



Nuclias Unity User Manual

Version 1.1.1

2026 | Cloud Network Management



Table of Contents

Introduction.....	3
Creating an Account.....	4
Device Configuration.....	10
Device Configuration.....	10
Software Installation.....	16
Zero Touch Provision.....	16
Nuclias Unity App.....	24
Nuclias Proxy.....	30
Device Setup.....	31
Proxy Installation.....	33
NCAP Installation.....	36
Launch Proxy.....	38
Add Device.....	40
Portal Overview.....	47
Interface Overview.....	47
Dashboard.....	49
Health AI Insight.....	54
Topology.....	64
Devices.....	69
Access points.....	73
Switches.....	81
Router (DBR-Series).....	87
Wi-Fi Planner Pro.....	88
Getting Started.....	90
Placement Settings.....	94
Heat Map.....	95
Report.....	96
Events.....	97
Clients.....	67
Wired.....	71
Wireless.....	75
Firmware Management.....	67
Settings.....	67
Wireless.....	71
SSID.....	71
Radio.....	71
Wired.....	143
Basic.....	143
Port Management.....	144
Config Provisioning.....	152
Captive Portal.....	163
Notifications.....	77
Profile.....	71
General.....	75
Support.....	122
What's News.....	77
Announcement.....	71
Resource Center.....	75

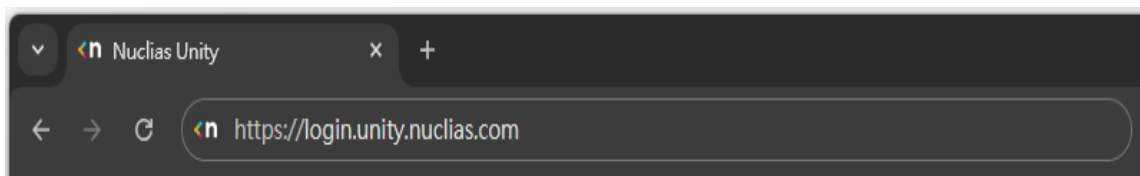
Introduction

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>

Getting Started with Nuclias Unity

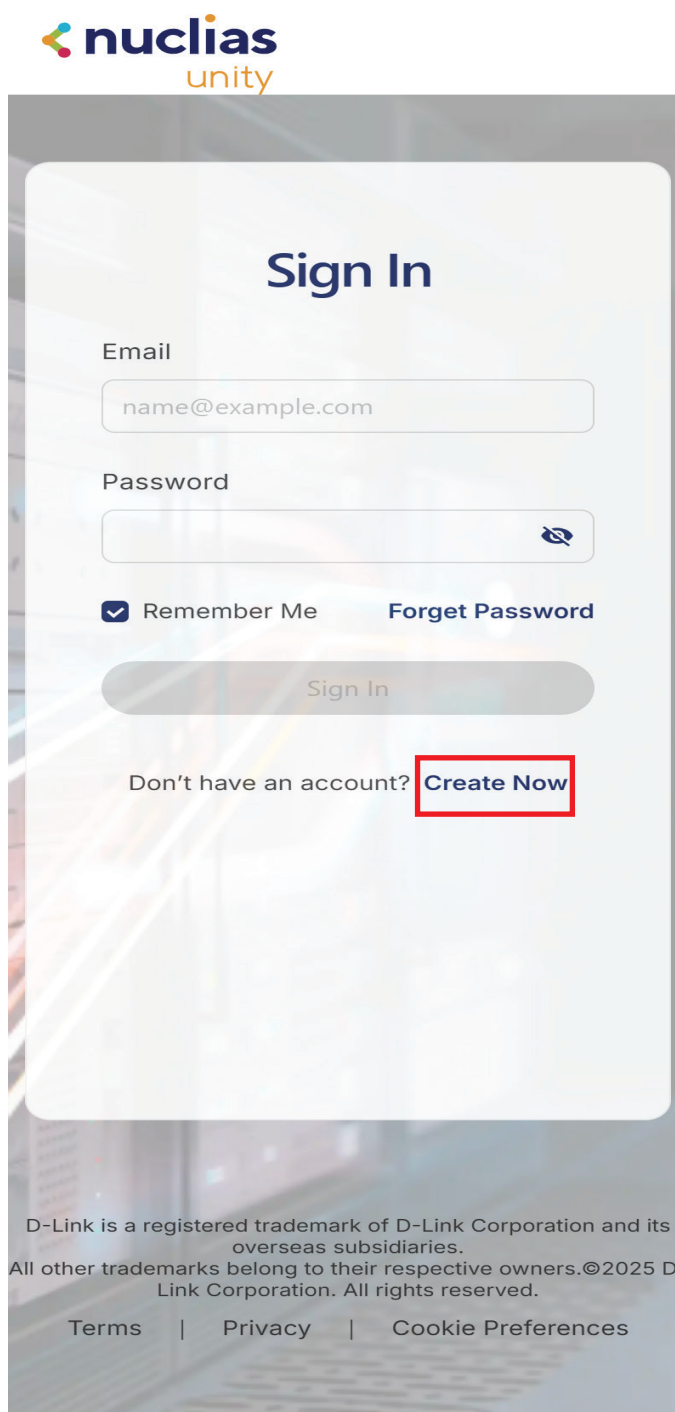
Create an Account

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.



The image shows a 'Sign In' form for Nuclias Unity. At the top is the Nuclias Unity logo. The form has a title 'Sign In'. Below it are two input fields: 'Email' with the placeholder 'name@example.com' and 'Password' with a toggle icon. There are two checkboxes: 'Remember Me' (checked) and 'Forget Password'. A 'Sign In' button is below these. At the bottom, it says 'Don't have an account?' followed by a 'Create Now' button, which is highlighted with a red rectangle. At the very bottom, there is a footer with legal text and links for 'Terms', 'Privacy', and 'Cookie Preferences'.

nuclias
unity

Sign In

Email
name@example.com

Password

☒ Remember Me [Forget Password](#)

[Sign In](#)

Don't have an account? [Create Now](#)

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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:

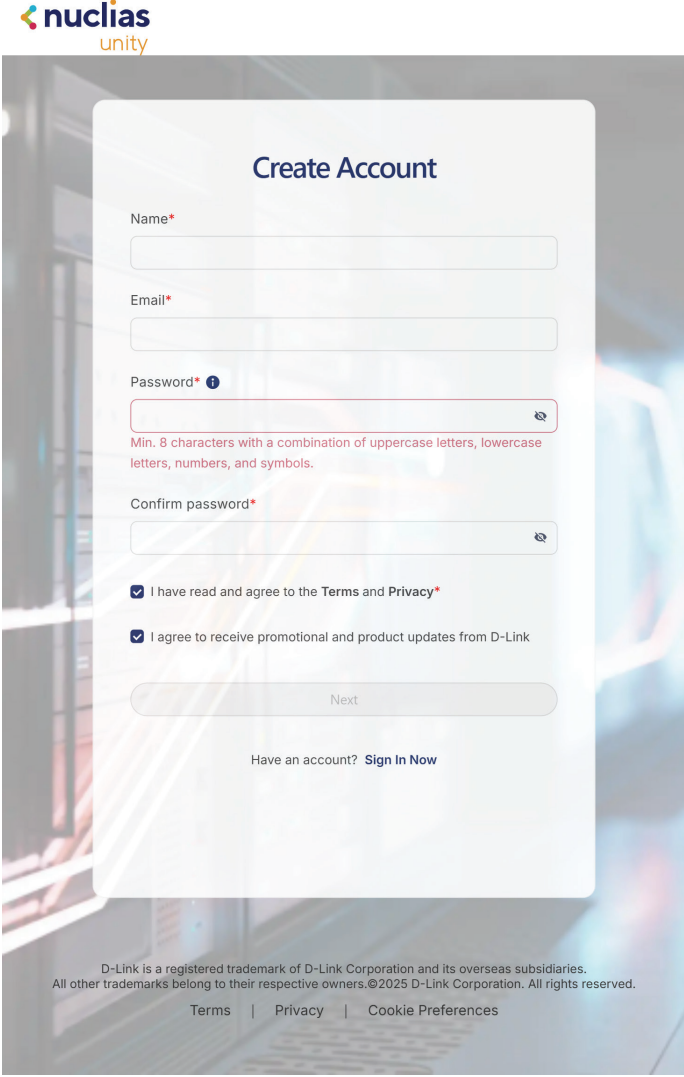
- Must include at least one uppercase letter (A–Z), one lowercase letter (a–z), and one number (0–9).
- Allowed at least one Special Characters: ~ ! @ # \$ % ^ & * { } [] () _ - + = . | : ; ' " < , > / \

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.



The image shows a screenshot of the 'Create Account' form for Nuclias Unity. The form is white with a blue header and a blue footer. It contains fields for Name, Email, Password, and Confirm password. There are checkboxes for agreeing to terms and privacy, and a checkbox for receiving promotional updates. A 'Next' button is at the bottom of the form. The background is a blurred image of a person using a laptop.

nuclias
unity

Create Account

Name*

Email*

Password* ⓘ
Min. 8 characters with a combination of uppercase letters, lowercase letters, numbers, and symbols.

Confirm password*

☒ I have read and agree to the [Terms](#) and [Privacy](#)*

☒ I agree to receive promotional and product updates from D-Link

Next

Have an account? [Sign In Now](#)

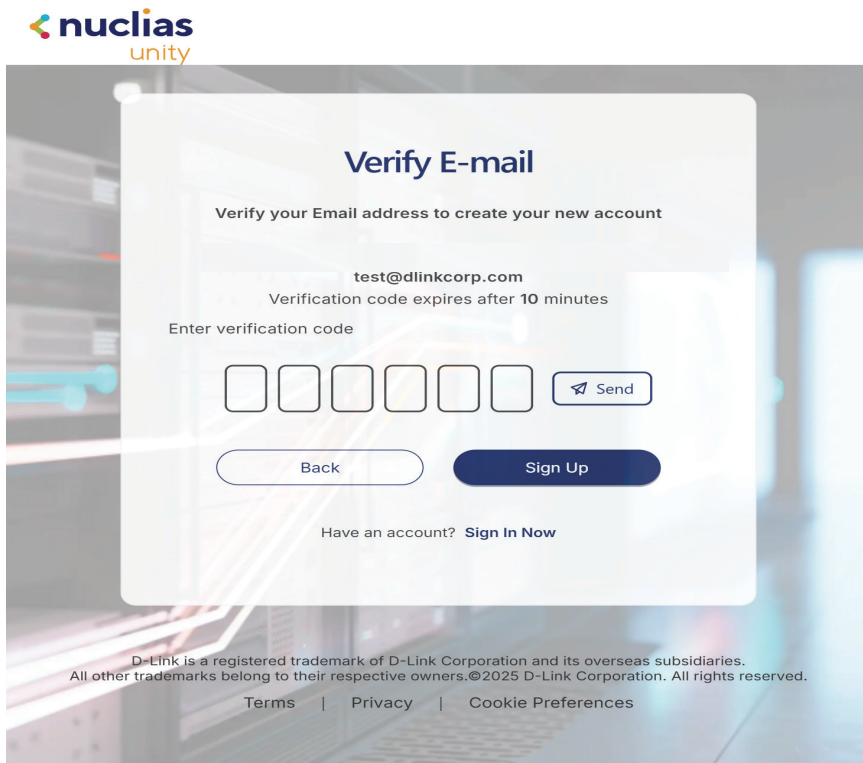
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.



The image shows a mobile application screen for verifying an email address. At the top left is the Nuclias Unity logo. The main heading is "Verify E-mail". Below it, a sub-heading says "Verify your Email address to create your new account". The email address "test@dlinkcorp.com" is displayed, followed by a note "Verification code expires after 10 minutes". Below this is a prompt "Enter verification code" and a row of six empty square boxes for input. To the right of these boxes is a "Send" button with an arrow icon. Below the input boxes are two buttons: "Back" and "Sign Up". At the bottom, there is a link "Have an account? Sign In Now". The footer contains a legal disclaimer: "D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries. All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved." and three links: "Terms", "Privacy", and "Cookie Preferences".

Verify E-mail

Verify your Email address to create your new account

test@dlinkcorp.com

Verification code expires after 10 minutes

Enter verification code

[Send](#)

[Back](#) [Sign Up](#)

Have an account? [Sign In Now](#)

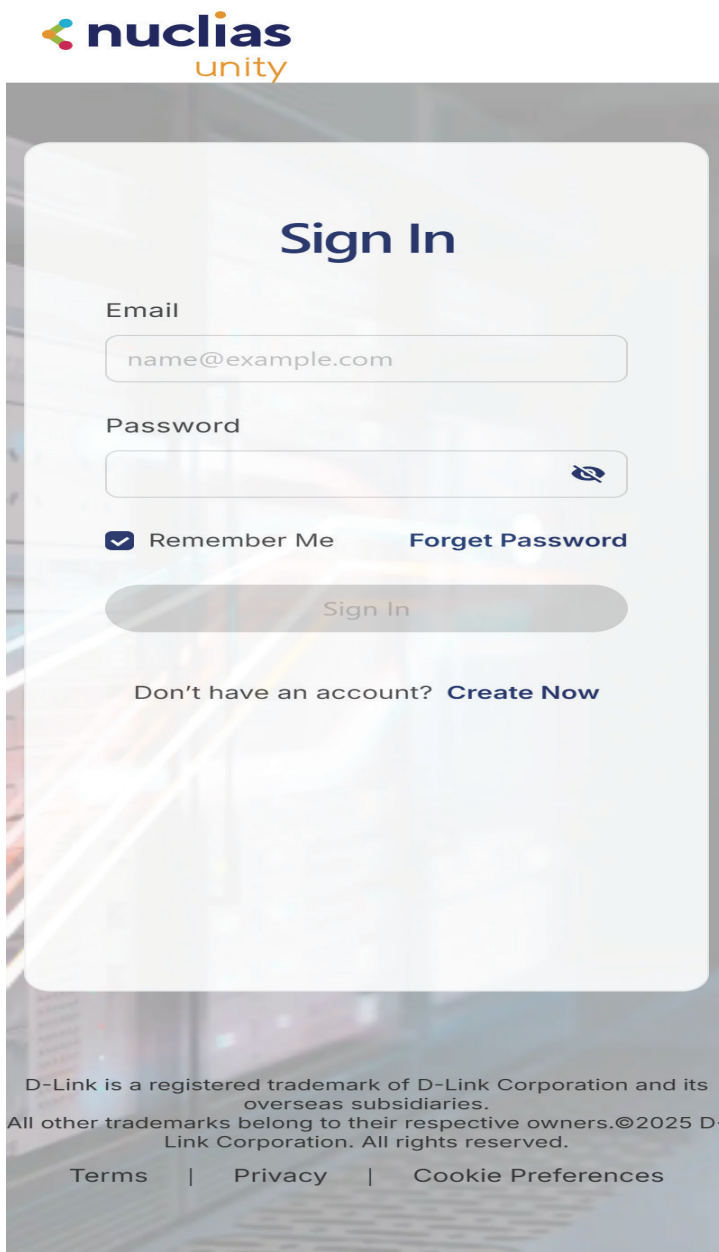
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.

The image shows the Nuclias Unity login interface. At the top left is the Nuclias Unity logo, with 'nuclias' in blue and 'unity' in orange. The main heading is 'Sign In' in a large, bold, dark blue font. Below this are two input fields: 'Email' with the placeholder 'name@example.com' and 'Password' with a toggle icon on the right. There are two checkboxes: 'Remember Me' (checked) and 'Forgot Password'. A large, rounded 'Sign In' button is centered below these. At the bottom of the form area, it says 'Don't have an account? [Create Now](#)'. The footer contains a copyright notice: 'D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries. All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.' and three links: 'Terms | Privacy | Cookie Preferences'.

nuclias
unity

Sign In

Email

name@example.com

Password

☒ Remember Me [Forgot Password](#)

[Sign In](#)

Don't have an account? [Create Now](#)

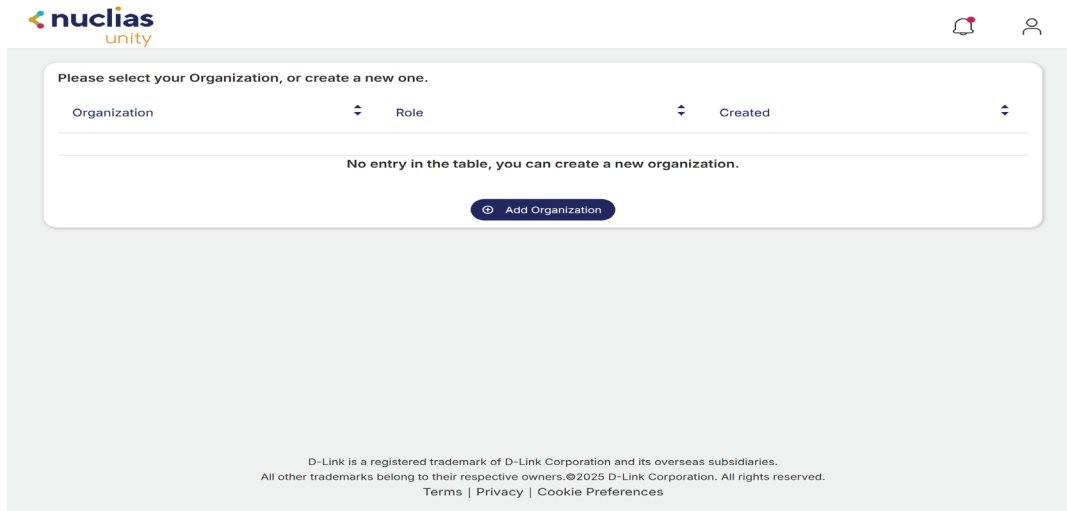
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.

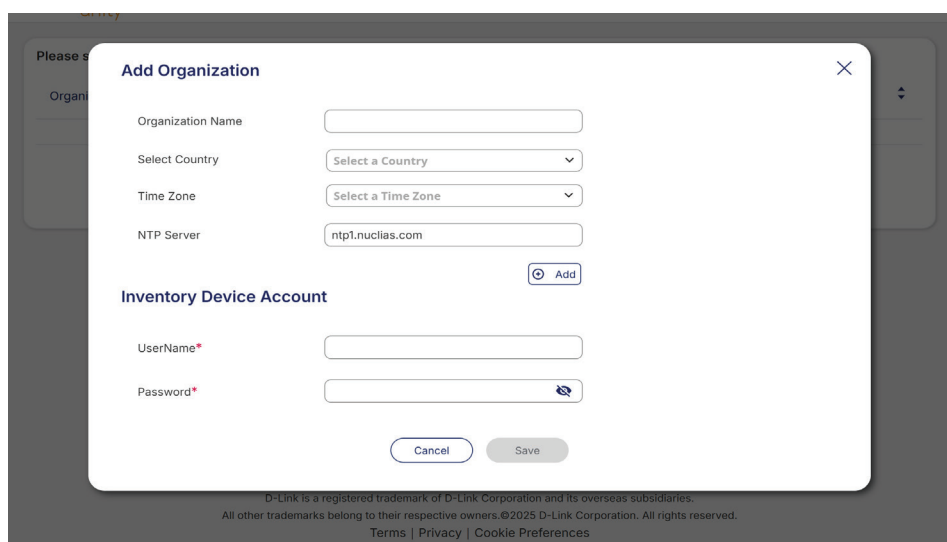


Enter the required organization details in the configuration page:

- **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.



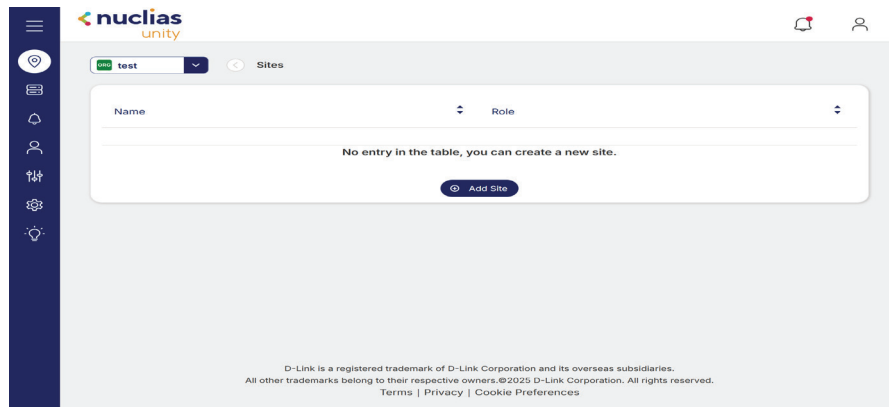
An Inventory Device Account is maintained at the organizational level to manage devices before they are deployed to specific sites. It provides centralized control over procurement, staging, and distribution, ensuring consistent oversight at the management level.

Getting 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

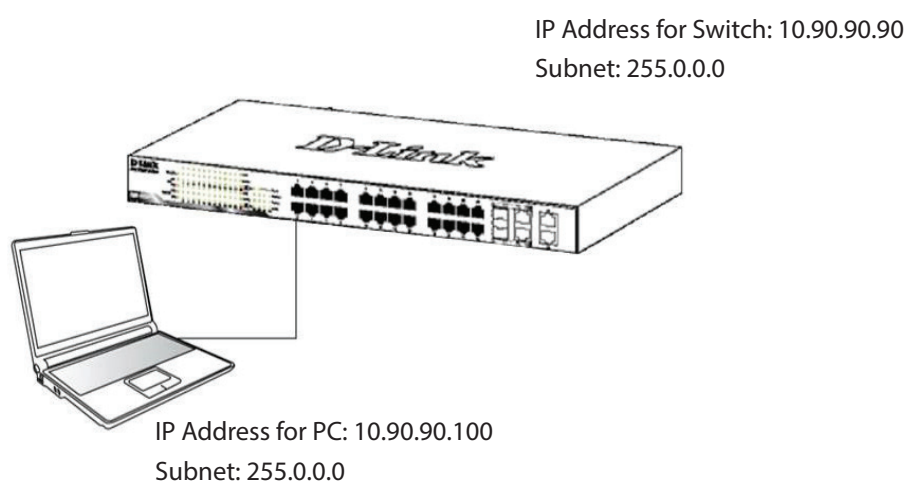
Ensure your PC is connected to the switch using an Ethernet cable. Before accessing the switch's web-based interface, you must configure your PC with an IP address and subnet mask that are compatible with the switch's default IP settings.

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

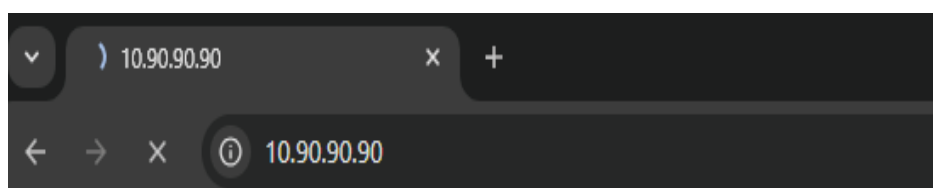
- IP Address: 10.90.90.X (where X is 1–89 or 91–254, for example, 10.90.90.100)
- Subnet Mask: 255.0.0.0

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.



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

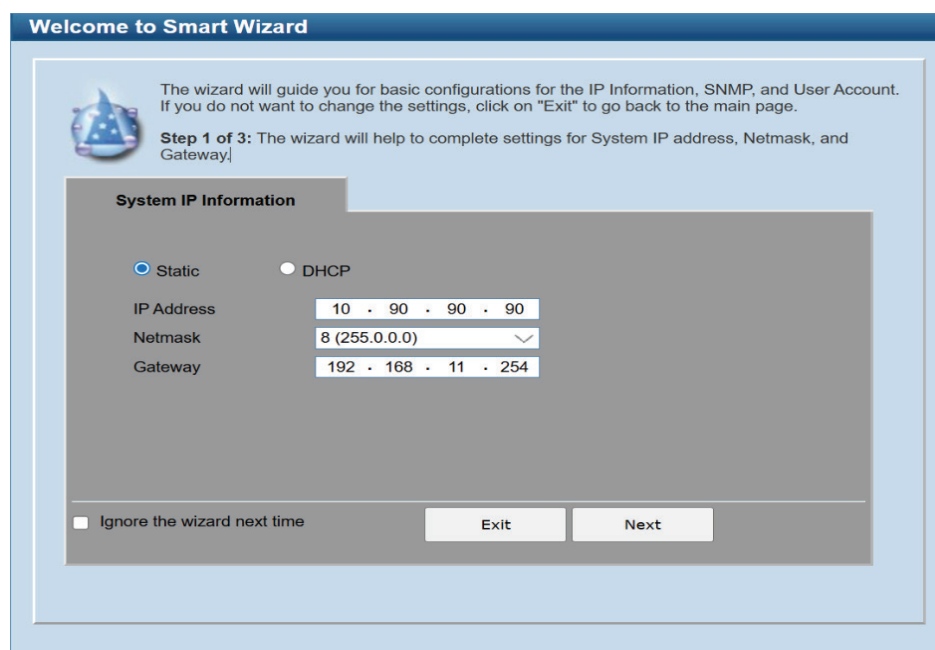
Before proceeding, you may also select your preferred language from the available options to navigate the interface more comfortably.

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



The login dialog box is titled "Connect to 10.90.90.90" and features a key icon. It prompts the user to "Enter your username and password". The form includes three input fields: "User Name" with the value "admin", "Password" with masked characters "*****", and "Language" with a dropdown menu set to "English". At the bottom right, there are two buttons: "Login" and "Reset".

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.

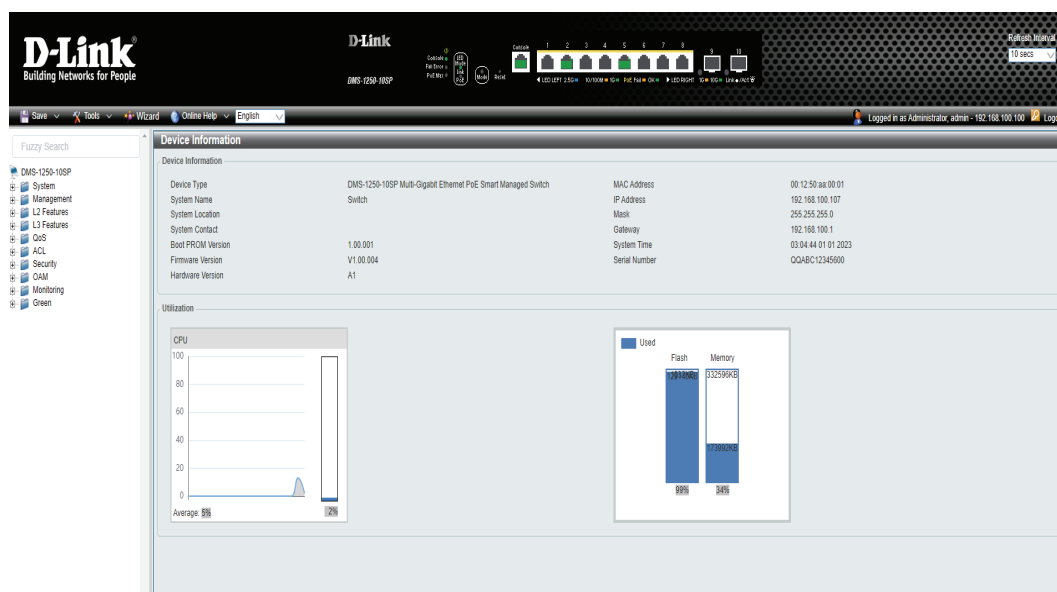


The "Welcome to Smart Wizard" page provides instructions for basic configurations. It indicates "Step 1 of 3: The wizard will help to complete settings for System IP address, Netmask, and Gateway." The "System IP Information" section shows two radio buttons: "Static" (selected) and "DHCP". Below these are input fields for "IP Address" (10 . 90 . 90 . 90), "Netmask" (8 (255.0.0.0) with a dropdown arrow), and "Gateway" (192 . 168 . 11 . 254). At the bottom, there is a checkbox for "Ignore the wizard next time" and two buttons: "Exit" and "Next".

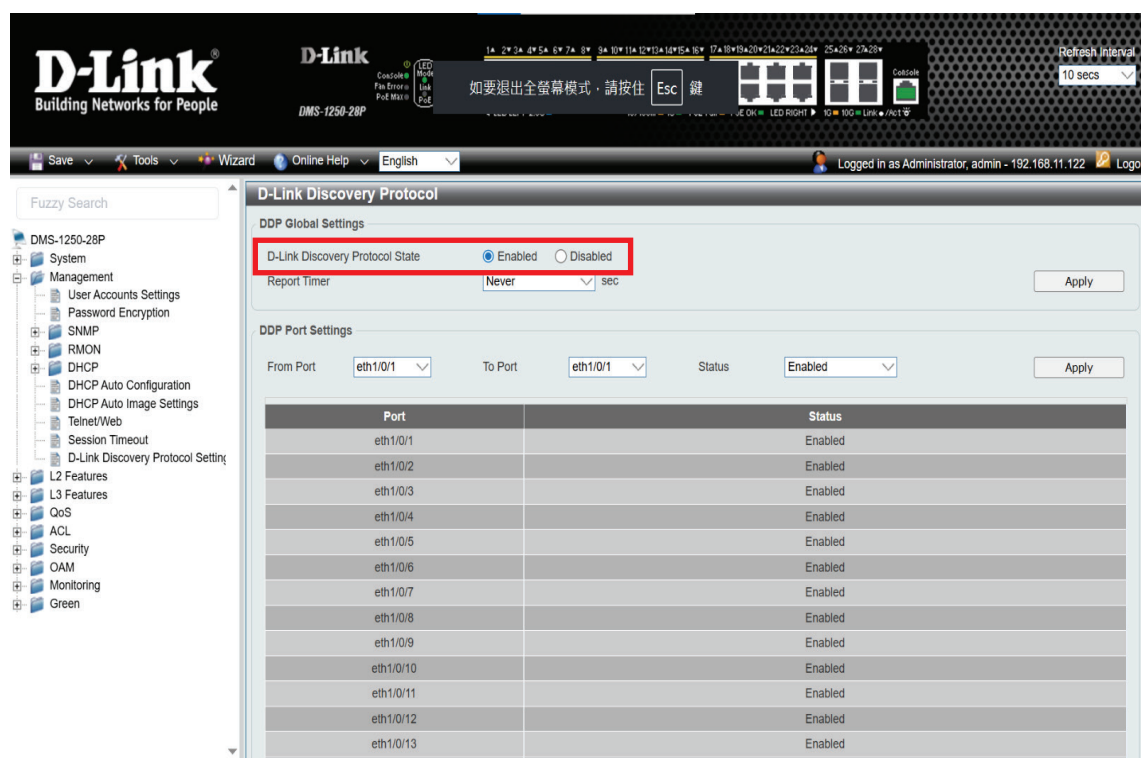
Device Configuration

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.

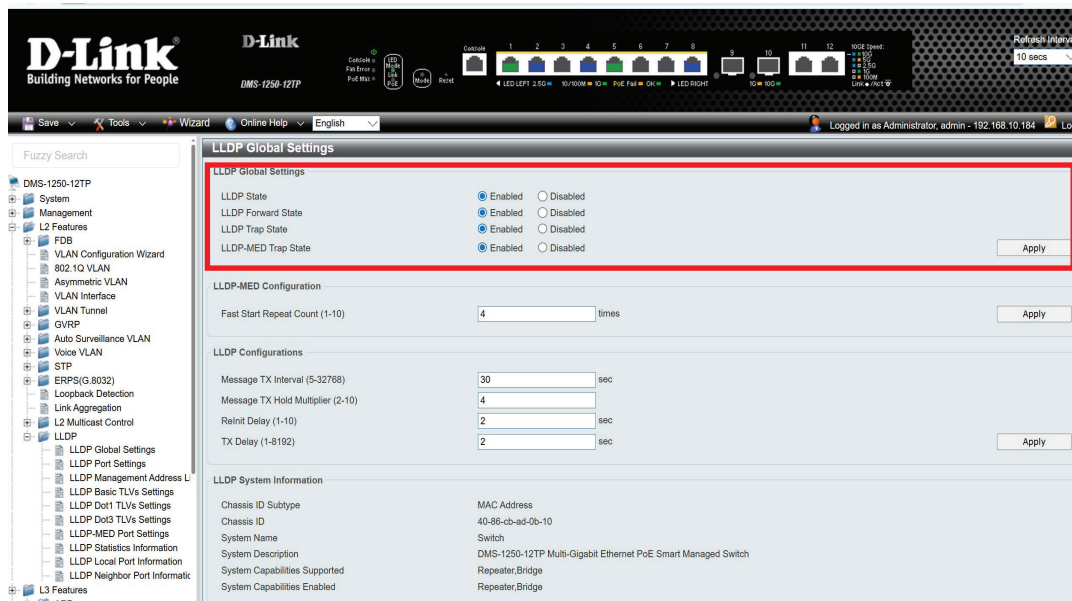


Device Configuration

DHCP Enable

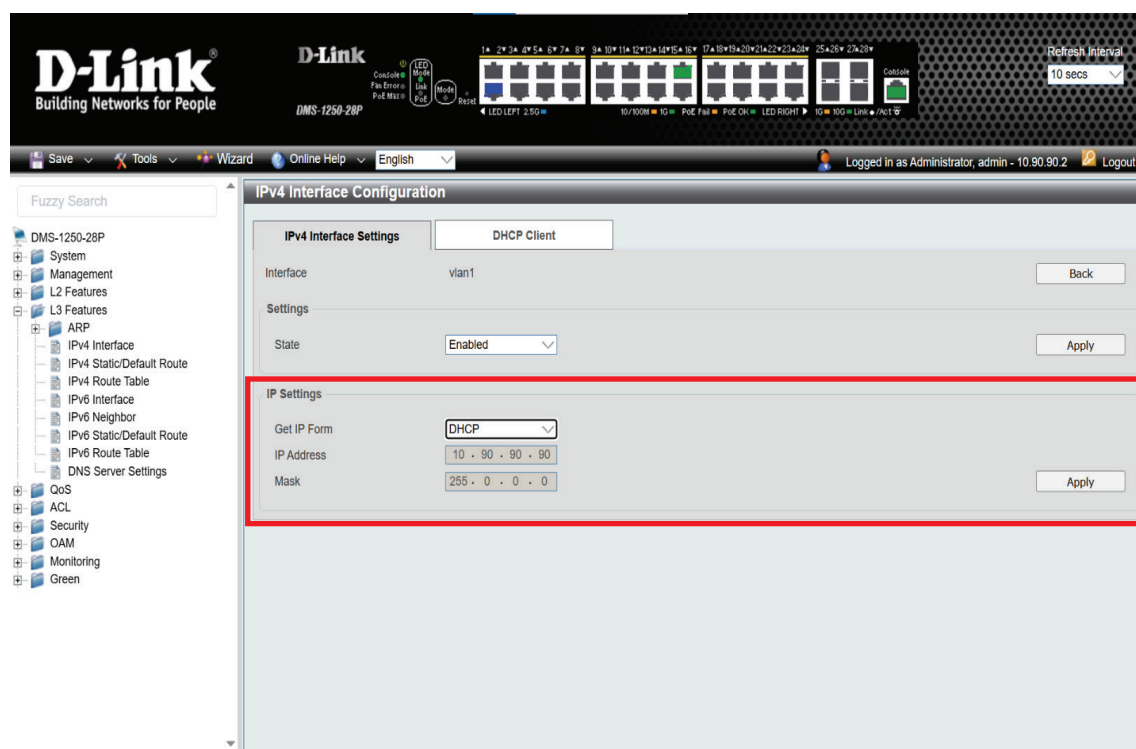
After enabling DDP, you also need to enable LLDP to ensure proper device discovery and communication.

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.

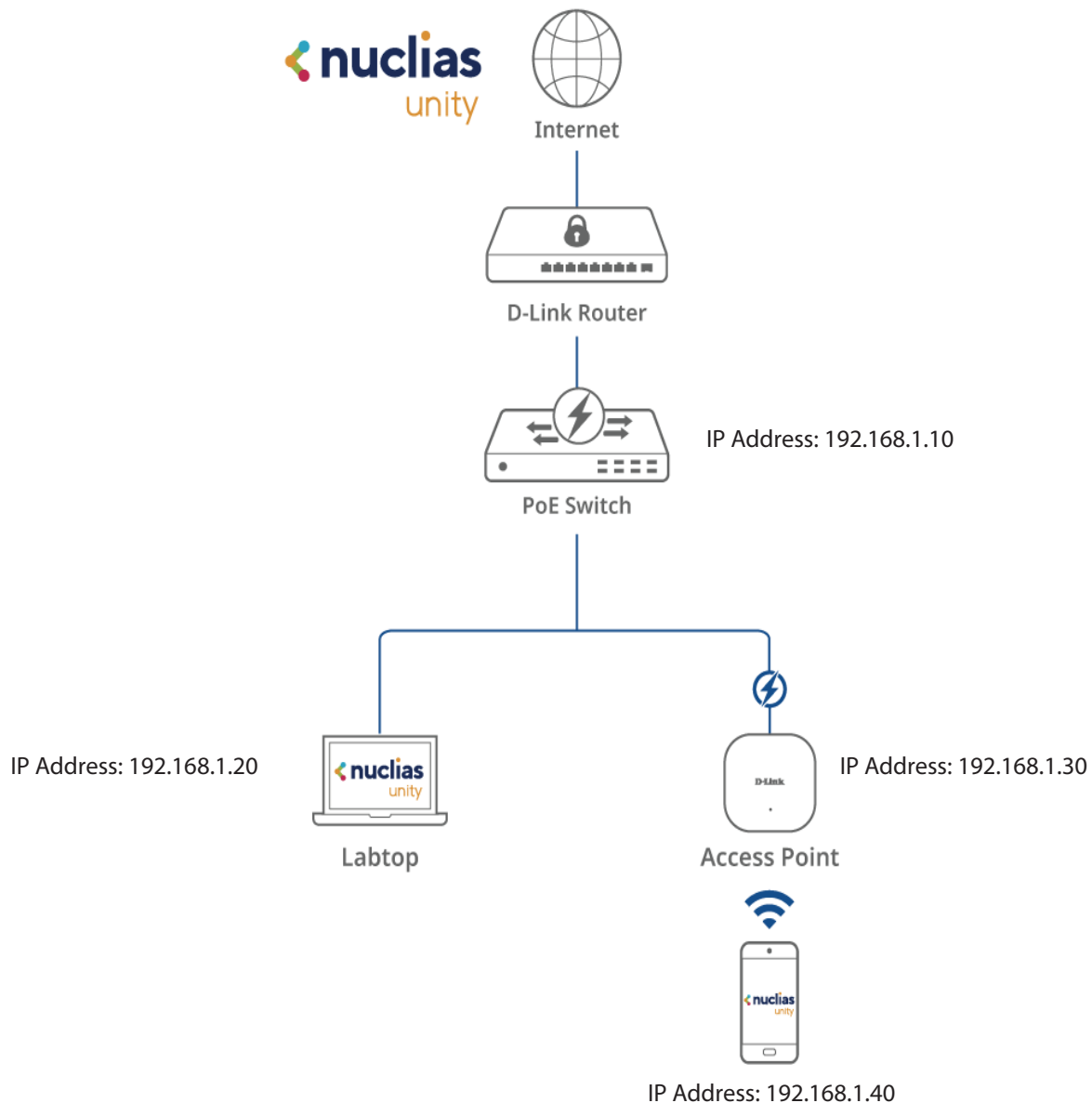
Note: By default, DHCP should be enabled on the access point. If it is not enabled, please log in to your access point and enable DHCP.

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

Zero Touch Provision

Zero Touch Provisioning allows switches and access points to be deployed quickly and easily without requiring manual device configuration on-site.

To begin deployment, connect the switches and access points to the network and power them on. Once the devices establish an Internet connection, they automatically connect to Nuclias Unity and retrieve the administrator-assigned preconfigured settings.

The downloaded configuration may include wireless settings, VLAN configurations, SSIDs, security policies, device profiles, and other network parameters. After the configuration is applied, the devices become operational automatically without additional setup steps.

This automated provisioning process reduces deployment time, minimizes configuration errors, and simplifies large-scale installations. It also enables non-technical staff to install and replace devices easily, making it ideal for branch offices, schools, hotels, retail stores, and other distributed network environments.

For non-technical users, Zero Touch Provisioning eliminates the need for complex setup procedures, commandline configuration, or advanced networking knowledge. Staff only need to connect the device to power and the network, while all required settings are applied automatically from NucliasUnity. This reduces the need for on-site IT support, simplifies device replacement, and helps organizations deploy networks consistently across multiple locations with minimal training.

Nuclias Unity Zero Touch Provisioning simplifies device deployment, making the setup process fast and hassle-free for both technical and non-technical users. With this feature, devices can automatically receive their assigned configuration settings without requiring manual setup or advanced networking knowledge.

Software Installation

Zero Touch Provisioning

Before starting, ensure that the organization and site have already been created in Nuclias Unity.

Step 1: Unpack and Power On the Device

Carefully unpack the switch or access point from its package and verify that all required accessories are included.

Connect the device to:

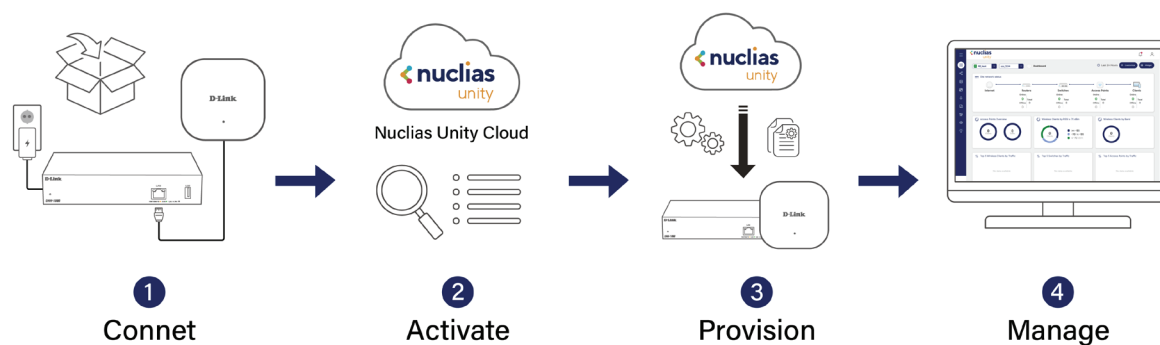
- A power source
- Network using DHCP for Internet access

Step 2: Log in to Nuclias Unity

Open a web browser and log in to the Nuclias Unity management platform using your administrator account credentials.

After logging in:

- Select the pre-created Organization.
- Select the appropriate Site for the device's deployment.



Software Installation

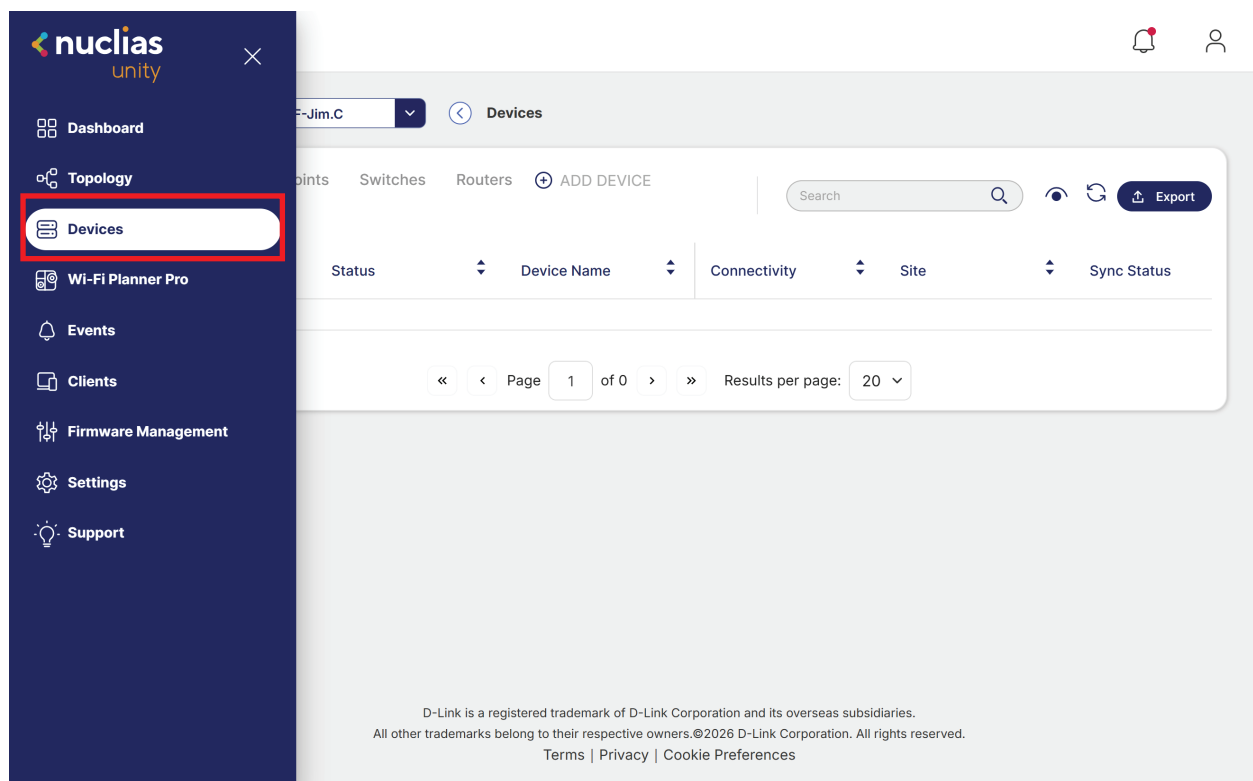
Zero Touch Provisioning

Step 3: Navigate to the Device Menu

From the left-side navigation menu, click Device to open the device management page.

This page allows administrators to:

- View connected devices
- Monitor device status
- Manage configurations and deployment settings

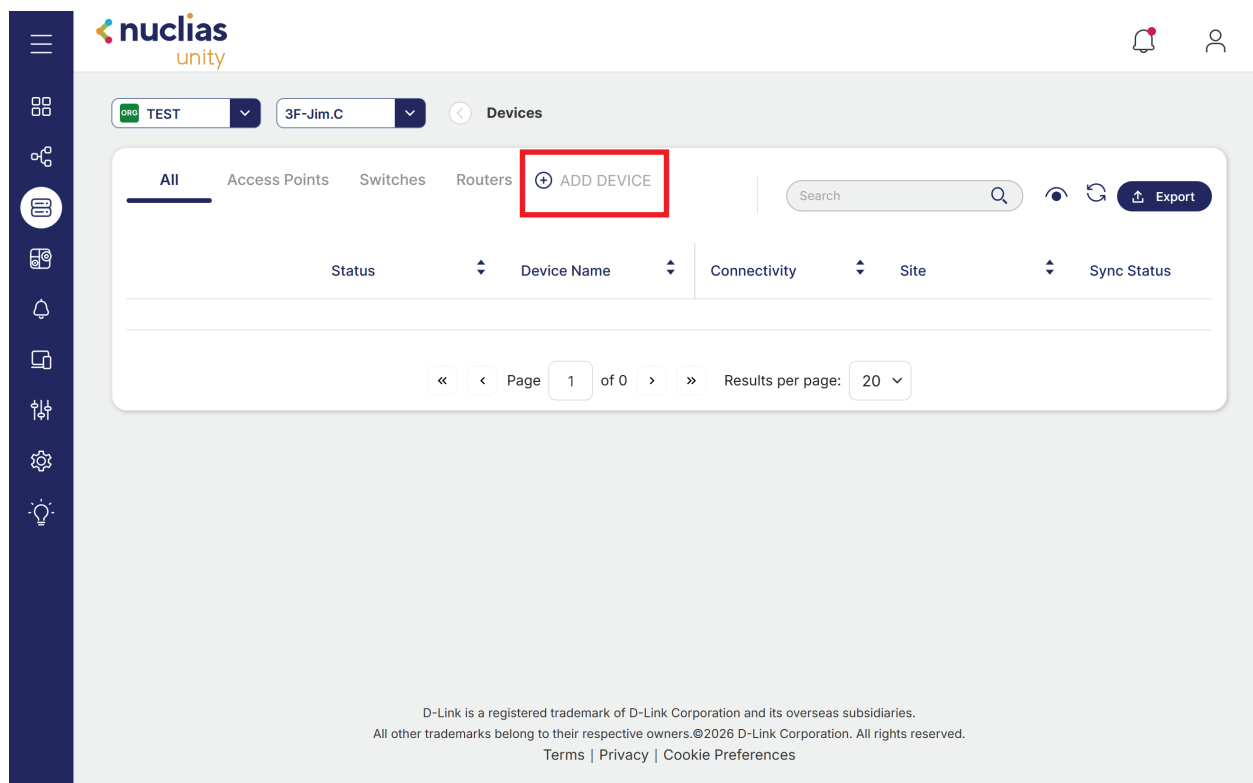


Software Installation

Zero Touch Provisioning

Step 4: Add a Device

On the Device page, click **Add Device** to begin the device onboarding process. Nuclias Unity will display the available methods for adding and provisioning devices to the selected site.

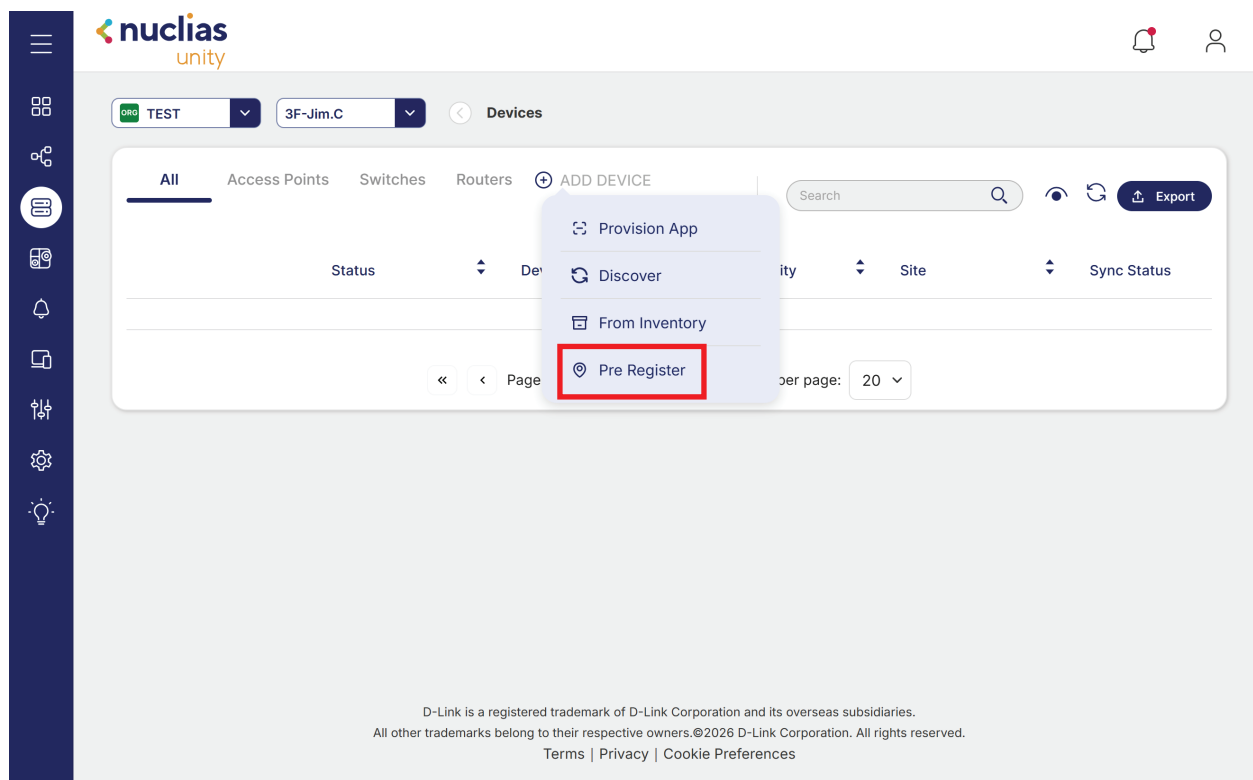


Software Installation

Zero Touch Provisioning

Step 5: Select Pre-Register

In the Add Device window, select **Pre-Register**. This option allows you to register devices in Nuclias Unity before they are deployed, ensuring they automatically receive the assigned configuration when they connect to the Internet.



Software Installation

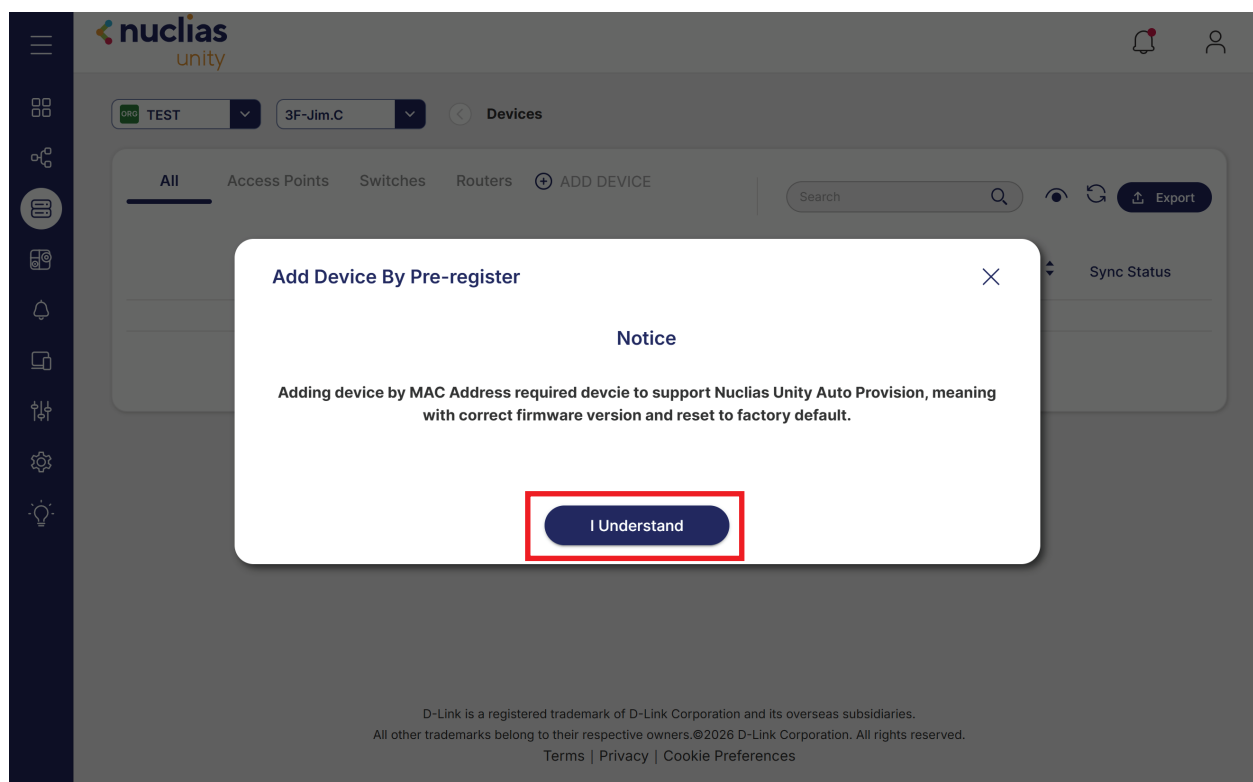
Zero Touch Provisioning

Step 6: Add Device by Pre-Register

When Pre-Register is selected, a notice is displayed informing the user that adding a device requires its **MAC Address** and that the device must support Nuclias Unity **Auto Provisioning**.

The device should also be running the correct firmware version and be reset to factory default settings before it can be successfully onboarded.

The user then clicks **I Understand** to acknowledge the notice and proceed with the device registration process.



Software Installation

Zero Touch Provisioning

Step 7: Add the MAC Address and Select the Site Name

Enter the correct **MAC Address** in the MAC Address field, then select the **Site Name** where the device will be added. This ensures the device is assigned to the correct location for provisioning and management in Nuclias Unity.

The screenshot shows the 'Device Adoption' modal form in the Nuclias Unity interface. The form is titled 'Device Adoption' and has a close button (X) in the top right corner. It contains the following fields and controls:

- Add MAC Address**: A button with an upload icon and the text 'Upload'.
- MAC Address**: A text input field containing the value '28 - 38 - 82 - 00 - 22 - 02'. This field is highlighted with a red rectangle.
- SN Information(Optional)**: A text input field.
- Add to Site**: A dropdown menu with the selected value 'TW_E9560'. This dropdown is highlighted with a red rectangle.
- Add**: A button with a plus icon and the text 'Add'.
- Next**: A blue button with the text 'Next'.

The background of the screenshot shows the Nuclias Unity dashboard with a sidebar on the left and a top navigation bar. The dashboard includes tabs for 'All', 'Access Points', 'Switches', 'Routers', 'Inventory', 'Unity Proxy', and 'ADD DEVICE'. The 'Switches' tab is currently selected.

