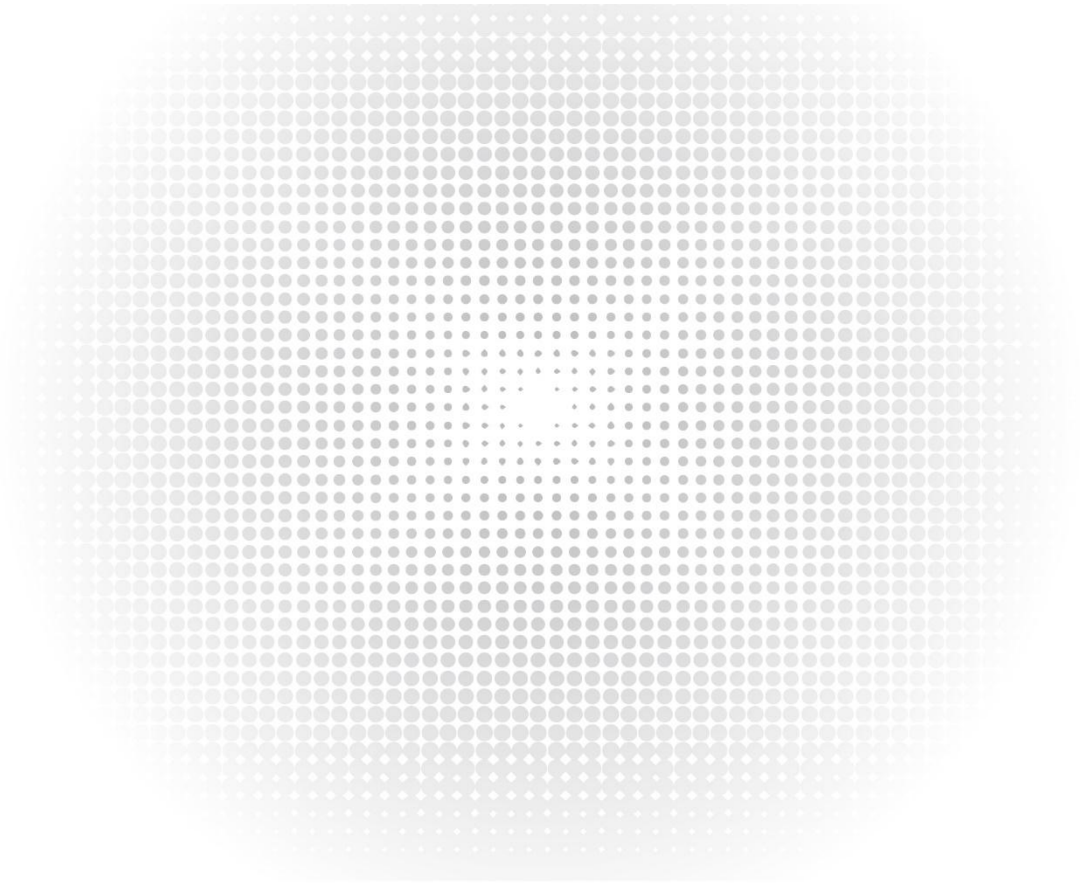
AmpCon-DC Management Platform

User Guide V2.5

Models: LIS-AMPCON-DC-FPSW-Foundation-1Y, LIS-AMPCON-DC-FPSW-Foundation-3Y,
LIS-AMPCON-DC-FPSW-Foundation-5Y



AmpCon-DC Management Platform 2.5 User Guide . . . 6
Release Notes . . . 8
AmpCon-DC 2.5.0 Release Notes . . . 9
AmpCon-DC 2.5.1 Release Notes . . . 12
Overview . . . 13
Quick Start . . . 27
Platform Installation Workflow . . . 28
PicOS Switch Onboarding Workflow . . . 35
PicOS Switch Configuration Workflow . . . 42
Physical Network Deployment Workflow . . . 48
Logical Network Deployment Workflow . . . 55
Ansible Automation Workflow . . . 63
Planning . . . 67
Supported Information . . . 68
Supported Switches for 2.5.0 . . . 70
Supported Switches for 2.5.1 . . . 78
Installation Requirements . . . 88
Deploying AmpCon-DC . . . 91
Installing the AmpCon-DC Server . . . 92
Installing on VMware ESXi . . . 94
Installing on QEMU or KVM . . . 100
Installing on VirtualBox for Lab Only . . . 106
Installing on Physical Machines (Ubuntu Docker) . . . 112
Multi-NIC Deployment for Switch Connectivity . . . 115
Troubleshooting for Server IP Changes . . . 117
Upgrading the AmpCon-DC Server . . . 119
Uninstalling the AmpCon-DC Server . . . 121
Working with the User Interface . . . 122
UI Conventions . . . 127
Onboarding Switches . . . 134
Importing Switches . . . 136
Deploying Switches through Normal ZTP . . . 141
How Normal ZTP Works . . . 142
Quick Deployment Guide for Normal ZTP . . . 145
Preparing Configurations . . . 150
Configuring Global Configurations . . . 151
Adding Switch Configurations . . . 155
Managing Global and Switch Configurations . . . 162
Configuring Switch Models . . . 164
Adding System Configurations . . . 166
Configuring a DHCP Server . . . 178
Provisioning Switches through Normal ZTP . . . 180
Deploying Physical and Logical Networks . . . 187
Network Architecture . . . 190
Configuring Resources . . . 195

Resource Pools . . . 196
IP Pools . . . 197
ASN Pools . . . 201
VNI Pools . . . 205
Resource Interconnections . . . 210
Point of Delivery . . . 211
vSphere PoD . . . 212
OpenStack PoD . . . 220
Bare Metal PoD . . . 229
Managing VPCs . . . 235
VLAN Domains . . . 245
Node Uplink . . . 251
Key Concepts for Node Uplink . . . 252
Configuring Node Uplink for Bare Metal Nodes . . . 254
Managing Node Templates . . . 265
Managing Bare Metal Node Groups . . . 270
Configuring Node Uplink for Cloud Platform Nodes . . . 279
Managing Node Uplink Configurations . . . 288
Node Uplink Scenarios in AI . . . 295
Single-Rail Access Scenarios . . . 296
Multi-Rail Access Scenarios . . . 301
Designing Physical Networks . . . 306
Physical Network Overview . . . 307
Key Concepts . . . 309
Recommended Switches for 2.5.0 . . . 313
Recommended Switches for 2.5.1 . . . 315
Quick Design Guide . . . 318
Designing Units . . . 319
Designing DC Templates . . . 323
Designing Fabrics . . . 330
Managing Fabrics . . . 340
Simplified ZTP Deployment . . . 352
Quick Deployment Guide for Simplified ZTP . . . 353
Preparing for Simplified ZTP . . . 354
Deploying through Simplified ZTP . . . 360
Post-Deployment Operations . . . 388
Troubleshooting Simplified ZTP . . . 392
Provisioning Overlay Services . . . 398
Logical Network Overview . . . 399
Deploying Logical Networks . . . 403
Creating Bare Metal VL2s . . . 417
Viewing and Managing VL2s . . . 423
Managing Logical Network Elements . . . 429
Managing Logical Networks . . . 430
Managing Logical Switches . . . 443

Managing Logical Routers . . . 450
Troubleshooting Guide . . . 458
Managing Third-Party Devices . . . 462
Adding Devices . . . 463
Managing Added Devices . . . 469
RoCE on NICs . . . 475
Supported NICs . . . 476
RoCE Overview . . . 482
Configuring RoCE . . . 484
Checking RoCE . . . 492
Verifying RoCE Configurations . . . 494
Configuring Lossless Networks . . . 496
Key Features of RoCE . . . 499
Configuring RoCE EasyDeploy and Easy ECN . . . 505
Configuring RoCE Policies . . . 514
Configuring Dynamic Load Balancing . . . 534
Managing Switches . . . 537
Viewing Managed Switches . . . 538
Uploading and Upgrading PicOS Images . . . 545
Uploading and Pushing Images . . . 546
Upgrading PicOS on Switches . . . 550
Managing the Parking Lot . . . 553
Returning Merchandise Authorization for Switches . . . 555
Decommissioning Switches . . . 561
Removing Switches . . . 562
Configuring Switches . . . 563
Adding Configuration Templates . . . 564
Pushing Configurations to Switches . . . 567
Managing Configuration Templates . . . 572
Managing Configuration Nodes . . . 576
Comparing Running Configurations with Initial Configurations . . . 578
Comparing Running or Backup Configurations . . . 581
Backing Up and Restoring Configurations . . . 583
Running Ansible Playbooks for Automation . . . 589
Examples for Ansible Playbooks . . . 590
Running Playbooks . . . 597
Managing Ansible Jobs . . . 605
Viewing Playbook Scheduling . . . 608
Troubleshooting . . . 611
Monitoring and Alerting . . . 615
System Overview . . . 616
Switch Overview . . . 619
Telemetry . . . 625
Telemetry Data of a Switch . . . 627
Performance Statistics . . . 644

Switch Performance Statistics . . . 645
NIC Performance Statistics . . . 649
RoCE Counters . . . 654
RoCE Data on Switches and NICs . . . 655
Buffer . . . 662
Dynamic Load Balancing . . . 668
Queue Congestion Visualization . . . 675
Topology . . . 680
Managing Topologies . . . 681
Planning Topologies . . . 683
Viewing Real-Time Topologies . . . 690
Viewing Historical Topologies . . . 692
Viewing Switch Details in Topologies . . . 695
NICs . . . 699
NIC Inventory . . . 700
Module Inventory . . . 703
Splunk Integration . . . 706
Splunk Integration Overview . . . 707
Accessing the Splunk UI . . . 710
Sending Logs to Splunk . . . 715
Troubleshooting Splunk Integration . . . 719
Alerts . . . 723
Alert Types and Levels . . . 724
Checking the Alert List . . . 730
Alert Notifications . . . 734
Sending Alerts to Splunk . . . 735
Sending Email Alert Notifications . . . 745
Viewing Historical Alert Notifications . . . 756
Managing Groups . . . 759
Managing Licenses . . . 768
Managing AmpCon-DC Licenses . . . 769
Importing Licenses for Deployed Switches . . . 771
Importing Licenses for Imported Switches . . . 778
Troubleshooting for License Importing . . . 783
Converting a Trial License to Standard Licenses . . . 786
Viewing AmpCon-DC Licenses . . . 790
Invalidating a License . . . 793
Checking License Logs and Alerts . . . 796
Managing PicOS Licenses . . . 799
Administering AmpCon-DC . . . 804
Managing User Access . . . 805
Configuring TACACS+ Authentication and Authorization . . . 821
Managing Roles . . . 825
Managing Tenants . . . 839
Assigning Roles and Tenants . . . 849

Updating the Encryption Key for Sensitive Data Encryption 854
Forwarding Logs to External Syslog Servers 855
Backing Up and Restoring the AmpCon-DC Database 859
Accessing Devices through SSH Sessions 863
Glossary 864

AmpCon-DC Management Platform 2.5 User Guide



Key Topics



Quick Start

- Quick Start
- Deploying AmpCon-DC
- Working with the User Interface
- Glossary



PicOS Switches

- Onboarding Switches
- Managing Switches
- Configuring Switches
- Monitoring and Alerting



Physical Networks

- Designing Physical Networks
- Simplified ZTP Deployment



Overlay Services

- Provisioning Overlay Services



Third-Party Devices

- Adding Devices
- Managing Added Devices
- RoCE on NICs



Lossless Networks

- Configuring RoCE EasyDeploy and Easy ECN
- Configuring RoCE Policies
- Configuring Dynamic Load



Ansible Playbooks

- Running Playbooks
- Managing Ansible Jobs
- Viewing Playbook Scheduling



Other Features

- Accessing Devices through SSH Sessions
- Managing Groups
- Managing Licenses

Balancing

- Administering AmpCon-DC

Other References

Blogs | Case Studies | Try Now

Release Notes

Before you install AmpCon-DC 2.5.x or upgrade AmpCon-DC to 2.5.x, click the following child topics to get a quick overview of what is added, improved, changed, or fixed in AmpCon-DC 2.5.x:

- AmpCon-DC 2.5.0 Release Notes
- AmpCon-DC 2.5.1 Release Notes

AmpCon-DC 2.5.0 Release Notes

Before you install AmpCon-DC 2.5.0 or upgrade AmpCon-DC to 2.5.0, read this topic to get a quick overview of what is added, improved, or changed in AmpCon-DC 2.5.0.

- New Features
  - Tenant Management
  - VLAN Template–Based ZTP and RoCE Deployment
- Improvements
  - License Management
  - Logical Network
  - Lossless Network
  - Point of Delivery (PoD)
  - Third-Party Device Management
  - User Access Management
- New Changes
  - Supported Switch List and PicOS Versions

New Features

The following features are added to AmpCon-DC 2.5.0:

Tenant Management

AmpCon-DC provides the tenant management feature to manage logical networks. Tenants are logical resource units used to deploy logical networks for overlay service provisioning. You can add and manage tenants in the AmpCon-DC UI.

For more information, see Managing Tenants.

VLAN Template–Based ZTP and RoCE Deployment

The simplified ZTP process now introduces VLAN templates, allowing you to deploy VLAN-type networks automatically. You can configure a RoCE policy within the VLAN template, and then AmpCon-DC will push the RoCE policy configurations (PFC, ECN, and QoS) to switches, enabling Zero Touch Provisioning (ZTP) for RoCE networks. This feature streamlines the deployment of both traditional VLANs and high-performance RoCE networks.

For more information, see Deploying through Simplified ZTP.

Improvements

The following improvements are added to AmpCon-DC 2.5.0:

License Management

From 15 days before a standard AmpCon-DC license expires until after the license expires, notification messages are displayed when you log in to the AmpCon-DC UI to remind you to renew the license.

Logical Network

The logical network deployment process is improved. When you create a logical network, you must designate the tenant who owns the logical network. You also need to assign Virtual Private Clouds (VPCs) in Point of Delivery (PoD) to the tenant so that the virtual networks of the VPCs can be added to the logical network.

For more information, see Deploying Logical Networks.

Lossless Network

The following improvements are added to the lossless network feature:

- On the “RoCE Policies” page, the process of creating a RoCE policy is improved to be consistent with the RoCE configurations in ZTP templates. For more information, see Configuring RoCE Policies.
- The RoCE EasyDeploy and Easy ECN functions are combined to the “Easy Deploy” page. For more information, see Configuring RoCE EasyDeploy and Easy ECN.

Point of Delivery (PoD)

In the **PoD** tab of the “Resource Interconnection” page, you can allocate VPCs to tenants and then add virtual networks of these VPCs to logical networks, achieving flexible and scalable network resource allocation. You can also unbind VPCs from tenants or search for VPCs.

For more information, see Point of Delivery.

Third-Party Device Management

The following improvements are added to the third-party device management feature:

- On the **Device Discovery** tab of the “Hosts” page, the **Sysname** field is renamed to **Device Alias**. When you add a new device, you can specify the device alias to better differentiate devices.
- On the **Inventory** tab of the “Hosts” page, the **Device Alias**, **Status**, **Device Name**, and **Manufacturer** columns are added.

For more information, see Adding Devices and Viewing Monitored Devices.

User Access Management

The following new features are added to the user access management feature:

- You can now create custom roles, assign page and tab access permissions to these custom roles, and then assign these custom roles to users. The users will have the permissions of these roles.
- You can assign tenants to users for logical network management. After a tenant is assigned to a user, the user can deploy and manage the logical networks belonging to the tenant.
- AmpCon-DC supports user group management. To assign the same roles and tenants to multiple users, add these users to a user group and then assign built-in or custom roles and tenants to the user group, instead of authorizing each user one by one, ensuring consistent access control and improved operational efficiency.

For more information, see Managing User Access.

