AmpCon-Campus Management Platform User Manual V2.2.0

Release Notes

Before you install or upgrade AmpCon-Campus, read this topic to get a quick overview of what is added, changed, improved, or deprecated in each release.

AmpCon-Campus 2.2.0

New Features

The following features are added to AmpCon-Campus 2.2.0:

- Supports designing MLAG campus fabrics for small or mid-size campus networks and designing IP Clos campus fabrics for large-scale campus networks. For more information, see Designing Campus Fabircs.
- Supports receiving immediate alarm notifications through emails when issues arise. For more information, see Alarm Notifications.
- Supports automatically identifying terminal devices connected to each managed switch and manually adding terminal devices. For more information, see Wired Clients.

Improvements

The following improvements are added to AmpCon-Campus 2.2.0:

- The supported switch list is updated with more supported switch models. For more information, see Supported Switches for 2.2.0.
- When you click a switch in a topology, the **Client Info** tab is displayed, where you can see metrics of terminal devices connected to the switch. For more information, see Client Info.
- The following telemetry metrics are added to the “Telemetry Dashboard” page. For more information, see Global Telemetry Data.
  - **CPU usage**
  - **Memory usage**
  - **Fan**
  - **In Bits Rate**
  - **Out Bits Rate**
  - **Out Pkts Rate**
  - **In Pkts Rate**
- The following telemetry metrics are added to the detail page of each managed switch. For more information, see Telemetry Data of a Switch.
  - Added **Version** (means PicOS version) in the **Device Information** tab
  - Added **In Bits Rate**, **Out Bits Rate**, **Out Pkts Rate**, **In Pkts Rate**, **Usage**, and **Fan** in the **Switch Overview** tab
  - Added **In Bandwidth Utilization**, **Out Bandwidth Utilization**, **Out Bits Rate**, **In Bits Rate**, **Out Pkts Rate**, and **In Pkts Rate** in the **Port Overview** tab
  - Added a **Device Overview** tab with Redundant Power Supply Unit (RPSUs) and fans related metrics
  - Added an **ARP** tab with ARP-related metrics
  - Added a **MAC** tab with MAC-related metrics
  - Added an **OSPF** tab with OSPF-related metrics
  - Added a **BGP** tab with BGP-related metrics
  - Added an **IP Route** tab with IP Route related metrics
- The following resource usage related alarms are supported. For more information, see Resource Usage Alarms.
  - The CPU usage is over 85%
  - The memory usage is over 85%

- The input bandwidth usage is over 85%
- The output bandwidth usage is over 85%
- The switch is offline
- The switch is powered down
- The proportion of the fan's Pulse Width Modulation (PWM) to the total width is over 85%

New Changes

- The recommended PicOS version for supported switches is PicOS 4.6.0E or later.
- Importing the AmpCon-Campus license is no longer required during initial UI login. You can log in to the AmpCon-Campus UI first and then import the license. For more information, see Importing AmpCon-Campus Licenses.

Overview

AmpCon-Campus Management Platform is a powerful management platform for PicOS® campus switches, offering automated Zero Touch Provisioning (ZTP), real-time telemetry monitoring, topology auto-discovery, and automated lifecycle management. In addition, AmpCon-Campus supports designing and managing MLAG fabrics and IP Clos fabrics and monitoring terminal devices.

With an intuitive web-based UI, AmpCon-Campus automates routine workflows, eliminating costly downtime and time-consuming manual tasks. By using AmpCon-Campus, you can efficiently deploy, orchestrate, and manage campus networks at scale.

Deployed as a software appliance on a virtual machine (VM) or Docker, AmpCon-Campus operates seamlessly in campus networks.

How AmpCon-Campus Can Help

AmpCon-Campus is highly scalable and includes only the features that you truly need. You can use it to build small, medium, and large campus networks.

- **Simplify physical network design**

By using AmpCon-Campus, you can design MLAG campus fabrics for small or mid-size campus networks and design IP Clos campus fabrics for large-scale campus networks.

AmpCon-Campus helps you eliminate the complex campus networking configurations during the fabric design and management process.

- **Enhance terminal device management**

AmpCon-Campus supports automatically identifying terminal devices connected to each managed switch and manually adding terminal devices.

By using this feature, you can accurately and securely identify terminal devices in your network and thus facilitate refined management of terminal devices.

- **Automate switch configurations and provide unified switch management**

AmpCon-Campus helps you to configure, monitor, and manage switches in campus networks.

By using AmpCon-Campus, you can maintain the High-Performance Network (HPN) architecture more efficiently, prevent and eliminate issues, and thus increase the resource utilization rate and decrease the operation costs.

- **Improve the efficiency of switch deployment by using ZTP**

AmpCon-Campus supports using ZTP to automatically deploy switches in campus networks.

- **Provide telemetry for real-time network monitoring**

AmpCon-Campus supports telemetry to capture rich information about real-time network telemetry information, application workload usage, and system configurations.

- **Provide automatic discovery of topology for visual switch management**

AmpCon-Campus supports automatic discovery of topology to provide the network view of switches in all locations. You can simplify the

network management by checking switch stats and port-level running status.

- **Automate daily operation tasks by using Ansible playbooks**

AmpCon-Campus supports using Ansible playbooks to automate daily network operations and decrease the operation cost.

- **Deliver multiple deployment solutions**

AmpCon-Campus provides multiple deployment solutions, including Docker, KVM, VMware, and Nutanix AHV.

- **Support deploying, configuring, and managing remote switches at scale**

AmpCon-Campus makes it easy to deploy, configure, and manage a large number of remote switches. You can use AmpCon-Campus to deploy, configure, or manage switches at scale.

Key Features

AmpCon-Campus provides a powerful feature set, which simplifies the deployment, configuration, and management of switches.

Zero Touch Provisioning

Zero Touch Provisioning (ZTP) is a technology for automated deployment and configuration of network devices. When large numbers of switches need to be deployed or upgraded, you can use ZTP to reduce labor costs and improve deployment efficiency. ZTP can help you to implement fast, accurate, and reliable switch deployments.

In scenarios like the construction or expansion of campus networks, a large number of switches are required. If these switches are configured manually, improper configurations might lead to errors, and it’s difficult to troubleshoot issues.

AmpCon-Campus provides ZTP, which improves the efficiency of switch deployment, daily maintenance, and fault handling, while reducing labor costs.

After you plug in the switch, the DHCP server automatically provides the switch with an IP address and the address of a provision script that is obtained from AmpCon-Campus server. The switch automatically runs the script to register with the AmpCon-Campus server, install PicOS (for white-box switches only), configure the switch based on system configurations and switch configurations, and install a valid license on the switch.

By using AmpCon-Campus, no experienced network personnel are required at the remote site; anyone who can put the switch in the right place and plug it in will do.

After switches are deployed through ZTP, they can be automatically added to sites and managed by AmpCon-Campus.

In traditional solutions, such tasks are manually performed by network administrators. The AmpCon-Campus ZTP solution, however, frees administrators from these tasks, allowing them to focus on the orchestration of core overlay services.

Full-Stack Network Design

AmpCon-Campus supports two standards-based campus fabric architectures, MLAG fabrics and IP Clos fabrics. These two fabric types cover the networking requirements of small, medium-sized, and large-scale campus fabrics.

By using AmpCon-Campus, 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 automatically pushes networking configurations to switches in batches, eliminating manual CLI work and cutting deployment time from weeks to hours.

AmpCon-Campus provides comprehensive lifecycle management of switches and supports managing and redesigning fabrics to meet changing requirements of campus networks.

Switch Lifecycle Management

AmpCon-Campus simplifies the management of switches, including configuration management, switch inventory, software updates, and more.

AmpCon-Campus includes native configuration management capabilities, which you can use to push an update to a single switch or to an entire group of switches. By using AmpCon-Campus, you don’t need to edit and push switch configurations one by one. In this way, the

likelihood of errors can be reduced, the switch configuration process can be simplified, and you don't need to deal with the added expense or headache of a third-party tool.

In practice, the configuration management feature can greatly simplify the job of updating switches to deal with a new class of devices, such as security devices to protect Internet of Things (IoT) sensors. Your network administrators can detail how the network needs to treat the security devices (such as putting them on your own VLAN), and detail where traffic from devices is allowed to go. By adding only one configuration in the AmpCon-Campus UI, you can push the update to appropriate switches.

AmpCon-Campus greatly simplifies the job of detailing network access level and priority each class of devices need to get and pushing the update to all relevant switches.

Once the desired configurations are set and the network is stable, you might want to make sure that accidental changes don't disrupt operations. When you make a configuration change such as adding devices or a VLAN, it is important to back up your configuration.

AmpCon-Campus makes configuration backup easy by automating and scheduling configuration backup on a specified date and time and saving the last N backups as you need. You can use the backup configuration to recover quickly from a crash or corruption of a switch. In addition, you can mark a specific backup instance as the Golden Config. The Golden Config will never be deleted and is used by default as the configuration to roll back a switch to a stable configuration when the switch operation is compromised. You can also use the Golden Config as the basis to run an automated compliance check to verify whether the network is operating as designed.

AmpCon-Campus also supports switch inventory features. Though third-party tools also support this capability, these tools add expense to your company. In addition, such tools typically run on a Windows Server Enterprise Edition machine, which also adds additional server licensing costs. In contrast, AmpCon-Campus can be deployed in minutes on a virtual machine.

AmpCon-Campus provides detailed inventory of all switches, including switch hardware details, software versions, configurations, and more.

AmpCon-Campus automates the process of checking and updating switch licenses with the latest support entitlements. A License Audit task checks whether a group of specified switches has valid licenses and creates a report of the license status including the support expiration date and other details.

The License Action task automatically updates the license keys on all switches whose support is due to expire in the next 30 days and logs the result to a report, which you can examine or download.

AmpCon-Campus incorporates a unique workflow to enable return merchandise authorization (RMA) replacements. When hardware of a switch fails and is replaced with new switch hardware, the RMA feature takes the configurations from the failed switch hardware, updates the serial number of the new switch, and pushes the configurations to the new switch to bring it up seamlessly in the network.

The nature of PicOS itself makes it simpler to manage switches compared to other legacy network operating system (NOS) of switches or routers. Because PicOS is Linux-based and compartmentalized, you can update or change one component or aspect without affecting other components. For example, if you're pushing a security patch, it affects only the security component of the NOS; you don't need to replace the entire software or firmware image.

- **Role-Based Access Control (RBAC)**
  AmpCon-Campus adopts role-based access control, which is used to permit individual users to perform specific actions and get visibility to an access scope. You can assign each user a specific role with associated permissions.
  In addition, you can authenticate user logins through a TACACS+ server, which also determines their access permissions based on their roles. If the TACACS+ server can't be reached from AmpCon-Campus, you can log in to the AmpCon-Campus UI with local users that are defined in AmpCon-Campus.
- **Parking lot**
  You can use parking lot to manage switches that have been shown in the network and registered with the AmpCon-Campus server but haven't been configured by the administrator.
- **Setting up a group of switches**

  To perform switch lifecycle operations more conveniently, you can organize switches in groups by region, location, building, and more.
- **Importing switches**
  For those switches that were not originally deployed through AmpCon-Campus, you can import them directly to AmpCon-Campus to manage them.
- **Decommission workflow**

  To shut a switch down temporarily and then redeploy it in another location, you can decommission the switch in the AmpCon-Campus UI.

- **Operational logs**

  You can use operational logs to track all activities and troubleshoot issues by drilling down and analyzing issues.

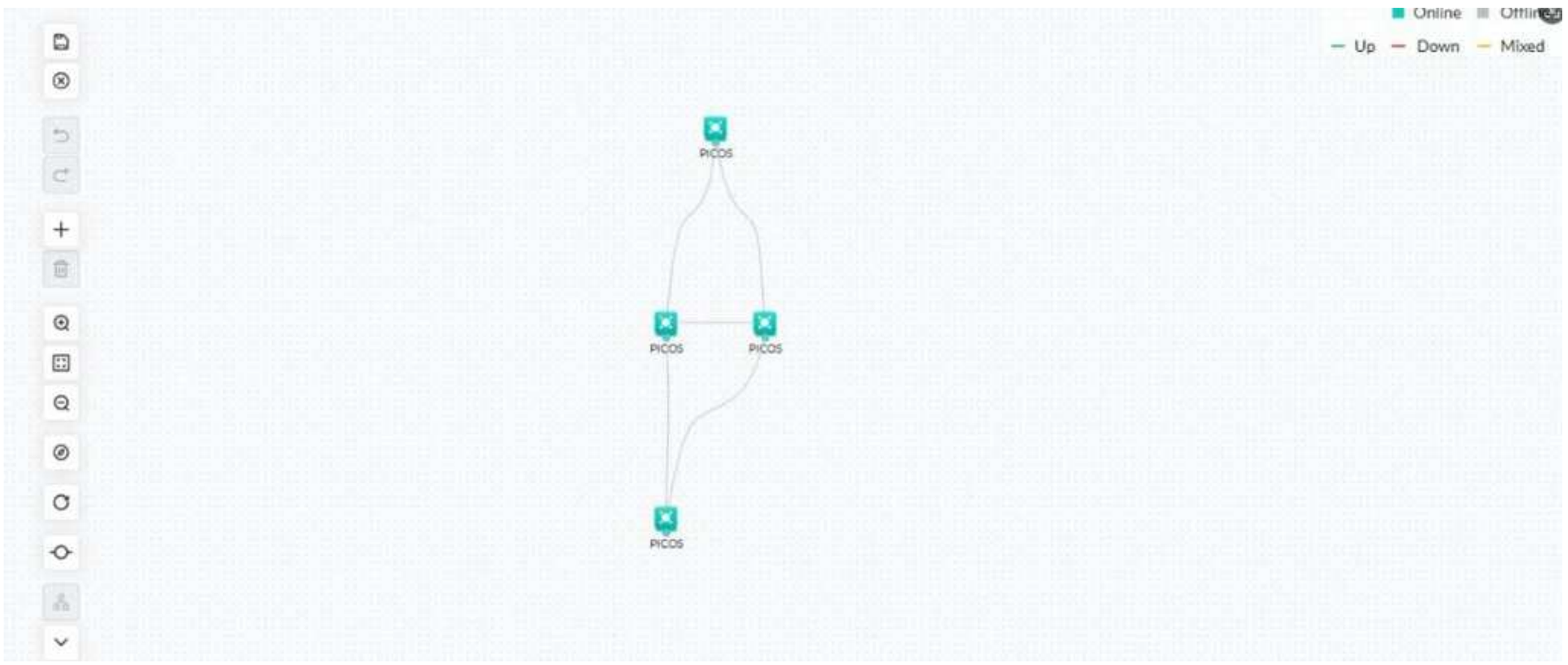
- **Monitoring**

  You can get an overview of all switches or drill down to a switch to check its status and metrics such as port stats.

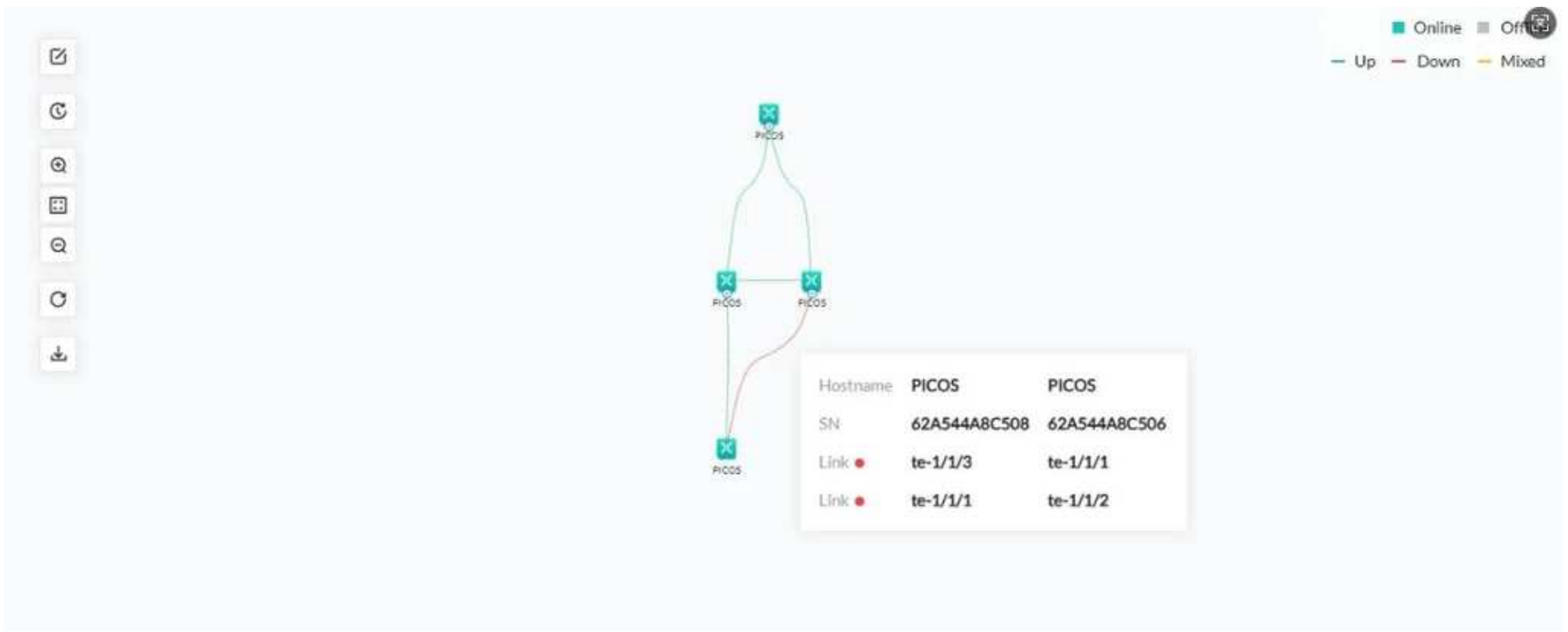
Automatic Discovery of Topology

AmpCon-Campus supports automatic discovery of topology for automated identification and visualization of the network structure. It provides a map view to display all the locations. You can use the map view to pull up any location and drill down into an individual switch, right to the port level, to check port stats and overall health of the switch. In this way, network management and maintenance can be simplified.

AmpCon-Campus supports automatic discovery of neighboring information to generate a topology map after switches are added. You can manually plan the topology and customize the network structure layout according to actual needs.

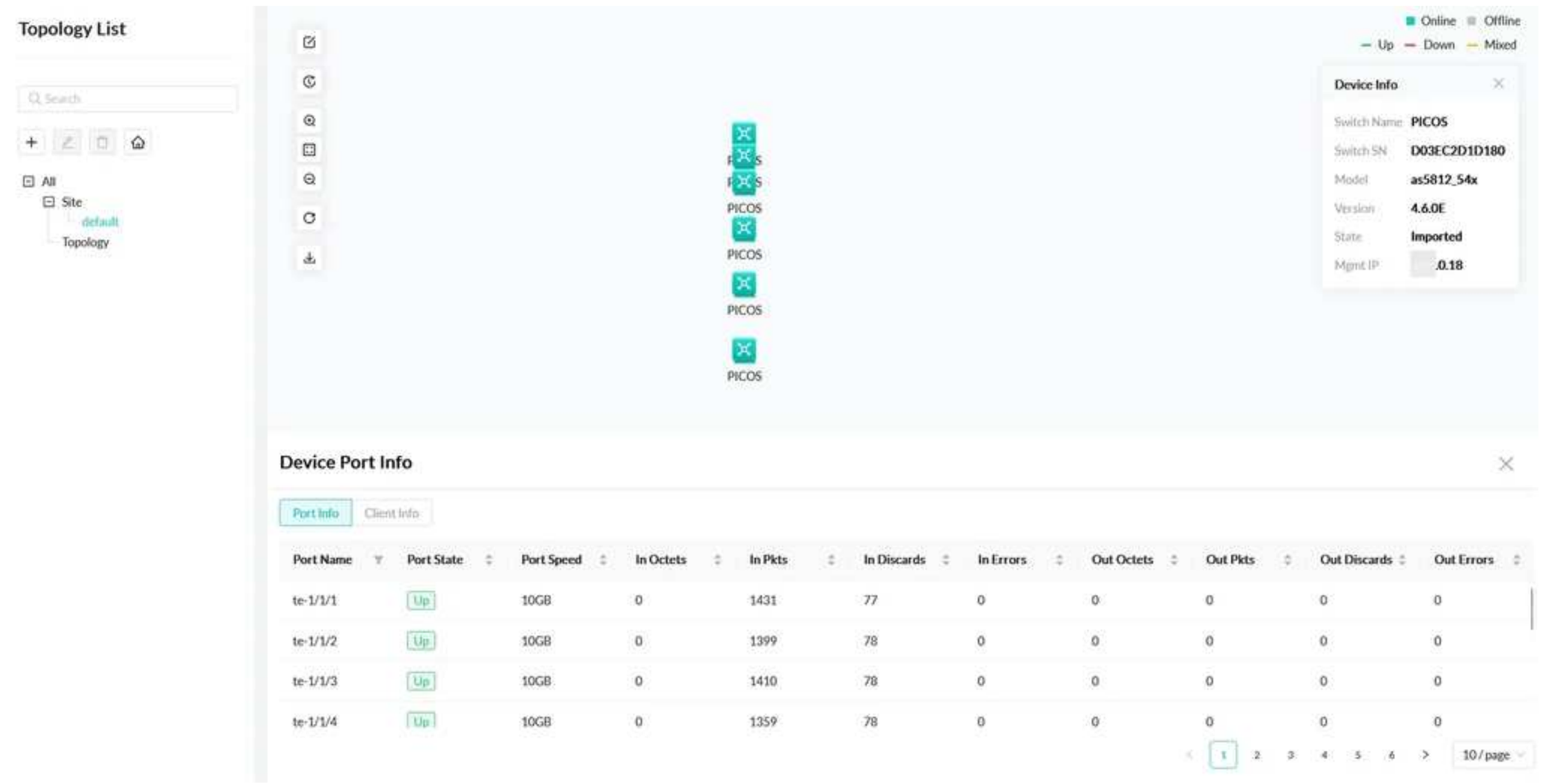


AmpCon-Campus dynamically shows the current network status, which reflects changes such as device online status and link faults in real time. By clicking a device or a link, you can see detailed stats information.



By selecting a timeline, you can see the network topology and device link status at different time. You can analyze the historical topology to trace problems.

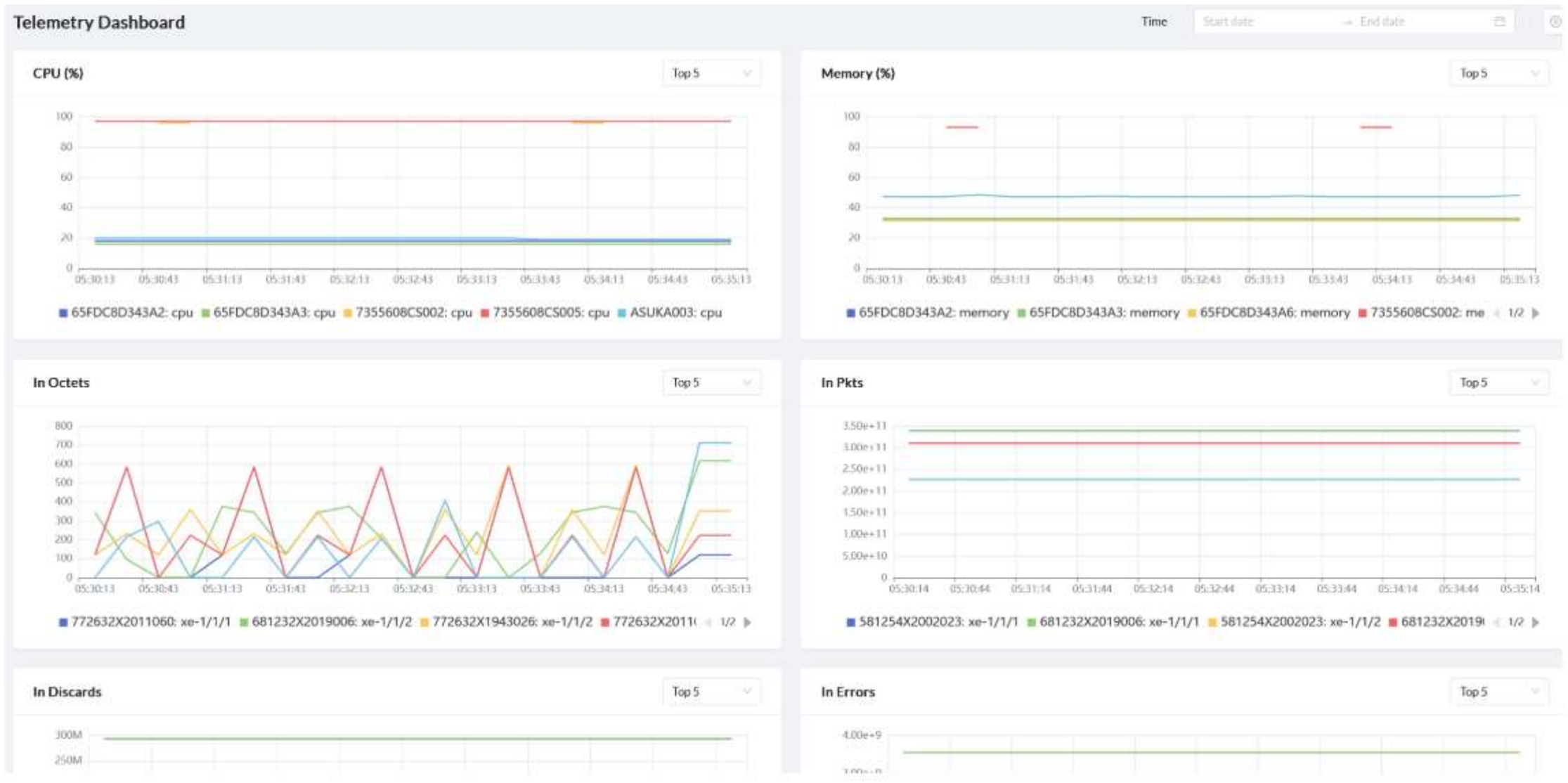
When you click a switch in a topology, you can view real-time or historical information about the switch, switch ports, and terminal devices connected to the switch.



Telemetry Monitoring

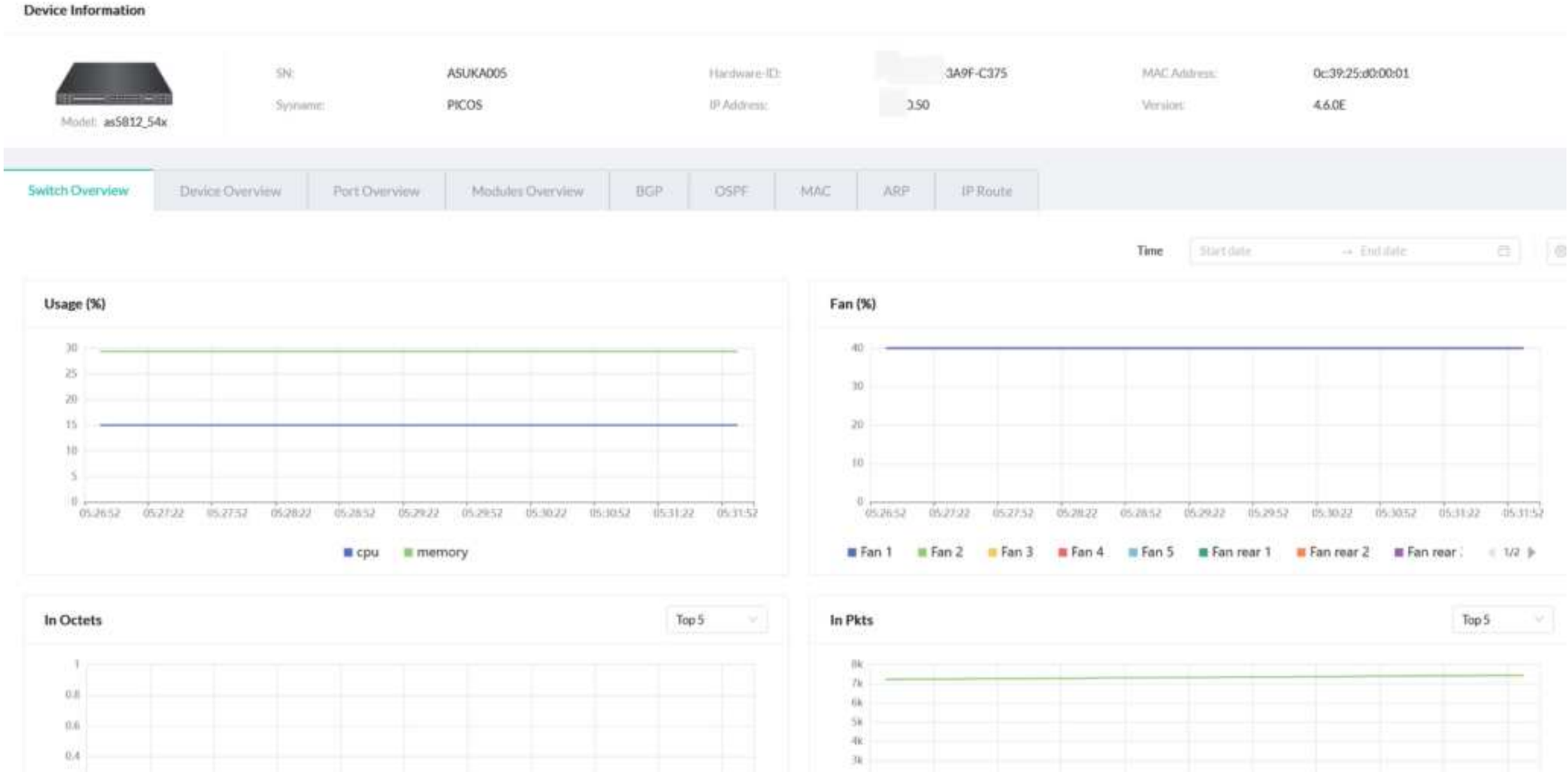
AmpCon-Campus uses the telemetry technology to automatically collect real-time or historical metric data from managed switches. In addition, AmpCon-Campus analyzes the telemetry data to predict equipment failures and performance anomalies and then trigger immediate alarms.

AmpCon-Campus collects real-time data from various network devices, including routing neighbors, switch utilization, and port stats. The data can help network administrators gain insights for quick decisions and network adjustments. You can view the telemetry data of all managed switches on the “Telemetry Dashboard” page.

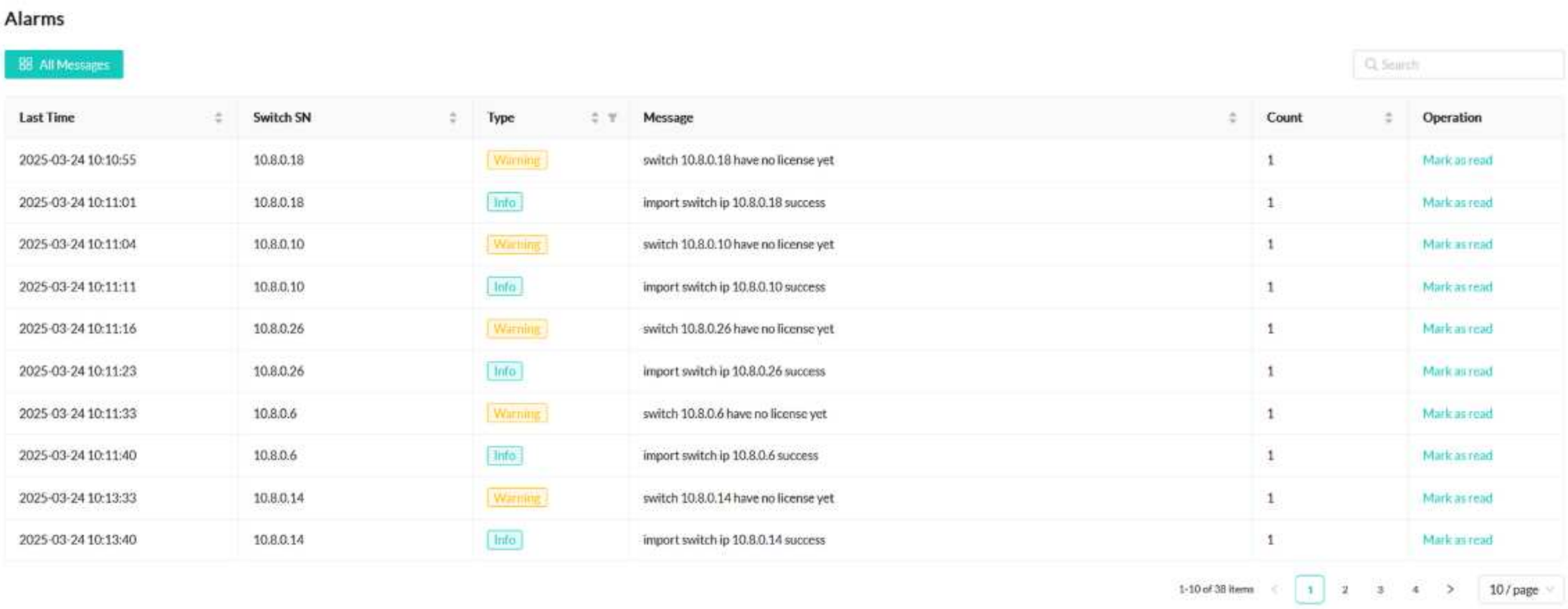


AmpCon-Campus uses telemetry to track performance metrics of each managed switch in real time, such as port traffic, bandwidth utilization, and packet loss rate. With telemetry information, you can identify bottlenecks, optimize configurations, and ensure efficient resource usage on a switch.

You can view the telemetry data of a specific switch on the detail page of the switch.



AmpCon-Campus uses real-time telemetry data to predict equipment failures and performance anomalies, issuing immediate alerts. The operation team can take corrective actions before issues are escalated. The downtime risk can be reduced, and the continuity and reliability of your campus networks can be improved.



If you can't access the AmpCon-Campus UI to view alarms but need immediate alerts when issues arise, use the alarm notification feature to receive real-time email notifications. In this way, you can promptly find problems and prevent incident escalation.

Flexible Ansible Extensions

Ansible is an open-source tool to automate configuration management, application deployment, and task automation. Ansible uses simple, declarative language written in YAML, which is called playbooks, to automate your tasks. You declare the desired state of a local or remote system in your playbook. Ansible ensures that the system remains in that state. For more information about Ansible, see Getting started with Ansible and Using Ansible playbooks.

AmpCon-Campus integrates with Ansible to automate and simplify network management, such as configuring interfaces, VLANs, and security settings.

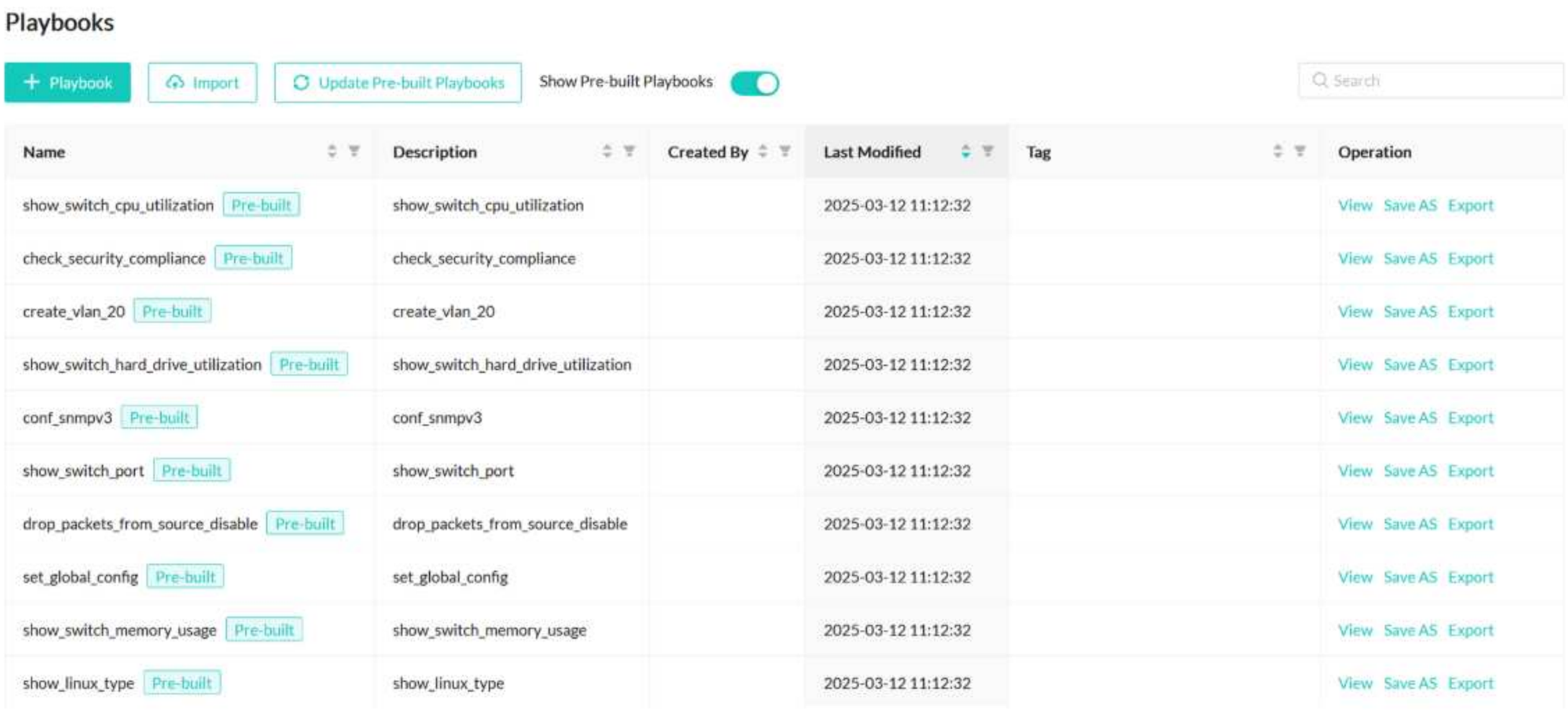
By using Ansible to automate network management, you can reduce errors, save time, and ensure consistency across your network. Then, you can focus on more strategic tasks.

AmpCon-Campus provides commonly used features that your network teams need for day-to-day operations. You can also use AmpCon-Campus to add capabilities that you might require by writing Ansible playbooks.