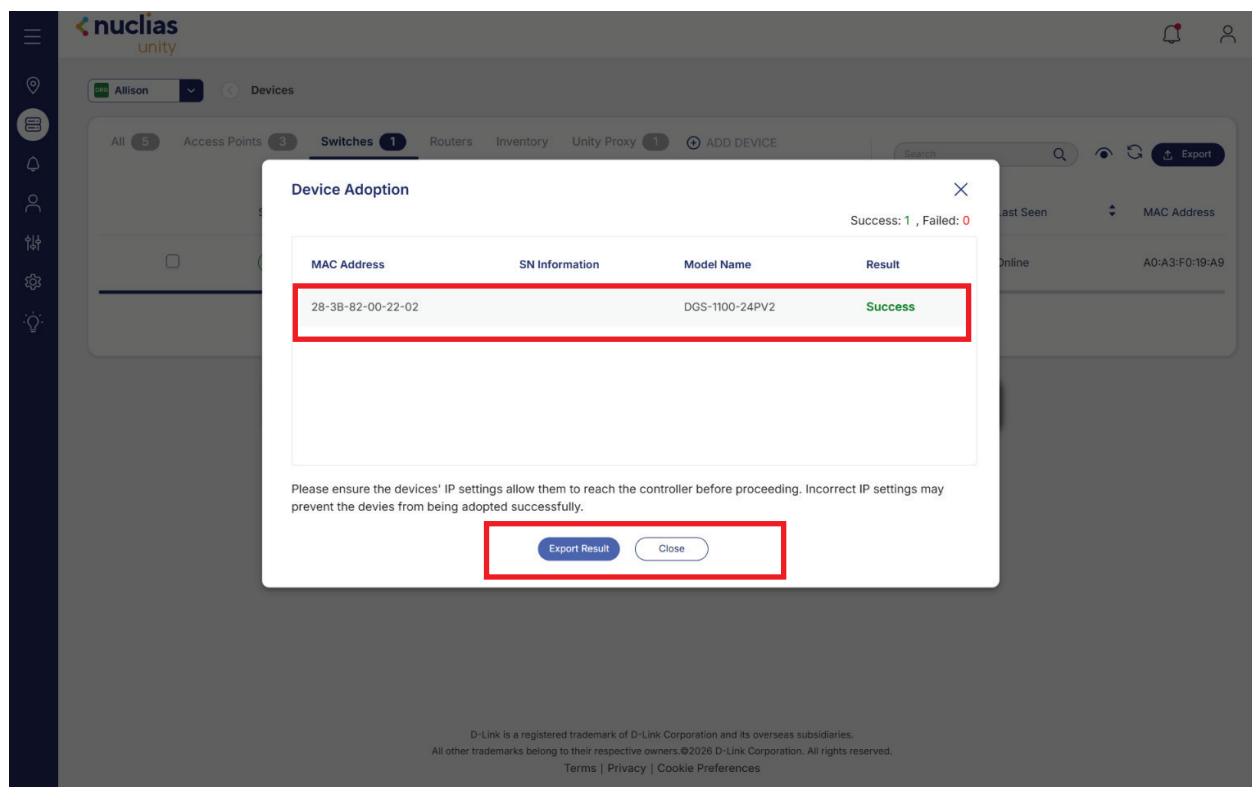
D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2026 D-Link Corporation. All rights reserved.
Terms | Privacy | Cookie Preferences

Software Installation

Zero Touch Provisioning

Step 8: Device Adaption

Once the device is added successfully, a **Success** message is displayed. The added device will also appear in the device list, along with its model information, confirming that it has been successfully registered in Nuclias Unity.



Software Installation

Zero Touch Provisioning

Router

Signing into Nuclias Unity

Using Nuclias Unity, administrators can centrally configure and monitor the DBR Router through an intuitive management interface. The platform enables you to manage router settings, monitor network status, view connected devices, and perform essential network configuration and maintenance tasks.

After creating and activating your Nuclias Unity account, you can sign in to the Nuclias Unity portal.

1. Open a web browser on your computer.
2. Enter the following URL in the address bar:
3. <https://login.unity.nuclias.com>
4. The Nuclias Unity sign-in page will appear.
5. Enter your registered Email address.
6. Enter your Password.
7. Select Remember Me if you want the browser to remember your login information.
8. Click Sign In to access the Nuclias Unity portal.
9. After signing in successfully, you will be directed to the Nuclias Unity portal dashboard.

Note: If you forget your password, click Forget Password on the sign-in page and follow the on-screen instructions to reset your password.



Sign In

Email

Password

☒ Remember Me

[Forget Password](#)

Sign In

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

Software Installation

Router

Device Configuration

Network Connection

Your Internet Service Provider (ISP) determines the required WAN connection type for the DBR router. Please contact your ISP or refer to the connection details they have provided. For this guide, the following connection types will be used as an example.

Primary WAN (WAN1): Dynamic IP (DHCP)

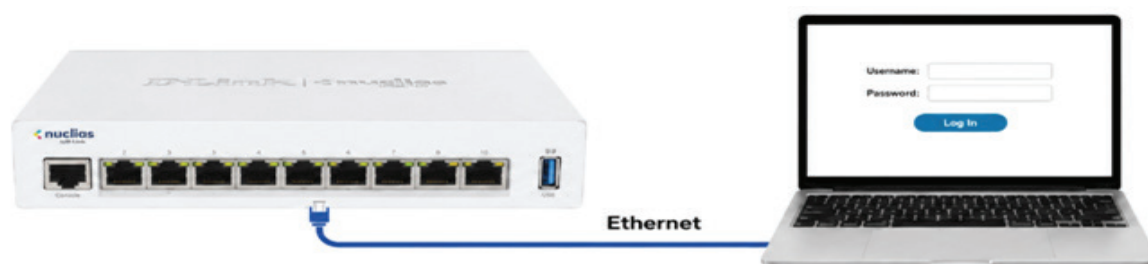
Accessing the DBR Router Web Interface

Step 1: Open your web browser and enter <https://192.168.10.1> (Default IP address).

Step 2: Log in to the DBR Router Web UI for the first time to change the default credentials:

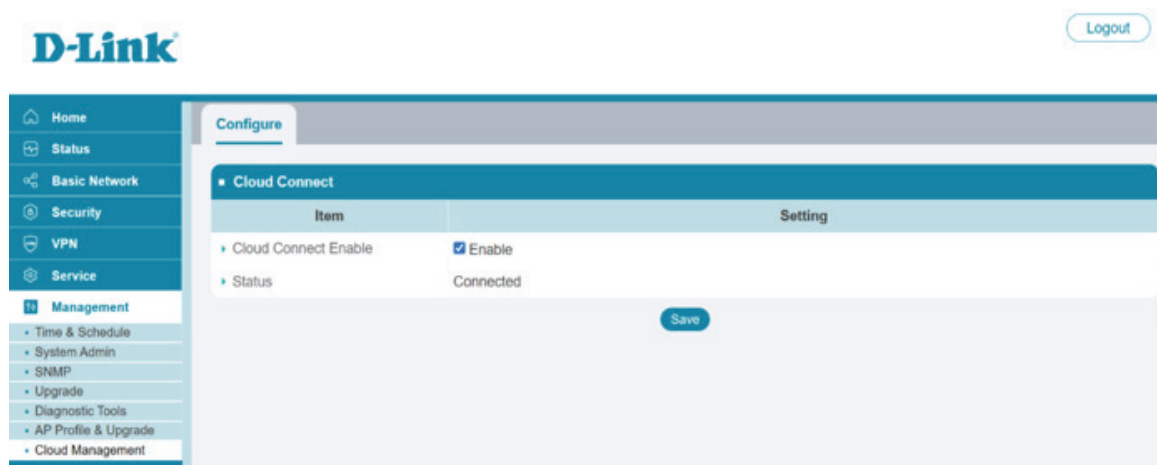
Username by default: admin

Password by default: Admin\$123



Enabling the DBR Router Cloud Connect

1. From the left navigation menu, go to: Management > Cloud Management
2. In the Cloud Connect section, select Enable.
3. Check the Status field: When the router is successfully connected to the cloud service, the status will show Connected



Software Installation

Router

Add Device

Adding a Device to Nuclias Unity

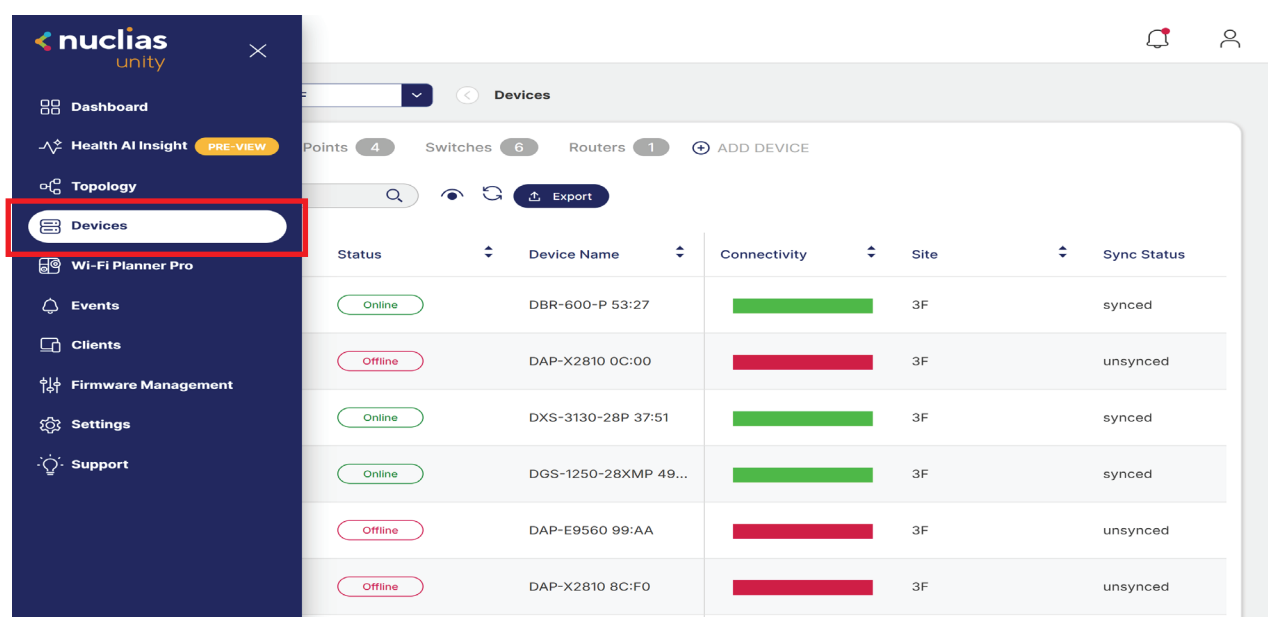
Before adding a DBR Router to Nuclias Unity, make sure you have already created an organization and site in the Nuclias Unity portal.

Log in to Nuclias Unity

1. Open a web browser and go to the Nuclias Unity management platform.
2. Sign in using your administrator account credentials.
3. After logging in, select the pre-created Organization.
4. Select the appropriate Site where the DBR Router will be deployed.

Navigate to the Device Menu

1. From the left-side navigation menu, click Device.
2. The device management page will appear.
3. Confirm that the correct organization and site are selected before adding the device.



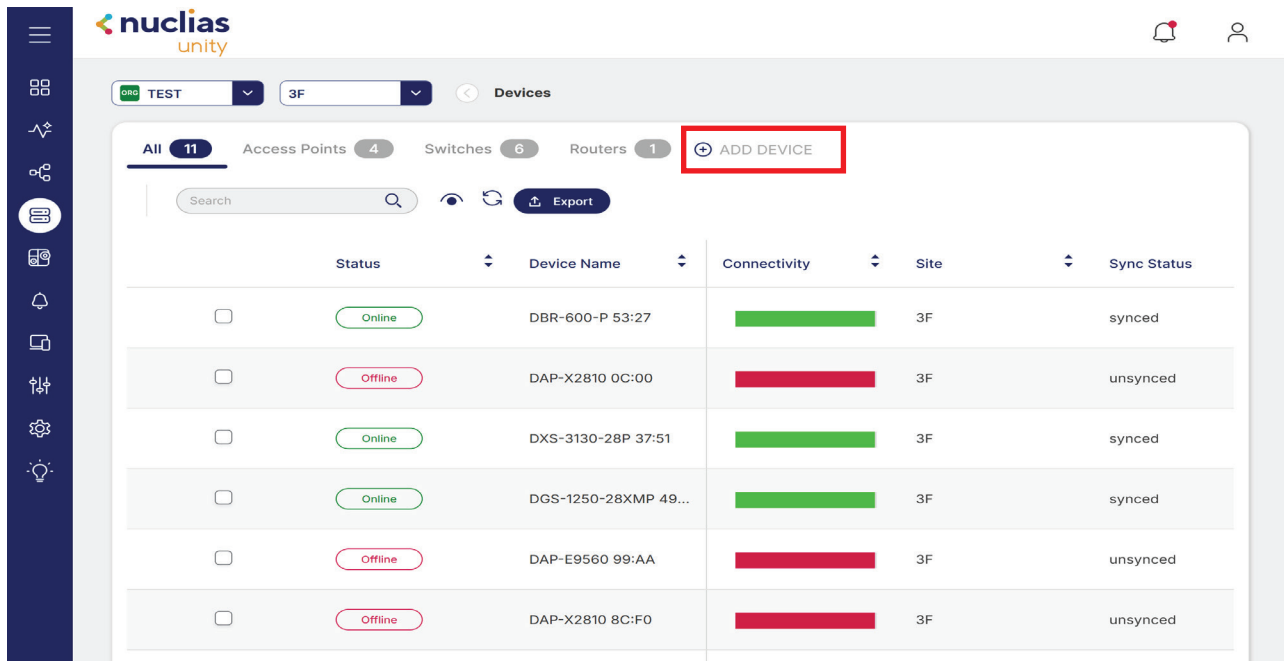
Software Installation

Router

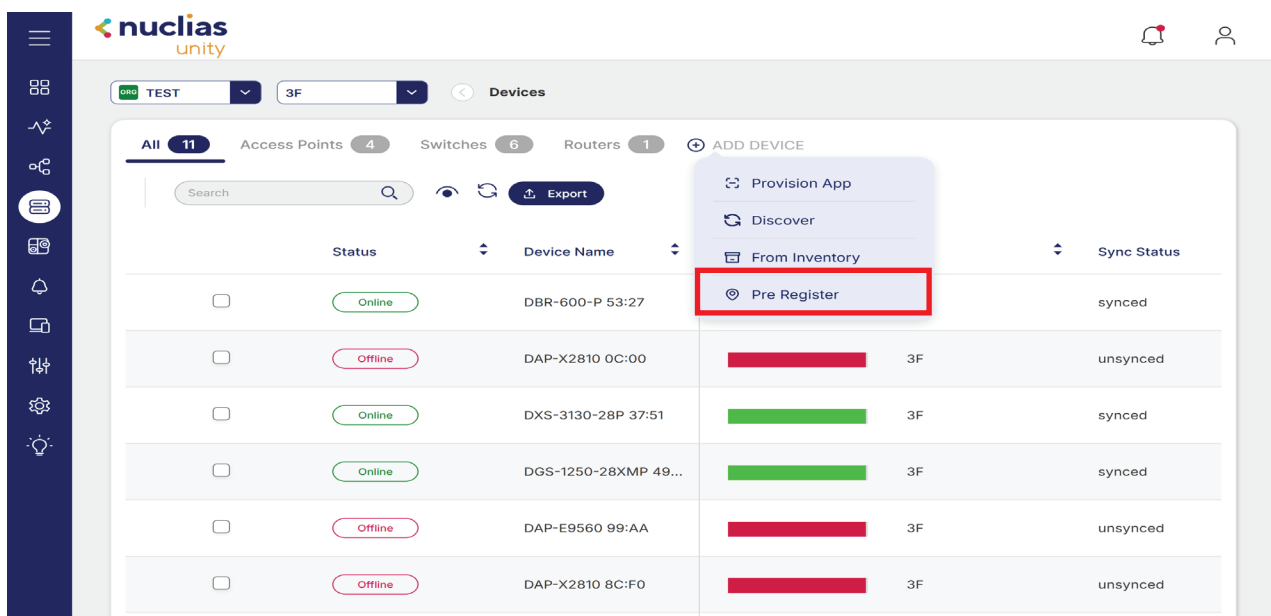
Add Device

Add a Device

1. On the Device page, click Add Device.
2. Nuclias Unity will display the available methods for adding and provisioning devices to the selected site.



3. In the Add Device window, select pre-register. This option allows you to register devices in Nuclias Unity before they are deployed, ensuring they automatically receive the assigned configuration when they connect to the Internet.



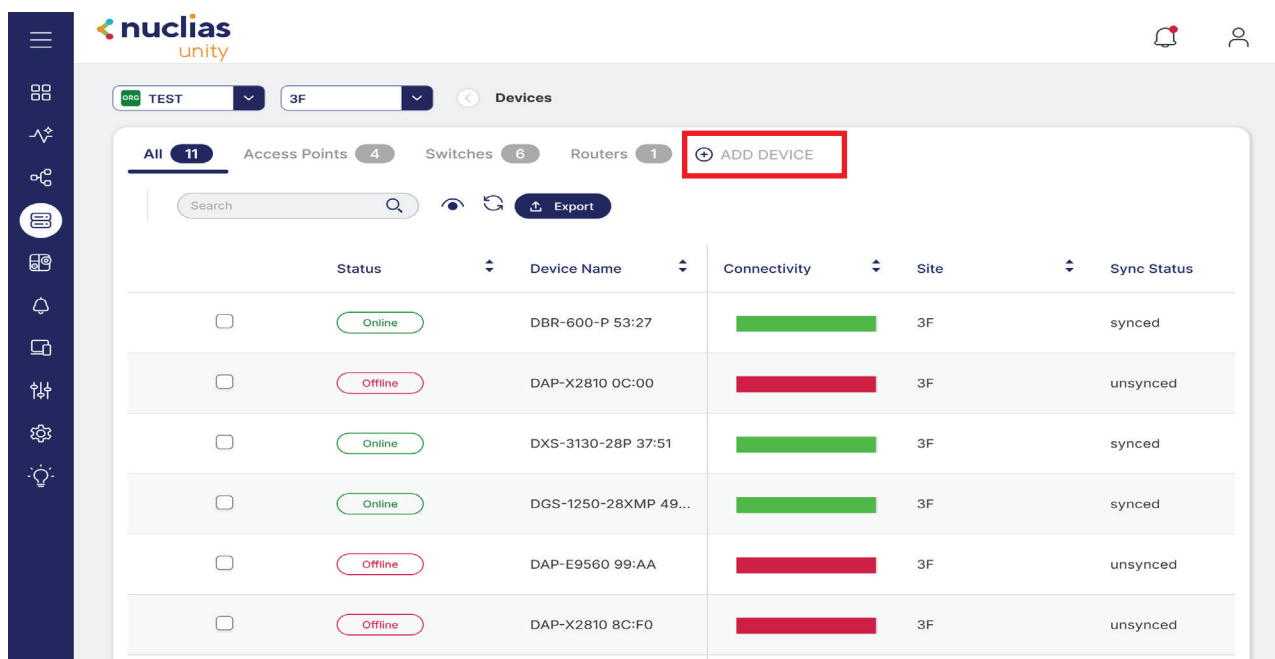
Software Installation

Router

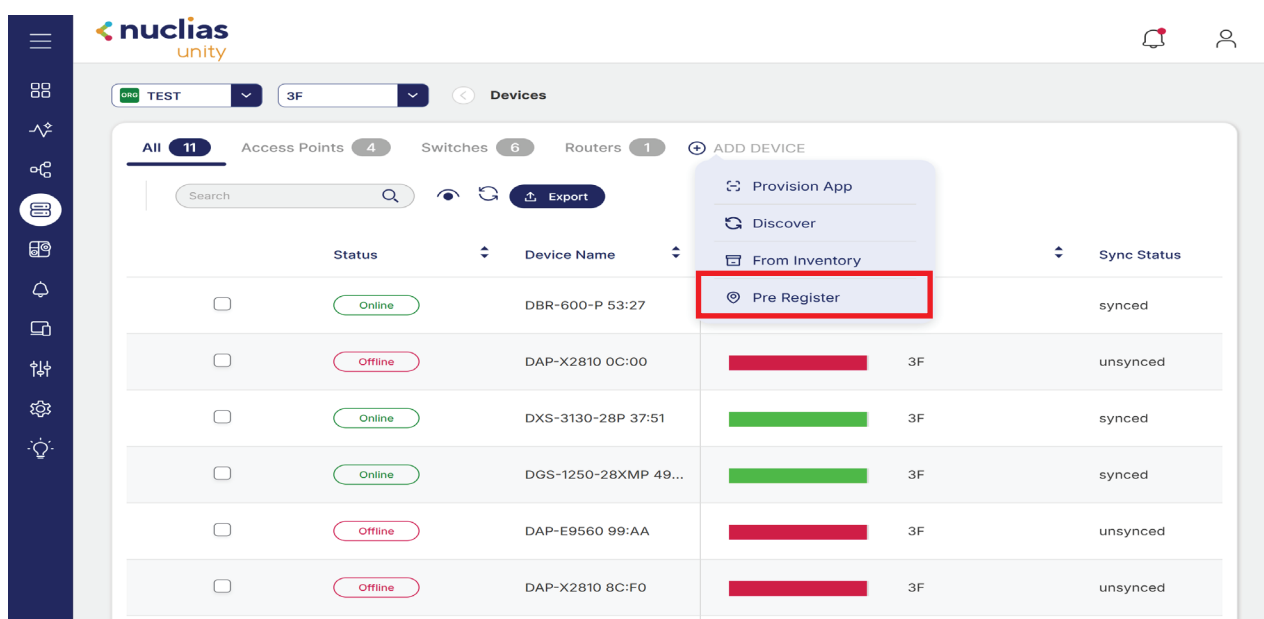
Add Device

Add a Device

1. On the Device page, click Add Device.
2. Nuclias Unity will display the available methods for adding and provisioning devices to the selected site.



3. In the Add Device window, select **Pre-Register**. This option allows you to register devices in Nuclias Unity before they are deployed, ensuring they automatically receive the assigned configuration when they connect to the Internet.

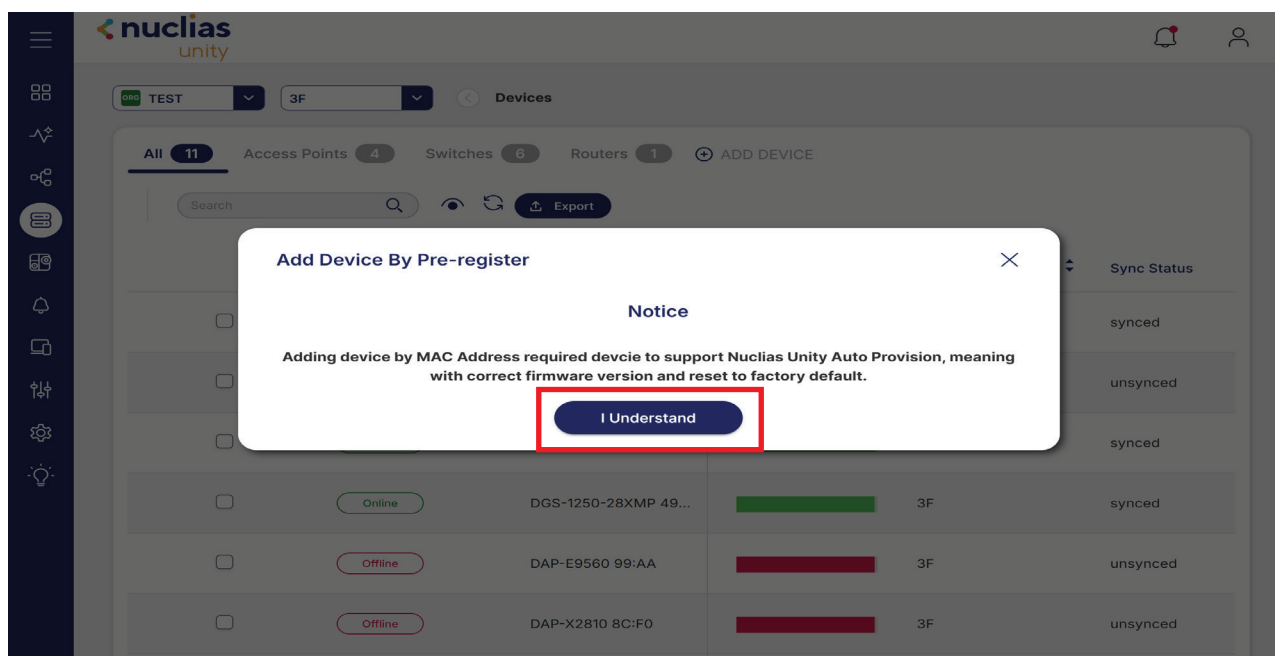


Software Installation

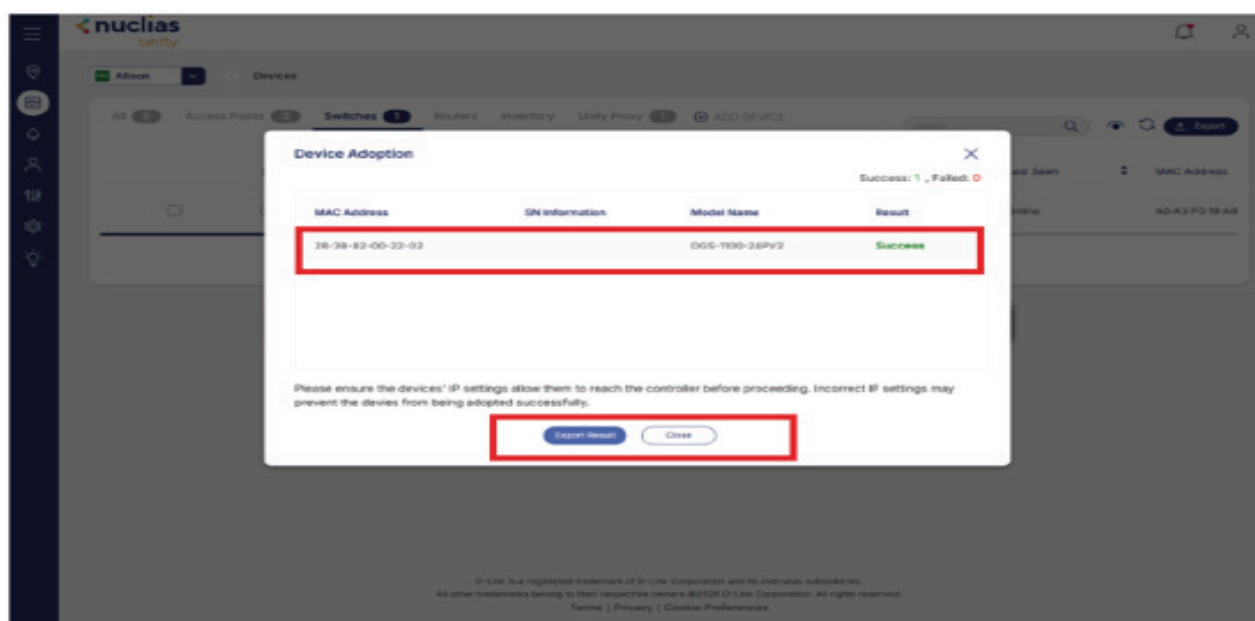
Router

Add Device

4. When **Pre-Register** is selected, a notice is displayed informing the user that adding a device requires its **MAC Address** and that the device must support Nuclias Unity Auto Provisioning.



5. Once the device is added successfully, a Success message is displayed. The added device will also appear in the device list, along with its model information, confirming that it has been successfully registered in Nuclias Unity



Nuclias Unity

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.

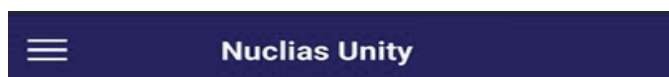
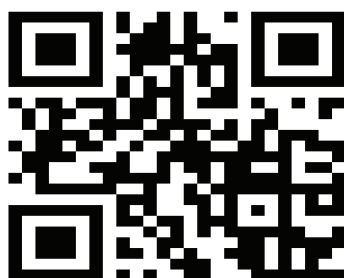
Before launching the app, confirm that you have already created your Organization and Site Name through the Nuclias Unity web browser interface.

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:



Quick Setup

Quick and simple deployment of network devices to Nuclias Unity

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.



Sign In

Username

Password



☒ Remember Me [Forget Password](#)

Sign In

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.

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.

Nuclias Unity

Select an Organization and a Site to manage your devices.

Select an Organization

Select a Site

If you do not have an Organization to select, please add and manage your Organization through the Nuclias Unity Portal Website.

Next

Nuclias Unity

Select an Organization and a Site to manage your devices.

Select an Organization

Unity_Test_GMD

Select a Site

GMD-Test

If you do not have an Organization to select, please add and manage your Organization through the Nuclias Unity Portal Website.

Next

Page 33

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.

Nuclias Unity

Search for Nuclias Unity supported device within your connected network.

Scan (Multicast)

IP Range (Unicast)

From

192.168.0.1

to

192.168.0.255

Add an IP range

Next

Device Found

8 devices have been found. Please select device(s) for operation.

DXS-1210-16TC
V2.03.008

10.90.90.90
64:29:43:91:fa:20

DAP-X3060OU
1.01

192.168.11.81
bc:22:28:e7:a6:30

DAP-X3060W
1.00

192.168.11.110
bc:22:28:e7:af:00

DAP-X3060
1.01

192.168.11.159
00:25:50:60:49:39

DMS-1250-28P
V1.03.005

10.90.90.90
dc:ea:e7:cc:27:70

DAP-E9560
1.00

192.168.11.117
bc:22:28:e7:af:20

DMS-1250-12TP
V1.03.005

192.168.11.91
bc:22:28:e7:9d:eb

DGS-1100-24PV2
v4.00.B021

10.90.90.90
28:3b:82:00:22:02

Selected 1 devices

Authenticate

Page 34

Software Installation

Adding Devices into Nuclias Unity

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

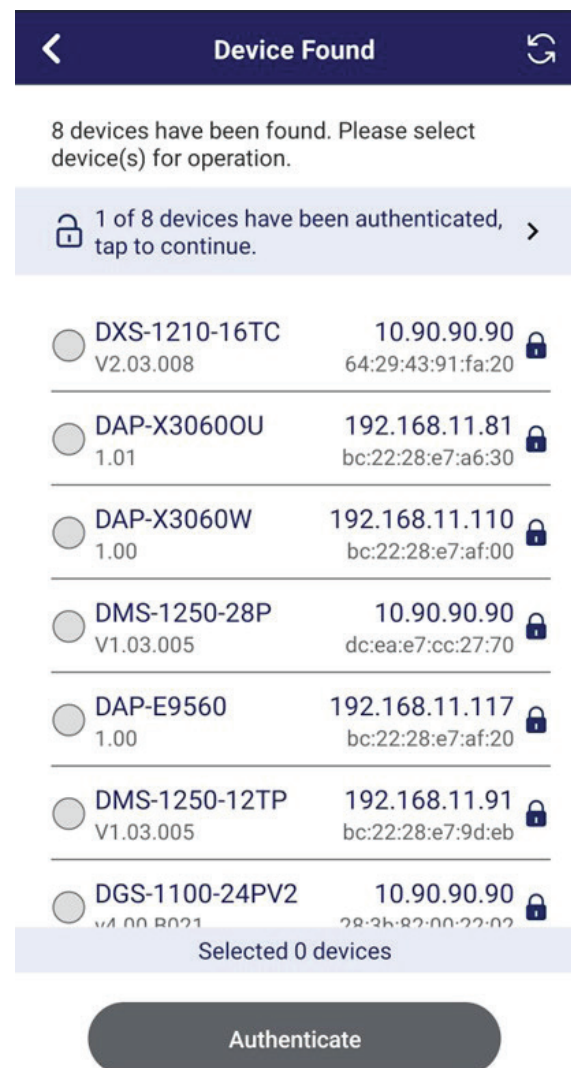
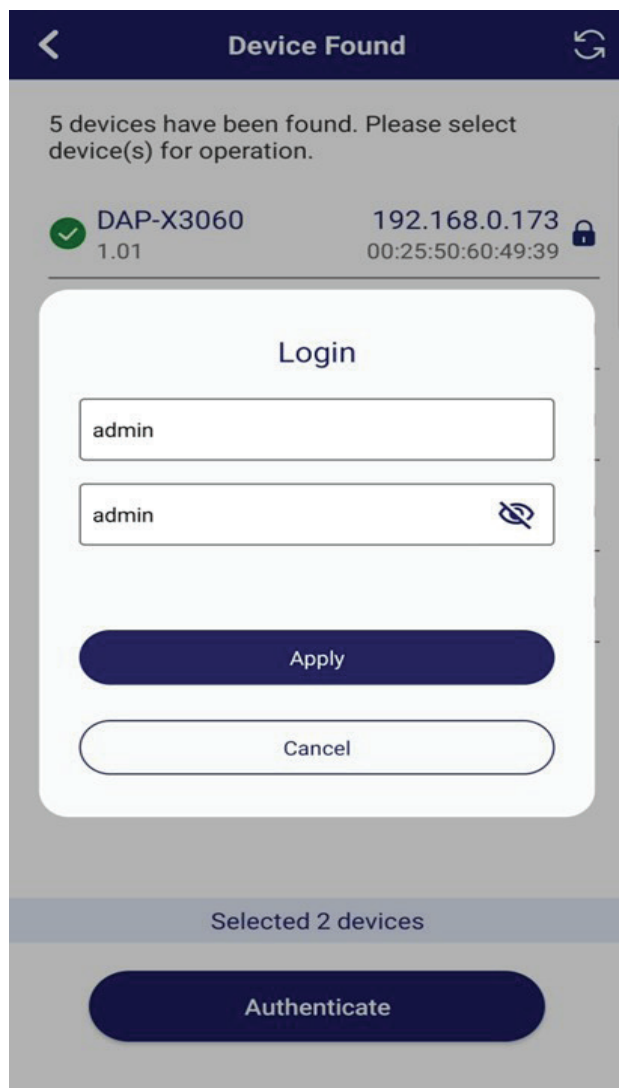
If authentication fails, it may indicate that the device credentials have been changed from the default settings. In this case, perform a hardware reset on the device to restore the factory default settings, and then repeat the adoption process.

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.

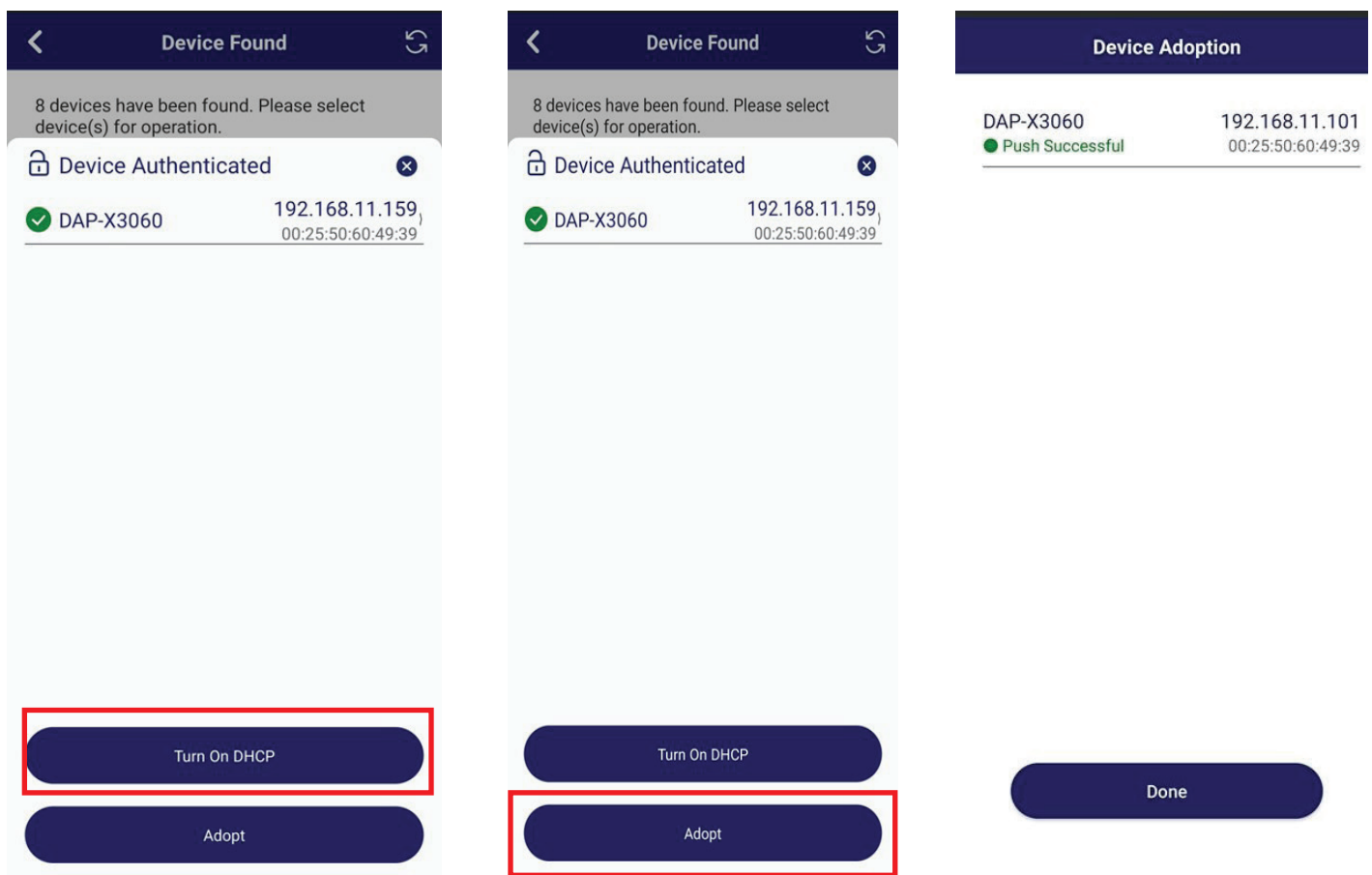
Before proceeding with adoption, click **Turn On DHCP**, as shown in the image below. This step enables DHCP on the device, allowing it to automatically obtain an IP address from the network's DHCP server. Ensure that your network has an active DHCP server available.

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.

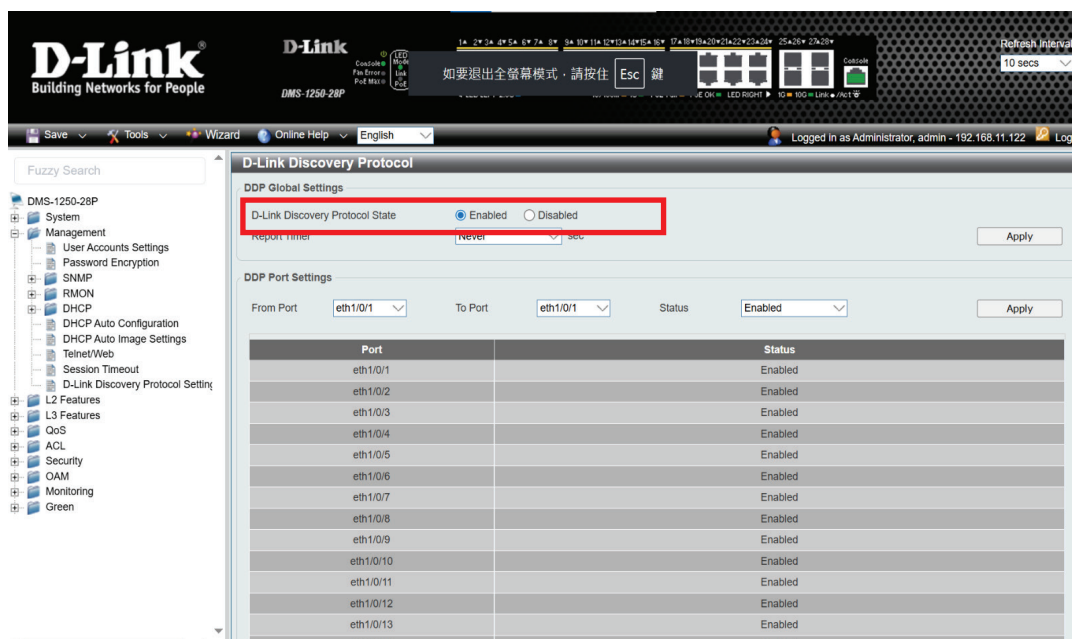
Here are the key details about Unity Proxy based on the provided documents:

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.



Nuclias Unity

Configuration

Device Setup

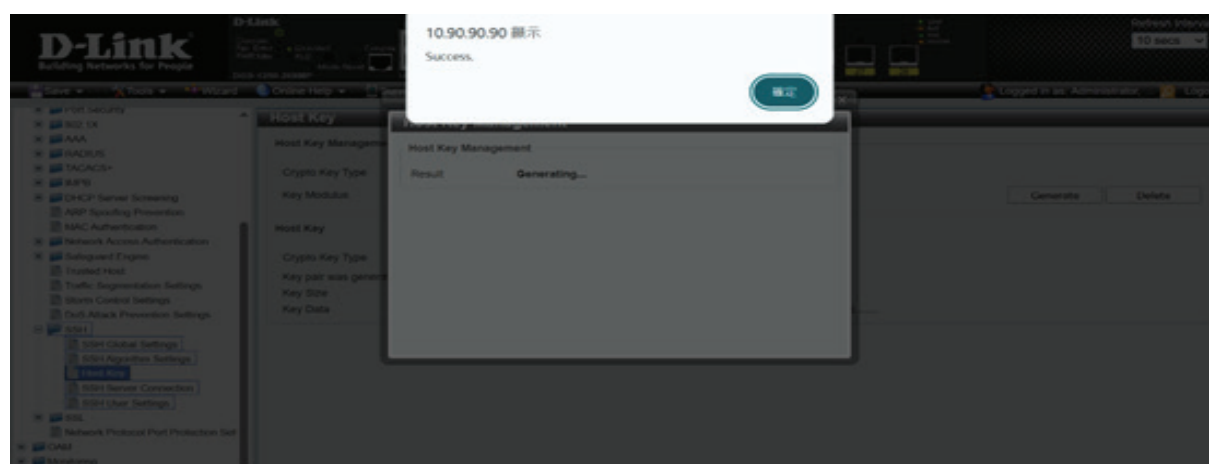
SSH Global Setting: Enable – Enables Secure Shell (SSH) access, allowing secure remote management of the device through an encrypted command-line connection.



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.



Nuclias Unity

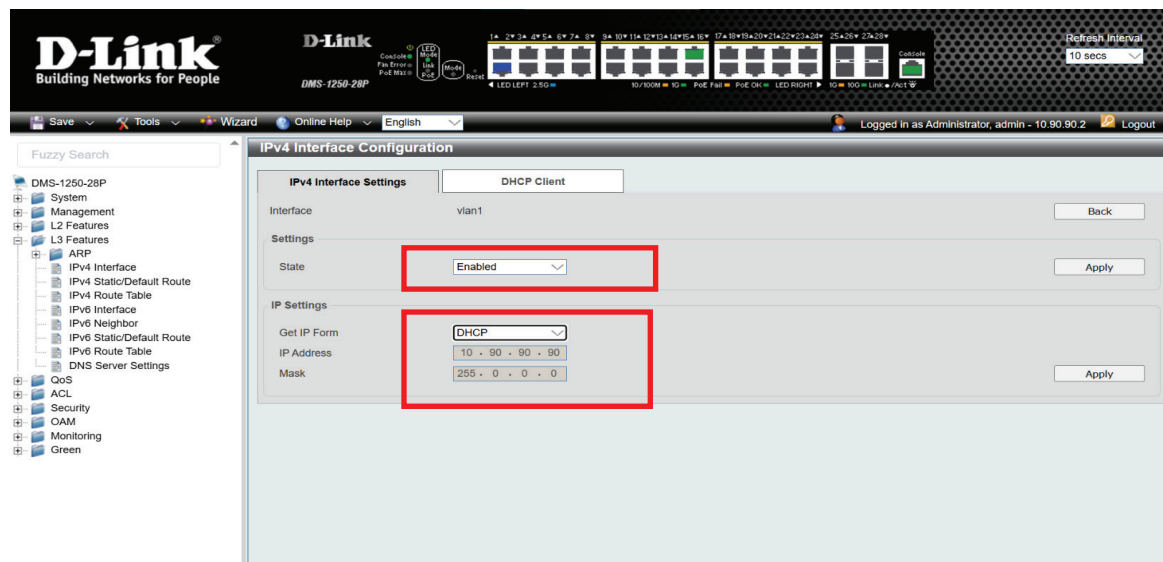
Configuration

Device Setup

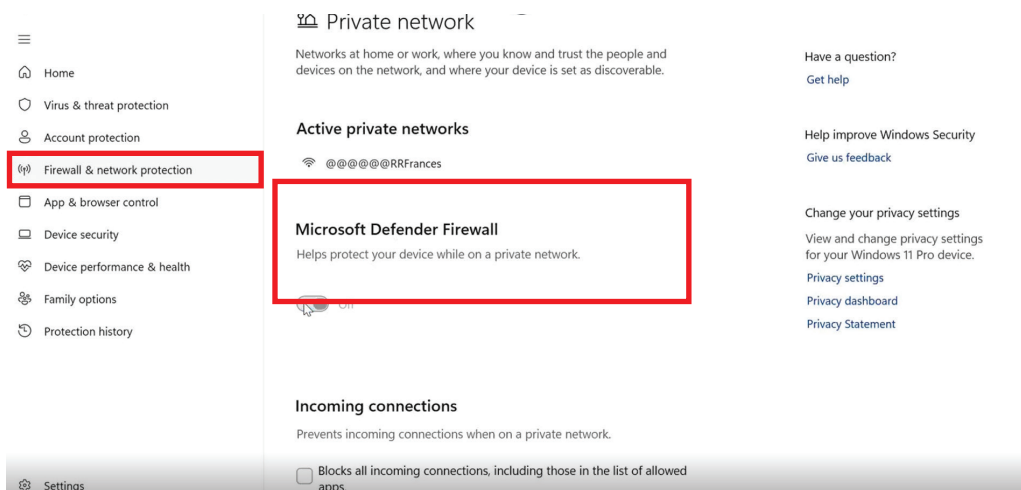
After generation, the key data will be displayed.



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.

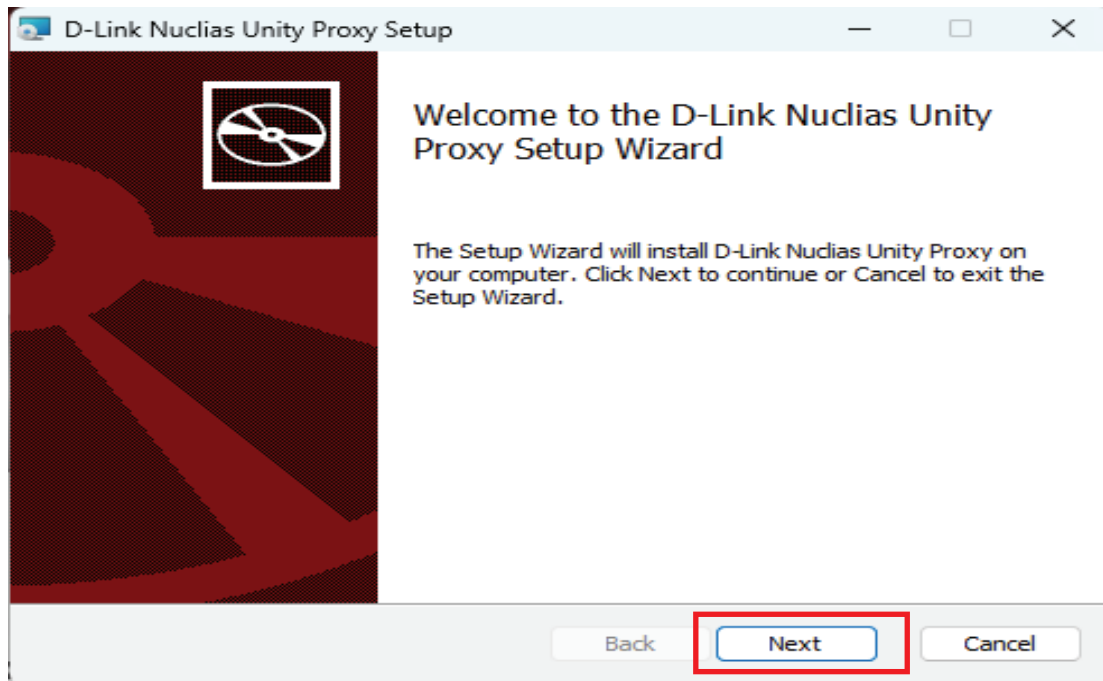


Nuclias Unity

Nuclias Proxy

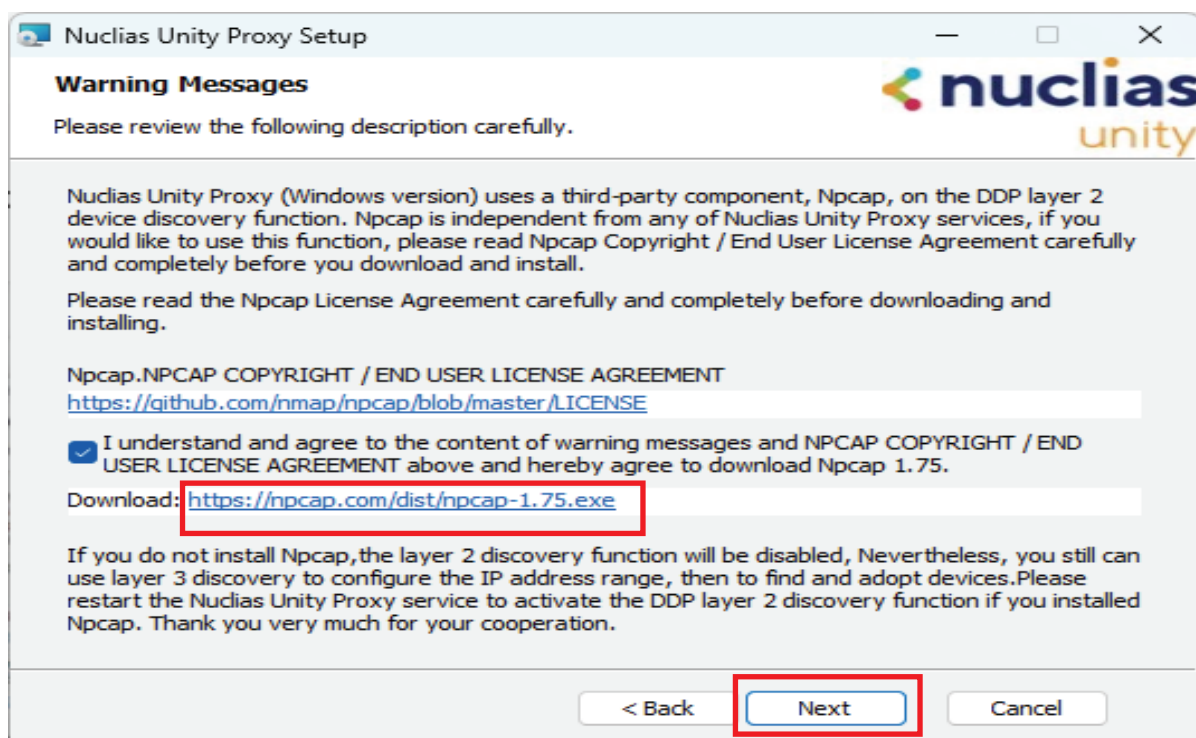
Proxy Installation

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.

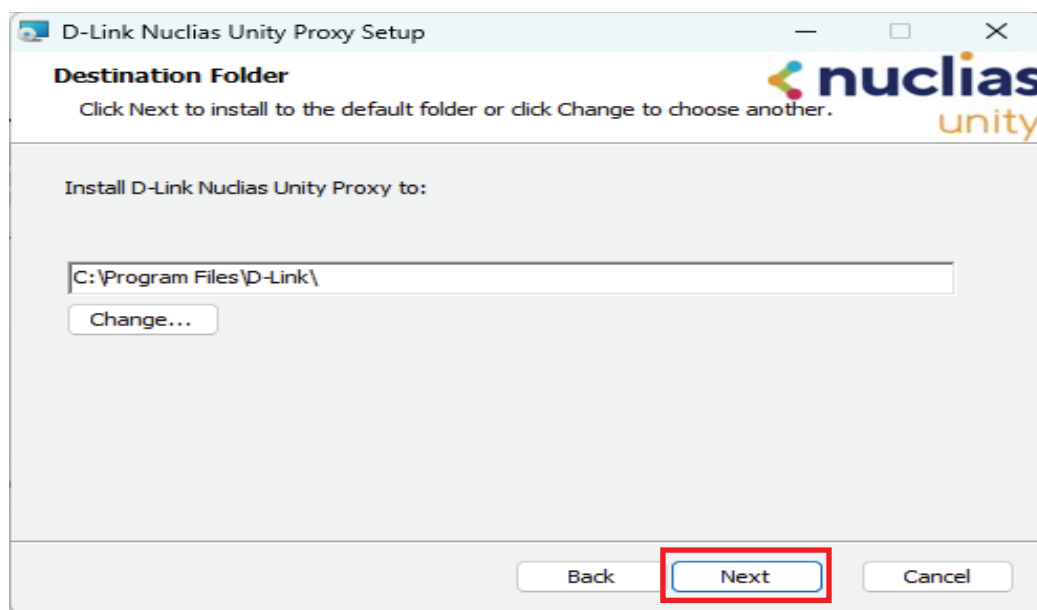


Nuclias Unity

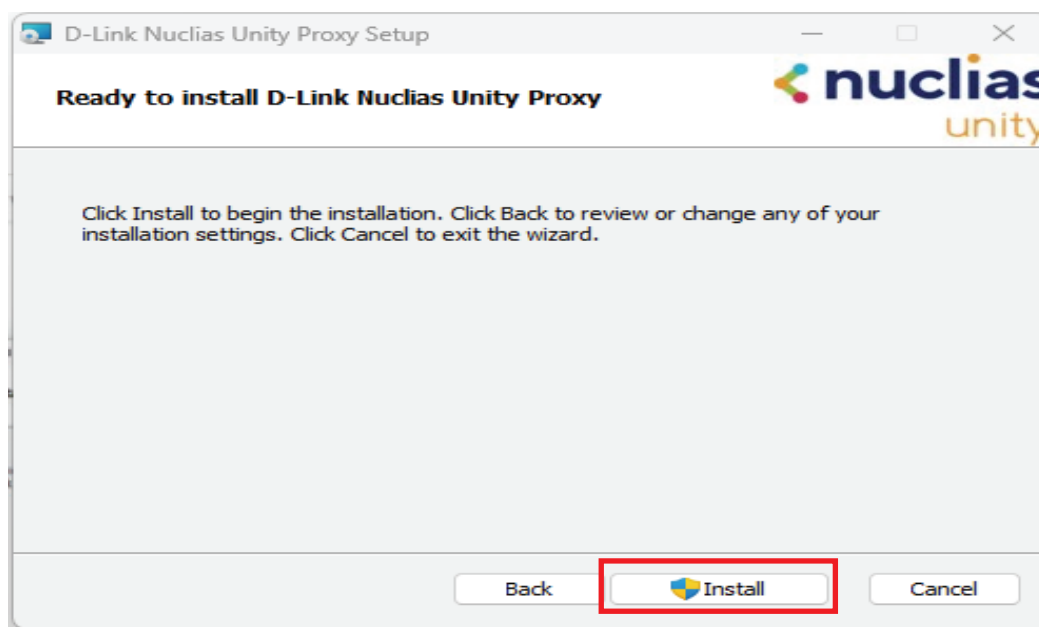
Nuclias Proxy

Proxy Installation

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.

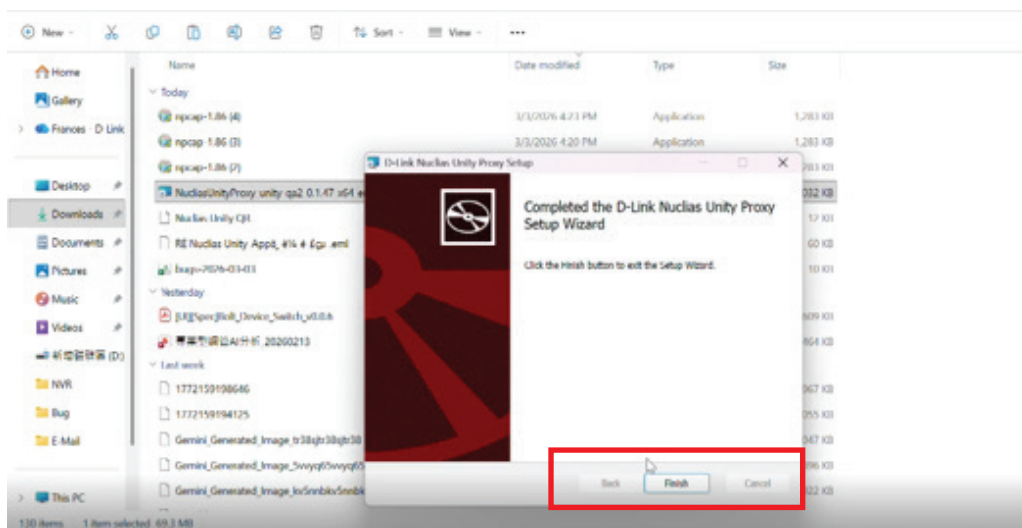


Nuclias Unity

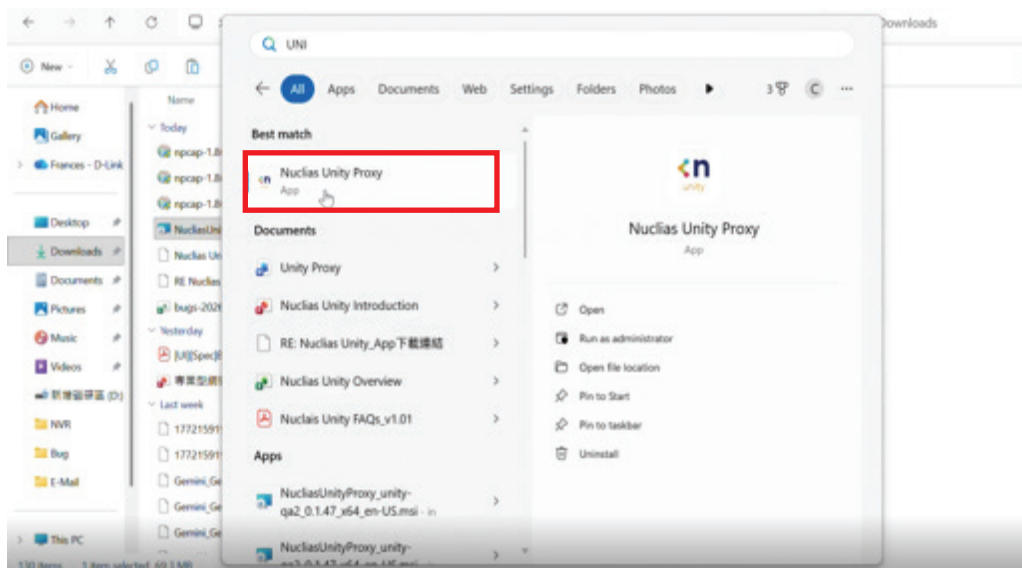
Nuclias Proxy

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.