New Changes

The following changes are added to AmpCon-DC 2.5.0:

Supported Switch List and PicOS Versions

The supported switch list and the recommended PicOS versions are updated. For more information, see Supported Switches for 2.5.0.

AmpCon-DC 2.5.1 Release Notes

Before you upgrade AmpCon-DC to 2.5.1, read this topic to get a quick overview of what is improved in AmpCon-DC 2.5.1.

Improvement

Compared with AmpCon-DC 2.5.0, the following improvements are added to AmpCon-DC 2.5.1:

- The switches of the models N5580-32CB, N8650-64OD, N5570-48X6C, N5580-32C, N5580-48Y8C, N5680-32D, and N5630-64C are supported to be managed by AmpCon-DC.

  For switches of the model N5580-32CB, you are recommended to install PicOS 4.7.6E.

  For switches of the model N8650-64OD, you are recommended to install PicOS 4.5.3.3.

  For switches of the model N5570-48X6C, N5580-32C, N5580-48Y8C, N5680-32D, and N5630-64C, you are recommended to install PicOS 4.7.1E.

- The switches of the S5810 series (including S5810-28FS, S5810-28TS, S5810-48FS, S5810-4BTS, and S5810-48TS-P), S5860 series (S5860-20SQ, S5860-24MG-U, S5860-24XB-U, S5860-24XMG, S5860-48MG-U, S5860-48XMG, and S5860-48XMG-U), and S5580 series (S5580-48Y) are supported to be managed by AmpCon-DC.

  For these switches, you are recommended to install PicOS 4.7.1M.

  For more information, see Supported Switches for 2.5.1.

- The switches of the models N5570-48X6C, N5580-32C, N5580-48Y8C, N5680-32D, and N5630-64C can be used to deploy physical networks. For more information, see Recommended Switches for 2.5.1.

Overview

AmpCon-DC is a multivendor automation solution that empowers you to design, deploy, monitor, and manage data center networks. AmpCon-DC simplifies, automates, and transforms network operations from Day 0 through Day 2+.

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

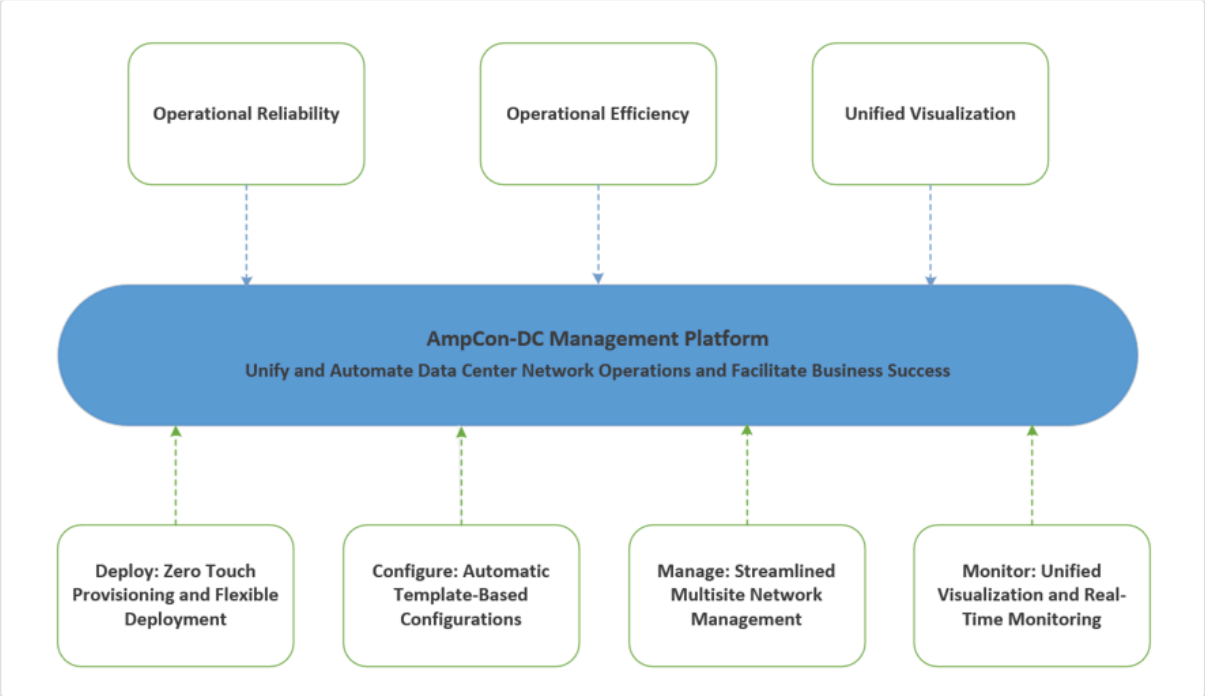
Product Overview

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

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

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

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



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

- **Deploy:** Use normal Zero Touch Provisioning (ZTP) for automated deployment of switches, use simplified ZTP to deploy switches and physical networks in one go, customize physical network design on AmpCon-DC to meet specific networking requirements, and deploy logical networks to provision overlay services.

  All these AmpCon-DC solutions help users deploy switches and build complete physical or logical data center networks quickly, reducing the time to service from weeks to just hours.
- **Configure:** Leverage a centralized user interface to push template-based configurations to switches across multiple sites, minimizing errors and simplifying configuration processes. You can easily roll back a switch to a stable backup configuration to decrease the downtime and ensure network reliability.
- **Manage:** Streamline lifecycle management of deployed networks and managed switches, and integrate with the open-source automation tool Ansible to enhance network and device management automation, helping users increase network management efficiency and focus on more strategic tasks.
- **Monitor:** Provide a unified view and real-time telemetry data of deployed networks, managed switches, connected terminal devices, and Network Interface Cards (NICs), helping users eliminate the time of juggling multiple monitoring tools and gain comprehensive network insights.

AmpCon-DC analyzes telemetry data and issues immediate alerts when a device failure or a performance shift is detected, helping users diagnose root causes and resolve problems quickly and minimize downtime.

Highlights

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

  AmpCon-DC provides powerful features to automate full-lifecycle network operations from Day 0 through Day 2+, helping users accelerate network operations in every phrase, eliminate the downtime risk, and move to more automated network management.

- **Flexible and Efficient Underlay Deployment**

  AmpCon-DC offers flexible VXLAN physical network (underlay) deployment options to meet different networking requirements of users. You can customize physical network design by providing detailed network configurations, or you can provide simple configurations and then AmpCon-DC will automatically design the physical network for you.

- **Automated Overlay Configurations for Service Provisioning**

  AmpCon-DC supports provisioning overlay services, which means users can deploy logical networks on existing physical networks, enabling logical network isolation and flexible service deployment and network configurations without modifying the underlying infrastructure.

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

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

- **Support Batch End-to-End RoCE Deployment**

  AmpCon-DC streamlines end-to-end lossless network configurations (RoCE configurations) for switch and NIC management, helping users easily achieve high-throughput and low-latency data transmission over Ethernet.

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

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

- **Telemetry Visualization to Optimize Network Performance**

AmpCon-DC displays real-time and historical telemetry data, such as performance, buffer, and Dynamic Load Balancing (DLB) data, giving users comprehensive visibility with a time-series view and helping users gain insights for quick decisions and network adjustments.

- **Fault Alerts via Visual Interface, Email Notifications, and Splunk Integration**

  AmpCon-DC displays real-time and historical alerts by analyzing telemetry data, sends alert notifications through emails, and sends alerts to the leading intelligence analysis platform Splunk, helping users find problems quickly and prevent incident escalation.

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

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

Features and Benefits

Platform Features

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

Table 1. Platform Features

Feature	Benefit	Reference Link
Unified Platform	AmpCon-DC is a unified platform that automates network operations from Day 0 through Day 2+, delivers comprehensive network visibility, automation, and operational simplicity, and eliminates the complexity of juggling multiple tools.	• No reference link
Platform Deployment	AmpCon-DC offers flexible platform deployment options: • For organizations seeking virtualization flexibility, AmpCon-DC can be installed on a virtual machine (VMware ESXi 6.7, 7.0, 8.0, QEMU / KVM for Ubuntu 22.04 LTS, or Oracle VirtualBox), enabling deployment on	• Platform Installation Workflow • Installing the AmpCon-DC Server

	existing virtual infrastructure without the need for dedicated hardware. • For organizations without virtual infrastructure, AmpCon-DC can be installed on a physical machine based on Ubuntu 22.04 with Docker installed.	
User Experience	AmpCon-DC features a modern, intuitive, user-friendly user interface (UI) for managing data center networks and devices, providing you unified and consistent experience across the whole network operation process. When you click the question icon **?** on a page in the AmpCon-DC UI, a help document related to this page is displayed in a pop-up window. In-product guidance documents can help you quickly understand the usage of each AmpCon-DC feature, simplifying user onboarding and accelerating time-to-value.	• Working with the User Interface
AmpCon-DC License Import and Management	You can import a new or updated AmpCon-DC license to manage PicOS switches, view all imported AmpCon-DC licenses, convert a trial AmpCon-DC license to a standard AmpCon-DC license, invalidate the AmpCon-DC license on a switch to release the license, or check license-related logs and alerts.	• Managing AmpCon-DC Licenses
Role-Based Access Control	After you deploy AmpCon-DC, you can manage AmpCon-DC user access so that each AmpCon-DC user is assigned with appropriate permissions:	• Managing User Access

	• AmpCon-DC provides Role-Based Access Control (RBAC) to define different permission levels through roles. You can assign one or multiple built-in or custom roles to users. • AmpCon-DC enables users to manage tenants. Each tenant can manage specific logical networks. A user can be assigned one or multiple tenants. Then, when you log in to the AmpCon-DC UI with a user, you can manage the logical networks belonging to the tenants managed by the user. • AmpCon-DC supports user group management. To assign the same roles and tenants to multiple users, you can add these users to a user group and then assign roles and tenants to the user group. All these mechanisms ensure secure, segmented, and efficient management of network operations and help organizations enforce compliance, reduce risk, and streamline collaboration.	
System Overview	You can check the overall status of the AmpCon-DC server, such as CPU, memory, and hard disk usage of the AmpCon-DC server.	• System Overview
Backup and Restore	AmpCon-DC provides the platform backup and restore feature as a critical safeguard for maintaining resilience and operational continuity of the management platform.	• Backing Up and Restoring the AmpCon-DC Database

	In the event of a failure or disaster-recovery scenario, you can quickly restore the AmpCon-DC database securely to a known good state with minimal downtime.	
Encryption Key for Sensitive Data Encryption	AmpCon-DC uses an encryption key to encrypt sensitive data in the AmpCon-DC database, ensuring sensitive data security.	• Updating the Encryption Key for Sensitive Data Encryption

Deployment Features

The following features are used to deploy data center networks and switches:

Table 2. Deployment Features

Feature	Benefit	Reference Link
Deploying Switches	You can deploy PicOS switches through normal ZTP, simplifying the switch deployment and reducing manual operations. After you plug in and reboot a switch, DHCP automatically provides the switch with an IP address and the address of a provision shell script that is obtained from the AmpCon-DC server. Then, the switch automatically runs the shell script to complete the normal ZTP deployment: • A **white-box** switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-DC server, update switch configurations, and reboot the switch. • An **integrated hardware and software** switch runs the shell script to register with the AmpCon-DC	• Deploying Switches through Normal ZTP

	server, update switch configurations, and reboot the switch.	
Deploying Switches and a Physical Network and Configuring RoCE In One Go	The simplified ZTP process can complete the following tasks in one go, simplifying network and switch deployment and RoCE configuration: • A physical network (fabric) is deployed automatically. • All switches in the fabric are bulk onboarded to AmpCon-DC. • Optional: RoCE policy configurations are applied to the switches in the fabric.	• Simplified ZTP Deployment
Designing a Physical Network	If you have a network plan, you can customize the physical network (3-stage fabric) design in the AmpCon-DC UI to meet specific networking requirements.	• Designing Physical Networks
Deploying Logical Networks	You can deploy logical networks on existing physical networks for overlay service provisioning, enabling logical network isolation and flexible service deployment and network configurations without modifying the underlying infrastructure. In AmpCon-DC, a tenant is a logical resource unit used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other. Using tenants to manage logical networks provides the following benefits: • **Resource control** A tenant has quotas for logical routers	• Provisioning Overlay Services

	and logical switches. Logical networks owned by the tenant consume resources from these quotas, ensuring controlled resource usage. • **Restricted resource scope** A tenant can use only the Virtual Private Clouds (VPCs) and fabrics bound to it for logical network deployment. Therefore, logical networks owned by the tenant can add only virtual networks from these VPCs and can be deployed only on the associated fabrics. • **Tenant isolation and access control** Tenants are isolated from each other. AmpCon-DC users can manage the tenants assigned to them. As a result, each AmpCon-DC user can manage only the logical networks owned by the tenants the user manages.	

Management Features

The following features are used to manage data center networks and devices:

Table 3. Configuration and Management Features

Feature	Benefit	Reference Link
Managing Physical and Logical Networks	You can manage the deployed physical and logical networks efficiently through robust management capabilities, providing streamlined and secure network management.	• Managing Fabrics • Managing Logical Network Elements
Importing Switches	If switches have PicOS installed, you can import them to AmpCon-DC directly for management.	• Importing Switches

Managing PicOS Switches	You can manage the lifecycle of PicOS switches to reduce the complexity and workload of switch management while improving efficiency: • Push configurations to switches through configuration templates. • Back up and restore configurations for disaster recovery. • Compare configurations on the same or different switches for troubleshooting or auditing. • Check the switch inventory and telemetry data of each switch. • Upgrade PicOS on a single switch or on multiple switches at scale. • Use Returning Merchandise Authorization (RMA) to replace a switch with another switch of the same switch model. • Decommission (DECOM) a deployed switch to clear the configurations pushed by AmpCon-DC from the switch. • Remove a switch from the AmpCon-DC database and the AmpCon-DC UI. • Check or update PicOS licenses with the latest support entitlements.	• Configuring Switches • Managing Switches • Managing PicOS Licenses
Managing Third-Party Devices	You can manage terminal devices (Linux servers) in your networks: • Add third-party Linux servers to AmpCon-DC to monitor these devices. • Check the device inventory and detailed metrics. • View device information in real-time or historical topologies.	• Managing Third-Party Devices • NICs • RoCE Counters • Running Ansible Playbooks for Automation

	• Monitor Network Interface Cards (NICs) and RoCE related telemetry data for performance tuning. • Run Ansible playbooks on these devices for operational automation.	
Configuring Lossless Networks	You can use AmpCon-DC to streamline lossless network configurations (RoCE configurations) on NICs and switches, achieving high-throughput and low-latency data transmission over Ethernet. • By using the “EasyDeploy” page, you can apply RoCE configurations to switches through the RoCE EasyDeploy function, or you can apply ECN configurations to switches through the Easy ECN function. • If RoCE EasyDeploy and Easy ECN can’t meet your needs, you can apply RoCE configurations to switches through customized RoCE policies that adapt to real-time network conditions and traffic patterns. • You can easily enable or disable dynamic load balancing (DLB) for Equal-Cost Multi-Path (ECMP) on switches. • You can check and configure RoCE on the NIC side with several clicks and monitor RoCE-related telemetry data for performance tuning.	• Configuring Lossless Networks • RoCE on NICs
Accessing Devices through SSH Sessions	You can connect to a device (such as a switch or terminal device) from the AmpCon-DC UI by creating an SSH session.	• Accessing Devices through SSH Sessions

Monitoring and Visibility Features

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

Table 4. Monitoring and Visibility Features

Feature	Benefit	Reference Link
Switch Overview	You can check the overall status of managed PicOS switches.	• Switch Overview
Telemetry Data	You can check real-time or historical telemetry data to monitor the operational state of PicOS switches and connected Linux servers, gaining detailed insights into network performance and device health.	• Telemetry
Queue Congestion Visualization	You can monitor congestion-related metrics for switch port queues, analyze congestion details, and optimize your network for better performance.	• Queue Congestion Visualization
Topology	You can check the network structure in real-time or historical topologies and drill down into an individual switch, right to the port level, to check port stats, overall health of the switch, connected Linux servers, and more.	• Topology
NICs	You can monitor metrics of NICs and connected modules on added Linux servers to evaluate network performance, diagnose issues, and thus ensure optimal network performance.	• NICs
PoD	You can view VPC, network, and VM (available for only vSphere or OpenStack PoD) resources of each added PoD.	• Point of Delivery
Alerts	AmpCon-DC issues an immediate alert when a failure or performance shift is detected, helping you diagnose root causes and resolve problems quickly.	• Alerts

	You can use this feature to achieve the following goals: • View different levels and types of alerts in the AmpCon-DC UI. • Receive real-time email alert notifications if you need to be notified immediately. • View and analyze alerts in the Splunk UI to get more detailed insights.	