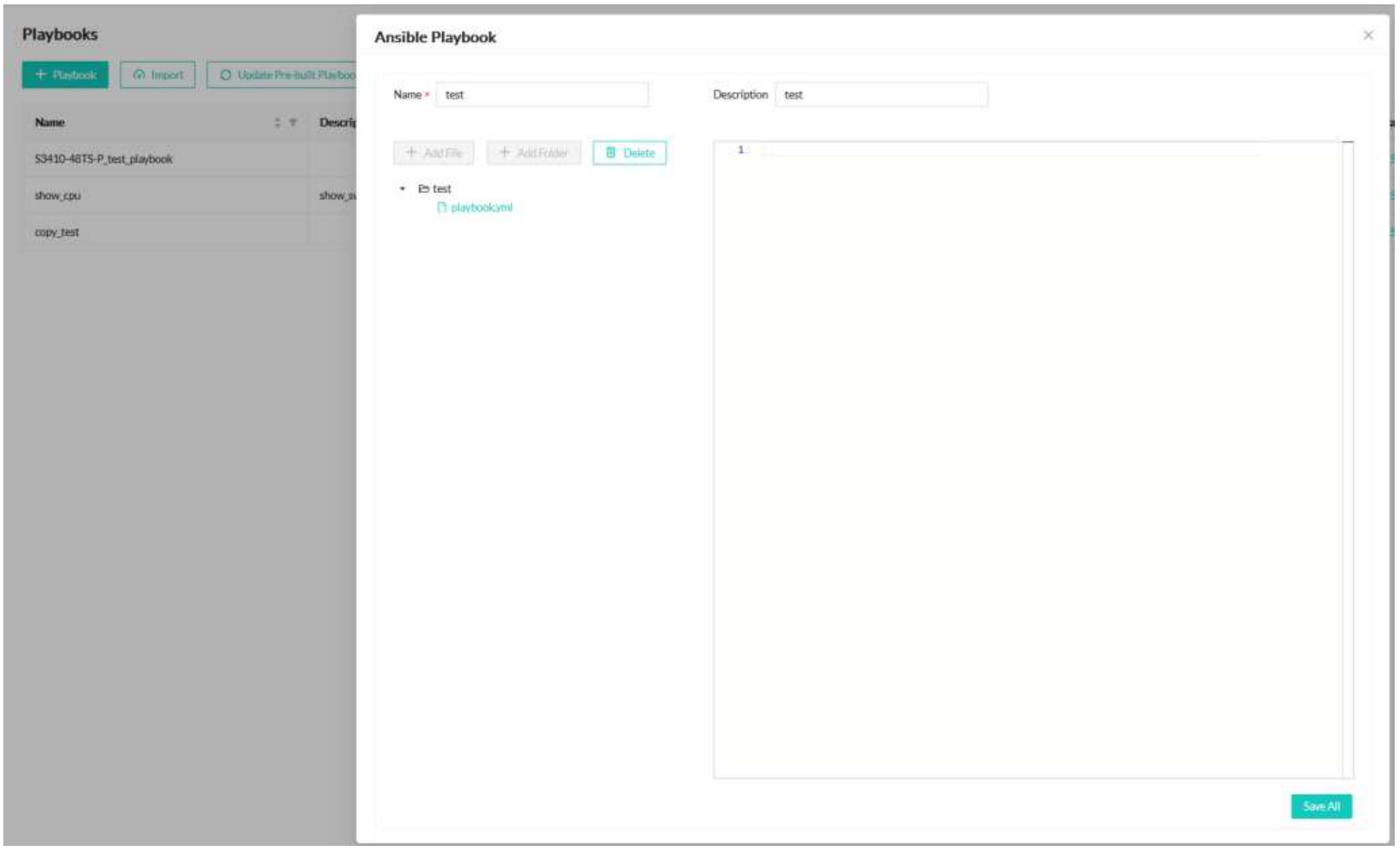
If a network management task follows a certain routine regularly, build an Ansible playbook to automate the task.

AmpCon-Campus offers a series of Ansible playbooks, which are templates for automating the following routines:

- Compliance and consistency checks, to ensure switches stay in compliance with industry regulations that require a certain configuration to maintain proper security and privacy
- Connectivity checks for PicOS Software Switches
- Network operation and remediation routines such as dynamic policy enforcement

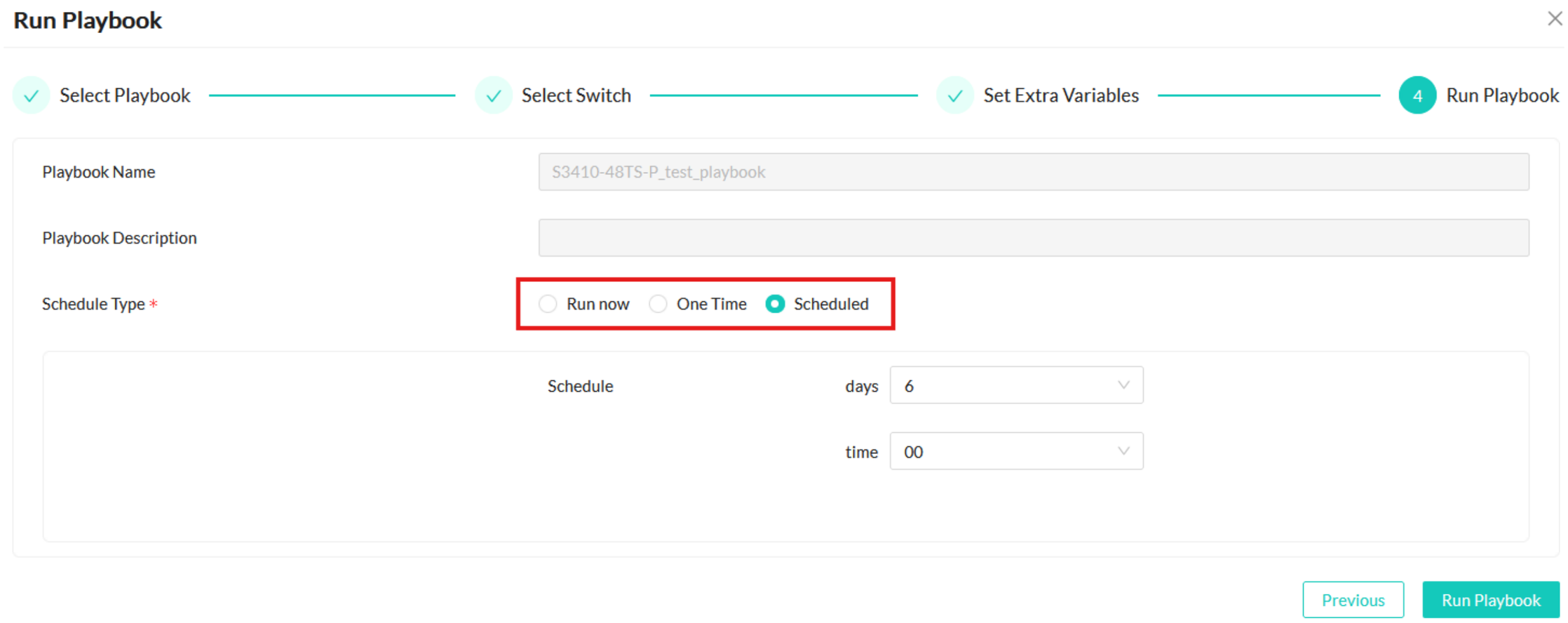


If the pre-built Ansible playbooks can't meet your needs, you can customize an automation workflow by writing a playbook on AmpCon-Campus or importing a local playbook to AmpCon-Campus.



AmpCon-Campus supports the following schedule types of playbook run:

- **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



An Ansible job is a single execution of an Ansible playbook. AmpCon-Campus displays the list of Ansible jobs, the list of switches with Ansible jobs, the execution results, and the output of these jobs.

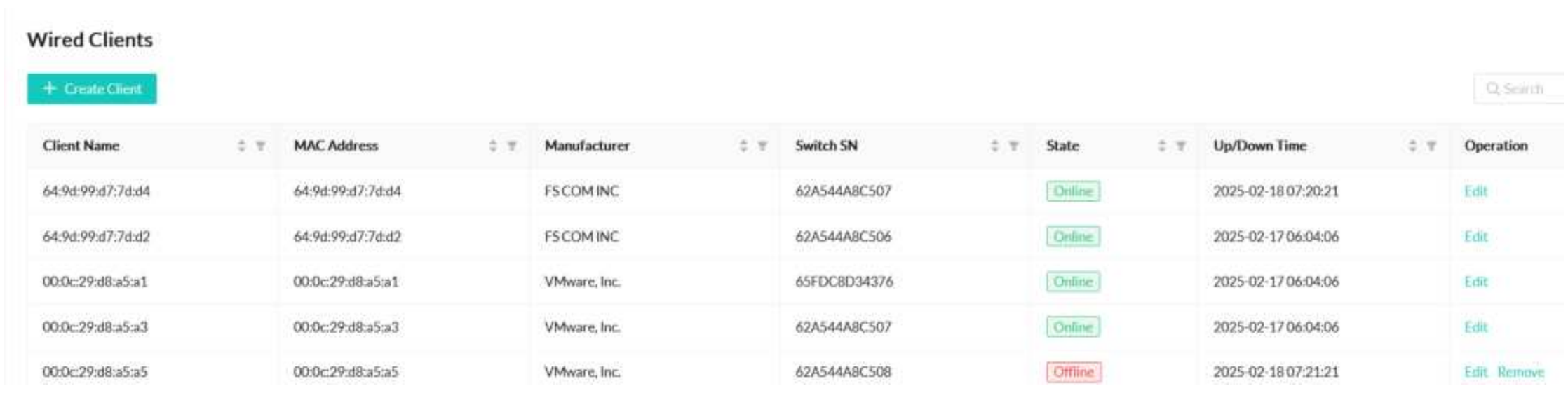
In addition to running Ansible playbooks on managed switches, AmpCon-Campus supports running Ansible playbooks on the Linux servers that you added.

Terminal Device Management

In the AmpCon-Campus UI, you can easily monitor third-party devices and track their status. By using this feature, you can view terminal devices connecting to each managed switch in your network and thus facilitate refined management of terminal devices.

AmpCon-Campus supports automatically identifying terminal devices. But if a terminal device is removed or always offline, you might not see the terminal device in the AmpCon-Campus UI. To monitor the status of the terminal device, you can manually add it to AmpCon-Campus.

When you click a switch in a topology, you can see the real-time or historical information about the terminal devices connected to this switch in the topology.



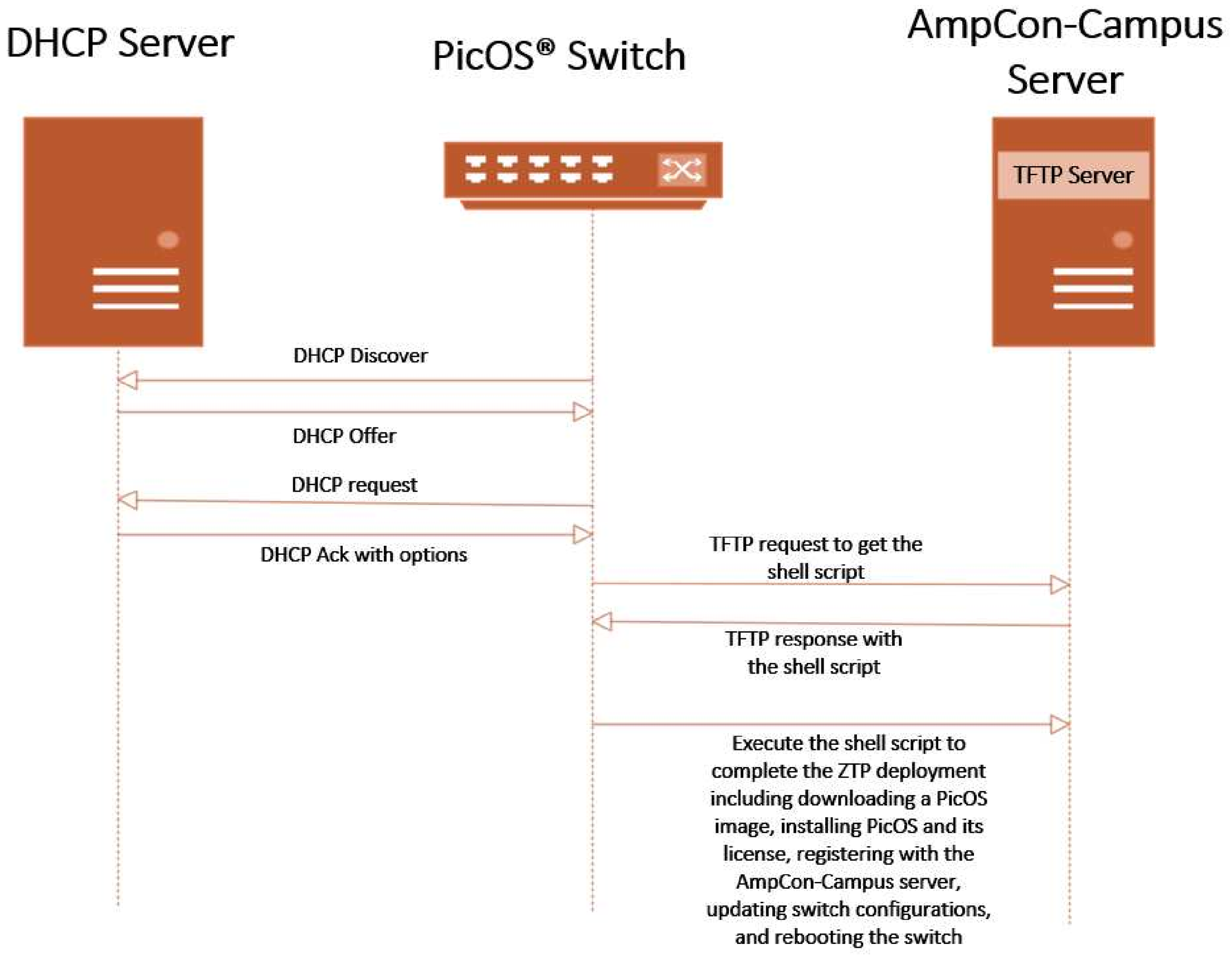
Architecture

AmpCon-Campus is built on Ubuntu Linux and incorporates a web GUI and a MySQL database with Python codes built on top of an Ansible

engine. Switches and AmpCon-Campus communicate with the SSH protocol. AmpCon-Campus gets switch stats through gNMI.

Zero Touch Provisioning (ZTP) Workflow

Figure 1. ZTP Workflow of White-Box Switches



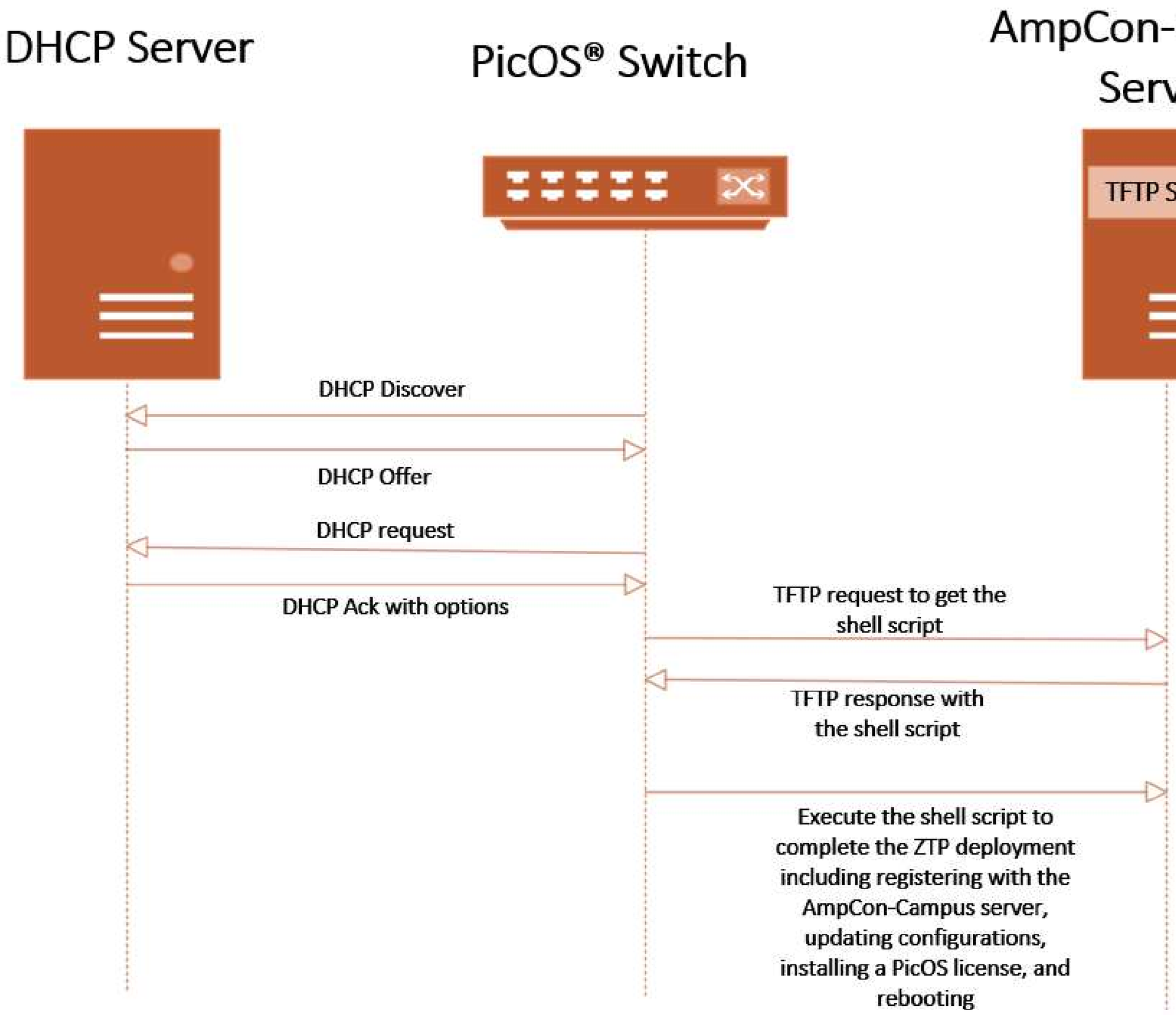
After a switch is powered on, the switch sends DHCP Discover to get an IP address, and the DHCP server provides the switch with an IP address.

The switch sends a request to the DHCP server, and the DHCP server sends a response including the HTTP server address.

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.

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.

Figure 2. ZTP Workflow of Integrated Hardware and Software Switches



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.

The switch sends a DHCP request to the DHCP server, and the DHCP server sends a DHCP response including the TFTP server address.

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.

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.

Switch Configuration Workflow

The AmpCon-Campus server includes a component called Configuration Manager, which is used to create a standard configuration to configure switches. All configurations are tied to specific switches by the switch serial number (or Service Tag) and are stored in the AmpCon-Campus database.

After you use the AmpCon-Campus UI to push configurations to switches, each switch then downloads its appropriate configurations. At the same time, the switch accesses another AmpCon-Campus server component, License Manager, which accesses the customer's account on the License Portal to generate a license key and install the license on the switch.

The switch runs a shell script to automatically apply and validate the new configurations, update its status in the AmpCon-Campus database, and join the network. From your perspective, all these switch configurations happen with the touch of a button in the AmpCon-Campus UI. You can use the AmpCon-Campus UI to deploy dozens or hundreds of switches to far-flung sites while your network team stays at home and monitors the process centrally.

Getting Started

Welcome to the AmpCon-Campus management platform. AmpCon-Campus helps you deploy and manage your network more efficiently and gives you deep visibility into your network.

Read “how to” guides to learn how to use AmpCon-Campus with your network landscape, and then start your AmpCon-Campus tour based on the quick start flow.

Managing Switch Lifecycle

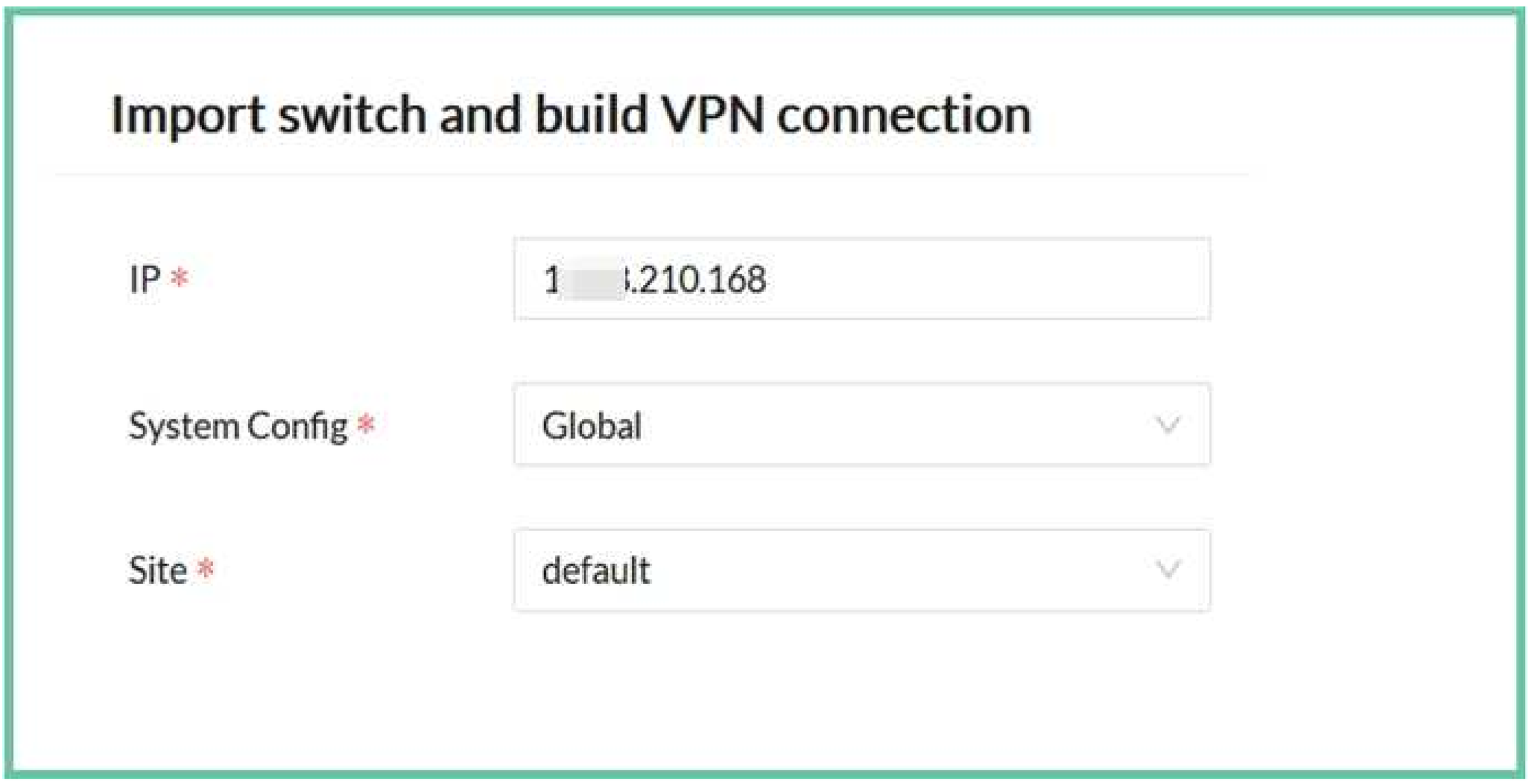
Deploy, configure, and manage switches in one click with AmpCon-Campus.

- Step 1: Importing or Deploying Switches
- Step 2: Configuring Switches
- Step 3: Managing Switch Lifecycle

Step 1: Importing or Deploying Switches

To manage switches with AmpCon-Campus, you need to deploy switches or import switches first.

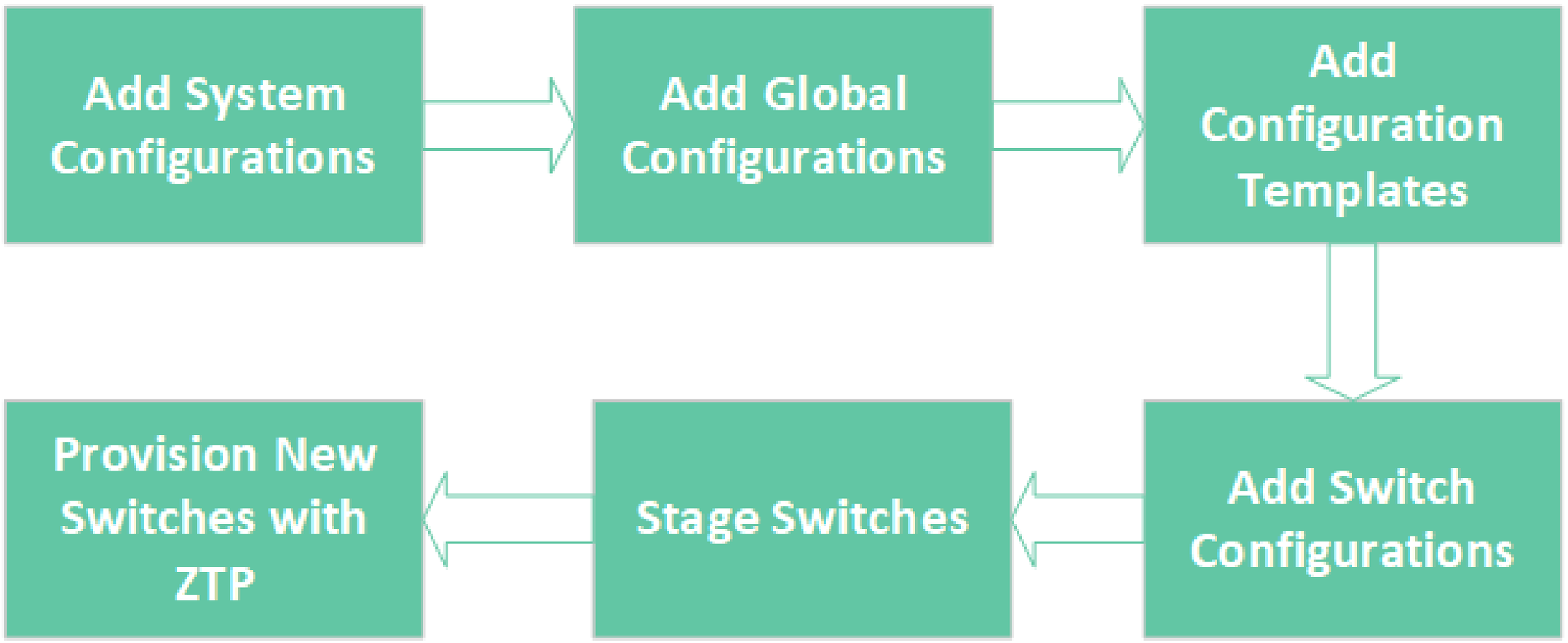
- For switches that are deployed but not deployed with AmpCon-Campus, you need to import these switches to AmpCon-Campus via IP Discovery. The importing process can be easily done through the AmpCon-Campus UI.



After you import switches, you can use AmpCon-Campus to configure and monitor these switches and manage the lifecycle of these switches.

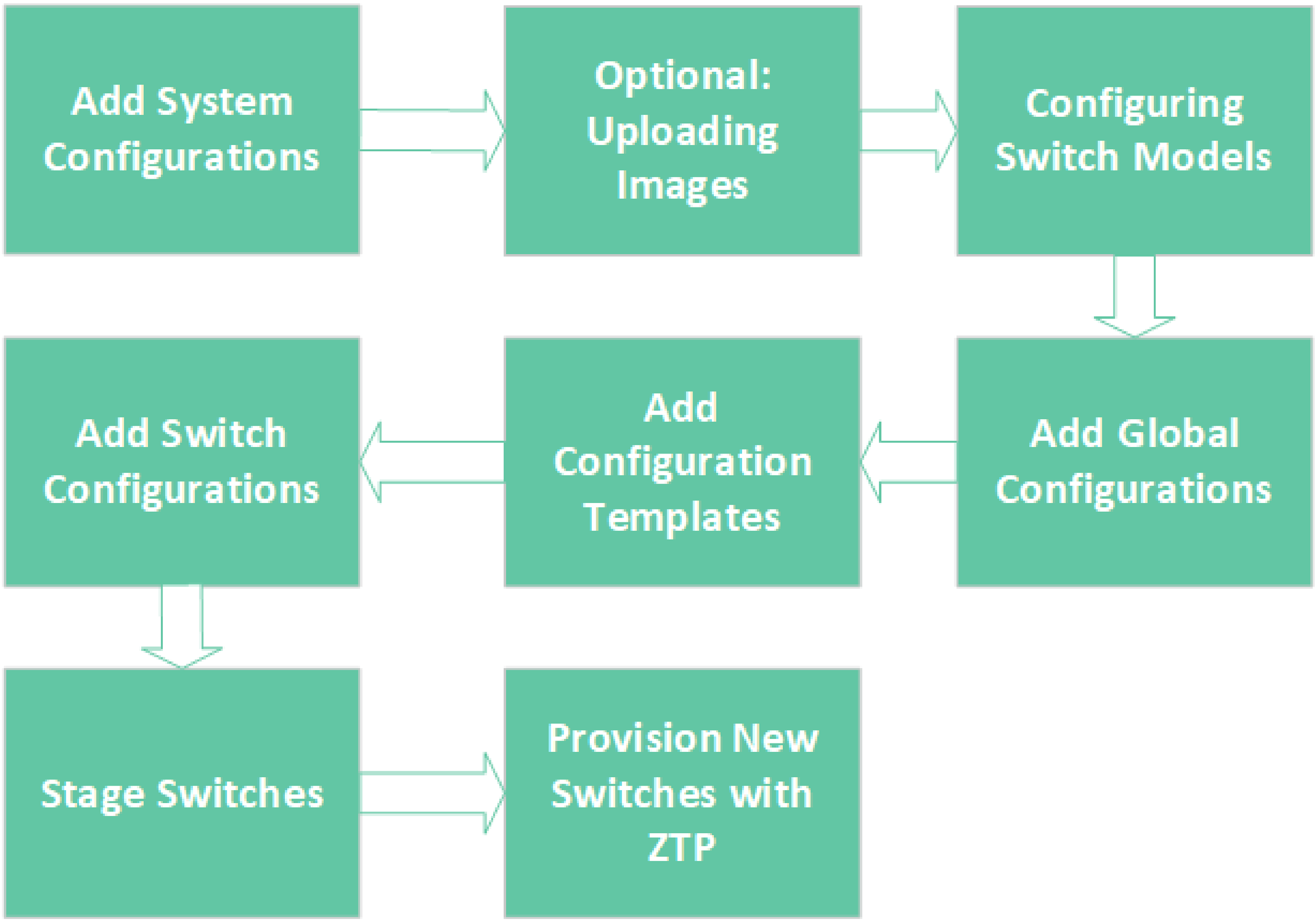
- For switches that are not deployed, you can deploy these switches with AmpCon-Campus via Zero Touch Provisioning (ZTP). AmpCon-Campus simplifies the switch deployment process.

For **white-box switches**, the deployment procedure is as follows:



Learn more about detailed deployment steps here.

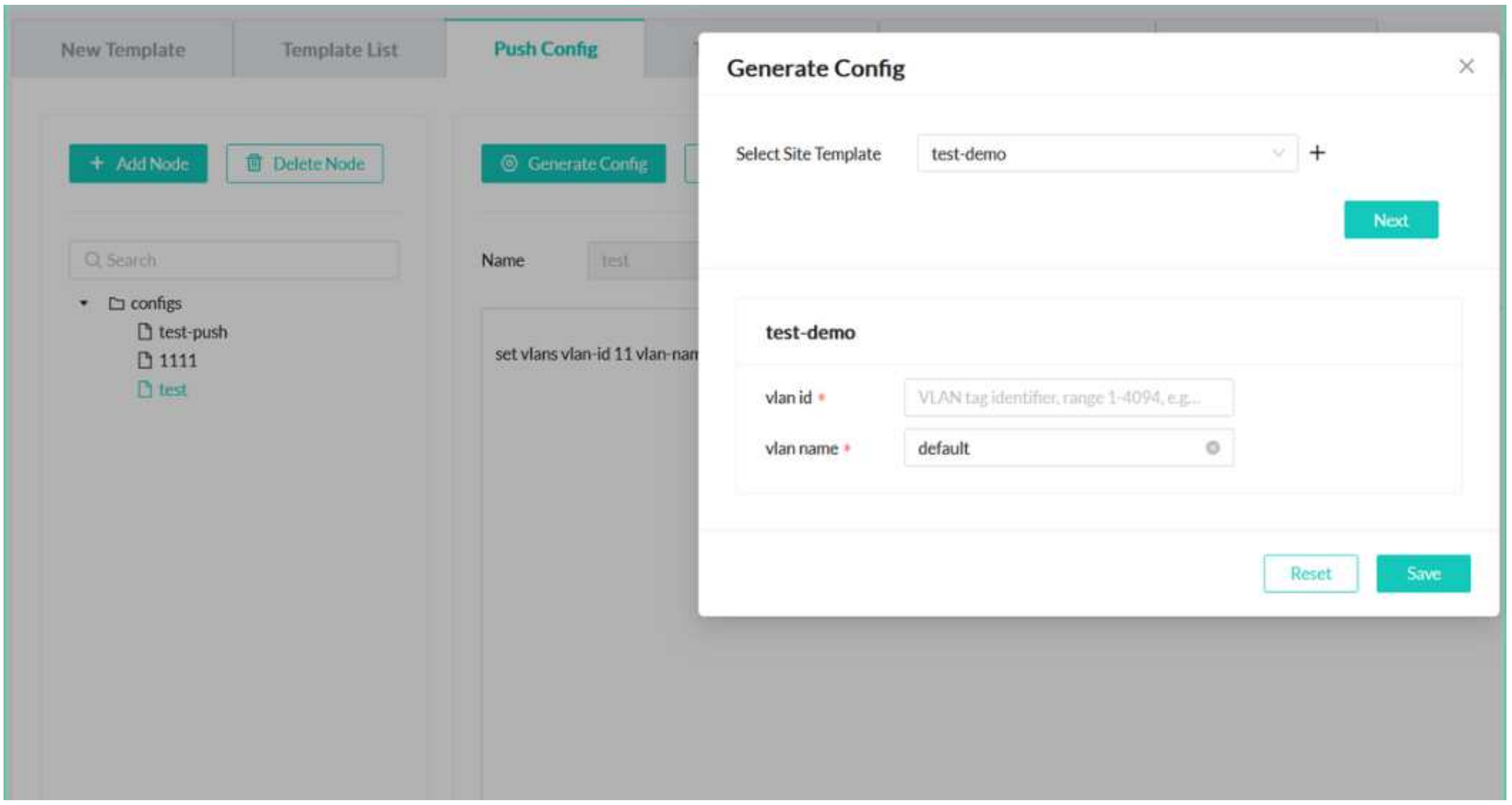
For integrated hardware and software switches, the deployment procedure is as follows:



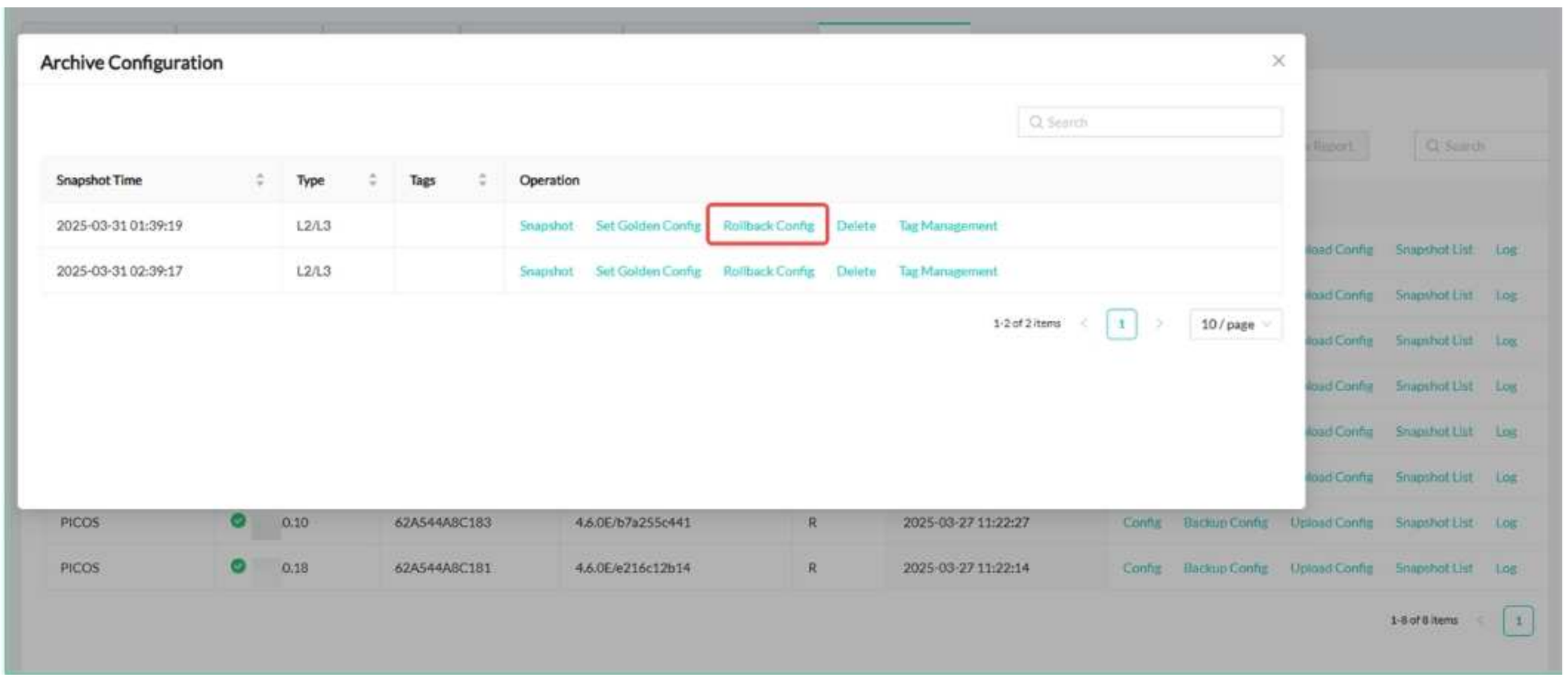
Learn more about detailed deployment steps here.

Step 2: Configuring Switches

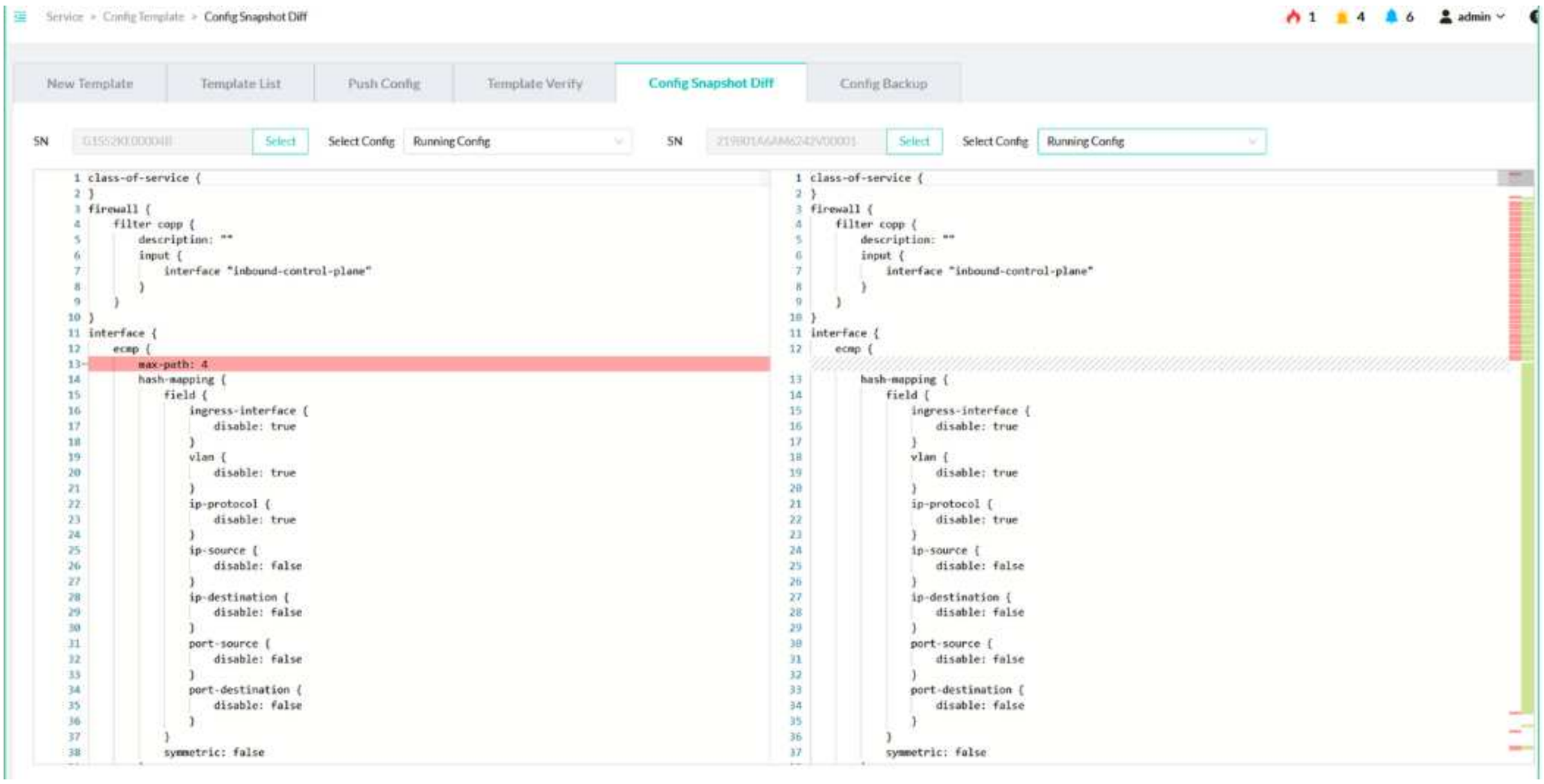
- AmpCon-Campus includes native switch configuration management capabilities, which you can use to push configurations to a single or multiple switches.