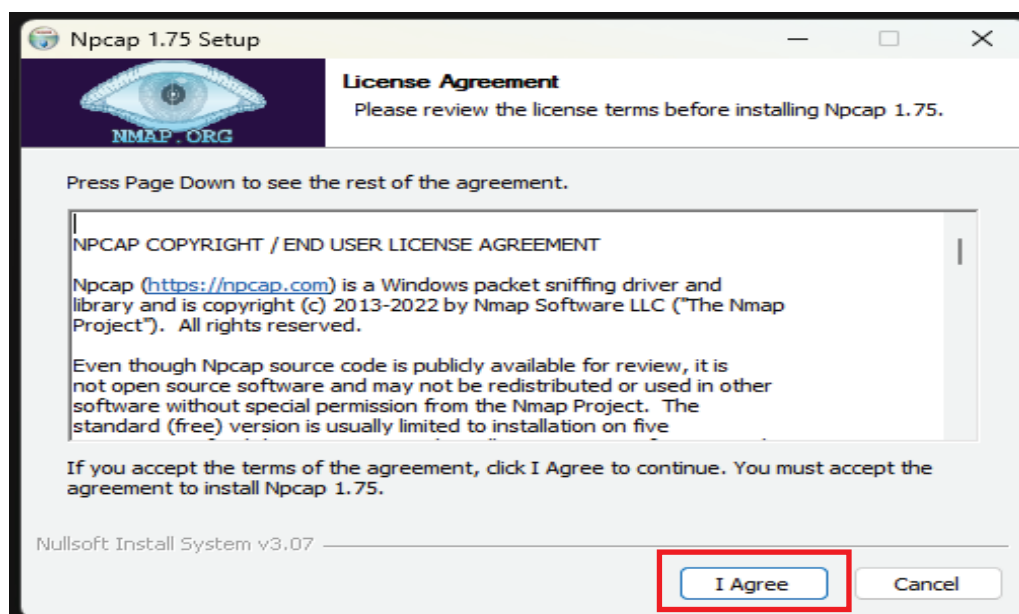


Nuclias Unity

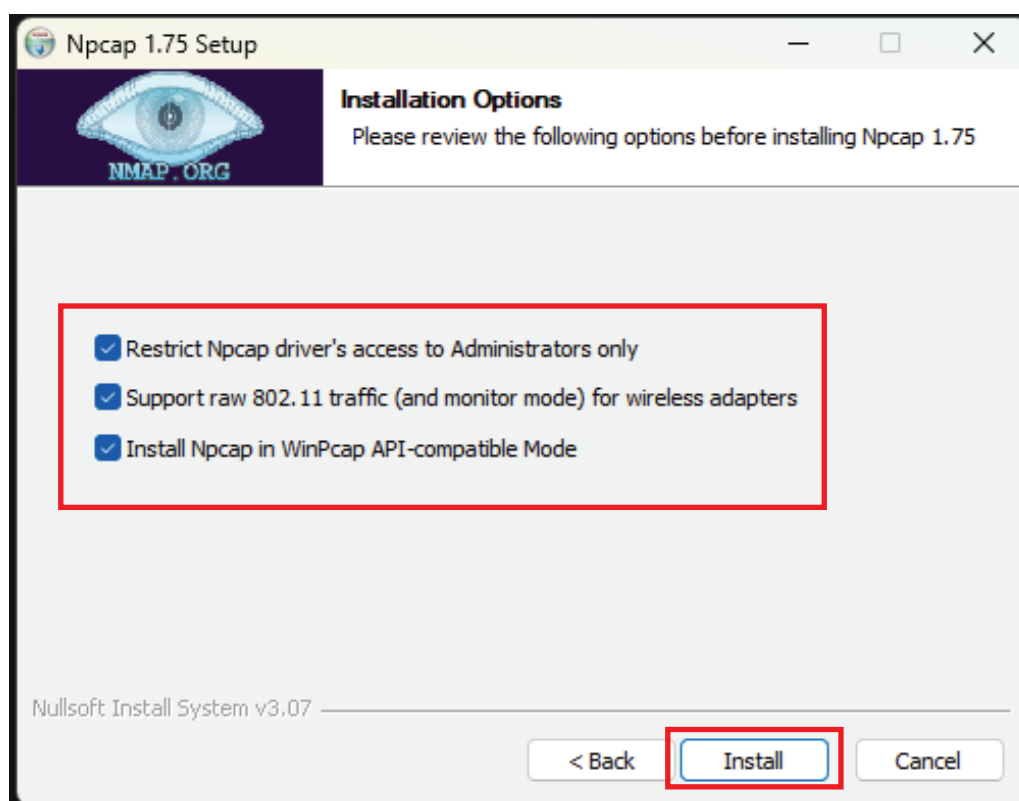
Nuclias Proxy

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.

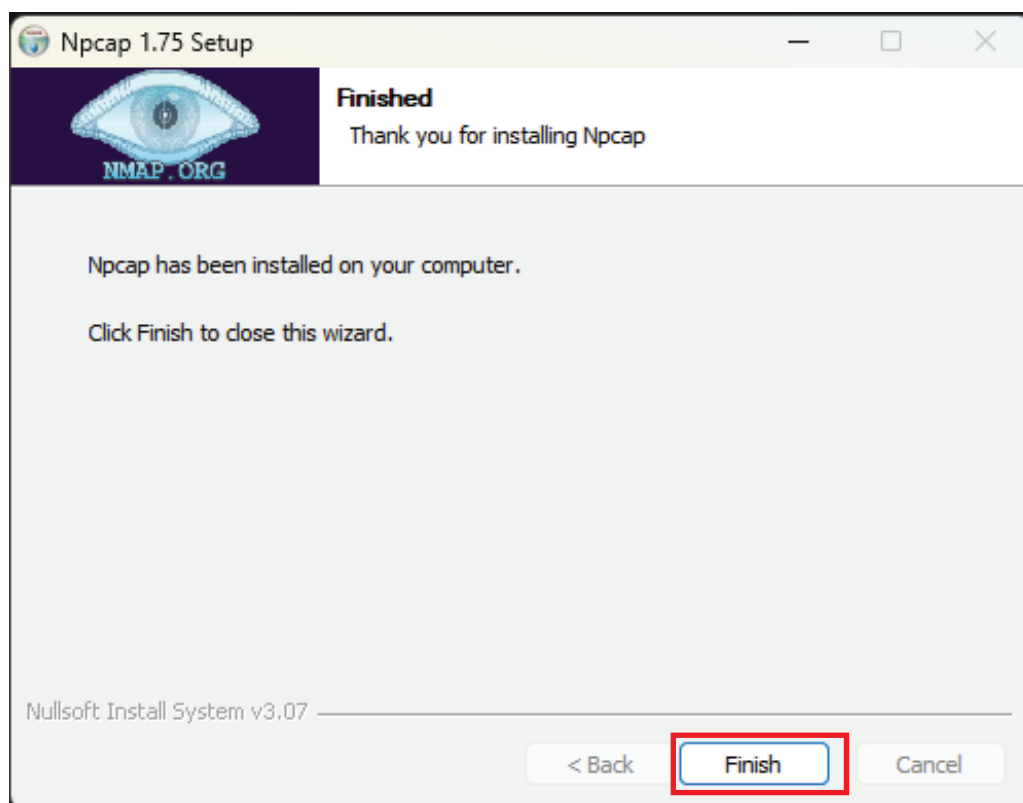


Nuclias Unity

Nuclias Proxy

NCAP Installation

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.



Welcome

Welcome to the Nuclias Unity Proxy installation.

This installation wizard will help you to setup a probe, allowing devices manageable by Nuclias Unity cloud using local SNMP and SSH protocol.

Check more information on this website.

Now you'll be asked to use your Nuclias Unity account to authorize this probe.

Next

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



Sign In

Email

name@example.com

Password

☒ Remember Me

[Forget Password](#)

Sign In

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.



Select the Home Organization

Select an Org where you need this probe belongs to

test

This probe can later be used for scan and adding device to selected organization and its sites, from Nuclias Unity web portal.

Cancel

Adopt

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.



About

Status Summary

Linked Organization

Organization: test

Unity Proxy ID: 909a4d79-28ba-4311-8bc8-afc99c75d4e6

Device ID: 45b09d20-7de6-4f89-b8d5-a85ea2ad6d4e

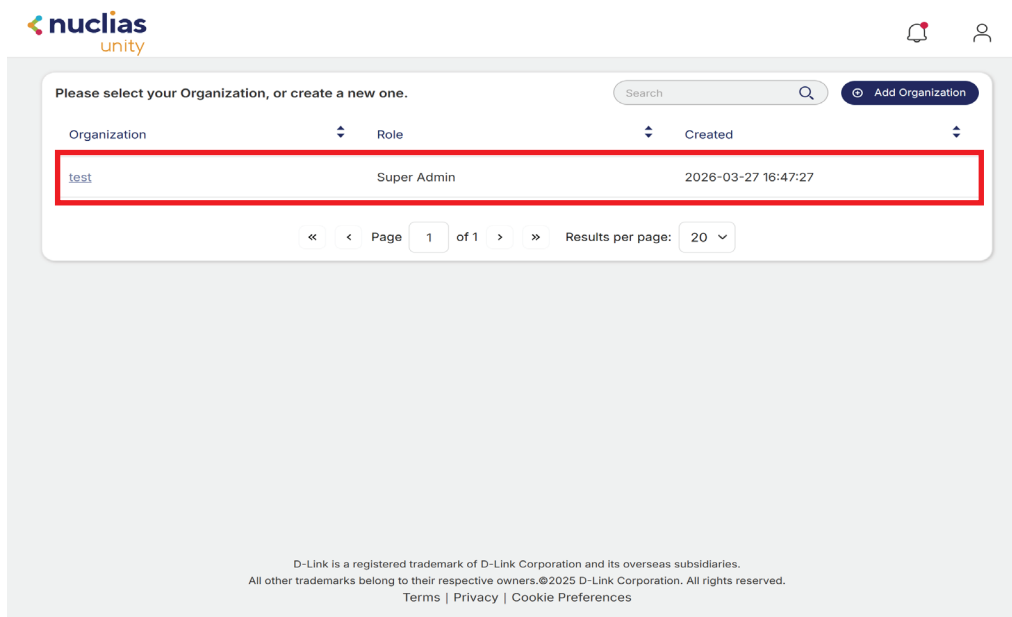
Status: Online

Nuclias Unity

Nuclias Proxy

Add Device

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

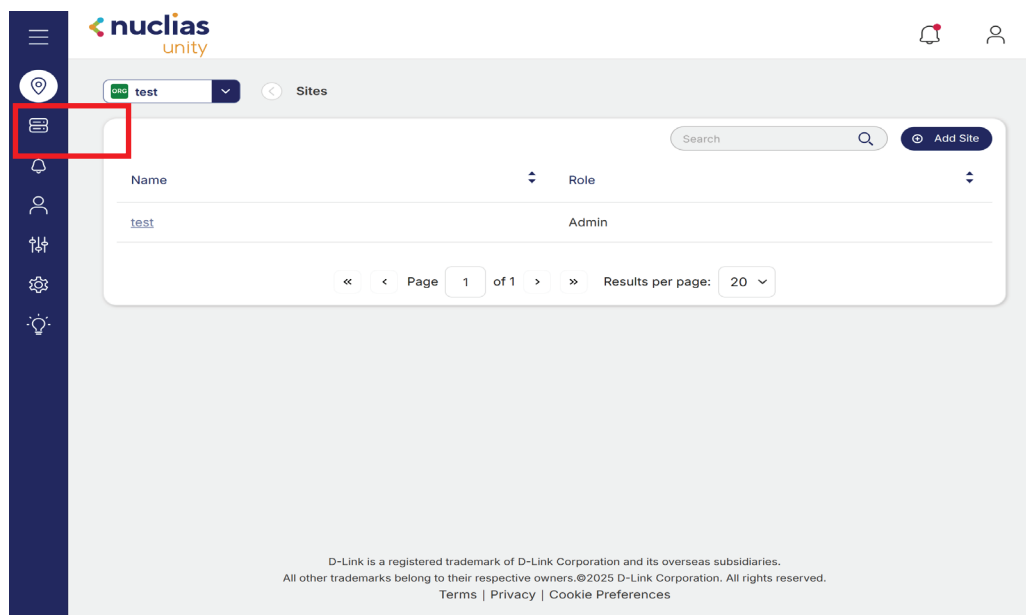


Nuclias Unity

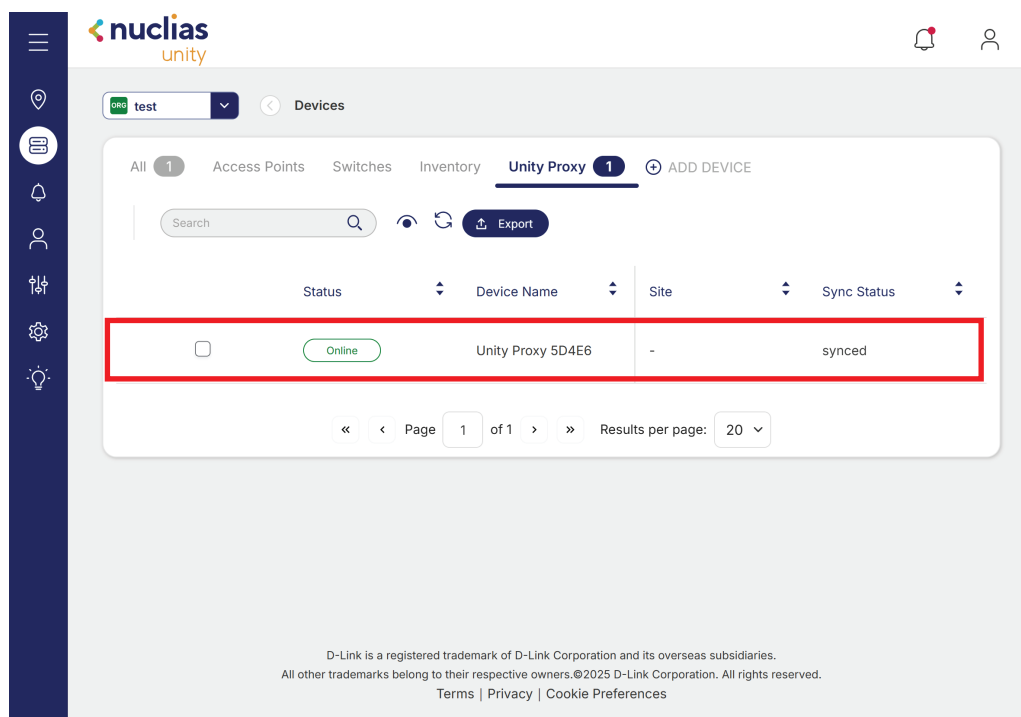
Nuclias Proxy

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**.

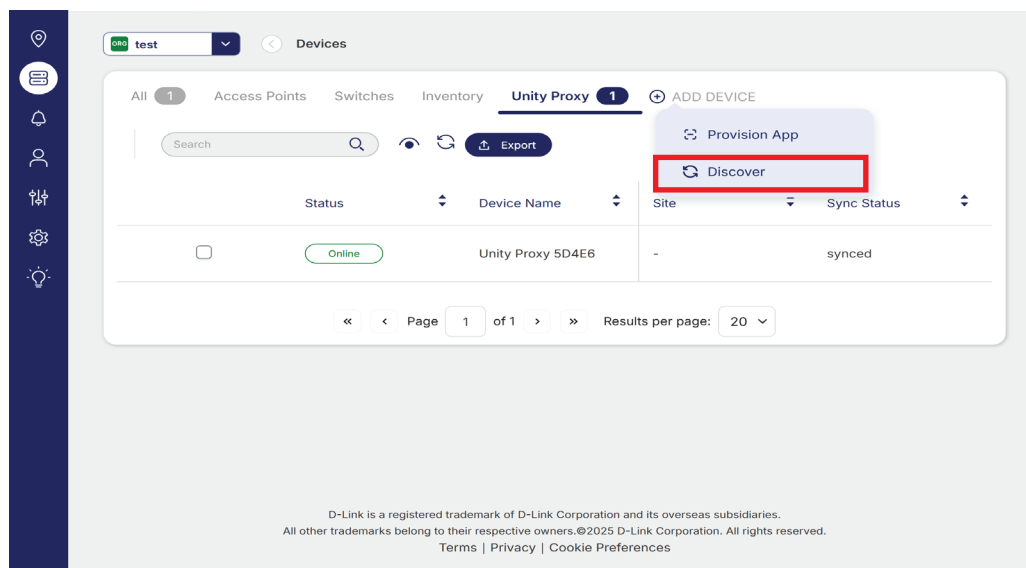


Nuclias Unity

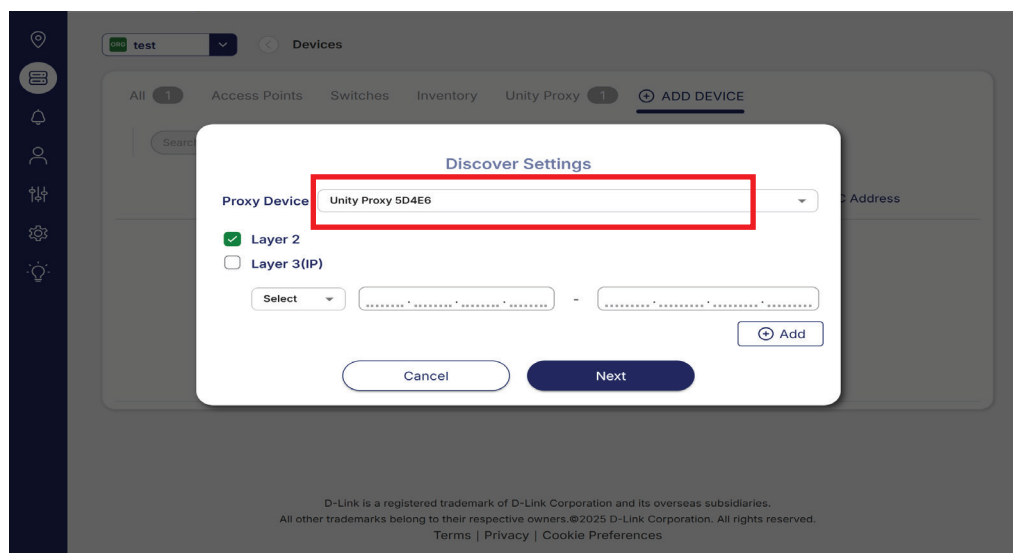
Nuclias Proxy

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.

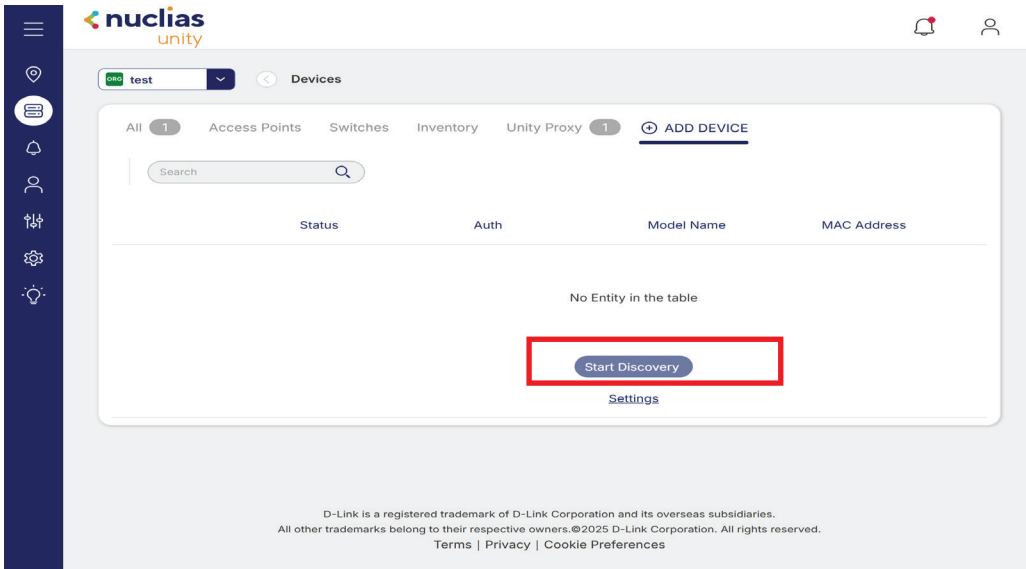


Nuclias Unity

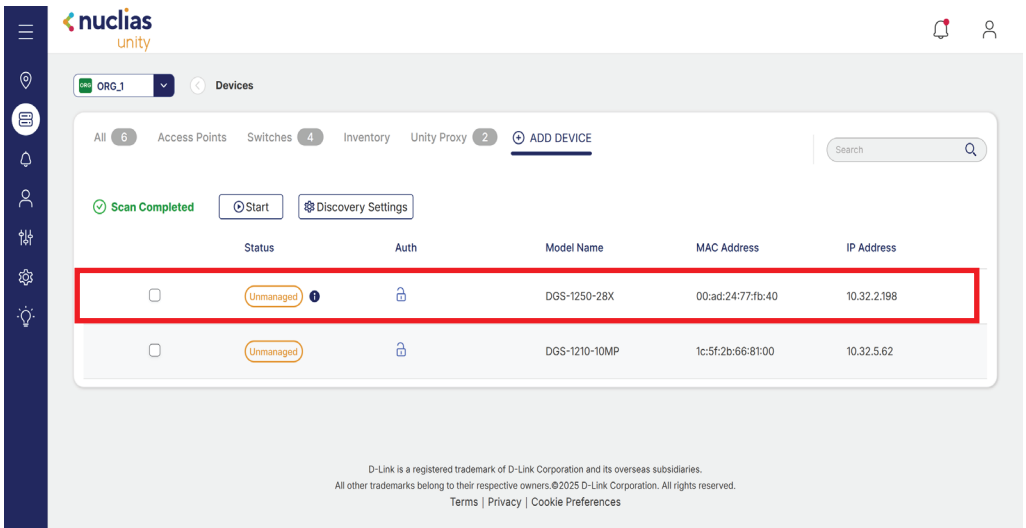
Nuclias Proxy

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.

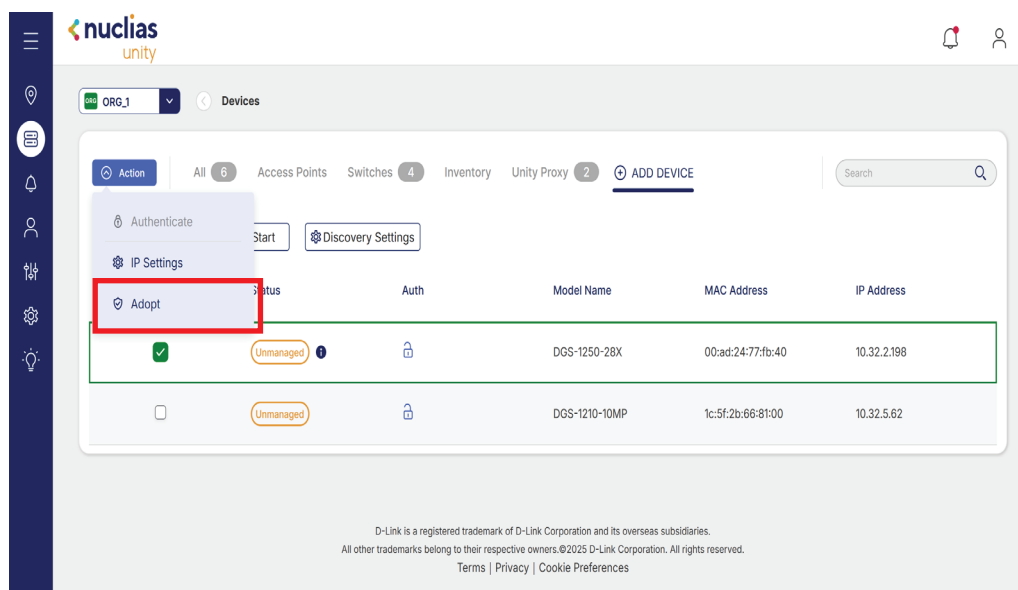


Nuclias Unity

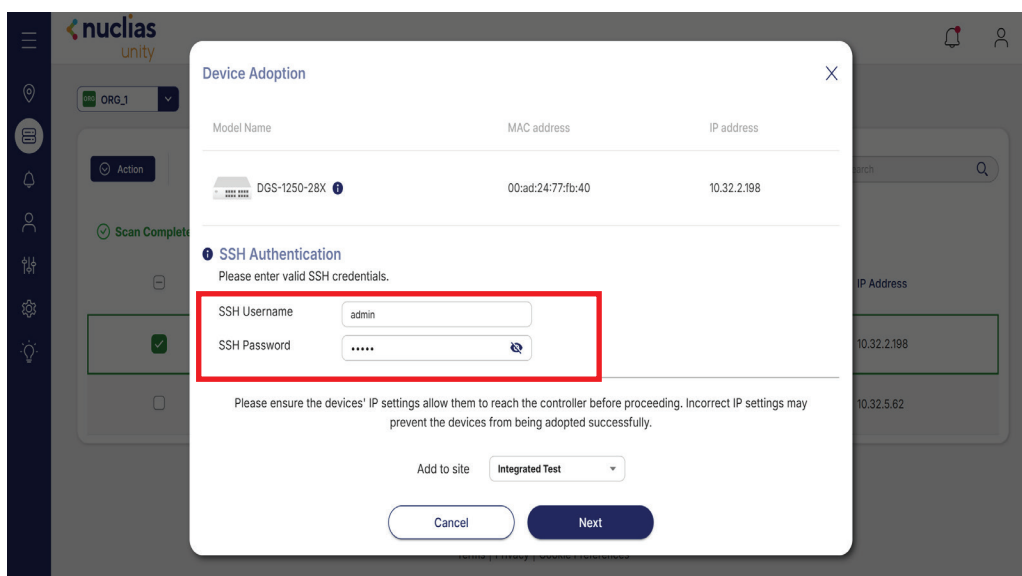
Nuclias Proxy

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.

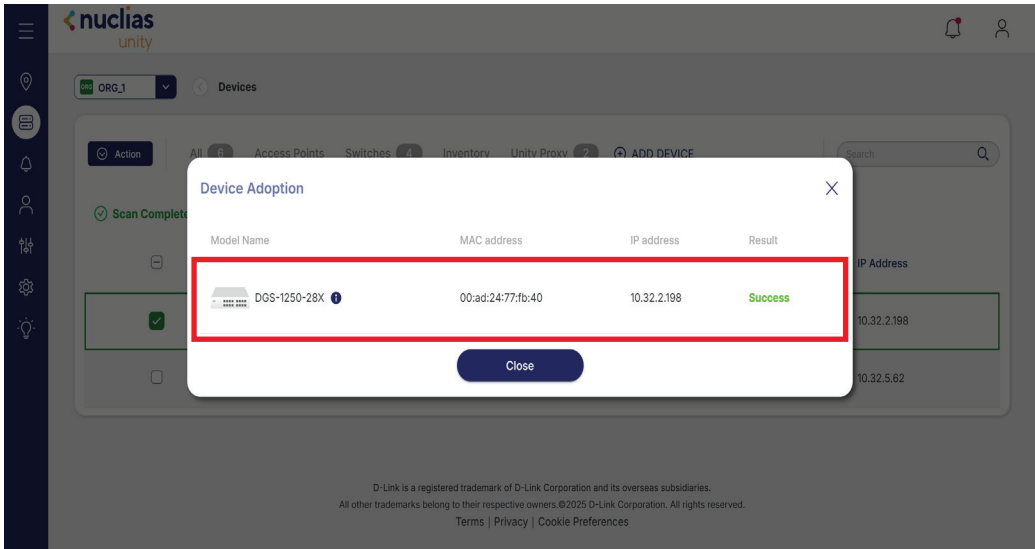


Nuclias Unity

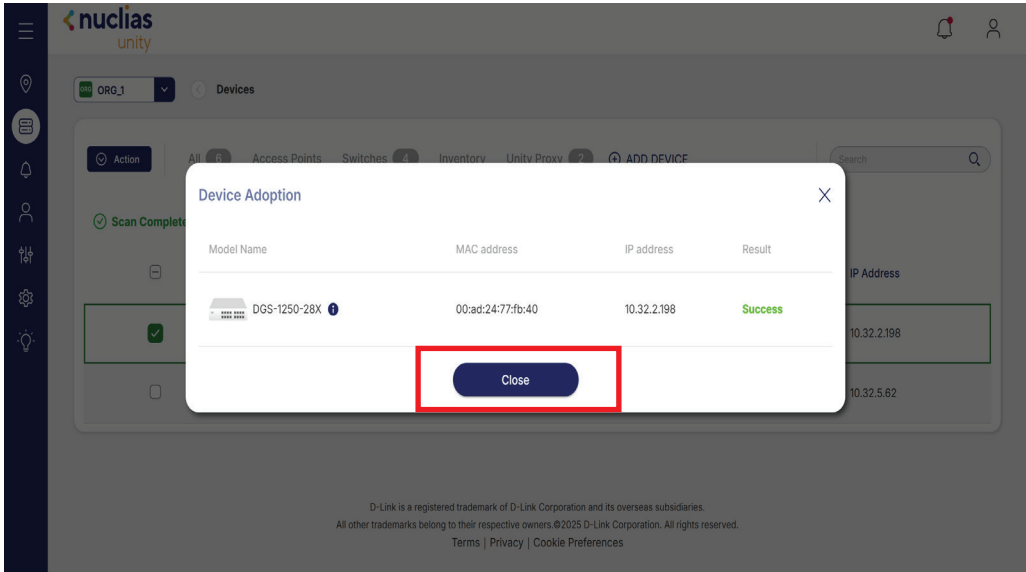
Nuclias Proxy

Add Device

The adopted devices will now display a Success status.



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

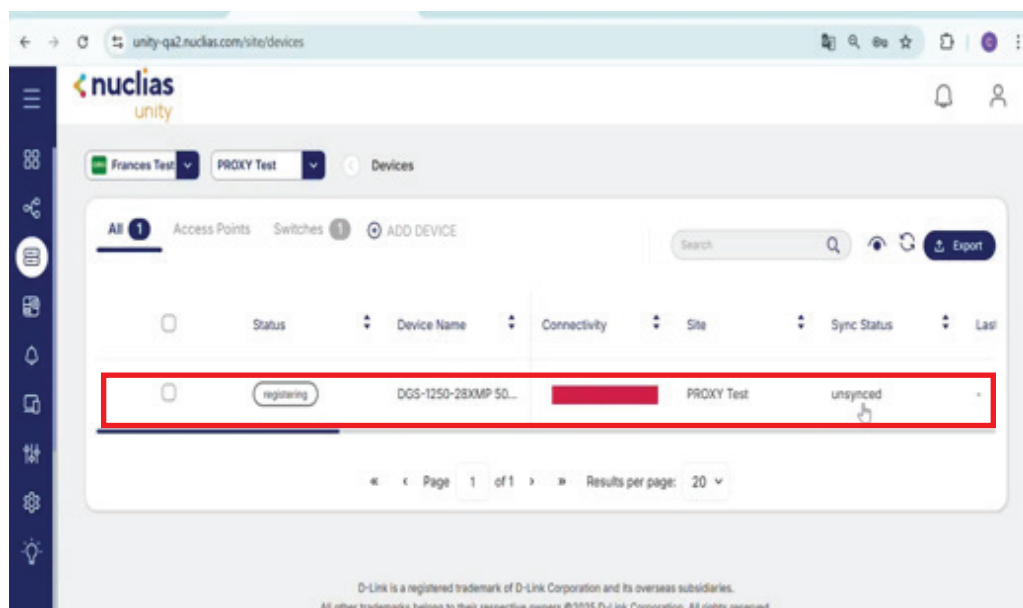


Nuclias Unity

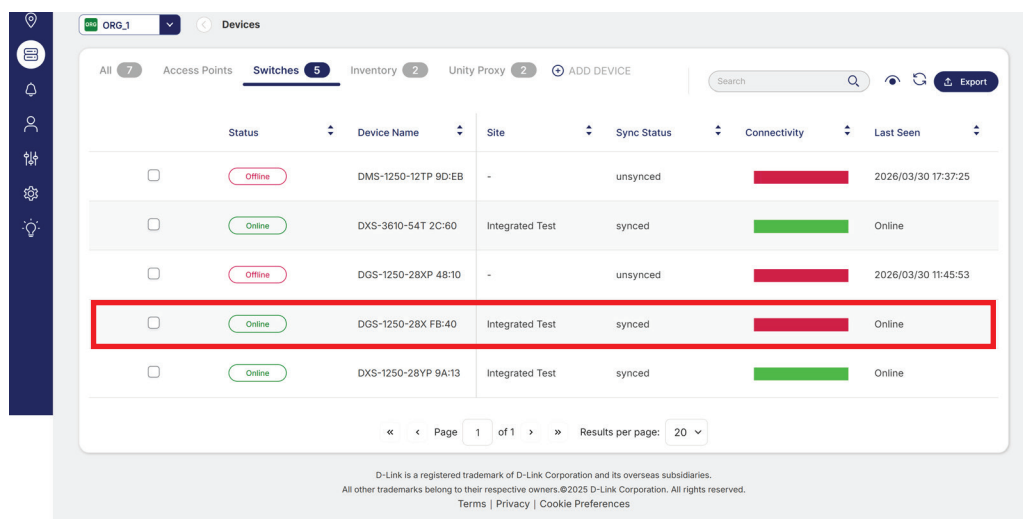
Nuclias Proxy

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, Firmware 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 visibility
- Apply consistent policies across locations

Each deployment must have at least one Organization.

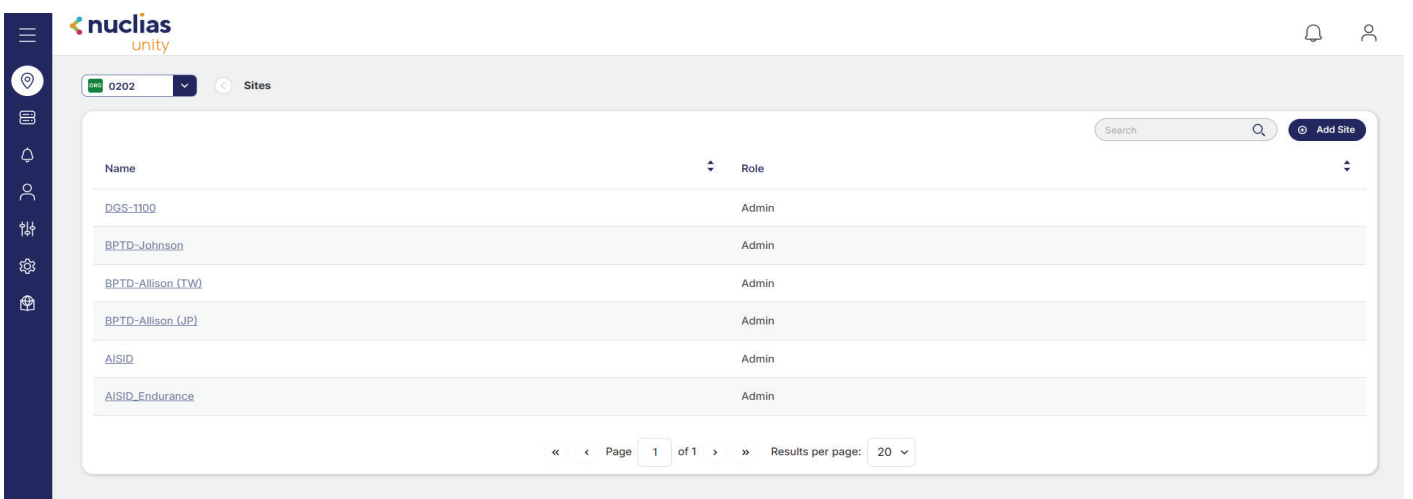
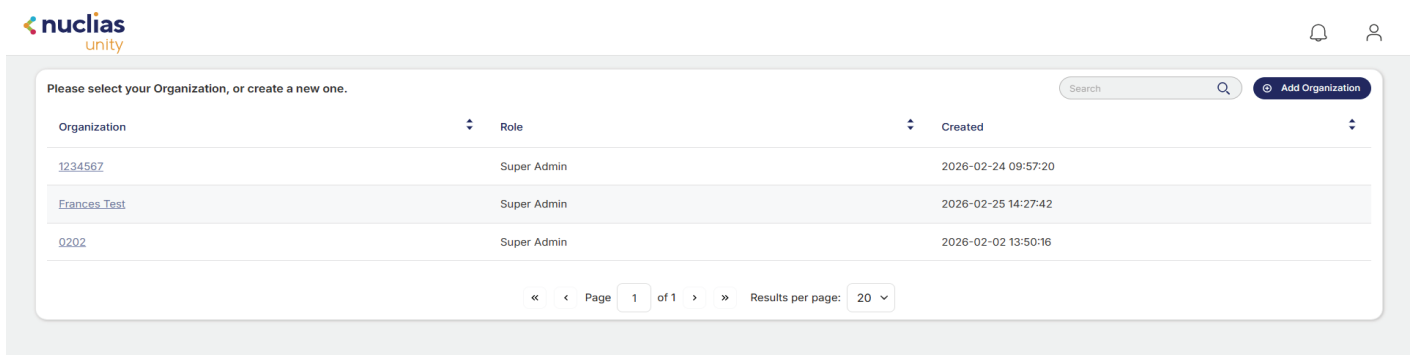
Site

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.

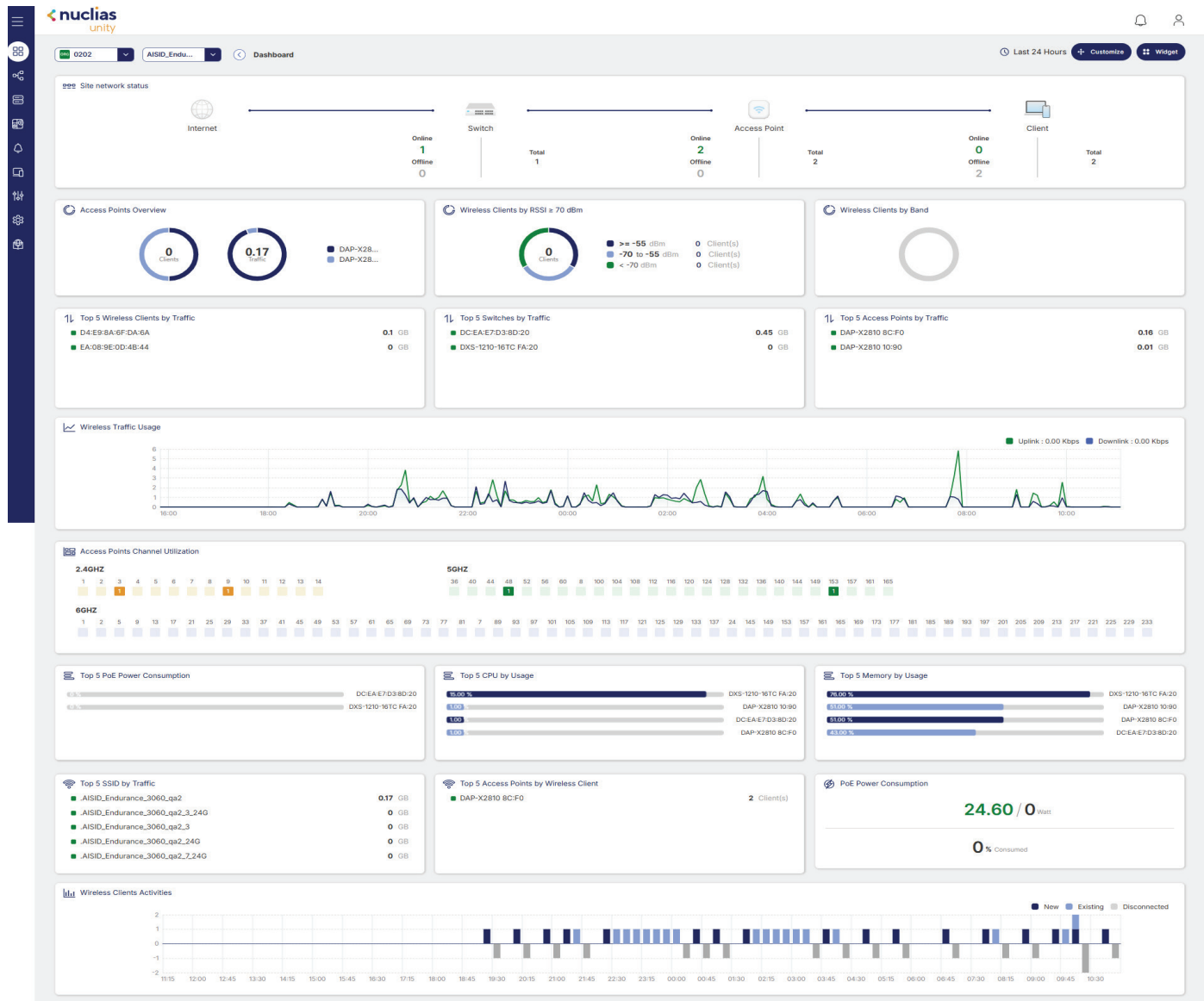


Nuclias Unity

Dashboard

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.



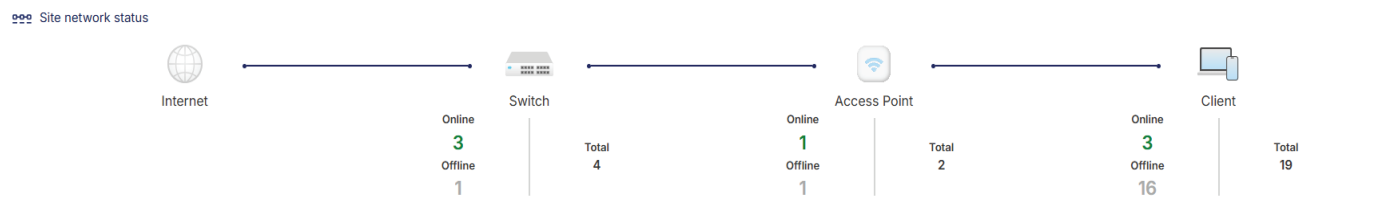
Nuclias Unity

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

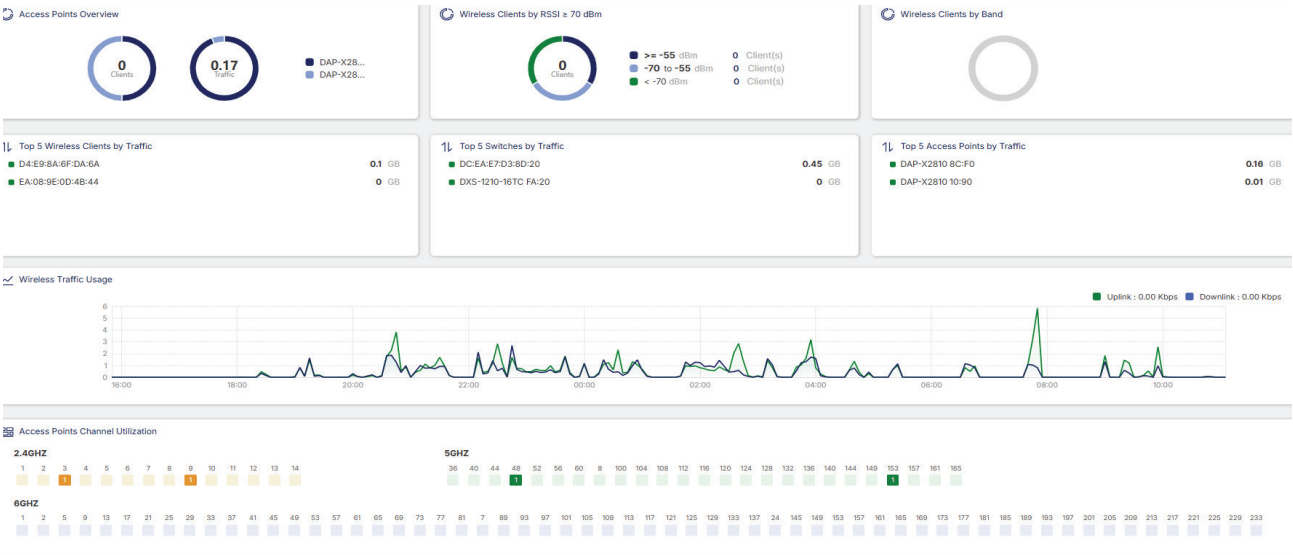
This section displays the top five wireless clients and access points ranked by traffic usage. It helps administrators identify high-bandwidth users and heavily utilized access points for better monitoring and performance optimization.

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

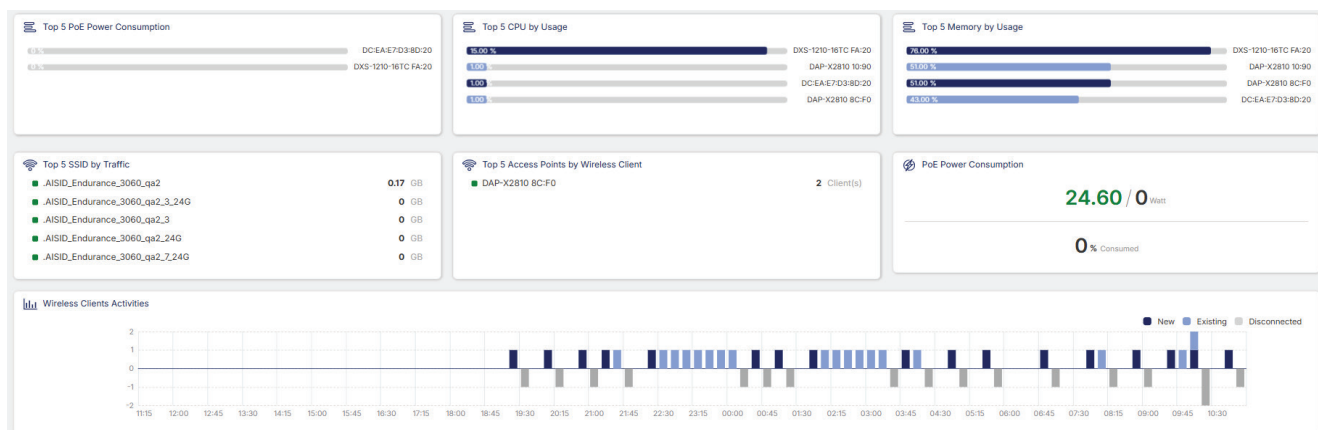
This section displays the top five SSIDs ranked by total traffic usage. It helps administrators identify the most heavily utilized wireless networks and monitor bandwidth distribution across SSIDs.

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.



Nuclias Unity

Dashboard

Clients

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

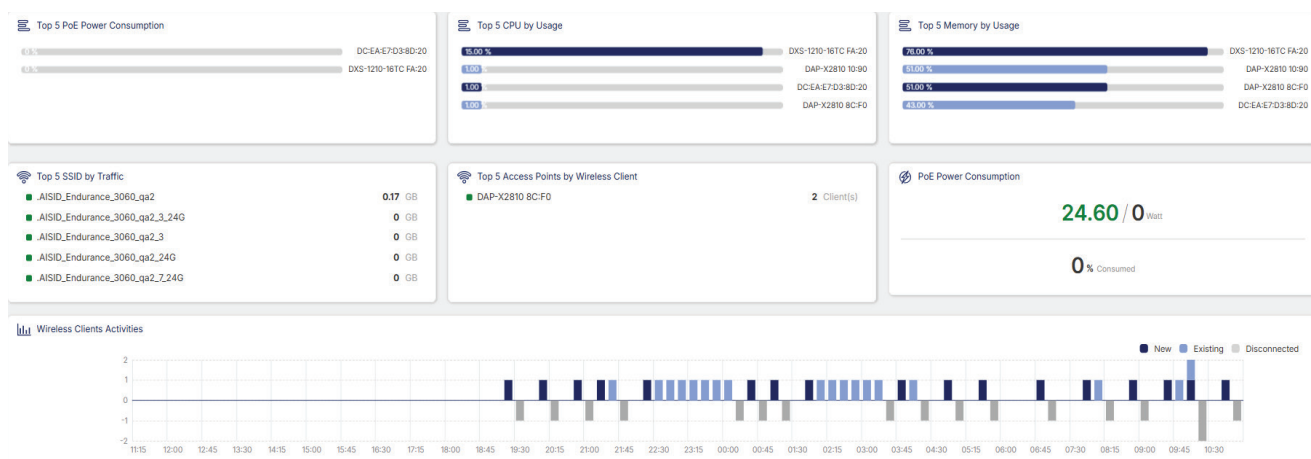
This section shows the top five switches or devices with the highest CPU usage. It helps administrators identify devices under heavy processing load, monitor performance trends, and take proactive measures to prevent network issues.

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

Health AI Insight

Health AI Insight is an AI-powered network analytics feature that continuously monitors network performance, connectivity, security, and infrastructure health. By analyzing operational data in real time, it helps administrators proactively identify potential issues, reduce downtime, and maintain an optimal user experience. AI-driven insights enable faster troubleshooting, improved network reliability, and more efficient network management.

Service Experience

Evaluate end-user connectivity and authentication performance to ensure a seamless network access experience. Health AI Insight analyzes user interactions and service quality to help identify authentication delays and connectivity issues before they affect productivity.

Metrics

- Captive Portal Connection Success Rate
- Captive Portal Authentication Time
- Captive Portal Satisfaction

Security

Detect potential security threats and network anomalies that may compromise the integrity of the network. AI-powered analysis helps identify rogue access point and unusual asset movements that require administrative attention.

Metrics

- Rogue Access Point Detection
- Abnormal Location & Asset Displacement

Roam

Analyze client roaming behavior across access points to ensure uninterrupted wireless connectivity. Roaming insights help administrators optimize wireless deployments and improve user mobility experiences.

Metrics

- Roaming Success Rate

Wireless Coverage

Assess wireless signal quality and coverage across the network. By correlating traffic demand with signal strength, Health AI Insight helps identify coverage gaps and areas requiring optimization.

Metrics

- Wireless Signal Quality

Nuclias Unity

Health AI Insight

Link Integrity

Monitor the health and performance of wired and wireless connections to identify throughput bottlenecks, interference, and link quality issues. These insights help maintain stable connectivity and optimize network performance.

Metrics

- Wireless Congestion Level
- Wired Congestion Level
- Wired Link Degradation
- Wired Cable Quality
- Wireless Channel Interference

Operations

Monitor infrastructure stability and device health to ensure reliable network operations. Health AI Insight tracks operational events and identifies issues that may impact network availability or performance.

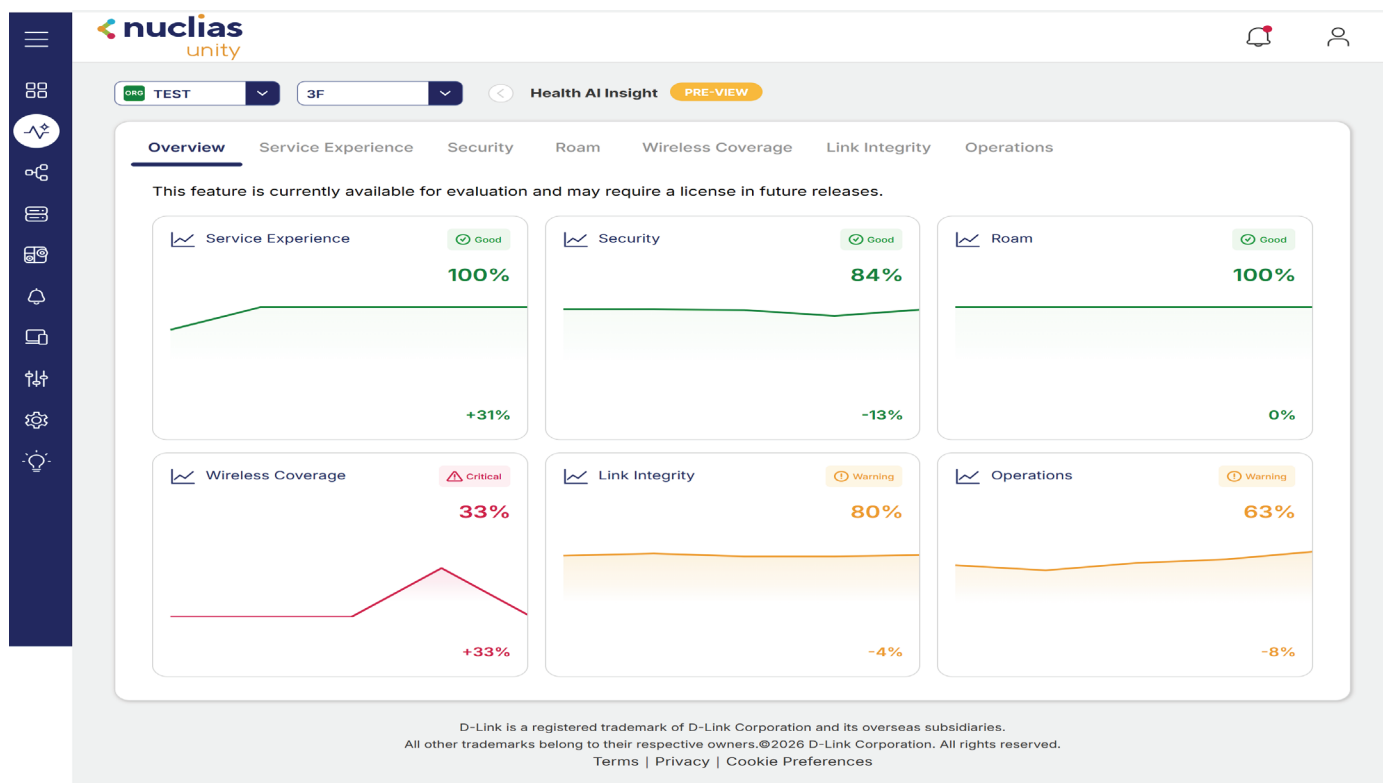
Metrics

- Unexpected Reboot
- PoE Status Detection
- Uplink Stability Status
- System Performance Bottleneck
- Firmware Update Status

Benefits

- Proactively identify network issues before they impact users
- Improve wireless and wired network performance
- Enhance guest and employee connectivity experiences
- Detect security threats and network anomalies
- Reduce troubleshooting time with AI-driven insights
- Improve infrastructure stability and operational efficiency
- Optimize wireless coverage and roaming performance

Health AI Insight enables organizations to transition from reactive troubleshooting to proactive network management, helping ensure a secure, reliable, and high-performing network environment.



Nuclias Unity

Health AI Insight

Service Experince

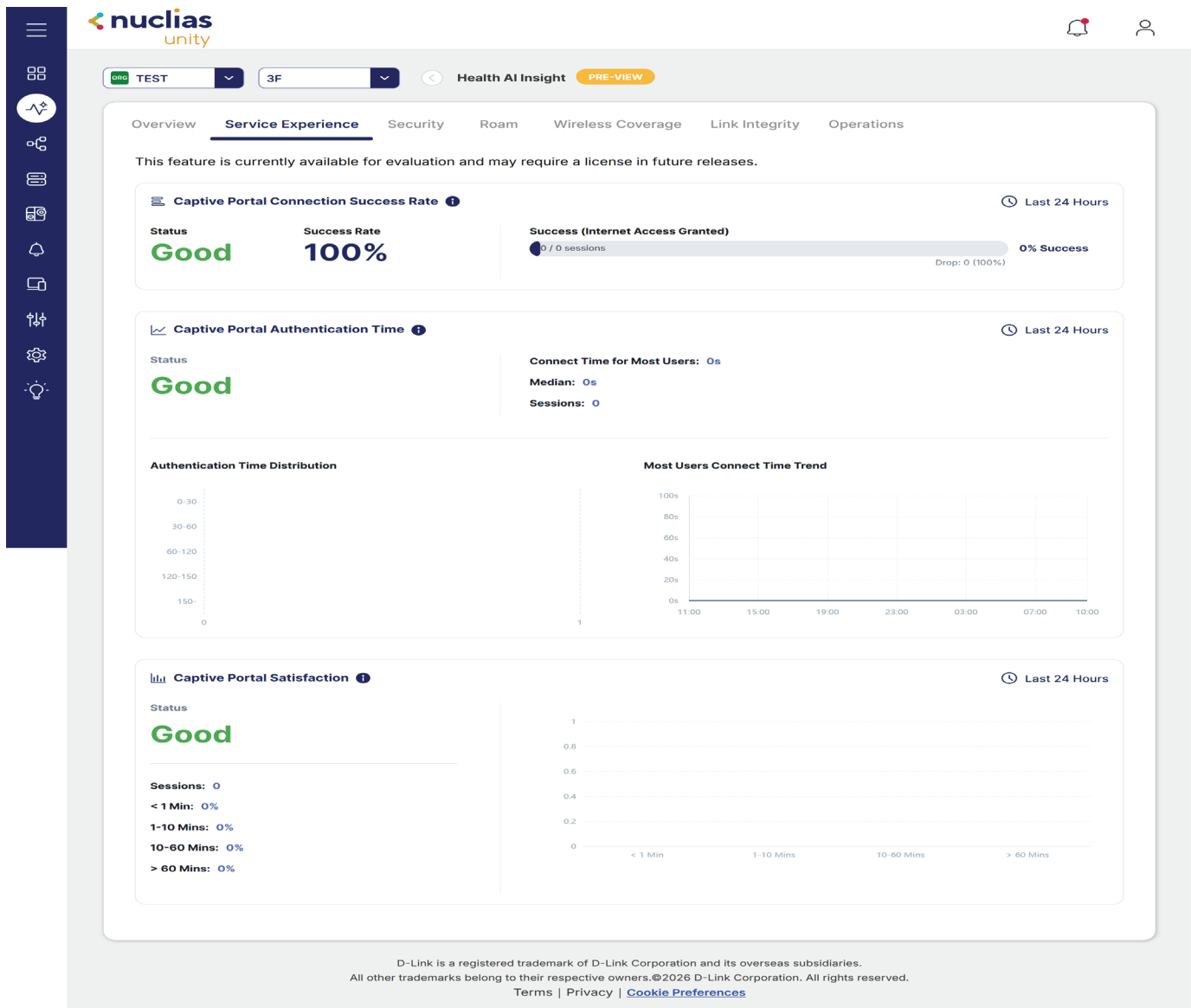
Sevice Experience

The Service Experience section provides visibility into user connectivity and authentication performance, helping administrators evaluate the quality of the network access experience. By monitoring captive portal usage and user behavior, administrators can quickly identify authentication issues, access delays, and trends that may affect user satisfaction.

Available Insights

- **Captive Portal Connection Status** – Displays the current operational status of the captive portal service.
- **Captive Portal Connection Success Rate** – Measures the percentage of users who successfully connect through the captive portal.
- **Authentication Time** – Tracks the average time required for users to complete the authentication process.

These insights enable administrators to optimize guest access services, improve authentication performance, and enhance the overall user experience.



