

AmpCon-Campus Management Platform

User Manual V2.3

Models: LIS-AMPCON-CAM-FPSW-Foundation

AmpCon-Campus Management Platform 2.3 User Guide	5
Release Notes	7
AmpCon-Campus 2.3.0 Release Notes	8
AmpCon-Campus 2.3.1 Release Notes	12
Overview	14
Quick Start	25
Platform Installation Workflow	26
FSOS Switch Importing Workflow	32
PicOS Switch Onboarding Workflow	36
PicOS Switch Configuration Workflow	43
Wireless Network Deployment Workflow	46
Wired Network Deployment Workflow	51
Ansible Automation Workflow	54
Planning	57
Supported Information	58
Supported PicOS Switches	60
Supported FSOS Switches	73
Supported APs	75
Installation Requirements	76
Deploying AmpCon-Campus	78
Installing the AmpCon-Campus Server	79
Installing on VirtualBox for Lab Only	81
Installing on VMware ESXi	87
Installing on QEMU or KVM	92
Installing on Physical Machines (Ubuntu Docker)	97
Multi-NIC Deployment for Switch Connectivity	100
Upgrading the AmpCon-Campus Server	102
Uninstalling the AmpCon-Campus Server	104
Working with the User Interface	105
UI Menus	110
UI Conventions	120
Managing Wireless Networks	125
Wireless Overview	126
Concepts	131
Deploying Wireless Networks	137
Adding APs	139
Adding SSID Configurations	142
Optional: Adding Wireless Profiles	164
Optional: Adding Radio Configurations	174
Optional: Adding Advanced Configurations	180
Maintaining Wireless Networks	194
Positioning APs	195
Rebooting APs	197
Editing Configurations of an AP	199
Pushing Configurations to APs	202

Upgrading AP Firmware	205
Capturing Remote Port Packets	207
Optimizing Wireless Networks	210
Restoring to Factory Settings	215
Exporting, Deleting, and Moving APs	217
Accessing APs	220
Advanced CLI Configurations	222
Monitoring Wireless Networks	224
Wireless View	225
Monitoring APs	227
Monitoring STAs	240
Monitoring Wireless Sites	243
Importing FSOS Switches	254
SNMP Overview	255
Importing through SNMP	258
Monitoring FSOS Switches	265
Viewing FSOS Switch Details	268
Filtering SNMP Data	278
Viewing SNMP Trend Graphs	287
Onboarding PicOS Switches	292
Importing PicOS Switches	293
Deploying PicOS Switches through ZTP	299
How ZTP Works	300
Quick Deployment Guide	302
Preparing Configurations	307
Configuring Global Configurations	308
Adding Switch Configurations	311
Optional: Managing Global and Switch Configurations	318
Configuring Switch Models	320
Adding System Configurations	322
Configuring a DHCP Server	334
Provisioning New Switches through ZTP	336
Designing Campus Fabrics	342
Key Concepts	343
Supported Switches for Campus Fabrics	347
Fabric Overview	350
Designing MLAG Fabrics	355
Designing IP Clos Fabrics	365
Provisioning Overlay Services	383
Managing Campus Fabrics	389
Managing Switches	391
Viewing Managed PicOS Switches	392
Managing the Parking Lot	400
Uploading and Upgrading PicOS Images	402
Uploading and Pushing Images	403

Upgrading PicOS on Switches	409
Returning Merchandise Authorization for Switches	416
Decommissioning Switches	420
Removing Switches	421
Configuring Switches	422
Switch Templates	423
Adding Switch Templates	424
Managing Switch Templates	442
Configuration Templates	445
Adding Configuration Templates	446
Pushing Configurations to Switches	449
Managing Configuration Templates	453
Managing General Configurations	457
Comparing Running Configurations with Initial Configurations	459
Comparing Running or Backup Configurations	462
Backing Up and Restoring Configurations	464
Running Ansible Playbooks for Automation	469
Examples for Ansible Playbooks	470
Running Playbooks	477
Adding Other Devices	484
Managing Ansible Jobs	486
Viewing Playbook Scheduling	489
Troubleshooting	492
Monitoring and Alerting	495
System Overview	496
Switch Overview	499
Terminals	505
Telemetry	513
Global Telemetry Data	515
Telemetry Data of a Switch	520
Topology	534
Managing Topologies	535
Planning Topologies	537
Viewing Real-Time Topologies	544
Viewing Historical Topologies	546
Viewing Switch Details, Ports, and Terminal Devices	549
Alerts	554
Alert Types and Levels	555
Checking the Alert List	560
Alert Notifications	564
Alerting Notification Guide	565
Configuring an SMTP Server	567
Configuring Notification Rules	570
Viewing Historical Alert Notification Logs	573
Managing Groups and Sites	575

Managing Groups	576
Managing Sites	580
Managing Licenses	584
Managing AmpCon-Campus Licenses	585
Importing Licenses for Deployed Switches	586
Importing Licenses for Imported Switches	592
Troubleshooting for License Importing	596
Converting a Trial License to Standard Licenses	599
Viewing AmpCon-Campus Licenses	603
Invalidating a License	606
Checking License Logs and Alerts	609
Managing PicOS Licenses	613
Managing User Access	618
User Permission Table	624
Configuring TACACS+ Authentication and Authorization	628
Administering AmpCon-Campus	632
Updating the Encryption Key for Sensitive Data Encryption	633
Forwarding Logs to External Syslog Servers	634
Backing Up and Restoring the AmpCon-Campus Database	636
Accessing Devices through SSH Sessions	639
Glossary	643

AmpCon-Campus Management Platform 2.3 User Guide

AmpCon-Campus Management Platform

A powerful platform for managing PicOS® campus switches, offering automated Zero Touch Provisioning (ZTP), real-time telemetry monitoring, topology auto-discovery, automated lifecycle management, and MLAG fabric and IP Clos fabric deployment. AmpCon-Campus also supports managing wireless networks and monitoring wired terminal devices and FSOS switches.



Key Topics



Quick Start

- [Overview](#)
- [Quick Start](#)
- [Planning](#)
- [Deploying AmpCon-Campus](#)
- [Working with the User Interface](#)



PicOS Switches

- [Onboarding PicOS Switches](#)
- [Configuring PicOS Switches](#)
- [Managing PicOS Switches](#)
- [Monitoring and Alerting for PicOS Switches](#)



Wireless Networks

- [Deploying Wireless Networks](#)
- [Maintaining Wireless Networks](#)
- [Monitoring Wireless Networks](#)



Wired Networks

- [Choosing Campus Fabric Types](#)
- [Designing MLAG Fabrics](#)
- [Designing IP Clos Fabrics](#)
- [Managing Campus Fabrics](#)
- [Provisioning Overlay Services](#)



Ansible Playbooks

- [Examples for Ansible Playbooks](#)
- [Running Playbooks](#)
- [Adding Other Devices](#)



FSOS Switches

- [Importing FSOS Switches through SNMP](#)
- [Monitoring FSOS Switches](#)



Wired Clients

- [Monitoring Terminals](#)



Other Features

- [Accessing Switches through SSH Sessions](#)
- [Managing Groups and Sites](#)
- [Managing Licenses](#)

- [Managing_ Ansible Jobs](#)
- [Viewing_ Playbook Scheduling](#)

- [Administering_ AmpCon- Campus](#)

Other References

Blogs

Case Study

Try Now

Release Notes

Before you install AmpCon-Campus 2.3.x or upgrade AmpCon-Campus to 2.3.x, click the following child topics to get a quick overview of what is added, improved, changed, or fixed in AmpCon-Campus 2.3.x:

- [AmpCon-Campus 2.3.0 Release Notes](#)
- [AmpCon-Campus 2.3.1 Release Notes](#)

AmpCon-Campus 2.3.0 Release Notes

Before installing or upgrading to AmpCon-Campus 2.3.0, read this topic to learn about new features and improvements in this release.

New Features

- [FSOS Switch Monitoring](#)

- [Overlay Configuration](#)

- [Switch Template](#)

- [Wireless Network Management](#)

Improvements

- [Alerting](#)

- [License Management](#)

- [PicOS Upgrading](#)

- [Site Management](#)

- [Switch Management](#)

- [Telemetry Data](#)

- [Terminal Monitoring](#)

New Changes

- [Deploying Switches](#)

- [Navigation Bar](#)

- [Supported PicOS Switch List and PicOS Versions](#)

New Features

The following features are added to AmpCon-Campus 2.3.0:

FSOS Switch Monitoring

In addition to managing PicOS switches, AmpCon-Campus supports importing FSOS switches through SNMP. You can monitor these imported FSOS switches with AmpCon-Campus. For more information, see [Importing FSOS Switches](#).

Overlay Configuration

AmpCon-Campus provides an “Overlay Service Activation” page for managing overlay configurations, including VRF, VNI, and DHCP relay configurations. For more information, see [Provisioning Overlay Services](#).

Switch Template

AmpCon-Campus adds the switch template feature, making it easy to apply the same settings to switches across your sites. You can configure switches by adding a switch configuration template and applying it to switches in one or multiple sites. For more information, see [Switch Templates](#).

Wireless Network Management

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, maintain, and monitor wireless networks more efficiently. For more information, see [Managing Wireless Networks](#).

Improvements

The following improvements are added to AmpCon-Campus 2.3.0:

Alerting

The following functions are added to the alerting feature:

- On the “Alert List” page, you can filter alerts by using the filter icon in the **Last Time**, **Switch SN**, or **Type** column.
- You can mark multiple or all unread alerts as read by using the **Mark Selected as Read** button.

For more information, see [Checking the Alert List](#).

License Management

The following functions are added to the AmpCon-Campus license management feature:

- You can automatically import AmpCon-Campus licenses for quick switch activation, eliminating the need for complex manual processes. For more information, see [Importing Licenses for Deployed Switches](#).
- You can convert a trial license to one or multiple standard licenses automatically. For more information, see [Converting a Trial License to Standard Licenses](#).
- Within 14 days before a standard AmpCon-Campus license expires, when you log in to the AmpCon-Campus UI, you will see the notification message “License ID: xx Some of the licenses are about to expire. If you wish to continue using this device, please renew the license. You can view the relevant information through the “License Alert” function.”

PicOS Upgrading

The following functions are added to the PicOS upgrading feature:

- Before you upgrade, you can check the release notes of the PicOS image to which you want to upgrade. For more information, see [Checking PicOS Release Notes](#).
- You can set the PicOS upgrade time for off-peak upgrade. For more information, see [Upgrade Procedure](#).
- You can check all upgrade tasks, cancel a running upgrade task, edit an upgrade task, check upgrade task logs, and delete upgrade tasks. For more information, see [Managing Upgrade Tasks](#).

Site Management

The following functions are added to the site management feature:

- After you remove switches from any other sites, these switches are added to the site named **default** automatically.
- After you upgrade AmpCon-Campus to 2.3.0, the switches that didn't belong to any sites previously are added to the site named **default** automatically.

For more information, see [Managing Sites](#).

Switch Management

The following functions are added to the switch management feature:

- On the “Switches” page, you can modify switch hostnames manually. For more information, see [Modifying Switch Hostnames Manually](#).
- The “Switches” page contains a new column, **VPN IP**, which means the IP address of the VPN tunnel established between the switch and AmpCon-Campus. For more information, see [Viewing the Switch List](#).

Telemetry Data

MLAG and PoE telemetry metrics are added to the detail page of each managed switch. For more information, see [Telemetry Data of a Switch](#).

Terminal Monitoring

The following functions are added to the terminal monitoring feature:

- For terminal devices connected to each managed switch, the following information can be automatically identified by AmpCon-Campus:
 - **IP Address:** The dynamic IP address of a terminal device.
 - **Port:** The switch port used to connect to a terminal device.
- You can manually enter the terminal type and static IP address when you add or edit a terminal device.

For more information, see [Terminals](#).

New Changes

The following changes are added to AmpCon-Campus 2.3.0:

Deploying Switches

The process of deploying switches is changed. After you provision new switches with ZTP and before you stage these new switches, you must import AmpCon-Campus licenses into AmpCon-Campus to ensure each switch is allowed to be managed. For more information, see [Provisioning New Switches through ZTP](#).

Navigation Bar

The layout and wording of the AmpCon-Campus navigation bar are changed.

Supported PicOS Switch List and PicOS Versions

The supported PicOS switch list and the recommended PicOS versions are updated. For more information, see [Supported PicOS Switches](#).

AmpCon-Campus 2.3.1 Release Notes

Before installing or upgrading to AmpCon-Campus 2.3.1, read this topic to learn about new features and improvements in this release.

New Features

[Supported PicOS Switches](#)

[Supported FSOS Switches](#)

Improvements

[Switch Monitoring](#)

[Wireless Configurations](#)

New Features

Supported PicOS Switches

AmpCon-Campus 2.3.1 supports the following PicOS switch models: S5570-48X, S5590-64C, S5440-24T, S8520-32D, and S8510-24CD.

PicOS 4.7.5E is recommended for S5570-48X and S5590-64C switches.

PicOS 4.7.3E is recommended for S5440-24T switches.

PicOS 4.5.4E is recommended for S8520-32D switches.

PicOS 4.5.5.1 is recommended for S8510-24CD switches

For more information, see [Supported PicOS Switches](#).

Supported FSOS Switches

AmpCon-Campus 2.3.1 supports TSN3220-10S-U switches.

For more information, see [Supported FSOS Switches](#).

Improvements

Switch Monitoring

The switch picture in the **Device Information** section of each switch page is updated.

Wireless Configurations

- When you configure SSID configurations:
 - The MPSK, Key Caching, and FT Roaming functions are not supported when APs operate in NAT (Router) mode. AmpCon-Campus 2.3.1 automatically disables MPSK, Key Caching, and FT Roaming when you enable AP Assign IP.
 - Captive Portal and MPSK are mutually exclusive. AmpCon-Campus 2.3.1 automatically disables the other when you enable one.
- When you configure advanced wireless configurations:
 - Each service can't use the HTTP port 0. AmpCon-Campus 2.3.1 adds the port restriction.

- Different services (SSH, HTTP, Log, and RTTY) can't use the same port number. AmpCon-Campus 2.3.1 adds the port restriction.
- When you configure MPSK profiles:
 - To make labels clearer, the **Name** column is updated to **Profile Name** and the **Create** button is updated to **Create Access Credential** in the **MPSK** tab of the “Wireless Profiles” page. Besides, the **Name** field is changed to **Profile Name** in the **Create MPSK Profile** and **Edit MPSK Profile** pop-up windows.
 - To facilitate user management in wireless Multi-Dwelling Unit (MDU) scenarios, a new **Name** field is added to the **Create Access Credential** and **Edit Access Credential** pop-up windows. Meanwhile, the valid **VLAN ID** range is adjusted to 2-4048.
- When you enter a MAC address, AmpCon-Campus will automatically insert a colon after every two characters, optimizing MAC address input convenience.

Overview

AmpCon-Campus is a multivendor automation solution that empowers you to deploy, manage, and monitor wired and wireless campus networks. AmpCon-Campus simplifies, automates, and transforms campus network 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](#)

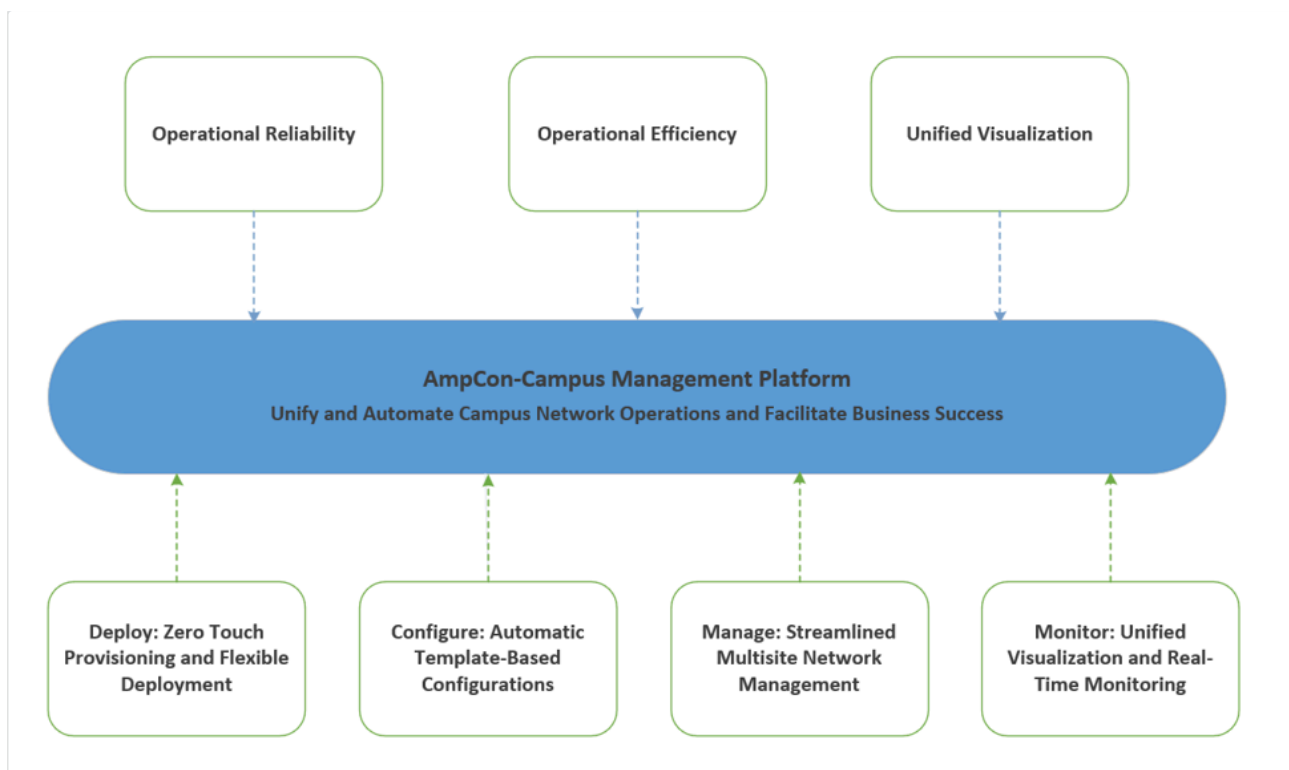
Product Overview

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

However, network operations and management is becoming more and more complicated, diverse, and distributed with multiple configuration sites, different monitoring tools, and large amounts of network devices and data. In addition, manual operations of networks often leads to human errors, security holes, outdated automation scripts, and undocumented configuration changes, increasing the downtime risk. Users demand a network management platform to resolve these challenges.

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

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



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

- **Deploy:** Simplify PicOS switch deployment through Zero-Touch Provisioning (ZTP), and automate deployment of wired physical networks (MLAG fabrics or IP Clos fabrics) and wireless networks, covering different requirements of small, medium-sized, and large-scale campus networks.

AmpCon-Campus covers different requirements of small, medium-sized, and large-scale campus networks, helps users deploy campus networks quickly, and reduces the time to service from weeks to just hours.

- **Configure:** Leverage a centralized user interface to push template-based configurations to PicOS switches and wireless access points (APs) across multiple sites, minimizing errors and simplifying configuration processes. Users can restore a PicOS switch to a stable backup configuration, decreasing the downtime and ensuring network reliability.
- **Manage:** Streamline lifecycle management of wired and wireless networks and devices (PicOS switches and APs), and integrate with the open-source automation tool Ansible to enhance network and device management automation, helping users increase network management efficiency and focus on more strategic tasks.
- **Monitor:** Provide a unified view and real-time monitoring data of wired and wireless networks, PicOS switches, FSOS switches, and APs, helping users eliminate the time of juggling multiple monitoring tools and gain comprehensive network insights.

Highlights

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

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

- **Powerful Wireless Network Deployment and Management**

AmpCon-Campus supports deploying and 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. Users can deploy, maintain, and monitor wireless networks more efficiently.

- **Flexible Wired Network Deployment and Management**

AmpCon-Campus offers flexible wired physical network deployment options to meet different networking requirements. Users can design and deploy MLAG campus fabrics for small or mid-size campus networks or IP Clos campus fabrics for large-scale campus networks, eliminating the complex campus networking configurations during the fabric design, deployment, and management processes.

- **Automated PicOS Switch Deployment and Management**

AmpCon-Campus makes it easy to deploy, configure, and manage a large number of PicOS switches. Users can manage the lifecycle of PicOS switches more efficiently, preventing 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 import FSOS switches to AmpCon-Campus and then monitor FSOS switches in the AmpCon-Campus UI.

- **Enhanced Terminal Device Monitoring**

AmpCon-Campus supports automatically identifying terminal devices connected to each managed PicOS switch and manually adding terminal devices. Users can accurately and securely identify terminal devices in your network and thus facilitate refined monitoring of terminal devices.

- **Powerful, Agentless Automation with Ansible Playbooks**

AmpCon-Campus integrates with the open-source automation tool Ansible. Users can automate virtually any task by writing and running Ansible playbooks in the AmpCon-Campus user interface, greatly enhancing network and device management automation.

- **Visual Management with Topology Auto-Discovery**

AmpCon-Campus supports automatic discovery of topologies to help users automatically identify and visualize the network structure. Users can check a topology and drill down into an individual PicOS switch, right to the port level, to check port stats, overall health of the switch, connected terminal devices, and more.

- **Telemetry Visualization to Optimize Network Performance**

AmpCon-Campus displays real-time and historical telemetry data such as performance monitoring metrics, giving users comprehensive visibility with a time-series view and helping users gain insights for quick decisions and network adjustments.

- **Fault Alerts via Visual Interface and Email Notifications**

AmpCon-Campus displays real-time and historical alerts by analyzing telemetry data and sends alert notifications through emails, helping users find problems quickly and prevent incident escalation.

- **Virtual Pre-Configuration with PicOS-V Integration**

AmpCon-Campus supports integration with PicOS-V. Users can push configurations to PicOS-V to verify the configurations first, and then push these verified configurations to PicOS switches, avoiding network issues due to wrong configurations.

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 wired and wireless network operations from Day 0 through Day 2+, delivers comprehensive network 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	• Platform Installation Workflow • Installing the AmpCon-Campus Server

	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.	
User Experience	AmpCon-Campus features a modern, intuitive, user-friendly user interface (UI) for managing campus networks and devices, providing you unified and consistent experience across the whole network operation process.	• Working with the User Interface
AmpCon-Campus License Import and Management	You can import a new or updated AmpCon-Campus license to manage PicOS switches, view all imported AmpCon-Campus licenses, convert a trial AmpCon-Campus license to a standard AmpCon-Campus license, invalidate the AmpCon-Campus license on a switch to release the license, or check license-related logs and alerts.	• Managing AmpCon-Campus Licenses
Role-Based Access Control	AmpCon-Campus supports Role-Based Access Control (RBAC), which is used to permit individual users to perform specific actions and get visibility to an access scope. Each user is assigned to a specific role with associated permissions. RBAC in AmpCon-Campus ensures secure, segmented, and efficient management of network operations and helps organizations enforce	• Managing User Access

	compliance, reduce risk, and streamline collaboration.	
System Overview	You can check the overall status of the AmpCon-Campus server, such as CPU, memory, and hard disk usage of the AmpCon-Campus00 server.	• System Overview
Backup and Restore	AmpCon-Campus provides the platform backup and restore feature as a critical safeguard for maintaining resilience and operational continuity of the management platform. In the event of a failure or disaster-recovery scenario, you can quickly restore the AmpCon-Campus database securely to a known good state with minimal downtime.	• Backing Up and Restoring the AmpCon-Campus Database
Encryption Key for Sensitive Data Encryption	AmpCon-Campus uses an encryption key to encrypt sensitive data in the AmpCon-Campus database, ensuring sensitive data security.	• Updating the Encryption Key for Sensitive Data Encryption

Deployment Features

The following features are used to deploy wired and wireless campus networks and PicOS switches:

Table 2. Deployment Features

Feature	Benefit	Reference Link
Deploying PicOS Switches	You can deploy PicOS switches through ZTP, simplifying the switch deployment and reducing manual operations. 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	• Deploying PicOS Switches through ZTP

	automatically runs the shell script to complete the ZTP deployment: • A white-box switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-Campus server, update switch configurations, and reboot the switch. • An integrated hardware and software switch runs the shell script to register with the AmpCon-Campus server, update switch configurations, and reboot the switch.	
Deploying Physical Networks	You can design and deploy MLAG campus fabrics for small or mid-size campus networks or IP Clos campus fabrics for large-scale campus networks, eliminating complex campus networking configurations.	• Designing Campus Fabrics
Deploying Wireless Networks	You can deploy wireless networks through ZTP, accelerating wireless network deployment. Add wireless access points (APs) to AmpCon-Campus first, and then configure the APs in the AmpCon-Campus UI. After you plug in and power on the added APs, the ZTP process will start. The APs will connect with AmpCon-Campus and retrieve configurations without manual intervention.	• Deploying Wireless Networks

Management Features

The following features are used to manage campus networks and devices:

Table 3. Configuration and Management Features

Feature	Benefit	Reference Link
Managing Wired and Wireless Networks	You can manage wired and wireless networks efficiently through robust management capabilities, providing streamlined and secure network management.	• Managing Campus Fabrics • Maintaining Wireless Networks
Importing PicOS Switches	If switches have PicOS installed, you can import them to AmpCon-Campus directly for management.	• Importing PicOS Switches
Managing PicOS Switches	You can manage the lifecycle of PicOS switches to reduce the complexity and workload of switch management while improving efficiency: • Apply standardized and consistent configurations to switches through switch templates. • Push customized configurations to switches through configuration templates. • Back up and restore switch configurations for disaster recovery. • Compare configurations on the same or different switches for troubleshooting or auditing. • Check the switch inventory and telemetry data of each switch. • Upgrade PicOS on a single switch or on multiple switches at scale. • Use Returning Merchandise Authorization (RMA) to replace a switch with another switch of the same switch model. • Decommission (DECOM) a deployed switch to clear the	• Configuring Switches • Managing Switches • Managing PicOS Licenses

	configurations pushed by AmpCon-Campus from the switch. • Remove a switch from the AmpCon-Campus database and the AmpCon-Campus UI. • Check or update PicOS licenses with the latest support entitlements.	
Accessing Devices through SSH Sessions	You can connect to a device (such as a switch or terminal device) from the AmpCon-Campus UI by creating an SSH session. AmpCon-Campus improves device access flexibility and security by supporting two types of authentication: password and SSH keys.	• Accessing Devices through SSH Sessions

Monitoring and Visibility Features

The following features are used to monitor and visualize campus networks and devices:

Table 4. Monitoring and Visibility Features

Feature	Benefit	Reference Link
FSOS Switches	You can import FSOS switches to AmpCon-Campus through Simple Network Management Protocol (SNMP) to monitor FSOS switches for performance analysis and fault diagnosis.	• Importing FSOS Switches
Switch Overview	You can check the overall status of managed PicOS switches.	• Switch Overview
Telemetry Data	You can check real-time or historical telemetry data to monitor operational state of PicOS switches, gaining detailed insights into network performance and device health.	• Telemetry

Terminal	AmpCon-Campus supports both automatically identifying terminal devices connected to each managed PicOS switch and manually adding terminal devices. You can accurately and securely monitor terminal devices in your network and thus facilitate refined management of terminal devices.	• Terminals
Topology	You can check the network structure in real-time or historical topologies and drill down into an individual PicOS switch, right to the port level, to check port stats, overall health of the switch, connected Linux servers, and more.	• Topology
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.	• Alerts

Integration Features

The following features are used to integrate with other tools:

Table 5. Integration Features

Feature	Benefit	Reference Link
Ansible Integration	AmpCon-Campus integrates with the open-source automation tool Ansible to automate virtually any task. See the following use cases:	• Running Ansible Playbooks for Automation

	• Eliminate repetition and simplify workflows. • Automate complex deployment. • Perform zero-downtime configurations. • Manage and maintain configurations.	
Syslog Server Integration	AmpCon-Campus supports forwarding system logs to external Syslog servers like Splunk. In this way, you can view and analyze AmpCon-Campus system logs more conveniently.	• Forwarding Logs to External Syslog Servers
TACACS+ Integration	AmpCon-Campus supports integrating with the Terminal Access Controller Access Control System (TACACS+) server to do authentication and authorization for the AmpCon-Campus login users.	• Configuring TACACS+ Authentication and Authorization

Quick Start

The following topics provide quick start guides for AmpCon-Campus, detailing the workflows of AmpCon-Campus server installation, FSOS switch importing, PicOS switch onboarding, template-based switch configuration, campus network deployment (wireless and wired), and Ansible Automation.

- [Platform Installation Workflow](#)
- [FSOS Switch Importing Workflow](#)
- [PicOS Switch Onboarding Workflow](#)
- [PicOS Switch Configuration Workflow](#)
- [Wireless Network Deployment Workflow](#)
- [Wired Network Deployment Workflow](#)
- [Ansible Automation Workflow](#)

Platform Installation Workflow

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

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

[Prerequisites](#)

[Installing on a Virtual Machine](#)

[Installing on a Physical Machine](#)

[What to Do Next](#)

Prerequisites

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

NOTE

To install the AmpCon-Campus server 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 server 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 the AmpCon-Campus server on a physical machine or 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
UDP	69	TFTP
UDP	80	OpenVPN

NOTES

- On AmpCon-Campus, each managed switch has two IP addresses: **Mgmt IP** and **VPN IP**.
 - **Mgmt IP** is the management IP address of a switch. **Mgmt IP** is used to connect to the AmpCon-Campus server during the switch onboarding process.
 - However, **Mgmt IP** might be changed. To ensure uninterrupted connection between the AmpCon-Campus server and a switch after **Mgmt 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 switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between the AmpCon-Campus server and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, the AmpCon-Campus server and the switch will communicate through the VPN tunnel.

- The AmpCon-Campus server 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.

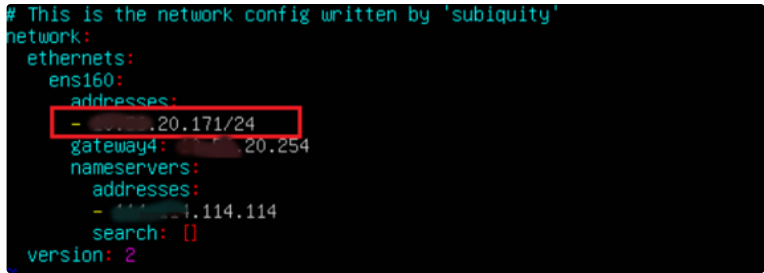
Installing on a Virtual Machine

To install the AmpCon-Campus server 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**

	The AmpCon-Campus server installed on Oracle VirtualBox can be used for lab purposes only.
Downloading the AmpCon-Campus Server Image	1. Download the compressed AmpCon-Campus server image by going to the FS AmpCon-Campus website and locating the image related to the hypervisor and the AmpCon-Campus version. 2. Put the compressed AmpCon-Campus server image to the machine where the hypervisor exists, and then unzip the image.
Importing the AmpCon-Campus Server Image	1. Import the unzipped AmpCon-Campus server image to the hypervisor. For different hypervisors, the steps of importing the AmpCon-Campus server 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 importing process to finish. Once completed, the virtual machine is successfully created, and the AmpCon-Campus server is installed. The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.
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 real IP address of the virtual machine as follows:  The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the real NIC name of the virtual machine. Therefore, you must check the real NIC name

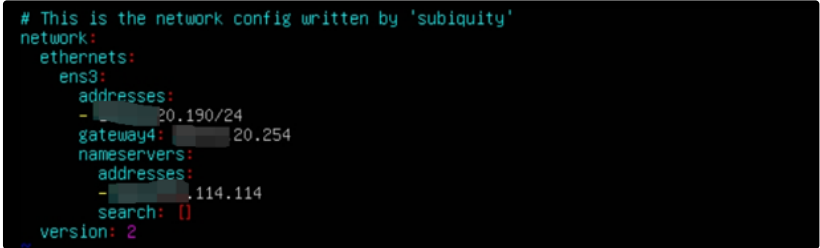
	of the virtual machine first by using the command ip addr show and then update the NIC name in the 00-installer-config.yaml file. 5. Apply the network interface configuration by running the sudo netplan apply command.
Starting the AmpCon-Campus Server	1. Go to the AmpCon-Campus installation directory by running the cd /usr/share/automation/server command. 2. Start the AmpCon-Campus server by running the sudo ./start.sh command.

Installing on a Physical Machine

To install the AmpCon-Campus server 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 AmpCon-Campus Server Installation Package	1. Download the compressed AmpCon-Campus server installation package by going to the FS AmpCon-Campus website and locating the package related to the AmpCon-Campus version. 2. Put the AmpCon-Campus server installation package to the prepared physical machine, and then extract the package by running the unzip <package_file_name>.zip command. A .tar.gz file is generated in the current directory. Extract the generated .tar.gz file by running the tar -zxvf <extracted_tar_file_name>.tar.gz command. A directory is generated with AmpCon-Campus server installation files. NOTES • Replace <package_file_name> in the command with the name of the AmpCon-Campus server installation package. • Replace <extracted_tar_file_name> in the command with the extracted .tar.gz 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 real IP address of the physical machine.  <pre># This is the network config written by 'subiquity' network: ethernets: ens3: addresses: - 10.190.24 gateway4: 20.254 nameservers: addresses: - 114.114 search: [] version: 2</pre> 3. Apply the network interface configuration by running the sudo netplan apply command.
Starting the AmpCon-Campus Server	1. Go to the directory where the unzipped AmpCon-Campus server installation files exist. 2. Install the AmpCon-Campus server by running the sudo ./install_or_upgrade.sh command. 3. Wait for the installation process to finish. Once completed, the AmpCon-Campus server is installed and started. The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.

What to Do Next

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

Table 5. Post-Installation Tasks

Task	Description
Configuring for Multi-NIC Deployment	If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-Campus server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-Campus server and managed switches might fail. For more

	information, see Multi-NIC Deployment for Switch Connectivity
Stopping the AmpCon-Campus Server	To stop the AmpCon-Campus server, follow the steps: 1. Go to the AmpCon-Campus installation directory by running the cd /usr/share/automation/server command. 2. Stop the AmpCon-Campus server by running the sudo ./stop.sh command.
Uninstalling the AmpCon-Campus Server	To uninstall the AmpCon-Campus server, follow the steps: 1. Go to the AmpCon-Campus installation directory by running the cd /usr/share/automation/server command. 2. Stop the AmpCon-Campus server by running the sudo ./stop.sh command. 3. Clear the files in the server directory by running the sudo rm -rf /usr/share/automation/server command.
Logging In to the AmpCon-Campus UI	The first time you log in 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 SuperAdmin role. It has all operation permissions on AmpCon-Campus. For security purposes, change the password upon the first login, update it periodically, and keep it secure. For how 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.

FSOS Switch Importing Workflow

AmpCon-Campus supports monitoring FSOS switches and doesn't support managing FSOS switches. To monitor FSOS switches with AmpCon-Campus, you need to import these switches to AmpCon-Campus through Simple Network Management Protocol (SNMP).

This guide provides a comprehensive overview of FSOS switch import procedures.

[Prerequisites](#)

[Procedure](#)

[What to Do Next](#)

Prerequisites

Before you import FSOS switches, ensure that the following prerequisite tasks have been completed:

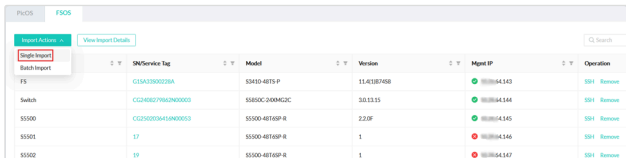
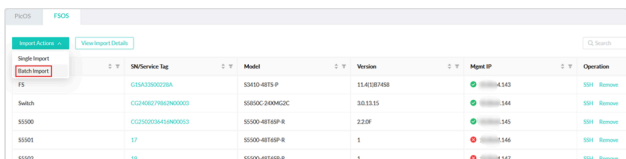
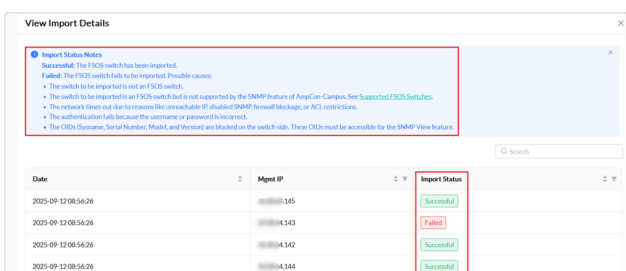
Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with the SuperAdmin , Admin , or Operator role.	• Working with the User Interface
Switch Requirement	Ensure that the FSOS switches are supported to be managed by AmpCon-Campus.	• Supported FSOS Switches
	Ensure that you have enabled SNMP and configured SNMP authentication on the FSOS switches.	• No Reference Link
	Ensure that the OIDs (Sysname, Serial Number, Model, and Version) are not blocked on the switch side. These OIDs must be accessible for the SNMP View feature.	• No Reference Link
Network Requirement	Ensure that the AmpCon-Campus server can connect with the FSOS switches and no network timeout issues exist due to reasons like unreachable IP, disabled SNMP, firewall blockage, or Access Control List (ACL) restrictions.	• No Reference Link

Procedure

Click **Wired > Switches** from the navigation bar, and then click the **FSOS** tab. In this tab, you can import a single FSOS switch or import multiple FSOS switches in batches.

Table 2. FSOS Switch Import Tasks and Links

Category	Task	Reference Link
Importing a Single FSOS Switch	To import a single FSOS switch, hover your mouse over Import Actions, and then click Single Import. 	Importing a Switch
Importing Multiple FSOS Switches in Batches	To import multiple FSOS switches in batches, hover your mouse over Import Actions, and then click Batch Import. 	Importing Switches in Batches
Checking Import Status	In the FSOS tab, click View Import Details. In the pop-up window, check the Import Status column. 	Checking Importing Results

What to Do Next

After you import FSOS switches, you can monitor these switches in the AmpCon-Campus UI.

Table 3. Monitoring Tasks and Links

Category	Task	Reference Link
Monitoring FSOS	Click Wired > Switches from the navigation bar. Click the FSOS tab, and then you can see	Viewing the Switch List

Switches

the list of imported FSOS switches.

FSOS

Imported Switches

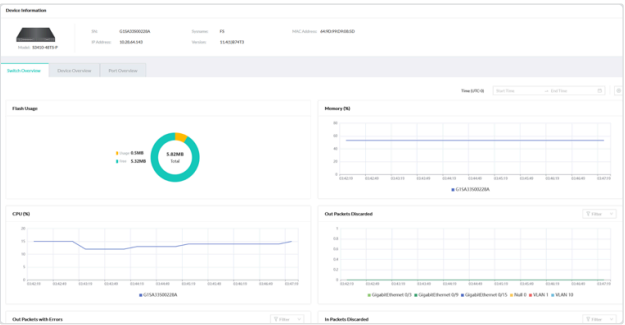
View Import Details

Search

System	SN/Service Tag	Model	Version	Model ID	Operation
swt1	1111	ar8011	1	 000004341	Deleting Remove
swt2	2222	ar8012	1	 000004342	Deleting Remove
swt3	3333	ar8013	1	 000004343	Deleting Remove
swt4	4444	ar8014	1	 000004344	Deleting Remove
swt5	5555	ar8015	1	 000004345	Deleting Remove

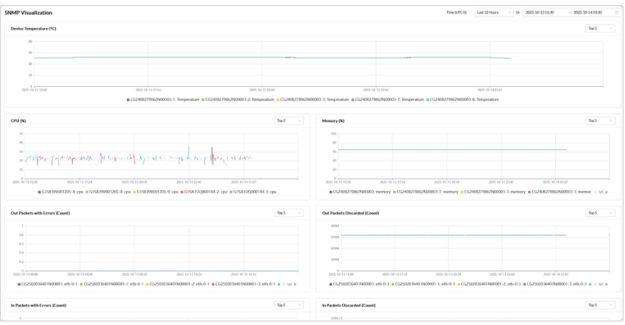
In the **FSOS** tab, locate an FSOS switch, and click the SN or service tag of the switch. Then, you can see detailed metrics of the switch.

- [Viewing FSOS Switch Details](#)



Click **Monitor > SNMP Management > SNMP Visualization** from the navigation bar. On the “SNMP Visualization” page, you can add and view item-based trend graphs for imported FSOS switches.

- [Viewing SNMP Trend Graphs](#)



Click **Monitor > SNMP Management > SNMP Data Filtering** from the navigation bar. On the “SNMP Data Filtering” page, you can filter SNMP data of all the imported FSOS switches.

- [Filtering SNMP Data](#)

SNMP Data Filtering

Switches: FS Item Name: Selected Location: 1 > 20 <

System	ID	ID	Item Name	Refresh Countdown (s)	Current Value
FS	C15A22000200A		System	5s	FS
FS	C15A22000200A		System Uptime	5s	13h 13m 45m 15s
FS	C15A22000200A		Device MAC	5s	A4:95:91:03:00:00
FS	C15A22000200A		Device SNMP Version	5s	1.4.0
FS	C15A22000200A		Device SNMP Version	5s	1.30
FS	C15A22000200A		Serial Number	5s	C15A22000200A
FS	C15A22000200A		CPU Utilization (5m)	5s	14%
FS	C15A22000200A		Device Temperature	5s	27.0°C
FS	C15A22000200A		Memory Used	5s	13.0%
FS	C15A22000200A		Memory Free	5s	22.7MB
FS	C15A22000200A		Memory Size	5s	5.12MB
FS	C15A22000200A		Flash Used	5s	5.18MB
FS	C15A22000200A		Flash Free	5s	5.32MB
FS	C15A22000200A		Flash Size	5s	5.81MB
FS	C15A22000200A		Fan Status	5s	OK
FS	C15A22000200A		Supply Status	5s	OK

PicOS Switch Onboarding Workflow

Onboard PicOS switches to bring them under AmpCon-Campus management. Once successfully onboarded, the PicOS switches are classified as managed devices and can be used to deploy wired networks.

This guide provides a comprehensive overview of the procedures for onboarding PicOS switches to AmpCon-Campus.

[Guidelines](#)

[Prerequisites](#)

[Importing a PicOS Switch](#)

[Deploying a Switch through ZTP](#)

[Deploying a White-Box Switch](#)

[Deploying an Integrated Hardware and Software Switch](#)

[What to Do Next](#)

Guidelines

To onboard PicOS switches, two options are provided: importing switches to AmpCon-Campus and deploying switches through Zero Touch Provisioning (ZTP).

- If the switches to be managed have PicOS installed, you can onboard these switches by importing them to AmpCon-Campus directly.
- If the switches to be managed don't have PicOS installed, or though the switches have PicOS installed but you want to onboard these switches through ZTP, you can use AmpCon-Campus to deploy these switches through ZTP.

NOTES

- Importing switches is not a ZTP method, which means that you still need to connect to the switches and do some operations on the switch side, such as obtaining IP addresses from the switches. The importing switch process doesn't push switch configurations.
- Deploying switches through ZTP is a ZTP method used for automated deployment of switches. After you reboot the switches, AmpCon-Campus will deploy the switches automatically. During the ZTP process, AmpCon-Campus will push pre-configured configurations to the switches.
- Integrated hardware and software switches have PicOS installed. To onboard these switches, you can import these switches to AmpCon-Campus directly, or you can deploy these switches through ZTP.

Prerequisites

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

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with an account of the SuperAdmin role.	• Working with the User Interface
Switch Requirement	Ensure that the switches to be onboarded are supported by AmpCon-Campus.	• Supported PicOS Switches
	For switches that have PicOS installed, 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 able to connect to the AmpCon-Campus server.	• No Reference Link
	If a firewall is configured between the AmpCon-Campus server 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

Importing a PicOS Switch

To onboard a PicOS switch by importing it to AmpCon-Campus, complete the following tasks:

Table 2. Switch Importing Tasks and Links

Category	Task	Reference Link
Importing Licenses	Obtain an AmpCon-Campus license (containing hardware IDs of the switches to be onboarded) from the FS sale team. Import the AmpCon-Campus license (containing hardware IDs of the switches to	• Importing Licenses for Imported Switches

	be imported) to AmpCon-Campus.	
Adding System Configuration	Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
Importing PicOS Switches	If you have obtained the IP address of the switch, you can use the automatic import method.	• Automatically Importing a Switch
	If you haven't obtained the IP address of the switch, you can use the manual import method.	• Manually Importing a Switch
Verifying Switch Status	Click Wired > Switches from the navigation bar. In the PicOS tab, check whether the imported switch is displayed in Imported status.	• Checking Importing Results

Deploying a Switch through ZTP

Deploying a White-Box Switch

To onboard a white-box switch by deploying it through ZTP, complete the following tasks:

Table 3. White-Box Switch Deployment Tasks and Links

Category	Task	Reference Link
System Configuration	Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
Switch Model	Click the Switch Model tab. In this tab, configure the switch model related to the switch.	• Configuring Switch Models

Global Configuration	Click the Global Configuration tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
Configuration Template	Click Wired > Config Templates from the navigation bar. Click the Template List tab. In this tab, check whether an existing configuration template meets your need. If not, click the New Template tab, and then add a new configuration template.	• Managing Configuration Templates • Adding Configuration Templates
Switch Configuration	Click Wired > Wired Profiles from the navigation bar. Click the Switch Configuration tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations
DHCP Server	Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
Switch Provisioning through ZTP	Provision the switch through ZTP to complete the switch deployment.	• Provisioning a White-Box Switch

NOTE

Pay attention to the following points. Or else, the switch will fail to be deployed. These points are also applicable to integrated hardware and software switch deployment.

- Be careful when you configure system configurations:
 - Ensure that the entered **Device Default Login User** and **Device Default Password** are correct and can be used to log in to the switch.
 - If the switch don't use the **Device Default Login User** and **Device Default Password** in the global system configuration, create a non-global system configuration for the switch, and ensure the **Device Default Login User** and **Device Default Password** match with the switch.
 - Ensure that the AmpCon-Campus server can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see [Checking License Portal Connectivity](#).
 - Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations or underlay/overlay related configurations.

- If you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-Campus parking lot. For more information, see [Managing the Parking Lot](#). To continue deploying the switches in the parking lot, follow these steps:
 - a. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar.
 - b. On the “Switches” page, click **Parking Lot**.
 - c. Locate the switch to be deployed, and then click **Create Config** to add a switch configuration. After you add the switch configuration, the switch will be listed on the “Switches” page with the **Configured** status.
 - d. Continue to provision the switch through ZTP to complete the switch deployment.

Deploying an Integrated Hardware and Software Switch

To onboard an integrated hardware and software switch by deploying it through ZTP, complete the following tasks:

Table 4. Integrated Hardware and Software Switch Deployment Tasks and Links

Category	Task	Reference Link
System Configuration	Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
Global Configuration	Click the Global Configuration tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
Configuration Template	Click Wired > Config Templates from the navigation bar. Click the Template List tab. In this tab, check whether an existing configuration template meets your need. If not, click the New Template tab, and then add a new configuration template.	• Managing Configuration Templates • Adding Configuration Templates
Switch Configuration	Click Wired > Wired Profiles from the navigation bar. Click the Switch Configuration tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations

DHCP Server	Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
Switch Provisioning through ZTP	Provision the switch through ZTP to complete the switch deployment.	• Provisioning an Integrated Hardware and Software Switch

What to Do Next

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

Table 5. Post-Onboarding Tasks and Links

Category	Task	Reference Link
Deploying Wired Networks	Deploy wired campus networks (fabrics) with PicOS switches.	• Wired Network Deployment Workflow
Configuring PicOS Switches	Use switch templates to satisfy general switch configuration through a full graphical interface.	• Switch Templates
	Use configuration templates to push specific configurations that can't be pushed through switch templates.	• Configuration Templates
Managing PicOS Switches	Manage the lifecycle of PicOS switches to reduce the complexity and workload of switch management while improving efficiency: • Check the switch inventory and telemetry data of each switch. • Upgrade PicOS on a single switch or on multiple switches at scale. • Use Returning Merchandise Authorization (RMA) to replace a switch with another switch of the same switch model. • Decommission (DECOM) a deployed switch to clear the configurations pushed by AmpCon-Campus from the switch. • Remove a switch from the AmpCon-Campus database and the AmpCon-Campus UI.	• Managing Switches • Managing PicOS Licenses

	• Check or update PicOS licenses with the latest support entitlements.	
Monitoring PicOS Switches	Monitor PicOS switches as follows: • Monitor metrics and topologies of PicOS switches. • Monitor terminal devices connected to PicOS switches. • Check alerts in the AmpCon-Campus UI. • Receive real-time email notifications when alerts are triggered.	• Monitoring and Alerting
Accessing Devices through SSH Sessions	Connect to PicOS switches from the AmpCon-Campus UI by creating SSH sessions.	• Accessing Devices through SSH Sessions

PicOS Switch Configuration Workflow

AmpCon-Campus simplifies the whole switch configuration process through the template-based configuration model, and allows you to apply consistent and standardized configurations across switches in one or multiple sites, making the configuration process more efficient and streamlined.

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

[Guidelines](#)

[Prerequisites](#)

[Procedure](#)

Guidelines

AmpCon-Campus supports two types of templates: switch templates and configuration templates. These two template types have different purposes:

Table 1. Template Types

Type	Description
Switch Template	Used to satisfy general switch configurations through a full graphical interface. You can provide parameter values for each input field in a switch template and select the switches to be configured. The configurations mapping these parameters will be pushed to the selected PicOS switches automatically by AmpCon-Campus.
Configuration Template	Used to push specific configurations that can't be pushed through switch templates. AmpCon-Campus provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands. When pushing configurations to PicOS switches, select the configuration templates containing the required CLI commands, and select the switches to be configured. Then, these CLI commands will be run on the selected PicOS switches automatically.

Prerequisites

Before you configure PicOS switches, ensure that the following prerequisite tasks have been completed:

Table 2. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with an account of the SuperAdmin , Admin , or Operator role.	• Working with the User Interface
Switch Requirement	Onboard PicOS switches to bring them under AmpCon-Campus management.	• PicOS Switch Onboarding Workflow
	Ensure that the PicOS switches are up and connected to the AmpCon-Campus server. You can check the connectivity by clicking Wired > Switches from the navigation bar and viewing the VPN IP column of the PicOS tab: • ✓: The switch is up and connected to the AmpCon-Campus server. • ✗: The switch is down or not connected to the AmpCon-Campus server.	• No Reference Link

Procedure

To configure PicOS switches, check whether the required configurations can be pushed through switch templates first. If not, use configuration templates to achieve your goal.

Table 3. Configuration Tasks and Links

Category	Task	Reference Link
Configuring through Switch Templates	Click Network Design > Switch Templates from the navigation bar. On the “Switch Templates” page, configure switches through a full graphical interface. The workflow is as follows: 1. Add a switch template. 2. Specify the switches to be configured. 3. Input configuration parameter values in the switch template as needed.	• Adding Switch Templates

	4. Apply the switch template. 5. Verify the template application result.	
Configuring through Configuration Templates	1. Click Wired > Config Templates from the navigation bar. In the New Template tab, create configuration templates with one or multiple required CLI commands. 2. Click the Push Config tab. In this tab, create a configuration node, select the configuration templates containing the required CLI commands, enter variable values for the CLI commands, and select the switches to be configured. 3. Verify the configuration pushing status and logs.	• Adding Configuration Templates • Pushing Configurations to Switches

Wireless Network Deployment Workflow

AmpCon-Campus supports deploying and managing wireless networks and access points (APs), providing flexible and secure network deployment and management through enhanced wireless configuration, advanced radio frequency optimization, and robust management capabilities.

This guide provides a comprehensive overview of wireless network deployment procedures.

NOTES

- The guide lists only the workflow of wireless network deployment. You need to check the reference links for detailed steps.
- Pay attention to the notes in each reference link. Or else, the deployment might fail.

[Prerequisites](#)

[Procedure](#)

[What to Do Next](#)

Prerequisites

Before you configure a wireless network, ensure that the following prerequisite tasks have been completed:

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with an account of the SuperAdmin role.	• Working with the User Interface
Site Requirement	Ensure that you have added the site where you will deploy the wireless network.	• Managing Sites
AP Requirement	Ensure that the APs to be added are supported by AmpCon-Campus.	• Supported APs
IP Address Requirement	Install a DHCP server, and configure the DHCP server to reserve an IP range for the APs to be added.	• No Reference Link
	Pre-configure the IP address of the AmpCon-Campus server by using one of the	• No Reference Link

following ways:

- Configure DHCP Option 138 as the IP address of the AmpCon-Campus server.
- Add the IP address of the AmpCon-Campus server in the **Redirector IP/URL** field of each AP webpage.

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 64.34
```

See the following AP webpage configuration example:



Network Requirement	Ensure that the APs to be added are able to access the IP address of the AmpCon-Campus server.	• No Reference Link
----------------------------	--	---

Procedure

To deploy a wireless network, complete the following tasks:

Table 2. Deployment Tasks and Links

Category	Task	Reference Link
Understanding Wireless Concepts and Highlights and AP ZTP Workflow	Learn about wireless network related concepts, highlights of wireless network management, and the Zero-Touch Provisioning (ZTP) workflow of APs.	• Wireless Overview • Concepts
Adding APs to AmpCon-Campus	Add APs to AmpCon-Campus one by one or import multiple APs in batches.	• Adding APs

Adding SSID Configurations	After adding APs to AmpCon-Campus, you must add SSID configurations for these APs.	• Adding SSID Configurations
Optional Configurations	On the “Wireless Profiles” page, configure some profiles, such as RADIUS servers, Multiple Pre-Shared Key (MPSK), Captive Portal, and the enabling time ranges for SSIDs or radio. Then, when you add SSID or radio configurations, you can use these pre-defined profiles.	• Adding Wireless Profiles
	AmpCon-Campus provides some default values for radio configurations. Check these default configuration values to see whether they meet your needs. If not, you must change the radio configurations as needed. NOTE Wireless regulatory requirements vary by country. Ensure that the country code in the radio configurations is consistent with the location of the AP.	• Adding Radio Configurations
	AmpCon-Campus provides some default values for advanced configurations. Check these default configuration values to see whether they meet your needs. If not, you must change the advanced configurations as needed.	• Adding Advanced Configurations
Plugging In and Powering On APs	Plug in and power on the added APs. Then, the ZTP process will start. Once completed, the wireless network is deployed, and the AP configurations will be pushed to the APs automatically.	• No Reference Link

What to Do Next

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

Table 3. Maintaining and Monitoring Tasks and Links

Category	Task	Reference Link
Maintaining Wireless Networks	When an AP goes offline, has signal anomalies, or requires maintenance or replacement, you can remotely trigger its LED to blink, enabling quick on-site localization.	• Positioning APs
	You can reboot one AP or all the APs in a site.	• Rebooting APs
	After a wireless network is deployed, you can edit configurations of each AP in the wireless network.	• Editing Configurations of an AP
	After a wireless network is deployed, you might need to edit configurations of an AP or update SSID, radio, or advanced configurations of a site. In these cases, you must manually push configurations to APs.	• Pushing Configurations to APs
	You can 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 AP Firmware
	You can capture remote packets from target ports of APs for rapid troubleshooting.	• Capturing Remote Port Packets
	You can optimize wireless networks immediately or at a fixed time. You can also customize network optimization configurations.	• Optimizing Wireless Networks
	You can restore managed APs to factory settings.	• Restoring to Factory Settings
	You can export APs to a .csv file, delete APs, or move APs from one site to another.	• Exporting, Deleting, and Moving APs
	You can connect to an AP from the AmpCon-Campus UI through remote TTY shell (RTTY).	• Accessing 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 FS support engineers to do AP debugging or configuration for you through this feature.	• Advanced CLI Configurations
Monitoring Wireless Networks	Click Dashboard > Wireless View from the navigation bar. On the “Wireless View” page, you can have a quick understanding of deployed wireless networks, such as managed APs, AP health status, and connected Stations (STAs).	• Wireless View
	Click Wireless > Access Points from the navigation bar. On the “Access Points” page, you can check detailed metrics of each managed AP.	• Monitoring APs
	Click Monitor > Wireless Clients from the navigation bar. On the “Wireless Clients” page, you can monitor STAs connected to each managed AP.	• Monitoring STAs
	Click Wireless > Manage from the navigation bar. In the Monitor tab, you can monitor the overall running status of each wireless site.	• Monitoring Wireless Sites

Wired Network Deployment Workflow

AmpCon-Campus offers flexible wired campus network (fabric) deployment to meet different networking requirements. You can design and deploy **MLAG fabrics** for small or mid-size campus networks or **IP Clos fabrics** for large-scale campus networks, eliminating complex networking configurations and enhancing deployment efficiency.

This guide provides a comprehensive overview of wired network deployment procedures.

NOTES

- The guide lists only the workflow of wired network deployment. You need to check the reference links for detailed steps.
- Pay attention to the notes in each reference link. Or else, the deployment might fail.

[Prerequisites](#)

[Procedure](#)

Prerequisites

Before you deploy a wired campus network, ensure that the following prerequisite tasks have been completed:

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with an account of the SuperAdmin role.	• Working with the User Interface
Network Requirement	Ensure that the PicOS switches are able to connect to the AmpCon-Campus server.	• No Reference Link
	If a firewall is configured between the AmpCon-Campus server 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

Switch Onboarding	Ensure that the PicOS switches used for wired network deployment are supported for campus fabrics.	• Supported Switches for Campus Fabrics
	Ensure that the PicOS switches retain only basic routing configurations, without any other service configurations.	• No Reference Link
	For switches that have PicOS installed, ensure that the Secure Shell (SSH) protocol is enabled on these switches. SSH is enabled on PicOS switches by default.	• No Reference Link
	Create a site in the AmpCon-Campus UI, and add the PicOS switches to the site.	• Managing Sites
	Onboard PicOS switches to bring them under AmpCon-Campus management. Once successfully onboarded, the PicOS switches are classified as managed devices and can be used to deploy wired networks.	• PicOS Switch Onboarding Workflow
	Ensure that the PicOS switches are up and connected to the AmpCon-Campus server. You can check the connectivity by clicking Wired > Switches from the navigation bar and viewing the VPN IP column of the PicOS tab: • : The switch is up and connected to the AmpCon-Campus server. • : The switch is down or not connected to the AmpCon-Campus server.	• No Reference Link

Procedure

To design and deploy a wired campus network, complete the following tasks:

Table 2. Fabric Deployment Tasks and Links

Category	Task	Reference Link
----------	------	----------------

Understanding MLAG Fabrics and IP Clos Fabrics	Understand the use cases, components, and architecture of MLAG fabrics and IP Clos fabrics.	• Fabric Overview
Understanding Key Concepts	Understand the concepts related to campus fabrics.	• Key Concepts
Deploying MLAG Fabrics	Design a two-layer MLAG fabric for small or mid-size campus networking.	• Designing MLAG Fabrics
Deploying IP Clos Fabrics	Design a 5-stage IP Clos fabric for large-scale campus networking.	• Designing IP Clos Fabrics
Provisioning Overlay Services	After you deploy an IP Clos fabric, if overlay configurations (VRF, VNI, and DHCP relay configurations) for the IP Clos fabric need to be changed, you can quickly modify these configurations on the “Overlay Service Activation” page.	• Provisioning Overlay Services

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 playbook, to automate your tasks.

By using AmpCon-Campus, you can write, run, and schedule Ansible playbooks on managed PicOS switches and added Linux servers, reducing manual work, eliminating configuration errors, and improving network management efficiency.

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

[Prerequisites](#)

[Procedure](#)

[What to Do Next](#)

Prerequisites

Before you run Ansible playbooks for automation, ensure that the following prerequisite tasks have been completed:

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-Campus UI with an account of the SuperAdmin , Admin , or Operator role.	• Working with the User Interface
Switch Requirement (Applicable only for running playbooks on PicOS switches)	Ensure that each PicOS switch to run Ansible playbooks has been onboarded to AmpCon-Campus.	• PicOS Switch Onboarding Workflow
	Ensure that the Device Default Login User and Device Default Password in the global system configuration can be used to log in to the PicOS switches. NOTE If the default username and password of a switch don't match the Device Default Login User and Device Default Password specified in the global	• Adding a Global System Configuration

	system configuration, the playbook will fail to be run on the switch.	
	Ensure that the PicOS switches are up and connected to the AmpCon-Campus server. You can check the connectivity by clicking Wired > Switches from the navigation bar and viewing the VPN IP column of the PicOS tab: • ✓: The switch is up and connected to the AmpCon-Campus server. • x: The switch is down or not connected to the AmpCon-Campus server.	• No Reference Link
Linux Server Requirement (Applicable only for running playbooks on Linux servers)	Ensure that the Linux servers have been added to AmpCon-Campus.	• Adding Other Devices

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. Click Maintain > Automation > Playbooks. On the “Playbooks” page, click the Show Pre-built Playbooks toggle. Check whether these pre-built Ansible playbooks meet your needs. If yes, click Save AS on the “Playbooks” page to create a copy playbook, and then run the playbook.	• No Reference Link
Writing or Importing	If the pre-built Ansible playbooks don’t meet your needs, write or import a	• Examples for Ansible Playbooks

Playbooks	playbook on the “Playbooks” page 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.	• Using Ansible playbooks • Writing a Playbook on AmpCon-Campus • Importing a Playbook
Checking Playbook Syntax	Before you run a playbook, check whether the playbook syntax is valid. On the “Playbooks” page, locate a playbook, and then click Check.	• No Reference Link
Running Playbooks	On the “Playbooks” page, locate the playbook, and then click Run to complete the automation operation.	• Running a Playbook
Checking Ansible Job Results and Output	An Ansible job is a single execution of an Ansible playbook. Click Maintain > Automation > Ansible Jobs from the navigation bar. On the “Ansible Jobs” page, check the playbook execution result and output.	• 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-Running Tasks and Links

Category	Task	Reference Link
Viewing Playbook Scheduling	View executed playbooks based on months, weeks, or days.	• Viewing Playbook Scheduling
Troubleshooting for Failed Ansible Jobs	If a playbook fails to be run on PicOS switches or Linux servers, check the possible reasons and solutions for troubleshooting.	• 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, DELL, Delta, and HPE switches. For detailed support lists, see [Supported PicOS Switches](#).

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](#).

NOTE

Though FSOS switches can be imported to AmpCon-Campus, they can't be managed by AmpCon-Campus. You can only monitor them as described in [Monitoring FSOS Switches](#).

Supported APs

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

Supported PicOS Switches

AmpCon-Campus 2.3.x supports managing the following PicOS switches:

[Guidelines](#)

[FS Hardware](#)

[Edgecore Hardware](#)

[DELL Hardware](#)

[Delta Hardware](#)

[HPE Hardware](#)

Guidelines

- For switches of FS models, you are recommended to install PicOS 4.7.1 M or later. O, some features of AmpCon-Campus might not work.

NOTES

- For N8550-64C and N5850-48X6C switches, you are recommended to install PicOS 4.6.0E.
- For S5570-48X and S5590-64C switches, you are recommended to install PicOS 4.7.5E.
- For S5440-12S and S5440-24T switches, you are recommended to install PicOS 4.7.3E.
- For S8520-32D switches, you are recommended to install PicOS 4.5.4E.
- For S8510-24CD switches, you are recommended to install PicOS 4.5.5.1.

- For switches of Edgecore, Dell, Delta, and HPE models, you are recommended to install PicOS 4.6.0E or later. Otherwise, some features of AmpCon-Campus might not work.
- The following switch models are supported only in AmpCon-Campus 2.3.1:
 - S5570-48X
 - S5590-64C
 - S5440-24T
 - S8520-32D
 - S8510-24CD

FS Hardware

Table 1. Supported FS Switches

Category	Model	Port Configuration	Switch A SIC	CPU
1G Switch Portfolio	S3270-10TM	10 x 1G/100M/10M copper, 2 x 2.5G/1G SFP	Wolfhound2	ARM Cortex A9
1G Switch Portfolio	S3270-10TM-P	10 x 1G/100M/10M copper PoE+, 2 x 2.5G/1G SFP	Wolfhound2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM	24 x 1G/100M/10M copper, 4 x 2.5G/1G SFP	Wolfhound2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM-P	24 x 1G/100M/10M copper PoE+, 4 x 2.5G/1G SFP	Wolfhound2	ARM Cortex A9
1G Switch Portfolio	S3270-48TM	48 x 1G/100M/10M copper, 4 x 2.5G/1G SFP	Wolfhound2	ARM Cortex A9
1G Switch Portfolio	S3410-24TS	24 x 1G/100M copper, 4 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410-24TS-P	24 x 1G/100M copper PoE+, 2 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410-48TS	48 x 1G/100M/10M copper, 4 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410-48TS-P	48 x 1G/100M/10M copper PoE+,	Hurricane2	ARM Cortex A9

		2 x 10G/1G SFP+		
1G Switch Portfol io	S3410C- 8TMS-P	2 x 10G/1G SFP+, 2 x 5G/2.5G/1G copper PoE+, 8 x 1G/100M/10M copper (the first 6 x 1G/100M/10M copper ports support PoE+)	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410C- 16TF	16 x 1G/100M/10M copper, 2 x 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410C- 16TF-P	2 x 1G SFP, 16 x 1G/100M/10M copper PoE+	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410C- 16TMS-P	2 x 10G/1G SFP+, 2 x 5G/2.5G/1G copper PoE+, 16 x 1G/100M/10M copper (the first 6 x 1G/100M/10M copper ports support PoE+)	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410L- 24TF	24 x 1G/100M/10M copper, 4 x 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410L- 24TF-P	24 x 1G/100M/10M copper PoE+, 4 x 1G SFP	Hurricane 2	ARM Cortex A9
1G Switch Portfol io	S3410L- 48TF	48 x 1G/100M/10M copper,	Hurricane 2	ARM Cortex A9

		4 x 1G SFP		
1G Switch Portfol io	S5810-28FS	20 x 1G/100M SFP, 8 x 1G/100M RJ45/SFP Combo, 4 x 10G/1G SFP+	Helix4	ARM Cortex A9
1G Switch Portfol io	S5810-28TS	24 x 1G/100M/10M RJ45, 4 x 1G RJ45/SFP Combo, 4 x 10G/1G SFP+	Helix4	ARM Cortex A9
1G Switch Portfol io	S5810-48FS	48 x 1G/100M SFP, 4 x 10G/1G SFP+	Helix4	ARM Cortex A9
1G Switch Portfol io	S5810-48TS	48 x 1G/100M/10 M copper, 4 x 10G/1G SFP+	Helix4	ARM Cortex A9
1G Switch Portfol io	S5810- 48TS-P	48 x 1G/100M RJ45 PoE+, 4 x 10G/1G SFP+	Helix4	ARM Cortex A9
1G Switch Portfol io	S5870- 48T6BC	48 x 1G/100M RJ45, 4 x 25G/10G SFP28, 2 x 100G/40G QSFP28	Trident3- X3	Intel x86
1G Switch Portfol io	S5870- 48T6BC-U	48 x 1G/100M/10M RJ45 PoE++, 4 x 25G/10G SFP28,	Trident3- X3	Intel x86

		2 x 100G/40G QSFP28		
1G Switch Portfolio	S5870-48MX6BC-U	36 x 2.5G/1G PoE++, 12 x 10G/5G/2.5G/1G/100M PoE++, 4 x 25G/10G SFP28, 2 x 100G/40G QSFP28	Trident3-X3	Intel x86
1G Switch Portfolio	S5870-48T6S	48 x 1G/100M/10M RJ45, 6 x 10G/1G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	S5870-48T6S-U	48 x 1G/100M PoE++, 6 x 10G/1G	Trident3-X2	Intel x86
5G Switch Portfolio	S5860-24MG-U	24 x 5G/2.5G/1G/100M copper PoE++, 4 x 25G/10G SFP28	Hurricane 3-MG	ARM Cortex A9
5G Switch Portfolio	S5860-48MG-U	48 x 5G/2.5G/1G/100M PoE++, 4 x 25G/10G SFP28, 2 x 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5440-12S	4 x 1G/100M/10M RJ45, 12 x 10G/1G SFP+	FSC 0440	ARM A53 Dual-Core
10G Switch Portfolio	S5440-24T	24 x 1G/100M/10M RJ45,	FSC 0440	ARM A53

		8 x 10G/1G SFP+		Dual-Core
10G Switch Portfolio	S5570-48X	48 x 10G/1G RJ45, 6 x 100G/40G QSFP28	Trident3-X5	Intel x86
10G Switch Portfolio	N5850-48X6C	48 x 10G RJ45, 6 x 100G QSFP28	Trident3-X5	Intel x86
10G Switch Portfolio	S5860-20SQ	20 x 10G/1G SFP+, 4 x 25G/10G SFP28, 2 x 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XB-U	24 x 10G/5G/2.5G/1G/100M PoE++, 4 x 10G/1G SFP+, 4 x 25G/10G SFP28	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XMG	24 x 10G/5G/2.5G/1G/100M, 4 x 10G/1G SFP+, 4 x 25G/10G SFP28	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG	48 x 10G/5G/2.5G/1G/100M, 4x 25G/10G SFP28, 2 x 40G QSFP+	Hurricane 3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG-U	48x 10G/5G/2.5G/1G/1	Hurricane 3-MG	ARM Cortex

		00M PoE++, 4x 25G/10G SFP28, 2 x 40G QSFP+		A9
25G Switch Portfolio	S5580-48Y	48 x 25G/10G SFP28, 8 x 100G/40G QSFP28, 2 x 10G/1G SFP+	Trident3-X7	Intel x86
100G Switch Portfolio	S5590-64C	64 x 100G/40G QSFP28	Tomahawk 2	Intel x86
100G Switch Portfolio	S5890-32C	32 x 100G/40G QSFP28	Trident3-X7	Intel x86
100G Switch Portfolio	N8550-64C	64 x 100G/40G QSFP28	Tomahawk2	Intel x86
200G Switch Portfolio	S8510-24CD	24 x 200G QSFP56, 8 x 400G QSFP-DD	Trident4-X9	Intel x86
400G Switch Portfolio	S8520-32D	32 x 400G QSFP-DD	Trident4-X11	Intel x86

Edgecore Hardware

Table 2. Supported Edgecore Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	AS4610-30P	24 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-30T	24 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9

1G Switch Portfolio	AS4610-54P	48 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54T(B)	48 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4625-54P	48 x 10/100/1000 BASE-T, 6 x 10G/1G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4625-54T	48 x 10/100/1000 BASE-T, 6 x 10G/1G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4630-54PE (EPS202)	48 x 1G PoE, 4 x 25G, 2 x 100G	Trident3	Intel x86
1G Switch Portfolio	AS4630-54TE (EPS201)	48 x 1G, 4 x 25G	Trident3	Intel x86
10G Switch Portfolio	AS5712-54X	48 x 10G, 6 x 40G	Trident2	Intel x86
10G Switch Portfolio	AS5812-54T (DCS209)	48 x 10G-T, 6 x 40G	Trident3	Intel x86
10G Switch Portfolio	AS5812-54X (DCS208)	48 x 10G, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	AS5835-54T (DCS202)	48 x 10G-T, 6 x 100G	Trident3	Intel x86
10G Switch Portfolio	AS5835-54X (DCS201)	48 x 10G SFP+, 6 x 100G QSFP28	Trident3	Intel x86
25G Switch Portfolio	AS7312-54X(S)	48 x 25G,	Tomahawk+	Intel x86

		6 x 100G		
25G Switch Portfolio	AS7326-56X (DCS203)	48 x 25G, 8x 100G, 2 x 10G	Trident3-X7	Intel x86
40G Switch Portfolio	AS6812-32X	32 x 40G	Trident2+	Intel x86
100G Switch Portfolio	AS7712-32X (DCS501)	32 x 100G	Tomahawk	Intel x86
100G Switch Portfolio	AS7726-32X (DCS204)	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	AS7816-64X (DCS500)	64 x 100G	Tomahawk2	Intel x86
Multi-Gig Switch Portfolio	AS4630-54NPE (EPS203)	36 x 2.5G/1G PoE, 12 x 10G/5G/2.5G/ 1G PoE, 4 x 25G, 2 x 100G	Trident3	Intel x86

DELL Hardware

Table 3. Supported DELL Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	N3024EP-ON	24 x 1G PoE, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3024ET-ON	24 x 1G, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3048EP-ON	48 x 1G PoE, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3048ET-ON	48 x 1G, 4 x 10G	Helix4	ARM Cortex A9

1G Switch Portfolio	N3224F-ON	24 x 1G SFP, 4 x 10 G, 2 x 100G/40G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224P-ON	24 x 1G 30W PoE, 4 x 10G, 2 x 100G/40G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224T-ON	24 x 1G, 4 x 10G, 2 x 100G/40G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248P-ON	48 x 1G 30W PoE, 4 x 10G, 2 x 100G/40G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248TE-ON	48 x 1G, 4 x 10G, 2 x 100G/40G	Trident3-X3	Intel x86
10G Switch Portfolio	S4048-ON	48 x 10G, 6 x 40G, 2 x 100G/40G	Trident2	Intel x86
10G Switch Portfolio	S4128F-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4128T-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4148F-ON	48 x 10G SFP, 2 x 40G, 4 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4148T-ON	48 x 10G BASE-T, 2 x 40G, 4 x 100G	Maverick	Intel x86

25G Switch Portfolio	S5212F-ON	12 x 25G, 3 x 100G	Trident3-X5	Intel x86
25G Switch Portfolio	S5224F-ON	24 x 25G, 4 x 100G	Trident3-X5	Intel x86
25G Switch Portfolio	S5248F-ON	48 x 25G, 8 x 100G	Trident3-X7	Intel x86
25G Switch Portfolio	S5296F-ON	96 x 25G, 8 x 100G	Trident3-X7	Intel x86
100G Switch Portfolio	S5232F-ON	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	Z9100-ON	32 x 100G, 2 x 10G	Tomahawk	Intel x86
100G Switch Portfolio	Z9264F-ON	64 x 100G, 2 x 10G	Tomahawk2	Intel x86
Multi-Gig Switch Portfolio	N2224PX-ON	24 x 2.5G/1G 30W/60W PoE, 4 x 25G, 2 x 40G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2224X-ON	24 x 2.5G/1G, 4 x 25G, 2 x 40G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248PX-ON	48 x 2.5G/1G 30W/60W PoE, 4 x 25G, 2 x 40G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248X-ON	48 x 1G/2.5G, 4 x 25G, 2 x 40G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N3132PX-ON	24 x 1G PoE,	Firebolt 4 FS	ARM Cortex A9

folio		8 x 5G/2.5G/1G PoE, 4 x 10G		
Multi-Gig Switch Portfolio	N3208PX-ON	4 x 5G/2.5G/1G PoE, 4 x 1G PoE, 2 x 10G SFP+	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N3224PX-ON	24 x 10G/5G/2.5G/1G 90W PoE, 4 x 25G, 2 x 100/40G	Trident3-X3	Intel x86
Multi-Gig Switch Portfolio	N3248PXE-ON	48 x 10G/5G/2.5G/1G 90W PoE, 4 x 25G, 2 x 100/40G	Trident3-X5	Intel x86
Multi-Gig Switch Portfolio	N3248X-ON	48 x 10G/5G/2.5G/1G, 4 x 25G, 2 x 100G/40G	Trident3-X5	Intel x86

Delta Hardware

Table 4. Supported Delta Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	AG7648	48 x 10G, 6 x 40G	Trident2	Intel x86
25G Switch Portfolio	AG5648 v1-R	48 x 25G, 6 x 100G	Tomahawk+	Intel x86

100G Switch Portfolio	AG9032 v1	32 x 100G	Tomahawk	Intel x86
-----------------------	-----------	-----------	----------	-----------

HPE Hardware

Table 5. Supported HPE Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	HPE AL 6921-54T	48 x 10G-T, 6 x 40G	Trident2 +	Intel x86
10G Switch Portfolio	HPE AL 6921-54X	48 x 10G-T, 6 x 40G	Trident2 +	Intel x86

Supported FSOS Switches

Before you import FSOS switches to AmpCon-Campus through SNMP, 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
TSN3220	TSN3220-10S-U NOTE TSN3220-10S-U switches are supported only in AmpCon-Campus 2.3.1.
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

Before you add access points (APs) to AmpCon-Campus, 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 the AmpCon-Campus server, ensure that the following requirements are met.

[Server Requirements](#)

[Network Requirements](#)

[License Requirements](#)

Server Requirements

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

NOTE

To install the AmpCon-Campus server 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 server 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 Server Machine

TCP/UDP	Port	Protocol
TCP	80	HTTP
TCP	443	HTTPS

UDP	69	TFTP
UDP	80	OpenVPN

NOTES

- On AmpCon-Campus, each managed switch has two IP addresses: **Mgmt IP** and **VPN IP**.
 - **Mgmt IP** is the management IP address of a switch. **Mgmt IP** is used to connect to the AmpCon-Campus server during the switch onboarding process.
 - However, **Mgmt IP** might be changed. To ensure uninterrupted connection between the AmpCon-Campus server and a switch after **Mgmt 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 switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between the AmpCon-Campus server and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, the AmpCon-Campus server and the switch will communicate through the VPN tunnel.

- The AmpCon-Campus server 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.

License Requirements

Obtain an AmpCon-Campus license from the FS sale team. The following AmpCon-Campus license types are supported:

- **Trial license:** The trial period lasts for 90 days and an additional 14 days. After the trial license is expired, you must install a standard license to continue using AmpCon-Campus.
- **Standard license:** After a standard license is installed, you cannot install a trial license.

Deploying AmpCon-Campus

To use the powerful features of AmpCon-Campus, you need to install the AmpCon-Campus server first. You can upgrade the AmpCon-Campus server to a later version or uninstall it if it's not needed.

See the following child topics:

- [Installing the AmpCon-Campus Server](#)
- [Upgrading the AmpCon-Campus Server](#)
- [Uninstalling the AmpCon-Campus Server](#)

Installing the AmpCon-Campus Server

You can install the AmpCon-Campus server on a virtual machine or a physical machine by using one of the following methods:

- [Installing on VMware ESXi](#)
- [Installing on QEMU or KVM](#)
- [Installing on VirtualBox for Lab Only](#)
- [Installing on Physical Machines \(Ubuntu Docker\)](#)

If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-Campus server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-Campus server and managed switches might fail.

For more information, see [Multi-NIC Deployment for Switch Connectivity](#).

NOTES

- On AmpCon-Campus, each managed switch has two IP addresses: **Mgmt IP** and **VPN IP**.
 - **Mgmt IP** is the management IP address of a switch. **Mgmt IP** is used to connect to the AmpCon-Campus server during the switch onboarding process.
 - However, **Mgmt IP** might be changed. To ensure uninterrupted connection between the AmpCon-Campus server and a switch after **Mgmt 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 switch is onboarded to AmpCon-Campus successfully, a VPN tunnel between the AmpCon-Campus server and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, the AmpCon-Campus server and the switch will communicate through the VPN tunnel.

- The AmpCon-Campus server 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.

Installing on VirtualBox for Lab Only

You can install the AmpCon-Campus server on VirtualBox for lab purposes only. Production environments require a proper enterprise-scale virtualization solution as described in [Supported Deployments](#). For how to use VirtualBox in general, see the [Oracle VirtualBox documentation](#).

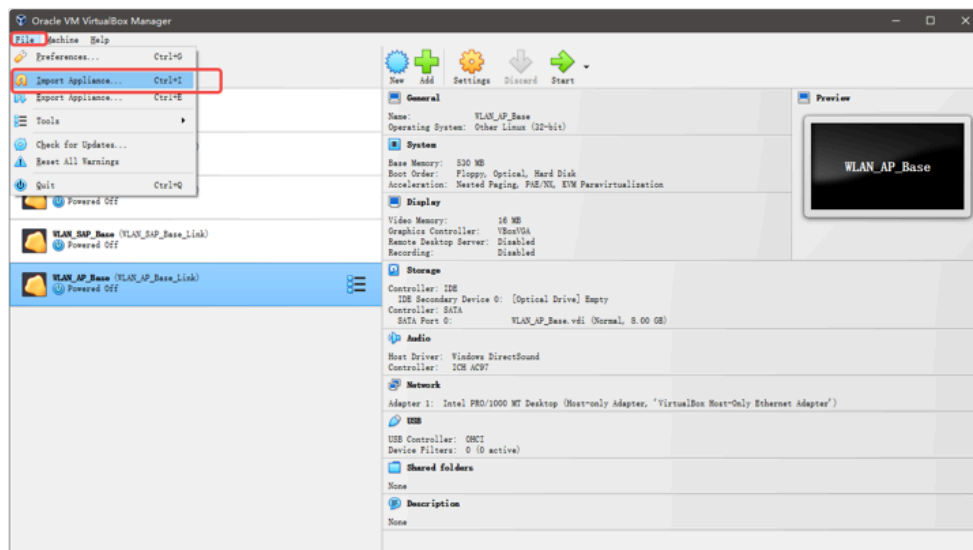
[Prerequisites](#)
[Installation Procedure](#)
[What to Do Next](#)

Prerequisites

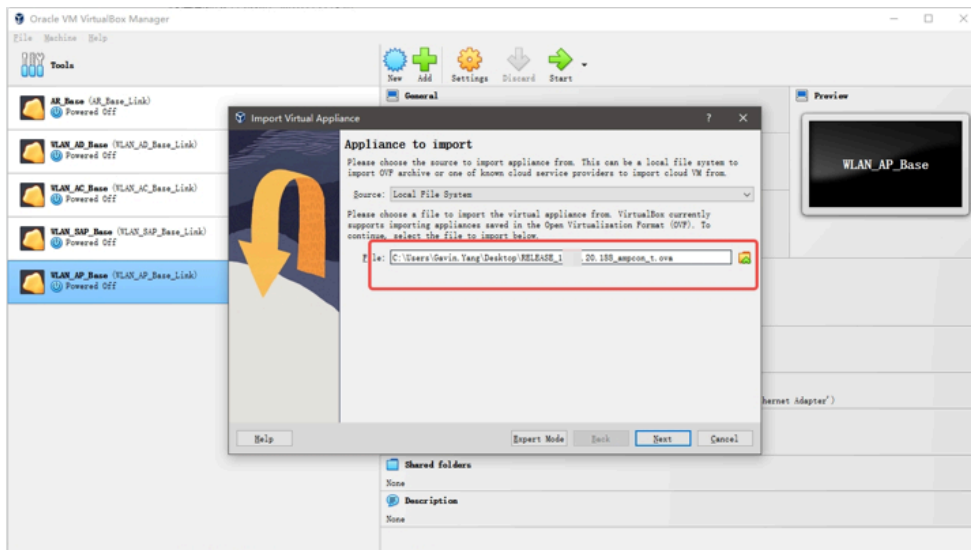
- Ensure that the [installation requirements](#) are met.
- Download the compressed AmpCon-Campus server image **AmpCon-Campus for VirtualBox V2.3.x Software** from the [FS AmpCon-Campus website](#).
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

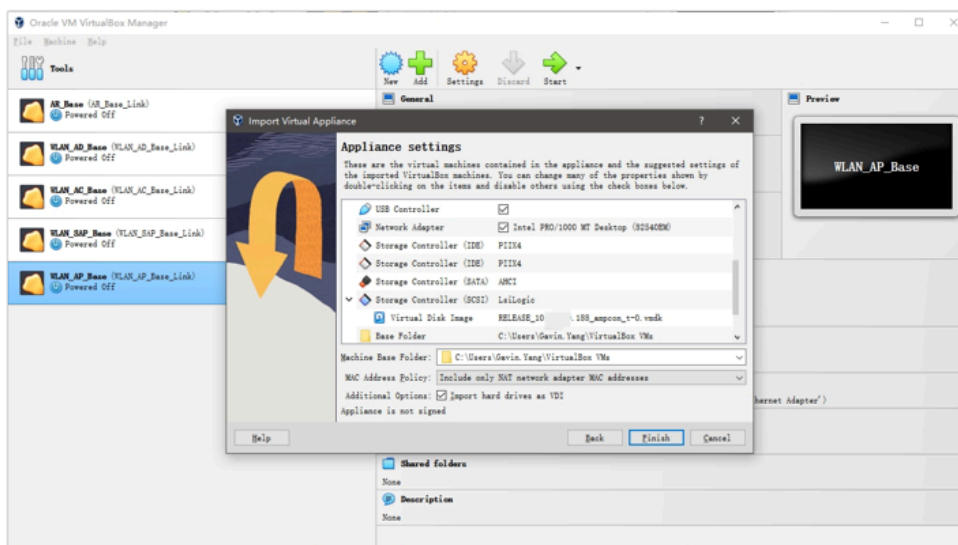
1. Open the VirtualBox console, and then click **File > Import Appliance**.



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



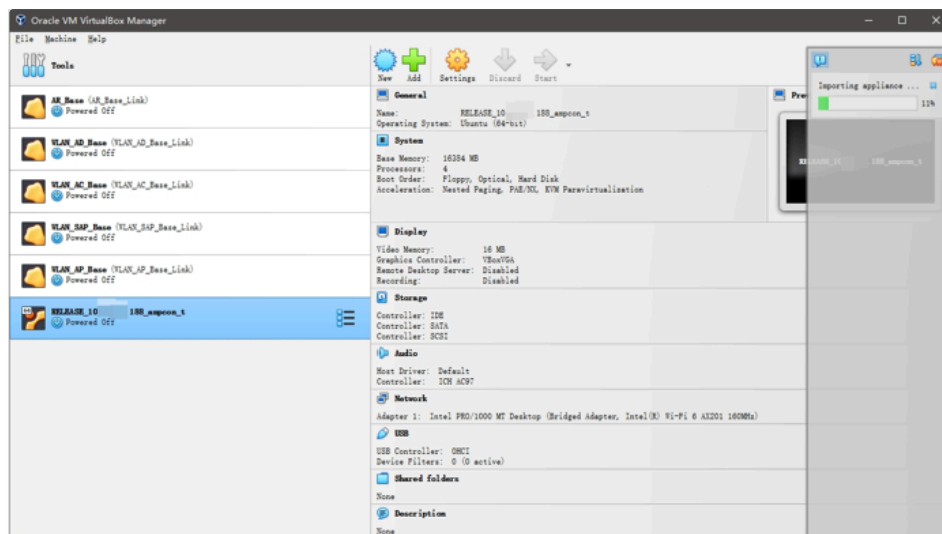
3. Confirm the settings for the .ova file, and then click **Finish**.



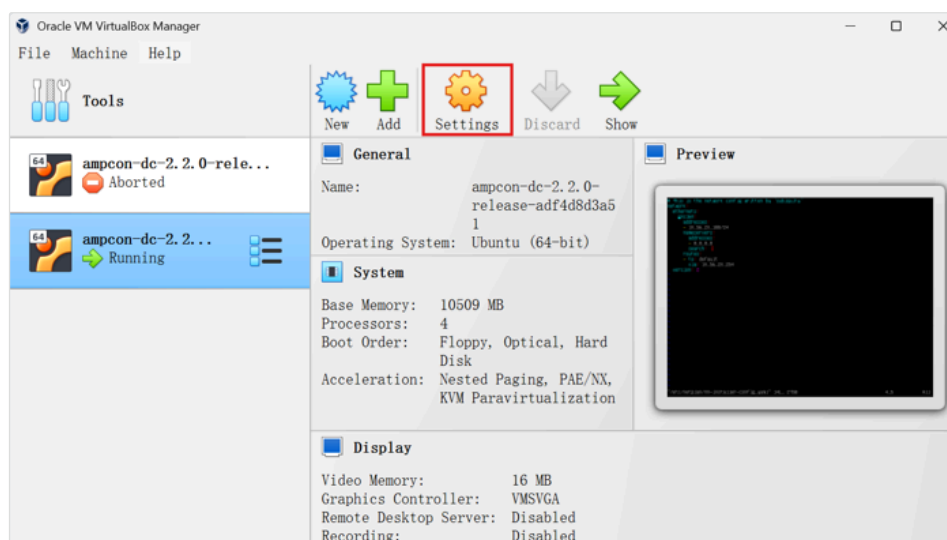
Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-Campus server is installed.

NOTE

The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.

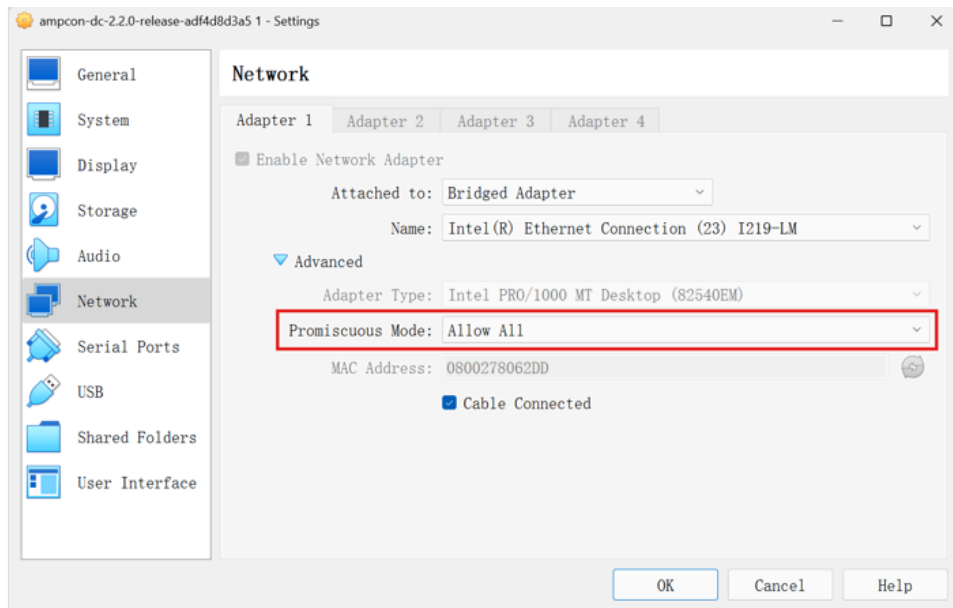


4. Click **Settings**, and then check the settings of the imported virtual machine.

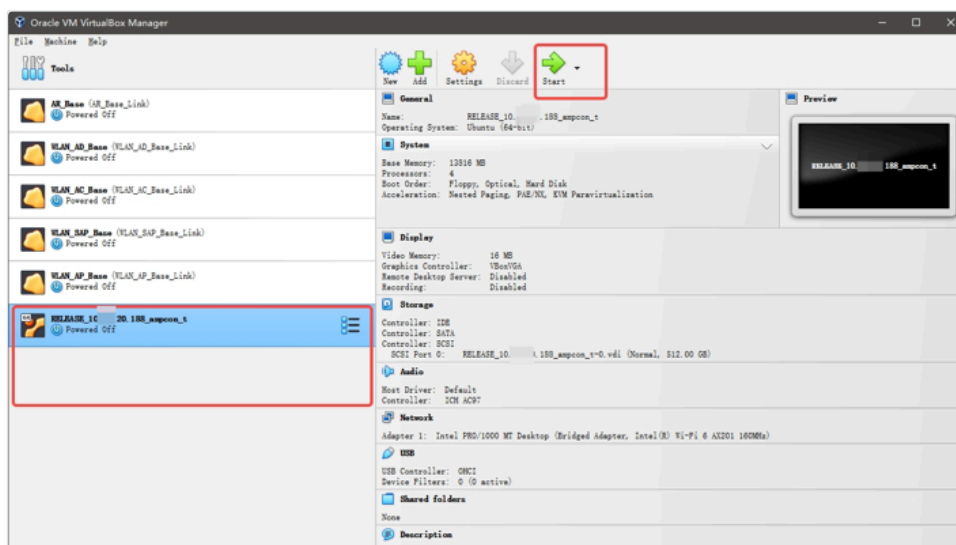


NOTE

In the **Network** column, the default value of the **Promiscuous Mode** is **Deny**. You must change it to **Allow All**.



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



6. Modify the network interface configuration.

- Log in to the virtual machine with the default username (pica8) and password (pica8).
- 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 real 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 real NIC name of the virtual machine.

Therefore, you must check the real 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.

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      addresses:
        - 10.0.2.15/24
      nameservers:
        addresses:
          - 10.0.2.8
        search: []
      routes:
        - to: default
          via: 10.0.2.254
      version: 2
```

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

```
sudo netplan apply
```

7. Start the AmpCon-Campus server:

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

```
cd /usr/share/automation/server
```

b. Start the AmpCon-Campus server by running the following command:

```
sudo ./start.sh
```

Now the AmpCon-Campus server is installed and started.

What to Do Next

- If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-Campus server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-Campus server and managed switches might fail.

For more information, see [Multi-NIC Deployment for Switch Connectivity](#).

- To stop the AmpCon-Campus server, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Stop the AmpCon-Campus server by running the **sudo ./stop.sh** command.
- To start the the AmpCon-Campus server after it is stopped, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.

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

Installing on VMware ESXi

You can install the AmpCon-Campus server on VMware ESXi 6.7, 7.0, 8.0. For how to use VMware ESXi in general, see the [VMware ESXi documentation](#).

[Prerequisites](#)

[Installation Procedure](#)

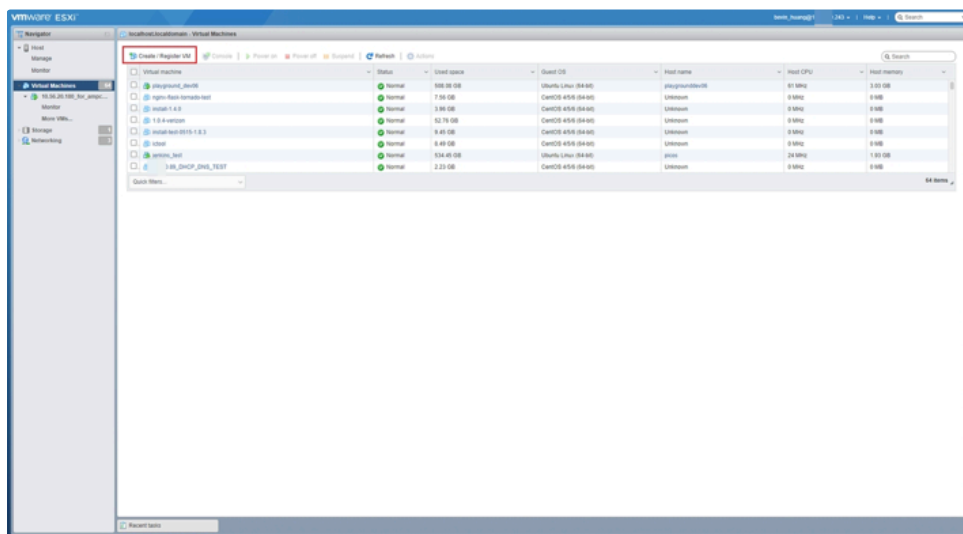
[What to Do Next](#)

Prerequisites

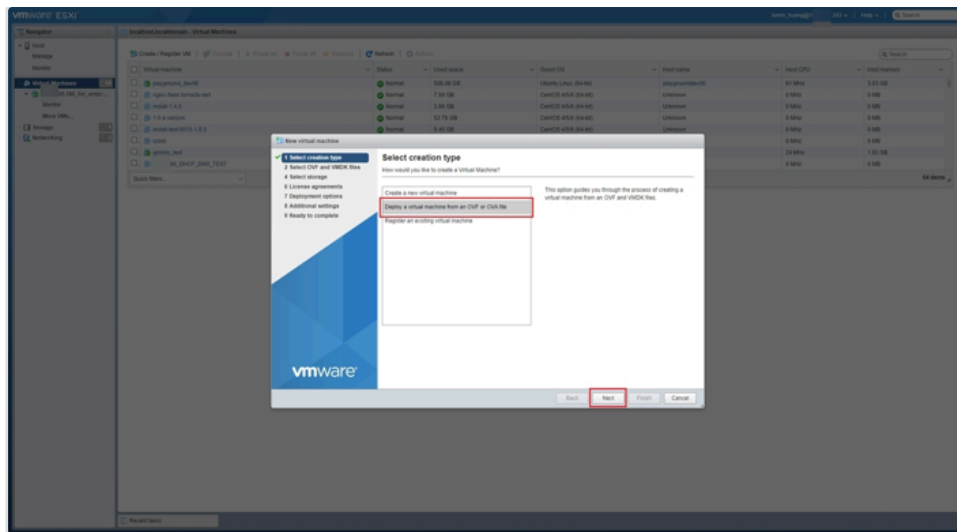
- Ensure that the [installation requirements](#) are met.
- Download the compressed AmpCon-Campus server image **AmpCon-Campus for VMWare ESXi V2.3.x Software** from the [FS AmpCon-Campus website](#).
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

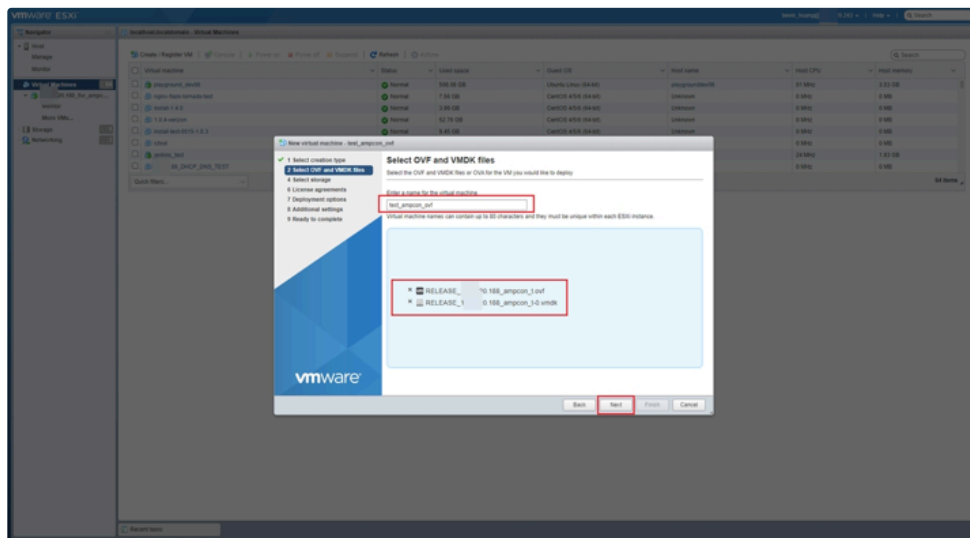
1. Open the VMware ESXi console, and then click **Create / Register VM**.



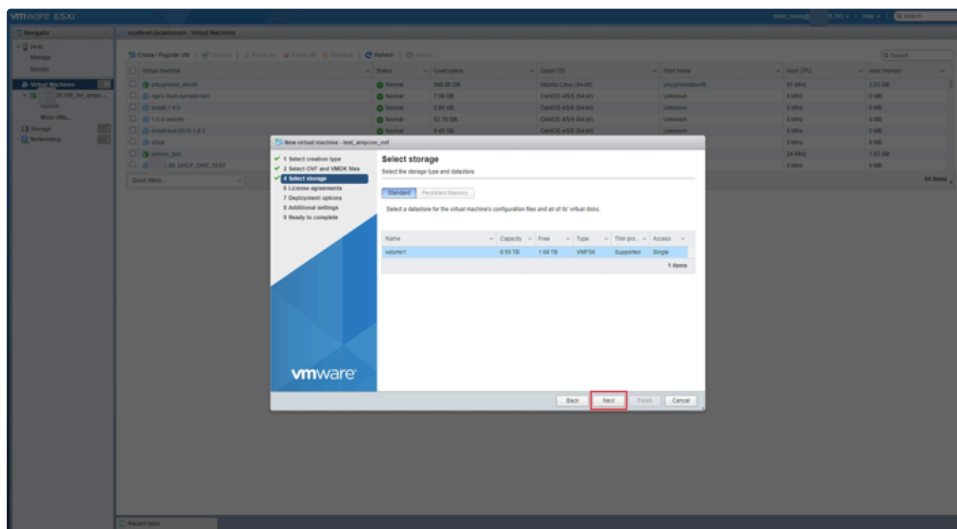
2. Select **Deploy a virtual machine from an OVF or OVA file**, and then click **Next**.



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

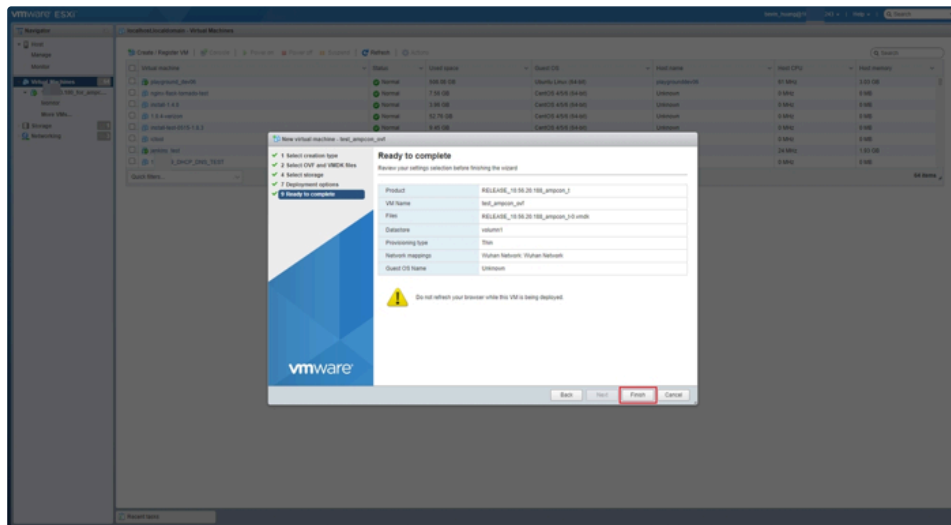


4. Confirm the storage type and datastore, and then click **Next**.



5. In the **Network mappings** drop-down list of the **Deployment Options** window, select the network adapter to which the virtual machine is connected, and then click **Next**.

6. Click **Finish**.

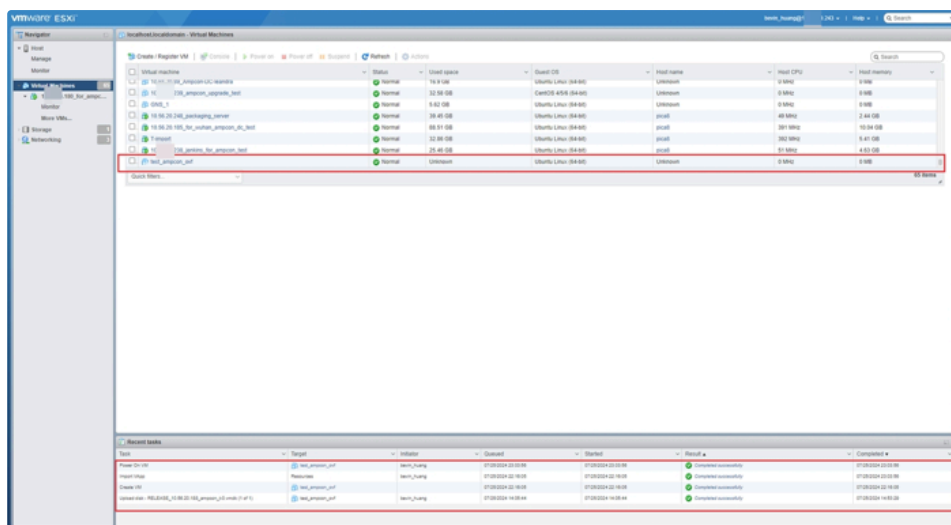


Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-Campus server is installed.

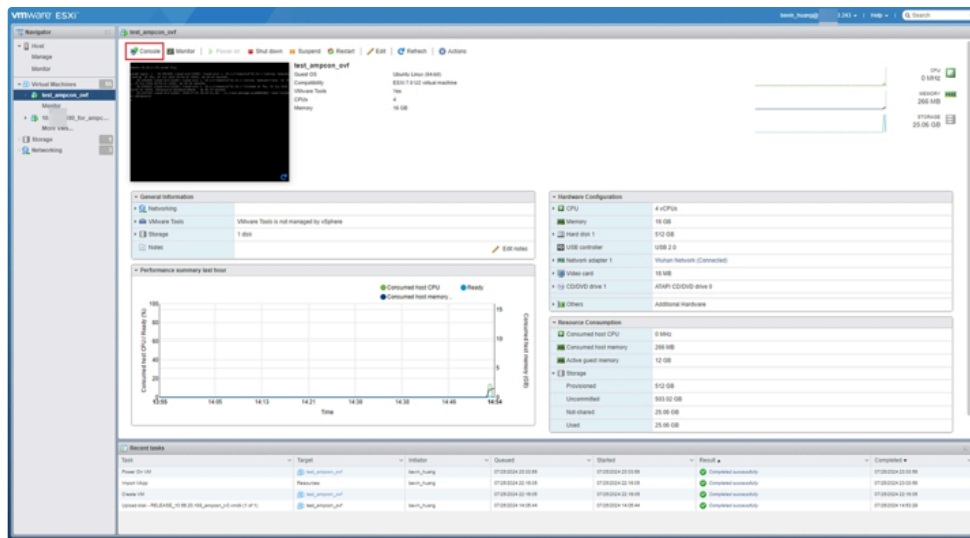
NOTE

The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.

7. On the VMware ESXi console, click the new virtual machine name that you specified in step 3.



8. Click **Console** to open the virtual machine console.

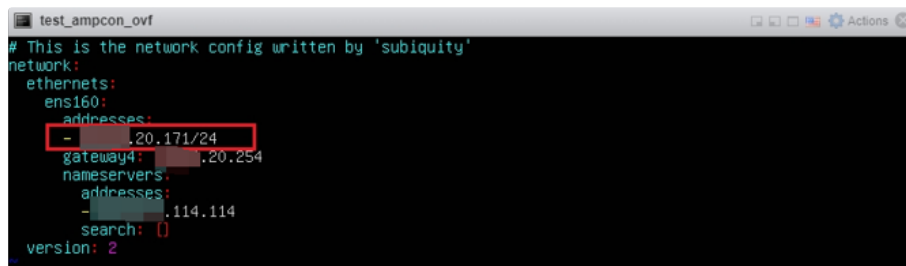


9. Modify the network interface configuration.

- Log in to the virtual machine with the default username (pica8) and password (pica8).
- Open the file named 00-installer-config.yaml by running the following command:

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

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



- Apply the network interface configuration by running the following command:

```
sudo netplan apply
```

10. Start the AmpCon-Campus server:

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

```
cd /usr/share/automation/server
```

- Start the AmpCon-Campus server by running the following command:

```
sudo ./start.sh
```

Now the AmpCon-Campus server is installed and started.

What to Do Next

- If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-Campus server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-Campus server and managed switches might fail.

For more information, see [Multi-NIC Deployment for Switch Connectivity](#).

- To stop the AmpCon-Campus server, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Stop the AmpCon-Campus server by running the **sudo ./stop.sh** command.
- To start the the AmpCon-Campus server after it is stopped, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Start the AmpCon-Campus server by running the **sudo ./start.sh** command.

Installing on QEMU or KVM

You can install the AmpCon-Campus server on QEMU or KVM. For how to use QEMU or KVM in general, see the [KVM documentation](#) and [QEMU documentation](#).

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

[Prerequisites](#)

[Installation Procedure](#)

[What to Do Next](#)

Prerequisites

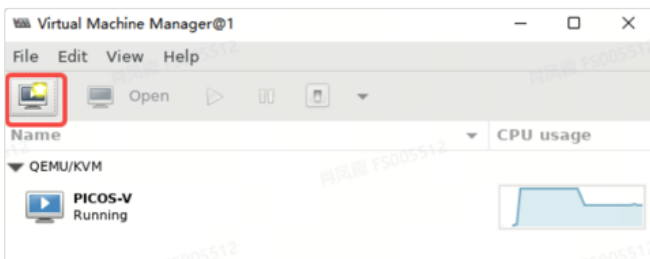
- Ensure that the [installation requirements](#) are met.
- Download the compressed AmpCon-Campus server image **AmpCon-Campus for QEMU/KVM V2.3.x Software** from the [FS AmpCon-Campus website](#).
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

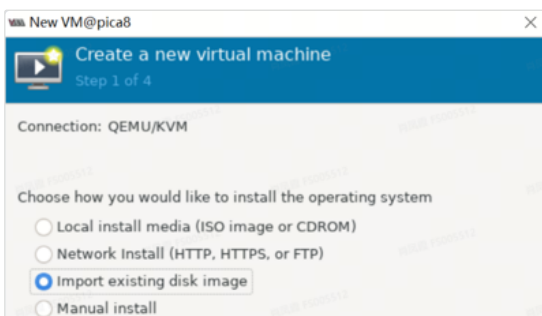
1. Open the virt-manager console by running the following command:

```
virt-manager
```

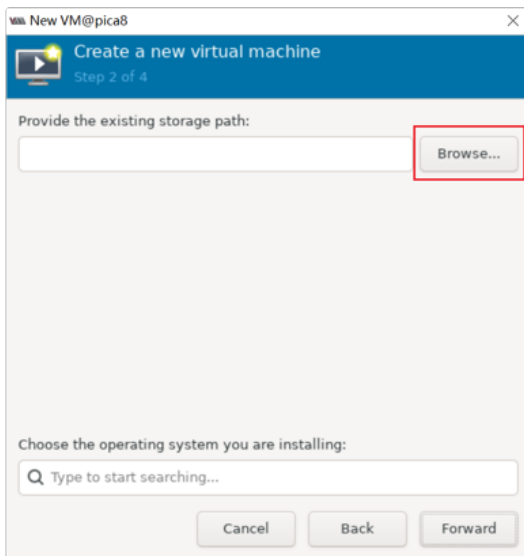
2. Click the following button to start the importing process.



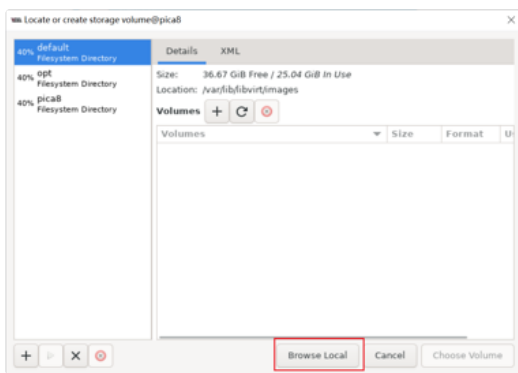
3. Select **Import existing disk image**, and then click **Forward**.



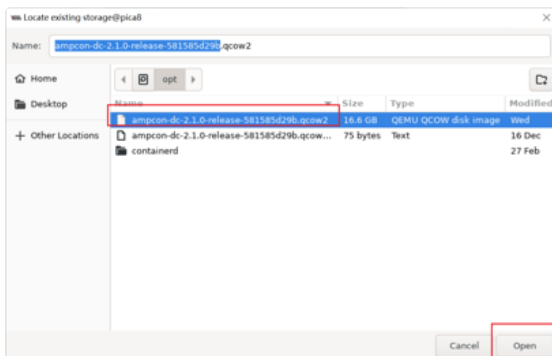
4. Click **Browse** to select the AmpCon-Campus server .qcow2 image file.



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



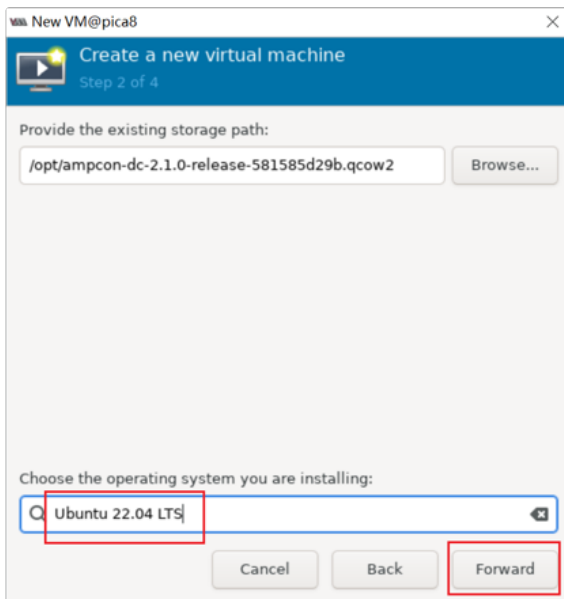
6. Find the location of the AmpCon-Campus server .qcow2 image file, and then click **Open**.



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

NOTE

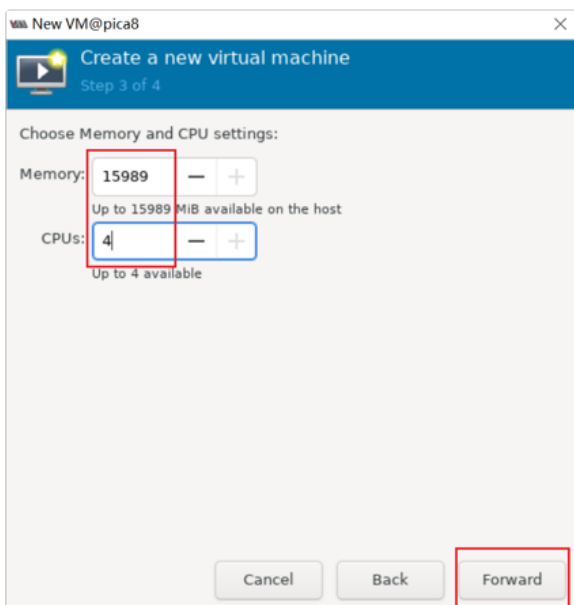
Do not select other operating systems because AmpCon-Campus supports only Ubuntu 22.04 currently.



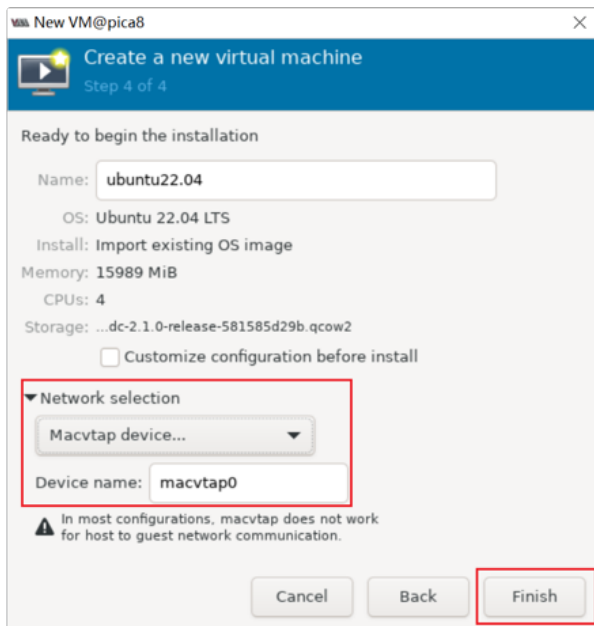
8. Adjust the memory and CPU settings as needed, and then click **Forward**.

NOTE

The memory and CPU settings need to meet the [Server Requirements](#).



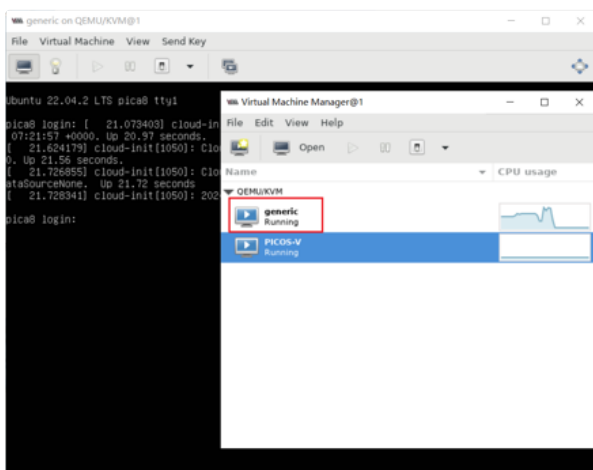
9. In the **Network selection** section, select **Macvtap device**, and enter the device name. Then, click **Finish**.



Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-Campus server is installed.

NOTE

The AmpCon-Campus server is installed in the `/usr/share/automation/server` directory. Currently, you can't customize the installation directory.



10. Modify the network interface configuration.

- Log in to the virtual machine with the default username (pica8) and password (pica8).
- Open the file named `00-installer-config.yaml` by running the following command:

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

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

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens3:
      addresses:
        - 10.190/24
      gateway4: 10.20.254
      nameservers:
        addresses:
          - 114.114
      search: []
  version: 2
```

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

```
sudo netplan apply
```

11. Start the AmpCon-Campus server:

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

```
cd /usr/share/automation/server
```

b. Start the AmpCon-Campus server by running the following command:

```
sudo ./start.sh
```

Now the AmpCon-Campus server is started.

What to Do Next

- If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-Campus server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-Campus server and managed switches might fail.

For more information, see [Multi-NIC Deployment for Switch Connectivity](#).

- To stop the AmpCon-Campus server, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Stop the AmpCon-Campus server by running the **sudo ./stop.sh** command.
- To start the the AmpCon-Campus server after it is stopped, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Start the AmpCon-Campus server by running the **sudo ./start.sh** command.

Installing on Physical Machines (Ubuntu Docker)

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

[Prerequisites](#)

[Installation Procedure](#)

[What to Do Next](#)

Prerequisites

- Prepare a physical machine based on Ubuntu 22.04 LTS with Docker installed.
- Ensure that the [installation requirements](#) are met.
- Download the compressed AmpCon-Campus server installation package **AmpCon-Campus for Ubuntu Docker V2.3.x Software** from the [FS AmpCon-Campus website](#).

Installation Procedure

1. Put the AmpCon-Campus server installation package to the prepared physical machine, and then extract the package by running the **unzip <package_file_name>.zip** command. A .tar.gz file is generated in the current directory.

Extract the generated .tar.gz file by running the **tar -zxvf <extracted_tar_file_name>.tar.gz** command. A directory is generated with AmpCon-Campus server installation files.

NOTES

- Replace <package_file_name> in the command with the name of the AmpCon-Campus server installation package.
- Replace <extracted_tar_file_name> in the command with the extracted .tar.gz file name.

2. On the physical machine, modify the network interface configuration as follows:
 - 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 real IP address of the physical machine.


```
# This is the network config written by 'subiquity'
network:
  ethernet:
    ens3:
      addresses:
        - 10.190.24
      gateway4: 10.254
      nameservers:
        addresses:
          - 114.114
      search: []
  version: 2
```

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

```
sudo netplan apply
```

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

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

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

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

```
sudo ./install_or_upgrade.sh
```

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

NOTE

The AmpCon-Campus server is installed in the `/usr/share/automation/server` directory. Currently, you can't customize the installation directory.

What to Do Next

- If multiple NICs are added to the virtual machine or physical machine, you must specify one NIC IP address, which is used by AmpCon-Campus server to establish connections with the switches to be managed, in the configuration file (`/usr/share/automation/server/.env`). Otherwise, the connections between the AmpCon-Campus server and the switches to be managed might fail.

For more information, see [Multi-NIC Deployment for Switch Connectivity](#).

- To stop the AmpCon-Campus server, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.

2. Stop the AmpCon-Campus server by running the **sudo ./stop.sh** command.
- To start the the AmpCon-Campus server after it is stopped, follow the steps:
 1. Go to the AmpCon-Campus installation directory by running the **cd /usr/share/automation/server** command.
 2. Start the AmpCon-Campus server by running the **sudo ./start.sh** command.

Multi-NIC Deployment for Switch Connectivity

As described in [Installing the AmpCon-Campus Server](#), you need to import the AmpCon-Campus image file to a virtual machine or unzip the AmpCon-Campus installation packet file on a physical machine to install the AmpCon-Campus server.

If multiple NICs are added to the virtual machine or physical machine, you must specify one NIC IP address, which is used by the AmpCon-Campus server to establish connections with the switches to be managed, in the configuration file (`/usr/share/automation/server/.env`).

Otherwise, the connections between the AmpCon-Campus server and the switches to be managed might fail.

NOTES

- When you install the AmpCon-Campus server on a virtual machine, the imported AmpCon-Campus image file contains only one Network Interface Card (NIC). But you can manually add more NICs.
- When you install the AmpCon-Campus server on a physical machine, 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.

[Prerequisite](#)

[Procedure](#)

Prerequisite

Ensure that the AmpCon-Campus server is installed on a virtual machine or a physical machine.

Procedure

1. Log in to the virtual machine or the physical machine, and then open the **`/usr/share/automation/server/.env`** file.

```
sudo vim /usr/share/automation/server/.env
```

2. Locate the line containing **`PROD_IP=`** in the file, and add the NIC IP address of the AmpCon-Campus server machine, which is used to connect to the switches to be managed.