Integration Features

The following features are used to integrate with other tools:

Table 5. Integration Features

Feature	Benefit	Reference Link
Ansible Integration	AmpCon-DC integrates with the open-source automation tool Ansible to automate virtually any task. See the following use cases: • Eliminate repetition and simplify workflows. • Automate complex deployment. • Perform zero-downtime configurations. • Manage and maintain configurations.	• Running Ansible Playbooks for Automation
Splunk Integration	AmpCon-DC integrates with the leading operational analysis platform Splunk, providing a fast, easy, and secure way to analyze alerts and system logs and turning them into detailed insights. You can use this feature to achieve the following goals: • Access the Splunk UI from the AmpCon-DC UI, enabling fluid platform switching. • Send alerts from AmpCon-DC to Splunk, and view or analyze these alerts in the Splunk UI.	• Splunk Integration • Sending Alerts to Splunk

	• Send AmpCon-DC system logs to Splunk, and view or analyze these logs in the Splunk UI.	
Syslog Server Integration	AmpCon-DC supports forwarding system logs to external Syslog servers. In this way, you can view and analyze AmpCon-DC system logs more conveniently.	• Forwarding Logs to External Syslog Servers
TACACS+ Integration	AmpCon-DC supports integrating with the Terminal Access Controller Access Control System (TACACS+) server to do authentication and authorization for the AmpCon-DC login users.	• Configuring TACACS+ Authentication and Authorization

Quick Start

The following topics provide quick start guides for AmpCon-DC, detailing the workflows of AmpCon-DC server installation, PicOS switch onboarding, template-based switch configuration, network deployment (physical and logical), and Ansible Automation.

- Platform Installation Workflow
- PicOS Switch Onboarding Workflow
- PicOS Switch Configuration Workflow
- Physical Network Deployment Workflow
- Logical Network Deployment Workflow
- Ansible Automation Workflow

Platform Installation Workflow

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

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

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

Prerequisites

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

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

Table 1. Machine Requirements

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

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

Table 2. Network Requirements

TCP/UDP	Port	Protocol

TCP	80	HTTP
TCP	443	HTTPS
UDP	69	TFTP
UDP	80	OpenVPN

NOTEs

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

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

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

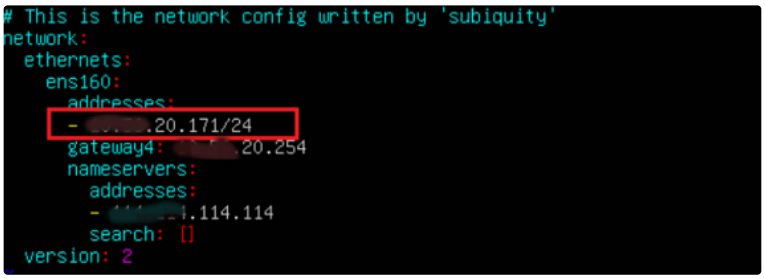
Installing on a Virtual Machine

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

Table 3. Tasks for Installation on Virtual Machines

Task	Description
Preparing a Hypervisor	Prepare the hypervisor used to create the virtual machine. The following hypervisors are supported: • VMware ESXi 6.7, 7.0, or 8.0

	• QEMU for Ubuntu 22.04 LTS • KVM for Ubuntu 22.04 LTS • Oracle VirtualBox **NOTE** The AmpCon-DC server installed on Oracle VirtualBox can be used for lab purposes only.
Downloading the AmpCon-DC Server Image	1. Download the compressed AmpCon-DC server image by going to the FS AmpCon-DC website and locating the image related to the hypervisor and the AmpCon-DC version. 2. Put the compressed AmpCon-DC server image to the machine where the hypervisor exists, and then unzip the image.
Importing the AmpCon-DC Server Image	1. Import the unzipped AmpCon-DC server image to the hypervisor. For different hypervisors, the steps of importing the AmpCon-DC server image are different. To check detailed importing steps on each hypervisor, see Installing on VMware ESXi, Installing on QEMU or KVM, and Installing on VirtualBox for Lab Only. 2. Wait for the importing process to finish. Once completed, the virtual machine is successfully created, and the AmpCon-DC server is installed. The AmpCon-DC server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory. 3. Wait for the importing process to finish. Once completed, the virtual machine is successfully created, and the AmpCon-DC server is installed.
Modifying the Network Interface Configuration	1. Start the virtual machine. 2. Log in to the virtual machine with the default username (pica8) and password (pica8). 3. Open the file named 00-installer-config.yaml by running the **sudo vi /etc/netplan/00-installer-config.yaml** command. 4. In the 00-installer-config.yaml file, modify the IP address with the real IP address of the virtual machine as follows:

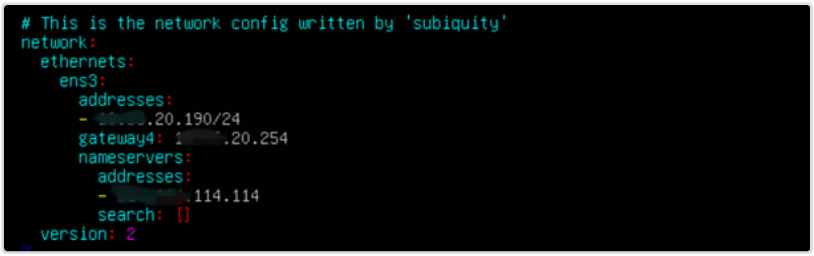
	 The Network Interface Card (NIC) name in the 00-installer-config.yaml file might not match the real NIC name of the virtual machine. Therefore, you must check the real NIC name of the virtual machine first by using the command **ip addr show** and then update the NIC name in the 00-installer-config.yaml file. 5. Apply the network interface configuration by running the **sudo netplan apply** command.
Starting the AmpCon-DC Server	1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command. 2. Start the AmpCon-DC server by running the **sudo ./start.sh** command.

Installing on a Physical Machine

To install the AmpCon-DC server on a physical machine, complete the following tasks:

Table 4. Tasks for Installation on Physical Machines

Task	Description
Preparing a Physical Machine	Prepare a physical machine based on Ubuntu 22.04 LTS with Docker installed.
Downloading and Unzipping the AmpCon-DC Server Installation Package	1. Download the compressed AmpCon-DC server installation package by going to the FS AmpCon-DC website and locating the package related to the AmpCon-DC version. 2. Put the AmpCon-DC server installation package to the prepared physical machine, and then extract the package by running the **unzip <*package_file_name*>.zip** command. A .tar.gz file is generated in the current directory. Extract the generated .tar.gz file by running the **tar -zxvf <*extracted_tar_file_name*>.tar.gz** command. A directory is

	generated with AmpCon-DC server installation files. **NOTEs** • Replace *<package_file_name>* in the command with the name of the AmpCon-DC server installation package. • Replace *<extracted_tar_file_name>* in the command with the extracted .tar.gz file name.
Modifying the Network Interface Configuration	1. Open the file named 00-installer-config.yaml by running the **sudo vi /etc/netplan/00-installer-config.yaml** command. 2. In the 00-installer-config.yaml file, modify the IP address with the real IP address of the physical machine.  3. Apply the network interface configuration by running the **sudo netplan apply** command.
Starting the AmpCon-DC Server	1. Go to the directory where the unzipped AmpCon-DC server installation files exist. 2. Install the AmpCon-DC server by running the **sudo ./install_or_upgrade.sh** command. 3. Wait for the installation process to finish. Once completed, the AmpCon-DC server is installed and started. The AmpCon-DC server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.

What to Do Next

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

Table 5. Post-Installation Tasks

Task	Description
Configuring for Multi-NIC Deployment	If multiple NICs are added to the virtual machine or physical machine, you must specify the NIC IP address used by the AmpCon-DC server to establish connections with managed switches, in the configuration file (/usr/share/automation/server/.env). Otherwise, the connections between the AmpCon-DC server and managed switches might fail. For more information, see Multi-NIC Deployment for Switch Connectivity
Stopping the AmpCon-DC Server	To stop the AmpCon-DC server, follow the steps: 1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command. 2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command.
Uninstalling the AmpCon-DC Server	To uninstall the AmpCon-DC server, follow the steps: 1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command. 2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command. 3. Clear the files in the server directory by running the **sudo rm -rf /usr/share/automation/server** command.
Logging In to the AmpCon-DC UI	The first time you log in to the AmpCon-DC UI, use the default username **admin** and password **admin**. For more information, see Working with the User Interface. **NOTEs** • The user **admin** is a built-in account of the **SuperAdmin** role. It has all operation permissions on AmpCon-DC. For security purposes, change the password upon the first login, update it periodically, and keep it secure. For how to update the password, see User Self-Management. • You can add other user accounts and enable limited access for the personnel who are working with you. For more information, see Managing User Access.

PicOS Switch Onboarding Workflow

Onboard PicOS switches to bring them under AmpCon-DC management. Once successfully onboarded, the PicOS switches are classified as managed devices of AmpCon-DC.

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

- Guidelines
- Prerequisites
- Importing a PicOS Switch
- Deploying a Switch through Normal ZTP
  - Deploying a White-Box Switch
  - Deploying an Integrated Hardware and Software Switch
- What to Do Next

Guidelines

To onboard PicOS switches, three options are provided: switch import, normal Zero Touch Provisioning (ZTP), and simplified ZTP.

- If the switches have PicOS installed, you can onboard these switches by importing them to AmpCon-DC directly.
- If the switches don't have PicOS installed, or though the switches have PicOS installed but you want to onboard these switches through normal ZTP, you can use AmpCon-DC to deploy these switches through normal ZTP.
- If you want to onboard switches, deploy physical networks, and configure RoCE (optional) in one go, use simplified ZTP. This topic doesn't contain the workflow of simplified ZTP deployment. For simplified ZTP procedures, see Physical Network Deployment Workflow - Using Simplified ZTP.

NOTEs

- Importing switches is not a ZTP method, which means that you still need to connect to the switches and do some operations on the switch side, such as obtaining IP addresses from the switches. The importing switch process doesn't push switch configurations.
- Deploying switches through normal ZTP is a ZTP method used for automated deployment of switches. After you reboot the switches, AmpCon-DC will deploy the switches automatically. During the normal ZTP process, AmpCon-DC will push pre-configured configurations to the switches.

- Integrated hardware and software switches have PicOS installed. To onboard these switches, you can import these switches to AmpCon-DC directly, or you can deploy these switches through normal ZTP.
- If you don't need to deploy physical networks, or if you want to design physical networks manually, do not use simplified ZTP.
- Simplified ZTP can be used only for switches with PicOS installed. For example, white-box switches with PicOS installed and integrated hardware and software PicOS switches.

Prerequisites

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

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-DC UI with an account of the **SuperAdmin** role.	• Working with the User Interface
Switch Requirement	Ensure that the switches to be onboarded are supported by AmpCon-DC.	• Supported Switches for 2.5.0 • Supported Switches for 2.5.1
	For switches that have PicOS installed, ensure that the Secure Shell (SSH) protocol is enabled on these switches. SSH is enabled on PicOS switches by default.	• No Reference Link
Network Requirement	Ensure that the switches are able to connect to the AmpCon-DC server.	• No Reference Link
	If a firewall is configured between the AmpCon-DC server and the switches, allow outbound access on the following ports to the management port of each switch. • **TCP**: 22 • **TCP**: 9339	• No Reference Link

	• **TCP**: 830	

Importing a PicOS Switch

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

Table 2. Switch Import Tasks and Links

Category	Task	Reference Link
License Import	Obtain an AmpCon-DC license (containing hardware IDs of the switches to be onboarded) from the FS sale team. Then, import the AmpCon-DC license to AmpCon-DC.	• Importing Licenses for Imported Switches
System Configuration	Click **Device > Device Profiles** from the navigation bar of the AmpCon-DC UI. Click the **System Configuration** tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
Switch Import	If you have obtained the IP address of the switch, you can use the automatic import method.	• Automatically Importing a Switch
	If you haven't obtained the IP address of the switch, you can use the manual import method.	• Manually Importing a Switch
Switch Import Result	Click **Device > Switches** from the navigation bar. On the "Switches" page, check whether the switch is displayed in **Imported** status.	• Checking Importing Results

Deploying a Switch through Normal ZTP

Deploying a White-Box Switch

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

Table 3. White-Box Switch Deployment Tasks and Links

Category	Task	Reference Link
System Configuration	Click **Device > Device Profiles** from the navigation bar of the AmpCon-DC UI. Click the **System Configuration** tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations
Switch Model	Click the **Switch Model** tab. In this tab, configure the switch model related to the switch.	• Configuring Switch Models
Global Configuration	Click the **Global Configuration** tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
Configuration Template	Click **Device > Config Templates** from the navigation bar. Click the **New Template** tab. In this tab, prepare a configuration template.	• Adding Configuration Templates
Switch Configuration	Click **Device > Device Profiles** from the navigation bar. Click the **Switch Configuration** tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations
DHCP Server	Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
Switch Provisioning through Normal ZTP	Provision the switch through normal ZTP to complete the switch deployment.	• Provisioning a White-Box Switch

NOTE

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

- Be careful when you configure system configurations:
  - Ensure that the entered **Device Default Login User** and **Device Default Password** are correct and can be used to log in to the switch.
  - If the switch doesn't use the **Device Default Login User** and **Device Default Password** in the global system configuration, create a non-global system configuration for the switch, and ensure the **Device Default Login User** and **Device Default Password** match with the switch.
  - Ensure that the AmpCon-DC server can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see Checking License Portal Connectivity.
  - Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations or underlay/overlay related configurations.
- If you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-DC parking lot. For more information, see Managing the Parking Lot. To continue deploying the switches in the parking lot, follow these steps:

  a. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar.

  b. On the "Switches" page, click **Parking Lot**.

  c. Locate the switch to be deployed, and then click **Create Config** to add a switch configuration. After you add the switch configuration, the switch will be listed on the "Switches" page with the **Configured** status.

  d. Continue to provision the switch through normal ZTP to complete the switch deployment.