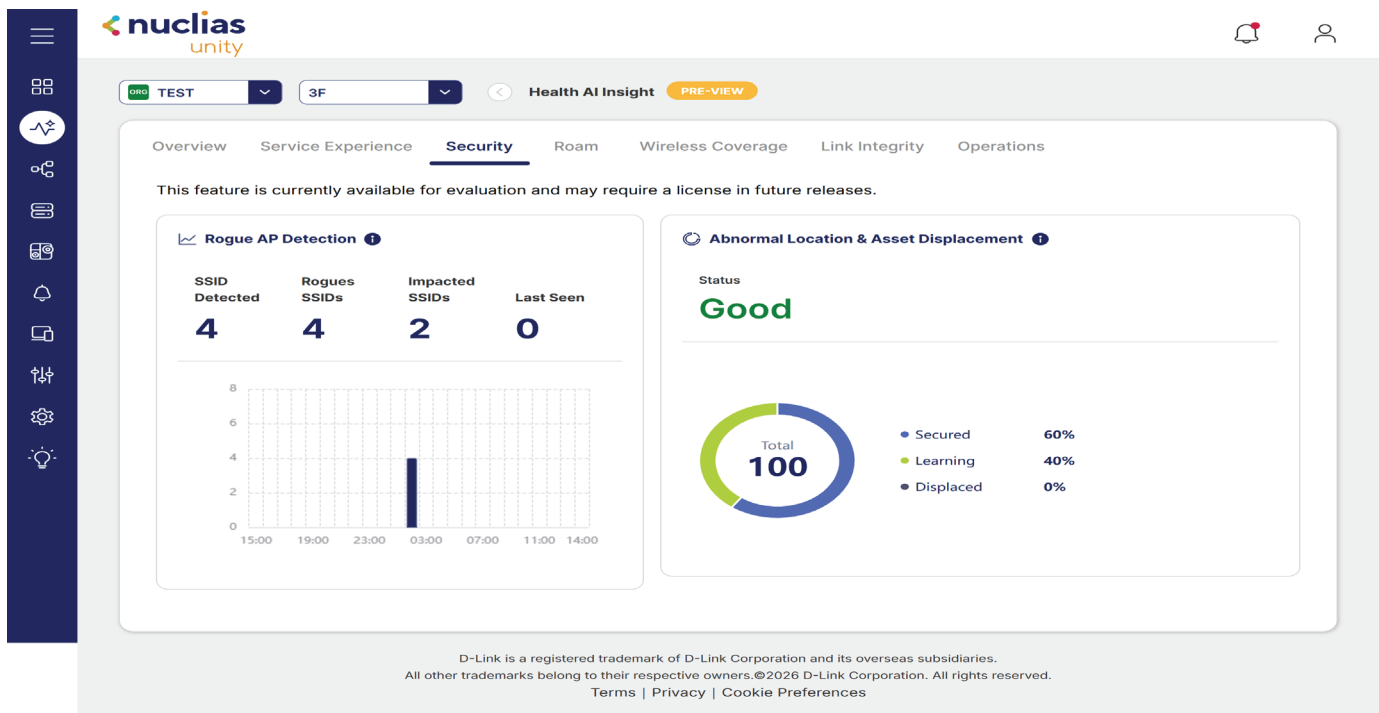
Security

The Security section provides visibility into potential wireless security threats and asset-related anomalies within the network. It helps administrators identify unauthorized access points, detect suspicious wireless activity, and monitor device location changes that may indicate operational or security concerns.

Available Insights

- SSID Detection – Displays all detected wireless networks within the surrounding environment.
- Rogue SSID Detection – Identifies unauthorized or suspicious SSIDs that may pose a security risk.
- Impacted SSIDs – Shows organization SSIDs that may be affected by rogue or unauthorized wireless networks.
- Abnormal Location & Asset Displacement Status – Monitors managed devices and reports unexpected location changes or asset movements that may require investigation.

These security insights help administrators strengthen network protection, identify potential threats, and maintain visibility over network assets and wireless environments.



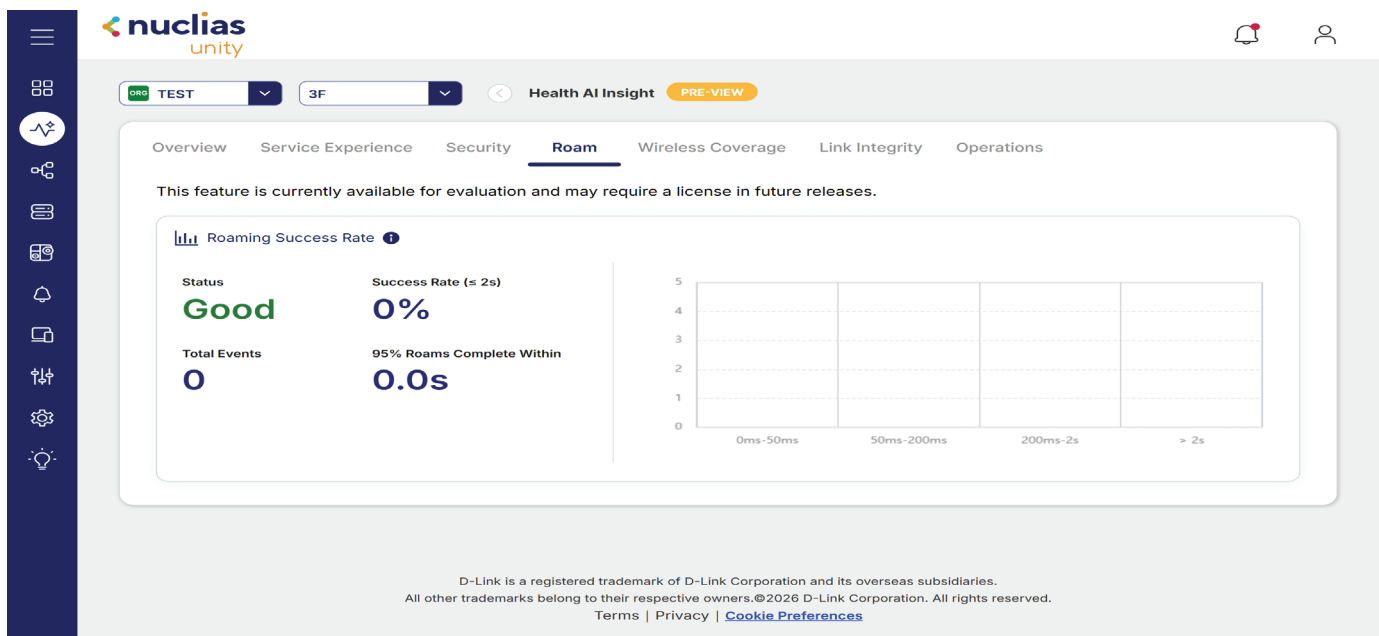
Roam

The Roaming section provides insights into wireless client transitions between access points, helping administrators evaluate roaming performance and maintain a seamless user experience. It measures how successfully clients move between access points without losing connectivity and highlights areas where roaming performance can be improved.

Available Insights

- Roaming Status – Displays the overall health and status of roaming activities across the network.
- Roaming Success Rate – Shows the percentage of successful roaming events between access points.
- Total Roaming Events – Displays the total number of roaming events detected during the selected time period.
- 95% Roam Completion Time – Indicates the time within which 95% of roaming events are successfully completed, helping administrators assess roaming efficiency and user mobility performance.

These insights help optimize wireless coverage, improve client mobility, and ensure a consistent connectivity experience for users moving throughout the network.



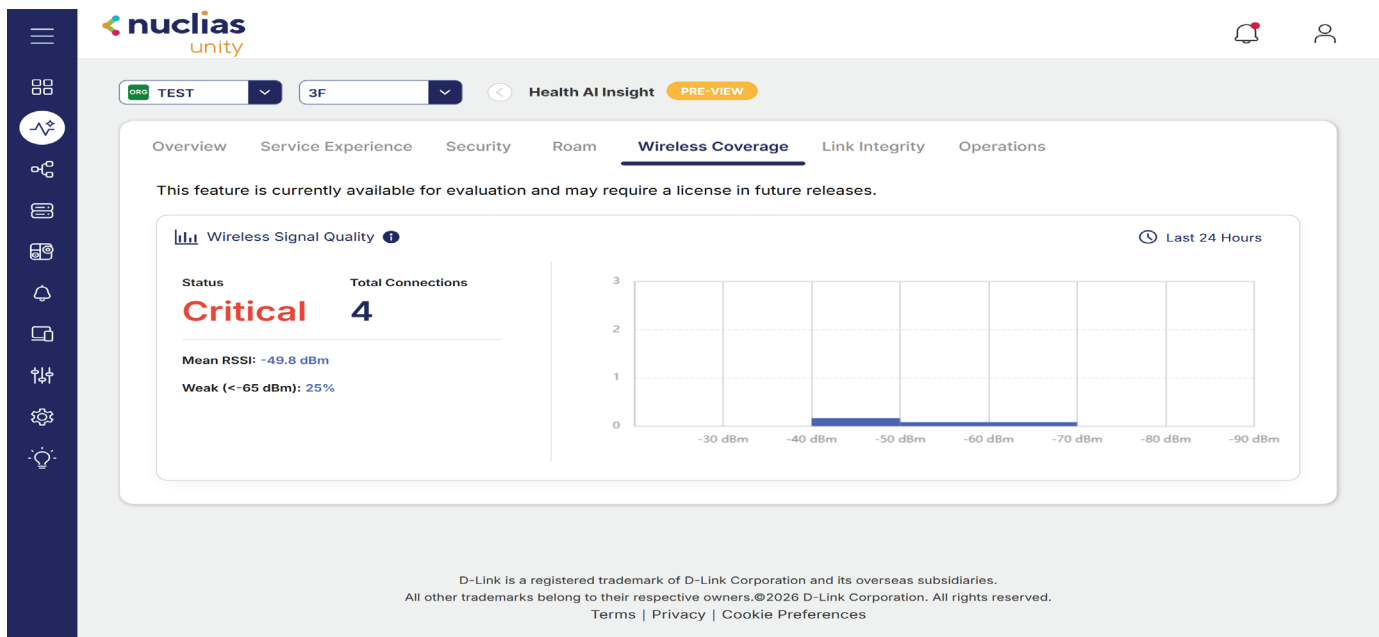
Wireless Coverage

The Wireless Coverage section provides visibility into wireless signal quality across the network, helping administrators assess coverage performance and identify areas that may require optimization. By monitoring signal strength and connection quality, administrators can ensure users receive a reliable and consistent wireless experience.

Available Insights

- **Status** – Displays the overall health and quality status of wireless coverage.
- **Total Connections** – Shows the total number of client connections used to evaluate wireless coverage performance.
- **Mean RSSI** – Displays the average Received Signal Strength Indicator (RSSI) value, providing an overall indication of signal quality across connected clients.
- **Weak Signal Connections (< -65 dBm)** – Identifies the number or percentage of client connections experiencing weak signal strength, helping administrators locate potential coverage gaps or areas with poor wireless performance.

These insights enable administrators to optimize access point placement, improve signal coverage, and maintain a high-quality wireless experience throughout the network.



Nuclias Unity

Health AI Insight

Link Integrity

Link Integrity

The Link Integrity section provides visibility into the health and performance of both wired and wireless network connections. It helps administrators identify congestion, interference, and link quality issues that may impact network performance, user experience, and overall connectivity.

The dashboard includes interactive maps and visual indicators that highlight network conditions and potential problem areas across the deployment.

Available Insights

- **Wireless Congestion Level** – Displays the level of wireless traffic congestion, helping identify areas where excessive client density or channel utilization may affect performance.
- **Wired Congestion Level** – Shows congestion levels on wired network links, enabling administrators to detect bandwidth bottlenecks and overloaded connections.
- **Wired Link Degradation** – Monitors wired link performance and identifies links experiencing reduced quality, instability, or abnormal behavior.
- **Wired Cable Quality** – Evaluates cable health and detects potential cabling issues that may impact network reliability and throughput.
- **Wireless Channel Interference** – Identifies interference sources and channel quality issues that may affect wireless connectivity and performance.

These insights help administrators proactively detect connectivity issues, optimize network performance, and maintain a stable and reliable network infrastructure.

Nuclias Unity

Health AI Insight

Link Integrity



TEST

3F

Health AI Insight

PRE-VIEW

Overview Service Experience Security Room Wireless Coverage **Link Integrity** Operations

This feature is currently available for evaluation and may require a license in future releases.

Wireless Congestion Level ⓘ

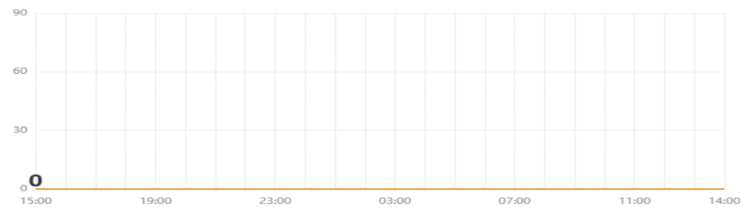
Last 24 Hours

Status
GoodTotal APs
2

Peak Congested: 0

Average Congested: 0

Client Capacity Threshold: 14



Wired Congestion Level ⓘ

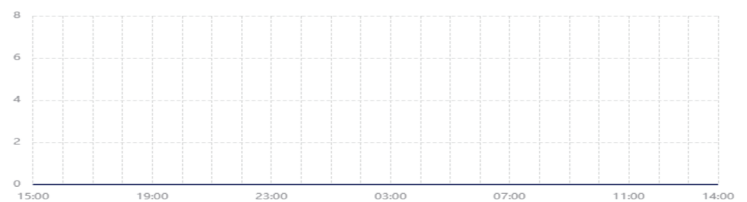
Last 24 Hours

Status
Good

Peak Congested:-

Most Congested:-

Threshold: 6

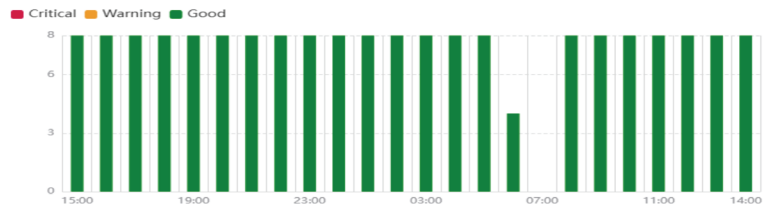


Wired Link Degradation ⓘ

Last 24 Hours

0 Degraded Port(s)

Impacted Switch: 0

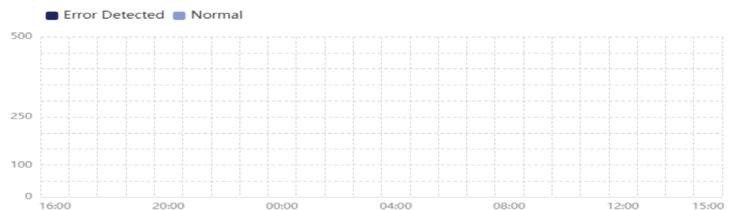


Wired Cable Quality ⓘ

Last 24 Hours

Status
GoodNoisy Port(s)
0
Port(s)

Impacted Switch: 0



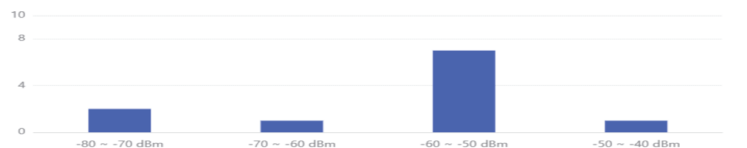
Wireless Channel Interference ⓘ

Last Scan : 2026/6/16 10:41

Status
Critical

Noisy SSIDs: 11

Average Noise: -53 dBm



D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.©2026 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

Operations

The Operations section provides comprehensive visibility into the health, stability, and operational status of network infrastructure. It helps administrators proactively identify device issues, power-related problems, performance bottlenecks, and software maintenance requirements to ensure reliable network operations.

Available Insights

- **Unexpected Reboots** – Detects and reports devices that have experienced unplanned or abnormal reboots, helping administrators identify potential hardware or software issues.
- **PoE Status Detection** – Monitors Power over Ethernet (PoE) status and identifies power-related issues that may affect connected devices.
- **Uplink Stability Status** – Evaluates the reliability and stability of uplink connections, helping detect intermittent connectivity or network disruptions.
- **System Performance Bottlenecks** – Identifies devices or network components experiencing resource constraints or performance issues that may impact network efficiency.
- **Firmware Update Status** – Displays the firmware status of managed devices and highlights devices that require updates to maintain security, stability, and feature compatibility.

These operational insights help administrators maintain network stability, reduce downtime, improve troubleshooting efficiency, and ensure devices operate with optimal performance and up-to-date firmware.

Operations

Page 71

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.

The screenshot displays the Nuclias Unity interface with the Topology view selected. The interface includes a left sidebar with navigation icons, a top header with the Nuclias Unity logo and user profile, and a main content area showing two network topology diagrams.

Top Diagram: Shows two switches connected by a wired line. The switches are labeled **DGS-1250-52XMP FC:78** (00:AD:24:88:FC:78) and **DXS-3410-325Y 98:00** (64:28:43:AC:98:00). The status bar indicates 2 Online and 0 Offline devices. A search bar is present on the right.

Bottom Diagram: Shows a single switch labeled **DGS-1210-10MP 97:20** (40:86:C8:08:97:20). The status bar indicates 0 Online and 1 Offline device. A search bar is present on the right.

Legend: Located at the bottom of each diagram, it defines the symbols used: Online (green dot), Offline (red dot), Dormant (grey dot), Warning (yellow dot), Wired Line (solid blue line), Wired Line High Traffic (thick solid blue line), Wireless Line (dotted blue line), Expand (plus icon), and Collapse (minus icon).

Footer: D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries. All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved. [Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.

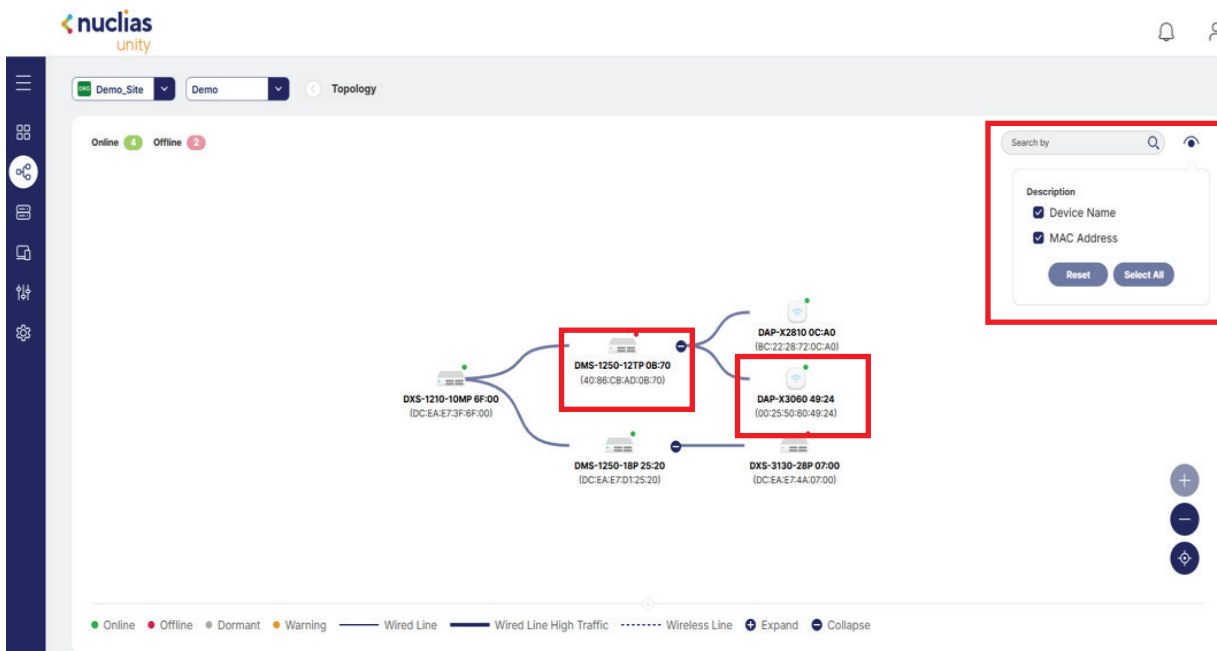
This visual layout helps users understand network structure at a glance, making it easier to monitor device availability, confirm connectivity, and troubleshoot potential network issues.



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:

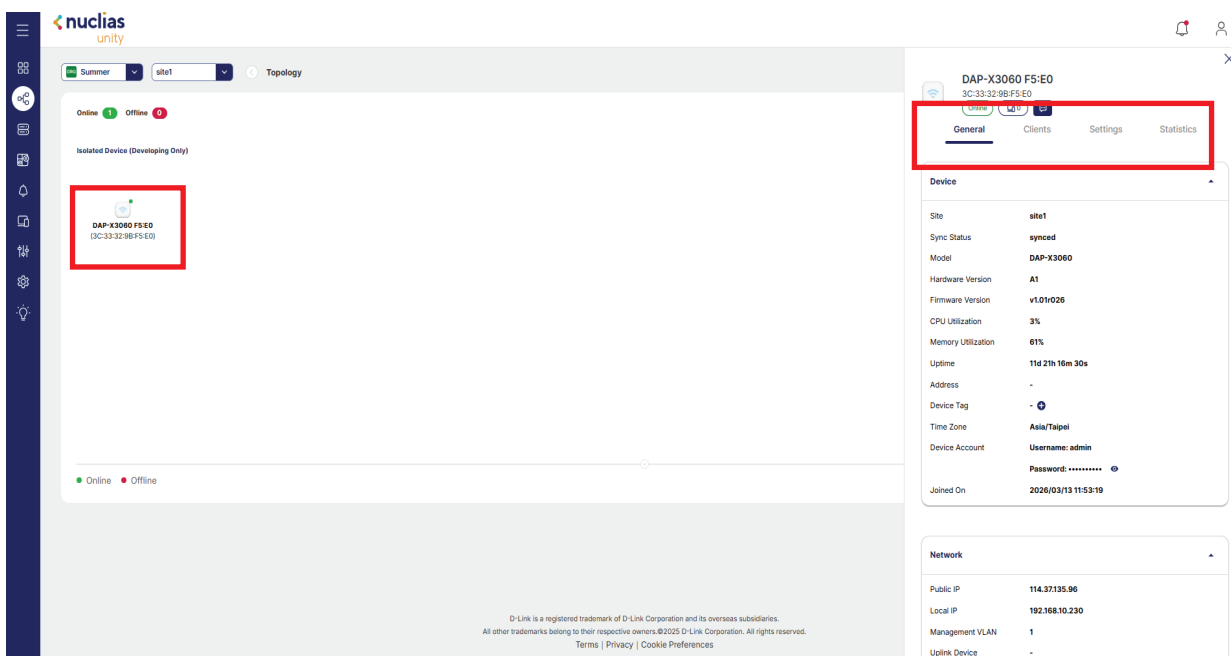
General: View basic device information such as device name, model, IP address, firmware version, and operational status.

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 operational 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.

Nuclias Unity

Devices

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

Devices



Dashboard

Topology

Devices

Wi-Fi Planner Pro

Events

Clients

Firmware Managements

Settings

Support

new tw

Devices

Points 2 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	-
Online	DMS-1250-12TP 9D:EB		new tw	synced	Online	BC:22:28:E7:9D:EB	192.168.1.160	DMS-1250-12TP	-
Online	DMS-3130-30PS 61:00		new tw	synced	Online	BC:22:28:D7:61:00	192.168.1.43	DMS-3130-30PS	-
Online	DAP-E9560 B2:60		new tw	synced	Online	BC:22:28:E7:82:60	192.168.1.126	DAP-E9560	-
Online	DAP-X3060OU A6:30		new tw	synced	Online	BC:22:28:E7:A6:30	192.168.1.42	DAP-X3060OU	-

<<

<

Page 1 of 1

>

>>

Results per page: 20



Dashboard

Topology

Devices

Wi-Fi Planner Pro

Events

Clients

Firmware Managements

Settings

Support

new tw

Devices

Points 2 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
Online	DMS-1250-12TP 9D:EB	-	-	-	-	288.37 MB	1%	43%	-
Online	DMS-3130-30PS 61:00	-	-	-	-	58.92 MB	19%	43%	-
Online	DAP-E9560 B2:60	Auto	Auto	Auto	-	-	1%	36%	DMS-1250-12TP 9D:EB
Online	DAP-X3060OU A6:30	Auto	Auto	-	-	-	5%	59%	DMS-1250-12TP 9D:EB

<<

<

Page 1 of 1

>

>>

Results per page: 20



Dashboard

Topology

Devices

Wi-Fi Planner Pro

Events

Clients

Firmware Managements

Settings

Support

new tw

Devices

Points 2 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
Online	DMS-1250-12TP 9D:EB	288.37 MB	1%	43%	-	-	2026/03/02 14:51:13	-	555
Online	DMS-3130-30PS 61:00	58.92 MB	19%	43%	-	0d 17h 26m 14s	2026/03/02 15:25:30	-	555
Online	DAP-E9560 B2:60	-	1%	36%	DMS-1250-12TP 9D:EB	0d 17h 54m 50s	2026/02/26 11:43:50	-	555
Online	DAP-X3060OU A6:30	-	5%	59%	DMS-1250-12TP 9D:EB	0d 17h 55m 08s	2026/03/02 14:54:21	-	555

<<

<

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.

The screenshot shows the Nuclias Unity interface with the 'Devices' section active. The 'Access Points' tab is highlighted with a red box. Below the tab, a table lists two access points:

Status	Device Name	Site	Sync Status	Connectivity	Last Seen	MAC Address	Local IP	Model Name	Tag
Online	DAP-E9560 B2-60	new tw	synced		Online	BC:22:28:E7:B2:60	192.168.1.126	DAP-E9560	-
Online	DAP-X3060OU A6-30	new tw	synced		Online	BC:22:28:E7:A6:30	192.168.1.142	DAP-X3060OU	-

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.

The screenshot shows the Nuclias Unity interface with the 'Devices' section active. The 'Access Points' tab is highlighted. The table lists two access points, and the first one, 'DAP-E9560 B2-60', is selected. A detailed view for this device is shown on the right, with the 'General' tab selected. The detailed view includes the following information:

- Device: DAP-E9560 B2-60
- MAC Address: BC:22:28:E7:B2:60
- Status: Online
- General tab selected
- Device details table:

Property	Value
Site	new tw
Sync Status	synced
Model	DAP-E9560
Hardware Version	A1
Firmware Version	v1.10B99v999
CPU Utilization	2%
Memory Utilization	36%
PoE Power Usage	-
Uptime	0d 02h 16m 46s
Address	555
Device Tag	-
Time Zone	Asia/Taipei
Device Account	Username: admin
	Password: *****
Joined On	2026/02/26 11:43:50

Nuclias Unity

Devices

Access Points

General

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

Device

Site	new tw
Sync Status	synced
Model	DAP-E9560
Hardware Version	A1
Firmware Version	v1.10B99r999
CPU Utilization	2%
Memory Utilization	36%
PoE Power Usage	-
Uptime	0d 02h 16m 46s
Address	555
Device Tag	- 
Time Zone	Asia/Taipei
Device Account	Username: admin Password: 
Joined On	2026/02/26 11:43:50

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 Account	- 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

Network

Public IP	36.224.15.177
Local IP	192.168.1.126
Management VLAN	1

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.

Wireless SSID

Name	Band	Client
a1.click	5GHz	0
a2	5GHz	0
More...		

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

Radio

2.4GHz

5GHz

6GHz

Channel

Auto

Channel Width

Auto

Mode

Auto

Transmit Power

100

Clients

0

RSSI Threshold

-

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 Threshold	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:

General

Clients

Settings

Statistics

Client

SSID

IP

No data

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.

General

Clients

Settings

Statistics

Device

Device Name

DAP-X3060OU A6:30

Address

555

NetWork

Management VLAN

1

(1~4094)

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.

Radio ▲

2.4GHz

5GHz

Override ☐

Channel

Channel Width

☐ HT20/40 Coexistence

Wireless Mode

Tx Power

RSSI Threshold

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.

Management

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.

StartStop

Remove from Site

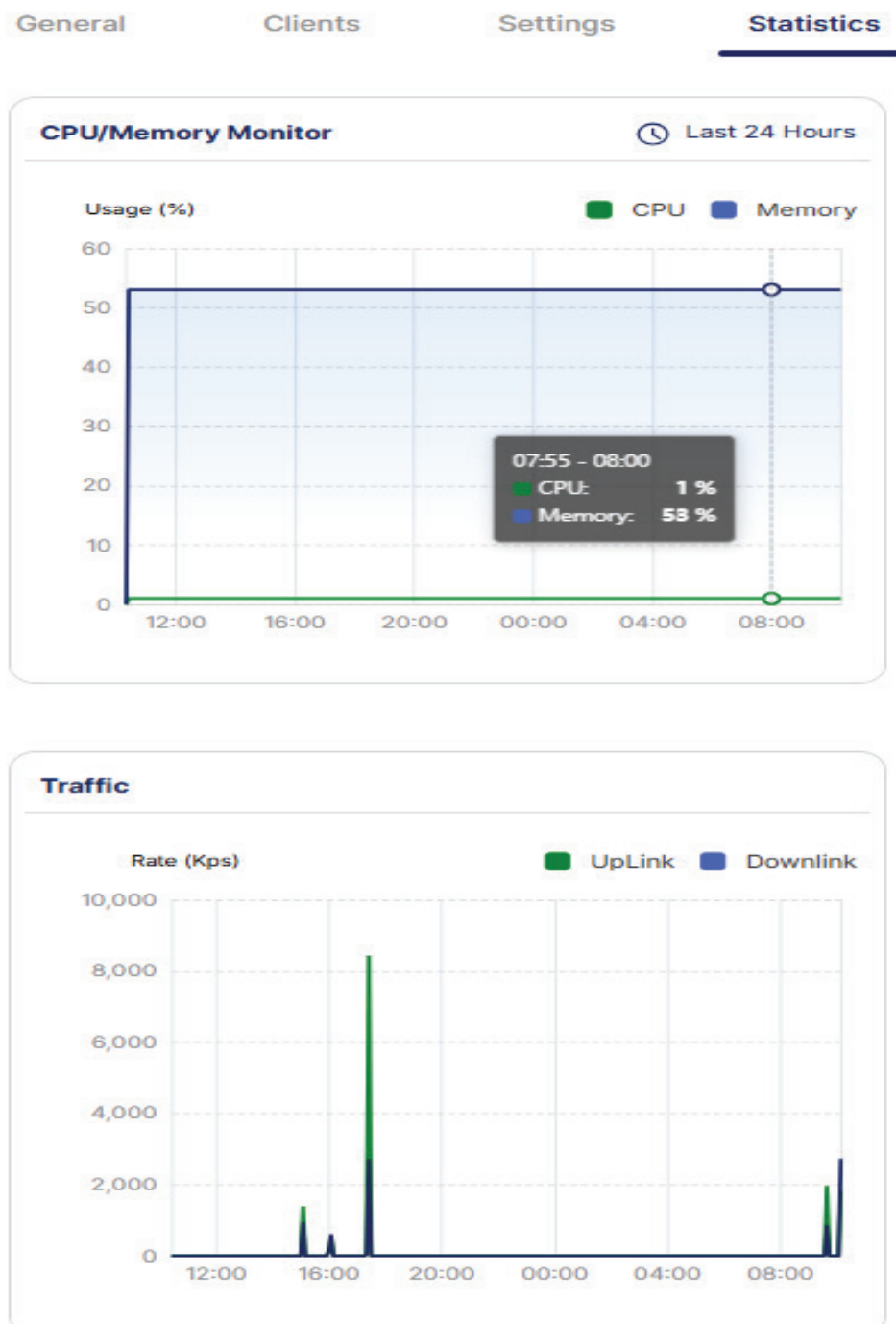
Remove device from current site but remain in the organization.

Remove

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.

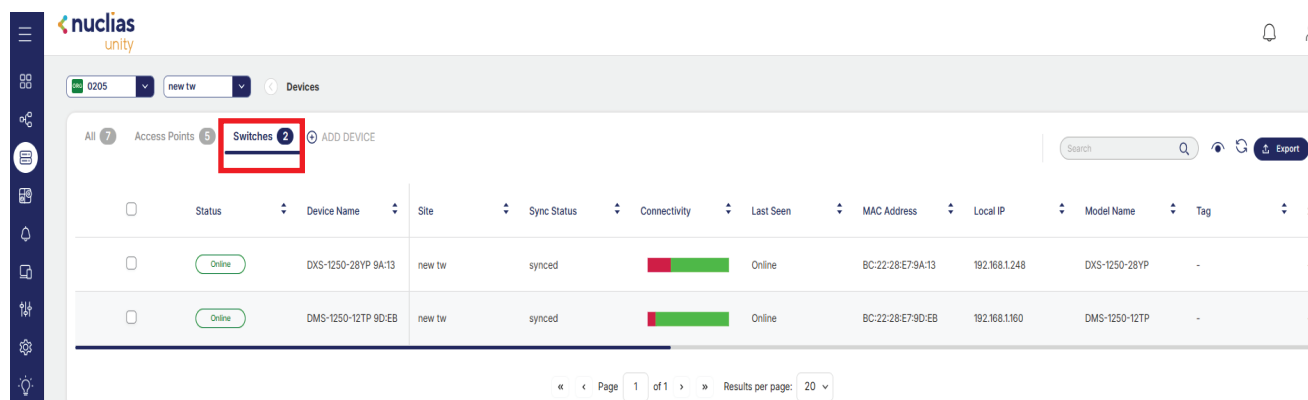


Nuclias Unity

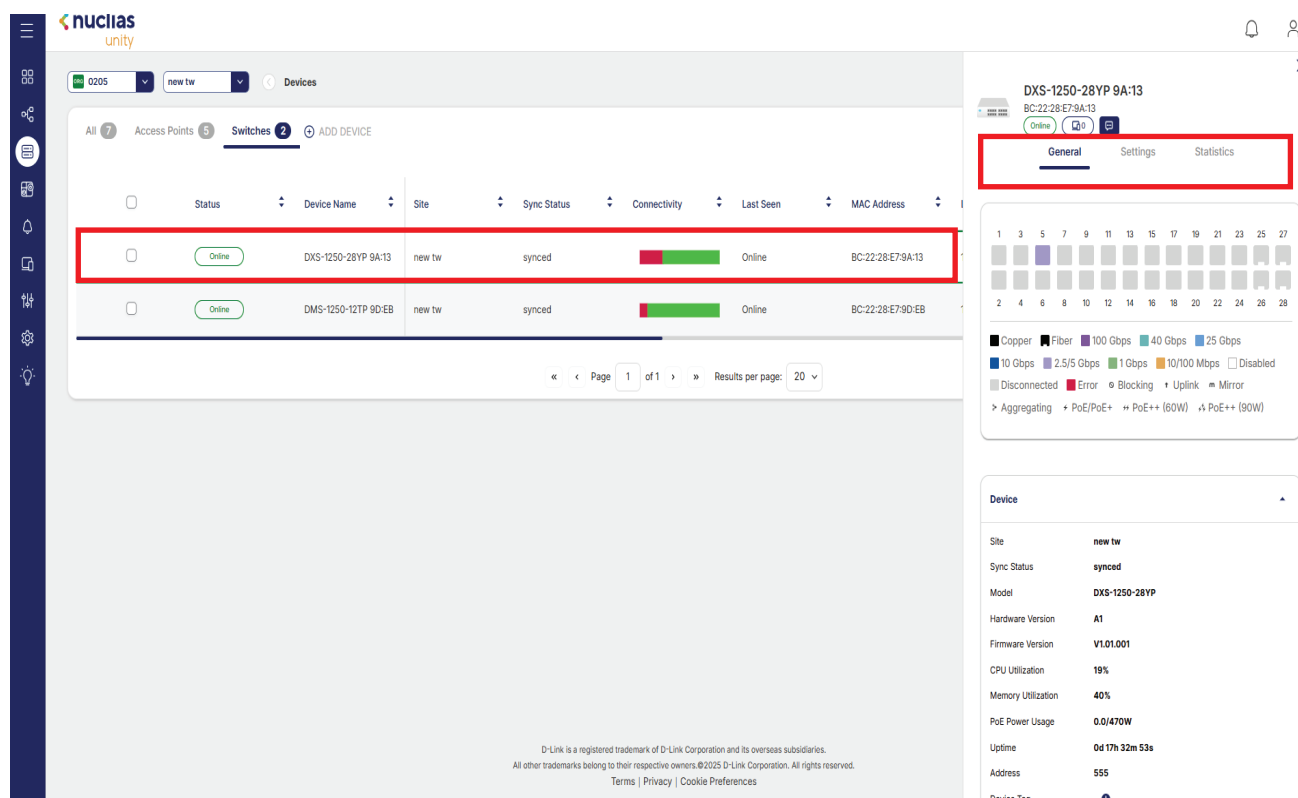
Devices

Switches

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.



Select any Switch from the list to view detailed information and configuration settings for the selected device. It provides comprehensive information under the **General**, **Settings**, and **Statistics** sections, allowing you to monitor the switch status, configure switch settings, manage port configurations, and review performance statistics.



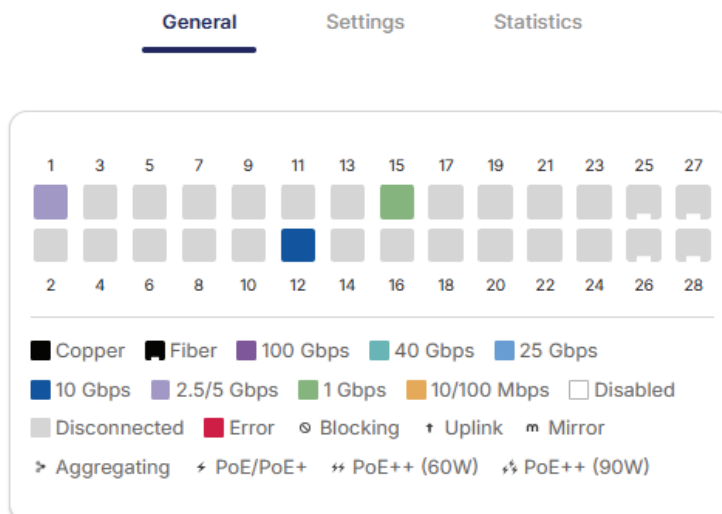
Nuclias Unity

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.

Device

Site	AISID
Sync Status	unsynced
Model	DXS-3130-28
Hardware Version	A1
Firmware Version	V1.31.001
CPU Utilization	20%
Memory Utilization	43%
PoE Power Usage	0.0/0W
Uptime	0d 22h 30m 46s
Address	Stanley_333
Device Tag	- 
Device Account	Username: admin Password: 
Joined On	2026/03/03 12:12:58

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.

Network

Public IP	36.224.7.175
Local IP	192.168.2.15
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Management VLAN	2
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.

General

Settings

Statistics

Device

Device Name

DXS-3130-28 A9:FF

Address

Stanley_333

Management

Remote Access

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

Terminal

Web

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.

Start

Stop

Remove from Site

Remove device from current site but remain in the organization.

Remove

Nuclias Unity

Devices

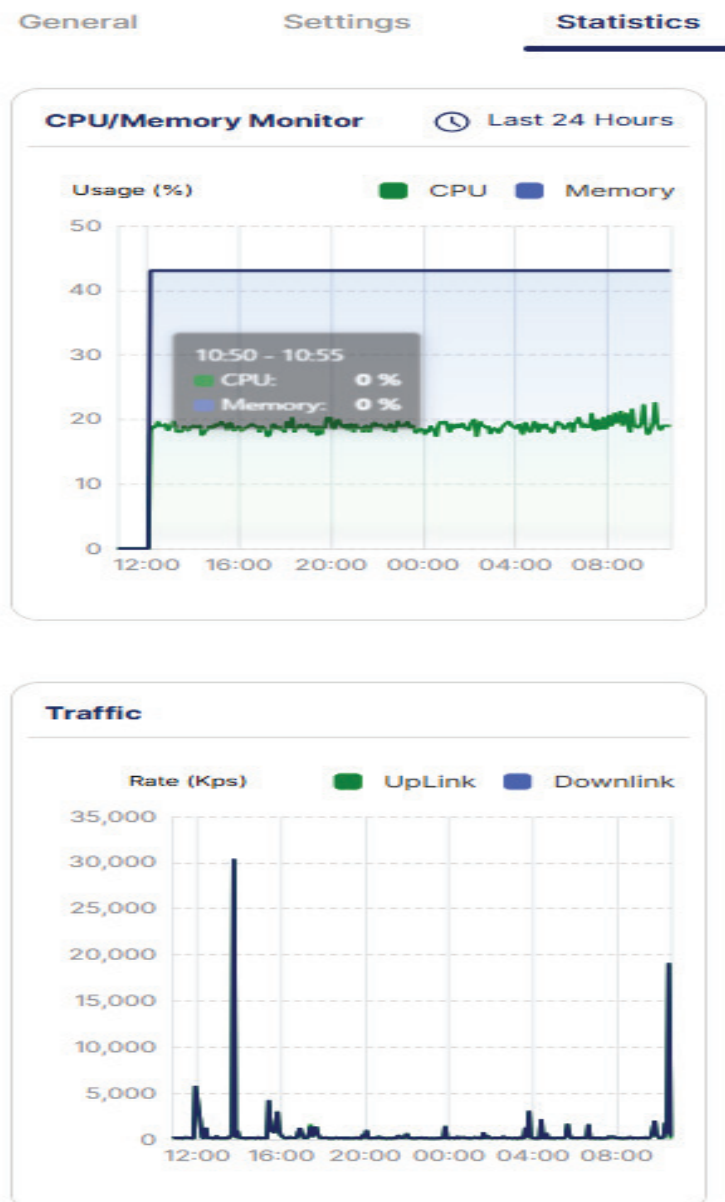
Switches

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

Devices

Routers

From the left-side menu bar, go to **Device** and select **Router**. Here, you can view the total number of connected routers, 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.

The screenshot displays the Nuclias Unity portal interface. On the left is a dark blue sidebar with various icons. The main content area has a header with the Nuclias logo and a navigation bar. Below the navigation bar, there are filters for 'TEST' and '3F', and a 'Devices' section. The 'Routers' tab is highlighted with a red box, showing a count of 1. Below this, there is a search bar and an 'Export' button. A table lists the router details:

Status	Device Name	Site	Sync Status	Connectivity
Online	DBR-600-P 53:27	3F	synced	

At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Results per page: 20'. Below the table, there is a footer with legal information:

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2026 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

Nuclias Unity

Devices

Routers

The Device Status Summary area provides a quick overview of the selected DBR Router, including its current connectivity status and the number of associated Smart APs.

The information displayed is:

- **Device Name** – Shows the name assigned to the selected DBR Router.
- **MAC Address** – Displays the router's MAC address for device identification.
- **Online Status** – Indicates whether the DBR Router is currently online and connected to Nuclias Unity.
- **Smart APs** – Displays the number of Smart APs currently associated with the selected DBR Router.
- **Description** – Provides descriptive information associated with the selected router.

The screenshot displays the Nuclias Unity web interface. The top navigation bar includes the Nuclias Unity logo, a search bar, and a user profile icon. The main content area is divided into two sections. The left section shows a list of devices under the 'Routers' tab, with a table listing the selected router 'DBR-600-P 53:27' as 'Online'. The right section provides a detailed view of the selected router, including its MAC address '48:EE:0C:AF:53:27' and various status metrics.

Site	Device Name	Status
3F	DBR-600-P 53:27	Online

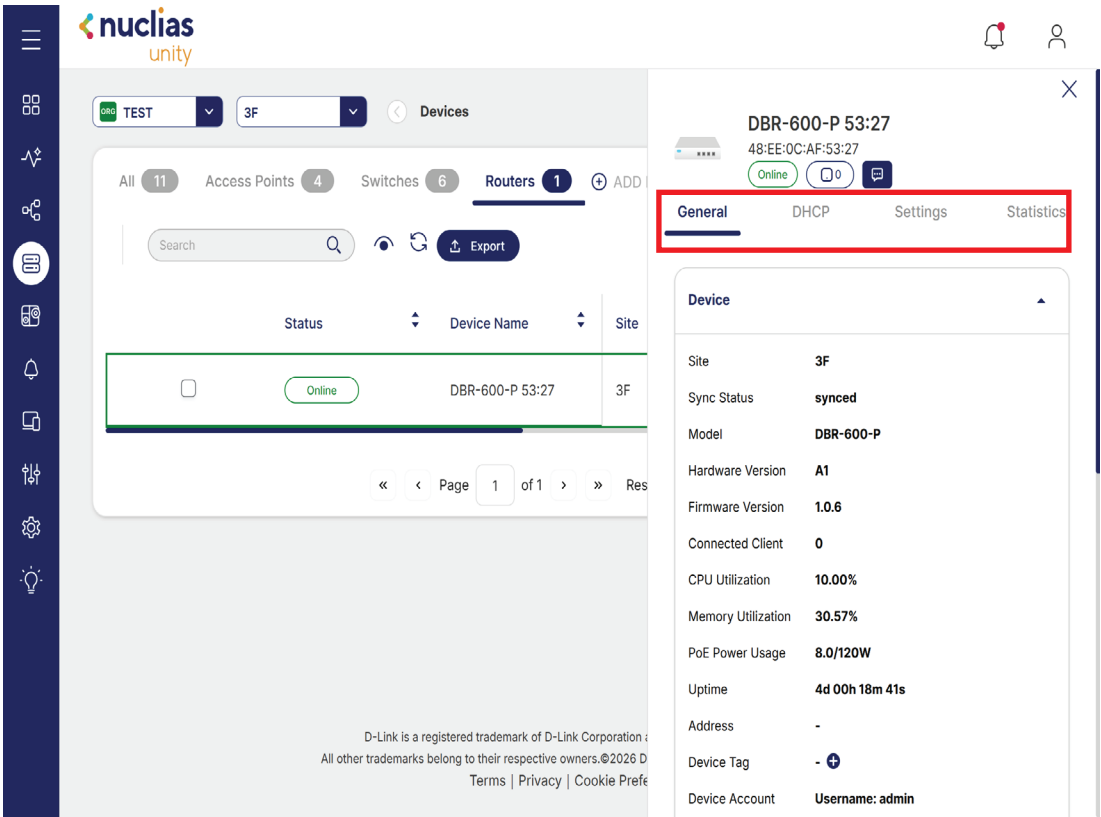
Device	
Site	3F
Sync Status	synced
Model	DBR-600-P
Hardware Version	A1
Firmware Version	1.0.6
Connected Client	0
CPU Utilization	10.00%
Memory Utilization	30.57%
PoE Power Usage	8.0/120W
Uptime	4d 00h 18m 41s
Address	-
Device Tag	-
Device Account	Username: admin

Nuclias Unity

Devices

Routers

Select any Router from the list to view detailed information and configuration settings for the selected device. It provides comprehensive information under the **General, DHCP, Settings, and Statistics** sections, allowing you to monitor router status, configure network settings, manage WAN and LAN interfaces, and review traffic and performance statistics.



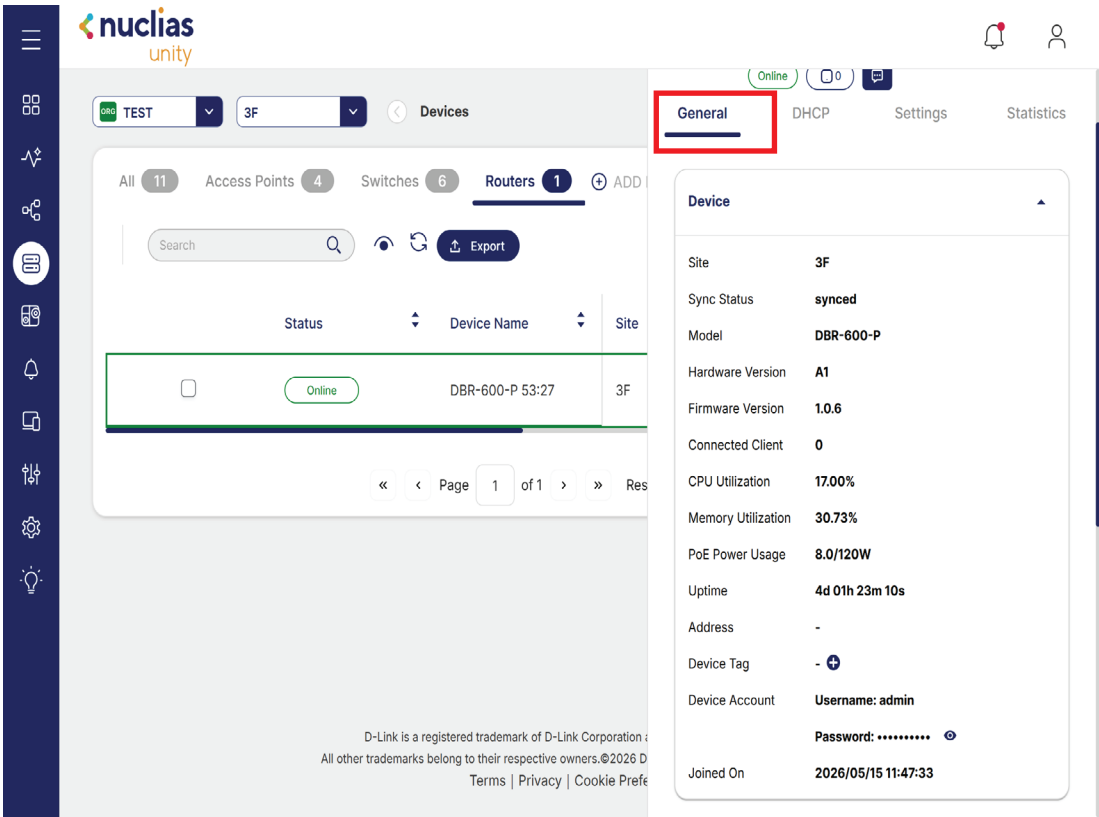
Nuclias Unity

Devices

Routers

General

The General tab provides an overview of the selected DBR Router, including device identification, synchronization status, hardware and firmware information, system resource usage, and management account details.



The General tab displays the following information:

Parameter	Description
Site	Displays the site to which the DBR Router is assigned.
Sync Status	Indicates whether the router configuration is synchronized with Nuclias Unity.
Model	Displays the DBR Router model name.
Hardware Version	Shows the hardware revision of the router.
Firmware Version	Displays the currently installed firmware version.
Connect Client	Shows the number of clients currently connected to the router.
CPU Utilization	Displays the current CPU usage of the router.
Memory Utilization	Shows the current memory usage.
PoE Power Usage	Displays the current Power over Ethernet power consumption, when supported by the device.
Uptime	Shows how long the router has been operating since the last restart.
Address	Displays the configured device address information, when available.
Device Tag	Displays or allows management of tags assigned to the device.
Device Account	Shows the local device management account information.
Joined On	Displays the date and time when the DBR Router was added to Nuclias Unity.

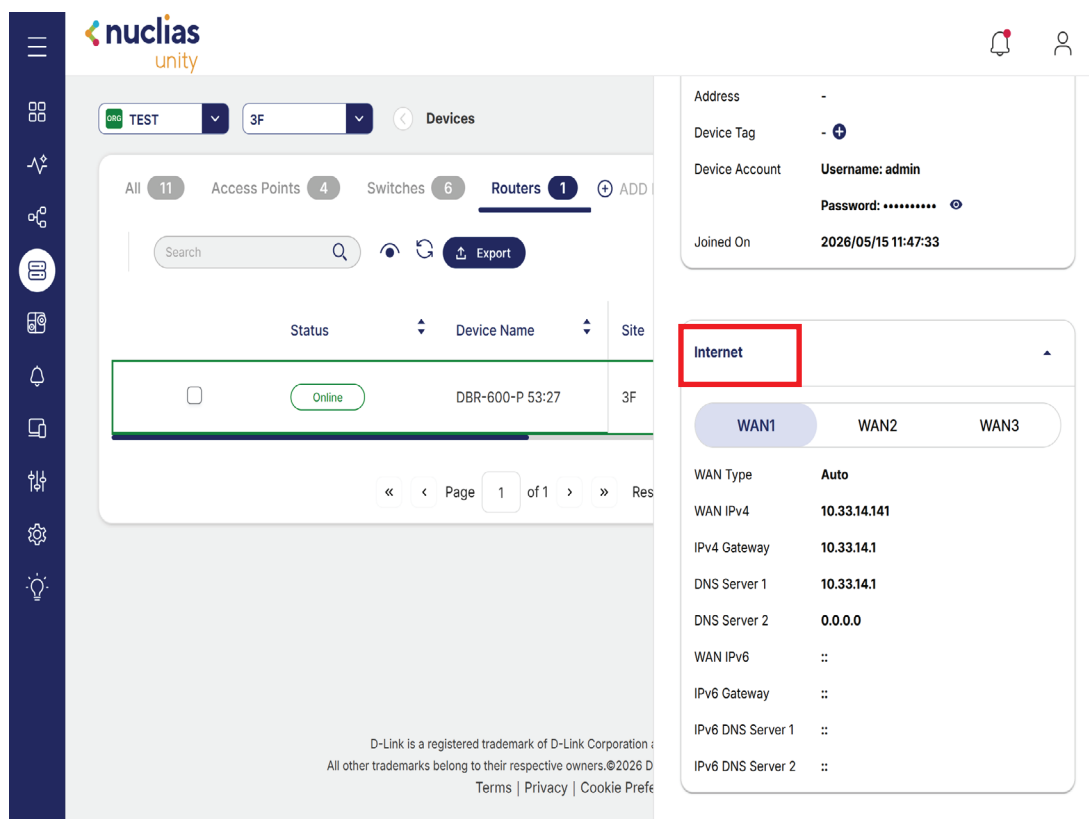
Nuclias Unity

Devices

Routers

General

The General page displays device information, system status, and Internet connection details for **WAN1, WAN2, and WAN3** allowing you to quickly verify the status of each WAN interface.



The WAN section displays the connection status and IP configuration for each WAN interface (WAN1, WAN2, and WAN3). The following information is available:

Parameter	Description
WAN Type	Displays the current WAN connection type.
WAN IPv4	Displays the assigned IPv4 address.
IPv4 Gateway	Displays the default IPv4 gateway address.
DNS Server 1	Displays the primary IPv4 DNS server address.
DNS Server 2	Displays the secondary IPv4 DNS server address.
WAN IPv6	Displays the assigned IPv6 address.
IPv6 Gateway	Displays the default IPv6 gateway address.
IPv6 DNS Server 1	Displays the primary IPv6 DNS server address.
IPv6 DNS Server 2	Displays the secondary IPv6 DNS server address.

Nuclias Unity

Devices

Routers

DHCP

The DHCP tab provides an overview of the DHCP address allocation status for the selected DBR Router. It allows administrators to quickly review the IP address ranges configured for each network interface and monitor the availability of DHCP addresses.

The screenshot shows the Nuclias Unity web interface. On the left is a dark blue sidebar with various icons. The top bar has a 'TEST' dropdown and a '3F' dropdown. The main content area is divided into sections. The 'Routers' section is active, showing a list of routers. One router, 'DBR-600-P 53:27', is selected and highlighted with a green border. To the right of this list, a detailed view of the selected router is shown. The 'DHCP' tab is selected and highlighted with a red box. Below the tab, a table displays the DHCP configuration for the selected router.

#	Interface	IP Range	Lease	Free
1	VLAN1	192.168.10.2 - 192.168.10.252	0	251

The DHCP information includes:

Parameter	Description
Interface	Displays the network interface or VLAN associated with the DHCP address pool.
IP Range	Shows the IP address range available for assignment to client devices.
Lease	Displays the number of IP addresses currently leased to connected client devices.
Free	Shows the number of IP addresses that remain available for new DHCP assignments.

Administrators can use this information to monitor IP address utilization across different VLANs or network segments and identify potential DHCP address pool capacity issues.

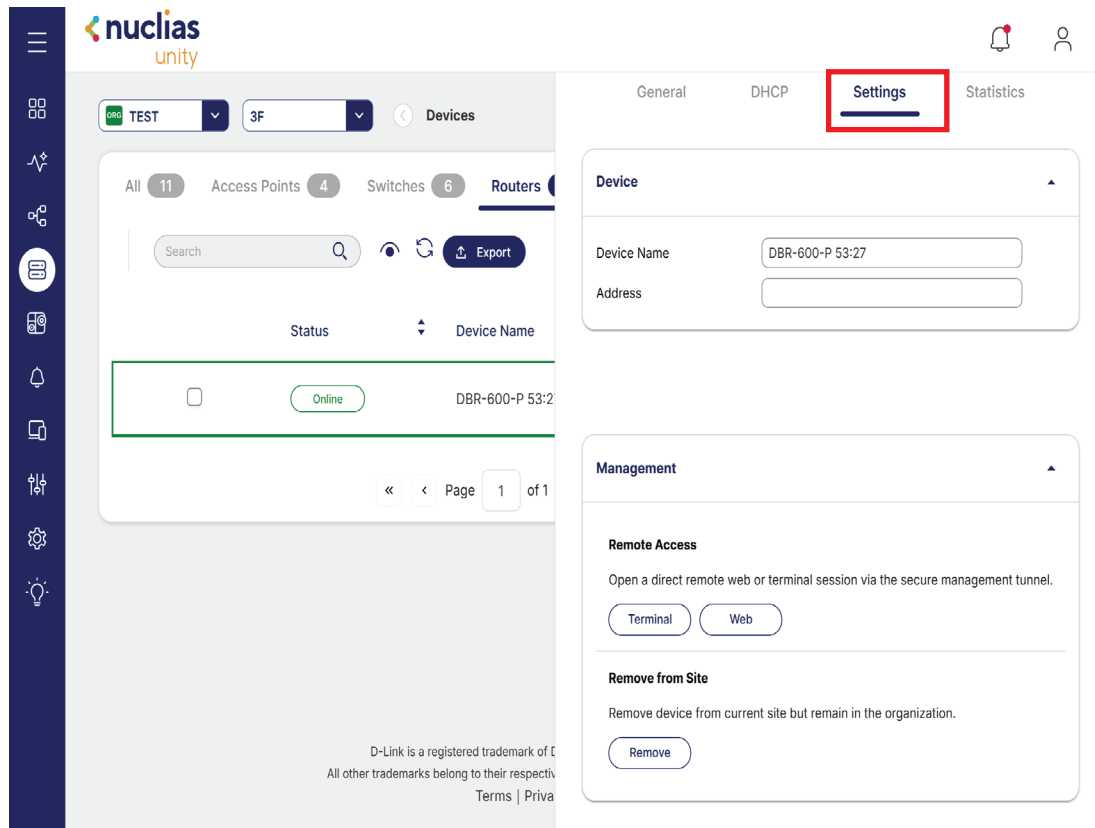
Nuclias Unity

Devices

Routers

Settings

The Settings tab provides device-level configuration and management options for the selected DBR Router. Administrators can review basic device information and access remote management functions through Nuclias Unity.