```
pica8@pica8:~$ cat /usr/share/automation/server/.env
PRO_TYPE=ampcon-campus
PROD_IP=
BUILD_PATH=dist
GENERATE_SOURCEMAP=false
REACT_APP_PRE_VERSION=9e16b9971d
REACT_APP_VERSION=e95150caad
REACT_APP_BRANCH=2.3.0-dev-campus
REACT_APP_MAJOR_VERSION=2.3.0
IMG_CENTER_PROXY_DOMAIN=harbor.ampcon.com/ampcon-t-base
IMG_CENTER_PROXY_IP=10.56.20.229
```

3. Restart the AmpCon-Campus server by the following commands:

```
cd /usr/share/automation/server/
```

```
sudo ./start.sh
```

Upgrading the AmpCon-Campus Server

To upgrade AmpCon-Campus to 2.3.0 or 2.3.1, see the following upgrading path and procedure.

[Upgrading Path](#)

[Upgrading Procedure](#)

Upgrading Path

- You can upgrade AmpCon-Campus 2.1.x (2.1.0 or 2.1.1), 2.2.x (2.2.0 or 2.2.1) or 2.3.0E to 2.3.0 or 2.3.1.
- You can upgrade AmpCon-Campus 2.3.0 to 2.3.1.

Upgrading Procedure

1. Download the AmpCon-Campus server upgrade package **Software Upgrade Package for AmpCon-Campus V2.3.x** from the [FS AmpCon-Campus website](#). Then, the upgrade package will be downloaded to your local machine.
2. Copy the upgrade package to the AmpCon-Campus server machine, and then extract the package by running the following command:

```
unzip <upgrade_package_file_name>.zip
```

Replace *<upgrade_package_file_name>* with the real upgrade package name.

Then, a .tar.gz file is generated in the current directory.

Run the following command to extract the .tar.gz file:

```
tar -zxvf <extracted_tar_file_name>.tar.gz
```

Replace *<extracted_tar_file_name>* with the real extracted .tar.gz file name.

3. After extracting the .tar.gz file, go to the extracted directory, and then run the following upgrade command:

4. Wait for the upgrade process to complete. Once you see a success message, the upgrade is finished.

5. Log in to the AmpCon-Campus UI, and then click **admin > Version** to check the current AmpCon-Campus version.



Uninstalling the AmpCon-Campus Server

To uninstall the AmpCon-Campus server, follow these steps:

Procedure

1. Go to the root directory of the AmpCon-Campus server, and run the stop script with sudo privileges:

```
cd /usr/share/automation/server
```

```
sudo ./stop.sh
```

2. Clear the files in the server directory with sudo privileges:

```
sudo rm -rf /usr/share/automation/server
```

Working with the User Interface

After you install the AmpCon-Campus server, you can use the AmpCon-Campus user interface (UI).

[Prerequisites](#)

[Logging In](#)

[Logging Out](#)

[UI Overview](#)

[UI Menus](#)

[UI Conventions](#)

Prerequisites

Before you use the AmpCon-Campus UI, ensure that the following prerequisites are met:

- The network connection between your local computer and the AmpCon-Campus server is available, and the AmpCon-Campus server is started and running properly.
- To use the Terminal Access Controller Access Control System (TACACS+) server for authentication and authorization of AmpCon-Campus login users, enable the TACACS+ integration first. For more information, see [Configuring TACACS+ Authentication and Authorization](#).
- 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 **SuperAdmin** role. It has all operation permissions on AmpCon-Campus. For security purposes, change the password upon the first login, update it periodically, and keep it secure. For how 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 web browser, enter the URL of the AmpCon-Campus server in the format of "https://<AmpCon-Server-IP-or-Domain-Name>/login".

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

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.

Welcome to AmpCon-Campus

Username

Password

☒ Keep me signed in

LOGIN

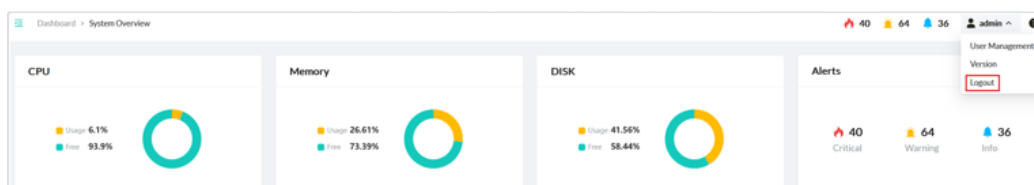
4. Optional: Select **Keep me signed in** to extend the allowed inactivity time of the AmpCon-Campus UI.

- 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 365 days of inactivity in the AmpCon-Campus UI.
- If AmpCon-Campus services are restarted, all AmpCon-Campus UI sessions will be logged out.

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

Logging Out

To log out of the AmpCon-Campus UI, hover your mouse over the username at the top right corner of the homepage, and then click **Logout**.



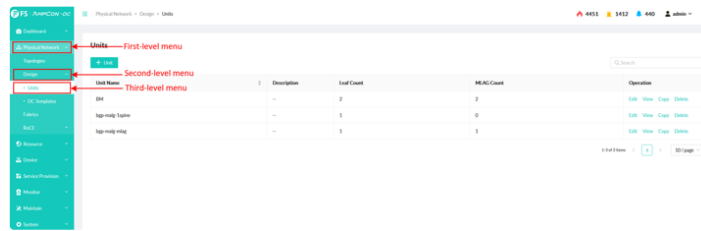
UI Overview

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

Table 1. Homepage Descriptions

Section	Description
Navigation Bar	Click a first-level menu from the navigation bar, and then click a second-level menu. If the second-level menu contains third-level menus, click a third-level menu.

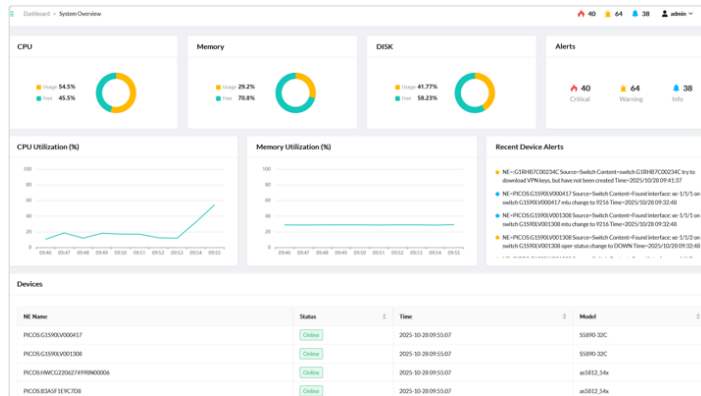
Then, you can see a specific page on the right.



Page

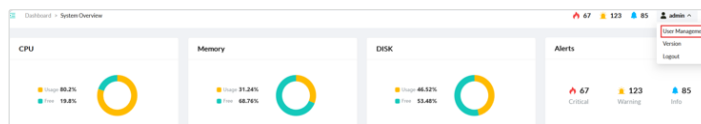
After clicking a second-level or third-level menu from the navigation bar, you can see a specific page on the right.

For example, click **Dashboard > System Overview** from the navigation bar. Then, you can see the “System Overview” page on the right, where you can check managed switches and the health of the AmpCon-Campus server.

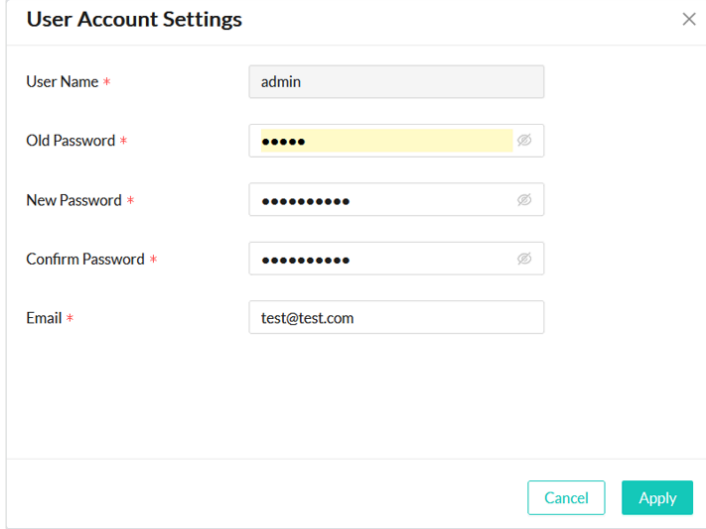
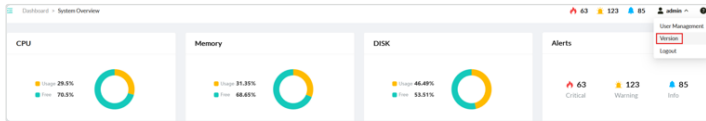
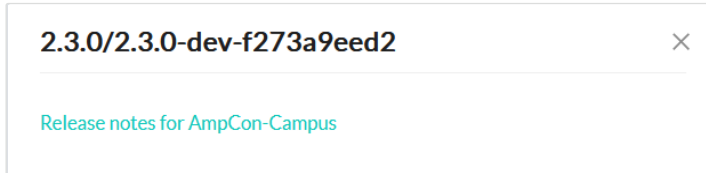
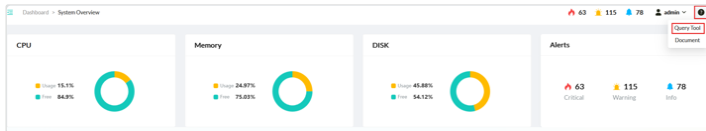


User Management

Hover your mouse over the username at the top right corner of the homepage, and then click **User Management**.



In the pop-up window, you can change the user password and associated email address.

	 User Account Settings User Name * admin Old Password * [masked] New Password * [masked] Confirm Password * [masked] Email * test@test.com Cancel Apply
Version	Hover your mouse over the username at the top right corner of the homepage, 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. 
Query Tool	Hover over the question icon at the top right corner of the homepage, and then click Query Tool.  Then, you will be redirected to the FS Query Tool page.
Document	Hover your mouse over the question icon at the top right corner of the homepage, and then click Document. Then, you will be redirected to the AmpCon-Campus doc site.

	
Alert	Check the total number of alerts in the Critical (also called Error), Info, or Warning level. For the definition of each alert level, see Alert Types and Levels. 

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

The AmpCon-Campus UI enables you to deploy, configure, and manage your networks easily. In addition, it gives you deep visibility into your networks and managed devices.

To quickly master the use of the AmpCon-Campus UI, learn the purposes of the following UI menus:

NOTE

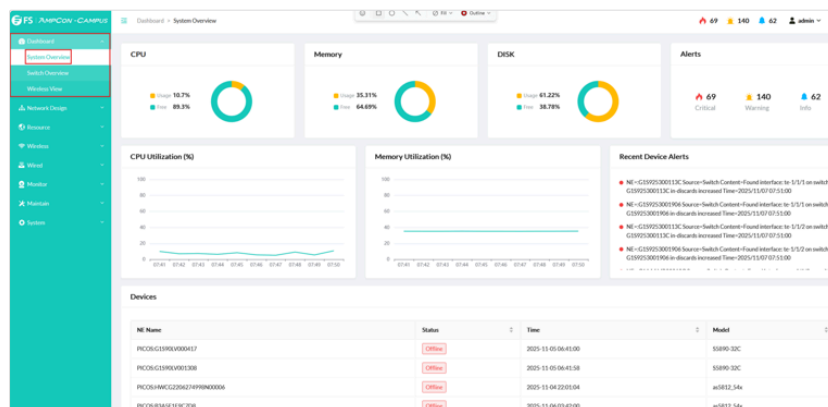
Only the AmpCon-Campus users with the **SuperAdmin** role can use all the following UI menus. For UI menu permissions of each user role, see [User Permission Table](#).

Dashboard
Network Design
Resource
Wireless
Wired
Monitor
Maintain
System

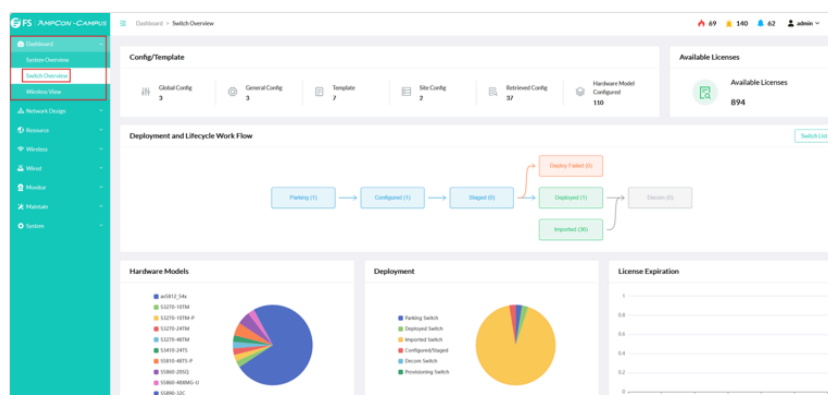
Dashboard

In the navigation bar, click the **Dashboard** first-level menu. You can see three second-level menus: **System Overview**, **Switch Overview**, and **Wireless Overview**.

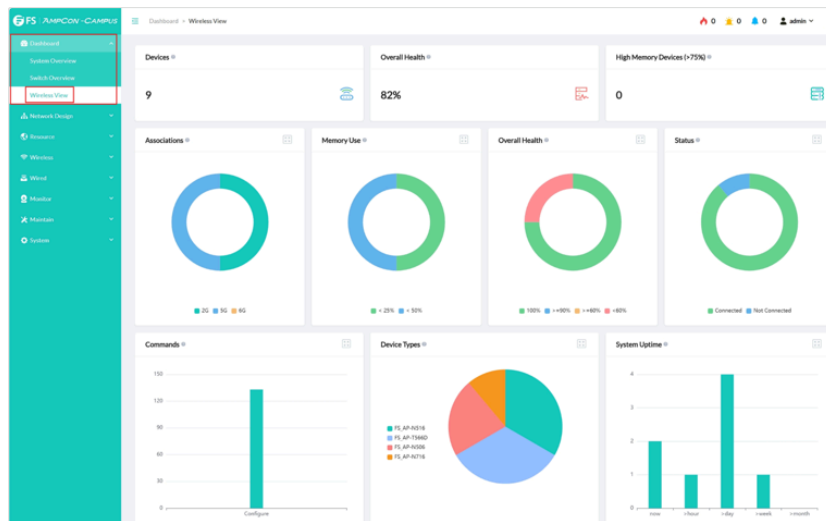
Click **Dashboard > System Overview**. On the “System Overview” page, you can check managed PicOS switches and the health of the AmpCon-Campus server. For more information, see [System Overview](#).



Click **Dashboard > Switch Overview**. On the “Switch Overview” page, you can have a basic overview of PicOS switch statistics and graphs. For more information, see [Switch Overview](#).



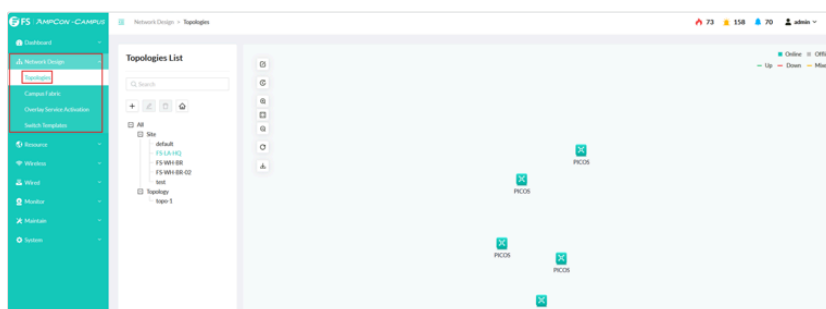
Click **Dashboard > Wireless View**. On the “Wireless View” page, you can have a quick understanding of deployed wireless networks, such as managed access points (APs), AP health status, and connected terminal devices (STAs). For more information, see [Wireless View](#).



Network Design

In the navigation bar, click the **Network Design** first-level menu. You can see four second-level menus: **Topologies**, **Campus Fabric**, **Overlay Service Activation**, and **Switch Templates**.

Click **Network Design > Topologies**. On the “Topologies” page, you can visualize your PicOS switches in all locations and drill down into an individual PicOS switch, right to the port level, to check port stats and overall health of the switch. For more information, see [Topology](#).

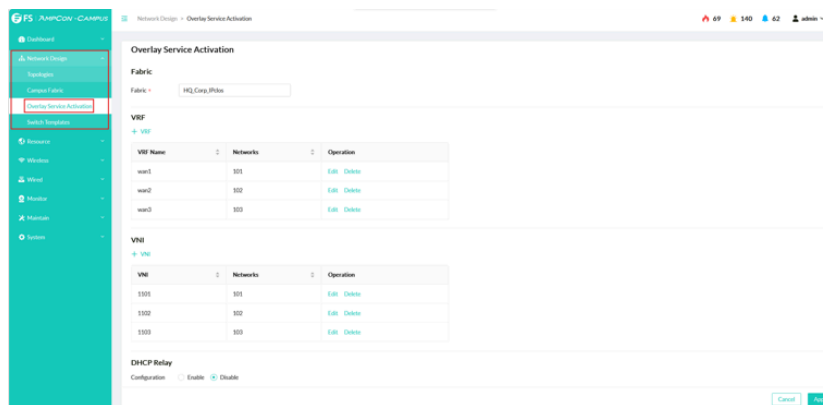


Click **Network Design > Campus Fabric**. On the “Campus Fabric” page, you can design and deploy IP Clos fabrics and MLAG fabrics. For more information, see [Designing Campus Fabrics](#).

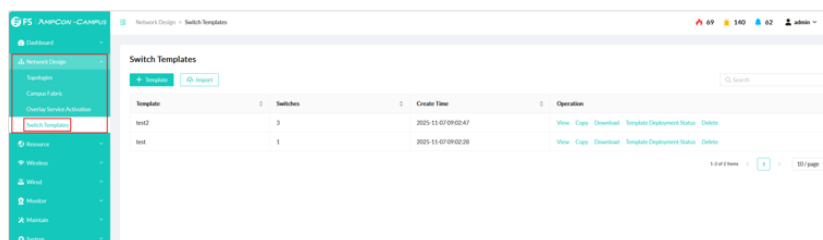
The screenshot displays the 'Campus Fabric' page in the FS AMPON-CAMPUS interface. The left sidebar has 'Network Design' highlighted, and 'Campus Fabric' is selected. The main content area shows a table of campus fabrics.

Name	Site	Topology Type	Date Created	Operation
HQ-Corp-IP-Clos-Type	FS-WH01-BB	IP-Clos	2025-10-29 10:10:29	View Delete
HQ-Corp-IP-Clos-Rep-02	FS-WH01-BB-02	IP-Clos	2025-10-29 10:36:16	View Delete
1000-mlag	default	IP-Clos	2025-10-30 09:58:23	View Delete
HQ-Corp-IP-Clos	FS-WH01-BB	IP-Clos	2025-11-05 11:42:50	View Delete
HQ-Corp-MLAG-Type	FS-LA-HQ	MLAG	2025-11-07 07:30:15	View Delete

Click **Network Design > Overlay Service Activation**. On the “Overlay Service Activation” page, you can modify overlay-related configurations (VRF, VNI, and DHCP relay configurations) for added IP Clos fabrics. For more information, see [Provisioning Overlay Services](#).



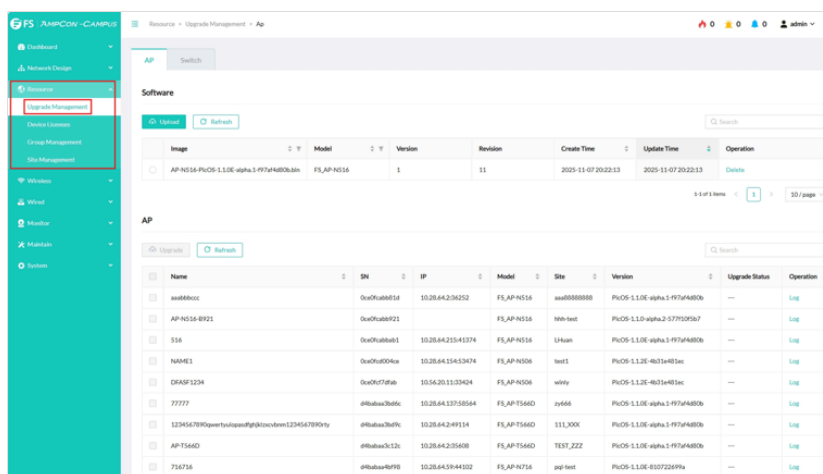
Click **Network Design > Switch Templates**. On the “Switch Templates” page, you can configure PicOS switches by adding a switch configuration template and applying it to PicOS switches in one or multiple sites. For more information, see [Switch Templates](#).



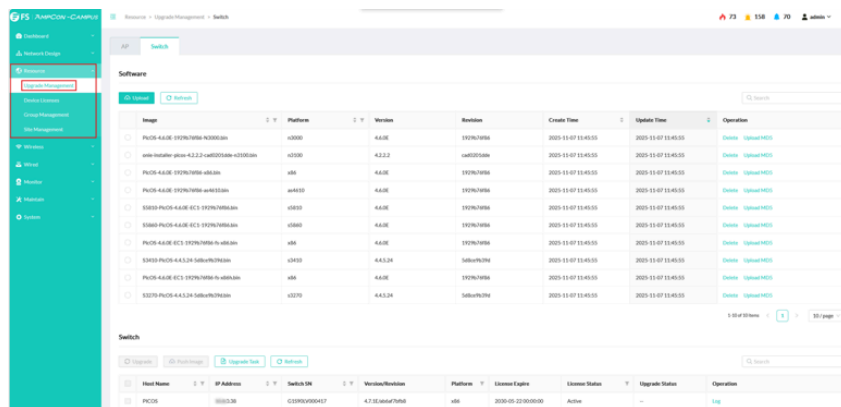
Resource

In the navigation bar, click the **Resource** first-level menu. You can see four second-level menus: **Upgrade Management**, **Device Licenses**, **Group Management**, and **Site Management**.

Click **Resource > Upgrade Management**. In the **AP** tab, you can upgrade AP firmware one by one or in batches. For more information, see [Upgrading AP Firmware](#).



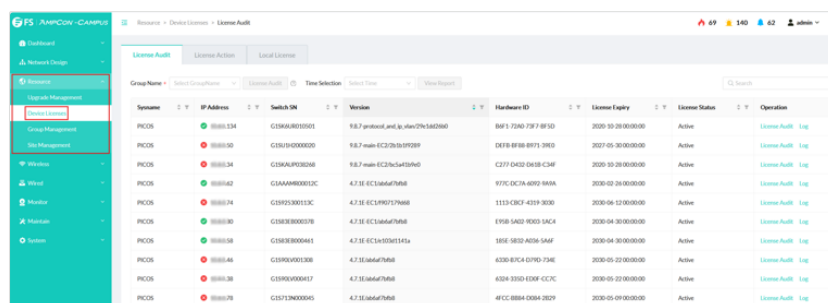
In the **Switch** tab, you can upload PicOS images and upgrade PicOS on a single PicOS switch or on multiple PicOS switches in bulk. For more information, see [Uploading and Upgrading PicOS Images](#).



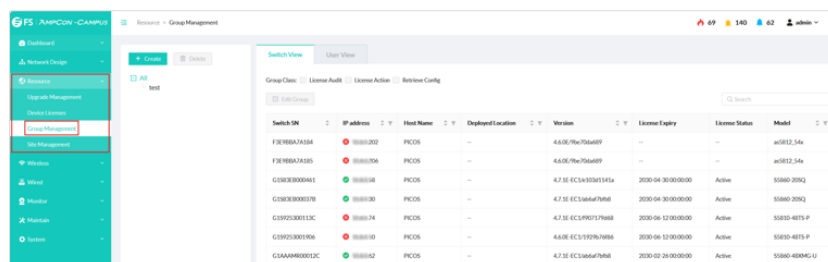
Click **Resource > Device Licenses**. On the “Device Licenses” page, you can do the following operations:

- In the **License Audit** tab, verify whether PicOS licenses are valid or not.
- In the **License Action** tab, verify whether PicOS licenses are valid and extend expired PicOS licenses.
- In the **Local License** tab, add local PicOS licenses to AmpCon-Campus manually if the AmpCon-Campus server can’t access the License Portal.

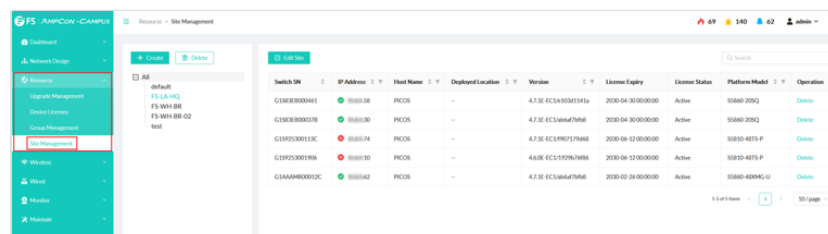
For more information, see [Managing PicOS Licenses](#).



Click **Resource > Group Management**. On the “Group Management” page, you can add PicOS switches to a switch group and designate operation permissions for PicOS switches in the switch group. For more information, see [Managing Groups](#).



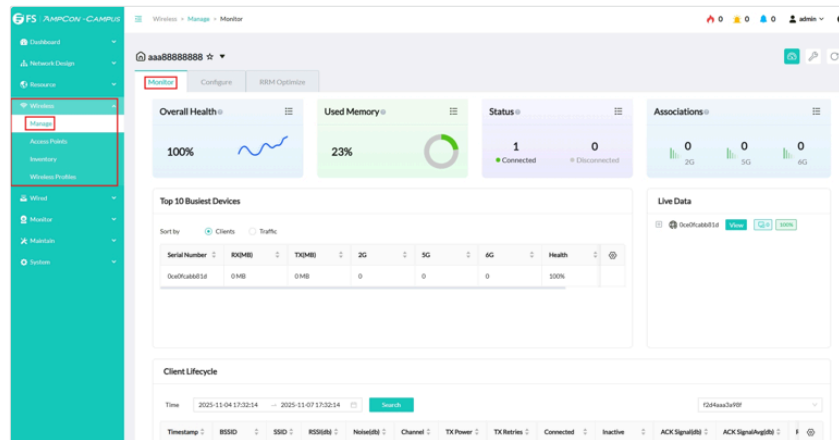
Click **Resource > Site Management**. On the “Site Management” page, you can add PicOS switches to a site. For more information, see [Managing Sites](#).



Wireless

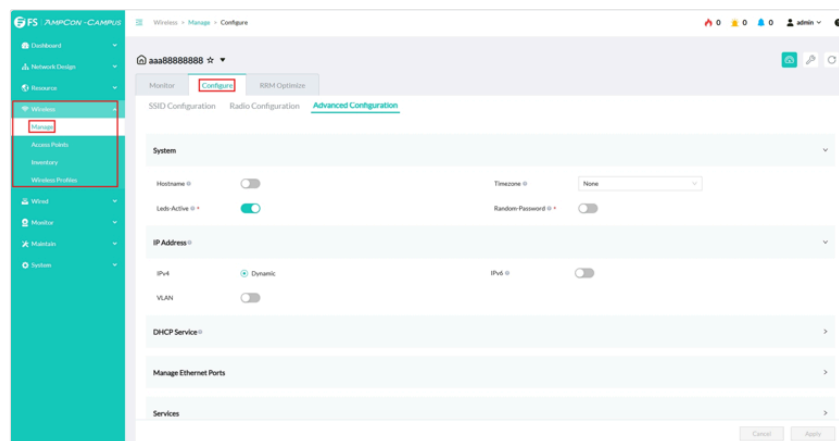
In the navigation bar, click the **Wireless** first-level menu. You can see four second-level menus: **Manage**, **Access Points**, **Inventory**, and **Wireless Profiles**.

Click **Wireless > Manage**. In the **Monitor** tab, you can monitor the overall running status of each wireless site. For more information, see [Monitoring Wireless Sites](#).

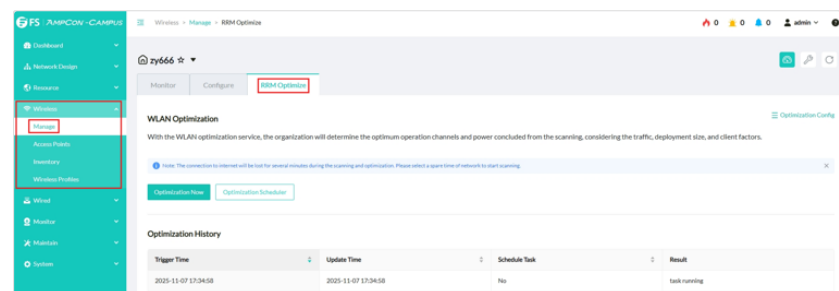


In the **Configure** tab, you can add SSID configurations, radio configurations, and advanced configurations for all APs in a wireless site. For more information, see the following topics:

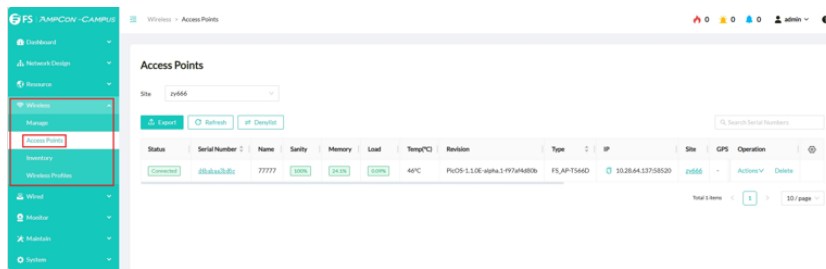
- [Adding SSID Configurations](#)
- [Optional: Adding Radio Configurations](#)
- [Optional: Adding Advanced Configurations](#)



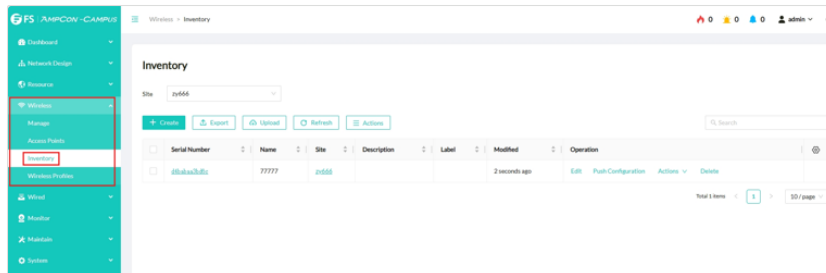
In the **RRM Optimize** tab, you can optimize wireless networks immediately or at a fixed time. You can also customize network optimization configurations. For more information, see [Optimizing Wireless Networks](#).



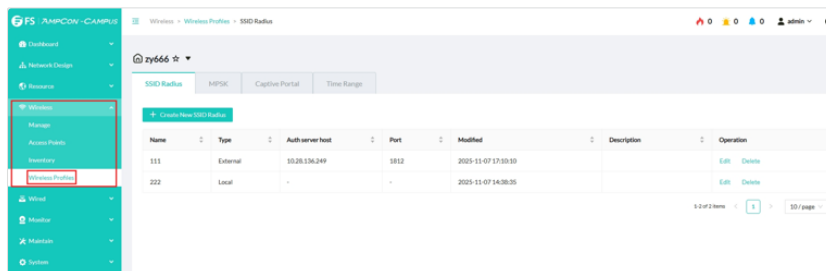
Click **Wireless > Access Points**. On the “Access Points” page, you can check detailed metrics of each managed AP. For more information, see [Monitoring APs](#).



Click **Wireless > Inventory**. On the “Inventory” page, you can maintain wireless networks, such as accessing, positioning, or rebooting APs. For more information, see [Maintaining Wireless Networks](#).



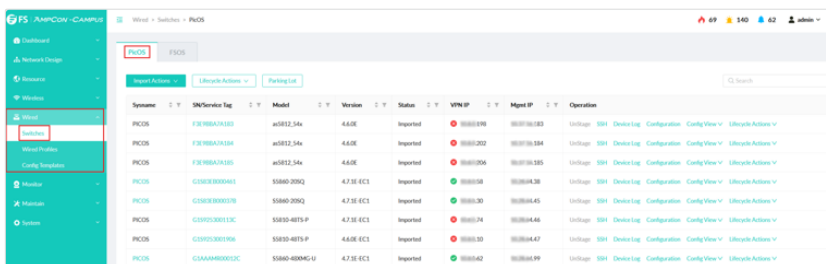
Click **Wireless > Wireless Profiles**. On the “Wireless Profiles” page, you can configure some profiles, such as RADIUS servers, Multiple Pre-Shared Key (MPSK), Captive Portal, and the enabling time ranges for SSIDs or radio. Then, when you add SSID configurations or radio configurations, you can use these pre-defined profiles. For more information, see [Adding Wireless Profiles](#).



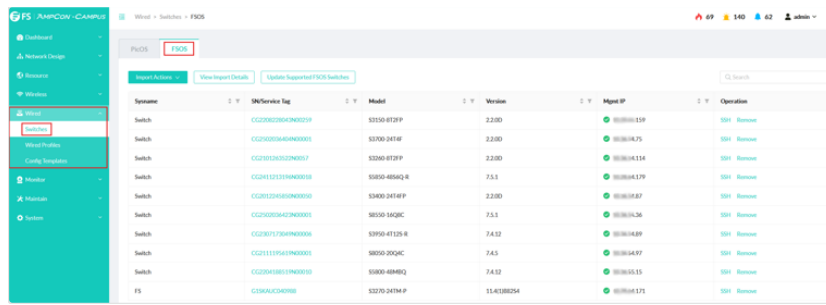
Wired

In the navigation bar, click the **Wired** first-level menu. You can see three second-level menus: **Switches**, **Wired Profiles**, and **Config Templates**.

Click **Wired > Switches**. In the **PiCOS** tab, you can import, view, and manage PiCOS switches. For more information, see [Importing PiCOS Switches](#) and [Managing Switches](#).

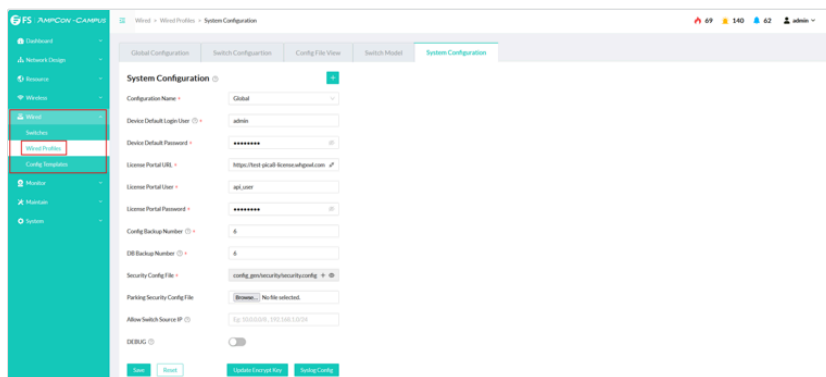


In the **FSOS** tab, you can import and view FSOS switches. For more information, see [Importing FSOS Switches](#).

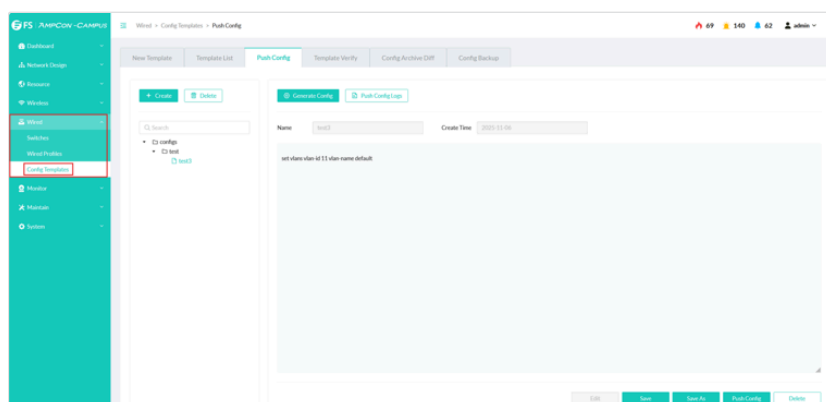


Click **Wired > Wired Profiles**. On the “Wired Profiles” page, you can add the configurations used for PicOS switch deployment. For more information, see the following documents:

- [Configuring Global Configurations](#)
- [Adding Switch Configurations](#)
- [Managing Global and Switch Configurations](#)
- [Configuring Switch Models](#)
- [Adding System Configurations](#)



Click **Wired > Config Templates**. On the “Config Templates” page, you can configure and manage configuration templates, push configurations to PicOS switches, back up and restore configurations for disaster recovery, or compare configurations for troubleshooting or auditing. For more information, see [Configuration Templates](#).

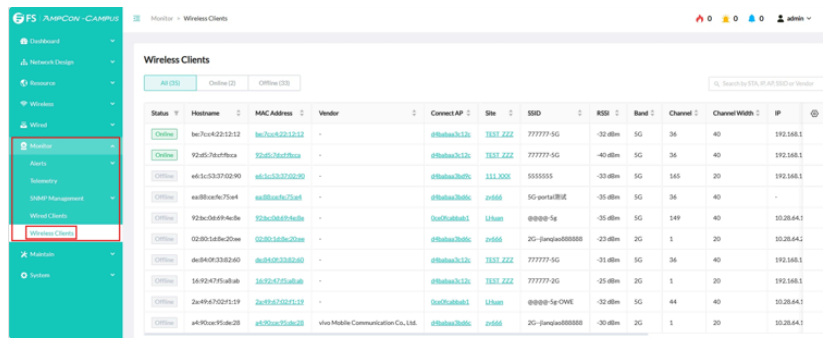


Monitor

In the navigation bar, click the **Monitor** first-level menu. You can see five second-level menus: **Alerts**, **Telemetry**, **SNMP Management**, **Wired Clients**, and **Wireless Clients**.

Click **Monitor > Alerts**. You can see three third-level menus: **Alert List**, **Notification Rules**, and **Notification History**.

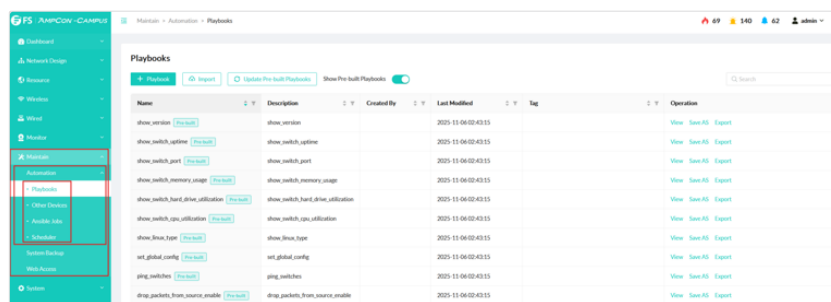
By using these menus, you can view all triggered alerts, configure real-time email notifications, and check email notification history. For more information, see [Alerts](#).



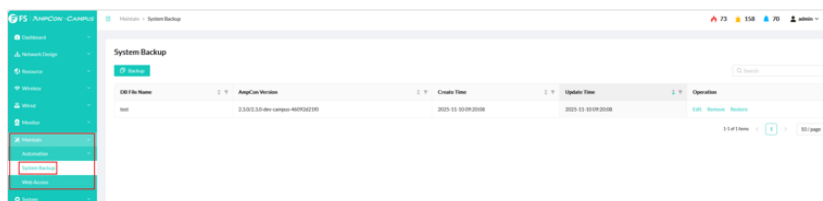
Maintain

In the navigation bar, click the **Maintain** first-level menu. You can see three second-level menus: **Automation**, **System Backup**, and **Web Access**.

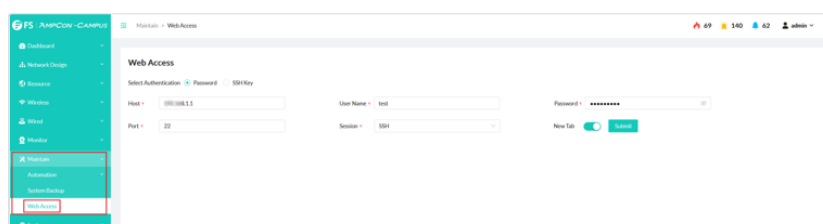
Click **Maintain > Automation**. You can see four third-level menus: **Playbooks**, **Other Devices**, **Ansible Jobs**, and **Scheduler**. By using these menus, you can write, run, schedule, and manage Ansible playbooks on managed PicOS switches and added Linux servers. For more information, see [Running Ansible Playbooks for Automation](#).



Click **Maintain > System Backup**. On the “System Backup” page, you can back up and restore the AmpCon-Campus database securely for disaster recovery. For more information, see [Backing Up and Restoring the AmpCon-Campus Database](#).



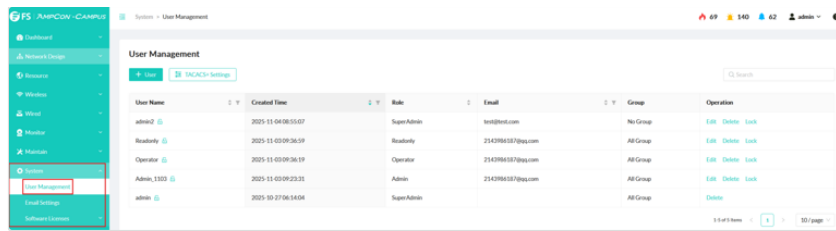
Click **Maintain > Web Access**. On the “Web Access” page, you can connect to a device (such as a switch or terminal device) by creating an SSH session. For more information, see [Accessing Devices through SSH Sessions](#).



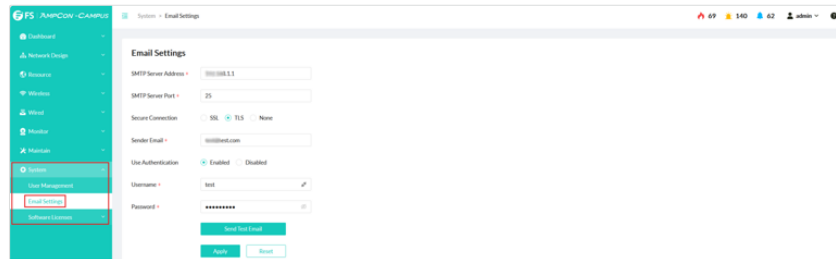
System

In the navigation bar, click the **System** first-level menu. You can see three second-level menus: **User Management**, **Email Settings**, and **Software Licenses**.

Click **System > User Management**. On the “User Management” page, you can manage user access so that users are assigned with appropriate permissions. For more information, see [Managing User Access](#).

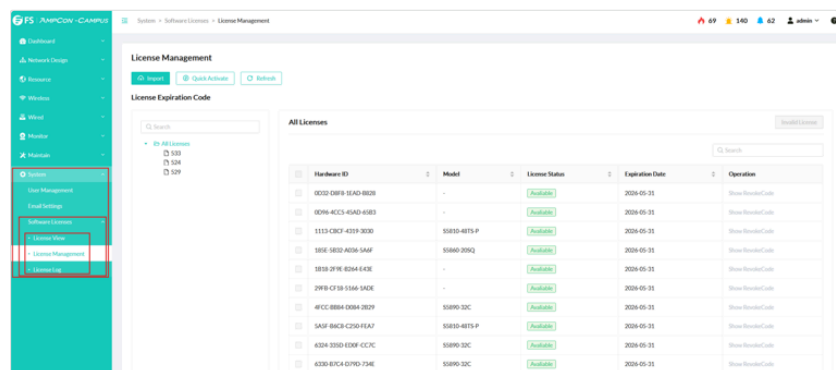


Click **System > Email Settings**. On the “Email Settings” page, you can configure an SMTP server to receive alert notifications through emails. For more information, see [Configuring an SMTP Server](#).



Click **System > Software Licenses**. You can see three third-level menus: **License View**, **License Management**, and **License Log**.

By using these menus, you can import AmpCon-Campus licenses, convert a trial AmpCon-Campus license to a standard AmpCon-Campus license, or invalidate the AmpCon-Campus license on a PicOS switch to release the license. In addition, you can check operation logs and alerts related to AmpCon-Campus licenses. For more information, see [Managing AmpCon-Campus Licenses](#).



UI Conventions

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

- Graph
- Highlighting
- Mandatory Configurations
- Search
- Time Selection
- Time Zone
- General Buttons
 - Apply Button
 - Cancel Button
 - Delete Button
 - Edit Button
 - Export Button
 - Log Button
 - Refresh Button
 - View Button
- General Icons
 - Close Icon
 - Download Icon
 - Filter Icon
 - Help Icon
 - Metric Selection Icon
 - Remove Icon
 - Sort Icon
 - Unfold Icon

Graph

For each monitoring graph, you can hover your mouse over a time point to check for detailed metric data at that time point.



Highlighting

Some columns have information displayed in green. Click the information in green, and then you can edit the information or be redirected to another page.

PcOS

FSOS

Import Actions

Lifecycle Actions

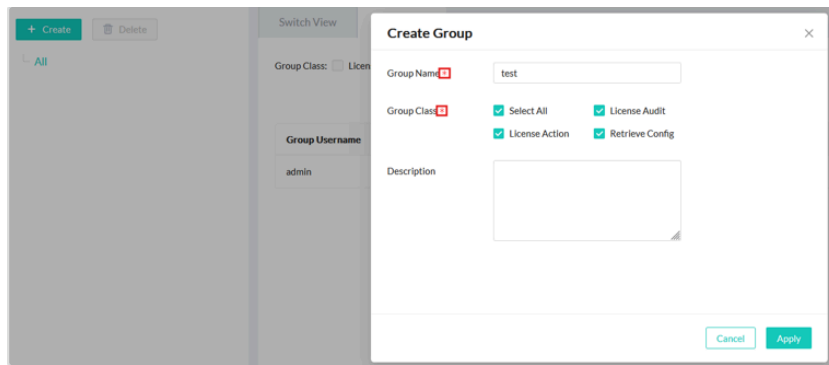
Parking List

Q Search

Sysname	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation
PCOS	G1590LV000417	S5800-32C	4.7.1E	Imported	0.38	64.39	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PCOS	G1590LV001308	S5800-32C	4.7.1E	Imported	0.46	64.48	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PCOS	HWCC2206274919N00006	as5812_54a	4.6.0E	Imported	0.42	20.60	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PCOS	B3A5F1E9C7D8	as5812-54a	4.6.0E	Imported	0.98	16.92	Unstage SSH Device Log Configuration Config View Lifecycle Actions

Mandatory Configurations

All the configuration parameters marked with asterisks must be configured. Other configurations are optional.



Search

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

Alert List

Search

☐	Last Time	Switch SN	Type	Message	Count	Operation
☐	2025-10-29 01:40:47	G18HDXC00234C	Warning	switch G18HDXC00234C try to download VPN keys, but have not been created	2131	Mark as Read
☐	2025-10-29 01:40:05	G1890V001308	Error	Found interface: ve-1/1/31 on switch G1890V001308 in-discards increased	2197	Mark as Read
☐	2025-10-29 01:40:05	G1892S3001908	Error	Found interface: te-1/1/1 on switch G1892S3001908 in-discards increased	2189	Mark as Read

Time Selection

Some pages have the time selection box. Select the start date and end date to display only the data in the selected time range.

By default, the data in the last 5 minutes are displayed.



Time Zone

All times displayed in the AmpCon-Campus UI are in the UTC+0 time zone.

New Template Template List Push Config Template Verify Config Archive Diff Config Backup

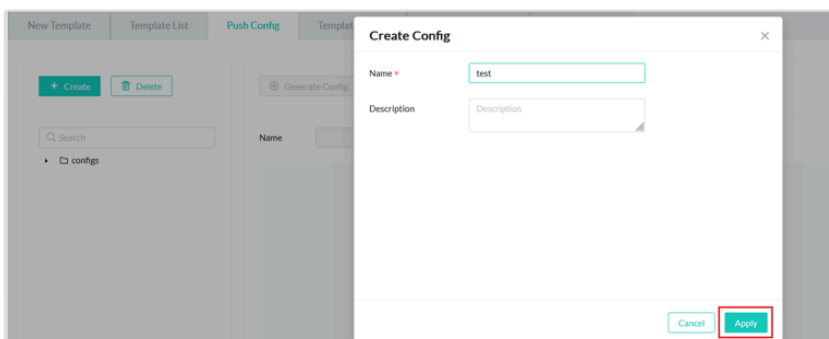
Search

Template Name	Description	Create Time	Tag	Operation
c410-24h		2025-10-28 02:11:07		View Template Remove Template Copy Export Tag Management
c5270-50m		2025-10-27 08:29:17		View Template Remove Template Copy Export Tag Management
test		2025-10-27 07:20:59		View Template Remove Template Copy Export Tag Management

General Buttons

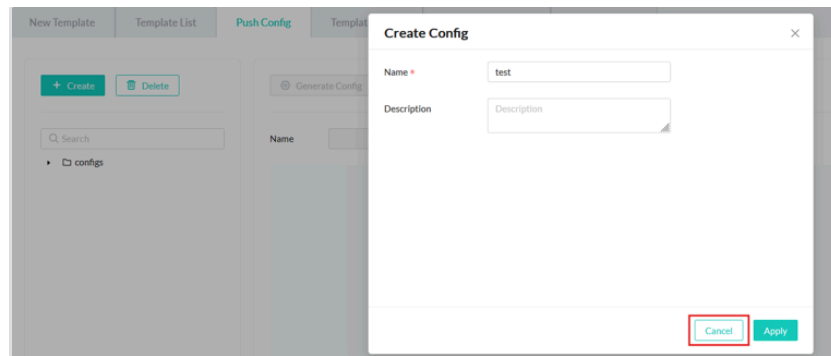
Apply Button

Some pages have the **Apply** button. Click the button to apply configurations.



Cancel Button

Some pages have the **Cancel** button. Click the button to cancel an operation.



Delete Button

Some pages have the **Delete** button. Click the button to delete an item.

Global Configuration		Switch Configuration		Config File View		Switch Model		System Configuration			
											Q Search
Config File Name		Model		Type		Last Update Time		Operation			
G38H@FC00234C_40s_config		S343D-24T5		site		2025-10-28 02:13:22		View	Associated	Delete	
2025-10-28-glob-S343D-24T5-333		S343D-24T5		global		2025-10-28 02:10:35		View	Associated	Delete	
G35U1H000000_40s_config		S327D-10T1M		site		2025-10-28 02:00:02		View	Associated	Delete	
2025-10-27-glob-S586D-480MG-U-666		S586D-480MG-U		global		2025-10-27 09:21:44		View	Associated	Delete	
2025-10-27-glob-S327D-10T1M-111		S327D-10T1M		global		2025-10-27 08:50:49		View	Associated	Delete	

Edit Button

Some pages have the **Edit** button. Click the button to edit an item.

VNI		
+ VNI		
VNI	Networks	Operation
11	HQ-Corp-Internet-01	Edit Delete
12	HQ-Corp-Internet-02	Edit Delete
13	HQ-Corp-Internet-03	Edit Delete

Export Button

Some pages have the **Export** button. Click the button to export data. You might need to select the items to be exported first.

License Log				
Export Refresh				
Name	Create Time	Operation	Status	
S33	2025-10-27 07:26:56	Import License	Success	
S33	2025-10-27 07:26:02	Import License	Success	
S24	2025-10-27 06:49:46	Import License	Success	
S33	2025-10-27 06:41:27	Import License	Success	
-	2025-10-27 06:29:50	Import License	Error	

Log Button

Some pages have the **Log** button. Click the button to view log details.

License Audit						
License Action		Local License				
Group Name	Select Group Name	License Audit	Time Selection	Select Time	View Report	
System	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status
NE560-32C	10.0.0.10	C157136000205	4.0.0 OCN1929v7686	1399-1554-0C8F-7F61	2024-02-26 00:00:00	Active
NE560-32C	10.0.0.14	C157136000196	4.0.0 OCN1929v7686	72FCAE3-BE7B-9730	2024-02-26 00:00:00	Active
NE560-32C	10.0.0.70	C15713600021C	4.0.0 OCN1929v7686	E36D-000D-2903-0D48	2024-02-26 00:00:00	Active
NE560-32C	10.0.0.18	C1590XV00085	4.0.0 OCN1929v7686	73D1-D494-06C4-2385	2030-05-22 00:00:00	Active

Refresh Button

Some pages have the **Refresh** button. Click the button to refresh data.

License Management				
Import Quick Activate Refresh				
License Expiration Code				
Search				
All Licenses				
Hardware ID	Model	License Status	Expiration Date	Operation
00102-08F8-15AD-8626	-	Available	2024-05-31	View Record Code
0094-4CC3-45AD-418D	-	Available	2024-05-31	View Record Code
1113-CR0F-4219-3030	S581D-4815-P	Available	2024-05-31	View Record Code

View Button

Some pages have the **View** button. Click the button to view data.

Campus Fabric

+ Campus Fabric

Search

Name	Site	Topology Type	Date Created	Operation
HQ_Comp_MLAG_Type	F3-LA-HQ	MLAG	2025-10-27 07:25:20	View Delete
HQ_Comp_IP_Clan_Type	F3-WIN-BR	IP_Clan	2025-10-29 05:52:39	View Delete

General Icons

Close Icon

Each pop-up window has a close icon. To close a pop-up window, click the close icon.

System Backup

Backup

DB File Name

AmpCon Ver

Create Backup Config

Backup Name *

test

Encrypt Key *

test-key

AmpCon Version *

2.3.0/2.3.0-dev-f9ee4afc52

Cancel

Apply

Download Icon

Some pages have the **Download** icon. Click the icon to download data.

PicOS FSOS

Import Actions

View Import Details

Update Supported FSOS Sw

Sysname	SN/Service Tag
S3400C	CG2408279857N00009
FS	G15A31UQ000144
FS	G15A33S00228A
Switch	CG2412161022N00027
FS	G15KALJC040988
FS	G15L77C00066A
FS	G18U7A7000421

Batch Import

Download Template

JSON Template

Upload File

Drag and drop a file here or Choose File (Join File)

Cancel

Apply

Filter Icon

Some columns have the filter icon. To set the displayed information, click the icon, enter keywords, and then click **Search**. To clear the filter condition, click **Reset**.

Sysname	SN/Service Tag	Model	Version	Status	VFIN IP	Mgmt IP	Operation
PICOS	G139LV000417	S5890-32C	4.6.0E	Imported	10.1.1.38	10.1.1.44.29	UnitLog SSH Device Log Configuration Config View Lifecycle Actions
PICOS	G139LV001308	S5890-32C	4.6.0E	Imported	10.1.1.346	10.1.1.44.48	UnitLog SSH Device Log Configuration Config View Lifecycle Actions
PICOS	HWCG2206274998N00006	ac5812-24e	4.6.0E	Imported	10.1.1.042	10.1.1.0.60	UnitLog SSH Device Log Configuration Config View Lifecycle Actions

Help Icon

Some page names, buttons, or field names are marked with the question icons. Hover your mouse over question icons to check notes.

Port Profile

+ Port Profile

Name

Default

Port Profile Application

Management

Local User

Login Banner

On S3000 series switches, uppercase letters are not supported.

Username

admin2

User Level *

super-user

Password *

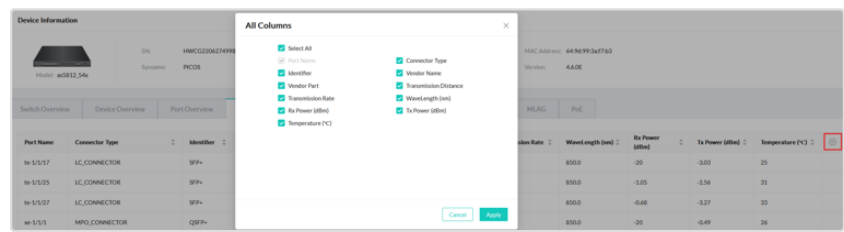
Confirm Password *

Cancel

Apply

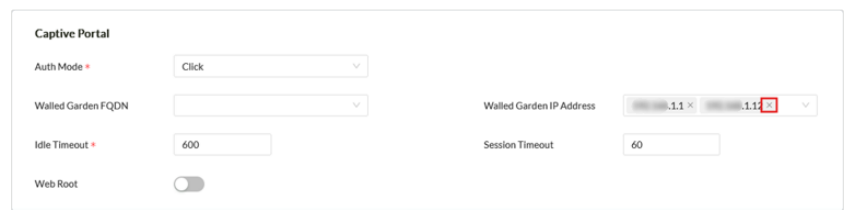
Metric Selection Icon

Some pages have the metric selection icon. Click the icon to specify the metrics to be displayed.



Remove Icon

After you add one or multiple items to a field or a search box, to remove an item, click the remove icon.



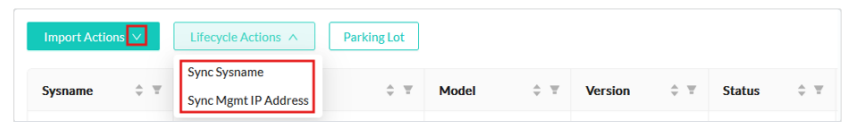
Sort Icon

Some columns have the sort icons. Click the up arrow icon to display data in ascending order. Click the down arrow icon to display data in descending order.

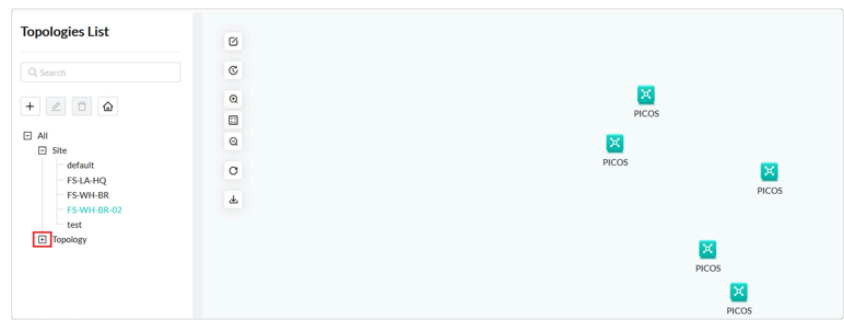
❏	Last Time	Switch SN	Type	Message	Count	Operation
❏	2025-10-28 02:1443	G15712N000045	Error	Found interface: ne-1/1/31 on switch G15712N000045 not discarded increased	1022	Mark as Read
❏	2025-10-29 01:5324	G1590V0001308	Error	Found interface: ne-1/1/2 on switch G1590V0001308 not discarded increased	4	Mark as Read
❏	2025-10-29 01:5325	G1590V000417	Error	Found interface: ne-1/1/31 on switch G1590V000417 not discarded increased	1024	Mark as Read
❏	2025-10-29 01:5325	G1590V0001308	Error	Found interface: ne-1/1/31 on switch G1590V0001308 not discarded increased	1024	Mark as Read

Unfold Icon

Some buttons have the unfold icon similar to a down arrow. Hover your mouse over or click the unfold icon, and then you can see sub buttons.



Some pages have the unfold icon shown as a plus icon surrounded by a square. Click the unfold icon to view sub elements.



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, maintain, and monitor wireless networks more efficiently. See the following child topics:

- [Wireless Overview](#)
- [Deploying Wireless Networks](#)
- [Maintaining Wireless Networks](#)
- [Monitoring Wireless Networks](#)

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](#).

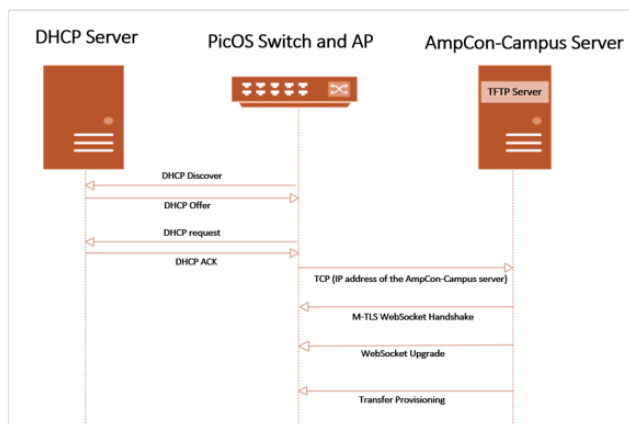
Highlights

Zero-Touch Provisioning

AmpCon-Campus uses Zero-Touch Provisioning (ZTP) to simplify wireless network deployment. After you plug in and power on an AP, the AP initiates a connection request to AmpCon-Campus through the IP address of the AmpCon-Campus server.

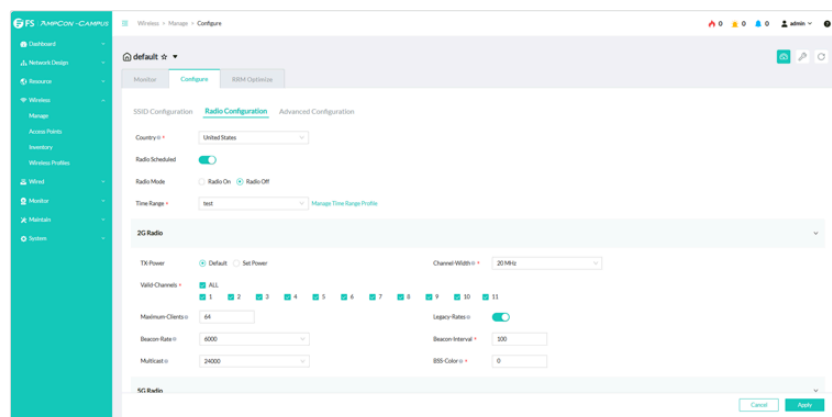
After the connection is established, the AP retrieves its configurations without manual intervention.

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)**

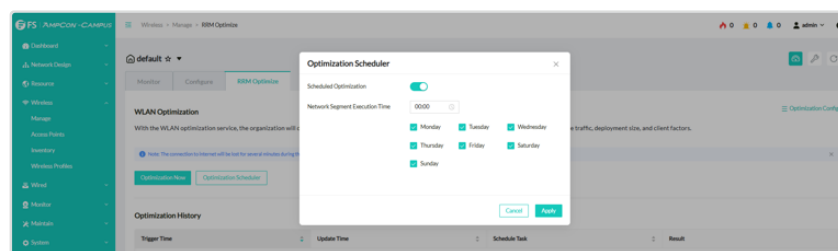
- AmpCon-Campus supports enabling or disabling specific SSIDs or radio bands based on a time schedule, optimizing energy consumption and network usage. For example, you can enable employee Wi-Fi during work hours and disable guest Wi-Fi at night.

- **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.
- Protected Management Frames (PMF) can be protected and encrypted to defend against wireless attacks.
- Captive Portal can be customized to simplify public Wi-Fi deployment.

Intelligent RF and Network Optimization

AmpCon-Campus supports intelligent Radio Frequency (RF) and network optimization:



- **Autonomous radio resource management**

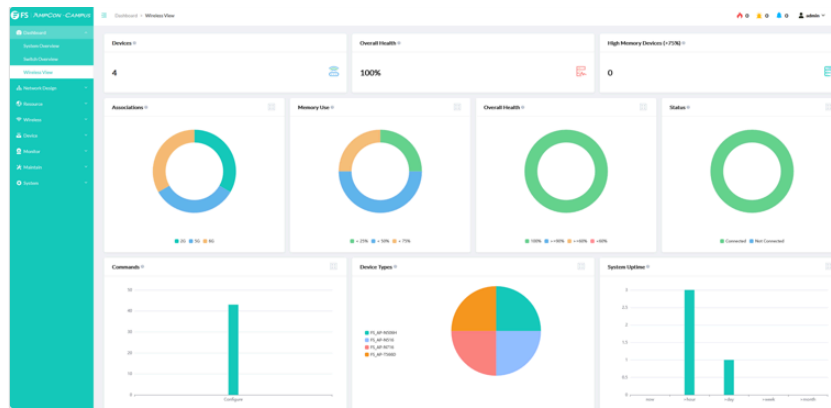
- Supports scheduled and immediate network optimization. You can customize optimization rules for different scenarios.
- Supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to optimize channels automatically and reduce interference.
- Supports IEEE 802.11k, 802.11r, and 802.11v 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

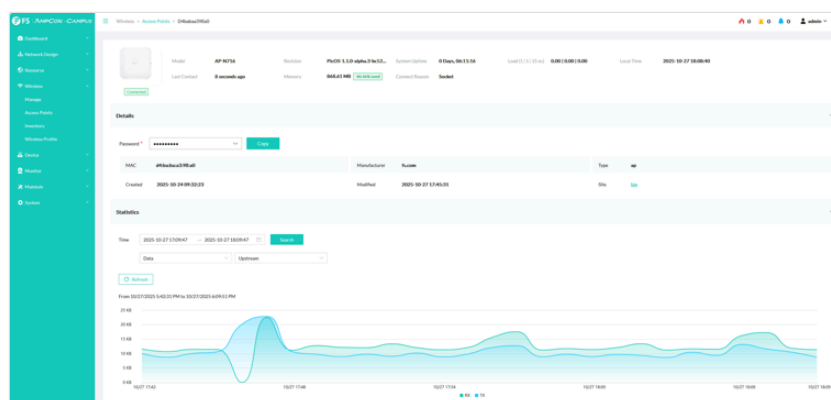
- Supports real-time monitoring of AP status, SSID configurations, and network performance.
- Supports bulk configurations and firmware upgrade, simplifying large-scale network management.
- Supports unified management of stations (STAs), providing insights into the entire connection process of each 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 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

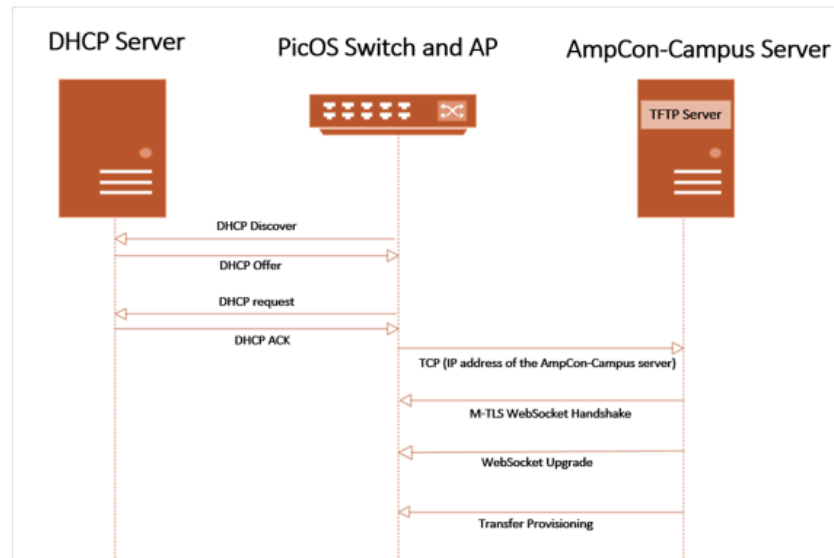
ZTP is an automated technology for deploying and configuring network devices. If a large number of APs need to be deployed, ZTP can reduce labor costs and improve deployment efficiency. ZTP enables fast, accurate, and reliable device deployment.

AmpCon-Campus uses ZTP to simplify AP deployment. After you plug in and power on an AP, the AP initiates a connection request to AmpCon-Campus through the IP address of the AmpCon-Campus server. After the connection is established, the AP retrieves configurations from AmpCon-Campus without manual intervention.

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 site-level wireless configurations for the site to which the AP belongs.
- d. Onboard APs to AmpCon-Campus, and assign APs to a 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 pre-defined configurations and pushes JSON configuration blocks to 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
 - 2.4GHz Radio Band
 - 5GHz Radio Band
 - 6GHz 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. 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)

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.

2.4GHz 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.

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 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

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 wireless network, you need to add access points (APs) to AmpCon-Campus and then configure the APs in the AmpCon-Campus UI.

After you plug in and power on the added APs, the Zero-Touch Provisioning (ZTP) process will start. The APs will connect with AmpCon-Campus and retrieve configurations without manual intervention.

[Prerequisites](#)

[Procedure](#)

[1. Adding APs](#)

[2. Configuring APs](#)

[3. Plug In and Power On APs](#)

[What to Do Next](#)

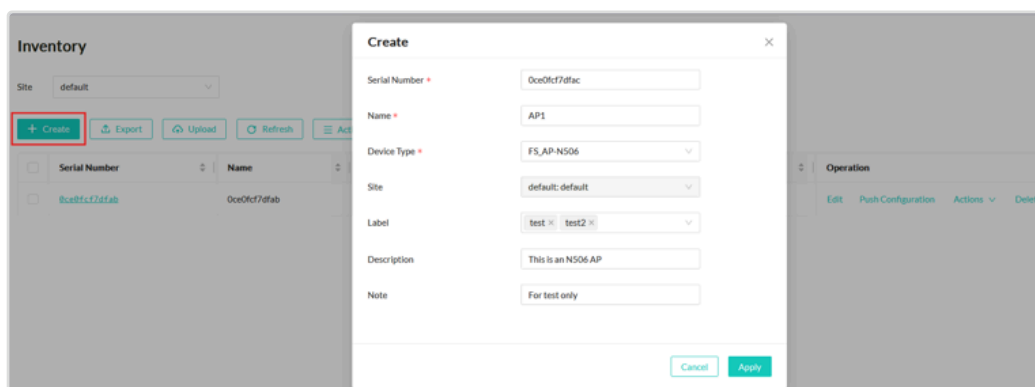
Prerequisites

Ensure that the prerequisite tasks described in [Prerequisites](#) have been completed. Or else, the wireless network deployment will fail.

Procedure

1. Adding APs

To deploy a wireless network, you need to add APs to AmpCon-Campus first. You can add APs one by one or import APs in batches. For more information, see [Adding APs](#).



2. Configuring APs

After you add APs to AmpCon-Campus, you must add SSID configurations for these APs. For more information, see [Adding SSID Configurations](#).

Monitor							
Configure							
SSM Optimize							
SSID Configuration							
Radio Configuration							
Advanced Configuration							
+ Create New SSID							
SSID Name	Security	Radio	VLAN	AP Label	WLAN Status	Operation	
esp104	WPA2-PSK	2G.5G	-		☒	Edit Copy Delete	
new_esp104	WPA2-PSK	2G.5G	-		☒	Edit Copy Delete	

The following configurations are not mandatory, and you can configure if needed:

- AmpCon-Campus provides some default values for radio configurations and advanced configurations. Check these default configuration values to see whether they meet your needs. If not, you must change the configurations as needed. For more information, see [Adding Radio Configurations](#) and [Adding Advanced Configurations](#).

NOTE

Wireless regulatory requirements vary by country. In the radio configurations, ensure that the country code is consistent with the location of the AP.

- When you add SSID or radio configurations, you can use pre-defined wireless profiles, such as RADIUS servers, Multiple Pre-Shared Key (MPSK), Captive Portal, and the enabling time ranges for radio and SSIDs. For more information, see [Adding Wireless Profiles](#).

3. Plug In and Power On APs

Plug in and power on the added APs. Then, the ZTP process will start. Once completed, the wireless network is deployed, and the AP configurations will be pushed to the APs automatically.

What to Do Next

- After you deploy a wireless network, you can maintain the network as needed. For more information, see [Maintaining Wireless Networks](#).
- After you deploy wireless networks, you can monitor different wireless networks, APs, wireless devices (STAs), and wireless sites. For more information, see [Monitoring Wireless Networks](#).

Adding APs

To deploy a wireless network, you need to add APs to AmpCon-Campus first. You can add APs one by one or import APs in batches.

[Prerequisites](#)

[Adding One AP](#)

[Importing APs in Batches](#)

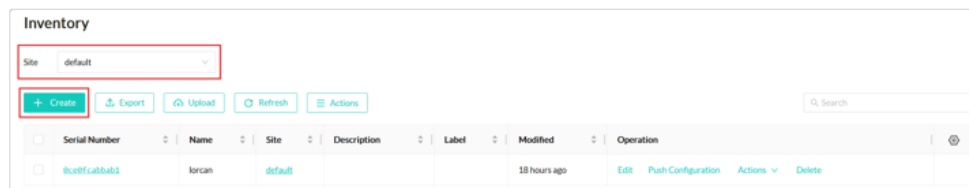
Prerequisites

Ensure that the prerequisite tasks described in [Prerequisites](#) have been completed. Or else, the wireless network deployment will fail.

Adding One AP

To add a single AP, follow these steps:

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list of the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
3. Click **+ Create**.



4. In the pop-up window, input the following information:

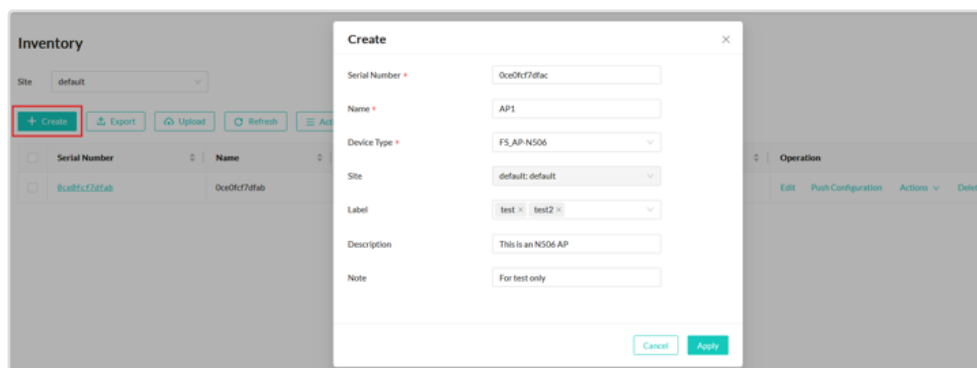


Table 1. AP Parameters

Parameter	Description
Serial Number	The serial number of the AP.
Name	The name of the AP.

Device Type	The type of the AP.
Site	Optional. The site to which the AP belongs. i NOTES • If you select a site in Step 2, the site value here is automatically entered and can't be modified. • If you select All Sites in Step 2, you can select a site here. ◦ By default, None is selected, which means the AP doesn't belong to any site. ◦ If None is selected, the Label drop-down list can't be selected.
Label	Optional. The label of the AP. i NOTES • You can select one or multiple AP labels. To add a new label, click the drop-down list, and then click + Create Label. • AP labels can be used in applying SSIDs. You can apply an SSID to APs with a specific label. • An AP label can contain only letters and numbers.
Description	Optional. The description of the label.
Note	Optional. The note of the label.

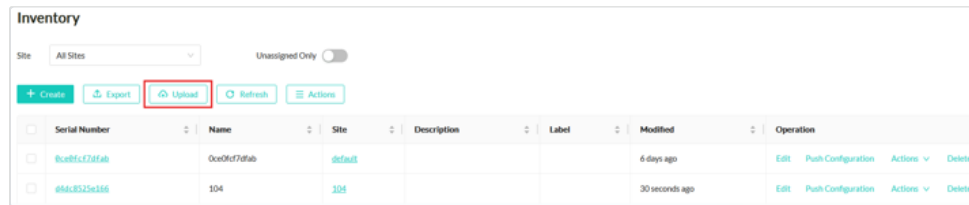
5. Click **Apply** to complete the AP addition.

After the AP is added successfully, you can see the AP in the AP list of the “Inventory” page.

Importing APs in Batches

To import multiple APs in batches, follow these steps:

1. In the **Site** drop-down list of the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
2. Click **Upload**.

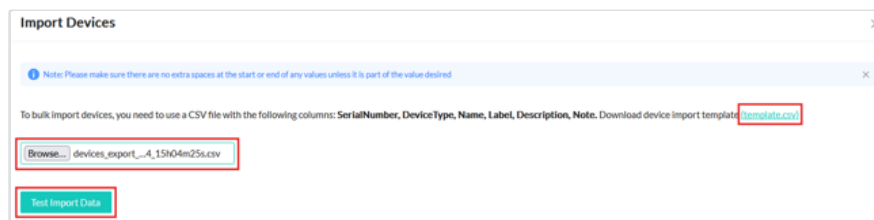


3. In the pop-up window, add APs as follows:
 - a. Click **template.csv** to download the template file.
 - b. Open the template file, and then enter serial number, type, name, label, description, and note of each AP in the template file.

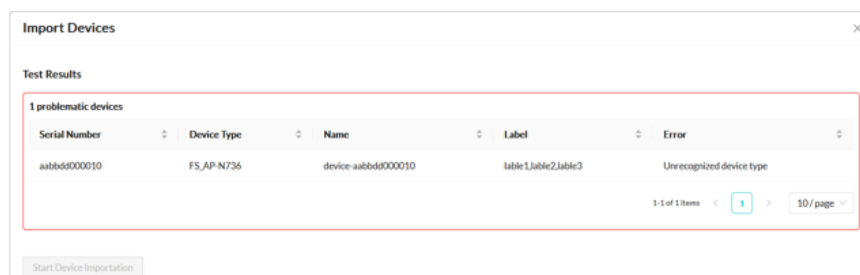
NOTE

Ensure that no extra spaces are added at the start or end of any values.

- c. Click **Browse**, and then select the updated template file.
- d. Click **Test Import Data**, and then check the test result.



If you see error information in the **Error** column, close the pop-up window, resolve issues in the template file, and then click **Upload** on the “Inventory” page to upload the template file again.



- e. Click **Start Device Importation**.

After the APs are imported successfully, you can see the APs in the AP list of the “Inventory” page.

Adding SSID Configurations

After you add access points (APs) to AmpCon-Campus, you must add SSID configurations for these APs.

[Guidelines](#)

[Procedure](#)

[Basic SSID Configurations](#)

[Authentication Configurations](#)

[Advanced Configurations](#)

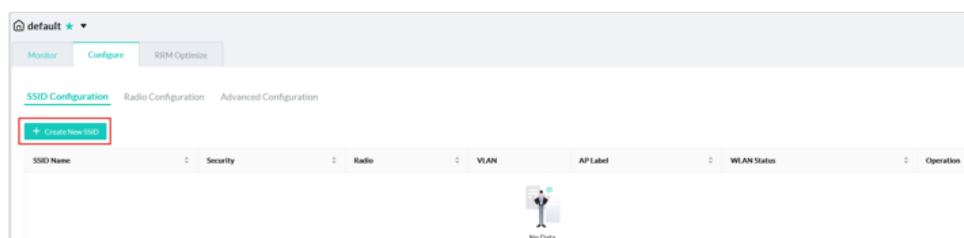
Guidelines

Compared with AmpCon-Campus 2.3.0, AmpCon-Campus 2.3.1 includes the following changes:

- The MPSK, Key Caching, and FT Roaming functions are not supported when APs operate in NAT (Router) mode. AmpCon-Campus 2.3.1 automatically disables MPSK, Key Caching, and FT Roaming when you enable AP Assign IP.
- Captive Portal and MPSK are mutually exclusive. AmpCon-Campus 2.3.1 automatically disables the other when you enable one.

Procedure

1. Click **Wireless > Manage** from the navigation bar, and then click the **Configure** tab.
2. In the **Site** drop-down list, select the site to which the APs belong.
3. Click the **SSID Configuration** sub-tab, and then click **+ Create New SSID**.



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

NOTES

- All the configuration parameters marked with asterisks must be configured. Other configuration parameters are not mandatory.
- Some configurations contain default values. You need to check whether these default values meet your needs.

Basic SSID Configurations

Table 1. Basic Configuration Parameters

Parameter	Description
SSID	The Service Set Identifier (SSID) that the Station (STA) connects to. The SSID is the logical name of a wireless network.
Wi-Fi Bands	The radio band to be enabled on the APs, 2G, 5G, or 6G. You can enable one or multiple radio bands.
Schedule Switch-on	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. For more information, see Configuring Time Ranges. 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 radio, see Adding Radio Configurations.
AP Label	The AP labels to associate with the SSID. You can apply the SSID to the APs with the selected labels in this site. NOTES • The labels displayed in the drop-down list are those labels created when you add APs. • If you don't see any labels in the drop-down list, it means that no labels are added to the APs, and thus you can't select labels. • If no labels are selected, the SSID will be applied to all the APs in this site.
VLAN	Toggle it on to enable the VLAN function. Then, enter a VLAN ID ranging from 1 to 4050. • If the function is disabled, STAs connected to LAN ports and APs will be in the same subnet segment. • If the function is enabled, you can configure VLAN ID for the SSID to make APs 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. Or else, the wireless network will not work. • Ensure that the uplink network also creates this VLAN and switch ports allow this VLAN to pass through. • This section is available only when you don't enable the AP Assign IP function.
AP Assign IP	Toggle it on to enable the AP Assign IP function, which makes APs work in NAT mode

	and acts as a gateway. Then, APs can assign IP addresses to connected STAs. NOTE This section is available only when you don't enable the VLAN function.
DHCP Service Name	The DHCP address pool used for APs to assign IP addresses to connected STAs. To add a DHCP address pool, click + Create New DHCP Service from the drop-down list. For more information, see DHCP Service. NOTE This field is available only when you enable the AP Assign IP function.

Authentication Configurations

You can select an authentication mode based on service requirements:

Table 2. SSID Authentication Modes

Mode	Description
Open	Commonly used for guest networks and works with Captive Portal. FS provides four types of built-in Captive Portal for immediate use.
Personal	Typically used in home, Small and Medium-sized Business (SMB), or hotel scenarios. FS AP now supports Multiple Pre-Shared Key (MPSK), allowing different terminals to connect with different passwords while maintaining L2 isolation.
Enterprise	Widely used in large corporate networks, where users authenticate with usernames and passwords for enhanced security. This mode requires a RADIUS server, but FS APs also offer built-in RADIUS function to meet

customer needs.

- If you select the **Open** mode, select the encryption protocol, **None**, **OWE**, or **OWE Transition**.

NOTES

- **None** means no encryption protocol is used.
- If **6G** is enabled in the **Wi-Fi Bands** section, you can't select **None**.
- If **OWE** or **OWE Transition** protocol is selected, Management Frame Protection (MFP) is forcibly enabled.

The screenshot shows the 'Authentication' settings page. At the top, there's a 'Security Level' section with three radio buttons: Enterprise (green), Personal (orange), and Open (red). The 'Open' button is selected. Below this is a 'Protocol' dropdown menu that is currently open, showing three options: 'None' (highlighted in green), 'OWE', and 'OWE-Transition'. To the left of the dropdown is a red asterisk icon. At the bottom left, there's an 'Advanced Settings' link with a right-pointing arrow.

- If you select the **Personal** mode, input the following information:

The screenshot shows the 'Authentication' settings page with the 'Personal' mode selected. The 'Security Level' section has three radio buttons: Enterprise (green), Personal (orange, selected), and Open (red). Below this, the 'Protocol' dropdown is set to 'WPA-PSK'. To the left of the dropdown is a red asterisk icon. Below the protocol is the 'IEEE80211W' dropdown, which is set to 'Required'. To the left of this dropdown is a red asterisk icon. To the right of the 'IEEE80211W' dropdown is the 'Key' field, which is currently empty and has a red asterisk icon. Below the 'Key' field is a password input field with a red asterisk icon. At the bottom left, there's an 'MPK' toggle switch that is turned on. Below the toggle is a dropdown menu set to 'test'. To the right of the dropdown is a 'Manage MPK Profile' link.

Table 3. Personal Mode Parameters

Parameter	Description
Protocol	Select the security protocol used for the APs, WPA-PSK , WPA2-PSK , PSK2-RADIUS , WPA-PSK/WPA2-PSK Personal Mixed , WPA3-SAE , or WPA2/WPA3 Transitional . NOTES • If PSK2-RADIUS is selected, APs can be integrated with an external RADIUS server to enable MPK. Different STAs can use different

	passwords for network access and can be assigned to distinct VLANs. For 6GHz SSIDs, you must select WPA3-SAE or WPA2/WPA3 Transitional as the security protocol.
IEEE80211W	Also called Management Frame Protection (MFP), which adds signing or encryption to 802.11 management frames. MFP helps to prevent forgery, tampering, and replay attacks, thereby mitigating common wireless Denial of Service (DoS) and disconnection vulnerabilities. Values are Disabled, Optional, Required. Disabled Completely disable 802.11w MFP. No matter whether STAs support MFP or not, no protection mechanism will be used. 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 MFP without enforcing client support. The STAs supporting MFP can use the protection mechanisms. The STAs that don't support MFP can still connect normally but can't use the management frame protection function. Required Enforces mandatory MFP. Only the STAs compliant with 802.11w are allowed to connect; the STAs without MFP support are denied access. In this way, all management frames can be protected.  NOTE

	If WPA3-SAE or WPA2/WPA3 Transitional protocol is selected, MFP is forcibly enabled.
Key	The password to connect to the SSID, which must contain 8 to 64 characters. NOTE You can connect to the SSID by using the Key value. The standard VLAN will be assigned.
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. For more information, see Configuring MPSK. NOTES • Different from PSK2-RADIUS, MPSK is built on APs and does not rely on any external RADIUS server. • After MPSK is enabled, you can still connect to the SSID by using the Key value above. In this case, the standard VLAN will be assigned. • If you connect to the SSID by using the Key value in the MPSK profile, the VLAN included in the MPSK profile will be assigned.

- If you select the **Enterprise** mode, input the following information:

Authentication

Security Level Enterprise Personal Open

Protocol WPA-Enterprise

IEEE80211W Required

Radius test [Manage Radius Profile](#)

Table 4. Enterprise Mode Parameters

Parameter	Description
Protocol	Select the security protocol used for the APs, WPA-Enterprise, WPA2-Enterprise, EAP-TLS, WPA-Enterprise-Mixed, WPA3-Enterprise, EAP-TLS, WPA3-192-Enterprise, EAP-TLS, or WPA3-Enterprise-Mixed. NOTES - If PSK2-RADIUS is selected, APs can be integrated with an external RADIUS server to enable MPSK. Different STAs can use different passwords for network access and can be assigned to distinct VLANs. - For 6GHz SSIDs, you must select WPA3-SAE or WPA2/WPA3 Transitional as the security protocol.
IEEE80211W	Also called Management Frame Protection (MFP), which adds signing or encryption to 802.11 management frames. MFP helps to prevent forgery, tampering, and replay attacks, thereby mitigating common wireless DoS and disconnection vulnerabilities. NOTE If WPA3-Enterprise EAP-TLS, WPA3-192-Enterprise EAP-TLS, or

	WPA3-Enterprise-Mixed protocol is selected, MFP is forcibly enabled.
RADIUS	The centralized authentication server. You can select the RADIUS server built on each AP, or you can select an external RADIUS server. To add an external RADIUS server, click + Create RADIUS Profile from the drop-down list. For more information, see Adding External RADIUS Servers.

Advanced Configurations

You can add more configurations as needed.

Create New SSID

Advanced Settings

Hidden SSID

Maximum Clients

64

Dtim-Period

2

Power Save

Unicast Conversion

Disassoc Low Ack

Wi-Fi Steering

Fils-Discovery-Interval

20

Isolate Clients

Broadcast Time

Proxy ARP

Roaming

Key-Caching

FT Roaming

Off

Rate Limit

Rate Limit

Access Control List

Access-Control-List

Cancel

Apply

Table 5. Advanced Parameters

Parameter	Description
Hidden SSID	Toggle it on to enable the Hidden SSID function, which will hide the SSID so that STAs can't detect the SSID.
Wi-Fi Steering	Toggle it on to enable the WIFI Steering function. WIFI Steering dynamically guides

	STAs to select the radio bands, optimizing network load and performance. NOTE After enabling this feature, ensure that Wi-Fi Steering is enabled and reasonable parameters are configured in the Wireless > Manage > Configure > Advanced Configuration tab. For more information, see Adding Advanced Configurations - Services.
Maximum Clients	The maximum number of client connections per Virtual Access Point (VAP). For example, if an SSID enables both the 2.4GHz and 5GHz radio and this parameter is set to 10, it means: • The maximum limit for the 2.4GHz radio is 10 clients. • The maximum limit for the 5GHz radio is also 10 clients. • The total maximum limit for this SSID is 20 clients.
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, STAs can discover APs faster in dense-channel environments like 6 GHz. The unit is Time Unit (TU). 1 TU equals to 1.024 ms.
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.

	• A lower value such as 1 or 2 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 such as 3, 4, or 5 saves power but increases latency. Higher values are more applicable to low-power scenarios, such as smart-home sensors.
Isolate Clients	Toggle it on to enable L2 isolation between STAs connected to the same SSID.
Power Save	Toggle it on to enable the power-saving mode. In the power-saving mode, STAs enter periodic sleep states, and wake up only during the AP-designated “awake window” to transmit or receive data. STAs 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 Broadcast Time function, which enables APs to include time information in its Beacon frames.
Unicast Conversion	Toggle it on to enable the conversion of broadcast and multicast data to unicast data, for fewer packet losses, lower power consumption, and smoother video streaming. However, duplicating the same contents into multiple unicast streams increases air interface overhead, which might slow down the entire network in high-density scenarios
Proxy ARP	Toggle it on to enable the Proxy ARP function. By using this function, APs will respond to ARP requests on behalf of STAs, reducing airtime and average latency. However, this function might not work in certain network environments.

Disassoc Low Ack	Toggle it on to enable APs to actively disconnect STAs with weak signals. If an AP fails to receive ACK confirmation from an STA for consecutive times, the AP will immediately force disconnect the STA to remove clients with extremely poor link quality.
Key-Caching	Toggle it on to enable Key-Caching. 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. Key-Caching allows faster re-authentication for roaming clients without re-executing a full authentication protocol.
FT Roaming	The protocol defined by IEEE 802.11r to enable seamless and low-latency roaming for STAs between APs within the same Mobility Domain (MD). Also called 802.11r roaming. Select one option: • Custom: Customizes FT Roaming configurations: ◦ Message Exchange: Select air or ds, which means pre-authenticated messages are exchanged over the air or distribution system. ◦ Generate PSK: Toggle it on to generate Fast BSS Transition (FT) responses locally for Pre-Shared Key (PSK) networks, and thus avoid the use of PMK-R1 push or pull from other APs within FT-PSK networks. ◦ Domain Identifier: The Mobility Domain identifier. The value must contain exactly 4 hexadecimal characters.

	• Auto: Uses pre-defined FT Roaming configurations. ◦ Message Exchange: Pre-authenticated messages are exchanged over the air or distribution system. ◦ Generate PSK: Fast BSS Transition (FT) responses are generated locally for Pre-Shared Key (PSK) networks. ◦ Domain Identifier: A random value (4 hexadecimal characters) is generated as the Mobility Domain identifier. • Off: Disables FT Roaming.
Rate Limit	Toggle it on to enable clients to limit uplink and downlink rates. Once enabled, you must enter the following information: • Ingress Rate: The ingress rate to which STAs will be limited. The unit is Mbps. • Egress Rate: The egress rate to which STAs will be limited. The unit is Mbps.  NOTE The value 0 means unlimited speed.
Access-Control-List	Toggle it on to add the MAC addresses of STAs allowed or denied to access to this SSID. Input the following information: • Mode: Select Allow or Deny. • MAC Address: The MAC addresses of STAs allowed or denied to access to this SSID.  NOTES • After you input a MAC address, press Enter. • You can input one or multiple MAC addresses.

In the **Captive Portal** section, you can configure whether to enable Captive Portal and select the authentication mode. In the **Auth Mode** drop-down list, select one mode.

Table 6. Captive Portal Auth Modes

Mode	Description
None	Disables Captive Portal.
Click	Connects to the wireless network without entering a password. After a portal authentication page pops up, users can click to access the Internet.
RADIUS	Connects to the SSID through credentials stored in an external RADIUS server.
Credentials	The account and password based authentication method. Users can directly store credentials on APs without deploying a RADIUS server.
UAM	Connects to the SSID through credentials stored in an external Universal Access Method (UAM) server.

- If you select **Click**, input the following information:

The screenshot shows the 'Captive Portal' configuration page. The 'Auth Mode' is set to 'Click'. The 'Walled Garden FQDN' field contains 'test.com' and 'test2.com'. The 'Walled Garden IP Address' is set to '192.168.1.1'. The 'Idle Timeout' is set to '600' and the 'Session Timeout' is set to '6553'. The 'Web Root' is set to 'test' and is enabled with a toggle switch. A link 'Manage Web Root Profile' is visible next to the Web Root field.

Table 7. Click Mode Parameters

Parameter	Description
Walled Garden FQDN	The Fully Qualified Domain Name (FQDN) of the Walled Garden. NOTES • After you input an FQDN, press Enter. • You can input one or multiple FQDNs.

Walled Garden IP Address	The IPv4 address of the Walled Garden.  NOTES • After you input an IP address, press Enter. • You can input one or multiple IP addresses.
Idle Timeout	If an STA has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The default value is 600 seconds. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of a client connection, measured in seconds. When the time is exceeded, STAs will be forcibly disconnected. The value must be greater than 0 and less than 65535.  NOTE The value 0 means that sessions will not have timeout.
Web Root	Toggle it on to customize the Captive Portal authentication page. Then, select a Web Root profile. Each Web Root profile defines a Captive Portal authentication page. To add a Web Root profile, click + Create Web Root Profile from the drop-down list. For more information, see Configuring Captive Portal.

- If you select **RADIUS**, input the following information:

Captive Portal

Auth Mode *
Radius

Walled Garden FQDN
test.com ✕

Walled Garden IP Address
192.168.1.1 ✕

Idle Timeout *
600

Session Timeout
6553

Auth Server *
192.168.1.10

Auth Secret *

Auth Port *
1812

Acct Server
192.168.1.11

Acct Secret

Acct Port
1813

Acct Interval
60

Web Root
☒ test2

Manage Web Root Profile

Table 8. RADIUS Mode Parameters

Parameter	Description
Walled Garden FQDN	The FQDN of the Walled Garden. NOTES - After you input an FQDN, press Enter. - You can input one or multiple FQDNs.
Walled Garden IP Address	The IPv4 address of the Walled Garden. NOTES - After you input an IP address, press Enter. - You can input one or multiple IP addresses.
Idle Timeout	If an STA has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The default value is 600. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of client connections, measured in seconds. When the time is exceeded, STAs will be forcibly disconnected.

	The value must be greater than 0 and less than 65535.  NOTE The value 0 means that sessions will not have timeout.
Auth Server	The IPv4 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 IPv4 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.
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.
Web Root	Toggle it on to customize the Captive Portal authentication page. Then, select a Web Root profile. Each Web Root profile defines a Captive Portal authentication page. To add a Web Root profile, click + Create Web Root Profile from the drop-down list.

For more information, see [Configuring Captive Portal](#).

- If you select **Credentials**, input the following information:

The screenshot shows the 'Captive Portal' configuration page. The 'Auth Mode' is set to 'Credentials'. Below this, there are fields for 'Walled Garden FQDN', 'Walled Garden IP Address', 'Idle Timeout' (set to 600), and 'Session Timeout'. A '+ Credentials' button is present. Below the button is a table with columns 'Username', 'Password', and 'Operation'. The table contains one entry: 'admin' for both Username and Password, with a 'Delete' link in the Operation column. At the bottom right of the table, it says 'Total 1 items' and '1 / 10 / page'. There is also a 'Web Root' toggle switch at the bottom left. 'Cancel' and 'Apply' buttons are at the bottom right.

Table 9. Credentials Mode Parameters

Parameter	Description
Walled Garden FQDN	The FQDN of the Walled Garden. NOTES • After you input an FQDN, press Enter. • You can input one or multiple FQDNs.
Walled Garden IP Address	The IPv4 address of the Walled Garden. NOTES • After you input an IP address, press Enter. • You can input one or multiple IP addresses.
Idle Timeout	If an STA has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The default value is 600 seconds. The value must be greater than 0 and less than 65535.

Session Timeout	The maximum duration of client connections, measured in seconds. When the time is exceeded, STAs will be forcibly disconnected. The value must be greater than 0 and less than 65535. NOTE The value 0 means that sessions will not have timeout.
Credentials	Click + Credentials to add a user and password to access the SSID.
Web Root	Toggle it on to customize the Captive Portal authentication page. Then, select a Web Root profile. Each Web Root profile defines a Captive Portal authentication page. To add a Web Root profile, click + Create Web Root Profile from the drop-down list. For more information, see Configuring Captive Portal.

- If you select **UAM**, input the following information:

Captive Portal

Auth Mode *
Walled Garden FQDN
Idle Timeout *
UAM Server *
UAM Port *
NAS ID *
MAC Format *
Auth Server *
Auth Port *
Acct Server
Acct Port

UAM
test.com
600
https://YOUR-LOGIN-ADDRESS.YOURS
3990
TestLab
aabbccddeeff
192.168.1.10
1812
192.168.1.11
1813

Walled Garden IP Address
Session Timeout
UAM Secret *
NAS MAC
Auth Secret *
Acct Secret
Acct Interval

192.168.1.1
222

60

Cancel Apply

Table 10. UAM Mode Parameters

Parameter	Description
Walled Garden FQDN	The FQDN of the Walled Garden. NOTES - After you input an FQDN, press Enter. - You can input one or multiple FQDNs.
Walled Garden IP Address	The IPv4 address of the Walled Garden. NOTES - After you input an IP address, press Enter. - You can input one or multiple IP addresses.
Idle Timeout	If an STA has no network activity for a specified time (in seconds), the wireless network will be automatically disconnected. The default value is 600 seconds. The value must be greater than 0 and less than 65535.
Session Timeout	The maximum duration of client connection, in seconds. When the time is exceeded, STAs will be forcibly disconnected. The value must be greater than 0 and less than 65535. NOTE The value 0 means that sessions will not have timeout.
UAM Server	The IPv4 address of the UAM server.
UAM Secret	The secret of the UAM server.
UAM Port	The port used to connect with the UAM server.

	The value must be greater than 1023 and less than 65535.
NAS ID	The identifier to distinguish this wireless network identity in the external Portal system. Based on the Network Access Server (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 the consistent with the expected format of the external Portal system. Otherwise, authentication requests might be rejected or fail to match policies.
Auth Server	The IPv4 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 IPv4 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.
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.

Optional: Adding Wireless Profiles

On the “Wireless Profiles” page, you can configure some profiles, such as RADIUS servers, Multiple Pre-Shared Key (MPSK), Captive Portal, and the enabling time ranges for SSIDs or radio.

Then, when you add SSID or radio configurations, you can use these pre-defined profiles.

NOTE

The configurations in a wireless profile can be pushed to APs only when the following prerequisites are met:

- The profile is used in SSID or radio configurations.
- The SSID or radio configurations are [pushed to APs](#).

[Guidelines](#)

[Procedure](#)

[Configuring RADIUS Servers](#)

[Adding Built-in RADIUS Servers](#)

[Adding External RADIUS Servers](#)

[Configuring MPSK](#)

[Configuring Captive Portal](#)

[Configuring Time Ranges](#)

Guidelines

Compared with AmpCon-Campus 2.3.0, AmpCon-Campus 2.3.1 includes the following changes:

- When you configure MPSK profiles:
 - To make labels clearer, the **Name** column is updated to **Profile Name** and the **Create** button is updated to **Create Access Credential** in the **MPSK** tab of the “Wireless Profiles” page. Besides, the **Name** field is changed to **Profile Name** in the **Create MPSK Profile** and **Edit MPSK Profile** pop-up windows.
 - To facilitate user management in wireless Multi-Dwelling Unit (MDU) scenarios, a new **Name** field is added to the **Create Access Credential** and **Edit Access Credential** pop-up windows. Meanwhile, the valid **VLAN ID** range is adjusted to 2-4048.
- When you enter a MAC address, AmpCon-Campus will automatically insert a colon after every two characters, optimizing MAC address input convenience.

Procedure

1. Click **Wireless > Wireless Profiles** from the navigation bar.
2. In the **Site** drop-down list, select a site to which the APs belong.

3. Add the following configurations as needed:

NOTES

- All the configuration parameters marked with asterisks in each profile must be configured. Other configuration parameters are not mandatory.
- AmpCon-Campus provides some default configurations in each profile. Check whether these default configurations meet your needs.

Configuring RADIUS Servers

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.

Add built-in RADIUS servers or external RADIUS servers as needed.

NOTE

These configurations can be used when you configure an SSID. In the SSID configuration process, you can select the RADIUS server used as the centralized authentication server, and customize the Captive Portal display for the RADIUS authentication mode.

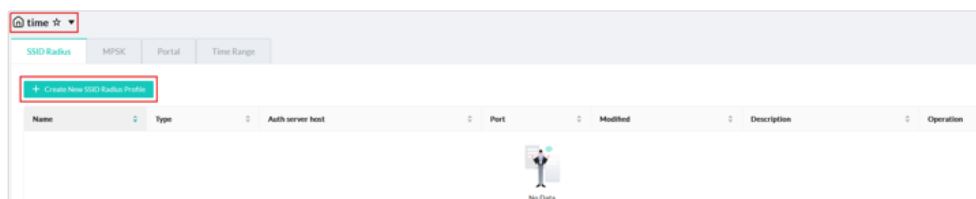
For more information, see [Adding SSID Configurations](#).

Adding Built-in RADIUS Servers

You can add one or multiple built-in RADIUS servers by creating RADIUS profiles.

To add the built-in RADIUS server on each AP, follow these steps:

1. In the **SSID RADIUS** tab, click **+ Create New SSID Radius Profile**.



2. In the pop-up window, input the following information:

Table 1. Built-in RADIUS Parameters

Parameter	Description
Name	The name of the RADIUS profile.
Mode	Select Local , which means adding the built-in RADIUS server on each AP.
Description	The description of the RADIUS profile.

3. Click **+ User**.

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

Table 2. User Parameters

Parameter	Description
User Name	The username used to connect to an SSID.
Password	The password of the user. Valid values contain 8 to 63 characters.

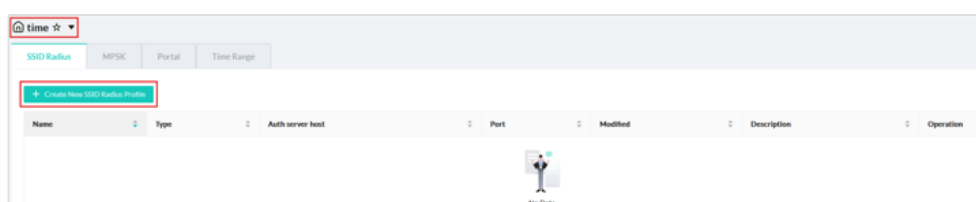
5. Click **Apply** to complete the RADIUS Profile creation.

Adding External RADIUS Servers

You can add one or multiple external RADIUS servers by creating RADIUS profiles.

To add an external RADIUS server, follow these steps:

1. In the **SSID RADIUS** tab, click **+ Create New SSID RADIUS Profile**.



2. In the pop-up window, input the following information:

Create SSID Radius Profile

Name *

test

Mode *

External

Description

Authentication Host *

192.168.178.192

Authentication Port *

1812

Authentication Secret *

MAC Filter

☒

Enable Accounting

☒

Accounting Host *

192.168.178.192

Accounting Port *

1813

Accounting Secret *

Enable Dynamic Auth

☒

Dynamic Auth Host *

192.168.178.192

Dynamic Auth Port *

1814

Dynamic Auth Secret *

NAS Identifier

test

Chargeable User ID

☒

Cancel

Apply

Table 3. External RADIUS Parameters

Parameter	Description
Name	The name of the RADIUS profile.
Mode	Select External , which means adding an external RADIUS server.
Description	The description of the RADIUS profile.
Authentication Host	The IPv4 address of the RADIUS Authentication server.
Authentication Port	The port used to access the RADIUS Authentication server.
Authentication Secret	The security secret used to access the RADIUS Authentication server.
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 black or white list management.
Enable Accounting	Toggle it on to enable a RADIUS Accounting server. Once enabled, configure the following parameters: • Accounting Host: The IPv4 address of the RADIUS Accounting server. • Accounting Port: The port used to access the RADIUS Accounting server. • Accounting Secret: The security secret used to access the RADIUS Accounting server.
Enable Dynamic Auth	Toggle it on to enable the RADIUS Dynamic Auth server. Once enabled, configure the following parameters: • Dynamic Auth Host: The IPv4 address of the Dynamic Auth server. • Dynamic Auth Port: The port used to access the Dynamic Auth server. • Dynamic Auth Secret: The security secret used to access the Dynamic Auth server.
NAS Identifier	The attribute identifying 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's anonymous but uniquely identifies users. It's designed for cross-domain authentication, accounting, and auditing scenarios to ensure traceability and billability while concealing real identities.
---------------------------	---

3. Click **Apply** to complete the configuration.

Configuring MPSK

Multiple Pre-Shared Keys (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:

- **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.

To configure MPSK, follow these steps:

NOTE

These configurations can be used when you configure an SSID. In the SSID configuration process, you can enable the MPSK function to configure multiple PSKs for the same SSID.

For more information, see [Authentication Configurations](#).

1. Click the **MPSK** tab, and then click **+ Create New MPSK Profile**.
2. In the pop-up window, enter the name and description of the MPSK profile.
3. Click **+ Create**. In the pop-up window, input the following information, and then click **Apply**.

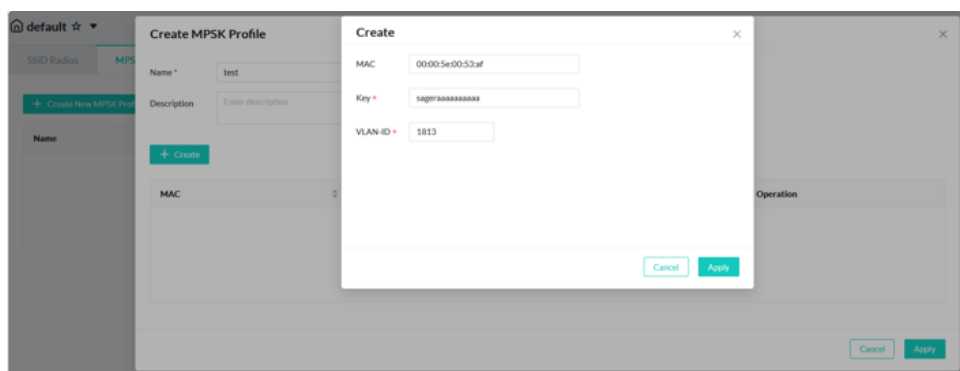


Table 4. MPSK Parameters

Parameter	Description
MAC	The MAC address of the STA connected to the SSID.
Key	The key used by the STA to connect to the SSID. The value must contain 8 to 63 characters.
VLAN ID	The VLAN ID assigned to the STA. Valid values range from 1 to 4050. NOTE Do not enter the native VLAN ID of the uplink switch. Or else, the wireless network will not work.

4. Click **Apply** to complete the configuration.

Configuring Captive Portal

You can configure the Captive Portal display, such as display of authentication, billing, and brand.

NOTE

These configurations can be used when you configure an SSID. In the SSID configuration process, you can enable Captive Portal, select the authentication mode, and then select a Web Root profile.

For more information, see [Adding SSID Configurations](#).

To configure Captive Portal, add a Web Root profile. Follow these steps:

1. Click the **Portal** tab, and then click **+ Create New Portal Webroot Profile**.
2. In the pop-up window, input the following information:

Table 5. Portal Configuration Parameters

Parameter	Description
Name	The name of the Web Root profile.
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 the external RADIUS server. • Credentials: An account and password based authentication method. Users can directly store credentials in the AP without deploying a RADIUS server.
Description	The description of the Web Root profile.
Background	The background color of Captive Portal. Click Color, and then select a color or enter a color value.
Upload Logo	The logo of Captive Portal.

	Click Upload Logo, and then upload a logo file. NOTE Only PNG, JPG, JPEG, and GIF files can be uploaded. The uploaded file needs to be less than 10 KB.
Welcome Message	The welcome message of Captive Portal.
Terms of Service	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.
Copyright	The copyright displayed in Captive Portal.

3. Click **Apply** to complete the configuration.

Configuring Time Ranges

You can create multiple weekly-based time ranges.

NOTE

These configurations can be used when you configure an SSID or a radio. In the SSID or radio configuration process, you can use these time ranges to schedule the enabling time for different SSIDs or radio.

For more information, see [Adding SSID Configurations](#) and [Adding Radio Configurations](#).

To create a time range, follow these steps:

1. Click the **Time Range** tab, click **+ Create New Time Range Profile**.
2. In the pop-up window, enter the name and description of the profile.
3. Select the day and time range as needed.

Create Time Range Profile

Name *

test

Description

Enter description

☒ Monday

08:00

18:00

0

2

4

6

8

10

12

14

16

18

20

22

24

☒ Tuesday

08:00

18:00

0

2

4

6

8

10

12

14

16

18

20

22

24

☒ Wednesday

08:00

18:00

0

2

4

6

8

10

12

14

16

18

20

22

24

☒ Thursday

08:00

18:00

0

2

4

6

8

10

12

14

16

18

20

22

24

☒ Friday

08:00

18:00

0

2

4

6

8

10

12

14

16

18

20

22

24

☐ Saturday

0

2

4

6

8

10

12

14

16

18

20

22

24

☐ Sunday

0

2

4

6

8

10

12

14

16

18

20

22

24

Cancel

Apply

4. Click **Apply**.

Optional: Adding Radio Configurations

After you add access points (APs) to AmpCon-Campus, you can customize radio configurations for these APs.

Procedure

Basic Configurations

2G, 5G, and 6G Radio Configurations

Procedure

1. Click **Wireless > Manage** from the navigation bar, and then click the **Configure** tab.
2. In the **Site** drop-down list, select a site to which the APs belong.
3. Click the **Radio Configuration** sub-tab, input the following information, and then click **Apply**.

i NOTES

- Some radio configurations have default values. Check whether these default configurations meet your needs.
- All the configuration parameters marked with asterisks must be configured. Other configuration parameters are not mandatory.

Basic Configurations

The screenshot displays the 'Radio Configuration' tab within a management console. The interface is divided into three main sections: 'SSID Configuration', 'Radio Configuration' (which is the active tab), and 'Advanced Configuration'. The 'Radio Configuration' section contains several fields: 'Country' (set to 'United States'), 'Radio Scheduled' (a toggle switch that is turned on), 'Radio Mode' (radio buttons for 'Radio On' and 'Radio Off', with 'Radio Off' selected), and 'Time Range' (set to 'test' with a link to 'Manage Time Range Profile'). Below this, the '2G Radio' section is visible, showing 'TX-Power' (set to 'Set Power' at 1 dBm), 'Channel-Width' (set to 20 MHz), 'Valid-Channels' (a row of checkboxes for channels 1 through 11, all of which are checked), 'Maximum-Clients' (set to 64), 'Beacon-Rate' (set to 6000), 'Multicast' (set to 24000), 'Legacy-Rates' (a toggle switch that is turned on), 'Beacon-Interval' (set to 100), and 'BSS-Color' (set to 0). The 'Country' field is highlighted with a red rectangle.

Table 1. Basic Radio Parameters

Parameter	Description
Country	The country where the APs are deployed. i

	NOTE Wireless regulatory requirements vary by country. You must select the corresponding country code based on the location of the AP.
Radio Scheduled	Toggle it on to set time-based policies for enabling or disabling radio. i 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 Basic SSID Configurations.
Radio Mode	Select Radio On or Radio Off to enable or disable radio. i 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. For more information, see Time Range. i NOTE This section is available only when you toggle Radio Scheduled on.

2G, 5G, and 6G Radio Configurations

i NOTE You need to unfold the 2G Radio, 5G Radio, or 6G Radio section to see related configuration parameters.
--

2G Radio

TX-Power

☐ Default
☒ Set Power

1

dBm

Channel-Width

20 MHz

Valid-Channels

☒ ALL

☒ 1
☒ 2
☒ 3
☒ 4
☒ 5
☒ 6
☒ 7
☒ 8
☒ 9
☒ 10
☒ 11

Maximum-Clients

64

Legacy-Rates

☒

Beacon-Rate

6000

Beacon-Interval

100

Multicast

24000

BSS-Color

0

5G Radio

6G Radio

Table 2. 2G, 5G, and 6G Radio Parameters

Parameter	Description
TX-Power	The transmission power of the radio. Select Default or Set Power. • Default: APs will work at the maximum transmission power that the located country allows. • Set Power: APs will work at a customized transmission power. You can customize the transmission power within the range of 0 to 30. The unit is dBm. NOTE The maximum power limit might vary depending on the country code.
Channel-Width	The channel width that the radio uses. • 2G Radio: Supports 20 MHz and 40 MHz. • 5G Radio: Supports 20 MHz, 40 MHz, 80 MHz, and 160 MHz. • 6G Radio: Supports 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz. NOTE Some APs might not support 160 MHz and 320 MHz. For these APs, after the Channel-Width configuration is pushed, the channel bandwidth might fall back to

	the maximum bandwidth that these APs support.
Valid-Channels	The AP channel set that can dynamically adjust based on channel bandwidth changes. APs will select the optimal channel for communication within the chosen channel set according to the Radio Frequency (RF) environment.
Maximum-Clients	The maximum number of stations (STAs) allowed to connect to the current radio. If this threshold is exceeded, STAs can't connect to the radio. NOTE This value is accumulative for all attached Virtual Access Point (VAP) interfaces. For example, if the Maximum-Clients value of the 2G radio is 64 and the 2G radio is bound with multiple SSIDs, at most 64 STAs 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 2G radio configurations.
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 default value is 100. 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 The value must be greater than 14 and less than 65535.
Multicast	The multicast rate that the Basic Service Set (BSS) uses, measured in Kbps.
BSS-Color	Whether to enable BSS Coloring on the Physical Layer (PHY). Values 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 radio to use Dynamic Frequency Selection (DFS) channels. Once enabled, APs will automatically detect radar channels and switch channels upon detection.  NOTE This section is available only for 5G radio configurations.

Optional: Adding Advanced Configurations

After you add access points (APs) to AmpCon-Campus, you can add advanced configurations for these APs.

[Guidelines](#)

[Procedure](#)

[System](#)

[IP Address](#)

[DHCP Service](#)

[Manage Ethernet Ports](#)

[Services](#)

Guidelines

Compared with AmpCon-Campus 2.3.0, AmpCon-Campus 2.3.1 includes the following changes:

- Each service can't use the HTTP port 0. AmpCon-Campus 2.3.1 adds the port restriction.
- Different services (SSH, HTTP, Log, and RTTY) can't use the same port number. AmpCon-Campus 2.3.1 adds the port restriction.

Procedure

1. Click **Wireless > Manage** from the navigation bar, and then click the **Configure** tab.
2. In the **Site** drop-down list, select a site to which the APs belong.
3. Click the **Advanced Configuration** sub-tab, input the following information, and then click **Apply**.

NOTES

- You need to click each section to unfold configuration parameters.
- Some advanced configurations have default values. Check whether these default configurations meet your needs.
- All the configuration parameters marked with asterisks must be configured. Other configuration parameters are not mandatory.

System

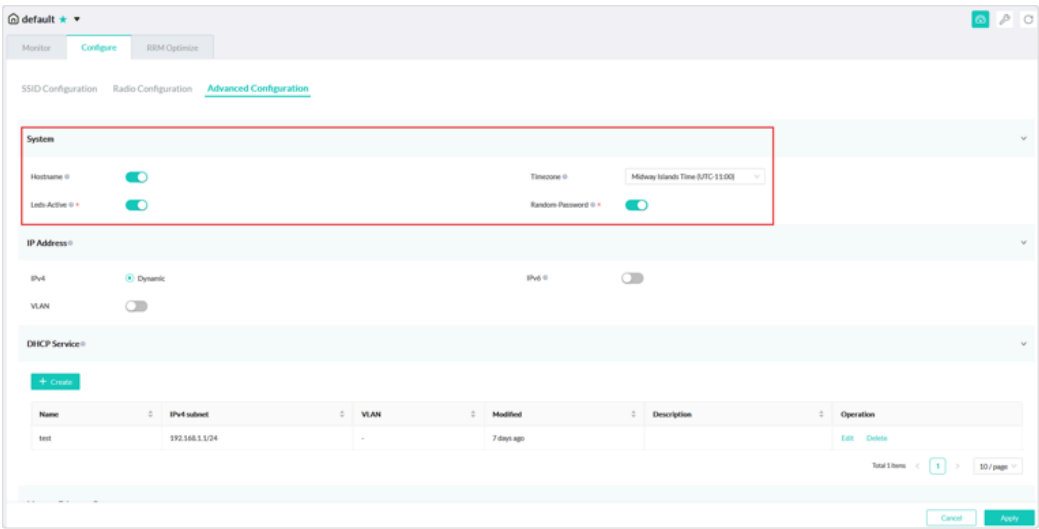


Table 1. System Parameters

Parameter	Description
Hostname	Toggle it on to push AP names specified on the “Inventory” page to each AP.
Timezone	The time zone of the APs. None means the UTC-0 time zone.
Leds-Active	Toggle it off to force all LEDs to shut down.
Random-Password	Toggle it on to generate a random root password for each AP and notify AmpCon-Campus.

IP Address

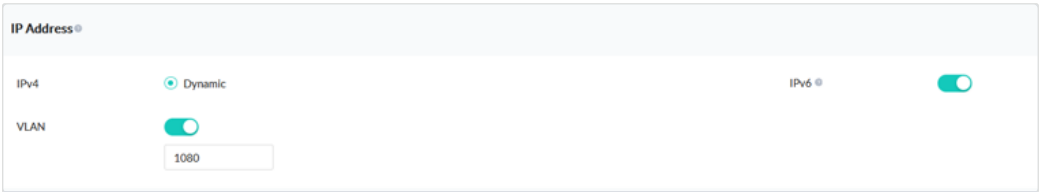


Table 2. IP Parameters

Parameter	Description
IPv4	You can select only Dynamic , which means that each AP acts as a DHCP client and successfully obtains an IP address from the DHCP server.

IPv6	Toggle it on to obtain an IPv6 address for each AP 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 1 to 4050. NOTES - Do not enter the native VLAN ID of the uplink switch. Or else, the wireless network will not work. - Ensure that switches permit the VLAN.

DHCP Service

If you enable the NAT mode (non-Bridge mode) on each AP, the APs in this mode can assign IP addresses to STAs. To make the NAT mode work, you need to configure an IP address pool (DHCP pool).

In the **DHCP Service** section, add a DHCP pool by clicking **+ Create**.

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

The screenshot shows the 'Create' dialog box for a DHCP pool. The background interface shows the 'DHCP Service' section with a '+ Create' button highlighted. The 'Create' dialog box contains the following fields:

- Name:** test
- Description:** (empty)
- IPv4 Subnet:** 192.168.1.0/24
- IPv4 Gateway:** 192.168.1.1
- DHCPv4 Lease First:** 1
- DHCPv4 Lease Count:** 128
- DHCPv4 Lease Time:** 6h
- IPv6 Subnet:** 2001:db8:10::/64
- IPv6 Gateway:** 2001:db8:10::1/64
- DHCPv6 Profile Size:** 64
- DHCPv6 Mode:** hybrid
- DHCPv6 Filter Profile:** 0/0
- VLAN ID:** 1123

Table 3. DHCP Parameters

Parameter	Description
Name	The name of the DHCP pool.
Description	The description of the DHCP pool.

Subnet	The IPv4 subnet address, such as 192.168.1.1/24.  NOTE Do not use loopback addresses.
Gateway	The IPv4 address of the gateway, such as 192.168.1.1.  NOTE Do not use any loopback address.
Lease-First	The starting IP address of this DHCP pool.
Lease-Count	The number of IP addresses that can be assigned in the DHCP pool.
Lease-Time	The DHCP lease time, which means the duration a client can use an IP address after obtaining it from a DHCP server. When the lease time expires, the client must send a renewal request to the DHCP server. See the following example lease time: • 6d2h5m: Means 6 days, 2 hours, and 5 minutes. • 6h: Means 6 hours. • 2h5m: Means 2 hours and 5 minutes. • 5m: Means 5 minutes.
IPv6	Toggle it on to enable IPv6 address pools. Once enabled, configure the following parameters: • Subnet: The IPv6 subnet address. • Gateway: The IPv6 address of the gateway. • Prefix-Size: The prefix length of IPv6 addresses. • DHCPv6: Toggle it on to enable each AP as an IPv6 DHCP server. Once enabled, configure the following parameters:

	◦ Mode: The operation mode of the IPv6 DHCP server. ▪ stateless: The system will announce only router advertisements, without offering stateful DHCPv6 services. ▪ stateful: The emitted router advertisements will instruct clients to obtain a lease through DHCPv6. ▪ hybrid: Clients can freely choose to self-assign a random IPv6 address through Stateless Address Autoconfiguration (SLAAC), to request an IPv6 address through DHCPv6, or both. For compatibility with different clients, it is recommended to use the hybrid mode. ◦ Announce-DNS: Overrides the DNS server to announce in DHCPv6 and RA messages. By default, an AP will announce its local interface address as the DNS server, acting as proxy for downstream clients. By specifying a non-empty list of IPv6 addresses here, this default behavior can be overridden. After you enter an IPv6 address, remember to press Enter. ◦ Filter-Prefix: The specific downstream prefix or a number of downstream prefix ranges to announce in DHCPv6 and RA messages. By default, all prefixes configured on a given downstream interface are advertised. By specifying an IPv6 prefix in Classless Inter-Domain Routing (CIDR) notation here, only prefixes covered by this CIDR are selected.
VLAN ID	The VLAN ID for subnets on APs.  NOTES

- If **VLAN** is not configured in the [IP Address](#) section, do not configure **VLAN ID** here.
- If **VLAN** is configured in the [IP Address](#) section, enter the same VLAN value here.

Manage Ethernet Ports

To configure physical ports of APs, click **+ Create** in the **Manage Ethernet Ports** section.

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

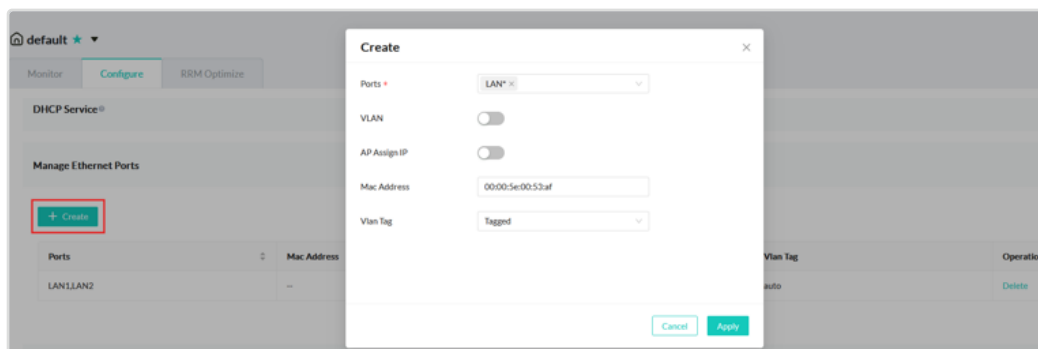


Table 4. Ethernet Port Configuration Parameters

Parameter	Description
Ports	The physical Ethernet ports to be configured. You can select one or multiple ports. NOTES • Only LAN ports are supported. • Uplink ports cannot be configured. • LAN* represents all LAN ports. • Some APs have only 1 LAN port, and thus configuring other LAN ports might not work.
VLAN	Toggle it on to enable the VLAN function for Ethernet ports. Then, enter a VLAN ID ranging from 1 to 4050. • After you disable the function, STAs and APs will be in the same VLAN.

	- After you enable the function, you can configure a VLAN ID for the selected Ethernet ports to make the AP work in Bridge mode. Then, the Ethernet ports will operate on an independent VLAN.  NOTES - This section is available only when you don't enable the AP Assign IP function. - Do not enter the native VLAN ID of the uplink switch. Or else, the wireless network will not work. - Ensure that the uplink network also creates this VLAN and that switch ports allow this VLAN to pass through.
AP Assign IP	Toggle it on to make APs work in NAT mode and act as a gateway. Then, APs can assign IP addresses to connected STAs.  NOTE This section is available only when you don't enable the VLAN function.
DHCP Service Name	The required DHCP address pool for the SSID. To add a DHCP address pool, click + Create New DHCP Service from the drop-down list. For more information, see DHCP Service.  NOTE This field is available only when you enable the AP Assign IP function.
Mac Address	The MAC address of the terminal device connected through the selected Ethernet ports.
Vlan Tag	Select whether to tag VLAN frames: Tagged: The ports carry tagged VLAN frames. Data in multiple VLANs can be

transmitted simultaneously through the same port. Uplink switches or APs distinguish different services based on VLAN tags.

- **Un-tagged:** The ports carry untagged VLAN frames.
- **Auto:** If VLAN is enabled, frames will be tagged. Otherwise, frames remain untagged.

NOTE

You are not suggested to select **Auto**. Or else, the network connectivity might be impacted.

Services

In the **Services** section, you can configure different services used by wireless networks.

Table 5. Service Parameters

Parameter	Description
SSH	Toggle it on to enable the SSH remote access. Then, configure the following parameters: • Port: The SSH port used to connect to an AP through SSH. • Password-Authentication: Toggle it on to enable the password authentication. If the password authentication is not enabled, the SSH key authentication will be used. In this

	case, you must enter a private SSH key in the authorized-keys field.
HTTP	Toggle it on to enable the HTTP web interface access. Then, configure the HTTP port in the HTTP-Port field. Once enabled, you can access an AP web interface by entering its IP address in a browser.
MDNS	Toggle it on to enable the Multicast DNS (MDNS) service. Once enabled, STAs 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. However, 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.

	If the service is enabled, configure the following parameters: • Describe: The name of the AP. The default value is auto, which means the AP name on the “Inventory” page will be broadcast. • Location: The location of the AP. The default value is auto, which means the site of the AP will be broadcast as the AP location.
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 IPv4 address of the upstream NTP server. You can input one or multiple NTP servers. After you enter one FQDN or IPv4 address, remember to press Enter. • 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 STAs.
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 IP 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 0 to 65535. • Proto: 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.
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. • Token: The token of the RTTY server. Then, you can access APs through a web interface for remote debugging, configuration, and maintenance without physical access. For more information, see Accessing APs.
Wifi 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 dBm) to allow connections. 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. Valid values range from 0 to 100. • Required-Roam-Snr: The minimum required signal level (in dBm) that triggers roaming evaluation. If the SNR of an associated terminal is below this threshold, an attempt is made to roam the client to a better AP. Valid values range from 0 to 100. • load-kick-threshold: The channel utilization threshold (in percentage) for client kickouts. If the radio air interface utilization exceeds this threshold, the system will kick out the clients with fewer kickouts and weaker signals. Valid values range from 0 to 100.
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 can't access the Internet (online). Select one of or both the following actions: ◦ wifi: All Wi-Fi on the AP will be disabled when the AP can't access the Internet (offline). ◦ leds: The AP LEDs will blink rapidly when the AP can't 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 can't check whether application-layer services work well.

- Ensure that ICMP packets are allowed. Or else, the ping command will fail even though APs can access the Internet.
- You can input one or multiple hosts.
- After you input an FQDN or IP address, remember to press **Enter**.
- **Download-Hosts:** The FQDN or IP address of the hosts for HTTP or HTTPS downloading tests.
 - After you input an FQDN or IP address, remember to press **Enter**.
 - You can input one or multiple hosts.
 - 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 allowed failure count threshold. before an AP considers it as 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.

i 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.

Maintaining Wireless Networks

After you deploy a wireless network, you can maintain the network as needed.

See the following child topics:

- [Positioning APs](#)
- [Rebooting APs](#)
- [Editing Configurations of an AP](#)
- [Pushing Configurations to APs](#)
- [Upgrading AP Firmware](#)
- [Capturing Remote Port Packets](#)
- [Optimizing Wireless Networks](#)
- [Restoring to Factory Settings](#)
- [Exporting, Deleting, and Moving APs](#)
- [Accessing APs](#)
- [Advanced CLI Configurations](#)

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 goes offline, 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.

Procedure

[From the Inventory Page](#)

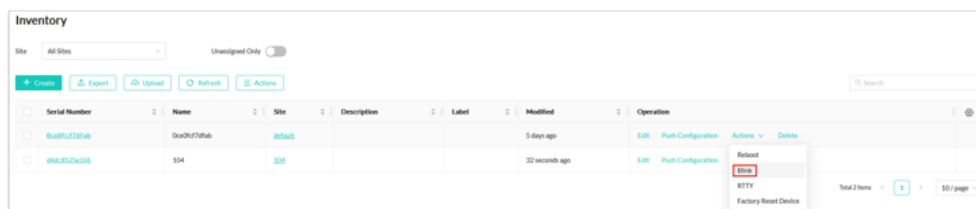
[From the AP Detail Page](#)

Procedure

To make an AP blink, use the “Inventory” page or the AP detail page.

From the Inventory Page

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, click **Actions**, and then click **Blink**.



Then, the LED of the AP will keep blinking for 30 seconds, and thus you can locate the AP easily.

From the AP Detail Page

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click its serial number.
4. On the AP detail page, click **Actions**, and then click **Blink**.



Then, the LED of the AP will keep blinking for 30 seconds, and thus you can locate the AP easily.

Rebooting APs

By using AmpCon-Campus, you can reboot one access point (AP) or all the APs in a site.

[Rebooting One AP](#)

[From the Inventory Page](#)

[From the AP Detail Page](#)

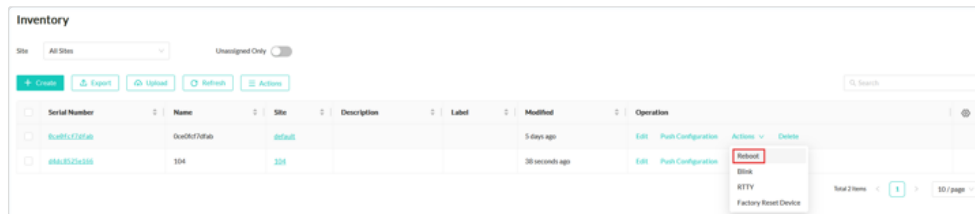
[Rebooting All APs](#)

Rebooting One AP

To reboot an AP, use the “Inventory” page or the AP detail page.

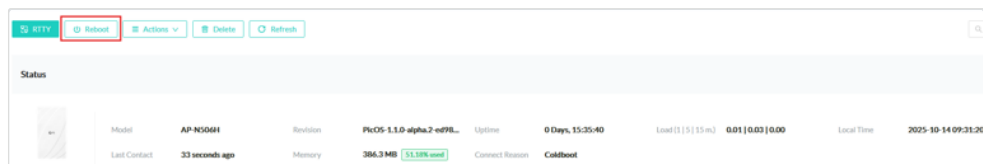
From the Inventory Page

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, click **Actions**, and then click **Reboot**.



From the AP Detail Page

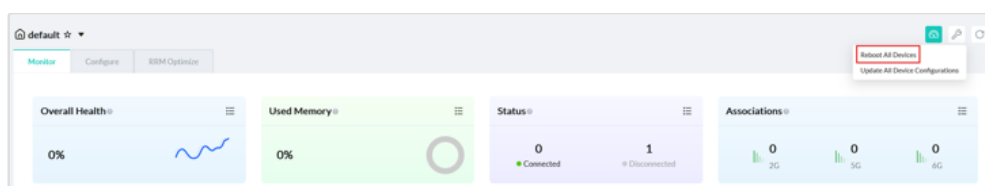
1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click its serial number.
4. On the AP detail page, click **Reboot**.



Rebooting All APs

To reboot all the APs in a site, follow these steps:

1. Click **Wireless > Manage** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the APs belong.
3. Click the setting icon in the top right, and then click **Reboot All Devices**.



Editing Configurations of an AP

After a wireless network is deployed, you can edit configurations of each AP in the wireless network.

Procedure

[Basic Configurations](#)

[Radio Configurations](#)

[Notes](#)

[What to Do Next](#)

Procedure

To edit configurations of an AP, follow these steps:

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list of the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click **Edit**.
4. Optional: To check the current configurations on the AP, click the **Computed Config** tab in the pop-up window.
5. Click other tabs in the pop-up window, edit basic, radio, or note configurations as needed, and then click **Apply**.

Basic Configurations

Click the **Main** tab, and then modify the site, AP name, description, device type, or label as needed.

NOTE

If you don't see any labels in the **Label** drop-down list, it means that no labels are added to the APs, and thus you can't select labels.

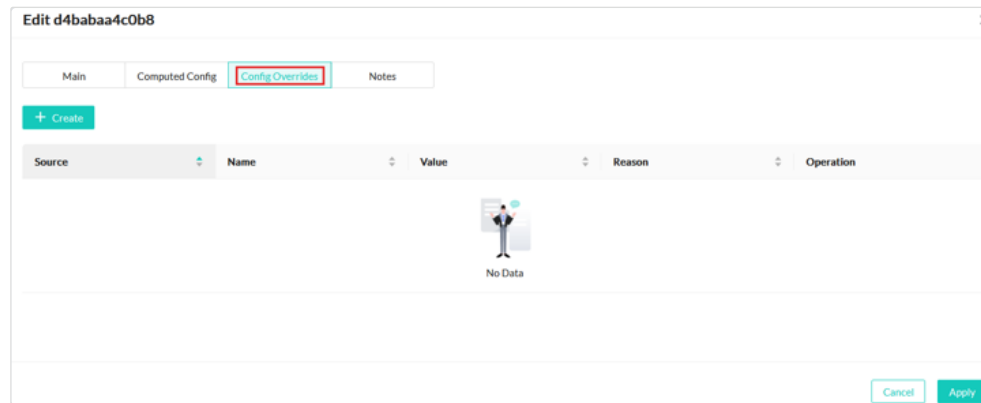
The screenshot shows a web interface window titled "Edit d4dc8525e166". It has four tabs: "Main" (selected), "Computed Config", "Config Overrides", and "Notes". The "Main" tab contains the following fields:

Field	Value
Serial Number *	d4dc8525e166
Name *	104
Description	
Device Type *	FS_AP-N506H
Site	104
Label	

At the bottom right of the window are "Cancel" and "Apply" buttons.

Radio Configurations

1. Click the **Config Overrides** tab.



2. Click **+ Create**, and then input the configurations as follows:

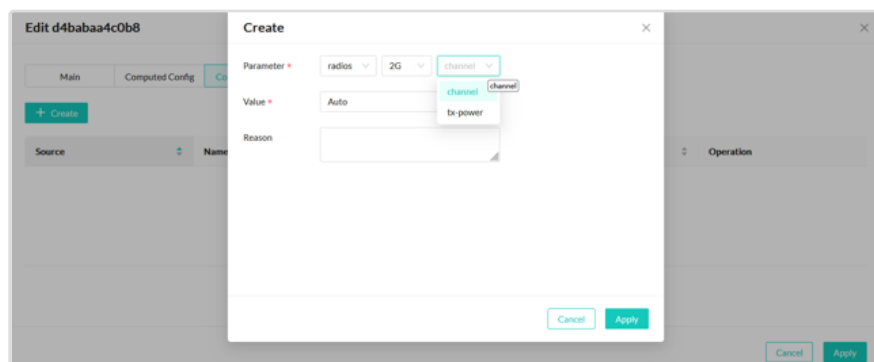
a. In the **Parameter** section, select **2G**, **5G**, or **6G**, and then select **channel** or **tx-power**.

i NOTES

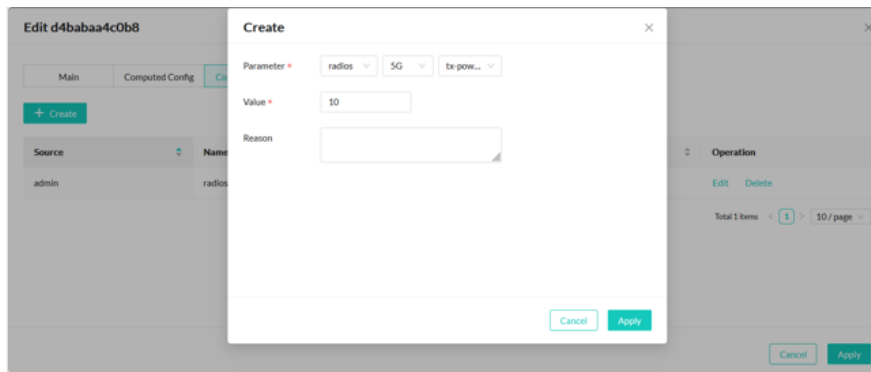
- Each AP radio band supports only one channel or one TX Power.
- The channel value and AP transmission power value must be based on regulations of the country where the AP is deployed.

If you select **channel**, select the channel value in the **Value** drop-down list. You can select a specific value or select **Auto**.

Auto means allocating the optimal channel for the wireless network by dynamically detecting environmental interference and channel load.



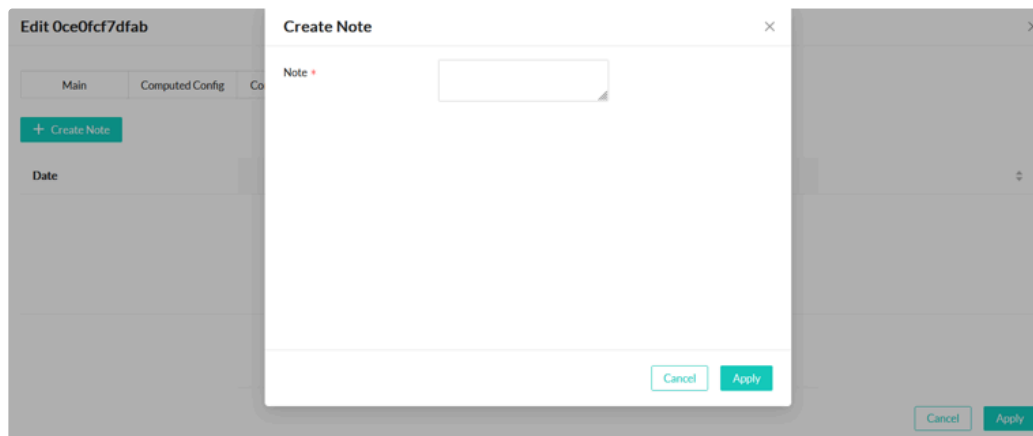
If you select **tx-power**, enter the AP transmission power value in the **Value** drop-down list.



- b. Optional: In the **Reason** field, input the reason of the configuration.
- c. Click **Apply** to complete the radio configuration.

Notes

1. Click the **Notes** tab.
2. Click **+ Create Note**.
3. Input a note in the **Note** field.



4. Click **Apply** to complete the note addition.

What to Do Next

After you edit an AP, you must push the updated configurations to the AP manually. For more information, see [Pushing Configurations to One AP](#).

Pushing Configurations to APs

When you deploy APs through AmpCon-Campus, configurations can be pushed to APs automatically after you plug in and power on APs. When you assign an AP from one site to another, the new site configuration is also pushed to the AP automatically.

After APs are deployed through AmpCon-Campus, you might need to [edit configurations of an AP](#) or update [SSID](#), [radio](#), or [advanced](#) configurations of a site. In these cases, you must manually push configurations to APs.

You can push configurations to a single AP or to all the APs in a site.

[Pushing to One AP](#)

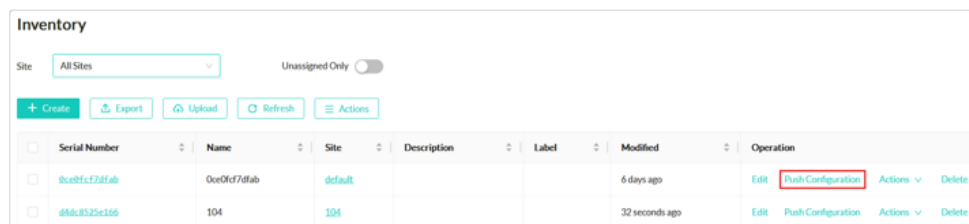
[Pushing to All APs in a Site](#)

[Checking Pushing Results](#)

Pushing to One AP

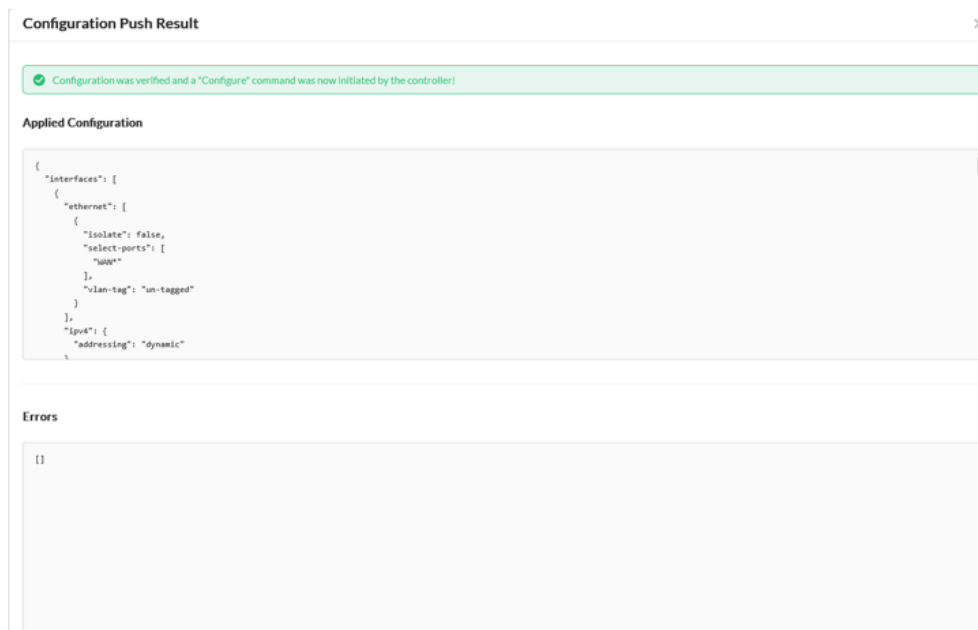
After you edit an AP, you must manually push configurations to the AP. Follow these steps:

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list of the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
3. On the “Inventory” page, locate the AP, and click **Push Configuration**.
4. In the pop-up window, click **Yes**.



	Serial Number	Name	Site	Description	Label	Modified	Operation
☐	0ce8fc72dfab	0ce8fc72dfab	default			6 days ago	Edit Push Configuration Actions ▾ Delete
☐	d8db0522e166	104	104			32 seconds ago	Edit Push Configuration Actions ▾ Delete

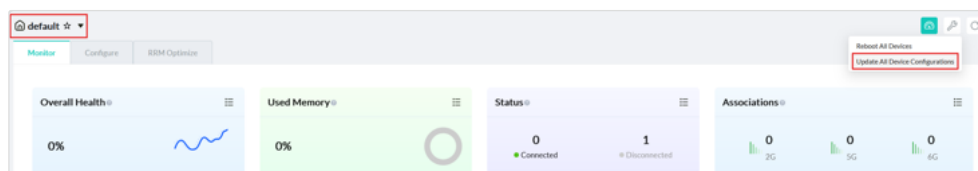
Then, the configurations will be pushed to the AP.



Pushing to All APs in a Site

After you update SSID, radio, or advanced configurations in a site, you must manually push configurations to all the APs in the site. Follow these steps:

1. Click **Wireless > Manage** from the navigation bar.
2. In the **Site** drop-down list, select the site to which you want to push configurations.
3. Click the setting icon in the top right, and then click **Update All Device Configuration**.



Then, the configurations will be pushed to all the APs in the site.

Checking Pushing Results

1. On the "Inventory" page, locate the AP, and then click its serial number.
2. On the AP detail page, scroll down to the **Commands** tab, locate the **Configure** command, and check whether the **Status** is displayed as **Completed**.

Commands						
Health Checks Logs Crash Logs Reboot Logs						
Time Start Time End Time						
Refresh						
Submitted	Command	Status	Executed	Completed	Error Code	Operation
4 minutes ago	Configure	Pending	-	-	0	Delete View
7 days ago	Configure	Completed	7 days ago	7 days ago	0	Delete View
7 days ago	Configure	Completed	7 days ago	7 days ago	0	Delete View
7 days ago	Configure	Completed	7 days ago	7 days ago	0	Delete View
7 days ago	Configure	Completed	7 days ago	7 days ago	0	Delete View
7 days ago	Configure	Completed	7 days ago	7 days ago	0	Delete View

If not, click **View** to check for error details.

Configure - 2025-09-17 15:22:39

Preview

