AmpCon Campus Management Software

User Manual V3.0.0

Models: AmpCon Campus

AmpCon-Campus Management Platform 3.0 User Guide . . . 4
Release Notes . . . 5
AmpCon-Campus 3.0.0 Release Notes . . . 6
Overview . . . 11
Quick Start . . . 19
Platform Installation Workflow . . . 20
Device Onboarding Workflow . . . 29
PicOS Switch Configuration Workflow . . . 46
Wireless Network Deployment Workflow . . . 57
Ansible Automation Workflow . . . 60
Planning . . . 66
Supported Information . . . 67
Supported PicOS Switches for 3.0.0 . . . 69
Supported FSOS Switches for 3.0.0 . . . 79
Supported APs for 3.0.0 . . . 81
Installation Requirements . . . 82
Deploying AmpCon-Campus . . . 84
Installing AmpCon-Campus . . . 85
Installing on VirtualBox for Lab Only . . . 86
Installing on VMware ESXi . . . 93
Installing on QEMU or KVM . . . 101
Installing on Physical Machines (Ubuntu Docker) . . . 111
Uninstalling on Physical Machines (Ubuntu Docker) . . . 115
Working with the User Interface . . . 117
UI Menus . . . 122
UI Conventions . . . 129
Managing Sites . . . 139
Onboarding Switches and APs . . . 143
Onboarding PicOS Switches . . . 144
How ZTP Works . . . 158
Configuring a DHCP Server . . . 161
Onboarding FSOS Switches . . . 163
Onboarding APs . . . 171
Configuring PicOS Switches . . . 180
Applying Site Configurations . . . 181
Applying Quick Configurations . . . 188
Applying Port Configurations . . . 199
Configuring a Single Switch . . . 210
Applying Template Configurations . . . 222
Checking Configuration Results . . . 232
Comparing Switch Configurations . . . 235
End-to-End Campus Deployment Scenario . . . 238
Managing PicOS Switches . . . 248
Accessing Switches . . . 249
Deleting Switches . . . 253

Rebooting Switches . . . 255
Upgrading Switches . . . 257
Managing License Portals . . . 272
Managing PicOS Licenses . . . 277
Moving Switches to Another Site . . . 286
Backing Up Configurations . . . 290
Return Merchandise Authorization . . . 294
Managing Wireless Networks . . . 297
Wireless Overview . . . 298
Concepts . . . 303
Deploying Wireless Networks . . . 309
Mesh Network Scenario . . . 311
Configuring Wireless Networks . . . 320
SSID Configurations . . . 344
Adding Wireless Profiles . . . 366
Maintaining Wireless Networks . . . 377
Upgrading APs . . . 388
Optimizing Wireless Networks . . . 399
Configuring APs via CLI . . . 404
Automation with Ansible Playbooks . . . 406
Examples for Ansible Playbooks . . . 407
Running Playbooks . . . 411
Managing Ansible Jobs . . . 421
Viewing Playbook Schedules . . . 426
Accessing Devices through SSH . . . 429
Monitoring . . . 433
Dashboard . . . 434
Topology . . . 443
PicOS Switches . . . 452
PicOS Switch List . . . 453
Basic Information of a PicOS Switch . . . 459
Deep Insights into a PicOS Switch . . . 465
Configurations and Operations of a PicOS Switch . . . 482
FSOS Switches . . . 488
SNMP Overview . . . 489
FSOS Switch List . . . 492
Information of an FSOS Switch . . . 498
Monitoring Limitations . . . 512
Access Points . . . 516
AP List . . . 517
Basic Information of an AP . . . 524
Deep Insights into an AP . . . 529
Configurations and Operations of an AP . . . 542
Clients . . . 554
Wired Clients . . . 555

Wireless Clients 564
Alerting 575
Alert Types 576
Checking the Alert List 580
Sending Email Alert Notifications 588
Managing User Access 598
Troubleshooting 608
Device Onboarding Troubleshooting 609
Ansible Playbook Troubleshooting 616
Alert Notification Troubleshooting 618
Glossary 620

AmpCon Campus Management Software 3.0 User Guide



Key Topics



Quick Start

- Overview
- Quick Start
- Planning
- Deploying AmpCon-Campus
- Working with the User Interface
- Managing User Access



PicOS Switches

- Onboarding PicOS Switches
- Configuring PicOS Switches
- Managing PicOS Switches
- Monitoring PicOS Switches



Wireless Networks

- Wireless Overview
- Deploying Wireless Networks
- Configuring Wireless Networks
- Maintaining Wireless Networks
- Monitoring Access Points



Ansible Playbooks

- Examples for Ansible Playbooks
- Running Playbooks
- Managing Ansible Jobs
- Viewing Playbook Schedules



FSOS Switches

- Onboarding FSOS Switches
- Monitoring FSOS Switches



Wired Clients

- Monitoring Wired Clients
- Monitoring Wireless Clients



Other Features

- Topology
- Dashboard
- Alerting
- Managing Sites
- Accessing Devices through SSH

Other References

Blogs | Case Study | Try Now

Release Notes

Before you install AmpCon-Campus 3.0.0 or upgrade AmpCon-Campus to 3.0.0, click the following child topic to get a quick overview of what is added, improved, changed, or fixed in AmpCon-Campus 3.0.0:

- AmpCon-Campus 3.0.0 Release Notes

AmpCon-Campus 3.0.0 Release Notes

Before installing AmpCon-Campus 3.0.0, read this topic to learn about the highlights, upgrade limitations, supported devices, improvements, and removed features in this release.

- Highlights
- Upgrade Limitations
- Supported Devices
- Improvements
  - UI Restructuring
  - Time Zone
  - AmpCon-Campus Deployment
  - AmpCon-Campus License
  - User Access Management
  - Site Management
  - Device Onboarding
  - PicOS Switch Configuration
  - PicOS Switch Management
  - Wireless Management
  - Monitoring
  - Alerting

Highlights

Compared with AmpCon-Campus 2.3.x, AmpCon-Campus 3.0.0 places greater focus on simplified deployment, streamlined configuration, and visualized operations and maintenance:

- **More Intuitive User Experience:** Centered on site management, the UI menus and feature layouts are restructured to simplify operation workflows and improve overall user experience.
- **Simplified Deployment:** Complex deployment procedures such as importing AmpCon-Campus licenses are eliminated. AmpCon-Campus 3.0.0 supports automatic AP discovery and Mesh Zero Touch Provisioning (ZTP) and simplifies onboarding parameters of PicOS switches to accelerate device onboarding.
- **Improved Configuration Efficiency:** A dedicated entry for port operations and maintenance is added. Service configurations for PicOS switches and APs are enhanced to support GUI-based bulk configuration. You can view execution statuses and results in real time, improving configuration efficiency and operation visibility.
- **Clearer Management:** Site-oriented views and permission controls are enhanced. Automatic topology discovery and visualized client monitoring are strengthened, providing unified visibility into device, link, and client statuses to help quickly locate network issues.

Upgrade Limitations

You cannot upgrade directly from previous AmpCon-Campus versions to AmpCon-Campus 3.0.0; a fresh installation of AmpCon-Campus 3.0.0 is required.

Supported Devices

- The supported PicOS switches and recommended PicOS versions are updated. For more information, see Supported PicOS Switches for 3.0.0.
- The supported FSOS switches are updated. For more information, see Supported FSOS Switches for 3.0.0.
- The supported APs are updated. For more information, see Supported APs for 3.0.0.

Improvements

UI Restructuring

AmpCon-Campus 3.0.0 redesigns UI menus and layouts around site management. Operation-relevant functions are grouped by site, reducing navigation steps and improving operation efficiency for campus network administrators.

Time Zone

AmpCon-Campus 3.0.0 displays data according to your browser's time zone instead of the previously used UTC+0 time zone. This improvement eliminates the need to manually convert times from UTC+0.

AmpCon-Campus Deployment

During AmpCon-Campus installation, you can specify the NIC IP address and OpenVPN subnet.

For more information, see Deploying AmpCon-Campus.

AmpCon-Campus License

AmpCon-Campus 3.0.0 is a free-to-use version. You don’t need to import AmpCon-Campus licenses for device onboarding.

User Access Management

The following improvements are introduced in AmpCon-Campus 3.0.0:

- The supported user roles of AmpCon-Campus are optimized, delivering finer-grained permission control aligned with multi-site workflows.
- The password cannot be specified during user creation, and every new user initially uses the default password **pica8**. For the built-in user **admin**, the password is **admin**. For security purposes, change the default password immediately after the first login.

For more information, see Managing User Access.

Site Management

In AmpCon-Campus 3.0.0, a site acts as the core scope for multi-site management, configuration inheritance, data isolation, and access control:

- After switching sites, the entire UI updates according to the currently selected site.
- Device scope is explicitly extended to PicOS switches, FSOS switches, and APs.
- After a device (PicOS switch or AP) joins a site, site-level configurations can be automatically pushed to the device.
- Site permission rules based on **Owner**, **Super Admin**, **Site Admin**, and **Readonly** roles are introduced.

For more information, see Managing Sites.

Device Onboarding

AmpCon-Campus 3.0.0 provides more onboarding methods, simplifies onboarding workflows, and supports automatic deployment of site-level configurations.

- For PicOS switches, AmpCon-Campus supports three onboarding methods: adopting switches from the auto-discovery list, importing switches by SN, and importing switches by IP address.

  Adopting switches and importing switches by SN are ZTP methods. Importing switches by IP address is a non-ZTP method.
- For APs, AmpCon-Campus supports two onboarding methods: adopting APs from the auto-discovery list and importing APs by SN.

  Adopting APs and importing APs by SN are ZTP methods.
- In AmpCon-Campus 3.0.0, FSOS switches are onboarded through Simple Network Management Protocol (SNMP), the same as in AmpCon-Campus 2.3.x. However, the onboarding steps are different.

For more information, see Onboarding Switches and APs.

PicOS Switch Configuration

The following improvements are introduced in AmpCon-Campus 3.0.0:

- AmpCon-Campus supports more configuration methods: site configuration, quick configuration, port configuration, single-switch configuration, and template configuration. You can select appropriate configuration methods for different scenarios.
- AmpCon-Campus provides a “Configuration Result” page to check configuration results of PicOS switches, centralizing configuration-result viewing and enabling easier troubleshooting.
- In AmpCon-Campus, the configuration comparison feature is more powerful. You can compare configurations between two external files, compare running or backup

configurations from the same or different PicOS switches, or compare configurations from an external file with running or backup configurations on a PicOS switch.

For more information, see Configuring PicOS Switches.

PicOS Switch Management

The following improvements are introduced in AmpCon-Campus 3.0.0:

- The Return Merchandise Authorization (RMA) process is simplified.
- The upgrade process is optimized to minimize upgrade failures.
- AmpCon-Campus supports batch switch deletion and single-switch reboot, streamlining maintenance workflows for multi-device deployments.
- AmpCon-Campus provides a centralized UI page ("Portal Configuration" page) to manage license portal information. **License Audit** and **License Action** are based on license portals on the "Portal Configuration" page.

For more information, see Managing PicOS Switches.

Wireless Management

The following improvements are introduced in AmpCon-Campus 3.0.0:

- Mesh ZTP and wireless topologies are supported.
- More wireless configurations are provided, such as Wireless Meshing, Seamless Authentication, and backup RADIUS server configuration.
- Single-AP configuration is supported, enabling per-AP custom configurations that override site-level configurations for special deployment scenarios.
- More wireless client metrics are added, helping you gain deep insights into each wireless client.
- Wireless network maintenance features are optimized, minimizing wireless operation failures.

For more information, see Managing Wireless Networks.

Monitoring

The following improvements are introduced in AmpCon-Campus 3.0.0:

- The "Dashboard" page contains more comprehensive monitoring data, covering managed device counts, the AmpCon-Campus platform status, triggered alerts, and wireless networks.
- The "Topology" page displays a clearer view of the network structure, including PicOS switches, APs, clients, and their links.
- The "Clients" page centralizes monitoring data of wireless and wired clients on the same UI page and allows you to filter client data.

- The “Devices” page reorganizes switch and AP monitoring data into the **Overview** and **Insight** tabs, making it more convenient for you to view metrics and trend graphs.

For more information, see Monitoring.

Alerting

The following improvements are introduced in AmpCon-Campus 3.0.0:

- More alert types are supported with more precise trigger conditions.
- AmpCon-Campus supports alert acknowledgment, closure, archiving, and deletion, making it better suited for team-based alert handling.
- Notification rules have been changed from cross-site rules to site-level rules, aligning with the multi-site permission model in AmpCon-Campus 3.0.0.
- AmpCon-Campus allows you to view the reasons for email notification failures, helping you identify and resolve issues faster.

For more information, see Alerting.

Overview

AmpCon-Campus is a multivendor automation solution that empowers you to deploy, configure, manage, and monitor wired and wireless devices. AmpCon-Campus simplifies, automates, and transforms device operations from Day 0 through Day 2+.

- Product Overview
- Highlights
- Features and Benefits
  - Platform Features
  - Deployment Features
  - Management Features
  - Monitoring and Visibility Features
  - Integration Features

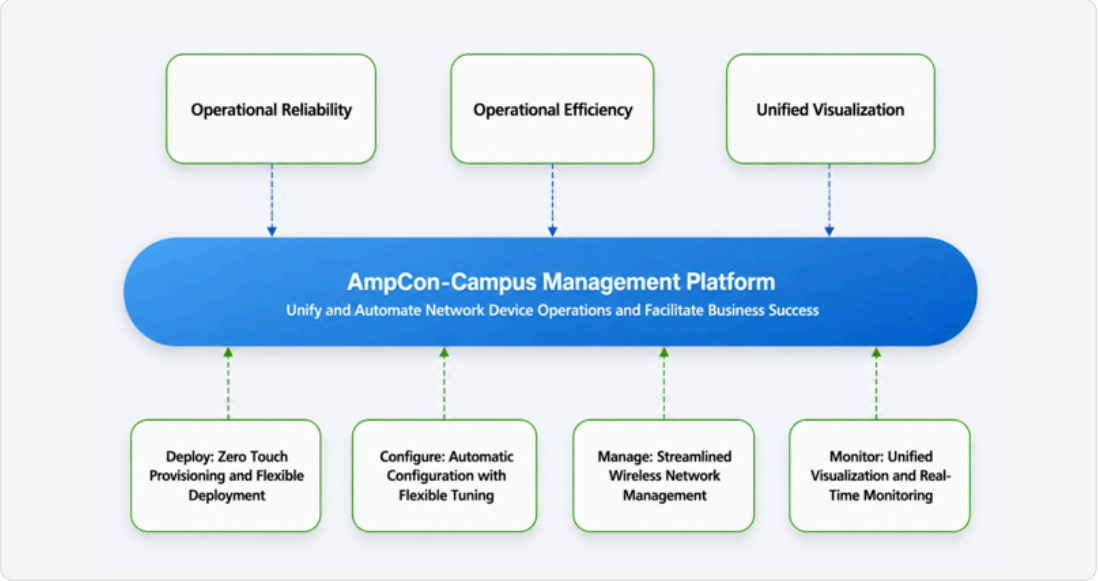
Product Overview

In the current digital transformation era, network devices play an extremely important role in the business success of an organization, and experiencing downtime caused by human errors or other factors is unacceptable.

However, device management is becoming increasingly complicated, diverse, and distributed, with multiple configuration sites, disparate monitoring tools, and a large volume of network devices and data. In addition, manual operations of network devices often lead to human errors, security vulnerabilities, outdated automation scripts, and undocumented configuration changes, increasing the downtime risk. Users need a network device management platform to address these challenges.

AmpCon-Campus is an automated and unified management platform that can enhance operational reliability, efficiency, and visualization of network devices, powering the business success of organizations.

Figure 1. AmpCon-Campus Unifies and Automates Network Device Operations, Powering Business Success



AmpCon-Campus helps you automate the following network device operations from Day 0 through Day 2+:

- **Deploy:** Simplify network device onboarding and automate deployment of wireless networks, covering diverse requirements of small, medium-sized, and large-scale campus networks.
- **Configure:** Leverage a centralized user interface to push configurations to network devices (PicOS switches and APs), minimizing errors and simplifying configuration processes.
- **Manage:** Streamline lifecycle management of wired and wireless network devices (PicOS switches and APs), and integrate with the open-source automation tool Ansible to enhance device management automation, helping you increase management efficiency and focus on more strategic tasks.
- **Monitor:** Provide a unified view and real-time monitoring data of network devices (PicOS switches, FSOS switches, and APs), helping you gain comprehensive insights and eliminate the need to switch between multiple monitoring tools.

Highlights

- **Continuous Day 0 to Day 2+ Operational Automation**

  AmpCon-Campus provides powerful features to automate network device operations from Day 0 through Day 2+, helping you accelerate network device operations in every phase, reduce the downtime risk, and move to more automated network device management.

- **Unified Multi-Site Management for a Seamless Management Experience**

  AmpCon-Campus centrally manages switches and APs in campus networks, enabling unified operation and maintenance and site-level management. It reduces the complexity of network device deployment and maintenance, and improves fault response efficiency and data security.

- **License-Free Activation and Zero Touch Provisioning (ZTP)**

  With license-free AmpCon-Campus activation and ZTP, AmpCon-Campus simplifies network device (PicOS switch and AP) deployment and expansion. It reduces on-site deployment and manual configuration efforts, enabling fast, standardized deployment across campuses, branches, and multiple sites.

- **Flexible Configuration Across Scenarios and Easily Scalable Deployment**

  Use the intuitive user interface and guided workflows to flexibly configure switches, ports, and wireless networks for diverse network requirements. Reusable templates enable bulk configuration, improving efficiency and consistency at scale.

- **End-to-End Network Observability for Faster Troubleshooting and Better Experiences**

  Gain unified visibility into the network topology, device health, and client experience to monitor wired and wireless network status in real time. Receive timely email alerts for critical events, helping you quickly assess the scope of issues, identify root causes, and minimize network downtime.

- **Smarter Automation for Network Operations at Scale**

  Automate routine tasks with Ansible playbooks and dynamically optimize wireless Radio Frequency (RF) parameters based on real-time environmental data, reducing manual effort and operational complexity across large, high-density deployments.

- **Powerful Wireless Network Deployment and Management**

  AmpCon-Campus supports deploying and managing wireless networks and APs, providing flexible and secure network management through enhanced wireless configuration, advanced Radio Frequency (RF) optimization, and robust management capabilities. You can deploy, configure, maintain, and monitor wireless networks more efficiently.

- **Automated PicOS Switch Management**

  AmpCon-Campus makes it easy to manage a large number of PicOS switches. You can manage the lifecycle of PicOS switches more efficiently, reducing the risk of human errors and decreasing operational costs.

- **Multi-Dimensional FSOS Switch Monitoring**

  AmpCon-Campus uses Simple Network Management Protocol (SNMP) to monitor the status, performance metrics, and other statistics of FSOS switches. You can onboard FSOS switches to AmpCon-Campus and then monitor FSOS switches in the AmpCon-Campus UI.

Features and Benefits

Platform Features

The following features are related to the AmpCon-Campus platform itself:

Table 1. Platform Features

Feature	Benefit	Reference Link
Unified Platform	AmpCon-Campus is a unified platform that automates network device operations from Day 0 through Day 2+, delivers comprehensive visibility, automation, and operational simplicity, and eliminates the complexity of juggling multiple tools.	• No reference link
Platform Deployment	AmpCon-Campus offers flexible platform deployment options: • For organizations seeking virtualization flexibility, AmpCon-Campus can be installed on a virtual machine (VMware ESXi 6.7, 7.0, 8.0, QEMU/KVM for Ubuntu 22.04 LTS, or Oracle VirtualBox), enabling deployment on existing virtual infrastructure without the need for dedicated hardware. • For organizations without virtual infrastructure, AmpCon-Campus can be installed on a physical machine based on Ubuntu 22.04 with Docker installed.	• Platform Installation Workflow • Installing AmpCon-Campus
User Experience	AmpCon-Campus features a modern, intuitive, user-friendly user interface (UI) for managing network devices, providing a unified and consistent experience across the whole device operation process.	• Working with the User Interface
Role-Based Access Control	AmpCon-Campus supports Role-Based Access Control (RBAC), which is used to permit individual users to	• Managing User Access

	perform specific actions and gain visibility within an authorized scope. Each user is assigned to a specific role with associated permissions. Owner and Super Admin are global roles. Custom users receive Site Admin or Read-only permissions for each assigned site. RBAC in AmpCon-Campus ensures secure, segmented, and efficient management of network device operations and helps organizations enforce compliance, reduce risk, and streamline collaboration.	
Platform Status	On the “Dashboard” page, you can get a global overview of the AmpCon-Campus status.	• AmpCon-Campus Status

Deployment Features

The following features are used to deploy network devices and wireless networks.

Table 2. Deployment Features

Feature	Benefit	Reference Link
Onboarding PicOS Switches	You can onboard PicOS switches to AmpCon-Campus for centralized and efficient switch management. Onboarding PicOS switches means bringing switches under the management of AmpCon-Campus. After PicOS switches are onboarded, they can be managed by AmpCon-Campus.	• Onboarding PicOS Switches
Onboarding FSOS Switches	You can onboard FSOS switches to AmpCon-Campus. Once onboarded, these FSOS switches can only be monitored and	• Onboarding FSOS Switches

	cannot be configured or managed by AmpCon-Campus.	
Onboarding APs	You can onboard APs to AmpCon-Campus. Onboarding APs means bringing APs under the management of AmpCon-Campus. Once onboarded, APs can be managed by AmpCon-Campus.	• Onboarding APs
Deploying Wireless Networks	You can deploy wireless networks through AmpCon-Campus, accelerating wireless network deployment.	• Deploying Wireless Networks

Management Features

The following features are used to manage network devices and wireless networks:

Table 3. Configuration and Management Features

Feature	Benefit	Reference Link
Managing Sites	A site is a logical management unit that groups resources for centralized device configuration, management, monitoring, and permission isolation. You can manage sites to meet your needs. You can organize network devices by site, enabling site-level management and visibility and improving multi-site operational efficiency.	• Managing Sites
Managing Wireless Networks	You can configure and maintain wireless networks and access points (APs) through automatic wireless configuration, advanced radio frequency optimization, and robust management capabilities.	• Configuring Wireless Networks • Maintaining Wireless Networks
Managing PicOS Switches	You can manage the lifecycle of PicOS switches to reduce the	• Managing PicOS Switches

	complexity and workload of switch management while improving efficiency.	
Configuring PicOS Switches	You can use different ways to configure PicOS switches, minimizing errors and simplifying configuration processes.	• Configuring PicOS Switches
Accessing Devices through SSH Sessions	You can connect to a device (such as a switch or client device) from the AmpCon-Campus UI by establishing an SSH session.	• Accessing Devices through SSH Sessions

Monitoring and Visibility Features

The following features are used to monitor and visualize network devices:

Table 4. Monitoring and Visibility Features

Feature	Benefit	Reference Link
Dashboard	You can get a global overview of managed devices, triggered alerts, and wireless networks.	• Dashboard
Topology	You can view real-time topologies of devices (PicOS switches, APs, and their connected client devices) in each site.	• Topology
PicOS Switches	You can continuously monitor PicOS switches for performance analysis and fault diagnosis.	• PicOS Switches
FSOS Switches	You can continuously monitor FSOS switches through Simple Network Management Protocol (SNMP).	• FSOS Switches
Access Points	You can continuously monitor APs to gain deep insight into each managed AP.	• Access Points
Clients	You can accurately and securely monitor client devices connected to	• Clients

	managed PicOS switches and APs, facilitating refined management of client devices.	
Alerts	AmpCon-Campus issues an immediate alert when a failure or performance shift is detected, helping you diagnose root causes and resolve problems quickly. You can use this feature to achieve the following goals: • View different levels and types of alerts in the AmpCon-Campus UI. • Receive real-time email alert notifications if you need to be notified immediately.	• Alerting

Integration Features

The following features are used to integrate with another tool:

Table 5. Integration Features

Feature	Benefit	Reference Link
Ansible Integration	You can write, import, run, and schedule Ansible playbooks on managed PicOS switches, reducing manual work and configuration errors and improving PicOS switch management efficiency.	• Running Ansible Playbooks for Automation

Quick Start

The following topics provide quick start guides for AmpCon-Campus, detailing the workflows of AmpCon-Campus installation, device onboarding, PicOS switch configuration, wireless network deployment, and Ansible automation.

- Platform Installation Workflow
- Device Onboarding Workflow
- PicOS Switch Configuration Workflow
- Wireless Network Deployment Workflow
- Ansible Automation Workflow

Platform Installation Workflow

To use the powerful features of AmpCon-Campus, install AmpCon-Campus on a virtual machine or a physical machine.

This guide provides a comprehensive overview of AmpCon-Campus installation procedures.

Prerequisites
Installing on a Virtual Machine
Installing on a Physical Machine
What to Do Next

Prerequisites

If you want to install AmpCon-Campus on a **physical machine**, ensure that the physical machine meets the following requirements:

> **NOTE**
>
> To install AmpCon-Campus on a **virtual machine**, ensure that the hypervisor has the following resources (CPU, memory, and hard disk) to be allocated when you import the AmpCon-Campus image to the hypervisor.

Table 1. Machine Requirements

Resource	Requirement
CPU	Clock speed: 2.0 GHz or faster
	Number of cores: At least 4 CPU cores
Memory	At least 16 GB
Hard Disk	At least 512 GB
Operating System	Ubuntu 22.04 LTS (X86 architecture) with Docker

Whether you want to install AmpCon-Campus on a physical machine or a virtual machine, if a firewall is used, configure the firewall properly to allow the following network access:

Table 2. Network Requirements

TCP/UDP	Port	Protocol
TCP	80	HTTP
TCP	443	HTTPS

TCP	15002	WebSocket
UDP	69	TFTP
UDP	80	OpenVPN

NOTEs

- On AmpCon-Campus, each managed PicOS switch has two IP addresses: **Registration IP** and **VPN IP**.
  - **Registration IP** is the management IP address of a PicOS switch. **Registration IP** is used to connect to AmpCon-Campus during the switch onboarding process.
  - However, **Registration IP** might be changed. To ensure uninterrupted connection between AmpCon-Campus and a PicOS switch after **Registration IP** is changed, OpenVPN is introduced to AmpCon-Campus.
  - OpenVPN is an open-source virtual private network (VPN) solution designed to create secure, encrypted communication tunnels over networks.

    After a PicOS switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between AmpCon-Campus and the switch is established, and **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-Campus and the switch will communicate through the VPN tunnel.
- AmpCon-Campus also functions as the OpenVPN server, and its OpenVPN IP address is 10.8.0.1. The default subnet for OpenVPN is 10.8.0.0/20.

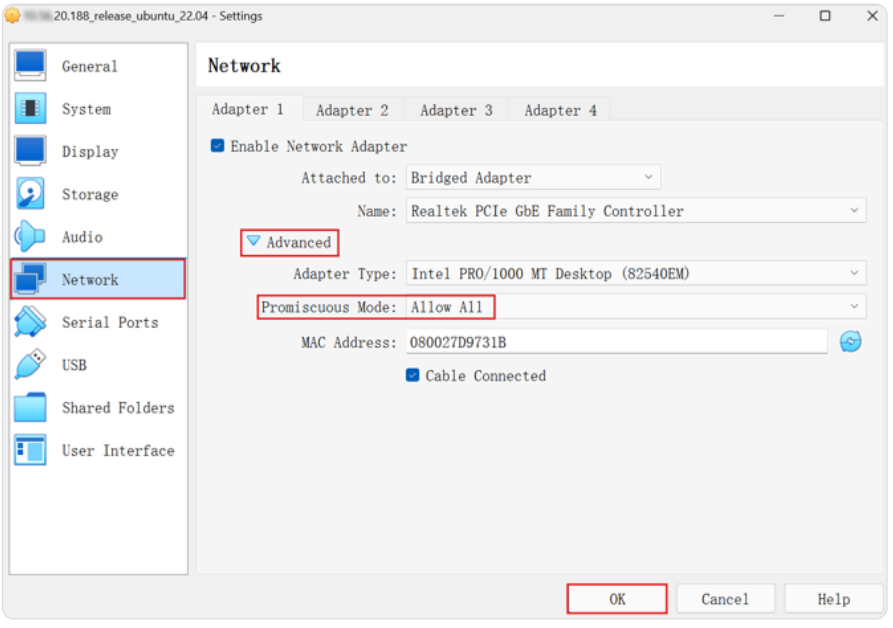
  If the default subnet conflicts with your network, AmpCon-Campus can't work well. Contact the support team to resolve this issue.

Installing on a Virtual Machine

To install AmpCon-Campus on a virtual machine, complete the following tasks:

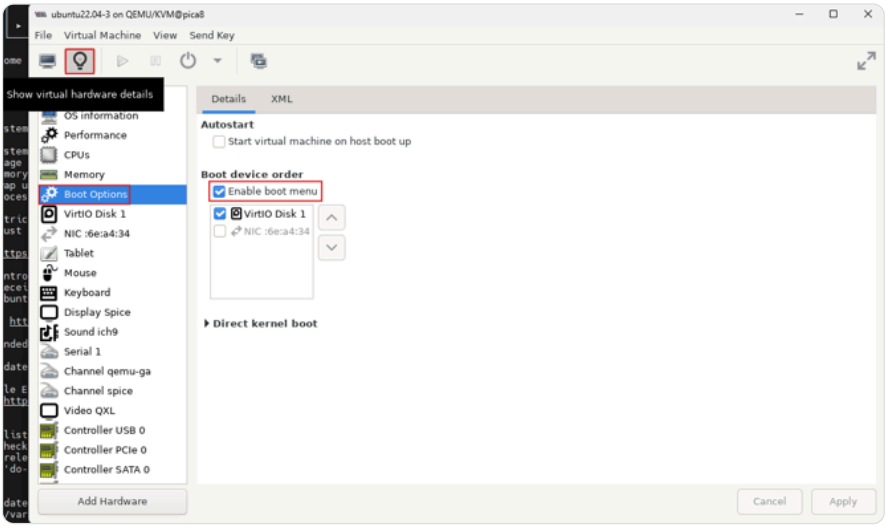
Table 3. Tasks for Installation on Virtual Machines

Task	Description
Preparing a Hypervisor	Prepare the hypervisor used to create the virtual machine. The following hypervisors are supported: • VMware ESXi 6.7, 7.0, or 8.0 • QEMU for Ubuntu 22.04 LTS • KVM for Ubuntu 22.04 LTS • Oracle VirtualBox

	NOTE AmpCon-Campus installed on Oracle VirtualBox can be used for lab purposes only.
Downloading and Unzipping the AmpCon-Campus Image	1. Download the zipped AmpCon-Campus image from the AmpCon-Campus download page according to the hypervisor and the AmpCon-Campus version. On the AmpCon-Campus download page, you must select **United States** as the region. Otherwise, you might not be able to find the image file. 2. Copy the zipped AmpCon-Campus image to the machine where the hypervisor exists, and then unzip it.
Importing the AmpCon-Campus Image	1. Import the AmpCon-Campus image to the hypervisor. For different hypervisors, the steps of importing the AmpCon-Campus image are different. To check detailed importing steps on each hypervisor, see Installing on VMware ESXi, Installing on QEMU or KVM, and Installing on VirtualBox for Lab Only. 2. Wait for the import process to complete. After it finishes, the virtual machine is successfully created. AmpCon-Campus is placed in the default directory /opt/ampcon. Currently, you can't customize the installation directory. 3. Enable the **EFI** mode of the virtual machine 4. Change the promiscuous mode to **Allow All**. This configuration is needed only if AmpCon-Campus is installed on VirtualBox. 

5. Enable the boot menu.

   This configuration is needed only if AmpCon-Campus is installed on QEMU or KVM.



Modifying the Network Interface Configuration

1. Start the virtual machine.
2. Log in to the virtual machine with the default username (**pica8**) and password (**pica8**).
3. Open the file named 00-installer-config.yaml by running the **sudo vi /etc/netplan/00-installer-config.yaml** command.
4. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the virtual machine as follows:

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens34:
      addresses:
      - [redacted].20.188/24
      nameservers:
        addresses:
        - [redacted].8.8
        search: []
      routes:
      - to: default
        via: [redacted].20.254
  version: 2
```

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the virtual machine.
>
> Therefore, you must check the actual NIC name of the virtual machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.

5. Apply the network interface configuration by running the **sudo netplan apply** command.

Activating AmpCon-Campus	1. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command. 2. Activate AmpCon-Campus by running the **sudo ./activate.sh** command. Then, AmpCon-Campus is installed. **NOTEs** You can append any supported parameters to the **sudo ./activate.sh** command: • **--global-ip <*ip*>**: Specifies the NIC IP used by managed devices to access AmpCon-Campus. The imported AmpCon-Campus image file contains only one Network Interface Card (NIC). But you can manually add more NICs. You **must** specify this parameter if the virtual machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail. • **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 is used as the OpenVPN subnet. See the following configuration example: **sudo ./activate.sh --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24** The global IP address must not fall within the VPN subnet. Otherwise, the command will fail.

Installing on a Physical Machine

To install AmpCon-Campus on a physical machine (Ubuntu 22.04 LTS with Docker installed), complete the following tasks:

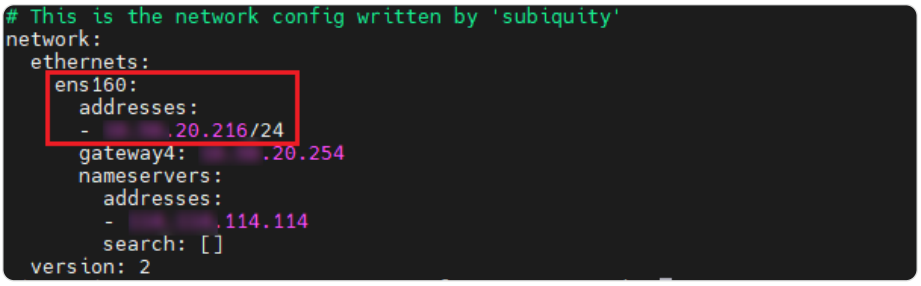
Table 4. Tasks for Installation on Physical Machines

Task	Description
Preparing a Physical Machine	Prepare a physical machine based on Ubuntu 22.04 LTS with Docker installed.
Downloading and Unzipping the	1. Download the AmpCon-Campus zipped installation package from the AmpCon-Campus download page according to your required

AmpCon-Campus Installation Package	AmpCon-Campus version. On the AmpCon-Campus download page, you must select **United States** as the region. Otherwise, you might not be able to find the image file. 2. Copy the downloaded zipped package to the prepared physical machine, and then unzip the package by running the **unzip <*package_name*>.zip** command. A .tar file is generated in the current directory. Extract the .tar file by running the **tar -xvf <*tar_file_name*>.tar** command. A directory is generated containing AmpCon-Campus installation files. **NOTEs** Replace <*package_name*> in the command with the name of the AmpCon-Campus installation package. Replace <*tar_file_name*> in the command with the extracted .tar file name.

Modifying the Network Interface Configuration

1. On the physical machine, open the file named 00-installer-config.yaml by running the **sudo vi /etc/netplan/00-installer-config.yaml** command.
2. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the physical machine.



3. Apply the network interface configuration by running the **sudo netplan apply** command.

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the physical machine.
>
> Therefore, you must check the actual NIC name of the physical machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.

Installing AmpCon-Campus

1. Go to the directory where the extracted AmpCon-Campus installation files exist.
2. Install AmpCon-Campus by running the **sudo ./install.sh** command.
3. Wait for the installation process to finish. Once completed, AmpCon-Campus is installed and started.

> **NOTE**
>
> You can append any supported parameters to the **sudo ./install.sh** command:
>
> - **--home <*path*>**: Specifies the AmpCon-Campus installation directory. If it's not specified, AmpCon-Campus is installed in the /opt/ampcon directory.
> - **--global-ip <*ip*>**: Specifies the NIC IP used by managed devices to access AmpCon-Campus.
>   The AmpCon-Campus installation package file is not an image file, and thus no NIC is contained in the file. But you can manually add one or multiple NICs to the physical machine.

You **must** specify this parameter if the physical machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.

- **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 is used as the OpenVPN subnet.

See the following configuration example:

sudo ./install.sh --home /opt/ampcon --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24

The global IP address must not fall within the VPN subnet. Otherwise, the command will fail.

What to Do Next

After you install AmpCon-Campus, check the following tasks. These tasks are **not mandatory** and can be performed only when needed.

Table 5. Post-Installation Tasks

Task	Description
Configuring for Multi-NIC Deployment	If multiple NICs are added to the virtual or physical machine where AmpCon-Campus is installed and the global IP is not specified during activation or installation, you must contact support engineers to specify the NIC IP address. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
Stopping AmpCon-Campus	To stop AmpCon-Campus, follow these steps: 1. Go to the AmpCon-Campus installation directory by running the **cd <*AmpCon-Campus installation directory*>** command. For a virtual machine, replace <*AmpCon-Campus installation directory*> with /opt/ampcon. For a physical machine, replace <*AmpCon-Campus installation directory*> with the actual AmpCon-Campus installation directory. If you don't set a custom one, the default installation directory is /opt/ampcon. 2. Stop AmpCon-Campus by running the **sudo ./stop.sh** command. **NOTEs** To start AmpCon-Campus after it is stopped, follow the steps:

	1. Go to the AmpCon-Campus installation directory by running the **cd <*AmpCon-Campus installation directory*>** command. Replace <*AmpCon-Campus installation directory*> as described in **Step 1** above. 2. Start AmpCon-Campus by running the **sudo ./start.sh** command.
Uninstalling AmpCon-Campus on Physical Machines (Ubuntu Docker)	To uninstall AmpCon-Campus, follow these steps: 1. Obtain the AmpCon-Campus installation directory and assign it to the **AMPCON_HOME** environment variable by running the **AMPCON_HOME="$(dirname "$(readlink -f /etc/ampcon/active.env)")"** command. 2. Go to the AmpCon-Campus installation directory by running the **cd "$AMPCON_HOME"** command. 3. Run the **sudo ./uninstall.sh** command. 4. Confirm the uninstallation by entering the **UNINSTALL AMPCON** confirmation phrase. **NOTE** Currently, only AmpCon-Campus installed on a physical machine can be uninstalled. For AmpCon-Campus installed on a virtual machine, remove the AmpCon-Campus virtual machine instance directly by shutting it down and deleting it from the hypervisor.
Logging In to the AmpCon-Campus UI	On the first login to the AmpCon-Campus UI, use the default username (**admin**) and password (**admin**). For more information, see Working with the User Interface. **NOTEs** • The user **admin** is a built-in account of the **Owner** role. It has full operational permissions on AmpCon-Campus. For security purposes, change your password on first login, update it regularly, and store it securely. To update the password, see User Self-Management. • You can add other user accounts and enable limited access for the personnel who are working with you. For more information, see Managing User Access.

Device Onboarding Workflow

AmpCon-Campus supports onboarding PicOS switches, FSOS switches, and access points (APs). After onboarding, PicOS switches and APs can be managed by AmpCon-Campus. FSOS switches cannot be managed by AmpCon-Campus. You can only monitor them as described in Monitoring - FSOS Switches.

This guide provides a comprehensive overview of device onboarding procedures.

> **NOTE**
>
> The guide lists only the workflow of device onboarding. You must check the reference links for detailed information.

- Onboarding PicOS Switches
  - Guidelines
  - Prerequisites
  - Adopting PicOS Switches
  - Importing PicOS Switches by SN
  - Importing PicOS Switches by IP Address
  - What to Do Next
- Onboarding FSOS Switches
  - Prerequisites
  - Procedure
  - What to Do Next
- Onboarding APs
  - Guidelines
  - Prerequisites
  - Adopting APs
  - Importing APs by SN
  - What to Do Next

Onboarding PicOS Switches

Guidelines

To onboard switches with PicOS installed, use one of the following methods:

Table 1. PicOS Switch Onboarding Methods

Category	Method	Description
ZTP Method	**Adopting Switches**	After you have configured the DHCP server as described in Configuring a DHCP Server, AmpCon-Campus can discover these switches automatically and add them to the auto-discovery list. Then, you can adopt the switches in the auto-discovery list directly.

	Importing Switches by SN	If you have configured the DHCP server and have obtained switch serial numbers (SNs), you can import these switches by SN.
Non-ZTP Method	**Importing Switches by IP Address**	If you have obtained switch IP addresses, you can import these switches by IP address.

ZTP methods rely on the DHCP service. For the ZTP process, see How ZTP Works.

To onboard switches without PicOS installed, you can use only the **Adopting Switches** or **Importing Switches by SN** method.

NOTEs

- After a switch is onboarded, if its SSH username or password is changed on the switch, you must update the credentials for device management. Otherwise, AmpCon-Campus cannot manage the switch. For more information, see Configuring a Single Switch.
- When you configure the DHCP server or when you import switches by IP address, you have provided the IP addresses of the switches to be onboarded.

  However, these IP addresses might be changed over time. To ensure uninterrupted connection between AmpCon-Campus and switches, OpenVPN is introduced to AmpCon-Campus.

  After a PicOS switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between AmpCon-Campus and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-Campus and the switch will communicate through the VPN tunnel.

Prerequisites

Before onboarding PicOS switches, ensure that the following prerequisites are met:

Table 2. Prerequisite Tasks and Links for Onboarding PicOS Switches

Category	Task	Reference Link
Site Requirement	Ensure that the site to which the PicOS switches belong has been created.	• Managing Sites
Switch Requiremen	Ensure that the PicOS switches are supported by AmpCon-Campus.	• Supported PicOS Switches for

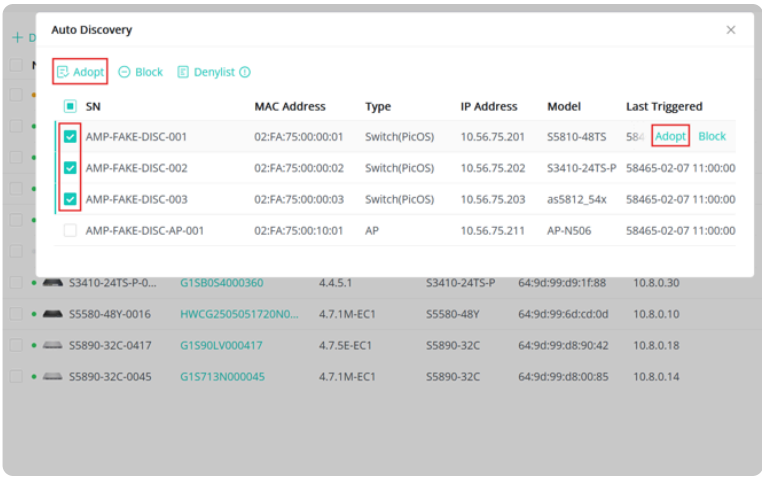
t		3.0.0
	Ensure that the Secure Shell (SSH) protocol is enabled on these PicOS switches. SSH is enabled on PicOS switches by default.	• No Reference Link
Network Requirement	Ensure that the PicOS switches are up and able to connect to AmpCon-Campus.	• No Reference Link
	If a firewall is configured between AmpCon-Campus and the PicOS switches, allow outbound access on the following ports to the management port of each switch. • **TCP**: 22 • **TCP**: 9339 • **TCP**: 830	• No Reference Link
DHCP Requirement	If you use the **Adopting Switches** or **Importing Switches by SN** method, ensure that you have configured the DHCP server.	• Configuring a DHCP Server

Adopting PicOS Switches

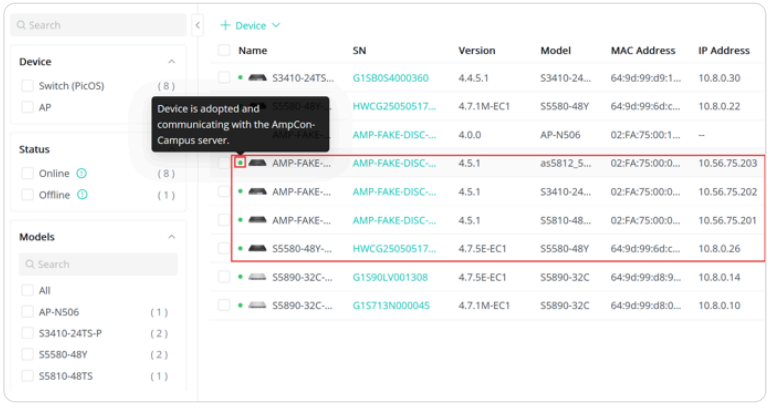
To adopt PicOS switches, complete the following tasks:

Table 3. Tasks and Links for Adopting PicOS Switches

Category	Task	Reference Link
Adopting PicOS Switches	1. Select the site to which the switches belong. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Auto Discovery**. 3. Adopt one or multiple switches by using the **Adopt** button.	• Adopting Switches



4. In the pop-up window, check whether the default username (**admin**) and password (**pica8**) can be used to log in to each switch. If not, enter a correct username and password.
5. Click **Apply**.

Verifying Adoption Status	Check whether the PicOS switches are added to the device list and whether each switch's status circle is in green. Hover over the status circle to view the switch adoption status. 	• No Reference Link

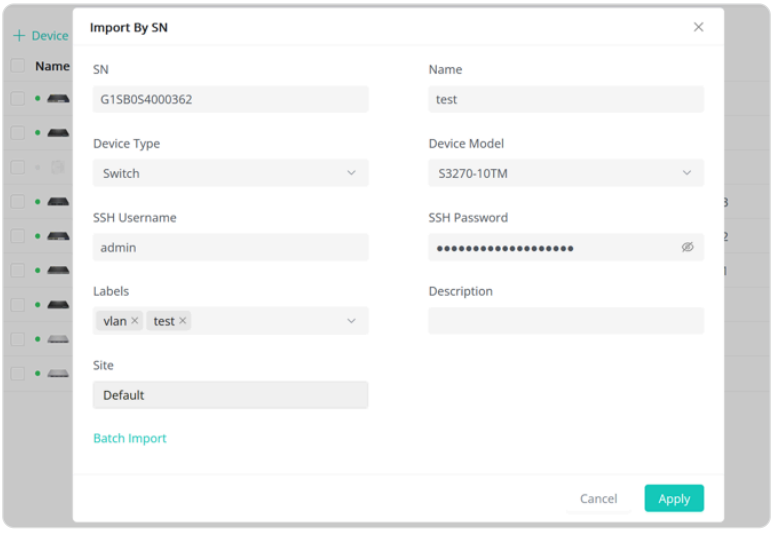
Importing PicOS Switches by SN

To import PicOS switches by SN, complete the following tasks:

Table 4. Tasks and Links for Importing PicOS Switches by SN

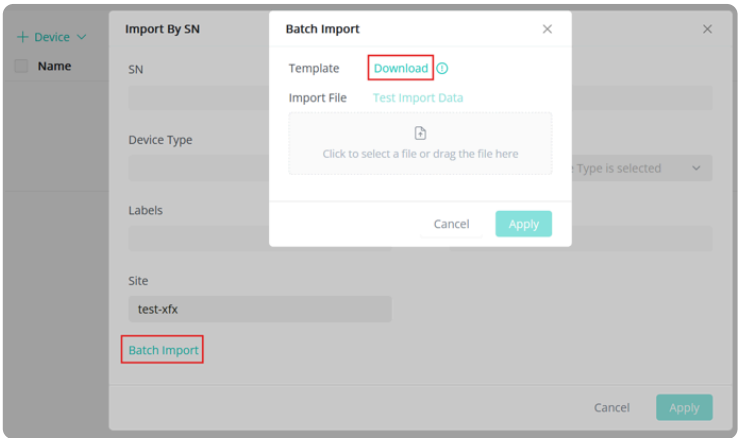
Category	Task	Reference Link
Importing PicOS Switches by SN	1. Select the site to which the switches belong. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Import by SN**.	• Importing Switches by SN

3. To import a single PicOS switch, input the switch information in the pop-up window, and then click **Apply**.



4. To bulk import multiple PicOS switches, configure as follows:

   a. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.



   b. Open the template file, and then enter correct information in the **SN**, **DeviceType**, **DeviceModel**, **Name**, **Labels**, and **Description** columns for each switch to be imported.

   c. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file.

   d. Optional: Click **Test Import Data**. In the new pop-up window, check the test result.

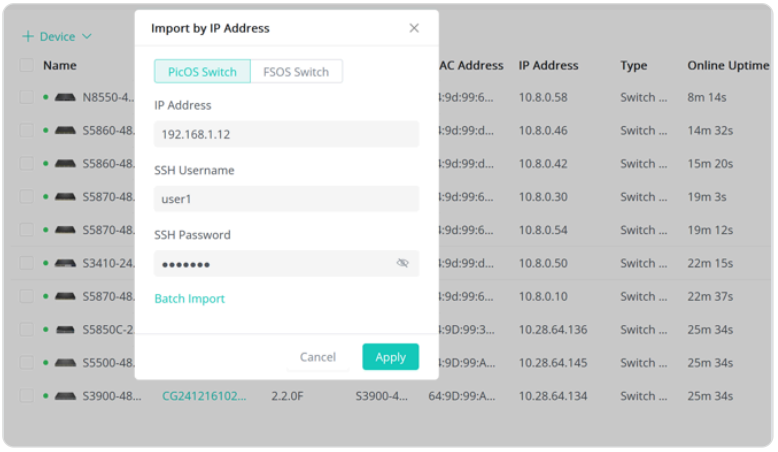
   e. Click **Apply**.

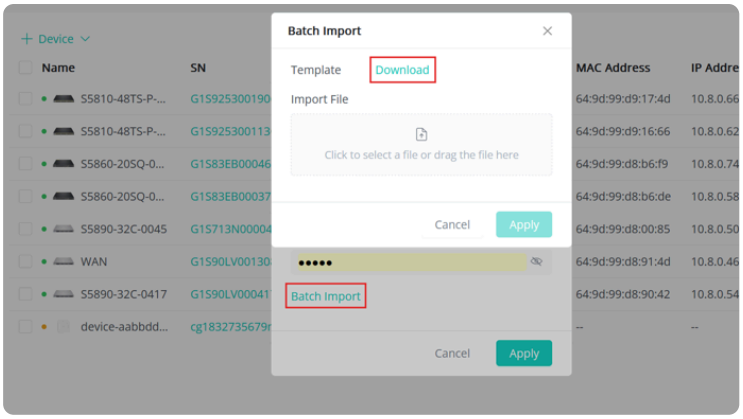
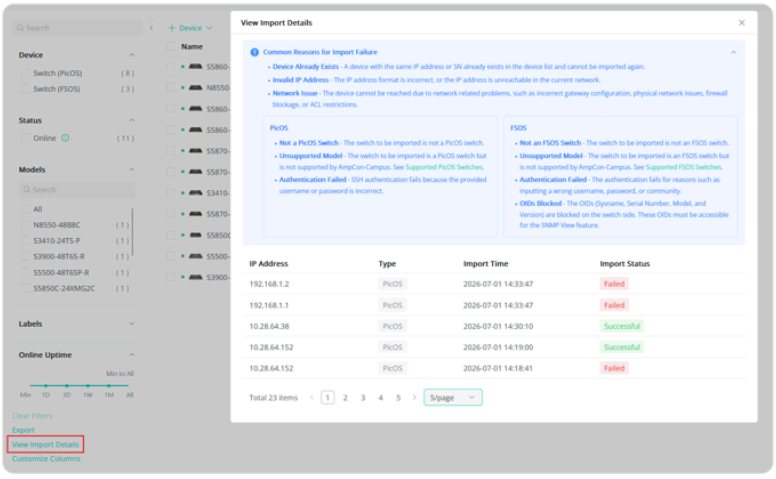
Verifying Import Status	Check whether the PicOS switches are listed in the device list and whether each switch's status circle is in green. Hover over the status circle to view the switch import status.	• No Reference Link

Importing PicOS Switches by IP Address

To import PicOS switches by IP address, complete the following tasks:

Table 5. Tasks and Links for Importing PicOS Switches by IP Address

Category	Task	Reference Link
Importing PicOS Switches by IP Address	1. Select the site to which the switches belong. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Import by IP Address**. 3. To import a single PicOS switch, input the switch information in the pop-up window, and then click **Apply**.  4. To bulk import multiple PicOS switches, configure as follows: a. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.	• Importing Switches by IP Address

	 b. Open the template file, and then enter the description (optional), IPv4 address, SSH username, and SSH password for each switch to be imported. c. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. d. Click **Apply**.	
Verifying Import Status	1. On the “Devices” page, click **View Import Details**. 2. In the pop-up window, locate the PicOS switches, and then check whether the import status is **Successful**. 	• No Reference Link

What to Do Next

After you onboard PicOS switches, check the following tasks. These tasks are **not mandatory** and can be performed only when needed.

Table 6. Post-Onboarding Tasks and Links for PicOS Switches

Category	Task	Reference Link
Configuring PicOS	Apply site configurations, quick configurations, port configurations, or template configurations to PicOS	• Configuring PicOS Switches

Switches	switches, or configure a single switch. Then, verify the configuration results or compare switch configurations as needed.	
Managing PicOS Switches	Manage the lifecycle of PicOS switches to increase network management efficiency and focus on more strategic tasks.	• Managing PicOS Switches • Accessing Devices through SSH
Monitoring PicOS Switches	Monitor PicOS switches to gain deep insights into each switch. View switch-related alerts in the AmpCon-Campus UI, or receive timely email alerts for critical events. View PicOS switches and their connected devices to understand the network structure of the currently selected site.	• PicOS Switches • Alerting • Topology

Onboarding FSOS Switches

Prerequisites

Before importing FSOS switches, ensure that the following prerequisites are met:

Table 7. Prerequisite Tasks and Links for Onboarding FSOS Switches

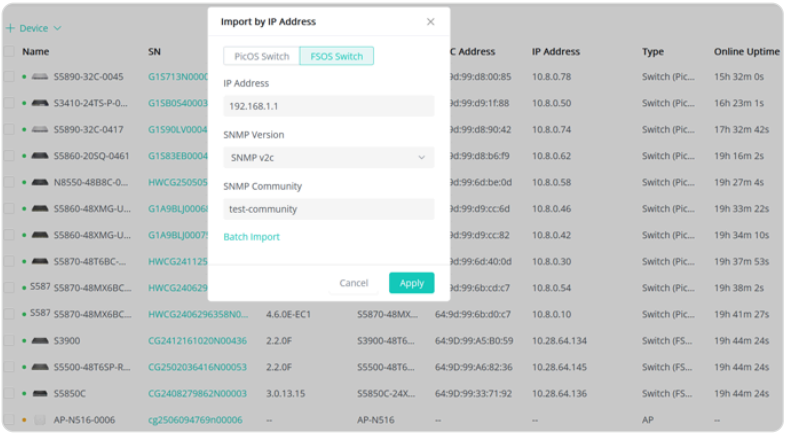
Category	Task	Reference Link
Site Requirement	Ensure that the site to which the FSOS switches belong has been created.	• Managing Sites
Switch Requirement	Ensure that AmpCon-Campus supports the FSOS switches.	• Supported FSOS Switches for 3.0.0
	Ensure that you have enabled SNMP and configured SNMP authentication on the FSOS switches.	• No Reference Link
	The OIDs (Sysname, Serial Number, Model, System Description, MAC Address, and Version) are not blocked on the switch. These OIDs must be accessible for the SNMP View feature.	• No Reference Link

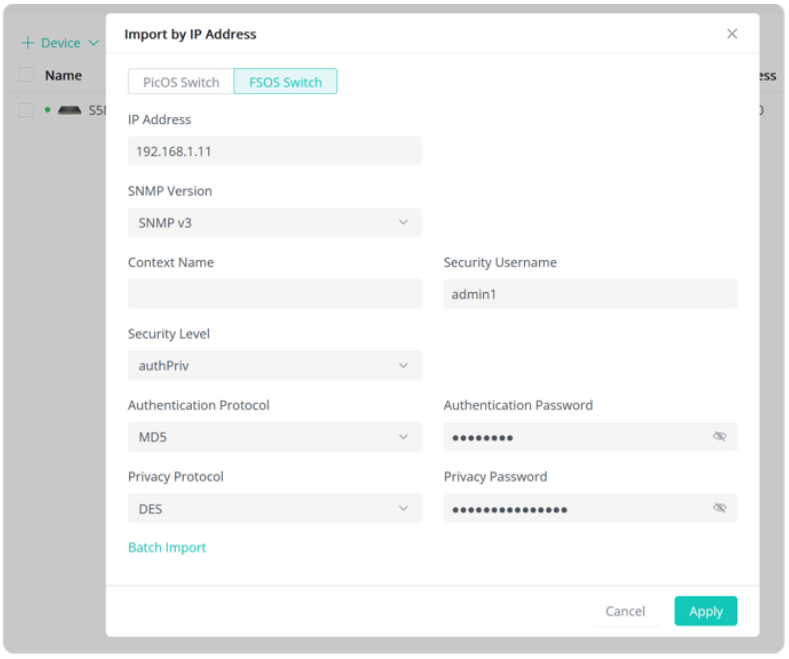
Network Requirement	Ensure that the switches are up and able to connect to AmpCon-Campus. No network timeout issues occur due to unreachable IP addresses, disabled SNMP services, firewall blockages, or Access Control List (ACL) restrictions.	• No Reference Link

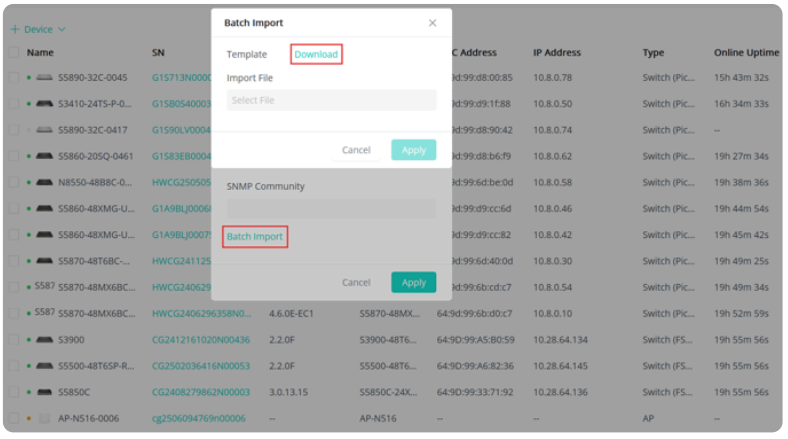
Procedure

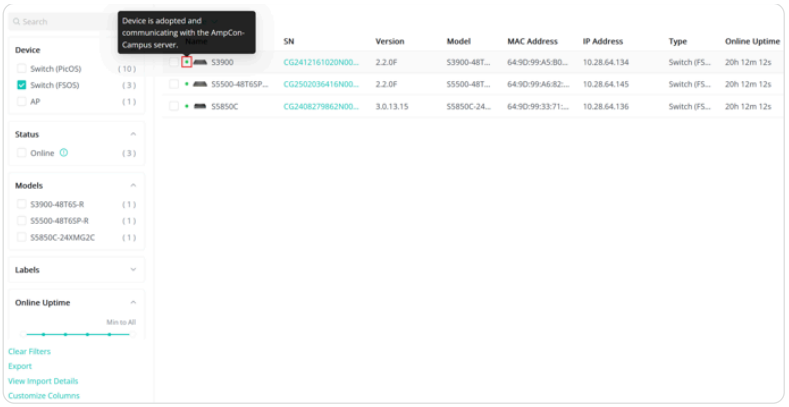
To onboard FSOS switches, complete the following tasks:

Table 8. Tasks and Links for Onboarding FSOS Switches

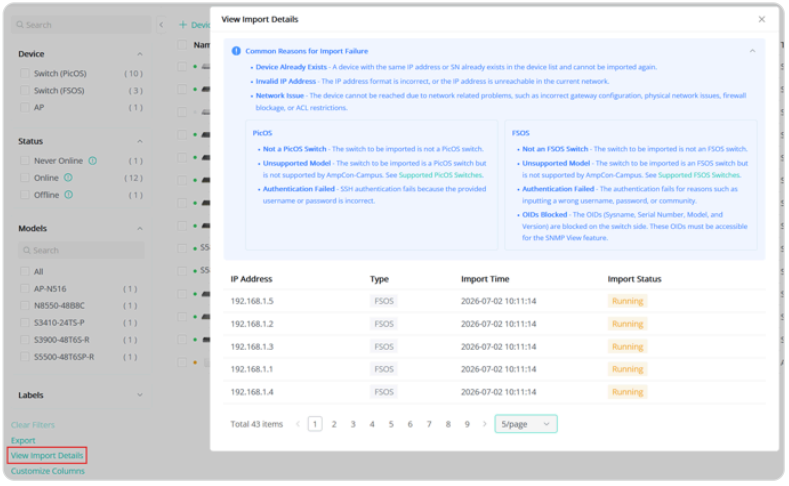
Category	Task	Reference Link
Importing a Single FSOS Switch	1. Select the site to which the switch belongs. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Import by IP Address**. 3. Click the **FSOS Switch** tab, input the switch information, and then click **Apply**. • If the switch to be imported has SNMP v1 or SNMP v2c enabled, input the following information:  • If the switch to be imported has SNMP v3 enabled, input the following information:	• Importing a Single FSOS Switch



Importing FSOS Switches in Batches	1. Select the site to which the switches belong. 2. On the “Devices” page, hover over **+ Device**, and then click **Import by IP Address**. 3. In the pop-up window, click the **FSOS Switch** tab, and then click **Batch Import**. 4. Click **Download** to download the template file.  5. Open the template file, and then enter switch information. 6. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. Then, click **Apply**.	• Importing FSOS Switches in Batches
Checking Import Results	1. On the “Devices” page, check whether the switches are listed in the device list and whether the status circle of each switch is in green. Hover over the status circle, and then you can see the switch import status.	• Checking Import Results



2. On the “Devices” page, click **View Import Details**. In the pop-up window, locate the FSOS switches, and then check whether the import status is **Successful**.



What to Do Next

After onboarding FSOS switches to AmpCon-Campus, you can continuously monitor the switches for performance analysis and fault diagnosis through Simple Network Management Protocol (SNMP). For more information, see FSOS Switches.

Onboarding APs

Guidelines

During wireless network deployment, use one of the following two methods to onboard APs:

Table 9. AP Onboarding Methods

Method	Description
Adopting APs	After you pre-configure the IP address of the AmpCon-Campus server as described in the Prerequisites section, AmpCon-Campus can discover APs automatically and add them to the auto-discovery list. You can adopt the APs in the auto-discovery list directly.

Importing APs by SN	If you have the serial number list of the APs, you can import the APs by SN.

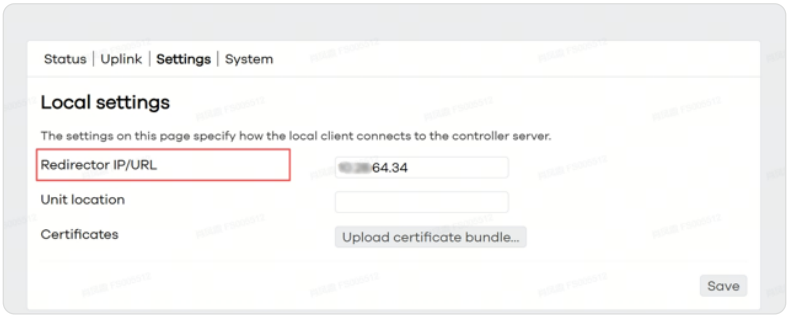
Adopting APs and **Importing APs by SN** are Zero Touch Provisioning (ZTP) methods. For the ZTP workflow, see AP ZTP Workflow.

Prerequisites

Before you onboard APs, ensure that the following prerequisite tasks have been completed:

Table 10. Prerequisite Tasks and Links for Onboarding APs

Category	Task	Reference Link
Site Requirement	Ensure that the site to which the APs belong has been created.	• Managing Sites
AP Requirement	Ensure that the APs are supported by AmpCon-Campus.	• Supported APs for 3.0.0
IP Address Requirement	Install a DHCP server, and configure the DHCP server to reserve an IP range for the APs.	• No Reference Link

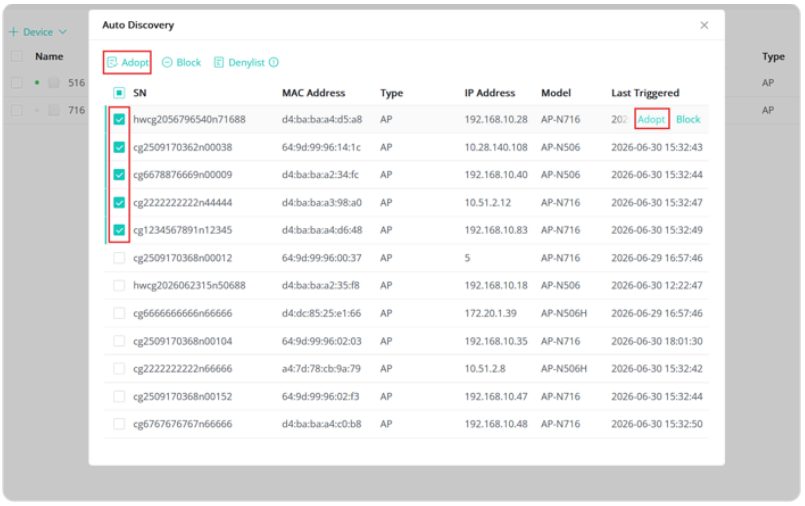
	Pre-configure the IP address of AmpCon-Campus by using one of the following ways: • Configure DHCP Option 138 as the IP address of AmpCon-Campus. See the following DHCP Option 138 configuration example:  • Add the IP address of AmpCon-Campus in the **Redirector IP/URL** field of each AP webpage. See the following AP webpage configuration example: 	• No Reference Link
Network Requirement	Plug in and power on the APs, and ensure that the APs are able to connect to AmpCon-Campus.	• No Reference Link

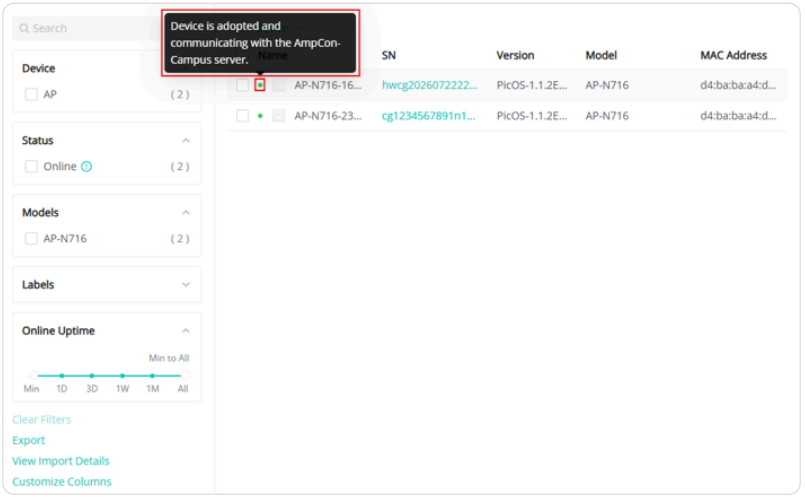
Adopting APs

To adopt APs, complete the following tasks:

Table 11. Tasks and Links for Adopting APs

Category	Task	Reference Link
Adopting APs	1. Select the site to which the APs belong. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Auto Discovery**. 3. Adopt one or multiple APs by using the **Adopt** button.	• Adopting APs



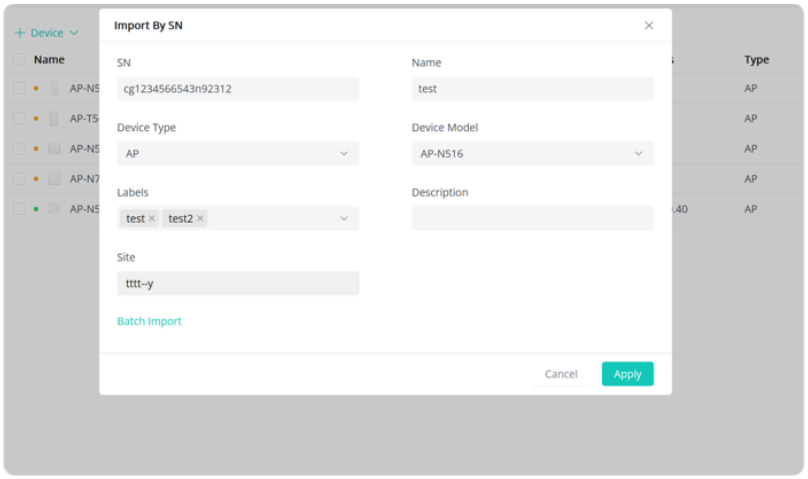
Verifying Adoption Status	Check whether the APs are listed in the device list and whether the status circle of each AP is in green. Hover over the status circle to view the AP adoption status. 	• No Reference Link

Importing APs by SN

To import APs by SN, complete the following tasks:

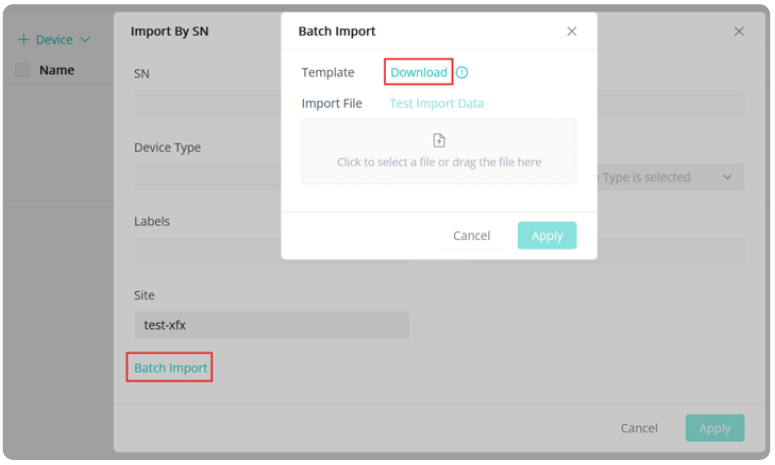
Table 12. Tasks and Links for Importing APs by SN

Category	Task	Reference Link
Importing APs by SN	1. Select the site to which the APs belong. 2. Click the **Devices** icon from the navigation bar. On the "Devices" page, hover over **+ Device**, and then click **Import by SN**. 3. To import a single AP, input the AP information in the pop-up window, and then click **Apply**.	• Importing APs by SN



4. To bulk import multiple APs, configure as follows:

   a. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.



   b. Open the template file, and then enter correct information in the **SN**, **DeviceType**, **DeviceModel**, **Name**, **Labels**, and **Description** columns for each AP to be imported.

   c. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file.

   d. Optional: Click **Test Import Data**. In the new pop-up window, check the test result.

   e. Click **Apply**.

Verifying Import Status	Check whether the APs are listed in the device list and whether the status circle of each AP is in green. Hover over the status circle to view the AP import status.	• No Reference Link

What to Do Next

After you onboard APs, check the following tasks. These tasks are **not mandatory** and can be performed only when needed.

Table 13. Post-Onboarding Tasks and Links for APs

Category	Task	Reference Link
Configuring Wireless Networks	Configure site-level wireless configurations, or fine-tune wireless configurations of a specific AP.	• Configuring Wireless Networks
Maintaining Wireless Networks	Establish a remote terminal session to an AP through remote TTY shell (RTTY).	• Accessing APs
	When an AP experiences signal anomalies or requires maintenance or replacement, you can remotely trigger its LED to blink, enabling quick on-site localization.	• Positioning APs
	Reboot a single online AP or multiple online APs in batches.	• Rebooting APs
	Upgrade AP firmware one by one or in batches. In addition, you can upgrade AP firmware immediately or at a scheduled date and time.	• Upgrading APs
	Wipe all custom settings and restore an online AP to its original status (factory settings). This action is irreversible.	• Restoring to Factory Settings
	Capture remote packets from target ports of an online AP for rapid troubleshooting.	• Capturing Remote Port Packets
	Clear all device-specific configurations for an AP and force the AP to inherit site-level configurations.	• Enforcing Site Configurations
	Use one-click network optimization to rapidly optimize wireless network performance through automation technologies.	• Optimizing Wireless Networks
	If some issues can be resolved only through CLI configurations or some advanced functions can be achieved only through CLI configurations, contact support engineers to perform AP debugging or configuration for you through this feature.	• Configuring APs via CLI
	Delete a single AP or multiple APs in batches.	• Deleting APs

	Move a single AP or multiple APs to another site.	• Moving APs to Another Site
Monitoring Wireless Networks	Get an overview of the wireless network in the currently selected site on the “Dashboard” page.	• Wireless Networks
	View APs and their connected devices to understand the network structure of the currently selected site.	• Topology
	View basic information, in-depth metrics, and configurations of APs.	• Access Points
	Monitor wireless clients connected to each managed AP.	• Wireless Clients

PicOS Switch Configuration Workflow

AmpCon-Campus provides multiple methods for configuring PicOS switches, including site configuration, quick configuration, port configuration, single-switch configuration, and template configuration.

Select a configuration method based on the target scope and use case. Site configuration provides a common baseline for switches in a site, while the other methods support guided bulk configuration, port-level changes, device-specific tuning, and advanced custom configurations.

This guide provides a comprehensive overview of PicOS switch configuration procedures.

> **NOTE**
>
> The guide lists only the workflow of PicOS switch configuration. You must check the reference links for detailed information.

Guidelines
Prerequisites
Procedure
Verifying Configuration Results
What to Do Next

Guidelines

AmpCon-Campus supports different PicOS switch configuration methods. These methods have different purposes:

Table 1. Configuration Methods

Method	Description
Site Configuration	Add site-level switch configurations for a site. Then, managed PicOS switches in the site are automatically configured. After you move a PicOS switch to another site or onboard a PicOS switch to a site, if the site has site-level switch configurations, these configurations will be automatically pushed to the switch.
Quick Configuration	Apply quick configurations (including Layer 3 interface, DHCP, port, static route, and OSPF configurations) to managed PicOS switches through the **Quick Config** wizard.
Port Configuration	Configure PicOS switch ports through a predefined port profile, or configure PicOS switch ports directly.

Single-Switch Configuration	Fine-tune configurations of a single PicOS switch.
Template Configuration	Use configuration templates to push specific configurations that can't be pushed through other configuration methods.

NOTEs

- Ensure that AmpCon-Campus can reach and authenticate against managed PicOS switches over SSH. The **SSH Username** and **SSH Password** must exactly match the credentials configured on the switches. Otherwise, configuration delivery and other device-management operations will fail. For more information, see Device Credential Configurations.

  If AmpCon-Campus can access and manage a PicOS switch through a specific **SSH Username** and **SSH Password**, it's not recommended to modify the **SSH Username** and **SSH Password**.
- Use AmpCon-Campus as the primary management interface for switch configurations. **Do not** configure the same objects directly through the switch CLI, because device-side changes might cause configuration conflicts or drift, resulting in failures for subsequent configuration pushes.
  If a required configuration is not supported by AmpCon-Campus, contact support engineers before configuring it through the switch CLI. After making an approved switch-side change, review its dependencies and align the switch's running configuration with AmpCon-Campus's configuration database before the next configuration push.
- Network-related site configurations are pushed to PicOS switches only when you apply port configurations or quick configurations referencing the added networks. After you modify system-related site configurations and click **Apply**, the site-level system configurations will be directly pushed to associated switches.
- Any custom configurations applied to a single PicOS switch will be pushed to that switch as device-specific configurations, while other site-level configurations are still applied to the switch.

Prerequisites

You can create site-level configurations before onboarding PicOS switches. After you onboard a PicOS switch to a site, if the site has site-level switch configurations, these configurations will be automatically pushed to the switch.

To apply configurations to already onboarded PicOS switches, ensure that the following prerequisites are met during configuration. Otherwise, the configuration will fail.

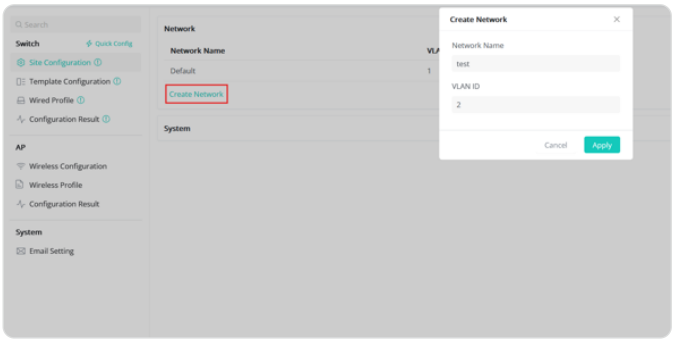
Table 2. Prerequisites

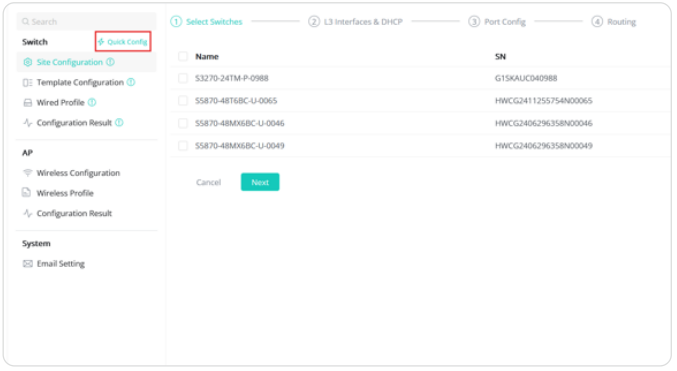
Prerequisite	Reference Link
Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List
No configurations are being pushed or waiting to be pushed to the PicOS switches.	• No Reference Link
No upgrade tasks are running on the PicOS switches.	• No Reference Link

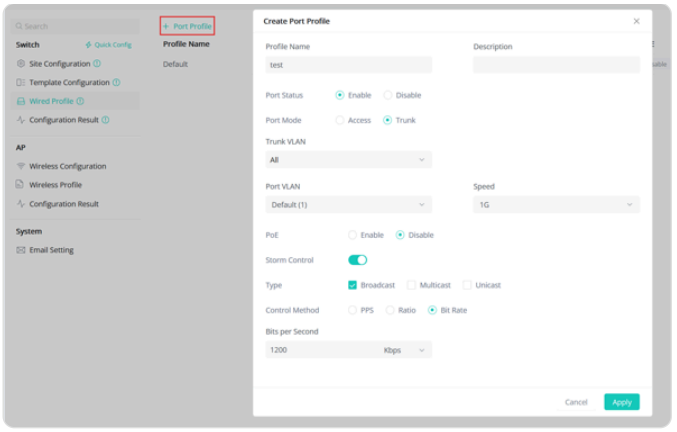
Procedure

Refer to the following procedures for each configuration method:

Table 3. Procedure and Link for Each Configuration Method

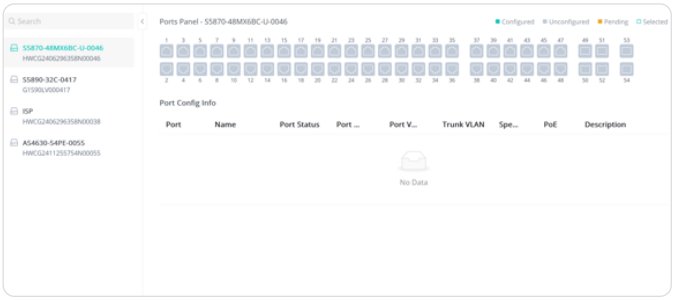
Configuration Method	Procedure	Reference Link
Applying Site Configurations	1. Select the site to which the switches to be configured belong. 2. Click the **Settings** icon from the navigation bar, and then click **Site Configuration** in the sidebar. 3. In the **Network** section, add one or multiple networks by clicking **Create Network**. In the pop-up window, enter the following information, and then click **Apply** to save the network configuration.  4. In the **System** section, add system-related configurations. 5. Click **Apply** to deploy the site-level system configurations to PicOS switches in the selected site.	• Applying Site Configurations

	6. If the current site-level system configurations differ from the last successfully applied ones on some switches, click **Sync Site Config** to synchronize the current site-level system configurations to these switches.	
Applying Quick Configurations	1. Select the site to which the switches to be configured belong. 2. Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar. 3. In the **Quick Config** wizard, select one or multiple switches to be configured, and then click **Next**.  4. In the **L3 Interfaces & DHCP** tab, add L3 interface and DHCP configurations, and then click **Next**. 5. In the **Port Config** tab, configure switch ports, and then click **Next**. 6. In the **Routing** tab, add one or multiple static routes, and add Open Shortest Path First (OSPF) configurations. 7. Click **Apply**.	• Applying Quick Configurations
Applying Port Configurations through Port Profiles	1. Select a site to which the PicOS switches to be configured belong. 2. Click the **Settings** icon from the navigation bar, and then click **Wired Profile** in the sidebar. 3. On the “Wired Profile” page, check whether an existing port profile meets your needs. If not, click **+ Port Profile** to add a port profile.	• Configuring Switch Ports through Port Profiles



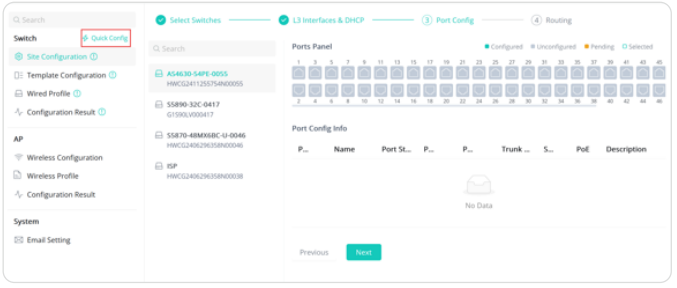
4. Go to the port panel through one of the following ways:

- Click the **Ports** icon from the navigation bar to go to the “Ports” page.



- Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar to open the **Quick Config** wizard.

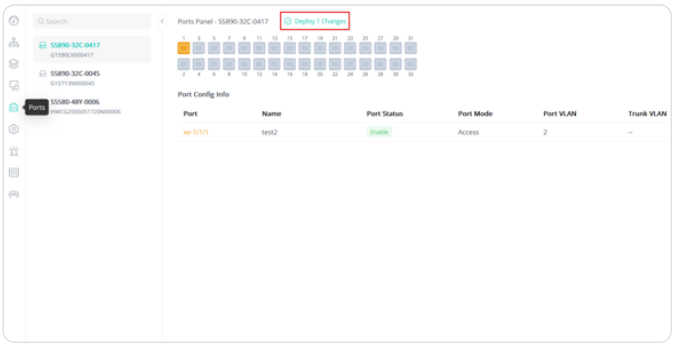
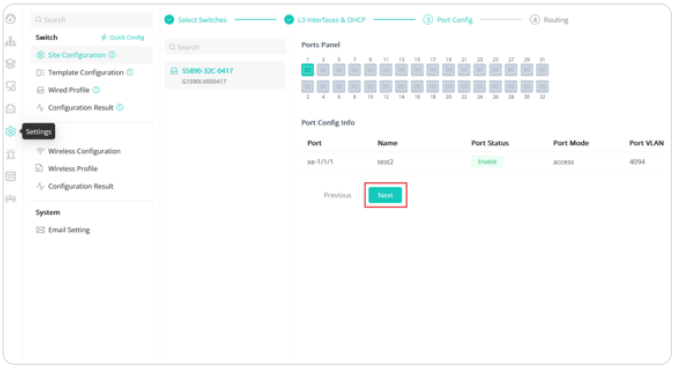
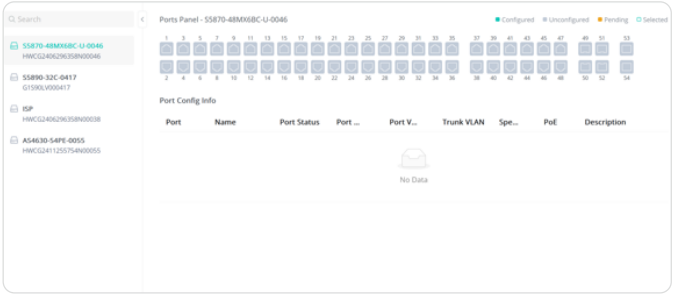
  In the **Select Switches** tab, select the switches to be configured, and then click **Next** until going to the **Port Config** tab.

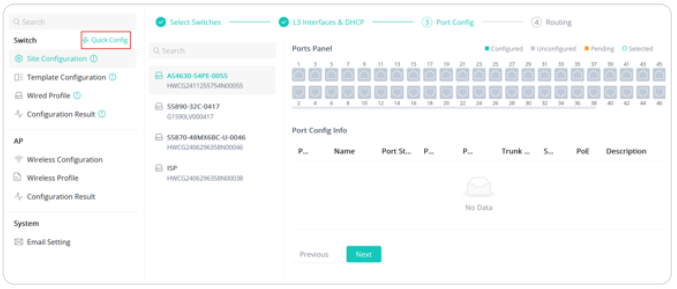
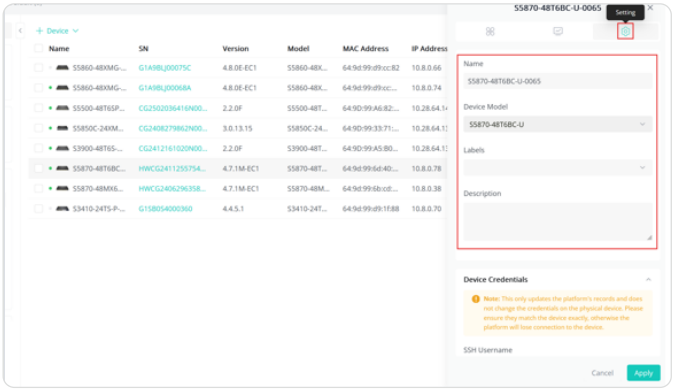


5. Click the switch to be configured, and then select one or multiple ports in the port panel.

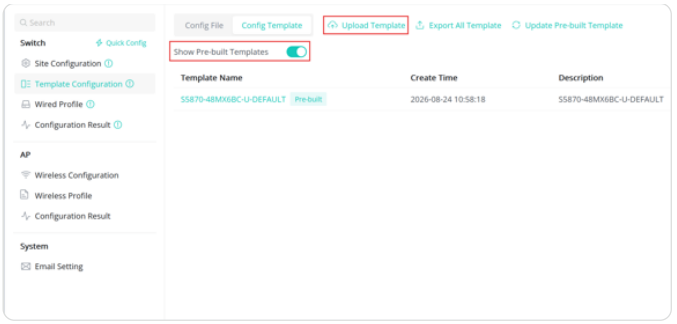
   To select multiple ports, hold down **Ctrl** while clicking multiple ports.

6. In the pop-up window, click the **Port Profile** tab. Select a port profile from the drop-down list, and then click **Save**.

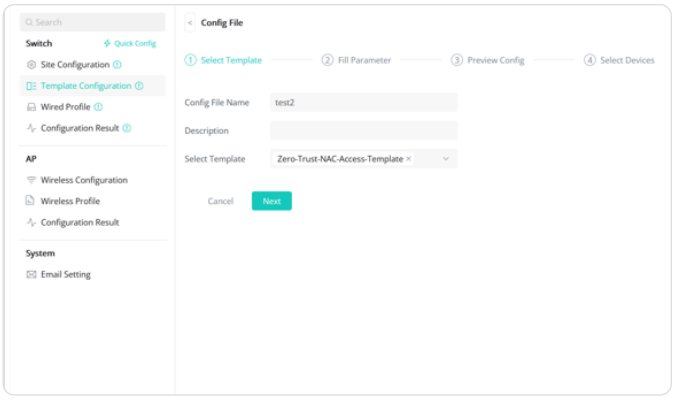
	7. Apply port configurations to the switch as follows: • If you configure switch ports through the “Ports” page, click **Deploy x Changes**.  • If you configure switch ports through the **Quick Config** wizard, click **Next** and then click **Apply** to complete the quick configuration. 	
Applying Port Configurations Directly	1. Select a site to which the PicOS switches to be configured belong. 2. Go to the port panel through one of the following ways: • Click the **Ports** icon from the navigation bar to go to the “Ports” page.  • Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar to open the **Quick Config** wizard.	• Configuring Switch Ports Directly

	In the **Select Switches** tab, select the switches to be configured, and then click **Next** until going to the **Port Config** tab.  3. Click the switch to be configured, and then select one or multiple ports in the port panel. To select multiple ports, hold down **Ctrl** while clicking multiple ports. 4. In the **Custom** tab of the pop-up window, customize port configurations. 5. Apply port configurations to the switch as follows: • If you configure switch ports through the “Ports” page, click **Deploy x Changes**. • If you configure switch ports through the **Quick Config** wizard, click **Next** and then click **Apply** to complete the quick configuration.	
Configuring a Single Switch	1. Select the site to which the PicOS switch belongs. 2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click a PicOS switch, and then click the **Setting** tab of the side panel. 3. At the top of the **Setting** tab, modify general switch configurations if needed. 	• Configuring a Single Switch

	4. In the **Device Credentials** section, modify the **SSH Username** and **SSH Password** if needed. Ensure that the username and password match the switch exactly. Otherwise, AmpCon-Campus cannot access and manage the switch. If the **SSH Username** and **SSH Password** are incorrect, you can modify them here. The updated username and password will update the credentials on AmpCon-Campus but will not change the credentials on the switch side. 5. In the **L3 Interface & DHCP** section, click **+ Create L3 Interface & DHCP** to create an L3 interface and DHCP configuration item. 6. In the **Static Route** section, click **+ Static Route** to create a static route configuration item. 7. In the **OSPF** section, customize OSPF configurations. 8. Click **Apply**. Then, the configurations will be pushed to the switch.	
Applying Template Configurations through Templates	1. Select the site to which the PicOS switches to be configured belong. 2. Click the **Settings** icon from the navigation bar, and then click **Template Configuration** in the sidebar. 3. On the “Template Configuration” page, click the **Config Template** tab, and then click **Show Pre-built Templates**. Check whether the built-in template meets your needs. If not, add a new template by clicking **Upload Template**.	• Configuring through Templates

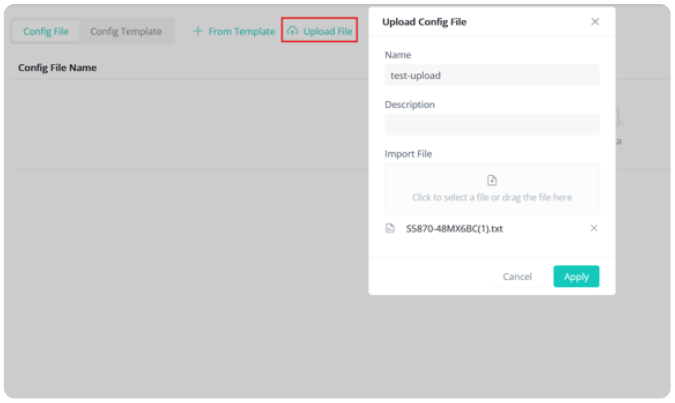


4. Click the **Config File** tab, and then click **+ From Template**.
5. In the **Select Template** tab, input the following information, and then click **Next**.

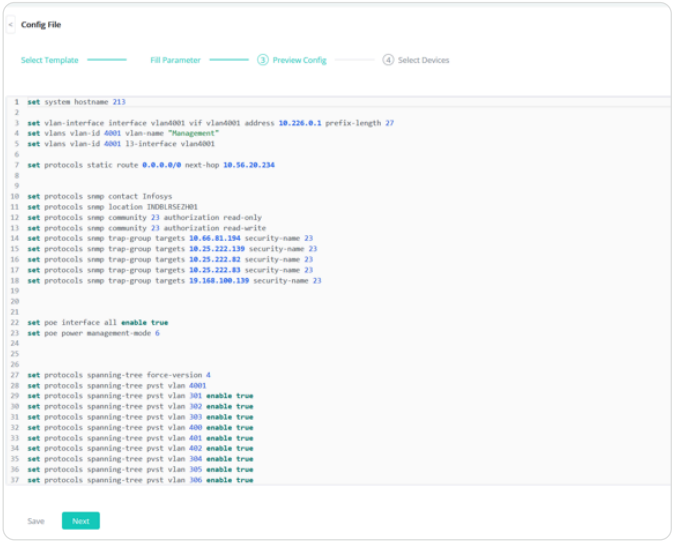


6. In the **Fill Parameter** tab, specify values for all required parameters, and then click **Next**.
7. In the **Preview Config** tab, check the CLI commands generated based on the provided parameter values, and then click **Next**.
8. In the **Select Devices** tab, select the switches to be configured, and then click **Apply**.

Applying Template Configurations by Uploading Configuration Files	1. Select the site to which the PicOS switches to be configured belong. 2. Click the **Settings** icon from the navigation bar, and then click **Template Configuration** in the sidebar. 3. In the **Config File** tab of the “Template Configuration” page, click **Upload File**. In the pop-up window, input the following information, and then click **Apply**. Then, you can see the configuration file in the **Config File** tab.	• Configuring by Uploading Configuration Files



4. Click the configuration file name.
5. In the **Preview Config** tab, check the CLI commands generated based on the provided parameter values, and then click **Next**.



6. In the **Select Devices** tab, select the switches to be configured, and then click **Apply**.

Verifying Configuration Results

After configuration, click **Configuration Result** from the sidebar. On the “Configuration Result” page, verify whether configurations are applied to PicOS switches successfully. For more information, see Checking Configuration Results.

What to Do Next

After you configure PicOS switches, check the following tasks. These tasks are **not mandatory** and can be performed only when needed.

Table 4. Post-Configuration Tasks and Links

Category	Task	Reference Link

Comparing Configurations	Compare configurations between two external files, compare running or backup configurations from the same or different PicOS switches, or compare configurations from an external file with running or backup configurations on a PicOS switch.	• Comparing Switch Configurations
Backing Up Configurations	Back up switch configurations at a specified interval and time, or back up the currently running configuration on switches. Check the currently running configurations on a PicOS switch.	• Backing Up Configurations

Wireless Network Deployment Workflow

AmpCon-Campus supports deploying wireless networks through Zero Touch Provisioning (ZTP). This guide provides a comprehensive overview of wireless network deployment procedures.

> **NOTE**
>
> The guide lists only the workflow of wireless network deployment. You must check the reference links for detailed information.

Procedure
What to Do Next

Procedure

To deploy a wireless network, complete the following tasks:

Table 1. Deployment Tasks and Links

Task	Reference Link
1. Learn about wireless network-related concepts, highlights of wireless network management, and the Zero Touch Provisioning (ZTP) workflow of APs.	• Wireless Overview • Concepts
2. Select an existing site for the APs, or add a new site as needed.	• Adding a Site
3. Configure site-level wireless configurations for the site.	• Configuring All APs in a Site
4. Onboard APs to AmpCon-Campus. The ZTP process will start. The APs will connect to AmpCon-Campus and retrieve site-level wireless configurations without manual intervention. For the ZTP workflow, see AP ZTP Workflow. Once completed, the APs are managed by AmpCon-Campus, the wireless network is deployed, and site-level wireless configurations are pushed to the APs automatically.	• Onboarding APs
5. Confirm that AP onboarding succeeds, the APs become online, and the site-level wireless configurations are applied successfully. When possible, verify the expected	• No Reference Link

SSIDs and connect a test client to confirm service availability.	
6. Optional: After onboarding, add device-specific configurations to an AP when it requires configurations different from other APs in the site. **NOTE** You can configure a single AP only after you add site-level wireless configurations.	• Configuring a Single AP

What to Do Next

After you deploy a wireless network, check the following tasks for network monitoring and maintenance. These tasks are **not mandatory** and can be performed only when needed.

Table 2. Maintaining and Monitoring Tasks and Links

Category	Task	Reference Link
Maintaining Wireless Networks	Establish a remote terminal session to an AP through remote TTY shell (RTTY).	• Accessing APs
	When an AP experiences signal anomalies or requires maintenance or replacement, you can remotely trigger its LED to blink, enabling quick on-site localization.	• Positioning APs
	Reboot a single online AP or multiple online APs in batches.	• Rebooting APs
	Upgrade AP firmware one by one or in batches. In addition, you can upgrade AP firmware immediately or at a scheduled date and time.	• Upgrading APs
	Wipe all custom settings and restore an online AP to its original status (factory settings). This action is irreversible.	• Restoring to Factory Settings
	Capture remote packets from target ports of an online AP for rapid troubleshooting.	• Capturing Remote Port Packets
	Clear all device-specific configurations for an AP and force the AP to inherit site-level	• Enforcing Site Configurations

	configurations.	
	Use one-click network optimization to rapidly optimize wireless network performance through automation technologies.	• Optimizing Wireless Networks
	If some issues can be resolved only through CLI configurations or some advanced functions can be achieved only through CLI configurations, you can contact FS support engineers to perform AP debugging or configuration for you through this feature.	• Configuring APs via CLI
	Delete a single AP or multiple APs in batches.	• Deleting APs
	Move a single AP or multiple APs to another site.	• Moving APs to Another Site
Monitoring Wireless Networks	Get an overview of the wireless network in the currently selected site on the “Dashboard” page.	• Wireless Networks
	View APs and their connected devices to understand the network structure of the currently selected site.	• Topology
	View basic information, in-depth metrics, and configurations of APs.	• Access Points
	Monitor wireless clients connected to each managed AP.	• Wireless Clients

Ansible Automation Workflow

Ansible is an open-source tool to automate configuration management, application deployment, and task automation. Ansible uses the simple, declarative language written in YAML, which is called playbooks, to automate your tasks.

By using AmpCon-Campus, you can write, import, run, and schedule Ansible playbooks on managed PicOS switches, reducing manual effort and configuration errors while improving network management efficiency.

This guide provides a comprehensive overview of Ansible playbook running procedures.

> **NOTE**
>
> The guide lists only the workflow of Ansible playbook running. You must check the reference links for detailed information.

Guidelines
Prerequisites
Procedure
What to Do Next

Guidelines

- Playbooks can be run only on PicOS switches managed by AmpCon-Campus.
- Before running Ansible playbooks, pay attention to the following best practices:
  - **Test in a lab:** Always test your automation scripts in a lab or on non-production devices to ensure they work as expected.
  - **Idempotency:** Ansible playbooks must be idempotent, meaning running the playbook multiple times will not cause unintended changes.
  - **Backups:** Before applying any configuration, ensure that you have backups of the current configurations. For more information, see Backing Up Configurations.

Prerequisites

Before you run Ansible playbooks for automation, ensure that the following prerequisite tasks have been completed. Otherwise, Ansible playbook execution will fail.

Table 1. Prerequisite Tasks and Links

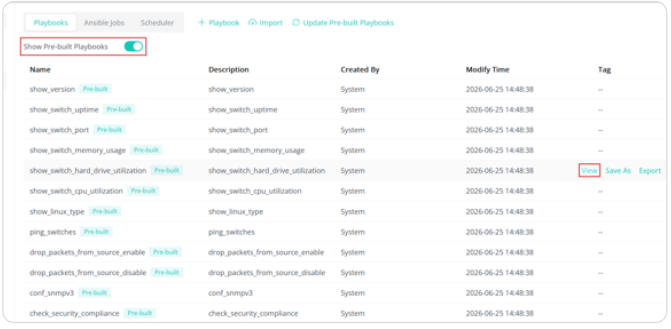
Task	Reference Link
Each PicOS switch to run Ansible playbooks is successfully onboarded to AmpCon-Campus.	• Onboarding PicOS Switches

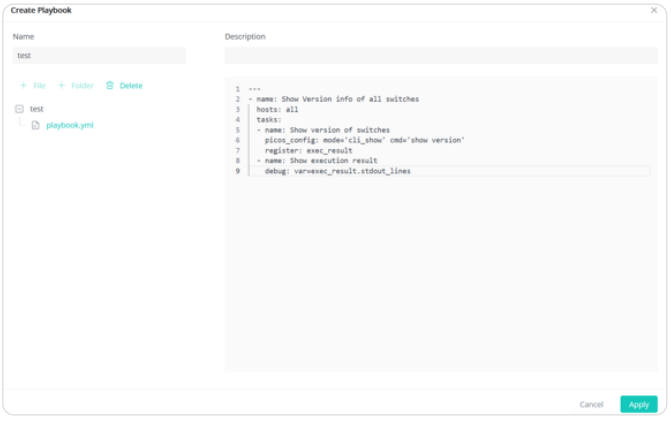
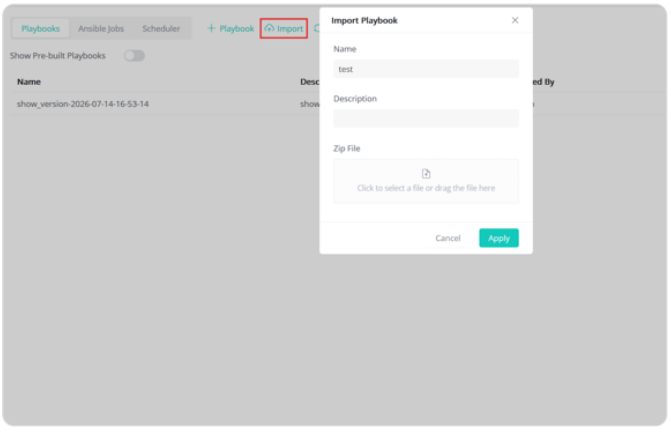
Each PicOS switch to run Ansible playbooks is online (connected to AmpCon-Campus).	• Viewing the PicOS List
Ensure that the **SSH Username** and **SSH Password** in the device credential configuration match the PicOS switches exactly.	• Device Credential Configurations

Procedure

To run an Ansible playbook with AmpCon-Campus, complete the following tasks:

Table 2. Playbook Running Tasks and Links

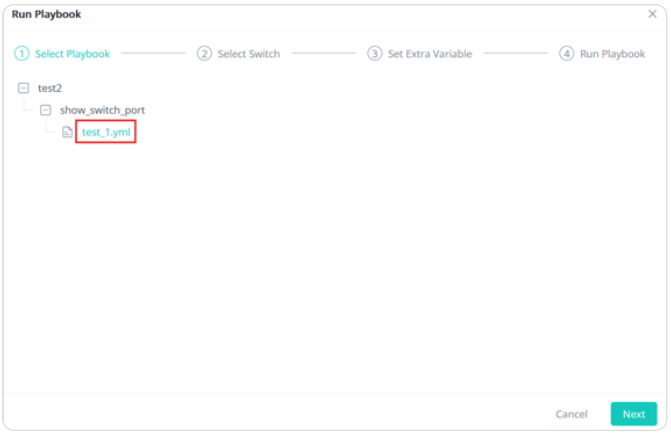
Category	Task	Reference Link
Checking Pre-Built Playbooks	AmpCon-Campus offers a series of pre-built Ansible playbooks. 1. Select a site to which the PicOS switches belong. 2. Click the **Maintain** icon from the navigation bar, and then click **Automation** from the sidebar. 3. In the **Playbooks** tab, toggle on **Show Pre-built Playbooks**. 4. Hover over each pre-built playbook, and then click **View**.  5. In the pop-up window, click **playbook.yml**, and then check whether the configurations in the right panel meet your needs. If yes, hover over it, and then click **Save As** to copy it as a new playbook. **NOTEs** • Pre-built playbooks cannot be run directly.	• Using Pre-Built Playbooks

	• Pre-built playbooks are not guaranteed to be compatible with all PicOS models. You need to evaluate pre-built playbooks based on the target switch model, firmware version, and supported commands.	
Writing or Importing Playbooks	If the pre-built Ansible playbooks don't meet your needs, write or import a playbook in the **Playbooks** tab as follows: • Click **+ Playbook**, and then write a playbook in the AmpCon-Campus UI.  • Click **Import**, and then import a local playbook to AmpCon-Campus. 	• Examples for Ansible Playbooks • Writing a Playbook • Importing a Playbook • Using Ansible playbooks
Optional: Checking Playbook Syntax	Before you run a playbook, check whether the playbook syntax is valid. 1. In the **Playbooks** tab, hover over the playbook, and then click **Check**. 2. In the pop-up window, click the .yml file, and then click **Check**.	• Checking the Syntax for a Playbook

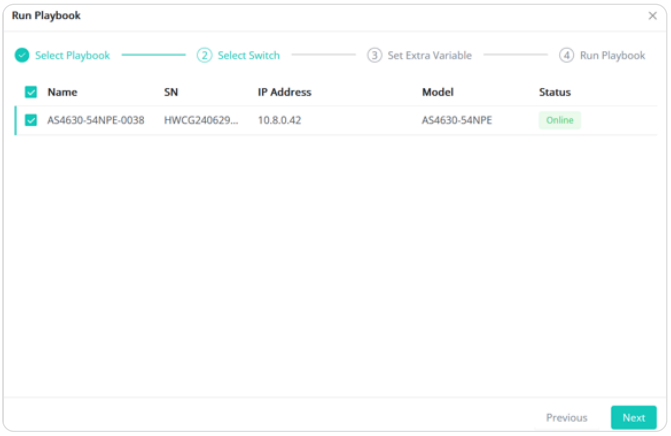


Running Playbooks

1. In the **Playbooks** tab, hover over the playbook, and then click **Run**.
2. In the **Select Playbook** tab of the pop-up window, click the .yml file under the playbook name, and then click **Next**.

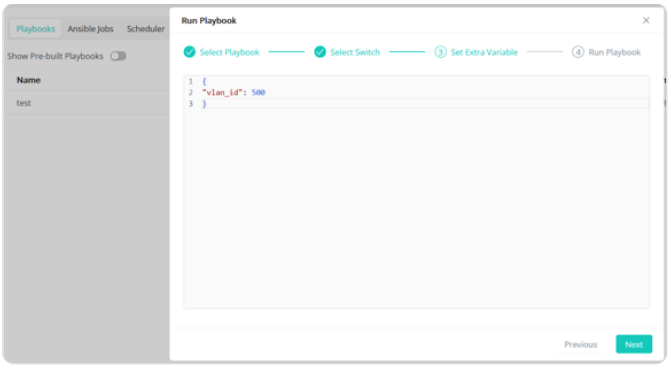


3. In the **Select Switch** tab, select one or multiple PicOS switches, and then click **Next**.

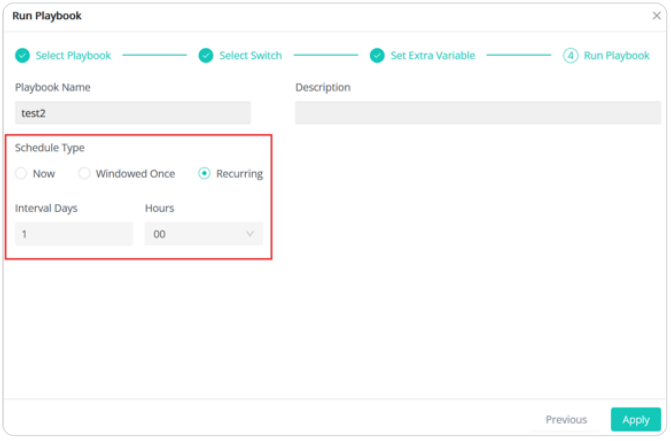


4. If variables are specified in the playbook, enter variable values in the **Set Extra Variable** tab, and then click **Next**.

- Running Playbooks



5. In the **Run Playbook** tab, select a playbook execution type, and then click **Apply**.
   You can run the playbook immediately, once within a specified time range, or periodically at specified intervals.



Checking Ansible Job Results and Output	An Ansible job is a single execution of an Ansible playbook. After running Ansible playbooks, view the Ansible jobs and PicOS switches related to these playbooks. You can also check the execution results and output of these jobs.	• Managing Ansible Jobs

What to Do Next

After you run an Ansible playbook, check the following tasks. These tasks are **not mandatory** and can be used only when needed.

Table 3. Post-Execution Tasks and Links

Category	Task	Reference Link
Viewing Playbook Schedules	View playbook schedules in the calendar view or list view.	• Viewing Playbook Schedules

Troubleshooting for Failed Ansible Jobs	If a playbook fails to run on PicOS switches, check the possible reasons and solutions for troubleshooting.	• Ansible Playbook Troubleshooting

Planning

Before you install the AmpCon-Campus server, you must check supported information and prepare installation requirements.

For detailed information, see the following child topics:

- Supported Information
- Installation Requirements

Supported Information

Before you deploy AmpCon-Campus, check the supported AmpCon-Campus deployments and supported switches.

Supported AmpCon-Campus Deployments
Supported Switches
Supported APs

Supported AmpCon-Campus Deployments

The following AmpCon-Campus deployments are supported:

Table 1. Supported Deployment Information

Indicator	Support information
Deployment method	VMware ESXi 6.7, 7.0, 8.0, QEMU / KVM for Ubuntu 22.04 LTS, Oracle VirtualBox for lab only, physical machine based on Ubuntu 22.04 LTS with Docker
Maximum number of switches supported	1000
Maximum number of registered users	1000
Maximum number of online users	100
Storage duration of system logs	2 months
Storage duration of operation logs	2 months
Maximum storage of current alerts	Unlimited
Maximum storage of historical alerts	2 months

Supported Switches

- AmpCon-Campus supports **managing** switches with PicOS installed, including FS, Edgecore, and DELL switches. For detailed support lists, see Supported PicOS Switches for 3.0.0.

> **NOTE**
>
> Managing switches means that you can use AmpCon-Campus to manage the lifecycle of switches, such as deploying and configuring switches.

- AmpCon-Campus supports **monitoring** FSOS switches. For the detailed support list, see Supported FSOS Switches for 3.0.0.

  > **NOTE**
  >
  > Though FSOS switches can be onboarded to AmpCon-Campus, they can't be managed by AmpCon-Campus. You can only monitor them as described in FSOS Switches.

Supported APs

AmpCon-Campus supports deploying and managing wireless networks and access points (APs). For the detailed support list, see Supported APs for 3.0.0.

Supported PicOS Switches for 3.0.0

AmpCon-Campus 3.0.0 supports managing the following PicOS switches:

Guidelines
FS Hardware
Edgecore Hardware
DELL Hardware

Guidelines

- For most FS switches, it is recommended to install PicOS 4.7.1M or later. But for specific FS switch models, refer to **Table 1** for the recommended PicOS versions.

Table 1. Recommended PicOS Versions for Specific FS Switch Models

FS Models	Version
S3540L-24P, S3540L-24T, S3540L-48T	PicOS 4.7.3M
S5470-48Y, S5470-24Y, S5470-16Q, S5470-48S, S5440-12S, S5440-24T	PicOS 4.7.4M
S5570-48X, S5590-64C	PicOS 4.7.5E
S8510-24CD	PicOS 4.5.5.1
S8520-32D	PicOS 4.5.4E

- For Edgecore and DELL switches, it is recommended to install PicOS 4.6.0E or later. Otherwise, some features of AmpCon-Campus might not work.

FS Hardware

Table 2. Supported FS Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	S3270-10TM	10 × 10M/100M/1G copper, 2 × 1G/2.5G SFP	Wolfhound 2	ARM Cortex A9

1G Switch Portfolio	S3270-10TM-P	10 × 10M/100M/1G copper PoE, 2 × 1G/2.5G SFP	Wolfhound 2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM	24 × 10M/100M/1G copper, 4 × 1G/2.5G SFP	Wolfhound 2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM-P	24 × 10M/100M/1G copper PoE, 4 × 1G/2.5G SFP	Wolfhound 2	ARM Cortex A9
1G Switch Portfolio	S3270-48TM	48 × 10M/100M/1G BASE-T RJ45, 4 × 1G/2.5G SFP	Wolfhound 2	ARM Cortex A9
1G Switch Portfolio	S3410-24TS	24 × 10M/100M/1G BASE-T RJ45, 4 × 1G/10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410-24TS-P	24 × 10M/100M/1G BASE-T RJ45, 2 × 1G RJ45/SFP Combo, 2 × 1G/10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410-48TS	48 × 10M/100M/1G BASE-T RJ45, 4 × 1G/10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410-48TS-P	48 × 10M/100M/1G BASE-T RJ45 PoE+, 2 × 1G RJ45/SFP Combo,	Hurricane 2	ARM Cortex A9

		2 × 1G/10G SFP+		
1G Switch Portfolio	S3410C-8TMS-P	8 × 10M/100M/1G BASE-T PoE+, 2 × 1G/2.5G/5G BASE-T, 2 × 1G/10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410C-16TF	16 × 10M/100M/1G BASE-T RJ45, 2 × 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410C-16TF-P	16 × 10M/100M/1G BASE-T RJ45 8 × PoE+, 2 × 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410C-16TMS-P	16 × 10M/100M/1G BASE-T 8 × PoE+, 2 × 1G/2.5G/5G BASE-T, 2 × 1G/10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410L-24TF	24 × 10M/100M/1G BASE-T RJ45, 4 × 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410L-24TF-P	24 × 10M/100M/1G BASE-T RJ45 PoE+, 4 × 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3410L-48TF	48 × 10M/100M/1G BASE-T RJ45, 4 × 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3540L-24P	24 × 1G-T PoE+, 4 × 10G SFP+	Hurricane 2	ARM Cortex A9

1G Switch Portfolio	S3540L-24T	24 × 1G-T, 4 × 10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S3540L-48T	48 × 1G-T, 4 × 10G SFP+	Hurricane 2	ARM Cortex A9
1G Switch Portfolio	S5440-24T	24 × 10M/100M/1G BASE-T RJ45, 8 × 1G/10G SFP+	Tsingma_mx	ARM 64
1G Switch Portfolio	S5810-28FS	20 × 1G SFP, 8 × 1G RJ45/SFP Combo, 4 × 1G/10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-28TS	24 × 10M/100M/1G BASE-T RJ45, 4 × 1G RJ45/SFP Combo, 4 × 1G/10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48FS	48 × 100M/1G SFP, 4 × 1G/10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48TS	48 × 10M/100M/1G BASE-T, 4 × 1G/10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48TS-P	48 × 100M/1G BASE-T RJ45 PoE+, 4 × 1G/10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5860-24MG-U	24 × 100M/1G/2.5G/5G BASE-T PoE++, 4 × 10G/25G SFP28	Hurricane 3-MG	ARM Cortex A9

1G Switch Portfolio	S5860-48MG-U	48 × 100M/1G/2.5G/5G BASE-T PoE++, 4 × 10G/25G SFP28, 2 × 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
1G Switch Portfolio	S5870-48T6BC	48 × 10M/100M/1G BASE-T RJ45, 4 × 10G/25G SFP28, 2 × 40G/100G QSFP28	Trident3-X3	Intel x86
1G Switch Portfolio	S5870-48T6BC-U	48 × 10M/100M/1G BASE-T RJ45 PoE++, 4 × 10G/25G SFP28, 2 × 100G QSFP28	Trident3-X3	Intel x86
1G Switch Portfolio	S5870-48MX6BC-U	36 × 1G/2.5G PoE++, 12 × 1G/2.5G/5G/10G PoE++, 4 × 25G SFP28, 2 × 100G QSFP28	Trident3-X3	Intel x86
10G Switch Portfolio	S5440-12S	4 × 10M/100M/1G BASE-T RJ45, 12 × 1G/10G SFP+	Tsingma_mx	ARM 64
10G Switch Portfolio	S5470-48S	48 × 1G/10G SFP+, 6 × 40G QSFP+ (split to 4 × 10G)	Tsingma_mx	ARM 64
10G Switch Portfolio	S5570-48X	48 × 10G RJ45, 6 × 40G/100G QSFP28	Trident3-X5	Intel x86

10G Switch Portfolio	S5860-20SQ	20 × 1G/10G SFP+, 4 × 10G/25G SFP28, 2 × 40G QSFP+ (split to 4 × 10G)	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XB-U	24 × 100M/1G/2.5G/5G/10G BASE-T PoE++, 4 × 1G/10G SFP+, 4 × 10G/25G SFP28	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XMG	24 × 100M/1G/2.5G/5G/10G BASE-T, 4 × 1G/10G SFP+, 4 × 10G/25G SFP28	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG	48 × 100M/1G/2.5G/5G/10G BASE-T, 4 × 10G/25G SFP28, 2 × 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG-U	48 × 100M/1G/2.5G/5G/10G BASE-T PoE++, 4 × 10G/25G SFP28, 2 × 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
25G Switch Portfolio	S5470-24Y	24 × 10G/25G SFP28, 4 × 40G/100G QSFP28 (split to 4 × 10G/25G)	Tsingma_mx	ARM 64

25G Switch Portfolio	S5470-48Y	48 × 10G/25G SFP28 8 × 40G/100G QSFP28 (split to 4 × 10G/25G)	Tsingma_mx	ARM 64
25G Switch Portfolio	S5580-48Y	48 × 10G/25G SFP28, 8 × 40G/100G QSFP28 (split to 4 × 10G/25G), 2 × 1G/10G SFP+	Trident3-X7	Intel x86
40G Switch Portfolio	S5470-16Q	16 × 40G QSFP+ (split to 4 × 10G), 8 × 100G QSFP28 (split to 4 × 10G/25G)	Tsingma_mx	ARM 64
100G Switch Portfolio	S5590-64C	64 × 100G QSFP28 (split to 4 × 10G/25G)	Tomahawk 2	Intel x86
100G Switch Portfolio	S5890-32C	32 × 40G/100G QSFP28 (split to 4 × 10G/25G)	Trident3-X7	Intel x86
200G Switch Portfolio	S8510-24CD	24 × 200G QSFP56, 8 × 400G QSFP-DD	Trident4-X9	Intel x86
400G Switch Portfolio	S8520-32D	32 × 400G QSFP-DD, 2 × 10G SFP+	Trident4-X11	Intel x86

Edgecore Hardware

Table 3. Supported Edgecore Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	AS4610-30T	24 × 1G-T, 4 × 10G	Helix4	ARM Cortex A9

1G Switch Portfolio	AS4610-30P	24 × 1G PoE, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54P	48 × 1G PoE, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54T	48 × 1G-T, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54T(B)	48 × 1G-T, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4625-54P	48 × 1G PoE, 6 × 10G	Trident3-X2	Intel x86
1G Switch Portfolio	AS4625-54T	48 × 1G-T, 6 × 10G	Trident3-X2	Intel x86
1G Switch Portfolio	AS4630-54PE	48 × 1G PoE, 4 × 25G	Trident3	Intel x86
1G Switch Portfolio	AS4630-54TE	48 × 1G, 4 × 25G	Trident3-X3	Intel x86
10G Switch Portfolio	AS5812-54X	48 × 10G , 6 × 40G	Trident2+	Intel x86
10G Switch Portfolio	AS5835-54T	48 × 10G-T, 6 × 40G	Trident3-X5	Intel x86
25G Switch Portfolio	AS7312-54X	48 × 25G, 6 × 100G	Tomahawk+	Intel x86
25G Switch Portfolio	AS7326-56X	48 × 25G, 8 × 100G	Trident3-X7	Intel x86
40G Switch Portfolio	AS6812-32X	32 × 40G	Trident2+	Intel x86
100G Switch Portfolio	AS7726-32X	32 × 100G	Trident3-X7	Intel x86
100G Switch Portfolio	AS7816-64X	64 × 100G	Tomahawk2	Intel x86
Multi-Gig Switch	AS4630-54NPE	36 × 1G/2.5G PoE+,	Trident3-X3	Intel x86

Portfolio		12 × 1G/2.5G/5G/10G PoE		

DELL Hardware

Table 4. Supported DELL Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	N3024ET-ON	24 × 1G, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3048EP-ON	48 × 1G PoE, 4 × 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3224P-ON	24 × 1G 30W PoE, 4 × 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224T-ON	24 × 1G, 4 × 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248P-ON	48 × 1G 30W PoE, 4 × 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248TE-ON	48 × 1G, 4 × 10G	Trident3-X3	Intel x86
10G Switch Portfolio	S4148T-ON	48 × 10G BASE-T, 2 × 40G, 4 × 100G	Maverick	Intel x86
25G Switch Portfolio	S5248F-ON	48 × 25G, 8 × 100G	Trident3-X7	Intel x86
Multi-Gig Switch Portfolio	N2248PX-ON	48 × 1G/2.5G 30W/60W PoE, 4 × 25G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248X-ON	48 × 1G/2.5G, 4 × 25G	Hurricane3-MG	Intel x86

Multi-Gig Switch Portfolio	N3132PX-ON	24 × 1G PoE+, 8 × 1G/2.5G/5G PoE+, 4 × 10G	Firebolt 4 FS	ARM Cortex A9
Multi-Gig Switch Portfolio	N3224PX-ON	24 × 1G/2.5G/5G/10G 90W PoE+, 4 × 25G	Trident3-X3	Intel x86
Multi-Gig Switch Portfolio	N3248PXE-ON	48 × 1G/2.5G/5G/10G 90W PoE, 4 × 25G	Trident3-X5	Intel x86
Multi-Gig Switch Portfolio	N3248X-ON	48 × 1G/2.5G/5G/10G, 4 × 25G	Trident3-X5	Intel x86

Supported FSOS Switches for 3.0.0

Before you onboard FSOS switches to AmpCon-Campus 3.0.0, ensure that the FSOS switches are supported by AmpCon-Campus.

See the following support list:

Table 1. Supported FSOS Switch List

Switch Series	Switch Model
IES3110	IES3110-8TFM-P, IES3110-8TFP-R, IES3110-8TF-R
TSN3220	TSN3220-10S-U
S3100	S3100-8TMS-P, S3100-16TMS-P, S3100-16TF, S3100-16TF-P
S3270	S3270-10TM, S3270-10TM-P, S3270-24TM, S3270-24TM-P, S3270-48TM
S3410	S3410-24TS-P, S3410-48TS-P, S3410-24TF-P
S3910	S3910-24TS, S3910-24TF, S3910-48TF, S3910-48TS
S5810	S5810-48FS, S5810-28FS, S5810-28TS, S5810-48TS, S5810-48TS-P
S5860	S5860-20SQ, S5860-48SC, S5860-24XMG, S5860-24MG-U, S5860-48XMG, S5860-48XMG-U, S5860-24XB-U
S5800	S5800-48T4S, S5800-48MBQ
S5850	S5850-48S6Q-R, S5850-48B8C, S5850-24B4C, S5850-24XMG-U
S3950	S3950-4T12S-R
S5850C	S5850C-24XMG2C, S5850C-24S2C
S8050	S8050-20Q4C
S8550	S8550-16Q8C
S3150	S3150-8T2FP
S3260	S3260-8T2FP

S3400	S3400-24T4FP
S3700	S3700-24T4F
S3900-R	S3900-48T6S-R
S5500	S5500-48T6SP-R

Supported APs for 3.0.0

Before you onboard access points (APs) to AmpCon-Campus 3.0.0, ensure that the APs are supported by AmpCon-Campus.

See the following support list:

Table 1. Supported APs

Product	Product Description
AP-N716	AP-N716, Wi-Fi 7 802.11be 9300 Mbps Indoor Access Point, Seamless Roaming & 2 x 2 MU-MIMO Three Radios, PicOS®, Manageable via AmpCon-Campus (Without PoE Injector)
AP-N516	AP-N516, Wi-Fi 6 802.11ax 3000 Mbps Indoor Access Point, Seamless Roaming & 4 x 4 MU-MIMO Dual Radios, PicOS®, Manageable via AmpCon-Campus (Without PoE Injector)
AP-N506	AP-N506, Wi-Fi 6 802.11ax 1800 Mbps Indoor Access Point, Seamless Roaming & 2 x 2 MU-MIMO Dual Radios, PicOS®, Manageable via AmpCon-Campus (Without PoE Injector)
AP-N506H	AP-N506H, Wi-Fi 6 802.11ax 3000 Mbps Indoor Access Point, Seamless Roaming & 2 x 2 MU-MIMO Dual Radios, PicOS®, Manageable via AmpCon-Campus (Without PoE Injector)
AP-T566D	AP-T566D, Wi-Fi 6 802.11ax 1800 Mbps Outdoor Access Point, Seamless Roaming & 2 x 2 MU-MIMO Dual Radios, PicOS®, Manageable via AmpCon-Campus (Without PoE Injector)

Installation Requirements

Before you install AmpCon-Campus, ensure that the following requirements are met.

Server Requirements
Network Requirements

Server Requirements

If you want to install AmpCon-Campus on a **physical machine**, ensure that the physical machine meets the following requirements:

> **NOTE**
>
> To install AmpCon-Campus on a **virtual machine**, ensure that the hypervisor has the following resources (CPU, memory, and hard disk) to be allocated when you import the AmpCon-Campus image.

Table 1. Machine Requirements

Indicators		Requirements
CPU	Clock speed	2.0 GHz or faster
	Number of cores	At least 4 CPU cores
Memory		At least 16 GB
Hard disk		At least 512 GB
Operating system		Ubuntu 22.04 LTS (X86 architecture) with Docker

Network Requirements

Before you install AmpCon-Campus, set the firewall and proxy properly to allow the following network access:

Table 2. Network Requirement for the AmpCon-Campus Machine

TCP/UDP	Port	Protocol
TCP	80	HTTP
TCP	443	HTTPS

TCP	15002	WebSocket
UDP	69	TFTP
UDP	80	OpenVPN

NOTEs

- On AmpCon-Campus, each managed PicOS switch has two IP addresses: **Registration IP** and **VPN IP**.
  - **Registration IP** is the management IP address of a PicOS switch. **Registration IP** is used to connect to AmpCon-Campus during the switch onboarding process.
  - However, **Registration IP** might be changed. To ensure uninterrupted connection between AmpCon-Campus and a PicOS switch after **Registration IP** is changed, OpenVPN is introduced to AmpCon-Campus.
  - OpenVPN is an open-source virtual private network (VPN) solution designed to create secure, encrypted communication tunnels over networks.

    After a PicOS switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between AmpCon-Campus and the switch is established, and **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-Campus and the switch will communicate through the VPN tunnel.
- AmpCon-Campus also functions as the OpenVPN server, and its OpenVPN IP address is 10.8.0.1. The default subnet for OpenVPN is 10.8.0.0/20.

  If the default subnet has conflicts with your network, AmpCon-Campus can't work well. Contact the FS support team to resolve this issue.

Deploying AmpCon-Campus

To use AmpCon-Campus features, install AmpCon-Campus first.

You cannot upgrade directly from previous AmpCon-Campus versions to AmpCon-Campus 3.0.0; a fresh installation of AmpCon-Campus 3.0.0 is required.

See the following child topics:

- Installing AmpCon-Campus
- Uninstalling on Physical Machines (Ubuntu Docker)

Installing AmpCon-Campus

To use AmpCon-Campus features, install AmpCon-Campus on a virtual or physical machine.

Installation Steps

To install AmpCon-Campus on a virtual machine, see the following topics:

- Installing on VirtualBox for Lab Only
- Installing on VMware ESXi
- Installing on QEMU or KVM

To install AmpCon-Campus on a physical machine, see Installing on Physical Machines (Ubuntu Docker).

What to Do Next

If multiple NICs are added to the virtual or physical machine where AmpCon-Campus is installed and the global IP is not specified during activation or installation, you must contact support engineers to specify the NIC IP address.
Otherwise, the connections between AmpCon-Campus and the switches and access points (APs) to be managed might fail.

Installing on VirtualBox for Lab Only

You can install AmpCon-Campus on VirtualBox for lab purposes only. For production environments, you are advised to use a supported enterprise-grade virtualization solution, as described in Supported Information.

To use VirtualBox in general, see the Oracle VirtualBox documentation.

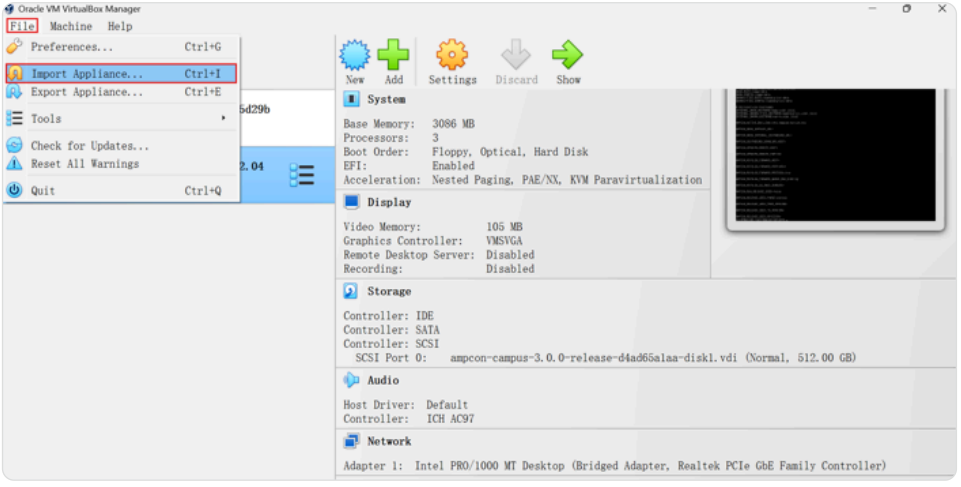
Prerequisites
Installation Procedure
What to Do Next

Prerequisites

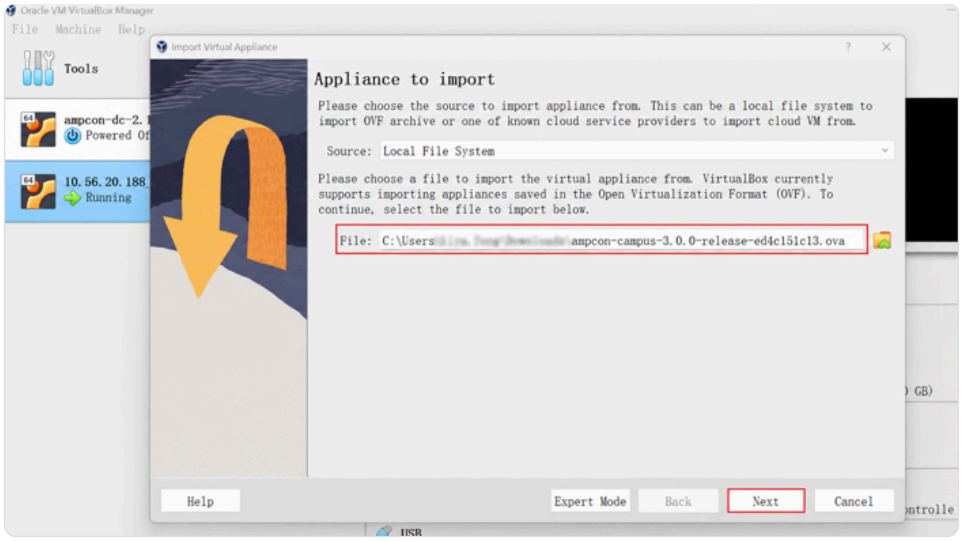
- Ensure that the installation requirements are met.
- Open the AmpCon-Campus download page, and select **United States** as the region. Then, download the zipped AmpCon-Campus image (**AmpCon-Campus for VirtualBox V3.0.0 Software**).
- Copy the zipped AmpCon-Campus image file to the host machine where the hypervisor exists, and then unzip it.

Installation Procedure

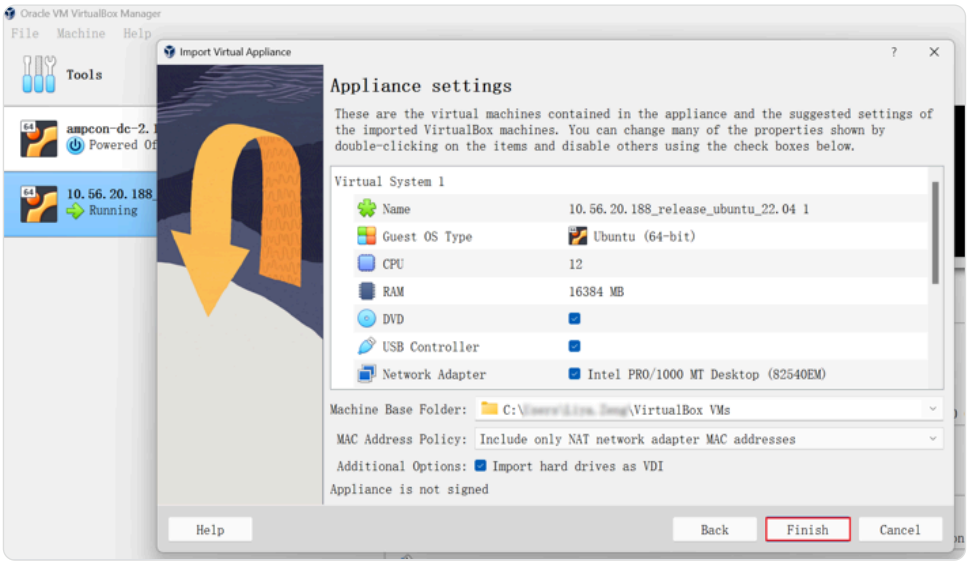
1. Open the VirtualBox console, and then click **File > Import Appliance**.



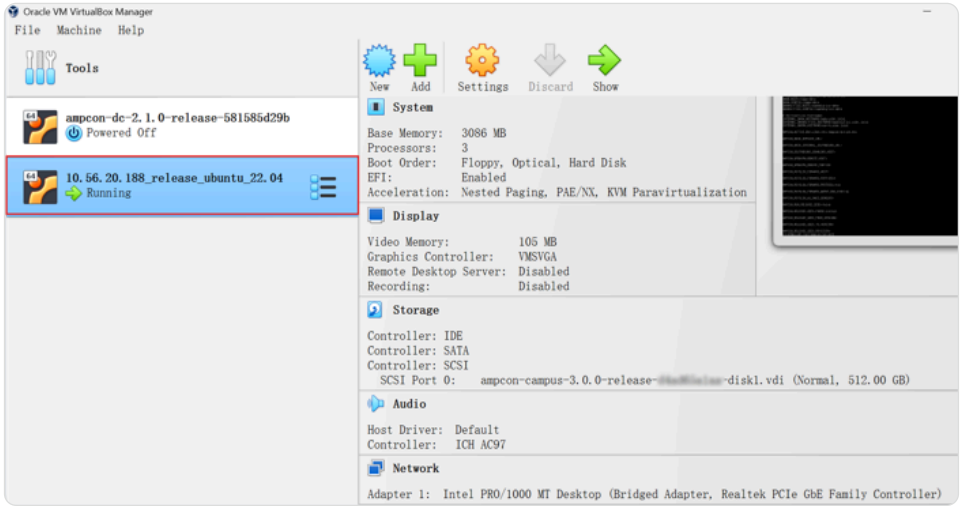
2. Select **Local File System**, import the AmpCon-Campus .ova image file, and then click **Next**.



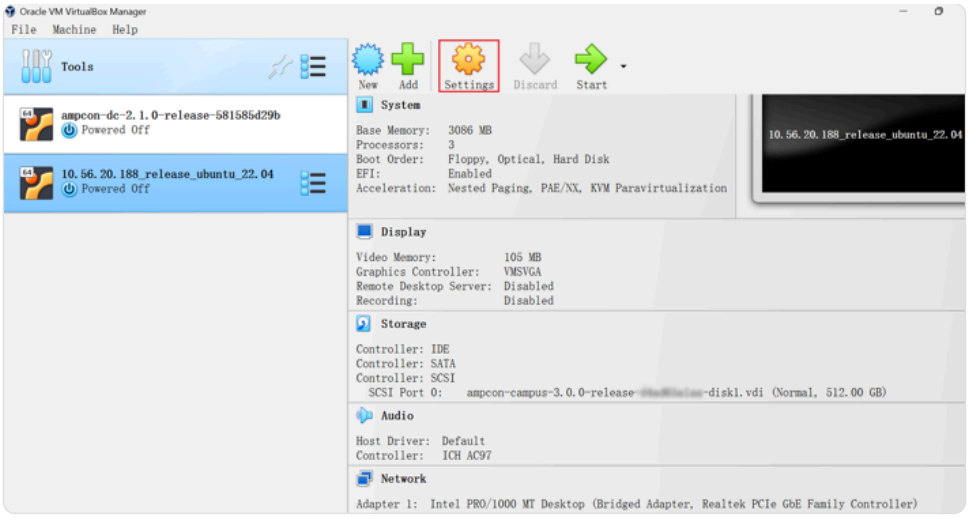
3. Confirm the settings for the .ova file, and then click **Finish**.



Wait for the import process to finish. Once completed, the virtual machine is successfully imported.



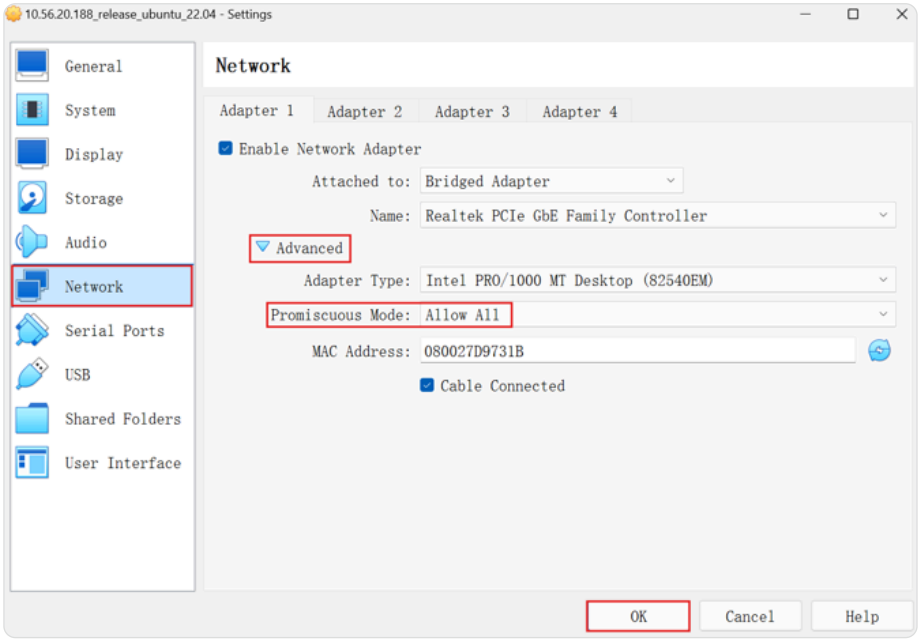
4. Click **Settings**, and then change the promiscuous mode of the imported virtual machine as follows:



a. Click **Network**, and then click **Advanced** in the **Adapter 1** tab.

b. Change the promiscuous mode to **Allow All**.

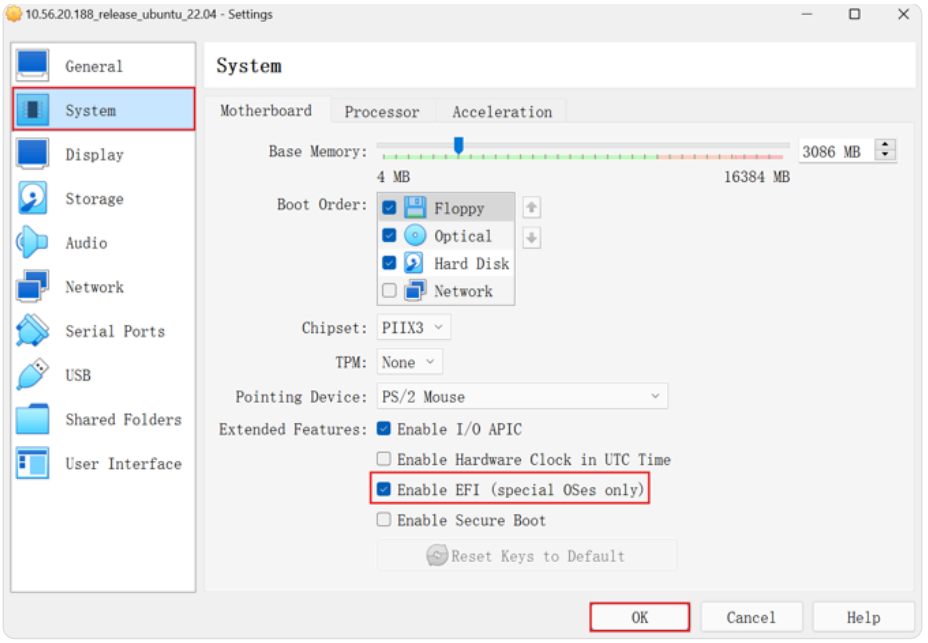
c. Click **OK**.



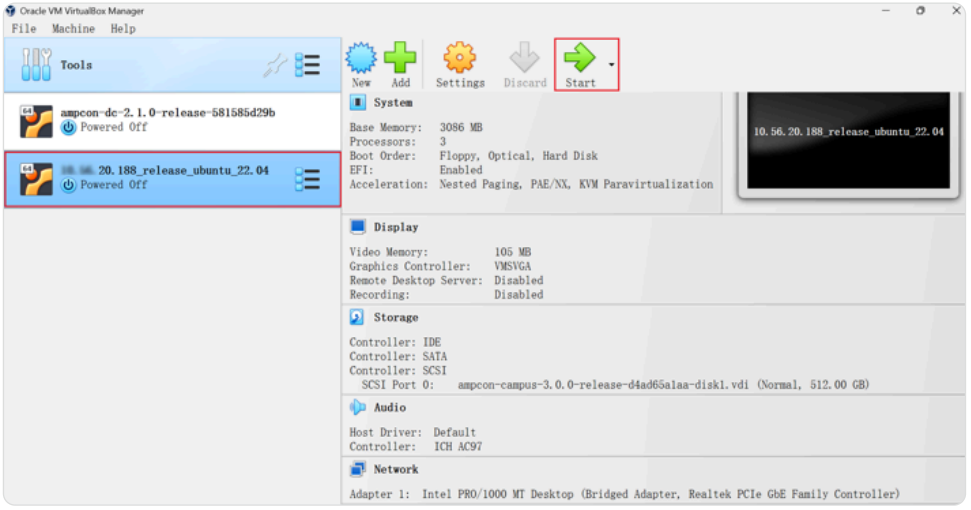
5. Enable the **EFI** mode of the virtual machine as follows:

a. Click **System**, and then select **Enable EFI (special OSes only)** in the **Extended Features** section.

b. Click **OK**.



6. Start the imported virtual machine by clicking the virtual machine and then clicking **Start**.



7. Modify the network interface configuration.

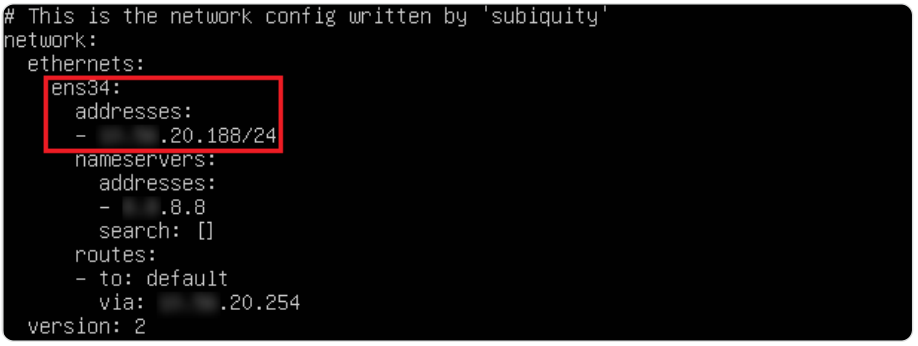
   a. Log in to the virtual machine with the default username (**pica8**) and password (**pica8**).

   b. Open the file named 00-installer-config.yaml by running the following command:

```
sudo vi /etc/netplan/00-installer-config.yaml
```

   c. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the virtual machine as follows:

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the virtual machine.
>
> Therefore, you must check the actual NIC name of the virtual machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.



d. Apply the network interface configuration by running the following command:

```
sudo netplan apply
```

8. Activate AmpCon-Campus:

a. Go to the AmpCon-Campus installation directory by running the following command:

```
cd /opt/ampcon
```

b. Activate AmpCon-Campus by running the following command:

```
sudo ./activate.sh
```

NOTE

You can append the following parameters to the command if needed:

- **--global-ip <*ip*>**: Specifies the NIC IP address used by managed devices to access AmpCon-Campus.
  The imported AmpCon-Campus image file contains only one Network Interface Card (NIC). But you can manually add more NICs.

  You **must** specify this parameter if the virtual machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 will be used as the OpenVPN subnet.

See the following configuration example:

sudo ./activate.sh --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24

The global IP address must not fall within the VPN subnet.

Once activated, AmpCon-Campus is installed.

NOTEs

- Activation is a one-time step that must be performed only on the first boot after importing the virtual machine.
  Once activated, AmpCon-Campus is installed, and the AmpCon-Campus service is automatically started.
- AmpCon-Campus is installed in the /opt/ampcon directory.
  Currently, you can't customize the installation directory.

What to Do Next

- If multiple NICs are added to the virtual machine where AmpCon-Campus is installed and the global IP is not specified during activation, you must contact support engineers to specify the NIC IP address.
  Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.

- To stop AmpCon-Campus, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.

  b. Stop AmpCon-Campus by running the **sudo ./stop.sh** command.

- To start AmpCon-Campus after it is stopped, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.

  b. Start AmpCon-Campus by running the **sudo ./start.sh** command.

> **NOTE**
>
> Starting is a routine operation that you can perform after stopping AmpCon-Campus.

Installing on VMware ESXi

You can install AmpCon-Campus on VMware ESXi 6.7, 7.0, 8.0. To use VMware ESXi in general, see the VMware ESXi documentation.

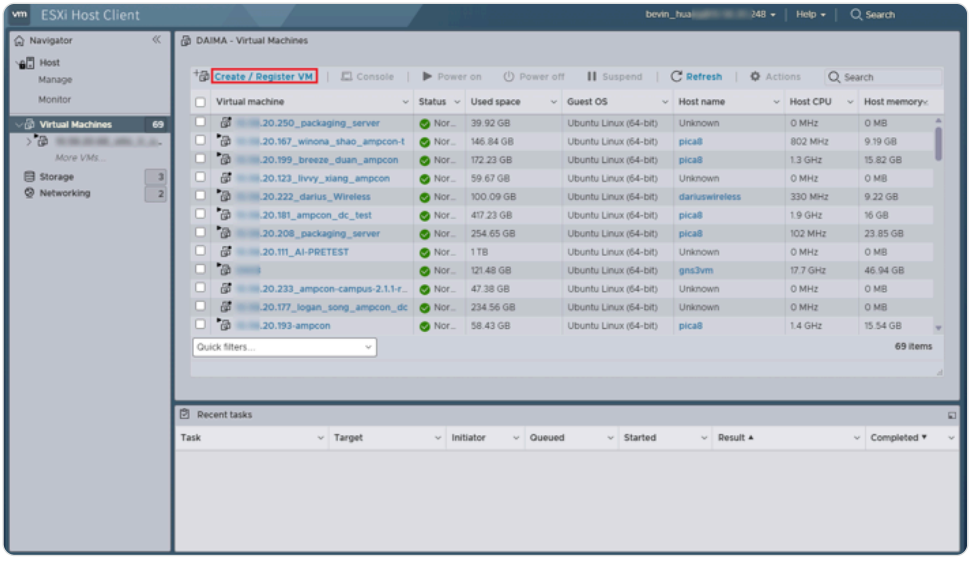
Prerequisites
Installation Procedure
What to Do Next

Prerequisites

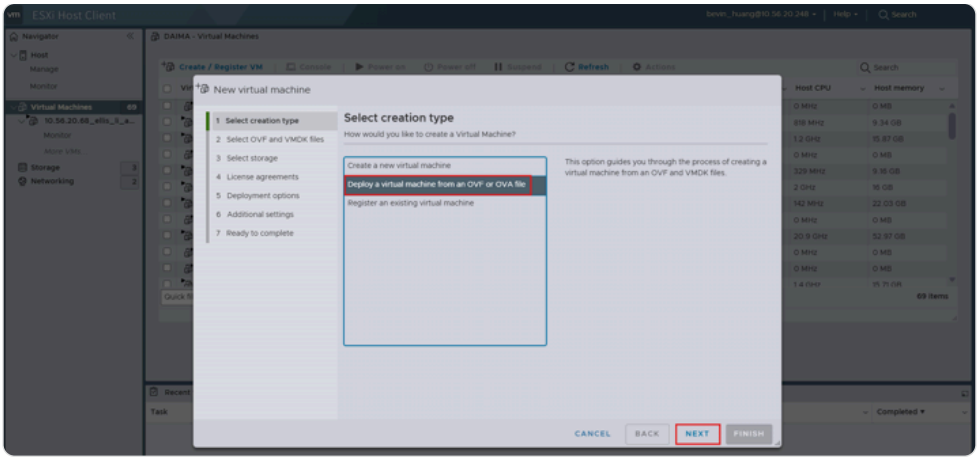
- Ensure that the installation requirements are met.
- Open the AmpCon-Campus download page, and select **United States** as the region. Then, download the zipped AmpCon-Campus image (**AmpCon-Campus for VMware ESXi V3.0.0 Software**).
- Copy the zipped AmpCon-Campus image file to the host machine where the hypervisor exists, and then unzip it.

Installation Procedure

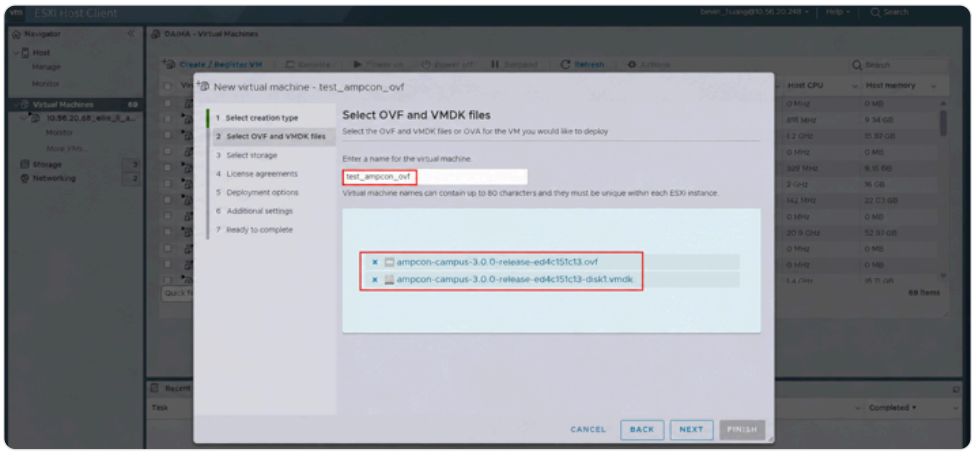
1. Open the VMware ESXi console, and then click **Create / Register VM**.



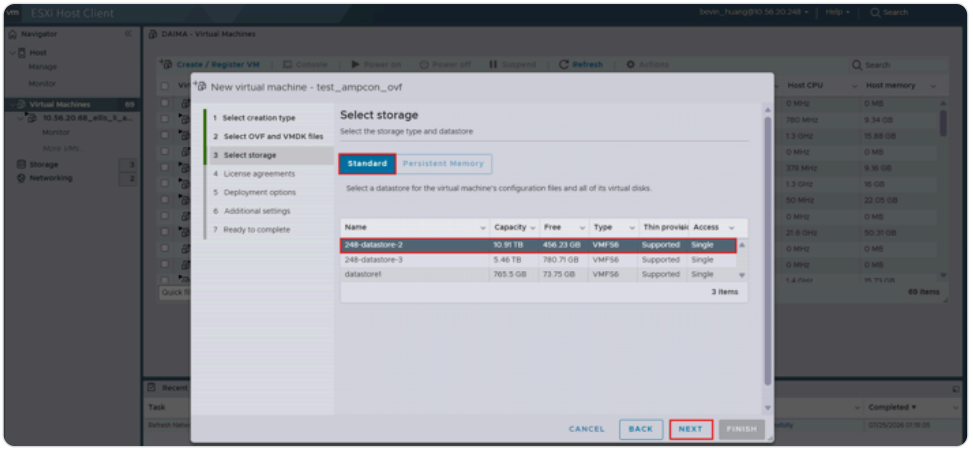
2. Select **Deploy a virtual machine from an OVF or OVA file**, and then click **Next**.



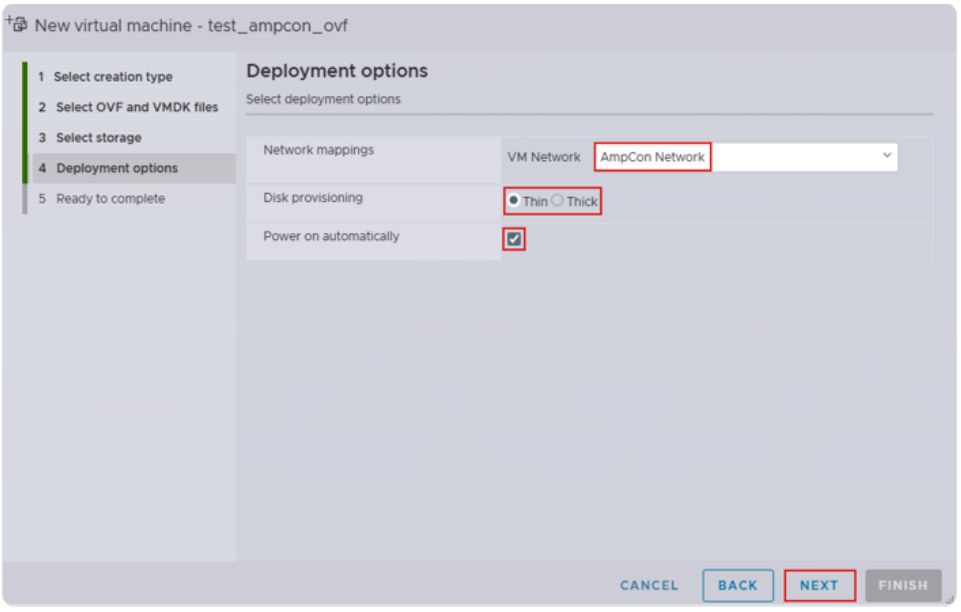
3. Enter the virtual machine name, upload the AmpCon-Campus .ovf and .vmdk files, and then click **Next**.



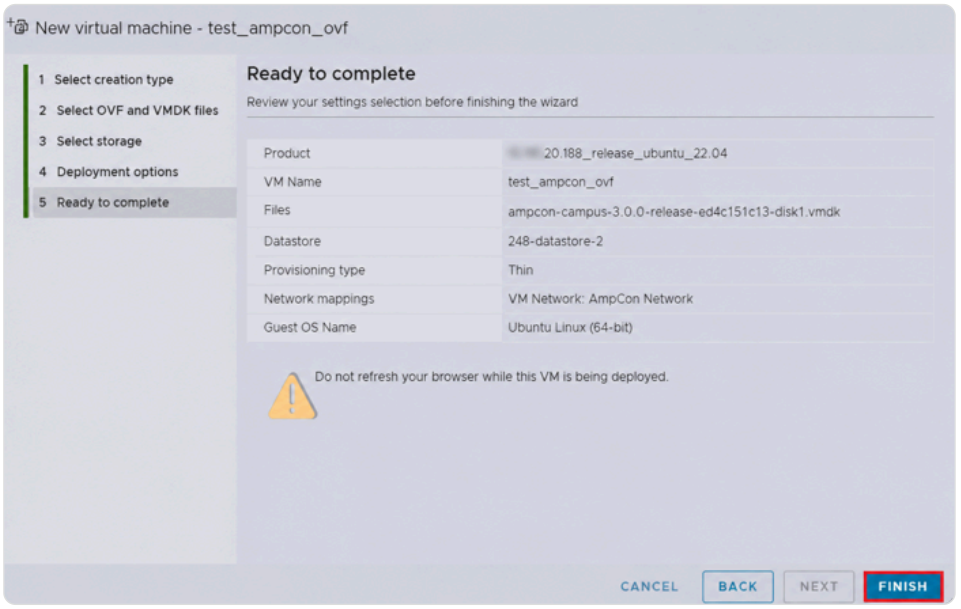
4. Select the storage type and datastore, and then click **Next**.



5. Configure the deployment options as follows:
   a. In the **Network mappings** drop-down list of the **Deployment Options** window, select the network adapter to which the virtual machine is connected.
   b. Select the disk provisioning type, and choose whether to enable **Power on automatically**.
   c. Click **Next**.

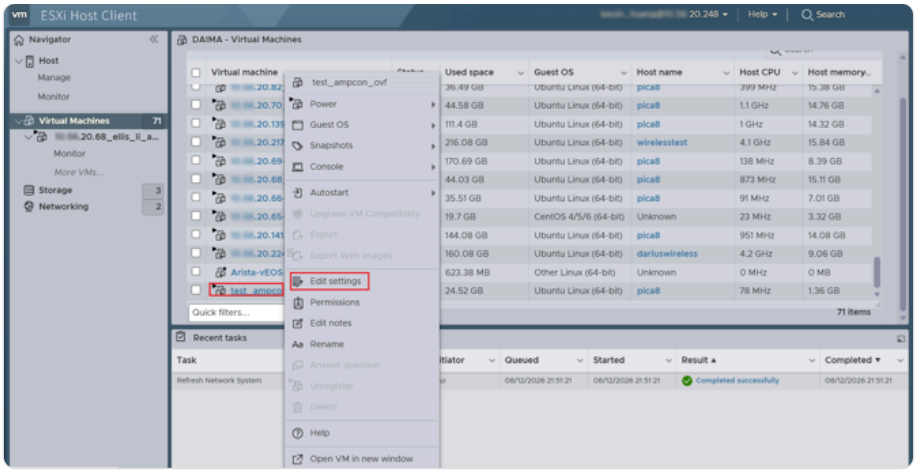


6. Click **Finish**.

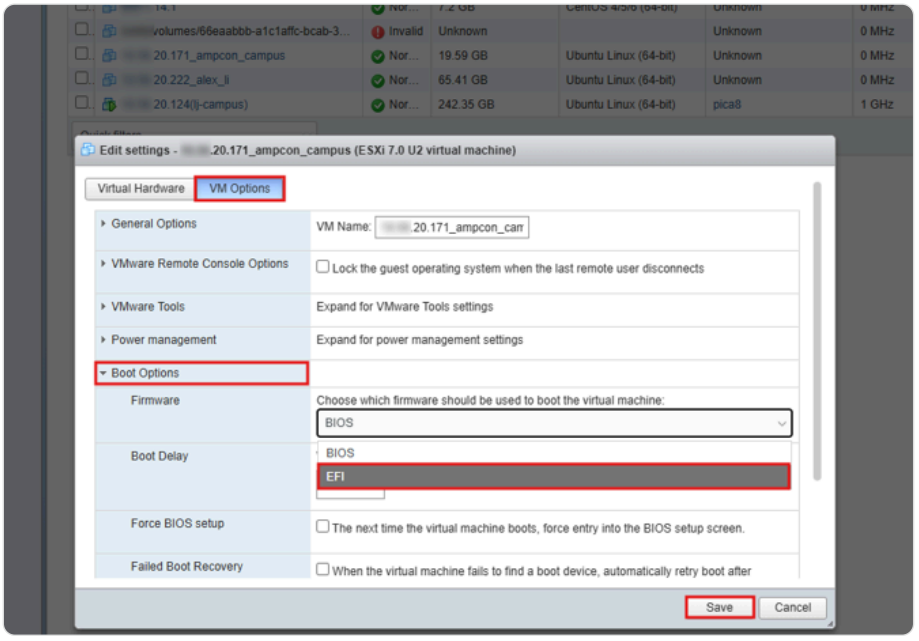


Wait for the import process to finish. Once completed, the virtual machine is successfully imported.

7. Enable the **EFI** mode of the virtual machine as follows:
   a. Right-click the new virtual machine name that you specified in **Step 3**, and then click **Edit settings**.

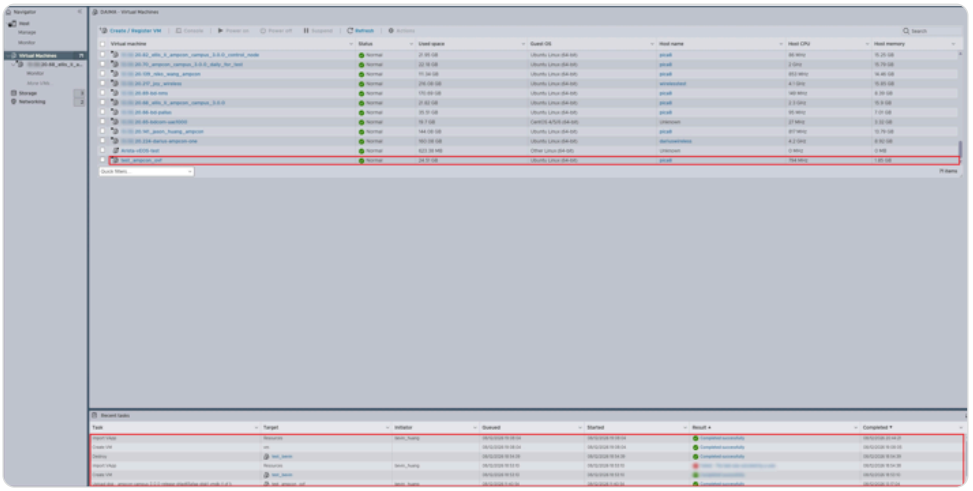


b. Click **VM Options** > **Boot Options**, and then select **EFI** in the drop-down list.

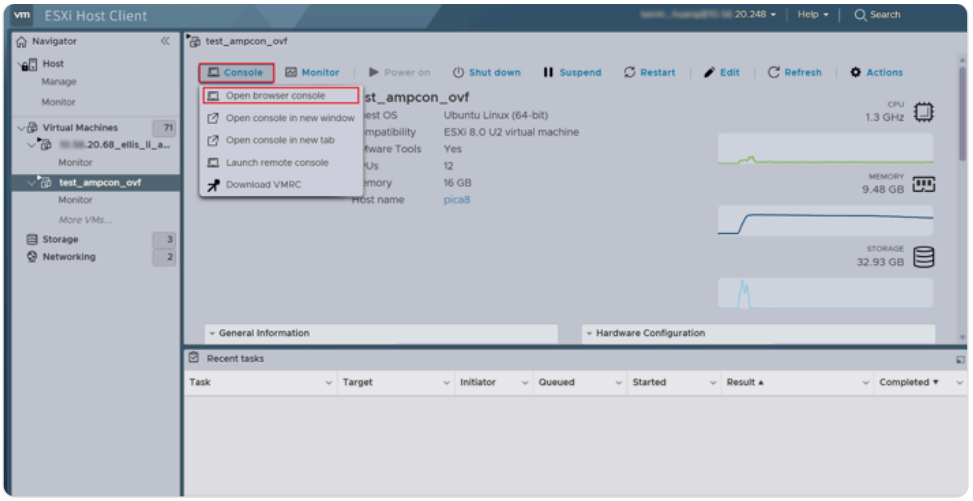


c. Click **Save**.

8. On the VMware ESXi console, click the new virtual machine name that you specified in **Step 3**.



9. Click **Console > Open browser console** to open the virtual machine console.



10. Modify the network interface configuration.

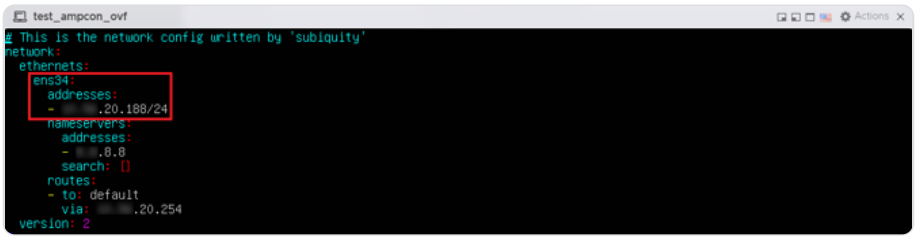
    a. Log in to the virtual machine with the default username (**pica8**) and password (**pica8**).

    b. Open the file named 00-installer-config.yaml by running the following command:

```
sudo vi /etc/netplan/00-installer-config.yaml
```

    c. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the virtual machine as follows:

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the virtual machine.
>
> Therefore, you must check the actual NIC name of the virtual machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.



    d. Apply the network interface configuration by running the following command:

```
sudo netplan apply
```

11. Activate AmpCon-Campus:

a. Go to the AmpCon-Campus installation directory by running the following command:

```
cd /opt/ampcon
```

b. Activate AmpCon-Campus by running the following command:

```
sudo ./activate.sh
```

NOTEs

You can append the following parameters to the command if needed:

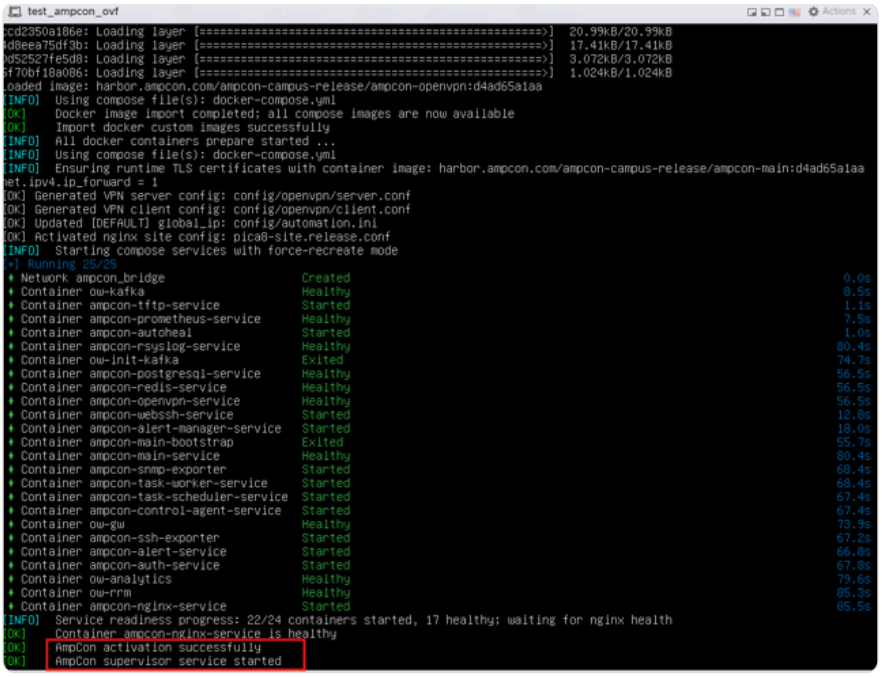
- **--global-ip <*ip*>**: Specifies the NIC IP address used by managed devices to access AmpCon-Campus.
  The imported AmpCon-Campus image file contains only one Network Interface Card (NIC). But you can manually add more NICs.

  You **must** specify this parameter if the virtual machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 will be used as the OpenVPN subnet.

See the following configuration example:

sudo ./activate.sh --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24

The global IP address must not fall within the VPN subnet.



Once activated, AmpCon-Campus is installed.

> **NOTEs**
>
> - Activation is a one-time step that must be performed only on the first boot after importing the virtual machine.
>
> Once activated, AmpCon-Campus is installed, and the AmpCon-Campus service is automatically started.
> - AmpCon-Campus is installed in the /opt/ampcon directory.
>
> Currently, you can't customize the installation directory.

What to Do Next

- If multiple NICs are added to the virtual machine where AmpCon-Campus is installed and the global IP is not specified during activation, you must contact support engineers to specify the NIC IP address.

  Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- To stop AmpCon-Campus, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.

  b. Stop AmpCon-Campus by running the **sudo ./stop.sh** command.
- To start AmpCon-Campus after it is stopped, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.

b. Start AmpCon-Campus by running the **sudo ./start.sh** command.

> **NOTE**
>
> Starting is a routine operation that you can perform after stopping AmpCon-Campus.

Installing on QEMU or KVM

You can install AmpCon-Campus on QEMU or KVM. To use QEMU or KVM in general, see KVM documentation and QEMU documentation.

In this topic, KVM virt-manager is used to demonstrate the AmpCon-Campus installation steps.

Prerequisites
Installation Procedure
What to Do Next

Prerequisites

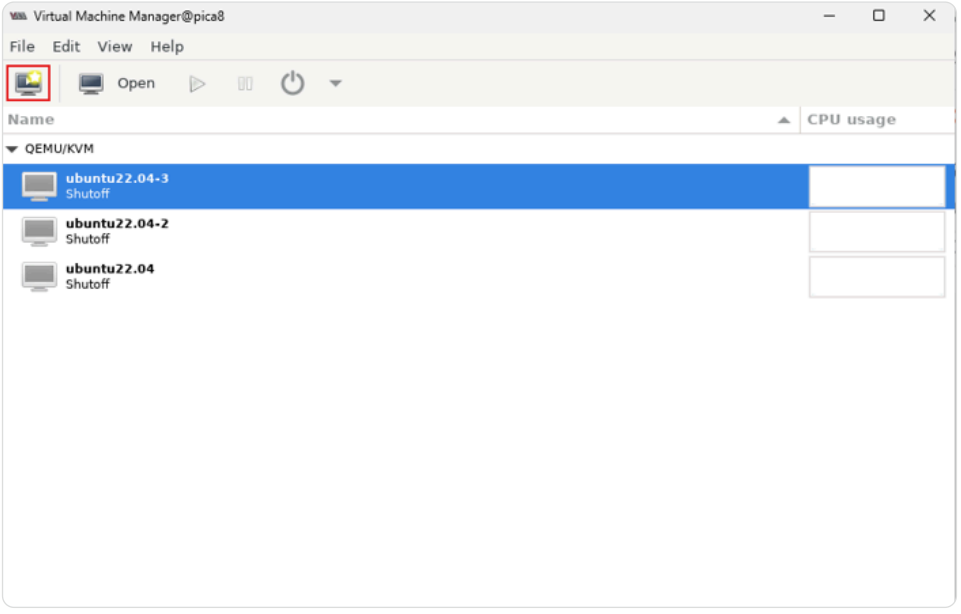
- Ensure that the installation requirements are met.
- Open the AmpCon-Campus download page, and select **United States** as the region. Then, download the zipped AmpCon-Campus image (**AmpCon-Campus for QEMU/KVM V3.0.0 Software**).
- Copy the zipped AmpCon-Campus image file to the host machine where the hypervisor exists, and then unzip it.

Installation Procedure

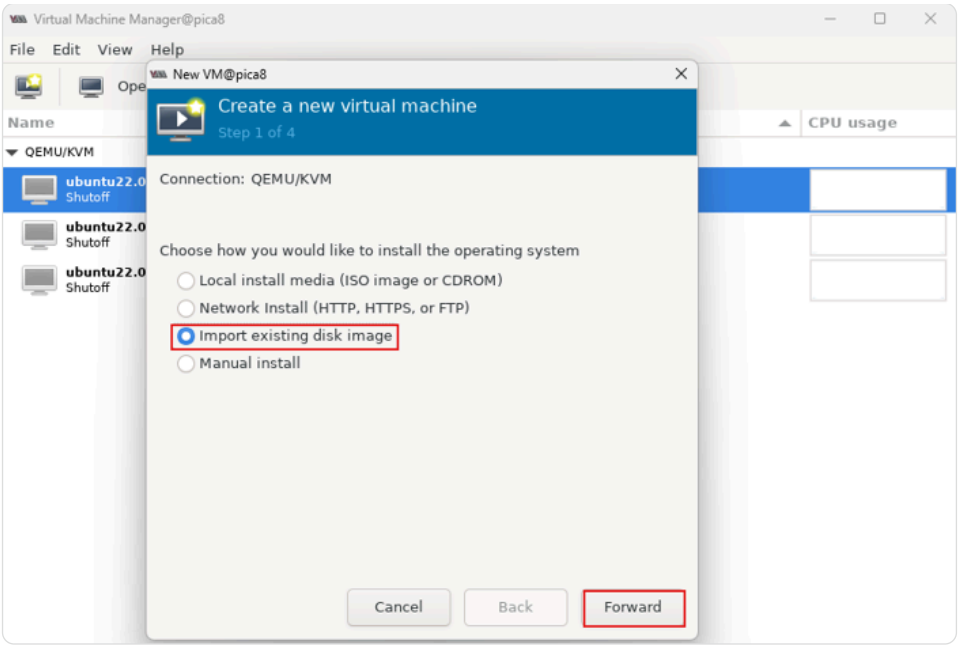
1. Open the virt-manager console by running the following command:

```
virt-manager
```

2. Click the following button to start the import process.

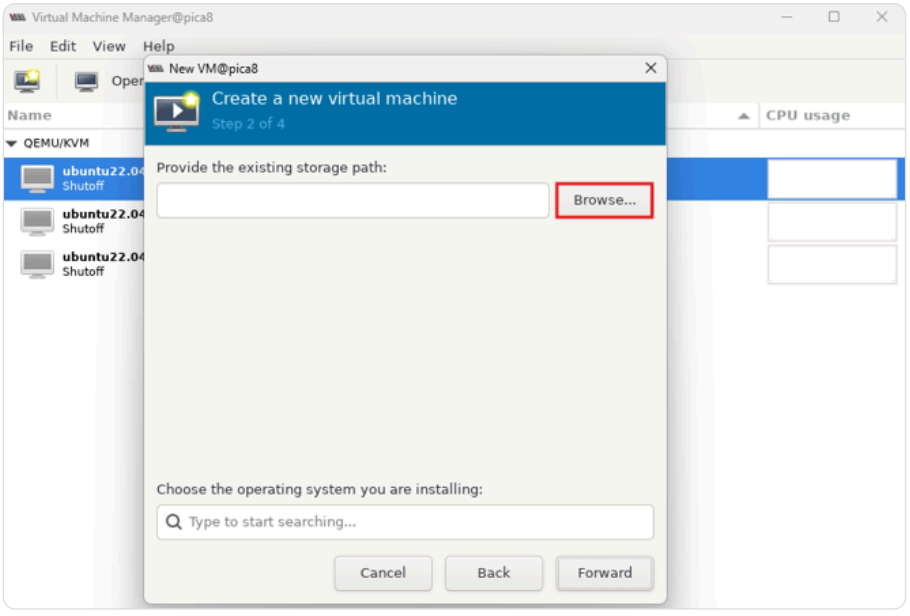


3. In the pop-up window, select **Import existing disk image**, and then click **Forward**.

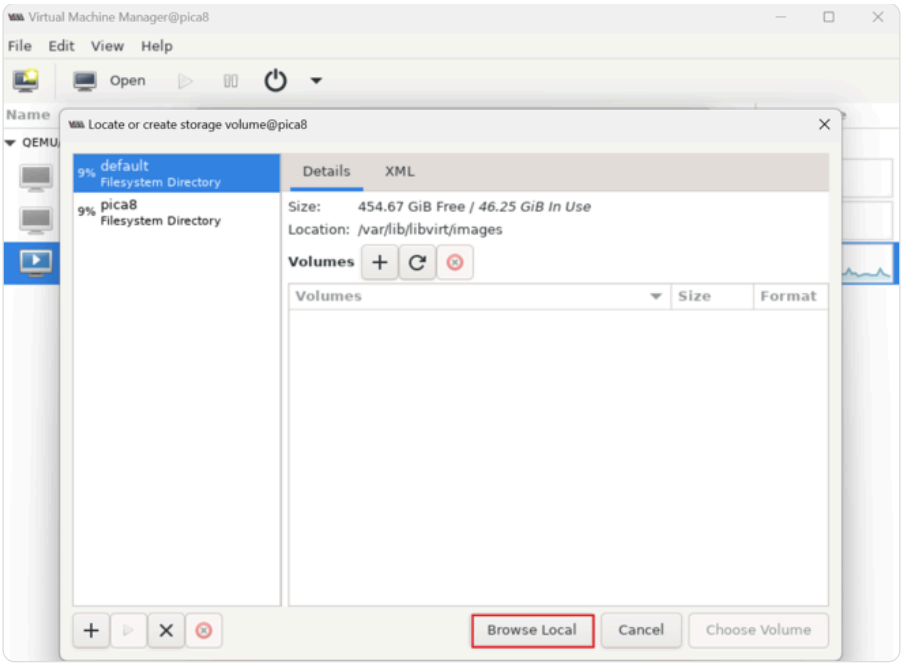


4. Select the AmpCon-Campus .qcow2 image file as follows:

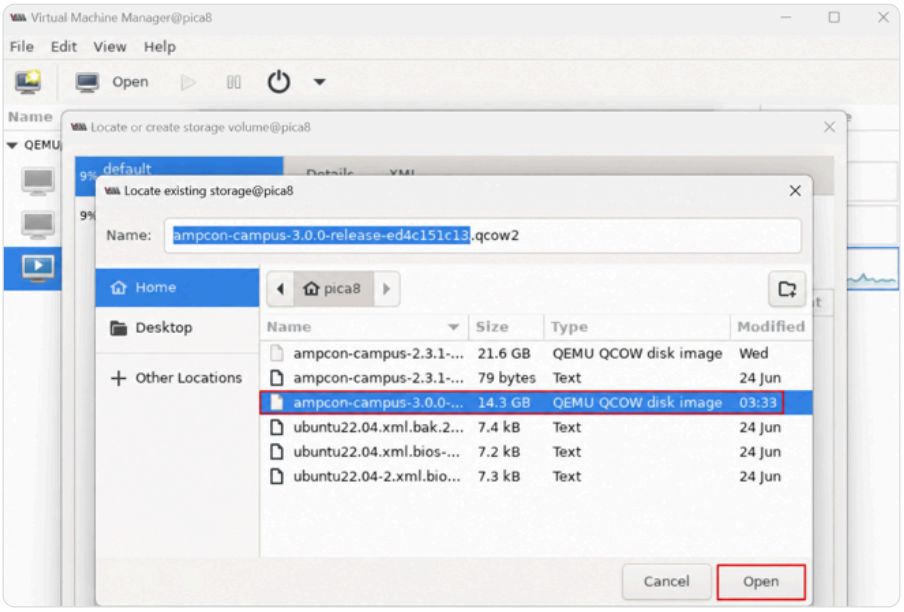
   a. Click **Browse**.



   b. Click **Browse Local** to add a local location.

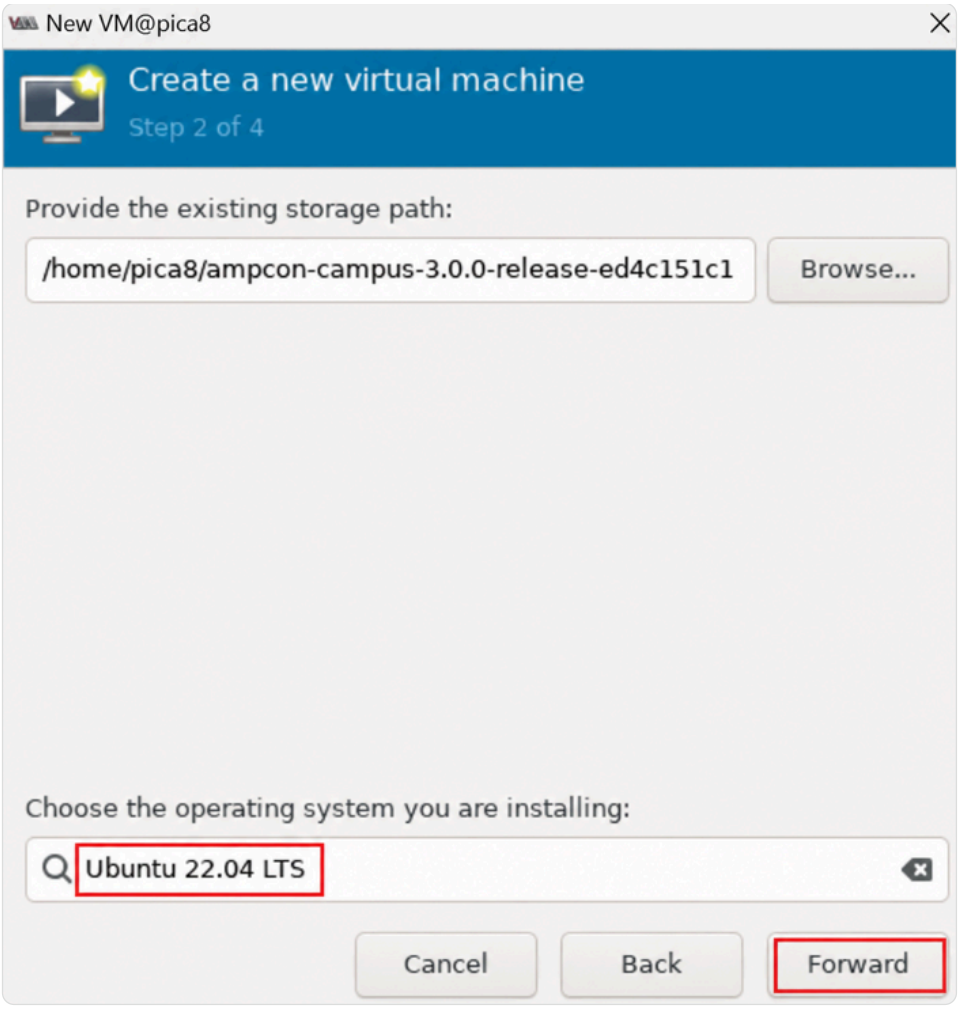


c. Click the location of the AmpCon-Campus .qcow2 image file, and then click **Open**.



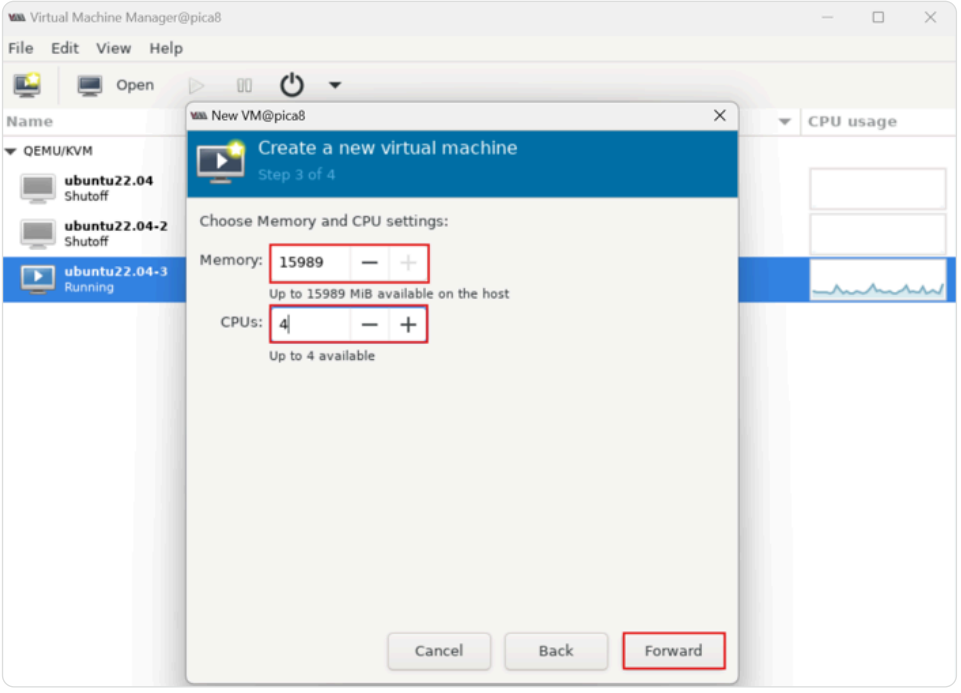
5. Select **Ubuntu 22.04 LTS**, and then click **Forward**.

> **NOTE**
>
> Do not select other operating systems. Currently, AmpCon-Campus supports only Ubuntu 22.04.

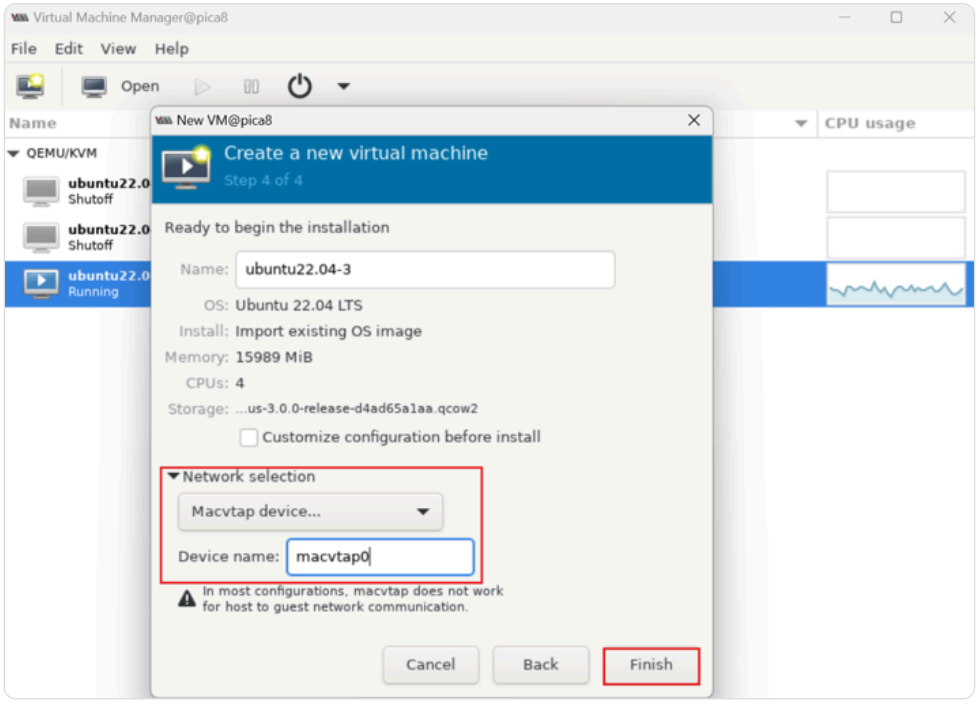


6. Adjust the memory and CPU settings as needed, and then click **Forward**.

> **NOTE**
>
> Ensure that the memory and CPU settings meet the Installation Requirements.

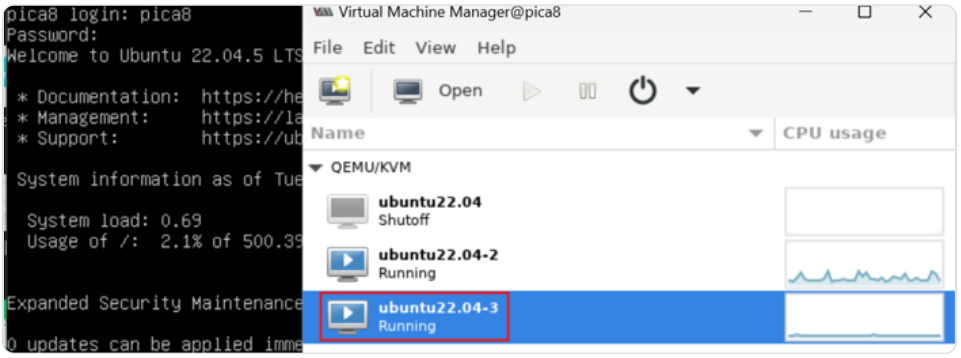


7. In the **Network selection** section, select **Macvtap device**, and enter the device name. Then, click **Finish**.



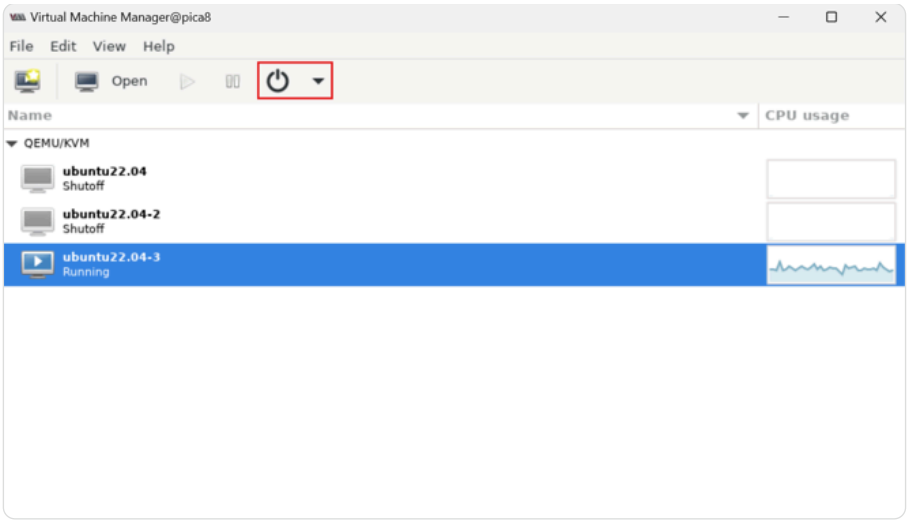
> **Tip**
>
> In the **Ready to begin the installation** section, the **Name** field is pre-filled with a generated virtual machine name. You can edit it as needed.

Wait for the import process to finish. Once completed, the virtual machine is successfully imported.

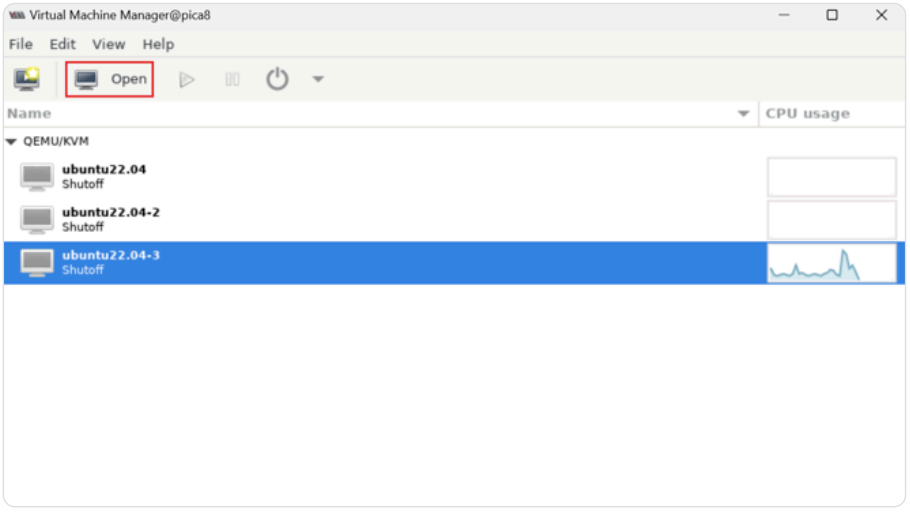


8. Enable the boot menu as follows:

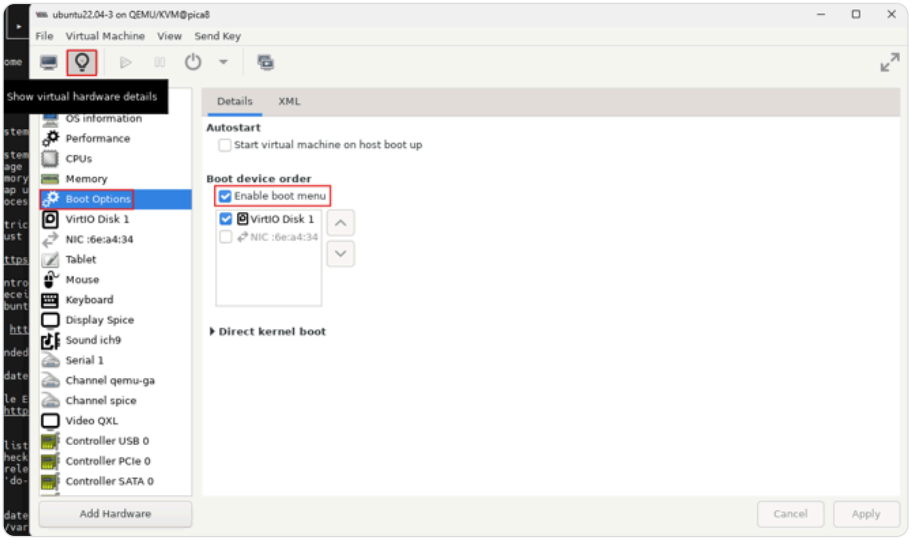
   a. Shut down the virtual machine by clicking the following icon.



b. Click the **Open** icon.



c. Click the detail icon, and then click **Boot Options**. In the **Details** tab, select **Enable boot menu**.



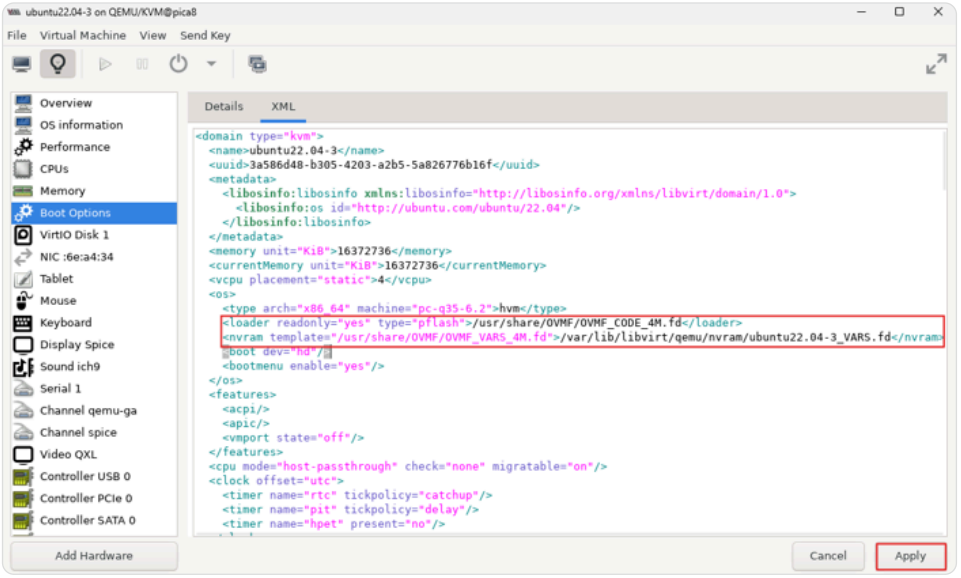
9. Configure the virtual machine firmware mode to EFI.

   In the XML tab, add the following block:

```
<loader readonly="yes"
type="pflash">/usr/share/OVMF/OVMF_CODE_4M.fd</loader>

<nvram
template="/usr/share/OVMF/OVMF_VARS_4M.fd">/var/lib/libvirt/qe
mu/nvram/<virtual_machine_name>_VARS.fd</nvram>
```

Replace <*virtual_machine_name*> with the imported virtual machine name (specified in the **Name** field of **Step 7**). Then, click **Apply**.



10. Modify the network interface configuration.

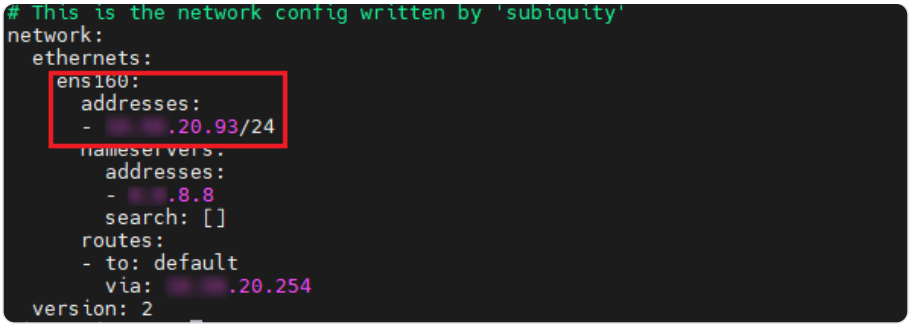
    a. Log in to the virtual machine with the default username (**pica8**) and password (**pica8**).

    b. Open the file named 00-installer-config.yaml by running the following command:

```
sudo vi /etc/netplan/00-installer-config.yaml
```

    c. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the virtual machine as follows:

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the virtual machine.
>
> Therefore, you must check the actual NIC name of the virtual machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.



d. Apply the network interface configuration by running the following command:

```
sudo netplan apply
```

11. Activate AmpCon-Campus:

a. Go to the AmpCon-Campus installation directory by running the following command:

```
cd /opt/ampcon
```

b. Activate AmpCon-Campus by running the following command:

```
sudo ./activate.sh
```

NOTE

You can append the following parameters to the command if needed:

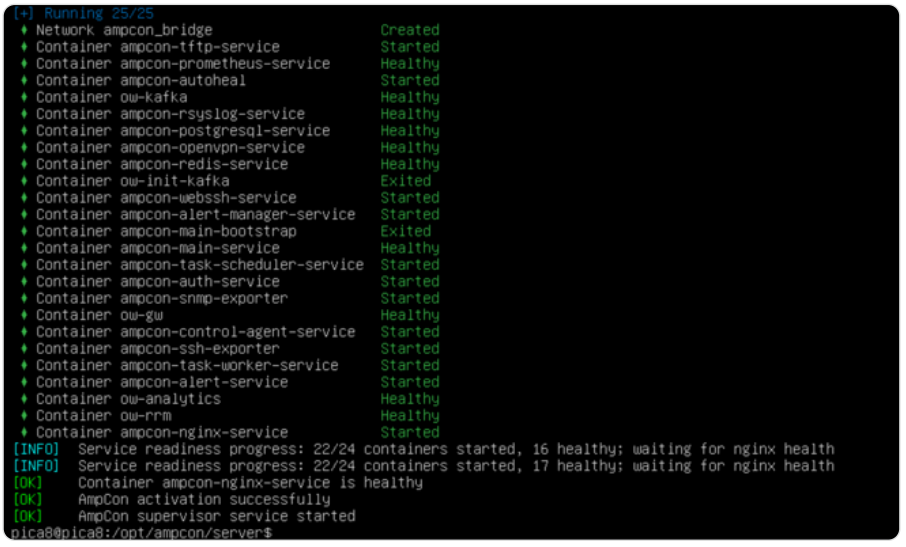
- **--global-ip <*ip*>**: Specifies the NIC IP address used by managed devices to access AmpCon-Campus.
  The imported AmpCon-Campus image file contains only one Network Interface Card (NIC). But you can manually add more NICs.

  You **must** specify this parameter if the virtual machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 will be used as the OpenVPN subnet.

See the following configuration example:

sudo ./activate.sh --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24

The global IP address must not fall within the VPN subnet.



Once activated, AmpCon-Campus is installed.

NOTEs

- Activation is a one-time step that must be performed only on the first boot after import the virtual machine.
  Once activated, AmpCon-Campus is installed, and the AmpCon-Campus service is automatically started.
- AmpCon-Campus is installed in the /opt/ampcon directory. Currently, you can't customize the installation directory.

What to Do Next

- If multiple NICs are added to the virtual machine where AmpCon-Campus is installed and the global IP is not specified during activation, you must contact support engineers to specify the NIC IP address.
  Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- To stop AmpCon-Campus, follow these steps:
  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.
  b. Stop AmpCon-Campus by running the **sudo ./stop.sh** command.
- To start AmpCon-Campus after it is stopped, follow these steps:
  a. Go to the AmpCon-Campus installation directory by running the **cd /opt/ampcon** command.
  b. Start AmpCon-Campus by running the **sudo ./start.sh** command.

NOTE

Starting is a routine operation that you can perform after stopping AmpCon-Campus.

Installing on Physical Machines (Ubuntu Docker)

You can install AmpCon-Campus on a physical machine based on Ubuntu 22.04 with Docker installed.

Prerequisites
Installation Procedure
What to Do Next

Prerequisites

- Ensure that the installation requirements are met.
- Prepare a physical machine based on Ubuntu 22.04 with Docker installed.
- Ensure that the physical machine where you want to install AmpCon-Campus meets the following conditions:
  - The physical machine has Python 3 installed.
  - The physical machine has no versions of AmpCon-Campus installed.
- Open the AmpCon-Campus download page and select **United States** as the region. Then, download the zipped AmpCon-Campus installation package (**AmpCon-Campus for Ubuntu Docker V3.0.0 Software**), and unzip it.

Installation Procedure

1. Copy the AmpCon-Campus installation package to the prepared physical machine, and then extract the package by running the following command:

   ```
   tar -xvf <package_name>.tar
   ```

   Replace *<package_name>* in the command with the name of the AmpCon-Campus installation package.

   > **NOTE**
   >
   > A directory will be generated containing the extracted AmpCon-Campus installation files.

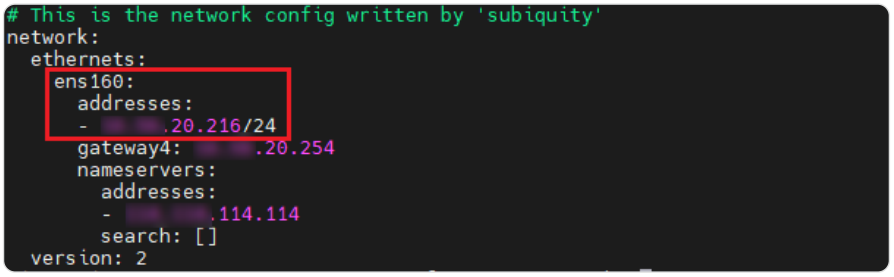
2. On the machine where you want to install AmpCon-Campus, modify the network interface configuration.

   a. Open the file named 00-installer-config.yaml by running the following command:

   ```
   sudo vi /etc/netplan/00-installer-config.yaml
   ```

   b. In the 00-installer-config.yaml file, modify the IP address with the actual IP address of the physical machine.

> **NOTE**
>
> The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the actual NIC name of the physical machine.
>
> Therefore, you must check the actual NIC name of the physical machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file.



c. Apply the network interface configuration by running the following command:

```
sudo netplan apply
```

3. Go to the directory where the extracted AmpCon-Campus installation files exist.

```
cd <AmpCon-Campus package directory>
```

Replace *<AmpCon-Campus package directory>* with the name of the directory containing the extracted AmpCon-Campus installation files.

4. Install AmpCon-Campus by running the following command:

```
sudo ./install.sh
```

NOTE

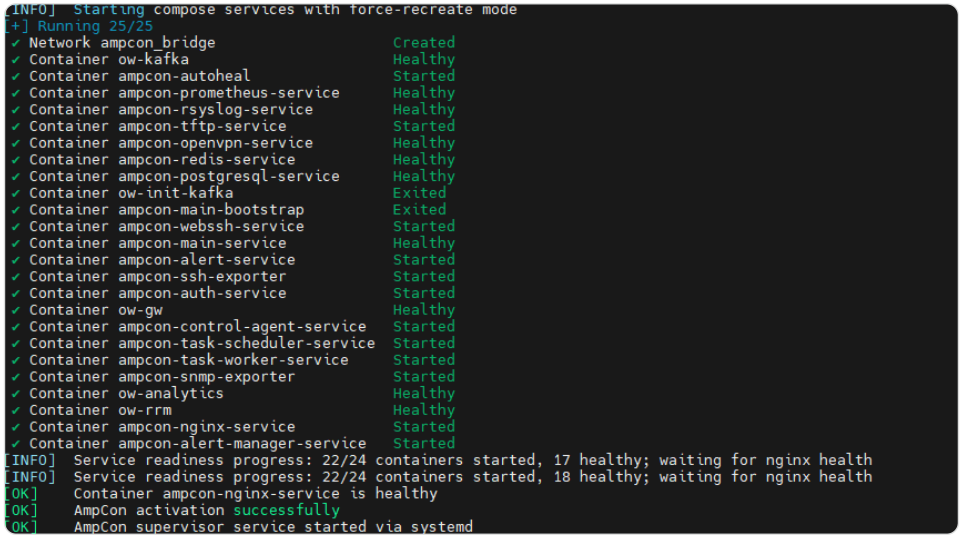
You can append the following parameters to the command if needed:

- **--home <*path*>**: Specifies the AmpCon-Campus installation directory. If it's not specified, AmpCon-Campus is installed in the /opt/ampcon directory.
- **--global-ip <*ip*>**: Specifies the NIC IP used by managed devices to access AmpCon-Campus.
  The AmpCon-Campus installation package file is not an image file, and thus no NIC is contained in the file. But you can manually add one or multiple NICs to the physical machine.
  You **must** specify this parameter if the physical machine has multiple NICs. Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- **--vpn-subnet <*network-cidr*>**: Specifies the OpenVPN subnet in CIDR format. If it's not specified, 10.8.0.0/20 will be used as the OpenVPN subnet.

See the following configuration example:

sudo ./install.sh --home /opt/ampcon --global-ip 192.168.2.11 --vpn-subnet 192.168.1.0/24

The global IP address must not fall within the VPN subnet.



Wait for the installation process to finish. Once completed, AmpCon-Campus is installed and started.

What to Do Next

- If multiple NICs are added to the physical machine where AmpCon-Campus is installed and the global IP is not specified during installation, you must contact support engineers to specify the NIC IP address.
  Otherwise, the connections between AmpCon-Campus and the switches and APs to be managed might fail.
- To stop AmpCon-Campus, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd** <*AmpCon-Campus installation directory*> command.

  > **NOTE**
  >
  > Replace <*AmpCon-Campus installation directory*> with the actual installation directory of AmpCon-Campus. If you don't set a custom directory, replace with the default directory /opt/ampcon.

  b. Stop AmpCon-Campus by running the **sudo ./stop.sh** command.
- To start AmpCon-Campus after it is stopped, follow these steps:

  a. Go to the AmpCon-Campus installation directory by running the **cd** <*AmpCon-Campus installation directory*> command.

  > **NOTE**
  >
  > Replace <*AmpCon-Campus installation directory*> with the actual installation directory of AmpCon-Campus. If you don't set a custom directory, replace with the default directory /opt/ampcon.

  b. Start AmpCon-Campus by running the **sudo ./start.sh** command.

Uninstalling on Physical Machines (Ubuntu Docker)

You can uninstall AmpCon-Campus only when it's installed on a physical machine.

> **NOTE**
>
> For AmpCon-Campus installed on a virtual machine, you can remove the AmpCon-Campus virtual machine instance by shutting it down and deleting it from the hypervisor.

Guidelines

- The uninstallation is irreversible. Once completed, all local AmpCon-Campus data will be permanently deleted and cannot be recovered.
- After AmpCon-Campus is uninstalled, the entire Ubuntu 22.04 operating system environment (including Docker and all other files unrelated to AmpCon-Campus) is retained.
- If uninstallation fails, **do not** manually remove any AmpCon-Campus resources. Instead, keep the log output and contact support engineers for assistance.

Prerequisites

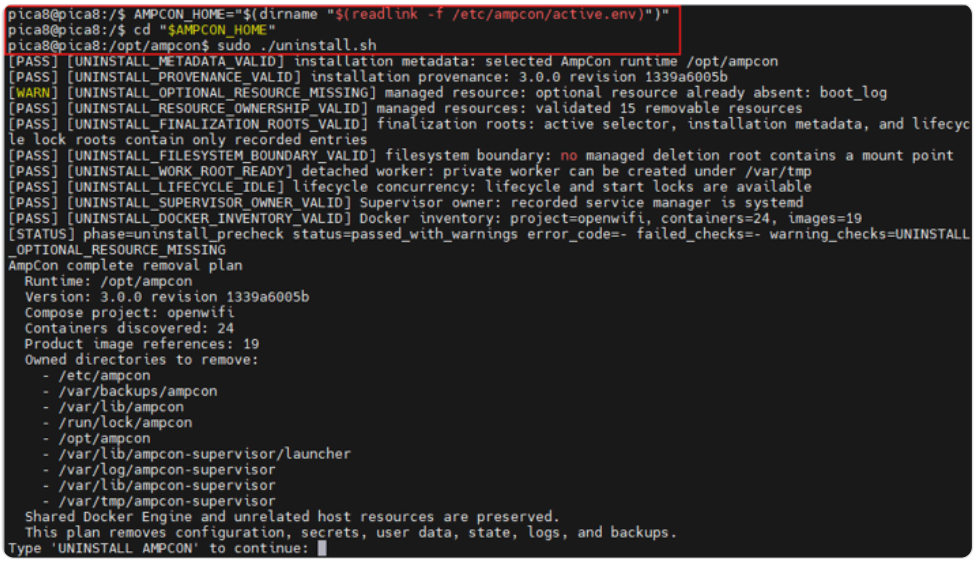
- Ensure that AmpCon-Campus is not being installed, started, or stopped.
- Ensure that the physical machine where AmpCon-Campus is installed has Python 3 installed.

Procedure

To uninstall AmpCon-Campus, follow these steps:

1. Obtain the AmpCon-Campus installation directory and assign it to the **AMPCON_HOME** environment variable by running the following command:

```
AMPCON_HOME="$(dirname "$(readlink -f /etc/ampcon/active.env)")"
```



2. Go to the AmpCon-Campus installation directory by running the following command:

```
cd "$AMPCON_HOME"
```

3. Run the uninstall script with sudo privileges:

```
sudo ./uninstall.sh
```

4. Confirm the uninstallation by entering the following confirmation phrase:
   The phrase is case-sensitive, and spacing must be preserved.

```
UNINSTALL AMPCON
```

Working with the User Interface

After you install AmpCon-Campus, you can log in to the AmpCon-Campus user interface (UI).

Prerequisites
Logging In
Logging Out
UI Overview
UI Menus
UI Conventions

Prerequisites

Before logging in to the AmpCon-Campus UI, ensure that the following prerequisites are met:

- The network connection between your local computer and AmpCon-Campus is available, and AmpCon-Campus is started and running properly.
- You have obtained the AmpCon-Campus username and password for login.
  - The first time you log in to the AmpCon-Campus UI, use the default username **admin** and password **admin**.
  - The user **admin** is a built-in account of the **Owner** role. It has all operation permissions on AmpCon-Campus. For security purposes, change your password on first login, update it regularly, and store it securely. To update the password, see User Self-Management.
  - You can add other user accounts and enable limited access for the personnel who are working with you. For more information, see Managing User Access.

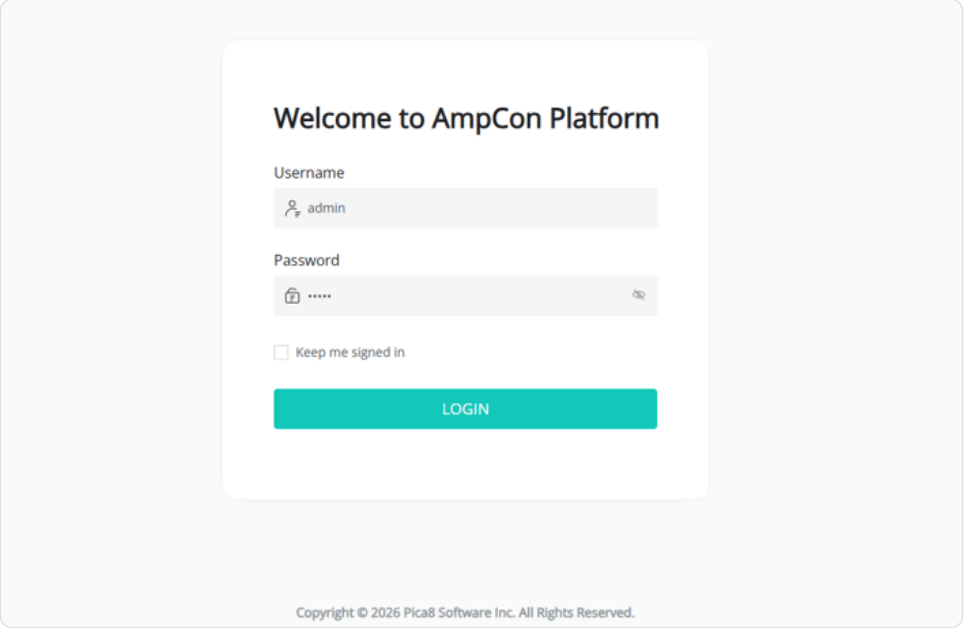
Logging In

To log in to the AmpCon-Campus UI, follow these steps:

1. In a supported web browser (Google Chrome 150.0.7871.187 or later, Microsoft Edge 151.0.4129.59 or later, Firefox 153.0.1 or later), enter the AmpCon-Campus URL in the format of "https://*<AmpCon-IP-or-Domain-Name>*/login".

   Replace *<AmpCon-IP-or-Domain-Name>* with the IP address or domain name of AmpCon-Campus.

2. In the **Username** field, enter the username of an AmpCon-Campus user.
3. In the **Password** field, enter the password of the AmpCon-Campus user.



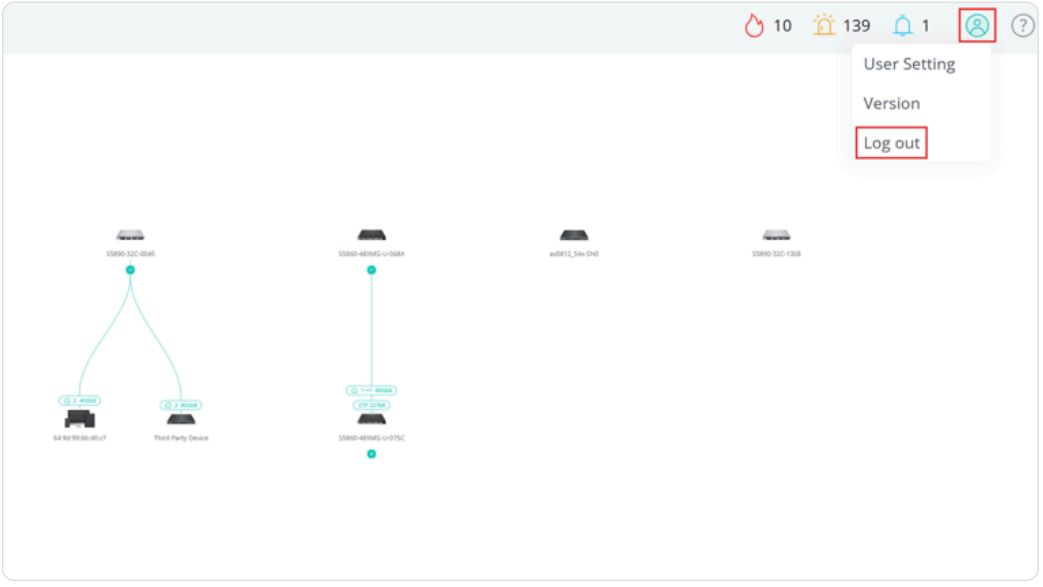
4. Optional: Select **Keep me signed in** to extend the allowed inactivity time of the AmpCon-Campus UI.

- If **Keep me signed in** is not selected, your session will be logged out after 30 minutes of inactivity in the AmpCon-Campus UI.
- If **Keep me signed in** is selected, your session will be logged out after 7 days of inactivity in the AmpCon-Campus UI.

5. Click **LOGIN**. Then, the AmpCon-Campus homepage will appear.

Logging Out

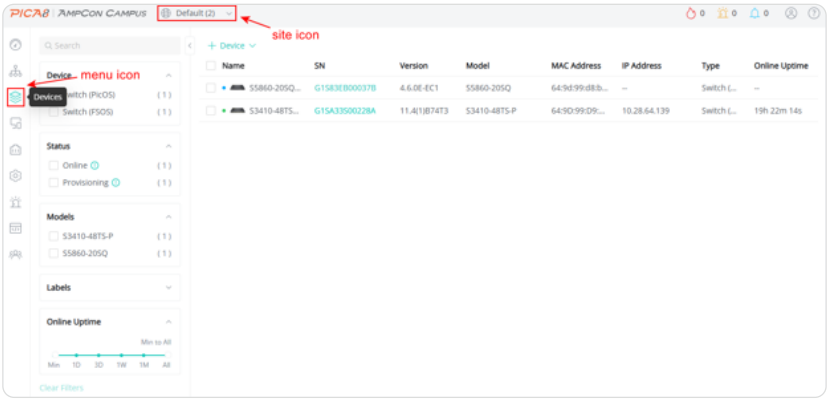
To log out of the AmpCon-Campus UI, hover over the user avatar in the top-right corner, and then click **Log Out**.

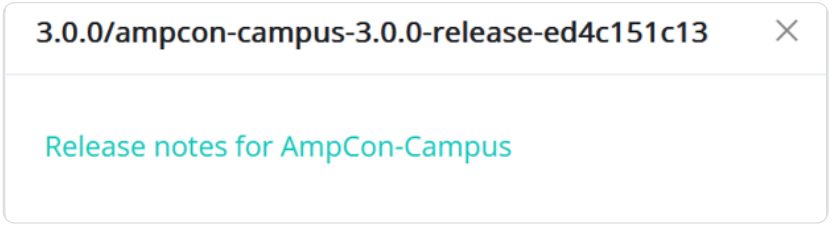
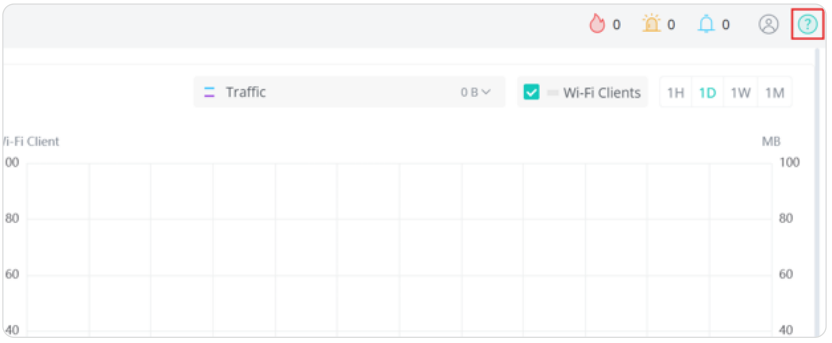


UI Overview

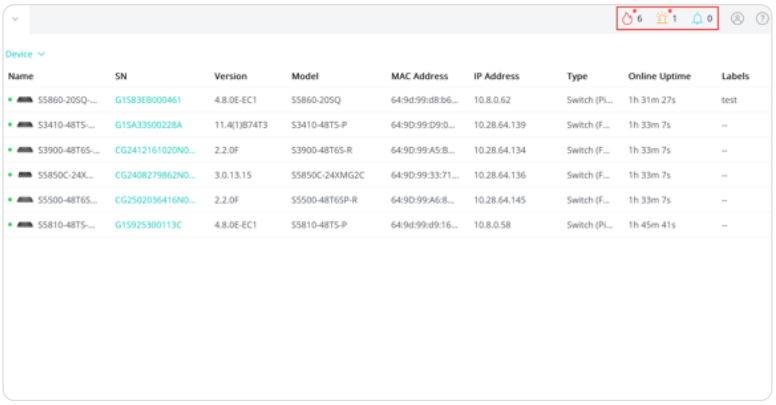
In the AmpCon-Campus UI, you can see the following sections:

Table 1. Homepage Descriptions

Section	Description
Navigation Bar	Click the site icon to select a site first, and then click a menu icon from the navigation bar. Then, you can see a specific page for the selected site. 
Page	After clicking a menu icon from the navigation bar, you can see a specific page on the right. For example, click the **Dashboard** icon from the navigation bar. Then, you can see the “Dashboard” page on the right, where you can check managed switches and the health of AmpCon-Campus. 
User Setting	Hover over the user avatar icon in the top-right corner, and then click **User Setting**. In the pop-up window, you can change the user password and associated email address.

	
Version	Hover over the user avatar in the top-right corner, and then click **Version**. In the pop-up window, you can see the current AmpCon-Campus version. Click **Release notes for AmpCon-Campus** to check the release note document. 
Document	Click the question icon in the top-right corner. Then, you will be redirected to the AmpCon-Campus doc site. 
Alert	In the top-right corner, you can view the count of firing Error alerts, firing Warning alerts, and unacknowledged Event alerts. • If any **Error alerts** are firing and have not been viewed by any user, the Error alert icon is highlighted with a red circle. Click the icon to view these alerts. • If any **Warning alerts** are firing and have not been viewed by any user, the Warning alert icon is highlighted with a red circle. Click the icon to view these alerts. • If any **Event alerts** have not been acknowledged by any user, the Event alert icon is highlighted with a red circle. You

can click the icon to view or acknowledge these alerts. For more information, see Acknowledging Alerts.



UI Menus

Read the UI menus to learn the purpose of each UI menu and quickly master the use of the AmpCon-Campus UI.

UI Conventions

Read the UI conventions for how to use common elements (such as common buttons and icons) in the AmpCon-Campus UI.

UI Menus

To quickly use the AmpCon-Campus UI, learn the purpose of each UI menu:

> **NOTE**
>
> Only **Owner** or **Super Admin** users can view all the following UI menus. For UI menu permissions of each user role, see User Permissions on Menu Pages.

- Dashboard
- Topology
- Devices
- Clients
- Ports
- Settings
- Alerts
- Maintain
- User

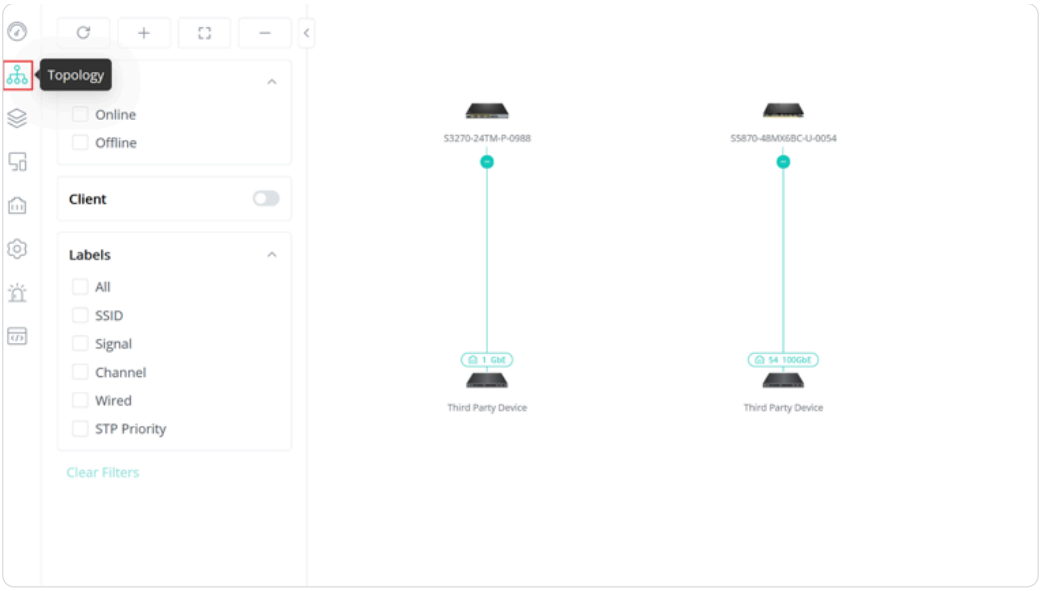
Dashboard

In the AmpCon-Campus UI, select a site, and then click the **Dashboard** icon from the navigation bar. On the “Dashboard” page, you can get a global overview of managed devices, the AmpCon-Campus status, triggered alerts, and wireless networks. For more information, see Dashboard.



Topology

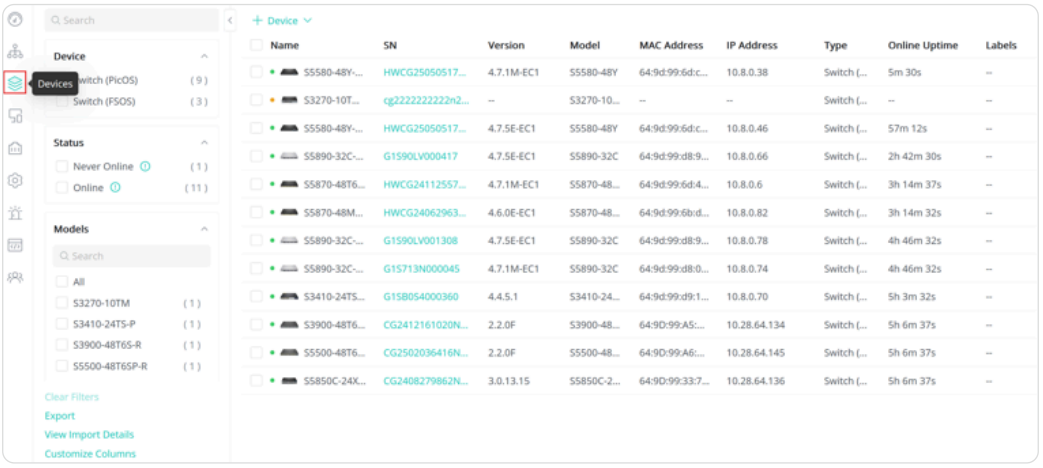
Click the **Topology** icon from the navigation bar. On the “Topology” page, you can see real-time topology diagrams of wireless and wired network devices (PicOS switches, APs, and clients) within the selected site. For more information, see Topology.



Devices

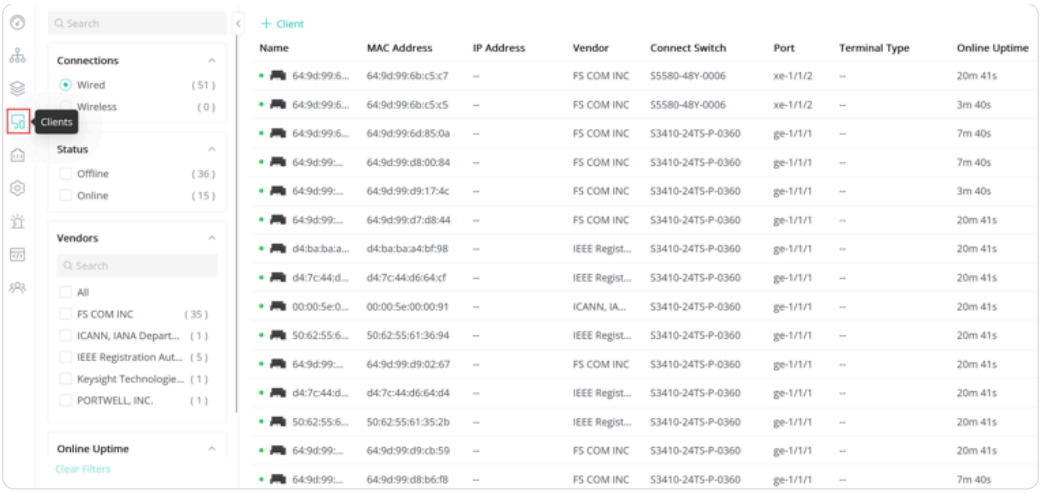
Click the **Devices** icon from the navigation bar. On the “Devices” page, you can view and manage devices (PicOS switches, FSOS switches, and APs). For more information, see the following topics:

- Monitoring - Access Points
- Monitoring - PicOS Switches
- Monitoring - FSOS Switches



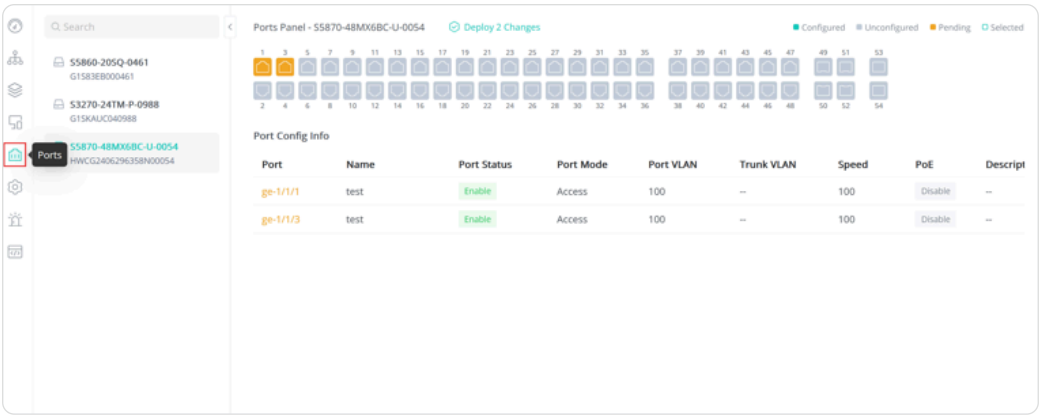
Clients

Click the **Clients** icon from the navigation bar. On the “Clients” page, you can centrally manage and monitor all wireless and wired clients across your campus network. For more information, see Monitoring - Clients.



Ports

Click the **Ports** icon from the navigation bar. On the “Ports” page, select a switch from the sidebar, and then configure its switch ports directly. For more information, see Applying Port Configurations.



Settings

Click the **Settings** icon from the navigation bar. In the **Switch** section of the sidebar, you can perform the following configurations for managed PicOS switches:

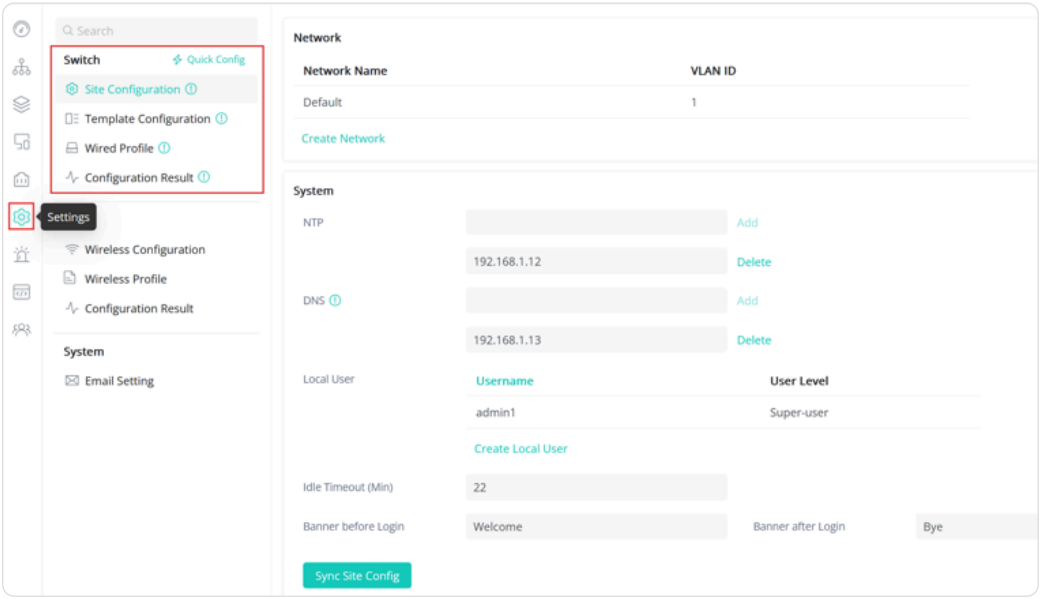
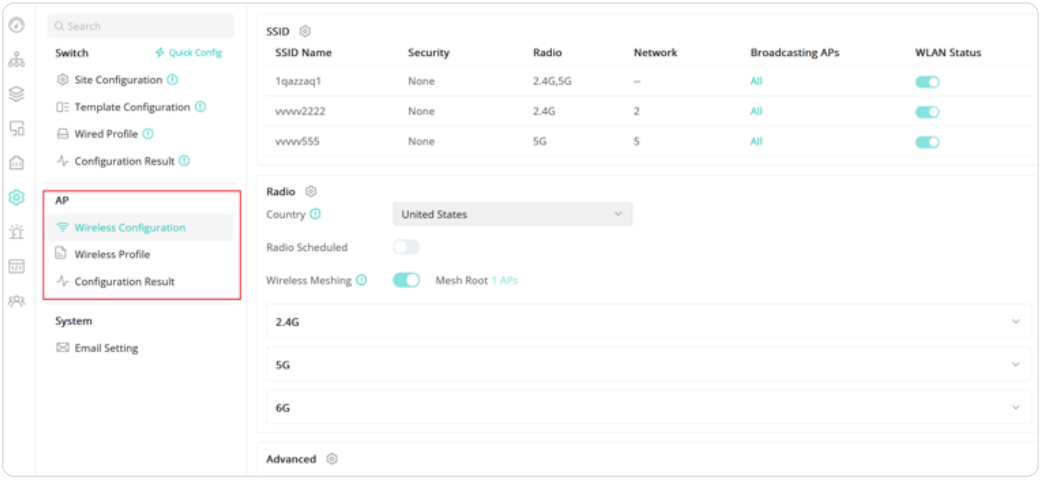


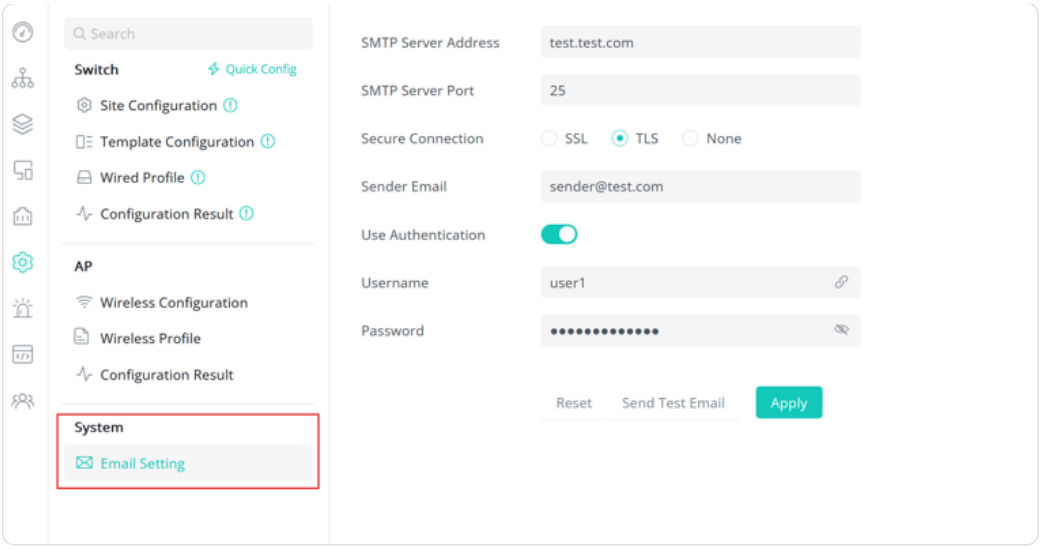
Table 1. Switch Configurations

Switch Configuration	Reference Link
Add site-level switch configurations for a site.	• Applying Site Configurations
Apply quick configurations to these switches through the **Quick Config** wizard.	• Applying Quick Configurations
Use configuration templates to push specific switch configurations.	• Applying Template Configurations
Add port profiles for PicOS switches.	• Adding a Port Profile
Check configuration results.	• Checking Configuration Results

In the **AP** section of the sidebar, you can add site-level wireless configurations, add different profiles, and check configuration results. For more information, see Configuring Wireless Networks.



In the **System** section of the sidebar, you can add SMTP configurations for alert notifications. For more information, see Adding SMTP Configurations.



Alerts

Click the **Alerts** icon from the navigation bar. You can view triggered alerts, configure alert notification rules, and check historical alert notifications. For more information, see Alerting.



Maintain

Click the **Maintain** icon from the navigation bar. You can perform the following maintenance operations:

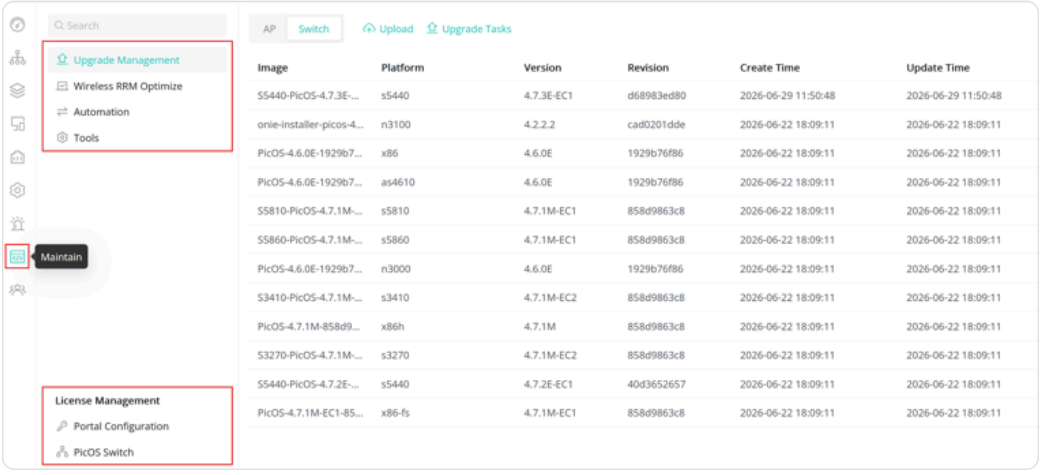
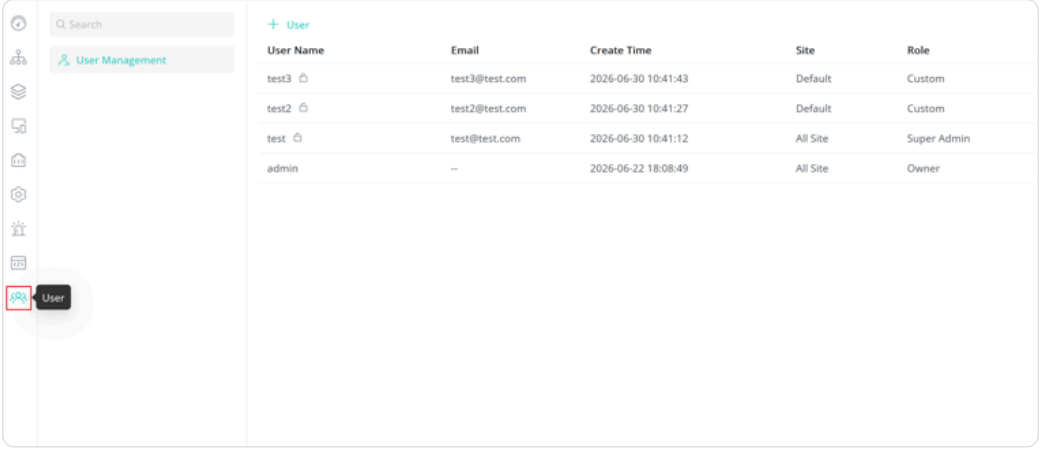


Table 2. Maintenance Operations

Maintenance Operation	Reference Link
Upload PicOS or AP images, upgrade switches or APs, and manage upgrade tasks.	• Upgrading Switches • Upgrading APs
Perform network optimization for managed APs in a site.	• Optimizing Wireless Networks
Write, import, run, and schedule Ansible playbooks on managed PicOS switches.	• Automation with Ansible Playbooks
Connect to a device (such as a switch or terminal device) from the AmpCon-Campus UI by creating an SSH session.	• Accessing Devices through SSH
Compare configurations from external files or from managed PicOS switches.	• Comparing Switch Configurations
Configure the **Global** license portal, or add more license portals.	• Managing License Portals
Use the **License Audit** feature to check the validity information of the PicOS license installed on a switch. Use the **License Action** feature to extend expired or expiring PicOS licenses for switches with PicOS licenses installed or install PicOS licenses for switches without PicOS licenses installed.	• Managing PicOS Licenses

User

Click the **User** icon from the navigation bar. On the “User” page, you can view and manage users. For more information, see Managing User Access.



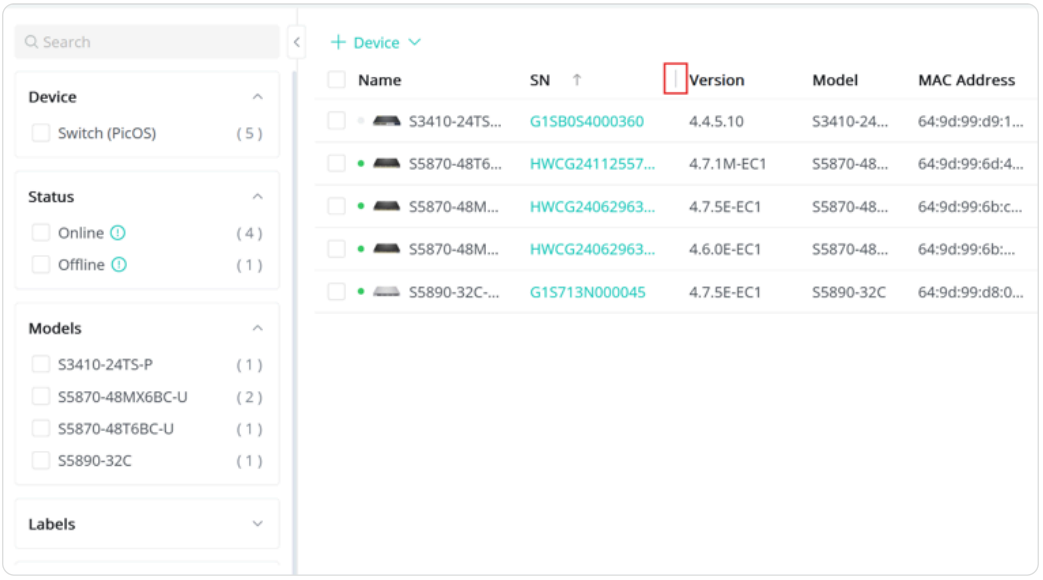
UI Conventions

To learn how to use common elements in the AmpCon-Campus UI, read the following UI conventions:

- Column Width
- Filter
- Graph
- Mouse Hover
- Selection
- Search
- Time Selection
- General Buttons
- General Icons

Column Width

If a column is too narrow to show full content, hover over the column header, and drag the column border to resize the column.

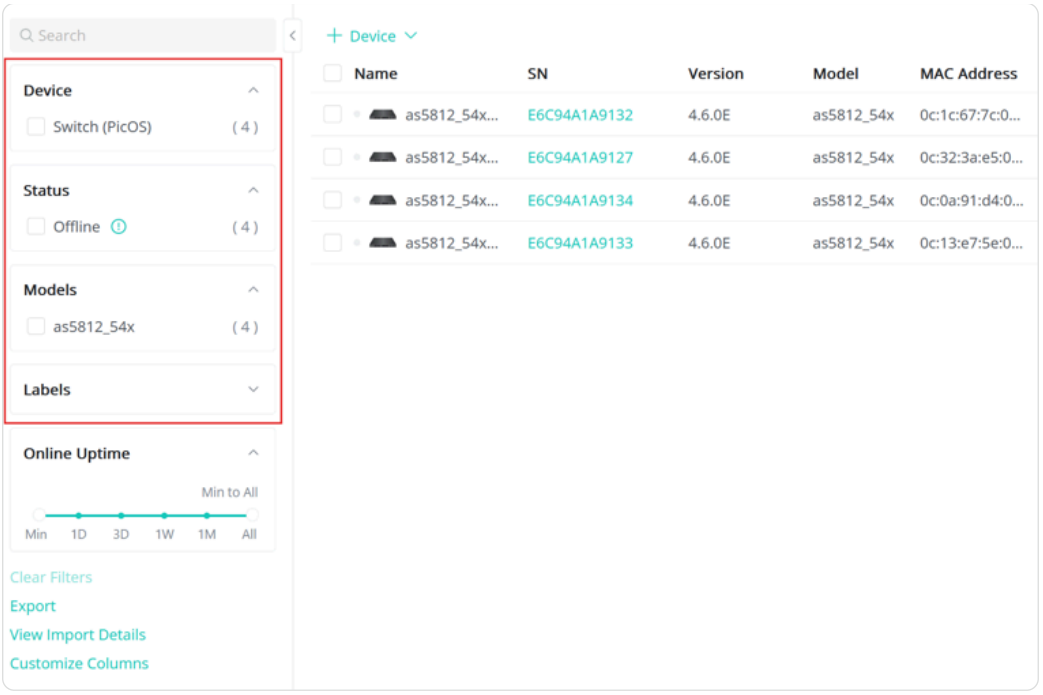


Filter

For each filter section, only the filter options matching the items in the list are displayed.

For example, in the following screenshot, only PicOS switches are in the device list and all these switches are offline. Therefore, only **Switch (PicOS)** is displayed in the **Device** filter section. Only **Offline** is displayed in the **Status** filter section.

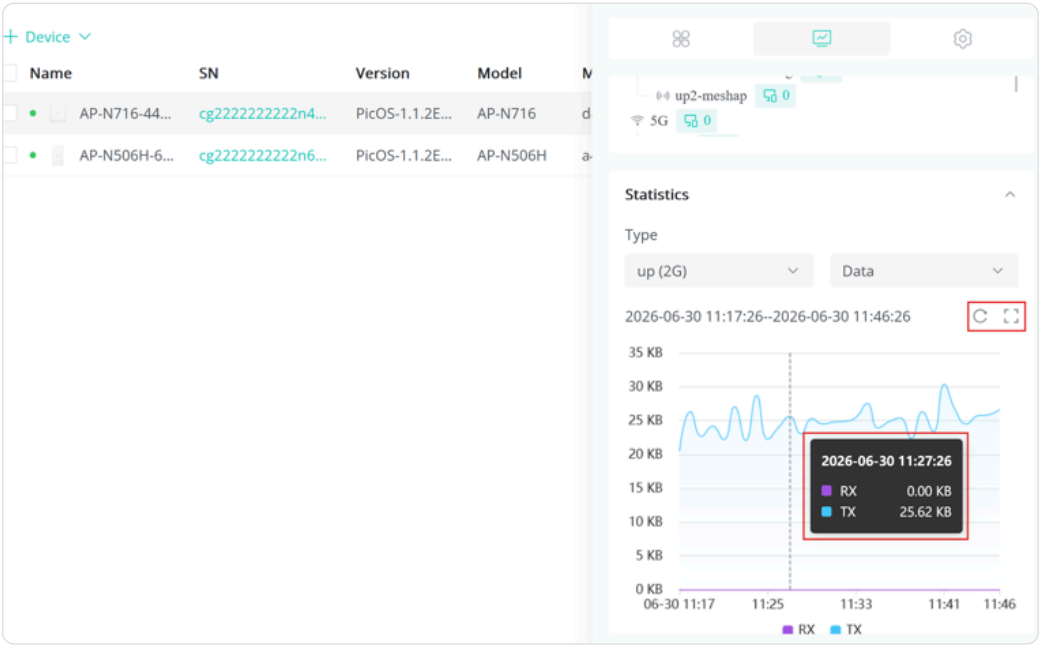
Each filter option is followed by the count of the matching items. Selecting no filter options equals selecting all filter options. To clear all filter options, click **Clear Filters**.



Graph

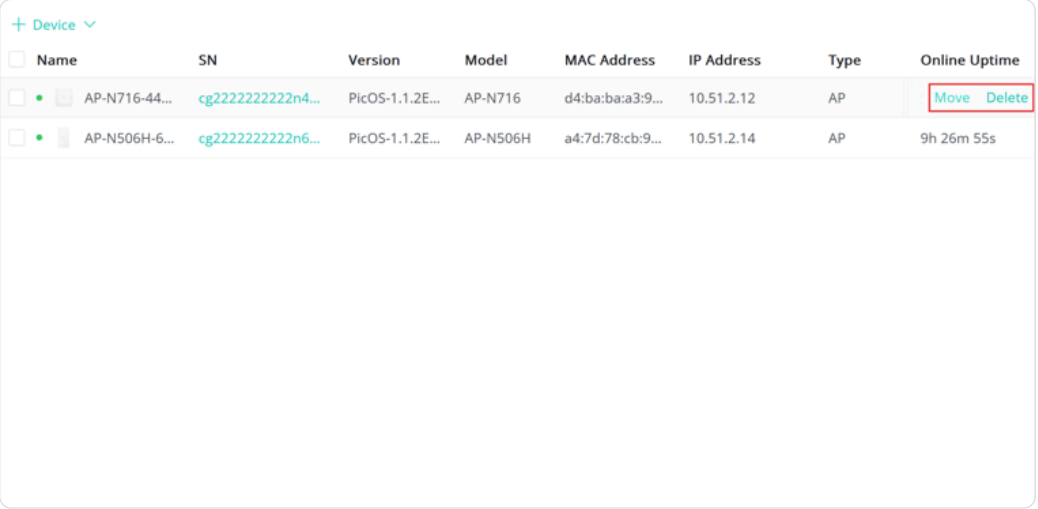
For each monitoring graph, you can hover over a time point to check detailed metric data at that time point. All data in the graph is displayed based on your browser's time zone.

To see more information, click the expand icon. To refresh the graph, click the refresh icon.



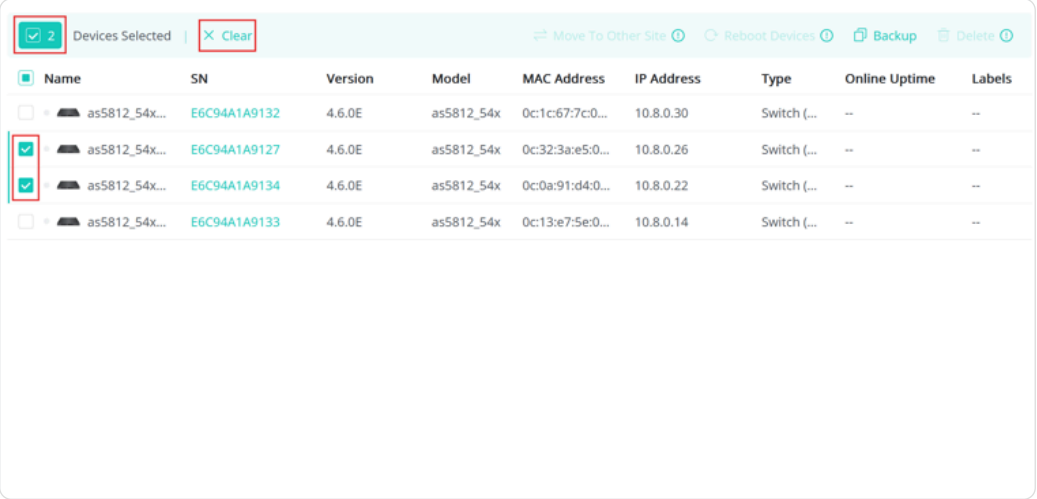
Mouse Hover

When you hover over an item, you can see related action buttons. If an action button is grayed out, it means the action button is unavailable for the item.



Selection

To perform batch operations, you need to select the items first. The count of selected items is displayed. To clear the selection, click **Clear**.

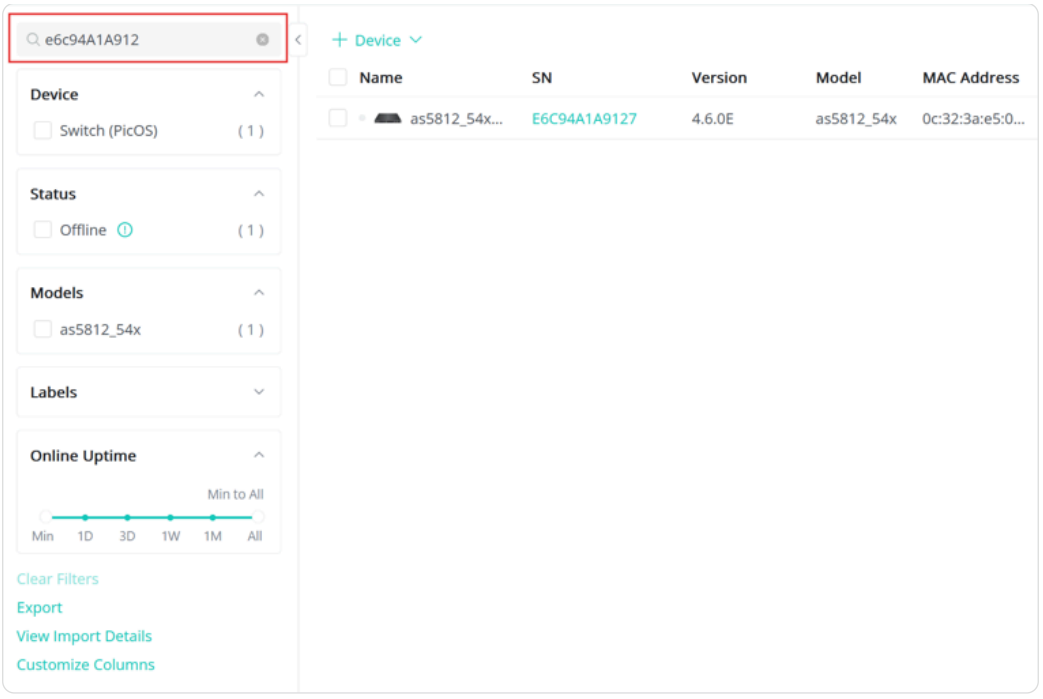


Search

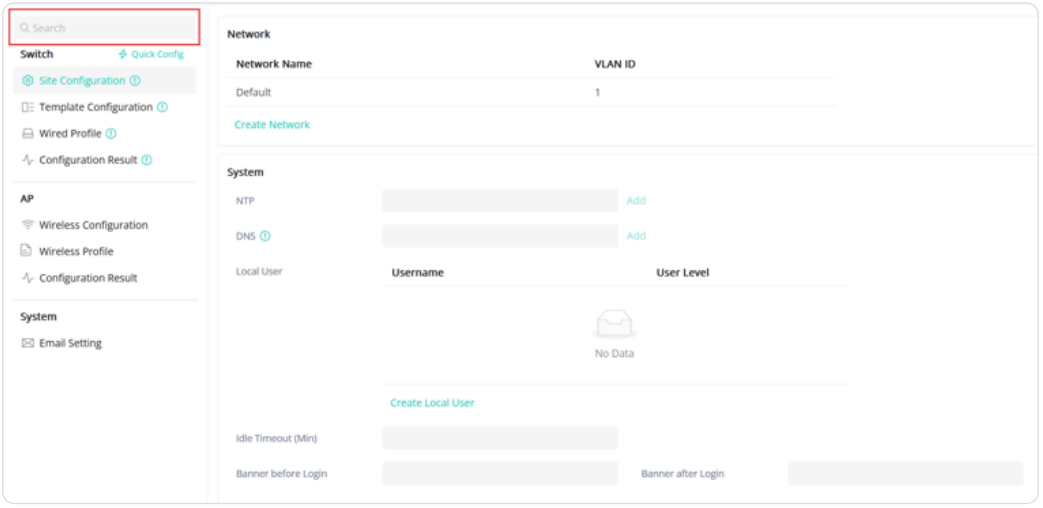
Some pages have a search box. Enter keywords in the search box to display only the information that you need.

AmpCon-Campus supports full-text search and fuzzy search, and all searches are case-insensitive.

The search box can be used on AmpCon-Campus pages containing only a list on the right.



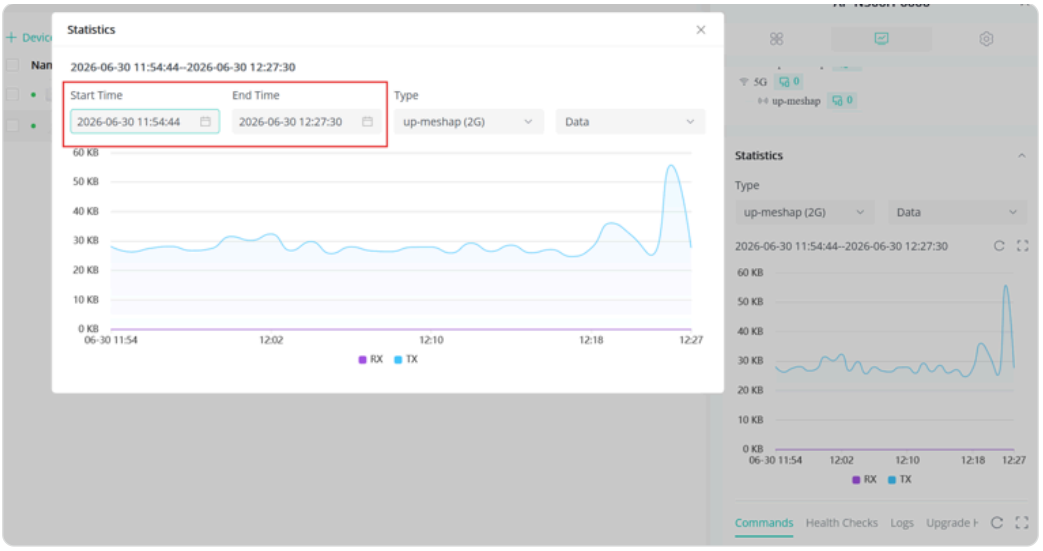
The search box cannot be used for AmpCon-Campus pages containing configurations.



Time Selection

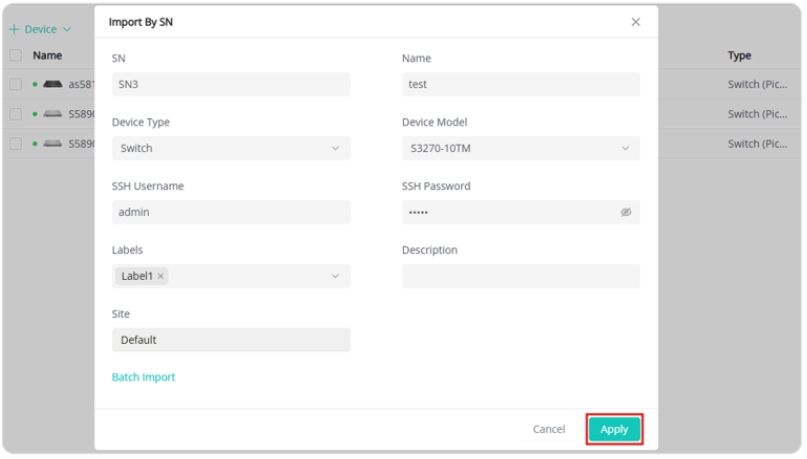
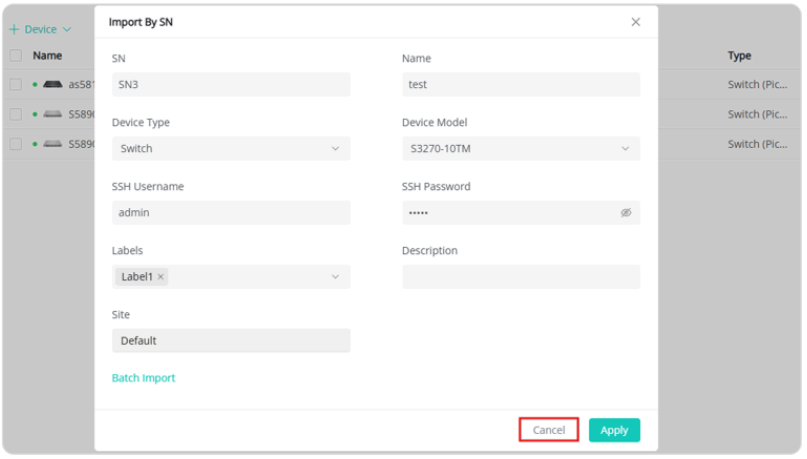
Some pages or pop-up windows have a time selection box. Select the start date and end date to display only the data in the selected time range.

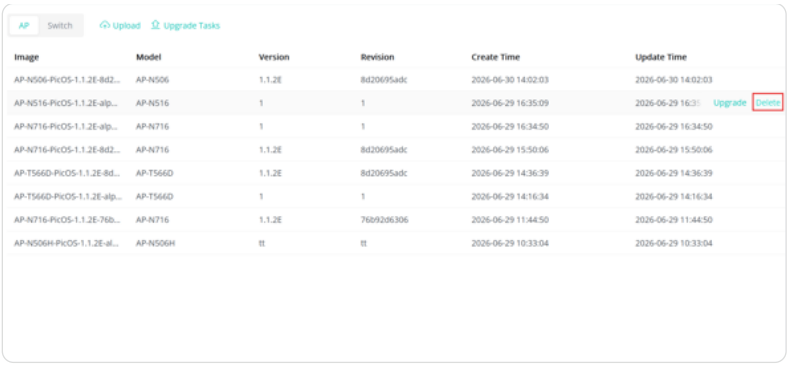
All times displayed in the AmpCon-Campus UI are based on your browser's time zone.

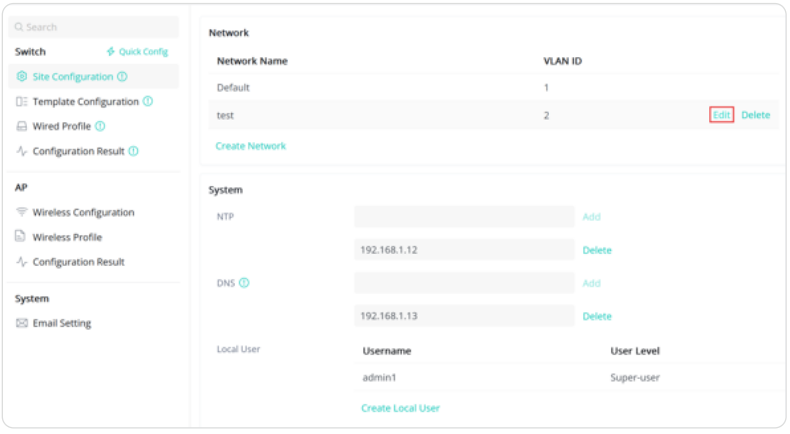
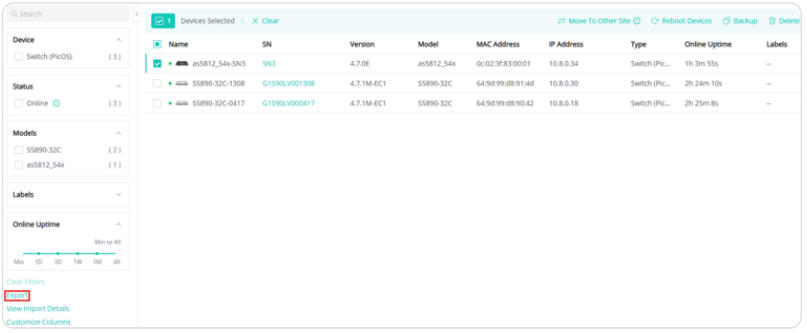
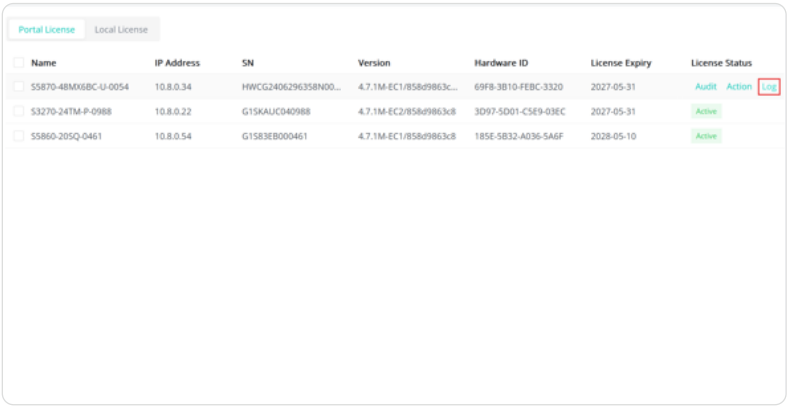


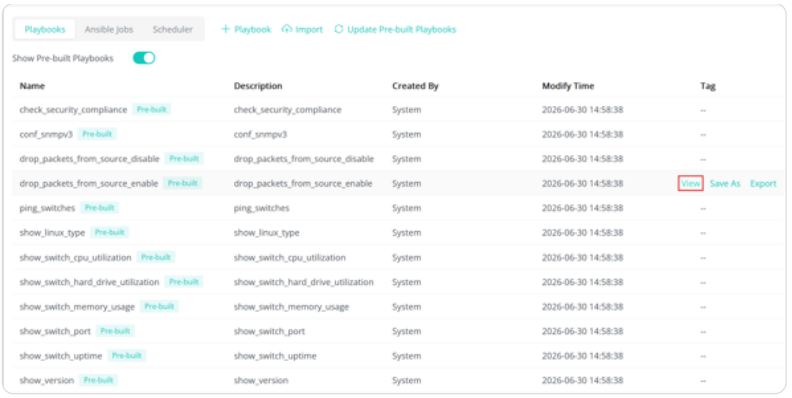
General Buttons

Table 1. General Buttons

Button	Description
Apply Button	Click the **Apply** button to apply configurations.
Cancel Button	Click the **Cancel** button to cancel an operation.
Delete Button	Hover over an item and then click the **Delete** button to delete it.

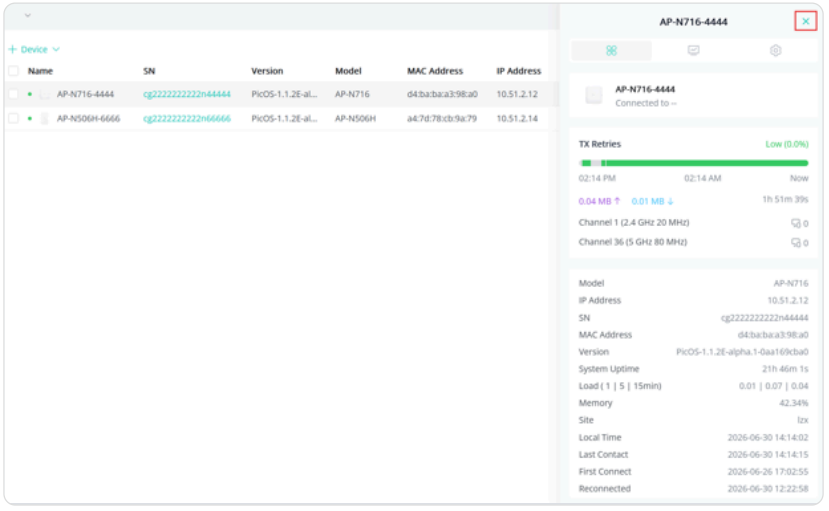
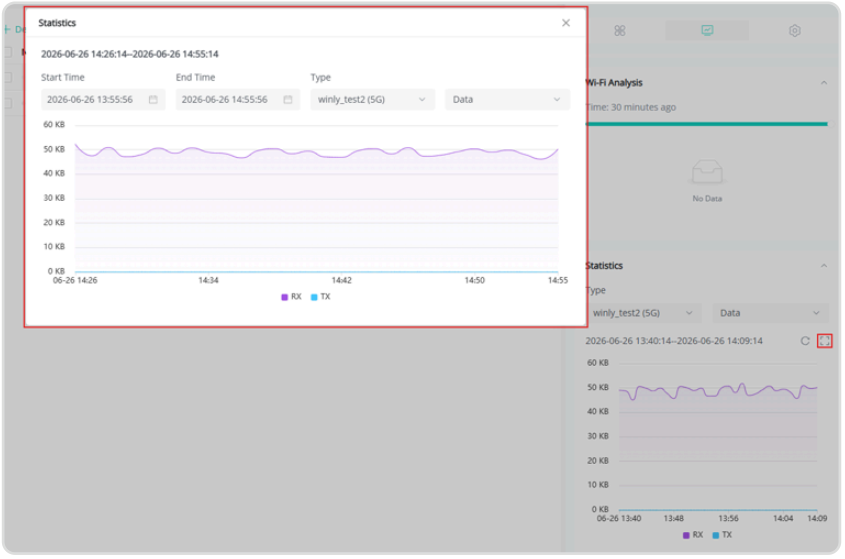


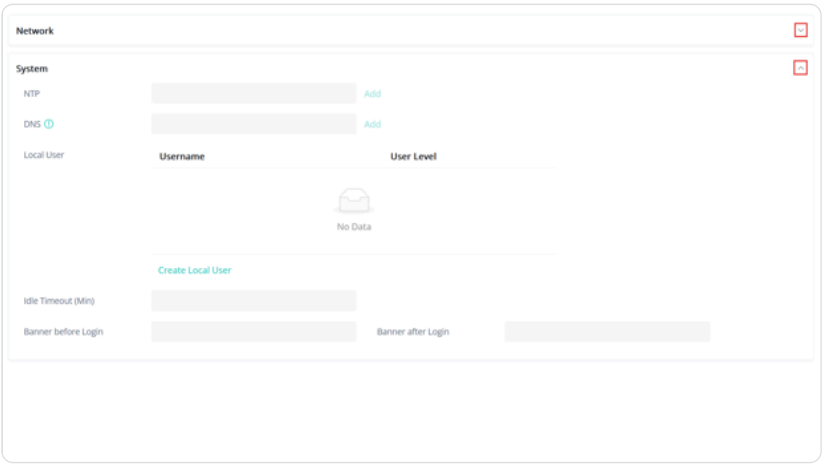
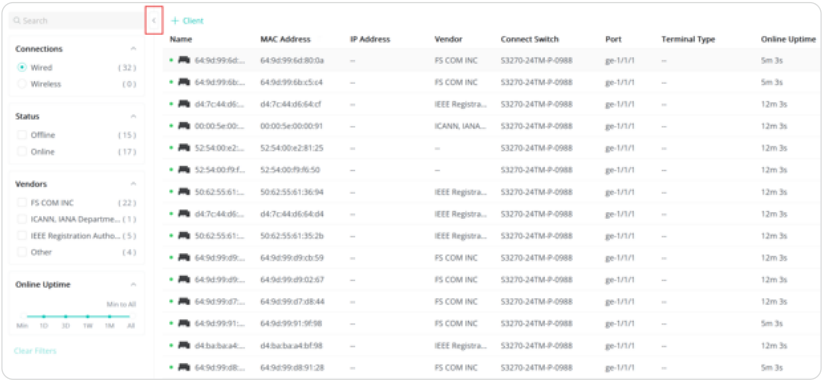
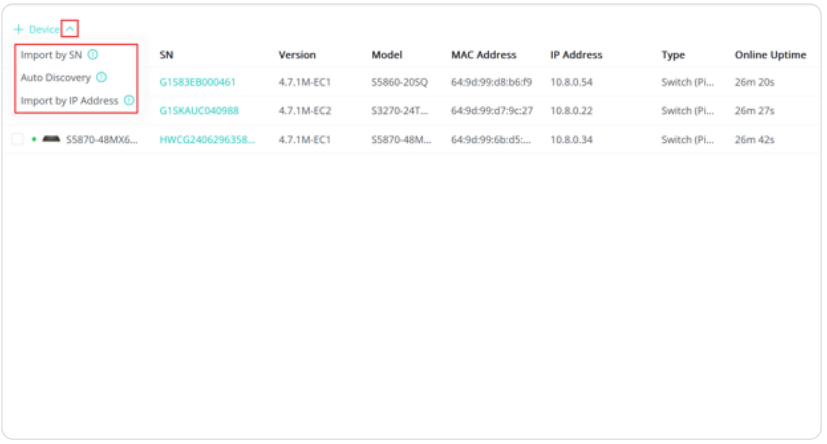
Edit Button	Hover over an item and then click the **Edit** button to edit it. 
Export Button	Click the **Export** button to export data. 
Log Button	Hover over an item and then click the **Log** button to view log details. 
View Button	Hover over an item and then click the **View** button to view data.

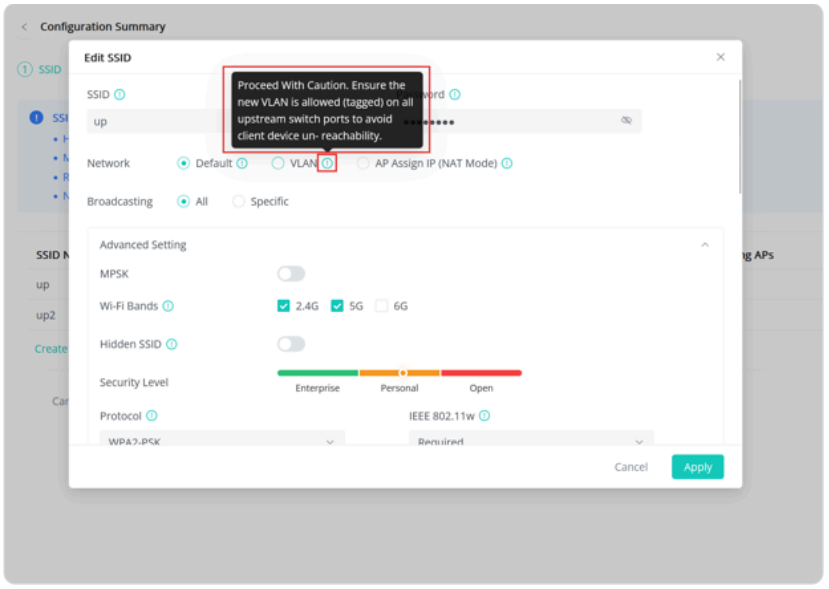


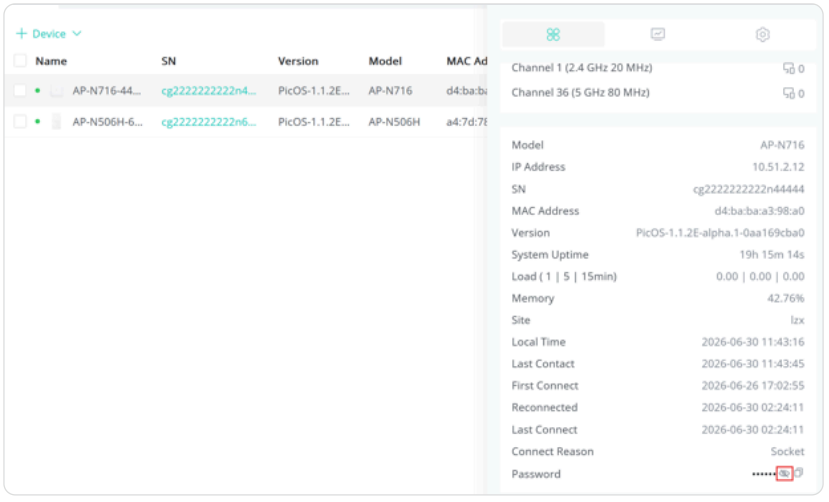
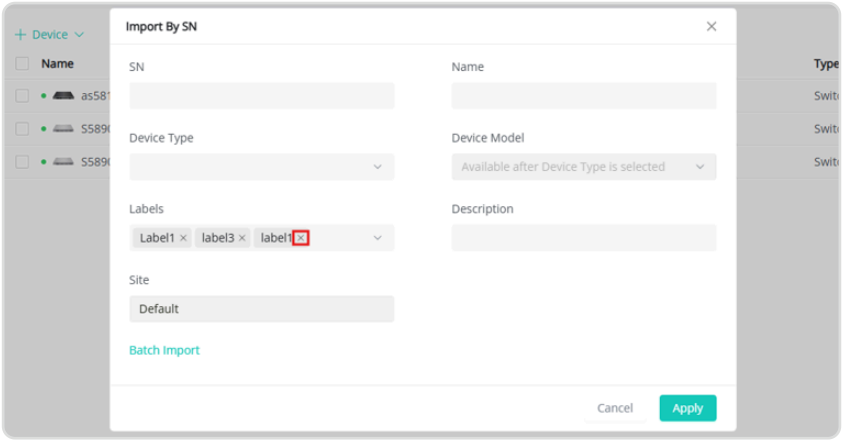
General Icons

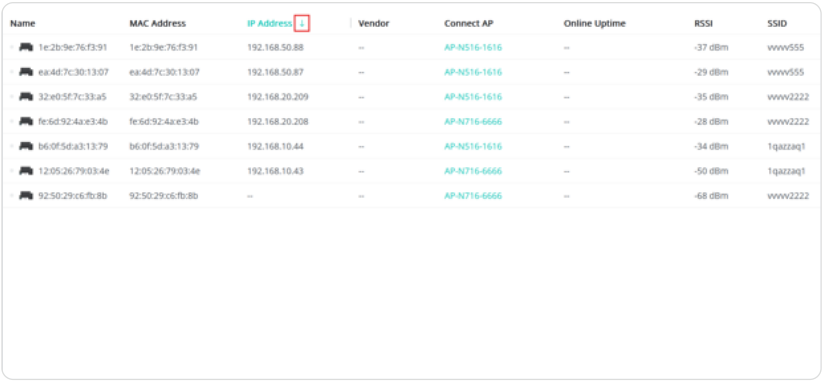
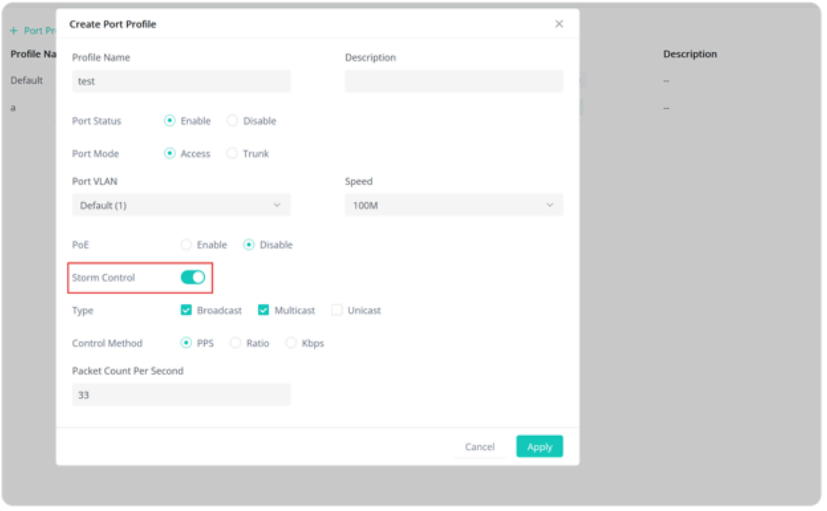
Table 2. General Icons

Icon	Description
Close Icon	To close a pop-up window, click the close icon. 
Expand Icon	Click the expand icon to view more information in a pop-up window. 

Fold/Unfold Icon	Click the fold or unfold icon to collapse or expand contents.   Some buttons have an unfold icon similar to a down arrow. Hover over or click the unfold icon, and then you can see sub-buttons. 
Help Icon	Some page names, buttons, or field names are marked with the exclamation mark icons. Hover over an exclamation mark icon to check notes.



Password Icon	To view the clear-text password, click the eye icon. To hide the clear-text password, click the eye icon again. 
Remove Icon	After adding one or more items to a field or box, click the remove icon to delete an entry. 
Sort Icon	Hover over an item, and then click the up arrow icon to display data in ascending order.

	Click the down arrow icon to display data in descending order. 
Toggle Icon	Click the toggle icon to toggle a function on or off. 

Managing Sites

A site is a logical management unit that groups resources for centralized device configuration, management, monitoring, and permission isolation. You can use sites to meet your needs.

Guidelines
Viewing All Sites
Adding a Site
Switching to Another Site
Moving Devices to Another Site
Editing a Site
Deleting a Site

Guidelines

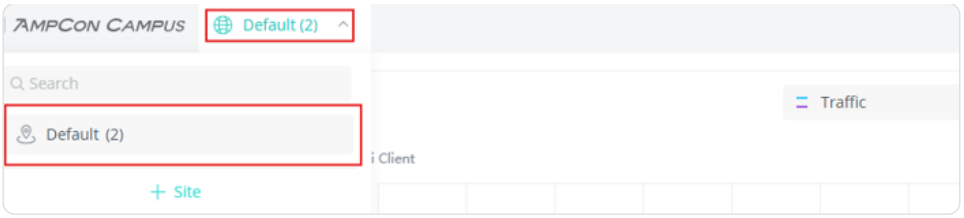
- You can view or manage only the sites accessible to the currently logged-in AmpCon-Campus user.
  - Only **Owner** and **Super Admin** users can manage sites. **Site Admin** and **Readonly** users assigned to specific sites can only view the assigned sites.
  - If a **Site Admin** user is assigned to only one site and that site is deleted, the user will no longer have any accessible site until another site is assigned.
- After you select a site, the AmpCon-Campus UI displays only the information for that site. You can configure, manage, and monitor only the devices in the selected site. To manage devices in other sites, switch to the corresponding sites.
- The following information is consistent across all sites:
  - User information on the “User” page
  - Uploaded images on the “Upgrade Management” page
  - SMTP configurations on the “Email Setting” page
  - License portal configurations on the “Portal Configuration” page

Viewing All Sites

To view all added sites, follow these steps:

1. In the AmpCon-Campus UI, click the site area.
2. In the drop-down list, view all added sites.

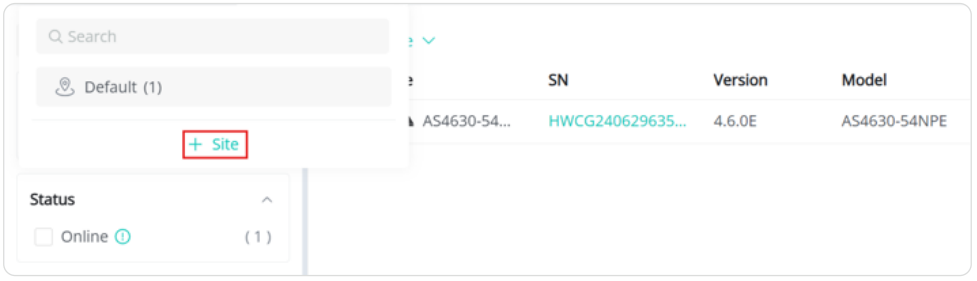
   Each site name is followed by the count of devices (APs and switches) belonging to this site. For example, **lr_roam (2)** means the site named **lr_roam** has 2 devices.



Adding a Site

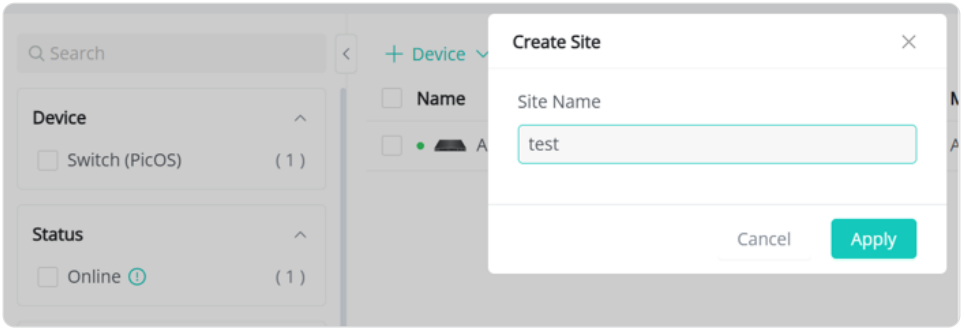
The site named **Default** is a built-in site. You can use it or add new sites. To add a site, follow these steps:

1. Click the site area, and then click **+ Site**.



2. In the pop-up window, enter the site name.

   The site name must be unique. The site name can contain at most 64 characters and cannot contain only spaces.

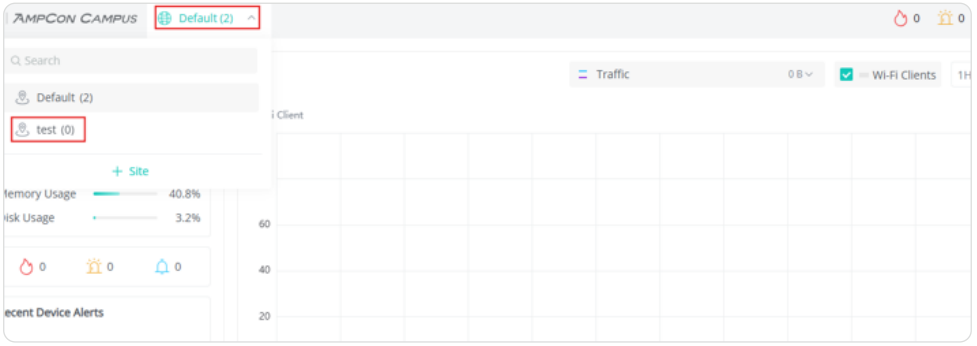


3. Click **Apply**.

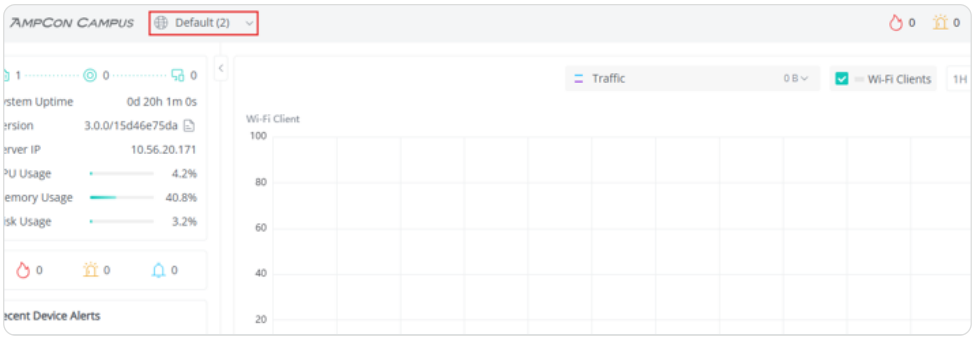
Switching to Another Site

To switch the AmpCon-Campus UI from one site to another, follow these steps:

1. Click the site area, and then click the target site name.



2. Check the site area to see whether the target site name is displayed.



Moving Devices to Another Site

To move devices (switches or APs) from one site to another, refer to the following topics:

- Moving Switches to Another Site
- Moving FSOS Switches to Another Site
- Moving APs to Another Site

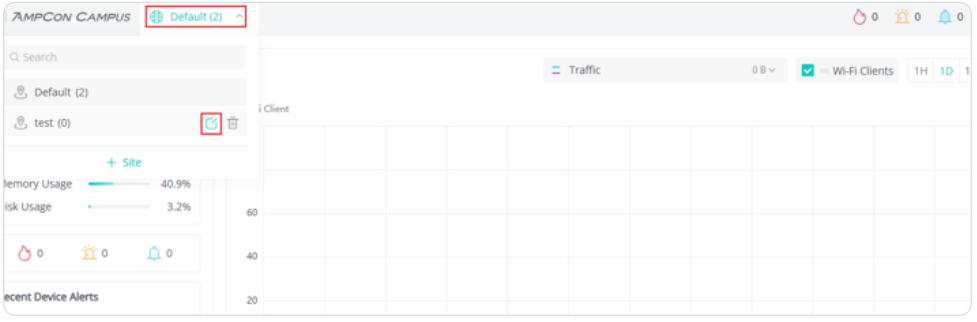
> **NOTEs**
>
> - After you move a PicOS switch to another site or onboard a PicOS switch to a site, if the site has site-level switch configurations, the configurations will be automatically pushed to the switch.
> - After you move an AP to another site or onboard an AP to a site, if the site has site-level wireless configurations, the configurations will be automatically pushed to the AP.

Editing a Site

To edit a site name, follow these steps:

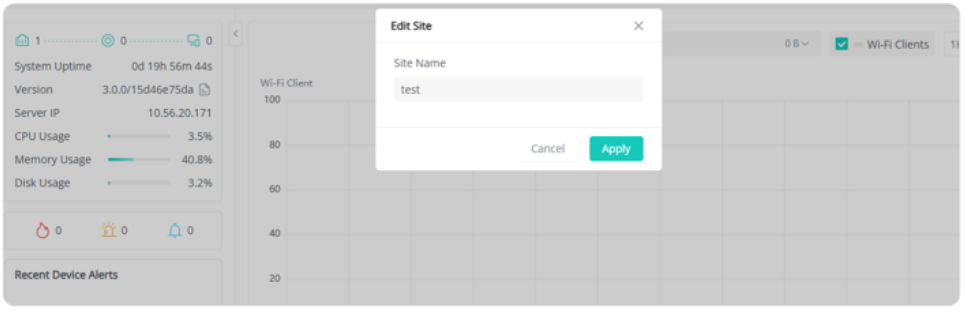
1. Click the site area, hover over the site to be edited, and then click the edit icon.

> **NOTE**
>
> The site **Default** cannot be edited.、



2. In the pop-up window, enter a new site name, and then click **Apply**.

The site name must be unique. The site name can contain at most 64 characters and cannot contain only spaces.

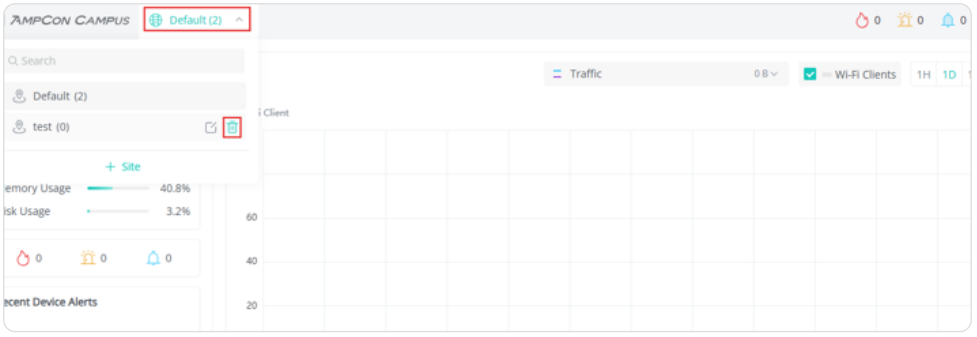


Deleting a Site

To delete a site, follow these steps:

1. Click the site area, hover over the site to be deleted, and then click the delete icon.

> **NOTEs**
>
> - The site **Default** cannot be deleted.
> - If the site contains APs or switches, you must delete the devices first or move the devices to other sites before deleting the site. Otherwise, the site deletion will fail.
> - After you delete a site, its site-level wireless and switch configurations will also be deleted. The deletion cannot be undone.



2. In the pop-up window, click **Yes** to confirm the deletion.

   After the site is deleted, if the currently logged-in AmpCon-Campus user has access to the site **Default**, the user will be redirected to the site **Default**. Otherwise, the user will be redirected to another site that the user can access.

Onboarding Switches and APs

After you install AmpCon-Campus and create sites, you can onboard access points (APs), PicOS switches, and FSOS switches to AmpCon-Campus.

- To deploy a wireless network, you need to onboard access points (APs) to AmpCon-Campus first. Onboarding APs means bringing APs under management of AmpCon-Campus. After APs are onboarded, they can be managed by AmpCon-Campus.
- Onboarding PicOS switches means bringing switches under management of AmpCon-Campus. After PicOS switches are onboarded, they can be managed by AmpCon-Campus.
- You can onboard FSOS switches by importing these switches to AmpCon-Campus. Though FSOS switches can be onboarded to AmpCon-Campus, they can't be managed by AmpCon-Campus. You can only monitor them as described in Monitoring - FSOS Switches.

See the following child topics:

- Onboarding PicOS Switches
- Onboarding FSOS Switches
- Onboarding APs

Onboarding PicOS Switches

Onboarding PicOS switches means bringing switches under the management of AmpCon-Campus. After PicOS switches are onboarded, they can be managed by AmpCon-Campus.

You can onboard PicOS switches to AmpCon-Campus for centralized and efficient switch management.

- Guidelines
- Prerequisites
- Adopting Switches
- Importing Switches by SN
- Importing Switches by IP Address

Guidelines

To onboard switches with PicOS installed, use one of the following methods:

Table 1. PicOS Switch Onboarding Methods

Category	Method	Description
ZTP Method	**Adopting Switches**	After you configure the DHCP server as described in Configuring a DHCP Server, AmpCon-Campus can discover these switches automatically and add them to the auto-discovery list. Then, you can adopt the switches in the auto-discovery list directly.
	Importing Switches by SN	If you have configured the DHCP server and obtained switch serial numbers (SNs), you can import these switches by SN.
Non-ZTP Method	**Importing Switches by IP Address**	If you have obtained switch IP addresses, you can import these switches by IP address.

ZTP methods rely on the DHCP service. For the ZTP process, see How ZTP Works.

To onboard switches without PicOS installed, you can use only the **Adopting Switches** or **Importing Switches by SN** method.

NOTEs

- After a switch is onboarded, if its SSH username or password is changed on the switch, you must update the credentials for device management. Otherwise, AmpCon-Campus cannot manage the switch. For more information, see Configuring a Single Switch.
- When you configure the DHCP server or when you import switches by IP address, you have provided the IP addresses of the switches to be onboarded.

  However, these IP addresses might be changed over time. To ensure uninterrupted connection between AmpCon-Campus and switches, OpenVPN is introduced to AmpCon-Campus.

  After a PicOS switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between AmpCon-Campus and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-Campus and the switch will communicate through the VPN tunnel.

Prerequisites

Before onboarding PicOS switches, ensure that the following prerequisites are met:

Table 2. Onboarding Prerequisites

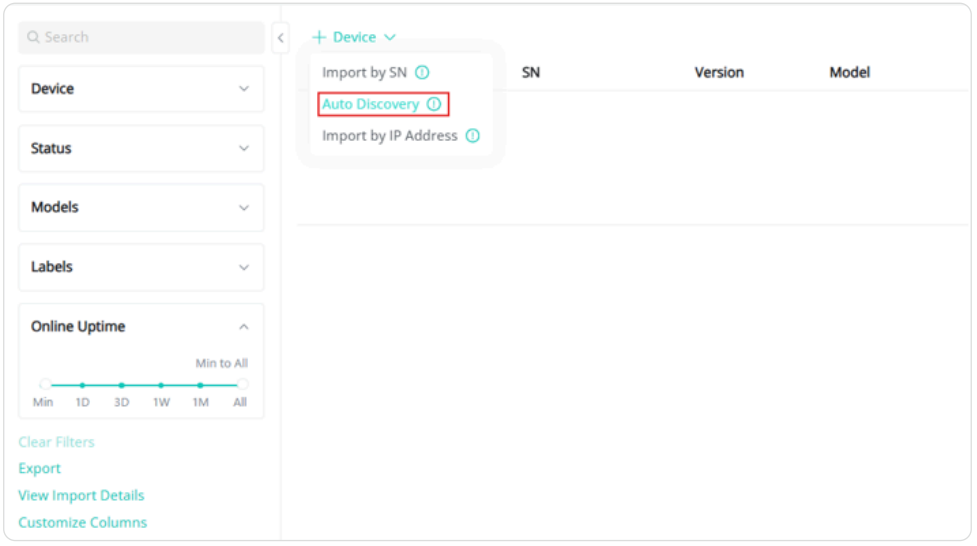
Category	Task	Reference Link
Site Requirement	Select an existing site for the PicOS switches, or add a new site as needed.	• Managing Sites
Switch Requirement	Ensure that the switches are supported by AmpCon-Campus.	• Supported PicOS Switches for 3.0.0
	Ensure that the Secure Shell (SSH) protocol is enabled on these switches. SSH is enabled on PicOS switches by default.	• No Reference Link
Network Requirement	Ensure that the switches are up and able to connect to AmpCon-Campus.	• No Reference Link

	If a firewall is configured between AmpCon-Campus and the switches, allow outbound access on the following ports to the management port of each switch. • **TCP**: 22 • **TCP**: 9339 • **TCP**: 830	• No Reference Link
DHCP Requirement	If you use the **Adopting Switches** or **Importing Switches by SN** method, ensure that you have configured the DHCP server.	• Configuring a DHCP Server

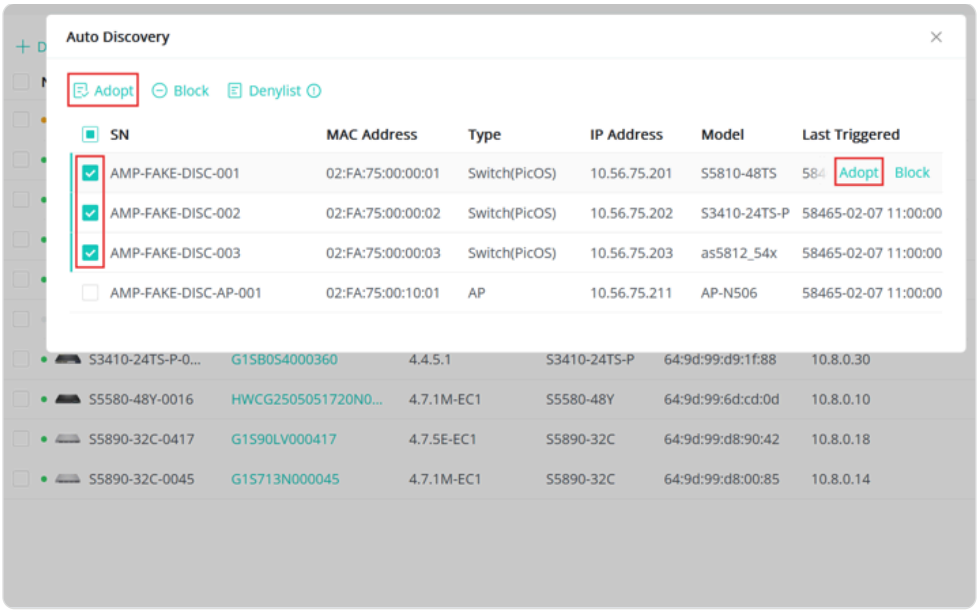
Adopting Switches

To adopt the PicOS switches in the auto-discovery list directly, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, hover over **+ Device**, and then click **Auto Discovery**.



3. In the pop-up window, adopt PicOS switches as follows:

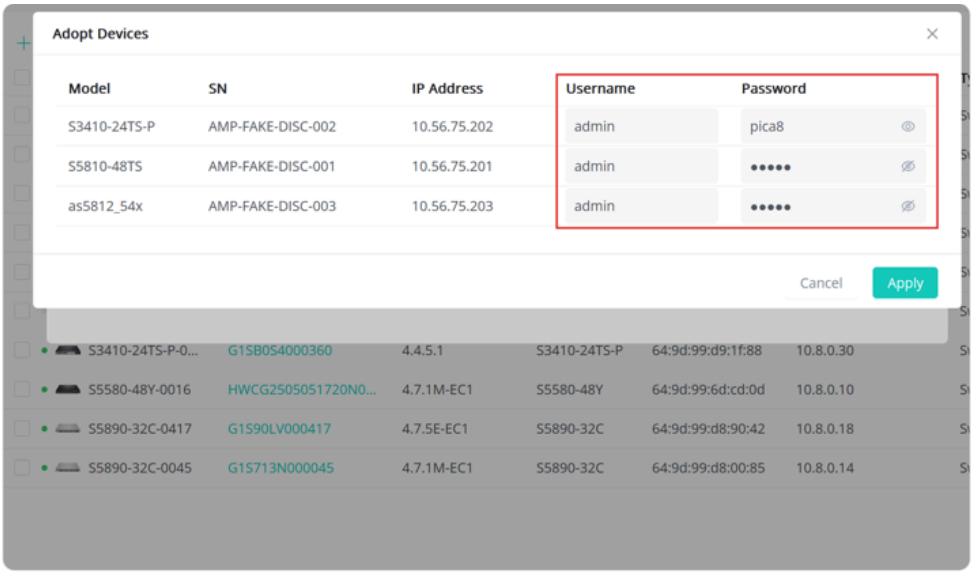


- To adopt multiple PicOS switches, select the switches, and then click **Adopt** at the top.
- To adopt a PicOS switch, select the switch, hover over the switch, and then click **Adopt** on the right. Or select the switch, and then click **Adopt** at the top.

> **Tips**
>
> - The **Last Triggered** column displays the last time AmpCon-Campus received a registration request from the switch.
> - To avoid onboarding some PicOS switches, block these switches. The blocked switches will be removed from the auto-discovery list and added to the denylist.
>   - To block a switch, hover over the switch, and then click **Block** on the right.
>   - To block multiple switches, select the switches, and then click **Block** at the top.
> - Click **Denylist**. In the pop-up window, you can see all the blocked switches. You can unblock switches when needed.
>   - To unblock a switch, hover over the switch, and then click **Unblock** on the right.
>   - To unblock multiple switches, select the switches, and then click **Unblock** at the top.

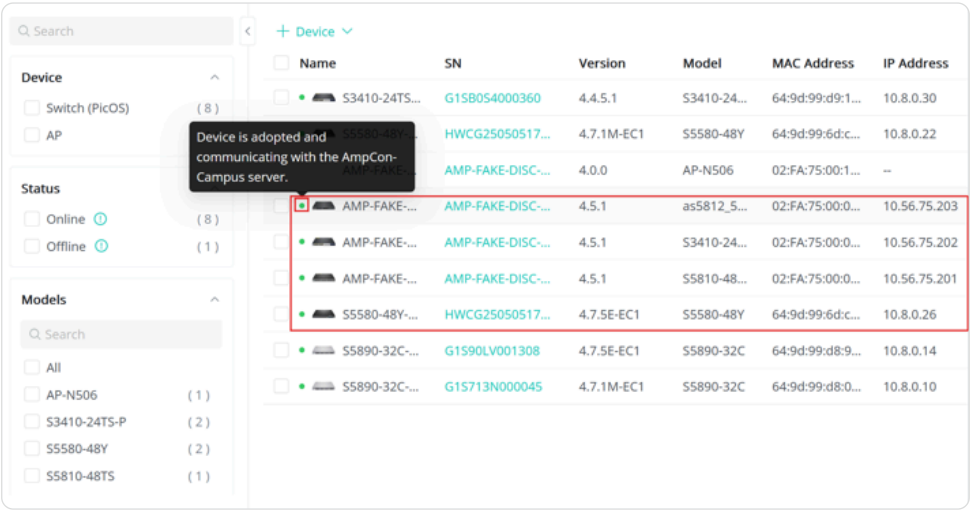
4. In the pop-up window, check whether the default username (**admin**) and password (**pica8**) can be used to log in to each switch.

   If not, enter a correct username and password. The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. The username can contain at most 32 characters.



5. In the pop-up window, you can see the quantity of switches that are successfully adopted or fail to be adopted.
6. Check whether the switches are added to the device list and whether the status circle of each switch is in green. Hover over the status circle, and then you can see the switch adoption status.

   If the adoption fails, see Device Onboarding Troubleshooting for possible reasons.



Different circle colors indicate different statuses:

Table 3. Color Meanings

Color	Description
Green	The switch is in **Online** status, which means the switch is successfully onboarded to AmpCon-Campus and is currently connected to AmpCon-Campus.

Grey	The switch is in **Offline** status, which means the switch is successfully onboarded to AmpCon-Campus but is currently disconnected from AmpCon-Campus.
Yellow	The switch is in **Never Online** status, which means the switch has been added to AmpCon-Campus but hasn't connected to AmpCon-Campus.
Blue	The switch is in **Provisioning** status, which means AmpCon-Campus is verifying authentication information of the switch or establishing an OpenVPN tunnel with the switch.
Red	The switch is in **Failed** status, which means the switch fails to be onboarded to AmpCon-Campus.

Tip

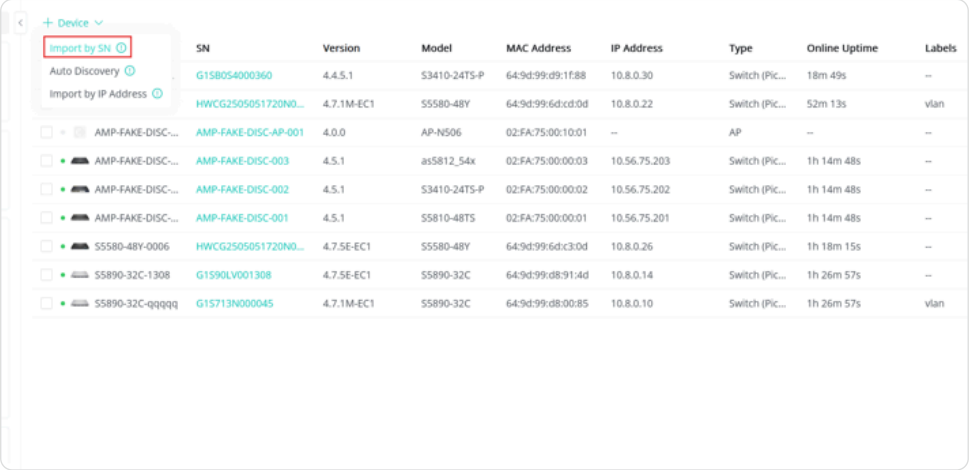
For a PicOS switch, the IP addresses shown in the auto-discovery list and the device list are different:

- In the auto-discovery list, the IP address is the one specified when configuring the DHCP server.
- In the device list, the IP address is the VPN IP automatically assigned to the switch by AmpCon-Campus.

Importing Switches by SN

To import PicOS switches by SN, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, hover over **+ Device**, and then click **Import by SN**.



3. Import a single PicOS switch or import multiple PicOS switches in batches:

- To import a single PicOS switch, input the following information in the pop-up window, and then click **Apply**.

  The **Site** value is always the site that you selected in **Step 1** and cannot be changed.

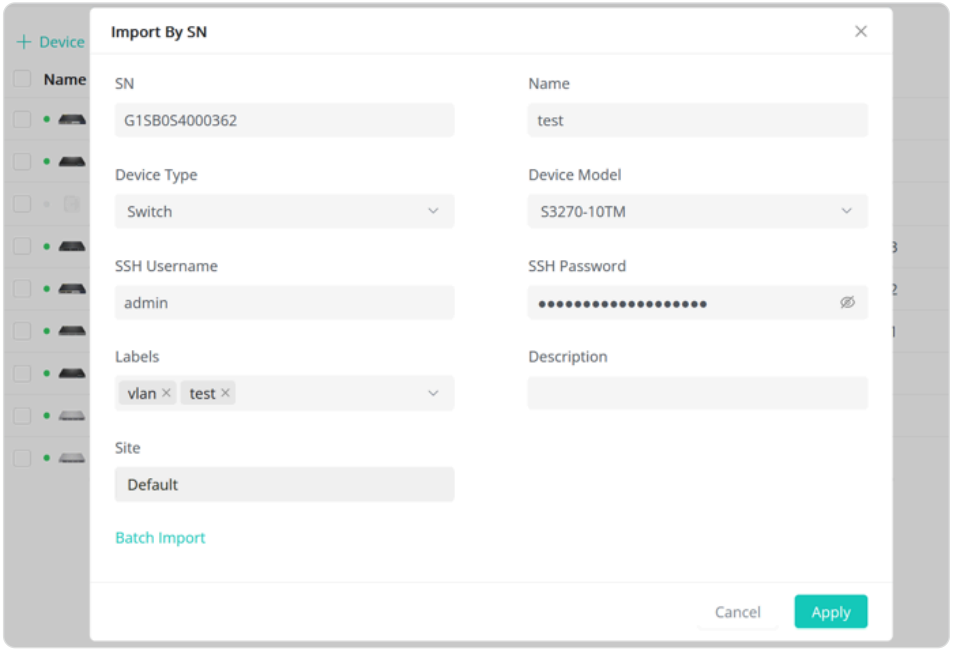


Table 4. Parameters for Import by SN

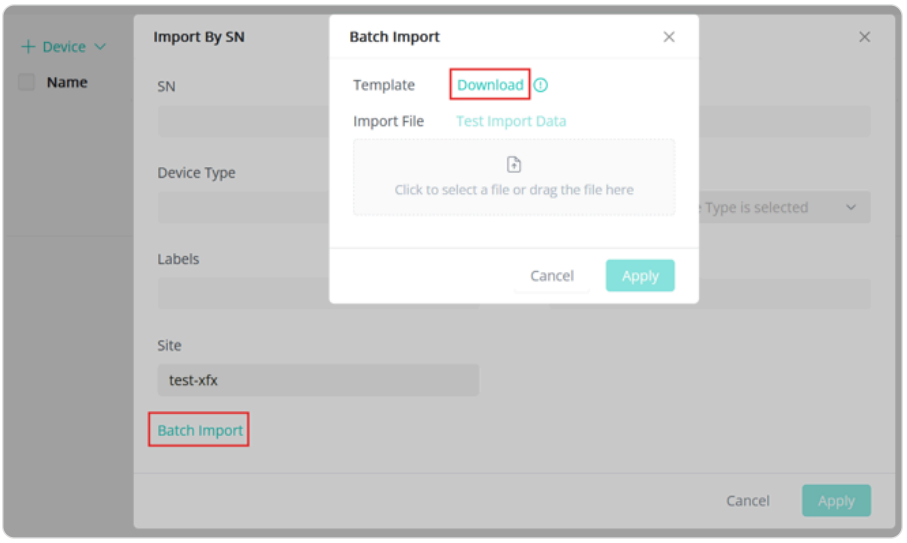
Parameter	Description
SN	The serial number (SN) of the switch. **NOTE** Ensure that the SN is correct and the corresponding switch has not been onboarded to AmpCon-Campus. Otherwise, the import might fail.

Name	Optional. The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side. The alias can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The alias cannot start or end with a hyphen or underscore. If you don't enter the alias, AmpCon-Campus automatically generates the alias for each device. The alias contains the device model and the last four digits of the switch serial number (SN).
Device Type	Select **Switch**.
Device Model	The model of the switch.
SSH Username	The username used to log in to the switch. The default username is **admin**. The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, and a trailing $. The username can contain at most 32 characters.
SSH Password	The password of the user. The default password is **pica8**. Only ASCII characters are supported. Click the eye icon to see the clear-text password. **NOTE** Ensure that the SSH username and password match the switch exactly. Otherwise, the switch cannot be imported.
Labels	Optional. The switch labels used for switch filtering and management. You can select one or multiple labels. To add a new label, click the **Labels** drop-down list, and then click **Create Label**. Each label can contain

	only letters and numbers and can contain at most 64 characters.
Description	Optional. The description of the switch. The description can contain at most 256 characters.

- To bulk import multiple PicOS switches, configure as follows:

  a. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.



  b. Open the template file, and then enter correct information in the **SN**, **DeviceType**, **DeviceModel**, **Name**, **Labels**, and **Description** columns for each switch to be imported.

> **NOTEs**
>
> - The requirements of these columns are almost the same as described in **Table 4. Parameters for Import by SN**.
> - Enter **Switch (PicOS)** in the **DeviceType** column.
> - To add multiple labels in the **Labels** column, use **$** as the separator. For example, **label1$label2$label3**.

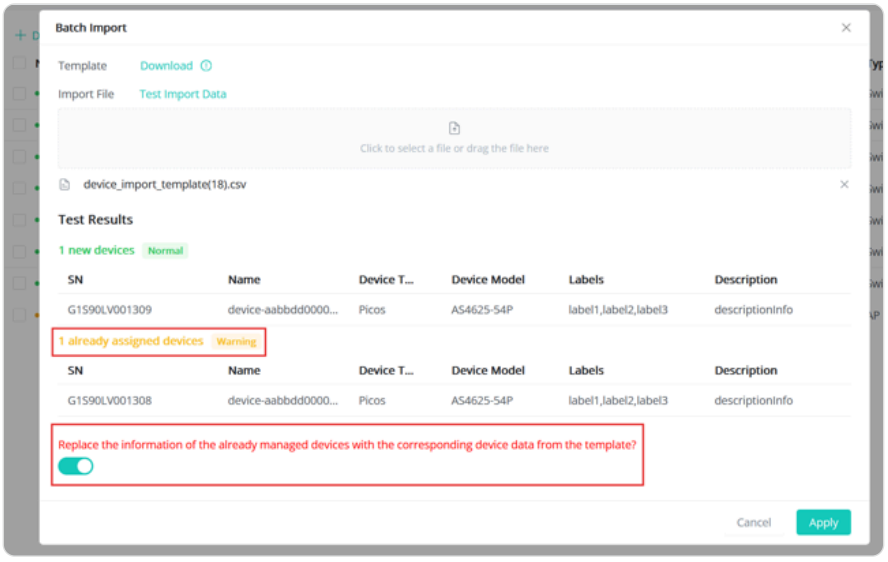
  c. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. The maximum file size is 5 MB.

  d. Optional: Click **Test Import Data**. In the new pop-up window, check the test result.

NOTEs

- If you see problematic devices in the test result, resolve the issues in the template file, and then upload the template file again.
- If a switch has been listed in the device list of the current site, you can see the **Warning** message.

  You can click the toggle to replace the device information in the list with the corresponding device data from the template. If you don't need the replacement, leave the toggle off.

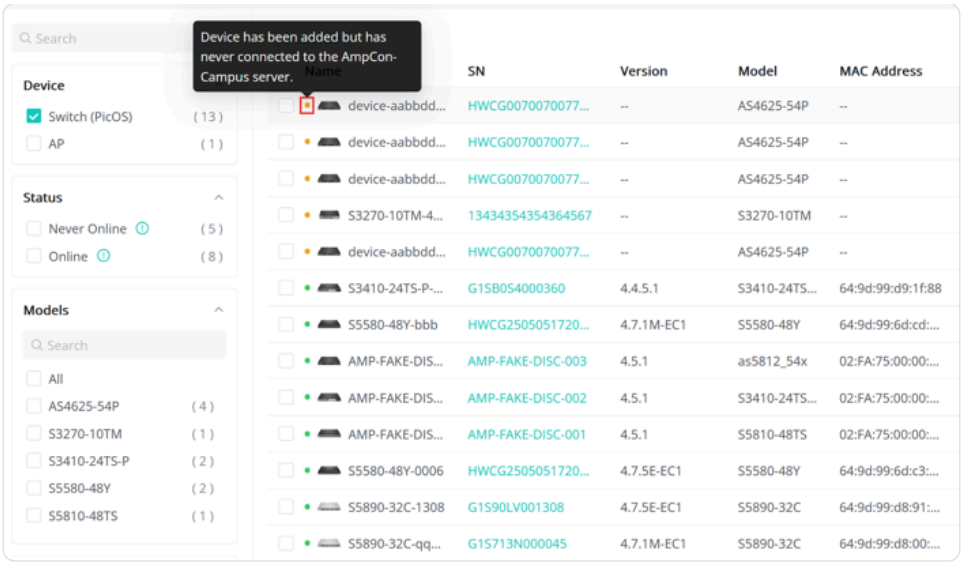


e. Click **Apply**.

4. Check whether the switches are listed in the device list and whether the status circle of each switch is in green. For the meaning of each color, see **Table 3. Color Meanings**.

   Hover over the status circle, and then you can see the switch import status.

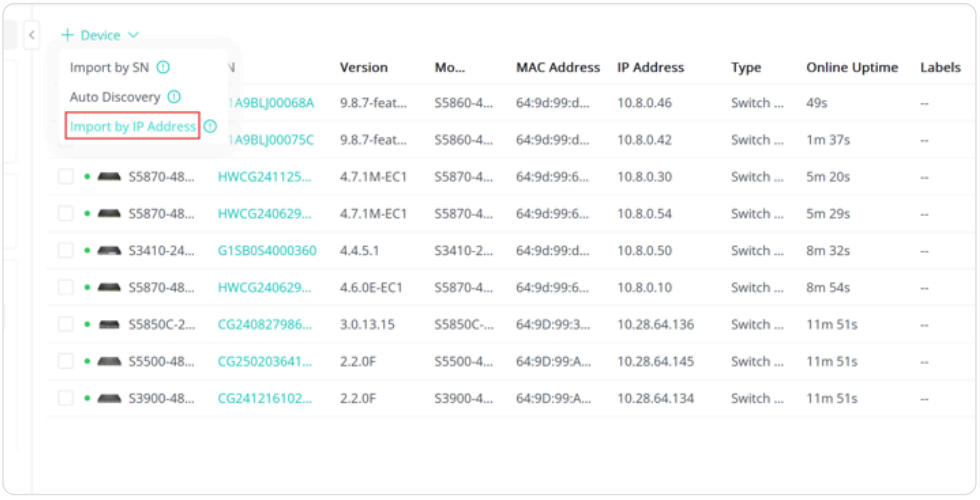
   If the import fails, see Device Onboarding Troubleshooting for possible reasons.



Importing Switches by IP Address

To import these switches by IP address, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, hover over **+ Device**, and then click **Import by IP Address**.



3. Import a single PicOS switch or multiple PicOS switches in batches:

- To import a single PicOS switch, input the following information in the pop-up window, and then click **Apply**.

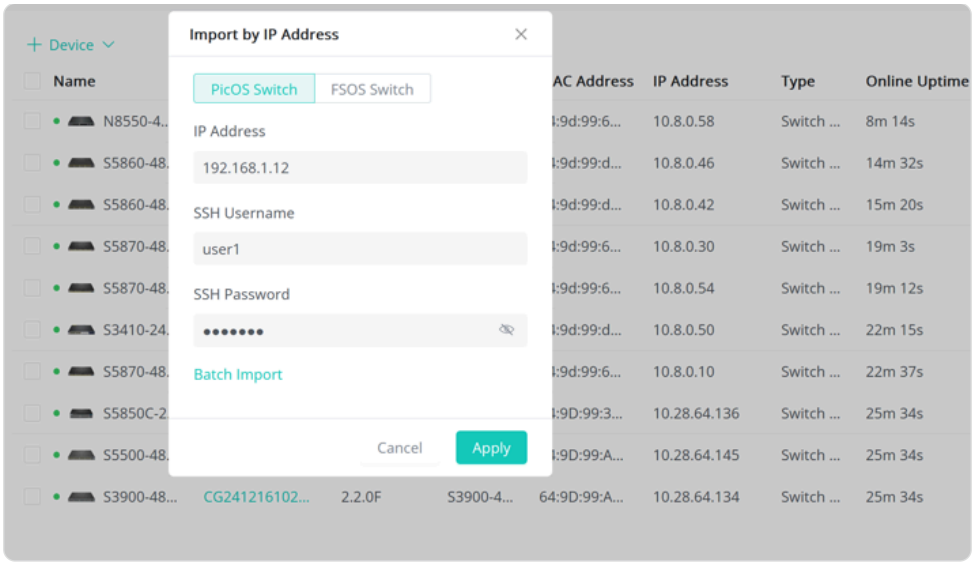
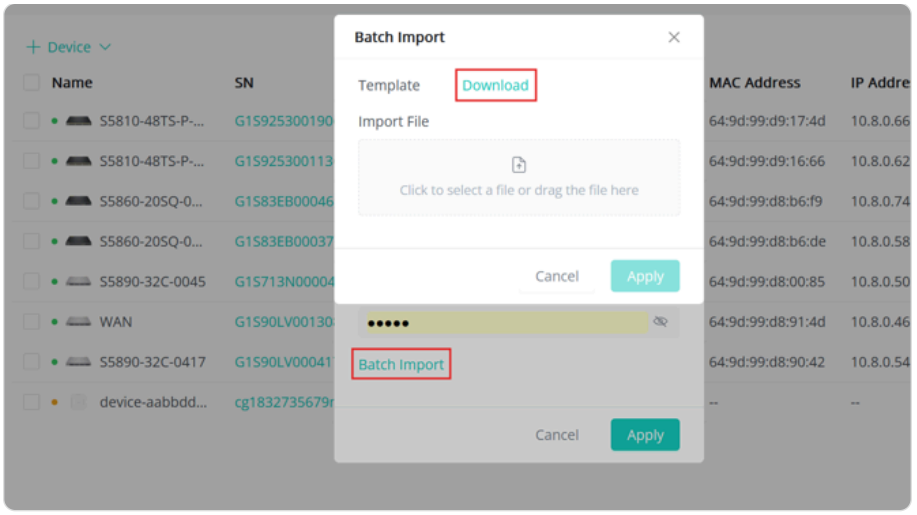


Table 5. Parameters for Import by IP Address

Parameter	Description
IP Address	The IPv4 address of the switch. **NOTE** Ensure that the IPv4 address can be reached by AmpCon-Campus and the corresponding switch has not been onboarded to AmpCon-Campus. Otherwise, the import will fail.
SSH Username	The username used to log in to the switch. The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. The username can contain at most 32 characters.
SSH Password	The password of the user. Only ASCII characters are supported. **NOTE** Ensure that the username and password are correct. Otherwise, the import will fail.

- To bulk import multiple PicOS switches, configure as follows:

  a. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.



b. Open the template file, and then enter the description (optional), IPv4 address, SSH username, and SSH password for each switch to be imported.

> **NOTEs**
>
> - The requirements of the parameters in the template file are the same as described in **Table 6. Parameters for Import by IP Address**.
> - Ensure that the information entered in the template file is correct. Otherwise, the import will fail.
> - A maximum of 500 switches can be added to a single template file.

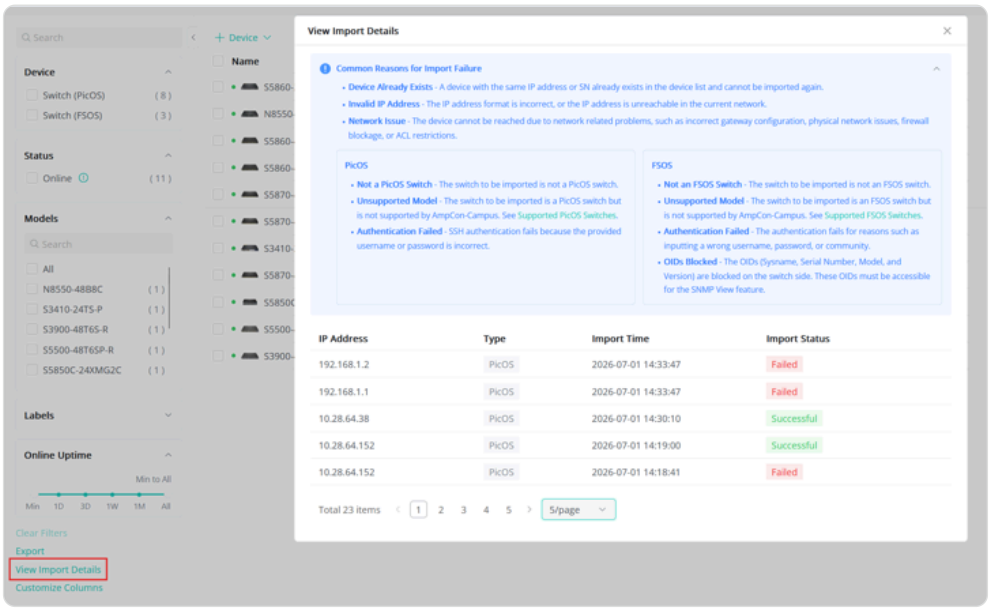
```
[
 {
  "description": "Example for PicOS Switch - sshUsername and sshPassword are required",
  "ip": "192.168.1.1",
  "sshUsername": "admin",
  "sshPassword": "password123"
 },
 {
  "description": "Example for PicOS Switch - sshUsername and sshPassword are required",
  "ip": "192.168.1.2",
  "sshUsername": "admin",
  "sshPassword": "password456"
 }
]
```

c. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. Then, click **Apply**.

4. On the “Devices” page, click **View Import Details**. In the pop-up window, locate the PicOS switches, and then check whether the import status is **Successful**.

NOTEs

- Only the switches imported by IP address are displayed in the **View Import Details** pop-up window.
- If the import fails, see Device Onboarding Troubleshooting for possible reasons.



How ZTP Works

Zero Touch Provisioning (ZTP) is a technology for automated deployment and configuration of unconfigured network devices without manual intervention.

Adopting Switches and **Importing Switches by SN** methods are ZTP methods, which rely on the DHCP service. After you plug in and reboot a switch, DHCP automatically provides the switch with an IP address and the address of a provision shell script that is obtained from the AmpCon-Campus server. Then, the switch automatically runs the shell script to complete the ZTP deployment.

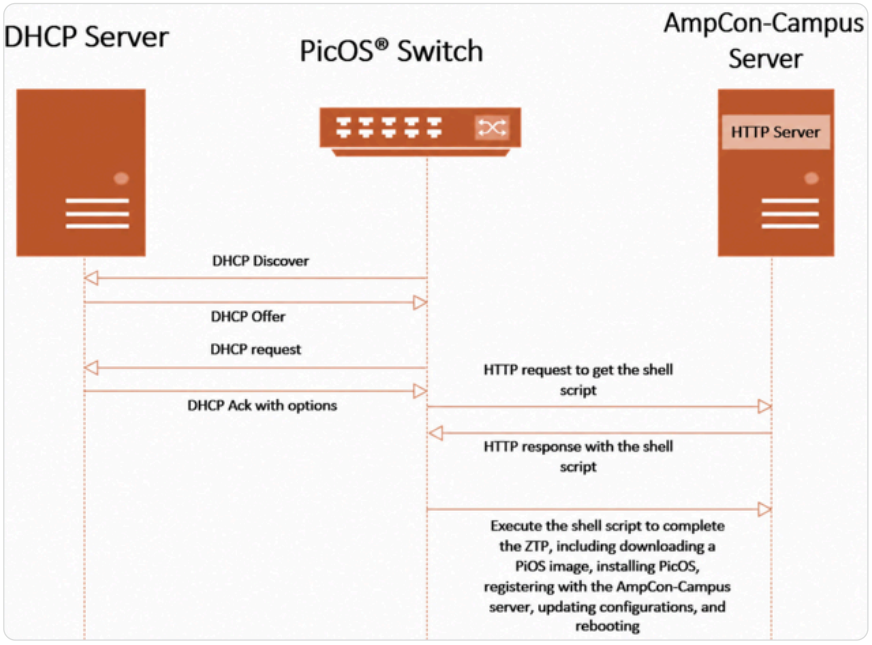
Check the following workflows to understand how ZTP works.

White-Box Switch Onboarding
Integrated Hardware and Software Switch Onboarding
PicOS License Installation and Extending

White-Box Switch Onboarding

The workflow of onboarding white-box switches is as follows:

Figure 1. Management Workflow of White-Box Switches



1. After a switch is powered on, the switch sends DHCP Discover to get an IP address, and the DHCP server provides the switch with an IP address.
2. The switch sends a request to the DHCP server, and the DHCP server sends a response including the HTTP server address.
3. The switch sends an HTTP request to the HTTP server to get the shell script, and the HTTP server sends an HTTP response with the shell script.

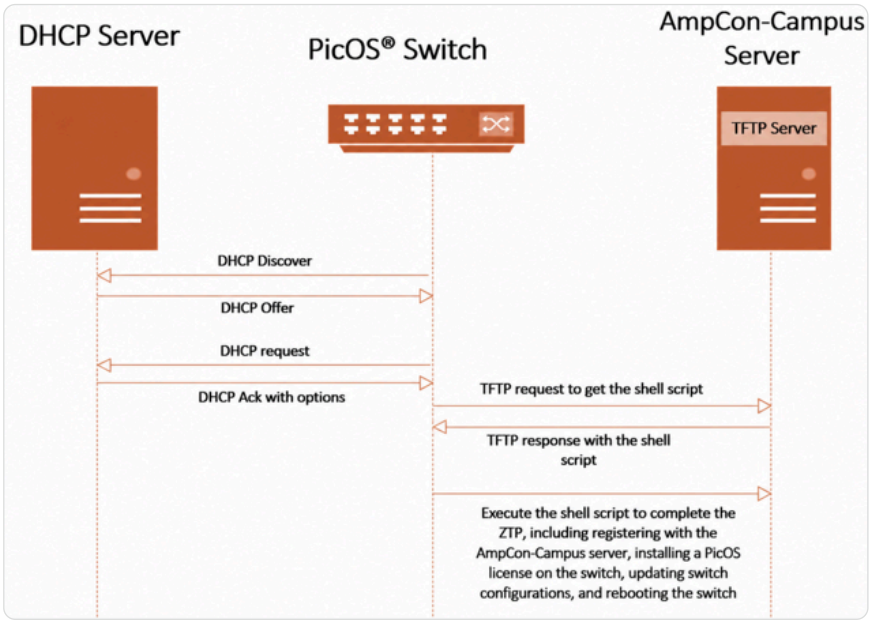
4. The switch executes the shell script to complete the ZTP deployment, including downloading a PicOS image, installing PicOS, installing a PicOS license, registering with AmpCon-Campus, updating site-level switch configurations, and rebooting the switch.

   Only if you have added site-level switch configurations for the switch's site, can these configurations be automatically pushed to the switch during switch onboarding. For more information, see Applying Site Configurations.

Integrated Hardware and Software Switch Onboarding

The workflow of onboarding integrated hardware and software switches is as follows:

Figure 2. Management Workflow of Integrated Hardware and Software Switches



1. After a switch is powered on, the switch sends DHCP Discover to get an IP address, and the DHCP server provides the switch with an IP address.
2. The switch sends a DHCP request to the DHCP server, and the DHCP server sends a DHCP response including the TFTP server address.
3. The switch sends a TFTP request to the TFTP server to get the shell script, and the TFTP server sends a TFTP response with the shell script.
4. The switch executes the shell script to complete the ZTP deployment, including registering with AmpCon-Campus, extending its PicOS license, updating site-level switch configurations, and rebooting the switch.

   Only if you have added site-level switch configurations for the switch's site, can these configurations be automatically pushed to the switch during switch onboarding. For more information, see Applying Site Configurations.

PicOS License Installation and Extending

For a PicOS switch being onboarded to AmpCon-Campus, if the switch has a PicOS license installed and the license is expired or expiring (will expire within 30 days), AmpCon-Campus will try to extend the PicOS license on the switch. If the switch has no PicOS license installed, AmpCon-Campus will try to install a PicOS license on the switch.

- If the **Global** license portal is **not** configured, AmpCon-Campus cannot install or extend a PicOS license on the switch.
- If the **Global** license portal **cannot** be accessed by AmpCon-Campus, AmpCon-Campus checks whether a local PicOS license for the switch is added to AmpCon-Campus. If yes, AmpCon-Campus installs or extends the license on the switch.
- If the **Global** license portal is configured correctly and can be accessed by AmpCon-Campus, AmpCon-Campus checks whether the switch has a PicOS license assigned in the license portal. If yes, AmpCon-Campus installs or extends the PicOS license on the switch.
- If the **Global** license portal **can** be accessed by AmpCon-Campus but no PicOS license is assigned to the switch in the license portal, AmpCon-Campus checks whether a local PicOS license for the switch is added to AmpCon-Campus. If yes, AmpCon-Campus installs the license on the switch.
- If no PicOS license is assigned to the switch in the license portal and no local PicOS license is added to AmpCon-Campus, AmpCon-Campus checks whether the license portal has available PicOS license quotas. If yes, a PicOS license is automatically assigned to the switch and installed on the switch. If not, the switch will be onboarded to AmpCon-Campus without a PicOS license installed.

For more information about PicOS licenses, see Managing PicOS Licenses.

Configuring a DHCP Server

Zero Touch Provisioning (ZTP) in AmpCon-Campus relies on DHCP. Before onboarding PicOS switches through the **Adopting Switches** or **Importing Switches by SN** method, you must configure the DHCP server as follows:

Procedure

1. Deploy a DHCP server on a Linux host.
2. Add configurations to the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server.

- For white-box PicOS switches, add the following configurations for each PicOS switch to be onboarded:

```
host 4610_54t_02 {
hardware ethernet C4:39:3A:FF:2C:C0;
fixed-address 10.10.51.198;
option default-url "http://10.56.20.15/ampcon/southbound/ztp/download_onie_start_script";
}
```

Replace “C4:39:3A:FF:2C:C0” with the MAC address of the PicOS switch.

Replace “10.10.51.198” with the IP address of each PicOS switch. The IP address is used as the DHCP IP address of the PicOS switch.

Replace “10.56.20.15” with the IP address of AmpCon-Campus.

> **NOTE**
>
> The following DHCP option is used:
>
> Option default-url: 114

- For integrated hardware and software PicOS switches, add the following configurations for each PicOS switch to be onboarded:

```
host S5860-20Q-9-8 {
hardware ethernet 64:9d:99:d2:56:54;
fixed-address 10.10.51.4;
option bootfile-name "system_ztp_start.sh";
option tftp-server-name "10.56.20.180";
}
```

Replace “64:9d:99:d2:56:54” with the MAC address of the PicOS switch.

Replace “10.10.51.4” with the IP address of the PicOS switch. The IP address is used as the DHCP IP address of the PicOS switch.

Replace “10.56.20.180” with the IP address of AmpCon-Campus.

> **NOTE**
>
> The following DHCP options are used：
>
> - Option bootfile-name: 67
> - Option tftp-server-name: 66

3. After the DHCP configurations are added, reboot the PicOS switches to be onboarded. Otherwise, the ZTP will fail.

Onboarding FSOS Switches

You can onboard FSOS switches by importing these switches to AmpCon-Campus.

Once onboarded, these FSOS switches cannot be managed by AmpCon-Campus. You can only monitor them as described in Monitoring - FSOS Switches.

Prerequisites
Importing a Single FSOS Switch
Importing FSOS Switches in Batches
Checking Import Results

Prerequisites

Before importing FSOS switches, ensure that the following prerequisites are met:

Table 1. Prerequisite Tasks and Links

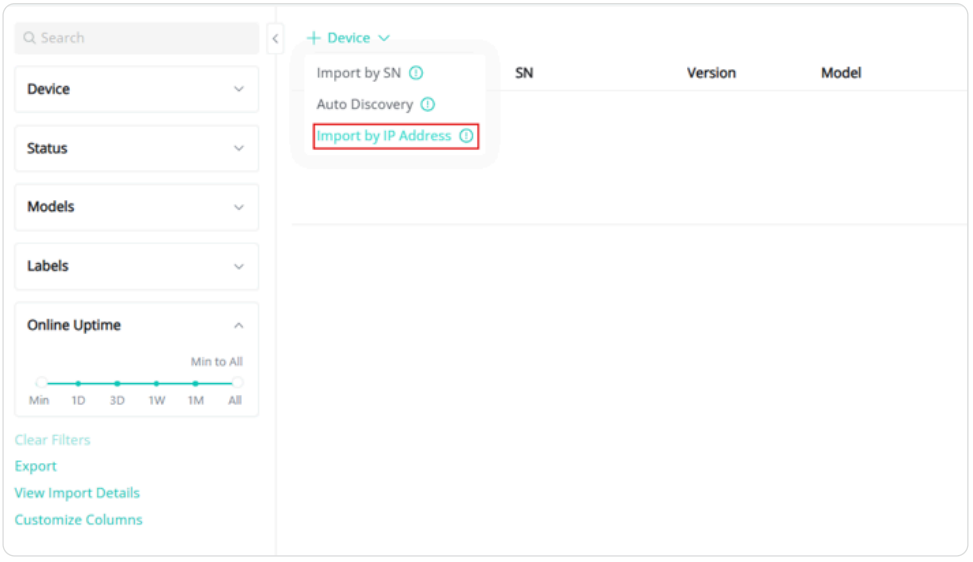
Category	Task	Reference Link
Switch Requirement	Ensure that AmpCon-Campus supports the FSOS switches.	• Supported FSOS Switches for 3.0.0
	Ensure that you have enabled SNMP and configured SNMP authentication on the FSOS switches.	• No Reference Link
	The OIDs (Sysname, Serial Number, Model, System Description, MAC Address, and Version) are not blocked on the switch. These OIDs must be accessible for the SNMP View feature.	• No Reference Link
Network Requirement	Ensure that the switches are up and able to connect to AmpCon-Campus. No network timeout issues occur due to unreachable IP addresses, disabled SNMP services, firewall blockages, or Access Control List (ACL) restrictions.	• No Reference Link

Importing a Single FSOS Switch

To import a single FSOS switch, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the FSOS switch belongs.

2. Click the **Devices** icon from the navigation bar. On the “Devices” page, hover over **+ Device**, and then click **Import by IP Address**.



3. In the pop-up window, click the **FSOS Switch** tab, and then input the following information:

> **NOTE**
>
> Ensure that the entered SNMP authentication information matches the configurations on the target switch. Otherwise, the import will fail.

- If the switch to be imported has SNMP v1 or SNMP v2c enabled, input the following information, and then click **Apply**.

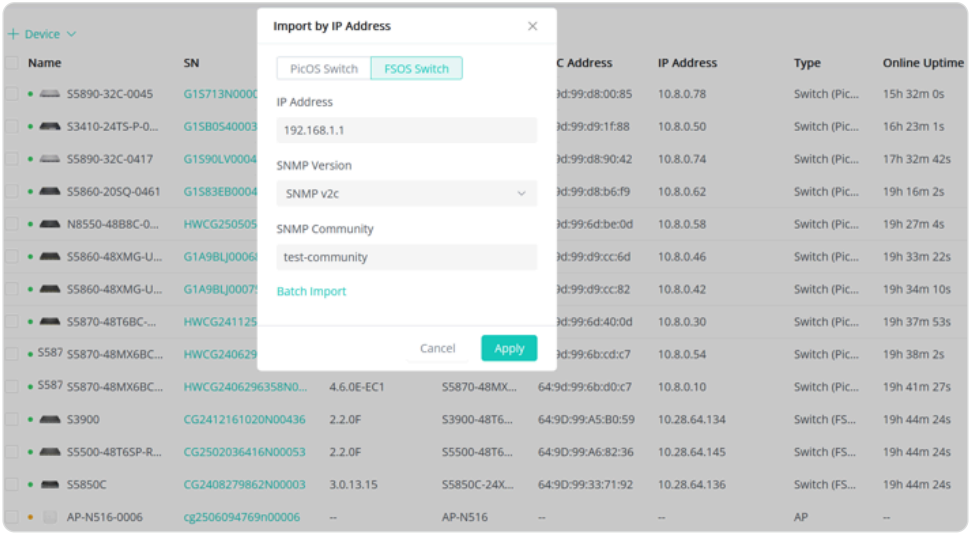


Table 2. SNMP v1 or SNMP v2c Parameters

Parameter	Description
IP Address	The IPv4 address of the switch. **NOTE**

	Ensure that the IPv4 address can be reached by AmpCon-Campus and the corresponding switch has not been onboarded to AmpCon-Campus. Otherwise, the import will fail.
SNMP Version	The version of SNMP. Select **SNMP v1** or **SNMP v2c**.
SNMP Community	The SNMP community string, which is a secret for SNMP authentication. The value can contain at most 255 characters.

- If the switch to be imported has SNMP v3 enabled, input the following information, and then click **Apply**.

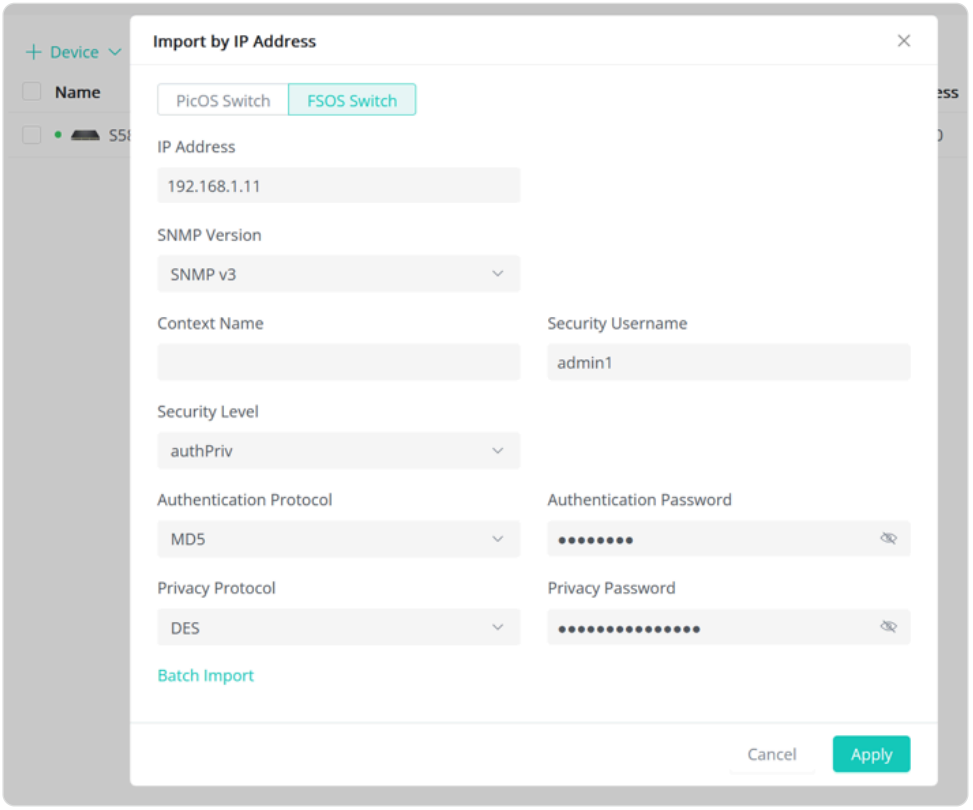


Table 3. SNMP v3 Parameters

Parameter	Description
IP Address	The IPv4 address of the switch. **NOTE** Ensure that the IPv4 address can be reached by AmpCon-Campus and the corresponding

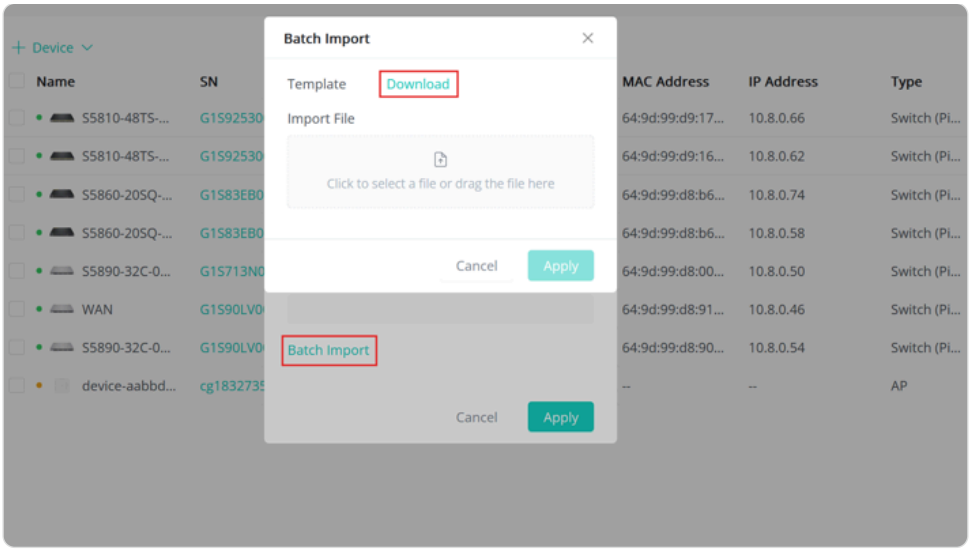
	switch has not been onboarded to AmpCon-Campus. Otherwise, the import will fail.
SNMP Version	The version of SNMP. Select **SNMP v3**.
Context Name	Optional. The string identifier used in SNMP v3 to distinguish items on an SNMP subnet. The value can contain at most 255 characters.
Security Username	The configured user who authenticates the communication identity between the SNMP management station (NMS) and the SNMP agent to prevent unauthorized access. The value can contain at most 32 characters and can contain only the following characters: • **Letters:** A-Z, a-z • **Digits:** 0-9 • **ASCII punctuation and symbols:** ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~` Spaces, tabs, line breaks, Chinese characters, full-width characters, and emojis are not allowed.
Security Level	Determines whether authentication and privacy protocols are enforced, providing granular control over data integrity and confidentiality. The following security levels are supported: • **noAuthNoPriv:** No authentication and no privacy protocols are used. • **authNoPriv:** An authentication protocol is used, but no privacy protocol is used. • **authPriv:** Both authentication and privacy protocols are used.
Authentication Protocol	The authentication protocol used for SNMP v3 agent checks. Values are **MD5**, **SHA**, and **SHA-256.** **NOTE**

	This field is required only when you select **authNoPriv** or **authPriv** in the **Security Level** drop-down list.
Authentication Password	The authentication passphrase used for SNMP v3 agent checks. The value can contain at most 255 characters. **NOTE** This field is required only when you select **authNoPriv** or **authPriv** in the **Security Level** drop-down list.
Privacy Protocol	The privacy protocol used for SNMP v3 agent checks. Values are **DES**, **AES-128**, and **AES-256.** **NOTE** This field is required only when you select **authPriv** in the **Security Level** drop-down list.
Privacy Password	The privacy passphrase used for SNMP v3 agent checks. The value can contain at most 255 characters. **NOTE** This field is required only when you select **authPriv** in the **Security Level** drop-down list.

Importing FSOS Switches in Batches

To import multiple FSOS switches in batches, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the FSOS switches belong.
2. On the “Devices” page, hover over **+ Device**, and then click **Import by IP Address**.
3. In the pop-up window, click the **FSOS Switch** tab, and then click **Batch Import**.
4. In the new pop-up window, click **Download** to download the template file.



5. Open the template file, and then enter the following information.

> **NOTEs**
>
> - Ensure that the entered SNMP authentication information matches the configurations on each target switch. Otherwise, the import will fail.
> - Enter **v1**, **v2c**, or **v3** as the **snmpVersion** value.The requirements of the parameters in the template file are almost the same as described in **Table 2. SNMP v1 or SNMP v2c Parameters** and **Table 3. SNMP v3 Parameters**.
> - Each template supports up to 500 FSOS switch entries.

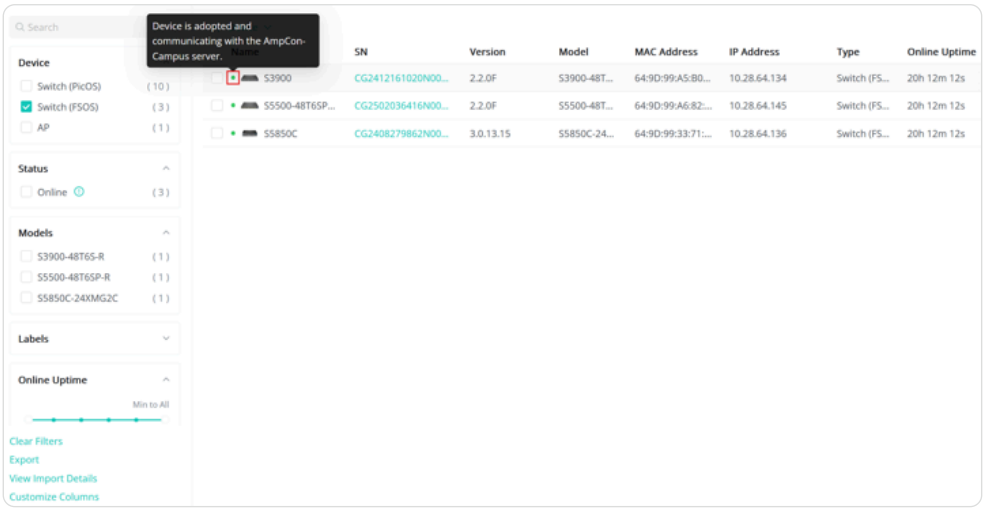
```
[
  {
    "description": "Example for SNMP v1 - all fields are required",
    "ip": "192.168.1.1",
    "snmpVersion": "v1",
    "community": "public"
  },
  {
    "description": "Example for SNMP v2c - all fields are required",
    "ip": "192.168.1.2",
    "snmpVersion": "v2c",
    "community": "public"
  },
  {
    "description": "Example for SNMP v3 with securityLevel 'noAuthNoPriv' - contextName is optional. If the device does not require a specific SNMP context, use an empty string (do not use spaces).",
    "ip": "192.168.1.3",
    "snmpVersion": "v3",
    "contextName": "",
    "securityUser": "user1",
    "securityLevel": "noAuthNoPriv"
  },
  {
    "description": "Example for SNMP v3 with securityLevel 'authNoPriv' - contextName is optional. If the device does not require a specific SNMP context, use an empty string (do not use spaces).",
    "ip": "192.168.1.4",
    "snmpVersion": "v3",
    "contextName": "",
    "securityUser": "user2",
    "securityLevel": "authNoPriv",
    "authProtocol": "MD5",
    "authPassword": "AuthPass123"
  },
  {
    "description": "Example for SNMP v3 with securityLevel 'authPriv' - contextName is optional. If the device does not require a specific SNMP context, use an empty string (do not use spaces).",
    "ip": "192.168.1.5",
    "snmpVersion": "v3",
    "contextName": "",
    "securityUser": "user3",
    "securityLevel": "authPriv",
    "authProtocol": "SHA",
    "authPassword": "AuthPass456",
    "privProtocol": "AES-128",
    "privPassword": "PrivPass789"
  }
]
```

6. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. Then, click **Apply**.

Checking Import Results

1. On the “Devices” page, check whether the switches are listed in the device list and whether the status circle of each switch is in green.

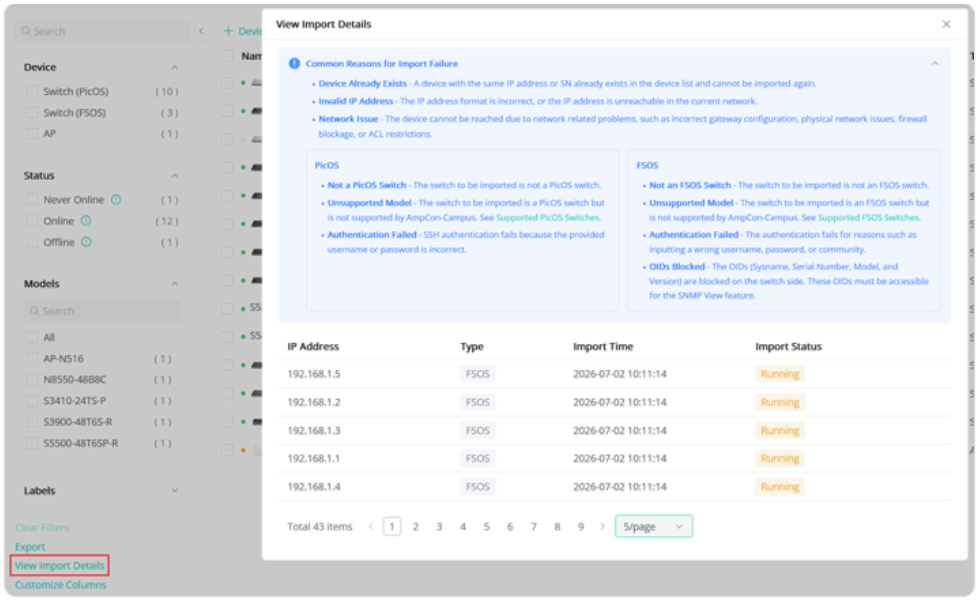
   Hover over the status circle, and then you can see the switch import status.



> **Tip**
>
> Different circle colors indicate different statuses:
>
> - **Green:** The switch is in **Online** status, which means the switch is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus.
> - **Grey:** The switch is in **Offline** status, which means the switch is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus.

2. On the “Devices” page, click **View Import Details**. In the pop-up window, locate the FSOS switches, and then check whether the import status is **Successful**.

   If the import fails, see Device Onboarding Troubleshooting for possible reasons.


Search
Device
Switch (PicOS) (10)
Switch (FSOS) (3)
AP (1)
Status
Never Online (1)
Online (12)
Offline (1)
Models
Search
All
AP-N516 (1)
NI8550-48B8C (1)
S3410-24TS-P (1)
S3900-48T6S-R (1)
S5500-48T6SP-R (1)
Labels
Clear Filters
Export
View Import Details
Customize Columns
View Import Details
Common Reasons for Import Failure
Device Already Exists - A device with the same IP address or SN already exists in the device list and cannot be imported again.
Invalid IP Address - The IP address format is incorrect, or the IP address is unreachable in the current network.
Network Issue - The device cannot be reached due to network related problems, such as incorrect gateway configuration, physical network issues, firewall blockage, or ACL restrictions.
PicOS
Not a PicOS Switch - The switch to be imported is not a PicOS switch.
Unsupported Model - The switch to be imported is a PicOS switch but is not supported by AmpCon-Campus. See Supported PicOS Switches.
Authentication Failed - SSH authentication fails because the provided username or password is incorrect.
FSOS
Not an FSOS Switch - The switch to be imported is not an FSOS switch.
Unsupported Model - The switch to be imported is an FSOS switch but is not supported by AmpCon-Campus. See Supported FSOS Switches.
Authentication Failed - The authentication fails for reasons such as inputting a wrong username, password, or community.
OIDs Blocked - The OIDs (Sysname, Serial Number, Model, and Version) are blocked on the switch side. These OIDs must be accessible for the SNMP View feature.
IP Address
Type
Import Time
Import Status
192.168.1.5 FSOS 2026-07-02 10:11:14 Running
192.168.1.2 FSOS 2026-07-02 10:11:14 Running
192.168.1.3 FSOS 2026-07-02 10:11:14 Running
192.168.1.1 FSOS 2026-07-02 10:11:14 Running
192.168.1.4 FSOS 2026-07-02 10:11:14 Running
Total 43 items
1 2 3 4 5 6 7 8 9
5/page

Onboarding APs

To deploy a wireless network, you need to onboard access points (APs) to AmpCon-Campus first.

Onboarding APs means bringing APs under the management of AmpCon-Campus. Once onboarded, APs can be managed by AmpCon-Campus.

- Guidelines
- Prerequisites
- Adopting APs
- Importing APs by SN
  - Importing a Single AP
  - Importing APs in Batches

Guidelines

To onboard APs, use one of the following two methods:

Table 1. AP Onboarding Methods

Method	Description
Adopting APs	After you pre-configure the IP address of AmpCon-Campus as described in the Prerequisites section, AmpCon-Campus can discover APs automatically and add them to the auto-discovery list. You can adopt the APs in the auto-discovery list directly.
Importing APs by SN	If you have the serial number (SN) list of the APs, you can import the APs by SN.

Adopting APs and **Importing APs by SN** are Zero Touch Provisioning (ZTP) methods. For the ZTP workflow, see AP ZTP Workflow.

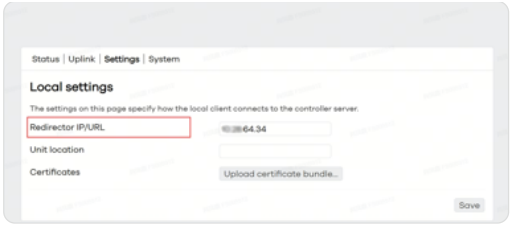
> **NOTE**
>
> During AP onboarding, if you have added site-level wireless configurations for the APs' site, these wireless configurations will be automatically pushed to the APs. For more information, see Configuring Wireless Networks.

Prerequisites

Before onboarding APs, ensure that the following prerequisites are met:

Table 2. Prerequisite Tasks and Links

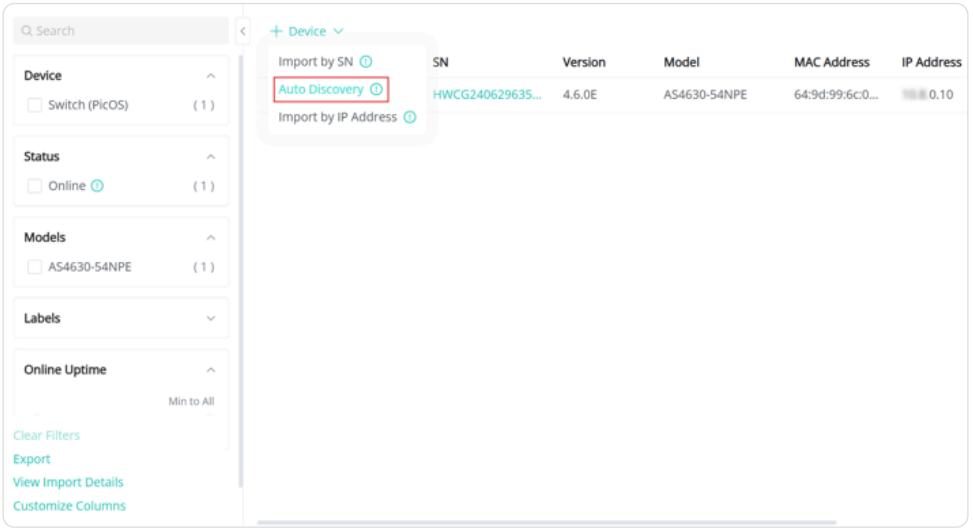
Category	Task	Reference Link
Site Requirement	Prepare an existing site for the APs, or add a new site as needed.	• Managing Sites
AP Requirement	Ensure that the APs are supported by AmpCon-Campus.	• Supported APs for 3.0.0
IP Address Requirement	Ensure that a reachable DHCP server is available on the upstream network of the APs. Configure the DHCP server to reserve an IP range for the APs.	• No Reference Link
	Pre-configure the IP address of AmpCon-Campus by using one of the following ways: • On the DHCP server, configure DHCP Option 138 as the IP address of AmpCon-Campus. See the following DHCP Option 138 configuration example:  • Connect to the **Pica8-WiFi** SSID (each AP broadcasts the **Pica8-WiFi** SSID), and then enter **10.254.254.1** in a web browser to access the AP configuration page. In the **Redirector IP/URL** field, enter the IP address of AmpCon-Campus as shown in the following screenshot, and then click **Save** to save the configuration. If an AP does not broadcast the **Pica8-WiFi** SSID, reset the AP to factory defaults first.	• No Reference Link

		
Network Requirement	Plug in and power on the APs. Ensure that the APs are able to connect to AmpCon-Campus and the DHCP server. Ensure that the APs are connected to wired networks. **NOTE** In the mesh network scenario, ensure that the mesh root AP is connected to a wired network. Mesh child APs are not required to connect to wired networks. To deploy a mesh network, refer to the workflow described in Mesh Network Scenario.	• No Reference Link

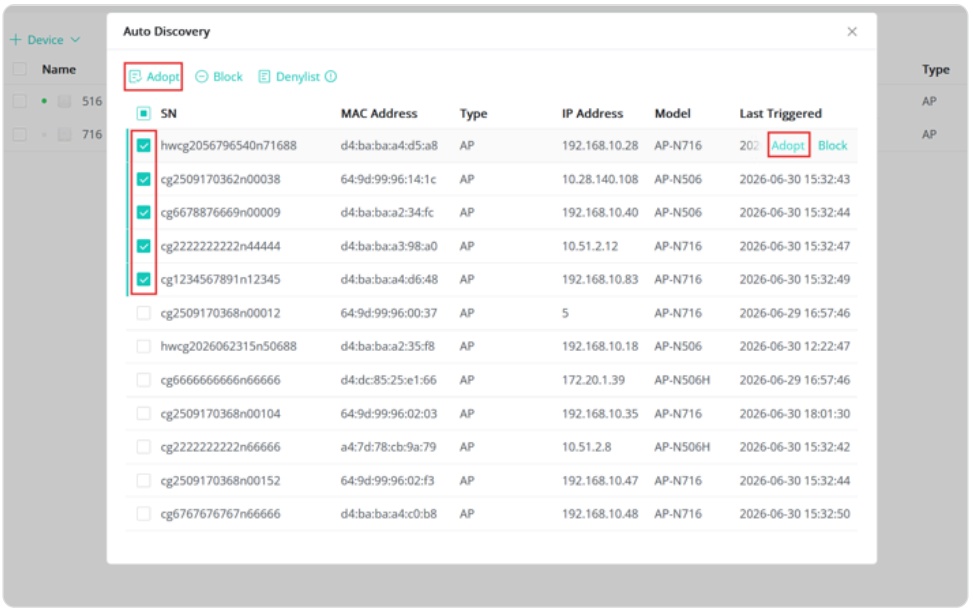
Adopting APs

To adopt the APs in the auto-discovery list, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, hover over **+ Device**, and then click **Auto Discovery**.



4. In the pop-up window, adopt APs as follows:



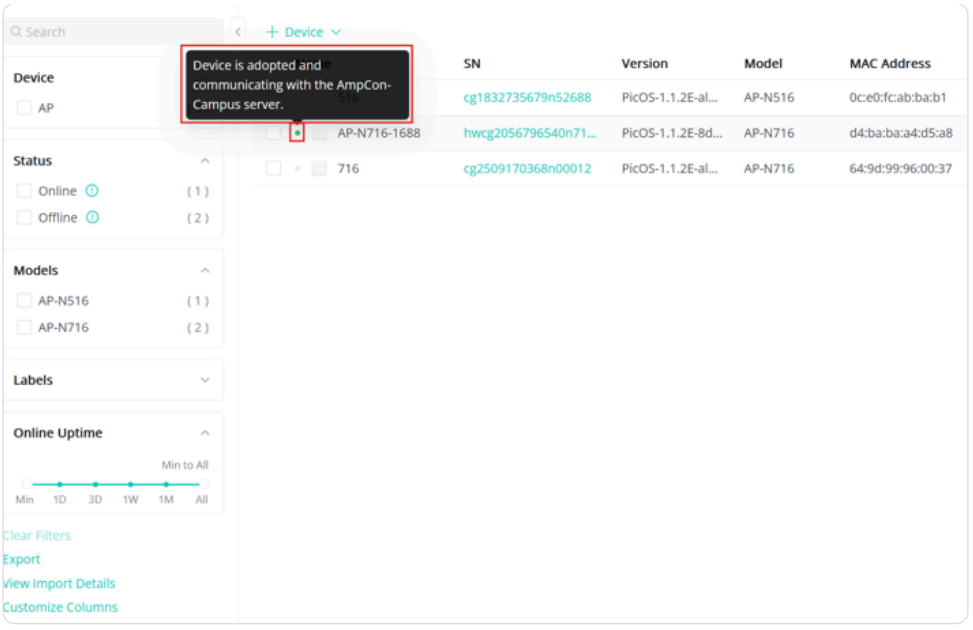
- To adopt multiple APs, select the APs, and then click **Adopt** at the top.
- To adopt an AP, hover over the AP, and then click **Adopt** on the right.

> **Tips**
>
> - The **Last Triggered** column displays the last time AmpCon-Campus received a registration request from the AP.
> - To avoid onboarding some APs, block these APs. The blocked APs will be removed from the auto-discovery list and added to the denylist.
>   - To block multiple APs, select the APs, and then click **Block** at the top.
>   - To block an AP, hover over the AP, and then click **Block** on the right.
> - Click **Denylist**. In the pop-up window, you can see all the blocked APs, and you can unblock APs when needed.
>   - To unblock multiple APs, select the APs, and then click **Unblock** at the top.
>   - To unblock an AP, hover over the AP, and then click **Unblock** on the right.

5. Check whether the APs are added to the device list. Then, check the **Name** column to see whether the status circle of each AP is in green.

   Hover over the status circle, and then you can see the AP adoption status.

   If the adoption fails, see Device Onboarding Troubleshooting for possible reasons.



Different circle colors indicate different statuses:

Table 3. Color Meanings

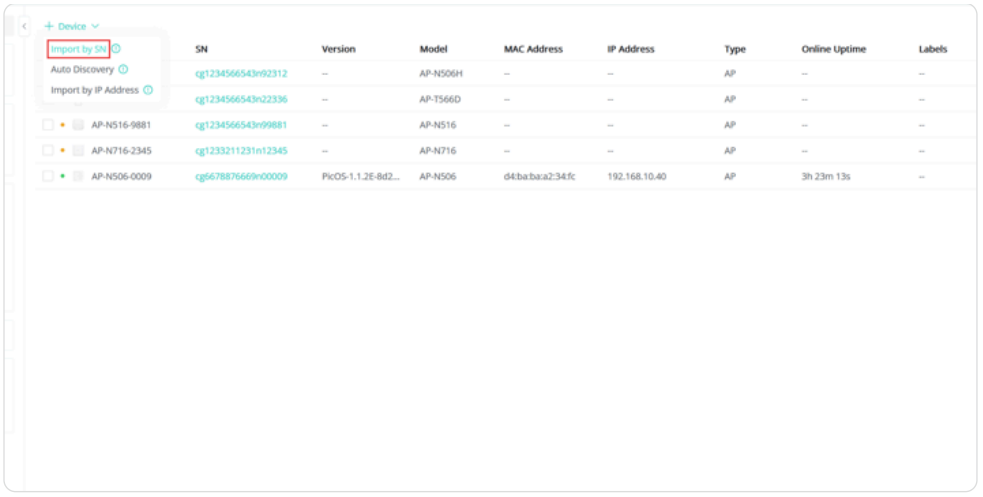
Color	Description
Green	The AP is in **Online** status, which means the AP is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus.
Gray	The AP is in **Offline** status, which means the AP is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus.
Yellow	The AP is in **Never Online** status, which means the AP has been added to AmpCon-Campus but has never connected to AmpCon-Campus.

Importing APs by SN

Importing a Single AP

To import a single AP, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, hover over **+ Device**, and then click **Import by SN**.



4. In the pop-up window, input the following information, and then click **Apply**.

   The **Site** value is always the site name selected in **Step 1** and cannot be modified.

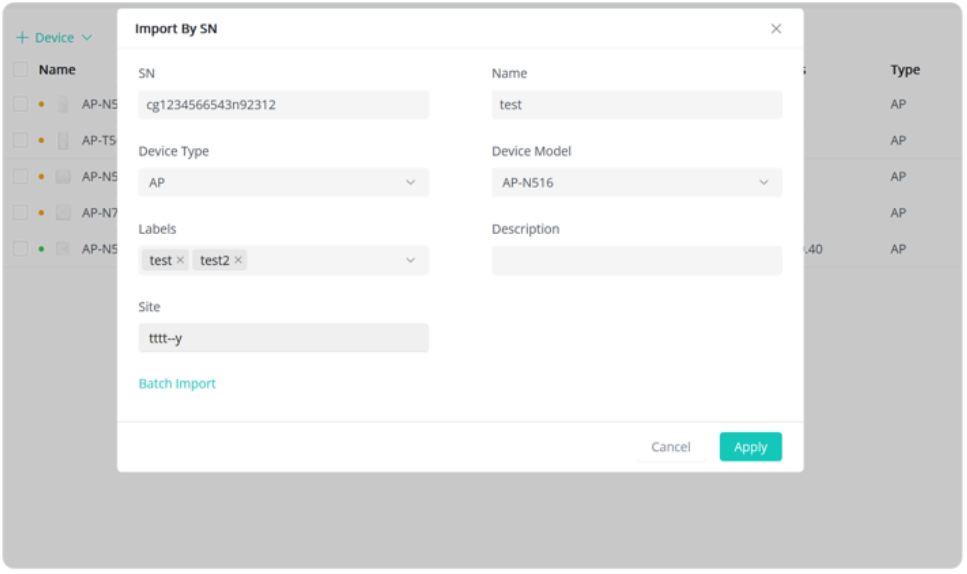


Table 4. AP Parameters

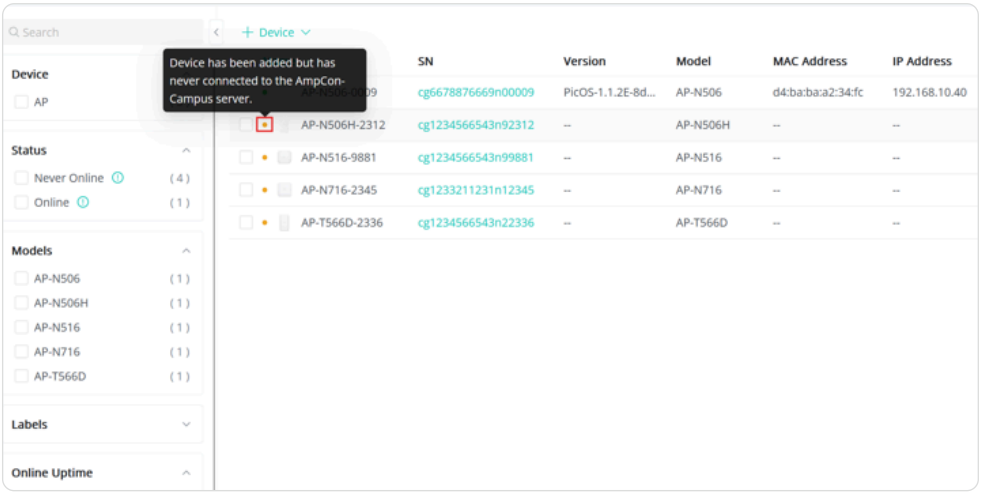
Parameter	Description
SN	The SN of the AP.
Name	Optional. The AP alias, used to differentiate the AP in the AmpCon-Campus UI and will not be pushed to the AP side. The alias can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The alias cannot start or end with a hyphen or underscore. If you do not enter the alias, AmpCon-Campus automatically generates an alias for each device. The

	alias contains the device model and the last four digits of the AP serial number (SN).
Device Type	Select **AP**.
Device Model	The model of the AP.
Labels	Optional. The AP labels used for AP filtering and management. AP labels can also be used in applying SSIDs. For more information, see General Configurations. You can select one or multiple labels. To add a new label, click the **Labels** drop-down list, and then click **Create Label**. Each label can contain only letters and numbers and can contain at most 64 characters.
Description	Optional. The description of the AP. The description can contain at most 256 characters.

5. Check whether the AP is listed in the device list and whether the status circle of the AP is in green. For the meaning of each color, see **Table 3. Color Meanings**.

   Hover over the status circle, and then you can see the AP import status.

   If the import fails, see Device Onboarding Troubleshooting for possible reasons.

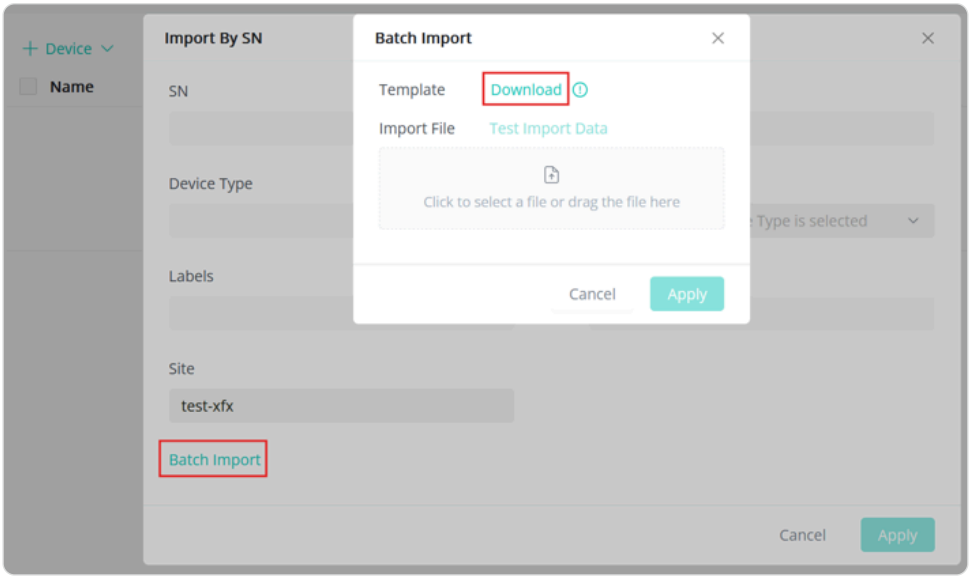


Importing APs in Batches

To import multiple APs in batches, follow these steps:

1. On the “Devices” page, hover over **+ Device**, and then click **Import by SN**.

2. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.

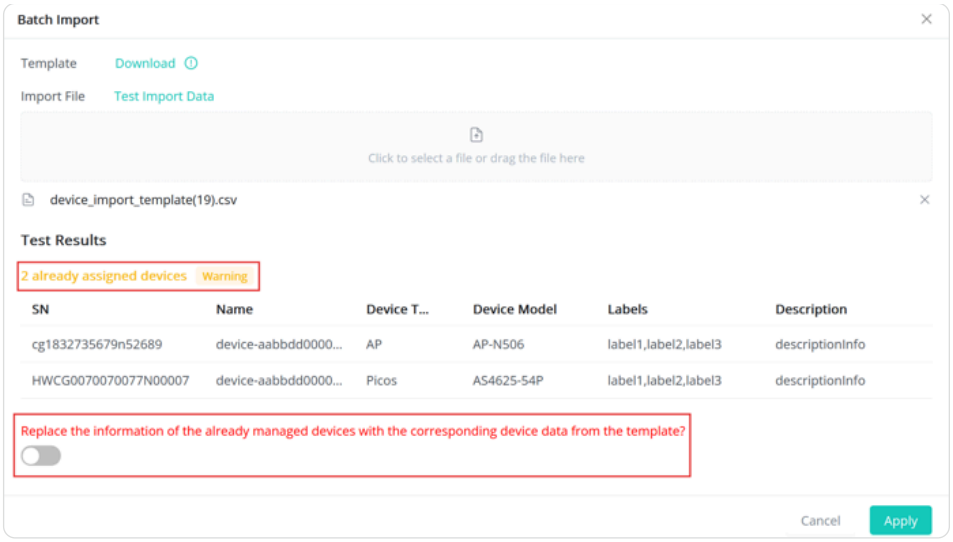


3. Open the template file, and then enter correct information in the **SN**, **DeviceType**, **DeviceModel**, **Name**, **Labels**, and **Description** columns for each AP to be imported.

> **NOTEs**
>
> - The requirements of these columns are almost the same as described in **Table 4. AP Parameters**.
> - Enter **AP** in the **DeviceType** column.
> - To add multiple labels in the **Labels** column, use **$** as the separator. For example, **label1$label2$label3**.

4. In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. The maximum file size is 5 MB.
5. Optional: Click **Test Import Data**. In the new pop-up window, check the test result.

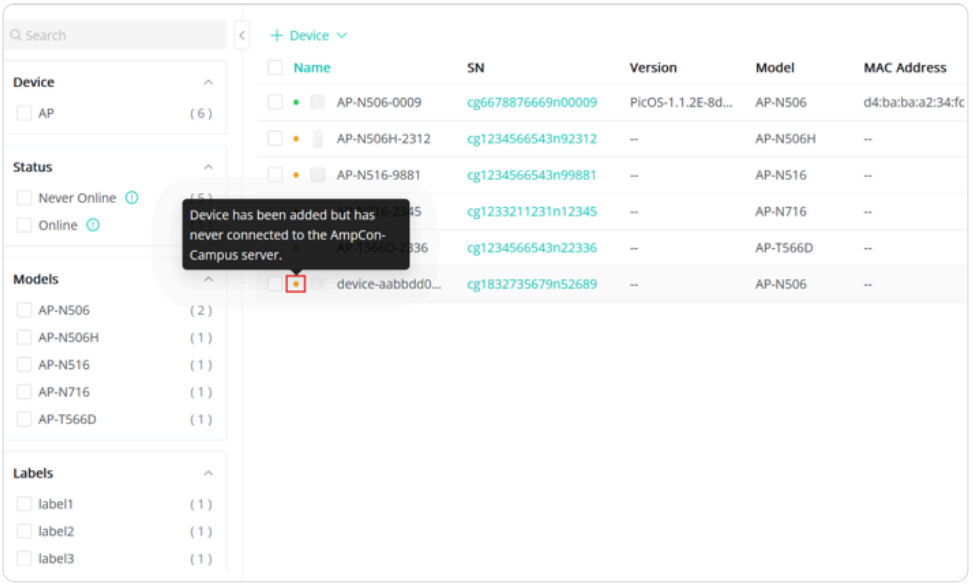
> **NOTEs**
>
> - If you see problematic devices in the test result, check the warning message, resolve the issues in the template file, and then upload the template file again.
> - If an AP has been listed in the device list of the current site, you can see the warning message.
>
> You can click the toggle to replace the device information in the list with the corresponding device data from the template. If you don't need the replacement, leave the toggle off.



6. Click **Apply**. Then, check whether the APs are listed in the device list and whether the status circle of each AP is in green. For the meaning of each color, see **Table 3. Color Meanings**.

   Hover over the status circle, and then you can see the AP import status.

   If the import fails, see Device Onboarding Troubleshooting for possible reasons.



Configuring PicOS Switches

After you onboard PicOS switches, you can use different methods to configure these switches, minimizing errors and simplifying configuration processes.

See the following child topics:

- Applying Site Configurations
- Applying Quick Configurations
- Applying Port Configurations
- Configuring a Single Switch
- Applying Template Configurations
- Checking Configuration Results
- Comparing Switch Configurations
- End-to-End Campus Deployment Scenario

NOTEs

- Ensure that AmpCon-Campus can reach and authenticate against managed PicOS switches over SSH. The **SSH Username** and **SSH Password** must exactly match the credentials configured on the switches. Otherwise, configuration delivery and other device-management operations will fail. For more information, see Device Credential Configurations.

  If AmpCon-Campus can access and manage a PicOS switch through a specific **SSH Username** and **SSH Password**, it's not recommended to modify the **SSH Username** and **SSH Password**.
- Use AmpCon-Campus as the primary management interface for switch configurations. **Do not** configure the same objects directly through the switch CLI, because device-side changes might cause configuration conflicts or drift, resulting in failures for subsequent configuration pushes.
  If a required configuration is not supported by AmpCon-Campus, contact support engineers before configuring it through the switch CLI. After making an approved switch-side change, review its dependencies and align the switch's running configuration with AmpCon-Campus's configuration database before the next configuration push.

Applying Site Configurations

You can add site-level switch configurations for a site. Then, managed PicOS switches in the site can be automatically configured.

After you move a PicOS switch to another site or onboard a PicOS switch to a site, if the site has site-level switch configurations, the configurations will be automatically pushed to the switch.

Guidelines
Prerequisites
Procedure

Guidelines

- All the following configurations on the “Site Configuration” page are optional. Add only the configurations that you need.
- After you configure networks in the **Network** section, the configurations are not pushed to PicOS switches. Network-related configurations are pushed to PicOS switches only when you apply port configurations or quick configurations referencing the added networks.

  After you modify system configurations in the **System** section and click **Apply**, the site-level system configurations will be directly pushed to associated switches.
- AmpCon-Campus applies system configurations only to PicOS switches that meet all the following requirements:
  - The switches have been successfully onboarded to AmpCon-Campus and belong to the configured site.
  - No configurations are being or waiting to be pushed to the switches.
  - No upgrade tasks are running on the switches.
- After system configurations are applied to managed PicOS switches or PicOS switches newly moved to this site, you can see configuration results on the “Configuration Result” page.

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the configuration will fail.

Table 1. Prerequisites

Prerequisite	Reference Link
Onboard PicOS switches to bring them under AmpCon-Campus management.	• Onboarding PicOS Switches

Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List

Procedure

To add site-level switch configurations, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches to be configured belong.
2. Click the **Settings** icon from the navigation bar, and then click **Site Configuration** in the **Switch** section of the sidebar.
3. In the **Network** section, add one or multiple networks by clicking **Create Network**. In the pop-up window, enter the following information, and then click **Apply**.

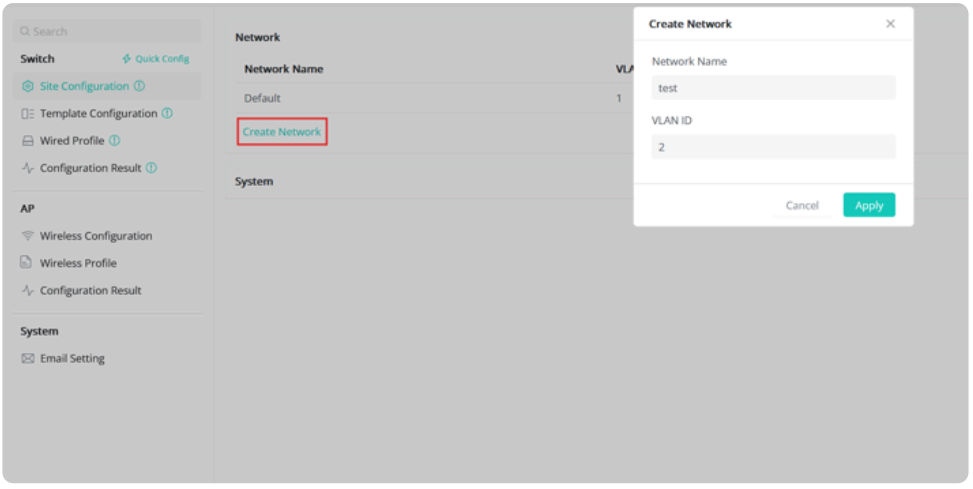


Table 2. Network Parameters

Parameter	Description
Network Name	The name of the Layer 3 VLAN interface. The value needs to be unique and can contain at most 11 characters. The value can contain only letters, numbers, and supported special characters (- . _ @ = #).
VLAN ID	The VLAN identifier. The VLAN ID needs to be unique. The value must range from 2 to 4094.

Tips

- A network is a named VLAN ID. The network named **Default** is a built-in network.

- After adding a network, you can edit or delete it:
  - To edit a network, hover over the network, and then click **Edit**.
  - To delete a network, hover over the network, and then click **Delete**.
- The following networks can't be edited or deleted:
  - The built-in network named **Default**.
  - The networks referenced by port profiles, port configurations, quick configurations, or L3 interface and DHCP configurations in the **Setting** tab of the "Device" page.

4. In the **System** section, add system-related configurations as follows:

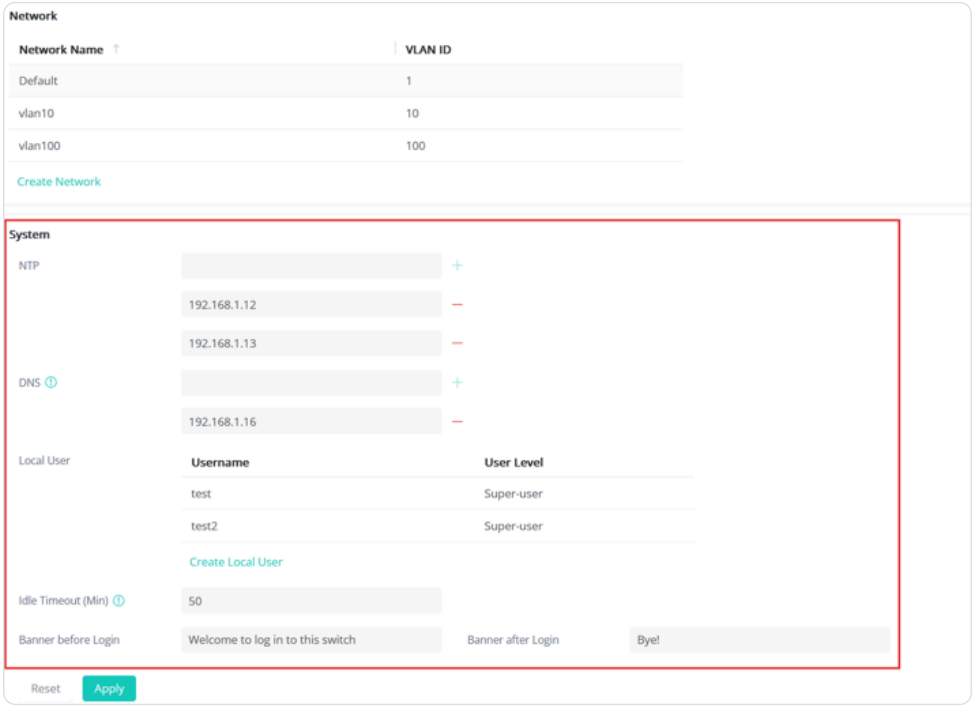


Table 3. System Configurations

Configuration	Description
NTP	The IPv4 addresses of NTP servers. You can add at most 6 NTP servers. To add multiple NTP servers, click **+**. To remove a NTP server, click **-**. After adding an NTP server, you cannot edit it. **NOTEs** • Network Time Protocol (NTP) is used to synchronize the clocks of the switch and

	other hardware devices on the Internet. • NTP server IP addresses cannot be within the following address ranges: ◦ Link-local addresses: 169.254.0.0 to 169.254.255.255 ◦ Loopback addresses: 127.0.0.0 to 127.255.255.255 ◦ Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 ◦ Special reserved addresses: 0.0.0.0 to 0.255.255.255
DNS	The IPv4 addresses of DNS servers. You can add at most 6 DNS servers. The first added DNS server serves as the primary DNS server. To add multiple DNS servers, click **+**. To remove a DNS server, click **-**. After adding a DNS server, you cannot edit it. **NOTE** DNS server IP addresses cannot be within the following address ranges: • Link-local addresses: 169.254.0.0 to 169.254.255.255 • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 • Special reserved addresses: 0.0.0.0 to 0.255.255.255
Local User	The local user accounts used to log in to the PicOS switches. Click **Create Local User** to add local user accounts. In the pop-up window, input the following information, and then click **Apply**. • **Username:** The name of the user.

	The username must start with a lowercase letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $.
	
	The username can contain at most 32 characters. The username cannot be **admin** (case-insensitive).
	
	• **User Level:** The permission level of the user. The value can be **Super User** or **Readonly**.
	  ◦ **Readonly:** Gives read-only permissions to a user.
	  ◦ **Super User:** Gives all permissions to a user.
	• **Password:** The password for the user.
	
	The password can contain 6 to 64 ASCII characters. The password must contain letters, digits, and special characters (@ # $ % !).
	• **Confirm Password:** The same as the value entered in the **Password** field.
	
	NOTEs
	• You can add one or multiple local users.
	• After adding a local user, you can edit or delete it:
	  ◦ To edit a local user, hover over the user, and then click **Edit**.
	  ◦ To remove a local user, hover over the user, and then click **Delete**.

Idle Timeout	The maximum idle time in minutes before an SSH connection is automatically disconnected. The value can be 0 or an integer ranging from 40 to 20000. **NOTEs** • If the value is set to 0, the remote SSH shell session will not be automatically disconnected. • S3540, S3410, and S3270 series switches support a maximum of 60 minutes. For these switches, if the **Idle Timeout** value is set to

	an integer greater than 60, the effective value used will be 60.
Banner before Login	The login banner message that you want users to see **before** they log in to a switch. The message can contain at most 80 characters.
Banner after Login	The login banner message that you want users to see **after** they log in to a switch. The message can contain at most 80 characters. **Example:** “Warning! This switch is managed by AmpCon-Campus. Do not make any CLI changes.”

5. Click **Apply**. Then, site-level system configurations will be pushed to PicOS switches in the selected site.

> **NOTEs**
>
> - To reset the system configurations, click **Reset**.
> - You can see the **Apply** and **Reset** buttons only after you modify system configurations.

6. Click **Configuration Result** from the sidebar. On the “Configuration Result” page, verify whether site-level system configurations are applied to switches successfully.

   For more information, see Checking Configuration Results.

7. If the current site-level system configurations differ from the last successfully applied ones on some switches, click **Sync Site Config** to synchronize the current site-level system configurations to these switches. Follow these steps:

   a. In the **System** section, click **Sync Site Config**.

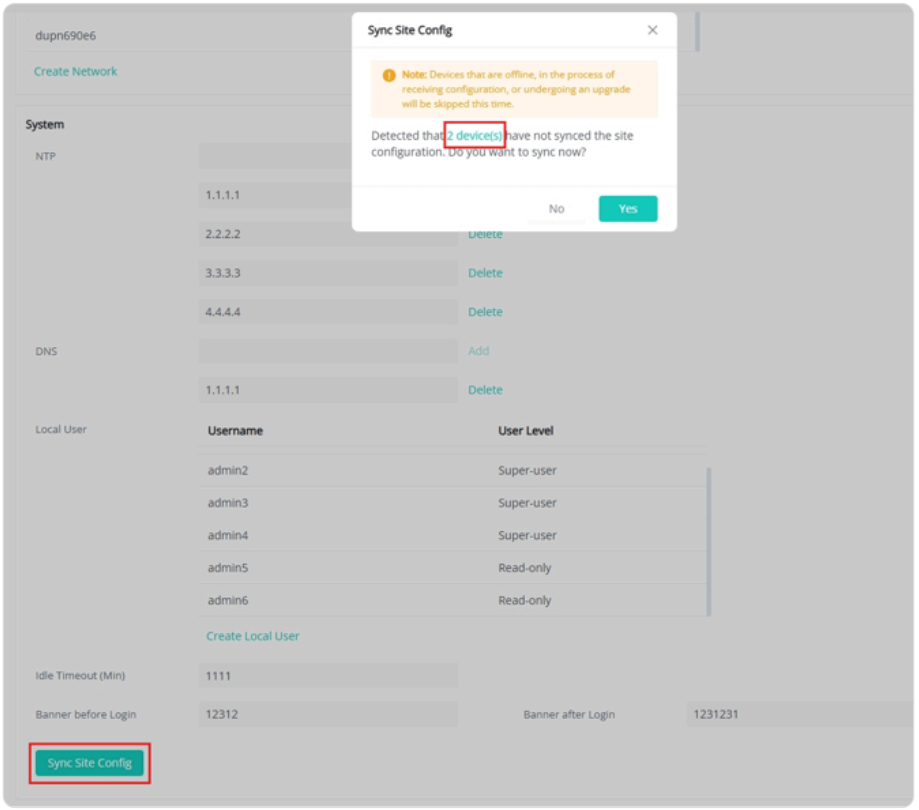
   b. In the pop-up window, check the count of switches to be synchronized, and then click **Yes**.

   You can click the switch count to view detailed switch information.

NOTE

The switches to be synchronized here meet all the following requirements:

- The switches are successfully onboarded to AmpCon-Campus.
- The switches are online and belong to the selected site.
- The current site-level system configurations differ from the last successfully applied ones on these switches.
- No configurations are being or waiting to be pushed to the switches.
- No upgrade tasks are running on the switches.



c. Click **Configuration Result** from the sidebar. On the “Configuration Result” page, verify whether site-level system configurations are applied to switches successfully.

Applying Quick Configurations

After onboarding PicOS switches, you can apply quick configurations to these switches through the **Quick Config** wizard. These configurations include Layer 3 interface, DHCP, port, static route, and OSPF configurations.

You only need to follow the step-by-step wizard and fill in the required parameters. AmpCon-Campus will then automatically apply the related configurations to associated switches.

Guidelines
Prerequisites
Procedure

Guidelines

- All the following configurations in the **Quick Config** wizard are optional. Add only the configurations that you need. AmpCon-Campus will apply only the added configurations to associated switches.
- Configurations applied through the **Quick Config** wizard are synchronized to the **Setting** tab of each associated switch and the port configurations on the “Ports” page, and vice versa.
- Each IP address that you enter in the **Quick Config** wizard must not be within the following address ranges:
  - Link-local addresses: 169.254.0.0 to 169.254.255.255
  - Loopback addresses: 127.0.0.0 to 127.255.255.255
  - Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255
  - Special reserved addresses: 0.0.0.0 to 0.255.255.255

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the configuration will fail.

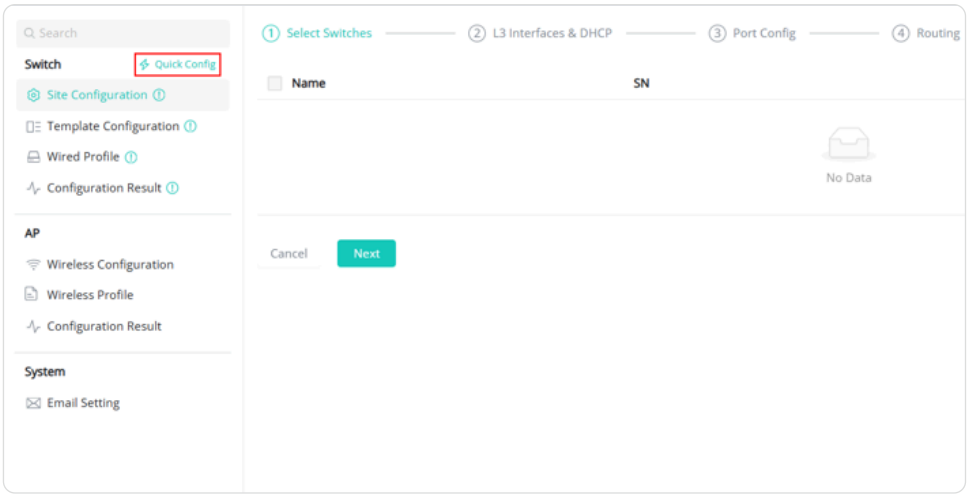
Table 1. Prerequisites

Prerequisite	Reference Link
Onboard PicOS switches to bring them under AmpCon-Campus management.	• Onboarding PicOS Switches
Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List

Procedure

1. In the AmpCon-Campus UI, select the site to which the switches to be configured belong.

2. Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar.



3. In the **Quick Config** wizard, select one or multiple switches to be configured, and then click **Next**.

> **NOTE**
>
> You can select only the PicOS switches that meet all the following conditions:
>
> - The switches are online (connected to AmpCon-Campus).
> - No configurations are being pushed to the switches.
> - No upgrade tasks are running on the switches.

4. In the **L3 Interfaces & DHCP** tab, add L3 interface and DHCP configurations as follows, and then click **Next**.

> **NOTEs**
>
> - L3 interface configurations are used to configure a VLAN interface with an IP address, enabling Layer 3 routing for devices in the VLAN.
>
>   DHCP configurations determine how IP addresses are assigned to devices in the corresponding VLAN.
> - You can add one or multiple L3 interface and DHCP configuration items for each switch.

a. Select a switch in the sidebar.

b. Click **Create L3 Interfaces & DHCP** to add an L3 interface and DHCP configuration item. You can add one or multiple L3 interface and DHCP configuration items for each switch.

c. In the pop-up window, input the following information, and then click **Save**.

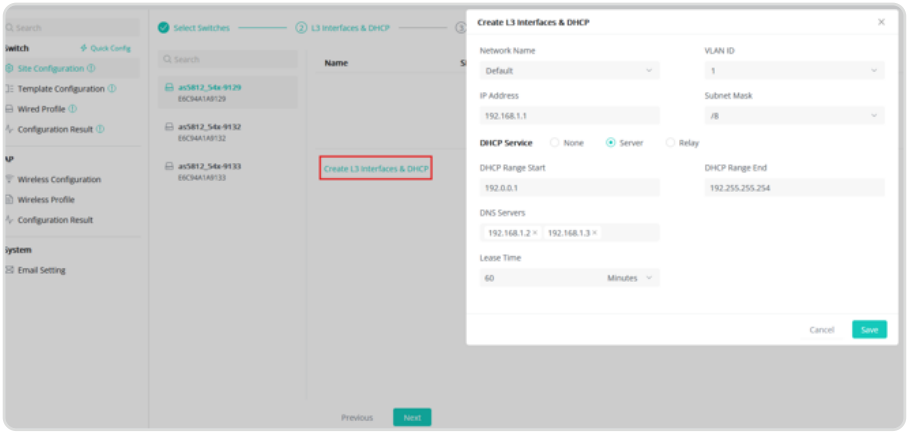


Table 2. L3 Interface and DHCP Parameters

Parameter	Description
Network Name	The name of the Layer 3 VLAN interface. You can select the built-in network named **Default** or select a network that you added in the **Network** section of the “Site Configuration” page. For more information, see Applying Site Configurations. **NOTE** Within the same site, each network can be configured with only one DHCP server or DHCP relay.
VLAN ID	The VLAN identifier. The **VLAN ID** will be automatically filled after you select the **Network Name**, and vice versa.
IP Address	The IPv4 address assigned to the Layer 3 interface. **NOTEs** • The IP address must be unique within the site. • Based on the **IP Address** and **Subnet Mask**, AmpCon-Campus automatically calculates the subnet for the Layer 3 interface. This subnet must not overlap

	with subnets of other Layer 3 interfaces on the same switch. • The **IP Address** cannot be the loopback address, the subnet network address, or the subnet broadcast address.
Subnet Mask	The subnet mask of the Layer 3 interface, such as **/24**.
DHCP Service	The DHCP mode for this subnet. The value can be **None**, **Server**, or **Relay**. • **None:** DHCP is disabled. • **Server:** The switch acts as a DHCP server. • **Relay:** The switch acts as a DHCP Relay and forwards DHCP requests to an external DHCP server. **NOTE** The **Server** option is not displayed for S3410, S3270, and S3540 switches.
DHCP Range Start	The starting IPv4 address of the DHCP address pool, which is used to assign IP addresses. **NOTEs** • This field is displayed only if you select **Server** in the **DHCP Service** section. • The **DHCP Range Start** cannot be the network address or broadcast address of the subnet. • AmpCon-Campus automatically calculates and displays the **DHCP Range Start** and **DHCP Range End** values based on the **IP Address** and **Subnet Mask**. You can modify the **DHCP Range Start** and **DHCP Range End** values as needed. • The DHCP address pool must be within the subnet of the configured L3 interface.

DHCP Range End	The ending IPv4 address of the DHCP address pool, which is used to assign IP addresses. **NOTEs** • This field is displayed only if you select **Server** in the **DHCP Service** section. • The **DHCP Range End** must be greater than the **DHCP Range Start**. • The **DHCP Range End** cannot be the network address or broadcast address of the subnet.
DNS Servers	Optional. The IPv4 addresses of DNS servers, which are used for dynamic domain name resolution. You can add at most 2 DNS servers. After you add each DNS server IP address, be sure to press **Enter**. **NOTE** This field is displayed only if you select **Server** in the **DHCP Service** section.
Lease Time	The valid lease duration of each IP address assigned by a DHCP server to a client device. You can click the drop-down arrow to select **Minutes**, **Hours**, or **Days**. • If you select **Minutes**, the value must range from 2 to 43200. • If you select **Hours**, the value must range from 1 to 720. • If you select **Days**, the value must range from 1 to 30. **NOTE** This field is displayed only if you select **Server** in the **DHCP Service** section.

Relay Server IP	The IPv4 address of the external DHCP server to which DHCP requests are forwarded. **NOTEs** • The **Relay Server IP** value cannot be the same as the **IP Address** value. • This field is displayed only if you select **Relay** in the **DHCP Service** section.

Tip

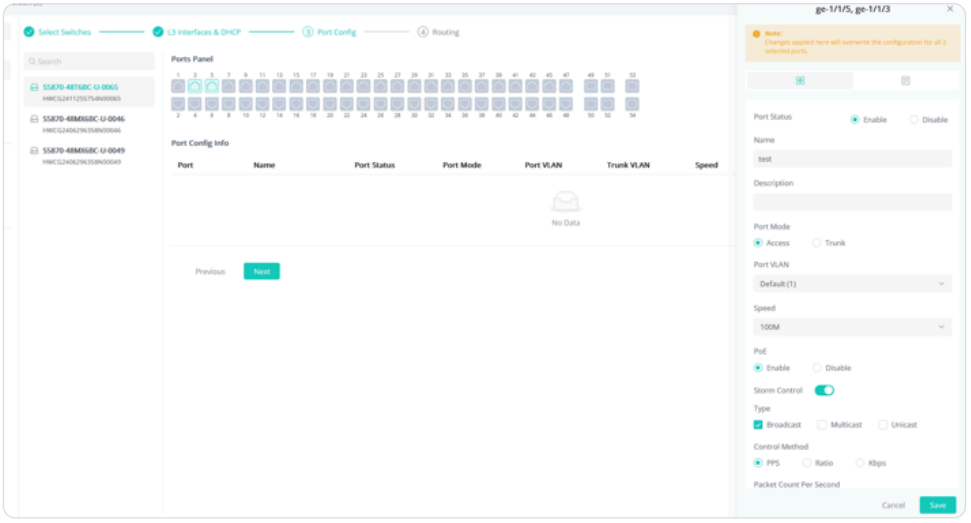
After adding an L3 interface and DHCP configuration item, you can edit or delete it:

- To delete an L3 interface and DHCP configuration item, hover over the item, and then click **Delete**.
- To edit an L3 interface and DHCP configuration item, hover over the item, and then click **Edit**.
- You cannot edit or delete an L3 interface and DHCP configuration item while it is being pushed to the switch.

d. Repeat **Step a** to **Step c** to add L3 interface and DHCP configuration items for other switches.

5. In the **Port Config** tab, configure switch ports, and then click **Next**.

   For how to configure switch ports, see Applying Port Configurations.



6. In the **Routing** section, add one or multiple static routes as follows:

   a. Select a switch in the sidebar.

b. Click **Create Static Route** to create a static route configuration item. You can add one or multiple static route configuration items for each switch.

c. In the pop-up window, specify the destination and next hop of the static route, and then click **Save**.

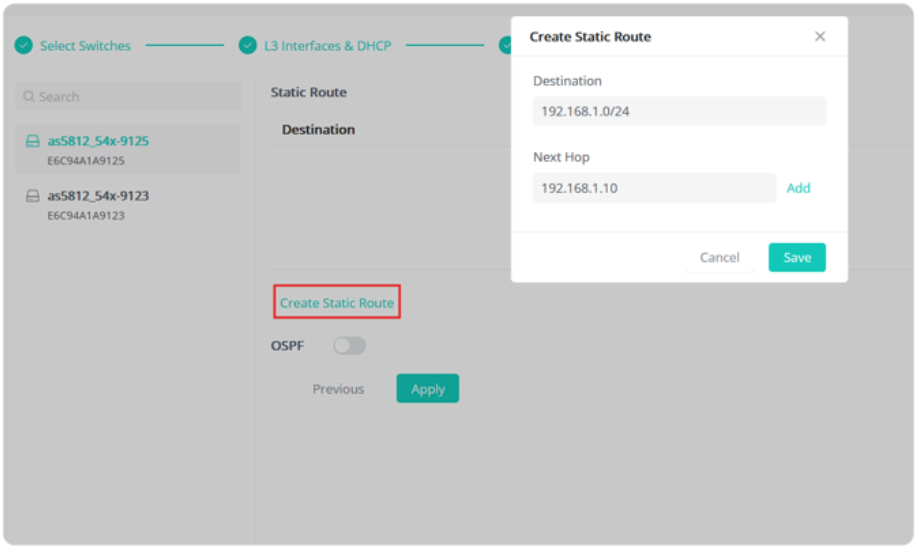


Table 3. Static Route Parameters

Parameter	Description
Destination	The destination IPv4 address and the prefix length. For example, 192.168.4.5/22. The valid prefix length ranges from 1 to 32. The destination must be unique on the same switch and in IPv4 format. The destination must not be within the following address ranges: • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 **NOTE** For the **Destination** values, AmpCon-Campus automatically calculates and displays the network address based on the IPv4 address and the prefix length you input.

	For example, if you input 192.168.4.5/22, 192.168.4.0/22 will be displayed.
Next Hop	The next hop IPv4 addresses. The **Next Hop** cannot be a loopback, broadcast, or multicast address. You can click **+** to add more next-hop IP addresses or click **-** to delete next-hop IP addresses. **NOTE** For the same destination, **Next Hop** values cannot be the same. For different destinations, **Next Hop** values can be the same.

Tip

After adding a static route configuration item, you can edit or delete it:

- To delete a static route configuration item, hover over the item, and then click **Delete**.
- To edit a static route configuration item, hover over the item, and then click **Edit**.
- You cannot edit or delete a static route configuration item while it is being pushed to the switch.

d. Repeat **Step a** to **Step c** to add static route configuration items for other switches.

7. Add Open Shortest Path First (OSPF) configurations. OSPF is a link-state routing protocol used to determine the best path for forwarding IP packets within an IP network.

   a. Select a switch in the sidebar.

   b. In the **OSPF** field, toggle it on or off to enable or disable OSPF configurations.

   c. If you toggle **OSPF** on, click the edit icon in the **Router ID** field, and then enter the router ID, which uniquely identifies a router. The router ID must be in IPv4 format and must be unique within the site.

d. Click **Create OSPF** to add an OSPF configuration item. You can add one or multiple OSPF configuration items for each switch.

e. In the pop-up window, input the following parameters, and then click **Save**.

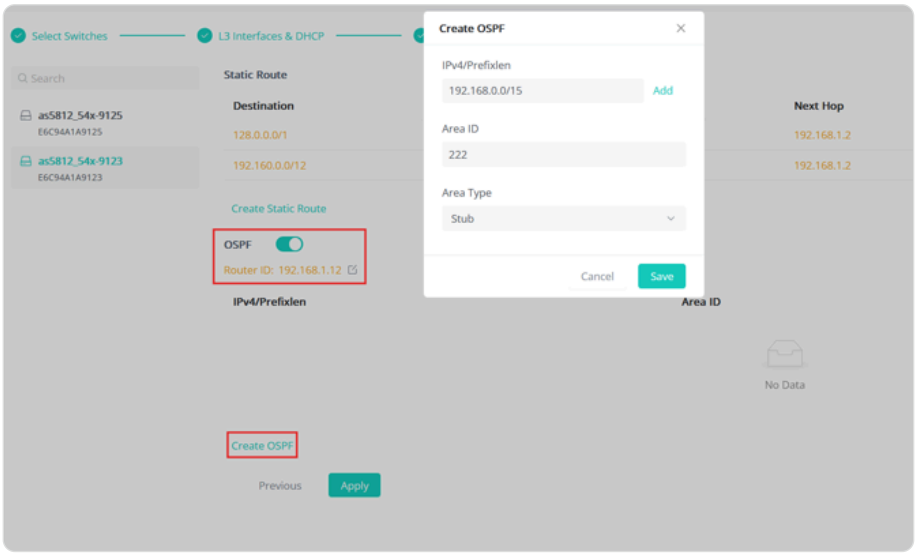


Table 4. OSPF Parameters

Parameter	Description
IPv4/Prefixlen	The IPv4 address and prefix length. The IPv4/Prefixlen must be unique within the same OSPF configuration item. The IPv4/Prefixlen must not be within the following address ranges: • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 Click **+** to add more IPv4/Prefixlen. Click **-** to delete an IPv4/Prefixlen. After adding an IPv4/Prefixlen, you cannot edit it. **NOTE** For the **IPv4/Prefixlen** values, AmpCon-Campus automatically calculates and displays the network address based on the IPv4 address and the prefix length you input.

	For example, if you input 192.168.4.5/22, 192.168.4.0/22 will be displayed.
Area ID	The ID of the OSPF area. OSPF divides a network into areas to improve scalability and control the flow of routing information. Each Area ID must be unique on the same switch. The area ID can be in IPv4 format or an integer ranging from 0 to 4294967295.
Area Type	The type of the OSPF area. Values can be **Stub**, **NSSA**, and **Default**. • **Stub:** An OSPF stub area is a special type of OSPF area designed to optimize routing efficiency by blocking external route advertisements while maintaining internal and inter-area connectivity. • **NSSA:** A Not-So-Stubby Area (NSSA) is a special OSPF area type that combines features of stub areas and standard areas, allowing limited external route redistribution while blocking most external LSAs. • **Default:** The default area in OSPF (also called standard area) refers to a non-specialized OSPF area that permits all types of LSAs (Type 1-5) without restrictions. **NOTE** If the **Area ID** that you entered is **0.0.0.0** or **0**, only **Default** can be selected as the **Area Type**.

Tip

After adding an OSPF configuration item, you can edit or delete it:

- To delete an OSPF configuration item, hover over the item, and then click **Delete**.
- To edit an OSPF configuration item, hover over the item, and then click **Edit**.
- You cannot edit or delete OSPF configurations while they are being pushed to the switch.

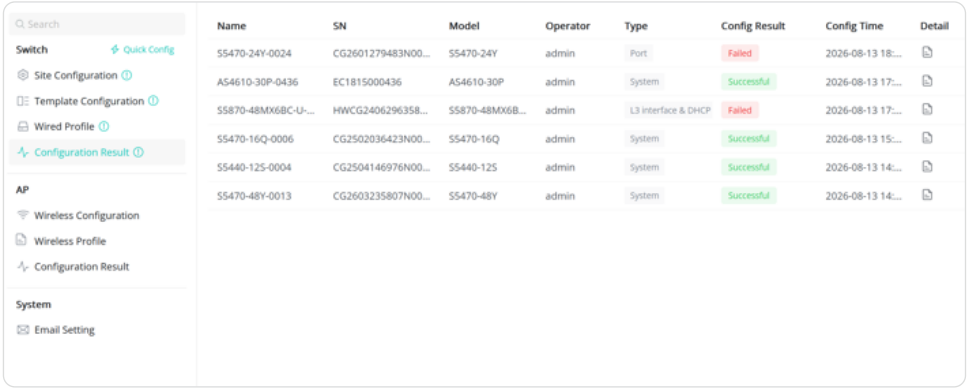
f. Repeat **Step a** to **Step e** to add OSPF configuration items for other switches.

8. Click **Apply**. You will be redirected to the “Configuration Result” page.

> **NOTE**
>
> The configurations can be pushed to the selected switches only after you click **Apply**.

9. On the “Configuration Result” page, check the configuration result for each configured switch.

   For more information, see Checking Configuration Results.



Applying Port Configurations

After onboarding PicOS switches, you can configure switch ports through the “Ports” page or **Quick Config** wizard, improving configuration efficiency and consistency.

- Guidelines
- Prerequisites
- Configuring Switch Ports through Port Profiles
  - Adding a Port Profile
  - Pushing Port Configurations to Switches
- Configuring Switch Ports Directly
- Checking Configuration Results

Guidelines

- You can configure switch ports through a predefined port profile, or you can configure switch ports directly:
  - **Configuring switch ports through port profiles**
    Select a predefined port profile for one or multiple switch ports. Then, AmpCon-Campus will automatically apply port configurations defined in the profile to the switch. This method is suitable for batch configuration or standardized deployment.
  - **Configuring switch ports directly**
    Customize configurations of individual ports based on specific requirements. This method is suitable for per-port adjustments.
- Port configurations applied through the **Quick Config** wizard are synchronized to the port configurations on the “Ports” page, and vice versa.

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the configuration will fail.

Table 1. Prerequisites

Prerequisite	Reference Link
Onboard PicOS switches to bring them under AmpCon-Campus management.	• Onboarding PicOS Switches
Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List

Configuring Switch Ports through Port Profiles

Adding a Port Profile

Prepare a port profile first. Follow these steps:

1. In the AmpCon-Campus UI, select a site to which the PicOS switches to be configured belong.
2. Click the **Settings** icon from the navigation bar, and then click **Wired Profile** in the sidebar.
3. On the “Wired Profile” page, click **+ Port Profile**. In the pop-up window, input the following information:

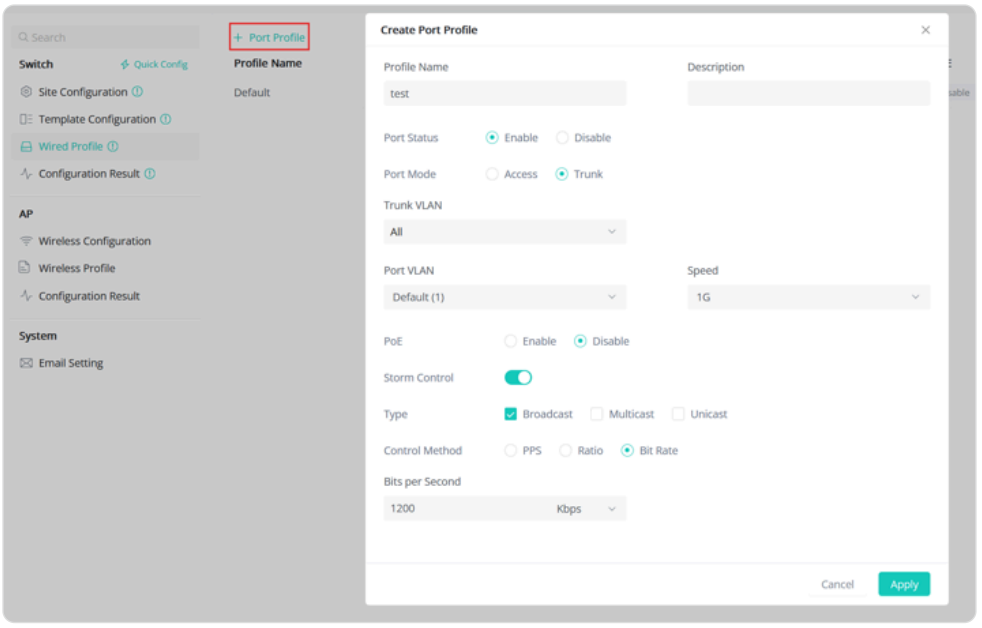


Table 2. Port Profile Parameters

Parameter	Description
Profile Name	The name of the port profile. • The name needs to be unique. • The name cannot be set to **Default** (case-insensitive). • The name can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The name cannot start or end with a hyphen or an underscore.
Description	Optional. The description of the port profile. The description can contain at most 100 characters. Only English characters (letters, numbers, and special characters) and spaces are allowed. Quotes, backslashes, and question marks are not allowed.
Port Status	Enables or disables the associated ports.
Port Mode	The mode of the port, **Access** or **Trunk**.

	• **Access:** Mainly used to connect terminal devices such as PCs. All data packets sent to and received by terminal devices are untagged. • **Trunk:** Mainly used to connect network devices that support VLANs, such as switches and routers. Packets with specific VLAN tags are allowed to pass through the trunk port, enabling transparent VLAN transmission across devices.
Trunk VLAN	The networks with their VLAN IDs. Trunk ports allow frames of these selected networks to pass. In the drop-down list, select one or multiple networks. The networks displayed here include the system-defined network named **Default** and the networks that you added on the “Site Configuration” page. For more information, see Applying Site Configurations. **NOTE** The section is available only if you select **Trunk** in the **Port Mode** section.
Port VLAN	The network corresponding to the ports' native VLAN ID. In the drop-down list, select the system-defined network named **Default** or a network that you added on the “Site Configuration” page.
Speed	The port speed. • If you select **Auto**, the port will work in the auto-negotiation mode. In the auto-negotiation mode, both ports of a link negotiate any rate supported by the two switches. • If you select a specific speed value (such as **100M)**, the ports are set to the selected speed (such as 100 Mb/s). **NOTE** Only 10G RJ45, 5G/2.5G RJ45, and 1G RJ45 ports support selecting the auto-negotiation

	mode. For other port types, even though you select **Auto**, the port speed will be set to the supported maximum speed of each port after the port profile is applied.
PoE	Enables or disables the associated ports to support Power over Ethernet (PoE).
Storm Control	Enables or disables storm control to actively prevent packet proliferation and maintain the performance of the VLAN.
Type	The packet types (broadcast, multicast, or unknown unicast packets) dropped automatically when the traffic exceeds the traffic level specified in the **Control Method** section. Values are **Broadcast**, **Multicast**, and **Unicast**. You can select one or multiple packet types.
Control Method	The method of storm control. Values are **PPS**, **Ratio**, and **Bit Rate**. You need to specify the traffic level triggering the dropping of packets as follows: • If you select **PPS**, you can see the **Packet Count per Second** field. Enter a value ranging from 0 to 30000000. • If you select **Ratio**, you can see the **Percentage of Physical Link** field. Enter a value ranging from 0 to 100, which means the rate of ingress traffic on the physical port. The value is the percentage of the physical link speed. • If you select **Bit Rate**, you can see the **Bits per Second** section. Select **Kbps**, **Mbps**, or **Gbps** as the unit, and enter a bit rate value. The **Bits per Second** value cannot exceed the port speed selected in the **Speed** drop-down list. If you select **Auto** in the **Speed** drop-down list, the **Bits per Second** value cannot exceed 400 Gbps (400000 Mbps or 400000000 Kbps).

> **NOTE**
>
> For these three triggering methods, if the value is set to **0**, it means that data packets are not allowed to pass.

4. Click **Apply**.

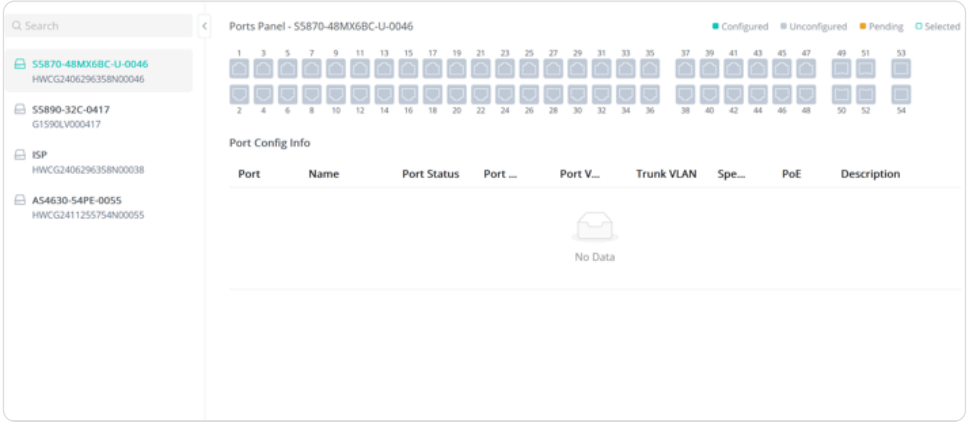
> **NOTEs**
>
> - After adding a port profile, you can edit or delete it:
>   - To edit a port profile, hover over the profile, and then click **Edit**.
>   - To delete a port profile, hover over the profile, and then click **Delete**.
> - The built-in port profile named **Default** cannot be deleted or edited. To view the configurations in this profile, hover over it, and then click **View**.
> - If a port profile is currently referenced by port configurations, editing or deleting it will remove the reference.
>
>   The configurations included in the port profile will be displayed in the **Custom** tab of the port configuration pop-up window.

Pushing Port Configurations to Switches

After creating a port profile, configure switch ports by using the port profile. Follow these steps:

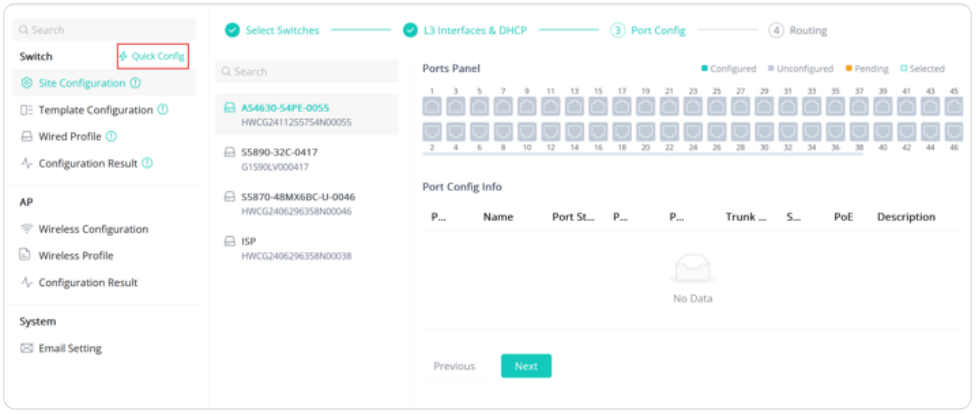
1. Go to the port panel through one of the following ways:

- Click the **Ports** icon from the navigation bar to go to the “Ports” page.



- Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar to open the **Quick Config** wizard.

In the **Select Switches** tab, select the switches to be configured, and then click **Next** until going to the **Port Config** tab.



2. Click the switch to be configured, and then select one or multiple ports in the port panel.

   To select multiple ports, hold down **Ctrl** while clicking multiple ports.

   NOTEs

   - If you select multiple ports, ensure that these ports have the same port speed and PoE support.
   - A combo port refers to one logical port mapped to two physical ports: an electrical port and an optical port. These two physical ports are displayed in the port panel but share the same logical port name.

     When you select either physical port in the port panel, the other physical port belonging to the same logical port will also be selected synchronously.
   - In the port panel, different colors indicate different port statuses:
     - Configured ports are marked in green.
     - Unconfigured ports are marked in grey.
     - Ports pending configuration or being configured are marked in yellow.

3. In the pop-up window, click the **Port Profile** tab. Select a port profile from the drop-down list, and then click **Save**.

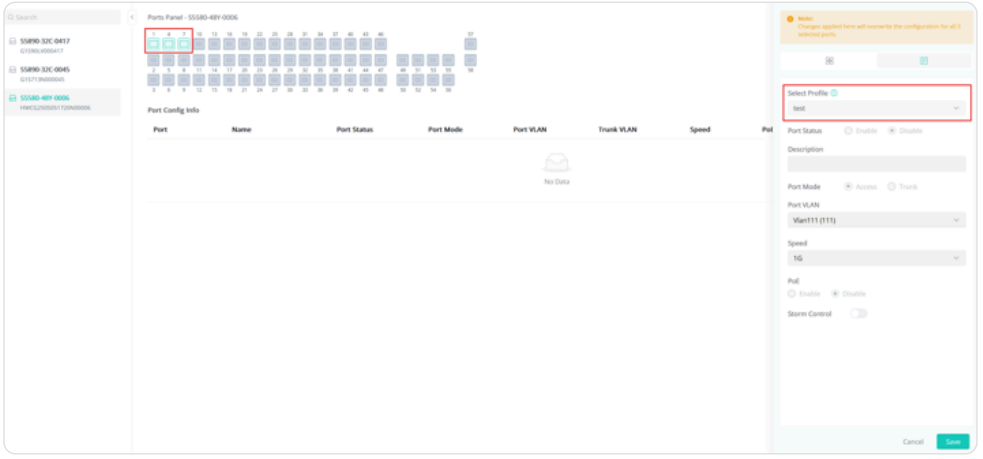
   After you click **Save**, the configuration item is displayed in the **Port Config Info** section, but the port configurations are not applied to the selected switch yet.

   To delete a port configuration item from the **Port Config Info** list, hover over the configuration item, and then click **Delete**.

NOTEs

- After you select a port profile, the configurations in the **Port Profile** tab are automatically populated and cannot be changed.
- Port configurations cannot be applied in the following cases:
  - The speed defined in the port profile does not match the speed of the selected ports.
  - The selected port profile enables PoE, but the selected ports do not support PoE.
- For combo ports, you can select only a port profile in which the port speed is 1G.

  The combo ports (when working as electrical ports) only support auto-negotiation mode; that is, even though you configure the port speed as 1G, the auto-negotiation mode is used for the combo port when it works as an electrical port.



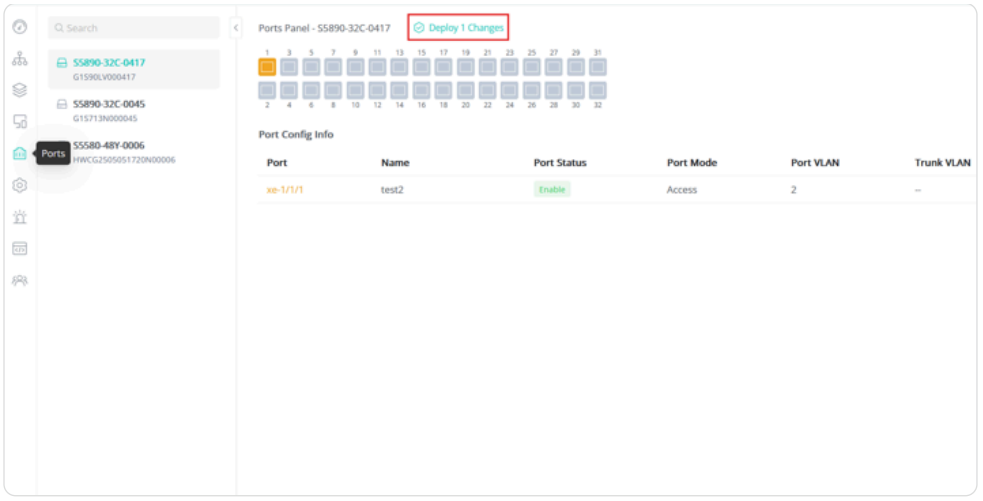
4. Apply port configurations to the switch as follows:

NOTE

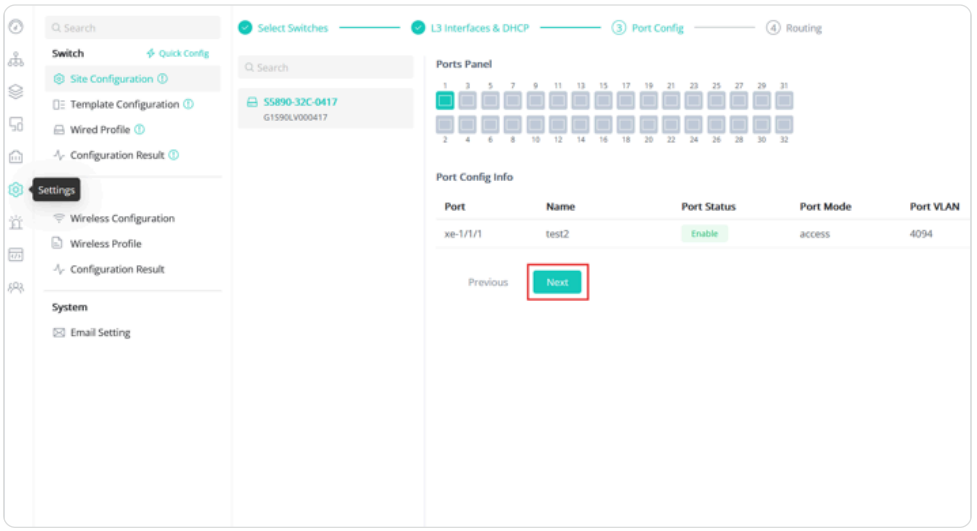
AmpCon-Campus applies port configurations only to PicOS switches that meet all the following requirements:

- The switches are online (connected to AmpCon-Campus).
- No configurations are being pushed or waiting to be pushed to the switches.
- No upgrade tasks are running on the switches.

- If you configure switch ports through the “Ports” page, click **Deploy x Changes**.



- If you configure switch ports through the **Quick Config** wizard, click **Next** and then click **Apply** to complete the quick configuration.



Configuring Switch Ports Directly

In addition to configuring switch ports through port profiles, you can also configure switch ports directly. Follow these steps:

1. Go to the port panel as described in **Step 1** of the Pushing Port Configurations to Switches section.
2. Click the switch to be configured, and then select one or multiple ports in the port panel.

   To select multiple ports, hold down **Ctrl** while clicking multiple ports.

NOTEs

- If you select multiple ports, ensure that these ports have the same port speed and PoE support.
- A combo port refers to one logical port mapped to two physical ports: an electrical port and an optical port. These two physical ports are displayed in the port panel but share the same logical port name.

  When you select either physical port in the port panel, the other physical port belonging to the same logical port will also be selected synchronously.
- In the port panel, different colors indicate different port statuses:
  - Configured ports are marked in green.
  - Unconfigured ports are marked in grey.
  - Ports pending configuration or being configured are marked in yellow.

3. In the **Custom** tab of the pop-up window, enter the name and description (optional) of the port configuration.

   The name can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The name cannot start or end with a hyphen or underscore.

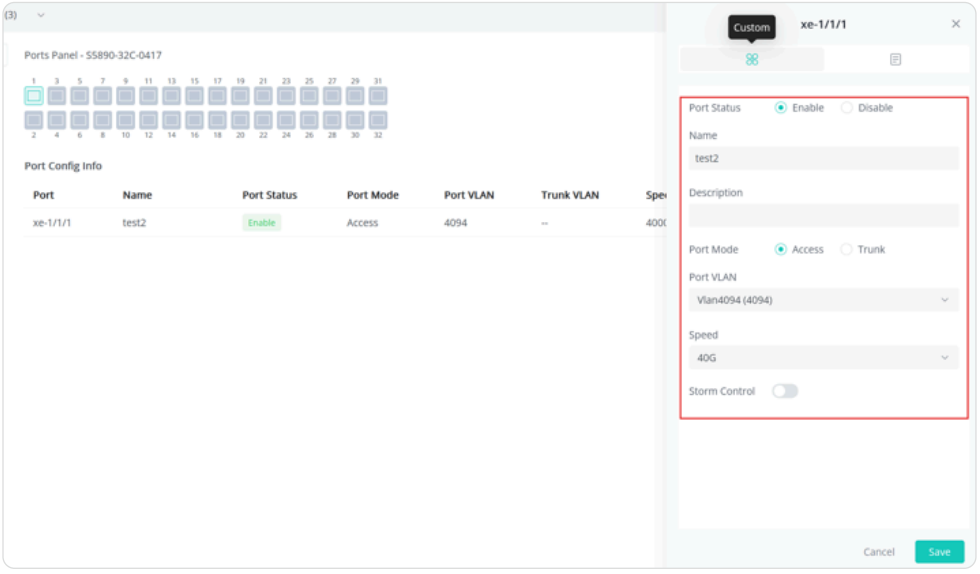
   Then, configure other port parameters as needed, and click **Save**. For port parameter descriptions, see **Table 2. Port Profile Parameters**.

NOTEs

- The **PoE** section will not appear if the selected ports do not support PoE.
- The **Speed** drop-down list displays only the speeds supported by the selected ports.
- For combo ports, you can select only **1G** as the port speed .

  The combo ports (when working as electrical ports) only support auto-negotiation mode; that is, even though you configure the port speed as 1G, the auto-negotiation mode is used for the combo port when it works as an electrical port.
- After you click **Save**, the configuration item is displayed in the **Port Config Info** list, and the port configurations are not applied to the selected switch yet.

  To delete a port configuration item from the **Port Config Info** list, hover over the configuration item, and then click **Delete**.



4. Apply port configurations to the switch as follows:

- If you configure switch ports through the “Ports” page, click **Deploy x Changes**.
- If you configure switch ports through the **Quick Config** wizard, click **Next** and then click **Apply** to complete the quick configuration.

NOTE

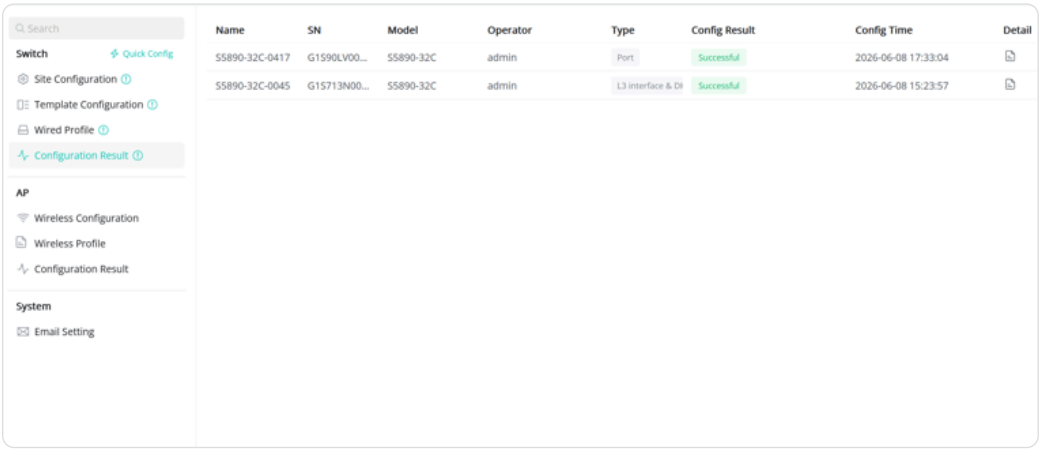
AmpCon-Campus applies port configurations only to PicOS switches that meet all the following requirements:

- The switches are online (connected to AmpCon-Campus).
- No configurations are being pushed or waiting to be pushed to the switches.
- No upgrade tasks are running on the switches.

Checking Configuration Results

Click the **Settings** icon from the navigation bar, and then click **Configuration Result** from the sidebar. On the “Configuration Result” page, check the port configuration result.

For more information, see Checking Configuration Results.



Configuring a Single Switch

After onboarding a PicOS switch to AmpCon-Campus, you can fine-tune configurations of the switch.

Click the **Devices** icon from the navigation bar. On the “Devices” page, click a specific PicOS switch. You can see a side panel on the right. In the **Setting** tab of the side panel, you can modify the switch configurations as needed.

Guidelines
Prerequisites
Procedure

Guidelines

- All configurations in the **Setting** tab are optional. Modify only the configurations that you need. AmpCon-Campus will apply only the modified configurations to the switch.
- Any custom configurations applied to a single PicOS switch will be pushed to that switch as device-specific configurations, while other site-level configurations are still applied to the switch.
- If the PicOS switch is offline (disconnected from AmpCon-Campus), modifications to L3 interface, DHCP, static route, and OSPF configurations will fail.
- Each IP address that you enter in the **Setting** tab must not be within the following address ranges:
  - Link-local addresses: 169.254.0.0 to 169.254.255.255
  - Loopback addresses: 127.0.0.0 to 127.255.255.255
  - Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255
  - Special reserved addresses: 0.0.0.0 to 0.255.255.255
- L3 interface, DHCP, static route, and OSPF configurations applied in the **Setting** tab will be automatically synchronized to the **Quick Config** wizard, and vice versa. For more information about the **Quick Config** wizard, see Applying Quick Configurations.

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the configuration will fail.

Table 1. Prerequisites

Prerequisite	Reference Link
Onboard PicOS switches to bring them under AmpCon-Campus management.	• Onboarding PicOS Switches

Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List

Procedure

1. In the AmpCon-Campus UI, select the site to which the PicOS switch belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click a PicOS switch, and then click the **Setting** tab of the side panel.
3. At the top of the **Setting** tab, modify general switch configurations if needed:

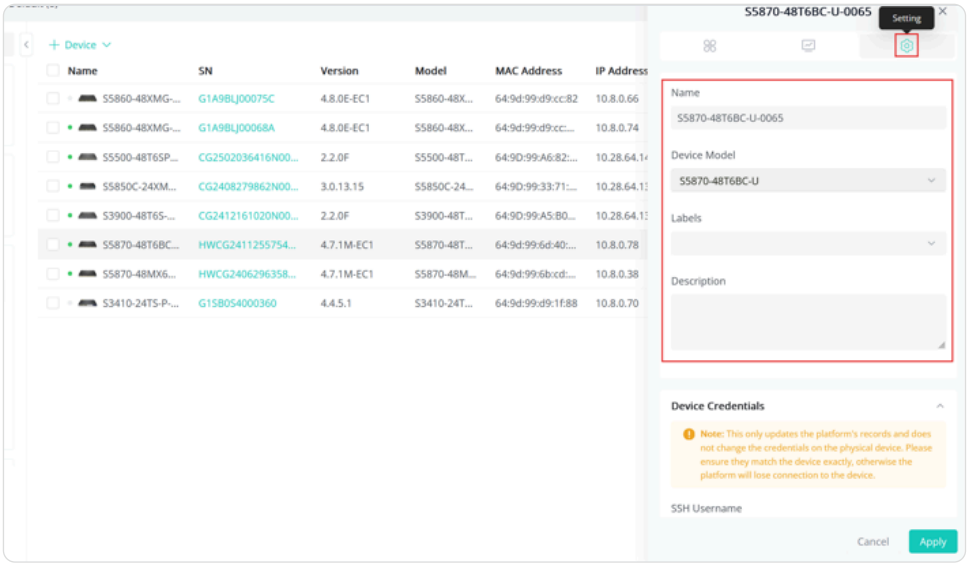


Table 2. General Switch Configurations

Parameter	Description
Name	The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side. The alias can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The alias cannot start or end with a hyphen or an underscore.
Device Model	The model of the switch. AmpCon-Campus automatically retrieves the switch model and displays it here. The model can’t be changed.
Labels	The switch labels used for switch filtering and management. You can select one or multiple labels. To add a new label, click the **Labels** drop-down list, and then click **Create Label**. Each label can contain

	only letters and numbers and can contain at most 64 characters.
Description	The description of the switch. The description can contain at most 256 characters.

4. In the **Device Credentials** section, modify the **SSH Username** and **SSH Password** if needed:

> **NOTEs**
>
> - Ensure that the username and password match the switch exactly. Otherwise, AmpCon-Campus cannot access and manage the switch.
> -
> - If the **SSH Username** and **SSH Password** are incorrect, you can modify them here. The updated username and password will update the credentials on AmpCon-Campus but will not change the credentials on the switch side.

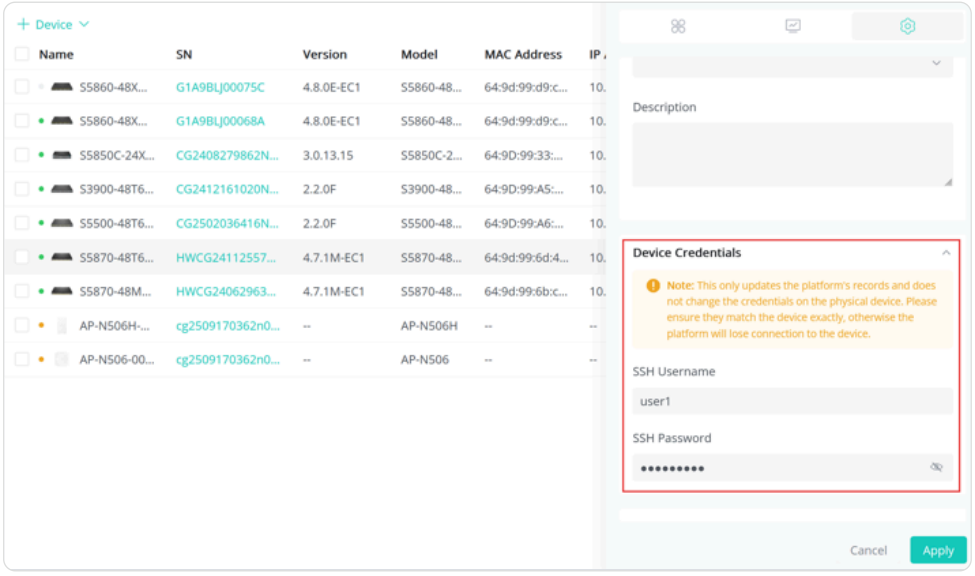


Table 3. Device Credential Configurations

Parameter	Description
SSH Username	The username used to log in to the switch. The username must start with a letter or an underscore and can contain letters, digits, underscores, hyphens, and a trailing $.

	The username can contain at most 32 characters.
SSH Password	The password of the user. Only ASCII characters are supported. Click the eye icon to see the clear-text password.

5. In the **L3 Interface & DHCP** section, click **+ Create L3 Interface & DHCP** to create an L3 interface and DHCP configuration item. Input the following information, and then click **Save**.

> **NOTEs**
>
> - L3 interface configurations are used to configure a VLAN interface with an IP address, enabling Layer 3 routing for devices in the VLAN.
>
> DHCP configurations determine how IP addresses are assigned to devices in the corresponding VLAN.
> - You can add one or multiple L3 interface and DHCP configuration items for each switch.

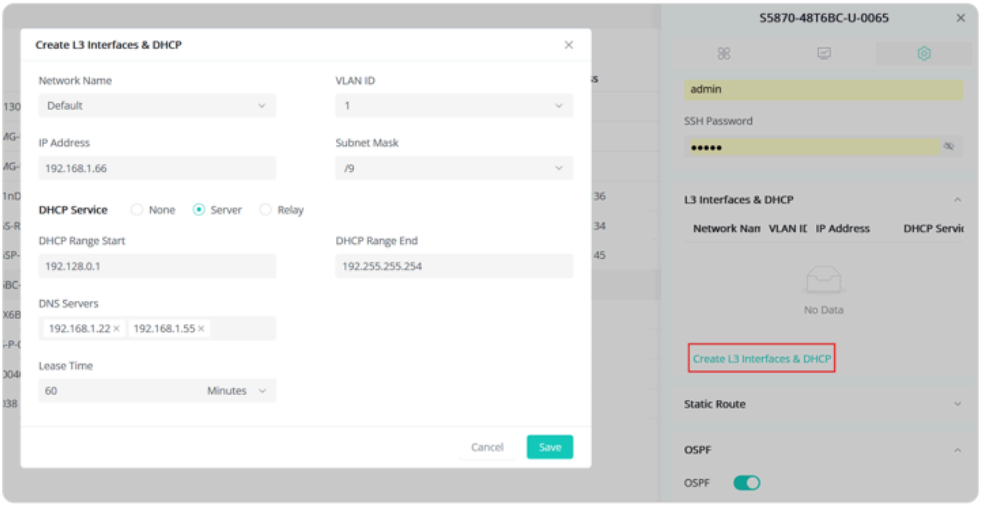


Table 4. L3 Interface and DHCP Parameters

Parameter	Description
Network Name	The name of the Layer 3 VLAN interface. You can select the built-in network named **Default** or select a network that you added in the **Network** section of the “Site Configuration” page. For more information, see Adding Network Configurations.

	NOTE Within the same site, each network can be configured with only one DHCP server or DHCP relay.
VLAN ID	The VLAN identifier. The **VLAN ID** will be automatically filled after you select the **Network Name**, and vice versa.
IP Address	The IPv4 address assigned to the Layer 3 interface. **NOTEs** • The IP address must be unique within the site. • The **IP Address** cannot be the loopback address, the subnet network address, or the subnet broadcast address. • Based on the **IP Address** and **Subnet Mask**, AmpCon-Campus automatically calculates the subnet for the Layer 3 interface. This subnet must not overlap with subnets of other Layer 3 interfaces on the same switch.
Subnet Mask	The subnet mask of the Layer 3 interface, such as **/24**.
DHCP Service	The DHCP mode for this subnet. The value can be **None**, **Server**, or **Relay**. • **None:** DHCP is disabled. • **Server:** The switch acts as a DHCP server. • **Relay:** The switch acts as a DHCP Relay and forwards DHCP requests to an external DHCP server. **NOTE** The **Server** option is not displayed for S3270 and S3410 switches.
DHCP Range Start	The starting IPv4 address of the DHCP address pool, which is used to assign IP addresses. **NOTEs**

	• This field is displayed only if you select **Server** in the **DHCP Service** section. • The **DHCP Range Start** cannot be the network address or broadcast address of the subnet. • AmpCon-Campus automatically calculates and displays the **DHCP Range Start** and **DHCP Range End** values based on the **IP Address** and **Subnet Mask**. You can modify the **DHCP Range Start** and **DHCP Range End** values as needed. • The DHCP address pool must be within the subnet of the configured L3 interface.
DHCP Range End	The ending IPv4 address of the DHCP address pool, which is used to assign IP addresses. **NOTEs** • This field is displayed only if you select **Server** in the **DHCP Service** section. • The **DHCP Range End** must be greater than the **DHCP Range Start**. • The **DHCP Range End** cannot be the network address or broadcast address of the subnet.
DNS Servers	The IPv4 addresses of DNS servers, which are used for dynamic domain name resolution. You can add at most 2 DNS servers. After you add each DNS server IPv4 address, be sure to press **Enter**. **NOTE** This field is displayed only if you select **Server** in the **DHCP Service** section.
Lease Time	The valid lease duration of each IP address assigned by a DHCP server to a client device. You can click the drop-down arrow to select **Minutes**, **Hours**, or **Days**.

	• If you select **Minutes**, the value must range from 2 to 43200. • If you select **Hours**, the value must range from 1 to 720. • If you select **Days**, the value must range from 1 to 30. **NOTE** This field is displayed only if you select **Server** in the **DHCP Service** section.
Relay Server IP	The IPv4 address of the external DHCP server to which DHCP requests are forwarded. **NOTEs** • The **Relay Server IP** value cannot be the same as the **IP Address** value. • This field is displayed only if you select **Relay** in the **DHCP Service** section.

Tip

After adding an L3 interface and DHCP configuration item, you can edit or delete it:

- To delete an L3 interface and DHCP configuration item, hover over the item, and then click **Delete**.
- To edit an L3 interface and DHCP configuration item, hover over the item, and then click **Edit**.
- You cannot edit or delete an L3 interface and DHCP configuration item while it is being pushed to the switch.

6. In the **Static Route** section, click **+ Static Route** to create a static route configuration item. Input the following information, and then click **Save**.

NOTE

You can add one or multiple static route configuration items for each switch.

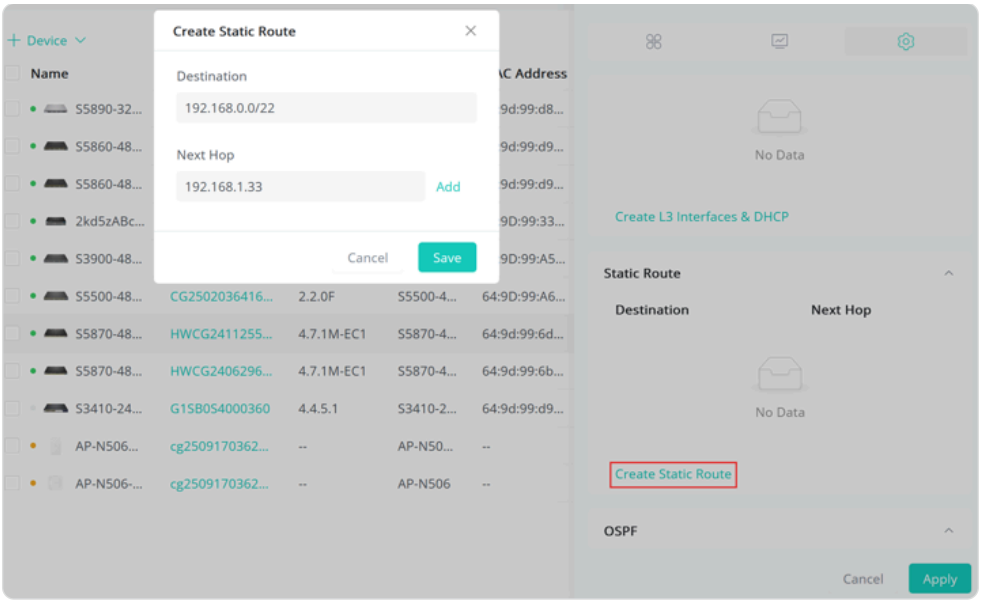


Table 5. Static Route Parameters

Parameter	Description
Destination	The destination IPv4 address and the prefix length. For example, 192.168.4.5/22. The valid prefix length ranges from 1 to 32. The destination must be unique on the same switch and in IPv4 format. The **Destination** must not be within the following address ranges: • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 **NOTE** For the **Destination** values, AmpCon-Campus automatically calculates and displays the network address based on the IPv4 address and the prefix length you input. For example, if you input 192.168.4.5/22, 192.168.4.0/22 will be displayed.
Next Hop	The next hop IPv4 addresses. The **Next Hop** cannot be a loopback, broadcast, or multicast address.

You can click **+** to add more next-hop IP addresses or click **-** to delete next-hop IP addresses.

> **NOTE**
>
> For the same destination, **Next Hop** values cannot be the same. For different destinations, **Next Hop** values can be the same.

> **Tip**
>
> After adding a static route configuration item, you can edit or delete it:
>
> - To delete a static route configuration item, hover over the item, and then click **Delete**.
> - To edit a static route configuration item, hover over the item, and then click **Edit**.
> - You cannot edit or delete a static route configuration item while it is being pushed to the switch.

7. In the **OSPF** section, configure OSPF configurations as follows:

   a. Toggle on or off **OSPF** to enable or disable OSPF.

   b. If you toggle **OSPF** on, click the edit icon in the **Router ID** field, and then enter the router ID, which uniquely identifies a router. The router ID must be in IPv4 format and must be unique within the site.

   c. Click **+ Create OSPF** to add an OSPF configuration item. Input the following information, and then click **Save**.

   > **NOTE**
   >
   > You can add one or multiple OSPF configuration items for each switch.

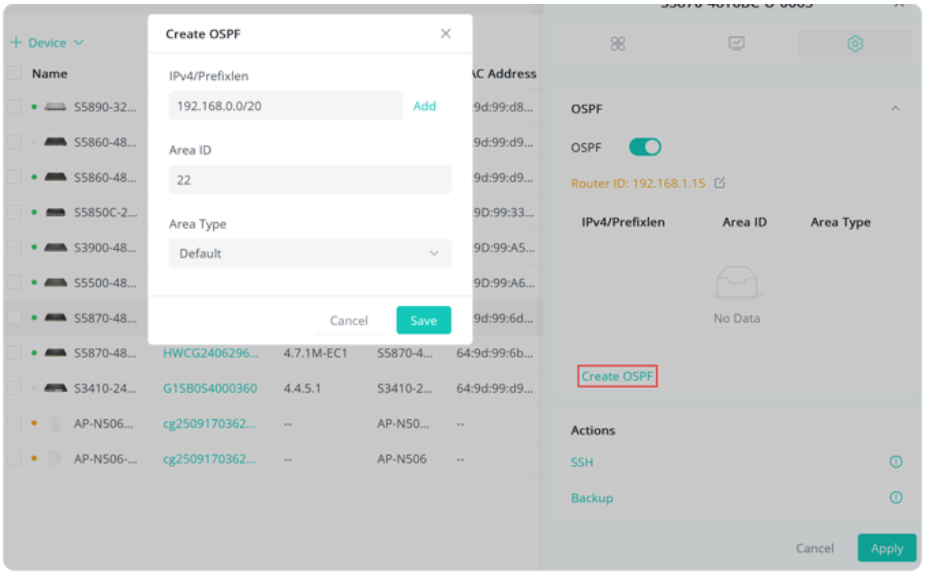


Table 6. OSPF Parameters

Parameter	Description
IPv4/Prefixlen	The IPv4 address and prefix length. The IPv4/Prefixlen must be unique within the same OSPF configuration item. The IPv4/Prefixlen must not be within the following address ranges: • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 Click **+** to add more IPv4/Prefixlen. Click **-** to delete an IPv4/Prefixlen. After adding an IPv4/Prefixlen, you cannot edit it. **NOTE** For the **IPv4/Prefixlen** values, AmpCon-Campus automatically calculates and displays the network address based on the IPv4 address and the prefix length you input. For example, if you input 192.168.4.5/22, 192.168.4.0/22 will be displayed.
Area ID	The ID of the OSPF area.

	OSPF divides a network into areas to improve scalability and control the flow of routing information. Each Area ID must be unique on the same switch. The area ID can be in IPv4 format or an integer ranging from 0 to 4294967295.
Area Type	The type of the OSPF area. Values can be **Stub**, **NSSA**, and **Default**. • **Stub:** An OSPF stub area is a special type of OSPF area designed to optimize routing efficiency by blocking external route advertisements while maintaining internal and inter-area connectivity. • **NSSA:** A Not-So-Stubby Area (NSSA) is a special OSPF area type that combines features of stub areas and standard areas, allowing limited external route redistribution while blocking most external LSAs. • **Default:** The default area in OSPF (also called standard area) refers to a non-specialized OSPF area that permits all types of LSAs (Type 1-5) without restrictions. **NOTE** If the **Area ID** that you entered is **0.0.0.0** or **0**, only **Default** can be selected as the **Area Type**.

Tip

After adding an OSPF configuration item, you can edit or delete it:

- To delete an OSPF configuration item, hover over the item, and then click **Delete**.
- To edit an OSPF configuration item, hover over the item, and then click **Edit**.

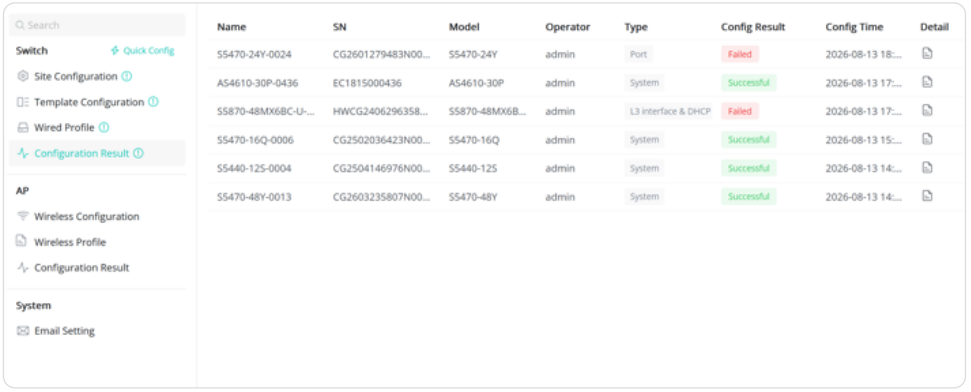
- You cannot edit or delete OSPF configurations while they are being pushed to the switch.

8. Click **Apply**. Then, the configurations will be pushed to the switch.

> **NOTEs**
>
> - Only after you change at least one configuration of the switch, is the **Apply** button displayed.
> - Each time you modify switch configurations, you must click **Apply** to save the changes. Otherwise, the configuration changes will be lost.
> - L3 interface, DHCP, static route, and OSPF configurations will not be pushed to the switch in the following cases:
>   - Other configuration tasks are running on the switch.
>   - The switch is being upgraded.
>   - The switch is not managed by AmpCon-Campus.

9. If L3 interface, DHCP, static route, or OSPF configurations are modified in the **Setting** tab, check the configuration result on the “Configuration Result” page.

   For more information, see Checking Configuration Results.



Applying Template Configurations

After onboarding PicOS switches, you can use configuration templates to push specific configurations that can't be pushed through other configuration methods.

You can upload templates to AmpCon-Campus. Then, create a configuration file by selecting the configuration templates containing required CLI commands, specifying values for each parameter in the templates, and selecting the PicOS switches to be configured. These CLI commands will be run on the switches automatically.

In addition to using templates, you can configure switches by uploading a configuration file to AmpCon-Campus directly.

- Prerequisites
- Configuring through Templates
  - Preparing Templates
  - Pushing Template Configurations to Switches
- Configuring by Uploading Configuration Files

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the configuration will fail.

Table 1. Prerequisites

Prerequisite	Reference Link
Onboard PicOS switches to bring them under AmpCon-Campus management.	• Onboarding PicOS Switches
Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List

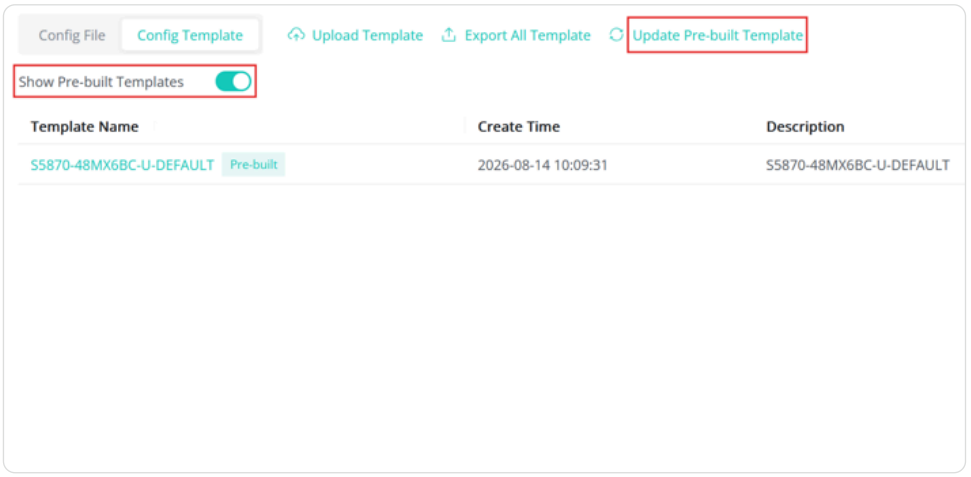
Configuring through Templates

Preparing Templates

Prepare one or multiple templates containing required CLI commands. You can use the built-in template or add new ones. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the PicOS switches to be configured belong.
2. Click the **Settings** icon from the navigation bar, and then click **Template Configuration** in the sidebar.
3. On the "Template Configuration" page, click the **Config Template** tab, and then click **Show Pre-built Templates**. Check whether the built-in template meets your needs.

> **NOTE**
>
> To refresh the built-in template list, click **Update Pre-built Template**.
>
> If AmpCon-Campus can't access the Internet, the refresh will fail.



4. If the built-in template cannot meet your needs, create a new template as follows:
   a. Click **Upload Template**.
   b. In the pop-up window, input the following information, and then click **Apply**.

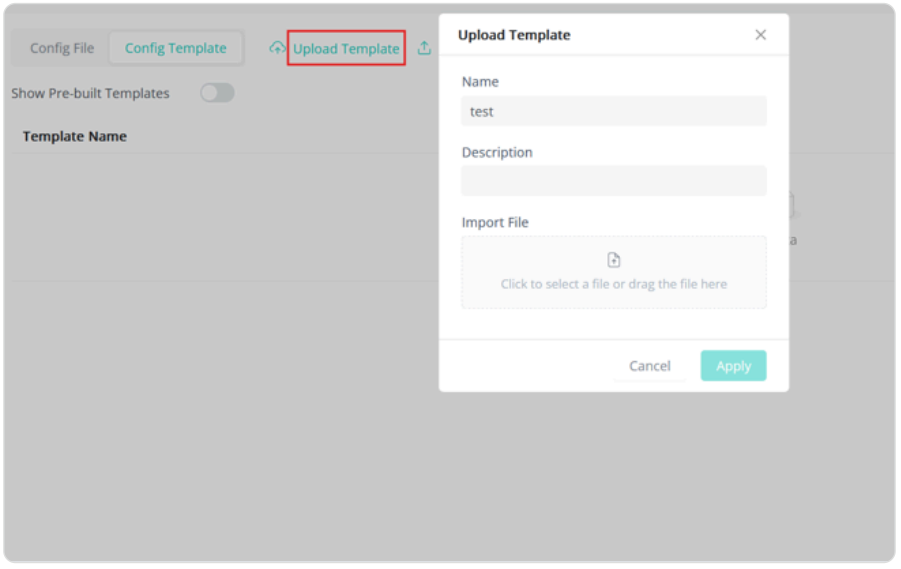


Table 2. Template Parameters

Parameter	Description
Name	The name of the template. • The name must be unique in the selected site. • The name can contain at most 64 characters.

	• Only letters, numbers, hyphens (-), and underscores (_) are allowed. • The name cannot start or end with a hyphen or an underscore.
Description	Optional. The description of the template. The description can contain at most 512 characters.
Import File	Click the upload icon to select a .txt template file. • The maximum size of the .txt file is 64 MB. • The contents in the .txt file must use UTF-8 encoding. • All commands in the .txt file must use the **set** or **delete** syntax. Example: **set system syslog server-ip 10.8.14.5 source-interface "vlan4001"** • All parameters in the .txt file must be defined in JSON format.

Tips

- To view an added template, hover over the template, and then click **View**.

  In the pop-up window, select the configuration display format in the **Template Files** drop-down list.

  You can edit the configurations in the template if needed. Don't forget to click **Apply** after you make changes.
- To edit the template name and description, hover over the template, and then click **Edit**. To delete a template, hover over the template, and then click **Delete**.

  The built-in template can't be edited or deleted.
- To copy a template as a new one, hover over the template, and then click **Copy**.

  Enter the name and description (optional) of the new template, and then click **Apply**.

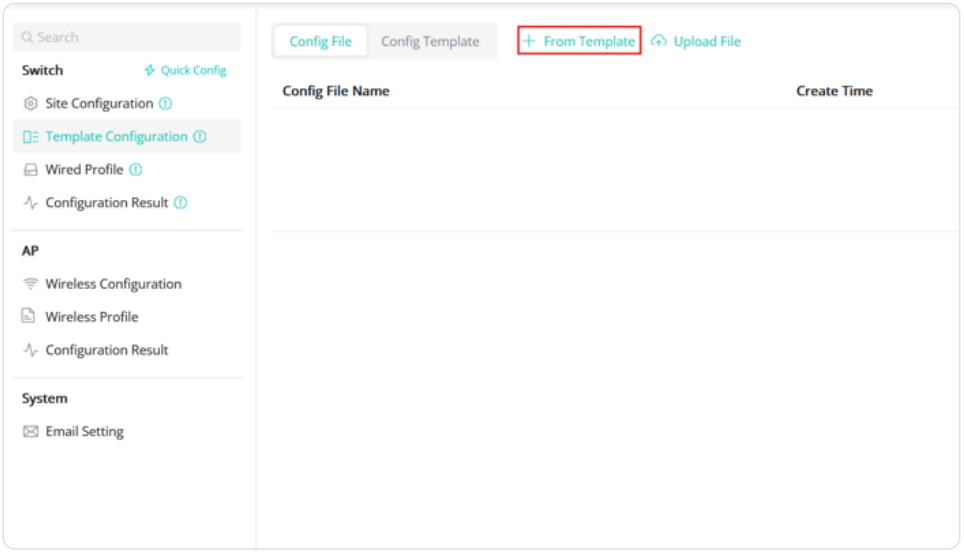
- To export a template, hover over the template, and then click **Export**.

  To export all templates, click **Export All Template** at the top of the **Config Template** tab.

Pushing Template Configurations to Switches

After preparing templates, push configurations in the templates to switches. Follow these steps:

1. Click the **Config File** tab, and then click **+ From Template**.



2. In the **Select Template** tab, input the following information, and then click **Next**.

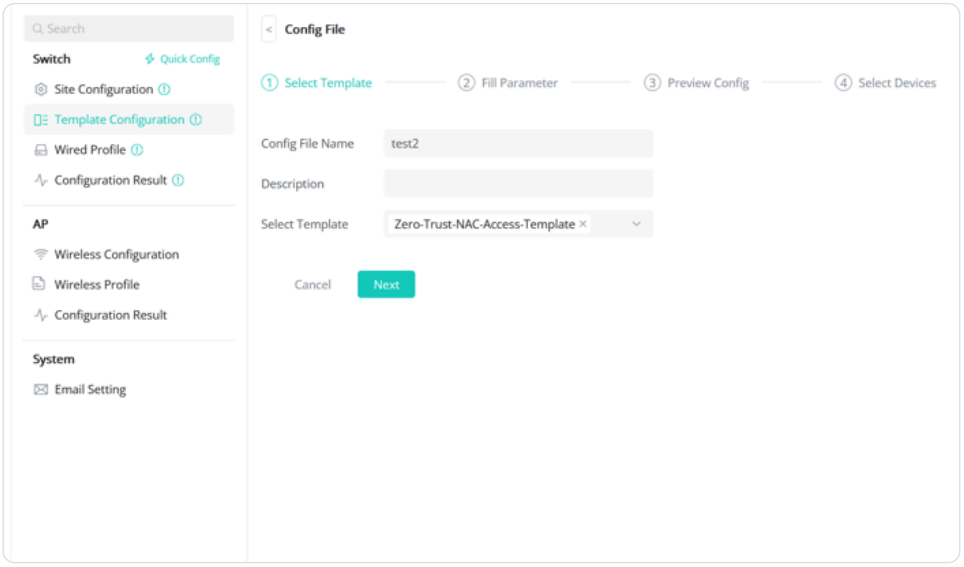
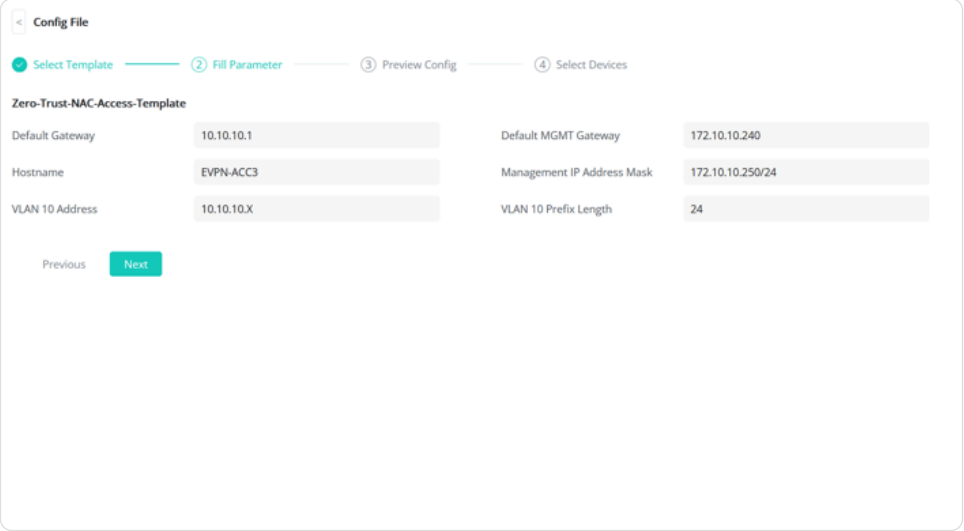


Table 3. Template Selection Parameters

Parameter	Description

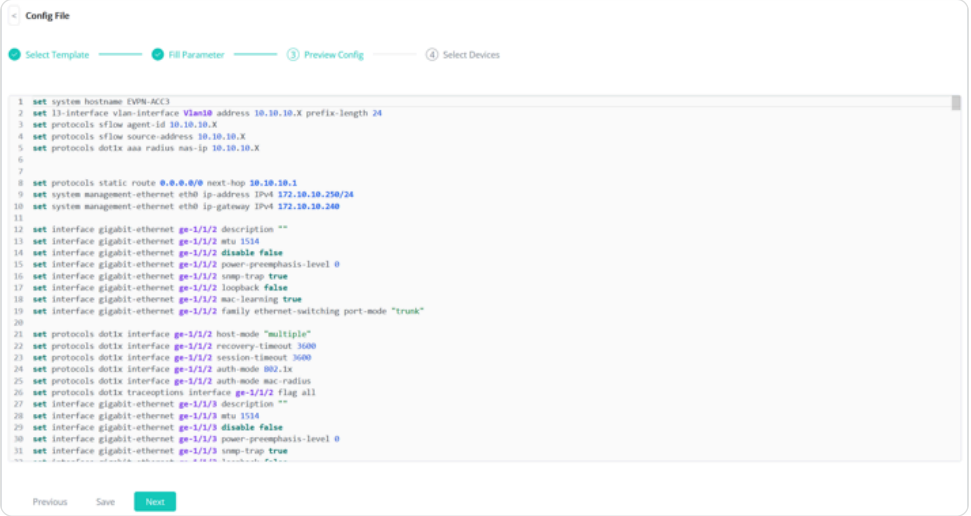
Config File Name	The name of the configuration file. • The name must be unique in the selected site. • The name can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. • The name cannot start or end with a hyphen or underscore.
Description	Optional. The description of the configuration file. The description can contain at most 512 characters.
Select Template	The templates containing required configurations. You can select one or multiple templates. To create a new template, click **Upload Template** at the bottom of the drop-down list.

3. In the **Fill Parameter** tab, specify each parameter value, and then click **Next**.



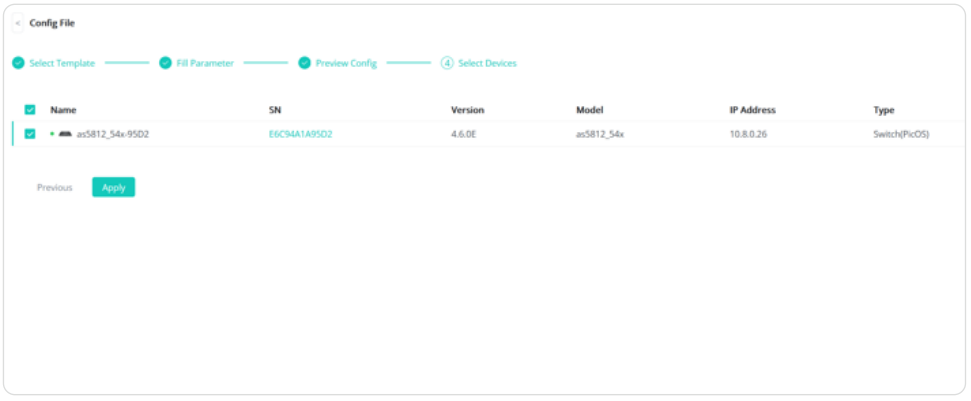
4. In the **Preview Config** tab, check the CLI commands generated based on the provided parameter values, and then click **Next**.

> **NOTE**
>
> You can edit the CLI commands here. Ensure to click **Save** to save the changes.



5. In the **Select Devices** tab, select the switches to be configured.

> **NOTE**
>
> You can select only the PicOS switches that meet all the following requirements:
>
> - The switches are currently online (connected to AmpCon-Campus).
> - No configurations are being pushed or waiting to be pushed to the switches.
> - No upgrade tasks are running on the switches.



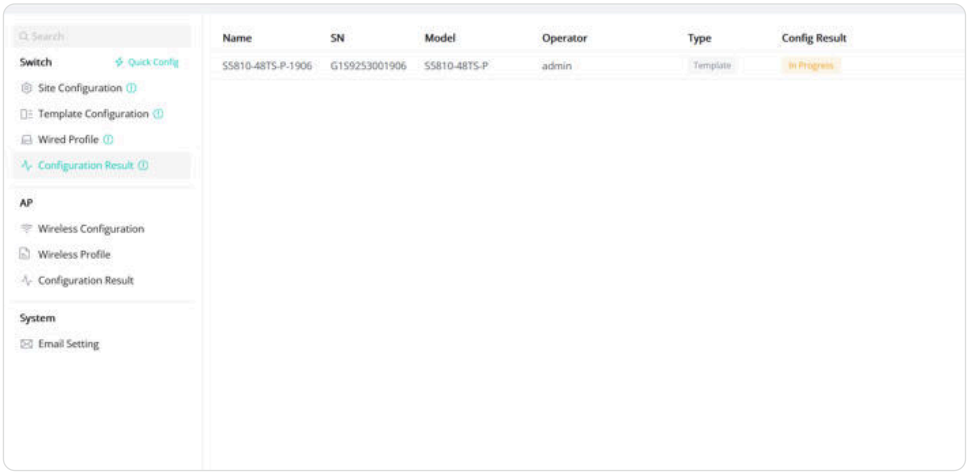
6. Click **Apply**. You will be redirected to the “Configuration Result” page, and the configuration file will be added to the **Config File** tab.

> **Tips**
>
> - To edit a configuration file, hover over the configuration file, and then click **Edit**.
> - To delete a configuration file, hover over the configuration file, and then click **Delete**. You can’t delete the configuration file that is being pushed to switches.

- To copy a config file, hover over the configuration file, and then click **Copy**.

7. On the “Configuration Result” page, check the configuration results.

   For more information, see Checking Configuration Results.



Configuring by Uploading Configuration Files

In addition to configuring switches through templates, you can configure switches by uploading a configuration file to AmpCon-Campus directly. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the PicOS switches to be configured belong.
2. Click the **Settings** icon from the navigation bar, and then click **Template Configuration** in the sidebar.
3. In the **Config File** tab of the “Template Configuration” page, click **Upload File**. In the pop-up window, input the following information, and then click **Apply**.

   Then, you can see the configuration file in the **Config File** tab.

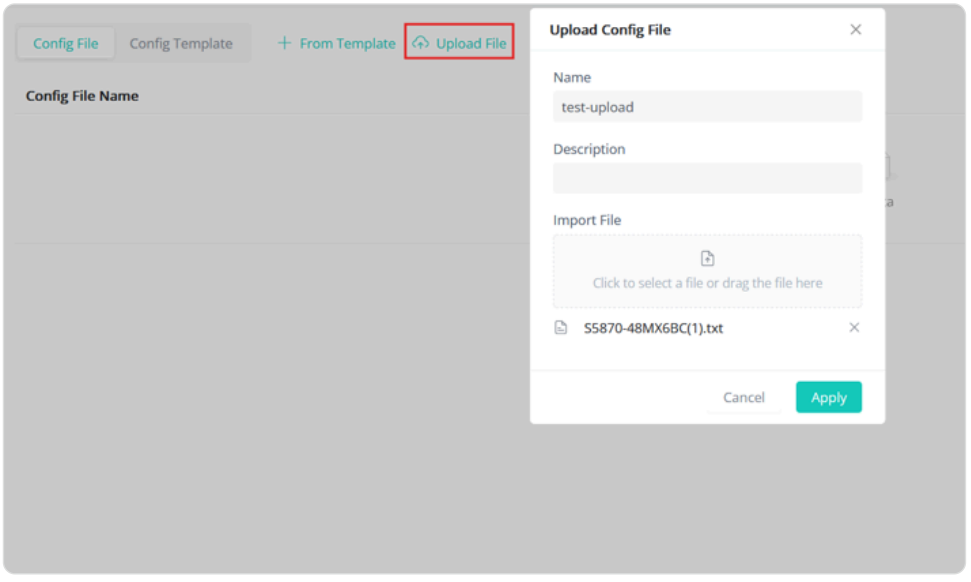
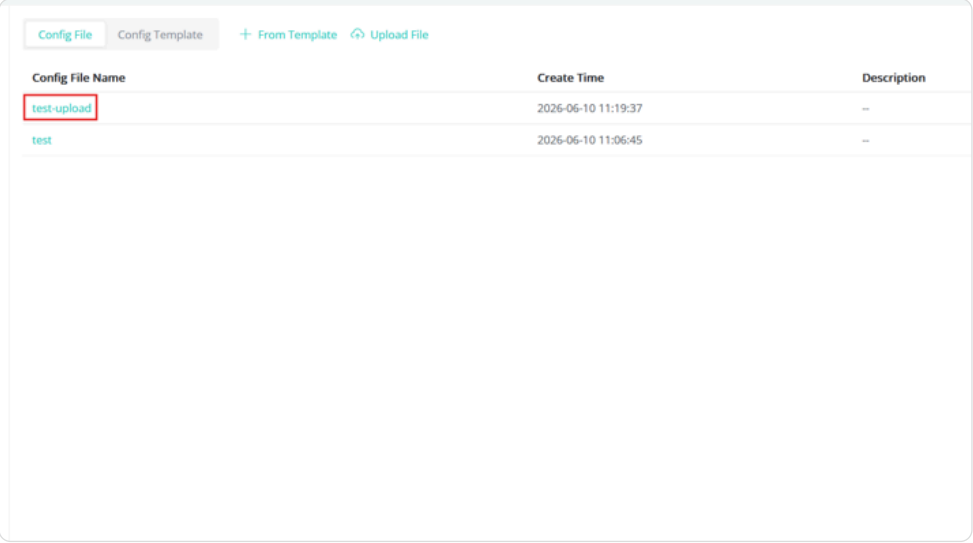


Table 4. Configuration File Parameters

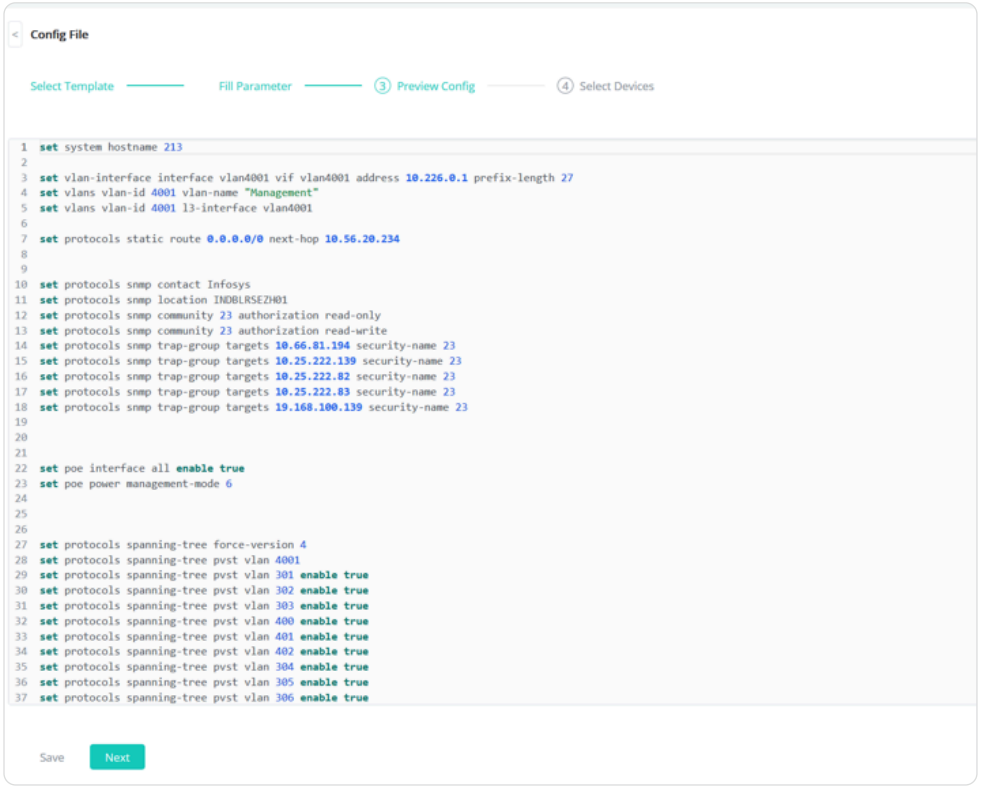
Parameter	Description
Name	The name of the configuration file. • The name must be unique in the selected site. • The name can contain at most 64 characters. • Only letters, numbers, hyphens (-), and underscores (_) are allowed. • The name cannot start or end with a hyphen or underscore.
Description	Optional. The description of the configuration file. The description can contain at most 512 characters.
Import File	Click the upload icon to select a .txt configuration file. • The maximum size of the .txt file is 64 MB. • The contents in the .txt file must use UTF-8 encoding. • All commands in the .txt file must use the **set** or **delete** syntax. Example: **set system syslog server-ip 10.8.14.5 source-interface "vlan4001"**

4. Click the configuration file name.



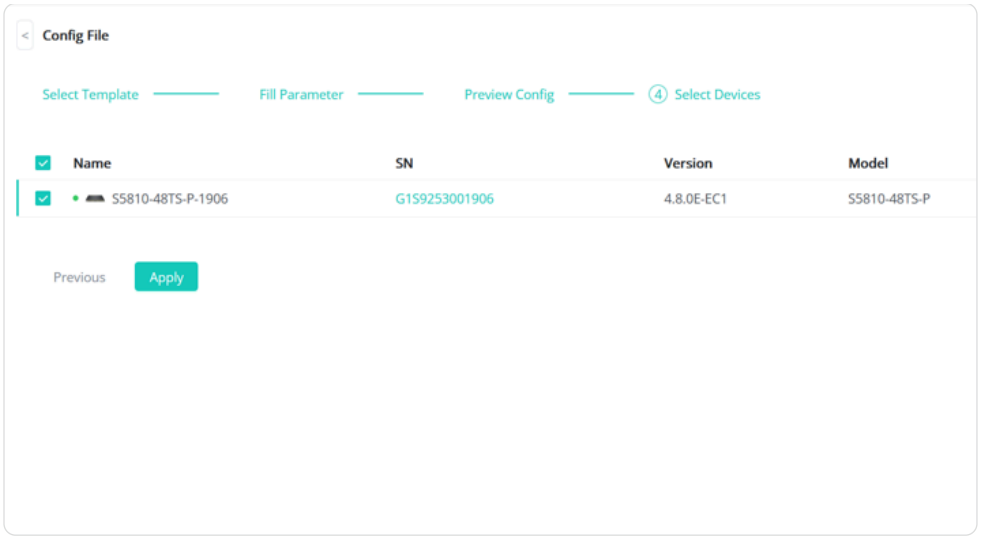
5. In the **Preview Config** tab, check the CLI commands generated based on the provided parameter values, and then click **Next**.

> **NOTE**
>
> You can edit the CLI commands here. Be sure to click **Save** to save the changes.



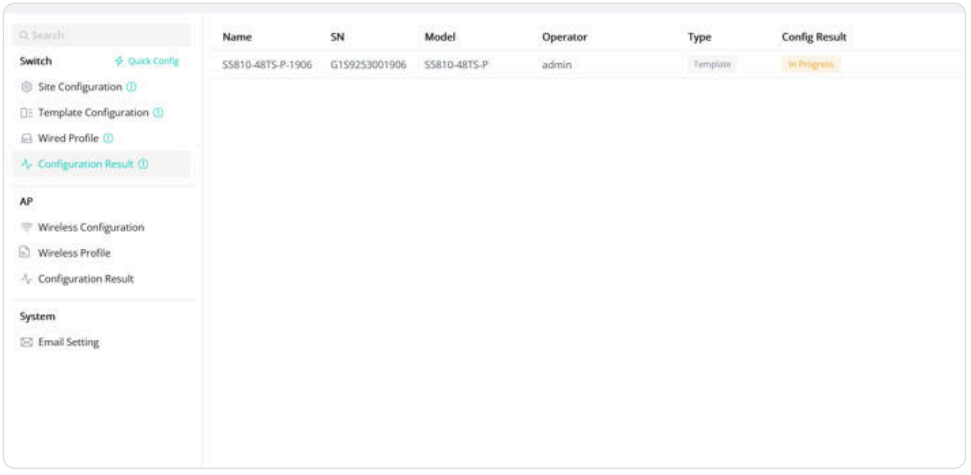
6. In the **Select Devices** tab, select the switches to be configured.

> **NOTE**
>
> You can select only the PicOS switches that meet all the following requirements:
>
> - The switches are managed by AmpCon-Campus and are currently online (connected to AmpCon-Campus).
> - No configurations are being pushed or waiting to be pushed to the switches.
> - No upgrade tasks are running on the switches.



7. Click **Apply**. You will be redirected to the “Configuration Result” page.

   On the “Configuration Result” page, check the configuration results.

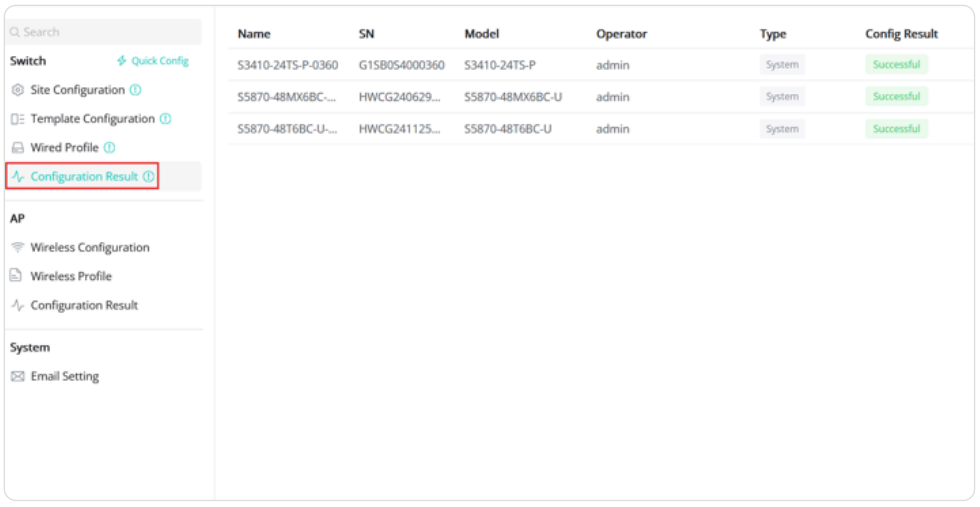


Checking Configuration Results

On the “Configuration Result” page, you can check the configuration push results of PicOS switches.

Procedure

1. In the AmpCon-Campus UI, select the site to which the PicOS switches belong.
2. Click the **Settings** icon from the navigation bar, and then click **Configuration Result** in the **Switch** section.



3. On the “Configuration Result” page, check the configuration results for each switch in the selected site.

> **NOTEs**
>
> - Configuration results are displayed on a per-switch basis, with only the latest configuration record shown for each switch in the site.
> - After a PicOS switch is moved to another site, its configuration results are also moved to the new site.

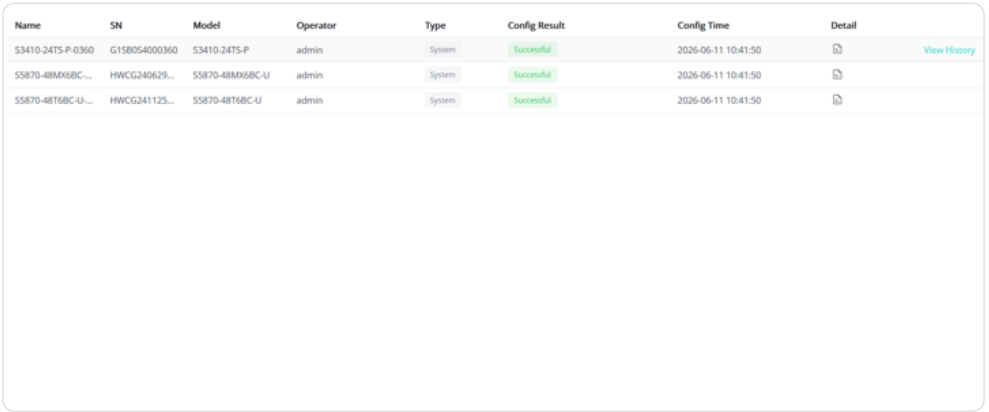


Table 1. Configuration Result Parameters

Parameter	Description
Name	The alias of the switch.
SN	The serial number of the switch.
Model	The model of the switch.
Operator	The AmpCon-Campus user who executes the configuration operation.
Type	The type of the configuration. You can see the following types: • **System:** Indicates site-level system configurations. • **L3 Interface & DHCP:** Indicates L3 interface and DHCP configurations. • **Port:** Indicates port configurations. • **OSPF:** Indicates OSPF configurations. • **Static Route:** Indicates static route configurations. • **Template:** Indicates template configurations.
Config Result	The result of the configuration. You can see the following configuration results: • **In Progress:** The configurations are being pushed to the switch. • **Pending:** The configuration push is queued and waiting to be executed. • **Successful:** The configurations are pushed to the switch successfully. • **Failed:** The configurations fail to be pushed to the switch.
Config Time	The time when the configuration task started. If the task has not started yet, the task creation time is displayed.

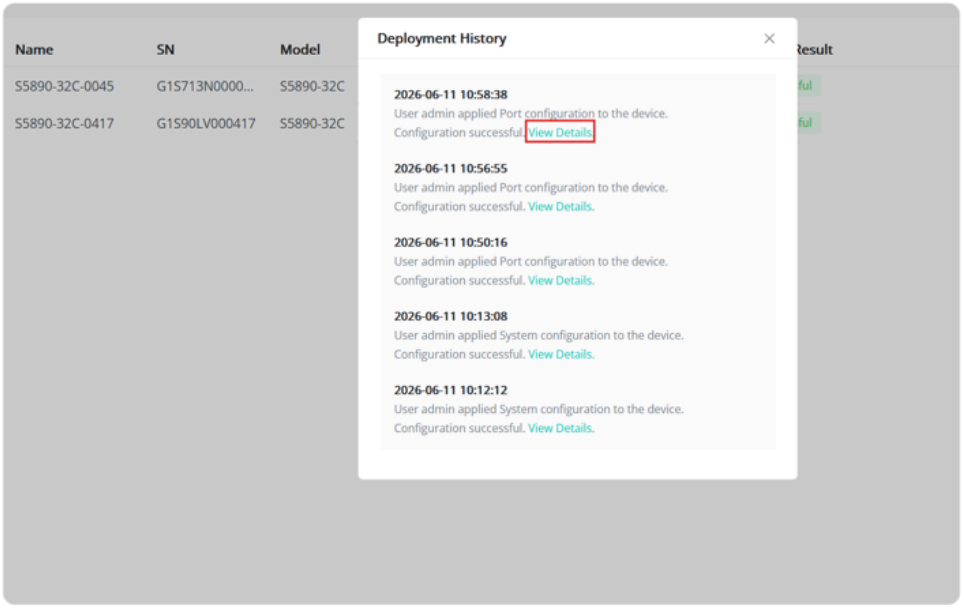
4. Optional: To check configuration result details, locate the configuration result, and then click the detail icon in the **Detail** column.

> **NOTE**
>
> If the **Config Result** of a switch is **In Progress** or **Pending**, you cannot see the detail icon, and you can see only **--**.



5. Optional: To view the configuration history, hover over the switch, and then click **View History**.

   In the pop-up window, view the configuration history of the switch. For each configuration history item, click **View Details** to check configuration result details.



Comparing Switch Configurations

In the AmpCon-Campus UI, you can compare configurations from external files or from managed PicOS switches.

Guidelines
Procedure

Guidelines

- AmpCon-Campus supports the following comparison scenarios:
  - Compare configurations between two external files.
  - Compare running or backup configurations from the same or different PicOS switches.
  - Compare configurations from an external file with running or backup configurations on a PicOS switch.
- Ensure that the PicOS switches to be compared are onboarded to AmpCon-Campus successfully.
- Running configurations refer to the configurations currently running on a switch. Backup configurations refer to the configuration files backed up as described in Backing Up Configurations.

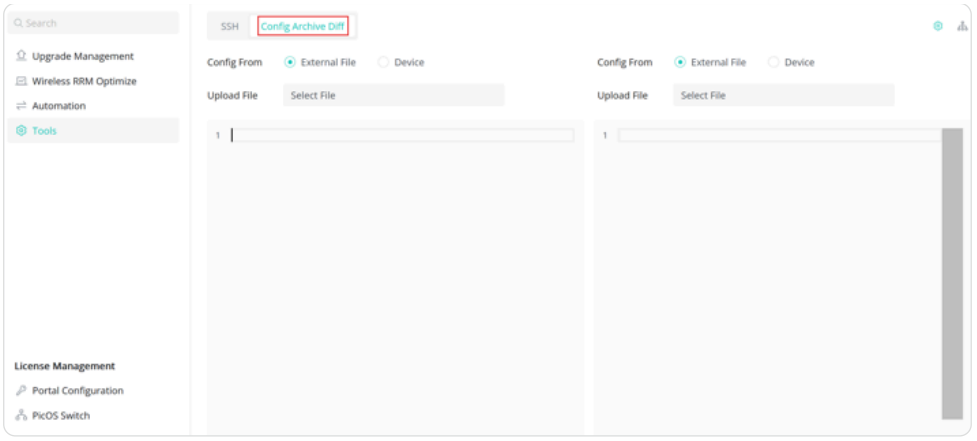
Procedure

1. In the AmpCon-Campus UI, select a site.

   NOTEs

   - To compare configurations from managed switches, you must select the site to which those switches belong.
   - You cannot compare configurations from two managed switches belonging to different sites.
   - To compare configurations between two external files, you don't need to select a site.

2. Click the **Maintain** icon from the navigation bar.
3. In the sidebar, click **Tools**, and then click the **Config Archive Diff** tab. You can see two comparison panels.

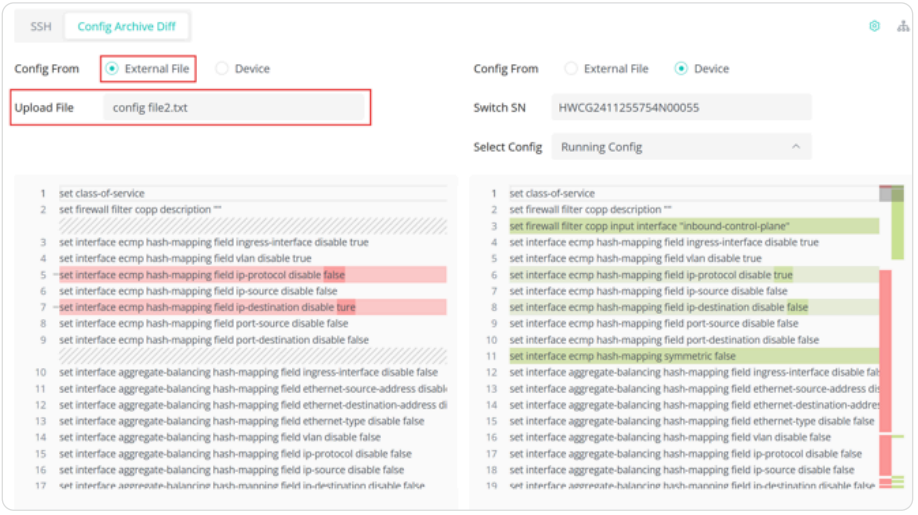


4. In each comparison panel, upload an external configuration file, or select running or backup configurations from a managed switch.

- To upload an external configuration file, follow these steps:

  a. In the **Config From** section, select **External File**.

  b. In the **Upload File** section, click **Select File**, and then select an external configuration file (.txt file, .conf file, or .cfg file) in the pop-up window.



- To select running or backup configurations from a managed switch, follow these steps:

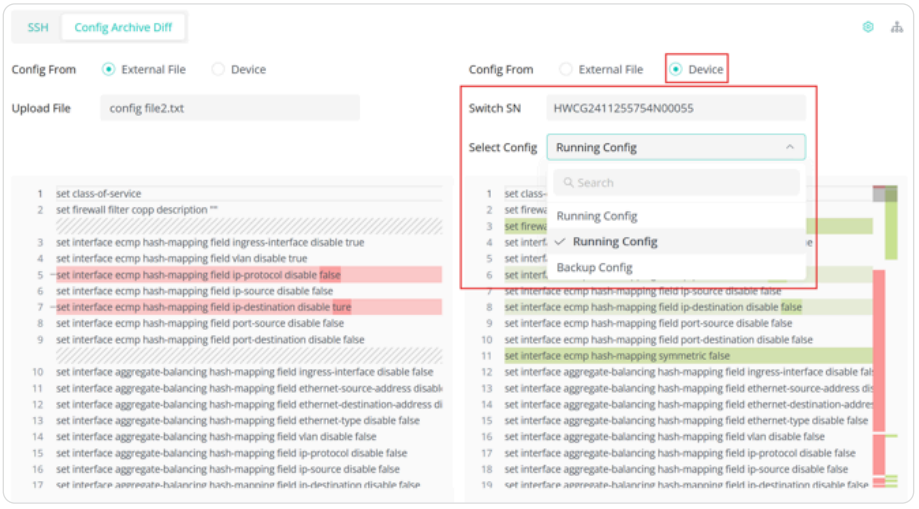
  a. In the **Config From** section, select **Device**.

  b. In the **Switch SN** section, click **Select Switch**. In the pop-up window, select a switch, and then click **Apply**.

  c. In the **Select Config** drop-down list, select **Running Config** or a backup configuration file.

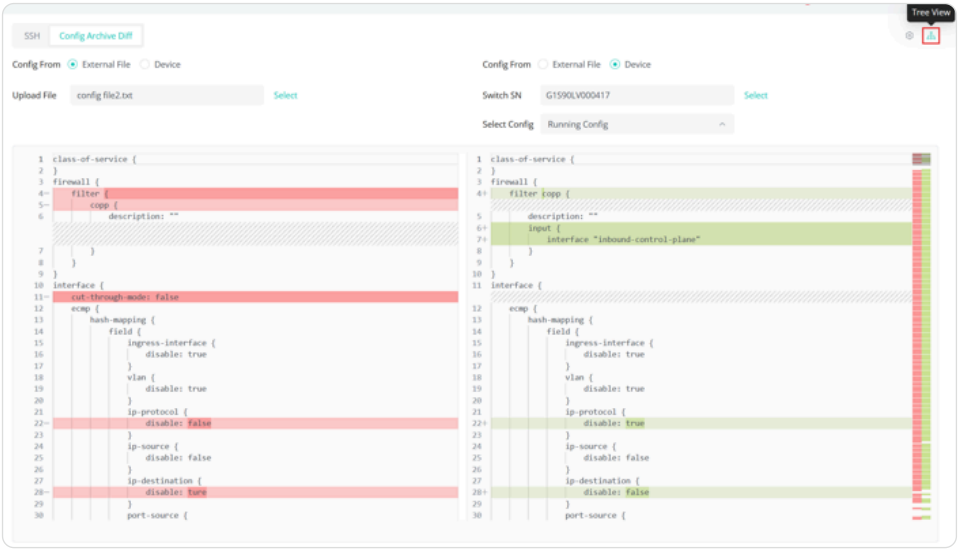
NOTEs

- For offline switches (disconnected from AmpCon-Campus) or switches not managed by AmpCon-Campus, **do not** select **Running Config**. This is because AmpCon-Campus cannot retrieve the current configurations from these switches.
- If no backup configuration files are displayed, you can create a new backup configuration file. For more information, see Backing Up Configurations.



5. Check the differences between these two comparison panels. The areas highlighted in red and green indicate the differences.

   By default, the configurations are displayed in the set view. To display configurations in the tree view, click the **Tree View** icon. To display configurations in the set view, click the **Set View** icon.



End-to-End Campus Deployment Scenario

AmpCon-Campus supports Zero Touch Provisioning (ZTP) and multiple configuration methods, accelerating end-to-end campus deployment.

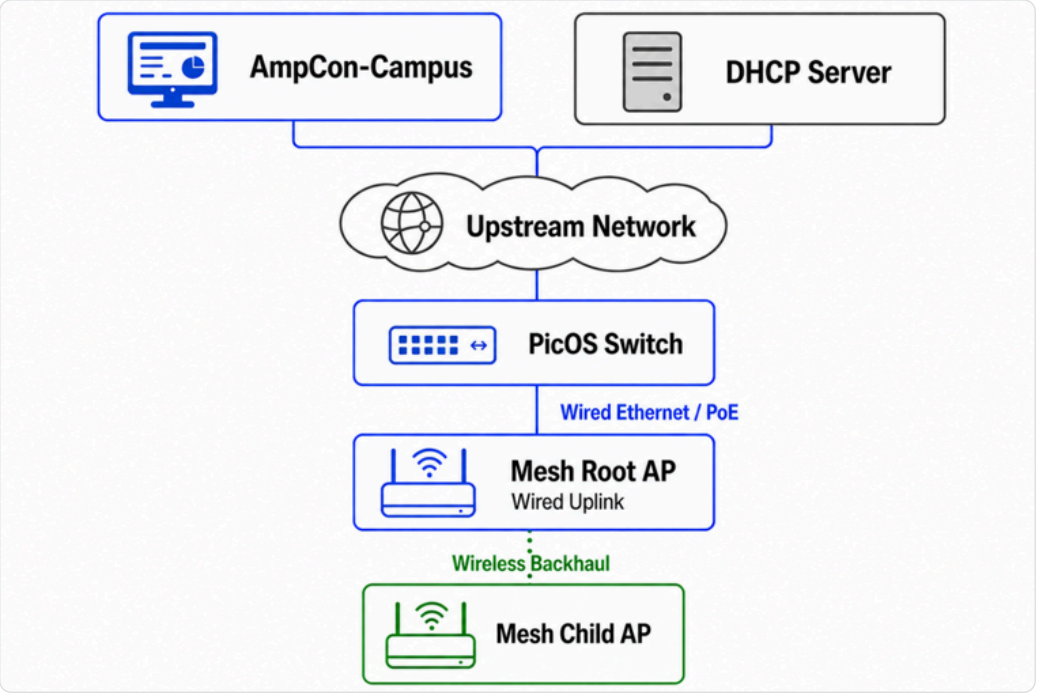
This topic describes the workflow of end-to-end deployment for a new campus network.

- Scenario Description
- Prerequisites
- Procedure
  - Importing PicOS Switches and APs
  - Adding Site-Level Configurations
  - Enabling Mesh Root APs
  - Completing ZTP and Verifying ZTP Results
  - Provisioning Services
- Verifying the Deployment
- What to Do Next

Scenario Description

In the following scenario, a company needs to deploy a new campus network containing PicOS switches and access points (APs). The wireless network in the campus is a mesh network containing one mesh root AP and one mesh child AP.

Figure 1. Campus Network Scenario



Before the devices (PicOS switches and APs) arrive, the administrators prepare for the deployment, such as completing the prerequisite tasks, importing devices to AmpCon-Campus, adding site configurations, and preparing quick configuration parameters, wireless policies, and configuration templates.

After the devices arrive, on-site personnel are mainly responsible for installing, cabling, and powering on the devices. Then, the devices can be successfully onboarded to AmpCon-Campus and retrieve the site-level configurations.

After onboarding, the administrators can use appropriate configuration methods of AmpCon-Campus to provision services and continuously monitor the network.

Prerequisites

Before you start the deployment, complete the following prerequisite tasks. Otherwise, the deployment will fail.

Table 1. Deployment Prerequisites

Task	Reference Link
The management network, service VLANs, gateways, DHCP services, routes, SSIDs, and authentication methods have been planned.	• No Reference Link
The PicOS switches and APs are supported by AmpCon-Campus.	• Supported PicOS Switches for 3.0.0 • Supported APs for 3.0.0
The site to which the PicOS switches and APs belong has been created.	• Managing Sites
The prerequisites for onboarding PicOS switches and APs are met. **NOTE** In this scenario, you do not need to plug in and power on the switches and APs and complete their uplink connection during the **Prerequisites** phase. This task is performed in the Completing ZTP and Verifying ZTP Results phase.	• Onboarding PicOS Switches - Prerequisites • Onboarding APs - Prerequisites

Procedure

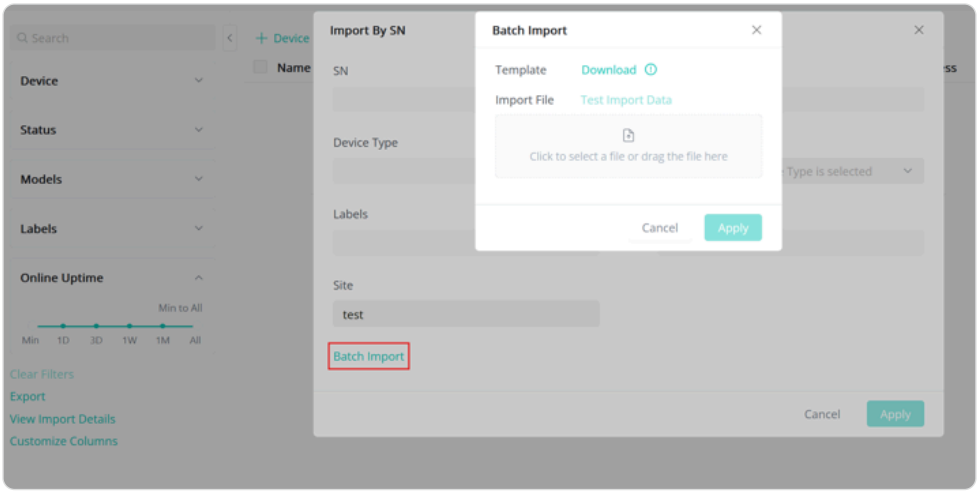
Importing PicOS Switches and APs

1. In the AmpCon-Campus UI, select the prepared site.
2. Click the **Devices** icon from the navigation bar.

3. On the “Devices” page, hover over **+ Device**, and then click **Import by SN**.
4. In the pop-up window, click **Batch Import**. In the new pop-up window, click **Download** to download the template file.

   Open the template file, and then enter the correct information for each PicOS switch and AP.

   In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. Then, click **Apply**.

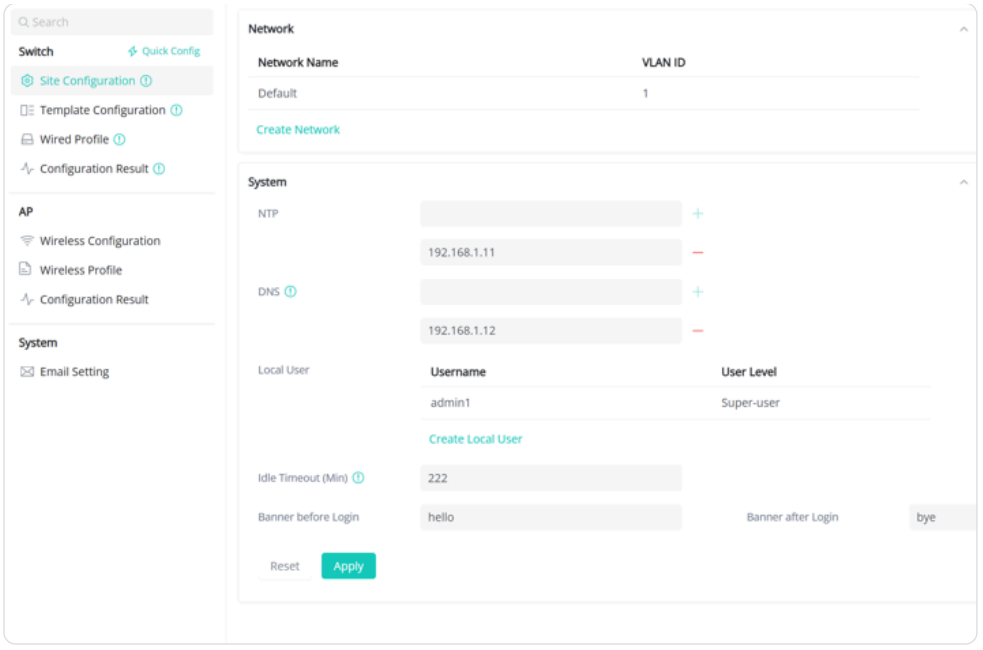


Adding Site-Level Configurations

1. Click the **Settings** icon from the navigation bar.
2. Click **Site Configuration** in the **Switch** section of the sidebar. Configure site-level wired configurations such as NTP and DNS, and then click **Apply**.

   For more information, see Applying Site Configurations.

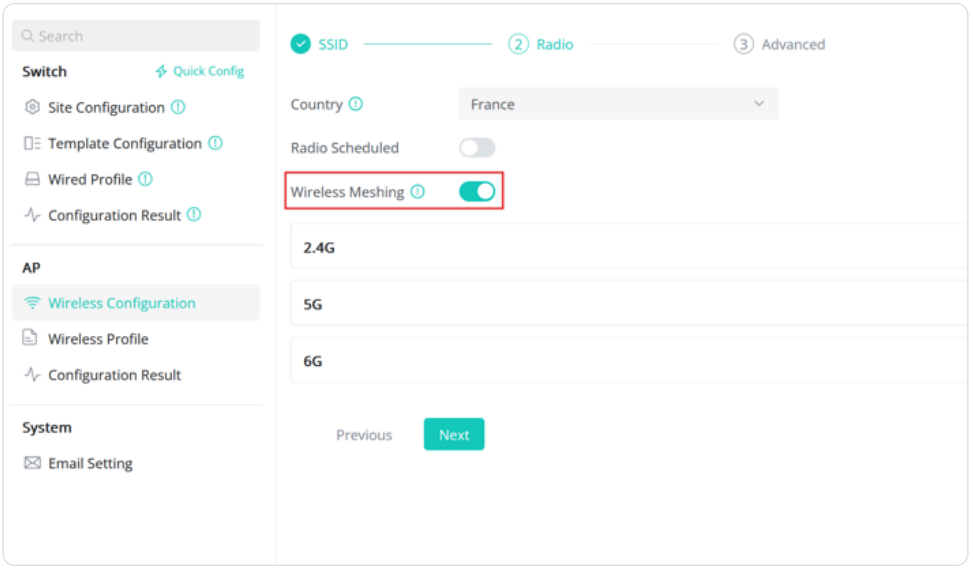
> **NOTE**
>
> - Network-related site configurations are pushed to PicOS switches only when you apply port configurations or quick configurations referencing the added networks.
> - After you modify system-related site configurations and click **Apply**, the site-level system configurations will be directly pushed to associated switches.



3. Click **Wireless Configuration** in the **AP** section of the sidebar. Configure site-level wireless configurations such as SSID, radio, and advanced configurations, and then click **Apply**.

   For more information, see Configuring Wireless Networks.

> **NOTE**
>
> Ensure that **Wireless Meshing** is enabled.



Enabling Mesh Root APs

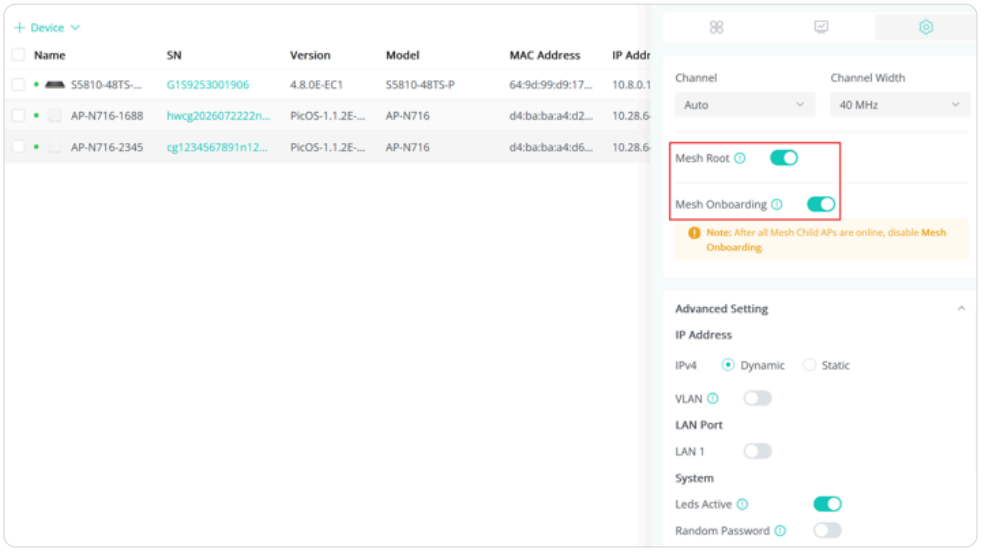
1. On the “Devices” page, click the AP that will serve as a mesh root AP. A side panel is displayed on the right.
2. Click the **Setting** tab of the side panel, toggle on **Mesh Root** to enable this AP as a mesh root AP, and ensure **Mesh Onboarding** is also enabled. Then, click **Apply**.

   For more information, see Configurations and Operations of an AP.

NOTEs

- After all mesh child APs are online, disable **Mesh Onboarding** for security concerns.
- When **Mesh Onboarding** is enabled, the mesh root AP broadcasts an SSID named **Pica8WiFi-Onboarding**.

  New mesh child APs will connect to this SSID in STA mode by using certificates to securely retrieve their initial network settings and platform configurations.

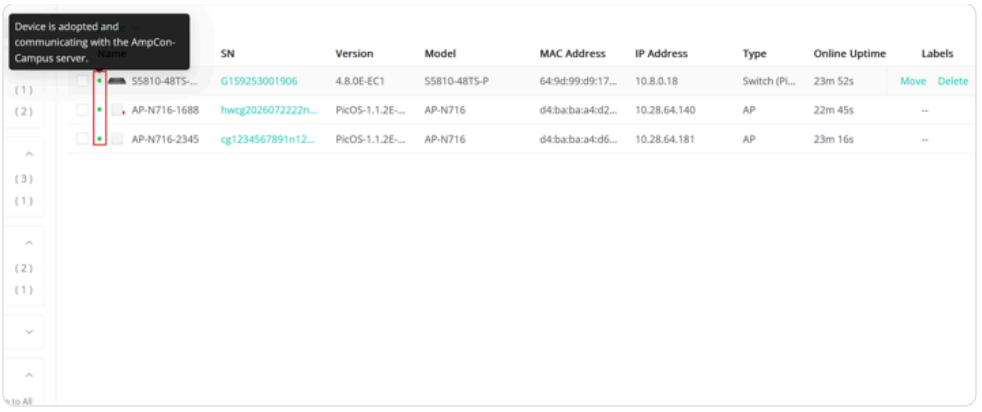