Device

The Device section displays and allows administrators to manage basic information for the selected DBR Router.

- **Device Name** – Displays the name assigned to the router. The device name can be modified to simplify device identification and management.
- **Address** – Allows administrators to enter location or address information associated with the device.

Management

The Management section provides remote access and device management options.

Administrators can securely access the selected DBR Router through the Nuclias Unity secure management tunnel using one of the following methods:

- **Terminal** – Opens a secure remote terminal session for advanced diagnostics, troubleshooting, and command-line operations.
- **Web** – Opens the DBR Router Web GUI through a secure remote connection for graphical configuration and management.

Remove From Site

Removes the router from the current site while keeping it registered within the organization. The device can be assigned to another site without requiring re-registration.

Remove – Removes the router from the site. The device will no longer be managed by Nuclias Unity unless it is added to the site again.

Nuclias Unity

Devices

Routers

Statistics

The Statistics tab provides performance and traffic monitoring information for the selected DBR Router. It allows administrators to review router resource utilization and network usage trends over a selected time.

The screenshot displays the Nuclias Unity portal interface. On the left, a dark blue sidebar contains navigation icons. The main content area is divided into two sections. The top section shows the 'Devices' tab with a list of devices, including 'DBR-600-P 53:27' which is 'Online'. The bottom section shows the 'Statistics' tab for the selected router. The 'Statistics' tab includes a 'CPU/Memory Monitor' graph showing usage (%) over the last 24 hours, with a tooltip indicating CPU usage at 18% and Memory usage at 28.95% for the period 04:45 - 04:50. Below this is an 'Internet Usage' graph showing the rate (MB) over the last 24 hours, with a tooltip indicating Tx rate at 0.8 MB and Rx rate at 0.4 MB for the period 04:45 - 04:50.

DBR-600-P 53:27
48:EE:0C:AF:53:27
Online 0 0

General DHCP Settings **Statistics**

CPU/Memory Monitor Last 24 Hours

Usage (%) CPU Memory

04:45 - 04:50
CPU: 18 %
Memory: 28.95 %

Internet Usage Interface Type: WAN1 Last 24 Hours

Rate (MB) Tx Rx

04:45 - 04:50
Tx: 0.8 MB
Rx: 0.4 MB

The Statistics page includes the following information:

CPU/Memory Monitor

The CPU/Memory Monitor displays historical CPU and memory utilization for the selected DBR Router.

- **CPU** – Shows the router CPU usage as a percentage over time.
- **Memory** – Shows the router memory utilization as a percentage over time.
- **Time Range** – Displays performance data for the selected monitoring period, such as the last 24 hours.

Administrators can use this information to identify unusual resource consumption, monitor system load, and evaluate overall router performance.

Internet Usage

The Internet Usage section displays network traffic statistics for the selected WAN interface.

- **Interface Type** – Allows administrators to select the WAN interface to be monitored.
- **Tx** – Shows transmitted traffic from the router.
- **Rx** – Shows received traffic to the router.
- **Time Range** – Displays traffic usage over the selected monitoring period.

This information helps administrators review Internet traffic trends, compare transmitted and received traffic, and identify unusual bandwidth usage.

Router Configuration

Nuclias Unity provides two secure methods for accessing and managing the DBR Router remotely. Administrators can choose the appropriate method based on the required configuration or troubleshooting task.

Secure Access to the Router Web GUI

Administrators can securely access the DBR Router Web GUI through Nuclias Unity without directly exposing the router management interface to the public Internet.

The Router Web GUI provides a graphical interface for viewing device status and managing router settings, such as network, security, VPN, service, and system configuration.

This method is recommended for general configuration and day-to-day router management.

Secure Access to the Router Terminal

Administrators can also securely access the DBR Router terminal through Nuclias Unity.

The Router Terminal provides a command-line interface for advanced configuration, diagnostics, troubleshooting, and system-level operations.

This method is recommended for experienced administrators who require command-line access for advanced maintenance and troubleshooting tasks.

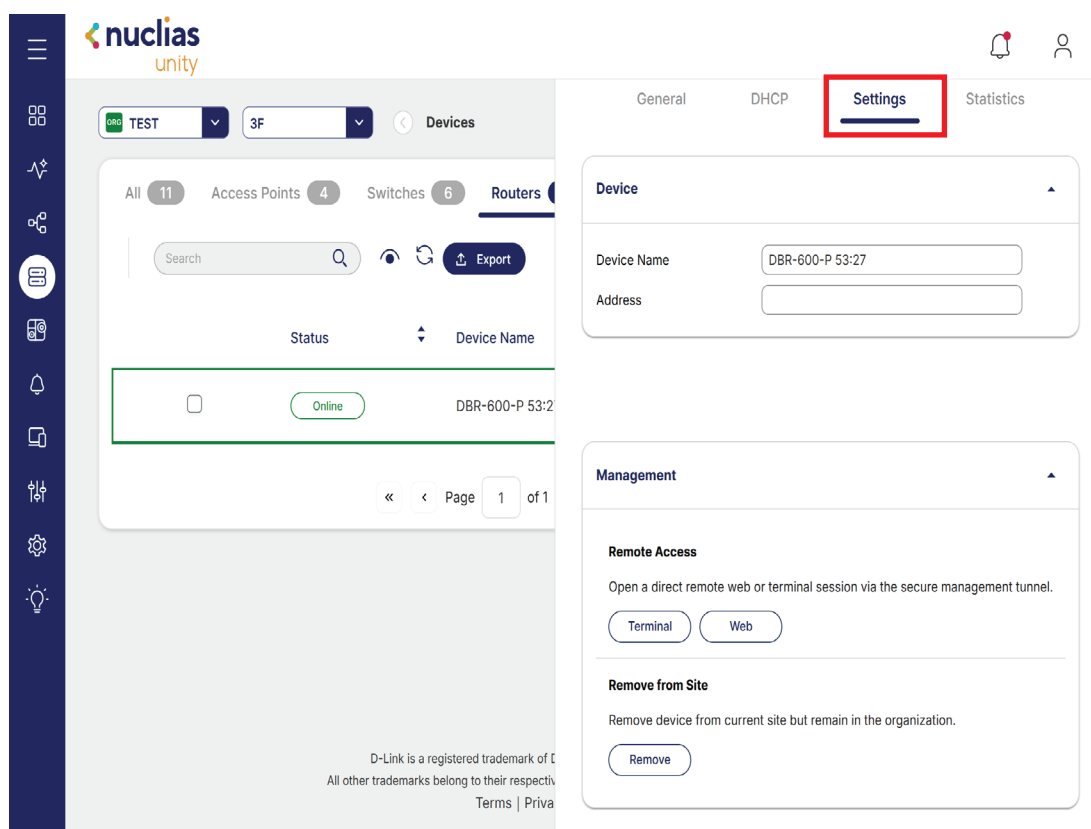
Accessing Remote Router Management

To access the DBR Router remotely through Nuclias Unity, follow the path below:

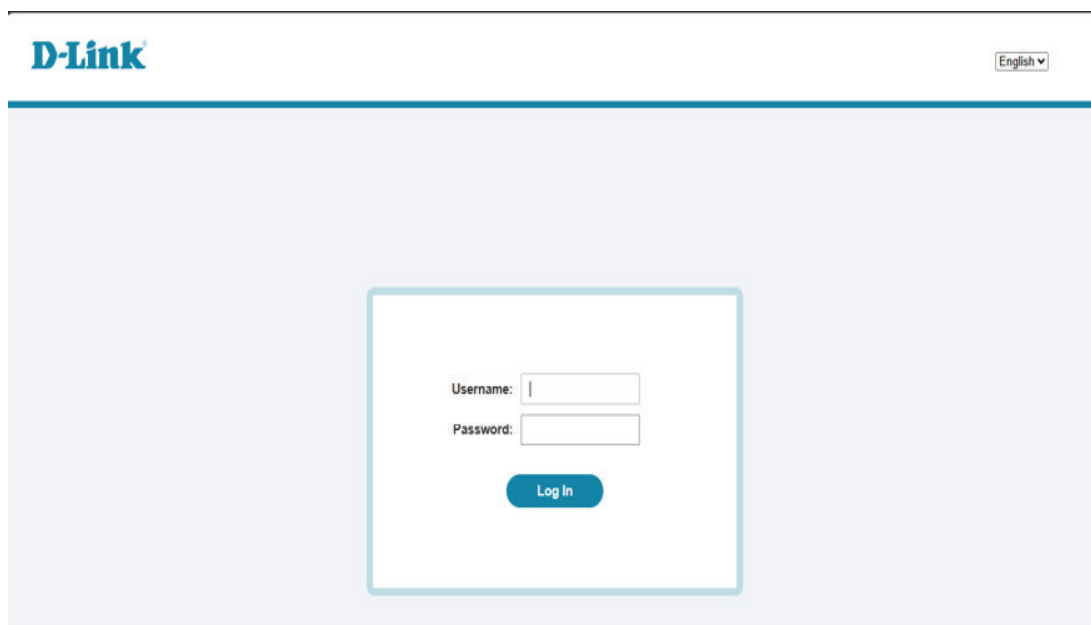
Devices > Select the DBR Router > Settings > Management > Remote Access

Under Remote Access, select one of the following options:

- **Terminal** – Opens a secure remote terminal session to the DBR Router.
- **Web** – Opens the DBR Router Web GUI through a secure management tunnel.



Click Web to open the DBR Router Web GUI, where you can access advanced configuration and management settings for the device.



Click Terminal to open a secure remote terminal session to the DBR Router for command-line configuration, troubleshooting, and management.



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:

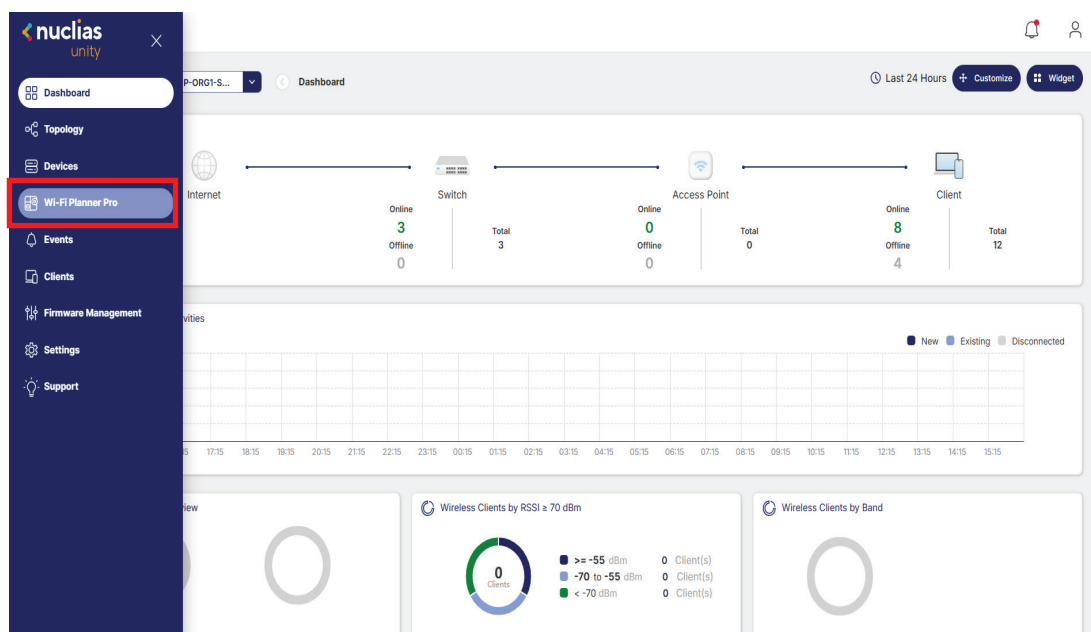
- Import or draw a floor plan
- Define walls, rooms, and obstacles
- Set coverage requirements
- Place APs on the map
- Simulate signal coverage
- Estimate the number of APs required
- Improve AP placement for better performance

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

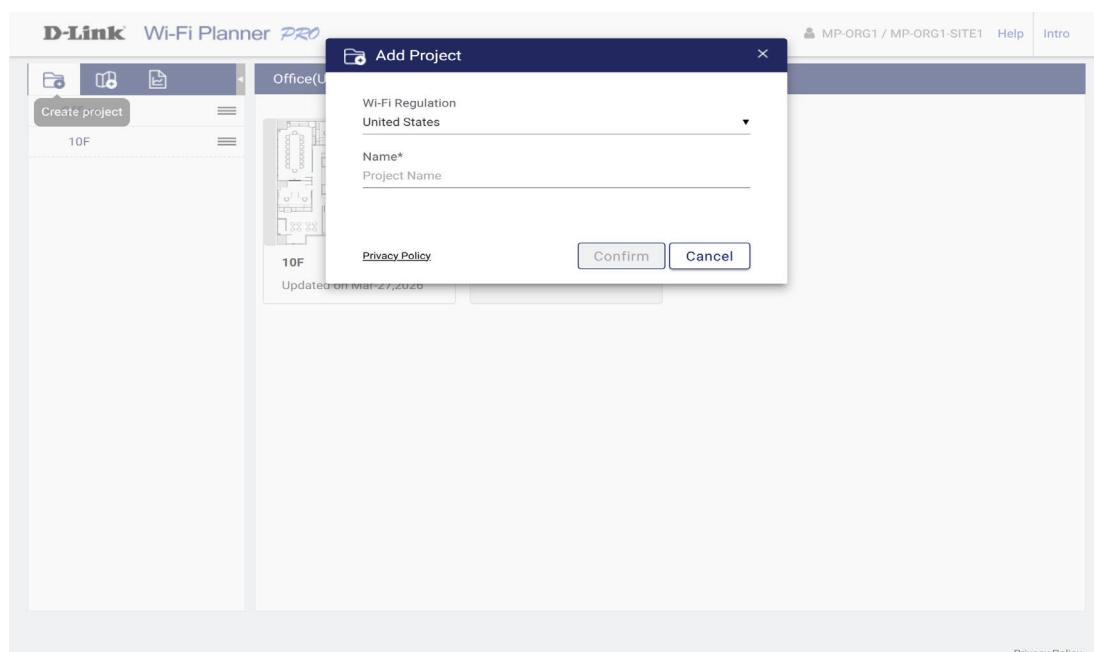
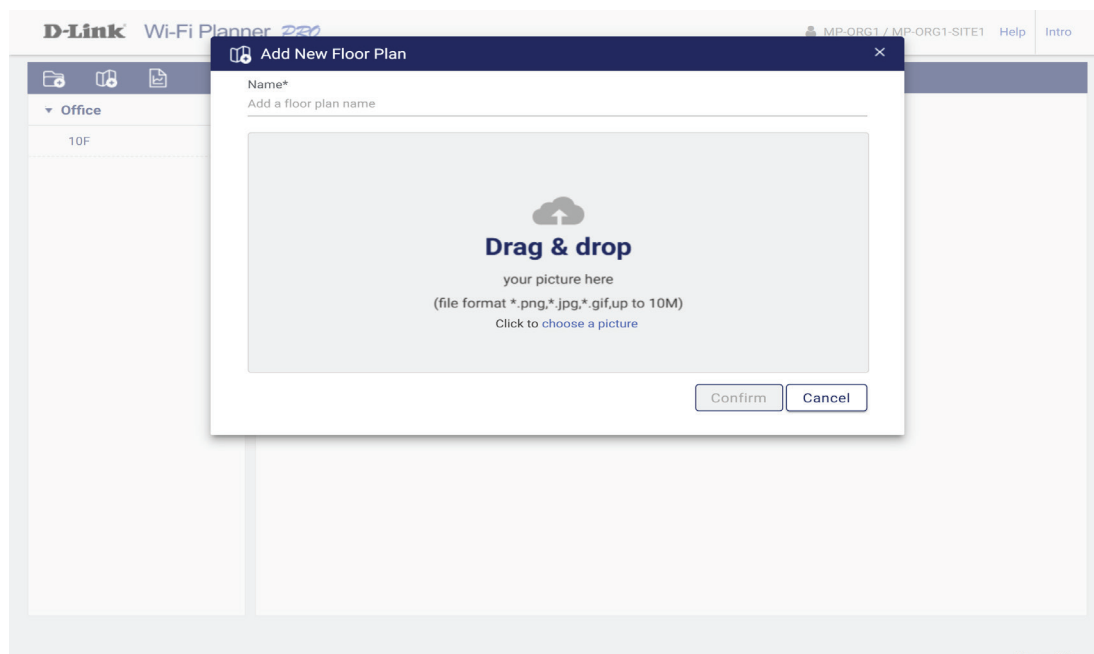
Dashboard

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.



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.

D-Link Wi-Fi Planner *PRO*

MP-ORG1 / MP-ORG1-SITE1 [Help](#) [Intro](#)

Office(United States)

Office / 10F

0 2 4 6m

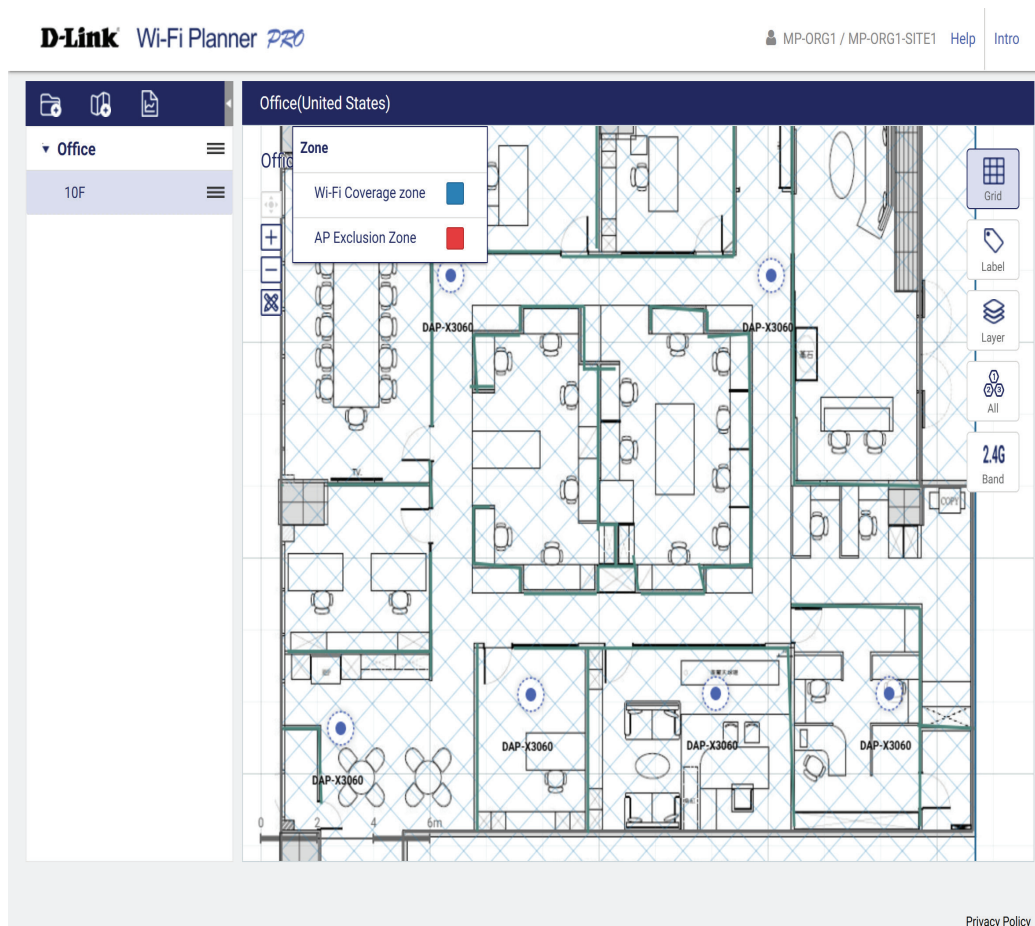
10樓辦公室平面配置圖

Grid
Label
Layer
All
2.4G
Band

[Privacy Policy](#)

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.



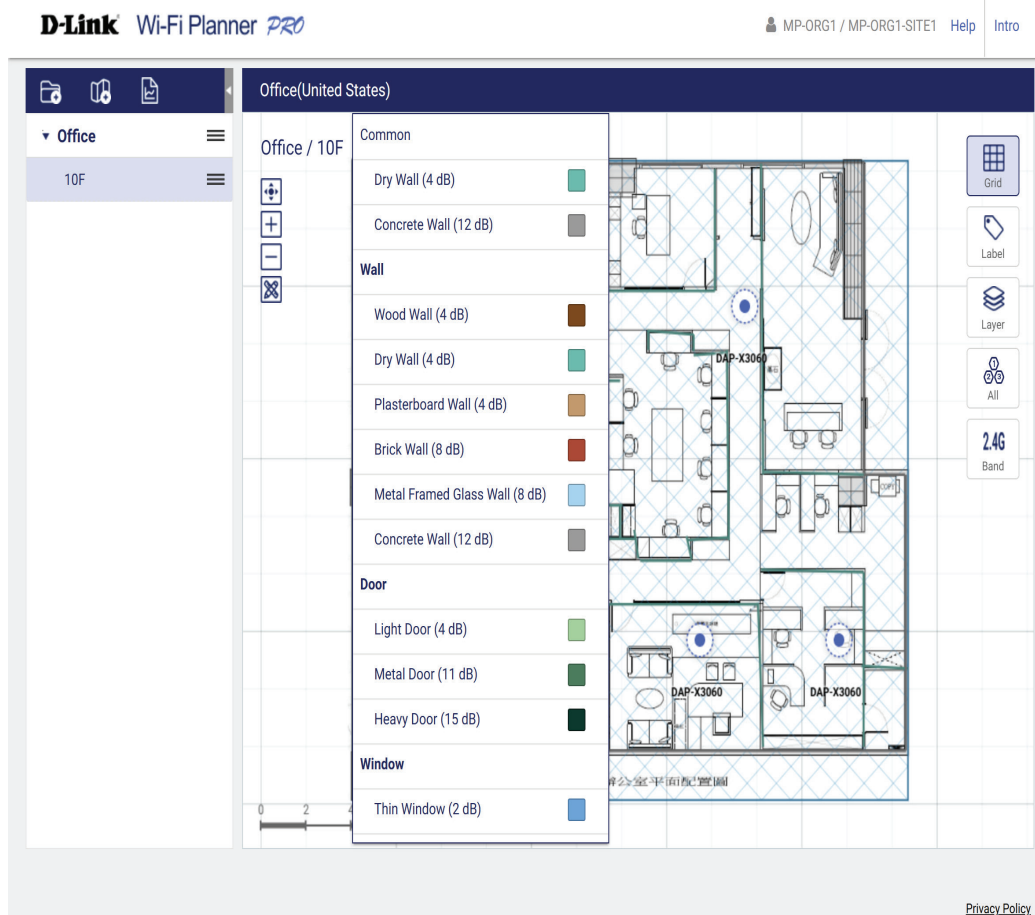
Nuclias Unity

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.

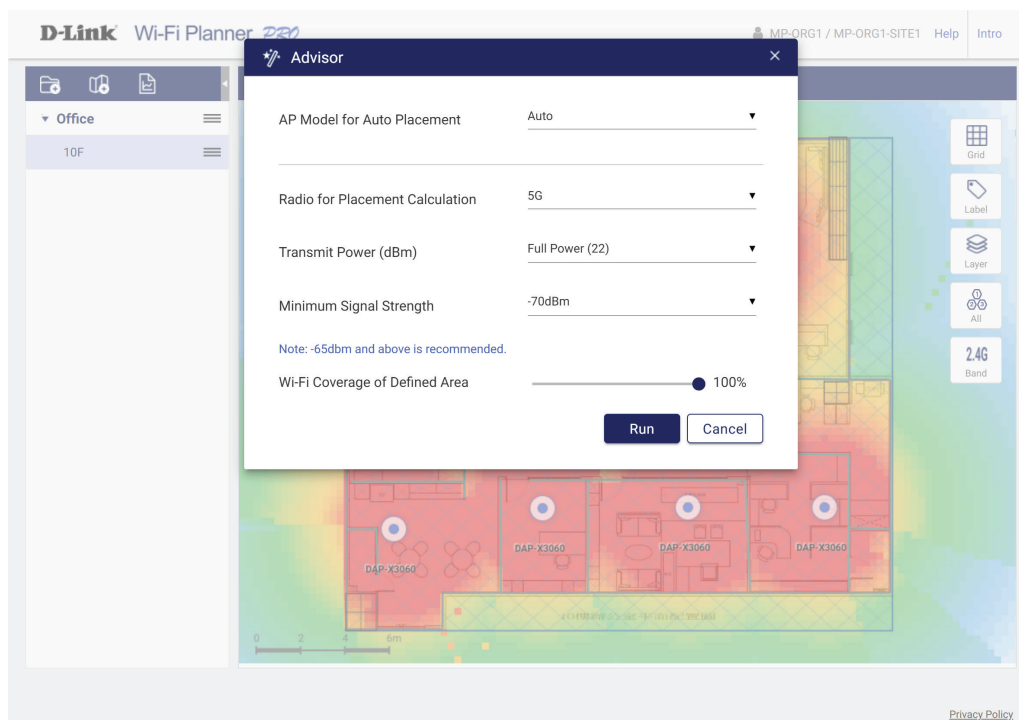


Nuclias Unity Wi-Fi Planner Pro

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

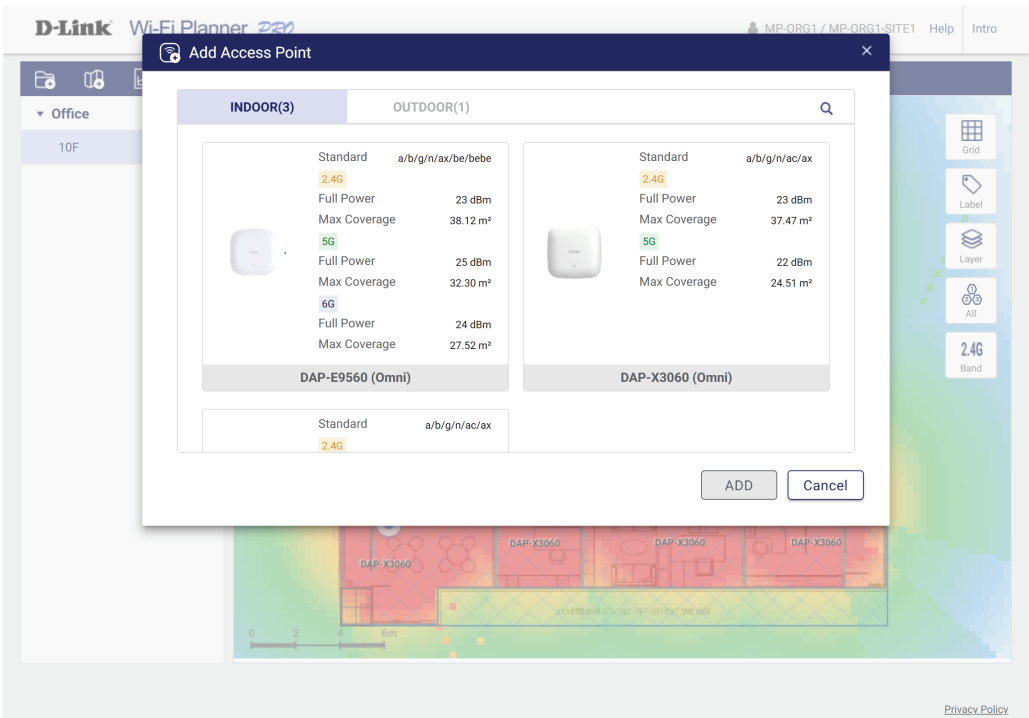
Reviewing Deployment and Heat Map

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.



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

D-Link Wi-Fi Planner PRO MP-ORG1 / MP-ORG1-SITE1 Help Intro

DOWNLOAD REPORT Overview Save as PDF

Overview

Project Overview

Name	Number of Floor Plan	Number of AP	AP Model Details
Office	1	6	DAP-X3060*6

Floor Plan Overview

Name	Floor Plan	Coverage Area	Number of AP
10F		Coverage area: 548m²	Indoor: 6 AP Model Details: DAP-X3060*6

Total Floor Plan: 1
Total APs: 6(Indoor)

[Privacy Policy](#)

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.

The screenshot shows the Nuclias Unity Events dashboard. At the top, there are tabs for 'All' (selected), 'Access Points', 'Switches', and 'System Audit'. Below the tabs is a search bar and a 'Report' button. The main table has columns for Severity, Time, Site, Event Type, Device Type, Device Name, Mac Address, Description, Client Name, and Client MAC Address. The table contains 15 rows of events, all with a severity of 'Info' and occurring at the 'AISD' site. The events are related to client IP changes, associations, and disassociations for an Access Point (Yulin_DAP-X3060) and a client device (D4E8BA9F-D45A).

Severity	Time	Site	Event Type	Device Type	Device Name	Mac Address	Description	Client Name	Client MAC Address
Info	Today, 6:58:39 AM	AISD	Client IP change	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:37 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:35 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:28 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:26 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:26 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:58:24 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:57 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:57 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:54 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:53 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:45 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:45 AM	AISD	Client Disassociation	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A
Info	Today, 6:57:42 AM	AISD	Client Association	Access Point	Yulin_DAP-X3060	3C-33-32-98-F6-F0	Client D4E8BA9F-D45A...	-	D4E8BA9F-D45A

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.

The screenshot shows the Nuclias Unity Events page. The top navigation bar includes the Nuclias Unity logo, a dropdown menu for '0319_Stanley', a dropdown for 'AISID_Stanley', and a 'Events' tab. Below the navigation bar, there are filters for 'All 131', 'Access Points 37', 'Switches 91', and 'System Audit'. The main content area displays a table of events with columns for Severity, Time, Site, Event Type, and Device. A filter panel is open on the right side, showing dropdown menus for Severity, Site, Event Type, and Device Type, along with 'Clear' and 'Apply' buttons. The filter panel is highlighted with a red box.

Severity	Time	Site	Event Type	Device
Critical	Today, 8:45:06 AM	AISID_Stanley	Device Offline	Switch
Info	Mar 18, 2026, 5:58:59 PM	AISID_Stanley	Client IP change	Switch
Info	Mar 18, 2026, 5:28:56 PM	AISID_Stanley	Device Online	Access
Info	Mar 18, 2026, 5:29:55 PM	AISID_Stanley	System Audit	Access Point
Critical	Mar 18, 2026, 5:29:21 PM	AISID_Stanley	Device Offline	Access Point
Info	Mar 18, 2026, 5:28:58 PM	AISID_Stanley	Client IP change	Switch
Info	Mar 18, 2026, 5:28:31 PM	AISID_Stanley	System Audit	Access Point
Info	Mar 18, 2026, 5:28:20 PM	AISID_Stanley	System Audit	Access Point

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.

The screenshot displays the Nuclias Unity interface. At the top, there's a navigation bar with 'Nuclias Unity', 'Dashboard', 'Event', and 'View' tabs. Below this, a header section shows '0313_Stanley' and 'AISID_Stanley' with a dropdown menu. The main content area is titled 'Events' and features a table with columns: Severity, Time, Site, Event Type, Device Type, and Description. The table lists several events, including 'Device Offline', 'Client IP change', 'Device Online', and 'System Audit'. A red box highlights a custom view configuration panel on the right side of the table. This panel allows users to select which fields to display in the event log. The fields listed are: Status, Severity, Time, Site, Event Type, Device Type, Device Name, Mac Address, Description, Client Name, and Client MAC Address. The 'Mac Address', 'Description', 'Client Name', and 'Client MAC Address' fields are currently checked.

Severity	Time	Site	Event Type	Device Type	Description
Critical	Today, 8:45:06 AM	AISID_Stanley	Device Offline	Switch	Switch DMS-12F
Info	Mar 18, 2026, 5:58:59 PM	AISID_Stanley	Client IP change	Switch	Client 0A:18:EB
Info	Mar 18, 2026, 5:29:56 PM	AISID_Stanley	Device Online	Access Point	Access point D
Info	Mar 18, 2026, 5:29:55 PM	AISID_Stanley	System Audit	Access Point	The device DAF
Critical	Mar 18, 2026, 5:29:21 PM	AISID_Stanley	Device Offline	Access Point	Access point D
Info	Mar 18, 2026, 5:28:58 PM	AISID_Stanley	Client IP change	Switch	Client 0A:18:EB
Info	Mar 18, 2026, 5:28:31 PM	AISID_Stanley	System Audit	Access Point	Radio settings f
Info	Mar 18, 2026, 5:28:20 PM	AISID_Stanley	System Audit	Access Point	The device DAF

Nuclias Unity

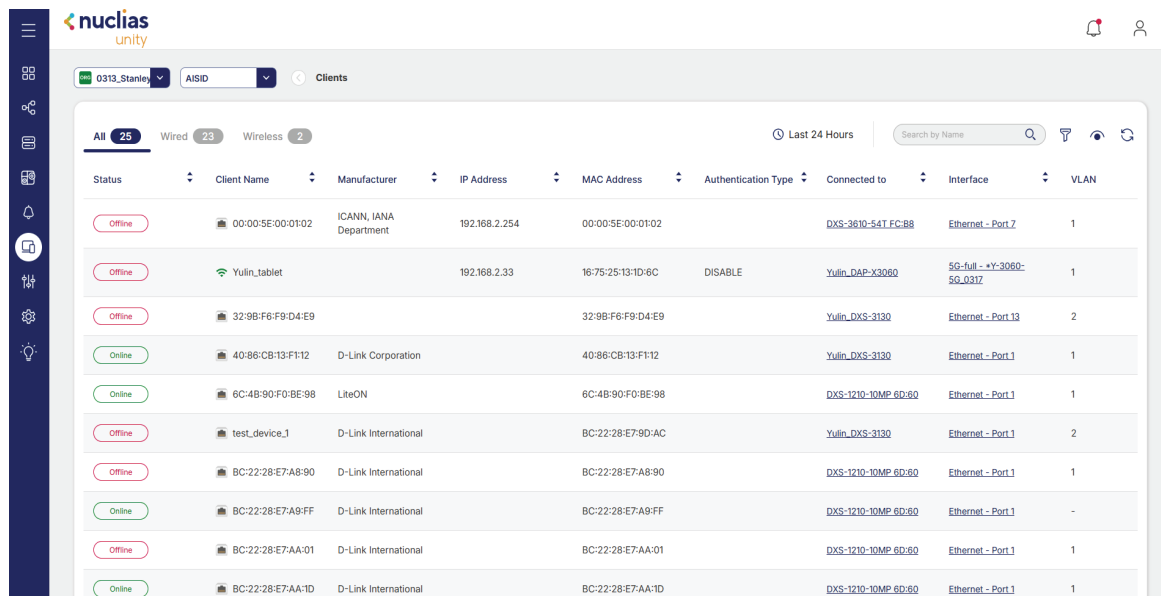
Dashboard

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.



Status	Client Name	Manufacturer	IP Address	MAC Address	Authentication Type	Connected to	Interface	VLAN
Offline	00:00:5E:00:01:02	ICANN, IANA Department	192.168.2.254	00:00:5E:00:01:02		DXS-3610-54T-FC-B8	Ethernet - Port 7	1
Offline	Yulin_tablet		192.168.2.33	16:75:25:13:1D:6C	DISABLE	Yulin_DAP-X3060	5G-full - *Y-3060-5G_0317	1
Offline	32:9B:F6:F9:D4:E9			32:9B:F6:F9:D4:E9		Yulin_DXS-3130	Ethernet - Port 13	2
Online	40:86:CB:13:F1:12	D-Link Corporation		40:86:CB:13:F1:12		Yulin_DXS-3130	Ethernet - Port 1	1
Online	6C:4B:90:F0:BE:98	LiteON		6C:4B:90:F0:BE:98		DXS-1210-10MP-6D:60	Ethernet - Port 1	1
Offline	test_device_1	D-Link International		BC:22:28:E7:9D:AC		Yulin_DXS-3130	Ethernet - Port 1	2
Offline	BC:22:28:E7:A8:90	D-Link International		BC:22:28:E7:A8:90		DXS-1210-10MP-6D:60	Ethernet - Port 1	1
Online	BC:22:28:E7:A9:FF	D-Link International		BC:22:28:E7:A9:FF		DXS-1210-10MP-6D:60	Ethernet - Port 1	-
Offline	BC:22:28:E7:AA:01	D-Link International		BC:22:28:E7:AA:01		DXS-1210-10MP-6D:60	Ethernet - Port 1	1
Online	BC:22:28:E7:AA:1D	D-Link International		BC:22:28:E7:AA:1D		DXS-1210-10MP-6D:60	Ethernet - Port 1	1

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

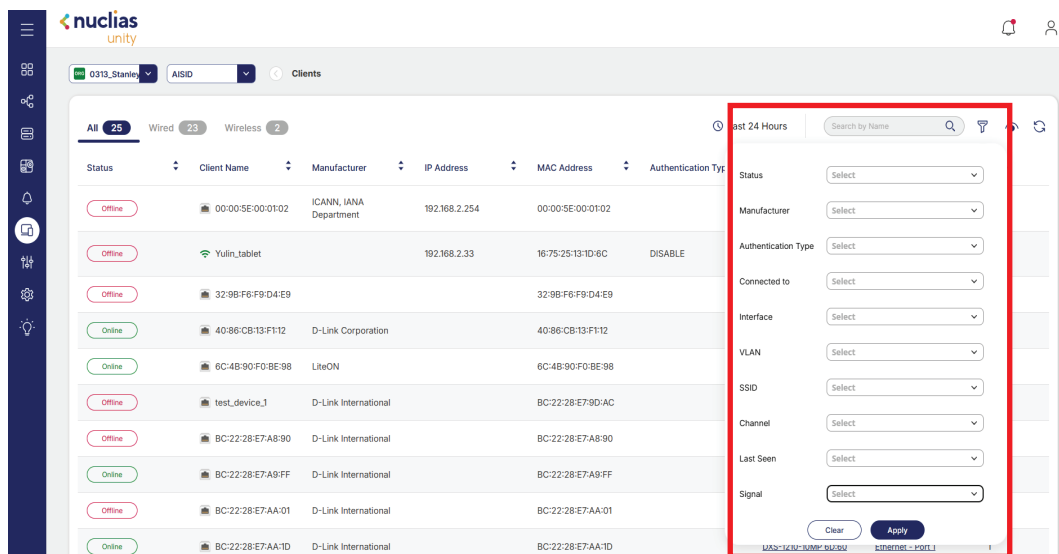
Filter

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.



The screenshot displays the Nuclias Unity interface. On the left is a dark sidebar with navigation icons. The main area shows the 'Clients' section with a table of client data. At the top right of the main area is a filter panel, which is highlighted with a red rectangle. The filter panel contains dropdown menus for Status, Manufacturer, Authentication Type, Connected to, Interface, VLAN, SSID, Channel, Last Seen, and Signal. Below these are 'Clear' and 'Apply' buttons. The table below the filter panel lists clients with columns for Status, Client Name, Manufacturer, IP Address, MAC Address, and Authentication Type. The table shows a mix of 'Offline' and 'Online' clients from various manufacturers like ICANN, IANA, D-Link, and LiteON.

Status	Client Name	Manufacturer	IP Address	MAC Address	Authentication Type
Offline	00:00:5E:00:01:02	ICANN, IANA Department	192.168.2.254	00:00:5E:00:01:02	
Offline	Yulin_Tablet		192.168.2.33	16:75:25:13:1D:6C	DISABLE
Offline	32:9B:F6:F9:D4:E9			32:9B:F6:F9:D4:E9	
Online	40:86:CB:13:F1:12	D-Link Corporation		40:86:CB:13:F1:12	
Online	6C:4B:90:F0:BE:98	LiteON		6C:4B:90:F0:BE:98	
Offline	test_device_1	D-Link International		BC:22:28:E7:9D:AC	
Offline	BC:22:28:E7:A8:90	D-Link International		BC:22:28:E7:A8:90	
Online	BC:22:28:E7:A9:FF	D-Link International		BC:22:28:E7:A9:FF	
Offline	BC:22:28:E7:AA:01	D-Link International		BC:22:28:E7:AA:01	
Online	BC:22:28:E7:AA:1D	D-Link International		BC:22:28:E7:AA:1D	

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.

The screenshot displays the Nuclias Unity interface. At the top, there's a navigation bar with 'Nuclias unity' logo and a 'Clients' tab. Below the navigation bar, there's a filter section with 'All 25', 'Wired 23', and 'Wireless 2'. The main content area shows a table of client information. A column selector menu is open on the right side, allowing users to choose which data fields to display. The menu is divided into two columns: 'Status' and 'Statistic'. The 'Status' column includes checkboxes for Status, Manufacturer, IP Address, MAC Address, Authentication Type, Connected to, Interface, VLAN, SSID, Channel, Last Seen, and Signal. The 'Statistic' column includes checkboxes for SNR, Download, Upload, Traffic (24HR), and Uptime. At the bottom of the menu, there are 'Reset' and 'Show All' buttons.

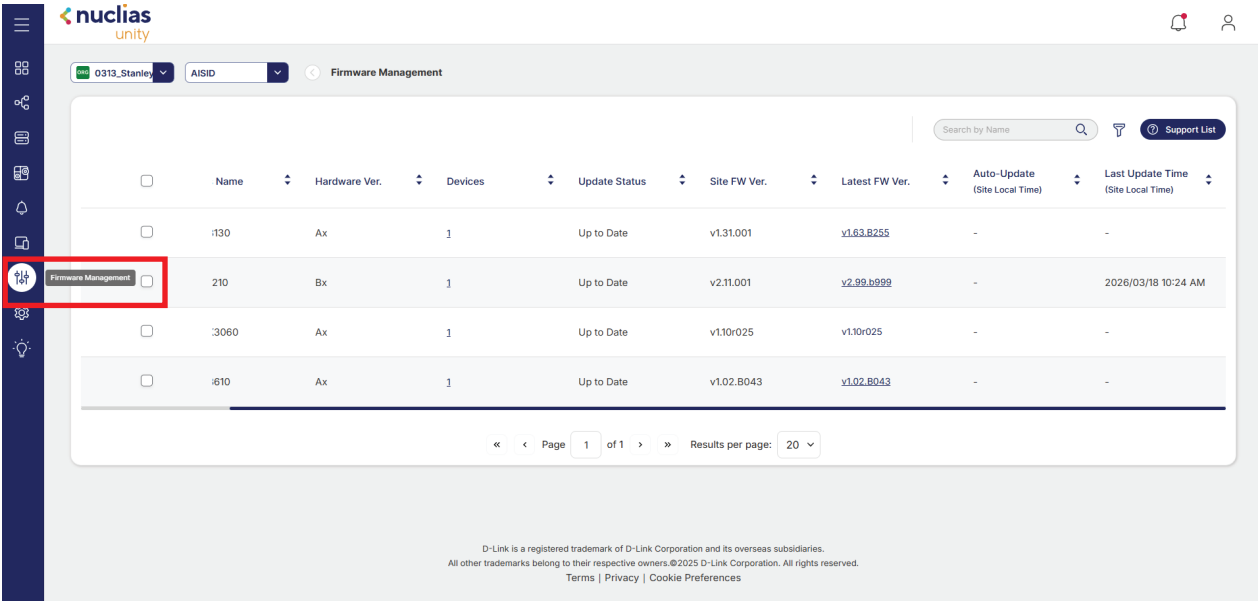
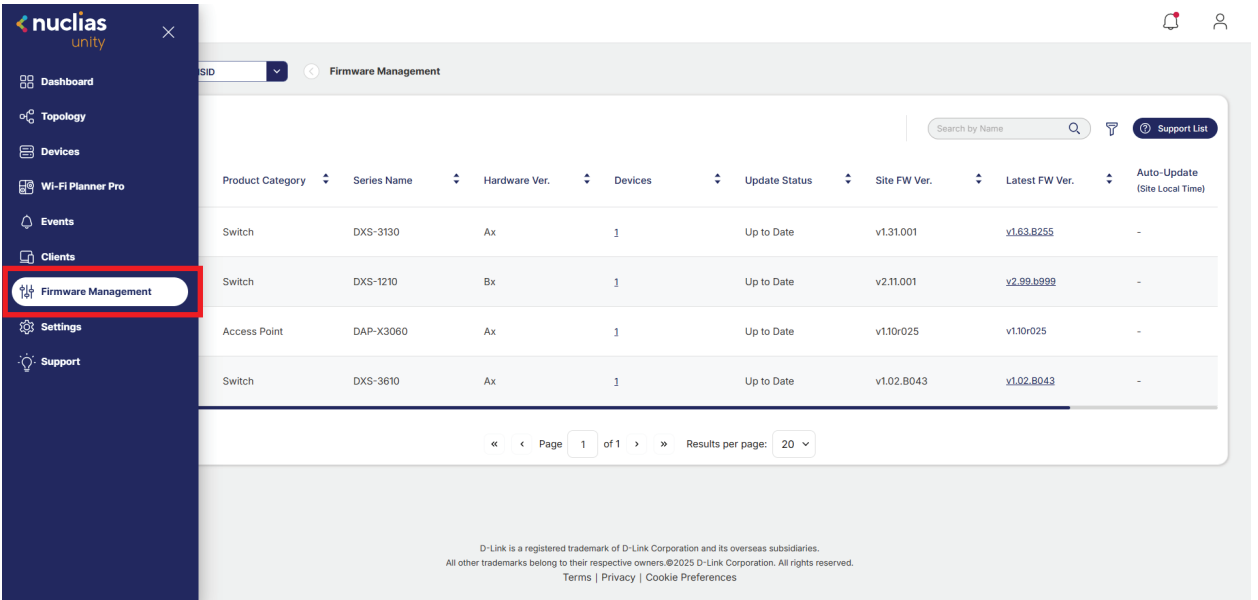
Status	Client Name	Manufacturer	IP Address	MAC Address	Authentication Type
Offline	00:00:5E:00:01:02	ICANN, IANA Department	192.168.2.254	00:00:5E:00:01:02	
Offline	Yulin_tablet		192.168.2.33	16:75:25:13:1D:8C	DISABLE
Offline	32:9B:F6:F9:D4:E9			32:9B:F6:F9:D4:E9	
Online	40:86:CB:13:F1:12	D-Link Corporation		40:86:CB:13:F1:12	
Online	6C:4B:90:F0:BE:98	LiteON		6C:4B:90:F0:BE:98	
Offline	test_device_1	D-Link International		BC:22:28:E7:9D:AC	
Offline	BC:22:28:E7:A8:90	D-Link International		BC:22:28:E7:A8:90	
Online	BC:22:28:E7:A9:FF	D-Link International		BC:22:28:E7:A9:FF	
Offline	BC:22:28:E7:AA:01	D-Link International		BC:22:28:E7:AA:01	
Online	BC:22:28:E7:AA:1D	D-Link International		BC:22:28:E7:AA:1D	

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.
Hardware 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.

The screenshot shows the Nuclias Unity Firmware Management interface. At the top, there's a header with the Nuclias Unity logo, a user profile icon, and a notification bell. Below the header, there's a navigation bar with tabs for '0313_Stanley', 'AISID', and 'Firmware Management'. The main content area features a table with columns: Product Category, Series Name, Hardware Ver., Devices, Update Status, Site FW Ver., Latest FW Ver., and Auto-Update (Site Local Time). The first row of the table is highlighted with a red border, indicating it is selected. The first row contains a green checkmark in the 'Action' column, 'Switch' in 'Product Category', 'DXS-1210' in 'Series Name', 'Bx' in 'Hardware Ver.', '1' in 'Devices', 'Up to Date' in 'Update Status', 'v2.11.001' in 'Site FW Ver.', 'v2.99.b999' in 'Latest FW Ver.', and '-' in 'Auto-Update'. Below the table, there's a pagination bar showing 'Page 1 of 1' and 'Results per page: 20'. At the bottom, there's a footer with legal disclaimers and links for Terms, Privacy, and Cookie Preferences.

Action	Product Category	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
☒	Switch	DXS-1210	Bx	1	Up to Date	v2.11.001	v2.99.b999	-
☐	Access Point	DAP-X3060	Ax	1	Up to Date	v1.10r025	v1.10r025	-
☐	Switch	DXS-3130	Ax	1	Up to Date	v1.31.001	v1.63.B255	-
☐	Switch	DXS-3610	Ax	1	Up to Date	v1.02.B043	v1.02.B043	-

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.

This screenshot shows the same Nuclias Unity Firmware Management interface as the previous one, but with the 'Action' dropdown menu open. The 'Action' button is highlighted with a red box, and the dropdown menu shows three options: 'Update Now' (with a lightning bolt icon), 'Schedule Update' (with a calendar icon), and 'Cancel Update' (with a trash can icon). The 'Update Now' option is selected. The table below the dropdown menu remains the same, with the first row highlighted in red. The pagination bar and footer are also visible.

Action	Product Category	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
☒	Switch	DXS-1210	Bx	1	Up to Date	v2.11.001	v2.99.b999	-
☐	Access Point	DAP-X3060	Ax	1	Up to Date	v1.10r025	v1.10r025	-
☐	Switch	DXS-3130	Ax	1	Up to Date	v1.31.001	v1.63.B255	-
☐	Switch	DXS-3610	Ax	1	Up to Date	v1.02.B043	v1.02.B043	-

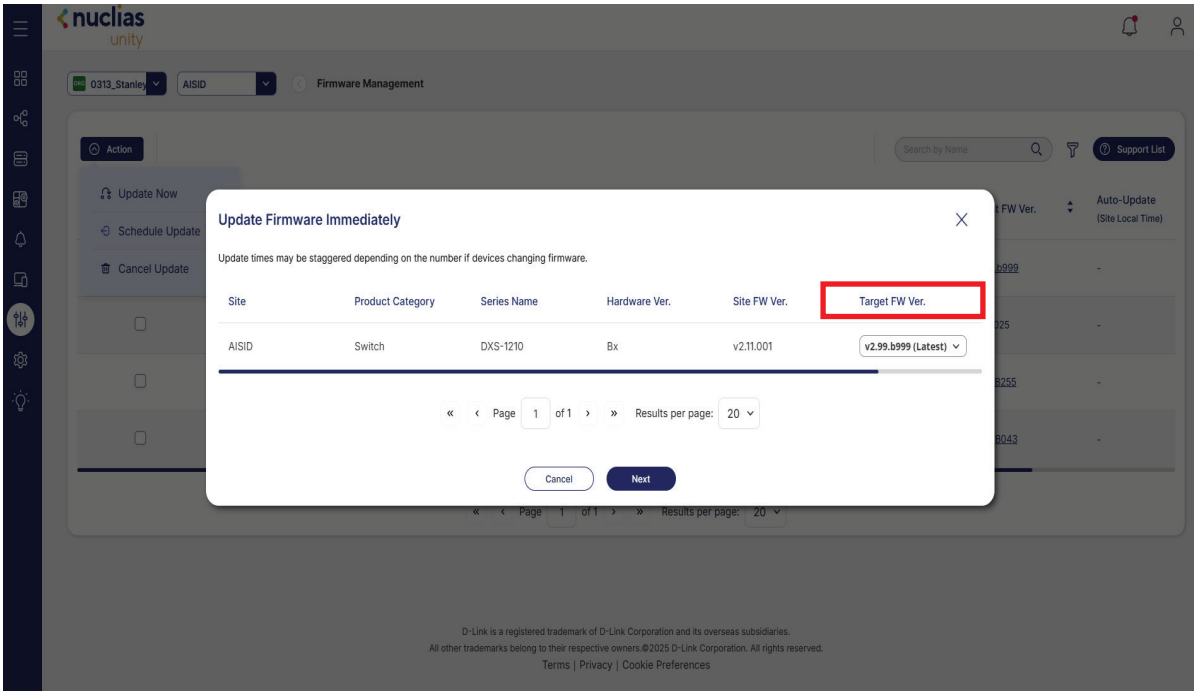
Nuclias Unity

Dashboard

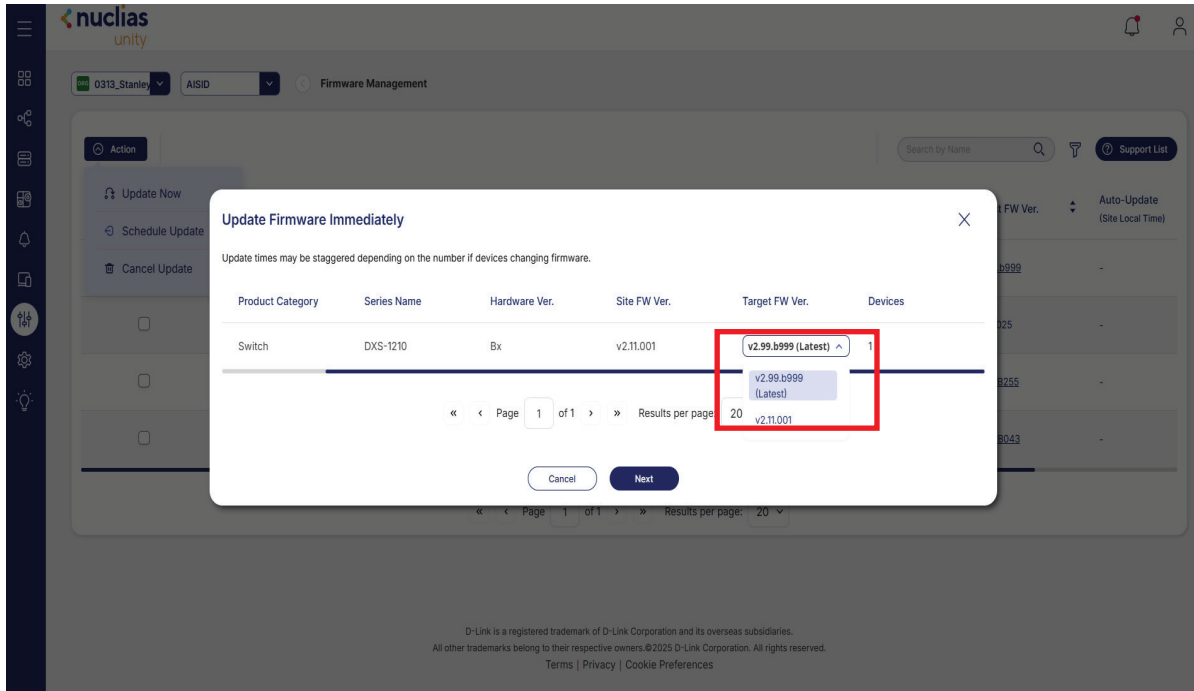
FW Management

Update Now

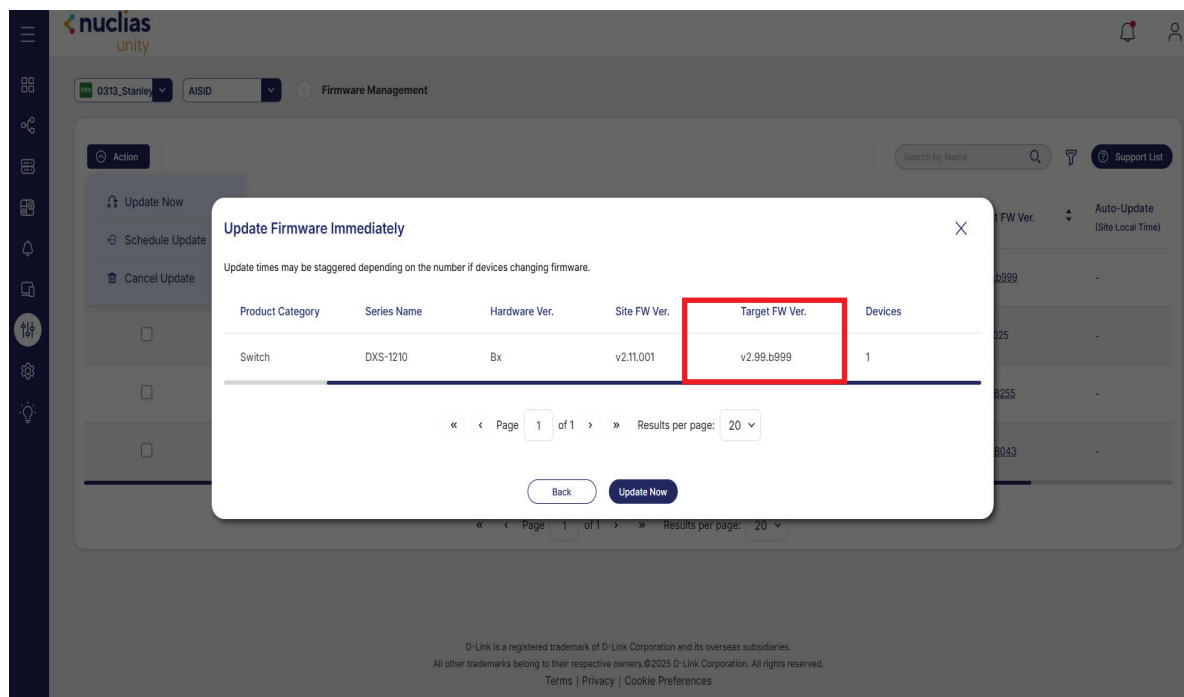
After clicking Update Now, navigate to Target Firmware Version to select the desired firmware version for the update.



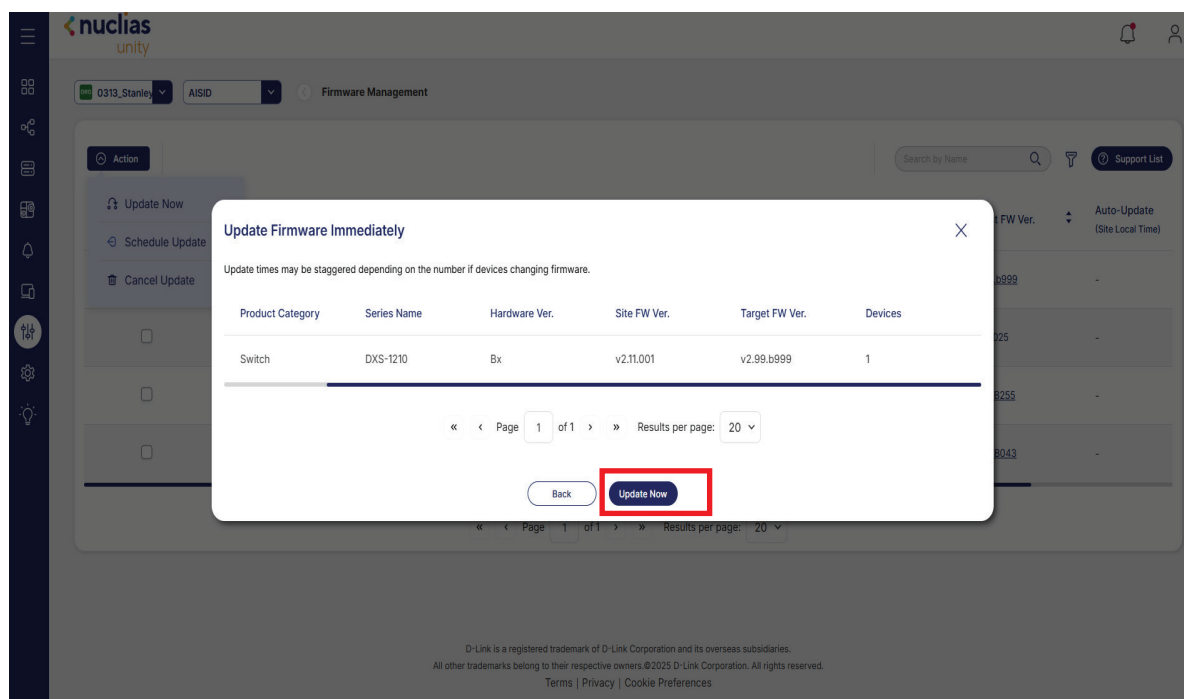
From there, you can choose the appropriate **firmware version** to apply to the selected device before proceeding with the update process.