Deploying an Integrated Hardware and Software Switch

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

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

Category	Task	Reference Link
System Configuration	Click **Device > Device Profiles** from the navigation bar of the AmpCon-DC UI. Click the **System Configuration** tab. In this tab, configure the global system configuration. If the global system configuration	• Adding System Configurations

	doesn't match with the switch, create a non-global system configuration.	
Global Configuration	Click the **Global Configuration** tab. In this tab, prepare the global configuration to be pushed to the switch.	• Configuring Global Configurations
Configuration Template	Click **Device > Config Templates** from the navigation bar. Click the **New Template** tab. In this tab, prepare a configuration template.	• Adding Configuration Templates
Switch Configuration	Click **Device > Device Profiles** from the navigation bar. Click the **Switch Configuration** tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations
DHCP Server	Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
Switch Provisioning through Normal ZTP	Provision the switch through normal ZTP to complete the switch deployment.	• Provisioning an Integrated Hardware and Software Switch

What to Do Next

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

Table 5. Post-Onboarding Tasks and Links

Category	Task	Reference Link
Physical Network	Design and deploy physical networks with PicOS switches.	• Physical Network Deployment Workflow
Configuring PicOS Switches	Use configuration templates to push specific configurations to PicOS switches.	• Configuring Switches

Managing PicOS Switches	Manage the lifecycle of PicOS switches to reduce the complexity and workload of switch management while improving efficiency: • Check the switch inventory and telemetry data of each switch. • Upgrade PicOS on a single switch or on multiple switches at scale. • Use Returning Merchandise Authorization (RMA) to replace a switch with another switch of the same switch model. • Decommission (DECOM) a deployed switch to clear the configurations pushed by AmpCon-DC from the switch. • Remove a switch from the AmpCon-DC database and the AmpCon-DC UI. • Check or update PicOS licenses with the latest support entitlements.	• Managing Switches • Managing PicOS Licenses
Monitoring PicOS Switches	Monitor PicOS switches as follows: • Monitor metrics and topologies of PicOS switches. • Monitor added Linux servers, such as NICs and connected optical modules. • View different levels and types of alerts in the AmpCon-DC UI. • Receive real-time email alert notifications if you need to be notified immediately. • View and analyze alerts in the Splunk UI to get more detailed insights.	• Monitoring and Alerting
Accessing Devices through SSH Sessions	Connect to PicOS switches from the AmpCon-DC UI by creating SSH sessions.	• Accessing Devices through SSH Sessions

PicOS Switch Configuration Workflow

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

After you onboard PicOS switches to AmpCon-DC, you can push RoCE configurations through RoCE dashboards or push general configurations through configuration templates.

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

- Guidelines
- Pushing RoCE Configurations
  - Prerequisites
  - Procedure
- Pushing General Configurations
  - Prerequisites
  - Procedure
- What to Do Next

Guidelines

To push configurations to PicOS switches, AmpCon-DC provides two options:

Table 1. Switch Configuration Options

Option	Description
RoCE Configurations	Use RoCE dashboards to push **RoCE configurations** to switches, achieving high-throughput and low-latency data transmission over Ethernet.
General Configurations	Use configuration templates to push **general configurations**. AmpCon-DC provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands. When pushing configurations to PicOS switches, select the configuration templates containing the required CLI commands, and select the switches to be configured. Then, these CLI commands will be run on the selected PicOS switches automatically.

Pushing RoCE Configurations

Prerequisites

Before you push RoCE configurations to PicOS switches through RoCE dashboards, ensure that the following prerequisite tasks have been completed:

Table 2. Prerequisite Tasks and Links for RoCE Configurations

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-DC UI with a **SuperAdmin**, **Admin**, or **Operator** role.	• Working with the User Interface
Switch Requirement	Ensure that the switches to be configured support the RoCE features to be configured.	• PICOS Supported Features
	Onboard supported PicOS switches to bring them under AmpCon-DC management.	• PicOS Switch Onboarding Workflow
	Ensure that the PicOS switches are up and connected to the AmpCon-DC server. You can check the connectivity by clicking **Device > Switches** from the navigation bar and viewing the **VPN IP** column: • ✓: The switch is up and connected to the AmpCon-DC server. • x: The switch is down or not connected to the AmpCon-DC server.	• No Reference Link
Fabric Requirement (Applies to the RoCE Policy feature only)	If you want to apply RoCE policy configurations to a fabric in **Simplified ZTP** type, deploy a fabric through simplified ZTP. Ensure that the fabric meets all of the following conditions: • The fabric is successfully deployed through simplified ZTP.	• Simplified ZTP Deployment • Viewing All Fabrics

	• The **Service Network Type** specified in the related ZTP template is **VLAN**. • The **Leaf Strategy** specified in the related ZTP template is **None**. • No RoCE policy has been configured for the fabric.	
	If you want to apply RoCE policy configurations to a fabric in **Manual** type, add a fabric, and add onboarded PicOS switches to the fabric. Ensure that the fabric meets all of the following conditions: • The fabric has not been associated with a DC template. • No RoCE policy has been configured for the fabric.	• Adding a Fabric • Adding Switches to a Manual Fabric

Procedure

To push RoCE configurations to PicOS switches through RoCE dashboards, complete the following tasks:

NOTEs

- Pay attention to the **guidelines** and **notes** in each reference link. Or else, RoCE configurations might fail to be pushed.
- The following tasks are **not mandatory** and can be used only when needed.

Table 3. RoCE Configuration Tasks and Links

Category	Task	Reference Link
RoCE EasyDeploy	Click **Physical Network > RoCE > EasyDeploy** from the navigation bar. In the **RoCE EasyDeploy** tab, click **+ Configuration** to push RoCE EasyDeploy configurations to switches.	• Configuring RoCE EasyDeploy

Easy ECN	Click **Physical Network > RoCE > EasyDeploy** from the navigation bar. In the **Easy ECN** tab, click **+ Configuration** to push Easy ECN configurations to switches.	• Configuring Easy ECN
RoCE Policy	Click **Physical Network > RoCE > RoCE Policies** from the navigation bar, and then click **+ RoCE Policy** to push RoCE policy configurations to switches in a specific fabric.	• Configuring RoCE Policies
DLB Configuration	Click **Physical Network > RoCE > Load Balancing** from the navigation bar. In the **Deployment** tab, push Dynamic Load Balancing (DLB) configurations to switches.	• Configuring Dynamic Load Balancing

Pushing General Configurations

Prerequisites

Before you push general configurations to PicOS switches, ensure that the following prerequisite tasks have been completed:

Table 4. Prerequisite Tasks and Links for General Configurations

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-DC UI with a **SuperAdmin**, **Admin**, or **Operator** role.	• Working with the User Interface
Switch Requirement	Onboard supported PicOS switches to bring them under AmpCon-DC management.	• PicOS Switch Onboarding Workflow
	Ensure that the PicOS switches are up and connected to the AmpCon-DC server. You can check the connectivity by clicking **Device > Switches** from the navigation bar and viewing the **VPN IP** column:	• No Reference Link

	• ✓: The switch is up and connected to the AmpCon-DC server. • x: The switch is down or not connected to the AmpCon-DC server.	

Procedure

To push general configurations to PicOS switches through configuration templates, complete the following tasks:

Table 5. Configuration Template Tasks and Links

Category	Task	Reference Link
Adding Configuration Templates	Click **Device > Config Templates** from the navigation bar. In the **New Template** tab, create configuration templates with one or multiple required CLI commands.	• Adding Configuration Templates
Creating a Configuration Node	Click the **Push Config** tab. In this tab, create a configuration node, select the configuration templates containing the required CLI commands, enter variable values for the CLI commands, and select the switches to be configured.	• Pushing Configurations to Switches
Verifying Configuration Pushing	Verify the configuration pushing status and logs.	• Verifying the Pushing Status and Log

What to Do Next

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

Table 6. Post-Configuration Tasks and Links

Category	Task	Reference Link

Managing Configuration Templates	Manage the added configuration templates.	• Managing Configuration Templates
Managing Configuration Nodes	View, edit, or delete the added configuration nodes.	• Managing Configuration Nodes
Comparing Configurations	Compare running configurations with initial configurations on the same switch.	• Comparing Running Configurations with Initial Configurations
	Compare running configurations or backup configurations on one switch or on different switches.	• Comparing Running or Backup Configurations
Backing Up and Restoring Configurations	Back up and restore configurations for disaster recovery.	• Backing Up and Restoring Configurations

Physical Network Deployment Workflow

Underlay means the physical network infrastructure that serves as the foundational layer for data transmission. **Physical networks** are used for underlay provisioning. On AmpCon-DC, you can deploy physical networks by deploying fabrics.

This guide provides a comprehensive overview of physical network (fabric) deployment procedures.

NOTEs

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

Guidelines
Designing Physical Networks
  Prerequisites
  Procedure
Using Simplified ZTP
  Prerequisites
  Procedure

Guidelines

AmpCon-DC offers flexible VXLAN physical network deployment options to meet different networking requirements of users.

To deploy a physical network, you are provided with two options:

Table 1. Deployment Options

Option	Description
Simplified ZTP	Use simplified ZTP to onboard switches, deploy physical networks, and configure RoCE (optional) in one go. • Applies to the scenario where you have no network plan but need to quickly deploy a physical network. • Requires less configurations to complete the switch onboarding and physical network deployment. • Used only for the supported switches with PicOS installed.

	• Allows you to choose whether to configure RoCE, achieving zero-touch RoCE deployment.
Physical Network Design	Onboard switches through switch import or normal ZTP first, and then design a physical network with AmpCon-DC. • Applies to the scenario where you have a network plan and want to customize the network. • Requires more configurations to complete the switch onboarding and physical network design. • Used for supported switches, regardless of whether PicOS is installed or not.

Designing Physical Networks

Prerequisites

Before you design a physical network, ensure that the following prerequisite tasks have been completed:

Table 2. Designing Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-DC UI with an account of the **SuperAdmin** role.	• Working with the User Interface
Fabric Requirement	Create a fabric. A fabric is the logical representation of an actual physical network.	• Adding a Fabric
Switch Requirement	Ensure that the PicOS switches are supported for physical network deployment.	• Recommended Switches for 2.5.0 • Recommended Switches for 2.5.1
	Onboard the PicOS switches through switch import or normal ZTP. Ensure that the switches are added to the fabric.	• PicOS Switch Onboarding Workflow • Adding Switches to a Manual Fabric

	Ensure that Google Remote Procedure Call (gRPC) is enabled on the PicOS switches. By default, gRPC is enabled automatically.	• No Reference Link
	Ensure that the PicOS switches are up and connected to the AmpCon-DC server. You can check the connectivity by clicking **Device > Switches** from the navigation bar and viewing the **VPN IP** column on the “Switches” page: • ✓: The switch is up and connected to the AmpCon-DC server. • x: The switch is down or not connected to the AmpCon-DC server.	• No Reference Link
Resource Requirement	Prepare IP pools with enough available IP addresses, which will be used for unit and DC Template design.	• IP Pools
	Prepare ASN pools with enough available ASNs, which will be used for DC Template design.	• ASN Pools
Learning Physical Network Overview	Understand the architecture, networking elements, and key concepts of physical network deployment.	• Physical Network Overview

Procedure

To design a physical network, complete the following tasks:

Table 3. Designing Tasks and Links

Category	Task	Reference Link
Designing Units	Add one or multiple units used by the DC Template as follows: 1. Click **Physical Network > Design > Units** from the navigation bar.	• Designing Units

	2. On the “Units” page, click **+ Unit**, and then design the unit.	
Designing a DC Template	Add the DC Template used to design a fabric as follows: 1. Click **Physical Network > Design > DC Templates** from the navigation bar. 2. On the “DC Templates” page, click **+ Template**, and then design the DC Template.	• Designing DC Templates
Designing a Fabric	1. Click **Physical Network > Fabrics** from the navigation bar. 2. On the “Fabrics” page, click the name of the fabric that you want to design, import a DC Template to the fabric, and then design the fabric.	• Designing Fabrics
Checking Fabric Status	Check whether the fabric is deployed successfully. 1. On the “Fabrics” page, locate the fabric. 2. In the **Status** column, check the fabric deployment status. The **Deployed** status means that the fabric is deployed successfully.	• Checking Fabric Status

Using Simplified ZTP

Prerequisites

Before you use simplified ZTP to deploy a physical network, ensure that the following prerequisite tasks have been completed:

Table 4. Simplified ZTP Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow

	Log in to the AmpCon-DC UI with an account of the **SuperAdmin** role.	• Working with the User Interface
Switch Requirement	Complete all the switch preparations.	• Preparing PicOS Switches
DHCP Server Requirement	Configure the DHCP server.	• Configuring a DHCP Server
System Configuration Requirement	Configure global or non-global system configurations matching the switches used for the network deployment. System configurations contain important information used for the simplified ZTP deployment.	• Adding System Configurations
AmpCon-DC License Requirement	Import AmpCon-DC licenses containing the switches to be deployed. AmpCon-DC licenses decide whether switches can be onboarded for AmpCon-DC management.	• Importing AmpCon-DC Licenses
Resource Pool Requirement	Prepare IP pools and ASN pools, and ensure these pools have enough available IP addresses and ASNs. IP pools and ASN pools are used for automatic assignment of IP addresses and ASNs during the simplified ZTP process.	• Preparing Resource Pools
Learning Architecture	Understand the architecture of simplified ZTP deployment.	• Simplified ZTP Architecture

Procedure

To deploy a physical network through simplified ZTP, complete the following tasks:

Table 5. Simplified ZTP Tasks and Links

Category	Task	Reference Link

Adding a ZTP Template	Add a ZTP template as follows: 1. Click **Physical Network > Design > ZTP Templates** from the navigation bar. 2. On the “ZTP Templates” page, click **+ Template**, and enter information to complete the template creation. After you create a ZTP template, you will be redirected to the fabric page.	• Adding ZTP Templates
Completing Physical Connections	Based on the ZTP template, AmpCon-DC automatically generates the topology, device information, and link information of the physical network. You must complete physical connections between switches based on the generated information displayed in the **Configuration Preview** tab of the fabric page.	• Completing Physical Connections
Bringing Switches Online	Bring all spine switches online as follows: 1. In the **Configuration Preview** tab of the fabric page, select all the switches with the **Spine** role. 2. Click **Enable ZTP**.	• Bringing All Spine Switches Online
	Bring all leaf switches online as follows: 1. In the **Configuration Preview** tab of the fabric page, select all switches with the **Leaf** role. 2. Click **Enable ZTP**.	• Bringing All Leaf Switches Online
Checking Fabric Status	Check whether the fabric is deployed successfully. 1. Click **Physical Network > Fabrics** from the navigation bar. 2. On the “Fabrics” page, locate the fabric deployed through simplified ZTP.	• Checking Fabric Status

	3. In the **Status** column, check the fabric deployment status. The **Deployed** status means that the fabric is deployed successfully.	
Checking Switch Status	Check whether switches are deployed successfully. 1. Click **Device > Switches** from the navigation bar. 2. On the “Switches” page, locate the switch deployed through simplified ZTP. 3. In the **Status** column, check the switch deployment status. The **Provisioning Success** status means that the switches are deployed successfully.	• Checking Switch Status

Logical Network Deployment Workflow

Overlay is a virtual network architecture built on top of an existing physical network (underlay). Overlay services refer to virtualized network functions or logical layers, which enable logical network isolation and flexible service deployment and network configuration without modifying the underlying infrastructure. **Logical networks** are logical spaces to provision overlay services.

After a physical network is deployed, you can deploy logical networks to meet overlay service provisioning requirements.

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

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

Guidelines
Prerequisites
Procedure
What to Do Next

Guidelines

Understand the following concepts used for logical network deployment. For more information, see Logical Network Overview.

- **Logical networks**

  The core of overlay service provisioning. A logical network holds other logical network elements, including logical routers, logical switches, and virtual networks, to instantiate an overlay service network.

- **Tenants**

  The logical resource units used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other.

- **Logical routers**

  The Layer 3 distributed routing network elements that connect with logical switches and virtual routers. Similar to Layer 3 Virtual Network Instance (L3 VNI), logical routers are

designed to enable Layer 3 communication across VLAN Domains and manage the pushing of VRF configurations.

- **Logical switches**

  The Layer 2 network elements that connect with resources (such as physical servers and virtual machines) within the same service system. Logical switches exist only on server leaf switches and handle configuration pushing of gateway interfaces, Network Virtualization Edge (NVE), and Bridge Domain (BD).

- **Virtual networks**

  The virtual Layer 2 network devices used in vSphere or bare metal Point of Delivery (PoD). The ports of virtual networks are attached to logical switches. The virtual network for bare metal PoD is called VL2.