Completing ZTP and Verifying ZTP Results

1. Plug in and power on the PicOS switches and APs, and complete their uplink connections.

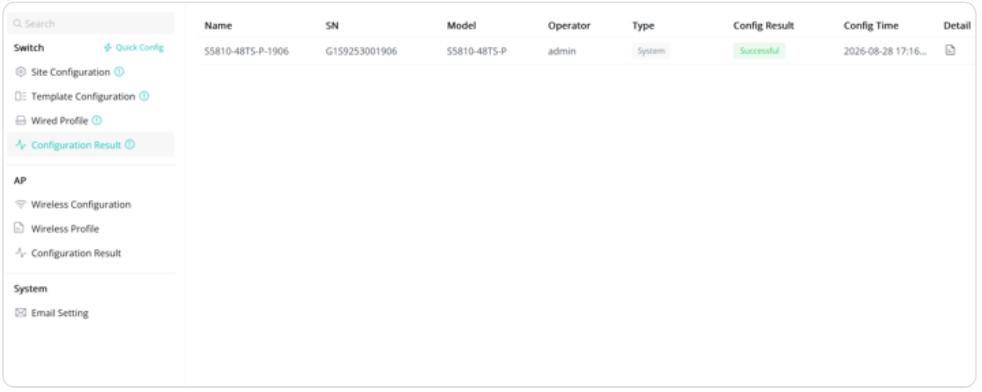
   Then, the PicOS switches and APs can connect to AmpCon-Campus and complete the ZTP process. The site configurations are automatically pushed to the PicOS switches and APs.
2. On the “Devices” page, verify that all PicOS switches and APs are online (connected to AmpCon-Campus).

   You can check the status circle in the **Name** column. The color green means that the PicOS switch or AP is online.

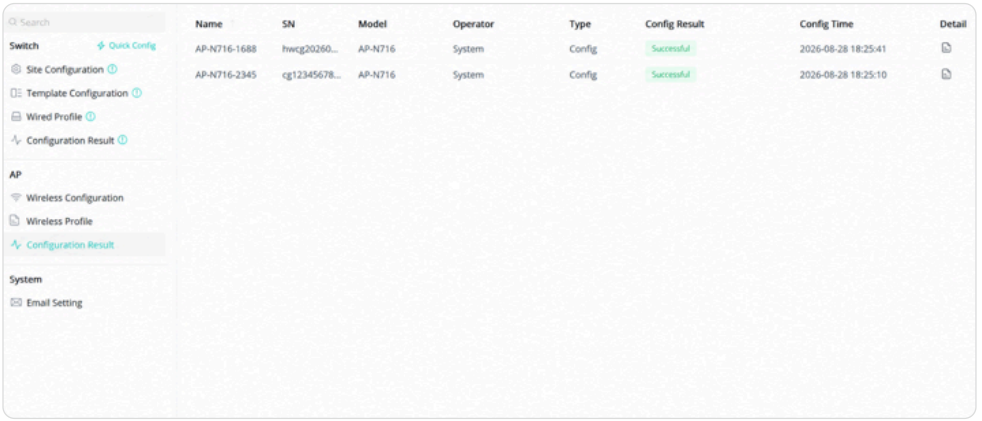


3. Click the **Settings** icon from the navigation bar, and then click **Configuration Result** in the **Switch** section.

   Verify that the site configurations are successfully pushed to the PicOS switches. For more information, see Checking Configuration Results.



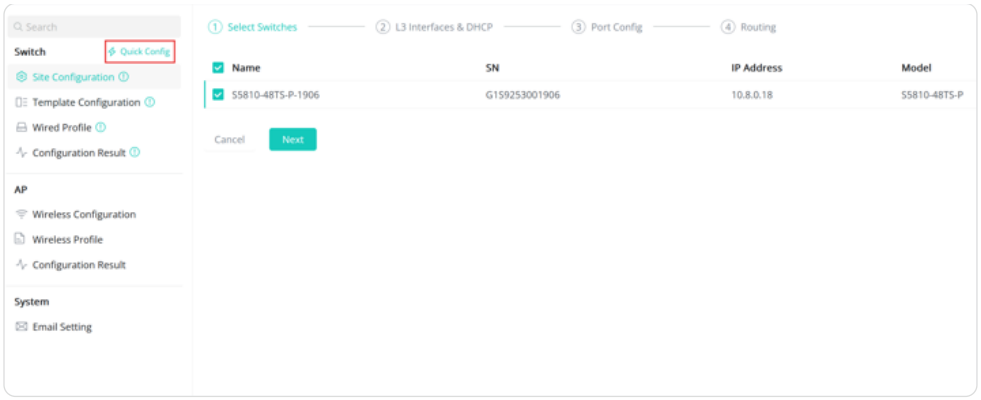
4. Click **Configuration Result** in the **AP** section. Verify that the site configurations are successfully pushed to the APs.



Provisioning Services

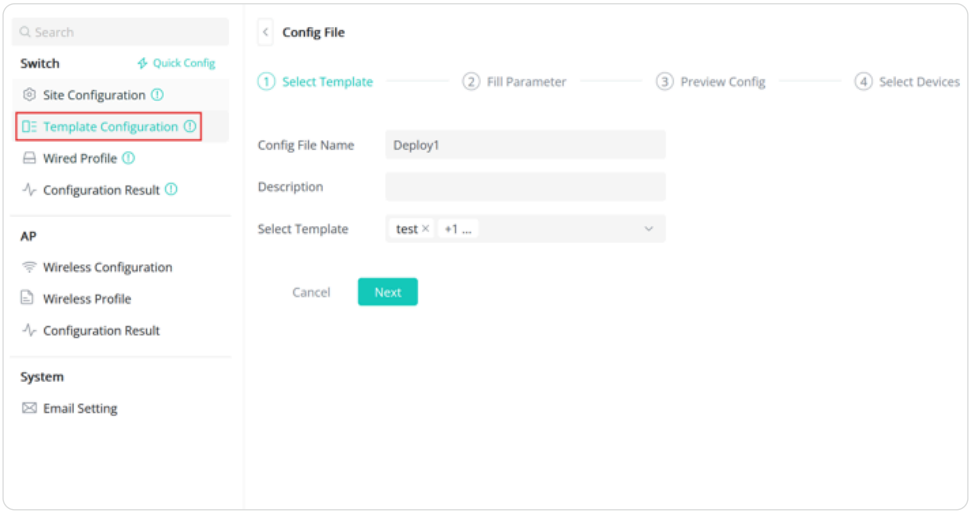
1. Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar.

   In the **Quick Config** wizard, configure switch configurations such as Layer 3 interfaces, ports, and routes.
   For more information, see Applying Quick Configurations.



2. For specific switch configurations that can't be pushed through other configuration methods of AmpCon-Campus, click **Template Configuration** in the sidebar to apply template configurations.

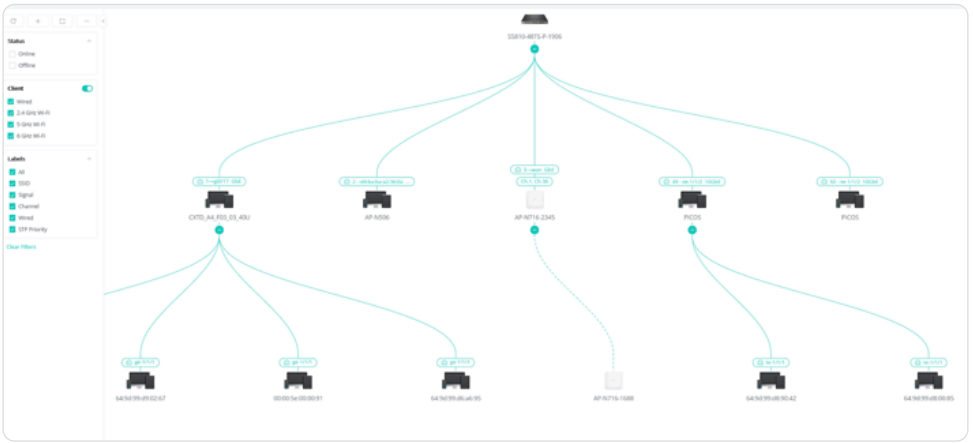
   For more information, see Applying Template Configurations.



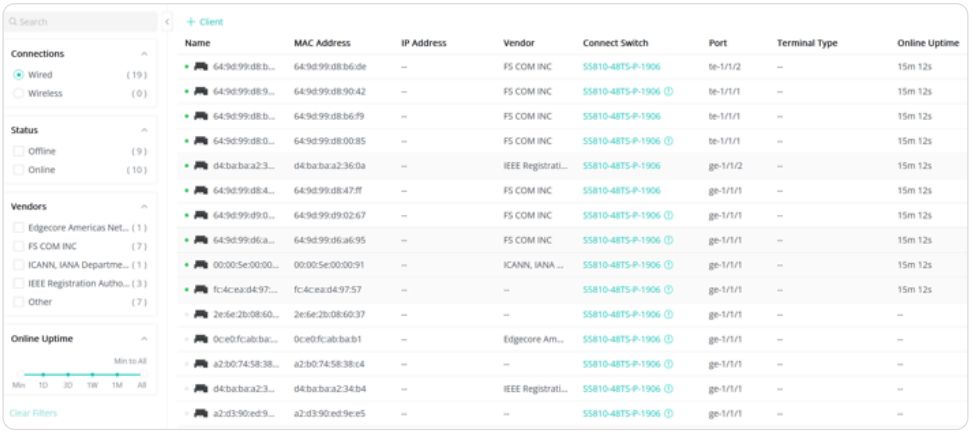
3. Click **Configuration Result** in the **Switch** section. Verify that the quick configurations and template configurations are successfully pushed to the PicOS switches.

Verifying the Deployment

1. On the "Topology" page, verify that the PicOS switches, APs, clients, and their links are displayed correctly. For more information, see Topology.



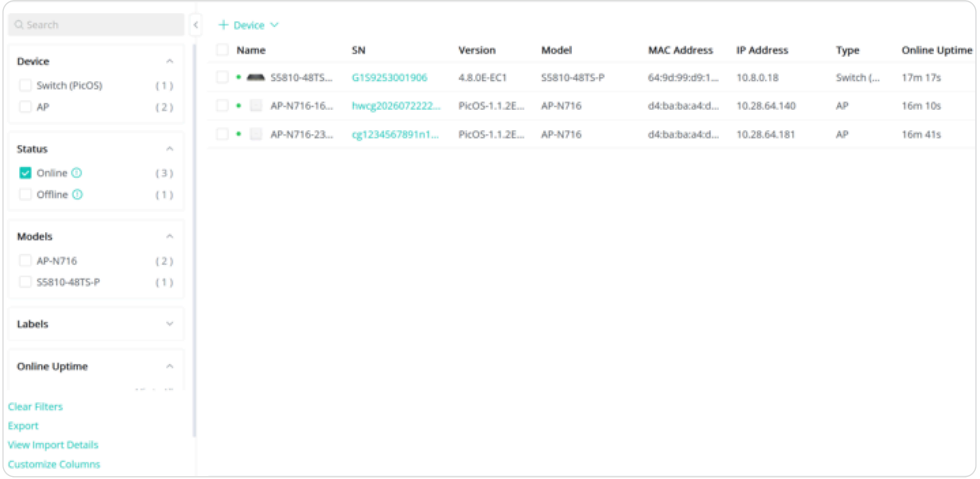
2. On the “Clients” page, verify that wired clients are connected to the PicOS switches and obtain correct IP addresses. For more information, see Wired Clients.



3. On the “Dashboard” page, verify that wireless information (such as top APs, traffic volume, and client counts) is displayed. For more information, see Dashboard.



4. On the “Devices” page, verify that the mesh child APs are connected to the mesh root AP and are broadcasting the configured service SSIDs. For more information, see Access Points.

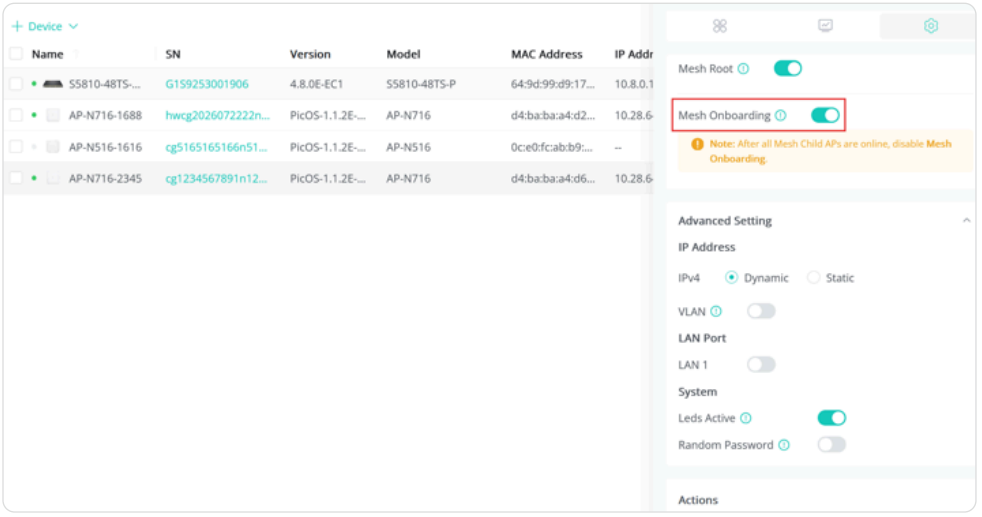


What to Do Next

After the campus network is ready, you might need to add new PicOS switches and mesh child APs. In this case, you can reuse existing site configurations, minimizing on-site operations and disruption to the existing network. Follow these steps:

1. On the “Devices” page, click the mesh root AP. Click the **Setting** tab of the side panel, toggle on **Mesh Onboarding**, and then click **Apply**.

   > **NOTE**
   >
   > After all mesh child APs are online, disable **Mesh Onboarding** for security concerns.



2. Onboard the PicOS switches and APs to AmpCon-Campus. For more information, see Onboarding PicOS Switches and Onboarding APs.

   > **NOTE**
   >
   > Ensure that the PicOS switches and APs belong to the prepared site. During onboarding, site configurations will be automatically pushed to the PicOS switches and APs.

3. Click the **Settings** icon from the navigation bar, and then click **Quick Config** in the sidebar.

   In the **Quick Config** wizard, configure switch configurations such as Layer 3 interfaces, DHCP, ports, and routes, and push the configurations to the newly onboarded PicOS switches.

4. For specific switch configurations that can’t be pushed through other configuration methods of AmpCon-Campus, click **Template Configuration** in the sidebar to apply template configurations.
5. Verify the following points:

- On the “Devices” page, verify that the newly onboarded PicOS switches and APs are online (connected to AmpCon-Campus).
- Click **Configuration Result** in the **Switch** section. Verify that the site configurations, quick configurations, and template configurations are successfully pushed to the PicOS switches.
- Click **Configuration Result** in the **AP** section. Verify that the site configurations are successfully pushed to the APs.
- On the “Topology” page, verify that the newly onboarded PicOS switches and APs join the current network topology.
- Verify that the mesh child APs are connected to the mesh root AP and are broadcasting the configured service SSIDs.

Managing PicOS Switches

After onboarding PicOS switches, you can manage these switches with AmpCon-Campus.

AmpCon-Campus streamlines lifecycle management of PicOS switches, helping you increase network management efficiency and focus on more strategic tasks.

See the following child topics:

- Accessing Switches
- Deleting Switches
- Rebooting Switches
- Upgrading Switches
- Managing License Portals
- Managing PicOS Licenses
- Moving Switches to Another Site
- Backing Up Configurations
- Return Merchandise Authorization

Accessing Switches

After successfully onboarding PicOS switches to AmpCon-Campus, you can connect to a PicOS switch from the AmpCon-Campus UI by creating an SSH session.

AmpCon-Campus supports two types of authentication: password authentication and SSH key authentication.

Guidelines
Password Authentication
SSH Key Authentication

Guidelines

- Password authentication is suitable for environments with lower security and higher usability demands.
- SSH key authentication provides stronger security for high-security scenarios. During password authentication, a password is transmitted over the network, which might expose passwords to interception. In contrast, the private key in SSH keys is uploaded to AmpCon-Campus and used to authenticate with the target switch, reducing theft risk and enhancing session security.
- Only the PicOS switches that are currently online (connected to AmpCon-Campus) can be accessed through SSH sessions.

Password Authentication

To access a PicOS switch by using password authentication, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, click the switch. In the side panel on the right, click the **Setting** tab.
4. In the **Actions** section, click **SSH**. In the pop-up window, input the following information:

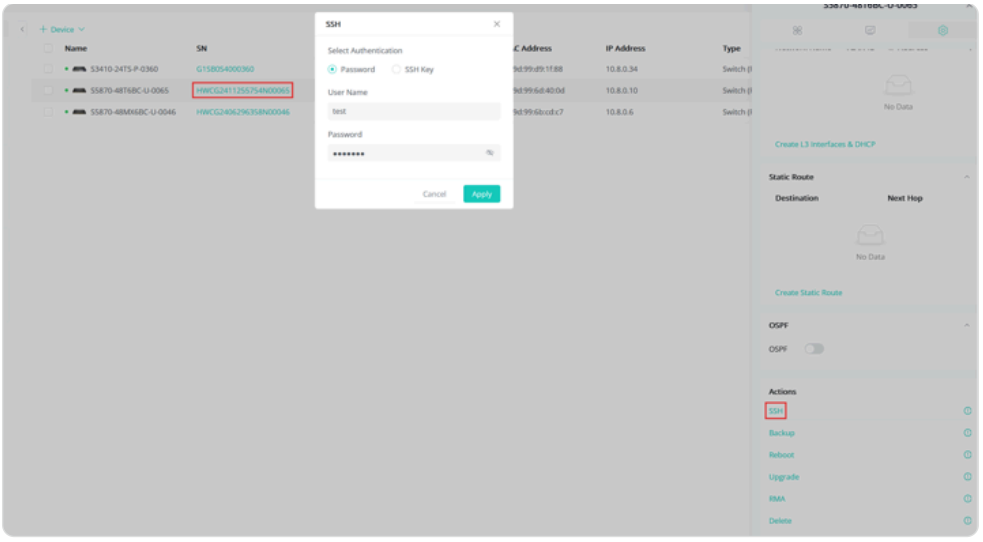


Table 1. Password Parameters

Parameter	Description
Select Authentication	Select **Password**.
User Name	The username to log in to the switch. • The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. • The username can contain at most 32 characters. • Uppercase letters are not supported on S3270 and S3410 series switches. • Only ASCII characters are supported.
Password	The password of the user. **NOTE** Ensure the username and password are valid for switch login. Otherwise, the SSH session cannot be established.

5. Click **Apply**.

SSH Key Authentication

SSH key authentication requires a public key and a private key. When you log in to the AmpCon-Campus UI and access a switch through SSH keys, the session between AmpCon-

Campus and the target switch is authenticated by using the private key uploaded in the AmpCon-Campus UI and the public key stored on the switch.

To access a switch by using SSH key authentication, follow these steps:

Prerequisites

- On a server (for example, 10.56.xx.xx), run the **ssh-keygen** command to generate the SSH keys (including a public key and a private key).
- Put the generated public key in the **~/.ssh/authorized_keys** file of the switch to be accessed. You can use the **scp** command. For example, run the following command on the switch.

  sudo scp pica8@10.56.xx.xx:/home/pica8/.ssh/id_rsa.pub /home/admin/.ssh/authorized_keys

  Then, the public key will be copied from the server 10.56.xx.xx to the switch.

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, click the switch. In the side panel on the right, click the **Setting** tab.
4. In the **Actions** section, click **SSH**. In the pop-up window, input the following information:

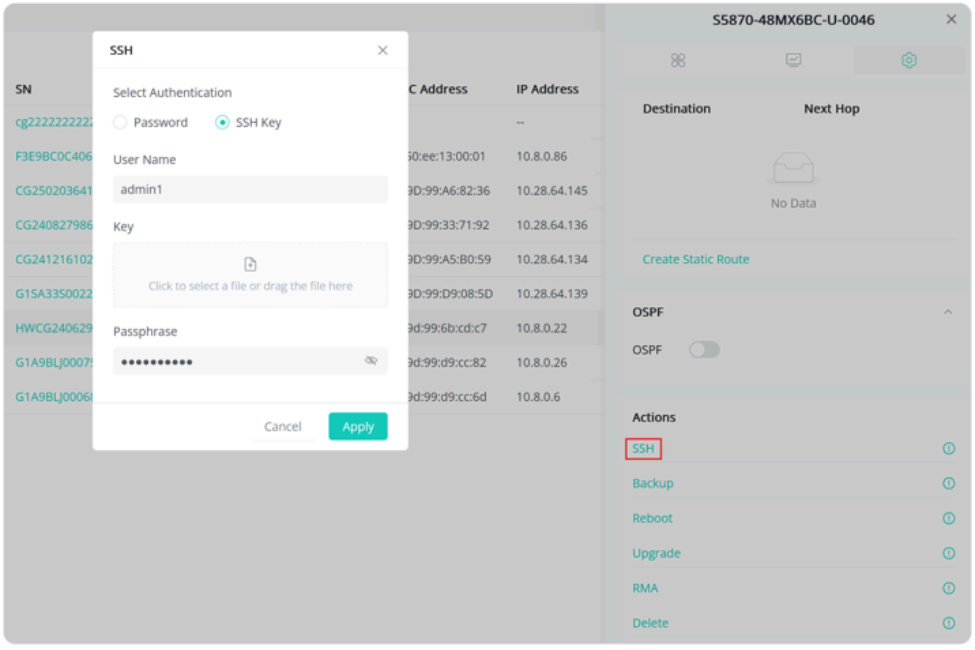


Table 2. SSH Key Parameters

Parameter	Description

Select Authentication	Select **SSH Key**.
User Name	The username to log in to the switch. • The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. • The username can contain at most 32 characters. • Uppercase letters are not supported on S3270 and S3410 series switches. • Only ASCII characters are supported.
Key	The private key generated by using the **ssh-keygen** command. Click **Select File** to upload the private key file. The size of the private key file cannot exceed 16 KB. **NOTE** Ensure the username and key file are valid for switch login. Otherwise, the SSH session cannot be established.
Passphrase	Optional. The password used to protect the SSH keys. You can choose whether to specify a passphrase when generating the SSH keys. If no passphrase was set during key generation, leave this field empty.

5. Click **Apply**.

Deleting Switches

On the “Devices” page, you can delete a single switch or multiple PicOS switches in batches. The deleted switches are removed from the device list and are not managed by AmpCon-Campus.

Guideline
Deleting a Single Switch
Deleting Multiple Switches

Guideline

The PicOS switches in any of the following cases cannot be deleted:

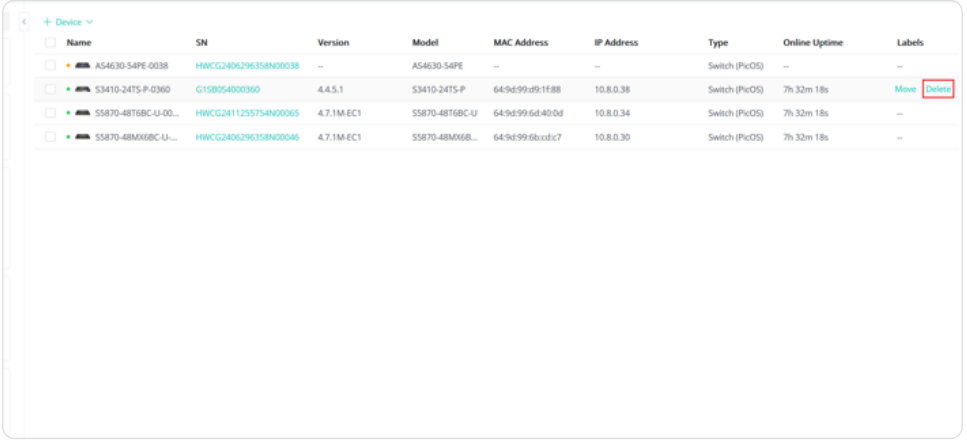
- The switches are in **Provisioning** status, which means AmpCon-Campus is verifying authentication information of the switch or establishing an OpenVPN tunnel with the switch.
- Configurations are being pushed or waiting to be pushed to the switches.
- Reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
- The switches are being moved to another site.
- **License Audit** or **License Action** is currently in progress on the switches.

Deleting a Single Switch

To delete a single PicOS switch, follow these steps:

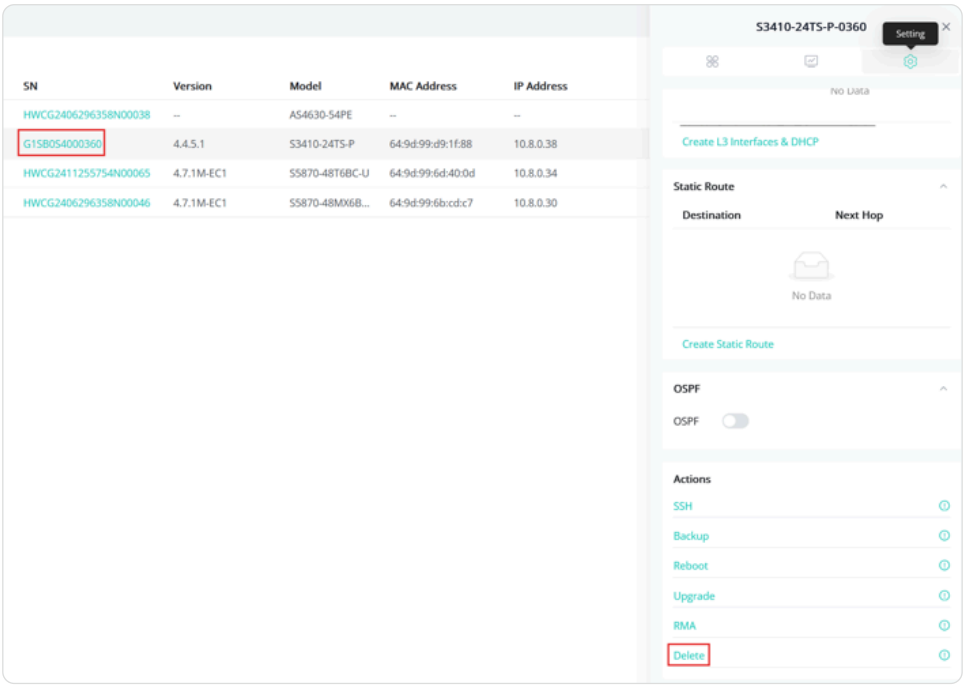
1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, delete the switch through one of the following ways:

- Hover over the switch, and then click **Delete**. In the pop-up window, click **Yes** to confirm the action.



- Click the switch. In the side panel, click the **Setting** tab, and then click **Delete** in the **Actions** section.

  In the pop-up window, click **Yes** to confirm the action.

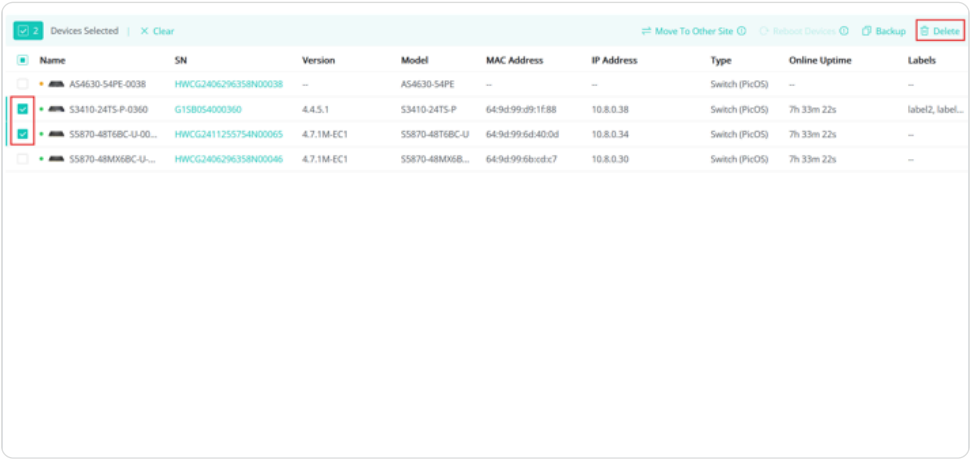


Deleting Multiple Switches

To delete multiple PicOS switches, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, select the switches to be deleted, and then click **Delete**.

   To clear the switch selection, click **Clear**.



4. In the pop-up window, click **Yes** to confirm the action.

Rebooting Switches

After successfully onboarding PicOS switches to AmpCon-Campus, you can reboot a PicOS switch. During reboot, the switch will briefly go offline and then come back online to AmpCon-Campus.

Guideline
Procedure

Guideline

Only the PicOS switches meeting all the following conditions can be rebooted:

- The switches are currently online (connected to AmpCon-Campus).
- The switches are not being moved to another site.
- No configurations are being pushed or waiting to be pushed to the switches.
- No reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
- No **License Audit** or **License Action** is currently in progress on the switches.

Procedure

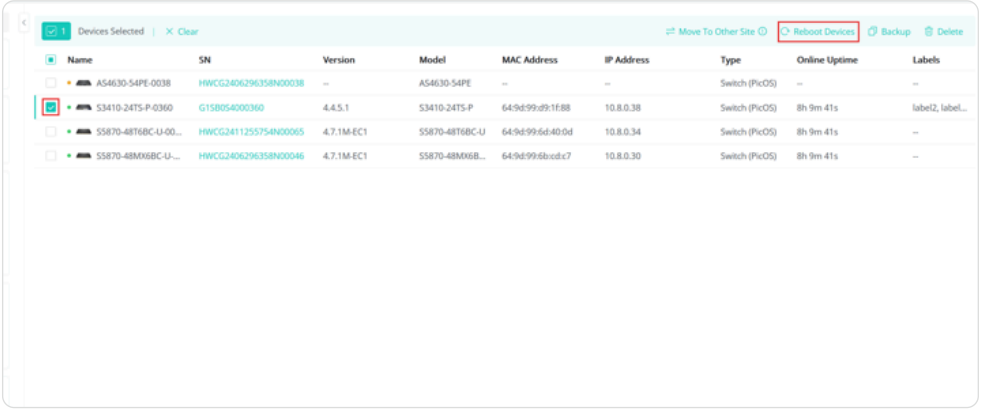
To reboot a single PicOS switch, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, reboot the switch by using one of the following ways:

- Select the switch, and then click **Reboot Devices** at the top.

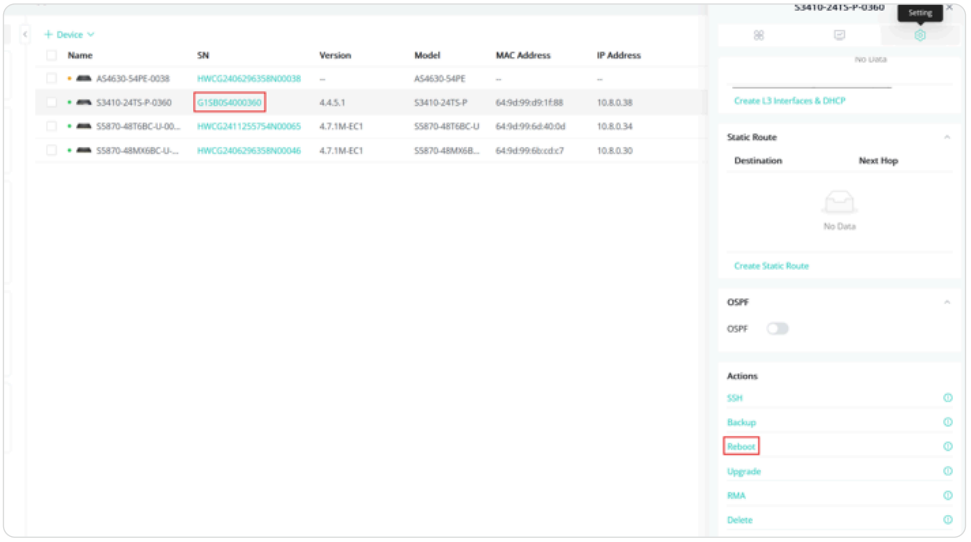
  In the pop-up window, click **Yes** to confirm the reboot.

> **NOTE**
>
> Batch reboot is not supported. The **Reboot Devices** button will be grayed out if multiple switches are selected.



- Click the switch in the device list. In the **Setting** tab of the side panel, click **Reboot**.

  In the pop-up window, click **Yes** to confirm the reboot.



Upgrading Switches

After successfully onboarding PicOS switches to AmpCon-Campus, you can upload PicOS images, upgrade switches individually or in bulk, schedule upgrade time, and manage upgrade tasks.

You can schedule automatic upgrades during off-peak hours (such as at night or on holidays), so that your services experience minimal disruption.

- Guidelines
- Prerequisites
- Procedure
  - Checking Images
  - Uploading Images
  - Upgrading Multiple Switches
  - Upgrading a Single Switch
  - Checking Upgrade Task Results
- Optional Operations
  - Managing Upgrade Tasks
  - Uploading MD5 Files
  - Deleting PicOS Images

Guidelines

Only the PicOS switches that meet all the following conditions can be upgraded:

- The switches are not being moved to another site.
- No **License Audit** or **License Action** is currently in progress on the switches.
- No reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
- No configurations are being pushed or waiting to be pushed to the switches.

Prerequisites

Before upgrading PicOS switches, ensure that the following prerequisites are met:

Table 1. Prerequisites

Prerequisite	Reference Link
The PicOS switches to be upgraded are onboarded to AmpCon-Campus.	• Onboarding PicOS Switches
The PicOS switches to be upgraded are online (connected to AmpCon-Campus).	• Viewing the PicOS List

Procedure

Checking Images

Check whether the required PicOS image exists in the image list. Follow these steps:

1. Click the **Maintain** icon from the navigation bar.
2. On the “Upgrade Management” page, click the **Switch** tab.
3. In the **Switch** tab, check whether the required PicOS image exists in the image list. If not, upload the PicOS image as described in Uploading Images.

> **NOTEs**
>
> AmpCon-Campus provides some built-in PicOS images.

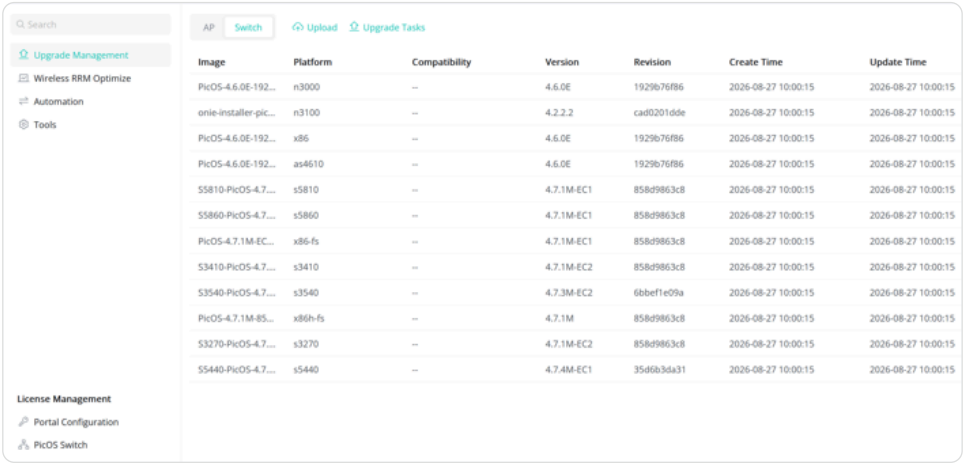


Table 2. Image Metrics

Parameter	Description
Image	The name of the PicOS image.
Platform	The switch platform compatible with the PicOS image.
Compatibility	The switch models compatible with the PicOS image. You can use the PicOS image to upgrade only these switches. **NOTEs** • Compatible switch models are displayed only for PicOS 4.9 and later images. • The metric is displayed as **--** for PicOS image versions **earlier than 4.9**. This is because AmpCon-Campus cannot retrieve compatible switch models of these image versions.

Version	The version of the PicOS image.
Revision	The revision of the PicOS image.
Create Time	The upload time of the PicOS image. **NOTE** For built-in images, the **Create Time** is the time when AmpCon-Campus is installed.
Update Time	The last time the PicOS image is updated (uploading an MD5 file for the image). **NOTEs** • For built-in images, the value is the time when AmpCon-Campus is installed. • The **Update Time** is the same as the **Create Time** if no updates are made.

Uploading Images

If the required PicOS image does not exist in the image list, upload the PicOS image. Follow these steps:

1. In the **Switch** tab of the “Upgrade Management” page, click **Upload**.
2. In the pop-up window, select **Switch** in the **Device Type** section.
3. Upload an image by using one of the following methods:

NOTEs

- When selecting an image file or entering an image URL, ensure that the image filename or URL is in the correct format and contains correct version, revision, and platform information.

  AmpCon-Campus will automatically extract version, revision, and platform information based on the image filename or URL.
- If the image filename or URL is not in the correct format, AmpCon-Campus cannot automatically extract version, revision, and platform information, and the **Platform** value will be set to **Other**.
- You can manually change the **Version**, **Revision**, and **Platform** values.

  These values must match the image file. Otherwise, even if the image is uploaded successfully, upgrade tasks that use this image might fail.
- It is not recommended to set an image's platform to **Other** because this might lead to upgrade failure for platform inconsistency.

- In the **File** tab, click the upload icon to select a PicOS image, or drag and drop the image. Then, click **Apply**.

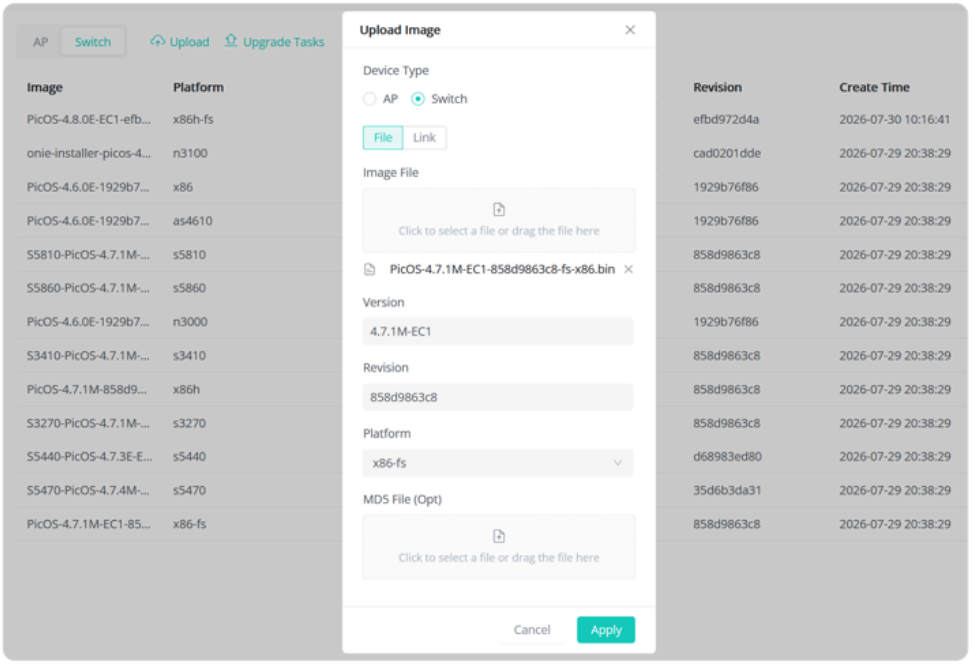
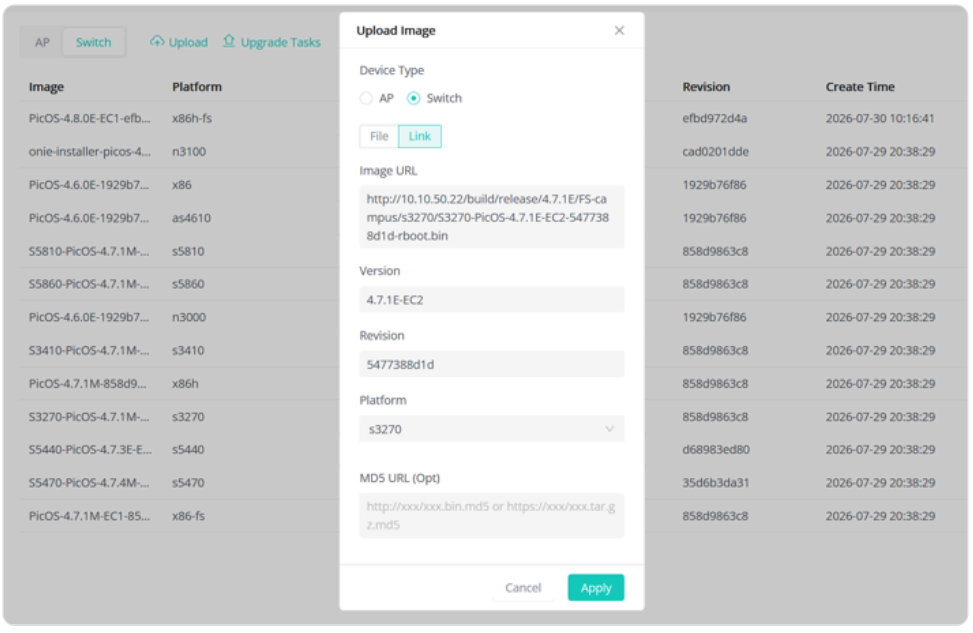


Table 3. Image Parameters

Parameter	Description

Version	The version of the PicOS image, such as **4.7.1M-EC1**.
Revision	The revision of the PicOS image, such as **858d9863c8**.
Platform	The switch platform compatible with the PicOS image, such as **as4610**.
MD5 File	Optional. Click **Select** to upload the MD5 file of the image. MD5 files are used to verify the completeness of the corresponding PicOS images. If the MD5 file does not match the image, the upgrade will fail. If the MD5 file is not uploaded, AmpCon-Campus will not verify the completeness of the PicOS image during upgrade.

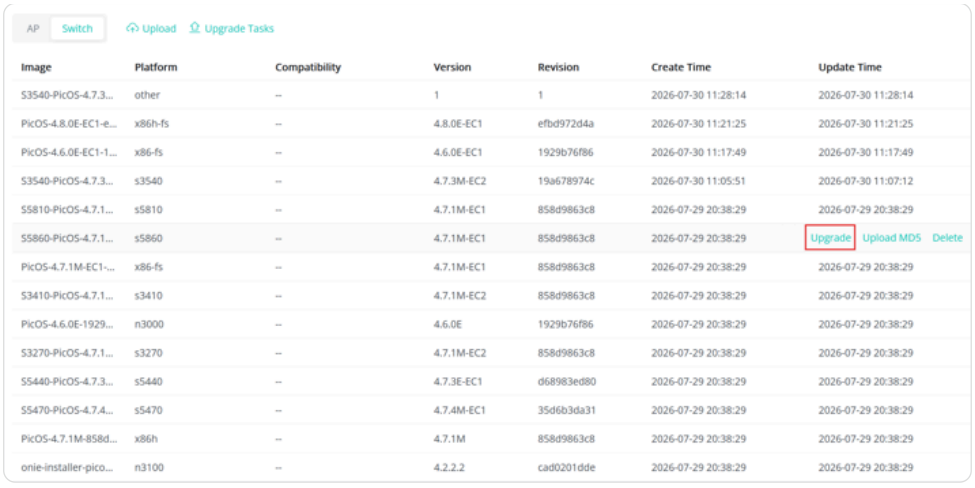
- In the **Link** tab, enter the image URL and the MD5 file URL (optional), and then click **Apply**.



Upgrading Multiple Switches

To upgrade multiple PicOS switches, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. In the **Switch** tab of the “Upgrade Management” page, hover over the PicOS image to which you want to upgrade, and then click **Upgrade**.



3. In the pop-up window, input the following information, and then click **Apply**.

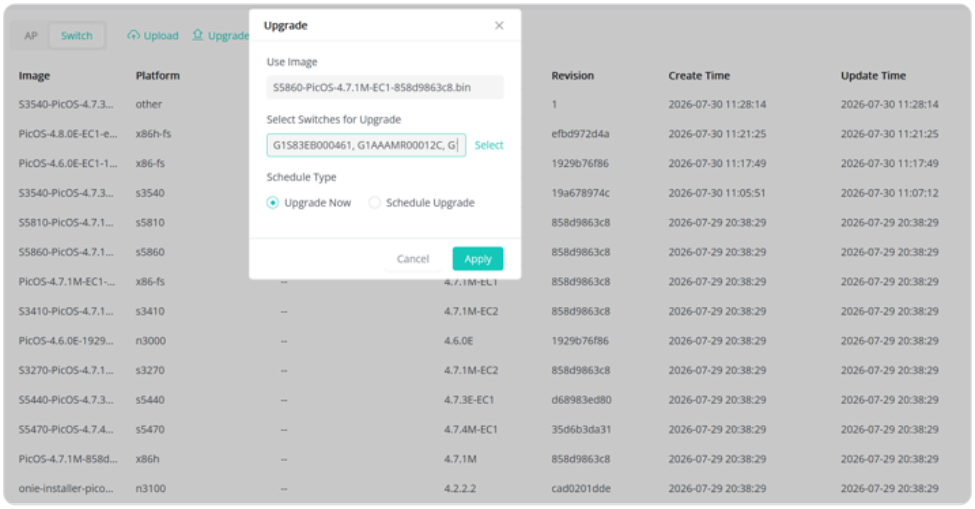
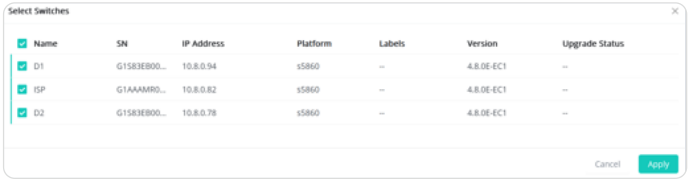


Table 4. Parameters for Upgrading Multiple Switches

Parameter	Description
Select Switches for Upgrade	Click **Select** to select the switches for upgrade.  **NOTEs** • Only PicOS switches whose platforms match the PicOS image's platform are displayed. When an image's platform is set to **Other**, all switch platforms are regarded as a match. • For PicOS 4.9 and later images, switches whose modes are not listed in the

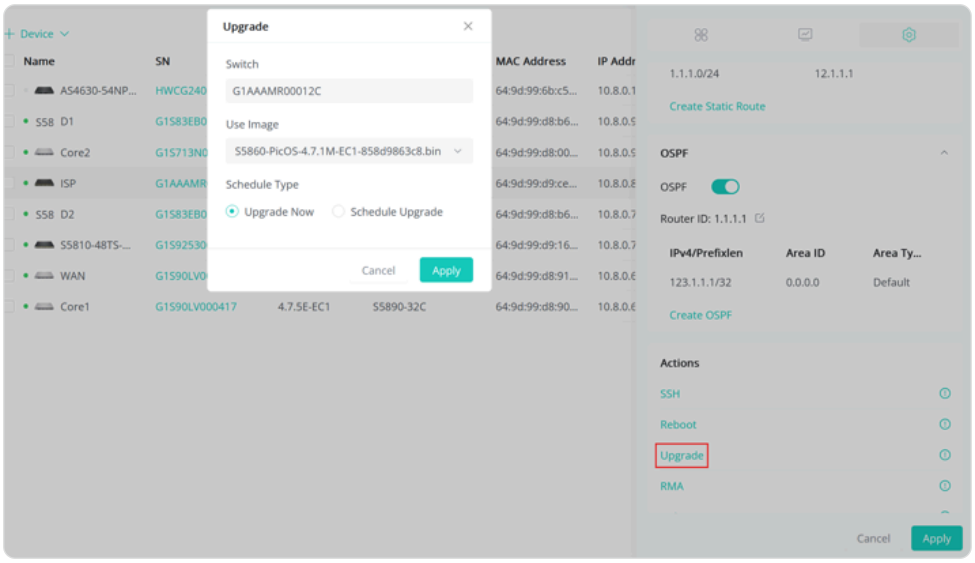
	Compatibility column cannot be selected. • Ensure that the selected switches are online. Upgrades for offline switches will fail.
Schedule Type	Select whether you want to upgrade the switches immediately or at a specified time. • **Upgrade Now:** Upgrades the switches immediately. • **Schedule Upgrade:** Upgrades the switches at a specified time. If you select this schedule type, select the upgrade time in the **Upgrade Time** section. **NOTEs** • The time is based on your browser's time zone. • You cannot select a time point earlier than the current time.

Upgrading a Single Switch

To upgrade a PicOS switch, in addition to the method described in Upgrading Multiple Switches, you can use the following method:

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click the switch in the device list.
3. In the side panel on the right, click the **Setting** tab.
4. In the **Actions** section, click **Upgrade**.

> **NOTE**
>
> The **Upgrade** button is available only if the switch meets all the following conditions:
>
> - The switch is currently online (connected to AmpCon-Campus).
> - No configurations are being pushed or waiting to be pushed to the switch.
> - The switches are not being moved to another site.
> - No **License Audit** or **License Action** is currently in progress on the switches.
> - No reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.



5. In the pop-up window, input the following information, and then click **Apply**.

Table 5. Parameters for Upgrading a Single Switch

Parameter	Description
Use Image	Click the drop-down list to select a PicOS image. **NOTE** Only the PicOS images matching the platform of the switch can be selected.
Schedule Type	Select whether you want to upgrade the switch immediately or at a specified time. • **Upgrade Now:** Upgrades the switch immediately.

- **Schedule Upgrade:** Upgrades the switch at a specified time. If you select this schedule type, select the upgrade time in the **Upgrade Time** section.

> **NOTEs**
>
> - The time is based on your browser's time zone.
> - You cannot select a time point earlier than the current time.

Checking Upgrade Task Results

To check upgrade task results, follow these steps:

1. In the **Switch** tab of the “Upgrade Management” page, click **Upgrade Tasks**.
2. In the pop-up window, check the upgrade task details:

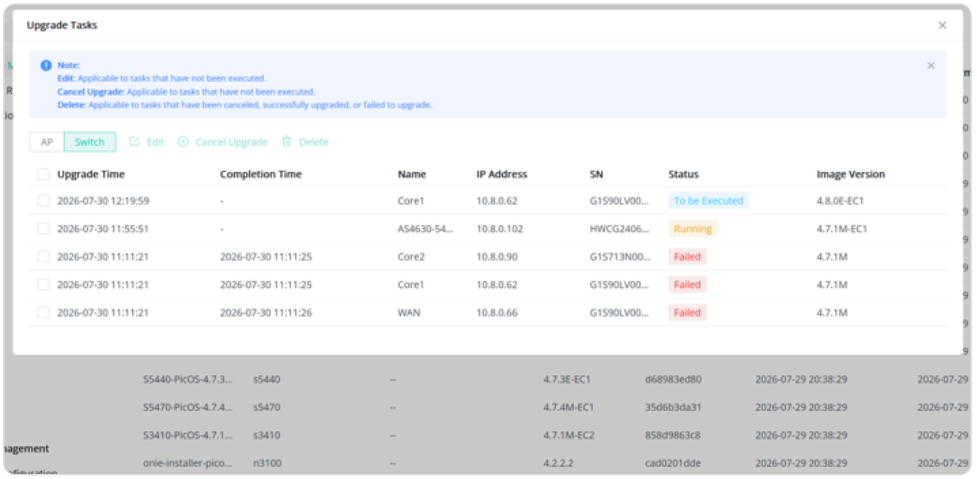


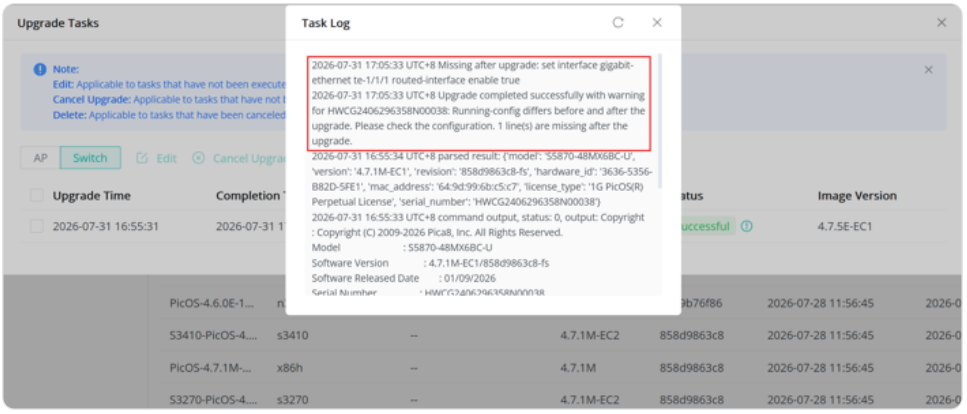
Table 6. Upgrade Task Metrics

Metric	Description
Upgrade Time	The start time of the upgrade task.
Completion Time	The completion time of the upgrade task. • If the upgrade task is not completed, the completion time is displayed as **--**. • If the upgrade task is canceled, the completion time is the time when the task is canceled.
Name	The switch alias.

IP address	The IP address of the switch.
SN	The serial number of the switch.
Status	The status of the upgrade task. • **To be Executed:** The upgrade task is waiting to be executed. • **Running:** The upgrade task is in progress. • **Successful:** The upgrade task is completed successfully. • **Failed:** The upgrade task fails. The switch retains its pre-upgrade PicOS version. • **Cancel Upgrade:** The upgrade task is canceled. The switch retains its pre-upgrade PicOS version. **NOTEs** • For a switch that has an upgrade task in **To be Executed** status, if you create a new upgrade task for the switch, the previous task will be deleted, and the new one will be displayed in the upgrade task list. • For a switch that has an upgrade task in **Running** status, you cannot create a new upgrade task for the switch. • For an upgrade task in **Running** status, if AmpCon-Campus cannot connect to the associated switches for approximately 20 minutes, the task status will change to **Failed**. • If switch configurations are changed (lost, newly added, or modified) after the upgrade, the status shows **Successful** with an exclamation mark. Hover over the exclamation mark, and then you can see the tip: "Running-config differs between pre-upgrade and post-upgrade. Please check the configuration."
Image Version	The version of the PicOS image to which you want to upgrade.

3. Optional: To view the upgrade task logs, hover over the upgrade task, and then click **Task Log**.

   For example, if switch configurations are changed (lost, newly added, or modified) after the upgrade, you can see the configuration changes in the task log pop-up window.

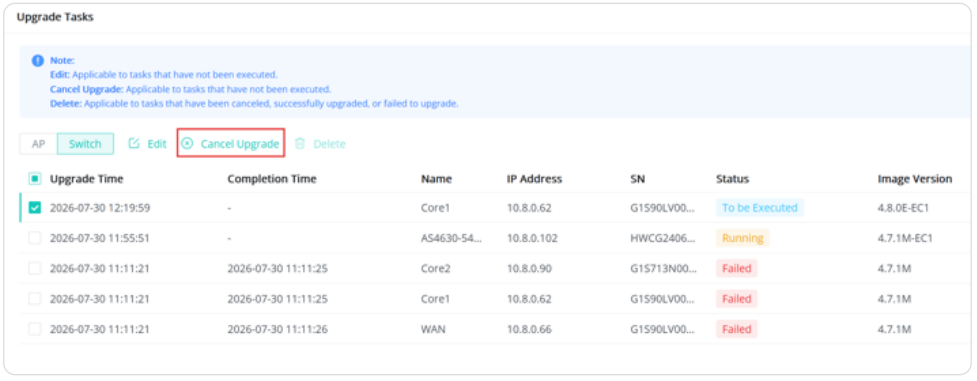


Optional Operations

Managing Upgrade Tasks

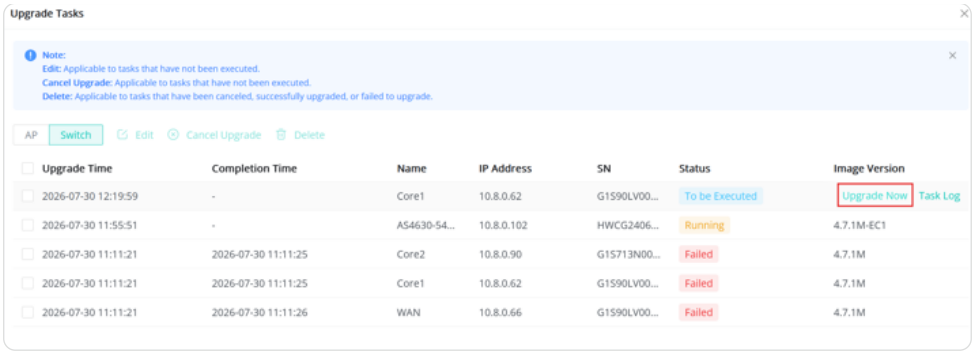
- To cancel one or multiple upgrade tasks, select the tasks, and then click **Cancel Upgrade** at the top.

> **NOTE**
>
> You can cancel only the upgrade tasks in **To be Executed** status.



- To execute an upgrade task immediately, hover over the upgrade task, and then click **Upgrade Now**.

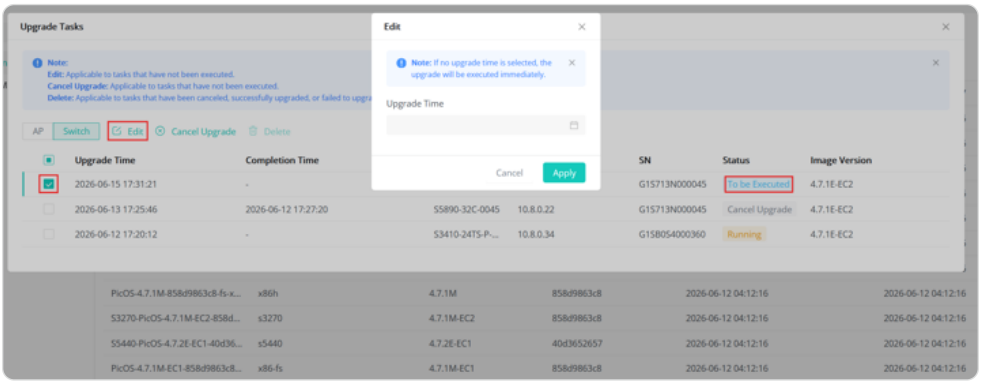
> **NOTE**
>
> You can immediately execute only the upgrade tasks in **To be Executed** status.



- To change the execution time of one or multiple upgrade tasks, select the upgrade tasks, and then click **Edit** at the top.

  In the pop-up window, select the execution time in the **Upgrade Time** section, and then click **Apply**.

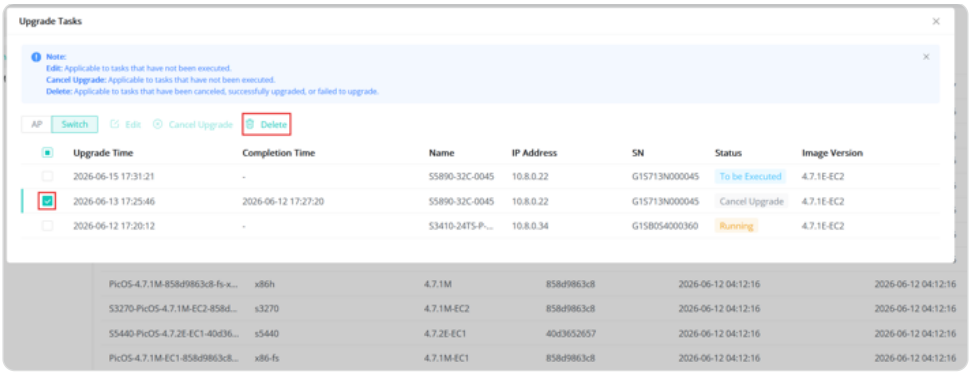
> **NOTEs**
>
> - You can edit only the upgrade tasks in **To be Executed** status.
> - In the **Edit** pop-up window, the **Upgrade Time** is blank by default. If you click **Apply** without selecting a time, the upgrade task will be executed immediately.



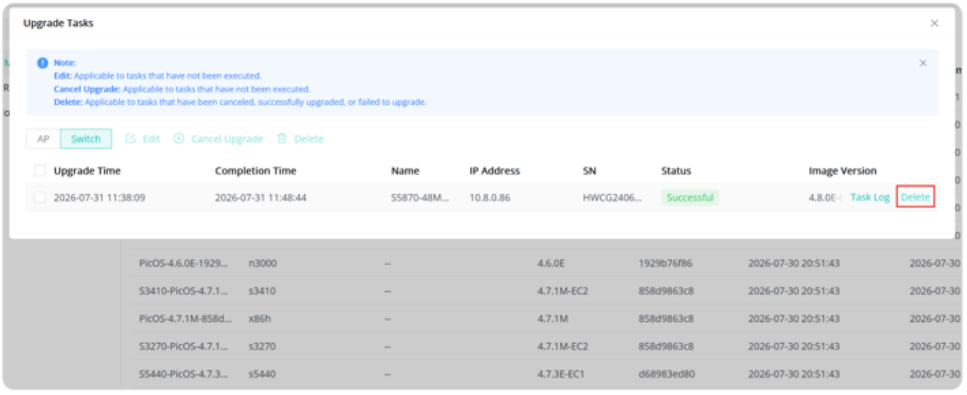
- To delete upgrade tasks, use one of the following methods:

> **NOTE**
>
> You can delete only the upgrade tasks in **Successful**, **Failed**, or **Cancel Upgrade** status.

To delete multiple upgrade tasks, select the upgrade tasks, and then click **Delete** at the top. In the pop-up window, click **Yes** to confirm the deletion.



To delete a single upgrade task, hover over the upgrade task, and then click **Delete** on the right. In the pop-up window, click **Yes** to confirm the deletion.

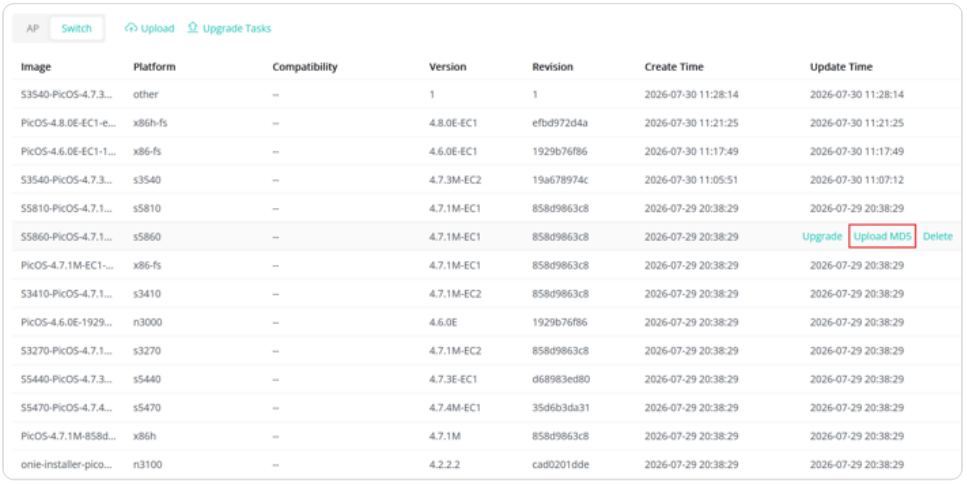


Uploading MD5 Files

MD5 files are used to verify the completeness of corresponding PicOS images. If the MD5 file does not match the image, the upgrade will fail. If no MD5 file is uploaded, AmpCon-Campus will not verify the completeness of the PicOS image during upgrade.

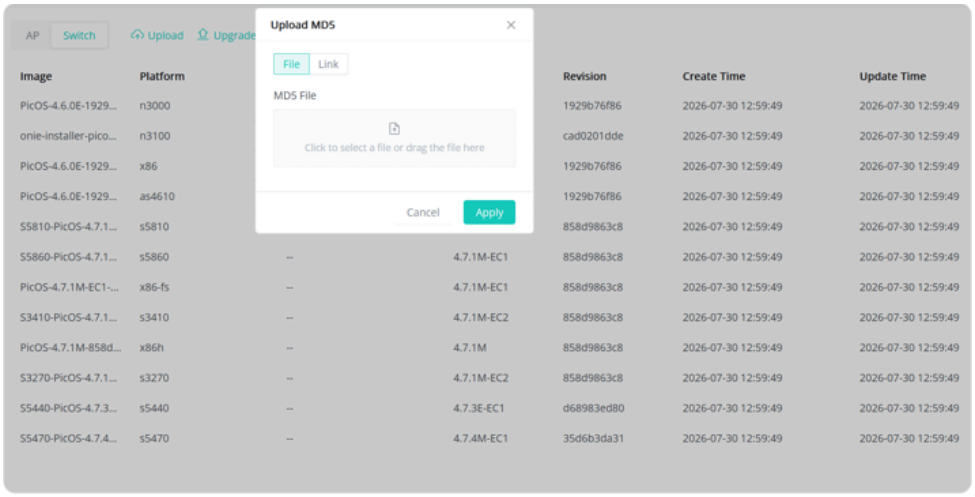
To upload an MD5 file for a PicOS image, follow these steps:

1. In the **Switch** tab, hover over the PicOS image, and then click **Upload MD5**.

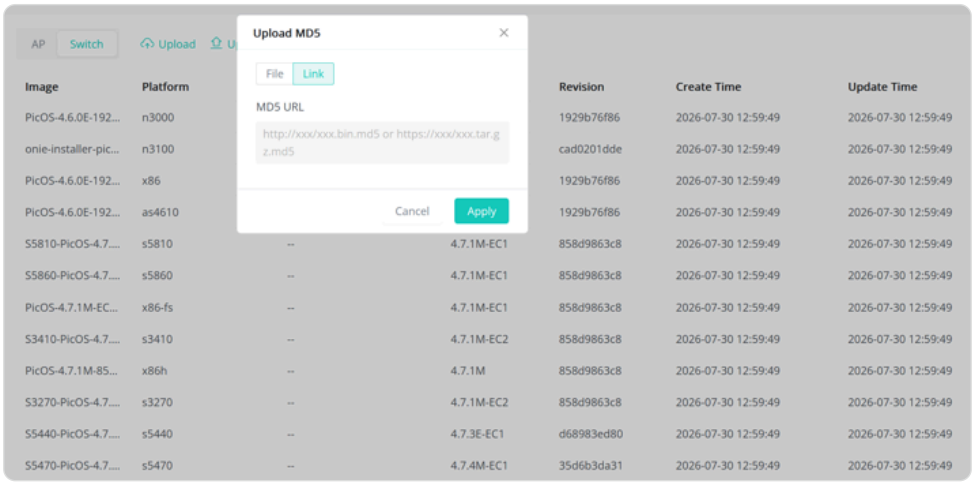


2. Upload the MD5 file by using one of the following methods:

- In the **File** tab, click the upload icon to select an MD5 file, or drag and drop the MD5 file. Then, click **Apply**.



- In the **Link** tab, enter the URL of the MD5 file, and then click **Apply**.

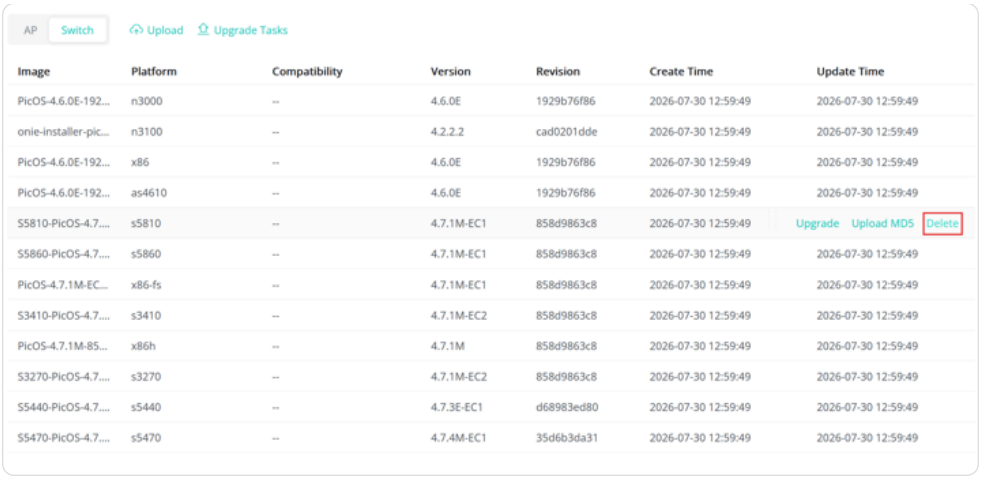


Deleting PicOS Images

To delete a PicOS image, follow these steps:

1. In the **Switch** tab, hover over the PicOS image, and then click **Delete**.

> **NOTEs**
>
> - Built-in PicOS images cannot be deleted.
> - If a PicOS image is associated with upgrade tasks, you can delete it only when the upgrade tasks are in **Successful**, **Failed**, or **Cancel Upgrade** status.



2. In the pop-up window, click **Yes** to confirm the deletion.

Managing License Portals

License portals on AmpCon-Campus are used to check PicOS license validity and install or extend PicOS licenses on switches.

The first time you log in to AmpCon-Campus, the **Global** license portal is unconfigured. You must configure the **Global** license portal first. Otherwise, you cannot perform **License Audit** and **License Action** for managed PicOS switches, and PicOS licenses cannot be installed or extended on switches during onboarding.

After configuring the **Global** license portal, if it does not meet the requirements of all switches, you can add more license portals. For example, you can add multiple license portals with the same portal URL and different user accounts.

Guidelines
Configuring the Global License Portal
Adding Non-Global License Portals

Guidelines

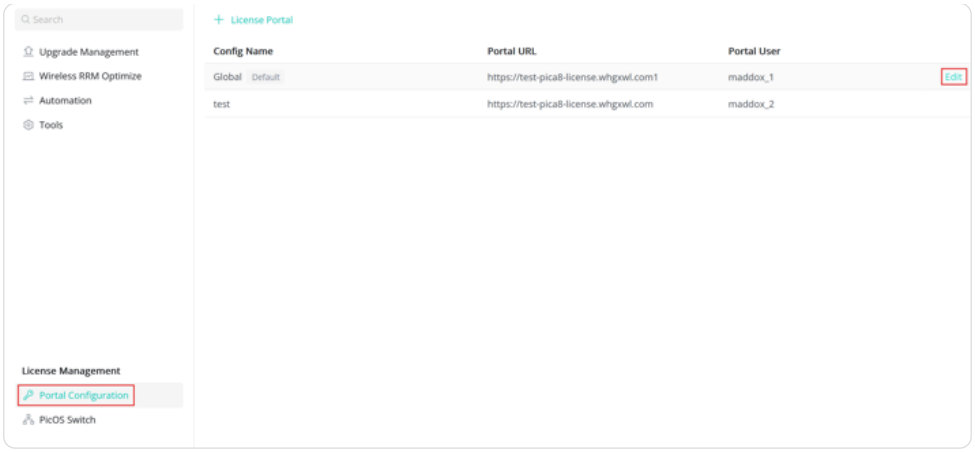
- License portal configurations are consistent across all sites.
- When you onboard a PicOS switch, AmpCon-Campus uses the **Global** license portal to install or extend PicOS licenses on switches.

  If the **Global** license portal cannot be accessed by AmpCon-Campus, AmpCon-Campus checks whether a local PicOS license for the switch is added to AmpCon-Campus and installs or extends the license on the switch based on the local license.
- When you perform **License Audit** or **License Action**, you can select the **Global** license portal or a non-global license portal. For more information, see Managing PicOS Licenses.

Configuring the Global License Portal

To configure the **Global** license portal, follow these steps:

1. Click the **Maintain** icon from the navigation bar.
2. In the sidebar, click **Portal Configuration** in the **License Management** section.
3. Hover over the **Global** license portal, and then click **Edit**.



4. In the pop-up window, edit the following parameters. The **Config Name** cannot be edited.

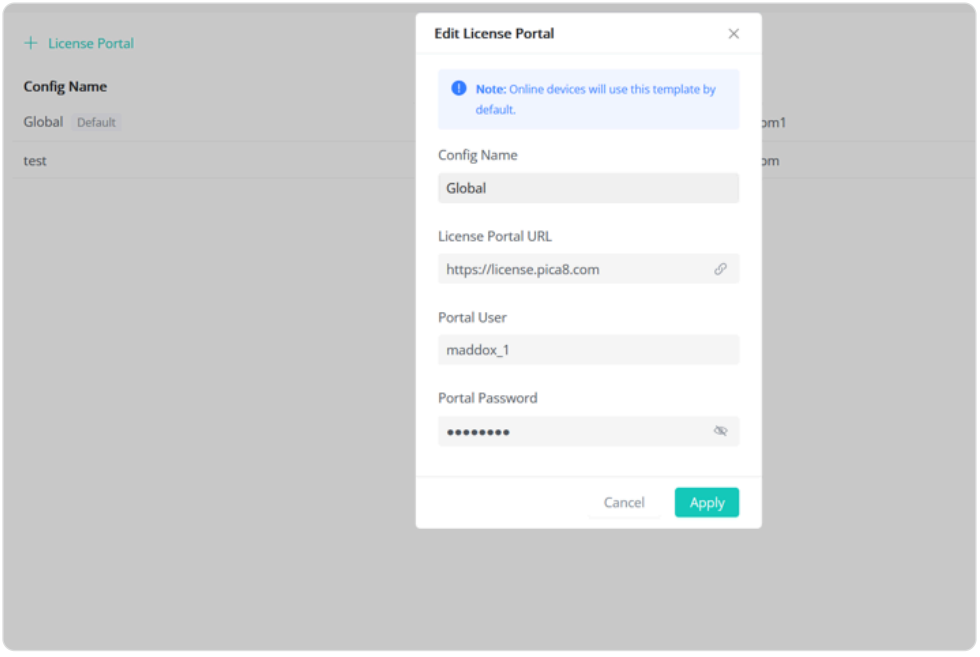


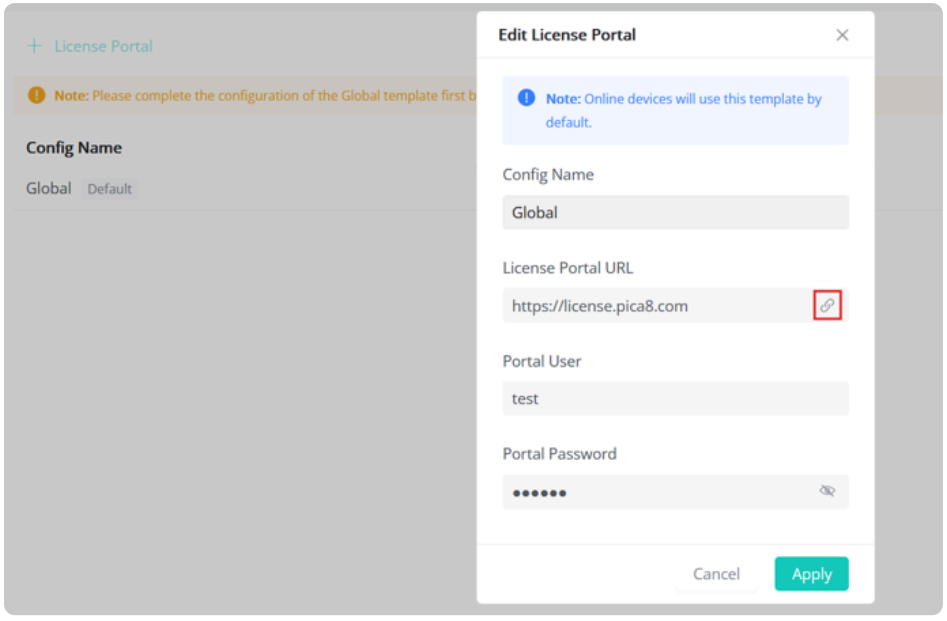
Table 1. Global License Portal Parameters

Parameter	Description
License Portal URL	The license portal URL (https://license.pica8.com).
Portal User	The username used to log in to the license portal. • The username can contain letters, numbers, and special characters (_ . @ + -). • The username can contain at most 50 characters. **NOTE** The combination of the **License Portal URL** and **Portal User** must be unique.

Portal Password	The password of the user. • The password can contain letters, numbers, and special characters (~ ! @ # $ % ^ & * ( ) _ + - = [ ] { } | \ : ; " ' < > , . ? / `). • The password cannot contain spaces. • The password can contain at most 255 characters.

5. Test whether AmpCon-Campus can access the license portal by clicking the test connection icon in the **License Portal URL** field.

> **NOTEs**
>
> - The connection test will adopt the updated portal password if you have modified it, even if you do not click **Apply**.
> - Ensure that AmpCon-Campus can access the license portal. Otherwise, you cannot use the license portal to install and extend PicOS licenses on switches.



6. Click **Apply**.

> **Tip**
>
> The **Global** license portal cannot be deleted.

Adding Non-Global License Portals

To add a non-global license portal, follow these steps:

1. Click the **Maintain** icon from the navigation bar.
2. In the sidebar, click **Portal Configuration** in the **License Management** section.
3. On the “Portal Configuration” page, click **+ License Portal**. In the pop-up window, input the following information:

> **NOTE**
>
> Ensure that you have configured the **Global** license portal. Otherwise, the **+ License Portal** button is grayed out.

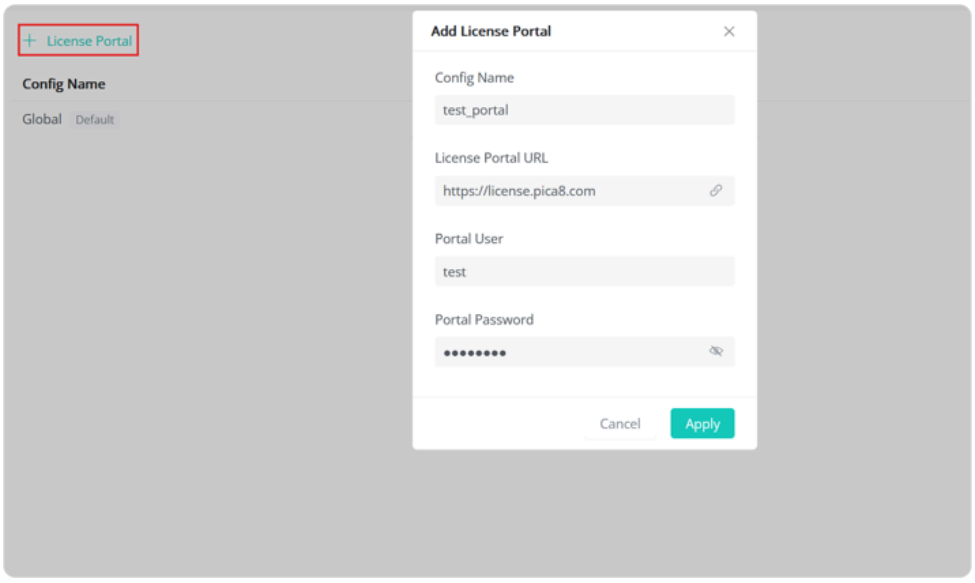


Table 2. Non-Global License Portal Parameters

Parameter	Description
Config Name	The name of the license portal. • The name must be unique. • The name cannot be any case-insensitive form of **Global** (such as **GLOBAL** or **global**). • The name can contain at most 64 characters. • The name can contain letters, numbers, and special characters (**-** **_**). • The name cannot start or end with special characters (**-** **_**).
License Portal URL	The license portal URL (https://license.pica8.com).
Portal User	The username used to log in to the license portal.

	• The username can contain letters, numbers, and special characters (_ . @ + -). • The username can contain at most 50 characters. **NOTE** The combination of the **License Portal URL** and **Portal User** must be unique.
Portal Password	The password of the user for the License Portal. • The password can contain letters, numbers, and special characters (~ ! @ # $ % ^ & * ( ) _ + - = [ ] { } | \ : ; " ' < > , . ? / `). • The password cannot contain spaces. • The password can contain at most 255 characters.

4. Test whether AmpCon-Campus can access the license portal by clicking the test connection icon in the **License Portal URL** field.

> **NOTEs**
>
> - The connection test will adopt the updated portal password if you have modified it, even if you do not click **Apply**.
> - Ensure that AmpCon-Campus can access the license portal. Otherwise, you cannot use the license portal to install and extend PicOS licenses on switches.

5. Click **Apply**.

> **Tips**
>
> After adding a license portal, you can edit or delete it:
>
> - To edit a license portal, hover over the license portal name, and then click **Edit**.
> - To delete a license portal, hover over the license portal name, and then click **Delete**.

Managing PicOS Licenses

You can use the **License Audit** feature to check the validity (license expiry and license status) information of the PicOS license installed on the switch.

You can also use the **License Action** feature to extend expired or expiring PicOS licenses for switches with PicOS licenses installed or to install PicOS licenses for switches without PicOS licenses installed. After licenses are extended or installed through **License Action**, AmpCon-Campus will display the latest license expiry and license status in the **Portal License** tab.

If AmpCon-Campus cannot access the license portal for reasons like network issues, add local PicOS licenses to AmpCon-Campus. Then, you can perform **License Action** based on the added licenses.

Guidelines
Prerequisites
License Audit
License Action
Adding Local Licenses
License Installation and Extension Workflow

Guidelines

- During **License Audit**, AmpCon-Campus checks the validity information of the licenses installed on switches, and then displays the information in the **Portal License** tab.
- For how licenses are installed or extended through **License Action**, see the License Installation and Extension Workflow section.
- **License Audit** or **License Action** can be performed only on the switches that meet all the following conditions:
  - The switches are not being moved to another site.
  - No **License Audit** or **License Action** is currently in progress on the switches.
  - No reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
  - No configurations are being pushed or waiting to be pushed to the switches.

  Otherwise, **License Audit** or **License Action** will fail.
- You can add local PicOS licenses for PicOS switches that have or have not been onboarded to AmpCon-Campus. After a PicOS switch is deleted from AmpCon-Campus, its local PicOS license will not be deleted synchronously.

Prerequisites

To use the **License Audit** or **License Action** feature, ensure that the following prerequisites are met. Adding local licenses does not have the following prerequisites.

Table 1. Prerequisites for License Audit and License Action

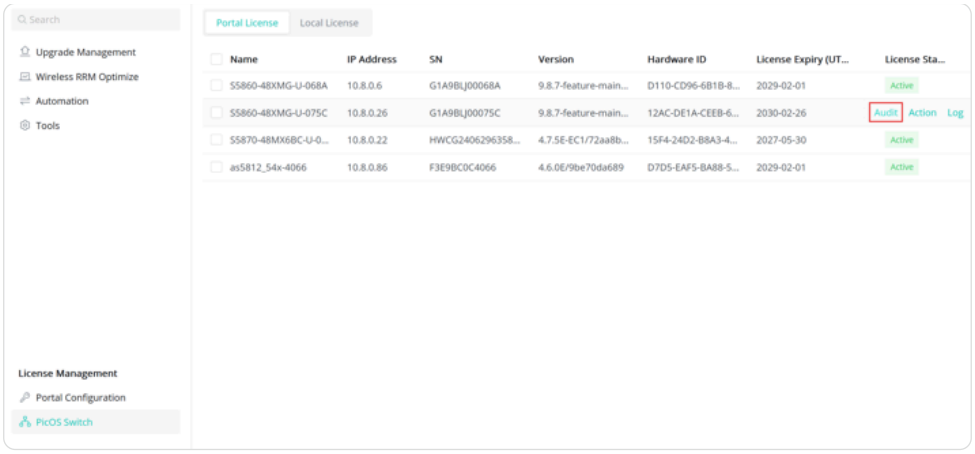
Prerequisite	Reference Link
Onboard the PicOS switches to AmpCon-Campus.	• Onboarding PicOS Switches
Ensure that the PicOS switches are online (connected to AmpCon-Campus).	• Viewing the PicOS List
Correctly configure the **Global** license portal or other required license portal.	• Managing License Portals
To perform **License Action**, if AmpCon-Campus cannot access the license portal for reasons like network issues, you must add local PicOS licenses to AmpCon-Campus.	• Adding Local Licenses

License Audit

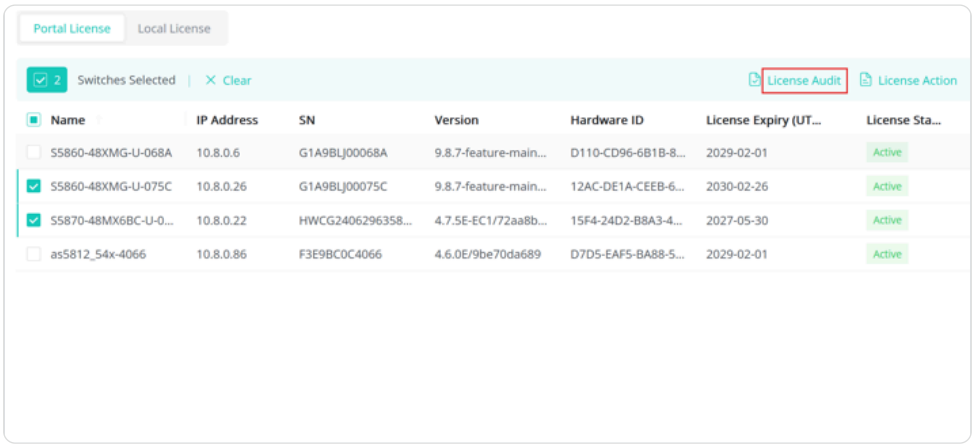
1. In the AmpCon-Campus UI, select the site to which the PicOS switches belong.
2. Click the **Maintain** icon from the navigation bar.
3. In the left sidebar, click **PicOS Switch** in the **License Management** section.
4. In the **Portal License** tab, operate as follows:

> **NOTEs**
>
> - Only the PicOS switches successfully onboarded to AmpCon-Campus are displayed in the **Portal License** tab.
> - After clicking **Audit** or **License Audit**, if you haven't configured the **Global** license portal, you can see a pop-up window with the message "Global Portal Unconfigured".
>
>   Click **Go to Portal Config** in the pop-up window to configure the **Global** license portal first.

- To verify license validity for a single switch, hover over the switch, and then click **Audit**.



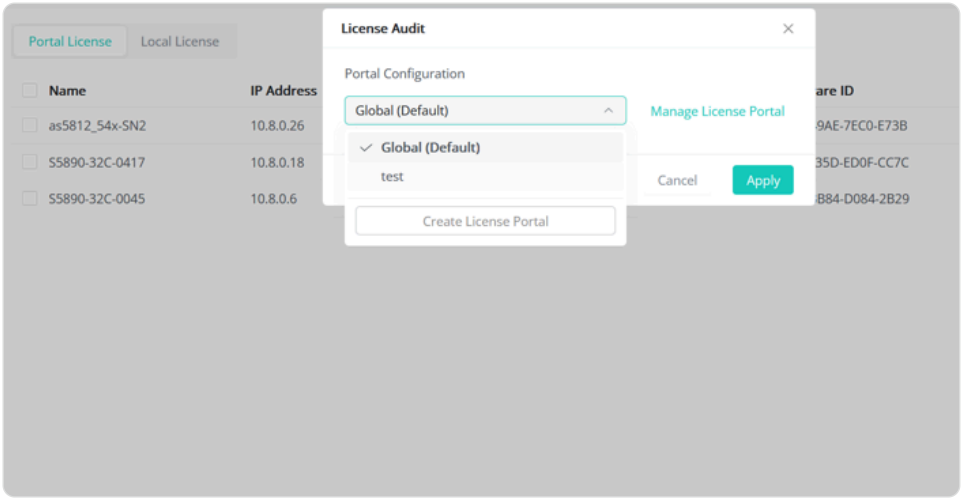
- To verify license validity for multiple switches, select the switches in the **Name** column, and then click **License Audit**.



5. In the pop-up window, select a PicOS license portal, and then click **Apply**.

   To create a new license portal, click **Create License Portal** in the drop-down list.

   To manage license portals, click **Manage License Portal**. For more information, see Managing License Portals.



6. Check the **License Status** and **License Expiry (UTC+0)** columns.

License Expiry (UTC+0) shows the expiration date of the PicOS license in UTC+0.
License Status shows the current status of the PicOS license. You might see the following license statuses:

> **NOTE**
>
> If switches are offline (disconnected from AmpCon-Campus), AmpCon-Campus can't retrieve license expiry and license status information from the switches.

Table 2. License Status

Status	Description
Expired	The PicOS license is expired.
Expiring	The PicOS license is still valid but will expire within 30 days.
Active	The PicOS license is valid and will not expire in the next 30 days.
Unknown	The PicOS license status on the switch cannot be retrieved.
No License	The switch has no PicOS license installed.

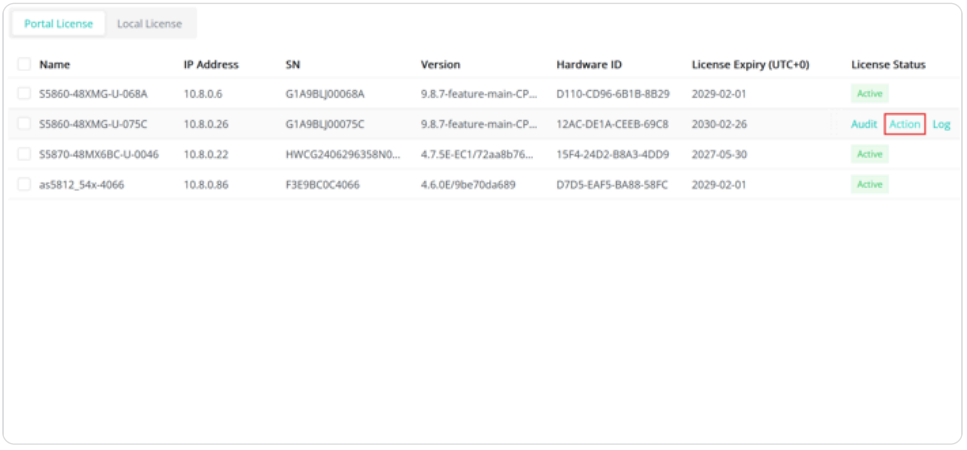
7. Optional: To view **License Audit** logs, hover over the switch, and then click **Log**.

License Action

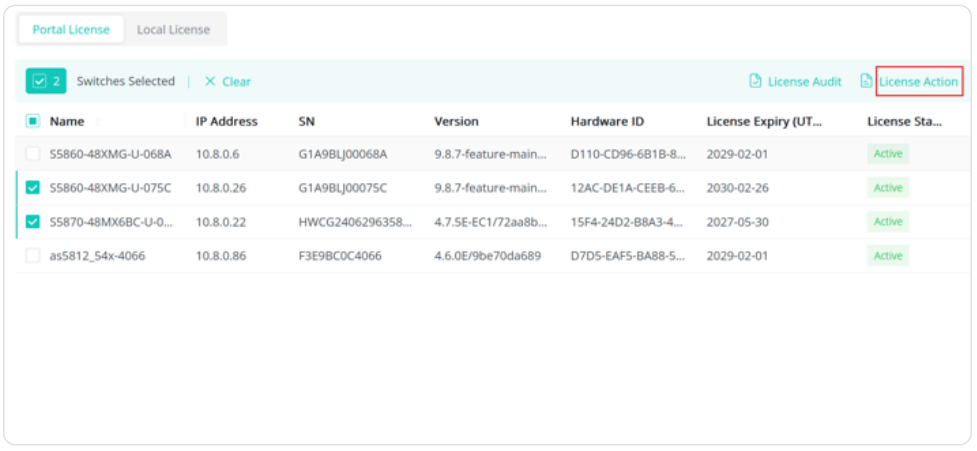
1. In the AmpCon-Campus UI, select the site to which the PicOS switches belong.
2. Click the **Maintain** icon from the navigation bar.
3. In the left sidebar, click **PicOS Switch** in the **License Management** section.
4. In the **Portal License** tab, operate as follows:

> **NOTEs**
>
> - Only the PicOS switches successfully onboarded to AmpCon-Campus are displayed in the **Portal License** tab.
> - After clicking **Action** or **License Action**, if you haven't configured the **Global** license portal, a pop-up window with the message "Global Portal Unconfigured" is displayed. Click **Go to Portal Config** in the pop-up window to configure the **Global** license portal first.

- To perform **License Action** for a single switch, hover over the switch, and then click **Action**.



- To perform **License Action** for multiple switches, select the switches in the **Name** column, and then click **License Action**.



5. In the pop-up window, select a PicOS license portal in the drop-down list, and then click **Apply**.

NOTEs

- Sometimes AmpCon-Campus might fail to retrieve license information from the selected license portal for reasons like network issues and wrong license portal URL, username, and password.
- In this case, AmpCon-Campus checks whether local PicOS licenses for the switches have been added to AmpCon-Campus.
  - For a switch **with** a PicOS license installed, if the license is expired or expiring (will expire within 30 days), AmpCon-Campus tries to **extend** the license on the switch based on the local license.
  - For a switch **without** a PicOS license installed, AmpCon-Campus tries to **install** a license on the switch based on the local license.
  - After licenses are extended or installed through **License Action**, AmpCon-Campus displays the latest license expiry and license status in the **Portal License** tab.

6. Check the **License Status** and **License Expiry (UTC+0)** columns.

   License Expiry (UTC+0) shows the expiration date of the PicOS license in UTC+0. **License Status** shows the current status of the PicOS license. For a description of each status, see **Table 2. License Status**.
7. Optional: To view **License Action** logs, hover over the PicOS switch, and then click **Log**.

Adding Local Licenses

1. In the AmpCon-Campus UI, select the site to which the PicOS switches belong.
2. Click the **Maintain** icon from the navigation bar.
3. In the left sidebar, click **PicOS Switch** in the **License Management** section.
4. Click the **Local License** tab, and then click **+ License**.
5. In the pop-up window, input the following information:

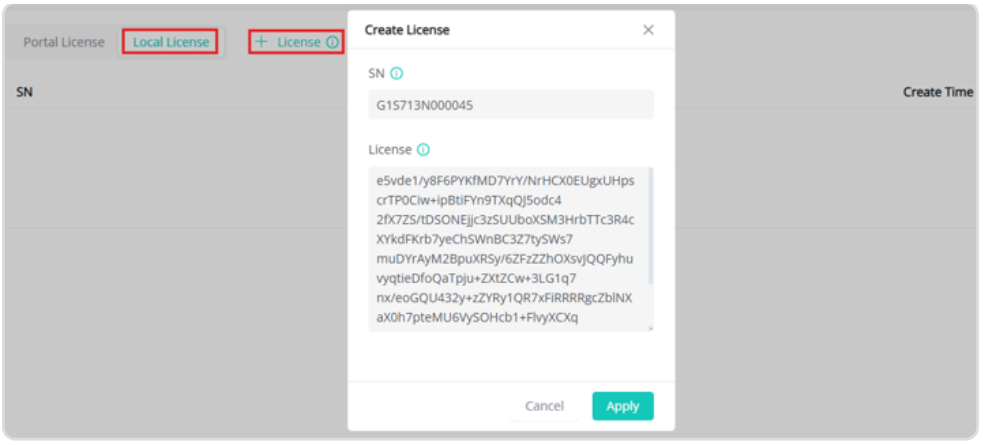


Table 3. Local License Parameters

Parameter	Description
SN	The SN of the switch. The SN must be unique. **NOTE** You can enter the SN of a switch that has or has not been onboarded to AmpCon-Campus.
License	The PicOS license key.

6. Click **Apply**.

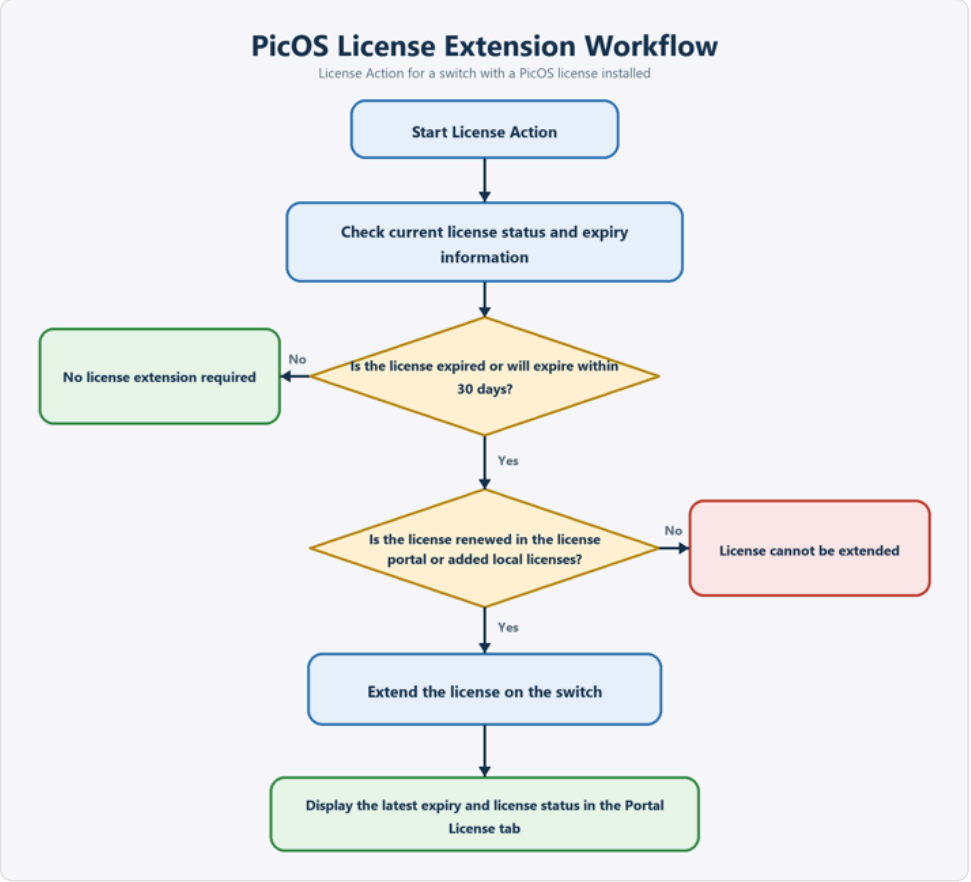
Tips

After adding a local license, you can edit or delete the license:

- To edit a local license, hover over the license, and then click **Edit** on the right.
- To delete a local license, hover over the license, and then click **Delete** on the right.
- To delete multiple local licenses, select the licenses in the **SN** column, and then click **Delete** at the top.

License Installation and Extension Workflow

- For a switch **with** a PicOS license installed, during **License Action**, AmpCon-Campus will try to **extend** the license. See the following flow chart:

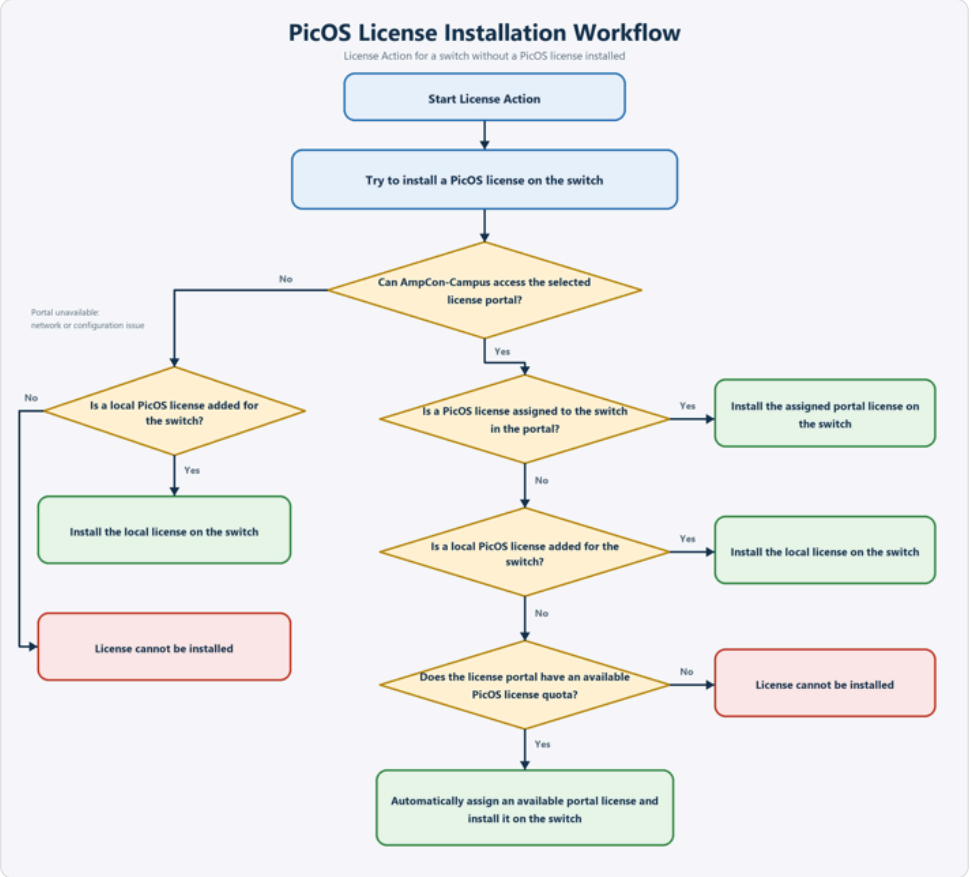


a. AmpCon-Campus first checks the current license status and license expiry information on the switch.

b. If the license is expired or expiring (will expire within 30 days), AmpCon-Campus checks the license portal or added local license to see whether the license is renewed.

c. If yes, AmpCon-Campus tries to extend the license on the switch, and then displays the latest license expiry and license status in the **Portal License** tab.

- For a switch **without** a PicOS license installed, during **License Action**, AmpCon-Campus will try to **install** a PicOS license on the switch. See the following flow chart:



a. If the **selected** license portal **cannot** be accessed by AmpCon-Campus for reasons like network issues or wrong license portal URL, username, and password, AmpCon-Campus checks whether a local PicOS license for the switch is added to AmpCon-Campus. If yes, AmpCon-Campus installs the license on the switch.

b. If the **selected** license portal is configured correctly and can be accessed by AmpCon-Campus, AmpCon-Campus checks whether the switch has a PicOS license assigned in the license portal. If yes, AmpCon-Campus installs the PicOS license on the switch.

c. If the **selected** license portal **can** be accessed by AmpCon-Campus but no PicOS license is assigned to the switch in the license portal, AmpCon-Campus checks whether a local PicOS license for the switch is added to AmpCon-Campus. If yes, AmpCon-Campus installs the license on the switch.

d. If no PicOS license is assigned to the switch in the license portal and no local PicOS license is added to AmpCon-Campus, AmpCon-Campus checks whether the license portal has available PicOS license quotas. If yes, an available PicOS license is automatically assigned to the switch and installed on the switch. If not, AmpCon-Campus cannot install a PicOS license on the switch.

Moving Switches to Another Site

On the “Devices” page, you can move one or multiple PicOS switches to a new site.

After a PicOS switch is moved to a new site, if the new site has site-level system configurations, the configurations will be automatically pushed to the switch.

Guideline
Moving a Single Switch
Moving Multiple Switches
What to Do Next

Guideline

The PicOS switches in any of the following cases cannot be moved to a new site:

- The switches are in **Provisioning** status, which means AmpCon-Campus is verifying authentication information of the switch or establishing an OpenVPN tunnel with the switch.
- Configurations are being pushed or waiting to be pushed to the switches.
- Reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
- The switches are being moved to another site.
- **License Audit** or **License Action** is currently in progress on the switches.

Moving a Single Switch

To move a single PicOS switch to a new site, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, hover your mouse over the switch, and then click **Move**.

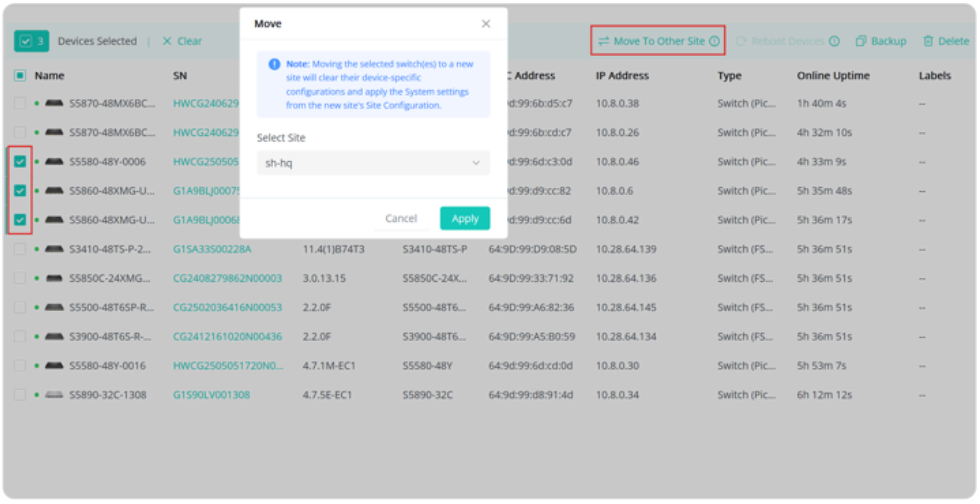


4. In the pop-up window, select the new site, and then click **Apply**.

Moving Multiple Switches

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, select the switches to be moved, and then click **Move To Other Site**.

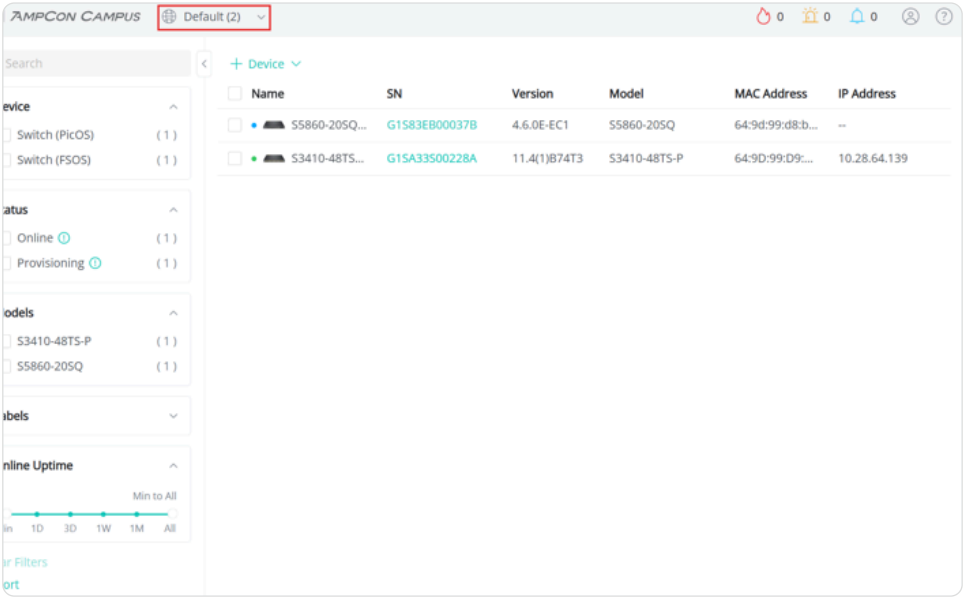
   To clear the switch selection, click **Clear**.



4. In the pop-up window, select the new site, and then click **Apply**.

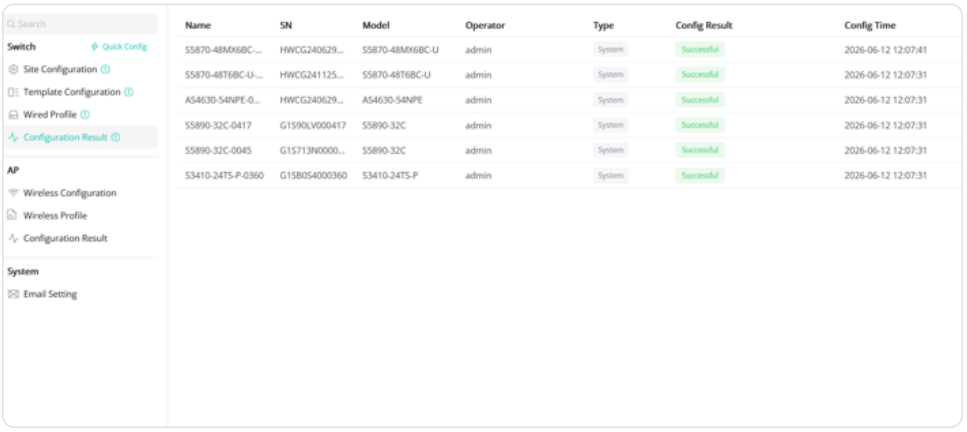
What to Do Next

- Select the new site, and then check whether the switches are listed on the “Devices” page.



- Click the **Settings** icon from the navigation bar, and then click **Configuration Result** in the **Switch** section. On the “Configuration Result” page, check whether the site-level system configurations of the new site are pushed to the switches successfully.

> **NOTE**
>
> If the new site has no site-level system configurations, no configurations will be pushed to the switches, so no relevant records will appear on the “Configuration Result” page.



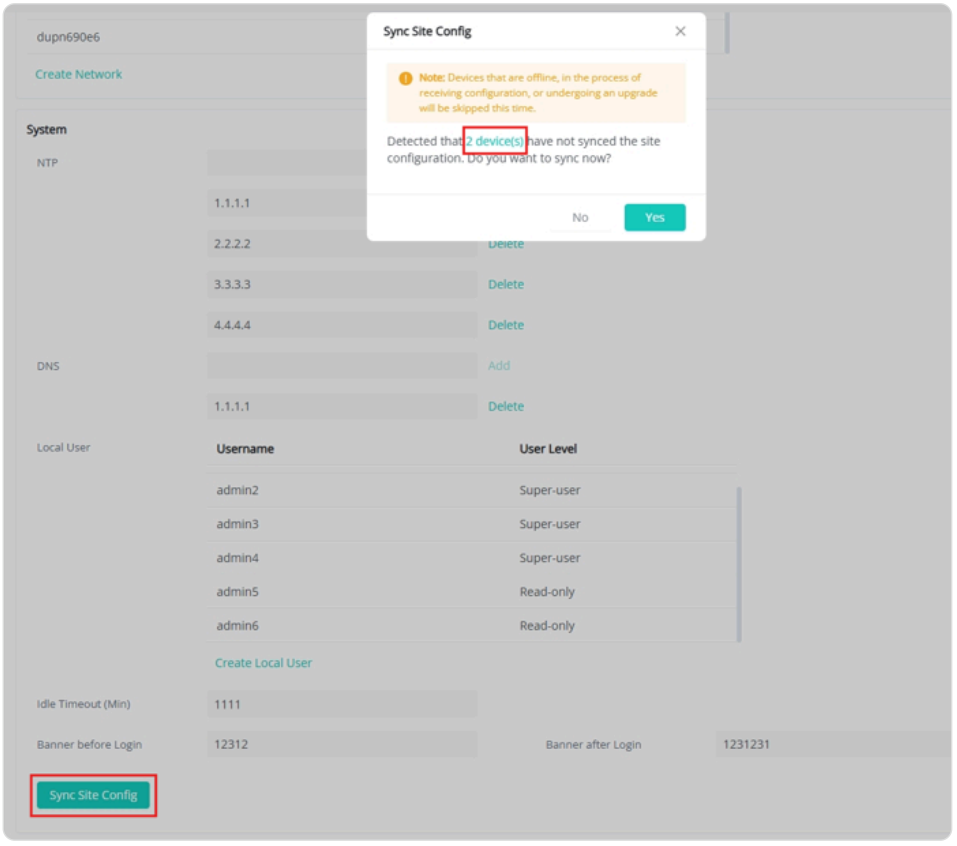
- If the configuration fails for a switch, check the following possible reasons and solutions:

  Table 1. Site Configuration Failure Reasons

Reason	Solution
The site-level system configurations of the new site conflict with existing configurations on the switch.	On the switch, clear the configurations leading to the conflict.
The switch SSH username and password stored on AmpCon-Campus are incorrect.	Modify the switch SSH username and password on AmpCon-Campus. For more information, see Configuring a Single Switch.
The switch is offline (disconnected from AmpCon-Campus).	Bring the switch online (successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus).

  To push the site-level system configurations of the new site to the switch, click the **Settings** icon from the navigation bar, and then click **Site Configuration** in the sidebar.

On the “Site Configuration” page, click **Sync Site Config**. For more information, see **Step 7** of Applying Site Configurations.



Backing Up Configurations

After successfully onboarding PicOS switches to AmpCon-Campus, you can back up switch configurations at a specified interval and time, or you can back up the currently running configuration on switches.

Currently, AmpCon-Campus does not support rolling back configurations based on backup configurations. You can view the backup configurations.

Guidelines
Backing Up Configurations for Multiple Switches
Backing Up Configurations for a Single Switch
Other Operations

Guidelines

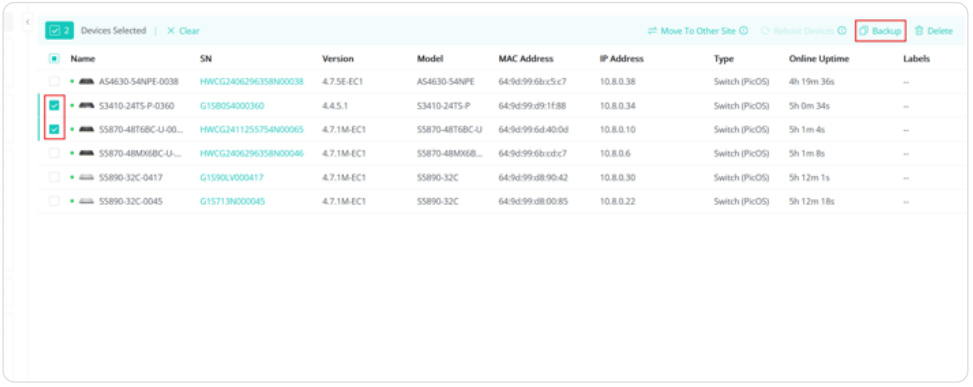
The PicOS switches in any of the following cases cannot be backed up:

- Configurations are being pushed or waiting to be pushed to the switches.
- Reboot, upgrade, backup, Return Merchandise Authorization (RMA), or deletion tasks are running on the switches.
- The switches are being moved to another site.
- **License Audit** or **License Action** is currently in progress on the switches.

Backing Up Configurations for Multiple Switches

To back up configurations for multiple PicOS switches, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, select the switches, and then click **Backup** at the top.

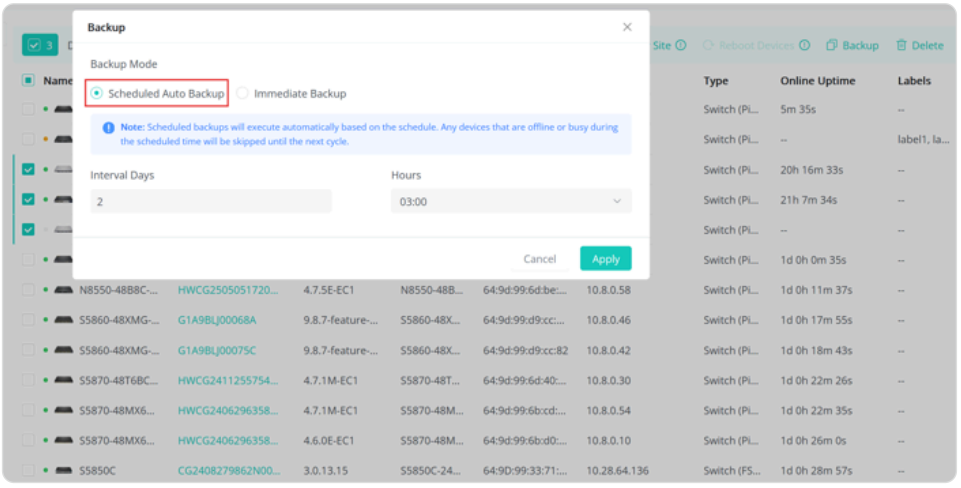


3. In the pop-up window, select the backup mode.

- To back up switch configurations at a specific interval and time, select **Scheduled Auto Backup**. In the pop-up window, input the **Interval Days** and **Hours**, and then click **Apply**.

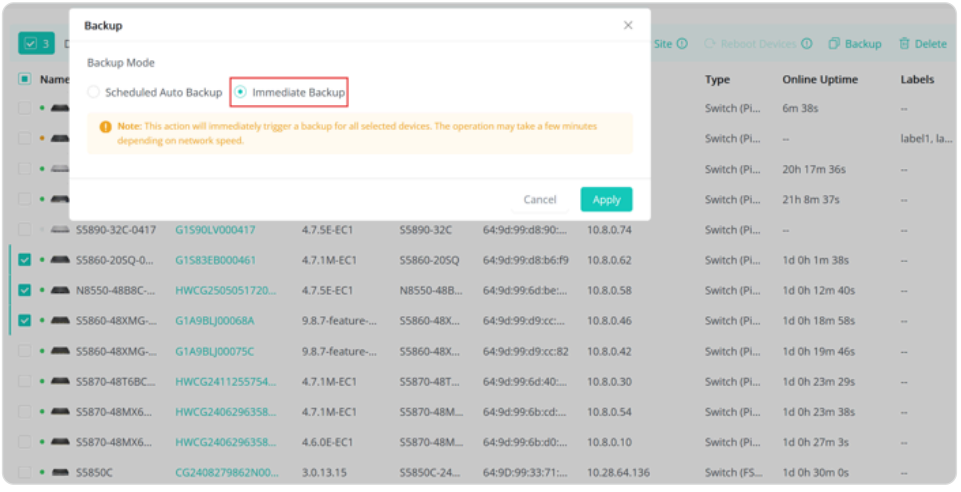
Interval Days indicates the interval in days between each backup. **Hours** indicates the time (a specific hour) when a backup is started.

> **NOTEs**
>
> - If you have configured the automatic backup before, you can see the pre-configured backup schedule in the pop-up window.
> - Any switches that are offline or busy during the scheduled time will be skipped until the next cycle.



- To back up the currently running configuration on switches, select **Immediate Backup**, and then click **Apply**.

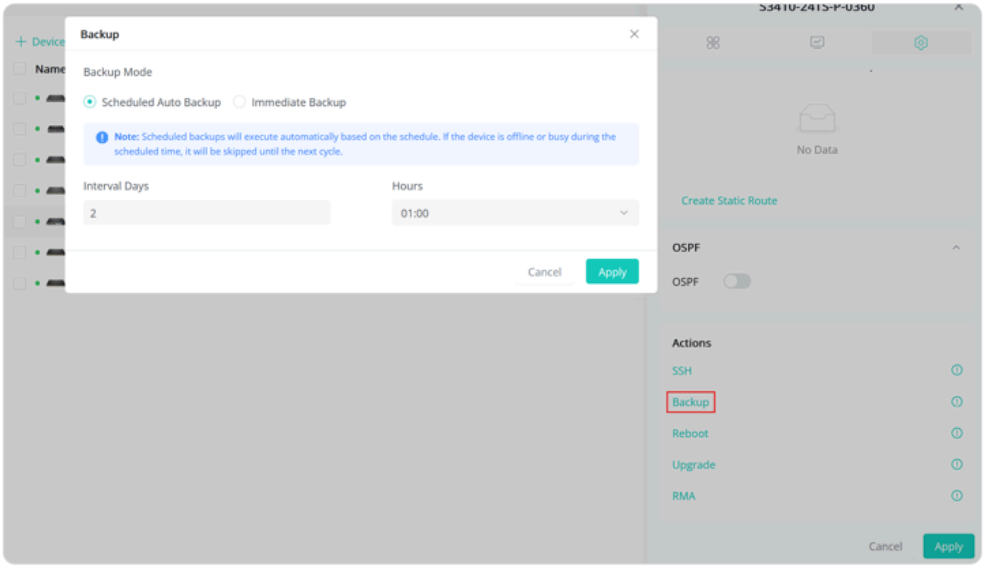
> **NOTE**
>
> Ensure that the switches are currently online (connected to AmpCon-Campus). Otherwise, the immediate backup operation will fail.



Backing Up Configurations for a Single Switch

To back up configurations for a single PicOS switch, in addition to the method described above, you can use the following method:

1. In the AmpCon-Campus UI, select the site to which the switch belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click the switch.
3. In the side panel on the right, click the **Setting** tab.
4. In the **Actions** section, click **Backup**.



5. In the pop-up window, select the backup mode.

- To back up switch configurations at a specific interval and time, select **Scheduled Auto Backup**. In the pop-up window, input the **Interval Days** and **Hours**, and then click **Apply**.

  Interval Days indicates the interval in days between each backup. **Hours** indicates the time (a specific hour) when a backup is started.

  > **NOTEs**
  >
  > - If you have configured the automatic backup before, you can see the pre-configured backup schedule in the pop-up window.
  > - Any switches that are offline or busy during the scheduled time will be skipped until the next cycle.

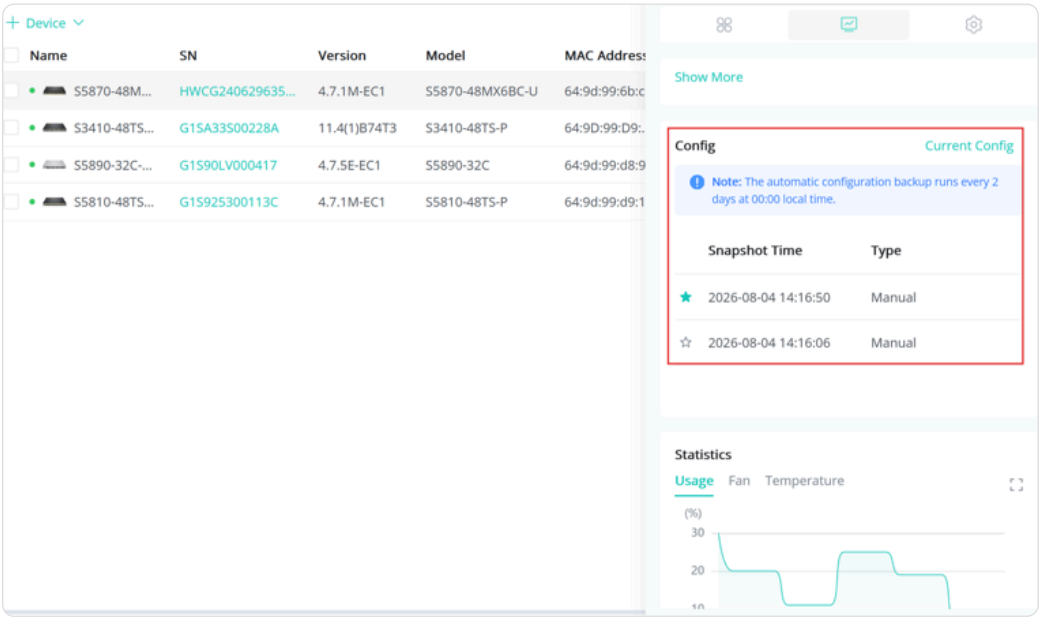
- To back up the currently running configuration on switches, select **Immediate Backup**, and then click **Apply**.

  > **NOTE**
  >
  > Ensure that the switches are currently online (connected to AmpCon-Campus). Otherwise, the immediate backup operation will fail.

Other Operations

In the **Config** section of the **Insight** tab, you can see the latest four backups in the backup list.

> **NOTEs**
>
> - **Snapshot Time** indicates the time when the switch was backed up.
> - **Type** can be **Auto** or **Manual**, which indicates the **Scheduled Auto Backup** or **Immediate Backup** option selected when you back up configurations.
> - The scheduled auto backups that have not been executed will not be displayed in the backup list.
>
>   If you have configured automatic backups for the switch, you can see the note with the current automatic backup schedule. For example, “The automatic configuration backup runs every 2 days at 14:00”.



- To mark an important backup, locate the backup item, and then click ☆ to change it to ★. Click ★ to downgrade it to a normal backup.

  The marked backup item will always be displayed here and cannot be overwritten by newer backup items. At most 2 backups can be marked with ★.
- To check the configurations of a backup, hover over the backup item, and then click **View**.
- To delete a backup, click **Delete**. In the pop-up window, click **Yes**.
- To check the currently running configurations on the switch, click **Current Config**.

  In the pop-up window, you can click **Show SET-format** to display the configurations in **set xx** format.

Return Merchandise Authorization

AmpCon-Campus supports Return Merchandise Authorization (RMA), which means replacing a failed PicOS switch with another switch of the same model. When the hardware of a PicOS switch fails and is replaced with a new switch, you can use RMA to configure the new switch based on the backup configuration of the old switch (the switch to be replaced).

In this way, you can seamlessly manage the new switch with AmpCon-Campus. The old switch will not be managed by AmpCon-Campus.

Guideline
Prerequisites
RMA Procedure

Guideline

The PicOS switches in any of the following cases cannot be replaced through RMA:

- Configurations are being pushed or waiting to be pushed to the switches.
- Reboot, upgrade, backup, RMA (Return Merchandise Authorization), or deletion tasks are running on the switches.
- The switches are being moved to another site.
- **License Audit** or **License Action** is currently in progress on the switches.

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the RMA process will fail.

Table 1. Prerequisites

Prerequisite	Reference Link
The old switch is managed by AmpCon-Campus and is currently online (connected to AmpCon-Campus).	• Onboarding PicOS Switches
The old switch has at least one configuration backup.	• Backing Up Configurations
The new switch configurations are added to the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server. After that, the new switch is rebooted.	• Configuring a DHCP Server
The new switch meets all the following conditions:	• No Reference

- It is not onboarded to AmpCon-Campus yet.
- It is up and able to connect to AmpCon-Campus.
- It has the same model as the old switch.
- It has PicOS installed.

RMA Procedure

1. In the AmpCon-Campus UI, select the site to which the old PicOS switch belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click the old switch.
3. In the side panel on the right, click the **Setting** tab. In the **Actions** section of the **Setting** tab, click **RMA**.
4. In the pop-up window, input the following information:

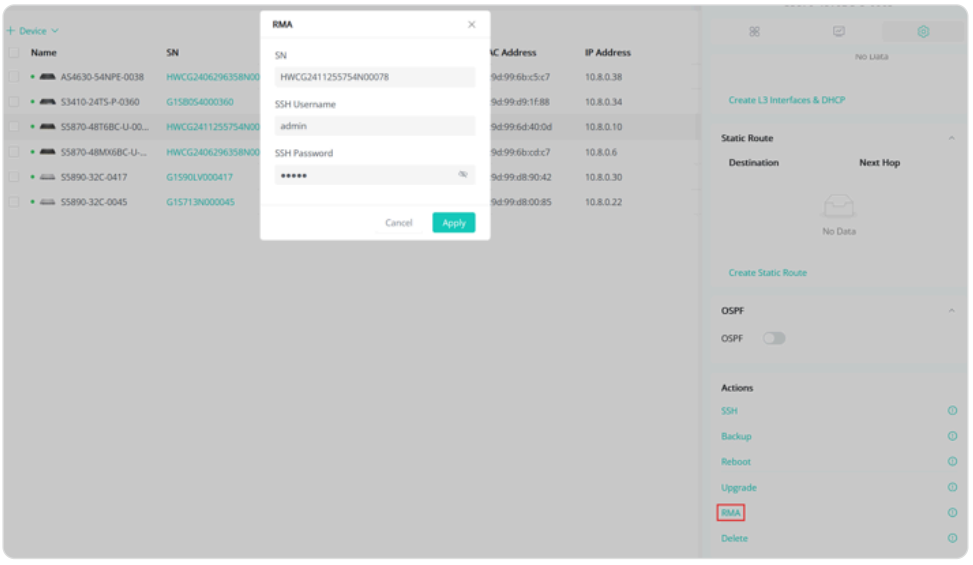
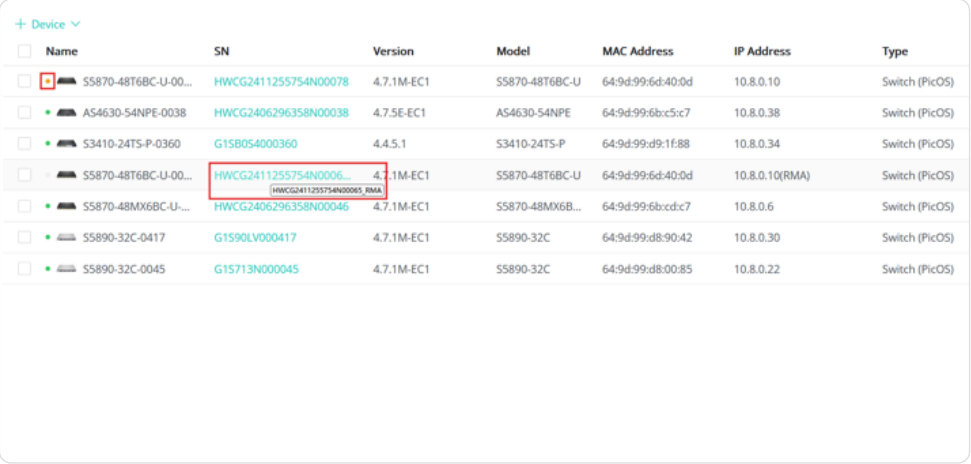


Table 2. RMA Parameters

Parameter	Description
SN	The serial number of the new switch.
SSH Username	The username to log in to the new switch. The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. The username can contain at most 32 characters.
SSH Password	The password of the user. Click the eye icon to see the clear-text password. **NOTE**

Ensure the username and password are valid for switch login. Otherwise, the RMA process will fail.

5. Click **Apply**. After the RMA process is completed successfully, the new switch will replace the old switch on related AmpCon-Campus pages.
6. On the “Devices” page, check whether the SN of the old switch ends with **_RMA** and whether the status circle of the new switch is in green.



Tip

Different circle colors indicate different statuses:

- **Green:** The switch is in **Online** status, which means the switch is successfully onboarded to AmpCon-Campus and is currently connected to AmpCon-Campus.
- **Grey:** The switch is in **Offline** status, which means the switch is successfully onboarded to AmpCon-Campus but is currently disconnected from AmpCon-Campus.
- **Yellow:** The switch is in **Never Online** status, which means the switch is added to AmpCon-Campus but hasn't connected to AmpCon-Campus.
- **Blue:** The switch is in **Provisioning** status, which means AmpCon-Campus is verifying the authentication information of the switch or establishing an OpenVPN tunnel with the switch.
- **Red:** The switch is in **Failed** status, which means the switch fails to be onboarded to AmpCon-Campus.

Managing Wireless Networks

AmpCon-Campus supports managing wireless networks and access points (APs), providing flexible and secure network management through enhanced wireless configuration, advanced radio frequency optimization, and robust management capabilities.

By using AmpCon-Campus, you can deploy, configure, maintain, and monitor APs more efficiently.

See the following child topics:

- Wireless Overview
- Deploying Wireless Networks
- Configuring Wireless Networks
- Maintaining Wireless Networks

> **NOTE**
>
> For how to monitor wireless networks, see Access Points, Dashboard, and Topology.

Wireless Overview

Before you deploy wireless networks, learn about the highlights of wireless network management, wireless network related concepts, and the Zero Touch Provisioning (ZTP) workflow of access points (APs).

- Concepts
- Highlights
  - Zero-Touch Provisioning
  - Simplified Wireless Network Configuration
  - Intelligent RF and Network Optimization
  - Powerful Platform Management and Integration
  - Comprehensive Telemetry and Diagnostics
- AP ZTP Workflow

Concepts

You need to understand wireless network related concepts. For more information, see Concepts.

Highlights

Zero-Touch Provisioning

AmpCon-Campus uses Zero Touch Provisioning (ZTP) to simplify wireless network deployment.

For more information, see AP ZTP Workflow.

Simplified Wireless Network Configuration

AmpCon-Campus simplifies wireless network configuration:

- **Multiple Service Set Identifier (SSID) support and radio management**
  - AmpCon-Campus supports configuring 2.4 GHz, 5 GHz, and 6 GHz radio bands. Each radio band can be configured with multiple SSIDs for enterprise, guest, and Internet of Things (IoT) scenarios.
  - Each SSID supports independent 802.1Q VLAN, 802.1d bridging, or NAT gateway mode, enabling fine-grained network segmentation.
- **Wi-Fi schedule (scheduled Wi-Fi on and off)**
  - AmpCon-Campus supports enabling or disabling specific SSIDs or radio bands based on a time schedule, optimizing energy consumption and network usage. For example, you can enable employee Wi-Fi during work hours and disable guest Wi-Fi at night.
- **Advanced authentication and security**
  - AmpCon-Campus supports multiple wireless security protocols, such as WPA, WPA2, WPA3 (Personal or Enterprise), and OWE, ensuring seamless mobile offloading and enterprise security.

- Management Frame Protection (MFP) can be configured to defend against wireless attacks.
- Captive Portal can be customized to simplify public Wi-Fi deployment.

  By enabling seamless authentication, wireless clients need to authenticate only one time through the Captive Portal. Subsequent connections will be automatically authorized until the session or validity period expires.

Intelligent RF and Network Optimization

AmpCon-Campus supports intelligent Radio Frequency (RF) and network optimization:

- **Autonomous radio resource management**
  - Supports scheduled and immediate network optimization. You can customize optimization rules for different scenarios.
  - Supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to optimize channels automatically and reduce interference.
  - Supports IEEE 802.11k, 802.11r, and 802.11v to improve client connection speed and roaming experience.
  - Supports Wi-Fi guide configuration for dynamic load balancing based on real-time network load.
- **Wi-Fi optimization**
  - Supports BSS coloring to minimize co-channel interference and improve performance in high-density environments.
    Supports allocation of uplink and downlink Orthogonal Frequency Division Multiple Access (OFDMA) sub-carrier to optimize spectrum usage.
  - Supports Channel Switch Announcement (CSA) to switch channels seamlessly.

Powerful Platform Management and Integration

AmpCon-Campus provides powerful wireless management and integration functions:

- **Intuitive web user interface**
  - Supports real-time monitoring of AP status, SSID configurations, and network performance.
  - Supports bulk configurations and firmware upgrade, simplifying large-scale network management.
  - Supports unified management of stations (STAs), providing insights into the entire connection process of each STA.
- **Security and reliability**
  - Supports northbound security interfaces and encrypted communication, ensuring management data security.

- Supports Link Layer Discovery Protocol (LLDP) for network topology discovery.

Comprehensive Telemetry and Diagnostics

AmpCon-Campus monitors telemetry data in wireless networks, provides network analysis reports, and helps you diagnose and troubleshoot network issues:

- **Real-time network telemetry**
  - Supports collecting telemetry metrics for APs, STAs, sites, and wireless networks, providing a data foundation for performance optimization and fault prediction.
- **Analytics and insights**
  - Provides network performance analysis reports to optimize decisions.
  - Supports real-time dashboards to display the connected STA count, uplink or downlink traffic, and active SSIDs.
- **Advanced diagnostic tools**
  - Provides system logs (Syslog) and health check reports to identify issues quickly.
  - Supports remote TTY shell (RTTY) and packet capture (PCAP) for real-time troubleshooting.

AP ZTP Workflow

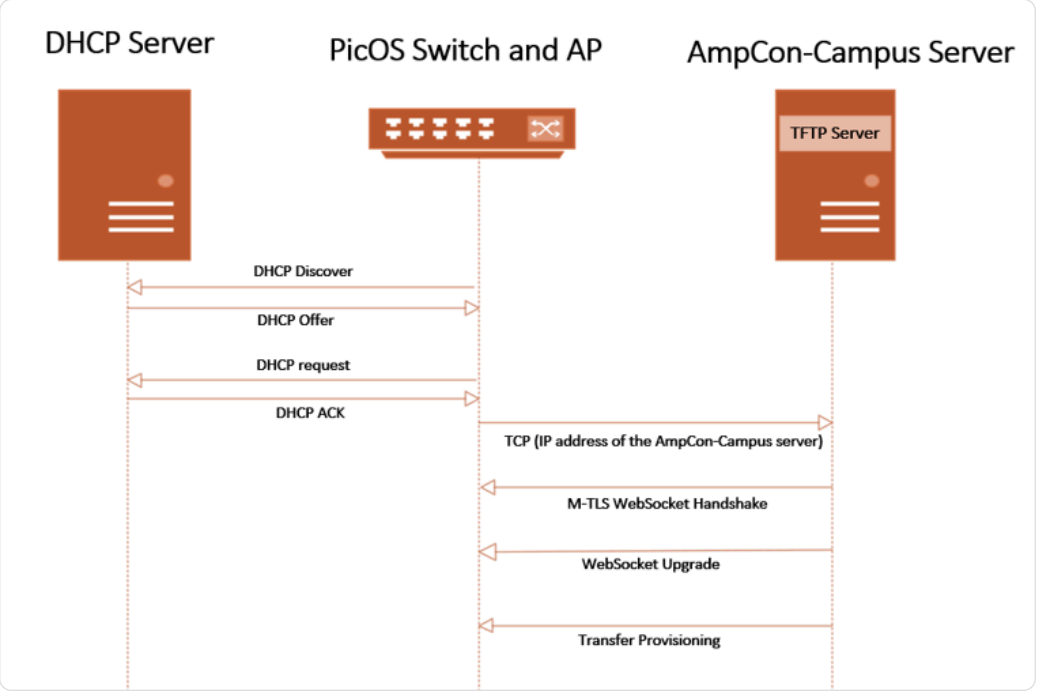
ZTP is an automated technology for deploying and configuring network devices. If a large number of APs need to be deployed, ZTP can reduce labor costs and improve deployment efficiency. ZTP enables fast, accurate, and reliable device deployment.

AmpCon-Campus uses ZTP to simplify AP deployment. When you onboard APs to AmpCon-Campus, the ZTP process starts. The APs will connect to AmpCon-Campus and retrieve site-level wireless configurations without manual intervention. Once completed, the wireless network is deployed, and the site-level wireless configurations will be pushed to the APs automatically.

By using AmpCon-Campus, remote sites no longer require experienced network personnel; anyone who can place the AP in the correct location and plug it into a power source can complete the deployment.

See the following workflow description:

Figure 1. AP ZTP Workflow



1. Network preparation:

   a. After a DHCP server is installed and ready, configure the DHCP server to reserve an IP range for APs.

   b. Configure DHCP Option 138 as the IP address of the AmpCon-Campus server, or add the IP address of the AmpCon-Campus server in the **Redirector IP/URL** field of the **Settings** section on each AP webpage.

   c. Add a site to AmpCon-Campus, and then configure site-level wireless configurations for the site, including SSID, radio, and advanced configurations.

   d. Onboard the APs to AmpCon-Campus, and assign the APs to the site.

2. DHCP request:

   a. After you plug in and power on the APs, each AP sends a DHCP Discover to the DHCP server.

   b. The DHCP server responds with a DHCP Offer, which not only includes the IP address, mask, gateway, and DNS of each AP, but also carries the IP address of the AmpCon-Campus server specified in DHCP Option 138 or on the AP webpage.

3. DHCP response:

   a. The AP selects the first valid DHCP Offer and completes the four-message DHCP process (DHCP Request > DHCP ACK).

   b. The AP is now reachable at Layer 3 and can resolve the IP address of the AmpCon-Campus server.

4. Discovery and connection:

a. Each AP attempts to establish a TCP connection to the AmpCon-Campus server through the IP address of the AmpCon-Campus server.

b. After the connection is successful, the TLS handshake process starts.

5. Mutual TLS (M-TLS) WebSocket Handshake:

   a. Each AP sends its pre-installed certificate as the client certificate.

   b. AmpCon-Campus validates the certificate chain.

   c. In the TLS tunnel, the HTTP request is upgraded to WebSocket to establish a bidirectional JSON-RPC streaming channel.

   d. After authentication, AmpCon-Campus identifies the model, serial number (SN), and MAC address of each AP, and matches each AP to its predefined site.

6. Transfer provisioning:

   a. AmpCon-Campus generates the full configurations based on site-level wireless configurations and pushes JSON configuration blocks to the APs through the WebSocket channel.

   b. After the configurations are pushed successfully, each AP sends a “Config Succeed” notification to AmpCon-Campus.

Concepts

Before you manage wireless networks, understand the following concepts:

- Basic Concepts
  - Access Point (AP)
  - Antenna
  - Basic Service Set Identifier (BSSID)
  - BSS Coloring
  - Captive Portal
  - Channel
  - Channel Switch Announcement (CSA)
  - Dynamic Frequency Selection (DFS)
  - Management Frame Protection (MFP)
  - Multiple Pre-Shared Keys (MPSK)
  - One-Click Network Optimization
  - Radio Band
    - 2.4 GHz Radio Band
    - 5 GHz Radio Band
    - 6 GHz Radio Band
  - Radio Frequency (RF)
  - Remote Authentication Dial-In User Service (RADIUS)
  - Roaming
  - Service Set Identifier (SSID)
  - Station (STA)
  - Universal Access Method (UAM)
  - Wireless Fidelity (Wi-Fi)
  - Wi-Fi Steering
  - Wireless NIC
  - 802.11 Standards
- Performance Concepts
  - AP Overloading
  - AP Transmission Power
  - Channel Width
  - Co-Channel Interference
  - Intermittent Connectivity
  - Modulation and Coding Scheme (MCS)
  - Noise
  - Received Signal Strength Indicator (RSSI)
  - Signal-to-Noise Ratio (SNR)

Basic Concepts

Access Point (AP)

The networking device that enables wireless devices (such as smartphones, laptops, and tablets) to connect to a wired local area network (LAN) or the Internet through Wi-Fi.

It acts as a bridge between wired and wireless networks, allowing wireless devices to communicate without using physical cables.

Antenna

The device that transmits or receives wireless signals for wireless data transmission between devices.

Basic Service Set Identifier (BSSID)

The unique 48-bit identifier assigned to each Basic Service Set (BSS) in a wireless network.

Typically, the value is derived from the MAC address of the AP.

BSS Coloring

The technology used in wireless networks to assign unique identifiers (colors) to different Basic Service Sets (BSS).

BSS Coloring enables efficient spectrum sharing and interference management within the same radio band.

Captive Portal

The authentication and access control technology forcibly redirecting users to a login page for wireless network permission management.

Channel

The frequency range allocated within the radio spectrum for transmitting data. Each channel has its designated center frequency and bandwidth.

By allocating channels reasonably, mutual interference between devices can be reduced, and network performance can be improved.

Channel Switch Announcement (CSA)

The management frame mechanism through which an AP notifies stations (STAs) to switch channels. Notifications are triggered in the following scenarios:

- Channel interference or congestion avoidance
- Spectrum optimization (such as co-channel interference management of BSS Coloring)
- Regulatory compliance requirements (such as radar signal avoidance)

Dynamic Frequency Selection (DFS)

The technology used in wireless networks to avoid interference with radar systems (such as military, weather, or satellite radar), enabling spectrum sharing by dynamically detecting and switching channels.

Management Frame Protection (MFP)

The security technology used to add signing or encryption to 802.11 management frames.

MFP can help to prevent forgery, tampering, and replay attacks, thereby mitigating common wireless Denial of Service (DoS) and disconnection vulnerabilities.

Multiple Pre-Shared Keys (MPSK)

The technology used to assign different Pre-Shared Keys (PSKs) to different users or devices in a wireless network, enhancing wireless security and management flexibility.

One-Click Network Optimization

The function used to rapidly optimize wireless network performance, simplifying optimization processes and reducing operational complexity.

Radio Band

The frequency range allocated within radio waves for wireless communication. Different radio bands differ in wavelength, penetration, and transmission distances and are used for different network scenarios.

2.4 GHz Radio Band

Covers radio waves from 2.400 GHz to 2.4835 GHz (the exact range varies by region).

The 2.4 GHz radio band provides extensive coverage but is susceptible to interference from other electronic devices.

5 GHz Radio Band

Covers radio waves from 5.170 GHz to 5.850 GHz (the exact range varies by region).

The 5 GHz radio band is fast in transmission speeds but weak in signal penetration.

6 GHz Radio Band

Covers radio waves from 5.925 GHz to 7.125 GHz (the exact range varies by region).

The 6 GHz radio band combines the advantages of wide coverage and large transmission capacity.

It provides faster transmission speeds and lower latency and resolves connectivity and congestion issues, meeting the demands of high-performance gaming and high-definition multimedia.

Radio Frequency (RF)

The high frequency alternating electromagnetic waves with a frequency range of 30 kHz to 300 GHz.

RF is used to transmit digital signals by modulating the amplitude, frequency, or phase of carrier waveforms.

Remote Authentication Dial-In User Service (RADIUS)

The network protocol used to provide centralized Authentication, Authorization, and Accounting (AAA) services for users to access network resources.

Roaming

The technology that allows wireless devices to automatically switch the network connection from one AP to another, while maintaining an uninterrupted connection.

Service Set Identifier (SSID)

The logical name of a wireless network. SSIDs serve as critical identifiers to distinguish different wireless networks.

Station (STA)

The device connected to a wireless network through a wireless network card or built-in Wi-Fi module. The STA might be a laptop, smartphone, tablet, smart-home device, or others.

In a wireless network, an STA acts as a client, establishing a connection with an AP for network access.

Universal Access Method (UAM)

The web-browser-based access method. Users can connect to a wireless network after they access specific web pages to complete authentication.

Wireless Fidelity (Wi-Fi)

The wireless Local Area Network (LAN) technology based on the IEEE 802.11 standard. Wi-Fi enables network access and data transmission between devices through radio waves.

Wi-Fi Steering

The technology that guides STAs to connect to a more suitable radio band through intelligent algorithms, optimizing network load and performance.

Wireless NIC

The hardware component that enables an STA to connect to a wireless network.

It receives and transmits radio wave signals through antennas, enabling data transmission between the STA and wireless network.

802.11 Standards

A set of wireless networking communication standards established by IEEE. It covers multiple versions, such as 802.11a, 802.11b, 802.11be, 802.11g, 802.11n, 802.11ac, 802.11ax, 802.11k, 802.11r, and 802.11v.

802.11 standards provide the foundation for interoperability in wireless networks.

Performance Concepts

AP Overloading

The performance degradation issue occurring when an excessive number of STAs connect to one AP.

AP Transmission Power

The energy output level of AP radio frequency. A higher level of AP transmission power means:

- A larger signal coverage range
- A higher probability of interference from other wireless devices

Channel Width

The frequency range (such as 80MHz) occupied by wireless signals in the frequency spectrum.

It directly affects the data transmission rate, signal coverage range, and anti-interference capability in a wireless network. A wider channel width means:

- A higher data transmission rate
- A weaker signal penetration
- A smaller signal coverage range
- Higher probability of interference from other wireless devices

Co-Channel Interference

The issue that wireless devices on the same channel interfere with each other.

Intermittent Connectivity

The issue that the wireless network is unstable, often caused by co-channel interference or improper AP configurations.

Modulation and Coding Scheme (MCS)

The core technology used to dynamically adapt to channel conditions by defining the combination of parameters like modulation schemes, coding rates, and the number of spatial streams.

MCS is used to optimize the data transmission rate and reliability in a wireless network.

Noise

The unwanted electrical signals that interfere with the transmission and reception of wireless communication signals.

It is a key factor that affects the quality and reliability of wireless communication.

Received Signal Strength Indicator (RSSI)

The parameter to evaluate the strength of wireless signals. The RSSI value reflects the quality of wireless connections.

Signal-to-Noise Ratio (SNR)

The ratio of the useful signal power to the background noise power. The SNR value reflects the quality of wireless communication.

A higher SNR value indicates that the useful signal is stronger than the noise, resulting in more reliable data transmission and a lower Bit Error Rate (BER).

Deploying Wireless Networks

To deploy a non-mesh wireless network, complete the following tasks:

> **NOTE**
>
> To deploy a mesh network, see Mesh Network Scenario.

Task	Reference Link
1. Learn about wireless network-related concepts, highlights of wireless network management, and the Zero Touch Provisioning (ZTP) workflow of APs.	• Wireless Overview • Concepts
2. Select an existing site for the APs, or add a new site as needed.	• Adding a Site
3. Configure site-level wireless configurations for the site.	• Configuring All APs in a Site
4. Onboard APs to AmpCon-Campus. The ZTP process will start. The APs will connect to AmpCon-Campus and retrieve site-level wireless configurations without manual intervention. For the ZTP workflow, see AP ZTP Workflow. Once completed, the APs are managed by AmpCon-Campus, the wireless network is deployed, and site-level wireless configurations are pushed to the APs automatically.	• Onboarding APs
5. Confirm that AP onboarding succeeds, the APs become online, and the site-level wireless configurations are applied successfully. When possible, verify the expected SSIDs and connect a test client to confirm service availability.	• No Reference Link
6. Optional: After onboarding, add device-specific configurations to an AP when it requires configurations different from other APs in the site. **NOTE**	• Configuring a Single AP

You can configure a single AP only after you add site-level wireless configurations.

Mesh Network Scenario

In a store, warehouse, or office, wired uplink connections might not be available for every AP. In this case, APs connected to wired networks can be configured as mesh root APs, while the remaining APs operate as mesh child APs and access the network by connecting to mesh root APs.

AmpCon-Campus supports Zero Touch Provisioning (ZTP) for mesh APs. During mesh ZTP, on-site personnel can deploy a mesh network without the need to manually configure mesh SSIDs, security keys, or neighbor relationships.

This topic describes the workflow for deploying a mesh network containing one mesh root AP and two mesh child APs.

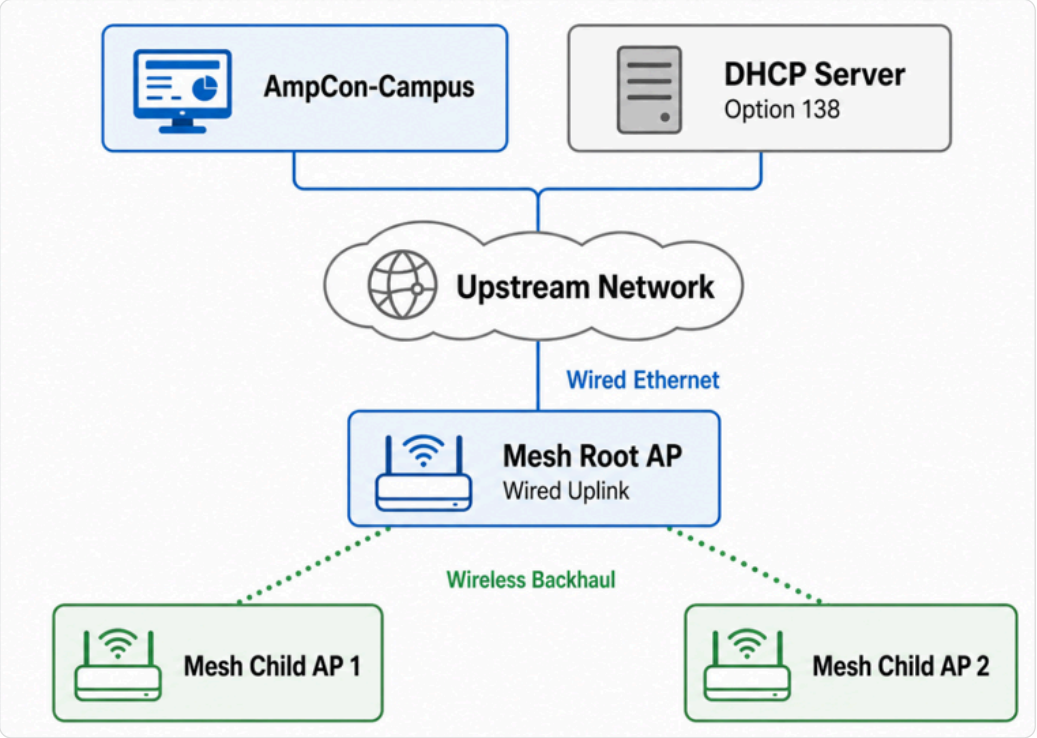
- Scenario Description
- Prerequisites
- Procedure
- Verifying the Mesh Network
- What to Do Next
- Troubleshooting

Scenario Description

In the following scenario, one mesh root AP with a wired uplink provides network access for the mesh child APs, and two mesh child APs without wired uplinks connect to the mesh root AP.

After ZTP is completed and the mesh connections are established, the mesh child APs can access the network through wireless backhaul links.

Figure 1. Mesh Network Scenario



Prerequisites

Before configuring the mesh network, ensure that the following prerequisites are met:

Table 1. Prerequisites for Mesh Networks

Task	Reference Link
• Ensure that the site to which the APs belong has been created.	• Managing Sites
• Ensure that the APs are supported by AmpCon-Campus.	• Supported APs for 3.0.0

• Ensure that a reachable DHCP server is available on the upstream network of the APs.
• Configure the DHCP server to reserve an IP range for these APs.
• Configure DHCP Option 138 as the IP address of AmpCon-Campus. See the following DHCP Option 138 configuration example:
`FS#con ter`
`Enter configuration commands, one per line. End with CNTL/Z.`
`FS(config)#ip dhcp pool STA`
`FS(dhcp-config)#option 138 ip [redacted] 64.34`
	• No Reference Link

• Ensure that the mesh root AP is connected to a wired network. An AP without a wired uplink cannot function correctly as a mesh root AP.	• No Reference Link

• The upstream network of the mesh root AP can reach both the DHCP server and AmpCon-Campus.	
• Ensure that the mesh child APs are within the effective wireless coverage area of the mesh root AP. • Effective wireless coverage depends on distance, physical obstructions, installation location, channel interference, and transmit power. Perform an on-site test before production deployment.	• No Reference Link

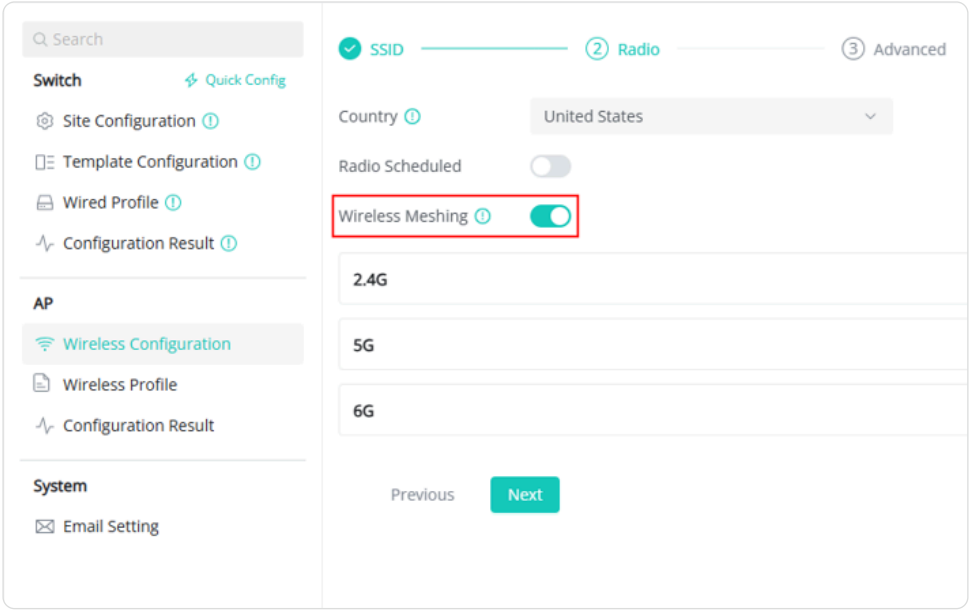
Procedure

Preparing Site-Level Wireless Configurations

1. Select the site to which the APs belong.
2. Click the **Settings** icon from the navigation bar, and then click **Wireless Configuration** in the sidebar.
3. Configure SSID, radio, and advanced configurations as needed, and then click **Apply**.

   For more information, see Configuring Wireless Networks.

> **NOTE**
>
> **Wireless Meshing** must be enabled before an AP can be configured as a mesh root AP.



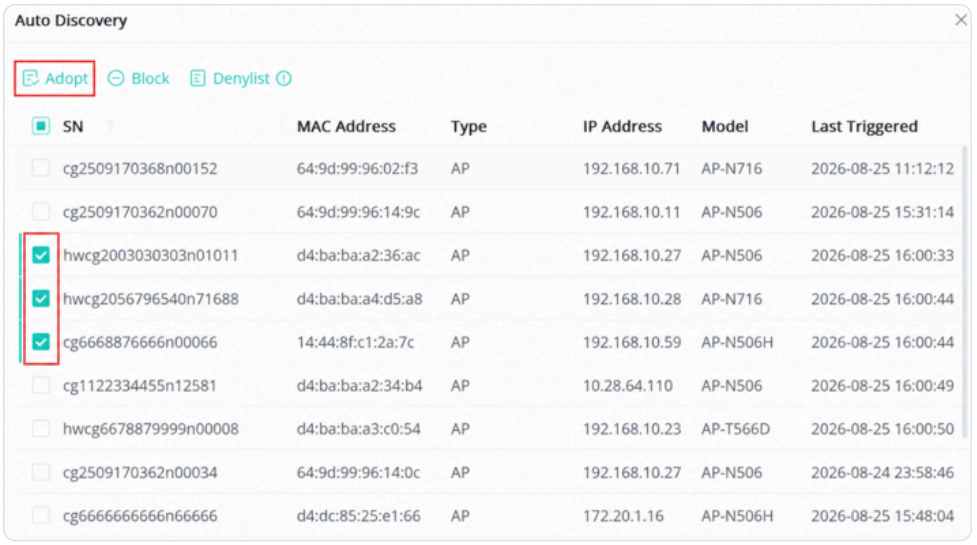
Onboarding APs to AmpCon-Campus

1. Within the same site, click the **Devices** icon from the navigation bar.

2. On the “Devices” page, onboard the mesh root AP and mesh child APs by adopting APs or importing APs by SN:

- To adopt APs, hover over **+ Device**, and then click **Auto Discovery**. Select the mesh root AP and mesh child APs, and then click **Adopt**.

> **NOTEs**
>
> - If the mesh child APs are not displayed in the auto-discovery list, onboard the mesh root AP and enable **Mesh Root** and **Mesh Onboarding** first. Then, the mesh child APs will be displayed in the auto-discovery list.
> - The mesh child APs must be in their factory-default state. If the mesh child APs have been configured, restore them to factory settings before onboarding these APs.



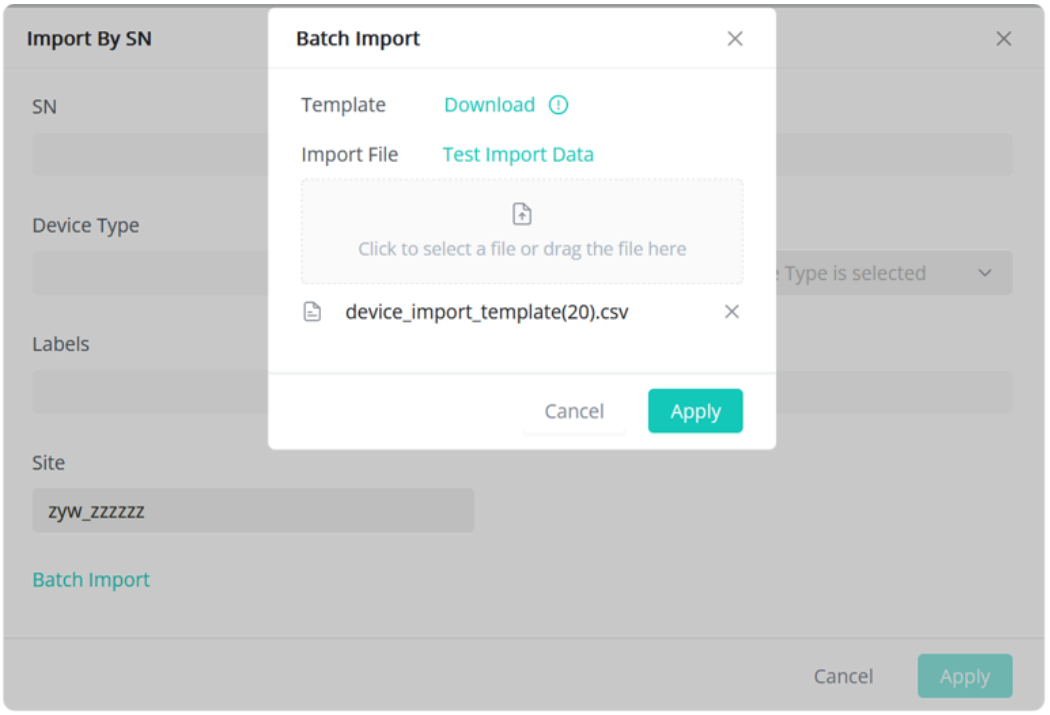
SN	MAC Address	Type	IP Address	Model	Last Triggered
cg2509170368n00152	64:9d:99:96:02:f3	AP	192.168.10.71	AP-N716	2026-08-25 11:12:12
cg2509170362n00070	64:9d:99:96:14:9c	AP	192.168.10.11	AP-N506	2026-08-25 15:31:14
hwcg2003030303n01011	d4:ba:ba:a2:36:ac	AP	192.168.10.27	AP-N506	2026-08-25 16:00:33
hwcg2056796540n71688	d4:ba:ba:a4:d5:a8	AP	192.168.10.28	AP-N716	2026-08-25 16:00:44
cg6668876666n00066	14:44:8f:c1:2a:7c	AP	192.168.10.59	AP-N506H	2026-08-25 16:00:44
cg1122334455n12581	d4:ba:ba:a2:34:b4	AP	10.28.64.110	AP-N506	2026-08-25 16:00:49
hwcg6678879999n00008	d4:ba:ba:a3:c0:54	AP	192.168.10.23	AP-T566D	2026-08-25 16:00:50
cg2509170362n00034	64:9d:99:96:14:0c	AP	192.168.10.27	AP-N506	2026-08-24 23:58:46
cg6666666666n66666	d4:dc:85:25:e1:66	AP	172.20.1.16	AP-N506H	2026-08-25 15:48:04

- To import APs by SN, hover over **+ Device**, and then click **Import by SN**. In the pop-up window, click **Batch Import**.

  Open the template file, and then enter correct information in the **SN**, **DeviceType**, **DeviceModel**, **Name**, **Labels**, and **Description** columns for the mesh root AP and mesh child APs.

	A	B	C	D	E	F
1	SN	DeviceType	DeviceModel	Name	Labels	Description
2	hwcg2056796540n71688	AP	AP-N716	AP-N716mesh-root-AP	label1$label2$label3	descriptionInfo
3	cg6668876666n00066	AP	AP-N506H	mesh-child-AP2	label1$label2$label3	descriptionInfo
4	hwcg2003030303n01011	AP	AP-N506	mesh-child-AP1	label1$label2$label3	descriptionInfo

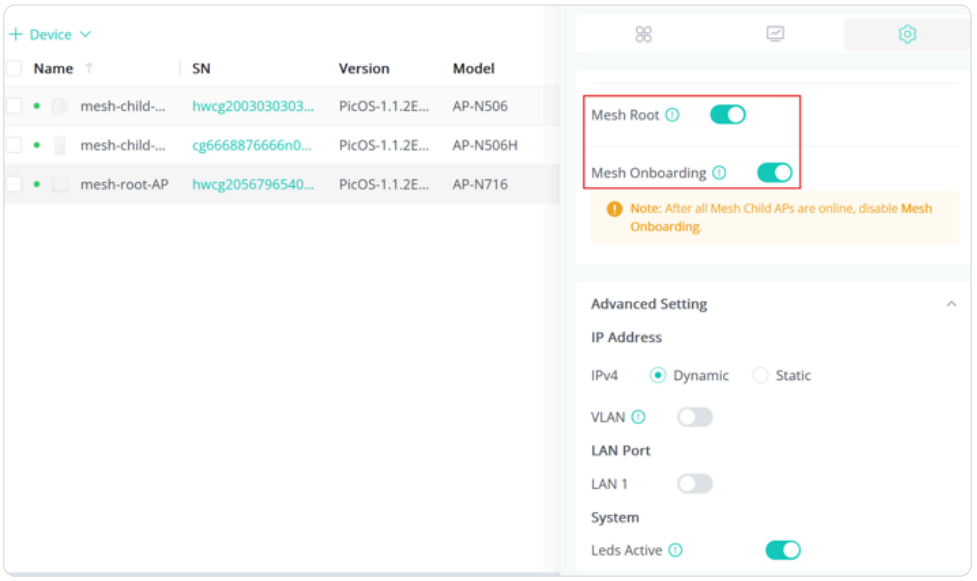
  In the **Import File** section, click the upload icon and select the template file, or drag and drop the template file. Then, click **Apply**.



Enabling an AP as the Mesh Root AP

1. On the “Devices” page, click the AP that will work as a mesh root AP. A side panel is displayed on the right.
2. Click the **Setting** tab of the side panel, toggle on **Mesh Root** to enable this AP as a mesh root AP, and ensure **Mesh Onboarding** is also enabled. Then, click **Apply**.

> **NOTE**
>
> When **Mesh Onboarding** is enabled, the mesh root AP broadcasts an SSID named **Pica8WiFi-Onboarding**.
>
> New mesh child APs will connect to this SSID in STA mode by using certificates to securely retrieve their initial network settings and platform configurations.

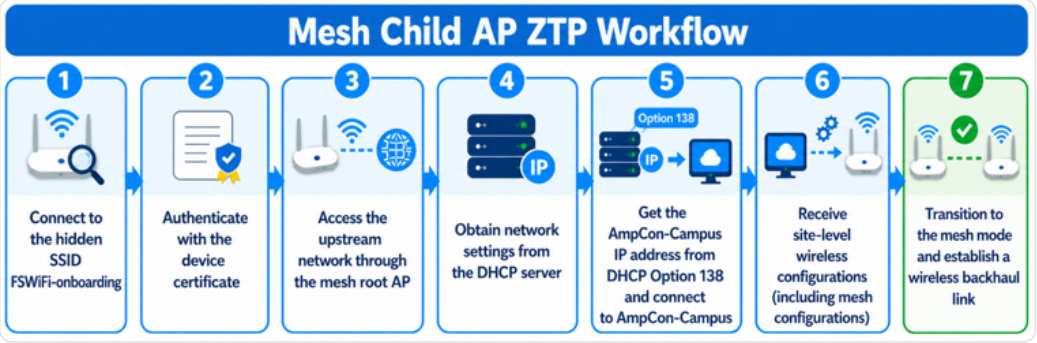


Plugging in and Powering on Mesh Child APs

Plug in and power on the mesh child APs. Wired uplink connections are not required for the mesh child APs.

Then, these mesh child APs will automatically complete the following ZTP process:

Figure 2. ZTP Process of Mesh Child AP

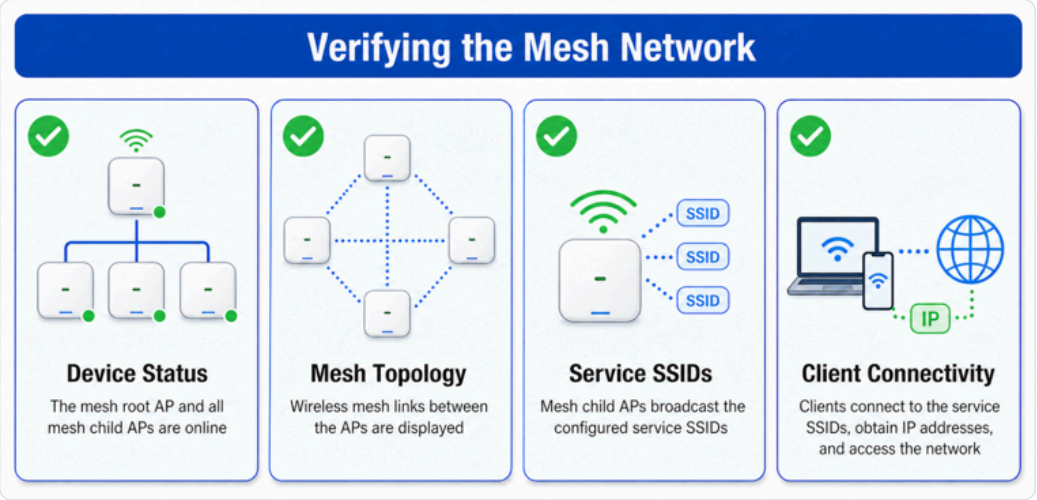


1. Search for and connect to the 2.4 GHz SSID **Pica8WiFi-Onboarding**, which is provided by the mesh root AP.
2. Use their device certificates for secure authentication.
3. Access the upstream network through the wireless connection provided by the mesh root AP.
4. Obtain an IP address, default gateway, and other network settings from the DHCP server.
5. Obtain the AmpCon-Campus IP address from DHCP Option 138, and initiate a connection to AmpCon-Campus.
6. Receive site-level wireless configurations (including mesh configurations) from AmpCon-Campus.
7. Transition from the onboarding connection mode to the mesh connection mode, and establish a wireless backhaul link with the mesh root AP.

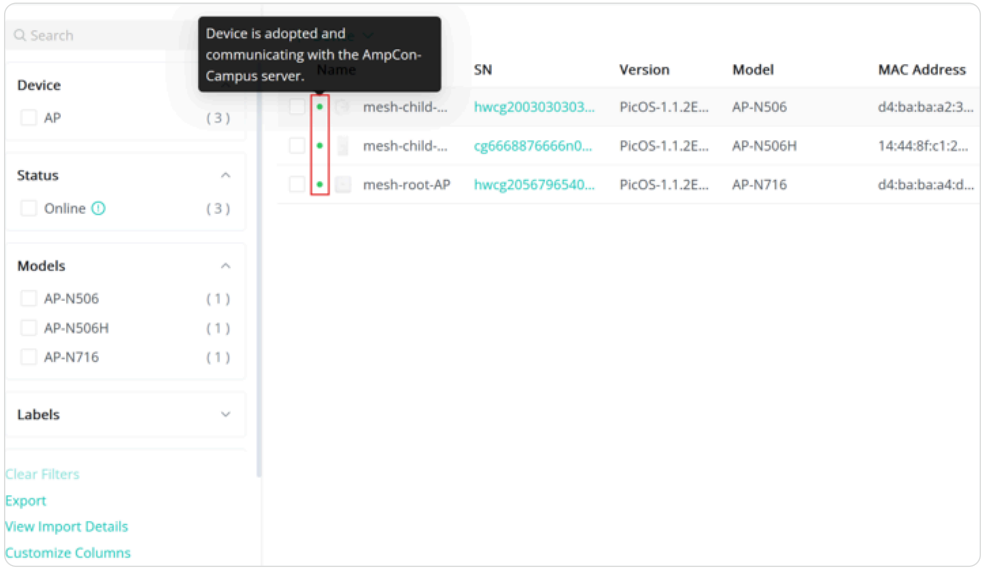
Verifying the Mesh Network

To verify the mesh network, complete the following tasks:

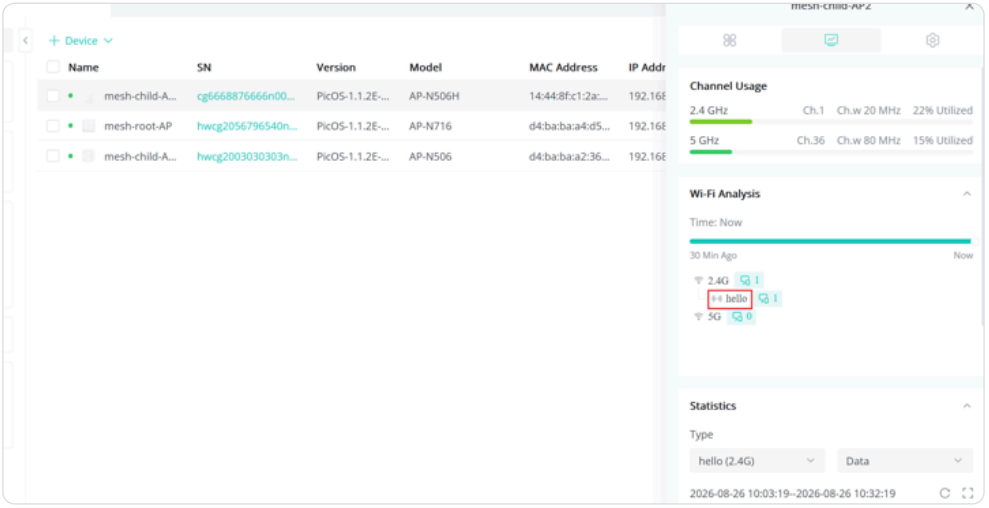
Figure 3. Verifying Tasks



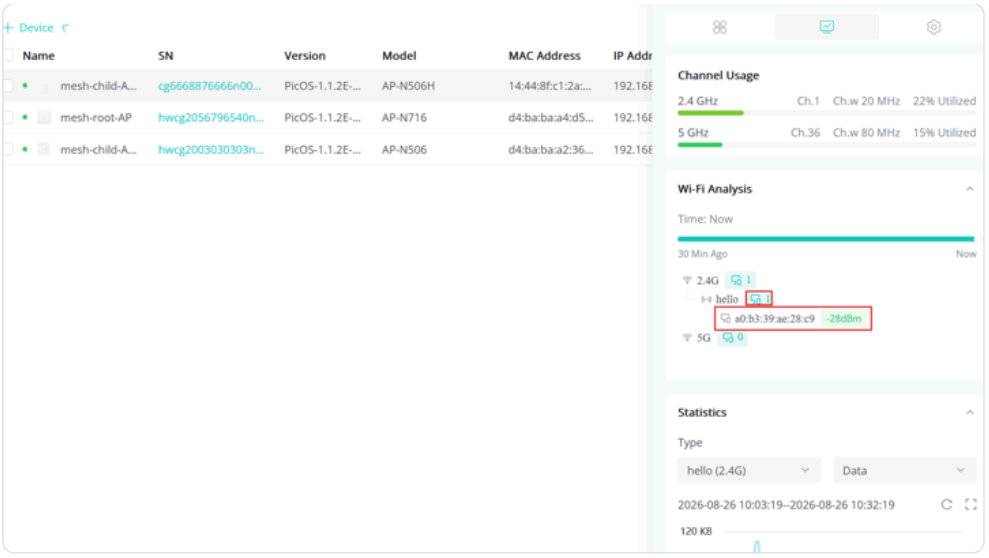
1. On the “Devices” page, verify that the mesh root AP and all mesh child APs are online (connected to AmpCon-Campus). You can check the status circle in the **Name** column. The color green means that the AP is online.



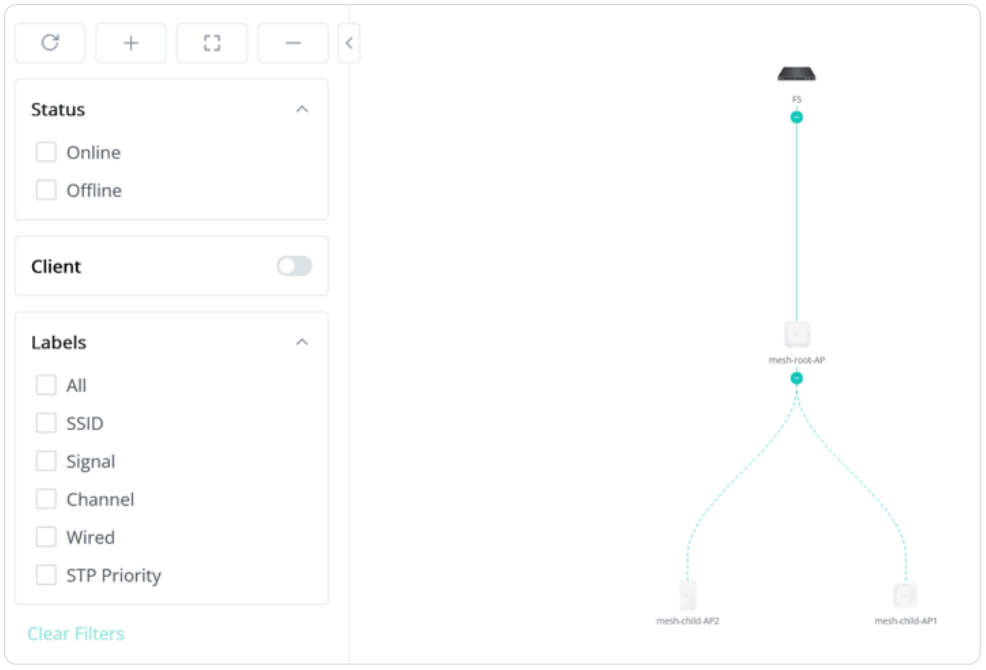
2. Verify that the mesh child APs are broadcasting the configured service SSIDs.



3. Verify that wireless clients can connect to the service SSIDs, obtain IP addresses, and access the network.



4. On the “Topology” page, verify that the wireless mesh links between the APs are displayed.

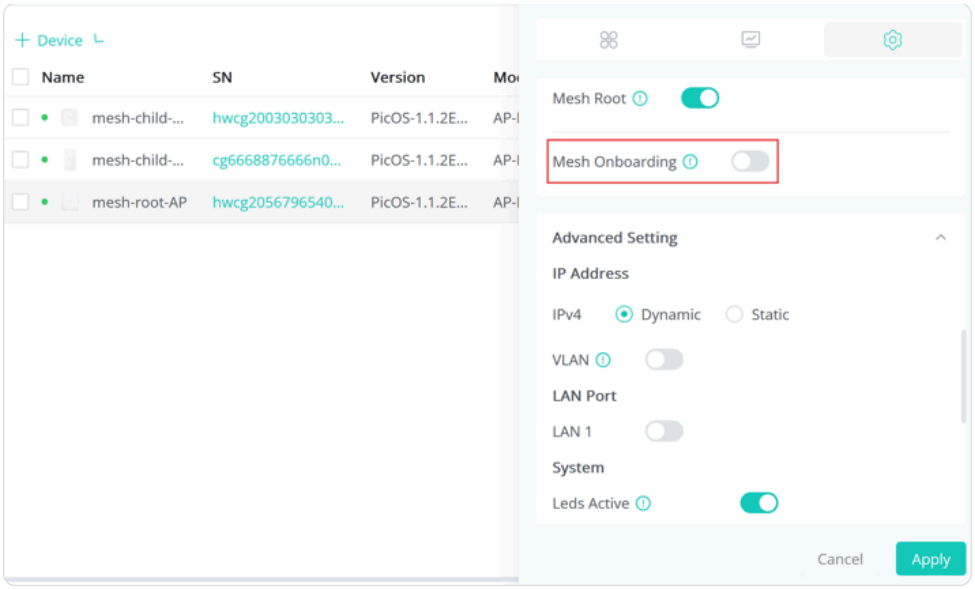


What to Do Next

After all mesh child APs are online, disable **Mesh Onboarding** for security concerns.

1. On the “Devices” page, click the mesh root AP in the device list, and then click the **Setting** tab in the sidebar.
2. Disable **Mesh Onboarding** by toggling it off, and then click **Apply**.

   The mesh root AP will stop broadcasting the SSID named **Pica8WiFi-Onboarding**. Temporarily enable **Mesh Onboarding** again when additional mesh child APs need to be added.



Troubleshooting

If a mesh child AP cannot join the network automatically, check the following points:

- Verify that the mesh root AP is online (connected to AmpCon-Campus) and connected to the wired network.
- Verify that the mesh child APs are able to connect to AmpCon-Campus.
- Verify that **Wireless Meshing** is enabled for the site.
- Verify that **Mesh Root** and **Mesh Onboarding** are enabled on the mesh root AP.
- Verify that the mesh child APs are onboarded to the same site as the mesh root AP.
- Verify that the mesh child APs are within the effective wireless coverage area of the mesh root AP.
- Verify that the upstream DHCP server is reachable.
- Verify that DHCP Option 138 contains the correct and reachable AmpCon-Campus IP address.

Configuring Wireless Networks

You can add site-level wireless configurations for a site. These configurations will be pushed to all the managed APs in the site.

After adding site-level wireless configurations, you can also fine-tune wireless configurations of a specific AP.

- Guidelines
- Prerequisites
- Configuring All APs in a Site
  - Adding SSID Configurations
  - Adding Radio Configurations
  - Adding Advanced Configurations
- Configuring a Single AP
- Checking Configuration Results

Guidelines

- You can configure a single AP only after you add site-level wireless configurations. For more information, see Configurations and Operations of an AP.

  Any custom configurations applied to a single AP will be pushed to that AP as device-specific configurations, while other wireless parameters defined in site-level configurations are still applied to the AP.
- After you move an AP to another site or onboard an AP to a site, if the site has site-level wireless configurations, the configurations will be automatically pushed to the AP. This might cause temporary network disruption.
- AmpCon-Campus supports up to 16 SSIDs per radio for N506 and N716 APs and up to 8 SSIDs per radio for N516, N506H, and T566D APs. To ensure system stability, SSIDs exceeding this limit cannot be applied.
- Each mesh child AP occupies 1 slot on the 5 GHz radio. Each mesh root AP occupies 1 slot on the 5 GHz radio and 1 slot on the 2.4 GHz radio (for bootstrap).

Prerequisites

Ensure that the APs to be configured meet the following prerequisites:

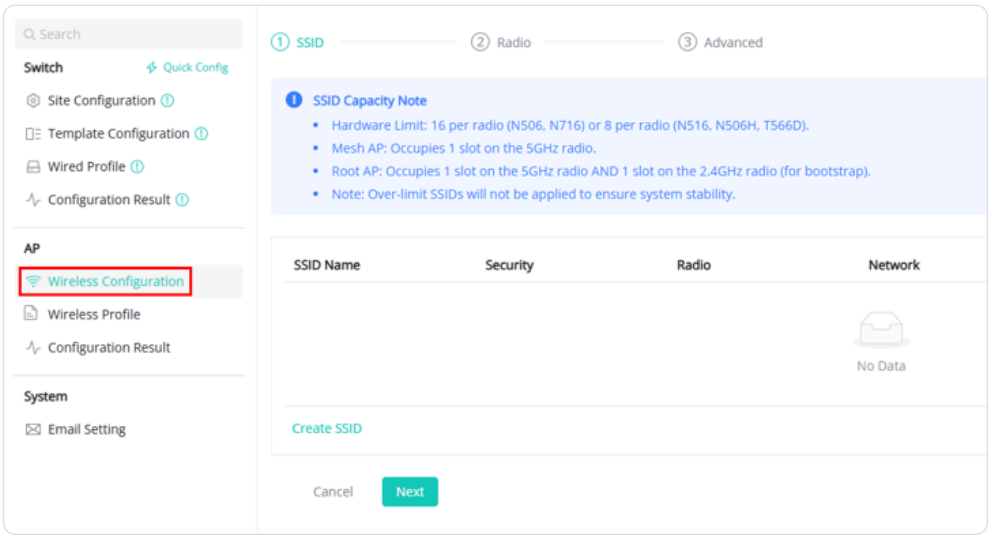
Table 1. Prerequisites

Prerequisite	Reference Link
Onboard APs to bring them under AmpCon-Campus management.	• Onboarding APs
Ensure that the APs are online (connected to AmpCon-Campus).	• Viewing the AP List

Configuring All APs in a Site

To add site-level wireless configurations, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Settings** icon from the navigation bar, and then click **Wireless Configuration** in the sidebar.



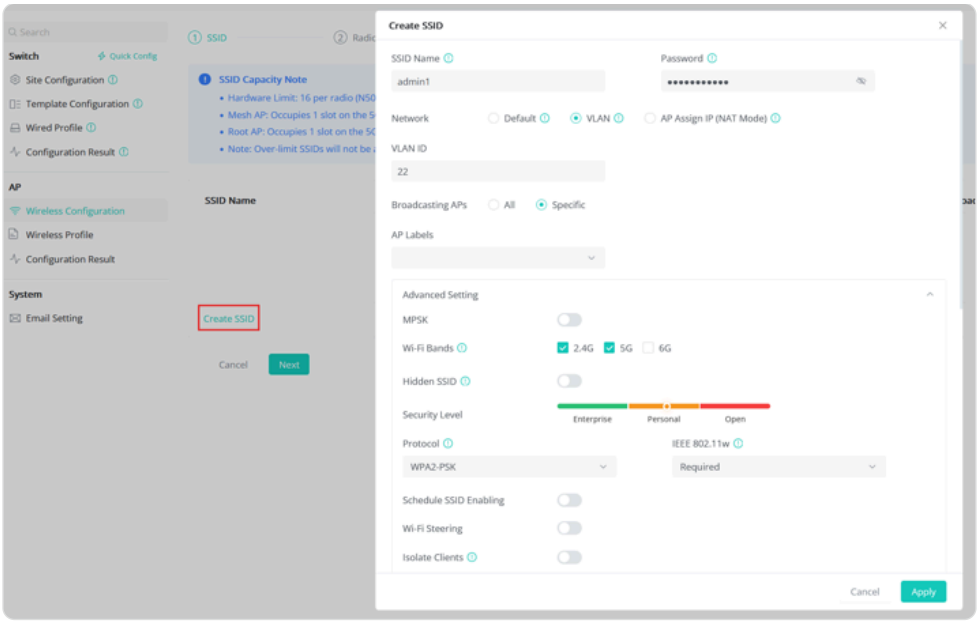
Then, you can add SSID, radio, and advanced configurations.

> **NOTE**
>
> All the following configurations (SSID, radio, and advanced configurations) are optional. Add only the configurations that you need. AmpCon-Campus will apply only the added configurations to APs in the selected site.

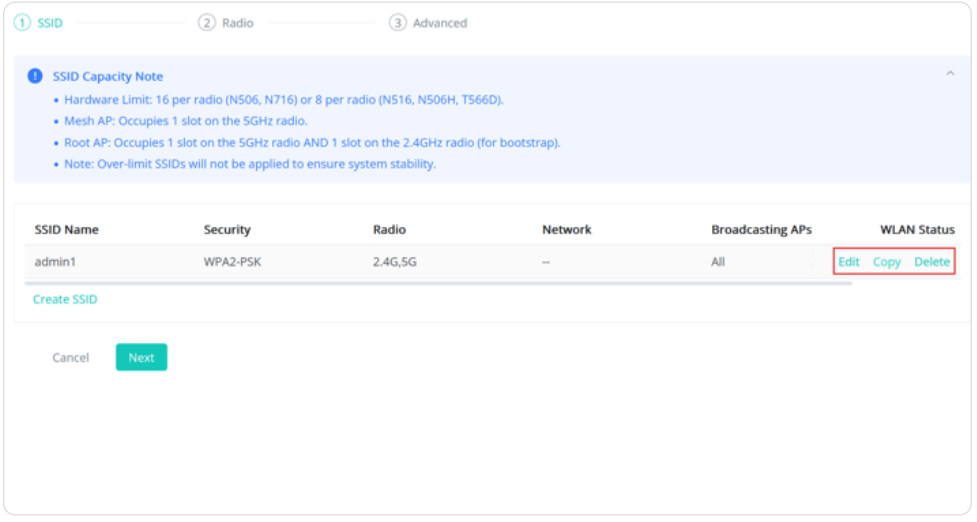
Adding SSID Configurations

1. In the **SSID** tab, click **Create SSID**.
2. In the pop-up window, configure SSID-related parameters, and then click **Apply**.

   For SSID parameters, see SSID Configurations.



3. Optional: Edit, copy, or delete SSID configurations as needed.



- To edit configurations of an SSID, hover over the SSID, and then click **Edit**. In the pop-up window, edit SSID configurations, and then click **Apply**.
- To delete an SSID, hover over the SSID, and then click **Delete**. In the pop-up window, click **Yes**.
- To copy an SSID, hover over the SSID, and then click **Copy**. In the pop-up window, click **Apply**.

4. Click **Next** to go to the **Radio** tab.

Adding Radio Configurations

1. In the **Radio** tab, configure radio-related parameters, and then click **Next**.

   a. Input the following basic configurations:

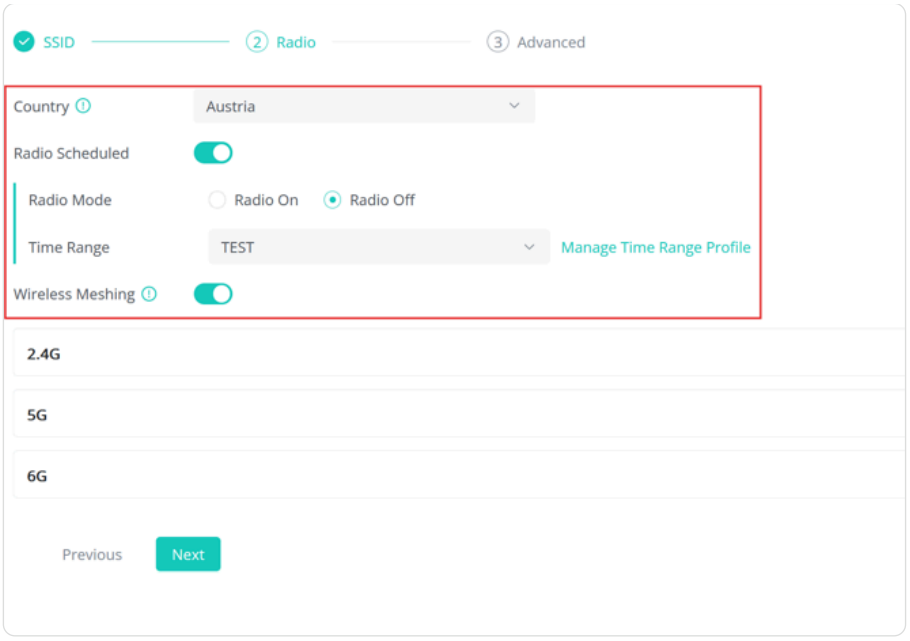
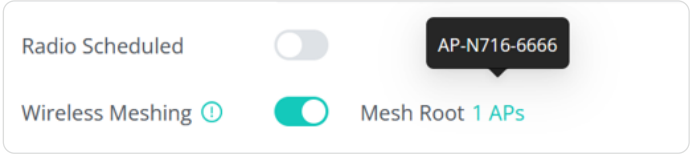


Table 2. Basic Radio Parameters

Parameter	Description
Country	The country where the APs are deployed. **NOTEs** • Available radio configurations, including supported radio bands, channels, and maximum transmit power, vary by country to comply with local regulatory standards. You must select the corresponding country code based on the location of the APs. • Changing the country will reset your custom channel, channel width, and transmit power configurations. This action will cause temporary network disruption. • To keep existing mesh links active, custom 5G radio configurations for mesh root APs and mesh child APs will remain unchanged. All the other radio settings will be reset.
Radio Scheduled	Toggle it on to set time-based policies for enabling or disabling radio. **NOTE** When both the SSID and radio have time-based policies configured, the radio's time-

	based policy takes precedence. For time-based policies of SSIDs, see SSID Configurations - Advanced Configurations.
Radio Mode	Select **Radio On** or **Radio Off** to enable or disable radio. **NOTE** This section is available only when you toggle **Radio Scheduled** on.
Time Range	The time range during which radio is enabled or disabled. Select a time range from the drop-down list. To add a time range, click **Create Time Range Profile** from the drop-down list. If you click **Manage Time Range Profile**, you will be redirected to the **Time Range** tab of the "Wireless Profile" page. For more information, see Adding Time Range Profiles. **NOTE** This section is available only when you toggle **Radio Scheduled** on.
Wireless Meshing	Toggle it on to enable **Wireless Meshing**. APs will connect wirelessly to each other to extend Wi-Fi coverage. After you enable **Wireless Meshing**, if some APs in this site work as mesh root APs, you can see **Mesh Root x APs**. For example, **Mesh Root 2 APs**, which means the site has 2 mesh root APs. Hover over **2 APs**, and then you can see the mesh root AP names.  **NOTEs**

- To configure an AP as a mesh root AP, go to the AP side panel. In the **Setting** tab, toggle on **Mesh Root** . For more information, see Configurations and Operations of an AP - Radio Configurations.
- Disabling **Wireless Meshing** will prevent new devices from being adopted wirelessly:
  - **No New Mesh Roots:** You will no longer be able to configure new APs as mesh root APs.
  - **Existing Links Remain Active:** Currently operating mesh root APs and mesh child APs will not be automatically demoted to non-mesh APs or disconnected.
  - **How to Demote:** To revert an existing mesh root AP to a non-mesh AP, go to the AP side panel. In the **Setting** tab, either click **Enforce Site Config** or toggle off **Mesh Root**.

    Updating site-level wireless configurations alone will not demote the mesh root AP.

b. Unfold the **2.4G Radio**, **5G Radio**, or **6G** section to configure parameters related to each radio band.

NOTE

Some AP models or the countries where the APs are deployed don't support some radio bands (such as 6G). After you configure the radio band, though the configurations are pushed to these APs, the radio band configurations will not work.

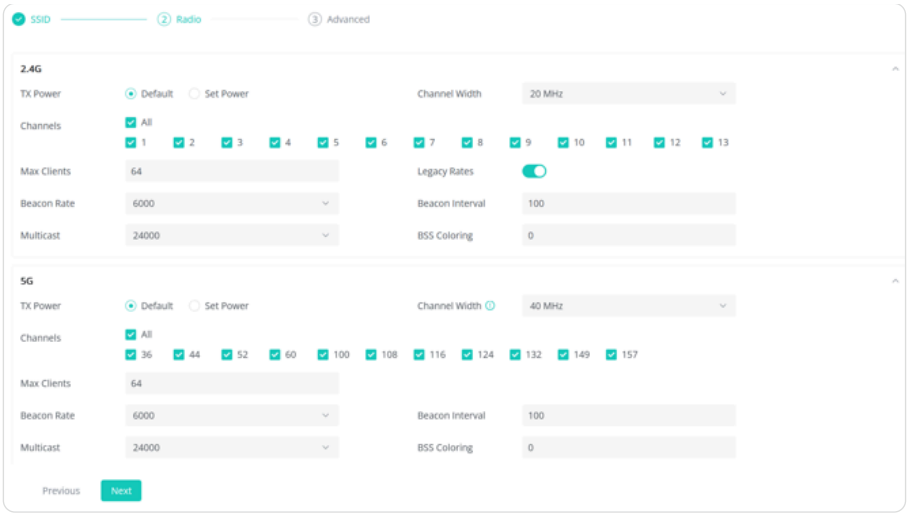


Table 3. 2.4G, 5G, and 6G Radio Parameters

Parameter	Description
TX Power	The transmit power of the radio. Select **Default** or **Set Power**. • **Default:** APs will work at the maximum transmit power that the located country allows. • **Set Power:** APs will work at a customized transmit power. You can customize the transmit power within the range of 1 to 30. The unit is dBm. **NOTE** The maximum TX power limit might vary depending on the country code.