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.

The screenshot shows the Nuclias Unity Firmware Management interface. At the top, there's a header with the Nuclias Unity logo, a dropdown menu for '0313_Stanley', and a 'Firmware Management' tab. Below the header, there's a table with columns: Product Category, Series Name, Hardware Ver., Devices, Update Status, Site FW Ver., Latest FW Ver., and Auto-Update (Site Local Time). The table contains four rows of data. The first row is for a Switch (DXS-3610, Ax, 1 device, Up to Date, v1.02.B043, y1.02.B043). The second row is for a Switch (DXS-1210, Bx, 1 device, Update Available, v2.99.b999, y2.99.b999). The third row is for a Switch (DXS-3130, Ax, 1 device, Up to Date, v1.31.001, y1.63.B255). The fourth row is for an Access Point (DAP-X3060, Ax, 1 device, Up to Date, v1.10r025, v1.10r025). This row is highlighted with a red box. At the bottom of the table, there's a pagination bar showing 'Page 1 of 1' and 'Results per page: 20'.

Product Category	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
Switch	DXS-3610	Ax	1	Up to Date	v1.02.B043	y1.02.B043	-
Switch	DXS-1210	Bx	1	Update Available	v2.99.b999	y2.99.b999	-
Switch	DXS-3130	Ax	1	Up to Date	v1.31.001	y1.63.B255	-
Access Point	DAP-X3060	Ax	1	Up to Date	v1.10r025	v1.10r025	-

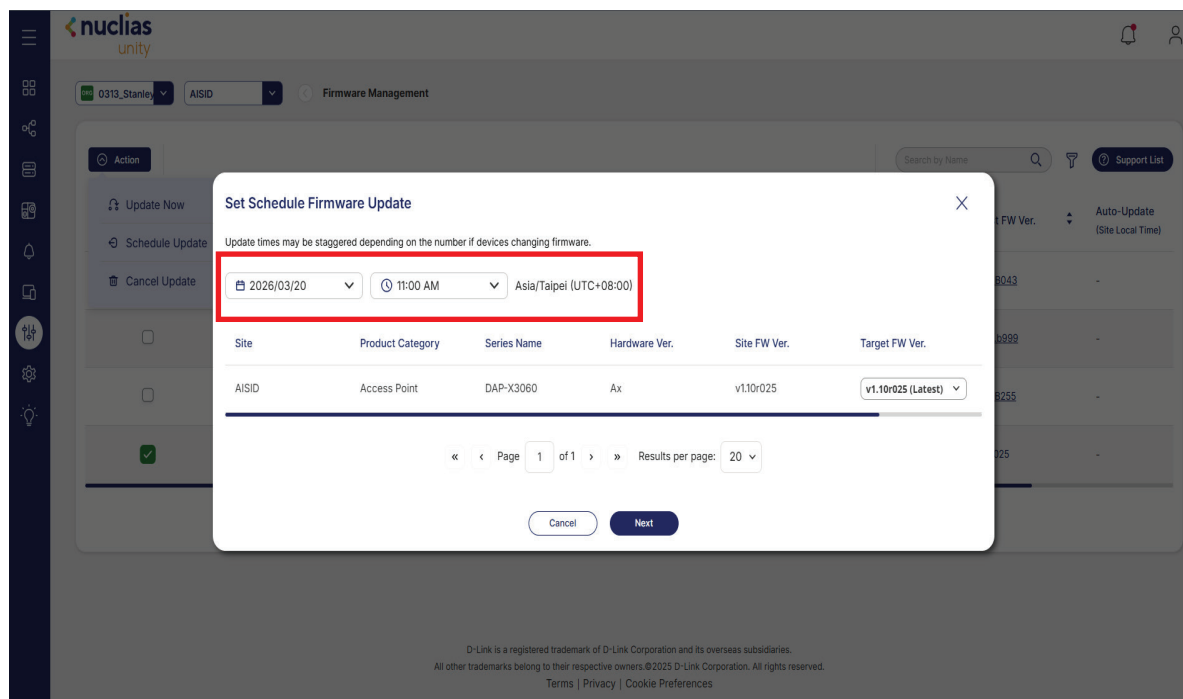
After selecting the device, the **Action** option appears on the top left corner. Click **Action** and select **Schedule Update**.

The screenshot shows the Nuclias Unity Firmware Management interface with the 'Action' dropdown menu open. The menu options are 'Update Now', 'Schedule Update', and 'Cancel Update'. The 'Schedule Update' option is highlighted with a red box. The background table is the same as in the previous screenshot, showing the list of devices.

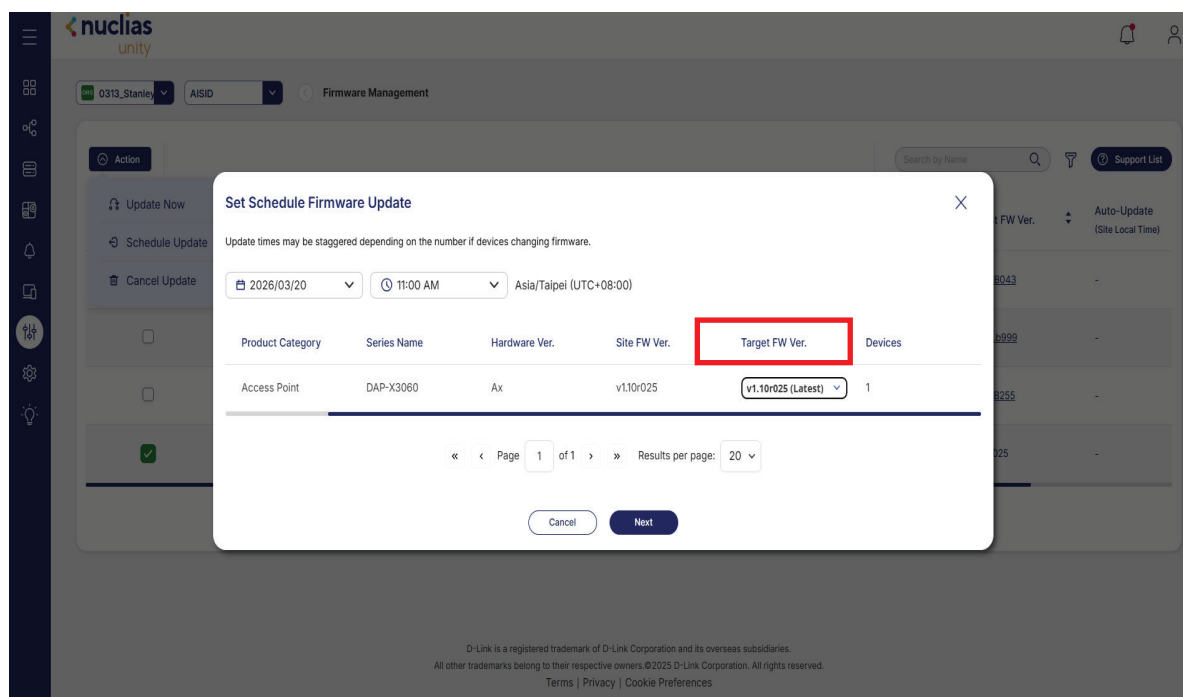
Product Category	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
Switch	DXS-3610	Ax	1	Up to Date	v1.02.B043	y1.02.B043	-
Switch	DXS-1210	Bx	1	Update Available	v2.99.b999	y2.99.b999	-
Switch	DXS-3130	Ax	1	Up to Date	v1.31.001	y1.63.B255	-
Access Point	DAP-X3060	Ax	1	Up to Date	v1.10r025	v1.10r025	-

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.

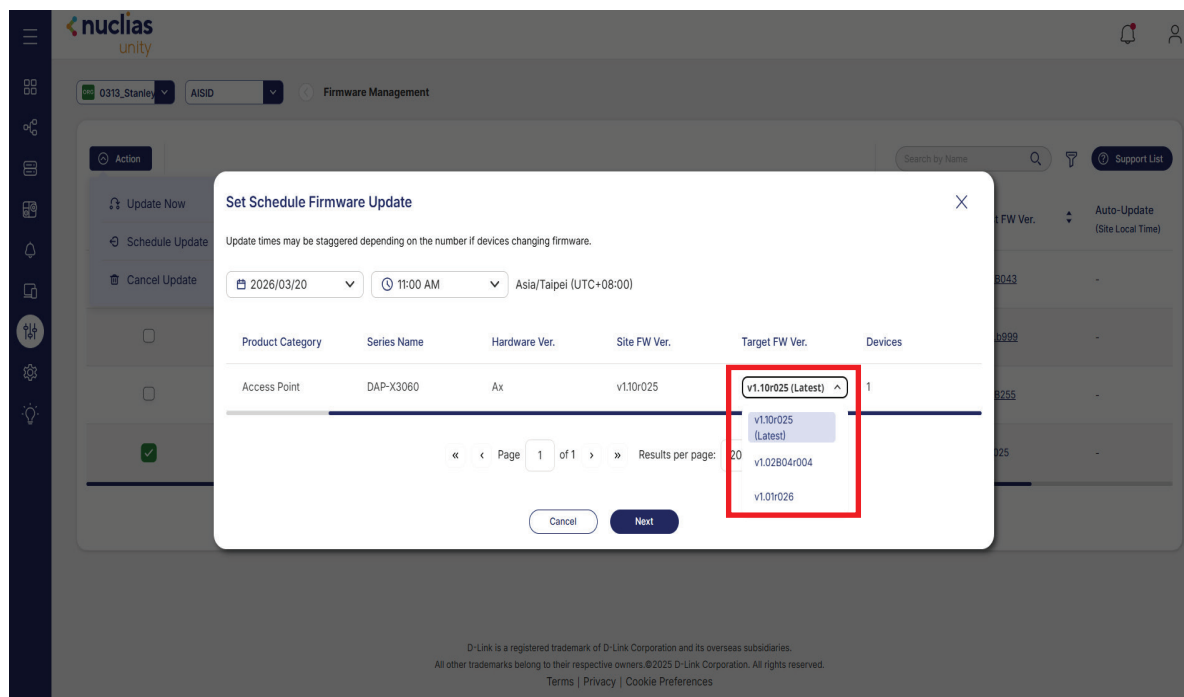


Then navigate to **Target Firmware Version** and select the firmware version that needs to be applied for the update.

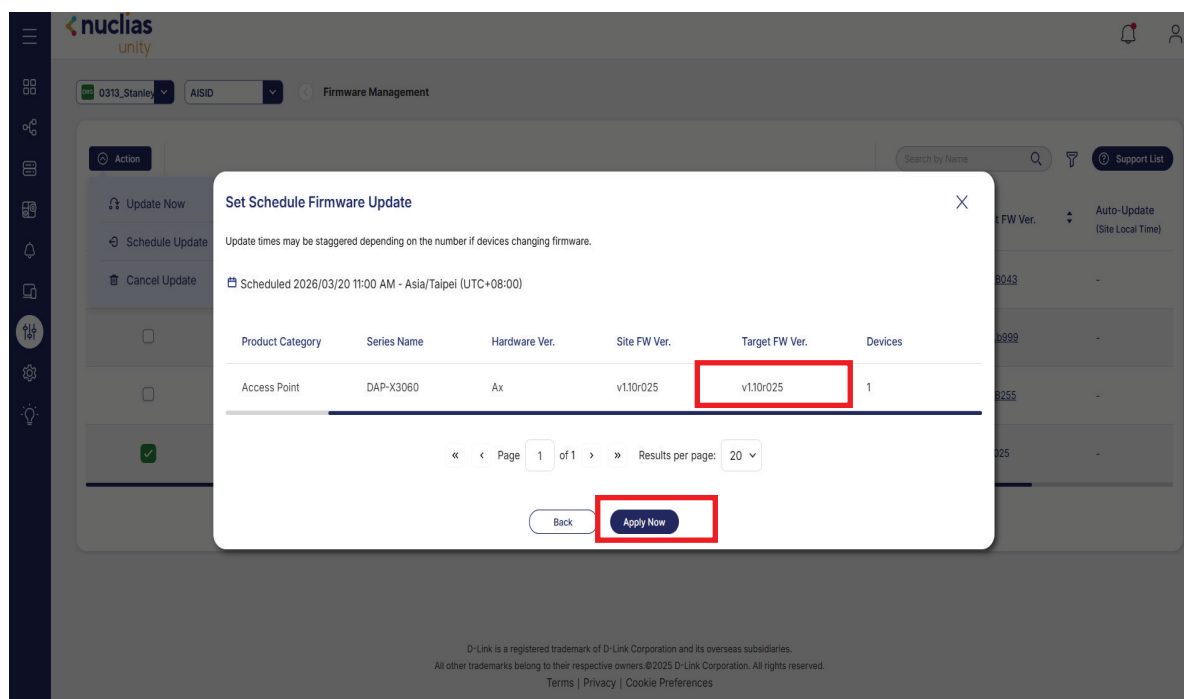


Nuclias Unity Dashboard FW Management Schedule Update

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



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



Schedule Update

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

0313_Stanley

AISID

Firmware Management

☐	Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)	Last Update Time (Site Local Time)
☐	210	Bx	1	Update Available	v2.99.b999	v2.99.b999	-	2026/03/20 9:42 AM
☐	:3060	Ax	1	Up to Date	v1.10r025	v1.10r025	2026/03/20 11:00 AM	-
☐	:i610	Ax	1	Up to Date	v1.02.B043	v1.02.B043	-	-
☐	:i30	Ax	1	Up to Date	v1.31.001	v1.63.B255	-	-

«

<

Page 1 of 1

>

»

Results per page:

20

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.©2025 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.

The screenshot shows the Nuclias Unity Firmware Management interface. The 'Action' button is highlighted in the top left corner of the table. The table lists devices with columns for Series Name, Hardware Ver., Devices, Update Status, Site FW Ver., Latest FW Ver., Auto-Update, and Last Upda. The device DAP-X3060 is highlighted with a red box.

Action	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)	Last Upda (Site Local 1)
☐	DXS-1210	Bx	1	Update Available	v2.99.b999	v2.99.b999	-	2026/03/2
☒	DAP-X3060	Ax	1	Up to Date	v110r025	v110r025	2026/03/20 11:00 AM	-
☐	DXS-3610	Ax	1	Up to Date	v1.02.B043	v1.02.B043	-	-
☐	DXS-3130	Ax	1	Up to Date	v1.31.001	v1.63.B255	-	-

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

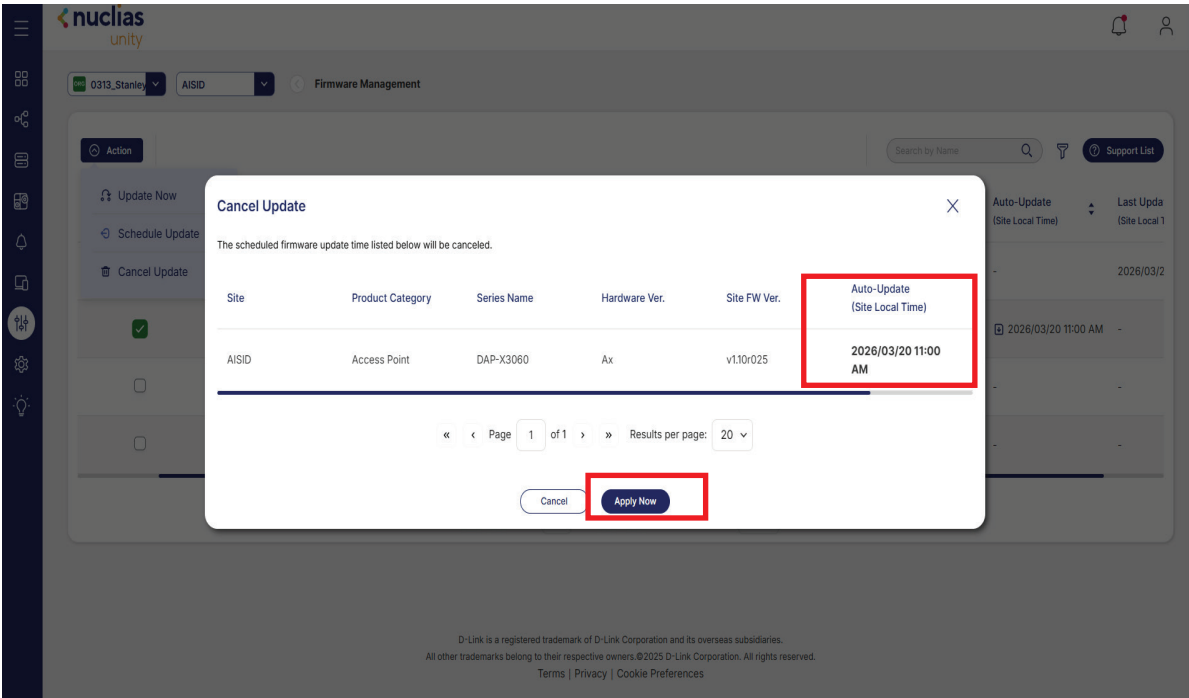
The screenshot shows the Nuclias Unity Firmware Management interface. The 'Action' button is highlighted in the top left corner of the table. The 'Cancel Update' option is highlighted in the dropdown menu.

Action	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
☒	Access Point	DAP-X3060	Ax	Up to Date	v110r025	v110r025	-
☐	Switch	DXS-3130	Ax	Up to Date	v1.31.001	v1.63.B255	-
☐	Switch	DXS-1210	Bx	Update Available	v2.99.b999	v2.99.b999	-
☐	Switch	DXS-3610	Ax	Up to Date	v1.02.B043	v1.02.B043	-

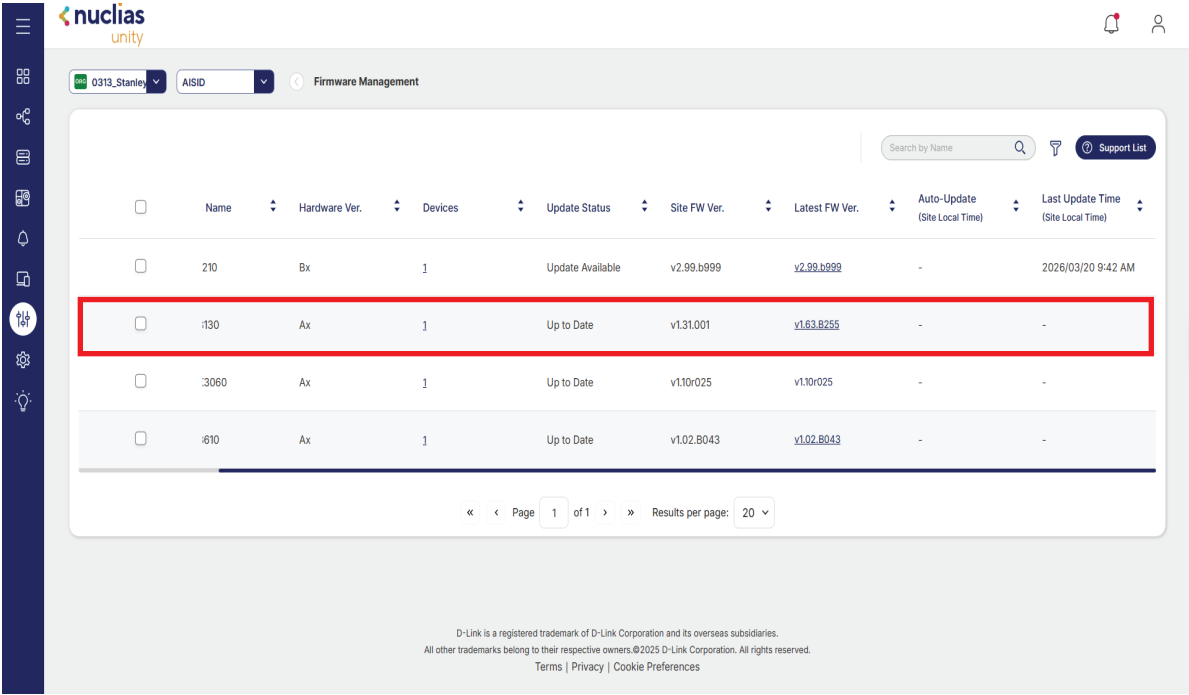
Nuclias Unity Dashboard FW Management

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.



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.

The screenshot displays the Nuclias Unity Firmware Management interface. At the top, there's a header with the Nuclias logo and navigation tabs for '0313_Stanley', 'AISID', and 'Firmware Management'. Below the header, a table lists devices with columns: Product Category, Series Name, Hardware Ver., Devices, and Update Status. A filter panel is open on the right, showing dropdown menus for Product Category, Series Name, and Update Status, along with 'Clear' and 'Apply' buttons. The table contains five rows of device information. At the bottom, there's a pagination bar showing 'Page 1 of 1' and 'Results per page: 20'. A footer section contains legal disclaimers and links for Terms, Privacy, and Cookie Preferences.

	Product Category	Series Name	Hardware Ver.	Devices	Update Status
☐	Switch	DXS-1210	Bx	1	Update Availat
☐	Switch	DXS-3130	Ax	1	Up to Date
☐	Access Point	DAP-X3060	Ax	1	Up to Date
☐	Switch	DXS-3610	Ax	1	Up to Date

Product Category: Select
Series Name: Select
Update Status: Select
Clear Apply

« < Page 1 of 1 > » Results per page: 20

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.
Terms | Privacy | Cookie Preferences

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.

The screenshot shows the Nuclias Unity Firmware Management interface. The top navigation bar includes the Nuclias Unity logo, a user profile icon, and a notification bell. The main content area is titled 'Firmware Management' and features a search bar labeled 'Search by Name'. A red box highlights the 'Support List' button in the top right corner. Below the search bar is a table with the following columns: Product Category, Series Name, Hardware Ver., Devices, Update Status, Site FW Ver., Latest FW Ver., and Auto-Update (Site Local Time). The table contains five rows of data, each with a checkbox in the first column. The bottom of the interface shows pagination controls: 'Page 1 of 1' and 'Results per page: 20'.

	Product Category	Series Name	Hardware Ver.	Devices	Update Status	Site FW Ver.	Latest FW Ver.	Auto-Update (Site Local Time)
☐	Switch	DXS-1210	Bx	1	Update Available	v2.99.b999	v2.99.b999	-
☐	Switch	DXS-3130	Ax	1	Up to Date	v1.31.001	v1.63.B255	-
☐	Access Point	DAP-X3060	Ax	1	Up to Date	v1.10r025	v1.10r025	-
☐	Switch	DXS-3610	Ax	1	Up to Date	v1.02.B043	v1.02.B043	-

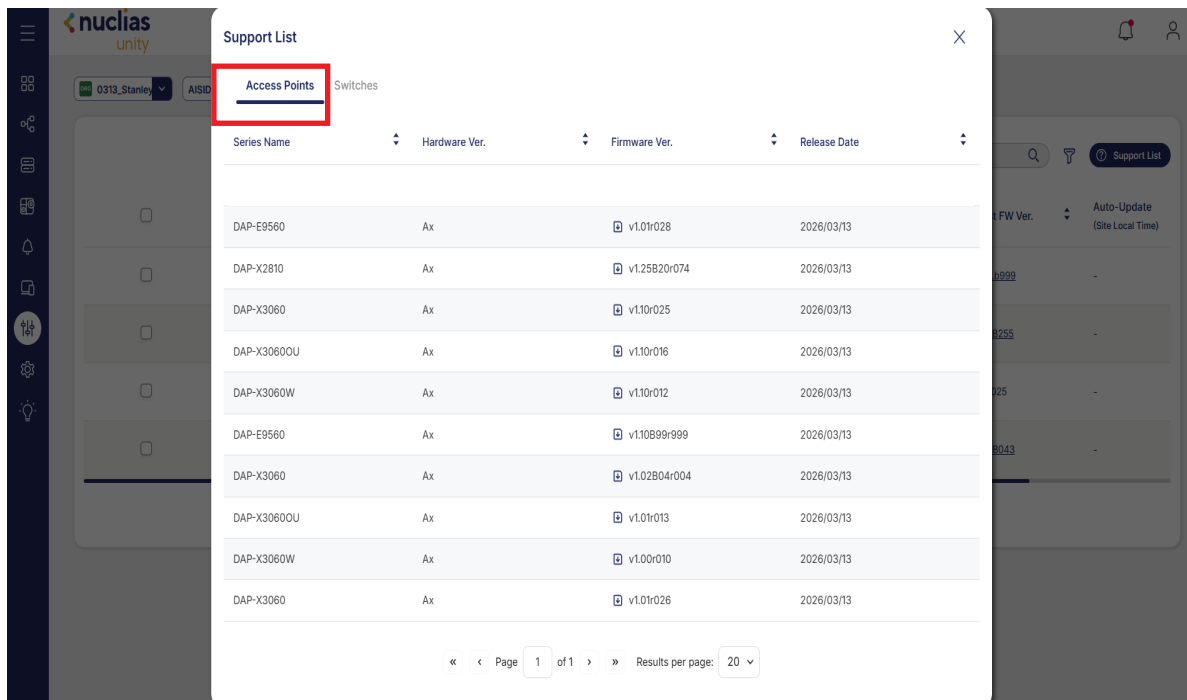
« < Page 1 of 1 > » Results per page: 20

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2025 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

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.



Series Name	Hardware Ver.	Firmware Ver.	Release Date
DAP-E9560	Ax	v1.01r028	2026/03/13
DAP-X2810	Ax	v1.25B20r074	2026/03/13
DAP-X3060	Ax	v1.10r025	2026/03/13
DAP-X3060OU	Ax	v1.10r016	2026/03/13
DAP-X3060W	Ax	v1.10r012	2026/03/13
DAP-E9560	Ax	v1.10B99r999	2026/03/13
DAP-X3060	Ax	v1.02B04r004	2026/03/13
DAP-X3060OU	Ax	v1.01r013	2026/03/13
DAP-X3060W	Ax	v1.00r010	2026/03/13
DAP-X3060	Ax	v1.01r026	2026/03/13

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.

The screenshot shows the Nuclias Unity Support List interface. The 'Switches' tab is selected and highlighted with a red box. The table displays various switch models, their hardware versions, firmware versions, and release dates.

Series Name	Hardware Ver.	Firmware Ver.	Release Date
DKS-3610	Ax	v1.02.8043	2026/03/13
DKS-3410	Ax	v1.00.8029	2026/03/13
DKS-3130	Ax	v1.31.001	2026/03/13
DMS-3130	Ax	v1.31.001	2026/03/13
DKS-1250	Ax	v1.01.001	2026/03/13
DKS-1210	Bx	v2.11.001	2026/03/13
DMS-1250	Ax	v1.02.012	2026/03/13
DGS-3130	Bx	v2.04.001	2026/03/13
DGS-1250	Ax	v2.10.8008	2026/03/13
DGS-1250	Bx	v1.00.010	2026/03/13
DGS-1210	F	v8.33.003	2026/03/13
DKS-3130	Ax	v1.63.8255	2026/03/13
DMS-3130	Ax	v1.63.8255	2026/03/13
DKS-1250	Ax	v1.63.8255	2026/03/13
DKS-1210	Bx	v2.89.0899	2026/03/13
DMS-1250	Ax	v1.89.0899	2026/03/13
DGS-3130	Bx	v2.63.8255	2026/03/13
DGS-1250	Bx	v1.89.0899	2026/03/13
DGS-1210	F	v8.89.0899	2026/03/13
DGS-1100	Ax	v4.00.0080A	2026/03/20

Page 1 of 2 Results per page: 20

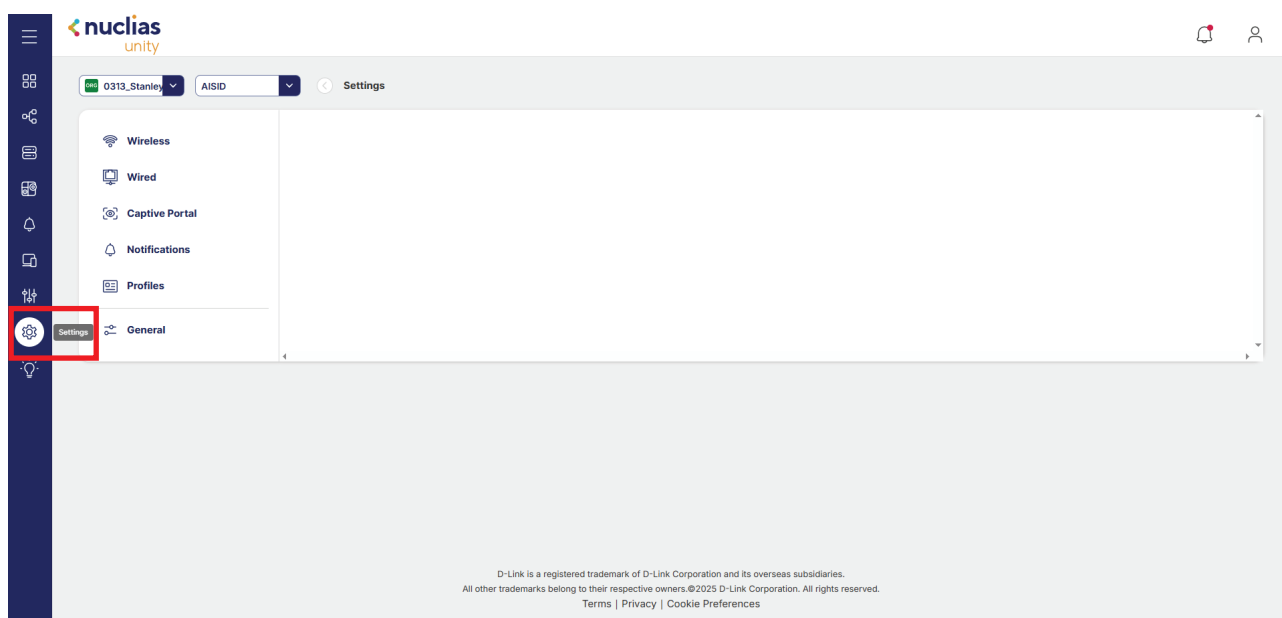
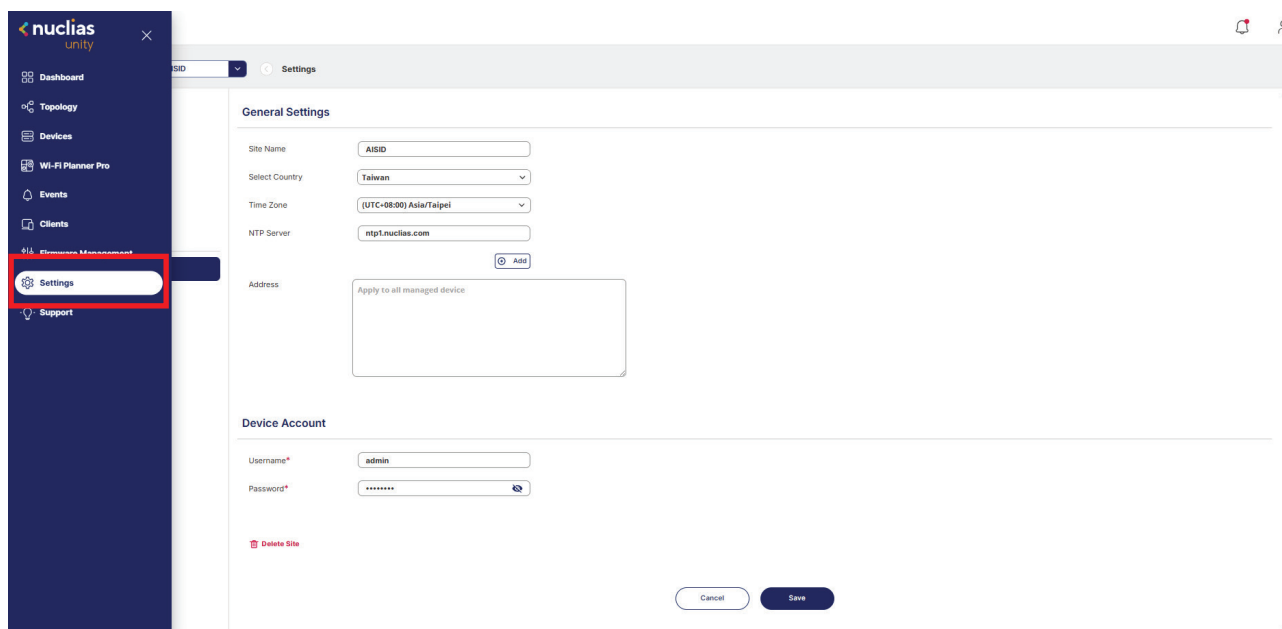
Parameter	Description
Series Name	Indicates the specific product series or model family of the device, allowing administrators to easily identify and group compatible devices.
Hardware Version	Displays the hardware revision of the device, which is essential for selecting the correct firmware version 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.

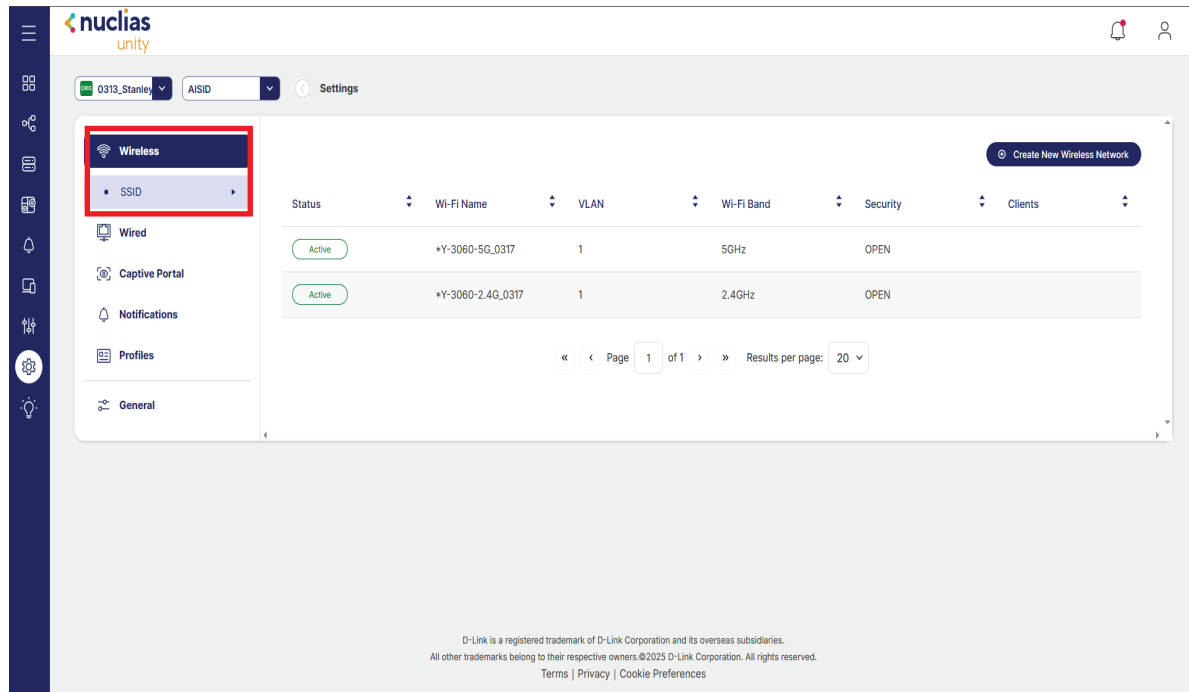


Nuclias Unity Dashboard

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.

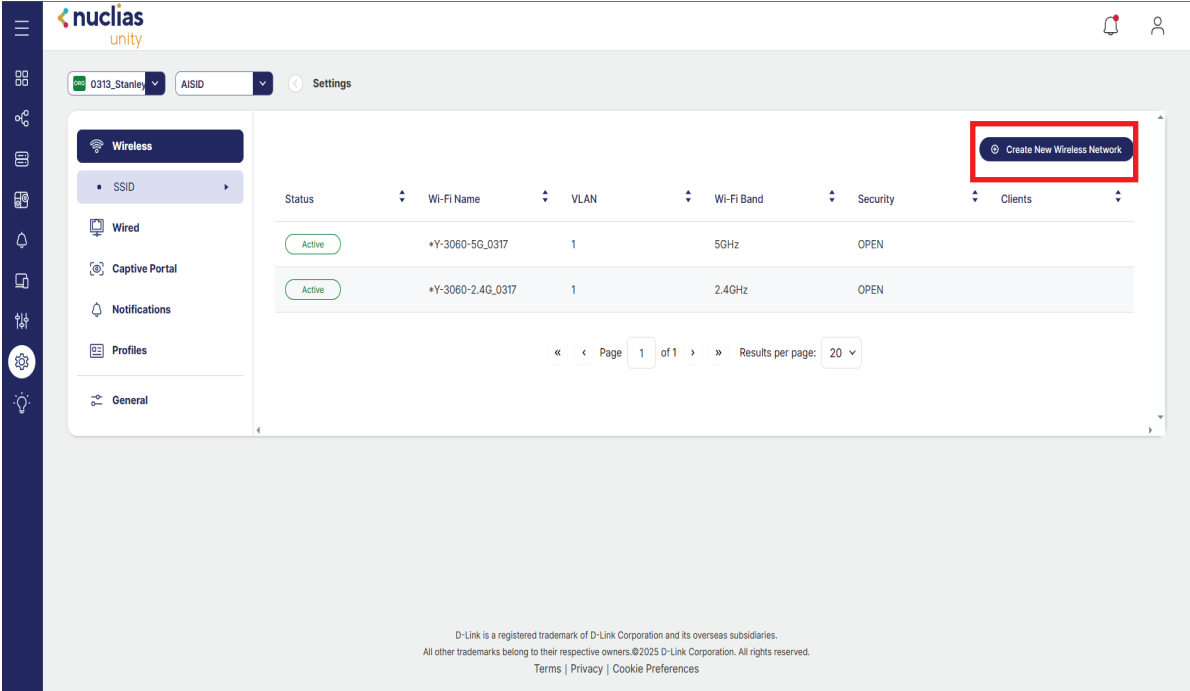
Nuclias Unity

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.



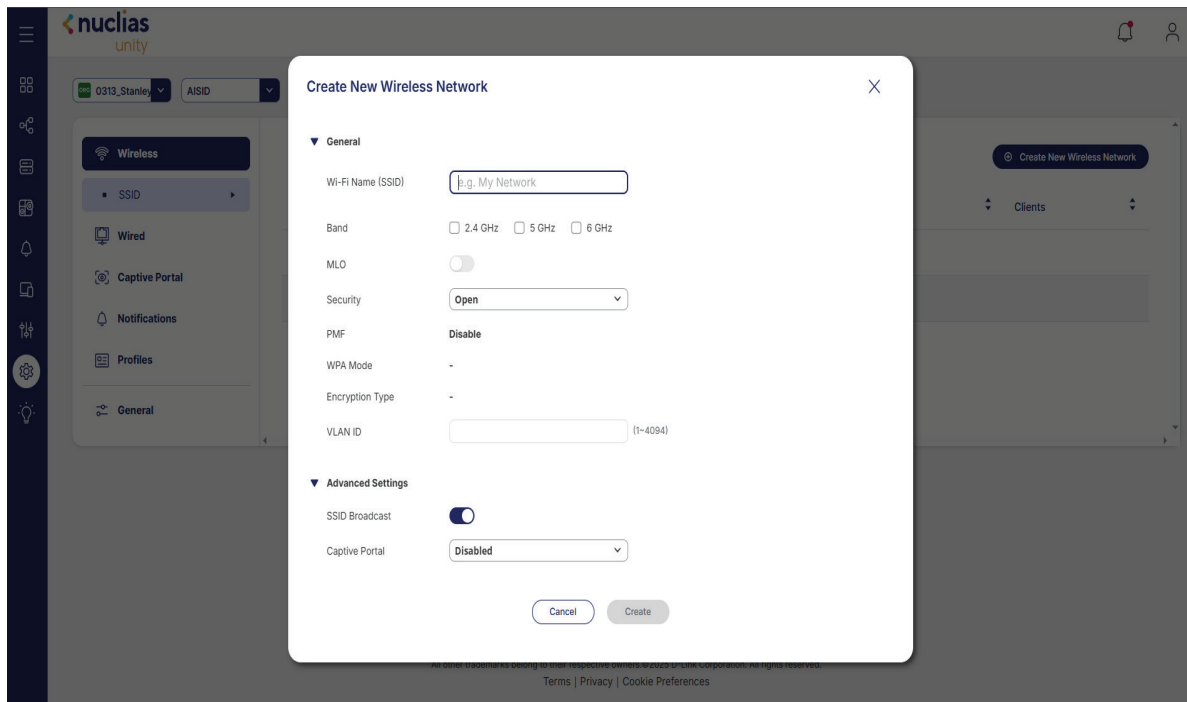
Nuclias Unity Dashboard

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 **enable 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.



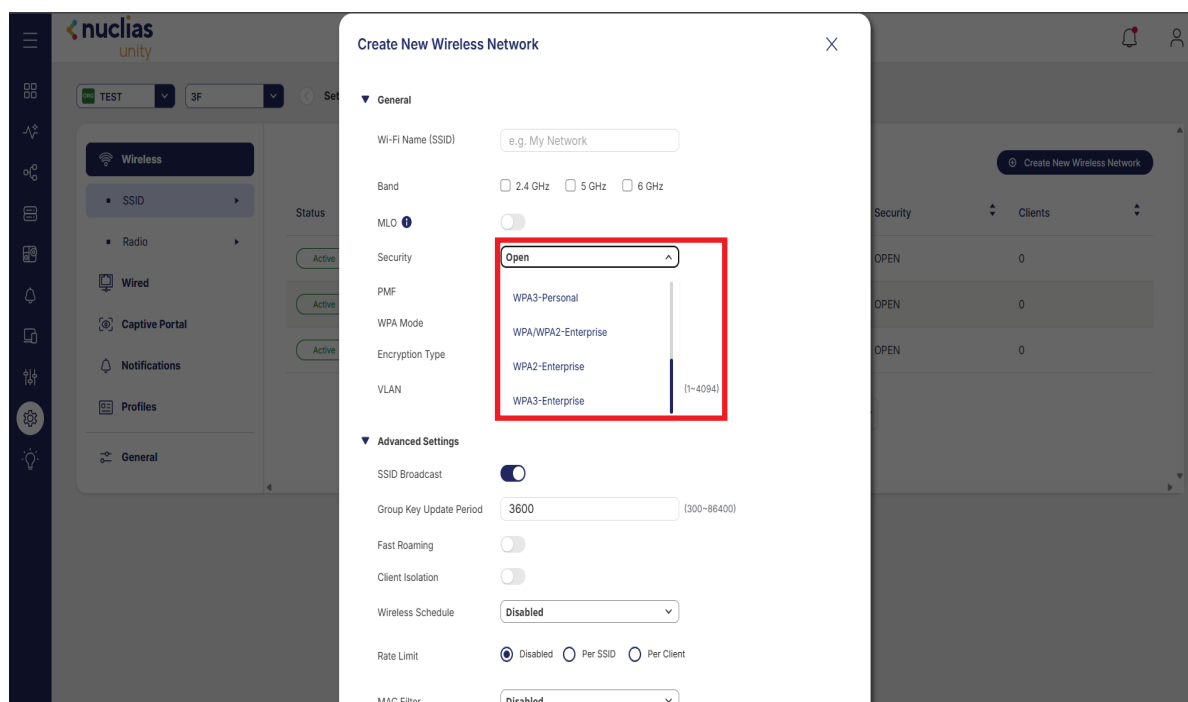
Wireless Enterprise Security

Configure the wireless security mode for the SSID to protect wireless network access. Select the authentication and encryption method that best matches your network requirements and client device compatibility.

When creating a new **SSID** under **Settings > Wireless**, select the desired wireless security protocol. Multiple enterprise-grade security options are available to provide the appropriate level of authentication, encryption, and compatibility for your wireless network.

The available security modes are:

- **Open** – No authentication or encryption. Suitable only for public or temporary networks.
- **Enhanced Open** – Provides opportunistic wireless encryption (OWE) without requiring a password.
- **Enhanced Open + Open** – Supports both Open and Enhanced Open clients for improved compatibility during migration.
- **WPA/WPA2-Personal** – Supports both WPA and WPA2-Personal security using a pre-shared key (PSK).
- **WPA2-Personal** – Uses WPA2 security with a pre-shared key (PSK) for secure wireless access.
- **WPA2/WPA3-Personal** – Supports both WPA2-Personal and WPA3-Personal clients, enabling a smooth transition to WPA3.
- **WPA3-Personal** – Uses the latest WPA3 security with SAE (Simultaneous Authentication of Equals) for enhanced protection.
- **WPA/WPA2-Enterprise** – Supports both WPA and WPA2-Enterprise authentication using a RADIUS server.
- **WPA2-Enterprise** – Uses WPA2-Enterprise authentication with a RADIUS server for enterprise environments.
- **WPA3-Enterprise** – Provides the highest level of enterprise wireless security using WPA3-Enterprise with RADIUS authentication.



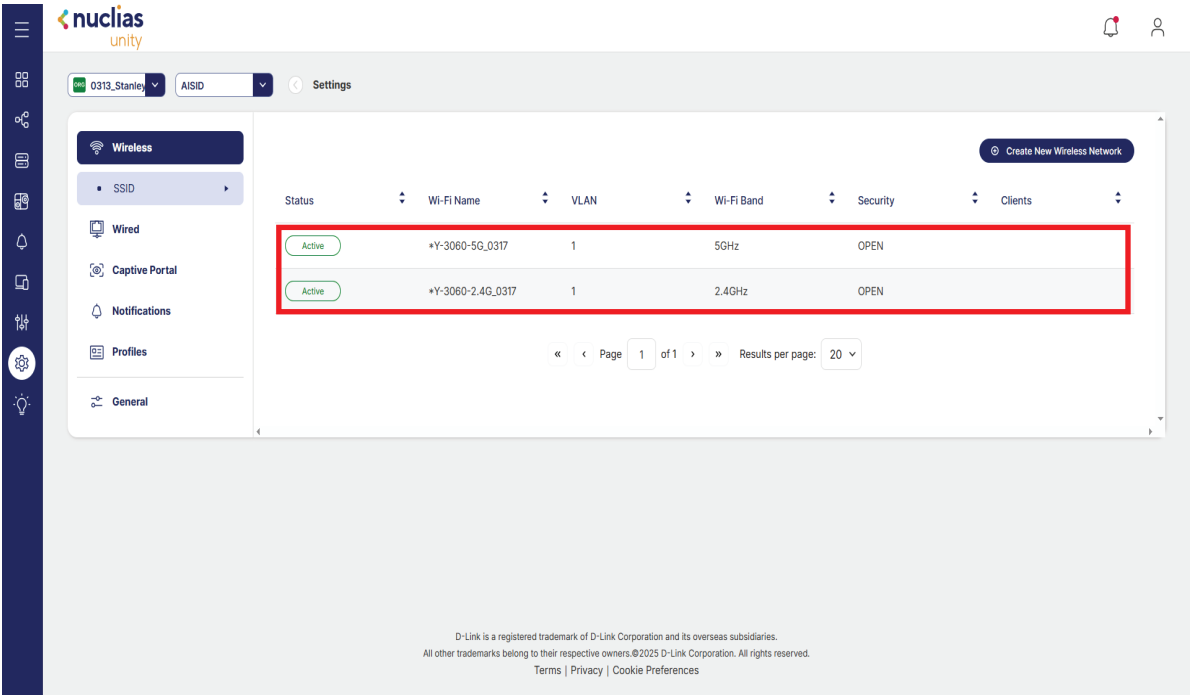
Nuclias Unity

Dashboard

Settings

Wireless

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.



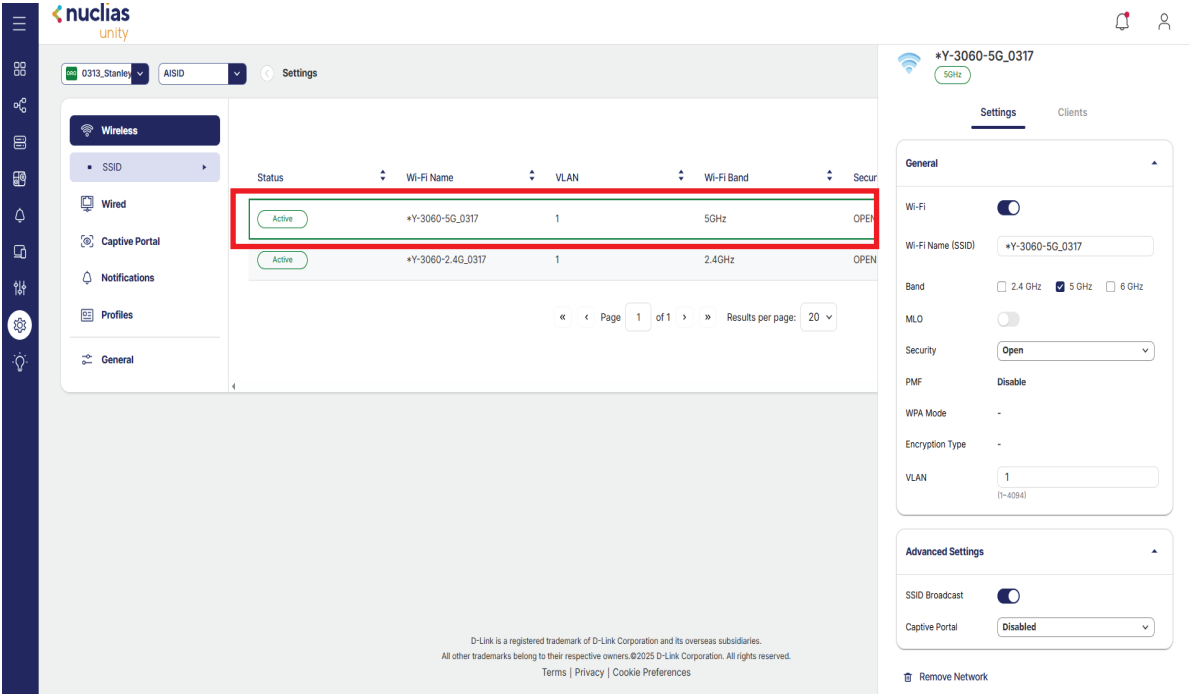
Nuclias Unity

Dashboard

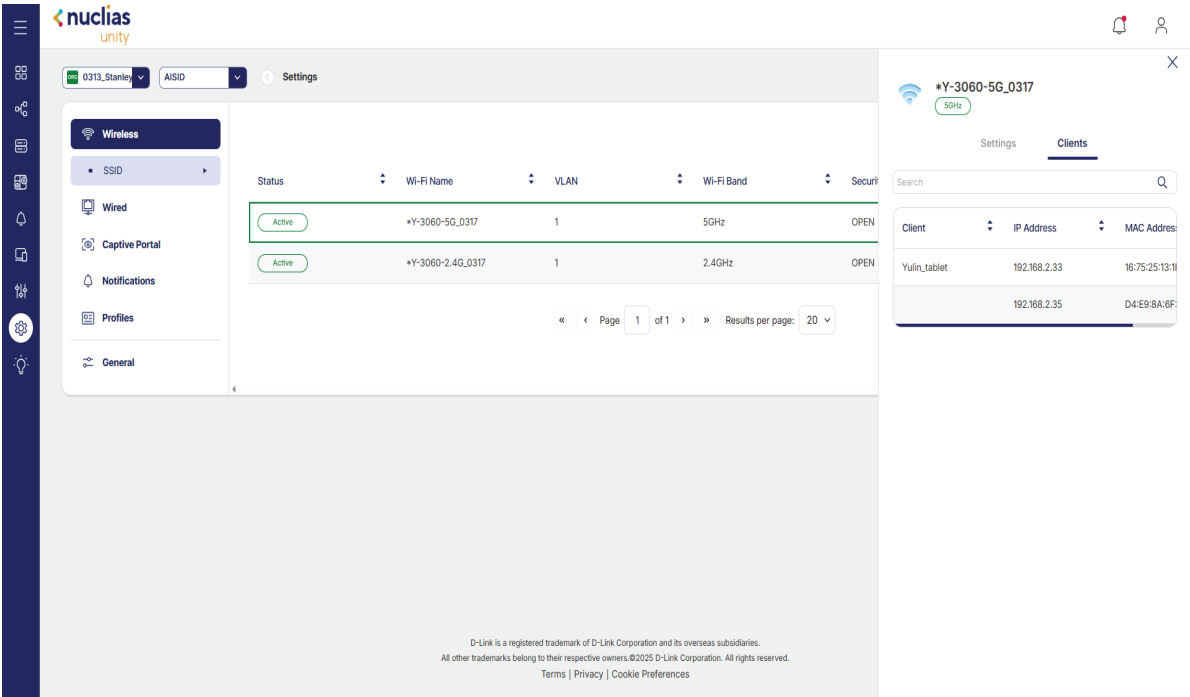
Settings

Wireless

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

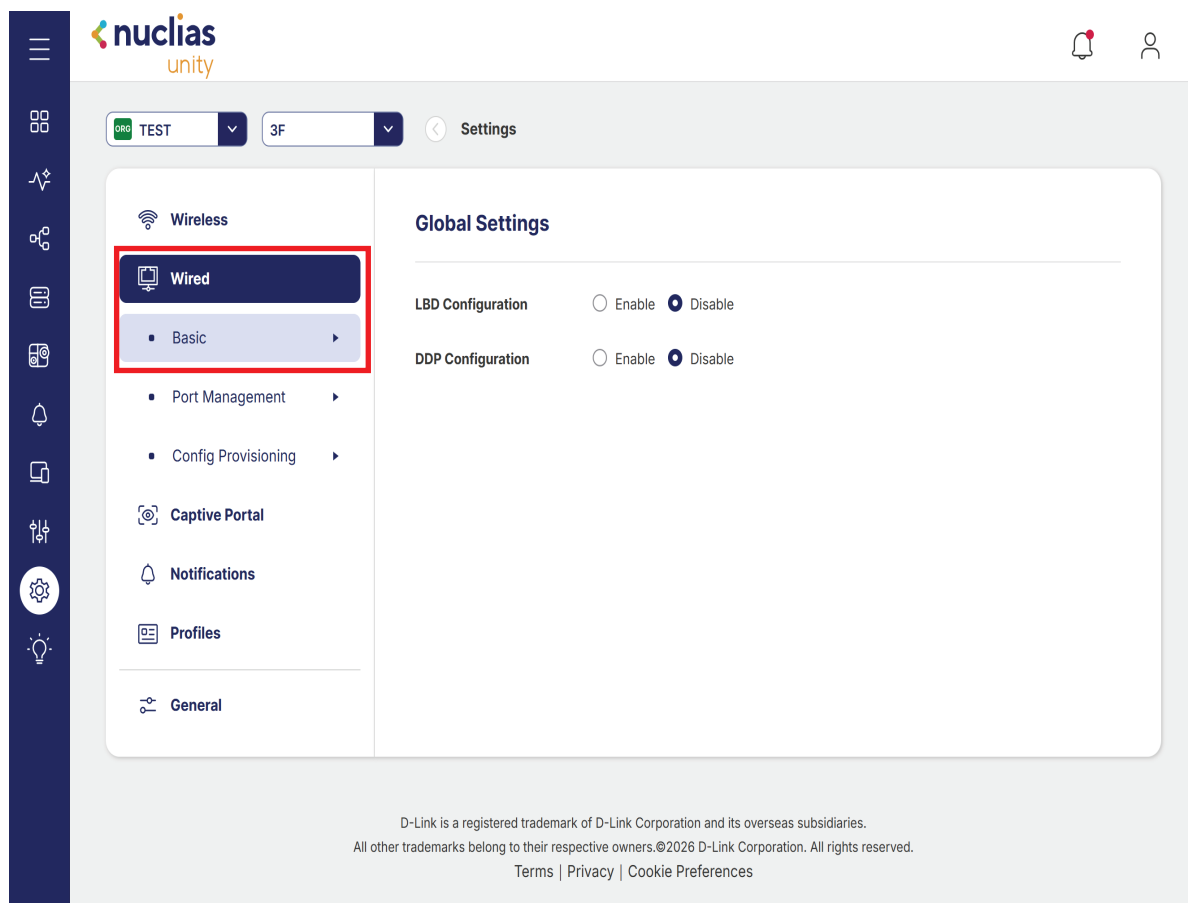
Wired

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.



