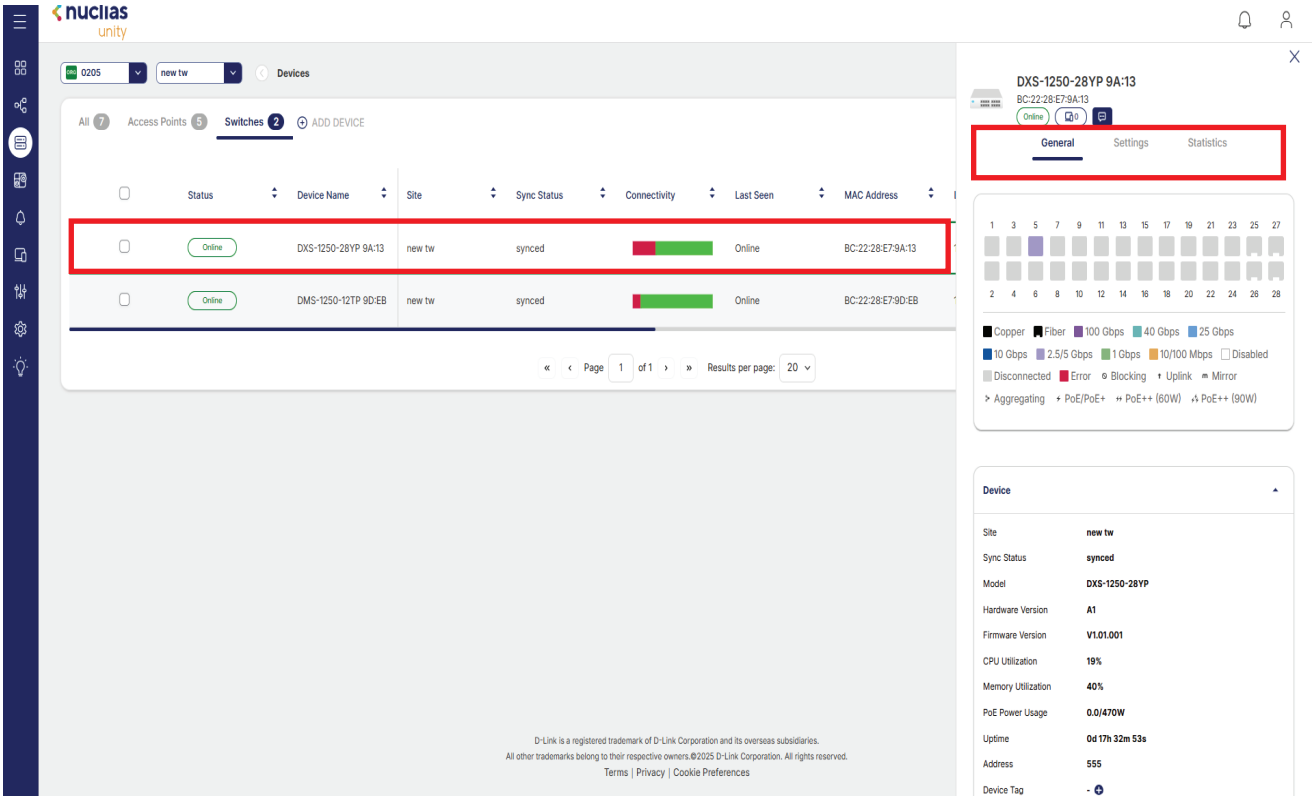
This information helps administrators monitor device performance and identify potential network or resource issues.



From the left-side menu bar, go to **Device** and select **Switches**. Here, you can view the total number of connected switches, along with their **status, model, MAC address, and other device details**. This section allows you to monitor and manage all switches connected to the network.

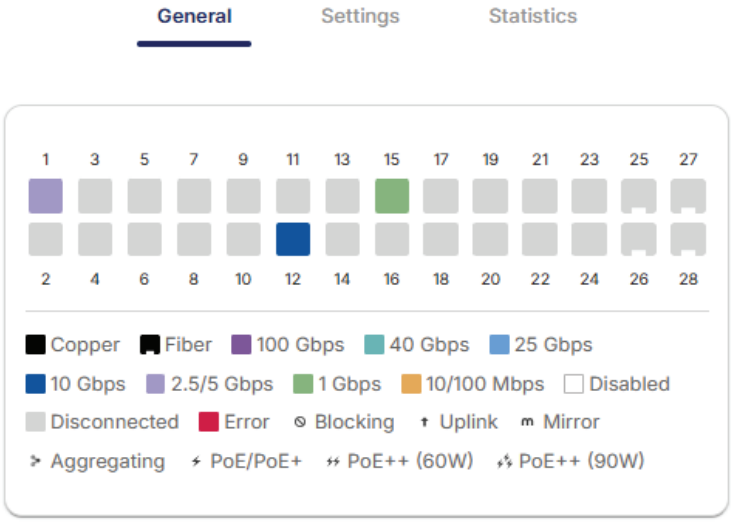


If switch support remote access then the navigate have General Settings and Statistic. Others the navigate have General, Ports, Settings and Statistics.



Nuclias Unity Devices Switches General

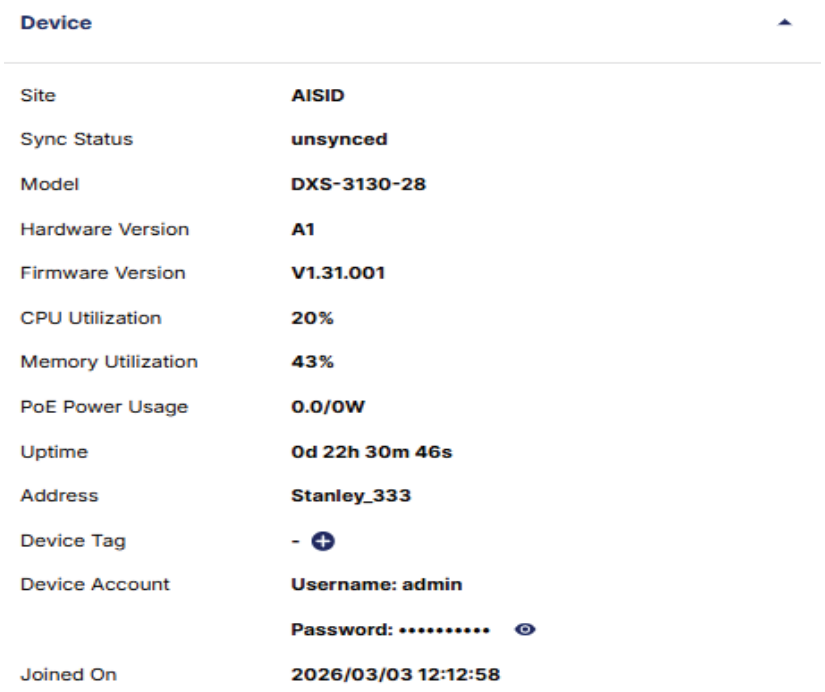
Under **General**, users can view information about the **Ports, Device, and Network**. The Ports section shows information about **Port Numbers, Port Speed, and Port Types**.



Parameter	Description
Port Number	Displays the identification number assigned to each physical port on the switch.
Copper	Indicates that the port uses a copper Ethernet interface (RJ-45) for network connectivity.
Fiber	Indicates that the port uses a fiber optic interface (such as SFP/SFP+/QSFP) for high-speed optical connectivity.
100 Gbps	Shows that the port supports or is operating at a maximum data transfer speed of 100 Gigabits per second.
40 Gbps	Indicates that the port supports or is operating at 40 Gigabits per second.
25 Gbps	Indicates that the port supports or is operating at 25 Gigabits per second.
10 Gbps	Indicates that the port supports or is operating at 10 Gigabits per second.
2.5/5 Gbps	Indicates that the port supports multi-gigabit speeds of 2.5 Gbps or 5 Gbps.
1 Gbps	Indicates that the port supports or is operating at 1 Gigabit per second.
10/100 Mbps	Indicates that the port supports 10 Mbps or 100 Mbps Ethernet speeds.
Disabled	Indicates that the port has been manually disabled and will not pass any network traffic.
Disconnected	Indicates that no device or cable is currently connected to the port.
Error	Indicates that the port has encountered an operational issue or fault that may affect connectivity.
Uplink	Indicates that the port is used to connect the switch to an upstream network device such as another switch or router.
Mirror	Indicates that the port is configured for port mirroring, allowing traffic to be copied for monitoring or analysis.
Aggregating	Indicates that the port is part of a Link Aggregation Group (LAG) to increase bandwidth and provide redundancy.
PoE/PoE+	Indicates that the port supports Power over Ethernet (PoE) or PoE+, allowing it to supply power to connected devices such as IP cameras, access points, or VoIP phones.
PoE++ (60W)	Indicates that the port supports high-power PoE++ with a maximum power output of 60 watts.
PoE++ (90W)	Indicates that the port supports ultra-high-power PoE++ with a maximum power output of 90 watts for devices requiring higher power.

Nuclias Unity Devices Switches

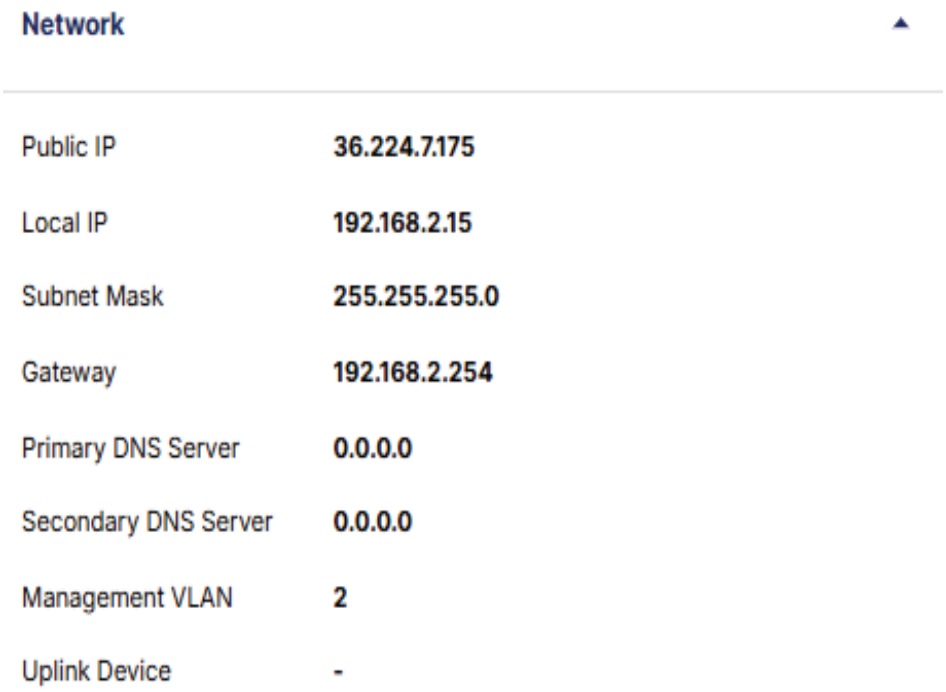
The Device section contains information about the physical details of the connected switch, including hardware-related information and device identification.



Parameter	Description
Site	Displays the site where the switch is currently assigned or deployed within the network.
Sync Status	Indicates whether the switch configuration is synchronized with the controller or management platform.
Model	Shows the model number of the connected switch.
Hardware Version	Displays the hardware revision of the switch.
Firmware Version	Indicates the current firmware version running on the switch.
CPU Utilization	Shows the percentage of CPU resources currently being used by the switch.
Memory Utilization	Displays the percentage of memory currently in use on the switch.
PoE Power Usage	Indicates the total amount of Power over Ethernet (PoE) power currently being used by connected devices.
Uptime	Shows the amount of time the switch has been running since the last reboot.
Address	Displays the IP address assigned to the switch.
Device Tag	Shows the label or tag assigned to the device for easier identification and management.
Device Account	Indicates the account or organization associated with the device in the management platform.
Joined On	Displays the date and time when the switch was added to the management system.

Nuclias Unity Devices Switches

The Network section contains all the information related to the switch's network connectivity, including IP addresses, subnet mask, gateway, DNS servers, management VLAN, and uplink device.



Parameter	Description
Public IP	Shows the public IP address assigned to the switch for external network access.
Local IP	Displays the local (private) IP address of the switch within the internal network.
Subnet Mask	Indicates the subnet mask used to define the network segment of the local IP.
Gateway	Shows the default gateway IP address used by the switch to communicate outside the local network.
Primary DNS Server	Displays the IP address of the primary DNS server used for domain name resolution.
Secondary DNS Server	Displays the IP address of the secondary DNS server used as a backup for domain name resolution.
Management VLAN	Indicates the VLAN assigned for switch management traffic.
Uplink Device	Shows the device to which the switch is connected for uplink or upstream network connectivity.

Nuclias Unity Devices Switches **Settings**

The Settings function contains information about the Device Name and management details. From here, you can manage the device using options such as Remote Access, Locate Device, and Remove Device.

Device Name – Displays the name assigned to the switch, which can be customized for easy identification and management within the network.

Address – Shows the physical or network location of the switch, such as its IP address or the site location where it is deployed, for identification and management purposes.

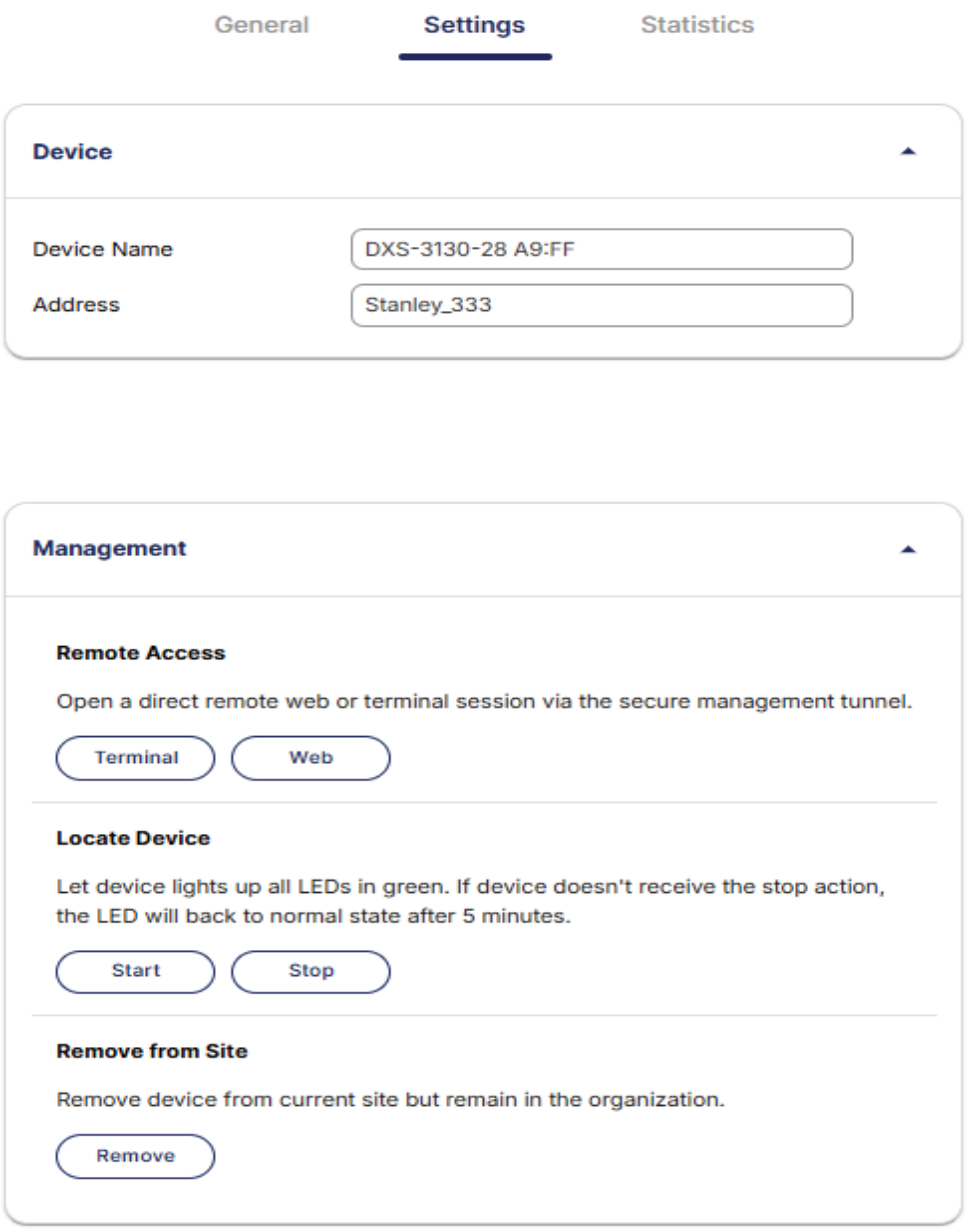
Management

Remote Access – Open a direct remote web or terminal session via the secure management tunnel.

Note: If the device is managed via Remote Access, it will not synchronize with the platform's configuration profiles other than the device login credentials. All settings must be configured remotely via CLI or Web interface.

Locate Device – Let device lights up all LEDs in green. If device doesn't receive the stop action, the LED will back to normal state after 5 minutes.

Remove from Site – Remove device from current site but remain in the organization.

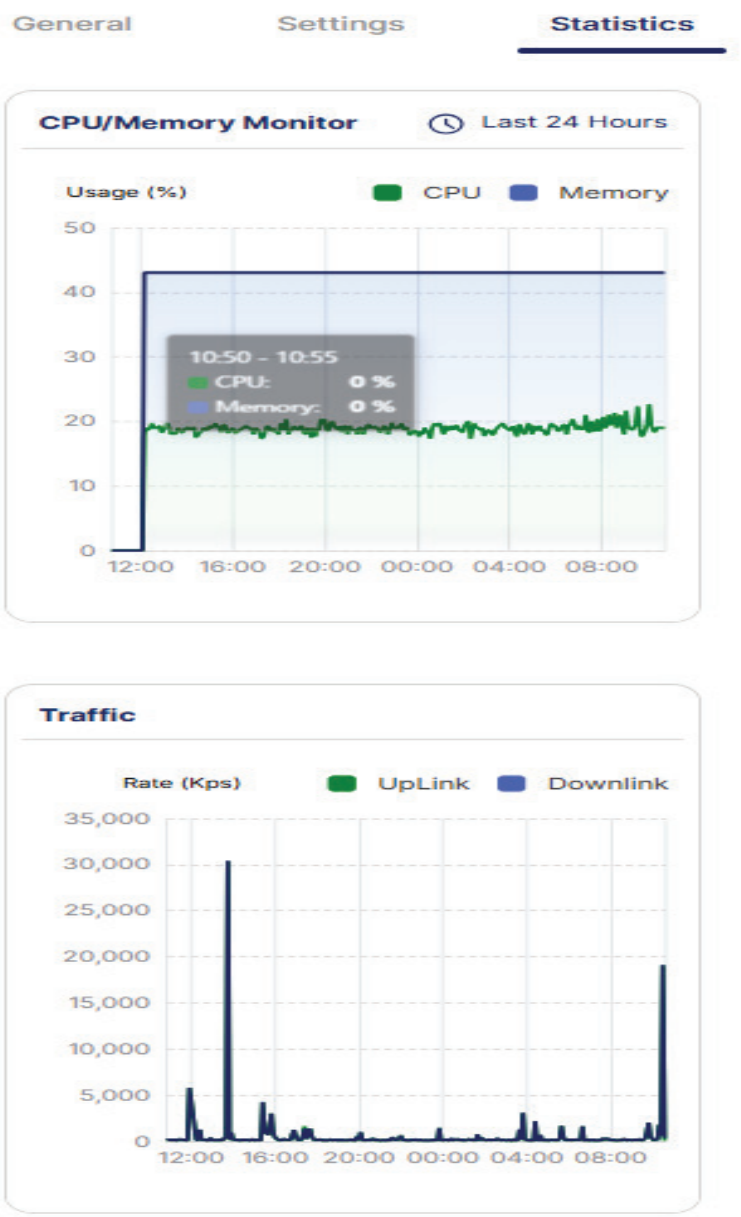


Nuclias Unity Devices Switches **Statistics**

The **Statistics** section provides detailed insights into the performance and health of the switch, helping administrators monitor and optimize network operations. It includes:

- **CPU Usage** – Displays the percentage of CPU resources used over the last 24 hours, helping identify periods of high processing load or potential bottlenecks.
- **Memory Usage** – Shows memory consumption trends over the last 24 hours, allowing you to monitor for potential memory overloads or inefficient resource usage.
- **Uplink Traffic** – Provides real-time and historical data on the traffic flowing from the switch to upstream devices, including throughput and utilization trends.
- **Downlink Traffic** – Shows traffic data for all devices connected downstream to the switch, helping track bandwidth usage, detect congestion, and plan capacity.
- **Traffic Graphs** – Visual representation of uplink and downlink traffic over time for easier analysis and monitoring.
- **Alerts & Thresholds** – Some systems may provide notifications if CPU, memory, or traffic exceeds predefined thresholds, allowing proactive management.

This section is essential for network monitoring, troubleshooting, and performance optimization, ensuring the switch and connected devices operate efficiently.



Nuclias Unity Dashboard Wi-Fi Planner Pro

What is WiFi Planner?

WiFi Planner is a tool used to help users design and optimize wireless network coverage before actual deployment. It helps estimate how many access points (APs) are needed, where they should be placed, and what kind of coverage users can expect in a specific area.

Why is WiFi Planner important?

A good WiFi network is not only about installing APs. If APs are placed in the wrong locations, users may experience weak signal, dead zones, interference, or poor performance. WiFi Planner helps reduce these problems by giving a visual plan in advance.

What can WiFi Planner do?

WiFi Planner can usually help users:

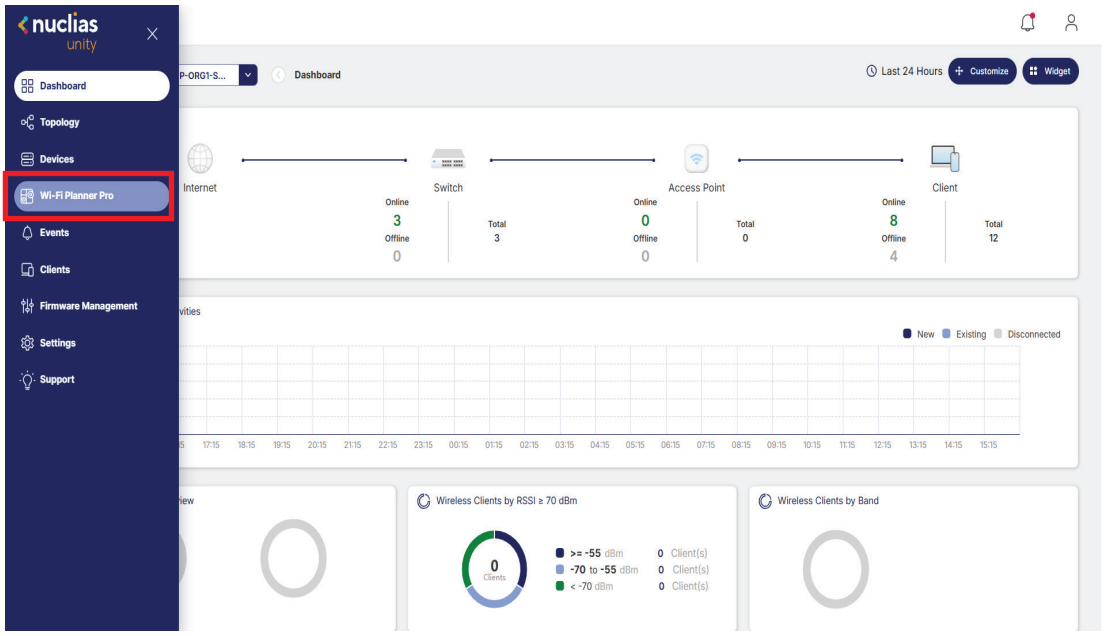
- Import or draw a floor plan
- Define walls, rooms, and obstacles
- Set coverage requirements
- Place APs on the map
- Simulate signal coverage
- Estimate the number of APs required
- Improve AP placement for better performance

Who uses WiFi Planner?

It is mainly used by network planners, system integrators, installers, and IT administrators who want to build a reliable wireless network in offices, schools, hotels, retail stores, or other indoor environments.

User need to click WiFi Planner Pro in Nuclias Unity side menu to access WiFi Planner Pro.

To access the **Wi-Fi Planner Pro** tool in Nuclias Unity, navigate from the **Dashboard** to **Wi-Fi Planner Pro** on the left side menu bar. This feature provides a comprehensive solution for designing, planning, and optimizing wireless network deployments.

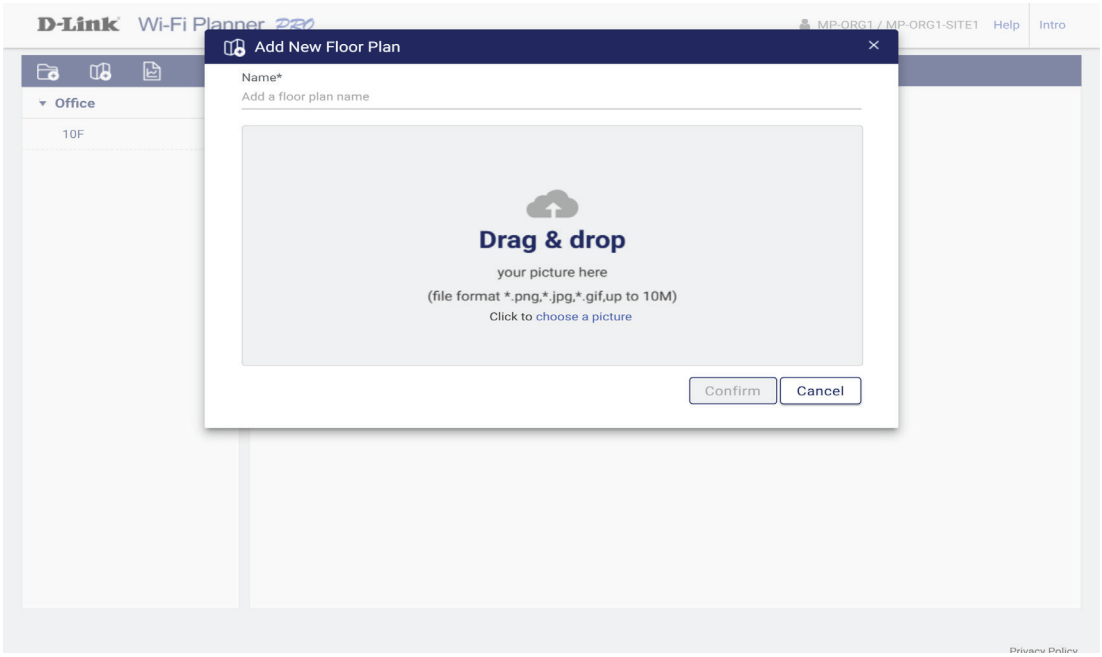


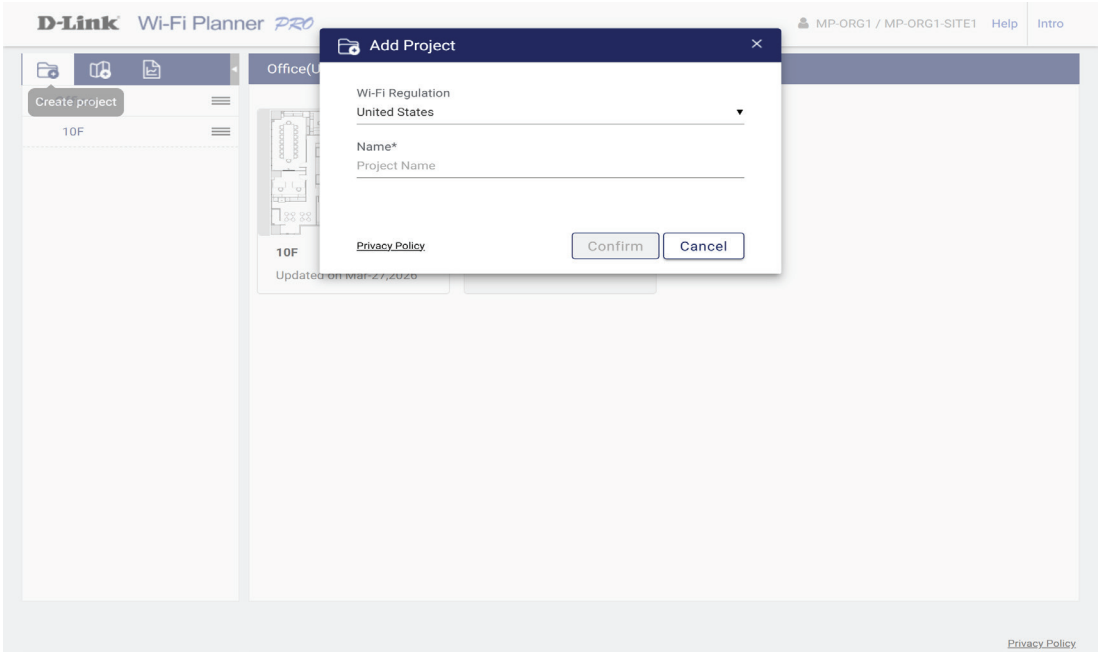
Nuclias Unity Dashboard Wi-Fi Planner Pro

Administrators can create floor plans, place virtual access points, and simulate Wi-Fi coverage to ensure optimal signal strength and performance before physical installation. Key capabilities include:

- **Floor Plan Import:** Upload building floor plans to create accurate site maps for network planning.
- **Access Point Placement:** Drag and drop access points onto the floor plan to model optimal positioning for maximum coverage.
- **Signal Heatmap Visualization:** View simulated Wi-Fi coverage heatmaps to identify potential dead zones and adjust access point placement accordingly.
- **Site Survey:** Perform predictive site surveys to assess signal strength, interference, and channel utilization.
- **Deployment Recommendations:** Receive intelligent recommendations for access point placement based on site dimensions, materials, and user density.