Channel Width	The continuous frequency span allocated to a wireless channel. **NOTEs** • The supported channel widths for each radio band differ by country. • If the configured channel width is not supported by an AP, the AP will automatically fall back to its maximum supported channel width.
Channels	The channels of the radio. Each channel is a sub-division within a radio band for transmitting and

	receiving wireless signals. You can select one or multiple channels. If you click **All**, all the channels will be selected automatically. **NOTEs** • The AP channel set is dynamically adjusted based on the selected **Channel Width**. • APs will select the optimal channel for communication within the chosen channel set according to the Radio Frequency (RF) environment.
Max Clients	The maximum number of wireless clients allowed to connect to the current radio. The value must range from 1 to 2007. If this threshold is exceeded, wireless clients cannot connect to the radio. **NOTE** This value is accumulative for all attached Virtual Access Point (VAP) interfaces. For example, if the **Max Clients** value of the 2.4G radio is 64 and the 2.4G radio is bound with multiple SSIDs, at most 64 wireless clients can connect to all these SSIDs.
Legacy Rates	Toggle it on to enable support for legacy data rates. Once enabled, older devices (such as outdated phones or laptops) that support only 802.11b/g can connect to Wi-Fi. **NOTE** This section is available only for 2.4G radios.
Beacon Rate	The transmission rate of Beacon frames, measured in Kbps. Beacon frames are management frames periodically broadcast by APs to announce some critical

	information, such as network presence, SSID broadcast, and timestamp synchronization. • If the value is too large, older devices that support only 802.11b/g might fail to decode Beacon frames, and these devices will fail to discover the wireless network. • If the value is too small, the airtime resources might be wasted.
Beacon Interval	The interval of sending Beacon frames, measured in milliseconds (ms). The value must range from 15 to 1000. If the interval is 100 ms, it means that 10 Beacon frames are sent every second. See the following calculation: **1000 ms ÷ 100 ms = 10**
Multicast	The multicast rate that the Basic Service Set (BSS) uses, measured in Kbps.
BSS Coloring	Whether to enable BSS coloring on the Physical Layer (PHY). The value must range from 0 to 64. • **0:** Disables this feature. • **1 to 63:** Manually defines a specific BSS color identifier. • **64:** Automatically allocates a random color.
Allow DFS	Toggle it on to enable Dynamic Frequency Selection (DFS) channels for the radio. Once enabled, APs will automatically detect radar channels and switch channels upon detection. This provides more available bandwidth and reduces interference, but might cause disconnections if radar signals are detected nearby. **NOTE** This section is available only for 5G radios.

2. Click **Next** to go to the **Advanced** tab.

Adding Advanced Configurations

1. In the **Advanced** tab, configure the following advanced parameters:

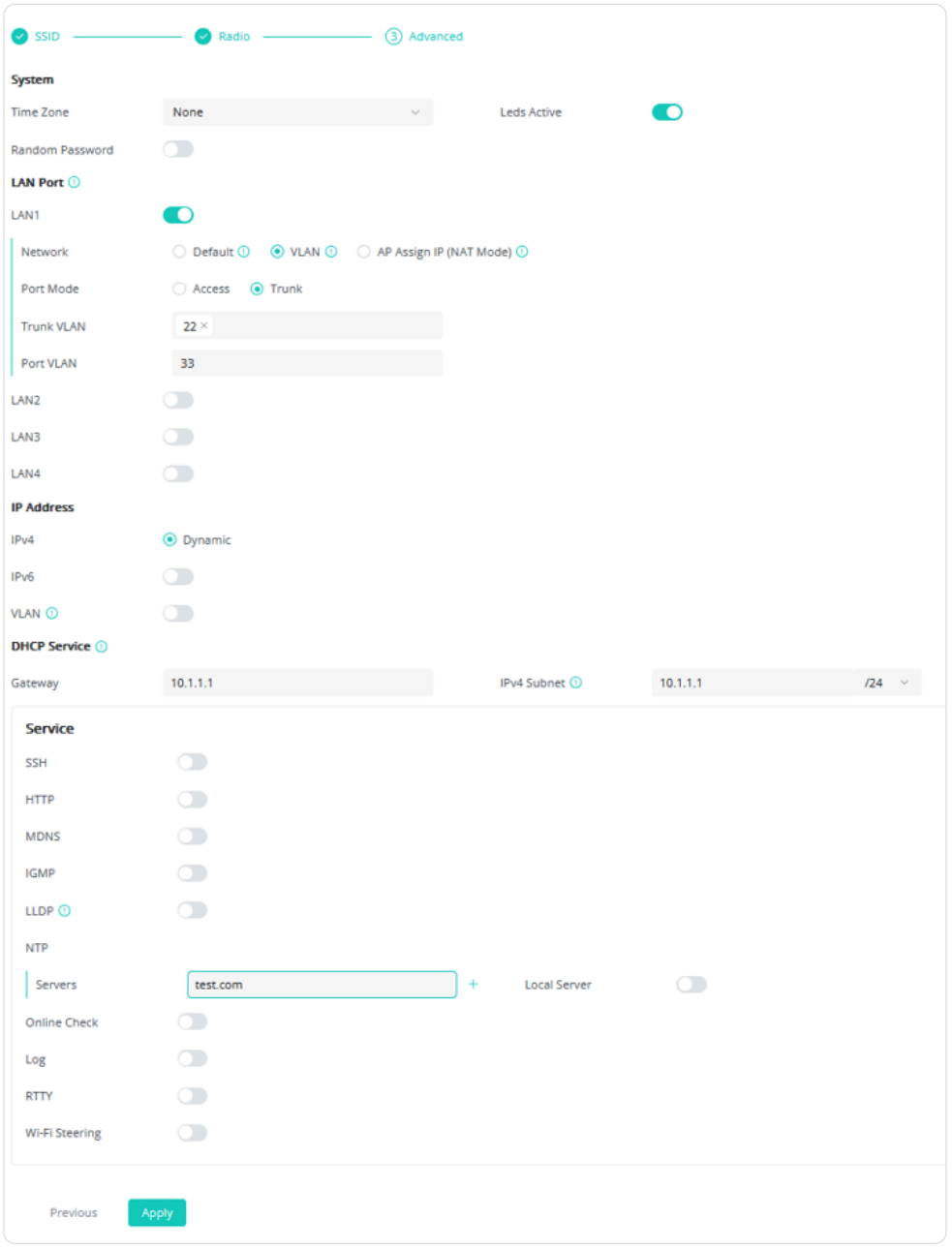


Table 4. Advanced Parameters

Category	Parameter	Description
System	**Timezone**	The time zone of the APs. **None** means the UTC+0 time zone.
	Leds Active	Toggle it on to force all LED lights to turn on. Toggle it off to force all LED lights to turn off.
	Random	Toggle it on to generate a random root password for the AP.

	Password	You can check the password in the **Overview** tab of the device page. For more information about the **Overview** tab, see Basic Information of an AP.
LAN Port	**Network**	Toggle on to enable LAN ports, or toggle off to disable them. After you toggle on a LAN port, select how downstream wired devices access the upstream network. • **Default:** In this mode, the physical port acts as a basic port, and data traffic is directly forwarded in Bridge mode. Terminal devices connected to this LAN port obtain IP addresses directly from the upstream network and are in the same LAN segment as the AP's management IP. • **VLAN:** In this mode, you can perform fine-grained isolation and tag management for port traffic. Wired terminals can be assigned to specific service subnets to achieve complete isolation from other networks (such as guest wireless networks). • **AP Assign IP (NAT Mode):** In this mode, each AP operates in Network Address Translation (NAT) mode and acts as a gateway. Each AP assigns an independent private IP address (the private 10.1.1.0/24 network) to the downstream device. APs perform NAT when the downstream device connects to the internet. Make sure that the upstream network does not contain a 10.1.1.0/24 subnet. If the upstream network contains a 10.1.1.0/24 subnet, modify the subnet by going to the **DHCP Service** section. **NOTEs** • The configurations of a specific LAN port can take effect only if the APs have the

	LAN port. ◦ AP-N716 APs have only LAN 1. ◦ AP-N516 APs have only LAN 1. ◦ AP-N506 APs have only LAN 1. ◦ AP-N506H APs have LAN 1, LAN 2, LAN 3, and LAN 4. ◦ AP-T566D APs have no LAN ports. • If a LAN port is not connected to any client device, it is recommended to disable the LAN port for network security purposes. In this way, you can prevent unauthorized devices from accessing the network through physical Ethernet cables.
Port Mode	The mode of the LAN port, **Access** or **Trunk**. • **Access:** Mainly used to connect terminal devices such as PCs. All packets sent to and received by terminal devices are untagged. APs automatically add or remove VLAN tags for these packets internally. • **Trunk:** Mainly used to connect network devices that support VLANs, such as switches and routers. Packets with specific VLAN tags are allowed to pass through the trunk port, enabling transparent VLAN transmission across devices. **NOTE** This section is displayed only if you select **VLAN** in the **Network** section.
Trunk VLAN	The VLAN allowlist of the LAN port. You can enter one or multiple VLAN IDs. After you enter a VLAN ID, ensure to press **Enter**. Only the packets from the VLAN allowlist are permitted to pass through the LAN port. Packets

		from VLANs not included in the allowlist will be discarded by the LAN port. **NOTEs** • This section is displayed only if you select **VLAN** in the **Network** section and select **Trunk** in the **Port Mode** section. • The **Trunk VLAN** list and the **Port VLAN** list cannot contain overlapping VLAN IDs.
	Port VLAN	The default VLAN membership of this LAN port. When a port receives untagged packets, the AP will automatically assign the port to the default VLAN ID. The VLAN ID must range from 2 to 4048. **NOTEs** • This section is displayed only if you select **VLAN** in the **Network** section. • The **Trunk VLAN** list and the **Port VLAN** list cannot contain overlapping VLAN IDs.
IP Address	**IPv4**	You must select **Dynamic** to make each AP act as a DHCP client and obtain an IPv4 address from the DHCP server.
	IPv6	Toggle it on to make each AP obtain an IPv6 address from the IPv6 address pool of the DHCP server.
	VLAN	Toggle it on to configure a management VLAN for each AP. Then, enter a VLAN ID ranging from 2 to 4048. • If the function is disabled, wireless clients will be in the same subnet segment as connected APs. • If the function is enabled, you can configure a VLAN ID for the SSID to make the AP work in Bridge mode. Then, LAN ports will operate on an independent subnet.

		NOTEs • Do not enter the native VLAN ID of the uplink switch. Otherwise, the wireless network will not work. • Ensure the new VLAN is allowed (tagged) on all upstream switch ports to avoid client device unreachability.
DHCP Service	**DHCP Service**	If you enable the NAT mode for APs, the APs can assign IP addresses to wireless clients. To make the NAT mode work, you need to configure an IP address pool (DHCP pool). Input the following information of the DHCP pool: • **Gateway**: The IPv4 address of the gateway, such as 192.168.1.12. • **IPv4 Subnet**: The IPv4 subnet address, such as 192.168.1.0/24. The value is pre-filled based on the gateway IP address. You can specify the prefix length. **NOTE** The DHCP gateway cannot be a loopback address, multicast address, broadcast address, or network address.
Service	**SSH**	Toggle it on to enable the SSH remote access. Once enabled, configure the following parameters: • **Port:** The SSH port used to connect to an AP through SSH. The port value must range from 1 to 65535. • **Password Authentication:** Toggle it on to enable the password authentication. • **Authorized Keys:** The public SSH keys used for authentication. You can add one or multiple SSH keys. To add an SSH key, enter the key, and then click **+**. To delete an SSH key, click **-**.

	NOTEs • If the password authentication is enabled, the **Authorized Keys** field is not displayed. • If the password authentication is disabled, the SSH key authentication will be used. In this case, you must enter public SSH keys in the **Authorized Keys** section. • Different services (SSH, HTTP, Log, and RTTY) cannot use the same port.
HTTP	Toggle it on to enable the HTTP web interface access. Once enabled, configure the HTTP port in the **HTTP Port** field. The port value must range from 1 to 65535. Then, you can access an AP web interface by entering its IP address in a browser. **NOTE** Different services (SSH, HTTP, Log, and RTTY) cannot use the same port.
MDNS	Toggle it on to enable the Multicast DNS (MDNS) service. Once enabled, wireless clients can be accessed through names instead of IP addresses. Devices (such as AirPlay speakers and network printers) in a local network can discover each other automatically. **NOTE** In large-scale enterprise networks, enabling MDNS might generate additional multicast traffic, potentially impacting performance. If you don't need automatic device discovery, disable the MDNS service.

IGMP	Toggle it on to enable the IPv4 IGMP service. Once enabled, multicast group members can be managed, and multicast streams can be forwarded to subscribed terminals. IPv4 IGMP service can help avoid network bandwidth waste and better support multimedia and real-time data transmission scenarios, such as IPTV, video conferences, and screen casting that rely on multicast.
LLDP	Toggle it on to enable the Link Layer Discovery Protocol (LLDP) service. Once enabled, each AP will broadcast its name, location, and other information at Layer 2. This service is most helpful for visual topology and rapid troubleshooting. **NOTEs** • LLDP is automatically enabled in mesh networking. • If **Wireless Meshing** is enabled in site-level radio configurations, LLDP cannot be disabled because mesh APs require LLDP to obtain connection relationships. • Disabling LLDP will affect the generation of network topology.
NTP	Toggle it on to enable the Network Time Protocol (NTP) service. Once enabled, configure the following parameters as needed: • **Servers:** The Fully Qualified Domain Name (FQDN) or IP address of the upstream NTP servers. AmpCon-Campus provides 3 NTP servers. You can input other NTP servers as needed. To add an NTP server, enter the server IP address or FQDN, and then click **+**. To delete

		an NTP server, click **-**. • **Local Server:** Toggle it on to enable a local NTP server if needed. Then, each AP will act as an NTP server to provide time synchronization services for connected wireless clients.
	Online Check	Toggle it on to enable the online status detection service, which primarily checks whether APs can access the Internet. Once enabled, configure the following parameters: • **Action:** The actions that an AP executes when it cannot access the Internet. Select one of or both the following actions: ◦ **wifi:** All Wi-Fi on the AP will be disabled when the AP cannot access the Internet. ◦ **leds:** The AP LEDs will blink rapidly when the AP cannot access the Internet. • **Ping Hosts:** The FQDN or IP address of the hosts to be pinged for online status detection. Pay attention to the following notes: ◦ The ICMP ping can detect network-layer connectivity, but it cannot check whether application-layer services work well. ◦ Ensure that ICMP packets are allowed. Otherwise, the ping command will fail even though APs can access the Internet. ◦ You can input one or multiple hosts. To add a host, enter the server IP address or FQDN, and then click **+**. To delete a host, click **-**. • **Download Hosts:** The FQDN or IP address of the hosts for HTTP downloading tests. ◦ You can input one or multiple hosts. To add a host, enter the server IP address or FQDN, and then click **+**. To delete a host, click **-**. ◦ APs will attempt to download the file **http://<host>/online.txt** from each host and

		verify whether the downloading is successful. • **Check Interval:** The online check interval (in seconds), controlling how frequently online checks are performed. ◦ Valid values range from 10 to 300. ◦ You are suggested to set it to 60, which means checking every 60 seconds. ◦ Too frequent checking will impact AP performance. • **Check Threshold:** The maximum failure count before an AP considers it a connection failure. ◦ Valid values range from 1 to 6. If the failure count reaches this threshold, the AP will consider it as a connection failure and then perform predefined actions, such as disabling Wi-Fi or blinking LEDs. **NOTE** An AP will track the success count of all ping and downloading tests and work as follows: • If no tests succeed, the failure counter keeps increasing. • If any test succeeds, the failure counter is reset to 0. • When the failure counter reaches the threshold while the AP is online, an offline action is triggered. • When the failure counter is reset to 0 while the AP is offline, an online action is triggered.
	Log	Toggle it on to enable the Log service, which will forward AP logs to a remote Syslog server. Once enabled, configure the following parameters:

	• **Host:** The IPv4 address of the Syslog server to which logs are forwarded.
	• **Port:** The port of the remote Syslog server used for log forwarding. Valid values range from 1 to 65535.
	• **Protocol:** The protocol used for log forwarding, **tcp** or **udp**.
	  ◦ **udp**: Faster in transmission but less reliable.
	  ◦ **tcp**: More reliable but slower in transmission.
	• **Size:** The local send buffer size (in KB), determining how many logs are bundled per transmission. Valid values range from 32 to 65535.
	
	NOTE
	Different services (SSH, HTTP, Log, and RTTY) cannot use the same port.

RTTY	Toggle it on to add an external RTTY server. Once enabled, configure the following parameters: • **Host:** The FQDN of the RTTY server. • **Port:** The port of the RTTY server. Valid values range from 1 to 65535. • **Token:** The token of the RTTY server. The token must be exactly 32 characters long. Then, you can access APs through a web interface for remote debugging, configuration, and maintenance without physical access. For more information, see Accessing APs. **NOTE** Different services (SSH, HTTP, Log, and RTTY) cannot use the same port.
Wi-Fi Steering	Toggle it on to enable the Wi-Fi Steering service. Once enabled, configure the following parameters:

- **Assoc Steering:** Toggle it on to enable roaming association stage guidance.

  When a client has not connected to an AP (only sends an association request), if the AP determines that the current radio band, channel, or node is unsuitable, the AP will reject the association request. Then, the client can connect to a more suitable Basic Service Set (BSS).
- **Auto Channel:** Toggle it on to enable automatic channel selection.

  In this way, each AP can periodically detect surrounding channels, select better channels based on collected Radio Frequency (RF) metrics, and ensure radar avoidance and compliance with regulatory channels.
- **Required Probe SNR:** The minimum required signal level (in dB) to allow connections. Valid values range from 0 to 100.

  If the Signal-to-Noise Ratio (SNR) of an associated terminal is below this threshold, probe requests will be ignored, preventing distant weak-signal terminals from slowing down the entire network.
- **Required Roam SNR:** The minimum required signal level (in dB) that triggers roaming evaluation. Valid values range from 0 to 100.

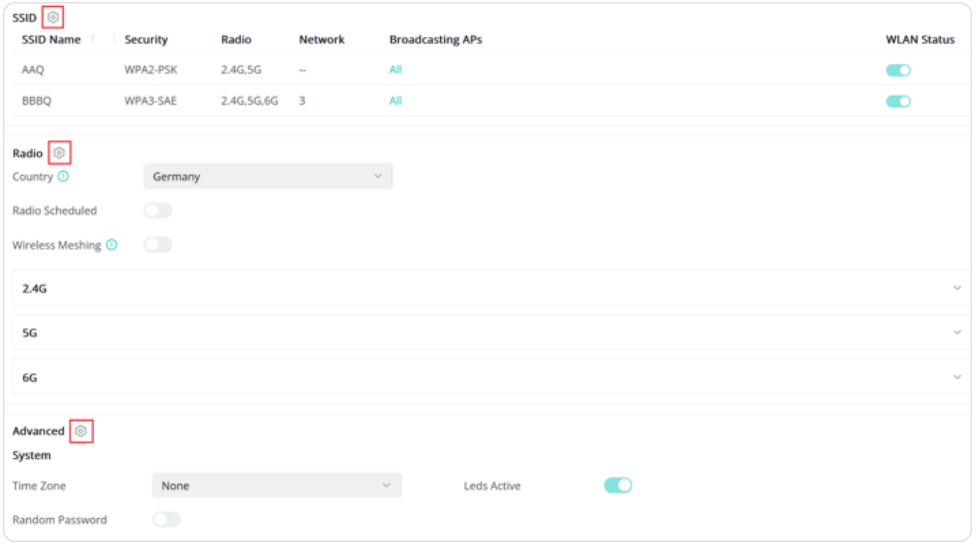
  If the SNR of an associated terminal is below this threshold, an attempt is made to roam the client to a better AP.
- **Kick Threshold:** The channel utilization threshold (in percentage) for client kickouts. Valid values range from 0 to 100.

  If the channel utilization exceeds this threshold, the AP will proactively disconnect weak-signal clients to free up airtime. To prevent connection loops (thrashing), the AP avoids repeatedly disconnecting the same client.

2. Click **Apply** to save the wireless configurations.
3. On the “Wireless Configuration” page, check the added wireless configurations.

   To change site-level wireless configurations, click the setting icons near **SSID**, **Radio**, and **Advanced**.

   You must click **Apply** to save the configuration changes. Otherwise, the configuration changes will be lost.



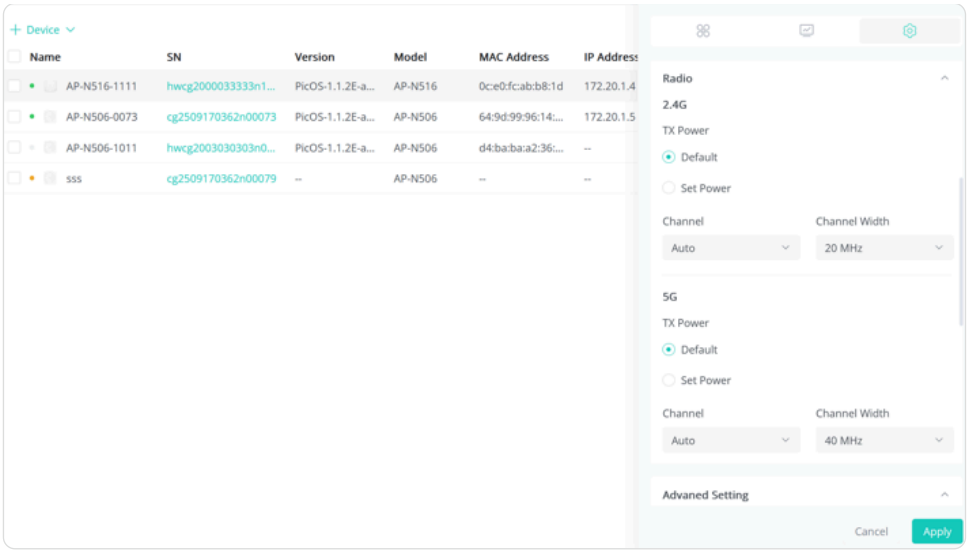
Configuring a Single AP

To configure a single AP, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP to be configured belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click the AP. You can see a side panel on the right.
3. Click the **Setting** tab of the side panel, modify wireless configurations for the AP, and then click **Apply**.

   For configuration parameters, see Configurations and Operations of an AP.

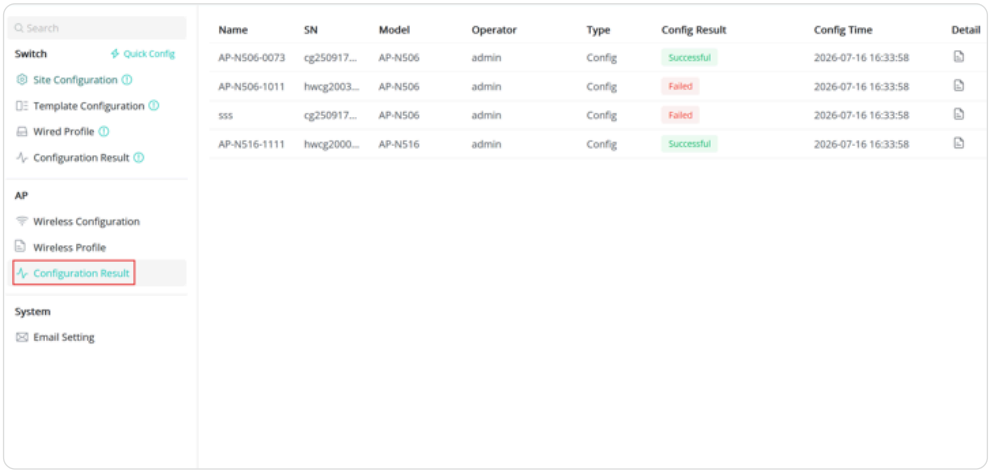
> **NOTEs**
>
> - The **Apply** button is displayed only after you modify at least one configuration of the AP.
> - You must click **Apply** to save the configuration changes. Otherwise, the configuration changes will be lost.



Checking Configuration Results

After you configure site-level wireless configurations or AP-specific configurations, check configuration results on the “Configuration Result” page. Follow these steps:

1. Click the **Settings** icon from the navigation bar, and then click **Configuration Result** in the **AP** section.



2. On the “Configuration Result” page, locate the APs, and then check the configuration result:

> **NOTEs**
>
> - Configuration results are displayed on a per-AP basis, with only the latest configuration record shown for each AP in the site.
> - After an AP is moved to another site, its configuration results are also moved to the new site.

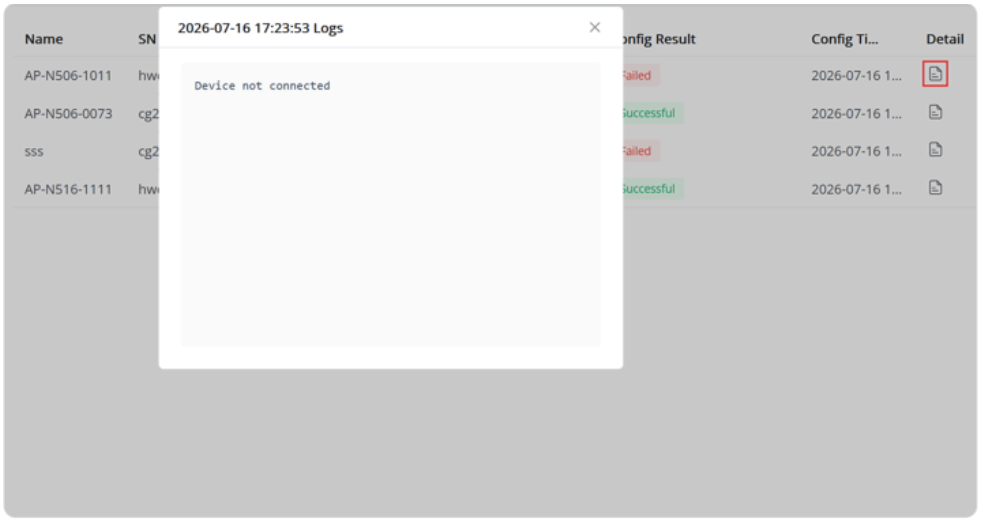
Table 5. Configuration Result Parameters

Parameter	Description

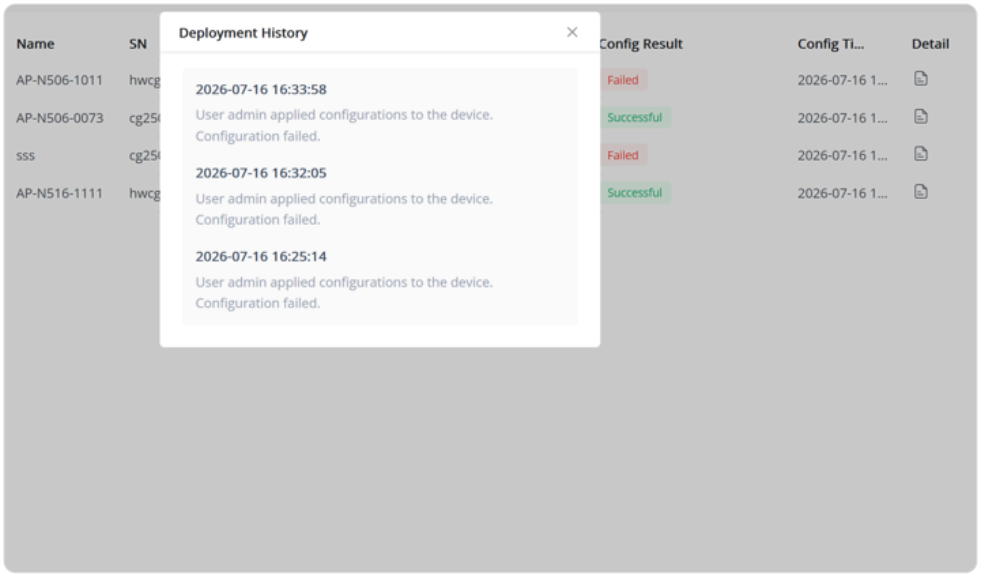
Name	The AP alias.
SN	The SN of the AP.
Model	The model of the AP.
Operator	The AmpCon-Campus user who executes the configuration operation.
Type	The type of the configuration. Currently, you can see only **Config**.
Config Result	The result of the configuration. • **In Progress**: The configurations are being pushed to the AP. • **Pending**: The configuration push is queued and waiting to be executed. • **Successful**: The configurations are successfully pushed to the AP. • **Failed**: The configurations fail to be pushed to the AP.
Config Time	The time when the configuration task started.

- To check the latest configuration details of an AP, locate the configuration result, and then click the detail icon in the **Detail** column.

> **NOTE**
>
> If the **Config Result** of an AP is **In Progress** or **Pending**, you might not see the detail icon, and you can see only **--**.



- To view the configuration history of an AP, hover over the AP, and then click **View History**.



SSID Configurations

This topic describes SSID-related configurations. For how to add Service Set Identifier (SSID) configurations, see Adding SSID Configurations.

General Configurations
Advanced Configurations

General Configurations

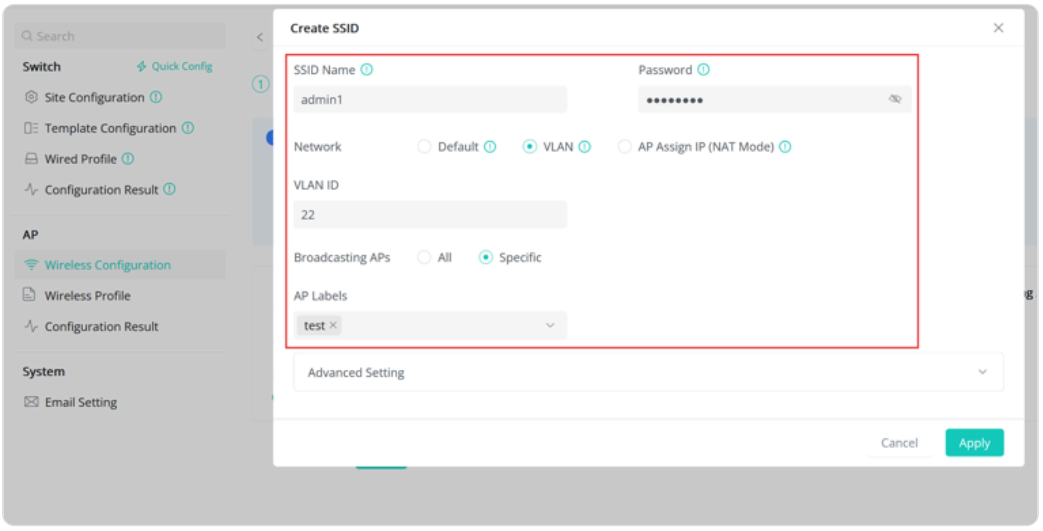


Table 1. General SSID Parameters

Parameter	Description
SSID Name	The SSID to which wireless clients connect. Each SSID is the logical name of a wireless network. The SSID must be unique and cannot be set to **Pica8WiFi-Onboarding**. The SSID must be 1 to 32 bytes long. Normally, an English character occupies a byte, and a non-English character occupies more bytes.
Password	The Pre-Shared Key (PSK) used for encryption on the BSS when any WPA-PSK mode is used. The password can contain 8 to 63 characters. **NOTE** This field is not displayed in the following cases: • If you select **Open** or **Enterprise** in the **Security Level** section. • If you select **Personal** in the **Security Level** section and select **PSK2-RADIUS** in the **Protocol**

	section.
Network	Select how downstream wireless devices access the upstream network. • If you select **Default**, the wireless clients connected to this SSID will have the same VLAN as the AP. • If you select **VLAN,** you need to input a VLAN ID, which will be assigned to the SSID. Avoid inputting the native VLAN ID of the upstream switch. Ensure the VLAN ID is allowed (tagged) on all upstream switch ports to avoid client device unreachability. • If you select **AP Assign IP (NAT Mode)**, each AP acts as a DHCP server/router for wireless clients, assigning IP addresses to downstream devices from a private 10.1.1.0/24 subnet. APs perform Network Address Translation (NAT) when the downstream devices connect to the internet. To avoid routing conflicts, ensure that the upstream network does not contain a 10.1.1.0/24 subnet. If the upstream network contains a 10.1.1.0/24 subnet, modify the subnet by going to the **DHCP Service** section. For more information, see Adding Advanced Configurations. **NOTE** The MPSK, Key Caching, and FT Roaming functions are not supported when APs operate in NAT (Router) mode. AmpCon-Campus automatically disables MPSK, Key Caching, and FT Roaming when you select **AP Assign IP (NAT Mode)**.
Broadcasting APs	Select which APs can broadcast this SSID. • If you select **All**, all APs in this site can broadcast this SSID. The configurations of this SSID will be pushed to all these APs. • If you select **Specific**, only specific APs can broadcast this SSID. You must select labels from the **AP Label** drop-down list.

Then, the configurations of this SSID will be pushed only to the APs with these labels.

To add a label, click **Create Label** from the drop-down list.

Advanced Configurations

Unfold the **Advanced Setting** section. Then, you can configure the following advanced configurations:

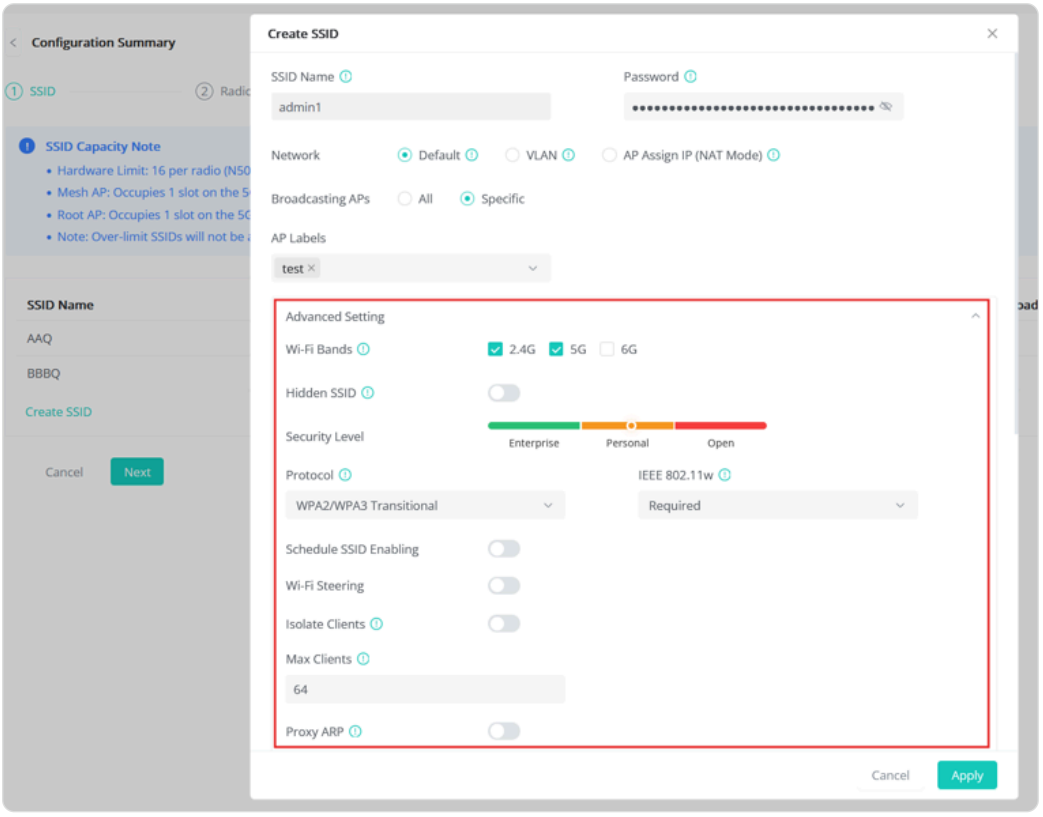


Table 2. Advanced SSID Parameters

Parameter	Description
MPSK	Toggle it on to enable the MPSK function, which can configure multiple Pre-Shared Keys (PSKs) for the same SSID. After enabling this function, select an MPSK profile. • To add an MPSK profile, click **Create MPSK Profile** from the drop-down list. In each MPSK profile, you can add one or multiple access credentials. In each access credential, you can define a wireless client MAC address, the key used by

	the wireless client to connect to the SSID, and the VLAN ID assigned to the wireless client. If you click **Manage MPSK Profile**, you will be redirected to the **MPSK** tab of the "Wireless Profile" page. For more information, see Adding MPSK Profiles. **NOTEs** • This section is displayed only when you select **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/WPA2-PSK Personal Mixed** in the **Protocol** section. • The MPSK function is automatically disabled by AmpCon-Campus and cannot be enabled if you select **AP Assign IP (NAT Mode)** in the **Network** section. • Captive Portal and MPSK are mutually exclusive. AmpCon-Campus automatically disables the other when you enable one.
Wi-Fi Bands	The radio bands to be enabled on the APs, **2.4G**, **5G**, and **6G**. You must select at least one radio band. **NOTE** Ensure that each AP model and the located country support the enabled radio bands.
Hidden SSID	Toggle it on to enable the Hidden SSID function. Once enabled, the SSID will not be broadcast, and thus wireless clients cannot detect the SSID. You must manually enter the network name to connect to the SSID.
Security Level	Select the password security level, **Enterprise**, **Personal**, or **Open**. • **Enterprise:** Widely used in large corporate networks, where users authenticate with usernames and passwords for enhanced security. This security level requires RADIUS servers, but APs also offer built-in RADIUS servers to meet customer needs.

	• **Personal:** Typically used in home, small and medium-sized business (SMB), or hotel scenarios. APs support MPSK, allowing different wireless clients to connect to an SSID with different keys while maintaining L2 isolation. If you select **PSK2-RADIUS** in the **Protocol** section, you can select a RADIUS server containing external RADIUS servers or RADIUS servers built in APs. • **Open:** Commonly used in guest networks and works with Captive Portal. The four types of built-in Captive Portal are provided for immediate use. This security level does not need any encryption or authentication mechanisms.
Protocol	Select the security protocol to encrypt this Wi-Fi network. • If you select **Enterprise** as the security level, the supported protocols are: **WPA-Enterprise**, **WPA2-Enterprise EAP-TLS**, **WPA-Enterprise-Mixed**, **WPA3-Enterprise EAP-TLS**, **WPA3-192-Enterprise EAP-TLS**, or **WPA3-Enterprise-Mixed**. If **6G** is enabled in the **Wi-Fi Bands** section, you can select only **WPA3-Enterprise EAP-TLS**, **WPA3-192-Enterprise EAP-TLS**, or **WPA3-Enterprise-Mixed**. • If you select **Personal** as the security level, the supported protocols are: **WPA-PSK**, **WPA2-PSK**, **PSK2-RADIUS**, **WPA-PSK/WPA2-PSK Personal Mixed**, **WPA3-SAE**, or **WPA2/WPA3 Transitional**. If **6G** is enabled in the **Wi-Fi Bands** section, you can select only **WPA3-SAE** or **WPA2/WPA3 Transitional**. • If you select **Open** as the security level, the supported protocols are: **None**, **OWE**, or **OWE Transition**. **None** means no encryption protocol is used. If **6G** is enabled in the **Wi-Fi Bands** section, you can select only **OWE**.
IEEE 802.11w	Configures the 802.11w Management Frame Protection (MFP) mode to secure this network against

	deauthentication attacks. MFP adds signing or encryption to 802.11 management frames and helps to prevent forgery, tampering, and replay attacks, thereby mitigating common wireless Denial of Service (DoS) and disconnection vulnerabilities. The value can be **Disabled**, **Optional**, or **Required**. • **Disabled** Completely disables 802.11w MFP. No protection mechanism will be applied regardless of whether wireless clients support MFP. Management frames (such as deauthentication and disassociation frames) will be transmitted in clear text, and thus the network is vulnerable to forged management frame attacks. • **Optional** Enables 802.11w MFP without enforcing client support. The wireless clients supporting MFP can use the protection mechanisms. The wireless clients that do not support MFP can still connect normally but cannot use the management frame protection function. • **Required** Enforces mandatory 802.11w MFP. Only the wireless clients compliant with 802.11w are allowed to connect; the wireless clients without MFP support are denied access. In this way, all management frames can be protected. **NOTEs** • If you select **OWE** or **OWE Transition** in the **Protocol** section, the **IEEE 802.11w** value must be **Optional** or **Required**. • If you select the following protocols in the **Protocol** section, the **IEEE 802.11w** value must be **Required**. ◦ **WPA3-Enterprise EAP-TLS** ◦ **WPA3-192-Enterprise EAP-TLS** ◦ **WPA3-Enterprise-Mixed** ◦ **WPA3-SAE**
RADIUS	The RADIUS profile containing external RADIUS servers or RADIUS servers built in APs. The RADIUS servers are used

	as centralized authentication servers for wireless client authentication. To add a RADIUS profile, click **Create RADIUS Profile** from the drop-down list. If you click **Manage RADIUS Profile**, you will be redirected to the **SSID RADIUS** tab of the “Wireless Profile” page. For more information, see Adding RADIUS Profiles. **NOTE** This section is displayed only in the following cases: • If you select **Enterprise** in the **Security Level** section. • If you select **Personal** in the **Security Level** section and select **PSK2-RADIUS** in the **Protocol** section.
RADIUS MAC Authentication	Toggle it on to use the MAC ID as credentials of RADIUS authentication. After you toggle it on, select a RADIUS profile from the **RADIUS** drop-down list. To add a RADIUS profile, click **Create RADIUS Profile** from the drop-down list. If you click **Manage RADIUS Profile**, you will be redirected to the **SSID RADIUS** tab of the “Wireless Profile” page. **NOTE** This section is displayed only if you select **Open** in the **Security Level** section.
Schedule SSID Enabling	Toggle it on to schedule the enabling time for the SSID. Then, select a time range from the drop-down list. To add a time range, click **Create Time Range Profile** from the drop-down list. If you click **Manage Time Range Profile**, you will be redirected to the **Time Range** tab of the “Wireless Profile” page. For more information, see Adding Time Range Profiles.

	NOTE If both an SSID and a radio have time-based policies configured, the radio's time-based policy takes precedence. For time-based policies of radios, see Adding Radio Configurations.
Wi-Fi Steering	Toggle it on to enable the Wi-Fi Steering function. Wi-Fi Steering dynamically guides wireless clients to select optimal radio bands, optimizing network load and performance. **NOTE** After you enable Wi-Fi Steering here, the Wi-Fi Steering in the **Advanced** tab is also enabled automatically. For more information about the **Advanced** tab, see Adding Advanced Configurations.
Isolate Clients	Toggle it on to enable L2 isolation between wireless clients connected to the same SSID. Once enabled, wireless clients connected to this SSID cannot communicate directly with each other.
Max Clients	The maximum number of concurrent wireless clients allowed to connect to this SSID. The value must range from 1 to 2007. For example, if an SSID enables both the 2.4G and 5G radios and the **Max Clients** value is set to 10: • The maximum limit for the 2.4G radio is 10 clients. • The maximum limit for the 5G radio is 10 clients. • The total maximum limit for this SSID is 20 clients.
Proxy ARP	Toggle it on to enable the Proxy ARP function. Once enabled, the AP responds to ARP requests on behalf of connected wireless clients. This reduces broadcast traffic and improves network performance. **NOTE** Proxy ARP might cause issues in some enterprise networks. It might conflict with security policies like Dynamic ARP Inspection (DAI) on upstream

	switches, or cause temporary routing issues during rapid client roaming. Disable Proxy ARP if you experience connectivity drops or ARP conflicts.
Unicast Conversion	Toggle it on to enable the conversion of multicast data to unicast data. This function can significantly improve airtime efficiency and network performance. **NOTE** Duplicating traffic into multiple unicast streams increases air interface overhead, which might slow down the entire network in high-density scenarios.
FILS Discovery Interval	The transmission interval of Fast Initial Link Setup (FILS) discovery frames. FILS discovery frames are “lightweight beacons” that carry only the most critical information, such as SSID, BSSID, and channel. By using FILS discovery frames, wireless clients can discover the Wi-Fi network faster, especially on 6 GHz channels. The unit is Time Unit (TU). 1 TU equals 1.024 ms. The value must range from 1 to 20. • A lower value reduces the latency for wireless clients to discover APs, but increases air interface overhead. • A higher value optimizes air interface efficiency and improves client battery life, while extending the initial AP discovery time for wireless clients.
DTIM Period	Determines how many Beacon frames occur before a Delivery Traffic Indication Message (DTIM) appears. The value controls how frequently clients wake up to receive broadcast and multicast data. The value must range from 1 to 255. • A lower value improves real-time delivery but increases power consumption. Lower values are more applicable to low-latency scenarios, such as video conferencing and online gaming.

	• A higher value saves power but increases latency. Higher values are more applicable to low-power scenarios, such as smart-home sensors.
Disassoc Low Ack	Toggle it on to enable APs to actively disconnect wireless clients with weak signals. If an AP fails to receive ACK confirmation from a wireless client for consecutive times, the AP will immediately force disconnect the wireless client to remove clients with extremely poor link quality.
Power Save	Toggle it on to enable U-APSD (WMM Power Save) to significantly extend the battery life of connected wireless clients. In the power-saving mode, wireless clients enter periodic sleep states, and wake up only during the AP-designated “awake window” to transmit or receive data. Wireless clients keep the Wi-Fi radio off at other times to save power at the cost of potentially increased downlink latency.
Broadcast Time	Toggle it on to enable the time broadcast function. Once enabled, each AP will broadcast its current system time within beacon frames, allowing wireless clients to synchronize their internal clocks.
Key Caching	Toggle it on to enable the Key Caching function. Key Caching is a security mechanism in wireless networks where the Pairwise Master Key Security Association (PMKSA) is temporarily stored after successful authentication through Extensible Authentication Protocol (EAP) or Robust Security Network (RSN) pre-authentication. Once enabled, security keys are cached to allow faster re-authentication for roaming clients without re-executing a full authentication protocol. **NOTE** The Key Caching function is disabled automatically by AmpCon-Campus and cannot be enabled in the

	following cases: • If you select **AP Assign IP (NAT Mode)** in the **Network** section. • If you select **Personal** in the **Security Level** section and select **WPA-PSK** in the **Protocol** section. • If you select **Open** in the **Security Level** section and select **None** in the **Protocol** section.
FT Roaming	Toggle it on to enable seamless and low-latency 802.11r roaming for wireless clients between APs within the same Mobility Domain (MD). **NOTEs** • If you select **AP Assign IP (NAT Mode)** in the **Network** section, the FT Roaming function is disabled automatically by AmpCon-Campus and cannot be enabled. • The FT Roaming function is not displayed in the following cases: ◦ If you select **Enterprise** in the **Security Level** section and select **WPA-Enterprise** in the **Protocol** section. ◦ If you select **Personal** in the **Security Level** section and select **WPA-PSK** in the **Protocol** section. ◦ If you select **Open** in the **Security Level** section.
Rate Limit	Toggle it on to set the maximum ingress and egress data rate for connected wireless clients. Once enabled, enter the following information: • **Ingress Rate:** The maximum ingress data rate for each connected wireless client. The unit is Mbps. The value can be 1 to 65534. • **Egress Rate:** The maximum egress data rate for each connected wireless client. The unit is Mbps. The value can be 1 to 65534.

Access Control List	Toggle it on to add the MAC addresses of wireless clients allowed or denied to access this SSID. Input the following information: • **Mode:** Select **Allow** or **Deny**. • **MAC Address:** The MAC addresses of wireless clients allowed or denied to access this SSID. You can input one or multiple MAC addresses. To add a MAC address, enter the MAC address, and then click **+**. To delete a MAC address, click **-**. After adding a MAC address, you cannot edit it. **NOTE** When you enter a MAC address, AmpCon-Campus automatically inserts a colon after every two characters.
Captive Portal	Toggle it on to enable Captive Portal. A Captive Portal is a web-based authentication mechanism. When a wireless client connects to the SSID, all web traffic is temporarily intercepted and redirected to a dedicated login webpage. Users must complete verification such as accepting terms of service, entering a password, or logging in with credentials before obtaining full internet access. **NOTE** Captive Portal and MPSK are mutually exclusive. AmpCon-Campus automatically disables the other when you enable one.
Auth Mode	The Captive Portal authentication mode. • **Click:** Connects to an SSID without entering a password. After a portal authentication page pops up, you can click to access the internet. • **RADIUS:** Connects to an SSID through credentials stored in an external RADIUS server. • **Credentials:** Connects to an SSID through the username and password.

- **UAM:** Connects to an SSID through credentials stored in an external Universal Access Method (UAM) server.

> **NOTEs**
>
> - If you select **Enterprise** in the **Security Level** section or select **PSK2-RADIUS** in the **Protocol** section, Captive Portal authentication might fail or be bypassed for wireless clients that use dynamic VLAN assignment.
> - All SSIDs that use the same **Auth Mode** within the same site share one portal profile. If you modify the portal profile of one SSID, all the other SSIDs within the same site will automatically adopt this profile.

- If you select **Click** in the **Auth Mode** section, input the following information:

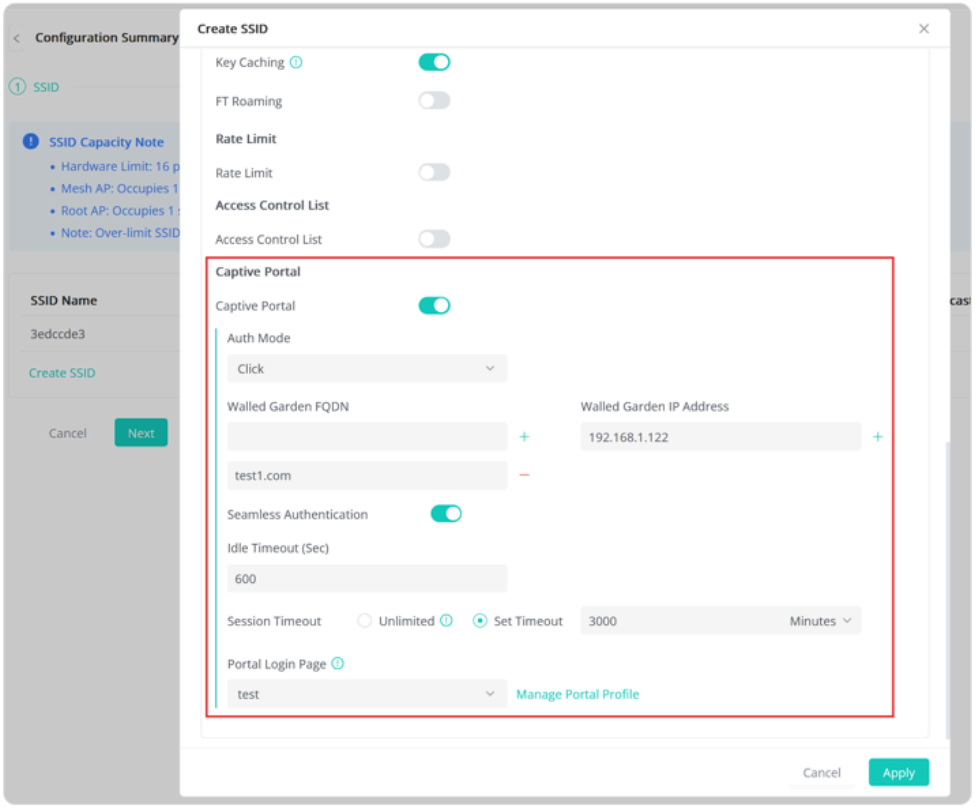


Table 3. Click Mode Parameters

Parameter	Description
Walled Garden FQDN	The Fully Qualified Domain Name (FQDN) of the Walled Garden.

	Be sure to enter a valid FQDN, such as **portal.example.com**. The FQDN can contain at most 253 characters. You can add one or multiple FQDNs. To add an FQDN, enter the FQDN, and then click **+**. To delete an FQDN, click **-**. After adding an FQDN, you cannot edit it.
Walled Garden IP Address	The IPv4 address of the Walled Garden. You can add one or multiple IPv4 addresses. To add an IPv4 address, enter the IPv4 address, and then click **+**. To delete an IPv4 address, click **-**. After adding an IPv4 address, you cannot edit it.
Seamless Authentication	Toggle it on to enable seamless authentication. Then, wireless clients only need to complete Captive Portal authentication once. Subsequent connections will be automatically authorized until the session or validity period expires.
Idle Timeout	The idle timeout. If a wireless client has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of a client connection. When this duration is exceeded, wireless clients will be forcibly disconnected. • If you select **Unlimited**, each client connection will not be automatically disconnected. • If you select **Set Timeout**, specify the maximum duration of a client connection by selecting a time unit (**Minutes**, **Hours**, or **Days**) and entering an integer value for the time period. Valid values range from 30 minutes to 180 days.
Portal Login Page	Select a portal profile of the **Click** mode. Each portal profile defines a Captive Portal authentication page.

To add a portal profile, click **Create Portal Profile** from the drop-down list.

If you click **Manage Portal Profile**, you will be redirected to the **Portal** tab of the “Wireless Profile” page. For more information, see Adding Portal Profiles.

NOTE

- If this section is left blank, AmpCon-Campus will automatically apply a default built-in portal profile corresponding to the selected **Auth Mode**.
- All SSIDs within the same site and using the same **Auth Mode** share one portal profile. If you modify the portal profile of one SSID, all other SSIDs in the same site will automatically adopt this profile.

- If you select **RADIUS**, input the following information:

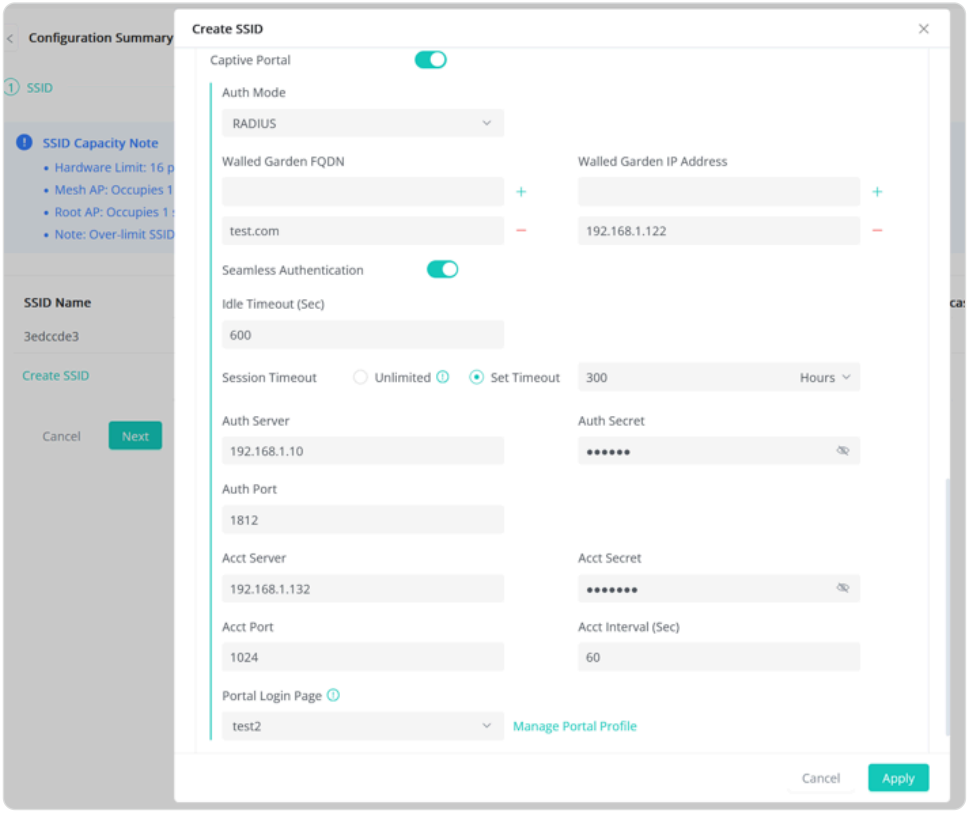


Table 4. RADIUS Mode Parameters

Parameter	Description

Walled Garden FQDN	The Fully Qualified Domain Name (FQDN) of the Walled Garden. Be sure to enter a valid FQDN, such as **portal.example.com**. The FQDN can contain at most 253 characters. You can add one or multiple FQDNs. To add an FQDN, enter the FQDN, and then click **+**. To delete an FQDN, click **-**. After adding an FQDN, you cannot edit it.
Walled Garden IP Address	The IPv4 address of the Walled Garden. You can add one or multiple IPv4 addresses. To add an IPv4 address, enter the IPv4 address, and then click **+**. To delete an IPv4 address, click **-**. After adding an IPv4 address, you cannot edit it.
Seamless Authentication	Toggle it on to enable seamless authentication. Then, wireless clients only need to complete Captive Portal authentication once. Subsequent connections will be automatically authorized until the session or validity period expires.
Idle Timeout	The idle timeout. If a wireless client has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of a client connection. When this duration is exceeded, wireless clients will be forcibly disconnected. • If you select **Unlimited**, each client connection will not be automatically disconnected. • If you select **Set Timeout**, specify the maximum duration of a client connection by selecting a time unit (**Minutes**, **Hours**, or **Days**) and entering an integer value for the time period. Valid values range from 30 minutes to 180 days.

Auth Server	The FQDN or IP address of the RADIUS authentication server.
Auth Secret	The secret of the RADIUS authentication server.
Auth Port	The port used to access the RADIUS authentication server. The value must be greater than 1023 and less than 65535.
Acct Server	The FQDN or IP address of the RADIUS accounting server.
Acct Secret	The secret of the RADIUS accounting server.
Acct Port	The port used to access the RADIUS accounting server. The value must be greater than 1023 and less than 65535.
Acct Interval	The time interval (in seconds) at which the RADIUS accounting server periodically sends accounting update messages during a user session, enabling dynamic resource usage monitoring. The value must be greater than 0 and less than 65535.
Portal Login Page	Select a portal profile of the **RADIUS** mode. Each portal profile defines a Captive Portal authentication page. To add a portal profile, click **Create Portal Profile** from the drop-down list. If you click **Manage Portal Profile**, you will be redirected to the **Portal** tab of the “Wireless Profile” page. **NOTE** If this section is left blank, AmpCon-Campus will automatically apply a default built-in portal profile corresponding to the selected **Auth Mode**.

- If you select **Credentials**, input the following information:

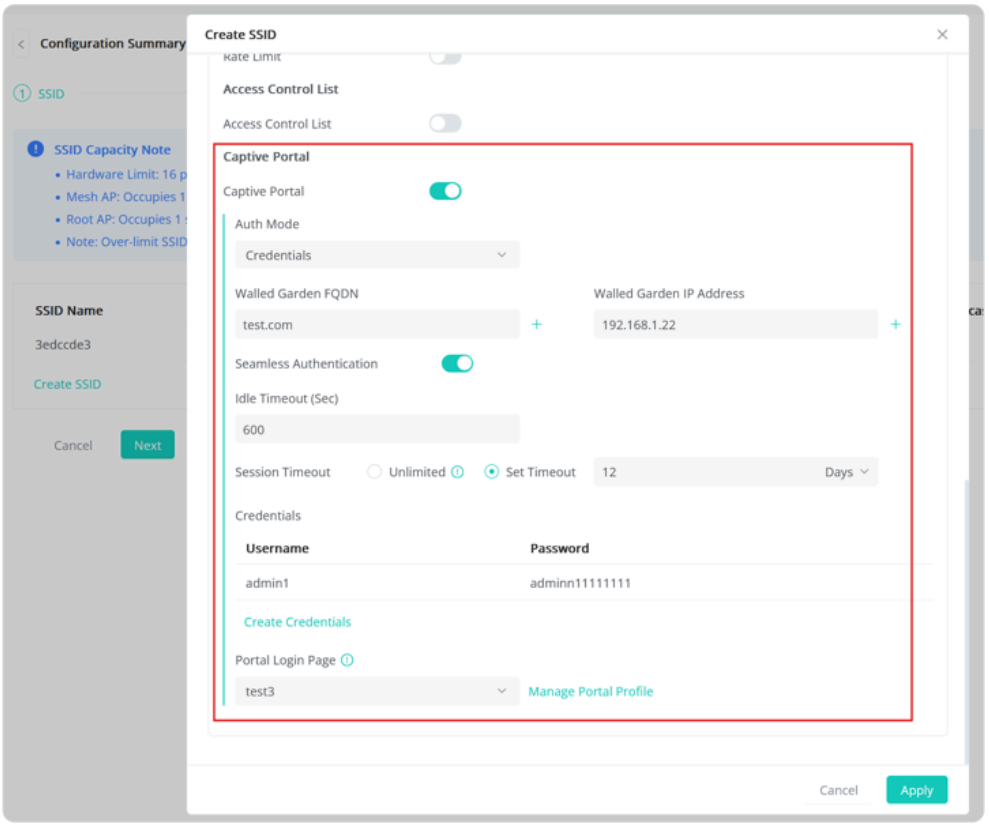


Table 5. Credentials Mode Parameters

Parameter	Description
Walled Garden FQDN	The Fully Qualified Domain Name (FQDN) of the Walled Garden. Be sure to enter a valid FQDN, such as **portal.example.com**. The FQDN can contain at most 253 characters. You can add one or multiple FQDNs. To add an FQDN, enter the FQDN, and then click **+**. To delete an FQDN, click **-**. After adding an FQDN, you cannot edit it.
Walled Garden IP Address	The IPv4 address of the Walled Garden. You can add one or multiple IPv4 addresses. To add an IPv4 address, enter the IPv4 address, and then click **+**. To delete an IPv4 address, click **-**. After adding an IPv4 address, you cannot edit it.
Seamless Authenticati	Toggle it on to enable seamless authentication.

on	Then, wireless clients only need to complete Captive Portal authentication once. Subsequent connections will be automatically authorized until the session or validity period expires.
Idle Timeout	The idle timeout. If a wireless client has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of a client connection. When this duration is exceeded, wireless clients will be forcibly disconnected. • If you select **Unlimited**, each client connection will not be automatically disconnected. • If you select **Set Timeout**, specify the maximum duration of a client connection by selecting a time unit (**Minutes**, **Hours**, or **Days**) and entering an integer value for the time period. Valid values range from 30 minutes to 180 days.
Credentials	Click **Create Credentials** to add one or multiple credentials. You need to enter the username and password used to access this SSID and then click **Apply**. The username must start with a letter and contain only letters and numbers. The password must contain 8 to 63 characters.
Portal Login Page	Select a portal profile of the **Credentials** mode. Each portal profile defines a Captive Portal authentication page. To add a portal profile, click **Create Portal Profile** from the drop-down list. If you click **Manage Portal Profile**, you will be redirected to the **Portal** tab of the “Wireless Profile” page. **NOTE**

If this section is left blank, AmpCon-Campus will automatically apply a default built-in portal profile corresponding to the selected **Auth Mode**.

- If you select **UAM**, input the following information:

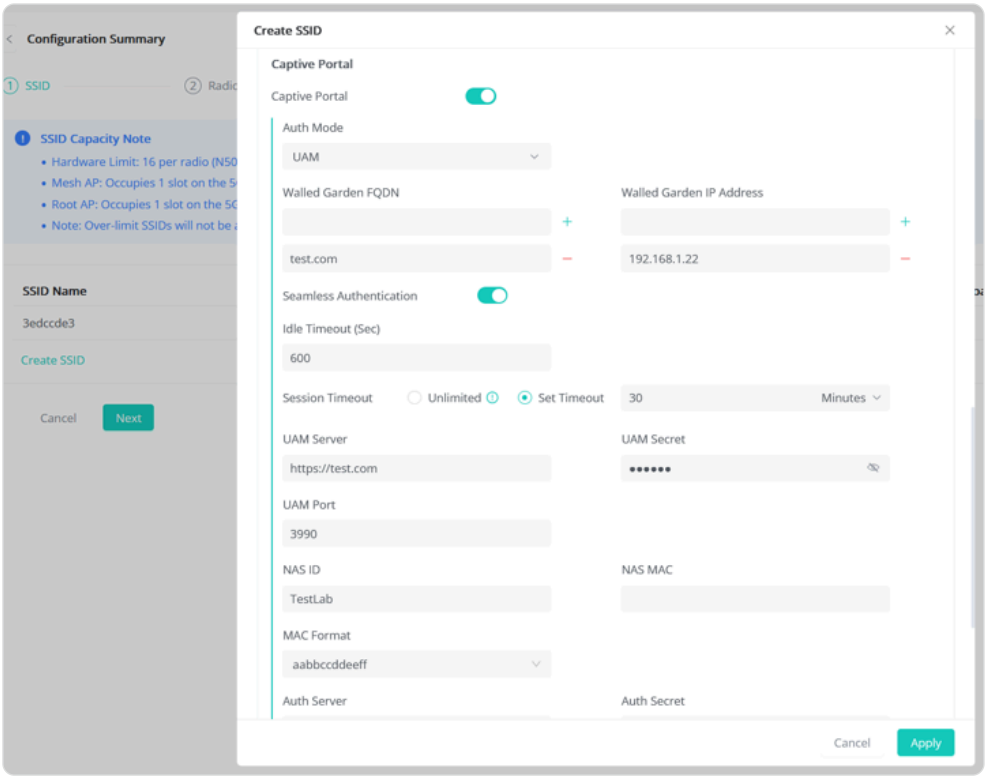


Table 6. UAM Mode Parameters

Parameter	Description
Walled Garden FQDN	The Fully Qualified Domain Name (FQDN) of the Walled Garden. Be sure to enter a valid FQDN, such as **portal.example.com**. The FQDN can contain at most 253 characters. You can add one or multiple FQDNs. To add an FQDN, enter the FQDN, and then click **+**. To delete an FQDN, click **-**. After adding an FQDN, you cannot edit it.
Walled Garden IP Address	The IPv4 address of the Walled Garden. You can add one or multiple IPv4 addresses. To add an IPv4 address, enter the IPv4 address, and then

	click **+**. To delete an IPv4 address, click **-**. After adding an IPv4 address, you cannot edit it.
Seamless Authentication	Toggle it on to enable seamless authentication. Then, wireless clients only need to complete Captive Portal authentication once. Subsequent connections will be automatically authorized until the session or validity period expires.
Idle Timeout	The idle timeout. If a wireless client has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of a client connection. When this duration is exceeded, wireless clients will be forcibly disconnected. • If you select **Unlimited**, each client connection will not be automatically disconnected. • If you select **Set Timeout**, specify the maximum duration of a client connection by selecting a time unit (**Minutes**, **Hours**, or **Days**) and entering an integer value for the time period. Valid values range from 30 minutes to 180 days.
UAM Server	The FQDN or IP address of the UAM server.
UAM Secret	The secret of the UAM server.
UAM Port	The port used to connect to the UAM server. The value must be greater than 1023 and less than 65535.
NAS ID	The Network Access Server (NAS) identifier to distinguish this wireless network identity in the external portal system. Based on the NAS ID, the external portal system will differentiate authentication requests from different sources, and then match the requests with the corresponding portal project configurations.

	This parameter must be the same as the NAS ID configured in the external portal server.
NAS MAC	The unique physical identifier used by the external portal system to identify APs. It is used for auditing, matching policies, and preventing identity spoofing.
MAC Format	The format for transmitting NAS MAC addresses in authentication messages, such as AA:BB:CC:DD:EE:FF or AABBCCDDEEFF. The format must be consistent with the expected format of the external portal system. Otherwise, authentication requests might be rejected or fail to match policies.
Auth Server	The FQDN or IP address of the UAM authentication server.
Auth Secret	The secret of the UAM authentication server.
Auth Port	The port used to access the UAM authentication server. The value must be greater than 1023 and less than 65535.
Acct Server	The FQDN or IP address of the UAM accounting server.
Acct Secret	The secret of the UAM accounting server.
Acct Port	The port used to access the UAM accounting server. The value must be greater than 1023 and less than 65535.
Acct Interval	The time interval (in seconds) at which the UAM accounting server periodically sends accounting update messages during a user session, enabling dynamic resource usage monitoring. The value must be greater than 0 and less than 65535.

Adding Wireless Profiles

On the “Wireless Profile” page, you can configure different profiles, including RADIUS server profiles, Multiple Pre-Shared Key (MPSK) profiles, Captive Portal profiles, and time range profiles.

You can use these pre-defined profiles when adding SSID or radio configurations, eliminating repetitive manual configuration and improving configuration efficiency.

Guidelines
Procedure
- Adding RADIUS Profiles
- Adding MPSK Profiles
- Adding Portal Profiles
- Adding Time Range Profiles

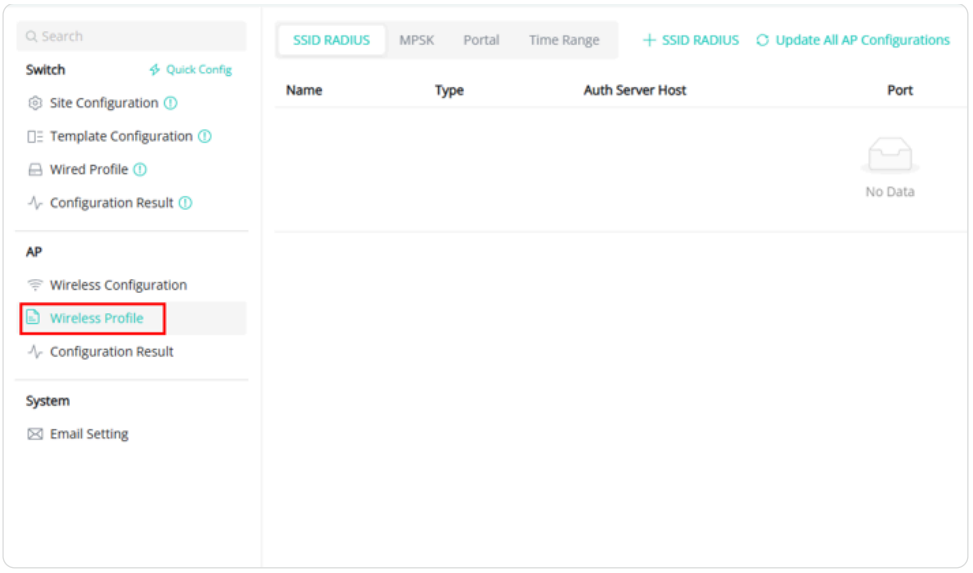
Guidelines

- The configurations in wireless profiles can be pushed to APs only when all the following prerequisites are met:
  - The profile is used in SSID or radio configurations. For more information, see Adding SSID Configurations and Adding Radio Configurations.
  - The SSID or radio configurations are pushed to APs successfully. To check configuration results, see Checking Configuration Results.
- After a profile is added, you can delete, modify, or copy the profile:
  - To delete a profile, hover over the profile, and then click **Delete**.
  - To modify a profile, hover over the profile, and then click **Edit**.
  - To copy a profile, hover over the profile, and then click **Copy**.
  - The profiles that are currently in use by SSID or radio configurations cannot be deleted.
- After the configurations in a wireless profile are pushed to APs, if you modify the profile, the configuration changes will not be automatically pushed to these APs.

  To apply the configuration changes to these APs, click **Update All AP Configurations**.

Procedure

1. In the AmpCon-Campus UI, select the site to which the APs to be configured belong.
2. Click the **Settings** icon from the navigation bar, and click **Wireless Profile** in the **AP** section.



Then, add RADIUS profiles, MPSK profiles, portal profiles, and time range profiles as needed.

Adding RADIUS Profiles

To add a RADIUS profile, follow these steps:

> **Tips**
>
> - You can use external RADIUS servers or use the built-in RADIUS server on each AP.
> - External RADIUS servers are suitable for medium-to-large scenarios, offering more flexible configurations.
> - Built-in RADIUS servers on APs are ideal for small-to-medium scenarios, enabling users to use security features like 802.1x without deploying or purchasing an external RADIUS server.

1. In the **SSID RADIUS** tab, click **+ SSID RADIUS**.
2. In the pop-up window, add an external RADIUS server or the built-in RADIUS server on each AP:

- To add a built-in RADIUS server on each AP, input the following information, and then click **Apply**.

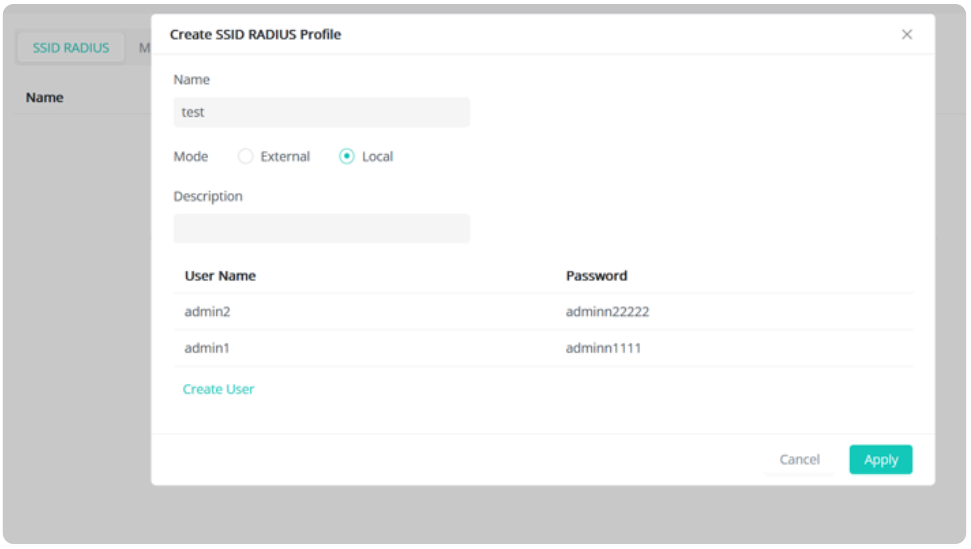


Table 1. Built-in RADIUS Server Parameters

Parameter	Description
Name	The name of the RADIUS profile. The name can contain at most 64 characters.
Mode	Select **Local**, which means adding the built-in RADIUS server on each AP.
Description	Optional. The description of the RADIUS profile. The description can contain at most 128 characters.
User	Click **Create User**. In the pop-up window, input the following information, and then click **Apply** to complete the user addition. • **User Name:** The username used to connect to an SSID. The username must be unique and can contain at most 64 characters. • **Password:** The password of the user. The password must contain 8 to 63 characters. To delete a user, hover over it, and then click **Delete**.

- To add an external RADIUS server, input the following information, and then click **Apply**.

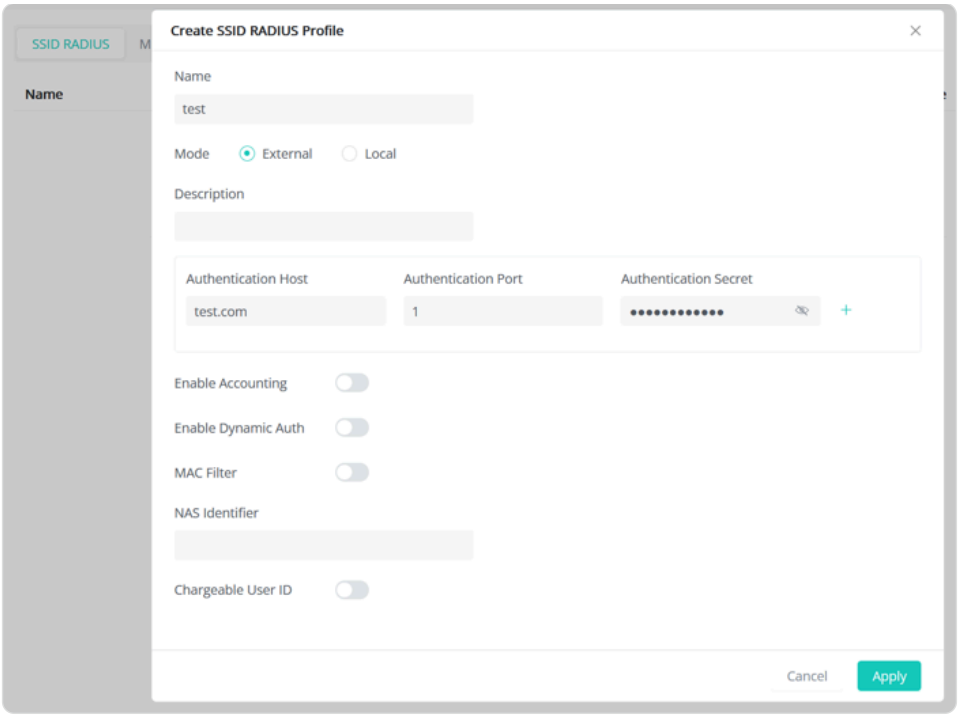


Table 2. External RADIUS Server Parameters

Parameter	Description
Name	The name of the RADIUS profile. The name can contain at most 64 characters.
Mode	Select **External**, which means adding an external RADIUS server.
Description	Optional. The description of the RADIUS profile. The description can contain at most 128 characters.
Authentication Host	The Fully Qualified Domain Name (FQDN) or IP address of the RADIUS authentication server.
Authentication Port	The port used to access the RADIUS authentication server. The value must be between 1024 and 65535.
Authentication Secret	The security secret used to access the RADIUS authentication server. To add another external RADIUS authentication server, click **+**. To delete an external RADIUS authentication server, click **-**.

Enable Accounting	Toggle it on to enable a RADIUS accounting server. Once enabled, configure the following parameters: • **Accounting Host:** The FQDN or IP address of the RADIUS accounting server. • **Accounting Port:** The port used to access the RADIUS accounting server. The value must be between 1024 and 65535. • **Accounting Secret:** The security secret used to access the RADIUS accounting server. To add another RADIUS accounting server, click **+**. To delete a RADIUS accounting server, click **-**.
Enable Dynamic Auth	Toggle it on to enable the RADIUS Dynamic Auth server. Once enabled, configure the following parameters: • **Dynamic Auth Host:** The FQDN or IP address of the Dynamic Auth server. • **Dynamic Auth Port:** The port used to access the Dynamic Auth server. The value must be between 1024 and 65535. • **Dynamic Auth Secret:** The security secret used to access the Dynamic Auth server. To add another Dynamic Auth server, click **+**. To delete a Dynamic Auth server, click **-**.
MAC Filter	Toggle it on to enable the MAC filter function. Once enabled, client MAC addresses can be passed to RADIUS as attributes like Calling-Station-ID, enabling terminal-identity-based authentication and authorization control. This method is commonly used for MAC Authentication Bypass (MAB), device binding, and blacklist or whitelist management.
NAS Identifier	The attribute used to identify the Network Access Server (NAS) that sends the access request.

	If you enter an **NAS Identifier** value, the NAS identifier can be explicitly passed during RADIUS authentication, enhancing the identification of access devices and policy control.
Chargeable User ID	Toggle it on to enable the chargeable user ID attribute. This attribute is assigned by a RADIUS server. It is anonymous yet uniquely identifies users. It's designed for cross-domain authentication, accounting, and auditing scenarios to ensure traceability and billability while concealing real identities.

Adding MPSK Profiles

To add an MPSK profile, follow these steps:

> **Tips**
>
> - MPSK is an extension of WPA2/3-Personal, enabling an SSID to support multiple pre-shared keys (PSKs). By using MPSK, you can achieve fine-grained access management, including user differentiation, policy control, and password isolation.
> - See the following example scenarios of MPSK:
>   - **Enterprise or campus networks:** Each employee uses an independent Wi-Fi password while sharing a unified SSID.
>   - **Hotel or guesthouse networks:** Each room or guest is assigned a unique PSK to prevent cross-room usage.
>   - **Home networks:** Internet of Things (IoT) devices use a dedicated PSK while family members use another PSK. You can also isolate the VLANs used by IoT devices and family members.

1. In the **MPSK** tab, click **+ MPSK**.
2. In the pop-up window, input the following information, and then click **Apply**.

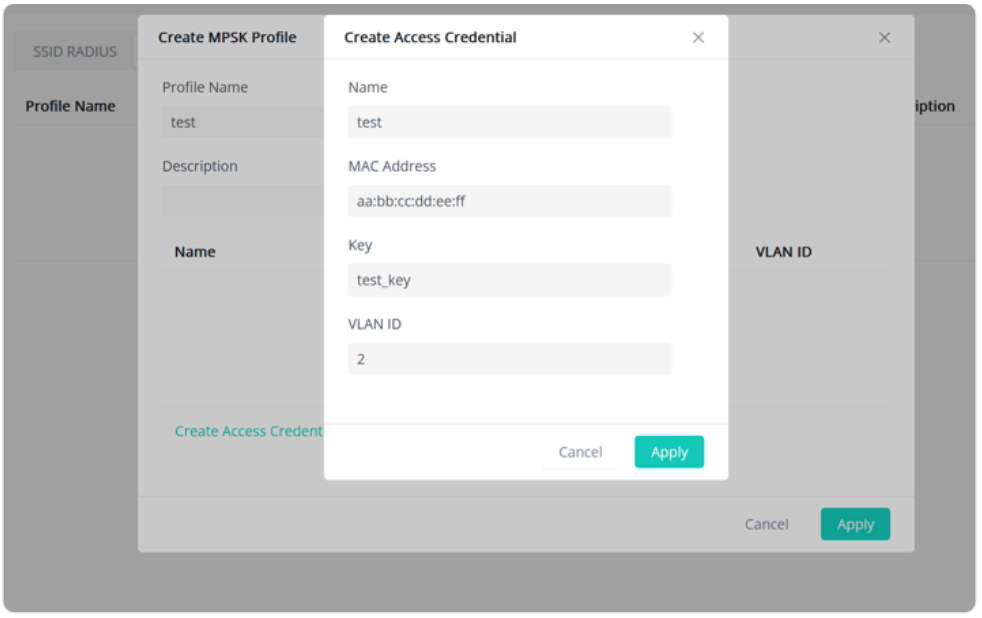


Table 3. MPSK Parameters

Parameter	Description
Profile Name	The name of the MPSK profile. The name can contain at most 64 characters.
Description	Optional. The description of the MPSK profile. The description can contain at most 128 characters.
Credential	Add one or multiple wireless client credentials. To add a credential of a wireless client, click **Create Access Credential**. Then, enter the following information, and click **Apply**. • **Name:** The name of the wireless client. The name can contain at most 64 characters. • **MAC Address:** Optional. The MAC address of a wireless client. • **Key:** The key used by the wireless client to connect to the SSID. The value must contain 8 to 63 ASCII characters. • **VLAN ID:** The VLAN ID assigned to the wireless client. The value must range from 2 to 4048. Do not enter the native VLAN ID of the uplink switch. Otherwise, the wireless network will not work. To edit a credential, hover over it, and then click **Edit**. To delete a credential, hover over it, and then click

	Delete.

Adding Portal Profiles

To add a portal profile, follow these steps:

> **Tips**
>
> - A Captive Portal is a web-based authentication mechanism. When a wireless client connects to the SSID, all web traffic is temporarily intercepted and redirected to a dedicated login webpage. Users must complete verification such as accepting terms of service, entering a password, or logging in with credentials before obtaining full internet access.
> - By adding portal profiles, you can configure the Captive Portal display, such as display of authentication, billing, and brand.

1. Click the **Portal** tab, and then click **+ Portal**.
2. In the pop-up window, input the following information, and then click **Apply**.

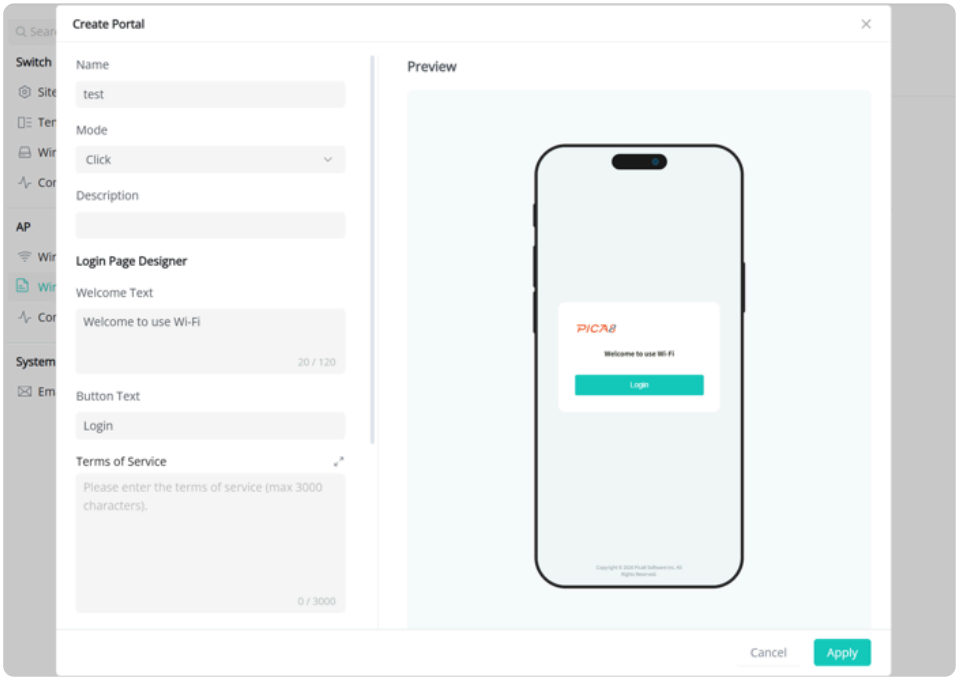


Table 4. Portal Parameters

Parameter	Description
Name	The name of the portal profile. The name can contain at most 64 characters.
Mode	The authentication mode.

	• **Click:** Connects to the Wi-Fi without entering a password. After a portal authentication page pops up, users can click to access the internet. • **RADIUS:** Connects to the Wi-Fi through credentials stored in an external RADIUS server. • **Credentials:** A username and password based authentication method. You can directly store credentials on the AP side without deploying a RADIUS server.
Description	Optional. The description of the portal profile. The description can contain at most 128 characters.
Welcome Text	Optional. The welcome text of Captive Portal. The text can contain at most 120 characters.
Button Text	Optional. The text of the login button, such as **Login**. The text can contain at most 20 characters.
Terms of Service	Optional. The detailed terms of service, which define the rights, obligations, and scope of responsibilities for the service provider and the user. After you enter terms of service, you can see “I agree to Terms of Service” in the **Preview** section. The value can contain at most 3000 characters.
Upload Logo	Optional. The logo of Captive Portal. Drag and drop a logo file, or click **Choose File** and select a logo file. Only PNG, JPG, JPEG, and GIF files can be uploaded. The uploaded file size must be less than 40 KB.
Background	The background color of Captive Portal. Click the **Background** field to select a color or enter the color values.
Copyright	Optional. The copyright displayed in Captive Portal. The value can contain at most 120 characters.

Adding Time Range Profiles

To add a time range profile, follow these steps:

> **Tips**
>
> - By adding a time range profile, you can schedule weekly-based enabling or disabling time ranges for different SSIDs or radios.
> - If both an SSID and a radio have time-based policies configured, the radio's time-based policy takes precedence.

1. Click the **Time Range** tab, and then click **+ Time Range**.
2. In the pop-up window, input the following information, and then click **Apply**.

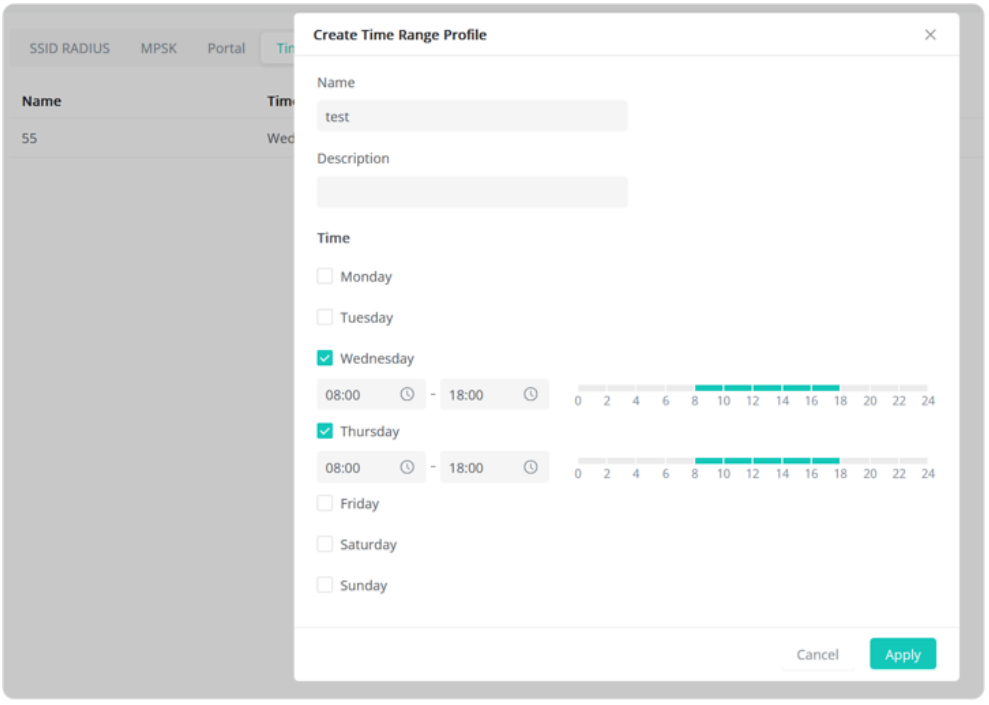


Table 5. Time Range Parameters

Parameter	Description
Name	The name of the time range profile. The name can contain at most 64 characters.
Description	Optional. The description of the time range profile. The description can contain at most 128 characters.
Time	Select days of a week. For each selected day, click the start time and end time fields to select the start time and end time, or click the time bar to specify the time range.

Maintaining Wireless Networks

After onboarding access points (APs) to AmpCon-Campus, you can maintain APs as needed.

- Accessing APs
- Positioning APs
- Rebooting APs
- Upgrading APs
- Restoring to Factory Settings
- Capturing Remote Port Packets
- Enforcing Site Configurations
- Optimizing Wireless Networks
- Advanced CLI Configurations
- Deleting APs
- Moving APs to Another Site

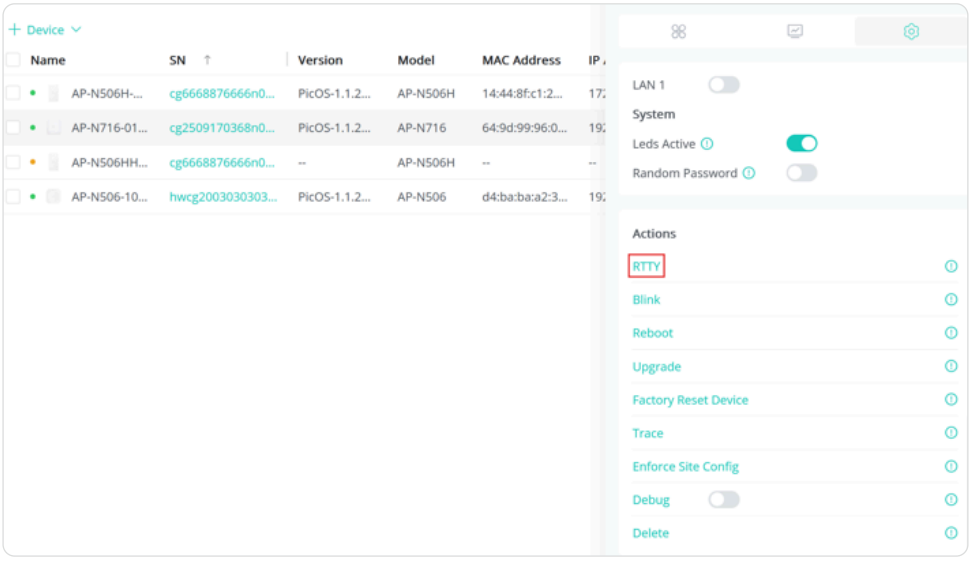
Accessing APs

You can establish a remote terminal session to an AP through remote TTY shell (RTTY). Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP.

> **NOTE**
>
> Only online APs can be accessed through RTTY. Online APs refer to APs connected to AmpCon-Campus.

3. Click the **Setting** tab of the side panel. In the **Actions** section, click **RTTY**.



4. In the newly-opened browser tab, enter the AP username and password.

Positioning APs

In large office buildings, shopping malls, schools, hospitals, airports, convention centers, and other locations, dozens or even hundreds of access points (APs) might be deployed. These APs look similar and are installed in dispersed locations, making AP identification difficult.

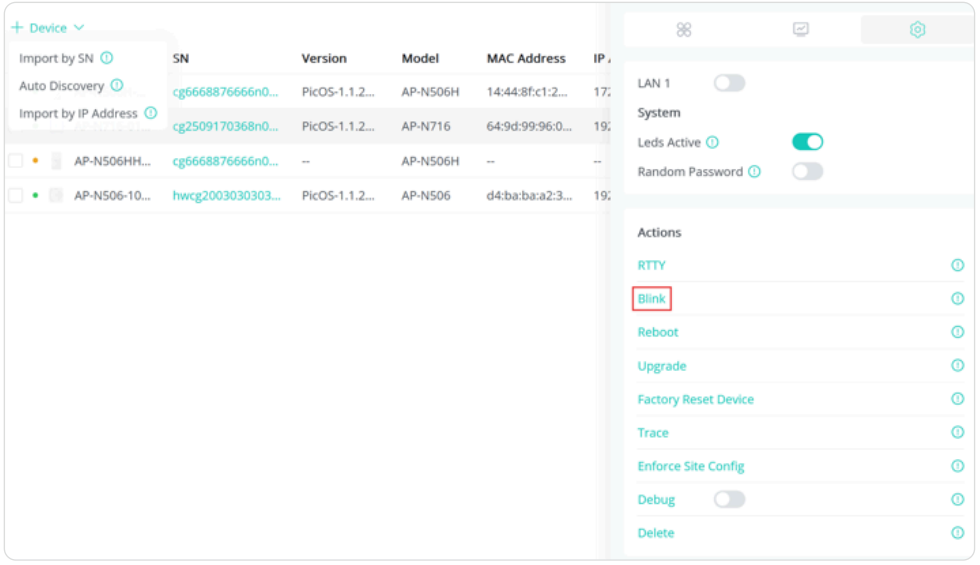
By using AmpCon-Campus, you can position APs more easily. When an AP has signal anomalies or requires maintenance or replacement, you can remotely trigger its LED to blink, enabling quick on-site localization. This feature is also useful for scenarios where AP labels are missing or fuzzy.

To position an online AP, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP.

> **NOTE**
>
> Only online APs can be positioned through this feature.

3. Click the **Setting** tab of the side panel. In the **Actions** section, click **Blink**.



4. In the pop-up window, click **Yes** to confirm the action.

Rebooting APs

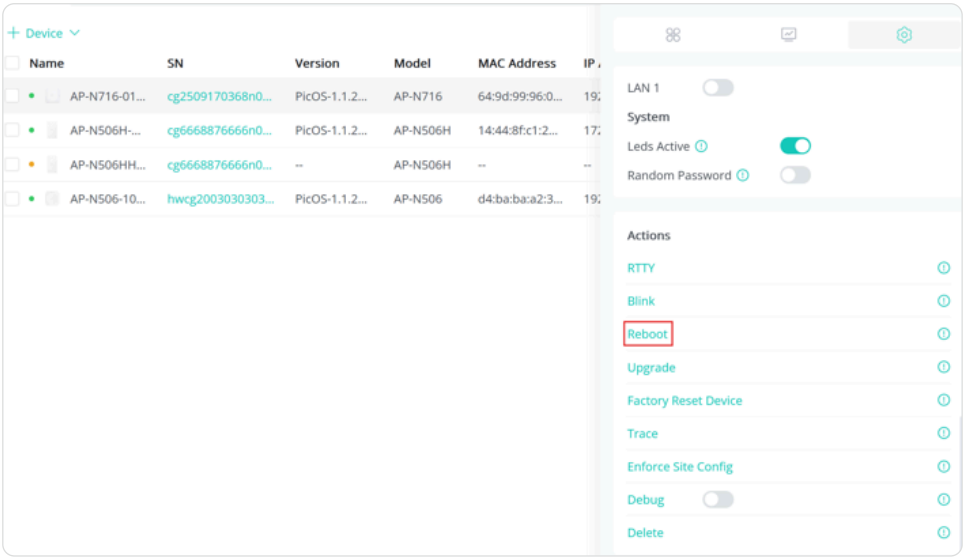
You can reboot a single online AP or multiple online APs in batches. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, reboot APs by using one of the following ways:

> **NOTE**
>
> Only the APs meeting all the following conditions can be rebooted:
>
> - The APs are currently online (connected to AmpCon-Campus).
> - No upgrade tasks are running on the APs.

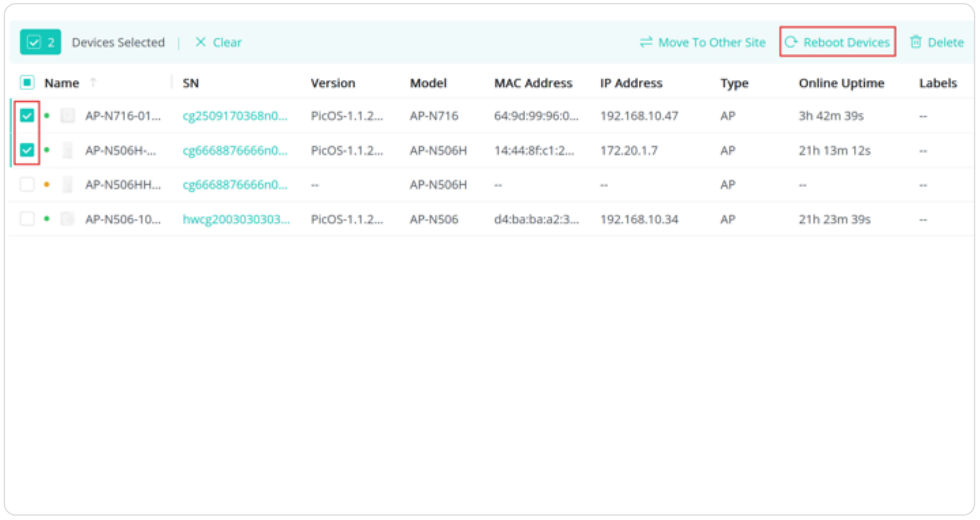
- To reboot a single AP, click the AP in the device list. In the **Setting** tab of the side panel, click **Reboot**.

  In the pop-up window, click **Yes** to confirm the reboot.



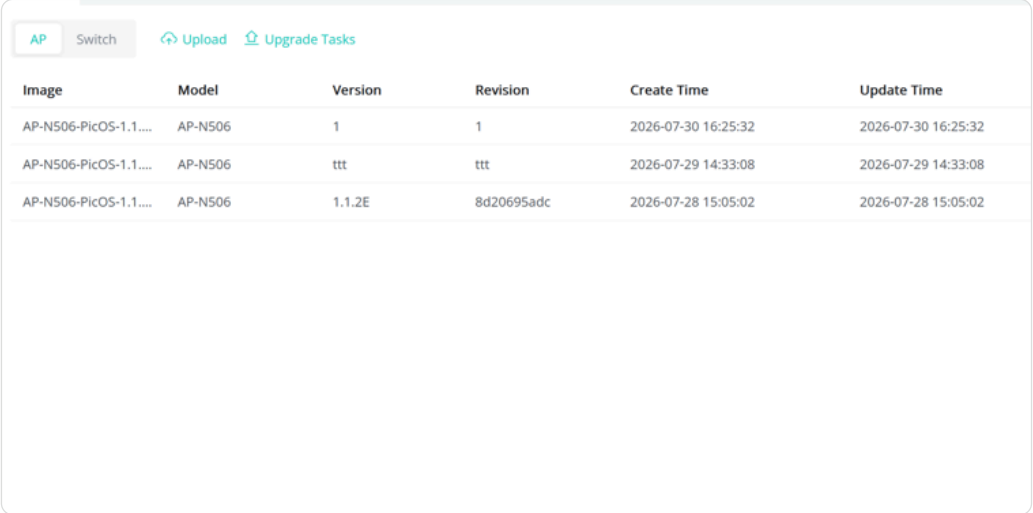
- To reboot multiple APs, select the APs in the device list, and then click **Reboot Devices** at the top.

  In the pop-up window, click **Yes** to confirm the reboot.



Upgrading APs

You can upgrade AP firmware one by one or in batches. In addition, you can upgrade AP firmware immediately or at a scheduled time. For more information, see Upgrading APs.



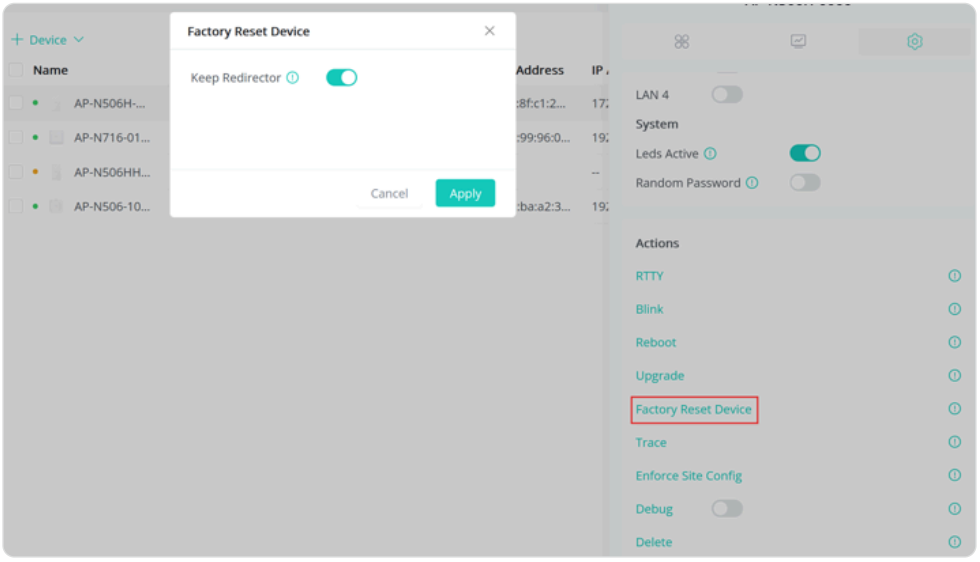
Restoring to Factory Settings

You can wipe all custom settings and restore an online AP to its original status (factory settings). This action is irreversible. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP.

> **NOTE**
>
> Only online APs can be restored to factory settings.

3. Click the **Setting** tab of the side panel. In the **Actions** section, click **Factory Reset Device**.
4. In the pop-up window, toggle on or toggle off **Keep Redirector**, and then click **Apply**.



- If you toggle on **Keep Redirector**, the AP will automatically reconnect to AmpCon-Campus and will still be managed by AmpCon-Campus after restoration.
- If you toggle off **Keep Redirector**, the AP will not reconnect to AmpCon-Campus and will not be managed by AmpCon-Campus after restoration.

You need to onboard the AP to AmpCon-Campus again.

Capturing Remote Port Packets

You can capture remote packets from target ports of an online AP for rapid troubleshooting. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP.

> **NOTE**
>
> You can capture remote packets from only online APs.

3. Click the **Setting** tab of the side panel. In the **Actions** section, click **Trace**.
4. In the pop-up window, input the following information:

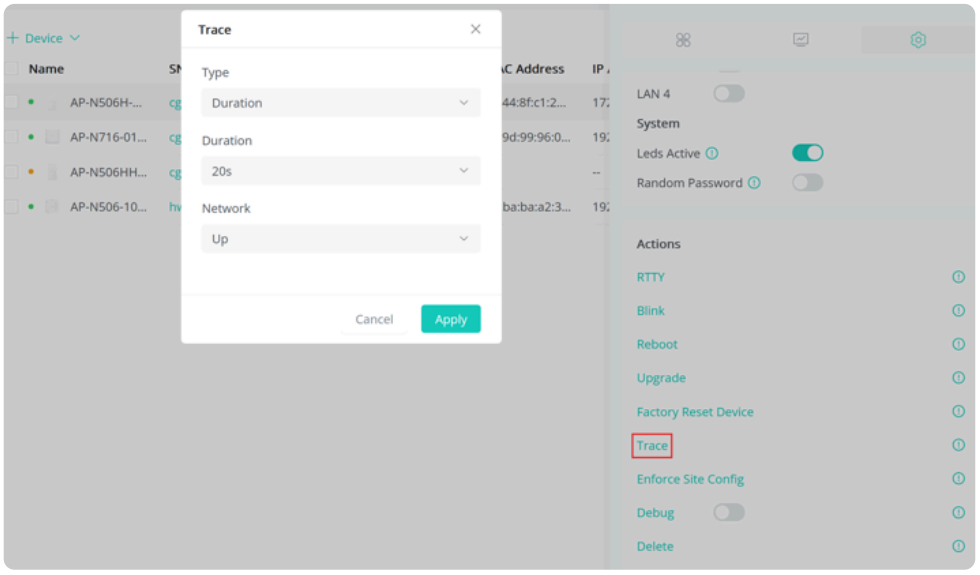


Table 1. Trace Parameters

Parameter	Description
Type	The packet capturing type. • If you select **Duration** as the type, select a duration in the **Duration** drop-down list. Then, AmpCon-Campus will capture packets for the selected duration after you start the packet capturing. • If you select **Packets** as the type, select a packet count in the **Packets** drop-down list.

	Then, AmpCon-Campus will capture the specified count of packets after you start the packet capturing.
Network	The ports to be captured. Currently, you can select only **Up** because only ports in **Up** status can be captured.

5. Click **Apply**. After the trace operation is completed, the trace file will be automatically downloaded to your local machine.

Enforcing Site Configurations

To clear all device-specific configurations for this AP and force the AP to inherit site-level configurations, follow these steps:

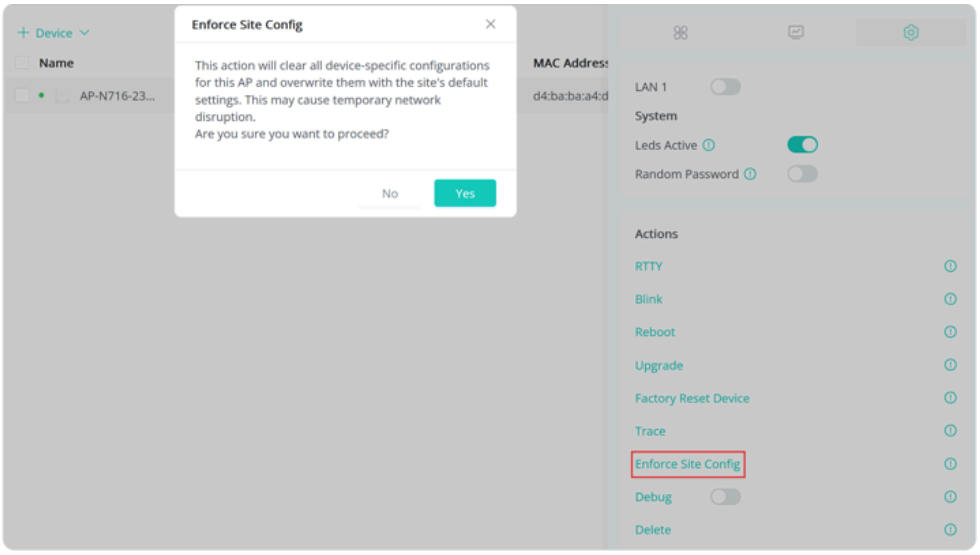
1. In the AmpCon-Campus UI, select the site to which the AP belongs.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP.

> **NOTE**
>
> This **Enforce Site Config** button is unavailable in any of the following cases:
>
> - The site to which the AP belongs has no site-level wireless configurations.
> - **Wireless Meshing** is enabled in the site-level radio configurations, and the AP is a mesh root AP or mesh child AP.
>
> For more information, see Adding Radio Configurations.

3. Click the **Setting** tab of the side panel. In the **Actions** section, click **Enforce Site Config**.

   In the pop-up window, click **Yes**.

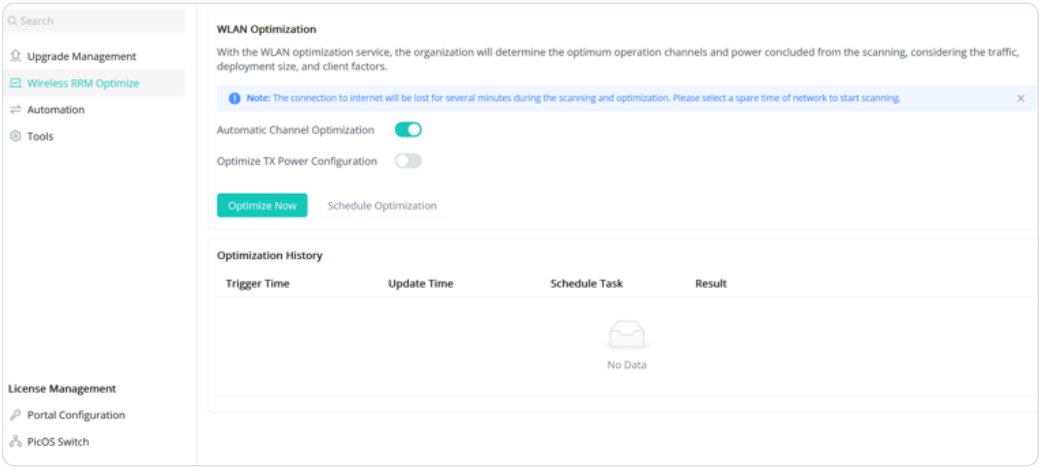
> **NOTE**
>
> This action is irreversible and will cause temporary network disruption.



Optimizing Wireless Networks

You can use one-click network optimization to rapidly optimize wireless network performance through automation technologies.

For more information, see Optimizing Wireless Networks.

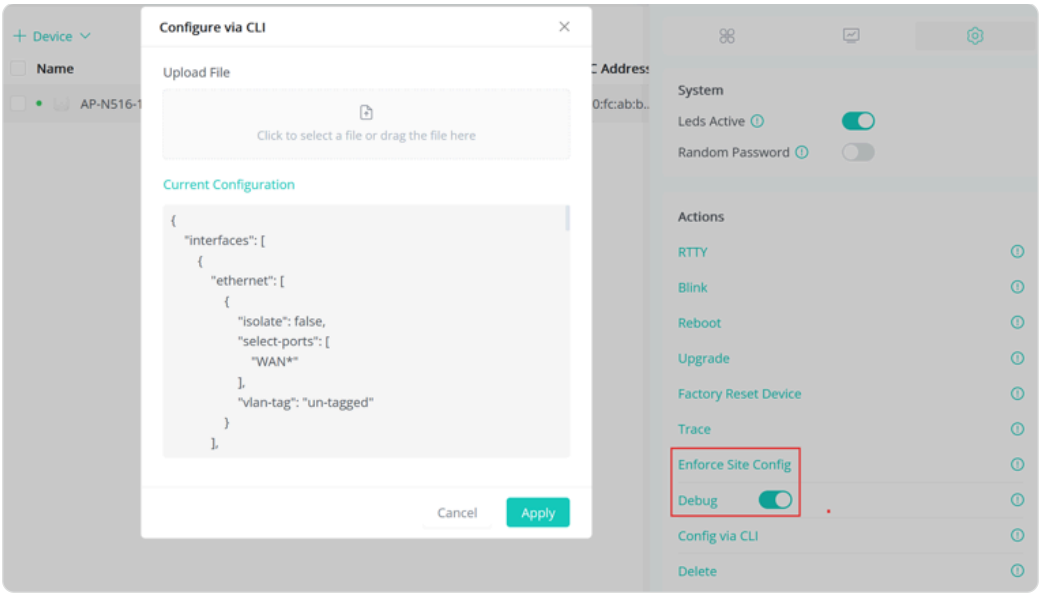


Advanced CLI Configurations

AmpCon-Campus supports CLI configurations for APs. If some issues can be resolved only through CLI configurations or some advanced functions can be achieved only through CLI configurations, contact support engineers to perform AP debugging or configuration for you through this feature.

Do not use this feature independently. Contact support engineers for assistance. Otherwise, incorrect CLI configurations might disrupt device operation.

For more information, see Configuring APs via CLI.



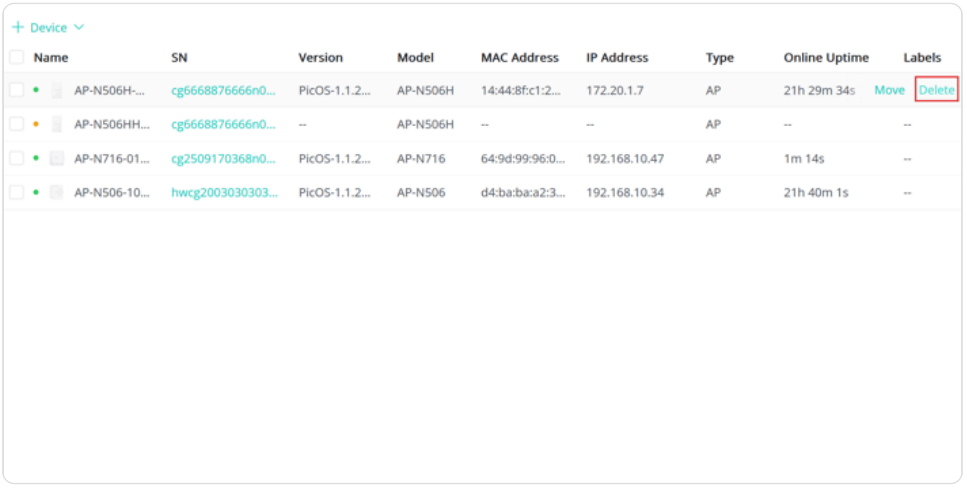
Deleting APs

On the “Devices” page, you can remove a single AP or multiple APs in batches. The deleted APs will be removed from the device list. Follow these steps:

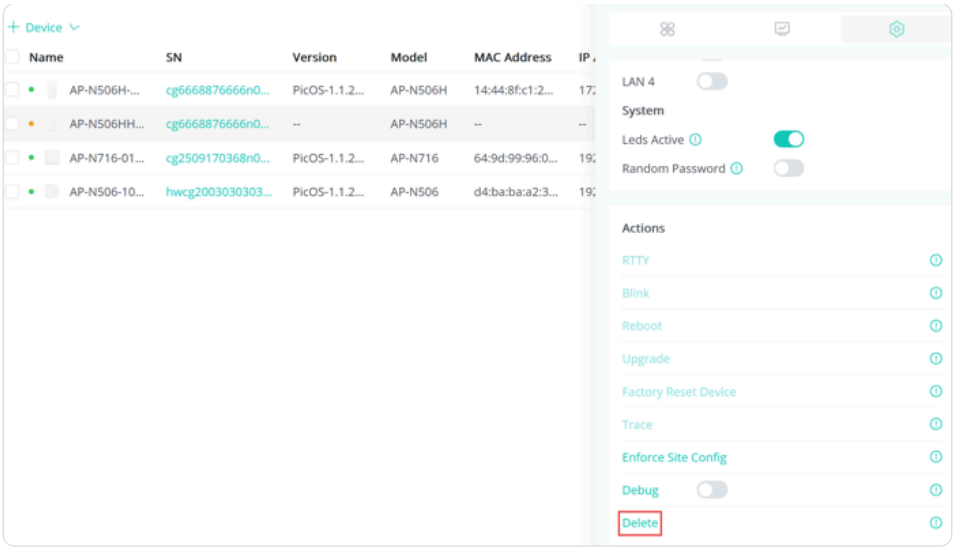
1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, delete a single AP or multiple APs by using one of the following ways:

> **NOTE**
>
> Only the APs that are not being upgraded can be deleted.

- To delete a single AP, hover over the AP, and then click **Delete**. In the pop-up window, click **Yes** to confirm the action.

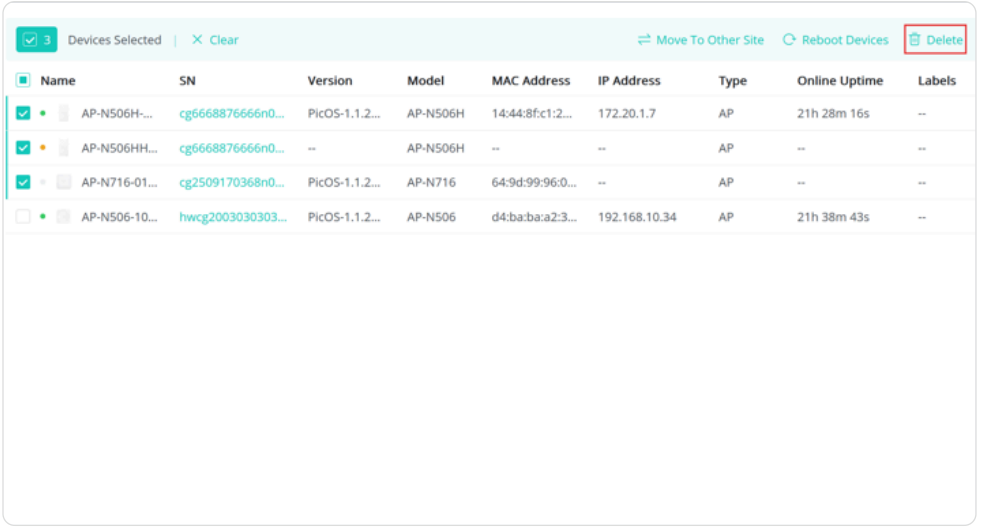


You can also delete an AP by clicking the AP, clicking the **Setting** tab of the side panel, and clicking **Delete** in the **Actions** section. In the pop-up window, click **Yes** to confirm the action.



- To delete multiple APs, select the APs in the device list, and then click **Delete**.

  In the pop-up window, click **Yes** to confirm the action.



Moving APs to Another Site

On the “Devices” page, you can move a single AP or multiple APs to another site. Follow these steps:

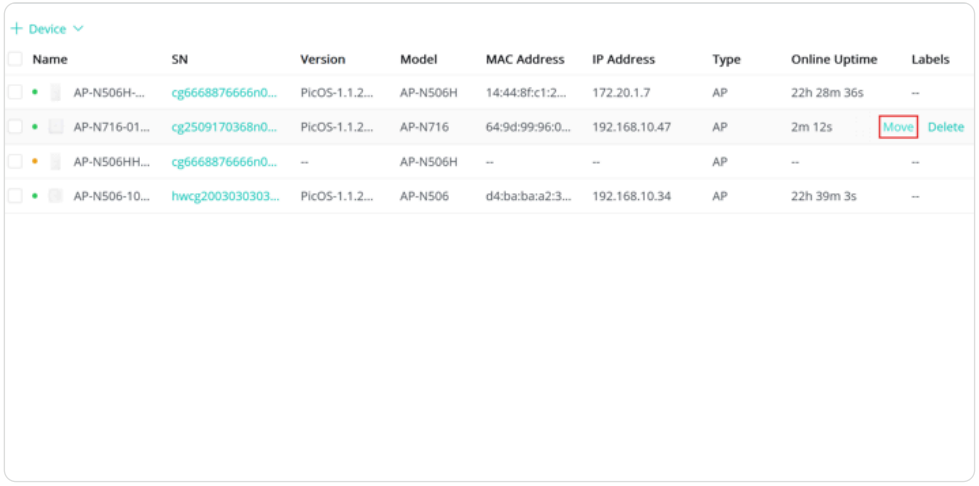
1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, move a single AP or multiple APs by using one of the following ways:

NOTEs

- APs that are being upgraded cannot be moved.
- Before moving mesh child APs to another site, reset the AP configurations. Otherwise, APs cannot be managed by AmpCon-Campus.
- Moving a non-mesh AP to a new site will clear all its device-specific configurations (such as custom radio configurations). The AP will adopt the new site's site-level configurations, causing a network disruption.
- Moving a mesh AP to a new site will disconnect its active mesh link and clear all its device-specific configurations. The AP will adopt the new site's site-level configurations, causing a network disruption.

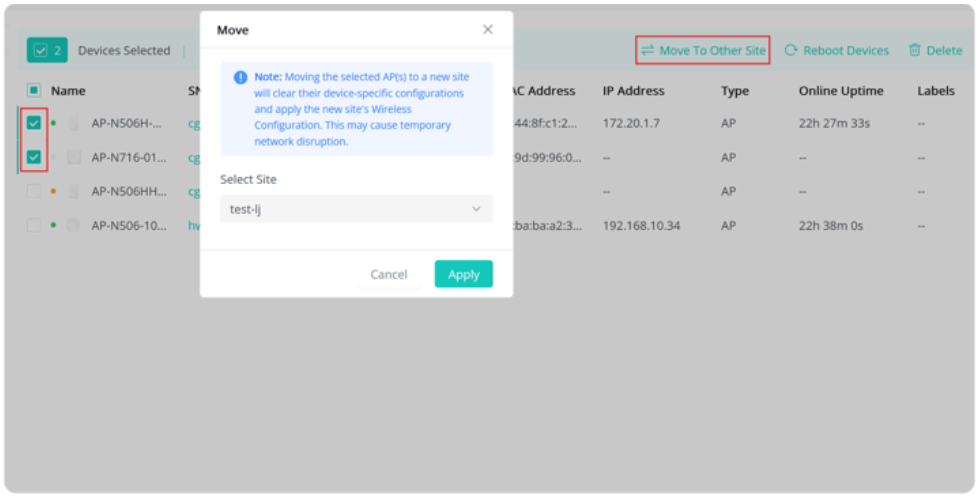
- To move a single AP to another site, hover over the AP, and then click **Move**.

  In the pop-up window, select the site to which the AP will be moved, and then click **Apply**.



- To move multiple APs to another site, select the APs in the device list, and then click **Move To Other Site**.

  In the pop-up window, select the site to which the APs will be moved, and then click **Apply**.


2 Devices Selected
Move To Other Site
Reboot Devices
Delete
Name
AP-N506H-...
AP-N716-01...
AP-N506HH...
AP-N506-10...
44:8f:c1:2...
9d:99:96:0...
ba:ba:a2:3...
172.20.1.7
192.168.10.34
AP
22h 27m 33s
22h 38m 0s
Move
Note: Moving the selected AP(s) to a new site will clear their device-specific configurations and apply the new site's Wireless Configuration. This may cause temporary network disruption.
Select Site
test-lj
Cancel
Apply

Upgrading APs

After successfully onboarding APs to AmpCon-Campus, you can upload AP images, upgrade AP firmware individually or in bulk, schedule upgrade time, and manage upgrade tasks.

You can schedule automatic upgrades during off-peak hours (such as at night or on holidays), so that your services experience minimal disruption.

- Prerequisites
- Procedure
  - Checking Images
  - Uploading Images
  - Upgrading Multiple APs
  - Upgrading a Single AP
  - Checking Upgrade Task Results
- Optional Operations
  - Managing Upgrade Tasks
  - Deleting Images

Prerequisites

Ensure that the following prerequisites are met:

Table 1. Prerequisites

Prerequisite	Reference Link
The APs to be upgraded are onboarded to AmpCon-Campus.	• Onboarding APs
The APs to be upgraded are online (connected to AmpCon-Campus).	• Viewing the AP List

Procedure

Checking Images

Check whether the required AP image exists in the image list. Follow these steps:

1. Click the **Maintain** icon from the navigation bar.
2. In the **AP** tab of the “Upgrade Management” page, check whether the required AP image exists in the image list. If not, upload the AP image as described in Uploading Images.

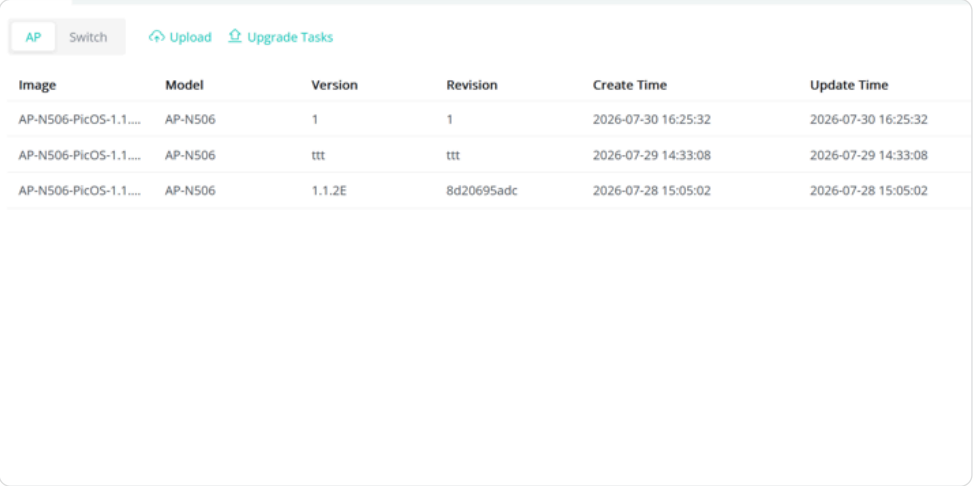


Table 2. Image Metrics

Parameter	Description
Image	The name of the AP image.
Model	The AP model compatible with the image.
Version	The version of the AP image.
Revision	The revision of the AP image.
Create Time	The upload time of the AP image.
Update Time	The update time of the AP image. **NOTE** Currently, the AP image cannot be updated, and thus the **Update Time** is the same as the **Create Time**.

Uploading Images

If the AP image that you need has been uploaded to AmpCon-Campus, skip this section. If not, upload the AP image first. Follow these steps:

1. In the **AP** tab of the “Upgrade Management” page, click **Upload**.
2. In the pop-up window, select **AP** in the **Device Type** section.
3. Upload an image by using one of the following methods:

NOTEs

- When selecting an image file or entering an image URL, ensure that the image filename or URL is in the correct format and contains correct version, revision, and model information.

  AmpCon-Campus will automatically extract version, revision, and model information based on the image filename or URL.
- If the image filename or URL is not in the correct format, AmpCon-Campus cannot automatically extract version, revision, and model information.
- You can manually change the **Version**, **Revision**, and **Model** values.

  These values must match the image file. Otherwise, even if the image is uploaded successfully, upgrade tasks that use this image might fail.

- In the **File** tab, click the upload icon to select an AP image, or drag and drop the image.

  Then, check the automatically generated **Version**, **Revision**, and **Model** values, and click **Apply**.

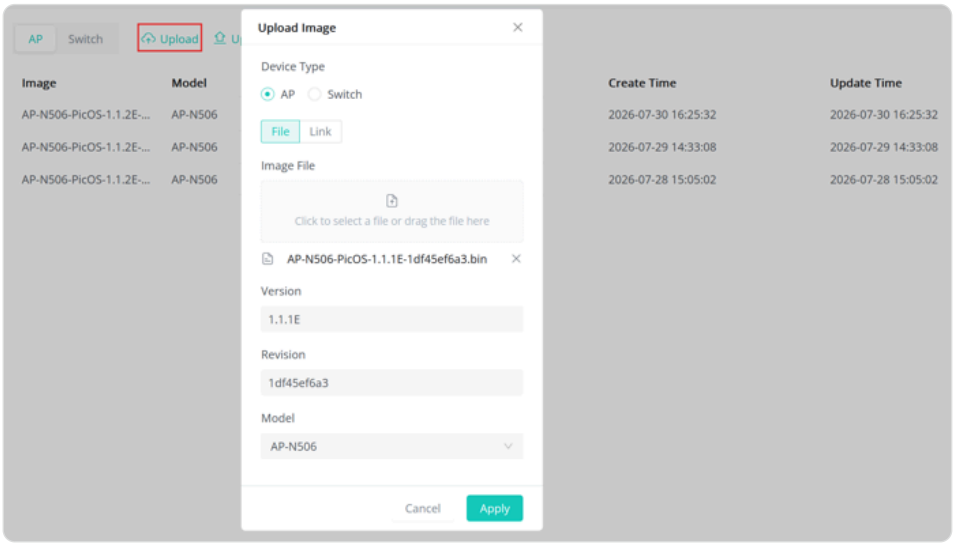
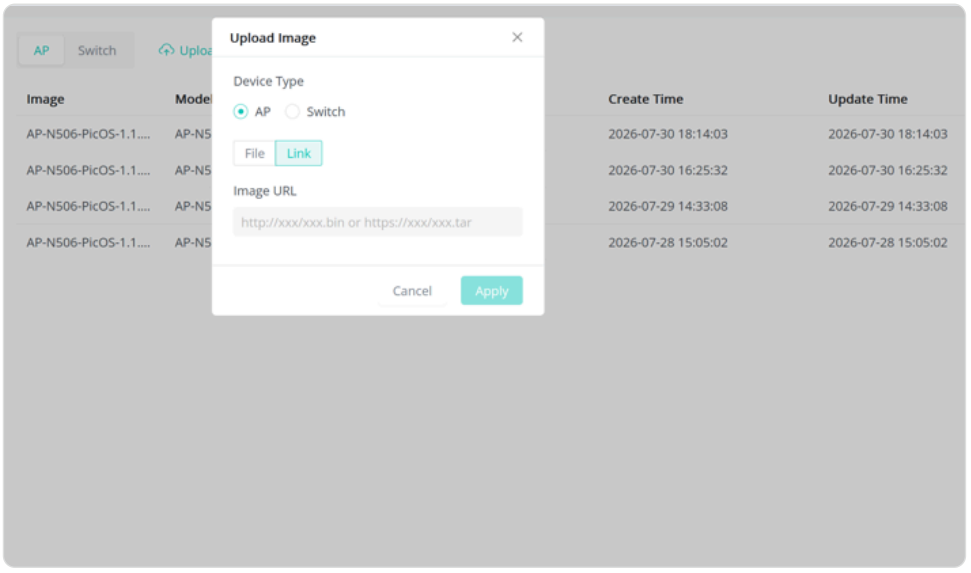


Table 3. Image Parameters

Parameter	Description
Version	The version of the AP image, such as **1.1.1E**.
Revision	The revision of the AP image, such as **8d20695adc**.

Model	The AP model compatible with the AP image, such as **AP-N506**.

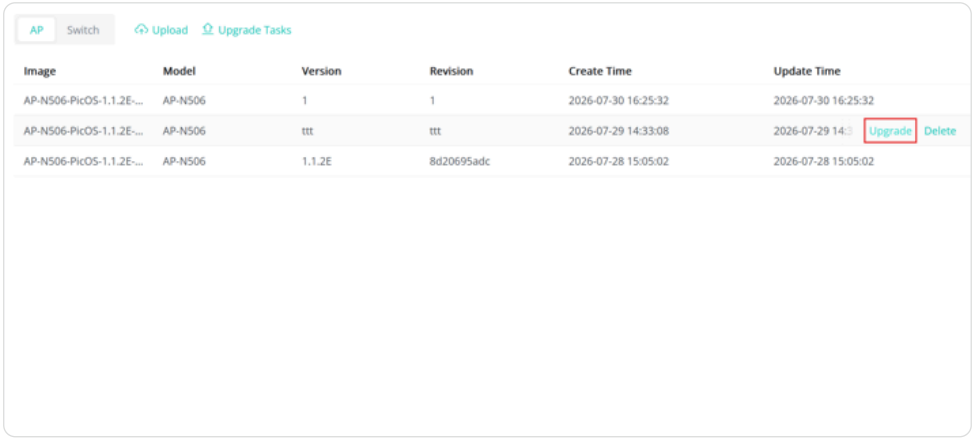
- In the **Link** tab, enter the image URL, and then click **Apply**.



Upgrading Multiple APs

To upgrade multiple APs, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. In the **AP** tab of the “Upgrade Management” page, hover over the AP image to which you want to upgrade, and then click **Upgrade**.



3. In the pop-up window, input the following information, and then click **Apply**.

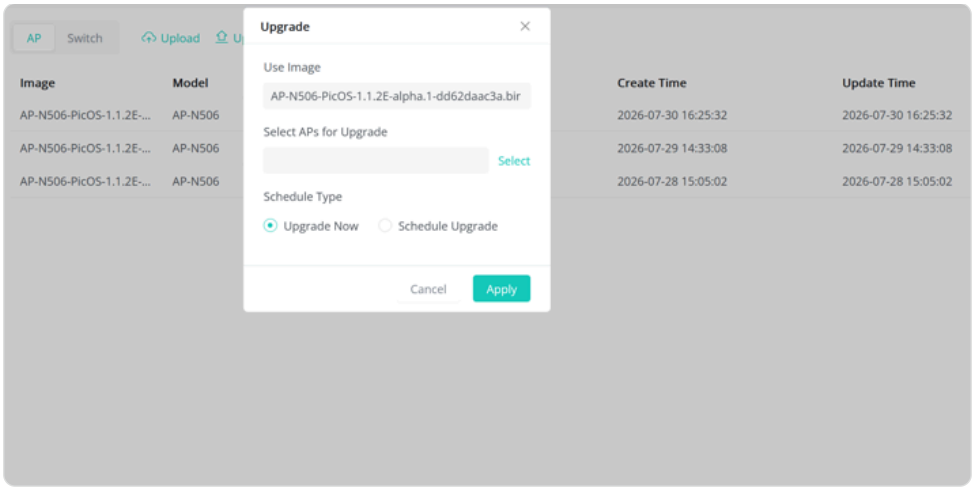


Table 4. Parameters for Upgrading Multiple APs

Parameter	Description
Select APs for Upgrade	Click **Select** to select the APs for upgrade. **NOTE** Only online APs whose models match the AP image's model are displayed.
Schedule Type	Select whether you want to upgrade the APs immediately or at a specified time. • **Upgrade Now:** Upgrades the APs immediately. • **Schedule Upgrade:** Upgrades the APs at a specified time. If you select this schedule type, select the upgrade time in the **Upgrade Time** section. **NOTEs** • The time is based on your browser's time zone. • You cannot select a time point earlier than the current time.

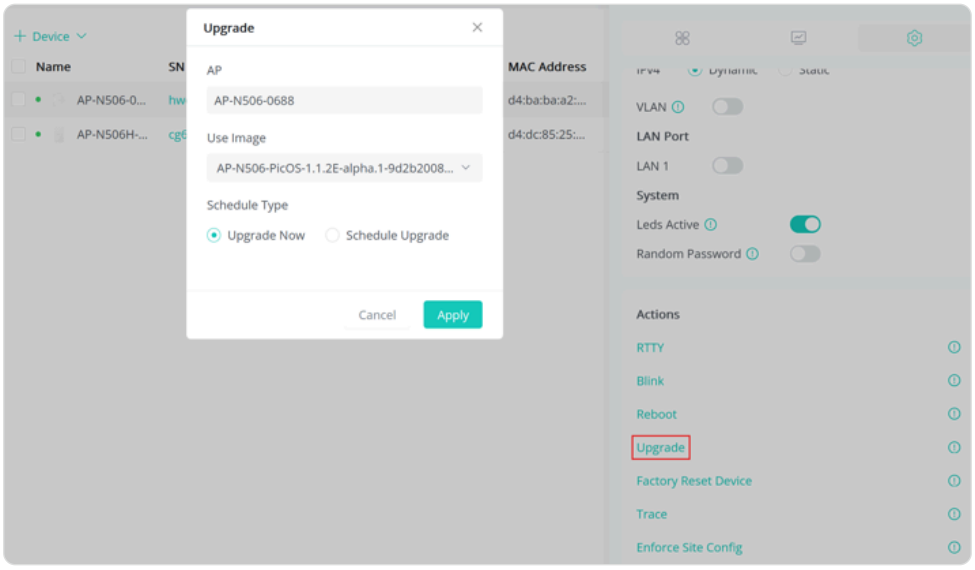
Upgrading a Single AP

To upgrade a single AP, in addition to the method described in Upgrading Multiple APs, you can use the following method:

1. In the AmpCon-Campus UI, select the site to which the AP belongs.

2. Click the **Devices** icon from the navigation bar. On the “Devices” page, click the AP in the device list.
3. In the side panel on the right, click the **Setting** tab.
4. In the **Actions** section, click **Upgrade**.

> **NOTE**
>
> The **Upgrade** button is available only if the AP meets all the following conditions:
>
> - The AP is currently online (connected to AmpCon-Campus).
> - No upgrade tasks are running on the AP.



5. In the pop-up window, input the following information, and then click **Apply**.

Table 5. Parameters for Upgrading a Single AP

Parameter	Description
Use Image	Click the drop-down list to select an AP image. **NOTEs** • Only the AP images matching the model of the AP can be selected. • If no matching images are listed in the drop-down list, upload a matching image as described in Uploading Images.
Schedule Type	Select whether you want to upgrade the AP immediately or at a specified time.

- **Upgrade Now:** Upgrades the AP immediately.
- **Schedule Upgrade:** Upgrades the AP at a specified time. If you select this schedule type, select the upgrade time in the **Upgrade Time** section.

NOTEs

- The time is based on your browser's time zone.
- You cannot select a time point earlier than the current time.

Checking Upgrade Task Results

To check upgrade task results, follow these steps:

1. In the **AP** tab of the “Upgrade Management” page, click **Upgrade Tasks**.
2. In the pop-up window, check the upgrade task details:

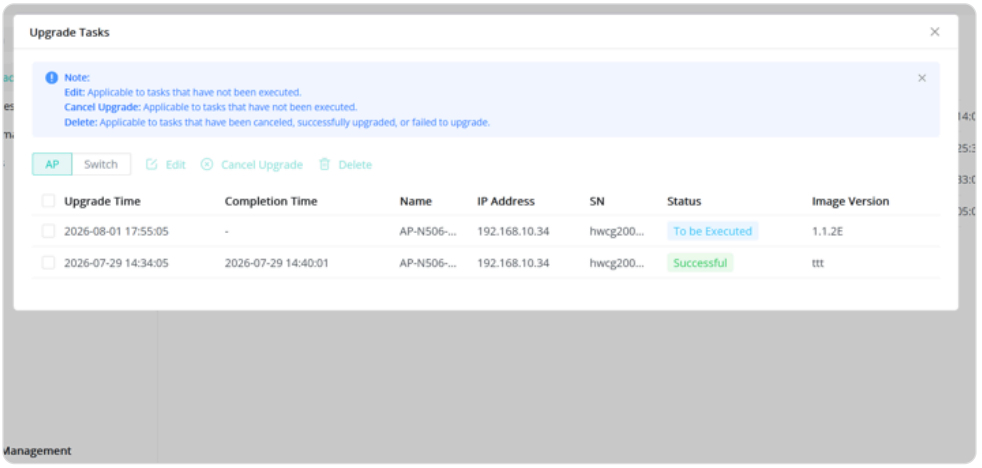


Table 6. Upgrade Task Metrics

Metric	Description
Upgrade Time	The start time of the upgrade task.
Completion Time	The completion time of the upgrade task. • If the upgrade task is not completed, the completion time is displayed as **--**. • If the upgrade task is canceled, the completion time is the time when the task is canceled.

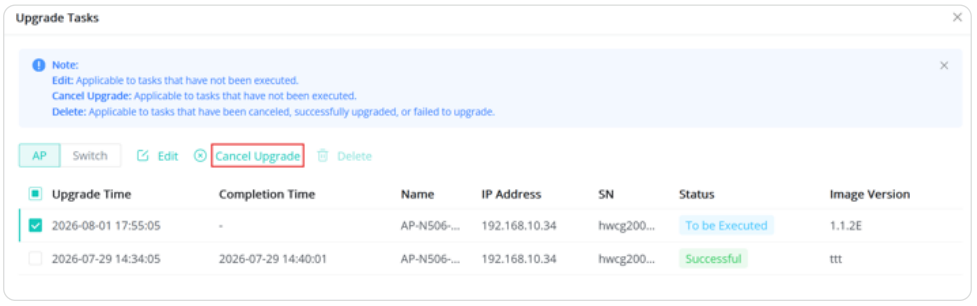
Name	The AP alias.
IP address	The IP address of the AP.
SN	The serial number of the AP.
Status	The status of the upgrade task. • **To be Executed:** The upgrade task is waiting to be executed. • **Running:** The upgrade task is in progress. • **Successful:** The upgrade task is completed successfully. • **Failed:** The upgrade task fails. The AP retains its pre-upgrade version. • **Cancel Upgrade:** The upgrade task is canceled. The AP retains its pre-upgrade version. **NOTEs** • For an AP that has an upgrade task in **To be Executed** status, if you create a new upgrade task, the previous task will be deleted, and the new one will be displayed in the upgrade task list. • For an AP that has an upgrade task in **Running** status, you cannot create a new upgrade task for the AP. • For an upgrade task in **Running** status, if AmpCon-Campus cannot connect to the associated APs for approximately 10-15 minutes, the task status will change to **Failed**.
Image Version	The version of the AP image to which you want to upgrade.

Optional Operations

Managing Upgrade Tasks

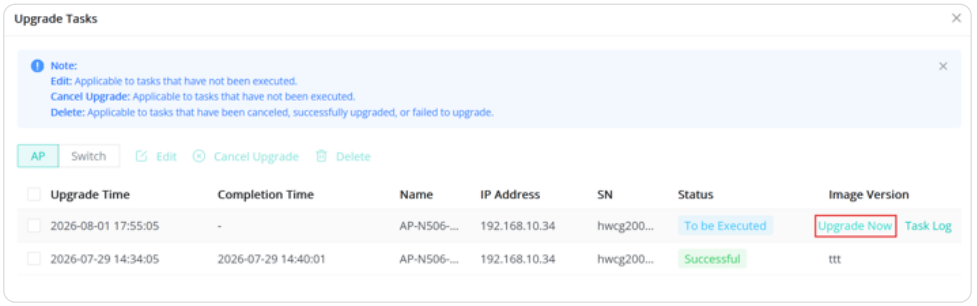
- To cancel one or multiple upgrade tasks, select the tasks, and then click **Cancel Upgrade** at the top.

> **NOTE**
>
> You can cancel only the upgrade tasks in **To be Executed** status.



- To execute an upgrade task immediately, hover over the upgrade task, and then click **Upgrade Now**.

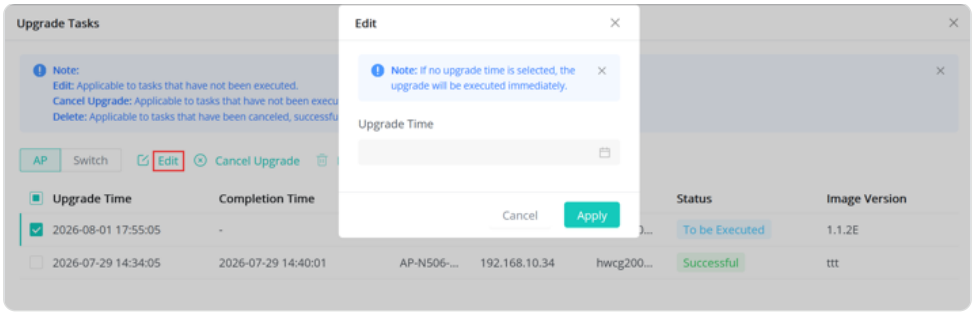
> **NOTE**
>
> You can immediately execute only the upgrade tasks in **To be Executed** status.



- To change the execution time of one or multiple upgrade tasks, select the upgrade tasks, and then click **Edit** at the top.

  In the pop-up window, select the execution time in the **Upgrade Time** section, and then click **Apply**.

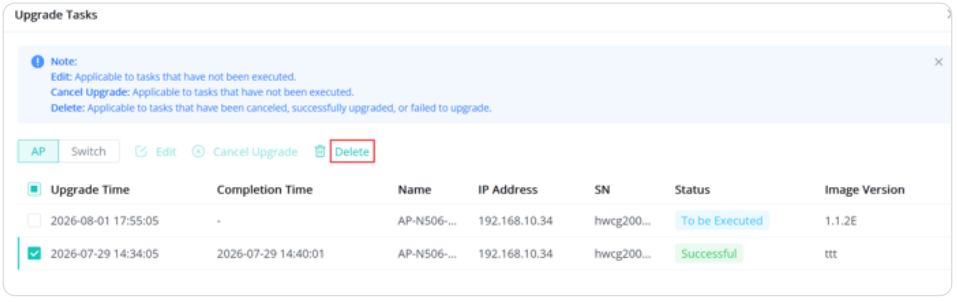
> **NOTEs**
>
> - You can edit only the upgrade tasks in **To be Executed** status.
> - In the **Edit** pop-up window, the **Upgrade Time** is blank by default. If you click **Apply** without selecting a time, the upgrade tasks will be executed immediately.



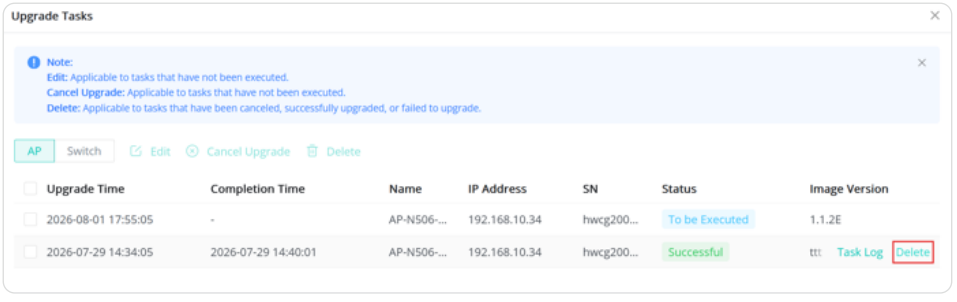
- To delete upgrade tasks, use one of the following methods:

> **NOTE**
>
> You can delete only the upgrade tasks in **Successful**, **Failed**, or **Cancel Upgrade** status.

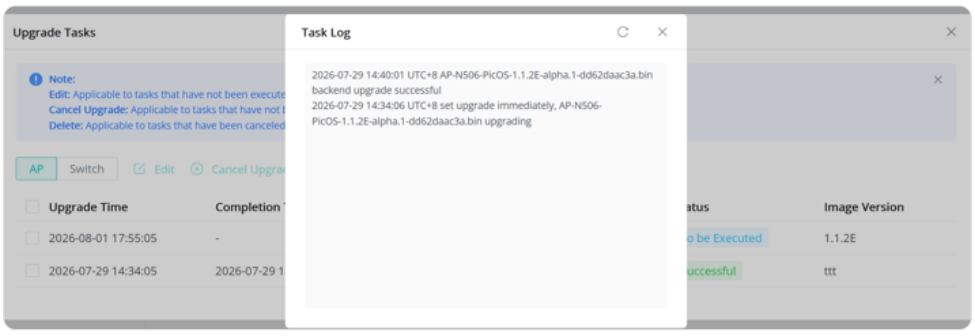
To delete multiple upgrade tasks, select the upgrade tasks, and then click **Delete** at the top. In the pop-up window, click **Yes** to confirm the deletion.



To delete a single upgrade task, hover over the upgrade task, and then click **Delete** on the right. In the pop-up window, click **Yes** to confirm the deletion.



- To check the logs of an upgrade task, hover over the task, and then click **Task Log**.

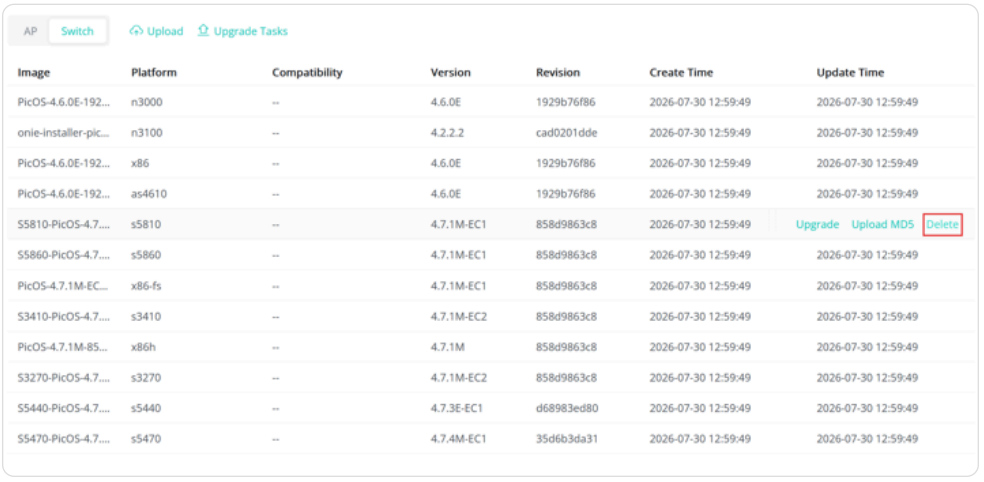


Deleting Images

To delete an AP image, follow these steps:

1. In the **AP** tab, hover over the AP image, and then click **Delete**.

> **NOTE**
>
> If an AP image is associated with upgrade tasks, you can delete it only when the upgrade tasks are in **Successful**, **Failed**, or **Cancel Upgrade** status.



2. In the pop-up window, click **Yes** to confirm the deletion.

Optimizing Wireless Networks

AmpCon-Campus provides one-click network optimization. By using this feature, you rapidly optimize wireless network performance through automation technologies, simplifying traditional optimization processes and reducing operational complexity.

Guidelines
Procedure

Guidelines

- One-click network optimization is mainly used in enterprise-level or high-density scenarios to address issues such as signal interference, load imbalance, and weak client connections.
- AmpCon-Campus supports two network optimization methods:

Table 1. Optimization Methods

Method	Description
Immediate optimization	Executes wireless network optimization immediately based on the current configurations. It is typically used in the following scenarios: • A wireless network is deployed but hasn't been optimized. • The wireless network experiences significant interference and thus requires prompt optimization.
Scheduled optimization	Optimizes wireless networks at a fixed time on a specific day, certain days, or daily.

- Network optimization does not take effect for mesh root and mesh child APs.
- Ensure that APs in the selected site are online (connected to AmpCon-Campus).

  Network optimization does not take effect for offline APs. After offline APs come online, you need to perform network optimization for these APs again.

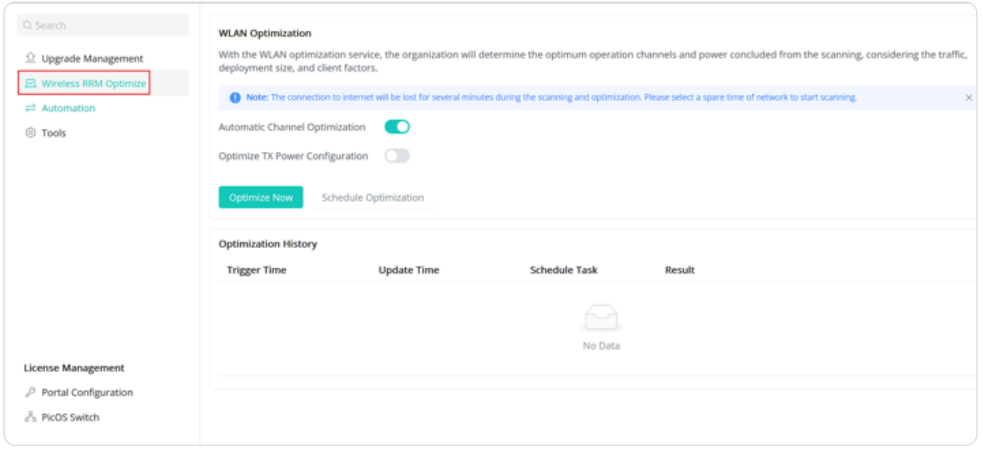
Procedure

To perform network optimization for APs in a site, follow these steps:

1. In the AmpCon-Campus UI, select a site to which the APs to be optimized belong.

> **NOTE**
>
> Ensure that the site contains at least one AP. Otherwise, the optimization will fail.

2. Click the **Maintain** icon from the navigation bar, and then click **Wireless RRM Optimize** from the sidebar.



3. Customize the optimization methods. You must use at least one of the following optimization methods:

Table 2. Optimization Parameters

Method	Description
Automatic Channel Optimization	Toggle it on to automatically select the optimal channel, ensuring efficient network operation by monitoring the channel usage of surrounding APs. You are recommended to toggle it on. If the performance can't meet your needs, enable **Optimize TX Power Configuration** separately for further tuning.
Optimize TX Power Configuration	Toggle it on to dynamically adjust the transmit power of APs, minimizing energy consumption, reducing interference, and ensuring communication quality. If you toggle it on, you need to configure the **Coverage Threshold** value. The value must range from -80 to -60. **NOTEs** • **Coverage Threshold** is the minimum signal strength for client devices to stably connect

to the AP. The unit is dBm.

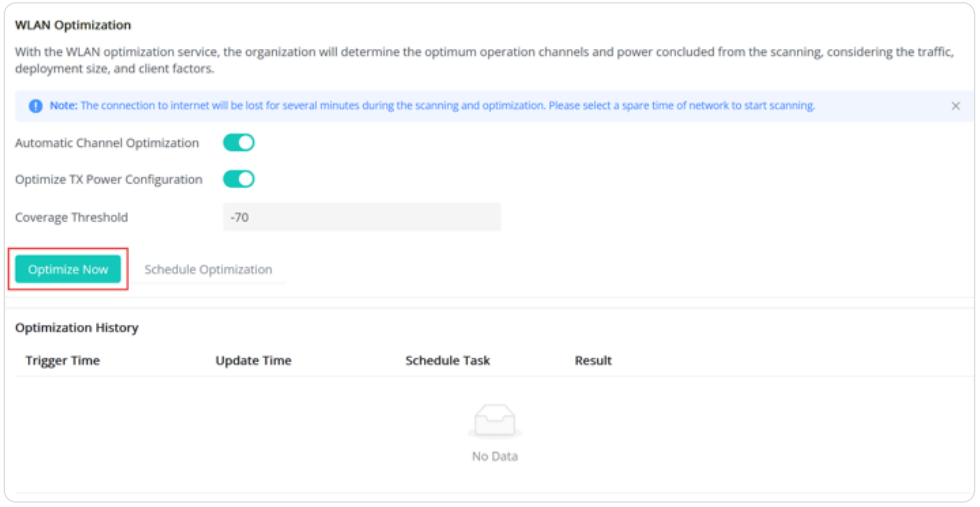
- **Coverage Threshold** dynamically adjusts the AP transmit power by monitoring the minimum Received Signal Strength Indicator (RSSI) value from neighboring APs.
- When the **Coverage Threshold** value increases (such as increasing from -70 dBm to -65 dBm), APs will determine that a stronger signal coverage is required and then increase their transmit power to expand the coverage range.
- You are recommended to increase the **Coverage Threshold** value in high-density environments to avoid interference with neighboring APs.

4. Perform network optimization for APs in the selected site immediately or at a fixed time:

NOTEs

- The whole optimization process will take several minutes. The connection to the internet will be interrupted during the process. You are advised to avoid executing optimization at peak hours.
- Network optimization might fail when you perform network optimization immediately after site creation. If this occurs, wait for a period of time, and retry the operation.

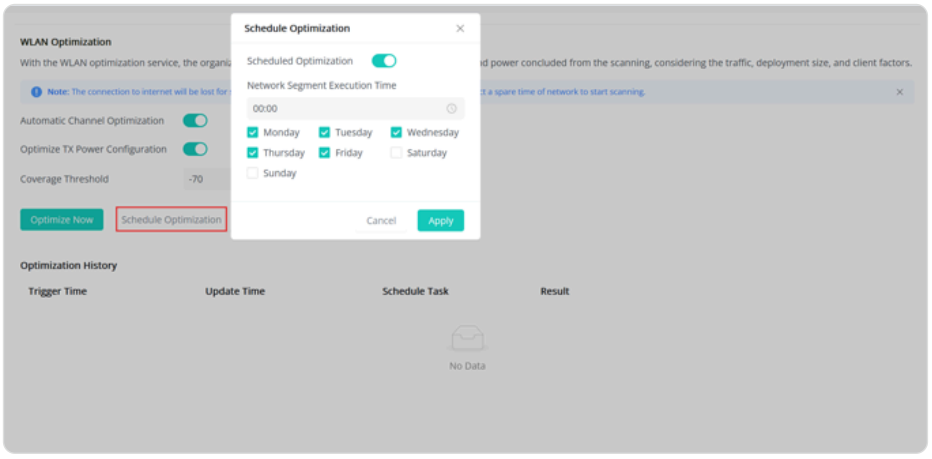
- To perform network optimization immediately, click **Optimize Now**, and then click **Yes** in the pop-up window.



- To perform network optimization at a fixed time on a specific day, certain days, or daily, follow these steps:

  a. Click **Schedule Optimization**.

  b. In the pop-up window, toggle on **Scheduled Optimization**. In the **Network Segment Execution Time** section, select the days of a week and the execution time, and then click **Apply**.



> **Tip**
>
> To disable the scheduled optimization, toggle off **Scheduled Optimization**, and then click **Apply**.

5. In the **Optimization History** section, check the optimization task that has been executed or is executing.

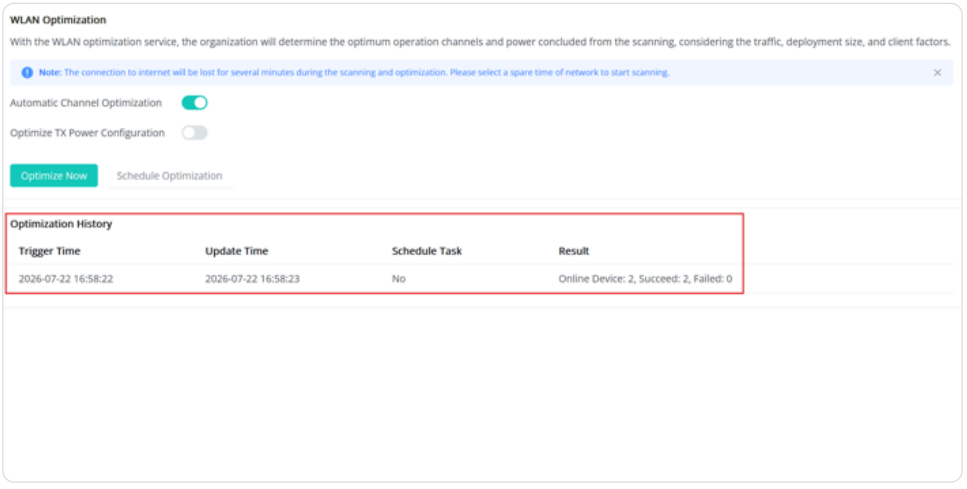


Table 3. Optimization Task Metrics

Metric	Description
Trigger Time	The time when the optimization task is triggered.

Update Time	The time when the optimization task completes successfully or fails.
Schedule Task	Whether the task is a scheduled optimization task.
Result	The result of the optimization task.

Configuring APs via CLI

AmpCon-Campus supports CLI configurations for APs. If some issues can be resolved only through CLI configurations or some advanced functions can be achieved only through CLI configurations, you can contact support engineers to perform AP debugging or configuration for you through this feature.

Do not use this feature independently. Contact support engineers for assistance. Otherwise, incorrect CLI configurations might disrupt device operation.

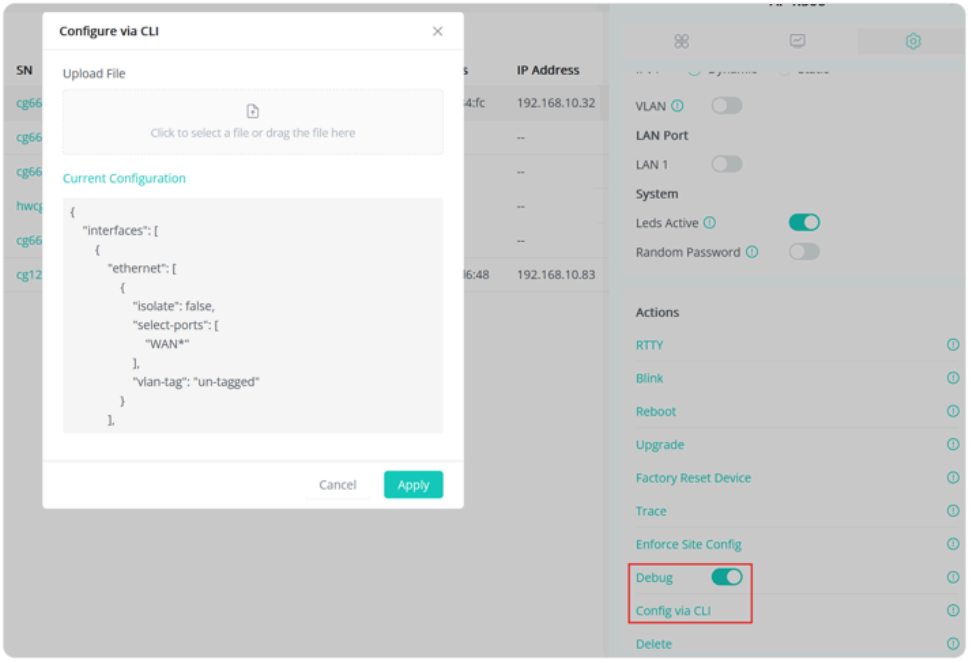
Procedure

To push advanced CLI configurations to an online AP, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar.
3. On the “Devices” page, click the AP in the device list.

> **NOTE**
>
> Ensure that the AP is online (connected to AmpCon-Campus). Otherwise, the configuration push will fail.

4. Click the **Setting** tab of the side panel. In the **Actions** section, toggle on **Debug**, and then click **Config via CLI**.



5. In the **Upload File** section, drag and drop a JSON file or click the upload icon to upload a JSON file, and then click **Apply**.

If the uploaded file does not contain valid JSON configurations, you can see the error message “Your new configuration needs to be valid JSON”.

Tips

- You can also modify the configurations directly in the configuration input box. Ensure that the configurations are correct.
- After clicking **Apply**, you can check the configuration result in the **Commands** tab. For more information, see Commands.
- To view the latest configurations that AmpCon-Campus successfully pushed to the AP, click **Current Configuration** in the pop-up window.

Automation with Ansible Playbooks

Ansible is an open-source tool to automate configuration management, application deployment, and task automation. Ansible uses the simple, declarative language written in YAML, which is called playbook, to automate your tasks. You declare the desired state of a local or remote system in your playbook. Ansible ensures that the system remains in that state. For more information about Ansible, see Getting started with Ansible.

AmpCon-Campus offers the picos_config Ansible module to interact with managed PicOS switches, making it easy to automate tasks such as configuring interfaces, VLANs, and managing security settings. The picos_config module is included in the AmpCon-Campus server.

By using AmpCon-Campus, you can write, import, run, and schedule Ansible playbooks on managed PicOS switches, reducing manual work, eliminating configuration errors, and improving network management efficiency.

See the following child topics:

- Examples for Ansible Playbooks
- Running Playbooks
- Managing Ansible Jobs
- Viewing Playbook Schedules

Examples for Ansible Playbooks

Ansible modules are code or binaries that Ansible executes on each managed device to accomplish the action defined in each Ansible task.

AmpCon-Campus offers the picos_config Ansible module to interact with managed PicOS switches. The picos_config module, included in the AmpCon-Campus server, makes it easy to automate tasks such as configuring interfaces, VLANs, and managing security settings.

Before you run Ansible playbooks on managed PicOS switches, write playbooks based on the following configuration examples, which are supported by the picos_config Ansible module.

> **NOTE**
>
> This topic only shows playbook examples for managed PicOS switches with PicOS installed.
>
> - To run Ansible playbooks, write playbooks based on playbook syntax described in Using Ansible playbooks.
> - For detailed steps of writing, importing, and running playbooks on AmpCon-Campus, see Running Playbooks.

Syntax Examples
- Running Linux Shell Commands
- Showing Switch Configurations or Status
- Modifying Switch Configurations
- Loading Configurations in a Configuration File
- Using Variables in a Playbook

Real-World Example: Automating VLAN Configurations

Syntax Examples

Running Linux Shell Commands

To run Linux shell commands on managed PicOS switches, use the **shell** mode.

Playbook YAML Example:

```
---
- name: Shows uptime info for all switches
  hosts: all
  tasks:
  - name: Shows uptime info for all switches
    picos_config: mode='shell' cmd='uptime'
    register: exec_result
  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the Linux shell command **uptime** under the **Linux shell** mode to show the current time, the time since the system and processes started, the number of

logged-in users, and the average time of system load in the last 1 minute, 5 minutes, and 15 minutes.

Replace the command in the **cmd** field with any other commands to meet your needs.

Showing Switch Configurations or Status

To show configurations or status of managed PicOS switches, use the **cli_show** mode.

Playbook YAML Example:

```
---
- name: Show Version info of all switches
  hosts: all
  tasks:
  - name: Show version of switches
    picos_config: mode='cli_show' cmd='show version'
    register: exec_result
  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the PicOS command **show version** under the **operation** mode to show switch version information. Replace the command in the **cmd** field with any other Linux shell commands to meet your needs.

Modifying Switch Configurations

To modify configurations of managed PicOS switches, use the **cli_config** mode.

Playbook YAML Example:

```
---
- name: Enable Global Config
  hosts: all
  tasks:

  - name: Enable Global Config
    picos_config:
      mode: 'cli_config'
      cmd: >
        set ip routing enable true;
        set protocols lldp enable true;
        set system services ssh idle-timeout 60;
        set system inband enable true;
        set system timezone "America/Los_Angeles";
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs PicOS commands under the **configuration** mode. Replace the commands in the **cmd** section with any other PicOS commands to meet your needs.

Loading Configurations in a Configuration File

To load configurations from a configuration file into an Ansible playbook, use the **config_load** mode.

Playbook YAML Example:

```
---
```

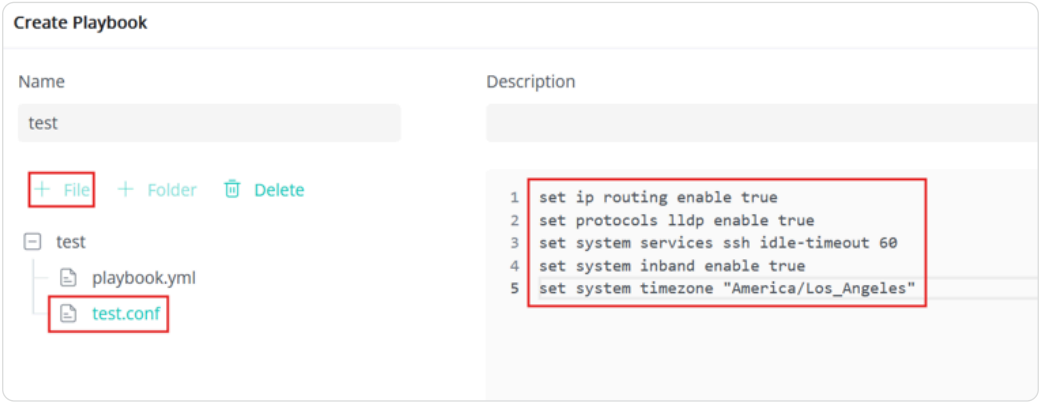
```
- name: Deploy services
  hosts: all
  tasks:
  - name: Transfer the script
    copy: src=set_global.conf dest=/home/admin/setconfig1.conf force=ye

  - name: Activate the configuration
    picos_config: mode='config_load' cmd='/home/admin/setconfig1.conf'
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example contains a syntax to copy the commands in the **set_global.conf** file (the file you added in the AmpCon-Campus UI) to the local **/home/admin/setconfig1.conf** file on the switch side. When you run the playbook on one or multiple PicOS switches, the copied commands will be loaded and then executed on these switches.

After you write the **playbook.yml** file, ensure to click **+ File** to add the **set_global.conf** file.



The **set_global.conf** file contains the following commands. Replace the commands with any other PicOS commands to meet your needs.

```
set ip routing enable true
set protocols lldp enable true
set system services ssh idle-timeout 60
set system inband enable true
set system timezone "America/Los_Angeles"
```

Using Variables in a Playbook

To define variables in an Ansible playbook, use the variable syntax {{*variable_name*}}.

Playbook YAML Example:

```
---
- name: Set Dynamic VLAN
  hosts: all
  tasks:

  - name: Set Dynamic VLAN
    picos_config: mode='cli_config' cmd='set vlans vlan-id {{vlan_id}}
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the PicOS command **set vlans vlan-id {{*vlan_id*}} vlan-name "{{*vlan_id*}}"** to create a VLAN. In the command, ***vlan_id*** is a variable and must be included in a set of curly braces.

When you run the playbook, ensure to set the variable value in JSON format as described in **Step 4** of Running a Playbook.

Real-World Example: Automating VLAN Configurations

As a network administrator, manual VLAN configuration across multiple switches is tedious and time-consuming. By using Ansible playbooks on AmpCon-Campus, you can automate this process.