- **Point of Delivery (PoD)**

  The minimum service unit of a data center, is a collection of resources in a data center. Currently, only bare metal PoD and vSphere PoD can be used for logical network deployment. You can connect virtual networks of bare metal PoD or vSphere PoD with logical switches.

- **VLAN Domain group**

  Each fabric contains one VLAN Domain group. Each VLAN Domain group contains one or multiple VLAN Domains. VLAN Domains restrict the allocation of VLAN IDs to a specific range for virtual networks connected to logical switches.

- **Node uplink configuration**

  Used to connect node devices in virtual networks with uplink switches after you connect virtual networks in PoD with logical switches.

Prerequisites

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

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow

	Log in to the AmpCon-DC UI with an account of the **SuperAdmin** role.	• Working with the User Interface
Physical Network Requirement	Ensure that you have completed the physical network (fabric) deployment through simplified ZTP or physical network design. **NOTE** If the fabric is deployed through simplified ZTP, ensure the **Service Network Type** is **VXLAN** in the related ZTP template. This is because logical networks cannot be deployed on VLAN fabrics.	• Physical Network Deployment Workflow
VNI Pool Requirement	Prepare VNI pools with enough available VNI values, which will be used for L2 VNI and L3 VNI assignment of the logical network.	• Adding VNI Pools
Tenant Requirement	Create a tenant to which the logical network belongs, and ensure that the tenant is associated with the fabric and is assigned enough logical router quotas and logical switch quotas. Assign the tenant to an AmpCon-DC user.	• Managing Tenants • Assigning Roles and Tenants
PoD Requirement	To add virtual networks of **vSphere Point of Delivery (PoD)** to the logical network, create a vSphere PoD, and then allocate VPCs in the vSphere PoD to the newly created tenant. To add virtual networks of **bare metal PoD** to the logical network, create a bare metal PoD, and make sure the PoD belongs to the fabric used for the logical network deployment. **NOTE** For each added vSphere PoD, pay attention to the following points. Or else,	• Adding a vSphere PoD • Adding a Bare Metal PoD • Allocating VPCs to Tenants

	the logical network deployment will fail. • When you create a vSphere PoD, make sure that the PoD belongs to the fabric used for the logical network deployment. • Ensure that the AmpCon-DC server is connected to the vSphere platform. You can check as follows: a. Click **Resource > Resource Interconnection** from the navigation bar. b. In the **PoD** tab, ensure that the PoD is in **Active** status.	
VLAN Domain Group Requirement	Ensure that you have added and configured a VLAN Domain group for the related physical network (fabric). **NOTEs** • Only after the physical network (fabric) is deployed successfully, can you configure a VLAN Domain group for the fabric. • Ensure that the **Bridge Domain Range** of each VLAN Domain has available intersections with the **Global VLAN** range of the related PoD. Or else, when you add a logical switch, VLAN will fail to be assigned.	• Adding a VLAN Domain Group
Node Uplink Requirement	To add virtual networks of **vSphere PoD** to the logical network, ensure that you have added node uplink configurations for the vSphere PoD. To add virtual networks of **bare metal PoD** to the logical network, ensure that you have added a bare metal node group (including	• Configuring Node Uplink for Cloud Platform Nodes • Configuring Node Uplink for Bare Metal Nodes

	node addition and node uplink configurations) for the bare metal PoD. **NOTE** Pay attention to the following points. Or else, the logical network deployment will fail. • The node uplink configurations must be consistent with actual physical connections. • When you configure node uplink, the speed of the NIC ports and connected switch ports must be the same.	
VL2 Requirement	After you create a bare metal PoD, no virtual networks (called VL2 for bare metal) exist in the bare metal PoD. If you need to add virtual networks of bare metal PoD to the logical network, you must add one or multiple VL2s for the bare metal PoD, and then associate bare metal node devices with the VL2s. **NOTEs** • The node devices used for VL2 association are those bare metal nodes you added in the bare metal node group. So, if you haven't added a bare metal node group for the related PoD to which the VL2 belongs, you can't associate bare metal node devices with the VL2. • When you add a VL2, pay attention to the **VLAN** field: ◦ If you don't enter any VLAN value in the **VLAN** field, AmpCon-DC will automatically assign a VLAN ID	• Adding a VL2 • Associating Bare Metal Nodes with a VL2

	from the **Global VLAN** range of the PoD. ◦ If you enter a VLAN ID here, ensure that the VLAN ID is in the intersections between the **Global VLAN** range of the PoD and the **Bridge Domain Range** of the related VLAN Domain, and the entered VLAN ID is not used by other VL2 of the same PoD. Or else, the logical network will fail to be deployed.	

Procedure

To deploy a logical network, complete the following tasks:

Table 2. Deployment Tasks and Links

Category	Task	Reference Link
Logging In to the UI	Log in to the AmpCon-DC UI with the prepared user to which the tenant is assigned.	• No Reference Link
Adding a Logical Network	Add a logical network as follows: 1. Click **Service Provision > Logical Networks** from the navigation bar. 2. On the “Logical Networks” page, click **+ Logical Network**. **NOTE** Ensure that you select the prepared tenant in the **Tenant** drop-down list.	• 1. Adding a Logical Network
Adding Virtual Networks	Add virtual networks to the logical network as follows: 1. Click **Service Provision > Logical Networks** from the navigation bar.	• 2. Adding Virtual Networks

	2. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page. 3. Drag the virtual network icon to the logical network provisioning canvas. **NOTE** Only the virtual networks of those VPCs that have been allocated to the tenant can be added to the the logical network.	
Provisioning Logical Switches	Provision logical switches as follows: 1. Adding logical switches by dragging the logical switch icon to the logical network provisioning canvas. 2. Connect logical switches with virtual networks by right-clicking each added logical switch in the canvas and then clicking **Add Connection**. 3. Check whether the connection is successful. The line between a logical switch and a virtual network is in green when the connection succeeds and in red when the connection fails.	• 3. Provisioning Logical Switches
Provisioning Logical Routers	Provision logical routers as follows: 1. Adding logical routers by dragging the logical router icon to the logical network provisioning canvas. 2. Connect logical routers with logical switches by right-clicking each added logical router in the canvas and then clicking **Add Connection**.	• 4. Provisioning Logical Routers

	3. Check whether the connection is successful. The line between a logical router and a logical switch is in green when the connection succeeds and in red when the connection fails.	

What to Do Next

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

Table 3. Post-Deployment Tasks and Links

Category	Task	Reference Link
Managing Logical Networks	Manage added logical networks as follows: • View, edit, or delete a logical network. • Delete logical elements from a logical network. • Disconnect the connections between a logical switch and the virtual network of specific node devices. • Disconnect the connections between a logical router and connected logical switches.	• Managing Logical Networks
Managing Logical Switches	View, edit, or delete added logical switches.	• Managing Logical Switches
Managing Logical Routers	View, edit, or delete added logical routers.	• Managing Logical Routers

Ansible Automation Workflow

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

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

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

Prerequisites
Procedure
What to Do Next

Prerequisites

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

Table 1. Prerequisite Tasks and Links

Category	Task	Reference Link
Platform Requirement	Install the AmpCon-DC server successfully.	• Platform Installation Workflow
	Log in to the AmpCon-DC UI with an account of the **SuperAdmin**, **Admin**, or **Operator** role.	• Working with the User Interface
Switch Requirement (Applicable only for running playbooks on PicOS switches)	Ensure that each PicOS switch to run Ansible playbooks has been onboarded to AmpCon-DC.	• PicOS Switch Onboarding Workflow
	Ensure that the **Device Default Login User** and **Device Default Password** in the global system configuration can be used to log in to the PicOS switches. **NOTE**	• Adding a Global System Configuration

	If the default username and password of a switch doesn't match the **Device Default Login User** and **Device Default Password** specified in the global system configuration, the playbook will fail to be run on the switch.	
	Ensure that the PicOS switches are up and connected to the AmpCon-DC server. You can check the connectivity by clicking **Device > Switches** from the navigation bar and viewing the **VPN IP** column: • ✓: The switch is up and connected to the AmpCon-DC server. • x: The switch is down or not connected to the AmpCon-DC server.	• No Reference Link
Linux Server Requirement (Applicable only for running playbooks on Linux servers)	Ensure that the Linux servers have been added to AmpCon-DC.	• Adding Devices

Procedure

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

Table 2. Playbook Running Tasks and Links

Category	Task	Reference Link
Checking Pre-Built Playbooks	AmpCon-DC offers a series of pre-built Ansible playbooks. Click **Maintain > Automation > Playbooks** from the navigation bar. On the "Playbooks" page, click the **Show Pre-built Playbooks**	• Using Pre-built Playbooks

	toggle, and then check whether the pre-built Ansible playbooks meet your needs. If yes, click **Save AS** on the "Playbooks" page to create a copy playbook, and then run the playbook.	
Writing or Importing Playbooks	If the pre-built Ansible playbooks don't meet your needs, write or import a playbook on the "Playbooks" page as follows: • Click **+ Playbook**, and then write a playbook in the AmpCon-DC UI. • Click **Import**, and then import a local playbook to AmpCon-DC.	• Examples for Ansible Playbooks • Using Ansible playbooks • Writing a Playbook on AmpCon-DC • Importing a Playbook
Checking Playbook Syntax	Before you run a playbook, check whether the playbook syntax is valid. On the "Playbooks" page, locate a playbook, and then click **Check**.	• Checking Syntax for a Playbook
Running Playbooks	On the "Playbooks" page, locate the playbook, and then click **Run** to complete the automation operation.	• Running a Playbook
Checking Ansible Job Results and Output	An Ansible job is a single execution of an Ansible playbook. Click **Maintain > Automation > Ansible Jobs** from the navigation bar. On the "Ansible Jobs" page, check the playbook execution result and output.	• Managing Ansible Jobs

What to Do Next

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

Table 3. Post-Running Tasks and Links

Category	Task	Reference Link

Viewing Playbook Scheduling	View executed playbooks based on months, weeks, or days.	• Viewing Playbook Scheduling
Troubleshooting for Failed Ansible Jobs	If a playbook fails to be run on PicOS switches or Linux servers, check the possible reasons and solutions for troubleshooting.	• Troubleshooting

Planning

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

For detailed information, see the following child topics:

- Supported Information
- Installation Requirements

Supported Information

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

Supported AmpCon-DC Deployments
Supported Switches

Supported AmpCon-DC Deployments

The following AmpCon-DC deployments are supported:

Table 1. Supported Deployment Information

Indicator	Support Information
Deployment Method	VMware ESXi 6.7, 7.0, 8.0, QEMU / KVM for Ubuntu 22.04 LTS, Oracle VirtualBox for lab only, physical machine based on Ubuntu 22.04 LTS with Docker
Maximum Number of Switches Supported	1000
Maximum Number of Registered Users	1000
Maximum Number of Online Users	100
Storage Duration of System Logs	2 months
Storage Duration of Operation Logs	2 months
Maximum Storage of Current Alerts	Unlimited
Maximum Storage of Historical Alerts	2 months

Supported Switches

AmpCon-DC supports FS, Edgecore, DELL, Delta, and HPE switches. For detailed support lists, see Supported Switches for 2.5.0 and Supported Switches for 2.5.1.

Supported Switches for 2.5.0

AmpCon-DC 2.5.0 supports managing the following switches:

FS Hardware
Edgecore Hardware
DELL Hardware
Delta Hardware
HPE Hardware

> **NOTEs**
>
> Use the following recommended PicOS versions. Or else, some features of AmpCon-DC might not work.
>
> - For FS switches, you are recommended to install PicOS 4.7.0E.
> - For switches of the model N8550-24CD8D, N9550-64D, and N9600-64OD, you are recommended to install PicOS 4.5.3.2.
> - For switches of the model N8610-32D and N8650-32OD, you are recommended to install PicOS 4.5.6E.
> - For switches of the model N8510-24CD8D, you are recommended to install PicOS 4.5.5E.
> - For switches of the model N8520-32D, you are recommended to install PicOS 4.5.4E.

FS Hardware

Table 1. Supported FS Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	N5570-48S6C	48 x 10G, 6 x 100G	Trident3-X5	Intel x86
10G Switch Portfolio	N5850-48S6Q	48 x 10G, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	N5850-48X6C	48 x 10G-T, 6 x 100G	Trident3-X5	Intel x86

25G Switch Portfolio	N8550-48B8C	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	N8550-32C	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	N8550-64C	64 x 100G	Tomahawk 2	Intel x86
100G Switch Portfolio	N8560-32C	32 x 100G QSPF28	Trident3	Intel x86
200G Switch Portfolio	N8510-24CD8D	24 x 200G QSFP56, 8 x 400G QSFP-DD	Trident4-X9	Intel x86
200G Switch Portfolio	N8550-24CD8D	24 x 200G, 8 x 400G	Trident4-X9	Intel x86
400G Switch Portfolio	N8520-32D	32 x 400G QSFP-DD	Trident4-X11	Intel x86
400G Switch Portfolio	N8610-32D	32 x 400G QSFP-DD	Tomahawk 4	Intel x86
400G Switch Portfolio	N9550-32D	32 x 400G	Tomahawk 3	Intel x86
400G Switch Portfolio	N9550-64D	64 x 400G	Tomahawk 4	Intel x86
800G Switch Portfolio	N8650-32OD	32 x 800G OSFP, 2 x 25G SFP28	Tomahawk 5	Intel x86
800G Switch Portfolio	N9600-64OD	64 x 800G	Tomahawk 5	Intel x86

Edgecore Hardware

Table 2. Supported Edgecore Switches

Category	Model	Port Configuration	Switch ASIC	CPU

1G Switch Portfolio	AS4610-30P	24 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-30T	24 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54P	48 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54T(B)	48 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4625-54P	48 x 10/100/1000 BASE-T, 6 x 1G/10G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4625-54T	48 x 10/100/1000 BASE-T, 6 x 1G/10G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4630-54PE (EPS202)	48 x 1G PoE, 4 x 25G, 2 x 100G	Trident3	Intel x86
1G Switch Portfolio	AS4630-54TE (EPS201)	48 x 1G, 4 x 25G	Trident3	Intel x86
Multi-Gig Switch Portfolio	AS4630-54NPE (EPS203)	36 x 1/2.5G PoE, 12 x 1/2.5/5/10G PoE	Trident3	Intel x86
10G Switch Portfolio	AS5712-54X	48 x 10G, 6 x 40G	Trident2	Intel x86
10G Switch Portfolio	AS5812-54T	48 x 10G-T, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	AS5812-54X	48 x 10G, 6 x 40G	Trident2+	Intel x86

10G Switch Portfolio	AS5835-54T (DCS202)	48 x 10G-T, 6 x 100G	Trident3	Intel x86
10G Switch Portfolio	AS5835-54X (DCS201)	48 x 10G, 6 x 100G	Trident3	Intel x86
25G Switch Portfolio	AS7312-54X (S)	48 x 25G, 6 x 100G	Tomahawk+	Intel x86
25G Switch Portfolio	AS7326-56X (DCS203)	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86
40G Switch Portfolio	AS6812-32X	32 x 40G	Trident2+	Intel x86
100G Switch Portfolio	AS7712-32X (DCS501)	32 x 100G	Tomahawk	Intel x86
100G Switch Portfolio	AS7726-32X (DCS204)	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	AS7816-64X (DCS500)	64 x 100G	Tomahawk2	Intel x86

DELL Hardware

Table 3. Supported DELL Switches

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

1G Switch Portfolio	N3048ET-ON	48 x 1G, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3224F-ON	24 x 1G SFP, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224P-ON	24 x 1 G 30W PoE, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224T-ON	24 x 1G, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248P-ON	48 x 1G 30W PoE, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248TE-ON	48 x 1G, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
10G Switch Portfolio	S4048-ON	48 x 10G, 6 x 40G, 2 x 40/100G	Trident2	Intel x86
10G Switch Portfolio	S4128F-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4128T-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4148F-ON	48 x 10G SFP, 2 x 40G, 4 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4148T-ON	48 x 10G BASE-T, 2 x 40G, 4 x 100G	Maverick	Intel x86
25G Switch Portfolio	S5212F-ON	12 x 25G, 3 x 100G	Trident3-X5	Intel x86

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

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

Delta Hardware

Table 4. Supported Delta Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	AG7648	48 x 10G, 6 x 40G	Trident2	Intel x86
25G Switch Portfolio	AG5648 v1-R	48 x 25G, 6 x 100G	Tomahawk+	Intel x86
100G Switch Portfolio	AG9032v1	32 x 100G	Tomahawk	Intel x86

HPE Hardware

Table 5. Supported HPE Switches

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

10G Switch Portfolio	HPE AL 6921-54X	48 x 10G-T, 6 x 40G	Trident2+	Intel x86

Supported Switches for 2.5.1

AmpCon-DC 2.5.1 supports managing the following switches:

FS Hardware
Edgecore Hardware
DELL Hardware
Delta Hardware
HPE Hardware

NOTEs

Use the following recommended PicOS versions. Or else, some features of AmpCon-DC might not work.