```
{ 3 Items
  "error": 1
  > "rejected": [ ... ] 1 Item
  "text": "Rejects"
}
```

Commands

Health C

Custom Time-Frame

Start

Refresh

Submitted

1 hour ago

1 hour ago

1 hour ago

1 hour ago

1 hour ago

5 hours ago

5 hours ago

Configure

Configure

Configure

Configure

Configure

Configure

Failed

Failed

Failed

Failed

Failed

Failed

1 hour ago

1 hour ago

1 hour ago

1 hour ago

1 hour ago

5 hours ago

5 hours ago

5 hours ago

5 hours ago

5 hours ago

5 hours ago

1

1

1

1

1

1

Delete

Delete

Delete

Delete

Delete

Delete

View

View

View

View

View

View

Upgrading AP Firmware

For the access points (APs) managed by AmpCon-Campus, you can upgrade their firmware one by one or in batches. In addition, you can upgrade AP firmware immediately or at a scheduled date and time.

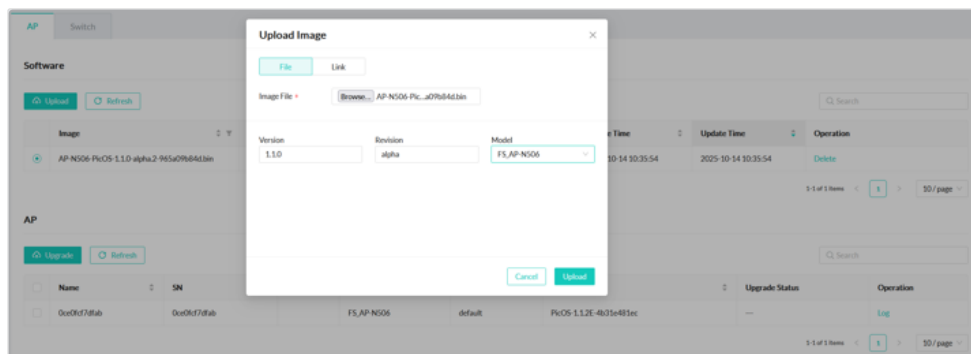
Procedure

1. Uploading AP Images
2. Upgrading APs

Procedure

1. Uploading AP Images

1. Click **Resource > Upgrade Management** from the navigation bar.
2. In the **Software** section of the **AP** tab, click **Upload**.
3. In the pop-up window, click **File**, and then input the following information:
 - a. Click **Browse**, and select a local AP image file.
 - b. In the **Version** field, enter the version of the AP image, such as **11.0**.
 - c. In the **Revision** field, enter the revision of the AP image, such as **alpha.3**.
 - d. In the **Model** drop-down list, select the AP model to which the AP image is applicable.



NOTE

Currently, the **Link** tab is not supported.

4. Click **Upload**.

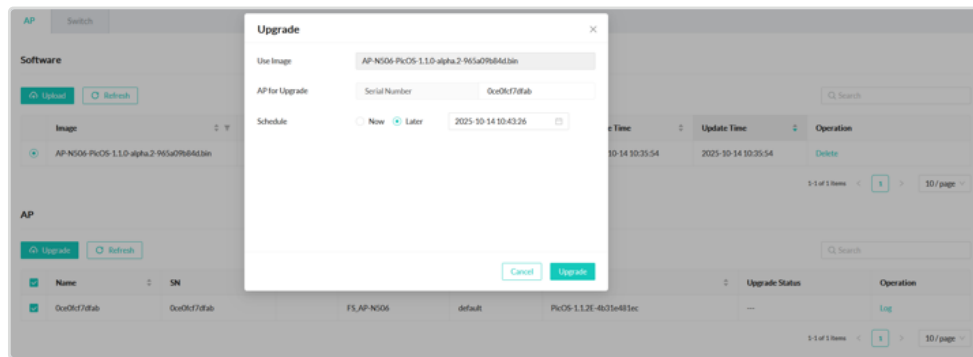
2. Upgrading APs

1. In the **Software** section of the **AP** tab, select the AP image to which you want to upgrade.

NOTE

Ensure that the AP image matches the model of APs to be upgraded. Or else, you might see no matching APs in the **AP** section.

2. In the **AP** section of the **AP** tab, select one or multiple APs.
3. Click **Upgrade**.
4. In the pop-up window, select the time to run the upgrade task.
 - If you select **Now**, the upgrade task will be run immediately.
 - If you select **Later**, select a specific time in the time box. Then, the upgrade task will be run at the selected time.



5. Check whether the upgrade is successful by locating the AP and then clicking **Log** in the **Operation** column.

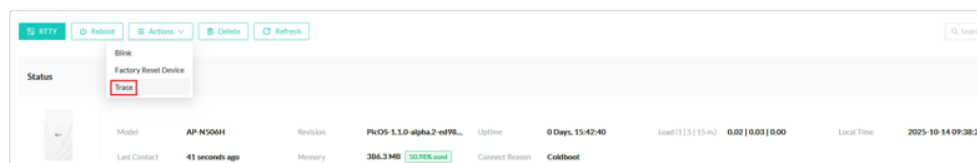
Capturing Remote Port Packets

By using AmpCon-Campus, you can capture remote packets from target ports of access points (APs) for rapid troubleshooting.

Procedure

To capture remote packets from target ports of an AP, follow these steps:

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click its serial number.
4. On the AP detail page, click **Actions**, and then click **Trace**.



5. In the pop-up window, input the following information:

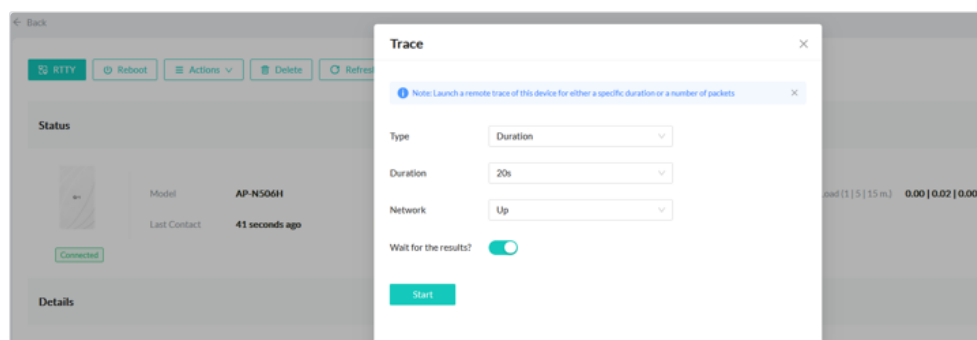
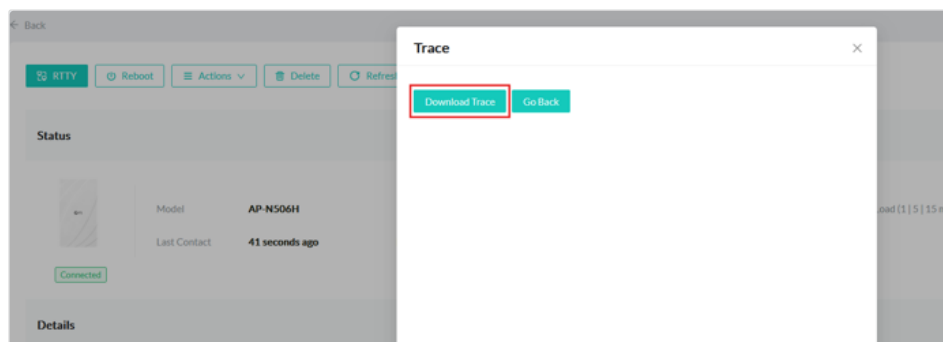


Table 1. Trace Configurations

Parameters	Description
Type	Captures packets based on the duration or packet count. • If you select Duration as the type, select the 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 the packet count in the Packets drop-down list. Then, AmpCon-Campus will

	capture the selected count of packets after you start the packet capturing.
Network	The network ports to be captured. Currently, you can select only Up because only ports in Up status can be captured.
Wait for the results?	Whether to wait for the packet capturing to complete. • If you toggle it off, the pop-up window will be closed automatically after you click Start. • If you toggle it on, the pop-up window will not be closed automatically after you click Start. You can click Go Back to start a new capturing or click the close icon to manually close the window.

6. Click **Start** to start the packet capturing. Wait for some time until the packet capturing is completed.
7. Download or check the captured packet traces.
 - From the **Trace** pop-up window
 - If the pop-up window has been closed, click **Actions** and then click **Trace** to open the pop-up window. Click **Download Trace** to download the captured packet traces.
 - If the pop-up window is not closed, click **Download Trace** directly in the pop-up window.



- From the **Commands** tab

On the AP detail page, scroll down to the **Commands** tab, locate the **Trace** type command, and then click **View**.

Then, you can see the captured trace in the pop-up window. To download the trace, click the download icon.

No Data

Trace - 2025-10-14 09:47:56

Preview

```
{ "id": "Trace", "error": 0, "resultCode": 0, "resultText": "uploading file", "text": "Success" }
```

Commands

Health Checks

Logs

Time

Start Time

End Time

Refresh

Submitted	Command	Completed	Error Code	Operation
34 seconds ago	Trace	Completed	0	Delete View
3 minutes ago	Trace	Completed	0	Delete View
4 minutes ago	Trace	Completed	0	Delete View
4 minutes ago	Configure	Failed	2	Delete View
16 hours ago	Configure	Completed	0	Delete View
16 hours ago	Rity	Completed	0	Delete View

Show More

Optimizing Wireless Networks

One-Click Network Optimization is a function that rapidly optimizes wireless network performance through automation technologies, simplifying traditional optimization processes and reducing operational complexity.

It's primarily applied in enterprise-level or high-density scenarios to address issues such as signal interference, load imbalance, and weak terminal connections.

By using AmpCon-Campus, you can optimize wireless networks immediately or at a fixed time. You can also customize network optimization configurations.

[Supported Optimization Methods](#)

[Immediate Network Optimization](#)

[Scheduled Network Optimization](#)

[Optional: Configuring Network Optimization](#)

Supported Optimization Methods

AmpCon-Campus supports the following optimization methods:

- **Immediate network 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 network optimization:** Optimizes wireless networks at a fixed time on a specific day, certain days, or daily.

NOTES

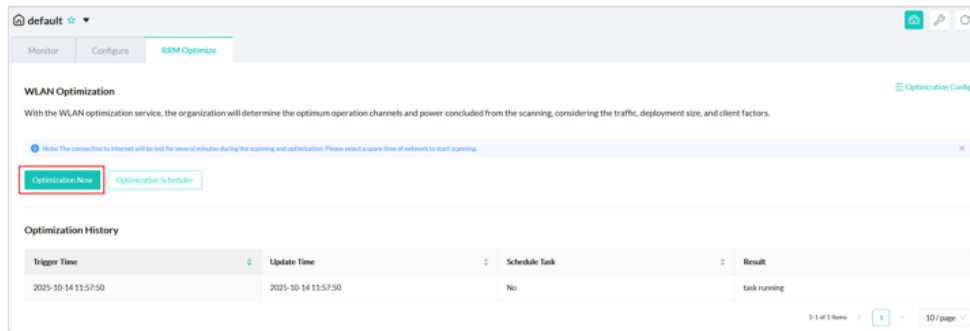
- For both optimization methods, you can [customize optimization configurations](#) as needed.
- If no custom optimization configurations are added, AmpCon-Campus will use the default optimization configurations, including channel optimization and power configurations.

Immediate Network Optimization

1. Click **Wireless > Manage** from the navigation bar.
2. In the **Site** drop-down list, select a specific site or select **All Sites**.
3. Click the **RRM Optimize** tab.
4. Click **Optimization Now**.

NOTES

- The whole optimization process is estimated to take 10 minutes. You are advised to avoid executing optimization at peak hours.
- Channel switching might occur during the optimization process, which might lead to user disconnection.



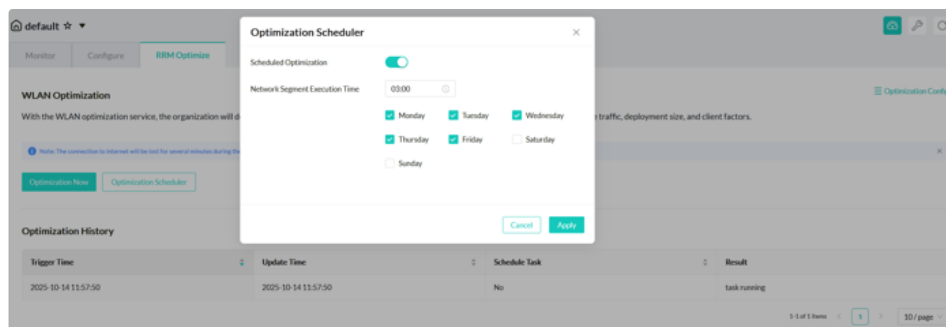
5. In the **Optimization History** section, check the information of the optimization task.

Table 1. Optimization History Metrics

Metric	Description
Trigger Time	The time when the optimization task is started.
Update Time	The time when the optimization configurations are pushed to APs.
Schedule Task	Whether the task is a scheduled optimization task.
Result	The current result of the optimization task.

Scheduled Network Optimization

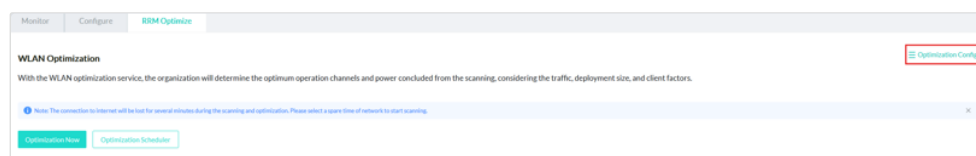
1. In the **RRM Optimize** tab, click **Optimization Scheduler**.
2. In the pop-up window, add the days and time to run the network optimization task.
 - a. Toggle on **Scheduled Optimization**.
 - b. In the **Network Segment Execution Time** section, select the days and time.
 - c. Click **Apply**.



Optional: Configuring Network Optimization

You can customize network optimization configurations as follows:

1. In the **RRM Optimize** tab, click **Optimization Config**.



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

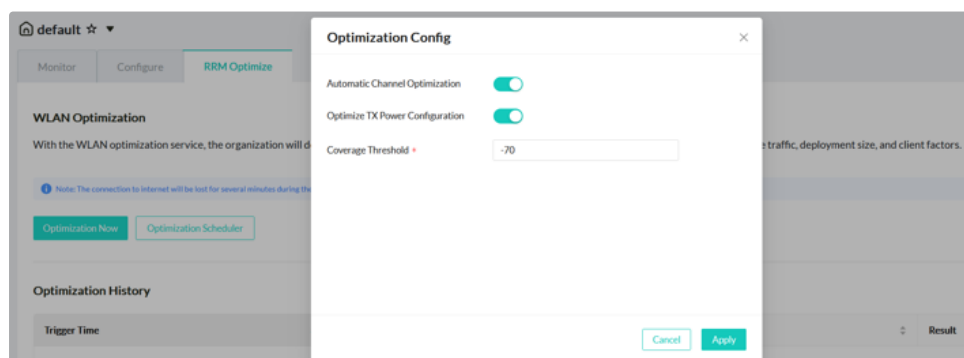


Table 2. Optimization Configurations

Configuration	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. NOTE You are recommended to toggle it on. If the performance can't meet your needs, enable Optimize Tx Power Optimization separately for further tuning.

Optimize TX Power Configuration	Toggle it on to dynamically adjust the transmission power of APs, minimizing energy consumption, reducing interference, and ensuring communication quality. NOTE If you toggle it on, configure the Coverage Threshold value.
Coverage Threshold	The minimum signal strength for client devices to stably connect to the AP. The unit is dBm. The default value is -70. Valid values range from -80 to -60. NOTES • This field is available only when you enable Optimize TX Power Configuration. • Coverage Threshold dynamically adjusts the AP transmission 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), the AP will determine that stronger signal coverage is required and then increase its transmission 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.

Restoring to Factory Settings

You can restore managed access points (APs) to factory settings.

Procedure

[From the Inventory Page](#)

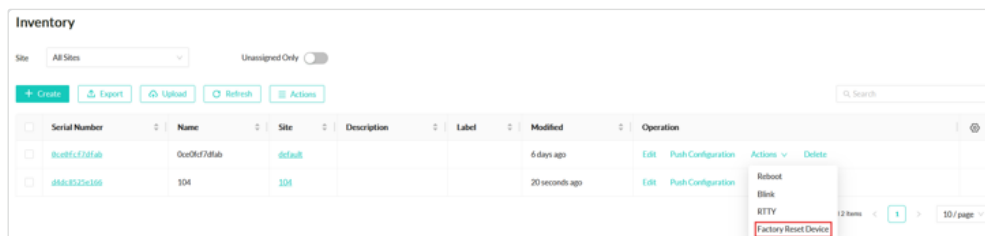
[From the AP Detail Page](#)

Procedure

To restore a managed AP to factory settings, use the “Inventory” page or the AP detail page.

From the Inventory Page

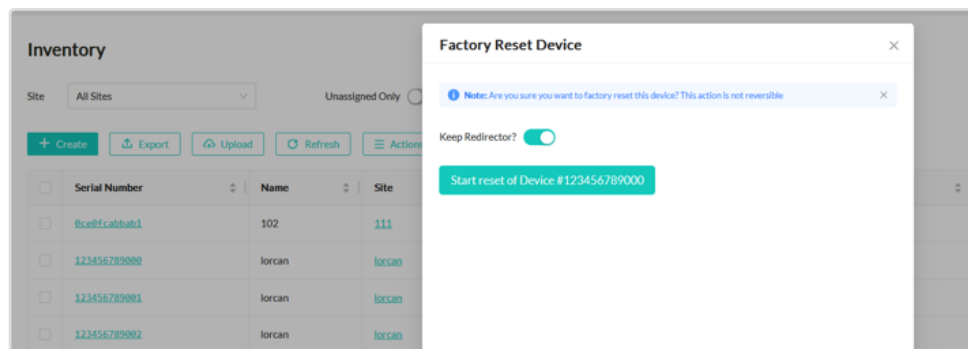
1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, click **Actions**, and then click **Factory Reset Device**.



4. Optional: To reserve the IP address of the AmpCon-Campus server in the **Redirector IP/URL** field of the AP webpage, toggle it on in the **Keep Redirector** section.

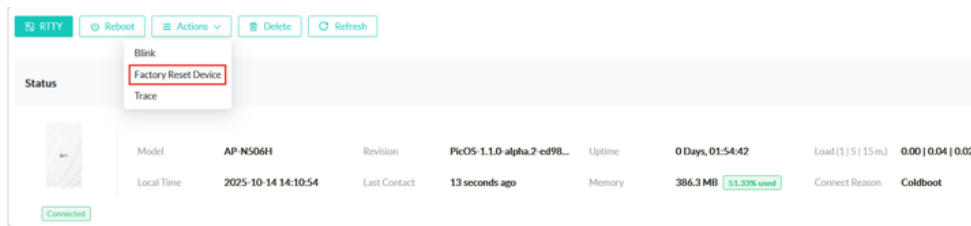
Then, the restoring to factory setting process will not clear the IP address of the AmpCon-Campus server from the AP webpage.

5. Click **Start reset of Device**.



From the AP Detail Page

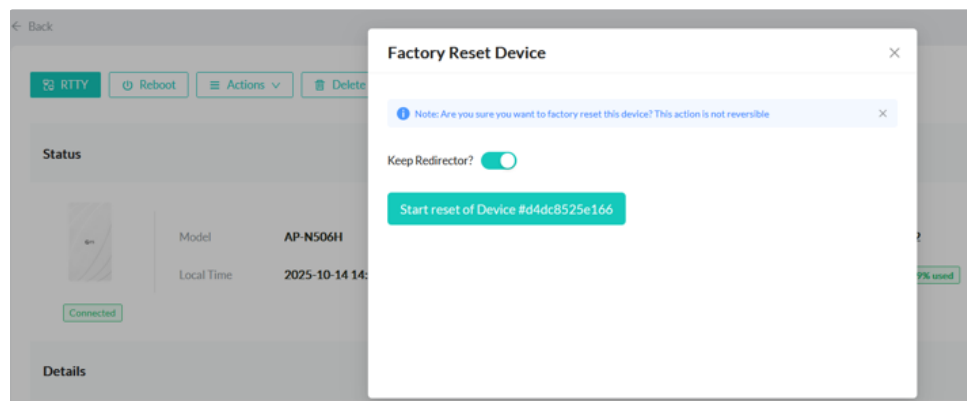
1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click its serial number.
4. On the AP detail page, click **Actions**, and then click **Factory Reset Device**.



- Optional: To reserve the IP address of the AmpCon-Campus server in the **Redirector IP/URL** field of the AP webpage, toggle it on in the **Keep Redirector** section.

Then, the restoring to factory setting process will not clear the IP address of the AmpCon-Campus server from the AP webpage.

- Click **Start reset of Device**.



Exporting, Deleting, and Moving APs

You can export access points (APs) to a .csv file, delete APs, or move APs from one site to another.

[Exporting APs](#)

[Deleting APs](#)

[From the Inventory Page](#)

[From the AP Detail Page](#)

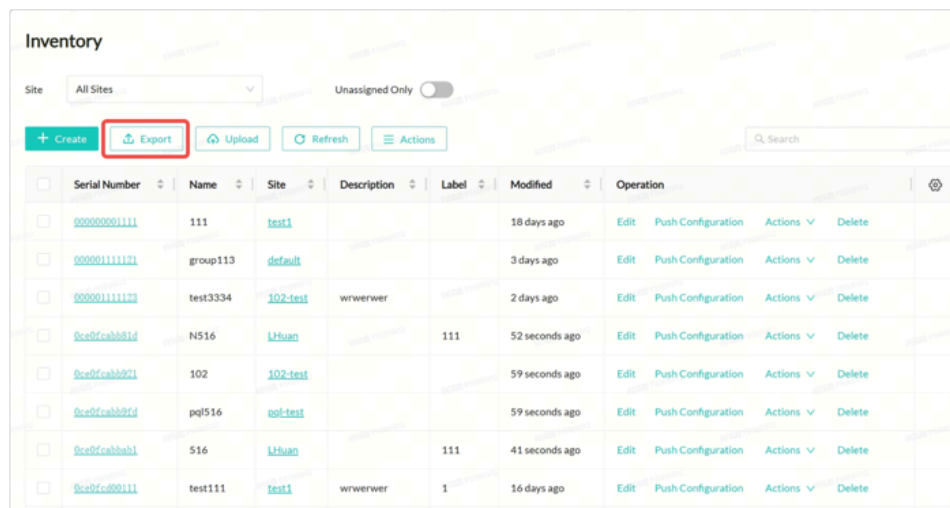
[Moving APs](#)

Exporting APs

To export APs to a .csv file, follow these steps:

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list of the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
3. Click **Export**.
4. Wait for the exporting process to complete. Once done, click **Download**.

Then, a .csv file will be downloaded to your local machine with APs in the selected site or all sites.



The screenshot shows the 'Inventory' page with a table of access points. The 'Export' button is highlighted with a red box. The table has columns for Serial Number, Name, Site, Description, Label, Modified, and Operation. The 'Operation' column contains links for Edit, Push Configuration, Actions, and Delete.

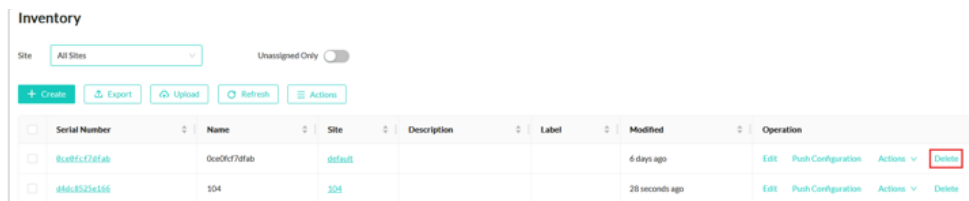
Serial Number	Name	Site	Description	Label	Modified	Operation
000000001111	111	test1			18 days ago	Edit Push Configuration Actions Delete
000001111121	group113	default			3 days ago	Edit Push Configuration Actions Delete
000001111122	test3334	102-test	wrwerwer		2 days ago	Edit Push Configuration Actions Delete
0c0fcaab81d	N516	LiHuan		111	52 seconds ago	Edit Push Configuration Actions Delete
0c0fcaab971	102	102-test			59 seconds ago	Edit Push Configuration Actions Delete
0c0fcaab9fd	pql516	ool-test			59 seconds ago	Edit Push Configuration Actions Delete
0c0fcaabab1	516	LiHuan		111	41 seconds ago	Edit Push Configuration Actions Delete
0c0fcaab0111	test111	test1	wrwerwer	1	16 days ago	Edit Push Configuration Actions Delete

Deleting APs

To delete APs, use the “Inventory” page or the AP detail page.

From the Inventory Page

1. On the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
2. Delete one or multiple APs as needed:
 - To delete an AP, locate the AP, and then click **Delete** on the right.



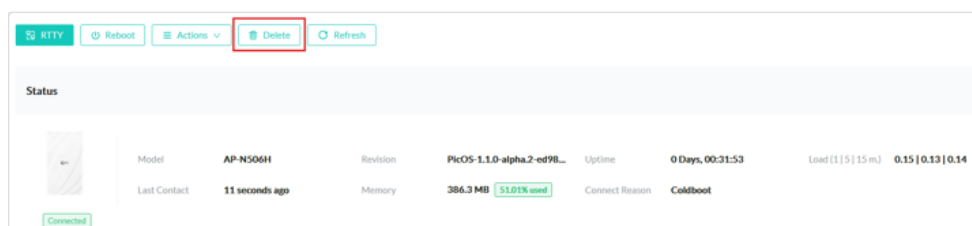
- To delete multiple APs, select these APs, click **Actions**, and then click **Delete**.



- Click **Yes** to confirm the deletion.

From the AP Detail Page

- On the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
- Locate the AP, and then click its serial number.
- On the AP detail page, click **Delete**.

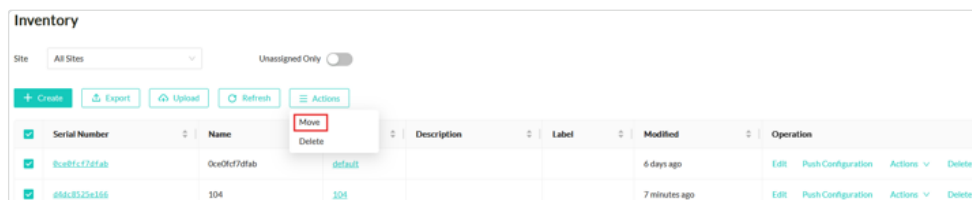


- Click **Yes** to confirm the deletion.

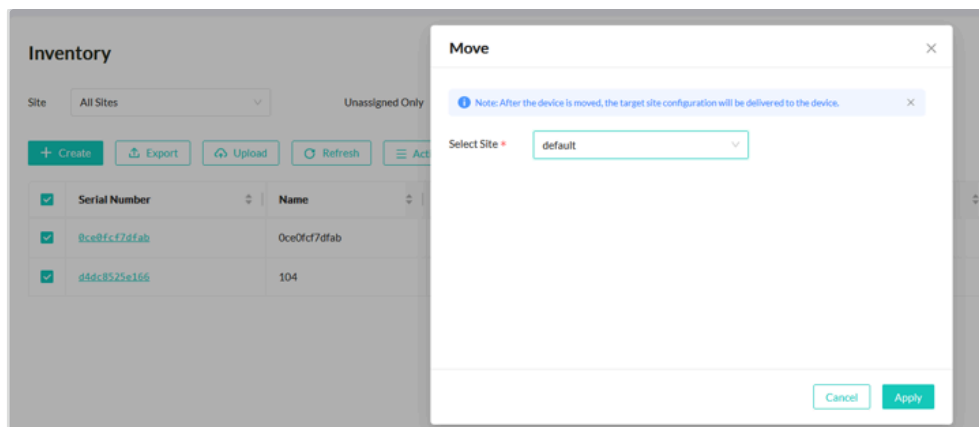
Moving APs

You can move one or multiple APs from one site to another. After the APs are moved, the target site configurations will be pushed to the APs automatically. Follow these steps:

- On the “Inventory” page, select the site to which the AP belongs or select **All Sites**.
- Select the APs to be moved.
- Click **Actions**, and then click **Move**.



- In the pop-up window, select the site to which the APs are moved, and then click **Apply**.



Accessing APs

You can connect to an access point (AP) from the AmpCon-Campus UI through remote TTY shell (RTTY).

[Optional: Preparing a RTTY Server](#)

[Connecting to an AP](#)

[From the Inventory Page](#)

[From the AP Detail Page](#)

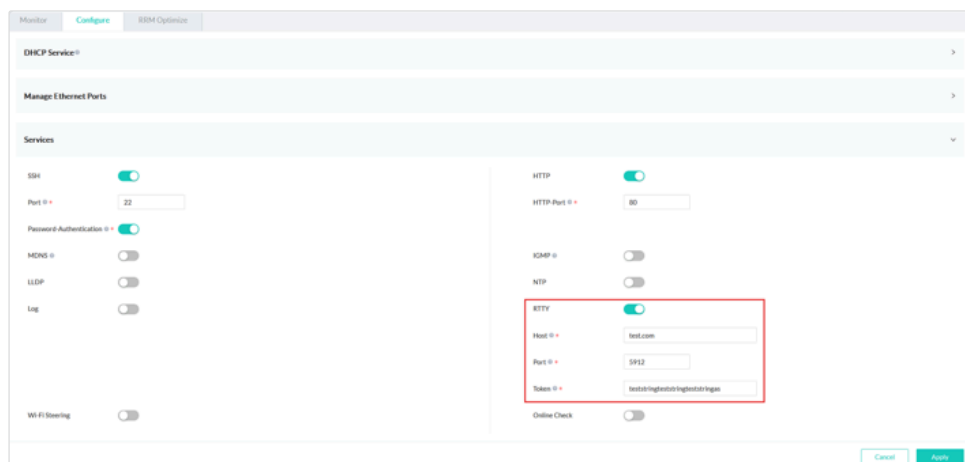
Optional: Preparing a RTTY Server

AmpCon-Campus has a built-in RTTY server, which you can use to connect to APs.

But if you want to use an external RTTY server, follow these steps:

1. Click **Wireless > Manage > Configure** from the navigation bar.
2. Click the **Advanced Configuration** tab.
3. In the **Services** section, enable RTTY and input the following information:
 - **Host:** The Fully Qualified Domain Name (FQDN) of the RTTY server.
 - **Port:** The port of the RTTY server.
 - **Token:** The token of the RTTY server.

For more information, see [Adding Advanced Configurations - Services](#).



The screenshot shows the 'Services' configuration page in the AmpCon-Campus UI. The 'RTTY' service is enabled (toggle is on). The configuration fields for RTTY are highlighted with a red box:

- Host:** test.com
- Port:** 3012
- Token:** test@ingest@ingest@ingest@ingest

Other services shown include SSH, HTTP, ICMP, UDP, Log, and Wi-Fi Streaming, each with its own set of configuration options and toggle switches.

4. Click **Apply**.

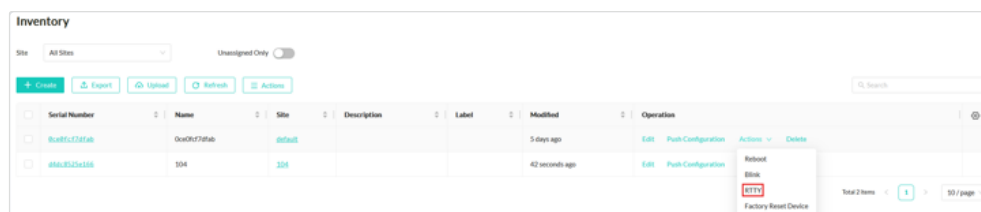
Connecting to an AP

To connect to an AP, use the “Inventory” page or the AP detail page.

From the Inventory Page

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, click **Actions**, and then click **RTTY**.

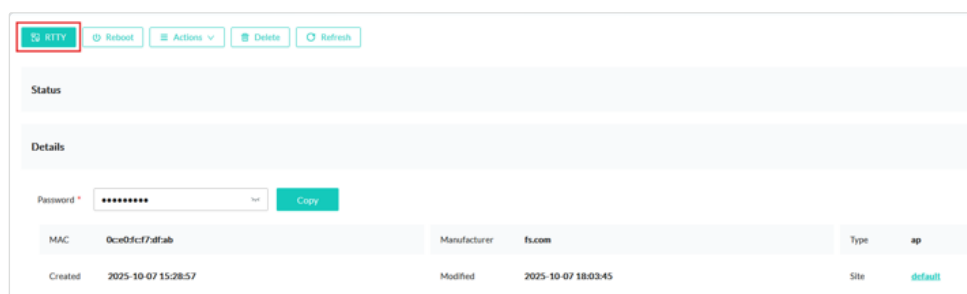
A new browser tab will be created.



4. In the new browser tab, enter the username and password of the AP, and then operate in the CLI as needed.

From the AP Detail Page

1. Click **Wireless > Inventory** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, and then click its serial number.
4. On the AP detail page, click **RTTY**.



A new browser tab will be created.

5. In the new browser tab, enter the username and password of the AP, and then operate in the CLI as needed.

Advanced CLI Configurations

AmpCon-Campus supports CLI configurations for access points (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 FS support engineers to do AP debugging or configuration for you through this feature.

Important

Do not use this feature by yourself. Or else, wrong CLI configurations might disrupt device operation.

Procedure

1. Click **Wireless > Access Points** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. Locate the AP, click **Actions**, and then click **Configure via CLI**.

Status	Serial Number	Name	Site	Memory	Load	Temp(°C)	Revision	Type	IP	Site	GPS	Online Uptime	Last Connected	Last Contact	Last Upgrade	Rx	Operation	5G
Connected	81081C48481	302	100%	90%	100%	52°C	Ph05-1.1.0-alpha.3-1c537a99	F3,AP-N016	10.28.64.215/24	102	-	05/05/2024	4 hours ago	4 seconds ago	4 hours ago	733.39	Actions	
Connected	49484812048	303	100%	90%	100%	48°C	Ph05-1.1.0-alpha.3-1c537a99	F3,AP-N016	10.28.64.215/24	102	-	05/05/2024	4 hours ago	4 seconds ago	4 hours ago	733.39	Actions	
Connected	49484812048	304	100%	90%	100%	48°C	Ph05-1.1.0-alpha.3-1c537a99	F3,AP-N016	10.28.64.215/24	102	-	05/05/2024	4 hours ago	4 seconds ago	4 hours ago	733.39	Actions	
Connected	49484812048	305	100%	90%	100%	48°C	Ph05-1.1.0-alpha.3-1c537a99	F3,AP-N016	10.28.64.215/24	102	-	05/05/2024	4 hours ago	4 seconds ago	4 hours ago	733.39	Actions	

4. In the pop-up window, do the following operations as needed:
 - Click **Current Configuration** to check the current configurations on the AP.
 - Modify the configurations directly in the configuration input box.
 - Click **Browse** to upload a .json configuration file.

Configure via CLI

Note: there will only be minimal tests done on this configuration

Browse... No file selected.

Current Configuration

```
{
  "interfaces": [
    {
      "name": "ethernet",
      "type": "ethernet",
      "isolate": false,
      "select-ports": [
        "WAN"
      ],
      "vlan-tag": "un-tagged"
    }
  ],
  "ipv4": {
    "addressing": "dynamic",
    "name": "default",
    "role": "upstream",
    "services": [
      "ssh",
      "http"
    ]
  }
}
```

Cancel Apply

5. Click **Apply**.

Monitoring Wireless Networks

After you deploy wireless networks, you can monitor different wireless networks, access points (APs), terminal devices (STAs), and wireless sites.

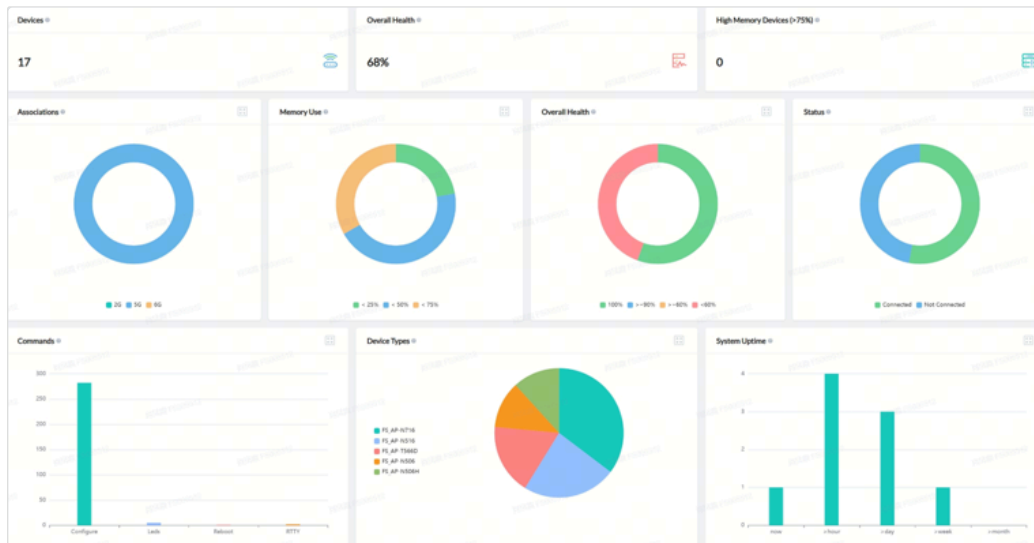
See the following child topics:

- [Wireless View](#)
- [Monitoring APs](#)
- [Monitoring STAs](#)
- [Monitoring Wireless Sites](#)

Wireless View

In the AmpCon-Campus UI, click **Dashboard > Wireless View** from the navigation bar.

On the “Wireless View” page, you can have a quick understanding of deployed wireless networks, such as managed access points (APs), AP health status, and connected terminal devices (STAs).



For the description of each section, see the following table:

Table 1. Section Descriptions

Section Name	Description
Devices	The count of APs currently connected to the AmpCon-Campus server.
Overall Health	The average health of all the currently connected APs. The value is calculated as follows: Average health = (Total APs with health as 100% * 100 + Total APs with health no less than 90% * 95 + Total APs with health no less than 60% * 75 + Total APs with health less than 60% * 30) / (Total APs * 100) * 100% Total APs above means the total number of APs currently connected to the AmpCon-Campus server.
High Memory Devices (>75%)	The count of APs with more than 75% memory usage.

Associations	The count and percentage of STAs connected to each radio band (2G, 5G, and 6G).
Memory Use	The count and percentage of APs with different levels of memory usage.
Overall Health	The count and percentage of APs with different levels of health.
Status	The count and percentage of APs currently connected or not connected with the AmpCon-Campus server.
Commands	The count and percentage of each type of executed commands. See the following command types and triggering operations: • Configure commands are run when AP configurations are pushed manually or automatically. • Leds commands are run when you position APs. • Factory commands are run when you restore APs to factory settings. • Trace commands are run when you capture remote port packets. • RTTY commands are run when you access APs. • Reboot commands are run when you reboot APs.
Device Types	The count and percentage of different types of APs.
Uptime	The count and percentage of APs with different levels of uptime. Uptime means the duration an AP has been running since its last startup.

Monitoring APs

On the “Access Points” page, you can check detailed metrics of each managed AP.

The metric data is automatically refreshed every minute. You can click **Refresh** to manually refresh the displayed metric data.

Procedure

Status

Details

Statistics

WiFi Analysis

Commands

Health Checks

Logs, Crash Logs, and Reboot Logs

Notes

Procedure

1. Click **Wireless > Access Points** from the navigation bar.
2. In the **Site** drop-down list, select the site to which the AP belongs or select **All Sites**.
3. On the “Access Points” page, check the metrics of managed APs:

Status	Serial Number	Name	Sanity	Memory	Load	Temp	Revision	Type	IP	Site	GPS	Outdoor Update	Last Connected	Last Contact	Last Upgrade	Rx	Operation	5G
Connected	000000000000	002	100%	100%	100%	52°C	PhyC 5.1.0-alpha.2-3c527a789	F3, AP-N016	10.20.4.215/24	102	-	000000000000	4 hours ago	4 seconds ago	4 hours ago	753.89	Active ✓	
Connected	000000000000	003	100%	100%	100%	40°C	PhyC 5.1.0-alpha.2-3c527a789	F3, AP-N016	10.20.4.216/24	103	-	000000000000	5 hours ago	30 seconds ago	3 days ago	405.34	Active ✓	
Connected	000000000000	004	100%	100%	100%	40°C	PhyC 5.1.0-alpha.2-3c527a789	F3, AP-N016	10.20.4.217/24	104	-	000000000000	21 hours ago	30 seconds ago	4 days ago	2.2 MB	Active ✓	
Connected	000000000000	005	100%	100%	100%	40°C	PhyC 5.1.0-alpha.2-3c527a789	F3, AP-N016	10.20.4.218/24	105	-	000000000000	3 hours ago	8 seconds ago	3 hours ago	411.37	Active ✓	

Table 1. Device Metrics

Metric	Description
Status	Whether the AP is currently connected with the AmpCon-Campus server.
Serial Number	The serial number of the AP.
Name	The name of the AP.
Sanity	The health grade of the AP. AmpCon-Campus calculates the Sanity value based on DHCP, DNS, RADIUS, and SSID health: Sanity = (100 - (interfaces with errors / total interfaces) * 100) * 100% In the following example, 2 interfaces have DNS issues, and the total number of interfaces is 4. So,

the **Sanity** is **50%**.

$$\text{Sanity} = (100 - (2 / 4) * 100) * 100\% = 50\%$$

Interface	DHCP	DNS	RADIUS	SSID	Error
default	✓	✓	✓	✓	No
vlan10	✓	✗	✓	✓	Yes
vlan20	✓	✓	✓	✓	No
vlan30	✓	✗	✓	✓	Yes

Memory	The memory usage percentage of the AP.
Load	The CPU load percentage of the AP.
Temp(°C)	The temperature of the AP. The unit is Celsius (°C).
Revision	The revision of the AP firmware.
Type	The type of the AP.
IP	The IP address of the AP.
Site	The site to which the AP belongs.
GPS	The longitude and latitude coordinates. NOTE The GPS value can be displayed only when the AP supports GPS.
Online Uptime	The duration during which the AP has been running since its last startup.
Last Connected	The last time when the connection between the AP and the AmpCon-Campus server was established.
Last Contact	The last time when the AP communicated with the AmpCon-Campus server.
Last Upgrade	The last time when the AP firmware was upgraded.
Rx	The total traffic that the AmpCon-Campus server sends to the AP.
Tx	The total traffic that the AP sends to the AmpCon-Campus server.
2G	The count of STAs connected to the 2G radio.

5G	The count of STAs connected to the 5G radio.
6G	The count of STAs connected to the 6G radio.
Connect Reason	The reason of the last connection between the AP and the AmpCon-Campus server. The following reasons are provided: • coldboot: The AP is powered on, or the process to connect the AP to the AmpCon-Campus server restarts. • socket: The AP is re-connected to the AmpCon-Campus server after a disconnection. • reboot: The AP is rebooted. • recovery: The AP is re-connected to the AmpCon-Campus server after a recovery. • upgrade failed: The AP is re-connected to the AmpCon-Campus server after an upgrade failure. • crashlog: The AP is re-connected to the AmpCon-Campus server after a crash.

Tips

- The following operations are the same as described in [Maintaining Wireless Networks](#).
 - To filter the metrics to be displayed, click the setting icon, and then select the metrics.
 - To export AP information, click **Export**.
 - To delete an AP, locate the AP, and then click **Delete**.
 - To restore an AP to factory settings, locate the AP, click **Actions**, and then click **Factory Reset Device**.
 - To make an AP blink, locate the AP, click **Actions**, and then click **Blink**.
 - To capture remote packets from target ports of an AP, locate the AP, click **Actions**, and then click **Trace**.
 - Click **Actions**, and then you can see **Configure via CLI**. This feature is used by FS support engineers to do AP debugging or advanced configuration. Do not use this feature by yourself. Or else, wrong CLI configurations might disrupt device operation.

- You can add some APs to the AmpCon-Campus denylist. Then, AmpCon-Campus will not monitor, configure, or manage these APs.
 - To add an AP to the denylist, click **Denylist**, and then click **+ Create**. In the pop-up window, enter the serial number of the AP and the deny reason (optional). Then, click **Apply**.
 - To remove an AP from the denylist, locate the AP in the denylist, and then click **Delete**.
 - To edit the deny reason, locate the AP in the denylist, and then click **Edit**.
 - To check the AP details retrieved before the AP is added to the denylist, locate the AP in the denylist, and then click **View Details**.

3. Locate the AP, and then click its serial number.

Then, on the AP detail page, you can see the following information:

Status

In the **Status** section, you can see **Connected** or **Disconnected**, which means whether the AP is currently connected with the AmpCon-Campus server or not.

In addition, you can check the following metrics:

Metric	Description
Model	AP-N506
Revision	Pfc05-1.1.2E-4b31e481ec
Uptime	5 Days, 00:18:23
Load (1 5 15 m.)	0.00 0.00 0.00
Local Time	2025-09-29 16:18:16

Table 2. Status Metrics

Metric	Description
Model	The model of the AP.
Revision	The revision of the AP firmware.
Uptime	The duration during which the AP has been running since its last startup.
Load (1 5 15 m.)	The average CPU load over the past 1, 5, and 15 minutes.
Local Time	The local time of the AP.

Last Contact	The last time when the AP communicated with the AmpCon-Campus server.
Memory	The used memory (size and percentage) of the AP.
Connect Reason	The reason of the last communication between the AP and the AmpCon-Campus server. The following reasons are provided: • coldboot: The AP is powered on or the process to connect the AP to the AmpCon-Campus server restarts. • socket: The AP is re-connected to the AmpCon-Campus server after a disconnection. • reboot: The AP is rebooted. • recovery: The AP is re-connected to the AmpCon-Campus server after a recovery. • upgrade failed: The AP is re-connected to the AmpCon-Campus server after an upgrade failure. • crashlog: The AP is re-connected to the AmpCon-Campus server after a crash.

Details

In the **Details** section, check the following metrics:

Details

Password * Copy

MAC	0c6bfc17affab	Manufacturer	itscom	Type	ap
Created	2025-09-26 14:51:50	Modified	2025-09-26 22:05:10	Site	winell

Table 3. AP Details

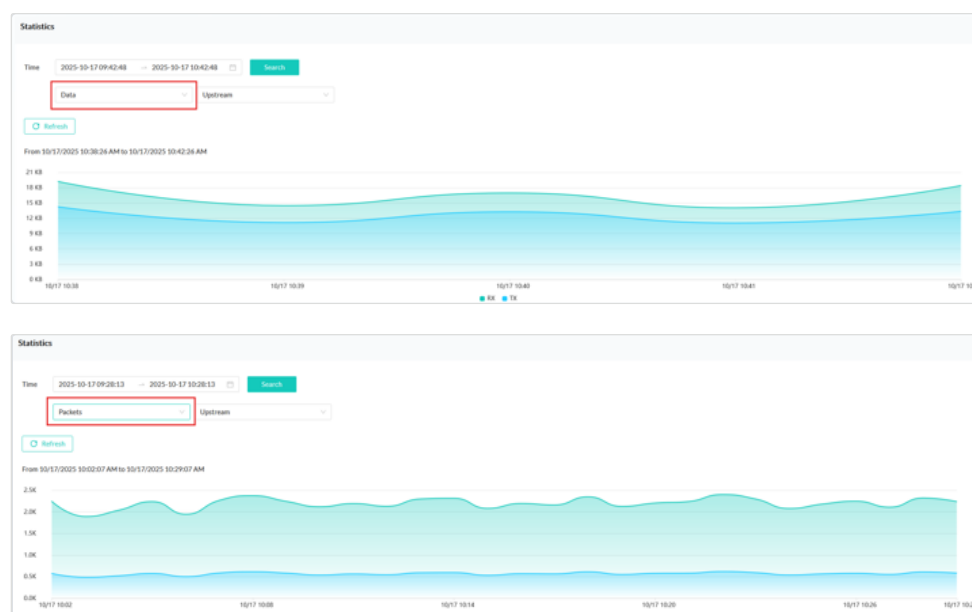
Metric	Description
Password	The password of the AP. • You can click the eye icon to view the clear-text password. Double click it, and then the password will be in encrypted text again. • You can copy the password by clicking Copy.
MAC	The MAC address of the AP.
Manufacturer	The manufacturer of the AP.

Type	The type of the AP.
Created	The first time when the AP is connected to the AmpCon-Campus server.
Modified	The last time when the channel connection between the AP and the AmpCon-Campus server was updated. A connection channel is established between an AP and the AmpCon-Campus server. To maintain security, the channel connection is periodically updated.
Site	The site to which the AP belongs. You can click the site name to view metrics of the wireless site. For more information, see Monitoring Wireless Sites.

Statistics

In the **Statistics** section, you can check upstream data or packets, downstream data or packets, and memory usage of the AP:

1. Select the start and end date and time in the **Time** section.
 2. Select **Upstream**, **Downstream**, or **Memory**.
- If you select **Upstream**, select **Data** or **Packets**. Then, you can see the trend graph of upstream traffic data or packets.

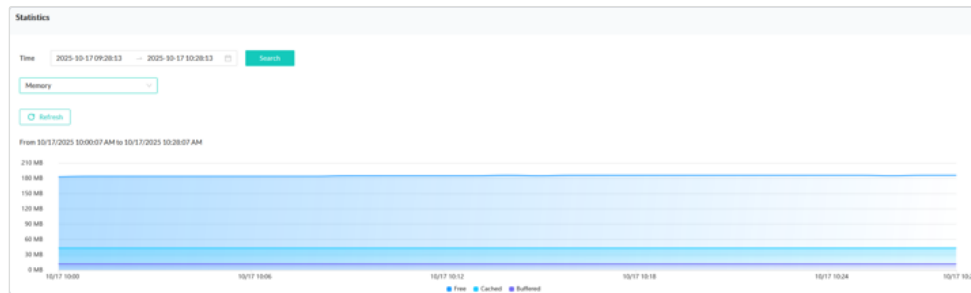


- If you select **Downstream**, select **Data** or **Packets**. Then, you can see the trend graph of downstream traffic data or packets.

NOTE

The **Downstream** option can be displayed only for the APs that have the [AP Assign IP](#) function enabled.

- If you select **Memory**, you can see the trend graph of memory usage.



3. Optional: To refresh the graph, click **Refresh**.

WiFi Analysis

In the **WiFi Analysis** section, click a time point in the time bar, and then check radio and STA related metrics at that time.

NOTE

To filter the metrics to be displayed, click the setting icon, and then select the metrics.

WiFi Analysis

When: 30 seconds ago

Radios (3)

	Ch.	Ch. W	Tx Pow.	Noise	Active (MS)	Busy (MS)	Receive (MS)	Send (MS)	Frequency	
2G	1	20	21	-101	59,624,126	8,914,284	75,766	1,079,780	2412	
5G	36	40	23	-109	1,079,350	54,576	884	18,162	5180, 5190	
6G	217	40	15	-108	1,083,351	4,452	0	4,452	7035, 7045	

Associations (2)

	Station	SSID	IPs	Fingerprint	Vendor	VLAN	Mode	RSSI	Rx Rate	Rx	Rx MCS	Rx NSS	Tx Rate	Tx	
2G	6c:f6:da:78:f4:1a	@@@@-2g	1			-	ap	-26	286700	7.14 MB	11	2	216600	28.08 MB	
5G	92:bc:0d:69:4e:8e	@@@@-5g	1			-	ap	-37	573500	833.02 KB	11	2	58500	1.2 MB	

Table 3. Radio Metrics

Metric	Description
Ch.	The channel of the radio.

Ch. W	The channel bandwidth. The unit is MHz.
Tx Pow.	The transmission power of the radio. The unit is dBm.
Noise	The external noise level between the STA and its connected AP. The unit is dB.
Active (MS)	The time during which the radio is active. The value refers to the total time during which the radio can be used for communication, including transmission, receiving, and idle listening states. The unit is millisecond.
Busy (MS)	The time during which the radio detects channel occupation, including sending or receiving packets from the radio and other devices. The unit is millisecond.
Receive (MS)	The time during which the radio receives packets. The unit is millisecond.
Send (MS)	The time during which the radio sends packets. The unit is millisecond.
Frequency	The used channel frequency and center frequency. If the channel frequency and center frequency are the same, you can see only one frequency displayed here.

Table 4. STA Metrics

Metric	Description
Station	The STA that connects to the AP, such as a laptop or smartphone.
SSID	The Service Set Identifier (SSID) that the STA connects to. An SSID is used to distinguish a wireless network.
IPs	The IP address of the STA.

Fingerprint	Currently, this metric is not supported.
Vendor	The vendor of the STA.
VLAN	The VLAN ID of the STA.  NOTE This value can be displayed only if the VLAN is automatically assigned by the radio.
Mode	The operating mode of the AP. Currently, only the ap mode can be displayed. The ap mode is the standard wireless access mode converting wired networks into wireless coverage. In this mode, APs connect to upstream switches through Ethernet cables and provide Wi-Fi access to nearby STAs.
RSSI	Short for Received Signal Strength Indicator. RSSI is used to indicate the strength of signals. The unit is dB. Normally, the value is a negative number. The closer to 0, the stronger the signal.
Rx Rate	The negotiated receiving rate of the STA.
Rx	The total traffic received by the STA.
Rx MCS	The Modulation and Coding Scheme (MCS) index used by the STA to receive data. A higher MCS value indicates a faster data rate and a less stable network.
Rx NSS	The number of antennas the STA uses for receiving data. The value 0 indicates no data transmission.
Tx Rate	The negotiated sending rate of the STA.
Tx	The total traffic sent by the STA.

Commands

In the **Commands** tab, select the start and end date and time in the **Time** section. Then, you can see the following metrics:

NOTES

- To delete a command, locate the command, and then click **Delete**.
- To refresh the command list, click **Refresh**.
- To filter the metrics to be displayed, click the setting icon, and then select the metrics.

Commands						
Time Start Time → End Time Refresh						
Submitted	Command	Status	Executed	Completed	Error Code	Operation
3 days ago	Configure	Completed	3 days ago	3 days ago	0	Delete View
3 days ago	Configure	Completed	3 days ago	3 days ago	0	Delete View
3 days ago	Configure	Completed	3 days ago	3 days ago	0	Delete View
3 days ago	Configure	Completed	3 days ago	3 days ago	0	Delete View
3 days ago	Configure	Completed	3 days ago	3 days ago	0	Delete View
3 days ago	Configure	Failed	3 days ago	3 days ago	1	Delete View

Table 5. Command Metrics

Metric	Description
Submitted	The time when the command is submitted.
Command	The count and percentage of each type of executed commands. See the following command types and triggering operations: • Configure commands are run when AP configurations are pushed manually or automatically. • Leds commands are run when you position APs. • Factory commands are run when you restore APs to factory settings. • Trace commands are run when you capture remote port packets. • RTTY commands are run when you access APs. • Reboot commands are run when you reboot APs.
Status	The status of the pushed command. • Completed: The command is pushed to the AP successfully.

	• Failed: The command fails to be pushed to the AP. • Executed: The command is submitted, but the AP doesn't send the command execution result to the AmpCon-Campus server for reasons like connection issues.
Executed	The time when the command is executed.
Completed	The time when the command is completed.
Error Code	The number of errors occurred in the command execution process. NOTES • If the command is pushed to APs successfully, the error code is 0. • If the error code value is not 0, you can click View in the Operation column to check for error details.

Health Checks

In the **Health Checks** tab, select the start and end date and time in the **Time** section. Then, you can see the following metrics:

NOTES

- To delete a health check item, locate the item, and then click **Delete**.
- To refresh the health check list, click **Refresh**.
- To filter the metrics to be displayed, click the setting icon, and then select the metrics.

Commands
Health Checks
Logs
Crash Logs
Reboot Logs

Time
Start Time
End Time

Delete
Refresh

Submitted	Config ID	Severity	Details	
50 seconds ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	
2 minutes ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	
3 minutes ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	
4 minutes ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	
5 minutes ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	
6 minutes ago	1758895532	50	["interface":"up047","dhcp":"false","location":"Interface07","warning":["DHCP did not offer any leases"],["vrf":["memory":246]]	

Show More

Table 6. Health Check Metrics

Metric	Description
--------	-------------

Submitted	The time when the command is submitted.																														
Config ID	The ID automatically generated by AmpCon-Campus to identify a health check item.																														
Sanity	The health grade of the AP. AmpCon-Campus calculates the Sanity value based on DHCP, DNS, RADIUS, and SSID health: Sanity = 100 - (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 sanity is 50. Sanity = 100 - (2 / 4) * 100 = 50 <table><tr><th>Interface</th><th>DHCP</th><th>DNS</th><th>RADIUS</th><th>SSID</th><th>Error</th></tr><tr><td>default</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>No</td></tr><tr><td>vlan10</td><td>✓</td><td>✗</td><td>✓</td><td>✓</td><td>Yes</td></tr><tr><td>vlan20</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>No</td></tr><tr><td>vlan30</td><td>✓</td><td>✗</td><td>✓</td><td>✓</td><td>Yes</td></tr></table>	Interface	DHCP	DNS	RADIUS	SSID	Error	default	✓	✓	✓	✓	No	vlan10	✓	✗	✓	✓	Yes	vlan20	✓	✓	✓	✓	No	vlan30	✓	✗	✓	✓	Yes
Interface	DHCP	DNS	RADIUS	SSID	Error																										
default	✓	✓	✓	✓	No																										
vlan10	✓	✗	✓	✓	Yes																										
vlan20	✓	✓	✓	✓	No																										
vlan30	✓	✗	✓	✓	Yes																										
Details	The issue details.																														

Logs, Crash Logs, and Reboot Logs

In the **Logs**, **Crash Logs**, and **Reboot Logs** tabs, select the start and end time, and then check system logs of the AP:

NOTES

- To delete a log item, locate the item, and then click **Delete**.
- To refresh the log list, click **Refresh**.
- To filter the metrics to be displayed, click the setting icon, and then select the metrics.

Commands	Health Checks	Logs	Crash Logs	Reboot Logs	
Time Start Time → End Time Delete Refresh					
Submitted	Config ID	Severity	Log	Details	
1 hour ago	1760752485	6	Initiating reboot	()	

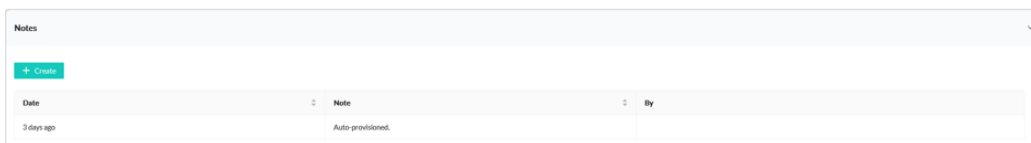
Table 7. Log Metrics

Metric	Description
--------	-------------

Submitted	The time when the log is sent to the AmpCon-Campus server successfully.
Config ID	The ID automatically generated by AmpCon-Campus to identify the log.
Severity	The severity of the log.
Log	The log information.
Details	The details of the log.

Notes

In the **Notes** tab, you can view the notes created for the AP. In addition, you can click **+ Create** to add a new note.



Notes		
+ Create		
Date	Note	By
3 days ago	Auto-provisioned.	

Table 8. Note Metrics

Metric	Description
Date	The date when the note is added.
Note	The note details.
By	The AmpCon-Campus user who creates the note.

Monitoring STAs

Stations (STAs) refer to terminal devices (such as smartphones and laptops) that connect to wireless networks through APs.

By using AmpCon-Campus, you can monitor STAs connected to each managed AP.

Procedure

1. Click **Monitor > Wireless Clients** from the navigation bar. Then, you can see these tabs: **All**, **Online**, and **Offline**.
2. Click each tab to view all STAs, online STAs, and offline STAs connected to managed APs.

Status	Hostname	MAC Address	Vendor	Connect AP	Site	SSID	RSSI	Band	Channel	Channel Width	IP	VLAN	Rx	Tx	Tx Packets	Rx Packets
Online	e0c26455-8f56	e0c26455-8f56	-	000b770dab	wh001	wh001	-47 dBm	5G	100	40	-	-	3239230	7419741	19918	17172
Offline	64a200e6-4c33	64a200e6-4c33	-	000b770dab	wh001	wh001	-44 dBm	2G	11	20	10.56.20.42	-	718343	994067	1849	2293

The following metrics are provided:

Table 1. Wireless Client Info

Metric	Description
Status	Whether the STA is currently connected to the AP. • Online: The STA is connected to the AP currently. • Offline: The STA is not connected to the AP currently.
Hostname	The hostname of the STA.
MAC Address	The MAC address of the STA.
Vendor	The vendor of the STA.
Connect AP	The AP to which the STA is connected.
Site	The site to which the AP belongs.
SSID	The Service Set Identifier (SSID) of the wireless network to which the STA is connected. An SSID is used to distinguish a wireless network.

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.
Band	The radio band to which the STA is connected.
Channel	The channel of the radio.
Channel Width	The channel bandwidth. The unit is MHz.
IP	The IP address of the STA.
VLAN	The VLAN ID of the STA.
Rx	The total traffic received by the STA. The unit is byte.
Tx	The total traffic sent by the STA. The unit is byte.
Tx Packets	The total number of packets sent by the STA.
Rx Packets	The total number of packets received by the STA.

3. Optional: To specify the metrics to be displayed, click the setting icon, and then select the metrics.



Status	Hostname	MAC Address	Vendor	Connect AP	Site	SSID	RSSI	Band	Channel	Channel Width	IP	VLAN	Rx	Tx	Tx Packets	Rx Packets
Offline	e0c24435-4f16	e0c24435-4f16	-	0a09c75dab	wh01	wh01	-46 dBm	5G	100	40	-	-	5107325	27934407	46841	31607
Offline	64a200e6-4c33	64a200e6-4c33	-	0a09c75dab	wh01	wh01	-45 dBm	2G	11	20	10.56.20.42	-	846305	1125458	2235	2773

4. Optional: To check historical metrics of the STA, locate the STA, and then click its MAC address.



Status	Hostname	MAC Address	Vendor	Connect AP	Site	SSID	RSSI	Band	Channel	Channel Width	IP	VLAN	Rx	Tx	Tx Packets	Rx Packets
Offline	e0c24435-4f16	e0c24435-4f16	-	0a09c75dab	wh01	wh01	-46 dBm	5G	100	40	-	-	5107325	27934407	46841	31607
Offline	64a200e6-4c33	64a200e6-4c33	-	0a09c75dab	wh01	wh01	-45 dBm	2G	11	20	10.56.20.42	-	846305	1125458	2235	2773

You will be redirected to the **Client Lifecycle** section, where you can see historical metrics. For more information, see [Client Lifecycle](#).

Monitor

Configure

SSM Optimize

Client Lifecycle

Time

2025-09-23 18:03:39

-- 2025-09-24 18:03:39

Search

e9c264554f16

Timestamp	BSSID	SSID	RSSI(dB)	Noise(dB)	Channel	TX Power	TX Retries	Connected	Inactive	ACK Signal(dB)	ACK SignalAvg(dB)	RX	RX MCS	RX NSS	TX	TX MCS
45 seconds ago	0ea0b77d7af	wireless	-48	-90	300	24	0	00a00033e40a	0 Seconds	-46	-45	5.14 MB	11	2	26.19 MB	0
2 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00033e40a	0 Seconds	-43	-43	5 MB	9	2	27.07 MB	0
2 minutes ago	0ea0b77d7af	wireless	-46	-90	300	24	0	00a00031e40a	0 Seconds	-42	-42	4.87 MB	10	2	26.64 MB	0
4 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00030e40a	0 Seconds	-44	-44	4.73 MB	11	2	24.35 MB	0
5 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00027e40a	0 Seconds	-45	-44	4.59 MB	11	2	24.02 MB	0
6 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00026e40a	0 Seconds	-44	-44	4.48 MB	11	2	23.71 MB	0
7 minutes ago	0ea0b77d7af	wireless	-49	-90	300	24	0	00a00027e40a	0 Seconds	-46	-46	4.28 MB	10	2	23.03 MB	0
8 minutes ago	0ea0b77d7af	wireless	-50	-90	300	24	0	00a00026e40a	0 Seconds	-46	-46	4.12 MB	11	2	22.24 MB	0
9 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00025e40a	0 Seconds	-43	-43	3.93 MB	11	2	18.3 MB	10
10 minutes ago	0ea0b77d7af	wireless	-47	-90	300	24	0	00a00024e40a	0 Seconds	-43	-43	3.74 MB	11	2	9.39 MB	0

Total 144 items

12345...15>

10/1000Go to

5. Optional: To check detailed information of the connected AP, locate the STA, and then click the serial number of the connected AP. For more information, see [Monitoring APs](#).

Wireless Clients																	
All (2) Online (2) Offline (2) Search by STA, AP, SSID or Vendor																	
Status	Hostname	MAC Address	Vendor	Connect AP	Site	SSID	RSSI	Band	Channel	Channel Width	IP	VLAN	Rx	Tx	Tx Packets	Rx Packets	
Offline	e9c264554f16	e9c264554f16	-	0ea0b77d7af	wireless	wireless	-47 dBm	5G	100	40	-	-	3239230	7419741	19918	17172	
Offline	64a200e64c33	64a200e64c33	-	0ea0b77d7af	wireless	wireless	-44 dBm	2G	11	20	10.56.20.42	-	718343	994067	1849	2293	
Total 2 items																	

6. Optional: To check the site of the connected AP, locate the STA, and then click the site name. For more information, see [Monitoring Wireless Sites](#).

Wireless Clients																	
All (2) Online (2) Offline (2) Search by STA, AP, SSID or Vendor																	
Status	Hostname	MAC Address	Vendor	Connect AP	Site	SSID	RSSI	Band	Channel	Channel Width	IP	VLAN	Rx	Tx	Tx Packets	Rx Packets	
Offline	e9c264554f16	e9c264554f16	-	0ea0b77d7af	wireless	wireless	-47 dBm	5G	100	40	-	-	3239230	7419741	19918	17172	
Offline	64a200e64c33	64a200e64c33	-	0ea0b77d7af	wireless	wireless	-44 dBm	2G	11	20	10.56.20.42	-	718343	994067	1849	2293	
Total 2 items																	

Monitoring Wireless Sites

A wireless site means an AmpCon-Campus site to which APs belong.

By using AmpCon-Campus, you can monitor the overall running status of each wireless site.

Procedure

[Overall Status](#)

[Live Data](#)

[Top 10 Busiest Devices](#)

[Client Lifecycle](#)

Procedure

1. Click **Wireless > Manage** from the navigation bar.
2. In the **Site** drop-down list of the **Monitor** tab, select the site to be monitored.

Then, you can see the following information:

Overall Status

At the top of the **Monitor** tab, check the following sections:

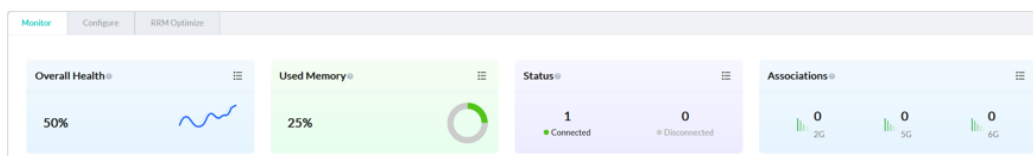


Table 1. Top Sections

Section	Description
Overall Health	The average health of all the currently connected APs in the site. The value is calculated as follows: $\text{Average health} = (\text{Total APs with health as } 100\% * 100 + \text{Total APs with health no less than } 90\% * 95 + \text{Total APs with health no less than } 60\% * 75 + \text{Total APs with health less than } 60\% * 30) / (\text{Total APs} * 100) * 100\%$ Total APs above means the total number of APs in the site that are currently connected to the AmpCon-Campus server.
Used Memory	The average memory usage of all currently connected APs in the site.

Status	The count of APs currently connected or not connected with the AmpCon-Campus server.
Associations	The count of STAs currently connected to each radio band.

Live Data

In the **Live Data** section, you can monitor the operating status and real-time performance of network devices in each radio band.

- Click **View** at the right of an AP name. Then, a new tab is opened, which displays [the AP detail page](#).



- Click the client icon at the right of an AP name. Then, you can see the following metrics in the pop-up window:



Table 2. Client Metrics for APs

Metric	Description
Health	The health grade of the AP. AmpCon-Campus calculates the Health value based on DHCP, DNS, RADIUS, and SSID health: Health = (100 - (interfaces with errors / total interfaces) * 100) * 100% In the following example, 2 interfaces have DNS issues, and the total number of interfaces is 4. So, the Health is 50%. Health = (100 - (2 / 4) * 100) * 100% = 50%

	<table><tr><th>Interface</th><th>DHCP</th><th>DNS</th><th>Radius</th><th>Error</th></tr><tr><td>Default</td><td>✓</td><td>✓</td><td>✓</td><td>No</td></tr><tr><td>vlan10</td><td>✓</td><td>✗</td><td>✓</td><td>Yes</td></tr><tr><td>vlan20</td><td>✓</td><td>✓</td><td>✓</td><td>No</td></tr><tr><td>vlan30</td><td>✓</td><td>✗</td><td>✓</td><td>Yes</td></tr></table>	Interface	DHCP	DNS	Radius	Error	Default	✓	✓	✓	No	vlan10	✓	✗	✓	Yes	vlan20	✓	✓	✓	No	vlan30	✓	✗	✓	Yes
Interface	DHCP	DNS	Radius	Error																						
Default	✓	✓	✓	No																						
vlan10	✓	✗	✓	Yes																						
vlan20	✓	✓	✓	No																						
vlan30	✓	✗	✓	Yes																						
Memory Used	The memory usage percentage of the AP.																									
Type	The type of the AP.																									
Firmware	The firmware of the AP.																									
2G Clients	The count of STAs currently connected to the 2G radio band.																									
5G Clients	The count of STAs currently connected to the 5G radio band.																									
6G Clients	The count of STAs currently connected to the 6G radio band.																									
Tx	The total traffic sent by the AP in the last 10 minutes.																									
Tx Packets	The total packets sent by the AP in the last 10 minutes.																									
Rx	The total traffic received by the AP in the last 10 minutes.																									
Rx Packets	The total packets received by the AP in the last 10 minutes.																									

- Click an AP name, and then click a radio band. You can see the following metrics in the pop-up window:

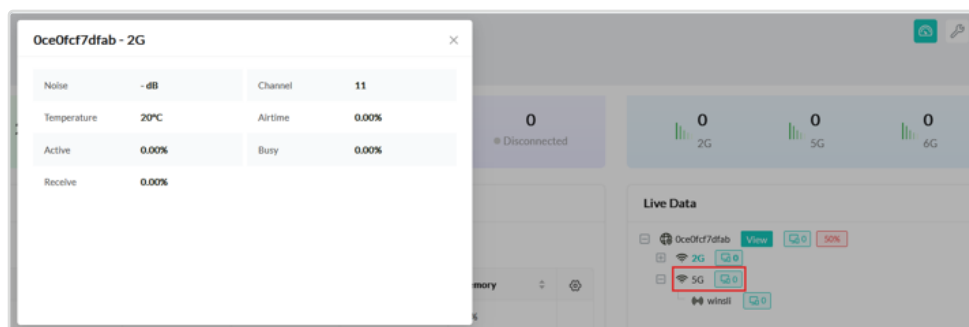


Table 3. Metrics for Radio Bands

Metric	Description
--------	-------------

Noise	The external noise level between the STA and its connected AP. The unit is dB.
Channel	The channel of the radio.
Temperature	The temperature of the AP. The unit is Celsius (°C).
Airtime	The percentage of the time during which the radio sends packets.
Active	The percentage of the time during which the radio is active. The radio is active when the radio can be used for communication, including transmission, receiving, and idle listening states.
Busy	The percentage of the time during which the radio detects channel occupation, including sending or receiving packets from the radio and other devices.
Receive	The percentage of the time during which the radio receives packets.

- Click a Service Set Identifier (SSID). Then, you can see the following metrics in the pop-up window:

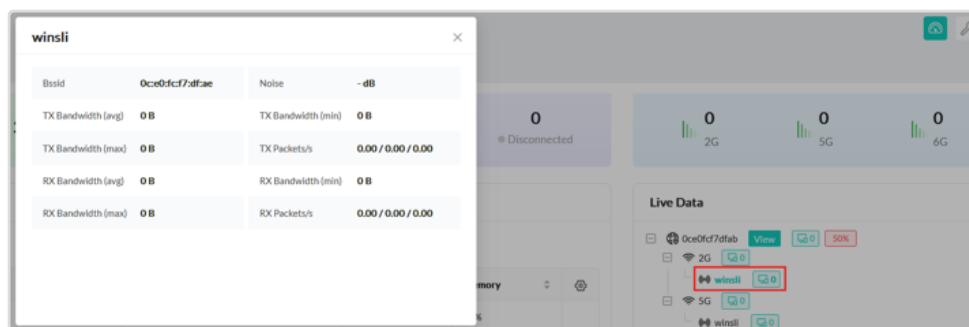


Table 4. Metrics for SSIDs

Metric	Description
Bssid	A 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.
Noise	The external noise level between the STA and its connected AP. The unit is dB.
TX Bandwidth (avg)	The average transmission bandwidth for the SSID. The unit is byte.
TX Bandwidth (min)	The minimum transmission bandwidth for the SSID. The unit is byte.
TX Bandwidth (max)	The maximum transmission bandwidth for the SSID. The unit is byte.
TX Packets/s	The minimum, maximum, and average transmission packets per second for the SSID.
RX Bandwidth (avg)	The average receiving bandwidth for the SSID. The unit is byte.
RX Bandwidth (min)	The minimum receiving bandwidth for the SSID. The unit is byte.
RX Bandwidth (max)	The maximum receiving bandwidth for the SSID. The unit is byte.
RX Packets/s	The minimum, maximum, and average receiving packets per second for the SSID.

- Click an STA. Then, you can see the following metrics in the pop-up window:



Table 5. Metrics for STAs

Metric	Description
Connected to	The SSID to which the STA is connected.

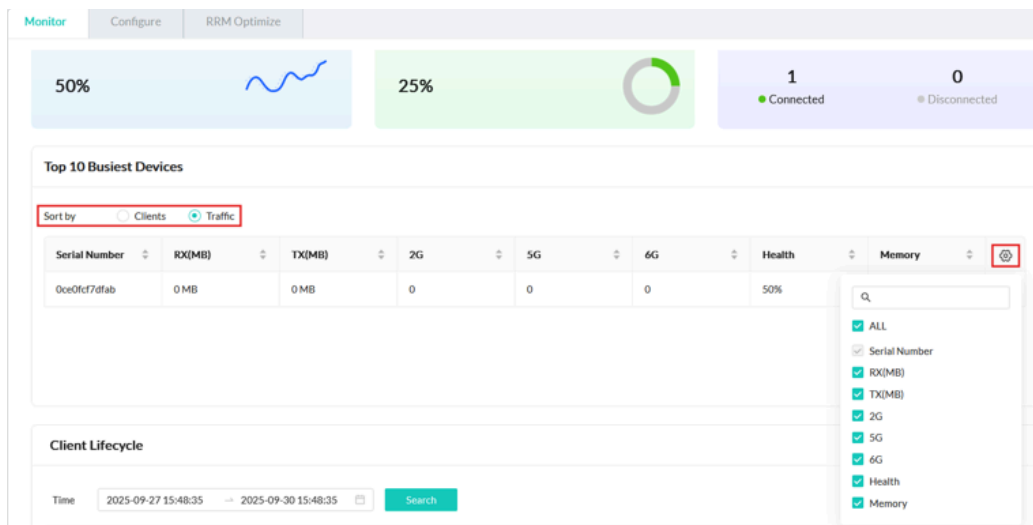
Total Data	The total data sent or received by the STA.
Delta	The incremental data sent or received by the STA. It's the difference between the current sampling value and the previous sampling value.
Bandwidth	The rate at which the STA sends and receives real-time data.
Packets/s	The rate at which the STA sends and receives real-time packets. The unit is packets/s.
MCS	The Modulation and Coding Scheme (MCS) index, which determines the modulation and coding scheme. A higher MCS value indicates a faster data rate but a less stable network.
NSS	The number of antennas the STA uses for sending and receiving data. The value 0 indicates no data transmission.

Top 10 Busiest Devices

In the **Top 10 Busiest Devices** section, you can see the top 10 busiest APs:

NOTES

- To sort APs based on the connected STA count or traffic volume, select **Clients** or **Traffic**.
- To specify the metrics to be displayed, click the setting icon, and then select the metrics.



The following metrics are provided:

Table 6. Busiest AP Metrics

Metric	Description
Serial Number	The serial number of the AP. NOTE This metric can't be hidden.
RX(MB)	The total traffic received by the AP. The unit is MB.
TX(MB)	The total traffic sent by the AP. The unit is MB.
2G	The count of STAs currently connected to 2G radio band.
5G	The count of STAs currently connected to 5G radio band.
6G	The count of STAs currently connected to 6G radio band.
Health	The health grade of the AP. AmpCon-Campus calculates the Health value based on DHCP, DNS, RADIUS, and SSID health: Health = (100 - (interfaces with errors / total interfaces) * 100) * 100% In the following example, 2 interfaces have DNS issues, and the total number of interfaces is 4.

So, the **Health** is **50%**.

Health = (100 - (2 / 4) * 100) * 100% = 50%

Interface	DHCP	DNS	Radius	Error
Default	✓	✓	✓	No
vlan10	✓	✗	✓	Yes
vlan20	✓	✓	✓	No
vlan30	✓	✗	✓	Yes

Memory

The memory usage percentage of the AP.

Client Lifecycle

In the **Client Lifecycle** section, select the start and end date and time in the **Time** section. Then, you can see historical metrics of STAs:

 **NOTE**

To specify the metrics to be displayed, click the setting icon, and then select the metrics.

Client Lifecycle																			
Time		2025-09-01 15:48:25 -- 2025-09-30 15:48:25		Search		v0264354f6													
Timestamp	BSSID	SSID	RSSI(dB)	Noise(dB)	Channel	TX Power	TX Retries	Connected	Inactive	ACK Signal(dB)	ACK Signal(Avg)(dB)	RX	RX MCS	RX NSS	TX	TX MCS	TX	TX	TX
4 days ago	00a00077a0af	wireless	-42	-90	100	24	0	00a00033e940s	0 Seconds	-39	-38	5.7 MB	9	2	30.46 MB	0			
4 days ago	00a00077a0af	wireless	-45	-90	100	24	0	00a00037e940s	0 Seconds	-41	-41	5.61 MB	9	2	30.04 MB	0			
4 days ago	00a00077a0af	wireless	-48	-90	100	24	0	00a00036e940s	0 Seconds	-45	-45	5.33 MB	11	2	29.76 MB	0			
4 days ago	00a00077a0af	wireless	-47	-90	100	24	0	00a00035e940s	0 Seconds	-43	-43	5.39 MB	10	2	29.15 MB	10			
4 days ago	00a00077a0af	wireless	-48	-90	100	24	0	00a00034e940s	0 Seconds	-44	-44	5.23 MB	11	2	28.43 MB	0			
4 days ago	00a00077a0af	wireless	-48	-90	100	24	0	00a00033e940s	0 Seconds	-46	-45	5.14 MB	11	2	28.19 MB	0			
4 days ago	00a00077a0af	wireless	-47	-90	100	24	0	00a00032e940s	0 Seconds	-43	-43	5 MB	9	2	27.07 MB	0			
4 days ago	00a00077a0af	wireless	-46	-90	100	24	0	00a00031e940s	0 Seconds	-42	-42	4.87 MB	10	2	26.44 MB	0			
4 days ago	00a00077a0af	wireless	-47	-90	100	24	0	00a00030e940s	0 Seconds	-44	-44	4.73 MB	11	2	24.35 MB	0			
4 days ago	00a00077a0af	wireless	-47	-90	100	24	0	00a00029e940s	0 Seconds	-45	-44	4.59 MB	11	2	24.02 MB	0			
Total 149 items																		1 / page	Go to Page

Table 7. Client Lifecycle Metrics

Metric	Description
Timestamp	The timestamp of the metric data.
BSSID	A unique 48-bit identifier assigned to each BSS in a wireless network. Typically, it's derived from the MAC address of the AP.
SSID	The SSID that the STA connects to. An SSID is a logical name of a wireless network.

RSSI(db)	Short for Received Signal Strength Indicator. RSSI is used to indicate the strength of signals. The unit is dB. Normally, the value is a negative number. The closer to 0, the stronger the signal.
Noise(db)	The external noise level between the STA and its connected AP. The unit is dB.
Channel	The channel of the radio.
TX Power	The transmission power of the AP. The unit is dBm.
TX Retries	The retransmission count between the STA and its connected AP.
Connected	The total time used by the STA to connect to the SSID.
Inactive	The time elapsed since the last frame (any frame like Data, ACK, Block-ACK, and QoS-Null) was received by the AP from the STA. A lower value means a more active STA.
ACK Signal(db)	The strength of the ACK signal. The unit is dB.
ACK SignalAvg(db)	The average strength of the ACK signal. The unit is dB.
RX	The total traffic received by the STA.
RX MCS	The Modulation and Coding Scheme (MCS) index used by the STA to receive data. A higher MCS value indicates a faster data rate and a less stable network.
RX NSS	The number of antennas the STA uses for receiving data. The value 0 indicates no data transmission.
TX	The total traffic sent by the STA.
TX MCS	The Modulation and Coding Scheme (MCS) index used by the STA to send data.

	A higher MCS value indicates a faster data rate and a less stable network.
TX NSS	The number of antennas the STA uses for sending data. The value 0 indicates no data transmission.
RX Bitrate	The data receiving rate of the STA. The unit is byte.
RX Ch Width	The channel width used by the STA for receiving data. The unit is MHz.
RX Duration	The duration during which the STA receives signals or packets.
RX Packets	The count of packets received by the STA.
RX VHT	Whether the VHT (802.11ac, also called WIFI5) mode is used by the STA to receive data.
TX Bitrate	The data transmission rate of the STA. The unit is byte.
TX Ch Width	The channel width used by the STA for sending data. The unit is MHz.
TX VHT	Whether the VHT (802.11ac, also called WIFI5) mode is used by the STA to send data.
TX Duration	The duration during which the STA sends signals or packets.
TX Packets	The count of packets sent by the STA.
IPv4	The IPv4 address of the STA.
IPv6	The IPv6 address of the STA.
Ch Width	The channel width of the radio to which the STA is connected. It's a parameter configured on the AP side for the radio, not for a specific STA. NOTES The Ch Width value represents the maximum channel width of the AP.

	• The TX Ch Width and RX Ch Width values are less than or equal to the Ch Width value, depending on the STA capabilities and signal quality.
Active MS	The time during which the radio is active. The value refers to the total time during which the radio can be used for communication, including transmission, receiving, and idle listening states.
Busy MS	The time during which the radio detects channel occupation, including sending or receiving packets from the radio and other devices.
Receive MS	The time during which the radio receives packets.
Mode	The operating mode of the AP. Currently, only the ap mode can be displayed. The ap mode is the standard wireless access mode converting a wired network into wireless coverage. In this mode, APs connect to upstream switches through Ethernet cables and provide Wi-Fi access to nearby STAs.

Importing FSOS Switches

Simple Network Management Protocol (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.

You can import FSOS switches to AmpCon-Campus through SNMP and then monitor FSOS switches in the AmpCon-Campus UI.

By using AmpCon-Campus, you don't need to use multiple tools to monitor PicOS and FSOS switches, reducing the complexity and workload of switch management while improving efficiency.

See the following child topics:

- [SNMP Overview](#)
- [Importing through SNMP](#)
- [Monitoring FSOS Switches](#)

NOTEs

- Ensure that the FSOS switches to be imported are supported by AmpCon-Campus. For more information, see [Supported FSOS Switches](#).
- Though FSOS switches can be imported to AmpCon-Campus, they can't be managed by AmpCon-Campus. You can only monitor them as described in [Monitoring FSOS Switches](#).

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.

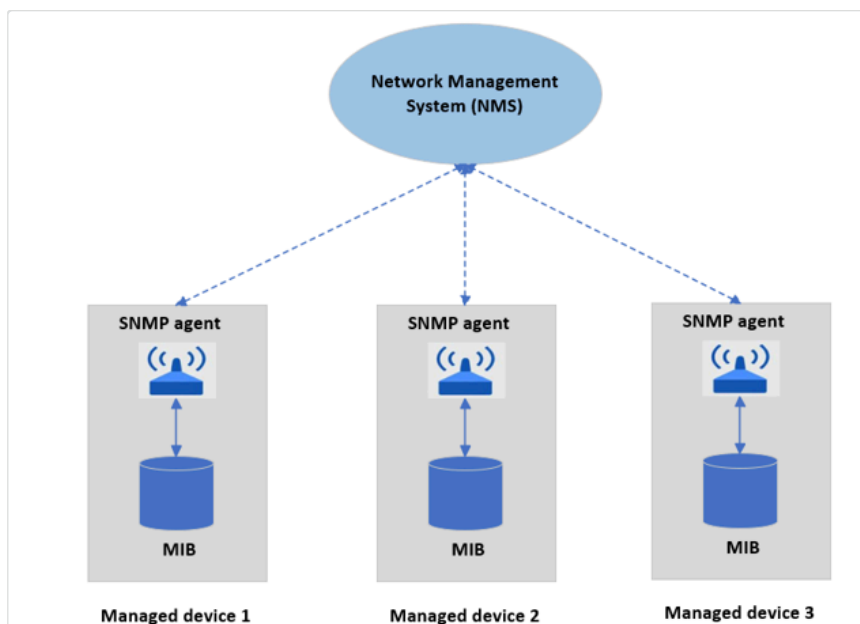
Each version differs in security, functionality, and performance. SNMP v3 is the most secure and powerful version, which supports encryption and authentication mechanisms.

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 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 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.

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.

- **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.

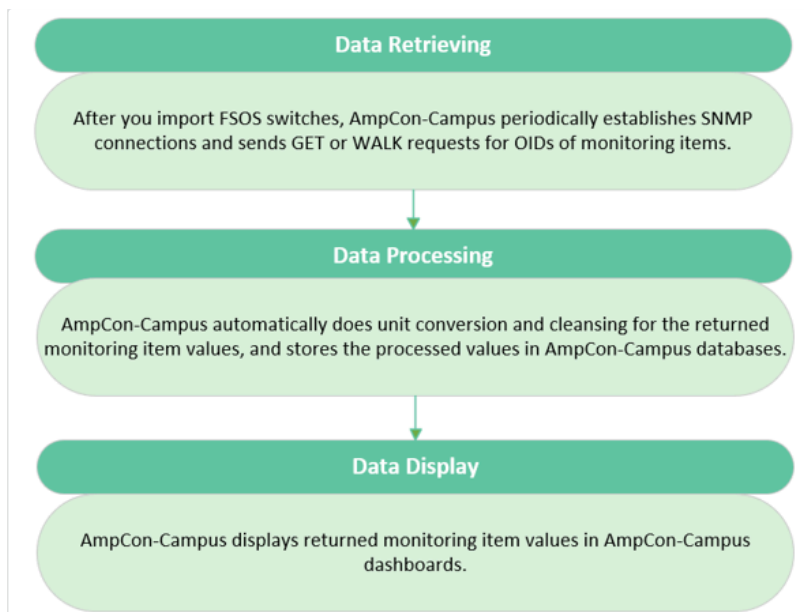
- **SNMP item**

The fundamental unit in NMS to define individual monitoring metrics. The SNMP manager uses OIDs to retrieve each item value on managed devices.

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



Importing through SNMP

To monitor FSOS switches with AmpCon-Campus, you need to import these switches to AmpCon-Campus through SNMP.

[Prerequisites](#)

[Importing FSOS Switches](#)

[Importing a Switch](#)

[Importing Switches in Batches](#)

[Checking Importing Results](#)

[Optional: Updating Supported FSOS Switches](#)

[Optional: Accessing Devices through SSH Sessions](#)

[Optional: Removing an FSOS switch](#)

Prerequisites

Before you import FSOS switches, ensure that the following prerequisites are met. Otherwise, FSOS switches might fail to be imported to AmpCon-Campus.

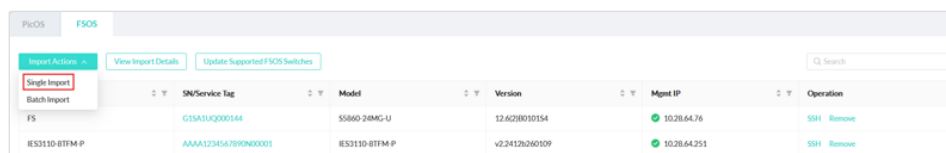
- Ensure that the FSOS switches are supported by AmpCon-Campus. For more information, see [Supported FSOS Switches](#).
- Ensure that you have enabled SNMP and configured SNMP authentication on the FSOS switches.
- Ensure that the OIDs (Sysname, Serial Number, Model, and Version) are not blocked on the switch side. These OIDs must be accessible for the SNMP View feature.
- Ensure that AmpCon-Campus can connect with the FSOS switches and no network timeout issues exist due to reasons like unreachable IP, disabled SNMP, firewall blockage, or Access Control List (ACL) restrictions.

Importing FSOS Switches

Importing a Switch

To import one FSOS switch, follow these steps:

1. Click **Wired > Switches** from the navigation bar.
2. Click the **FSOS** tab.
3. Hover over **Import Actions**, and then click **Single Import**.



	SN/Service Tag	Model	Version	Agent IP	Operation
FS	G15A1UQ000144	IS880-28MG-U	12.6(2)B010154	10.28.64.76	SSH Remove
IES3110-BTFM-P	AAAA1234567890N00001	IES3110-BTFM-P	v2.24126260109	10.28.64.251	SSH Remove

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

NOTE

Ensure that the SNMP authentication information you entered is correct and consistent with the switch. Or else, the import will fail.

- If the switches to be imported have SNMP v1 or SNMP v2c enabled, input the following information:

The screenshot shows the 'Single Import' dialog box in the FSOS interface. The background shows a table with columns 'Sysname' and 'SN/Service Tag'. The dialog box has three input fields: 'IP Address' with the value '192.168.1.1', 'SNMP Version' with a dropdown menu showing 'SNMP v2c', and 'SNMP Community' with the value 'test'. At the bottom right of the dialog are 'Cancel' and 'Apply' buttons.

Table 1. SNMP v1 or SNMP v2c Parameters

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

- If the switches to be imported have SNMP v3 enabled, input the following information:

The screenshot shows the 'Single Import' dialog box in the FSOS interface for SNMP v3 configuration. The background shows the same table as the previous screenshot. The dialog box has several input fields: 'IP Address' (192.168.1.1), 'SNMP Version' (dropdown showing 'SNMP v3'), 'Context Name' (test), 'Security User' (test_user), 'Security Level' (dropdown showing 'authPriv'), 'Authentication Protocol' (dropdown showing 'MD5'), 'Authentication Password' (masked with dots), 'Privacy Protocol' (dropdown showing 'DES'), and 'Privacy Password' (masked with dots). At the bottom right are 'Cancel' and 'Apply' buttons.

Table 2. SNMP v3 Parameters

Parameter	Description
IP Address	The IP address of the switch.
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.
Security User	The configured user who authenticates the communication identity between the SNMP management station (NMS) and the SNMP agent to prevent unauthorized access.
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 SHA256.  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.  NOTE This field is required only when you select authNoPriv or authPriv in the Security Level drop-down list.

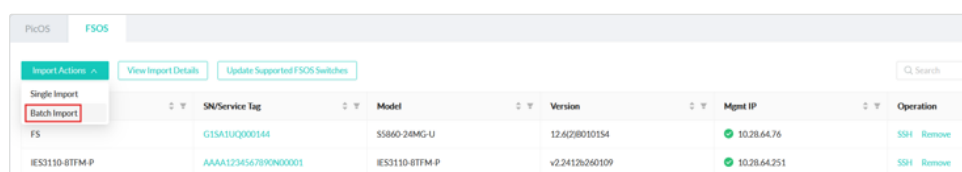
Privacy Protocol	The privacy protocol used for SNMP v3 agent checks. Values are DES, AES128, and AES256. NOTE This field is required only when you select authPriv in the Security Level drop-down list.
Privacy Password	The privacy passphrase used for SNMP v3 agent checks. NOTE This field is required only when you select authPriv in the Security Level drop-down list.

5. Click **Apply**.

Importing Switches in Batches

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

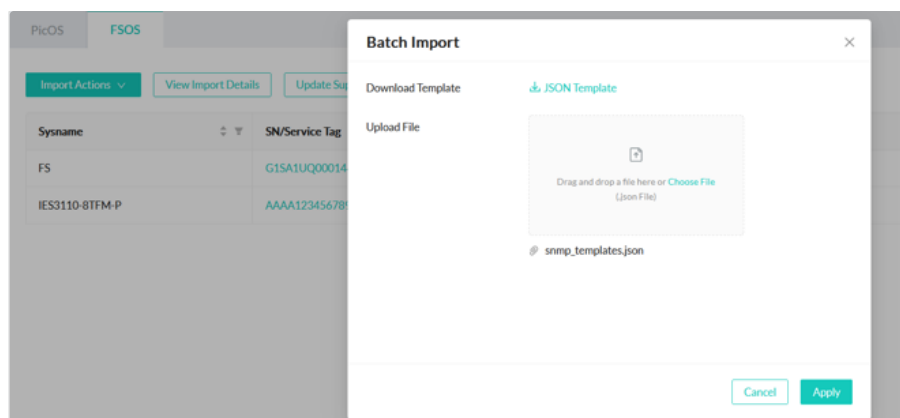
1. Click **Wired > Switches** from the navigation bar.
2. Click the **FSOS** tab.
3. Hover over **Import Actions**, and then click **Batch Import**.



4. In the pop-up window, configure as follows:
 - a. In the **Download Template** section, click **JSON Template** to download a template .json file.
 - b. In the .json file, enter information of the FSOS switches to be imported.
 - c. In the **Upload File** section, upload the .json file by dragging and dropping the file or clicking **Choose File** and then selecting the .json file.

NOTE

You can upload only one .json file in each batch import task.



5. Click **Apply**.

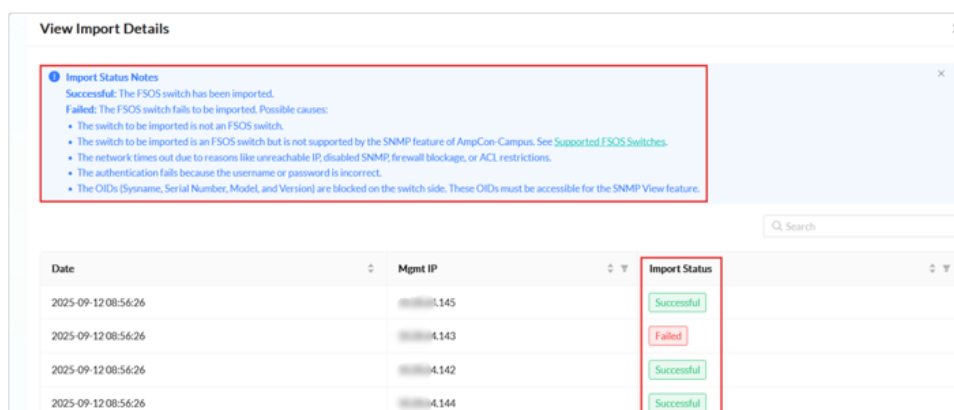
Checking Importing Results

Check whether FSOS switches are imported successfully. Follow these steps:

1. In the **FSOS** tab, click **View Import Details**.
2. In the pop-up window, check the **Import Status** column. You can see the following status:
 - **Successful**: The FSOS switch is imported successfully.
 - **Running**: The FSOS switch importing process is running.
 - **Pending**: The FSOS switch importing process is pending.
 - **Failed**: The FSOS switch fails to be imported.

NOTE

If the import status of a switch is **Failed**, check the **Import Status Notes** section for possible reasons, resolve the issues, and then re-import the switch.



Optional: Updating Supported FSOS Switches

Though some FSOS switches are included in the [supported FSOS switch list](#), they might fail to be imported with the error message “The switch model is not supported by AmpCon-Campus”. The reasons are as follows:

- After AmpCon-Campus 2.3 is released, more FSOS switches might be supported based on customers' needs.
- However, the AmpCon-Campus server is not updated with the latest FSOS switch support list.

Before you import these FSOS switches, you must update the supported FSOS switches on the AmpCon-Campus server first. Follow these steps:

1. In the **FSOS** tab, click **Update Supported FSOS Switches**.
2. In the pop-up window, select one of the following update methods:
 - Select **Online Update**. Then, AmpCon-Campus will automatically retrieve all the supported FSOS switches from GitHub and update the supported FSOS switches on the AmpCon-Campus server.

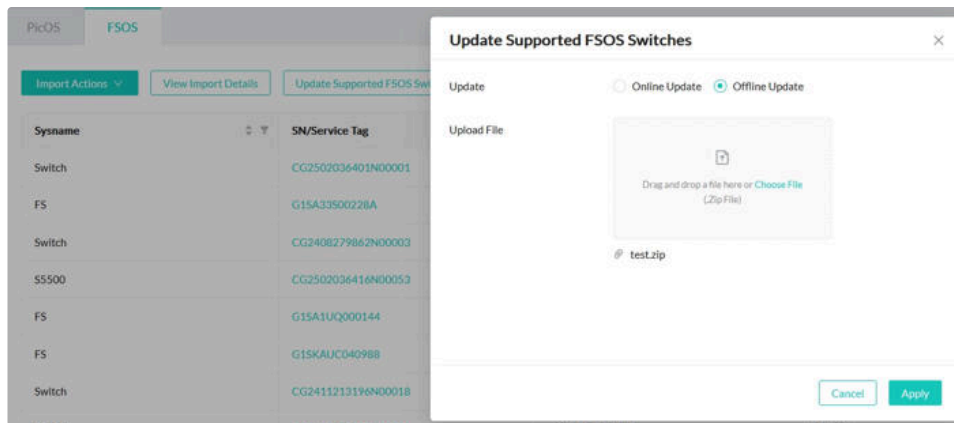
i NOTE

You can use this method only when the AmpCon-Campus server can access the [GitHub repository](#).

- Select **Offline Update**, and upload the .zip file by dragging and dropping it or clicking **Choose File** and then selecting the .zip file.

i NOTEs

- If the AmpCon-Campus server can't access the GitHub repository, use this offline update method.
- For the offline update method, pay attention to the following points:
 - You need to get the supported FSOS switch .zip file from the FS sale team. The .zip file contains a .json file listing all the supported FSOS switches.
 - Do not modify the .zip file manually. Or else, the update operation might fail.



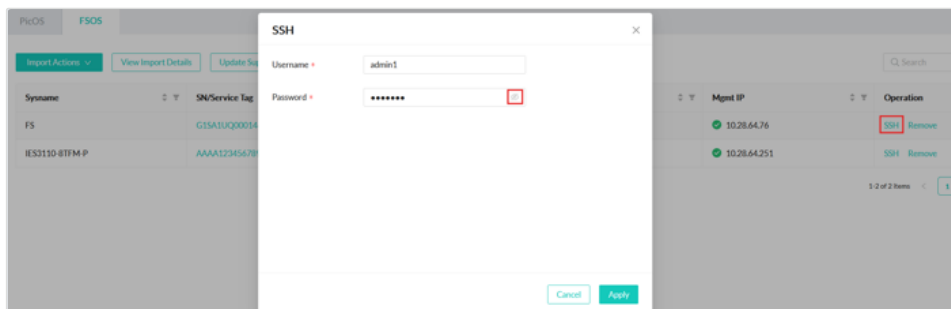
3. Click **Apply** to complete the update.

Optional: Accessing Devices through SSH Sessions

To connect to an FSOS switch from the AmpCon-Campus UI by creating an SSH session, follow these steps:

1. In the **FSOS** tab, locate the FSOS switch, and then click **SSH**.
2. In the **User Name** and **Password** fields, enter the username and password of the switch

In the **Password** field, you can click the eye icon to check the password in clear text or encrypted text.



3. Click **Apply**.

Then, an SSH session will be opened in a new browser tab.

Optional: Removing an FSOS switch

To remove an FSOS switch from AmpCon-Campus, follow these steps:

1. In the **FSOS** tab, locate the FSOS switch, and then click **Remove**.



2. Click **Yes**. Then, the removed FSOS switch will not be monitored by AmpCon-Campus.

Monitoring FSOS Switches

After you import FSOS switches through SNMP, you can continuously monitor the status, performance metrics, and other statistics in these switches for performance analysis and fault diagnosis.

[Prerequisites](#)

[Viewing the Switch List](#)

[Viewing Switch Details](#)

[Viewing SNMP Trend Graphs](#)

[Filtering SNMP Data](#)

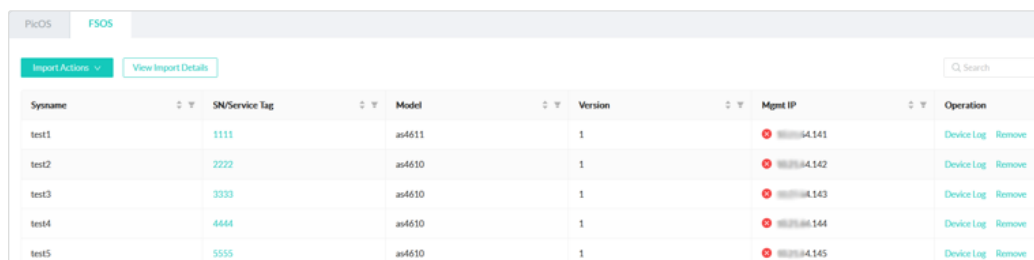
Prerequisites

Ensure that the following prerequisites are met. Otherwise, SNMP data might fail to be displayed in the AmpCon-Campus UI.

- The FSOS switches have been imported to AmpCon-Campus.
- SNMP is enabled on the FSOS switches.
- AmpCon-Campus can connect with the FSOS switches, and no network timeout issues exist due to reasons like unreachable IP, disabled SNMP, firewall blockage, or Access Control List (ACL) restrictions.
- The OIDs (Sysname, Serial Number, Model, and Version) are not blocked on the switch side. These OIDs must be accessible.

Viewing the Switch List

Click **Wired > Switches** from the navigation bar. Click the **FSOS** tab, and then you can see the list of all imported FSOS switches.



Sysname	SN/Service Tag	Model	Version	Mgmt IP	Operation
test1	1111	as4611	1	192.168.1.141	Device Log Remove
test2	2222	as4610	1	192.168.1.142	Device Log Remove
test3	3333	as4610	1	192.168.1.143	Device Log Remove
test4	4444	as4610	1	192.168.1.144	Device Log Remove
test5	5555	as4610	1	192.168.1.145	Device Log Remove

Table 1. Switch Metrics

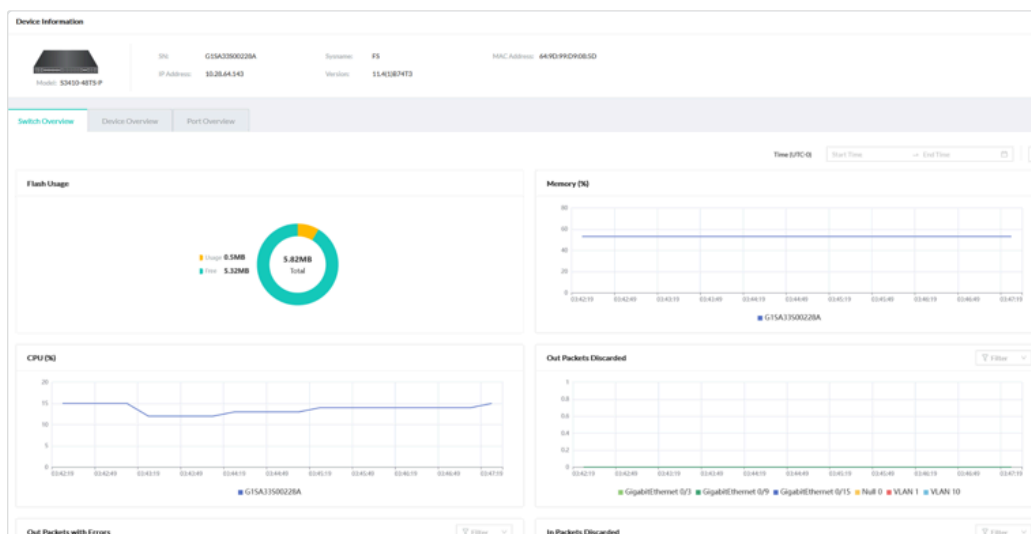
Metric	Description
Sysname	The hostname of the switch.
SN/Service Tag	The serial number (SN) or service tag of the switch.
Model	The model of the switch.

Version	The version of the switch.
Mgmt IP	The switch IP address used to connect to the AmpCon-Campus server. AmpCon-Campus detects the connectivity status every 60 seconds. The connectivity status is displayed based on the latest detection result: ✓: AmpCon-Campus can retrieve data from the switch through SNMP. ✗: AmpCon-Campus fails to retrieve data from the switch through SNMP.

Viewing Switch Details

In the **FSOS** tab, locate an FSOS switch, and click the SN or service tag of the switch.

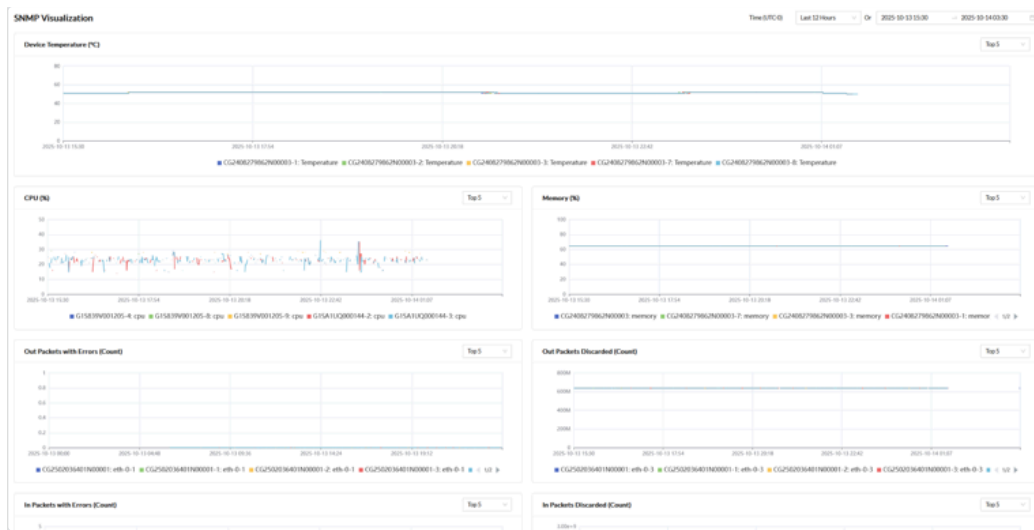
Then, you can see detailed metrics of the switch. For more information, see [Viewing FSOS Switch Details](#).



Viewing SNMP Trend Graphs

Click **Monitor > SNMP Management > SNMP Visualization** from the navigation bar.

On the “SNMP Visualization” page, you can add and view item-based trend graphs for imported FSOS switches. For more information, see [Viewing SNMP Trend Graphs](#).



Filtering SNMP Data

Click **Monitor > SNMP Management > SNMP Data Filtering** from the navigation bar.

On the “SNMP Data Filtering” page, you can filter SNMP data of all the imported FSOS switches. For more information, see [Filtering SNMP Data](#).

Switches: FS		Select	Item Name	Device Location: +32...	CL Search	
Sysname	SN	Item Name	Refresh Countdown (s)	Current Value		
FS	G1SA33900228A	Sysname	56	FS		
FS	G1SA33900228A	System Uptime	56	17d 19h 45m 59s		
FS	G1SA33900228A	Device MAC	56	64:9D:99:D9:08:5D		
FS	G1SA33900228A	Device SW Version	56	11.41J074T3		
FS	G1SA33900228A	Device HW Version	56	1.50		
FS	G1SA33900228A	Serial Number	56	G1SA33900228A		
FS	G1SA33900228A	CPU Utilization 5Sec	56	14%		
FS	G1SA33900228A	Device Temperature	56	27.0 °C		
FS	G1SA33900228A	Memory Used	56	53.0 %		
FS	G1SA33900228A	Memory Free	56	237 MB		
FS	G1SA33900228A	Memory Size	56	512 MB		
FS	G1SA33900228A	Flash Used	56	516 KB		
FS	G1SA33900228A	Flash Free	56	5.32 MB		
FS	G1SA33900228A	Flash Size	56	5.82 MB		
FS	G1SA33900228A	Fan Status	56	—		
FS	G1SA33900228A	Supply Status	56	—		

Viewing FSOS Switch Details

Click **Wired > Switches** from the navigation bar. In the **FSOS** tab, locate an FSOS switch, and click the serial number (SN) or service tag of the switch.

Then, you can see the following switch information on the switch detail page:

i NOTE

The displayed information is refreshed every 60 seconds.

[Prerequisite](#)

[Device Information](#)

[Switch Overview](#)

[Filtering Data](#)

[Device Overview](#)

[Port Overview](#)

Prerequisite

Ensure that all the [prerequisites](#) are met. Otherwise, SNMP data might fail to be displayed on the switch detail page.

Device Information

In the **Device Information** section, you can see the following information:

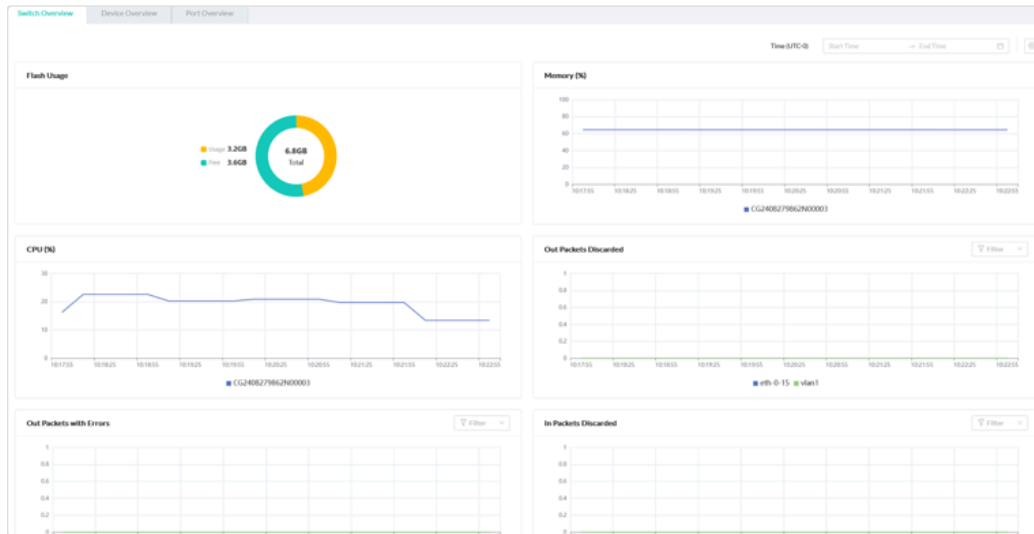
Device Information			
 Model: S5850C-24XMG2C	SN: CG2408279862N00003 IP Address: 10.1.1.144	Sysname: Switch Version: 3.0.13.15	MAC Address: 64:9D:99:33:71:92

Table 1. Device Information Metrics

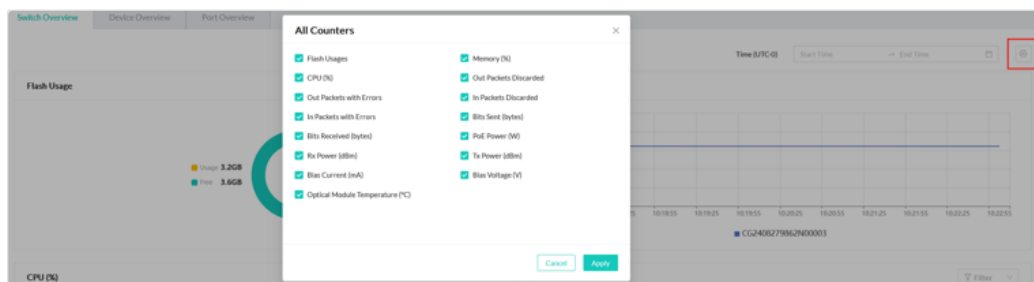
Metric	Description
Model	The model of the switch.
SN	The serial number of the switch.
Sysname	The hostname of the switch.
MAC Address	The MAC address of the switch.
IP Address	The IP address of the switch.
Version	The FSOS version of the switch.

Switch Overview

In the **Switch Overview** tab, you can see the following information:



To specify the metrics that you want to monitor, click the setting icon. In the pop-up window, select the metrics, and then click **Apply**.



The following metrics are provided:

Table 2. Switch Overview Metrics

Metric	Description
Flash Usage	The used, free, and total flash storage size. NOTE For switches of the following models, the Flash Usage data is not displayed: - S3950-4T12S-R - S5800-48T4S - S5800-48MBQ - S5850-48S6Q-R - S5850-48B8C - S5850-24B4C - S5850-24XMG-U

	• S8050-20Q4C • S8550-16Q8C • S5850C-24XMG2C • S5850C-24S2C • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F • S3900-48T6S-R • S5500-48T6SP-R
Memory	The memory usage, measured in percentage.  NOTE For switches of the IES3110-8TFM-P switch model, the Memory data is not displayed.
CPU	The CPU usage for the last 5 seconds, measured in percentage.
Out Packets Discarded	The number of outgoing packets that the switch port intentionally discards (drops).
Out Packets with Errors	The number of outgoing packets that the switch port fails to transmit due to errors.
In Packets Discarded	The number of incoming packets that the switch port intentionally discards (drops) during processing.
In Packets with Errors	The number of incoming packets that contain errors and are dropped by the switch port.
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.
PoE Power	The available power from the Power Sourcing Equipment (PSE) through the switch port. It's measured in watts (W).  NOTE

	For switches of the following models, the PoE Power data is not displayed: • IES3110-8TFM-P • S5850-24XMG-U • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S5500-48T6SP-R
Rx Power	The amount of Rx power received by the optical module. It's measured in dBm.
Tx Power	The amount of Tx power sent by the optical module. 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).

Filtering Data

To filter the data displayed in the **Switch Overview** tab, use the following methods:

- To specify a time range for the data display, select the start date and end date (within the last 30 days) in the **Time (UTC-0)** section.

NOTES

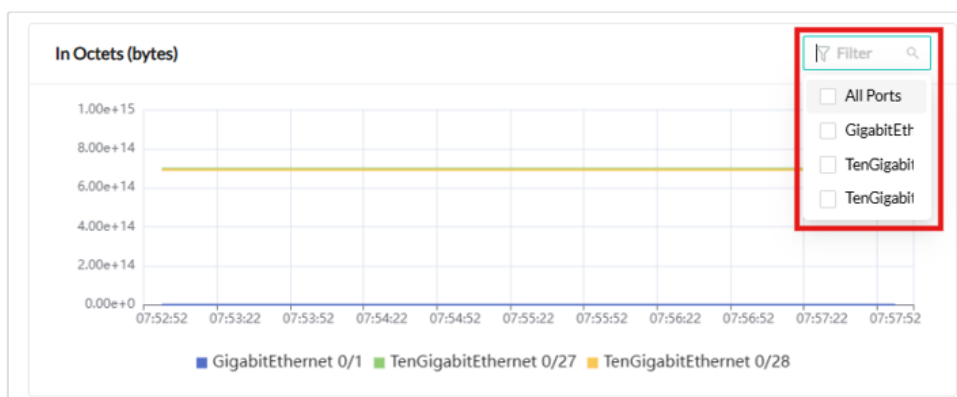
- The time in the **Time (UTC-0)** section is based on the **UTC-0** time zone.
- By default, the data in the last 5 minutes is displayed.
- The **Flash Usage** section always shows the latest retrieved data and thus is not impacted by the time filter.



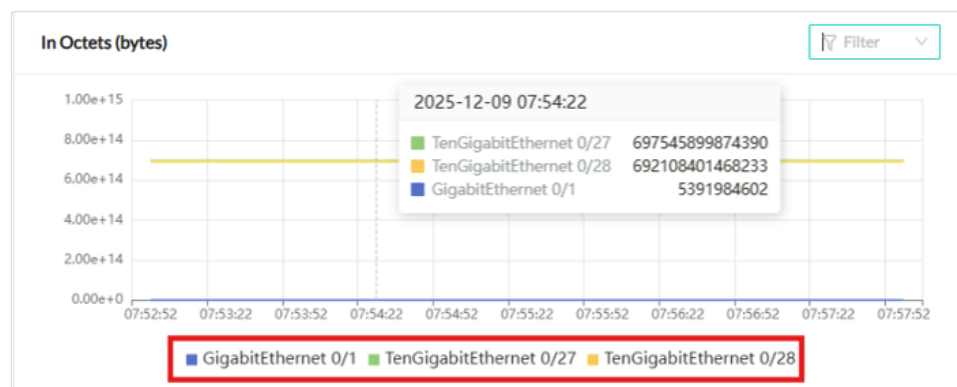
- To specify the ports to be monitored, click the filter field, and then select the ports.

NOTES

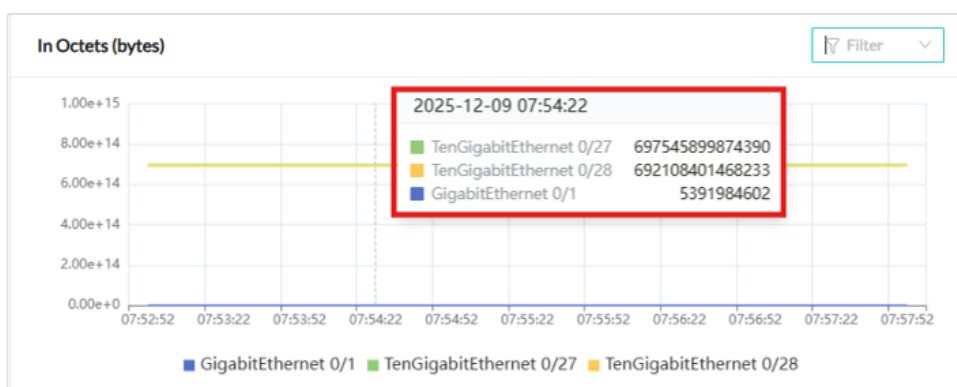
- Only the ports in **Up** status can be selected and displayed.
- The **Flash Usage**, **Memory**, and **CPU** sections don't have the filter field.



- 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 your mouse over that time point.



Device Overview

In the **Device Overview** tab, you can see the following information:

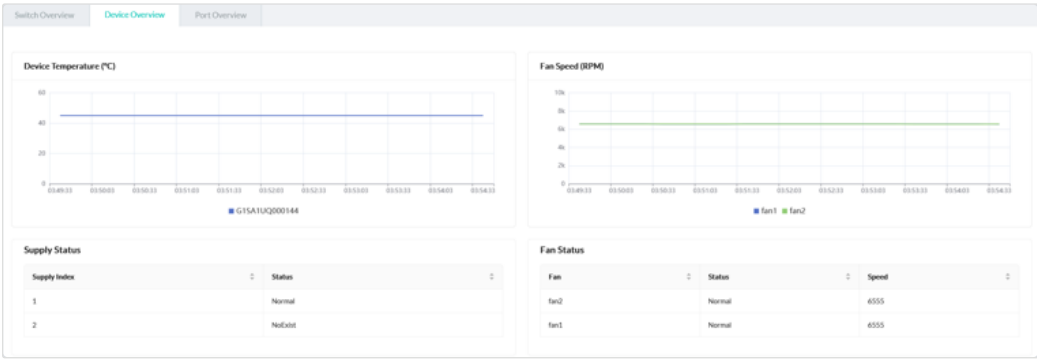


Table 3. Device Overview Metrics

Metric	Description
Device Temperature	The switch temperature, measured in Celsius (°C). NOTE For switches of the following models, the Device Temperature data is not displayed: • S3900-48T6S-R • S5500-48T6SP-R
Fan Speed	The fan speed, measured in Revolutions Per Minute (RPM). NOTE For switches of the following models, the Fan Speed data is not displayed: • IES3110-8TFM-P • S3270-24TM-P • S3270-10TM-P • S3270-48TM • S3410-48TS-P • S3410-24TF-P • S3410-24TS-P • S3910-24TF • S3260-8T2FP • S3400-24T4FP

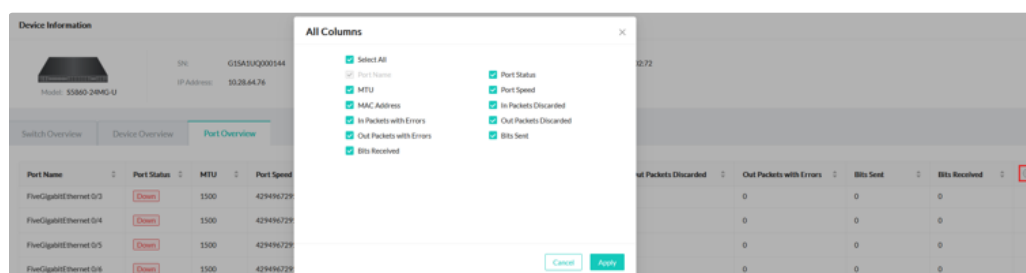
Supply Status	The latest retrieved index and status of Power Supply Unit (PSU). NOTE For switches of the following models, the Supply Status data is not displayed: • S3950-4T12S-R • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F
Fan Status	The latest retrieved fan position, status, and speed. NOTE For switches of the following models, the Fan Status data is not displayed: • IES3110-8TFM-P • S3260-8T2FP • S3400-24T4FP

Port Overview

In the **Port Overview** tab, you can see port-related information:

Port Name	Port Status	MTU	Port Speed	Mac Address	In Packets Discarded	In Packets with Errors	Out Packets Discarded	Out Packets with Errors	Bits Sent	Bits Received
eth-0-15	Up	1500	1000000000	64:9D:99:33:71:A1	0	0	0	0	14807138418	15850769627
vlan1	Up	1500	1000000000	64:9D:99:33:71:92	0	0	0	0	0	0
eth-0-1	Down	1500	1000000000	64:9D:99:33:71:93	0	0	0	0	0	0
eth-0-2	Down	1500	1000000000	64:9D:99:33:71:94	0	0	0	0	0	0

To specify the metrics to be monitored, click the setting icon. In the pop-up window, select the metrics, and then click **Apply**.



The following metrics are provided:

Table 4. Port Overview Metrics

Metric	Description
Port Name	The name of the switch port. NOTE The Port Name column is always displayed and can't be hidden.
Port Status	The state of the switch port.
MTU	The largest size of a data packet that can be transmitted over a network without being fragmented. It's measured in bytes.
Port Speed	An estimate of the interface's current bandwidth, measured in units of 1,000,000 bits per second. If this object reports a value of n, then the speed of the switch port is in the range of n-500,000 to n+499,999. NOTES • For switch ports that do not vary in bandwidth or for those where no accurate estimation can be made, this value contains the nominal bandwidth. • For a sub-layer that has no concept of bandwidth, this value is zero.
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.

Filtering SNMP Data

By using the “SNMP Data Filtering” page, you can filter SNMP data for all imported FSOS switches.

[Prerequisites](#)

[Procedure](#)

[Supported Items](#)

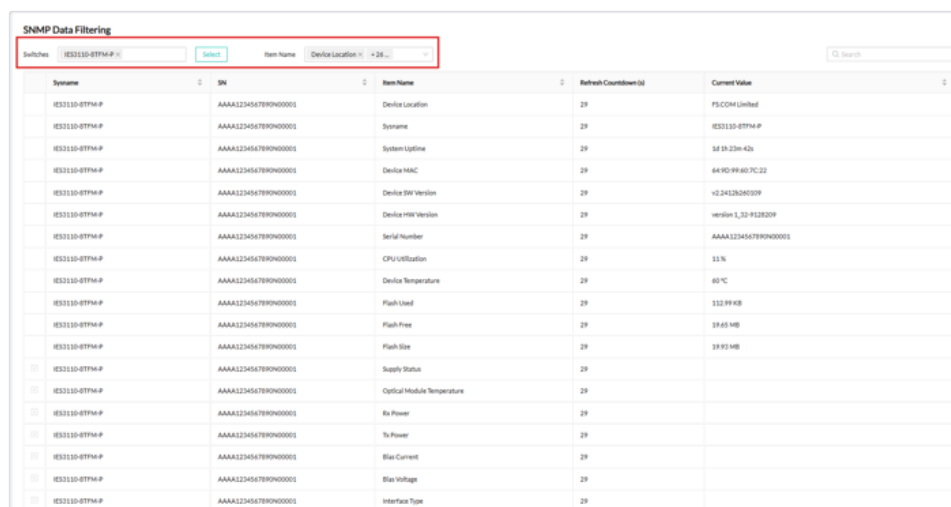
Prerequisites

Ensure that all the [prerequisites](#) are met. Otherwise, SNMP data might fail to be displayed on the “SNMP Data Filtering” page.

Procedure

1. Click **Monitor > SNMP Management > SNMP Data Filtering** from the navigation bar.
2. On the “SNMP Data Filtering” page, do the following operations as needed:
 - To display SNMP data of specific switches, click **Select** to select switches. You can select one or multiple switches.
 - To display SNMP data of specific monitoring items, select items from the **Item Name** drop-down list. You can select one or multiple monitoring items.

For supported monitoring items and descriptions, see the [Supported Items](#) section.



Sysname	SN	Item Name	Refresh Countdown (s)	Current Value
193110-07TH-P	AAAA1234567890000001	Device Location	29	FS.COM Limited
193110-07TH-P	AAAA1234567890000001	Sysname	29	193110-07TH-P
193110-07TH-P	AAAA1234567890000001	System Uptime	29	3d 1h 23m 42s
193110-07TH-P	AAAA1234567890000001	Device MAC	29	649D-99A0-7C22
193110-07TH-P	AAAA1234567890000001	Device SW Version	29	V2.3412826009
193110-07TH-P	AAAA1234567890000001	Device HW Version	29	version_1.30-9128209
193110-07TH-P	AAAA1234567890000001	Serial Number	29	AAAA1234567890000001
193110-07TH-P	AAAA1234567890000001	CPU Utilization	29	11%
193110-07TH-P	AAAA1234567890000001	Device Temperature	29	60°C
193110-07TH-P	AAAA1234567890000001	Flash Used	29	112.99 MB
193110-07TH-P	AAAA1234567890000001	Flash Free	29	18.65 MB
193110-07TH-P	AAAA1234567890000001	Flash Size	29	19.93 MB
193110-07TH-P	AAAA1234567890000001	Supply Status	29	
193110-07TH-P	AAAA1234567890000001	Optical Module Temperature	29	
193110-07TH-P	AAAA1234567890000001	Rx Power	29	
193110-07TH-P	AAAA1234567890000001	Tx Power	29	
193110-07TH-P	AAAA1234567890000001	Bias Current	29	
193110-07TH-P	AAAA1234567890000001	Bias Voltage	29	
193110-07TH-P	AAAA1234567890000001	Interface Type	29	

3. Check the filtered SNMP data.

Table 1. SNMP Data

Metric	Description
Sysname	The hostname of the switch.
SN	The serial number of the switch.

Item Name	The name of the item. An item means a metric.
Refresh Countdown	The countdown time to refresh the item value on the “SNMP Data Filtering” page.
Current Value	The latest value of the item, which is retrieved from the switch. Each item value is refreshed every 60 seconds.

Supported Items

On the “SNMP Data Filtering” page, AmpCon-Campus supports monitoring the following items:

Table 2. Supported Items for Filtering

Item	Description
Device Location	The physical location of the switch.
Sysname	The hostname of the switch.
System Uptime	The duration during which the switch has been running since its last reboot or startup.
Device MAC	The MAC address of the switch.
Device SW Version	The revision number of the switch software.
Device HW Version	The revision number of the switch hardware.
Serial Number	The serial number of the switch.
CPU Utilization	The CPU utilization, measured in percentage.
Device Temperature	The switch temperature, measured in Celsius (°C). NOTE For switches of the following models, the Device Temperature data is not displayed: • S3900-48T6S-R • S5500-48T6SP-R
Memory Used	The memory usage, measured in percentage.

	NOTE For switches of the IES3110-8TFM-P switch model, the Memory Used data is not displayed.
Memory Free	The free memory size. NOTE For switches of the following models, the Memory Free data is not displayed: • IES3110-8TFM-P • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F • S3900-48T6S-R • S5500-48T6SP-R
Memory Size	The total memory size. NOTE For switches of the following models, the Memory Size data is not displayed: • IES3110-8TFM-P • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F • S3900-48T6S-R • S5500-48T6SP-R
Flash Used	The used flash storage size. NOTE For switches of the following models, the Flash Used data is not displayed: • S3950-4T12S-R • S5800-48T4S • S5800-48MBQ

- S5850-48S6Q-R
- S5850-48B8C
- S5850-24B4C
- S5850-24XMG-U
- S8050-20Q4C
- S8550-16Q8C
- S5850C-24XMG2C
- S5850C-24S2C
- S3150-8T2FP
- S3260-8T2FP
- S3400-24T4FP
- S3700-24T4F
- S3900-48T6S-R
- S5500-48T6SP-R

Flash Free	The free flash storage size. NOTE For switches of the following models, the Flash Free data is not displayed: • S3950-4T12S-R • S5800-48T4S • S5800-48MBQ • S5850-48S6Q-R • S5850-48B8C • S5850-24B4C • S5850-24XMG-U • S8050-20Q4C • S8550-16Q8C • S5850C-24XMG2C • S5850C-24S2C • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F • S3900-48T6S-R • S5500-48T6SP-R
Flash Size	The total flash storage size. NOTE For switches of the following models, the Flash Size data is not displayed: • S3950-4T12S-R • S5800-48T4S • S5800-48MBQ • S5850-48S6Q-R • S5850-48B8C • S5850-24B4C • S5850-24XMG-U • S8050-20Q4C • S8550-16Q8C

	• S5850C-24XMG2C • S5850C-24S2C • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F • S3900-48T6S-R • S5500-48T6SP-R
Fan Speed	The fan speed, measured in Revolutions Per Minute (RPM).  NOTE For switches of the following models, the Fan Speed data is not displayed: • IES3110-8TFM-P • S3270-24TM-P • S3270-10TM-P • S3270-48TM • S3410-48TS-P • S3410-24TF-P • S3410-24TS-P • S3910-24TF • S3260-8T2FP • S3400-24T4FP
Fan Status	The fan status.  NOTE For switches of the following models, the Fan Status data is not displayed: • IES3110-8TFM-P • S3260-8T2FP • S3400-24T4FP
Supply Status	The status of the Power Supply Unit (PSU).  NOTE

	For switches of the following models, the Supply Status data is not displayed: • S3950-4T12S-R • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S3700-24T4F
Optical Module Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).
Rx Power	The amount of Rx power received by the optical module. It's measured in dBm.
Tx Power	The amount of Tx power sent by the optical module. 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).
PoE Power	The available power from the Power Sourcing Equipment (PSE) through the switch port. It's measured in watts (W).  NOTE For switches of the following models, the PoE Power data is not displayed: • IES3110-8TFM-P • S5850-24XMG-U • S3150-8T2FP • S3260-8T2FP • S3400-24T4FP • S5500-48T6SP-R
Interface Type	The type of switch port, distinguished by the physical or link protocols immediately below the network layer in the protocol stack.

Operational Status	The status of the switch port.
Port Speed	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of n, then the speed of the switch port is in the range of n-500,000 to n+499,999. NOTES - For switch ports that do not vary in bandwidth or for those where no accurate estimation can be made, this value contains the nominal bandwidth. - For a sub-layer that has no concept of bandwidth, this value is zero.
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.
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.

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 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 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.

Viewing SNMP Trend Graphs

By using the “SNMP Visualization” page, you can view SNMP trend graphs for all imported FSOS switches.

[Prerequisites](#)

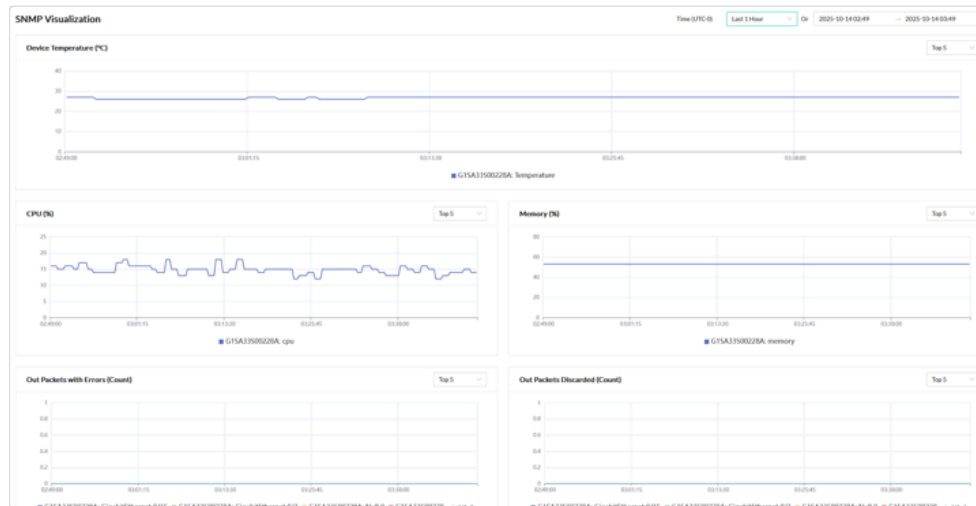
[Procedure](#)

Prerequisites

Ensure that all the [prerequisites](#) are met. Otherwise, SNMP data might fail to be displayed on the “SNMP Visualization” page.

Procedure

1. Click **Monitor > SNMP Management > SNMP Visualization** from the navigation bar.
2. Check the SNMP trend graphs.



The following trend graphs are provided:

Table 1. Supported Trend Graphs

Graph Name	Description
Device Temperature	The switch temperature, measured in Celsius (°C). NOTE For switches of the following models, the Device Temperature data is not displayed: • S3900-48T6S-R • S5500-48T6SP-R

CPU	The CPU utilization for the latest 5 seconds, measured in percentage.
Memory	The used memory, measured in percentage.
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 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.
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.
In Packets Discarded	The number of incoming packets that the switch port discards due to reasons like buffer exceptions. NOTES

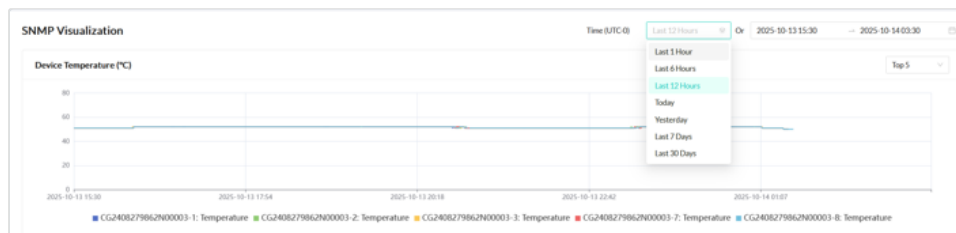
	• The metric value keeps increasing until it reaches the allowed maximum value 4,294,967,295 ($2^{32} - 1$). • After the metric value reaches 4,294,967,295, the value will be reset to 0 and then start counting again.
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
In Octets	The number of octets (8-bit bytes) received by the switch port.

3. On the “SNMP Visualization” page, filter data as needed:

- To specify the time range for the data display, select a time range or specify the start date and end date (within the last 30 days) in the **Time (UTC-0)** section.

NOTES

- The time in the **Time (UTC-0)** section is based on the **UTC-0** time zone.
- By default, the data in the last 5 minutes are displayed.

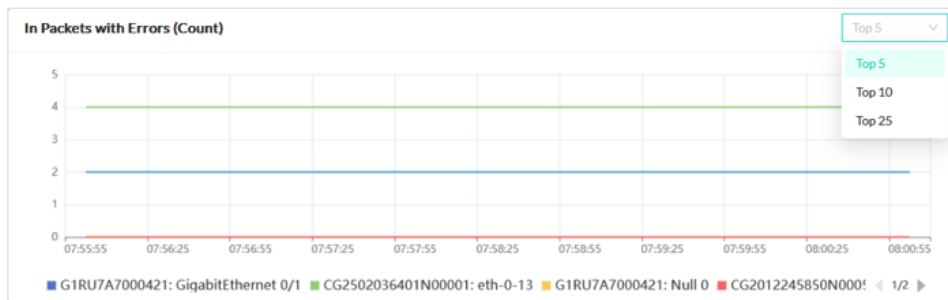


- To specify how many ports you want to monitor, select one of the following options:
 - **Top 5:** The 5 switch ports with the largest values. By default, **Top 5** is selected.
 - **Top 10:** The 10 switch ports with the largest values.
 - **Top 25:** The 25 switch ports with the largest values.

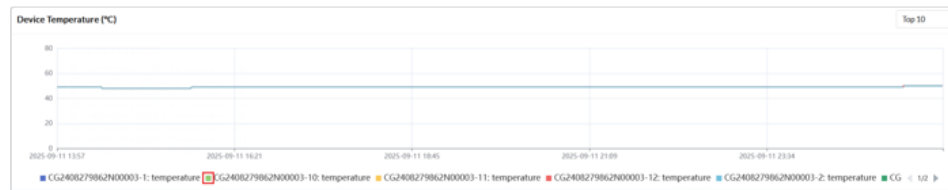
NOTES

- Only the ports in **Up** status can be displayed.
- Even though **Top X** (such as **Top 5**) is selected, you might see less than the selected number of switch ports in the trend graph when some ports are down.
- For **Device Temperature**, **CPU**, and **Memory** trend graphs, selecting **Top X** will display the switches with the largest

temperature, CPU, and memory values, instead of the switch ports with the largest values.



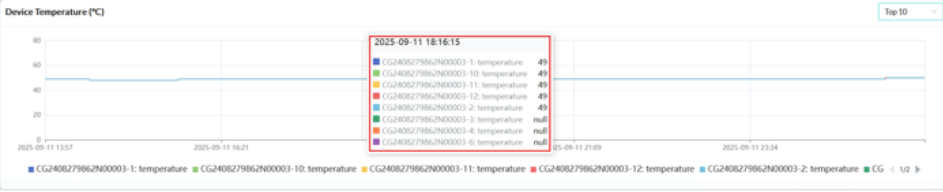
- To display or hide the data of a switch port, click the square before the port.



- To view the metric details at a specific time point, hover your mouse over that time point.

NOTES

- For all the trend graphs, pay attention to the following notes:
 - If a switch is connected with AmpCon-Campus and then disconnects during the selected time range, the metric values after the disconnection are displayed as **null**.
 - If a switch is always disconnected from AmpCon-Campus throughout the selected time range, the metric values will not be displayed.
 - After you remove an FSOS switch from AmpCon-Campus, the metric values will not be displayed.
- For **Out Packets with Errors, Out Packets Discarded, In Packets with Errors, In Packets Discarded, Out Octets, and In Octets** trend graphs, pay attention to the following notes:
 - If a switch port is up at any time of the selected time range, the metric values before the port is down are displayed during the port down period.
 - If a switch port is always down throughout the selected time range, the metric values of the port will not be displayed.



Onboarding PicOS Switches

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

To onboard PicOS switches, two options are provided: importing switches to AmpCon-Campus and deploying switches through Zero Touch Provisioning (ZTP).

- If the switches to be managed have PicOS installed, you can onboard these switches by importing them to AmpCon-Campus directly.
- If the switches to be managed don't have PicOS installed, or though the switches have PicOS installed but you want to onboard these switches through ZTP, you can use AmpCon-Campus to deploy these switches through ZTP.

NOTES

- Zero Touch Provisioning (ZTP) is a technology for automated deployment and configuration of unconfigured network devices without manual intervention.
- Importing switches is not a ZTP method, which means that you still need to connect to the switches and do some operations on the switch side, such as obtaining IP addresses from the switches. The importing switch process doesn't push switch configurations.
- Deploying switches through ZTP is a ZTP method used for automated deployment of switches. After you reboot the switches, AmpCon-Campus will deploy the switches automatically. During the ZTP process, AmpCon-Campus will push pre-configured configurations to the switches.
- Integrated hardware and software switches have PicOS installed. To onboard these switches, you can import these switches to AmpCon-Campus directly, or you can deploy these switches through ZTP.

See the following child topics:

- [Importing PicOS Switches](#)
- [Deploying PicOS Switches through ZTP](#)

Importing PicOS Switches

If the switches to be managed have PicOS installed, you can onboard these switches by importing them to AmpCon-Campus directly.

[Before You Begin](#)

[Import Procedure](#)

[Automatically Importing a Switch](#)

[Manually Importing a Switch](#)

[Checking Importing Results](#)

Before You Begin

Before you import switches, ensure that the following prerequisite tasks have been completed:

Task	Reference Link
Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
Log in to the AmpCon-Campus UI with a global user or group user of the SuperAdmin role.	• Working with the User Interface
Obtain an AmpCon-Campus license (containing hardware IDs of the switches to be onboarded) from the FS sale team. Import the AmpCon-Campus license to AmpCon-Campus.	• Importing Licenses for Imported Switches
Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switches, create a non-global system configuration.	• Adding System Configurations
Ensure that the switches to be imported are supported by AmpCon-Campus.	• Supported PicOS Switches
Ensure that the Secure Shell (SSH) protocol is enabled on these switches.	• No Reference Link

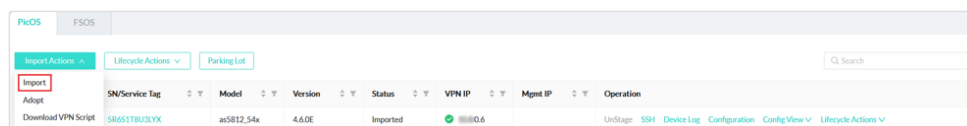
SSH is enabled on PicOS switches by default.	
Ensure that the switches are able to connect to the AmpCon-Campus server.	• No Reference Link
If a firewall is configured between AmpCon-Campus and the switches, allow outbound access on the following ports to the management port of each switch. • TCP: 22 • TCP: 9339 • TCP: 830	• No Reference Link

Import Procedure

Automatically Importing a Switch

If you have obtained the IP addresses of the switches, you can use the automatic import method. Follow the steps:

1. Log in to the AmpCon-Campus UI with a global user or group user.
2. Click **Wired > Switches** from the navigation bar. In the **PicOS** tab, hover over **Import Actions**, and then click **Import**.



3. In the pop-up window, configure as follows:
 - If you log in to AmpCon-Campus UI with a global user, input the following information:

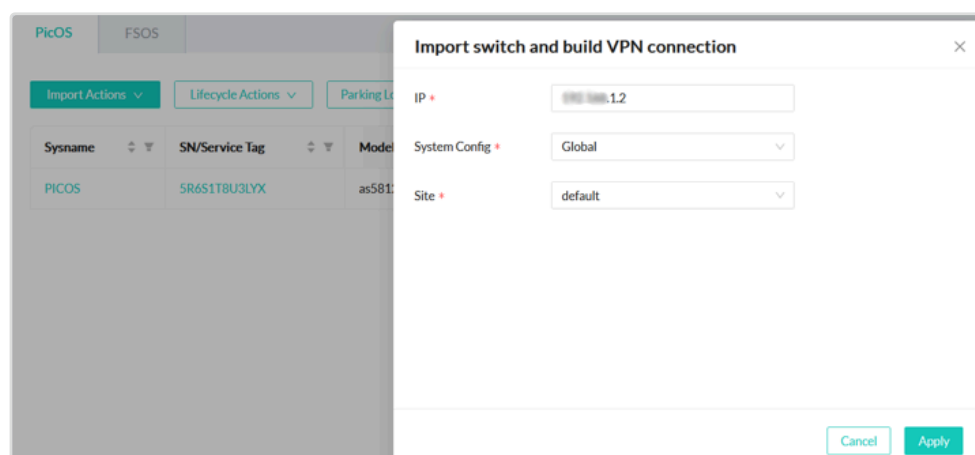


Table 1. Importing a Switch with a Global User

Parameter	Description
IP	Enter the IP address of the switch.
System Config	Select the appropriate system configuration. The selected system configuration needs to contain the default username and password of the switch. NOTES • Ensure that the system configuration contains the default username and password of the switch. • Ensure that AmpCon-Campus can connect with the License Portal. For more information, see Checking License Portal Connectivity.
Site	Select a site to which the switch belongs. For more information, see Adding a Site .

- If you log in to AmpCon-Campus UI with a group user, input the following information:

The screenshot shows the AmpCon-Campus UI. In the background, there is a table with the following data:

Sysname	SN/Service Tag	Model
PICOS	5R6S1T8U3LYX	as581

Overlaid on this is a dialog box titled "Import switch and build VPN connection". It contains the following fields:

- IP: 192.168.1.2
- System Config: Global
- Site: default
- Select Group: fs_group

At the bottom right of the dialog box are "Cancel" and "Apply" buttons.

Table 2. Importing a Switch with a Group User

Parameter	Description
IP	Enter the IP address of the switch.
System Config	Select the appropriate system configuration. The selected system configuration needs to contain the default username and password of

the switch.

NOTES

- Ensure that the system configuration contains the default username and password of the switch.
- Ensure that AmpCon-Campus can connect with the License Portal. For more information, see [Checking License Portal Connectivity](#).

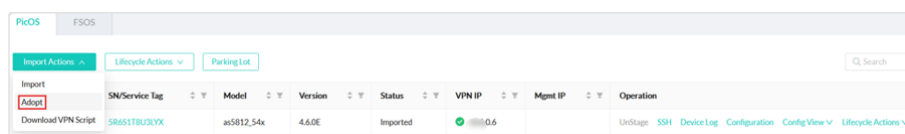
Site	Select a site to which the switch belongs.
Group	Select a group to which the switch belongs.

4. Click **Apply**.

Manually Importing a Switch

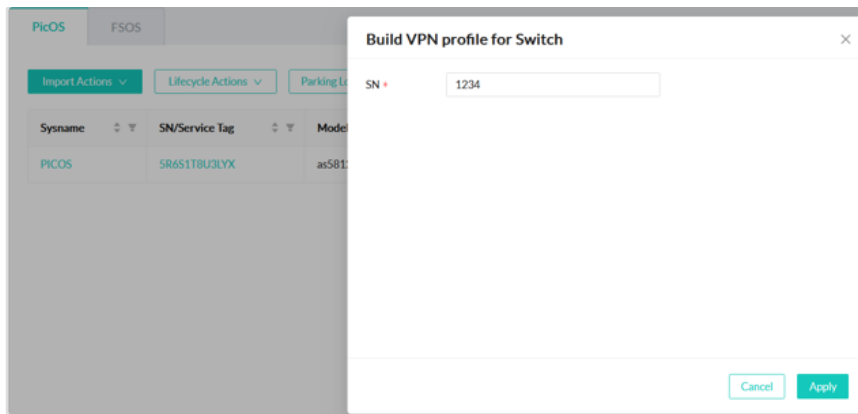
If you haven't obtained the IP addresses of the switches, you can use the manual import method. Follow the steps:

1. Generate the tunnel keys based on the input serial number. These keys are used to ensure that the VPN tunnel between the switch and the AmpCon-Campus server is encrypted.
 - a. Log in to the AmpCon-Campus UI with a global user or group user.
 - b. Click **Wired > Switches** from the navigation bar. In the **PicOS** tab, hover over **Import Actions**, and then click **Adopt**.

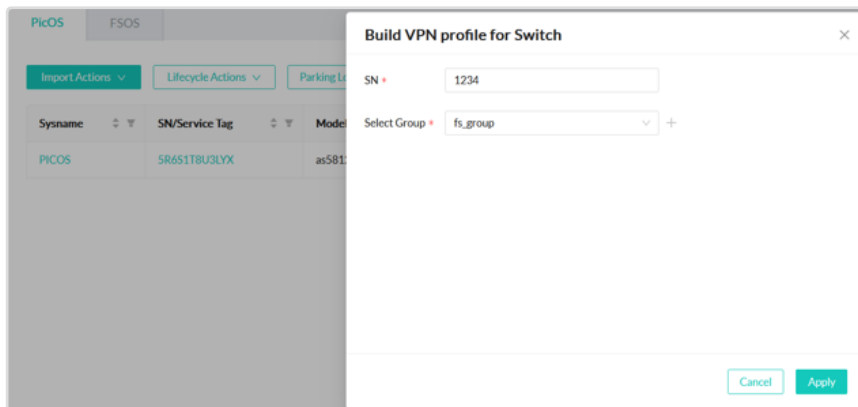


- c. In the pop-up window, configure as follows:

If you log in to AmpCon-Campus UI with a global user, enter the serial number of the switch in the **SN** field.



If you log in to AmpCon-Campus UI with a group user, enter the serial number of the switch in the **SN** field, and then select a switch group to which the switch belongs.



d. Click **Apply**.

2. Download the VPN script, and then run it on the switch. The script will retrieve the tunnel keys and establish a VPN tunnel between the switch and the AmpCon-Campus server.

a. Hover over **Import Actions**, and then select **Download VPN Script**. Then, the VPN script is downloaded to your local machine.

b. Copy the script to the PicOS switch.

c. SSH log in to the switch, enter the Linux shell mode, and then run the following commands:

```
curl -o /opt/auto-deploy/auto-deploy.conf -k -v
https://<ampcon-server-ip>/rma/file/agent/auto-deploy.conf
```

```
sudo ./enable_switch_vpn.sh <ampcon-server-ip>
```

NOTES

- You must run the first command to replace the **/opt/auto-deploy/auto-deploy.conf** file before running the second

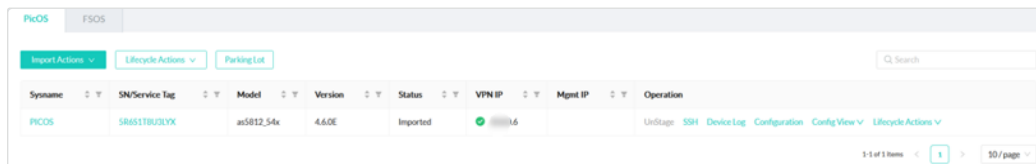
command to import the switch. Otherwise, the switch import might fail.

- You need to replace *<amp;con-server-ip>* with the IP address of your AmpCon-Campus server.

After you run the VPN script, the PicOS switch will be imported to AmpCon-Campus.

Checking Importing Results

Click **Wired > Switches** from the navigation bar. In the **PicOS** tab, check whether the imported switch is displayed in **Imported** status.



The screenshot shows the 'PicOS' tab in the AmpCon-Campus interface. It features a table with columns for Sysname, SN/Service Tag, Model, Version, Status, VPN IP, Mgmt IP, and Operation. A single switch is listed with the status 'Imported' and a green checkmark in the VPN IP column. The interface also includes buttons for 'Import Actions', 'Lifecycle Actions', and 'Parking Lot', along with a search bar and pagination controls.

Sysname	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation
PICOS	5B651TRU2LYX	as5812-54x	4.6.0E	Imported	 1.6		UnStage SSH Device Log Configuration Config View Lifecycle Actions

For more information about the PicOS tab, see [Viewing Managed PicOS Switches](#).

Deploying PicOS Switches through ZTP

If the switches to be managed don't have PicOS installed, or though the switches have PicOS installed but you want to onboard these switches through ZTP, you can use AmpCon-Campus to deploy these switches through ZTP.

After you deploy switches through ZTP, these switches can be deployed and managed by AmpCon-Campus.

See the following child topics:

- [How ZTP Works](#)
- [Quick Deployment Guide](#)
- [Preparing Configurations](#)
- [Provisioning New Switches through ZTP](#)

How ZTP Works

Check the following workflows to understand how ZTP works.

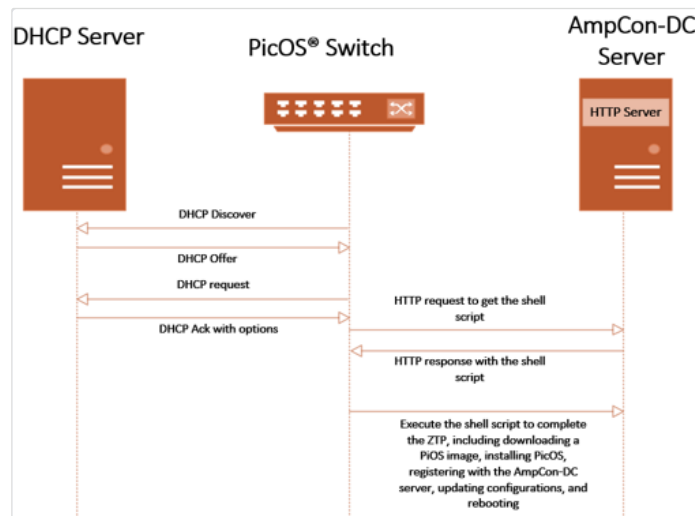
[Deploying White-Box Switches](#)

[Deploying Integrated Hardware and Software Switches](#)

Deploying White-Box Switches

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

Figure 1. Management Workflow of White-Box Switches

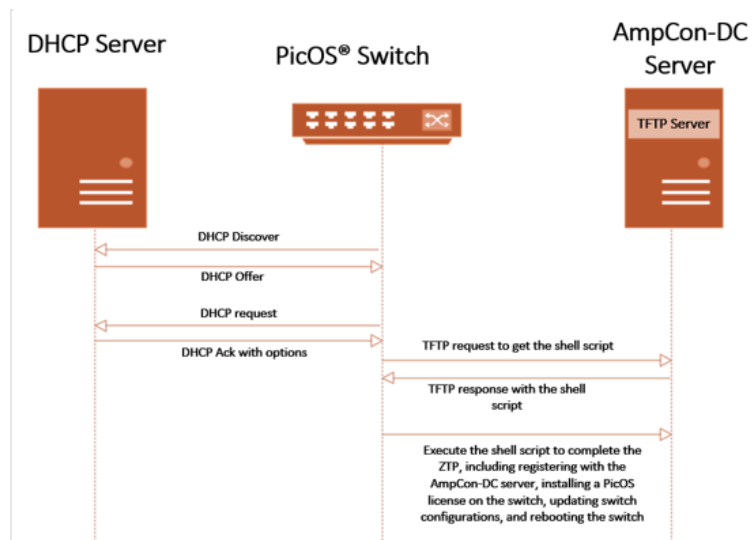


1. After a switch is powered on, the switch sends DHCP Discover to get an IP address, and the DHCP server provides the switch with an IP address.
2. The switch sends a request to the DHCP server, and the DHCP server sends a response including the HTTP server address.
3. The switch sends an HTTP request 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 and its license, registering with the AmpCon-Campus server, updating switch configurations, and rebooting the switch.

Deploying Integrated Hardware and Software Switches

The workflow of deploying 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 the AmpCon-Campus server, installing a PicOS license on the switch, updating switch configurations, and rebooting the switch.

Quick Deployment Guide

This topic describes how to complete the switch deployment through ZTP. Once successfully deployed, the PicOS switches are classified as managed devices of AmpCon-Campus.

[Guidelines](#)

[Prerequisites](#)

[Procedure](#)

[Deploying White-Box Switches](#)

[Deploying Integrated Hardware and Software Switches](#)

Guidelines

Pay attention to the following points. Or else, switches will fail to be deployed.

- Be careful when you configure system configurations:
 - Ensure that the entered **Device Default Login User** and **Device Default Password** are correct and can be used to log in to the switch.
 - If the switch don't use the **Device Default Login User** and **Device Default Password** in the global system configuration, create a non-global system configuration for the switch, and ensure the **Device Default Login User** and **Device Default Password** match with the switch.
 - Ensure that the AmpCon-Campus server can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see [Checking License Portal Connectivity](#).
 - Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations.
- If you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-Campus parking lot. For more information, see [Managing the Parking Lot](#).

To continue deploying the switches in the parking lot, follow these steps:

- a. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar.
- b. On the "Switches" page, click **Parking Lot**.
- c. Locate the switch to be deployed, and then click **Create Config** to add a switch configuration. After you add the switch configuration, the switch will be listed on the "Switches" page with the **Configured** status.
- d. Continue to provision the switch through ZTP to complete the switch deployment.

Prerequisites

Before you deploy PicOS switches, ensure that the following prerequisite tasks have been completed:

Table 1. Prerequisite Tasks and Links

Task	Reference Link
Install the AmpCon-Campus server successfully.	• Platform Installation Workflow
Log in to the AmpCon-Campus UI with an account of the SuperAdmin role.	• Working with the User Interface
Ensure that the switches to be onboarded are supported by AmpCon-Campus.	• Supported PicOS Switches
For switches that have PicOS installed, ensure that the Secure Shell (SSH) protocol is enabled on these switches. SSH is enabled on PicOS switches by default.	• No Reference Link
Ensure that the switches are able to connect to the AmpCon-Campus server.	• 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

Procedure

Deploying White-Box Switches

To deploy a white-box switch through ZTP, see the following diagram and tasks:

Figure 1. ZTP Workflow for White-Box Switches

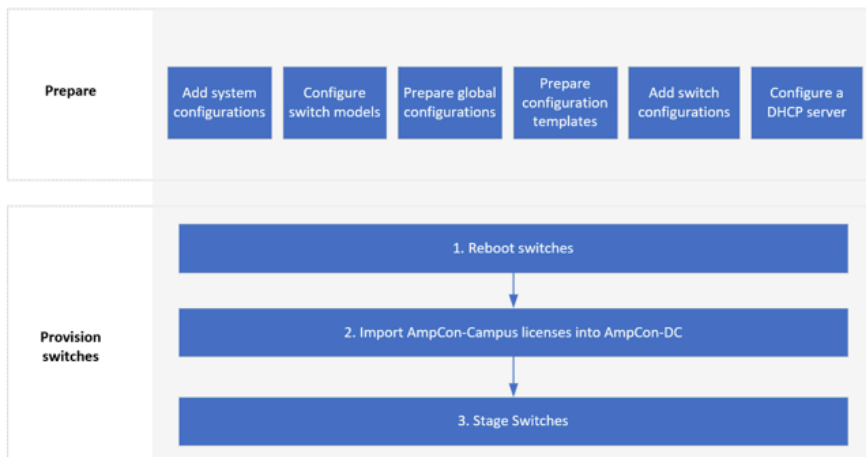


Table 2. White-Box Switch Deployment Tasks

Task	Reference Link
1. Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
2. Click the Switch Model tab. In this tab, configure the switch model related to the switch.	• Configuring Switch Models
3. Click the Global Configuration tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
4. Click Wired > Config Templates from the navigation bar. Click the Template List tab. In this tab, check whether an existing configuration template meets your need. If not, click the New Template tab, and then add a new configuration template.	• Managing Configuration Templates • Adding Configuration Templates
5. Click Wired > Wired Profiles from the navigation bar. Click the Switch Configuration tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations

6. Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
7. Provision the switch through ZTP to complete the switch deployment.	• Provisioning a White-Box Switch

Deploying Integrated Hardware and Software Switches

To deploy an integrated hardware and software switch through ZTP, see the following diagram and steps:

Figure 2. ZTP Workflow for Integrated Hardware and Software Switches

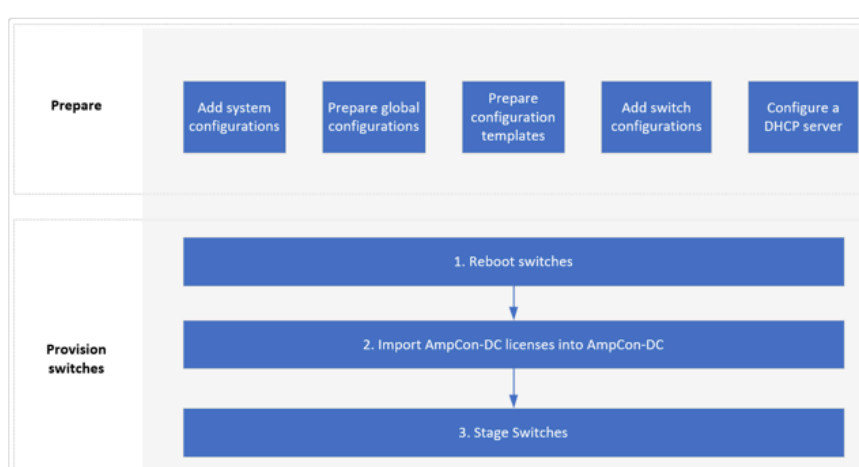


Table 3. Integrated Hardware and Software Switch Deployment Tasks

Task	Reference Link
1. Click Wired > Wired Profiles from the navigation bar of the AmpCon-Campus UI. Click the System Configuration tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
2. Click the Global Configuration tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
3. Click Wired > Config Templates from the navigation bar. Click the Template List tab. In this tab, check whether an existing configuration template meets your need.	• Managing Configuration Templates

If not, click the New Template tab, and then add a new configuration template.	• Adding Configuration Templates
4. Click Wired > Wired Profiles from the navigation bar. Click the Switch Configuration tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations
5. Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
6. Provision the switch through ZTP to complete the switch deployment.	• Provisioning an Integrated Hardware and Software Switch

Preparing Configurations

To deploy switches through ZTP, you need to prepare the required configurations first.

See the following child topics:

- [Configuring Global Configurations](#)
- [Adding Switch Configurations](#)
- [Optional: Managing Global and Switch Configurations](#)
- [Configuring Switch Models](#)
- [Adding System Configurations](#)
- [Configuring a DHCP Server](#)

Configuring Global Configurations

To deploy switches through ZTP, you must prepare global configurations. A global configuration file contains global configurations to be pushed to switches during the switch deployment process.

When you add a switch configuration, you must select a global configuration file. For more information, see [Adding a Switch Configuration](#).

[Adding a Global Configuration](#)

[Viewing a Global Configuration](#)

[Editing a Global Configuration](#)

Adding a Global Configuration

To add a global configuration, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar.
2. In the **Global Configuration** tab, input the following information, and then click **Generate**.

The screenshot shows the 'Admin Global Config Edit' interface. It features a navigation bar with tabs: 'Global Configuration' (selected), 'Switch Configuration', 'Config File View', 'Switch Model', and 'System Configuration'. The main form area is titled 'Admin Global Config Edit' and contains several input fields: 'Switch Model' (a dropdown menu with 'S5860-48MG-U' selected), 'Global Config Name' (a text input with '2025-12-26-glob-S586...' and a 'test-xfx' button), 'Generic Global File' (a file browser with 'test1.txt' selected), and 'Security Global File' (a file browser with 'test2.txt' selected). At the bottom of the form are 'Generate' and 'Reset' buttons. Below the form is a 'Historical Configuration' section with a search bar and a list item 'ag5648'.

Table 1. Global Configuration Parameters

Parameter	Description
Switch Model	The switch model.
Global Config Name	The name of the global configuration file.
Generic Global File	Select a .txt file with general global configurations to be pushed to the switch. Example configuration in the .txt file: set vlans vlan-id 303

Security Global File	Select a .txt file with security-related configurations to be pushed to the switch. Example configuration in the .txt file: <pre>set system login user automation2 authentication plain-text-password 12345678</pre> <pre>set system login user automation2 class super-user</pre> NOTE You might also add security-related configurations in the system configuration. If some configurations in the system configuration and in the uploaded Security Global File here overlap: - For the overlapping configurations, the configurations in the uploaded Security Global File here will overwrite the configurations in the system configuration. - For the non-overlapping configurations, the configurations in both the system configuration and the uploaded Security Global File here will be pushed to the switches.
-----------------------------	--

3. In the **Admin Global Config Preview** section, click **Save** to confirm the configurations retrieved from the **Generic Global File** and the **Security Global File**.

You can also click **Edit** and then click **Save** to modify the configurations.

The screenshot shows the 'Admin Global Config Edit' interface. On the left, there are fields for 'Switch Model' (S5860-48MG-U), 'Global Config Name' (2025-12-26-glob-5586...), 'Generic Global File' (test1.txt), and 'Security Global File' (test2.txt). Below these are 'Generate' and 'Reset' buttons. On the right, the 'Admin Global Config Preview' section is highlighted with a red border. It contains the following configuration text:

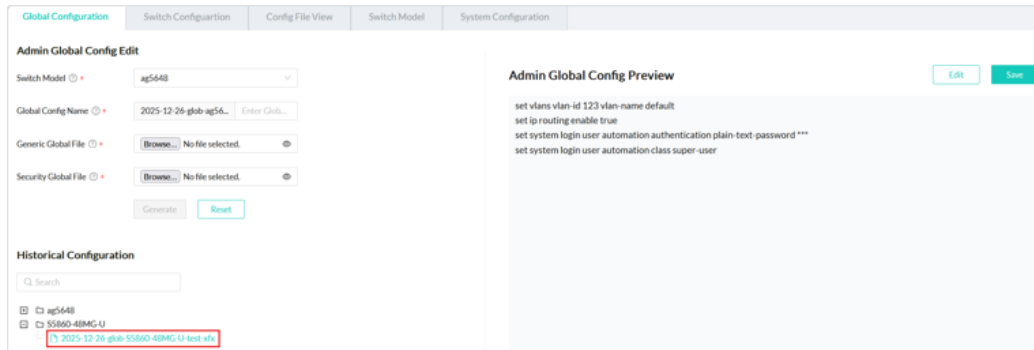
```
set vlan vlan-id 123 vlan-name default
set ip routing enable true
set system login user automation authentication plain-text password 234
set system login user automation class super-user
```

At the bottom left, there is a 'Historical Configuration' section with a search bar and a list item 'ap5648'.

Viewing a Global Configuration

In the **Historical Configuration** section, you can see all the added global configurations, which are grouped by switch model.

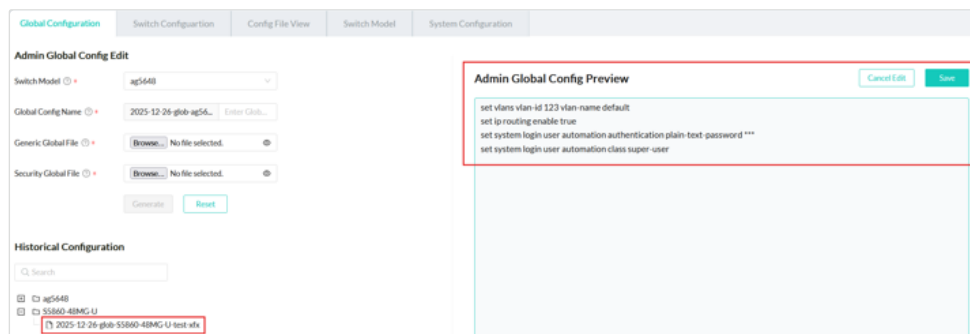
To check the configurations in a global configuration file, click the switch model, and then click the global configuration file name.



Editing a Global Configuration

To edit a global configuration, follow these steps:

1. In the **Historical Configuration** section, locate the global configuration, and then click it.
2. In the **Admin Global Config Preview** section, click **Edit**.
3. Edit the configurations as needed, and then click **Save**.



Adding Switch Configurations

To deploy switches through normal ZTP, you must prepare switch configurations for each switch.

[Overview](#)

[Prerequisites](#)

[Procedure](#)

[Adding a Switch Configuration](#)

[Adding Multiple Switch Configurations in Batches](#)

[Optional Operations](#)

[Viewing or Editing Switch Configurations](#)

[Checking the Switch Status](#)

Overview

A switch configuration contains the following configurations:

- The SN or service tag of the switch.
- The switch model of the switch.
- The location of the switch.
- The fabric to which the switch belongs.
- The global configuration file and configuration templates.
- Whether to enable automatic configuration backup for the switch.
- The system configuration related to the switch.

All these configurations are important for deploying switches through normal ZTP.

Prerequisites

Ensure that the global configuration files and configuration templates for the switches to be deployed have been created. For more information, see [Adding Global Configurations](#) and [Adding a Configuration Template](#).

Procedure

You can add switch configurations one by one or add multiple switch configurations in batches by using a JSON file.

Adding a Switch Configuration

To add one switch configuration, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar.
2. In the **Switch Configuration** tab, input the following information:

Global Configuration
Switch Configuration
Config File View
Switch Model
System Configuration

Switch Config Edit
Upload by JSON

Switch SN / Service Tag ⓘ * testsn

Switch Model ⓘ * ag5648

Deployment Location ⓘ * New_York

Site ⓘ * default

Select Global Config ⓘ * 2025-11-25-glob-ag5648-4610-30p

Select Site Template ⓘ * test1 +

Option Post-Deployed
☒ Backup Config
System config

Historical Switch Config Edit
Next

Search

ag5648

Table 1. Switch Configuration Parameters

Parameter	Description
Switch SN/Service Tag	The SN or service tag of the switch. The value can contain only letters and numbers.
Switch Model	The switch model.
Deployment Location	The location where the switch exists, such as New_York. The value can contain only the special character <code>_</code>, letters, and numbers.
Site	The site that the switch belongs to. - The default site is selected by default. - To add a new site, see Adding a Site.
Select Global Config	The global configuration file that contains configurations to be pushed to the switch. If the global configuration file in the drop-down list doesn't meet your needs, add a new global configuration file. For more information, see Configuring Global Configurations.
Select Site Template	The configuration template to use. - Click + to add multiple configuration templates if needed. - If the configuration template file in the drop-down list doesn't meet your needs, add a new configuration template file. For more

	information, see Adding a Configuration Template .
Option Post-Deployed	Select Backup Config to enable automatic switch configuration backup after the switch is deployed. After you select Backup Config, AmpCon-Campus will back up the switch configurations at 22:00 in the UTC-0 time zone every 3 days. You can change the interval and backup time. For more information, see Backing Up Configurations Automatically.

- Click **System Config**. In the pop-up window, select the system configuration related to the switch.

NOTE

Ensure that the **Device Default Login User** and **Device Default Password** on the “System Configuration” page can be used to log in to these switches. Or else, the switch will fail to be deployed.

The screenshot displays the 'Switch Configuration' page. At the top, there are tabs for 'Global Configuration', 'Switch Configuration' (active), 'Config File View', 'Switch Model', and 'System Configuration'. The main section is titled 'Switch Config Edit' and includes an 'Upload by JSON' button. Below this are several input fields: 'Switch SN / Service Tag' (testsn), 'Switch Model' (ag5648), 'Deployment Location' (New_York), 'Site' (default), 'Select Global Config' (2025-11-25-glob-ag5648-4610-30p), and 'Select Site Template' (test1). The 'Option Post-Deployed' section has a checked box for 'Backup Config' and a button for 'System Config' which is highlighted with a red box. At the bottom, there is a 'Historical Switch Config Edit' section with a search bar and a list of configurations, including 'ag5648'.

- Click **Next**. You can see an input section, which is related to the selected configuration template. Enter the relevant information.

5. Click **Save**.

6. In the **Preview Config** pop-up window, preview the configurations included in the global configuration file and configuration templates.

7. Click **Save**. The switch configuration is added now. On the “Switches” page, you can see the switch status is shown as **Configured**.

Adding Multiple Switch Configurations in Batches

To add multiple switch configurations in batches by uploading a JSON file, follow these steps:

1. Prepare a JSON file with switch configurations. See the following example:

NOTES

- You can add switch configurations for only the switches that haven't been managed by AmpCon-Campus. For more information, see [Viewing Managed PicOS Switches](#).
- The **retrieve_config** field is configured to enable or disable automatic switch configuration backup after the switch is deployed. For more information, see [Backing Up Configurations Automatically](#).
- The configurations in the **default_config_param** field will be pushed to all switches you specified in the **sn** field.

- You can add configurations for specific switches in the **unique_config_param** field. These configurations will be pushed to only these specified switches.
- All the configuration templates specified in the **default_config_param** and **unique_config_param** fields must be included in the **site_template_name** field.
- Ensure that the configurations in the **default_config_param** and **unique_config_param** fields match the configuration template used. For example, in the **unique_config_param** field, "**vlan_id**": "**99**" and "**vlan_name**": "**99**" are added to the **template_2** section. If the configuration template **template_2** doesn't contain the configuration **set vlans vlan-id {{ vlan_id }} vlan-name {{ vlan_name }}**, the JSON file will fail to be imported. To check the configurations included in a configuration template, see [Viewing or Editing a Configuration Template](#).

```
{
  "sn": ["EC1631000062", "EC1631000063"],
  "hardware_model": "ag5648",
  "location": "Beijing",
  "global_config_name": "2025-12-8-glob-ag5648-test-xfx",
  "site_template_name": ["template_2"],
  "retrieve_config": true,
  "default_config_param": {
    "template_2": {
      "vlan_id": "12",
      "vlan_name": "23"
    }
  },
  "unique_config_param": {
    "EC1631000062": {
      "template_2": {
        "vlan_id": "99",
        "vlan_name": "99"
      }
    }
  },
  "system_config_name": {
    "EC1631000062": "Global",
```

```
"EC1631000063": "Global"
}
}
```

2. In the AmpCon-Campus UI, click **Wired > Wired Profiles**.
3. In the **Switch Configuration** tab, click **Upload by JSON** from the navigation bar.
4. Click or drag a file to upload the JSON file.
5. Click **Upload**.

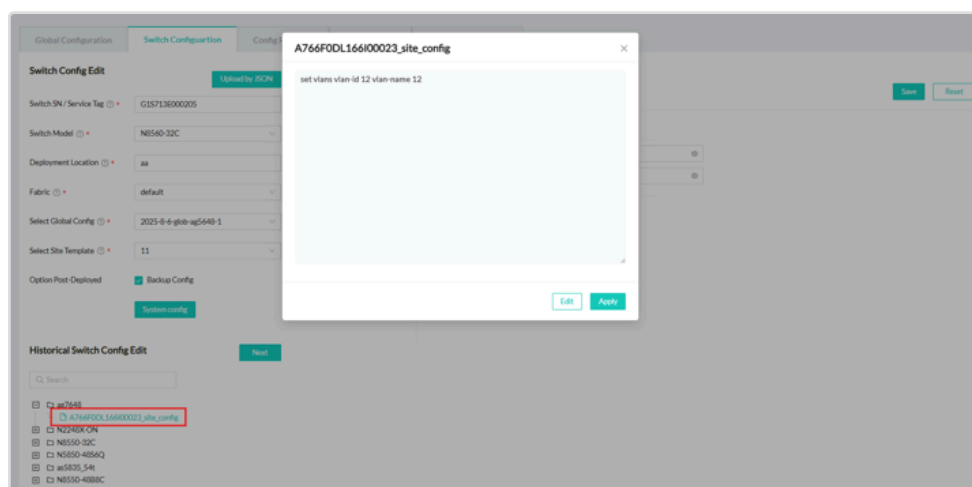
Optional Operations

Viewing or Editing Switch Configurations

In the **Historical Switch Config Edit** section, you can see all the added switch configurations, which are grouped by switch models.

To edit a switch configuration, follow these steps:

1. Locate the global configuration, and then click it.



2. In the pop-up window, click **Edit**.
3. Edit the configurations as you need.
4. Click **Apply**.

Checking the Switch Status

After you add a switch configuration, click **Wired > Switches** from the navigation bar, and then check whether the switch status is shown as **Configured** in the **PicOS** tab.

If not, locate the switch, and click **Device Log** to see more details.

For more information about the **PicOS** tab, see [Viewing Managed PicOS Switches](#).

Picos		FSOS											
Import Actions		Lifecycle Actions		Parking List		Search							
Sysname	Site/Service Tag	Model	Version	Status	VPN IP	Host IP	Operation						
PICOS	46255472336032_DEC0M	S5870-48T6S	4.7.0E	DEC0M	10.0.0.26		Unlodge	Device Log	Configuration	Config View	Lifecycle Actions		
PICOS	462554723360308	AS4625-54P	4.7.0E	Provisioning Success	10.0.22		Unlodge	SSH	Device Log	Configuration	Config View	Lifecycle Actions	
PICOS	46255472336032	AS4625-54T	4.7.0E	Provisioning Success	10.0.6		Unlodge	SSH	Device Log	Configuration	Config View	Lifecycle Actions	
PICOS	626A02A0900594	S5860-25SQ	4.7.0E-EC1	Provisioning Success	10.0.26		Unlodge	SSH	Device Log	Configuration	Config View	Lifecycle Actions	

Optional: Managing Global and Switch Configurations

In the **Config File View** tab, you can manage all added global configurations and switch configurations (also called site configurations).

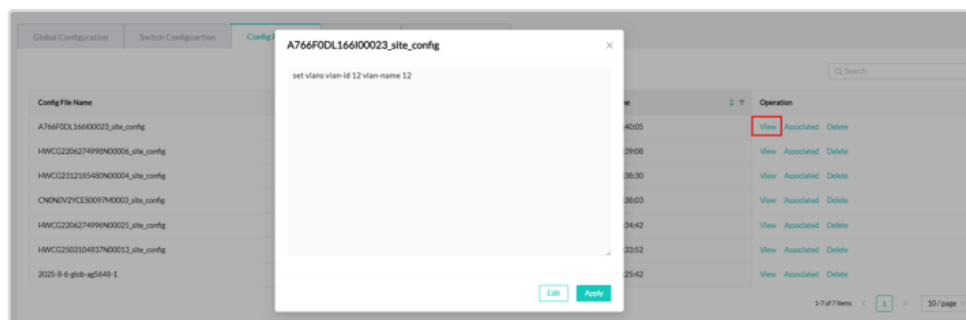
[Viewing or Editing Global and Site Configuration Files](#)

[Checking Switches Associated with a Configuration File](#)

[Deleting a Configuration File](#)

Viewing or Editing Global and Site Configuration Files

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar.
2. Click the **Config File View** tab, locate the configuration file, and then click **View**. You can see a pop-up window with detailed configurations.
3. To close the pop-up window, click the close icon.
4. To edit the configurations, click **Edit**, modify the configurations, and then click **Apply**.



Checking Switches Associated with a Configuration File

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar.
2. Click the **Config File View** tab, locate the configuration file, and then click **Associated**. You can see the switches that are associated with the configuration file.



3. To close the pop-up window, click the close icon.

Deleting a Configuration File

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar.
2. Click the **Config File View** tab, locate the configuration file, and then click **Delete**.
3. Click **Yes** to confirm the deletion.

NOTE

If a configuration file is still associated with one or multiple switches, the configuration file can't be deleted.

Global Configuration Switch Configuration Config File View Switch Model System Configuration						
Q Search						
Config File Name	Model	Type	Last Update Time	Operation		
A7MFDL16000023_site_config	ag764B	site	2025-06-12 04:40:05	View	Associated	Delete
HWC220627499N00006_site_config	N8550-4856Q	site	2025-06-12 04:39:08	View	Associated	Delete
HWC220218548N00004_site_config	ac5835_S4t	site	2025-06-12 04:38:30	View	Associated	Delete
CNDN0V2YCE50097M0003_site_config	N2248K-ON	site	2025-06-12 04:38:03	View	Associated	Delete
HWC220627499N000025_site_config	N8550-32C	site	2025-06-12 04:34:42	View	Associated	Delete
HWC2202104937N00013_site_config	N8550-4888C	site	2025-06-12 04:33:52	View	Associated	Delete
2025-8-6-global-ag564B-1	ag564B	global	2025-08-06 02:25:42	View	Associated	Delete
1-7 of 7 items 1 30 / page						

Configuring Switch Models

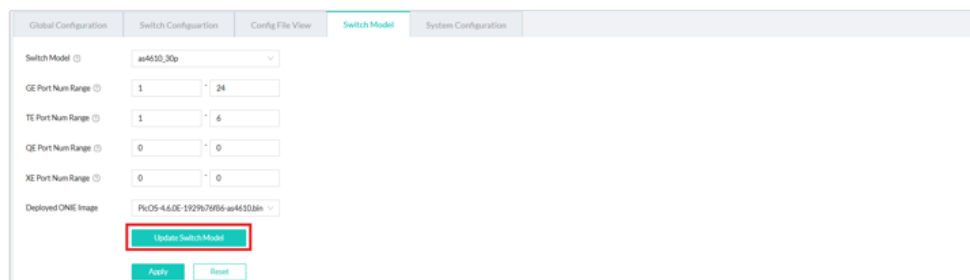
To deploy white-box PicOS switches, you must configure each switch model of these switches. Each switch model configuration contains the PicOS image used to deploy white-box switches of this model, and the port number range for each speed (GE, TE, QE, and XE).

To deploy integrated hardware and software switches, because these switches have PicOS installed, you don't need to configure switch models.

Procedure

To configure a switch model, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Wired Profiles** from the navigation bar, and then click the **Switch Model** tab.
2. To ensure the **Switch Model** drop-down list is the latest, click **Update Switch Model**, and then click **Yes**.



3. In the **Switch Model** drop-down list, select the switch model that you want to configure.
4. Configure the port number range for each speed (GE, TE, QE, and XE).

NOTE

For each switch model, a default port number range is configured for each speed (GE, TE, QE, and XE).

You must configure the port number ranges correctly based on real port ranges on switches of this switch mode. Or else, some AmpCon-Campus functions will fail.

5. In the **Deployed ONIE Image** drop-down list, select the PicOS image that you want to install for this switch model.

NOTE

For each switch model, a built-in PicOS image is specified for switch deployment.

If the PicOS image to install is not listed here, upload the PicOS image and its MD5 file to AmpCon-Campus first. For more information, see [Uploading Images](#).

The screenshot shows the 'Switch Model' configuration page. The 'Deployed ONIE Image' field is highlighted with a red rectangle. The field contains the text 'PicOS-4.6.0E-1929b79f56-ar4610.bin'. Below the field are three buttons: 'Update Switch Model', 'Apply', and 'Reset'.

6. Click **Apply**.

7. Optional: To reset a switch model, click **Reset**.

The screenshot shows the 'Switch Model' configuration page. The 'Reset' button is highlighted with a red rectangle. The 'Deployed ONIE Image' field now contains the text 'PicOS-4.6.0E-1929b79f56-ar4610.bin'. Below the field are three buttons: 'Update Switch Model', 'Apply', and 'Reset'.

After you reset a switch model, the port number range for each speed is set to zero, and the PicOS image in the **Deployed ONIE Image** drop-down list is reset to the built-in image.

Adding System Configurations

System configurations contain important information used for importing switches or deploying switches through ZTP. If a system configuration is not configured correctly, the switches related to this system configuration will fail to be deployed or imported.

The first time you log in to AmpCon-Campus, the global system configuration is blank. You must configure the global system configuration.

If the global system configuration doesn't meet all switch requirements, create one or multiple non-global system configurations.

[Overview](#)

[Types](#)

[Configurations](#)

[Procedure](#)

[Adding a Global System Configuration](#)

[Adding a Non-global System Configuration](#)

[Optional Operations](#)

[Checking License Portal Connectivity](#)

[Viewing or Modifying a System Configuration](#)

[Changing the Default Switch Password](#)

Overview

Types

System configurations contain the following two types:

- **Global system configuration**

The first time you log in to AmpCon-Campus, you must add information to the global system configuration. The global system configuration can't be removed.

- **Non-global system configuration**

If the default username and password of switches to be managed are different, you can add multiple non-global system configurations. You can remove a non-global system configuration if it is not needed.

Configurations

A system configuration contains the following information:

- The URL, username, and password of the License Portal. The information is used to send requests to the License Portal.
- Default username and password of switches to be managed. The information is used to access the switches.
- A security configuration file with PicOS security-related set CLIs. Before you deploy and configure a switch, the switch needs to be configured with an initial security configuration

to eliminate any unauthorized access. Security Config file is loaded to switch at the beginning of switch deployment.

- A parking security configuration file, which is used to push initial parking security configuration for those switches in the parking status. This configuration is not included in the non-global system configuration.

Available for only global system configurations.

- The maximum backup number for the configuration snapshots. This configuration is not included in the non-global system configuration.

Available for only global system configurations.

- The IP ranges of switches that are allowed for AmpCon-Campus management. This configuration is not included in the non-global system configuration.

Available for only global system configurations.

- Whether to enable debug logs for server-side operations or not. This configuration is not included in the non-global system configuration.

Available for only global system configurations.

Procedure

Adding a Global System Configuration

To add a global system configuration, follow these steps:

1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role. For more information about user roles, see [Managing User Access](#).
2. Click **Wired > Wired Profiles** from the navigation bar, and then input the following information in the **System Configuration** tab:

NOTE

Pay attention to the following points. Or else, switches will fail to be imported and deployed.

- Ensure that **Device Default Login User** and **Device Default Password** are correct and can be used to log in to these switches.
- If some switches don't use the **Device Default Login User** and **Device Default Password** in the global system configuration, create non-global system configurations for these switches, and ensure the **Device Default Login User** and **Device Default Password** match these switches.
- Ensure that AmpCon-Campus can connect with the License Portal through the entered **License Portal URL**, **License Portal**

User, and License Portal Password. For more information, see the [Checking License Portal Connectivity](#) section.

- Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations or underlay/overlay related configurations.

Table 1. Global System Configuration Parameters

Parameter	Description
Configuration Name	The name of the configuration.
Device Default Login User	The default username for switches to be managed. The default user is admin .
Device Default Password	The default password of the default user. The default password is pica8 .
License Portal URL	https://license.pica8.com
License Portal User	The user ID for the License Portal.
License Portal Password	The password of the user for the License Portal.
Config Backup Number	The maximum backup number for the configuration snapshots.
DB Backup Number	The allowed maximum number of database backups.
Security Config File	The .txt file with PicOS security-related set CLIs.

Example configuration in the .txt file:

```
set system login user testadmin
authentication plain-text-password
pica8pica8
```

```
set system login user testadmin class
super-user
```

NOTES

- The configurations in this file will be pushed to switches during the ZTP process.
- If you don't want to push configurations to switches during the ZTP process, you can use a blank .txt file.
- You might also add security-related configurations in the [global configuration](#). If some configurations in the global configuration and in the uploaded **Security Config File** here overlap:
 - For the overlapping configurations, the configurations in the global configuration will overwrite the configurations in the uploaded **Security Config File** here.
 - For the non-overlapping configurations, the configurations in both the global configuration and the **Security Config File** here will be pushed to the switches.

Parking Security Config File

Optional. To eliminate any unauthorized access, switches in the parking lot need to be configured with an initial parking security configuration. For more information about parking lot, see [Managing the Parking Lot](#).

	Example configuration in the .txt file: <pre>set system login user testadmin authentication plain-text-password pica8pica8 set system login user testadmin class super-user</pre> <i>i</i> NOTES • The configurations in this file will be pushed to switches when the switches go to the parking lot. • If you don't want to push configurations to switches when the switches go to the parking lot, you can use a blank .txt file.
Allow Switch Source IP	Optional. Allow specified subnets from which switches can access AmpCon-Campus.
Debug	Optional. Enable debug logs for server-side operations or not.

3. Click **Save**.

4. Optional: After you add a global system configuration, do the following actions as needed:

- To update the encrypt key used to encrypt sensitive data in the AmpCon-Campus database, click **Update Encrypt Key**. For more information, see [Updating the Encryption Key for Sensitive Data Encryption](#).

The screenshot displays the 'System Configuration' page with the following fields and values:

- Configuration Name:** Global
- Device Default Login User:** admin
- Device Default Password:** [masked]
- License Portal URL:** https://license.pica8.com
- License Portal User:** api_user
- License Portal Password:** [masked]
- Config Backup Number:** 3
- DB Backup Number:** 3
- Security Config File:** config_gen/security/security.config
- Parking Security Config File:** config_gen/security/parking_security.config
- Allow Switch Source IP:** 10.0.0/8, 192.168.1.0/24
- DEBUG:** [toggle switch]

At the bottom of the page, there are four buttons: 'Save', 'Reset', 'Update Encrypt Key' (highlighted with a red box), and 'Syslog Config'.

- To forward AmpCon-Campus system logs to external Syslog servers like Splunk, click **Syslog Config**. For more information, see [Forwarding Logs to External Syslog Servers](#).

The global system configuration is configured now. If you don't add non-global system configurations, the global system configuration will be used to deploy and import switches

Adding a Non-global System Configuration

To add a non-global system configuration, follow these steps:

1. Click **Wired > Wired Profiles** from the navigation bar.
2. Click the **+** icon in the **System Configuration** tab. The “Add New System Config” tab opens.
3. Input the following information :

NOTE

Pay attention to the following points. Or else, switches will fail to be imported and deployed.

- Ensure that the entered **Device Default Login User** and **Device Default Password** on the “System Configuration” page are correct and can be used to log in to these switches.
- Ensure to check whether AmpCon-Campus can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see the [Checking License Portal Connectivity](#) section.
- Ensure that the uploaded **Security Config File** doesn't contain wrong configurations or underlay/overlay related configurations.

Table 2. Non-Global System Configuration Parameters

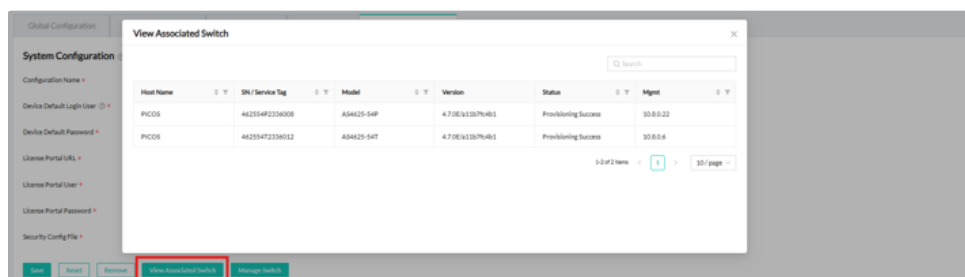
Parameter	Description
Configuration Name	The name of the configuration.
Device Default Login User	The default username of switches to be managed. The default user is admin .
Device Default Password	The default password of the default user. The default password is pica8 .
License Portal URL	https://license.pica8.com
License Portal User	The user ID for the License Portal.
License Portal Password	The password of the user for the License Portal. License Portal URL, License Portal User, and License Portal Password are used to access the License Portal.
Security Config File	The .txt file with PicOS security-related set CLIs. Example configuration in the .txt file: <pre>set system login user testadmin authentication plain-text-password pica8pica8 set system login user testadmin class super-user</pre> NOTES The configurations in this file will be pushed to switches during the ZTP process.

- If you don't want to push configurations to switches during the ZTP process, you can use a blank .txt file.
- You might also add security-related configurations in the [global configuration](#). If some configurations in the global configuration and in the uploaded **Security Config File** here overlap:
 - For the overlapping configurations, the configurations in the global configuration will overwrite the configurations in the uploaded **Security Config File** here.
 - For the non-overlapping configurations, the configurations in both the global configuration and the **Security Config File** here will be pushed to the switches.

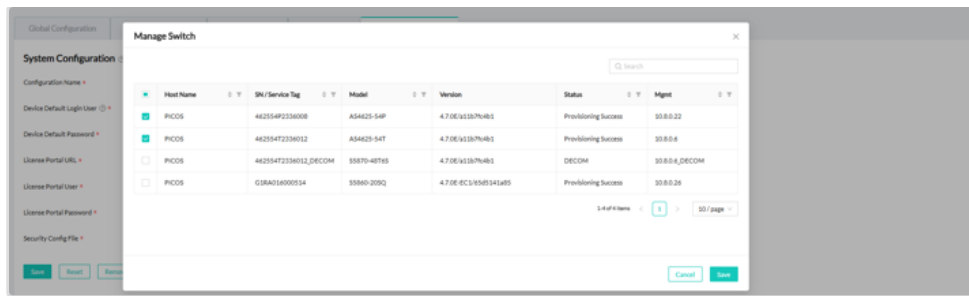
4. Click **Add**.

After you add the non-global system configuration, you can do the following actions:

- To view the switch information associated with the system configuration, click **View Associated Switch** in the **System Configuration** tab.



- To apply a non-global system configuration to specific switches, click **Manage Switch**, select the switches, and then click **Save**.



- To remove a non-global system configuration, click **View Associated Switch** to check whether the system configuration is associated with any switches or not. If not, click **Remove**.

NOTE

If the non-global system configuration is still associated with some switches, the removal will fail. You need to click **Manage Switch** to unselect these switches first.

Optional Operations

Checking License Portal Connectivity

To check whether AmpCon-Campus can connect with the License Portal, follow these steps:

1. Click **Wired > Wired Profiles** from the navigation bar.
2. In the **System Configuration** tab, select the system configuration to be checked in the **Configuration Name** drop-down list.
3. Check the connectivity by clicking the connect icon as follows.

NOTE

You can see the message “The license connect success.” only when the following conditions are met:

- The **License Portal URL**, **License Portal User**, and **License Portal Password** are entered correctly.
- The network between AmpCon-Campus and the License Portal is available.

Viewing or Modifying a System Configuration

To view or edit a system configuration, follow these steps:

1. Click **Wired > Wired Profiles** from the navigation bar.
2. In the **System Configuration** tab, click the **Configuration Name** drop-down list, and select the system configuration name. Then, you can view the details of the system configuration.

To modify the system configuration, modify the configuration items as needed, and then click **Save**.

Changing the Default Switch Password

In system configurations, the default switch username is **admin**, and the default password is **pica8**. To change the default password, follow these steps:

1. Click **Wired > Wired Profiles** from the navigation bar.
2. In the **System Configuration** tab, select the system configuration to be modified in the **Configuration Name** drop-down list.
3. Change the default switch password as follows:

- **For global system configurations**

- a. Enter a new password in the **Device Default Password** field.

b. Click **Browse** in the **Parking Security Config File** section, and then upload a .txt file containing the following command:

```
set system login user admin authentication plain-text-
password <New-Password>
```

Replace *<New-Password>* with the new password you want to use.

NOTE

Pay attention to the following notes. Or else, switches will fail to be deployed.

- Ensure that the new password in the .txt file and in the **Device Default Password** field are the same.
- Ensure that no service-related configurations are added to the **Parking Security Config File**.
- Ensure that the **Security Config File** doesn't contain any commands used to push service-related configurations or change the password of the **Device Default Login User**.

• For non-global configurations

a. Enter a new password in the **Device Default Password** field.

b. Click **Browse** in the **Security Config File** section, and then upload a .txt file containing the following command:

```
set system login user admin authentication plain-text-  
password <New-Password>
```

Replace <New-Password> with the new password you want to use.

i NOTE

Pay attention to the following notes. Or else, switches will fail to be deployed.

- Ensure that the new password in the command and in the **Device Default Password** field are the same.
- Ensure that the **Security Config File** doesn't contain commands used to push service-related configurations.

Configuring a DHCP Server

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

ZTP in AmpCon-Campus relies on DHCP. 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:

- A white-box switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-Campus server, update switch configurations, and reboot the switch.
- An integrated hardware and software switch runs the shell script to register with the AmpCon-Campus server, install a PicOS license on the switch, update switch configurations, and reboot the switch.

Before you provision switches through ZTP, you must configure the DHCP server as follows:

Procedure

1. Deploy a DHCP server on a Linux server.
 2. Add configurations to the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server.
- For white-box switches, add the following configurations for each switch to be deployed:

```
host 4610_54t_02 {  
  hardware ethernet C4:39:3A:FF:2C:C0;  
  fixed-address 10.10.51.198;  
  option default-url "http://10.56.20.184/onie";  
}
```

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

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

Replace “10.56.20.184” with the IP address of the AmpCon-Campus server.

NOTE

The following DHCP option is used :

Option default-url: 114

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

```
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 switch.

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

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

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 switches to be deployed. Or else, the ZTP will fail.

Provisioning New Switches through ZTP

ZTP relies on the DHCP service, and thus you need to configure DHCP first. 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:

- The white-box switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-Campus server, update switch configurations, and reboot the switch.
- The integrated hardware and software switch runs the shell script to register with the AmpCon-Campus server, update switch configurations, and reboot the switch.

To onboard switches through ZTP, you need to complete the following provisioning steps.

[Before You Begin](#)

[Provisioning a White-Box Switch](#)

[Provisioning an Integrated Hardware and Software Switch](#)

Before You Begin

- Before you provision switches through ZTP, ensure that the prerequisite tasks described in [Prerequisites](#) have been completed.
 - Ensure that you have prepared all the required configurations in the AmpCon-Campus UI.
- For more information, see the following documents:

White-Box Switch	Integrated Hardware and Software Switch
Configuring Global Configurations	Configuring Global Configurations
Adding Configuration Templates	Adding Configuration Templates
Adding Switch Configurations	Adding Switch Configurations
Configuring Switch Models	Adding System Configurations
Adding System Configurations	

- Ensure that you have configured the DHCP server. For more information, see [Configuring the DHCP Server](#).

Provisioning a White-Box Switch

1. Download and install MobaXterm.

2. Open MobaXterm, and then create a session to connect with the switch.
3. Run the following commands to enter the Linux shell mode and reboot the switch:

```
start shell sh
```

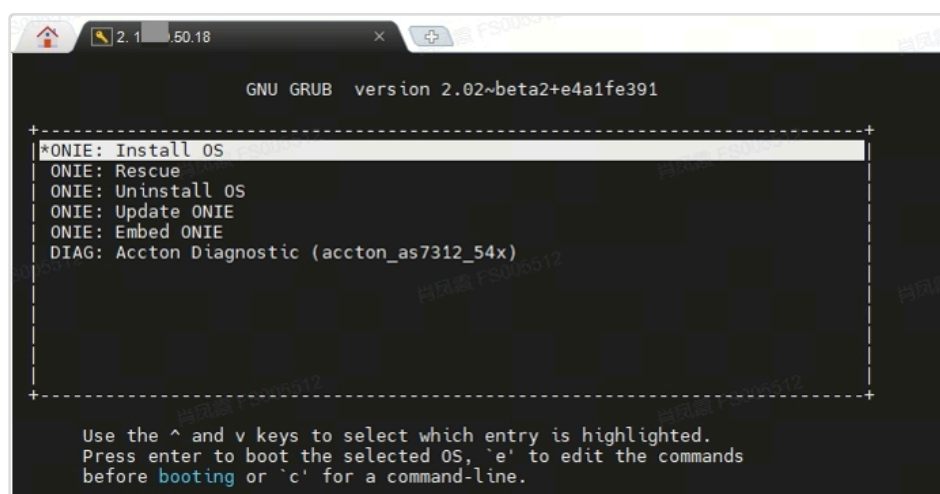
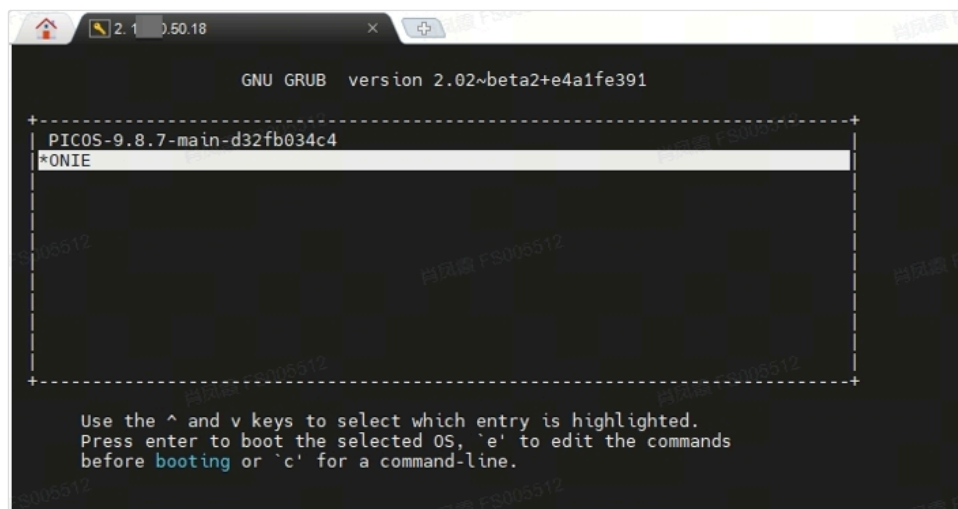
```
sudo reboot -f
```

4. If you see the “Hit any key to stop autoboot” message, press the **Enter** key to exit the autoboot mode.

If you don't see this message, go to step 5 directly.

5. Reboot the switch.

- For switches with the ONIE menu, select **ONIE**, and then select **ONIE: Install OS**.

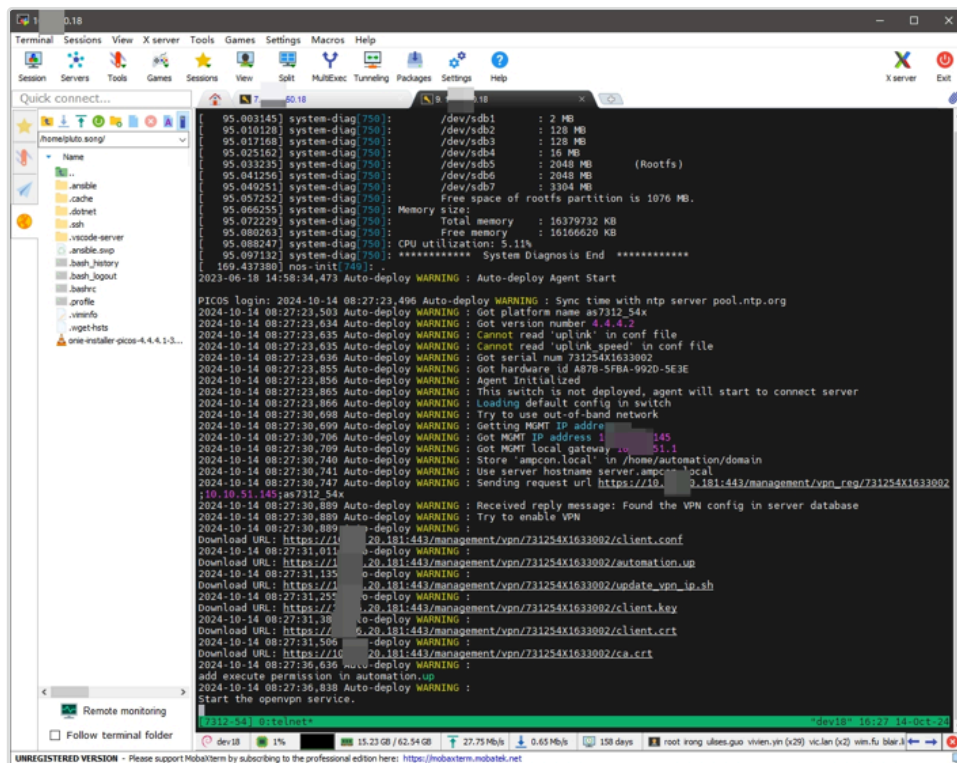


- For AS4610 switches, reboot from ONIE by running the following command:

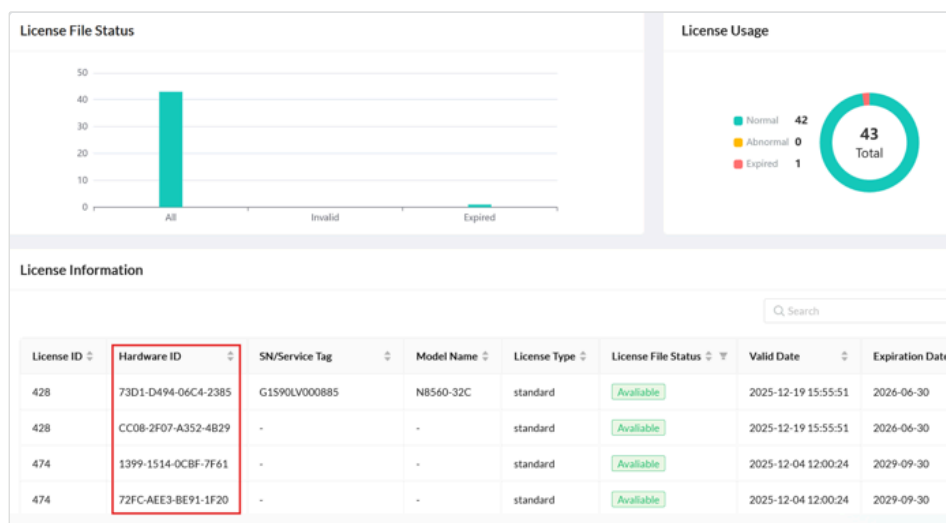
```
run onie bootcmd
```


Then, the switch will be restarted and automatically register with the AmpCon-Campus server.

6. Wait for the registration process to be completed.



7. Check whether the hardware ID of the switch is included in any imported AmpCon-Campus licenses. For more information, see [Viewing AmpCon-Campus Licenses](#).



If the hardware ID of the switch is not included in any imported AmpCon-Campus licenses, you must import an AmpCon-Campus license to AmpCon-Campus. Or else, the switch can't be provisioned successfully. For more information, see [Importing Licenses for Deployed Switches](#).

8. In the AmpCon-Campus UI, click **Wired > Switches**. In the **Switch** list, locate the switch, and then click **Stage**.

Switch Name	SN/Service Tag	Model	Version	Status	Mgmt IP	Operation
PIC05	EC342000063	as4830_548_3	4.5.0E	Provisioning Success	1.18	Unstage Log Configuration Config View Lifecycle Actions
PIC05	G186264000013_DECOM	S5860-205Q	4.5.0E	DECOM	1.18, DECOM	Unstage Log Configuration Config View Lifecycle Actions
	123454	ag548		Configured		Stage Log Configuration Config View Lifecycle Actions
	1234541	S5860-240B-U		Configured		Unstage Log Configuration Config View Lifecycle Actions

Then, the switch status will be shown as **Staged**.

Switch Name	SN/Service Tag	Model	Version	Status	Mgmt IP	Operation
PIC05	EC342000063	as4830_548_3	4.5.0E	Provisioning Success	1.18	Unstage Log Configuration Config View Lifecycle Actions
PIC05	G186264000013_DECOM	S5860-205Q	4.5.0E	DECOM	1.18, DECOM	Unstage Log Configuration Config View Lifecycle Actions
	123454	ag548		Configured		Stage Log Configuration Config View Lifecycle Actions
	1234541	S5860-240B-U		Staged		Unstage Log Configuration Config View Lifecycle Actions

After you stage the switch, the switch will be configured automatically based on the related system configuration and switch configuration. After the configurations are pushed successfully, the switch status will be changed to **Provisioning Success**.

System	SN/Service Tag	Model	Version	Status	VMIP	Mgmt IP	Operation
PIC05	4625472236012_DECOM	S5870-48T6S	4.7.0E	DECOM	1.18, DECOM		Unstage Device Log Configuration Config View Lifecycle Actions
PIC05	4625472236008	AS4625-54P	4.7.0E	Provisioning Success	1.18, 22		Unstage SSN Device Log Configuration Config View Lifecycle Actions
PIC05	4625472236012	AS4625-54T	4.7.0E	Provisioning Success	1.18		Unstage SSN Device Log Configuration Config View Lifecycle Actions
PIC05	G186264000013	S5860-205Q	4.7.0E-EC3	Provisioning Success	1.18, 24		Unstage SSN Device Log Configuration Config View Lifecycle Actions

Provisioning an Integrated Hardware and Software Switch

1. Download and install MobaXterm.
2. Open MobaXterm, and then create a session to connect with the switch.
3. Run the following commands to enter the Linux shell mode and reboot the switch:

```
start shell sh
```

```
sudo reboot -f
```

```

admin@PIC05:~$ sudo reboot
admin@PIC05:~$ [ 1451.427033 ] reboot: Restarting system

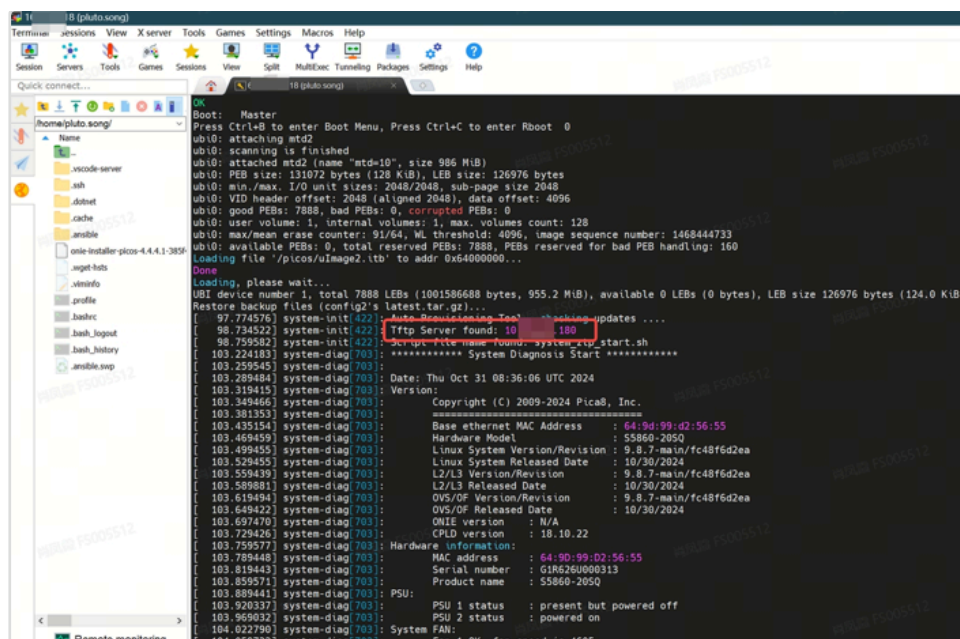
U-Boot 1.4.39--g7c55aac (Jan 10 2024 - 10:42:10 +0800)

I2C: ready
DRAM: 1 GiB
NAND: 1024 MiB
Loading Environment from SPI Flash... SF: Detected s25fl128s_64k with page size 256 Bytes, erase size 64 KiB, total 16 MiB
OK
Boot: Master
Press Ctrl+B to enter Boot Menu, Press Ctrl+C to enter Rboot 0
ubi0: scanning is finished
ubi0: attached mtd2 (name "mtd=10", size 986 MiB)
ubi0: PEB size: 131072 bytes (128 KiB), LEB size: 126976 bytes
ubi0: min./max. I/O unit sizes: 2048/2048, sub-page size 2048
ubi0: VID header offset: 2048 (aligned 2048), data offset: 4096
ubi0: good PEBs: 7888, bad PEBs: 0, corrupted PEBs: 0
ubi0: user volume: 1, internal volumes: 1, max. volumes count: 128
ubi0: max/mean erase counter: 91/64, ML threshold: 4096, image sequence number: 1468444733
ubi0: available PEBs: 0, total reserved PEBs: 7888, PEBs reserved for bad PEB handling: 160
Loading file '/picos/u/image2.itb' to addr 0x64000000...
Done

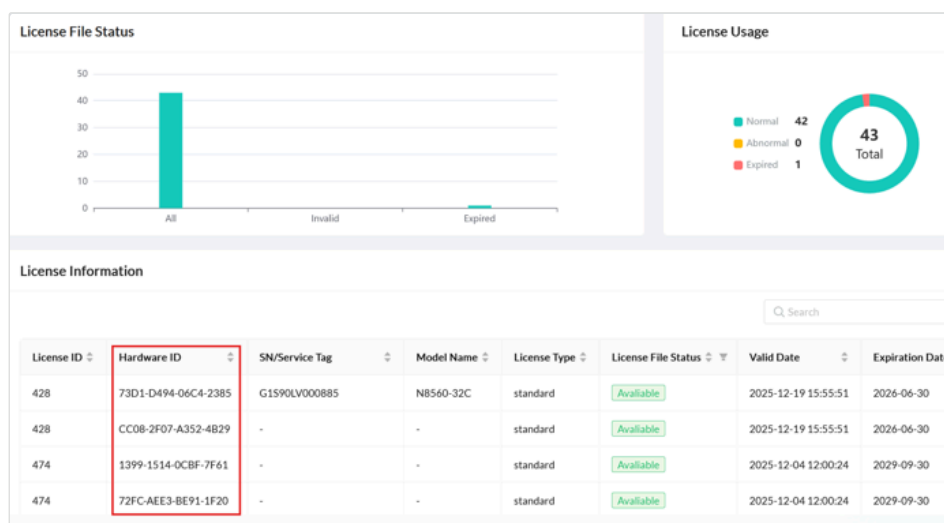
```

Then, the switch will be restarted and automatically register with the AmpCon-Campus server.

4. Wait for the registration process to be completed.



5. Check whether the hardware ID of the switch is included in any imported AmpCon-Campus licenses. For more information, see [Viewing AmpCon-Campus Licenses](#).



If the hardware ID of the switch is not included in any imported AmpCon-Campus licenses, you must import an AmpCon-Campus license to AmpCon-Campus. Or else, the switch can't be provisioned successfully. For more information, see [Importing Licenses for Deployed Switches](#).

6. In the AmpCon-Campus UI, click **Wired > Switches**. In the **Switch** list, locate the switch, and then click **Stage**.

Switch Name	SN/Service Tag	Model	Version	Status	Agent IP	Operation
PC05	EC161000063	ar410_548_b	4.5.0E	Provisioning Success	158	Unstage SN Log Configuration Config View Lifecycle Actions
PC05	G16260000013_DECOM	S5860-205Q	4.5.0E	DECOM	158	Unstage Log Configuration Config View Lifecycle Actions
	123454	ag5448		Configured		Stage Log Configuration Config View Lifecycle Actions
	1234541	S5860-2408-U		Configured		Stage Log Configuration Config View Lifecycle Actions

Then, the switch status will be shown as **Staged**.

Report Actions Lifecycle Actions Parking List Search									
Switch Name	SN/Service Tag	Model	Version	Status	Mgmt IP	Operation			
PC05	EC1610000603	as4805_540_3	4.5.0E	Provisioning Success	10.1.1.18	Unstage SSH Log Configuration Config View Lifecycle Actions			
PC05	G186380A000013_DECOM	S5860-205Q	4.5.0E	DECOM	10.1.1.18_DECOM	Unstage Log Configuration Config View Lifecycle Actions			
	123454	ag5648		Configured		Stage Log Configuration Config View Lifecycle Actions			
	1234541	S5860-2400-U		Staged		Unstage Log Configuration Config View Lifecycle Actions			

After you stage the switch, the switch will be configured automatically based on the related system configuration and switch configuration. After the configurations are pushed successfully, the switch status will be changed to **Provisioning Success**.

PC05 PC05 Report Actions Lifecycle Actions Parking List Search									
System	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation		
PC05	4625472236012_DECOM	S5870-48T6S	4.7.0E	DECOM	10.1.1.18_DECOM		Unstage	Device Log	Configuration Config View Lifecycle Actions
PC05	4625492236008	A54625-54P	4.7.0E	Provisioning Success	10.1.1.22		Unstage	SSH Device Log	Configuration Config View Lifecycle Actions
PC05	4625472236032	A54625-54T	4.7.0E	Provisioning Success	10.1.1.18		Unstage	SSH Device Log	Configuration Config View Lifecycle Actions
PC05	G186380A0000134	S5860-205Q	4.7.0E-6C1	Provisioning Success	10.1.1.24		Unstage	SSH Device Log	Configuration Config View Lifecycle Actions

Designing Campus Fabrics

AmpCon-Campus supports two standard-based campus fabric architectures, MLAG fabrics and IP Clos fabrics. These two fabric types, which have different use cases, cover the networking requirements of small, medium-sized, and large-scale campus fabrics.

You can deploy an MLAG campus fabric on a two-layer network with the collapsed core and access layers. Or you can deploy an IP Clos campus fabric on a campus-wide network that involves multiple buildings with separate distribution and core layers.

AmpCon-Campus helps you eliminate complex campus networking configurations during the fabric design and management process.

See the following child topics:

- [Key Concepts](#)
- [Supported Switches for Campus Fabrics](#)
- [Fabric Overview](#)
- [Designing MLAG Fabrics](#)
- [Designing IP Clos Fabrics](#)
- [Provisioning Overlay Services](#)
- [Managing Campus Fabrics](#)

Key Concepts

Before you design a campus fabric, you need to understand the following concepts:

- Autonomous System (AS)
- Border Gateway Protocol (BGP)
- DHCP Snooping
- DHCP Relay
- Ethernet Virtual Private Network (EVPN)
- Fabric
- Multi-Chassis Link Aggregation (MLAG)
- Network Access Control (NAC)
- Open Shortest Path First (OSPF)
- Overlay Network
- Overlay Network Control Plane
- Overlay Data Plane
- Underlay Network
- Virtual Routing and Forwarding (VRF)
- Virtual Extensible Local Area Network (VXLAN)

Autonomous System (AS)

A collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain, which presents a common and clearly defined routing policy to the Internet. Each AS is assigned an autonomous system number (ASN), for use in Border Gateway Protocol (BGP) routing.

An AS is a collection of routers and networks under a single technical administration, using an interior routing protocol and common metrics to determine how to route packets within the AS, and using an exterior routing protocol to determine how to route packets to other AS.

Border Gateway Protocol (BGP)

A 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).

DHCP Snooping

A 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

A function implemented in Layer 3 switches to forward DHCP messages between DHCP clients and servers across different subnets.

Ethernet Virtual Private Network (EVPN)

EVPN is a next-generation VPN solution that introduces a control plane to better control the MAC address learning process.

Fabric

The logistic representation of an actual physical network. You can deploy a physical network by designing a fabric.

Multi-Chassis Link Aggregation (MLAG)

Implements link aggregation among multiple devices. AmpCon-Campus networking solution supports using MLAG on leaf switches.

Two leaf switches set up an MLAG through peer links. Both peer leaf switches are displayed as a logical device on the forwarding plane and as two independent switches on the management control plane. Upgrading and replacing devices are carried out independently, achieving simple maintenance and high running reliability.

Network Access Control (NAC)

A security solution that ensures only authorized devices and users can access a network. It enforces policies to control access based on factors such as device type, user identity, and compliance with security standards. 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.

Open Shortest Path First (OSPF)

A 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.

Overlay Network

An overlay network is 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.

Technologies such as Virtual Extensible LAN (VXLAN) or EVPN are examples of overlay networks, providing advanced functionalities like network virtualization and multi-tenancy.

If the underlay network is like the physical roads connecting different cities (the devices), the overlay network is like the GPS that helps you navigate these roads most efficiently and can also create virtual pathways or tunnels (VXLAN) to reach distant cities more directly.

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 Network Control Plane

Manages the creation, maintenance, and tear-down of overlay networks, which are virtual networks built on top of an underlying physical network (the underlay). The control plane ensures efficient communication between endpoints, handles network virtualization, and supports advanced features like multi-tenancy, workload mobility, and scalability.

Overlay Data Plane

Responsible for the 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 using mechanisms like Equal-Cost Multi-Path (ECMP).

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.

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.

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 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.

Supported Switches for Campus Fabrics

Before you design your fabric, check the supported PicOS switches based on the campus fabric type that you choose.

NOTE

Only PicOS switches can be used for campus fabric design with AmpCon-Campus.

[MLAG Fabrics](#)

[IP Clos Fabrics](#)

MLAG Fabrics

See the following supported access-layer and core-layer switches for MLAG fabrics:

Table 1. Supported PicOS Switches for MLAG Fabrics

Access Layer	Core Layer
• All Edgecore, DELL, Delta, and HPE white-box switches supported by AmpCon-Campus • FS switches ◦ S5870-48T6BC ◦ S5870-48T6BC-U ◦ S5870-48T6S ◦ S5870-48T6S-U ◦ S5870-48MX6BC-U ◦ S5860-20SQ ◦ S5860-24MG-U ◦ S5860-24XB-U ◦ S5860-24XMG ◦ S5860-48MG-U ◦ S5860-48XMG ◦ S5860-48XMG-U ◦ S5810-28FS ◦ S5810-28TS ◦ S5810-48FS	• All Edgecore, DELL, Delta, and HPE white-box switches supported by AmpCon-Campus • FS switches ◦ S5860-20SQ ◦ N5850-48X6C ◦ S5890-32C ◦ S5580-48Y

◦ S5810-48TS ◦ S5810-48TS-P	
--	--

IP Clos Fabrics

See the following supported access-layer, distribution-layer, and core-layer switches for IP Clos fabrics:

Table 2. Supported PicOS Switches for IP Clos Fabrics

Access Layer	Distribution Layer	Core Layer
• Edgecore switches ◦ AS7726-32X (DCS204) ◦ AS6812-32X ◦ AS7326-56X (DCS203) ◦ AS5835-54T (DCS209) ◦ AS5835-54X (DCS208) ◦ AS5812-54T ◦ AS5812-54X ◦ AS4630-54NPE (EPS203) ◦ AS4630-54PE (EPS202) ◦ AS4630-54TE (EPS201) • DELL switches ◦ N3224F-ON ◦ N3224P-ON ◦ N3224PX-ON ◦ N3224T-ON ◦ N3248P-ON ◦ N3248PXE-ON ◦ N3248TE-ON ◦ N3248X-ON	• Edgecore switches ◦ AS7726-32X (DCS204) ◦ AS6812-32X ◦ AS7326-56X (DCS203) ◦ AS5835-54T (DCS209) ◦ AS5835-54X (DCS208) ◦ AS5812-54T ◦ AS5812-54X ◦ AS4630-54NPE (EPS203) ◦ AS4630-54PE (EPS202) ◦ AS4630-54TE (EPS201) • DELL switches ◦ N3224F-ON ◦ N3224P-ON ◦ N3224PX-ON ◦ N3224T-ON ◦ N3248P-ON ◦ N3248PXE-ON ◦ N3248TE-ON ◦ N3248X-ON	• Edgecore switches ◦ AS7726-32X (DCS204) ◦ AS6812-32X ◦ AS7326-56X (DCS203) ◦ AS5835-54T (DCS209) ◦ AS5835-54X (DCS208) ◦ AS5812-54T ◦ AS5812-54X ◦ AS4630-54NPE (EPS203) ◦ AS4630-54PE (EPS202) ◦ AS4630-54TE (EPS201) • DELL switches ◦ N3224F-ON ◦ N3224P-ON ◦ N3224PX-ON ◦ N3224T-ON ◦ N3248P-ON ◦ N3248PXE-ON ◦ N3248TE-ON ◦ N3248X-ON

◦ S5212F-ON ◦ S5224F-ON ◦ S5232F-ON ◦ S5248F-ON ◦ S5296F-ON • FS switches ◦ S5870-48T6BC ◦ S5870-48T6BC-U ◦ S5870-48T6S ◦ S5870-48T6S-U ◦ S5870-48MX6BC-U	◦ S5212F-ON ◦ S5224F-ON ◦ S5232F-ON ◦ S5248F-ON ◦ S5296F-ON • FS switches ◦ S5890-32C ◦ S5580-48Y	◦ S5212F-ON ◦ S5224F-ON ◦ S5232F-ON ◦ S5248F-ON ◦ S5296F-ON • FS switches ◦ S5890-32C
---	--	---

Fabric Overview

You can use AmpCon-Campus to design an MLAG campus fabric or an IP Clos campus fabric.

Currently, the IP Clos fabric feature is for experimental purposes only.

To determine which campus fabric type to use, see the following descriptions:

- [MLAG Campus Fabric](#)
 - [Use Cases](#)
 - [Components](#)
 - [Network Architecture](#)
- [IP Clos Campus Fabric](#)
 - [Use Cases](#)
 - [Components](#)
 - [Network Architecture](#)

MLAG Campus Fabric

Use Cases

AmpCon-Campus supports 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.

This architecture simplifies the network topology, reduces latency, and lowers costs by eliminating the need for separate core and distribution devices.

To avoid single-point failure, two collapsed core switches are added to MLAG, and each access switch connects to both collapsed core switches.

If your topology is simple and very small, the two-layer MLAG fabric is sufficient. However, when your topology is complex, you are suggested to deploy an IP Clos campus fabric.

Components

The two-layer MLAG fabric architecture contains the following components:

- **Collapsed core layer**

The layer where the core and distribution layers are consolidated into a single unified structure.

- **Access layer**

The layer that connects devices like computers, printers, and wireless access points to the rest of the network. 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.

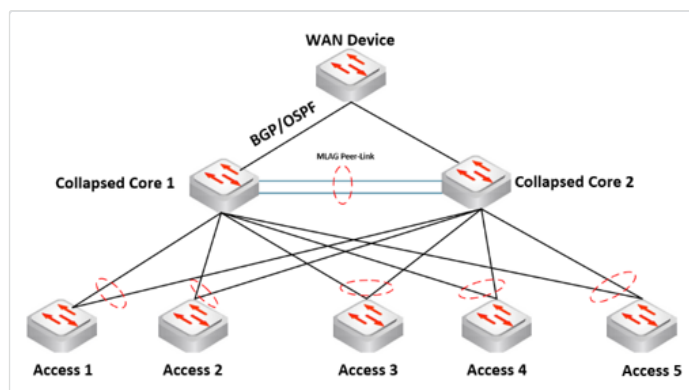
Network Architecture

The two-layer MLAG fabric architecture in AmpCon-Campus is as follows:

NOTE

You can specify the count of core and access switches as needed. Each MLAG fabric must have at least 2 core switches and one access switch.

Figure 1. MLAG Fabric Architecture



- The core layer consists of Layer 3 switches, the access layer consists of Layer 2 switches, and the access gateway is located at the core layer.
- MLAG is used among core switches to provide redundancy and high availability for downstream access switches.
- OSPF or BGP is used as the underlay routing protocol to establish Layer 3 routing and provide routing configurations for the core switches and uplink devices (such as routers, gateways, and firewalls).
- At the port level, you can select the uplink port of each core switch to be connected to a WAN device. After each uplink port is chosen, AmpCon-Campus automatically assigns an uplink IP address, adds the link subnet to BGP or OSPF, and creates a default route to the WAN device.

The core switches and the WAN device establish routing neighbor relationships and exchange routing information.

- The collapsed core switches handle both the aggregation of access-layer traffic and the high-speed forwarding of data across the network, making it suitable for smaller or less complex networks where scalability and redundancy requirements are not highly required.
- No overlay technology is introduced to this architecture.

IP Clos Campus Fabric

Use Cases

Enterprise campus networks are undergoing massive transitions to accommodate the growing demand for networks. To meet the demands of modern networks, campus networks must prioritize the most critical functionalities, such as robust network bandwidth, high availability, scalability, and security.

The IP Clos fabric architecture provides a scalable and flexible solution for interconnecting multiple switches in a hierarchical manner, allowing efficient utilization of network resources and simplified routing.

It's more suitable for large-scale campus networking.

- **Enhance network scalability**

The IP Clos fabric architecture extends EVPN to connect VXLANs across multiple buildings. You can rapidly and easily scale up your campus network without adding complexity.

By managing IP Clos fabrics with AmpCon-Campus, you can easily add core, distribution, or access layer switches when your business grows without having to redesign the network.

- **Improve network flexibility**

The IP Clos architecture uses a Layer 3 IP-based underlay network and an EVPN-VXLAN overlay network.

In the underlay, the simple IP-based Layer 3 underlay network limits the Layer 2 broadcast domain and eliminates the need for Spanning Tree Protocol (STP).

In the overlay, a flexible overlay network based on VXLAN tunnels combined with an EVPN control plane efficiently provides Layer 3 or Layer 2 connectivity.

- **Boost network security and segmentation**

By creating multiple VLANs based on VXLAN tunnels, devices and data in each VLAN are securely isolated from other VLANs in Layer 2.

By configuring different routing instances based on Virtual Routing and Forwarding (VRF), routing and switching tables on each VPN instance are isolated.

- **Increase network bandwidth and avoid Flooding**

The propagation of MAC-IP Network Layer Reachability Information (NLRI) is handled by BGP. The use of BGP for routing ensures updates are propagated efficiently throughout the network.

MAC address flooding and learning might use excessive network bandwidth. EVPN separates the control plane and data plane and makes the control plane based Layer 2 or Layer 3 learning faster. The EVPN control plane handles the exchange and learning of routes, and thus the MAC address flooding and learning mechanisms are not used.

Components

AmpCon-Campus supports the 5-stage IP Clos fabric architecture. This architecture contains the following layers:

- **Access layer**

The layer that connects devices like computers, printers, and wireless access points to the rest of the network. 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.

- **Distribution layer**

The layer that receives traffic from access switches and forwards it to core switches. Distribution switches act as intermediaries that aggregate data from multiple access switches before routing it to core switches.

- **Core layer**

The layer that receives traffic from the distribution switches. Core switches handle high-speed data transfer, connect different distribution switches, and ensure fast and reliable connections among devices in different subnets.

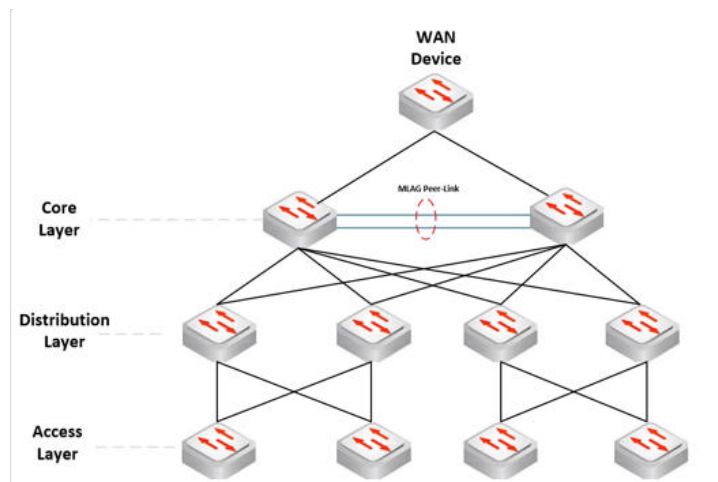
Network Architecture

The 5-stage IP Clos fabric architecture in AmpCon-Campus is as follows:

NOTE

You can specify the count of core, distribution, and access switches as needed. Each 5-stage IP Clos fabric must have at least 2 core switches, one distribution switch, and two access switches.

Figure 2. IP Clos Fabric Architecture



- All core switches, distribution switches, and access switches are connected in Layer 3.
- MLAG is used among core switches to provide redundancy and high availability for downstream distribution switches.
- EBGp is used as the underlay routing protocol. It provides better prefix filtering, traffic engineering, and route tagging.
- BGP unnumbered and loopback addresses are used to establish neighbors, thereby saving IP address resources.
- AmpCon-Campus automatically provisions ASN and BGP configurations for the overlay and underlay and provides routing configurations for core switches and uplink devices (such as routers, gateways, and firewalls).
- At the port level, you can select the uplink port of each core switch to be connected to a WAN device.

After each uplink port is chosen, AmpCon-Campus automatically assigns an uplink IP address, adds the link subnet to EBGp, and creates a default route to the WAN device.

Routing neighbor relationships are established and routing information is exchanged between core switches and the WAN device.

- The overlay data plane uses VXLAN as the encapsulation protocol, and the overlay control plane uses EVPN.
- Distributed VXLAN gateways are used, and the VXLAN L2 gateway is located at the access layer. VXLAN tunnels terminate at the access layer.

Designing MLAG Fabrics

AmpCon-Campus supports the two-layer (collapsed core layer and access layer) MLAG fabric architecture.

This architecture merges the core and distribution layers into a collapsed core layer. Merging these layers into a single layer turns the traditional three-tier hierarchical network into a two-tiered network.

By using AmpCon-Campus, you can design and manage two-layer MLAG fabrics to simplify the network topology, reduce latency, and lower costs by eliminating the need for separate core and distribution devices.

[Before You Begin](#)

[Adding MLAG Fabrics](#)

[1. Adding a Topology](#)

[2. Adding Switch Nodes](#)

[3. Configuring Networks](#)

[4. Allocating Ports](#)

[5. Confirming Configurations](#)

[Verifying the Deployment](#)

[Redeploying MLAG Fabrics](#)

Before You Begin

Before you design MLAG fabrics, ensure that the prerequisite tasks described in [Prerequisites](#) have been completed.

Adding MLAG Fabrics

1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** or **Admin** role.

NOTES

- AmpCon-Campus users with the **Readonly** role can't view and configure fabrics.
- AmpCon-Campus users with the **Operator** role can only view fabrics but can't configure fabrics.

2. Click **Design Network > Campus Fabric** from the navigation bar, and then click **+ Campus Fabric**.

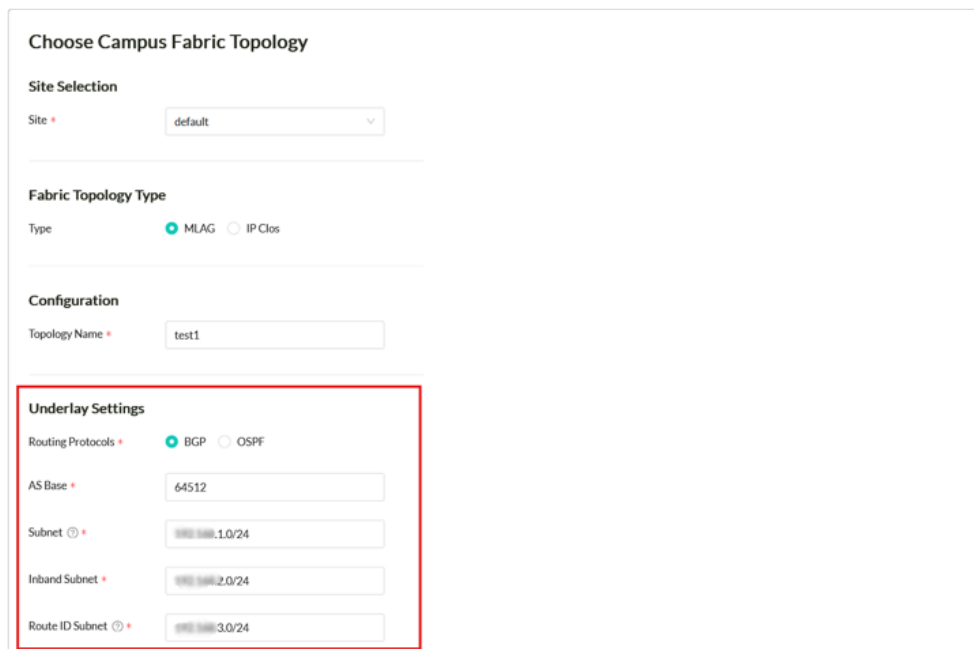
You are now redirected to the fabric design page. The fabric design includes the following processes:

1. Adding a Topology

1. In the **Site** drop-down list, select a site that you added.

If you didn't add any site as described in [Adding a Site](#), you can select the site **default**.

2. In the **Type** section, select **MLAG**, which means the fabric you are adding is an MLAG fabric.
3. In the **Topology Name** field, specify the name of the fabric topology. The name must be unique.
4. In the **Underlay Settings** section, select **BGP** or **OSPF**, which will be used as the underlay protocol.



Choose Campus Fabric Topology

Site Selection

Site *

Fabric Topology Type

Type ☒ MLAG ☐ IP Clos

Configuration

Topology Name *

Underlay Settings

Routing Protocols * ☒ BGP ☐ OSPF

AS Base *

Subnet ⓘ *

Inband Subnet *

Route ID Subnet ⓘ *

- If BGP is selected, enter the following information:
 - **AS Base:** The AS base number. Valid ranges are as follows:
 - 64512 to 65534 (16-bit)
 - 4200000000 to 4294967294 (32-bit)
 - **Subnet:** The IP address range used to allocate IP addresses to underlay physical interfaces.
 - **Inband Subnet:** The IP address range allocated to interconnection interfaces of core and access switches.
 - **Route ID Subnet:** The IP address range used to allocate Router IDs for each device in the fabric. Router IDs are loopback interfaces (lo0.0) for the route protocol peering between devices.

NOTES

- **Subnet, Inband Subnet, and Route ID Subnet** values can't overlap.
- The maximum allowed prefix length for the **Subnet, Inband Subnet, and Route ID Subnet** is 28.

- For **Subnet**, **Inband Subnet**, and **Route ID Subnet** values, AmpCon-Campus automatically calculates and displays the network address based on the IP address and prefix length you input. For example, if you input 192.168.4.5/22 in the **Subnet** field, 192.168.4.0/22 will be displayed.

- If **OSPF** is selected, enter the following information:
 - **Area ID:** The OSPF area ID allocated to core switches. The default value is 0.0.0.0 and cannot be changed.
 - **Subnet:** The IP address range used to allocate IP addresses to underlay physical interfaces.
 - **Inband Subnet:** The IP address range used to allocate IP addresses to interconnection interfaces of core and access switches.
 - **Route ID Subnet:** The IP address range used to allocate Router IDs for each device in the fabric. Router IDs are loopback interfaces (lo0.0) for the route protocol peering between devices.

NOTES

- **Subnet**, **Inband Subnet**, and **Route ID Subnet** values can't overlap.
- The maximum allowed prefix length for the **Subnet**, **Inband Subnet**, and **Route ID Subnet** is 28.
- For **Subnet**, **Inband Subnet**, and **Route ID Subnet** values, AmpCon-Campus automatically calculates and displays the network address based on the IP address and prefix length you input. For example, if you input 192.168.4.5/22 in the **Subnet** field, 192.168.4.0/22 will be displayed.

5. Click **Next** to add switches that form the campus fabric.

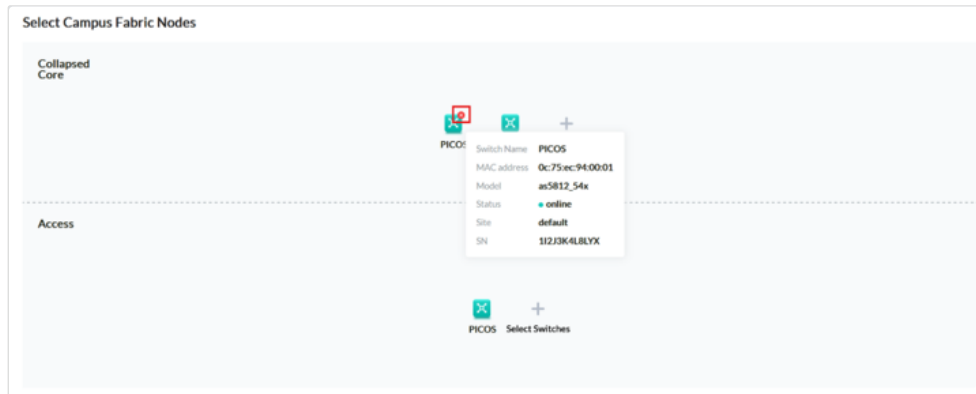
2. Adding Switch Nodes

1. In the **Collapsed Core** section, click **+** to add core switches. You must select two core switches.

NOTES

- Only online switches (can connect to the AmpCon-Campus server) can be added to the fabric.
- If a switch is added to a fabric, the switch can't be added to other fabrics.

2. In the **Access** section, click **+** to add access switches. You must select at least one access switch.
3. Optional: To remove a switch, hover over the switch, and then click the remove icon. Then, click **Yes** to complete the removal.



4. Click **Next** to add network configurations.

3. Configuring Networks

1. In the **Network** section, click **+ Add**, and then enter the following information:
 - **Name:** The network name. The name needs to be unique.
 - **VLAN ID:** The VLAN ID of the network. **VLAN ID** values in different networks can't be the same.
 - **Subnet:** Specify the subnet of the network. **Subnet** values in different networks can't overlap.
2. Click **Apply** to save the network configurations.

You can edit or delete networks as needed.

- To edit a network, locate the network, and then click **Edit**.
- To delete a network, locate the network, and then click **Delete**.

Network			
Network		+ Add	
Name	VLAN ID	Subnet	Operation
test_template	55	0.0.0/24	Edit Delete
test	23	3.1.0/24	Edit Delete

3. In the **Domain ID** field, enter the MLAG domain ID, which is the unique identifier of the core switch MLAG.
4. In the **NAC** section, select **Enable** or **Disable** to enable NAC server configurations or not. AmpCon-Campus supports only 802.1X authentication and MAC authentication.

If you selected **Enable**, add an NAC server by clicking **+ Add** and entering the following information:

- **Name:** The name of the NAC server.
- **Server Address:** The IPv4 address of the NAC server.
- **Port:** The port used to connect to the NAC server. The default value is 1812.
- **Shared Secret:** The confidential key used for secure communication between the NAC server and other network devices.

i Tip

You can add one or multiple NAC servers, and you can edit or delete these NAC servers.

- To add another NAC server, click **+ Add** again.
- To edit the configurations of an NAC server, locate the NAC server, and then click **Edit**.
- To delete an NAC server, locate the NAC server, and then click **Delete**.

NAC

Configuration ☒ Enable ☐ Disable

Server [+ Add](#)

Server Name	Server Address	Port	Operation
test	1.1	1812	Edit Delete

5. In the **DHCP Snooping** section, select **Enable** or **Disable** to enable DHCP snooping or not.

If you selected **Enable**, add the network where DHCP snooping is enabled.

a. Click **+ Add**.

b. In the **Network** drop-down list, select a network from all networks that you added in

Step 1.

In the **VLAN ID** field, the VLAN ID of the selected network is added automatically and can't be changed.

i Tip

You can add one or multiple networks for DHCP snooping, and you can edit or delete these networks.

- To add another network, click **+ Add** again.
- To edit a network, locate the network, and then click **Edit**.
- To delete a network, locate the network, and then click **Delete**.

DHCP Snooping

Configuration ☒ Enable ☐ Disable

DHCP [+ Add](#)

Network	VLAN ID	Operation
test_template	55	Edit Delete

6. In the **DHCP Relay** section, select **Enable** or **Disable** to enable DHCP relay or not.

If you selected **Enable**, add the DHCP relay server and the network where DHCP relay needs to be enabled .

a. Click **+ Add**.

b. In the **Network** drop-down list, select a network from all networks that you added in **Step 1**.

In the **VLAN ID** field, the VLAN ID of the selected network is added automatically and can't be changed.

c. In the **DHCP Server** field, enter the IPv4 address of the DHCP server. If a PicOS switch is used as the DHCP server, you need to enter the Layer 3 IPv4 address of the DHCP server.

i Tip

You can enable DHCP relay for one or multiple networks, and you can edit or delete these DHCP relay configurations.

- To enable DHCP relay for another network, click **+ Add** again.
- To edit a DHCP relay configuration, locate the DHCP relay configuration, and then click **Edit**.
- To remove a DHCP relay configuration, locate the DHCP relay configuration, and then click **Delete**.

DHCP Relay

Configuration ☒ Enable ☐ Disable

DHCP [+ Add](#)

Network	VLAN ID	DHCP Server	Operation
test_template	55	1.1.1.1	Edit Delete

7. Click **Next** to allocate connection ports for all selected collapsed core and access switches.

4. Allocating Ports

1. In the **Core** tab, click **+** before a switch, and select ports connected to another core switch (peer link), access switches, and WAN devices (optional).

- Allocate two ports connected to the peer core switch.
 - a. Click a port. In the pop-up window, click **Link to Core**.
 - b. Click another port. In the pop-up window, click **Link to Core**.

i NOTE

In MLAG fabrics, you can assign only two core switches. For each core switch, you need to allocate two ports to connect to the peer core switch.

- Allocate ports connected to all the access switches.
 - a. Check the **Link to Access** column to see how many ports need to be allocated.
 For example, **0/2** means that you must allocate two ports to connect to two access switches but now you haven't allocated any port.
 - b. Click a port. In the pop-up window, click **Link to Access**.
 - c. Repeat **Step b** to allocate all required number of ports.
- If core switches need to connect to a WAN device, allocate ports connected to the WAN device by clicking a port and then clicking **Link to WAN** in the pop-up window.

i NOTES

- For each core switch, you can allocate at most one port connected to a WAN device.
- If core switches don't need to connect to a WAN device, do not click **Link to WAN**.

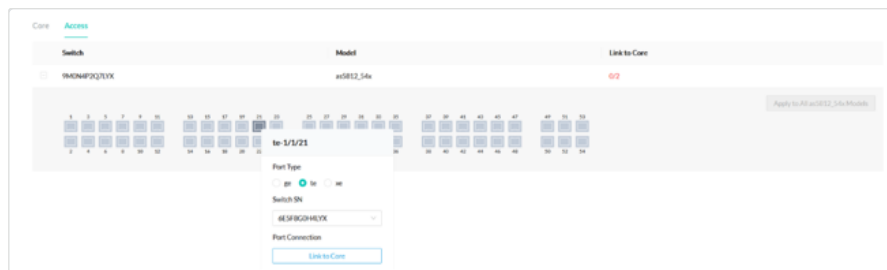
2. Repeat **Step 1** to allocate ports for the other core switch.

You can also click **Apply to All xx Models** to apply the port allocation choice to the other core switch of the same model.

3. In the **Access** tab, click **+** before an access switch, and select ports connected to two core switches.
 - a. Click a port.
 - b. In the pop-up window, select a core switch from the **Switch SN** drop-down list.
 - c. Click **Link to Core**.
 - d. Repeat **Step a to c** to allocate another port connected to the other core switch.

e. Check the **Link to Core** column of all access switches, and ensure that the numbers are displayed in green, which means all required ports have been allocated.

For example, the **Link to Core** column changes from 0/2 to 2/2.



4. Repeat **Step 3** to allocate ports for all the other access switches.

You can also click **Apply to All xx Models** to apply the port allocation choice to all the other access switches of the same model.

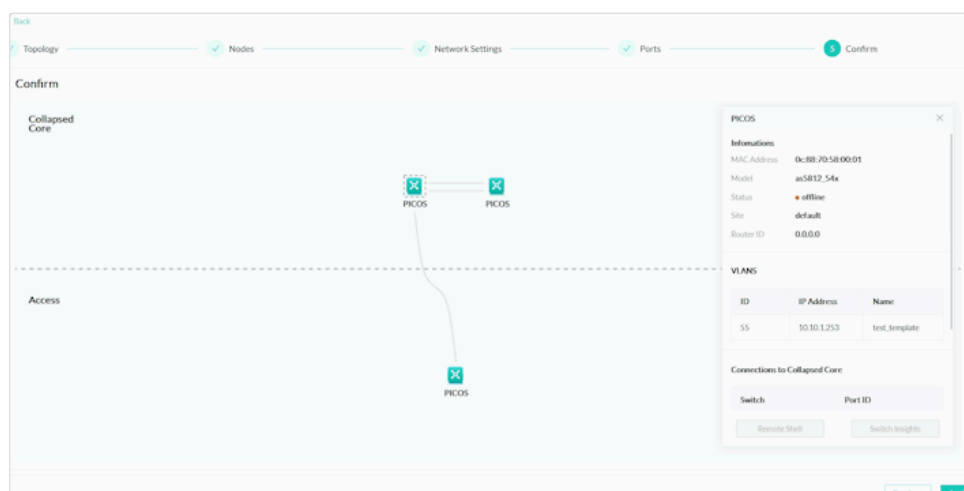
5. Click **Next** to confirm the fabric configurations.

5. Confirming Configurations

1. Click a blank space in the canvas to show all links in the topology, and then check whether the topology is correct.
2. Click each switch, and check fabric configurations in the pop-up window.

NOTE

You must check the **Status** column of each switch and ensure that all switches are in **online** status, which means the switches can connect to the AmpCon-Campus server. Fabric configurations will not be pushed to offline switches.



3. Optional: To check the details of a switch, click **Switch Insights** in the **PICOS** pop-up window. You can see the “Switch” page in a new browser tab.

NOTE

Only when the switch is online, the **Switch Insights** button can be clicked.

- Optional: To connect to a switch from the AmpCon-Campus UI through an SSH session, click **Remote Shell**. In the pop-up window, enter the username and password to log in to the switch.

NOTE

Only when the switch is online (can connect to the AmpCon-Campus server), the **Remote Shell** button can be clicked.

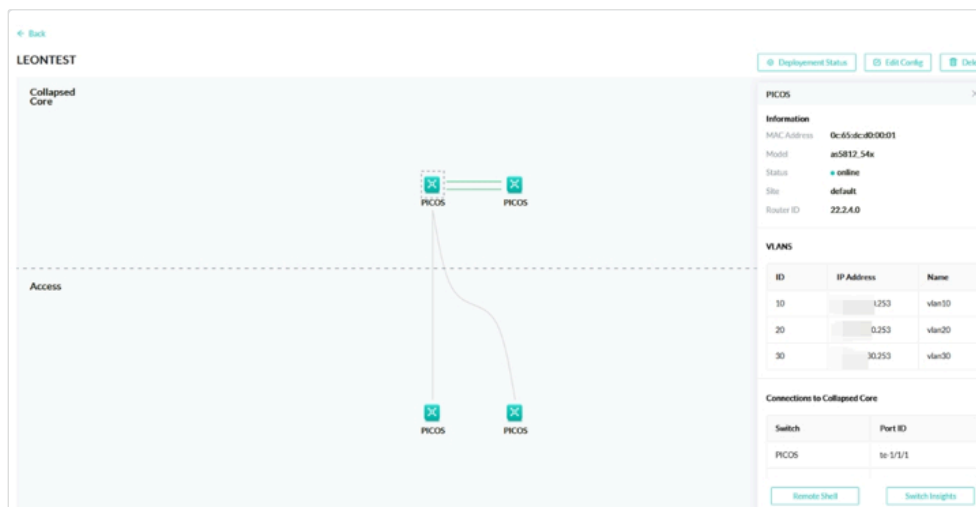
- Click **Apply** to push the fabric configurations to the selected core and access switches. You are redirected to the “Campus Fabric” page.

The configuration pushing process takes about 10 minutes (depending on the number of switches in the fabric) to complete.

Verifying the Deployment

To check whether the fabric configurations are pushed to switches successfully, follow these steps:

- On the “Campus Fabric” page, locate the fabric, and then click **View**.
- Click the **Deployment Status** button to go to the status page.



- Check the **Deployment Status** column to see whether the status is **SUCCEEDED**.

← Back

LEONTEST

Q Search

System	IP	Device Type	Deployment Status	Operation
PICOS	0.6/15 3.10.253	core	PENDING	Log
PICOS	1.10/ 68.10.252	core	PENDING	Log
PICOS	114	access	PENDING	Log
PICOS	.0.10	access	PENDING	Log

1-4 of 4 items 1 10 / page

- If the deployment status of any switch is **FAILED**, click **Log** to check more details for troubleshooting.

Example

You might see the error message “Error: Configuration failed on host xxx: commit;BGP instance is already running; AS is 111; Commit failed” in the log.

This error message means that the BGP local AS has been configured on the switch. You need to log in to the switch and delete these configurations first. Then, redeploy the fabric as described in [Redeploying MLAG Fabrics](#).

- If the deployment status of any switch is **PENDING**, the fabric is waiting to be deployed.
- If the deployment status of any switch is **RUNNING**, the fabric is being deployed.
- If the deployment status of all switches is **SUCCEED**, the fabric deployment is finished.

Redeploying MLAG Fabrics

If fabric configurations are not pushed to switches due to some reasons, resolve the issues based on switch logs, and then redeploy the fabric by following these steps:

1. On the “Campus Fabric” page, locate the fabric, and then click **View**.
2. Click **Edit Config** to edit the fabric.
3. Click **Next** until you go to the **Confirm** section.
4. Check whether all switches in the fabric are in online status, and then click **Apply**.

Designing IP Clos Fabrics

IP Clos is a network design architecture commonly used in large-scale campus networking.

The IP Clos fabric architecture provides a scalable and flexible solution for interconnecting multiple switches in a hierarchical manner, allowing efficient utilization of network resources and simplified routing.

By using AmpCon-Campus, you can design and manage 5-stage IP Clos fabrics to meet the increasing network challenges.

NOTE

Currently, this feature is for experimental purposes only.

[Before You Begin](#)

[Adding IP Clos Fabrics](#)

[1. Adding a Topology](#)

[2. Adding Switch Nodes](#)

[3. Configuring Networks](#)

[4. Allocating Ports](#)

[5. Confirming Configurations](#)

[Verifying the Deployment](#)

[Redeploying IP Clos Fabrics](#)

[What to Do Next](#)

Before You Begin

Before you design IP Clos fabrics, ensure that the prerequisite tasks described in [Prerequisites](#) have been completed.

Adding IP Clos Fabrics

1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** or **Admin** role.

NOTEs

- AmpCon-Campus users with the **Readonly** role can't view and configure fabrics.
- AmpCon-Campus users with the **Operator** role can only view fabrics but can't configure fabrics.

2. Click **Network Design > Campus Fabric** from the navigation bar, and then click **+ Campus Fabric**.

Campus Fabric						
+ Campus Fabric Q Search						
Name	Site	Topology Type	Date Created	Operation		
test_1009_ip_clos	default	IP Clos	2025-10-09 04:12:22	View	Delete	
test_1008_onsp_mlag	default	IP Clos	2025-10-09 06:58:32	View	Delete	
test_fabric_mlag	default	IP Clos	2025-10-10 02:29:37	View	Delete	
test_fabric_mh	default	IP Clos	2025-10-10 02:41:31	View	Delete	
test_MLAG	default	MLAG	2025-10-10 03:12:35	View	Delete	
1-5 of 5 items < 1 > 10 / page						

You are now redirected to the fabric design page. The fabric design includes the following processes:

1. Adding a Topology

1. In the **Site** drop-down list, select a site that you added.
- If you didn't add any sites as described in [Adding a Site](#), you can select the site **default**.
2. In the **Type** section, select **IP Clos**, which means the fabric you are adding is an IP Clos fabric.
3. In the **Virtualization Technology** section, select the virtualization technology used between core switches to provide redundancy and high availability for downstream distribution switches.
- Currently, only MLAG is supported, and MLAG is selected by default.
- When MLAG is selected, the two core switches operate as an MLAG pair. You must specify the MLAG domain ID in the **Domain ID** field to identify the MLAG domain uniquely.
4. In the **Topology Name** field, specify the name of the fabric topology. The name must be unique.
5. In the **Underlay Settings** section, enter the following information:

1

Topology

2

Nodes

3

Network Settings

4

Ports

5

Confirm

Choose Campus Fabric Topology

Site Selection

Site *

default

Fabric Topology Type

Type

MLAG

IP Clos

Virtualization Technology

Choose

MLAG

Domain ID *

23

Configuration

Topology Name *

a

Underlay Settings

BGP Local AS *

40002

Subnet *

192.168.1.0/24

Route ID Subnet *

192.168.1.0/24

Table 1. Underlay Settings Parameters

Parameter	Description
-----------	-------------

BGP Local AS	The AS base number. Valid ranges are as follows: • 64512 to 65534 (16-bit) • 4200000000 to 4294967294 (32-bit)
Subnet	The IP address range used to allocate IP addresses to underlay physical interfaces.
Route ID Subnet	The IP address range used to allocate Router IDs for each device in the fabric. Router IDs are loopback interfaces (lo0.0) for the route protocol peering between devices. NOTES • Subnet and Route ID Subnet values can't overlap. • The maximum allowed prefix length for the Subnet and Route ID Subnet is 28. • For Subnet and Route ID Subnet values, AmpCon-Campus automatically calculates and displays the network address based on the IP address and prefix length you input. For example, if you input 192.168.4.5/22 in the Subnet field, 192.168.4.0/22 will be displayed.

6. Click **Next** to add switches that form the campus fabric.

2. Adding Switch Nodes

1. In the **Core** section, click **+** to add core switches.

NOTES

- Only online switches (can connect to the AmpCon-Campus server) can be added to the fabric.
- If a switch is added to a fabric, the switch can't be added to other fabrics.
- You must add 2 core switches.

✓ Topology

2 Nodes

3 Network Settings

4 Ports

5 Confirm

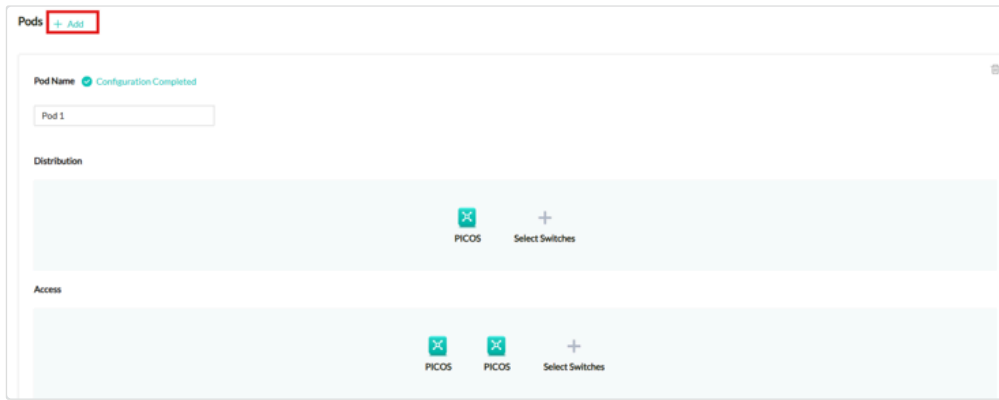
Select Campus Fabric Nodes

Core

+

Select Switches

2. In the **Pods** section, click **+ Add** to add pods. A pod is composed of distribution switches and access switches. You can add one or multiple pods.

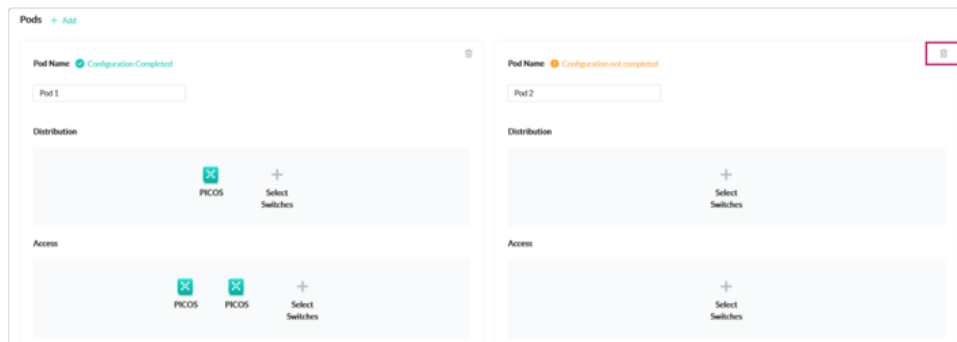


3. In each pod, click **+** to add distribution switches and access switches.

NOTES

- Add at least one distribution switch in each pod.
- If you add only one pod, add at least two access switches in the pod.
- If you add two or more pods, add at least one access switch in each pod.

To remove a pod, click the remove icon in the canvas.



To remove a switch, hover over the switch, and then click the remove icon. Then, click **Yes** to complete the removal.



4. Click **Next** to add network configurations.

3. Configuring Networks

1. In the **Network** section, click **+ Add**, and then enter the following information:

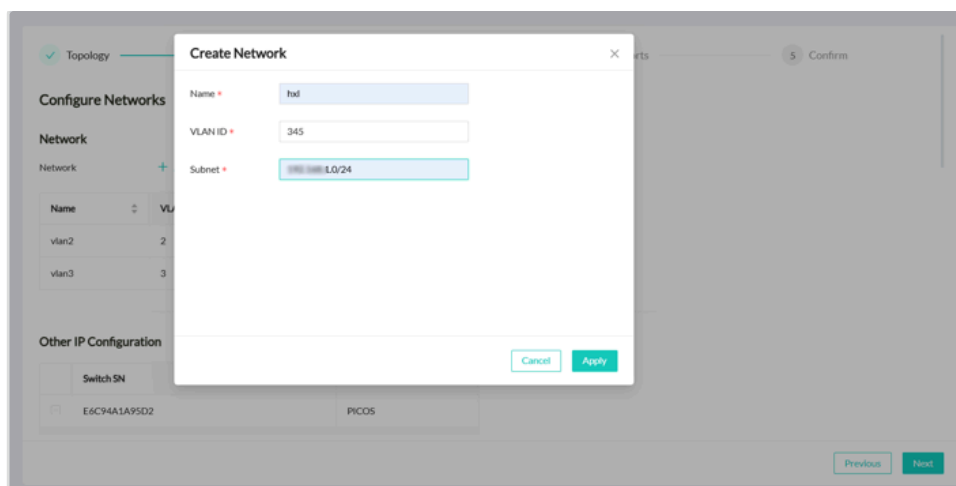


Table 2. Network Parameters

Parameter	Description
Name	Specify the network name. The name needs to be unique.
VLAN ID	Specify the VLAN ID of the network. The VLAN ID needs to be unique with valid ranges from 2 to 3837.
Subnet	Specify the subnet of the network. The subnet needs to be unique. NOTE Subnet values in different networks can't overlap.

Tip

You can add one or multiple networks, and you can edit or delete these networks.

- To add another network, click **+ Add** again.
- To edit a network, locate the network, and then click **Edit**.
- To delete a network, locate the network, and then click **Delete**.

2. In the **Other IP Configuration** section, you don't need to do anything. AmpCon-Campus automatically assigns an Anycast IP address to each switch in the fabric. The Anycast IP address is a virtual IP used for distributed VXLAN.

The screenshot shows a configuration page for a switch. At the top, there's a 'Network' section with a '+ Add' button and a table:

Name	VLAN ID	Subnet	Operation
vlan2	2	192.168.1.0/2	Edit Delete
vlan3	3	192.168.1.0/3	Edit Delete

Below this is the 'Other IP Configuration' section, which is highlighted with a red box. It contains two sub-tables:

Switch SN	Label
☐ E6C94A1A95D2	PICOS

Network	Anycast IP Address
vlan2	255.255.255.254
vlan3	223.255.255.254

At the bottom right, there are 'Previous' and 'Next' buttons.

3. In the **VRF** section, click **+ Add** and add a VRF instance as follows:

i **NOTE**

You must add at least one but no more than 128 VRF instances.

The screenshot shows a 'Create VRF' dialog box. It has two main fields:

- Name**: A text input field containing the value 'test'.
- Networks**: A dropdown menu with a green plus icon and the text 'Add', currently showing 'test'.

At the bottom of the dialog, there are 'Cancel' and 'Apply' buttons. The background shows a blurred view of the VRF configuration page.

Table 3. VRF Parameters

Parameter	Description
Name	The name of the VRF instance. <i>i</i> NOTES - The VRF name needs to be a string of 1 to 15 case-sensitive characters; spaces are not supported. - The VRF name can't be the same as any network name. - The VRF name can contain only letters, numbers, and special characters (- . _ @ = #).