Playbook YAML Example:

```
---
- name: Set VLAN Network
  hosts: all
  tasks:

  - name: Set VLAN Network
    picos_config:
      mode: 'cli_config'
      cmd: >
        set vlans vlan-id 10 l3-interface vlan10;
        set vlans vlan-id 20 l3-interface vlan20;
        set vlans vlan-id 30 l3-interface vlan30;
        set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
        set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
        set l3-interface vlan-interface vlan10 address 192.160.10.1 pre
        set l3-interface vlan-interface vlan20 address 192.160.20.1 pre
        set l3-interface vlan-interface vlan30 address 192.160.30.1 pre
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs multiple PicOS commands to achieve the following goals:

- Create vlan10, vlan20, and vlan30.
- Add a trunk LAG port (te-1/1/1) to vlan10, vlan20, and vlan30.
- Configure IPv4 addresses for L3 interfaces of vlan10, vlan20, and vlan30.

Running Playbooks

In the AmpCon-Campus UI, you can use pre-built playbooks, write or import playbooks, and run playbooks on managed PicOS switches.

In addition, AmpCon-Campus provides multiple playbook management functions, including editing, deleting, copying, or exporting playbooks and adding tags to playbooks.

- Guidelines
- Prerequisites
- Procedure
  - Using Pre-Built Playbooks
  - Writing a Playbook
  - Importing a Playbook
  - Running a Playbook
- Optional Operations
  - Viewing the Playbook List
  - Checking the Syntax for a Playbook
  - Editing, Deleting, Exporting, or Copying a Playbook
  - Adding Tags

Guidelines

- Playbooks can be run only on PicOS switches managed by AmpCon-Campus.
- Before running Ansible playbooks, pay attention to the following best practices:
  - **Test in a lab:** Always test your automation scripts in a lab or on non-production devices to ensure they work as expected.
  - **Idempotency**: Ansible playbooks must be idempotent, meaning running the playbook multiple times will not cause unintended changes.
  - **Backups**: Before applying any configuration, ensure that you have backups of the current configurations. For more information, see Backing Up Configurations.

Prerequisites

Before running Ansible playbooks, ensure that the following prerequisites are met. Otherwise, Ansible playbook execution will fail.

Table 1. Prerequisites

Task	Reference Link
Each PicOS switch to run Ansible playbooks is successfully onboarded to AmpCon-Campus.	• Onboarding PicOS Switches
Each PicOS switch to run Ansible playbooks is online (connected to AmpCon-Campus).	• Viewing the PicOS List

Ensure that the **SSH Username** and **SSH Password** in the device credential configuration match the PicOS switches exactly.	• Device Credential Configurations

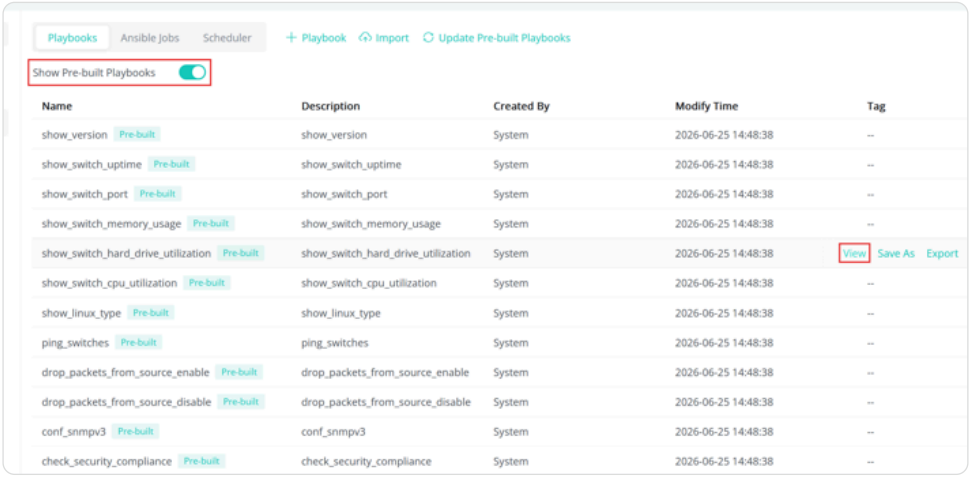
Procedure

Using Pre-Built Playbooks

Check whether pre-built playbooks meet your needs. Follow these steps:

1. In the AmpCon-Campus UI, select a site to which the PicOS switches belong.
2. Click the **Maintain** icon from the navigation bar, and then click **Automation** from the sidebar.
3. In the **Playbooks** tab, toggle on **Show Pre-built Playbooks**.

   Then, pre-built playbooks are displayed in the playbook list and are highlighted with **Pre-built**.
4. Hover over each pre-built playbook, and then click **View**.

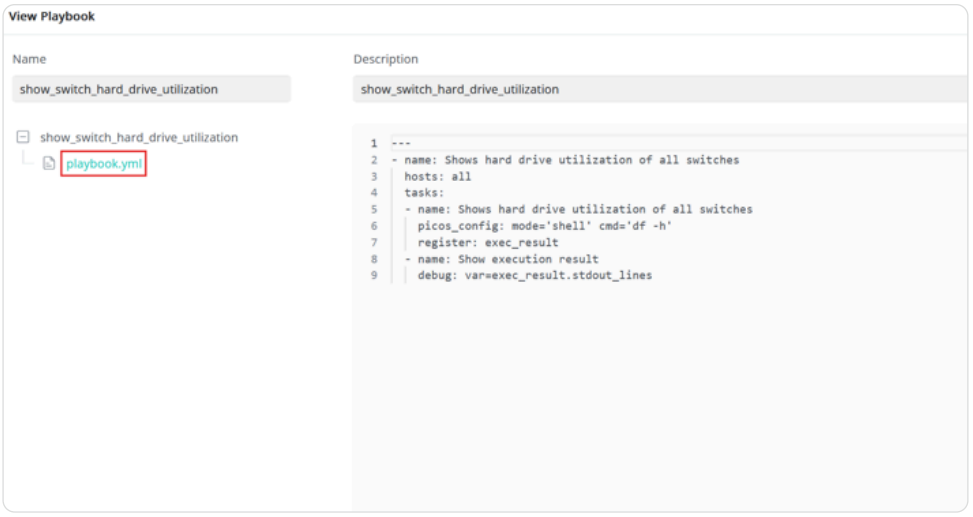


5. In the pop-up window, click **playbook.yml**, and then check whether the configurations in the right panel meet your needs.

> **NOTEs**
>
> - Pre-built playbooks cannot be run directly.
> - Pre-built playbooks are not guaranteed to be compatible with all PicOS models. You need to evaluate pre-built playbooks based on the target switch model, firmware version, and supported commands.

6. If a pre-built playbook meets your needs, hover over it, and then click **Save As** to copy it as a new playbook.

Then, run the new playbook as described in the Running a Playbook section.



Tips

- To hide pre-built playbooks, toggle off **Show Pre-built Playbooks**.
- To refresh the pre-built playbook list, click **Update Pre-built Playbooks**. If AmpCon-Campus cannot access the Internet, the refresh operation will fail.
- To export a pre-built playbook, hover over it, and then click **Export**.

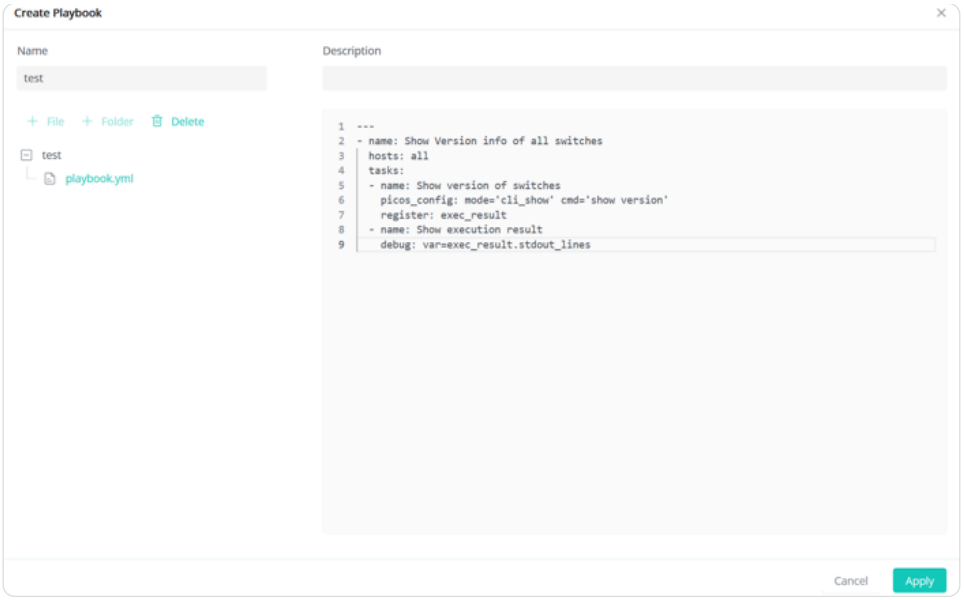
Writing a Playbook

If the pre-built playbooks do not meet your needs, you can write an Ansible playbook. Follow these steps:

1. Select a site to which the PicOS switches belong.
2. In the **Playbooks** tab, click **+ Playbook**.
3. In the pop-up window, enter the playbook name and description (optional).

NOTEs

- The playbook name must be unique.
- The playbook name can contain only letters, numbers, underscores (_), and hyphens (-) and supports a maximum of 64 characters. The name cannot start or end with a hyphen or an underscore.
- The playbook description can contain at most 128 characters.



4. Click **playbook.yml**, add configurations in the right panel, and then click **Apply**.

> **NOTEs**
>
> - Ensure that all configurations comply with Ansible playbook specifications.
> - If you need to add files or folders to the playbook, click the playbook name, and then click **+ File** or **+ Folder**.
>
> For example, to load a configuration file into the playbook in the screenshot above, click the playbook name **test**, and then click **+ File** to add a **.conf** file. For more information, see Loading Configurations in a Configuration File.
>
> The file or folder name can contain at most 64 characters. Only letters, numbers, hyphens (-), underscores (_), and periods (.) are allowed. The file or folder name cannot be **All** and cannot start or end with a hyphen or an underscore.

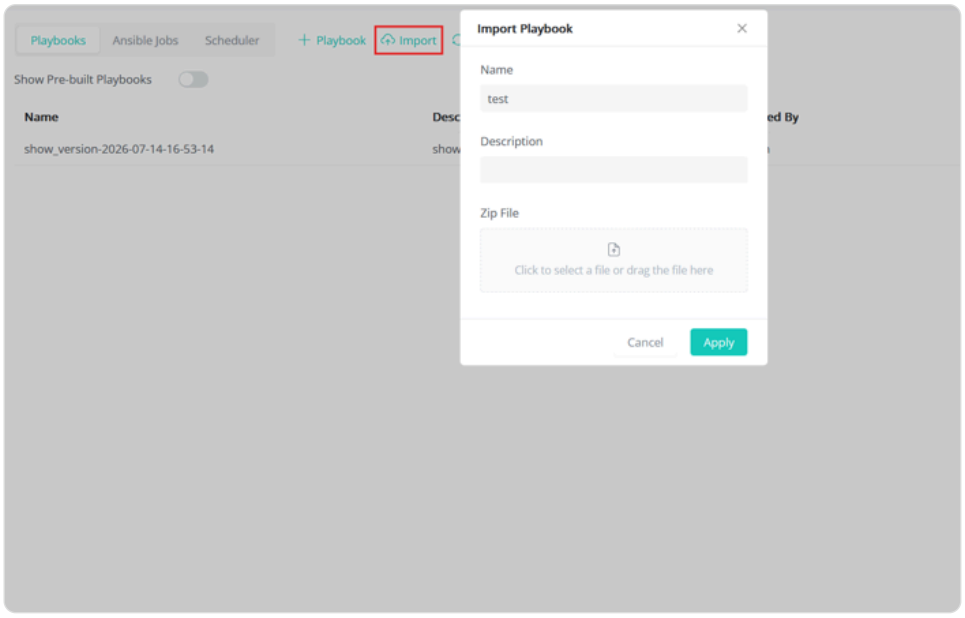
Importing a Playbook

If you have an available Ansible playbook YAML file, you can import it to AmpCon-Campus. Follow these steps:

1. Select a site to which the PicOS switches belong.
2. In the **Playbooks** tab, click **Import**.
3. In the pop-up window, enter the playbook name and description (optional).

NOTEs

- The playbook name must be unique.
- The playbook name can contain only letters, numbers, underscores (_), and hyphens (-) and supports a maximum of 64 characters. The name cannot start or end with a hyphen or an underscore.
- The playbook description can contain at most 128 characters.



4. Click the upload icon to upload a playbook .zip file, and then click **Apply**.

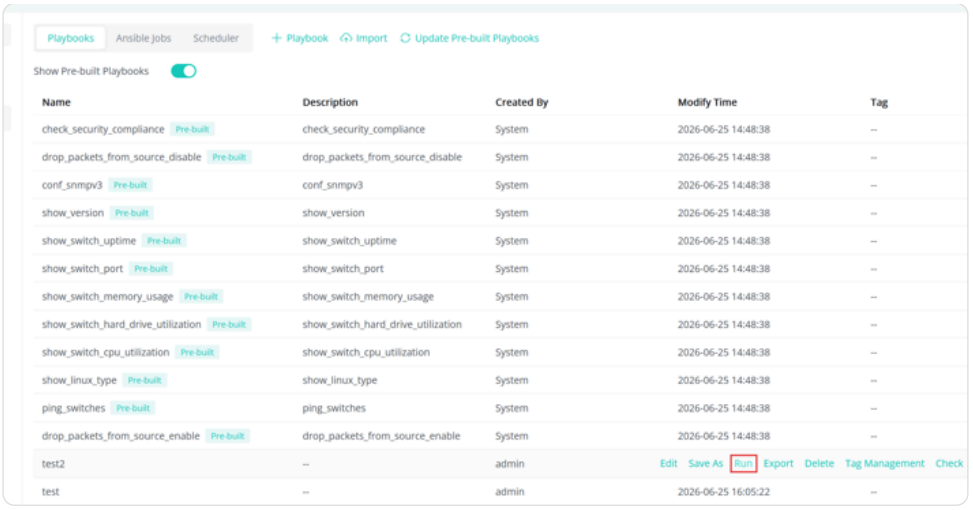
NOTEs

- The playbook .zip file must contain at least one playbook .yml file.
- All configurations in the .yml file must comply with Ansible playbook specifications.
- The .zip file size must not exceed 50 MB.
- The size of extracted contents must not exceed 200 MB.
- Each file within the .zip file cannot exceed 10 MB.
- The .zip file can contain a maximum of 500 files.

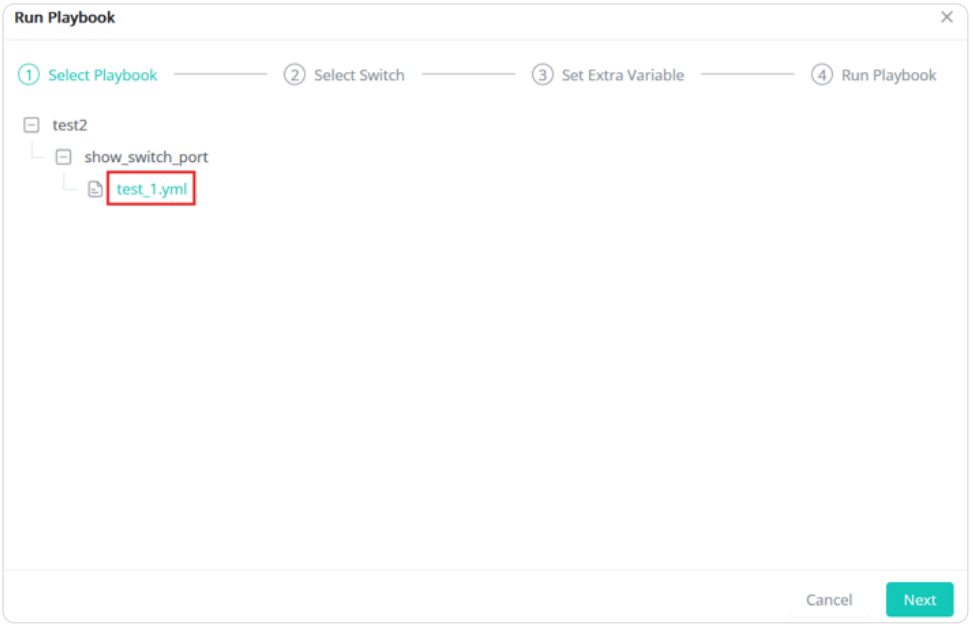
Running a Playbook

After writing or importing an Ansible playbook, run the playbook on target PicOS switches. Follow these steps:

1. In the **Playbooks** tab, hover over the playbook, and then click **Run**.

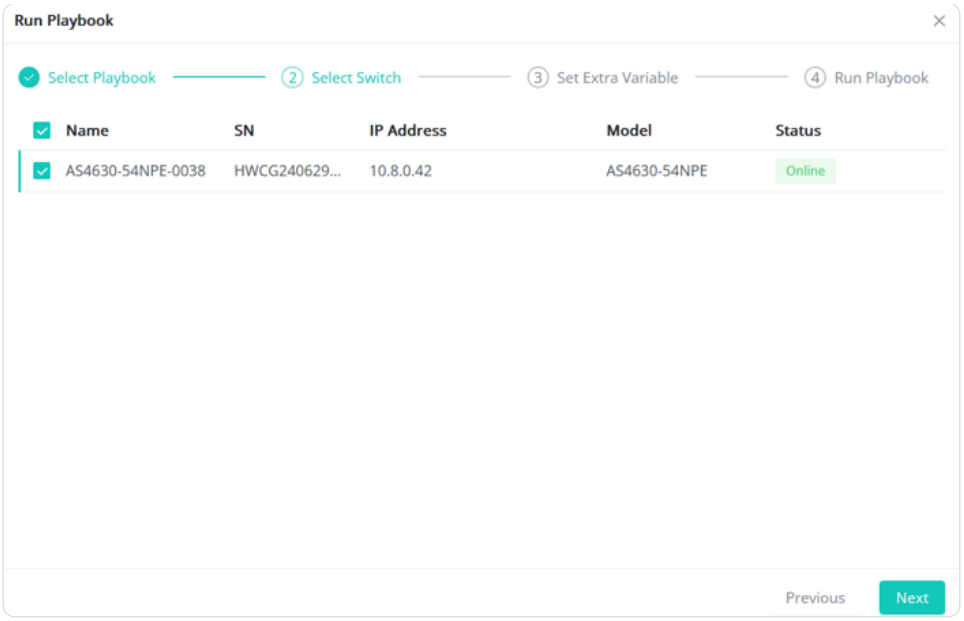


2. In the **Select Playbook** tab of the pop-up window, click the .yml file under the playbook name, and then click **Next**.



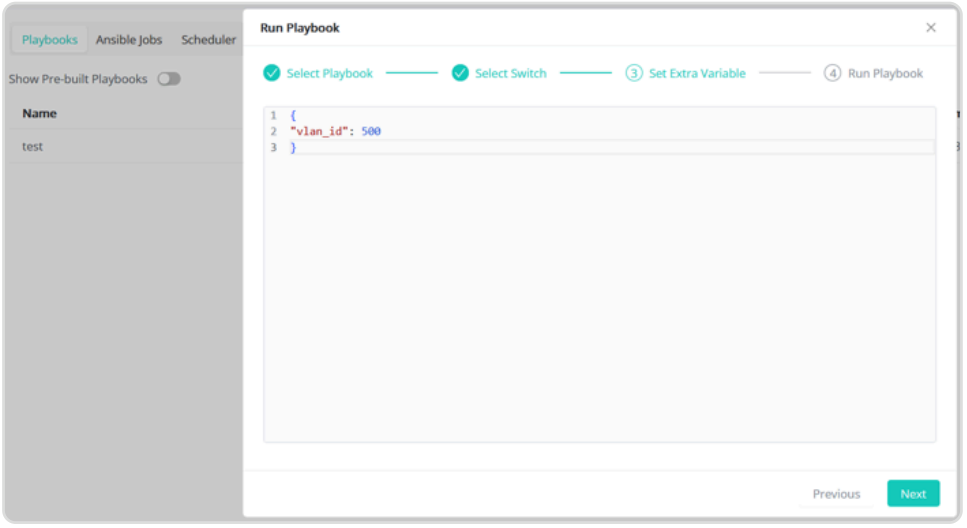
3. In the **Select Switch** tab, select one or multiple PicOS switches, and then click **Next**.

> **NOTEs**
>
> - Only the PicOS switches managed by AmpCon-Campus can be selected.
> - If a selected PicOS switch is offline (disconnected from AmpCon-Campus), the playbook execution will fail.



4. If variables are specified in the playbook, enter variable values in the **Set Extra Variable** tab, and then click **Next**. If not, click **Next** directly.

> **NOTE**
>
> The variable information must be in JSON format. Otherwise, the playbook cannot be run.

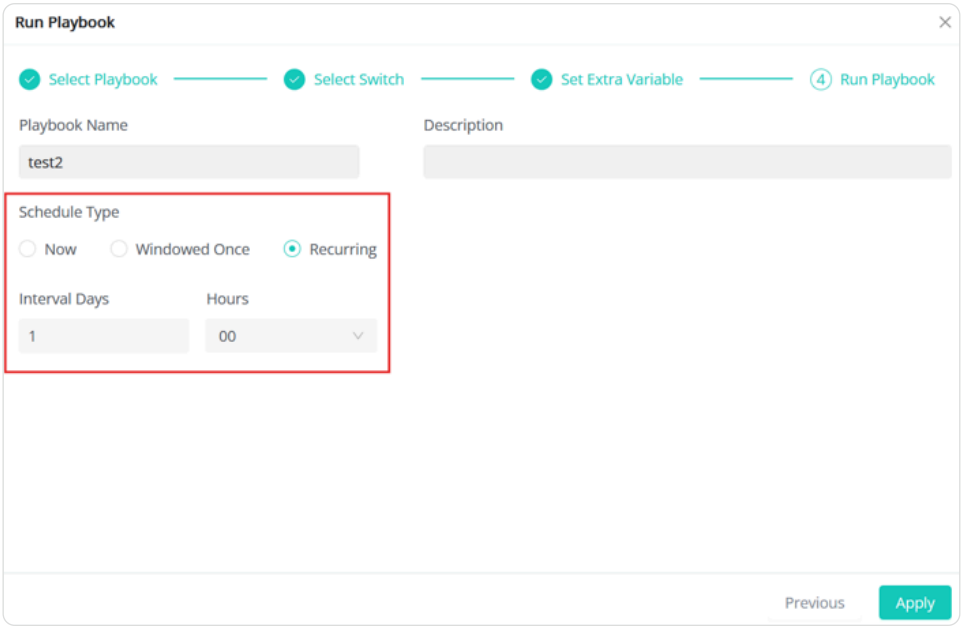


5. In the **Run Playbook** tab, select a playbook execution type.

- To run the playbook immediately, click **Now**.
- To run the playbook within a time range, click **Windowed Once**, and then select the start time and end time.

  The start and end times are displayed based on your browser's time zone. The start time cannot be earlier than the current time, and the end time must be at least two minutes after the start time.
- To run the playbook periodically at specified intervals (days and hours), click **Recurring**.

Then, enter an integer (1 to 31) in the **Days** field, and select an hour in the **Hours** drop-down list.



6. Click **Apply**. To check the playbook execution result, see Managing Ansible Jobs.

> **NOTE**
>
> If a playbook fails to be run on PicOS switches, check the possible reasons and solutions for troubleshooting. For more information, see Ansible Playbook Troubleshooting.

Optional Operations

Viewing the Playbook List

In the **Playbooks** tab, you can view the playbook list:

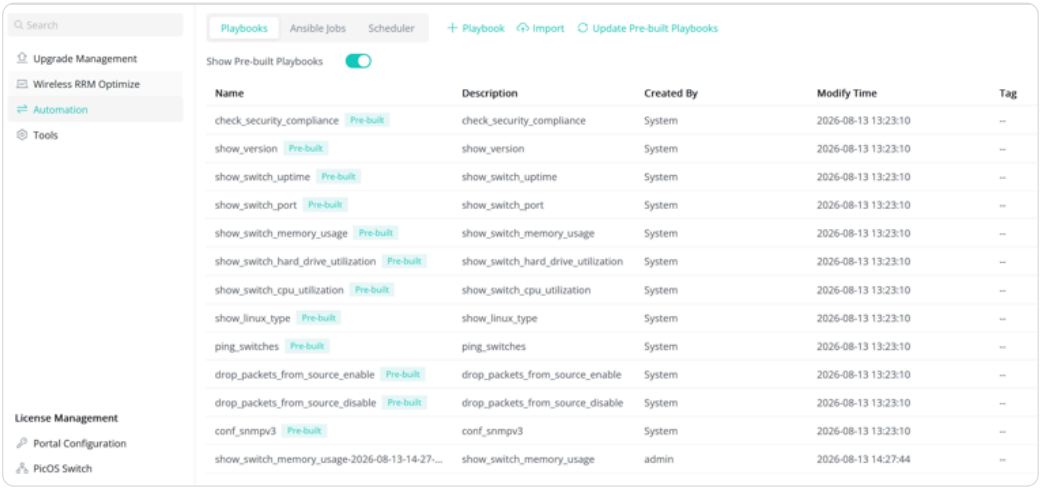


Table 2. Playbook Metrics

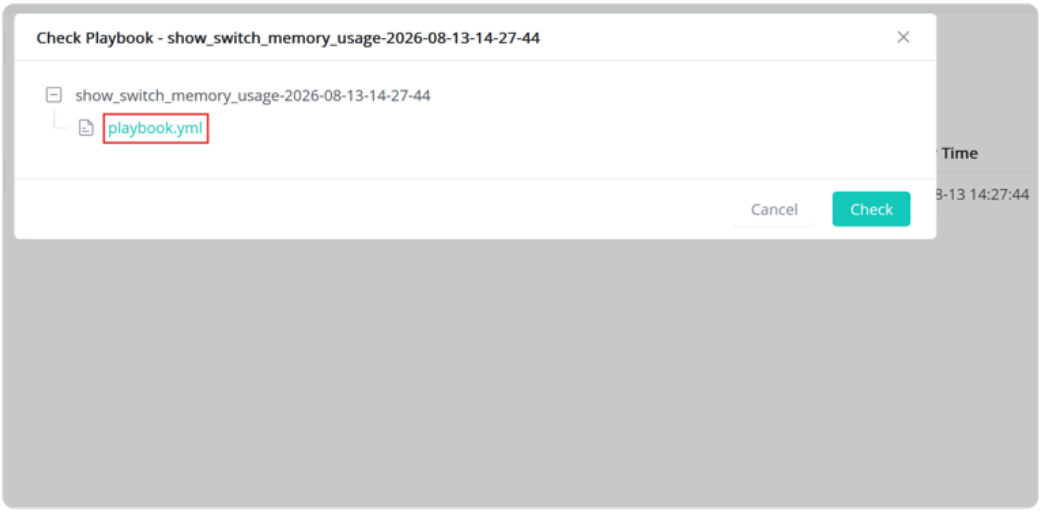
Metric	Description

Name	The playbook name.
Description	The description of the playbook.
Created By	The AmpCon-Campus user who created the playbook. **NOTEs** • The value is **System** for pre-built playbooks. • If the user who created the playbook is deleted from AmpCon-Campus, the value is highlighted with **(Deleted)**.
Modify Time	The last time the playbook was modified.
Tag	The tags added to the playbook.

Checking the Syntax for a Playbook

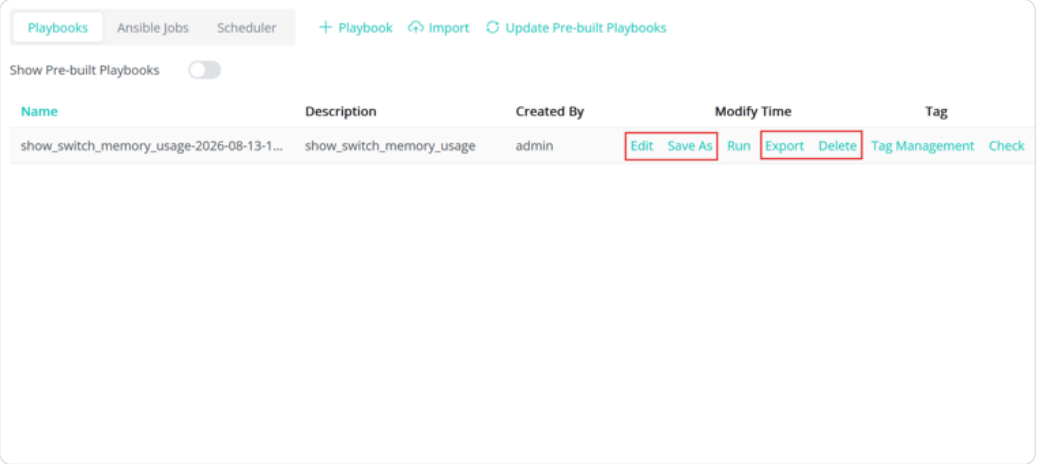
To check whether the syntax of a playbook is correct, hover over the playbook, and then click **Check**.

In the pop-up window, click the .yml file, and click **Check**. Then, you can see a message indicating whether the playbook is valid.



Editing, Deleting, Exporting, or Copying a Playbook

In the **Playbooks** tab, you can edit, delete, export, or copy playbooks.



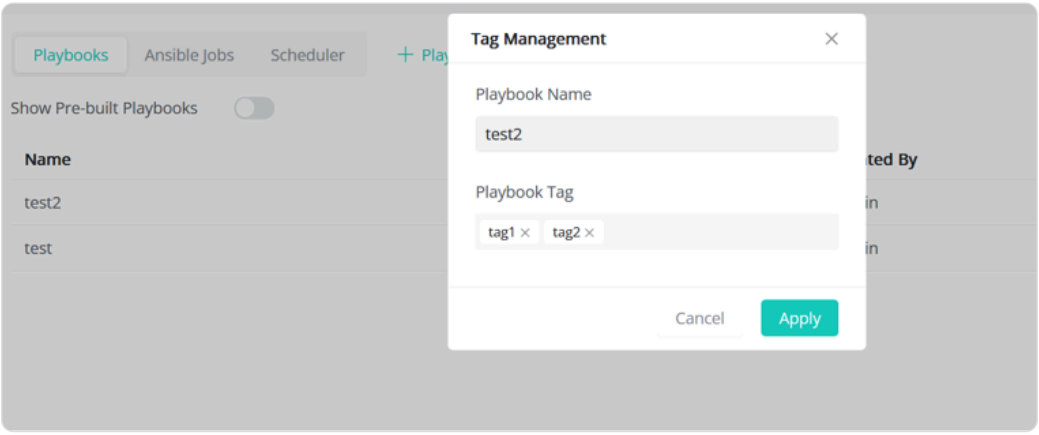
- To edit a playbook, hover over it, and then click **Edit**. In the pop-up window, modify the playbook as needed, and then click **Apply**.
- To delete a playbook, hover over it, and then click **Delete**. In the pop-up window, click **Yes**.
- To export a playbook, hover over it, and then click **Export**.
- To copy a playbook, hover over it, and then click **Save As**. In the **New Playbook Name** field, enter a new playbook name, and then click **Apply**.

Adding Tags

To add tags to a playbook, hover over the playbook, and then click **Tag Management**.

In the pop-up window, enter one or multiple tags in the **Playbook Tag** field, and then click **Apply**.

> **NOTEs**
>
> - Each time you enter a tag name, be sure to press **Enter**.
> - Each tag for the same playbook must be unique.
> - Each tag can contain only letters, numbers, underscores (_), and hyphens (-) and supports a maximum of 64 characters. Each tag cannot start or end with a hyphen or an underscore.



Managing Ansible Jobs

An Ansible job is a single execution of an Ansible playbook.

After you run Ansible playbooks, you can view the Ansible jobs and PicOS switches related to these playbooks. You can also check the execution results and output of these jobs.

Viewing Ansible Jobs
Viewing Switches

Viewing Ansible Jobs

1. Click the **Maintain** icon from the navigation bar, and then click **Automation** from the sidebar.
2. Click the **Ansible Jobs** tab. In the **Job View** section, view the list of Ansible jobs.

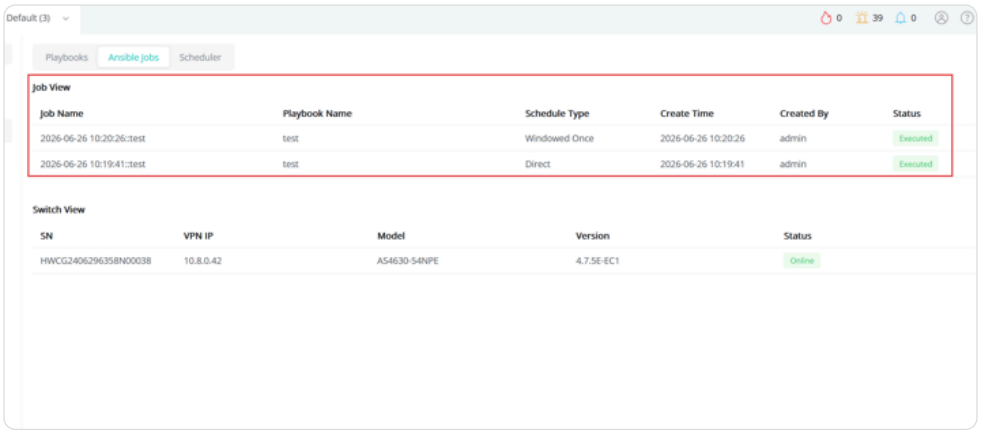


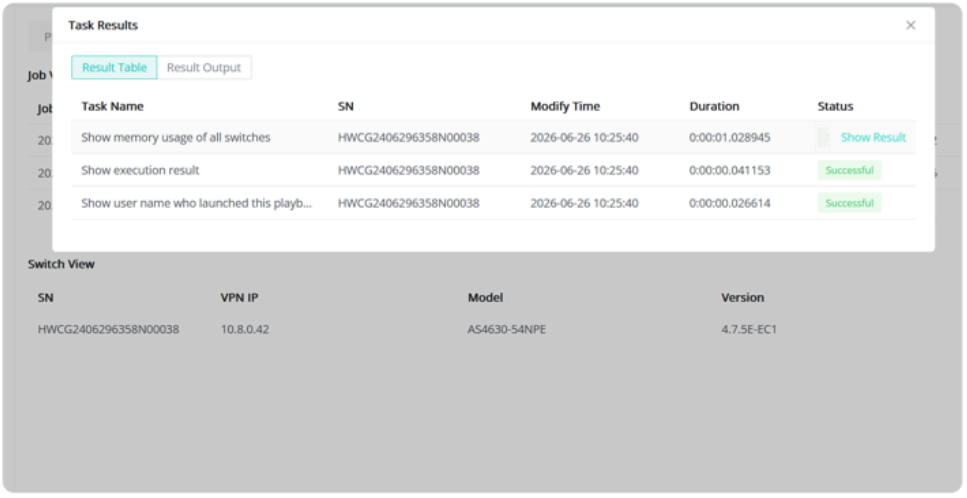
Table 1. Job View Metrics

Metric	Description
Job Name	The name of the Ansible job. The job name is automatically generated by AmpCon-Campus.
Playbook Name	The name of the playbook.
Schedule Type	The execution type of the Ansible playbook. • **Direct** is displayed if you select **Now** as the execution type when you run the playbook. • **Windowed Once** is displayed if you select **Windowed Once** as the execution type when you run the playbook.

	• **Recurring** is displayed if you select **Recurring** as the schedule type when you run the playbook.
Create Time	The time when the playbook was run.
Created By	The AmpCon-Campus user who run the Ansible playbook.
Status	The status of the Ansible job. • **Idle:** The playbook has not been executed. For playbooks with the schedule type of **Recurring**, the status is changed to **Idle** after the playbook is executed. • **Running:** The playbook is currently running. • **Executed:** The playbook execution has been completed. To check whether the playbook execution is successful, hover over the job, and click **Task Result**. • **Expired:** The **Windowed Once** type playbook is not run within its specified start and end time range.

3. Hover over an Ansible job, and then click **Task Result**.

- In the **Result Table** tab, you can see detailed tasks related to the Ansible job and each task execution status.



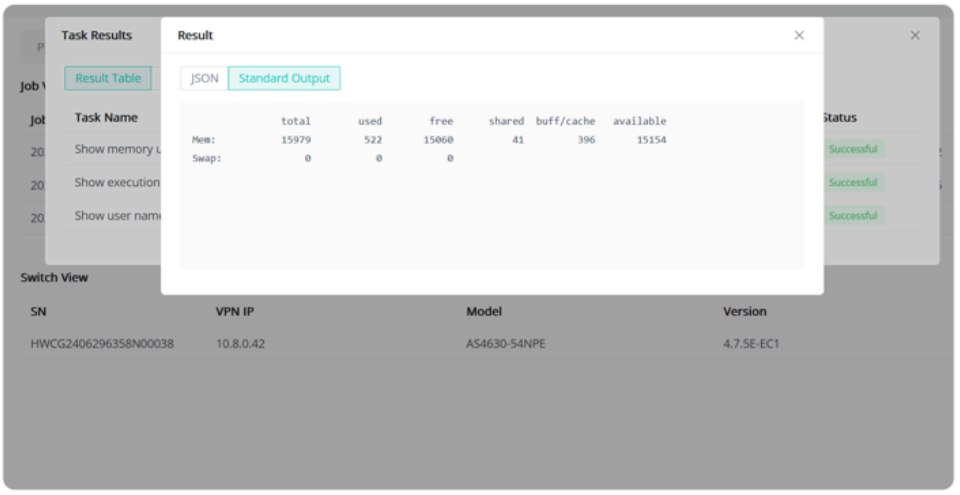
Tip

You might see the following task execution status:

- **Successful:** The task is executed successfully.
- **Failed:** The task fails to be executed.
- **Skipped:** The task is skipped by Ansible and thus not executed because the execution conditions are not met.
- **Unreachable:** The PicOS switch cannot be reached for reasons like SSH connectivity issues, SSH authentication failures, or network issues.

To view detailed result information for a task, hover over the task, and then click **Show Result**.

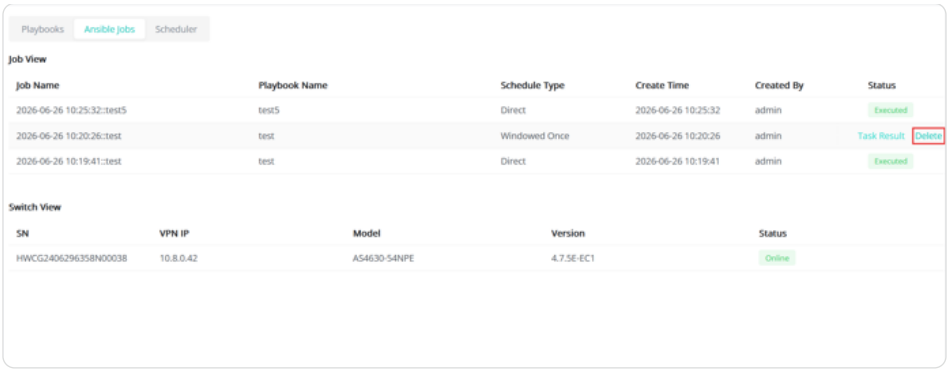
In the pop-up window, you can see the result information through the **JSON** and **Standard Output** tabs.



- In the **Result Output** tab, you can see the output of the playbook execution.



4. To delete an Ansible job, hover over it, and then click **Delete**. In the pop-up window, click **Yes**.



Viewing Switches

1. In the **Switch View** section, view the list of PicOS switches associated with Ansible jobs.

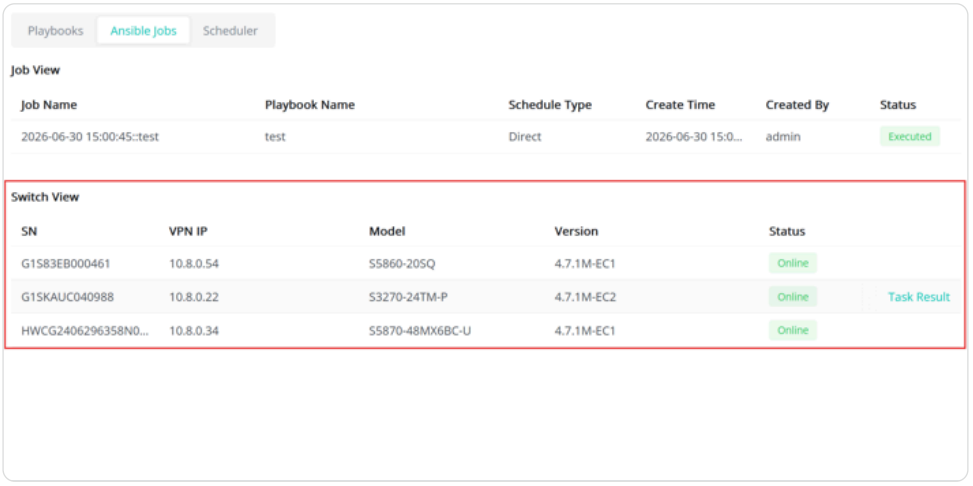
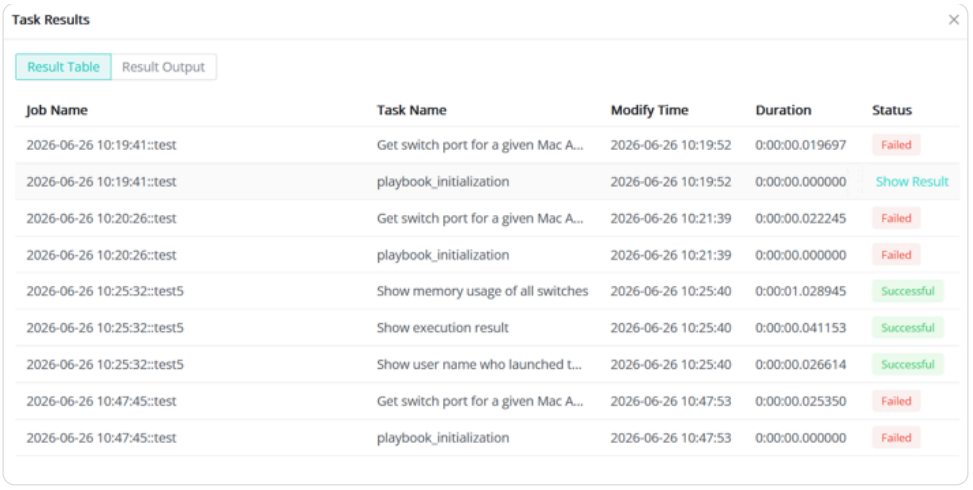


Table 2. Switch View Metrics

Metric	Description
SN	The serial number of the switch.
VPN IP	The VPN IP address of the switch.
Model	The model of the switch.
Version	The PicOS version of the switch.
Status	The status of the switch. • **Online:** The switch is connected to AmpCon-Campus. • **Offline:** The switch is disconnected from AmpCon-Campus.

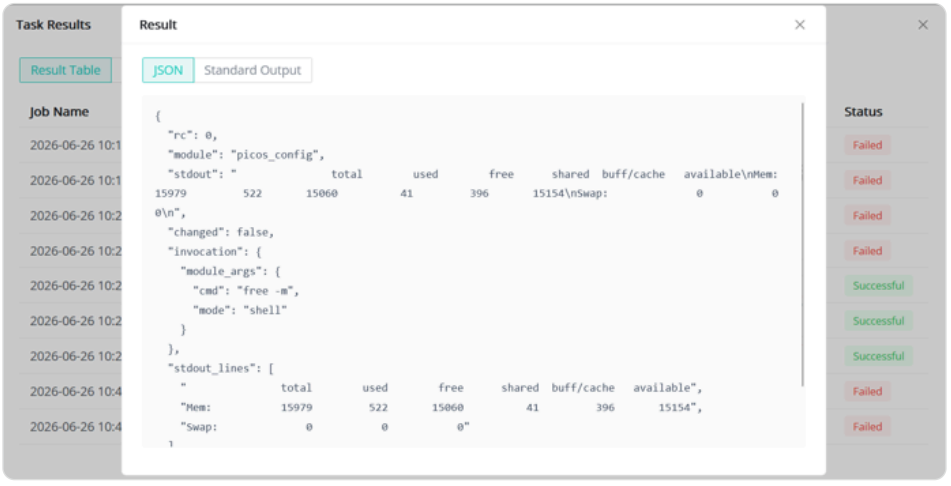
2. Hover over a switch, and then click **Task Result**.

- In the **Result Table** tab, you can see all Ansible jobs and tasks associated with the switch.



To view detailed result information for a task, hover over the task, and then click **Show Result**.

In the pop-up window, you can check the result information through the **JSON** and **Standard Output** tabs.



- In the **Result Output** tab, you can see the output of all Ansible tasks associated with the switch.

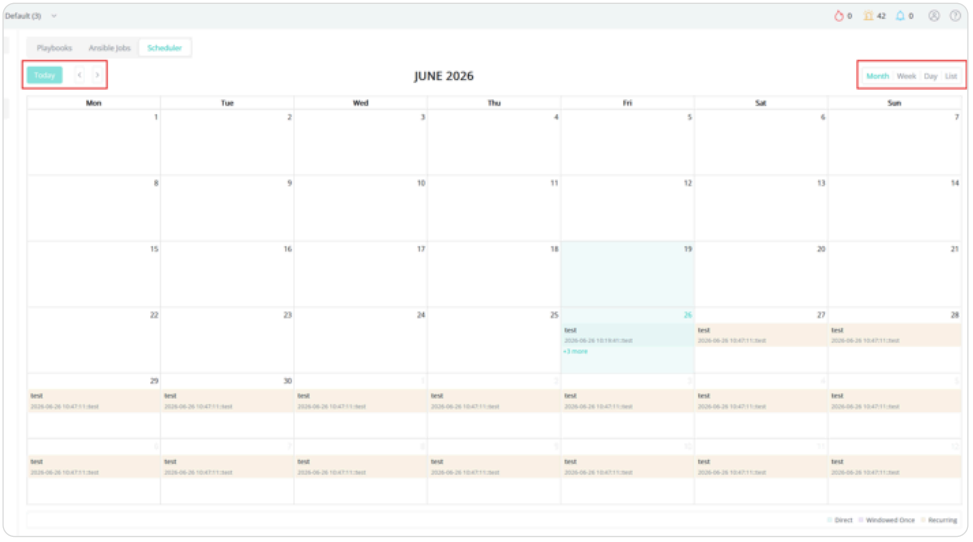


Viewing Playbook Schedules

On the “Scheduler” page, you can view playbook schedules in the calendar view or list view.

Procedure

1. Click the **Maintain** icon from the navigation bar, and then click **Automation** from the sidebar.
2. Click the **Scheduler** tab, and then view playbook schedules as follows:



- To view playbook schedules in the list view, click **List**.

  Click **<** to view playbook schedules in the previous week. Click **>** to view playbook schedules in the next week.

- If the current date does not fall within the displayed time window, click **Today** to jump to the view containing the current date.
- To view playbook schedules each month, click **Month**.

  Click **<** to view playbook schedules in the previous month. Click **>** to view playbook schedules in the next month.

- To view playbook schedules each week, click **Week**.

  Click **<** to view playbook schedules in the previous week. Click **>** to view playbook schedules in the next week.

- To view playbook schedules each day, click **Day**.

  Click **<** to view playbook schedules on the previous day. Click **>** to view playbook schedules on the next day.

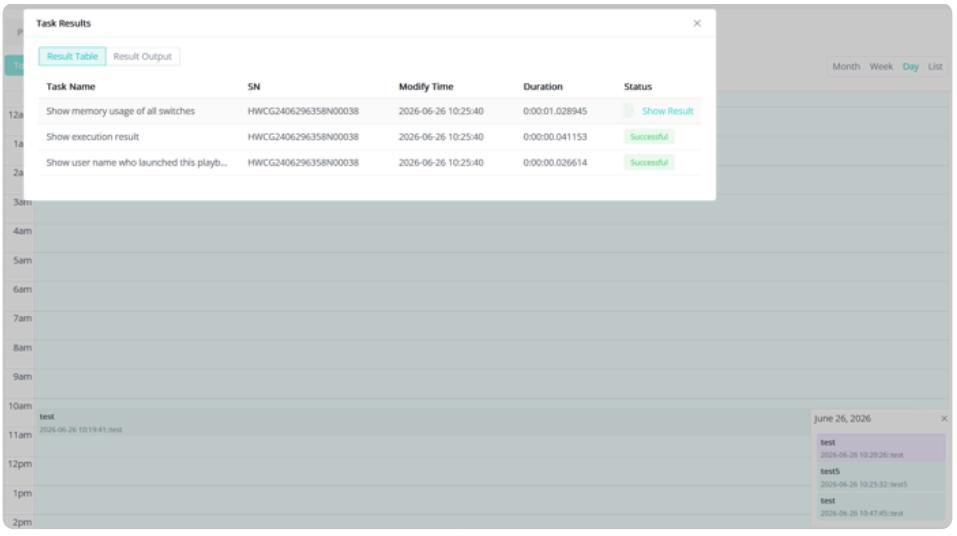
> **Tips**
>
> - Different types of playbooks are displayed in different colors.

- **Direct** playbooks are displayed in green.
- **Windowed Once** playbooks are displayed in purple.
- **Recurring** playbooks are displayed in yellow.

- If you click **Month** and multiple playbooks are displayed on the same day, you can see a button labeled **+3 More**. Click the button to see all remaining playbook schedules on the day.
- If you click **Week** or **Day** and multiple playbooks are displayed in the same hour, you can see a button labeled **+3**. Click the button to see all remaining playbook schedules in the hour.

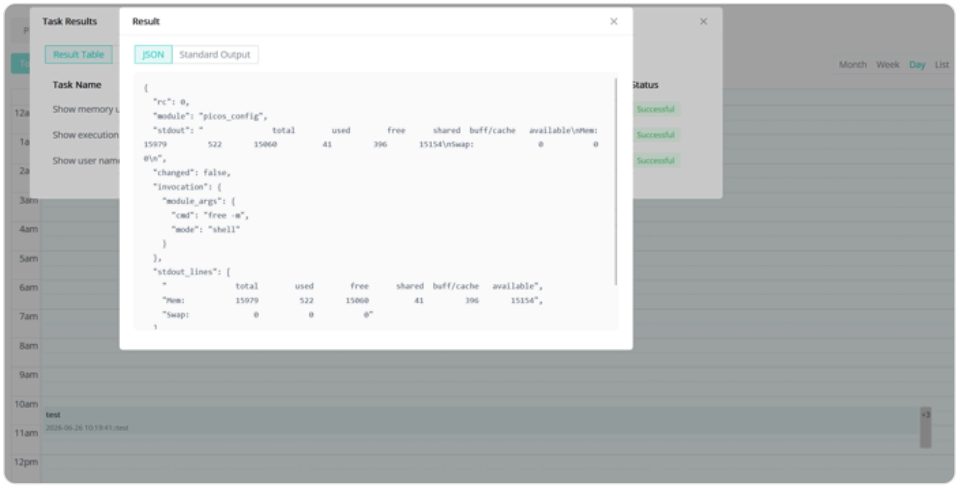
3. Click a playbook name to view the playbook execution result and output.

- In the **Result Table** tab, you can see detailed tasks for this Ansible job, along with the execution status of each task.

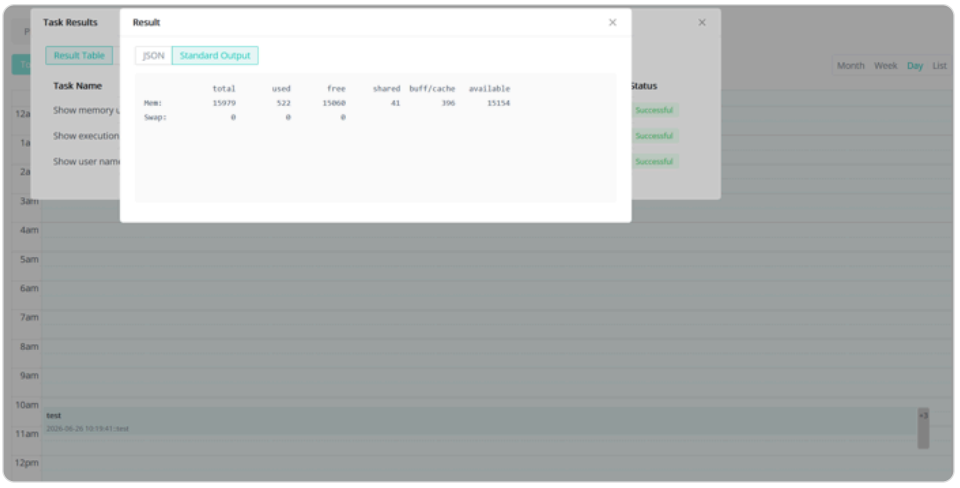


To view detailed result information for a task, hover over the task, and then click **Show Result**.

In the pop-up window, you can see the result information through the **JSON** and **Standard Output** tabs.



- In the **Result Output** tab, you can see the output of the playbook execution.



Accessing Devices through SSH

You can connect to a device (such as a switch or terminal device) from the AmpCon-Campus UI by establishing an SSH session. AmpCon-Campus provides device access flexibility and security by supporting two authentication modes: password authentication and SSH key authentication.

Use Cases
Password Authentication
SSH Key Authentication

Use Cases

- Password authentication is suitable for environments with lower security and higher usability demands.
- SSH key authentication provides stronger security for high-security scenarios.

  During password authentication, a password is transmitted over the network, which might expose passwords to interception. In contrast, the private key in SSH keys is uploaded to AmpCon-Campus and used to authenticate with the target device, reducing theft risk and enhancing session security.

Password Authentication

To access a device by using password authentication, follow these steps:

1. Click the **Maintain** icon from the navigation bar, and then click **Tools** in the left sidebar.
2. In the **SSH** tab, select **Password** in the **Select Authentication** section, and then input the following information:

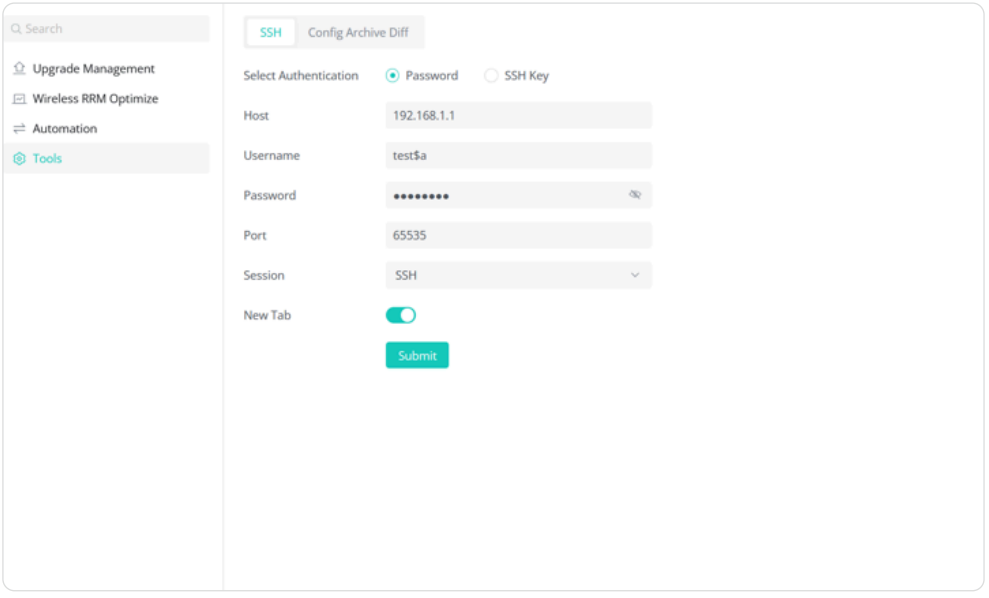


Table 1. Password Parameters

Parameter	Description
Host	The IPv4 or IPv6 address of the device.
User Name	The username to log in to the device. • The username can contain at most 32 characters. • Only ASCII characters are supported.
Password	The password of the user. Only ASCII characters are supported. **NOTE** Ensure the username and password are valid for device login. Otherwise, the SSH session cannot be established.
Port	The port used to establish the session. The port value must be between 1 and 65535.
Session	Select **SSH**.
New Tab	Toggle it on to view the SSH session in a new browser tab. Toggle it off to view the SSH session on the right side of the **SSH** tab.

3. Click **Submit**. Then, you can see the SSH session.

NOTE

The SSH session will fail in the following cases:

- The entered information above is incorrect.
- AmpCon-Campus cannot connect to the device due to network issues.

SSH Key Authentication

SSH keys consist of a public key and a private key. When you log in to the AmpCon-Campus UI and access a device through SSH keys, the session between AmpCon-Campus and the target device is authenticated by using the private key uploaded in the AmpCon-Campus UI and the public key stored on the device.

To access a device by using SSH key authentication, follow these steps:

Prerequisites

- On a server (for example, 10.56.xx.xx), run the **ssh-keygen** command to generate the SSH keys (including a public key and a private key).
- Put the generated public key in the **~/.ssh/authorized_keys** file of the device to be accessed. You can use the **scp** command. For example, run the following command on the device side.

  sudo scp pica8@10.56.xx.xx:/home/pica8/.ssh/id_rsa.pub /home/admin/.ssh/authorized_keys

  Then, the public key will be copied from the server 10.56.xx.xx to the device.

1. Click the **Maintain** icon from the navigation bar, and then click **Tools** in the left sidebar.
2. In the **SSH** tab, select **SSH Key** in the **Select Authentication** section, and then input the following information:

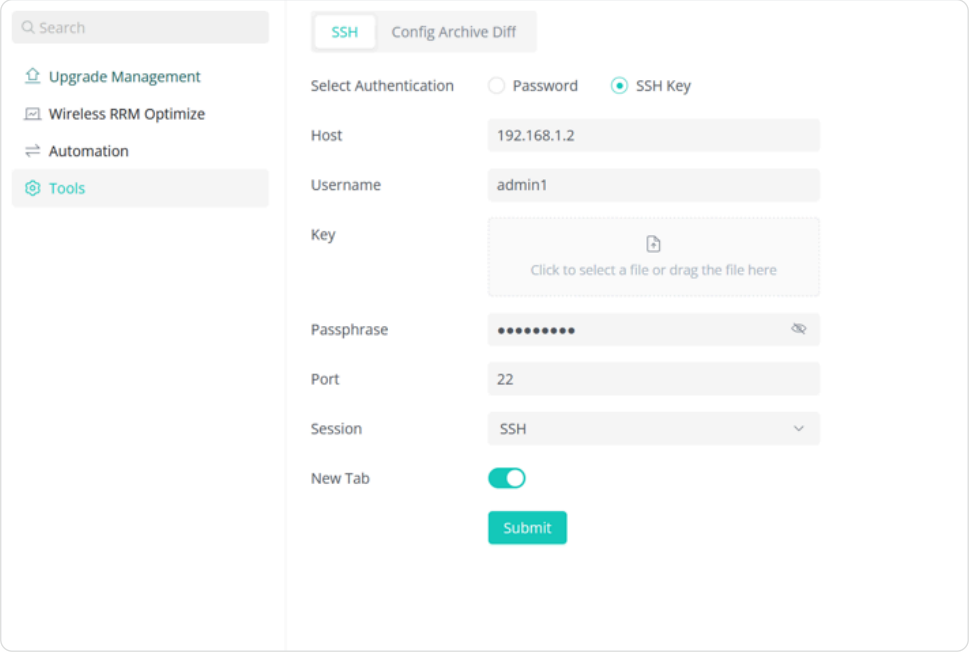


Table 2. SSH Key Parameters

Parameter	Description
Host	The IPv4 or IPv6 address of the device.
User Name	The username to log in to the device. • The username can contain at most 32 characters. • Only ASCII characters are supported.

Key	The private key file. Click the upload icon to upload the private key file, or drag and drop the private key file here. The size of the private key file cannot exceed 16 KB. **NOTE** Ensure the username and private key file are valid for device login. Otherwise, the SSH session cannot be established.
Passphrase	Optional. The password used to protect the SSH keys. You can choose whether to specify a passphrase when generating the SSH keys. If no passphrase was set during key generation, leave this field empty.
Port	The port used to establish the session. The port value must be between 1 and 65535.
Session	Select **SSH**.
New Tab	Toggle it on to view the SSH session in a new browser tab. Toggle it off to view the SSH session on the right side of the **SSH** tab.

3. Click **Submit**. Then, you can see the SSH session.

NOTE

The SSH session will fail in the following cases:

- The entered information above is incorrect.
- AmpCon-Campus cannot connect to the device due to network issues.

Monitoring

You can monitor real-time and historical metrics of devices in both wired and wireless networks. This eliminates the need to use multiple monitoring tools and helps you gain comprehensive insights into your networks.

See the following child topics:

- Dashboard
- Topology
- PicOS Switches
- FSOS Switches
- Access Points
- Clients

Dashboard

In the AmpCon-Campus UI, select a site, and then click the **Dashboard** icon from the navigation bar.

On the “Dashboard” page, you can get a global overview of managed devices, the AmpCon-Campus status, triggered alerts, and wireless networks.

- Managed Devices
- AmpCon-Campus Status
- Triggered Alerts
- Wireless Networks
  - Traffic and Client Trends
  - Top APs
  - Top STAs
  - Channel Utilization
  - Connections, Memory Usage, and AP Health

Managed Devices

At the top of the sidebar, you can see three device icons: switch icon, AP icon, and client icon.

Each device icon is followed by a number indicating the online device count for this device type within the selected site. If the switch icon or AP icon is highlighted with a red circle, it indicates some switches or APs are offline.

Hover over the switch or AP icon to view the count of all switches or APs and the count of offline switches or APs. Click the switch or AP icon to go to the “Devices” page.

Hover over the client icon to view the count of online clients. Click the client icon to go to the “Clients” page.



Tips

- The information is refreshed every 60 seconds.
- For a switch or an AP:
  - **Online** means the switch or AP is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus.
  - **Offline** means the switch or AP is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus.
- For a wireless or wired client:
  - **Online** means the client is connected to an AP or a switch.
  - **Offline** means the client is not connected to an AP or a switch.

AmpCon-Campus Status

In the section highlighted below, you can check the AmpCon-Campus status to ensure the platform is working. The information is refreshed every 60 seconds.



Table 1. AmpCon-Campus Information

Metric	Description
System Uptime	The time elapsed since the last time AmpCon-Campus was started.
Version	The version and revision of AmpCon-Campus. To view the AmpCon-Campus document site, click the document icon next to the version.
Server IP	The IP address of AmpCon-Campus. **NOTE** If the virtual machine or physical machine on which AmpCon-Campus is installed has multiple NICs, the specified NIC IP address is displayed here. If no NIC IP address is specified, the first NIC IP address is displayed here.
CPU Usage	The CPU utilization rate of AmpCon-Campus.
Memory Usage	The memory utilization rate of AmpCon-Campus.
Disk Usage	The hard disk utilization rate of AmpCon-Campus.

Triggered Alerts

Below the AmpCon-Campus status section, you can see three icons, which indicate firing Error alerts, firing Warning alerts, and unacknowledged Event alerts respectively.

Each icon is followed by the count of alerts of that type. Click these icons to view the full list of corresponding alerts.

In the **Recent Device Alerts** section, you can see unacknowledged Firing/Resolved/Event alerts that were triggered most recently. If an alert message is truncated, hover over the alert to display its complete content.

A maximum of six alerts can be displayed here. To view all alerts on the “Alerts” page, click **See All**. For more information, see Alerting.



Tips

- The information is refreshed in real time.
- A circle in red, yellow, or blue is displayed at the beginning of each alert entry. Different colors indicate different alert levels:
  - A **red** circle indicates an **Error Alert**.
  - A **yellow** circle indicates a **Warning Alert**.
  - A **blue** circle indicates an **Info Alert**.

Wireless Networks

You can see the following wireless network related information. The information is refreshed every 60 seconds.

Tips

- After an AP is moved from Site A to Site B, its traffic data will be reset and recalculated on the “Dashboard” page for Site B.
- If the AP is moved back to Site A, traffic statistics will resume based on its historical data for Site A.

Traffic and Client Trends

On the top right of the “Dashboard” page, you can see trend graphs of wireless traffic and client count within the selected site.

To display the trend of total wireless traffic, including RX traffic and TX traffic, select **Traffic** from the drop-down list.

To display the trend of RX traffic, select **RX Traffic** from the drop-down list.

To display the trend of TX traffic, select **TX Traffic** from the drop-down list.

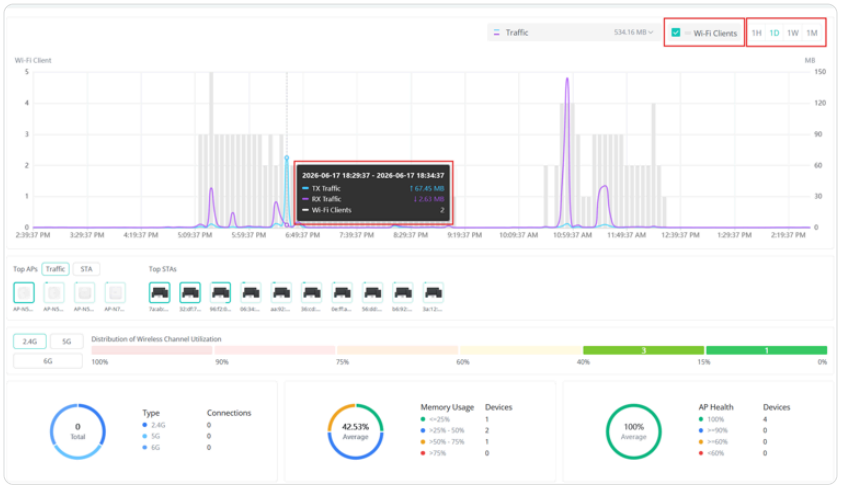
In the drop-down list, you can see the traffic volume of each traffic type.



To display the wireless client count trend, click the square before **Wi-Fi Clients**.

To check the traffic volume or wireless client count at a specific time point, hover over that time point.

To specify the trend display period, click **1H**, **1D**, **1W**, or **1M**, which represents the past 1 hour, 1 day, 1 week, or 1 month.

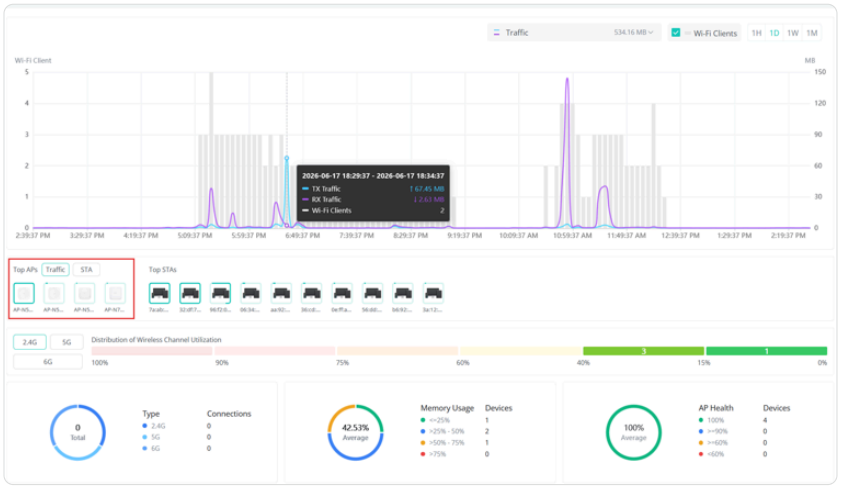


Top APs

In the **Top APs** section, you can see top 10 APs with the highest traffic or client count during the previously selected time period (**1H**, **1D**, **1W**, or **1M**).

To see top 10 APs with the highest traffic, click **Traffic**. The displayed APs are sorted by traffic volume.

To see top 10 APs with the highest client count, click **STA**. The displayed APs are sorted by wireless client count.



Hover over an AP. In the pop-up window, you can see the AP alias, the selected time period, TX traffic, RX traffic, the total traffic, and the wireless client count.

Click an AP, and then you can see the AP side panel. For more information, see Access Points.



Tips

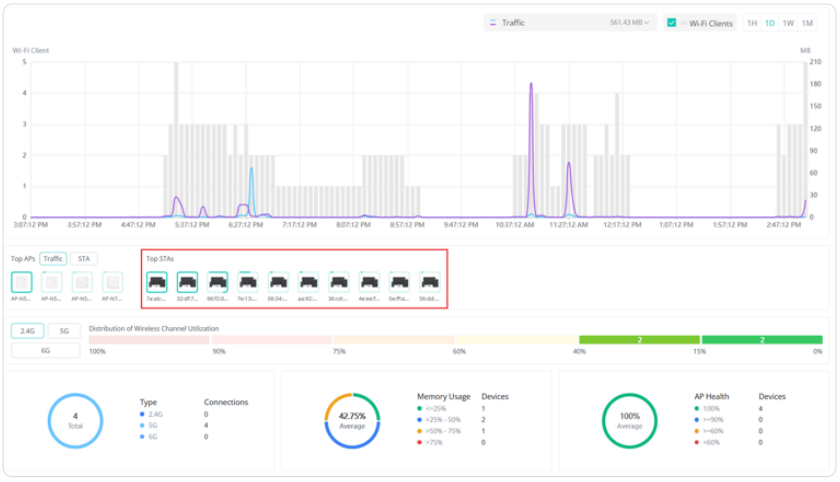
- When you hover over an AP, you might see its alias followed by **Moved** or **Deleted**, which means the AP has been moved to another site or deleted. You cannot click such an AP.
- When you hover over an AP that has been moved to another site, you can view the AP's current site in the pop-up window.
- If the selected site has less than 10 APs during the selected time period, all these APs are displayed here.
- Each AP is surrounded by a bar. The top-ranked AP displays a 100% full bar.

  For the 2nd-ranked AP, the bar length scales proportionally based on its value (total traffic or client count) relative to that of the top-ranked AP.

  The same rule applies to the 3rd-ranked AP and all subsequent APs. Their traffic bar length is determined by the ratio of their respective values (total traffic or client count) to the value of the top-ranked AP.

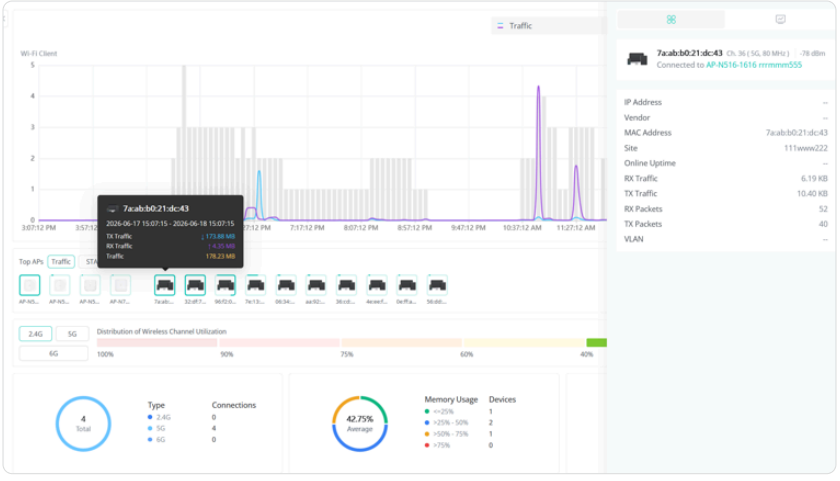
Top STAs

In the **Top STAs** section, you can see top 10 wireless clients with the highest traffic during the previously selected time period.



Hover over a wireless client. In the pop-up window, you can see the client name, the selected time period, TX traffic, RX traffic, and the total traffic.

Click a wireless client, and then you can see the client side panel. For more information, see Wireless Clients.



Tips

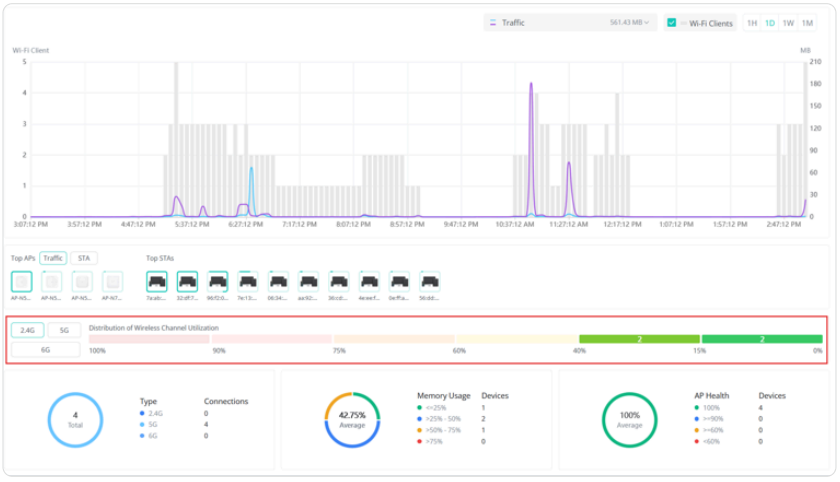
- If the selected site has less than 10 wireless clients during the selected time period, all these clients are displayed here.
- Each wireless client is surrounded by a bar. The bar proportion logic of clients is consistent with that of APs.

Channel Utilization

In the **Distribution of Wireless Channel Utilization** section, select the radio band, **2.4G**, **5G**, or **6G**.

Then, you can see 6 channel utilization ranges, along with the count of online APs whose current channel utilization (for the selected radio band) falls into each range. Different ranges are in different colors.

In the following screenshot, you can see 2 APs with current channel utilization ranging from 0% to 15%, and 2 APs with current channel utilization ranging from 15% to 40%.



For descriptions of channel utilization ranges, see the following table:

Table 2. Channel Utilization Range

Range	Level	Description
0%-15%	Idle	Extremely smooth in communication, with only Beacon frames and a minimal amount of data and without any interference.
16%-40%	Healthy	The optimal range and the most ideal load state for an enterprise network. Data transmission is smooth, with no jitter in voice and video conferences. The AP processing capacity is within its comfort zone.
41%-60%	Busy	Data services are operating normally, but real-time voice or video conferences might experience extremely slight jitter, and air interface collisions increase.
61%-75%	Congested	Web pages are loaded more slowly, and video conferences experience lag or a drop in video quality. The retry rate significantly increases, and the latency rises.

76%-90%	Saturated	The network is extremely slow with severe packet loss.
91%-100%	Unusable	The channel is completely occupied with extremely high noise levels or severe interference, making it almost impossible to transmit valid data.

Click a channel utilization range, and then you can see the APs whose current channel utilization rate falls into the range.

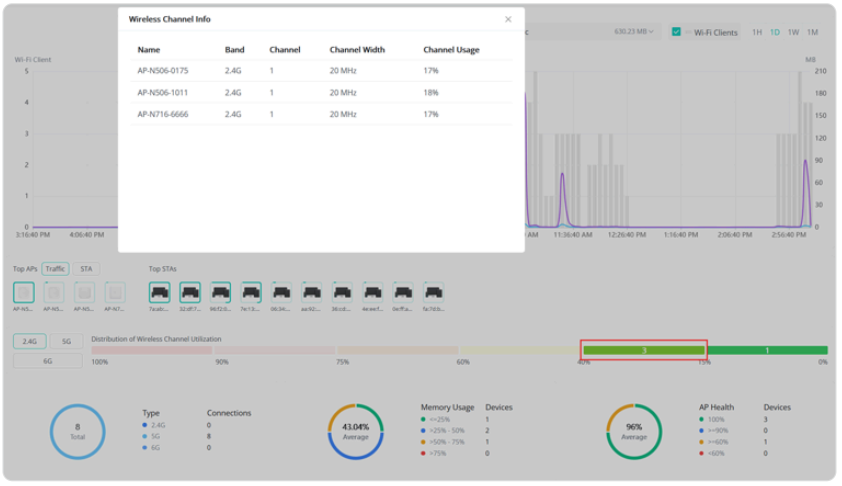


Table 3. Wireless Channel Information

Metric	Description
Name	The AP alias.
Band	The radio band, **2.4G**, **5G**, or **6G**.
Channel	The channel of the radio.
Channel Width	The channel width that the radio uses.
Channel Usage	The percentage of time the current channel is occupied by wireless signals (including data transmission and interference).

Connections, Memory Usage, and AP Health

On the lower right of the “Dashboard” page, you can see the following donut charts and real-time statistics:

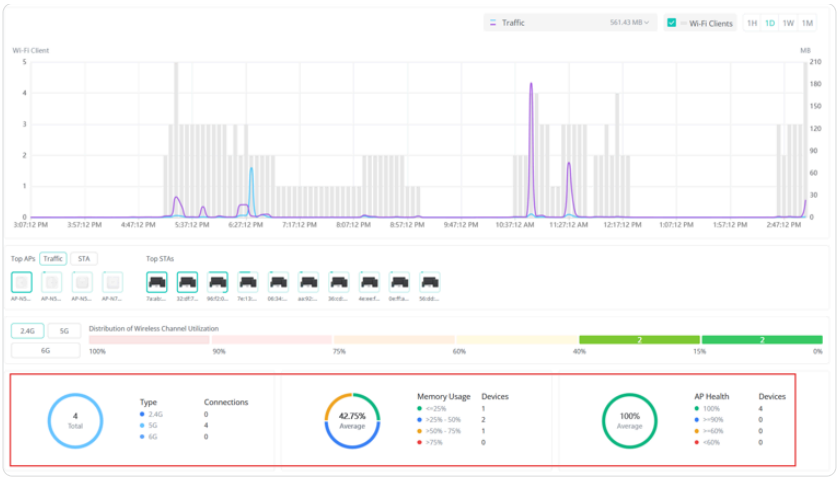


Table 4. Connections, Memory Usage, and AP Health

Metric	Description
Wireless Client Count	The count of online wireless clients associated with each radio band, and the total number of online wireless clients. **NOTEs** • **Online** wireless clients refer to wireless clients currently connected to managed APs within the selected site. • Hover over a segment of the donut chart. Then, you can see: ◦ The count of online wireless clients associated with this radio band. ◦ The percentage of online wireless clients associated with this radio band relative to all online wireless clients within the site.
Online AP Counts at Different Memory Utilization Levels	The count of online APs at different memory utilization levels, and the average memory utilization among all online APs. **NOTEs** • **Online** APs refer to APs currently connected to AmpCon-Campus within the selected site. • Hover over a segment of the donut chart. Then, you can see: ◦ The online AP count at this memory utilization level. ◦ The percentage of online APs at this memory utilization level relative to all online APs within this site.
Online AP Counts at Different Health Levels	The count of online APs at different health levels, and the average AP health among all online APs. **NOTEs**

- Hover over a segment of the donut chart. Then, you can see:
  - The online AP count at this health level.
  - The percentage of online APs at this health level relative to all online APs within this site.
- AmpCon-Campus calculates the health of an AP based on DHCP, DNS, RADIUS, and SSID health:

  AP Health = (1 - interfaces with errors / total interfaces) × 100 %

  In the following example, **2** interfaces have DNS issues, and the total number of interfaces is **4**. So, the **AP Health** is **50%**.

  AP Health = (1 - 2 / 4) × 100% = 50%



Interface	DHCP	DNS	RADIUS	SSID	Error
default	✓	✓	✓	✓	No
vlan10	✓	✗	✓	✓	Yes
vlan20	✓	✓	✓	✓	No
vlan30	✓	✗	✓	✓	Yes

Topology

In the AmpCon-Campus UI, select a site, and then click the **Topology** icon from the navigation bar.

On the “Topology” page, you can see real-time topologies of wireless and wired network devices (PicOS switches, APs, and clients) within the selected site. Topologies are refreshed every 60 seconds.

Prerequisites
Viewing Devices in a Topology
Filtering Devices in a Topology

Prerequisites

Ensure that the following prerequisites are met. Otherwise, the topology might fail to be displayed.

Table 1. Prerequisites

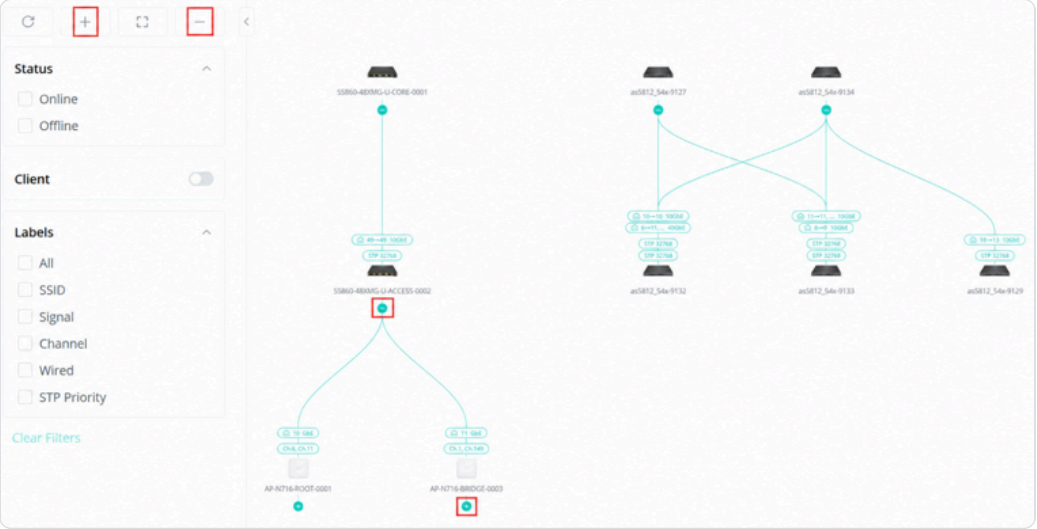
Prerequisite	Reference Link
PicOS switches and APs are successfully onboarded to AmpCon-Campus.	• Onboarding PicOS Switches • Onboarding APs
PicOS switches and APs are online (connected to AmpCon-Campus).	• Viewing the PicOS List
PicOS switches and APs belong to the correct site.	• Managing Sites
Link Layer Discovery Protocol (LLDP) is enabled on PicOS switches and APs.	• No reference link

Viewing Devices in a Topology

The first time you go to the “Topology” page, all PicOS switches and APs and their links appear in the topology, while clients and labels are hidden. To specify which devices and labels are displayed, see the Filtering Devices in a Topology section.

To zoom in on the topology, click the zoom-in icon. To zoom out of the topology, click the zoom-out icon. You can also zoom in or out of the topology by holding Ctrl and scrolling the mouse wheel.

To fold the devices connected to a switch or an AP, click the fold icon (**-**). To unfold the devices connected to a switch or an AP, click the unfold icon (**+**).



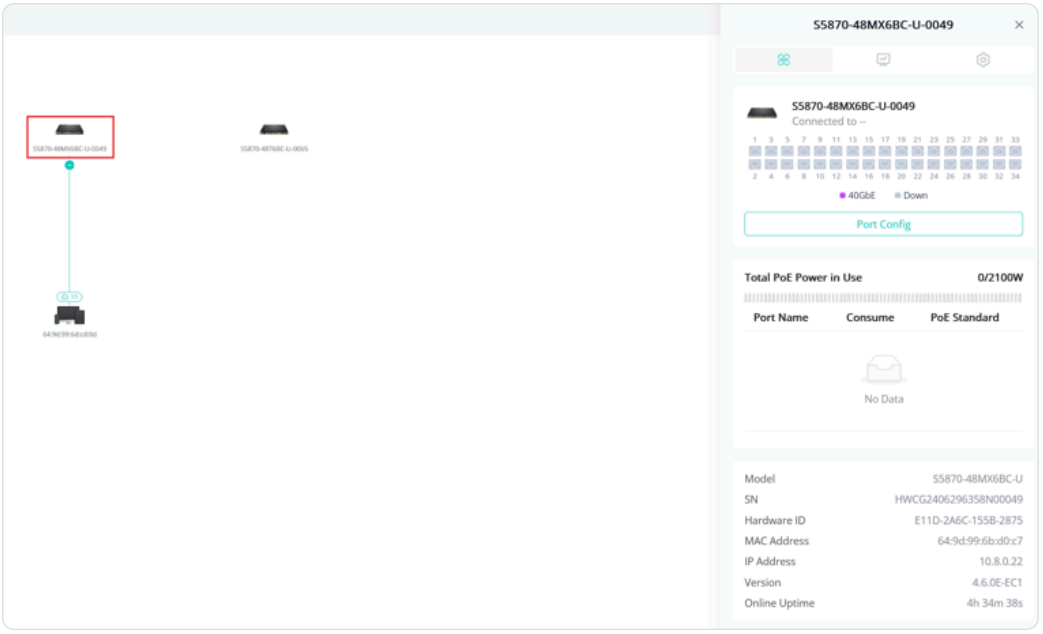
Tips

- PicOS switches, APs, and clients are displayed with different device icons.
  - For APs and PicOS switches listed on the “Devices” page, their aliases are displayed in the topology. For more information about the “Devices” page, see PicOS Switch List, FSOS Switch List, and AP List.
  - For clients, their hostnames are displayed in the topology. If AmpCon-Campus cannot retrieve their hostnames, their MAC addresses are displayed.
- PicOS switches and APs not in **Online** status are displayed in grey. Clients in **Offline** status cannot be displayed in the topology.
- Hover over an **Offline** PicOS switch or AP To view the last time the switch or AP was connected to AmpCon-Campus.
- If two devices are connected, the line between them is in green. If two devices are disconnected, the line between them is in grey.
- Solid lines are displayed for wired connections and dashed lines are displayed for wireless connections.
- If a switch fails to discover neighboring devices over LLDP but has learned multiple MAC addresses of connected devices, AmpCon-Campus creates a virtual device named **Third-Party Device** beneath the switch in the topology diagram.

  All devices corresponding to these MAC addresses are attached to this **Third-Party Device**.

To view detailed information of a device (PicOS switch, AP, or client), click the device in the topology. Then, you can see the device side panel on the right.

For more information about device details, see Monitoring - Access Points, Monitoring - PicOS Switches, and Monitoring - Clients.

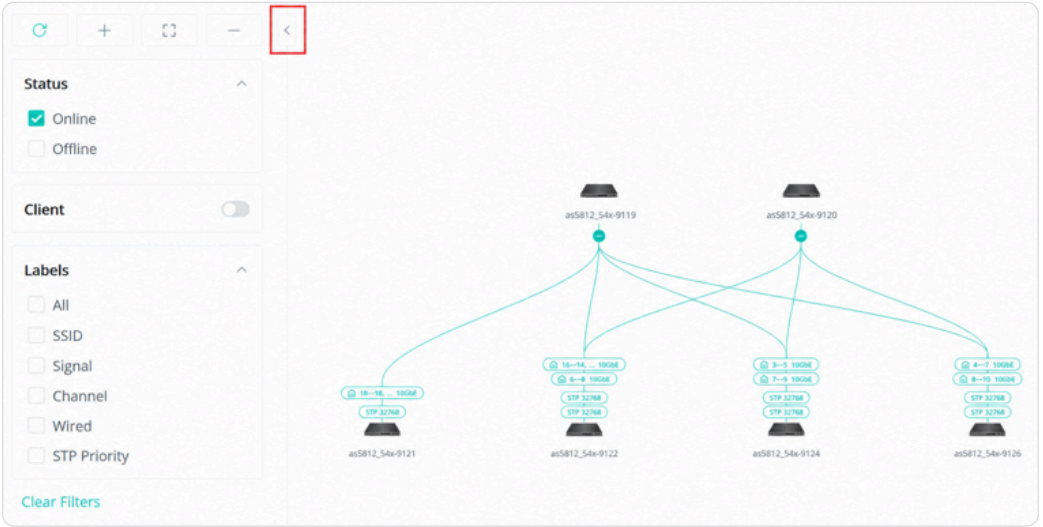


Tips

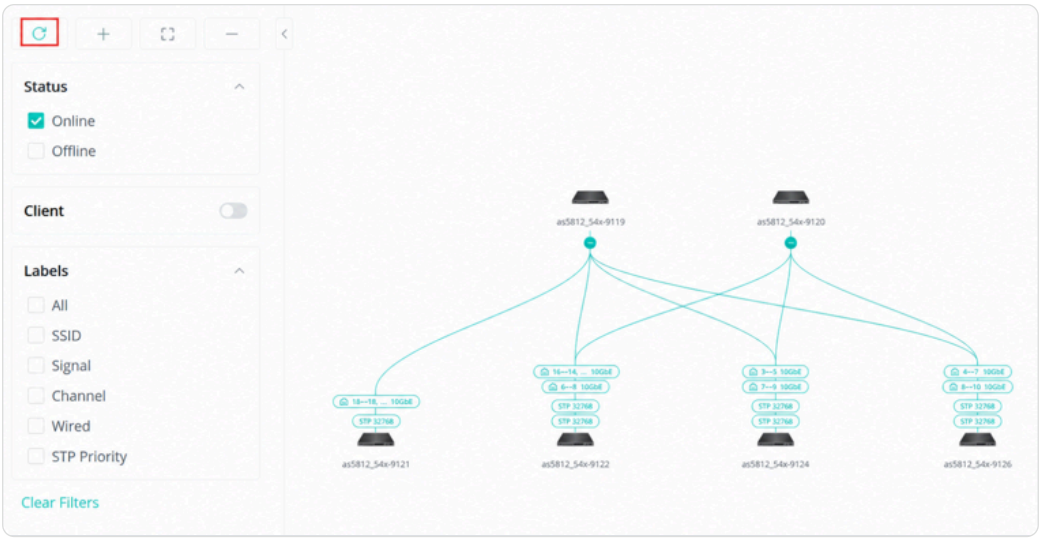
- PicOS switches and APs that have not been onboarded to AmpCon-Campus are displayed as client nodes in the topology. They share the same icon as clients and are collapsed by default.
- Some clients connected to a switch through **an intermediate device**. If the switch fails to discover **the intermediate device** over LLDP but has learned multiple MAC addresses of connected devices, AmpCon-Campus will create a virtual intermediate device in the topology.

  Clicking the virtual intermediate device does not open the side panel.

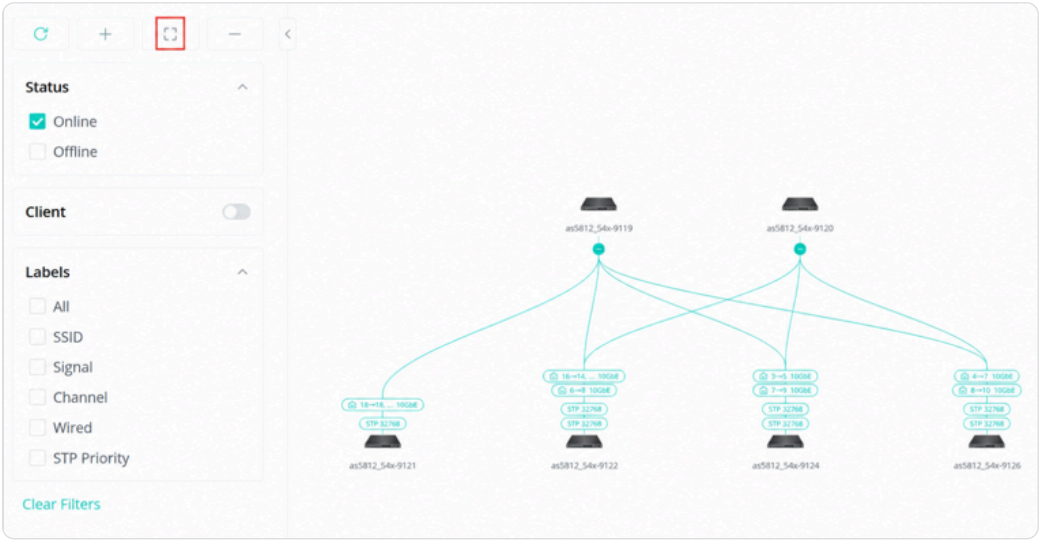
To hide the sidebar, click the left arrow. To display the sidebar, click the right arrow.



To change the topology layout orientation, click the rotation icon.



To automatically scale and center the topology within the current window, click the adaptive scaling icon.



Filtering Devices in a Topology

To specify which devices and labels are displayed, use the following methods:

- To display devices in **Online**, **Offline**, or both statuses, select **Online**, **Offline**, or both in the **Status** section. Selecting no options equals selecting all options.



Table 2. Device Statuses

Status	Description
Online	• For a PicOS switch or an AP, **Online** means the switch or AP is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus. • For a client, **Online** means the client is currently connected to an AP or a switch.
Offline	• For a PicOS switch or an AP, **Offline** means the switch or AP is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus. When you select **Offline**, you can also see the PicOS switches and APs that are listed on the “Devices” page but haven’t been onboarded to AmpCon-Campus. However, no connections will be displayed for these devices. • For a client, **Offline** means the client is not connected to an AP or switch.

- To display clients in the topology, toggle on **Client**. All clients are then selected automatically. You can select the client types to be displayed. Selecting no options equals selecting all options.

Click a client, and then you can see a side panel containing detailed information of the client.

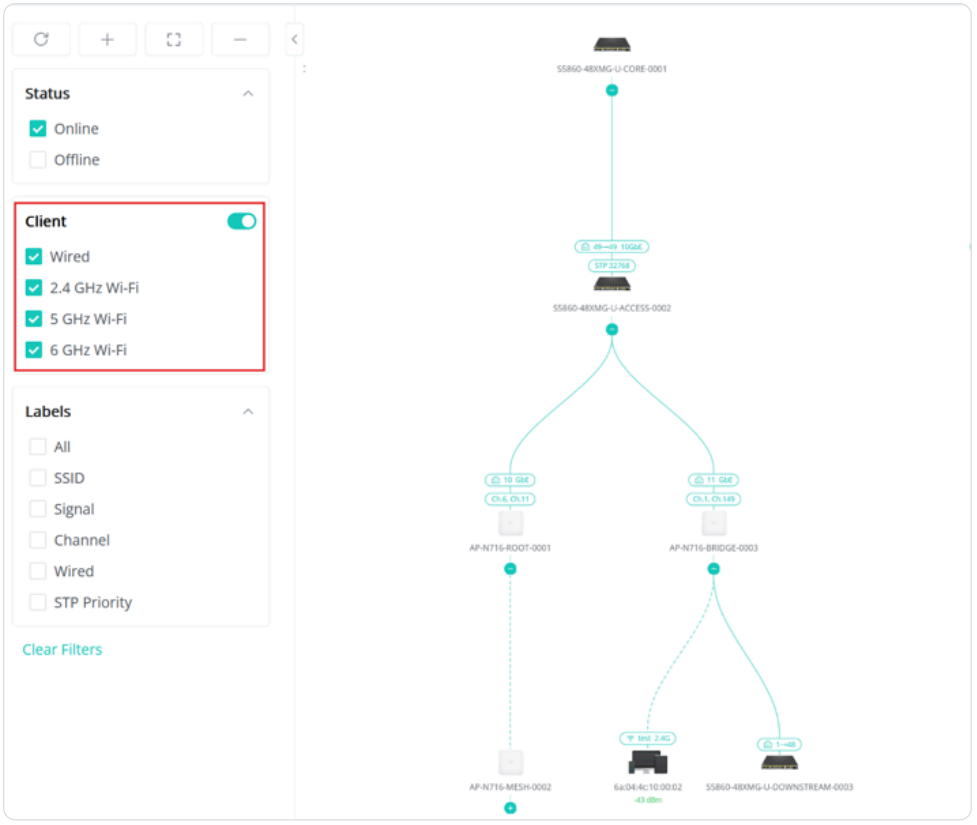


Table 3. Client Types

Option	Description
Wired	Displays wired clients connected to PicOS switches in this site.
2.4 GHz Wi-Fi	Displays wireless clients connected to APs in this site through the 2.4 GHz radio band.
5 GHz Wi-Fi	Displays wireless clients connected to APs in this site through the 5 GHz radio band.
6 GHz Wi-Fi	Displays wireless clients connected to APs in this site through the 6 GHz radio band.

> **Tip**
>
> If you don't need to display clients in the topology, toggle off **Client**.

- To specify the labels to be displayed in the topology, select one or multiple labels in the **Labels** section. To select all labels, click **All**. Selecting no options equals selecting all

options.

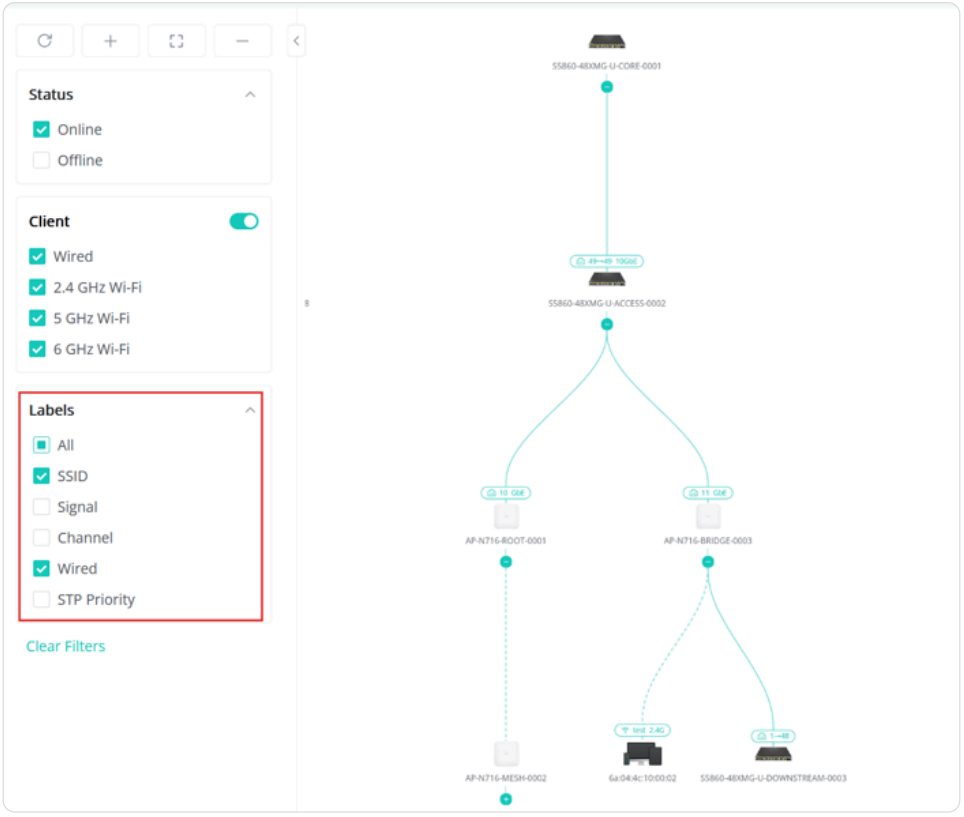
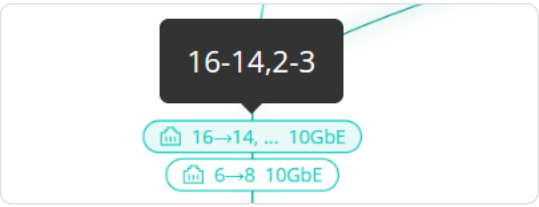


Table 4. Labels

Label	Description
SSID	Displays the Service Set Identifier (SSID) and radio band to which a wireless client connects. An SSID is the logical name of a wireless network.  **NOTE** The label is displayed only for wireless clients currently connected to an AP.
Signal	Displays the Received Signal Strength Indicator (RSSI) of a wireless client. RSSI is used to indicate the strength of signals. Normally, the RSSI value is a negative number. The closer to 0, the stronger the signal.

	 **NOTE** The label is displayed only for wireless clients currently connected to an AP.
Channel	Displays the radio channels that the AP uses. Each channel is a sub-division within a radio band for transmitting and receiving wireless signals. 
Wired	For two connected PicOS switches, the port numbers of the upstream switch and downstream switch and the port speed are displayed. For clients or APs connected to a switch, the switch port number and the port speed are displayed.  **NOTEs** • If a device is connected to two switches, hover over the label value to identify the upstream switch. The upstream switch will be highlighted. • If the label value contains **...**, hover over the value to see the full information.
STP Priority	Displays the STP priority of the link.  **NOTE**

The label is displayed only for links with STP enabled.

- To clear all the filter conditions above, click **Clear Filters**.

PicOS Switches

After onboarding PicOS switches to AmpCon-Campus, you can continuously monitor the switches for performance analysis and fault diagnosis.

See the following child topics:

- PicOS Switch List
- Basic Information of a PicOS Switch
- Deep Insights into a PicOS Switch
- Configurations and Operations of a PicOS Switch

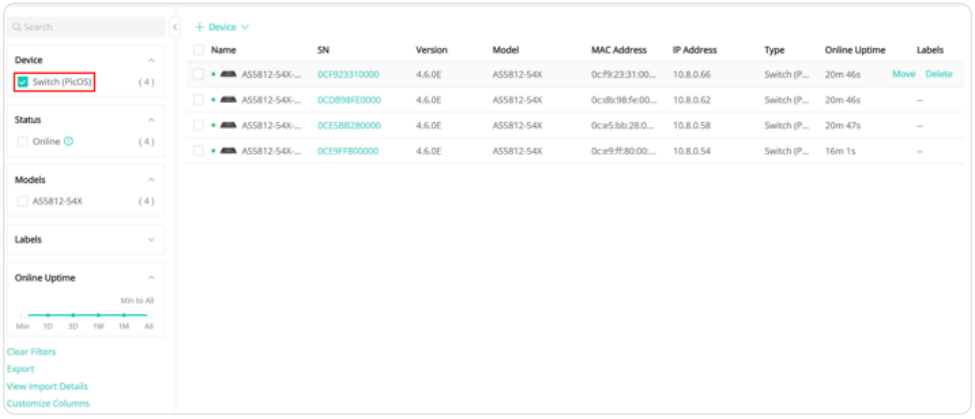
PicOS Switch List

On the “Devices” page, you can view the list of PicOS switches that fail to be onboarded, are being onboarded, or have already been onboarded to AmpCon-Campus.

Viewing the PicOS List
Filtering PicOS Switches
Exporting PicOS Switches

Viewing the PicOS List

1. In the AmpCon-Campus UI, select the site to which the PicOS switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, you can see all PicOS switches, FSOS switches, and access points (APs).
3. In the **Device** section of the sidebar, select **Switch (PicOS)** to display only PicOS switches.



By default, the following metrics are displayed:

Table 1. PicOS Switch Metrics

Metric	Description
Name	The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side. If you do not enter an alias, AmpCon-Campus automatically generates an alias for each device. The alias contains the device model and the last four digits of the switch serial number (SN). **NOTE** Pay attention to the color of the circle in the **Name** column. Different circle colors indicate different statuses:

	• **Green:** The switch is in **Online** status, which means the switch is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus. • **Grey:** The switch is in **Offline** status, which means the switch is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus. • **Yellow:** The switch is in **Never Online** status, which means the switch has been added to AmpCon-Campus but has never connected to AmpCon-Campus. • **Blue:** The switch is in **Provisioning** status, which means AmpCon-Campus is verifying authentication information of the switch or establishing an OpenVPN tunnel with the switch. • **Red:** The switch is in **Failed** status, which means the switch fails to be onboarded to AmpCon-Campus.
SN	The serial number of the switch.
Version	The PicOS version of the switch.
Model	The model of the switch.
MAC Address	The MAC address of the switch.
IP Address	The VPN IP address of the switch. **NOTE** After a PicOS switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between AmpCon-Campus and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-Campus and the switch will communicate through the VPN tunnel.

Type	The type of the switch. For PicOS switches, the type is **Switch (PicOS)**.
Online Uptime	The elapsed time since the switch last connected to AmpCon-Campus. Hover over the time to view the switch's last connection time to AmpCon-Campus.
Labels	The labels of the switch.

4. To view more PicOS switch metrics, click **Customize Columns** in the sidebar, select or deselect metrics in the pop-up window, and then click **Done**.

   In addition to the metrics above, you can select the following metrics:

   Table 2. Additional PicOS Switch Metrics

Metric	Description
Hardware ID	The hardware ID of the switch.
Backup Schedule	The backup schedule of the switch.
Site	The site to which the switch belongs.
Memory	The memory usage of the switch.
Temp	The temperature of the switch.
Last Upgrade	The last time when the switch was upgraded.

Tips

- The **Name**, **SN**, and **Model** columns cannot be deselected.
- To display only the default metrics, click **Restore**, and then click **Done**.
- You can select other metrics such as **AP Health** and **Load**, but their values appear as **--** for PicOS switches. This is because these metrics apply only to access points (APs).

Filtering PicOS Switches

On the “Devices” page, you can filter PicOS switches by status, model, label, or online uptime.

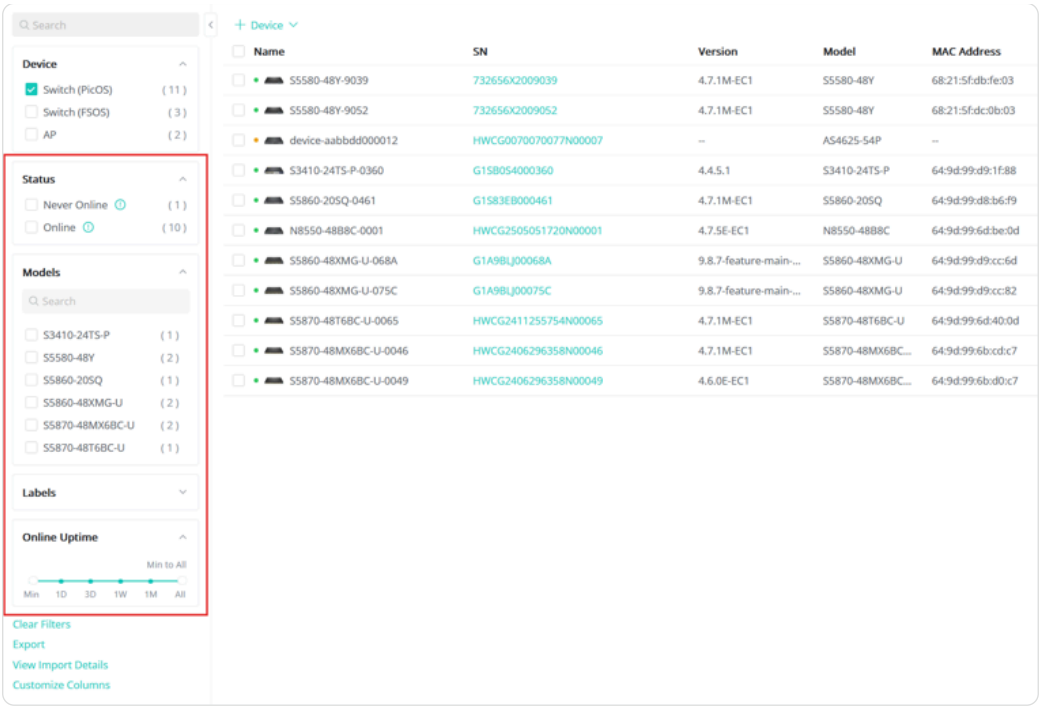


Table 3. Filter Sections

Filter Section	Description
Status	Select one or multiple switch statuses.
Models	Select one or multiple switch models.
Labels	Select one or multiple labels.
Online Uptime	**Online Uptime** means the continuous online duration of the switch. Select a time range in the **Online Uptime** section by clicking a start and end time point. The following time points can be clicked: • **Min** means the current time. • **1D** means 1 day. • **3D** means 3 days. • **1W** means 1 week. • **1M** means 1 month. • **All** means all times. **Examples:** • If you select the time range as **Min** to **All**, all switches are displayed. • If you select the time range as **Min** to **1D**, only online switches whose **Online Uptime** is less than or equal to

1 day are displayed.

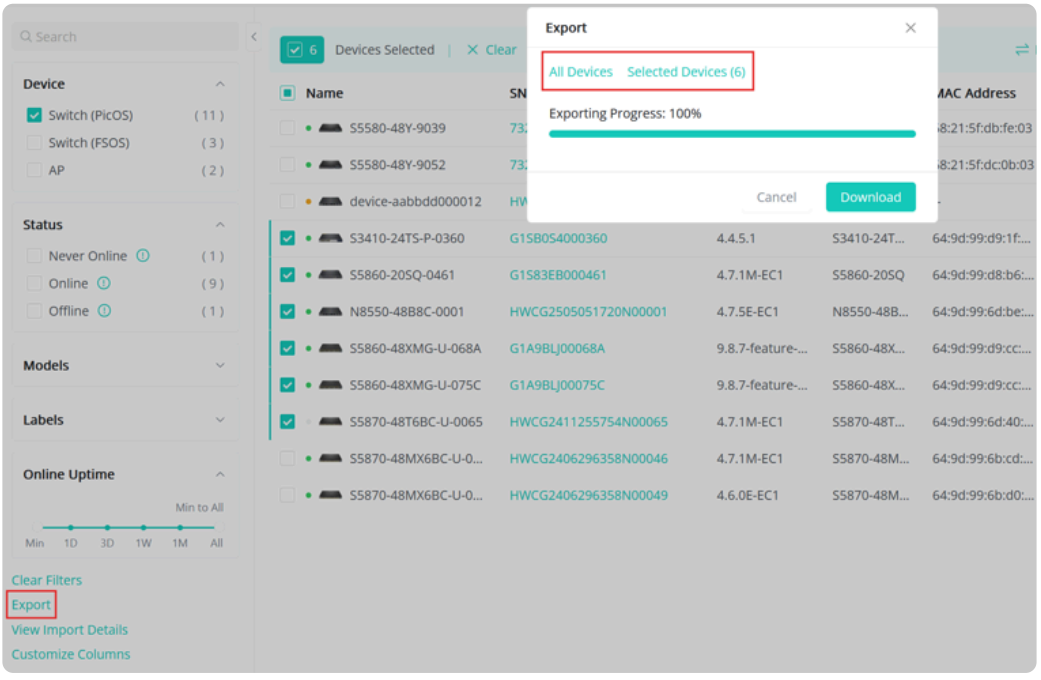
- If you select the time range as **3D** to **1M**, only online switches whose **Online Uptime** is between 3 days and 1 month are displayed.
- If you select the time range as **1W** to **All**, only online switches whose **Online Uptime** is greater than or equal to 1 week are displayed.

Tips

- If no devices match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of devices that match the filter option.
- To clear all these filter options, click **Clear Filters**.

Exporting PicOS Switches

On the “Devices” page, you can export PicOS switches to a .csv file:



- To export all PicOS switches, click **Export**. In the pop-up window, click **All Devices**, wait for the export to complete, and then click **Download**.
- To export specific PicOS switches, select the switches in the device list, and then click **Export**. In the pop-up window, click **Selected Devices**, wait for the export to complete, and then click **Download**.

Tip

To clear the switch selection, click **Clear**.

Basic Information of a PicOS Switch

Click the **Devices** icon from the navigation bar. On the “Devices” page, click a PicOS switch. You can see a side panel on the right.

In the **Overview** tab of the side panel, you can view basic information about the switch.

Guidelines
Basic Switch Information

Guidelines

- AmpCon-Campus can monitor only the PicOS switches that have been successfully onboarded.
- Some data in the **Overview** tab might not be displayed for offline PicOS switches (switches disconnected from AmpCon-Campus).

Basic Switch Information

For displayed data in the **Overview** tab, see the following table:

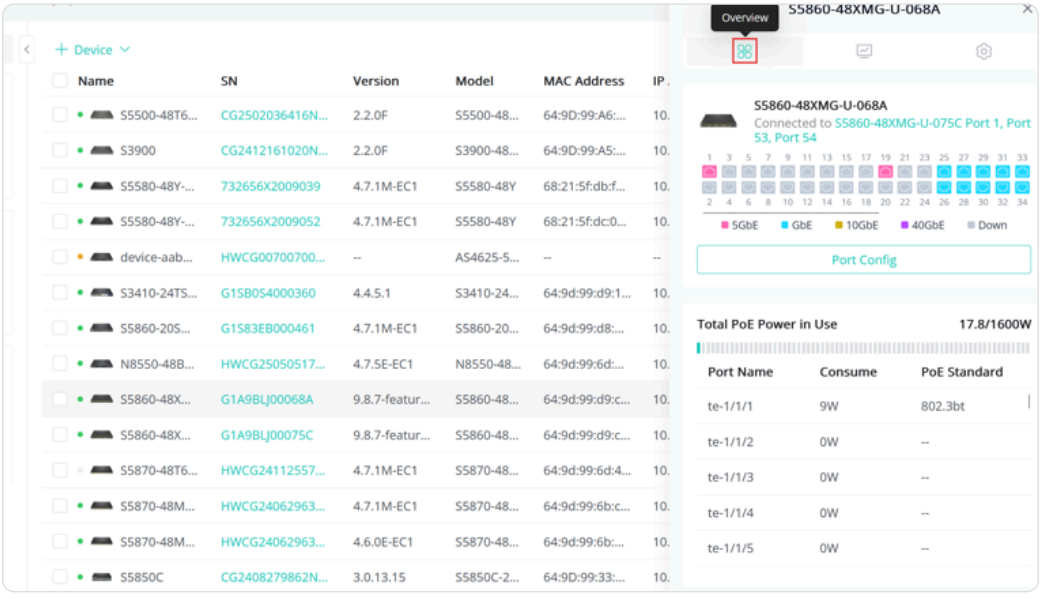
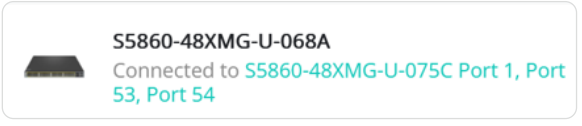
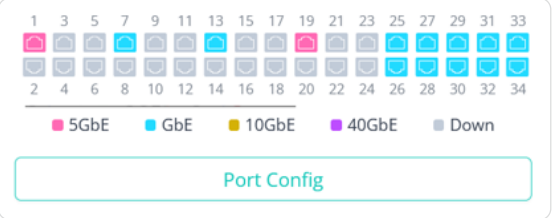
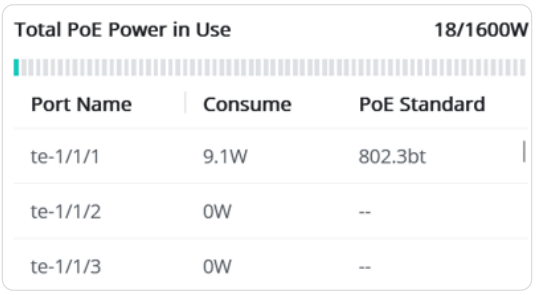


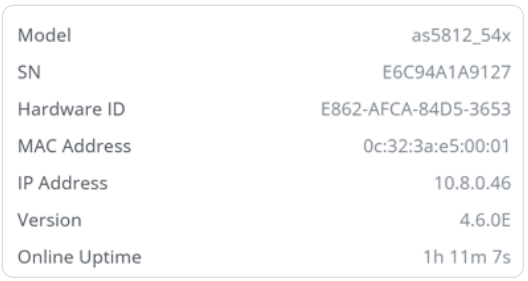
Table 1. PicOS Switch Overview

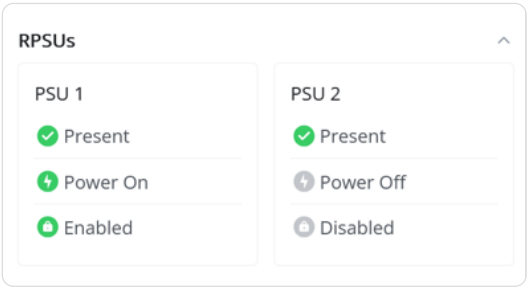
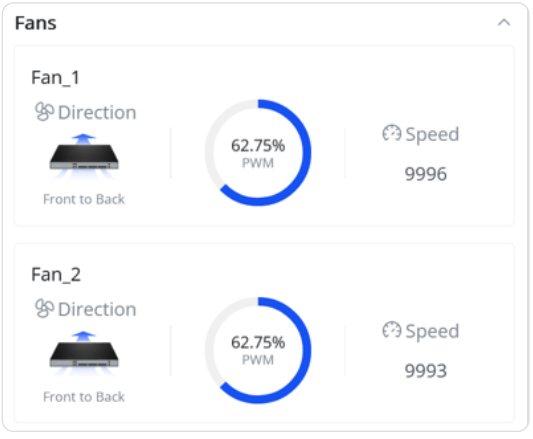
Metric	Description
Switch Image and Alias and Its Uplink Switch	The image and alias of the monitored switch. The monitored switch’s upstream switch, and the upstream switch’s downlink ports that connect to the monitored switch. 

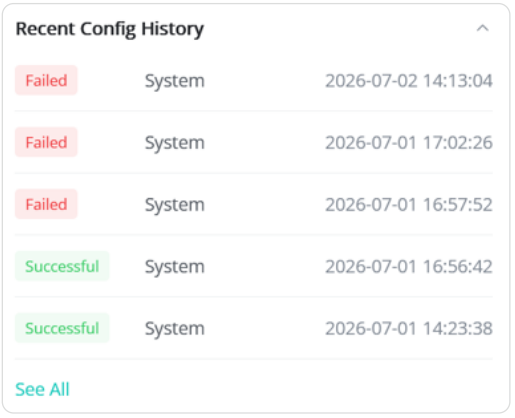
	NOTEs • For an online (connected to AmpCon-Campus) switch: ◦ If the switch is connected to a non-third-party uplink switch, information such as **Connected to S5580-48Y-0016 Port 56** is displayed. **S5580-48Y-0016** is the uplink switch alias, and **Port 56** is the port on the uplink switch that connects to the local switch ◦ If the switch is connected to a third-party uplink device, information such as **Connected to Third-Party Device (MAC: a1:b2:c3:d4:e5:f6) via local xe-1/1/1** is displayed. **local xe-1/1/1** is the switch's uplink port, and **a1:b2:c3:d4:e5:f6** is the switch's MAC address. ◦ If AmpCon-Campus cannot retrieve the MAC address of the third-party uplink device, information such as **Connected to Third-Party Device via local xe-1/1/1** is displayed. ◦ If the switch is not connected to any uplink switch, **Connected to --** is displayed. • For an offline (disconnected from AmpCon-Campus) switch: ◦ If the switch has previously connected to an uplink switch, information such as **Last Connected to S5580-48Y-0016 Port 56** is displayed. ◦ If the switch hasn't connected to any uplink switch, **Last Connected to --** is displayed. • If the uplink switch is also managed by AmpCon-Campus, you can click the uplink switch alias to open its side panel.
Port Panel	The port panel containing all ports of the switch. Hover over a port, and then you can see the following information: • **Port:** The port number. • **Name:** The port name.

	• **TX Traffic:** The total amount of data emitted from the port. • **RX Traffic:** The total amount of data received by the port. • **PoE Power:** The real-time PoE output power of the port. The metric values are displayed only for PoE ports. • **PoE Standard:** The currently negotiated PoE power supply standard, including 802.3af, 802.3at, or 802.3bt. The metric values are displayed only for PoE ports. • **Uplink:** The uplink switch and uplink port. The metric values are displayed only for switches that are currently connected to an uplink switch.  **NOTEs** • Different speeds of ports are marked in different colors. • The ports in **Down** status are displayed in grey. The ports in **Disabled** status are displayed in light grey. • To push port-related configurations to the switch, click **Port Config**. You will be redirected to the "Ports" page. For more information, see Applying Port Configurations. • If a physical port is split into multiple ports, hover over the physical port to view information for the physical port and each split port. Uplink switch and uplink port information is not displayed for these ports.
PoE	The PoE-related information on the switch: • The real-time total PoE output power of the switch, and the maximum PoE output power. • The progress bar showing the ratio of real-time total PoE output power to the maximum PoE output power.

	• The real-time PoE output power of each switch port.
	  ◦ **Port Name:** The port name.
	  ◦ **Consume:** The actual Power Sourcing Equipment (PSE) output power of the PoE port, accurate to two decimal places.
	  ◦ **PoE Standard:** The currently negotiated PoE power supply standard, including 802.3af, 802.3at, or 802.3bt.
	
	Total PoE Power in Use 18/1600W
	Port Name | Consume | PoE Standard
	te-1/1/1 | 9.1W | 802.3bt
	te-1/1/2 | 0W | --
	te-1/1/3 | 0W | --
	NOTEs
	• This section is displayed only if the PicOS switch supports PoE.
	• Only the ports in Up status are displayed in this section.

Basic Information	The basic information of the switch: • **Model:** The model of the switch. • **SN:** The SN of the switch. • **Hardware ID:** The hardware ID of the switch. • **MAC Address:** The MAC address of the switch. • **IP Address:** The VPN IP address of the switch. • **Version:** The PicOS version of the switch. • **Online Uptime:** The elapsed time since the switch last connected to AmpCon-Campus. Hover over the time to view the switch's last connection time to AmpCon-Campus.  Model as5812_54x SN E6C94A1A9127 Hardware ID E862-AFCA-84D5-3653 MAC Address 0c:32:3a:e5:00:01 IP Address 10.8.0.46 Version 4.6.0E Online Uptime 1h 11m 7s

Redundant Power Supply Units (RPSUs)	The status of each Power Supply Unit (PSU) on the switch. You can see the following statuses: • **Present:** The PSU is properly installed. • **Not Present:** The PSU is not properly installed. • **Power On:** The PSU is powered on. • **Power Off:** The PSU is powered off. • **Enabled:** The PSU is activated and turned on. • **Disabled:** The PSU is deactivated or turned off.  **NOTEs** • **Present**, **Power On**, or **Enabled** is marked with a green icon; **Not Present**, **Power Off**, or **Disabled** is marked with a gray icon. • For single-power switches, only the **Power On** status is displayed. No data is displayed in this section when the PSU is powered off.
Fans	The status of each fan on the switch. For each fan, you can see the following information: • **Direction:** The airflow direction, such as **Back to Front**. • **PWM:** The proportion of the fan's Pulse Width Modulation (PWM) to the total width. • **Speed:** The fan speed, measured in Revolutions Per Minute (RPM). 

Recent Config History	The execution result, operation type, and start time of the latest five configuration pushes. To check the full switch configuration history, click **See All**. You will be redirected to the “Configuration Result” page. 

Deep Insights into a PicOS Switch

Click the **Devices** icon from the navigation bar. On the “Devices” page, click a PicOS switch. You can see a side panel on the right.

In the **Insight** tab of the side panel, you can gain deep insight into the switch.

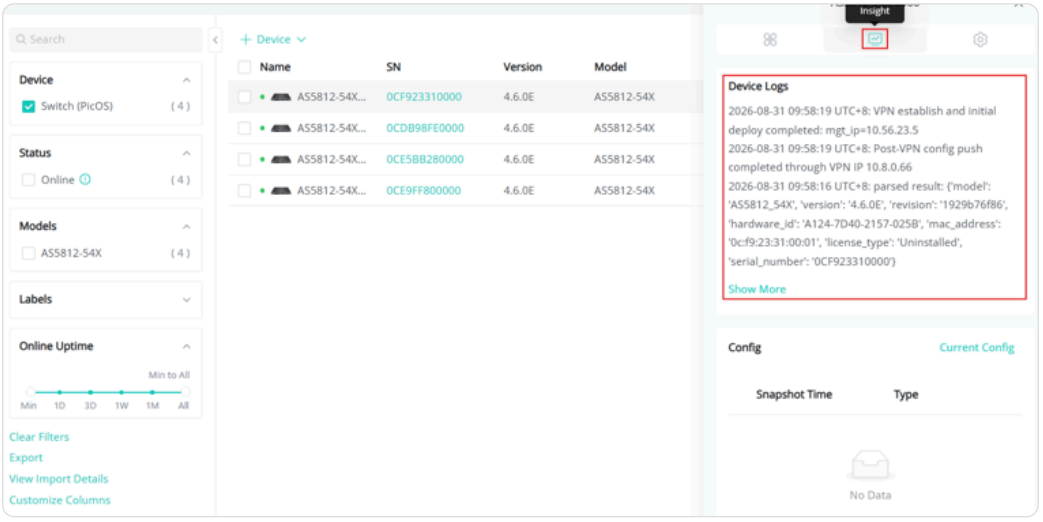
- Guidelines
- Device Logs
- Configuration Backup
- Switch Statistics
  - Switch Traffic
  - Module Metrics
  - Port Metrics
  - Protocol Status

Guidelines

- AmpCon-Campus can monitor only the PicOS switches that have been successfully onboarded.
- Some data in the **Insight** tab might not be displayed for offline PicOS switches (switches disconnected from AmpCon-Campus).

Device Logs

In the **Device Logs** section, you can see the latest three operation logs of the switch. To see more logs, click **Show More**.



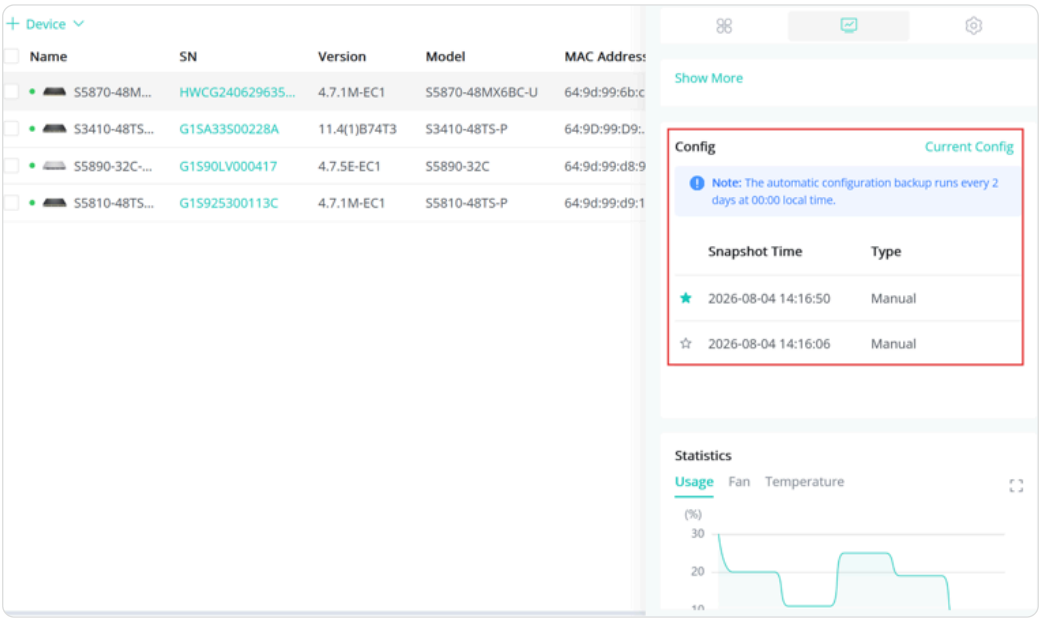
Configuration Backup

In the **Config** section, you can see the latest four backups in the backup list.

> **NOTEs**
>
> - **Snapshot Time** indicates the time when the switch was backed up.

- **Type** can be **Auto** or **Manual**, which indicates the **Scheduled Auto Backup** or **Immediate Backup** option selected when you back up configurations. For more information, see Backing Up Configurations.
- The scheduled auto backups that have not been executed are not displayed in the backup list.

  If you have configured automatic backups for the switch, you can see the note with the current automatic backup schedule. For example, “The automatic configuration backup runs every 2 days at 14:00”.



- To mark an important backup, locate the backup item, and then click ☆ to change it to ★. Click ★ to downgrade it to a normal backup.

  The marked backup item will always be displayed here and cannot be overwritten by newer backup items. At most 2 backups can be marked with ★.
- To check the configurations of a backup, hover over the backup item, and then click **View**.
- To delete a backup, click **Delete**. In the pop-up window, click **Yes**.
- To check the currently running configurations on the switch, click **Current Config**.

  In the pop-up window, you can click **Show SET-format** to display the configurations in **set xx** format.

Switch Statistics

In the **Statistics** section, you can see the following trend graphs:

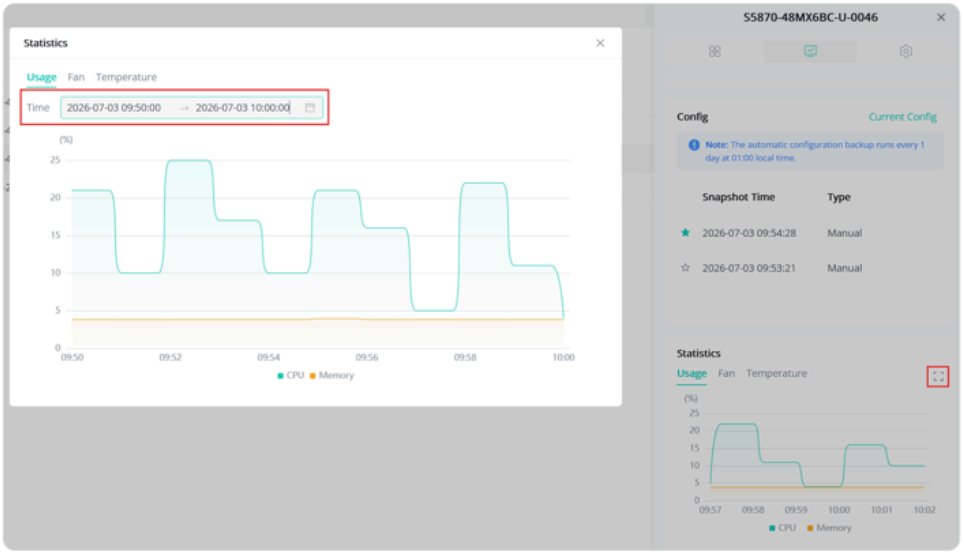
Table 1. Statistic Trend Graphs

Trend Graph	Description

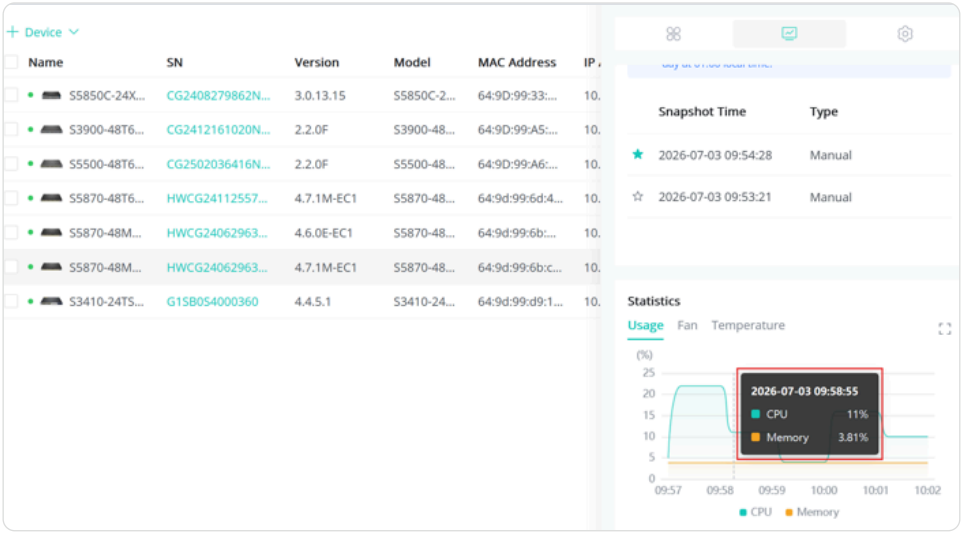
Usage	The CPU and memory usage of the switch. It's measured in percentage.
Fan	The proportion of the fan's PWM to the total width.
Temperature	The temperature of the switch.

- By default, the trend graphs display data in the last 5 minutes. To change the display time range, click the expand icon, and then select the start and end time point in the pop-up window.

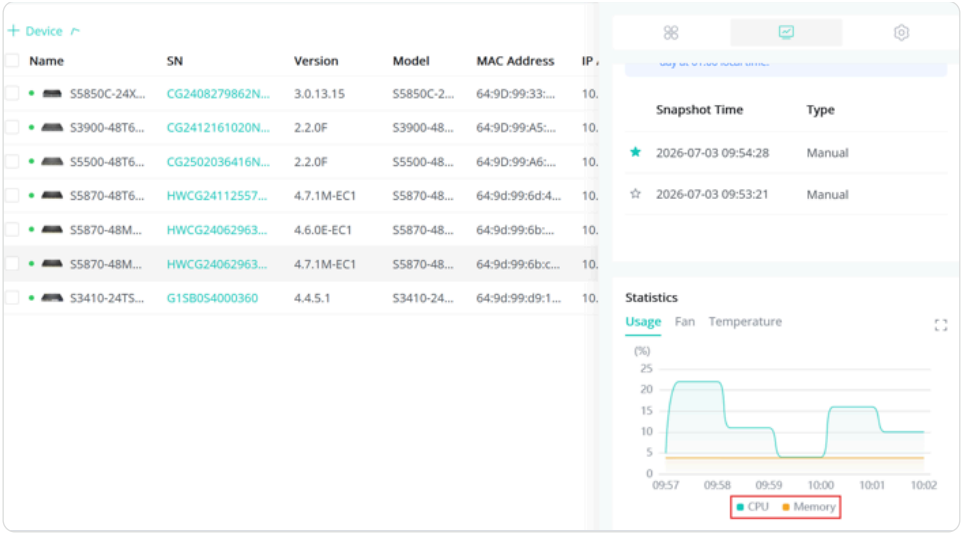
> **NOTEs**
>
> - All time points use your browser's time zone.
> - Only the data in the last 1 month can be displayed.



- To see the metric details at a specific time point, hover your mouse over that time point.



- To display or hide the data of a metric, click the square before the metric.



Switch Traffic

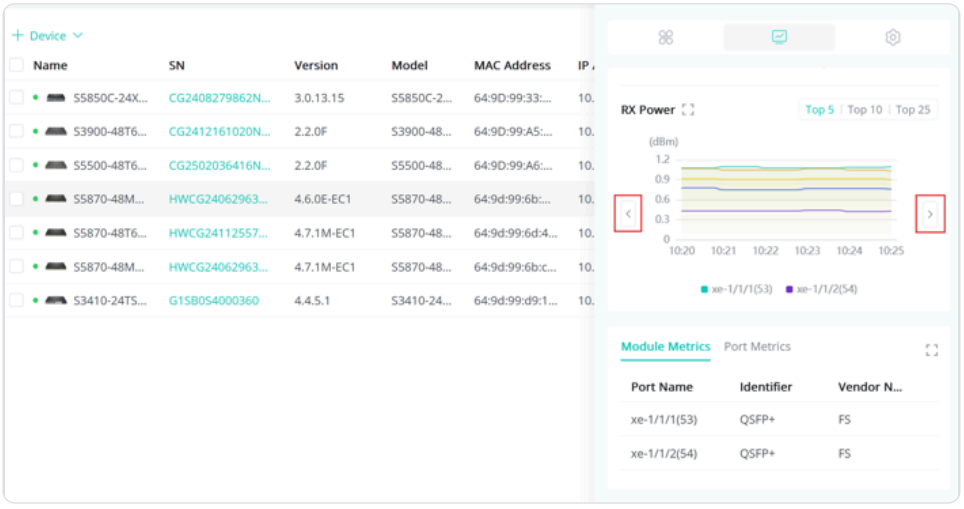
You can see the following trend graphs related to switch traffic:

Table 2. Switch Traffic Trend Graphs

Trend Graph	Description
In Octets	The number of octets (8-bit bytes) received by the switch port.
In Pkts	The number of incoming packets received by the switch port.
In Discards	The number of incoming packets that the switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by the switch port.
In Fcs Errors	The number of incoming packets that fail the Frame Check Sequence (FCS) validation.
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
Out Pkts	The number of packets transmitted out of the switch port.
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops).
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors.

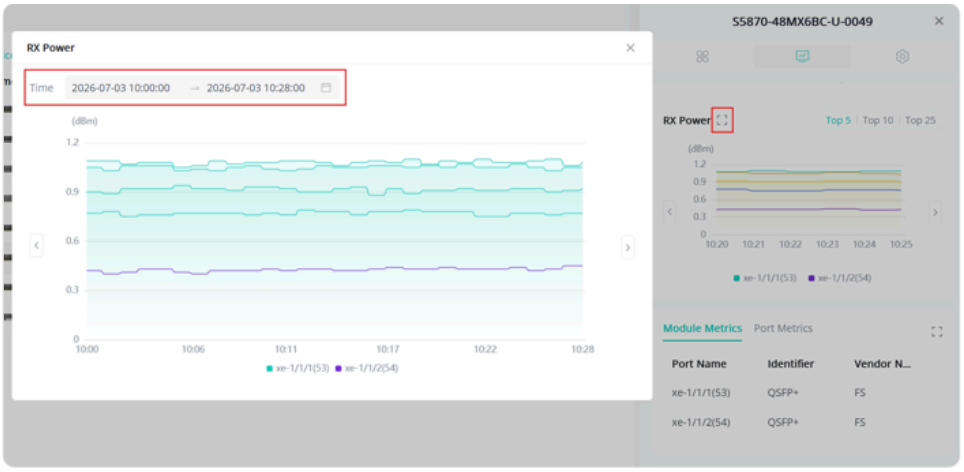
Out Bits Rate	The rate at which bits are transmitted from the switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by the switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from the switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by the switch port. It's measured in Packets Per Second (pps).
TX Power	The amount of optical power emitted by the optical module connected to the switch port. It's measured in dBm.
RX Power	The amount of optical power received by the optical module connected to the switch port. It's measured in dBm.

- To check the last and next trend graph, click **<** or **>**.



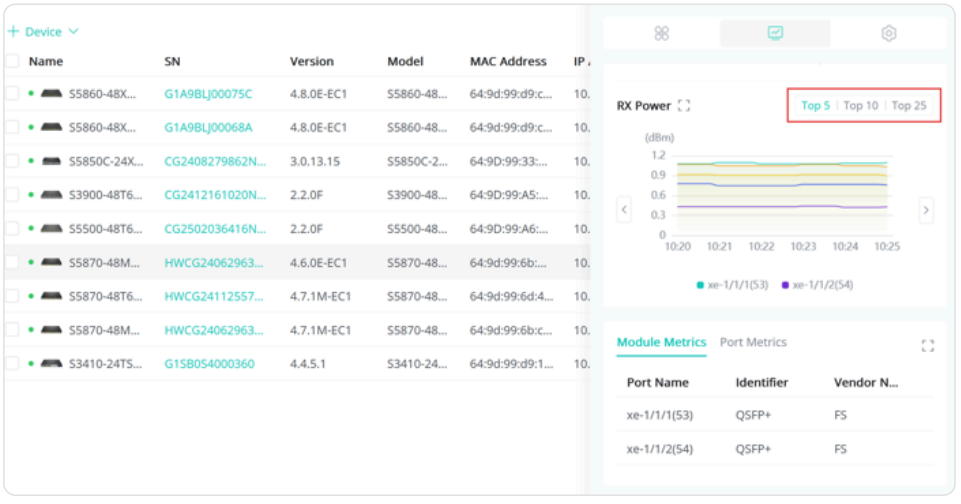
- By default, the trend graphs display data in the last 5 minutes. To change the display time range, click the expand icon, and then select the start and end time point in the pop-up window.

> **NOTEs**
>
> - All time points use your browser's time zone.
> - Only the data in the last 1 month can be displayed.

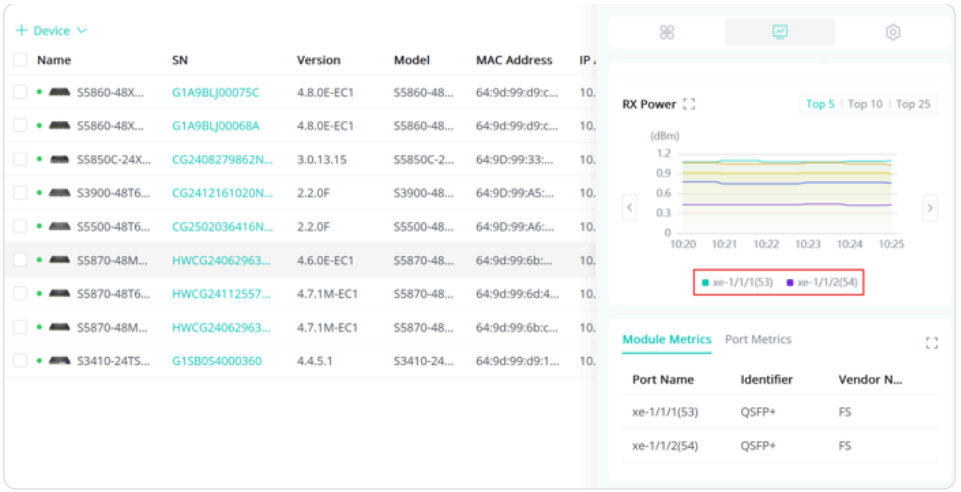


- To specify how many ports that you want to monitor, select one of the following options:
  - **Top 5:** The 5 switch ports with the largest values. By default, **Top 5** is selected.
  - **Top 10:** The 10 switch ports with the largest values.
  - **Top 25:** The 25 switch ports with the largest values.

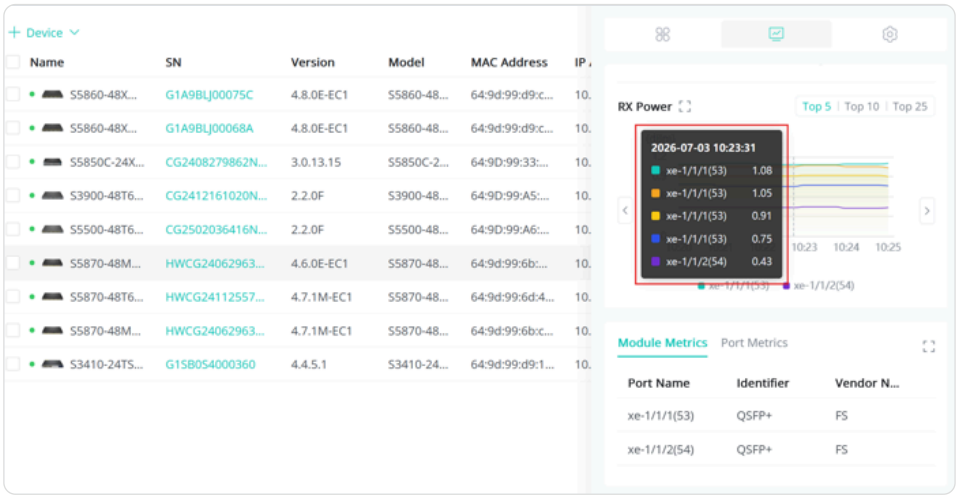
> **NOTEs**
>
> - Only the ports that are up at some time within the selected time range can be displayed. If a switch port goes down during a certain period, its metric data for that period will not be displayed.
> - Even though **Top X** (such as **Top 5**) is selected, you might see fewer than the selected number of switch ports in the trend graph when some ports are down.



- To display or hide the data of a switch port, click the square before the port.



- To see the metric details at a specific time point, hover your mouse over that time point.



Module Metrics

In the **Module Metrics** tab, you can see the following metrics related to optical modules:

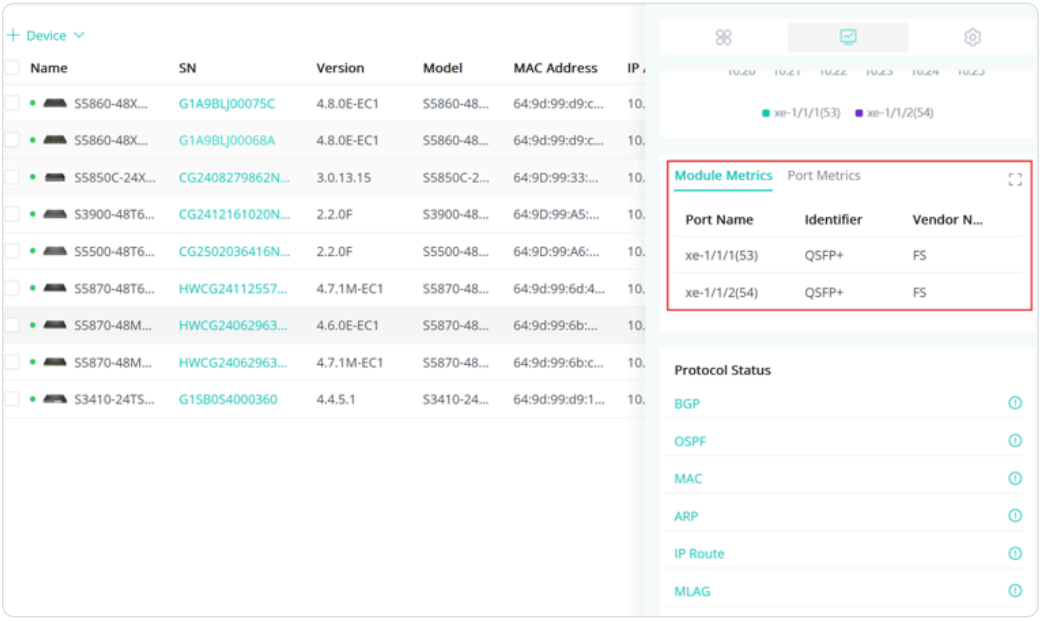


Table 3. Optical Module Metrics

Metric	Description
Port Name	The name of the switch port connected to the optical module.
Identifier	The identification code used to uniquely identify, locate, and manage the optical module.
Vendor Name	The manufacturer of the optical module.

To see more metrics, click the expand icon. You can then see the following metrics in addition to those listed above:

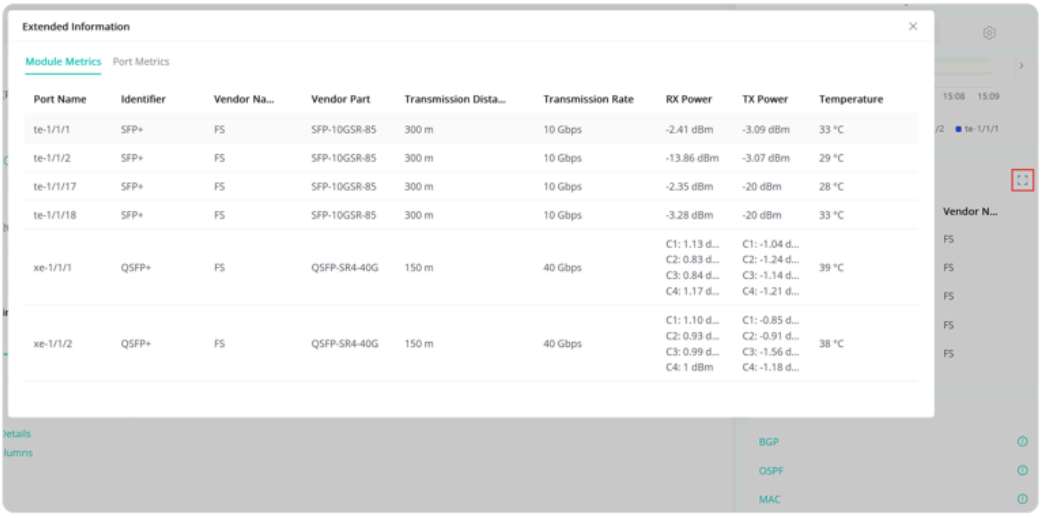


Table 4. Additional Module Metrics

Metric	Description
Vendor Part	The model name of the optical module.
Transmission Distance	The maximum distance over which an optical signal can be transmitted effectively through the module.
Transmission Rate	The speed at which data can be transmitted through the module.
RX Power	The amount of optical power received by the optical module connected to the switch port. It's measured in dBm.
TX Power	The amount of optical power emitted by the optical module connected to the switch port. It's measured in dBm.

Temperature	The temperature of the optical module. It's measured in Celsius (°C).

Port Metrics

In the **Port Metrics** tab, check the following metrics related to switch ports:

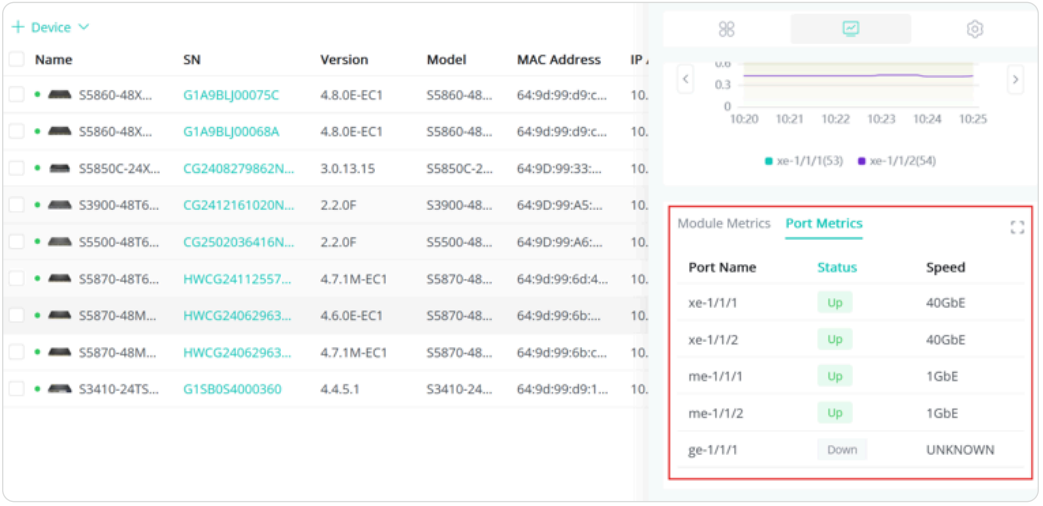


Table 5. Port Metrics

Metric	Description
Port Name	The name of the port. **NOTE** If a physical port is split into multiple ports, you can see an expand icon before the physical port name. Click the expand icon to view information for each split port.
Status	The status of the port, **Up** or **Down**.
Speed	The speed of the port. If the port is in **Down** status, the value is **UNKNOWN**.

To see more metrics, click the expand icon. You can then see the following metrics in addition to those listed above:

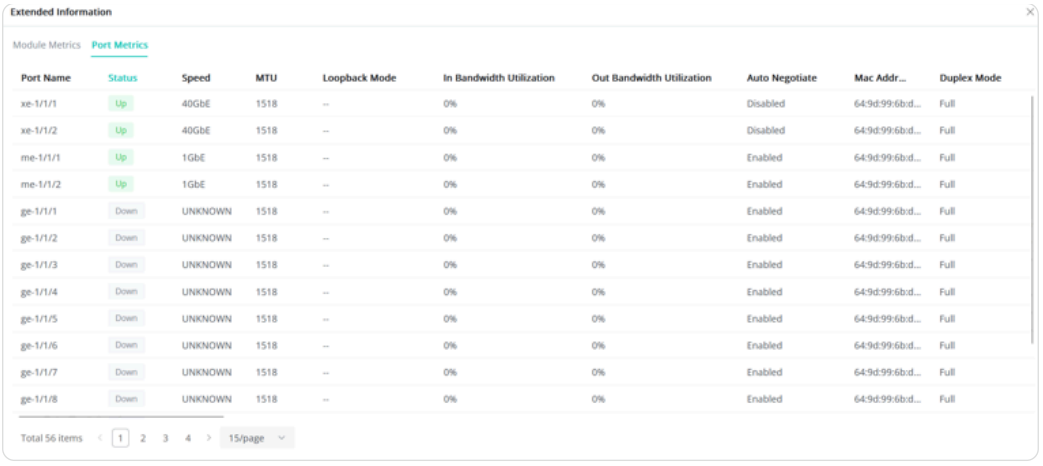


Table 6. Additional Port Metrics

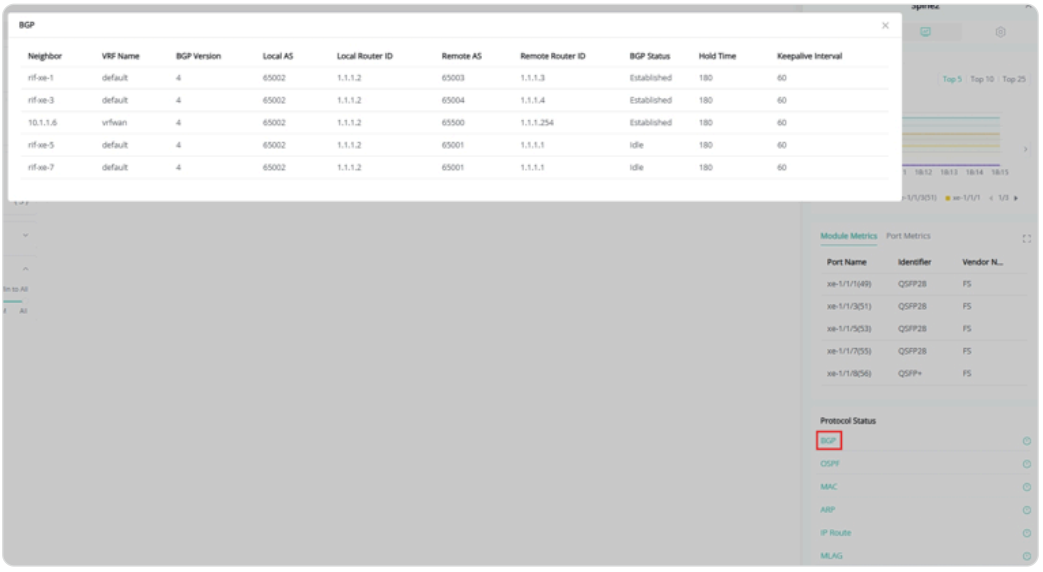
Metric	Description
MTU	The largest size of a data packet that can be transmitted over a network without being fragmented. It's measured in bytes.
Loopback Mode	Whether the loopback mode is enabled on this port. In loopback mode, the switch port sends data packets that are then routed back to itself. You can enable this mode to verify whether data can be sent or received as expected without involving external networks.
In Bandwidth Utilization	The percentage of the inbound bandwidth that is being used on the port.
Out Bandwidth Utilization	The percentage of the outbound bandwidth that is being used on the port.
Auto Negotiate	Whether the Auto Negotiate feature on the port is enabled. Auto Negotiate means the process of automatically negotiating and selecting the optimal operating parameters, such as the speed and duplex mode.
MAC Address	The MAC address of the switch port.
Duplex Mode	The transmission mode: **Half** or **Full**. • **Half:** Data can flow in one direction (half duplex) at a time.

	• **Full:** Data can flow in both directions (full duplex) simultaneously.
In Broadcast Pkts	The number of broadcast packets received by the port.
In Discards	The number of incoming packets that the switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by the switch port.
In Fcs Errors	The number of incoming packets that fail the Frame Check Sequence (FCS) validation.
In Multicast Pkts	The number of multicast packets received by the switch port.
In Octets	The number of octets (8-bit bytes) received by the switch port.
In Pkts	The number of incoming packets received by the switch port.
In Unicast Pkts	The number of unicast packets received by the switch port.
Out Broadcast Pkts	The number of broadcast packets sent by the switch port.
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops).
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors.
Out Multicast Pkts	The number of multicast packets sent by the switch port.
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
Out Pkts	The number of packets transmitted out of the switch port.

Out Unicast Pkts	The number of unicast packets sent by the switch port.
In Oversize Frames	The number of oversize frames received by a switch port. Oversize frames mean frames that exceed the typical maximum transmission unit (MTU) size.
In Undersize Frames	The number of undersize frames received by a switch port. Undersize frames mean frames with a length less than 64 bytes and a correct checksum.
Out Bits Rate	The rate at which bits are transmitted from the switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by the switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from the switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by the switch port. It's measured in Packets Per Second (pps).
In Frames 64 Octets	The number of 64-byte frame packets received by the switch port.
In Frames 65-127 Octets	The number of frame packets between 65 and 127 bytes received by the switch port.
In Frames 128-255 Octets	The number of frame packets between 128 and 255 bytes received by the switch port.
In Frames 256-511 Octets	The number of frame packets between 256 and 511 bytes received by the switch port.
In Frames 512-1023 Octets	The number of frame packets between 512 and 1023 bytes received by the switch port.
In Frames 1024-1518 Octets	The number of frame packets between 1024 and 1518 bytes received by the switch port.

Protocol Status

In the **Protocol Status** section, click a protocol (**BGP**, **OSPF**, **MAC**, **ARP**, **IP Route**, or **MLAG**), and then you can see detailed metrics related to the protocol.



See the following BGP metrics:

Table 7. BGP Metrics

Metric	Description
Neighbor	The BGP neighbors of the switch.
VRF Name	The name of the Virtual Routing and Forwarding (VRF) instance.
BGP Version	The version of Border Gateway Protocol (BGP).
Local AS	The Autonomous System Number (ASN) of the local switch.
Local Router ID	The unique BGP identifier of the local switch.
Remote AS	The ASN of the remote device.
Remote Router ID	The unique BGP identifier of the remote device.
BGP Status	The state of the BGP session.
Hold Time	The allowed maximum time between two BGP peers without receiving any messages. It's measured in seconds.

Keepalive Interval	The time interval for sending KEEPALIVE messages between BGP peers. It's measured in seconds.

See the following OSPF metrics:

Table 8. OSPF Metrics

Metric	Description
VRF Name	The name of the Virtual Routing and Forwarding (VRF) instance.
Neighbor ID	The unique identifier to distinguish a neighboring device.
Pri	The OSPF router priority, which is a parameter that influences the election process for the Designated Router (DR) and Backup Designated Router (BDR) within an OSPF network.
State	The current status of the OSPF router.
Dead Time	The amount of time that a router waits to receive a Hello packet from a neighboring router before it declares that neighbor as "dead" or unreachable. It's measured in seconds.
Address	The IP address of the neighbor.
Interface	The interface on a router to establish the OSPF neighbor relationship.
RXmtl	The total number of link state advertisements on the retransmission queue sent to neighbors.
Rqstl	The total number of link state advertisements on the request messages queue sent to neighbors.
DBsml	The total number of link state advertisements on the Database Description (DD) messages queue sent to neighbors.
DR	The Designated Router, a special router elected within an OSPF area to handle the exchange of link-state information.

BDR	The backup Designated Router, a backup to the DR in an OSPF network.

See the following MAC metrics:

Table 9. MAC Metrics

Metric	Description
MAC Address	The MAC address learned by the switch port from the connected device.
Interface	The physical port associated with the MAC address.
VLAN	The identifier of the VLAN including this MAC address.
Age	The duration during which the MAC address entry remains valid before it is deleted due to lack of updates. It's measured in seconds.
Type	The method used to obtain the MAC address, **Dynamic** or **Static**.

See the following ARP metrics:

Table 10. ARP Metrics

Metric	Description
Address	The IP address of the neighboring switch.
HW Address	The MAC address of the neighboring switch.
Type	The types of the ARP entry, **Dynamic** or **Static**.
Interface	The physical or logical port on the switch associated with the IP address and the MAC address.

See the following IP route metrics:

Table 11. IP Route Metrics

Metric	Description
Type	The protocol through which the route was learned or configured. The following types are supported:

	• **DIRECTLY_CONNECTED:** This is a directly connected network. • **STATIC:** This is a static route. • **OSPF:** This is a route learned through the OSPF protocol. • **BGP:** This is a route learned through the BGP protocol.
Destination Network	The address and subnet mask of the destination network.
Route Metrics	The metric (or cost) of the route, which determines the priority of the route. For example, [110/2] indicates that the route uses the OSPF protocol, where 110 is the OSPF priority and 2 is the metric of the route.
Next Hop	The next hop IP address to which packets are forwarded.
Outgoing Interface	The network interface from which packets are forwarded.
Route Age	The elapsed time since the route was learned or configured.

See the following MLAG metrics:

Table 12. MLAG Metrics

Metric	Description
Domain ID	The unique identifier to distinguish an MLAG domain. An MLAG domain is established between two switches configured with the same domain ID.
Domain MAC	The MAC address of an MLAG domain.
Node ID	The unique identifier to distinguish the MLAG peer devices. • **0:** Represents the primary device. • **1:** Represents the secondary device.
Peer Link	The local interface ID of the peer-link.
Peer IP	The IP address of the remote peer-link port.
Peer VLAN	The VLAN ID used for the peer-link.

Neighbor Status	The status of the MLAG peer connection. • **IDLE:** No peer-link is established. • **CONNECTING:** The peer-link is being established. • **ESTABLISHED:** The peer-link is established successfully.
Config Matched	Whether the configurations between MLAG peers are consistent. Values can be **Yes** or **No**.
MAC Synced	Whether the MAC address tables between MLAG peers are consistent. Values can be **Yes** or **No**.
MLAG Link Count	The total number of MLAG peer-links.

Configurations and Operations of a PicOS Switch

Click the **Devices** icon from the navigation bar. On the “Devices” page, click a PicOS switch. You can see a side panel on the right.

In the **Setting** tab of the side panel, you can view the configurations or perform switch management operations.

Guidelines
General Configurations
Device Credential Configurations
L3 Interface and DHCP Configurations
Static Route Configurations
OSPF Configurations
Switch Management Operations

Guidelines

- In the **Setting** tab, you can not only view but also modify configurations. For more information, see Configuring a Single Switch.
- If the PicOS switch is offline (disconnected from AmpCon-Campus), modifications to L3 interface, DHCP, static route, and OSPF configurations will fail.
- L3 interface, DHCP, static route, and OSPF configurations applied in the **Setting** tab will be automatically synchronized to the **Quick Config** wizard, and vice versa. For more information about the **Quick Config** wizard, see Applying Quick Configurations.

General Configurations

At the top of the **Setting** tab, you can view general configurations of the switch:

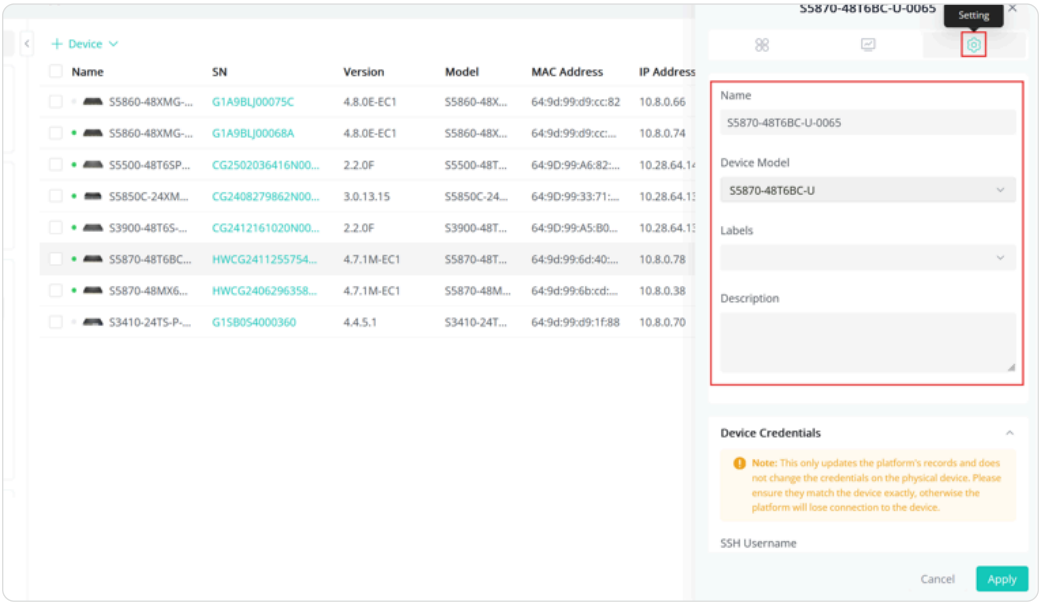


Table 1. General Switch Configurations

Configuration	Description
Name	The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side.
Device Model	The model of the switch. AmpCon-Campus automatically retrieves the switch model and displays it here. The model can't be changed.
Labels	The switch labels used for switch filtering and management.
Description	The description of the switch.

Device Credential Configurations

In the **Device Credentials** section, you can view the **SSH Username** and **SSH Password**.

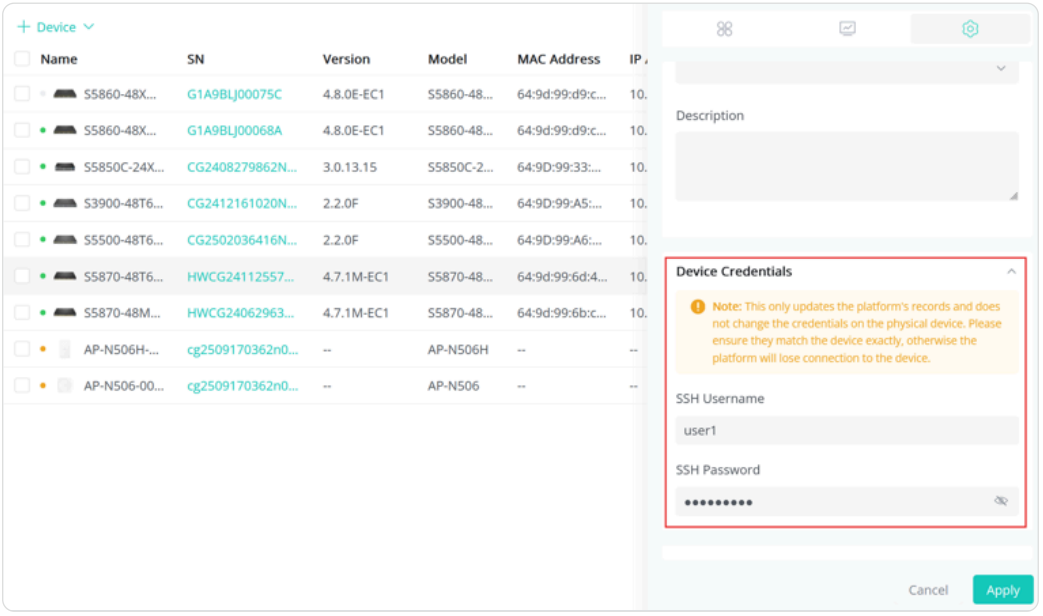


Table 2. Device Credential Configurations

Configuration	Description
SSH Username	The username of the switch.
SSH Password	The password of the user. Click the eye icon to see the clear-text password. **NOTE**

Ensure that the username and password match the switch exactly. Otherwise, AmpCon-Campus cannot access and manage the switch.

L3 Interface and DHCP Configurations

In the **L3 Interfaces & DHCP** section, you can view the previously configured L3 interface and DHCP configurations.

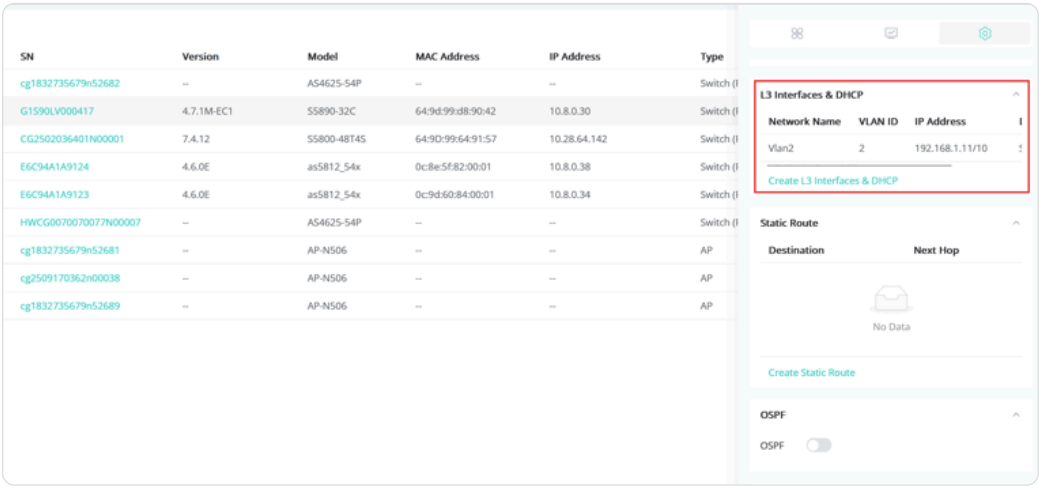


Table 3. L3 Interface and DHCP Configurations

Configuration	Description
Network Name	The name of the Layer 3 VLAN interface.
VLAN ID	The VLAN identifier.
IP Address	The IPv4 address and subnet mask assigned to the Layer 3 interface.
DHCP Service	The DHCP mode for this subnet. The value can be **None**, **Server**, or **Relay**. • **None:** DHCP is disabled. • **Server:** The switch acts as a DHCP server. • **Relay:** The switch acts as a DHCP relay and forwards DHCP requests to an external DHCP server.

Static Route Configurations

In the **Static Route** section, you can view the previously configured static route configurations.

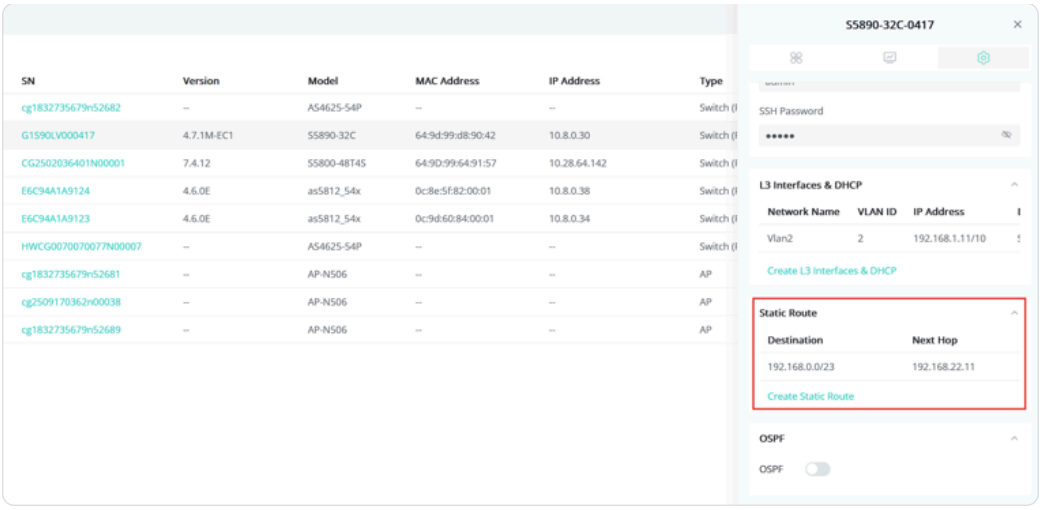


Table 4. Static Route Configurations

Parameter	Description
Destination	The destination IPv4 address and the prefix length. For example, 192.168.4.5/22.
Next Hop	The next hop IPv4 addresses.

OSPF Configurations

In the **OSPF** section, you can view the previously configured OSPF configurations.

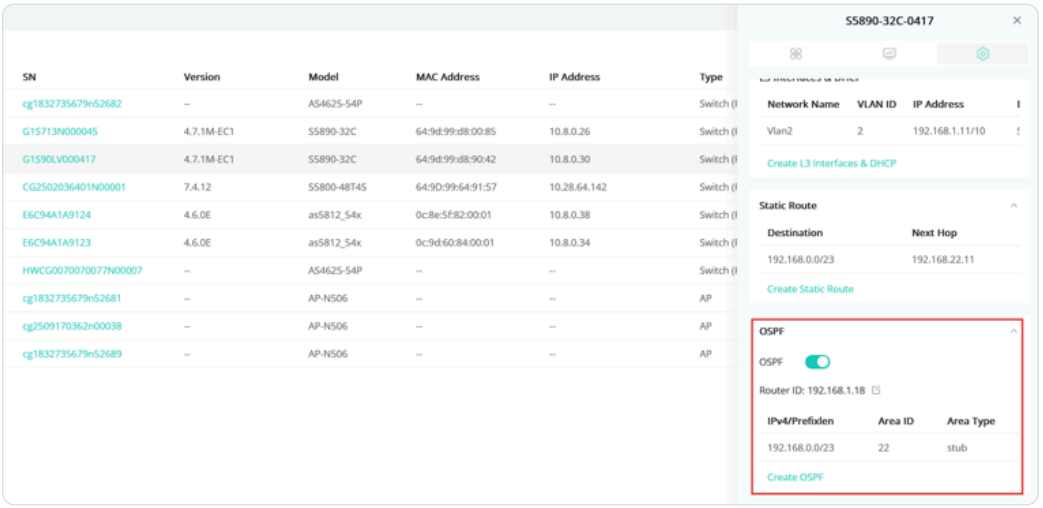


Table 5. OSPF Configurations

Parameter	Description
OSPF	Whether OSPF is enabled.
Router ID	The router ID, which uniquely identifies a router.
IPv4/Prefixlen	The IPv4 address and prefix length.

Area ID	The ID of the OSPF area. OSPF divides a network into areas to improve scalability and control the flow of routing information.
Area Type	The type of the OSPF area. Values can be **Stub**, **NSSA**, and **Default**. • **Stub:** An OSPF stub area is a special type of OSPF area designed to optimize routing efficiency by blocking external route advertisements while maintaining internal and inter-area connectivity. • **NSSA:** A Not-So-Stubby Area (NSSA) is a special OSPF area type that combines features of stub areas and standard areas, allowing limited external route redistribution while blocking most external LSAs. • **Default:** The default area in OSPF (also called standard area) refers to a non-specialized OSPF area that permits all types of LSAs (Type 1-5) without restrictions.

Switch Management Operations

In the **Actions** section, you can manage the switch by using the following buttons:

> **NOTEs**
>
> - Do not click any buttons during PicOS switch upgrade or switch configuration. Otherwise, the corresponding operations will fail.
> - For offline PicOS switches, do not click any buttons except the **Delete** button. Otherwise, the corresponding operations will fail.

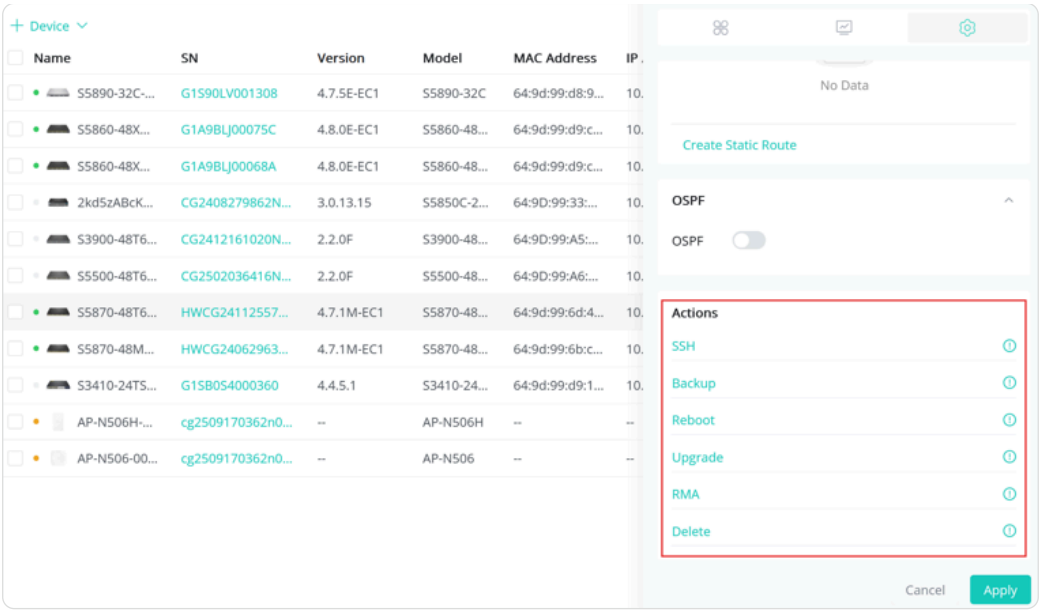


Table 6. Action Buttons

Button	Purpose	Reference Link
SSH	Connect to a PicOS switch from the AmpCon-Campus UI by creating an SSH session.	• Accessing Switches
Backup	Back up PicOS switch configurations automatically at a specified interval and time, or manually.	• Backing Up Configurations
Reboot	Reboot a PicOS switch.	• Rebooting Switches
Upgrade	Upgrade PicOS on a switch immediately or schedule an automatic upgrade during off-peak hours.	• Upgrading Switches
RMA	Use Return Merchandise Authorization (RMA) to replace a failed PicOS switch with a new switch of the same model, so that AmpCon-Campus can seamlessly manage the new switch.	• Return Merchandise Authorization
Delete	Delete a PicOS switch from AmpCon-Campus.	• Deleting Switches

FSOS Switches

After onboarding FSOS switches to AmpCon-Campus, you can continuously monitor the switches for performance analysis and fault diagnosis through Simple Network Management Protocol (SNMP).

SNMP is an application-layer protocol used for managing and monitoring network devices. SNMP in AmpCon-Campus is mainly used to monitor the status, metrics, and other statistics of FSOS switches for performance analysis and fault diagnosis. For more information, see SNMP Overview.

See the following child topics:

- SNMP Overview
- FSOS Switch List
- Information of an FSOS Switch
- Monitoring Limitations

SNMP Overview

Simple Network Management Protocol (SNMP) is a protocol used to monitor and manage different types of switches in your network.

SNMP Versions
SNMP Architecture
SNMP Workflow

SNMP Versions

AmpCon-Campus supports three versions: SNMP v1, SNMP v2c, and SNMP v3.

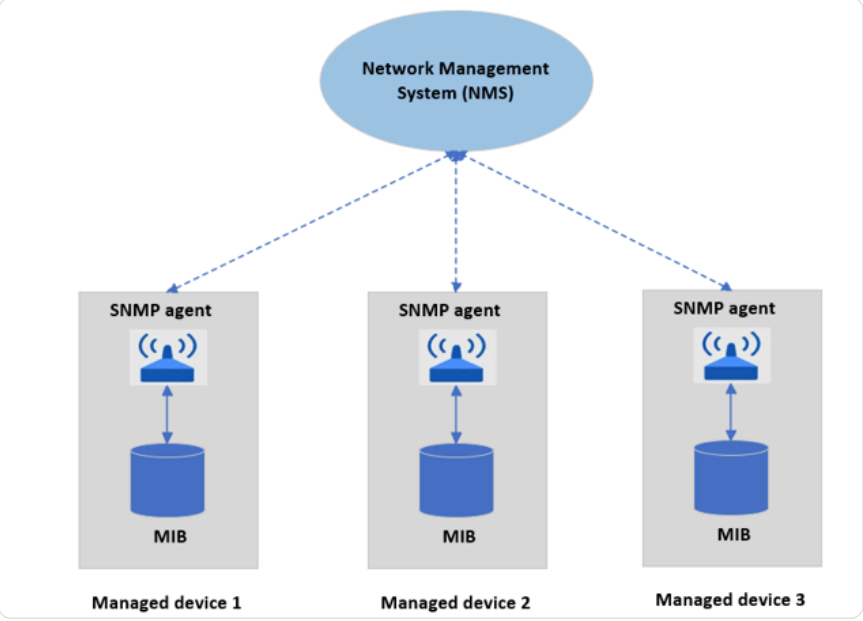
Each version differs in security, functionality, and performance. SNMP v3 is the most secure and powerful version, which supports encryption and authentication mechanisms.

To enhance security, you are recommended to use SNMP v3 with properly configured security parameters (encryption and authentication) to protect the confidentiality and integrity of device monitoring data.

SNMP Architecture

The SNMP architecture is as follows:

Figure 1. SNMP Architecture



- **Network Management System (NMS)**

  A combination of hardware (devices) and software (the SNMP manager). The SNMP manager monitors and administers a network by polling the devices on your network for information about network connectivity, activity, and events.

- **SNMP manager**

An application to collect and process information from SNMP agents. The SNMP manager sends requests (such as requests to retrieve device statuses) to SNMP agents and receives responses.

- **Managed device**

  The device on a network managed by the NMS. Routers and switches are common examples of managed devices.

- **SNMP agent**

  An SNMP process that resides on a managed device, responsible for collecting local device information and exposing it to the SNMP manager.

  The SNMP agent responds to requests from the SNMP manager and provides operational status, performance metrics, configuration data, and other device-specific information to the SNMP manager.

  The SNMP agent also controls access to the agent's MIB, the collection of objects that can be viewed or changed by the SNMP manager.

- **SNMP item**

  The fundamental unit in NMS to define individual monitoring metrics. The SNMP manager uses Object Identifiers (OIDs) to retrieve each item value on managed devices.

- **Management Information Base (MIB)**

  A hierarchical database that defines the data sets and object types exchanged between the SNMP manager and SNMP agents.

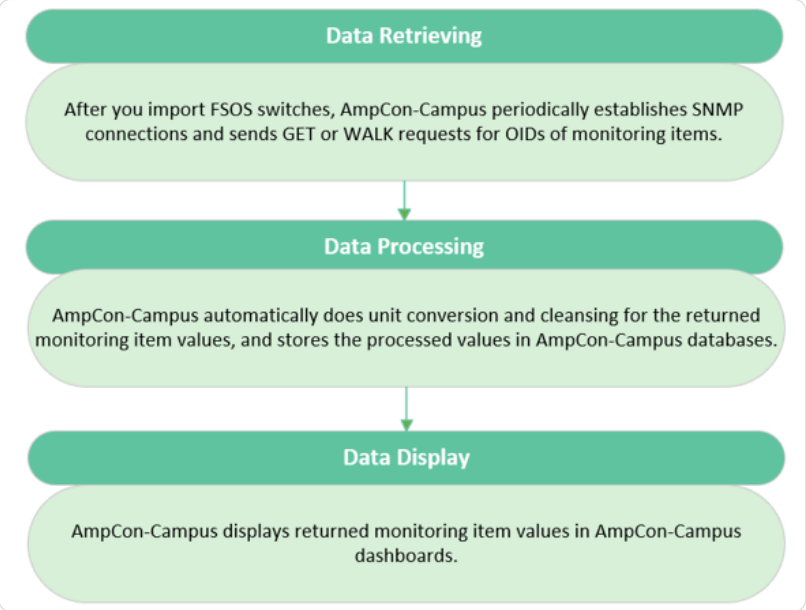
  Each managed device maintains its specific MIB, which contains detailed information about the device and its services.

  The SNMP manager uses MIB identifiers (OIDs) to retrieve and manage the information.

SNMP Workflow

AmpCon-Campus communicates with imported switches through SNMP, retrieves metric data from them, displays the collected data for visualization, and continuously monitors the metric data. See the following graph:

Figure 2. SNMP Workflow


Data Retrieving
After you import FSOS switches, AmpCon-Campus periodically establishes SNMP connections and sends GET or WALK requests for OIDs of monitoring items.
Data Processing
AmpCon-Campus automatically does unit conversion and cleansing for the returned monitoring item values, and stores the processed values in AmpCon-Campus databases.
Data Display
AmpCon-Campus displays returned monitoring item values in AmpCon-Campus dashboards.

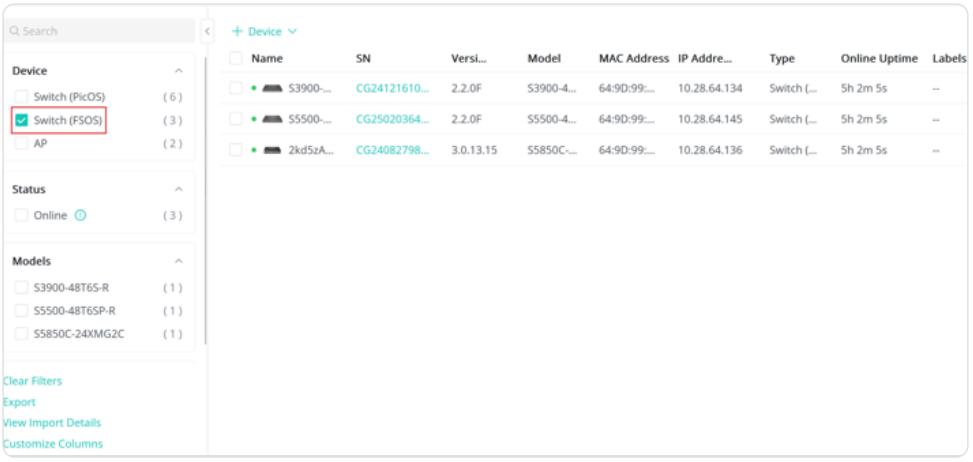
FSOS Switch List

On the “Devices” page, you can view the list of FSOS switches that fail to be onboarded, are being onboarded, or have already been onboarded to AmpCon-Campus.

- Viewing the FSOS List
- Filtering FSOS Switches
- Optional Operations
  - Exporting FSOS Switches
  - Deleting FSOS Switches
  - Moving FSOS Switches to Another Site

Viewing the FSOS List

1. In the AmpCon-Campus UI, select the site to which the FSOS switches belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, you can see all PicOS switches, FSOS switches, and access points (APs).
3. In the **Device** section of the sidebar, select **Switch (FSOS)** to display only FSOS switches.



By default, the following metrics are displayed:

Table 1. Device Metrics

Metric	Description
Name	The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side. If you do not enter an alias, AmpCon-Campus automatically generates an alias for each device. The alias contains the device model and the last four digits of the switch serial number (SN). **NOTE**

	Pay attention to the color of the circle in the **Name** column. Different circle colors indicate different statuses: • **Green:** The switch is in **Online** status, which means the switch is successfully onboarded to AmpCon-Campus and currently connected to AmpCon-Campus. • **Grey:** The switch is in **Offline** status, which means the switch is successfully onboarded to AmpCon-Campus but currently disconnected from AmpCon-Campus.
SN	The serial number of the switch.
Version	The FSOS version of the switch.
Model	The model of the switch.
MAC Address	The MAC address of the switch.
IP Address	The IP address of the switch.
Type	The type of the switch. For FSOS switches, the type is **Switch (FSOS)**.
Online Uptime	The elapsed time since the switch last connected to AmpCon-Campus. Hover over the time to view the switch's last connection time to AmpCon-Campus.
Labels	The labels of the switch.

4. To view more FSOS switch metrics, click **Customize Columns** in the sidebar, select or deselect metrics in the pop-up window, and then click **Done**.

   In addition to the metrics above, you can select the following metrics:

   Table 2. Additional FSOS Switch Metrics

Metric	Description
Site	The site to which the switch belongs.
Memory	The memory usage of the switch.

Temp	The temperature of the switch. **NOTE** The temperature data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - Device Temperature.

Tips

- The **Name**, **SN**, and **Model** columns cannot be deselected.
- To display only the default metrics, click **Restore**, and then click **Done**.
- You can select other metrics such as **Last Upgrade**, **AP Health**, and **Load**, but their values are displayed as **--** for FSOS switches. This is because these metrics apply only to access points (APs) or PicOS switches.

Filtering FSOS Switches

On the “Devices” page, you can filter FSOS switches by status, model, label, or online uptime.

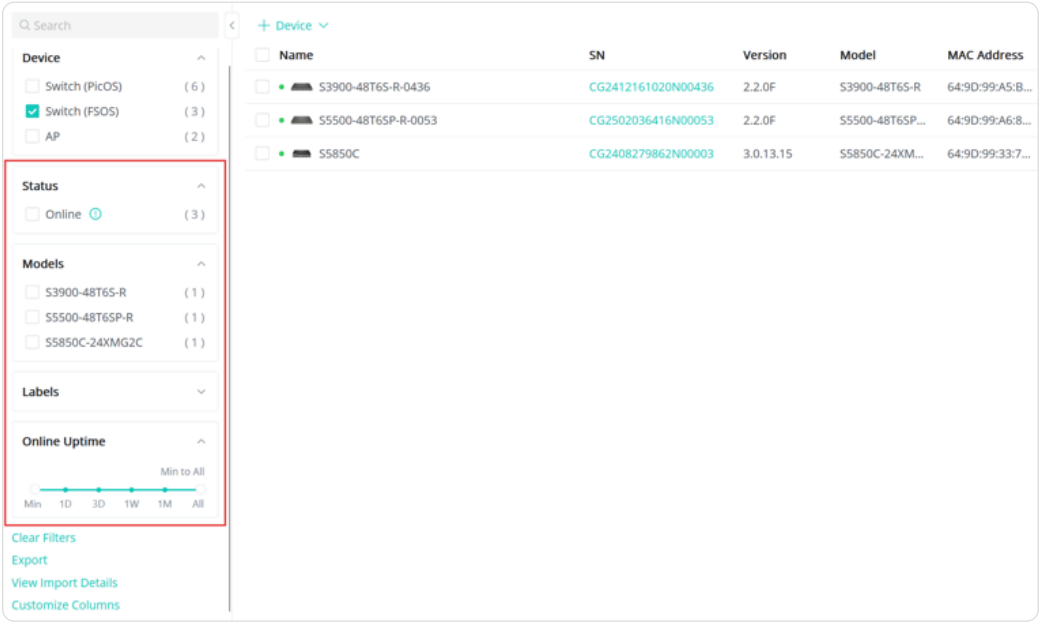


Table 3. Filter Conditions

Filter Condition	Description
Status	Select one or multiple switch statuses.

Models	Select one or multiple switch models.
Labels	Select one or multiple labels.
Online Uptime	**Online Uptime** means the continuous online duration of the switch. Select a time range in the **Online Uptime** section by clicking a start and end time point. The following time points can be clicked: • **Min** means the current time. • **1D** means 1 day. • **3D** means 3 days. • **1W** means 1 week. • **1M** means 1 month. • **All** means all times. **Examples:** • If you select the time range as **Min** to **All**, all switches are displayed. • If you select the time range as **Min** to **1D**, only online switches whose **Online Uptime** is less than or equal to 1 day are displayed. • If you select the time range as **3D** to **1M**, only online switches whose **Online Uptime** is between 3 days and 1 month are displayed. • If you select the time range as **1W** to **All**, only online switches whose **Online Uptime** is greater than or equal to 1 week are displayed.

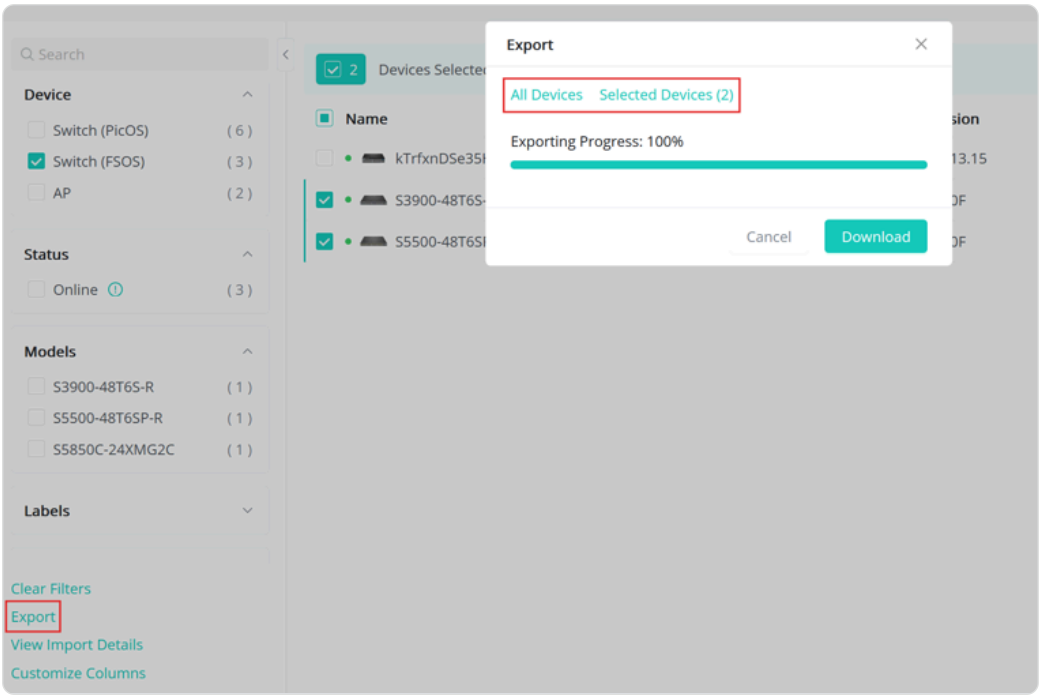
Tips

- If no devices match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of devices that match the filter option.
- To clear all these filter options, click **Clear Filters**.

Optional Operations

Exporting FSOS Switches

On the “Devices” page, you can export FSOS switches to a .csv file:

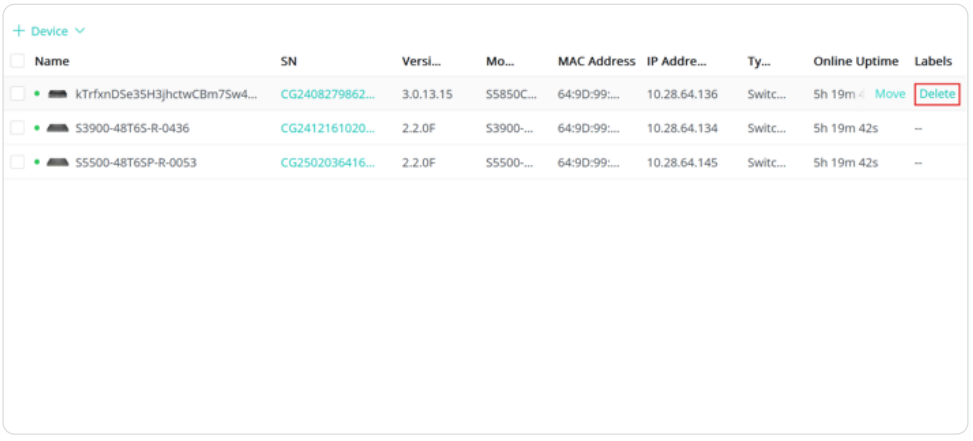


- To export all FSOS switches, click **Export**. In the pop-up window, click **All Devices**, wait for the export to complete, and then click **Download**.
- To export specific FSOS switches, select the switches, and then click **Export**. In the pop-up window, click **Selected Devices**, wait for the export to complete, and then click **Download**.

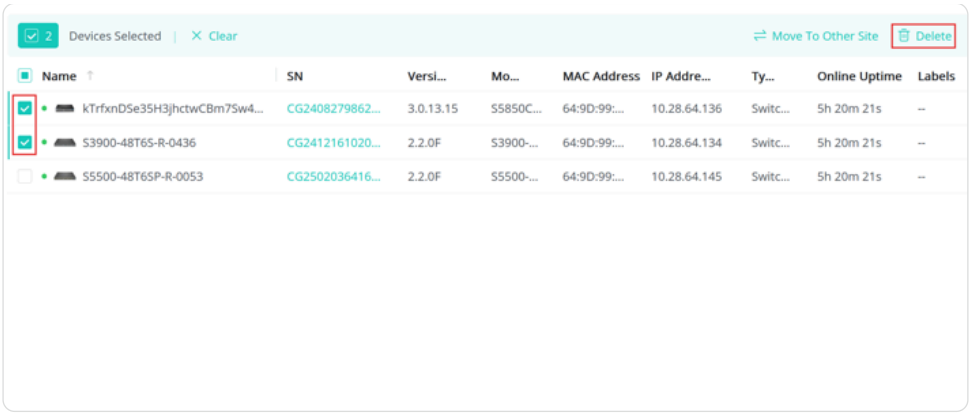
> **Tip**
>
> To clear the switch selection, click **Clear**.

Deleting FSOS Switches

- To delete a **single** FSOS switch, hover over the switch, and then click **Delete**. In the pop-up window, click **Yes**.



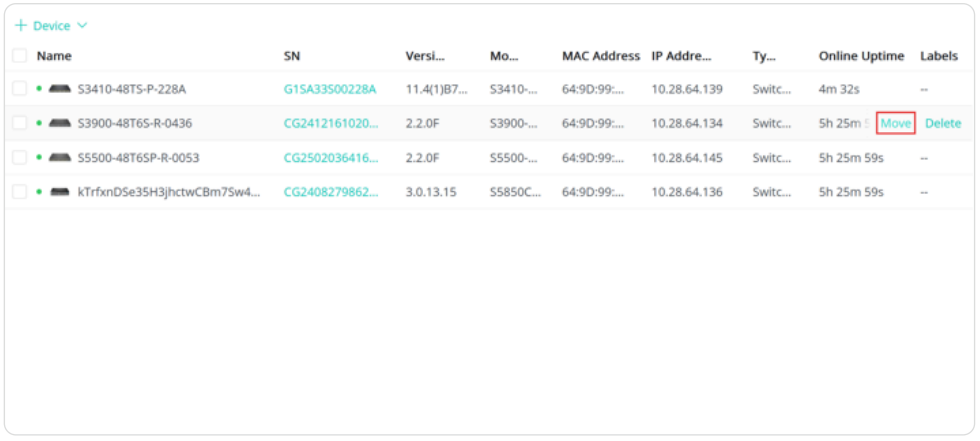
- To delete **multiple** FSOS switches, select the switches, and then click **Delete**. In the pop-up window, click **Yes**.



Moving FSOS Switches to Another Site

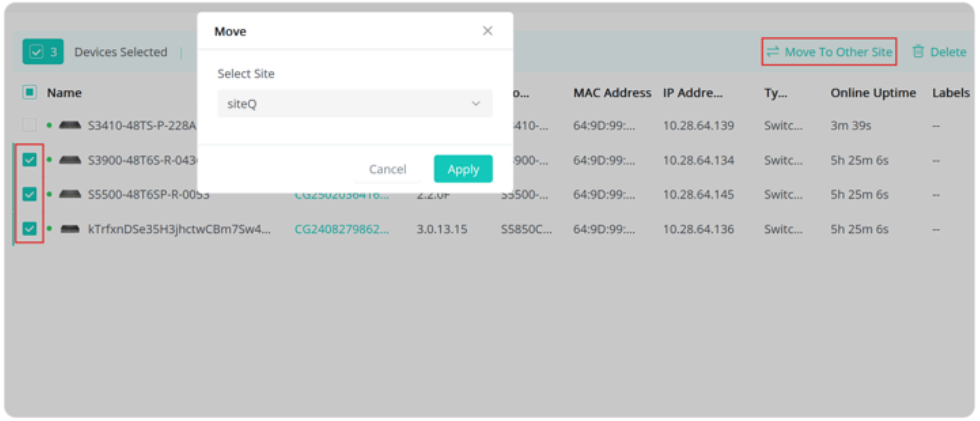
- To move a **single** switch to another site, hover over the switch, and then click **Move**.

  In the pop-up window, select the new site, and then click **Apply**.



- To move **multiple** switches to another site, select the switches, and then click **Move To Other Site**.

  In the pop-up window, select the new site, and then click **Apply**.



Information of an FSOS Switch

Click the **Devices** icon from the navigation bar. On the “Devices” page, click an FSOS switch. You can see a side panel on the right.

In the side panel, you can see detailed information about the switch.

Guidelines
Basic Switch Information
Deep Insights into an FSOS Switch
General Configurations and Management Operations

Guidelines

- AmpCon-Campus can monitor only the FSOS switches that have been successfully onboarded.
- Some data might not be displayed for offline FSOS switches (switches disconnected from AmpCon-Campus).

Basic Switch Information

In the **Overview** tab of the side panel, you can see basic information about the FSOS switch.

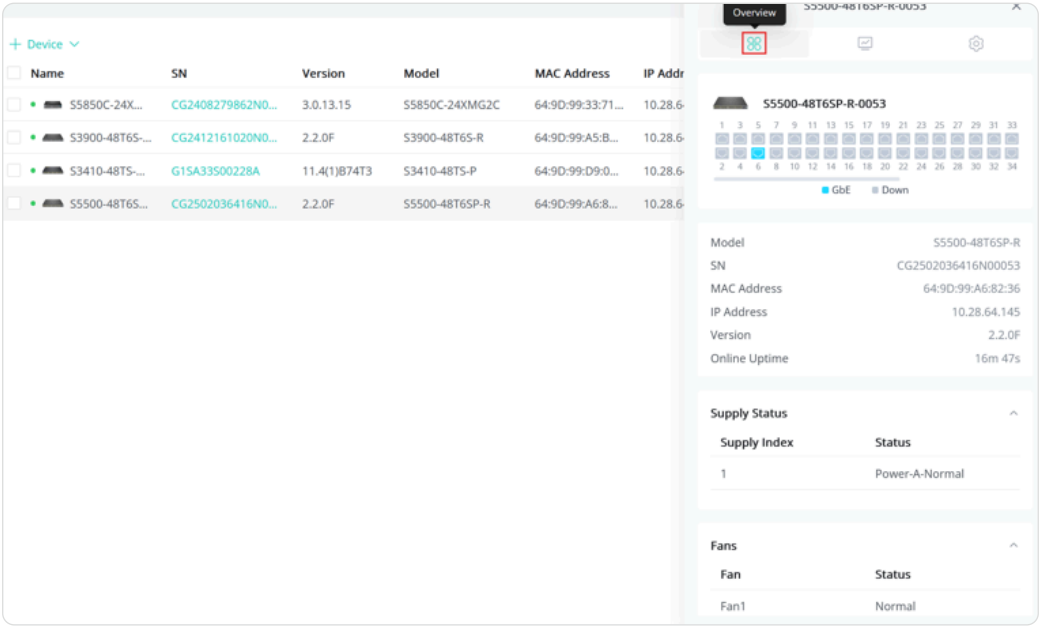
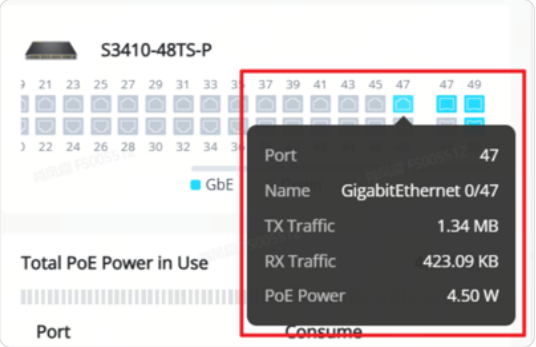
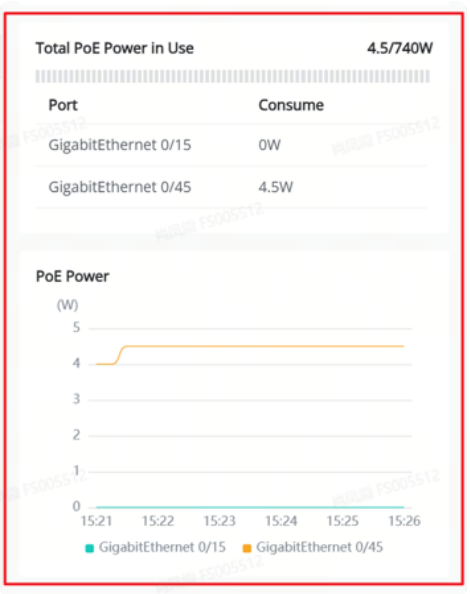
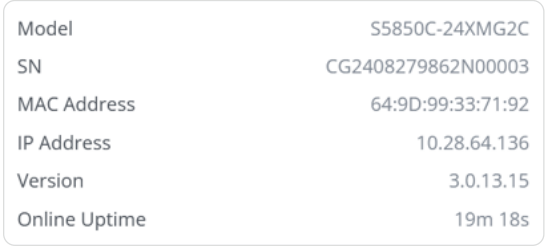
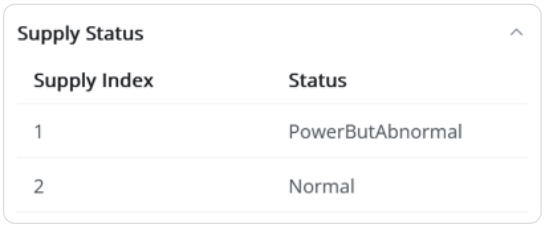
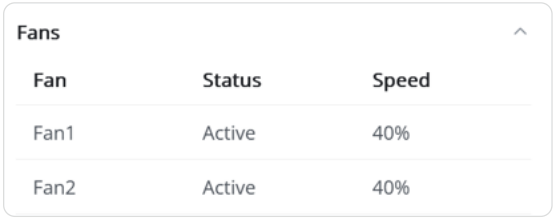


Table 1. FSOS Switch Overview

Metric	Description
Switch Image and Alias	The switch image and alias.  S5850C-24XMG2C-0003

Port Panel	The port panel containing all ports of the switch. Hover over a port, and then you can see the following information: • **Port:** The port number. • **Name:** The port name. • **TX Traffic:** The total amount of data emitted from the port. • **RX Traffic:** The total amount of data received by the port. • **PoE Power:** The real-time PoE output power of the port. This metric is not displayed for non-PoE ports.  **NOTEs** • Different speeds of ports are marked in different colors. • The ports in **Down** status are displayed in grey. • If a physical port is split into multiple ports, hover over the physical port to view information for the physical port and each split port.
PoE	The PoE-related information on the switch: • The real-time total PoE output power of the switch, and the maximum PoE output power. • The progress bar showing the ratio of real-time total PoE output power to the maximum PoE output power. If AmpCon-Campus cannot retrieve the maximum PoE output power, the progress bar will not be displayed. • The real-time PoE output power of each switch port. ◦ **Port Name:** The port name. ◦ **Consume:** The actual Power Sourcing Equipment (PSE) output power of the PoE port, accurate to two

	decimal places. • The trend graph of actual PSE output power for each PoE port.  **NOTEs** • PoE-related data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - PoE. • Only the ports in Up status are displayed in this section.
Basic Information	The basic information of the switch: • **Model:** The model of the switch. • **SN:** The SN of the switch. • **MAC Address:** The MAC address of the switch. • **IP Address:** The IP address of the switch. • **Version:** The FSOS version of the switch. • **Online Uptime:** The elapsed time since the switch last connected to AmpCon-Campus. Hover over the time to view the switch's last connection time to AmpCon-Campus. 

Supply Status	The latest retrieved index and status of Power Supply Unit (PSU). • **Supply Index:** The unique identifier of the PSU on the switch. For example, the supply index **1** represents the PSU 1. • **Status:** The power status of the PSU. Different FSOS switch vendors use different PSU statuses. For definitions of a power status, refer to the FSOS switch vendor documentation.  Supply Status Supply Index | Status 1 | PowerButAbnormal 2 | Normal **NOTE** Supply status data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - Supply Status.
Fans	The latest retrieved fan name, status, and speed. • **Name:** The fan name. • **Status:** The status of the fan. Different FSOS switch vendors use different fan statuses. For definitions of the fan status, refer to the FSOS switch vendor documentation. • **Speed:** The fan speed.  Fans Fan | Status | Speed Fan1 | Active | 40% Fan2 | Active | 40% **NOTE** Some fan-related data is not displayed for specific FSOS switches. For more information, see Monitoring Limitations - Fan.

Deep Insights into an FSOS Switch

In the **Insight** tab of the side panel, you can gain deep insights into the FSOS switch.

Switch Statistics

In the **Statistics** section, you can see the following trend graphs:

Table 2. Statistic Trend Graphs

Trend Graph	Description
Flash Usage	The used, free, and total flash storage size. **NOTE** Flash data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - Flash Usage.
CPU	The CPU utilization for the latest 5 seconds.
Memory	The memory usage. **NOTE** Memory data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - Memory.
Temperature	The temperature of the switch. **NOTE** Temperature data is not displayed for some FSOS switches. For more information, see Monitoring Limitations - Device Temperature.

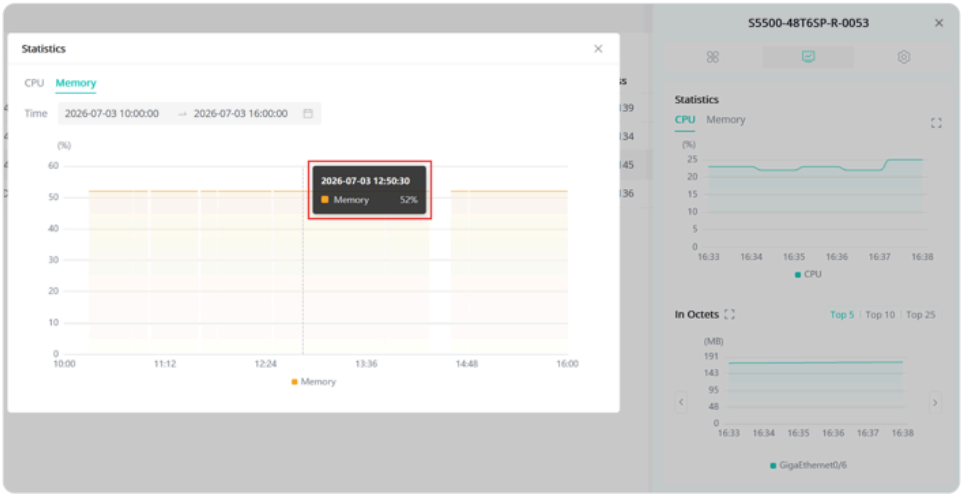
- By default, the **CPU**, **Memory**, and **Temperature** trend graphs display data in the last 5 minutes. To change the display time range, click the expand icon, and then select the start and end time point in the pop-up window.

  NOTEs

  - All time points use your browser's time zone.
  - Only the data in the last 1 month can be displayed.



- To view the metric details at a specific time point, hover over that time point.



Switch Traffic

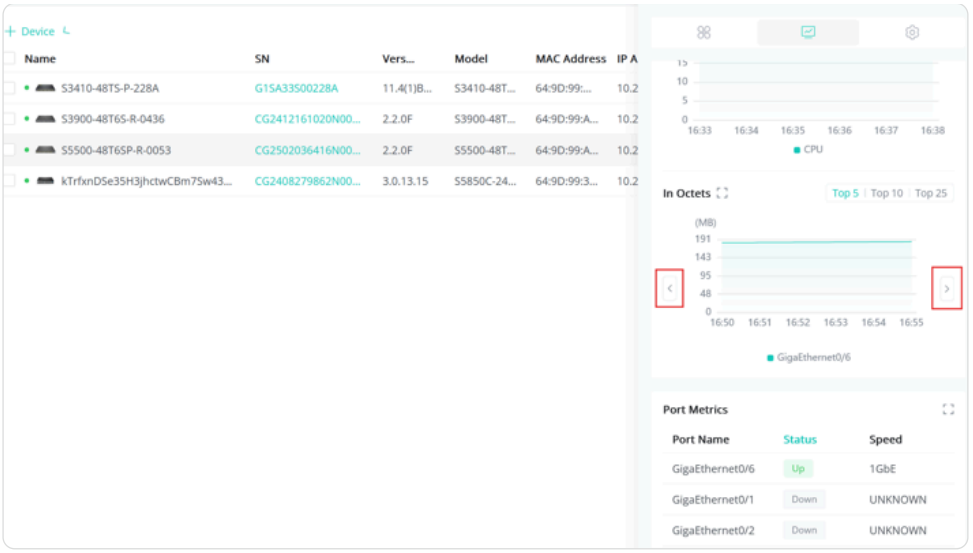
You can see the following trend graphs related to switch traffic:

Table 3. Switch Traffic Trend Graphs

Trend Graph	Description
In Octets	The number of octets (8-bit bytes) received by the switch port. **NOTE** The maximum value is 2^64 - 1. If the retrieved value exceeds this limit, the displayed value is calculated as follows: **Displayed value = Retrieved value – (2^64 – 1)**
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.

	NOTE The maximum value is 2^64 - 1. If the retrieved value exceeds this limit, the displayed value is calculated as follows: **Displayed value = Retrieved value – (2^64 – 1)**
In Packets Discarded	The number of incoming packets that the switch port discards due to reasons like buffer exceptions.
Out Packets Discarded	The number of outgoing packets that the switch port discards due to reasons like traffic control.
In Packets with Errors	The number of incoming packets that contain errors like Cyclic Redundancy Check (CRC) errors.
Out Packets with Errors	The number of outgoing packets that contain errors like link anomalies.
RX Power	The amount of optical power received by the optical module connected to the switch port. It's measured in dBm.
TX Power	The amount of optical power emitted by the optical module connected to the switch port. It's measured in dBm.
Bias Current	The bias current of the optical module connected to the switch port. It's measured in milliamperes (mA).
Bias Voltage	The bias voltage of the optical module connected to the switch port. It's measured in volts (V).
Optical Module Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).

- To check the last and next trend graph, click **<** or **>**.



- By default, the trend graphs display data in the last 5 minutes. To change the display time range, click the expand icon, and then select the start and end time point in the pop-up window.

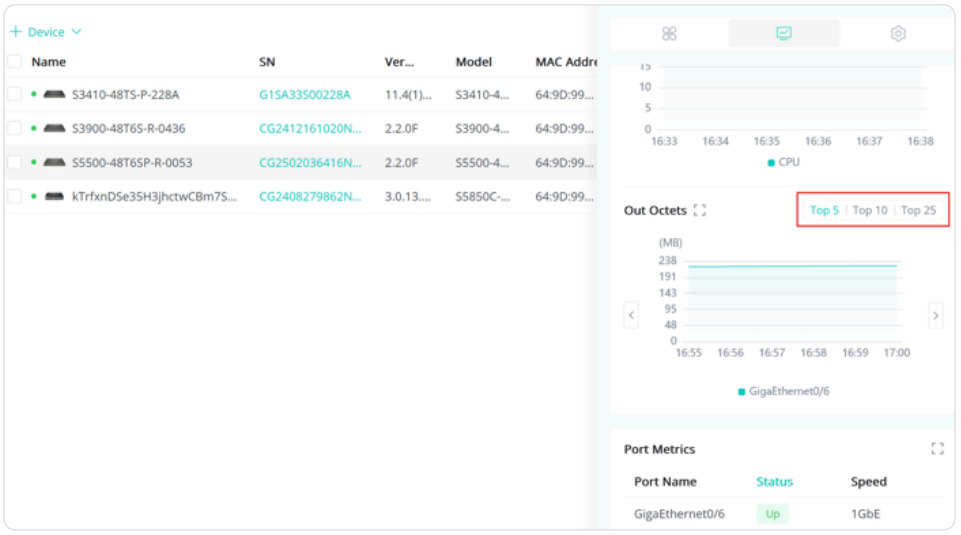
> **NOTEs**
>
> - All time points use your browser's time zone.
> - Only the data in the last 1 month can be displayed.



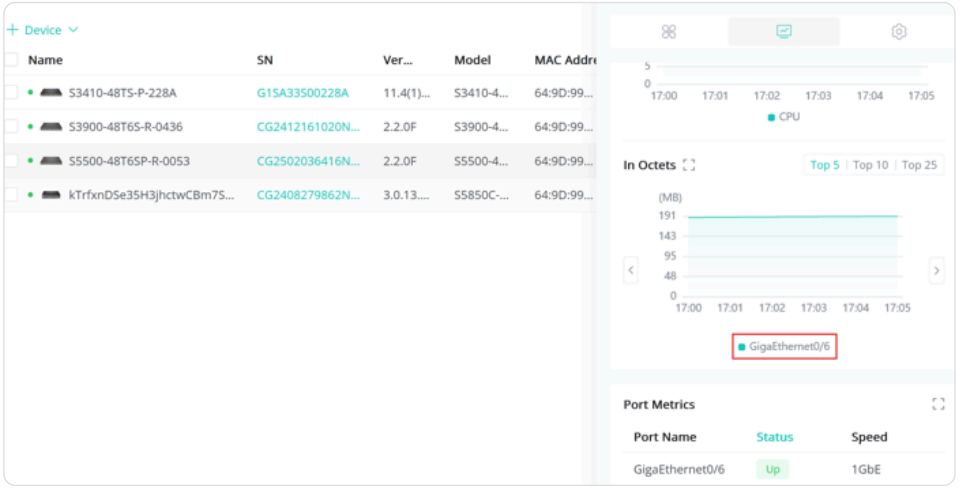
- To specify how many ports that you want to monitor, select one of the following options:
  - **Top 5:** The 5 switch ports with the largest values. By default, **Top 5** is selected.
  - **Top 10:** The 10 switch ports with the largest values.
  - **Top 25:** The 25 switch ports with the largest values.

> **NOTEs**
>
> - Only the ports that are up at some time within the selected time range can be displayed. If a switch port goes down during a certain period, its metric data for that period will not be displayed.

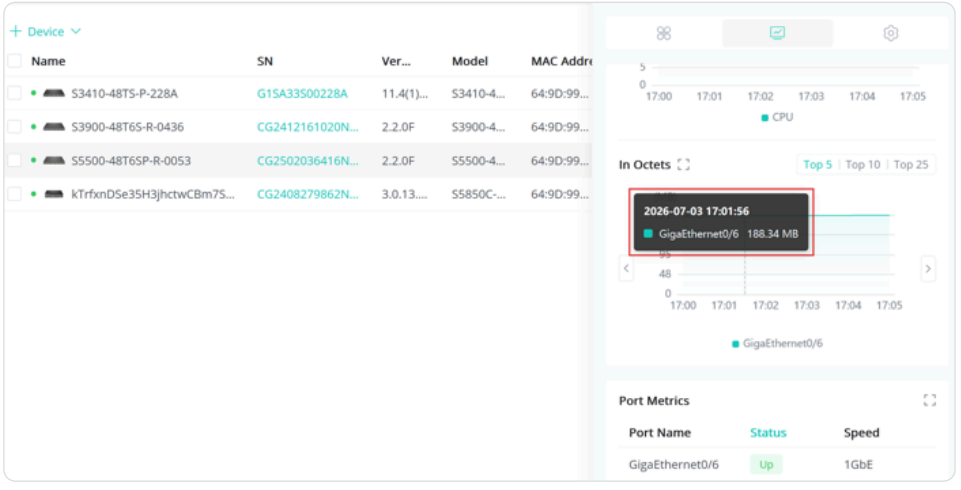
- Even though **Top X** (such as **Top 5**) is selected, you might see fewer than the selected number of switch ports in the trend graph when some ports are down.



- To display or hide the data of a switch port, click the square before the port.



- To view the metric details at a specific time point, hover over that time point.



Switch Ports

In the **Port Metrics** section, you can see the following metrics related to switch ports:

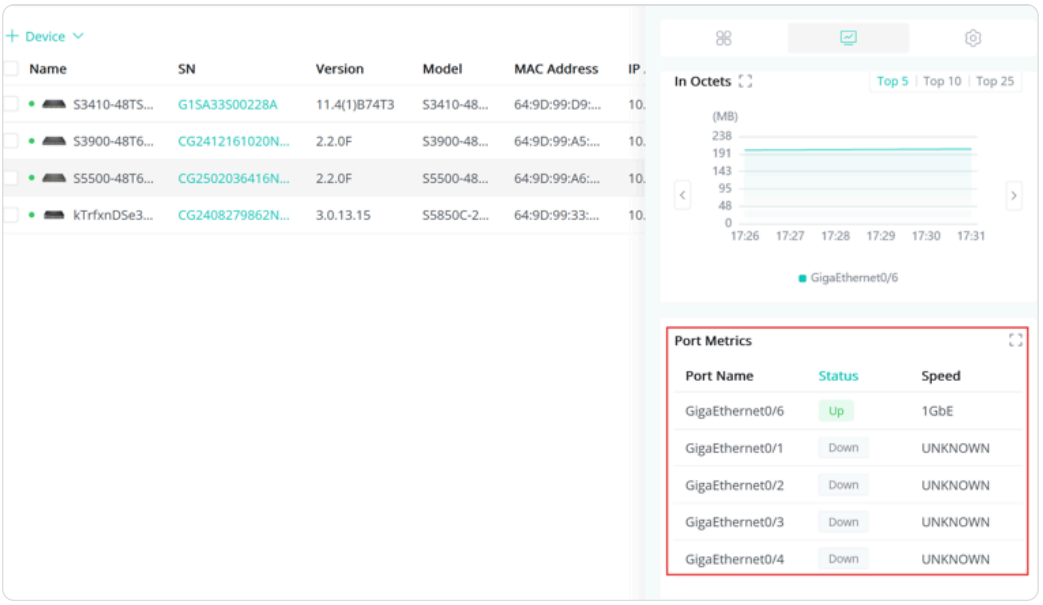


Table 4. Switch Port Metrics

Metric	Description
Port Name	The name of the switch port. **NOTE** If a physical port is split into multiple ports, you can see an expand icon before the physical port name. Click the expand icon to view information for each split port.
Status	The status of the switch port, **Up** or **Down**.
Speed	The port speed. If the port is in **Down** status, the value is **UNKNOWN**.

To see more metrics, click the expand icon. You can then see the following metrics in addition to those listed above:

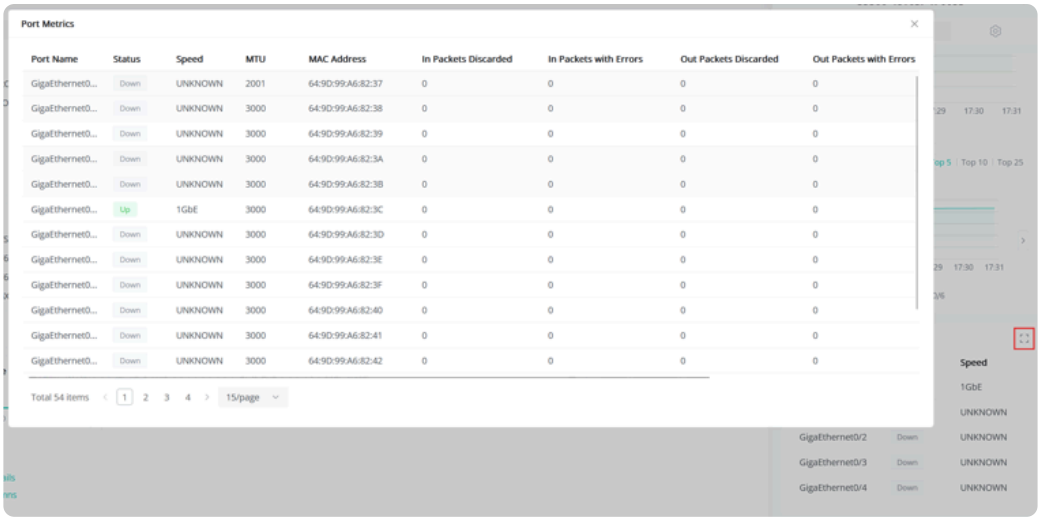


Table 5. Additional Port Metrics

Metric	Description
MTU	The largest size of a data packet that can be transmitted over a network without being fragmented. It's measured in bytes.
MAC Address	The MAC address of the switch port.
In Packets Discarded	The number of incoming packets that the switch port discards due to reasons like buffer exceptions. **NOTEs** • The metric value keeps increasing until it reaches the allowed maximum value 4,294,967,295 (2^32 - 1). • After the metric value reaches 4,294,967,295, the value will be reset to 0 and then start counting again.
In Packets with Errors	The number of incoming packets that contain errors like Cyclic Redundancy Check (CRC) errors. **NOTEs** • The metric value keeps increasing until it reaches the allowed maximum value 4,294,967,295 (2^32 - 1). • After the metric value reaches 4,294,967,295, the value will be reset to 0 and then start counting again.

Out Packets Discarded	The number of outgoing packets that the switch port discards due to reasons like traffic control. **NOTEs** • The metric value keeps increasing until it reaches the allowed maximum value 4,294,967,295 (2^32 - 1). • After the metric value reaches 4,294,967,295, the value will be reset to 0 and then start counting again.
Out Packets with Errors	The number of outgoing packets that contain errors like link anomalies. **NOTEs** • The metric value keeps increasing until it reaches the allowed maximum value 4,294,967,295 (2^32 - 1). • After the metric value reaches 4,294,967,295, the value will be reset to 0 and then start counting again.
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
In Octets	The number of octets (8-bit bytes) received by the switch port.

General Configurations and Management Operations

In the **Setting** tab of the side panel, you can view general configurations or perform management operations for the FSOS switch.

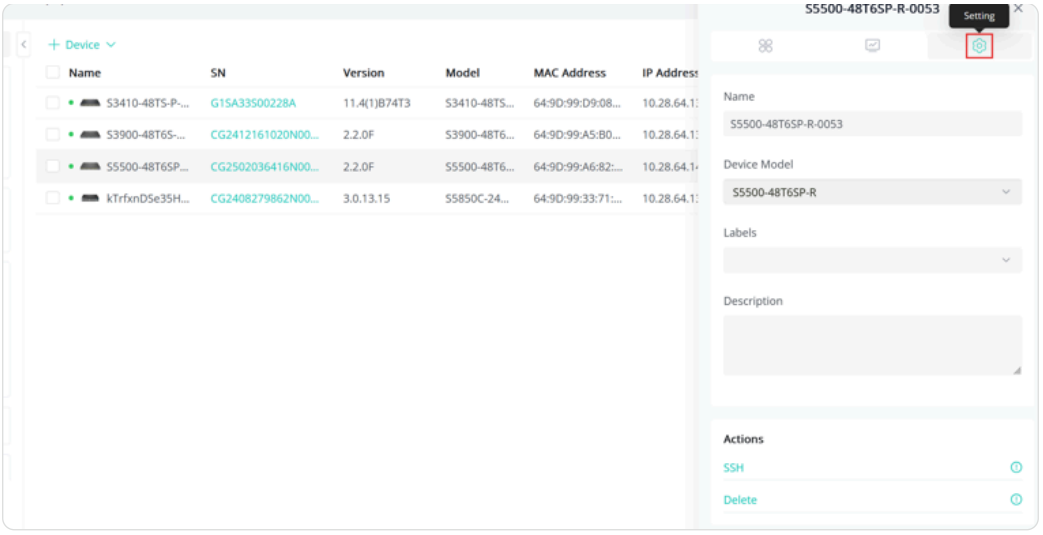


Table 6. General Switch Configurations

Configuration	Description
Name	The alias of the switch. Aliases are used to differentiate devices in the AmpCon-Campus UI and will not be pushed to the device side. The alias can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The alias cannot start or end with a hyphen or underscore.
Device Model	The model of the switch. AmpCon-Campus automatically retrieves the switch model and displays it here. The model cannot be changed.
Labels	The switch labels used for switch filtering and management. You can select one or multiple labels. To add a new label, click the **Labels** drop-down list, and then click **Create Label**. Each label can contain only letters and numbers and can contain at most 64 characters.
Description	The description of the switch. The description can contain at most 256 characters.

In the **Actions** section, you can do the following actions:

Table 7. Action Buttons

Button	Description

SSH	To connect to the switch from the AmpCon-Campus UI by creating an SSH session, click **SSH**. In the pop-up window, enter the SSH username and password, and then click **Apply**. **NOTEs** • Ensure the username and password are valid for switch login. Otherwise, the SSH session cannot be established. • The username must start with a letter or underscore and can contain letters, digits, underscores, hyphens, or a trailing $. • The username can contain at most 32 characters. • Uppercase letters are not supported on S3270 and S3410 series switches. • Only ASCII characters are supported.
Delete	To delete the switch from AmpCon-Campus, click **Delete**. In the pop-up window, click **Yes**.

Monitoring Limitations

See the following monitoring limitations for FSOS switches:

- Device Temperature
- Fan
- Flash Usage
- Memory
- PoE
- Supply Status

Device Temperature

For the following switch models, the device temperature data is not displayed:

- S3900-48T6S-R
- S5500-48T6SP-R
- IES3110-8TF-R
- IES3110-8TFP-R

Fan

- For the following switch models, the fan status data is not displayed:
  - S3100-8TMS-P
  - S3100-16TMS-P
  - S3100-16TF-P
  - S3100-16TF
  - S3270-10TM
  - S3270-24TM
  - S3150-8T2FP
  - S3260-8T2FP
  - S3400-24T4FP
  - S3700-24T4F
  - IES3110-8TFM-P
  - IES3110-8TF-R
  - IES3110-8TFP-R
  - TSN3220-10S-U
- For the following switch models, the fan speed data is not displayed:
  - S3100-8TMS-P
  - S3100-16TMS-P
  - S3100-16TF-P
  - S3100-16TF

- S3270-24TM-P
- S3270-10TM-P
- S3270-10TM
- S3270-24TM
- S3270-48TM
- S3410-48TS-P
- S3410-24TF-P
- S3410-24TS-P
- S3150-8T2FP
- S3910-24TF
- S3260-8T2FP
- S3400-24T4FP
- S3700-24T4F
- S3900-48T6S-R
- S5500-48T6SP-R
- IES3110-8TFM-P
- IES3110-8TF-R
- IES3110-8TFP-R
- TSN3220-10S-U

Flash Usage

For the following switch models, the flash data is not displayed:

- S3950-4T12S-R
- S5800-48T4S
- S5800-48MBQ
- S5850-48S6Q-R
- S5850-48B8C
- S5850-24B4C
- S5850-24XMG-U
- S8050-20Q4C
- S5850-16Q8C
- S5850C-24XMG2C
- S5850C-24S2C
- S3150-8T2FP
- S3260-8T2FP
- S3400-24T4FP

- S3700-24T4F
- S3900-48T6S-R
- S5500-48T6SP-R
- IES3110-8TF-R
- IES3110-8TFP-R

Memory

For the following switch models, the memory data is not displayed:

- S3150-8T2FP
- S3260-8T2FP
- S3400-24T4FP
- S3700-24T4F
- S3900-48T6S-R
- S5500-48T6SP-R
- IES3110-8TFM-P

PoE

For the following switch models, the PoE information is not displayed:

- S3100-16TF
- S3270-10TM
- S3270-24TM
- S3270-48TM
- S3910-48TF
- S3910-24TF
- S3910-24TS
- S3910-48TS
- S5810-48FS
- S5810-28FS
- S5810-28TS
- S5810-48TS
- S5860-20SQ
- S5860-24XMG
- S5860-48XMG
- S3950-4T12S-R
- S5800-48T4S
- S5800-48MBQ

- S5850-48S6Q-R
- S5850-48B8C
- S5850-24B4C
- S5860-48SC
- S8050-20Q4C
- S8550-16Q8C
- S5850C-24XMG2C
- S5850C-24S2C
- S5850-24XMG-U
- S3150-8T2FP
- S3260-8T2FP
- S3400-24T4FP
- S3700-24T4F
- S3900-48T6S-R
- S5500-48T6SP-R
- IES3110-8TFM-P
- IES3110-8TF-R

Supply Status

For the following switch models, the supply status data is not displayed:

- S3150-8T2FP
- S3260-8T2FP
- S3400-24T4FP
- S3700-24T4F
- S3950-4T12S-R
- IES3110-8TF-R
- IES3110-8TFP-R

Access Points

After onboarding access points (APs) to AmpCon-Campus, you can continuously monitor the APs for performance analysis and fault diagnosis.

See the following child topics:

- AP List
- Basic Information of an AP
- Deep Insights into an AP
- Configurations and Operations of an AP

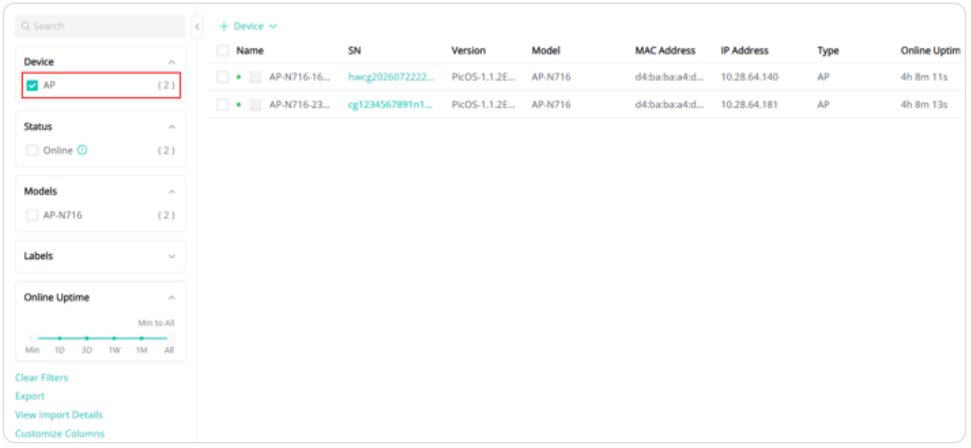
AP List

You can view the list of access points (APs) that fail to be onboarded, are being onboarded, or are already onboarded to AmpCon-Campus.

Viewing the AP List
Filtering APs in the List
Exporting APs in the List

Viewing the AP List

1. In the AmpCon-Campus UI, select the site to which the APs belong.
2. Click the **Devices** icon from the navigation bar. On the “Devices” page, you can see all PicOS switches, FSOS switches, and APs.
3. In the **Device** section of the sidebar, select **AP** to display only APs.



By default, the following metrics are displayed:

Table 1. AP Metrics

Metric	Description
Name	The AP alias. Aliases are used to differentiate APs in the AmpCon-Campus UI and will not be pushed to the AP side. If you do not enter the alias, AmpCon-Campus automatically generates an alias for each device. The alias contains the device model and the last four digits of the AP serial number (SN). **NOTE** Pay attention to the color of the circle in the **Name** column. Different circle colors indicate different statuses:

	• **Green:** The AP is in **Online** status, which means the AP is successfully onboarded to AmpCon-Campus and is currently connected to AmpCon-Campus. • **Grey:** The AP is in **Offline** status, which means the AP is successfully onboarded to AmpCon-Campus but is currently disconnected from AmpCon-Campus. • **Yellow:** The AP is in **Never Online** status, which means the AP has been added to AmpCon-Campus but has never connected to AmpCon-Campus.
SN	The serial number of the AP.
Version	The version of the AP firmware.
Model	The model of the AP.
MAC Address	The MAC address of the AP.
IP Address	The IP address of the AP.
Type	The type of the device. For APs, the type is **AP**.
Online Uptime	The elapsed time since the AP last connected to AmpCon-Campus. Hover over the time to view the AP's last connection time to AmpCon-Campus.
Labels	The labels of the AP.

4. To view more AP metrics, click **Customize Columns** in the sidebar, select or deselect metrics in the pop-up window, and then click **Done**.

   The following AP metrics can also be displayed:

   Table 2. Additional AP Metrics

Metric	Description
Site	The site to which the AP belongs.
Memory	The memory usage of the AP in percentage.

Temp	The temperature of the AP. The unit is Celsius (°C).
Last Upgrade	The last time when the AP firmware was upgraded.
AP Health	The health grade of the AP. AmpCon-Campus calculates the health grade based on DHCP, DNS, RADIUS, and SSID health: **AP Health = (1 - interfaces with errors / total interfaces) × 100 %** In the following example, **2** interfaces have DNS issues, and the total number of interfaces is **4**. Therefore, the **AP Health** is **50%**. **AP Health = (1 - 2 / 4) × 100% = 50%** 
Load	The CPU load percentage of the AP.
First Connect	The time when the AP first connected to AmpCon-Campus.
GPS	The longitude and latitude coordinates. **NOTE** The **GPS** value can be displayed only when the AP supports GPS.
Last Connect	The time when the AP last connected to AmpCon-Campus.
Last Contact	The time when the AP last communicated with AmpCon-Campus.
RX	The total traffic received by AmpCon-Campus from the AP.
TX	The total traffic transmitted from AmpCon-Campus to the AP. **NOTE**

	The **RX** and **TX** metrics are defined from the perspective of AmpCon-Campus.
2.4G	The count of wireless clients connected to the 2.4G radio.
5G	The count of wireless clients connected to the 5G radio.
6G	The count of wireless clients connected to the 6G radio.
Connect Reason	The reason for the last connection between the AP and AmpCon-Campus. The following reasons are supported: • **Coldboot**: The AP is powered on, or the process to connect the AP to AmpCon-Campus restarts. • **Socket**: The AP is re-connected to AmpCon-Campus after a disconnection. • **Reboot**: The AP is rebooted. • **Recovery**: The AP is re-connected to AmpCon-Campus after a recovery. • **Upgrade Failed**: The AP is re-connected to AmpCon-Campus after an upgrade failure. • **Crashlog**: The AP is re-connected to AmpCon-Campus after a crash.

Tips

- The **Name**, **SN**, and **Model** columns cannot be deselected.
- You can select **Hardware ID** and **Backup Schedule**, but their values appear as **--** for APs. This is because these metrics apply only to switches.
- To display only the default metrics, click **Restore**.

Filtering APs in the List

On the “Devices” page, you can filter APs by AP status, model, label, or online uptime.

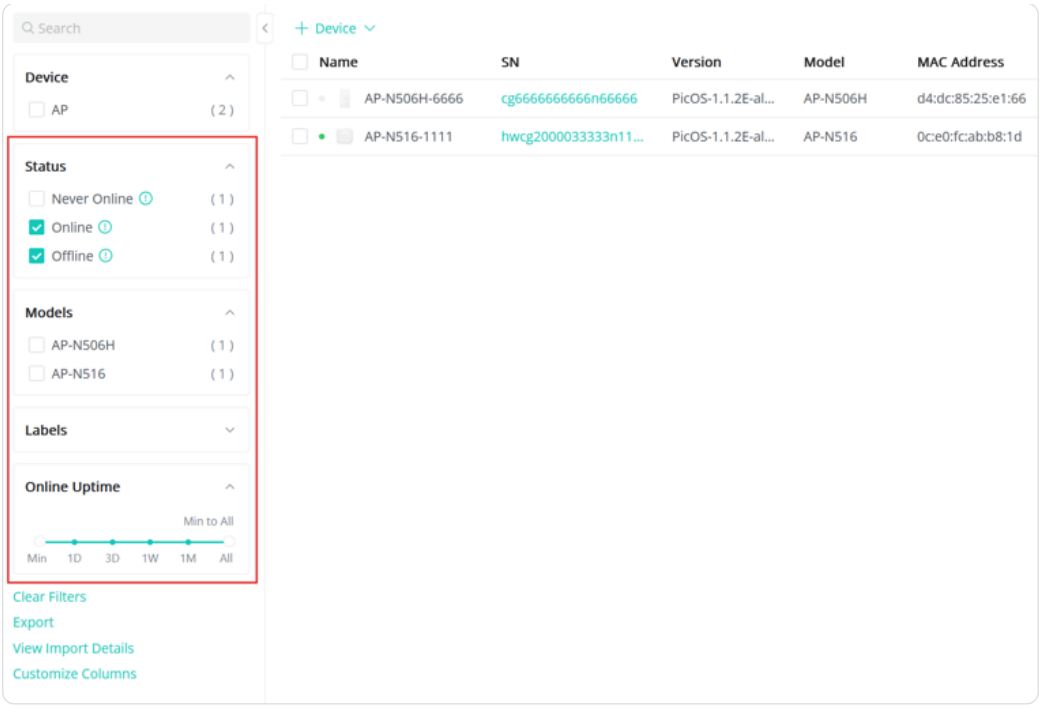


Table 3. Filter Sections

Filter Section	Description
Status	Select one or multiple AP statuses. The following AP statuses are supported: • **Online:** The AP is successfully onboarded to AmpCon-Campus and is currently connected to AmpCon-Campus. • **Offline:** The AP is successfully onboarded to AmpCon-Campus but is currently disconnected from AmpCon-Campus. • **Never Online:** The AP has been added to AmpCon-Campus but has never connected to AmpCon-Campus.
Models	Select one or multiple AP models.
Labels	Select one or multiple labels.
Online Uptime	The continuous online duration of the AP. Select a time range in the **Online Uptime** section by clicking the start and end time point. The following time points can be clicked: • **Min** means the current time. • **1D** means 1 day. • **3D** means 3 days.

- **1W** means 1 week.
- **1M** means 1 month.
- **All** means all times.

Examples:

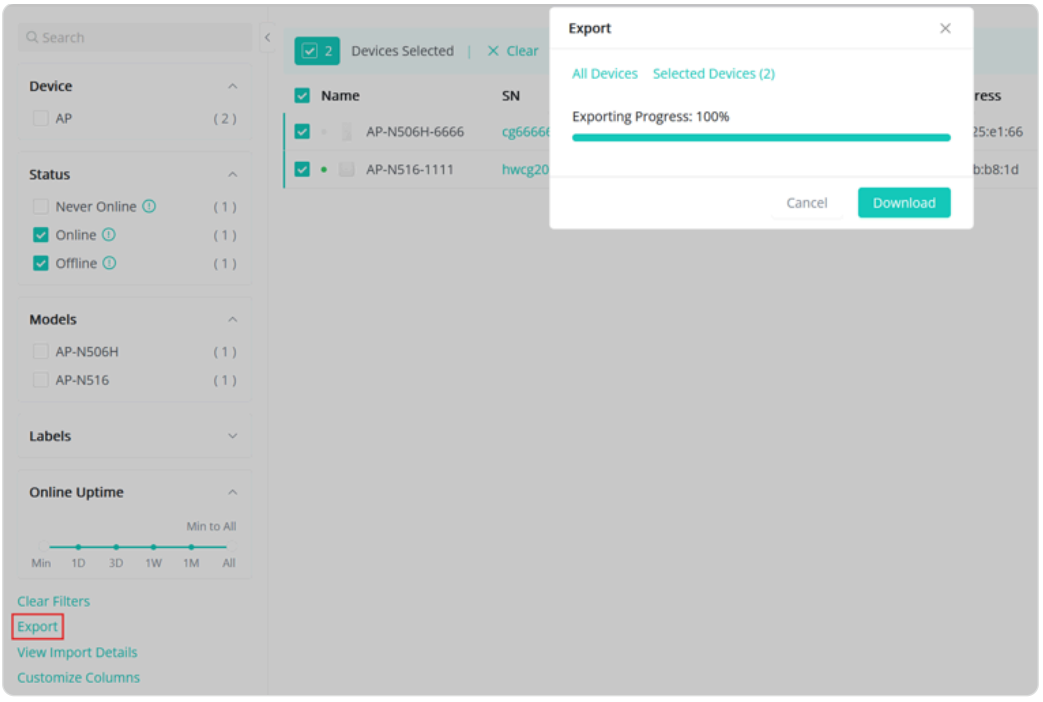
- If you select the time range as **Min** to **All**, all APs are displayed.
- If you select the time range as **3D** to **1M**, only online APs whose **Online Uptime** is between 3 days and 1 month are displayed.
- If you select the time range as **Min** to **1D**, only online APs whose **Online Uptime** is less than or equal to 1 day are displayed.
- If you select the time range as **1W** to **All**, only online APs whose **Online Uptime** is greater than or equal to 1 week are displayed.

Tips

- If no devices match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of devices that match the filter option.
- To clear all these filter options, click **Clear Filters**.

Exporting APs in the List

On the “Devices” page, you can export APs to a .csv file:



- To export all APs, click **Export**. In the pop-up window, click **All Devices**, wait for the export to complete, and then click **Download**.
- To export specific APs, select the APs in the device list, and then click **Export**. In the pop-up window, click **Selected Devices**, wait for the export to complete, and then click **Download**.

> **Tip**
>
> To clear the switch selection, click **Clear**.

Basic Information of an AP

Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP. You can see a side panel on the right.

In the **Overview** tab of the side panel, you can view basic information of the AP.

Guidelines
Basic AP Information

Guidelines

- AmpCon-Campus can monitor only the APs that have been successfully onboarded.
- Some data in the **Overview** tab is not displayed for offline APs (APs disconnected from AmpCon-Campus).

Basic AP Information

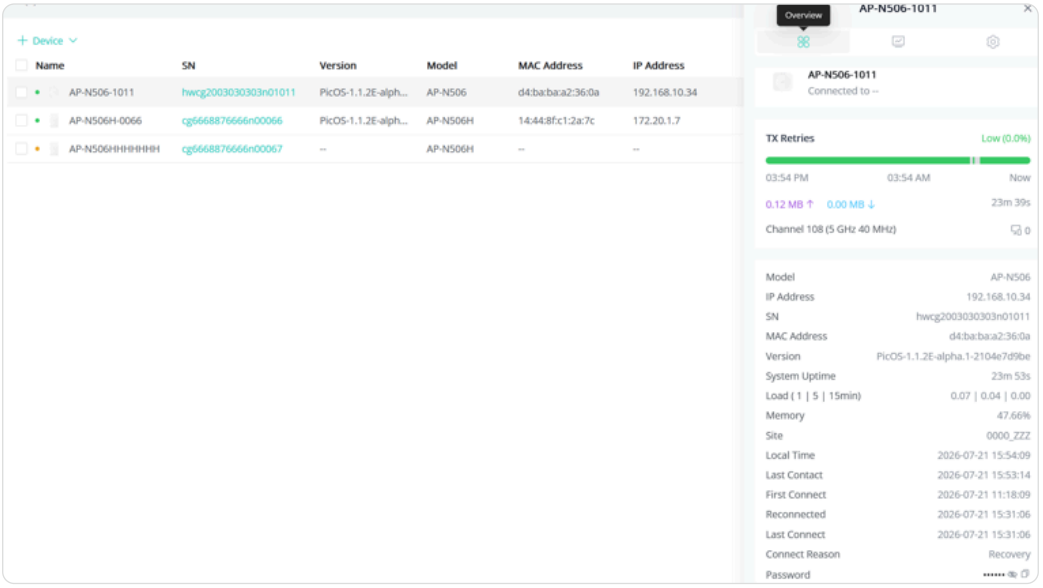
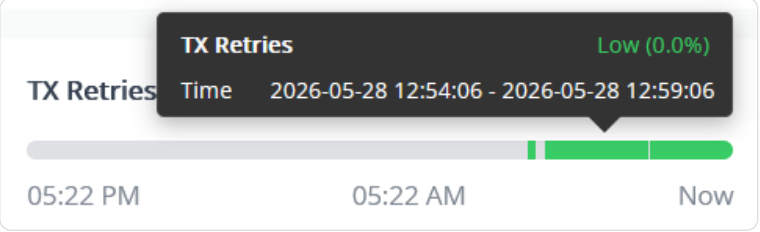
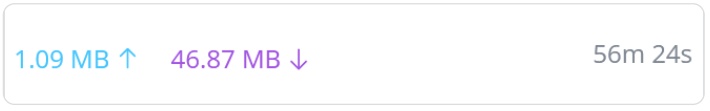
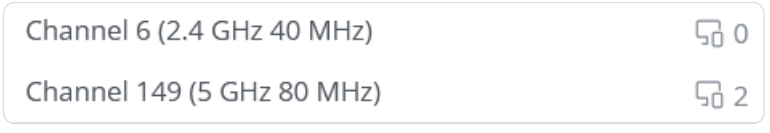


Table 1. AP Overview

Metric	Description
AP Name	The AP picture and the AP name.
Uplink Switch or Mesh Root AP	The uplink switch or mesh root AP information. • For non-mesh child APs: If the AP is connected to an uplink switch, the switch name and port are displayed, such as **Connected to S5580-48Y-0016 Port 56**. If the AP is online (connected to AmpCon-Campus) but not connected to any switch, **Connected to --** is

	displayed. If the AP is offline (disconnected from AmpCon-Campus), **Last Connected to --** is displayed. • For mesh child APs: If the AP is connected to a mesh root AP, the mesh root AP name is displayed, such as **Meshing to AP-N506H-11111**. If the AP is online (connected to AmpCon-Campus) but not connected to any mesh root AP, **Meshing to --** is displayed. If the AP is offline (disconnected from AmpCon-Campus), **Last Meshed to --** is displayed. • If the uplink switch or mesh root AP is managed by AmpCon-Campus, you can click the uplink switch or mesh root AP alias to open its side panel.
TX Retries	The retransmission rate of the AP. The retransmission rate is calculated as follows: **Retransmission Rate = TX_Retries / (TX_Retries + TX_Packets)** **TX_Packets** means the count of packets successfully sent from the AP to wireless clients. **TX_Retries** means the count of retransmitted packets sent from the AP to wireless clients. The bar chart displays the retransmission rates in the last 1 day. Hover over a time point in the bar chart, and then you can see the retransmission rate during the related time range (5 minutes).  **NOTE** Different retransmission rates are marked in different colors:

	• **Grey:** The retransmission rate is not collected by AmpCon-Campus. The retransmission rate is highlighted with the word **Not Reported**. • **Green:** The retransmission rate ranges from 0 to 20% (including 0 and 20%). The retransmission rate is highlighted with the word **Low**. • **Yellow:** The retransmission rate ranges from 20% to 30% (including 30%). The retransmission rate is highlighted with the word **Medium**. • **Red:** The retransmission rate is greater than 30%. The retransmission rate is highlighted with the word **High**.
RX, TX, and Online Uptime	• The total traffic received by AmpCon-Campus from the AP. The data will be reset after the AP is disconnected from AmpCon-Campus. • The total traffic transmitted from AmpCon-Campus to the AP. The data will be reset after the AP is disconnected from AmpCon-Campus. • The duration since the AP last connected to AmpCon-Campus. Hover your mouse over the duration, and then you can see the time when the AP last connected to AmpCon-Campus. 
Channel Related Information	The channel, radio band, channel bandwidth, and the count of currently connected wireless clients. Click the wireless client icon, and then you are redirected to the “Clients” page. 
Model	The model of the AP.
IP Address	The IP address of the AP.
SN	The serial number (SN) of the AP.
MAC Address	The MAC address of the AP.

Version	The version of the AP firmware.
System Uptime	The duration during which the AP has been running since its last startup. Hover over the duration to view the last startup time.
Load (1 | 5 | 15min)	The average CPU load over the past 1, 5, and 15 minutes.
Memory	The memory usage of the AP, measured in percentage.
Site	The site to which the AP belongs.
Local Time	The local time of the AP.
Last Contact	The time when the AP last communicated with AmpCon-Campus.
First Connect	The time when the AP first connected to AmpCon-Campus.
Reconnected	The time when the channel connection between the AP and AmpCon-Campus was last updated. A connection channel is established between an AP and AmpCon-Campus. To maintain security, the channel connection is periodically updated.
Last Connect	The time when the AP last connected to AmpCon-Campus.

Connect Reason	The reason for the last connection between the AP and AmpCon-Campus. The following reasons are provided: • **Coldboot:** The AP is powered on, or the process to connect the AP to AmpCon-Campus restarts. • **Socket:** The AP is reconnected to AmpCon-Campus after a disconnection. • **Reboot:** The AP is reconnected to AmpCon-Campus after the AP is rebooted. • **Recovery:** The AP is reconnected to AmpCon-Campus after a recovery. • **Upgrade Failed:** The AP is reconnected to AmpCon-Campus after an upgrade failure. • **Crashlog:** The AP is reconnected to AmpCon-Campus after a crash.
Password	The root password of the AP. • To view the plain-text password, click the eye icon. Click the eye icon again, and then the password will be masked. • To copy the password, click the copy icon.

Deep Insights into an AP

Click the **Devices** icon from the navigation bar. On the “Devices” page, click a specific AP. You can see a side panel on the right.

In the **Insight** tab of the side panel, you can gain deep insights into the AP.

- Guidelines
- Channel Usage
- Wi-Fi Analysis
- Statistics
- Commands
- Health Checks
- Logs
- Upgrade Histories
- Computed Configurations

Guidelines

- AmpCon-Campus can monitor only the APs that have been successfully onboarded.
- Some data in the **Insight** tab is not displayed for offline APs (APs disconnected from AmpCon-Campus).

Channel Usage

In the **Channel Usage** section, you can see the following channel-related information:

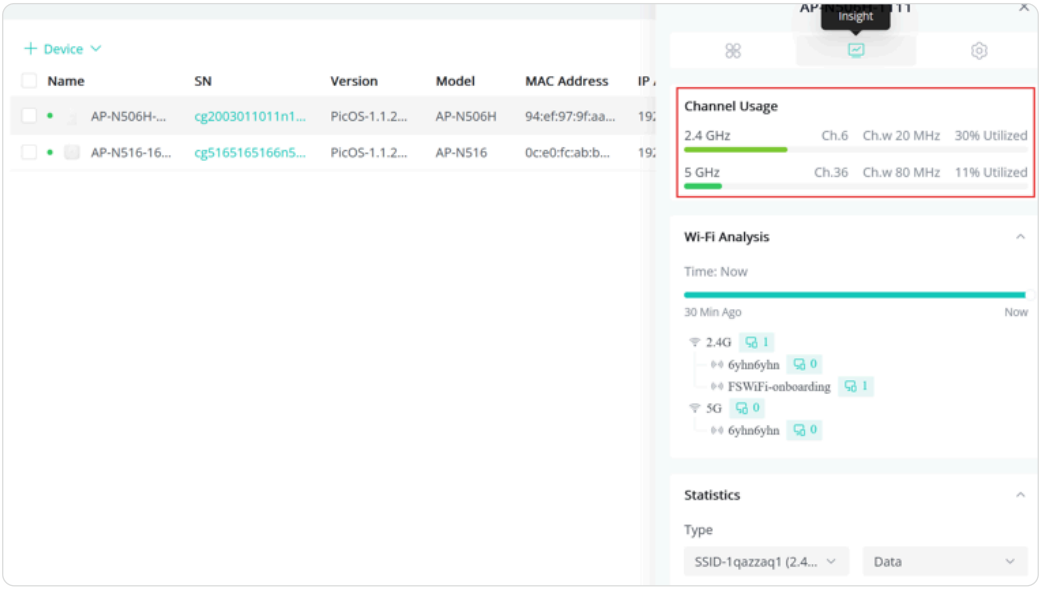


Table 1. Channel Metrics

Metric	Description
Radio Band	The frequency range allocated within radio waves for wireless communication.

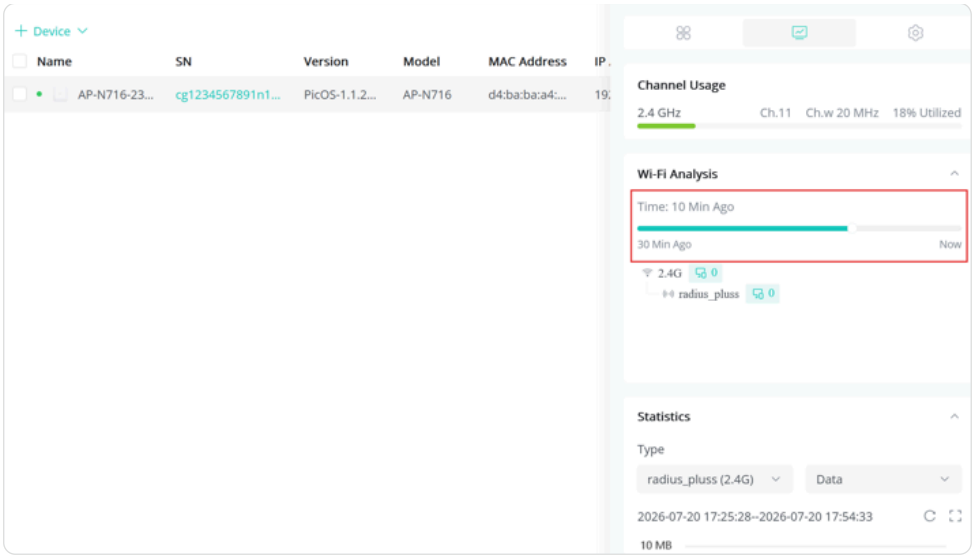
	Radio bands vary in wavelength, penetration, and transmission distances, and apply to different network scenarios. The following radio bands are supported by AmpCon-Campus: • 2.4 GHz, also called 2.4G • 5 GHz, also called 5G • 6 GHz, also called 6G
Channel	The channel of the radio. Each channel is a sub-division within a radio band for transmitting and receiving wireless signals.
Channel Width	The continuous frequency span allocated to a wireless channel. **NOTE** The supported channel widths for each radio band differ by country.
Channel Utilization	The channel utilization of each supported radio band. Channel utilization means the percentage of time that a wireless channel is occupied.

Wi-Fi Analysis

In the **Wi-Fi Analysis** section, you can see the enabled radio bands and the count of wireless clients connected to each radio band.

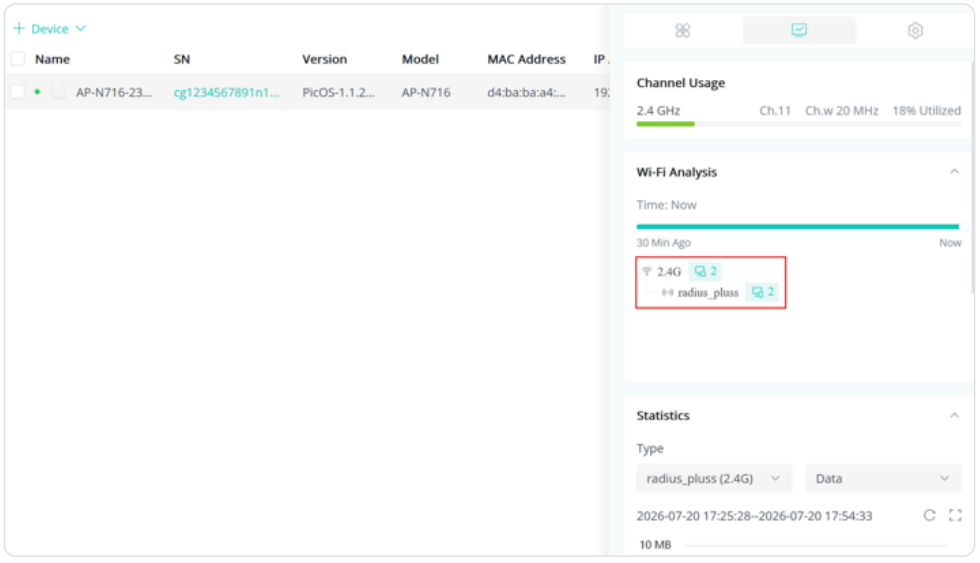