- After the desired configurations are pushed to switches and the network is stable, you might want to make sure that accidental changes don't disrupt operations. You can back up and restore configurations for disaster recovery.

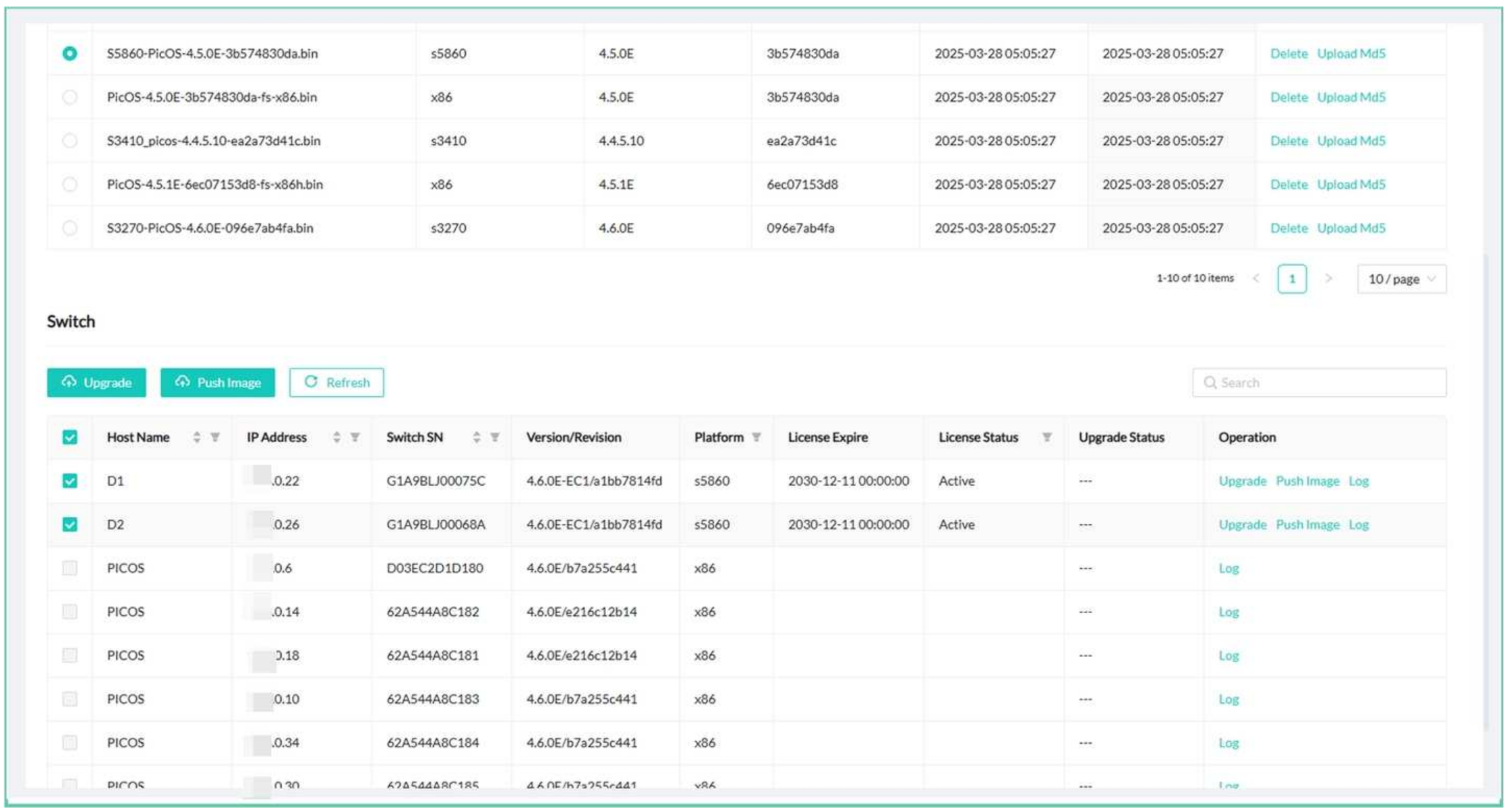


- You can compare configurations for troubleshooting or auditing.
  - Compare running configurations with initial configurations on the same switch
  - Compare running configurations or backup configurations on one switch or on different switches



Step 3: Managing Switch Lifecycle

- By using AmpCon-Campus, you can upgrade PicOS on a single switch or on multiple switches at scale.



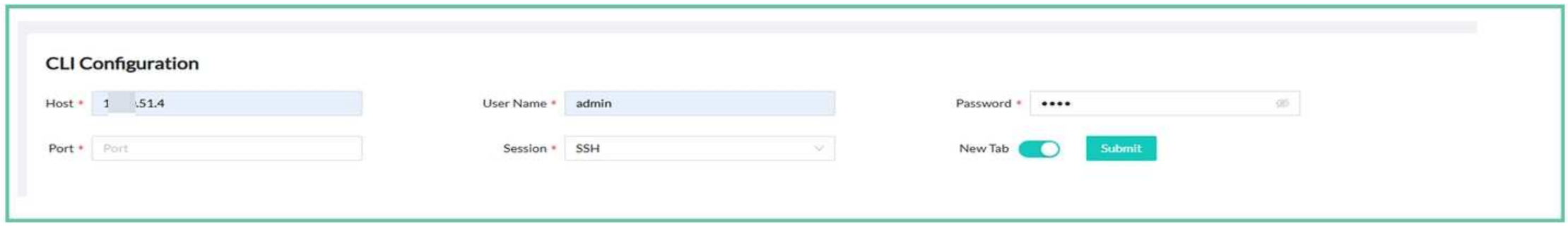
- AmpCon-Campus supports Returning Merchandise Authorization (RMA), which means replacing a switch with another switch of the same switch model.

  When the hardware of a switch fails and is replaced with a new switch, you can RMA to 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.

- You can decommission (DECOM) a deployed switch to revoke the PicOS license and configurations from the switch. The decommissioned switch will not be managed by AmpCon-Campus.
- 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.

- You can connect to a switch from the AmpCon-Campus UI by creating an SSH session.



Viewing Network Landscape

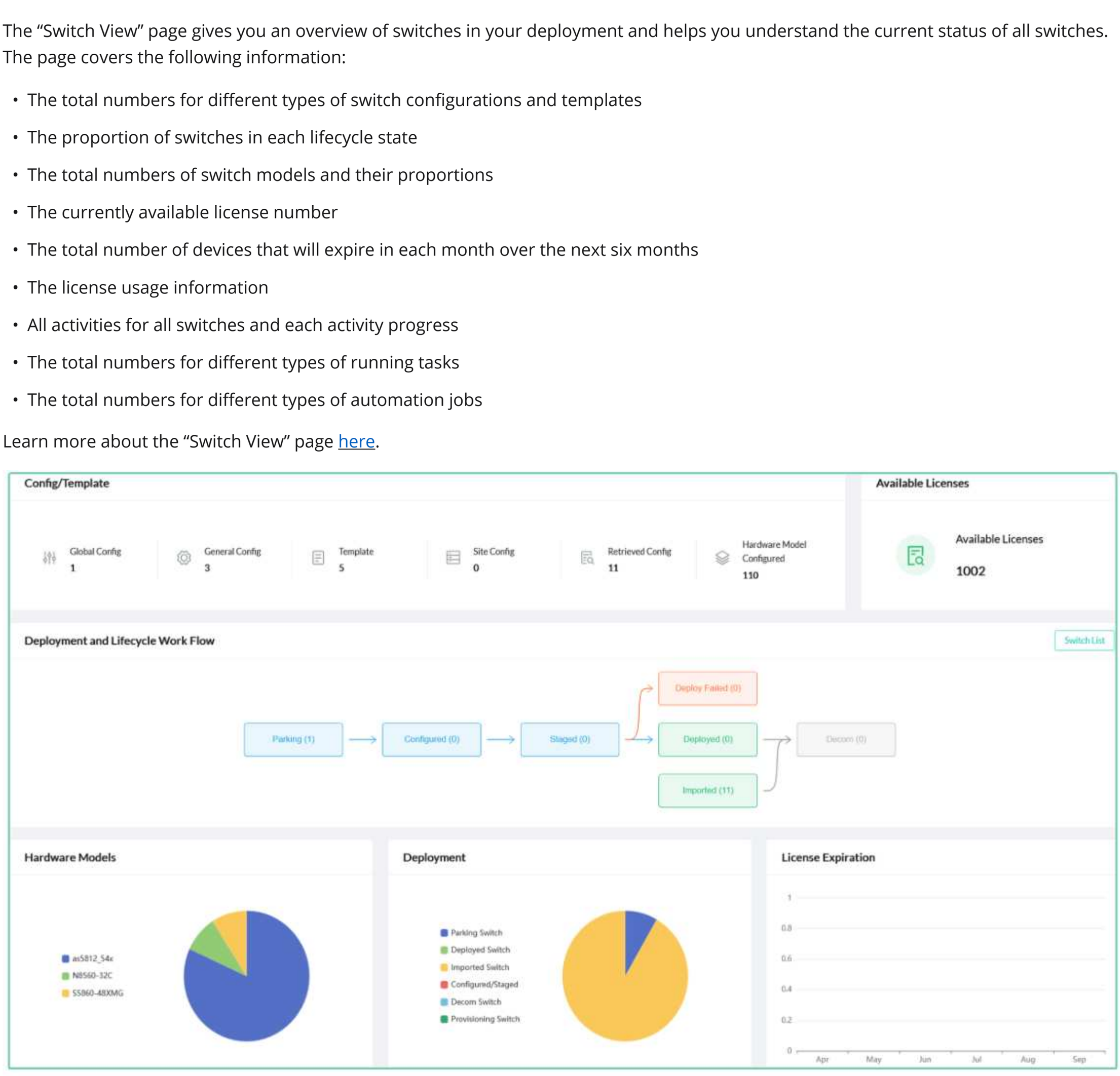
Explore powerful dashboards in AmpCon-Campus to have deep visibility into your network and devices.

Switch View Page: Getting an Overview of All Switches

The “Switch View” page gives you an overview of switches in your deployment and helps you understand the current status of all switches. The page covers the following information:

- The total numbers for different types of switch configurations and templates
- The proportion of switches in each lifecycle state
- The total numbers of switch models and their proportions
- The currently available license number
- The total number of devices that will expire in each month over the next six months
- The license usage information
- All activities for all switches and each activity progress
- The total numbers for different types of running tasks
- The total numbers for different types of automation jobs

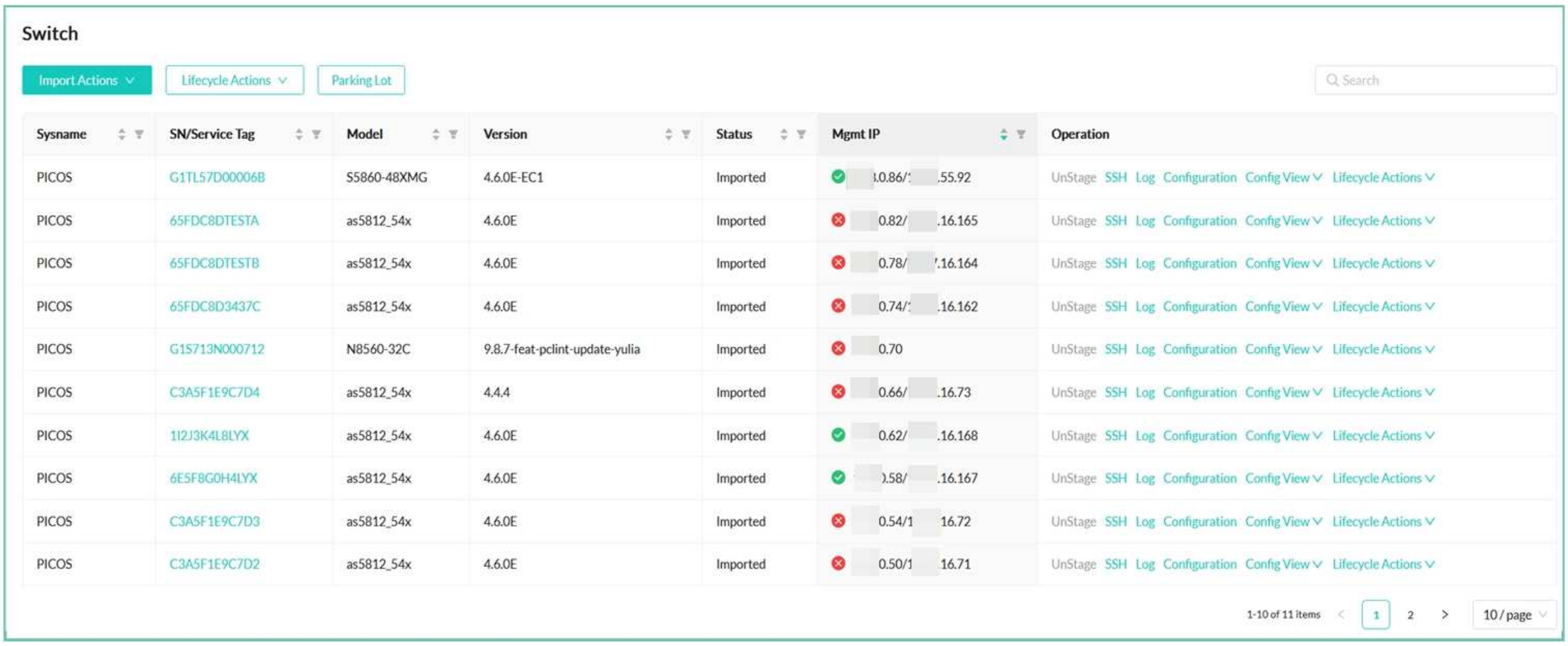
Learn more about the “Switch View” page here.



Switch Page: Diving Deep into Each Switch

The “Switch” page lets you view all managed switches at a glance and monitors each switch by analyzing detailed telemetry metrics.

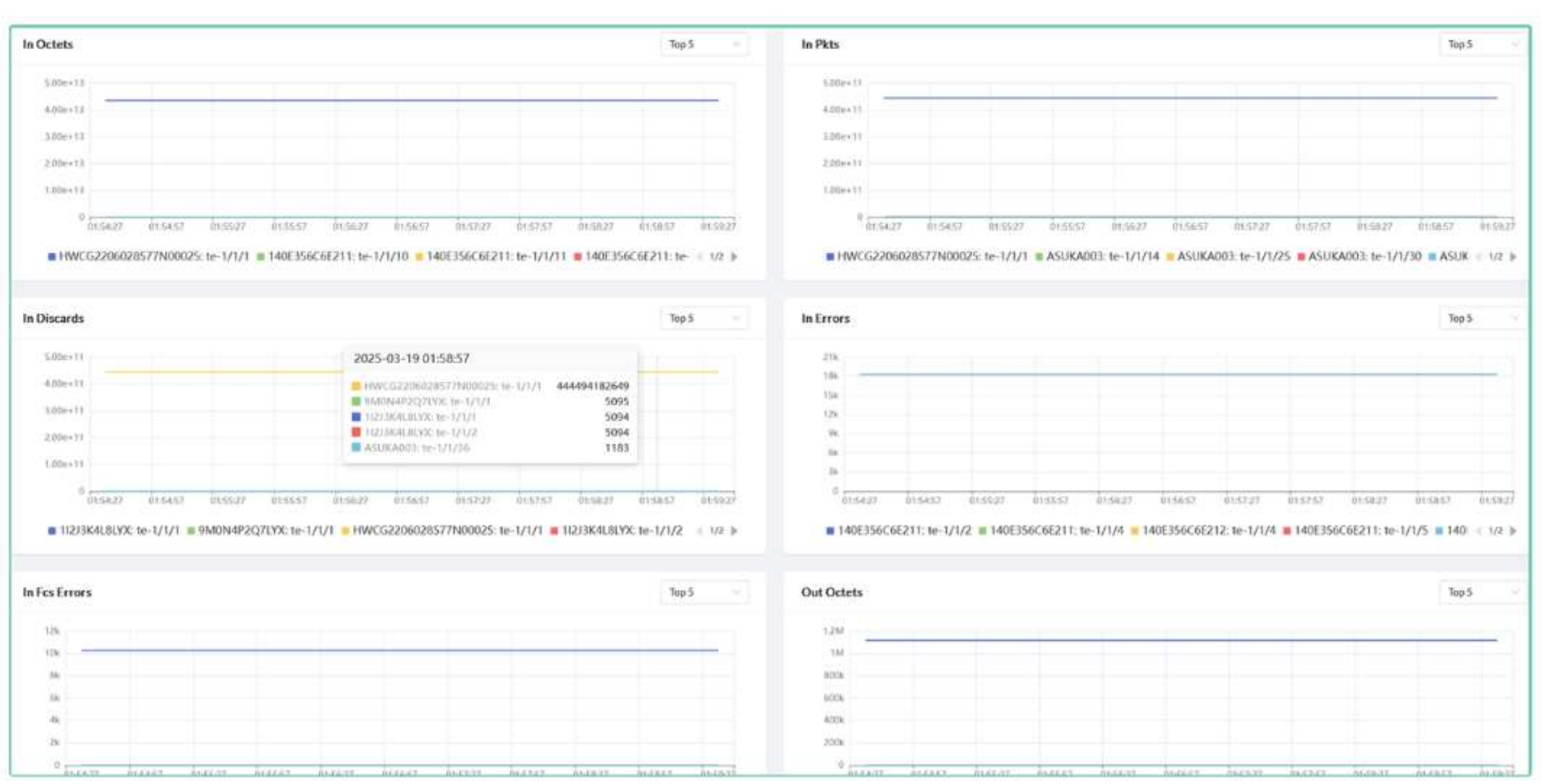
Learn more about the “Switch” page here.



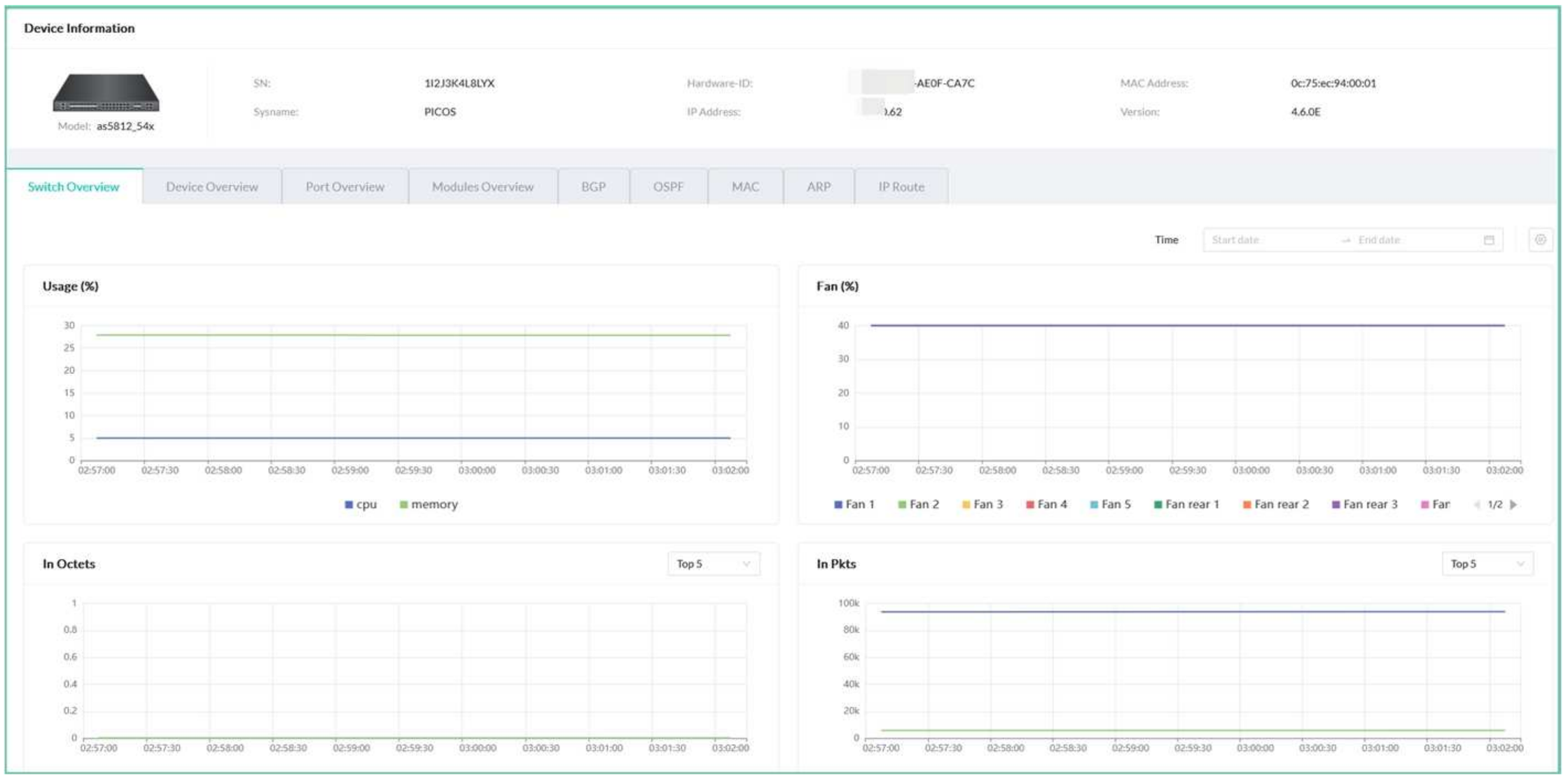
Telemetry Pages: Monitoring Switch Metrics

To ensure the network is healthy and switches are working well, AmpCon-Campus uses the telemetry technology to automatically collect real-time and historical metric data from managed switches.

- You can view telemetry data of all managed switches in the “Telemetry Dashboard” page.
  Learn more about the “Telemetry Dashboard” page here.



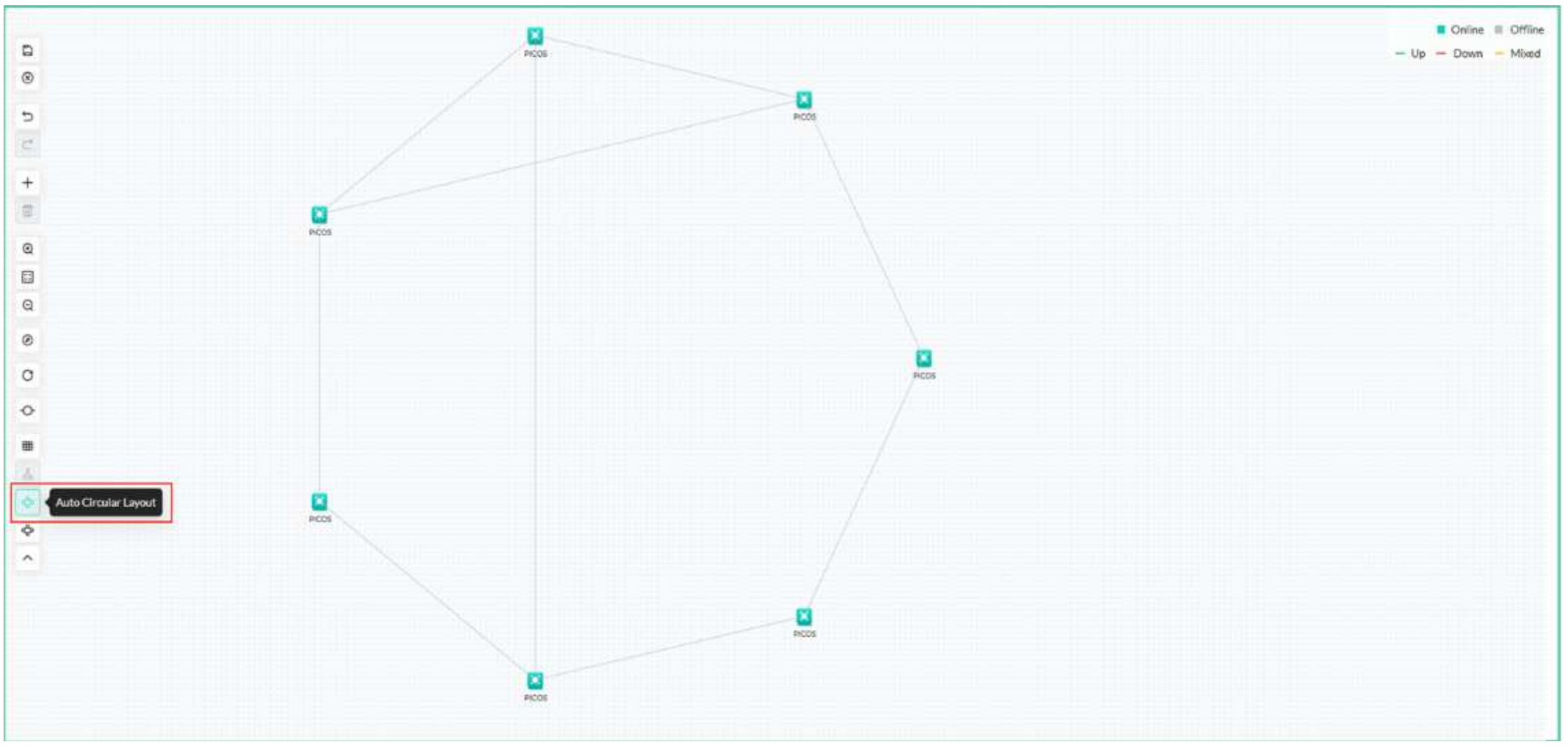
- You can view the telemetry data of a specific switch on the switch detail page to gain detailed insights into the switch.
  Learn more about the telemetry data on the switch detail page here.



Topology Page: Visualizing Your Network Structure

The “Topology” page provides a map view to display switches and their connectivity status. You can drill down into an individual switch, right to the port level, to check port stats and overall health of the switch.

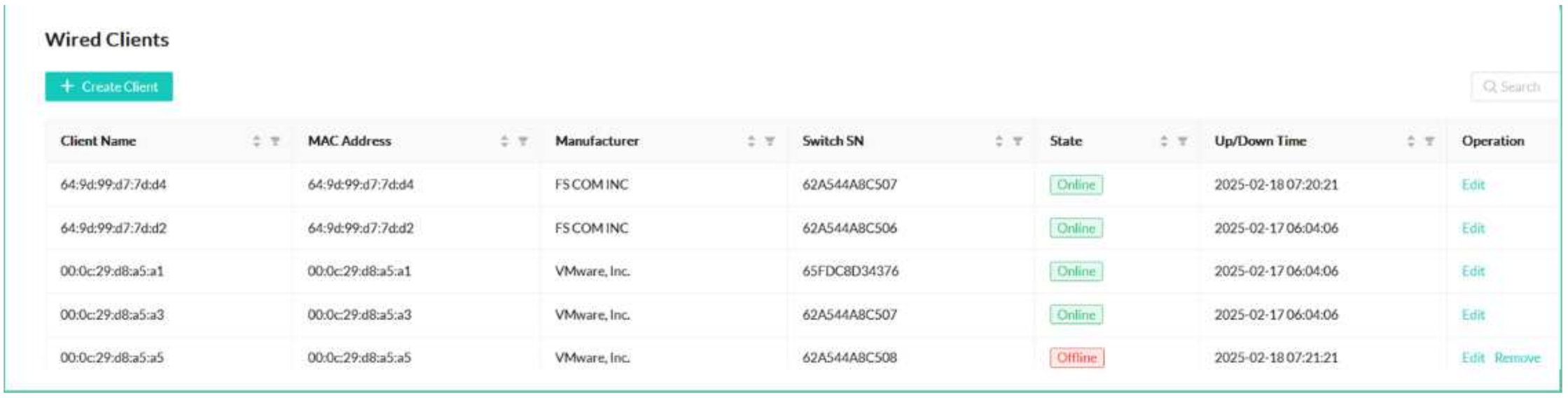
Learn more about the “Topology” page here.



Wired Clients Page: Identifying Terminal Devices

The “Wired Clients” page displays terminal devices connected to each managed switch. AmpCon-Campus supports automatically identifying terminal devices and manually adding terminal devices.

Learn more about the “Wired Clients” page here.



Designing a Campus Fabric

Design your campus fabric with AmpCon-Campus to eliminate complex networking configurations.

- Step 1: Preparing Supported Switches
- Step 2: Choosing Campus Fabric Types
- Step 3: Designing a Campus Fabric
- Step 4: Verifying the Fabric Deployment

Step 1: Preparing Supported Switches

Check the supported switches for fabric design.

Import or deploy switches used for the fabric design.

Add a site used for the fabric design. If you don't create a site, you can use the built-in site **default**.

Add switches to the site. These added switches will be used for the fabric design.

Ensure that all switches used for the fabric design are up and connected to AmpCon-Campus. You can verify by clicking **Service > Switch** from the navigation bar and checking the **Mgmt IP** column.

✓: The switch is up and connected to AmpCon-Campus.

x: The switch is down or not connected to AmpCon-Campus.

Ensure that all switches used for the fabric design retain only basic routing configurations, without any other service configurations.

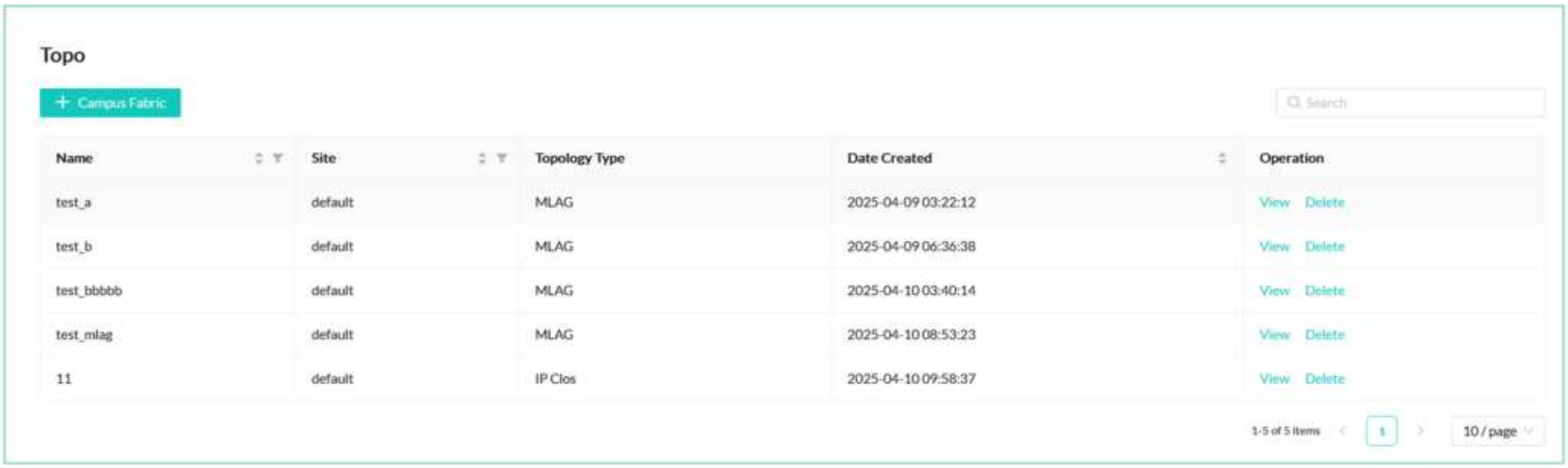
Step 2: Choosing Campus Fabric Types

AmpCon-Campus supports two standard-based campus fabric architectures, MLAG fabrics and IP Clos fabrics. These two fabric types cover the networking requirements of small, medium-sized, and large-scale campus fabrics.

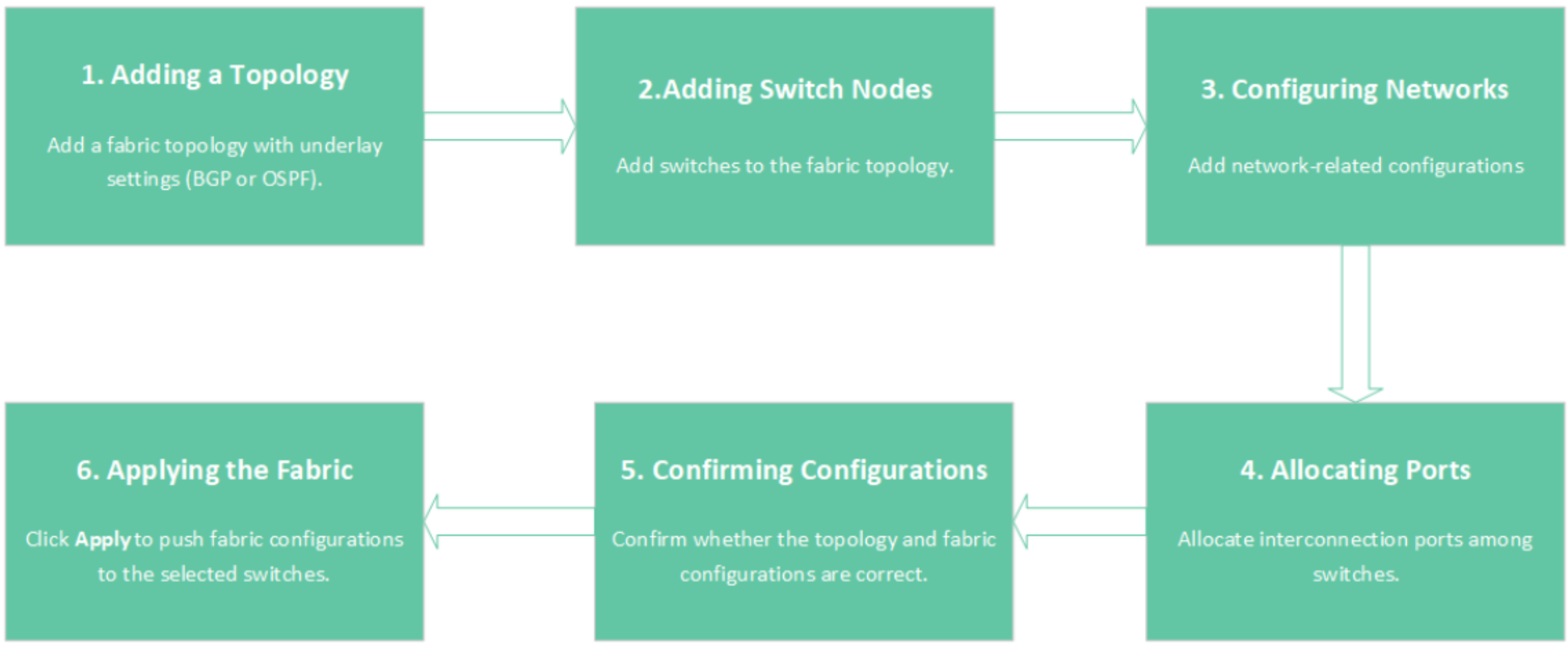
- The MLAG fabric architecture is applicable to small or mid-size campus networking.
  This architecture simplifies the network topology, reduces latency, and lowers costs by eliminating the need for separate core and distribution devices.
- The 5-stage IP Clos fabric architecture is applicable to large-scale campus networking.
  This architecture provides a scalable and flexible solution for interconnecting multiple switches in a hierarchical manner, allowing efficient utilization of network resources and simplified routing.

Step 3: Designing a Campus Fabric

Click **Topo > Campus Fabric** from the navigation bar. On the "Topo" page, click **+ Campus Fabric**.



Start to design a campus fabric by using AmpCon-Campus. The MLAG fabric design procedure and IP Clos fabric design procedure are similar. See the following diagram:



Learn more about the MLAG fabric design procedure here.

Learn more about the IP Clos fabric design procedure here.

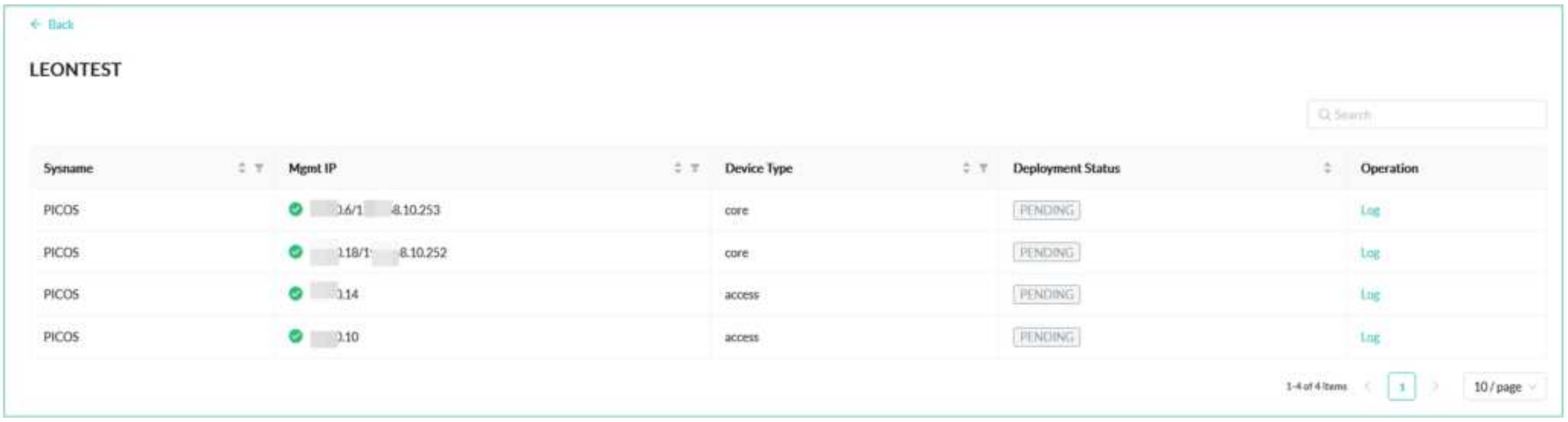
Step 4: Verifying the Fabric Deployment

On the “Topo” 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 **SUCCEED**.