	• The keywords tun0, lo, mgmt-vrf, default, eth0, eth1, gretap0, bridge0, erspan0, bridge, sit0, pimreg, and ipmr-lo cannot be configured as VRF names. • The keywords starting with te, ge, eth, ae, and xe followed by numbers cannot be configured as VRF names. For example, test is a valid VRF name, but te01 is not a valid VRF name. • The keywords starting with vlan followed by any characters cannot be configured as VRF names. For example, vlan0 or vlan.0 is not a valid VRF name.
Networks	The networks to which the VRF belongs. The optional networks are those you added in Step 1 of this section, and you can select one or multiple of them. NOTE If all networks have already been bound to VRFs, you cannot add a new VRF.

Tip

You can add one or multiple VRF instances, and you can edit or delete these VRF instances.

- To add another VRF instance, click **+ Add** again.
- To edit a VRF instance, locate the VRF instance, and then click **Edit**.
- To delete a VRF instance, locate the VRF instance, and then click **Delete**.

4. In the **NAC** section, select **Enable** or **Disable** to enable NAC server configurations or not. AmpCon-Campus supports only 802.1X authentication and MAC authentication.

If you selected **Enable**, add an NAC server by clicking **+ Add** and entering the following information:

Table 4. NAC Server Parameters

Parameter	Description
Name	The name of the NAC server.
Server Address	The IPv4 address of the NAC server.
Port	The port used to connect to the NAC server. The default value is 1812.
Shared Secret	The confidential key used for secure communication between the NAC server and other network devices.

Tip

You can add one or multiple NAC servers, and you can edit or delete these NAC servers.

- To add another NAC server, click **+ Add** again.
- To edit the configurations of an NAC server, locate the NAC server, and then click **Edit**.
- To delete an NAC server, locate the NAC server, and then click **Delete**.

5. In the **VNI** section, click **+ Add** to add a VNI as follows:

NOTES

- A VLAN can only be bound to one VNI, and a VNI can also be bound to one VLAN.

- The number of VNIs that can be added is equal to the number of networks in the IP Clos fabric

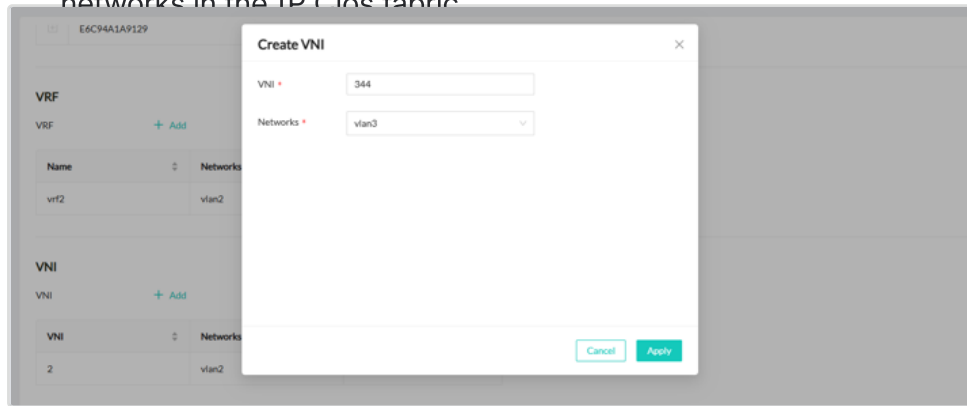


Table 5. VNI Parameters

Parameter	Description
VNI	The value of VNI. The available value of VNI ranges from 1 to 16777086.
Networks	The VLAN to which you want to bind the VNI. The optional networks are those you added in Step 1 of this section.

Tip

You can add one or multiple VNIs, and you can edit or delete these VNIs.

- To add another VNI instance, click **+ Add** again.
- To edit a VNI, locate the VNI, and then click **Edit**.
- To delete a VNI, locate the VNI, and then click **Delete**.

6. In the **DHCP Relay** section, select **Enable** or **Disable** to enable DHCP relay or not.

If you selected **Enable**, click **+ Add** and add the DHCP relay server and the network where the DHCP relay needs to be enabled.

Table 6. DHCP Relay Parameters

Parameter	Description
Network	The network to which the DHCP relay belongs. The optional networks are those you added in Step 1 of this section.
VLAN ID	The VLAN ID of the selected network. It is added automatically and can't be changed.
DHCP Server	The IPv4 address of the DHCP relay server.

Tip

You can enable DHCP relay for one or multiple networks, and you can edit or delete these DHCP relay configurations.

- To enable DHCP relay for another network, click **+ Add** again.
- To edit a DHCP relay configuration, locate the DHCP relay configuration, and then click **Edit**.
- To remove a DHCP relay configuration, locate the DHCP relay configuration, and then click **Delete**.

4. Allocating Ports

NOTE

The ports allocated must be consistent with the actual physical port connections. Or else, even though the fabric configurations can be pushed to switches, the fabric will not work.

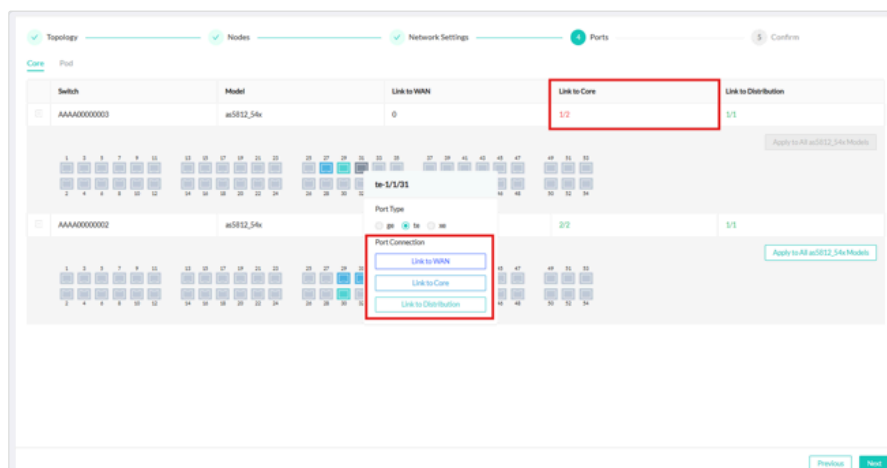
1. In the **Core** tab, click **+** before a core switch, and select the ports connected to a core switch, a WAN device, or distribution switches.

Switch	Model	Link to WAN	Link to Distribution
E6CHASAP131	ac5812_54e	1/1	1/1
E6CHASAP132	ac5812_54e	1/1	1/1

- You need to select the ports connected to distribution switches.
 - a. Check the **Link to Distribution** column to see how many ports need to be allocated.
 - b. Click a port. In the pop-up window, click **Link to Distribution**.
 - c. Repeat **Step b** to allocate the ports connected to all the other distribution switches.
- You need to select the ports connected to another core switch.
 - a. Click a port. In the pop-up window, click **Link to Core**.
 - b. Repeat **Step a** to allocate the next port connected to another core switch.

NOTE

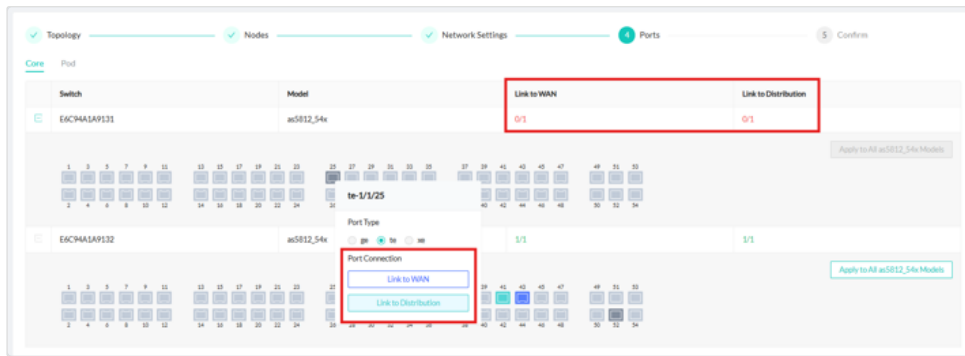
For each core switch, you must allocate two ports connected to another core switch.



- If core switches need to connect to a WAN device, allocate the ports connected to WAN devices by clicking a port and then clicking **Link to WAN** in the pop-up window.

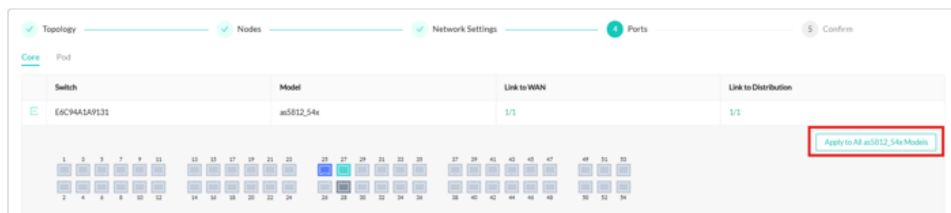
NOTES

- For each core switch, you can allocate at most one port connected to a WAN device.
- If core switches don't need to connect to a WAN device, do not click **Link to WAN**.



2. Repeat **Step 1** to allocate ports for the other core switches.

You can also click **Apply to All xx Models** to apply the port allocation choice to the other core switches of the same model.



3. In the **Distribution** section of the **Pod** tab, click **+** before a distribution switch, and select ports connected to core and access switches.

a. Check the **Link to Core** column to see how many ports need to be allocated.

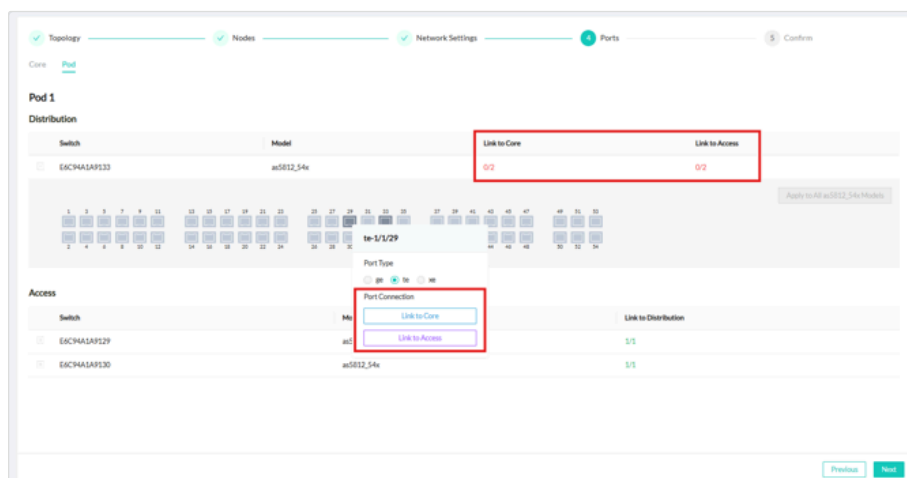
b. Click a port. In the pop-up window, click **Link to Core**.

c. Repeat **Step b** to allocate ports connected to all the other core switches.

d. Check the **Link to Access** column to see how many ports need to be allocated.

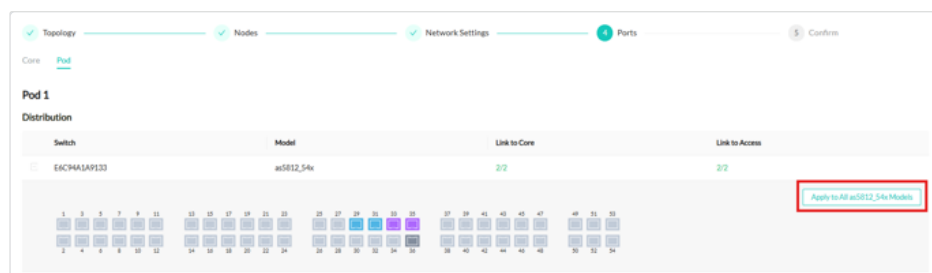
f. Click a port. In the pop-up window, click **Link to Access**.

g. Repeat **Step f** to allocate ports connected to all the other access switches.

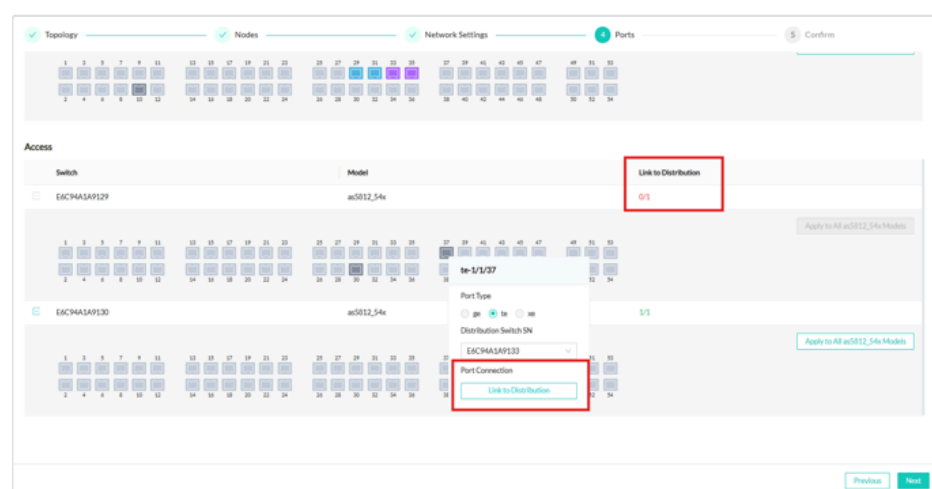


4. Repeat **Step 3** to allocate ports for the other distribution switches.

You can also click **Apply to All xx Models** to apply the port allocation choice to the other distribution switches of the same model.

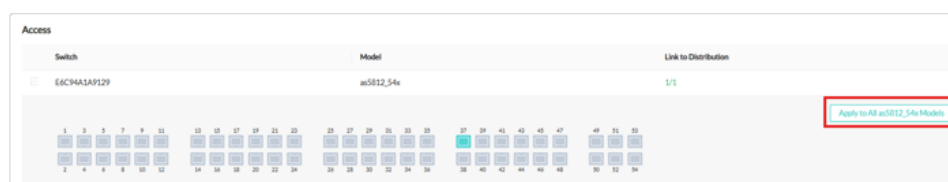


5. In the **Access** section of the **Pod** tab, click **+** before an access switch, and select ports connected to distribution switches.
 - a. Check the **Link to Distribution** column to see how many ports need to be allocated.
 - b. Click a port. In the pop-up window, select a distribution switch from the **Distribution Switch SN** list.
 - c. Click **Link to Distribution**.
 - d. Repeat **Step b to c** to allocate ports connected to all the other distribution switches.



6. Repeat **Step 5** to allocate ports for the other access switches.

You can also click **Apply to All xx Models** to apply the port allocation choice to the other access switches of the same model.



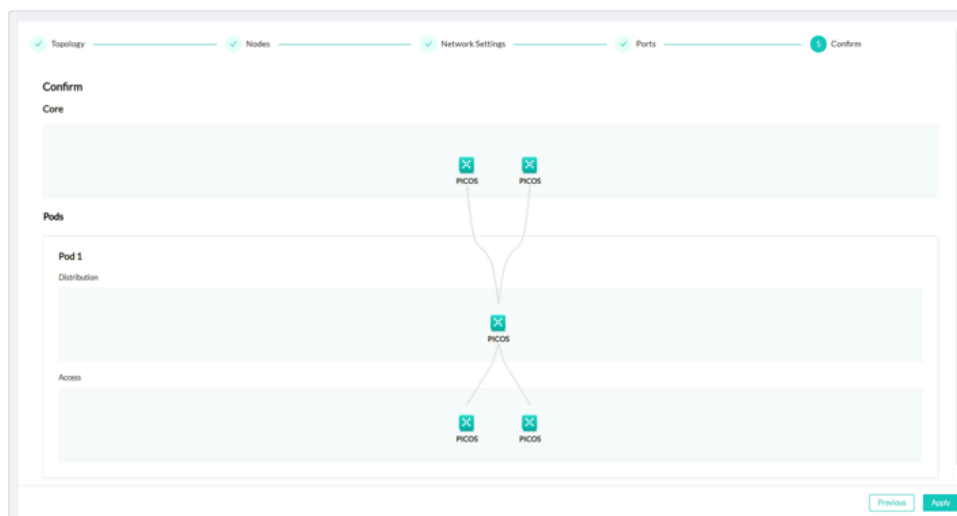
7. Click **Next** to confirm the fabric configurations.

5. Confirming Configurations

1. Click a blank space in the canvas to show all links in the topology, and then check whether the topology is correct and whether links are displayed in green.

NOTES

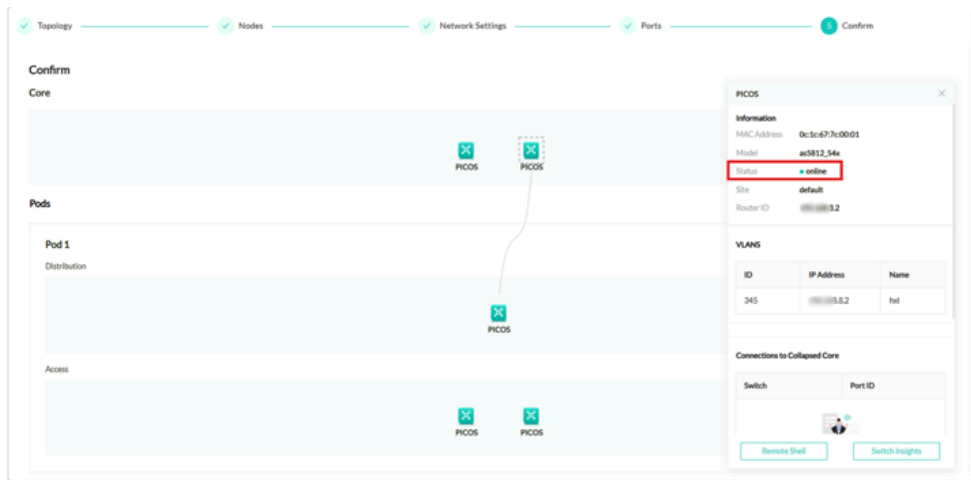
- When the ports allocated match the actual physical port connections, the port connections in the IP Clos fabric are displayed in **green**.
- When the ports allocated don't match the actual physical port connections, the port connections in the IP Clos fabric are displayed in **gray**.



2. Click each switch, and check fabric configurations in the pop-up window.

NOTE

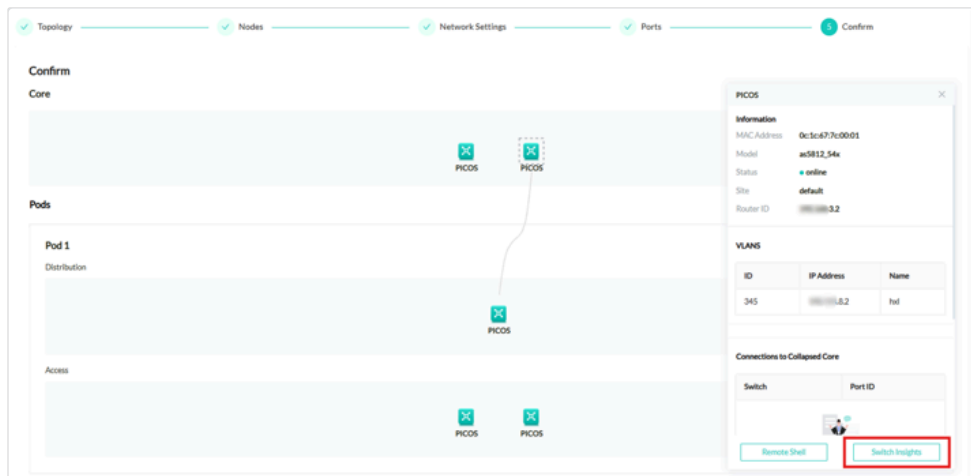
You must check the **Status** column of each switch and ensure that all switches are in **online** status, which means the switches can connect to the AmpCon-Campus server. Fabric configurations will not be pushed to offline switches.



3. Optional: To check the details of a switch, click **Switch Insights** in the **PICOS** pop-up window. You can see the “Switches” page in a new browser tab.

NOTE

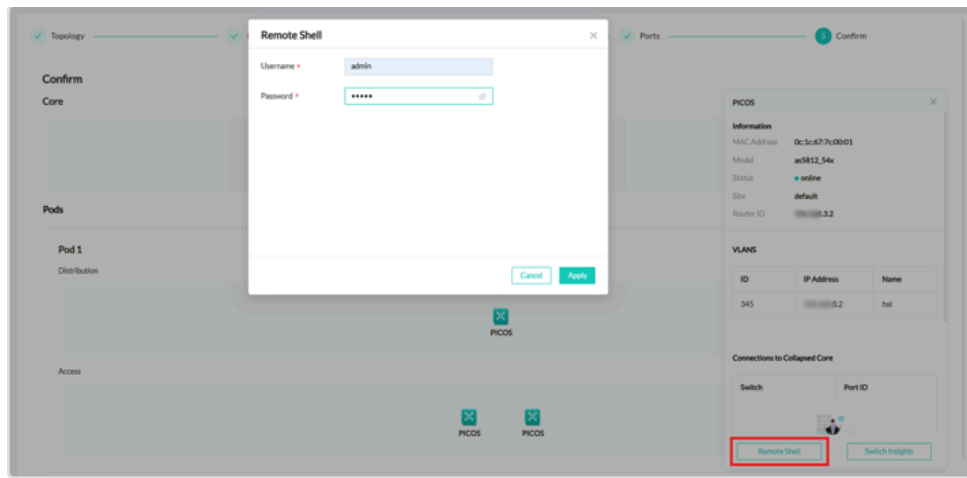
Only when the switch is online, the **Switch Insights** button can be clicked.



4. Optional: To connect to a switch from the AmpCon-Campus UI through an SSH session, click **Remote Shell**. In the pop-up window, enter the username and password to log in to the switch.

NOTE

Only when the switch is online (can connect to the AmpCon-Campus server), the **Remote Shell** button can be clicked.

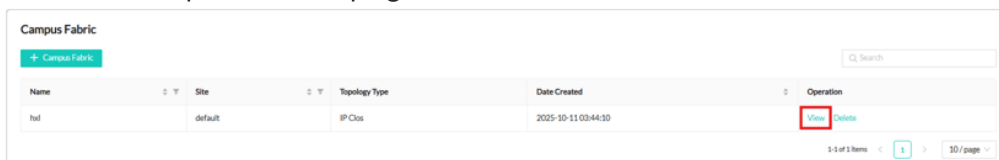


5. Click **Apply** to push the fabric configurations to the selected switches. You are redirected to the “Campus Fabric” page.

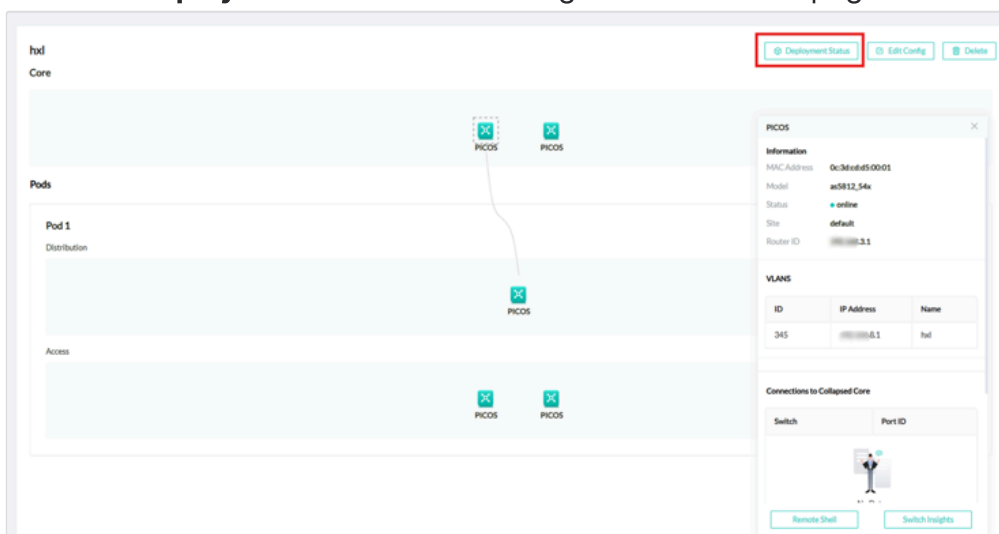
Verifying the Deployment

To check whether the fabric configurations are pushed to switches successfully, follow these steps:

1. On the “Campus Fabric” page, locate the fabric, and then click **View**.



2. Click the **Deployment Status** button to go to the “Status” page.



3. Check the **Deployment Status** column to see whether the status is **SUCCEED**.

- If the deployment status of any switch is **FAILED**, click **Log** to check more details for troubleshooting.

Sysname	SN	VPN IP	Mgmt IP	Device Type	Deployment Status	Operation
PICOS	E6C94A1A9131	10.10.10.14		core	SUCCESS	Log
PICOS	E6C94A1A9132	10.10.10.30		core	FAILED	Log
PICOS	E6C94A1A9133	10.10.10.42		distribution	FAILED	Log
PICOS	E6C94A1A9129	10.10.10.46		access	FAILED	Log
PICOS	E6C94A1A9130	10.10.10.30		access	FAILED	Log

Example

You might see the error message “Error: Configuration failed on host xxx: commit;BGP instance is already running; AS is 111; Commit failed” in the log.

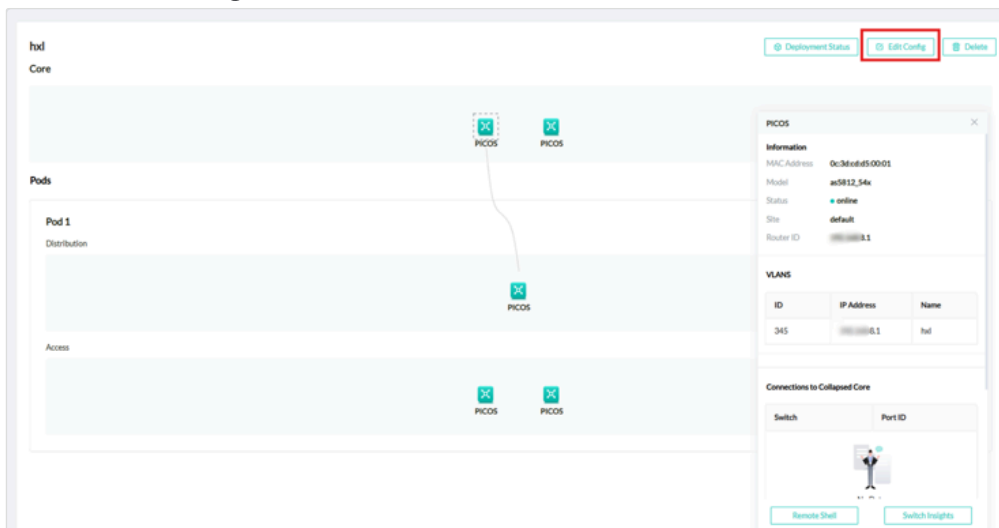
This error message means that the BGP local AS has been configured on the switch. You need to log in to the switch and delete these configurations first. Then, redeploy the fabric as described in [Redeploying IP Clos Fabrics](#).

- If the deployment status of any switch is **PENDING**, the fabric is waiting to be deployed.
- If the deployment status of any switch is **RUNNING**, the fabric is being deployed.
- If the deployment status of all switches is **SUCCEED**, the fabric deployment is finished.

Redeploying IP Clos Fabrics

If fabric configurations are not pushed to switches for some reason, resolve the issues based on switch logs, and then redeploy the fabric by following these steps:

1. On the “Campus Fabric” page, locate the fabric, and then click **View**.
2. Click **Edit Config** to edit the fabric.



3. Click **Next** until you go to the **Confirm** section.
4. Check whether all switches in the fabric are in online status, and then click **Apply**.

What to Do Next

After the IP Clos fabric is created, if you need to modify the overlay-related configurations (VRF, VNI, and DHCP relay configurations), you can quickly modify these configurations on the "Overlay Service Activation" page. For more information, see [Provisioning Overlay Services](#).

Provisioning Overlay Services

Overlay is a virtual network architecture built on top of an existing physical network (underlay). Overlay services refer to virtualized network functions or logical layers, which enable flexible service deployment and network configurations without modifying the underlying infrastructure.

After you create an IP Clos fabric on the “Campus Fabric” page, if overlay configurations (VRF, VNI, and DHCP relay configurations) for the IP Clos fabric need to be changed, you can quickly modify these configurations on the “Overlay Service Activation” page.

After you modify overlay configurations for an IP Clos fabric on the “Overlay Service Activation” page, these configurations will be directly pushed to switches in the IP Clos fabric, and you don’t need to redeploy this IP Clos fabric on the “Campus Fabric” page.

NOTE

The overlay configurations are used only for IP Clos fabrics.

[Prerequisites](#)

[Procedure](#)

Prerequisites

You have created IP Clos fabrics on the “Campus Fabric” page.

Procedure

To modify overlay configurations for switches in an IP Clos fabric, follow these steps:

1. Click **Network Design > Overlay Service Activation** from the navigation bar.
2. Input or select an IP Clos fabric from the **Fabric** drop-down list.

Overlay Service Activation

Fabric

Fabric *

VRF

+ VRF

VRF Name	Networks	Operation
hsl-ver	hsl	Edit Delete

VNI

+ VNI

VNI	Networks	Operation
344	hsl	Edit Delete

Cancel Apply

3. In the **VRF** section, click **+ VRF** to add a VRF instance:

NOTE

You must add at least one but no more than 128 VRF instances.

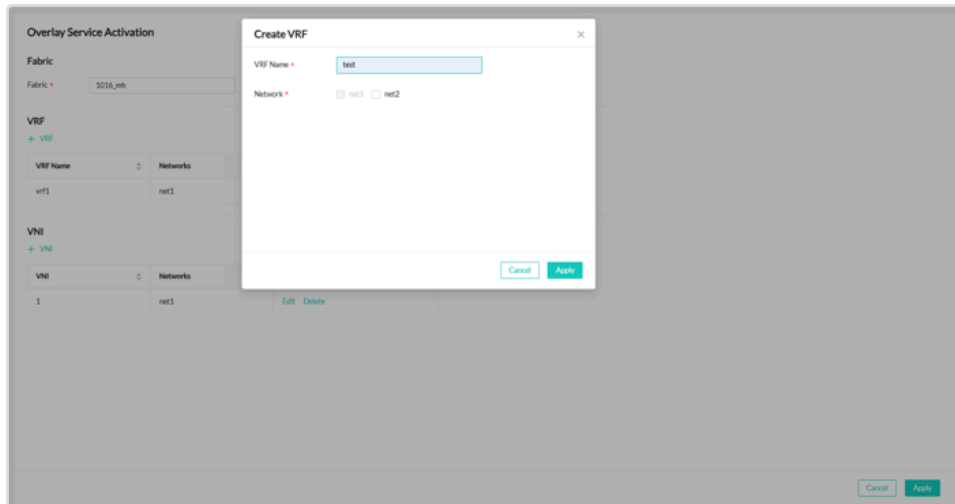


Table 1. VRF Parameters

Parameter	Description
VRF Name	The name of the VRF instance. NOTES - The VRF name needs to be a string of 1 to 15 case-sensitive characters; spaces are not supported. - The VRF name can contain only letters, numbers, and special characters (- . _ @ = #). - The VRF name can't be the same as any network name. - The keywords tun0, lo, mgmt-vrf, default, eth0, eth1, gretap0, bridge0, erspan0, bridge, sit0, pimreg, and ipmr-lo cannot be configured as VRF names. - The keywords starting with te, ge, eth, ae, and xe followed by numbers cannot be configured as VRF names. For example, test is a valid VRF name, but te01 is not a valid VRF name. - The keywords starting with vlan followed by any characters cannot be configured as VRF names.

	For example, vlan0 or vlan.0 is not a valid VRF name.
Networks	The networks to which the VRF belongs. The optional networks are those you added in Configuring Networks, and you can select one or multiple of them. NOTE If all networks have already been bound to VRFs, you cannot add a new VRF.

Tip

You can add one or multiple VRF instances, and you can edit or delete these VRF instances.

- To add another VRF instance, click **+ VRF** again.
- To edit a VRF instance, locate the VRF instance, and then click **Edit**.
- To delete a VRF instance, locate the VRF instance, and then click **Delete**.

4. In the **VNI** section, click **+ VNI** to add a VNI:

NOTES

- A VLAN can be bound to only one VNI, and each VNI can be bound to only one VLAN.
- The number of VNIs that can be added is equal to the number of networks in the IP Clos fabric.

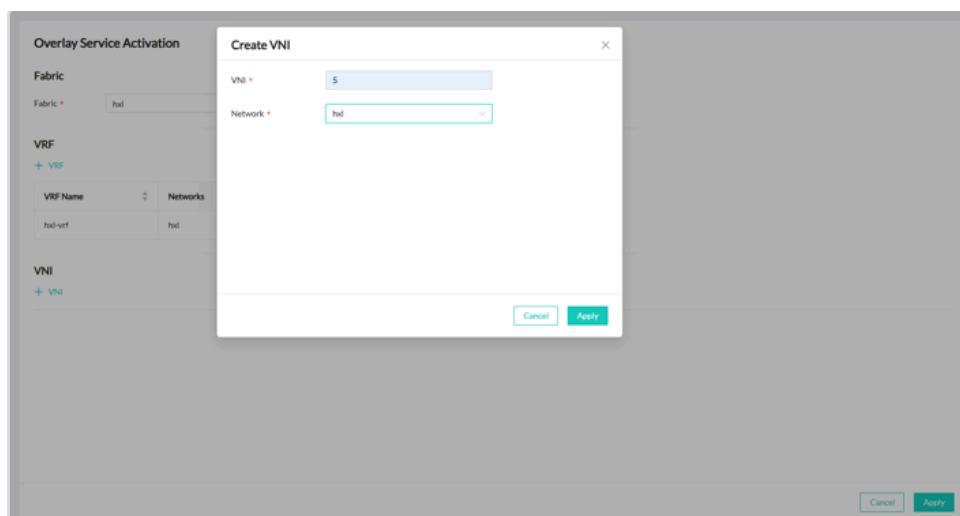


Table 2. VNI Parameters

Parameter	Description
VNI	The value of VNI. The available value of VNI ranges from 1 to 16777086.
Networks	The VLAN to which you want to bind the VNI. The optional networks are those you added in Configuring Networks .

Tip

You can add one or multiple VNIs, and you can edit or delete these VNIs.

- To add another VNI instance, click **+ VNI** again.
- To edit a VNI, locate the VNI and then click **Edit**.
- To delete a VNI, locate the VNI, and then click **Delete**.

5. In the **DHCP Relay** section, select **Enable** or **Disable** to enable DHCP relay or not.

If you selected **Enable**, click **+ DHCP Relay** and add the DHCP relay server and the network where the DHCP relay needs to be enabled.

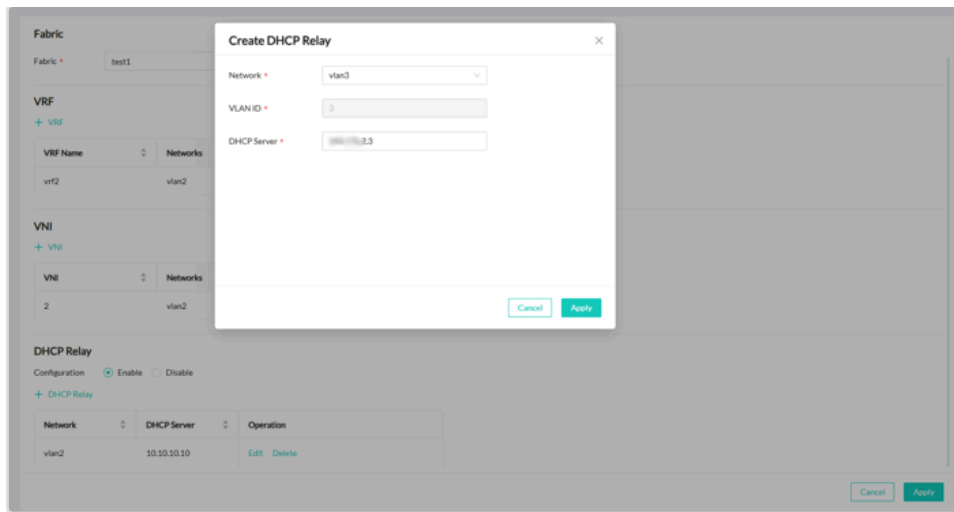


Table 3. DHCP Relay Parameters

Parameter	Description
Network	The network to which the DHCP relay belongs. The optional networks are those you added in Configuring Networks .
VLAN ID	The VLAN ID of the selected network. It is added automatically and can't be changed.
DHCP Server	The IPv4 address of the DHCP relay server.

Tip

You can enable the DHCP relay for one or multiple networks, and you can edit or delete these DHCP relay configurations.

- To enable the DHCP relay for another network, click **+ DHCP Relay** again.
- To edit a DHCP relay configuration, locate the DHCP relay configuration, and then click **Edit**.
- To remove a DHCP relay configuration, locate the DHCP relay configuration, and then click **Delete**.

6. Click **Apply** to push the modified configurations to switches in the IP Clos fabric.

Then, you are redirected to the “Status” page.

NOTE

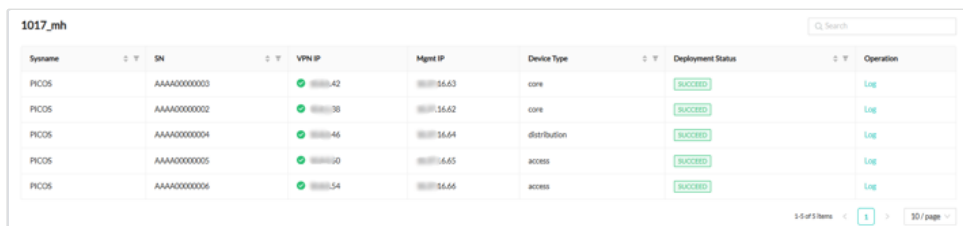
Before clicking **Apply**, pay attention to the following considerations:

- The **VRF** section must have at least one configuration.
- The **VNI** section must have at least one configuration.
- If you select **Enable** in the **DHCP Relay** section, this section must have at least one configuration.

7. Check whether the pushing result is **SUCCEED** on the “Status” page:

NOTE

After clicking **Apply**, the status page might not have data for a short time. This is because the task record has not been created in the database, and data will appear after the task record is created.



Sysname	SN	VPN IP	Mgmt IP	Device Type	Deployment Status	Operation
PC05	AAAA00000003	10.1.1.42	16.63	core	SUCCESS	Log
PC05	AAAA00000002	10.1.1.38	16.62	core	SUCCESS	Log
PC05	AAAA00000004	10.1.1.46	16.64	distribution	SUCCESS	Log
PC05	AAAA00000005	10.1.1.50	16.65	access	SUCCESS	Log
PC05	AAAA00000006	10.1.1.54	16.66	access	SUCCESS	Log

- If the deployment status of any switch is **FAILED**, click **Log** to check more details for troubleshooting.
- If the deployment status of any switch is **PENDING**, the fabric is waiting to be deployed.
- If the deployment status of any switch is **RUNNING**, the fabric is being deployed.
- If the deployment status of all switches is **SUCCEED**, the fabric deployment is finished.

Managing Campus Fabrics

You can manage the added fabrics in the AmpCon-Campus UI, such as redesigning a fabric, viewing fabric topology and configurations, and deleting a fabric.

[Viewing All Fabrics](#)

[Deleting a Fabric](#)

Viewing All Fabrics

In the AmpCon-Campus UI, click **Network Design > Campus Fabric** from the navigation bar. On the “Campus Fabric” page, you can see all the added fabrics.

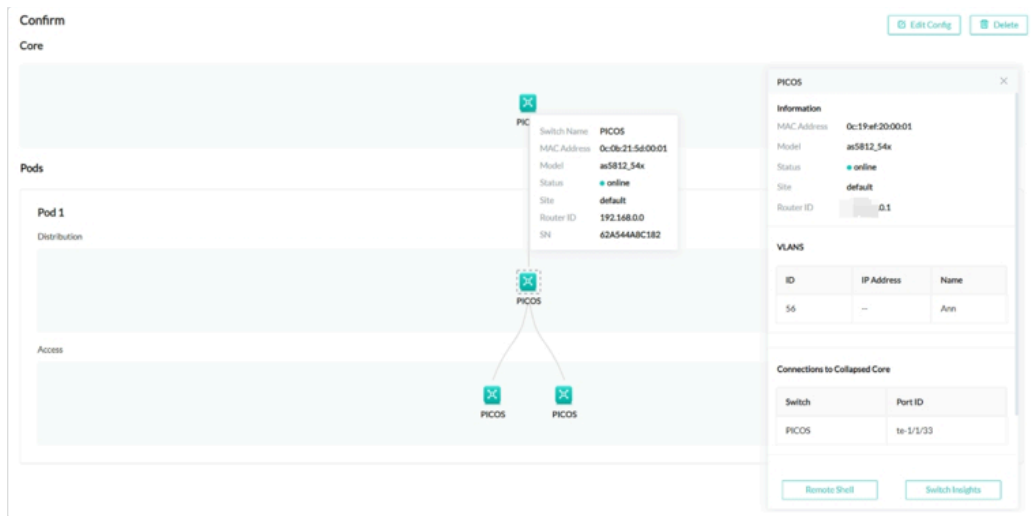
Topo						
+ Campus Fabric Q Search						
Name	Site	Topology Type	Date Created	Operation		
65101q	default	IP Clos	2025-03-20 03:32:30	View	Delete	
test	default	IP Clos	2025-03-20 03:58:23	View	Delete	
test_m	default	MLAG	2025-03-20 06:57:17	View	Delete	
test1	default	IP Clos	2025-03-20 08:03:40	View	Delete	
test_a	default	IP Clos	2025-03-20 09:37:50	View	Delete	

Table 1. Fabric Metrics

Metric	Description
Name	The name of the fabric.
Site	The site containing the fabric.
Topology Type	The type of the fabric, IP Clos or MLAG .
Date Created	The last time when you created the fabric.

To check the fabric configurations and topology, locate the fabric, click **View**. Click a blank space in the canvas, and then the whole topology is displayed.

To check the details of a switch, hover over the switch in the canvas.



Deleting a Fabric

To delete a fabric, use either of the following ways:

- Deleting through the “Campus Fabric” page
 1. On the “Campus Fabric” page, locate the fabric, and then click **Delete**.
 2. Click **Yes** to confirm the deletion.
- Deleting through the fabric view page
 1. On the “Campus Fabric” page, locate the fabric, and click **View**.
 2. On the fabric view page, click **Delete**.
 3. Click **Yes** to confirm the deletion.

Managing Switches

After onboarding PicOS switches, you can manage these switches with AmpCon-Campus.

AmpCon-Campus streamline lifecycle management of PicOS switches, helping you increase network management efficiency and focus on more strategic tasks.

See the following child topics:

- [Viewing Managed PicOS Switches](#)
- [Managing the Parking Lot](#)
- [Uploading and Upgrading PicOS Images](#)
- [Returning Merchandise Authorization for Switches](#)
- [Decommissioning Switches](#)
- [Removing Switches](#)

NOTE

These child topics are applicable to only PicOS switches.

Viewing Managed PicOS Switches

You can view managed switches as follows:

[Viewing the Switch List](#)

[Viewing Telemetry Data of a Switch](#)

[Viewing the Parking Lot](#)

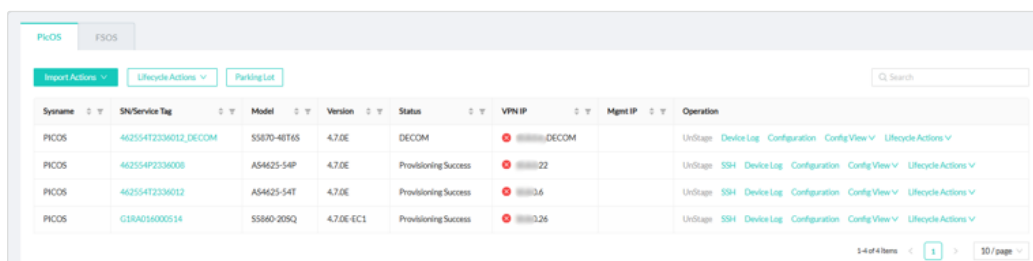
[Refreshing Switch Hostnames Automatically](#)

[Modifying Switch Hostnames Manually](#)

[Updating the Switch Mgmt IP Address](#)

Viewing the Switch List

In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar. In the **PicOS** tab, you can see the list of all managed PicOS switches.



Sysname	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation
PICOS	4625472336012_DECOM	S5870-48T6S	4.7.0E	DECOM	10.10.10.10		Unstage Device Log Configuration Config View Lifecycle Actions
PICOS	46254P2336008	AS4625-S4P	4.7.0E	Provisioning Success	10.10.10.22		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	4625472336012	AS4625-S4T	4.7.0E	Provisioning Success	10.10.10.36		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	G18A016000514	S5860-20S2	4.7.0E-EC1	Provisioning Success	10.10.10.126		Unstage SSH Device Log Configuration Config View Lifecycle Actions

Table 1. Switch Metrics

Metric	Description
Sysname	The hostname of the switch.
SN/Service Tag	The serial number or service tag of the switch.
Model	The model of the switch.
Version	The version of the switch.
Status	The state of the switch. The following states are supported: • Imported: The switch is imported to AmpCon-Campus. • Provisioning Success: The switch is deployed by using AmpCon-Campus. • Configured: After you add a switch configuration, the switch is in Configured status. • Staged: After you stage a switch, the switch is in Staged status.

	• Registered: The switch has registered with AmpCon-Campus but hasn't been deployed completely. • Provisioning Failed: The switch fails to be deployed by using AmpCon-Campus. • DECOM: The deployed switch is decommissioned (DECOM) when it's online. • DECOM-Manual: The deployed switch is decommissioned (DECOM) when it's offline. • RMA: The switch is replaced with another switch of the same switch model by using Return Merchandise Authorization (RMA).
VPN IP	The IP address of the VPN tunnel established between the switch and AmpCon-Campus. The following status icons are supported: • : The VPN tunnel between the switch and AmpCon-Campus is available. • : The VPN tunnel between the switch and AmpCon-Campus is unavailable.  NOTE Mgmt IP might be changed. To ensure uninterrupted connection between AmpCon-Campus and a switch after Mgmt 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 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.

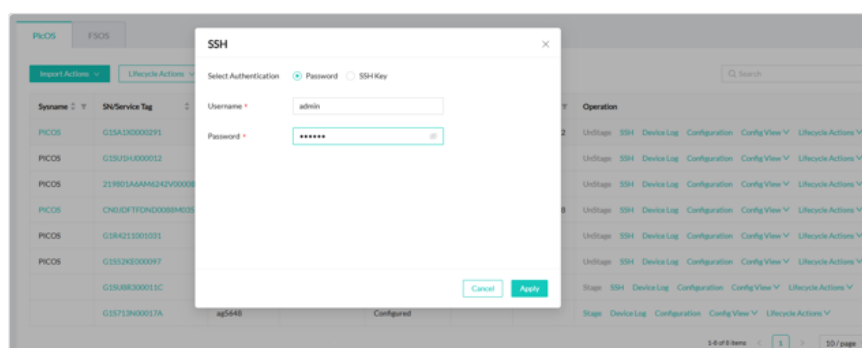
Mgmt IP	The management IP address of the switch. Mgmt IP is used to connect to AmpCon-Campus.
----------------	--

In the **Operation** column, you can manage the switch as follows:

- To connect to the switch from the AmpCon-Campus UI through an SSH session, follow these steps:
 - Click **SSH**. You can select either **Password** or **SSH Key** to access a device in the **Select Authentication** section.
 - If you select **Password**, input the following information:

Table 1. Password Parameters

Parameter s	Description
Username	The username to log in to the switch. NOTES - The value is a string with at most 32 characters. The following characters are supported: - Lowercase letters including a to z. - Uppercase letters including A to Z. - Digits including 0 to 9. - Special characters (_ - .). - Username cannot start with a special character (_ - .).
Password	The password of the user.



- If you select **SSH Key**, input the following information:

Table 2. SSH Key Parameters

Parameter	Description
User Name	The username to log in to the device. NOTES • The value is a string with at most 32 characters. The following characters are supported: ◦ Lowercase letters including a to z. ◦ Uppercase letters including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ - .). • Usernames cannot start with a special character (_ - .).
Key	The private key generated by using the ssh-keygen command. Click Upload, find the file where the private key is saved, and upload it.
Passphrase	Optional. The password used to protect the SSH keys. You can choose whether to specify a passphrase when generating the SSH keys. If you do not specify a passphrase when generating SSH keys, you must leave this field blank.

For more information about SSH keys, see [SSH Key Authentication](#).

2. Click **Apply**.

- To check the operation log of the switch, click **Device Log**.
- To change the system configuration of the switch, click **Configuration**.
- In the **Config View** section, you can manage configurations as follows:
 - To check the agent configurations, click **Agent Config**. The agent configurations are automatically uploaded to the switch during the Zero Touch Provisioning (ZTP) process.
 - To check the initial configurations of the switch, click **Init Deploy Config**. Initial configurations mean the configurations that are pushed to a switch by AmpCon-

Campus during the ZTP process.

- To check the latest backup configurations, click **Current Config**. For more information, see [Viewing Configurations](#). If the switch doesn't have backup configurations, the configurations generated when you add a switch configuration for the switch are displayed.
- To back up configurations for the switch, hover your mouse over **Config View**, and then click **Backup Config**. For more information, see [Backing Up Switch Configurations](#).
- To upload configurations of the switch, hover your mouse over **Config View**, and then click **Upload Config**. For more information, see [Uploading Configurations](#).

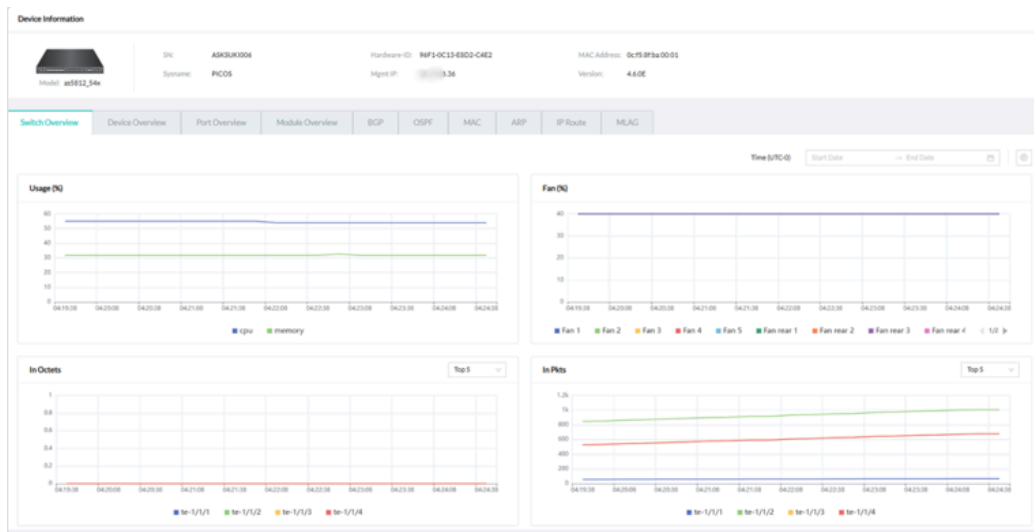
i NOTES

- For switches deployed through ZTP, when you hover your mouse over **Config View**, the **Agent Config**, **Init Deploy Config**, **Current Config**, **Backup Config**, and **Upload Config** are displayed.
- For switches imported to AmpCon-Campus (instead of provisioned with ZTP), when you hover your mouse over **Config View**, the **Backup Config** and **Upload Config** are displayed.

- To replace the switch with another switch of the same switch model, hover your mouse over **Lifecycle Actions**, and then click **RMA**. For more information, see [Returning Merchandise Authorization for Switches](#).
- To remove the switch from AmpCon-Campus, hover your mouse over **Lifecycle Actions**, and then click **Remove**. For more information, see [Removing Switches](#).
- To decommission the switch from AmpCon-Campus, hover your mouse over **Lifecycle Actions**, and then click **DECOM**. For more information, see [Decommissioning Switches](#).

Viewing Telemetry Data of a Switch

Click a specific switch SN or service tag in the switch list. You can see detailed telemetry data related to the switch. For more information, see [Telemetry Data of a Switch](#).



Viewing the Parking Lot

If you provisioned a switch without adding a switch configuration beforehand, the switch will be in **Parking** status. The switch in **Parking** status is not listed on the “Switches” page and can’t be staged.

In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar. On the “Switches” page, click **Parking Lot**, and then you can see all switches in **Parking** status.

For more information, see [Managing the Parking Lot](#).

SN	Hardware ID	IP Address	Model	Register Count	Time In	Latest Time	Flag	Operation
732650X007098	88E9-CICA-7C3B-89F3	10.1.1.55.86	N8550-4880C	5616	2025-08-18 06:29:35	2025-08-20 09:17:57	Create Config	Investigated
EC1631000063	C2BF-1282-A372-55DC	10.1.1.1198	ar4630_54w	2	2025-08-25 08:14:57	2025-08-25 08:15:31	Create Config	Investigated

Refreshing Switch Hostnames Automatically

During the switch lifecycle, switch hostnames might be changed on the switch side.

AmpCon-Campus can retrieve the latest hostnames from managed switches and then refresh the displayed hostnames in the AmpCon-Campus UI.

To refresh switch hostnames, follow these steps:

1. Log in to the AmpCon-Campus UI, and then click **Wired > Switches** from the navigation bar.
2. Click **Lifecycle Actions**, and then select **Sync Sysname**.

Sysname	SN	Model	Version	Status	VPN IP	Mgmt IP	Operation
PIC05	G15A300000191	S5860-24RG-U	9.8.7-for-S5860-EC1	Provisioning Success	10.0.1.18	10.0.1.192	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G15U14000012	S3270-24TM-P	4.4.5.26	Imported	10.0.1.26		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	219801A6A46242V00008	S6860-24CDB	4.5.3E	Provisioning Success	10.0.1.30	10.0.1.55.87	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	CND0FTF0ND0008M0259	N3048EP-ON	9.8.7-main	Provisioning Success	10.0.1.38	10.0.1.55.138	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G184211001001	S5860-24GB-U	4.7.0E-EC1	Provisioning Success	10.0.1.42	10.0.1.55.25	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G1552K0000097_DECOM	S5810-48TS-P	4.7.0E-EC1	DECOM-Manual	10.0.1.434_DECOM	10.0.1.55.47	Unstage Device Log Configuration Config View Lifecycle Actions
	G15U8R3000113C			Imported			Stage SSH Device Log Configuration Config View Lifecycle Actions
	G15712400017A	ag5648		Configured			Stage Device Log Configuration Config View Lifecycle Actions

3. Click **Yes**.

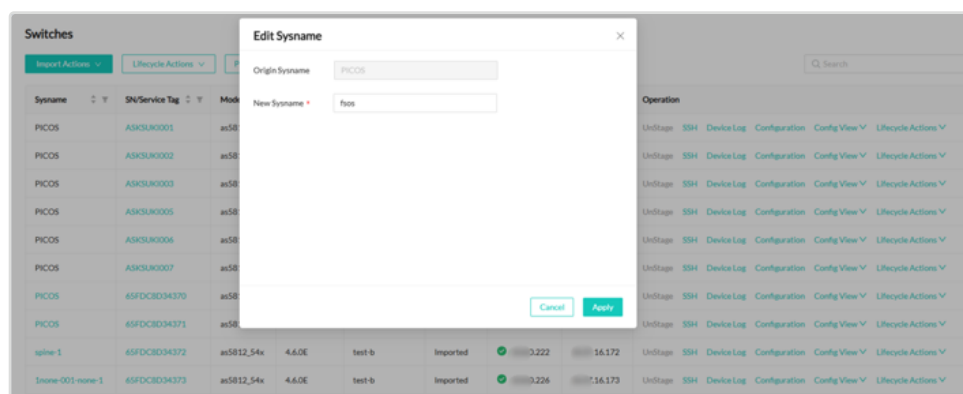
Modifying Switch Hostnames Manually

In addition to automatically retrieving and displaying the latest hostnames, you can modify switch hostnames manually. Follow the steps:

NOTES

- If you refresh switch hostnames by clicking **Sync Sysname** and then modify the switch hostname manually, the manually entered switch hostname will be displayed in the AmpCon-Campus as the switch hostname.
- If you modify the switch hostname manually and then refresh switch hostnames by clicking **Sync Sysname**, the manually entered switch hostname will be overwritten by the real hostname that AmpCon-Campus retrieves from the switch.

1. Log in to the AmpCon-Campus UI, and then click **Wired > Switches** from the navigation bar.
2. Locate the switch in the switch list, and then click the hostname of the switch.
3. In the **Edit Sysname** pop-up window, input a new hostname as needed.

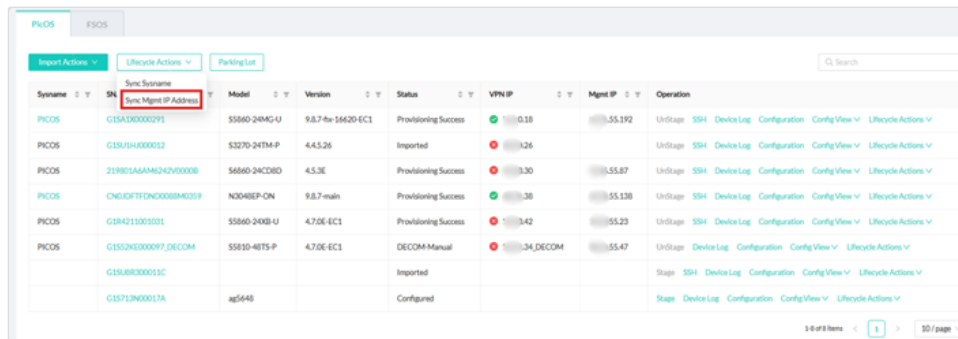


4. Click **Apply**.

Updating the Switch Mgmt IP Address

During the switch lifecycle, you might need to change their Mgmt IP addresses, which are used to connect to AmpCon-Campus. To see the latest Mgmt IP addresses, follow these steps:

1. Log in to the AmpCon-Campus UI, and then click **Wired > Switches** from the navigation bar.
2. Click **Lifecycle Actions**, and then select **Sync Mgmt IP Address**.



The screenshot shows the AmpCon-Campus UI interface. At the top, there are tabs for 'PcOS' and 'FSOS'. Below these, there are three buttons: 'Import Actions', 'Lifecycle Actions', and 'Parking Lot'. The 'Lifecycle Actions' button is highlighted with a red box, and a dropdown menu is open, showing 'Sync Mgmt IP Address' as the selected option. Below the buttons is a table with columns: SysteName, SN, Model, Version, Status, VPN IP, Mgmt IP, and Operation. The table contains several rows of switch data. At the bottom right, there is a pagination bar showing '1 of 8 items' and '1 / page'.

SysteName	SN	Model	Version	Status	VPN IP	Mgmt IP	Operation
PIC05	G15A100000191	S5660-24R4G-U	9.8.7-for-S5620-EC1	Provisioning Success	0.18	55.192	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G15U1H0000012	S3270-24T4-P	4.4.5.26	Imported	0.26		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	219901A6AM6242V00008	S6660-24CD6D	4.5.3E	Provisioning Success	0.30	55.87	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	CND0F7F1CND00008M0359	N3048EP-ON	9.8.7-main	Provisioning Success	0.38	55.138	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G15A211000001	S5660-24R4G-U	4.7.0E-EC1	Provisioning Success	0.42	55.23	Unstage SSH Device Log Configuration Config View Lifecycle Actions
PIC05	G1552K0000097_DECOM	S5810-48TS-P	4.7.0E-EC1	DECOM Manual	0.34_DECOM	55.47	Unstage Device Log Configuration Config View Lifecycle Actions
	G15U4R0000011C			Imported			Stage SSH Device Log Configuration Config View Lifecycle Actions
	G15713N000017A	ap5648		Configured			Stage Device Log Configuration Config View Lifecycle Actions

3. Click **Yes**.

Managing the Parking Lot

During the ZTP process, if you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-Campus parking lot. If you add a switch configuration before configuring the DHCP server, the switch will go to the “Switches” page.

During the RMA process, after you configure the DHCP server and reboot the switches to be deployed, these switches will go to the AmpCon-Campus parking lot. You can view and manage the parking lot.

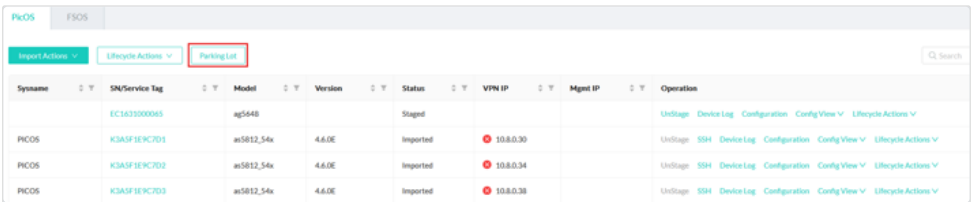
NOTE

The DHCP configuration steps for ZTP and RMA are the same. For more information, see [Configuring a DHCP Server](#).

[Procedure](#)
[What to Do Next](#)

Procedure

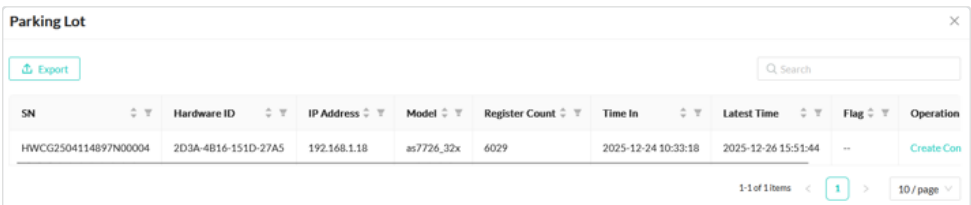
1. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar.
2. In the **PicOS** tab, click **Parking Lot**.



The screenshot shows the AmpCon-Campus UI with the PicOS tab selected. The 'Parking Lot' button is highlighted with a red box. Below the button is a table with columns: System, SN/Service Tag, Model, Version, Status, VFN IP, Mgmt IP, and Operation. The table contains three rows of data for PicOS switches.

System	SN/Service Tag	Model	Version	Status	VFN IP	Mgmt IP	Operation
PicOS	EC1A32000065	ag5648		Staged			Unstage Device Log Configuration Config View Lifecycle Actions
PicOS	K3ASF1E9C7D1	as5812_54x	4.6.0E	Imported	10.8.0.30		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PicOS	K3ASF1E9C7D2	as5812_54x	4.6.0E	Imported	10.8.0.34		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PicOS	K3ASF1E9C7D3	as5812_54x	4.6.0E	Imported	10.8.0.38		Unstage SSH Device Log Configuration Config View Lifecycle Actions

3. In the pop-up window, check the switches in the parking lot:



The screenshot shows the 'Parking Lot' pop-up window. It has an 'Export' button and a search bar. Below is a table with columns: SN, Hardware ID, IP Address, Model, Register Count, Time In, Latest Time, Flag, and Operation. The table contains one row of data for a switch.

SN	Hardware ID	IP Address	Model	Register Count	Time In	Latest Time	Flag	Operation
HWCG2504114897N00004	2D3A-4B16-151D-27A5	192.168.1.18	as7726_32x	6029	2025-12-24 10:33:18	2025-12-26 15:51:44	--	Create Con

Table 1. Switch Metrics

Metric	Description
SN	The serial number of the switch.
Hardware ID	The Hardware ID of the switch.

IP Address	The switch IP address used to connect to the AmpCon-Campus server.
Model	The model of the switch.
Register Count	The number of times the switch initiates ZTP authentication with the AmpCon-Campus server.
Time In	The time when the switch initiates the first ZTP authentication with the AmpCon-Campus server.
Latest Time	The time when the switch initiates the last ZTP authentication with the AmpCon-Campus server.
Flag	Whether the switch has been investigated.

4. In the **Operation** column, do the following operations as needed:

- To deploy a switch through normal ZTP, locate the switch, and then click **Create Config** to add a switch configuration. For more information, see [Preparing Configurations for ZTP](#).
- To confirm whether you have viewed a switch, locate the switch, and then click **Investigated**. After you click the button, the value of the **Flag** column will be "I".
- To remove a switch from the parking lot, locate the switch, and then click **Remove**.

4. To save all the switch information in the parking lot to a local file, click **Export** in the top-left corner.

What to Do Next

After a switch go to the parking lot, you can deploy the switch through ZTP. Or you can replace a failed switch with the switch through Returning Merchandise Authorization (RMA).

For more information, see the following documents:

- [Deploying PicOS Switches through ZTP](#)
- [Returning Merchandise Authorization for Switches](#)

Uploading and Upgrading PicOS Images

By using AmpCon-Campus, you can upload PicOS images, push PicOS images to a single switch or multiple switches in bulk, check release notes of each PicOS image, upgrade PicOS on a single switch or on multiple switches in bulk, set the PicOS upgrade time, and manage upgrade tasks.

You no longer need to visit the FS website to download images or view release notes. Both upgrades and release notes are available directly within the AmpCon-Campus UI, saving your time and effort.

You can schedule automatic upgrades during off-peak hours (such as at night or on holidays), so that your operations will face minimal disruption.

See the following child topics:

- [Uploading and Pushing Images](#)
- [Upgrading PicOS on Switches](#)

Uploading and Pushing Images

AmpCon-Campus provides multiple built-in PicOS images, which you can use to deploy switches.

To deploy a switch with a PicOS image that is not built in AmpCon-Campus, upload the image and its MD5 file first before you deploy the switch.

By using AmpCon-Campus, you can push PicOS images to a single switch or multiple switches in bulk and check the release notes of the PicOS image to which you want to upgrade.

[Prerequisite](#)

[Uploading Images](#)

[Pushing Images](#)

[Optional: Checking PicOS Release Notes](#)

[Optional: Uploading MD5 Files](#)

[Optional: Removing Images](#)

Prerequisite

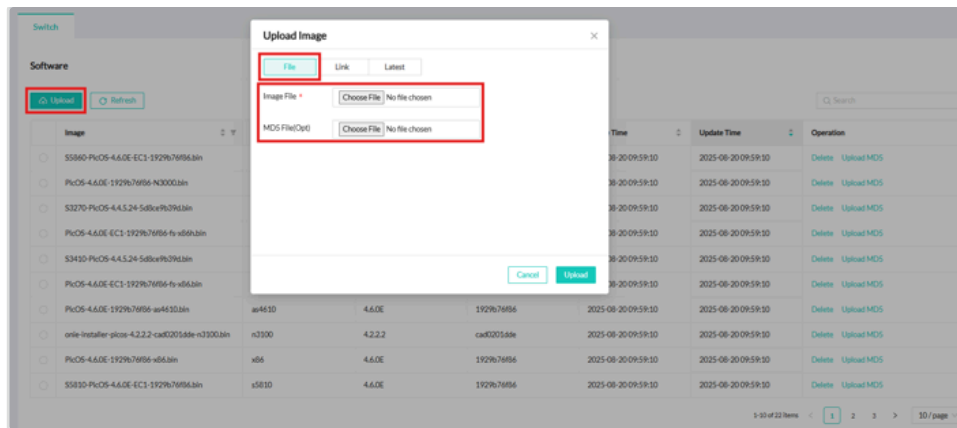
Click **Wired > Wired Profiles** in the AmpCon-Campus UI, click the **Switch Model** tab, and then check whether the PicOS image to deploy is listed in the **Deployed ONIE Image** drop-down list.

- If the image is not listed there, upload the PicOS image and its MD5 file to AmpCon-Campus as described in the [Uploading Images](#) section.
- If the image is listed there, you don't need to upload the PicOS image and its MD5 file.

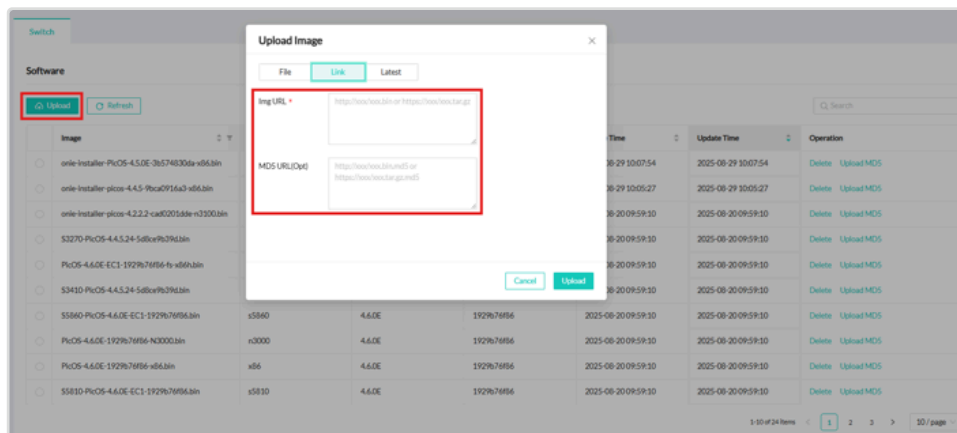
Uploading Images

To upload a PicOS image, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management**.
2. Click the **Switch** tab.
3. In the **Software** section, click **Upload**.
4. In the pop-up window, upload an image by using one of the following methods:
 - Click **File**, and select a local image file (required) and its MD5 file (optional).



- Click **Link**, and enter the image URL (required) and the MD5 file URL (optional).



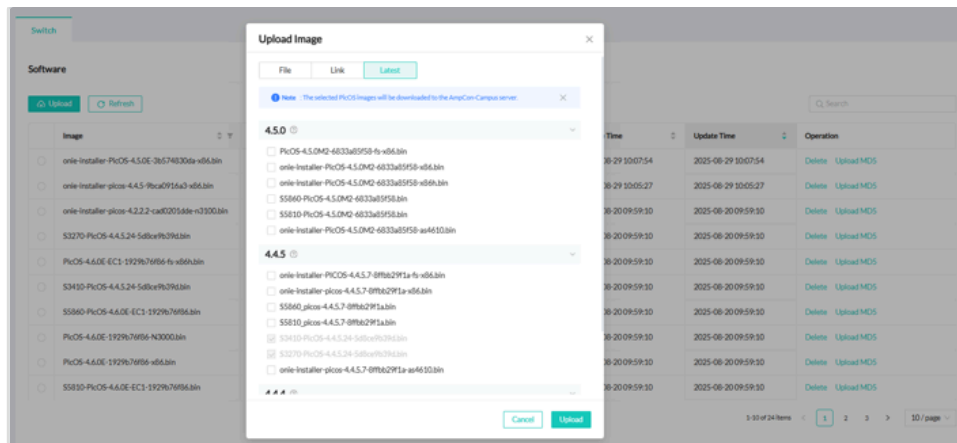
- Click **Latest**, and then you can see images classified by PicOS version. You can select one or multiple images that you want to upload.

You cannot select images that are being uploaded or have already been uploaded to AmpCon-Campus.

NOTE

Before you upload images in the **Latest** tab, ensure that the following requirements are met:

- You have completed the global system configuration, and the license portal is configured correctly. For more information, see [Adding a Global System Configuration](#).
- AmpCon-Campus can connect to the Internet.



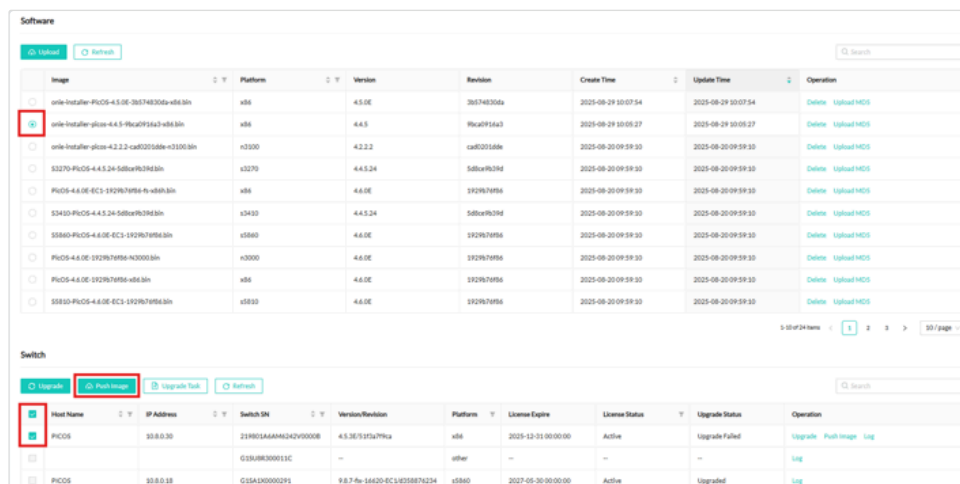
4. Click **Upload**.

Pushing Images

You can push PicOS images to one or multiple switches. The pushed images are located in the **/home/automation** directory on the switch side.

To push a PicOS image to switches, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management**.
2. Click the **Switch** tab.
3. In the **Software** section, select the PicOS image that you want to push.
4. In the **Switch** section, select one or multiple switches, and then click **Push Image**.



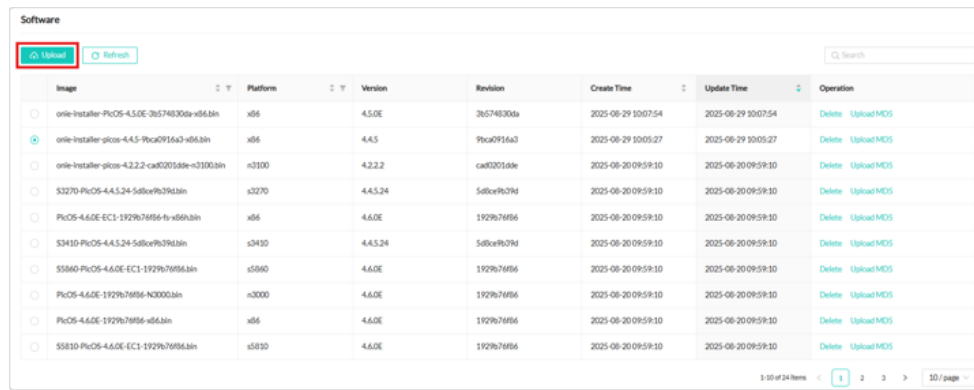
4. In the pop-up window, click **Push Image**.

Optional: Checking PicOS Release Notes

To check the release notes of the PicOS image to which you want to upgrade, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management** from the navigation bar.
2. Click the **Switch** tab.

3. In the **Software** section, click **Upload**.



3. In the **Upload Image** pop-up window, click **Latest**.

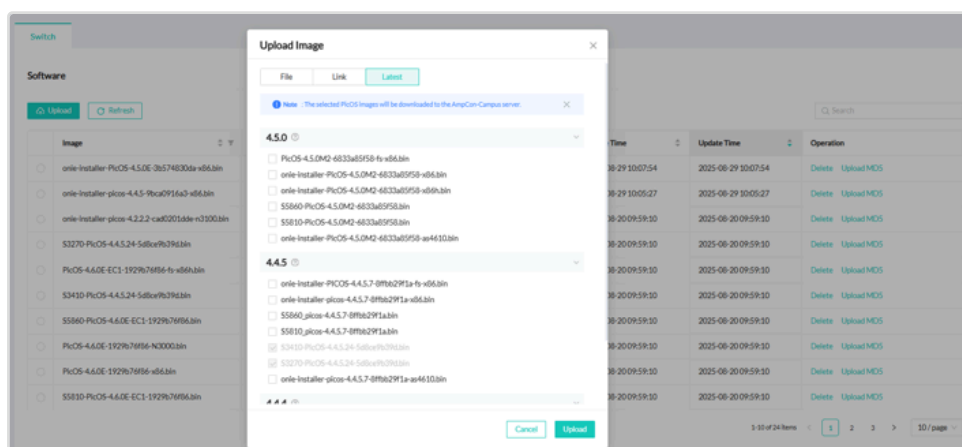
NOTE

To check release notes in the **Latest** tab, ensure that the following requirements are met:

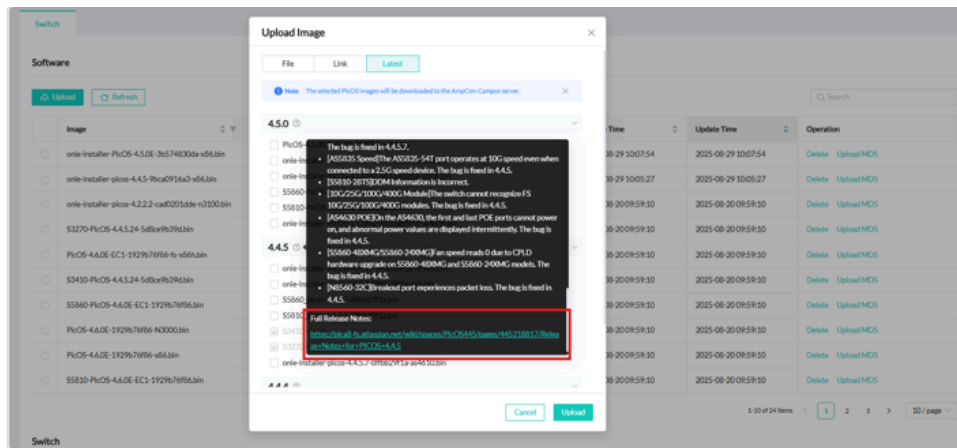
- You have completed the global system configuration, and the license portal is configured correctly. For more information, see [Adding a Global System Configuration](#).
- AmpCon-Campus can connect to the Internet.

4. Locate the PicOS image version to which you want to upgrade, and hover your mouse over the question mark icon.

Then, in the pop-up window, you can see the release notes of the PicOS image, including new features, changes, and fixed issues of the PicOS image.



5. Optional: To see the complete release notes of the PicOS image, click the hyperlink in the **Full Release Notes** section.



Optional: Uploading MD5 Files

An MD5 file is used to verify the completeness of the corresponding PicOS image. If the MD5 file is not uploaded when you upload the PicOS image, AmpCon-Campus will not verify the completeness of the PicOS image when it installs the PicOS image.

To upload an MD5 file for a PicOS image, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management**.
2. Click the **Switch** tab.
3. In the **Software** section, locate the PicOS image, and then click **Upload MD5**.

Software							
Upload Refresh		Search					
Image	Platform	Version	Revision	Create Time	Update Time	Operation	
☐ PicOS-4.6.0E-1929b7686-N3000.bin	n3000	4.6.0E	1929b7686	2025-08-26 07:32:57	2025-08-26 07:32:57	Delete	Upload MD5
☐ onie-installer-picos-4.2.2.2-ca00201d8e-n3100.bin	n3100	4.2.2.2	ca00201d8e	2025-08-26 07:32:57	2025-08-26 07:32:57	Delete	Upload MD5
☐ PicOS-4.6.0E-1929b7686-x86.bin	x86	4.6.0E	1929b7686	2025-08-26 07:32:57	2025-08-26 07:32:57	Delete	Upload MD5
☐ PicOS-4.6.0E-1929b7686-aa610.bin	aa610	4.6.0E	1929b7686	2025-08-26 07:32:57	2025-08-26 07:32:57	Delete	Upload MD5
☐ S5810 PicOS-4.6.0E-EC1-1929b7686.bin	s5810	4.6.0E	1929b7686	2025-08-26 07:32:57	2025-08-26 07:32:57	Delete	Upload MD5

3. Upload the MD5 file by using either of the following ways:

- Click **File**, and select the MD5 file.
- Click **Link**, and enter the URL of the MD5 file.

4. Click **Upload**.

Optional: Removing Images

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management**.
2. Click the **Switch** tab.
3. In the **Software** section, locate an image, and then click **Delete**.

Software

Upload

Refresh

Q Search

	Image	Platform	Version	Revision	Create Time	Update Time	Operation
☐	onie-installer-PicOS-4.5.0E-3b574830da-v86.bin	x86	4.5.0E	3b574830da	2025-06-29 10:07:54	2025-06-29 10:07:54	DeleteUpload MDS
☒	onie-installer-picoo-4.4.5-P9ca0916a3-v86.bin	x86	4.4.5	99ca0916a3	2025-06-29 10:05:27	2025-06-29 10:05:27	DeleteUpload MDS
☐	onie-installer-picoo-4.2.2.2-ca802016de-v3100.bin	n3100	4.2.2.2	ca802016de	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	S3270-PicOS-4.4.5.24-5d8ce9b396a1n	s3270	4.4.5.24	5d8ce9b396	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	PicOS-4.6.0E-EC1-1929b76f86-fv-x86h.bin	x86	4.6.0E	1929b76f86	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	S3410-PicOS-4.4.5.24-5d8ce9b396a1n	s3410	4.4.5.24	5d8ce9b396	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	S5860-PicOS-4.6.0E-EC1-1929b76f86a1n	s5860	4.6.0E	1929b76f86	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	PicOS-4.6.0E-1929b76f86-N3000.bin	n3000	4.6.0E	1929b76f86	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	PicOS-4.6.0E-1929b76f86-v86.bin	x86	4.6.0E	1929b76f86	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS
☐	S5810-PicOS-4.6.0E-EC1-1929b76f86a1n	s5810	4.6.0E	1929b76f86	2025-06-20 09:59:10	2025-06-20 09:59:10	DeleteUpload MDS

1-10 of 24 items

123>

10 / page

3. Click **Yes**.

Upgrading PicOS on Switches

By using AmpCon-Campus, you can upgrade PicOS on a single switch or on multiple switches in bulk, set the PicOS upgrade time, and manage upgrade tasks.

Upgrade Procedure

Optional: Managing Upgrade Tasks

Checking Upgrade Tasks

Executing an Upgrade Task Immediately

Canceling Upgrade Tasks

Editing Upgrade Tasks

Checking Logs for a Failed Upgrade Task

Deleting an Upgrade Task

Deleting Multiple Upgrade Tasks

Upgrade Procedure

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management**.
2. Click the **Switch** tab.
3. In the **Software** section, select the PicOS image to which you want to upgrade.
4. In the **Switch** section, select one or multiple switches whose platforms are compatible with the image you select, and then click **Upgrade**.

Software										
<button>+ Install</button> <button>+ Refresh</button>										
	Image	Platform	Version	Revision	Create Time	Update Time	Operation			
☒	win-installer-PiCOS-4.3.0E-38574830da-v86.bin	x86	4.3.0E	38574830da	2025-08-29 10:07:54	2025-08-29 10:07:54	Delete	Upload	Md5	
☒	win-installer-picos-4.4.5-R9ca9f2ba2-v86.bin	x86	4.4.5	R9ca9f2ba2	2025-08-29 10:05:27	2025-08-29 10:05:27	Delete	Upload	Md5	
☒	win-installer-picos-4.2.2.2-ca820558de-x3000.bin	n3000	4.2.2.2	ca820558de	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	S3270-PiCOS-4.4.5.24-f8bce9f596e.bin	i3270	4.4.5.24	f8bce9f596	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	PiCOS-4.4.0E-EC3-1927678f56-nv-v86h.bin	x86	4.4.0E	1927678f56	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	S3430-PiCOS-4.4.5.24-f8bce9f596e.bin	s3430	4.4.5.24	f8bce9f596	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	S5860-PiCOS-4.4.0E-EC3-1927678f56e.bin	s5860	4.4.0E	1927678f56	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	PiCOS-4.4.0E-1927678f56-N3000e.bin	n3000	4.4.0E	1927678f56	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	PiCOS-4.4.0E-1927678f56-v86h.bin	x86	4.4.0E	1927678f56	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	
☐	S5830-PiCOS-4.4.0E-EC3-1927678f56e.bin	s5830	4.4.0E	1927678f56	2025-08-20 09:59:30	2025-08-20 09:59:30	Delete	Upload	Md5	

1/37 of 234 items 1 2 3 > 37 / page

- Optional: In the **Upgrade** pop-up window, click or drag upgrade scripts to the **Scripts** section. The upgrade scripts will run automatically after the upgrade task is completed.

NOTES

- You can upload one or multiple scripts, but one of the uploaded scripts must be named `post-xorplus`.
- For the content of the script named `post-xorplus`, it must follow the syntax rules of the script language you use. See the following example:


```
#!/bin/bash
```

```
sudo echo "123\n" >> /home/automation/test_cc.txt  
sudo echo "456" >> /home/automation/test_cc.txt  
sync
```

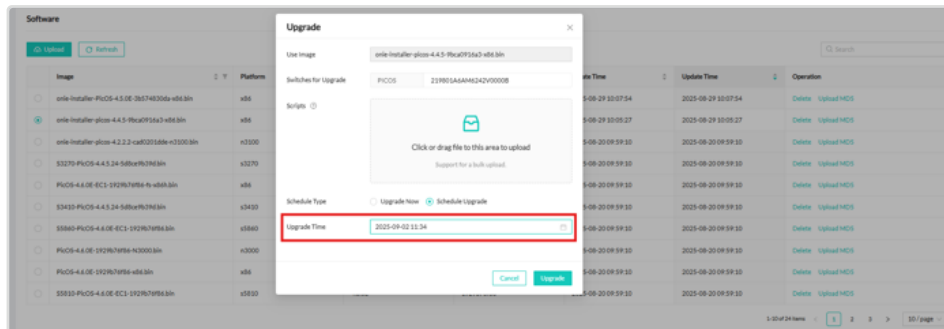
5. In the **Schedule Type** section, select whether you want to upgrade immediately or upgrade at a specified time.

- **Upgrade Now:** Upgrades PicOS immediately.
- **Schedule Upgrade:** Upgrades PicOS at a specified time.

If you select this schedule type, select the upgrade time in the **Upgrade Time** section.

NOTE

You cannot select a time point earlier than the current system moment. The system time is set to the UTC+0 time zone.



6. Click **Upgrade**.

Optional: Managing Upgrade Tasks

Checking Upgrade Tasks

To check all the upgrade tasks, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Upgrade Management** from the navigation bar.
2. Click the **Switch** tab.
3. In the **Switch** section, click **Upgrade Task**. Then, you can see detailed information about all the upgrade tasks.

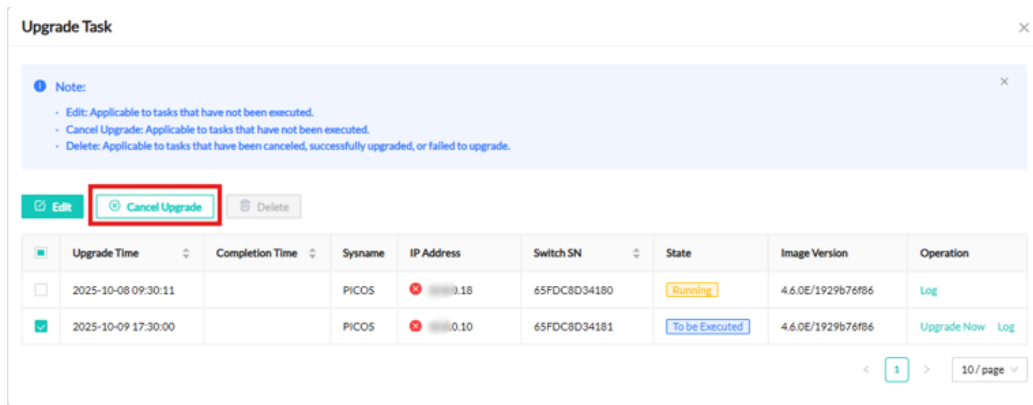
NOTES

- Each switch can have only one upgrade task in the **To be Executed** state.
- For a switch that has an upgrade task in the **To be Executed** state, 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.

Upgrade Time	Completion Time	Sysname	IP Address	Switch SN	State	Image Version	Operation
2025-09-13 02:09:28		PC05	10.10.10.10	219801A0A0H242V00008	Failed	4.5.1.5/73b478386d	Log
2025-09-13 10:11:21	2025-09-13 10:13:33	PC05	10.10.10.10	219801A0A0H242V00008	Failed	4.5.1.5/73b478386d	Delete Log
2025-09-13 09:32:53	2025-09-13 09:33:05	PC05	10.10.10.10	01842110010031	Failed	4.6.0E/1929679958	Delete Log
2025-09-13 04:57:51	2025-09-13 07:00:02	PC05	10.10.10.10	219801A0A0H242V00008	Failed	4.5.1.5/73b478386d	Delete Log
2025-09-14 01:54:34	2025-09-14 02:00:44	PC05	10.10.10.10	219801A0A0H242V00008	Failed	4.7.0E/94942d7f9	Delete Log
2025-09-13 14:29:00	2025-09-13 14:31:30	PC05	10.10.10.10	01842110010031	Failed	4.6.1E/4e4e52b2c	Delete Log
2025-09-13 10:28:45	2025-09-13 10:39:40	PC05	10.10.10.10	219801A0A0H242V00008	Failed	4.5.1.5/73b478386d	Delete Log
2025-09-13 07:57:20	2025-09-13 07:59:30	PC05	10.10.10.10	01842110010031	Failed	4.6.1E/4e4e52b2c	Delete Log
2025-09-13 07:28:54	2025-09-13 07:33:04	PC05	10.10.10.10	01842110010031	Failed	4.6.1E/4e4e52b2c	Delete Log
2025-09-13 04:24:00	2025-09-13 04:24:07	PC05	10.10.10.10	CNDJ0FTYF0C0008M0359	Failed	4.6.0E/1929679958	Delete Log

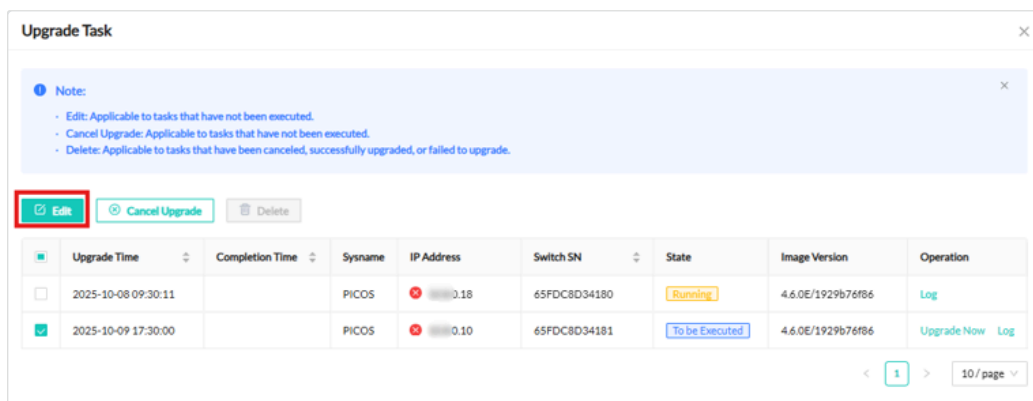
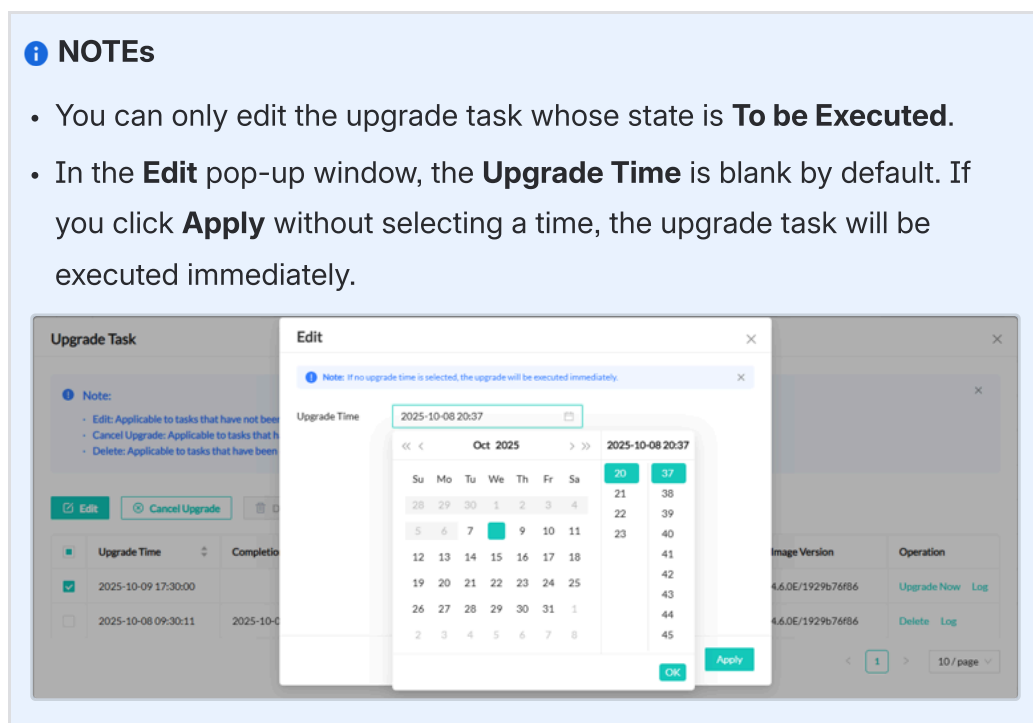
Table 1. Upgrade Task Metrics

Metrics	Description
Upgrade time	The upgrade time of the upgrade task, which is set to the UTC-0 time zone.
Completion Time	The completion time of the upgrade task, which is set to the UTC-0 time zone. For the upgrade tasks waiting to be executed, the completion time is blank. For the canceled upgrade tasks, the completion time is the time when the task is canceled
Sysname	The hostname of the switch in the upgrade task.
IP address	The IP address of the switch in the upgrade task.
Switch SN	The serial number of the switch in the upgrade task.



Editing Upgrade Tasks

In the **Upgrade Task** pop-up window, select upgrade tasks, and then click **Edit** in the top. If you select multiple upgrade tasks, their scheduled times will all be modified to the time you set.



Checking Logs for a Failed Upgrade Task

To check reasons for a failed upgrade task, use one of the following methods:

- In the **Switch** section, locate the switch whose upgrade task failed, and then click **Log** to see more details for troubleshooting.

Host Name	IP Address	Switch SN	Version/Revision	Platform	License Engine	License Status	Upgrade Status	Operation
PC05	18	G15AD0000295	9.8.7-Rev-16420-EC14255876234	s5840	2027-05-20 00:00:00	Active	Upgraded	Log
PC05	24	G15U1H000012	4.4.3.26/264462949	s5270	--	--	Upgrade Failed	Log
PC05	30	219901A6AH424V00008	4.5.15/73647936d	s56	2025-12-31 00:00:00	Active	Upgrade Failed	Log
PC05	38	CN0J0FTFDND008M0359	9.8.7-mali/9442a076	s3000	2027-05-20 00:00:00	Active	Upgraded	Log
PC05	42	G18421100101	4.7.0E-EC14255876234	s5840	2020-02-26 00:00:00	Active	Upgrade Failed	Log
		G15U1H000012	--	other	--	--	--	Log

- In the **Upgrade Task** pop-up window, locate the failed upgrade task, and then click **Log** to see more details for troubleshooting.

Upgrade Time	Completion Time	Synonym	IP Address	Switch SN	State	Image Version	Operation
2025-09-15 02:08:28		PC05	30	219901A6AH424V00008	Running	4.5.15/73647936d	Log
2025-09-18 10 11 21	2025-09-18 10 13 33	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-18 09 32 53	2025-09-18 09 33 05	PC05	42	G18421100101	Failed	4.6.0E/192967956	Delete Log
2025-09-18 06 57 51	2025-09-18 07 00 02	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-18 01 54 34	2025-09-18 02 05 44	PC05	30	219901A6AH424V00008	Failed	4.7.0E/9442a076	Delete Log
2025-09-15 16 29 00	2025-09-15 16 31 30	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 10 28 45	2025-09-15 10 29 40	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-15 07 57 20	2025-09-15 07 59 30	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 07 28 54	2025-09-15 07 31 04	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 04 24 00	2025-09-15 04 24 07	PC05	38	CN0J0FTFDND008M0359	Failed	4.6.0E/192967956	Delete Log

Deleting an Upgrade Task

In the **Upgrade Task** pop-up window, locate an upgrade task, and then click **Delete** on the right.

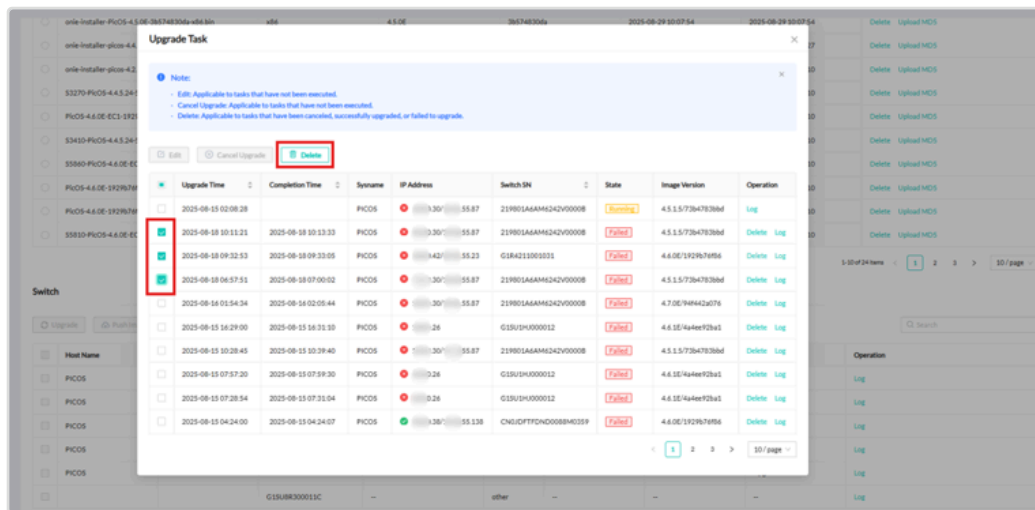
NOTE

You can delete only the upgrade task whose state is **Success**, **Failed**, or **Cancel Upgrade**.

Upgrade Time	Completion Time	Synonym	IP Address	Switch SN	State	Image Version	Operation
2025-09-15 02:08:28		PC05	30	219901A6AH424V00008	Running	4.5.15/73647936d	Log
2025-09-18 10 11 21	2025-09-18 10 13 33	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-18 09 32 53	2025-09-18 09 33 05	PC05	42	G18421100101	Failed	4.6.0E/192967956	Delete Log
2025-09-18 06 57 51	2025-09-18 07 00 02	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-18 01 54 34	2025-09-18 02 05 44	PC05	30	219901A6AH424V00008	Failed	4.7.0E/9442a076	Delete Log
2025-09-15 16 29 00	2025-09-15 16 31 30	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 10 28 45	2025-09-15 10 29 40	PC05	30	219901A6AH424V00008	Failed	4.5.15/73647936d	Delete Log
2025-09-15 07 57 20	2025-09-15 07 59 30	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 07 28 54	2025-09-15 07 31 04	PC05	24	G15U1H000012	Failed	4.6.1E/4a4ef23a5	Delete Log
2025-09-15 04 24 00	2025-09-15 04 24 07	PC05	38	CN0J0FTFDND008M0359	Failed	4.6.0E/192967956	Delete Log

Deleting Multiple Upgrade Tasks

In the **Upgrade Task** pop-up window, select these upgrade tasks, and then click **Delete** in the top.



Returning Merchandise Authorization for Switches

AmpCon-Campus supports Returning Merchandise Authorization (RMA), which means replacing 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 install or upgrade PicOS on the new switch and push configurations to the new switch through AmpCon-Campus. In this way, you can seamlessly manage the new switch with AmpCon-Campus.

[RMA Workflow](#)
[Configuration Rules](#)
[Before You Begin](#)
[RMA Procedure](#)
[What to Do Next](#)

RMA Workflow

- **For white-box switches**

During the RMA process, AmpCon-Campus deploys PicOS on the new switch based on the **Deployed ONIE Image** setting in the switch model configuration. For more information, see [Configuring Switch Models](#).

Then, AmpCon-Campus configures the new switch based on the backup configuration file or uploaded configurations of the old switch (the switch to be replaced). For more information about backup and uploaded configuration files, see [Backing Up and Restoring Configurations](#).

NOTES

To ensure that the PicOS versions on the new switch and the old switch are the same, use one of the following ways:

- Before the RMA process, ensure that the **Deployed ONIE Image** of the related switch model is the same as the PicOS version on the old switch.
- After the RMA process, if the PicOS version on the old switch is higher than the PicOS version on the new switch, upgrade the new switch. For more information, see [Uploading and Upgrading PicOS Images](#).

- **For integrated hardware and software PicOS switches**

During the RMA process, AmpCon-Campus configures the new switch based on the backup configuration file or uploaded configurations of the switch to be replaced.

Configuration Rules

During the RMA process, AmpCon-Campus configures a new switch based on the following configuration rules:

1. If the switch to be replaced doesn't have backup configuration files marked with the **GOLDEN_CONFIG** tag, the backup configuration file marked with the **GOLDEN_CONFIG** tag is used to configure the new switch.
2. If the switch to be replaced doesn't have backup configuration files marked with the **GOLDEN_CONFIG** tag but has other backup configuration files, the latest backup configuration file is used to configure the new switch.
3. If the switch to be replaced doesn't have backup configuration files but has uploaded configurations, the uploaded configurations are used to configure the new switch.
4. If the switch to be replaced doesn't have backup configuration files and uploaded configurations, the RMA process will fail. In this case, back up or upload configurations first, and then start the RMA process again.

Before You Begin

Before you start the RMA process, ensure that the following prerequisites are met. Or else, the RMA process will fail.

1. In the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server, add the configurations for the new switch. Then, reboot the new switch. For more information, see **Step 2** and **Step 3** of [Configuring a DHCP Server](#).

The new switch will go to the AmpCon-Campus parking lot after the DHCP server is configured and the new switch is rebooted.

2. Check whether the hardware ID of the new switch is included in any imported AmpCon-Campus licenses. For more information, see [Viewing AmpCon-Campus Licenses](#).

If the hardware ID of the new switch is not included in any imported AmpCon-Campus licenses, you must import an AmpCon-Campus license to AmpCon-Campus. For more information, see [Importing Licenses for Deployed Switches](#).

3. Ensure that the switch to be replaced is in **Provisioning Success** or **Imported** status and has backup configuration files or uploaded configurations. For more information about switch status, see [Viewing the Switch List](#).
4. Ensure that the new switch is up and has the same switch model as the switch to be replaced.

RMA Procedure

1. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar. On the "Switches" page, you can see a list of managed switches.

2. Locate the switch to be replaced, and then click **Lifecycle Actions > RMA**.
3. In the **Switch RMA** pop-up window, input the following information:

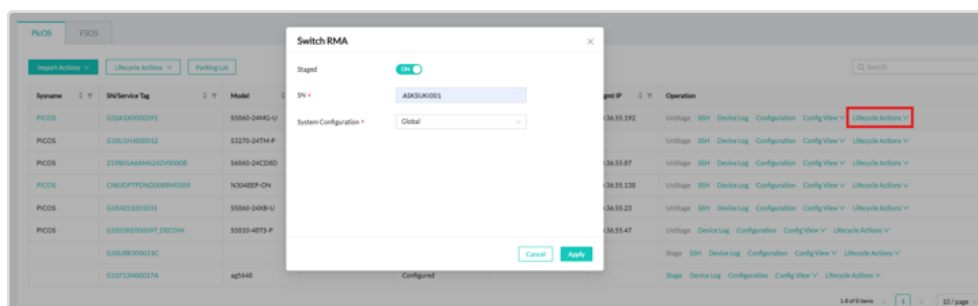


Table 1. RMA Parameters

Parameter	Description
Staged	Toggle it on to stage the new switch. NOTE The new switch can be deployed successfully only when you stage it.
SN	The serial number (SN) of the new switch.
System Configuration	The system configuration applicable to the new switch. NOTE Pay attention to the following points. Or else, the RMA process will fail. • Ensure that the Device Default Login User and Device Default Password on the “System Configuration” page are correct and can be used to log in to the new switch. • Ensure to check whether AmpCon-Campus can connect with the License Portal through the entered License Portal URL, License Portal User, and License Portal Password. For more information, see Checking License Portal Connectivity. • Ensure that the uploaded Security Config File and Parking Security Config File don’t contain wrong configurations.

4. Click **Apply**.

After the RMA process is completed successfully, the new switch will replace the old switch on related AmpCon-Campus pages.

What to Do Next

After the RMA process, do the following operations:

- **Complete physical connections for the new switch**

If the old switch was used for MLAG or IP Clos fabric deployment, the new switch will replace the old switch in the physical network. The underlay configurations will be automatically pushed to the new switch after RMA, and thus you don't need to re-deploy the physical network in the AmpCon-Campus UI.

However, you must complete physical connections for the new switch based on the topology and link information on the fabric page. For more information, see [Designing MLAG Fabrics](#) and [Designing IP Clos Fabrics](#).

i NOTE

If you don't complete physical connections for the new switch based on the topology and link information on the fabric page, the physical network and related logical networks will not work.

- **Check RMA results**

Click **Wired > Switches** from the navigation bar. On the "Switches" page, check whether the old switch is in **RMA** status and whether the new switch is in **Provisioning Success** status.

i NOTEs

- If the new switch fails to be deployed, the status will be displayed as **Provisioning Failed**. In this case, check the [Before You Begin](#) section to ensure that you have completed all the prerequisites. In addition, check the selected system configuration to ensure that the system configuration is correct. AmpCon-Campus will retry deploying the new switch automatically.
- If the new switch is not staged and the switch is in **Configured** status on the "Fabrics" page, click **Stage** on the "Switches" page to stage the new switch. Then, the new switch will be deployed.

Decommissioning Switches

You can decommission (DECOM) a deployed PicOS switch to revoke the PicOS license and configurations from the switch. The decommissioned switch will not be managed by AmpCon-Campus.

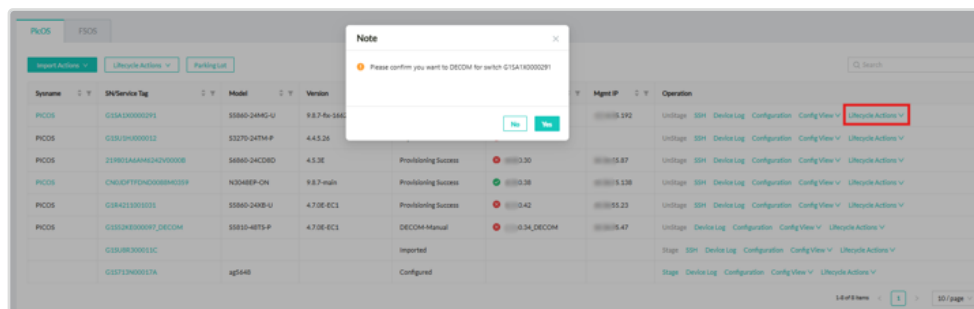
NOTES

- The imported switches can't be decommissioned. But after an imported switch is upgraded, the switch can be decommissioned.
- The switches in RMA status can't be decommissioned.
- The decommissioned switches are still displayed in the switch list. To remove the switches from the list, see [Removing Switches](#).

Procedure

To DECOM a switch, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar.
2. In the **PicOS** tab, locate the switch, click **Lifecycle Actions**, and then select **DECOM**.
3. Click **Yes** to confirm the deletion.



4. In the **PicOS** tab, check whether the decommissioned switch is in **DECOM** or **DECOM-Manual** status.

- **DECOM:** The deployed switch is decommissioned (DECOM) when it's online.
- **DECOM-Manual:** The deployed switch is decommissioned (DECOM) when it's offline. In this case, the configurations pushed by AmpCon-Campus are not cleared successfully.

Removing Switches

You can remove a deployed or imported switch from AmpCon-Campus. The switch will be removed from the AmpCon-Campus database and thus not be displayed in the AmpCon-Campus UI.

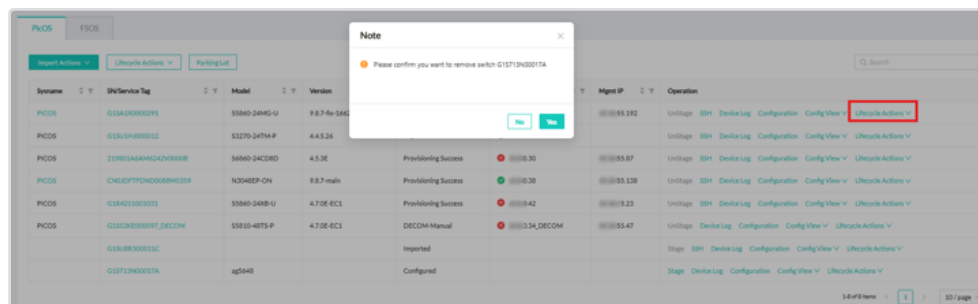
NOTES

- Removing a switch doesn't revoke the PicOS license and configurations from the switch.
- The switches in **Provisioning Success** status can't be removed. To remove a switch in **Provisioning Success** status, RMA or decommission (DECOM) the switch first to change the switch status, and then remove the switch.

Procedure

To remove a switch, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Switches** from the navigation bar.
2. In the **PicOS** tab, locate the switch, click **Lifecycle Actions**, and select **Remove**.
3. Click **Yes** to confirm the deletion.



4. In the **PicOS** tab, check whether the switch is removed from the switch list.

Configuring Switches

After you onboard PicOS switches, you can use switch templates or configuration templates to configure these switches, minimizing errors and simplifying configuration processes.

See the following child topics:

- [Switch Templates](#)
- [Configuration Templates](#)

NOTE

These child topics are applicable to only PicOS switches.

Switch Templates

After onboarding PicOS switches, you can use switch templates to satisfy general switch configurations through a full graphical interface.

You can provide parameter values for each input field in a switch template and select the switches to be configured. The configurations mapping these parameters will be pushed to the selected PicOS switches automatically by AmpCon-Campus.

Switch templates make it easy to apply the same configurations to switches across one or multiple sites, making the configuration process more efficient and streamlined.

See the following child topics:

- [Adding Switch Templates](#)
- [Managing Switch Templates](#)

Adding Switch Templates

You can configure switches by adding a switch template and applying it to switches in one or multiple sites.

NOTE

Currently, the S3000 series switches (S3410 and S3270) are not supported by this feature.

[Prerequisites](#)

[Guidelines](#)

[Procedure](#)

[1. Specifying the Template Application Scope](#)

[2. Adding Switch-Related Configurations](#)

[3. Adding Management-Related Configurations](#)

[Verifying Template Application Results](#)

Prerequisites

Ensure that the prerequisite tasks described in [Prerequisites](#) have been completed.

Guidelines

Read the following guidelines before you add a switch template:

- All the following configurations in the [Adding Switch-Related Configurations](#) and [Adding Management-Related Configurations](#) sections are optional.

Add only the configurations that you need to the switch template. AmpCon-Campus will apply only the added configurations to associated switches.

- Applying a switch template will not impact existing switch configurations done through other methods other than AmpCon-Campus switch templates.

For example, static routes on associated switches are enabled through **switch CLI**. After some time, you apply a switch template to disable static routes. Then, static routes on associated switches are still enabled.

- If you apply multiple switch templates to a switch, the newly applied template will overwrite the template previously applied to the selected switches.

For example, you apply a switch template to disable static routes. After some time, you apply another switch template to enable static routes. Then, static routes on associated switches are enabled by AmpCon-Campus.

- If configurations in a switch template have conflict with existing configurations on a switch, the switch template will fail to be applied to the switch.

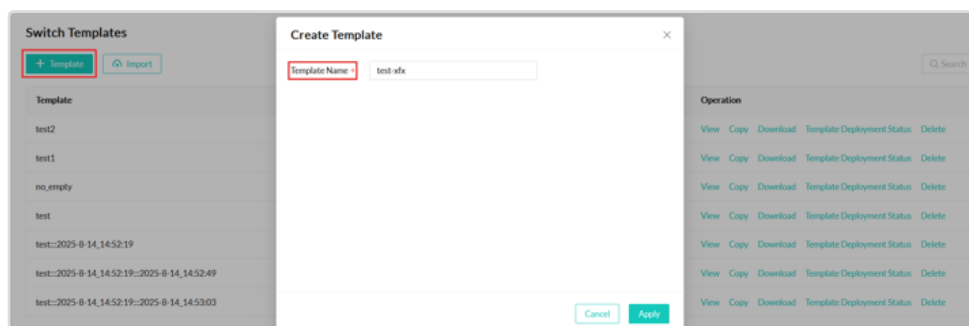
In this case, check error messages and logs in the AmpCon-Campus UI, resolve the conflicts on the switch, and then reapply the switch template to the switch.

- Switch template configurations can be applied to only switches that are connected to the AmpCon-Campus server.

Procedure

To apply a switch template to switches, follow these steps:

1. Click **Network Design > Switch Templates** from the navigation bar.
2. Click **+ Template**.
3. In the pop-up window, enter the switch template name, and then click **Apply**. The template name needs to be unique.

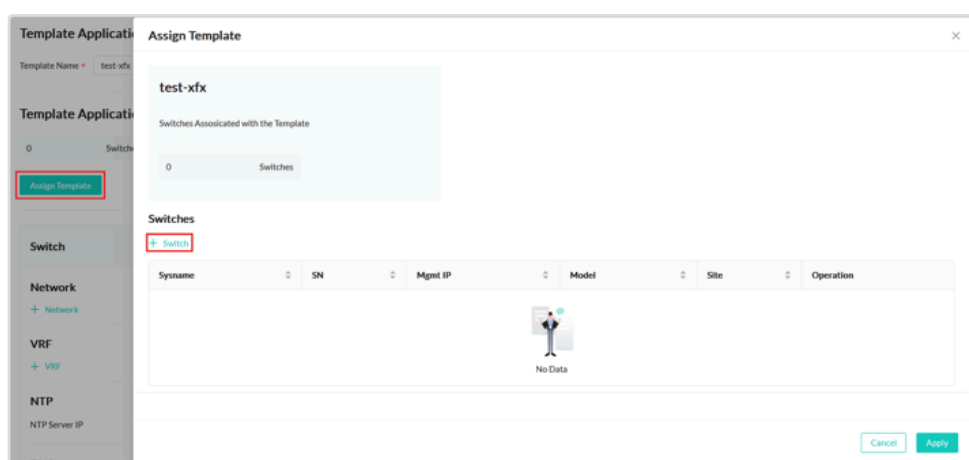


Then, the switch template configuration page appears, where you need to configure the template as follows:

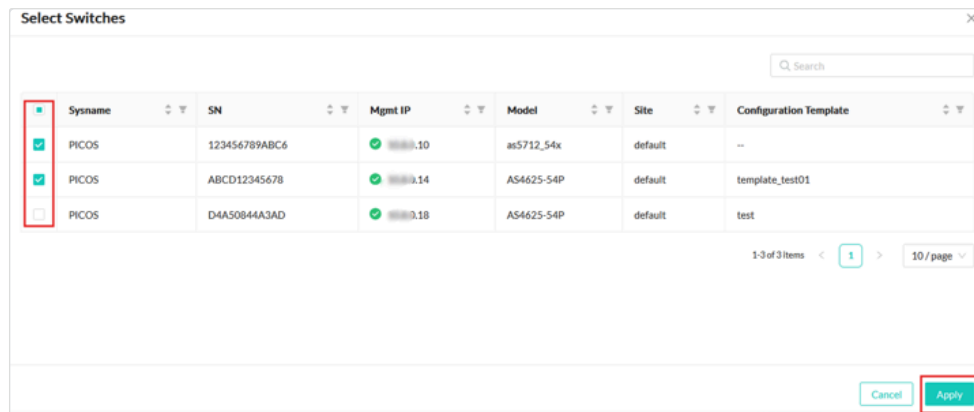
1. Specifying the Template Application Scope

Specify one or multiple switches to which this switch template will be applied. Follow these steps:

1. In the **Template Application Scope** section, click **Assign Template**.
2. In the **Assign Template** pop-up window, locate the **Switches** section, and then click **+ Switch**.

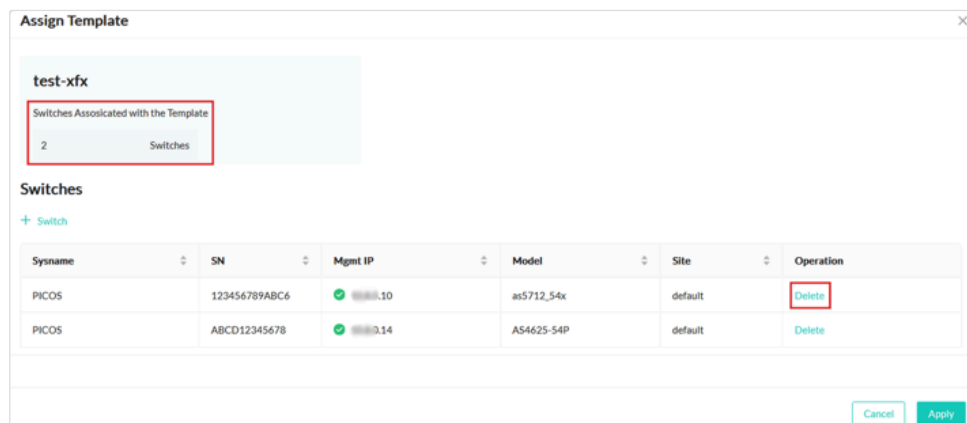


3. In the **Select Switches** pop-up window, select one or multiple switches to apply this switch template, and then click **Apply**.



4. Check the associated switches that you selected in the switch list.

To remove a switch from the associated switch list, locate the switch, and then click **Delete**.

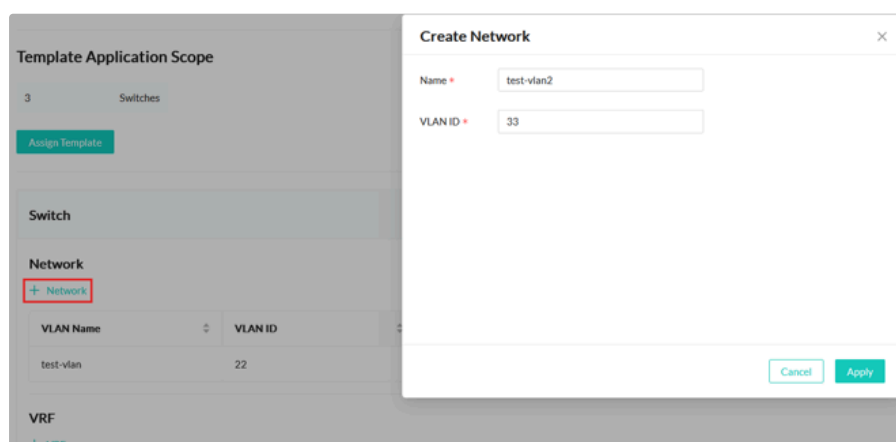


5. Click **Apply**.

2. Adding Switch-Related Configurations

In the **Switch** section, add switch-related configurations:

1. Add networks to the template. A network is a named VLAN ID.
 - a. In the **Network** section, click **+ Network**.



b. In the pop-up window, specify the name and VLAN ID of the network, and then click **Apply**.

Table 1. Network Parameters

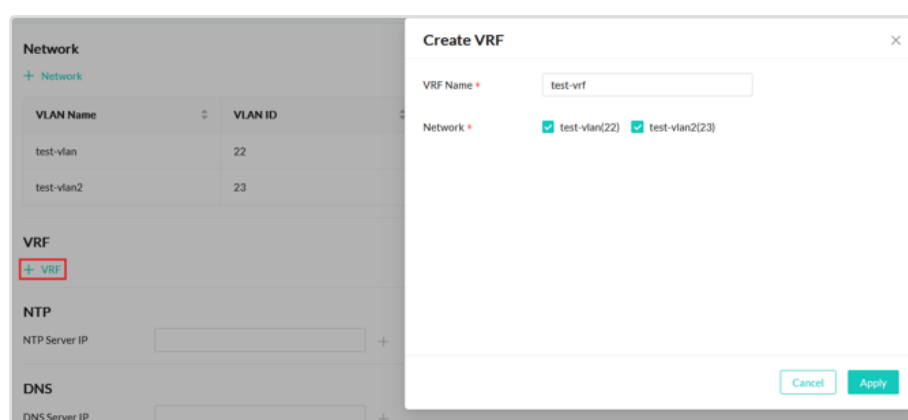
Parameter	Description
Name	The name of the Layer 3 VLAN interface. NOTES • The name needs to be unique and needs to be a string of 1 to 11 case-sensitive characters. • The value can contain only letters, numbers, and supported special characters (- . _ @ = #). • The name can't be duplicate with the VRF Name value in the VRF section.
VLAN ID	The VLAN identifier. The VLAN ID needs to be unique. Valid values range from 2 to 4094.

c. Optional: To add multiple networks, click **+ Network**.

2. Add VRF configurations to this template. By using VRF, you can divide a switch into multiple virtual routing instances, effectively isolating the traffic within the network.

You are recommended to use VRFs in network segments where traffic isolation and overlapping IP address spaces are required.

a. In the **VRF** section, click **+ VRF**.



b. In the pop-up window, specify the VRF name, select one or multiple networks associated with the VRF, and then click **Apply**.

Table 2. VRF Parameters

Parameter	Description
VRF Name	The name of the VRF that you want to create.  NOTES • The VRF name can't be the same with the Name value in the Network section. • A switch supports a maximum of 128 VRFs. • The VRF name is a string of 1 to 15 case-sensitive characters. • The VRF name can contain only letters, numbers, and supported special characters (- . _ @ = #). Spaces are not supported. • The keywords tun0, lo, mgmt-vrf, default, eth0, eth1, gretap0, bridge0, erspan0, bridge, sit0, pimreg, and ipmr-lo cannot be configured as VRF names. • The keywords starting with te, ge, eth, ae, and xe followed by numbers cannot be configured as VRF names. For example, test is a valid VRF name, but te01 is not a valid VRF name. • The keywords starting with vlan followed by any characters cannot be configured as VRF names. For example, vlan0 or vlan.0 is not a valid VRF name.
Network	The Layer 3 interface name that you just created. You can select one or multiple Layer 3 interface names. By binding Layer 3 VLAN interfaces to different VRFs, the system segregates the IP routing table, ARP table, hardware forwarding table, and host hardware forwarding table of different VRFs in edge devices.

NOTES

- Only networks that you added in **Step 1** are listed here.
- The Layer 3 VLAN interface is in the default VRF if not explicitly bound to any VRF.

c. Optional: To add multiple VRFs, click **+ VRF**.

3. Add Network Time Protocol (NTP) configurations to this template. NTP is used to synchronize the clocks of the switch and other hardware devices on the Internet.

a. In the **NTP Server IP** field of the **NTP** section, enter the IPv4 address of the NTP server.

NOTES

- The route between the NTP server and the NTP source interfaces needs to be reachable.
- The **NTP Server IP** value needs to be unique.

VRF
[+ VRF](#)

VRF Name	Networks	Operation
test-vrf	test-vlan(22) test-vlan2(23)	Edit Delete

NTP

NTP Server IP

192.168.1.2

+

192.168.1.3

-

DNS

DNS Server IP

+

Static Route

Configuration ☐ Enable ☒ Disable

OSPF

Configuration ☐ Enable ☒ Disable

b. Optional: To add multiple NTP servers, click **+**. To remove a NTP server, click **-**.

4. Add Domain Name System (DNS) configurations to this template for dynamic domain name resolution.

a. In the **DNS Server IP** field of the **DNS** section, enter the IPv4 address of the DNS server.

NOTE

The **DNS Server IP** value needs to be unique.

NTP

NTP Server IP +
 -

DNS

DNS Server IP +
 -

Static Route

Configuration ☐ Enable ☒ Disable

OSPF

Configuration ☐ Enable ☒ Disable

b. Optional: To add multiple DNS servers, click **+**. To remove a DNS server, click **-**.

5. Add static route configurations to this template.

NOTE

A switch can use static routes in the following cases:

- It doesn't have a route with a better (lower) preference value.
- It can't determine the route to a destination.
- It needs to forward packets that can't be routed.

a. In the **Static Route** section, click **Enable** or **Disable** to enable or disable static routes.

b. If you click **Enable**, click **+ Static Route** to add a static route.

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

NOTES

- The destination needs to be unique and in IPv4 format.
- For the same destination, next hop values can't be duplicate.
- For different destinations, next hop values can be duplicate.

Static Route

Configuration ☒ Enable ☐ Disable

+ Static Route

OSPF

Configuration ☐ Enable ☒ Disable

Port Profile

+ Port Profile

Name

Default ☐

Port Profile Application

+ Port Profile Application

Create Static Route

Destination *

Next Hop *

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. 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. You can add one or multiple next-hop addresses, separated by commas.

d. Optional: To add multiple static routes, click **+ Static Route**.

6. Add Open Shortest Path First (OSPF) configurations to this template. OSPF is a link-state routing protocol used to determine the best path for forwarding IP packets within an IP network. OSPF divides a network into areas to improve scalability and control the flow of routing information.

a. In the **OSPF** section, click **Enable** or **Disable** to enable or disable OSPF configurations.

b. If you click **Enable**, click **+ OSPF** to add an OSPF entry.

c. In the pop-up window, specify OSPF parameters, and then click **Apply**.

The screenshot shows a network configuration interface. On the left, the 'Static Route' section is visible, with 'OSPF' configuration options. The 'OSPF' section has 'Configuration' set to 'Enable' (indicated by a red box). Below it, a '+ OSPF' button is highlighted with a red box. On the right, a 'Create OSPF' pop-up window is open. It contains the following fields: 'IPv4/Prefixed' with the value '192.168.1.1/24', 'Area ID' with the value '235', and 'Area Type' with a dropdown menu set to 'Stub'. At the bottom of the pop-up window, there are 'Cancel' and 'Apply' buttons.

Table 4. OSPF Parameters

Parameter	Description
IPv4/Prefixlen	The network prefix and prefix length in IPv4 format. Click + to add more IPv4/Prefixlen. 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. NOTES • The area ID can be in IPv4 format or an integer ranging from 0 to 4294967295. • The area ID needs to be unique.
Area Type	The type of the OSPF area. Values are 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**.

d. Optional: To add multiple OSPF configurations, click **+ OSPF**.

7. Add port profiles. A port profile contains a set of port-related configurations to be applied to switch ports.

NOTE

AmpCon-Campus provides a built-in port profile named **Default**. Click **View** to check whether the profile meets your needs.

a. In the **Port Profile** section, click **+ Port Profile**.

b. In the pop-up window, enter the following information, and then click **Apply**.

Table 5. Port Profile Parameters

Parameter	Description
Profile Name	The name of the port profile.
NOTES	

	• The name needs to be unique. • The profile name needs to be a string of 1 to 32 case-sensitive characters; spaces are not supported.
Port Enable	Enables or disables the associated ports.
Description	Optional. The description of the port profile.
Port Mode	The port mode used to connect with the associated switches, Access or Trunk. • Access: Access ports typically connect to network devices, such as PCs, printers, IP phones, and IP cameras. In this mode, the ports can be in only one VLAN. • Trunk: Trunk ports typically connect to other switches, APs, and routers on the LAN. In this mode, the ports can be in multiple VLANs and can multiplex traffic between different VLANs.
Port VLAN	The native VLAN ID to which the port belongs. i NOTES • You can select only one VLAN ID. • You can select the VLAN ID 1, which is a system-defined VLAN ID. Or you can select one of the VLAN IDs that you added in the Network section.
Trunk VLAN	The VLAN ID of the trunk interface that allows frames from multiple networks (named VLAN IDs) to pass. i NOTES • The section is available only when you have select the Trunk mode. • You can select one or multiple VLANs by using either of the following ways:

	◦ To select all VLAN IDs ranging from 2 to 4094, click the All VLAN check box. ◦ If All VLAN is not selected, you can select VLAN IDs from the drop-down list below the All VLAN check box. • In the drop-down list, you can select the VLAN ID 1, which is a system-defined VLAN ID. And you can also select the VLAN IDs that you added in the Network section.
Speed	The port speed. Values are Auto, 10M, 100M, 1G, 2.5G, 5G, 10G, 25G, 40G, and 100G. • Auto means setting the port to work in the auto-negotiation mode. In the auto-negotiation mode, both ports of a link negotiate any rate supported by the two switches. • Selecting a specific speed value means manually specifying the speed value. For example, selecting 10M means the port speed is set to 10 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 switch template is applied. For more information, see set interface gigabit-ethernet speed.
PoE	Enables or disables the associated ports to support Power over Ethernet (PoE).

	 NOTE Ensure that the selected switches support PoE. PoE configurations will not be applied to the switches without PoE support. For more information, see Configuring PoE.
Storm Control	Enables or disables storm control to actively prevent packet proliferation and maintain the performance of the VLAN. For more information, see Storm Control in Ethernet Port Configuration.
Type	The packet types (broadcast, multicast, or unknown unicast packets) dropped automatically when the traffic exceeds the traffic level that you 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 Kbps. You need to specify the traffic level triggering the dropping of packets as follows: - When you select PPS, you can see the Packet Count per Second field. Enter a value ranging from 0 to 30000000. - When 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. - When you select Kbps, you can see the Kilobits per Second field. Enter a value ranging from 0 to 10000000.  NOTES

- For these three triggering methods, if the value is set to **0**, it means that data packets are not allowed to pass.
- For the platform of Trident4-X9 (switch model S6860-24CD8D), if you select **PPS** and enter **0** as the **Packet Count per Second** value, the value will be automatically changed to **1** when the configuration is pushed to associated PicOS switches.

c. Optional: Click **+ Port Profile** to add more port profiles.

8. Add a port configuration application to the template. A port configuration application associates a port profile with switch ports.

i NOTES

- A switch port can be associated with only one port profile.
- Each port profile can be associated with one or multiple switch ports.

a. Click **+ Port Profile Application**.

The screenshot shows the OSPF configuration page with a sidebar containing 'Port Profile' and 'Port Profile Application' sections. The 'Port Profile Application' section has a red box around the '+ Port Profile Application' button. A modal dialog titled 'Create Port Profile Application' is open, showing input fields for 'Ports' (with the value 'ge-1/1/1,ge-1/1/2') and 'Port Profile' (with the value 'test'). The dialog also has 'Cancel' and 'Apply' buttons.

b. In the pop-up window, enter the port profile name and one or multiple port names to apply the port profile, and then click **Apply**.

Table 6. Port Configuration Application Parameters

Parameter	Description
Ports	The port names to apply the port profile.
i NOTES	

	- Valid port names are in ge-x/x/x, te-x/x/x, qe-x/x/x, or xe-x/x/x format. - You can enter one or multiple port names. Example: ge-1/1/1, ge-1/1/2-10
Port Profile	The port profile name.

c. Optional: Click **+ Port Profile Application** to associate more port profiles with switch ports.

3. Adding Management-Related Configurations

In the **Management** section, add management-related configurations:

1. Add switch local users for device management purposes.

a. Click **+ Local User**.

b. In the pop-up window, input the username, user level, and password of the switch user, and confirm the password. Then, click **Apply**.

Table 7. Local User Parameters

Parameter	Description
Username	The name of the user. NOTES - The value is a string with at most 32 characters. The following characters are supported: - Lowercase letters including a to z. - Uppercase letters including A to Z. - Digits including 0 to 9.

	◦ Supported special characters (_ - \$). The character \$ can only be placed at the end of the string. • Usernames can start with an uppercase letter, a lowercase letter, or the special character (_).
User Level	The permission level of the user. Read-only or SuperAdmin. Read-only: Gives view-only or read-only permissions to a user. SuperAdmin: Gives all permissions to a user.
Password	The password for the user. The value is a string with at least 6 characters. The following characters must be included in each password: • Lowercase letters including a to z. • Uppercase letters including A to Z. • Digits including 0 to 9. • Supported special characters (@ # \$ % ! .).  NOTES • The value is a string with at least 6 characters. • The following characters must be included in each password: ◦ Lowercase letters including a to z. ◦ Uppercase letters including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (@ # \$ % ! .).
Confirm Password	The same as the value entered in the Password field.

c. Optional: Click + **Local User** to add more users.