- For FS switches, you are recommended to install PicOS 4.7.0E.
- For switches of the model N8550-24CD8D, N9550-64D, and N9600-64OD, you are recommended to install PicOS 4.5.3.2.
- For switches of the model N8610-32D and N8650-32OD, you are recommended to install PicOS 4.5.6E.
- For switches of the model N8510-24CD8D, you are recommended to install PicOS 4.5.5E.
- For switches of the model N8520-32D, you are recommended to install PicOS 4.5.4E.
- For switches of the model N5580-32CB, you are recommended to install PicOS 4.7.6E.
- For switches of the model N8650-64OD, you are recommended to install PicOS 4.5.3.3.
- For switches of the model N5570-48X6C, N5580-32C, N5580-48Y8C, N5680-32D, and N5630-64C, you are recommended to install PicOS 4.7.1E.
- For switches of the S5810 series (including S5810-28FS, S5810-28TS, S5810-48FS, S5810-4BTS, and S5810-48TS-P), S5860 series (S5860-20SQ, S5860-24MG-U, S5860-24XB-U, S5860-24XMG, S5860-48MG-U, S5860-48XMG, and S5860-48XMG-U), and S5580 series (S5580-48Y), you are recommended to install PicOS 4.7.1M.

FS Hardware

Table 1. Supported FS Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	N5570-48S6C	48 x 10G, 6 x 100G	Trident3-X5	Intel x86
10G Switch Portfolio	N5850-48S6Q	48 x 10G, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	N5570-48X6C	48 x 10G-T, 6 x 100G	Trident3-X5	Intel x86
10G Switch Portfolio	N5850-48X6C	48 x 10G-T, 6 x 100G	Trident3-X5	Intel x86
25G Switch Portfolio	N5580-48Y8C	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86
25G Switch Portfolio	N8550-48B8C	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	N5580-32C	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	N5580-32CB	32 x 100G QSFP28	Trident3-X7	Intel x86
100G Switch Portfolio	N8550-32C	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	N5630-64C	64 x 100G	Tomahawk 2	Intel x86
100G Switch Portfolio	N8550-64C	64 x 100G	Tomahawk 2	Intel x86
100G Switch Portfolio	N8560-32C	32 x 100G QSPF28	Trident3	Intel x86
200G Switch Portfolio	N8510-24CD8D	24 x 200G QSFP56, 8 x 400G	Trident4-X9	Intel x86

		QSFP-DD		
200G Switch Portfolio	N8550-24CD8D	24 x 200G, 8 x 400G	Trident4-X9	Intel x86
400G Switch Portfolio	N8520-32D	32 x 400G QSFP-DD	Trident4-X11	Intel x86
400G Switch Portfolio	N8610-32D	32 x 400G QSFP-DD	Tomahawk 4	Intel x86
400G Switch Portfolio	N5680-32D	32 x 400G	Tomahawk 3	Intel x86
400G Switch Portfolio	N9550-32D	32 x 400G	Tomahawk 3	Intel x86
400G Switch Portfolio	N9550-64D	64 x 400G	Tomahawk 4	Intel x86
800G Switch Portfolio	N8650-32OD	32 x 800G OSFP, 2 x 25G SFP28	Tomahawk 5	Intel x86
800G Switch Portfolio	N9600-64OD	64 x 800G	Tomahawk 5	Intel x86
800G Switch Portfolio	N8650-64OD	64 x 800G	Tomahawk 5	Intel x86
1G Switch Portfolio	S5810-28FS	8x1G RJ45/SFP combo, 20 x 1G SFP, 4 x 10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-28TS	24 x 1G copper, 4x1G RJ45/SFP combo, 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

1G Switch Portfolio	S5810-48TS	48 x 1G copper, 4 x 10G SFP+	Helix4	ARM Cortex A9
1G Switch Portfolio	S5810-48TS-P	48 x 1G copper, 4 x 10G SFP+	Helix4	ARM Cortex A9
5G Switch Portfolio	S5860-24MG-U	24 x 5G copper, 4 x 25G SFP28	Hurricane3-MG	ARM Cortex A9
5G Switch Portfolio	S5860-48MG-U	48 x 5G 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 POE, 4 x 10G SFP+, 4 x 25G SFP28	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	S5860-48XMG-U	48 x 10G copper, 4 x 25G SFP28, 2 x 40G QSFP+	Hurricane3-MG	ARM Cortex A9
25G Switch Portfolio	S5580-48Y	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86

Edgecore Hardware

Table 2. Supported Edgecore Switches

Category	Model	Port Configuration	Switch ASIC	CPU
1G Switch Portfolio	AS4610-30P	24 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-30T	24 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54P	48 x 1G PoE, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-54T(B)	48 x 1G-T, 4 x 10G, 2 x 20G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4625-54P	48 x 10/100/1000 BASE-T, 6 x 1G/10G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4625-54T	48 x 10/100/1000 BASE-T, 6 x 1G/10G SFP+	Trident3-X2	Intel x86
1G Switch Portfolio	AS4630-54PE (EPS202)	48 x 1G PoE, 4 x 25G, 2 x 100G	Trident3	Intel x86
1G Switch Portfolio	AS4630-54TE (EPS201)	48 x 1G, 4 x 25G	Trident3	Intel x86
Multi-Gig Switch Portfolio	AS4630-54NPE (EPS203)	36 x 1/2.5G PoE, 12 x 1/2.5/5/10G PoE	Trident3	Intel x86
10G Switch Portfolio	AS5712-54X	48 x 10G, 6 x 40G	Trident2	Intel x86

10G Switch Portfolio	AS5812-54T	48 x 10G-T, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	AS5812-54X	48 x 10G, 6 x 40G	Trident2+	Intel x86
10G Switch Portfolio	AS5835-54T (DCS202)	48 x 10G-T, 6 x 100G	Trident3	Intel x86
10G Switch Portfolio	AS5835-54X (DCS201)	48 x 10G, 6 x 100G	Trident3	Intel x86
25G Switch Portfolio	AS7312-54X (S)	48 x 25G, 6 x 100G	Tomahawk+	Intel x86
25G Switch Portfolio	AS7326-56X (DCS203)	48 x 25G, 8 x 100G, 2 x 10G	Trident3-X7	Intel x86
40G Switch Portfolio	AS6812-32X	32 x 40G	Trident2+	Intel x86
100G Switch Portfolio	AS7712-32X (DCS501)	32 x 100G	Tomahawk	Intel x86
100G Switch Portfolio	AS7726-32X (DCS204)	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	AS7816-64X (DCS500)	64 x 100G	Tomahawk2	Intel x86

DELL Hardware

Table 3. Supported DELL Switches

Category	Model	Port Configuration	Switch ASIC	CPU

1G Switch Portfolio	N3024EP-ON	24 x 1G PoE, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3024ET-ON	24 x 1G, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3048ET-ON	48 x 1G, 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	N3224F-ON	24 x 1G SFP, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224P-ON	24 x 1 G 30W PoE, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3224T-ON	24 x 1G, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248P-ON	48 x 1G 30W PoE, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
1G Switch Portfolio	N3248TE-ON	48 x 1G, 4 x 10G, 2 x 40/100G	Trident3-X3	Intel x86
10G Switch Portfolio	S4048-ON	48 x 10G, 6 x 40G, 2 x 40/100G	Trident2	Intel x86
10G Switch Portfolio	S4128F-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4128T-ON	28 x 10G, 2 x 100G	Maverick	Intel x86
10G Switch Portfolio	S4148F-ON	48 x 10G SFP, 2 x 40G, 4 x 100G	Maverick	Intel x86

10G Switch Portfolio	S4148T-ON	48 x 10G BASE-T, 2 x 40G, 4 x 100G	Maverick	Intel x86
25G Switch Portfolio	S5212F-ON	12 x 25G, 3 x 100G	Trident3-X5	Intel x86
25G Switch Portfolio	S5224F-ON	24 x 25G, 4 x 100G	Trident3-X5	Intel x86
25G Switch Portfolio	S5248F-ON	48 x 25G, 8 x 100G	Trident3-X7	Intel x86
25G Switch Portfolio	S5296F-ON	96 x 25G, 8 x 100G	Trident3-X7	Intel x86
100G Switch Portfolio	S5232F-ON	32 x 100G, 2 x 10G	Trident3-X7	Intel x86
100G Switch Portfolio	Z9100-ON	32 x 100G, 2 x 10G	Tomahawk	Intel x86
100G Switch Portfolio	Z9264F-ON	64 x 100G, 2 x 10G	Tomahawk2	Intel x86
Multi-Gig Switch Portfolio	N2224PX-ON	24 x 1G/2.5G 30W/60W PoE, 4 x 25G, 2 x 40G	Hurricane 3-MG	Intel x86
Multi-Gig Switch Portfolio	N2224X-ON	24 x 1G/2.5G, 4 x 25G, 2 x 40G	Hurricane 3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248PX-ON	48 x 1G/2.5G 30W/60W PoE, 4 x 25G, 2 x 40G	Hurricane 3-MG	Intel x86
Multi-Gig Switch Portfolio	N2248X-ON	48 x 1G/ 2.5G, 4 x 25G, 2 x 40G	Hurricane 3-MG	Intel x86
Multi-Gig Switch Portfo	N3132PX-ON	24 x 1G PoE,	Firebolt 4 FS	ARM Cortex A9

lio		8 x 1/2.5/5G PoE, 4 x 10G		
Multi- Gig Switch Portfo lio	N3208PX -ON	4 x 1/2.5/5G PoE, 4 x 1G PoE, 2 x 10G SFP+	Hurricane 3-MG	Intel x86
Multi- Gig Switch Portfo lio	N3224PX -ON	24 x 1/2.5/5/10G 90W PoE, 4 x 25G, 2 x 40/100G	Trident3- X3	Intel x86
Multi- Gig Switch Portfo lio	N3248PX E-ON	48 x 1/2.5/5/10G 90W PoE, 4 x 25G, 2 x 40/100G	Trident3- X5	Intel x86
Multi- Gig Switch Portfo lio	N3248X- ON	48 x 1/2.5/5/10G, 4 x 25G, 2 x 40/100G	Trident3- X5	Intel x86

Delta Hardware

Table 4. Supported Delta Switches

Category	Model	Port Configuration	Switch ASIC	CPU
10G Switch Portfolio	AG7648	48 x 10G, 6 x 40G	Trident2	Intel x86
25G Switch Portfolio	AG5648 v1-R	48 x 25G, 6 x 100G	Tomahawk+	Intel x86
100G Switch Portfolio	AG9032v1	32 x 100G	Tomahawk	Intel x86

HPE Hardware

Table 5. Supported HPE Switches

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

Installation Requirements

Before you deploy AmpCon-DC, check the following requirements:

- Server Requirements
- Network Requirements
- License Requirements

Server Requirements

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

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

Table 1. Machine Requirements

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

Network Requirements

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

Table 2. Network Requirement for the AmpCon-DC Server Machine

TCP/UDP	Port	Protocol
TCP	80	HTTP

TCP	443	HTTPS
UDP	69	TFTP
UDP	80	OpenVPN

NOTEs

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

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

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

License Requirements

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

- **Trial license**: The trial period lasts for 90 days and an additional 14 days. After the trial license is expired, you must install a standard license to continue using AmpCon-DC.

- **Standard license**: After a standard license is installed, you cannot install a trial license.

Deploying AmpCon-DC

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

See the following child topics:

- Installing the AmpCon-DC Server
- Upgrading the AmpCon-DC Server
- Uninstalling the AmpCon-DC Server

Installing the AmpCon-DC Server

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

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

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

For more information, see Multi-NIC Deployment for Switch Connectivity.

NOTEs

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

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

10.8.0.0/20.

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

Installing on VMware ESXi

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

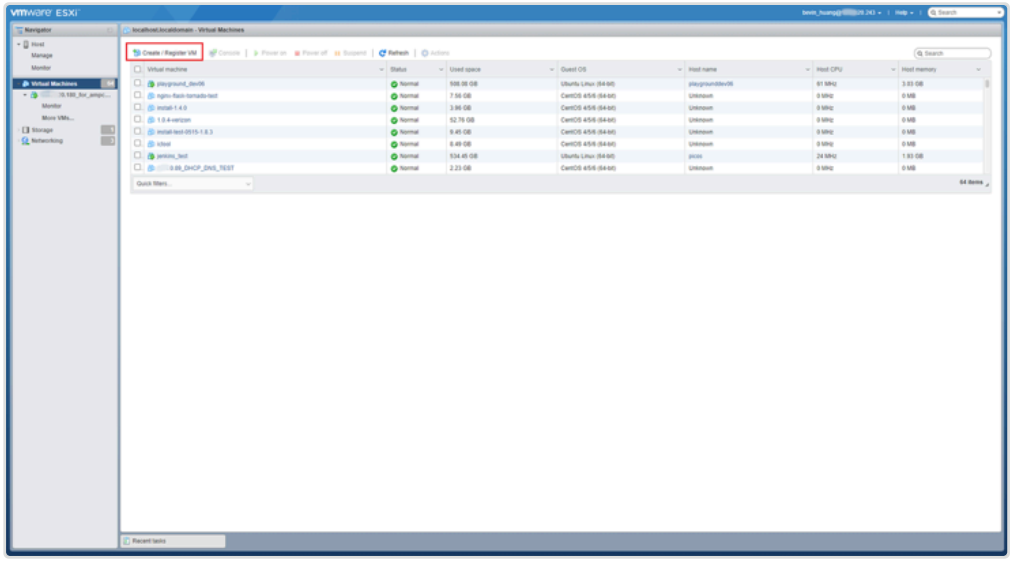
Prerequisites
Installation Procedure
What to Do Next