Wi-Fi Planner Pro helps network administrators streamline wireless network design, reduce deployment costs, and ensure reliable Wi-Fi performance across the deployment site.

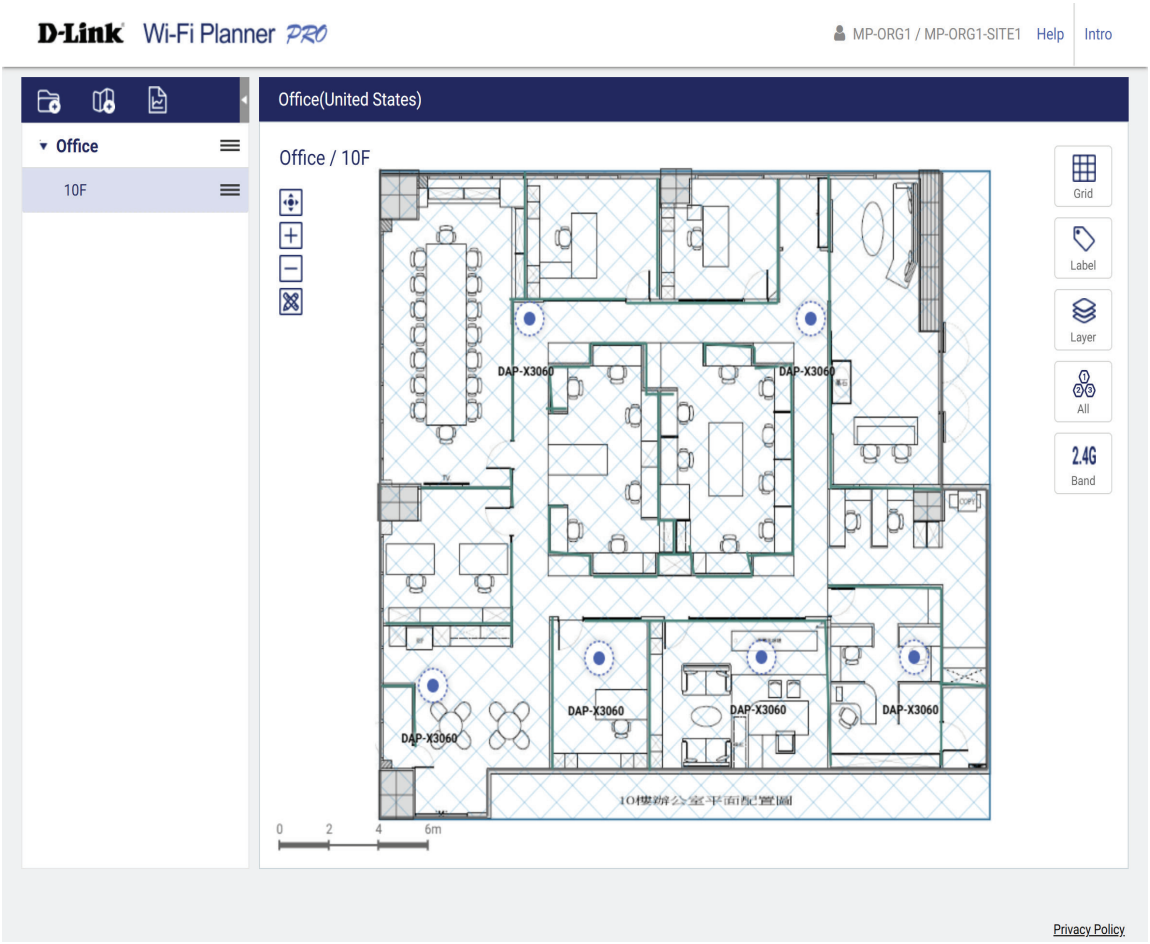




Nuclias Unity Vi-Fi Planner Pro Getting Started

Create a Project

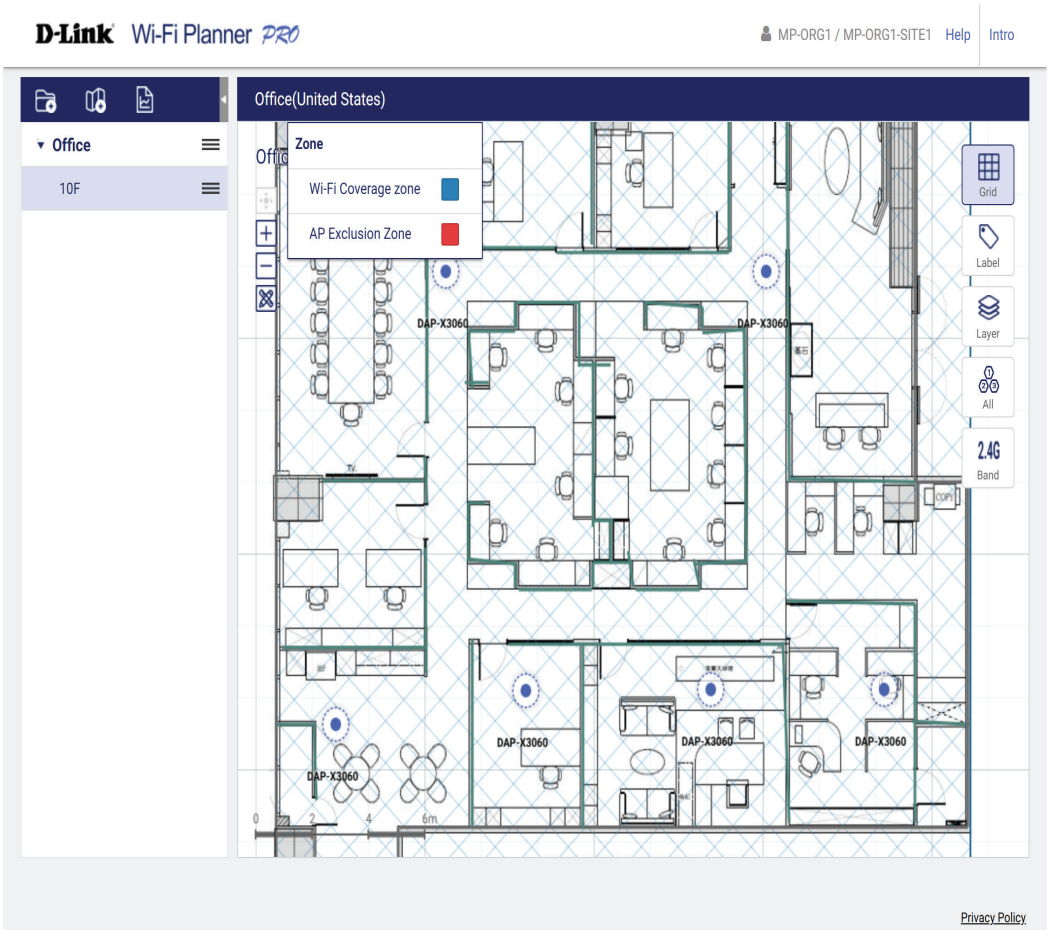
Start by creating a project folder. Then upload an image of the floor plan for your Wi-Fi project. The floor plan can be provided by the customer or drawn by you.



Nuclias Unity Wi-Fi Planner Pro Zone Type

Defining Zones, Obstacles, and Areas

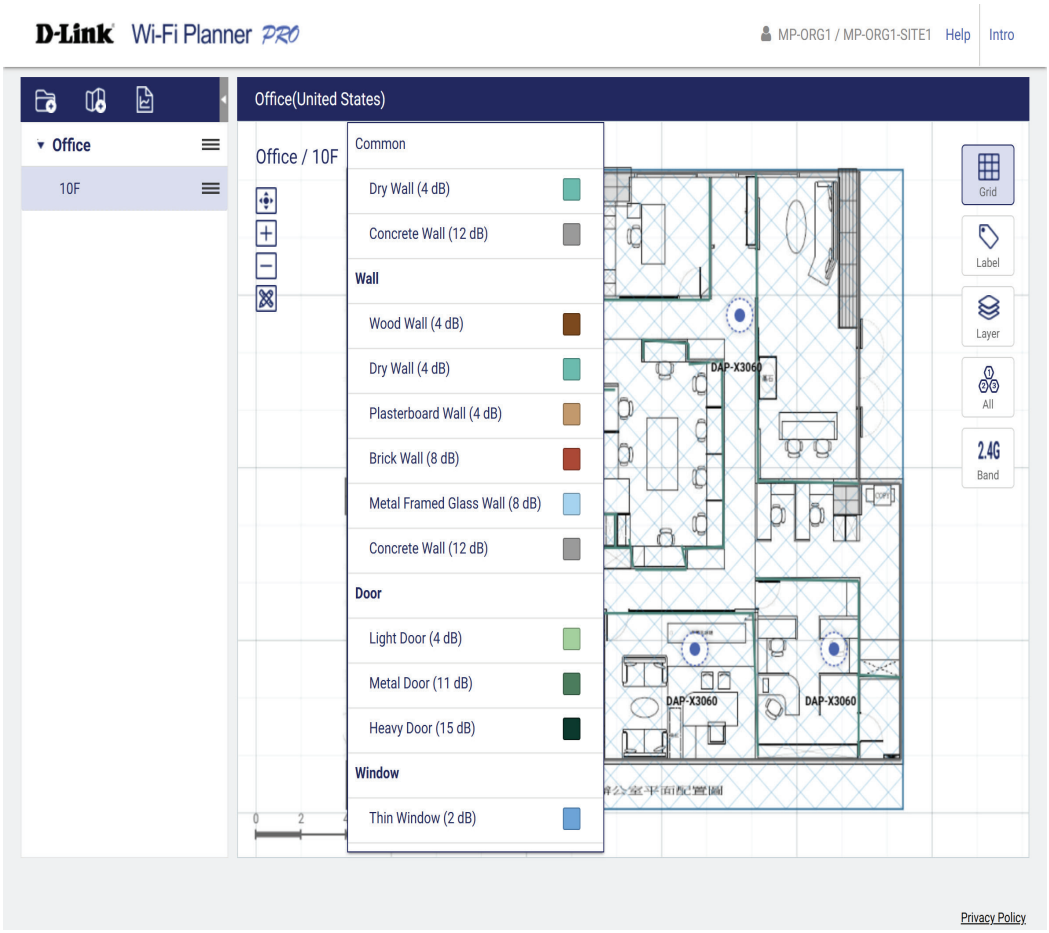
Next, define the Wi-Fi coverage zone and access point exclusion zone. Mark obstacles such as walls or doors, and indicate special zones like closed office spaces or warehouses. This helps the WFP produce a more accurate simulation.



Nuclias Unity Wi-Fi Planner Pro Obstacle Type

Defining Zones, Obstacles, and Areas

Next, define the Wi-Fi coverage zone and access point exclusion zone. Mark obstacles such as walls or doors, and indicate special zones like closed office spaces or warehouses. This helps the WFP produce a more accurate simulation.



Nuclias Unity Wi-Fi Planner Pro Area Type

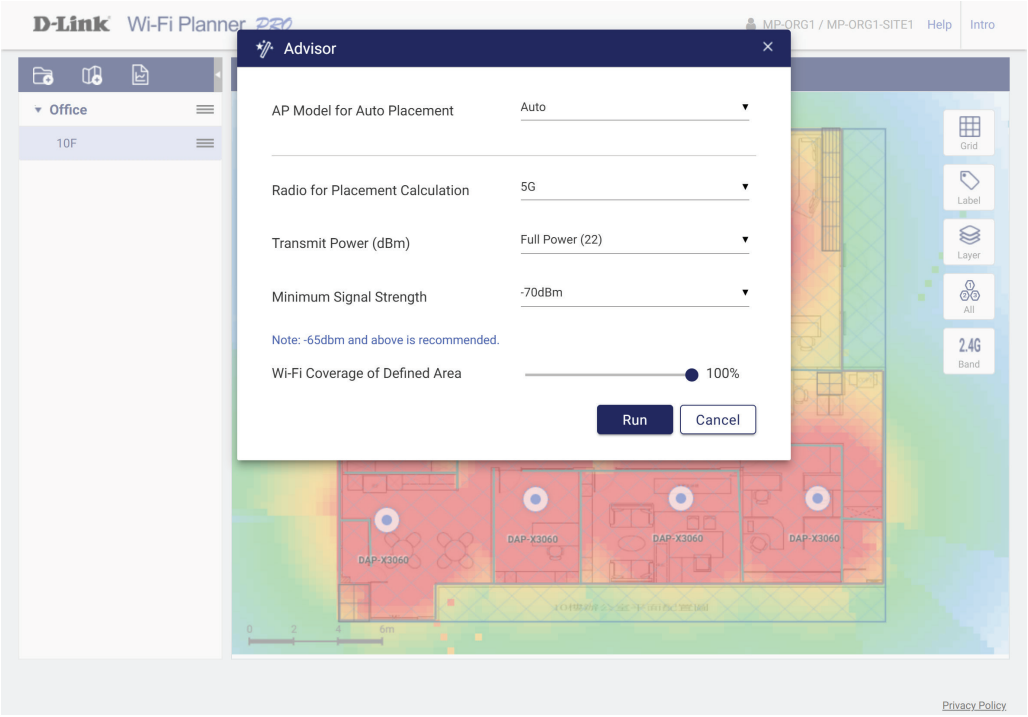
Defining Zones, Obstacles, and Areas

Next, define the Wi-Fi coverage zone and access point exclusion zone. Mark obstacles such as walls or doors, and indicate special zones like closed office spaces or warehouses. This helps the WFP produce a more accurate simulation.

Nuclias Unity Wi-Fi Planner Pro Placement Settings

Placing Access Points with Advisor

Once all conditions are set, the built-in AP Placement Advisor will suggest the number of access points required and recommend their placement for optimal Wi-Fi planning.



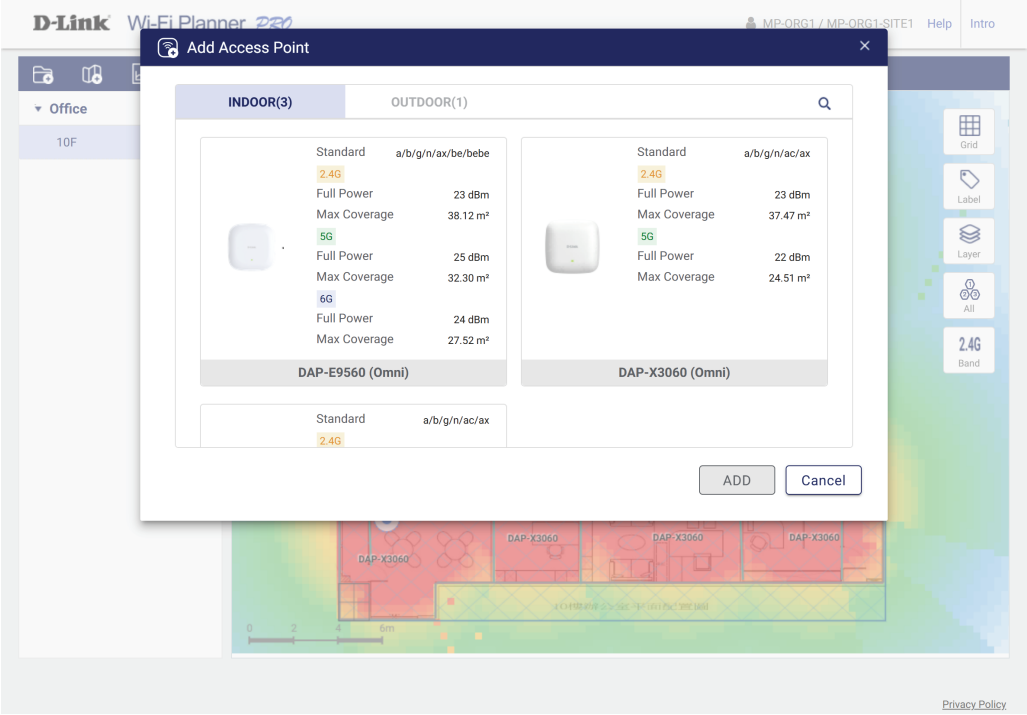
Nuclias Unity | Wi-Fi Planner Pro | Heat Map

Reviewing Deployment and Heat Map

Once the calculation is complete, you will see the number and placement of access points, along with AP details and a heat map showing the simulated Wi-Fi coverage.

Changing to a Different Model

If the Advisor's suggestion is not satisfactory, click on any access point on the floor map to change it to a different D-Link model. You may adjust its parameters as needed.



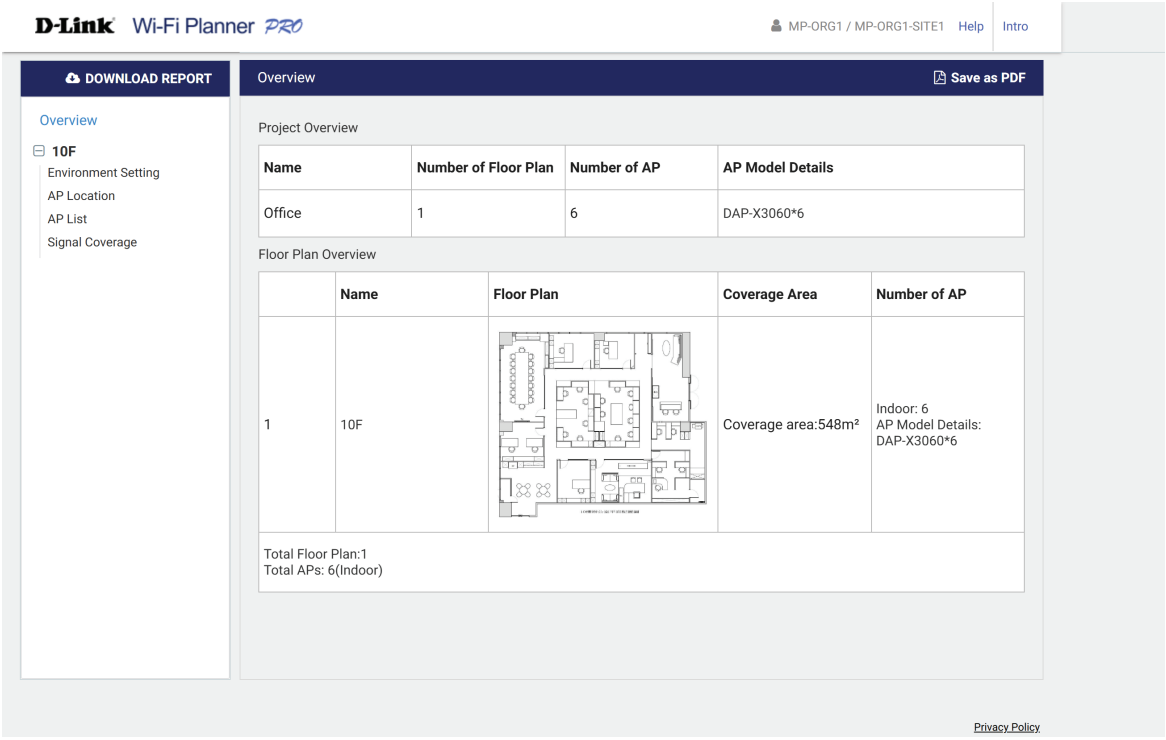
Nuclias Unity Wi-Fi Planner Pro **Report**

Generating Reports

WFP can provides reports in two formats : PDF and Word files.

Key items included in the report are:

- AP inventory list
- AP details
- AP location map
- Wi-Fi heat map



One Last Thing Before You Start

Before using this tool in your wireless projects, please note the following precautions:

Simulation ≠ Reality:
The WFP result is a simulation of Wi-Fi planning before deployment and should not replace an actual post-deployment survey.

Environment Matters:
WFP is not suitable for outdoor environments or indoor spaces with distinct floor surface levels.

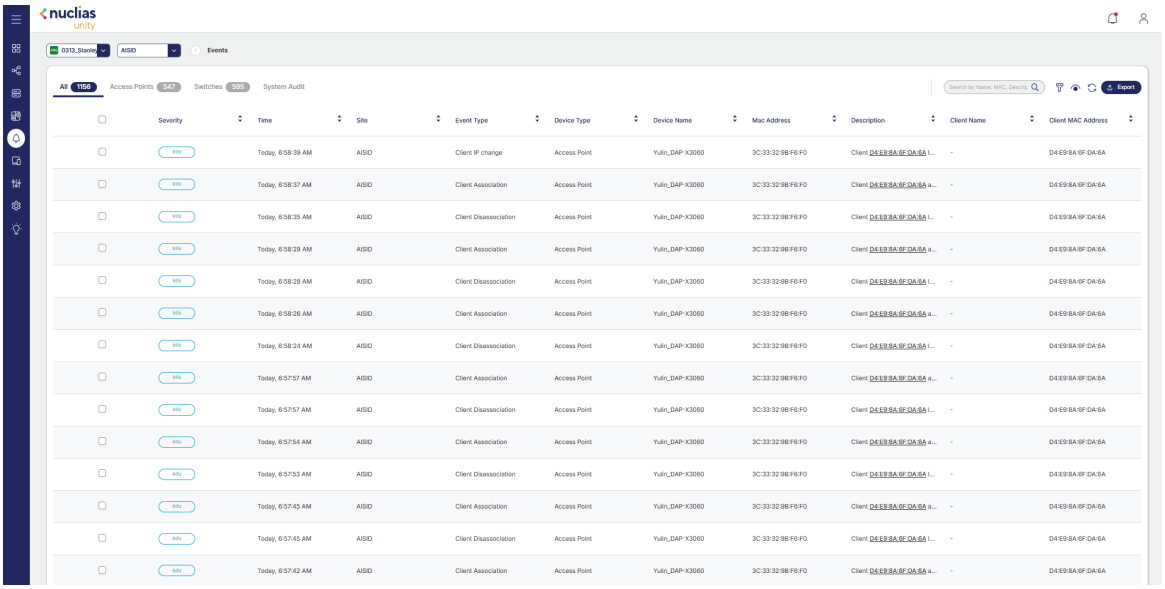
Height Matters:
The simulation may not be accurate if access points are installed on the roof of high-ceiling buildings such as warehouses or halls.

Nuclias Unity Dashboard Events

The Events section provides a centralized log of activities and notifications across your network. It includes:

- **Access Point Events:** Track AP connections, disconnections, reboots, configuration changes, and signal-related alerts.
- **Switch Events:** Monitor switch status changes, port connections, power over Ethernet (PoE) events, and link fluctuations.
- **System Audit Events:** Review administrative actions such as user logins, setting changes, firmware updates, and security-related activities.
- **Search Bar:** Quickly locate specific events by typing keywords, device names, MAC addresses, or descriptions.
- **Filter Options:** Narrow down events by criteria such as severity, time range, site, event type, or device type for more focused troubleshooting.
- **Export:** Download the event log as a file (e.g., CSV or PDF) for external reporting, record-keeping, or further analysis.

These events help you monitor network health, troubleshoot issues, and maintain an audit trail for compliance and security purposes.



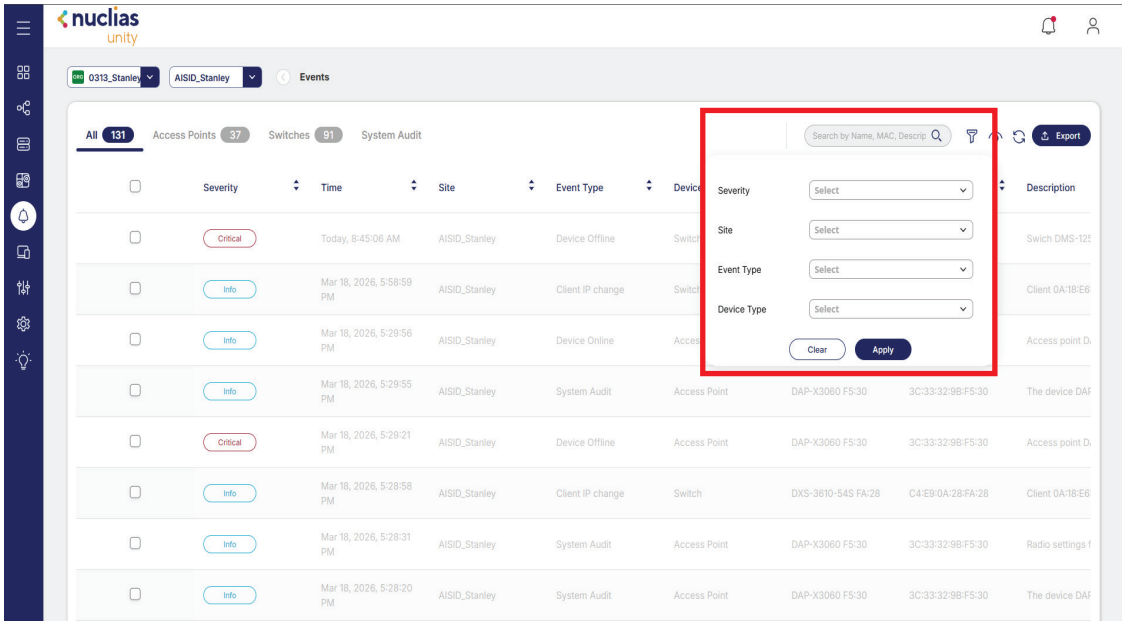
Parameter	Description
Severity	Indicates the importance level (e.g., Info, Warning, Critical).
Time	Shows the exact date and time when the event occurred.
Site	Indicates the subnet mask used to define the network segment of the local IP.
Event Type	Identifies the specific site where the event originated.
Device Type	Specifies the type of device involved, such as Access Point or Switch.
Device Name	Displays the name of the affected device.
MAC Address	Provides the unique hardware identifier of the device.
Description	Offers a brief explanation of what triggered the event.
Client Name	Shows the name of the client device connected to the network.
Client MAC Address	Displays the unique hardware identifier of the client device.

Nuclias Unity Dashboard Events Filter

To access the Event section on the Nuclias Unity Dashboard and utilize the filtering options, navigate to the Event section from the main navigation panel. Once inside the Event section, locate the filter interface in the top right corner of the main content area, represented by a funnel icon or a dedicated Filter button. Click this button to expand the filtering panel, where you can refine the event list according to the following criteria:

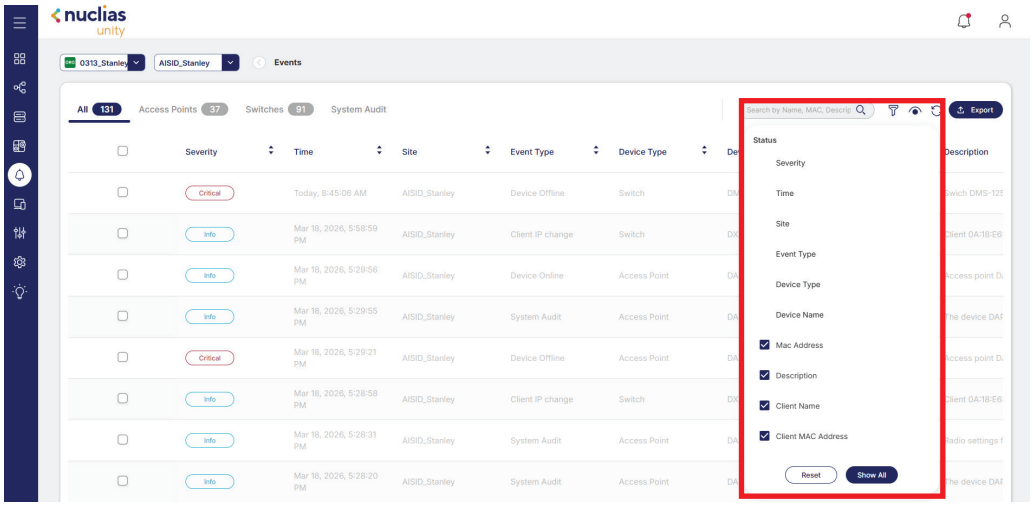
- Severity: Filter events by severity level, such as Critical, Warning, or Info.
- Site: Narrow down events based on specific Site locations.
- Event Type: Select specific Event Type categories to view relevant logs.
- Device Type: Filter events by the type of device involved.