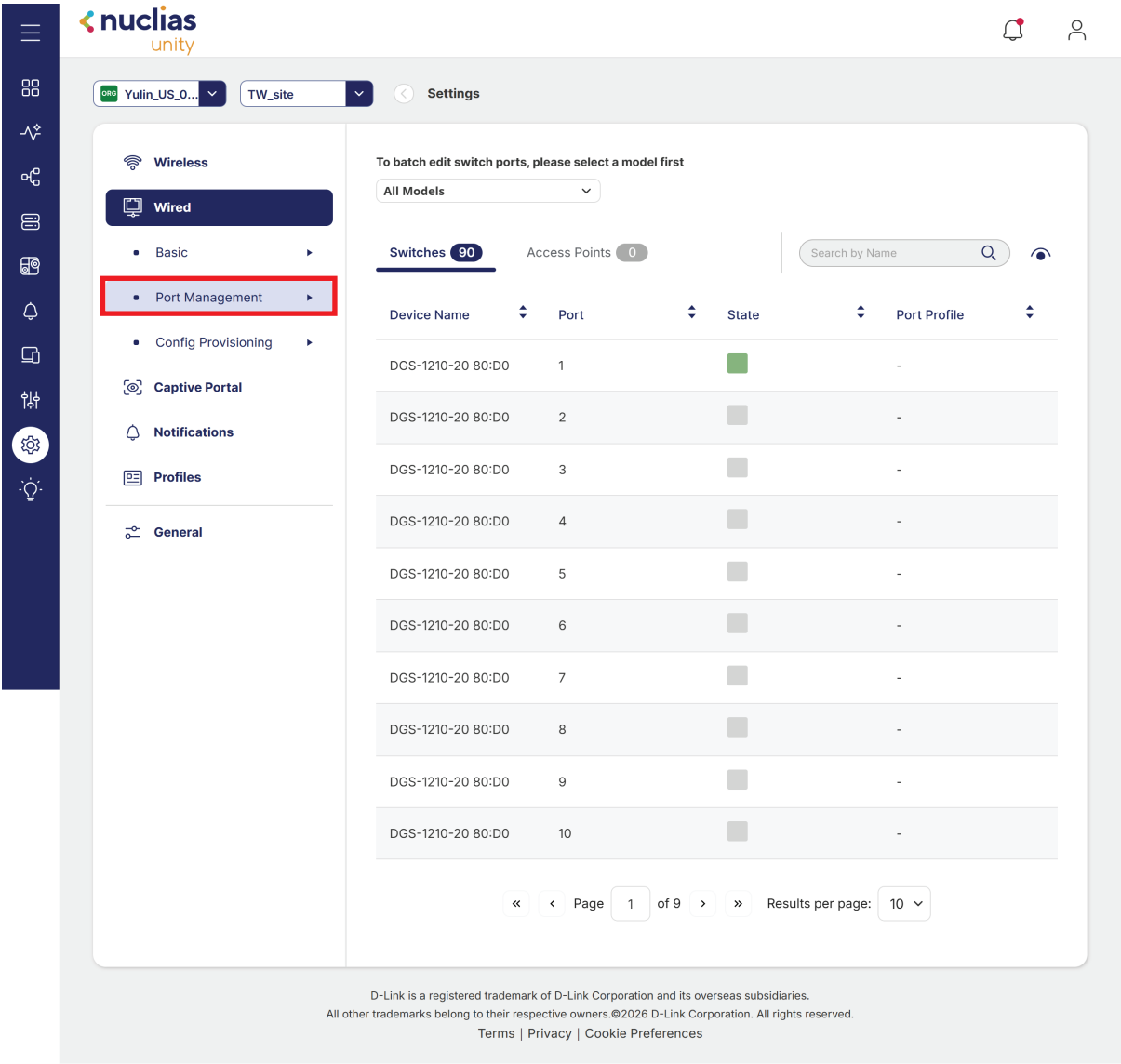
Nuclias Unity

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.

Nuclias Unity Dashboard

Settings

Wired

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.

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:

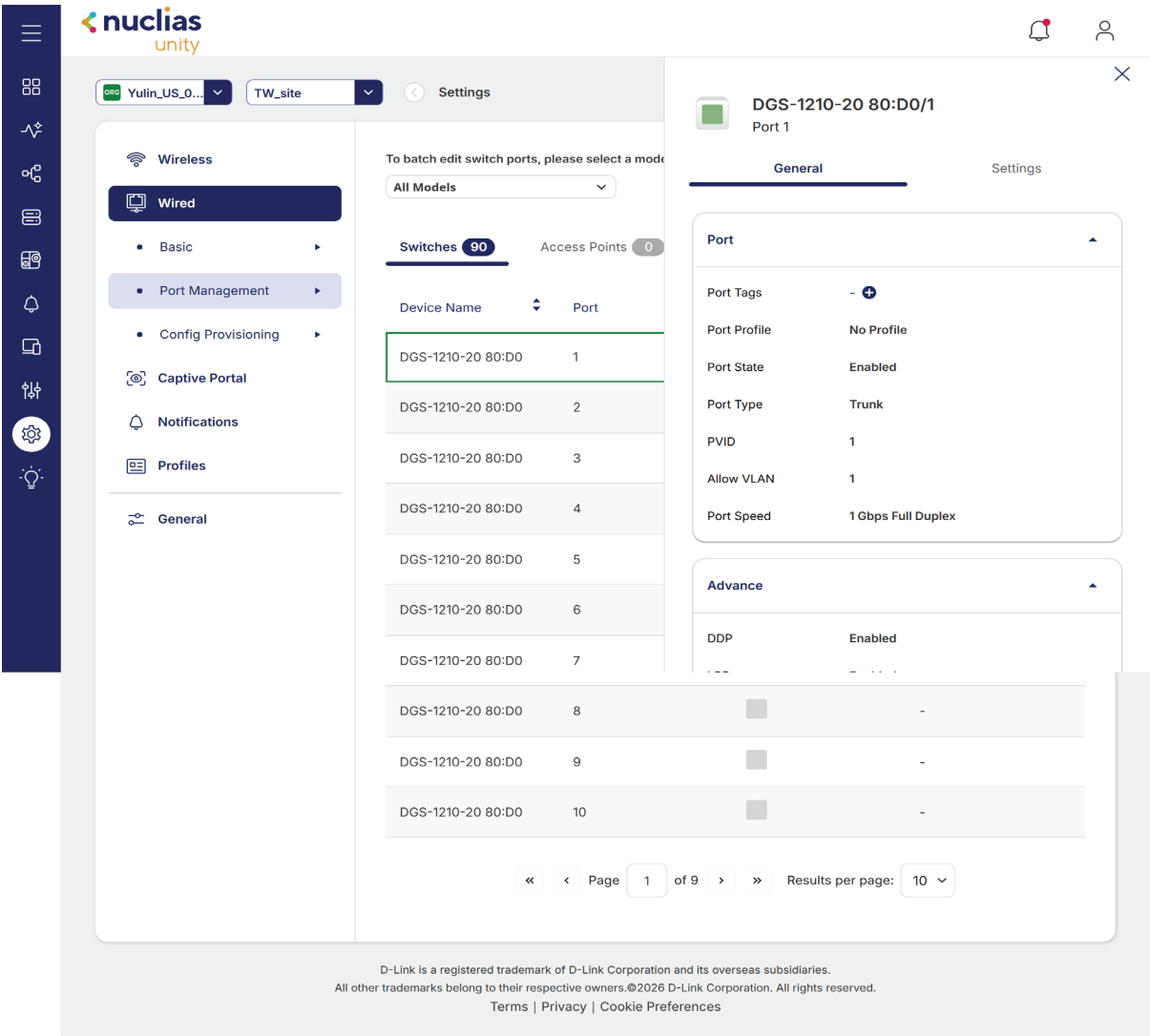
Port Information: Displays basic port details such as port name, port status, link speed, duplex mode, and PVID. This information helps administrators quickly assess the operational state of the port.

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

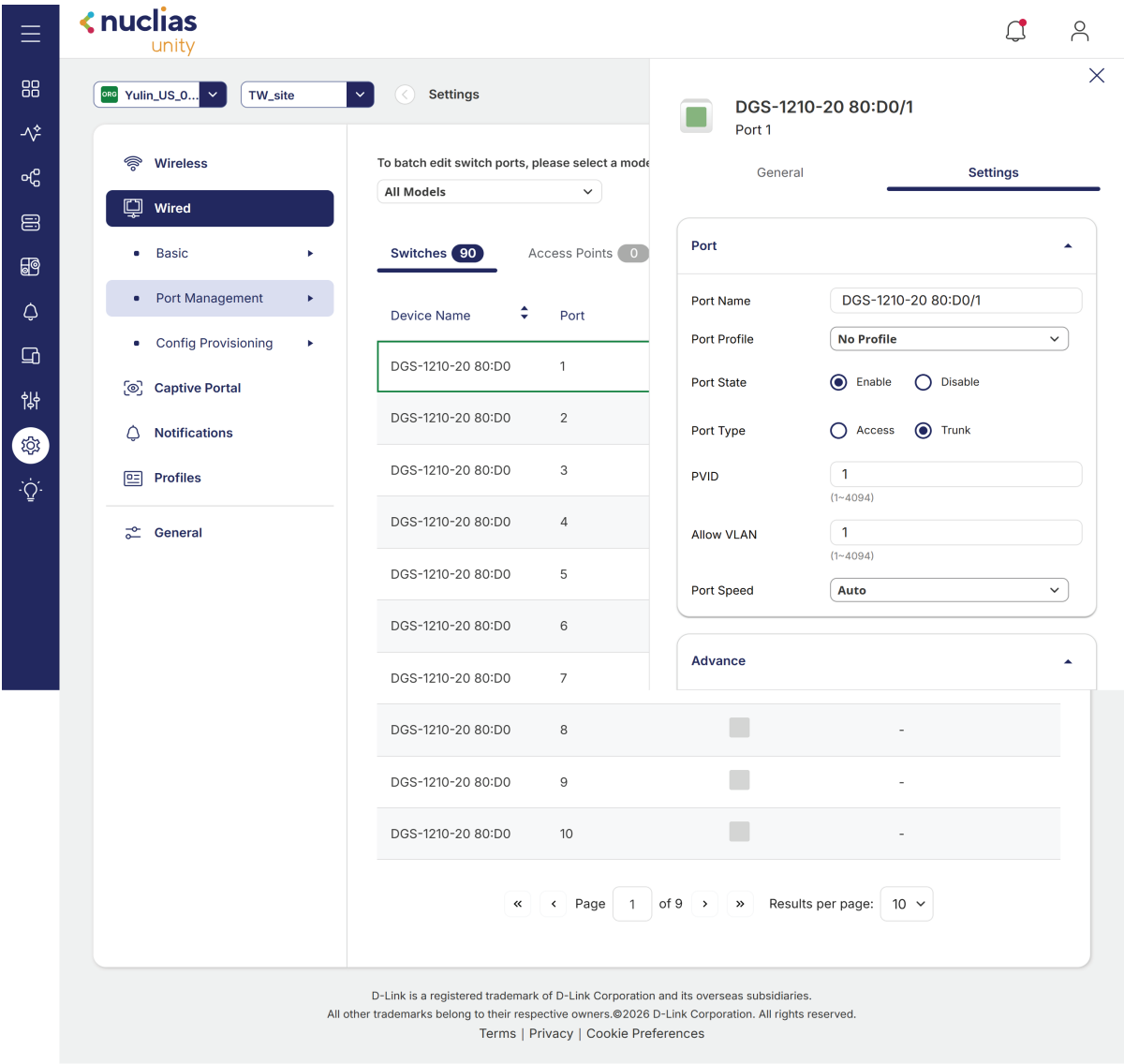
In **Port Management**, after selecting a port, administrators can configure its settings directly within the **Settings** section. The following configuration options are available for modification:

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.



Nuclias Unity Dashboard

Settings

Wired

To configure a port in Nuclias Unity, navigate to **Settings > Port Management**. From this page, you can configure port profiles and assign them to supported switches and access points.

The Port Management page displays the total number of connected switches and access points, allowing you to view and manage the ports of supported devices.

To begin port configuration, select the desired switch or access point model. The available port settings for the selected model will then be displayed for configuration.

The screenshot displays the Nuclias Unity interface. On the left, a vertical sidebar contains navigation icons and labels: Wireless, Wired, Basic, Port Management (highlighted with a red box), Config Provisioning, Captive Portal, Notifications, Profiles, and General. The main content area is titled 'Settings' and shows a message: 'To batch edit switch ports, please select a model first'. Below this, there is a dropdown menu for 'All Models'. The page displays two sections: 'Switches' with a count of 80 and 'Access Points' with a count of 1. A search bar labeled 'Search by Name' is present. A table lists the ports for the selected switch model, DMS-1250-10SP 9D:AB. The table has columns for Device Name, Port, State, and Port Profile. The ports are numbered 1 through 10. The State column shows different colored squares representing the state of each port. The Port Profile column shows a dash '-' for all ports. At the bottom of the table, there is a pagination control showing 'Page 1 of 8' and a 'Results per page' dropdown set to 10. The footer contains legal notices and links for Terms, Privacy, and Cookie Preferences.

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2026 D-Link Corporation. All rights reserved.
[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

Nuclias Unity Dashboard

Settings

Wired

To configure a port, select the desired switch or access point from the drop-down list in the top-left corner of the Port Management page.

Before port configuration, a notification prompts the user to select a device model. Once a supported switch or access point model is selected, the port configuration settings become available. The notification displayed is:

"To batch edit switch ports, please select a model first."

The screenshot displays the Nuclias Unity dashboard interface. On the left is a dark blue sidebar with various icons. The top navigation bar includes the Nuclias logo, a dropdown menu showing 'Yulin_US_0...', another dropdown showing 'TW_site', and a 'Settings' button. The main content area is divided into two sections. The left section contains a sidebar with 'Wireless' and 'Wired' tabs, and sub-sections like 'Basic', 'Port Management', 'Config Provisioning', 'Captive Portal', 'Notifications', 'Profiles', and 'General'. The right section is titled 'Settings' and contains a notification box with the text 'To batch edit switch ports, please select a model first'. Below this notification are two dropdown menus: 'DMS-1250-10SP' and 'Select Device'. The main content area shows a table of switches and access points. The 'Switches' tab is active, showing 10 switches. The table has columns for checkboxes, Device Name, Port, and State. The switches are all 'DMS-1250-10SP 9D:AB' with ports 1 through 10. The states are represented by colored squares: purple, grey, green, and purple. At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Results per page: 10'.

	Device Name	Port	State
☐	DMS-1250-10SP 9D:AB	1	
☐	DMS-1250-10SP 9D:AB	2	
☐	DMS-1250-10SP 9D:AB	3	
☐	DMS-1250-10SP 9D:AB	4	
☐	DMS-1250-10SP 9D:AB	5	
☐	DMS-1250-10SP 9D:AB	6	
☐	DMS-1250-10SP 9D:AB	7	
☐	DMS-1250-10SP 9D:AB	8	
☐	DMS-1250-10SP 9D:AB	9	
☐	DMS-1250-10SP 9D:AB	10	

Batch Commit Change

The **Batch Commit Change** allows you to make multiple configuration changes on a device without applying each change immediately. Instead, all pending changes are stored temporarily and are sent to the device together when you click the Apply icon.

This feature improves configuration efficiency, reduces communication between the Unity server and managed devices, and prevents temporary service interruptions caused by multiple consecutive configuration updates.

How It Works

Without Batch Configuration

- Each time a setting is modified, the Unity server immediately sends the updated configuration to the device.
- The device applies the change instantly.
- If multiple settings are changed, the device receives and processes each change separately.

Example:

- Change the SSID name --> Sent immediately.
- Change the VLAN ID --> Sent immediately.
- Change the security mode --> Sent immediately.
- Change the transmit power --> Sent immediately.

In this example, the device receives four separate configuration updates, which may briefly interrupt wireless service or require multiple configuration reloads.

With Batch Configuration

- Configuration changes are saved as pending changes.
- No settings are sent to the device while you continue making additional modifications.
- When all required changes have been completed, click the Apply icon.
- The Unity server combines all pending modifications into a single configuration package and sends it to the device.
- The device applies all changes at the same time.

Example:

- Change the SSID name.
- Change the VLAN ID.
- Change the security mode.
- Change the transmit power.
- Click Apply.

The Unity server sends one configuration update containing all four changes, allowing the device to apply them in a single operation.

Typical Use Cases

Batch Configuration is particularly useful when:

- Creating or modifying an SSID.
- Updating wireless security settings.
- Changing VLAN assignments.
- Configuring radio settings.
- Editing multiple device parameters at the same time.

Using Batch Configuration ensures that all related settings are applied together, making deployment more efficient and reducing the risk of partial or inconsistent configurations.

To begin batch editing switch ports, ensure that the appropriate switch model is selected. Next, select one or more ports to configure.

Once the desired ports have been selected, click the **Edit** button in the top-left corner to open the Batch Edit configuration page for the selected ports.

The screenshot displays the Nuclias Unity dashboard interface. On the left is a vertical sidebar with various icons. The main content area is titled 'Settings' and shows the 'Wired' configuration page. At the top, there are dropdowns for 'Yulin_US_0...' and 'TW_site'. Below these, a message states: 'To batch edit switch ports, please select a model first'. A dropdown menu shows 'DGS-1250-52X' selected. To the right of this is a 'Select Device' dropdown. Below the message, there is an 'Edit' button (highlighted with a red box) and a 'Switches 52' tab. To the right of the tab is an 'Access Points 1' tab and a search bar labeled 'Search by Name'. Below the tabs is a table with columns: 'Device Name', 'Port', and 'State'. The table contains 10 rows. The first four rows are highlighted with a red box and have a green checkmark in the 'Device Name' column. The remaining six rows have an empty checkbox in the 'Device Name' column. At the bottom of the table, there is a pagination bar showing 'Page 1 of 6' and 'Results per page: 10'.

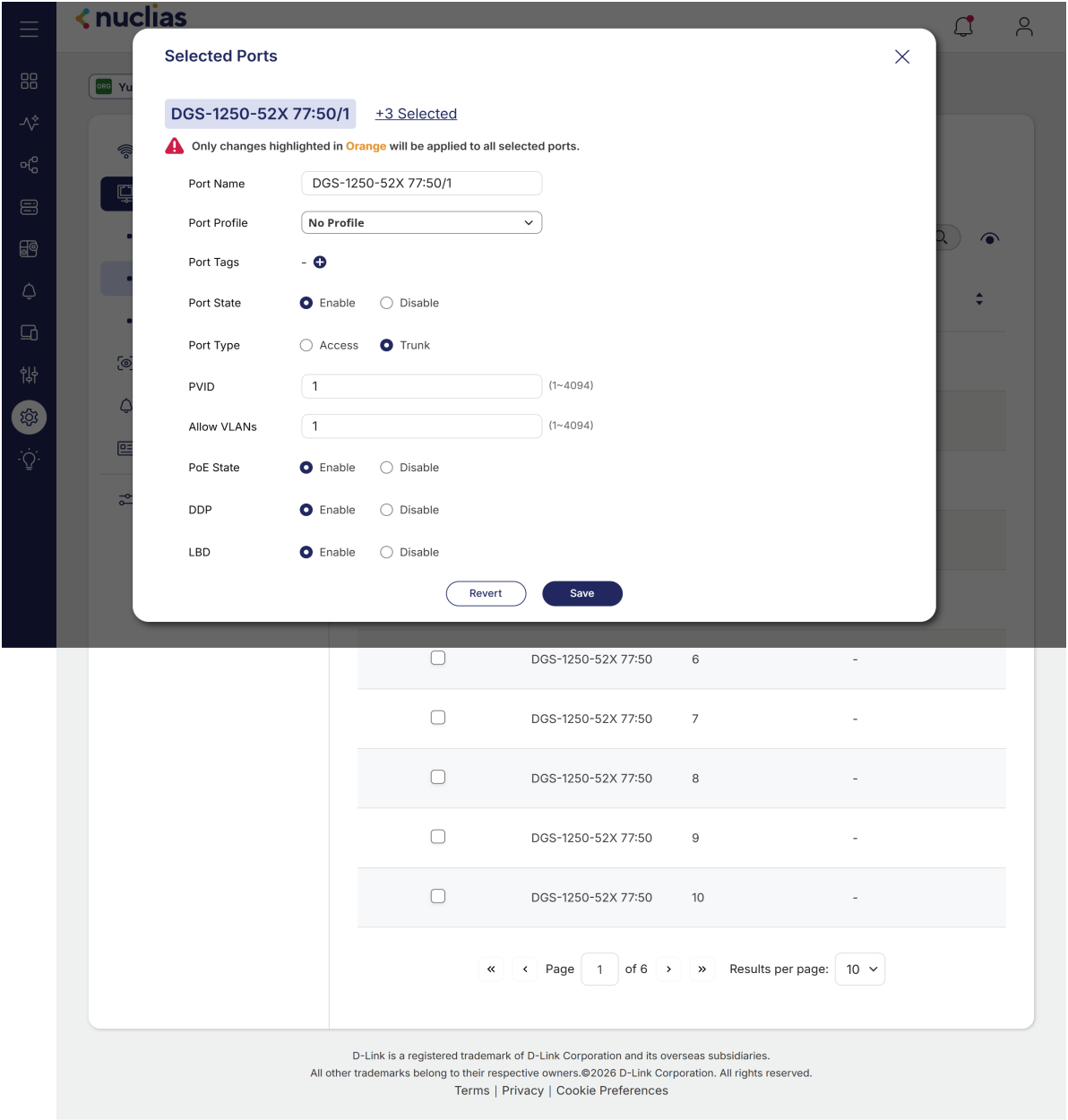
	Device Name	Port	State
☒	DGS-1250-52X 77:50	1	-
☒	DGS-1250-52X 77:50	2	-
☒	DGS-1250-52X 77:50	3	-
☒	DGS-1250-52X 77:50	4	-
☐	DGS-1250-52X 77:50	5	-
☐	DGS-1250-52X 77:50	6	-
☐	DGS-1250-52X 77:50	7	-
☐	DGS-1250-52X 77:50	8	-
☐	DGS-1250-52X 77:50	9	-
☐	DGS-1250-52X 77:50	10	-

« < Page 1 of 6 > » Results per page: 10 ▾

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2026 D-Link Corporation. All rights reserved.
Terms | Privacy | Cookie Preferences

To begin batch editing switch ports, ensure that the appropriate switch model is selected. Next, select one or more ports to configure.

Once the desired ports have been selected, click the **Edit** button in the top-left corner to open the Batch Edit configuration page for the selected ports.

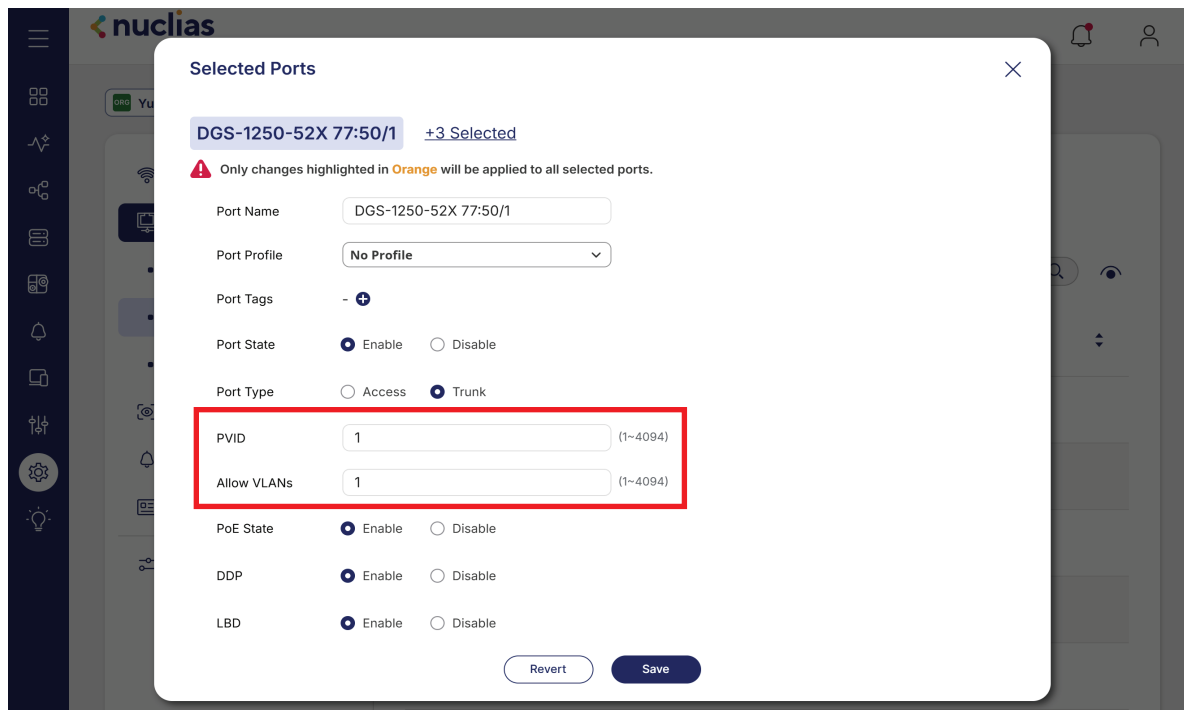


Nuclias Unity Dashboard

Settings

Wired

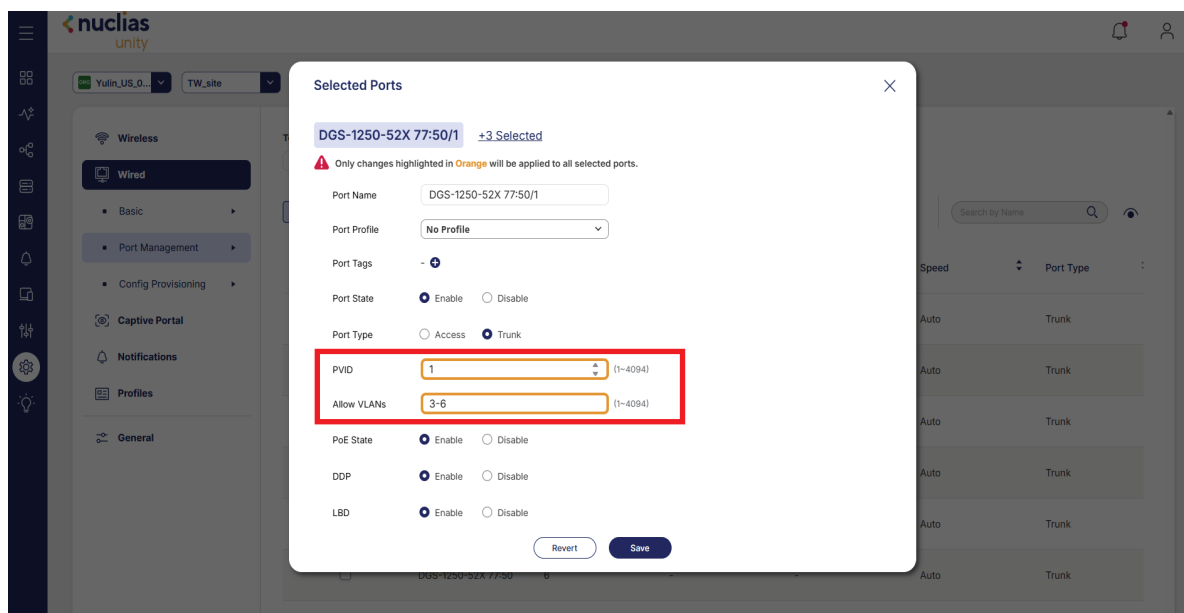
After clicking Edit, the selected switch model and the selected port numbers are displayed in the top-left corner of the Batch Edit page. Configure the required **PVID** and **Allowed VLANs** settings for the selected ports, then click **Save** to save the configuration.



Parameter	Description
Port Name	Specifies a descriptive name for the selected port to simplify identification and management.
Port Profile	Assigns a predefined port profile containing configuration settings that can be applied to the selected port.
Port Tags	Displays or assigns tags to categorize and organize ports for easier management.
Port State	Enables or disables the selected port. A disabled port does not forward network traffic.
Port Type	Defines the operating mode of the port, such as Access, Trunk, or other supported port types.
PVID	Specifies the Port VLAN ID (PVID) assigned to untagged incoming traffic on the port.
Allow VLANs	Defines the VLAN IDs that are permitted to pass through the selected port.
PoE Status	Enables or disables Power over Ethernet (PoE) on supported PoE ports to provide power to connected devices.
DDP	Enables or disables D-Link Discovery Protocol (DDP) for device discovery and management.
LBD	Enables or disables Loopback Detection (LBD) to detect and prevent network loops on the selected port.

Only settings highlighted in orange will be applied to all selected ports. Settings that are not highlighted remain unchanged on the selected ports.

Enter the required **PVID** and **Allowed VLANs** values for the selected ports, then click Save to apply the configuration.

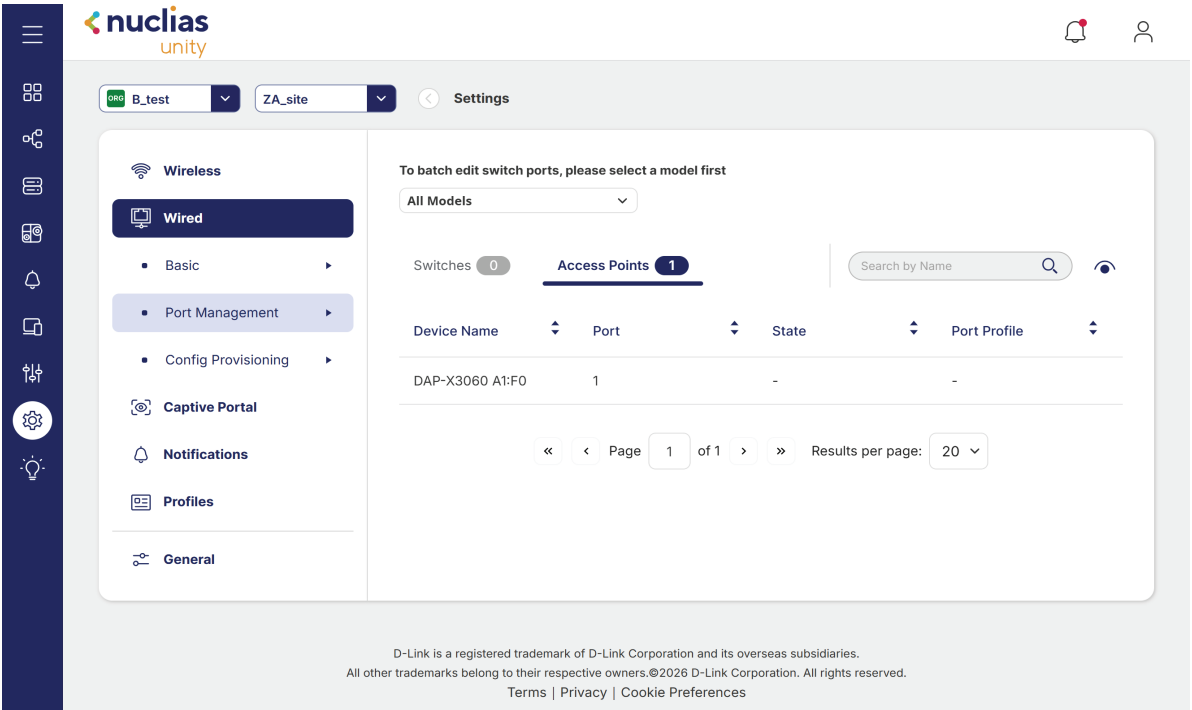


After the configuration is applied, the assigned PVID and VLAN ID is displayed in both the PVID and Allowed VLANs columns for the selected ports.

Once all required changes have been made, click **Apply Changes** to apply the updated configuration to the selected ports. If you do not want to keep the pending changes, click **Discard Changes** to remove all unapplied configuration changes.

[illegible]

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.

In **Port Management**, select any access point to view all the information in the **General** section. This section provides a comprehensive overview of the port and Device information.

Port

The Port section displays the VLAN and profile configuration for each switch port.

Port Tags – Displays the VLAN tagging mode configured for the port, indicating whether VLAN traffic is transmitted as tagged or untagged.

Port Profile – Displays the port profile assigned to the port. A port profile applies predefined network settings, such as VLAN membership and other port configurations.

PVID – Displays the Port VLAN ID (PVID) assigned to the port. The PVID determines the VLAN to which incoming untagged traffic is assigned.

Allowed VLANs – Displays the list of VLANs that are permitted to pass through the port. Only traffic associated with the configured VLANs is allowed on the port.

Device

The Device section displays general information about the selected device.

Device Name – Displays the name assigned to the device.

MAC Address – Displays the unique Media Access Control (MAC) address of the device.

Model – Displays the device model number.

Hardware Version – Displays the hardware revision of the device.

Firmware Version – Displays the currently installed firmware version.

The screenshot displays the Nuclias Unity dashboard interface. On the left is a dark blue sidebar with various navigation icons. The main content area is divided into two sections. The left section, titled 'Settings', contains a list of configuration categories: Wireless, Wired (selected), Basic, Port Management (selected), Config Provisioning, Captive Portal, Notifications, Profiles, and General. The right section, titled 'DAP-X3060 A1:F0/1 Port 1', shows the configuration for a specific port. It includes a 'General' tab and a 'Settings' tab. The 'General' tab displays the following information:

Port	
Port Tags	- +
Port Profile	No Profile
PVID	1
Allow VLAN	1

Below the 'Port' section is the 'Device' section, which displays the following information:

Device	
Device Name	DAP-X3060 A1:F0
MAC Address	BC:22:28:E7:A1:F0
Model	DAP-X3060
Hardware	A1

At the bottom of the dashboard, there is a footer with the following text: 'D-Link is a registered trademark of D-Link Corporation. All other trademarks belong to their respective owners. ©2026 Terms | Privacy | Cookie Pre'.

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

Settings

The Settings section allows you to configure the basic settings for the port profile.

Profile Name – Specifies the name of the port profile.

Port Profile – Selects the type of port profile to apply to the port.

PVID – Specifies the Port VLAN ID (PVID) used to assign incoming untagged traffic to a VLAN.

Allowed VLANs – Specifies the VLANs that are permitted to pass through the port. Only traffic associated with the selected VLANs is allowed on the port.

The screenshot displays the Nuclias Unity web interface. On the left is a dark blue sidebar with navigation icons. The main content area is titled 'Settings' and includes a breadcrumb trail: 'B_test' > 'ZA_site' > 'Settings'. Below the breadcrumb, there are tabs for 'Wireless' and 'Wired', with 'Wired' being the active tab. Under 'Wired', there are sub-tabs: 'Basic', 'Port Management', 'Config Provisioning', 'Captive Portal', 'Notifications', 'Profiles', and 'General'. The 'Port Management' sub-tab is selected, showing a table of access points. The table has columns for 'Device Name' and 'Port'. One entry is visible: 'DAP-X3060 A1:F0' with port '1'. To the right of the table is a detailed configuration panel for 'DAP-X3060 A1:F0/1 Port 1'. This panel has two tabs: 'General' and 'Settings', with 'Settings' being the active tab. The 'Settings' tab contains a 'Basic' section with the following fields: 'Port Name' (DAP-X3060 A1:F0/1), 'Port Profile' (No Profile), 'PVID' (1, with a range of 1~4094), and 'Allow VLAN' (1, with a range of 1~4094). At the bottom of the page, there is a footer with legal disclaimers and links for Terms, Privacy, and Cookie Policy.

D-Link is a registered trademark of D-Link Corporation
All other trademarks belong to their respective owners. ©2026
Terms | Privacy | Cookie Pre

The batch port configuration procedure for access points is the same as for switches. Select the desired access point model, choose the ports to configure, modify the required settings, and click Save. After completing all changes, click **Apply Changes** to apply the configuration or **Discard Changes** to remove any pending changes.

To configure access point ports, navigate to **Settings > Port Management**. Select Access Point, then choose the desired access point model from the top-right corner of the page.

The screenshot displays the Nuclias Unity web interface. On the left is a dark blue sidebar with various icons and a menu. The main content area is titled 'Settings' and features a dropdown menu for 'DAP-X3060' (highlighted with a red box) and a 'Select Device' dropdown. Below this, there are tabs for 'Switches' (142) and 'Access Points' (1, highlighted with a red box). A table lists the selected device 'DAP-X3060 F6:F0' with port '1'. The page footer includes a disclaimer about D-Link trademarks and copyright information.

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.©2026 D-Link Corporation. All rights reserved.
Terms | Privacy | Cookie Preferences

Nuclias Unity Dashboard

Settings

Wired

The batch port configuration procedure for access points is the same as for switches. Select the desired access point model, choose the ports to configure, modify the required settings, and click Save. After completing all changes, click **Apply Changes** to apply the configuration or **Discard Changes** to remove any pending changes.

To configure access point ports, navigate to **Settings > Port Management**. Select Access Point, then choose the desired access point model from the top-right corner of the page.

The screenshot shows the Nuclias Unity Settings page. On the left sidebar, the 'Wired' section is expanded, and 'Port Management' is selected. The main content area shows the 'Access Points' tab with a table of devices. The 'DAP-X3060' model is selected, and the table lists the device name 'DAP-X3060 F6:F0' and port '1'. The 'Edit' button is visible next to the device name.

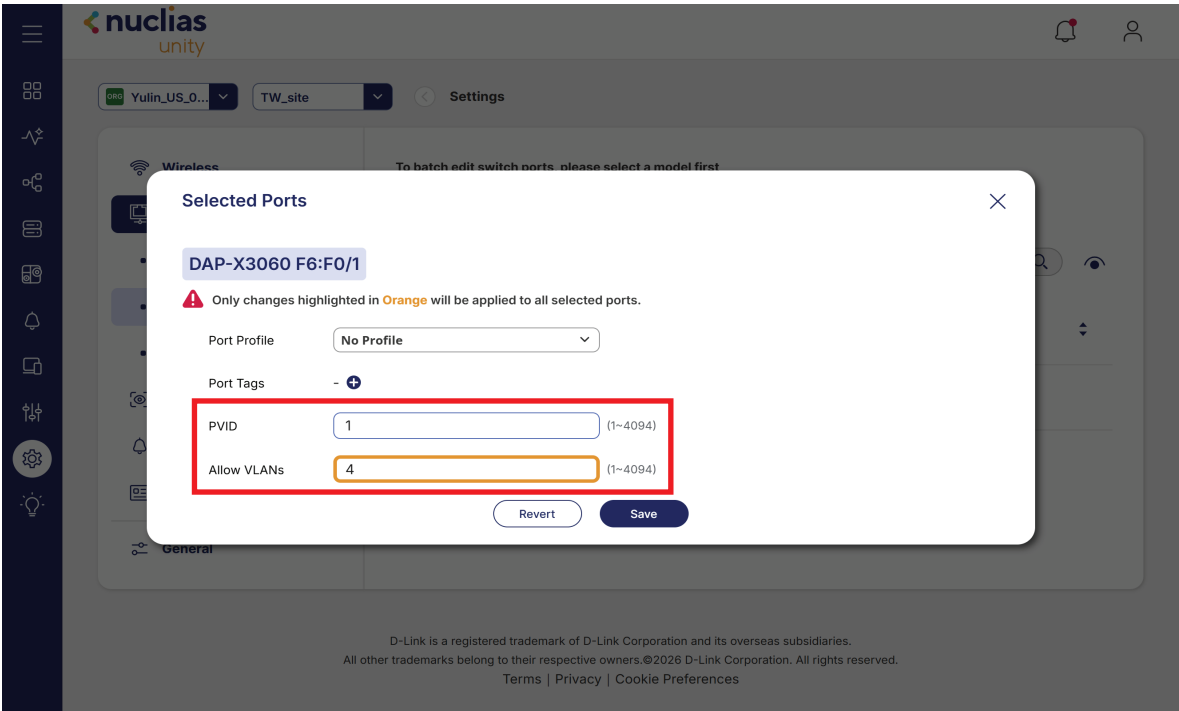
Device Name	Port	State
DAP-X3060 F6:F0	1	-

After selecting the desired access point port(s), click **Edit** to configure the port settings. Modify the required parameters, then click Save to save the configuration.

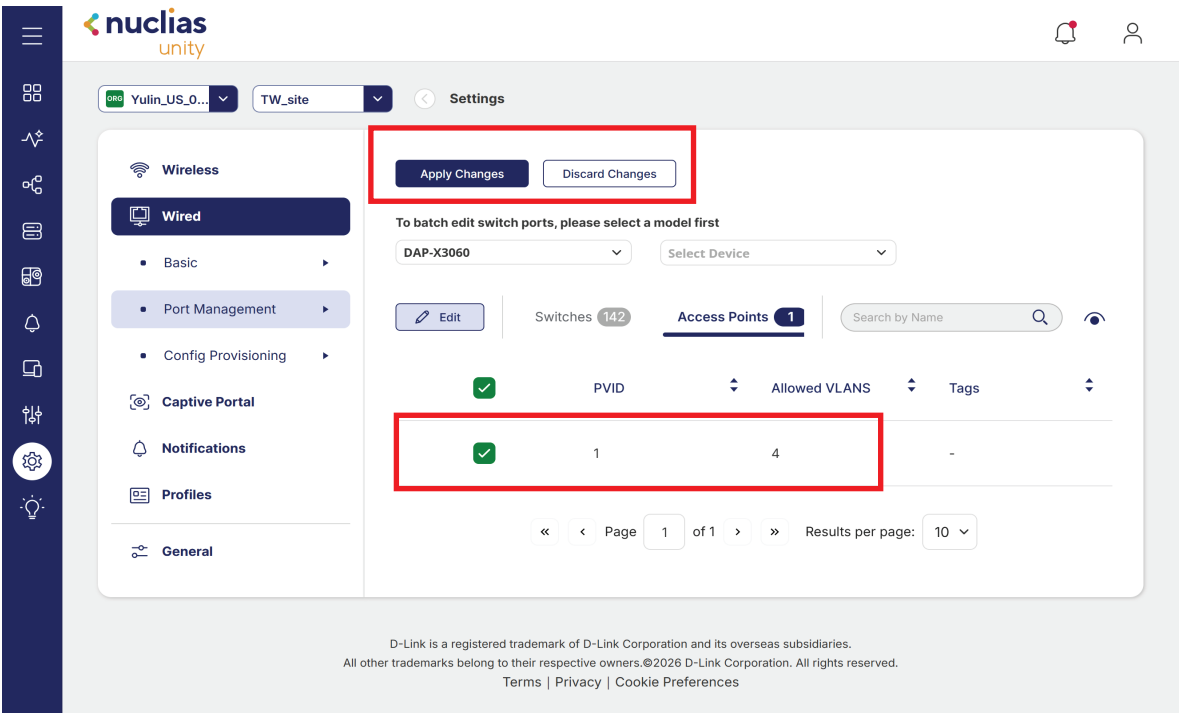
The screenshot shows the Nuclias Unity Settings page. On the left sidebar, the 'Wired' section is expanded, and 'Port Management' is selected. The main content area shows the 'Access Points' tab with a table of devices. The 'DAP-X3060' model is selected, and the table lists the device name 'DAP-X3060 F6:F0' and port '1'. The 'Edit' button is visible next to the device name.

Device Name	Port	State
DAP-X3060 F6:F0	1	-

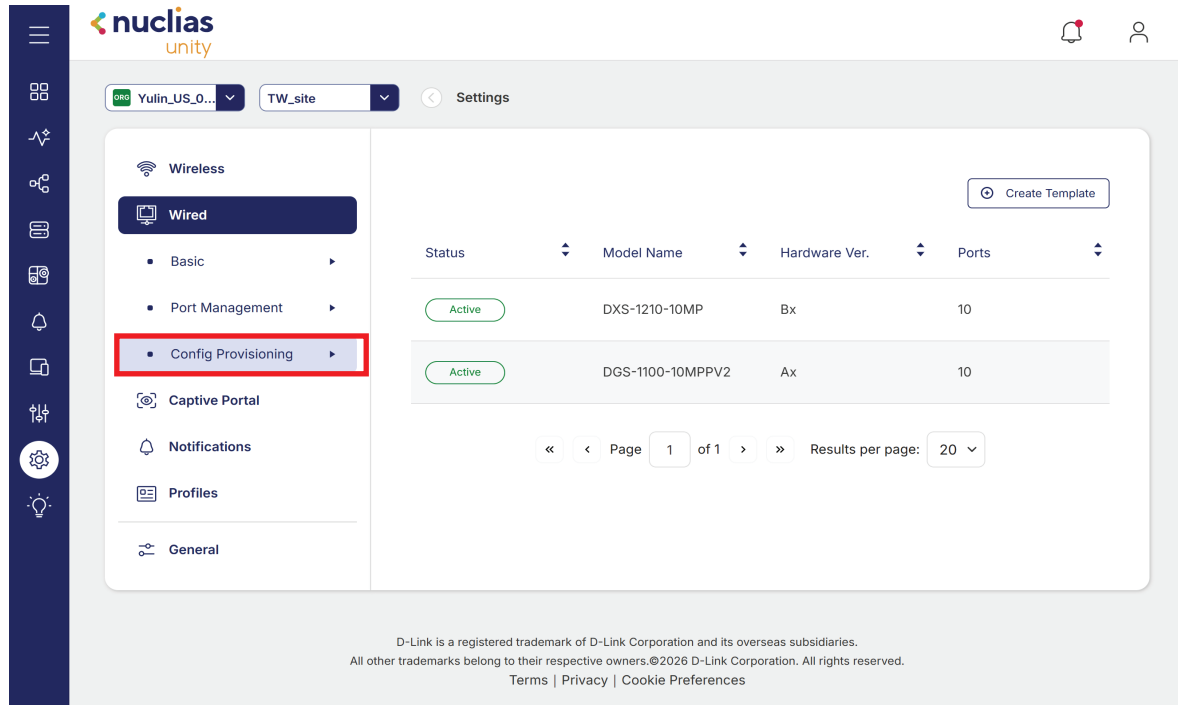
Enter the required **PVID** and **Allowed VLANs** values for the selected access point port, then click **Save** to save the configuration.



The configured **PVID** and **Allowed VLANs** values are displayed in the corresponding **PVID** and **Allowed VLANs** columns. After verifying the configuration, click **Apply Changes** to apply the new settings. To remove any pending changes without applying them, click **Discard Changes**.



The **Config Provision** section allows you to assign a port profile template to a specific port on a selected switch or access point. After the configuration is saved and provisioned, the template settings are automatically deployed to the assigned port on the selected switch or access point.



In Config Provision under the Wired section, administrators can view and configure the following parameters for Switches and Access Points:

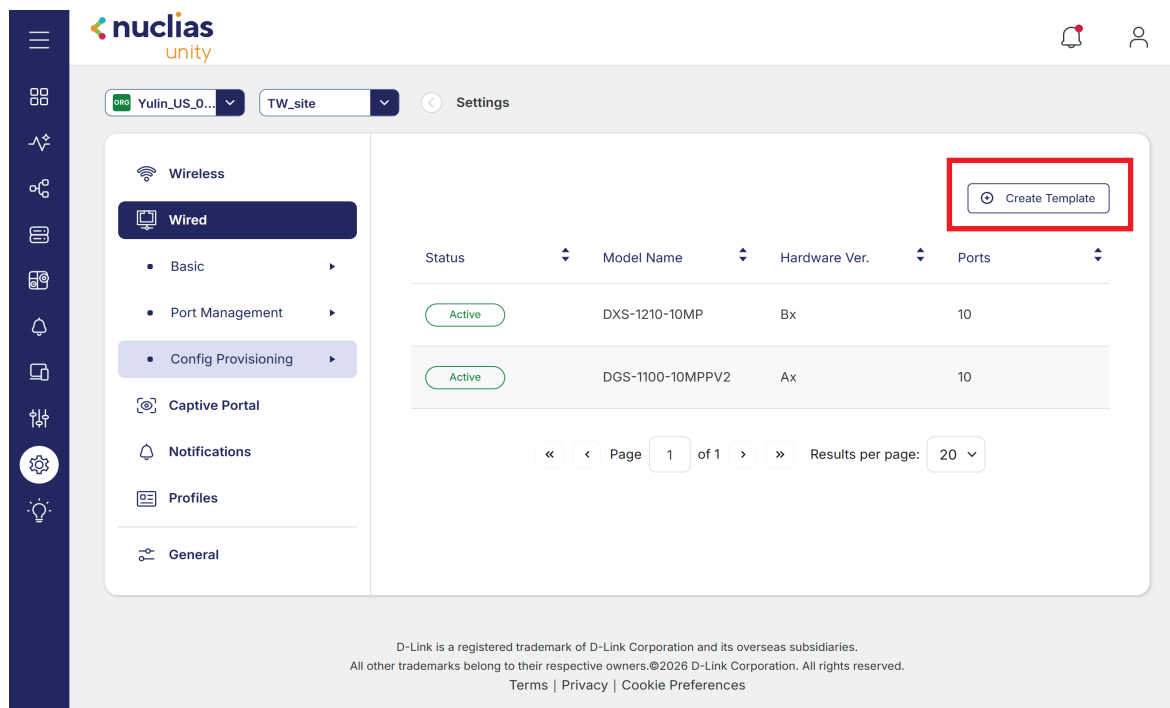
Parameter	Description
Status	Displays the current provisioning status of the assigned port profile on the selected device.
Model Name	Displays the model name of the selected switch or access point.
Hardware Version	Displays the hardware revision of the selected device.
Ports	Displays the port(s) on the selected device to which the port profile template is assigned.
Action	Provides options to manage the provisioning entry, such as editing or removing the assigned port profile.

Nuclias Unity Dashboard

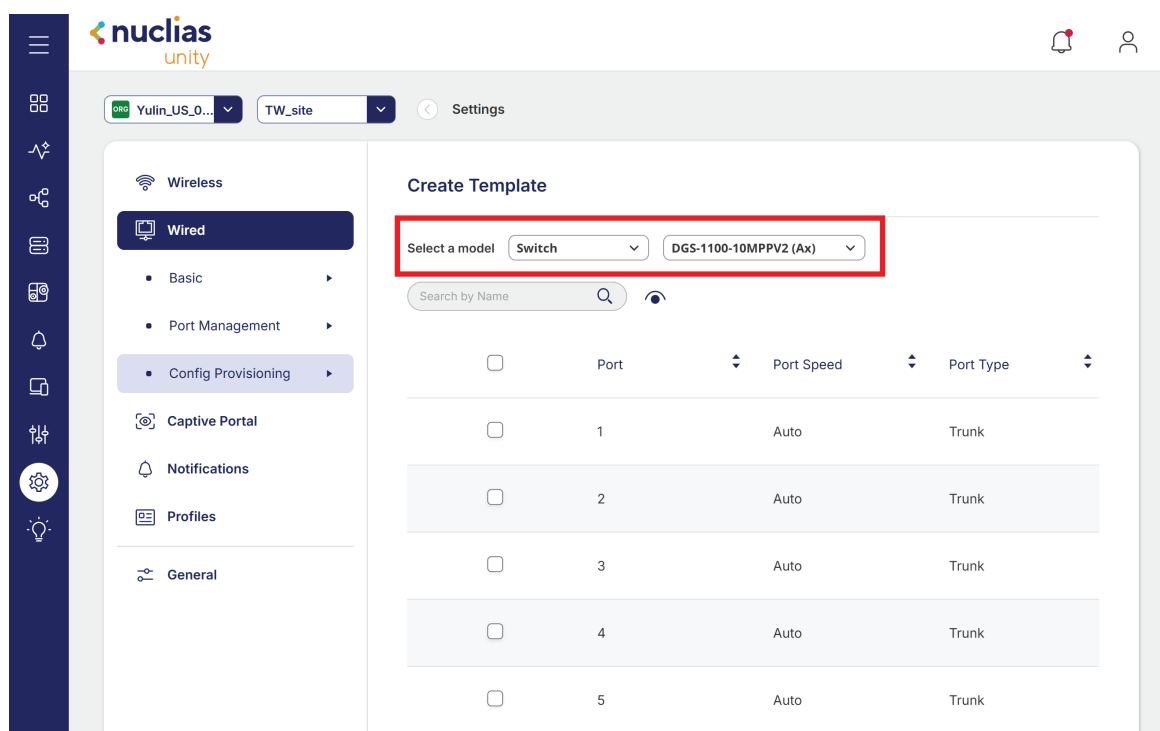
Settings

Wired

The Create Template section allows you to create a new port profile template that can be applied to ports on supported switches and access points. Configure the required settings, such as the profile name, port profile, PVID, and allowed VLANs, then save the template for future provisioning.



Create Template allows you to create a new port profile template for supported devices. To begin, select the device Category, such as Switch, Router, or Access Point, and then choose the corresponding device Model. The available configuration options are based on the selected device model. After selecting the category and model, configure the required port profile settings and save the template. The saved template can then be provisioned and applied to compatible ports on supported devices.



Nuclias Unity Dashboard

Settings

Wired

In Config Provision under the Wired section, administrators can view and configure the following parameters for Switches, Routers and Access Points:

Parameter	Description
Port	Selects the physical port on the device to which the port profile template will be applied.
Port Speed	Displays or configures the operating speed of the selected port, such as Auto, 10 Mbps, 100 Mbps, 1 Gbps, or higher, depending on the device model.
Port Type	Specifies the port operating mode, such as Access, Trunk, or Hybrid, depending on the device's supported features.
Aggregate	Displays or configures the link aggregation group (LAG) assigned to the port, if supported.
PVID	Specifies the Port VLAN ID (PVID) used to assign incoming untagged traffic to a VLAN.
Allowed VLANs	Specifies the VLANs that are permitted to pass through the port. Only traffic associated with the selected VLANs is allowed.
PoE	Enables or disables Power over Ethernet (PoE) on the selected port, allowing power to be supplied to compatible powered devices.
PoE Power Usage	Displays the current power consumption of the connected PoE device on the selected port.
RSTP	Enables or disables Rapid Spanning Tree Protocol (RSTP) on the port to help prevent network loops while providing fast network convergence.
LBD	Enables or disables Loopback Detection (LBD) to detect and prevent Layer 2 network loops caused by incorrect cabling or configuration.
DDP	Enables or disables D-Link Discovery Protocol (DDP) to allow the device to discover and exchange information with other compatible D-Link devices.
LLDP	Enables or disables Link Layer Discovery Protocol (LLDP) to advertise and discover information about directly connected network devices.
STP Guard	Configures Spanning Tree Protocol (STP) Guard features to protect the network from topology changes or unauthorized devices that could affect STP operation.

Yulin_US_0... TW_site Settings

Wireless

Wired

- Basic
- Port Management
- Config Provisioning**

Captive Portal

Notifications

Profiles

General

Create Template

Select a model Switch DGS-1100-10MPPV2 (Ax)

	Port	Port Speed	Port Type
☐	1	Auto	Trunk
☒	2	Auto	Trunk
☐	3	Auto	Trunk
☐	4	Auto	Trunk
☐	5	Auto	Trunk
☐	6	Auto	Trunk
☐	7	Auto	Trunk
☐	8	Auto	Trunk
☐	9	-	Trunk
☐	10	-	Trunk

<< < Page 1 of 1 > >> Results per page: 20

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners.©2026 D-Link Corporation. All rights reserved.

[Terms](#) | [Privacy](#) | [Cookie Preferences](#)

Nuclias Unity Dashboard

Settings

Wired

After selecting a port, configure the required port settings, such as Port Type, PVID, and Allowed VLANs. You can also configure additional port parameters, including port speed, PoE, and other supported features. In the Advanced section, you can enable or disable features such as D-Link Discovery Protocol (DDP) and Loopback Detection (LBD) for the selected port.

Port

The Port section allows you to view and configure the settings for the selected port.

Port Name – Specifies the name or description assigned to the port for easy identification

Port Profile – Displays or selects the port profile applied to the port. The port profile contains predefined network settings that can be assigned to one or more ports.

Port State – Enables or disables the selected port. When disabled, the port does not transmit or receive network traffic.

Port Type – Specifies the operating mode of the port, such as Access, Trunk, or Hybrid, depending on the supported device model.

PVID – Specifies the Port VLAN ID (PVID) used to assign incoming untagged traffic to the designated VLAN.

Allowed VLANs – Specifies the VLANs that are permitted to pass through the port. Only traffic associated with the configured VLANs is allowed.

Port Speed – Configures the operating speed and duplex mode of the port, or allows the device to automatically negotiate the optimal connection speed with the connected device.

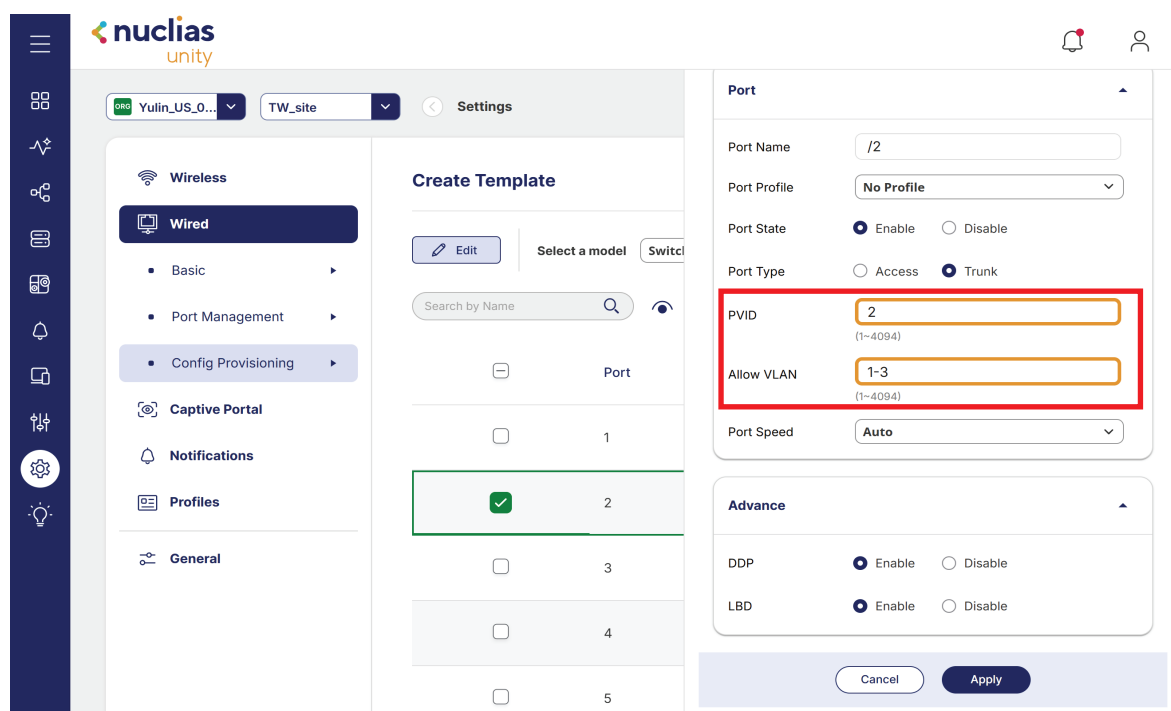
Advanced

The Advanced section allows you to configure additional features for the selected port.

DDP – Enables or disables D-Link Discovery Protocol (DDP), allowing the device to discover and exchange information with other compatible D-Link devices.

LBD – Enables or disables Loopback Detection (LBD) to detect and prevent Layer 2 network loops caused by incorrect cabling or network configuration.

After configuring the required settings, click **Apply** to save the port profile template. The template can then be provisioned and assigned to supported switches or access points.



After completing all the required port configuration changes, click **Save** to apply and store the new settings for the selected port.

The screenshot displays the 'Create Template' configuration page in the Nuclias Unity interface. The left sidebar contains navigation options: Wireless, Wired (selected), Basic, Port Management, Config Provisioning, Captive Portal, Notifications, Profiles, and General. The main content area is titled 'Create Template' and includes an 'Edit' button, a 'Select a model' dropdown set to 'Switch', and a 'DGS-1100-10MPPV2 (Ax)' dropdown. Below these is a search bar and a table of 10 ports. The table has columns for 'Port', 'Port Speed', and 'Port Type'. Port 2 is selected with a green checkmark. The 'Save' button at the bottom is highlighted with a red box.