- 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.



Alerting for Predictive Maintenance

Check for alarms to find issues, and enable email notifications to get informed and take actions when something unusual happens.

Checking Alarms

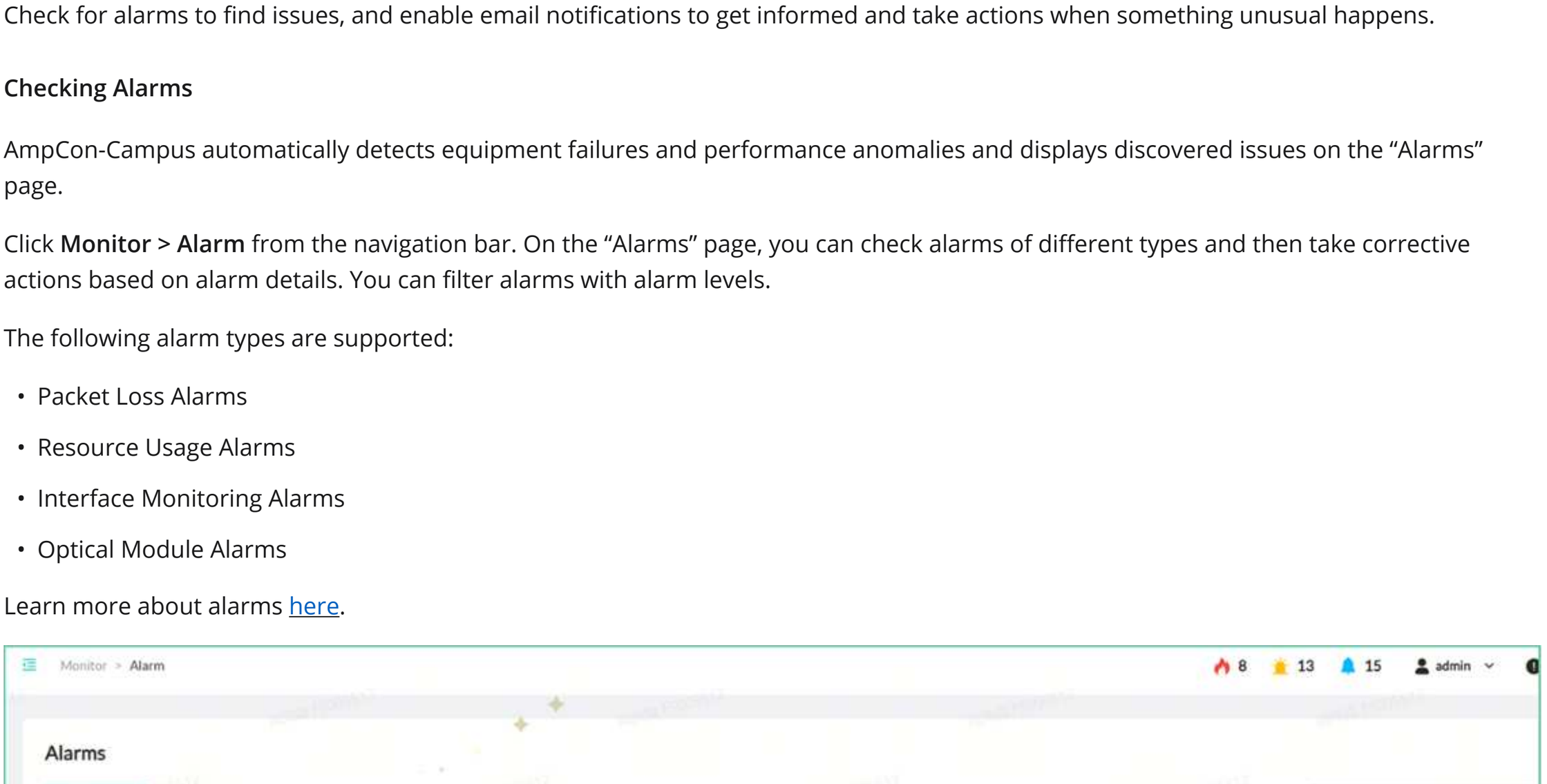
AmpCon-Campus automatically detects equipment failures and performance anomalies and displays discovered issues on the “Alarms” page.

Click **Monitor > Alarm** from the navigation bar. On the “Alarms” page, you can check alarms of different types and then take corrective actions based on alarm details. You can filter alarms with alarm levels.

The following alarm types are supported:

- Packet Loss Alarms
- Resource Usage Alarms
- Interface Monitoring Alarms
- Optical Module Alarms

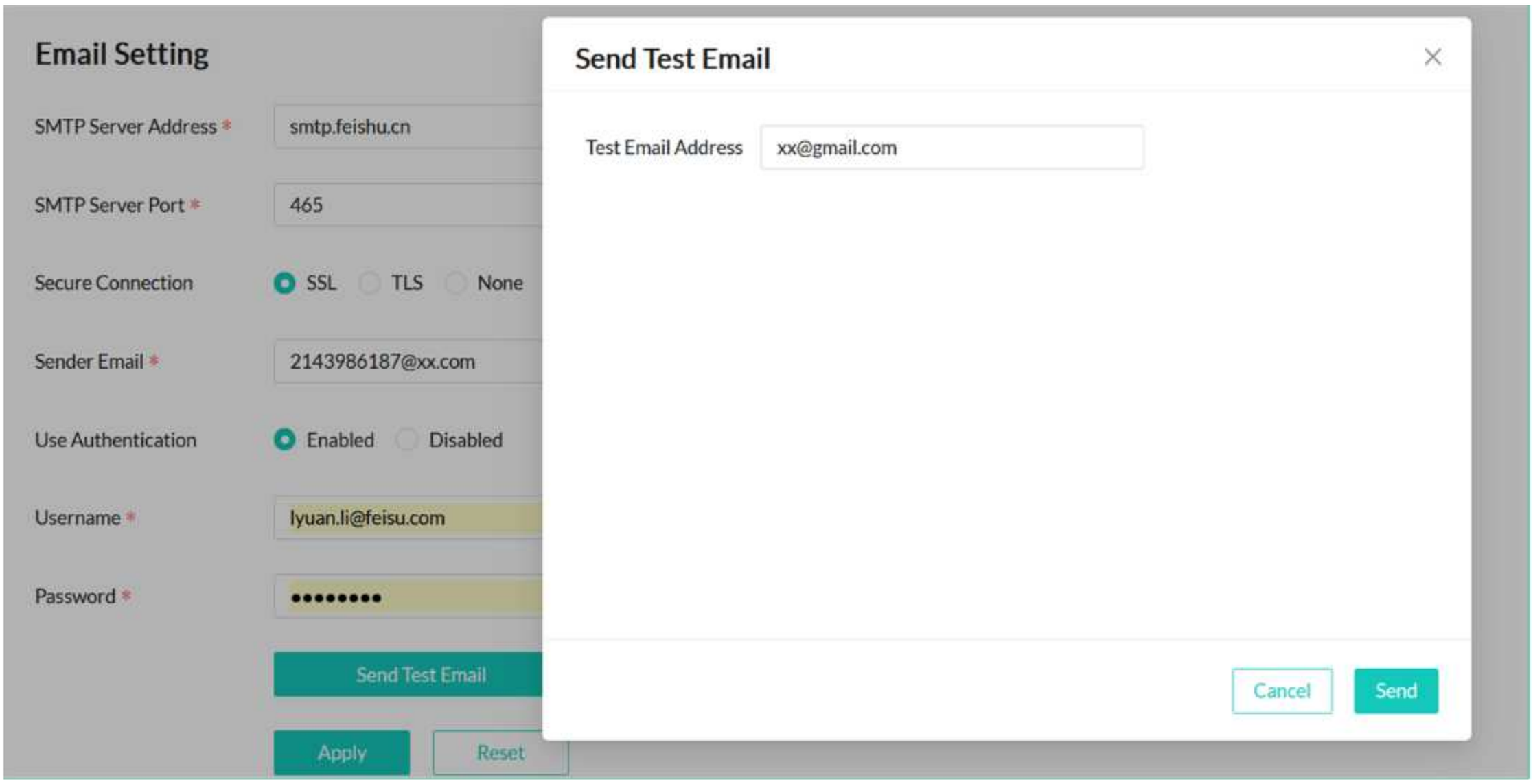
Learn more about alarms here.



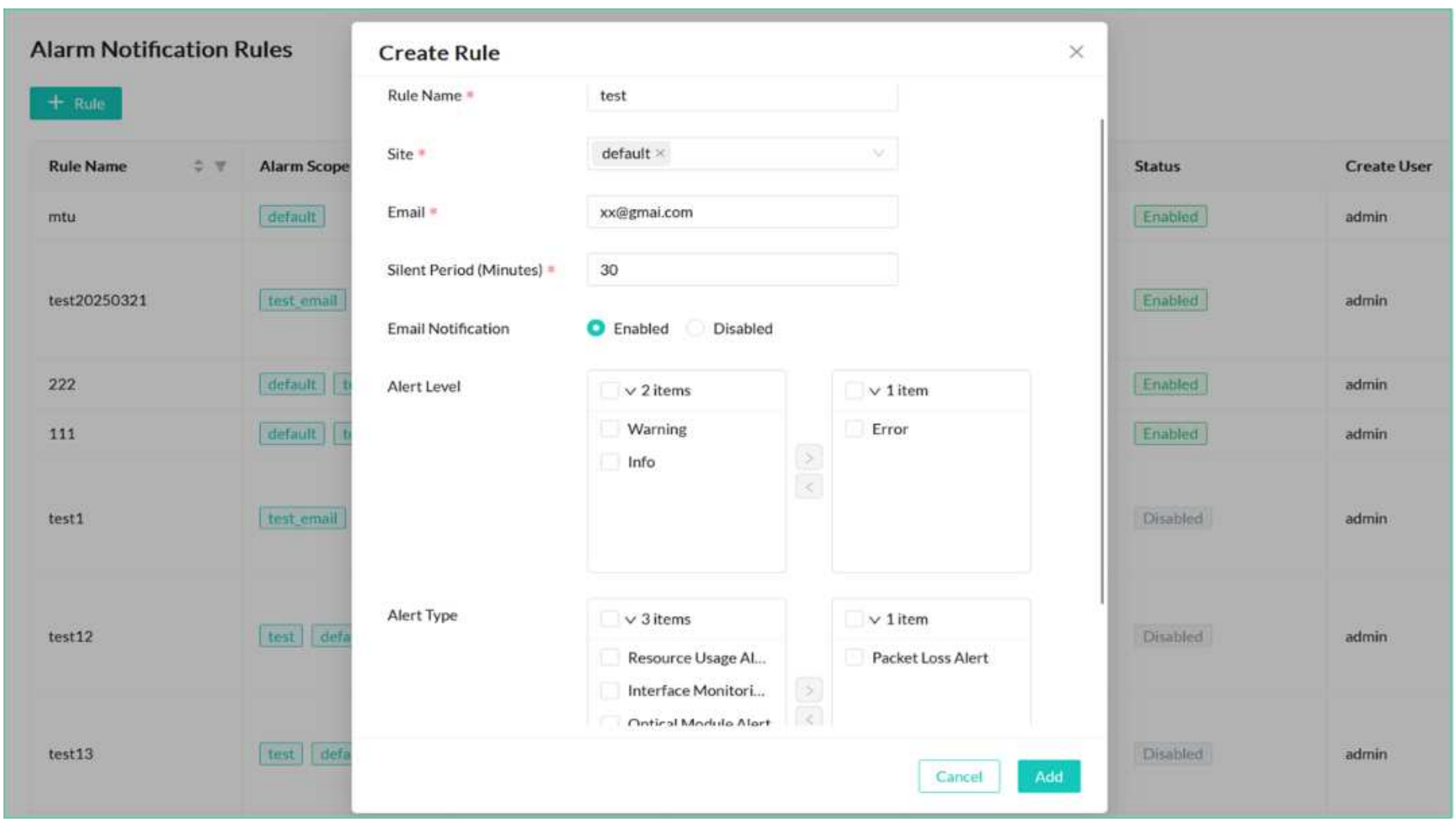
Setting and Receiving Alarm Notifications

If you need to be notified immediately when issues happen, you can enable the alarm notification feature to receive real-time notifications through emails.

Configure an SMTP Server for sending, relaying, and routing email messages.

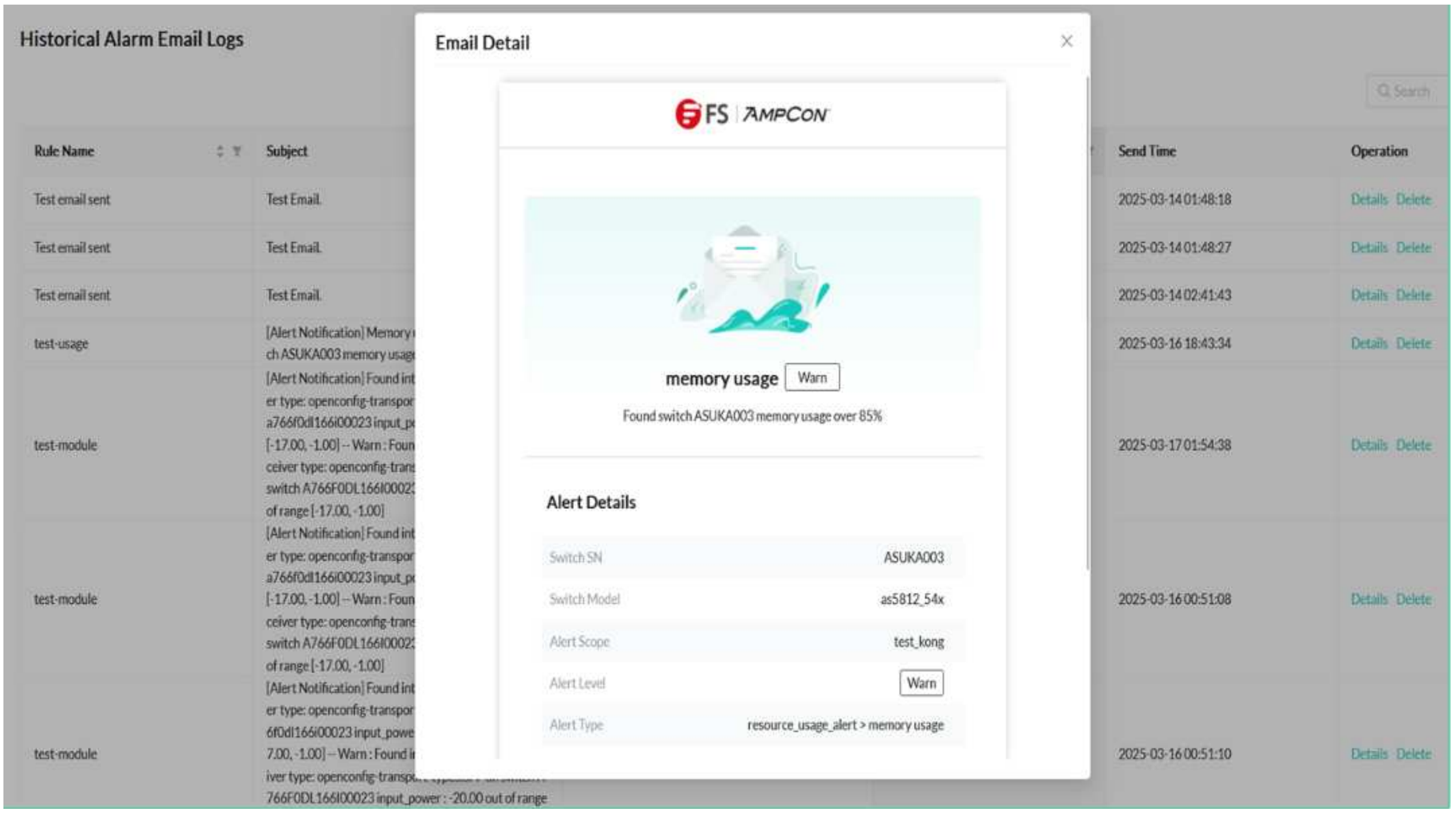


Configure a notification rule to define the alarm types, alarm levels, and fabrics to be monitored and to designate the email address to be notified.



Once done, alarm 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.

View all historical alarm notifications sent in the last 30 days for root cause analysis or auditing.



Running Ansible Playbooks

Run Ansible playbooks on AmpCon-Campus to automate routine operations in your network.

Prerequisites

Ensure that each switch to run Ansible playbooks is managed by AmpCon-Campus. For more information, see Prerequisites.

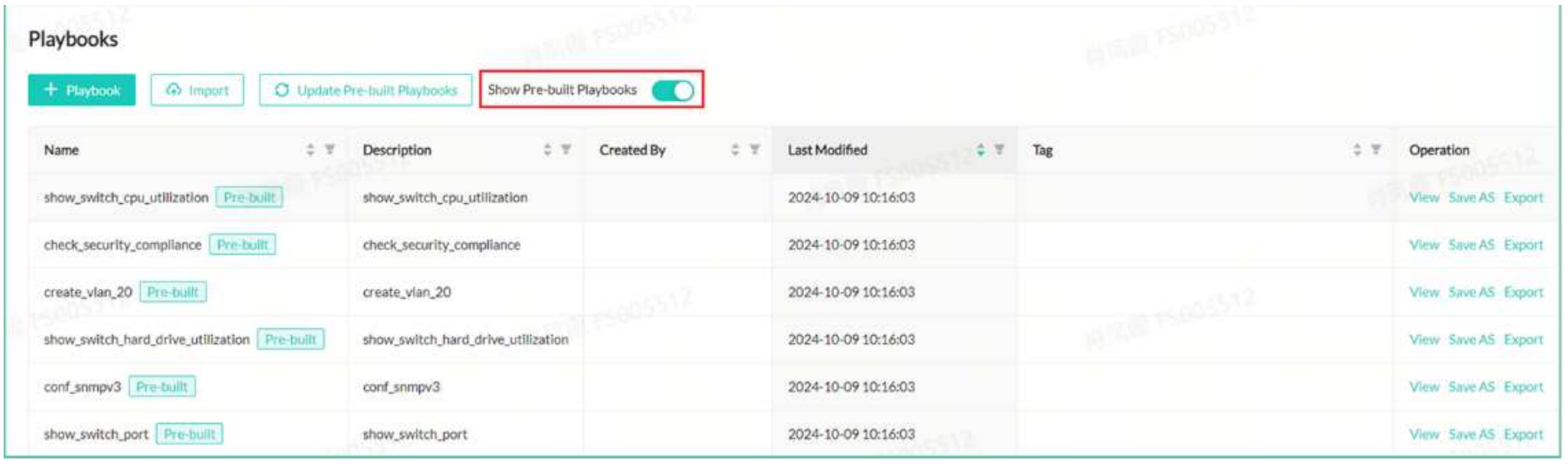
Step 1: Checking Pre-Built Playbooks

AmpCon-Campus offers a series of pre-built Ansible playbooks for automating the following routines:

- Compliance and consistency checks, to ensure switches stay in compliance with industry regulations that require a certain configuration to maintain proper security and privacy
- Connectivity checks for PicOS Software Switches
- Network operation and remediation routines such as dynamic policy enforcement

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.

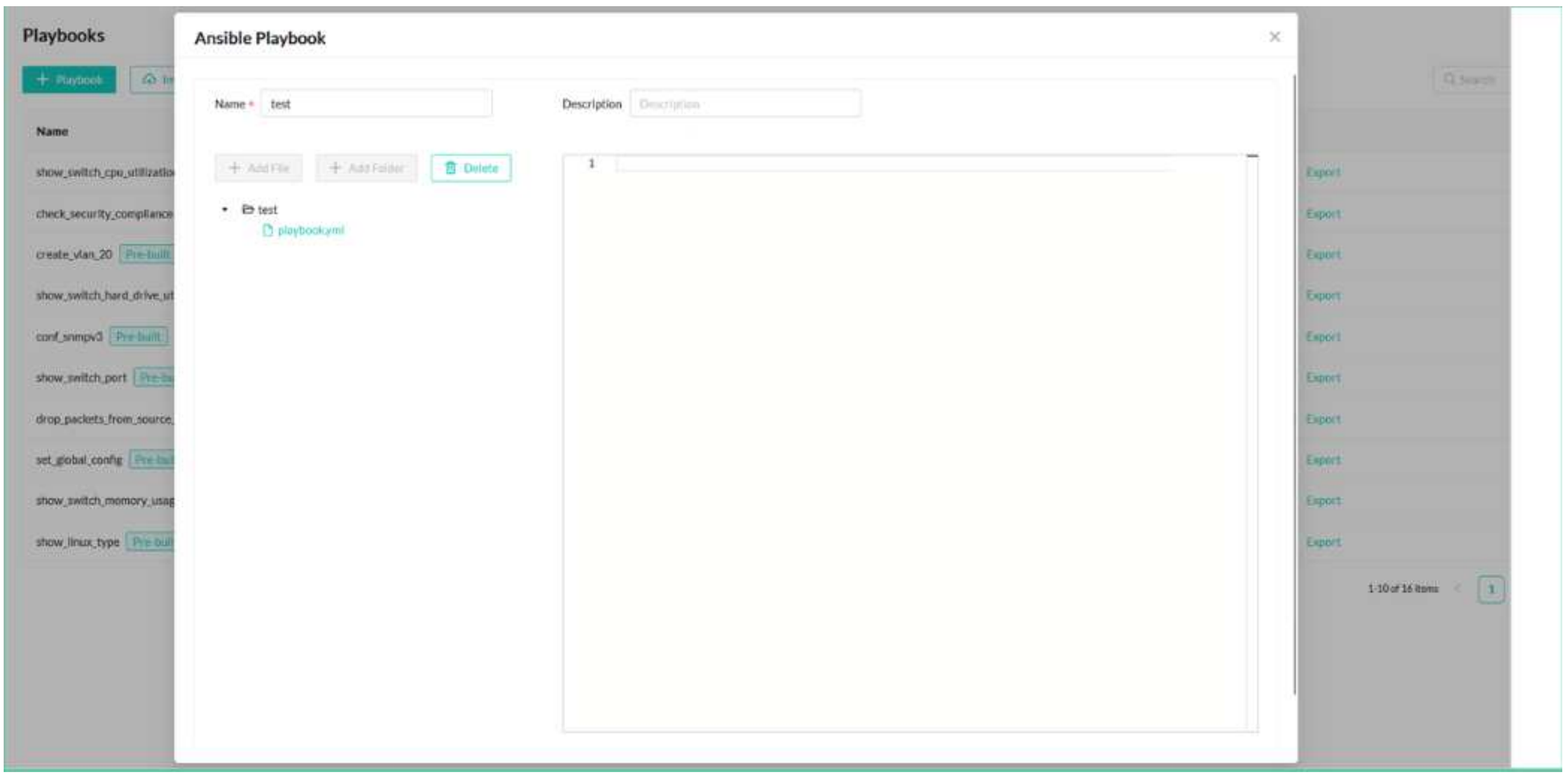
If yes, click **Save AS** on the “Playbooks” page to create a copy playbook, and then go to Step 4: Running Playbooks.



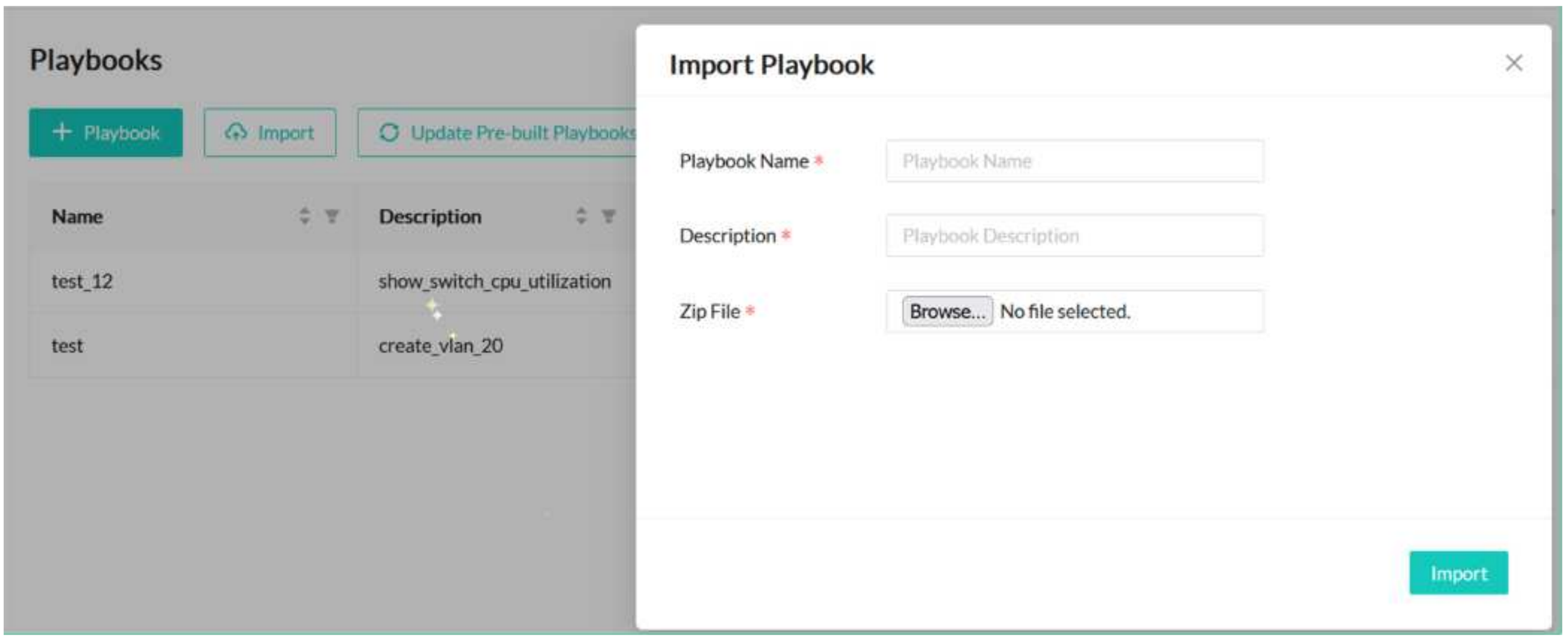
Step 2: Writing or Importing Playbooks

If the pre-built Ansible playbooks can't meet your needs, you can create a customized workflow by writing a playbook on AmpCon-Campus or importing a local playbook to AmpCon-Campus.

- Click **Maintain > Automation > Playbooks**. On the "Playbooks" page, click **+ Playbook**, and then write a playbook in the AmpCon-Campus UI.
  - When you write playbooks for managed switches, refer to Examples for Ansible Playbooks.
  - When you write playbooks for added Linux servers, refer to Using Ansible playbooks.

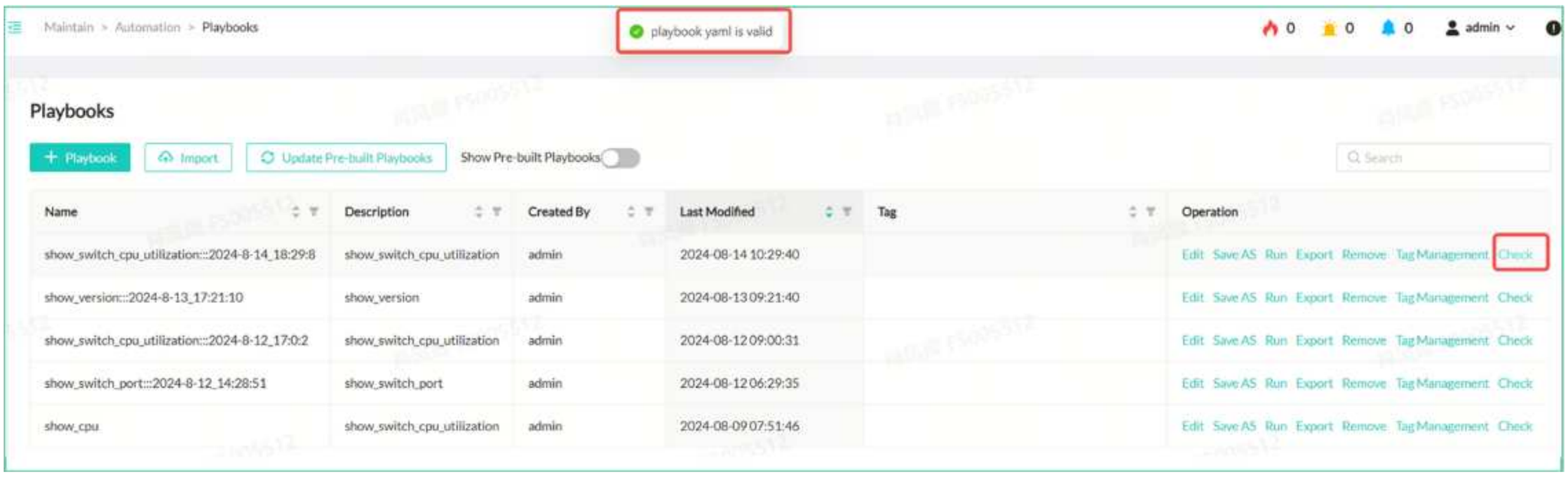


- Click **Import**, and then Import a local playbook to AmpCon-Campus.



Step 3: Checking Playbook Syntax

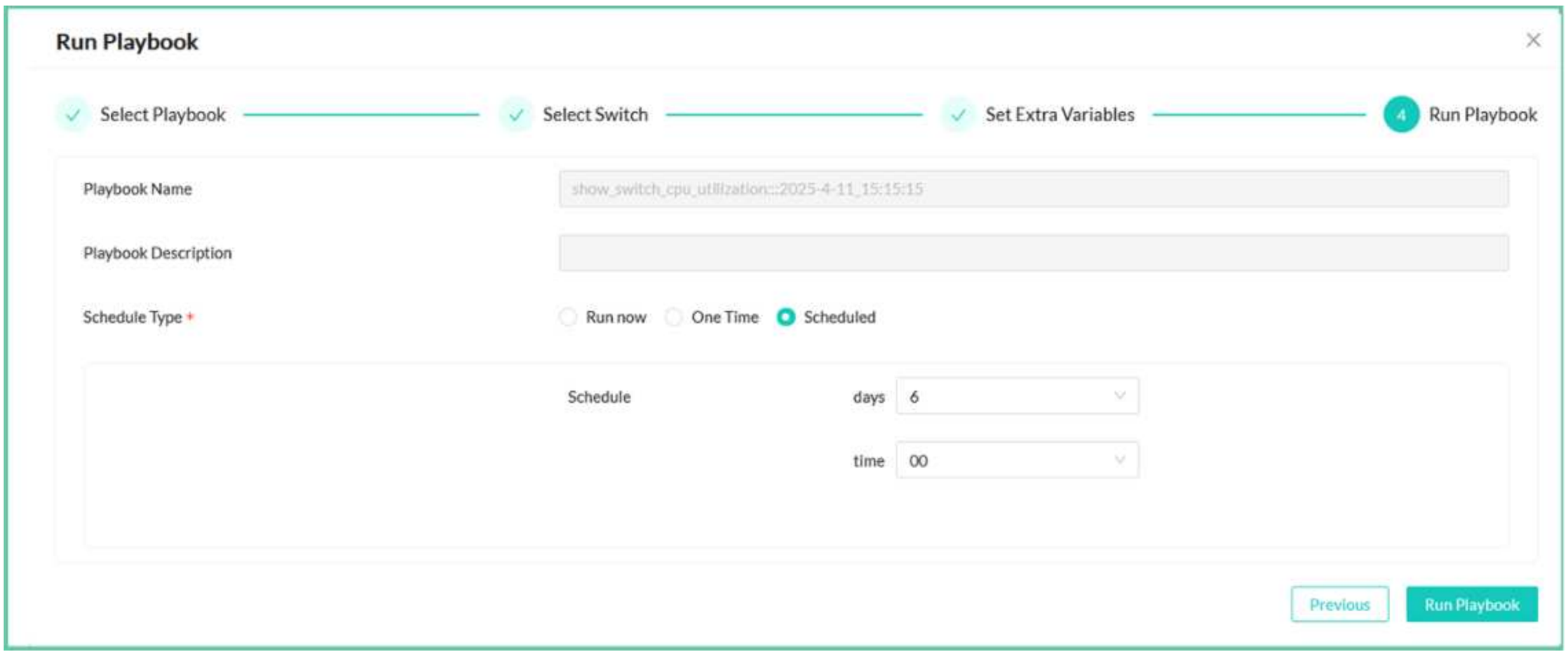
Before you run a playbook, check whether the playbook syntax is valid or not.



Step 4: Running Playbooks

Run a playbook to complete the automation operations. You can designate the schedule type of the playbook run.

- **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



Step 5: Checking Ansible Job Results and Output

After you run the Ansible playbook, you can check the execution result and output of the Ansible job.

Planning

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

Supported Information

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

For detailed information, see the following child topics:

Supported Deployments

AmpCon-Campus supports the following deployments:

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 TLS 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 for 2.2.0

AmpCon-Campus 2.2.0 supports managing the following switches:

> ⓘ **NOTE**You are recommended to install PicOS 4.6.0E or later. Or else, some features of AmpCon-Campus might not work.

Table 1. Supported FS Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	S5870-48T6BC	48 x 1G, 4 x 25G,2 x 100G	Trident3-X3	Intel x86
1G Switch Portfolio	S5870-48T6BC-U	48 x 1G PoE, 4 x 25G, 2 x 100G	Trident3-X3	Intel x86
1G Switch Portfolio	S5870-48MX6BC-U	36 x 1/2.5G PoE, 12 x 1/2.5/5/10G PoE, 4 x 25G, 2 x 100G	Trident3-X3	Intel x86
1G Switch Portfolio	S5810-48TS-P	48 x 1G copper, 4 x 10G SFP+	Helix4	ARM Cortex A9

1G Switch Portfolio	S5810-28TS	28 x 1G copper, 4 x 1G SFP, 4 x 10G SFP+ The last 4 x 1G copper ports and 4 x 1G SFP ports are combo ports.	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-28FS	8 x 1G copper, 28 x 1G SFP, 4 x 10G SFP+ The 8 x 1G copper ports and the first 8 x 1G SFP ports are combo ports.	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48TS	48 x 1G copper,4 x 10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48FS	48 x 1G SFP,4 x 10G SFP+	Helix4	ARM Cortex A9
5G Switch Portfolio	S5860-24MG-U	24 x 5G copper UPOE,4 x 25G SFP28	Hurricane3-MG	ARM Cortex A9
5G Switch Portfolio	S5860-48MG-U	48 x 5G copper UPOE, 4 x 25G SFP28, 2 x 40G QSFP+	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG-U	48 x 10G copper UPOE, 4 x 25G SFP28, 2 x 40G QSFP+	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XMG	24 x 10G copper, 4 x 10G SFP+, 4 x 25G SFP28	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-48XMG	48 x 10G copper, 4 x 25G SFP28, 2 x 40G QSFP+	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-20SQ	20 x 10G SFP+, 4 x 25G SFP28, 2 x 40G QSFP+	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	S5860-24XB-U	24 x 10G copper UPOE, 4 x 10G SFP+, 4 x 25G SFP28	Hurricane3-MG	ARM Cortex A9
10G Switch Portfolio	N5850-48S6Q	48 x 10G, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	N5850-48S6C	48 x 10G, 6 x 100G	Trident3-X5	Intel x86
10G Switch Portfolio	N5850-48X6C	48 x 10G-T, 6 x 100G	Trident3-X5	Intel x86
200G Switch Portfolio	S6860-24CD8D	24 x 200G, 8 x 400G	Trident4-X9	Intel x86
1G Switch Portfolio	S3410-24TS	24 x 1G/100M/10M copper, 4 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410-24TS-P	24 x 1G/100M/10M 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,4 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410C-16TF	16 x 1G/100M/10M copper, 2 x 1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410C-16TF-P	2 x 1G SFP,16 x 1G/10M/100M copper The first 8 copper ports support PoE.	Hurricane2	ARM Cortex A9
1G Switch Portfolio	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.	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410C-8TMS-P	2 x 10G/1G SFP+,2 x 5G/2.5G/1G copper PoE, 8 x 1G/100M/10M copperThe first 6 x 1G copper ports support PoE.	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410L-24TF	24 x 1G/100M/10M copper, 4 x 1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410L-24TF-P	24 x 1G/100M/10M copper PoE, 4 x 1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3410L-48TF	48 x 1G/100M/10M copper, 4 x 10G/1G SFP+	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3270-10TM	10 x 1G/100M/10M copper, 2 x 2.5G/1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM	24 x 1G/100M/10M copper, 4 x 2.5G/1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3270-48TM	48 x 1G/100M/10M copper, 4 x 2.5G/1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3270-10TM-P	10 x 1G/100M/10M copper PoE, 2 x 2.5G/1G SFP	Hurricane2	ARM Cortex A9
1G Switch Portfolio	S3270-24TM-P	24 x 1G/100M/10M copper PoE, 4 x 2.5G/1G SFP	Hurricane2	ARM Cortex A9
200G Switch Portfolio	N8550-24CD8D	24 x 200G, 8 x 400G	Trident4-X9	Intel x86
1G Switch Portfolio	S5870-48T6S	48 x 1G-T, 6 x 10G	Trident3-X2	Intel x86
1G Switch Portfolio	S5870-48T6S-U	48 x 1G PoE, 6 x 10G	Trident3-X2	Intel x86
25G Switch Portfolio	N8550-48B8C	48 x 25G, 8 x 100G	Trident3-X7	Intel x86

100G Switch Portfolio	N8550-32C	32 x 100G	Trident3-X7	Intel x86
100G Switch Portfolio	N8550-64C	64 x 100G	Tomahawk2	Intel x86
100G Switch Portfolio	N8560-32C	32 x 100G QSFP28	Trident3	Intel x86
100G Switch Portfolio	S5890-32C	32 x 100G QSFP28	Trident3-X7	Intel x86
25G Switch Portfolio	S5580-48Y	48 x 25G, 8 x 100G	Trident3-X7	Intel x86

Table 2. Supported Edgecore Switches

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	Trident3-X3	Intel x86
1G Switch Portfolio	N3224P-ON	24 x 1G 30W PoE, 4 x 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224T-ON	24 x 1G, 4 x 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248P-ON	48 x 1G 30W PoE, 4 x 10G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248TE-ON	48 x 1G, 4 x 10G	Trident3-X3	Intel x86
Multi-Gig Switch Portfolio	N2224PX-ON	24 x 1G/2.5G30W/60W PoE, 4 x 25G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2224X-ON	24 x 1G/2.5G, 4 x 25G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248PX-ON	48 x 1G/2.5G30W/60W PoE, 4 x 25G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248X-ON	48 x 1G/2.5G, 4 x 25G	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N3132PX-ON	24 x 1G PoE,8 x 1/2.5/5G PoE, 4 x 10G	Firebolt 4 FS	ARM Cortex A9
Multi-Gig Switch Portfolio	N3208PX-ON	4 x 1/2.5/5G PoE,4 x 1G PoE, 2 x 10G SFP+	Hurricane3-MG	Intel x86
Multi-Gig Switch Portfolio	N3224PX-ON	24 x 1/2.5/5/10G 90W PoE, 4 x 25G	Trident3-X3	Intel x86
Multi-Gig Switch Portfolio	N3248PXE-ON	48 x 1/2.5/5/10G 90W PoE, 4 x 25G	Trident3-X5	Intel x86
Multi-Gig Switch Portfolio	N3248X-ON	48 x 1/2.5/5/10G, 4 x 25G	Trident3-X5	Intel x86

10G Switch Portfolio	S4048-ON	48 x 10G, 6 x 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	Z9100-ON	32 x 100G	Tomahawk	Intel x86
100G Switch Portfolio	Z9264F-ON	64 x 100G	Tomahawk2	Intel x86
100G Switch Portfolio	S5232F-ON	32 x 100G	Trident3-X7	Intel x86

Table 4. Supported Delta Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	AG7648	48 x 10G	Trident2	Intel x86
25G Switch Portfolio	AG5648 v1-R	48 x 25G	Tomahawk+	Intel x86
100G Switch Portfolio	AG9032 v1	32 x 100G	Tomahawk	Intel x86

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

Installation Requirements

Before you install AmpCon-Campus, check the following requirements:

Server Requirements

Ensure that the machine to install the AmpCon-Campus server meets the following requirements:

Table 1. Server Requirement Details

Indicators		Requirements
CPU	Clock speed	2.0 GHz or faster
	Number of cores	4 CPU cores
Memory		16 GB
Hard disk		512 GB

Operating systems	Ubuntu 22.04 X86 architecture

Network Requirements

Set the firewall and proxy properly to allow the following network access.