Using these filters allows you to efficiently narrow down the event list to only the most relevant entries for your analysis or troubleshooting needs.



Nuclias Unity Dashboard Event View

To view specific information such as Severity, Time, Site, Event Type, Device Type, Device Name, MAC Address, Description, Client Name, and Client MAC Address, users can customize the event log display to suit their monitoring preferences. This flexibility allows you to select which data fields to show based on what you want to view about the device—whether for access points or switches. To configure the display, locate the Columns or Customize View option, typically found in the top right corner of the event list or within the filter interface. From there, you can check or uncheck the desired fields to tailor the event table to your specific analysis, troubleshooting, or reporting needs.

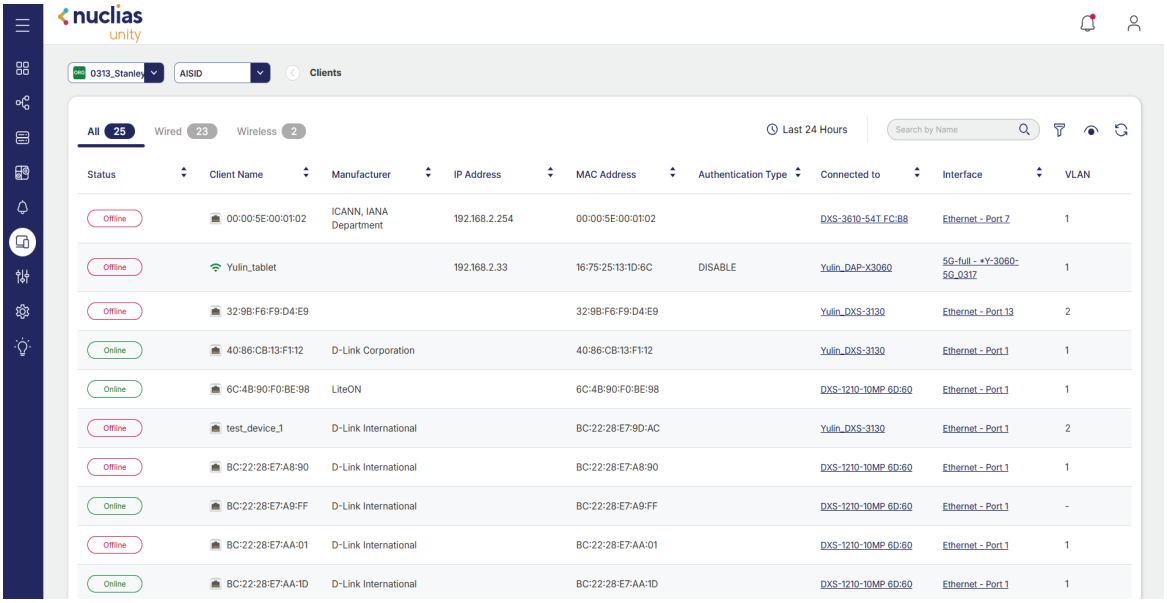


Nuclias Unity Dashboard Clients

To navigate to the **Clients** section from the Nuclias Unity Dashboard, locate the left side menu bar and click on the **Clients** option from the available menu items. This will direct you to the Clients page, where you can view and manage all client devices connected to your network. The page displays both **Wired** and **Wireless** connected clients, providing a comprehensive overview of all active client connections for easy monitoring and troubleshooting.

The Clients function provides the following options to view and manage client information:

- **Wired:** Filter the client list to show only devices connected through switches, enabling focused viewing of wired client connections.
- **Wireless:** Filter the client list to show only devices connected through access points, allowing you to monitor wireless client activity.
- **Last 24 Hours:** Apply a time filter to display client activity and data from the last 24 hours, providing a quick overview of recent network usage.
- **Search Bar:** Enter keywords such as client name, IP address, or MAC address to quickly locate a specific client within the list.
- **Filter:** Click the filter icon (funnel) to refine the client list by criteria such as status, authentication type, VLAN, or connected device.
- **Export:** Click the export icon (download) or Export button to generate and download a report of the current client list in your preferred format, ideal for auditing or offline analysis.



Parameter	Description
Status	Indicates whether the client is currently Online or Offline.
Client Name	The name assigned to the client device.
Manufacturer	The device manufacturer, if detected.
IP Address	The IP address assigned to the client.
MAC Address	The unique MAC address of the client device.
Authentication Type	The method used to authenticate the client on the network.
Connected To	The access point or switch the client is connected to.
Interface	The specific interface port used by the client.
VLAN	The VLAN assigned to the client.
SSID	The service set identifier for wireless clients.
Channel	The wireless channel being used.
Signal	The signal strength of the wireless connection.
SNR	The signal-to-noise ratio for the wireless connection.
Download	The current download throughput.
Upload	The current upload throughput.
Traffic (24HR)	Total traffic usage over the last 24 hours.
Last Seen	The timestamp when the client was last detected.
Uptime	The total time the client has been connected.

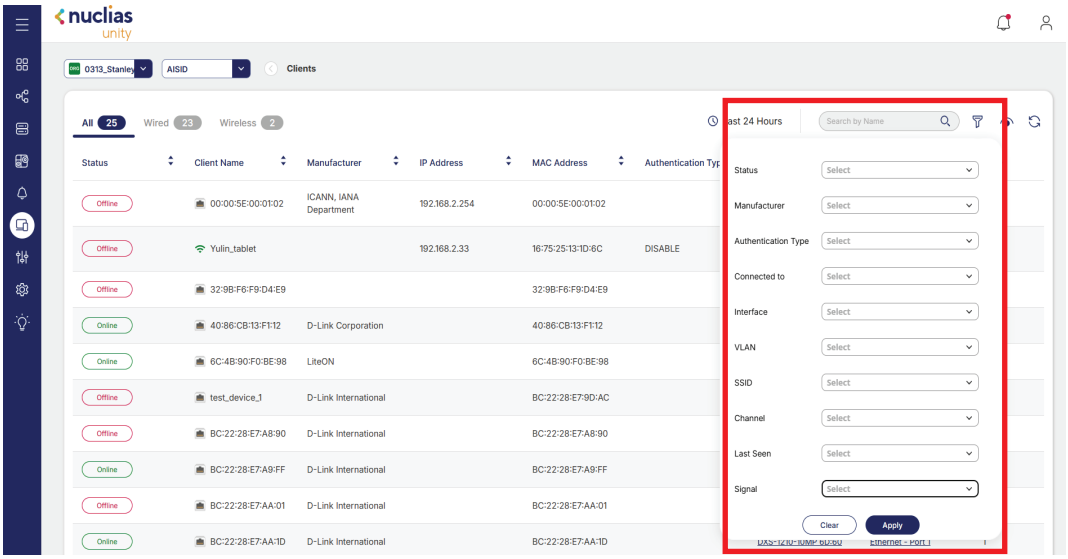
Nuclias Unity Dashboard Clients Filter

To access the Clients section on the Nuclias Unity Dashboard and utilize the filtering options, navigate to the Clients section from the left side menu bar. Once inside the Clients section, locate the filter interface in the top right corner of the main content area, represented by a funnel icon or a dedicated Filter button.

Click this button to expand the filtering panel, where you can refine the client list according to the following criteria:

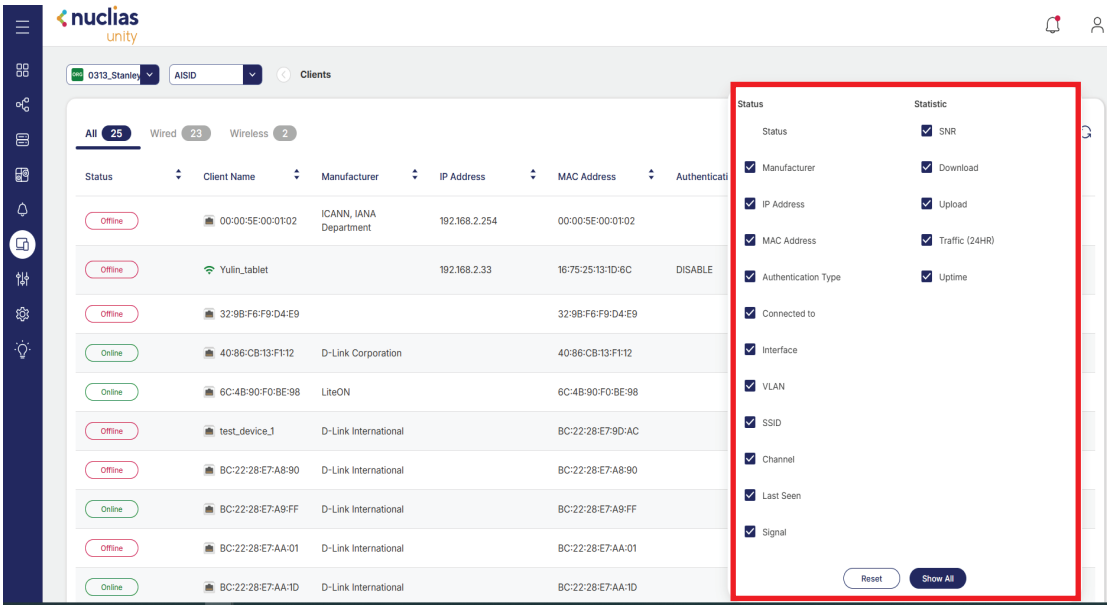
- **Status:** Filter clients by their current connection state (e.g., Offline or Online).
- **Manufacturer:** Narrow down the list by client device manufacturer.
- **Authentication Type:** Filter by the authentication method used by clients.
- **Connected To:** View clients connected to specific access points or switches.
- **Interface:** Refine by the specific network interface or port used.
- **VLAN:** Filter clients assigned to a particular VLAN.
- **SSID:** Narrow down wireless clients by the SSID they are connected to.
- **Channel:** Filter wireless clients by the channel they are operating on.
- **Last Seen:** Set a time range to view clients based on when they were last detected.
- **Signal:** Refine wireless clients by signal strength thresholds.

Applying these filters allows you to efficiently narrow down the client list to only the most relevant entries for your analysis, monitoring, or troubleshooting needs.



Nuclias Unity Dashboard Clients View

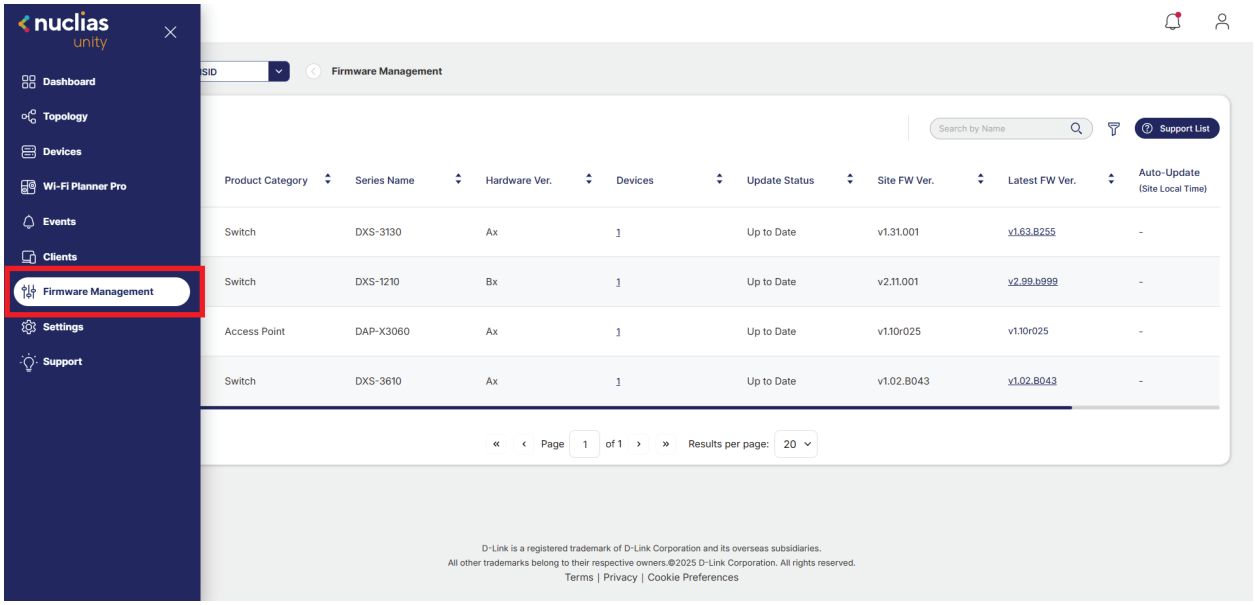
In the **Clients** section on the Nuclias Unity Dashboard, click the **eye icon** located in the top right corner of the main content area to customize the display of client information. This opens a column selector menu, allowing you to choose which specific data fields to view about the connected clients, including Status, Client Name, Manufacturer, IP Address, MAC Address, Authentication Type, Connected To, Interface, VLAN, SSID, Channel, Signal, SNR, Download, Upload, Traffic (24HR), Last Seen, and Uptime. This customization feature enables network administrators to tailor the client table to display only the most relevant information for their specific analysis, troubleshooting, or reporting needs.

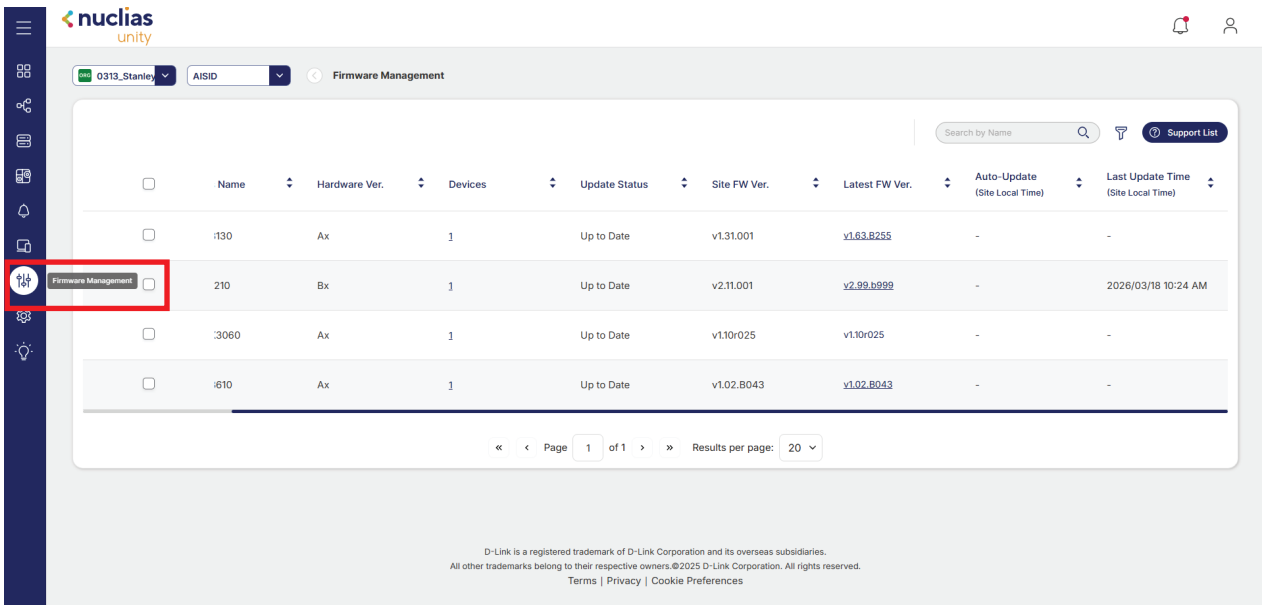


.

Nuclias Unity Dashboard Firmware Management

In the Nuclias Unity cloud management platform, you can update the firmware for both connected switches and access points. To do so, Navigate from the Nuclias Unity **Dashboard** and select **Firmware Management** from the left side menu bar. This section allows you to manage firmware for both **Switches** and **Access Points**, including viewing current firmware versions, checking for updates, and initiating firmware upgrades across your network devices. Regularly updating firmware ensures optimal performance, enhanced security, and access to the latest features for your entire network infrastructure.





Parameter	Description
Product Category	Identifies the type of device, such as Access Point or Switch, allowing you to distinguish between different device classes during firmware management.
Series Name	Displays the specific product series or model family of the device, helping you group and manage devices with similar hardware characteristics.
Harware Version	Indicates the hardware revision of the device, which is essential for selecting the correct firmware version compatible with the device's physical components.
Devices	Shows the total number of devices within that specific product category, series, or site that are eligible for firmware management.
Update Status	Provides the current firmware update state for the device, such as Up to Date, Update Available, Update Failed, or In Progress, enabling quick identification of devices requiring attention.
Site FW Version	Displays the current firmware version running on devices at a specific site, allowing you to assess the firmware baseline across different locations.
Latest FW Version	Shows the most recent firmware version available for the device from Nuclias Unity, helping you determine if an update is needed.
Auto-Update (Site Local Time)	Indicates whether auto-update is enabled for the site and specifies the scheduled time (based on the site's local time zone) when automatic firmware updates will occur.
Last-Update Time (Site Local Time)	Displays the timestamp of the most recent firmware update performed on the device, shown in the site's local time zone for accurate tracking across different locations.

Nuclias Unity Dashboard FW Management Update Now

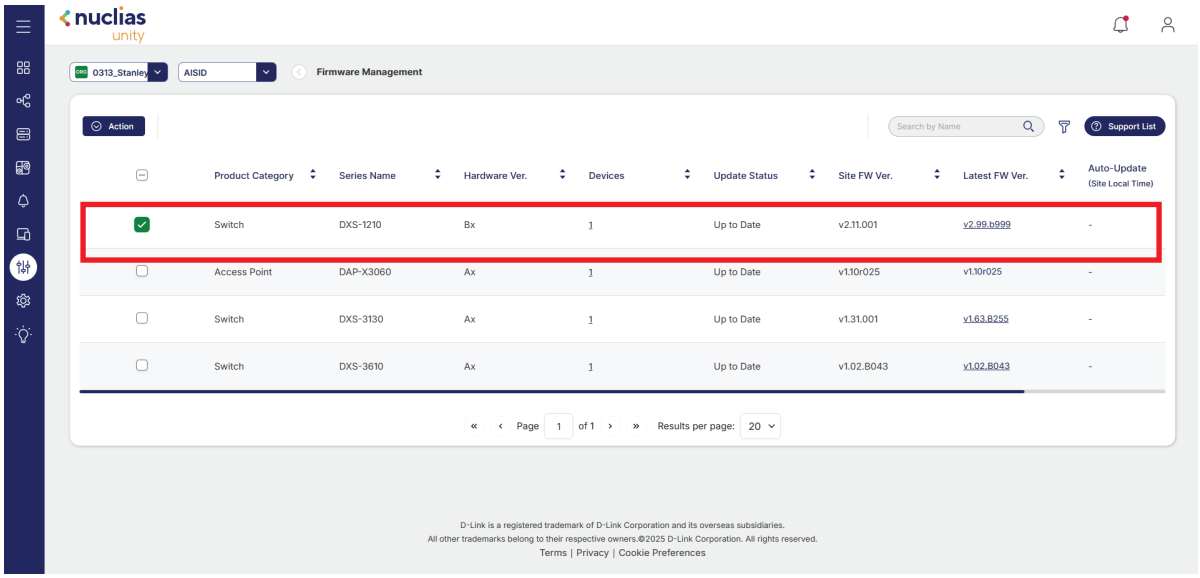
To update the firmware of connected devices such as switches and access points, navigate to Firmware Management from the left side menu bar on the Nuclias Unity Dashboard. Once in the Firmware Management section, select the devices you wish to update by checking the corresponding boxes next to each device.

After making your selection, will be presented with three different options to proceed:

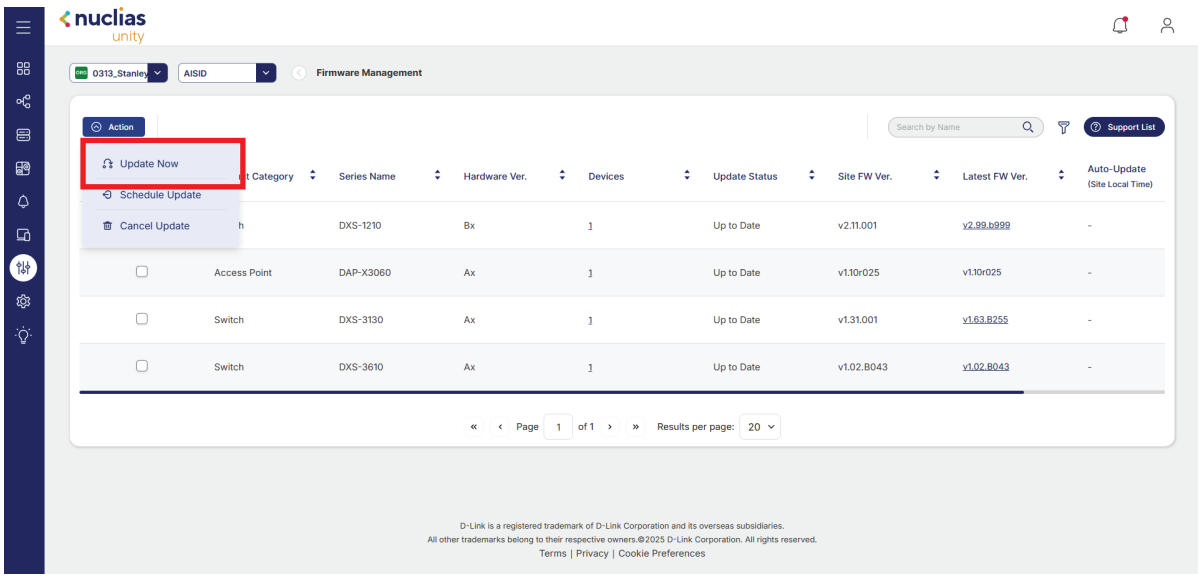
- **Update Now:** Initiates the firmware update immediately on the selected devices, applying the latest available firmware version without delay.
- **Schedule Update:** Allows you to set a specific date and time for the firmware update to occur, enabling you to perform updates during maintenance windows or off-peak hours to minimize network disruption.
- **Cancel Update:** Aborts any pending or scheduled firmware updates for the selected devices, giving you the flexibility to postpone or halt update operations as needed.

These options provide network administrators with flexible control over firmware management, ensuring devices remain up to date while minimizing impact on network operations.

To update the firmware, select the device from the drop-down list.

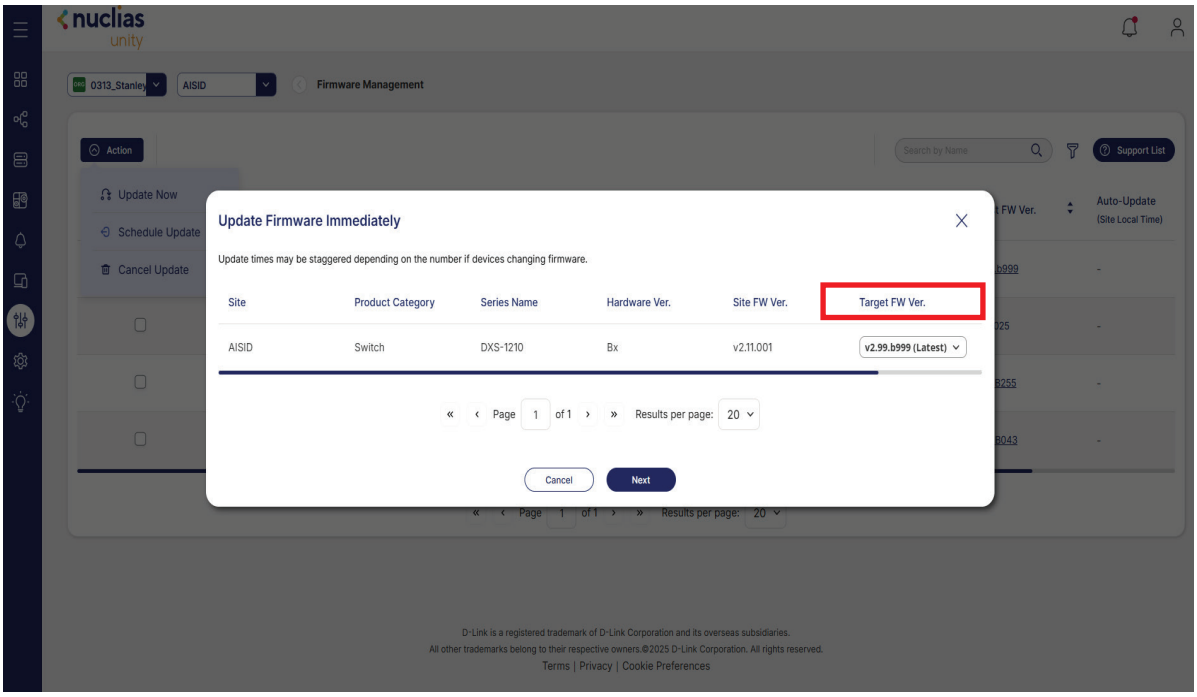


When the user selects a device, the **Action** option appears on the top left corner. Click **Action** and select **Update Now** to initiate the firmware update immediately.

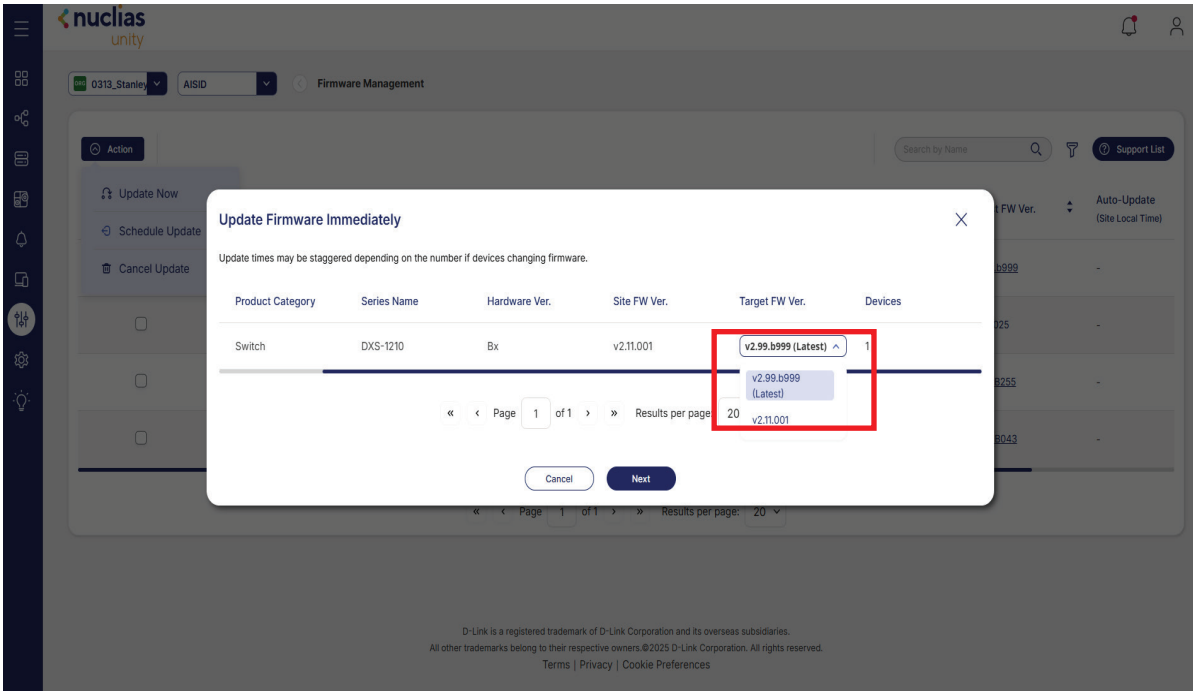


Nuclias Unity Dashboard FW Management Update Now

After clicking Update Now, navigate to Target Firmware Version to select the desired firmware version for the update.