Prerequisites

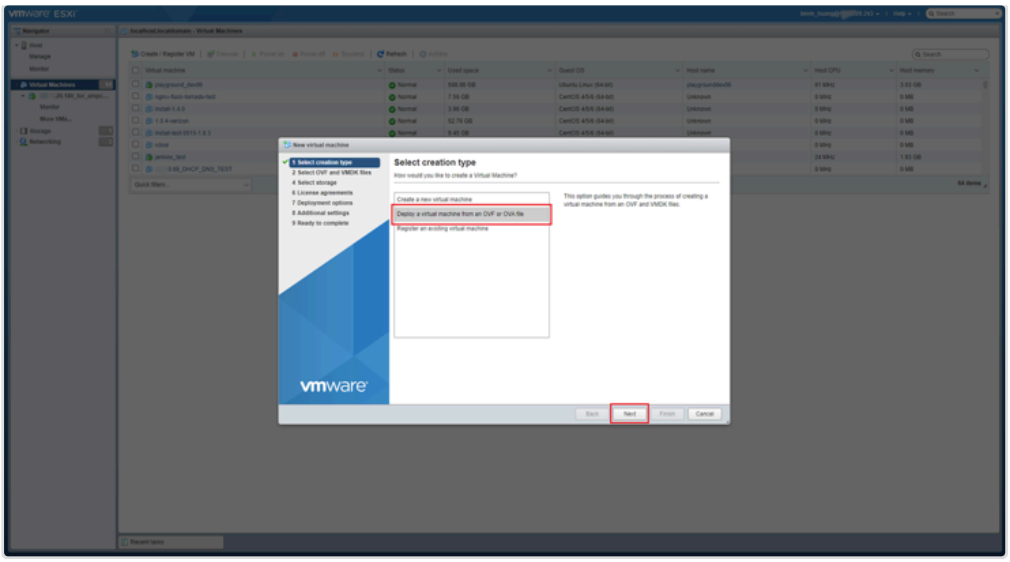
- Ensure that the installation requirements are met.
- Download the compressed AmpCon-DC server image **AmpCon-DC for VMWare ESXi V2.5.x Software** from the FS AmpCon-DC website.
- Put the compressed AmpCon-DC server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

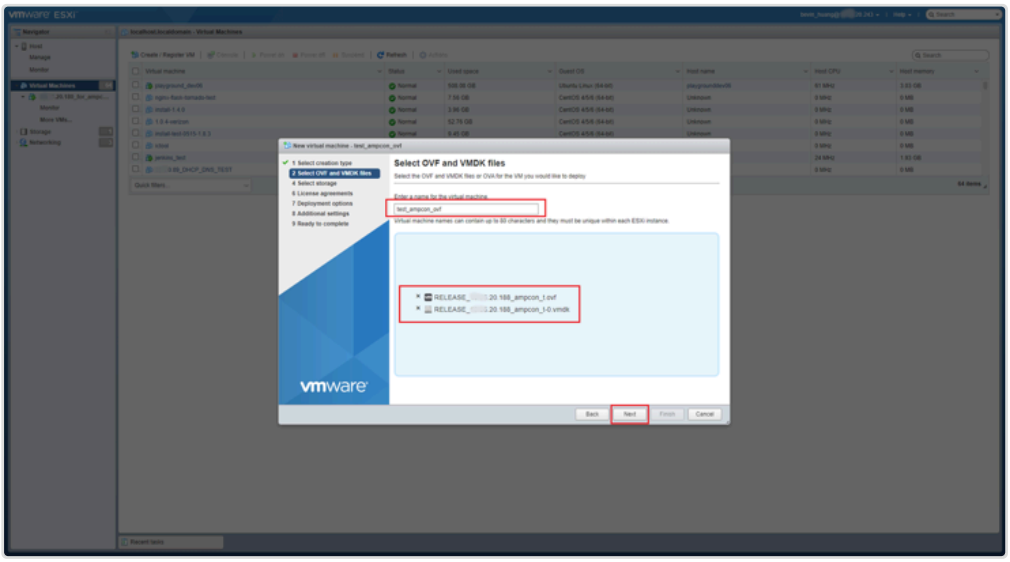
1. Open the VMware ESXi console, and then click **Create / Register VM**.



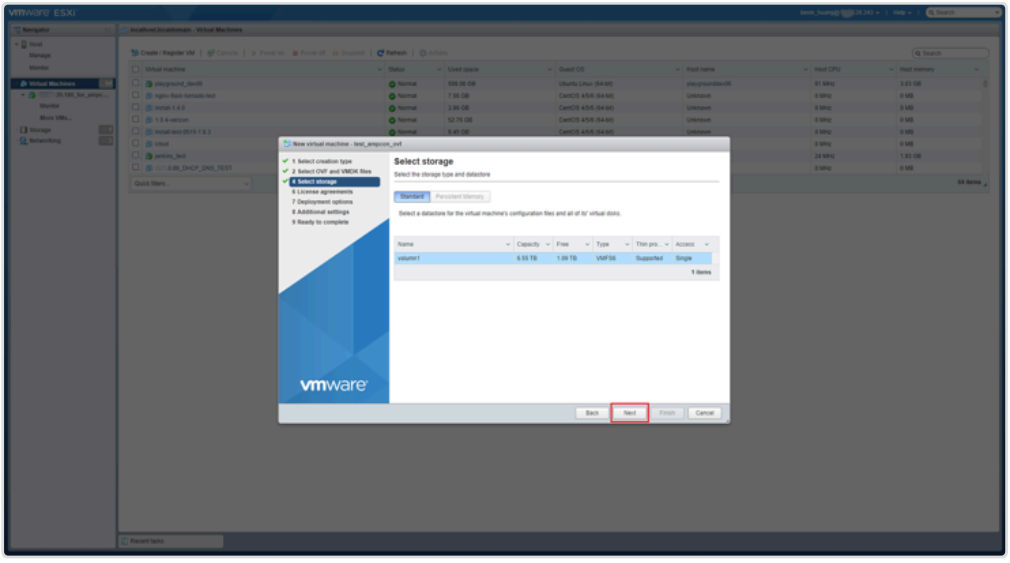
2. Select **Deploy a virtual machine from an OVF or OVA file**, and then click **Next**.



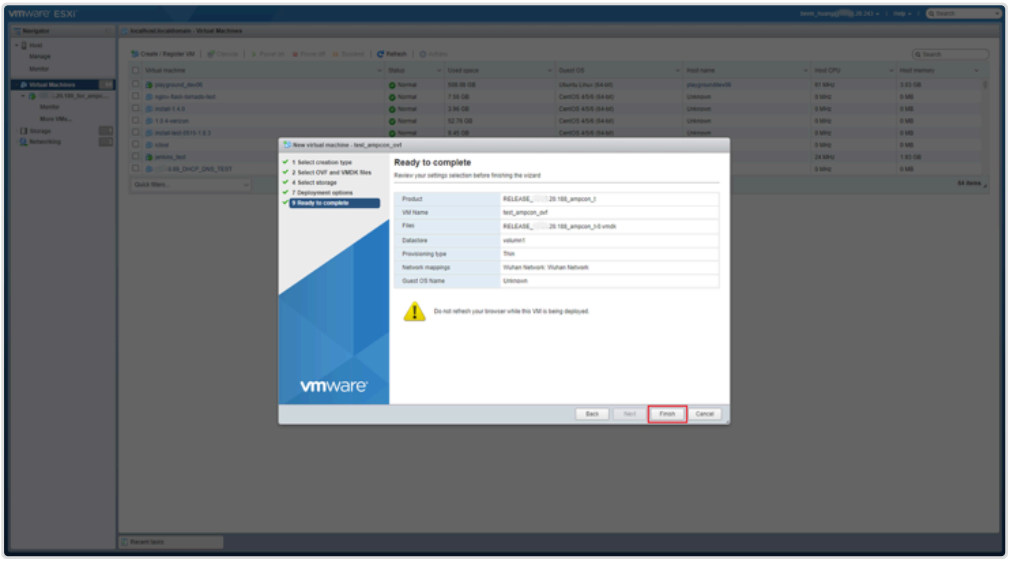
3. Enter the virtual machine name, upload the AmpCon-DC server .ovf and .vmdk files, and then click **Next**.



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



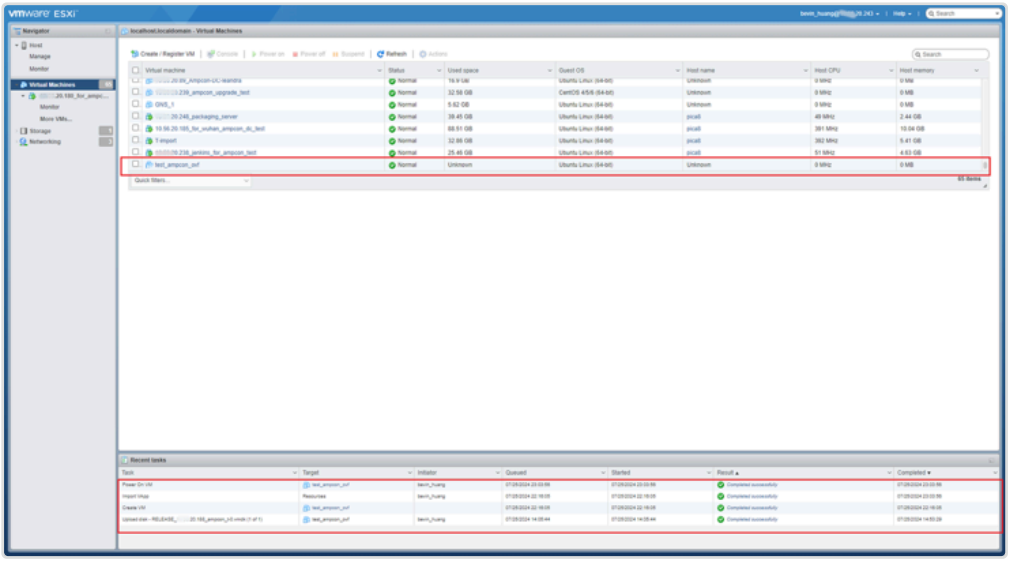
5. In the **Network mappings** drop-down list of the **Deployment Options** window, select the network adapter to which the virtual machine is connected, and then click **Next**.
6. Click **Finish**.



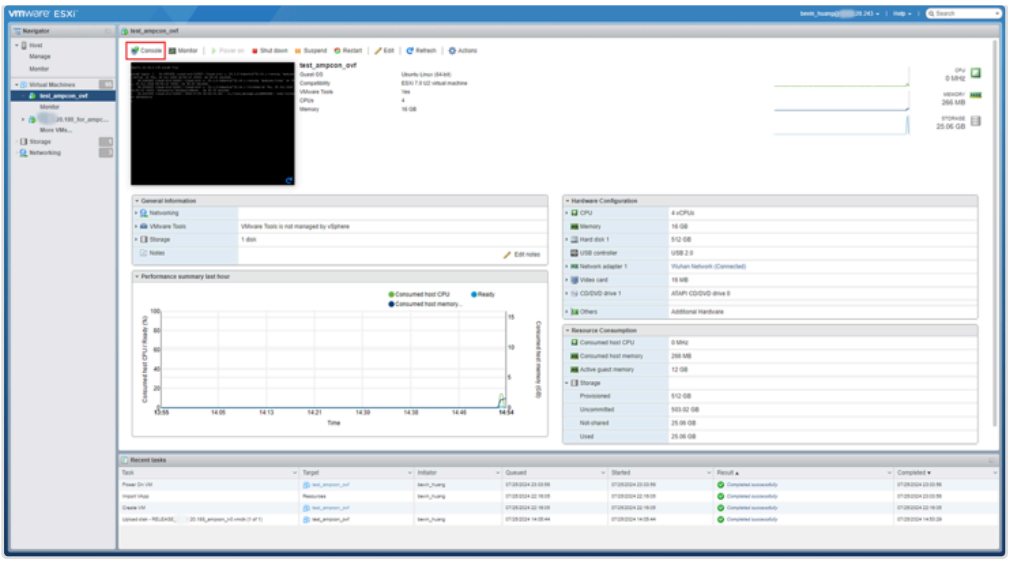
Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-DC server is installed.

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

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



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



9. Modify the network interface configuration.

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

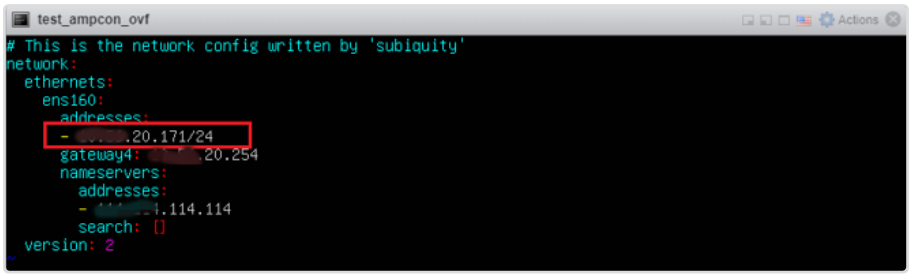
   b. Enter the 00-installer-config.yaml file by running the following command:

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

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

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

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



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

```
sudo netplan apply
```

10. Start the AmpCon-DC server:

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

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

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

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

Now the AmpCon-DC server is installed and started.

What to Do Next

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

  For more information, see Multi-NIC Deployment for Switch Connectivity.

- To stop the AmpCon-DC server, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.
  2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command.

- To start the the AmpCon-DC server after it is stopped, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.

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

Installing on QEMU or KVM

You can install the AmpCon-DC 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-DC server installation steps.

Prerequisites
Installation Procedure
What to Do Next

Prerequisites

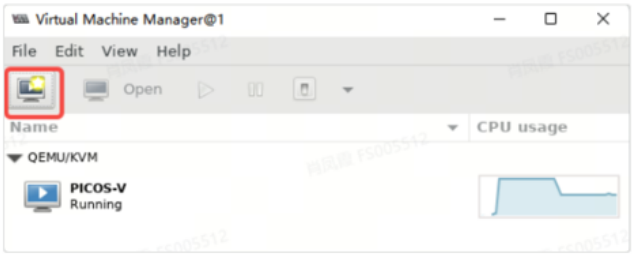
- Ensure that the installation requirements are met.
- Download the compressed AmpCon-DC server image **AmpCon-DC for QEMU/KVM V2.5.x Software** from the FS AmpCon-DC website.
- Put the compressed AmpCon-DC server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

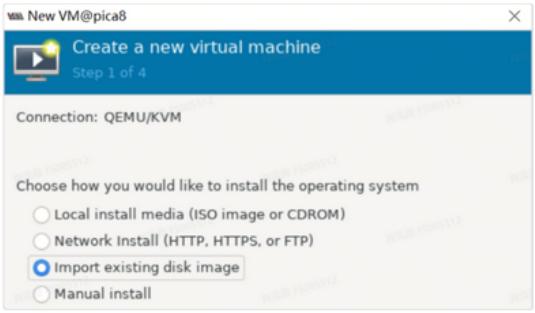
1. Open the virt-manager console by running the following command:

```
virt-manager
```

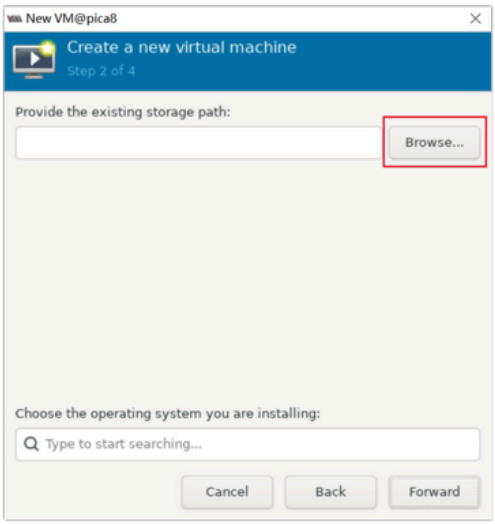
2. Click the following button to start the importing process.



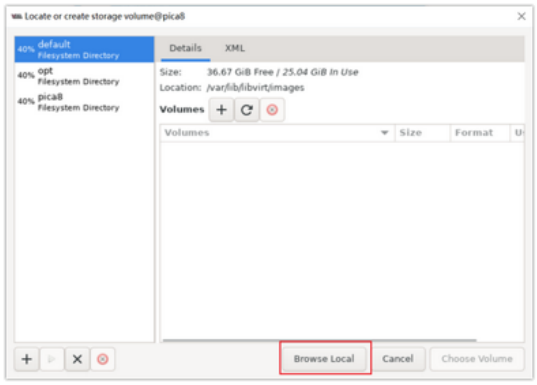
3. Select **Import existing disk image**, and then click **Forward**.