- Ensure that the AmpCon-Campus server machine allows the following protocols and ports:

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

- Ensure that the switch machines to be managed allow the following protocols and ports:

Table 3. Network Requirement for Switches

TCP/UDP	Port	Protocol
TCP	22	SSH
TCP	9339	gRPC/gNMI

Browser Requirements

When you use a browser to log in to the AmpCon-Campus UI, use Chrome 98, Edge 98, Firefox 94, or higher versions.

Deploying AmpCon-Campus

To deploy AmpCon-Campus, see the following instructions:

Installing the AmpCon-Campus Server

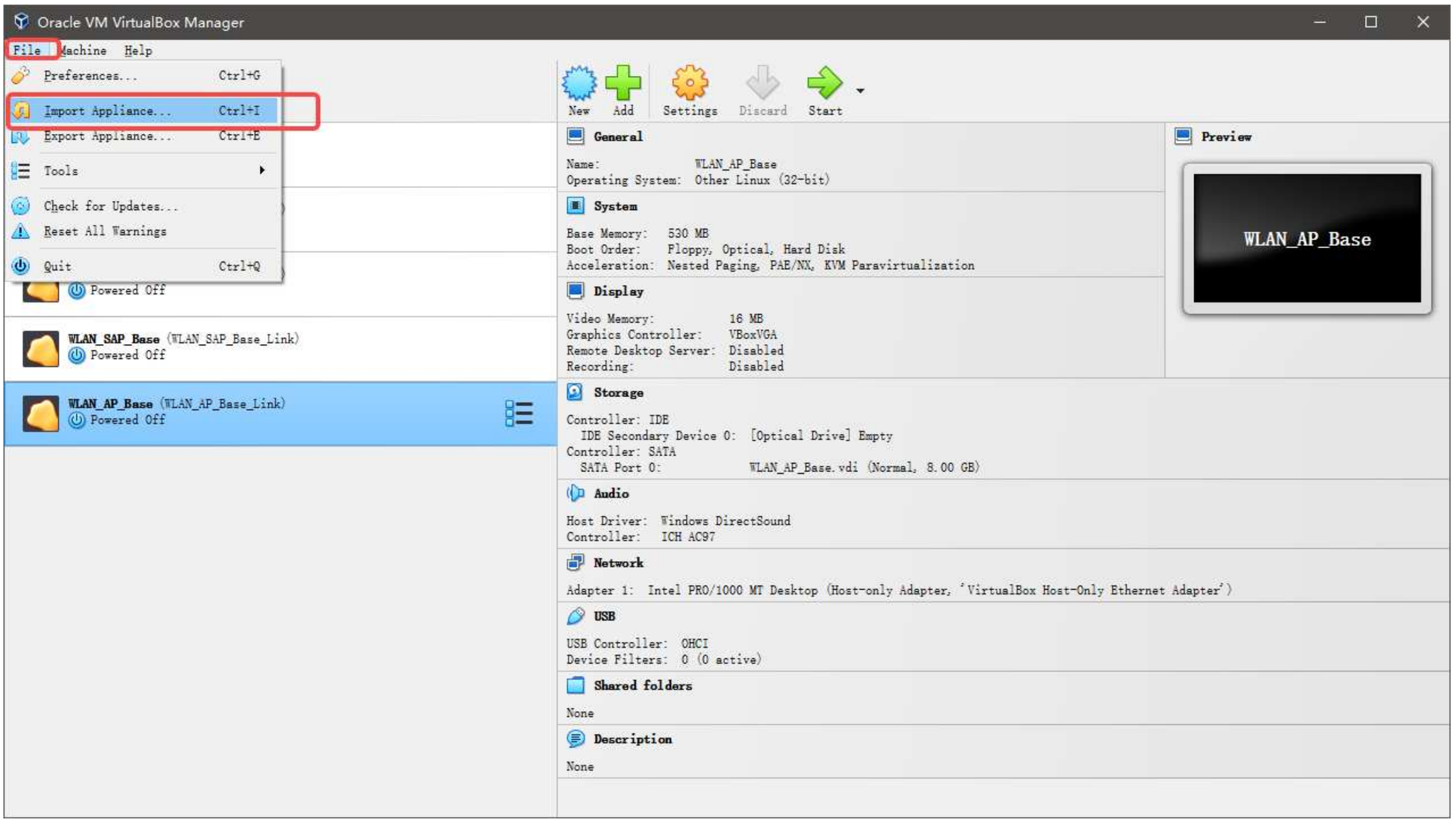
You can install the AmpCon-Campus server on a virtual machine or a physical machine by using one of the following methods:

Installing on VirtualBox for Lab Only

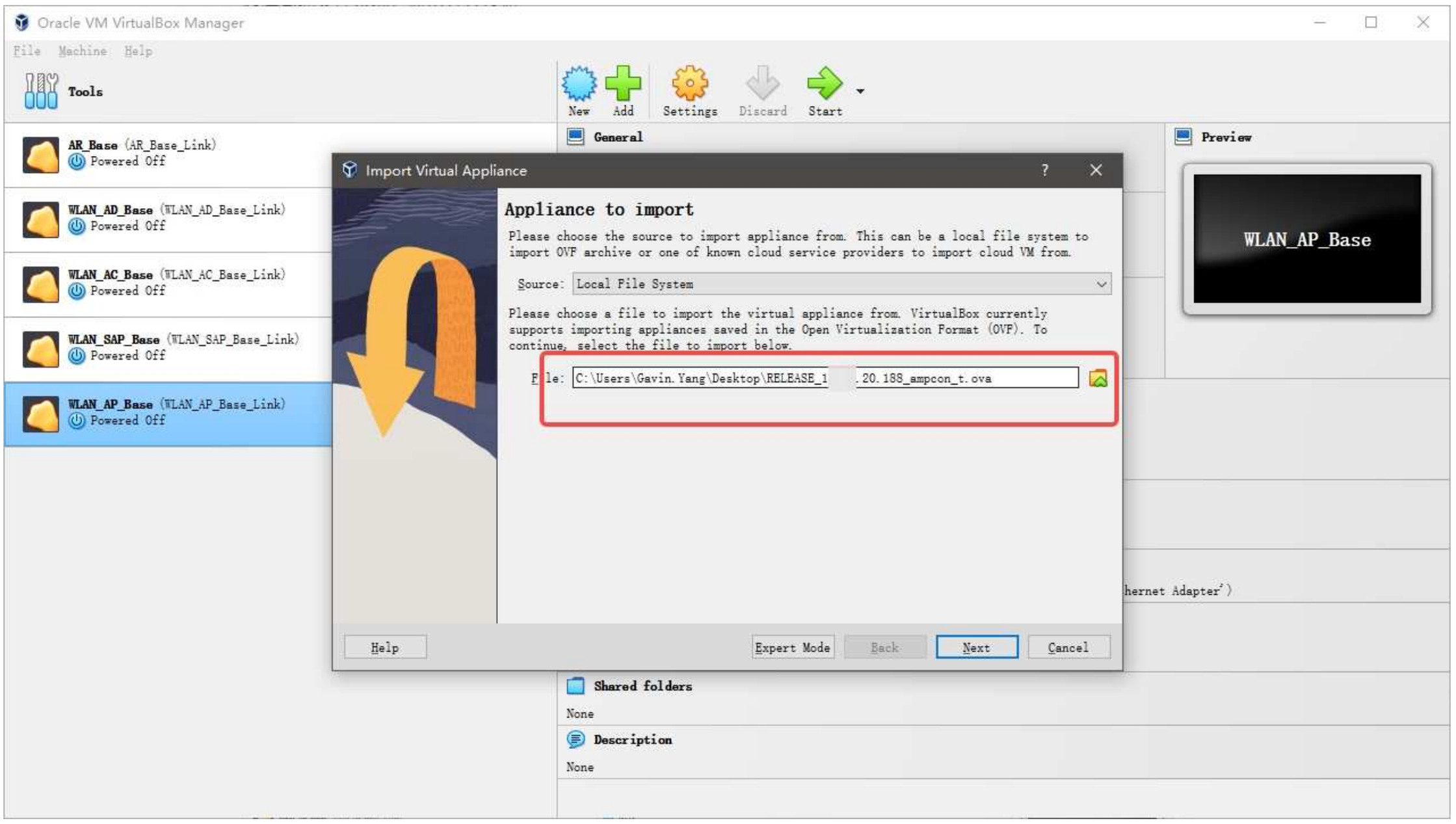
You can install the AmpCon-Campus server on VirtualBox for lab purposes only. Production environments require a proper enterprise-scale virtualization solution as described in Supported Deployments. For how to use VirtualBox in general, see the Oracle VirtualBox documentation.

- Ensure that the installation requirements are met.
- Download the compressed AmpCon-Campus server image file by going to the FS AmpCon-Campus website and then clicking **AmpCon-Campus for VirtualBox 2.2.x Software** in the **Resources** section.
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

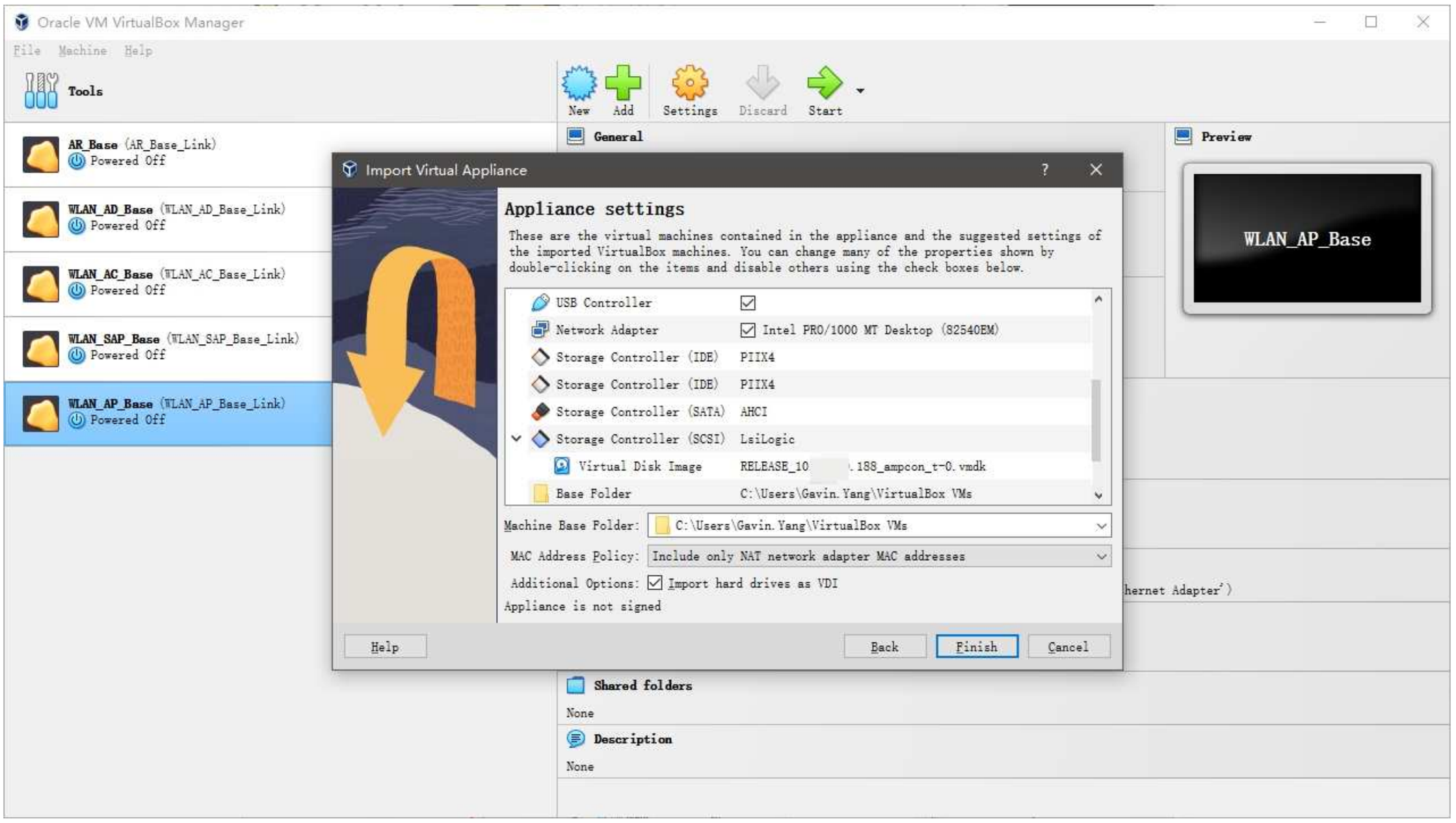
Open the VirtualBox console, and then click **File** > **Import Appliance**.



Select **Local File System**, and then select the AmpCon-Campus server .ova image file.

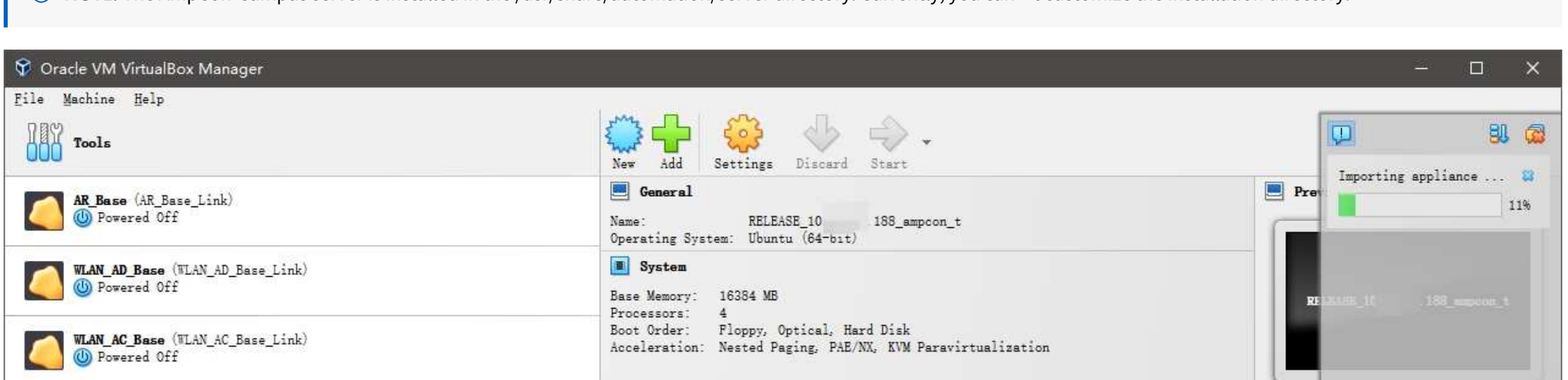


Confirm the settings for the .ova file, and then click **Finish**.

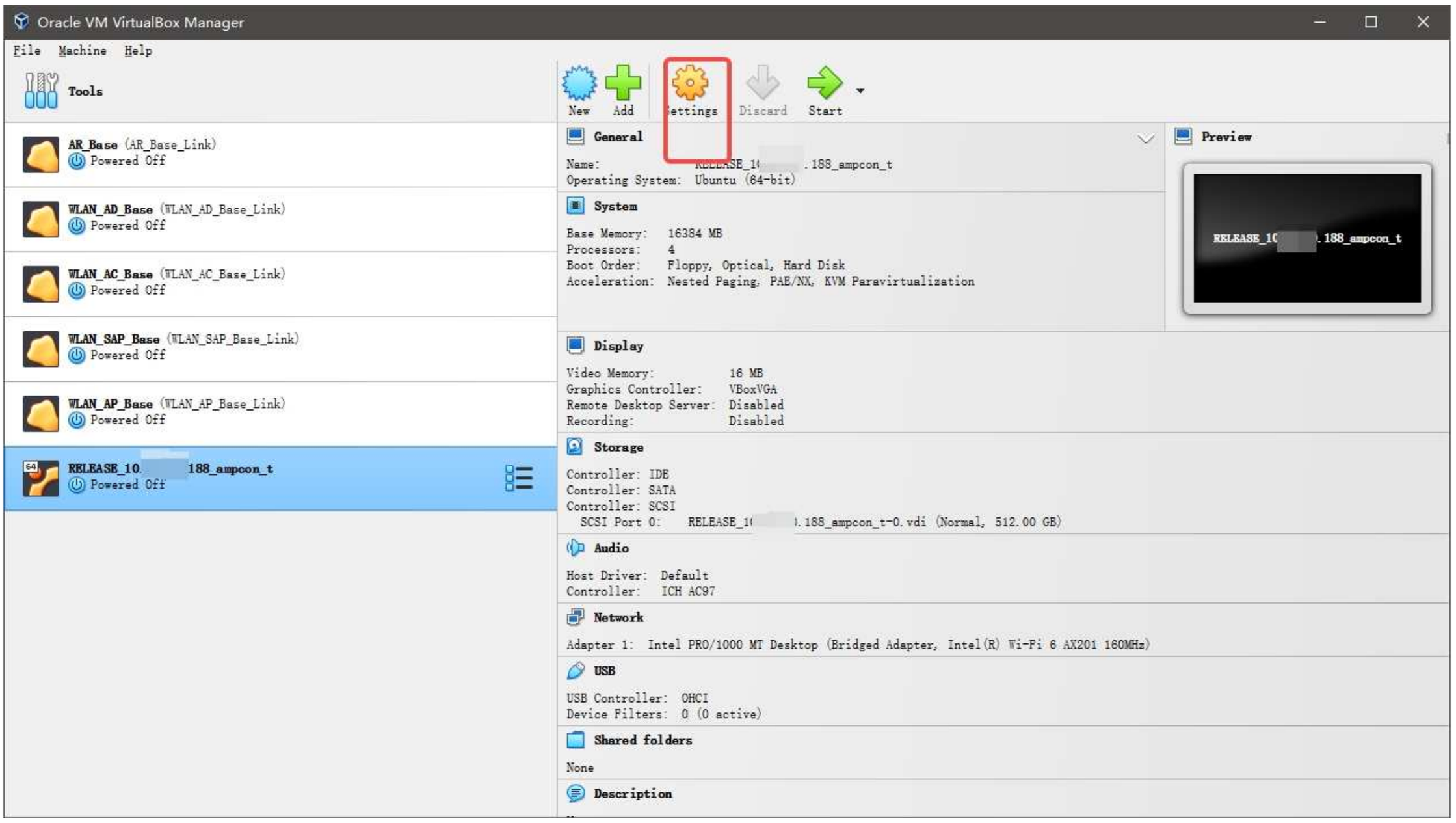


Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-Campus server is installed.

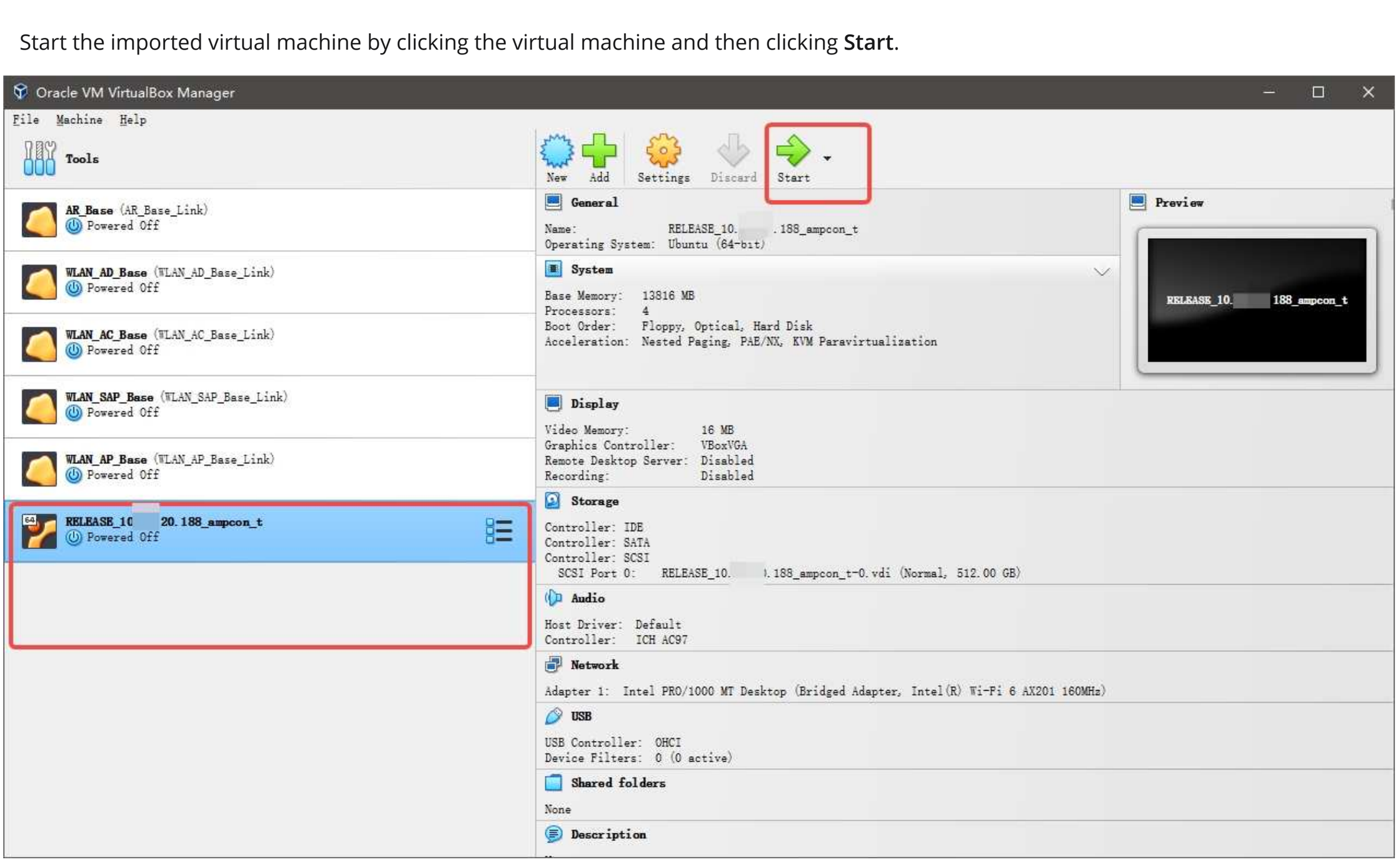
> ⓘ **NOTE:** The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can’ t customize the installation directory.



Check the settings of the imported virtual machine.



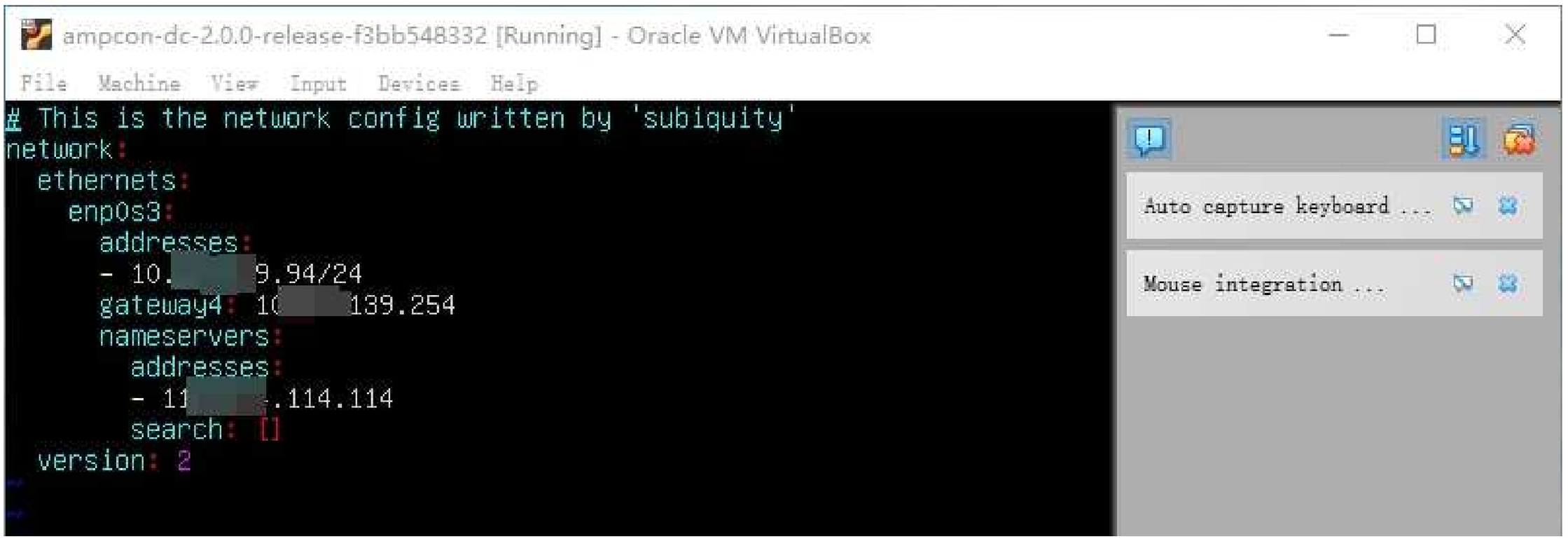
Start the imported virtual machine by clicking the virtual machine and then clicking **Start**.



Modify the network interface configuration.

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

b. Modify the IP address with the real IP address of the virtual machine.



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

```
sudo netplan apply
```

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.

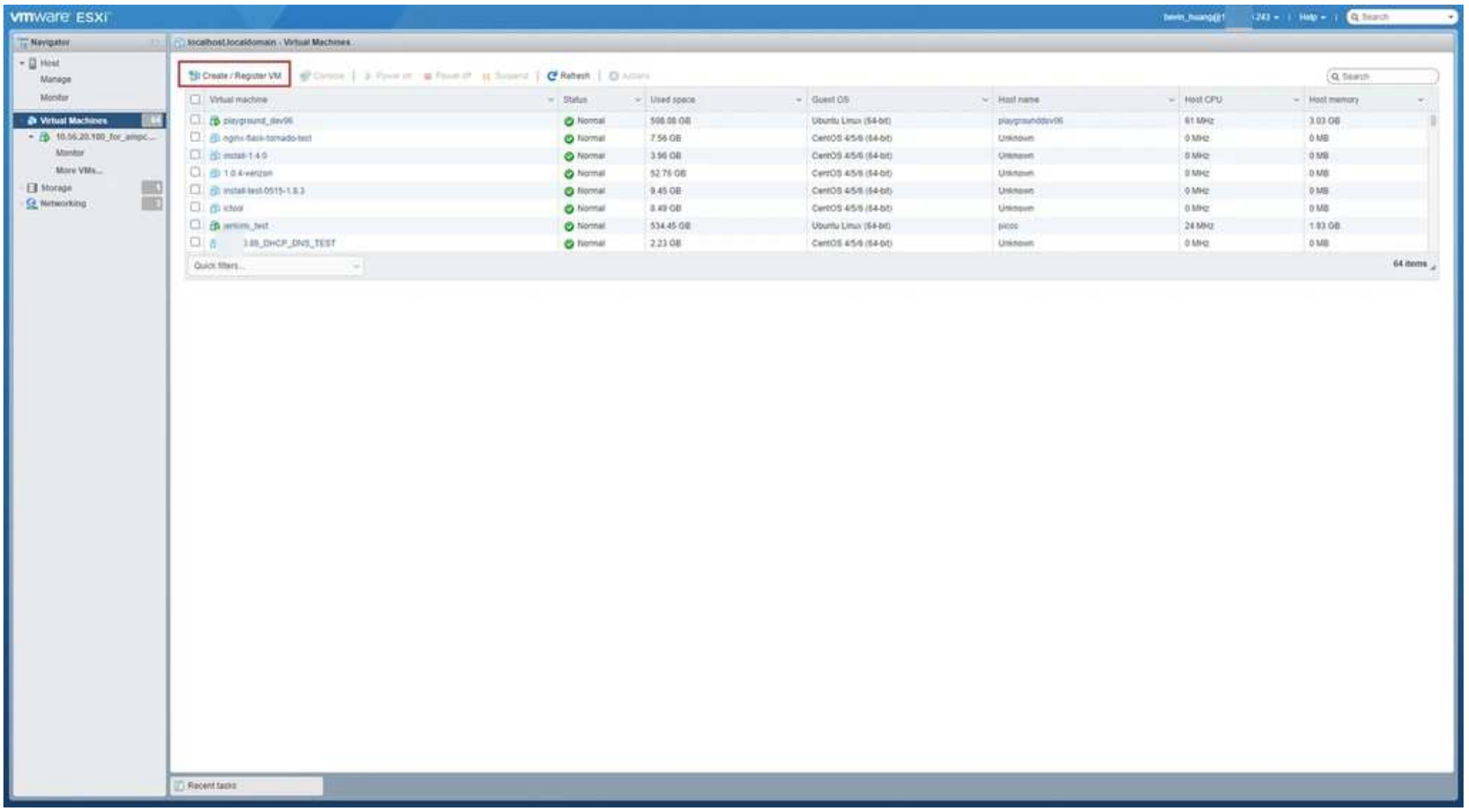
After you install the AmpCon-Campus server, you need to add system configurations and import AmpCon-Campus Licenses.

Installing on VMware ESXi

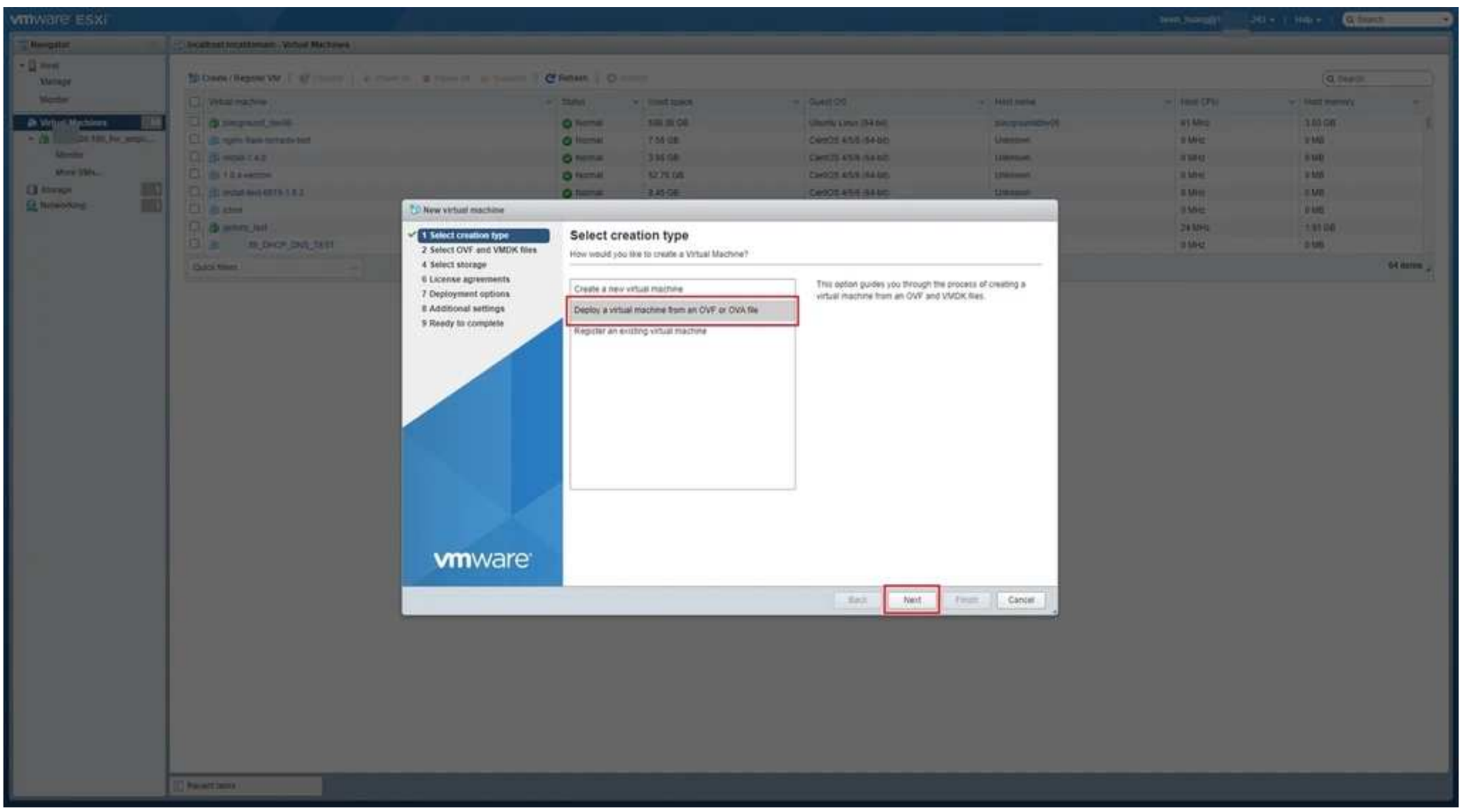
You can install the AmpCon-Campus server on VMware ESXi 6.7, 7.0, 8.0. For how to use VMware ESXi in general, see the VMware ESXi documentation.

- Ensure that the installation requirements are met.
- Download the compressed AmpCon-Campus server image file by going to the FS AmpCon-Campus website and then clicking **AmpCon-Campus for VMWare ESXi 2.2.x Software** in the **Resources** section.
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

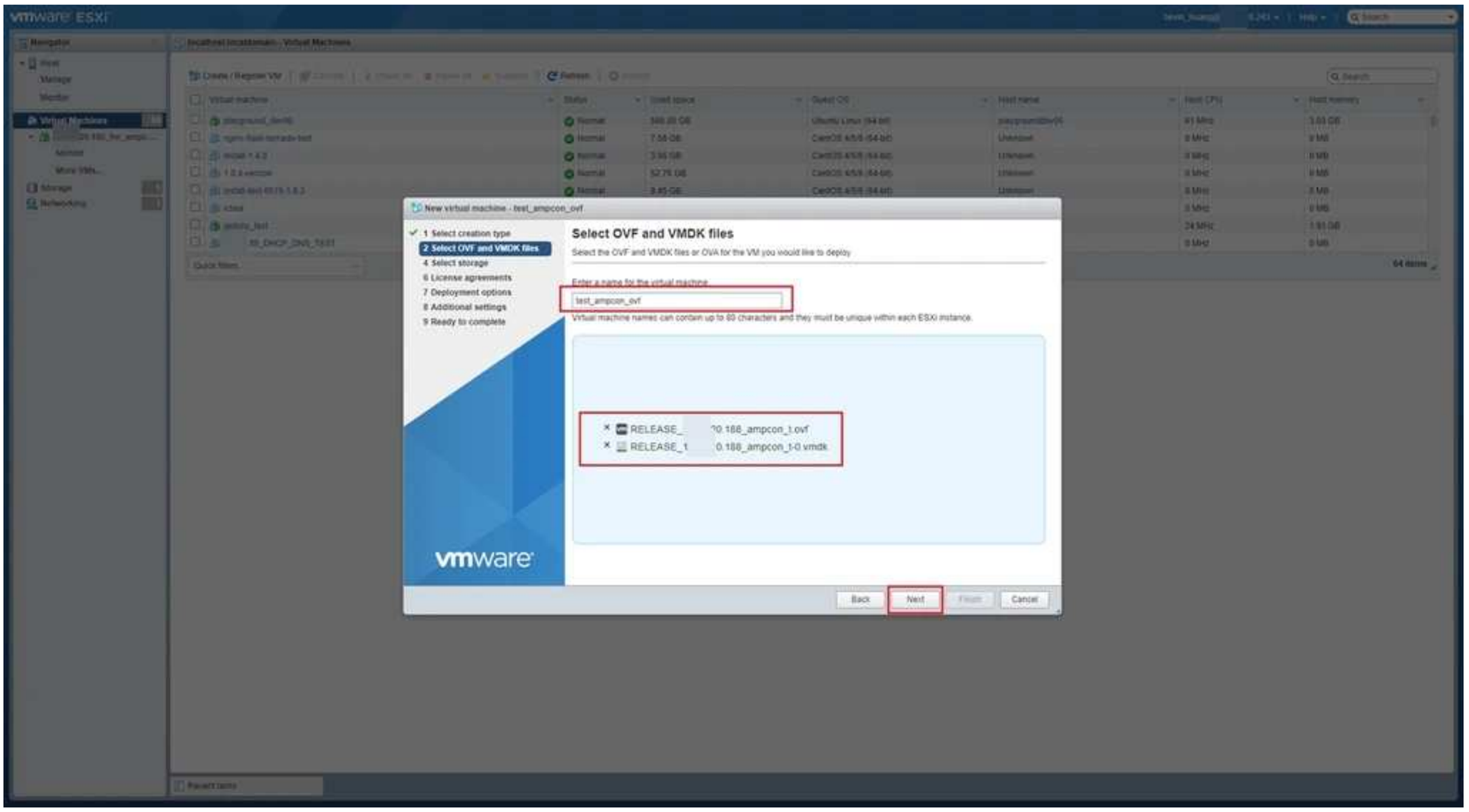
Open the VMware ESXi console, and then click **Create / Register VM**.