2. Add login banner messages to the template.

- a. In the **Banner before Login** section, add a login banner message that you want users to see **before** they log in to a switch. You can enter up to 20 lines.
- b. In the **Banner after Login** section, add a login banner message that you want users to see **after** they log in to a switch. You can enter up to 20 lines.

Example: “Warning! This switch is managed by AmpCon-Campus. Do not make any CLI changes.”

Management

Local User

+ Local User

Username	User Level	Operation
test-xfx	super-user	Edit Delete

Login Banner

Banner before Login: Welcome to log in to this switch.

Banner after Login: Warning! This switch is managed by AmpCon-Campus. Do not make any CLI changes.

Idle Timeout (in Minutes)

Idle Timeout: 5

3. In the **Idle Timeout** field, enter the maximum number of minutes that a remote shell session can be idle. When this limit is reached, users are logged out.

Valid values range from 0 to 20000.

4. Click **Apply** to complete the switch template addition.

Verifying Template Application Results

Verify whether a switch template is applied successfully, follow these steps:

1. On the “Switch Templates” page, locate the switch template, and then click **Template Deployment Status**.

Template	Switches	Create Time	Operation
test-xfx	0	2025-08-20 02:56:29	View Copy Download Template Deployment Status Delete
test2	0	2025-08-19 04:06:20	View Copy Download Template Deployment Status Delete
test1	0	2025-08-19 04:00:25	View Copy Download Template Deployment Status Delete
no_empty	0	2025-08-19 03:17:55	View Copy Download Template Deployment Status Delete
test	0	2025-08-14 06:28:18	View Copy Download Template Deployment Status Delete
test::2025-8-14,14:52:19	0	2025-08-14 06:28:18	View Copy Download Template Deployment Status Delete
test::2025-8-14,14:52:19::2025-8-14,14:52:49	0	2025-08-14 06:28:18	View Copy Download Template Deployment Status Delete
test::2025-8-14,14:52:19::2025-8-14,14:53:03	0	2025-08-14 06:28:18	View Copy Download Template Deployment Status Delete

2. In the **Deployment Status** column of the pop-up window, check whether the switch template is applied to each listed switch.
- **Success:** The switch template is applied to a switch successfully.
 - **Running:** The switch template is being applied to a switch.

- **Pending:** The applying switch template process is pending and will begin after some time.
- **Failed:** The switch template fails to be applied to a switch.

Model	SN	Mgmt IP	Site	Deployment Status	Operation
S3410C-16TF	G18UBR1000297	10.14	default	Failed	Log
S3410-48TS-P	G18B0A002385	10.38	default	Failed	Log
as5812_54a	B3ASF1E9C7D1	10.46	default	Running	Log

3. If the status is **Failed**, click **Log** to see more details for troubleshooting.

NOTES

- If the status is **Running**, the switch template can't be edited or deleted.
- Switch template configurations can be applied to only switches that are connected to the AmpCon-Campus server.
- If a switch is displayed with a icon in the **Mgmt IP** column, it means that the switch is not connected to the AmpCon-Campus server. You need to resolve the connection issue first.

Managing Switch Templates

After you add switch templates, you can manage switch templates efficiently in the AmpCon-Campus UI.

[Viewing or Editing Switch Templates](#)

[Copying a Switch Template](#)

[Downloading a Switch Template](#)

[Importing a Switch Template](#)

[Deleting a Switch Template](#)

Viewing or Editing Switch Templates

Click **Network Design > Switch Templates** from the navigation bar. On the “Switch Templates” page, you can see all the added switch templates.

- To view detailed configurations of a switch template or edit a switch template, locate the template, and then click **View**.
- To edit a switch template, locate the template, and then click **View**. Modify the template configurations, and then click **Apply**.

Switch Templates				
+ Template Import				
Template	Switches	Create Time	Operation	
test-afa	0	2025-08-20 02:56:29	View	Copy Download Template Deployment Status Delete
test2	0	2025-08-19 04:06:20	View	Copy Download Template Deployment Status Delete
test1	0	2025-08-19 04:00:25	View	Copy Download Template Deployment Status Delete
no_empty	0	2025-08-19 03:17:55	View	Copy Download Template Deployment Status Delete
test	0	2025-08-14 06:28:18	View	Copy Download Template Deployment Status Delete
test::2025-8-14_14:52:19	0	2025-08-14 06:28:18	View	Copy Download Template Deployment Status Delete
test::2025-8-14_14:52:19::2025-8-14_14:52:49	0	2025-08-14 06:28:18	View	Copy Download Template Deployment Status Delete
test::2025-8-14_14:52:19::2025-8-14_14:53:03	0	2025-08-14 06:28:18	View	Copy Download Template Deployment Status Delete

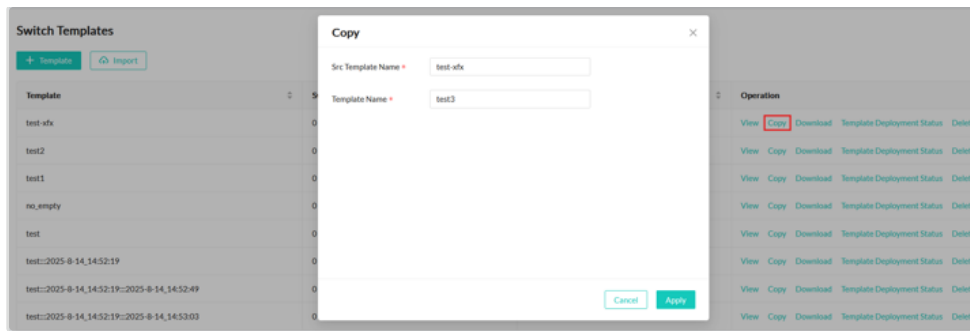
Copying a Switch Template

To copy a switch template, follow these steps:

NOTE

This operation will not copy the associated switches in the **Template Application Scope** section. In the new switch template, you need to [specify the template application scope](#).

1. Locate the template, and then click **Copy** on the “Switch Templates” page.
2. Enter a new name in the **Template Name** field. The name needs to be unique.



3. Click **Apply**.

Downloading a Switch Template

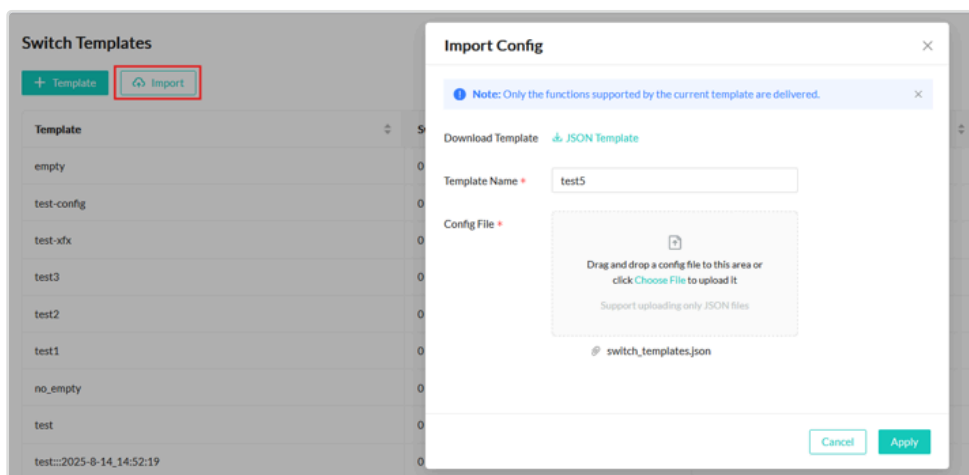
To download a switch template, locate the template, and then click **Download** on the “Switch Templates” page.

Template	Switches	Create Time	Operation
test-config	0	2025-08-20 03:09:56	View Copy Download Template Deployment Status Delete
test-xfx	0	2025-08-20 02:56:29	View Copy Download Template Deployment Status Delete
test3	0	2025-08-20 02:56:29	View Copy Download Template Deployment Status Delete
test2	0	2025-08-19 04:06:20	View Copy Download Template Deployment Status Delete
test1	0	2025-08-19 04:00:25	View Copy Download Template Deployment Status Delete
no_empty	0	2025-08-19 03:17:55	View Copy Download Template Deployment Status Delete

Importing a Switch Template

To import a switch template to AmpCon-Campus, follow these steps:

1. Click **Import** on the “Switch Templates” page.
2. In the pop-up window, click **JSON Template** to download a template JSON file, and then modify the file as needed.
3. In the **Template Name** field, enter the name of the switch template.
4. In the **Config File** section, upload the modified JSON file by dragging and dropping it here or clicking **Choose File**.



5. Click **Apply**.

Deleting a Switch Template

To delete a switch template, locate the template, and then click **Delete** on the “Switch Templates” page.

NOTE

After you delete a switch template, if the switch template has been applied, the configurations in the switch template are not deleted from applied switches.

Switch Templates				
+ Template Import				
Template	Switches	Create Time	Operation	
test-config	0	2025-08-20 03:09:56	View Copy Download Template Deployment Status Delete	
test-sfx	0	2025-08-20 02:56:29	View Copy Download Template Deployment Status Delete	
test3	0	2025-08-20 02:56:29	View Copy Download Template Deployment Status Delete	
test2	0	2025-08-19 04:06:20	View Copy Download Template Deployment Status Delete	
test1	0	2025-08-19 04:00:25	View Copy Download Template Deployment Status Delete	
no_empty	0	2025-08-19 03:17:55	View Copy Download Template Deployment Status Delete	

Configuration Templates

After onboarding PicOS switches, you can use configuration templates to push specific configurations that can't be pushed through switch templates.

AmpCon-Campus provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands. When pushing configurations to PicOS switches, select the configuration templates containing the required CLI commands, and select the switches to be configured. Then, these CLI commands will be run on the selected PicOS switches automatically.

You can also back up and restore configurations for disaster recovery, or compare configurations for troubleshooting or auditing.

See the following child topics:

- [Adding Configuration Templates](#)
- [Pushing Configurations to Switches](#)
- [Managing Configuration Templates](#)
- [Managing General Configurations](#)
- [Comparing Running Configurations with Initial Configurations](#)
- [Comparing Running or Backup Configurations](#)
- [Backing Up and Restoring Configurations](#)

Adding Configuration Templates

AmpCon-Campus provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands.

When deploying a PicOS switch to onboard it for AmpCon-Campus management, you must add a switch configuration with a configuration template.

After onboarding PicOS switches, when you push configurations to these PicOS switches, you can select one or multiple configuration templates to increase switch configuration pushing efficiency and reliability.

[Procedure](#)

[What to Do Next](#)

Procedure

To add a configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. In the **New Template** tab, input the following information:

The screenshot shows the 'New Template' form in the AmpCon-Campus UI. The form has tabs: New Template, Template List, Push Config, Template Verify, Config Archive Diff, and Config Backup. The 'New Template' tab is active. It contains fields for Name (test5), Descr, Model (as4610_30p), Version (4.5.0E), and Action (Config). A red box highlights the Name, Model, Version, and Action fields. Below these fields is a 'CLI Tree' section with a search bar and a list of hierarchical categories like protocols, system, interface, poe, alias, class-of-service, firewall, ip, vlans, xovs, I3-Interface, routing, mac-map, tracemac, ip-source-guard, and ipv6-source-guard. At the top right of the form are 'Save' and 'Update CLI Tree' buttons.

Table 1. Template Fields

Parameter	Description
Name	The name of the configuration template.
Descr	Optional. The description of the configuration template.

Model	The switch model that is applicable to the configuration template.  NOTE The CLI commands displayed in the CLI Tree section are different for different switch models.
Version	The PicOS version that is applicable to the configuration template.  NOTE The CLI commands in the CLI Tree section are different for different PicOS versions.
Action	Select Config or Delete.  NOTE If Config is selected, the commands in the CLI Tree section are in set type. If Delete is selected, the commands in the CLI Tree section are in delete type.

- Optional: Click **Update CLI Tree** to refresh the CLI tree. The CLI commands in the **CLI Tree** section will be refreshed automatically.
- In the **CLI Tree** section, add one or multiple CLI commands to the configuration template by clicking the plus icon. The selected CLI commands will appear on the right.

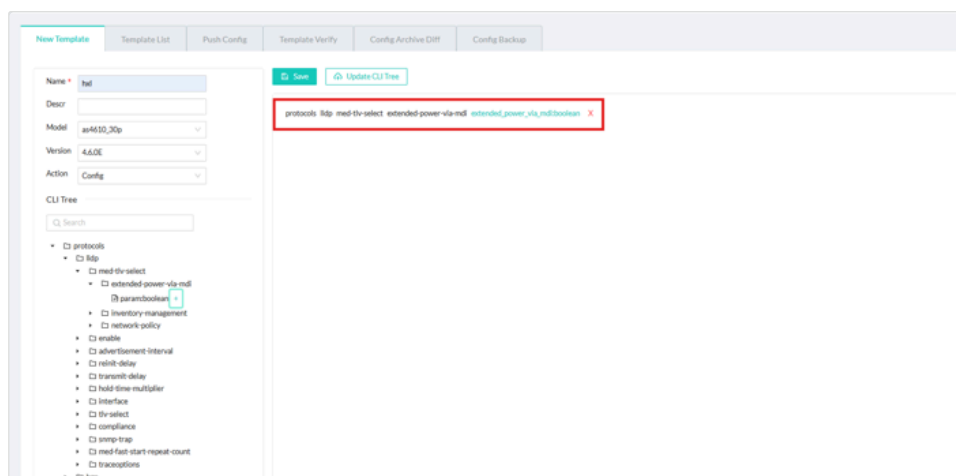
To remove a CLI command from the configuration template, click the icon **x**.

 NOTE

Ensure that a configuration template contains at least a command with variables. Or else, you will fail to push configurations to switches with this configuration template and fail to add a switch configuration with this configuration template.

In the following screenshot, because you select **Config** in the **Action** drop-down list, the complete command is **set protocols lldp med-tlv-select extended-power-via-mdi <extended_power_via_mdi>**.

<**extended_power_via_mdi**> is the variable that requires you to input when you push configurations to switches or add a switch configuration.



5. Click **Save**.

What to Do Next

- [Adding Switch Configurations](#)
- [Pushing Configurations to Switches](#)
- [Managing Configuration Templates](#)

Pushing Configurations to Switches

After onboarding PicOS switches, you can use configuration templates to push specific configurations that can't be pushed through switch templates.

[Prerequisite](#)

[Procedure](#)

[Verifying Pushing Status and Logs](#)

Prerequisite

- Ensure that the prerequisite tasks described in [Prerequisites](#) have been completed.
- Ensure that you have created the configuration templates with the required CLI commands. For more information, see [Adding Configuration Templates](#).

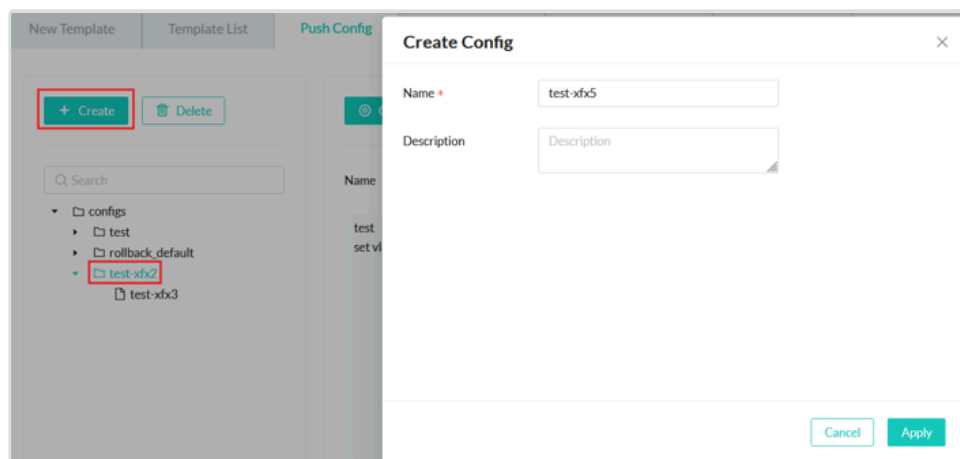
Procedure

To push configurations to one or multiple PicOS switches, follow these steps:

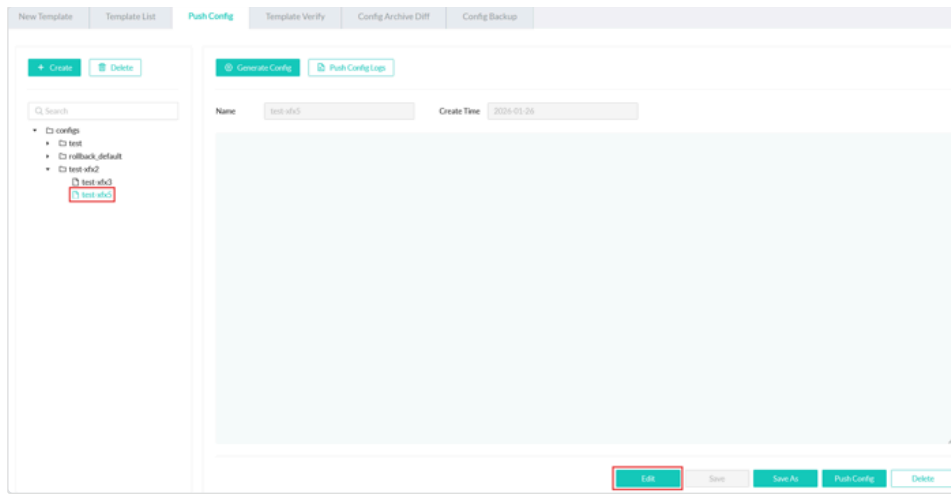
1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. In the **Push Config** tab, select a folder in the left panel, and then click **+ Create** to create a configuration node. The node will be displayed under the folder.

NOTES

- A configuration node represents a configuration file.
- AmpCon-Campus provides a built-in root folder named **configs**. After you add configuration nodes, these nodes can also be used as folders.



3. In the pop-up window, enter the configuration node name and its description (optional).
4. Click **Apply**.
5. Click the configuration node that you just created, and click **Edit**.

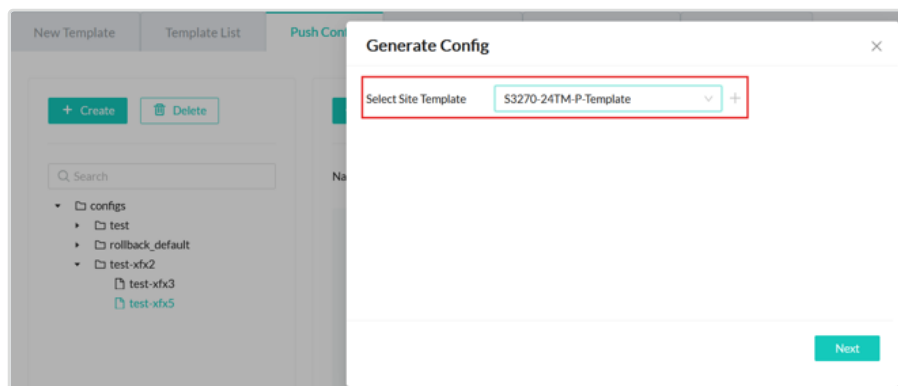


6. Add configurations to be pushed to switches by using either of the following ways:

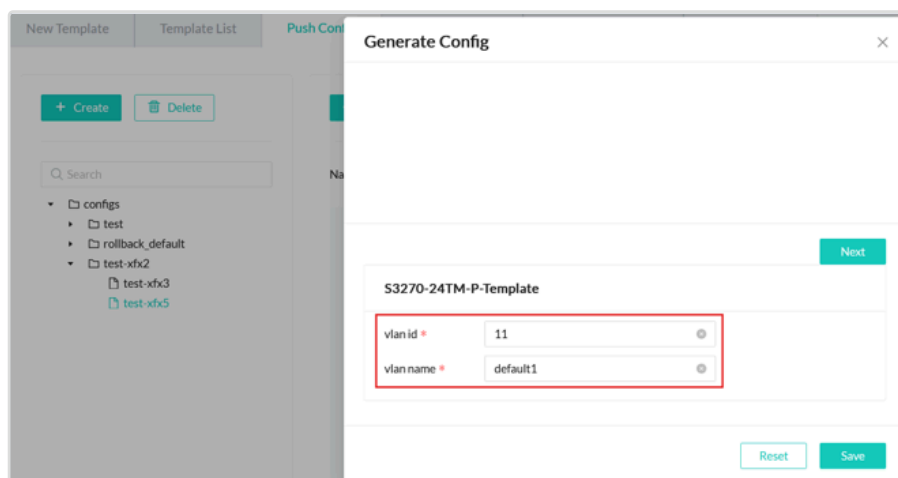
- Enter the CLI commands manually. This method is not recommended because manual CLI commands might lead to human errors.
- Use the configuration templates that you created before:

a. Click **Generate Config**.

b. Select a configuration template file from the drop-down list. You can also click the plus icon to add multiple configuration template files.

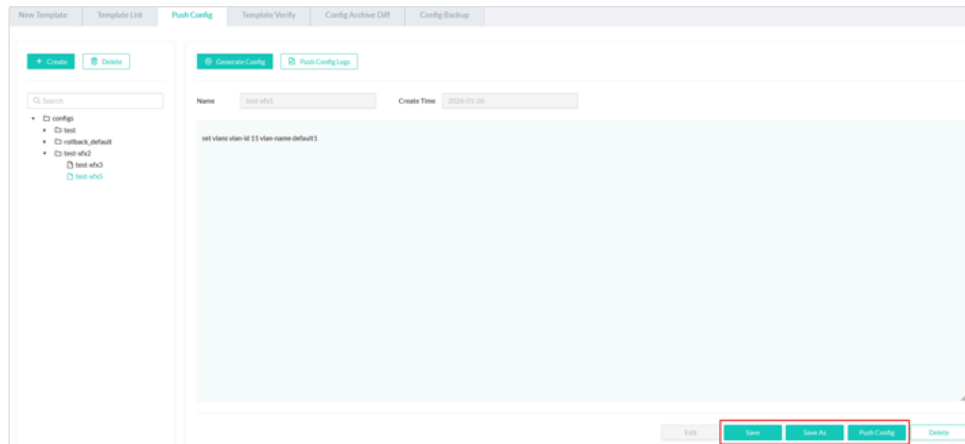


c. Click **Next**, and then enter the value for each variable.



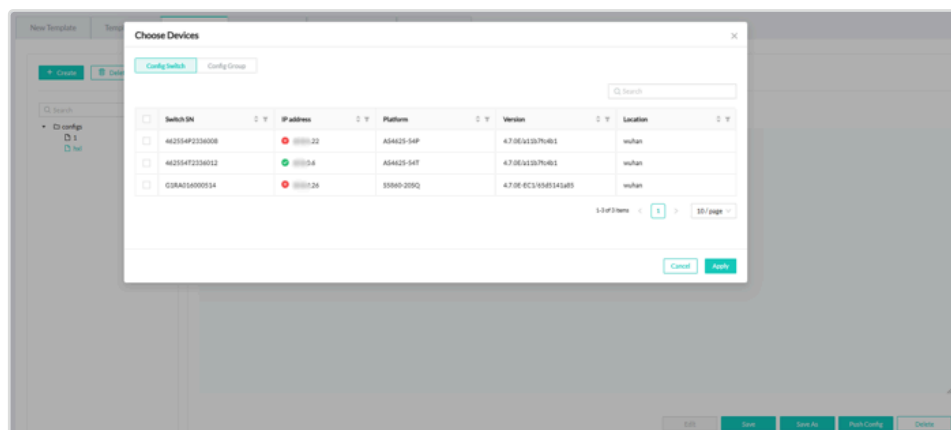
d. Click **Save**.

- Click **Save** to save this configuration node, or click **Save As** to generate a new configuration node with these added configurations.



- Click **Push Config**, and then select the PicOS switches to be configured.

You can select specific switches in the **Config Switch** tab or select a group in the **Config Group** tab. For how to add a group or manage PicOS switches in a group, see [Managing Groups](#).



- Click **Apply** to start the configuration pushing.

Verifying Pushing Status and Logs

To verify whether the configurations are pushed to each switch successfully, follow these steps:

- Click **Wired > Config Templates** from the navigation bar.
- Click the **Push Config** tab. In this tab, click **Push Config Logs**.
- In the pop-up window, locate the configuration pushing task related to the configuration node, and then click **Task List**.

NOTES

- A task name is ended with the related configuration node name.

- To check the configurations included in a configuration node, click **Config Content**.
- To mark a task as read, click **Mark As Read**.

Push Config Tasks Log

Task Name	Status	Create User	Create Time	Operation
2026-01-26 02:27:07.946417:test-xf5	Running	admin	2026-01-26 02:27:08	Task List Config Content Delete Mark As Read
2026-01-26 02:26:06.202830:test-6	Finished	admin	2026-01-26 02:26:06	Task List Config Content Delete Mark As Read
2026-01-23 02:03:14.867458:rollback_default	Finished	admin	2026-01-23 02:03:15	Task List Config Content Delete Mark As Read
2026-01-23 01:59:40.347651:rollback_default	Finished	admin	2026-01-23 01:59:40	Task List Config Content Delete Mark As Read
2026-01-23 01:58:17.066487:rollback_default	Finished	admin	2026-01-23 01:58:17	Task List Config Content Delete Mark As Read
2026-01-23 01:57:47.422177:rollback_default	Finished	admin	2026-01-23 01:57:47	Task List Config Content Delete Mark As Read
2026-01-22 10:21:10.290621:test	Finished	admin	2026-01-22 10:21:10	Task List Config Content Delete Mark As Read

1-7 of 7 items < 1 10 / page

4. In the **Task List** pop-up window, check whether the pushing status is **Success**.

If the pushing status is not **Success**, click **Push Log** to check more pushing details for troubleshooting.

Task List

SN	Push Status	End Time	Operation
G1590LV001308	Success	Fri, 23 Jan 2026 02:03:24 GMT	Push Log
G1590LV000417	Success	Fri, 23 Jan 2026 02:03:32 GMT	Push Log
HWCG2505051720N00001	Success	Fri, 23 Jan 2026 02:03:42 GMT	Push Log
HWCG2505051720N00006	Success	Fri, 23 Jan 2026 02:03:52 GMT	Push Log
HWCG2505051720N00016	Success	Fri, 23 Jan 2026 02:04:02 GMT	Push Log
G15713N000045	Success	Fri, 23 Jan 2026 02:04:14 GMT	Push Log
HWCG2411255754N00055	Success	Fri, 23 Jan 2026 02:04:20 GMT	Push Log
HWCG2411255754N00065	Success	Fri, 23 Jan 2026 02:04:25 GMT	Push Log
HWCG2406296358N00038	Success	Fri, 23 Jan 2026 02:04:32 GMT	Push Log
HWCG2406296358N00049	Success	Fri, 23 Jan 2026 02:04:38 GMT	Push Log

1-5 of 5 items < 1 10 / page

Managing Configuration Templates

You can manage all the added configuration templates as follows:

[Viewing or Editing a Configuration Template](#)

[Removing a Configuration Template](#)

[Viewing or Updating Pre-Built Templates](#)

[Copying a Configuration Template](#)

[Exporting a Configuration Template](#)

[Exporting All Configuration Template](#)

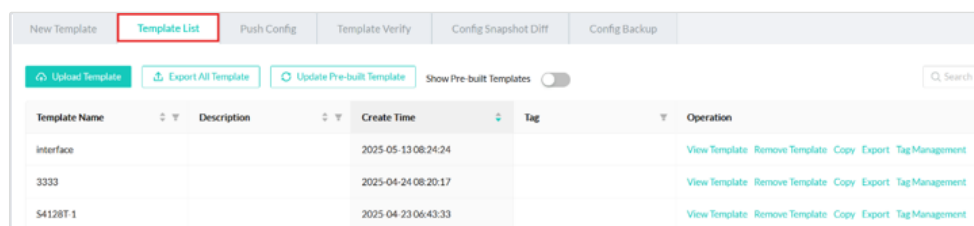
[Adding a Label to a Configuration Template](#)

[Uploading a Local Configuration Template](#)

Viewing or Editing a Configuration Template

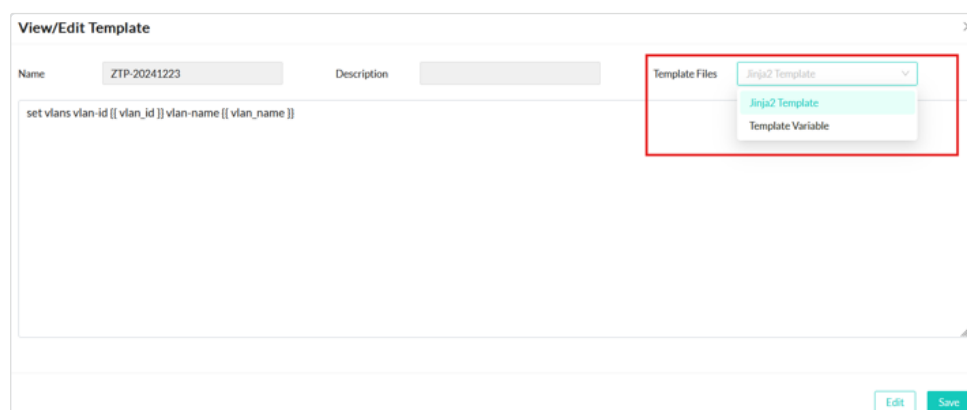
To view or edit a configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab.



New Template	Template List	Push Config	Template Verify	Config Snapshot Diff	Config Backup
Upload Template	Export All Template	Update Pre-built Template	Show Pre-built Templates	Search	
Template Name	Description	Create Time	Tag	Operation	
interface		2025-05-13 08:24:24		View Template Remove Template Copy Export Tag Management	
3333		2025-04-24 08:20:17		View Template Remove Template Copy Export Tag Management	
S4128T1		2025-04-23 06:43:33		View Template Remove Template Copy Export Tag Management	

3. Locate a switch, and then click **View Template**.
4. To view a configuration template, select the format for viewing the template in the pop-up window. Then, you can see the template configurations.



View/Edit Template

Name: ZTP-20241223 Description:

Template Files: Jinja2 Template Jinja2 Template Template Variable

set vlans vlan-id {{ vlan_id }} vlan-name {{ vlan_name }}

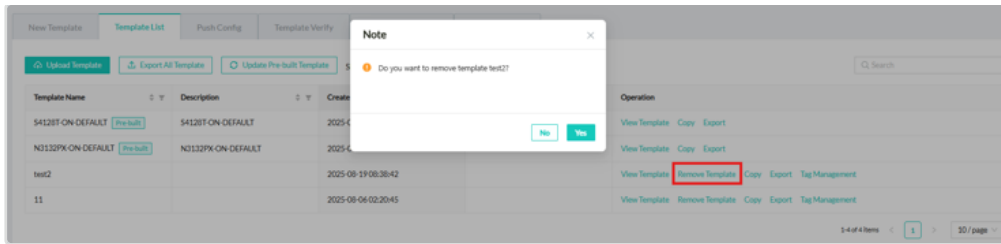
Edit Save

5. To edit a configuration template, click **Edit** in the pop-up window, and then click **Save**.

Removing a Configuration Template

To remove a configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, locate a switch, and then click **Remove Template**.

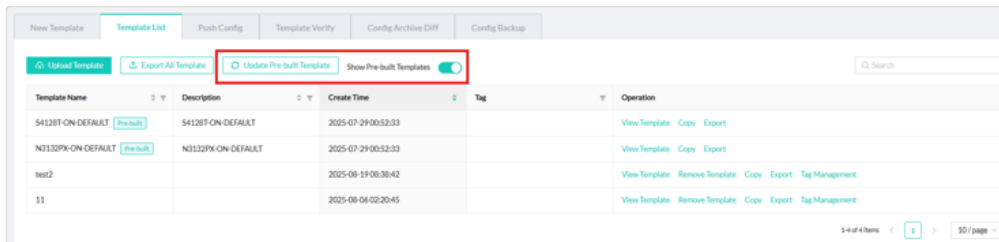


3. Click **Yes** to confirm the deletion.

Viewing or Updating Pre-Built Templates

To view or update pre-built configuration templates, follow these steps:

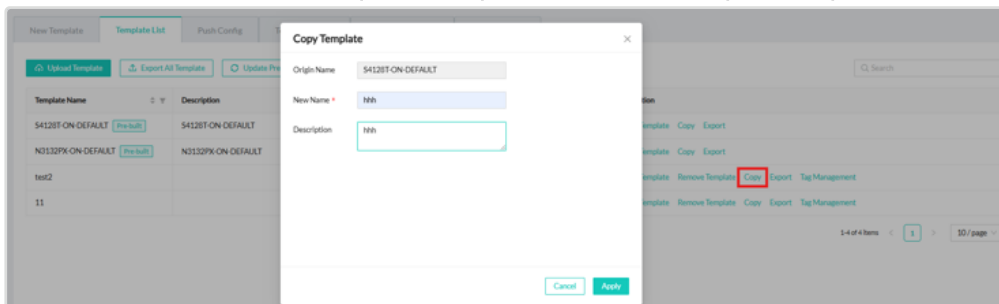
1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, do the following operations as needed:
 - To view the pre-built templates, click **Show Pre-built Template**.
 - To refresh the pre-built template list, click **Update Pre-built Template**.



Copying a Configuration Template

To copy a configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, locate a switch, and then click **Copy**.
3. Enter the name for the copied template and a description (optional).

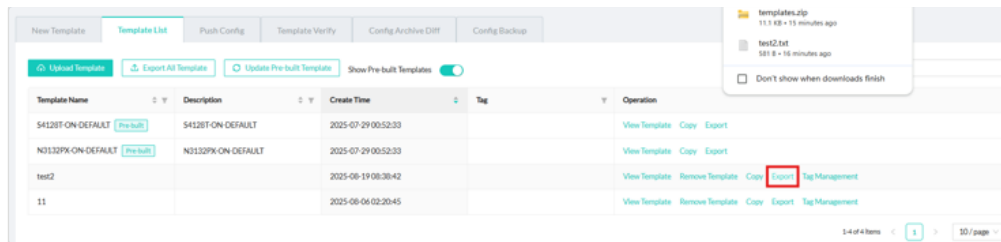


4. Click **Apply**.

Exporting a Configuration Template

To export a configuration template, follow these steps:

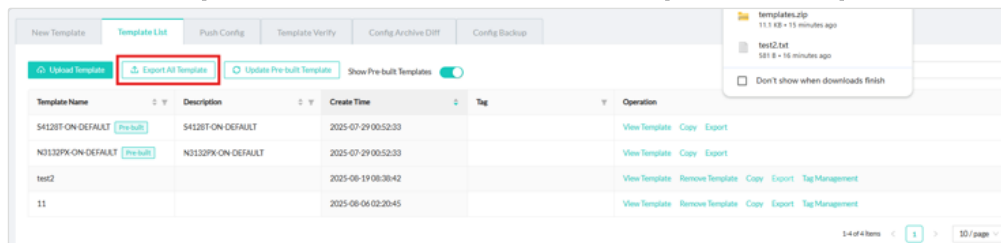
1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, locate a switch, and then click **Export**.



Exporting All Configuration Template

To export all configuration templates, follow these steps:

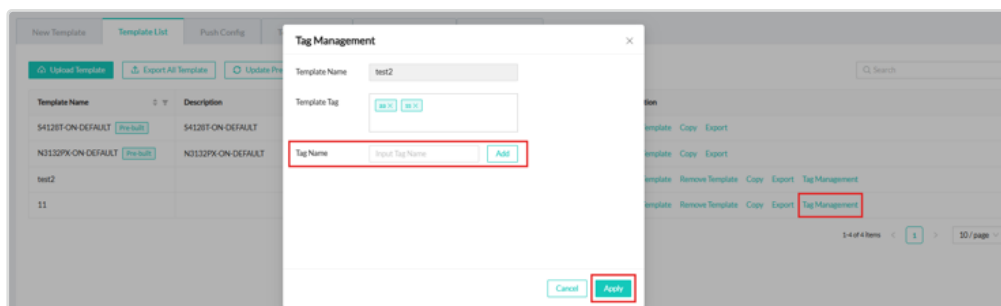
1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, click **Export All Template**.



Adding a Label to a Configuration Template

To add a label to a configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, locate a switch, and then click **Tag Management**.
3. In the pop-up window, enter the name of the tag.
4. Click **Add**.

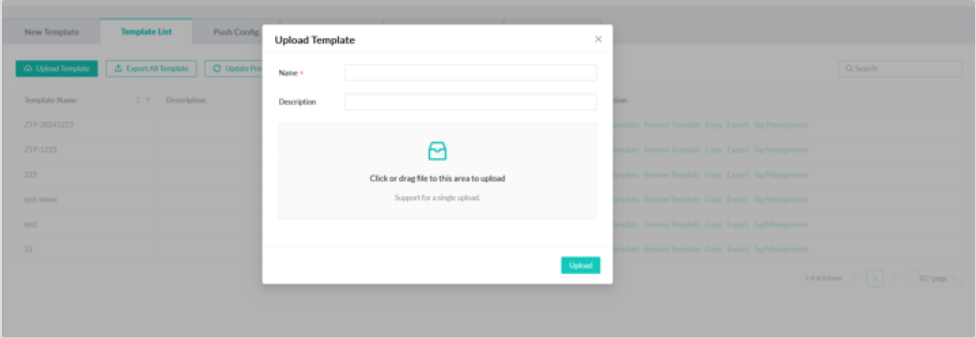


5. Click **Apply**.

Uploading a Local Configuration Template

To upload a local configuration template, follow these steps:

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. Click the **Template List** tab. In this tab, click **Upload Template**.
3. In the pop-up window, enter the name of the configuration template and the template description (optional).
4. Click or drag a .txt template file to upload it.
5. Click **Upload**.



Managing General Configurations

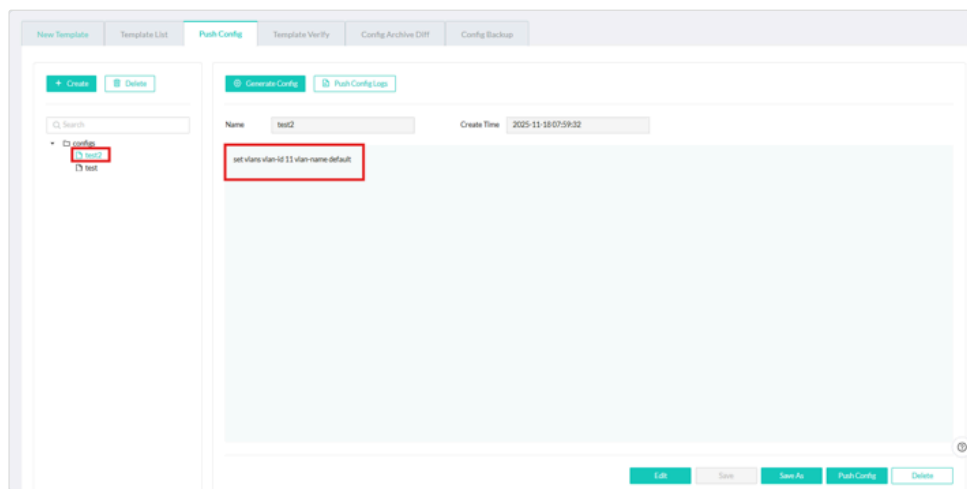
You can view, edit, or delete the configuration nodes that you created as described in [Pushing Configurations to Switches](#).

[Viewing or Editing a Configuration Node](#)

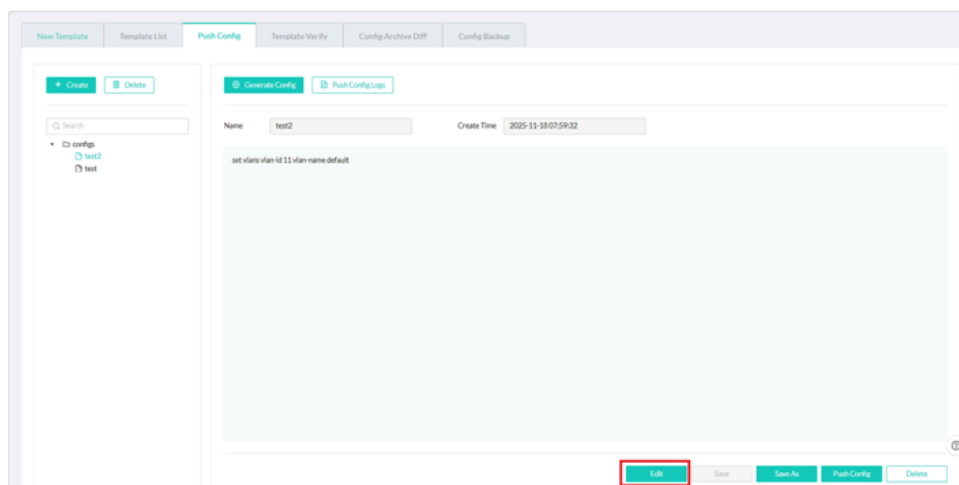
[Deleting a Configuration Node](#)

Viewing or Editing a Configuration Node

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. In the **Push Config** tab, click the configuration node that you want to view or edit. You can see the CLI commands in the right panel.

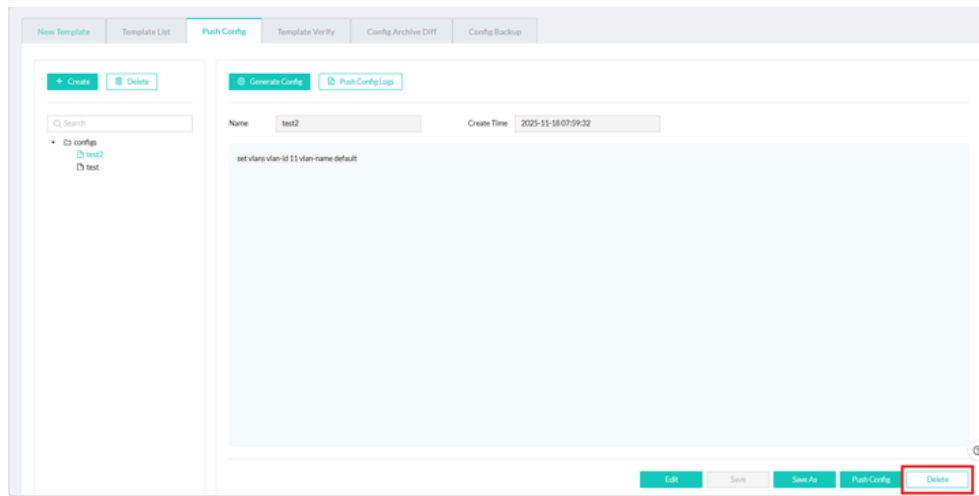


To edit a configuration node, click **Edit**, modify the CLI commands included in the node, and then click **Save**.



Deleting a Configuration Node

1. In the **Push Config** tab, click the configuration node that you want to delete.
2. Click **Delete**, and then click **Yes** to confirm the deletion.



Comparing Running Configurations with Initial Configurations

You can compare running configurations with initial configurations on the same switch.

- **Initial configurations**

Configurations that you selected when you add a switch configuration, including the global configuration file and the configuration template

- **Running configurations**

Configurations that are currently running on the switch

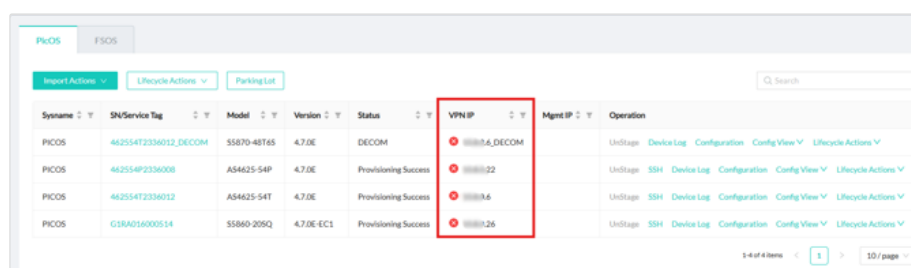
NOTE

This feature doesn't support the following scenarios:

- Comparing configurations on two different switches.
- Comparing configurations on imported switches.
- Comparing configurations on disconnected switches (switches can't connect with the AmpCon-Campus server).

Prerequisites

- Check the **VPN IP** column on the “Switches” page, and ensure that the switch to compare is connected to the AmpCon-Campus server.
 - ✓: The switch is connected to the AmpCon-Campus server.
 - ✗: The switch is not connected to the AmpCon-Campus server.



Sysname	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation
PICOS	46255472336012_DECOM	S5870-48T6S	4.7.0E	DECOM	192.168.1.22		Unstage Device Log Configuration Config View Lifecycle Actions
PICOS	462554P2336008	A54625-54P	4.7.0E	Provisioning Success	192.168.1.22		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	46255472336012	A54625-54T	4.7.0E	Provisioning Success	192.168.1.6		Unstage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	G5RA016000514	S5860-205Q	4.7.0E-EC1	Provisioning Success	192.168.1.25		Unstage SSH Device Log Configuration Config View Lifecycle Actions

- Check the **Status** column, and ensure that the switch to compare is not in **Imported** status.

After you replace an imported switch with a new switch through RMA, the new switch is shown as **Provisioning Success**. However, you still can't compare running configurations with initial configurations on this new switch.

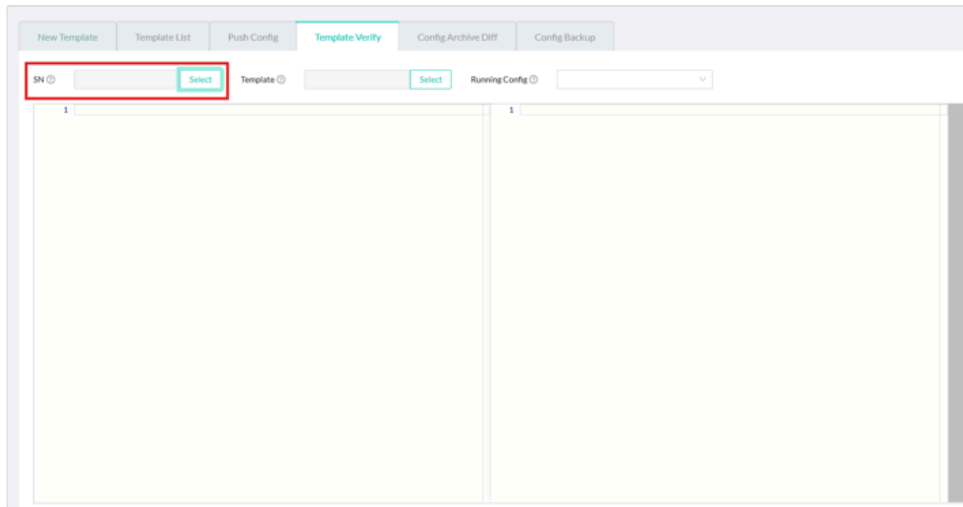
This is because the new switch is configured through the backup configuration file or uploaded configurations of the imported switch during the deployment process, instead of creating a switch configuration.

Procedure

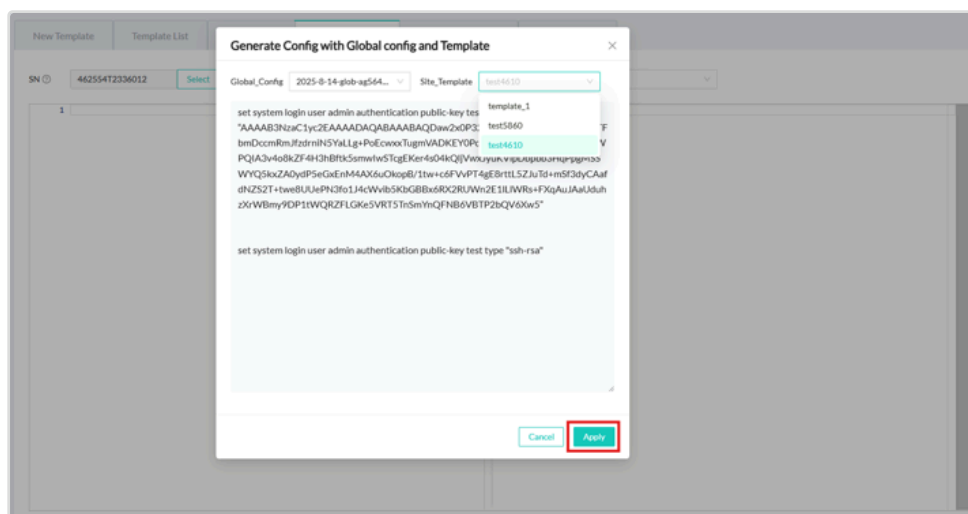
1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. In the **Template Verify** tab, click **Select** in the **SN** field.

NOTE

Ensure that the selected switch is online, which means the switch is not connect with the AmpCon-Campus server.

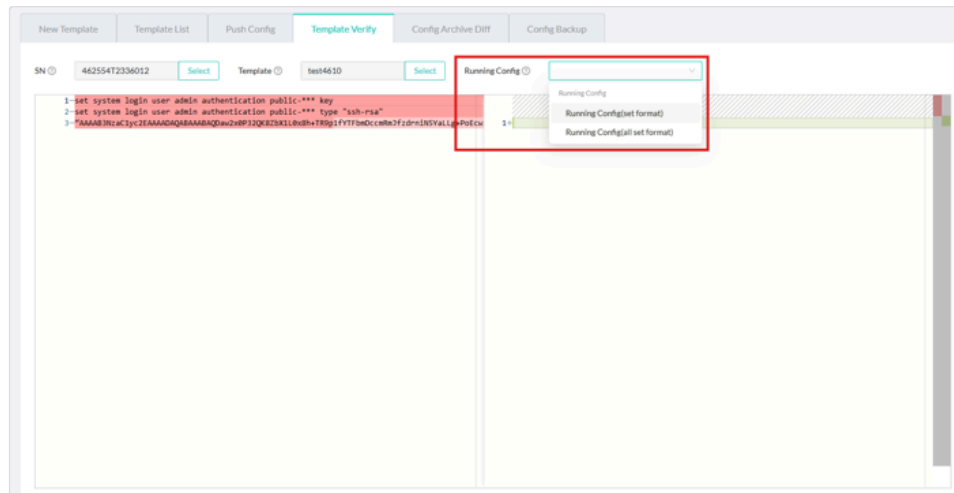


3. In the pop-up window, select the switch to compare.
4. In the **Template** field, click **Select**.
5. In the pop-up window, select the global configuration file and the configuration template that you pushed to the switch during the initial switch deployment process. Then, click **Apply**.



6. In the **SN** drop-down list, select **Running Config(set format)** or **Running Config(all set format)**.
- **Running Config(set format):** Displays configurations as the **show | display set** command result in the switch.

- **Running Config(all set format):** Displays configurations as the **show all | display set** command result in the switch.



Then, you can see differences between the running configurations and the initial configurations on the switch.

Comparing Running or Backup Configurations

You can compare running configurations or backup configurations on one switch or on different switches.

- **Running configurations**

Configurations that are currently running on a switch.

- **Backup configurations**

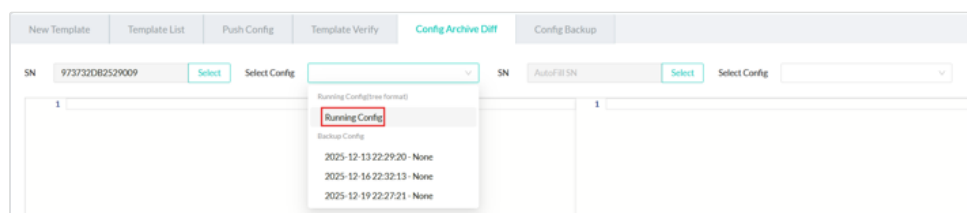
Configuration files that were backed up as described in [Backing Up Configurations](#).

Procedure

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
2. In the **Config Archive Diff** tab, click **Select** in the first **SN** section. In the pop-up window, select a switch.
3. In the first **Select Config** drop-down list, select **Running Config** or a backup configuration file.

NOTES

- For offline switches (switches are not connect with the AmpCon-Campus server), **do not** select **Running Config**. This is because AmpCon-Campus can't retrieve the current configurations from the offline switch.
- If no backup configuration files are displayed, create a new backup configuration file. For more information, see [Backing Up Configurations](#).



4. In the second **SN** section, click **Select**. In the pop-up window, select another switch.
5. In the second **Select Config** drop-down list, select a running configuration file or a backup configuration file.

Then, you can see configuration differences as follows:

New Template

Template List

Push Config

Template Verify

Config Archive Diff

Config Backup

SN

97373202529009

Select

Select Config

Running Config

SN

HWC6250411489760004

Select

Select Config

Running Config

72

}

73

}

74

symmetric: false

75

}

76

flowset-count: 1

77

}

78

cut-through-mode: false

79

gigabit-ethernet "xe-1/1/1.1" {

80

description: ""

81

mtu: 1514

82

disable: false

83

power-preemphasis-level: 0

84

smp-trap: true

85

loopback: false

86

mac-learning: true

87

acceptable-frame: "all"

88

training: false

89

speed: "auto"

90

}

91

gigabit-ethernet "xe-1/1/1.2" {

92

description: ""

93

mtu: 1514

94

disable: false

95

power-preemphasis-level: 0

96

smp-trap: true

97

loopback: false

98

mac-learning: true

99

acceptable-frame: "all"

100

training: false

101

speed: "auto"

102

}

103

gigabit-ethernet "xe-1/1/1.3" {

104

description: ""

105

mtu: 1514

106

disable: false

107

power-preemphasis-level: 0

108

smp-trap: true

109

loopback: false

110

}

111

.....

112

.....

72

}

73

}

74

symmetric: false

75

}

76

flowset-count: 1

77

}

78

cut-through-mode: false

79

gigabit-ethernet "xe-1/1/1.1" {

80

description: ""

81

mtu: 1514

82

disable: false

83

power-preemphasis-level: 0

84

smp-trap: true

85

loopback: false

86

mac-learning: true

87

}

88

gigabit-ethernet "xe-1/1/1.2" {

89

description: ""

90

mtu: 1514

91

disable: false

92

power-preemphasis-level: 0

93

smp-trap: true

94

loopback: false

95

mac-learning: true

96

}

97

gigabit-ethernet "xe-1/1/1.3" {

98

description: ""

99

mtu: 1514

100

disable: false

101

power-preemphasis-level: 0

102

smp-trap: true

103

loopback: false

104

}

105

.....

106

.....

Backing Up and Restoring Configurations

For the PicOS switches managed by AmpCon-Campus, you can automatically back up configurations at a specific interval and time or manually back up configurations. In addition, you can restore configurations based on a backup configuration file for disaster recovery.

Backing Up Configurations

[Backing Up Configurations Automatically](#)

[Backing Up Configurations Manually](#)

[Checking Backup Configuration Files](#)

[Rolling Back Configurations](#)

[Optional Operations](#)

[Uploading Configurations](#)

[Viewing Configurations](#)

[Viewing Backup Logs](#)

Backing Up Configurations

Backing Up Configurations Automatically

To back up configurations for switches periodically and automatically, follow these steps:

NOTES

- For a switch deployed through ZTP, if **Backup Config** is not selected in the **Option Post-Deployed** section when you add the switch configuration, the automatic backup will not work for this switch. You can manually back up configurations for this switch.
- For a switch imported to AmpCon-Campus, the automatic backup is enabled by default. You don't need to configure the switch configuration interval for this switch.

- In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
- Click the **Config Backup** tab. In this tab, set the automatic backup interval and time:

Host Name	IP address	Switch SN	Version	Flag	Last Backup Time	Operation
RuCE-1-157	10.1.1.14	G15R0LV00085	4.6.0E-DCN/192967696	R	2025-08-20 08:47:19	Config Backup Config Upload Config Archive List Device Log
RuCE-2-304	10.1.1.46	G15R0LV00135	4.6.0E-DCN/192967696	R	2025-08-20 07:30:19	Config Backup Config Upload Config Archive List Device Log
Inone-001-mone-1	10.1.1.226	65FDC8D34373	4.6.0E/99a70d689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
PIC05	10.1.1.234	65FDC8D34371	4.6.0E/99a70d689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
Pluto-0804-001-MAC2-1	10.1.1.82	HWCG2406296359N00099	4.6.0E-EC/192967696	R	2025-08-19 22:24:22	Config Backup Config Upload Config Archive List Device Log
spine-1	10.1.1.198	A76F0DL36600023	4.6.0E-DCN/192967696	R	2025-08-19 22:24:20	Config Backup Config Upload Config Archive List Device Log
spine-2	10.1.1.190	HWCG2312185480N00004	4.6.0E-DCN/192967696	R	2025-08-19 22:24:16	Config Backup Config Upload Config Archive List Device Log
PIC05	10.1.1.122	HWCG220627499N000025	4.6.0E-DCN/192967696	R	2025-08-19 22:23:15	Config Backup Config Upload Config Archive List Device Log
PIC05	10.1.1.194	HWCG2500104937N000013	4.6.0E-DCN/192967696	R	2025-08-19 22:23:13	Config Backup Config Upload Config Archive List Device Log
PIC05	10.1.1.130	DHA03844A3M	4.6.0E/99a70d689	R	2025-08-19 22:11:08	Config Backup Config Upload Config Archive List Device Log

- Interval Days:** The interval in days between each backup.

- **Hours:** The time (a specific hour) when a backup is started.

3. Click **Save**. Then, AmpCon-Campus will automatically back up configurations at the specific interval and time.

Backing Up Configurations Manually

1. In the AmpCon-Campus UI, click **Wired > Config Templates** from the navigation bar.
 2. Click the **Config Backup** tab. In this tab, manually back up configurations for a single switch or all switches in a switch group:
- To back up configurations for a single switch, locate the switch, and then click **Backup Config**.

Host Name	IP address	Switch SN	Version	Flag	Last Backup Time	Operation
RUCF-1-157	10.8.0.114	G19X0U00085	4.6.0E OCN/1929676956	R	2025-08-20 08:47:19	Config Backup Config Upload Config Archive List Device Log
RUCF-2-104	10.8.0.46	G19X0U001185	4.6.0E OCN/1929676956	R	2025-08-20 07:30:19	Config Backup Config Upload Config Archive List Device Log
PICO5	10.8.0.224	45FDCID04371	4.6.0E/9b70da689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
Spine-003-nore-1	10.8.0.226	45FDCID04373	4.6.0E/9b70da689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
Photo-0804-003-MAC2-1	10.8.0.182	HWCG2406296359N00099	4.6.0E/6C1/1929676956	R	2025-08-19 22:24:22	Config Backup Config Upload Config Archive List Device Log
spine-1	10.8.0.196	A76AF0DL166000023	4.6.0E OCN/1929676956	R	2025-08-19 22:24:20	Config Backup Config Upload Config Archive List Device Log
spine-2	10.8.0.190	HWCG2312185480N00004	4.6.0E OCN/1929676956	R	2025-08-19 22:24:16	Config Backup Config Upload Config Archive List Device Log
PICO5	10.8.0.122	HWCG2206274999N00025	4.6.0E OCN/1929676956	R	2025-08-19 22:23:15	Config Backup Config Upload Config Archive List Device Log
PICO5	10.8.0.194	HWCG2503104937N00013	4.6.0E OCN/1929676956	R	2025-08-19 22:23:13	Config Backup Config Upload Config Archive List Device Log
PICO5	10.8.0.30	D4A308A4A3AF	4.6.0E/9b70da689	R	2025-08-19 22:11:08	Config Backup Config Upload Config Archive List Device Log

- To back up configurations for all switches in a switch group, select the switch group from the **Group Name** drop-down list, and then click **Backup Config**.

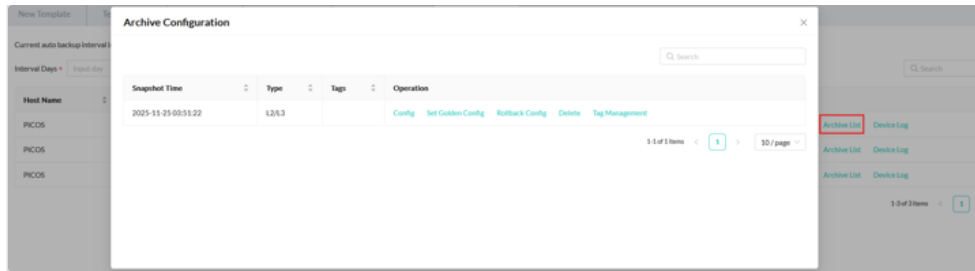
To add a new switch group, see [Adding a Switch Group](#).

Synonym	Address	Switch SN	Version	Flag	Last Backup Time	Operation
	10.8.0.142	HWCG2312185478N000031				Config Backup Config Upload Config Archive List Device Log
PICO5	10.8.0.46	G185147000410	4.7.0E/ovs-rgb/16a0568c6	R	2025-12-01 22:21:04	Config Backup Config Upload Config Archive List Device Log
leaf1-1	10.8.0.18	62A778A8FF3	4.6.0E/1929676956	R	2025-10-16 22:03:01	Config Backup Config Upload Config Archive List Device Log
spine-1	10.8.0.10	62A778A8FF1	4.6.0E/1929676956	R	2025-10-14 02:13:58	Config Backup Config Upload Config Archive List Device Log
spine-2	10.8.0.14	62A778A8FF2	4.6.0E/1929676956	R	2025-10-14 02:13:58	Config Backup Config Upload Config Archive List Device Log

Checking Backup Configuration Files

To check whether the backup configuration file for a switch is created successfully, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Archive List**.
2. In the pop-up window, check whether the backup configuration file is displayed in the archive list.



In the archive list, you can do the following operations if needed:

- To check the details in a backup configuration file, click **Config**.
- To mark a backup configuration file with the **Golden Config** tag, click **Set Golden Config**. Only one backup configuration file can be marked with **Golden Config**.

NOTES

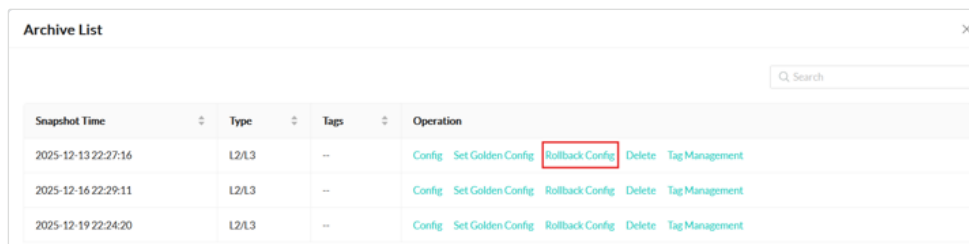
- The maximum number of backup configuration files that you can create is determined by the **Config Backup Number** value in the global system configuration. For more information, see [Adding a Global System Configuration](#).
- The backup configuration files marked with **Golden Config** are used for switch RMA. For more information, see [RMA Workflow](#).

- To delete a backup configuration file, click **Delete**.
- To add or delete tags for a backup configuration file, click **Tag Management**. The added tags will be displayed in the **Tags** column.

Rolling Back Configurations

To restore configurations based on a backup configuration file, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Archive List**.
2. Locate the back configuration file, and then click **Rollback Config**.

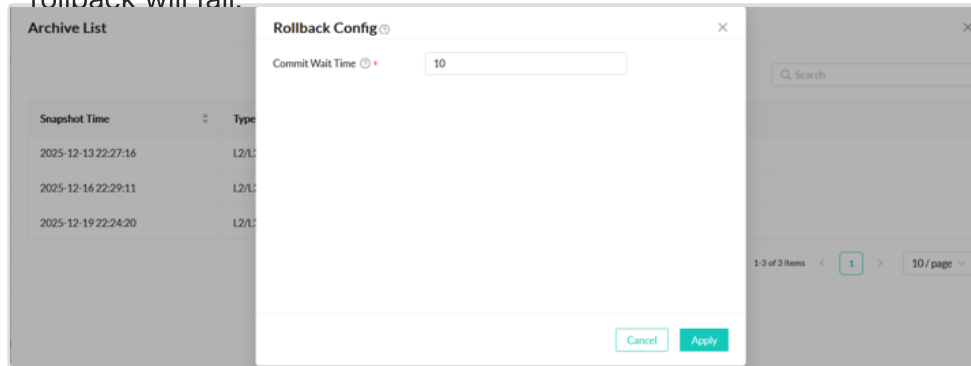


3. In the **Commit Wait Time** field of the pop-up window, set the wait time in seconds.

The default value is 10. The value needs to be an integer ranging from 10 to 240.

NOTE

In some cases, AmpCon-Campus can't access switches. After you click **Apply** in the pop-up window, if AmpCon-Campus still can't access the switch after the specified **Commit Wait Time**, the rollback will fail.



4. Click **Apply**.

Optional Operations

Uploading Configurations

You can upload a local switch configuration file to AmpCon-Campus. After you upload the configuration file, the uploaded configurations can't be pushed to the switch. These uploaded configurations can be pushed to only the new switch during the RMA process. For more information, see [RMA Workflow](#).

To upload local configurations for a switch, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Upload Config**.

Current auto backup interval is *days at time 22:00

Interval Days: 3 Hours: 03 Save Group Name: All Backup Config Select Time View Report Q Search

Host Name	IP address	Switch SN	Version	Flag	Last Backup Time	Operation
RuCE-1-157	1.14	G15903V00085	4.6.0E OCN192967686	R	2025-08-20 08:47:19	Config Backup Config Upload Config Archive List Device Log
RuCE-2-104	0.46	G15903V001185	4.6.0E OCN192967686	R	2025-08-20 07:10:19	Config Backup Config Upload Config Archive List Device Log
Inone-001 none-1	0.226	65FDC8D34373	4.6.0E 9bc70da689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
PIC05	0.234	65FDC8D34371	4.6.0E 9bc70da689	R	2025-08-20 04:04:47	Config Backup Config Upload Config Archive List Device Log
Pluto-0804-001-MLAG2-1	1.82	HWC22406296359N00099	4.6.0E EC1192967686	R	2025-08-19 22:24:22	Config Backup Config Upload Config Archive List Device Log
spline-1	1.98	A76AF0DL166000023	4.6.0E OCN192967686	R	2025-08-19 22:24:20	Config Backup Config Upload Config Archive List Device Log
spline-2	1.90	HWC22312185480N00004	4.6.0E OCN192967686	R	2025-08-19 22:24:16	Config Backup Config Upload Config Archive List Device Log
PIC05	1.22	HWC2206274996N00025	4.6.0E OCN192967686	R	2025-08-19 22:23:15	Config Backup Config Upload Config Archive List Device Log
PIC05	1.94	HWC22503104937N00013	4.6.0E OCN192967686	R	2025-08-19 22:23:13	Config Backup Config Upload Config Archive List Device Log
PIC05	0.30	D4A30844A3AF	4.6.0E 9bc70da689	R	2025-08-19 22:11:08	Config Backup Config Upload Config Archive List Device Log

5-10 of 17 items 1 2 3 4 10 / page

2. Select a .boot file containing switch configurations, and then upload the file.

Viewing Configurations

Each time you back up configurations for a switch, AmpCon-Campus will collect all the configurations from the switch and display these configurations in the **Configuration** pop-up window. The uploaded configurations are also displayed in the **Configuration** pop-up window.

To view these configurations, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Config**.

2. In the **Configuration** pop-up window, check the configurations as follows:



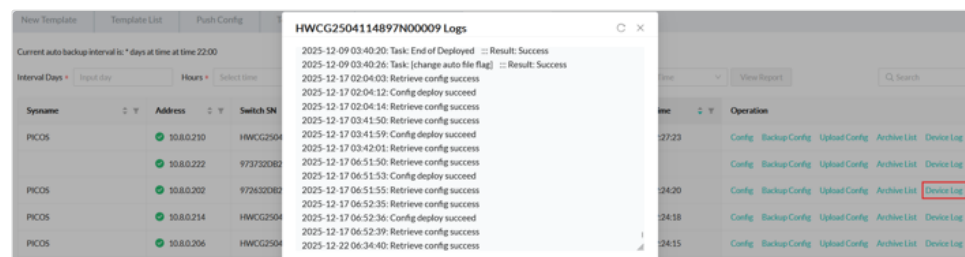
You can click **Show SET-format** to display the configurations in **set xx** format.



Viewing Backup Logs

To view backup logs of a switch, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Device Log**.
2. In the pop-up window, check whether the backup is successful. The message “Retrieve config success” indicates a successful backup.



Running Ansible Playbooks for Automation

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.

AmpCon-Campus offers the `picos_config` Ansible module to interact with managed devices, 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, run, and schedule Ansible playbooks on managed PicOS switches and added Linux servers, reducing manual work, eliminating configuration errors, and improving network management efficiency.

See the following child topics:

- [Examples for Ansible Playbooks](#)
- [Running Playbooks](#)
- [Adding Other Devices](#)
- [Managing Ansible Jobs](#)
- [Viewing Playbook Scheduling](#)
- [Troubleshooting](#)

NOTES

- For more information about Ansible, see [Getting started with Ansible](#).
- For the workflow of running Ansible playbooks with AmpCon-Campus, see [Ansible Automation Workflow](#).

Examples for Ansible Playbooks

Ansible modules are code or binaries that Ansible copies to and 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 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 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 switches with PicOS installed.

- To run Ansible playbooks on Linux servers that you added, write playbooks based on playbook syntax described in [Using Ansible playbooks](#).
- For the workflow of using Ansible playbooks on AmpCon-Campus, see [Ansible Automation Workflow](#).
- 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](#)

[Related PicOS References](#)

Syntax Examples

Running Linux Shell Commands

To run Linux shell commands in managed switches, use the **shell** mode.

Playbook YAML Example:

```
1 ---
2 - name: Shows uptime info for all switches
3   hosts: all
4   tasks:
5     - name: Shows uptime info for all switches
6       picos_config: mode='shell' cmd='uptime'
7       register: exec_result
8     - name: Show execution result
```

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 Linux shell command to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-Campus UI. For how to check playbook execution results, see [Managing Ansible Jobs](#).

Task Results

Result Table

Result Output

TASK [Show execution result] *****

SN: 65FDC8D34181, Status: OK

details:

```
{
  "_ansible_no_log": null,
  "_ansible_verbose_always": true,
  "changed": false,
  "exec_result.stdout_lines": [
    "02:47:11 up 4 days, 23:33, 2 users, load average: 0.11, 0.08, 0.09"
  ]
}
```

PLAY RECAP *****

SN[65FDC8D34181]: OK=2 CHANGED=0 UNREACHABLE=0 FAILED=0

Showing Switch Configurations or Status

To show configurations or status of managed switches, use the **cli_show** mode.

Playbook YAML Example:

```

1 ---
2 - name: Show Version info of all switches
3   hosts: all
4   tasks:
5     - name: Show version of switches
6       picos_config: mode='cli_show' cmd='show version'
7       register: exec_result
8     - name: Show execution result
9       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 command to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-Campus UI.

Result

JSON

STANDARD OUT

```

"admin@PICOS> ",
"Execute command: show version",
"",
"Copyright      : Copyright (C) 2009-2025 Pica8, Inc. All Rights Reserved.",
"Model          : AS5812_54X",
"Software Version : 4.6.0E/9c9dabd021",
"Software Released Date : 04/14/2025",
"Serial Number   : 65FDC8D34181",
"System Uptime    : 4 day 23 hour 38 minute",
"Hardware ID     : License Type      : Uninstalled",
"Device MAC Address : 0c:0e:7d:f4:00:01",
"admin@PICOS> "
}

```

Modifying Switch Configurations

To modify configurations of managed switches, use the **cli_config** mode.

Playbook YAML Example:

```

1  ---
2  - name: Enable Global Config
3    hosts: all
4    tasks:
5
6      - name: Enable Global Config
7        picos_config:
8          mode: 'cli_config'
9          cmd: >
10             set ip routing enable true;
11             set protocols lldp enable true;
12             set system services ssh idle-timeout 60;
13             set system inband enable true;
14             set system timezone "America/Los_Angeles";
15             register: exec_result
16
17      - name: Show execution result
18        debug: var=exec_result.stdout_lines

```

This playbook example runs the following PicOS commands under the **configuration** mode. Replace the commands in the **cmd** section with any other PicOS commands to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-Campus UI.

Result

JSON

STANDARD OUT

```

"admin@PICOS# ",
"Execute command: set protocols lldp enable true.",
"The same value is set to node \"protocols lldp enable\"",
"admin@PICOS# ",
"Execute command: set system services ssh idle-timeout 60.",
"The same value is set to node \"system services ssh idle-timeout\"",
"admin@PICOS# ",
"Execute command: set system inband enable true.",
"The same value is set to node \"system inband enable\"",
"admin@PICOS# ",
"Execute command: set system timezone \"America/Los_Angeles\"",
"The same value is set to node \"system timezone\"",
"admin@PICOS# ",
"Execute command: commit",

```

Loading Configurations in a Configuration File

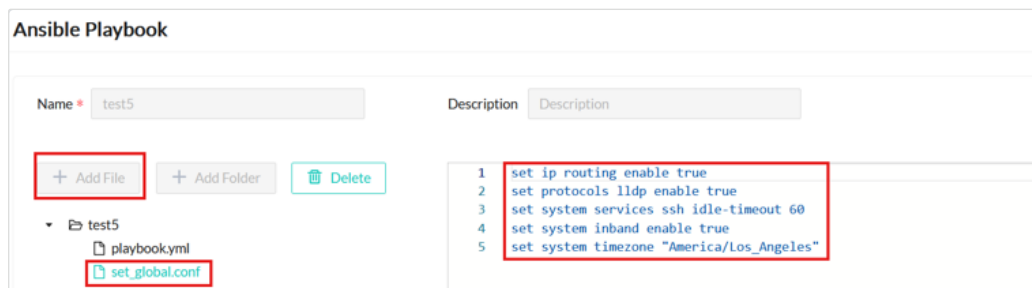
To load configurations from a configuration file into an Ansible playbook, use the **config_load** mode.

Playbook YAML Example:

```
1 ---
2 - name: Deploy services
3   hosts: all
4   tasks:
5     - name: Transfer the script
6       copy: src=set_global.conf dest=/home/admin/setconfig1.conf force=yes
7
8     - name: Activate the configuration
9       picos_config: mode='config_load' cmd='/home/admin/setconfig1.conf'
10      register: exec_result
11
12     - name: Show execution result
13       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 switches, the copied commands will be loaded and then executed on these switches.

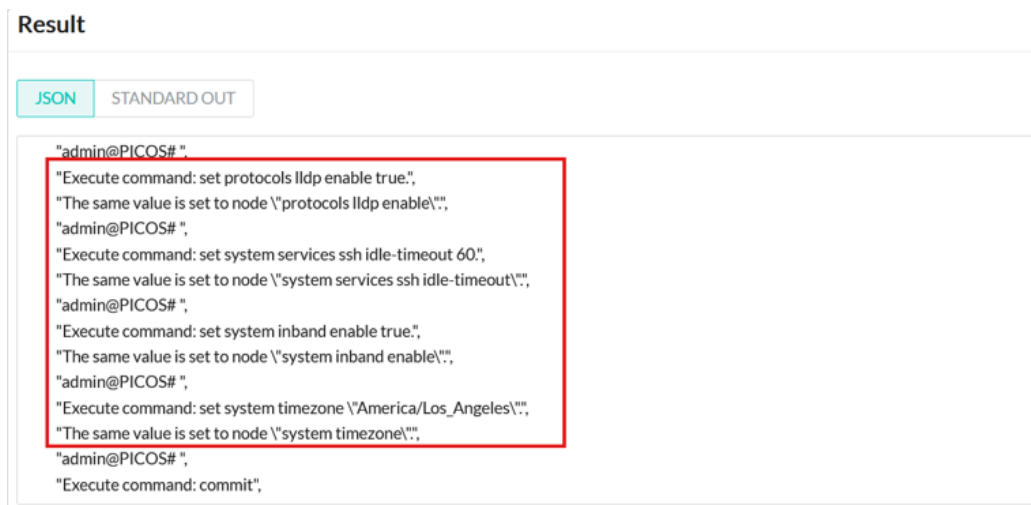
After you write the **playbook.yml** file, ensure to click **Add File** to add the **set_global.conf** file.



The **set_global.conf** file contains the following commands. Replace the commands with any other PicOS commands to meet your needs.

```
1 set ip routing enable true
2 set protocols lldp enable true
3 set system services ssh idle-timeout 60
4 set system inband enable true
5 set system timezone "America/Los_Angeles"
```

After you run this playbook, check the playbook execution result in the AmpCon-Campus UI.



Using Variables in a Playbook

To define variables in an Ansible playbook, use the variable syntax `{{variable_name}}`.

Playbook YAML Example:

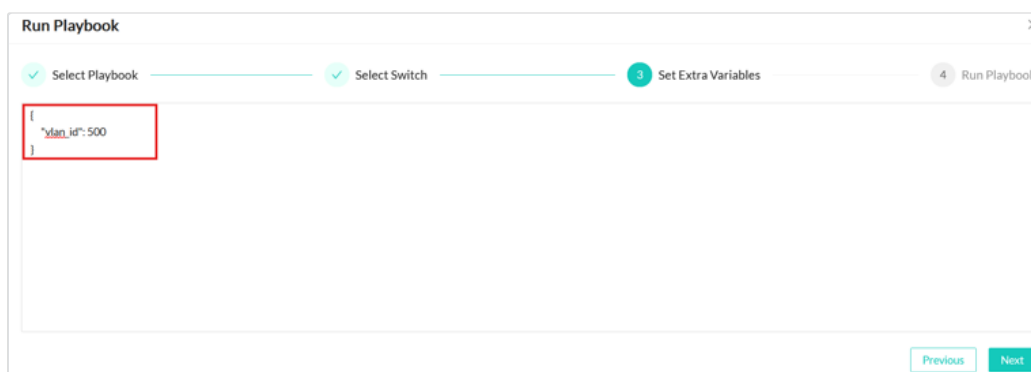
```

1 ---
2 - name: Set Dynamic VLAN
3   hosts: all
4   tasks:
5
6     - name: Set Dynamic VLAN
7       picos_config: mode='cli_config' cmd='set vlans vlan-id {{vlan_id}}
8       register: exec_result
9
10    - name: Show execution result
11      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 6** of [Running a Playbook](#).



After you run this playbook, check the playbook execution result in the AmpCon-Campus UI.

Result

JSON

STANDARD OUT

```

"admin@PICOS> ",
"Execute command: show version",
""
"Copyright      : Copyright (C) 2009-2025 Pica8, Inc. All Rights Reserved.",
"Model          : AS5812_54X",
"Software Version : 4.6.0E/9c9dabd021",
"Software Released Date : 04/14/2025",
"Serial Number   : 65FDC8D34181",
"System Uptime   : 4 day 23 hour 38 minute",
"Hardware ID     : License Type       : Uninstalled",
"Device MAC Address : 0c:0e:7d:f4:00:01",
"admin@PICOS> "
}

```

Real-World Example: Automating VLAN Configurations

As a network administrator, you might feel tedious and time-consuming to configure VLANs on multiple switches manually. By using Ansible playbooks on AmpCon-Campus, you can automate this process.

Playbook YAML Example:

```

1  ---
2  - name: Set VLAN Network
3    hosts: all
4    tasks:
5
6      - name: Set VLAN Network
7        picos_config:
8          mode: 'cli_config'
9          cmd: >
10         set vlans vlan-id 10 l3-interface vlan10;
11         set vlans vlan-id 20 l3-interface vlan20;
12         set vlans vlan-id 30 l3-interface vlan30;
13         set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
14         set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
15         set l3-interface vlan-interface vlan10 address 192.160.10.1 pre
16         set l3-interface vlan-interface vlan20 address 192.160.20.1 pre
17         set l3-interface vlan-interface vlan30 address 192.160.30.1 pre
18         register: exec_result
19
20      - name: Show execution result
21        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.

After you run this playbook, check the playbook execution result in the AmpCon-Campus UI.

Result

JSON STANDARD OUT

```
"Execute command: set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk";
"The same value is set to node \"interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode\"";
"admin@PICOS# ";
"Execute command: set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 10,20,30";
"Node \"10,20,30\" already exists.";
"admin@PICOS# ";
"Execute command: set l3-interface vlan-interface vlan10 address 192.160.10.1 prefix-length 24";
"The same value is set to node \"l3-interface vlan-interface vlan10 address 192.160.10.1 prefix-length\"";
"admin@PICOS# ";
"Execute command: set l3-interface vlan-interface vlan20 address 192.160.20.1 prefix-length 24";
"The same value is set to node \"l3-interface vlan-interface vlan20 address 192.160.20.1 prefix-length\"";
"admin@PICOS# ";
"Execute command: set l3-interface vlan-interface vlan30 address 192.160.30.1 prefix-length 24";
"The same value is set to node \"l3-interface vlan-interface vlan30 address 192.160.30.1 prefix-length\"";
"admin@PICOS# "
```

Related PicOS References

- [Linux Shell Mode, Operation Mode, and Configuration Mode](#)
- [Routing and Switching Command Reference](#)

Running Playbooks

On the “Playbooks” page, you can see the list of playbooks that are created. You can add or import a playbook, check syntax for a playbook, or run a playbook as needed.

In addition, AmpCon-Campus provides multiple playbook management functions including copying playbooks, using pre-built playbooks, editing, deleting, copying, or exporting playbooks, and adding tags to playbooks.

NOTE

Before you use 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 should be written to be idempotent, meaning running the playbook multiple times won’t cause unintended changes.
- **Backups:** Before applying any configuration, ensure that you have backups of the current configurations. For more information, see [Backing Up and Restoring Configurations](#).

Prerequisites

Procedure

[Writing a Playbook on AmpCon-Campus](#)

[Importing a Playbook](#)

[Running a Playbook](#)

Optional Operations

[Checking Syntax for a Playbook](#)

[Using Pre-built Playbooks](#)

[Editing a Playbook](#)

[Deleting a Playbook](#)

[Copying a Playbook](#)

[Exporting a Playbook](#)

[Adding or removing Tags to a Playbook](#)

Prerequisites

Before you run Ansible playbooks for automation, ensure that the following prerequisite tasks have been completed:

Table 1. Prerequisite Tasks and Links

Task	Reference Link
------	----------------

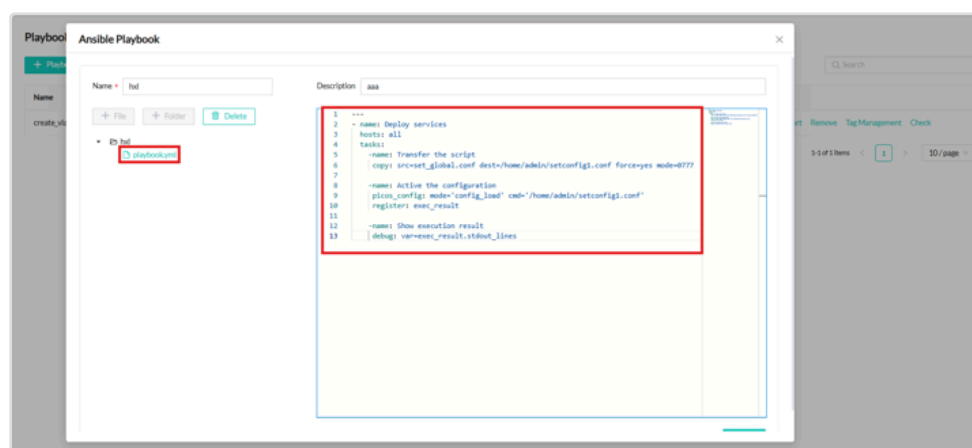
Ensure that each PicOS switch to run Ansible playbooks has been onboarded to AmpCon-Campus.	• PicOS Switch Onboarding Workflow
Ensure that the PicOS switches are up and connected to the AmpCon-Campus server.	• Viewing the PicOS List

Procedure

Writing a Playbook on AmpCon-Campus

If you don't have an available Ansible playbook, you can write an Ansible playbook on AmpCon-Campus. Follow these steps:

1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the "Playbooks" page, click **+ Playbook**.
3. Enter the playbook name and description (optional). Click **playbook.yml**, and add contents to the .yml file.



4. Optional: To add files or folders to the playbook, click the playbook name (click **hxl** in the following screenshot), and then click **+ File** or **+ Folder**.

For example, to load configurations from a configuration file to the playbook, click **+ File** to add a **.conf** file. For more information, see [Loading Configurations in a Configuration File](#).

5. Click **Apply**.

Importing a Playbook

If you have an available Ansible playbook, you can import the Ansible playbook to AmpCon-Campus. Follow these steps:

1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the “Playbooks” page, click **Import**.
3. Enter the playbook name and description (optional), and upload the playbook .zip file.

NOTE

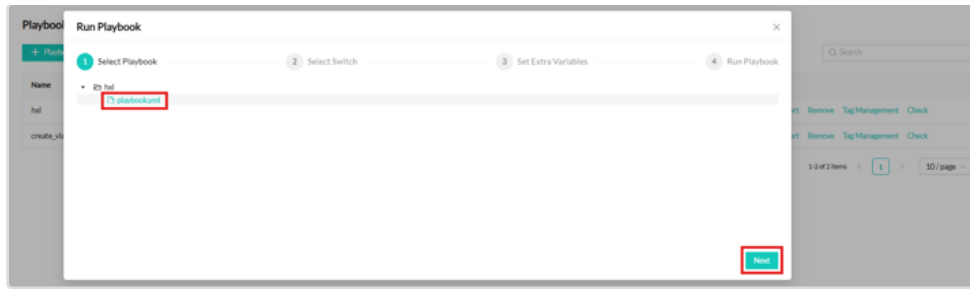
The playbook **.zip** file needs to contain a playbook **.yml** file and a configuration **.conf** file (optional).

4. Click **Apply**.

Running a Playbook

After you write or import the Ansible playbook, run the playbook in the AmpCon-Campus UI. Follow these steps:

1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the “Playbooks” page, locate a playbook, and then click **Run**.
3. Select the playbook.yml file, and then click **Next**.



4. Select target switches to run the playbook by using the following ways:

NOTE

If you select switches, groups, and other devices in the **Choose Switches**, **Choose Groups**, and **Choose Other Devices** tabs, the playbook will be run on all selected targets.

- Choose switches

In the **Choose Switches** tab, select one or multiple switches.

- Choose groups

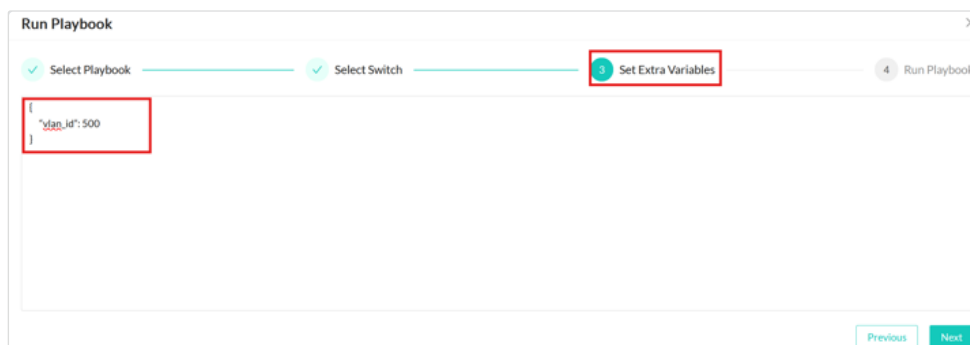
In the **Choose Groups** tab, select one or multiple groups.

- Choose other devices

In the **Choose Other Devices** tab, select one or multiple devices that you added in [Adding Other Devices](#).

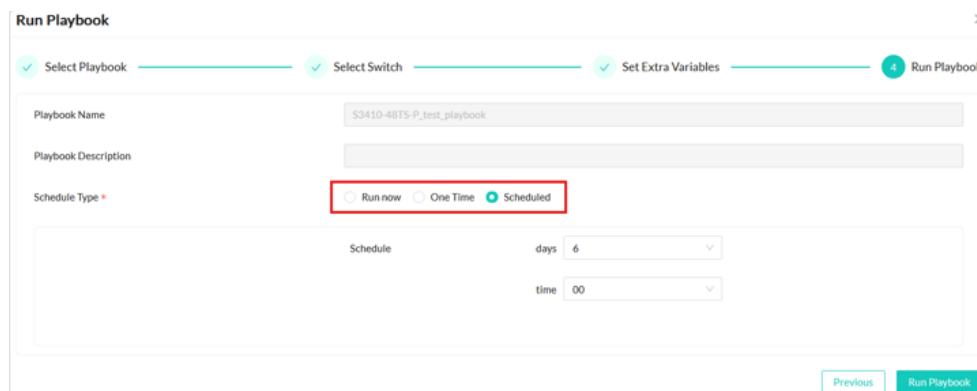
5. Click **Next**.

6. If variables are specified in the playbook, enter variable values in JSON format, and then click **Next**.



7. Select the schedule type to run the playbook.

- **Run Now:** Executes the task immediately upon creation
- **One Time:** Executes the task within the selected time range after creation
- **Scheduled:** Executes the task periodically after creation



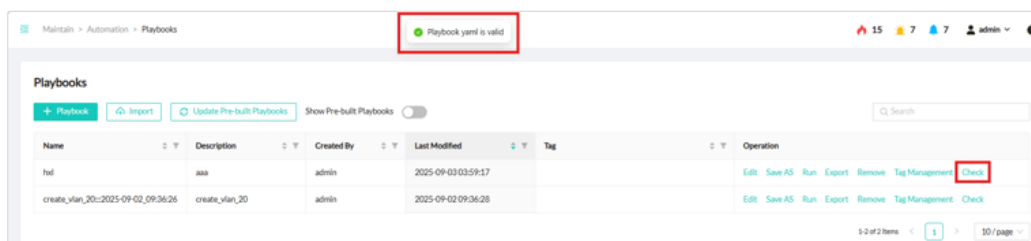
The "Run Playbook" dialog box shows a progress bar with four steps: "Select Playbook", "Select Switch", "Set Extra Variables", and "Run Playbook" (the current step, indicated by a blue circle with the number 4). Below the progress bar, there are input fields for "Playbook Name" (containing "S3410-48TS-P_test_playbook") and "Playbook Description". Under "Schedule Type", three radio buttons are present: "Run now", "One Time", and "Scheduled" (which is selected and highlighted with a red box). Below these, there are dropdown menus for "Schedule" (set to "days"), "days" (set to "6"), and "time" (set to "00"). At the bottom right, there are "Previous" and "Run Playbook" buttons.

8. Click **Run Playbook**.

Optional Operations

Checking Syntax for a Playbook

On the “Playbooks” page, locate a playbook, and then click **Check**. A message pops up with the checking result.



The "Playbooks" page shows a notification at the top: "Playbook yaml is valid" (highlighted with a red box). Below the notification, there are buttons for "+ Playbook", "Import", and "Update Pre-built Playbooks". A toggle switch for "Show Pre-built Playbooks" is turned off. A table lists playbooks with columns: Name, Description, Created By, Last Modified, Tag, and Operation. The "Operation" column for the first two playbooks includes a "Check" button (highlighted with a red box). The first playbook is "hsl" with description "asa", created by "admin", and last modified "2025-09-03 03:59:17". The second is "create_vlan_20" with description "create_vlan_20", created by "admin", and last modified "2025-09-02 09:36:26".

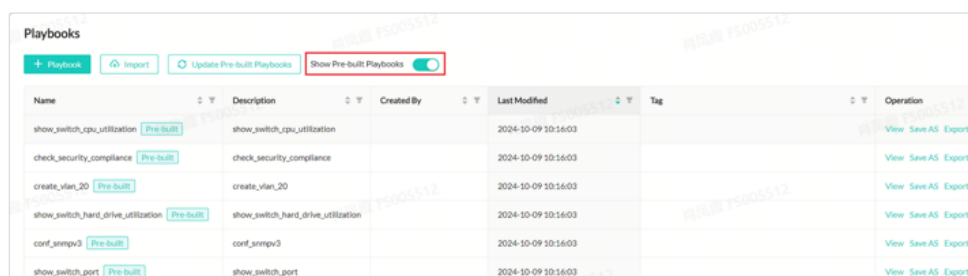
Using Pre-built Playbooks

AmpCon-Campus provides multiple pre-built playbooks, which are hidden by default.

NOTE

Pre-built playbooks can’t be run directly. You need to click **Save As** to copy a pre-built playbook as a new playbook and then run the new playbook. You can’t edit or remove pre-built playbooks. And you can’t add tags or check syntax for pre-built playbooks.

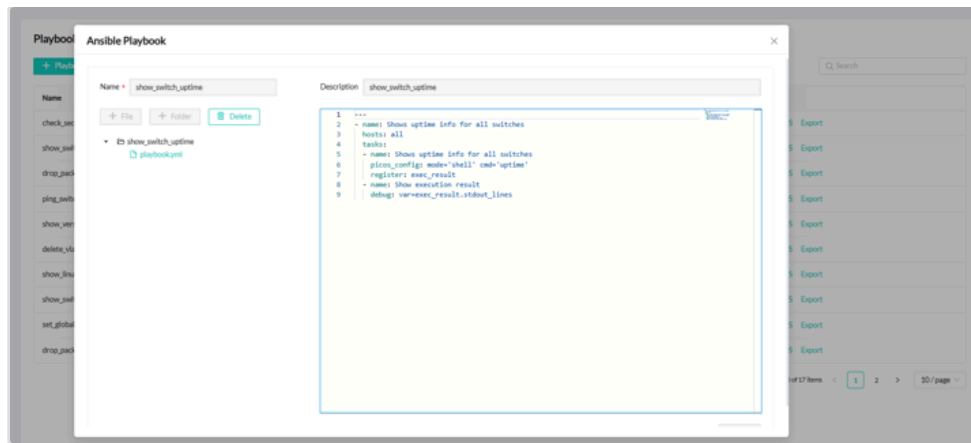
- To show the pre-built playbooks, click the **Show Pre-built Playbooks** toggle on the “Playbooks” page.



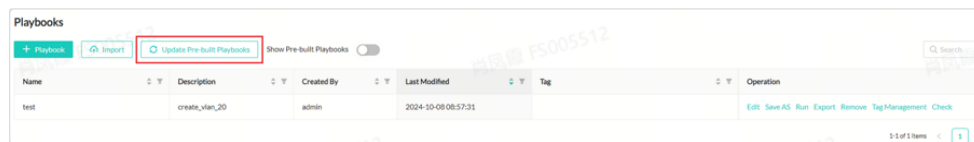
The "Playbooks" page now shows the "Show Pre-built Playbooks" toggle turned on (highlighted with a red box). The table lists several pre-built playbooks, each with a "Pre-built" label in a blue box. The playbooks are:

Name	Description	Created By	Last Modified	Tag	Operation
show_switch_cpu_utilization	show_switch_cpu_utilization		2024-10-09 10:16:03		View Save AS Export
check_security_compliance	check_security_compliance		2024-10-09 10:16:03		View Save AS Export
create_vlan_20	create_vlan_20		2024-10-09 10:16:03		View Save AS Export
show_switch_hard_drive_utilization	show_switch_hard_drive_utilization		2024-10-09 10:16:03		View Save AS Export
conf_snmpv3	conf_snmpv3		2024-10-09 10:16:03		View Save AS Export
show_switch_port	show_switch_port		2024-10-09 10:16:03		View Save AS Export

- To view a pre-built playbook, locate the playbook, and then click **View**.



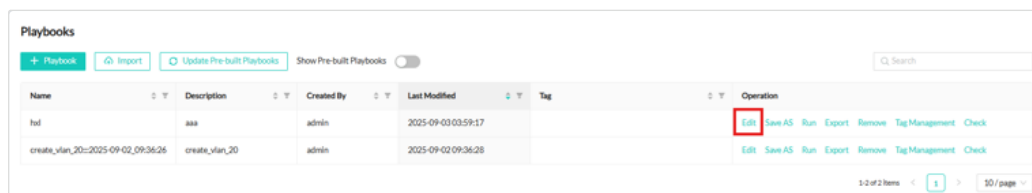
- To refresh the pre-built playbook list, click **Update Pre-built Playbooks**.



- To export a pre-built playbook, locate the playbook, and then click **Export**.

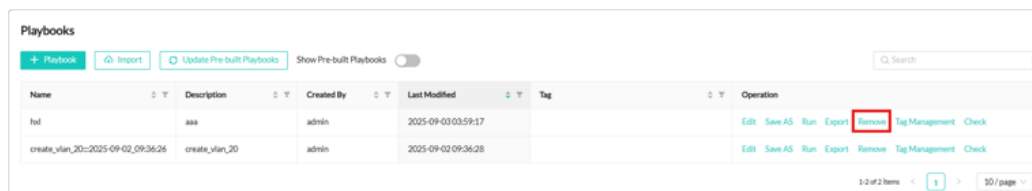
Editing a Playbook

On the “Playbooks” page, locate a playbook, and then click **Edit**. Modify the playbook contents as needed. You can also add or remove folders and files. Then, click **Save All**.



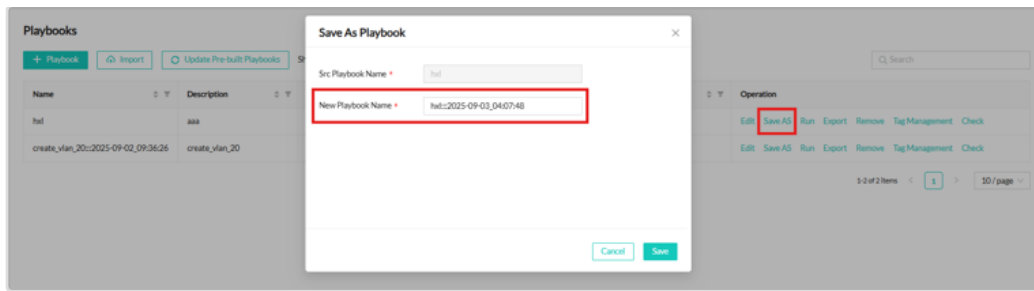
Deleting a Playbook

On the “Playbooks” page, locate a playbook, and then click **Remove**. Then, click **Yes** to confirm the deletion.



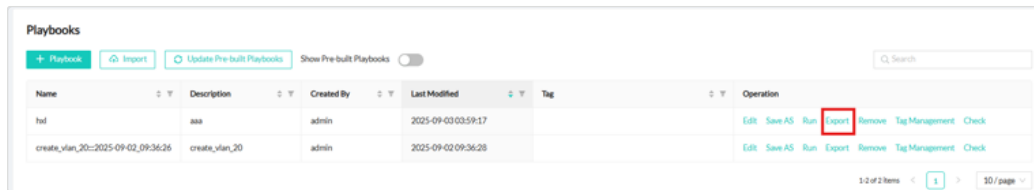
Copying a Playbook

On the “Playbooks” page, locate a playbook, and then click **Save As**. The new playbook has a default name, which you can modify as needed. Then, click **Save**.



Exporting a Playbook

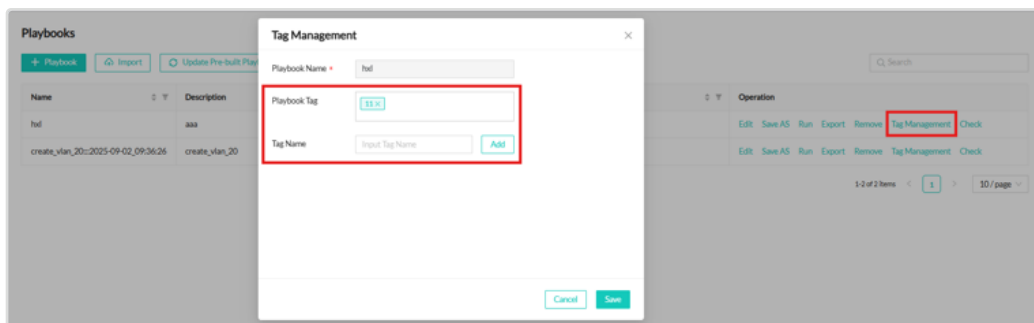
On the “Playbooks” page, locate a playbook, and then click **Export**.



Adding or removing Tags to a Playbook

On the “Playbooks” page, locate a playbook, and then click **Tag Management**. Enter the tag name in the **Tag Name** field, and then click **Add**.

You can remove a tag by clicking the removal icon.



Adding Other Devices

In addition to running Ansible playbooks on managed switches, you can add third-party Linux server devices and then run Ansible playbooks on these added devices.

This feature supports only Linux servers currently.

[Adding a Linux Server](#)

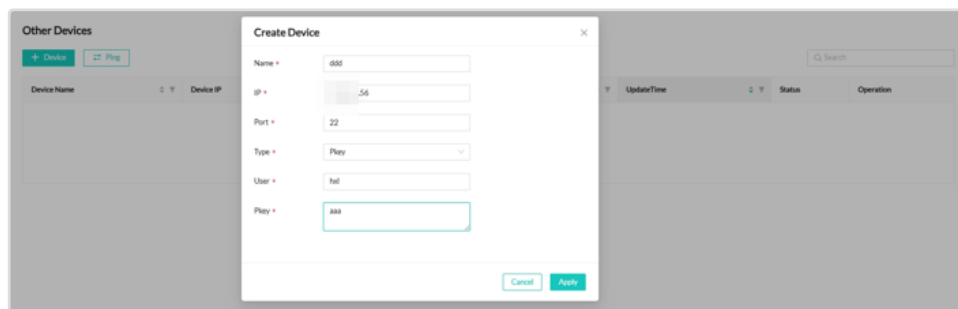
[Deleting a Linux Server](#)

[Testing Device Connectivity](#)

[Running Playbooks on Linux Servers](#)

Adding a Linux Server

1. Click **Maintain > Automation > Other Devices** in the AmpCon-Campus UI.
2. Click **+ Device**.
3. Enter the following information:
 - **Name:** The name of the Linux server.
 - **IP:** The IP address of the Linux server.
 - **Type:** Select **Password** or **Pkey**.
 - **User:** The name of the user to log in to the Linux server.
 - **Password:** The password of the user to log in to the Linux server. This field can be seen only if you selected **Password** in the **Type** drop-down list.
 - **Pkey:** The public key to log in to the Linux server. This field can be seen only if you selected **Pkey** in the **Type** drop-down list.
 - **SudoPassword:** The password of the administrator user used by AmpCon-Campus to install a monitoring tool for device monitoring. This field can be seen only if you selected **Pkey** in the **Type** drop-down list.



4. Click **Apply**.

Deleting a Linux Server

1. Click **Maintain > Automation > Other Devices** in the AmpCon-Campus UI.
2. Locate a Linux server, and then click **Delete**.

Other Devices

[+ Device](#) [Ping](#)

Q Search

Device Name	Device IP	Device User	CreateTime	UpdateTime	Status	Operation
ddd	56	hnl	2025-09-03 03:45:29	2025-09-03 03:45:29	---	Delete

1 of 1 items [1](#) 10 / page

3. Click **Yes** to confirm the deletion.

Testing Device Connectivity

To check whether the added Linux servers can connect with AmpCon-Campus or not, click **Ping**. Then, you can see the connectivity status in the **Status** column.

Other Devices

[+ Device](#) [Ping](#)

Q Search

Device Name	Device IP	Device User	CreateTime	UpdateTime	Status	Operation
ddd	10.56.54.56	hnl	2025-09-03 03:45:29	2025-09-03 03:45:29	---	Delete

1 of 1 items [1](#) 10 / page

Running Playbooks on Linux Servers

To run an Ansible playbook on Linux servers that you added, follow the steps:

1. Write a playbook based on playbook syntax described in [Using Ansible playbooks](#).
2. Add the playbook to AmpCon-Campus by writing or importing the playbook in the AmpCon-Campus UI, and then run the playbook.

For more information, see [Running Playbooks](#).

3. Check the playbook execution result in the AmpCon-Campus UI. For more information, see [Managing Ansible Jobs](#).

Managing Ansible Jobs

An Ansible job is a single execution of an Ansible playbook. On the “Ansible Jobs” page, you can view the list of Ansible jobs and the list of switches with Ansible jobs. You can also check the execution results and output of these jobs.

Job View

[Viewing Ansible Jobs](#)

[Checking Ansible Job Results and Output](#)

[Removing an Ansible Job](#)

Switch View

[Viewing Switches with Ansible Jobs](#)

[Checking Ansible Job Results and Output](#)

Job View

Viewing Ansible Jobs

Click **Maintain > Automation > Ansible Jobs** in the AmpCon-Campus UI. In the **Job View** tab, you can see the list of playbook execution jobs.

Job View

Switch View

Q Search

Job Name	Playbook Name	Schedule Type	Job Creation Time	Create By(user)	Status	Operation
2025-01-10 02:29:33--S3410-48TS-P_test_playbook	S3410-48TS-P_test_playbook	DIRECT	2025-01-10 02:29:33	admin	EXECUTED	Task Results Remove
2025-01-09 06:42:33--S3410-48TS-P_test_playbook	S3410-48TS-P_test_playbook	DIRECT	2025-01-09 06:42:33	admin	EXECUTED	Task Results Remove
2025-01-09 06:08:20--copy_test	copy_test	DIRECT	2025-01-09 06:08:20	admin	EXECUTED	Task Results Remove

The **Schedule Type** column including the following types:

- **DIRECT**

Playbooks are executed with "Run Now".

- **ONCE**

Playbooks are executed with "One Time".

- **SCHEDULED**

Playbooks are executed with "Scheduled".

The **Status** column includes the following status:

- **IDLE**

The playbook has not been executed. For example, after a playbook is created and before it's executed, the status is IDLE.

NOTE

For playbooks with the schedule type of "SCHEDULED", the status is changed to **IDLE** after the playbook execution is completed.

• RUNNING

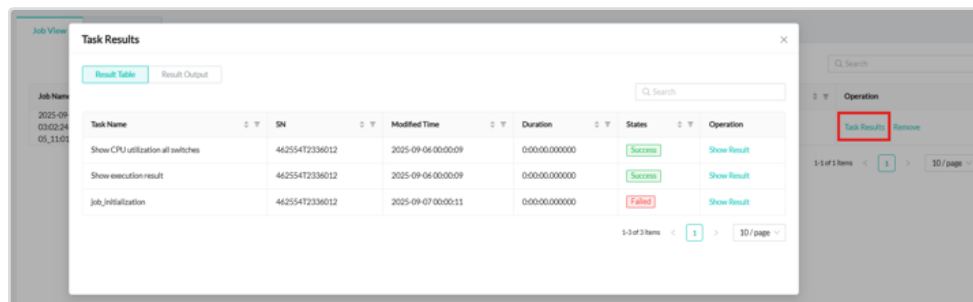
The playbook is currently running.

• EXECUTED

The playbook execution has been completed.

Checking Ansible Job Results and Output

1. In the **Job View** tab, locate a job, and then click **Task Results**. You can see the playbook execution result in the **Result Table** tab.

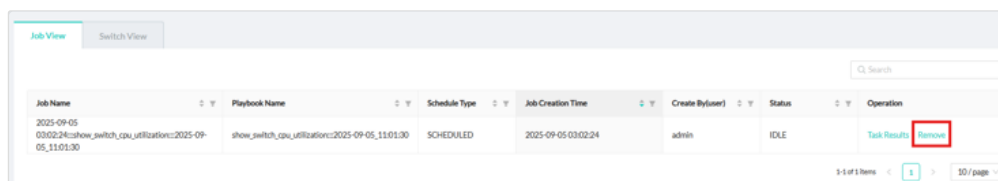


2. To view detailed result information, click **Show Result**.
3. To view the output of the playbook execution, click the **Result Output** tab.



Removing an Ansible Job

1. In the **Job View** tab, locate a job, and then click **Remove**.
2. Click **Yes** to confirm the deletion.



Switch View

Viewing Switches with Ansible Jobs

In the **Switch View** tab, you can see the list of switches that have playbook execution jobs.

Job View

Switch View

Q Search

SN	VPN IP	Model	Version	Status	Operation
462554P2336008	10.8.0.22	AS4625-54P	4.7.0E	Provisioning Success	Task Results
462554T2336012	10.8.0.6	AS4625-54T	4.7.0E	Provisioning Success	Task Results
G19A016000514	10.8.0.26	S5860-205Q	4.7.0E-EC1	Provisioning Success	Task Results

1 of 3 items

1

10 / page

1 of 3 items < 1 > 10 / page

Checking Ansible Job Results and Output

1. In the **Switch View** tab, locate a switch, and then click **Task Results**.

Job View

Switch

Task Results

Result Table

Result Output

Q Search

Job Name	Task Name	Modified Time	Duration	State	Operation
2024-10-14 06:47:06::test	job_initialization	2024-10-14 06:47:30	0:00:00.000000	Failed	Show Result

1-1 of 1 items < 1 > 10/page

1 of 1 items < 1 > 10 / page

2. To view detailed result information, click **Show Result**.
3. To view the output of the playbook execution, click the **Result Output** tab.

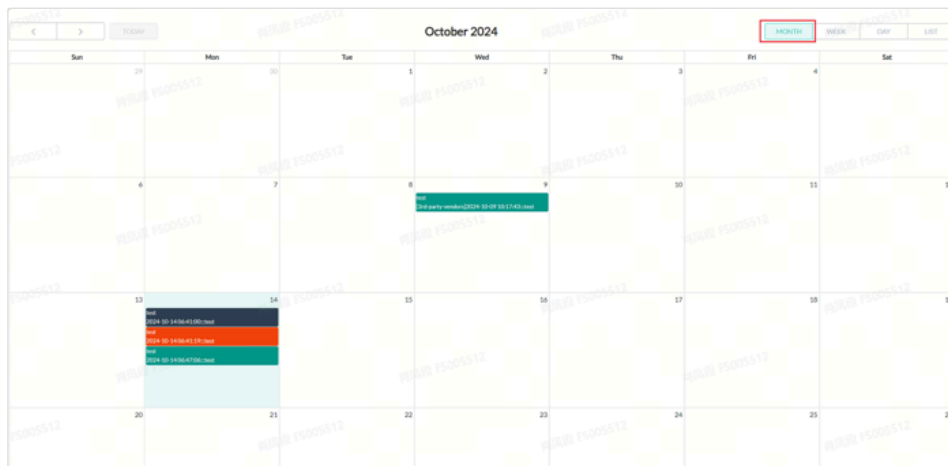
Viewing Playbook Scheduling

On the “Scheduler” page, you can view executed playbooks based on months, weeks, or days. You can also view executed playbooks in the list format.

Procedure

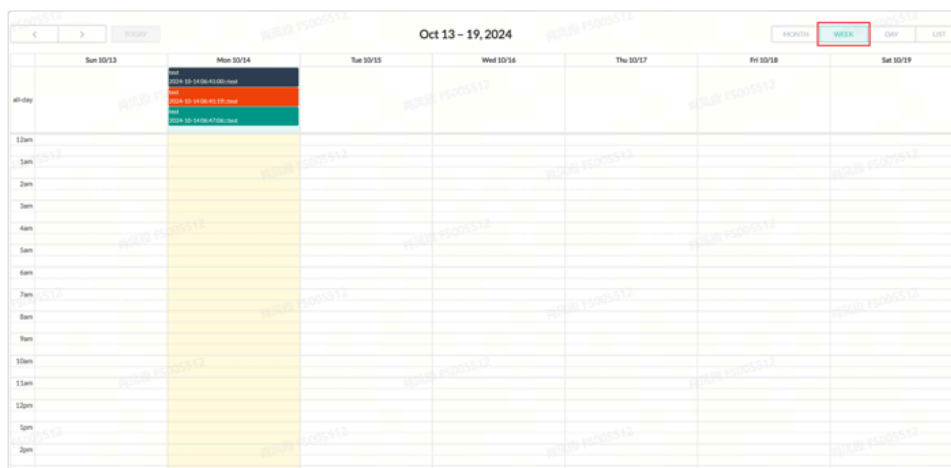
1. Click **Maintain > Automation > Scheduler** from the navigation bar.
2. On the “Scheduler” page, view executed playbooks by using the following ways:
 - To view executed playbooks each month, click **MONTH**.

Click < to view playbooks executed in the previous month. Click > to view playbooks executed in the next month.



- To view executed playbooks each week, click **WEEK**.

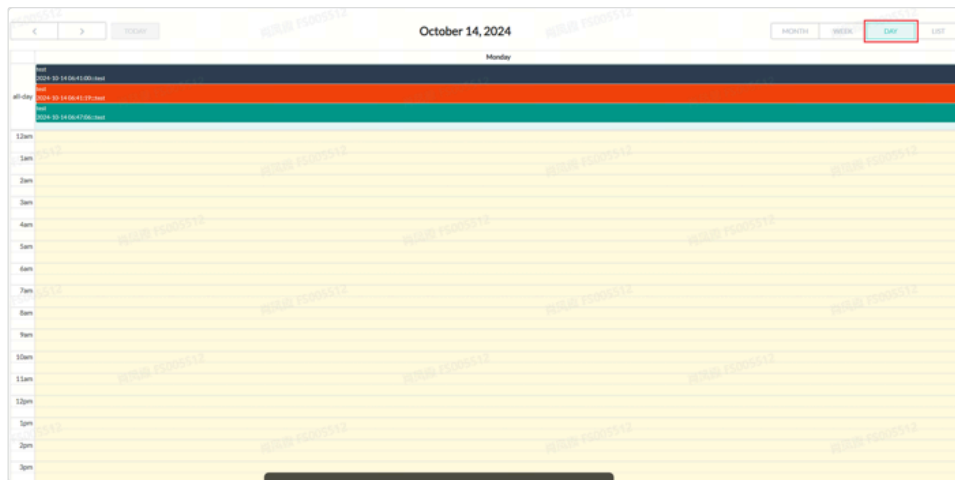
Click < to view playbooks executed in the previous week. Click > to view playbooks executed in the next week.



- To view executed playbooks each day, click **DAY**.

Click < to view playbooks executed on the previous day. Click > to view playbooks executed on the next day.

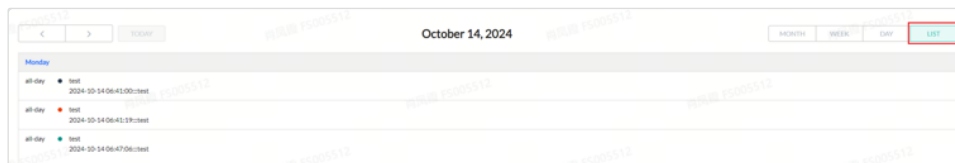
Click **Today** to view playbooks executed today.



- To view executed playbooks in the list format, click **LIST**.

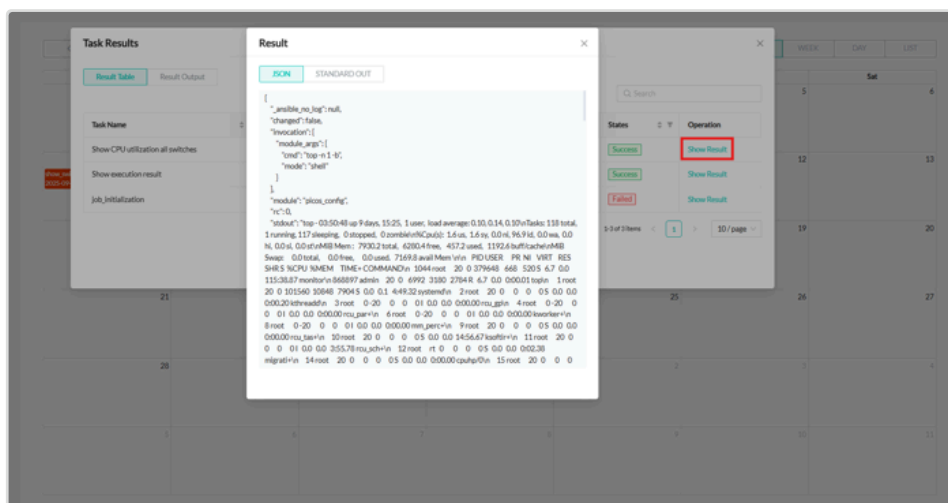
Click **<** to view playbooks executed on the previous day. Click **>** to view playbooks executed on the next day.

Click **Today** to view playbooks executed today.



3. Optional: Click a playbook, and then you can see the playbook execution result and output.

In the **Result Table** tab, you can see the playbook execution result. To view detailed result information, click **Show Result**.



In the **Result Output** tab, you can see the playbook execution output.

Task Results

Result Table

Result Output

Run Time: 2025-09-07 00:00:10

Job Name: 2025-09-05 03:02:24:show_switch_cpu_utilization:2025-09-05_11:01:30

Task Name: job_initialization

Task Status: Failed

SN: 46255472336012

Task Result:

[

"changed": false,

"msg": "Failed to connect to the host via ssh: ssh: connect to host 10.8.0.6 port 22: Connection timed out",

"unreachable": true

]

Run Time: 2025-09-06 00:00:09

Job Name: 2025-09-05 03:02:24:show_switch_cpu_utilization:2025-09-05_11:01:30

Task Name: Show CPU utilization all switches

Task Status: Success

SN: 46255472336012

Task Result:

[

"_ansible_no_log": null,

"changed": false,

]

WEEK

DAY

LIST

Sat

5

6

12

13

19

20

26

27

3

4

5

6

7

8

9

10

11

Troubleshooting

If a playbook fails to be run on switches or Linux servers, refer to the following reasons and solutions:

Playbook Syntax Issues

Symptom

Solutions

Connection Issues

Symptom

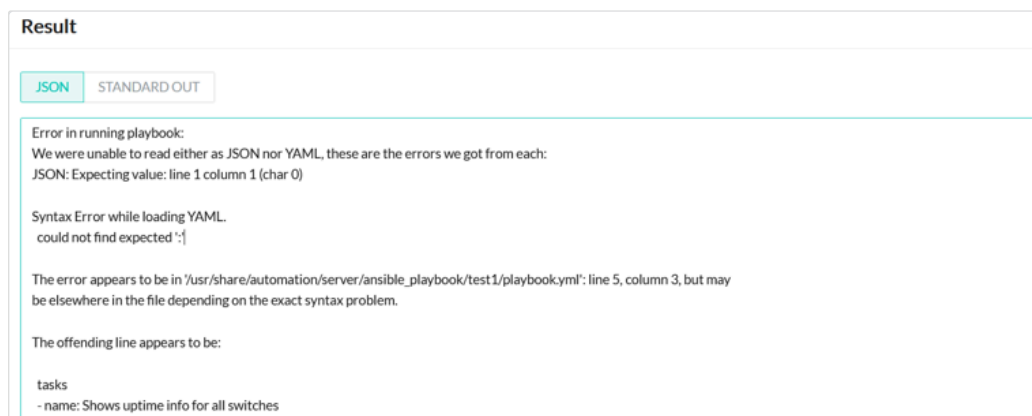
Solutions

Playbook Syntax Issues

If the playbook syntax is wrong, the playbook can't be run on specified devices.

Symptom

When you check the playbook execution result in the AmpCon-Campus UI, you can see the error log as follows:



Solutions

- For playbooks run on switches, check as follows:
 - 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 designated, check whether you have set the variable values in JSON format as described in **Step 6** of [Running a Playbook](#).
 - When you run a playbook with a configuration file (**.conf**) specified, check whether you have clicked **Add File** to add the configuration file.
- For playbooks run on added Linux servers, check whether you follow the playbook syntax as described in [Using Ansible playbooks](#).

Connection Issues

If the AmpCon-Campus server fails to access the switches or added Linux servers, the playbook can't be run on these devices.

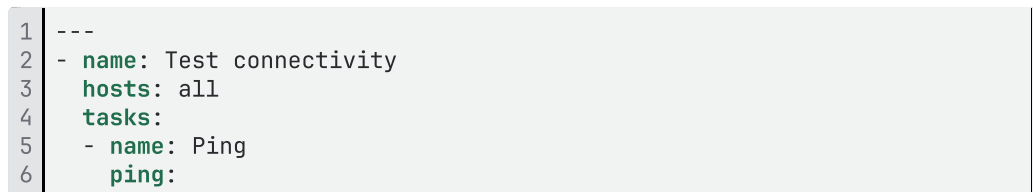
Symptom

When checking the playbook execution result in the AmpCon-Campus UI, you can see the error log as follows:



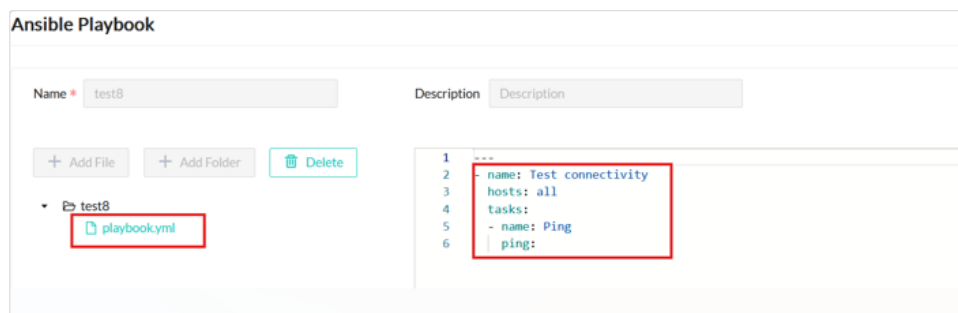
Solutions

Test the connectivity between the problematic switches (or Linux servers) and the AmpCon-Campus server by running the following Ansible playbook:

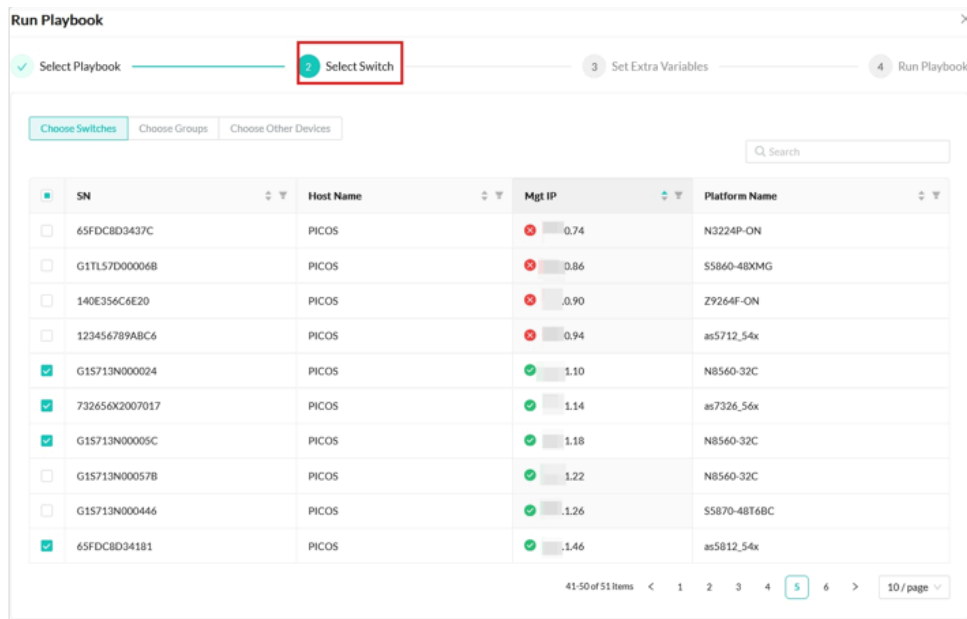


You can write and run the playbook in the AmpCon-Campus UI. Follow these steps:

1. Write a playbook.

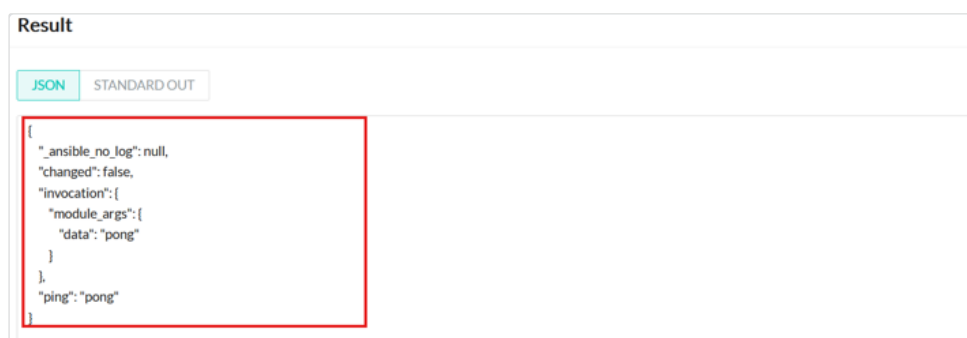


2. Run the playbook on problematic switches or Linux servers.

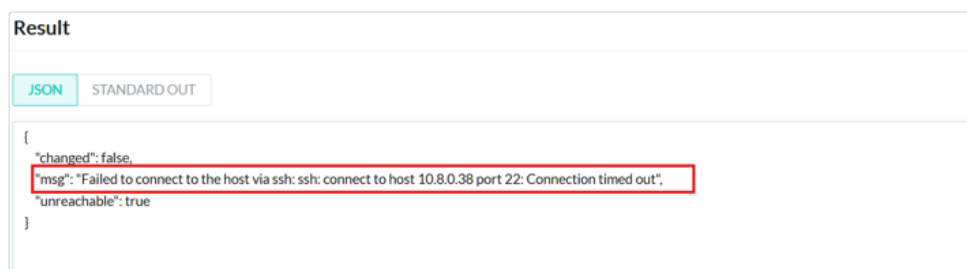


3. Check the playbook execution result in the AmpCon-Campus UI to see whether the AmpCon-Campus server can access the problematic switches or Linux servers.

- If the AmpCon-Campus server can access the problematic switches or Linux servers, the result is as follows:



- If the AmpCon-Campus server can't access the problematic switches or Linux servers, the result is as follows:



In this case, check whether the prerequisites for running playbooks are met. For more information, see [Running Playbooks - Prerequisites](#).

Monitoring and Alerting

After you onboard PicOS switches to AmpCon-Campus, you can view real-time and historical metrics of the managed switches. In addition, you can check alerts in the AmpCon-Campus UI or use the alert notification feature to receive real-time email notifications.

See the following child topics:

- [System Overview](#)
- [Switch Overview](#)
- [Terminals](#)
- [Telemetry](#)
- [Topology](#)
- [Alerts](#)

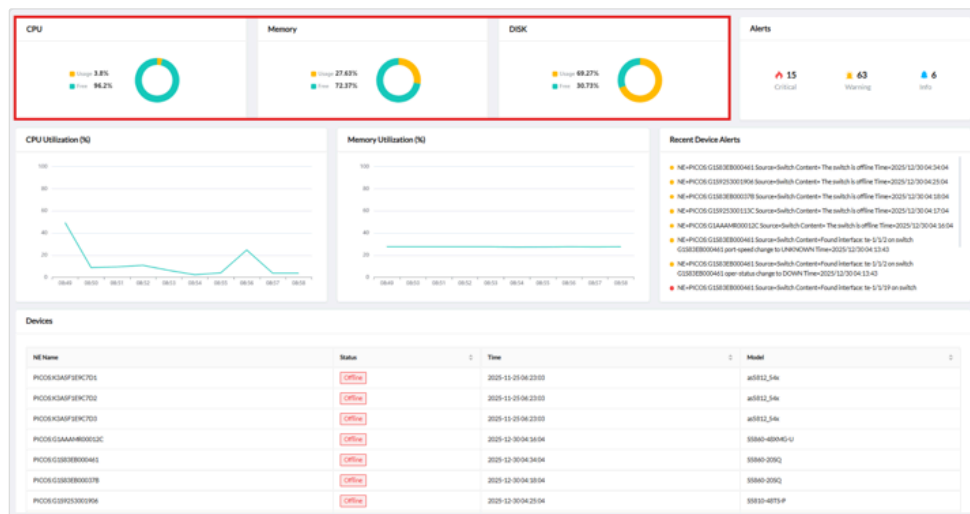
NOTE

The child topics are applicable to only PicOS switches.

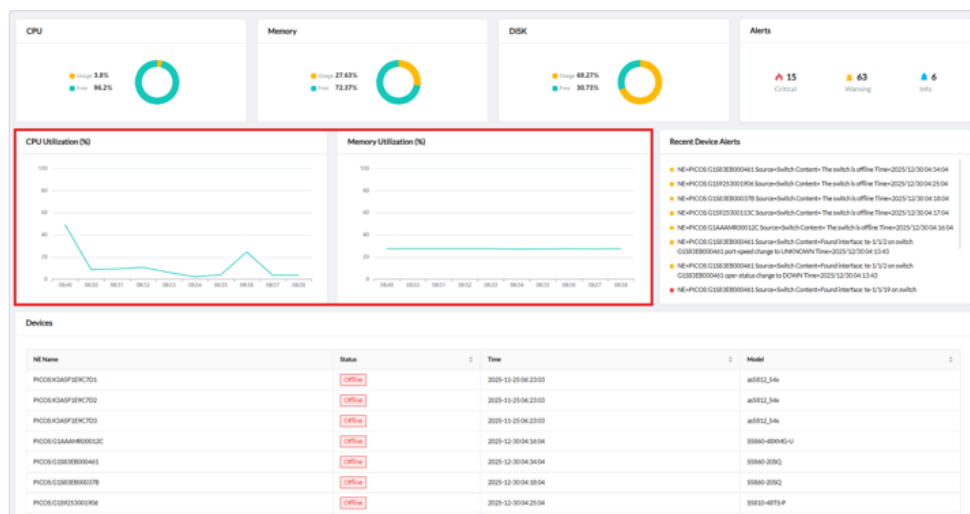
System Overview

In the AmpCon-Campus UI, click **Dashboard > System Overview**. On the “System Overview” page, you can check managed switches and the health of the AmpCon-Campus server.

- In the **CPU**, **MEM**, and **DISK** sections, you can see the status of the AmpCon-Campus server, including CPU, memory, and hard disk.



- In the **CPU Utilization** and **Memory Utilization** sections, you can see the historical utilization curves for CPU and memory in the AmpCon-Campus server.

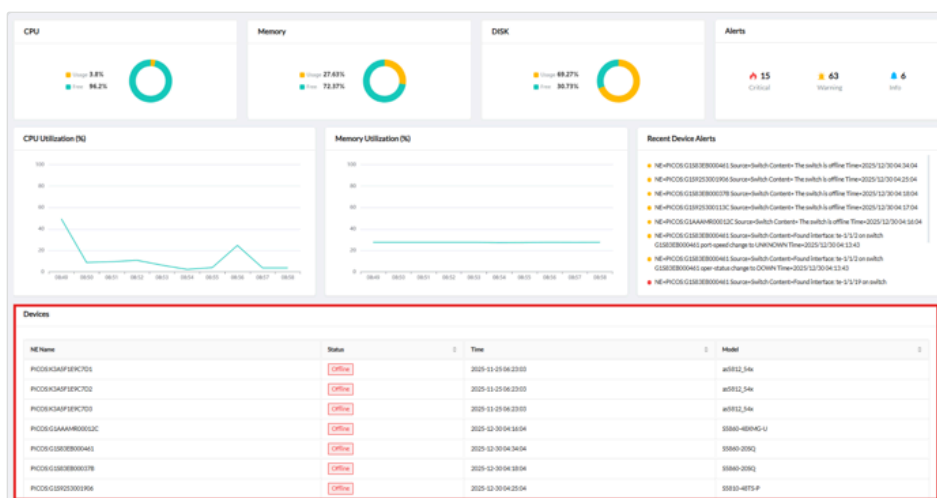


- In the **Devices** section, you can see information about managed switches.