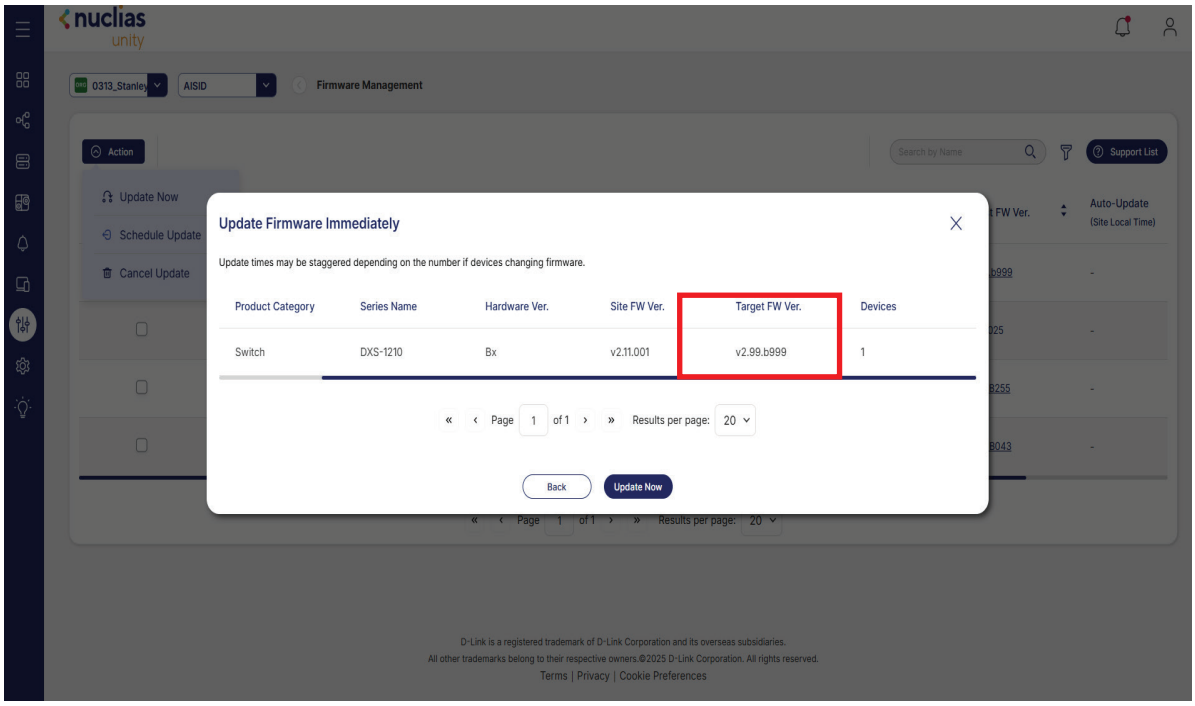


From there, you can choose the appropriate **firmware version** to apply to the selected device before proceeding with the update process.

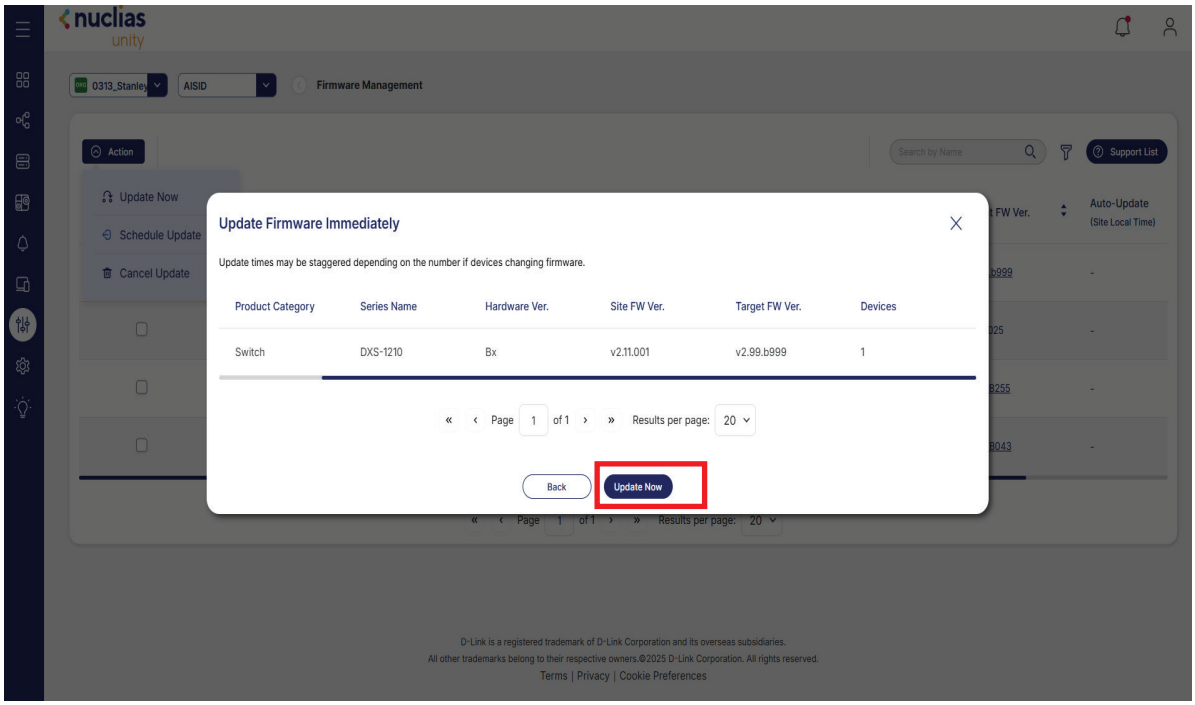


Nuclias Unity Dashboard FW Management Update Now

Ensure the desired firmware is selected from the **Target Firmware Version** drop-down list before proceeding with the update.



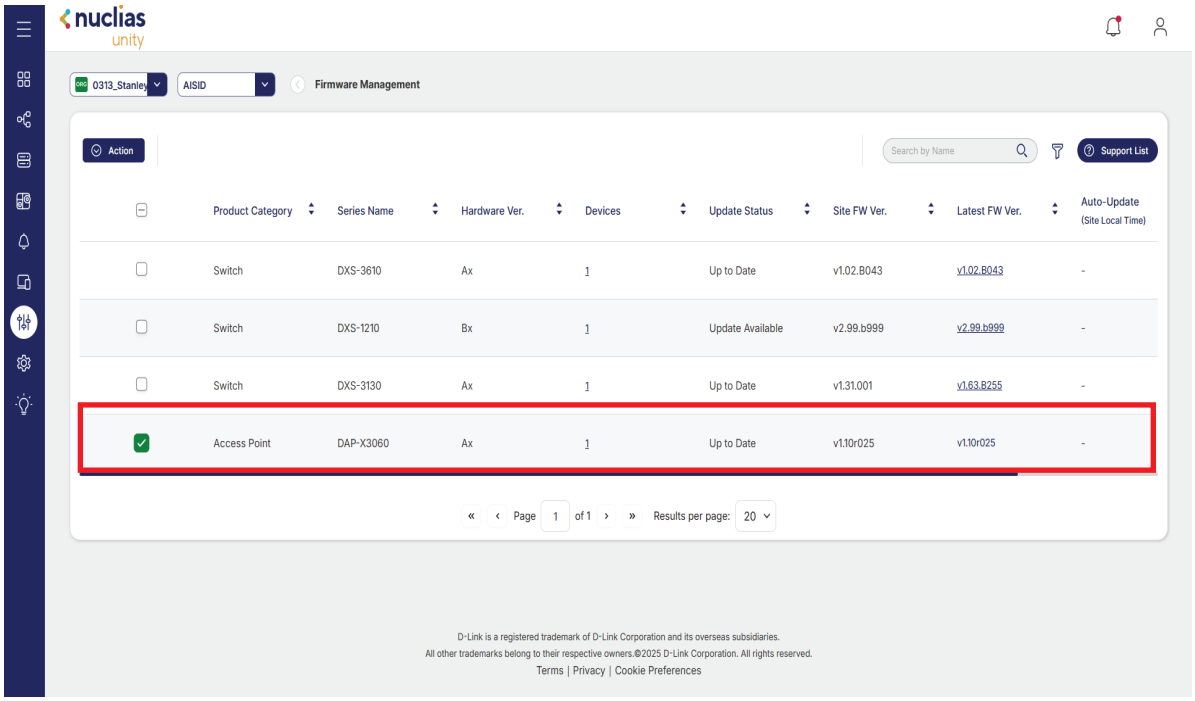
After that, click **Apply Now** to update the firmware for your desired connected device.



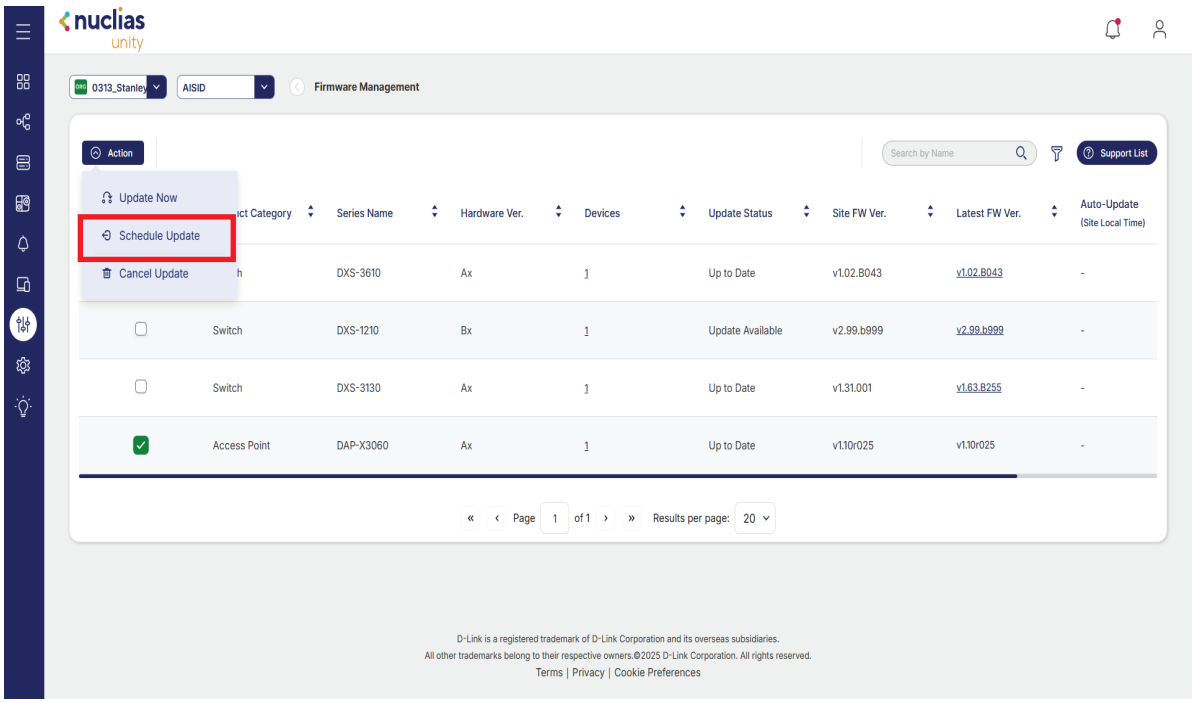
Nuclias Unity Dashboard FW Management Schedule Update

For a **Schedule Update**, first select the device that needs to be updated, then specify the desired date and time for the firmware update to occur.

Click to select the desired switch or access point.

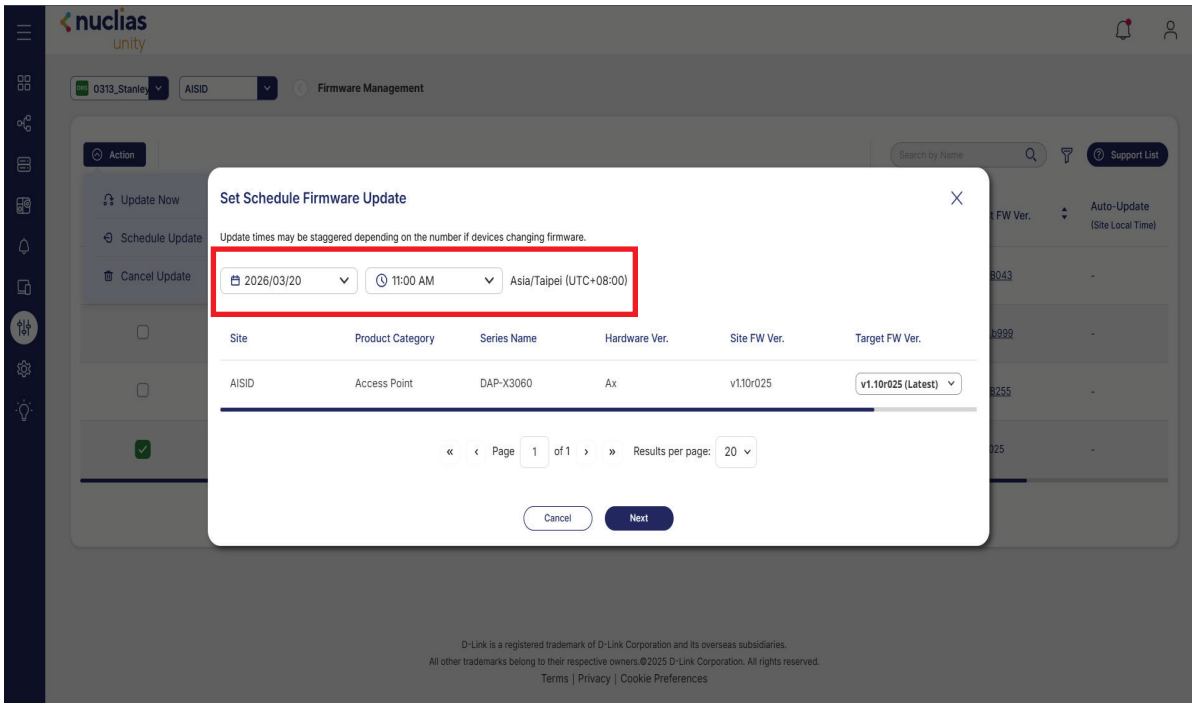


After selecting the device, the **Action** option appears on the top left corner. Click **Action** and select **Schedule Update**.

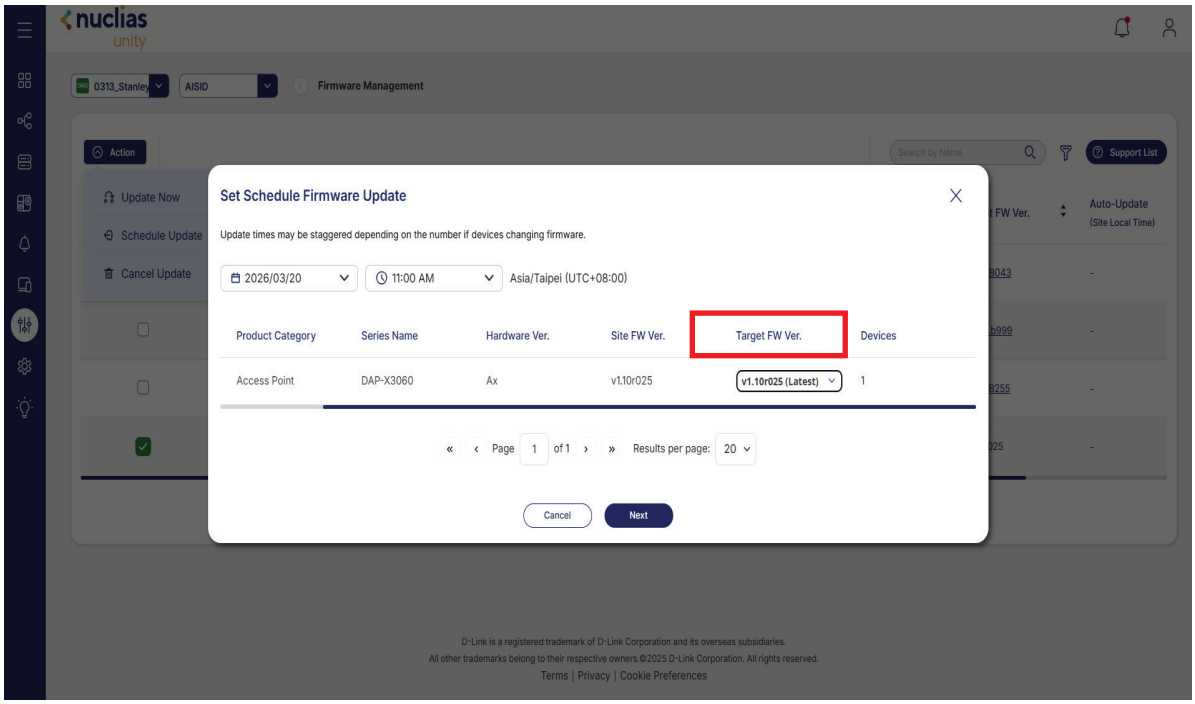


Nuclias Unity Dashboard FW Management Schedule Update

After clicking Schedule Update, a new window will appear. In this window, select the desired Date and Time for the automatic firmware update to occur at the specified time.

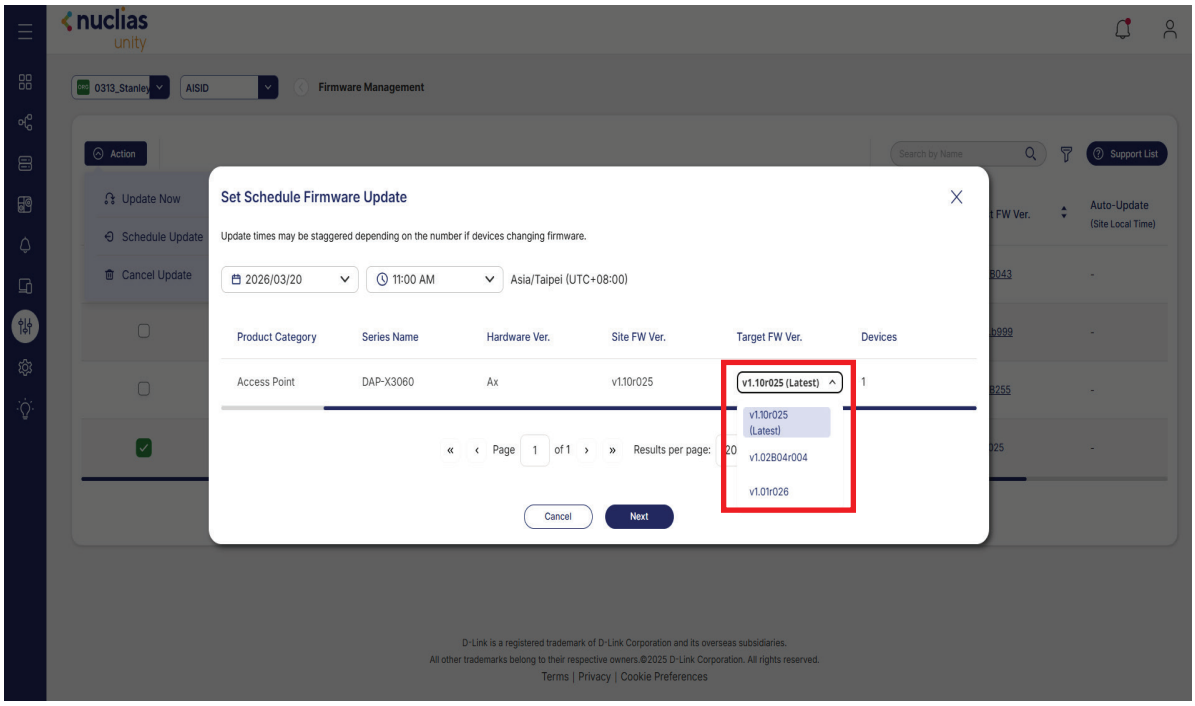


Then navigate to **Target Firmware Version** and select the firmware version that needs to be applied for the update.

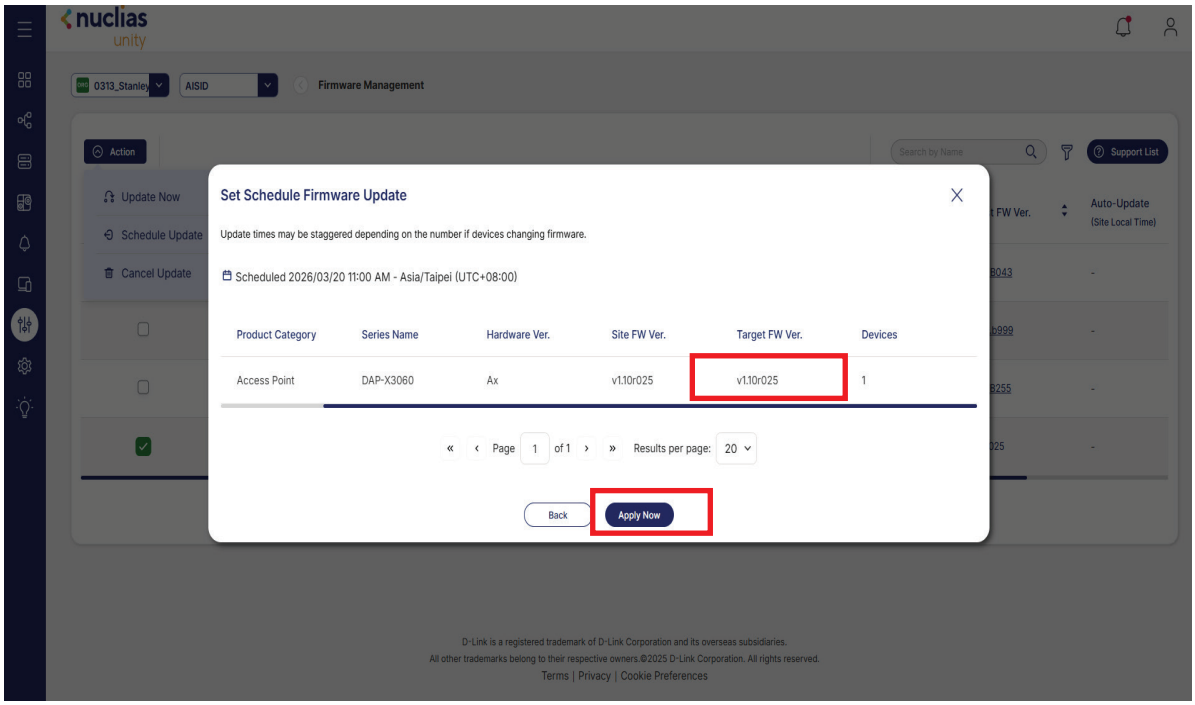


Nuclias Unity Dashboard FW Management Schedule Update

Select the appropriate firmware version from the drop-down list.

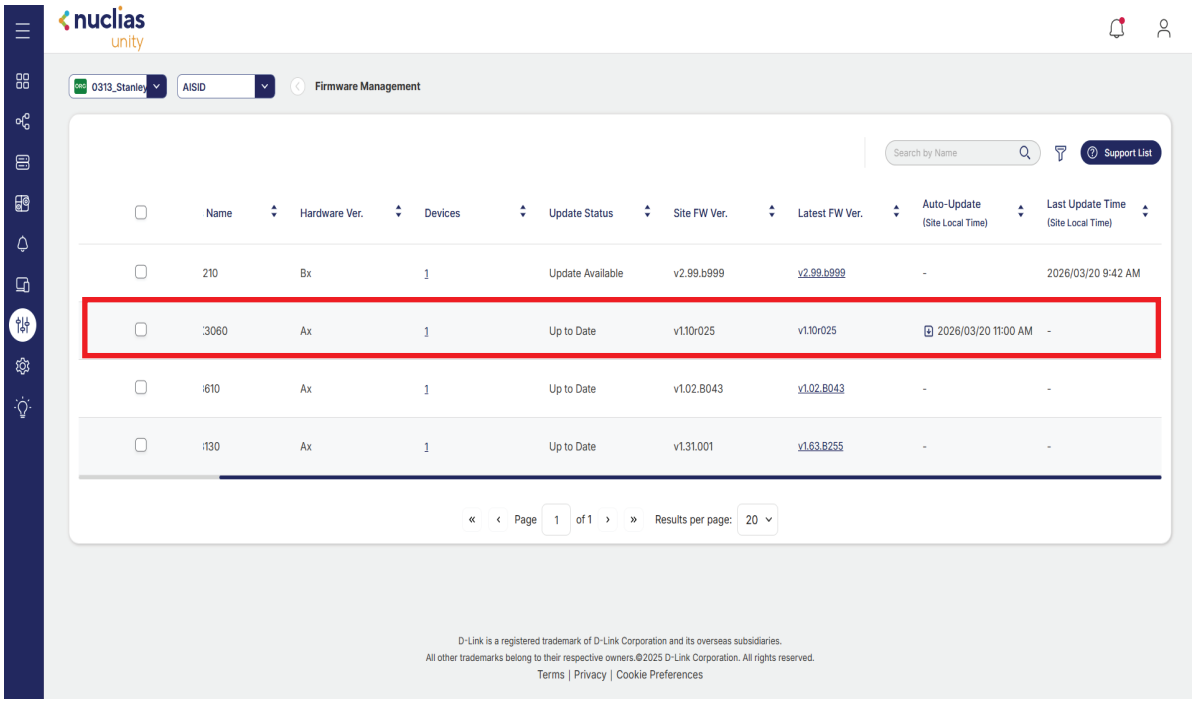


Ensure the correct firmware version is selected, then click **Apply Now**.



Nuclias Unity Dashboard FW Management Schedule Update

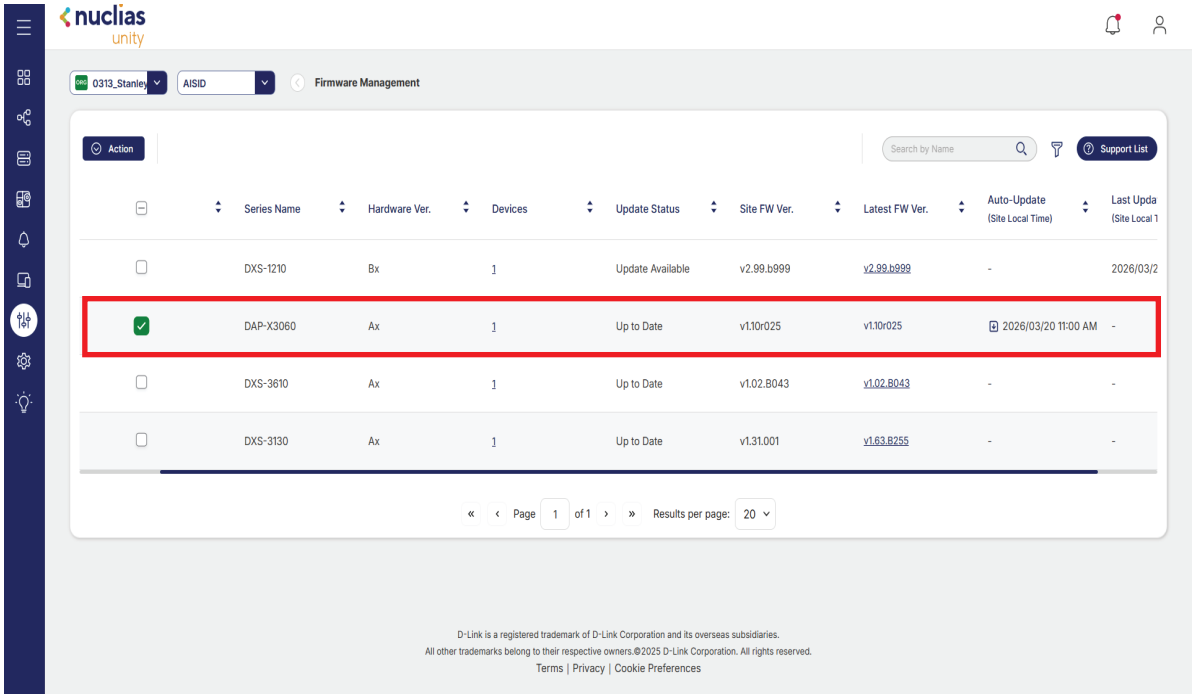
To review the scheduled date and time of the firmware update, the information will appear in the Auto-Update section.