- By default, the latest collected data is displayed. To display data at a specific time point, click the time point on the time slider.

  For example, after you click the time point (**10 minutes ago**) on the time slider, you can see the data collected between 10 and 11 minutes ago.



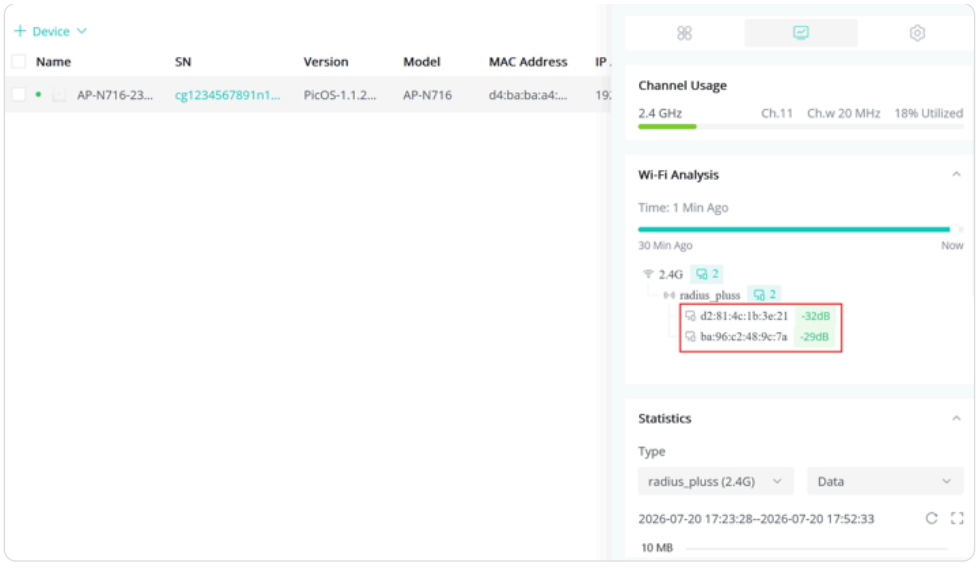
- Under a radio band, you can see the Service Set Identifiers (SSIDs) with this radio band and the count of wireless clients connected to each SSID.

  In the following screenshot, the SSID is named **radius_pluss**, and **2** wireless clients are connected to the SSID.

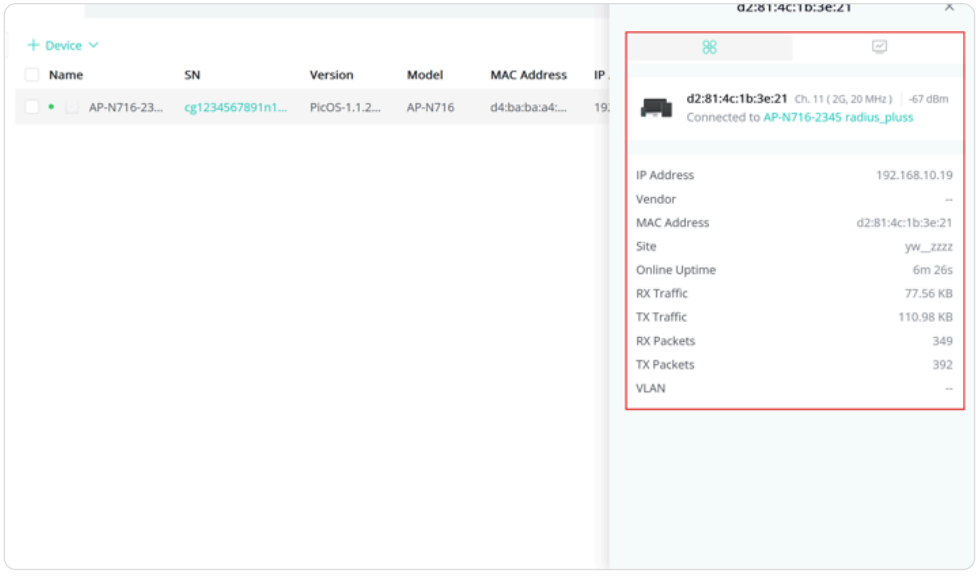


- Click an SSID to view the MAC address and Received Signal Strength Indicator (RSSI) of each wireless client connected to the SSID.

  RSSI is used to indicate the strength of signals. Normally, the RSSI value is a negative number. The closer to 0, the stronger the signal.



- Click a client MAC address to view the wireless client information in the pop-up window. For more information, see Wireless Clients.

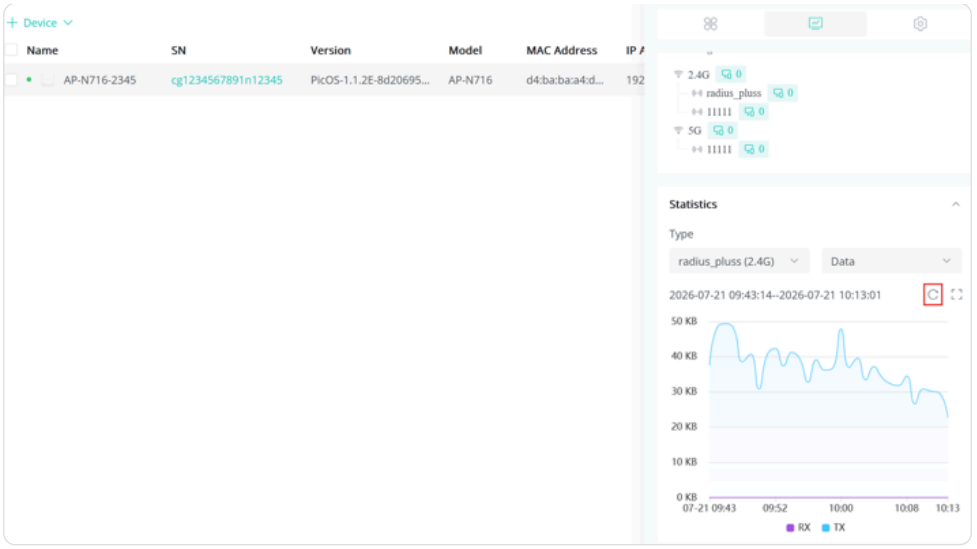


Statistics

In the **Statistics** section, you can see trend graphs of the AP traffic and memory usage.

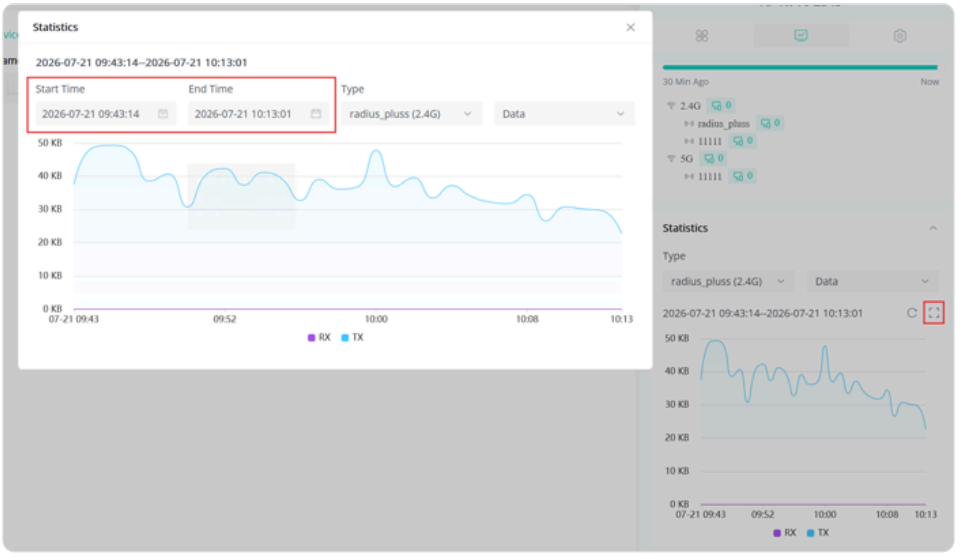
AP traffic includes each SSID traffic, WAN port traffic, and LAN port traffic. If an AP has no LAN ports, the LAN port traffic is not displayed.

- By default, the displayed time range covers the last 30 reported data entries. To refresh the trend graphs, click the refresh icon.

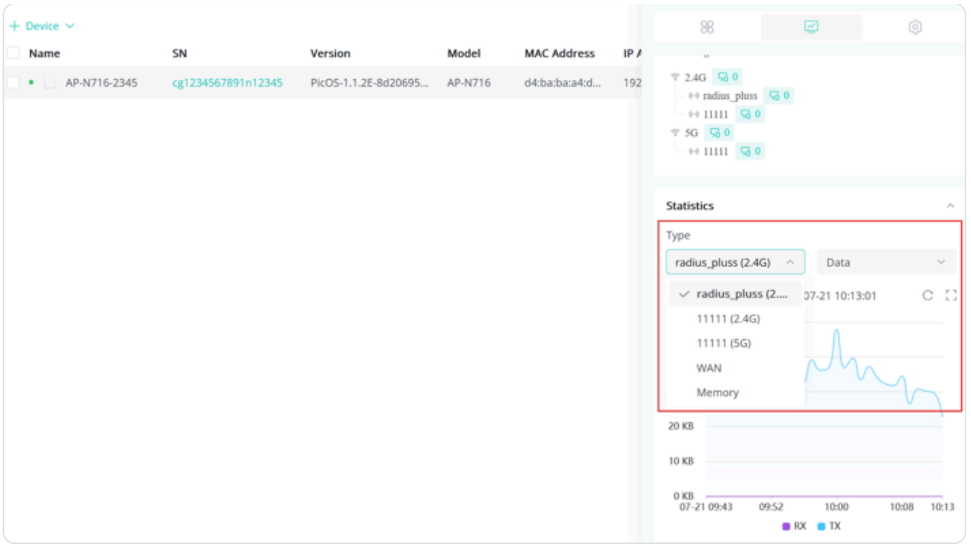


- To change the display time range, click the expand icon, and then select the start and end time point in the pop-up window.

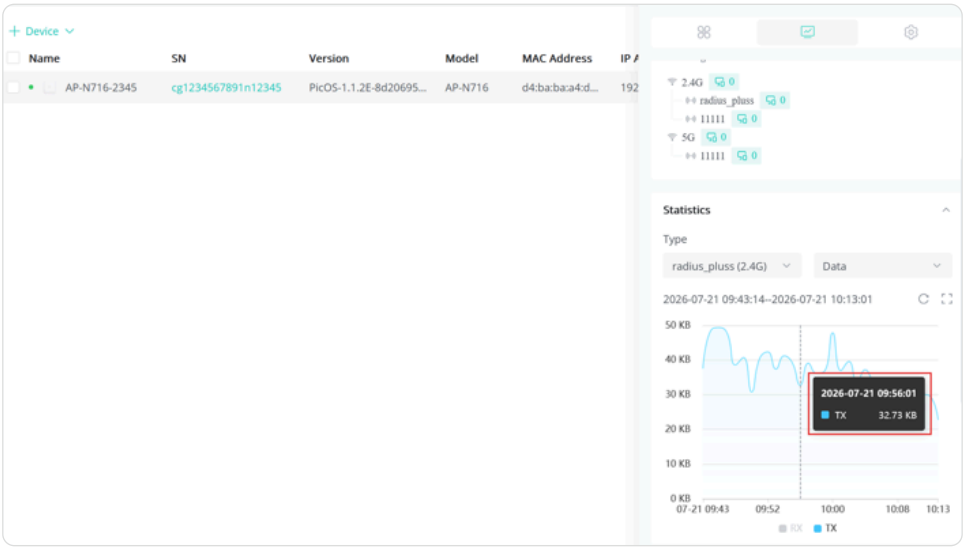
> **NOTEs**
>
> - All time points use your browser's time zone.
> - Only the data in the last 7 days can be displayed.



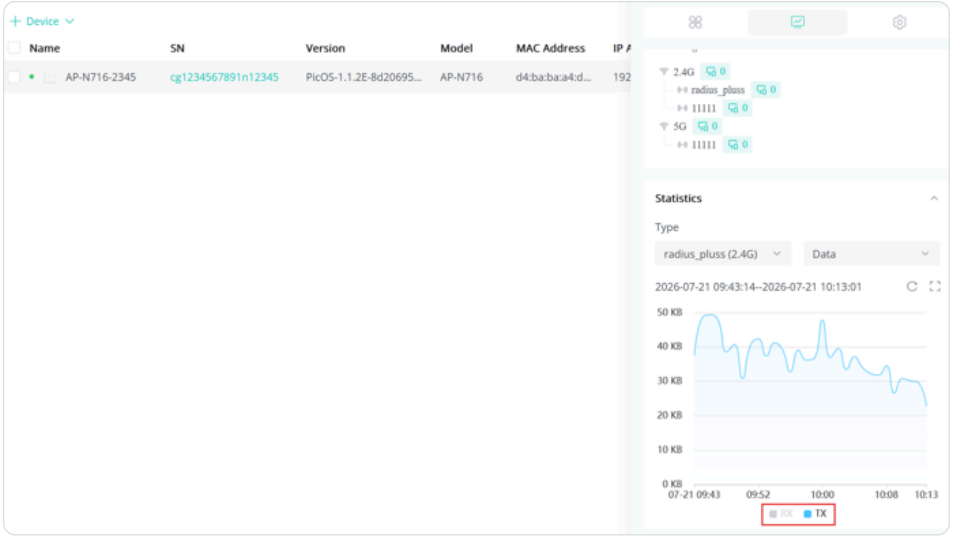
- In the **Type** drop-down list, select the trend graph type:
  - **Memory:** Displays the trend graph of memory usage.
  - **WAN:** Displays the WAN traffic trend graphs. You can select either **Data** or **Packets** to view the corresponding WAN traffic metric.
  - **SSID name (Radio band):** Displays the traffic trend graphs of each SSID. You can select either **Data** or **Packets** to view the corresponding metric of each SSID.



- To view the metric details at a specific time point, hover over that time point.



- To display or hide the data of a metric, click the square before the metric.



Commands

In the **Commands** tab, you can see the commands pushed to the AP.

- By default, the latest 5 commands are displayed. To refresh the command data, click the refresh icon.

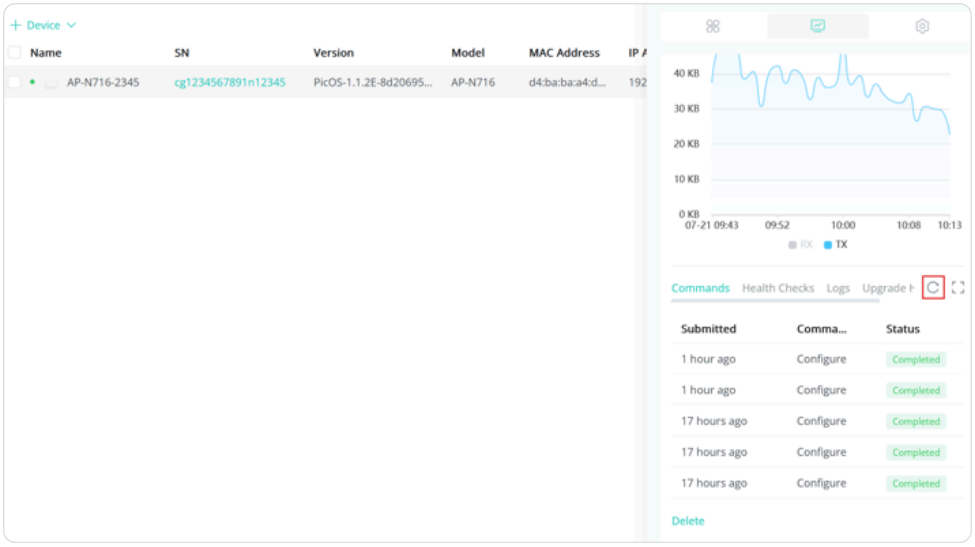


Table 2. Command Metrics

Metric	Description
Submitted	The time when the command was submitted.
Command	The command type. See the following command types and the associated commands: • **Configure:** The commands related to Configuring Wireless Networks. • **Leds:** The commands related to Positioning APs. • **Factory:** The commands related to Restoring to Factory Settings. • **Trace:** The commands related to Capturing Remote Port Packets. • **RTTY:** The commands related to Accessing APs. • **Reboot:** The commands related to Rebooting APs.
Status	The status of the command execution. • **Pending:** The command is waiting to be executed. • **Executed:** The command is executed, but the AP doesn't send the command execution result to AmpCon-Campus for reasons like connection issues. • **Completed:** The AP has sent the command execution result to AmpCon-Campus with an error

code of 0.

- **Failed:** The command failed, or the AP sent the command execution result to AmpCon-Campus with a non-zero error code.

- To see more commands, click the expand icon, and then select the start and end time point in the pop-up window.

> **NOTEs**
>
> - All time points use your browser's time zone.
> - Only the commands in the last 7 days can be displayed.

You can see the following metrics in addition to those listed above.

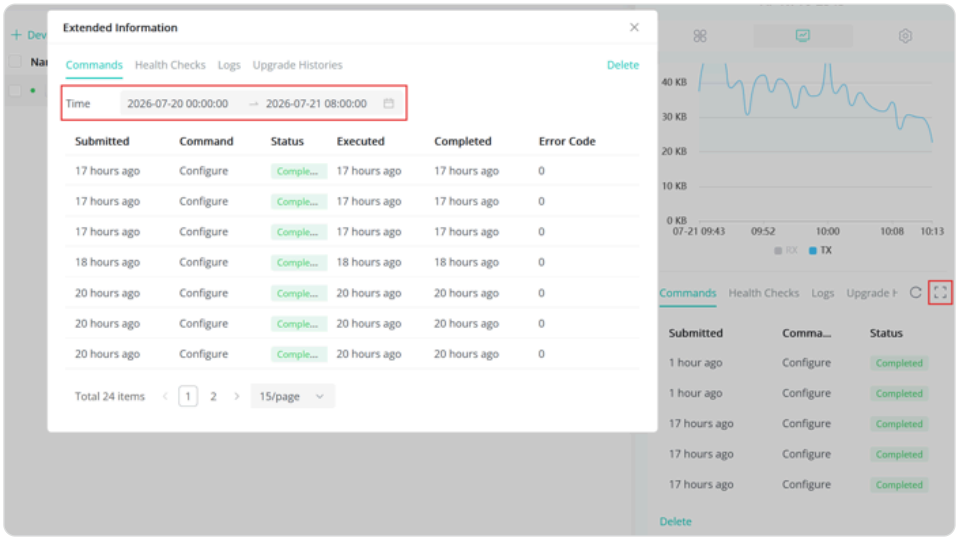


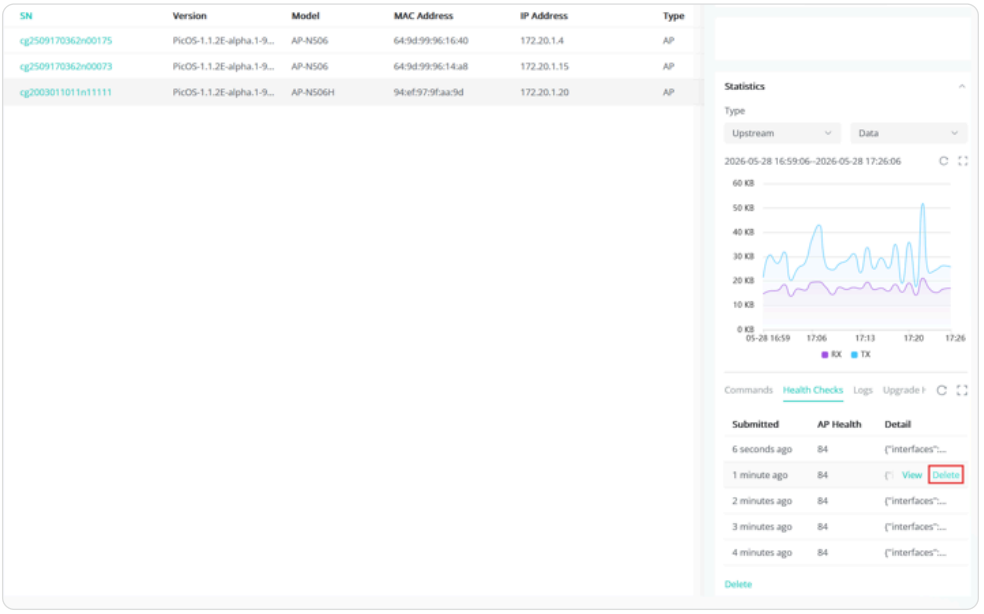
Table 3. Additional Command Metrics

Metric	Description
Executed	The time when the command execution started.
Completed	The time when the command execution completed.
Error Code	The error code of the command execution. **NOTEs** • If the command is pushed to the AP successfully, the error code is **0**. • If the error code value is not **0**, check the error details by hovering over the command

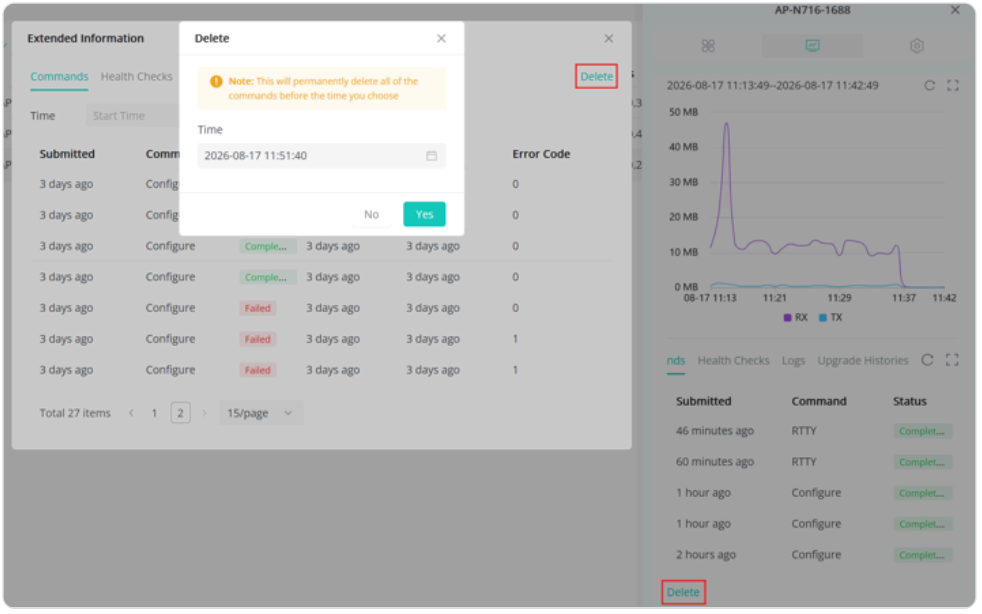
and then clicking **View** in the **Operation** column.

- To delete the command, hover over the command, and then click **Delete**.

- To delete a command, hover over the command, click **Delete**, and then click **Yes** in the pop-up window.



- To delete all commands before a specific time, click **Delete**, select a time in the pop-up window, and then click **Yes**.



Health Checks

In the **Health Checks** tab, you can see the health checks for the AP:

- By default, the latest 5 health checks are displayed. To refresh the health check data, click the refresh icon.

Table 4. Health Check Metrics

Metric	Description
Submitted	The time of the health check.
AP Health	The health grade of the AP. AmpCon-Campus calculates the **AP Health** value based on DHCP, DNS, RADIUS, and SSID health: **AP Health = 100 - (interfaces with errors / total interfaces) * 100** In the following example, **2** interfaces have DNS issues, and the total number of interfaces is **4**. Therefore, the AP health is **50**. **AP Health = 100 - (2 / 4) * 100 = 50** 
Detail	The health check details. To view more details of the health check, hover over the health check, and then click **View**. To delete the health check, hover over the health check, and then click **Delete**.

- To see more health checks, click the expand icon, and then select the start and end time point in the pop-up window.

> **NOTEs**
> - All time points use your browser's time zone.
> - Only the health checks in the last 7 days can be displayed.

- To delete a health check, hover over the health check, and then click **Delete**. In the pop-up window, click **Yes**.
- To delete all health checks before a specific time, click **Delete**, select a time in the pop-up window, and then click **Yes**.

Logs

In the **Logs** tab, you can check the logs of the AP, including general logs, reboot logs, and crash logs.

- By default, the latest 5 logs are displayed. To refresh the log data, click the refresh icon.

  Table 5. Log Metrics

Metric	Description
Submitted	The time when the log was sent to AmpCon-Campus successfully.
Severity	The severity of the log.
Detail	The details of the log. To view more details of the log, hover over the log, and then click **View**. To delete the log, hover over the log, and then click **Delete**.

- To see more metrics, click the expand icon, and then select the start and end time point in the pop-up window.

  NOTEs

  - All time points use your browser's time zone.
  - Only the logs in the last 7 days can be displayed.

  You can then see the following metric in addition to those listed above:

  Table 6. Additional Log Metrics

Metric	Description
Log	The log information.

- To delete a log, hover over the log, and then click **Delete**. In the pop-up window, click **Yes**.

  To delete all logs before a specific time, click **Delete**, select a time in the pop-up window, and then click **Yes**.

Upgrade Histories

In the **Upgrade Histories** tab, you can check the upgrade history records of the AP.

- By default, the latest 5 upgrade history records are displayed. To refresh the upgrade history data, click the refresh icon.

Table 7. Upgrade History Metrics

Metric	Description
Submitted	The time when the upgrade operation was submitted.
Version	The version to which the AP is upgraded.
Upgrade Status	The status of the upgrade operation. • **Successful:** The upgrade is completed successfully. • **Failed:** The upgrade fails. • **Cancel:** The upgrade is cancelled.

- To see more metrics, click the expand icon, and then select the start and end time point in the pop-up window.

> **NOTE**
>
> All time points use your browser's time zone.

You can then see the following metrics in addition to those listed above:

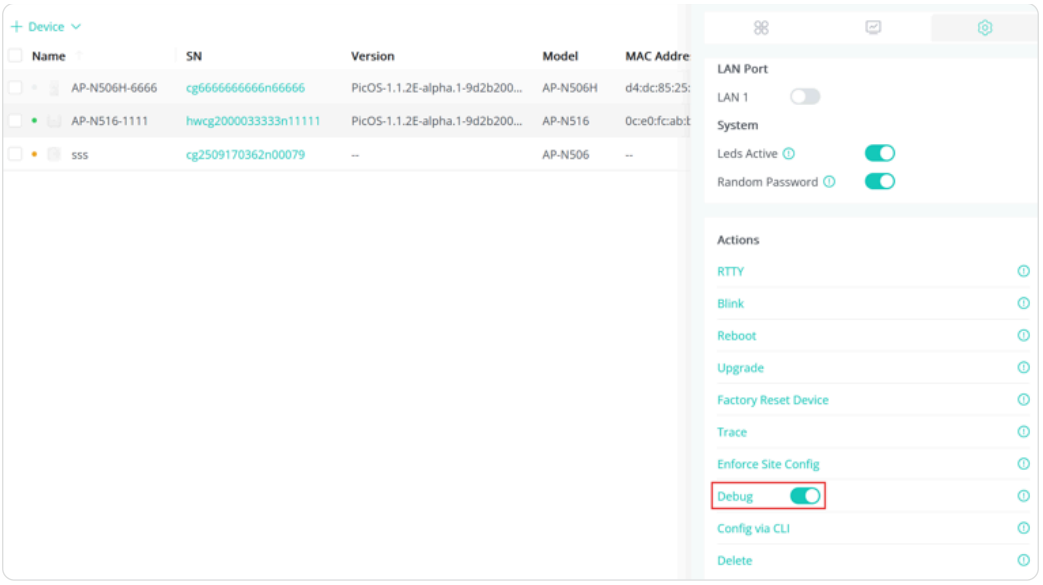
Table 8. Additional Upgrade History Metrics

Metric	Description
Detail	The details of the upgrade operation. To view details of the upgrade operation, hover over the upgrade history record, and then click **View**. To delete the upgrade operation, hover over the upgrade history record, and then click **Delete**.

- To delete an upgrade history record, hover over the record, and then click **Delete**. In the pop-up window, click **Yes**.
- To delete all upgrade history records before a specific time, click **Delete** at the bottom of the section, select a time in the pop-up window, and then click **Yes**.

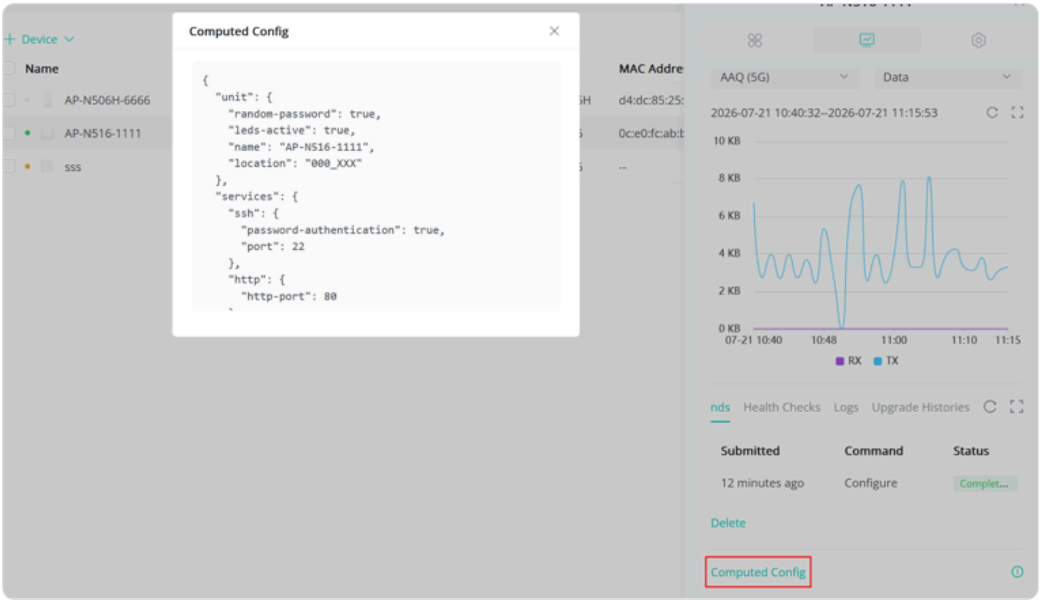
Computed Configurations

In the side panel on the right, click the **Setting** tab, and enable **Debug** in the **Actions** section.



Then, you can see the **Computed Config** button displayed in the **Insight** tab. Click **Computed Config**, and then you can see the configurations to be pushed to the AP.

> **NOTE**
>
> After you close the side panel on the right, the **Debug** function will be automatically disabled. So each time you open the side panel, the **Computed Config** button is not displayed in the **Insight** tab by default.



Configurations and Operations of an AP

Click the **Devices** icon from the navigation bar. On the “Devices” page, click an AP. You can see a side panel on the right.

Click the **Setting** tab of the side panel, and then you can view configurations or perform management operations for the AP.

Guidelines
General Configurations
Radio Configurations
Advanced Configurations
AP Management Operations

Guidelines

- In the **Setting** tab, you can not only view but also modify configurations of each AP. Modifying configurations in the **Radio** or **Advanced Setting** section will apply device-specific wireless configurations to the AP.
- Click **Apply** after you change configurations of an AP. Otherwise, the configuration changes will not be pushed to the AP.
- For an offline AP (AP disconnected from AmpCon-Campus), although you can modify AP configurations, the changes cannot be pushed to the AP successfully.
- You can change radio and advanced configurations for a specific AP only after you have added site-level wireless configurations. For more information, see Configuring Wireless Networks.

General Configurations

At the top of the **Setting** tab, you can see general configurations of the AP:

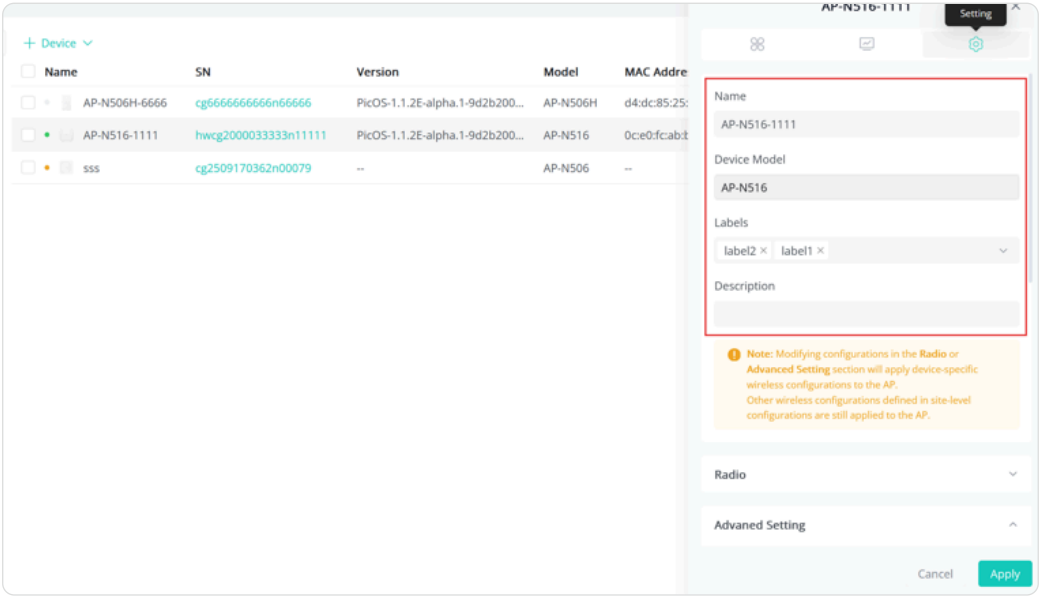


Table 1. General AP Configurations

Configuration	Description
Name	The AP alias. Aliases are used to differentiate APs in the AmpCon-Campus UI and will not be pushed to the AP side. If you do not enter the alias during AP onboarding, AmpCon-Campus automatically generates an alias for each device. The alias contains the device model and the last four digits of the AP SN. The alias can contain at most 64 characters. Only letters, numbers, hyphens (-), and underscores (_) are allowed. The alias cannot start or end with a hyphen or underscore.
Device Model	The model of the AP. AmpCon-Campus automatically retrieves the AP model and displays it here. The model cannot be changed.
Labels	Optional. The labels of the AP. You can select one or multiple labels. To add a new label, click the **Labels** drop-down list, and then click **Create Label**. Each label name can contain only letters and numbers and can contain at most 64 characters.
Description	Optional. The description of the AP. The description can contain at most 256 characters.

Radio Configurations

In the **Radio** section, you can see radio configurations of the AP:

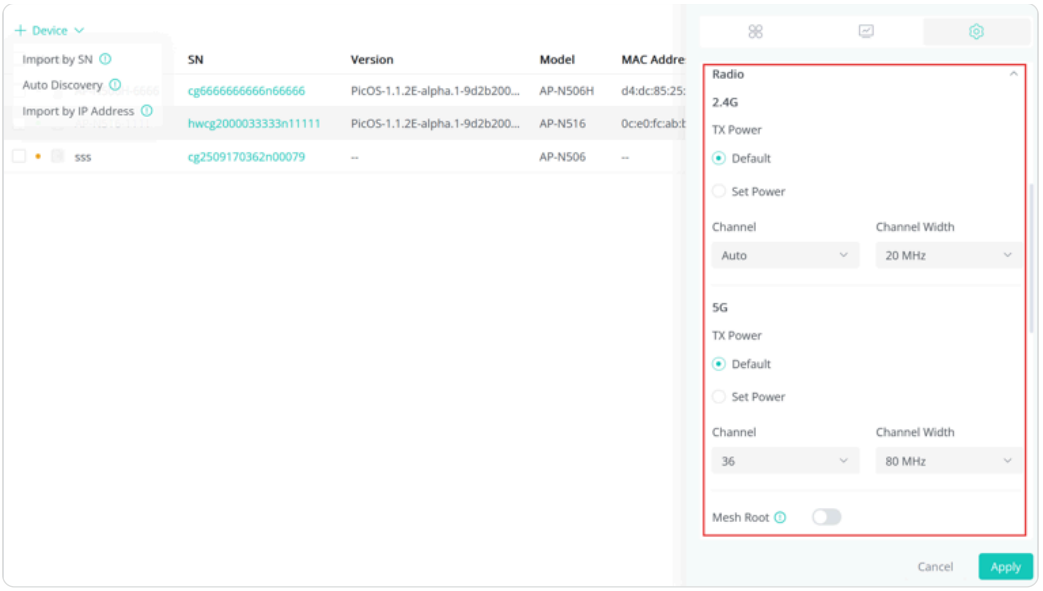
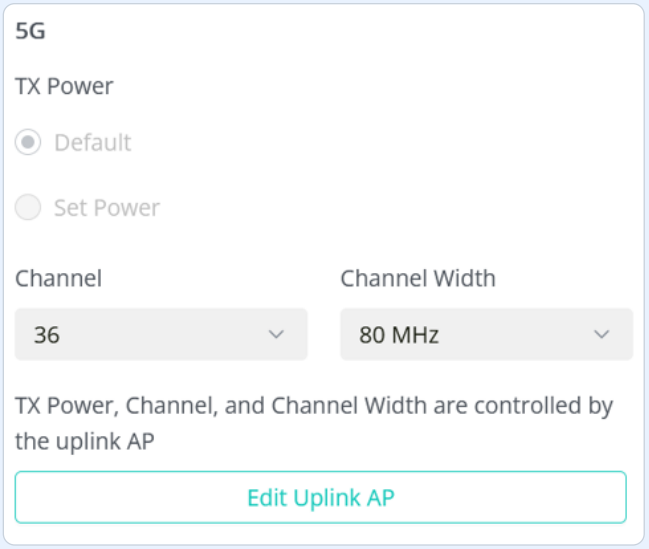
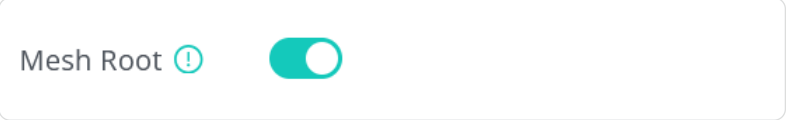


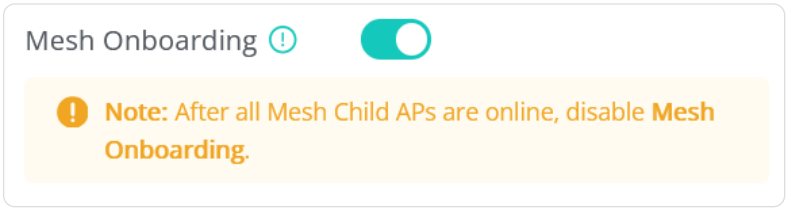
Table 2. Radio Configurations

Configuration	Description
Radio	The radio band, **2.4G**, **5G,** or **6G**. **NOTE** Only the radio bands satisfying all of the following conditions are displayed: • The radio bands are supported by the AP model. • The radio bands are permitted for use in the country where the AP is deployed.
TX Power	The transmit power of the radio. Select **Default** or **Set Power**. • **Default:** The AP will work at the maximum transmit power that the located country allows. • **Set Power:** The AP will work at a customized transmit power. You can customize the transmit power within the range of 1 to 30. The unit is dBm. **NOTEs** • The maximum TX power limit might vary depending on the country code. • For a mesh child AP, the 5G **TX Power**, **Channel**, and **Channel Width** values are the same as those of its mesh root AP and cannot be changed.

	To change mesh root AP configurations, click **Edit Uplink AP**. In the **Setting** tab of the mesh root AP, change the TX power, channel, and channel width, and then click **Apply**. The changes will be automatically synchronized to the mesh child AP. 
Channel	The channel of the radio. Each channel is a sub-division within a radio band for transmitting and receiving wireless signals. If you select **Auto**, the AP will automatically select the optimal channel. **NOTE** For a mesh root AP, the **Auto** option is grayed out in the **Channel** drop-down list for the 5 GHz radio band. This is because a fixed channel is required to maintain stable connections between the mesh root AP and its mesh child APs.
Channel Width	The continuous frequency span allocated to a wireless channel. **NOTEs** • The supported channel widths for each radio band differ by country. • Some APs don't support 160 MHz and 320 MHz. For these APs, 160 MHz and 320 MHz are not displayed.

	• For 5G and 6G radio bands, if a channel is a DFS channel, its channel width is marked with a **DFS** label.
Mesh Root	Toggle it on to enable this AP as a mesh root AP. After you toggle on **Mesh Root** and click **Apply**, this AP acts as a mesh root AP, providing network access for wireless mesh child APs. A mesh child AP is an AP that is only powered on and not connected to an Ethernet cable. Once powered on, the mesh child AP will attempt to establish a mesh connection with the mesh root AP. After the connection is successfully established, the mesh network is connected and normal data transmission can be realized.  **NOTEs** • The **Mesh Root** toggle is visible only after you enable **Wireless Meshing** on the “Wireless Configuration” page. For more information, see Adding Radio Configurations. • If an AP is not powered on or not connected to an Ethernet cable, it cannot function as a mesh root AP. • Toggling **Mesh Root** off will disconnect mesh child APs. As a result, all wireless client devices connected to those APs will lose network access. • For mesh root APs, it’s not recommended to use the default channel 36 and the default channel width 80 MHz. This channel is heavily utilized and prone to high interference, resulting in poor network performance. Select another idle channel to enhance network performance.
Mesh Onboarding	Broadcasts an SSID named **Pica8WiFi-Onboarding**.

New mesh child APs will connect to this SSID in STA mode by using certificates to securely retrieve their initial network settings and platform configurations.



NOTEs

- This section is displayed only if you toggle **Mesh Root** on.
- **Mesh Onboarding** is automatically enabled to help new mesh child APs join.
  After all mesh child APs are online, disable **Mesh Onboarding** for security concerns.

Advanced Configurations

In the **Advanced Setting** section, you can see advanced configurations of the AP:

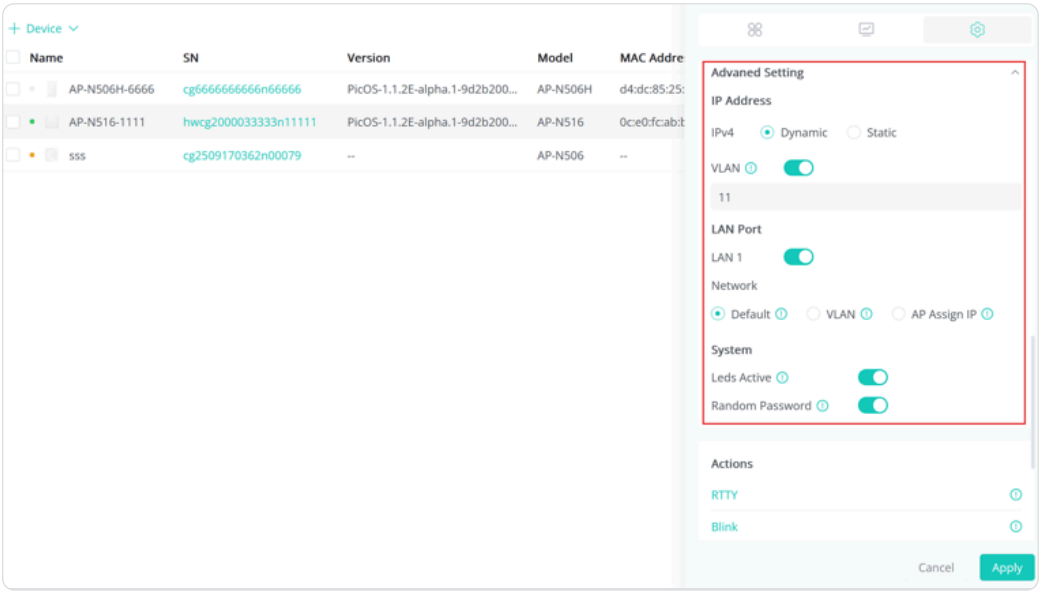


Table 3. Advanced Configurations

Configuration	Description
IPv4	Select **Dynamic** or **Static**. • If you select **Dynamic**, the AP will act as a DHCP client and obtain an IP address from the DHCP server.

	• If you select **Static**, you can assign a static IPv4 address to the AP.
VLAN	Toggle it on to configure a management VLAN for each AP. Then, enter a VLAN ID ranging from 2 to 4048. You can also toggle it off to disable the function. • If the function is disabled, wireless clients will be in the same subnet segment as connected APs. • If the function is enabled, you can configure a VLAN ID for the SSID to make the AP work in Bridge mode. Then, LAN ports will operate on an independent subnet. **NOTEs** • Do not enter the native VLAN ID of the uplink switch. Otherwise, the wireless network will not work. • Ensure the new VLAN is allowed (tagged) on all upstream switch ports to avoid client device unreachability.
IPv4 Address (CIDR)	The IPv4 address assigned to the AP, such as 10.1.1.10/24. **NOTEs** • This section is displayed only if you select **Static** in the **IPv4** section. • The IPv4 address cannot be a loopback address, multicast address, broadcast address, or network address.
Gateway	The IPv4 address of the gateway, such as 10.1.1.1. **NOTEs** • This section is displayed only if you select **Static** in the **IPv4** section. • The gateway cannot be a loopback address, multicast address, broadcast address, or network address.
Use DNS	The IPv4 addresses of DNS servers to be used.

	You can enter at most 3 DNS server IPv4 addresses. After you enter an IP address, ensure to press **Enter**. **NOTE** This section is displayed only if you select **Static** in the **IPv4** section.
LAN Port	Toggle on to enable LAN ports, or toggle off to disable them. After you toggle on a LAN port, select how downstream wired devices access the upstream network in the **Network** section: • **Default:** In this mode, the physical port acts as a basic switch port, and traffic is directly forwarded in Bridge mode. Client devices connected to this LAN port obtain IP addresses directly from the upstream network and are in the same LAN segment as the AP's management IP. • **VLAN:** In this mode, you can perform fine-grained isolation and tag management for port traffic. Wired terminals can be assigned to specific service subnets to achieve complete isolation from other networks (such as guest wireless networks). • **AP Assign IP:** In this mode, each AP operates in Network Address Translation (NAT) mode and acts as a gateway. Each AP assigns an independent private IP address (the private 10.1.1.0/24 network) to the downstream device. The AP performs NAT when the downstream device connects to the internet. Make sure that the upstream network does not use a 10.1.1.0/24 subnet. If the upstream network contains a 10.1.1.0/24 subnet, modify the subnet by going to the **DHCP Service** section of advanced wireless configurations. For more information, see Configuring Wireless Networks - Adding Advanced Configurations. **NOTEs** • **AP Assign IP** is unavailable for mesh child APs. For a mesh child AP:

	◦ **AP Assign IP** is not displayed after you toggle on a LAN port. ◦ If a LAN port is set to **AP Assign IP** in site-level wireless configurations, this LAN port is toggled off here. ◦ If a LAN port is set to **Default** or **VLAN** in site-level wireless configurations, the same LAN port configurations are displayed here. • Different AP models have different counts of LAN ports: ◦ **AP-N716:** Displays LAN 1. ◦ **AP-N516:** Displays LAN 1. ◦ **AP-N506:** Displays LAN 1. ◦ **AP-N506H:** Displays LAN 1, LAN 2, LAN 3, and LAN 4. ◦ **AP-T566D:** Displays no LAN ports. • The configurations for a specific LAN port can take effect only on APs equipped with this port. • If a LAN port is not connected to any terminal device, it is recommended to disable the LAN port for network security purposes. In this way, you can prevent unauthorized devices from accessing the network through physical Ethernet cables.
Port Mode	The mode of the LAN port, **Access** or **Trunk**. • **Access:** Mainly used to connect terminal devices such as PCs. All data packets sent to and received by terminal devices are untagged. APs automatically add or remove VLAN tags for these packets internally. • **Trunk:** Mainly used to connect network devices that support VLANs, such as switches and routers. Packets with specific VLAN tags are allowed to pass through the trunk port, enabling transparent VLAN transmission across devices. **NOTE**

	This section is displayed only if you select **VLAN** in the **Network** section.
Trunk VLAN	The VLAN allowlist of the LAN port. You can enter one or multiple VLAN IDs. After you enter a VLAN ID, ensure to press **Enter**. Only the packets from the VLAN allowlist are permitted to pass through the LAN port. Packets from VLANs not included in the allowlist will be discarded by the LAN port. **NOTEs** • This section is displayed only if you select **VLAN** in the **Network** section and select **Trunk** in the **Port Mode** section. • The **Trunk VLAN** list and the **Port VLAN** list cannot contain overlapping VLAN IDs.
Port VLAN	The default VLAN membership of this LAN port. When a port receives untagged data packets, the AP will automatically assign the port to the default VLAN ID. The VLAN ID must range from 2 to 4048. **NOTEs** • This section is displayed only if you select **VLAN** in the **Network** section. • The **Trunk VLAN** list and the **Port VLAN** list cannot contain overlapping VLAN IDs.
Leds Active	Toggle it on to force all LED lights to turn on. Toggle it off to force all LED lights to turn off.
Random Password	Toggle it on to generate a random root password for the AP. You can check the password at the bottom of the **Overview** tab. For more information about the **Overview** tab, see Basic Information of an AP.

AP Management Operations

In the **Actions** section, you can manage the AP through the following buttons:

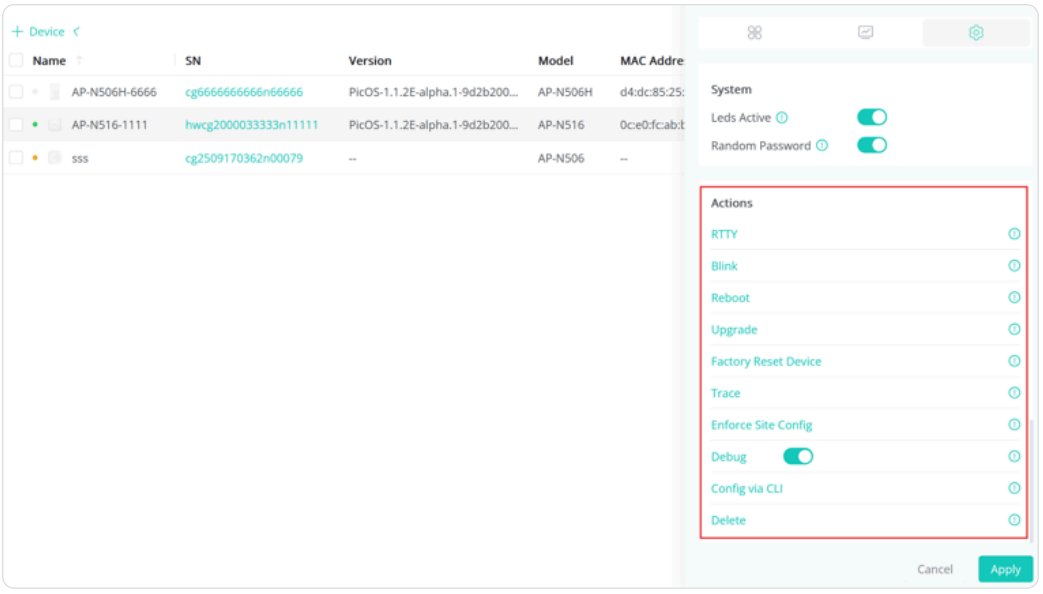


Table 4. Action Buttons

Button	Purpose	Reference Link
RTTY	Establish a remote terminal session to the AP through remote TTY shell (RTTY).	• Accessing APs
Blink	Make the AP's LED lights flash to help with physical identification in the location.	• Positioning APs
Reboot	Safely reboot the AP.	• Rebooting APs
Upgrade	Upgrade the AP firmware to ensure optimal performance and security.	• Upgrading APs
Factory Reset Device	Wipe all custom settings and restore the AP to its original status (factory settings). This action is irreversible.	• Restoring to Factory Settings
Trace	Capture remote packets from target ports of the AP for rapid troubleshooting.	• Capturing Remote Port Packets
Enforce Site Config	Clear all device-specific configurations for this AP, and overwrite them with site-level wireless configurations.	• Enforcing Site Configurations

Debug	After **Debug** is enabled, you can use the following specialized tools: • **Config via CLI:** Click **Current Configuration** to check the current AP configurations, or click the upload icon to upload a JSON file and then click **Apply** for AP debugging or advanced configuration. • **Computed Config:** Click **Computed Config** at the bottom of the **Insight** tab to view the configurations to be pushed to the AP. **NOTE** Contact support engineers and **do not** use the **Config via CLI** feature by yourself. Otherwise, incorrect CLI configurations might disrupt device operation.	• Advanced CLI Configurations • Computed Configurations
Delete	Permanently remove this AP from AmpCon-Campus.	• Deleting APs

Clients

AmpCon-Campus provides comprehensive client monitoring capabilities for both wired and wireless client devices. You can centrally manage and monitor all wireless and wired clients across your campus network.

- **Wired Clients**: AmpCon-Campus supports automatically identifying wired clients connected to each managed PicOS switch, as well as manually adding wired clients. You can accurately and securely monitor wired clients.
- **Wireless Clients**: Wireless clients refer to devices (such as smartphones and laptops) that connect to wireless networks through access points (APs). You can monitor wireless clients connected to each managed AP.

See the following child topics:

- Wired Clients
- Wireless Clients

Wired Clients

AmpCon-Campus supports both automatically identifying wired clients connected to each managed PicOS switch and manually adding wired clients.

By using the wired client monitoring feature, you can achieve the following goals:

- View detailed information for all wired clients across the network to gain a comprehensive visualization of wired clients.
- Classify wired clients by specific attributes for rapid inventory management, eliminating common blind spots such as unclear wired client counts and unknown access locations.
- Rapidly identify abnormal wired clients and locate the affected wired clients and ports, facilitating early detection and handling of faults.

Automatic Identification Methods
Prerequisites
Viewing the Wired Client List
Adding Wired Clients Manually

Automatic Identification Methods

AmpCon-Campus uses the following technologies to automatically identify wired clients:

- **MAC OUI**

  A MAC Organizationally Unique Identifier (OUI) is the first 24 bits of a device's MAC address. MAC OUIs are assigned to manufacturers by the Institute of Electrical and Electronics Engineers (IEEE).

  Switches report wired clients' OUIs to AmpCon-Campus, and then AmpCon-Campus references its fingerprint database to identify wired client manufacturers.

- **DHCP Snooping**

  During Dynamic Host Configuration Protocol (DHCP) interactions, switches with DHCP Snooping enabled capture DHCP packets and extract the mappings of the wired client MAC address, IP address, and switch port.

  After a switch records these mappings in the binding table, the data is collected and returned to AmpCon-Campus through SSH Exporter. Meanwhile, the switch updates the binding table based on the packets, enabling continuous and precise wired client monitoring.

Prerequisites

If you need AmpCon-Campus to discover the IP addresses of wired clients automatically, the following conditions must be met:

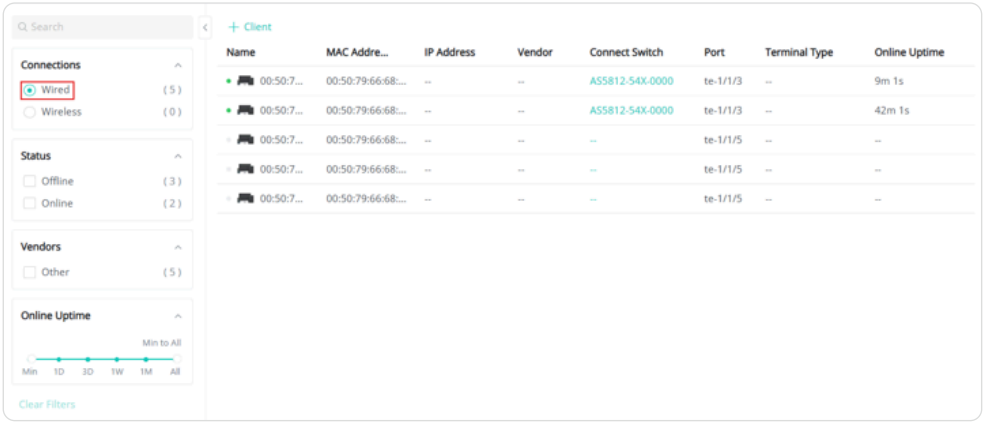
- The networks to which the wired clients belong have DHCP servers configured.

- The uplink PicOS switches of the wired clients are online (connected to AmpCon-Campus).
- DHCP Snooping and Link Layer Discovery Protocol (LLDP) are enabled on the uplink PicOS switches of the wired clients. Otherwise, some client information might be wrong.

Viewing the Wired Client List

To view wired clients automatically identified by AmpCon-Campus and added manually, follow these steps:

1. In the AmpCon-Campus UI, select the site to which the wired clients belong, and then click the **Clients** icon from the navigation bar.
2. In the **Connections** section of the sidebar, select **Wired** to filter wired clients.



3. On the “Clients” page, view the wired client list, which contains the following metrics:

Table 1. Wired Client Metrics

Metric	Description

Name	The name of the wired client. During automatic client identification, AmpCon-Campus automatically assigns the MAC address of the wired client as its name. **NOTE** The circle color in the **Name** column indicates the status of the wired client: • **Green:** The wired client is in **Online** status, which represents it's up and connected to its uplink switch. • **Gray:** The wired client is in **Offline** status, which represents it is down or isn't connected to its uplink switch.
MAC Address	The MAC address of the wired client.
IP Address	The IPv4 address of the wired client. **NOTE** The **IP Address** is displayed as **--** in the following cases: • The client is automatically identified by AmpCon-Campus, but no IP address is assigned to the client through DHCP. • The client is automatically identified by AmpCon-Campus, but DHCP Snooping isn't enabled on the uplink PicOS switch of the client. • The client is manually added to AmpCon-Campus, and you haven't configured the client IP address when adding or editing the client.
Vendor	The manufacturer of the wired client. **NOTE**

	The **Vendor** is displayed as **--** in the following cases: • The wired client is automatically identified by AmpCon-Campus, but its vendor cannot be recognized. • The client is manually added to AmpCon-Campus, and you haven't configured the vendor when adding or editing the client.
Connect Switch	The alias of its uplink switch. If the client is currently offline, the last uplink switch is displayed. **NOTEs** • If a client is connected to a switch through **an intermediate device** not managed by AmpCon-Campus, an exclamation mark is displayed in the **Connect Switch** column of the client. When you hover over the exclamation mark, you can see the tip: "Connected via a third-party device". • If a switch fails to discover **the intermediate device** over LLDP but has learned multiple MAC addresses of connected devices, an exclamation mark is also displayed in the **Connect Switch** column of the intermediate device.
Port	The switch port used to connect to the wired client.
Terminal Type	The type of the wired client. You can see a built-in type (**PC**, **Printer**, **IP Camera**, **IP Phone**, or **WAP**) or a custom type. **NOTE** Currently, AmpCon-Campus cannot recognize client types automatically. If you haven't configured this field manually, the type is displayed as **--**.

Online Uptime	The continuous online duration of the wired client. Hover over the duration to view the client's last connection time to its uplink switch. **NOTE** The value is **--** if the wired client is down or isn't connected to the switch.

4. To filter wired clients, use the following filter conditions in the sidebar:

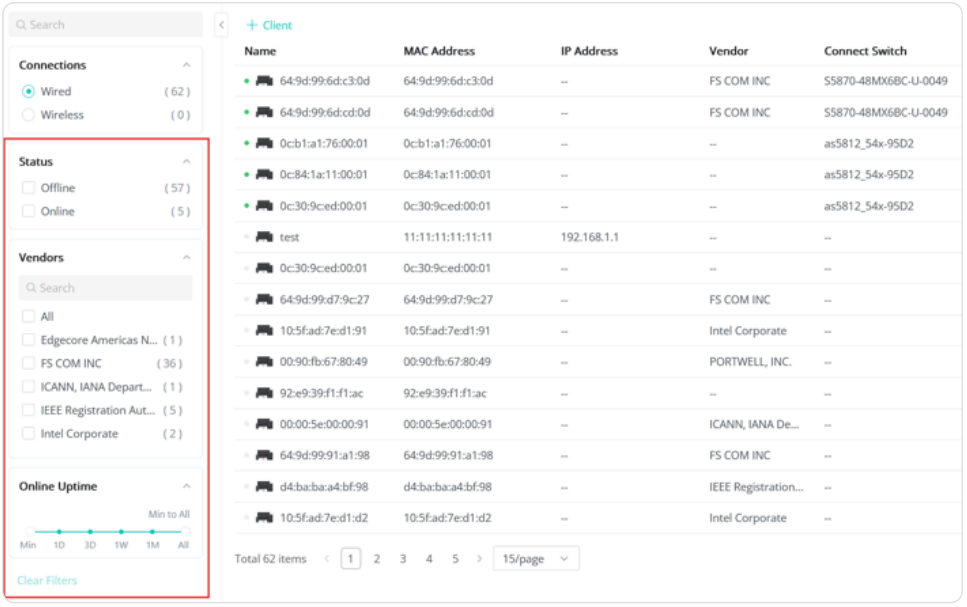


Table 2. Filter Conditions

Filter Condition	Description
Status	The statuses of wired clients: **Online** or **Offline**. • **Online:** The client is online (the client is up and connected to its uplink switch). • **Offline:** The client is offline (the client is down or isn't connected to its uplink switch).
Vendors	The manufacturers of wired clients. **NOTE** If you select **Other**, the following wired clients are displayed:

	• Wired clients that are automatically identified by AmpCon-Campus but whose vendors cannot be recognized. • Wired clients that are manually added to AmpCon-Campus with no vendor specified.
Online Uptime	The continuous online duration of the wired clients. Select a time range in the **Online Uptime** section by clicking the starting time point and the end time point. The following time points can be clicked: • **Min** represents the current time. • **1D** represents 1 day. • **3D** represents 3 days. • **1W** represents 1 week. • **1M** represents 1 month. • **All** represents all times. **Examples:** • If you select the time range as **Min** to **All**, all clients are displayed. • If you select the time range as **3D** to **1M**, only online clients whose **Online Uptime** is between 3 days and 1 month are displayed. • If you select the time range as **Min** to **1D**, only online clients whose **Online Uptime** is less than or equal to 1 day are displayed. Offline clients are also displayed. • If you select the time range as **1W** to **All**, only online clients whose **Online Uptime** is greater than or equal to 1 week are displayed.

Tips

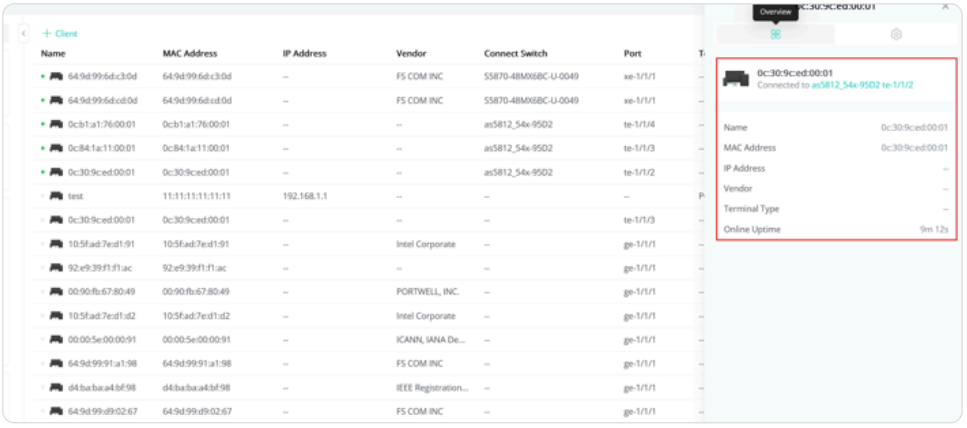
- If no devices match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of devices that match the filter option.
- To clear all these filter options, click **Clear Filters**.

5. To view detailed information of a wired client, click the wired client in the client list. A side panel is displayed on the right.

- In the **Overview** tab, you can see the uplink switch and port and detailed client metrics if the client is online.

  Click the uplink switch alias, and then you can see the switch side panel. For more information, see PicOS Switches.

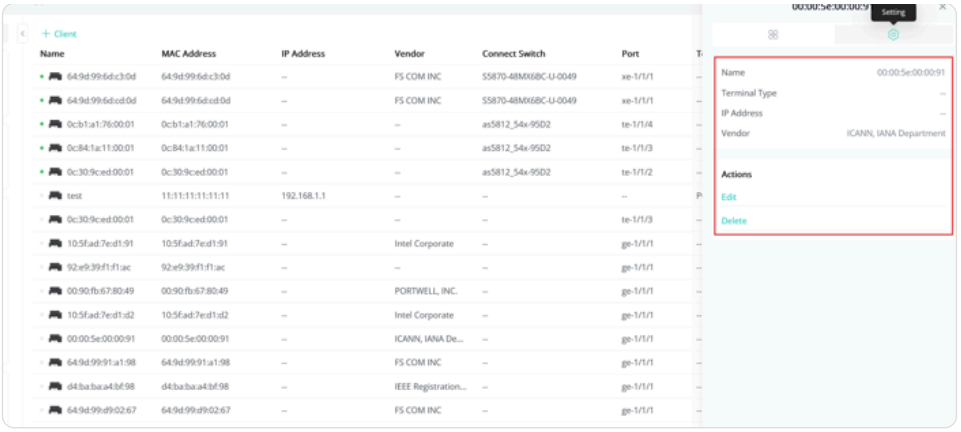
  If the client is offline, the last uplink switch, corresponding port, and last connection time will be displayed.



- In the **Setting** tab, you can view client metrics, and you can delete or edit the client.

  To delete or edit a wired client, click **Delete** or **Edit** respectively in the **Actions** section.

> **NOTEs**
>
> - For an online wired client, the **Delete** button is not displayed, and thus you cannot delete the client.
> - If AmpCon-Campus automatically identifies a wired client after the client has been deleted, the client will reappear in the client list.
> - For an online wired client, if its IP address is assigned by DHCP, you cannot edit its IP address.
> - When you edit a wired client, you can select a vendor from the drop-down list, or click the input field and then enter a custom vendor.
>
>   The custom vendor can contain at most 128 characters and cannot contain only spaces. Chinese characters are not supported.



Adding Wired Clients Manually

If AmpCon-Campus cannot identify a wired client automatically, you can't see the wired client on the "Clients" page. You can add the wired client to AmpCon-Campus manually. Follow these steps:

1. In the AmpCon-Campus UI, select the site to which the wired client belongs, and then click the **Clients** icon from the navigation bar.
2. On the "Clients" page, click **+ Client**.
3. In the pop-up window, input the following information, and then click **Apply**.

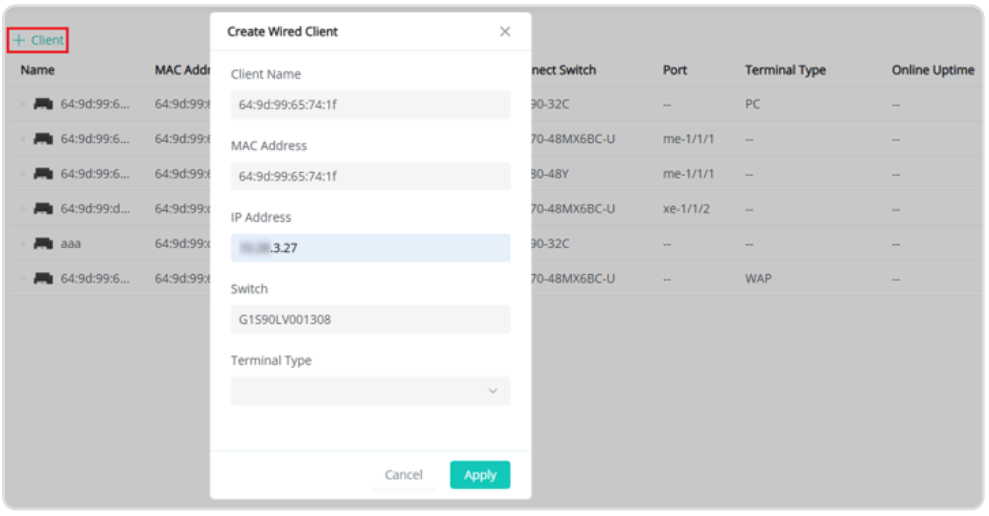


Table 3. Wired Client Parameters

Parameter	Description
Client Name	The name to distinguish the wired client. The name can contain at most 64 characters and cannot contain only spaces.
MAC Address	The MAC address of the wired client. **NOTEs**

	• You must enter a valid MAC address. Otherwise, the verification will fail. • You do not need to manually input a colon after every two characters. AmpCon-Campus automatically adds colons after every two characters.
IP Address	Optional. The IPv4 address of the wired client. The **IP Address** cannot be within the following address ranges: • Link-local addresses: 169.254.0.0 to 169.254.255.255 • Loopback addresses: 127.0.0.0 to 127.255.255.255 • Multicast and reserved addresses: 224.0.0.0 to 255.255.255.255 • Special reserved addresses: 0.0.0.0 to 0.255.255.255
Switch	Click **Select Switch** to select the uplink switch of the wired client.
Terminal Type	Optional. The type of the wired client. You can select a type from the drop-down list, or you can click the input field and enter a custom type. The custom type can contain at most 32 characters and cannot contain only spaces. Chinese characters are not supported. After you successfully add a wired client with a custom type, the type will be added to the **Terminal Type** drop-down list.

Wireless Clients

Wireless clients refer to clients (such as smartphones and laptops) that connect to wireless networks through access points (APs).

AmpCon-Campus supports automatically identifying wireless clients connected to each managed AP. You can monitor wireless clients for full visibility into your wireless environment.

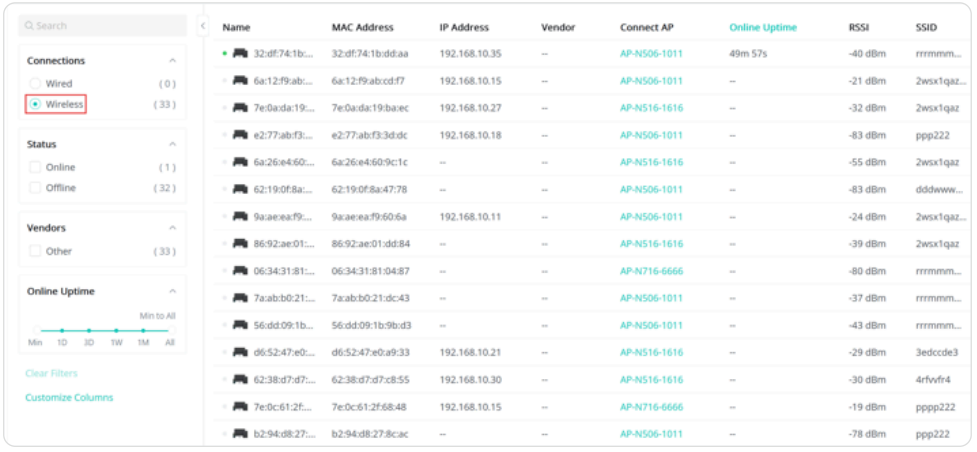
Prerequisite
Viewing the Wireless Client List
Viewing Details of a Wireless Client

Prerequisite

To monitor wireless clients, ensure the APs to which the wireless clients connect are managed by AmpCon-Campus and are currently online (connected to AmpCon-Campus).

Viewing the Wireless Client List

1. In the AmpCon-Campus UI, select a site to which the wireless clients belong, and then click the **Clients** icon from the navigation bar.
2. In the **Connections** section of the sidebar, select **Wireless** to filter wireless clients.



3. On the “Clients” page, view the wireless client list, which contains wireless clients connected to managed APs within the site. You can see the following wireless client metrics:

- By default, the following metrics are displayed:

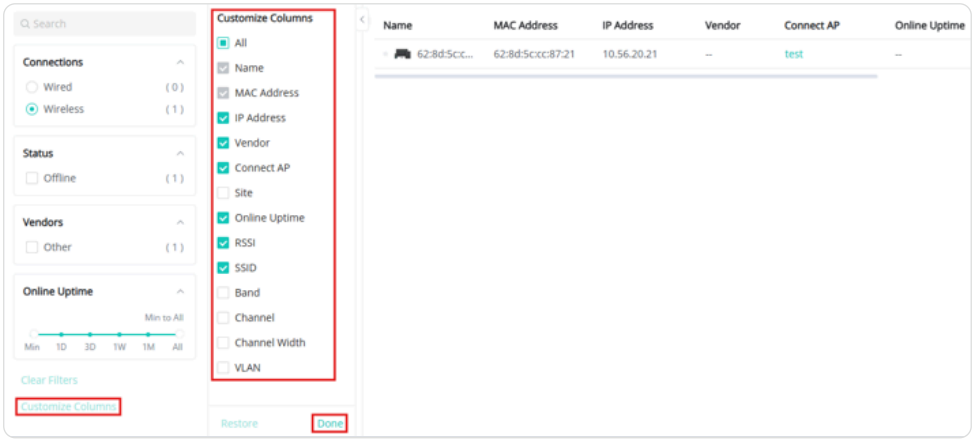
Table 1. Wireless Client Metrics

Metric	Description
Name	The name of the wireless client. During automatic client identification, AmpCon-Campus automatically assigns the MAC address of the

	wireless client as its name. **NOTE** The circle color in the **Name** column indicates the status of the wireless client: • **Green:** The wireless client is in **Online** status, which indicates it's up and connected to an AP. • **Gray:** The wireless client is in **Offline** status, which indicates it is down or isn't connected to any AP.
MAC Address	The MAC address of the wireless client.
IP Address	The IPv4 address of the wireless client. **NOTE** If the wireless client is offline, the value shown is the IP address obtained from the last connection with the AP.
Vendor	The manufacturer of the wireless client. **NOTE** The value is displayed as **--** if the wireless client is automatically identified by AmpCon-Campus but its vendor cannot be recognized.
Connect AP	The alias of its connected AP. You can click the AP name to view the AP side panel.
Online Uptime	The continuous online duration of the wireless client. Hover over the duration to view the last time this wireless client connected to the AP. **NOTE** The value is displayed as **--** if the wireless client is down or isn't connected to the AP.
RSSI	Short for Received Signal Strength Indicator. RSSI is used to indicate the strength of signals. The unit is

	dBm. Normally, the value is a negative number. The closer to 0, the stronger the signal.
SSID	The Service Set Identifier (SSID) of the wireless network to which the wireless client is connected. An SSID is used to distinguish a wireless network.

- To view more wireless client metrics, click **Customize Columns** in the sidebar, select or deselect metrics as needed, and then click **Done**.



The following client metrics can also be displayed:

Table 2. Additional Client Metrics

Metric	Description
Site	The currently selected site. You can click the site name to go to the site's "Dashboard" page.
Band	The radio band to which the wireless client is connected.
Channel	The channel of the radio.
Channel Width	The channel bandwidth. The unit is MHz.
VLAN	The VLAN ID of the wireless client. **NOTE** The value is displayed as **--** only when the network mode of the wireless client's SSID is

Default or **AP Assign IP (NAT_Mode)**.

For more information, see General Configurations-SSID Configurations.

Tips

- The **Name** and **MAC Address** metrics cannot be deselected.
- To display only the default metrics, click **Restore**.

4. To filter wireless clients, use the following filter conditions in the sidebar:

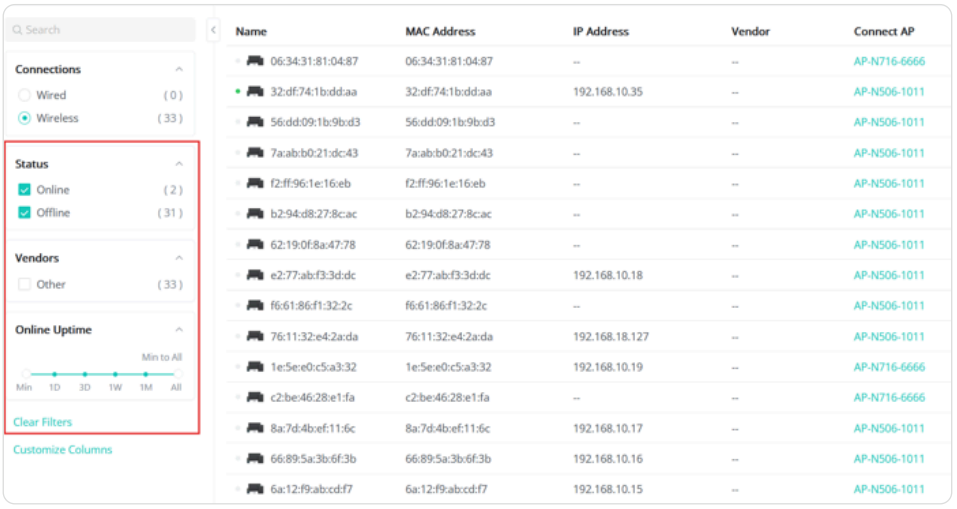


Table 3. Filter Conditions

Filter Condition	Description
Status	The statuses of wireless clients: **Online** or **Offline**. • **Online:** The client is online (the client is up and connected to an AP). • **Offline:** The client is offline (the client is down or isn't connected to an AP).
Vendors	The manufacturers of wireless clients. **NOTE** If you select **Other**, you can see wireless clients that are automatically identified by AmpCon-Campus but whose vendors cannot be recognized.

Online Uptime	The continuous online duration of the wireless clients. Select a time range in the **Online Uptime** section by clicking the starting time point and the end time point. The following time points can be clicked: • **Min** indicates the current time. • **1D** indicates 1 day. • **3D** indicates 3 days. • **1W** indicates 1 week. • **1M** indicates 1 month. • **All** indicates all times. **Examples:** • If you select the time range as **Min** to **All**, all clients are displayed. • If you select the time range as **3D** to **1M**, only online clients whose **Online Uptime** is between 3 days and 1 month are displayed. • If you select the time range as **Min** to **1D**, only online clients whose **Online Uptime** is less than or equal to 1 day are displayed. The clients that are not online are also displayed. • If you select the time range as **1W** to **All**, only online clients whose **Online Uptime** is greater than or equal to 1 week are displayed.

Tips

- If no devices match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of devices that match the filter option.
- To clear all these filter options, click **Clear Filters**.

Viewing Details of a Wireless Client

To view the detailed information of a wireless client, follow these steps:

1. On the “Clients” page, click the wireless client. You can see a side panel on the right.

2. In the **Overview** tab of the side panel, view the following information:

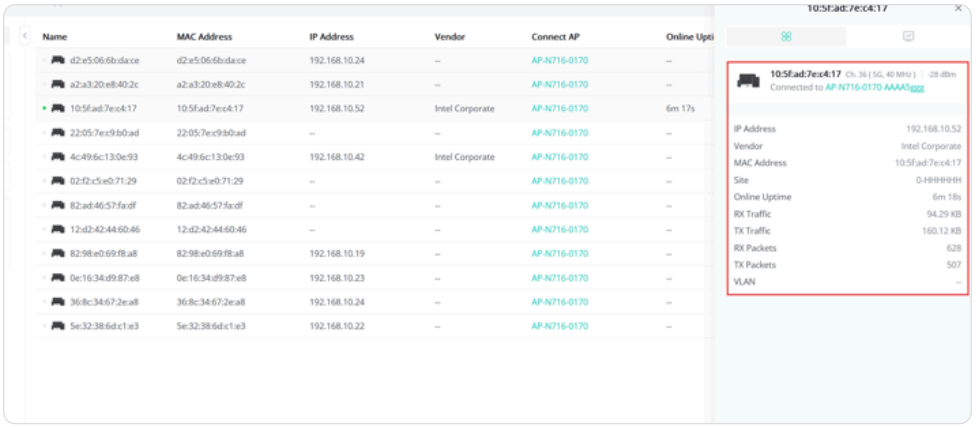


Table 4. Wireless Detail Metrics

Metric	Description
Name	The wireless client name.
Wireless Detail	The channel, radio band, channel bandwidth, RSSI, connected AP alias, and SSID. Click the AP alias or SSID, and then you can see the AP side panel. **NOTE** If the client is not connected to any AP currently, you can see the last connected AP and SSID and the last connection time.
IP Address	The IP address of the wireless client. **NOTE** If the wireless client is offline, the value shown is the IP address obtained from the last connection with the AP.
Vendor	The manufacturer of the wireless client. **NOTE** The value is displayed as **--** if the wireless client is automatically identified by AmpCon-Campus but its vendor cannot be recognized.

MAC Address	The MAC address of the wireless client.
Site	The currently selected site.
Online Uptime	The continuous online duration of the wireless client. Hover over the duration to view the last time this wireless client connected to the AP. **NOTE** The value is displayed as **--** if the wireless client is down or isn't connected to the AP.
RX Traffic	The total traffic received by the wireless client. **NOTE** The value is not reset after the client is disconnected from its AP. However, when the client reconnects to an AP, the value is reset and recalculated.
TX Traffic	The total traffic sent by the wireless client. **NOTE** The value is not reset after the client is disconnected from its AP. But when the client reconnects to an AP, the value is reset and recalculated.
RX Packets	The total number of packets received by the wireless client. **NOTE** The value is not reset after the client is disconnected from its AP. But when the client reconnects to an AP, the value is reset and recalculated.
TX Packets	The total number of packets sent by the wireless client. **NOTE**

	The value is not reset after the client is disconnected from its AP. But when the client reconnects to an AP, the value is reset and recalculated.
VLAN	The VLAN ID of the wireless client. **NOTE** The value is displayed as **--** only when the network mode of the wireless client's SSID is **Default** or **AP Assign IP (NAT_Mode)**. For more information, see General Configurations-SSID Configurations.

3. Click the **Insight** tab, and then view the following 3 sections:

- In the **Client Experience** section, view the client experience level, SNR, and status.

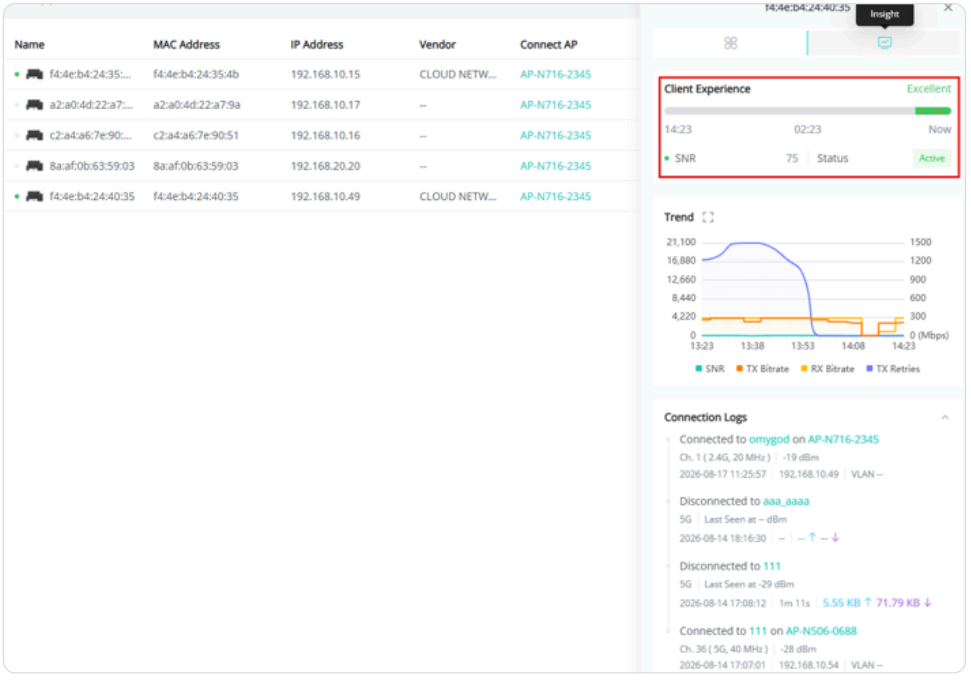
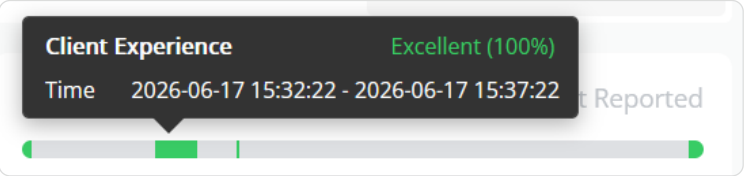


Table 5. Client Experience Information

Metric	Description
Client Experience	The client experience level. Different levels are marked in different colors. To view detailed client experience information in a time range, hover over the time range in the bar chart.

	• **Excellent:** The client experience score is equal to or greater than **80**. • **Good:** The client experience score is equal to or greater than **60** and less than **80**. • **Poor:** The client experience score is equal to or greater than **30** and less than **60**. • **Extremely Poor:** The client experience score is less than **30**. • **Not Reported:** AmpCon-Campus doesn't retrieve any information because the wireless client is disconnected from the AP during the time range.  **NOTEs** • The higher the client experience score, the better the user experience. • The **Poor** level indicates a degraded client experience and needs attention. • The **Extremely Poor** level indicates a nearly unusable client experience.
SNR	The ratio of signal power to noise power, which indicates the connection quality between the wireless client and the AP. • The higher the SNR, the better the connection quality. • The SNR is displayed as **--** if the wireless client is currently disconnected from the AP.
Status	The status of the wireless client. • **Active:** The wireless client is connected to the AP and is active. • **Inactive:** The wireless client is connected to the AP but is inactive. • **Offline:** The wireless client is not connected to the AP.

- In the **Trend** section, view the trend graphs of SNR, TX Bitrate, RX Bitrate, and TX Retries.

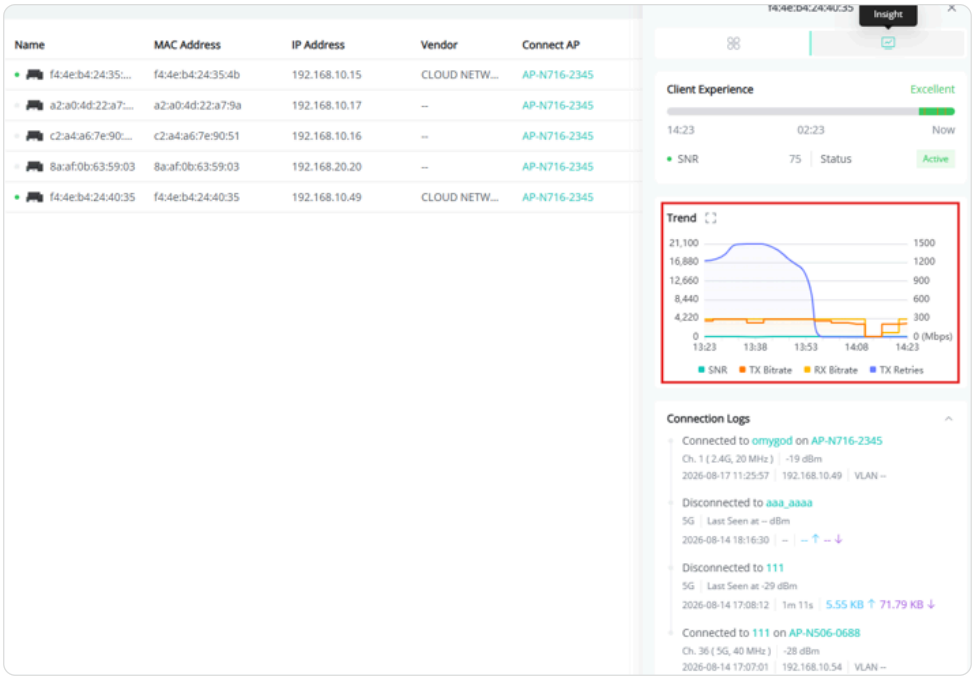


Table 6. Trend Graphs

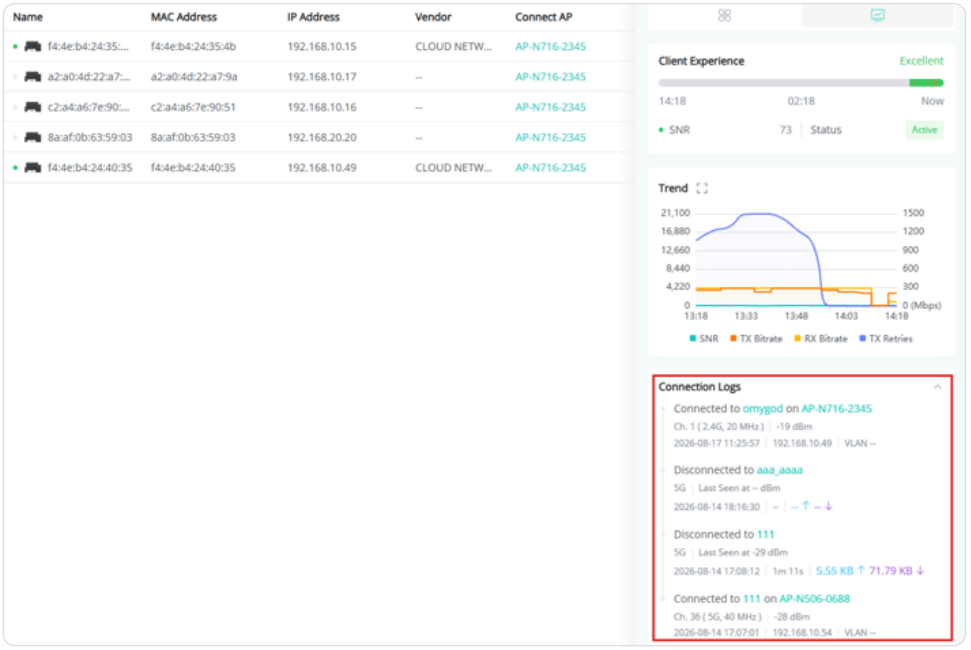
Metric	Description
SNR	The ratio of signal power to noise power, which indicates the connection quality between the wireless client and the AP. The higher the SNR, the better the connection quality.
TX Bitrate	The bitrate of data sent by the wireless client to the AP.
RX Bitrate	The bitrate of data received by the wireless client from the AP.
TX Retries	The number of transmission retries sent by the wireless client.

Tips

- By default, the trend graphs display data in the last 1 hour. To change the display time range, click the expand icon, and then click **6H** or **24H** in the pop-up window.
- To view the metric details at a specific time point, hover over that time point.

- To display or hide the data of a metric, click the square before the metric.

- In the **Connection Logs** section, view the connection and disconnection logs between the wireless client and its connected AP.



Tips

- At most 6 logs can be displayed. To view more logs, click **Show More**.
- Click the arrow to collapse the logs.
- Click the SSID or AP alias, and then you can see the AP side panel. For more information, see Basic Information of an AP, Deep Insights into an AP, and Configurations and Operations of an AP.

Alerting

AmpCon-Campus can issue immediate alerts when a device failure or a performance shift is detected. You can view these alerts to diagnose root causes and resolve problems quickly.

If you can't access the AmpCon-Campus UI to view alerts but need immediate alerts when issues arise, use the alert notification feature to receive real-time email notifications. In this way, you can promptly find problems and prevent incident escalation.

See the following child topics:

不能呈现 {children}。 无法向您显示此信息，因为您无权访问该内容。

Alert Types

AmpCon-Campus supports different types of alerts. Check the following supported alert types.

- Guidelines
- Device Offline Alerts
- Packet Loss Alerts
- Resource Usage Alerts
- Interface Monitoring Alerts
- Optical Module Alerts

Guidelines

- All the following types of alerts can be displayed in the alert list.
- All the following types of alerts except **Device Offline** alerts can be used for email alert notifications.

Device Offline Alerts

Table 1. Device Offline Alerts

Alert Metric	Alert Scope	Triggering Condition	Alert Level
Device Connectivity	PicOS switches	The switch status changes from **Online** to **Offline** compared with 1 minute earlier. Online means the switch is connected to AmpCon-Campus. Offline means the switch is disconnected from AmpCon-Campus.	Error

Packet Loss Alerts

Table 2. Packet Loss Alerts

Alert Metric	Alert Scope	Triggering Condition	Alert Level
In Errors	PicOS switches	Within 5 minutes, the increment of ingress erroneous packets on the port exceeds 500, or the ingress	Error

		erroneous packet rate exceeds 0.1%.	
Out Errors	PicOS switches	Within 5 minutes, the increment of egress erroneous packets on the port exceeds 500, or the egress erroneous packet rate exceeds 0.1%.	Error
In Discards	PicOS switches	Within 5 minutes, the increment of ingress discarded packets on the port exceeds 5000, or the ingress discarded packet rate exceeds 1%.	Error
Out Discards	PicOS switches	Within 5 minute, the increment of egress discarded packets on the port exceeds 5000, or the egress discarded packet rate exceeds 1%.	Error
In FCS Errors	PicOS switches	Within 5 minutes, the increment of ingress FCS error packets on the port exceeds 500, or the ingress FCS error packet rate exceeds 0.1%.	Error

Resource Usage Alerts

Table 3. Resource Usage Alerts

Alert Metric	Alert Scope	Triggering Condition	Alert Level
CPU Usage	PicOS switches	The CPU usage is greater than or equal to 85% and less than 95%.	Warning
		The CPU usage is greater than or equal to 95%.	Error
Memory Usage	PicOS switches	The memory usage is greater than or equal to 85% and less than 95%.	Warning

		The memory usage is greater than or equal to 95%.	Error
In Bandwidth Usage	PicOS switches	The inbound bandwidth usage is greater than or equal to 85%.	Warning
Out Bandwidth Usage	PicOS switches	The outbound bandwidth usage is greater than or equal to 85%.	Warning
Fan PWM Usage	PicOS switches	The fan PWM duty cycle (proportion of the fan's PWM to the total width) is greater than or equal to 85%, or less than or equal to 10%.	Warning
RPSU Power-on	PicOS switches	The PSU status (on or off) changes compared with 1 minute earlier.	Warning

Interface Monitoring Alerts

Table 4. Interface Monitoring Alerts

Alert Metric	Alert Scope	Triggering Condition	Alert Level
Admin Status	PicOS switches	The port status (**Up** or **Down**) manually configured by the network administrator changes compared with 1 minute earlier.	Info
Operation Status	PicOS switches	The actual operational port status changes from **Up** to **Down** compared with 1 minute earlier.	Error
MTU	PicOS switches	The MTU value changes compared with5 minutes earlier.	Info
Loopback Mode	PicOS switches	The loopback mode (enabled or disabled) on this port changes compared with 5 minutes earlier.	Info

Duplex Mode	PicOS switches	The duplex mode (half duplex or full duplex) changes compared with 1 minute earlier.	Warning
Port Speed	PicOS switches	The configured maximum data transfer rate changes compared with 1 minute earlier.	Warning

Optical Module Alerts

Table 5. Optical Module Alerts

Alert Metric	Alert Scope	Triggering Condition	Alert Level
Optical Module Temperature	PicOS switches	The temperature of the optical module connected to the switch is greater than or equal to 75 °C and less than 90 °C.	Warning
		The temperature of the optical module connected to the switch is greater than or equal to 90 °C.	Error

Checking the Alert List

AmpCon-Campus uses monitoring data to detect equipment failures and performance anomalies and to trigger immediate alerts.

By checking these alerts, you can take corrective actions before issues are escalated.

Viewing Alerts
Acknowledging Alerts
Closing Alerts
Deleting Alerts

Viewing Alerts

1. In the AmpCon-Campus UI, select a site that you want to monitor.
2. Click the **Alerts** icon from the navigation bar. On the “Alerts” page, you can see all alerts of the selected site by default.

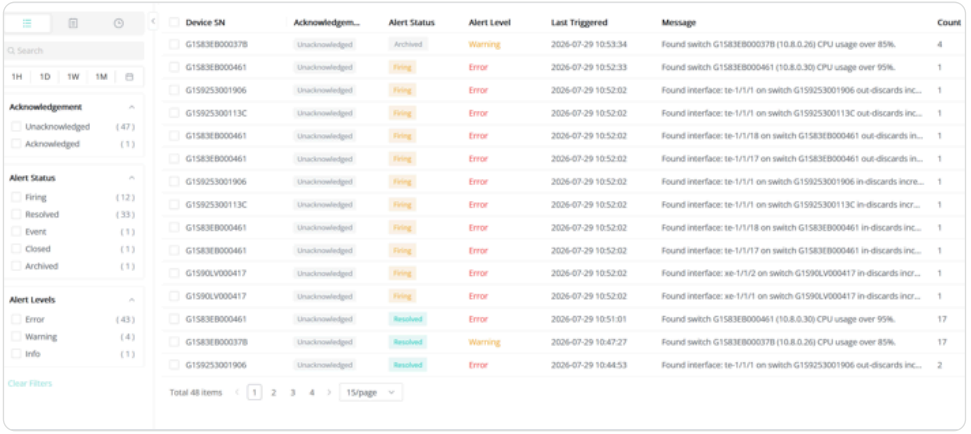


Table 1. Alert Metrics

Metric	Description
Device SN	The serial number (SN) of the device (switch or access point).
Acknowledgement	Indicates whether the alert has been acknowledged. To acknowledge an alert item, see Acknowledging Alerts.
Alert Status	The status of the alert. • **Firing:** The alert is being triggered. • **Resolved:** The associated issue has been resolved, and thus the triggering conditions are no longer met.

	• **Event:** This is a one-time event alert with no Firing-to-Resolved lifecycle. • **Closed:** The alert is manually closed by an AmpCon-Campus user. For more information, see Closing Alerts. • **Archived:** After the associated switch is deleted or moved to another site, the alert will transition to the **Archived** status. Alerts in **Archived** status will not participate in the Firing-to-Resolved lifecycle. Switch alerts triggered after switch deletion or site move will not be displayed in this site. **NOTE** AmpCon-Campus automatically deletes **Event** and **Resolved** alerts whose last trigger occurred more than 90 days ago.
Alert Level	The severity level of the alert. • **Error:** Error alert, which indicates a severe or critical fault that affects service availability, device functionality, or system operation. Immediate intervention is required to restore normal services. • **Warning:** Warning alert, which indicates a potential issue or abnormal state that does not immediately interrupt services but might lead to faults or performance degradation if not addressed in a timely manner. • **Info:** Info alert, which indicates a routine notification of normal system events for information reference only, with no fault or risk involved. **NOTE** Acknowledged Warning-level CPU usage, memory usage, and optical module temperature alerts revert to unacknowledged when escalated to the Error level.

Last Triggered	The last time the alert was triggered. The displayed time is based on your browser's time zone.
Message	The alert details.
Count	The number of times the alert has been triggered. **NOTEs** • After an alert item transitions to the **Resolved** status or an **Event** alert item is acknowledged, the alert count will not increase. The next time the same alert is triggered, a new alert item will be displayed in the alert list. • After an alert item is in **Closed** status, the alert count will not increase. The next time the same alert is triggered, no new alert item will be displayed. • After an alert item is deleted, the next time the same alert is triggered, a new alert item will be displayed in the alert list. For more information, see Deleting Alerts.

3. Optional: Filter alerts by using one or multiple filter options:

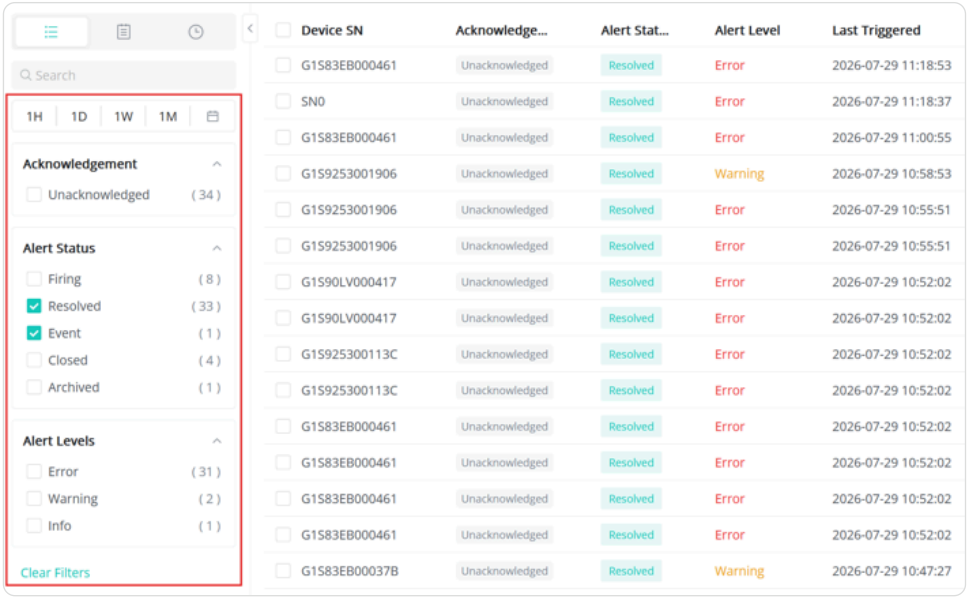


Table 2. Filter Options

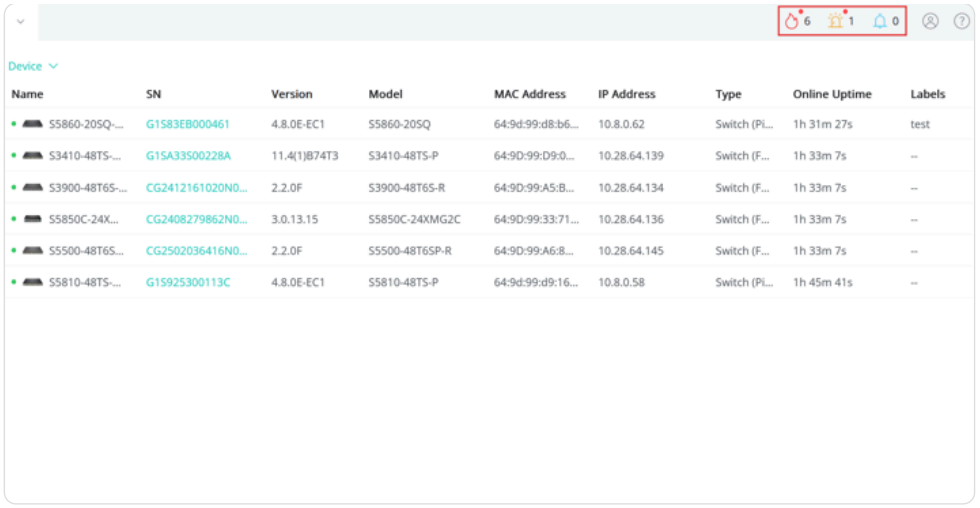
Option	Description
Time	Click **1H**, **1D**, **1W**, or **1M**. Then, the alerts in the last 1 hour, 1 day, 1 week, or 1 month are displayed. You can also specify the time range by clicking the calendar icon and selecting the start time and end time. By default, all alerts of the site are displayed.
Acknowledgement	Select **Unacknowledged**, **Acknowledged**, or both to display acknowledged alerts, unacknowledged alerts, or both.
Alert Status	Select one or multiple alert statuses: **Firing**, **Resolved**, **Event**, **Closed**, and **Archived**.
Alert Levels	Select one or multiple alert levels: **Error**, **Warning**, and **Info**.

Tips

- If no alerts match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of alerts that match the filter option.
- To clear all these filter options, click **Clear Filters**.

4. In the top-right corner, you can view the count of firing Error alerts, firing Warning alerts, and unacknowledged Event alerts.

- If any **Error alerts** are firing and have not been viewed by any user, the Error alert icon is highlighted with a red circle. Click the icon to view these alerts.
- If any **Warning alerts** are firing and have not been viewed by any user, the Warning alert icon is highlighted with a red circle. Click the icon to view these alerts.
- If any **Event alerts** have not been acknowledged by any user, the Event alert icon is highlighted with a red circle. You can click the icon to view these alerts.

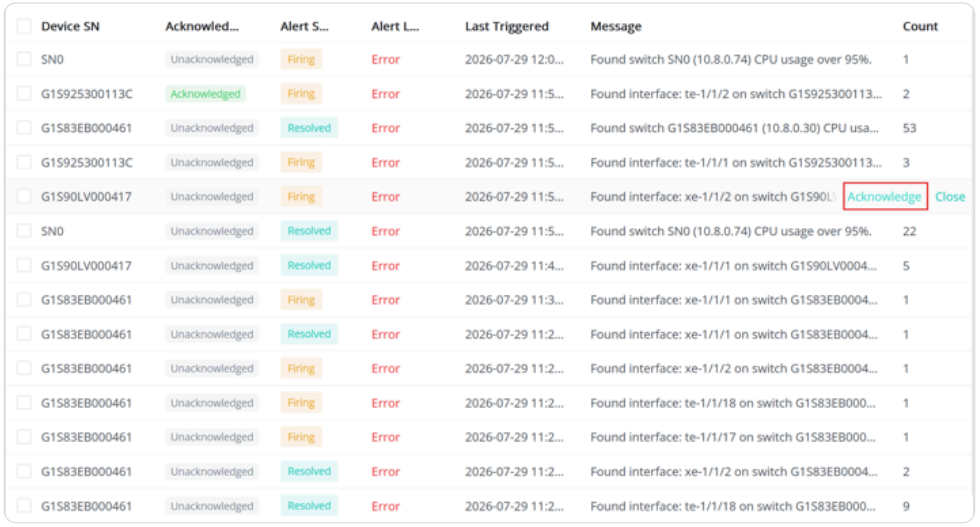


Acknowledging Alerts

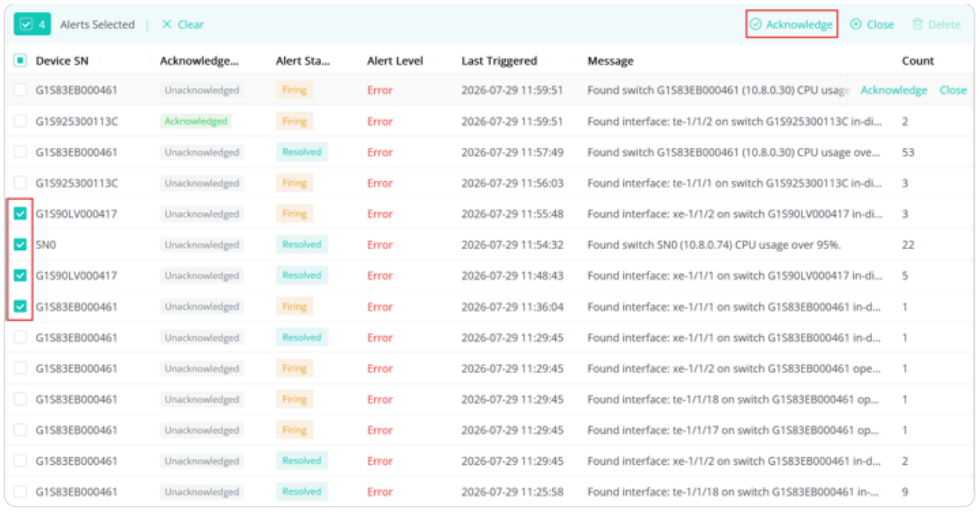
To acknowledge alert items, follow these steps:

> **NOTEs**
>
> - Acknowledging an alert item indicates that you are aware of the alert-related issue. It does **not** mean the issue is fixed.
> - The **Acknowledge** button is available only for unacknowledged alerts.

- To acknowledge an alert item, hover over it, and then click **Acknowledge**.



- To acknowledge multiple alert items, select these alerts, and then click **Acknowledge**.

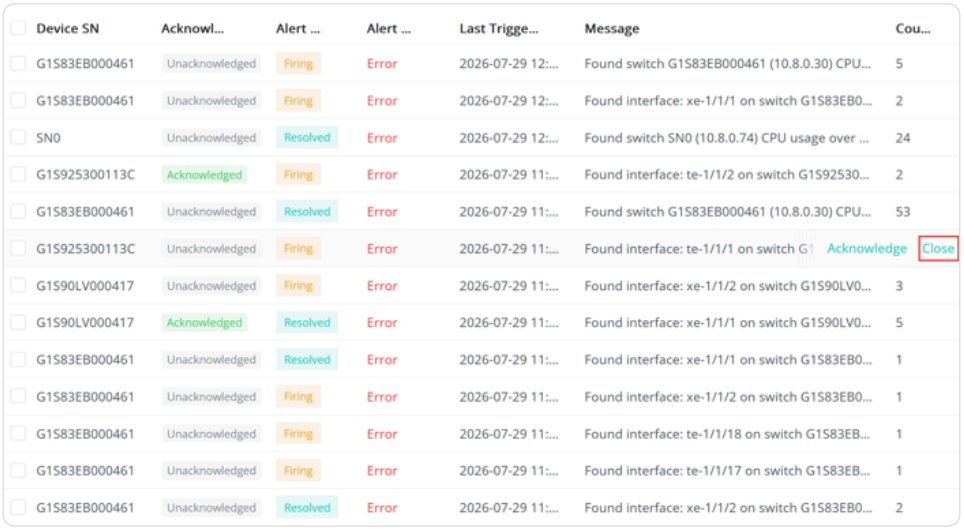


Closing Alerts

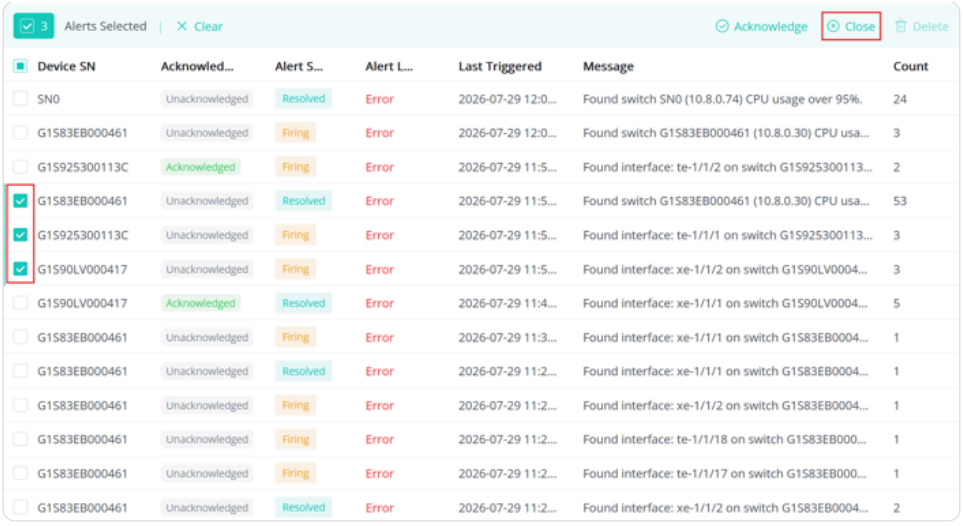
To close alert items, follow these steps:

> **NOTEs**
>
> - You can close an alert item if you no longer need the alert.
> - The **Close** button is available only for alerts that are not closed or archived.
> - Manually closed alert items are automatically marked as **Acknowledged**.

- To close an alert item, hover over it, and then click **Close**. In the pop-up window, click **Yes**.



- To close multiple alert items, select these alerts, and then click **Close**. In the pop-up window, click **Yes**.

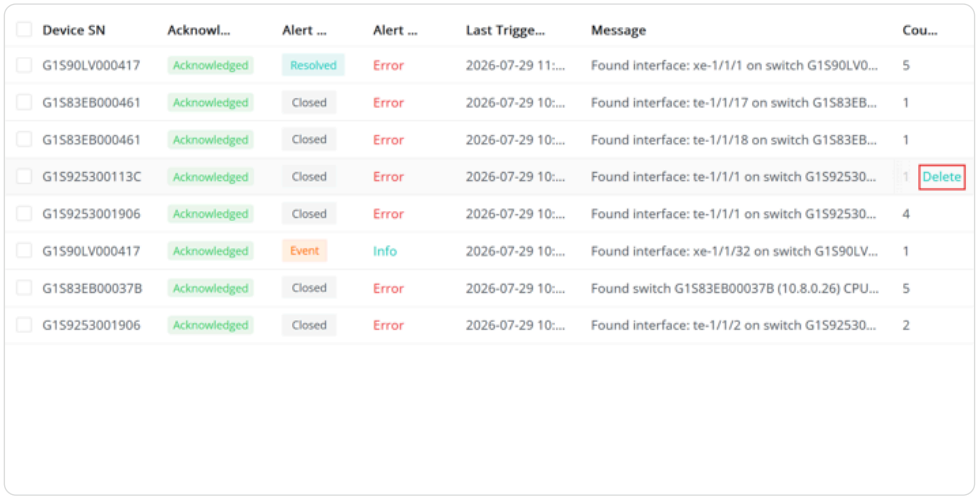


Deleting Alerts

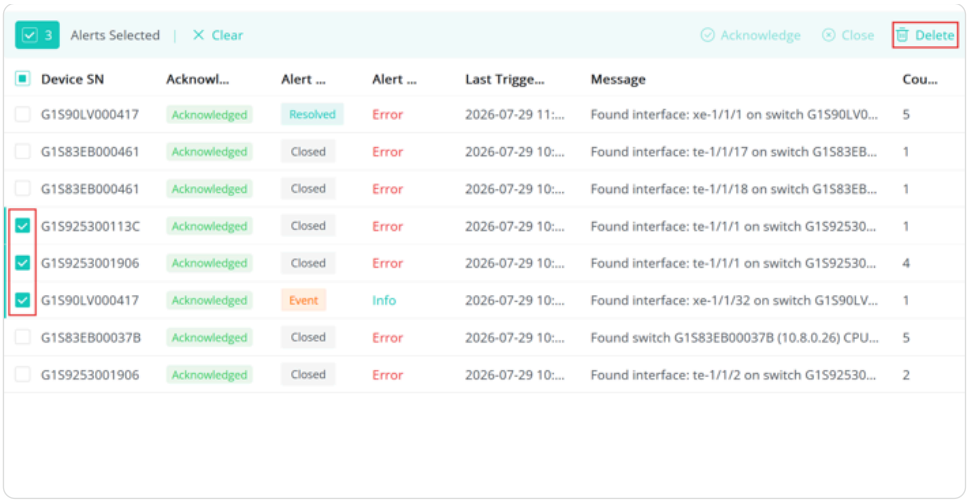
To delete alert items from the alert list, follow these steps:

> **NOTEs**
>
> The **Delete** button is unavailable for the following alert items:
>
> - Alert items in **Firing** status.
> - Unacknowledged alert items that are not in **Archived** status.

- To delete one alert, hover over the alert, and then click **Delete**. In the pop-up window, click **Yes**.



- To delete multiple alerts, select these alerts, and then click **Delete**. In the pop-up window, click **Yes**.


3 Alerts Selected
Clear
Acknowledge
Close
Delete
Device SN
Acknowl...
Alert ...
Alert ...
Last Trigge...
Message
Cou...
G1S90LV000417 Acknowledged Resolved Error 2026-07-29 11:... Found interface: xe-1/1/1 on switch G1S90LV0... 5
G1S83EB000461 Acknowledged Closed Error 2026-07-29 10:... Found interface: te-1/1/17 on switch G1S83EB... 1
G1S83EB000461 Acknowledged Closed Error 2026-07-29 10:... Found interface: te-1/1/18 on switch G1S83EB... 1
G1S925300113C Acknowledged Closed Error 2026-07-29 10:... Found interface: te-1/1/1 on switch G1S92530... 1
G1S9253001906 Acknowledged Closed Error 2026-07-29 10:... Found interface: te-1/1/1 on switch G1S92530... 4
G1S90LV000417 Acknowledged Event Info 2026-07-29 10:... Found interface: xe-1/1/32 on switch G1S90LV... 1
G1S83EB00037B Acknowledged Closed Error 2026-07-29 10:... Found switch G1S83EB00037B (10.8.0.26) CPU... 5
G1S9253001906 Acknowledged Closed Error 2026-07-29 10:... Found interface: te-1/1/2 on switch G1S92530... 2

Sending Email Alert Notifications

If you can't access the AmpCon-Campus UI to view alerts but need immediate notification when issues arise, use the alert notification feature to receive real-time email notifications. In this way, you can promptly find problems and prevent incident escalation.

To send alert notifications through emails, you need to add SMTP configurations and then configure notification rules.

- Prerequisite
- Procedure
  - Adding SMTP Configurations
  - Configuring Notification Rules
- Checking Alert Notification History

Prerequisite

Prepare an SMTP server and ensure it is available. AmpCon-Campus supports mainstream email service providers like Outlook and Gmail.

Procedure

Adding SMTP Configurations

SMTP servers are specialized applications responsible for sending, relaying, and routing email messages between senders and recipients over the internet or a network.

To receive alert notifications through emails, you must add SMTP configurations first.

1. In the AmpCon-Campus UI, click the **Settings** icon from the navigation bar.
2. In the sidebar, click **Email Setting**.
3. On the “Email Setting” page, input the following information:

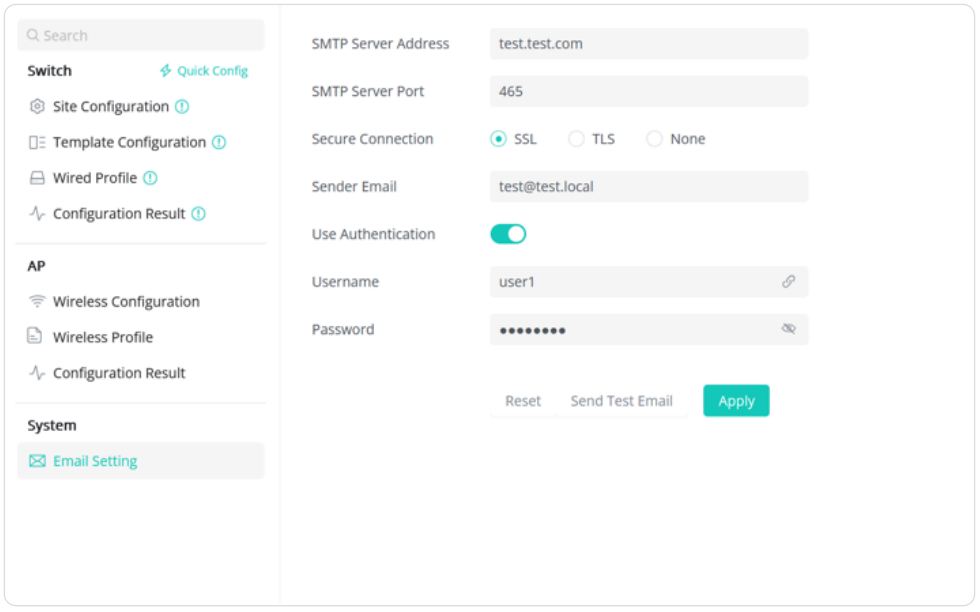


Table 1. SMTP Configuration Parameters

Parameter	Description
SMTP Server Address	The domain name or IP address of the SMTP server. The domain name or IP address must be correct and can contain at most 128 characters.
SMTP Server Port	The TCP port number used to connect to the SMTP server. The port number must range from 1 to 65535.
Secure Connection	The encryption method for secure email transmission, including **SSL**, **TLS**, or **None**. • **SSL:** The emails sent to this SMTP server are encrypted through SSL. • **TLS:** The emails sent to this SMTP server are encrypted through TLS. • **None:** The emails sent to this SMTP server are not encrypted.
Sender Email	The email address from which the email is sent. The email address must be correct and can contain at most 128 characters.

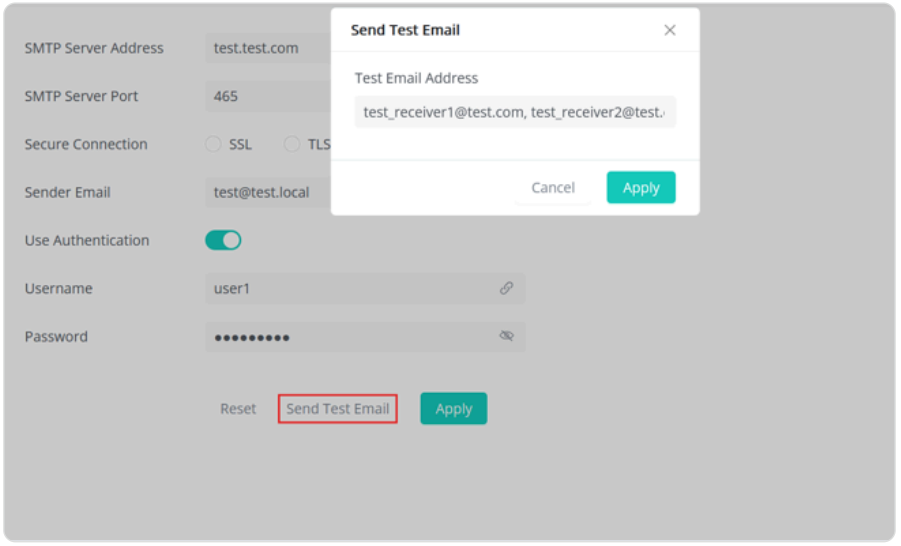
Use Authentication	Toggle it on to enable SMTP server authentication. Toggle it off to disable SMTP server authentication.
	
	• If you toggle it on, the SMTP server requires authentication for logged-in users. You must specify the following parameters:
	  ◦ **Username:** The name of the user to log in to the SMTP server.
	  ◦ **Password:** The password of the SMTP server user.
	• If you toggle it off, the SMTP server doesn't require authentication for logged-in users.
	
	NOTE
	
	The **Username** and **Password** can contain at most 128 characters.

4. Send a test email, and ensure that the test email can be received. Follow these steps:

   a. Click **Send Test Email**.

   b. In the **Test Email Address** field, enter one or multiple recipient email addresses, and then click **Apply**.

> **NOTEs**
>
> - Use commas (,) to separate email addresses.
> - Ensure that the recipient email addresses are correct. Otherwise, the test will fail.



5. Click **Apply** to complete the SMTP configuration.

> **Tips**
>
> - If SMTP configurations need to be changed, modify the configurations as needed, and then click **Apply**. Be sure to send a test email and verify that it can be received successfully.
> - To reset SMTP configurations, click **Reset**. After you reset SMTP configurations, configure a new SMTP server, and click **Apply**. Otherwise, AmpCon-Campus will still use the previous SMTP configurations.

Configuring Notification Rules

After you configure an SMTP server, configure notification rules. For each site, at most 100 notification rules can be added. Follow these steps:

1. Click the **Alerts** icon from the navigation bar.
2. Click the **Notification Rule** tab, and then click **+ Rule**.
3. In the pop-up window, input the following information, and then click **Apply**.

The **Site** field is automatically filled based on the current site and can't be changed.

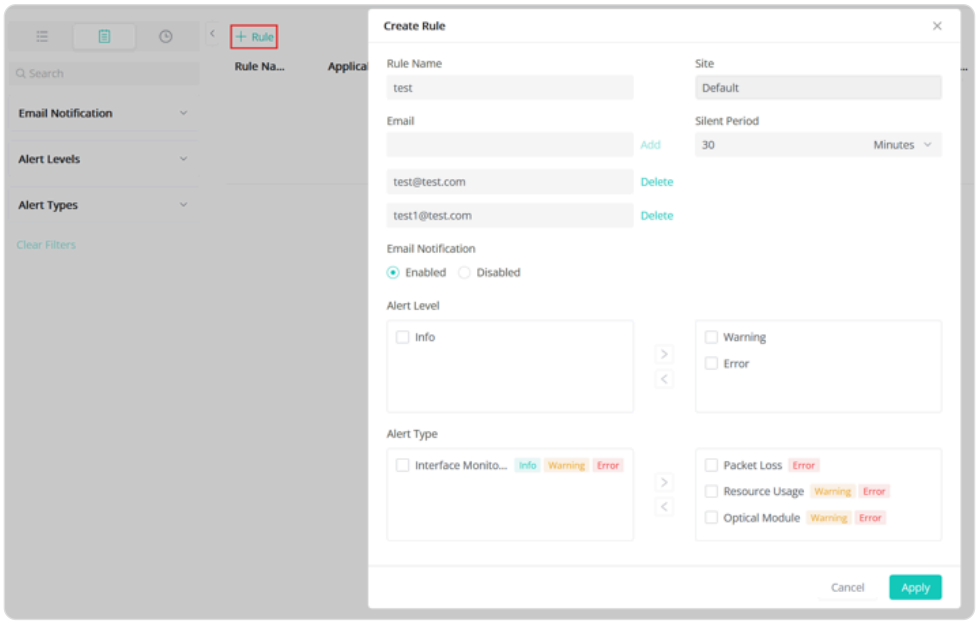


Table 2. Notification Rule Parameters

Parameter	Description
Rule Name	The name of the notification rule. • The rule name must be unique within a site. • The rule name can contain only letters, numbers, underscores, and hyphens. • The rule cannot start or end with a hyphen or underscore. • The rule name can contain at most 64 characters.
Email	The email addresses of the receivers to be notified. Each email address must be correct and can contain at most 128 characters. To add an email address, enter a valid email address, and then click **Add**. To delete an email address, click **Delete**. **NOTEs** • Within a site, recipient email addresses must be unique, and all notification rules can contain a maximum of 100 distinct recipient email addresses.

	• After an email address is added, you cannot edit it but can delete it and add a new one.
Silent Period	The period during which the same alert notification is not sent repeatedly. If the same alert is triggered multiple times during the silent period, you will receive only one alert notification. You can select **Minutes**, **Hours**, or **Days** as the time unit. To prevent email bombing, set the value to at least 30 minutes. If you set the silent period to a value less than 30 minutes, the silent period is changed to 30 minutes automatically. The maximum value is 43200 minutes (30 days or 720 hours).
Email Notification	Indicates whether to enable email notification. • **Enabled:** Alert notifications will be sent to the recipient email addresses and will be displayed on the “Notification History” page. • **Disabled:** Alert notifications will not be sent to the recipient email addresses and will not be displayed on the “Notification History” page. **NOTEs** • If you selected **Enabled**, only the selected levels and types of alerts can be sent to the recipient email addresses and displayed on the “Notification History” page. • Whether you enable email notification or not, all triggered alerts can be displayed in the alert list of the “Alerts” page. For more information, see Checking the Alert List.
Alert Level	Select the levels of alerts to be monitored in the left cell, including **Warning**, **Error**, and **Info**. Then, click **>**.

	To disable the monitoring of specific alert levels, select the alert levels in the right cell, and then click **<**.
Alert Type	Select the types of alerts to be monitored in the left cell, and then click **>**. To disable the monitoring of specific alert types, select the alert types in the right cell, and then click **<**. **NOTEs** • If you select an alert level, only the alert types associated with it can be selected. For alert types and associated alert levels, see Alert Types. • **Device Offline** alerts do not support email alert notifications.

4. Check the rule in the **Notification Rule** tab. You can filter notification rules through one or multiple filter options:

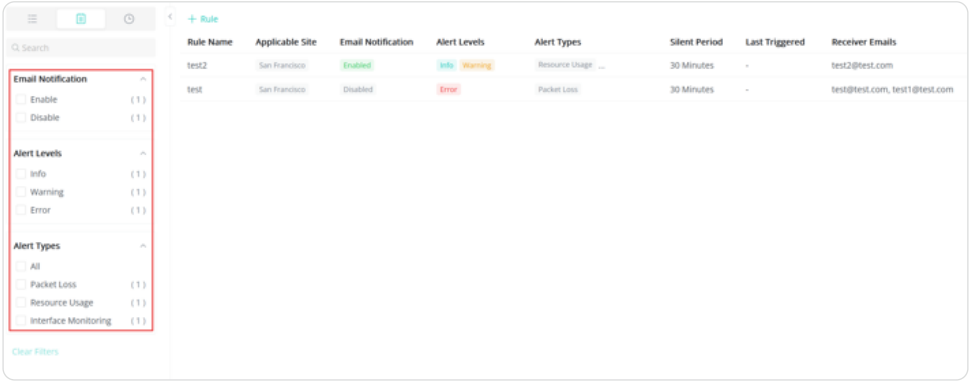


Table 3. Notification Rule Filter Options

Parameter	Description
Email Notification	Select **Enable**, **Disable**, or both. Then, the notification rules with email notification enabled, disabled, or both are displayed.
Alert Levels	Select one or multiple alert levels. Then, the notification rules monitoring these alert levels are displayed.

Alert Types	Select one or multiple alert types. Then, the notification rules monitoring these alert types are displayed.

Tips

- Selecting no filter options equals selecting all filter options.
- To clear all filter options, click **Clear Filters**.
- To edit a notification rule, hover over the rule, and then click **Edit**.
- To delete a notification rule, hover over the rule, and then click **Delete**.
- To check notification logs on the “Notification History” page, hover over the rule, and then click **Logs**.

5. Check whether you receive email notifications when alerts are triggered.

   If you do not receive email notifications, see Alert Notification Troubleshooting.

Checking Alert Notification History

You can view alert notifications for root cause analysis, fault prevention, or auditing. To check historical alert notifications in the last 30 days, follow these steps:

NOTE

AmpCon-Campus automatically deletes alert notifications sent more than 30 days ago.

1. Click the **Alerts** icon from the navigation bar.
2. Click the **Notification History** tab. On the “Notification History” page, view historical alert notifications.

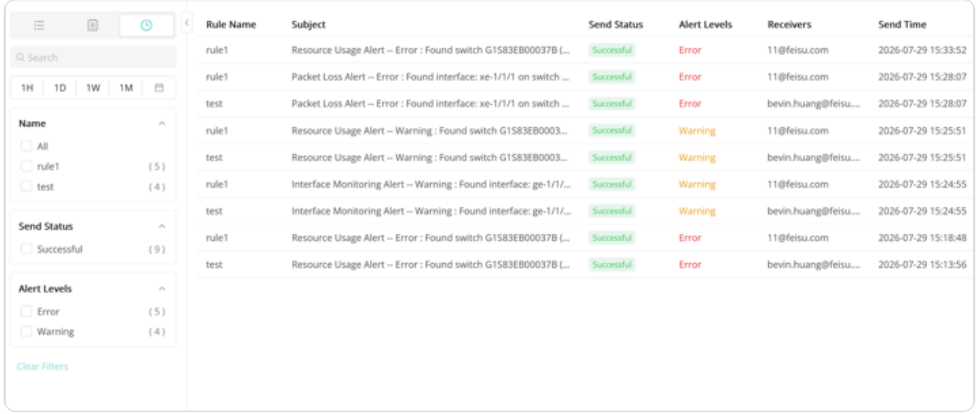


Table 4. Notification History Metrics

Metric	Description
Rule Name	The name of the alert notification rule. **NOTE** For those test emails specified when you add SMTP configurations, the **Rule Name** is displayed as **Test Email**.
Subject	The alert level and alert type related to the alert notification.
Send Status	Indicates whether the email is sent to recipient email addresses successfully.
Alert Levels	The alert level related to the alert notification.
Receivers	The email addresses of the receivers to be notified.
Send Time	The time the alert notification email was sent. **NOTE** The time is displayed based on your browser's time zone.

3. To filter alert notifications, use the following filter options:

Table 5. Alert Notification Filter Options

Parameter	Description
Time	Click **1H**, **1D**, **1W**, or **1M**. Then, the alerts in the last 1 hour, 1 day, 1 week, or 1 month are displayed. You can also specify the time range by clicking the calendar icon and selecting the start time and end time.
Name	Select one or multiple notification rule names. Then, alert notifications triggered by the selected notification rules are displayed.
Send Status	Select **Successful**, **Failed**, or both. Then, alert notifications that were sent successfully, failed, or

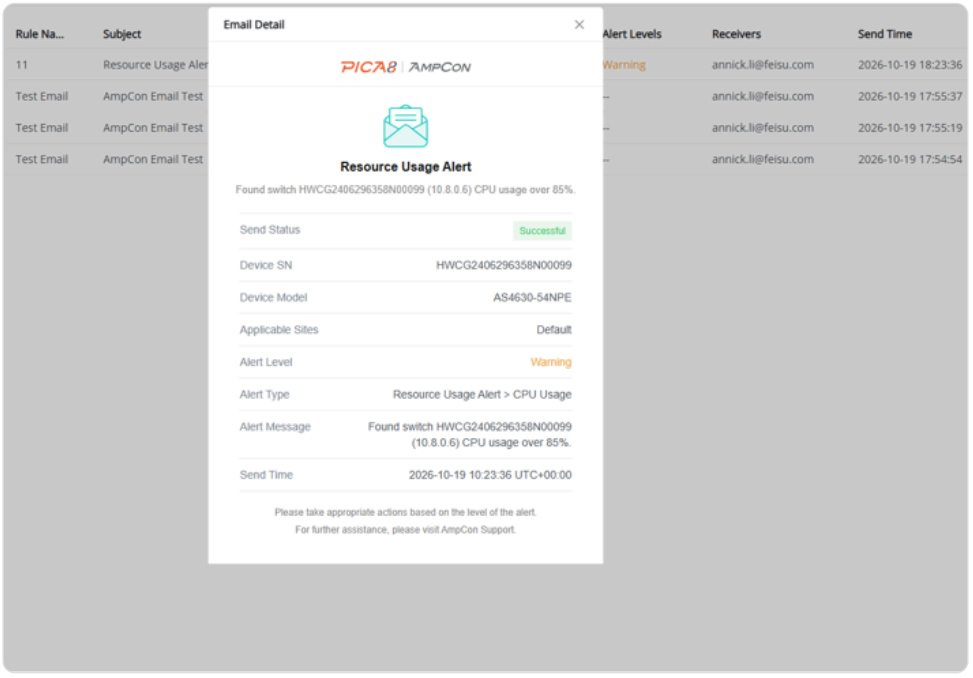
	both are displayed.
Alert Levels	Select one or multiple alert levels. Then, alert notifications for the selected alert levels are displayed.

Tips

- If no alert notifications match a filter option, the filter option is not displayed.
- Selecting no filter options equals selecting all filter options.
- Each filter option is followed by the count of alert notifications that match the filter option.
- To clear all filter options, click **Clear Filters**.

4. To view email contents of an alert notification, hover over the alert notification, and then click **Detail**.

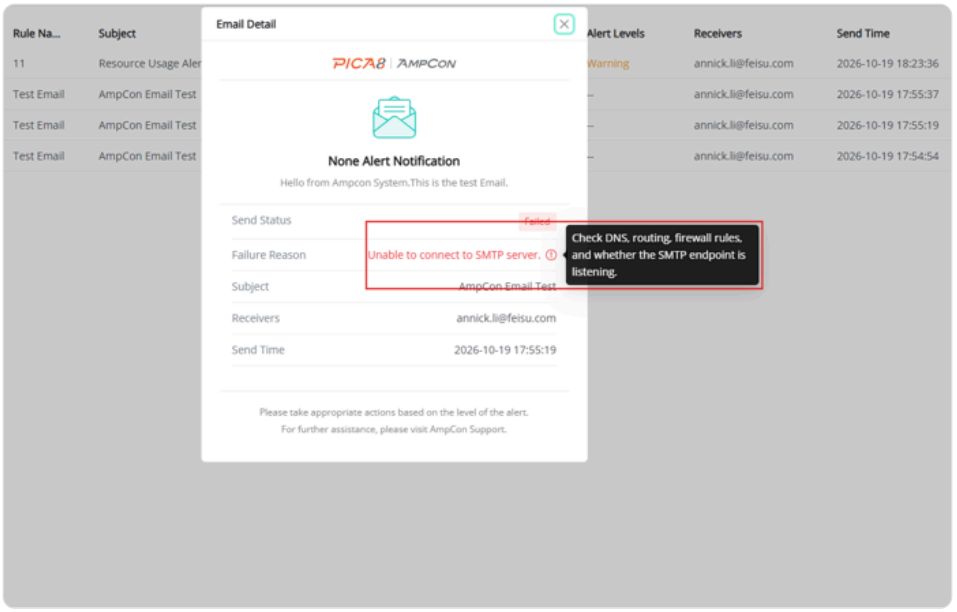
- If the **Send Status** is **Successful**, after you click **Detail**, you can see detailed information of the alert notification.



- If the **Send Status** is **Failed**, after you click **Detail**, you can see the failure reason in the pop-up window. Hover over the exclamation point (!) to see more information.

NOTEs

- If AmpCon-Campus successfully sends alert notification emails to the SMTP server, the **Send Status** is **Successful**. If not, the **Send Status** is **Failed**.
- If the **Send Status** is **Successful** but the recipient email addresses are incorrect, alert notifications will not be received by recipient email addresses.



5. To delete an alert notification, hover over it, and then click **Delete**.

Managing User Access

After deploying AmpCon-Campus, you can manage user access and assign proper permissions to each user.

AmpCon-Campus provides Role-Based Access Control (RBAC) to define different permission levels through roles. You can assign roles to users as needed.

- Guidelines
- Viewing Users
- Adding Users
- Managing Users
  - User Self-Management
  - Editing Users
  - Deleting Users
  - Locking or Unlocking Users
- User Permissions on Menu Pages

Guidelines

- The first time you log in to the AmpCon-Campus UI, use the default username **admin** and password **admin**. The user **admin** is the only account of the **Owner** role.
  - The user **admin** can view and manage all sites.
  - You cannot edit, delete, or lock the user **admin**.
- When you add or edit a user, assign the **Super Admin** or **Custom** role to the user.
  - **Super Admin** users can view and manage all sites.
  - If you select the **Custom** role, assign sites to the user, and set a site role for each assigned site. The site role can be **Site Admin** or **Readonly**.
  - A user with the **Site Admin** role of a site can view information and perform actions on pages under the site. A user with the **Readonly** role of a site can only view information under the site.
- Only **Owner** users and **Super Admin** users can view and manage user access on the “User” page.

Viewing Users

To view all users, follow these steps:

1. In the AmpCon-Campus UI, click the **User** icon from the navigation bar.
2. On the “User Management” page, view the following information:

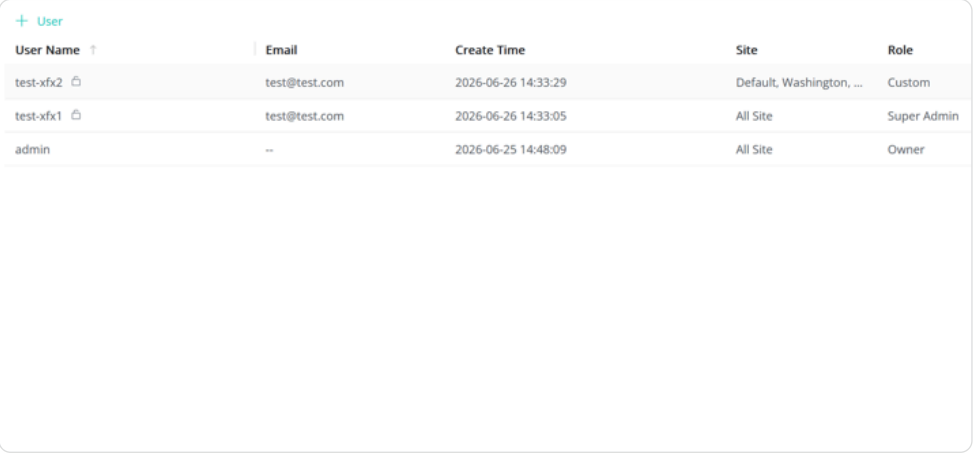


Table 1. User Metrics

Metric	Description
User Name	The name of the user.
Email	The email address of the user.
Create Time	The time when the user was added.
Site	The sites assigned to the user. For an **Owner** user or **Super Admin** user, **All Site** is displayed, indicating that the user can manage all sites. For a **Custom** user, only the sites assigned to the user are displayed. **NOTE** If a user is assigned only one site but the site is deleted, **--** is displayed. In this case, the user cannot log in to the AmpCon-Campus UI until additional sites are assigned to them.
Role	The role of the user. The value can be **Owner**, **Super Admin**, **Custom**, or **None**. **None** indicates the user has no role. **None** is displayed when all sites assigned to the user are deleted.

Adding Users

To add a user, follow these steps:

1. In the AmpCon-Campus UI, click the **User** icon from the navigation bar.
2. On the “User Management” page, click **+ User**.
3. In the pop-up window, input the following information:

> **NOTEs**
>
> - You cannot specify the user password here. All newly added users use the default password **pica8**.
> - Users can modify their own passwords. For more information, see the User Self-Management section.

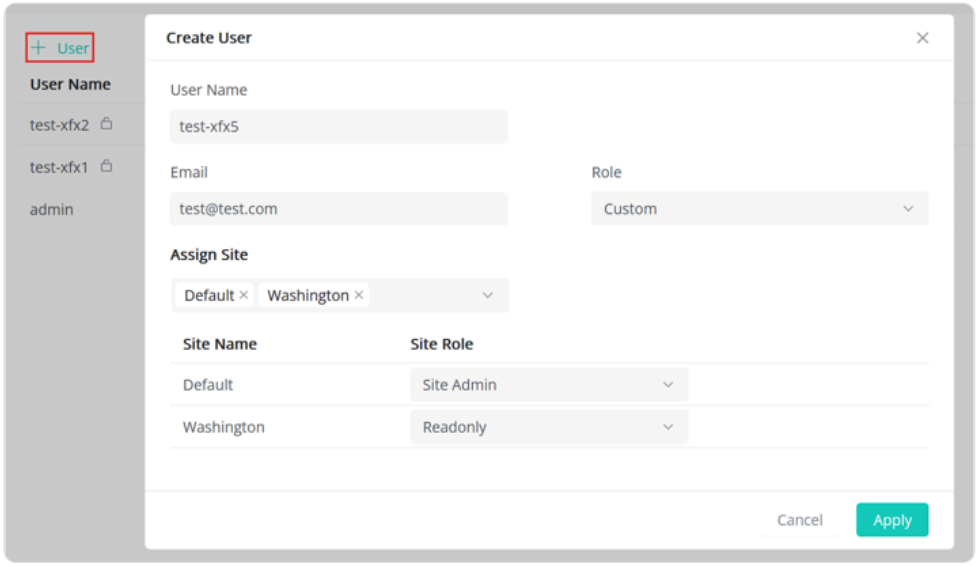


Table 2. User Parameters

Parameter	Description
User Name	The name of the user. • The name must be unique. • The name can contain only letters, numbers, underscores, and hyphens and supports a maximum of 64 characters. • The name cannot start or end with a hyphen (-) or underscore (_). • The name cannot match any case-insensitive variant of **admin** or **system**.
Email	The email of the user. The email address can contain at most 128 characters.
Role	The role of the user.

If you select **Super Admin (All Site)**, the user can view and manage all sites.

If you select **Custom**, you must assign sites to the user and specify site roles:

- In the **Assign Site** drop-down list, select one or multiple sites.
- Select a site role in the **Site Role** drop-down list for each selected site. The site role can be **Site Admin** or **Readonly**.

To deselect a site, click the delete icon in the **Assign Site** drop-down list, or hover over the site and then click **Delete**.

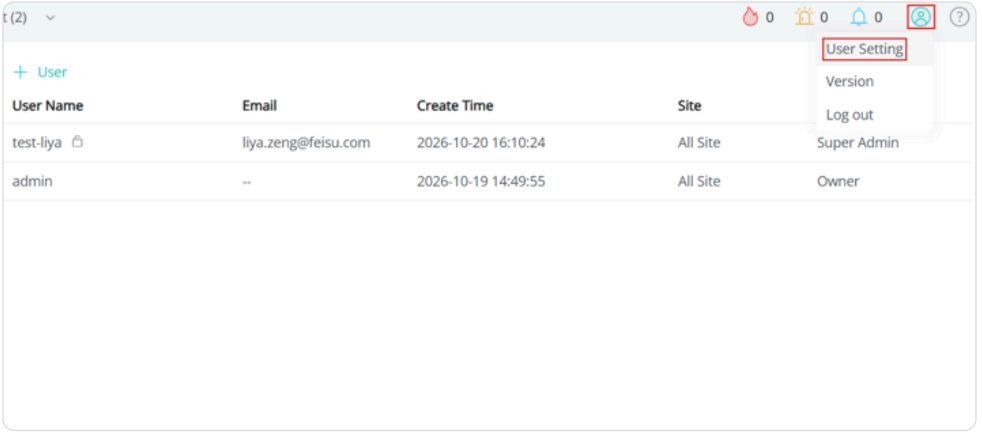
4. Click **Apply**.

Managing Users

User Self-Management

AmpCon-Campus users can change their own passwords and email addresses. Follow these steps:

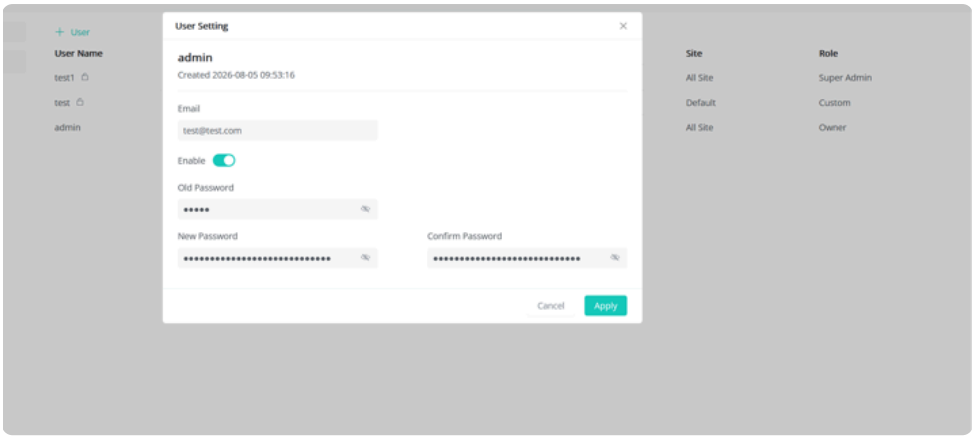
1. Click the user icon on the top right, and then click **User Setting**.



2. To change the email address associated with the currently logged-in user, enter a new email address in the **Email** field.
3. To change the user password, toggle on **Enable**, enter the old password in the **Old Password** field, enter a new password in the **New Password** field, and then enter the new password again in the **Confirm Password** field.

NOTEs

- You can enter a new password only if the entered old password is correct.
- The password needs to be a combination of uppercase letters, lowercase letters, numbers, and special symbols. The password must be 10 to 64 characters long.
- Click the eye icon to display the password. Click the eye icon again to hide the password.



4. Click **Apply**.

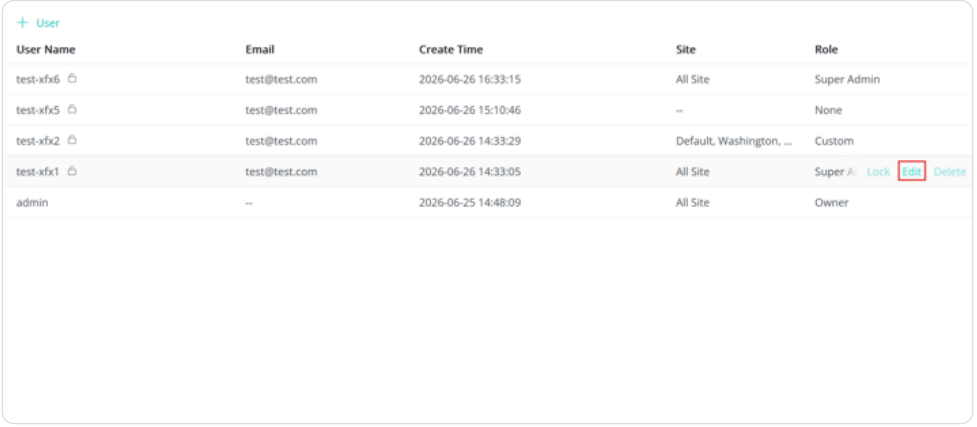
Editing Users

To edit an added user, follow these steps:

1. In the AmpCon-Campus UI, click the **User** icon from the navigation bar.
2. On the “User Management” page, hover over the user, and then click **Edit**.

NOTE

The built-in user **admin** cannot be edited.

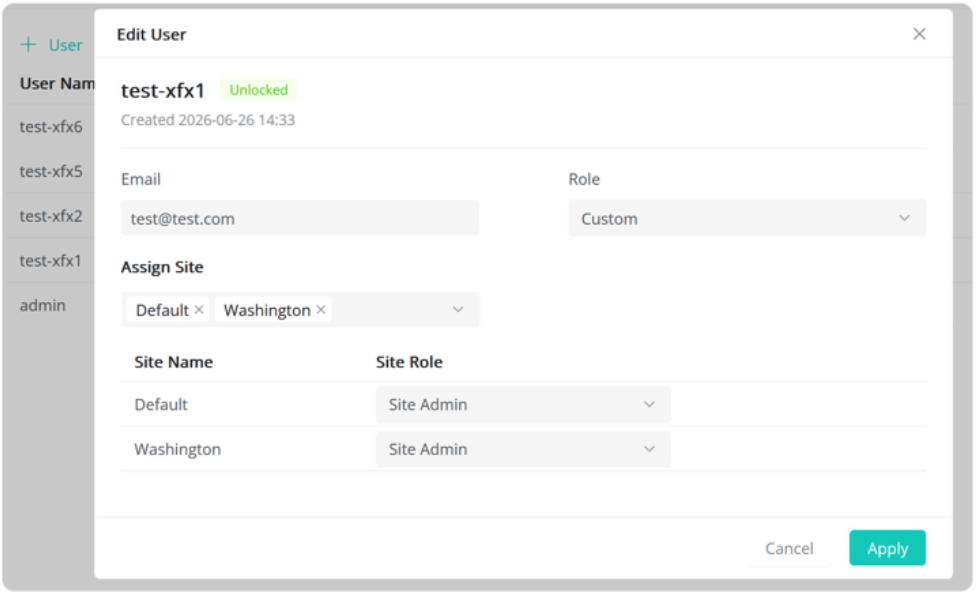


3. Modify the user information as needed, and then click **Apply**.

NOTEs

- If only one **Super Admin** user is left, you cannot change the user's role.
- Users can modify only their own email addresses here.
- A user can modify email addresses and roles and reset passwords for other users with the same role or lower roles here.

  For example, a **Super Admin** user can modify email addresses and roles and reset passwords for other **Super Admin** users, **Site Admin** users, and **Readonly** users.



Deleting Users

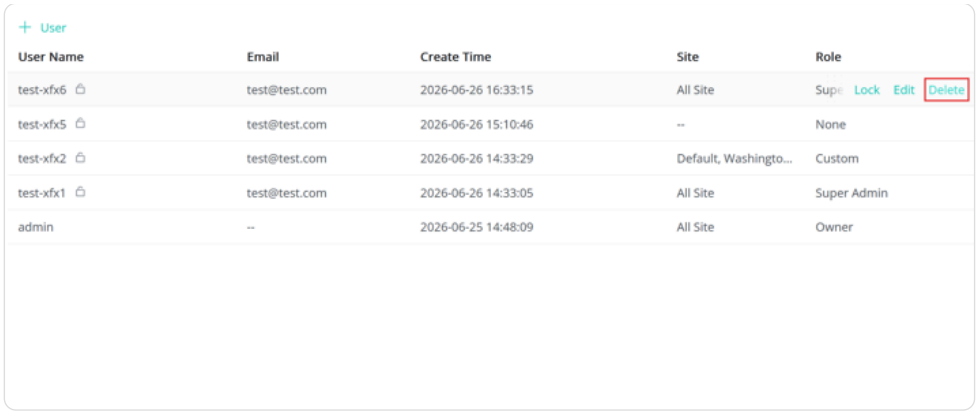
To delete a user, follow these steps:

1. On the "User Management" page, hover over the user, and then click **Delete**.

NOTEs

- The built-in user **admin** cannot be deleted.
- If only one **Super Admin** user is left, you cannot delete the user.
- Users cannot delete themselves.
- A user can delete other users with the same role or lower roles.

  For example, a **Super Admin** user can delete other **Super Admin** users, **Site Admin** users, and **Readonly** users.



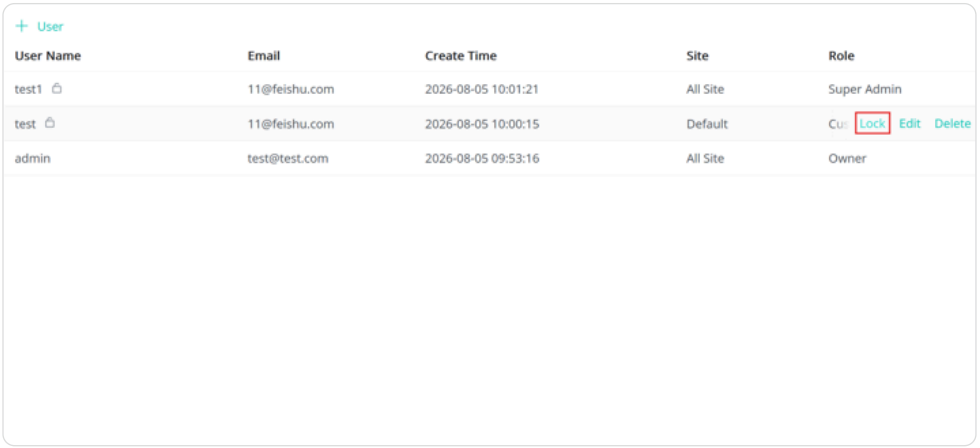
2. In the pop-up window, click **Yes** to confirm the deletion.

Locking or Unlocking Users

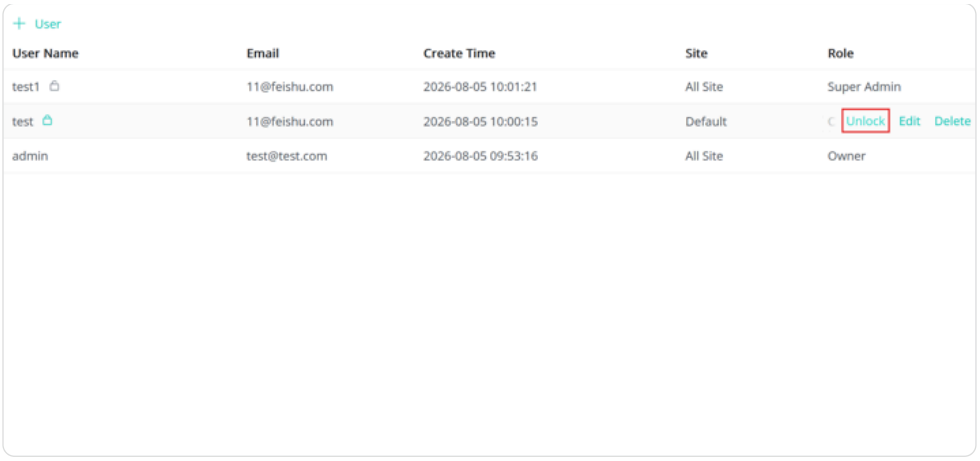
On the “User Management” page, you can lock a user to prevent the account from logging in to the AmpCon-Campus UI. Or you can unlock an added user to enable the login again.

> **NOTEs**
>
> - The built-in user **admin** cannot be locked or unlocked.
> - Users cannot lock or unlock themselves.
> - A user can lock or unlock other users with the same role or lower roles. For example, a **Super Admin** user can lock or unlock other **Super Admin** users, **Site Admin** users, and **Readonly** users.

- To lock an added user, hover over the user, and then click **Lock**. In the pop-up window, click **Yes**.



- To unlock an added user, hover over the user, and then click **Unlock**. In the pop-up window, click **Yes**.



User Permissions on Menu Pages

For menu pages in the AmpCon-Campus UI, different user roles have different permissions. AmpCon-Campus provides the following permission levels for pages and tabs:

- **Read**: Can only view information on a page or tab.
- **Write**: Can view information and perform actions (such as create, modify, and delete) on a page or tab.
- **No Access:** Cannot view information and perform actions on a page or tab.

For **Owner** users and **Super Admin** users, their permissions are granted for **all sites**. For **Site Admin** users and **Readonly** users, their permissions are granted only for **the assigned sites**.

Table 3. Menu Permissions

First-level menu	Second-level menu	Owner	Super Admin	Site Admin	Readonly
Site		Read & Write	Read & Write	Read	Read
Dashboard		Read & Write	Read & Write	Read & Write	Read
Topology		Read & Write	Read & Write	Read & Write	Read
Devices		Read & Write	Read & Write	Read & Write	Read
Clients		Read & Write	Read & Write	Read & Write	Read
Ports		Read & Write	Read & Write	Read & Write	Read

Settings	Switch	Read & Write	Read & Write	Read & Write	Read **Readonly** users cannot access the **Quick Config** wizard.
	AP	Read & Write	Read & Write	Read & Write	Read
	System	Read & Write	Read & Write	No Access	No Access
Alerts	Alert List	Read & Write	Read & Write	Read & Write **Site Admin** users can only delete or close alert items one by one.	Read
	Notification Rule	Read & Write	Read & Write	Read & Write	No Access
	Notification History	Read & Write	Read & Write	Read & Write	Read
Maintain	Upgrade Management	Read & Write	Read & Write	Read & Write **Site Admin** users cannot delete images.	No Access
	Wireless RRM Optimize	Read & Write	Read & Write	Read & Write	No Access
	Automation	Read & Write	Read & Write	Read & Write	No Access

	Tools	Read & Write	Read & Write	Read & Write	No Access
	Portal Configuration	Read & Write	Read & Write	No Access	No Access
	PicOS Switch	Read & Write	Read & Write	Read & Write	No Access
User	User management	Read & Write	Read & Write	No Access	No Access

Troubleshooting

To resolve common issues encountered while deploying or using AmpCon-Campus, see the troubleshooting topics below:

- Device Onboarding Troubleshooting
- Ansible Playbook Troubleshooting
- Alert Notification Troubleshooting

Device Onboarding Troubleshooting

If you fail to onboard switches and APs, refer to the following troubleshooting guides.

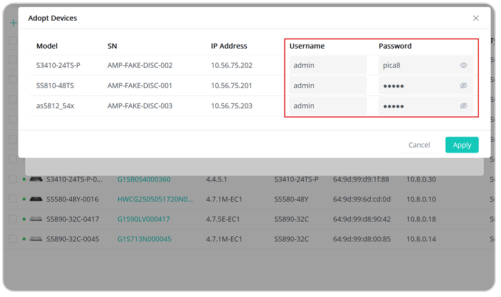
- Onboarding PicOS Switches
  - Adopting PicOS Switches
  - Importing PicOS Switches by SN
  - Importing PicOS Switches by IP Address
- Onboarding FSOS Switches
- Onboarding APs
  - Adopting APs
  - Importing APs by SN

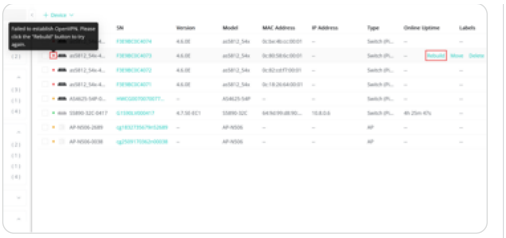
Onboarding PicOS Switches

Adopting PicOS Switches

If you fail to adopt a PicOS switch from the auto-discovery list, check the following possible reasons and solutions:

Table 1. PicOS Adoption Failure Reasons and Solutions

Reason	Solution
Unsupported Model: The switch is not supported by AmpCon-Campus.	Do not adopt the switch.
Failed SSH Authentication: The provided SSH username or password is incorrect, or SSH is disabled on the switch.	Ensure that the entered username and password can be used to log in to the switch. Ensure that SSH is enabled on the switch. 
Failed to Establish OpenVPN: The network between the switch and AmpCon-Campus is disconnected or unstable, or the ports 22, 9339, and 830 are suddenly blocked.	Resolve the connection issues first. Hover over the switch in the device list, and then click **Rebuild**. In the pop-up window, click **Yes** to re-establish OpenVPN.

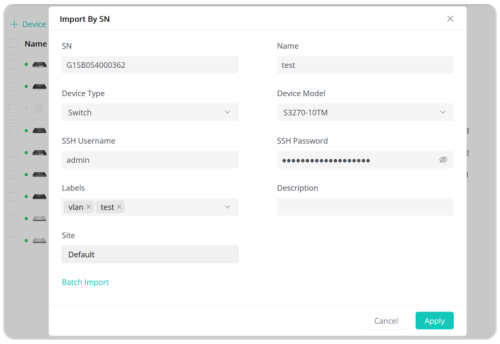
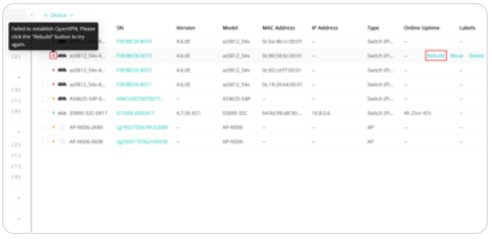


Importing PicOS Switches by SN

If you fail to import a PicOS switch by SN, check the following possible reasons and solutions:

Table 2. PicOS Import by SN Failure Reasons and Solutions

Reason	Solution
Device Already Exists: A switch with the same SN already exists in the device list and cannot be imported again.	No need to import the switch again.
Invalid SN: The SN is not correct.	Enter the correct SN of the switch.
Network Issue: The switch cannot be reached due to network-related problems, such as incorrect gateway configuration, physical network issues, firewall blockage, or ACL restrictions.	Resolve the network issues.
Not a PicOS Switch: The switch to be imported is not a PicOS switch.	Do not import the switch.
Unsupported Model: The switch is not supported by AmpCon-Campus.	Do not import the switch.
DHCP Not Configured: You haven't configured the DHCP server for the switch.	Configure the DHCP server. For more information, see Configuring a DHCP Server.
Failed SSH Authentication: The provided SSH username or password is incorrect, or SSH is disabled on the switch.	Ensure that the entered username and password can be used to log in to the switch. Ensure that SSH is enabled on the switch.

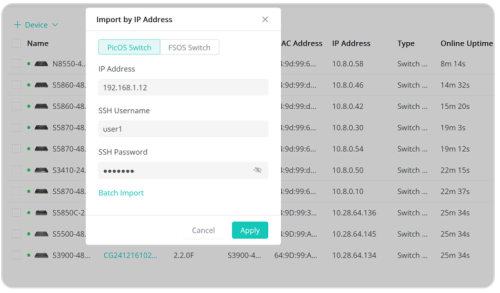
	
Incorrect Device Model: The device model selected in the pop-up window or entered in the template file does not match the switch.	Ensure that the device model matches the switch.
Failed to Establish OpenVPN: The network between the switch and AmpCon-Campus is disconnected or unstable, or the ports 22, 9339, and 830 are suddenly blocked.	Resolve the connection issues first. Hover over the switch in the device list, and then click **Rebuild**. In the pop-up window, click **Yes** to re-establish OpenVPN. 

Importing PicOS Switches by IP Address

If you fail to import a PicOS switch by IP address, check the following possible reasons and solutions:

Table 3. PicOS Import by IP Address Failure Reasons and Solutions

Reason	Solution
Invalid IP Address or Network Issue: The IP address is unreachable in the current network. The switch cannot be reached due to network-related problems, such as incorrect gateway configuration, physical network issues, firewall blockage, or ACL restrictions.	Enter a valid IPv4 address, and resolve the network issues.

Not a PicOS Switch: The switch to be imported is not a PicOS switch.	Do not import the switch.
Unsupported Model: The switch is not supported by AmpCon-Campus.	Do not import the switch.
Failed SSH Authentication: The provided SSH username or password is incorrect, or SSH is disabled on the switch.	Ensure that the entered username and password can be used to log in to the switch. Ensure that SSH is enabled on the switch. 
Failed to Establish OpenVPN: The network between the switch and AmpCon-Campus is disconnected or unstable, or the ports 22, 9339, and 830 are suddenly blocked.	Resolve the connection issues first. Hover over the switch in the device list, and then click **Rebuild**. In the pop-up window, click **Yes** to re-establish OpenVPN. 

Onboarding FSOS Switches

If you fail to import an FSOS switch, check the following possible reasons and solutions:

Table 4. FSOS Import Failure Reasons and Solutions

Reason	Solution
Invalid IP Address or Network Issue: The IP address is unreachable in the current network. The switch cannot be reached due to network-related problems, such as incorrect gateway configuration,	Enter a valid IPv4 address, and resolve the network issues.

physical network issues, firewall blockage, or ACL restrictions.	
Not an FSOS Switch: The switch to be imported is not an FSOS switch.	Do not import the switch.
Unsupported Model: The switch is not supported by AmpCon-Campus.	Do not import the switch.
Failed Authentication: The authentication fails for reasons such as entering a wrong username, password, or community.	Ensure that the entered SNMP authentication information matches the configurations on the target switch.
OIDs Blocked: The OIDs (Sysname, Serial Number, Model, System Description, MAC Address, and Version) are blocked on the switch. These OIDs must be accessible for the SNMP View feature.	Ensure that the OIDs are not blocked on the switch.

Onboarding APs

Adopting APs

If you fail to adopt an AP from the auto-discovery list, check the following possible reasons and solutions:

Table 5. AP Adoption Failure Reasons and Solutions

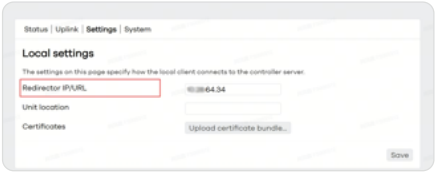
Reason	Solution
Network Issue: The network between the AP and AmpCon-Campus is disconnected or unstable.	Resolve the network issues.

Importing APs by SN

If you fail to import an AP by SN, check the following possible reasons and solutions:

Table 6. AP Import Failure Reasons and Solutions

Reason	Solution
Invalid SN: The AP SN is incorrect.	Enter the correct SN of the AP.
Incorrect Device Model: The device model selected in the pop-up window or entered in the template file does not match the AP.	Ensure that the device model matches the AP.
Network Issue: The AP cannot be reached due to network-related problems, such as incorrect gateway configuration, physical network issues, firewall blockage, or ACL restrictions.	Resolve the network issues.
Unsupported Model: The AP is not supported by AmpCon-Campus.	Do not import the AP.

AmpCon-Campus IP Address Not Configured: You have not pre-configured the IP address of AmpCon-Campus as described in the Prerequisites section.	Pre-configure the IP address of AmpCon-Campus by using one of the following ways: • Install a DHCP server, and configure the DHCP server to reserve an IP range for the APs. Configure DHCP Option 138 as the IP address of AmpCon-Campus. See the following DHCP Option 138 configuration example:  • Add the IP address of AmpCon-Campus in the **Redirector IP/URL** field of each AP webpage. See the following AP webpage configuration example: 

Ansible Playbook Troubleshooting

If a playbook fails to run on PicOS switches, refer to the following reasons and solutions:

- Playbook Content Issues
  - Symptom
  - Solutions
- Connection Issues
  - Symptom
  - Solutions

Playbook Content Issues

If the playbook content is wrong, the playbook cannot be run on selected PicOS switches.

Symptom

When you check the playbook execution result in the AmpCon-Campus UI, you can see the error log as follows:



Solutions

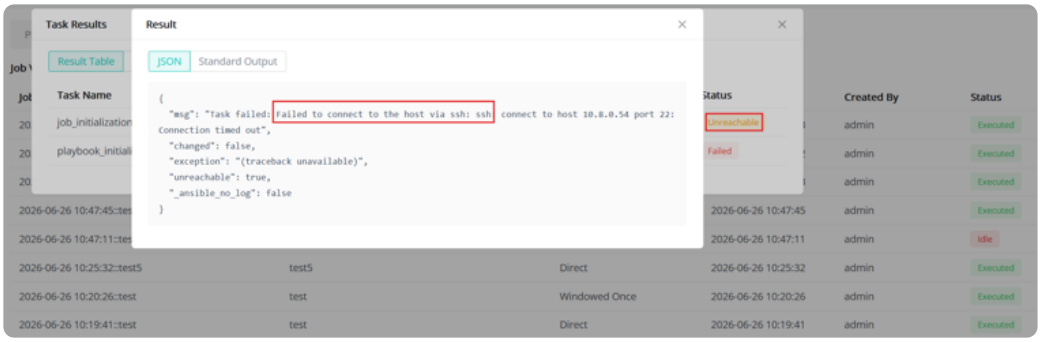
- Check whether you follow the syntax as described in Examples for Ansible Playbooks.
- Check whether the commands included in each playbook are correct.
- When you run a playbook with variables specified, check whether you have set the variable values in JSON format.
- If your playbook uses a configuration file, check whether you have clicked **+ File** to add the configuration file.

Connection Issues

If AmpCon-Campus fails to access the selected switches, the playbook cannot be run on these switches.

Symptom

When checking the playbook execution result in the AmpCon-Campus UI, you can see the error log as follows:



Solutions

- Bring the switches online (connected to AmpCon-Campus).
- Ensure that the **SSH Username** and **SSH Password** in the switch detail pop-up window are correct. For more information, see **Step 5** of Configuring a Single Switch.

Alert Notification Troubleshooting

If you fail to receive email notifications, check the following possible reasons and solutions:

Table 1. Failure Reasons

Reason	Solution
SMTP Configurations Not Added: You haven't added SMTP configurations.	Add correct SMTP configurations on the "Email Setting" page.
SMTP Server Inaccessible: AmpCon-Campus cannot connect to the SMTP server.	Ensure that the configured SMTP server is active and whitelisted in your firewalls and the configured SMTP port is allowed.
Authentication Failed: The configured username and password of the SMTP server are incorrect.	Ensure that the SMTP server's login username and password are correct.
Secure Connection Failed: The SSL or TLS configurations are incorrect in SMTP configurations.	Ensure that SSL or TLS protocol configurations are correct.
Sender Address Rejected: The sender email address configured in SMTP configurations is not allowed to send emails.	Ensure that the sender email address matches authorized sending lists in the SMTP gateway.
Recipient Address Rejected: The recipient email addresses configured in the notification rule are incorrect.	Check the recipient email list, and ensure no inactive or misspelled email address.
SMTP Sending Limit Reached: The SMTP sending limit is reached.	Request a higher rate limit quota from your mail delivery provider.
No Matching Alerts: No alerts matching the alert levels and alert types in the notification rule have been triggered.	Ensure that the alert levels and alert types configured in the notification rule meet your needs.

Email Notification Disabled: Email notification is disabled in the notification rule.	Ensure that email notification is enabled in the notification rule.
Silent Period Too Long: The **Silent Period** configured in the notification rule is too long. AmpCon-Campus suppresses duplicate alert notifications within the silent period.	Specify a shorter **Silent Period** in the notification rule.

Glossary

This glossary provides terms and definitions used on AmpCon-Campus. If you have feedback about how the glossary works, or have terms you'd like to see defined, let us know by adding a comment to this document.

Click one of the following letters to locate the terms and definitions starting with the letter.

A B C D E F G I M N O P R S T U V W Z

A

Access Switch

The switch that connects devices like computers, printers, and wireless access points to the rest of the network in an MLAG or IP Clos fabric.

Situated at the network's edge, access switches serve as the entry point for end user devices to communicate with each other and with the network infrastructure.

Access Point (AP)

The networking device that enables wireless devices (such as smartphones, laptops, and tablets) to connect to a wired local area network (LAN) or the Internet through Wi-Fi.

It acts as a bridge between wired and wireless networks, allowing wireless devices to communicate without using physical cables.

Alert

The event indicating a device failure or a performance shift.

Alert Level

The alert severity level. Alert levels include Error, Warning, and Info.

Alert Type

The type of each alert. Alert types include Packet Loss Alert, Resource Usage Alert, Interface Monitoring Alert, and Optical Module Alert.

Alert Notification

The method to receive real-time email notifications.

AmpCon-Campus License

The authorization license for managing PicOS switches through AmpCon-Campus.

Each AmpCon-Campus license contains Hardware IDs and expiration dates of PicOS switches to be managed by AmpCon-Campus. The AmpCon-Campus license needs to be imported to AmpCon-Campus.

Antenna

The device that transmits or receives wireless signals for wireless data transmission between devices.

Ansible

The open-source tool to automate configuration management, application deployment, and task automation.

Ansible Playbook

The simple, declarative language (written in YAML) used to automate your tasks.

You declare the desired state of a local or remote system in your playbook. Ansible ensures that the system remains in that state.

Ansible Job

The single execution of an Ansible playbook.

AP Overloading

The AP performance issue due to the fact that too many STAs are connected to a single AP.

AP Transmission Power

The energy output level of AP radio frequency. A higher level of AP transmission power means:

- A larger signal coverage range
- A higher probability of interference from other wireless devices

Address Resolution Protocol (ARP)

The Internet protocol used to map an IP address to a Media Access Control (MAC) address. It allows hosts and switches to determine the data link layer addresses through the ARP Request and ARP Response process.

Autonomous System (AS)

A collection of networks that are uniformly controlled by one or more management authorities and adopt the same routing strategy.

Each AS is assigned a globally unique 16-bit number, known as the Autonomous System Number (ASN).

B

Basic Service Set Identifier (BSSID)

The unique 48-bit identifier assigned to each Basic Service Set (BSS) in a wireless network.

Typically, the value is derived from the MAC address of the AP.

Border Gateway Protocol (BGP)

The routing protocol used to connect independent systems on the Internet. It is designed by the Internet Engineering Task Force (IETF) as a robust, scalable, and well-defined protocol for exchanging routing information among BGP routers within a single AS (IBGP) or among different AS (EBGP).

- External Border Gateway Protocol (EBGP): A routing protocol used to exchange routing information among different AS.
- Internal Border Gateway Protocol (IBGP): A routing protocol used to exchange routing information within a single AS.

BSS Coloring

The technology used in wireless networks to assign unique identifiers (colors) to different Basic Service Sets (BSS).

BSS Coloring enables efficient spectrum sharing and interference management within the same radio band.

C

Captive Portal

The authentication and access control technology forcibly redirecting users to a login page for wireless network permission management.

Channel

The frequency range allocated within the radio spectrum for transmitting data. Each channel has its designated center frequency and bandwidth.

By allocating channels reasonably, mutual interference between devices can be reduced, and network performance can be improved.

Channel Switch Announcement (CSA)

The management frame mechanism through which an AP notifies wireless devices (STAs) to switch channels. The notification is triggered in scenarios as follows:

- Channel interference or congestion avoidance
- Spectrum optimization (such as co-channel interference management of BSS Coloring)
- Regulatory compliance requirements (such as radar signal avoidance)

Channel Width

The frequency range (such as 80MHz) occupied by wireless signals in the frequency spectrum.

It directly affects the data transmission rate, signal coverage range, and anti-interference capability in a wireless network. A wider channel width means:

- A higher data transmission rate
- A weaker signal penetration
- A smaller signal coverage range
- Higher probability of interference from other wireless devices

Co-Channel Interference

The issue that wireless devices on the same channel interfere with each other.

Collapsed Core Switch

The switch situated in the collapsed core layer where the core and distribution layers are consolidated into a single unified structure.

Collapsed core switches exist in MLAG fabrics.

Core Switch

The switch that receives traffic from the distribution switches in an IP Clos fabric.

Core switches handle high-speed data transfer, connect different distribution switches, and ensure fast and reliable connections among devices in different subnets.

D

Database (DB)

A collection of structured data stored in computers and managed through the Database Management System (DBMS).

AmpCon-Campus stores its data in the AmpCon-Campus database.

Decommission (DECOM)

The method to revoke the PicOS license and configurations from a switch. The decommissioned switch will not be managed by AmpCon-Campus.

Dynamic Host Configuration Protocol (DHCP)

The network protocol used for automatically assigning IP addresses and related network configuration parameters.

DHCP Server

The system that dynamically assigns information such as IP addresses, subnet masks, default gateways, and DNS servers to devices like switches.

DHCP Snooping

The Layer 2 security function that monitors and controls DHCP traffic on a network. It inspects DHCP messages and blocks unauthorized DHCP servers from distributing IP addresses, thereby mitigating potential attacks such as DHCP spoofing or rogue server activity.

DHCP Relay

The function implemented in Layer 3 switches to forward DHCP messages between DHCP clients and DHCP servers across different subnets.

Distribution Switch

The switch that receives traffic from access switches and forwards it to core switches in an IP Clos fabric.

Distribution switches act as intermediaries that aggregate data from multiple access switches before routing it to core switches.

Dynamic Frequency Selection (DFS)

The technology used in wireless networks to avoid interference with radar systems (such as military, weather, or satellite radar), enabling spectrum sharing by dynamically detecting and switching channels.

E

Encrypt Key

The key generated to encrypt sensitive data in the AmpCon-Campus database. Then, plain text like password and sensitive TACACS+ keys is not shown in the AmpCon-Campus UI.

Ethernet Virtual Private Network (EVPN)

The next-generation VPN solution that introduces a control plane to better control the MAC address learning process.

F

Fabric

The logistic representation of an actual physical network. You can deploy a physical network by designing a fabric.

FSOS Switch

The switch with FSOS installed.

G

Global User

The AmpCon-Campus user that is not limited to any switch group. A global user can manage all PicOS switches.

Group User

The AmpCon-Campus user that can manage PicOS switches in one or multiple switch groups.

I

Intermittent Connectivity

The issue that the wireless network is unstable, often caused by co-channel interference or improper AP configurations.

IP Clos Fabric

The architecture that provides a scalable and flexible solution for interconnecting multiple switches in a hierarchical manner, allowing efficient utilization of network resources and simplified routing.

AmpCon-Campus supports the 5-stage IP Clos fabric architecture. This architecture contains the access layer, distribution layer, and core layer.

M

Media Access Control (MAC) Address

The physical address that uniquely identifies a network device on a local area network (LAN).

Management Frame Protection (MFP)

The security technology used to add signing or encryption to 802.11 management frames.

MFP can help to prevent forgery, tampering, and replay attacks, thereby mitigating common wireless Denial of Service (DoS) and disconnection vulnerabilities.

MD5 File

The file used to verify the completeness of another file. For example, a PicOS image MD5 file is used to verify the completeness of the related PicOS image file.

Mgmt IP

The management IP address of the switch. Mgmt IP is used to connect to AmpCon-Campus.

Multi-Chassis Link Aggregation (MLAG)

The technology used to implement link aggregation among multiple devices.

AmpCon-Campus supports using MLAG on leaf switches. Two leaf switches set up an MLAG through peer links.

MLAG Fabric

The two-layer (collapsed core layer and access layer) MLAG fabric architecture, which is scalable to a certain extent and is applicable to small or mid-size campus networking.

Modulation and Coding Scheme (MCS)

The core technology used to dynamically adapt to channel conditions by defining the combination of parameters like modulation schemes, coding rates, and the number of spatial streams.

MCS is used to optimize the data transmission rate and reliability in a wireless network.

Multihoming

The technology used to implement multi-path access by connecting a device to multiple leaf switches without link aggregation.

Multiple Pre-Shared Keys (MPSK)

The technology used to assign different Pre-Shared Keys (PSKs) to different users or devices in a wireless network, enhancing wireless security and management flexibility.

N

Network Access Control (NAC)

The security solution that ensures only authorized devices and users can access a network. AmpCon-Campus supports the following NAC authentication methods:

- 802.1X authentication offers a high level of security, but it requires the installation of an 802.1X client on the end-user devices, making network deployment less flexible.
- The MAC authentication method in NAC does not require client installation, but it necessitates registering MAC addresses on the authentication server, which complicates management.

Noise

The unwanted electrical signals that interfere with the transmission and reception of wireless communication signals.

It is a key factor that affects the quality and reliability of wireless communication.

Notification Rule

The rule that AmpCon-Campus uses for sending alert email notifications.

In a notification rule, specify alert types, alert levels, and fabrics to be monitored. Then, you will receive email notifications when these specified conditions are met.

Notification History

The historical alert notifications sent in the last 30 days.

O

One-Click Network Optimization

The function used to rapidly optimize wireless network performance, simplifying optimization processes and reducing operational complexity.

Open Shortest Path First (OSPF)

The dynamic interior gateway protocol that uses link-state information to build and maintain a complete and consistent map of the network topology within an AS.

It employs the Dijkstra algorithm to calculate the shortest path tree from each router to all the other routers in the AS, based on which routing tables are built.

Optical Module

The network device used for optoelectronic conversion in high-speed communication.

- At the transmitting end, optical modules convert electrical signals into optical signals for transmission through optical fiber.
- At the receiving end, optical modules re-convert the optical signals back into electrical signals.

Overlay Network

A virtual network built on top of the underlay network. It allows for the creation of logical, software-based networks that can span the entire physical network. This abstraction layer simplifies the management of network resources and services and allows for greater flexibility and scalability.

The underlay network refers to the physical infrastructure and protocols that make data transmission possible. In contrast, the overlay network is a virtual, software-defined layer that sits on top of the underlay network, allowing for advanced network functionalities and easier management.

Overlay Data Plane

Manages creation, maintenance, and tear-down of overlay networks, which are virtual networks built on top of an underlying physical network (underlay network).

The control plane ensures efficient communication between endpoints, handles network virtualization, and supports advanced features like multi-tenancy, workload mobility, and scalability.

Overlay Network Control Plane

Responsible for actual forwarding of traffic within an overlay network, including packet encapsulation, packet decapsulation, traffic forwarding, secure transmission of data, prioritizing certain types of traffic by using QoS policies, and distributing traffic across multiple paths in the underlay network by using mechanisms like Equal-Cost Multi-Path (ECMP).

P

Parking Lot

The panel containing all the PicOS switches in Parking status.

If you provision a PicOS switch without adding a switch configuration beforehand, the switch will be in Parking status and listed in the parking lot.

PicOS License

The authorization license for using functions of PicOS.

PicOS Switch

The switch with PicOS installed.

Power over Ethernet (PoE) Device

The technology that provides both data connection and electric power to devices such as wireless access points and IP cameras.

PoE devices are the systems that can pass electric power along with data on twisted pair Ethernet cabling.

R

Received Signal Strength Indicator (RSSI)

The parameter to evaluate the strength of wireless signals. The RSSI value reflects the quality of wireless connections.

Remote Authentication Dial-In User Service (RADIUS)

The network protocol used to provide centralized Authentication, Authorization, and Accounting (AAA) services for users to access network resources.

Radio Band

The frequency range allocated within radio waves for wireless communication. Different radio bands differ in wavelength, penetration, and transmission distances and are used for different network scenarios. The following radio bands are supported by AmpCon-Campus:

- 2.4GHz Radio Band: Covers radio waves from 2.400 GHz to 2.4835 GHz (the exact range varies by region). The 2.4GHz radio band provides extensive coverage but is susceptible to interference from other electronic devices.
- 5GHz Radio Band: Covers radio waves from 5.170 GHz to 5.850 GHz (the exact range varies by region). The 5GHz radio band is fast in transmission speeds but weak in signal penetration.
- 6GHz Radio Band: Covers radio waves from 5.925 GHz to 7.125 GHz (the exact range varies by region). The 6GHz radio band combines the advantages of wide coverage and

large transmission capacity. It provides faster transmission speeds and lower latency and resolves connectivity and congestion issues, meeting the demands of high-performance gaming and high-definition multimedia.

Radio Frequency (RF)

The high frequency alternating electromagnetic waves with a frequency range of 30 kHz to 300 GHz.

RF is used to transmit digital signals by modulating the amplitude, frequency, or phase of carrier waveforms.

Return Merchandise Authorization (RMA)

The method to replace a switch with another switch of the same switch model.

When the hardware of a switch fails and is replaced with a new switch, you can RMA to take the configurations from the failed switch, install or upgrade PicOS, update the serial number of the new switch, and push the configurations to the new switch to seamlessly manage it with AmpCon-Campus.

Roaming

The technology that allows wireless devices to automatically switch the network connection from one AP to another, while maintaining an uninterrupted connection.

Route

The path that network traffic takes from the source to the destination. Routes can change dynamically.

S

Service Set Identifier (SSID)

The logical name of a wireless network. SSIDs serve as critical identifiers to distinguish different wireless networks.

Signal-to-Noise Ratio (SNR)

The ratio of the useful signal power to the background noise power. The SNR value reflects the quality of wireless communication.

A higher SNR value indicates that the useful signal is stronger than the noise, resulting in more reliable data transmission and a lower Bit Error Rate (BER).

Simple Network Management Protocol (SNMP)

The application-layer protocol used for managing and monitoring network devices.

SNMP in AmpCon-Campus is mainly used to monitor the status, metrics, and other statistics of FSOS switches for performance analysis and fault diagnosis. The following concepts are

used in SNMP:

- Network Management System (NMS): A combination of hardware (devices) and software (the SNMP manager). The SNMP manager monitors and administers a network by polling the devices on your network for information about network connectivity, activity, and events.
- SNMP manager: An application to collect and process information from SNMP agents. The SNMP manager sends requests (such as requests of retrieving device status) to SNMP agents and receives responses.
- Managed device: The device on a network managed by the NMS. Routers and switches are common examples of managed devices.
- SNMP agent: An SNMP process that resides on a managed device, responsible for collecting local device information and exposing it to the SNMP manager. The SNMP agent responds to requests from the SNMP manager and provides operational status, performance metrics, configuration data, and other device-specific information to the SNMP manager.
- Management Information Base (MIB): A hierarchical database that defines the data sets and object types exchanged between the SNMP manager and SNMP agents. Each managed device maintains its specific MIB, which contains detailed information about the device and its services. The SNMP manager uses MIB identifiers (OIDs) to retrieve and manage the information.
- SNMP item: The fundamental unit in NMS to define individual monitoring metrics. The SNMP manager uses OIDs to retrieve each item value on managed devices.

Site

The site to which PicOS switches and APs belong.

Switch Group

The group to which PicOS switches belong.

Simple Mail Transfer Protocol (SMTP)

The TCP/IP protocol used to send and receive emails. SMTP specifies how two systems work with each other to transmit and receive emails and defines the formats of messages that are exchanged.

SMTP Server

The specialized application responsible for sending, relaying, and routing email messages between senders and recipients over the Internet or a network.

SSH Session

The secure, encrypted connection established between a client and a server for remote login, command execution, or file transfer.

SSH keys

The key pair (include a public key and a private key) used for establishing SSH sessions.

When you log in to the AmpCon-Campus UI and access a device through SSH keys, the session between the AmpCon-Campus server and the device to be accessed is verified through the private key entered in the AmpCon-Campus UI and the public key stored on the device side.

Station (STA)

The device connected to a wireless network through a wireless network card or built-in Wi-Fi module. The STA might be a laptop, smartphone, tablet, smart-home device, or others.

In a wireless network, an STA acts as a client, establishing a connection with an AP for network access.

802.11 Standards

A set of wireless networking communication standards established by IEEE. It covers multiple versions, such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, 802.11k, 802.11r, and 802.11v.

802.11 standards provide the foundation for interoperability in wireless networks.

Subnet Mask

The binary pattern used by the IP protocol to determine the destination network segment of packets.

Syslog Server

The centralized system that collects, stores, and manages system log messages generated by network devices, servers, and applications through the Syslog protocol.

T

Terminal Access Controller Access-Control System Plus (TACACS+)

The enhanced security protocol that provides centralized Authentication, Authorization, and Accounting services.

In addition to using local AmpCon-Campus users (global users or group users), you can also enable the TACACS+ integration to manage user access.

Telemetry

The technology to automatically collect real-time or historical metric data from managed switches.

Terminal

The terminal device connected to a wired network or wireless network. Terminals might be a laptop, smartphone, tablet, smart-home device, or others.

Terminal Identification

The technology used to automatically identify terminal devices connected to each managed switch, enabling accurate detection and management of terminal devices in the network.

Topology

The network arrangement formed by switch connections on a local area network (LAN) or among multiple LANs.

You can visualize your switches in all locations and drill down into an individual switch, right to the port level, to check port stats and overall health of the switch.

U

Universal Access Method (UAM)

The web-browser-based access method. Users can connect to a wireless network after they access specific web pages to complete authentication.

Underlay Network

The physical infrastructure (routers, switches, cabling) that transports the actual network traffic.

It is the foundational layer of your network that includes all the hardware and protocols needed for data transmission.

User Interface (UI)

The interaction interface between users and a digital product.

A UI includes all the visual and interactive elements that users see and interact with, such as buttons, icons, menus, and layouts.

V

Virtual Extensible Local Area Network (VXLAN)

The overlay network virtualization technology that enables the creation of virtual Layer 2 networks across Layer 3 network boundaries by encapsulating Layer 2 frames within Layer 3 UDP packets.

VXLAN extends the traditional VLAN technology, addresses the limitations of VLANs, such as the 4096-network limit, and meets the needs of large-scale, virtualized campus networks with multi-tenant capabilities.

Virtual Routing and Forwarding (VRF)

The technology that allows multiple instances of a routing table to coexist within the same router at the same time.

It enables logical isolation between different networks on the same physical device. By using VRF, different instances can use the same IP address without conflicts.

VPN IP

The IP address of the VPN tunnel established between the switch and AmpCon-Campus. The following icons are used to indicate the tunnel status:

- ✓: The VPN tunnel between the switch and AmpCon-Campus is available.
- x: The VPN tunnel between the switch and AmpCon-Campus is unavailable.

W

WAN Device

The device that connects local networks (LANs) to wide area networks (WANs), enabling communication over large geographical distances.

Wireless Fidelity (Wi-Fi)

The wireless Local Area Network (LAN) technology based on the IEEE 802.11 standard.

Wi-Fi enables network access and data transmission between devices through radio waves.

WIFI Steering

The technology that guides STAs to connect to a more suitable radio band through intelligent algorithms, optimizing network load and performance.

Wireless NIC

The hardware component that enables an STA to connect to a wireless network.

It receives and transmits radio wave signals through antennas, enabling data transmission between the STA and wireless network.

Z

Zero Touch Provisioning (ZTP)

The technology for automated deployment and configuration of network devices. AmpCon-Campus supports using ZTP to deploy PicOS switches and access points (APs).