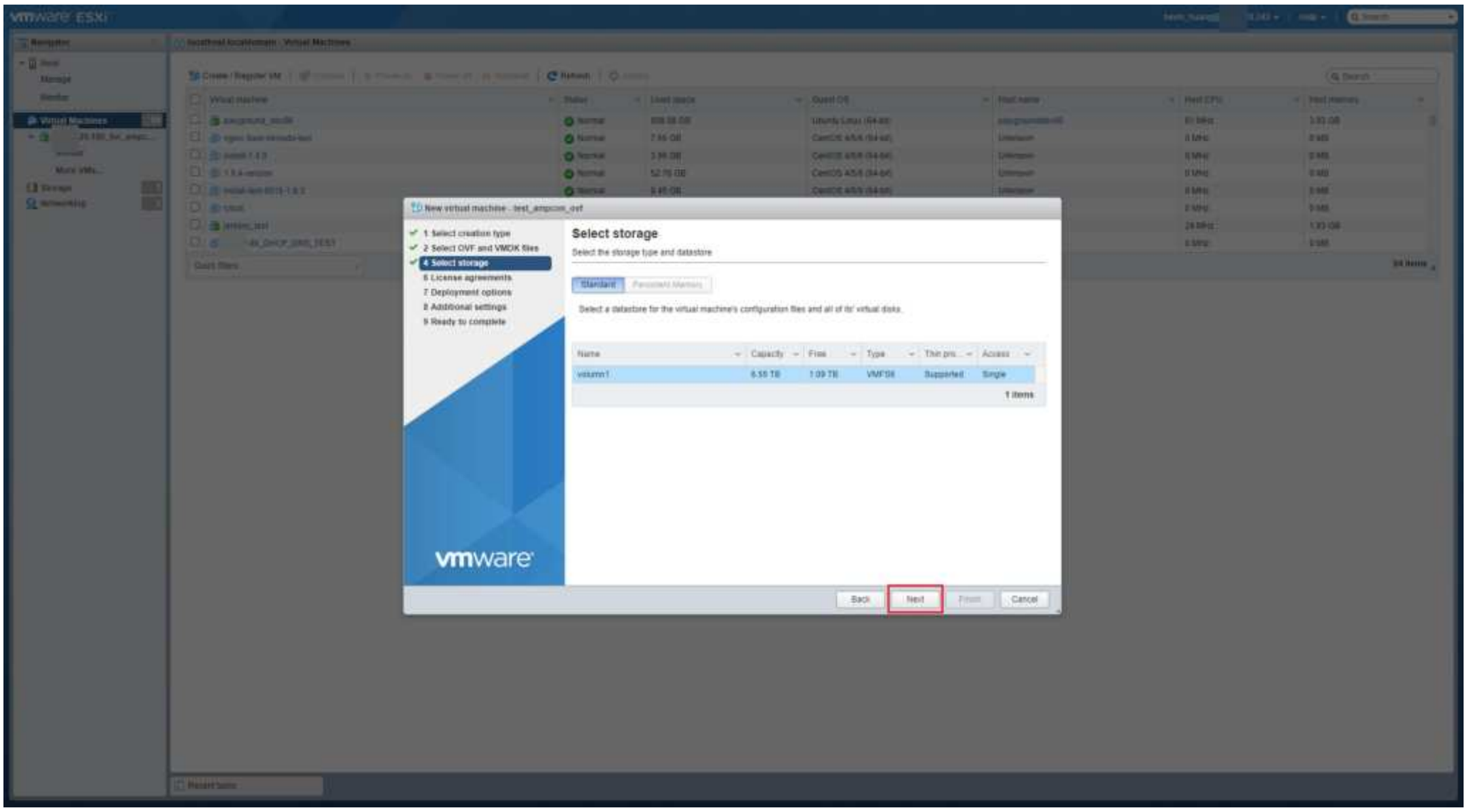
Select **Deploy a virtual machine from an OVF or OVA file**, and then click **Next**.



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

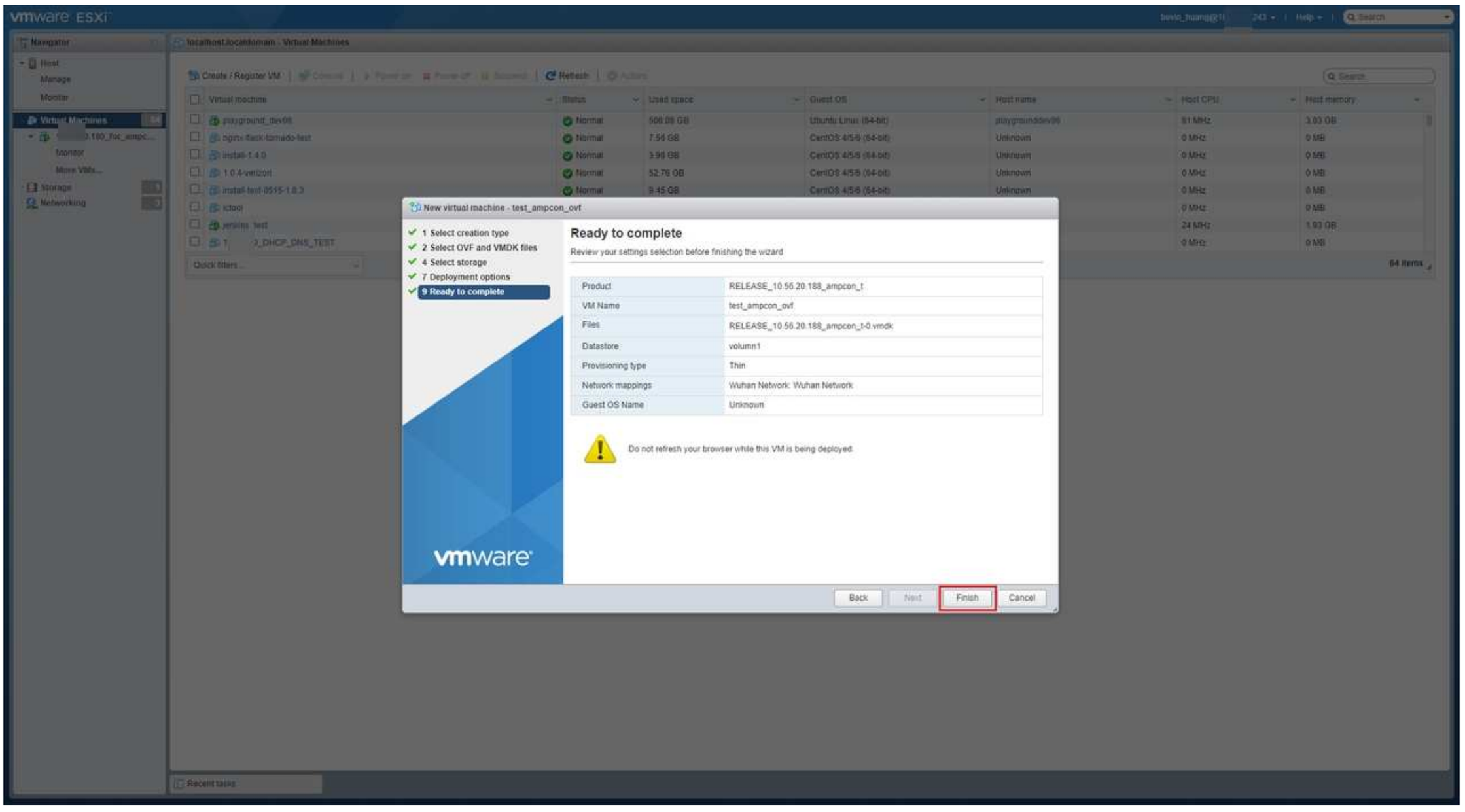


Confirm the storage type and datastore, and then click **Next**.



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**.

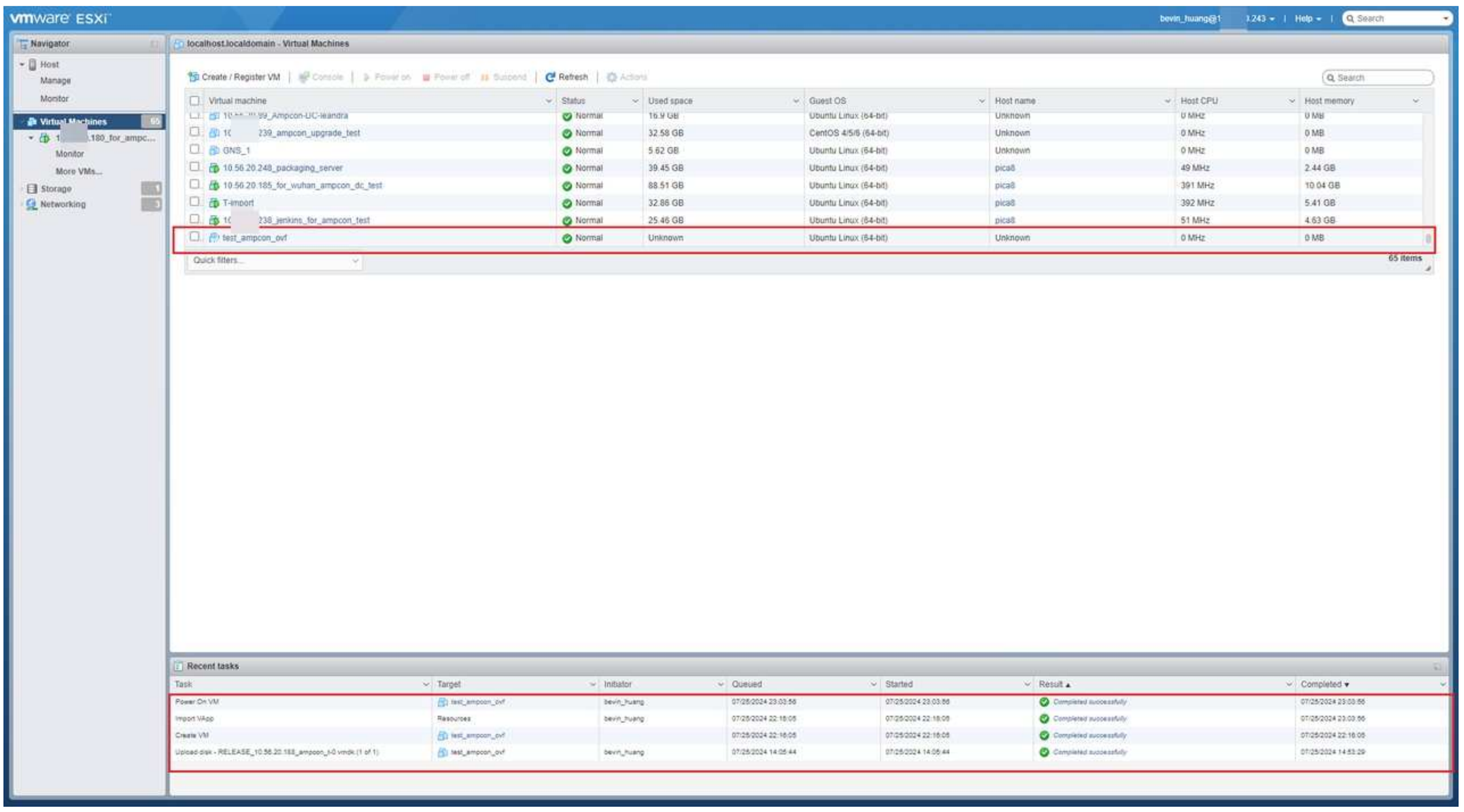
Click **Finish**.



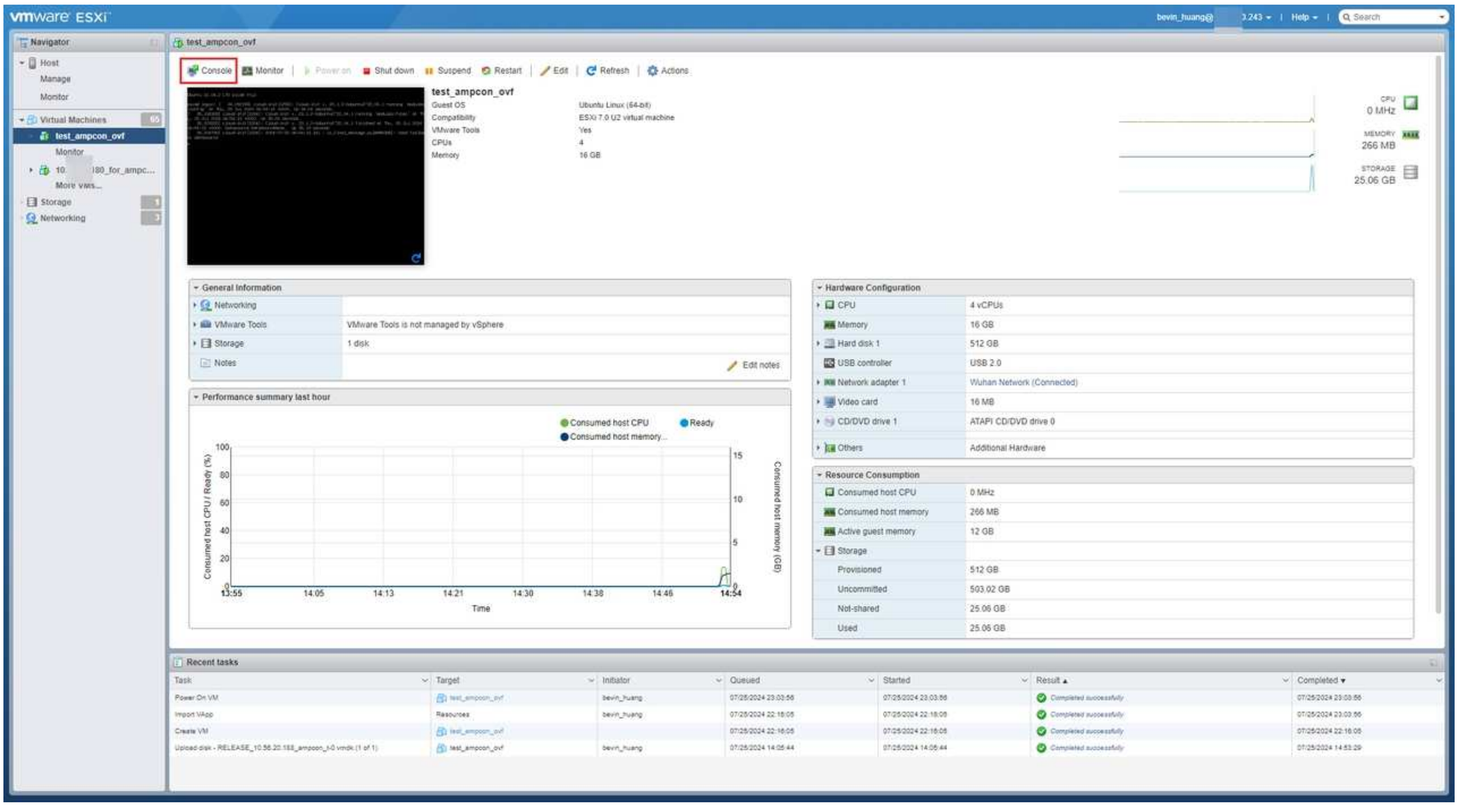
Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-Campus server is installed.

> ⓘ **NOTE**The AmpCon-Campus server is installed in the /usr/share/automation/server directory. Currently, you can’ t customize the installation directory.

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



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



Modify the network interface configuration.

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

b. Modify the IP address with the real IP address of the virtual machine.

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

test_ampcon_ovf — Actions

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      addresses:
      - [redacted].20.171/24
      gateway4: [redacted].20.254
      nameservers:
        addresses:
        - [redacted].114.114
        search: []
  version: 2
```

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

```
sudo netplan apply
```

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.

After you install the AmpCon-Campus server, you need to add system configurations and import AmpCon-Campus Licenses.

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.

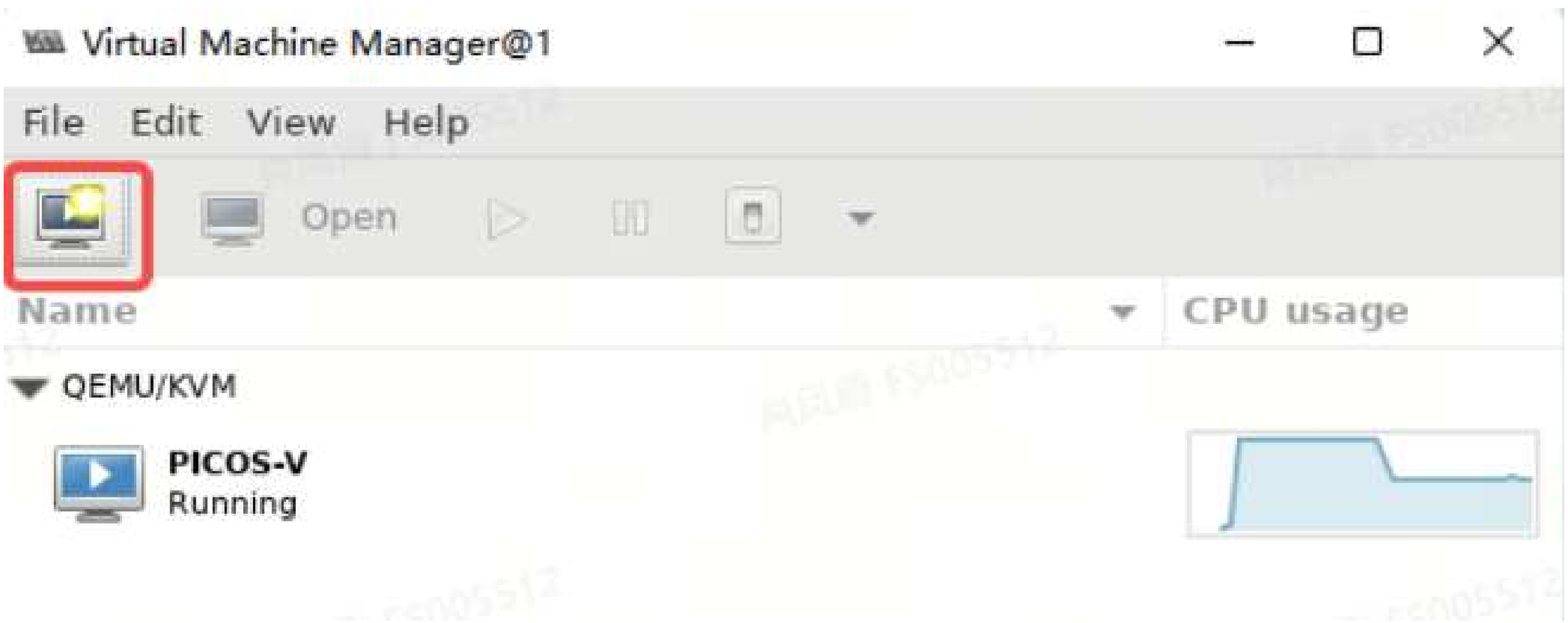
In this topic, KVM virt-manager is used to demonstrate the AmpCon-Campus server installation steps.

- Ensure that the installation requirements are met.
- Download the compressed AmpCon-Campus server image file by going to the FS AmpCon-Campus website and then clicking **AmpCon-Campus for QEMU/KVM 2.2.x Software** in the **Resources** section.
- Put the compressed AmpCon-Campus server image file to the machine where the hypervisor exists, and unzip the file.

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

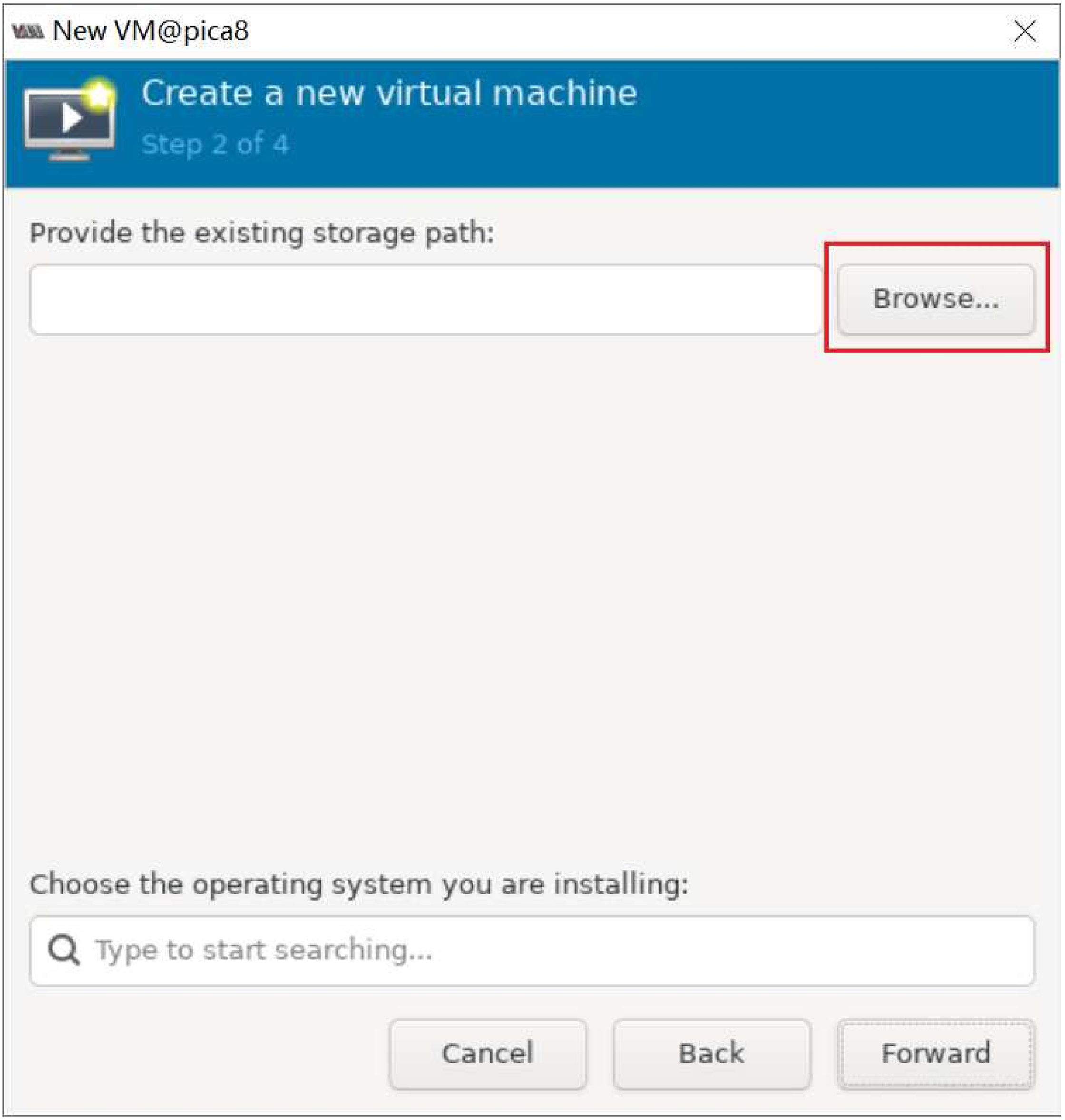
```
virt-manager
```

Click the following button to start the importing process.

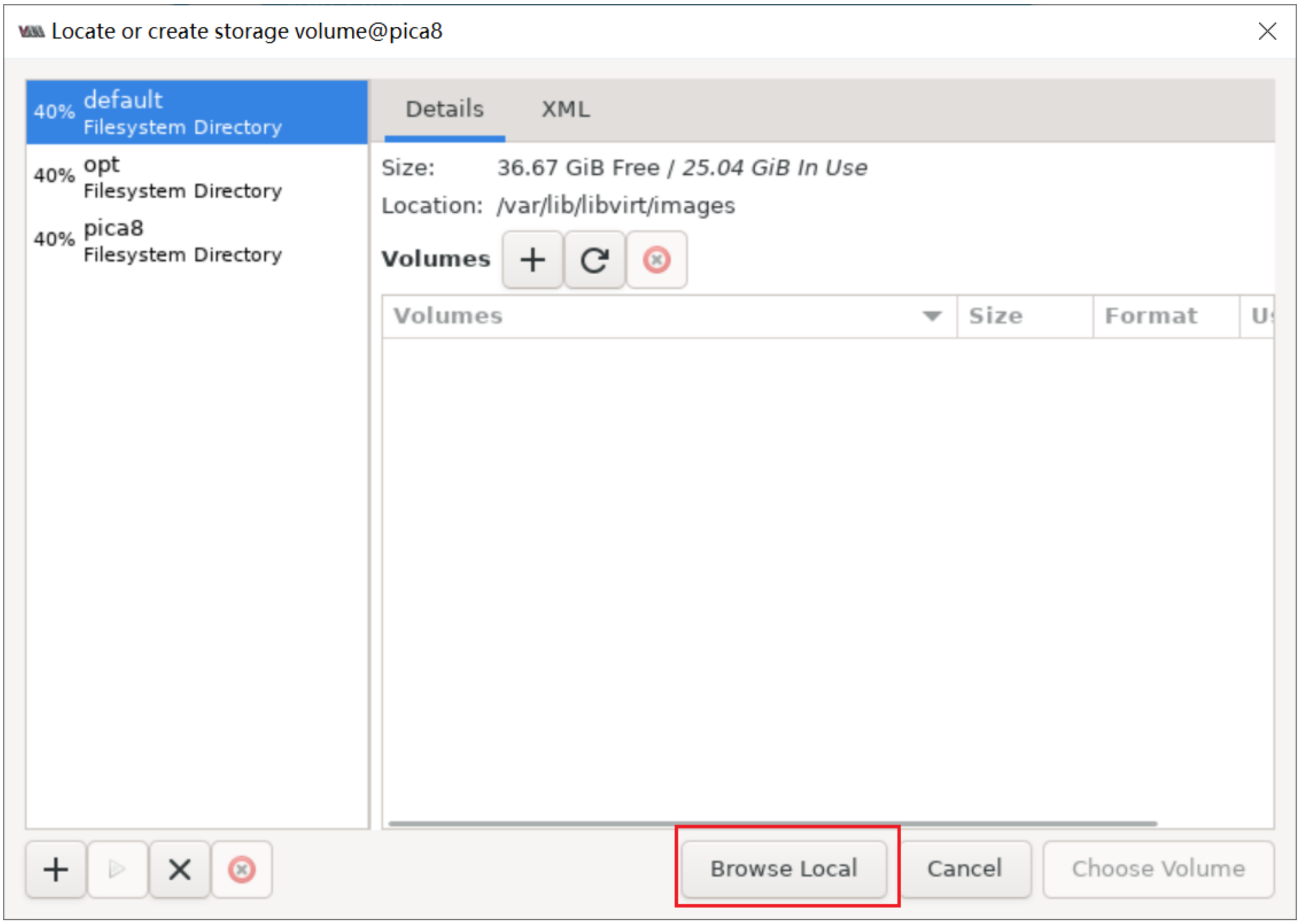


Select **Import existing disk image**, and then click **Forward**.

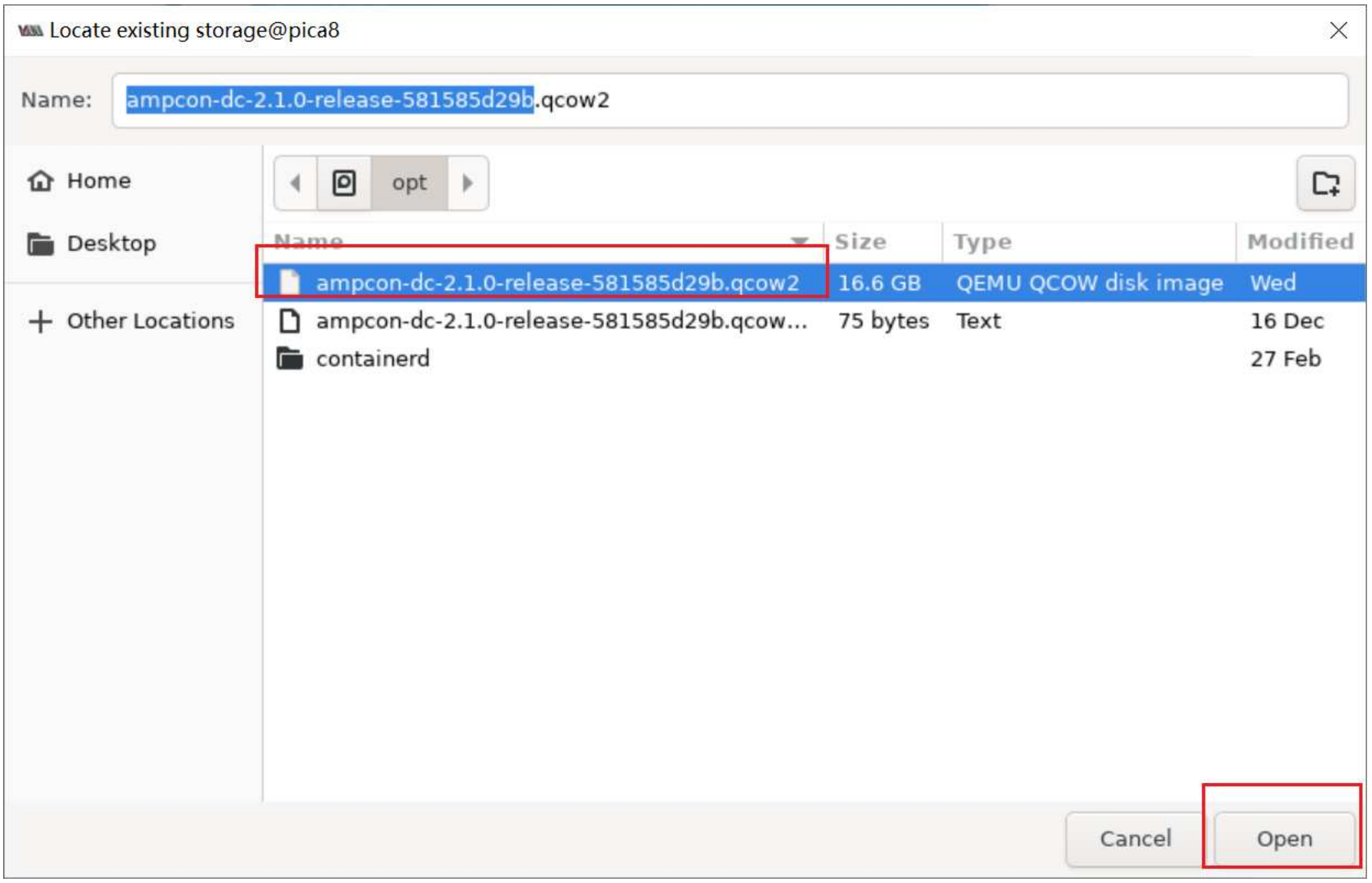
Click **Browse** to select the AmpCon-Campus server .qcow2 image file.



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

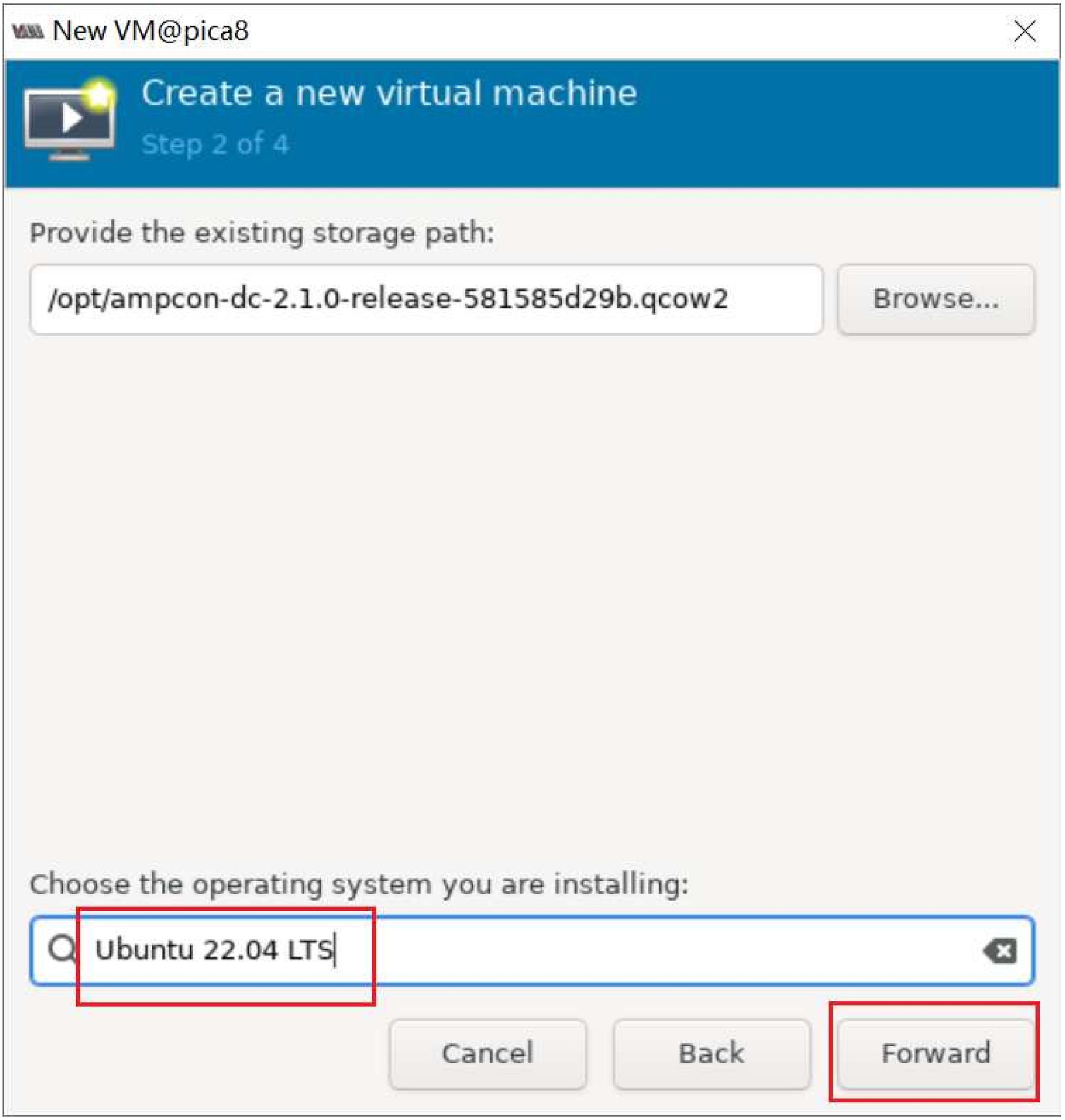


Find the location of the AmpCon-Campus server .qcow2 image file, and then click **Open**.



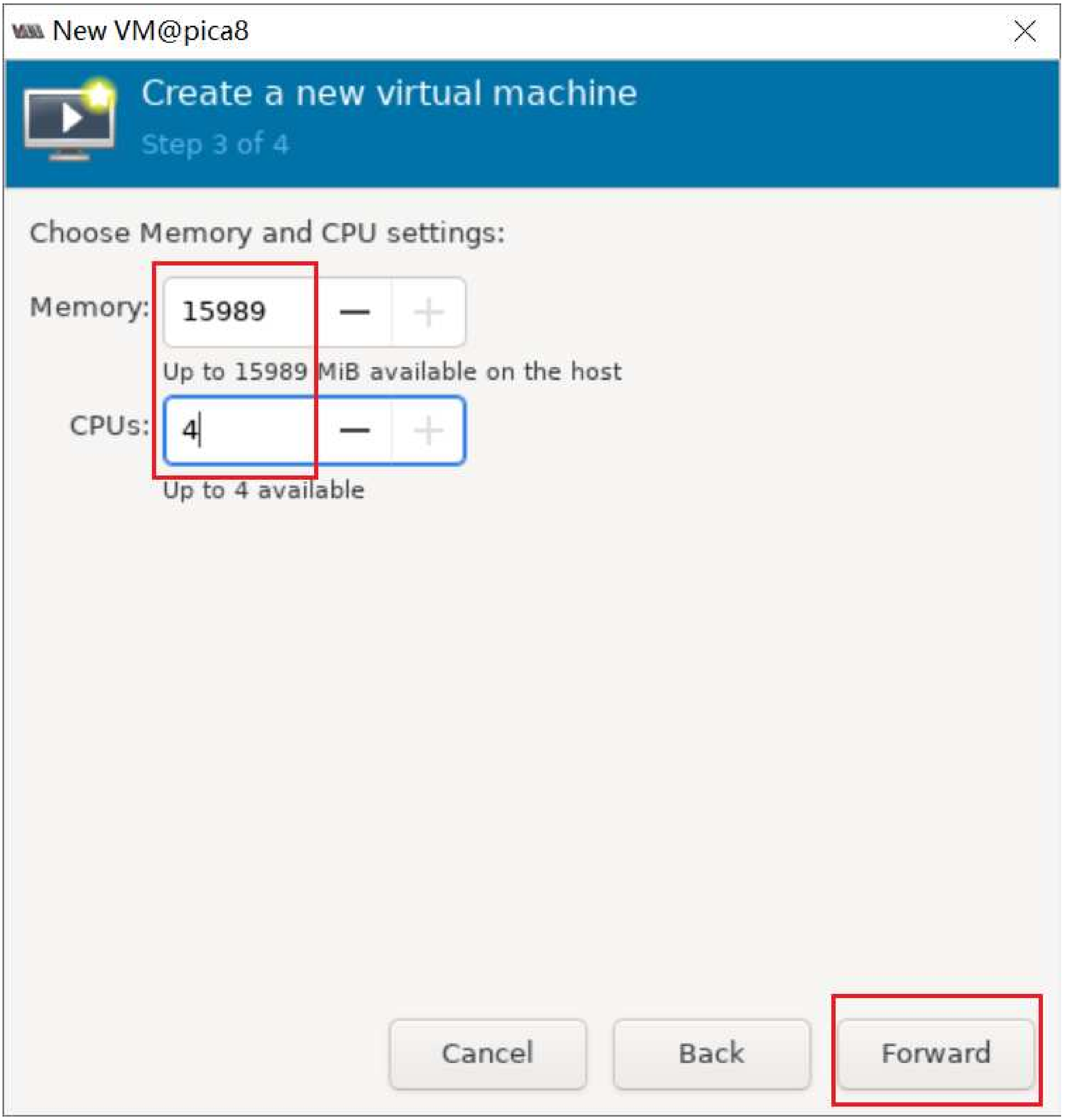
Select **Ubuntu 22.04 LTS**, and then click **Forward**.

> ⓘ **NOTE:** Do not select other operating systems because AmpCon-Campus supports only Ubuntu 22.04 currently.

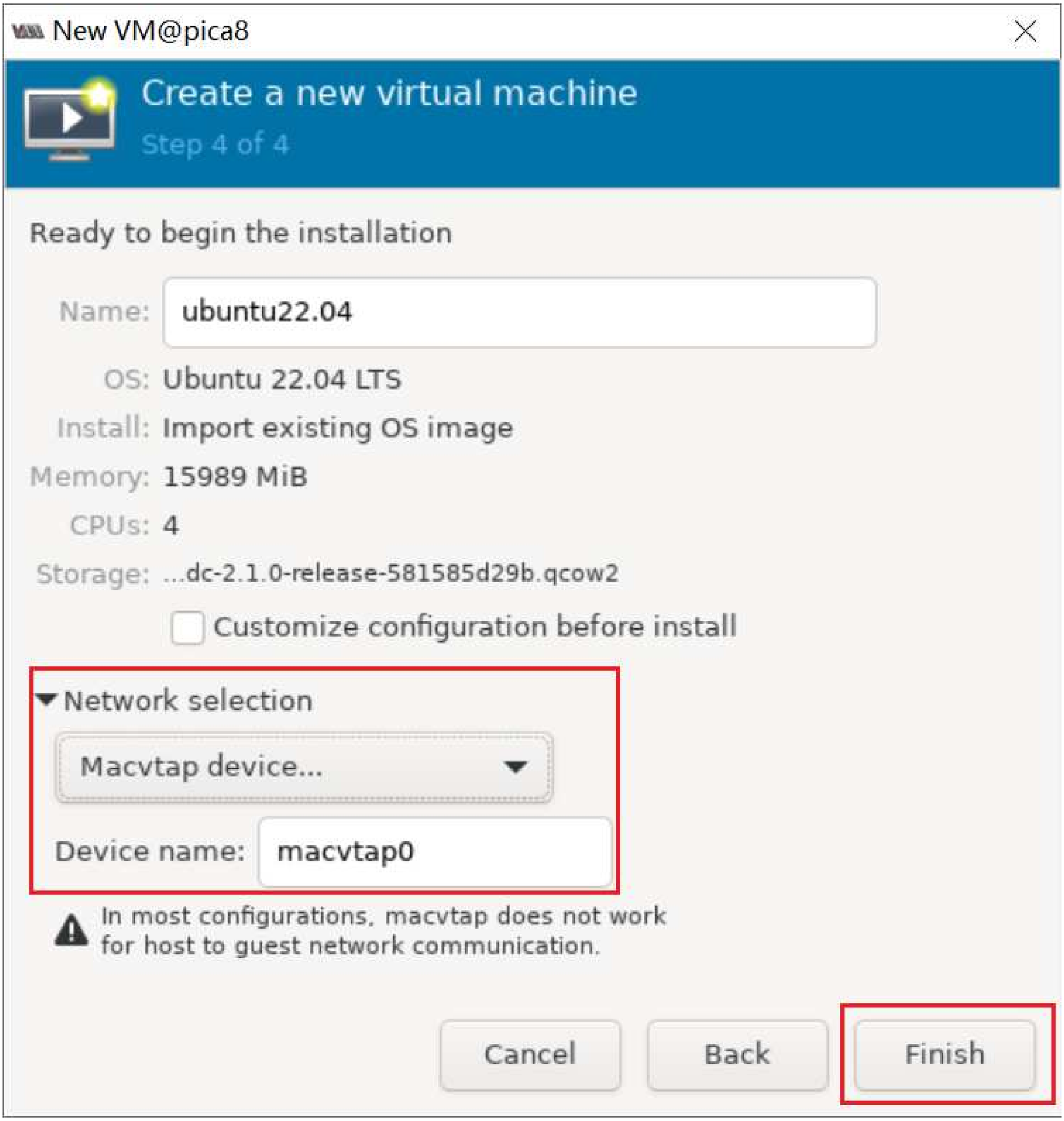


Adjust the memory and CPU settings as needed, and then click **Forward**.

> ⓘ **NOTE:** The memory and CPU settings need to meet the Server Requirements.

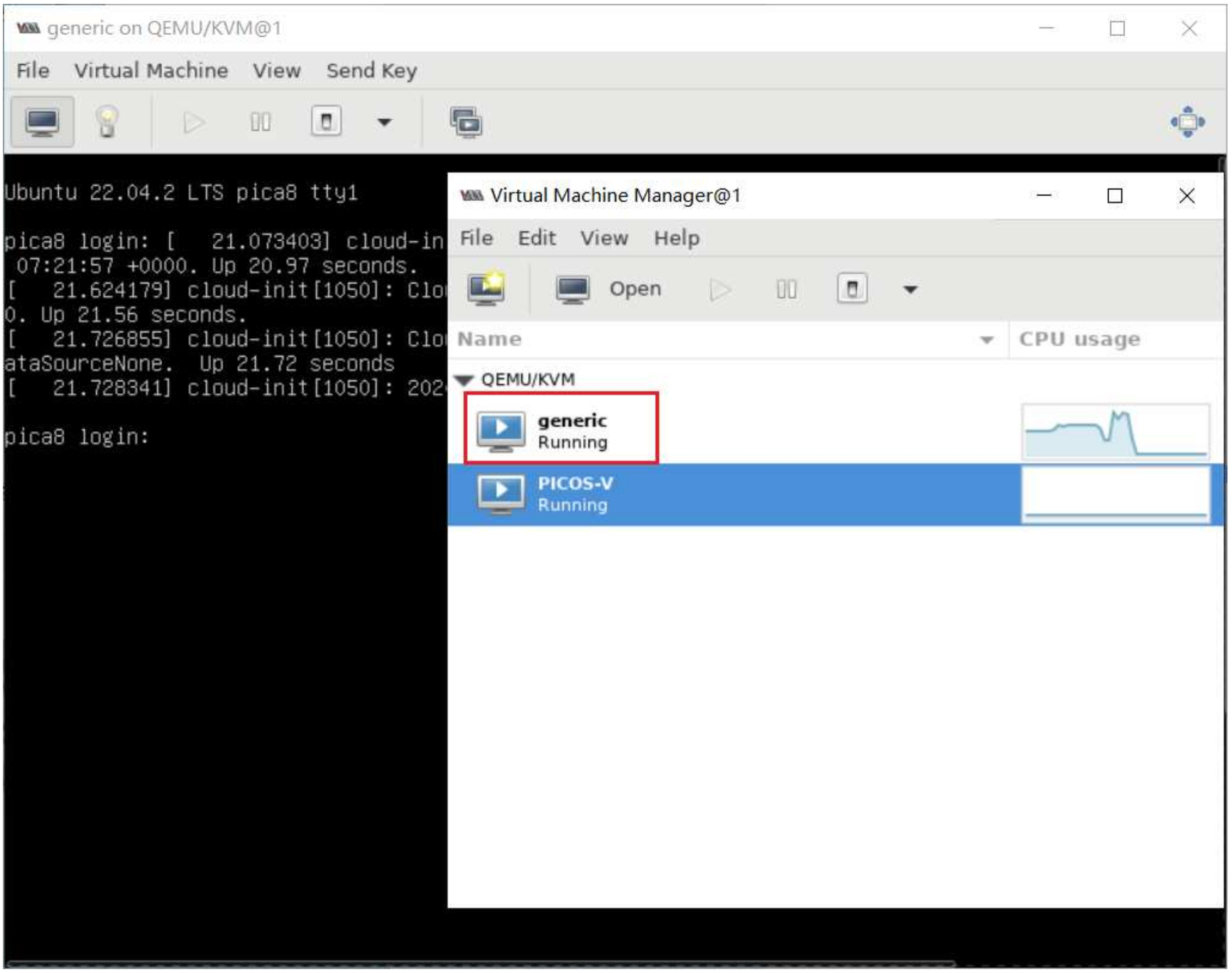


In the **Network selection** section, select **Macvtap device**, and enter the device name. Then, click **Finish**.



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.



Modify the network interface configuration.

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

b. Modify the IP address with the real IP address of the virtual machine.

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens3:
      addresses:
      - [redacted]0.190/24
      gateway4: [redacted].20.254
      nameservers:
        addresses:
        - [redacted].114.114
        search: []
  version: 2
```

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

```
sudo netplan apply
```

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.