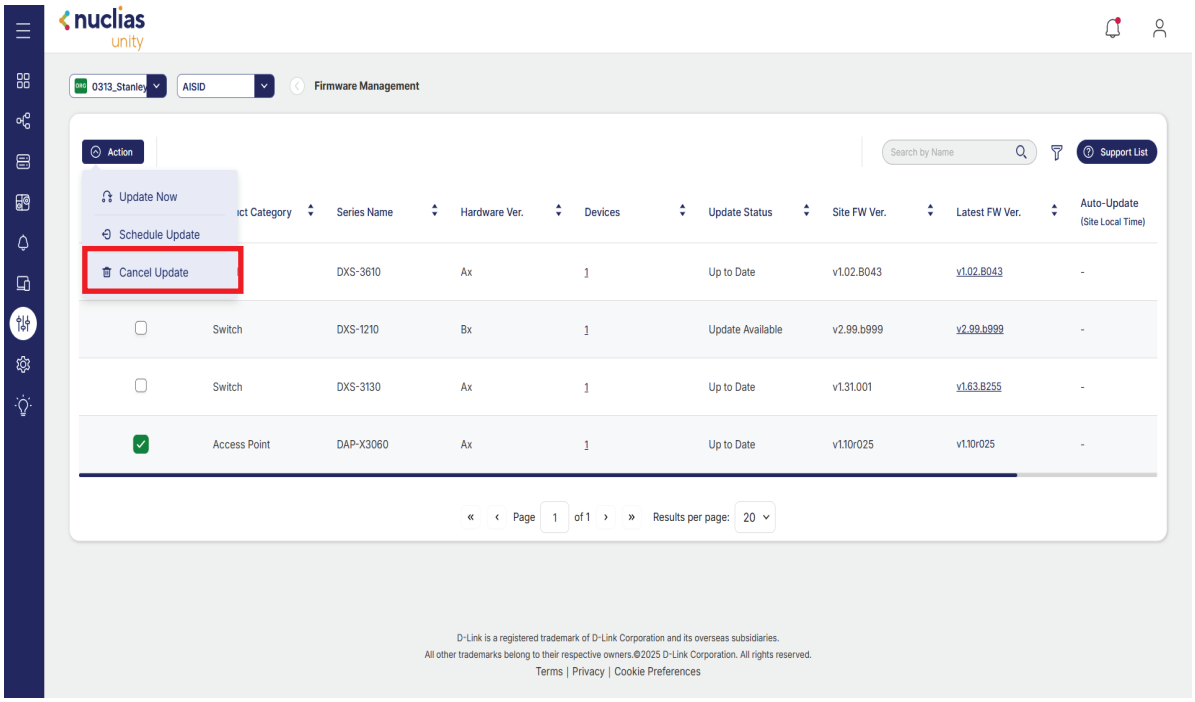
Nuclias Unity Dashboard FW Management Cancel Update

The scheduled update can also be canceled; you can cancel the firmware update before it begins.

Select the device for which you need to cancel the firmware update.

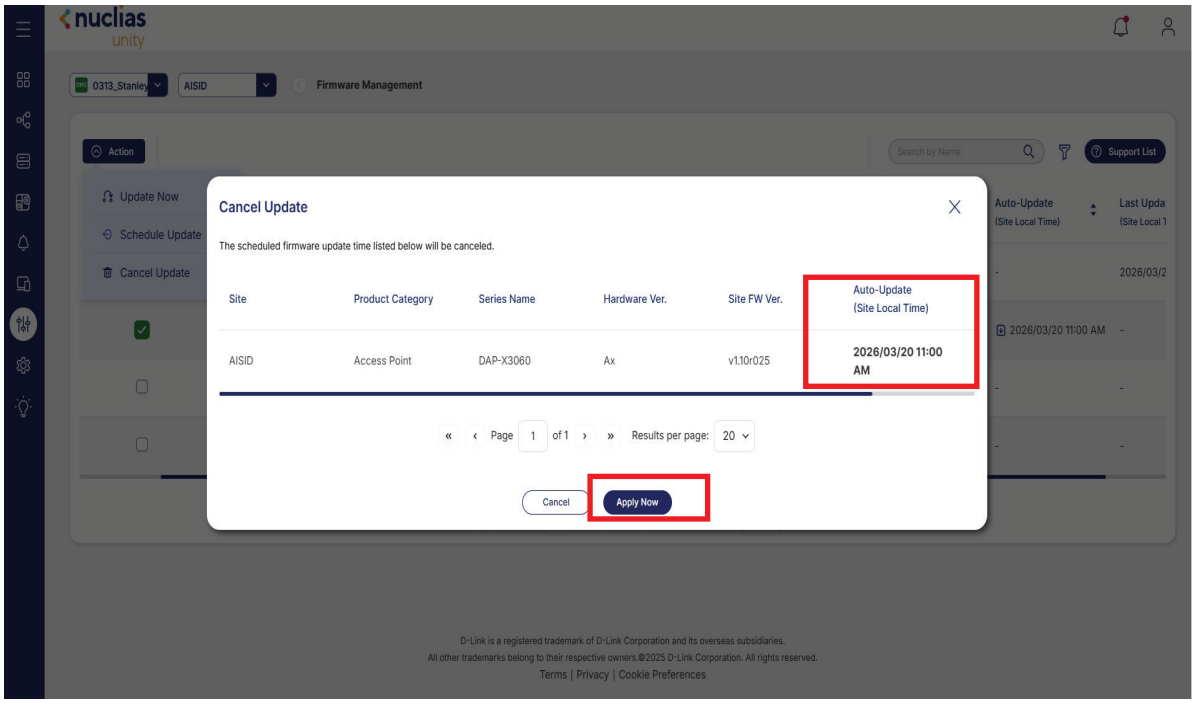


Then **Action** option will appear on the top left corner; click it and select **Cancel Update**.

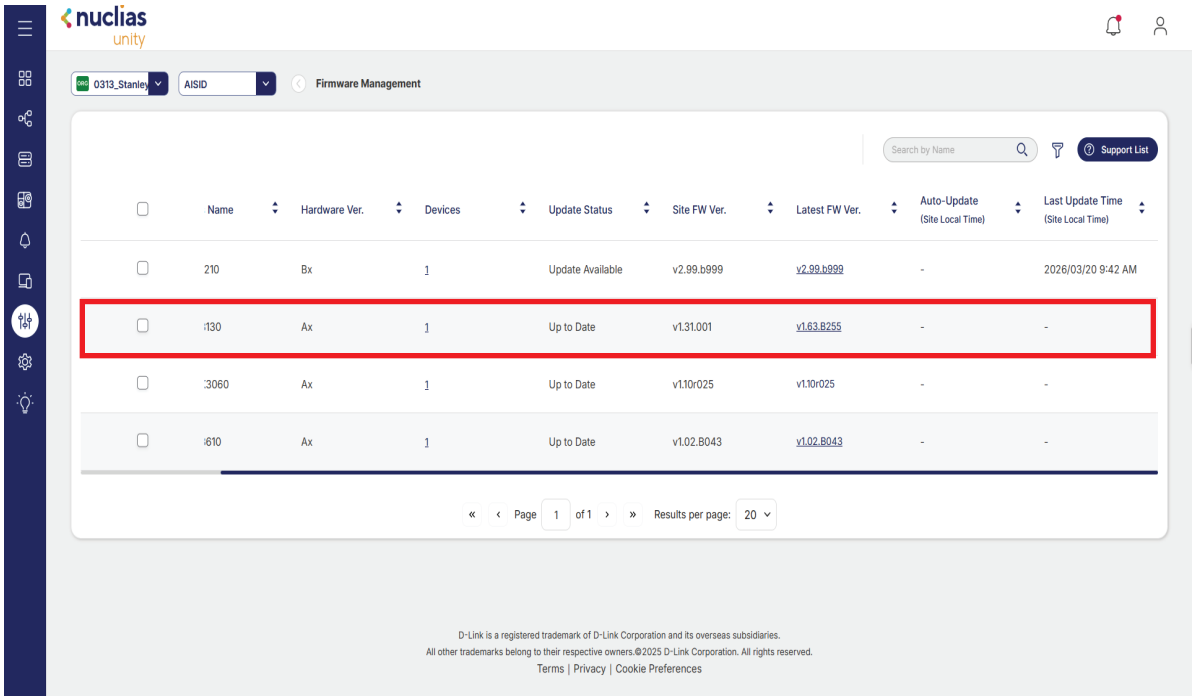


Nuclias Unity Dashboard FW Management Cancel Update

After selecting **Cancel Update**, a new window will appear. In this window, review the scheduled time and click **Apply Now** to confirm the cancellation.



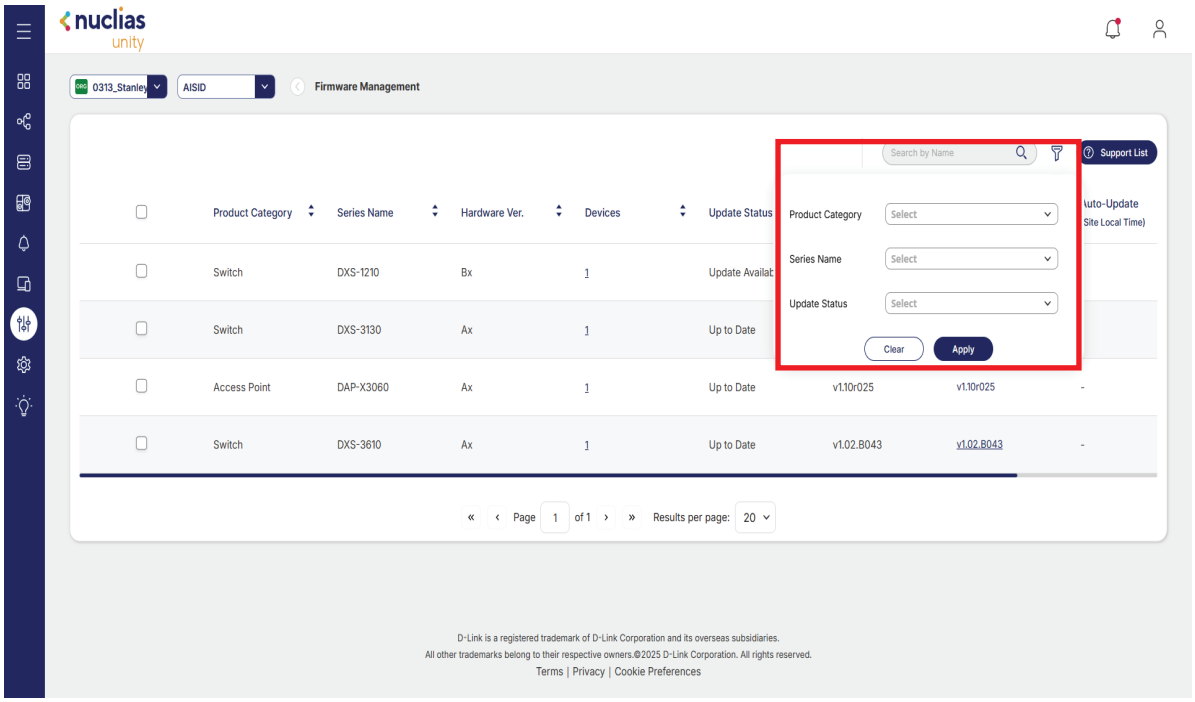
Now navigate back to the devices and check the **Auto-Update** section to ensure the scheduled updates have been canceled.



Nuclias Unity Dashboard FW Management Filter

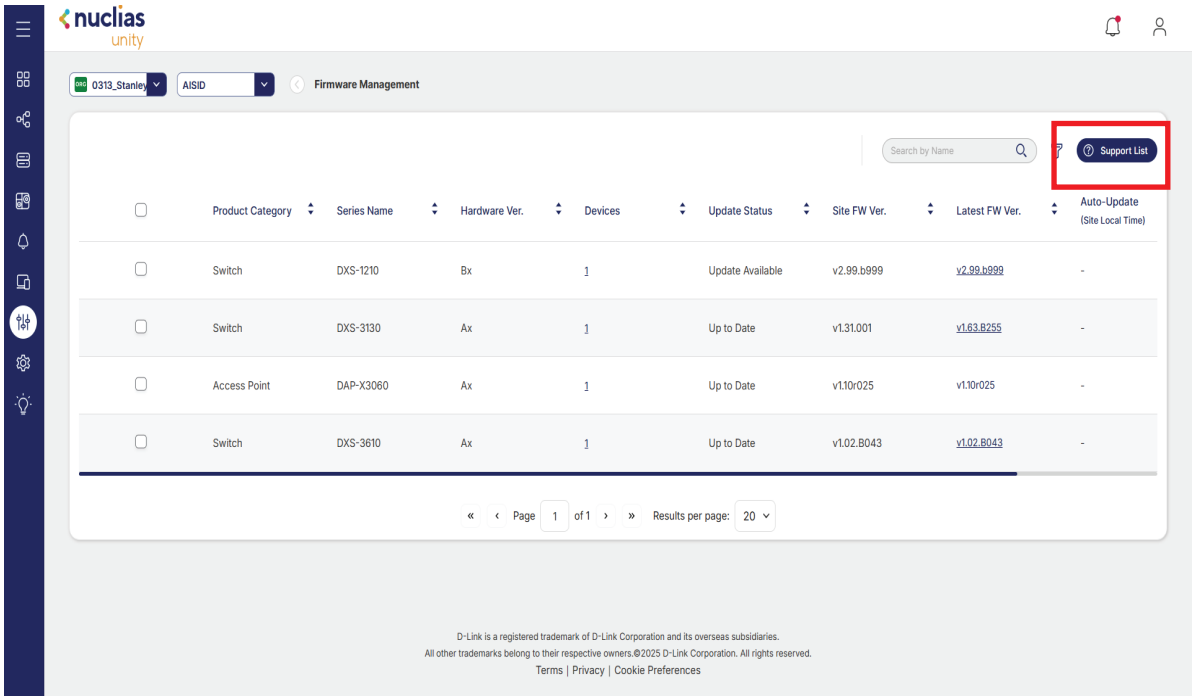
In Firmware Management, the **Filter** option allows you to refine the device list based on specific criteria such as **Product Category, Series Name and Update Status**. Click the filter icon located in the top right corner of the main content area to expand the filtering panel, then select your desired criteria to quickly locate and manage devices that require firmware updates. This feature helps streamline the firmware management process by allowing you to focus on specific devices or groups across your network.

- **Product Category:** Filter by device type, such as Access Point or Switch, to focus on either wireless or wired devices.
- **Series Name:** Filter by the specific product series or model family to manage devices with similar hardware characteristics.
- **Update Status:** Filter by the current firmware state, such as Up to Date, Update Available, Update Failed, or In Progress, to quickly identify devices that need attention.



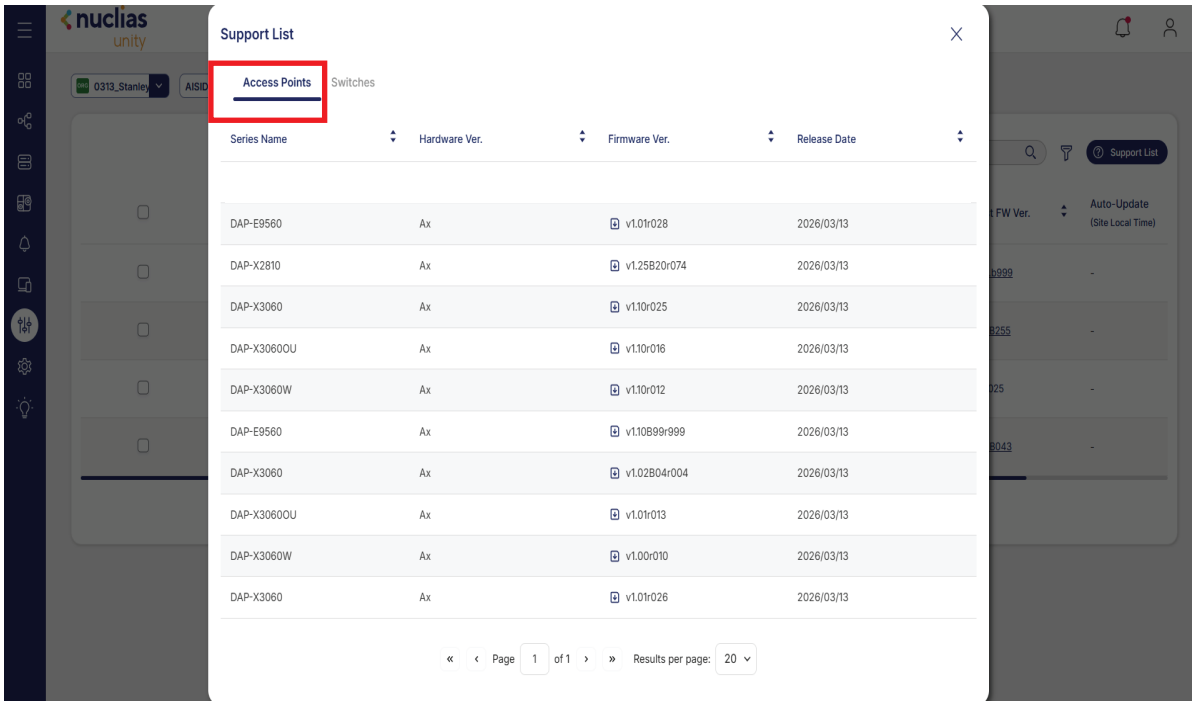
Nuclias Unity Dashboard FW Management Support List

In **Firmware Management**, users can view which supporting models can be managed through the Nuclias Unity Cloud Management platform for both Access Points and Switches. To access this information, navigate to **Firmware Management** from the left side menu bar, then click the **Support List** option located in the top right corner of the main content area. This will display a comprehensive list of all supported Access Point and Switch models that are compatible with firmware management through the Nuclias Unity platform, helping administrators verify device compatibility before performing updates.



Nuclias Unity Dashboard FW Management Support List

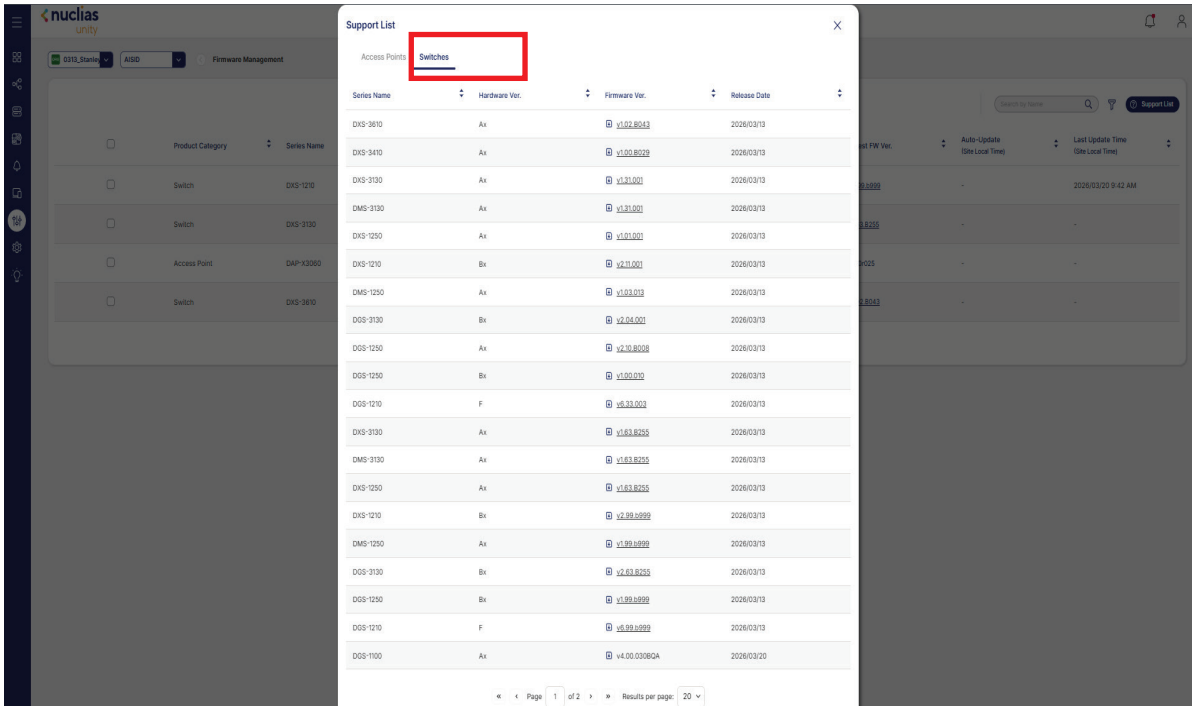
From the Support List, select **Access Points** to display all Access Point models that are compatible with firmware management through the Nuclias Unity Cloud Management platform. This allows network administrators to quickly verify device compatibility before performing firmware updates.



Parameter	Description
Series Name	Indicates the specific product series or model family of the device, allowing administrators to easily identify and group compatible devices.
Hardware Version	Displays the hardware revision of the device, which is essential for selecting the correct firmware version that is compatible with the device's physical components.
Firmware Version	Shows the latest available firmware version for the device, helping administrators verify the most current update available through the Nuclias Unity Cloud Management platform.
Release Date	Indicates the date when the firmware version was released, allowing administrators to track the recency of updates and plan upgrade schedules accordingly.

Nuclias Unity Dashboard FW Management Support List

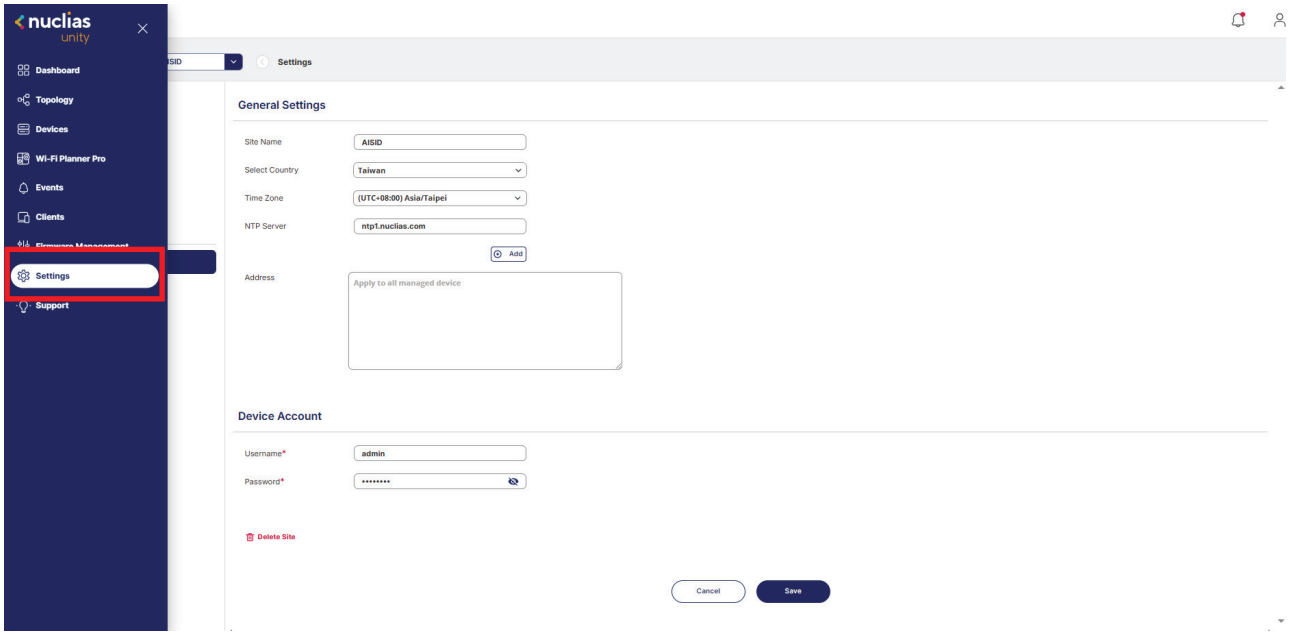
From the Support List, select **Switches** to display all Switch models that are compatible with firmware management through the Nuclias Unity Cloud Management platform. This allows network administrators to quickly verify device compatibility before performing firmware updates.

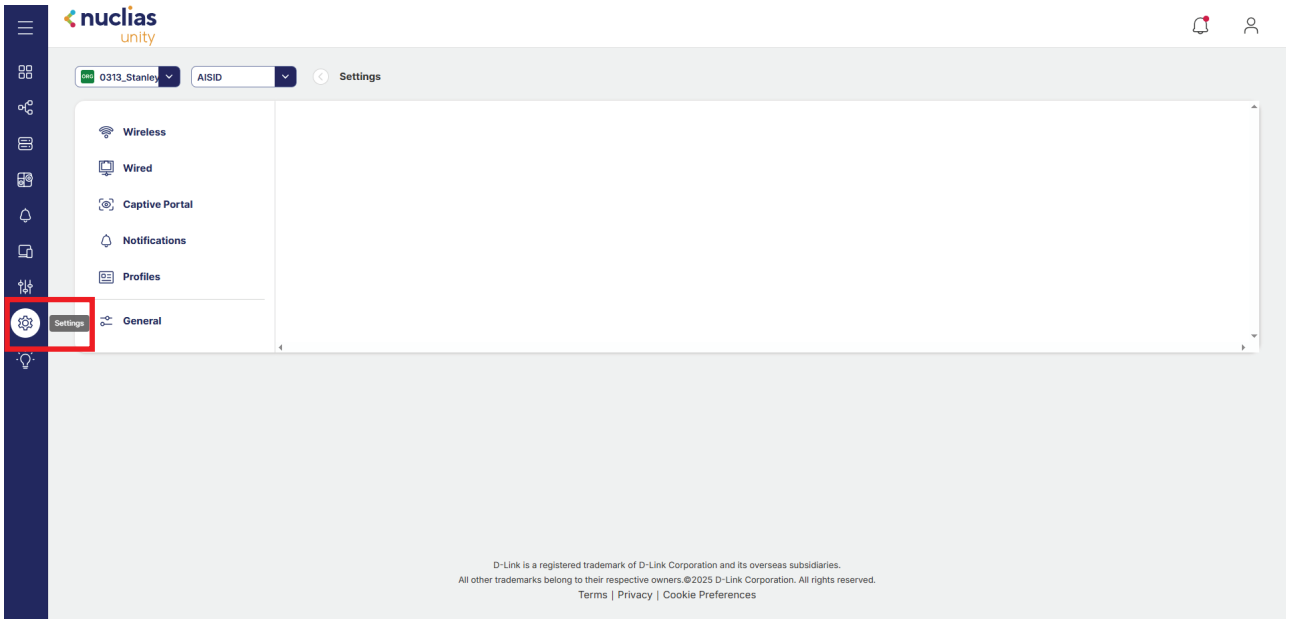


Parameter	Description
Series Name	Indicates the specific product series or model family of the device, allowing administrators to easily identify and group compatible devices.
Hardware Version	Displays the hardware revision of the device, which is essential for selecting the correct firmware version that is compatible with the device's physical components.
Firmware Version	Shows the latest available firmware version for the device, helping administrators verify the most current update available through the Nuclias Unity Cloud Management platform.
Release Date	Indicates the date when the firmware version was released, allowing administrators to track the recency of updates and plan upgrade schedules accordingly.

Nuclias Unity Dashboard Settings

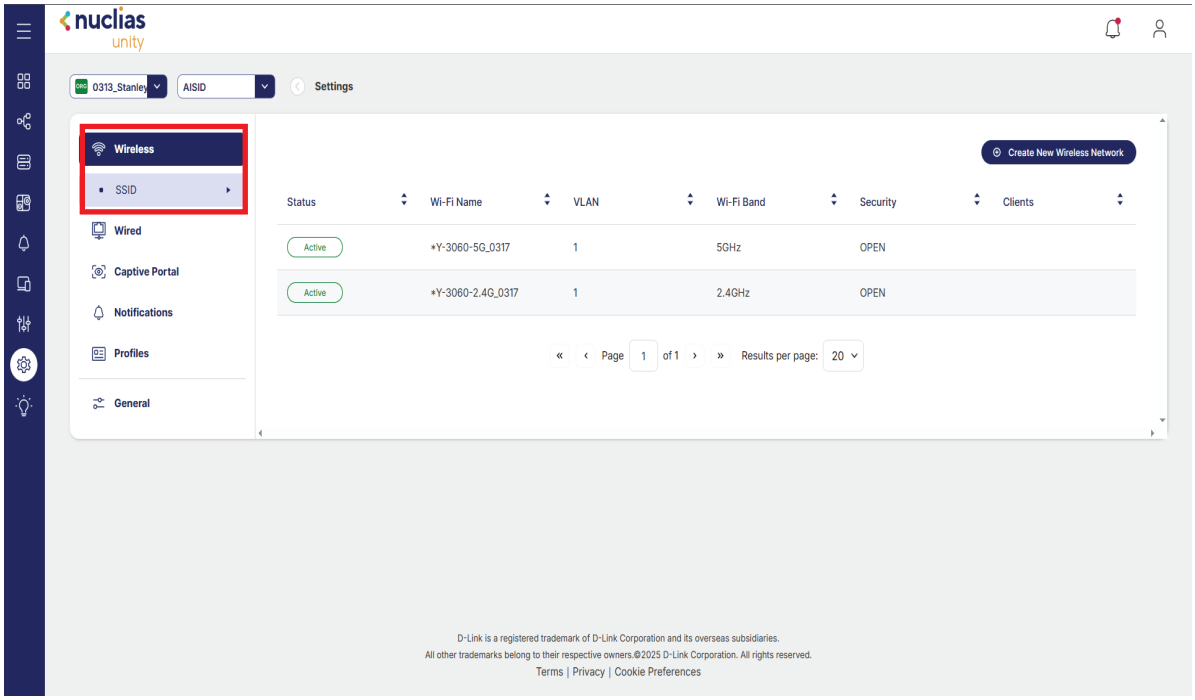
To access the **Settings** section in Nuclias Unity, navigate from the **Dashboard** and click **Settings** located on the left side menu bar. The **Settings** section allows network administrators to configure various system preferences, manage account settings, and customize platform behavior according to organizational requirements. From here, users can adjust global settings, site configurations, and other administrative controls to optimize their **Nuclias Unity Cloud Management** experience.