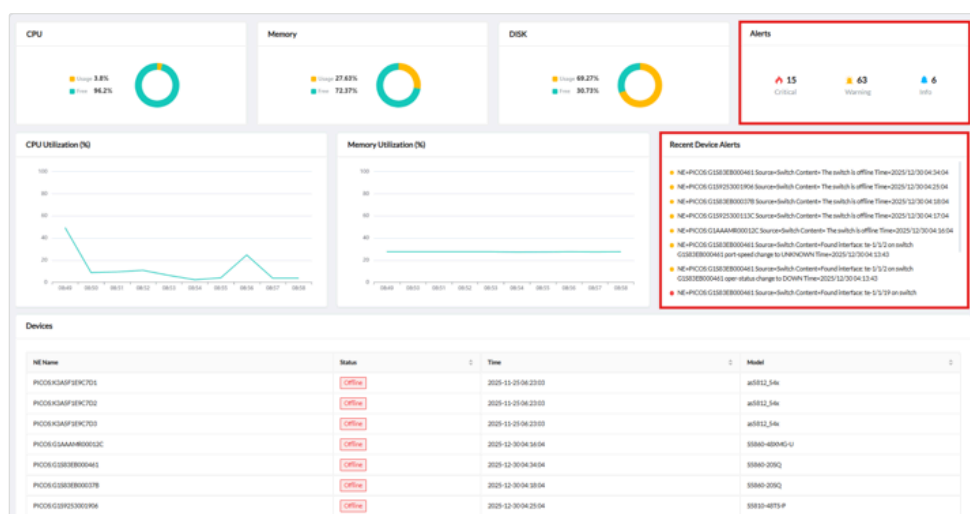
Table 1. Switch Metrics

Metric	Description
NE Name	The combination of the switch’s hostname and the SN/Service Tag.

	Example: If a switch's hostname is PICOS and the SN/Service Tag is G1S713E00021C, then the NE name is PICOS:G1S713E00021C.
Status	The status of the switch. • The Online status means that the switch can connect with the AmpCon-Campus server. • The Offline status means that the switch can't connect with the AmpCon-Campus server.
Time	The time of the most recent change of the Status value.
Model	The model of the switch.



- In the **Alerts** and **Recent Device Alerts** sections, you can see recent switch alerts and the numbers for different types of switch alerts.



Switch Overview

In the AmpCon-Campus UI, click **Dashboard > Switch Overview**. On the “Switch Overview” page, check the following information for managed switches:

[Checking Configurations or Templates](#)

[Checking Switches](#)

[Checking Lifecycle Workflow](#)

[Checking the Proportions of Switches in Each Lifecycle State](#)

[Checking Switch Models](#)

[Checking Licenses](#)

[Checking Available License Numbers](#)

[Checking License Expiration Dates](#)

[Checking License Usage](#)

[Checking Tasks](#)

[Checking All Switch Activities](#)

[Checking System Tasks](#)

[Checking Automation Jobs](#)

Checking Configurations or Templates

In the **Config/Templates** section, you can see the total numbers for different types of switch configurations and templates.



Click the number for one specific type. You are redirected to the related page in the **Service** menu:

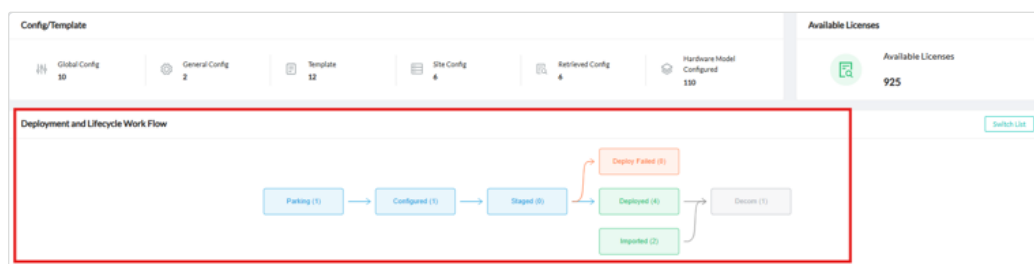
- Click **Global Config** to go to the **Global Configuration** tab of the “Device Profiles” page.
- Click **Site Config** to go to the **Switch Configuration** tab of the “Device Profiles” page.
- Click **General Config** to go to the **Push Config** section of the “Config Templates” page.
- Click **Retrieved Config** to go to the **Config Backup** section of the “Config Templates” page.
- Click **Template** to go to the **Template List** of the “Config Templates” page.
- Click **Hardware Model Configured** to go to the **Switch Model** tab of the “Device Profiles” page.

Checking Switches

Checking Lifecycle Workflow

In the **Deployment and Lifecycle Work Flow** section, you can see the lifecycle transition process of switches and the total number of each state. See the explanation of each state:

- **Parking:** If you provision a switch without adding a switch configuration beforehand, the switch is in **Parking** status.
- **Configured:** After you add a switch configuration, the switch is in **Configured** status.
- **Staged:** After you stage a switch, the switch is in **Staged** status.
- **Deploy Failed:** The switch fails to be deployed by using AmpCon-Campus.
- **Deployed:** The switch is deployed by using AmpCon-Campus.
- **Imported:** The switch is imported to AmpCon-Campus.
- **DECOM:** The deployed switch is decommissioned (DECOM) when it's online.



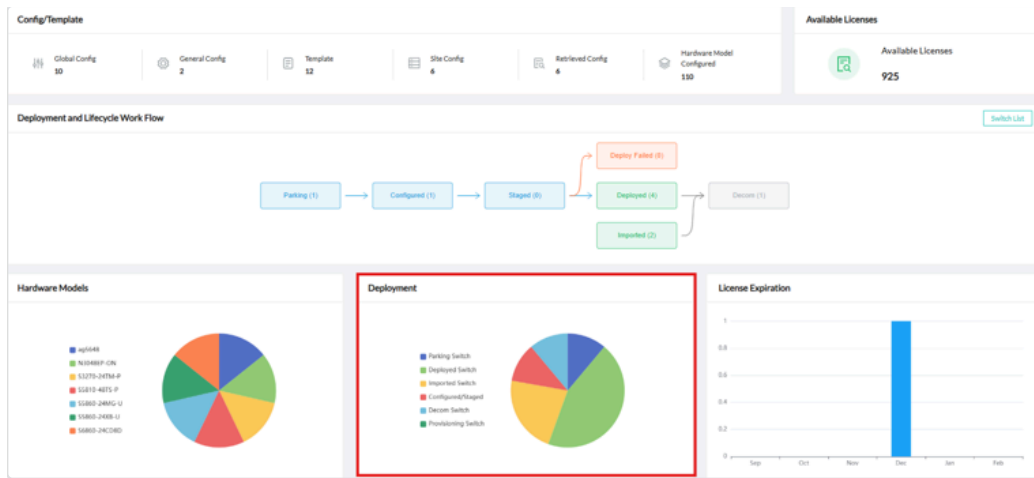
Click **Switch List**. You can check all managed switches on the “Switches” page.

Synname	SN/Service Tag	Model	Version	Status	VPN IP	Mgmt IP	Operation
PICOS	65FDC8D34180	as5812_54x	4.6.0E	Imported	10.0.18		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	65FDC8D34181	as5812_54x	4.6.0E	Imported	10.0.10		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	65FDC8D34185	as5812_54x	4.6.0E	Imported	10.0.14		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A95D2	as5812_54x	4.6.0E	Imported	10.0.50		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A9129	as5812_54x	4.6.0E	Imported	10.0.46		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A9131	as5812_54x	4.6.0E	Imported	10.0.34		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A9130	as5812_54x	4.6.0E	Imported	10.0.30		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A9132	as5812_54x	4.6.0E	Imported	10.0.38		UnStage SSH Device Log Configuration Config View Lifecycle Actions
PICOS	E6C94A3A9133	as5812_54x	4.6.0E	Imported	10.0.42		UnStage SSH Device Log Configuration Config View Lifecycle Actions

Checking the Proportions of Switches in Each Lifecycle State

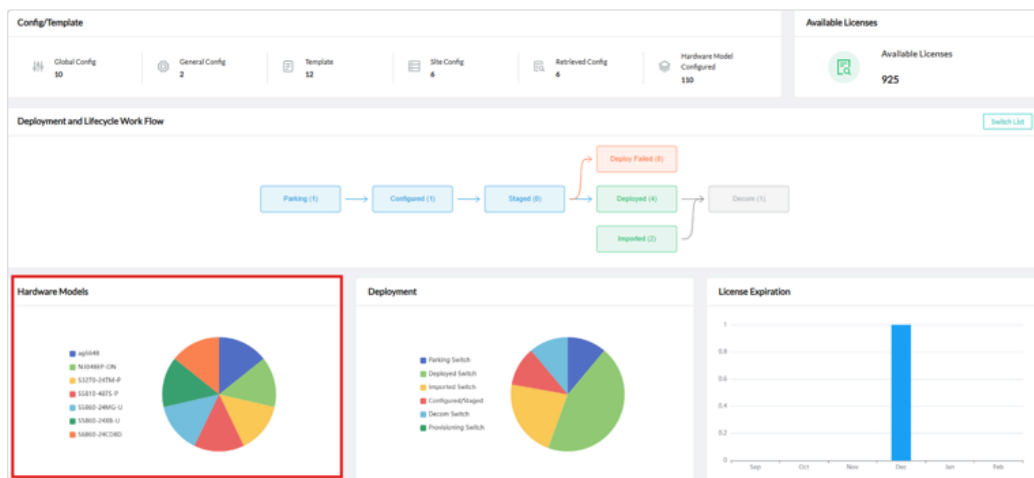
In the **Deployment** section, you can see the proportion of switches in each lifecycle state.

- **Parking Switch:** The total number of switches in **Parking** status
- **Deployed Switch:** The total number of switches in **Deployed** status
- **Imported Switch:** The total number of switches in **Imported** status
- **Configured/Staged:** The total number of switches in **Configured** or **Staged** status
- **Decom Switch:** The total number of switches in **DECOM** status
- **Provisioning Switch:** The total number of switches in **Provisioning** status



Checking Switch Models

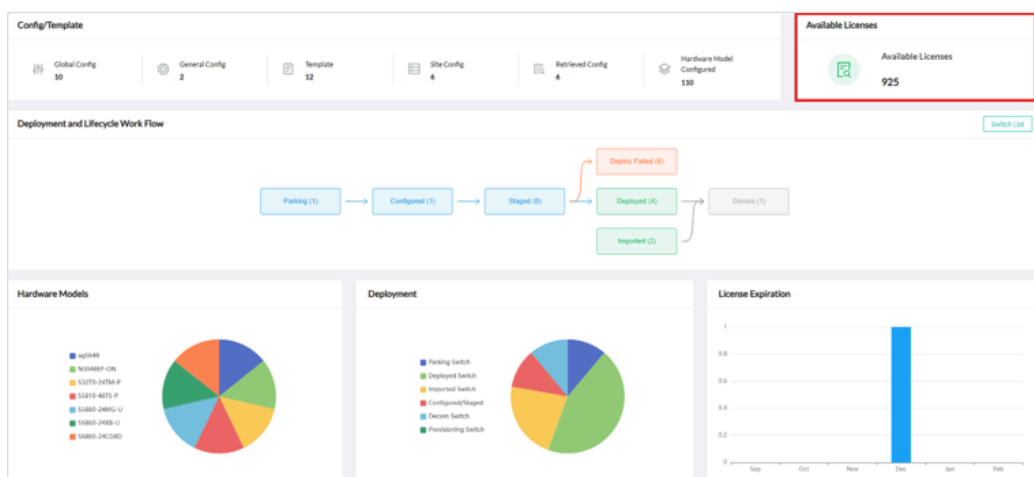
In the **Hardware Models** section, you can see the total numbers of switch models and their proportions.



Checking Licenses

Checking Available License Numbers

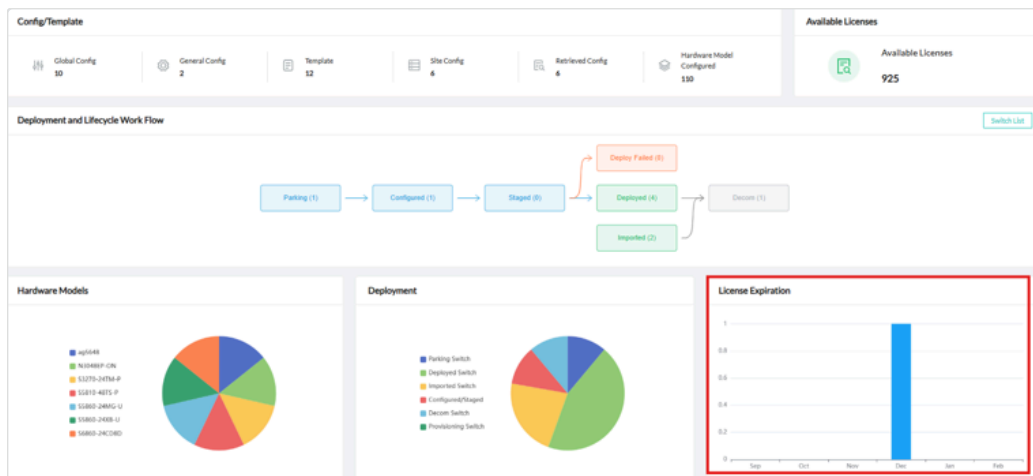
In the **Available Licenses** section, you can see the currently available license number.



Click **Available Licenses**, and then you are redirected to the [License Portal](#), where you can see more details about available licenses.

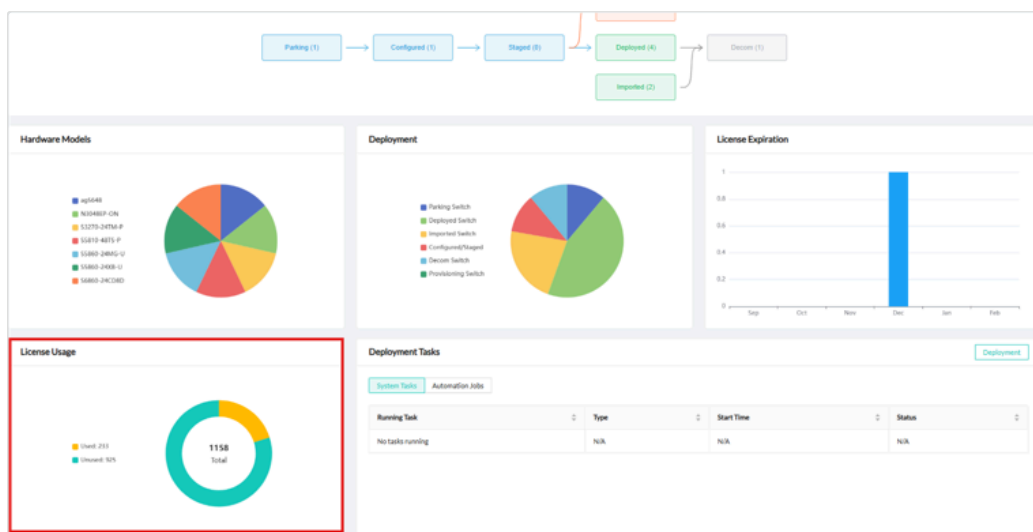
Checking License Expiration Dates

In the **License Expiration** section, you can see the total number of devices that will expire in each month over the next six months.



Checking License Usage

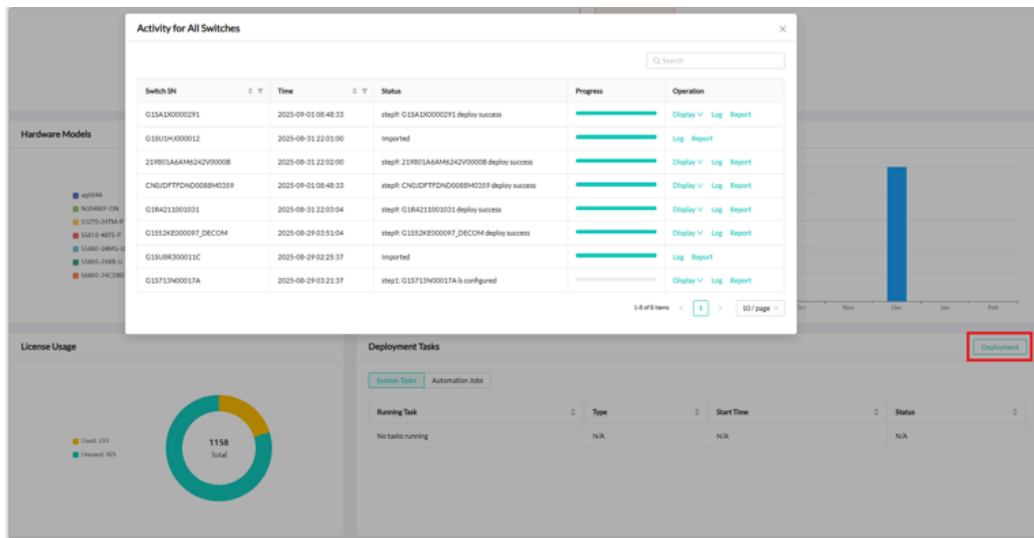
In the **License Usage** section, you can see the license usage information.



Checking Tasks

Checking All Switch Activities

In the **Deployment Tasks** section, click **Deployment**. You can see activities for all switches and each activity progress.

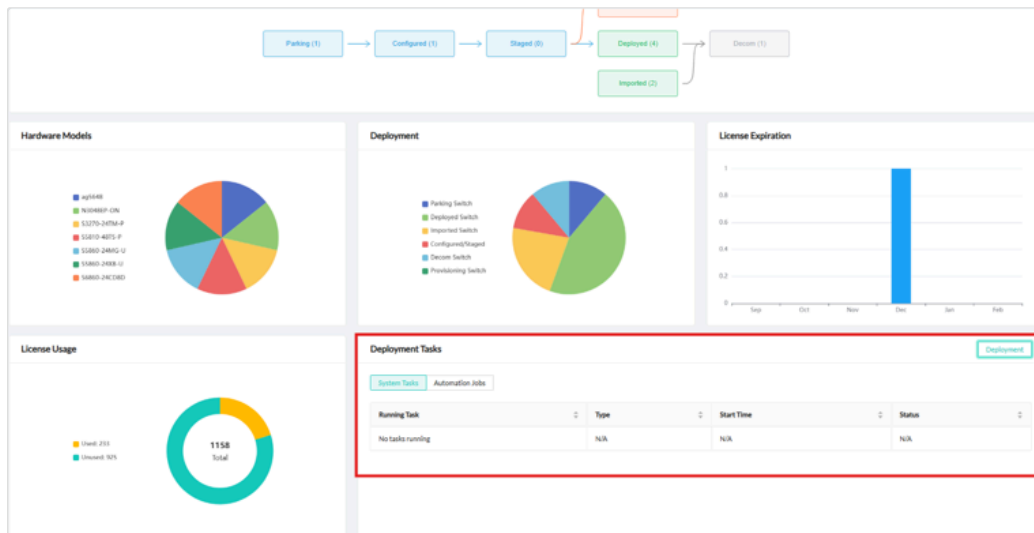


In the pop-up window, you can perform the following actions:

- Click **Display** to see the initial configurations during the switch deployment process. This button is not available for imported switches.
- Click **Log** to see the log information.
- Click **Report** to see the corresponding report.

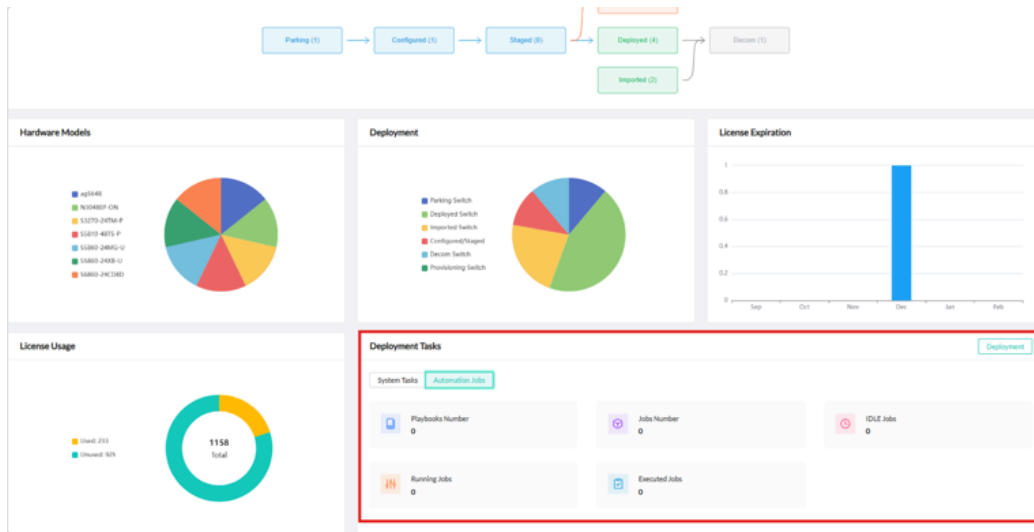
Checking System Tasks

In the **System Tasks** tab of the **Deployment Tasks** section, you can see the total numbers for different types of running tasks.



Checking Automation Jobs

In the **Automation Jobs** tab of the **Deployment Tasks** section, you can see the total numbers for different types of automation jobs.



Click the number for one specific type. You are redirected to the related page:

- Click **Playbooks Number** to go to the “Playbooks” page.
- Click **Jobs Number** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **IDLE Jobs** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **Running Jobs** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **Executed Jobs** to go to the **Job View** section of the “Ansible Jobs” page.

Terminals

AmpCon-Campus supports both automatically identifying terminal devices connected to each managed switch and manually adding terminal devices.

By using the terminal monitoring feature, you can accurately and securely monitor terminal devices in your network and thus facilitate refined monitoring of terminal devices.

[Use Cases](#)

[Terminal Identification Methods](#)

[Prerequisites](#)

[Viewing All Terminal Devices](#)

[Adding Terminals Manually](#)

[Viewing Terminal Devices in Topologies](#)

[Editing Terminal Device Information](#)

[Deleting Offline Terminal Devices](#)

NOTES

- For switches with PicOS 4.7.1M installed, the terminal monitoring feature is not supported.
- For switches of the following models, the terminal monitoring feature is not supported:
 - S3410L-24TF
 - S3410L-24TF-P
 - S3410-24TS
 - S3410-24TS-P
 - S3410C-16TF
 - S3410C-16TF-P
 - S3410C-16TMS-P
 - S3410C-8TMS-P
 - S3270-10TM
 - S3270-24TM
 - S3270-48TM
 - S3270-10TM-P
 - S3270-24TM-P

Use Cases

Terminal monitoring is helpful in the following use cases:

- **Network-wide terminal visualization**

View detailed information for all terminal devices across the network to gain a comprehensive visualization of terminals.

- **Categorized statistics and clear asset management**

Classify terminals by specific attributes for rapid inventory management, eliminating common blind spots such as unclear terminal counts and unknown access locations.

- **Status monitoring and anomaly detection**

Rapidly identify abnormal terminal devices and locate the affected terminal devices and physical ports, facilitating early detection and handling of faults.

Terminal Identification Methods

AmpCon-Campus uses the following technologies to automatically identify terminal devices, enabling accurate detection and management of terminal devices in the network.

- **MAC OUI Identification**

The first 24 bits of a device's MAC address, known as the Organizationally Unique Identifier (OUI), are assigned to manufacturers by the Institute of Electrical and Electronics Engineers (IEEE).

Switches report the terminal device's OUI to AmpCon-Campus, and then AmpCon-Campus references its fingerprint database to identify the device manufacturer.

- **DHCP Snooping Identification**

During Dynamic Host Configuration Protocol (DHCP) interactions, switches with DHCP Snooping enabled capture DHCP packets and extract the mappings of the terminal MAC address, IP address, and switch port. After recording these mappings in the binding table, the data is collected and returned to AmpCon-Campus through the Google Remote Procedure Call (gRPC) mechanism (typically through components like the gnmi exporter to perform collection operations). Meanwhile, the switch updates the binding table based on the packets, enabling precise device tracking and management.

Prerequisites

- Ensure that the networks to which the switches and terminal devices belong have DHCP servers configured.
- Ensure that DHCP Snooping, Link Layer Discovery Protocol (LLDP), and gRPC are enabled on the switches connected with the terminal devices to be managed.

Viewing All Terminal Devices

To view terminal devices that are automatically identified by AmpCon-Campus and added manually, click **Monitor > Wired Clients** from the navigation bar.

On the “Wired Clients” page, you can see the following information:

Tip

On the “Wired Clients” page, terminal devices are displayed based on the following priority order:

1. Online terminal devices with IP addresses identified.
2. Online terminal devices with no IP addresses identified.
3. Offline terminal device with IP addresses identified.
4. Offline terminal device with no IP addresses identified.

Wired Clients										
+ Wired Client										
Q Search										
Client Name	Status	MAC Address	IP Address	Switch SN	Port	Manufacturer	Terminal Type	Up/Down Time	Operation	
0c938b230001	Offline	0c938b230001		D4A50844A3A1	te-1/1/1			2025-09-08 10:19:06	Edit	Delete
0c4bf4b30001	Offline	0c4bf4b30001		D4A50844A3A1	ae1			2025-09-11 06:20:53	Edit	Delete
0c4bf4b30001	Offline	0c4bf4b30001		D4A50844A3A2	ae1			2025-09-11 10:42:54	Edit	Delete
0c938b230001	Offline	0c938b230001		D4A50844A3A2	ae1			2025-09-11 11:06:54	Edit	Delete
0c938b230001	Offline	0c938b230001		D4A50844A3A1	ae1			2025-09-11 06:20:53	Edit	Delete
0c4bf4b30001	Offline	0c4bf4b30001		D4A50844A3A1	te-1/1/2			2025-09-11 06:10:53	Edit	Delete
0c4bf4b30001	Offline	0c4bf4b30001		D4A50844A3A2	te-1/1/2			2025-09-09 03:22:09	Edit	Delete
485e73ff000a	Offline	485e73ff000a		D4A50844A3A1	te-1/1/48	Picall, Inc.		2025-09-08 11:26:06	Edit	Delete
0c938b230001	Offline	0c938b230001		D4A50844A3A1	te-1/1/48			2025-09-08 11:21:06	Edit	Delete
a201e909745c	Offline	a201e909745c		D4A50844A3A2	xe-1/1/1			2025-09-08 10:48:08	Edit	Delete
1-10 of 23 items < 1 2 3 > 10 / page										

Table 1. Wired Client Metrics

Metric	Description
Client Name	The name of the terminal device. • During the automatic terminal identification process, AmpCon-Campus assigns the MAC address of the terminal device as its client name. • For terminal devices displayed on the “Wired Clients” page, you can modify their client names as described in Editing Terminal Device Information.
Status	The status of the terminal device. • Online: The terminal device is up and connected to the switch. • Offline: The terminal device is down or isn’t connected to the switch.
MAC Address	The MAC address of the terminal device.
IP Address	The IP address of the terminal device.

	If DHCP Snooping is not enabled, or if the terminal is manually configured with a static IP address, this field will be empty. • For a dynamic IP address, AmpCon-Campus can automatically detect it. • For a static IP address, you can add it manually in Adding Terminals Manually or Editing Terminal Device Information.
Switch SN	The SN of the switch to which the terminal device connects. Click an SN, and then you are redirected to the “Switches” page, where you can see more details about the switch.
Port	The switch port used to connect to the terminal device.
Manufacturer	The manufacturer of the terminal device.
Terminal Type	The type of the terminal device, such as PCs, printers, cameras, smartphones, tablets, IP phones, or a custom type that you defined. NOTE Currently, AmpCon-Campus cannot recognize this field automatically. It has a value only for manually added terminals or when the manufacturer is entered in Editing Terminal Device Information.
Up/Down Time	The last time when the terminal device was online or offline. NOTE If the terminal device is added manually, the value will be empty temporarily. AmpCon-Campus retrieves the last up or down time of the terminal device after detecting the terminal device.

Adding Terminals Manually

If an identified terminal device is deleted or AmpCon-Campus cannot identify a terminal device automatically, you can't see the terminal device on the "Wired Clients" page.

To monitor the terminal device, add it to AmpCon-Campus manually. Follow these steps:

1. On the "Wired Clients" page, click **+ Wired Client**.
2. In the pop-up window, input the following information:

Table 1. Terminal Parameters

Parameters	Description
Client Name	The name to distinguish the terminal device. • This value must be no longer than 32 characters. • This value is unique when the MAC address, SN, and Port are all the same; otherwise, it can be duplicated.
MAC Address	The MAC address of the terminal device. You must enter a valid MAC address. Or else, the verification will fail.
IP Address	Optional. The IP address of the terminal device. The IP address needs to be in IPv4 format and does not include a subnet mask. • For a dynamic IP address, AmpCon-Campus can automatically detect it after you add the terminal. • For a static IP address, you need to add it manually.
Switch	Click Select to select the switch to which the terminal device connects.

Terminal Type	Optional. Select a built-in type from the Terminal Type drop-down list, or input a custom type. • The length of a custom type cannot exceed 32 characters. • After you input a custom type, the type will be added to the Terminal Type drop-down list.
----------------------	---

4. Click **Apply**.

NOTE

After you manually add a terminal device, AmpCon-Campus determines its status based on the following rules:

- If the terminal device is up and connected to the selected switch, the status is displayed as **Online**.
- If the terminal device is down or isn't connected to the selected switch, the status is displayed as **Offline**.
- If you remove the switch connected with the terminal device as described in [Removing Switches](#), the state of the terminal device is displayed as **Offline**.

Viewing Terminal Devices in Topologies

You can see real-time or historical information about the terminal devices connected to each managed switch in the topology. For more information, see [Client Info](#).

Device Port Info							
Port Info		Client Info					
Client Name	Status	MAC Address	IP Address	Port	Manufacturer	Terminal Type	
00:18:23:30:dd:53	Online	00:18:23:30:dd:53		te-1/1/2	Delta Electronics, Inc.		
60:18:95:71:a2:bf	Online	60:18:95:71:a2:bf		te-1/1/2	Dell Inc.		
64:9d:99:f8:23:1b1	Online	64:9d:99:f8:23:1b		te-1/1/2	FS COM INC		
6.30	Offline	0c:2f:19:69:00:01		1		PC	

Editing Terminal Device Information

To edit the information of a terminal device, follow these steps:

1. On the “Wired Clients” page, locate the terminal device, and then click **Edit**.
2. In the pop-up window, input the following information:

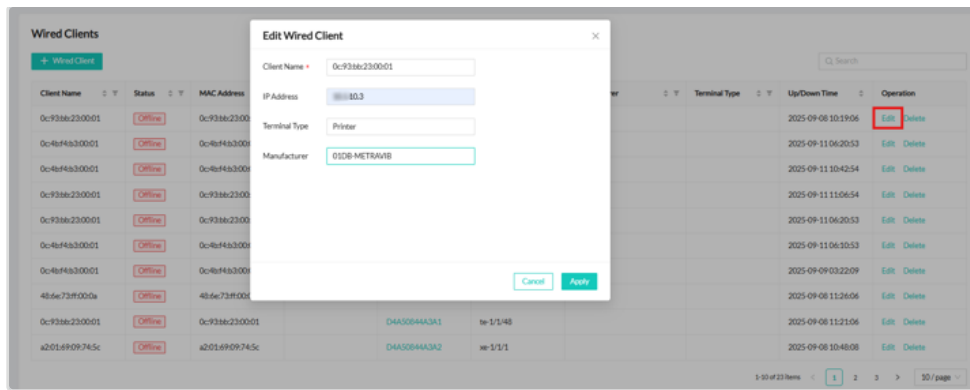


Table 2. Terminal Parameters

Metric	Description
Client Name	The name to distinguish the terminal device. - This value must be no longer than 32 characters. - This value is unique when the MAC address, SN, and Port are all the same; otherwise, it can be duplicated.
IP Address	Optional. The IP address of the terminal device. The IP address is in IPv4 format and does not include a subnet mask. NOTE You can edit the IP address when the terminal device is online and the IP address is not identified, or the terminal device is offline.
Terminal Type	Optional. Select a built-in type from the Terminal Type drop-down list, or input a custom type. - The length of a custom type cannot exceed 32 characters. - After you input a custom type, the type will be added to the Terminal Type drop-down list.
Manufacturer	Optional. Select a built-in manufacturer from the Manufacturer drop-down list, or input a custom manufacturer.

- The length of a custom manufacturer cannot exceed 128 characters.
- After you input a custom manufacturer, the manufacturer will be added to the **Manufacturer** drop-down list.
- You can enter keywords (at least 3 characters) to search for the manufacturer.

3. Click **Apply**.

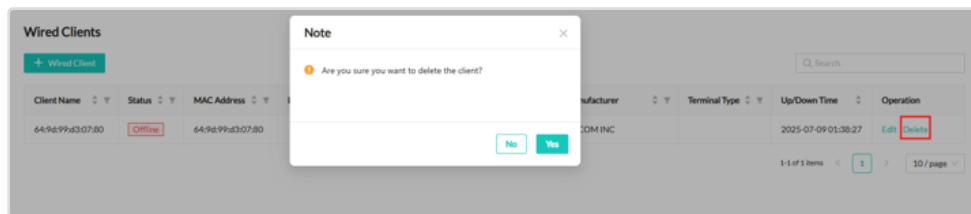
Deleting Offline Terminal Devices

To delete an offline terminal device from AmpCon-Campus, follow the steps:

1. On the “Wired Clients” page, locate the terminal device, and then click **Delete**.

NOTE

Only terminal devices in **Offline** status can be deleted.



2. Click **Yes** to confirm the deletion.

Telemetry

To ensure that the network is healthy and devices are working well, you need to continuously monitor and validate the operational state of your network and devices. AmpCon-Campus uses the telemetry technology to automatically collect real-time or historical metric data from managed switches.

By using AmpCon-Campus, you can view multi-dimensional telemetry data of all managed switches in a centralized user interface, gain detailed insights into network performance and device health, and proactively troubleshoot and optimize your network performance.

NOTE

For switches of the following models, the telemetry feature is not supported:

- S3410L-24TF
- S3410L-24TF-P
- S3410-24TS
- S3410-24TS-P
- S3410C-16TF
- S3410C-16TF-P
- S3410C-16TMS-P
- S3410C-8TMS-P
- S3270-10TM
- S3270-24TM
- S3270-48TM
- S3270-10TM-P
- S3270-24TM-P

The following scenarios are examples of using the telemetry data:

- **Monitor your network comprehensively with the telemetry data**

You can have an overall understanding about the network running status by checking telemetry metrics like routing neighbors, switch resource utilization, port counts, and Layer 2 and Layer 3 forwarding tables.

- **Track real-time performance metrics from various switches**

You can monitor performance-related telemetry metrics for all managed switches, such as port traffic, bandwidth utilization, and packet loss rate.

- **Optimize network performance based on the telemetry data**

You can better distribute the load based on the routing neighbor information, avoid excessive load on certain neighbors, and improve the overall network performance.

- **Decrease time and efforts on locating and resolving network problems**

You can get early warnings of network failures, be notified when equipment failures and performance anomalies happen, and quickly troubleshoot and address network issues.

See the following child topics:

- [Global Telemetry Data](#)
- [Telemetry Data of a Switch](#)

Global Telemetry Data

Click **Monitor > Telemetry** in the AmpCon-Campus UI, and then you can see the following telemetry data of all managed switches:

[Before You Begin](#)
[CPU and Memory](#)
[Port Metrics](#)
[Module Metrics](#)
[Filtering Telemetry Data](#)

Before You Begin

Real-time telemetry data can be displayed in the AmpCon-Campus UI only when the following prerequisites are met:

- The switch to be monitored is connected to the AmpCon-Campus server. Click **Wired > Switches** from the navigation bar, and then check the **VPN IP** column
 - ✓ means the switch is connected to the AmpCon-Campus server.
 - ✗ means the switch is not connected to the AmpCon-Campus server.
- Google Remote Procedure Call (gRPC) and Link Layer Discovery Protocol (LLDP) are enabled on the switch to be monitored. By default, gRPC and LLDP are enabled automatically after you deploy a switch with AmpCon-Campus or import a switch to AmpCon-Campus.

CPU and Memory



Table 1. CPU and Memory

Metric	Description
CPU	The CPU usage of a switch in percentage.
Memory	The memory usage of a switch in percentage.

NOTE

The **CPU** and **Memory** sections are always displayed and can't be hidden. You can display or hide other metrics by clicking the setting icon and

selecting the metrics to be monitored.

Port Metrics

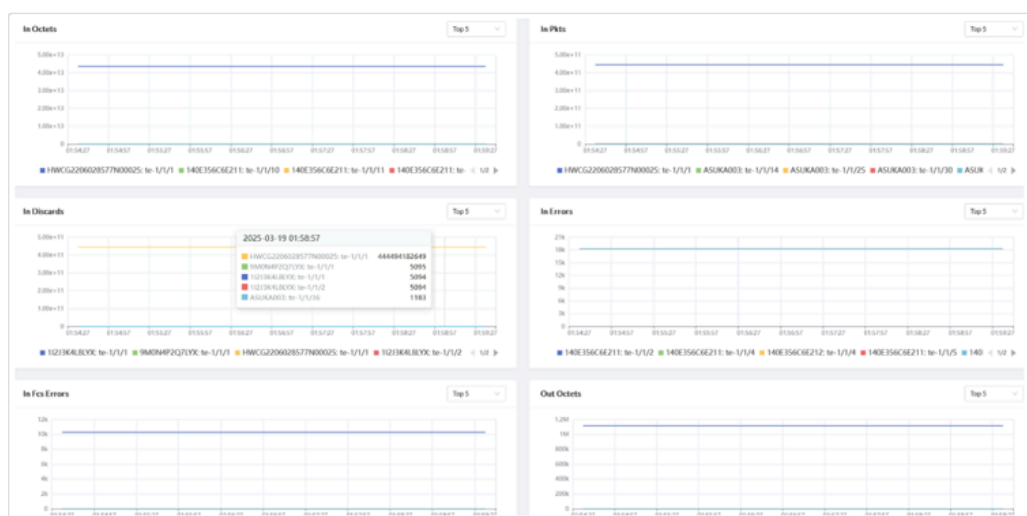


Table 2. Port Metrics

Metric	Description
In Octets	The number of octets (8-bit bytes) received by a switch port.
In Pkts	The number of incoming packets received by a switch port.
In Discards	The number of incoming packets that a switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by a 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 a switch port.
Out Pkts	The number of outgoing packets transmitted by a switch port.
Out Discards	The number of outgoing packets that a switch port intentionally discards (drops) before they are transmitted.

Out Errors	The number of outgoing packets that a switch port fails to transmit successfully due to errors.
Out Bits Rate	The rate at which bits are transmitted from a switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by a switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from a switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by a switch port. It's measured in Packets Per Second (pps).

Module Metrics

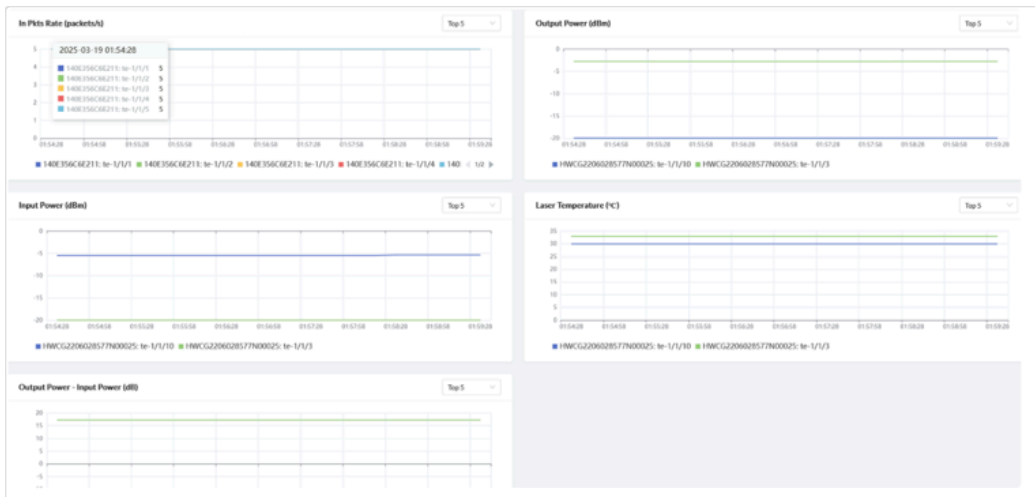


Table 3. Module Metrics

Metric	Description
Output Power	The amount of optical power delivered by the optical module connected to the switch port. It's measured in dBm.
Input Power	The amount of optical power consumed by the optical module connected to the switch port. It's measured in dBm.
Laser Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).
Output Power - Input Power	The difference between the output power and the input power.

Filtering Telemetry Data

To filter telemetry data as needed, use the following methods:

- To specify the metrics that you want to monitor, click the **All Counters** icon, select the metrics, and then click **OK**.
- 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.

NOTE

Even though **Top X** is selected, you might see less than the selected number of switch ports in the line chart when other ports are down.



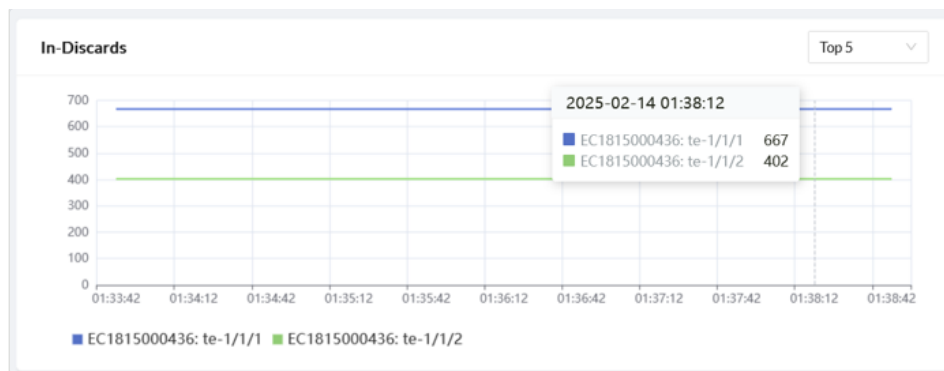
- To specify the time range for the data display, select the start date and end date in the **Time** section.

Time (UTC-0) →  

- To display or hide the data of a switch port, click the square before the port.



- To view the metric details in a specific time point, hover the mouse over that time point.



Telemetry Data of a Switch

Click **Wired > Switches** in the AmpCon-Campus UI, and click a specific switch SN or service tag in the switch list. Then, you can see the following telemetry data related to the switch:

[Before You Begin](#)

[Telemetry Data](#)

[Device Information](#)

[Switch Overview](#)

[Device Overview](#)

[Port Overview](#)

[Modules Overview](#)

[BGP](#)

[OSPF](#)

[MAC](#)

[ARP](#)

[IP Route](#)

[MLAG](#)

[PoE](#)

Before You Begin

Real-time telemetry data can be displayed in the AmpCon-Campus UI only when the following prerequisites are met:

- The switch to be monitored is connected to the AmpCon-Campus server. Click **Wired > Switches** from the navigation bar, and then check the **VPN IP** column
 -  means the switch is connected to the AmpCon-Campus server.
 -  means the switch is not connected to the AmpCon-Campus server.
- Google Remote Procedure Call (gRPC) and Link Layer Discovery Protocol (LLDP) are enabled on the switch to be monitored. By default, gRPC and LLDP are enabled automatically after you deploy a switch with AmpCon-Campus or import a switch to AmpCon-Campus.

Telemetry Data

Device Information

In the **Device Information** section, you can see the following information:

Device Information			
 Model: as5812_54x	SN: ASKSUK001	Hardware ID: C74D-32E6	MAC Address: 0c81fe9b0001
	Sysname: PICOS	Mgmt IP: 16.16	Version: 4.6.0E

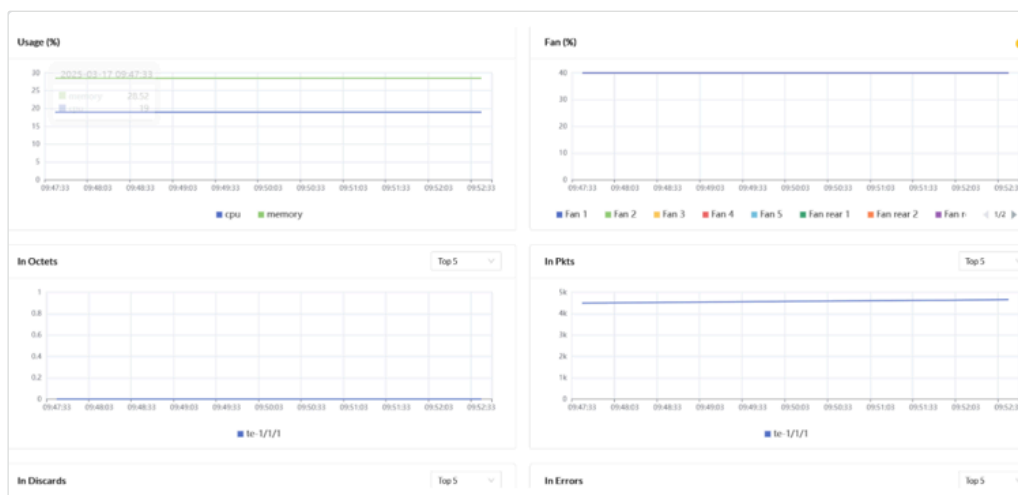
Table 1. Device Information Metrics

Metric	Description
--------	-------------

Model	The model of the switch.
SN	The serial number of the switch.
Hardware-ID	The hardware ID of the switch.
MAC Address	The MAC address of the switch.
Sysname	The hostname of the switch.
IP Address	The switch VPN IP address that is used to communicate with AmpCon-Campus.
Version	The PicOS version on the switch.

Switch Overview

Click the **Switch Overview** tab. Then, you can see the following line charts:



NOTE

The **Usage** and **Fan** sections are always displayed and can't be hidden. You can display or hide other metrics by clicking the setting icon and selecting the metrics to be monitored.

Table 2. Switch Overview Metrics

Metric	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.

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.

Laser Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).
Output Power - Input Power	The difference between the output power and the input power.

Device Overview

Click the **Device Overview** tab. Then, you can see the following tables:

RPSUs			
PSU Index	Power On	Enabled	Present
2	false	false	true
1	true	true	true

Fans			
Position	Direction	PWM	Speed
Fan 1	Forward	100.0%	21300
Fan 2	Forward	100.0%	20500

• Redundant Power Supply Units (RPSUs)

Table 3. RPSU Metrics

Metric	Description
PSU Index	The index of the Power Supply Unit (PSU).
Power on	Whether the PSU is powered on.
Enabled	Whether the PSU is activated or turned on.
Present	Whether the PSU is properly plugged.

• Fans

Table 4. Fan Metrics

Metric	Description
Position	The position of the fan.
Direction	The direction of the wind, forward or back.
PWM	The proportion of the fan's PWM to the total width.
Speed	The fan speed.

Port Overview

Click the **Port Overview** tab. Then, you can see the following table:

Port Name	Port State	MTU	Loopback Mode	Port Speed	In Bandwidth Utilization	Out Bandwidth Utilization	Auto Negotiate	Mac Addr	Duplex Mode	In Broadcast Pkts	In Discards	In Errors	In Fcs Errors	In Multicast Pkts	In Octets	In Pkts
te-1/1/1	UP	1514	false	100MB	-	-	true	0c:0b:75:a1:00:00	FULL	0	252	0	0	0	0	0
te-1/1/2	UP	1514	false	100MB	-	-	true	0c:0b:75:a1:00:00	FULL	0	252	0	0	0	0	0
te-1/1/3	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/4	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/5	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/6	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/7	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/8	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/9	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0
te-1/1/10	DOWN	1514	false	UNKNOWN	-	-	true	0c:0b:75:a1:00:00	FULL	0	0	0	0	0	0	0

Table 5. Port Overview Metrics

Metric	Description
Port Name	The name of the switch port.
Port State	The state of the switch port.
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.
Port Speed	The maximum data transfer rate that the port can support.
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 to automatically negotiate and select the optimal operating parameters, such as the speed and duplex mode.
Mac Addr	The MAC address of the switch port.

Duplex Mode	Whether data can flow in one direction (half duplex) at a time or 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 unknown 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 unknown 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.

Modules Overview

Click the **Modules Overview** tab. Then, you can see the following table:

Port Name	Connector Type	Identifier	Vendor Name	Vendor Part#	Transmission Distance	Transmission Rate	WaveLength (nm)	Rx Power (dBm)	Tx Power (dBm)	Power Budget (dB)	Temperature (°C)
te-1/1/1	COPPER_PIGTAIL_CONNECTOR	SFP_PLUS	Mellanox	MC3309130-003	2m(COPPER_OR_ACTIVE_CABLE)	10Gbps	0	0	0	0	0
te-1/1/3	LC_CONNECTOR	SFP_PLUS	DELTA	LCP-10G3A4EDR	30m(OM3) 80m(OM2) 300m(OM2)	10Gbps	8500	-20	-2.79	17.21	34
te-1/1/4	RJ45_CONNECTOR	SFP	OEM	SF-8TGP1-01	100m(COPPER_OR_ACTIVE_CABLE)	1Gbps	0	0	0	0	0
te-1/1/7	LC_CONNECTOR	SFP	H3C	SFP-GE-10G-S-U	20m(SM)	1Gbps	0	0	0	0	0
te-1/1/10	LC_CONNECTOR	SFP_PLUS	FS	SFP-10GBR-85	150m(OM3) 300m(OM2)	10Gbps	8500	-5.59	-20	-14.41	30
te-1/1/13	COPPER_PIGTAIL_CONNECTOR	SFP_PLUS	OEM	Q4SFP-40G-PCU2M	2m(COPPER_OR_ACTIVE_CABLE)	10Gbps	0	0	0	0	0
te-1/1/14	COPPER_PIGTAIL_CONNECTOR	SFP_PLUS	OEM	Q4SFP-40G-PCU2M	2m(COPPER_OR_ACTIVE_CABLE)	10Gbps	0	0	0	0	0

Table 6. Module Overview Metrics

Metric	Description
Port Name	The name of the switch port connected with the optical module.
Connector Type	The type of the connector used by the optical module.
Form Factor	The physical size, shape, and interface specifications of the optical module.
Vendor	The manufacturer of the optical module.
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. It's measured in gigabits per second (Gbps).
WaveLength	The distance between two corresponding points on an optical wave, typically measured from crest to crest (or trough to trough). It's measured in nanometers (nm).
Tx Power	The amount of optical power consumed by the optical module. It's measured in dBm.
Rx Power	The amount of optical power delivered by the optical module. It's measured in dBm.
Power Budget	The difference between the output power and the input power.
Temperature	The temperature of the optical module. It's measured in Celsius (°C).

BGP

Click the **BGP** tab. Then, you can see the following table:

VRF Name	BGP Version	Local AS	Local Router ID	Remote AS	Remote Router ID	BGP State	Hold Time (s)	Keepalive Interval (s)
default	4	110	0.92	0	0.0.0	ACTIVE	180	60
default	4	110	0.92	0	0.0.0	ACTIVE	180	60
default	4	110	0.92	0	0.0.0	ACTIVE	180	60
default	4	110	0.92	0	0.0.0	ACTIVE	180	60
default	4	110	0.92	0	0.0.0	ACTIVE	180	60

Table 7. BGP Metrics

Metric	Description
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 State	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.

OSPF

Click the **OSPF** tab. Then, you can see the following table:

VRF Name	Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtl	Rxptl	DBmtl	DR	BDR
default	0.87	1	FULL	2025-03-19 10:52:06	0.103	rif-te1:0.0.0	0	0	0	0.0.0	0.0.0
default	0.88	1	FULL	2025-03-19 10:52:10	0.107	rif-te2:0.0.0	0	0	0	0.0.0	0.0.0
default	0.90	1	FULL	2025-03-19 10:52:11	0.115	rif-te4:0.0.0	0	0	0	0.0.0	0.0.0
default	0.86	1	FULL	2025-03-19 10:52:13	0.99	rif-te5:0.0.0	0	0	0	0.0.0	0.0.0
default	0.89	1	FULL	2025-03-19 10:52:15	0.111	rif-te3:0.0.0	0	0	0	0.0.0	0.0.0

Table 8. OSPF Metrics

Metric	Description
--------	-------------

VRF Name	The name of the 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	Backup Designated Router, a backup to the DR in an OSPF network.

MAC

Click the **MAC** tab. Then, you can see the following table:

NOTE

For switches with PicOS 4.7.1M installed, the MAC data is not displayed.

MAC Address	Interface	Vlan	Age (s)	Type
0c25:26:7e:00:01	te 1/1/2	1	300	DYNAMIC
0c75:ec:94:00:01	te 1/1/1	1	300	DYNAMIC

Table 9. MAC Metrics

Metric	Description
MAC Address	The MAC address of the switch port connecting to this switch.
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 obtaining method of the MAC address, dynamic or static.

ARP

Click the **ARP** tab. Then, you can see the following table:

 **NOTE**

For switches with PicOS 4.7.1M installed, the ARP data is not displayed.

IP Address	HW Address	Type	Interface
.0.103	0c74:4a:dd:00:01	DYNAMIC	r/f-te1
.1.107	0c91:29:0c:00:01	DYNAMIC	r/f-te2
.0.111	0c92:a6:b9:00:01	DYNAMIC	r/f-te3
.1.115	0c65:cc:f5:00:01	DYNAMIC	r/f-te4
.1.99	0c75:6a:c8:00:01	DYNAMIC	r/f-te5

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.

IP Route

Type	Destination Network	Route Metrics	Next Hop	Outgoing Interface	Route Age
OSPF	0.98/31	[110/200]	197	rif-te5	01:12:52
DIRECTLY_CONNECTED	1.96/31	[0/0]	-	rif-te5	01:13:11
OSPF	0.96/31	[110/100]	-	rif-te5	01:13:04
OSPF	1.114/31	[110/200]	113	rif-te4	01:12:44
DIRECTLY_CONNECTED	1.112/31	[0/0]	-	rif-te4	01:13:11

Table 11. IP Route Metrics

Metric	Description
Type	The protocol through which the route was learned or configured. • 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 (cost) 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.

MLAG

Click the **MLAG** tab. Then, you can see the following table:

Domain ID	Domain MAC	Node ID	Peer Link	Peer IP	Peer VLAN	Neighbor Status	Config Matched	MAC Synced	MLAG Link Count
29	48:6E:73:FF:00:18	0	ar1	10.1.1.2	30	DOWN	No	No	1

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.

PoE

Click the **PoE** tab. Then, you can see the following table:

Port	Status	Consumption	PD-Class
ge-1/1/7	True	3.6 W	0

NOTE

Only switches that support PoE will have the PoE telemetry information displayed.

Table 13. PoE Metrics

Metric	Description
Port	The unique identifier to distinguish ports on the switch.
Status	The PoE function status of the port. • Disabled: PoE is turned off on the port. • Searching: The port is actively detecting whether a Powered Device (PD) is connected. • Delivering: Power is being supplied to a connected PD. • Test: The port is performing a test to verify the PD or power delivery. • Requesting: The PD is requesting power from the port. • Fault: A fault has occurred, preventing power delivery.
Consume	The power consumption of the port.
PD-Class	The PoE class of the connected PD. Values can be 1, 2, 3, 4, 5, 6, 7, and 8. Each class corresponds to a specific power level.

Topology

You can use the automatic discovery of topology feature to 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.

In addition, you can view real-time or historical information about terminal devices connected to the switch.

See the following child topics:

- [Managing Topologies](#)
- [Planning Topologies](#)
- [Viewing Real-Time Topologies](#)
- [Viewing Historical Topologies](#)
- [Viewing Switch Details, Ports, and Terminal Devices](#)

NOTE

For switches of the following models, the automatic discovery of topology feature is not supported:

- S3410L-24TF
- S3410L-24TF-P
- S3410-24TS
- S3410-24TS-P
- S3410C-16TF
- S3410C-16TF-P
- S3410C-16TMS-P
- S3410C-8TMS-P
- S3270-10TM
- S3270-24TM
- S3270-48TM
- S3270-10TM-P
- S3270-24TM-P

Managing Topologies

Topologies can help you identify and visualize your network structure. You can add, edit, or delete topologies by using the AmpCon-Campus UI.

NOTE

The topologies in the **Site** section are automatically created and can't be manually added or deleted. To add switches to a site or remove switches from a site, see [Managing Sites](#).

[Adding a Topology](#)

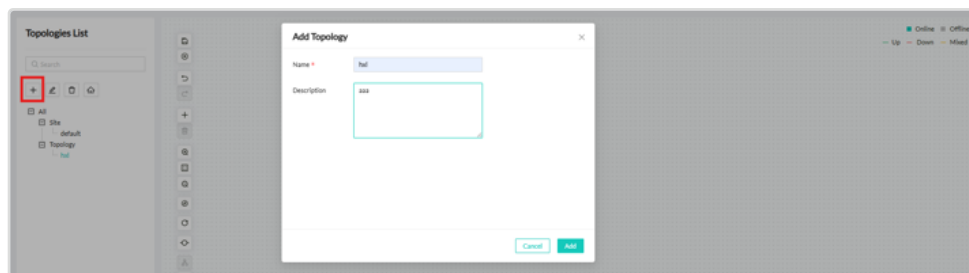
[Editing a Topology](#)

[Deleting a Topology](#)

[Setting or Unsetting a Default Topology](#)

Adding a Topology

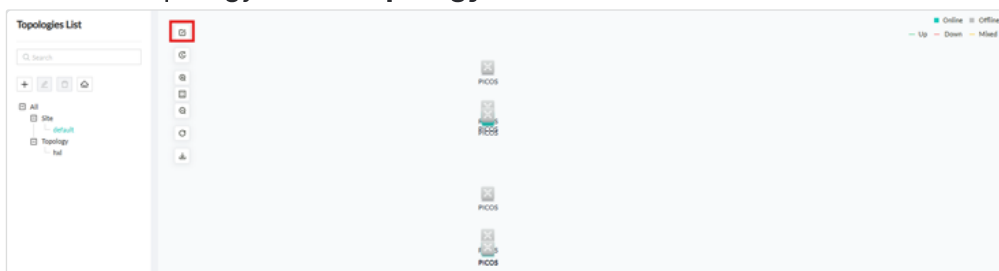
1. In the AmpCon-Campus UI, click **Network Design > Topologies**.
2. In the **Topology List** section, click the “Add Topology” icon.



3. Enter the topology name and description (optional), and then click **Add**.
4. Wait for the process to complete. Then, you can see the new topology in the **Topology** list.

Editing a Topology

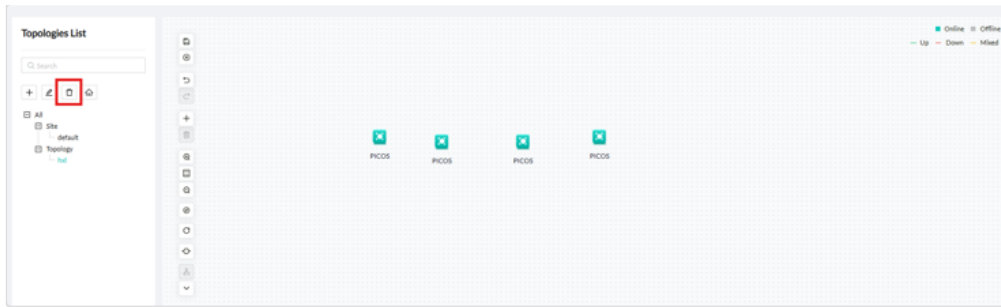
1. Click the topology in the **Topology List** section, and then click the edit icon.



2. Enter a new name or description, and then click **Save**.

Deleting a Topology

1. Click the topology in the **Topology List** section, and then click the delete icon.

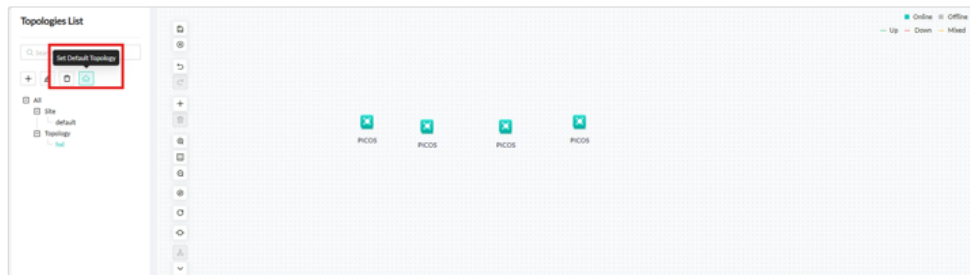


2. In the pop-up window, verify the name of the topology, and then click **Yes** to confirm the deletion.
3. Verify whether the topology is removed from the **Topology List** section.

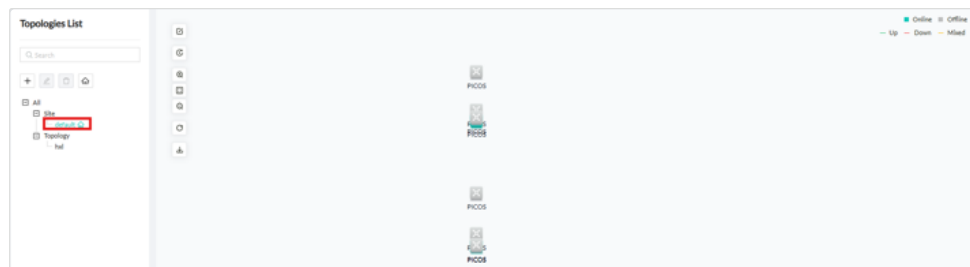
Setting or Unsetting a Default Topology

When you click **Network Design > Topologies**, the default topology is displayed. To set a default topology, follow these steps:

1. Click a non-default topology, and then click the “Set Default Topology” icon.



2. Verify whether the selected topology is marked with the default icon.



To unset a default topology, click the default topology, and then click the “Set Default Topology” icon again.

Planning Topologies

You can enter the topology edit mode to customize a topology based on your actual needs.

[Entering the Topology Edit Mode](#)

[Adding Switches to a Topology](#)

[Removing Switches from a Topology](#)

[Automatically Discovering Links](#)

[Manually Adding Links](#)

[Editing Links](#)

[Selecting a Topology Layout](#)

[Zooming in or out of a Topology](#)

[Undoing or Redoing Operations](#)

[Saving a Topology](#)

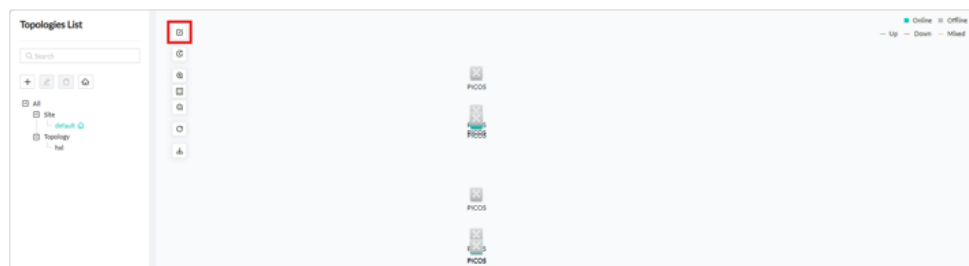
[Setting whether to Display the Legend](#)

[Refreshing the Current Topology](#)

[Exiting the Topology Edit Mode](#)

Entering the Topology Edit Mode

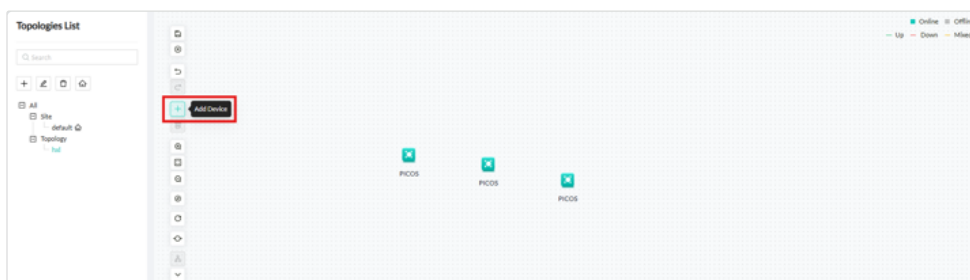
1. In the AmpCon-Campus UI, click **Network Design > Topologies**.
2. Select the topology in the **Topology List** section to enter the real-time topology mode.
3. Click the "Edit" icon to enter the topology edit mode.



Adding Switches to a Topology

To add switches to a topology, follow these steps:

1. Enter the topology edit mode as described in the last section.
2. Click the topology, and then click the "Add Device" icon.



3. Select the switches that you want to add, and then click **Save**.

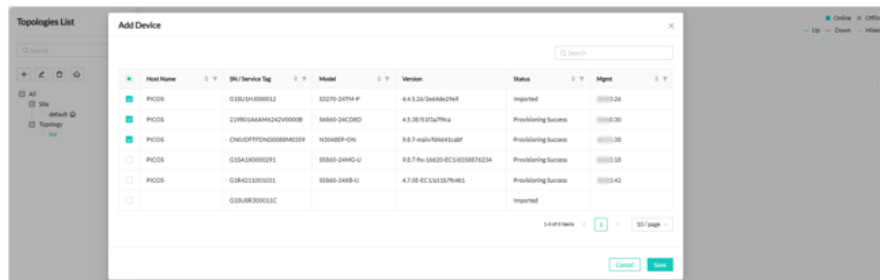
Removing Switches from a Topology

To remove switches from a topology, follow these steps:

1. Enter the topology edit mode as described in the [Entering the Topology Edit Mode](#) section.
2. Remove switches by using either of the following methods:

- **Using the "Add Device" icon**

1. Click the topology, and then click the "Add Device" icon.
2. Uncheck the switches that you want to remove, and then click **Save**.



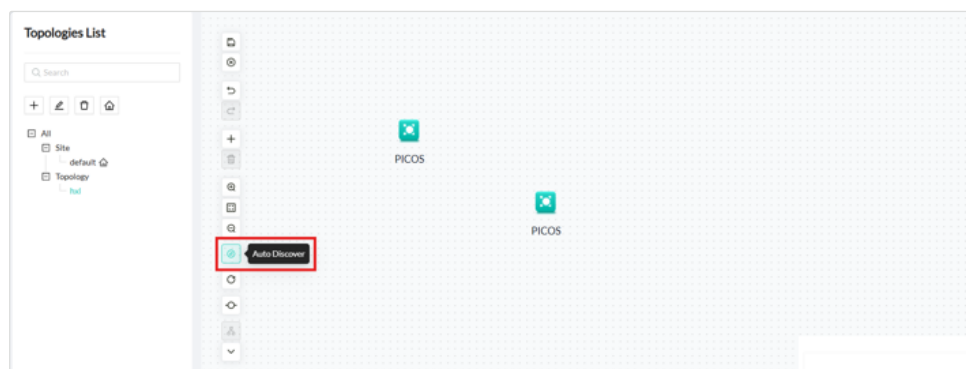
- **Using the "Delete Node" icon**

Click the topology, and then click the "Delete Node" icon.



Automatically Discovering Links

1. In the topology edit mode, click the "Auto Discover" icon.



2. In the pop-up window, click **Yes** to start the auto-discovery process.
3. Wait for the process to complete. Then, the links in the topology are updated.

NOTE

If switches in the topology don't connect with each other in the real network, you will not see links.

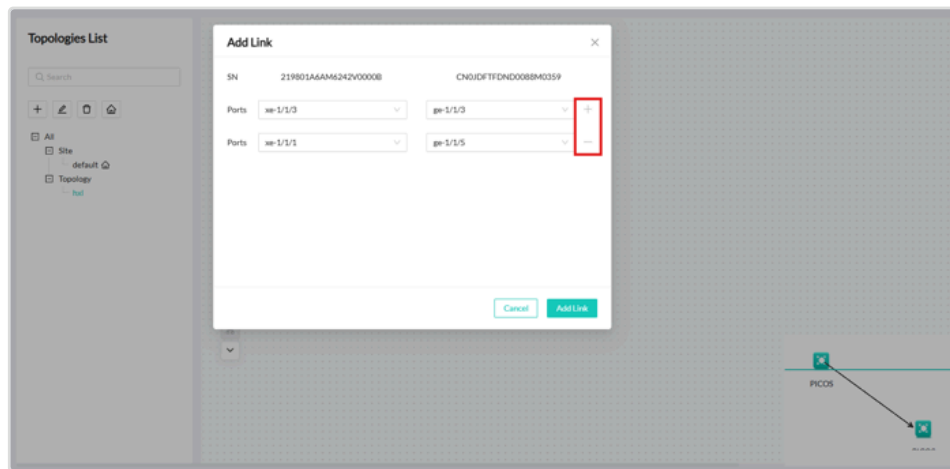
Manually Adding Links

To add a link, follow these steps:

1. In the topology edit mode, hover your mouse over a switch until you see a cross symbol.
2. Connect the switch with another switch. Then, you can see an **Add Link** pop-up window.
3. In the **Ports** section, input the connection ports for these two switches.

Click **+** on the right to add a new port connection, or click **-** to remove a port connection.

If a selected port is already in use by another link, a warning is displayed.



4. Click **Add Link**.

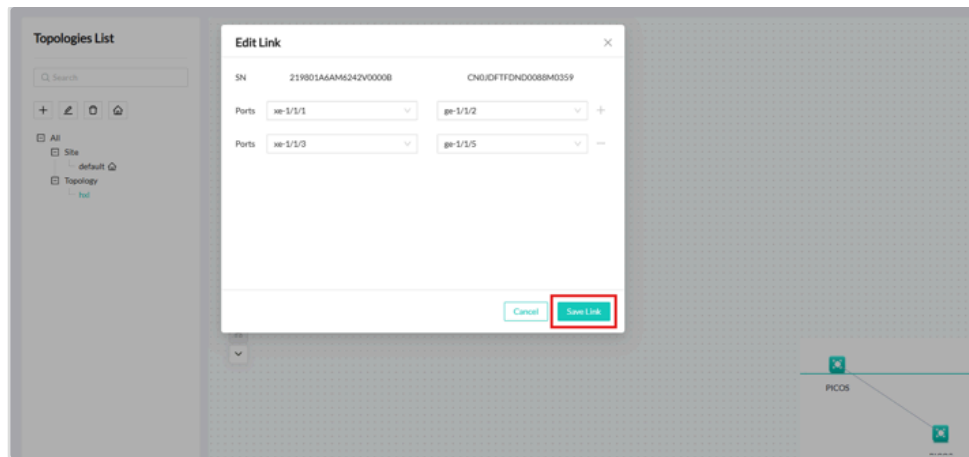
After you add a link and save the topology, the link is displayed in red or green based on the real connectivity status:

- If the link between these two switches doesn't exist in the real network, the link is marked in red.
- If the link between these two switches exists in the real network, the link is marked in green.

Editing Links

After a link is added, you can edit the link. Follow these steps:

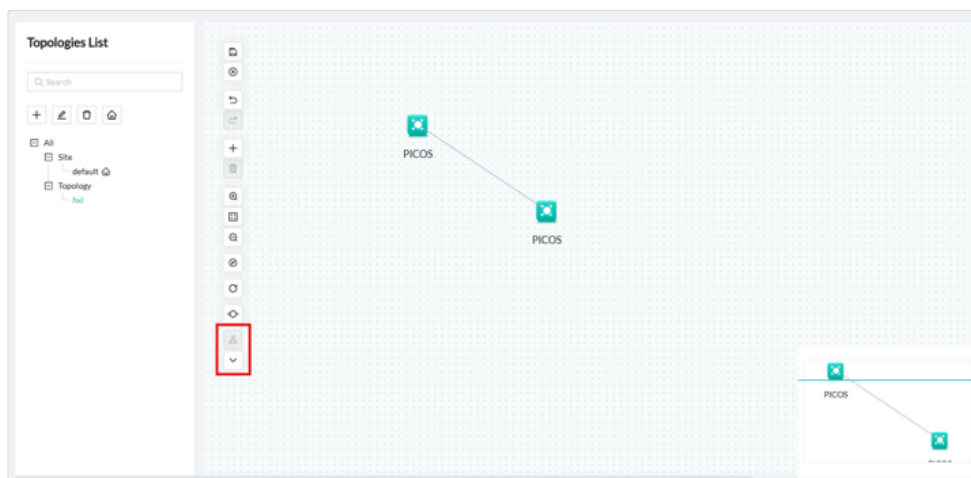
1. Right-click a link, and click **Edit**.
2. In the pop-up window, modify the link as needed.
3. Click **Save Link**.



Selecting a Topology Layout

In the topology edit mode, you can see the topology in the auto hierarchy layout by default. To select a topology layout, follow these steps:

1. Click the arrow below the **Auto Hierarchy Layout** button.



2. Select a layout from the following four layout styles:

- **Auto Hierarchy Layout (Tree Layout)**

Select a specific switch in the topology, and then click **Auto Hierarchy Layout**. You can see a tree layout with the switch as the root node.

The auto hierarchy layout cannot be applied when no switches are selected or no links exist among switches.

- **Grid Layout**

If no switches are selected, the grid layout automatically lays out all global elements.

If some switches are selected, the grid layout is applied only to the selected switches.

- **Circular Layout**

If no switches are selected, the circular layout automatically lays out all global elements.

If some devices are selected, the circular layout is applied only to the selected switches.

• Elliptical Layout

If no switches are selected, the elliptical layout automatically lays out all global elements.

If some switches are selected, the elliptical layout is applied only to the selected switches.

Zooming in or out of a Topology

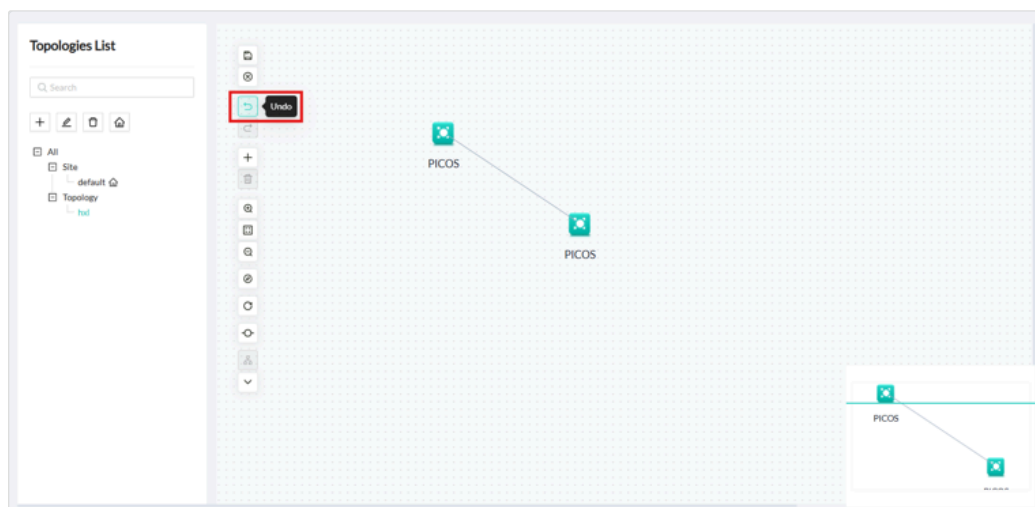
- To zoom in a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and scroll the mouse wheel backward.

Undoing or Redoing Operations

In the topology edit mode, you can undo or redo operations.

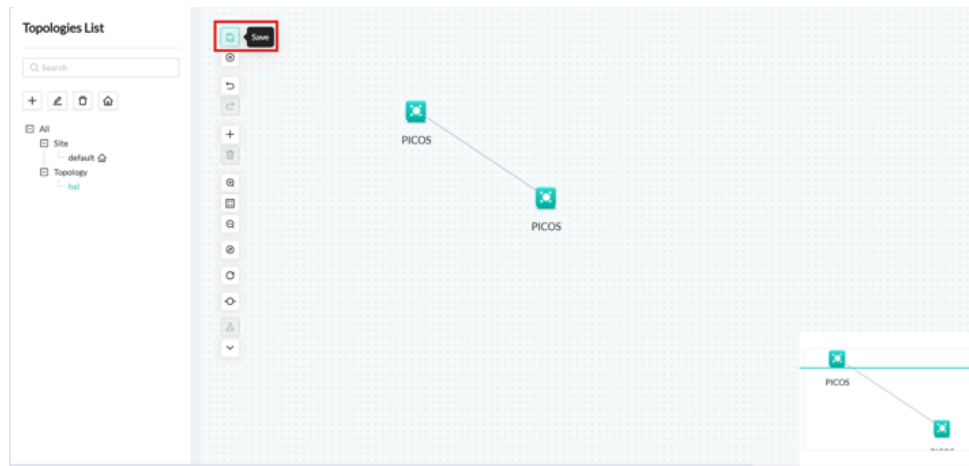
- To revert to the last operation, click **Undo**.
- To redo the last operation, click **Redo**.

If no undo or redo operations are available, these two buttons are grayed out and disabled.



Saving a Topology

1. In the topology edit mode, click **Save** to save the current topology.
2. Wait for the process to complete. After the topology is saved, you will automatically exit the topology edit mode.

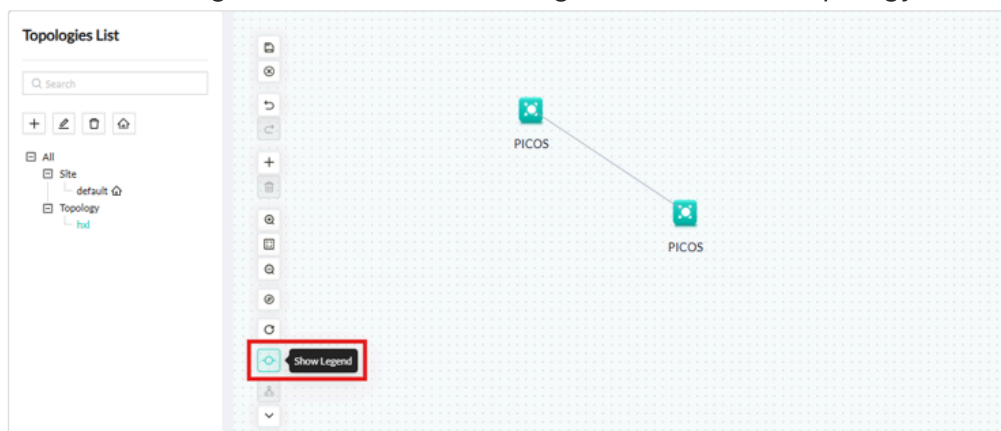


Setting whether to Display the Legend

- To hide the legend, click the "Hide Legend" icon in the topology edit mode.

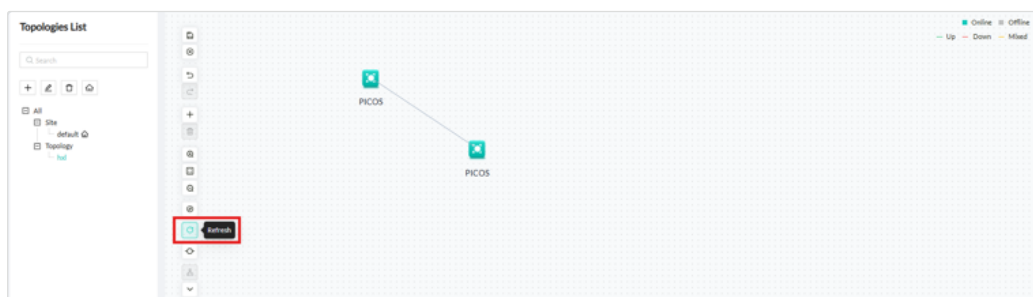


- To show the legend, click the "Show Legend" icon in the topology edit mode.



Refreshing the Current Topology

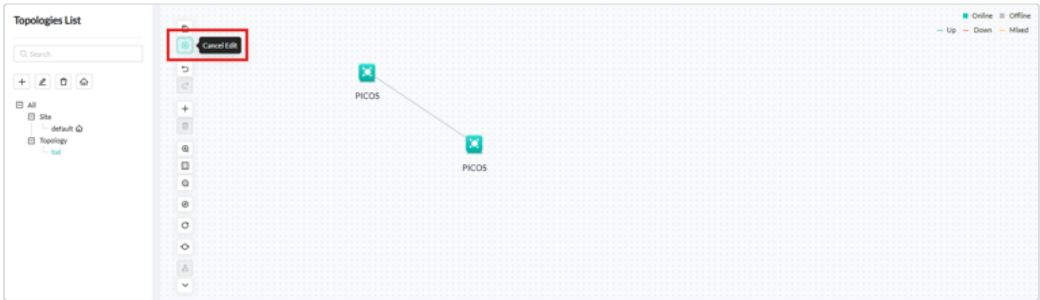
In the topology edit mode, click the "Refresh" icon.



The topology diagram will revert to the last saved state, and any unsaved changes will be lost.

Exiting the Topology Edit Mode

To exit the topology edit mode, click the "Cancel Edit" icon in the topology edit mode.



Viewing Real-Time Topologies

You can enter the real-time topology mode to view real-time network status, such as switch status and link faults. By clicking a switch or a link, you can see detailed stats information.

[Entering the Real-Time Topology mode](#)

[Refreshing the Topology](#)

[Zooming in or out of a Topology](#)

[Exporting a Topology](#)

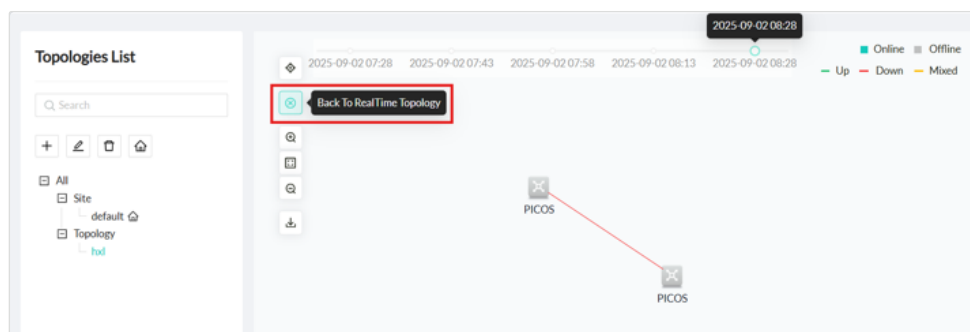
Entering the Real-Time Topology mode

1. In the AmpCon-Campus UI, click **Network Design > Topologies**.
2. Click the topology in the **Topologies List** section, and then you enter the real-time topology mode automatically.



NOTE

If you are in the historical topology mode, click the “Back To Real-Time Topology” icon to return to the real-time topology mode.



Refreshing the Topology

In the real-time topology mode, click the "Refresh" icon.



Zooming in or out of a Topology

- To zoom in a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel backward.

Exporting a Topology

In the real-time topology mode, click the "Download Image" icon. You can view the exported topology in the download history of your browser.



Viewing Historical Topologies

You can enter the historical topology mode to view the network status at different times or analyze the historical topology to trace problems.

[Viewing a Historical Topology](#)

[Zooming in or out of a Topology](#)

[Exporting a Topology](#)

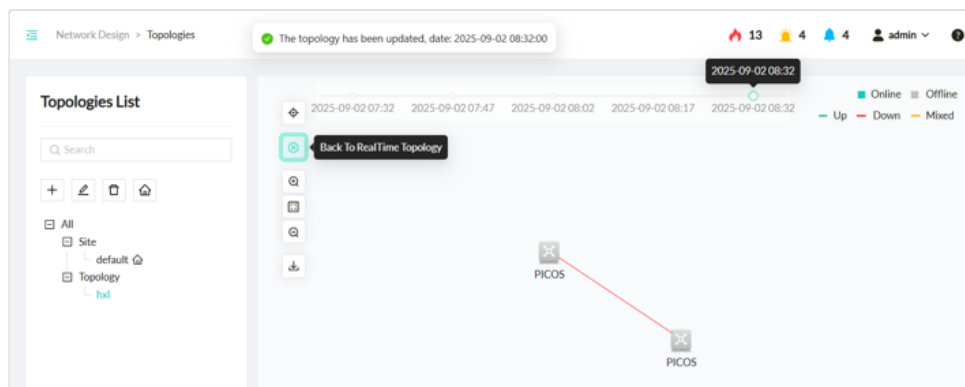
[Returning to the Real-Time Topology Mode](#)

Viewing a Historical Topology

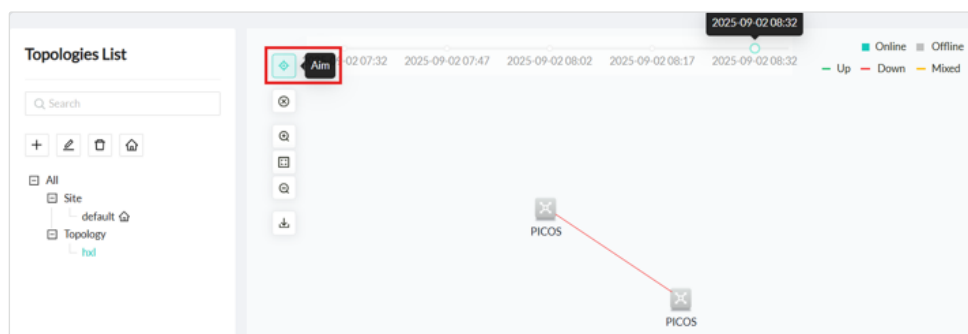
1. In the AmpCon-Campus UI, click **Network Design > Topologies**.
2. Click the topology in the **Topology List** section, and then you enter the real-time topology mode automatically.
3. To enter the historical topology mode, click the "History" icon.



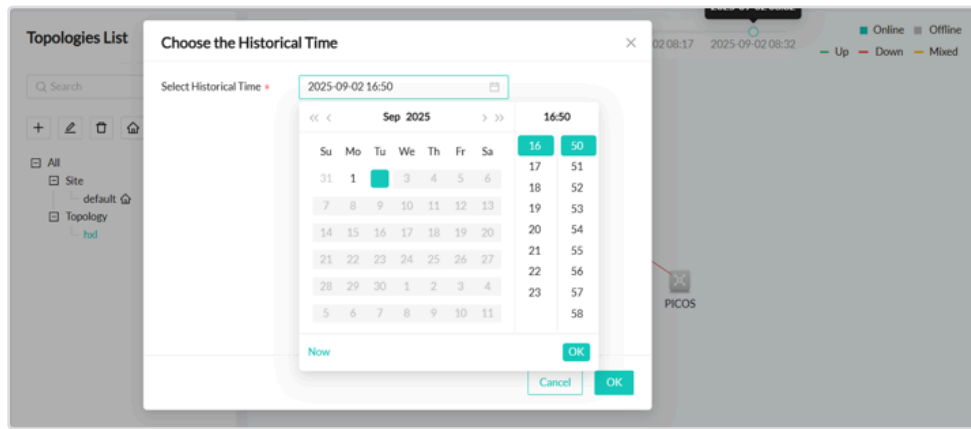
Then, you can see the historical topology as follows:



4. In the historical topology mode, click the "Aim" icon.



5. Modify the time as needed in the pop-up window, and click **OK**.



6. After the topology is loaded completely, the topology shows the state at the selected time point. The timeline shows 30 minutes forward or backward from that time point.

7. Click the time points in the timeline to view historical topologies at different times.

Zooming in or out of a Topology

- To zoom in a topology, hover the mouse over the topology, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel backward.

Exporting a Topology

In the historical topology mode, click the "Download Image" icon. You can view the exported topology in the download history of your browser.



Returning to the Real-Time Topology Mode

In the historical topology mode, click the "Back To Real-Time Topology" icon to leave the historical mode.

Topologies List

Q Search

+

All

Site

default

Topology

hxd

2025-09-02 07:32

2025-09-02 07:47

2025-09-02 08:02

2025-09-02 08:17

2025-09-02 08:32

Online

Offline

Up

Down

Mixed

Back To RealTime Topology

PICOS

PICOS

548

Viewing Switch Details, Ports, and Terminal Devices

When you click a switch in a topology, you can view real-time or historical information about the switch, switch ports, and terminal devices connected to the switch.

[Viewing Real-Time or Historical Data](#)

[Device Info](#)

[Port Info](#)

[Client Info](#)

Viewing Real-Time or Historical Data

To view real-time switch details, switch ports, and terminal devices, enter the real-time topology mode, and then click the switch to be monitored.

To view historical switch details, switch ports, and terminal devices, enter the historical topology mode, and then click the switch to be monitored.

Then, you can see the following sections in the topology:

Device Info

In the **Device Info** section, you can see the following switch-related information:

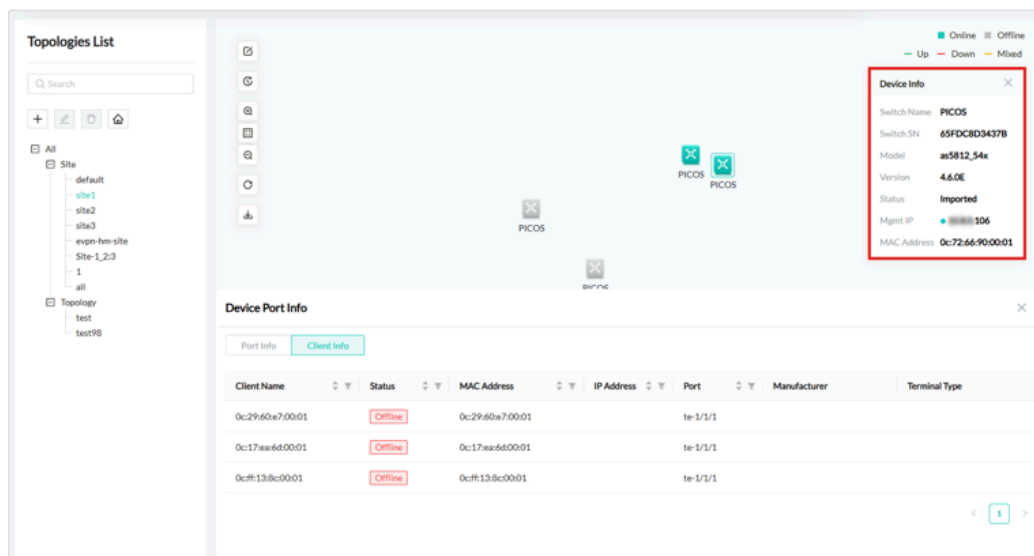


Table 1. Device Info Metrics

Metric	Description
Switch Name	The name of the switch.
Switch SN	The SN of the switch.
Model	The model of the switch.
Version	The PicOS version of the switch.

Status	The state of the switch. - For the topologies in the Site section, the following switch states are supported: Imported: The switch is imported to AmpCon-Campus. Provisioning Success: The switch is deployed by using AmpCon-Campus. Configured: After you add a switch configuration, the switch is in Configured status. Staged: After you stage a switch, the switch is in Staged status. Registered: The switch has registered with AmpCon-Campus but hasn't been deployed completely. Provisioning Failed: The switch fails to be deployed by using AmpCon-Campus. DECOM: The deployed switch is decommissioned (DECOM) when it's online. DECOM-Manual: The deployed switch is decommissioned when it's offline. RMA: The switch is replaced with another switch of the same switch model by using Return Merchandise Authorization (RMA). - For the topologies in the Topology section, the following switch states are supported: Imported: The switch is imported to AmpCon-Campus. Provisioning Success: The switch is deployed by using AmpCon-Campus.
Mgmt IP	The management IP address of the switch.
MAC Address	The MAC address of the switch.

Port Info

In the **Port Info** section, you can see the following port-related metrics:

Device Port Info											
Port Info											
Port Name	Status	Port Speed	In Octets	In Pkts	In Discards	In Errors	Out Octets	Out Pkts	Out Discards	Out Errors	
te-1/1/1	Up	10GB	0	196732	2	0	0	0	0	0	
te-1/1/2	Down	UNKNOWN	0	0	0	0	0	0	0	0	
te-1/1/3	Down	UNKNOWN	0	0	0	0	0	0	0	0	
te-1/1/4	Down	UNKNOWN	0	0	0	0	0	0	0	0	

Table 2. Port Info Metrics

Metric	Description
Port Name	The name of the switch port
Status	The status of the switch port, up or down
Port Speed	The maximum data transfer rate that the port can support
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
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port
Out Pkts	The number of outgoing packets transmitted by the switch port
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops) before they are transmitted
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors

Client Info

In the **Client Info** section, you can view the following metrics for terminal devices connected to the switch:

 **Tip**

Terminal devices are displayed based on the following priority order:

1. Online terminal devices with IP addresses identified.

2. Online terminal devices with no IP addresses identified.

3. Offline terminal device with IP addresses identified.

4. Offline terminal device with no IP addresses identified.

Device Port Info								
Port Info		Client Info						
Client Name	Status	MAC Address	IP Address	Port	Manufacturer	Terminal Type		
64:9d:99:d3:07:4a	Online	64:9d:99:d3:07:4a		te-1/1/2	FS COM INC			
64:9d:99:d9:e7:ef	Online	64:9d:99:d9:e7:ef		xe-1/1/2	FS COM INC			
64:9d:99:d8:9f:9d	Online	64:9d:99:d8:9f:9d		xe-1/1/2	FS COM INC			
64:9d:99:d3:72:5a	Offline	64:9d:99:d3:72:5a		xe-1/1/2	FS COM INC			

Table 3. Client Info Metrics

Metric	Description
Client Name	The name of the terminal device. • During the automatic terminal identification process, AmpCon-Campus assigns the MAC address of the terminal device as its client name. • During the Adding Terminals Manually, AmpCon-Campus assigns the value you input as its client name. • For terminal devices displayed on the “Wired Clients” page, you can modify their client names as described in Editing Terminal Device Information.
Status	The status of the terminal device, including Online and Offline: • Online: The terminal device is up and connected to the switch.

	• Offline: The terminal device is down or isn't connected to the switch.
MAC Address	The MAC address of the terminal device.
IP Address	The IP address of the terminal device.
Port	The port to connect to the terminal device.
Manufacturer	The manufacturer of the terminal device.
Terminal Type	The type of the terminal device such as PCs, printers, cameras, smartphones, tablets, IP phones, or a custom type that you defined.

Alerts

AmpCon-Campus uses telemetry data to issue immediate alerts on a visual interface when a device failure or a performance shift is detected, to help the network administrators diagnose the root cause 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:

NOTE

For switches of the following models, the alert feature is not supported:

- S3410L-24TF
- S3410L-24TF-P
- S3410-24TS
- S3410-24TS-P
- S3410C-16TF
- S3410C-16TF-P
- S3410C-16TMS-P
- S3410C-8TMS-P
- S3270-10TM
- S3270-24TM
- S3270-48TM
- S3270-10TM-P
- S3270-24TM-P



访问此内容时出现问题



请检查网络连接，[刷新](#)，然后重试。如果问题仍然存在，请联系您的管理员寻求帮助。

Alert Types and Levels

To check supported alert types and related alert levels, see the following tables:

[Packet Loss Alerts](#)

[Resource Usage Alerts](#)

[Interface Monitoring Alerts](#)

[Optical Module Alerts](#)

Packet Loss Alerts

Table 1. Packet Loss Alerts

Alert Metric	Description	Triggering Condition	Alert Level
In Errors	The number of incoming packets that contain errors and are dropped by a switch port increase	The metric value changes two times in the last four sampling cycles.	Error
Out Errors	The number of outgoing packets that a switch port fails to transmit successfully due to errors	The metric value changes two times in the last four sampling cycles.	Error
In Discards	The number of incoming packets that a switch port intentionally discards (drops) during processing	The metric value changes two times in the last four sampling cycles.	Error
Out Discards	The number of outgoing packets that a switch port intentionally discards (drops) before they are transmitted	The metric value changes two times in the last four sampling cycles.	Error

Resource Usage Alerts

Table 2. Resource Usage Alerts

Alert Metric	Description	Triggering Condition	Alert Level
CPU Usage	The CPU usage	The metric value exceeds 85%.	Warning

Memory Usage	The memory usage	The metric value exceeds 85%.	Warning
In Bandwidth Usage	The input bandwidth usage	The metric value exceeds 85%.	Warning
Out Bandwidth Usage	The output bandwidth usage	The metric value exceeds 85%.	Warning
Fan PWM Usage	The proportion of the fan's Pulse Width Modulation (PWM) to the total width	The metric value is over 85%.	Warning
RPSU Power-on	Whether the Power Supply Unit (PSU) is powered on or off	The metric value changes.	Info

Interface Monitoring Alerts

Table 3. Interface Monitoring Alerts

Alert Metric	Description	Triggering Condition	Alert Level
Admin Status	The port status (Up or Down) manually configured by the network administrator, including Up and Down	The metric value changes.	Info
Operation Status	The actual operational port status (Up or Down), which is detected by the switch	The metric value changes.	Warning
MTU	The largest size of a data packet that can be transmitted over a network without being fragmented. It's measured in bytes	The metric value changes.	Info
Loopback Mode	Whether the loopback mode is enabled on this port	The metric value changes.	Info

Duplex Mode	Whether data can flow in one direction (half duplex) at a time or both directions (full duplex) simultaneously	The metric value changes.	Warning
Port Speed	The maximum data transfer rate that the port can support	The metric value changes.	Warning

Optical Module Alerts

Table 4. Optical Module Alerts

Alert Metric	Description	Triggering Condition	Alert Level
Laser Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C)	The metric value exceeds 90 °C.	Warning
Tx Power	The amount of optical power delivered by the optical module connected to the switch port	The metric value is not in the output power range. See the Tx Power and Rx Power Ranges section.	Warning
Rx Power	The amount of optical power consumed by the optical module connected to the switch port	The metric value is not in the input power range. See the Tx Power and Rx Power Ranges section.	Warning
Power Budget	The difference between the output power and the input power	The metric value changes.	Info

Table 5. Tx Power and Rx Power Ranges

Optical Module Type	Input Power Range	Output Power Range
CFP	Min: -10, Max: 0	Min: -8, Max: 2
CFP2	Min: -10, Max: 0	Min: -8, Max: 2
CFP2_ACO	Min: -10, Max: 0	Min: -5, Max: 5
CFP4	Min: -10, Max: 0	Min: -8, Max: 2
QSFP	Min: -10, Max: 0	Min: -8, Max: 2
QSFP28	Min: -10, Max: 0	Min: -8, Max: 2
QSFP28_DD	Min: -10, Max: 0	Min: -8, Max: 2
QSFP56	Min: -10, Max: 0	Min: -8, Max: 2
QSFP56_DD	Min: -10, Max: 0	Min: -8, Max: 2
QSFP56_DD_TY PE1	Min: -10, Max: 0	Min: -8, Max: 2
QSFP56_DD_TY PE2	Min: -10, Max: 0	Min: -8, Max: 2
QSFP_PLUS	Min: -10, Max: 0	Min: -8, Max: 2
SFP	Min: -17, Max: -1	Min: -9, Max: -1
SFP_PLUS	Min: -17, Max: -1	Min: -9, Max: -1
SFP28	Min: -12, Max: -1	Min: -8, Max: 4
SFP56	Min: -12, Max: -1	Min: -8, Max: 4
SFP_DD	Min: -12, Max: -1	Min: -8, Max: 4
CPAK	Min: -10, Max: 0	Min: -8, Max: 2
CSFP	Min: -17, Max: -1	Min: -9, Max: -1
DSFP	Min: -12, Max: -1	Min: -8, Max: 4
XFP	Min: -10, Max: 0	Min: -8, Max: 2
X2	Min: -10, Max: 0	Min: -8, Max: 2

OSFP	Min: -10, Max: 0	Min: -8, Max: 2
-------------	------------------	-----------------

Checking the Alert List

AmpCon-Campus uses monitoring data to predict equipment failures and performance anomalies and then trigger immediate alerts. By checking these alerts, you can take corrective actions before issues are escalated.

[Supported Alert Types and Levels](#)

[Viewing Alerts](#)

[Viewing All Unread Alerts](#)

[Marking Unread Alerts as Read](#)

[Viewing All Unread "Error" Alerts](#)

[Viewing All Unread "Warning" Alerts](#)

[Viewing All Unread "Info" Alerts](#)

[Viewing All Alerts](#)

[Filtering Alerts](#)

Supported Alert Types and Levels

AmpCon-Campus supports the following alert levels:

- **Error**
- **Warning**
- **Info**

AmpCon-Campus supports the following alert types:

- Packet Loss Alert
- Resource Usage Alert
- Interface Monitoring Alert
- Optical Module Alert

For detailed alerts and related alert levels, see [Alert Types and Levels](#).

Viewing Alerts

Viewing All Unread Alerts

In the AmpCon-Campus UI, click **Monitor > Alerts > Alert List**. You can see all unread alerts.

Alert List							
All Messages		Mark Selected as Read		Q Search			
☐	Last Time	Switch SN	Type	Message	Count	Operation	
☐	2025-09-02 09:15:38	CNDJ0FTFOND00088M0359	Warning	The switch is offline	2	Mark as Read	
☐	2025-08-26 10:02:24	G184211001031	Warning	The switch is offline	2	Mark as Read	
☐	2025-08-26 04:27:26	CNDJ0FTFOND00088M0359	Info	The switch is online	1	Mark as Read	
☐	2025-08-26 04:27:26	G184211001031	Info	The switch is online	1	Mark as Read	
☐	2025-08-31 22:00:49	G1SA1X0000291	Info	The switch is online	2	Mark as Read	
☐	2025-08-29 02:25:37	G1S08R300011C	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 02:33:13	CNDJ0FTFOND00088M0359	Error	ey test key:ERROR: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 02:48:36	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 03:56:26	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	2	Mark as Read	

Marking Unread Alerts as Read

- To mark one unread alert as read, locate the alert, and then click **Mark as Read**.
- To mark multiple unread alerts as read, select these alerts, and then click **Mark Selected as Read**.
- To mark all unread alerts as read, click the square in the top to automatically select all unread alerts, and then click **Mark Selected as Read**.

Alert List							
All Messages		Mark Selected as Read		Q Search			
☐	Last Time	Switch SN	Type	Message	Count	Operation	
☒	2025-09-02 09:15:38	CNDJ0FTFOND00088M0359	Warning	The switch is offline	2	Mark as Read	
☒	2025-08-26 10:02:24	G184211001031	Warning	The switch is offline	2	Mark as Read	
☒	2025-08-26 04:27:26	CNDJ0FTFOND00088M0359	Info	The switch is online	1	Mark as Read	
☐	2025-08-26 04:27:26	G184211001031	Info	The switch is online	1	Mark as Read	
☐	2025-08-31 22:00:49	G1SA1X0000291	Info	The switch is online	2	Mark as Read	
☐	2025-08-29 02:25:37	G1S08R300011C	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 02:33:13	CNDJ0FTFOND00088M0359	Error	ey test key:ERROR: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 02:48:36	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 03:56:26	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	2	Mark as Read	

Viewing All Unread "Error" Alerts

Click the red flame icon, and then you can see all unread "error" alerts.

Alert List							
All Messages		Mark Selected as Read		Q Search			
☒	Last Time	Switch SN	Type	Message	Count	Operation	
☐	2025-09-02 09:15:38	CNDJ0FTFOND00088M0359	Warning	The switch is offline	2	Mark as Read	
☒	2025-08-26 10:02:24	G184211001031	Warning	The switch is offline	2	Mark as Read	
☒	2025-08-26 04:27:26	CNDJ0FTFOND00088M0359	Info	The switch is online	1	Mark as Read	
☐	2025-08-26 04:27:26	G184211001031	Info	The switch is online	1	Mark as Read	
☐	2025-08-31 22:00:49	G1SA1X0000291	Info	The switch is online	2	Mark as Read	
☐	2025-08-29 02:25:37	G1S08R300011C	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 02:33:13	CNDJ0FTFOND00088M0359	Error	ey test key:ERROR: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 02:48:36	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	1	Mark as Read	
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read	
☐	2025-08-29 03:56:26	G1SA1X0000291	Error	failed apply config to switch G1SA1X0000291, reason: auth error, Config: set system login user a dmin authentication public key test key "AAAA3NacC1yc2EAAAADAQABAAQDaw2dP32QK3ZbX1L0d8=TR9p1YTFbmDcmRnRt3dmN5Y6Lg= ...	2	Mark as Read	

Viewing All Unread "Warning" Alerts

Click the orange warning icon, and then you can see all unread "warning" alerts.

Monitor > Alerts > Alert List

13 4 4 admin

Alert List

All Messages Mark Selected as Read

Q Search

	Last Time	Switch SN	Type	Message	Count	Operation
☐	2025-09-02 09:15:38	CNDJFTFOND0088M0359	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 10:02:24	G184211001001	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 04:27:26	CNDJFTFOND0088M0359	Info	The switch is online	1	Mark as Read
☐	2025-08-26 04:27:26	G184211001001	Info	The switch is online	1	Mark as Read
☐	2025-08-31 22:00:49	G1SA3X0000291	Info	The switch is online	2	Mark as Read
☐	2025-08-29 02:25:37	G1SJR300011C	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 02:33:13	CNDJFTFOND0088M0359	Error	ev test key[ERROR]: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 02:46:36	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 03:56:26	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg=P_...	2	Mark as Read

1-10 of 30 items 1 2 3 10 / page

Viewing All Unread "Info" Alerts

Click the blue bell icon, and then you can see all unread "info" alerts.

Monitor > Alerts > Alert List

13 4 4 admin

Alert List

All Messages Mark Selected as Read

Q Search

	Last Time	Switch SN	Type	Message	Count	Operation
☐	2025-09-02 09:15:38	CNDJFTFOND0088M0359	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 10:02:24	G184211001001	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 04:27:26	CNDJFTFOND0088M0359	Info	The switch is online	1	Mark as Read
☐	2025-08-26 04:27:26	G184211001001	Info	The switch is online	1	Mark as Read
☐	2025-08-31 22:00:49	G1SA3X0000291	Info	The switch is online	2	Mark as Read
☐	2025-08-29 02:25:37	G1SJR300011C	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 02:33:13	CNDJFTFOND0088M0359	Error	ev test key[ERROR]: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 02:46:36	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 03:56:26	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg=P_...	2	Mark as Read

1-10 of 30 items 1 2 3 10 / page

Viewing All Alerts

Click **All Messages**, and then you can see all alerts.

Alert List

All Messages Mark Selected as Read

Q Search

	Last Time	Switch SN	Type	Message	Count	Operation
☐	2025-09-02 09:15:38	CNDJFTFOND0088M0359	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 10:02:24	G184211001001	Warning	The switch is offline	2	Mark as Read
☒	2025-08-26 04:27:26	CNDJFTFOND0088M0359	Info	The switch is online	1	Mark as Read
☐	2025-08-26 04:27:26	G184211001001	Info	The switch is online	1	Mark as Read
☐	2025-08-31 22:00:49	G1SA3X0000291	Info	The switch is online	2	Mark as Read
☐	2025-08-29 02:25:37	G1SJR300011C	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 02:33:13	CNDJFTFOND0088M0359	Error	ev test key[ERROR]: path "system login user admin authentication public key" is not valid, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 02:46:36	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg= ...	1	Mark as Read
☐	2025-08-29 03:21:37	G1S713N00017A	Warning	The switch is offline	1	Mark as Read
☐	2025-08-29 03:56:26	G1SA3X0000291	Error	failed apply config to switch G1SA3X0000291, reason: auth error, Config: set system login user admin authentication public key test key "AAAA3NzAc1yc2EAAAADAQABAAQAw2oGP32QK5ZbXK1OdH=TR9p1YTFBmDccmRnRtdmN5YkLg=P_...	2	Mark as Read

1-10 of 30 items 1 2 3 10 / page

Click **Back to Alerts**, and then you can see all unread alerts.

Alert List							
Back to Alerts		Remove Selected		Q Search			
☐	Last Time	Switch SN	Type	Message	Count	Operation	
☐	2025-08-16 12:19:48	G15713N00017A	Warning	The switch is offline	7	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Info	The switch is online	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Info	switch G15713N00017A deploy success	1	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/1 on switch G15713N00017A port-speed change to 100GB	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/3 on switch G15713N00017A oper-status change to UP	5	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/4 on switch G15713N00017A oper-status change to UP	4	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/4 on switch G15713N00017A port-speed change to 100GB	4	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/1 on switch G15713N00017A oper-status change to UP	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/2 on switch G15713N00017A port-speed change to 100GB	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/2 on switch G15713N00017A oper-status change to UP	2	Remove	

5-10 of 119 items 1 2 3 4 5 ... 12 30 / page

Filtering Alerts

On the “Alert List” page, you can filter alerts by using the filter icon in the **Last Time**, **Switch SN**, or **Type** column.

Alert List							
Back to Alerts		Remove Selected		Q Search			
☐	Last Time	Switch SN	Type	Message	Count	Operation	
☐	2025-08-16 12:19:48	G15713N00017A	Warning	The switch is offline	7	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Info	The switch is online	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Info	switch G15713N00017A deploy success	1	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/1 on switch G15713N00017A port-speed change to 100GB	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/3 on switch G15713N00017A oper-status change to UP	5	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/4 on switch G15713N00017A oper-status change to UP	4	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/4 on switch G15713N00017A port-speed change to 100GB	4	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/1 on switch G15713N00017A oper-status change to UP	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/2 on switch G15713N00017A port-speed change to 100GB	2	Remove	
☐	2025-08-18 17:32:00	G15713N00017A	Warning	Found interface: xe-1/3/2 on switch G15713N00017A oper-status change to UP	2	Remove	

5-10 of 119 items 1 2 3 4 5 ... 12 30 / page

Alert Notifications

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:

- [Alerting Notification Guide](#)
- [Configuring an SMTP Server](#)
- [Configuring Notification Rules](#)
- [Viewing Historical Alert Notification Logs](#)

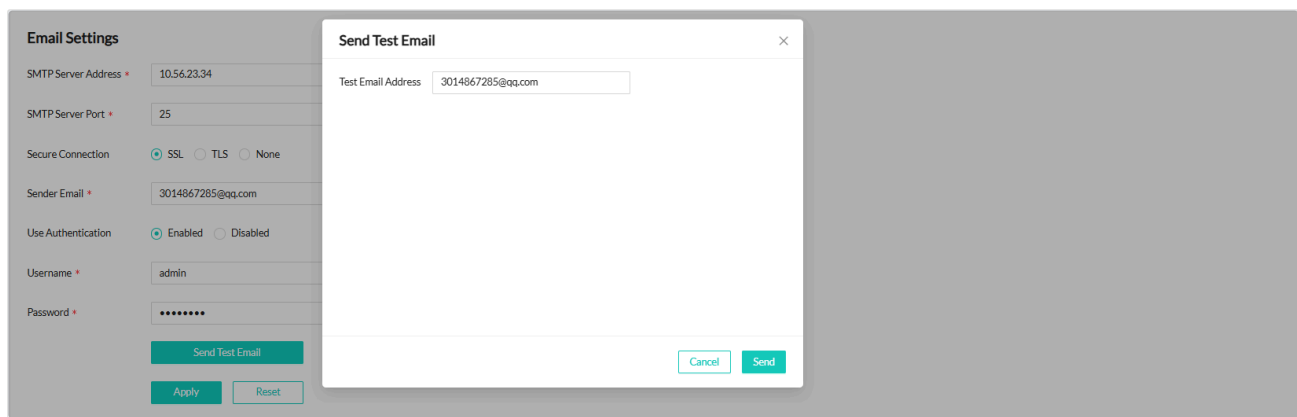
Alerting Notification Guide

If you need to be notified immediately when alerts happen, you can enable the alert notification feature to receive real-time notifications through emails.

1. [Configuring an SMTP Server](#)
2. [Configuring Notification Rules](#)
3. [Viewing Alert Notification History](#)

1. Configuring an SMTP Server

To receive alert notifications through emails, you need to configure an SMTP server first. For more information, see [Configure an SMTP Server](#).

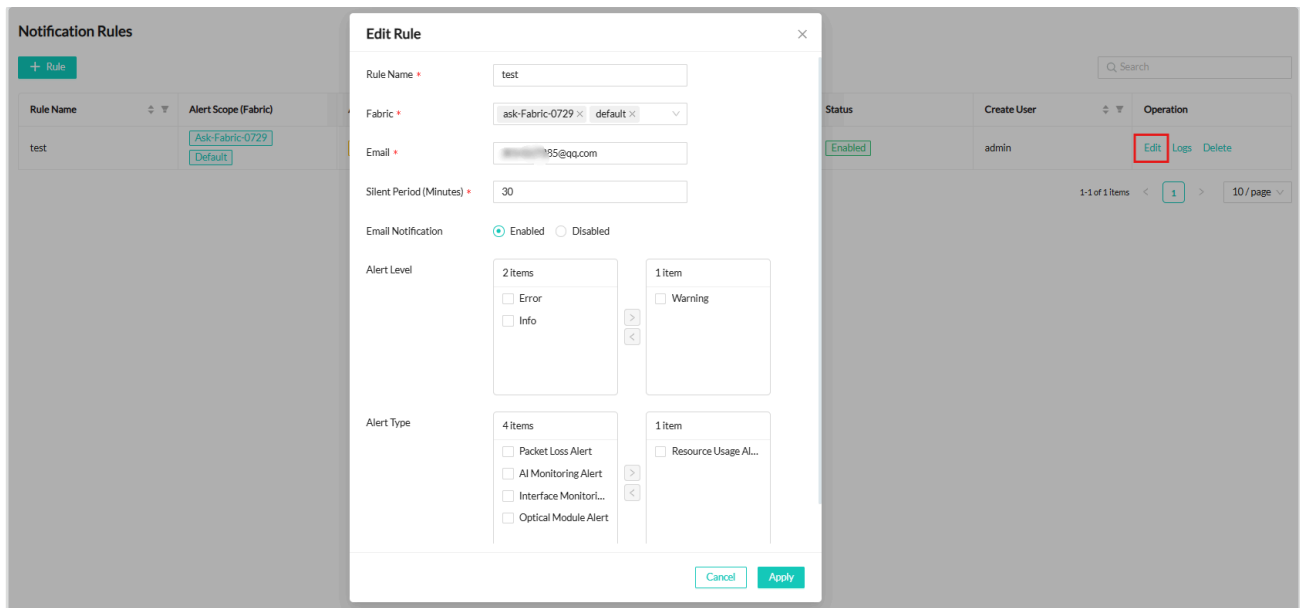


The screenshot shows the 'Email Settings' configuration page on the left and a 'Send Test Email' dialog box on the right. The 'Email Settings' page includes fields for SMTP Server Address (10.56.23.34), SMTP Server Port (25), Secure Connection (SSL selected), Sender Email (3014867285@qq.com), Use Authentication (Enabled selected), Username (admin), and Password (masked). There are buttons for 'Send Test Email', 'Apply', and 'Reset'. The 'Send Test Email' dialog box has a 'Test Email Address' field containing '3014867285@qq.com' and 'Cancel' and 'Send' buttons.

2. Configuring Notification Rules

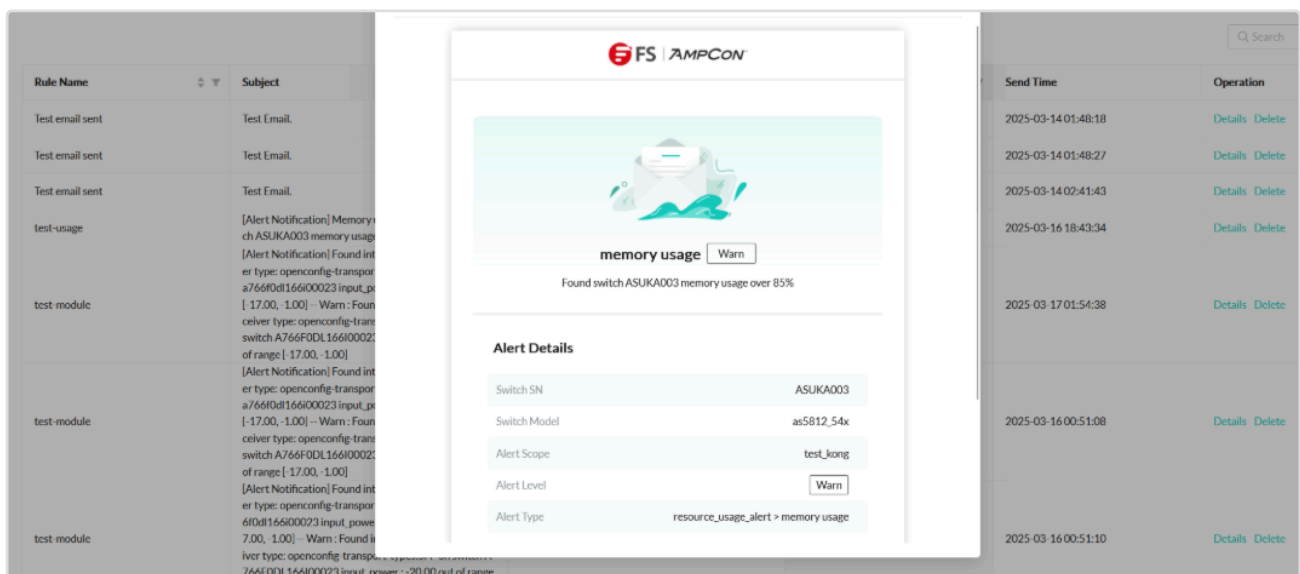
Configure notification rules to define the alert types, alert levels, and fabrics to be monitored and to designate the email address to be notified. For more information, see [Configuring Notification Rules](#).

Once done, alert notifications will be sent to the designated email address. You can get notified immediately when issues happen and then take correction actions to prevent issue escalation.



3. Viewing Alert Notification History

View all historical alert notifications sent in the last 30 days for root cause analysis or auditing. For more information, see [Viewing Historical Alert Notification Logs](#).



Configuring an SMTP Server

Simple Mail Transfer Protocol (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 need to configure an SMTP server first.

[Supported Information](#)

[Adding an SMTP Server](#)

[Optional: Editing an SMTP Server](#)

[Optional: Resetting an SMTP Server](#)

Supported Information

- AmpCon-Campus supports mainstream email service providers like Outlook and Gmail.
- AmpCon-Campus supports using email encryption transmission or not (SSL, TLS, or none).

Adding an SMTP Server

To add an SMTP server, follow these steps:

NOTE

When you add an SMTP server, ensure to send a test email and check whether the email can be received by the receiver.

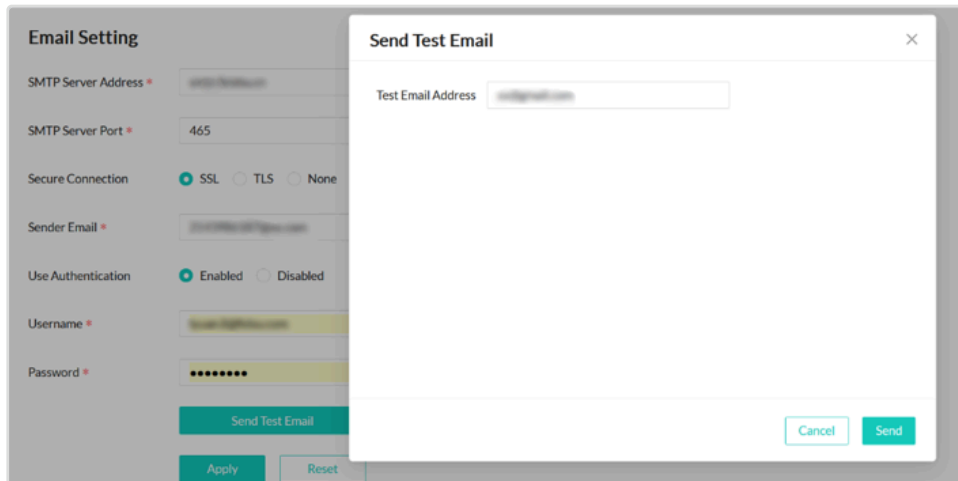
1. Click **System > Email Settings** in the AmpCon-Campus UI.
2. On the “Email Settings” page, input the following information:
 - **SMTP Server Address:** The hostname or IP address of the SMTP Server.
 - **SMTP Server Port:** The TCP port number to connect to the SMTP Server.
 - **Secure Connection:** The encryption method for secure email transmission, including **SSL**, **TLS**, or **None**. **None** means that the emails sent to this SMTP server are not encrypted.
 - **Sender Email:** The email address to send a test email.
 - **Use Authentication:** Select **Enabled** or **Disabled**. The default value is **Disabled**.
 - **Enabled:** The SMTP server requires authentication for logged-in users. If you selected **Enabled**, 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.
 - **Disabled:** The SMTP server doesn't require authentication for logged-in users.

NOTES

- If you selected **SSL** or **TLS** in the **Secure Connection** section, you must select **Enabled**.
- If you selected **None** in the **Secure Connection** section, you must select **Disabled**.

3. Click **Send Test Email**.

4. In the **Test Email Address** field of the pop-up window, enter the email address of the receiver.



5. Click **Send**.

6. Ensure that the test email can be received by the receiver.

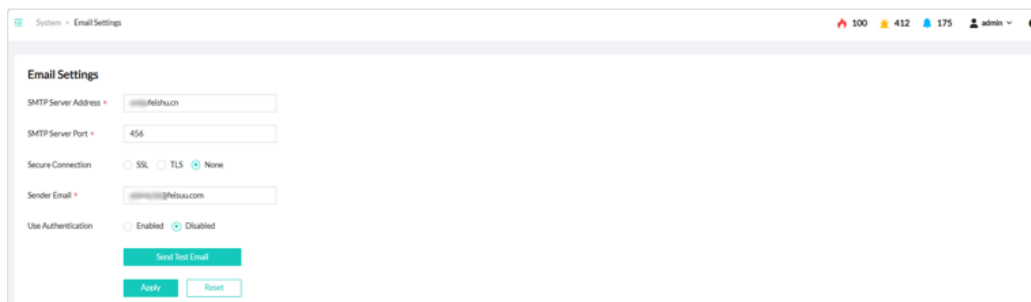
7. Click **Apply** to complete the SMTP server configuration.

Optional: Editing an SMTP Server

To edit an SMTP server, modify the configurations on the “Email Settings” page as needed, and then click **Apply**.

NOTE

Do not forget to send a test email and check whether the email can be received by the receiver.



Optional: Resetting an SMTP Server

To reset SMTP server configurations, click **Reset** on the “Email Settings” page.

NOTE

After you reset SMTP server configurations, configure a new SMTP server. Or else, AmpCon-Campus will still use the previous SMTP server configurations.

The screenshot shows the "Email Settings" page in the AmpCon-Campus interface. The page has a header with "System > Email Settings" and a top right corner with statistics (100, 412, 175) and a user profile (admin). The main content area is titled "Email Settings" and contains the following fields and options:

- SMTP Server Address:
- SMTP Server Port:
- Secure Connection: ☐ SSL ☐ TLS ☒ None
- Sender Email:
- Use Authentication: ☐ Enabled ☒ Disabled

At the bottom of the form, there are three buttons: "Send Test Email" (green), "Apply" (green), and "Reset" (green). The "Reset" button is highlighted with a red rectangular box.

Configuring Notification Rules

After you configure an SMTP server, configure notification rules. In notification rules, specify the alert types, alert levels, and sites to be monitored. You are informed of these specified alerts when they are triggered.

[Adding Notification Rules](#)

[Viewing Notification Rules](#)

[Optional: Editing Notification Rules](#)

[Optional: Deleting Notification Rules](#)

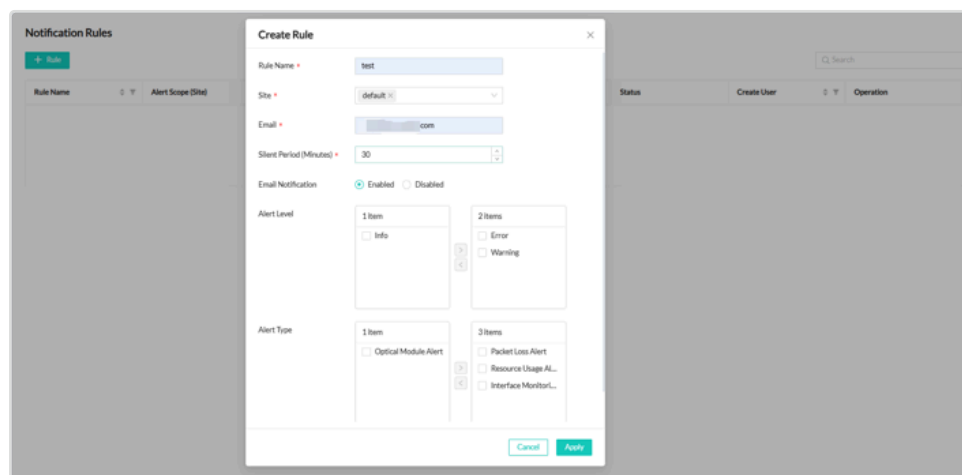
Adding Notification Rules

To add a notification rule, follow these steps:

NOTE

At most 100 notification rules can be added.

1. Click **Monitor > Alerts > Notification Rules** in the AmpCon-Campus UI.
2. On the “Notification Rules” page, click **+ Rule**.
3. In the pop-up window, input the following information:



- **Rule Name:** The name of the rule. The rule name needs to be unique.
- **Site:** The sites to be monitored. You can select one or multiple sites.
- **Email:** The email addresses of the receivers to be notified. You can enter one or multiple email addresses, which need to be separated by commas (,).
- **Silent Period (Minutes):** The period (in minutes) during which the same alert notification is not sent repeatedly.

To prevent email bombing, set the silent period to at least 30 minutes. If you set the silent period to a value less than 30, the silent period is changed to 30 automatically.

- **Email Notification:** Whether to enable email notifications.
 - **Enabled:** Alert notifications will be sent to the receiver email address and will be displayed on the “Notification History” page.
 - **Disabled:** Alert notifications will not be sent to the receiver email address and will not be displayed on the “Notification History” page.

NOTES

- If you selected **Enabled** to enable email notifications, only the selected levels and types of alerts can be sent to the receiver email address and displayed on the “Notification History” page. For how to select alert levels and alert types, see **step 4** and **step 5**.
- All triggered alerts can be displayed on the “Alert List” page no matter you enabled email notifications or not.

4. In the **Alert Level** section, 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 **<**.

5. In the **Alert Type** section, 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 **<**.

For supported alert types and alert levels, see [Alert Types and Levels](#).

4. Click **Apply**.

Viewing Notification Rules

On the “Notification Rules” page, you can see the following information:

Rule Name	Alert Scope (Site)	Alert Level	Alert Type	Silent Period (Minutes)	Status	Create User	Operation
test	Default	Error Warning	Packet Loss Alert Resource Usage Alert Interface Monitoring Alert	30	Enabled	admin	Edit Logs Delete

Table 1. Notification Rule Metrics

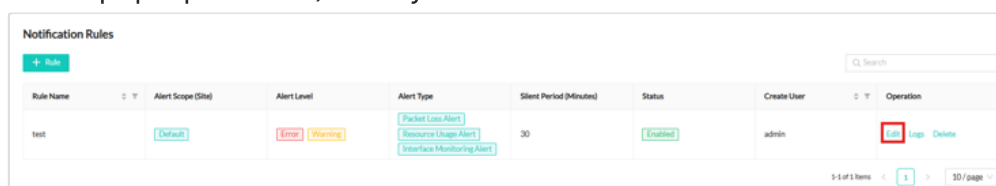
Metric	Description
Rule Name	The name of the rule.

Alert Scope (Site)	The site to be monitored.
Alert Level	The levels of alerts to be monitored, including Warning , Error , and Info .
Alert Type	The types of alerts to be monitored.
Silent Period (Minutes)	The period (in minutes) during which the same alert notification is not sent repeatedly.
Status	Whether alert notifications can be sent to the receiver's email address.
Create User	The AmpCon-Campus user who created the alert notification rule.

Optional: Editing Notification Rules

To edit a notification rule, follow these steps:

1. Locate the rule on the “Notification Rules” page, and then click **Edit**.
2. In the pop-up window, modify the rule as needed.

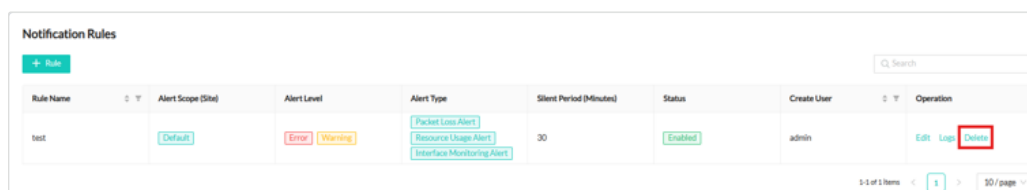


Rule Name	Alert Scope (Site)	Alert Level	Alert Type	Silent Period (Minutes)	Status	Create User	Operation
test	Default	Error Warning	Packet Loss Alert Resource Usage Alert Interface Monitoring Alert	30	Enabled	admin	Edit Logs Delete

3. Click **Apply**.

Optional: Deleting Notification Rules

To delete a notification rule, locate the rule on the “Notification Rules” page, and then click **Delete**.



Rule Name	Alert Scope (Site)	Alert Level	Alert Type	Silent Period (Minutes)	Status	Create User	Operation
test	Default	Error Warning	Packet Loss Alert Resource Usage Alert Interface Monitoring Alert	30	Enabled	admin	Edit Logs Delete

Viewing Historical Alert Notification Logs

You can view all alert notifications sent in the last 30 days for root cause analysis, fault prevention, or auditing.

[Checking Historical Alert Notifications](#)

[Deleting Historical Alert Notifications](#)

Checking Historical Alert Notifications

To check historical alert notifications, follow these steps:

1. Click **Monitor > Alerts > Notification History** in the AmpCon-Campus UI.

On the “Notification History” page, you can see all the historical alert notifications that are sent in the last 30 days.

Rule Name	Subject	Receivers	Status	Send Time	Operation
interface	【Alert Notification】 Output power input power - Info: Found interface: xe-1/1/5 on switch 581254K000023 output_power input_power changed from: 2.80 to: 2.79		Failed	2025-03-22 20:55:33	Delete
interface	【Alert Notification】 Interface in discards count - Error: Found interface: te-1/1/2 on switch 65FDC8D343A6 in discards increased		Failed	2025-03-21 08:30:59	Delete
interface	【Alert Notification】 Admin-status - Info: Fa und interface: te-1/1/1 on switch A9UKA003 ad min status change to DOWN		Success	2025-03-21 07:54:46	Details Delete
test-Packet Loss Alert	【Alert Notification】 Interface in discards count - Error: Found interface: te-1/1/1 on switch 65 FDC8D343A3 in discards increased		Success	2025-03-18 04:26:55	Details Delete

Table 1. Notification History Metrics

Metric	Description
Rule Name	The name of the alert notification rule
Subject	The alert levels and alert types
Receivers	The email addresses of the receivers to be notified
Status	Whether the email is sent to the receivers successfully
Send Time	The time when the alert notification email is sent

2. To view the email contents of a historical alert notification, locate the alert notification, and then click **Details**.