Port	Port Speed	Port Type
1	Auto	Trunk
2	Auto	Trunk
3	Auto	Trunk
4	Auto	Trunk
5	Auto	Trunk
6	Auto	Trunk
7	Auto	Trunk
8	Auto	Trunk
9	-	Trunk
10	-	Trunk

Page 1 of 1 Results per page: 20

Cancel Save

D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries.
All other trademarks belong to their respective owners. ©2026 D-Link Corporation. All rights reserved.
Terms | Privacy | Cookie Preferences

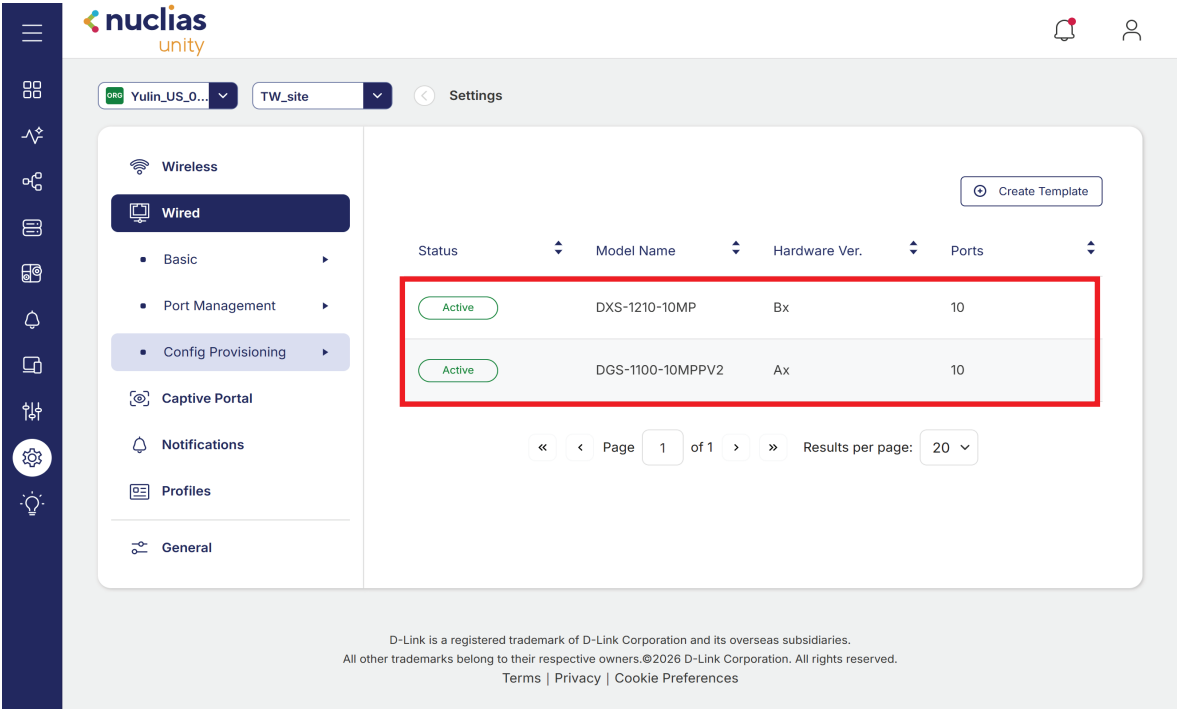
Nuclias Unity

Dashboard

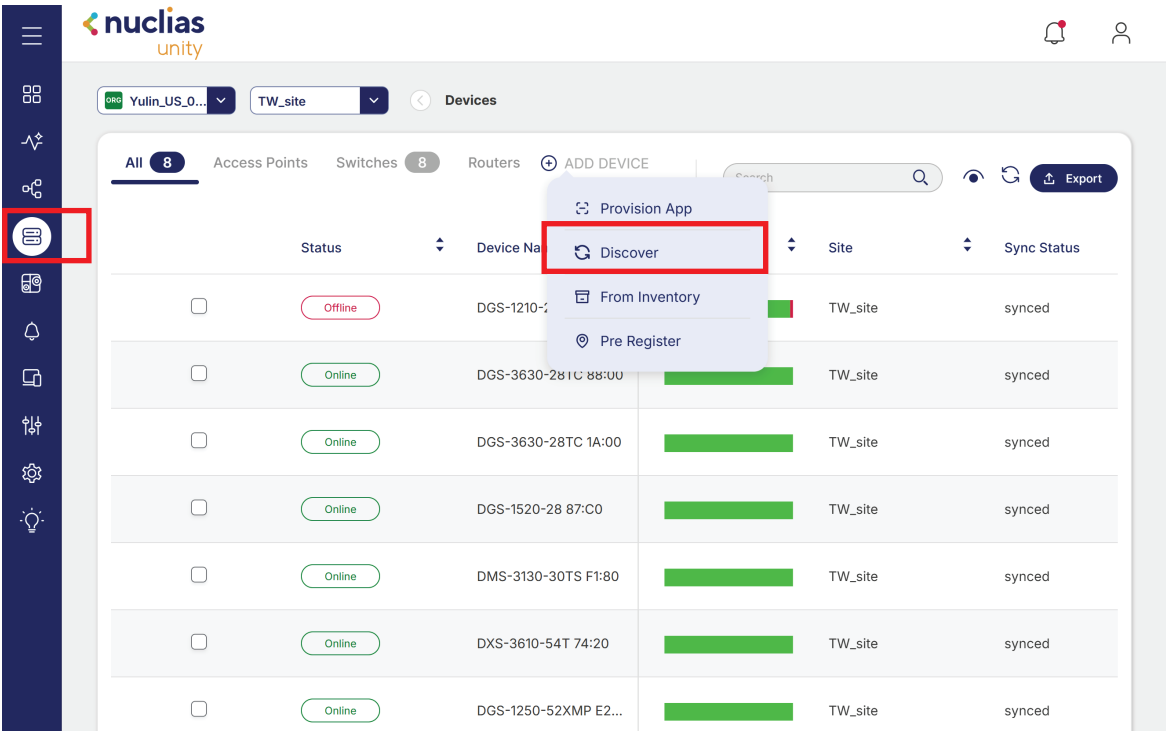
Settings

Wired

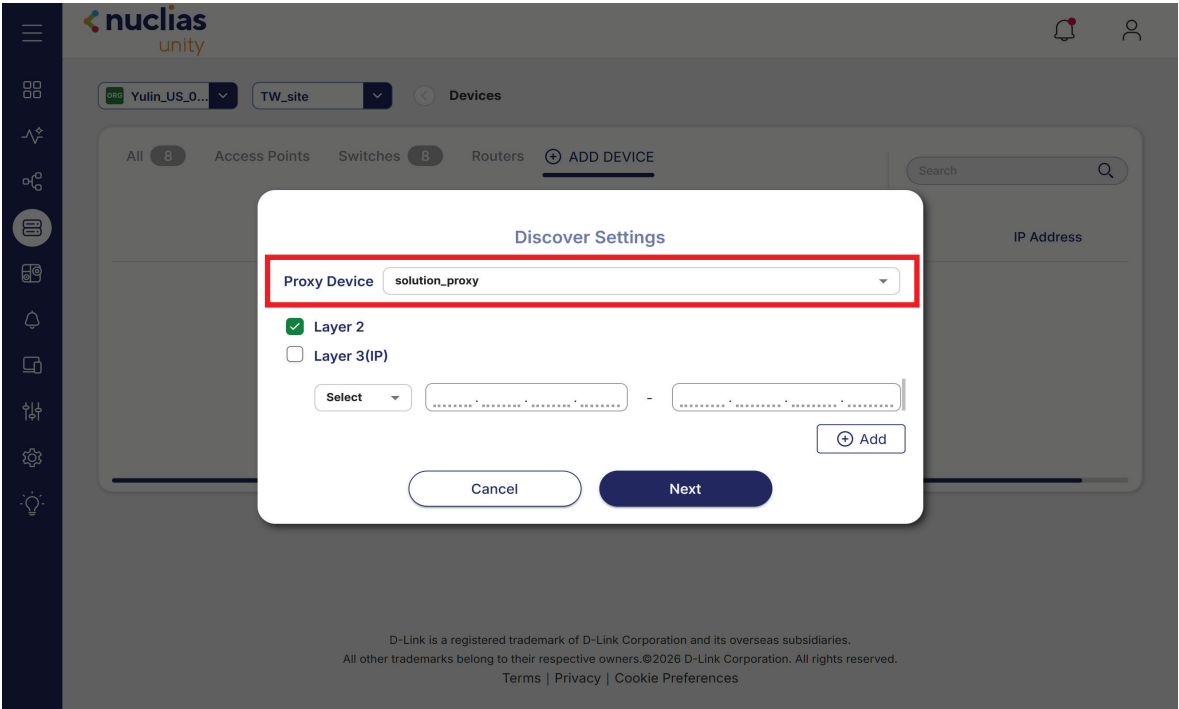
After the template is saved successfully, the newly created port profile appears in the Config Provision section, where it can be assigned and provisioned to supported switches or access points.



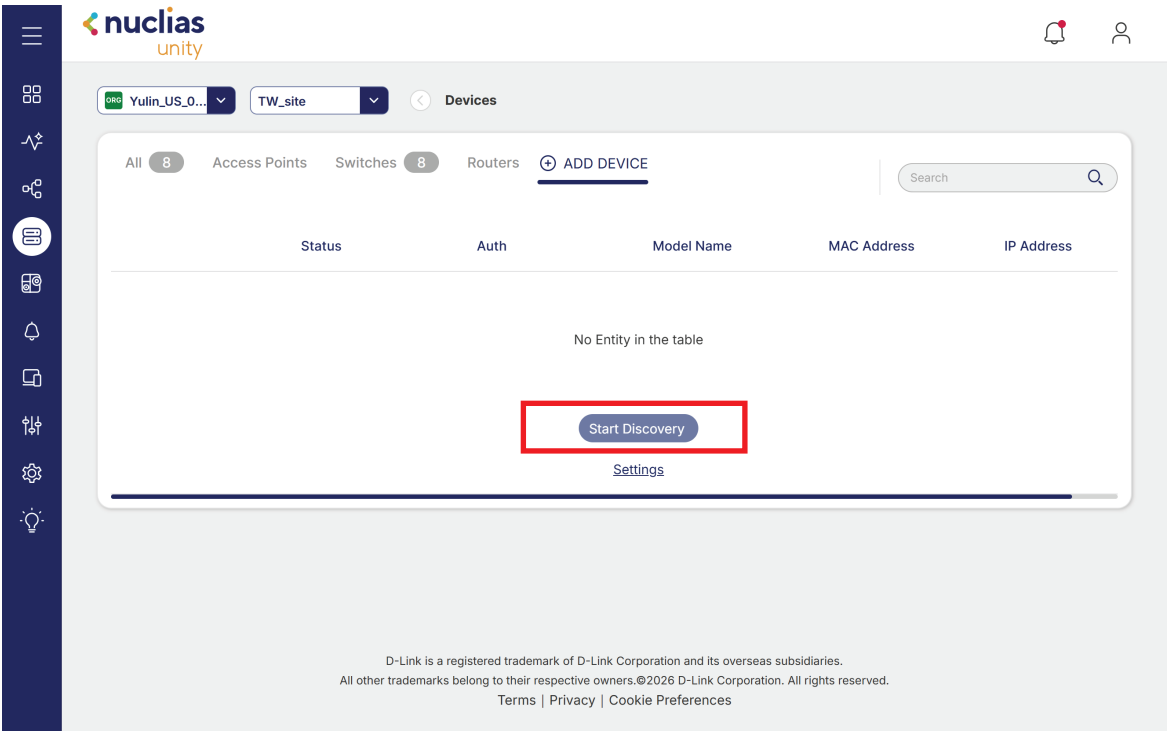
From the left-side navigation menu, select **Devices**, then click **Add Device** and choose the **Discover** option.



When you click Discover, the **Discovery Settings** dialog box appears. Select the Proxy Device, choose the discovery method by selecting Layer 2 or Layer 3, and then click Next to continue.



Click **Start Discovery** to scan the network and discover supported devices connected through the selected proxy device. Once the discovery process is complete, the detected devices are displayed in the results list for review and addition.



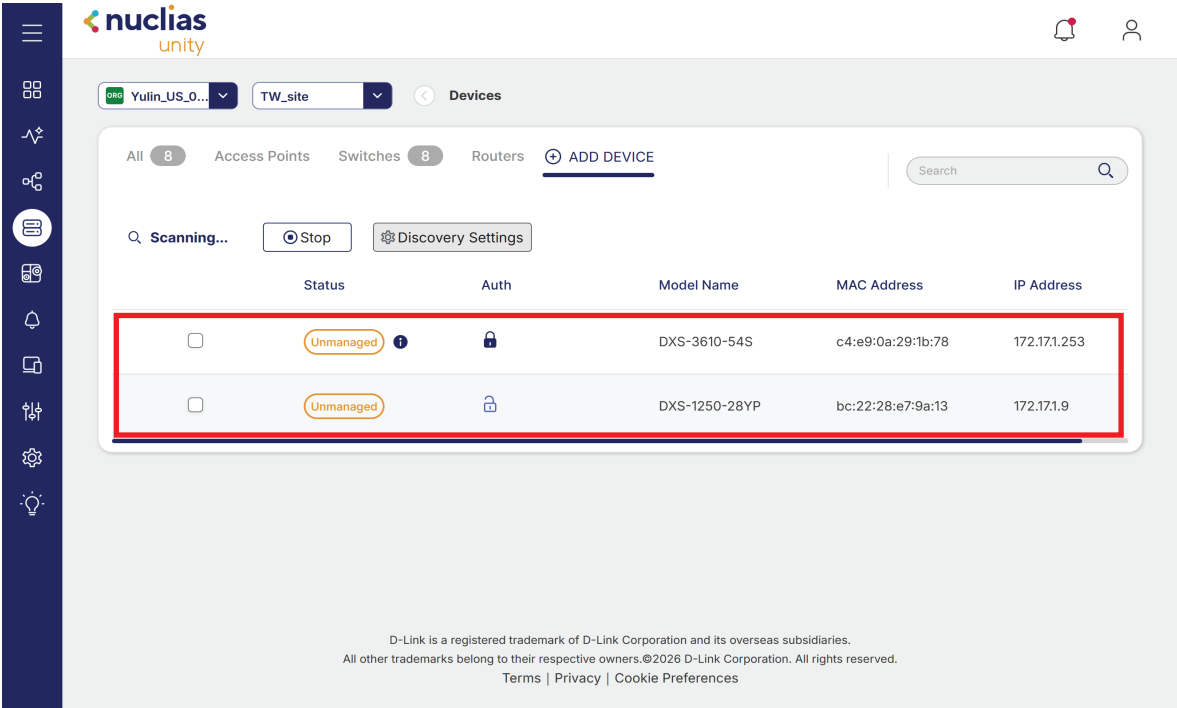
Nuclias Unity

Dashboard

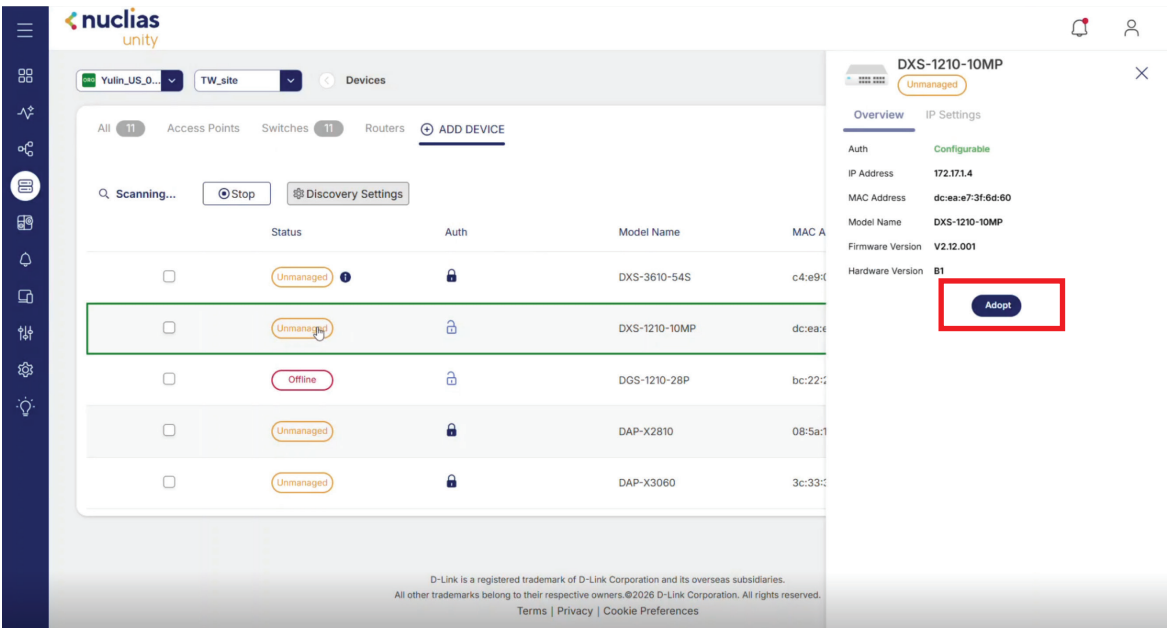
Settings

Wired

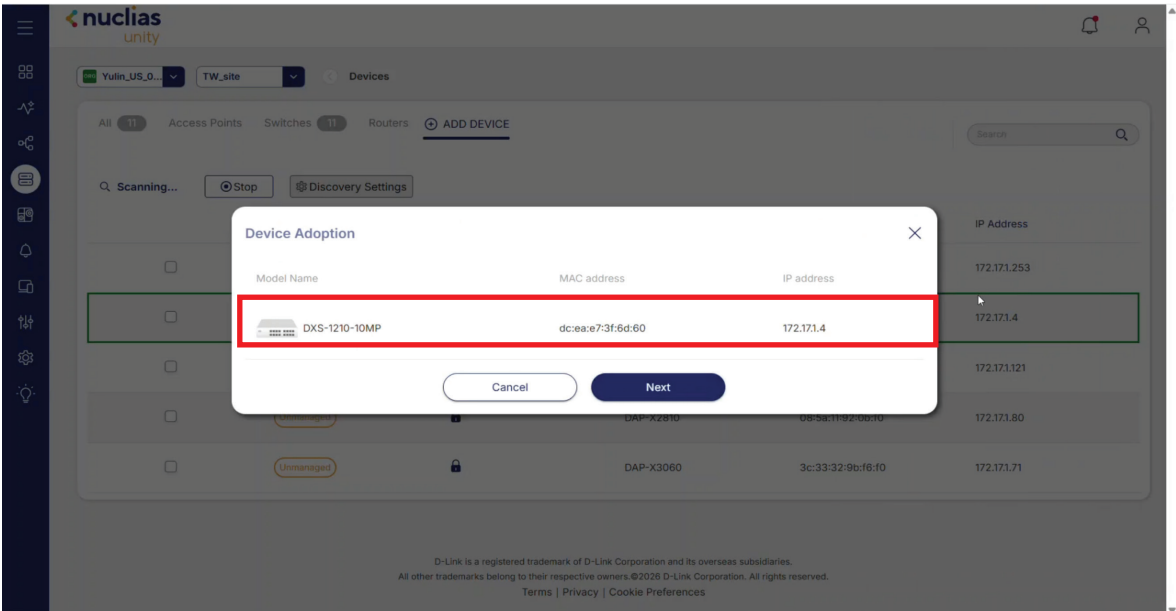
After the discovery process is complete, the detected devices are displayed in the results list with an **Unmanaged** status, indicating that they have been discovered but are not yet managed by the system.



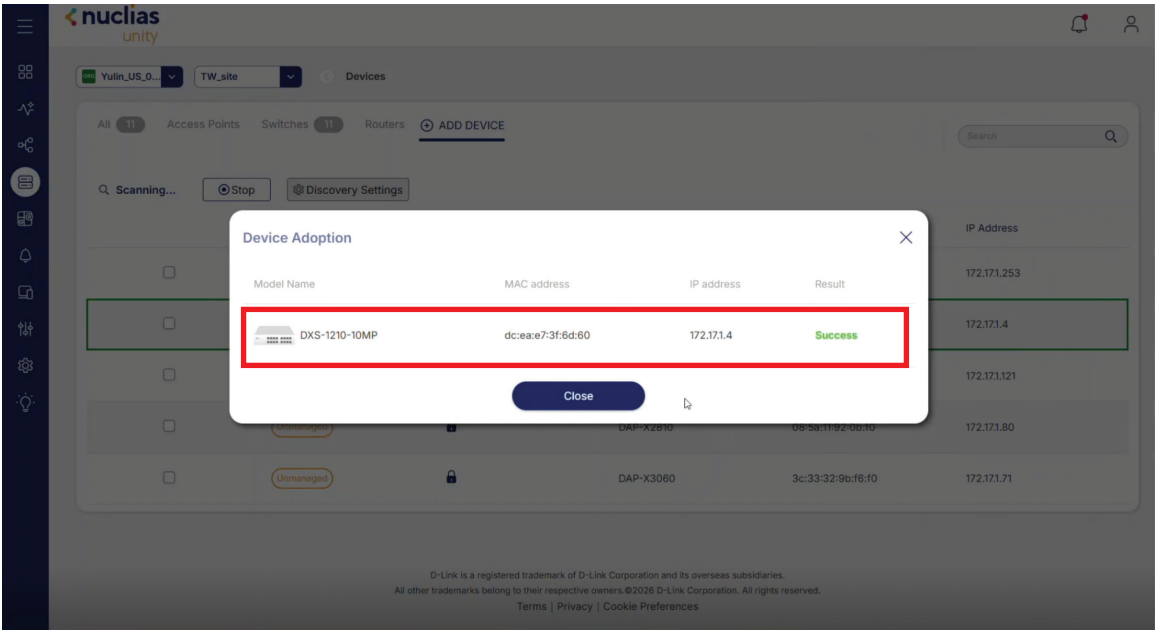
Select the device that you want to manage with Nuclias Unity, then click **Adopt**. The selected device is moved into the current organization and site, allowing it to be managed by Nuclias Unity.



The **Device Adoption** dialog displays the information for the selected device, including the **Model Name**, **MAC Address**, and **IP Address**. Review the device details, then proceed with the adoption process to add the device to Nuclias Unity.



After the adoption process is complete, wait a few minutes or refresh the web page. If the adoption is successful, the device status changes to **Success**, indicating that the device has been successfully adopted and is now managed by Nuclias Unity.



Nuclias Unity Dashboard

Settings

Wired

Navigate back to Settings, then go to Wired > Config Provision. Select the newly created port profile template to view its configuration and provision it to the desired device ports.

The screenshot shows the Nuclias Unity Settings page, specifically the 'Wired' > 'Config Provision' section. The left sidebar contains navigation options: Wireless, Wired (selected), Basic, Port Management, Config Provisioning (selected), Captive Portal, Notifications, Profiles, and General. The main content area displays a table of port profile templates. The table has columns for Status, Model Name, Hardware Ver., and Ports. The row for 'DGS-1100-10MPPV2' is highlighted with a red box. Below the table, there are pagination controls showing 'Page 1 of 1' and 'Results per page: 20'.

Status	Model Name	Hardware Ver.	Ports
Active	DXS-1210-10MP	Bx	10
Active	DGS-1100-10MPPV2	Ax	10

In the Config Provision section, locate the desired port profile template and click the Edit icon in the Action column. The template opens, allowing you to view or modify its configuration settings as required.

The screenshot shows the Nuclias Unity Settings page, specifically the 'Wired' > 'Config Provision' section. The left sidebar is the same as the previous screenshot. The main content area displays the 'Create Template' dialog. The 'Port' tab is selected, and the 'PVID' and 'Allow VLAN' fields are highlighted with a red box. The 'PVID' field is set to '2' and the 'Allow VLAN' field is set to '1-3'. The 'Port' tab also shows a list of ports (1-5) with checkboxes. The 'Advance' section shows 'DDP' and 'LBD' settings, both set to 'Enable'.

Create Template

Search by Name

Port

1

2

3

4

5

Port

Port Name: /2

Port Profile: No Profile

Port State: ☒ Enable ☐ Disable

Port Type: ☐ Access ☒ Trunk

PVID: 2 (1-4094)

Allow VLAN: 1-3 (1-4094)

Port Speed: Auto

Advance

DDP: ☒ Enable ☐ Disable

LBD: ☒ Enable ☐ Disable

Cancel Apply

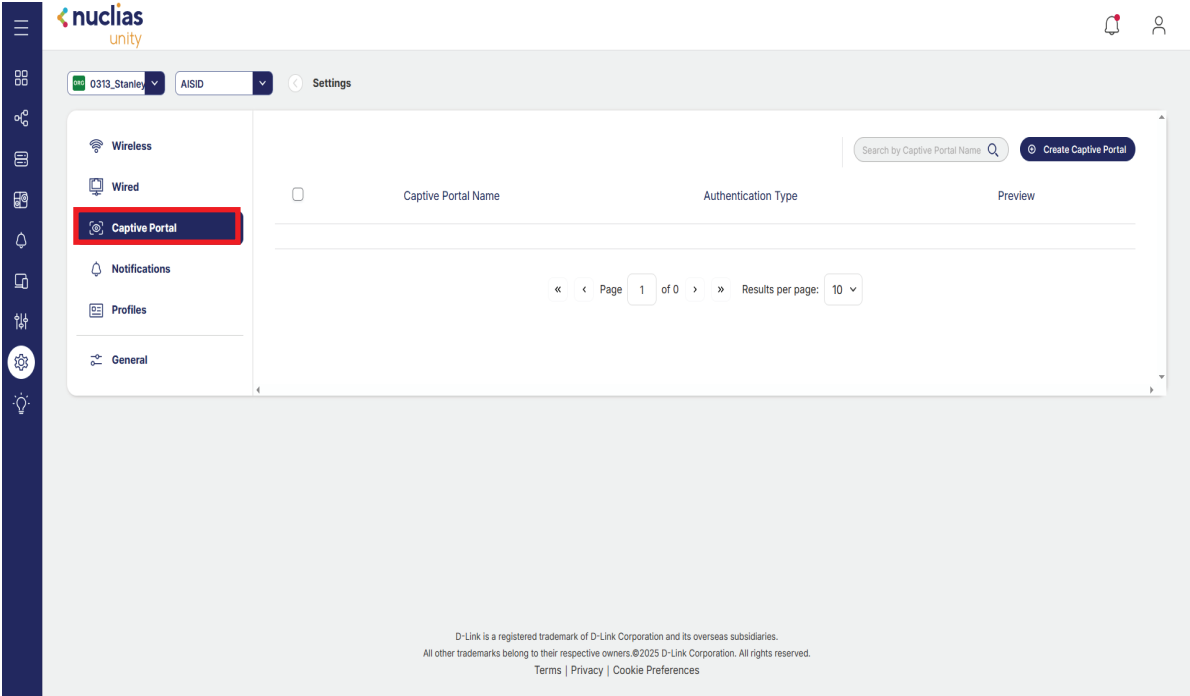
Nuclias Unity

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.

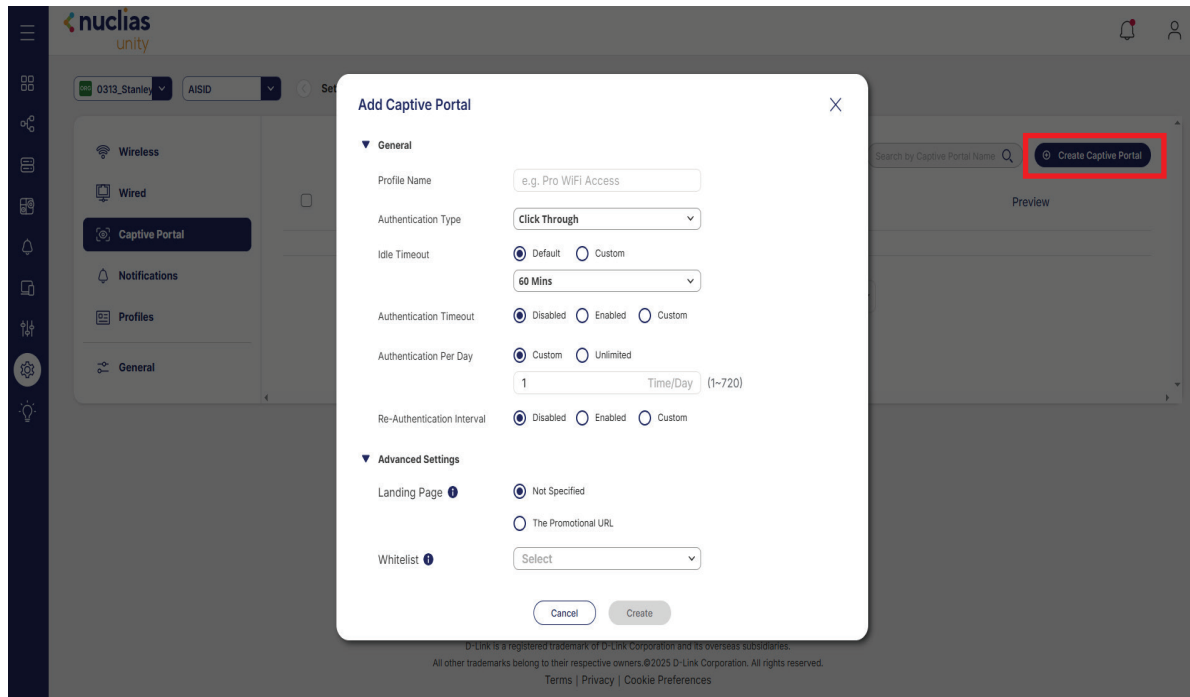
Nuclias Unity Dashboard

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.

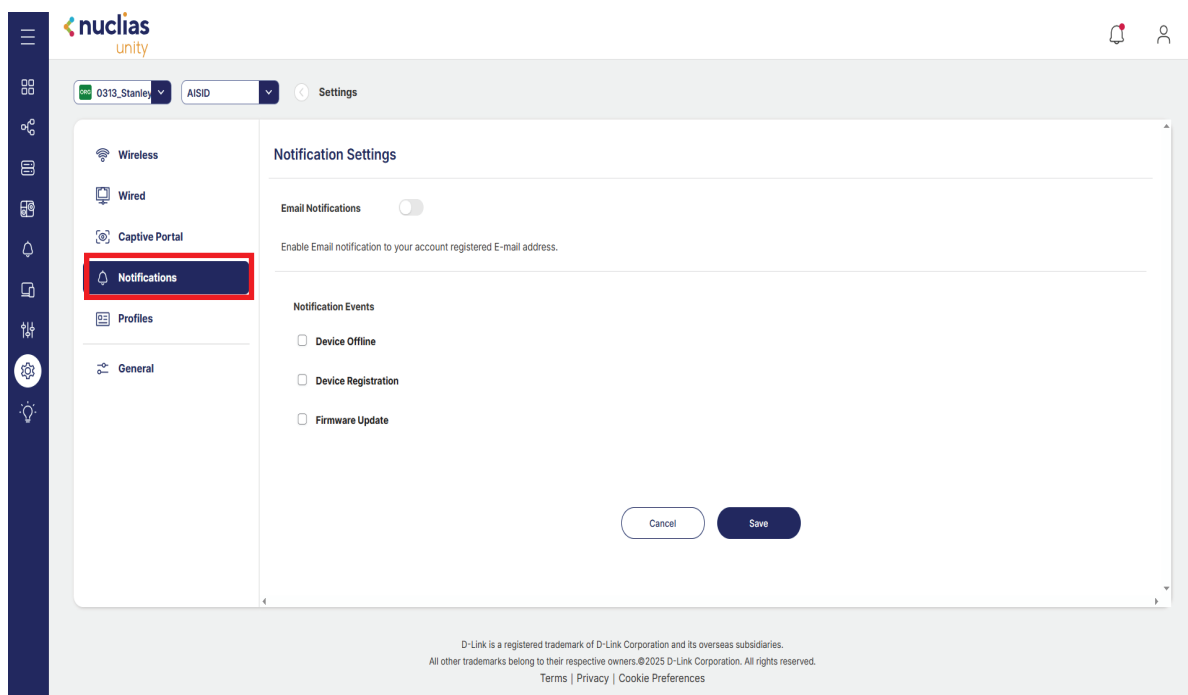
Email Notification: Enables or disables email alerts for system events and network notifications. When enabled, administrators can configure recipient email addresses and define which events trigger email alerts to ensure timely awareness of network activities.

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.

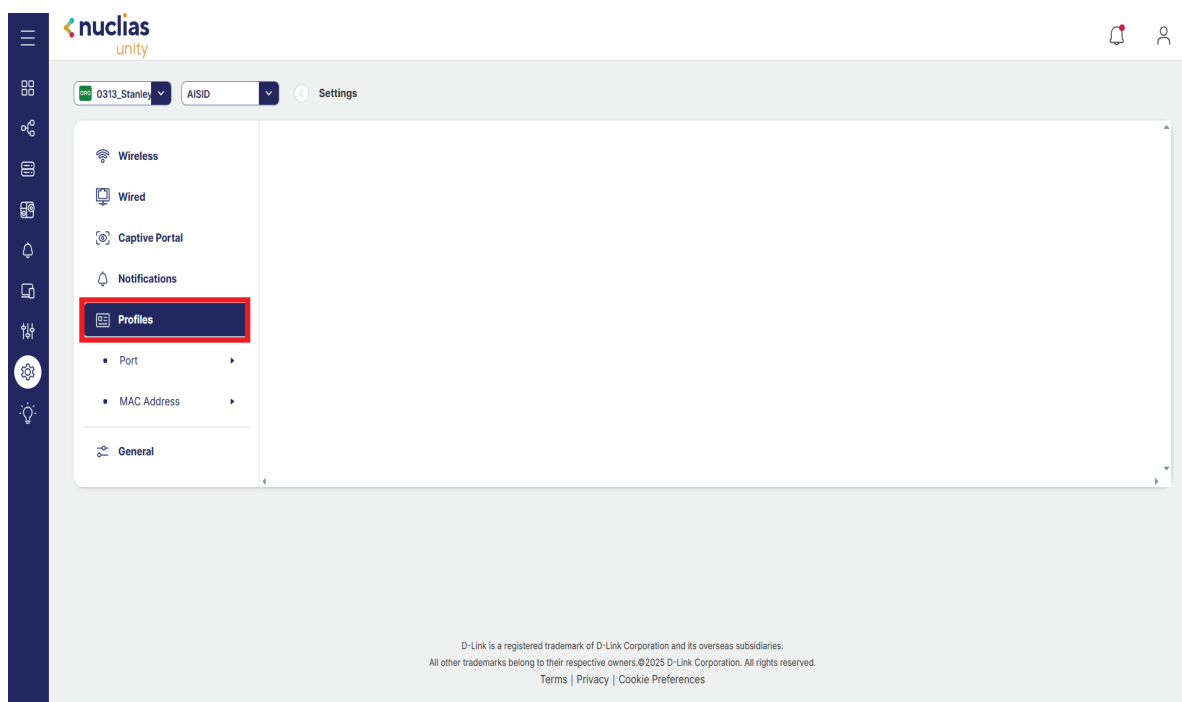


Nuclias Unity Dashboard

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.

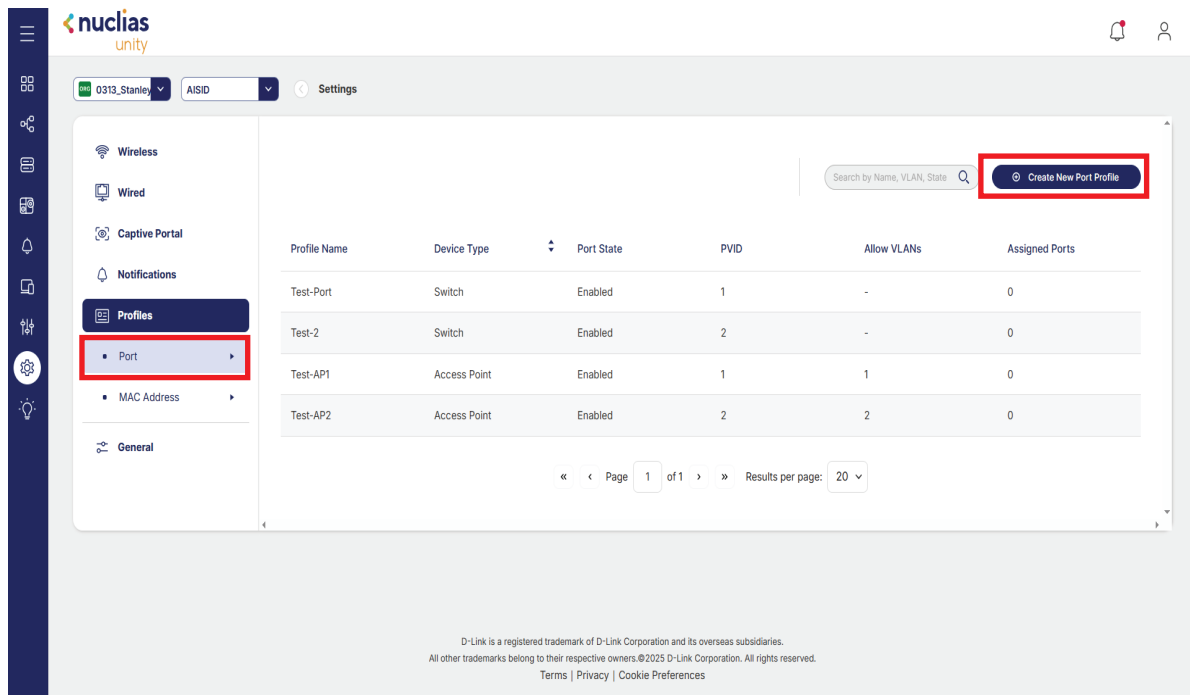


Nuclias Unity Dashboard

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.

Nuclias Unity Dashboard

Settings

Profiles

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.

The screenshot shows the 'Create New Port Profile' dialog box in the Nuclias Unity interface. The dialog is titled 'Create New Port Profile' and has a close button (X) in the top right corner. It contains the following fields and options:

- Device Type:** Two radio buttons: 'Switch' (selected, highlighted with a red box) and 'Access Point'.
- Profile Name:** A text input field with the placeholder 'e.g. My Office'.
- Port State:** Two radio buttons: 'Enabled' (selected) and 'Disabled'.
- Port Type:** Two radio buttons: 'Access' (selected) and 'Trunk'.
- PVID:** A text input field with a range indicator '(1-4094)'.
- Cooper Link Speed:** A dropdown menu with 'Auto (Default)' selected.
- Fiber Link Speed:** A dropdown menu with 'Auto (Default)' selected.
- DDP:** Two radio buttons: 'Enabled' (selected) and 'Disabled'.
- LBD:** Two radio buttons: 'Enabled' (selected) and 'Disabled'.

At the bottom of the dialog are two buttons: 'Cancel' and 'Create'.

Nuclias Unity Dashboard

Settings

Profiles

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

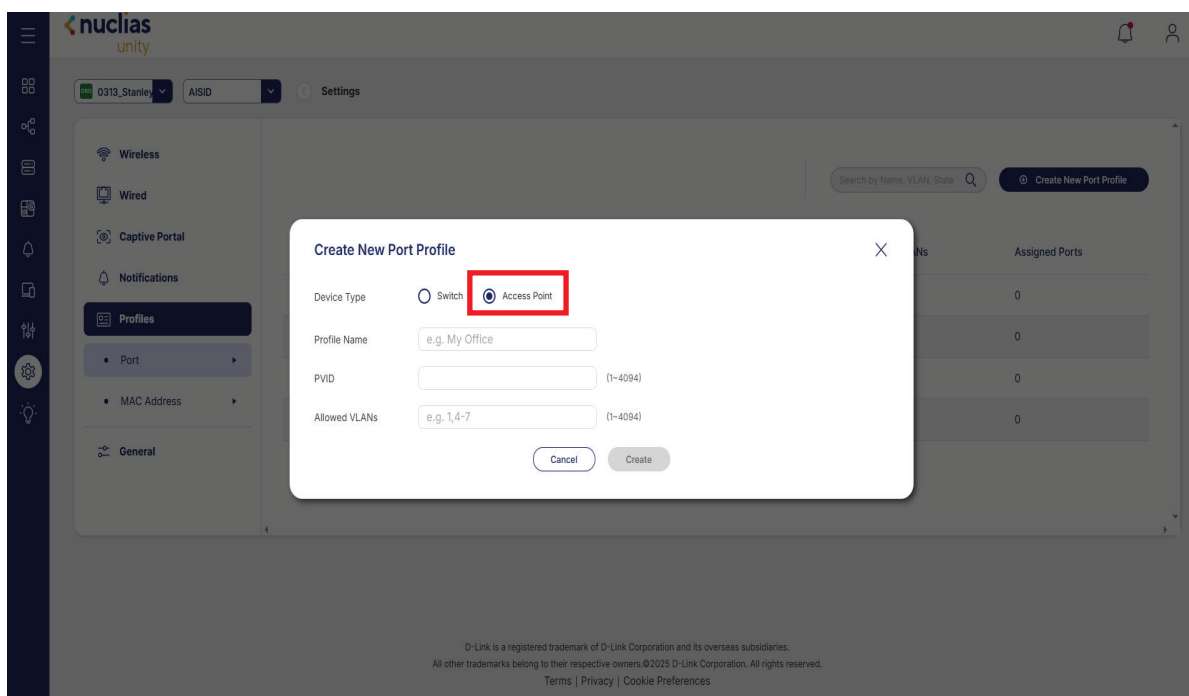
Device Type: Specifies whether the profile is intended for a Switch or Access Point, ensuring the appropriate settings are applied based on the device category.

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.

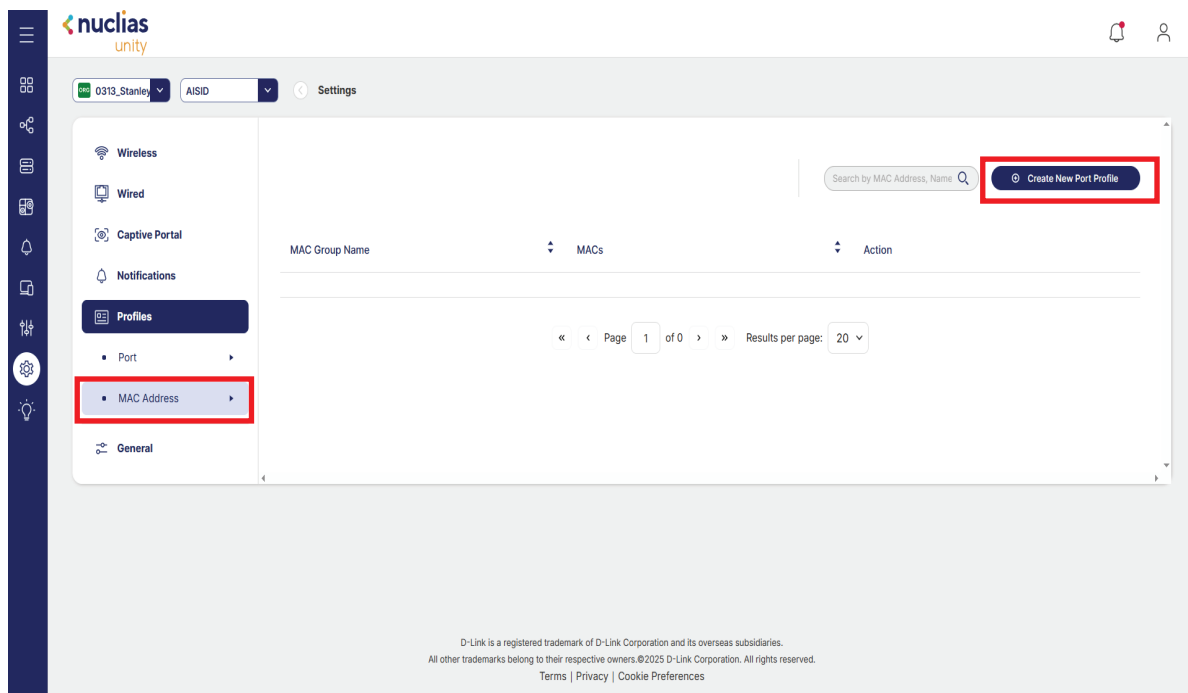
MACs: Specifies the list of MAC addresses to be included in the group. Each MAC address should be entered in the standard format (e.g., AA:BB:CC:DD:EE:FF) to ensure accurate identification of devices.

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.



Nuclias Unity Dashboard

Settings

Profiles

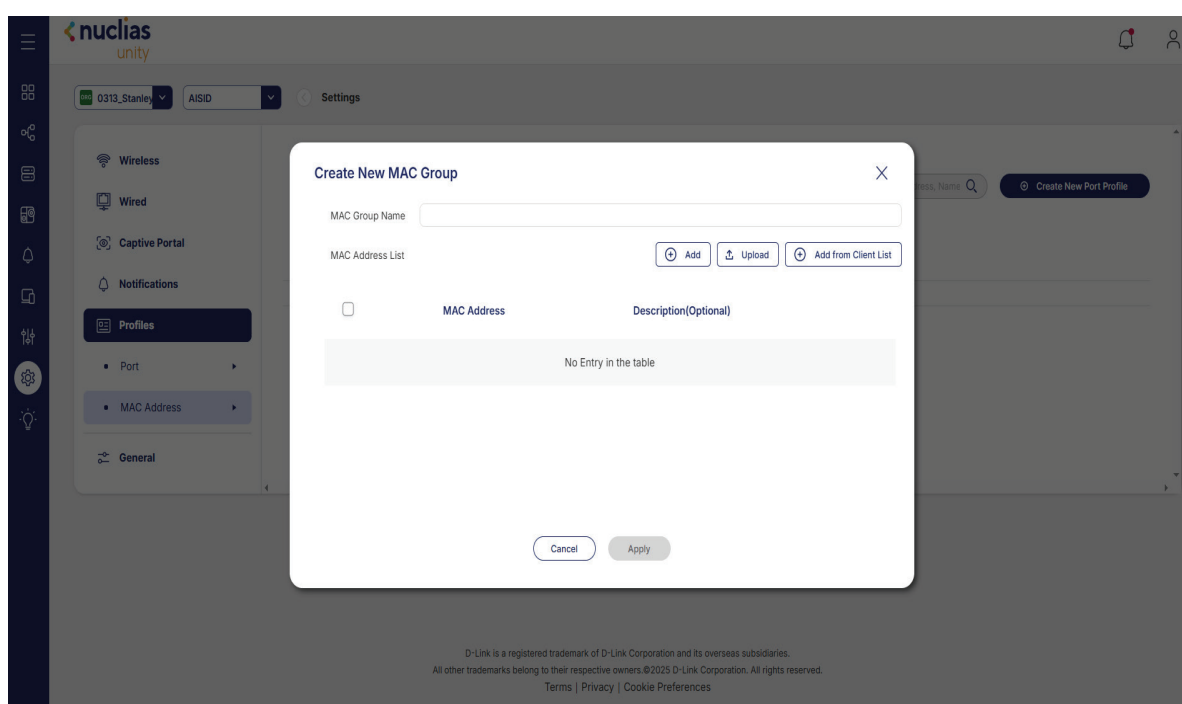
In the Create New MAC Group window, you can add MAC addresses to the group using multiple methods. First, specify a MAC Group Name to identify the group. Then, you can populate the MAC address list by selecting one of the following options:

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.

The screenshot shows the Nuclias Unity web interface. On the left is a dark blue sidebar with a menu containing icons for various settings. The 'General' option is highlighted with a red rectangle. The main content area is titled 'General Settings' and contains several input fields: 'Site Name' (text box with 'AISID'), 'Select Country' (dropdown menu with 'Taiwan'), 'Time Zone' (dropdown menu with '(UTC+08:00) Asia/Taipei'), 'NTP Server' (text box with 'ntp1.nuclias.com' and an 'Add' button), and 'Address' (a large text area with the placeholder 'Apply to all managed device'). Below these is the 'Device Account' section, which includes 'Username*' (text box with 'admin') and 'Password*' (password box with masked characters and an eye icon). At the bottom left of the settings area is a red 'Delete Site' button. At the bottom right are 'Cancel' and 'Save' buttons.

Nuclias Unity

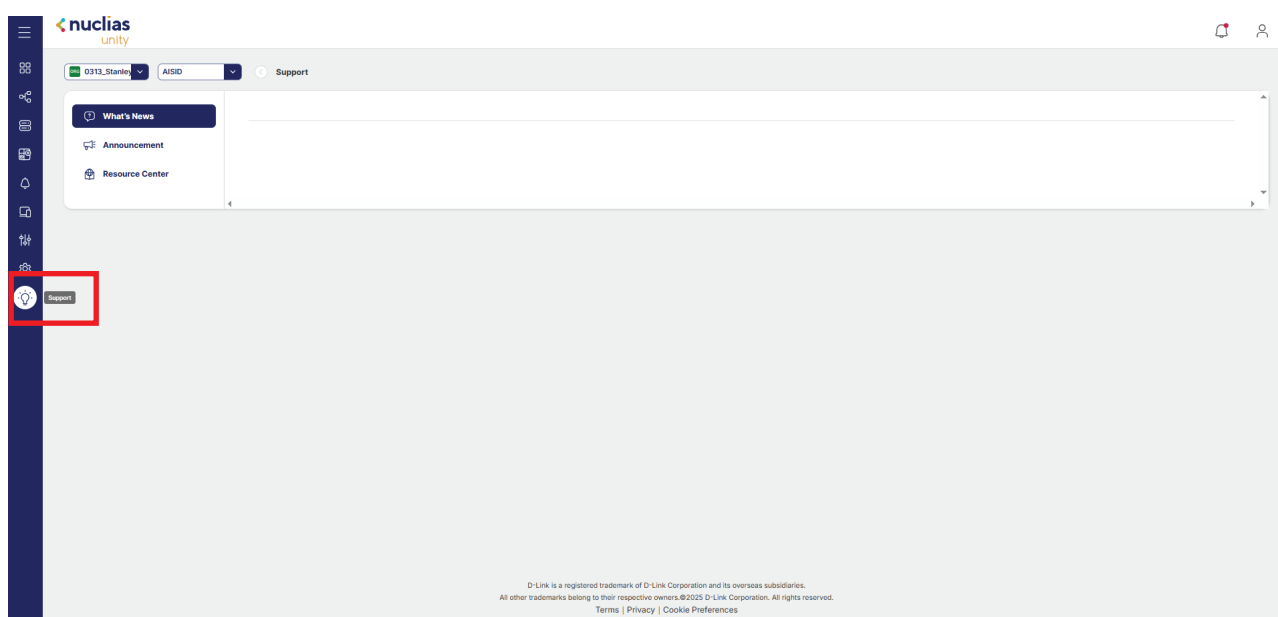
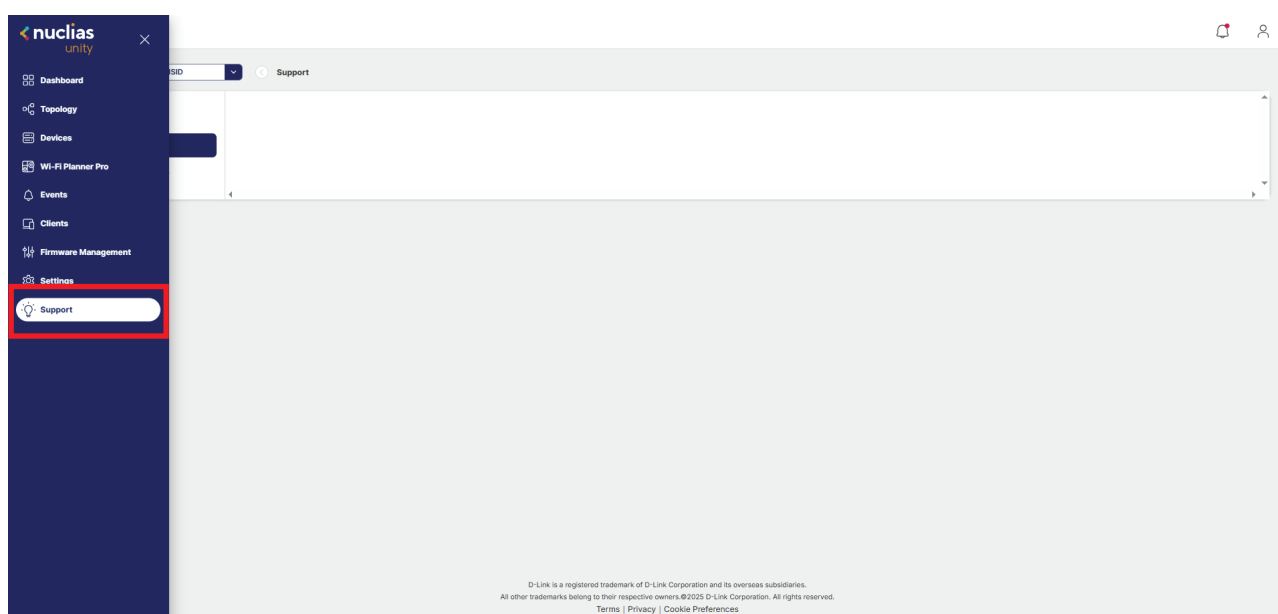
Dashboard

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.

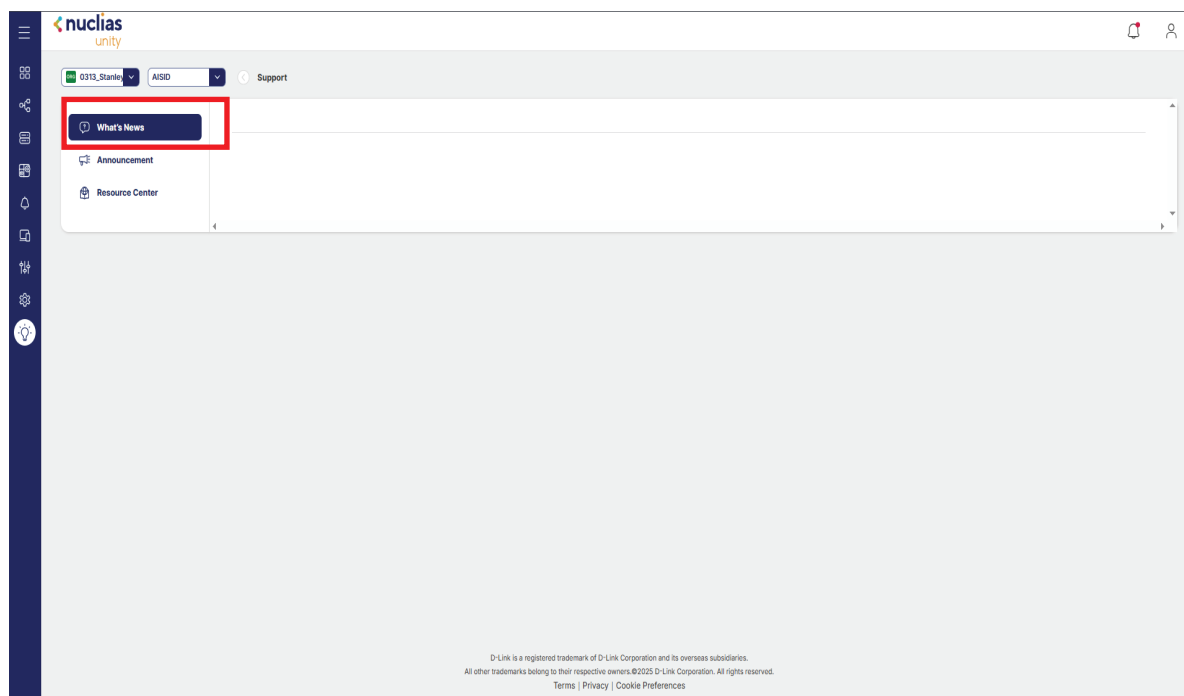


Nuclias Unity Dashboard

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.

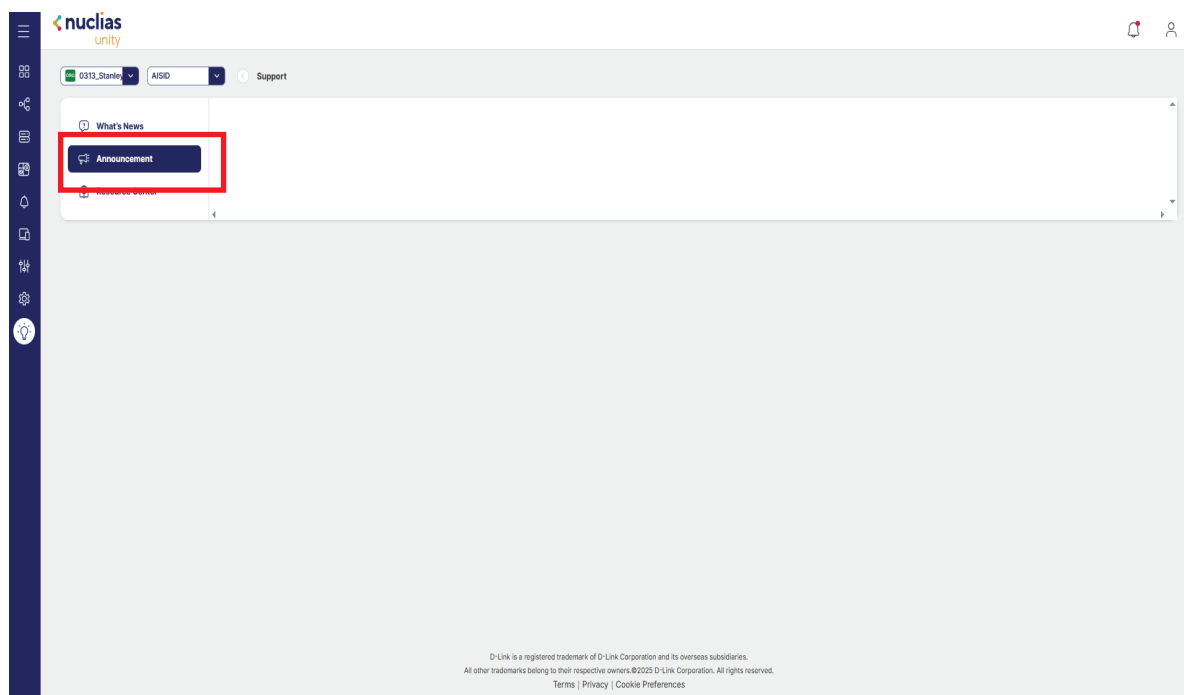


Nuclias Unity Dashboard

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.