After you install the AmpCon-Campus server, you need to add system configurations and import AmpCon-Campus Licenses.

Installing on Physical Machines (Ubuntu Docker)

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

- Ensure that the installation requirements are met.
- Prepare a physical machine based on Ubuntu 22.04 with Docker installed.
- Download the AmpCon-Campus server installation package by going to the FS AmpCon-Campus website and then clicking **AmpCon-Campus for Ubuntu Docker 2.2.x Software** in the **Resources** section.

Unzip the AmpCon-Campus server installation package by running the following command:

```
tar -zxvf
```

Replace with the name of the compressed AmpCon-Campus server installation package.

Modify the network interface configuration.

a. Modify the IP address with the real IP address of the physical machine.

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

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens3:
      addresses:
      - [redacted]20.190/24
      gateway4: [redacted]20.254
      nameservers:
        addresses:
        -[redacted].114.114
        search: []
  version: 2
```

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

```
sudo netplan apply
```

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

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

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

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.

After you install the AmpCon-Campus server, you need to add system configurations and import AmpCon-Campus Licenses.

Adding System Configurations

Before you deploy, configure, and manage switches with AmpCon-Campus, you must configure system configurations in the AmpCon-Campus UI.

System Configurations

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 the non-global system configuration if it is not needed.

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.
- The maximum backup number for the configuration snapshots. This configuration is not included in the non-global system configuration.
- The IP ranges of switches that are allowed for AmpCon-Campus management. This configuration is not included in the non-global system configuration.
- Whether to enable debug logs for server-side operations or not. This configuration is not included in the non-global system configuration.

Adding a Global System Configuration

The first time you log in to AmpCon-Campus, the global system configuration is blank. You must configure the global system configuration:

Log in to the AmpCon-Campus UI with the URL of the AmpCon-Campus server in the format of "https://.com/login" or "https:///login".

The default AmpCon-Campus UI username and password is admin/admin.

Click **Service** > **System Config** from the navigation bar.

On the “System Config” page, input the following information:

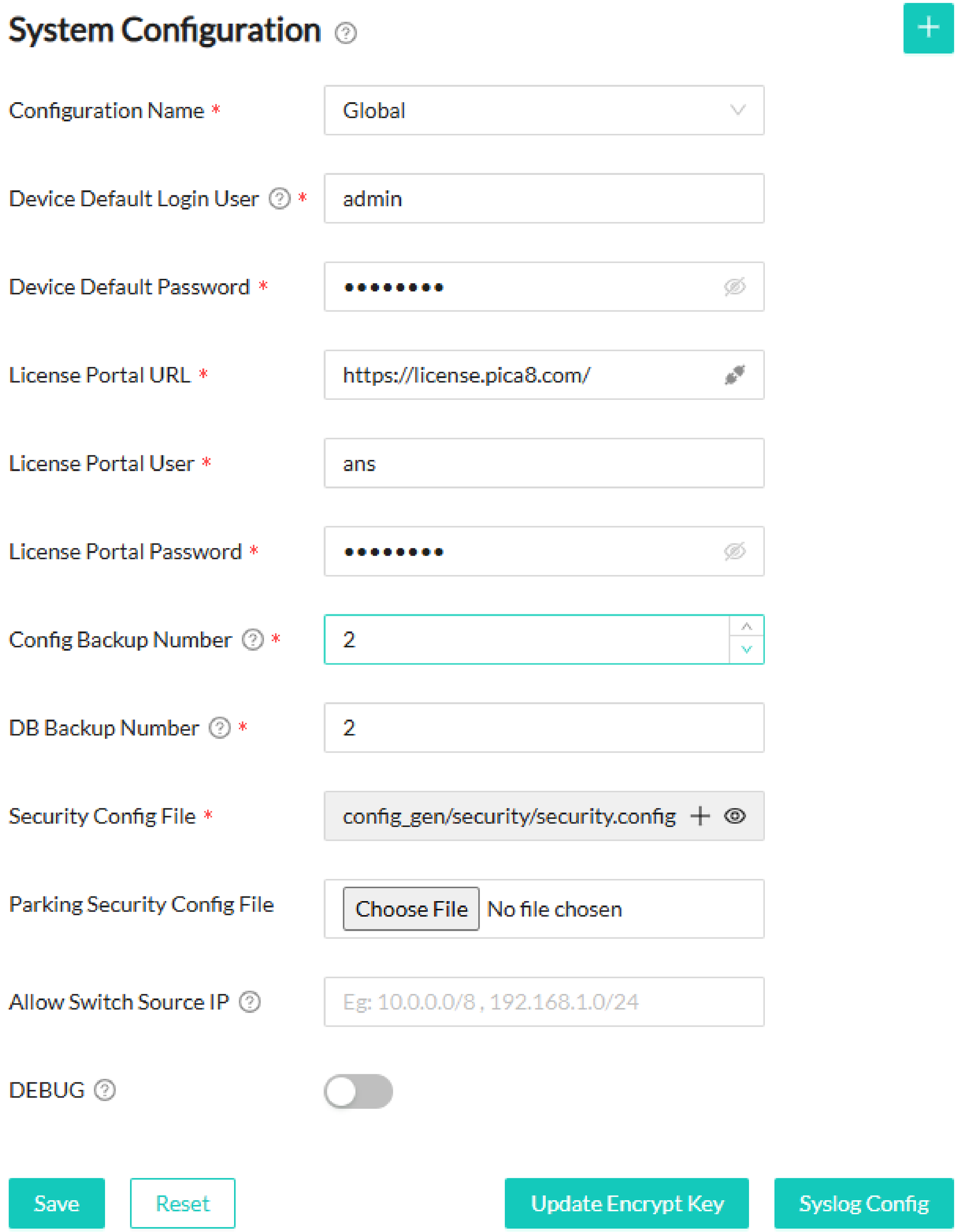
- **Configuration Name**: The name of the configuration.
- **Device Default Login User**: The default username of switches to be managed.
- **Device Default Password**: The default password of the default user.

ⓘ NOTEs

- 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.
- If the switches to be managed don’t share the same username and password in the global system configuration, create one or multiple non-global system configurations and apply system configurations to these switches based on the **Device Default Login User** and **Device Default Password** values.

- **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.
- **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. That is, configurations in Initial parking security config file will be pushed to switches that already registered to AmpCon-Campus but without generated configurations.
- **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.

Click **Save**.



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 switches.

Adding a Non-global System Configuration

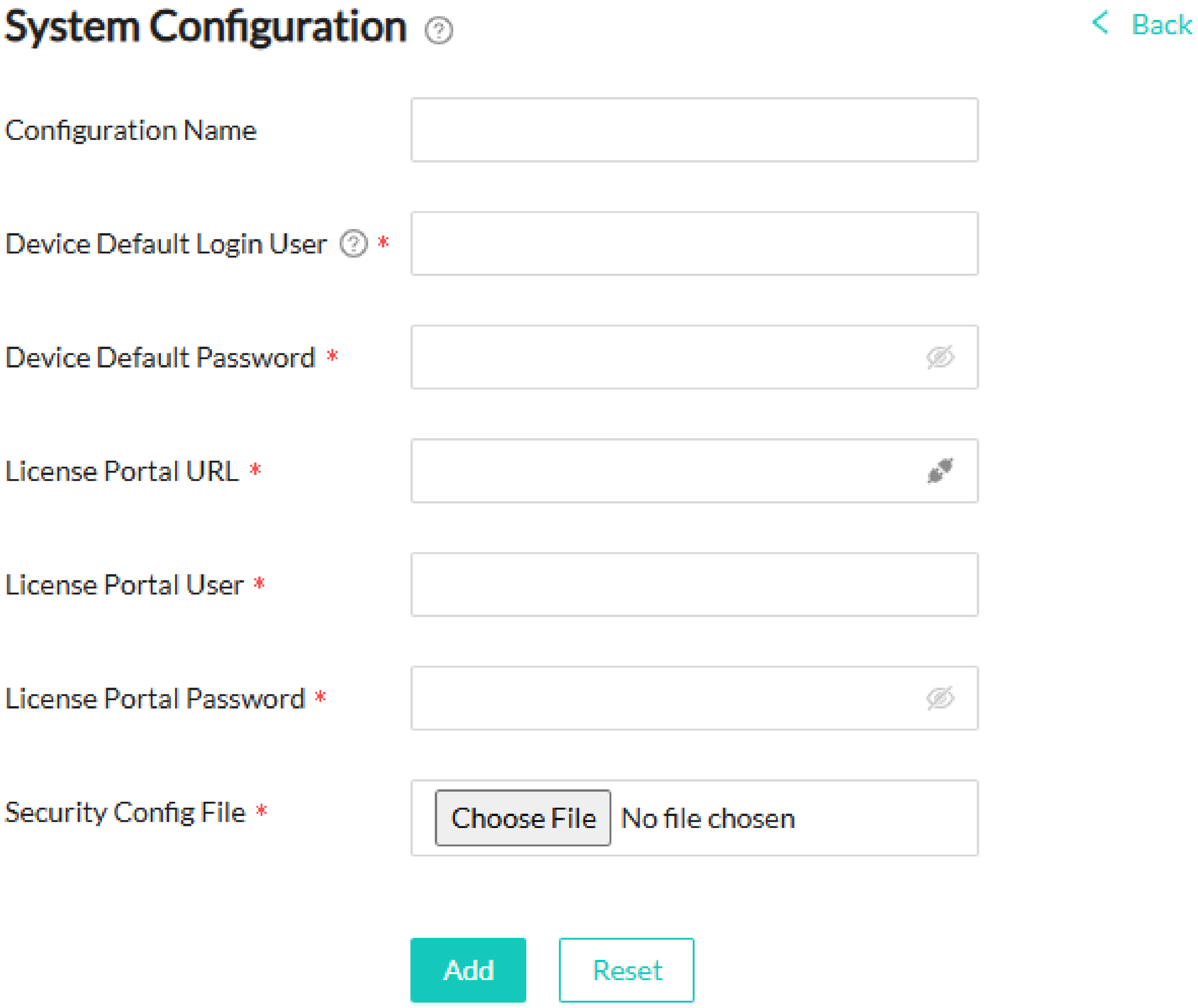
To add a non-global system configuration, follow these steps:

Log in to the AmpCon-Campus UI, and click **Service** > **System Config**.

Click the **+** icon. The “Add New System Config” page opens.

Input the following information：

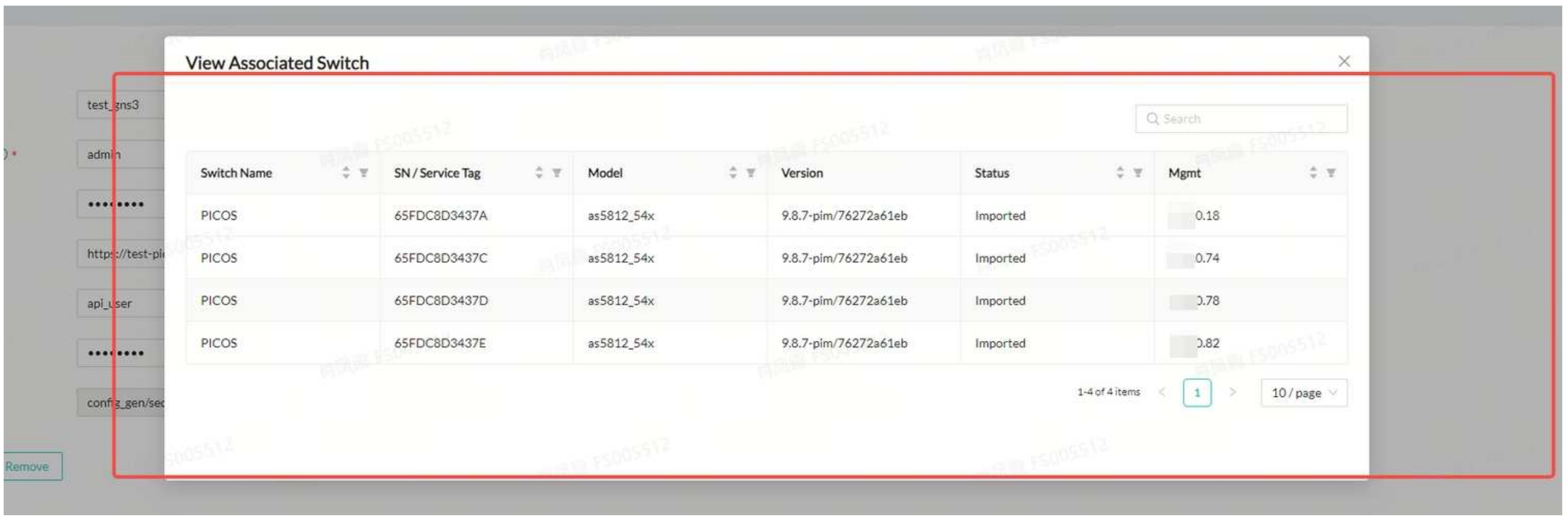
- **Configuration Name**: The name of the configuration.
- **Device Default Login User**: The default username of switches to be managed.
- **Device Default Password**: The default password of the default user.
- **License Portal URL**: https://license.pica8.com
- **License Portal User**: The user ID 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.



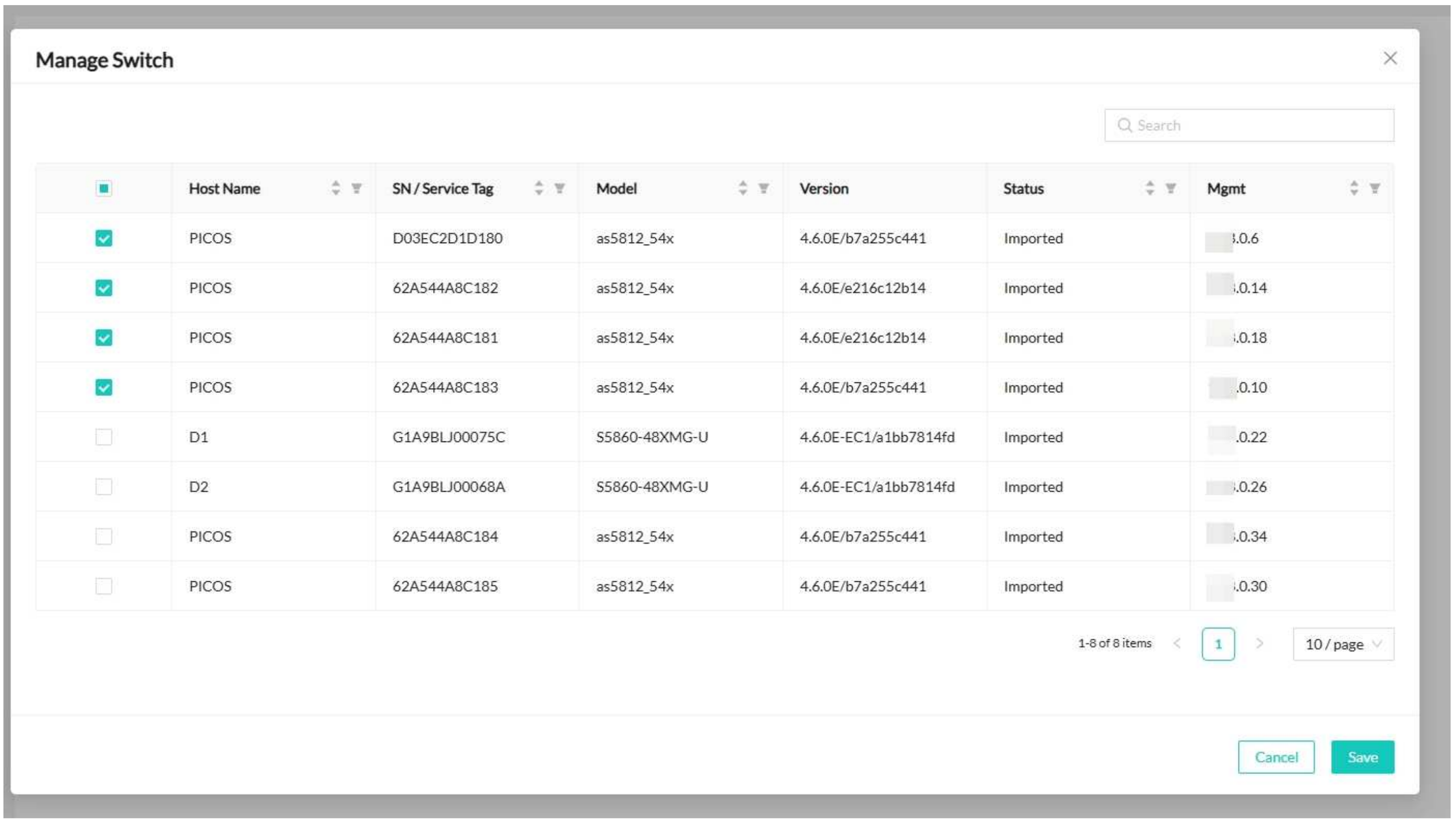
Click **Add**.

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** on the ”System Config” page.



- 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.

Importing AmpCon-Campus Licenses

AmpCon-Campus is the control center for all switch licensing. It tracks the current switch entitlement and allows the appropriate number of switches to be managed by AmpCon-Campus. AmpCon-Campus needs a valid license with active support to perform its functions.

The following license types are provided:

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

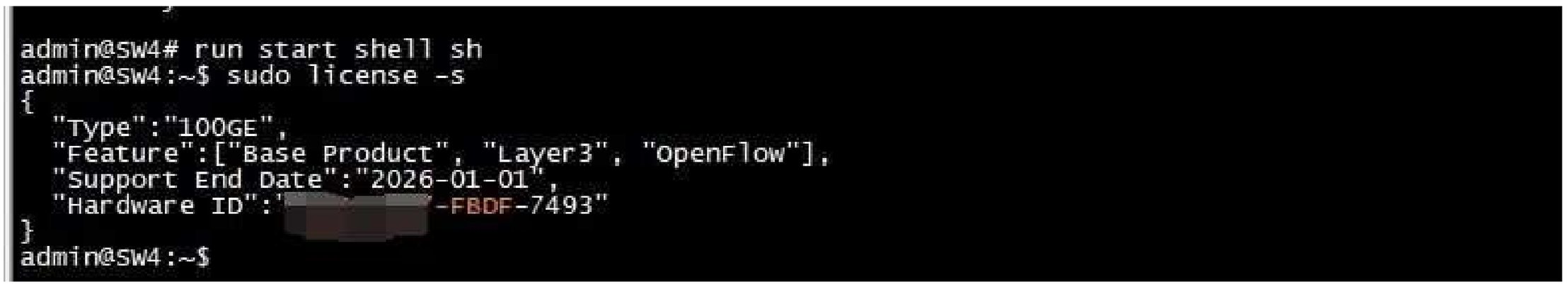
To manage switches with AmpCon-Campus, you need to add the Hardware IDs of the switches to an AmpCon-Campus license and then import the license to AmpCon-Campus.

Prerequisite

Obtain the Hardware ID of each switch that you want to manage by running the following commands in each switch:

```
run start shell sh
```

```
sudo license -s
```



Creating an AmpCon-Campus License

To create an AmpCon-Campus license, follow these steps:

Log in to the License Portal, and then click **AmpCon Licenses** > **New AmpCon License**.

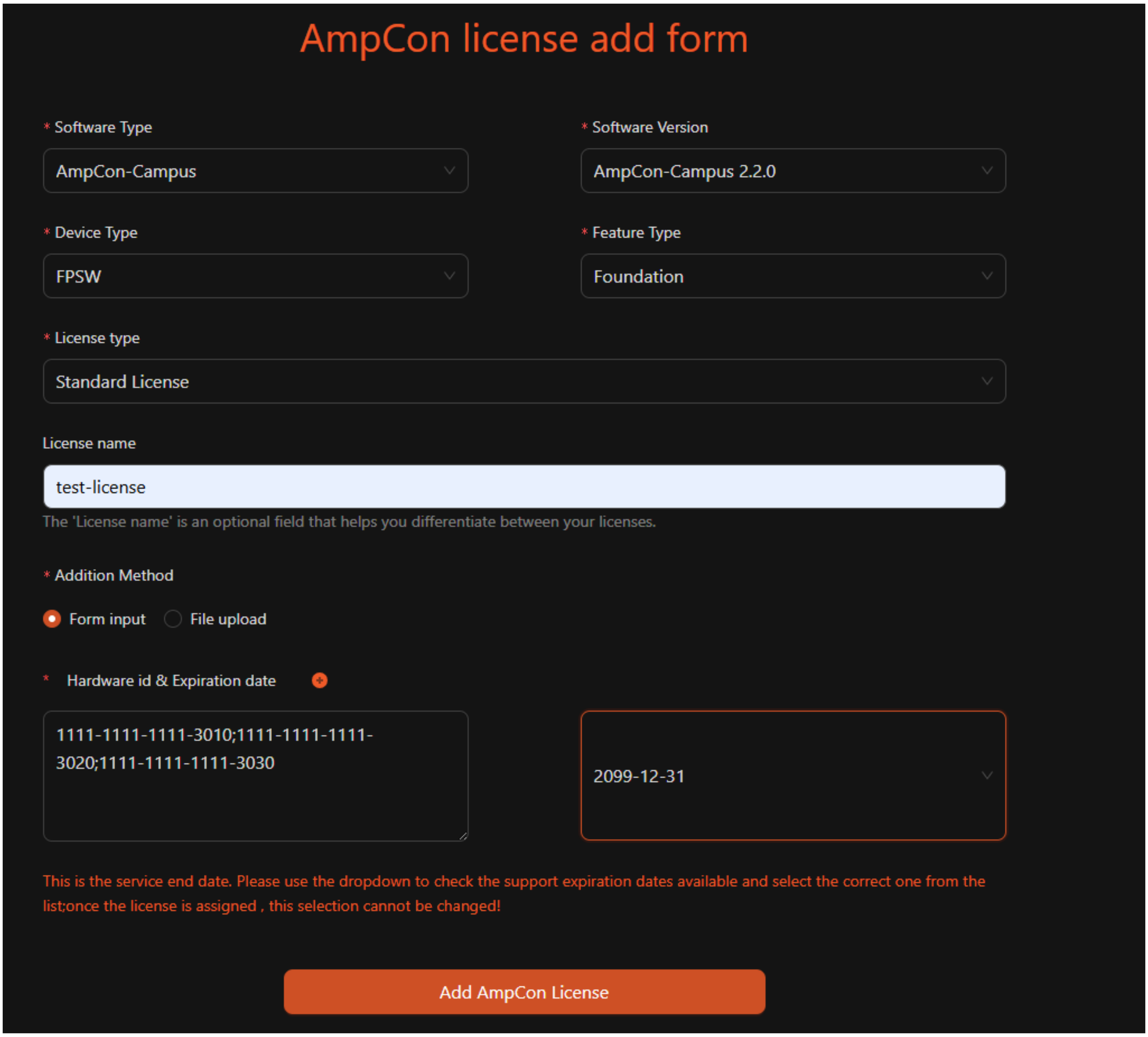
> ⓘ **NOTE**You can get the username and password of the License Portal from the sales team.

Input the following information:

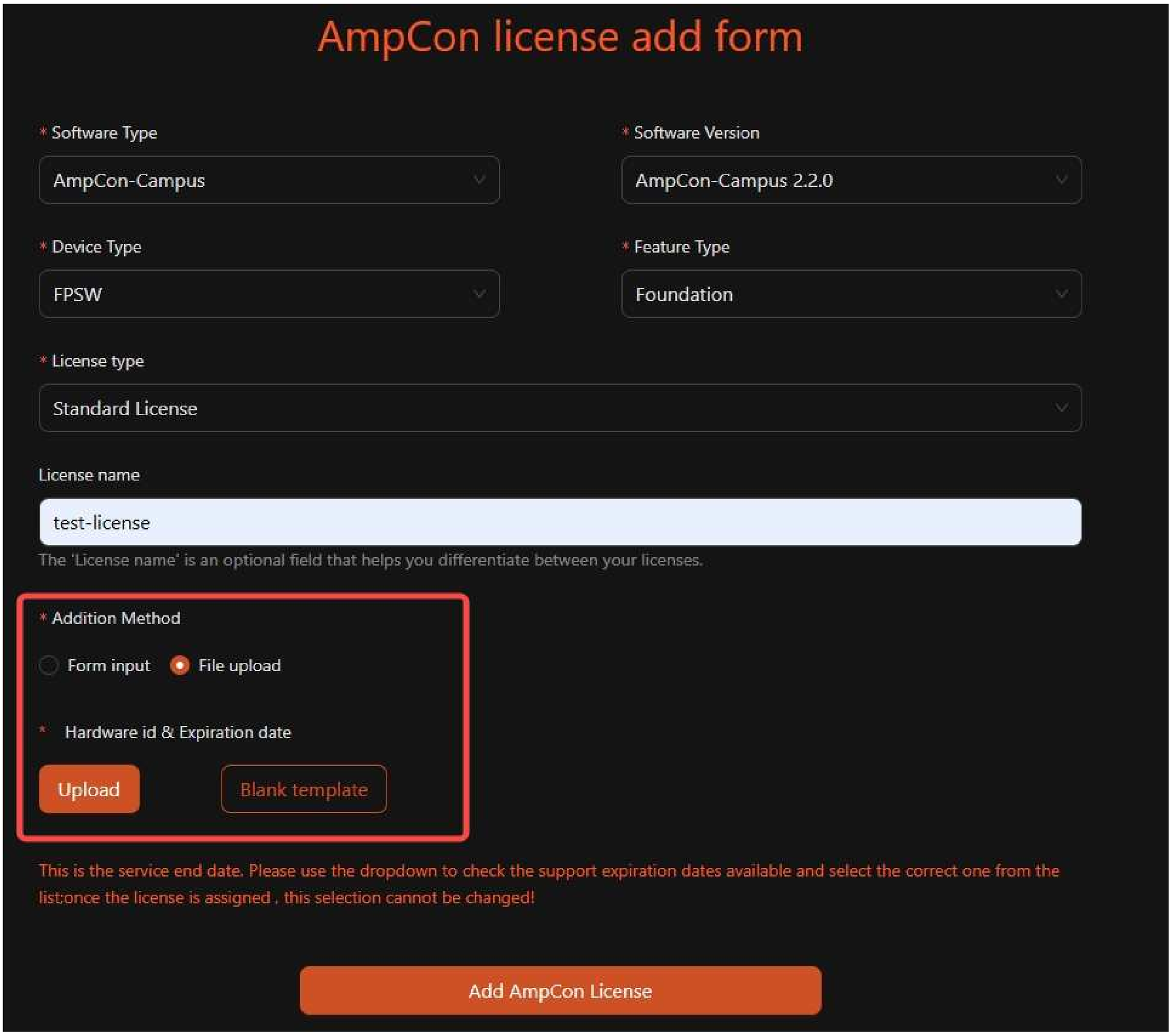
- **Software Type**: Select **Ampcon-Campus**.
- **Software Version**: Select **AmpCon-Campus 2.2.0**.
- **Device Type**: From the drop-down list, select a device type.
- **Feature Type**: Select **Foundation**. Currently, only the **Foundation** feature type is supported.
- **License Type**: Select **Trial License** or **Standard License**.
- **License Name**: The name of the license.

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.



- **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.



Click **Add AmpCon License**.

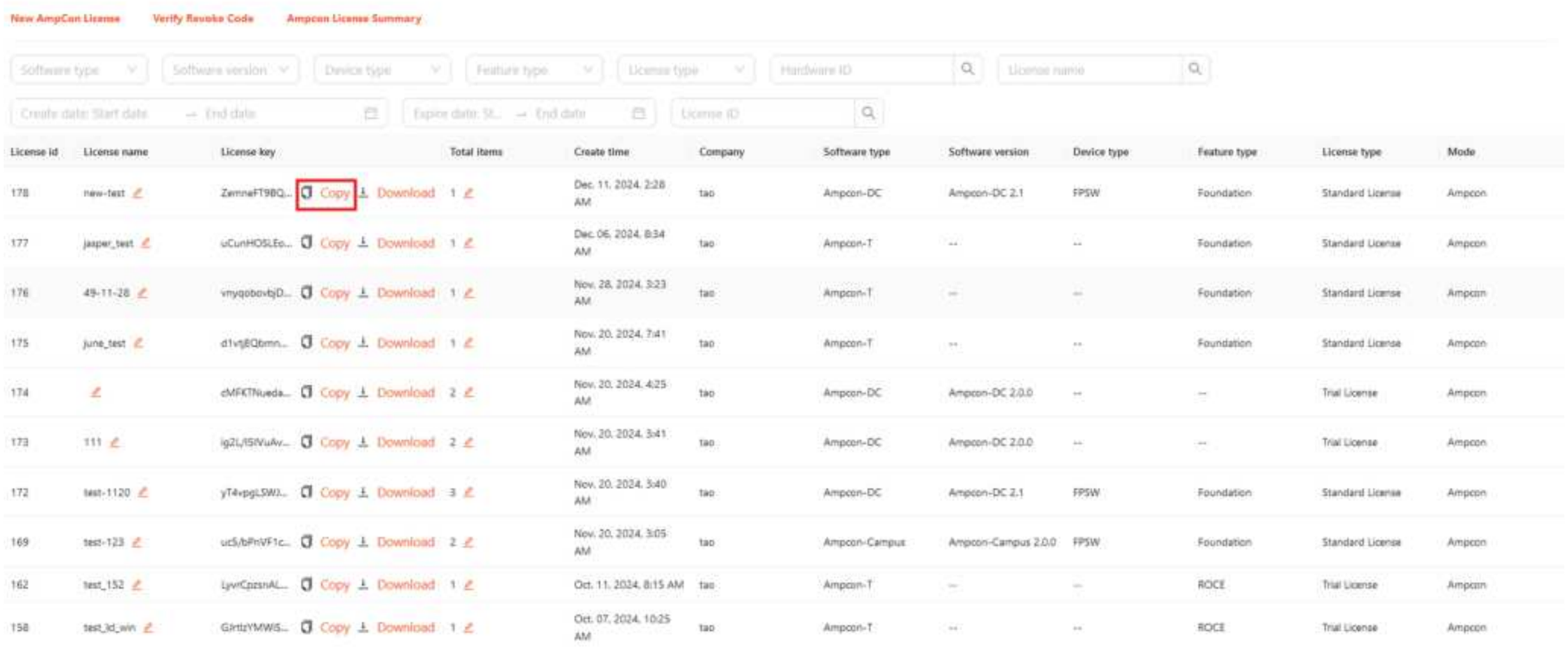
Importing an AmpCon-Campus License

To import an AmpCon-Campus license, follow these steps:

Get the updated or new license from the License Portal.

Log in to the License Portal, and then click **AmpCon Licenses**.

Click **Copy** to copy the license string or click **Download** to download the .lic license file.

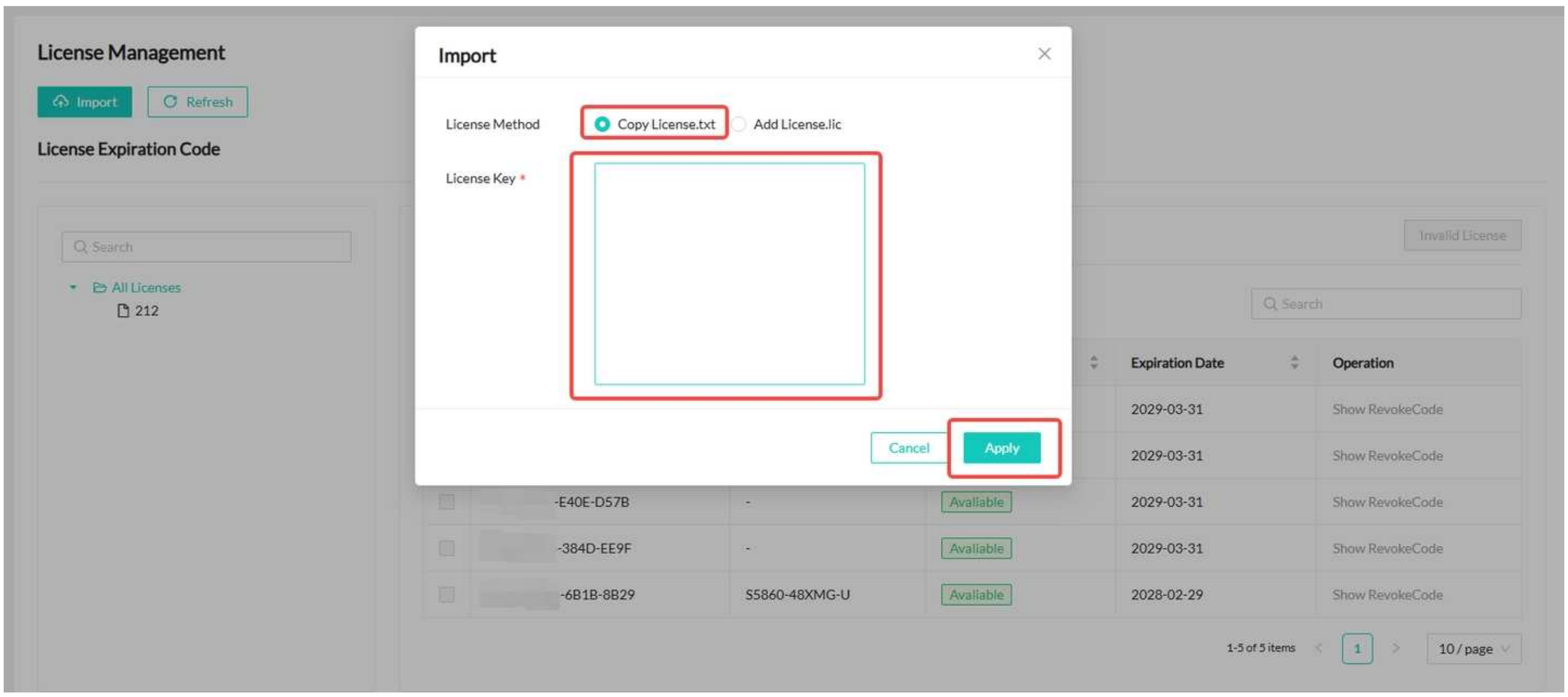


In the AmpCon-Campus UI, click **System > Software License > License Management** from the navigation bar.

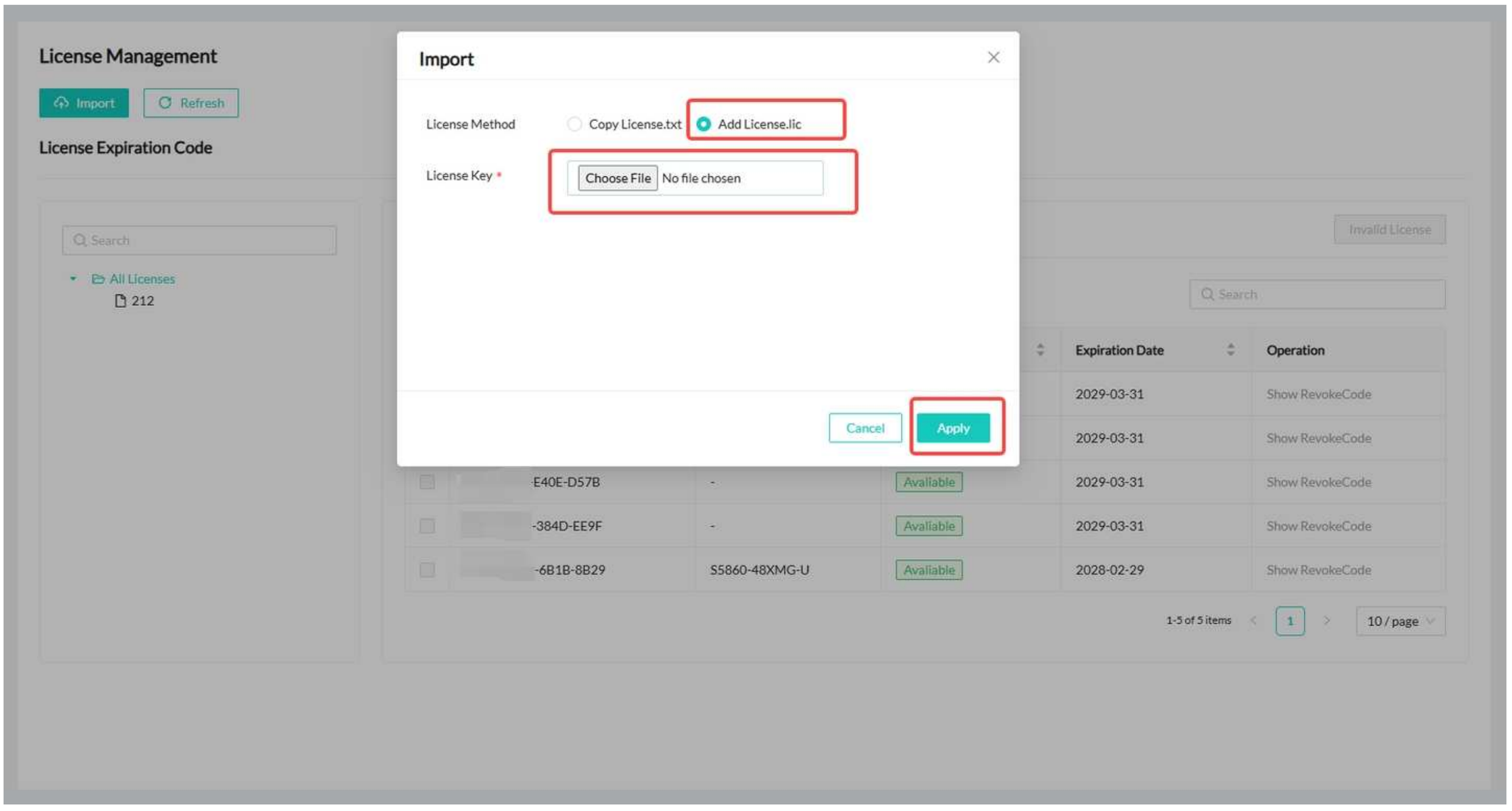
On the “License Management” page, click **Import**.

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.



Click **Apply**.

After you import the new license, the **All Licenses** table is refreshed.

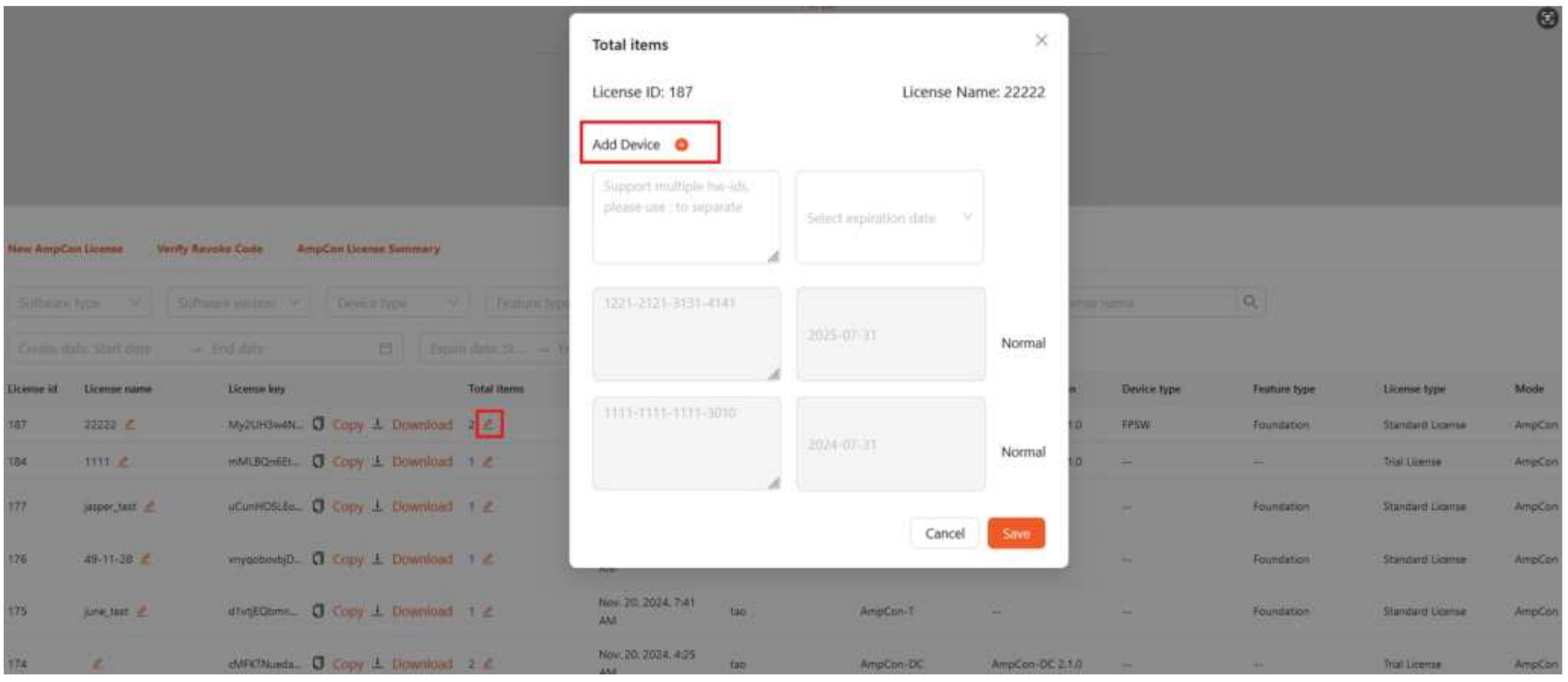
Optional: Editing an AmpCon-Campus License

After you create an AmpCon-Campus license, if you want to manage new switches with AmpCon-Campus, you can edit the license. Follow these steps:

Log in to the License Portal, and click **AmpCon Licenses**.

Locate the license that you want to edit, and click the edit icon in the **Total hw-ids** column.

Click the Add Device icon, enter the Hardware ID of each new switch that you want to manage, and select the expiration date.



Click **Save**.

> **NOTE**After you edit a license, import the updated license to AmpCon-Campus so that newly added switches can be managed by AmpCon-Campus. For more information, see Importing a License.

Upgrading the AmpCon-Campus Server

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

Procedure

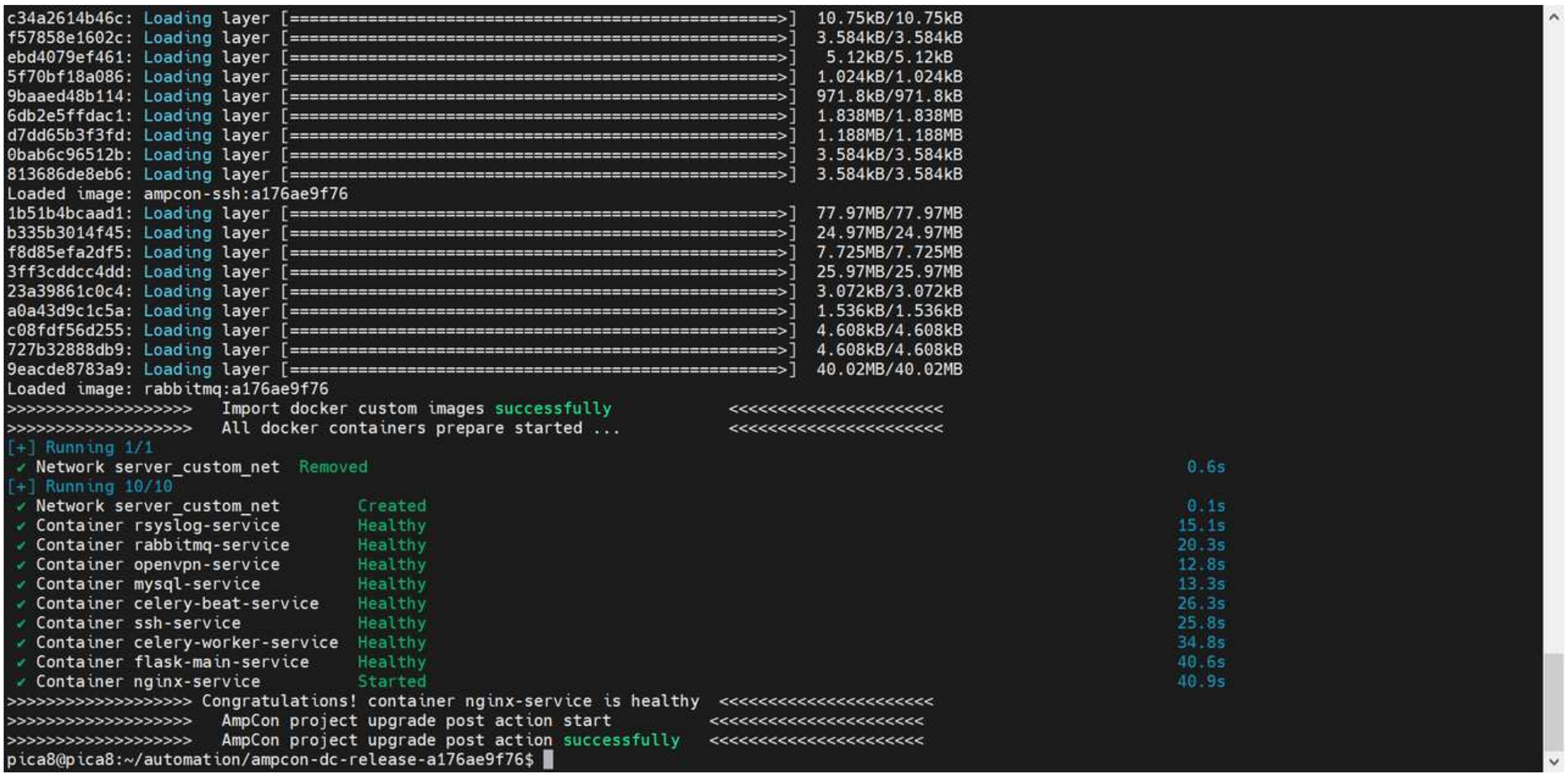
Download the new AmpCon-Campus server package from the FS website.

Go to the package directory, and run the following upgrade command:

```
sudo install_or_upgrade.sh
```

```
pica8@pica8:~/automation/ampcon-dc-release-a176ae9f76$ sudo ./install_or_upgrade.sh
>>>>>>>>>>>>>>>>>>> AmpCon project /usr/share/automation/server dir already exists, ready to upgrade     <<<<<<<<<<<<<<<<<<<<
<
e3b287efea45
d71d504c4246
61fd6c4243de
d48200740c1c
2d4be7cfb51a
371333d52cfc
8ad421c010f4
00d599689a78
f26ab79470f5
Untagged: ampcon-nginx:a176ae9f76
Deleted: sha256:4d48ec1f437c0ea5c305abbbde51c468bc2a2fe47ae261811ae34a8d13ceb093
Deleted: sha256:34b88254152158746a3974c46ac5b10bae0b72053ec0eb9d6a7f3634349223f8
Deleted: sha256:4e384544996e6b4ac348b975092642f9bb3160d9bd0dd180bf0b3aab3d61803c
Deleted: sha256:05b9c373a5059d7fe40e4af32db375f67fa0a7d6ee521a97ce49634f62704b36
Deleted: sha256:7d6854caa04cb169ea4c109ee01a9c4f24be1b7c3ab51ca530204c900e1725a4
Deleted: sha256:569225b98d5ed33c96a8e1a7f75747fa47847a359e30196008415fcbc3e62eaf
Deleted: sha256:5cb2a2a33f650d9481ed899a2c81dd20bdc284715cf905663aea281598b57bdd
Deleted: sha256:bf10bb318a4231fc808cbea0d378c3eafe1f2a245e4c32705c11ca28f66aebca
Deleted: sha256:9e50d14a0d7a41df98f36d31f9b9fa2086cd50768626465f160e08eb6c13c927
Deleted: sha256:14dfb5ada66aeea72ebea2df75f0d1d37e36b53d8cd810e27600bc2497811227
Deleted: sha256:c6cca6b860639299dcb4bba8ba074624e390001c65e6c5eaee37c9c5d089e730
Deleted: sha256:ff7064fa96621d2e10cd89ba2ce18271f5930a2f65e9e60795fa344956c2774c
Untagged: ampcon-main:a176ae9f76
Deleted: sha256:8aa61b8d2c4f52544ec0adf3f931d743e8db37c0c9bc2214bc6e54865093ad88
Deleted: sha256:2c2c212e2e95d7c9c1832d500ff4bd21516a232ed3ffc69ef55cf521d42c2eda
Deleted: sha256:01e573c4ecf6c026a4b21feba6c6ca8431f6c6071fb01f0d097455499b209b39
Deleted: sha256:cf18c8cae9138bb6aa4d5deaf7571e41cfcf337085aefc05e5036101a403d32f
Deleted: sha256:cbe7a9f34f5e0188eec16066f155cf6a743224809874879291c4339b38c78f6d
Deleted: sha256:218440e14f4bba0418b6543b8ca7f61d4f2fe8caa995ee4fe2cabaaebff6f106
Deleted: sha256:59edc750d53f6f675769dc61d41b9998aa9a9f7df6e94f95a52e1681eca46d34
```

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



Log in to the AmpCon-Campus UI to see whether the server is upgraded to the new version.

Uninstalling the AmpCon-Campus Server

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

Procedure

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
```

Clear the files in the server directory with sudo privileges:

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

Administering AmpCon-Campus

You can administer AmpCon-Campus by using the user interface. For more information, see the following child topics:

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

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.

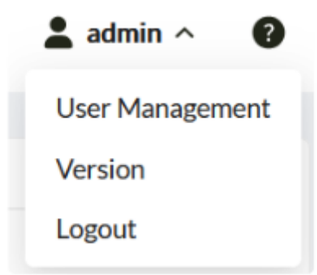
AmpCon-Campus supports the following user roles. The permission levels are as follows: SuperAdmin > Admin > Operator > Readonly.

- **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
- **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
- **Readonly**
  - Views limited pages such as Dashboard, Switch, Topology, Config Files View, and Alarms
  - Provides access to CLI Configuration, Template Verify, and Config Snapshot Diff

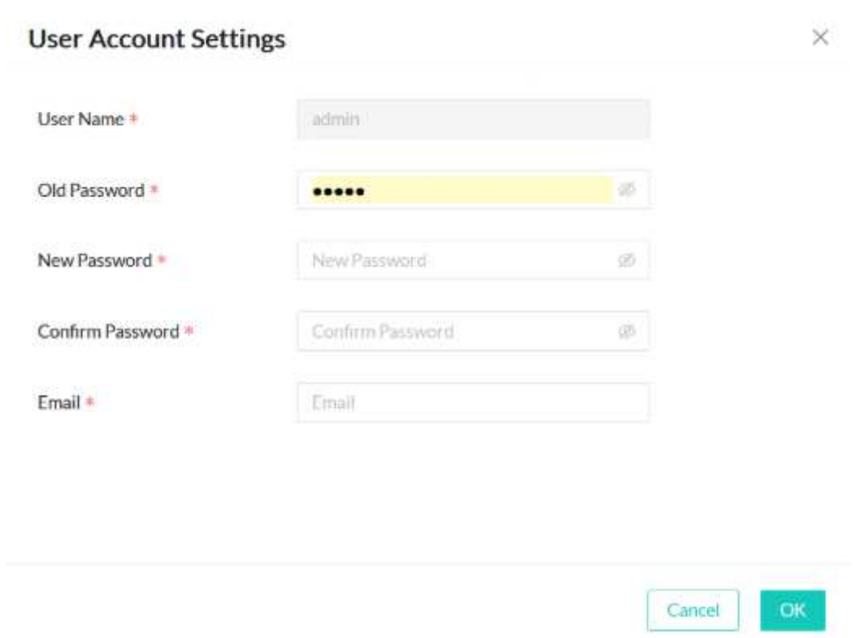
User Self-Management

All AmpCon-Campus users can change their own passwords and email addresses. Follow these steps:

In the AmpCon-Campus UI, click the username, and then click **User Management**.



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.



To change the email address associated with the AmpCon-Campus user, enter a new email address in the **Email** field.

Managing All Added Users

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 is a member of a specific group. A global user means that the user is not limited to a group.

To add a user, follow these steps:

Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.

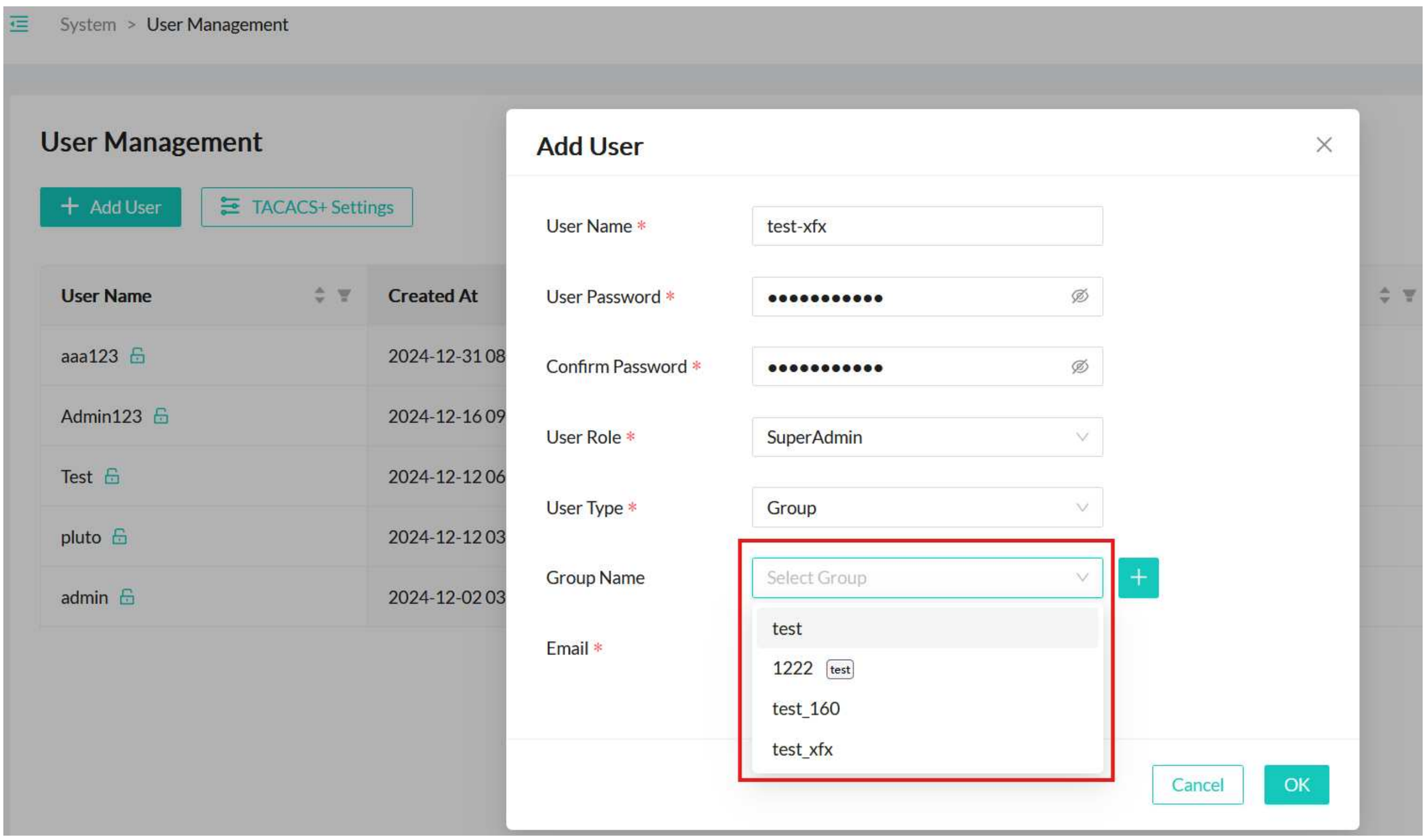
Click **System** > **User management** from the navigation bar.

Click **Add User**, and enter the following information:

- **User Name**: The username.
- **User Password**: 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**: The password of the user.
- **User Role**: SuperAdmin, Admin, Operator, or Readonly.
- **User Type**: Global or Group.
- **Email**: The email of the user.

If you select **Group** as the user type, select a group name from the **Group Name** drop-down list.

To assign the user to a new group that hasn't been created, create a group as described in Managing Groups.



Click **OK.**

To edit an added user, follow these steps:

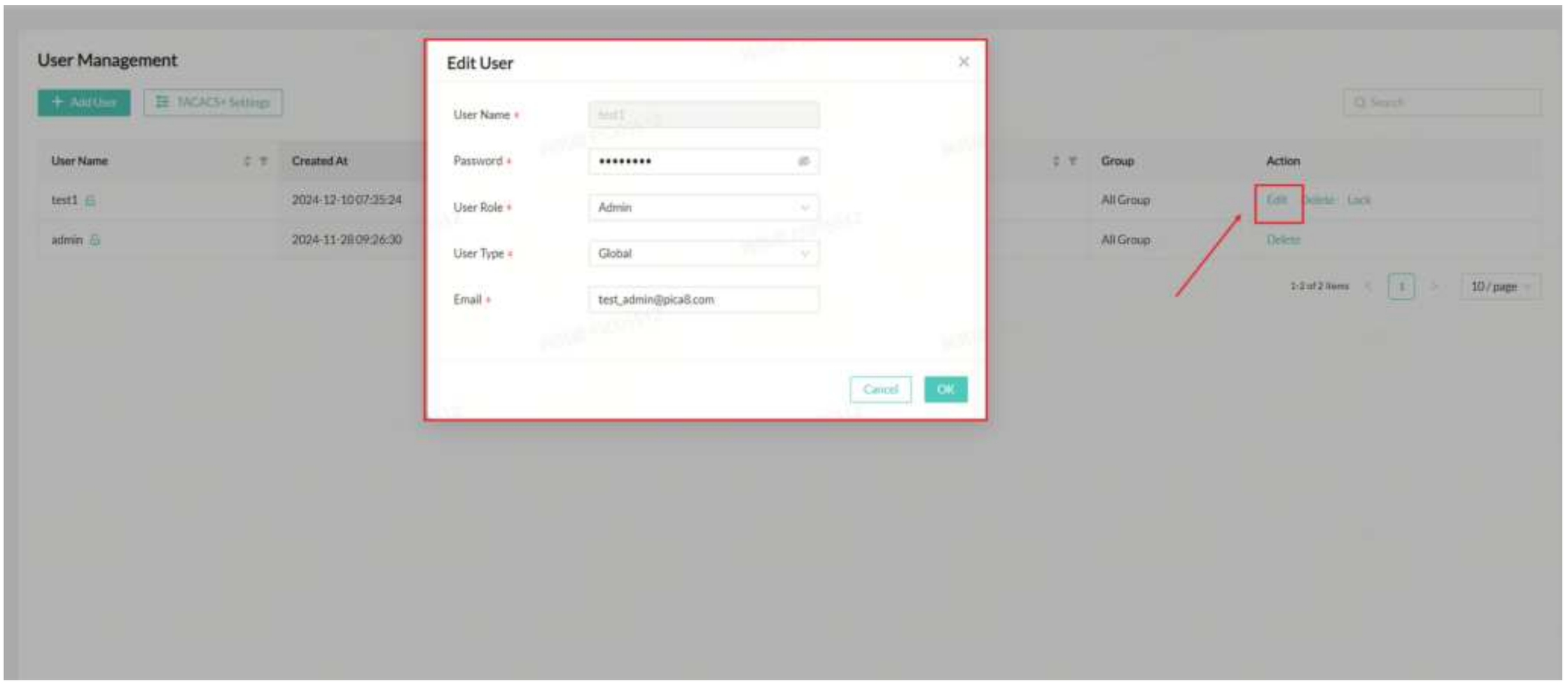
Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.

Click **System** > **User management** from the navigation bar.

On the "User Management" page, locate a user, and then click **Edit**.

> ⓘ **NOTE**The built-in user **admin** can't be edited here.

Modify user information as needed.



Click **OK**.

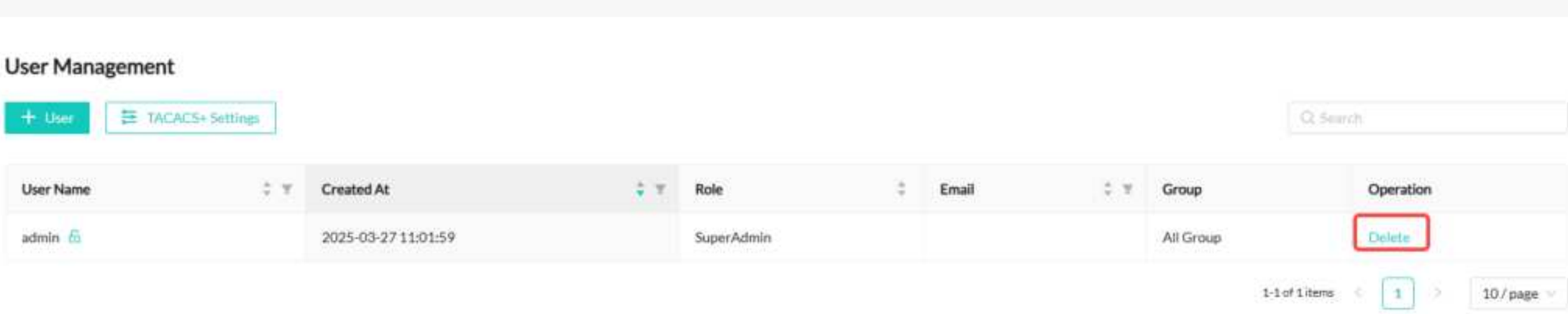
To delete an added AmpCon-Campus user, follow these steps:

Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.

Click **System > User management** from the navigation bar.

On the ”User Management” page, locate a user, and then click **Delete**.

> ⓘ **NOTE**The built-in user **admin** can’ t be deleted.



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

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:

Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.

Click **System > User management** from the navigation bar.

On the ”User Management” page, locate a user, and then click **Lock**.

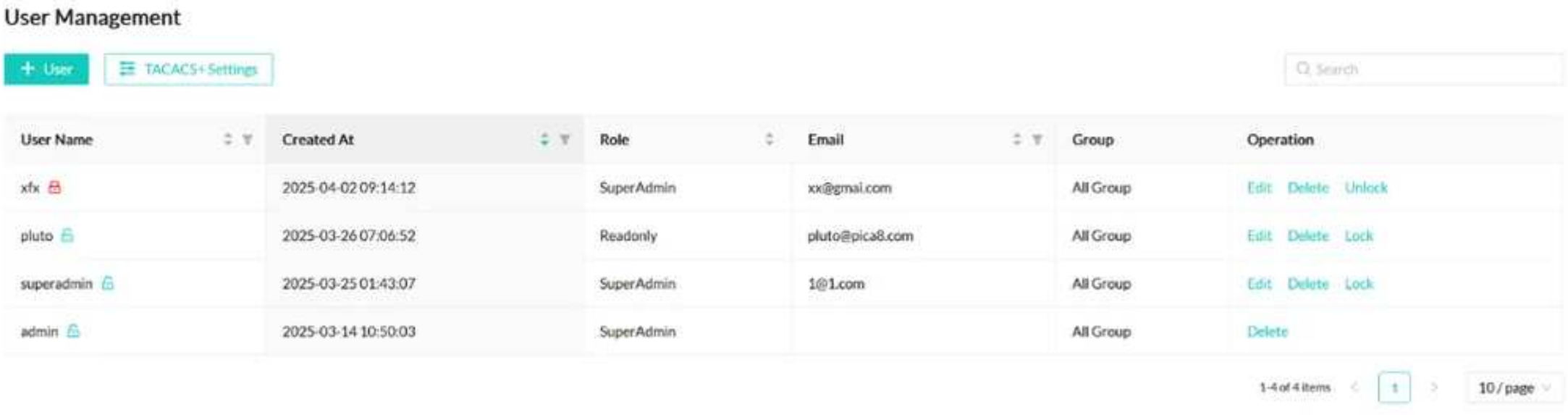
In the pop-up window, click **Yes** to confirm the lock operation.

- To unlock an added user, follow these steps:

Log in to the AmpCon-Campus UI with a user of the **SuperAdmin** role.

Click **System > User management** from the navigation bar.

On the ”User Management” page, locate the locked user, and then click **Unlock**.



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 in the AmpCon-Campus UI, different user roles have different permissions. See the following table:

Table 1. Menu Permissions

Configuring TACACS+ Authentication and Authorization

AmpCon-Campus supports integrating with the 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 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.

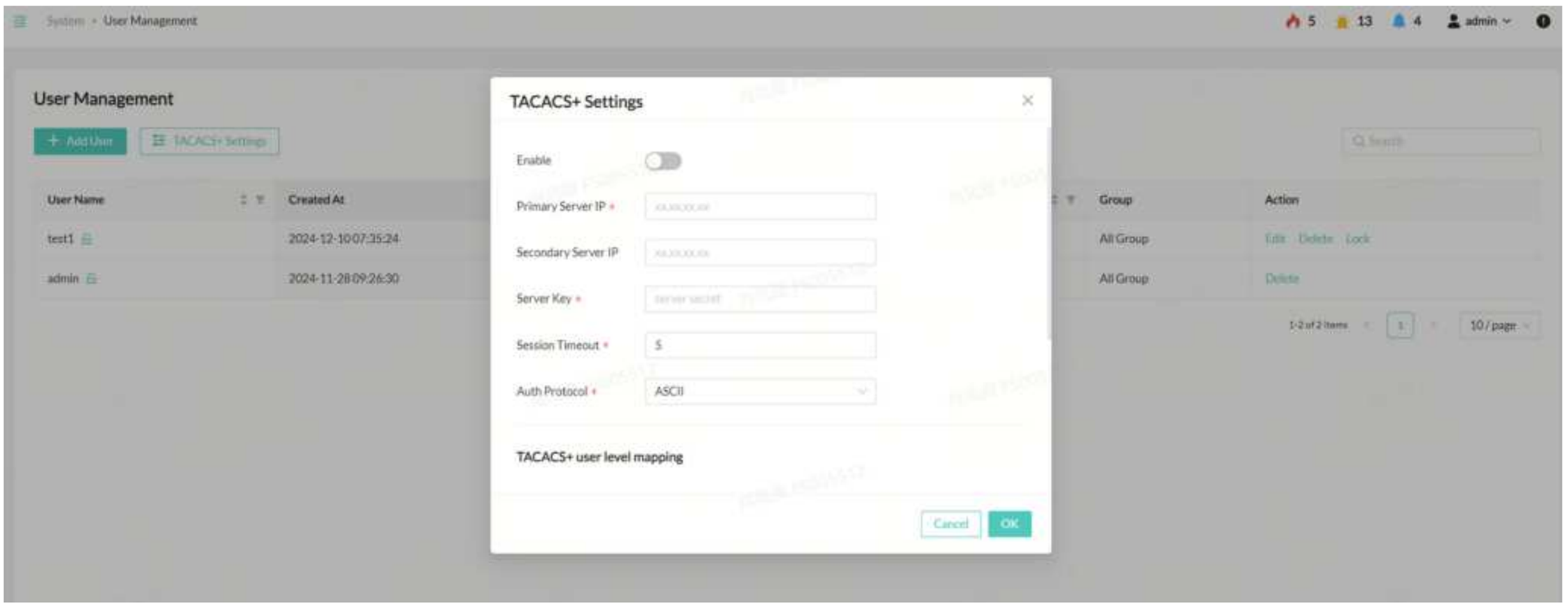
- AmpCon-Campus sends authorization requests with **“Arg[0]” service=AmpCon-Campus**. On the TACACS+ server, you need to set the value of the parameter **“service=AmpCon-Campus”** to process authorization requests of AmpCon-Campus users.
- If both the primary and the secondary TACACS+ servers are unreachable, you can use local users (global user or group user) to log in to the AmpCon-Campus UI.

To enable the TACACS+ integration, follow these steps:

In the AmpCon-Campus UI, click **System > User management**.

Click **TACACS+ Settings**.

Click **Enable** to activate the TACACS+ service. The **TACACS+ Settings** pop-up window is displayed.



Enter the following information:

Parameter	Description
Enable	Enable or disable 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 to15. 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.

Click **OK**.

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
 }
}
```

Updating the Encrypt Key for Sensitive Data Encryption

After you deploy AmpCon-Campus, a default encrypt key is generated to encrypt sensitive data in the AmpCon-Campus database. In this way, plain text like password and sensitive TACACS+ keys is not shown in the AmpCon-Campus UI. You can update the encrypt key as you need.

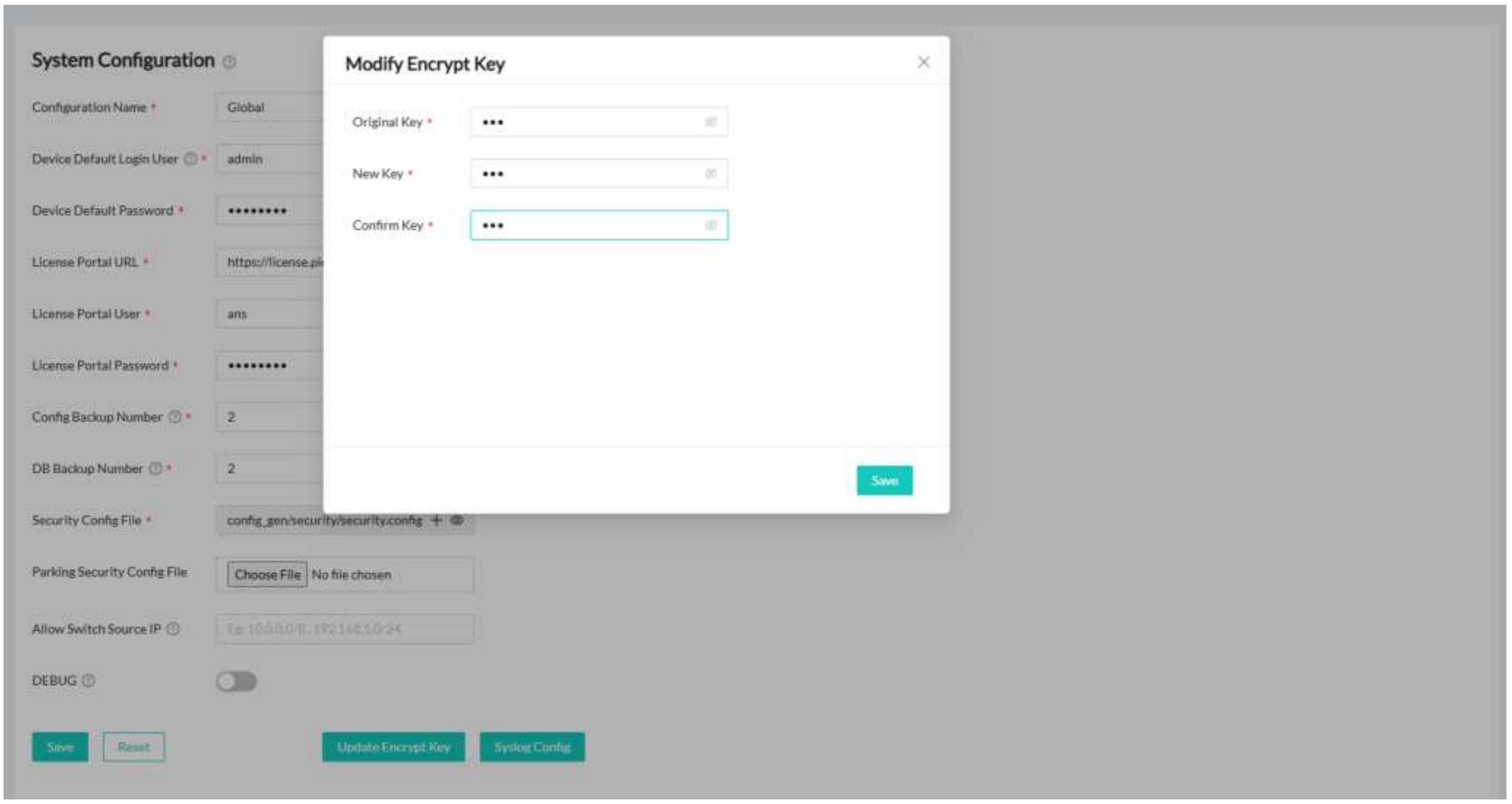
Procedure

To update the encrypt key, follow these steps:

Log in to the AmpCon-Campus UI, and click **Service** > **System Config**.

On the “Global System Config” page, click **Update Encrypt Key**.

Enter the original key and the new key. The default encrypt key is pica8pica8



Click **Save**.

Configuring External Syslog Servers

You can forward AmpCon-Campus logs to other external Syslog servers.

Prerequisite

Ensure that the Syslog service of the target server is enabled.

Procedure

To update the encrypt key, follow these steps:

Log in to the AmpCon-Campus UI, and click **Service > System Config**.

On the “Global System Config” page, click **Syslog Config.**

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.

Shenzhen（China）

Address：Room 1903-1904, Block C, China Resources Tower, Dachong Community, Yuehai Subdistrict, Nanshan District
Email：sales@feisu.com
Tel：+86(400)865 2852

Shanghai（China）

Address：Unit 1201, Lee Gardens Shanghai Office Tower, No. 668 Xinzha Road, Jing'an District
Email：sales@feisu.com
Tel：+86(400)865 2852

Wuhan（China）

Address：Building A1-A4, Chuangxin Tiandi, No. 88 Guanggu Sixth Road, Hongshan District
Email：sales@feisu.com
Tel：+86(400)865 2852