Rule Name	Subject
test_email_sent	Test Email.
test_email_sent	Test Email.
test_email_sent	Test Email.
test_usage	[Alert Notification] Memory usage ASUKA003 memory usage
test_module	[Alert Notification] Found input type: openconfig:transpo a766f0d16600023 input, p [17.00, 1.00] - Warn: Four
test_module	[Alert Notification] Found input type: openconfig:transpo a766f0d16600023 input, p [17.00, 1.00] - Warn: Four
test_module	[Alert Notification] Found input type: openconfig:transpo a766f0d16600023 input, p [17.00, 1.00] - Warn: Four
test_module	[Alert Notification] Found input type: openconfig:transpo a766f0d16600023 input, p [17.00, 1.00] - Warn: Four
test_module	[Alert Notification] Found input type: openconfig:transpo a766f0d16600023 input, p [17.00, 1.00] - Warn: Four

FS | AMPCON



memory usage Warn

Found switch ASUKA003 memory usage over 83%

Alert Details

Switch SN	ASUKA003
Switch Model	ar5812.54x
Alert Scope	test_long
Alert Level	Warn
Alert Type	resource_usage_alert - memory usage

Send Time	Operation
2025-03-14 01:48:18	Details Delete
2025-03-14 01:48:27	Details Delete
2025-03-14 02:41:43	Details Delete
2025-03-16 18:43:34	Details Delete
2025-03-17 01:54:38	Details Delete
2025-03-16 00:51:08	Details Delete
2025-03-16 00:51:10	Details Delete

Deleting Historical Alert Notifications

To delete a historical alert notification, locate the alert notification, and click **Delete**.

Managing Groups and Sites

You can create a **group** and then add PicOS switches and users to the group so that these users can manage only the assigned PicOS switches in this group. In addition, you can also designate the operation permissions for a group so that the users and PicOS switches in the group can only perform the allowed operations.

When you import a PicOS switch or add a PicOS switch configuration, you need to select which **site** the PicOS switch belongs to. Then, after PicOS switches are managed by AmpCon-Campus, you can also add PicOS switches to a site or remove PicOS switches from a site as needed.

When you add access points (APs) to AmpCon-Campus, you also need to select which site the APs belong to.

See the following child topics:

- [Managing Groups](#)
- [Managing Sites](#)

Managing Groups

You can create a group and then add switches and users to the group so that these users can manage only the assigned switches in this group.

You can also designate the operation permissions for a group so that the users and switches in the group can only perform the allowed operations.

[Adding a Switch Group](#)

[Editing a Switch Group](#)

[Assigning Groups to a User](#)

[Viewing All Switch Groups](#)

[Viewing Users Managing a Group](#)

[Deleting a Switch Group](#)

Adding a Switch Group

To add a switch group, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Group Management**.
2. On the “Group Management” page, click **+ Create**.
3. In the pop-up window, input the following information:

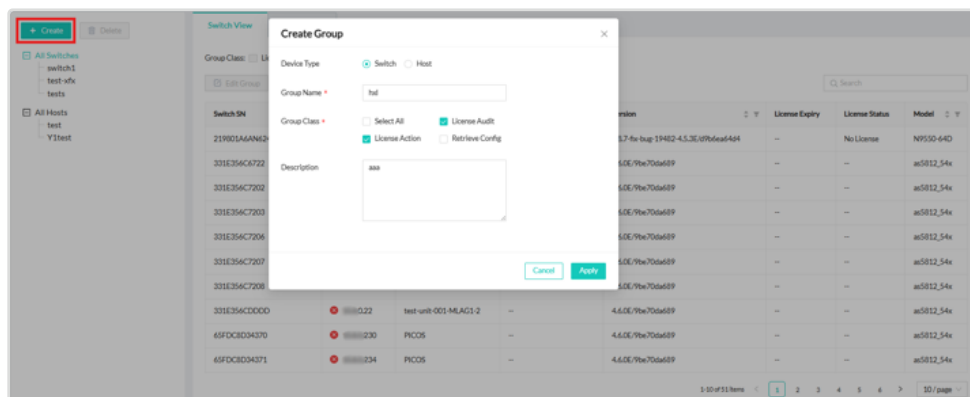


Table 1. Switch Group Parameters

Parameter	Description
Device Type	Select Switch to create a switch group.
Group Name	Specify the name of the switch group.
Group Class	Select one or multiple operation permissions allowed for switches in the switch group: • License Audit: You can perform the License Audit operation. • License Action: You can perform the License Action operation.

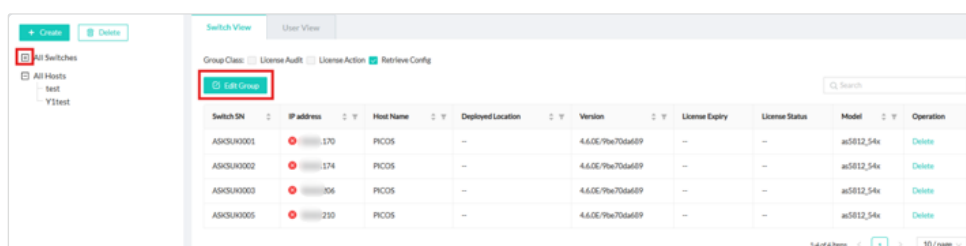
	• Retrieve Config: You can perform the configuration backup operation.
Description	Optional. Specify the description of the switch group.

4. Click **Apply**.

Editing a Switch Group

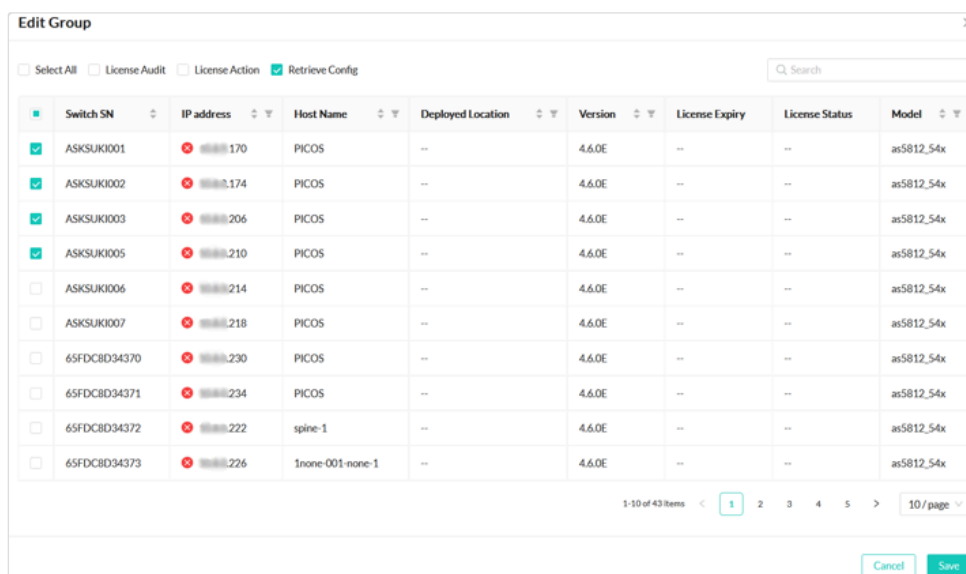
By editing a switch group, you can add switches to a group or remove switches from a group. In addition, you can modify the allowed operation permissions for switches in the group.

1. On the “Group Management” page, click **+** before **All Switches** in the left panel.
2. Click a switch group from the list.
3. In the **Switch View** tab, click **Edit Group**.



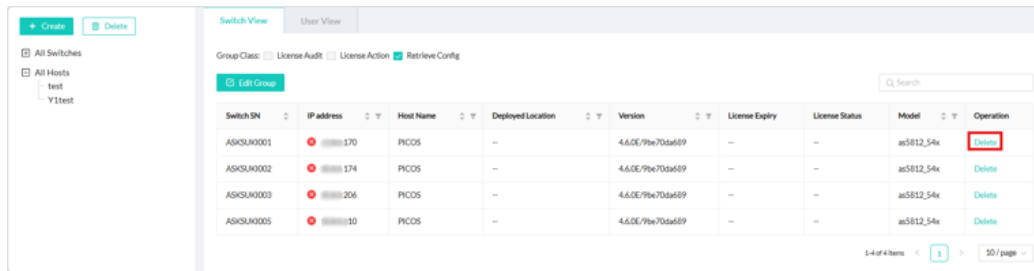
4. In the pop-up window, do the following operations:

- Select the switches to be added to the switch group.
- To remove switches from the switch group, unselect the switches.
- Select the allowed operation permissions, including **License Audit**, **License Action**, and **Retrieve Config**.



5. Click **Save**.

You can try another way to remove a switch from a switch group. In the **Switch View** tab, locate the switch, and then click **Delete**.

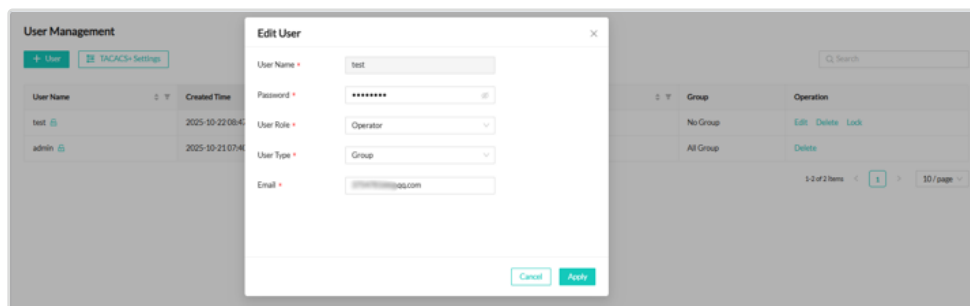


Assigning Groups to a User

After you add switch groups, you can assign switch groups to an existing or a new AmpCon-Campus group user. For more information about AmpCon-Campus users, see [Managing User Access](#).

To assign groups to an existing group user, follow these steps:

1. Click **System > User Management** from the navigation bar.
2. Locate the user, and then click **Edit**.
3. In the pop-up window, select **Group** in the **User Type** drop-down list.

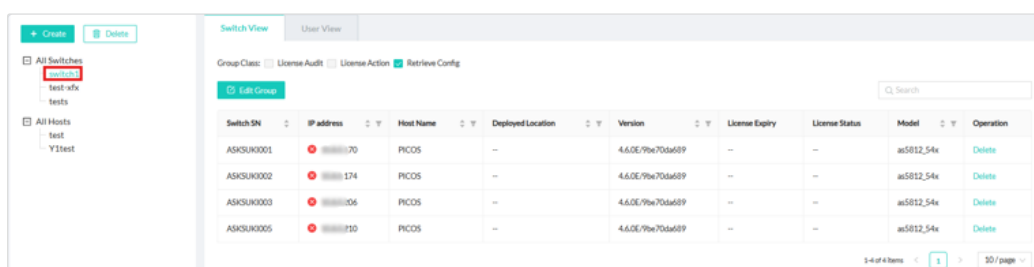


4. Click **Apply**.

Viewing All Switch Groups

To view all added switch groups, click **+** before **All** in the left panel of the “Group Management” page.

To view all switches in a switch group, click the switch group name, and then check the **Switch View** tab.

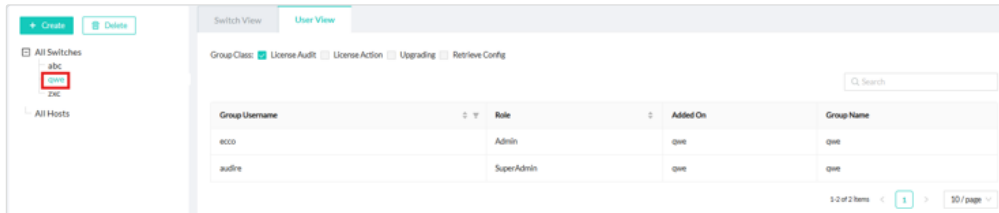


Viewing Users Managing a Group

You can view AmpCon-Campus users managing a switch group. If no users are listed, it means that you haven't assigned the group to any AmpCon-Campus users.

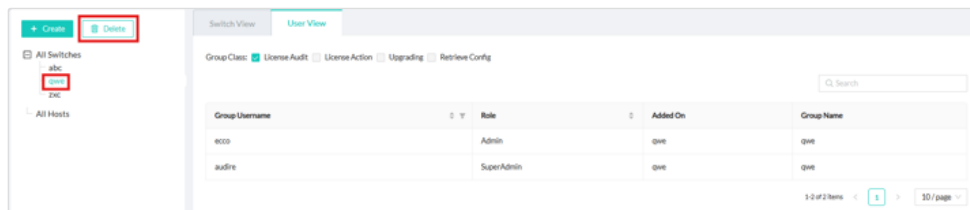
To view AmpCon-Campus users managing a switch group, follow these steps:

1. On the “Group Management” page, click **+** before **All**, and then click the switch group from the list.
2. Click the **User View** tab, and then check the users managing the switch group.



Deleting a Switch Group

1. On the “Group Management” page, click **+** before **All** in the left panel.
2. Click a switch group from the list, and then click **Delete**.



3. Click **Yes** to confirm the deletion.

Managing Sites

When you import a switch or add a switch configuration during the switch onboarding process, you must select which site the switch belongs to. After a switch is onboarded to AmpCon-Campus, you can also add the switch to another site.

When you add an access point (AP) to AmpCon-Campus, you must select which site the AP belongs to. After an AP is added to AmpCon-Campus, you can also add the AP to another site.

Topologies are created based on each site automatically. You can view the topology associated with switches in a site to check the linking of switches in the site.

[Guidelines](#)

[Adding a Site](#)

[Adding Switches to a Site](#)

[Removing Switches from a Site](#)

[Displaying the Topology Associated with a Site](#)

[Deleting a Site](#)

Guidelines

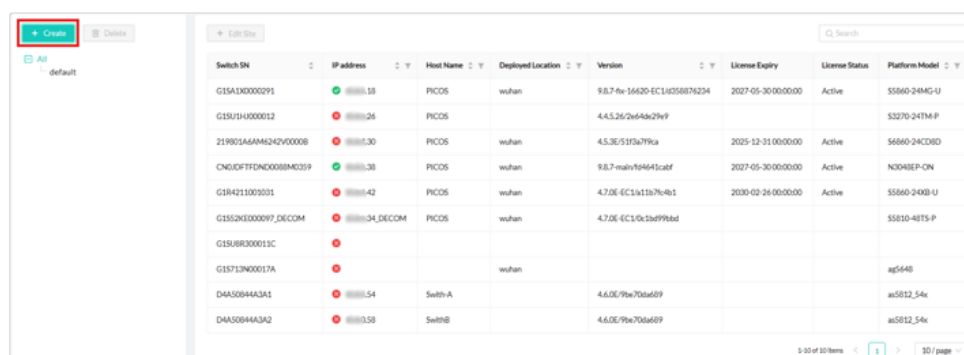
You must read the following guidelines:

- The site **default** is a built-in site. You can't edit it or remove switches from it directly.
- After you remove switches from any other sites, these switches are added to the **default** site automatically.
- After you add switches in the site **default** to any other sites, these switches are removed from the **default** site automatically.

Adding a Site

To add a site, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Site Management** from the navigation bar.
2. On the "Site Management" page, click **Create**.



Switch SN	IP Address	Host Name	Deployed Location	Version	License Expiry	License Status	Platform Model
G15A10000291	192.168.1.18	PC05	wuhan	9.8.7-6e15420-EC14055876234	2027-05-30 00:00:00	Active	S5660-24AG-U
G15U14000012	192.168.1.26	PC05		4.5.26/2e46a29e9			S3270-24TM-P
21981A6A6242V0000B	192.168.1.30	PC05	wuhan	4.5.36/515a791a	2025-12-31 00:00:00	Active	S6660-24CWD
CN0JFFDNDX0008M0359	192.168.1.38	PC05	wuhan	9.8.7-main104641catf	2027-05-30 00:00:00	Active	N3048EP-ON
G1R421100001	192.168.1.42	PC05	wuhan	4.7.0E-EC1a13167e4b1	2030-02-26 00:00:00	Active	S5660-24AB-U
G152K0000097_DECOM	192.168.1.54	PC05	wuhan	4.7.0E-EC15c1b4998bd			S5810-48TS-P
G15U6R300011C							
G15713N00017A			wuhan				ag54B
D4A50B44A3A1	192.168.1.54	Switch-A		4.6.0E/9be70da609			as5812_54e
D4A50B44A3A2	192.168.1.58	Switch-B		4.6.0E/9be70da609			as5812_54e

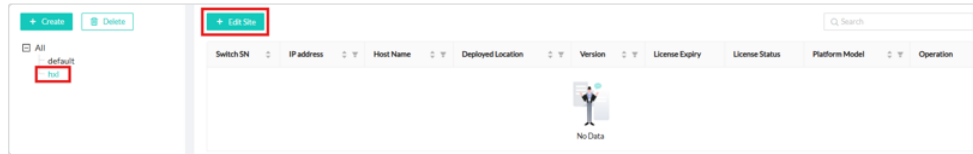
3. Enter the site name and the site description (optional).

4. Click **Apply**.

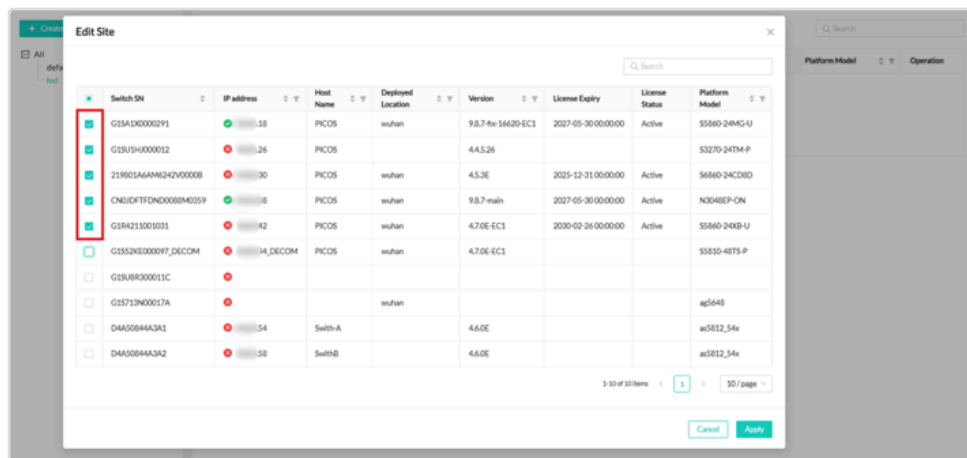
Adding Switches to a Site

To add switches to a site, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Site Management** from the navigation bar.
2. Click the site name, and then click **Edit Site**.



3. Select the switches to be added. You can filter switches by entering keywords in the search box.

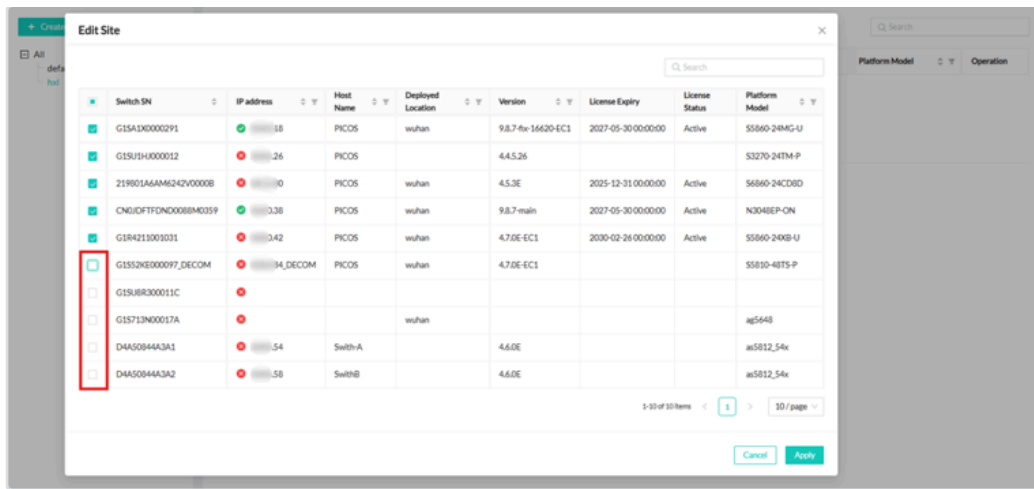


4. Click **Apply**.

Removing Switches from a Site

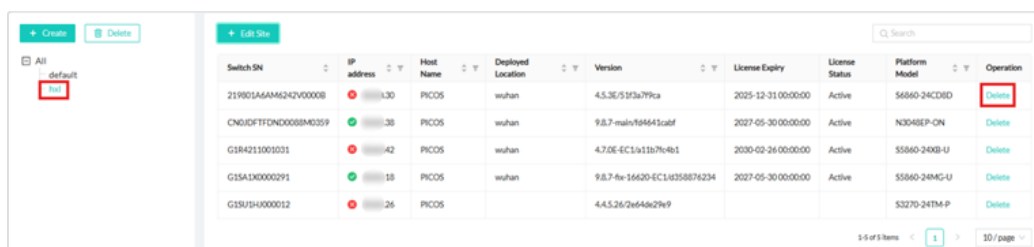
To remove switches from a site, follow these steps:

1. Click **Resource > Site Management** from the navigation bar.
2. Click the site name, and then click **Edit Site**.
3. In the pop-up window, unselect the switches to be removed. You can filter switches by entering keywords in the search box.



4. Click **Apply**.

You can use another way to remove a switch from a site. Click the site, locate the switch, and then click **Delete**.



Displaying the Topology Associated with a Site

To display the topology associated with a site, follow these steps:

1. In the AmpCon-Campus UI, click **Network Design > Topologies** from the navigation bar.
2. Click the corresponding site name. Then, you can see the topology graph of switches that belong to this site. For more information, see [Topology](#).



Deleting a Site

To delete a site, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Site Management** from the navigation bar.
2. On the "Site Management" page, click **Delete**.

CreateDelete

Alldefault

Edit Sns

Search

Switch SN	IP address	Host Name	Deployed Location	Version	License Expiry	License Status	Platform Model	Operation
21905A6A46242V0000B	30	PIC05	wuhan	4.5.3E/593a79fca	2025-12-31 00:00:00	Active	56860-24CD8D	Delete
CN0J0FTFDND00008M0359	8	PIC05	wuhan	9.8.7-main/f04641cadf	2027-05-30 00:00:00	Active	N3048EP-CN	Delete
G184211001001	42	PIC05	wuhan	4.7.0E-EC13x135764b1	2030-02-26 00:00:00	Active	55860-24XB-U	Delete
G15ALX0000291	18	PIC05	wuhan	9.8.7-8e-36620-EC14d358876234	2027-05-30 00:00:00	Active	55860-24MG-U	Delete
G15U1H-U000012	26	PIC05		4.4.5.26/2e648629e9			S3270-24TM-P	Delete

3 of 3 items110 / page

3. Click **Yes** to confirm the deletion.

Managing Licenses

In the AmpCon-Campus UI, you can manage AmpCon-Campus licenses and PicOS licenses.

For more information, see the following child topics:

- [Managing AmpCon-Campus Licenses](#)
- [Managing PicOS Licenses](#)

Managing AmpCon-Campus Licenses

You can import a new or updated AmpCon-Campus license to manage more switches, view all imported AmpCon-Campus licenses, convert a trial AmpCon-Campus license to a standard AmpCon-Campus license, invalidate the AmpCon-Campus license on a switch to release the license, or check license related logs and alerts.

See the following child topics:

NOTES

Before you import AmpCon-Campus licenses, pay attention to the following guidelines:

- The following AmpCon-Campus license types are supported:
 - **Trial license:** The trial period lasts for 90 days and an additional 14 days. After the trial license is expired, you must install a standard license to continue using AmpCon-Campus.
 - **Standard license:** After a standard license is installed, you cannot install a trial license.

Each AmpCon-Campus server supports managing only switches with the same license type.

- If AmpCon-Campus licenses are not imported or the imported AmpCon-Campus licenses are expired, some of the AmpCon-Campus features will not work, such as [Onboarding PicOS Switches](#).
- During the grace period of a trial AmpCon-Campus license, the AmpCon-Campus login interface displays "License is expired, you have a 14-day grace period". You can purchase a standard license to continue using AmpCon-Campus.
- Within 14 days before a standard AmpCon-Campus license expires, when you log in to the AmpCon-Campus UI, you will see the notification message "License ID: xx Some of the licenses are about to expire. If you wish to continue using this device, please renew the license. You can view the relevant information through the "License Alert" function."

In this case, go to the [License Alert section](#) of the AmpCon-Campus UI to check the expiring AmpCon-Campus license, and ask the sale team to renew the license in the License Portal. Then, download the renewed license, and import it to AmpCon-Campus.

Importing Licenses for Deployed Switches

To onboard switches through ZTP, you must import AmpCon-Campus licenses (containing the Hardware IDs of the switches) to AmpCon-Campus automatically or manually so that AmpCon-Campus can manage these switches.

Prerequisites

Importing Licenses Automatically

Importing Licenses Manually

1. Obtaining Hardware IDs in Batches
 2. Creating an AmpCon-Campus License
 3. Importing an AmpCon-Campus License to AmpCon-Campus
- Optional: Editing an AmpCon-Campus License

Prerequisites

- For white-box switches to be deployed, ensure that all the preparations in [Before You Begin](#) and **Step 1** to **Step 6** in [Provisioning a White-Box Switch](#) are completed.
- For integrated hardware and software switches to be deployed, ensure that all the preparations in [Before You Begin](#) and **Step 1** to **Step 4** in [Provisioning an Integrated Hardware and Software Switch](#) are completed.

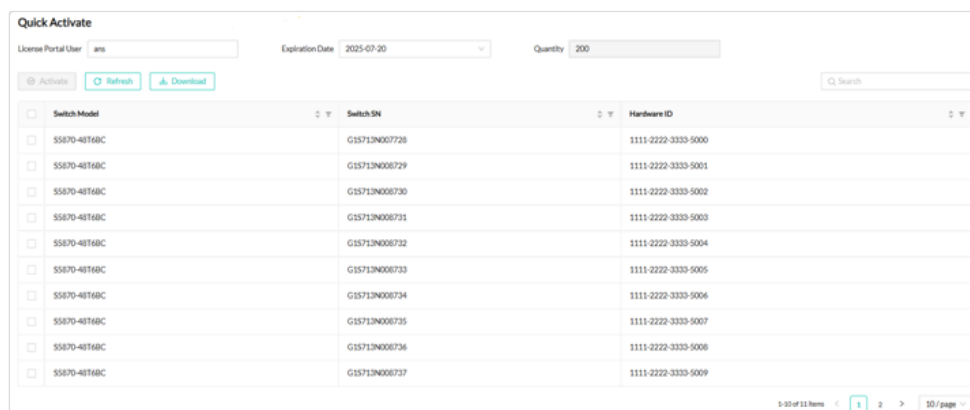
Importing Licenses Automatically

When AmpCon-Campus is stably connected to the License Portal, you can import AmpCon-Campus licenses to AmpCon-Campus automatically, eliminating the need for complex manual processes.

This feature significantly reduces time and operational costs, streamlines management, and is especially beneficial for large-scale switch license management scenarios.

To import an AmpCon-Campus license automatically, follow these steps:

1. Click **System > Software Licenses > Licenses Management** from the navigation bar, and then click **Quick Activate**. You can see all switches provisioned with ZTP and without AmpCon-Campus license assigned.



The screenshot shows the 'Quick Activate' interface. At the top, there are input fields for 'License Portal User' (ams), 'Expiration Date' (2025-07-20), and 'Quantity' (200). Below these are buttons for 'Activate', 'Refresh', and 'Download'. A search bar is also present. The main part of the interface is a table with three columns: 'Switch Model', 'Switch SN', and 'Hardware ID'. The table contains 11 rows of data, all with the same switch model 'S5870-48T6BC'. The switch SNs range from G15713N000728 to G15713N000737, and the hardware IDs range from 1111-2222-3333-5000 to 1111-2222-3333-5009. At the bottom right, there is a pagination bar showing '5-10 of 11 items' and a page number '1'.

Switch Model	Switch SN	Hardware ID
☐ S5870-48T6BC	G15713N000728	1111-2222-3333-5000
☐ S5870-48T6BC	G15713N000729	1111-2222-3333-5001
☐ S5870-48T6BC	G15713N000730	1111-2222-3333-5002
☐ S5870-48T6BC	G15713N000731	1111-2222-3333-5003
☐ S5870-48T6BC	G15713N000732	1111-2222-3333-5004
☐ S5870-48T6BC	G15713N000733	1111-2222-3333-5005
☐ S5870-48T6BC	G15713N000734	1111-2222-3333-5006
☐ S5870-48T6BC	G15713N000735	1111-2222-3333-5007
☐ S5870-48T6BC	G15713N000736	1111-2222-3333-5008
☐ S5870-48T6BC	G15713N000737	1111-2222-3333-5009

2. Optional: To manually refresh the list of switches with no AmpCon-Campus license assigned, click **Refresh**.

i NOTE

You are recommended to manually refresh the list of switches with no AmpCon-Campus license assigned. Reasons are as follows:

- If the network is available and stable, AmpCon-Campus will automatically retrieve the latest **Expiration Date** and **Quantity** information from the License Portal and display the latest switch list in the AmpCon-Campus UI.
- But if AmpCon-Campus fails to retrieve information from the License Portal due to network issues, you can manually refresh the latest **Expiration Date** and **Quantity** information and the list of switches with no AmpCon-Campus license assigned.

3. Check the quantity of Hardware IDs that can be bound with the AmpCon-Campus license for a specific expiration date:

- a. In the **Expiration Date** drop-down list, select an expiration date.

i NOTE

Trial licenses are marked with the string "(trial)".

- b. In the **Quantity** field, check the quantity of Hardware IDs that can be bound with the AmpCon-Campus license for the selected expiration date.

4. Select one or multiple switches to which you want to assign AmpCon-Campus licenses.

i NOTE

The total number of selected switches must be no longer than the value of **Quantity**. Or else, the **Activate** button cannot be clicked.

5. Click **Activate**.

Then, AmpCon-Campus uploads the information, including the switches and expiration date you selected, to the License Portal. The License Port will create the corresponding AmpCon-Campus license, which will be automatically imported to AmpCon-Campus.

Importing Licenses Manually

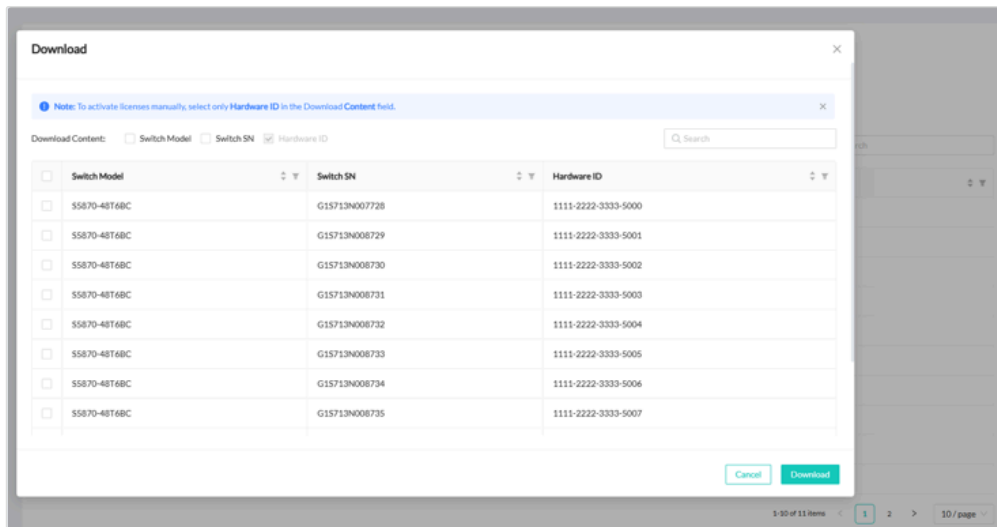
When AmpCon-Campus cannot connect to the License Portal or the connection is unstable, you need to import AmpCon-Campus licenses to AmpCon-Campus manually. To import an

AmpCon-Campus license manually, follow these steps:

1. Obtaining Hardware IDs in Batches

To manually import licenses to all switches, you need to obtain the hardware IDs of each switch that you want to manage first.

1. Click **System > Software Licenses > License Management** from the navigation bar, and then click **Quick Activate**. You can see all switches provisioned with ZTP and without AmpCon-Campus license assigned.
2. Click **Download**. In the **Download Content** section, the **Hardware ID** is selected by default.



3. Select one or multiple switches you want to retrieve hardware IDs.
4. Click **Download**. Then AmpCon-Campus will generate a .xlsx file with the hardware IDs of these switches.

NOTE

Don't modify the generated .xlsx file. Or else, the license creating process might fail.

2. Creating an AmpCon-Campus License

To create an AmpCon-Campus license, follow these steps:

1. Log in to the [License Portal](#), and then click **AmpCon Licenses > New AmpCon License**.

NOTE

You can get the username and password of the License Portal from the sale team.

2. Input the following information:

- **Software Type:** Select **AmpCon-Campus**.
 - **Software Version:** Select **AmpCon-Campus 2.3.0** or **AmpCon-Campus 2.3.1**.
 - **Device Type:** From the drop-down list, select a device type.
 - **Feature Type:** Select **Foundation**. Currently, only the **Foundation** feature type is supported.
 - **License Type:** Select **Trial License** or **Standard License**.
 - **License Name:** The name of the license.
3. In the **Addition Method** section, click **Form input**.
4. Click **Analysis Excel** to upload the .xlsx file generated in the [1. Obtaining Hardware IDs in Batches](#) section, and select the expiration date.

AmpCon license add form

* Software Type: AmpCon-Campus

* Software Version: AmpCon-Campus 2.3.0

* Device Type: FPSW

* Feature Type: Foundation

* License type: Standard License

License name: test-license

The 'License name' is an optional field that helps you differentiate between your licenses.

* Addition Method: ☒ Form input ☐ File upload

* Hardware id & Expiration date: **Analysis Excel**

Support multiple hw-ids, please use , or ; to separate

2024-11-01 Batch-Sync

Support multiple hw-ids, please use , or ; to separate

2024-11-01 Batch-Sync

This is the service end date. Please use the dropdown to check the support expiration dates available and select the correct one from the list once the license is assigned, this selection cannot be changed!

Add AmpCon License

i Tip

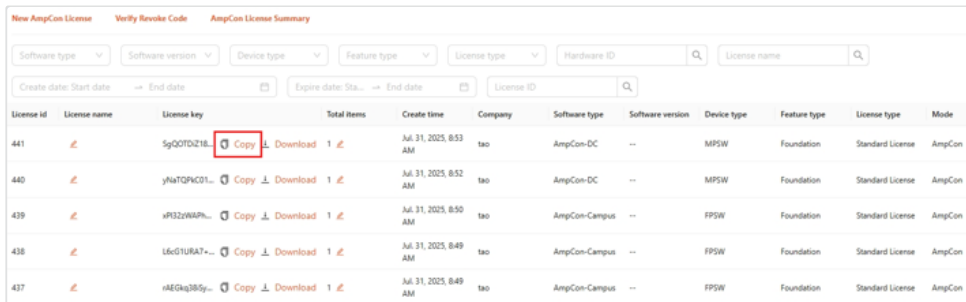
To apply a specific expiration date to all blank drop-down lists, locate the expiration date, and then click **Batch-Sync**.

5. Click **Add AmpCon License**.

3. Importing an AmpCon-Campus License to AmpCon-Campus

To import an AmpCon-Campus license to AmpCon-Campus, follow these steps:

1. Get the updated or new license from the License Portal.
 - a. Log in to the License Portal, and then click **AmpCon Licenses**.
 - b. Click **Copy** to copy the license string or click **Download** to download the .lic license file.



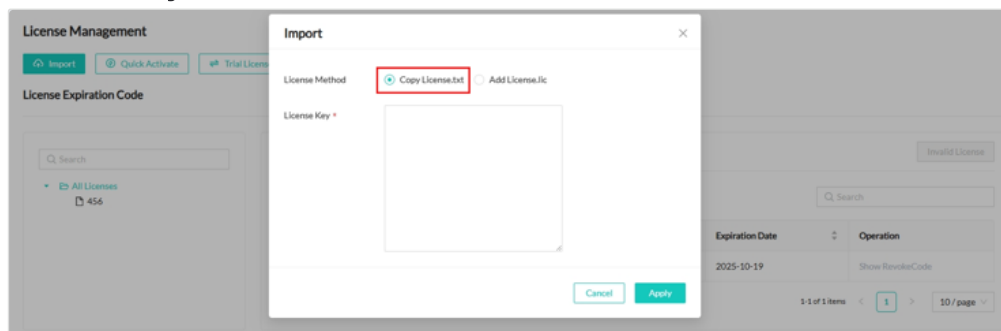
License id	License name	License key	Total items	Create time	Company	Software type	Software version	Device type	Feature type	License type	Mode
441		SgQOTDZ16...	1	Jul 31, 2025, 8:53 AM	tao	AmpCon-DC	--	MPSW	Foundation	Standard License	AmpCon
440		yNaTOPK31...	1	Jul 31, 2025, 8:52 AM	tao	AmpCon-DC	--	MPSW	Foundation	Standard License	AmpCon
439		vP3ZyWAPh...	1	Jul 31, 2025, 8:50 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon
438		L6d7URAT+	1	Jul 31, 2025, 8:49 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon
437		vAEGk385y...	1	Jul 31, 2025, 8:49 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon

2. In the AmpCon-Campus UI, click **System > Software Licenses > License Management** from the navigation bar.

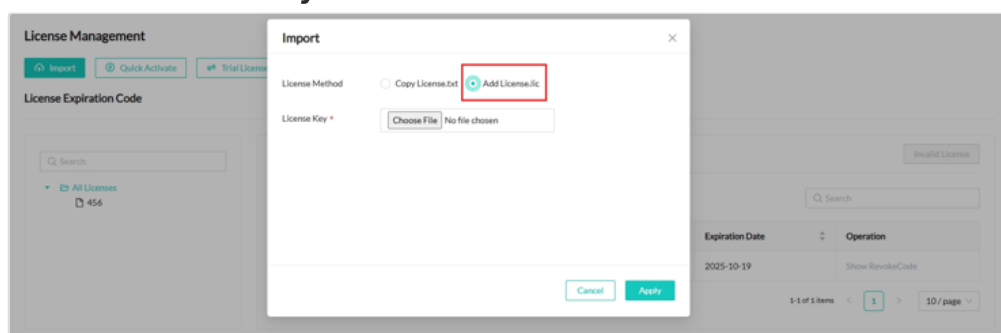
3. On the “License Management” page, click **Import**.

4. Select either of the following ways to import licenses:

- Select **Copy License.txt**, and paste the license strings that you copied in **step 1.b** to the **License Key** box.



- Select **Copy License.lic**, and then upload the .lic license file that you downloaded in **step 1.b** in the **License Key** selection box.



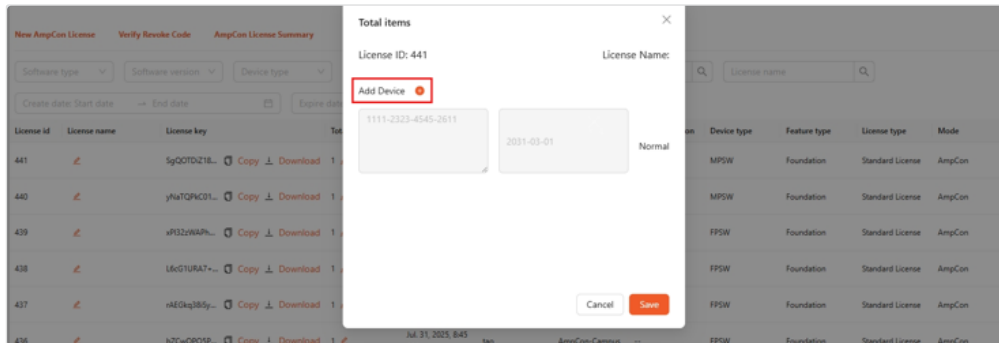
5. Click **Apply**.

After you import the new license, the **All Licenses** table is refreshed.

Optional: Editing an AmpCon-Campus License

After you create an AmpCon-Campus license, if you want to manage new switches with AmpCon-Campus, you can edit the AmpCon-Campus license. Follow these steps:

1. Log in to the License Portal, and click **AmpCon Licenses**.
2. Locate the license that you want to edit, and click the edit icon in the **Total hw-ids** column.
3. Click the Add Device icon, enter the Hardware ID of each new switch that you want to manage, and select the expiration date.



4. Click **Save**.

NOTE

After you edit a license, import the updated AmpCon-Campus license to AmpCon-Campus so that newly added switches can be managed by AmpCon-Campus.

Importing Licenses for Imported Switches

To onboard switches through importing switches, you must import AmpCon-Campus licenses (containing the Hardware IDs of the switches) to AmpCon-Campus manually so that AmpCon-Campus can manage these switches.

1. Obtaining Hardware IDs
 2. Creating an AmpCon-Campus License
 3. Importing an AmpCon-Campus License to AmpCon-Campus
- Optional: Editing an AmpCon-Campus License

1. Obtaining Hardware IDs

To manually import the licenses to all switches, you need to obtain the Hardware ID of each switch that you want to manage first. Follow these methods:

1. SSH log in to each switch and run the following commands:

```
run start shell sh
```

```
sudo license -s
```

```
admin@sw4# run start shell sh
admin@sw4:~$ sudo license -s
{
  "Type": "100GE",
  "Feature": ["Base Product", "Layer3", "OpenFlow"],
  "Support End Date": "2026-01-01",
  "Hardware ID": "██████████-F8DF-7493"
}
admin@sw4:~$
```

2. SSH log in to each switch and run the following command:

```
show version
```

```
admin@PIC0S> show version
Copyright                : Copyright (C) 2009-2025 Pica8, Inc. All Rights Reserved.
Model                    : AS9716_32D
Software Version         : 9.8.7-fix-bug19435/ace39ae71c
Software Released Date   : 08/08/2025
Serial Number            : 971632D1936013
System Uptime            : 0 day 4 hour 03 minute
Hardware ID              : ██████████-5866-E2B3
License type             : Uninstalled
Device MAC Address       : 1c:ea:0b:a2:6d:c3
```

2. Creating an AmpCon-Campus License

To create an AmpCon-Campus license, follow these steps:

1. Log in to the [License Portal](#), and then click **AmpCon Licenses > New AmpCon License**.

You can get the username and password of the License Portal from the sale team.

2. Input the following information:

- **Software Type:** Select **AmpCon-Campus**.
 - **Software Version:** Select **AmpCon-Campus 2.3.0** or **AmpCon-Campus 2.3.1**.
 - **Device Type:** From the drop-down list, select a device type.
 - **Feature Type:** Select **Foundation**. Currently, only the **Foundation** feature type is supported.
 - **License Type:** Select **Trial License** or **Standard License**.
 - **License Name:** The name of the license.
3. In the **Addition Method** section, select either of the following ways:
- **Form input:** Enter the Hardware IDs of switches to be managed with AmpCon-Campus, and select the expiration date.

AmpCon license add form

* Software Type

AmpCon-Campus

* Software Version

AmpCon-Campus 2.3.0

* Device Type

FPSW

* Feature Type

Foundation

* License type

Standard License

License name

test-license

The 'License name' is an optional field that helps you differentiate between your licenses.

* Addition Method

☒ Form input
 ☐ File upload

* Hardware id & Expiration date

Analysis Excel

Support multiple hw-ids, please use , or ; to separate

2024-11-01

Batch-Sync

Support multiple hw-ids, please use , or ; to separate

2024-11-01

Batch-Sync

This is the service end date. Please use the dropdown to check the support expiration dates available and select the correct one from the list; once the license is assigned, this selection cannot be changed!

Add AmpCon License

i Tip

To apply a specific expiration date to all blank drop-down lists, locate the expiration date, and then click **Batch-Sync**.

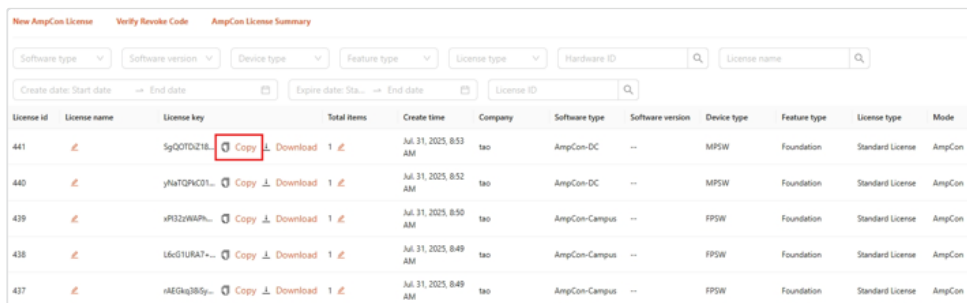
- **File upload:** Click **Upload** to upload a .xlsx file with the Hardware IDs of switches to be managed with AmpCon-Campus and the expiration date. You can click **Blank template** to download a .xlsx template file.

4. Click **Add AmpCon License**.

3. Importing an AmpCon-Campus License to AmpCon-Campus

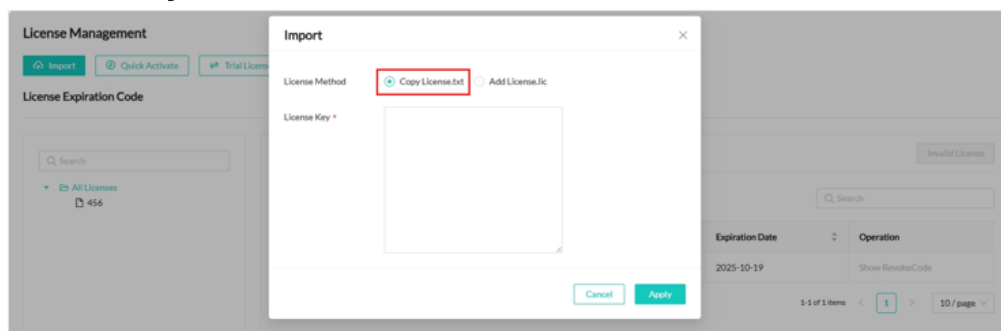
To import an AmpCon-Campus license to AmpCon-Campus, follow these steps:

1. Get the updated or new license from the License Portal.
 - a. Log in to the License Portal, and then click **AmpCon Licenses**.
 - b. Click **Copy** to copy the license string or click **Download** to download the .lic license file.

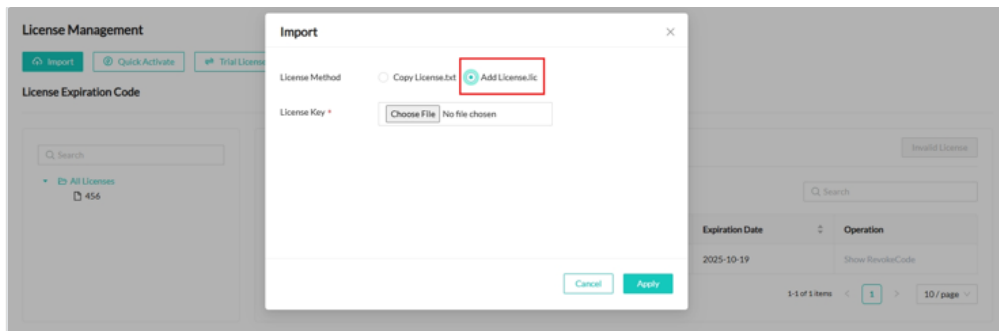


License ID	License name	License key	Total items	Create time	Company	Software type	Software version	Device type	Feature type	License type	Mode
441		5gQOTDZ16...	1	Jul 31, 2025, 8:53 AM	tao	AmpCon-DC	--	MPSW	Foundation	Standard License	AmpCon
440		yRaTOPKQ31...	1	Jul 31, 2025, 8:52 AM	tao	AmpCon-DC	--	MPSW	Foundation	Standard License	AmpCon
439		wP32zWAPh...	1	Jul 31, 2025, 8:50 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon
438		L6dSTURAT...	1	Jul 31, 2025, 8:49 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon
437		hAEqk385y...	1	Jul 31, 2025, 8:49 AM	tao	AmpCon-Campus	--	FPSW	Foundation	Standard License	AmpCon

2. In the AmpCon-Campus UI, click **System > Software Licenses > Licenses Management** from the navigation bar.
3. On the “Licenses Management” page, click **Import**.
4. Select either of the following ways to import licenses:
 - Select **Copy License.txt**, and paste the license strings that you copied in **step 1.b** to the **License Key** box.



- Select **Copy License.lic**, and then upload the .lic license file that you downloaded in **step 1.b** in the **License Key** selection box.



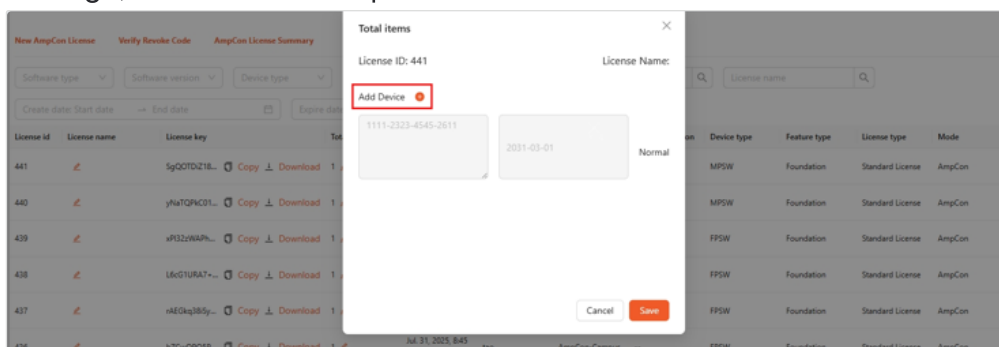
5. Click **Apply**.

After you import the new license, the **All Licenses** table is refreshed.

Optional: Editing an AmpCon-Campus License

After you create an AmpCon-Campus license, if you want to manage new switches with AmpCon-Campus, you can edit the AmpCon-Campus license. Follow these steps:

1. Log in to the License Portal, and click **AmpCon Licenses**.
2. Locate the license that you want to edit, and click the edit icon in the **Total hw-ids** column.
3. Click the Add Device icon, enter the Hardware ID of each new switch that you want to manage, and select the expiration date.



4. Click **Save**.

NOTE

After you edit a license, import the updated AmpCon-Campus license to AmpCon-Campus so that newly added switches can be managed by AmpCon-Campus.

Troubleshooting for License Importing

If you fail to import AmpCon-Campus licenses, refer to the following reasons and solutions:

[Automatic License Importing Issues](#)

[Abnormal Network Connection](#)

[Insufficient AmpCon-Campus Licenses](#)

[License Portal Authentication Failed](#)

[Outdated Information](#)

[Manual License Importing Issues](#)

[Abnormal Network Connection](#)

[Insufficient AmpCon-Campus Licenses](#)

[License Portal Authentication Failed](#)

[Outdated Information](#)

[Wrong Hardware ID in the Uploaded File](#)

Automatic License Importing Issues

When you automatically import an AmpCon-Campus license, you might see the following errors in the AmpCon-Campus UI. To resolve these issues, check related solutions:

Abnormal Network Connection

Error:

- Abnormal network connection.
- Failed to obtain the License Key. Please try again later.

Root Cause: The network between the License Portal and the AmpCon-Campus server is unavailable or unstable.

Solution: Check and resolve the network connection issues between the License Portal and the AmpCon-Campus server.

Insufficient AmpCon-Campus Licenses

Error: The number of selected switches can't be more than the number of Hardware IDs that can be bound with the AmpCon license for the selected expiration date.

Root Cause: The total number of selected switches is more than the number of Hardware IDs that can be bound with the AmpCon-Campus license for the selected expiration date.

Solution:

- Click **System > Software Licenses > Licenses Management** from the navigation bar, and then click **Quick Activate**. Click **Refresh** to manually refresh the number of remaining Hardware IDs that can be bound with the AmpCon-Campus license for the selected expiration date.
- Reduce the total number of switches selected with the expiration date specified.
- Select a different expiration date to activate the remaining switches.

- Purchase more AmpCon-Campus licenses.

License Portal Authentication Failed

Error: The License Portal authentication failed. Please try again after updating license portal information in the global system configuration.

Root Cause: The License Portal information that you entered in the global [system configuration](#) is incorrect.

Solution: Re-enter the **License Portal URL**, **License Portal User**, and **License Portal Password** in the global system configuration, and then check the connectivity. For more information, see [Checking License Portal Connectivity](#).

Outdated Information

Error: [xxx.xxx.xxx](#) (HW ID) has bound the license. Please check and try again.

Root Cause: The switch that you are activating has been assigned with an AmpCon-Campus license.

Solution:

- Click **Refresh** to manually refresh the list of switches with no AmpCon-Campus licenses.
- Resolve network issues between the AmpCon-Campus server and the License Portal.

Manual License Importing Issues

When you manually import an AmpCon-Campus license, you might see the following errors in the AmpCon-Campus UI. To resolve these issues, check related solutions:

Abnormal Network Connection

Error: Failed to obtain the License Key. Please try again later.

Root Cause: The network between the License Portal and the AmpCon-Campus server is unavailable or unstable.

Solution: Check and resolve the network connection issue between the License Portal and the AmpCon-Campus server.

Insufficient AmpCon-Campus Licenses

Error: The number of selected switches can't be more than the number of Hardware IDs that can be bound with the AmpCon license for the selected expiration date.

Root Cause: The total number of selected switches is more than the number of Hardware IDs that can be bound with the AmpCon-Campus license for the selected expiration date.

Solution:

- Reduce the total number of switches specified with the expiration date.

- Select a different expiration date to activate the remaining switches.
- Purchase more AmpCon-Campus licenses.

License Portal Authentication Failed

Error: The License Portal account or password does not match. Please check and try again.

Root Cause: The License Portal information that you entered in the License Portal is incorrect or does not match.

Solution: Re-enter the username and password you input to log in to the License Portal.

Outdated Information

Error: [xxx.xxx.xxx](#) (HW ID) has bound the license. Please check and try again.

Root Cause: The switch that you are activating has been assigned with an AmpCon-Campus license.

Solution:

- Click **Refresh** to manually refresh the list of switches AmpCon-Campus PicOS licenses.
- Resolve network issues between the AmpCon-Campus server and the License Portal.

Wrong Hardware ID in the Uploaded File

Error:

- There is no HW ID in the table. Please check and try again.
- [xxx.xxx](#) (HW ID) is repeated. Please check and try again.
- The format of the Hardware ID filled in is incorrect. Please check.

Root Cause: The hardware IDs are not entered, are repeated, or are in wrong format.

Solution: Ensure hardware IDs are correctly entered and not duplicated in the uploaded file.

Converting a Trial License to Standard Licenses

You can convert a trial AmpCon-Campus license to one or multiple standard AmpCon-Campus licenses automatically when AmpCon-Campus is stably connected to the License Portal.

NOTES

- On AmpCon-Campus, you have only one chance to convert trial licenses to standard licenses.
- If more switches need trial license conversion, perform the operation in the License Portal.

[Prerequisites](#)

[Procedure](#)

[Guidelines of Applying Expiration Date](#)

Prerequisites

- Ensure that AmpCon-Campus can connect with the License Portal through the entered username and password. Or else, switch deployment will fail. For more information, see [Checking License Portal Connectivity](#).
- Ensure that the sale team have created standard AmpCon-Campus licenses for you in the License Portal.

Procedure

To convert a trial AmpCon-Campus license to one or multiple standard licenses automatically, follow these steps:

1. Click **System > Software Licenses > Licenses Management** from the navigation bar, and then click **Trial License Conversion**.

You can view all switches managed by AmpCon-Campus with a trial license assigned.

NOTE

The **Trial License Conversion** button is visible only when a trial license has been imported into AmpCon-Campus and no standard license has been imported.

Convert Trial License

License Portal User: Available Expiration Date: Quantity:

Switch Model	Switch SN	Hardware ID	Expiration Date
S5870-48T6BC	1	1111-2222-3333-5000	Select Expiration Date
S5870-48T6BC	2	1111-2222-3333-5001	Select Expiration Date
S5870-48T6BC	3	1111-2222-3333-5002	Select Expiration Date
S5870-48T6BC	4	1111-2222-3333-5003	Select Expiration Date
S5870-48T6BC	5	1111-2222-3333-5004	Select Expiration Date
S5870-48T6BC	6	1111-2222-3333-5005	Select Expiration Date
S5870-48T6BC	7	1111-2222-3333-5006	Select Expiration Date
S5870-48T6BC	8	1111-2222-3333-5007	Select Expiration Date
S5870-48T6BC	9	1111-2222-3333-5008	Select Expiration Date
S5870-48T6BC	10	1111-2222-3333-5009	Select Expiration Date
S5870-48T6BC	1000	1111-2222-3333-5012	Select Expiration Date

2. Optional: To manually refresh the list of switches with a trial license assigned, click **Refresh**.

NOTE

You are recommended to manually refresh the list of switches with a trial license assigned. Reasons are as follows:

- If the network is available and stable, AmpCon-Campus will automatically retrieve the latest **Expiration Date** and **Quantity** information from the License Portal and display the latest switch list in the AmpCon-Campus UI.
- But if AmpCon-Campus fails to retrieve information from the License Portal due to network issues, manually refresh the latest **Expiration Date** and **Quantity** information and the list of switches with a trial license assigned.

3. Check the quantity of Hardware IDs that can be bound with the AmpCon-Campus license for a specific expiration date:

Convert Trial License

License Portal User: **Available Expiration Date**: **Quantity**:

Switch Model	Switch SN	Hardware ID	Expiration Date
S5870-48T6BC	1	1111-2222-3333-5000	Select Expiration Date
S5870-48T6BC	2	1111-2222-3333-5001	Select Expiration Date
S5870-48T6BC	3	1111-2222-3333-5002	Select Expiration Date
S5870-48T6BC	4	1111-2222-3333-5003	Select Expiration Date
S5870-48T6BC	5	1111-2222-3333-5004	Select Expiration Date
S5870-48T6BC	6	1111-2222-3333-5005	Select Expiration Date
S5870-48T6BC	7	1111-2222-3333-5006	Select Expiration Date

- In the **Available Expiration Date** drop-down list, select an expiration date.
- In the **Quantity** field, check the quantity of Hardware IDs allowed by the selected expiration date.

4. For switches with different expiration dates, locate each switch, and then select an expiration date in the **Expiration Date** drop-down list.
5. For switches with the same expiration date, select the expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. For how expiration dates are applied, see [Guidelines of Applying Expiration Date](#).
6. Click **Convert** to complete the conversion.

NOTE

The switches without **Expiration Date** specified will be removed from AmpCon-Campus after the operation.

Guidelines of Applying Expiration Date

After you click **Apply Expiration Date**, AmpCon-Campus will analyze the following counts first:

- **Count A:** The count of the switches without **Expiration Date** specified.
- **Count B:** The count of Hardware IDs allowed by the selected expiration date in the **Available Expiration Date** drop-down list.

If **Count A** is less than **Count B**, AmpCon-Campus will automatically apply the selected expiration date to all the switches without **Expiration Date** specified.

If **Count A** is more than **Count B**, AmpCon-Campus will automatically apply the selected expiration date to switches without **Expiration Date** specified from top to bottom.

For the remaining switches without **Expiration Date** specified, the **Expiration Date** drop-down list are blank. You can do as follows:

- Select another expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. This expiration date will be assigned to the remaining switches by AmpCon-Campus automatically.
- Select another expiration date in the **Expiration Date** drop-down list manually.

Example:

The screenshot shows the 'Convert Trial License' interface. At the top, there is a 'License Portal User' field with 'api_user' and an 'Available Expiration Date' dropdown set to '2025-08-29'. A 'Quantity' field is set to '4'. Below these are buttons for 'Convert', 'Refresh', and 'Apply Expiration Date'. The main area contains a table with columns 'Switch Model' and 'Switch SN'. The table lists five switches, all with model 'S5870-48T6BC' and SNs 1 through 5. To the right of the table is a column for 'Expiration Date' with five dropdown menus, each labeled 'Select Expiration Date'. A search bar is also present. A red box highlights the 'Available Expiration Date' dropdown, and another red box highlights the 'Expiration Date' dropdowns. A third red box highlights the 'Quantity' field.

The count of the switches without **Expiration Date** specified is 5, the selected expiration date (2025-08-29) allows for 4 Hardware IDs.

In this case, you click the **Apply Expiration Date** button. AmpCon-Campus will assign the selected expiration date (2025-08-29) to the first 4 switches. For the remaining 1 switch without an **Expiration Date** specified, you can do as follows:

- Select another expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. This expiration date will be assigned to the remaining 1 switch by AmpCon-Campus automatically.
- Select another expiration date in the **Expiration Date** drop-down list manually.

Viewing AmpCon-Campus Licenses

In the AmpCon-Campus UI, click **System > Software Licenses > License View**. You can see the AmpCon-Campus licenses that are imported to AmpCon-Campus.

In addition, you can see the status and usage information of these AmpCon-Campus licenses.

[License Status](#)

[License Usage](#)

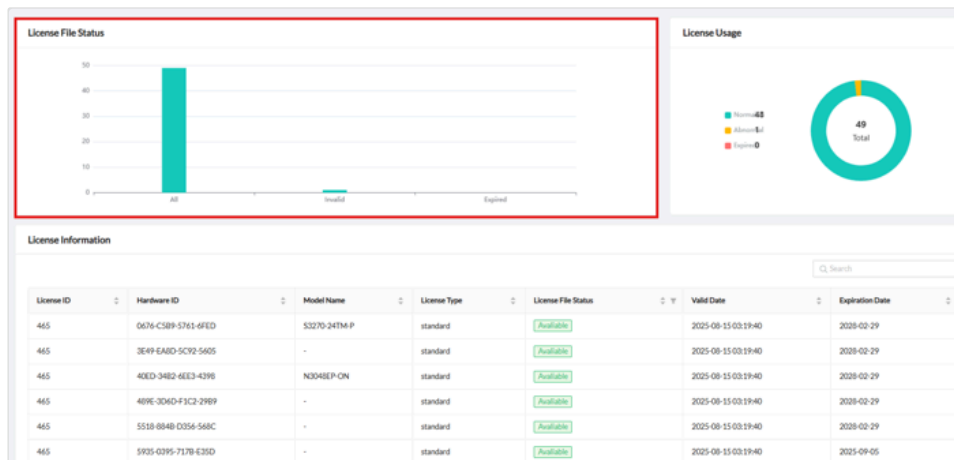
[License Details](#)

[Fuzzy Search for License Information](#)

License Status

In the **License File Status** section, you can see the numbers of **All**, **Invalid**, and **Expired** AmpCon-Campus licenses. See the following descriptions of each status:

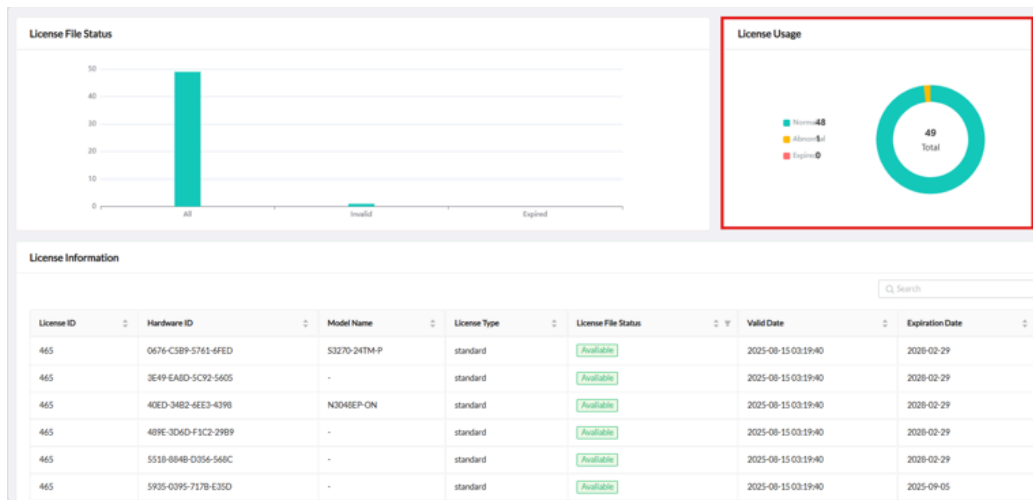
- **All:** All licenses.
- **Invalid:** The invalid licenses.
- **Expired:** The expired licenses.



License Usage

In the **License Usage** section, you can see the numbers of normal, abnormal, and expired AmpCon-Campus licenses. See the following descriptions of each status:

- **Normal:** The licenses that are both valid and not expired.
- **Abnormal:** The licenses that are invalid or expired or can't be verified by AmpCon-Campus.
- **Expired:** The expired licenses.

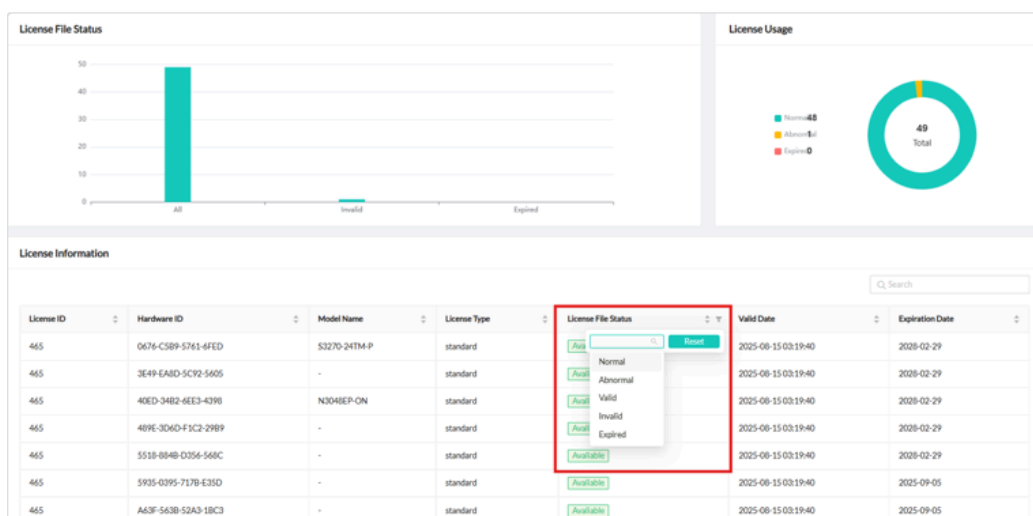


License Details

In the **License Information** section, you can view the following columns. All columns support ascending and descending sorting.

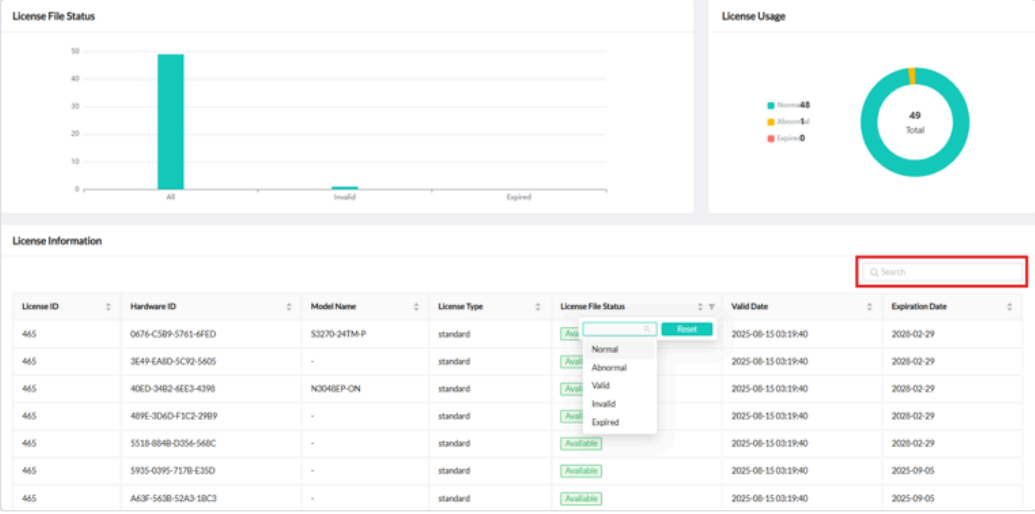
- **License ID:** The ID of the AmpCon-Campus license
- **Hardware ID:** The ID of the switch hardware
- **Model Name:** The name of the switch model
- **License Type:** Includes standard license (formal License) and trial license (temporary License)
- **License File Status:** The status of the AmpCon-Campus license for the switch
- **Valid Date:** The date from when the switch can be managed by AmpCon-Campus
- **Expiration Date:** The date until when the switch can be managed by AmpCon-Campus

You can filter licenses with the license status file keywords. In the **License Information** table, click the **License File Status** column, and select a status to view relevant licenses.



Fuzzy Search for License Information

In the search box of the **License Information** table, enter keywords to search for specific licenses.



Invalidating a License

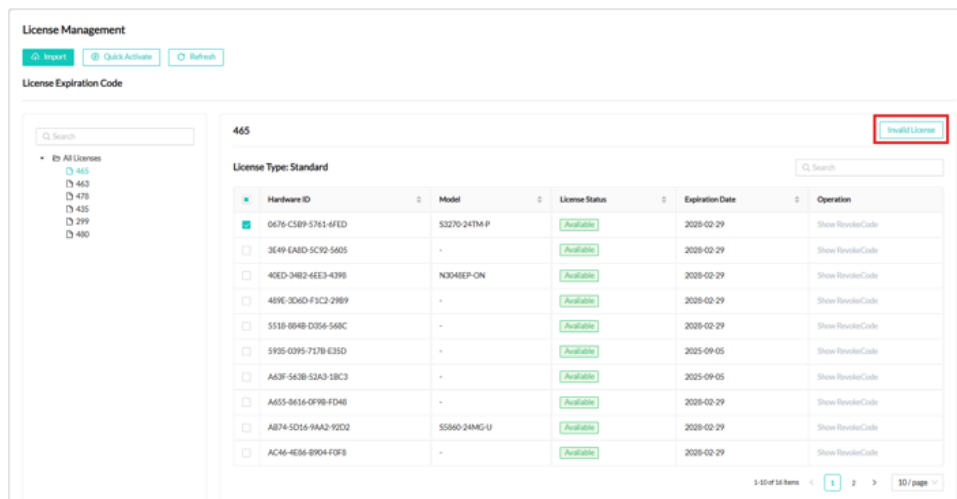
If you don't need to deploy and manage a switch with AmpCon-Campus, you can invalidate the AmpCon-Campus license on the switch to release this license.

NOTES

- The Hardware ID of a switch might exist in multiple AmpCon-Campus licenses. Ensure that you invalidate all AmpCon-Campus licenses on the switch.
- After you invalidate all AmpCon-Campus licenses on a switch, the switch can't be deployed and managed with AmpCon-Campus. The switch that has been deployed will be removed from the switch list on the "Switches" page.
- You can perform three invalidation operations at most.

Procedure

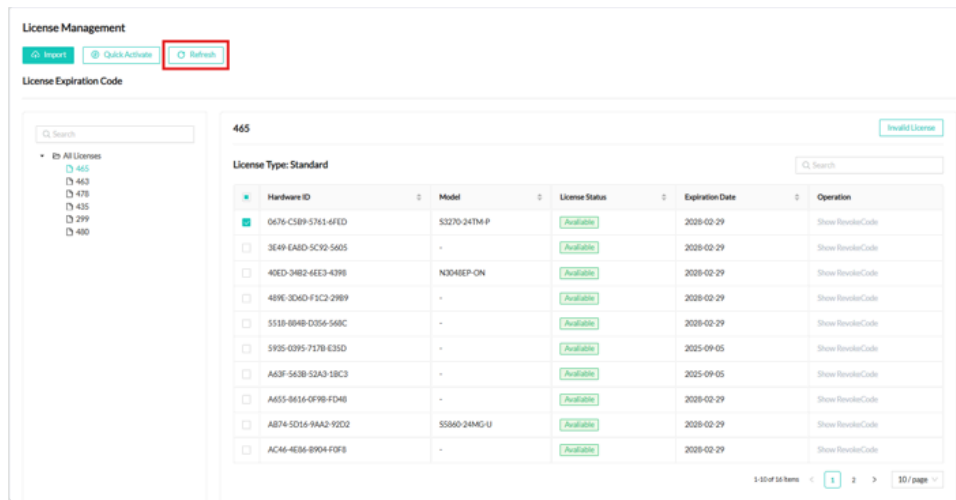
1. In the AmpCon-Campus UI, click **System > Software Licenses > Licenses Management**.
2. Click the license file, and click the Hardware ID to be invalidated. Then, click **Invalid License**.



3. In the pop-up window, click **Yes**.

You can see the invalid code is displayed in a pop-up window. The status of the license is changed to **Invalid**, and **show invalid code** in the **Operation** column is shown as clickable instead of grayed out.

If the license status is not displayed as **Invalid**, click **Refresh** to update the license status.



4. Click **Show Invalid Code** to copy the invalid code.
5. Release the invalidated license in the License Portal.
 - a. Log in to the License Portal, and then click **AmpCon Licenses > Verify Revoke Code**.
 - b. In the **Software Type** drop-down list, select **AmpCon-Campus**.
 - c. Use either of the following ways:
 - In the **Addition Method** section, select **Form Input**. In the **Revoke Code** field, paste the invalid code that you copied in step 4.

The screenshot shows the 'Verify revoke code' form. It has a title 'Verify revoke code' in orange. Below it, there's a section for 'Software Type' with a dropdown menu showing 'AmpCon-Campus'. Then, there's a section for 'Addition Method' with two radio buttons: 'Form input' (selected) and 'File upload'. Below that, there's a section for 'Revoke Code' with a text input field containing the placeholder 'Please enter device revoke code'. At the bottom, there's an orange 'Save' button.

- In the **Addition Method** section, select **File Upload**. Click **Blank template** to download a template file. Open the template file, and enter the invalid code in the .xlsx template file. Then, upload the file.

Verify revoke code

* Software Type

AmpCon-Campus

* Addition Method

☐ Form input ☒ File upload

* Revoke Code

Upload Blank template

Save

6. Click **Save**.

Checking License Logs and Alerts

In the AmpCon-Campus UI, click **System > Software Licenses > License Log**. You can check the operation logs and alerts that are related to AmpCon-Campus licenses.

[Viewing License Operation Logs](#)

[Exporting License Operation Logs](#)

[Searching for License Operation Logs](#)

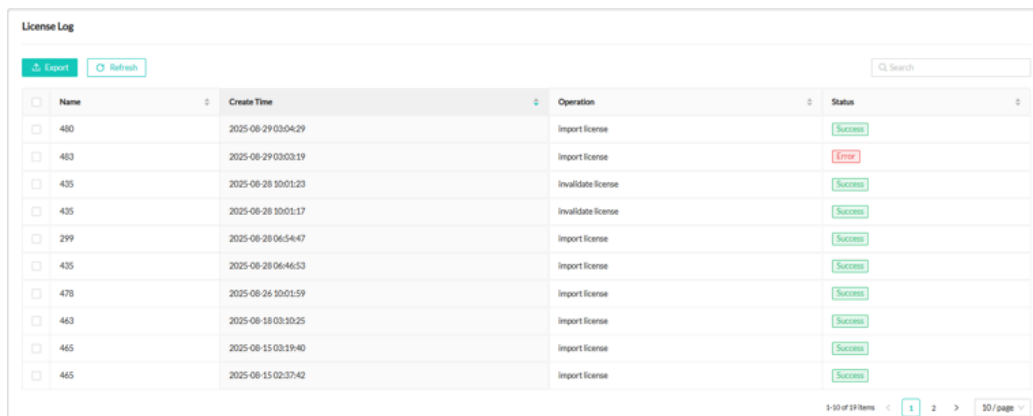
[Checking License Alerts](#)

[Exporting License Alerts](#)

[Searching for License Alerts](#)

Viewing License Operation Logs

On the “License Log” page, you can view license-related operation records (such as license import operations and license invalidation operations), the time of each operation, and the status of each operation.

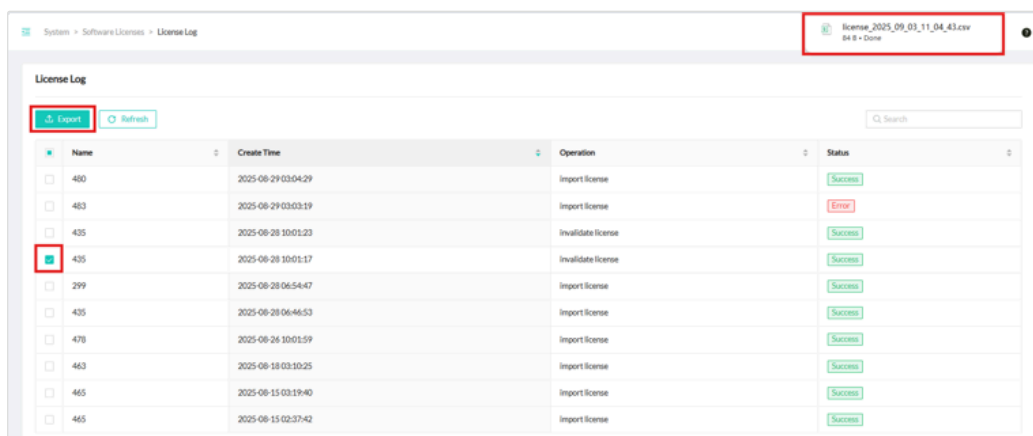


The screenshot shows the 'License Log' interface. At the top, there are buttons for 'Export' and 'Refresh', and a search bar. Below is a table with columns: Name, Create Time, Operation, and Status. The table contains 10 rows of data. The first row has Name 480, Create Time 2025-08-29 03:04:29, Operation Import license, and Status Success. The second row has Name 483, Create Time 2025-08-29 03:03:19, Operation Import license, and Status Error. The third row has Name 435, Create Time 2025-08-28 10:01:23, Operation Invalide license, and Status Success. The fourth row has Name 435, Create Time 2025-08-28 10:01:17, Operation Invalide license, and Status Success. The fifth row has Name 299, Create Time 2025-08-28 06:54:47, Operation Import license, and Status Success. The sixth row has Name 435, Create Time 2025-08-28 06:46:53, Operation Import license, and Status Success. The seventh row has Name 478, Create Time 2025-08-26 10:01:59, Operation Import license, and Status Success. The eighth row has Name 463, Create Time 2025-08-18 03:10:25, Operation Import license, and Status Success. The ninth row has Name 465, Create Time 2025-08-15 03:19:40, Operation Import license, and Status Success. The tenth row has Name 465, Create Time 2025-08-15 02:37:42, Operation Import license, and Status Success. At the bottom right, there is a pagination bar showing '1-10 of 10 items' and '10 / page'.

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import license	Success
483	2025-08-29 03:03:19	Import license	Error
435	2025-08-28 10:01:23	Invalide license	Success
435	2025-08-28 10:01:17	Invalide license	Success
299	2025-08-28 06:54:47	Import license	Success
435	2025-08-28 06:46:53	Import license	Success
478	2025-08-26 10:01:59	Import license	Success
463	2025-08-18 03:10:25	Import license	Success
465	2025-08-15 03:19:40	Import license	Success
465	2025-08-15 02:37:42	Import license	Success

Exporting License Operation Logs

To export license logs as a .csv file, select one or more entries, and then click **Export** in the **License Log** section.

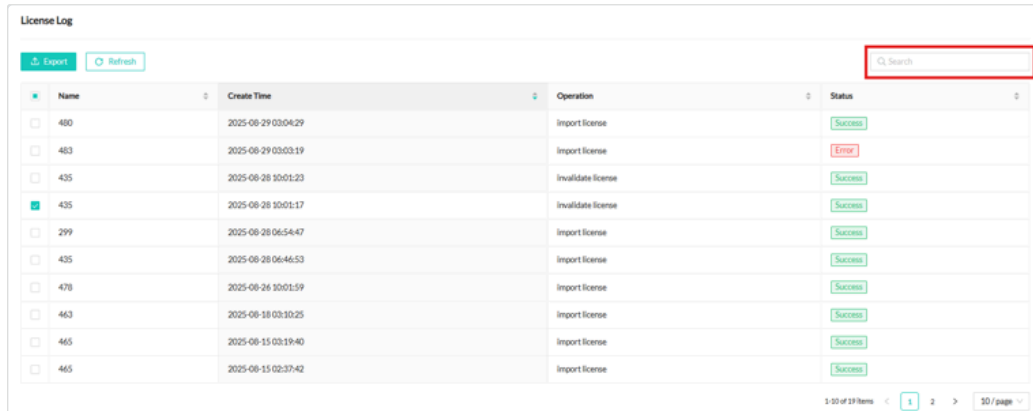


The screenshot shows the 'License Log' interface with the 'Export' button highlighted in a red box. The table is the same as in the previous screenshot. At the top right, there is a notification box that says 'license_2025_09_03_11_04_43.csv 84.8 K - Done'. The 'Export' button is located at the top left of the table area.

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import license	Success
483	2025-08-29 03:03:19	Import license	Error
435	2025-08-28 10:01:23	Invalide license	Success
435	2025-08-28 10:01:17	Invalide license	Success
299	2025-08-28 06:54:47	Import license	Success
435	2025-08-28 06:46:53	Import license	Success
478	2025-08-26 10:01:59	Import license	Success
463	2025-08-18 03:10:25	Import license	Success
465	2025-08-15 03:19:40	Import license	Success
465	2025-08-15 02:37:42	Import license	Success

Searching for License Operation Logs

To perform a fuzzy search for logs, enter keywords in the search box of the **License Log** section.



The screenshot shows the 'License Log' interface. At the top, there are 'Export' and 'Refresh' buttons. A search bar with the placeholder 'Q Search' is highlighted with a red box. Below the search bar is a table with columns: Name, Create Time, Operation, and Status. The table contains 10 rows of data. The first row has Name 480, Create Time 2025-08-29 03:04:29, Operation Import license, and Status Success. The second row has Name 483, Create Time 2025-08-29 03:03:19, Operation Import license, and Status Error. The third row has Name 435, Create Time 2025-08-28 10:01:23, Operation Invalidate license, and Status Success. The fourth row has Name 435, Create Time 2025-08-28 10:01:17, Operation Invalidate license, and Status Success. The fifth row has Name 299, Create Time 2025-08-28 06:54:47, Operation Import license, and Status Success. The sixth row has Name 435, Create Time 2025-08-28 06:46:53, Operation Import license, and Status Success. The seventh row has Name 478, Create Time 2025-08-26 10:01:59, Operation Import license, and Status Success. The eighth row has Name 463, Create Time 2025-08-18 03:30:25, Operation Import license, and Status Success. The ninth row has Name 465, Create Time 2025-08-15 03:19:40, Operation Import license, and Status Success. The tenth row has Name 465, Create Time 2025-08-15 02:37:42, Operation Import license, and Status Success. At the bottom right, there is a pagination bar showing '1-10 of 10 items', a page number '1' in a box, and '10 / page'.

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import license	Success
483	2025-08-29 03:03:19	Import license	Error
435	2025-08-28 10:01:23	Invalidate license	Success
435	2025-08-28 10:01:17	Invalidate license	Success
299	2025-08-28 06:54:47	Import license	Success
435	2025-08-28 06:46:53	Import license	Success
478	2025-08-26 10:01:59	Import license	Success
463	2025-08-18 03:30:25	Import license	Success
465	2025-08-15 03:19:40	Import license	Success
465	2025-08-15 02:37:42	Import license	Success

Checking License Alerts

To check license alert information, check the **License Alert** section.

NOTES

- During the grace period of a trial AmpCon-Campus license, the AmpCon-Campus login interface displays "License is expired, you have a 14-day grace period".
- If a standard AmpCon-Campus license expires, you can see the license status is expired in the **License Alert** section of the AmpCon-Campus UI.
- Within 14 days before a standard AmpCon-Campus license expires, when you log in to the AmpCon-Campus UI, you will see the notification message "License ID: xx Some of the licenses are about to expire. If you wish to continue using this device, please renew the license. You can view the relevant information through the "License Alert" function."

In this case, ask the sale team to renew the AmpCon-Campus license in the License Portal. Then, download the renewed license, and import it to AmpCon-Campus as described in [Importing Licenses for Deployed Switches](#).

License Log

Export Refresh

Search

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import License	Success
483	2025-08-29 03:03:19	Import License	Error
435	2025-08-28 10:01:23	Invalidate License	Success
435	2025-08-28 10:01:17	Invalidate License	Success
299	2025-08-28 06:54:47	Import License	Success
435	2025-08-28 06:46:53	Import License	Success
478	2025-08-26 10:01:59	Import License	Success
463	2025-08-18 03:10:25	Import License	Success
465	2025-08-15 03:19:40	Import License	Success
465	2025-08-15 02:37:42	Import License	Success

1-10 of 19 items 1 2 30 / page

License Alert

Export Refresh

Search

License ID	Hardware ID	Model Name	License Type	Valid Date	Expiration Date	Status Description
435	C28F-1282-A372-55DC	-	standard	2025-08-28 06:46:53	2025-08-29	Invalid

1-1 of 1 items 1 30 / page

Exporting License Alerts

To export alerts as a .csv file, select one or more alert entries, and then click **Export** in the **License Alert** section.

System > Software Licenses > License Log

License Log

Export Refresh

Search

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import License	Success
483	2025-08-29 03:03:19	Import License	Error
435	2025-08-28 10:01:23	Invalidate License	Success
435	2025-08-28 10:01:17	Invalidate License	Success
299	2025-08-28 06:54:47	Import License	Success
435	2025-08-28 06:46:53	Import License	Success
478	2025-08-26 10:01:59	Import License	Success
463	2025-08-18 03:10:25	Import License	Success
465	2025-08-15 03:19:40	Import License	Success
465	2025-08-15 02:37:42	Import License	Success

1-10 of 19 items 1 2 30 / page

License Alert

Export Refresh

Search

License ID	Hardware ID	Model Name	License Type	Valid Date	Expiration Date	Status Description
435	C28F-1282-A372-55DC	-	standard	2025-08-28 06:46:53	2025-08-29	Invalid

1-1 of 1 items 1 30 / page

License Alert - 100 B - Done
License Alert - 100 B - Done
License Alert - 100 B - Done

Searching for License Alerts

To perform a fuzzy search for alerts, enter keywords in the search box of the **License Alert** section.

License Log

Export Refresh

Search

Name	Create Time	Operation	Status
480	2025-08-29 03:04:29	Import License	Success
483	2025-08-29 03:03:19	Import License	Error
435	2025-08-28 10:01:23	Invalidate License	Success
435	2025-08-28 10:01:17	Invalidate License	Success
299	2025-08-28 06:54:47	Import License	Success
435	2025-08-28 06:46:53	Import License	Success
478	2025-08-26 10:01:59	Import License	Success
463	2025-08-18 03:10:25	Import License	Success
465	2025-08-15 03:19:40	Import License	Success
465	2025-08-15 02:37:42	Import License	Success

1-10 of 19 items 1 2 30 / page

License Alert

Export Refresh

Search

License ID	Hardware ID	Model Name	License Type	Valid Date	Expiration Date	Status Description
435	C28F-1282-A372-55DC	-	standard	2025-08-28 06:46:53	2025-08-29	Invalid

1-1 of 1 items 1 30 / page

Managing PicOS Licenses

You can verify whether PicOS licenses are valid or not by using the **License Audit** feature. Or you can verify whether PicOS licenses are valid and extend expired PicOS licenses by using the **License Action** feature.

If the AmpCon-Campus server can't access the License Portal, you can add local PicOS licenses to AmpCon-Campus so that AmpCon-Campus can install PicOS licenses on corresponding switches.

Prerequisites

Verifying License Validity

Verifying the PicOS License for a Switch

Verifying PicOS Licenses for a Group of Switches

Verifying License Validity and Extending Expired Licenses

Verifying and Extending the PicOS License for a Switch

Verifying and Extending PicOS Licenses for a Group of Switches

Adding Local PicOS Licenses

Prerequisites

- Check whether AmpCon-Campus can connect with the License Portal through the entered username and password in the system configuration. For more information, see [Checking License Portal Connectivity](#).
 - If the AmpCon-Campus server can access the License Portal that you specified in the system configuration, AmpCon-Campus automatically retrieves PicOS licenses from the License Portal. Then, when you deploy a switch with AmpCon-Campus, AmpCon-Campus automatically installs the PicOS license for the switch.
 - But sometimes the AmpCon-Campus server can't access the License Portal that you specified in the system configuration, for example in an air-gapped environment. In this case, you need to manually add local PicOS licenses to AmpCon-Campus so that AmpCon-Campus can install PicOS licenses on corresponding switches. For more information, see the [Adding Local PicOS Licenses](#) section.
- Ensure that the sale team has created PicOS licenses for the switches to be managed. Or else, some functions of AmpCon-Campus might not work.

Verifying License Validity

By using the **License Audit** feature, you can verify whether PicOS licenses are valid or not.

Verifying the PicOS License for a Switch

To check the PicOS license validity for a switch, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Device Licenses**.
2. In the **License Audit** tab, locate a PicOS license, and then click **License Audit**.

System Name	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.10.10.18	G1SA1X0000291	9.8.7-6w-36A20-EC142058876234	AB74-5D16-9AA2-92D2	2027-05-30 00:00:00	Active	License Audit Log
PICOS	10.10.10.26	G1SU1H000012	4.5.3E/2w4A9a29wP	0676-C5B9-5761-4FED	--	--	License Audit Log
PICOS	10.10.10.30	219801A6AM6242V00008	4.5.3E/513a799ca	FE09-5008-92FD-12FA	2025-12-31 00:00:00	Active	License Audit Log
PICOS	10.10.10.38	CN0ICFTTDCN008M035P	9.8.7-main/94641cauf	40ED-3482-4EE3-4398	2027-05-30 00:00:00	Active	License Audit Log
PICOS	10.10.10.42	G1R4213003031	4.7.0E-EC1a11b76461	0147-0C18-0A3F-358E	2030-02-26 00:00:00	Active	License Audit Log
		G1SUR8X000113C			--	--	License Audit Log
Switch-A	10.10.10.54	D4A50844A3A1	4.6.0E/9w70da68P	D3FA-87AD-64F1-C841	--	--	License Audit Log
Switch-B	10.10.10.58	D4A50844A3A2	4.6.0E/9w70da68P	BC3C-5F3A-DAB8-0A3A	--	--	License Audit Log

3. Click **Yes**.

4. Check the **License Expiry** and **License Status** columns.

- **License Expiry** means the expiration date of the PicOS license.
- **License Status** means the current status of the PicOS license. You might see the following license status:
 - **Expired:** The PicOS license is expired.
 - **Expiring:** The PicOS license will expire within the next 30 days.
 - **Active:** The PicOS license is valid and will not expire within the next 30 days.
 - **Unknown:** AmpCon-Campus hasn't retrieved the PicOS license status of the switch.
 - **No License:** The switch has no PicOS license installed.

5. Click **Log** to view the license audit logs.

G1SA1X0000291 logs

2025-08-12 04:24:19: start to upgrade switch image

2025-08-12 04:24:29: execute cmd [version] success, stdout:

```

[Copyright] : Copyright (C) 2009-2025 Picol, Inc. All Rights Reserved.
Model      : SS860-24MG-U
Software Version : 9.8.7-main-EC142058876234
Software Released Date : 08/05/2025
Serial Number : G1SA1X0000291
System Uptime : 0 day 0 hour 34 minute
Hardware ID : AB74-5D16-9AA2-92D2
License Type : 1G PicOS(R) Perpetual License
Device MAC Address : 64:96:9F:6F:05:3a
          
```

2025-08-12 04:24:29: execute cmd [cat ./etc/resolv.conf] success, stdout:

```

nameserver 1.0.0.1
nameserver 8.8.8.8
          
```

System Name	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.10.10.18	G1SA1X0000291	9.8.7-main-EC142058876234	AB74-5D16-9AA2-92D2	2027-05-30 00:00:00	Active	License Audit Log
PICOS	10.10.10.26	G1SU1H000012	4.5.3E/2w4A9a29wP	0676-C5B9-5761-4FED	--	--	License Audit Log
PICOS	10.10.10.30	219801A6AM6242V00008	4.5.3E/513a799ca	FE09-5008-92FD-12FA	2025-12-31 00:00:00	Active	License Audit Log
PICOS	10.10.10.38	CN0ICFTTDCN008M035P	9.8.7-main/94641cauf	40ED-3482-4EE3-4398	2027-05-30 00:00:00	Active	License Audit Log
PICOS	10.10.10.42	G1R4213003031	4.7.0E-EC1a11b76461	0147-0C18-0A3F-358E	2030-02-26 00:00:00	Active	License Audit Log
		G1SUR8X000113C			--	--	License Audit Log
Switch-A	10.10.10.54	D4A50844A3A1	4.6.0E/9w70da68P	D3FA-87AD-64F1-C841	--	--	License Audit Log
Switch-B	10.10.10.58	D4A50844A3A2	4.6.0E/9w70da68P	BC3C-5F3A-DAB8-0A3A	--	--	License Audit Log

Verifying PicOS Licenses for a Group of Switches

To check the PicOS license validity for a group of switches, follow these steps:

1. In the AmpCon-Campus UI, click **Resource > Device Licenses**.
2. In the **License Audit** tab, select a group name from the **Group Name** drop-down list, and then click **License Audit**.

System Name	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.10.10.26	G1SU1H000012	4.5.3E/2w4A9a29wP	0676-C5B9-5761-4FED	--	--	License Audit Log
PICOS	10.10.10.30	219801A6AM6242V00008	4.5.3E/513a799ca	FE09-5008-92FD-12FA	2025-12-31 00:00:00	Active	License Audit Log
PICOS	10.10.10.38	CN0ICFTTDCN008M035P	9.8.7-main/94641cauf	40ED-3482-4EE3-4398	2027-05-30 00:00:00	Active	License Audit Log

3. Check the **License Expiry** and **License Status** columns.

- **License Expiry** means the expiration date of the PicOS license.
 - **License Status** means the current status of the PicOS license. You might see the following license status:
 - **Expired:** The PicOS license is expired.
 - **Expiring:** The PicOS license will expire within the next 30 days.
 - **Active:** The PicOS license is valid and will not expire within the next 30 days.
 - **Unknown:** AmpCon-Campus hasn't retrieved the PicOS license status of the switch.
 - **No License:** The switch has no PicOS license installed.
4. Optional: Select the newly generated report from the **Time Selection** drop-down list, and then click **View Report**.

NOTE

The **View Report** button is applicable only to License Audit operations based on groups.

The screenshot shows the 'License Audit' tab in the AmpCon-Campus UI. At the top, there are tabs for 'License Audit', 'License Action', and 'Local License'. Below these, there's a 'Group Name' dropdown set to 'all', and a 'Time Selection' dropdown set to 'Select Time'. The 'View Report' button is highlighted with a red box. Below this is a table with the following data:

System	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.0.0.26	G1S134000012	4.4.5.26/2e549c29e9	0676-C5B9-5761-6FED	--	--	License Audit Log
PICOS	10.0.30	219801A6AM6242V0000B	4.5.3E/5173a799ca	FE09-500B-92FD-12FA	2025-12-31 00:00:00	Active	License Audit Log
PICOS	10.0.38	CN0J0FF0ND0008M0359	9.8.7-main/f9641c0af	40ED-34B2-4EE3-439B	2027-05-30 00:00:00	Active	License Audit Log

At the bottom right, it says '1 of 3 items' and '10 / page'.

Verifying License Validity and Extending Expired Licenses

By using the **License Action** feature, you can verify whether PicOS licenses are valid and extend expired PicOS licenses if these PicOS licenses are extended in the [License Portal](#).

Verifying and Extending the PicOS License for a Switch

1. In the AmpCon-Campus UI, click **Resource > Device Licenses**.
2. Click the **License Action** tab.

The screenshot shows the 'License Action' tab in the AmpCon-Campus UI. At the top, there are tabs for 'License Audit', 'License Action', and 'Local License'. Below these, there's a 'Group Name' dropdown set to 'Select Group Name', and a 'Time Selection' dropdown set to 'Select Time'. The 'View Report' button is also present. Below this is a table with the following data:

System	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.0.18	G1SA1X0000291	9.8.7-fw-16620-EC1a35887a294	AB74-5D16-9AA2-7D2D	2027-05-30 00:00:00	Active	License Action Log
PICOS	10.0.26	G1S134000012	4.4.5.26/2e549c29e9	0676-C5B9-5761-6FED	--	--	License Action Log
PICOS	10.0.30	219801A6AM6242V0000B	4.5.3E/5173a799ca	FE09-500B-92FD-12FA	2025-12-31 00:00:00	Active	License Action Log
PICOS	10.0.38	CN0J0FF0ND0008M0359	9.8.7-main/f9641c0af	40ED-34B2-4EE3-439B	2027-05-30 00:00:00	Active	License Action Log
PICOS	10.0.42	G1B4211001031	4.7.0E-EC1a31b7b4b1	0147-0C3B-0A3F-358E	2030-02-26 00:00:00	Active	License Action Log
PICOS	10.0.54	G1S18R300011C	--	--	--	--	License Action Log
Switch-A	10.0.54	DAA30844A3A1	4.6.0E/9bc70da609	D3FA-87AD-64F1-CB41	--	--	License Action Log
Switch-B	10.0.58	DAA30844A3A2	4.6.0E/9bc70da609	8C3C-5F3A-DAB8-0A3A	--	--	License Action Log

At the bottom right, it says '1 of 8 items' and '10 / page'.

3. Locate a license, and then click **License Action**.
4. Click **Yes**.

5. Check the **License Status** and **License Expiry** columns. License expiry means the expiration date of the PicOS license. License status means the current status of the PicOS license.
6. Optional: Click **Log** to view the License Action logging information.

Verifying and Extending PicOS Licenses for a Group of Switches

1. In the AmpCon-Campus UI, click **Resource > Device Licenses**.
2. Click the **License Action** tab.
3. Select a group name from the **Group Name** drop-down list, and then click **License Action**.

System	IP Address	Switch SN	Version	Hardware ID	License Expiry	License Status	Operation
PICOS	10.10.10.18	G15A3D0000291	9.8.7-6w-56420-EC14358876234	AB74-5D16-9AA2-70D2	2027-05-30 00:00:00	Active	License Action Log
PICOS	10.10.10.26	G15U1H0000012	4.4.5.26/2w44629wP	0679-C389-5761-6FED	--	--	License Action Log
PICOS	10.10.10.30	Z19801A6A44242V00008	4.5.3E/513a799ca	F009-5006-92FD-12FA	2025-12-31 00:00:00	Active	License Action Log
PICOS	10.10.10.38	CNDJFTYDNC0008H0359	9.8.7-main/56441ca4f	40ED-548D-4EE3-4398	2027-05-30 00:00:00	Active	License Action Log
PICOS	10.10.10.42	G1R4213001031	4.7.0E-EC13a116794b1	0147-0C38-0A3F-358E	2030-02-26 00:00:00	Active	License Action Log
		G15U6R300011C			--	--	License Action Log
Switch-A	10.10.10.54	D4A50844A3A1	4.6.0E/9w70a689	D3FA-B7AD-64F1-C841	--	--	License Action Log
SwitchB	10.10.10.58	D4A50844A3A2	4.6.0E/9w70a689	8C3C-5F3A-DA88-6A3A	--	--	License Action Log

4. Check the **License Status** and **License Expiry** columns. License expiry means the expiration date of the PicOS license. License status means the current status of the PicOS license.
5. Optional: Select the newly generated report from the drop-down list, and then click **View Report**.

NOTE

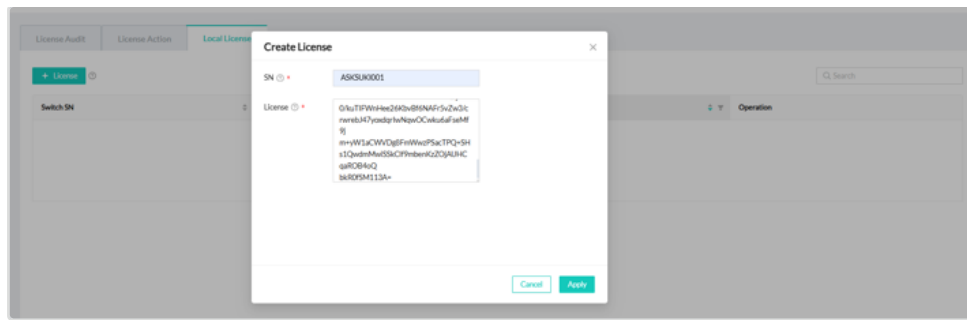
The **View Report** button is applicable to only License Action operations based on groups.

Adding Local PicOS Licenses

To add a local PicOS license, follow these steps:

1. Click **Resource > Device Licenses**.
2. Click the **Local License** tab, and then click **Add License**.

3. In the **SN** field, enter the SN of the switch with the uploaded PicOS license.
4. In the **License** field, enter the local PicOS license key.



5. Click **Apply**.

Managing User Access

After you deploy AmpCon-Campus, you can manage user access so that users are assigned with appropriate permissions.

NOTE

Only users with the **SuperAdmin** role have access to the “User Management” page. Adding, editing, or deleting users, login restrictions, and TACACS+ configuration are only available to AmpCon-Campus users with the **SuperAdmin** role.

[Role-Based Access Control](#)

[Adding a Global User or a Group User](#)

[Managing All Added Users](#)

[User Self-Management](#)

[Editing Users](#)

[Deleting Users](#)

[Setting Login Restrictions for AmpCon-Campus Users](#)

[User Permissions on Menu Pages](#)

[Configuring TACACS+ Authentication and Authorization](#)

Role-Based Access Control

Role-Based Access Control (RBAC) is used to permit individual users to perform specific actions and get visibility to an access scope. Each user can be assigned to a specific role with associated permissions.

AmpCon-Campus supports the following user roles. The permission levels are as follows: SuperAdmin > Admin > Operator > Readonly.

• **SuperAdmin**

- Provides access to all AmpCon-Campus functions
- The only role that can manage users and groups

• **Admin**

- Provides access to almost all AmpCon-Campus functions
- Can't manage users and groups
- Can't access Switch model and System Config
- Can't access Wireless-related pages and tabs (Wireless View, AP, Manage, Access Points, Inventory, Wireless Profiles, and Wireless Clients)

• **Operator**

- Provides access to most of AmpCon-Campus functions
- Can't manage users and groups

- Can't access Switch model and System Config
- Can't view and manage licenses and can't view license logs
- Can view but can't configure Campus Fabric and Wired Clients
- Can't access Wireless-related pages and tabs (Wireless View, AP, Manage, Access Points, Inventory, Wireless Profiles, and Wireless Clients)

• Readonly

- Views limited pages such as System Overview, Switch Overview, Topologies, Switches, Config Files View, Template Verify, Config Archive Diff, Alert List, Notification History, Telemetry, SNMP Management, and Web Access

Adding a Global User or a Group User

When you add a user, you need to select a user role for the user and specify the user type (a group user or a global user).

- A group user means that the user can manage one or multiple switch groups.
- A global user means that the user is not limited to any switch group.

To add a user, follow these steps:

1. Click **System > User management** from the navigation bar.
2. Click **+ User**, and enter the following information:

Table 1. User Parameters

Parameter	Description
User Name	Specify the username. The username must be unique.
User Password	Specify the password of the user. The password needs to be a combination of uppercase letters, lowercase letters, numbers, and special symbols. The character count needs to be greater than 10.

Confirm Password	Specify the password of the user.
User Role	Select SuperAdmin , Admin , Operator , or Readonly .
User Type	Select Global or Group, which means creating a global user or a group user. If you select Group, select an added switch group from the Group Name drop-down list. To add multiple switch groups, click the plus icon +. NOTE Ensure that the selected switch group has been created. For more information about creating groups, see Adding a Switch Group.
Email	Specify the email of the user.

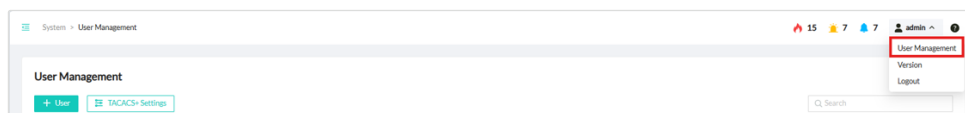
3. Click **Apply**.

Managing All Added Users

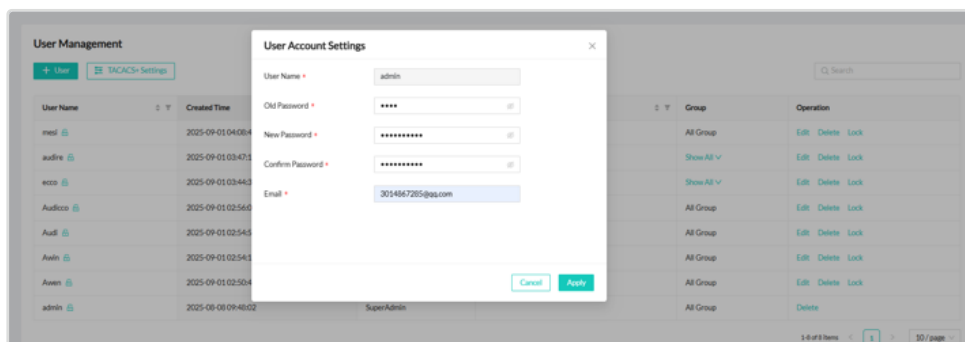
User Self-Management

All AmpCon-Campus users can change their own passwords and email addresses. Follow these steps:

1. In the AmpCon-Campus UI, click the username, and then click **User Management**.



2. To change the user password, enter a new password in the **New Password** field, and then enter the password again in the **Confirm Password** field.



3. To change the email address associated with the AmpCon-Campus user, enter a new email address in the **Email** field.
4. Click **Apply**.

Editing Users

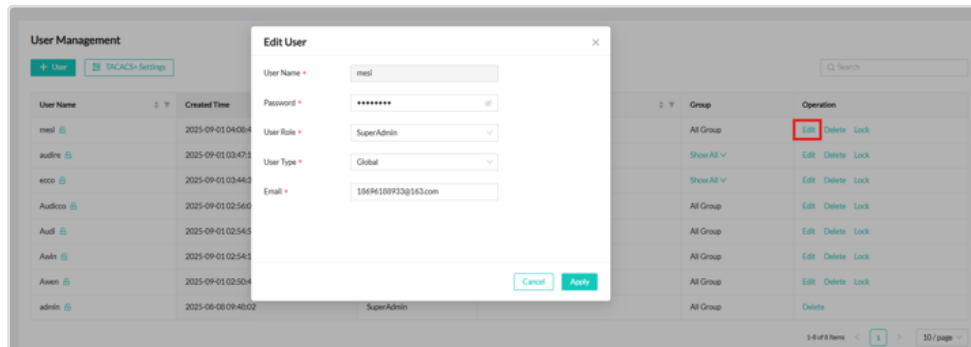
To edit an added user, follow these steps:

1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.
2. Click **System > User management** from the navigation bar.
3. On the “User Management” page, locate a user, and then click **Edit**.

NOTE

The built-in user **admin** can't be edited here.

4. Modify user information as needed.



5. Click **Apply**.

Deleting Users

To delete an added AmpCon-Campus user, follow these steps:

1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.
2. Click **System > User management** from the navigation bar.
3. On the “User Management” page, locate a user, and then click **Delete**.

NOTE

The built-in user **admin** can't be deleted.

User Management

+ User TACACS+ Settings

Q Search

User Name	Created Time	Role	Email	Group	Operation
meat	2025-09-01 04:08:42	SuperAdmin	18696188923@163.com	All Group	Edit Delete Lock
audre	2025-09-01 03:47:12	SuperAdmin	18696188923@163.com	Show All	Edit Delete Lock
ecco	2025-09-01 03:44:36	Admin	18696188923@163.com	Show All	Edit Delete Lock
Audico	2025-09-01 02:56:00	Readonly	18696188923@163.com	All Group	Edit Delete Lock
Audi	2025-09-01 02:54:53	Operator	18696188923@163.com	All Group	Edit Delete Lock
Awin	2025-09-01 02:54:11	Admin	18696188923@163.com	All Group	Edit Delete Lock
Awen	2025-09-01 02:50:42	SuperAdmin	18696188923@163.com	All Group	Edit Delete Lock
admin	2025-08-08 09:48:02	SuperAdmin		All Group	Delete

1-8 of 8 items 1 10 / page

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

Setting Login Restrictions for AmpCon-Campus Users

You can lock an added user so that the user can't be used to log in to the AmpCon-Campus UI. Or you can unlock an added user to enable the login again.

NOTE

The built-in user **admin** can't be locked or unlocked.

- To lock an added user, follow these steps:
 1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.
 2. Click **System > User management** from the navigation bar.
 3. On the "User Management" page, locate a user, and then click **Lock**.
 4. In the pop-up window, click **Yes** to confirm the lock operation.
- To unlock an added user, follow these steps:
 1. Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.
 2. Click **System > User management** from the navigation bar.
 3. On the "User Management" page, locate the locked user, and then click **Unlock**.

User Management

+ User TACACS+ Settings

Q Search

User Name	Created Time	Role	Email	Group	Operation
meat	2025-09-01 04:08:42	SuperAdmin	18696188923@163.com	All Group	Edit Delete Unlock
audre	2025-09-01 03:47:12	SuperAdmin	18696188923@163.com	Show All	Edit Delete Lock
ecco	2025-09-01 03:44:36	Admin	18696188923@163.com	Show All	Edit Delete Lock
Audico	2025-09-01 02:56:00	Readonly	18696188923@163.com	All Group	Edit Delete Lock
Audi	2025-09-01 02:54:53	Operator	18696188923@163.com	All Group	Edit Delete Lock
Awin	2025-09-01 02:54:11	Admin	18696188923@163.com	All Group	Edit Delete Lock
Awen	2025-09-01 02:50:42	SuperAdmin	18696188923@163.com	All Group	Edit Delete Lock
admin	2025-08-08 09:48:02	SuperAdmin		All Group	Delete

1-8 of 8 items 1 10 / page

4. In the pop-up window, click **Yes** to confirm the unlock operation.

Now you can log in to the AmpCon-Campus UI with the user again.

User Permissions on Menu Pages

For menu pages in the AmpCon-Campus UI, different user roles have different permissions. For more information, see the [User Permission Table](#) topic.

Configuring TACACS+ Authentication and Authorization

In addition to using local users (global users or group users), you can also enable the TACACS+ integration to manage user access. For more information, see the [Configuring TACACS+ Authentication and Authorization](#) topic.

User Permission Table

For menu pages and tabs in the AmpCon-Campus UI, different user roles have different permissions. See the following table:

NOTE

Tabs that share the same permission level under the same menu are not shown in the table.

User Permissions on Menu Pages and Tabs

Table 1. Menu and Tab Permissions

First-level menu	Second-level menu	Third-level menu	Tab	Super Admin	Admin	Operator	Read only
Dashboard	System Overview			✓	✓	✓	✓
	Switch Overview			✓	✓	✓	✓
	Wireless View			✓	✗	✗	✗
Network Design	Topologies			✓	✓	✓	✓
	Campus Fabric			✓	✓	✓	✗
	Overlay Service Activation			✓	✓	✓	✗
	Switch Templates			✓	✓	✓	✗
Resource	Upgrade Management		Switch	✓	✓	✓	✗
			AP	✓	✗	✗	✗

	Device Licenses		Licens e Audit	✓	✓	✓	✗
			Licens e Action	✓	✓	✓	✗
			Local Licens e	✓	✓	✓	✗
	Group Manage ment			✓	✗	✗	✗
	Site Manage ment			✓	✓	✓	✗
Wireles s	Manage			✓	✗	✗	✗
	Access Points			✓	✗	✗	✗
	Inventory			✓	✗	✗	✗
	Wireless Profiles			✓	✗	✗	✗
Wired	Switches			✓	✓	✓	✓
	Wired Profiles		Global Config uration	✓	✓	✓	✗
			Switch Config uration	✓	✓	✓	✗
			Config File View	✓	✓	✓	✓
			Switch Model	✓	✗	✗	✗

			System Configuration	✓	✗	✗	✗
		Config Templates	New Template	✓	✓	✓	✗
			Template List	✓	✓	✓	✗
			Push Config	✓	✓	✓	✗
			Template Verify	✓	✓	✓	✓
			Config Archive Diff	✓	✓	✓	✓
			Config Backup	✓	✓	✓	✗
Monitor	Alerts	Alert List		✓	✓	✓	✓
		Notification Rules		✓	✓	✓	✗
		Notification History		✓	✓	✓	✓
	Telemetry			✓	✓	✓	✓
	SNMP Management	SNMP Data Filtering		✓	✓	✓	✓
		SNMP Visualization		✓	✓	✓	✓

		tion					
	Wired Clients			✓	✓	✓	✗
	Wireless Clients			✓	✗	✗	✗
Maintain	Automation	Playbooks		✓	✓	✓	✗
		Other Devices		✓	✓	✓	✗
		Ansible Jobs		✓	✓	✓	✗
		Schedule		✓	✓	✓	✗
	System Backup			✓	✓	✓	✗
	Web Access			✓	✓	✓	✓
System	User Management			✓	✗	✗	✗
	Email Settings			✓	✓	✓	✗
	Software Licenses	License View		✓	✓	✗	✗
		License Management		✓	✓	✗	✗
		License Log		✓	✓	✗	✗

Configuring TACACS+ Authentication and Authorization

AmpCon-Campus supports integrating with the Terminal Access Controller Access Control System (TACACS+) server to do authentication and authorization for the AmpCon-Campus login users.

In addition to using local users (global users or group users), you can also enable the TACACS+ integration to manage user access.

[Before You Begin](#)

[Procedure](#)

[Sample Configuration of Authorization Level on TACACS+ Server \(Linux tac_plus\)](#)

Before You Begin

Before you enable the TACACS+ integration, read the following notes:

- You can configure at most two TACACS+ servers on the AmpCon-Campus server. One is the primary and active server, while the other one is the secondary server, which is used for backup. Configure the secondary server only when backup is needed.
- You can designate authorization levels by using the **priv-lvl** parameter on the TACACS+ server. The **priv-lvl** configuration is sent in the TACACS+ authorization response. The **priv-lvl** parameter value is mapped to one of these local role levels: Readonly, Operator, Admin, and Superadmin.

For how to configure authorization levels on the TACACS+ server, see the [Sample Configuration of Authorization Level on TACACS+ Server \(Linux tac_plus\)](#) section.

- AmpCon-Campus sends authorization requests with **“Arg[0]” service=AmpCon-Campus**. On the TACACS+ server, you need to set the value of the parameter **“service=AmpCon-Campus”** to process authorization requests of AmpCon-Campus users.
- If both the primary and the secondary TACACS+ servers are unreachable, you can use local users (global user or group user) to log in to the AmpCon-Campus UI.

Procedure

To enable the TACACS+ integration, follow these steps:

1. In the AmpCon-Campus UI, click **System > User management**.
2. Click **TACACS+ Settings**.



3. In the pop-up window, input the following information:

Table 1. TACACS+ Setting Parameters

Parameter	Description
Enable	Toggle it on to enable TACACS+ authentication and authorization.
Primary Server IP	The IP address of the primary TACACS+ server.
Secondary Server IP	Optional. The IP address of the backup TACACS+ server.
Server Key	The shared key of TACACS+. NOTE The value of the Server Key field needs to be the same as the shared keys of the primary and secondary TACACS+ servers. The shared keys on both TACACS+ servers need to be the same.
Session Timeout	The TACACS+ connection timeout in seconds.
Auth Protocol	The authentication protocol type of TACACS+ including ASCII , PAP , or CHAP .
TACACS+ User Level Mapping	The mapping ranges for TACACS+ authorization. The configuration page displays the default mapping values. You can configure a custom range for mapping values. The values are integers that range from 0 to 15.

NOTES

- Don't overlap any range with other ranges among different user levels.
- If the **priv-lvl** configuration of a user on the TACACS+ server is not found in the level-mapping configuration on AmpCon-Campus, the user role level is mapped to **Readonly**.

4. Click **Apply**.

Sample Configuration of Authorization Level on TACACS+ Server (Linux tac_plus)

For how to configure authorization levels on the TACACS+ server, see the following example:

```
user = leontest {
    global = cleartext "abc"
    service = AmpCon {
        default attribute = permit
        priv-lvl = 15
    }
}

user = automation1 {
    global = cleartext "automation"
    service = AmpCon {
        default attribute = permit
        priv-lvl = 10
    }
}

user = testtest {
    global = cleartext "testtest"
    service = AmpCon {
        default attribute = permit
        priv-lvl = 5
    }
}

user = testpica8 {
    global = cleartext "testpica8"
```

```
service = AmpCon {  
    default attribute = permit  
    priv-lvl = 1  
}  
}
```

Administering AmpCon-Campus

You can administer AmpCon-Campus by using the user interface. For more information, see the following child topics:

- [Updating the Encryption Key for Sensitive Data Encryption](#)
- [Forwarding Logs to External Syslog Servers](#)
- [Backing Up and Restoring the AmpCon-Campus Database](#)

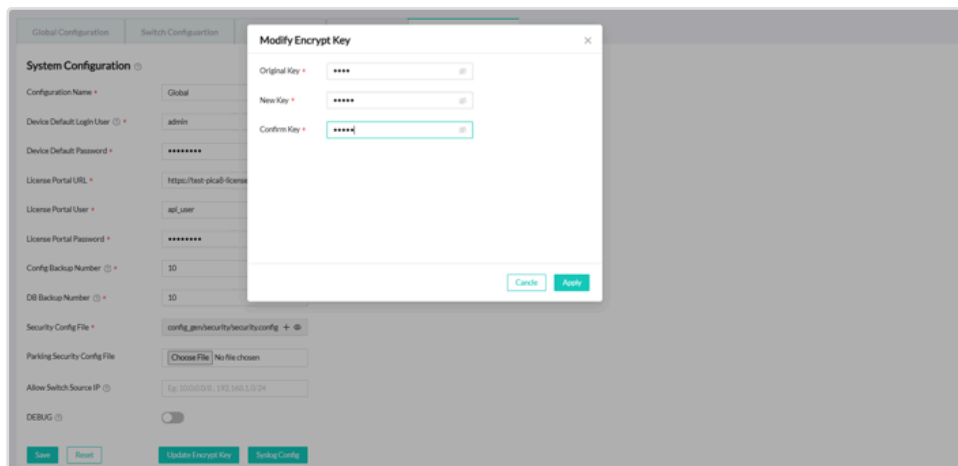
Updating the Encryption Key for Sensitive Data Encryption

After you deploy AmpCon-Campus, a default encryption key is generated to encrypt sensitive data (such as passwords) in the AmpCon-Campus database, ensuring sensitive data security. You can update the encryption key as you need.

Procedure

To update the encryption key, follow these steps:

1. Log in to the AmpCon-Campus UI, and click **Wired > Wired Profiles**.
2. In the **System Configuration** tab, click **Update Encrypt Key**.
3. Enter the original key and the new key. The default encryption key is **pica8pica8**



3. Click **Apply**.

Forwarding Logs to External Syslog Servers

You can forward AmpCon-Campus logs to other external Syslog servers.

[Prerequisite](#)

[Procedure](#)

[Verifying Syslog Forwarding](#)

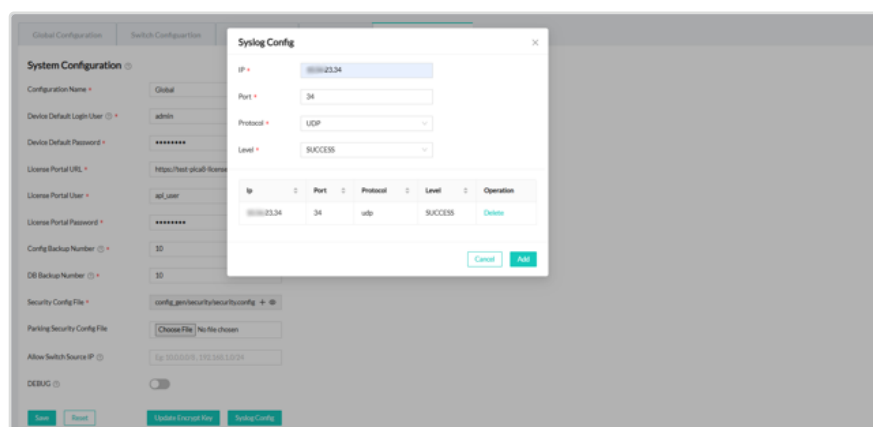
Prerequisite

Ensure that the Syslog service of the target server is enabled.

Procedure

1. Log in to the AmpCon-Campus UI, and click **Wired > Wired Profiles**.
2. In the **System Configuration** tab, click **Syslog Config**.
3. Enter the following information:
 - **IP:** The IP address of the external Syslog server.
 - **Port:** The port number of the external Syslog server.
 - **Protocol:** TCP or UDP.
 - **Level:** SUCCESS or ERROR. The mapping rules of AmpCon-Campus Log levels and Syslog rules are as follows:
 - **SUCCESS** is equal to **info (level=6)**
 - **ERROR** is equal to **warning (level=4)**

For example, if the ERROR level is specified, the Syslog server receives logs with a warning level or higher from AmpCon-Campus.



4. Click **Add**.

Verifying Syslog Forwarding

To verify whether AmpCon-Campus logs can be forwarded to the Syslog server, follow these steps:

1. Log in to the AmpCon-Campus UI, and click **Wired > Wired Profiles**.
2. Click the **System Configuration** tab.
3. In the **License Portal User** field, enter an incorrect username, and click **Save**.

The screenshot shows the 'System Configuration' tab in the AmpCon-Campus UI. The 'License Portal User' field is highlighted with a red box and contains the text 'not_'. A red error message at the top states: 'The license connect failed. (error: invalid username)'.

3. Access the AmpCon-Campus server by using MobaXterm for verification.

The screenshot shows a MobaXterm terminal window with a successful SSH connection to the AmpCon-Campus server. The terminal output includes system updates and network traffic details.

```

*** System restart required ***
Last login: Tue Aug 6 10:36:58 2024 from 10.30.1
pic@picad:~$ cd /usr/share/automation/server/
pic@picad:~$ sudo tcpdump -i any host 10.20.186 and port 22
tcpdump: data link type LINUX_SLL2
tcpdump: interface is: vethfd17c48
10:52:37.580600 vethfd17c48 P IP 128.2.56418 > 20.186.ssh: Flags [S], seq 686753351, win 64240,
options [mss 1460,sackOK,TS val 331022364,ecr 0,nop,wscale 7], length 0
10:52:37.580600 br-44b1e82bc238 In IP 128.2.56418 > 20.186.ssh: Flags [S], seq 686753351, win 64
240, options [mss 1460,sackOK,TS val 331022364,ecr 0,nop,wscale 7], length 0
10:52:38.606759 vethfd17c48 P IP 128.2.56418 > 20.186.ssh: Flags [S], seq 686753351, win 64240,
options [mss 1460,sackOK,TS val 331022364,ecr 0,nop,wscale 7], length 0
10:52:40.622770 vethfd17c48 P IP 128.2.56418 > 20.186.ssh: Flags [S], seq 686753351, win 64240,
options [mss 1460,sackOK,TS val 331022364,ecr 0,nop,wscale 7], length 0
10:52:40.622770 br-44b1e82bc238 In IP 128.2.56418 > 20.186.ssh: Flags [S], seq 686753351, win 64
240, options [mss 1460,sackOK,TS val 331022364,ecr 0,nop,wscale 7], length 0

```

Backing Up and Restoring the AmpCon-Campus Database

You can back up and restore the AmpCon-Campus database securely for disaster recovery.

[Prerequisite](#)

[Creating a Database Backup](#)

[Restoring from a Database Backup](#)

[Optional: Editing a Database Backup](#)

[Optional: Removing a Database Backup](#)

Prerequisite

The allowed maximum number of database backups is set based on the **DB Backup Number** field in the **System Configuration** tab.

Before you create a database backup, ensure that the current backup number doesn't reach the allowed maximum number. You can remove a database backup if it is not needed.

The screenshot shows the 'System Configuration' tab in the AmpCon-Campus UI. The 'DB Backup Number' field is highlighted with a red box, indicating the maximum number of database backups allowed. The value is set to 3. Other fields include Configuration Name (Global), Device Default Login User (admin), Device Default Password (masked), License Portal URL (https://license.pica8.com), License Portal User (api_user), License Portal Password (masked), Config Backup Number (3), Security Config File (config_gen/security/security.config), Parking Security Config File (config_gen/security/parking_security.config), Allow Switch Source IP (Eg: 10.0.0.0/8, 192.168.1.0/24), and DEBUG (disabled).

Creating a Database Backup

To create a database backup, follow these steps:

1. Log in to the AmpCon-Campus UI, and click **Maintain > System Backup**.
2. Click **Backup**. The **Create Backup Config** pop-up window opens.

The screenshot shows the 'Create Backup Config' pop-up window. The fields are: Backup Name (ltd), Encrypt Key (pica8pica8), and AmpCon Version (2.0.0/2.3.0-dev-420512957). The window has 'Cancel' and 'Apply' buttons at the bottom.

3. Enter the following information:

- **Backup Name:** The name of the backup to differentiate from the other backups.
- **Encrypt Key:** The encrypt key that you set in the global **System Config** tab. The default encrypt key is pica8pica8
- **AmpCon Version:** The version of AmpCon-Campus that you use.

4. Click **Apply**.

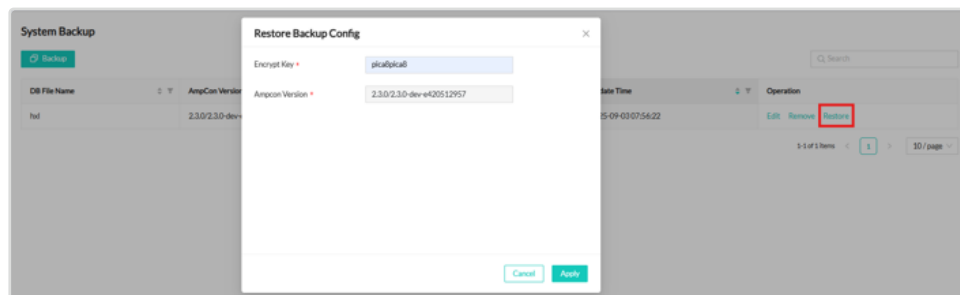
Restoring from a Database Backup

To restore from a database backup, follow these steps:

NOTE

The restore operation can only be executed once, and after an update, previous files cannot be restored.

1. Log in to the AmpCon-Campus UI, and click **Maintain > System Backup**.
2. Locate the backup, and click **Restore** on the right.
3. In the **Restore Backup Config** pop-up window, enter the following information:
 - **Encrypt Key:** The encrypt key that you set in the global **System Config** tab. The default encrypt key is pica8pica8
 - **AmpCon Version:** The version of AmpCon-Campus that you use.

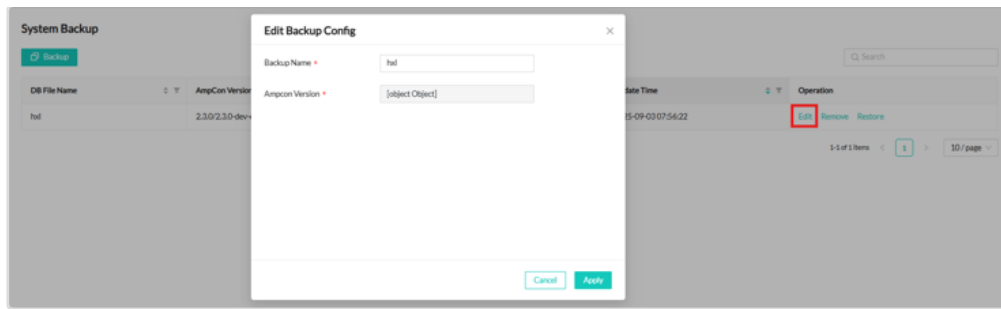


4. Click **Apply**.

Optional: Editing a Database Backup

To edit a database backup, follow these steps:

1. Log in to the AmpCon-Campus UI, and click **Maintain > System Backup**.
2. Locate the backup, and click **Edit** on the right.
3. In the **Edit Backup Config** pop-up window, modify the backup name or AmpCon-Campus version as you need.

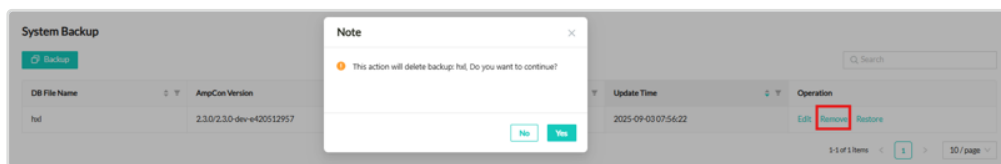


4. Click **Apply**.

Optional: Removing a Database Backup

To remove a database backup, follow these steps:

1. Log in to the AmpCon-Campus UI, and click **Maintain > System Backup**.
2. Select the backup, and click **Remove** on the right.
3. Click **Yes** to confirm the removal.



Accessing Devices through SSH Sessions

You can connect to a device (such as a switch or terminal device) from the AmpCon-Campus UI by creating an SSH session.

AmpCon-Campus improves device access flexibility and security by supporting two types of authentication: password and SSH keys.

[Benefits](#)

[Procedure](#)

[Password Authentication](#)

[SSH Key Authentication](#)

Benefits

You can choose either authentication type to access a device. The following benefits are provided:

- **Flexibility**

Password authentication is suitable for environments with lower security and higher usability demands, while SSH key authentication provides stronger security for high security scenarios. Choose the authentication type that best fits your needs for flexible device access.

- **Security**

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 securely stored and never transmitted over the network, eliminating theft risk and enhancing session security.

Procedure

Click **Maintain > Web Access** from the navigation bar, and then you can use either password or SSH key authentication to access a device.

Password Authentication

To access a device by using password authentication, follow these steps:

1. In the **Select Authentication** radio box, select **Password**.
2. Input the following information:

Web Access

Select Authentication ☒ Password ☐ SSH Key

Host * User Name * Password *

Port * Session *

New Tab ☒

Table 1. Password Parameters

Parameter	Description
Host	The IP address of the device.
User Name	The username to log in to the device. NOTES - The value is a string with at most 32 characters. The following characters are supported: - Lowercase letters including a to z. - Uppercase letters including A to Z. - Digits including 0 to 9. - Special characters (_ - .). - Username cannot start with a special character (_ - .).
Password	The password of the user.
Port	The port to establish the session.
Session	Select SSH .
New Tab	Toggle on or off to open the SSH session in a new browser tab or not.

3. Click **Submit**.

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 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.

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 are recommended to use the **scp**

command. For example, run the following command on the device side.

```
sudo scp pica8@10.56.xx.xx:/tmp/id_rsa.pub  
/home/key_user/.ssh/authorized_keys
```

Then, the public key will be copied from the server 10.56.x.x to the device.

1. In the **Select Authentication** radio box, select **SSH Key**.
2. Input the following information:

Web Access

Select Authentication ☐ Password ☒ SSH Key

Host *

User Name *

Key * [Upload](#)

Passphrase

Port *

Session *

New Tab ☒

[Submit](#)

Table 2. SSH Key Parameters

Parameter	Description
Host	The IP address of the device.
User Name	The username to log in to the device. NOTE • The value is a string with at most 32 characters. The following characters are supported: ◦ Lowercase letters including a to z. ◦ Uppercase letters including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ - .). • Usernames cannot start with a special character (_ - .).
Key	The private key generated by using the ssh-keygen command. Click Upload , find the file where the private key is saved, and upload it.

Passphrase	Optional. The password used to protect the SSH keys. You can choose whether to specify a passphrase when generating the SSH keys. If you do not specify a passphrase when generating SSH keys, you must leave this field blank.
Port	The port to establish the session.
Session	Select SSH .
New Tab	Toggle on or off to open the SSH session in a new browser tab or not.

3. Click **Submit**.

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](#) [H](#) [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.
- : 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).