Nuclias Unity Dashboard Settings Wireless

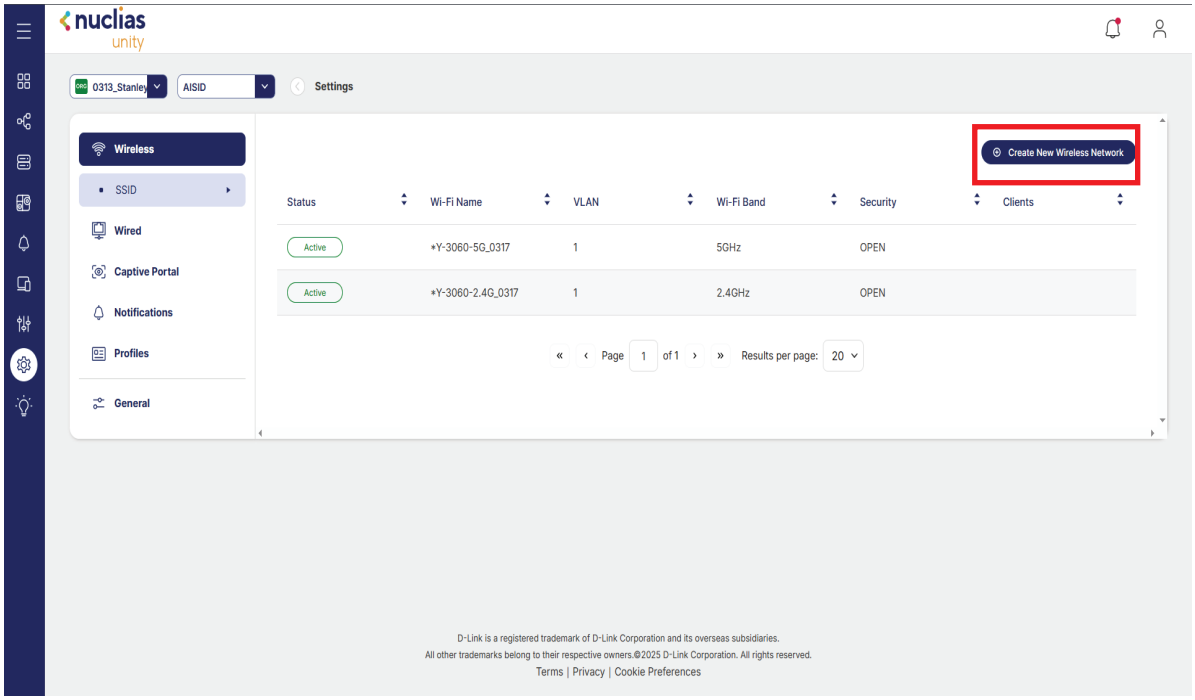
To configure wireless network settings in **Nuclias Unity**, navigate from the **Dashboard** to **Settings** on the left side menu bar. From there, select **Wireless**, then click **SSID** to access the SSID management section. This area allows network administrators to create, configure, and manage wireless network names (SSIDs) for access points across the network. Here, you can define SSID profiles, set security protocols, configure VLAN assignments, and apply SSID settings to specific sites or device groups to ensure secure and organized wireless connectivity.



Parameter	Description
Status	Indicates whether the SSID is currently enabled or disabled, allowing administrators to activate or deactivate the wireless network as needed.
Wi-Fi Name	Displays the service set identifier, which is the public name of the wireless network that appears to users when connecting.
VLAN	Shows the VLAN assigned to the SSID, enabling network segmentation and traffic isolation for the wireless network.
Wi-Fi Band	Indicates which wireless frequency band the SSID operates on, such as 2.4 GHz, 5 GHz, or both, allowing optimization for device compatibility and performance.
Security	Displays the security protocol applied to the SSID, such as WPA2, WPA3, or Open, ensuring appropriate encryption and access control for the wireless network.
Clients	Shows the number of client devices currently connected to the SSID, providing visibility into wireless network usage and capacity.

Nuclias Unity Dashboard Settings Wireless

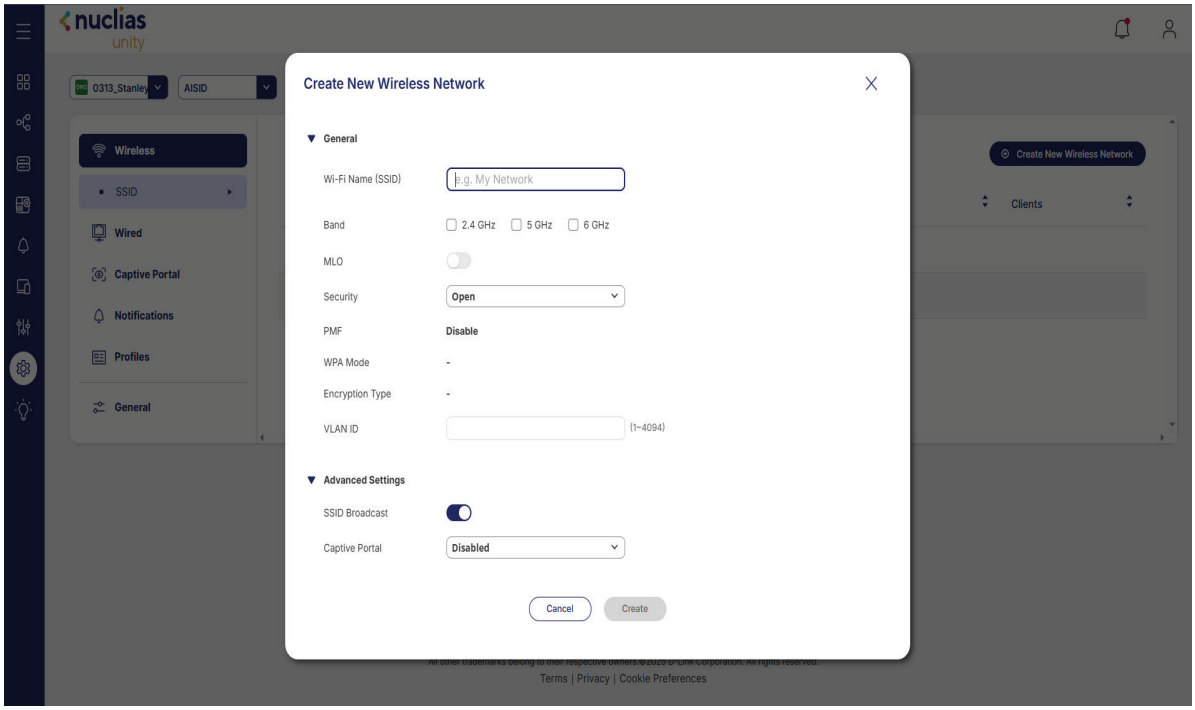
To create a new wireless network, click **Create New Wireless Network** in the SSID section. This will open a configuration wizard where you can define the settings for the new SSID, including the Wi-Fi Name, VLAN assignment, Wi-Fi Band, Security protocol, and other advanced options. Once configured, the new wireless network will be available for deployment to selected access points or sites across your network.



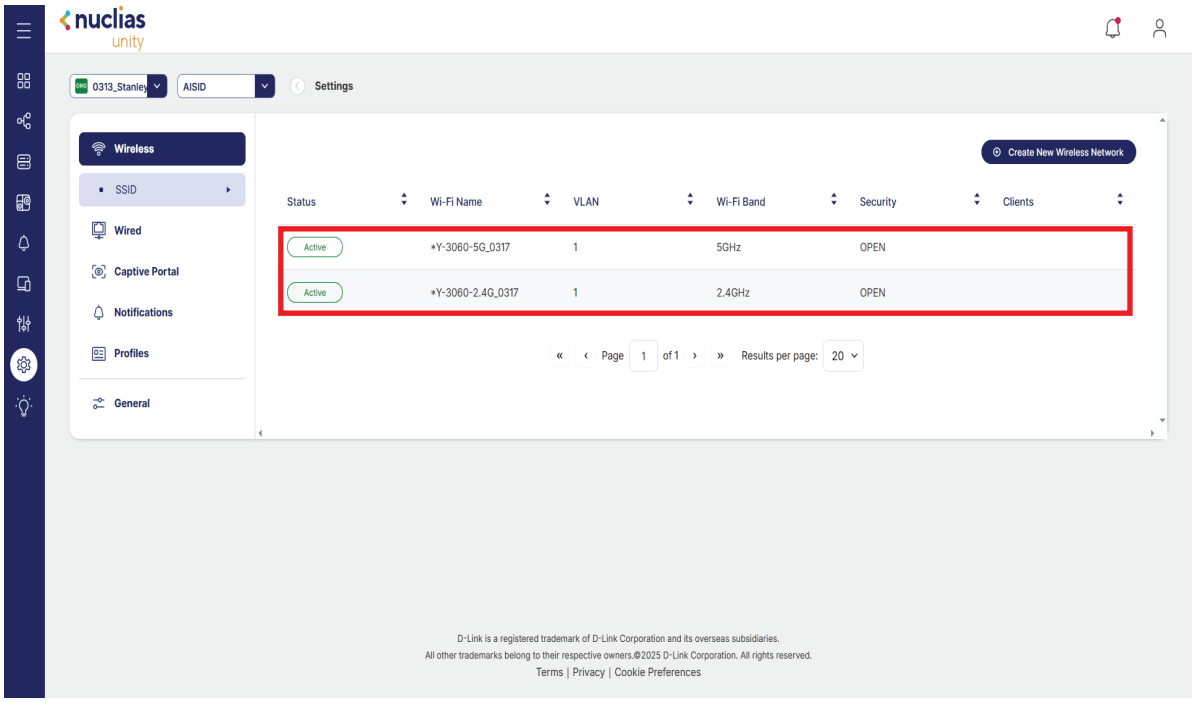
Nuclias Unity Dashboard Settings Wireless

To create a new wireless network, click **Create New Wireless Network** in the SSID section. This will open a configuration wizard where you can define the settings for the new SSID, including the Wi-Fi Name, VLAN assignment, Wi-Fi Band, Security protocol, and other advanced options. Once configured, the new wireless network will be available for deployment to selected access points or sites across your network.

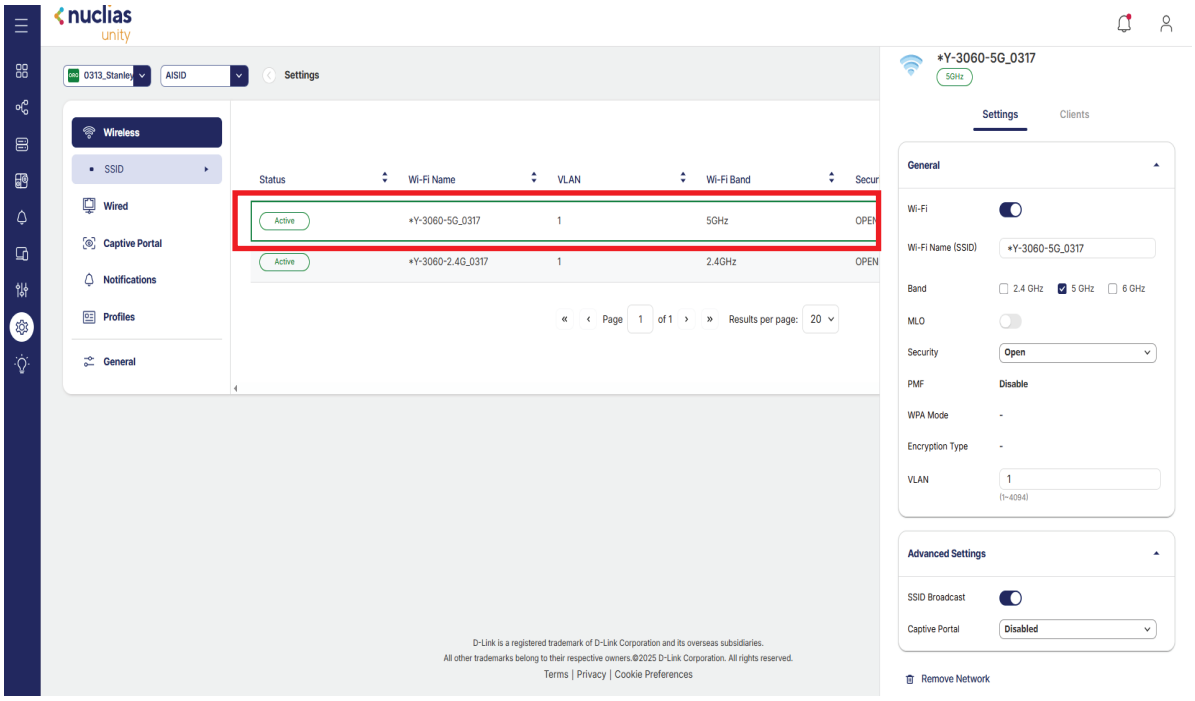
- After clicking **Create New Wireless Network**, begin by completing the **General** section with all required information. Enter the **SSID Name** to identify the wireless network, select the appropriate **Band** (2.4 GHz, 5 GHz, or both), choose the **Security protocol** (such as WPA2 or WPA3) to ensure network protection, and assign a **VLAN ID** for traffic segmentation.
- Once the general settings are configured, proceed to the **Advanced Settings** section, where you can **enable or disable SSID Broadcast** to control whether the network name is visible to clients, and e**nable or disable Captive Portal** to require user authentication or acceptance of terms before granting network access. After configuring these settings, click **Create** and save to create the new wireless network.



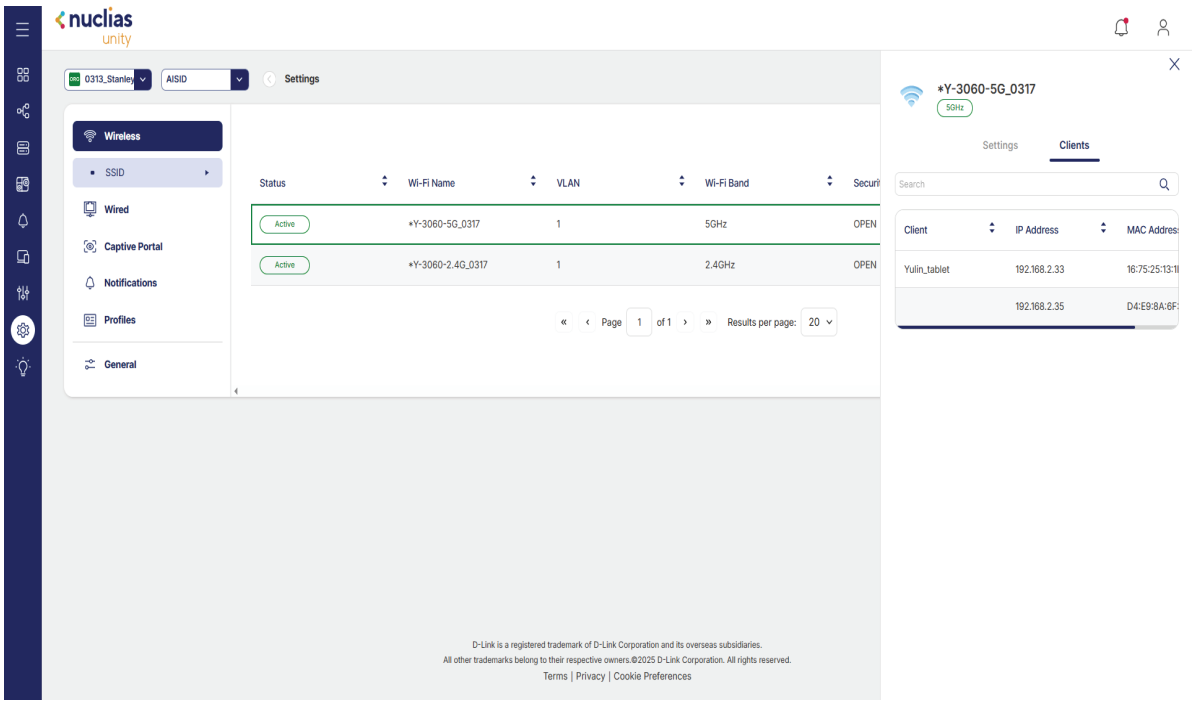
After creating a new wireless network, the newly created SSID name will appear in the **SSID** section, where you can view, edit, or manage its settings as needed.



Select the newly created SSID, and the settings window will appear on the right side. In this window, you can **Edit** the SSID information or **Remove** the active SSID as needed.



Following the Settings option, users can view connected client information in the **Client** section. This section displays detailed data about all clients currently connected to the network, including client name, **IP address, MAC address**, connection status, and other relevant details for monitoring and troubleshooting purposes.



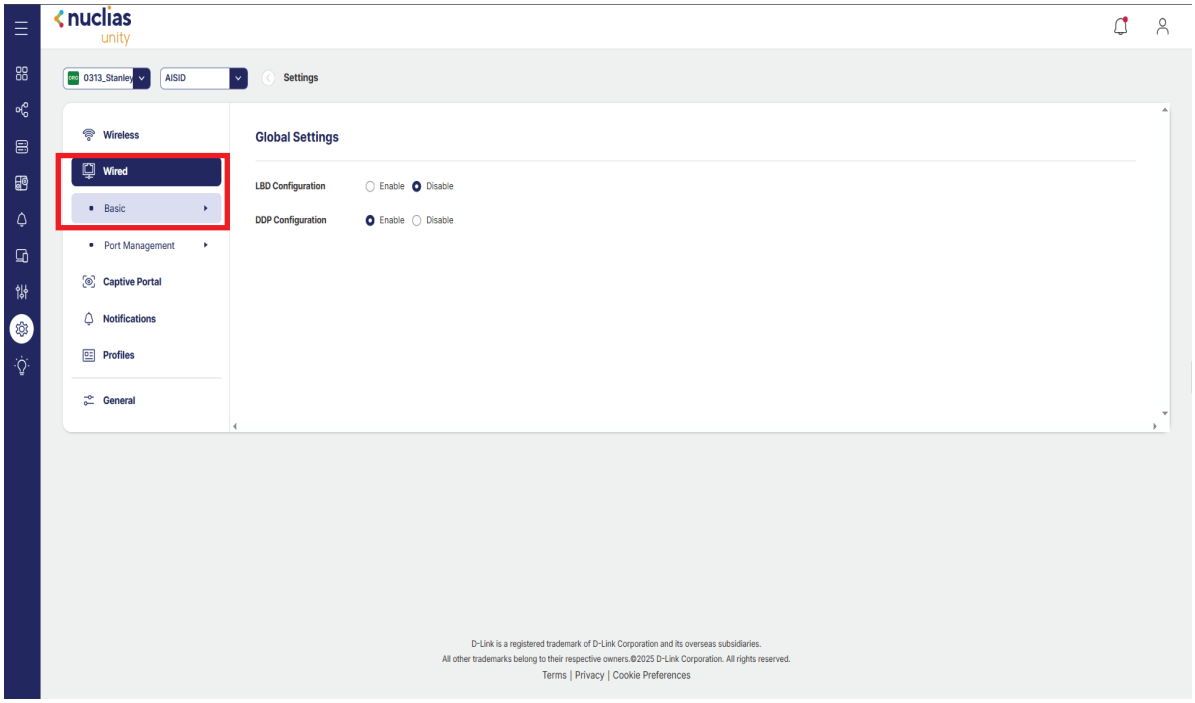
Nuclias Unity Dashboard Settings Wired

To configure wired network settings in Nuclias Unity, navigate from the **Dashboard** to **Settings** on the left side menu bar. From there, select **Wired** to access the wired network configuration section. This area allows network administrators to manage switch settings, configure VLANs, define port profiles, and apply wired network policies across connected switches to ensure optimal performance and security for the wired infrastructure.

Select **Basic** to access the **Global Settings**, where you can configure fundamental network parameters that apply across the entire wired infrastructure.

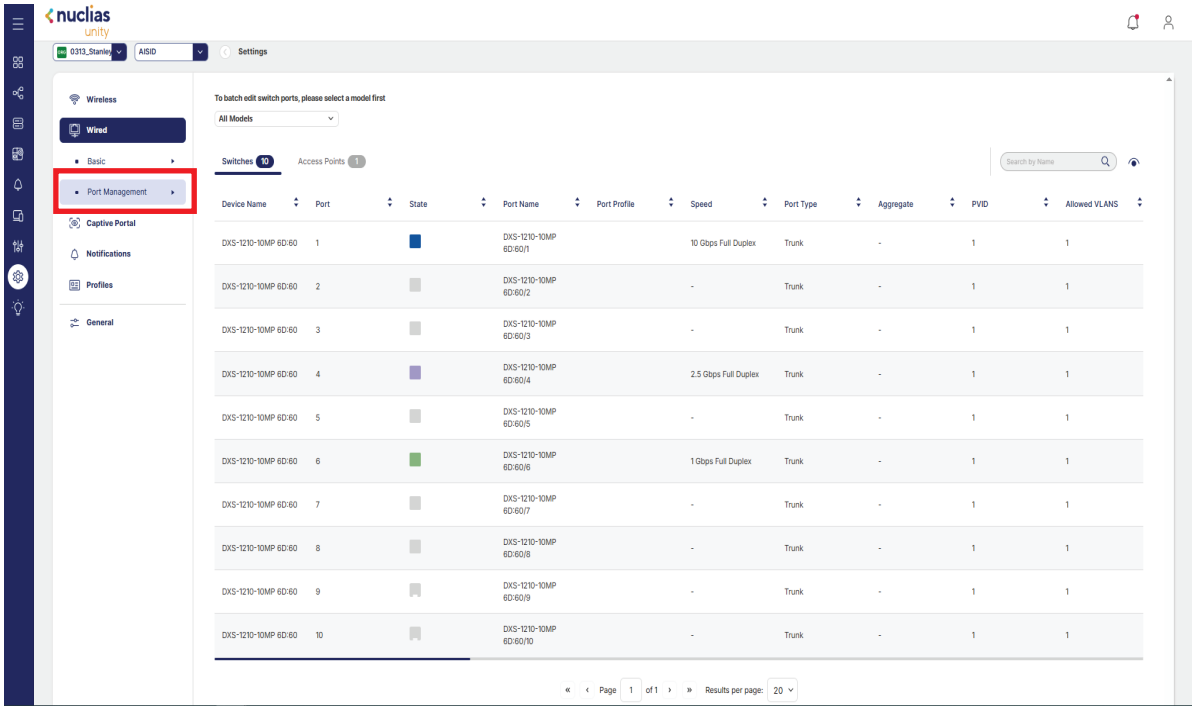
LBD Configuration (Loop Back Detection): Detects network loops on ports or VLANs and automatically blocks the affected traffic path to prevent broadcast storms and improve network stability.

DDP Configuration (Device Discovery Protocol): This feature enables automatic discovery and identification of connected devices on physical ports and port-channel interfaces, helping simplify device management and improve network visibility.



Nuclias Unity Dashboard Settings Wired

In the Wired section under Settings, **Port Management** allows administrators to configure and manage port settings for both **Switches** and **Access Points**. This feature provides control over individual port parameters such as enabling or disabling ports, configuring VLAN assignments, setting speed and duplex modes, and applying PoE (Power over Ethernet) settings. Port Management enables precise control over network connectivity and device power delivery, ensuring optimal performance and reliability for all wired connections across the network infrastructure.



Nuclias Unity Dashboard Settings **Wired**

In Port Management under the Wired section, administrators can view and configure the following parameters for Switches:

Parameter	Description
Device Name	Identifies the specific switch or access point being managed.
Port	Displays the physical port number or identifier on the device.
State	Indicates whether the port is currently enabled (up) or disabled (down).
Port Name	Allows a custom name to be assigned to the port for easy identification.
Port Profile	Shows the port profile applied, which contains predefined configuration settings.
Speed	Displays the negotiated or configured speed and duplex mode (e.g., 1 Gbps Full Duplex).
Port Type	Indicates the port type, such as Ethernet, SFP, or PoE.
Aggregation	Shows whether the port is part of a link aggregation group (LAG) for increased bandwidth.
PVID	Displays the Port VLAN ID used for untagged traffic on the port.
PoE Power Usage (W)	Shows the current Power over Ethernet consumption in watts for PoE-enabled ports.
Model Name	Displays the specific model of the switch or access point.
RSTP	Indicates whether RSTP is enabled to prevent network loops.
LBD	Shows whether loop detection is enabled to prevent network loops.
DDP	Indicates whether device discovery is enabled for automatic network device identification.
LLDP	Shows whether LLDP is enabled for neighbor device discovery and network topology mapping.
STP Guard	Displays whether Spanning Tree Protocol guard is enabled to prevent unauthorized topology changes.
Port Schedule	Shows whether a schedule is configured to automatically enable or disable the port at specific times.
PoE Schedule	Indicates whether a schedule is configured for PoE power delivery to connected devices.
Access Policies	Displays any access control policies applied to the port for security enforcement.
Mirror	Shows whether port mirroring is enabled for traffic analysis or monitoring.
Port Isolate	Indicates whether port isolation is enabled to prevent communication between specific ports.
Tags	Displays any metadata tags assigned to the port for organization and filtering.
Flow Control	Shows whether flow control is enabled to manage network congestion.
Number of IGMP Group	Indicates the number of IGMP groups active on the port for multicast traffic management.

Parameter	Description
Device IP	Displays the IP address assigned to the switch or access point for network identification and management.
Tx Traffic	Shows the total amount of transmitted data (outgoing traffic) on the port, typically measured in bytes or megabytes.
Rx Traffic	Shows the total amount of received data (incoming traffic) on the port, typically measured in bytes or megabytes.
Tx Multicast	Displays the total amount of multicast data transmitted from the port, used for one-to-many communication.
Rx Multicast	Displays the total amount of multicast data received on the port.
Tx Broadcast	Shows the total amount of broadcast data transmitted from the port, used for network-wide communication.
Rx Broadcast	Shows the total amount of broadcast data received on the port.
Tx Packets	Displays the total number of data packets transmitted from the port.
Rx Packets	Displays the total number of data packets received on the port.
Total Traffic	Shows the combined total of transmitted and received traffic on the port, providing an overall view of port utilization.

Nuclias Unity Dashboard Settings **Wired**

In **Port Management**, select any port to view all the information in the **General** section. This section provides a comprehensive overview of the selected port, organized into the following categories:

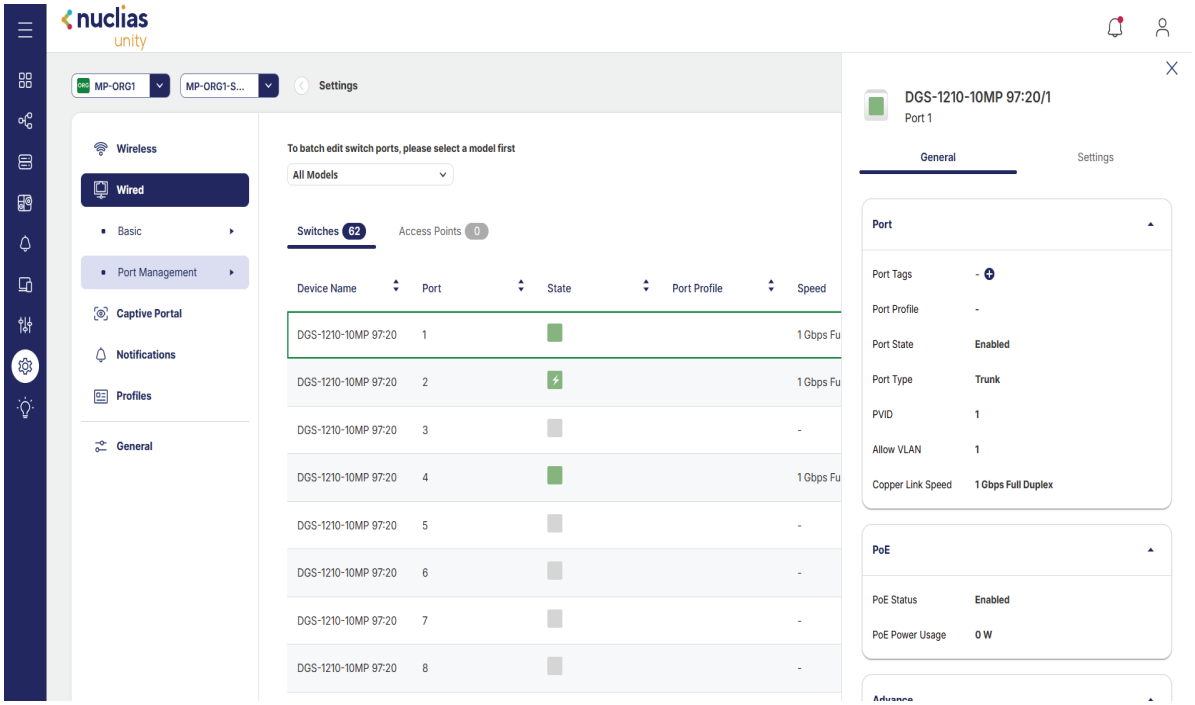
Port Information: Displays basic port details such as port name, port status, link speed, duplex mode, and PVID. This information helps administrators quickly assess the operational state of the port.

PoE Information: Shows Power over Ethernet details for PoE-enabled ports, including power consumption in watts, power allocation, and PoE status. This allows administrators to monitor power usage and ensure sufficient power delivery to connected devices.

Advanced Information: Provides additional configuration details such as port profile assignments, allowed VLANs, enabled features (e.g., LBD and DDP), and security settings like port isolation and flow control.

Device Information: Displays information about the device connected to the port, including device name, MAC address, and connection status, helping administrators identify and troubleshoot connected endpoints.

This centralized view enables efficient monitoring and management of individual ports, ensuring optimal network performance and quick resolution of port-related issues.



Nuclias Unity Dashboard Settings **Wired**

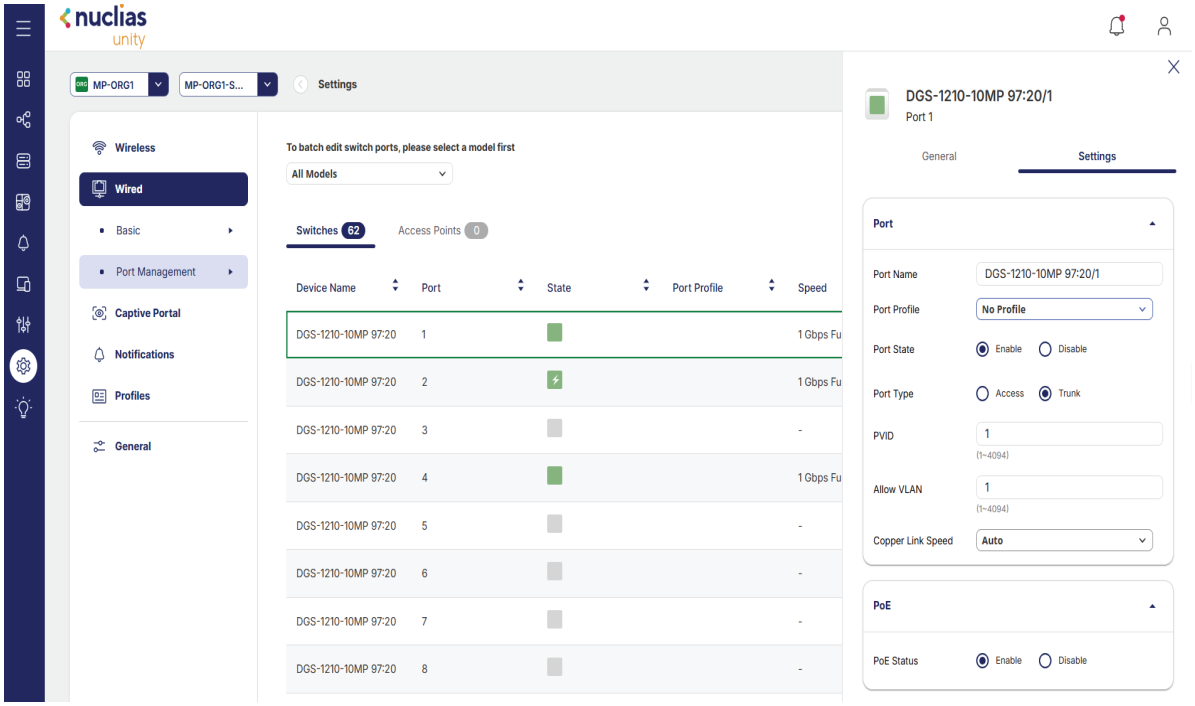
In **Port Management**, after selecting a port, administrators can configure its settings directly within the **Settings** section. The following configuration options are available for modification:

Port Settings: Modify basic port parameters such as port status (enable or disable), port name, link speed, duplex mode, and PVID to adjust connectivity and VLAN assignment.

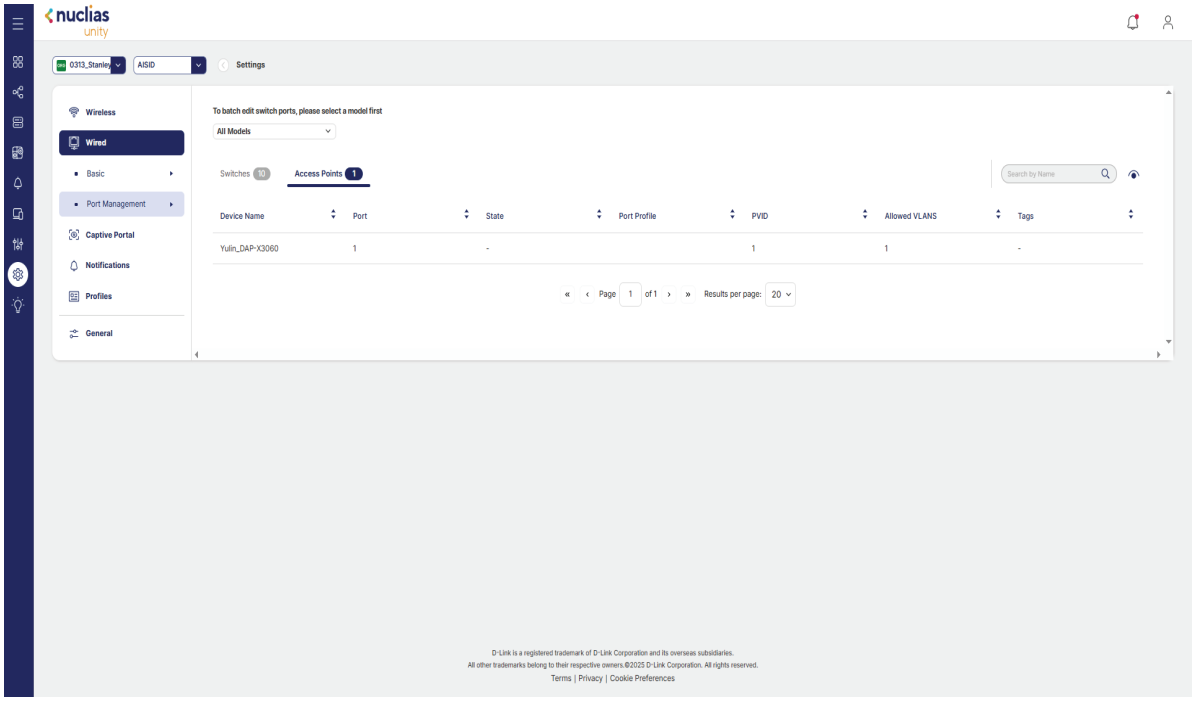
PoE Settings: Configure Power over Ethernet settings for PoE-enabled ports, including enabling or disabling PoE, setting power limits, and applying PoE schedules to control power delivery based on time or usage.

Advanced Settings: Adjust advanced port features such as enabling Loop Back Detection (LBD), Device Discovery Protocol (DDP), Link Layer Discovery Protocol (LLDP), port isolation, flow control, and port mirroring to enhance network performance, security, and monitoring capabilities.

These configurable options allow network administrators to fine-tune port behavior to meet specific network requirements and ensure optimal device connectivity.



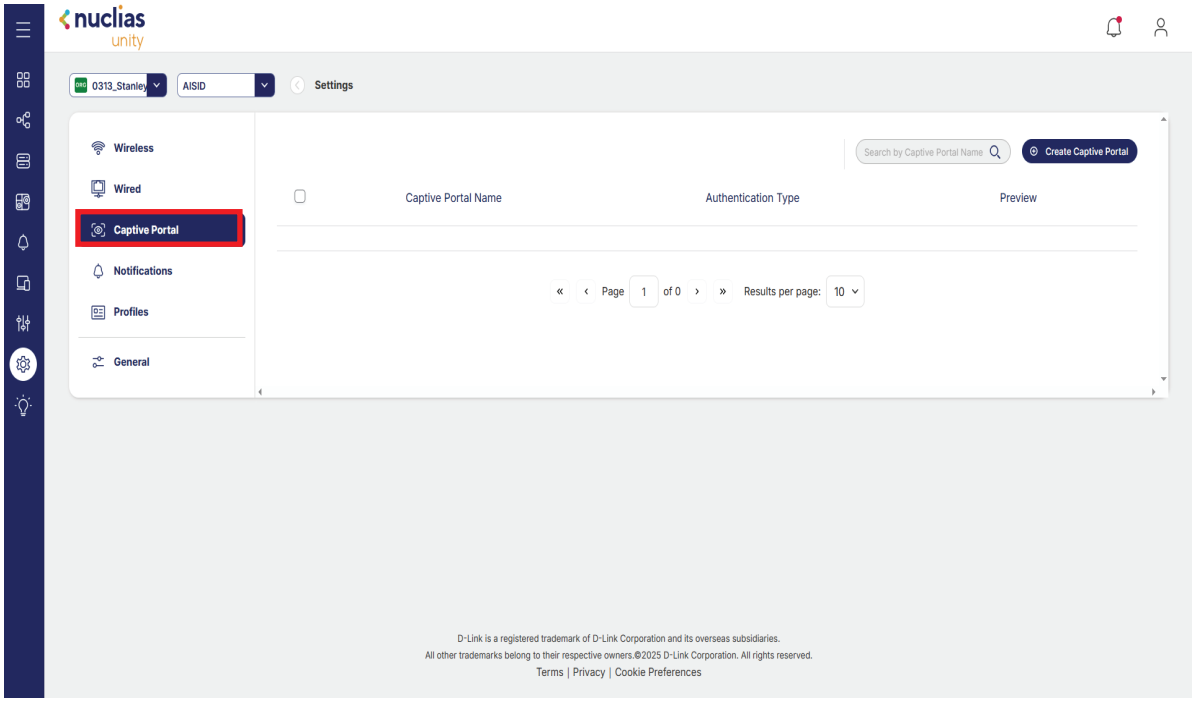
In Port Management under the Wired section, the following parameters are available for Access Points:



Parameter	Description
Device Name	Identifies the specific access point being managed.
Port	Displays the physical port number on the access point, typically indicating the Ethernet interface.
State	Indicates whether the port is currently enabled (up) or disabled (down).
Port profile	Shows the port profile applied to the access point port, which contains predefined configuration settings such as VLAN assignments and network policies.
PVID	Displays the total amount of multicast data received on the port. Displays the Port VLAN ID assigned to the access point port, which determines the VLAN for untagged traffic received on the port.
Allows VLANS	Lists the VLANs that are permitted on the access point port, allowing traffic from multiple VLANs to pass through while maintaining network segmentation.
Tags	Displays any metadata tags assigned to the access point port for organization, filtering, and easy identification within the network management platform.

Nuclias Unity Dashboard Settings Captive Portal

To configure **Captive Portal** settings in Nuclias Unity, navigate from the **Dashboard** to **Settings** on the left side menu bar. From there, select **Captive Portal** to access the captive portal configuration section. This area allows network administrators to create and manage captive portal authentication pages for guest access or network authentication. Captive portals require users to authenticate, accept terms of service, or provide credentials before gaining network access. Here, you can configure portal appearance, authentication methods (such as social login, RADIUS, or voucher-based access), access policies, and session settings to ensure secure and controlled network access for guests and temporary users.

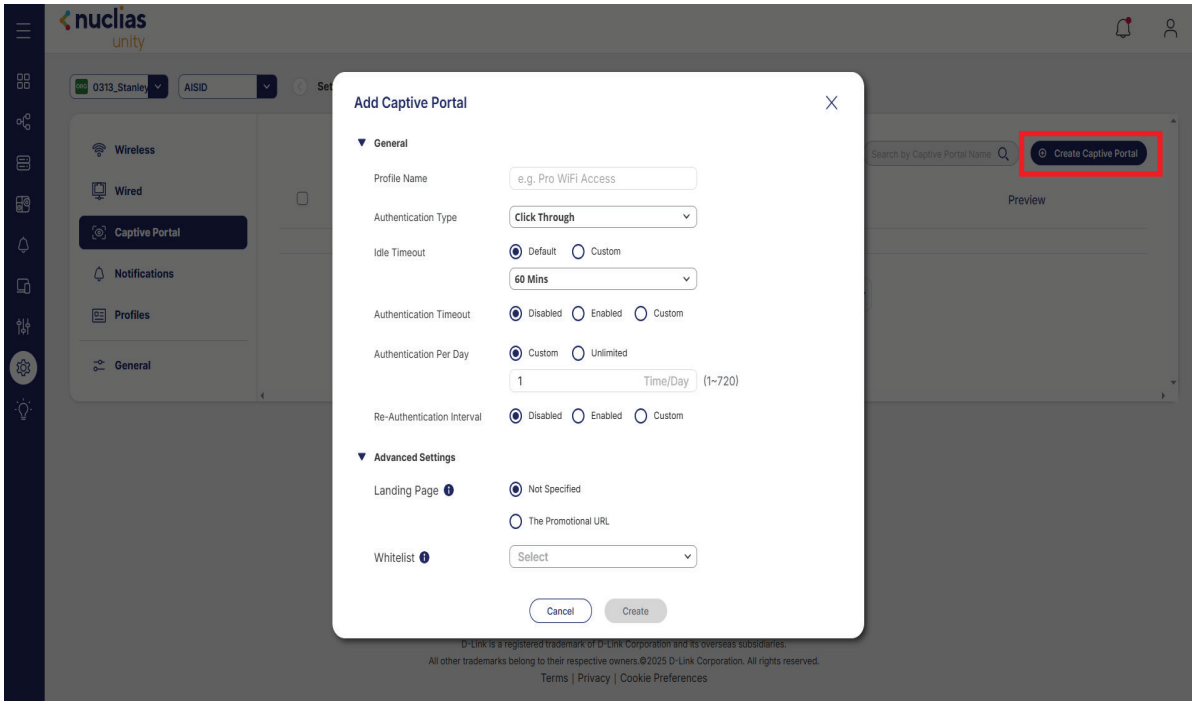


Parameter	Description
Captive Portal Name	Displays the unique name assigned to the captive portal profile, allowing administrators to easily identify and manage multiple portal configurations across different sites or networks.
Authentication Type	Indicates the authentication method used by the captive portal, such as Social Login (e.g., Facebook, Google), RADIUS Authentication, Local Authentication, Voucher-Based Access, or Simple Acceptance of terms and conditions.
Preview	Provides a preview option that allows administrators to view the captive portal login page as it will appear to end users before publishing or deploying the configuration, ensuring the design and functionality meet expectations.

Nuclias Unity Dashboard Settings **Captive Portal**

In the top right corner of the **Captive Portal** section, click **Create Captive Portal** to create a new profile. This will open a configuration wizard where you can define the captive portal settings, including the Captive Portal Name, Authentication Type, portal appearance, access policies, and session limitations. Once configured, the new captive portal profile will be available for deployment to selected SSIDs or networks to manage guest access and authentication.

In the **Add Captive Portal** window, fill in the required information to create a new captive portal. Enter a unique **Captive Portal Name** to identify the profile, select the desired Authentication Type (such as Social Login, RADIUS, Local Authentication, or Voucher), and configure additional settings such as portal appearance, access policies, session timeout, and terms of use as needed. Once all required fields are completed, click **Create** the new captive portal profile.



Nuclias Unity Dashboard Settings Notification

To configure **Notification** settings in Nuclias Unity, navigate from the Dashboard to **Settings** on the left side menu bar. From there, select **Notification** to access the notification configuration section. This area allows network administrators to manage alert preferences, define notification rules, and configure delivery methods for system events and network alerts. Here, you can set up email notifications, define severity levels for alerts (such as Critical, Warning, or Info), and specify which events trigger notifications for monitoring and troubleshooting purposes. Proper notification configuration ensures that administrators are promptly informed of important network events and potential issues.

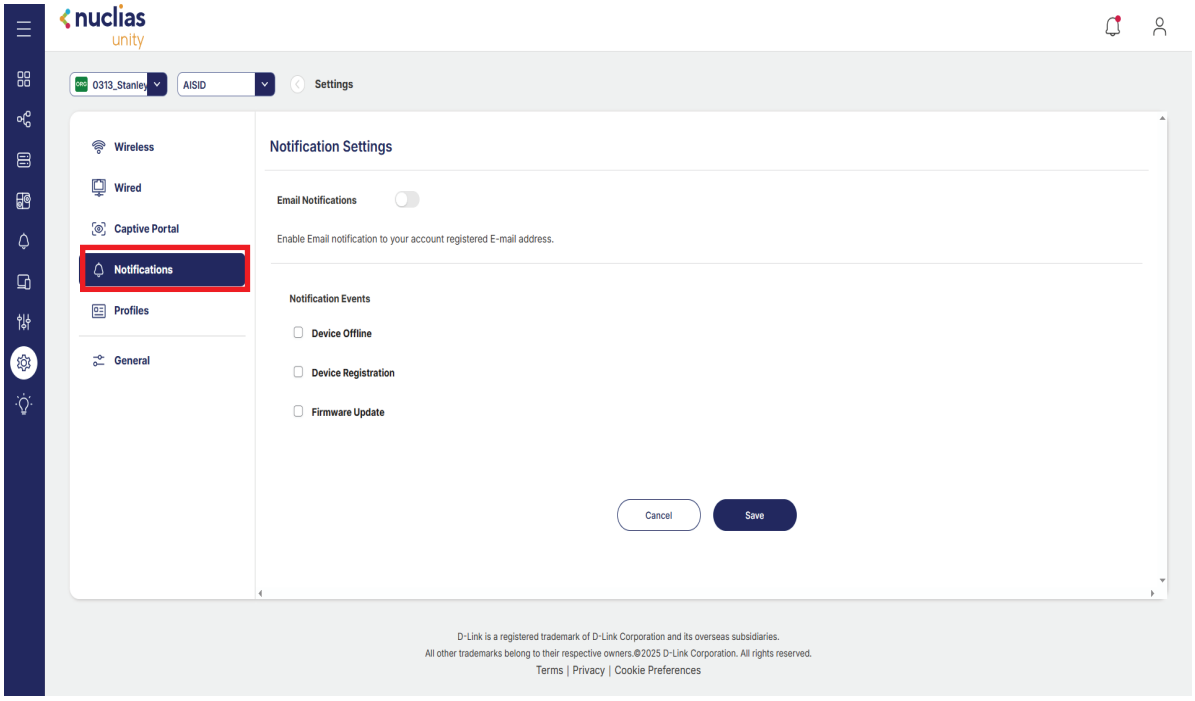
Email Notification: Enables or disables email alerts for system events and network notifications. When enabled, administrators can configure recipient email addresses and define which events trigger email alerts to ensure timely awareness of network activities.

Device Offline: Configures notifications for when devices such as access points or switches go offline. This alert helps administrators quickly respond to network disruptions and minimize downtime.

Device Registration: Configures notifications for device registration events, such as when new devices are added to the network or when device registration status changes. This provides visibility into network expansion and device inventory changes.

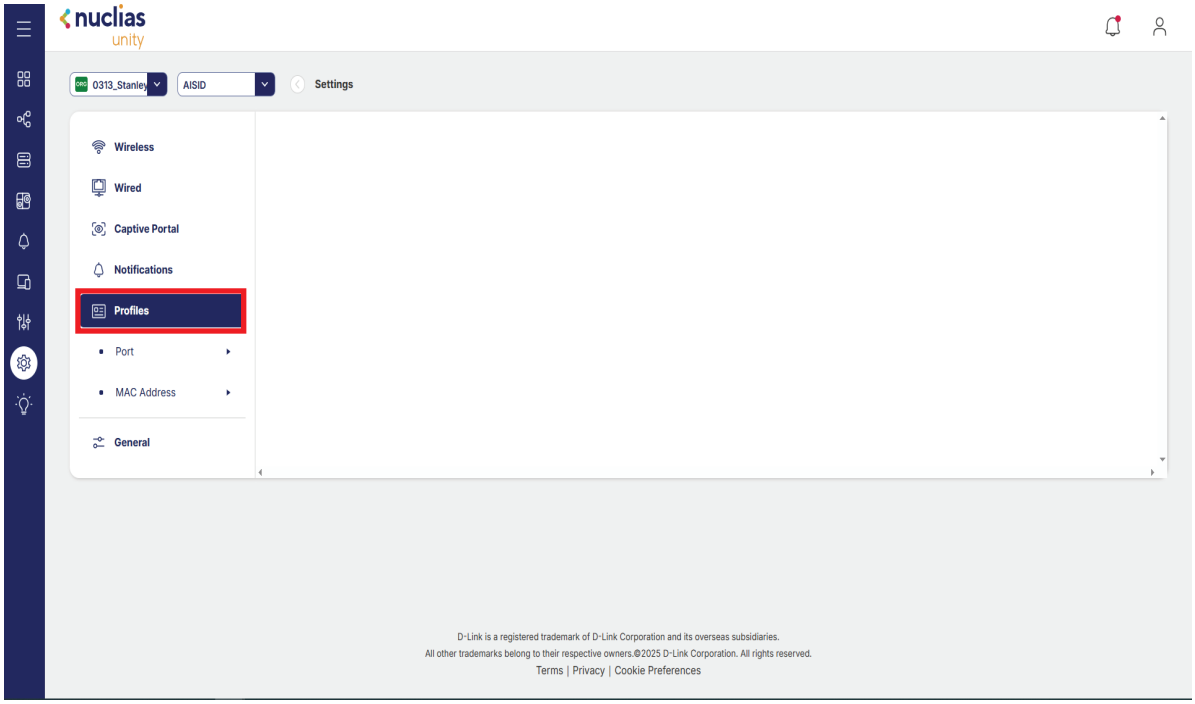
Firmware Upgrade: Configures notifications related to firmware updates, including successful upgrades, failed updates, and available firmware versions. This helps administrators stay informed about device maintenance and ensure devices remain current with the latest firmware releases.

These notification settings enable network administrators to stay informed about critical network events and maintain proactive network management.



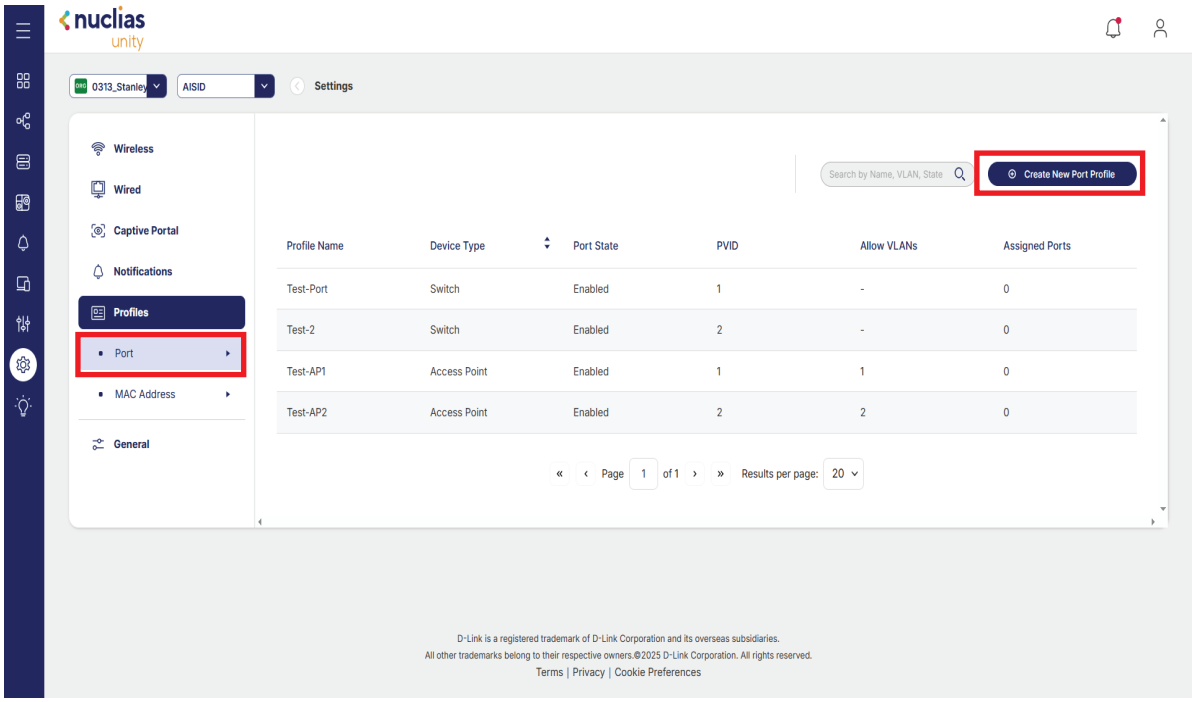
Nuclias Unity Dashboard Settings Profiles

To configure **Profile** for **Port** and **MAC Address** settings in Nuclias Unity, navigate from the **Dashboard** to **Settings** on the left side menu bar. From there, select **Profile** to access the profile management section, where you can configure both **Port Profiles** and **MAC Address Profiles**. Port Profiles allow administrators to define standardized configuration settings for switch ports, including VLAN assignments, PoE settings, and security policies, which can be applied across multiple ports for consistent network configuration. MAC Address Profiles enable the management of MAC-based access controls, allowing specific devices to be authorized, restricted, or assigned to particular VLANs based on their MAC addresses. These profiles streamline network management by simplifying configuration deployment and ensuring consistent policy enforcement across the network infrastructure.



Nuclias Unity Dashboard Settings Profiles

To create a port profile for Switches and Access Points, navigate to Settings from the left side menu bar, then select Profile followed by Port Profile. Click the **Create New Port Profile** button located in the top right corner of the main content area.



Parameter	Description
Profile Name	A unique identifier assigned to the port profile for easy recognition and management across the network.
Device Type	Specifies the type of device the profile is intended for, such as Switch or Access Point, ensuring appropriate settings are applied based on the device category.
Port Status	Defines the default operational state of the port when the profile is applied, allowing administrators to set ports as Enabled or Disabled as needed.
PVID	Sets the Port VLAN ID, which determines the VLAN assignment for untagged traffic received on the port, ensuring proper network segmentation.
Allow VLANs	Lists the VLANs permitted on the port, allowing traffic from multiple specified VLANs to pass through while maintaining network isolation and security.
Assigned Port	Displays the specific ports to which the port profile has been applied, providing visibility into where the profile configuration is currently deployed across switches and access points.

After clicking **Create New Port Profile**, a new window will appear. In this window, first choose either **Switch** or **Access Point** as the device type, then fill in the required information under the following sections:

Port Status: Defines the default operational state of the port when the profile is applied, allowing administrators to set ports as Enabled or Disabled as needed.

Port Type: Selects the specific port type, such as Ethernet, SFP, or PoE, ensuring the profile settings are compatible with the physical port characteristics.

PVID: Sets the Port VLAN ID, which determines the VLAN assignment for untagged traffic received on the switch port, ensuring proper network segmentation.

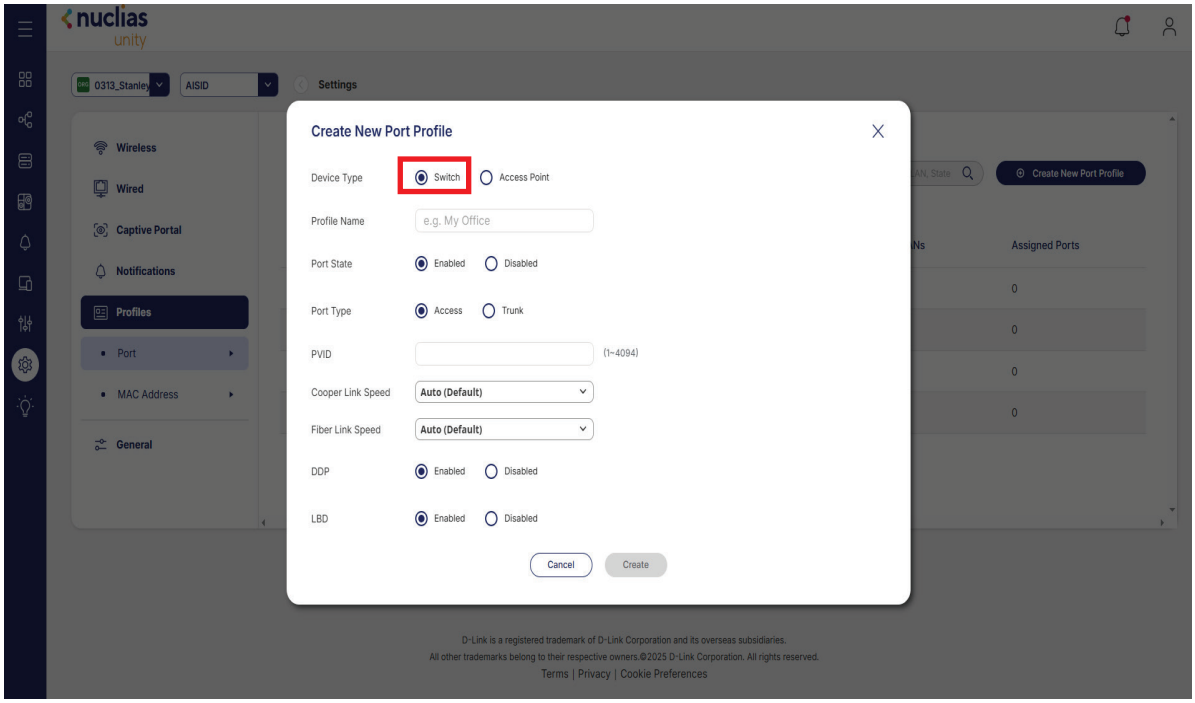
Copper Link Speed: Configures the link speed for copper (RJ-45) ports, such as Auto-Negotiation, 10 Mbps, 100 Mbps, or 1 Gbps, to optimize performance based on connected devices.

Fiber Link Speed: Configures the link speed for fiber (SFP) ports, such as 1 Gbps or 10 Gbps, ensuring proper connectivity for fiber uplinks.

DDP (Device Discovery Protocol): Enables or disables Device Discovery Protocol on the port, allowing automatic detection and identification of connected devices for simplified network management.

LBD (Loop Back Detection): Enables or disables Loop Back Detection on the port to identify and prevent network loops that can cause broadcast storms and network outages.

Once all required information is completed, click **Create** to create the new port profile, which can then be deployed to selected ports across switches or access points as needed.



When creating a port profile for an Access Point, the following parameters must be configured:

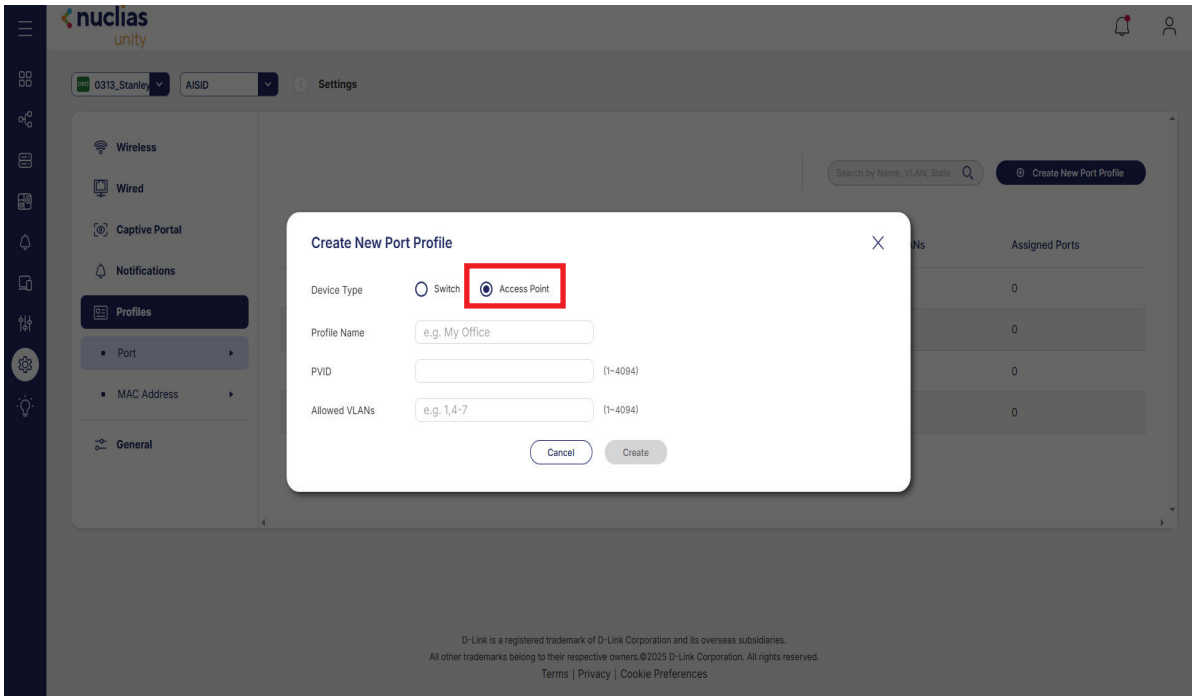
Device Type: Specifies whether the profile is intended for a Switch or Access Point, ensuring the appropriate settings are applied based on the device category.

Profile Name: Assigns a unique name to the port profile for easy identification and management across the network.

PVID: Sets the Port VLAN ID, which determines the VLAN assignment for untagged traffic received on the port, ensuring proper network segmentation.

Allowed VLANs: Defines the list of VLANs permitted on the port, allowing traffic from multiple specified VLANs to pass through while maintaining network isolation and security.

These parameters provide the foundational configuration for port profiles, enabling consistent and efficient deployment across switches and access points. Once these required fields are completed, click **Create** to save the Access Point port profile.



Nuclias Unity Dashboard Settings Profiles

In the Profile section under Settings, MAC Address Profile allows administrators to manage network access and policies based on device MAC addresses. MAC Address Profiles enable granular control over how specific devices connect to the network by defining rules for authentication, VLAN assignment, and access restrictions. These profiles are commonly used for:

MAC Group Name: Assigns a unique name to the MAC address group for easy identification and management across the network. This name helps organize multiple MAC address profiles and simplifies policy application.

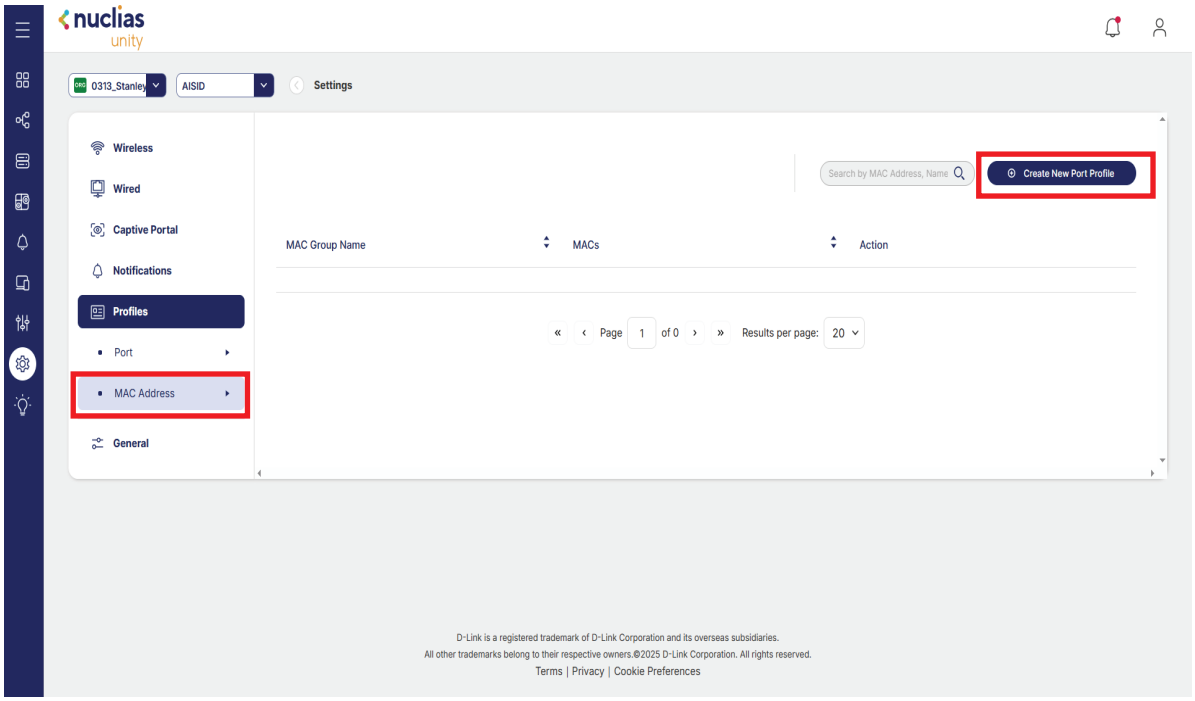
MACs: Specifies the list of MAC addresses to be included in the group. Each MAC address should be entered in the standard format (e.g., AA:BB:CC:DD:EE:FF) to ensure accurate identification of devices.

Action: Defines the policy applied to devices matching the MAC addresses in the group. Common actions include:

Allow: Grants network access to the specified devices.

Deny: Blocks network access for the specified devices.

These parameters enable network administrators to create granular access control policies, ensuring that only authorized devices gain network access and that devices are automatically placed in the appropriate network segments.



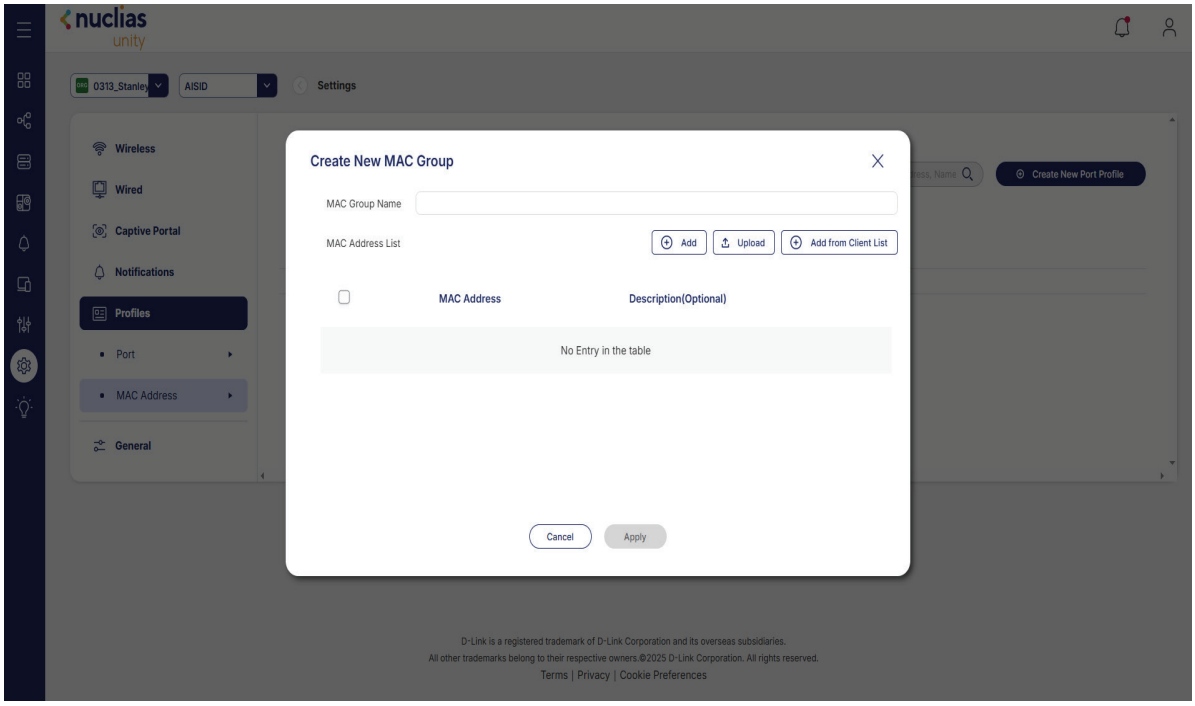
In the Create New MAC Group window, you can add MAC addresses to the group using multiple methods. First, specify a MAC Group Name to identify the group. Then, you can populate the MAC address list by selecting one of the following options:

Add: Manually enter individual MAC addresses one at a time.

Upload: Upload a file containing a list of MAC addresses for bulk import.

Add from Client List: Select MAC addresses directly from the existing client list, allowing you to quickly add devices that are already connected to the network.

Once the MAC addresses and group name are configured, click Save or Create to finalize the MAC group, which can then be applied to MAC Address Profiles for access control and policy enforcement across the network.



Nuclias Unity Dashboard Settings General

In **Settings**, select General to access the general configuration settings for the site. This section allows administrators to define essential site-level parameters. The following options are available:

Site Name: Assign a unique name to the site for identification and management across the Nuclias Unity platform.

Select Country: Choose the country where the site is located, which helps determine regional compliance settings and regulatory requirements.

Time Zone: Set the local time zone for the site to ensure accurate timestamps for logs, schedules, and notifications.

NTP Server: Configure the Network Time Protocol server address to synchronize the site's time with a reliable time source, ensuring consistent timekeeping across all devices.

Address: Enter the physical address of the site for location reference and documentation purposes.

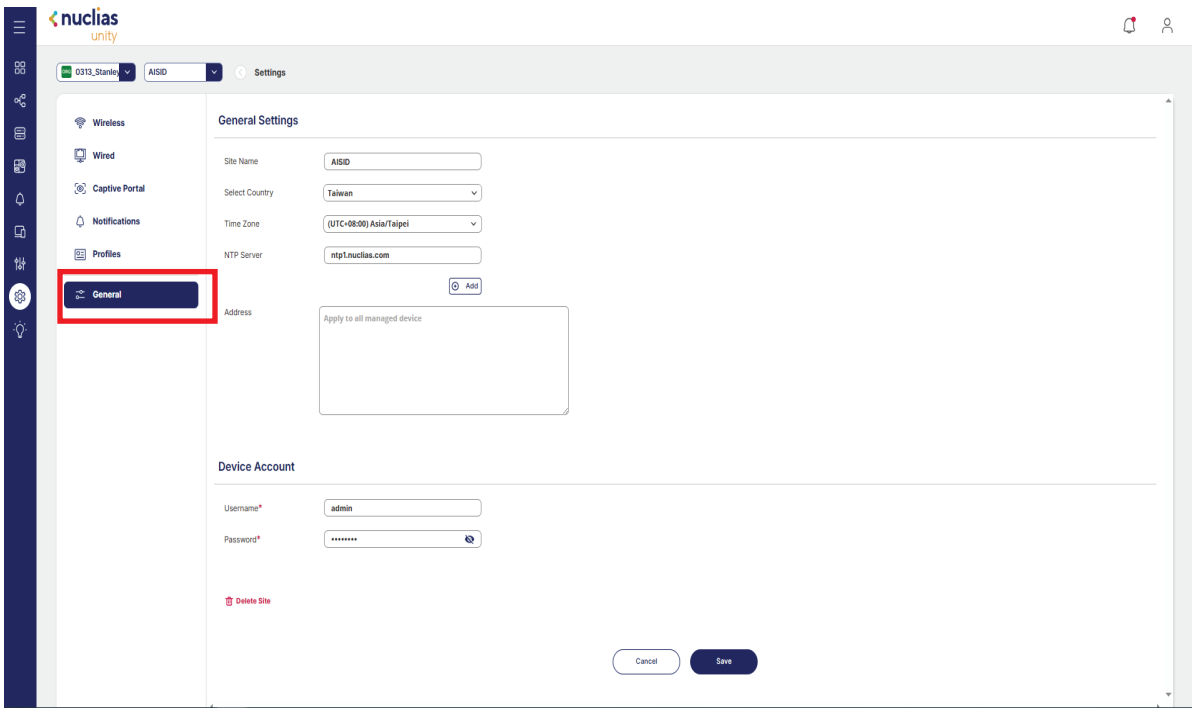
In the **Device Account** section, administrators can manage the credentials used for device communication:

Username: Specify the username for authenticating devices that connect to the Nuclias Unity platform.

Password: Set or update the password associated with the device account for secure device management.

Delete Site: Provides the option to permanently remove the current site from the Nuclias Unity platform. This action should be used with caution, as it will delete all associated site data and configurations.

These general settings ensure proper site identification, time synchronization, and secure device management within the Nuclias Unity cloud management platform.

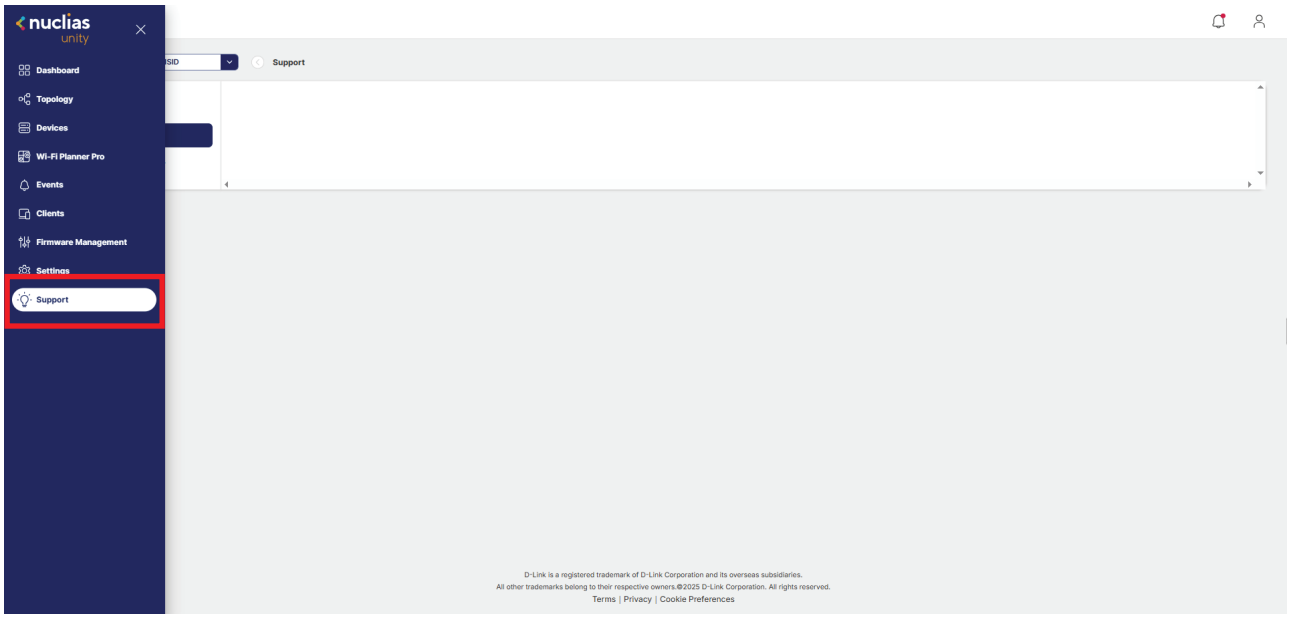


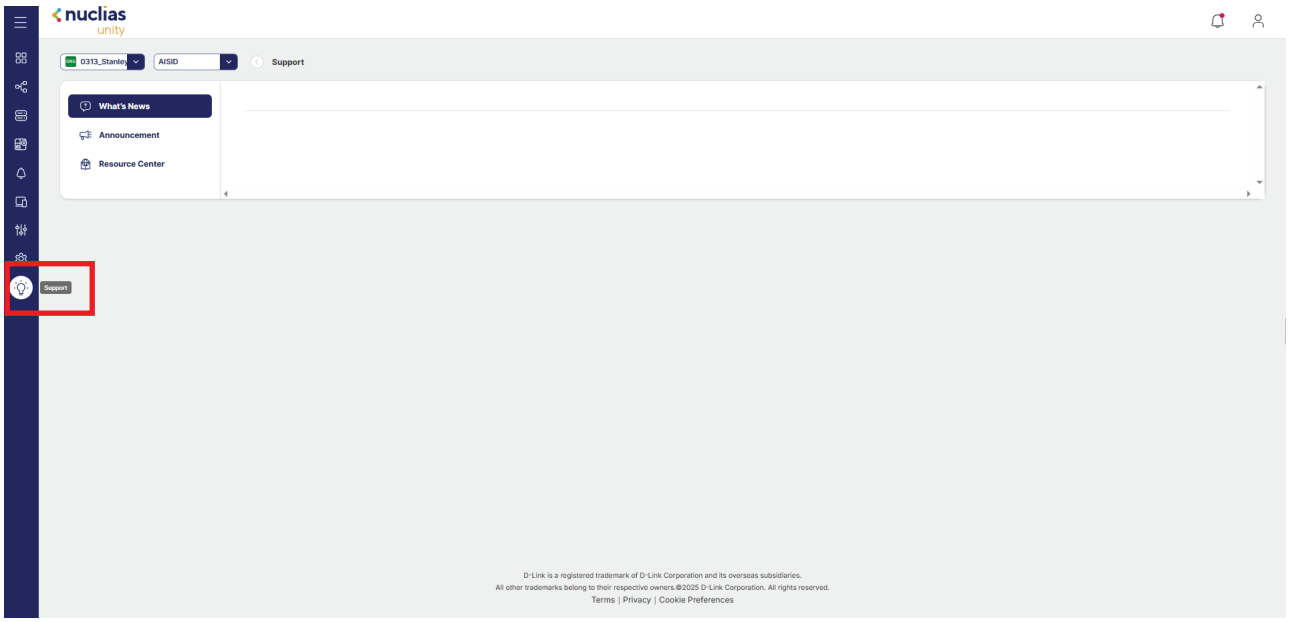
Nuclias Unity Dashboard Support

To access the Support section in Nuclias Unity, navigate from the Dashboard to Support on the left side menu bar. This section provides resources and tools to assist network administrators with technical support, troubleshooting, and platform information. Common features available in the Support section include:

- **What's New:** Stay updated on the latest features, enhancements, and bug fixes released for the Nuclias Unity platform.
- **Announcement:** View official notifications regarding system maintenance, scheduled downtime, critical updates, and important platform changes.
- **Resource Centers:** Access user manuals, configuration guides, video tutorials, technical notes, and FAQs for comprehensive platform support.

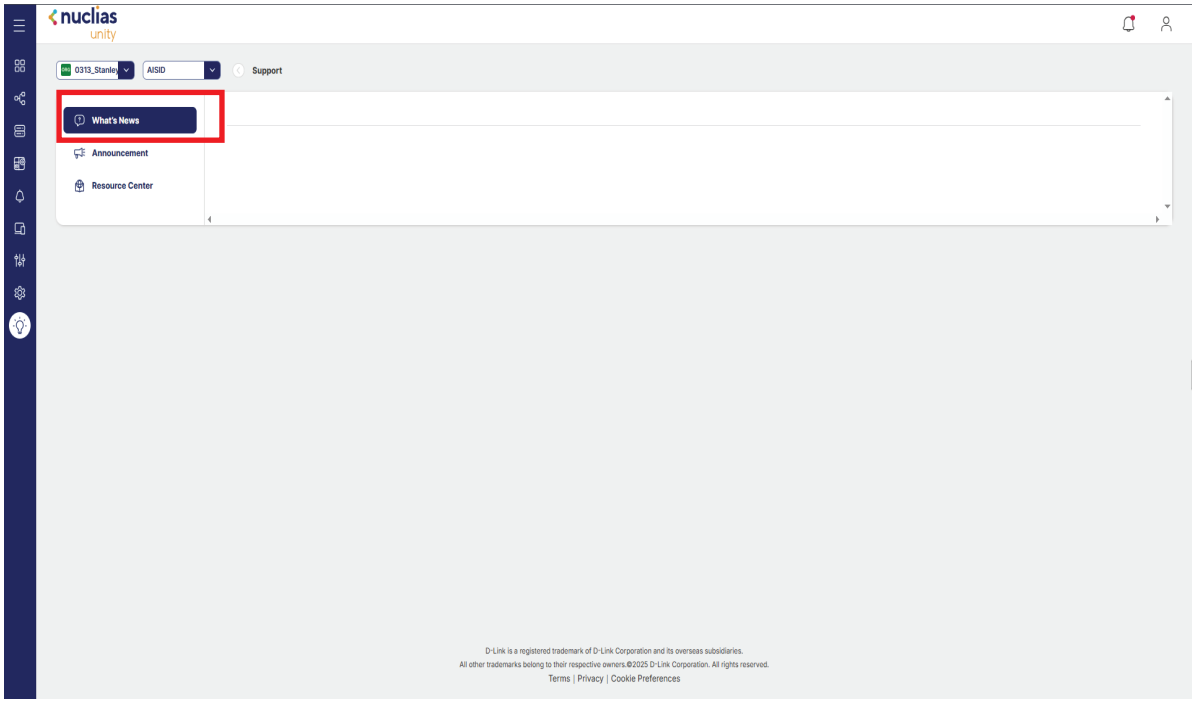
These resources help administrators stay informed and find the documentation needed to effectively manage their network infrastructure.





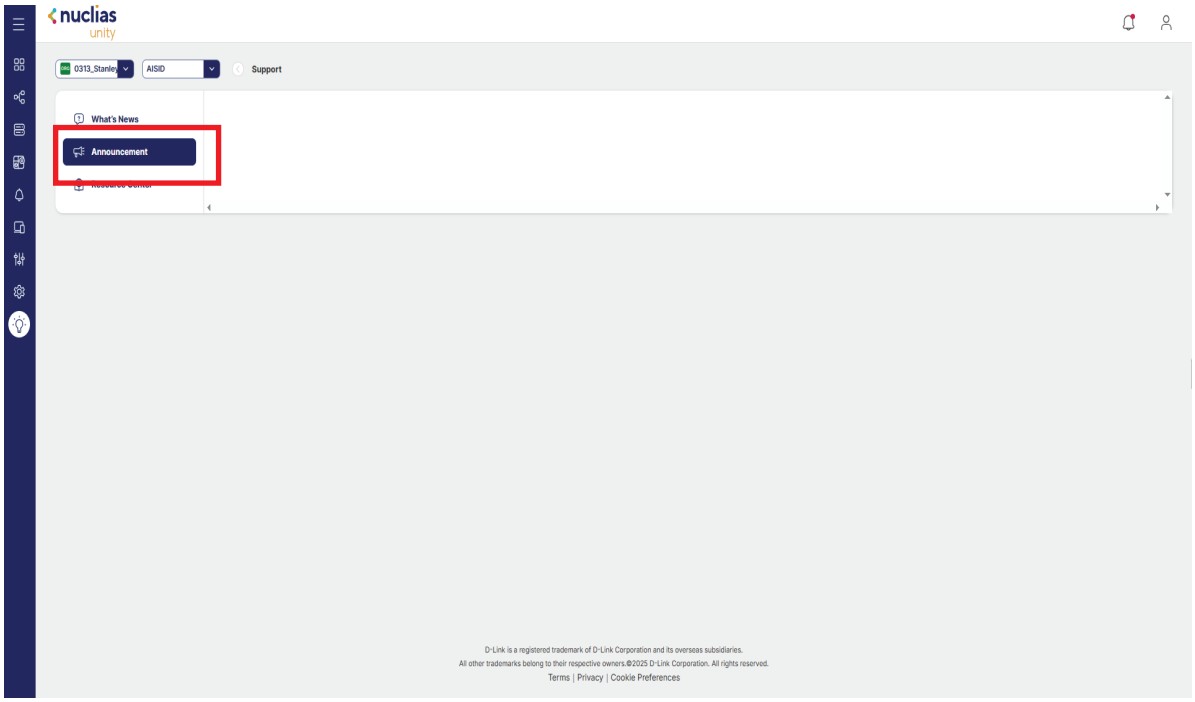
Nuclias Unity Dashboard Support **What's New**

In the Support section, click What's New to view the latest updates, features, and enhancements released for the Nuclias Unity platform. This section provides a summary of new functionality, improvements, and bug fixes introduced in recent updates. Administrators can use this information to stay informed about platform evolution, explore newly available tools, and understand how updates may impact network management practices. Regularly reviewing the What's New section helps ensure that administrators are leveraging the full capabilities of the Nuclias Unity cloud management platform.



Nuclias Unity Dashboard Support Announcement

In the Support section, click Announcement to view important notifications and updates from the Nuclias Unity platform team. This section displays official announcements regarding system maintenance, upcoming features, critical updates, and other platform-related information. Administrators can use this section to stay informed about scheduled downtime, new releases, and important changes that may affect network operations. Regularly checking the Announcement section ensures that administrators are aware of key platform events and can plan accordingly to maintain optimal network performance.



Nuclias Unity Dashboard Support Resource Center

To access the **Resource Center** in Nuclias Unity, navigate from the Dashboard to Support on the left side menu bar, then select **Resource Center**. This section provides a centralized repository of technical documentation and learning materials to assist network administrators in managing their network infrastructure.