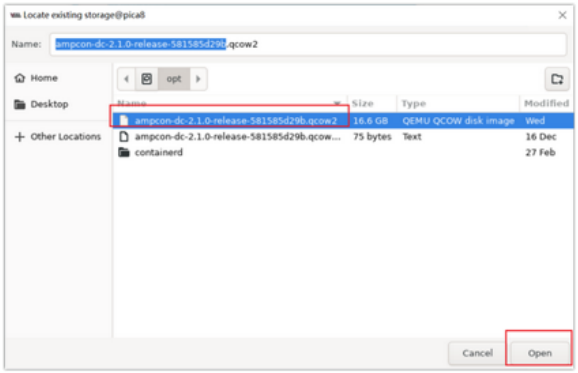
5. Click **Browse** to select the AmpCon-DC server .qcow2 image file.



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

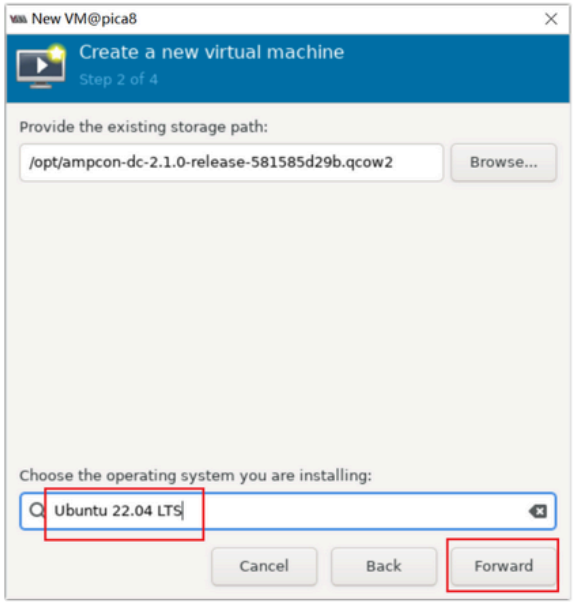


7. Find the location of the AmpCon-DC server .qcow2 image file, and then click **Open**.



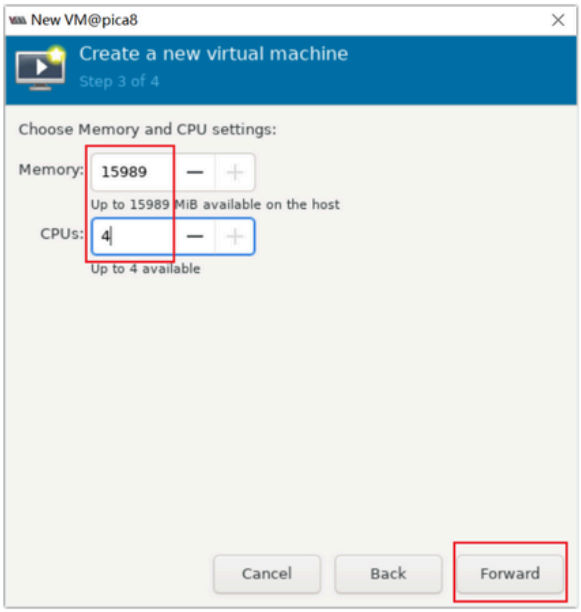
8. Select **Ubuntu 22.04 LTS**, and then click **Forward**.

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

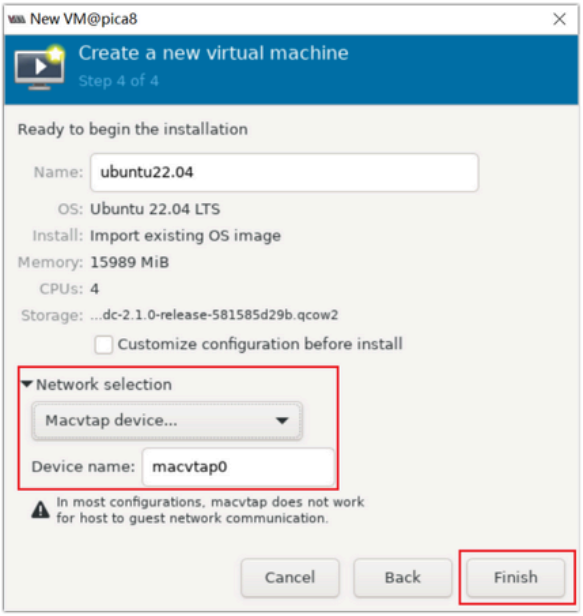


9. Adjust the memory and CPU settings as needed, and then click **Forward**.

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

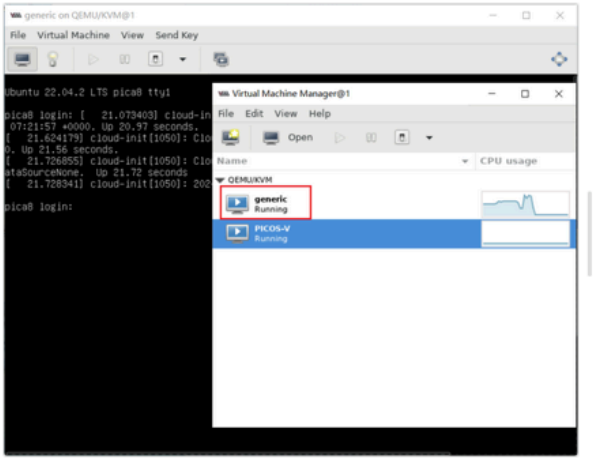


10. In the **Network selection** section, select **Macvtap device**, and enter the device name. Then, click **Finish**.



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

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



11. Modify the network interface configuration.

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

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

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

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

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

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens3:
      addresses:
      - [redacted].20.190/24
      gateway4: 1[redacted].20.254
      nameservers:
        addresses:
        - [redacted].114.114
        search: []
  version: 2
```

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

```
sudo netplan apply
```

12. Start the AmpCon-DC server:

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

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

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

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

Now the AmpCon-DC server is installed and started.

What to Do Next

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

  For more information, see Multi-NIC Deployment for Switch Connectivity.

- To stop the AmpCon-DC server, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.
  2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command.

- To start the the AmpCon-DC server after it is stopped, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.
  2. Start the AmpCon-DC server by running the **sudo ./start.sh** command.

Installing on VirtualBox for Lab Only

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

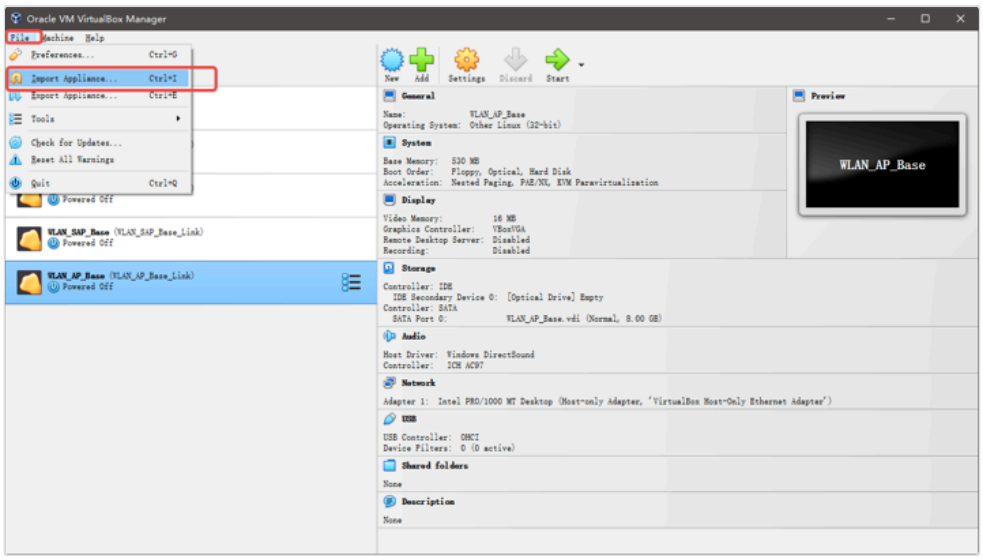
Prerequisites
Installation Procedure
What to Do Next

Prerequisites

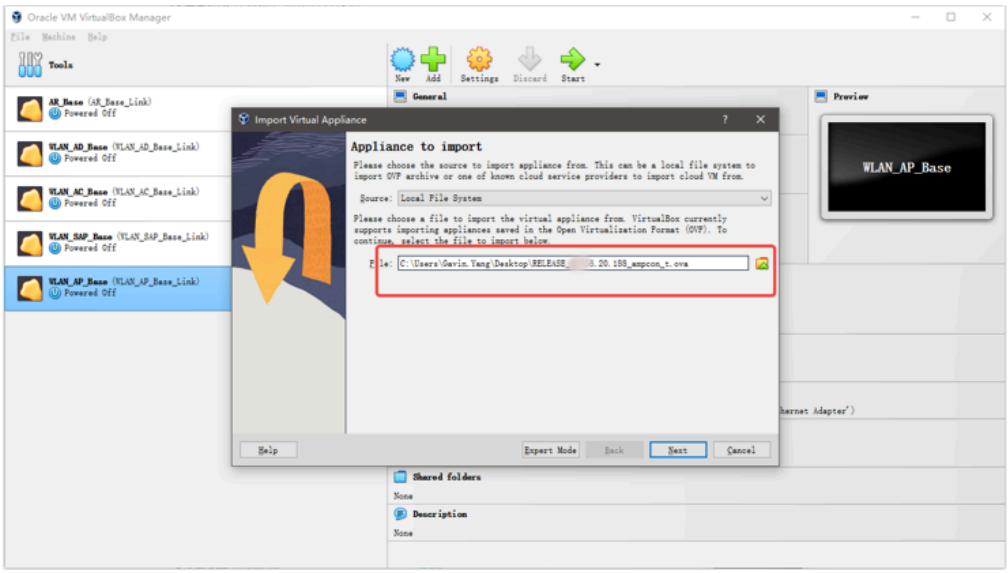
- Ensure that the installation requirements are met.
- Download the compressed AmpCon-DC server image **AmpCon-DC for VirtualBox V2.5.x Software** from the FS AmpCon-DC website.
- Put the compressed AmpCon-DC server image file to the machine where the hypervisor exists, and unzip the file.

Installation Procedure

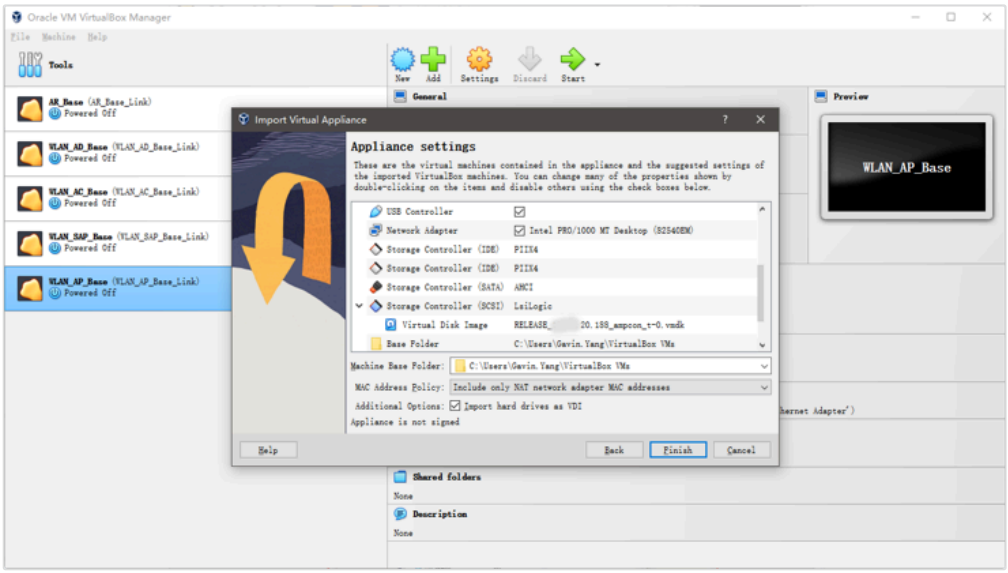
1. Open the VirtualBox console, and then click **File > Import Appliance**.



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

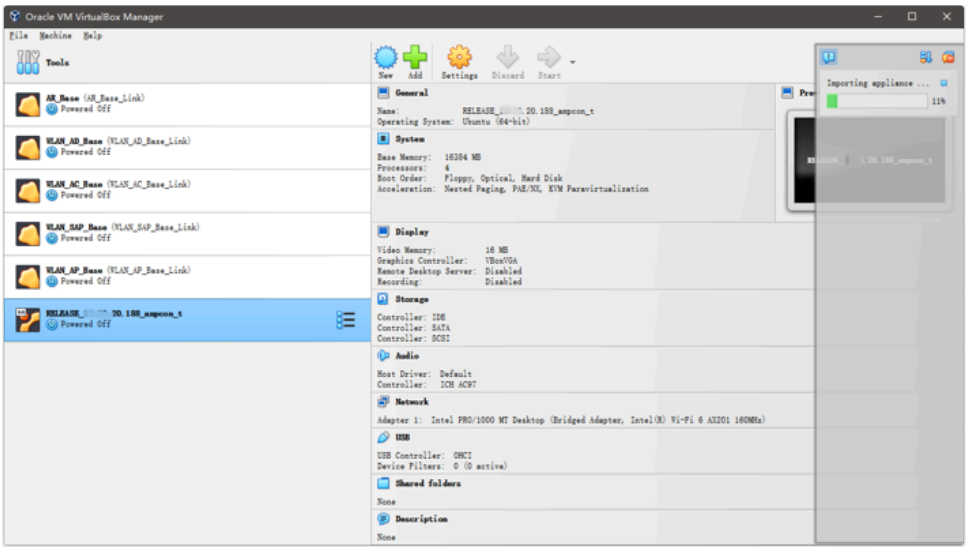


3. Confirm the settings for the .ova file, and then click **Finish**.

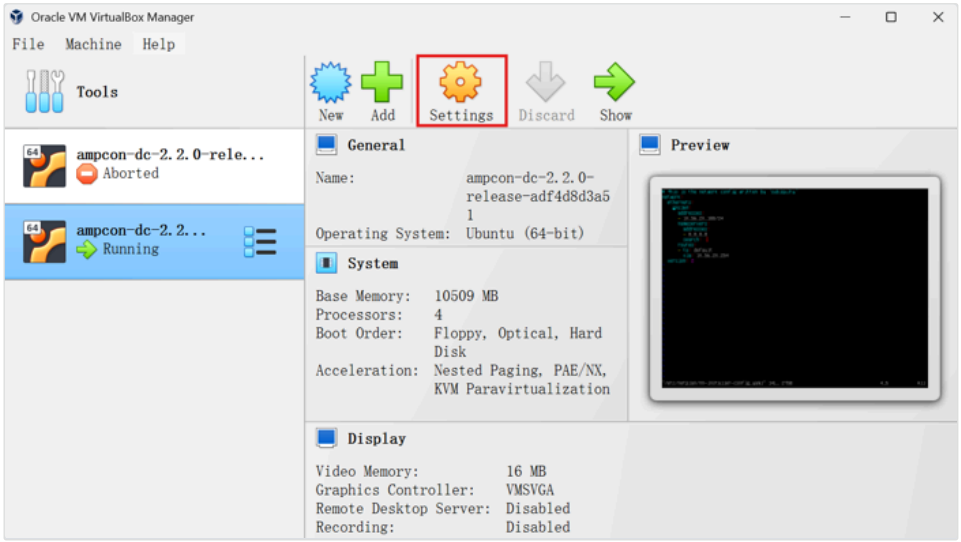


Wait for the importing process to finish. Once completed, the virtual machine is successfully imported, and the AmpCon-DC server is installed.

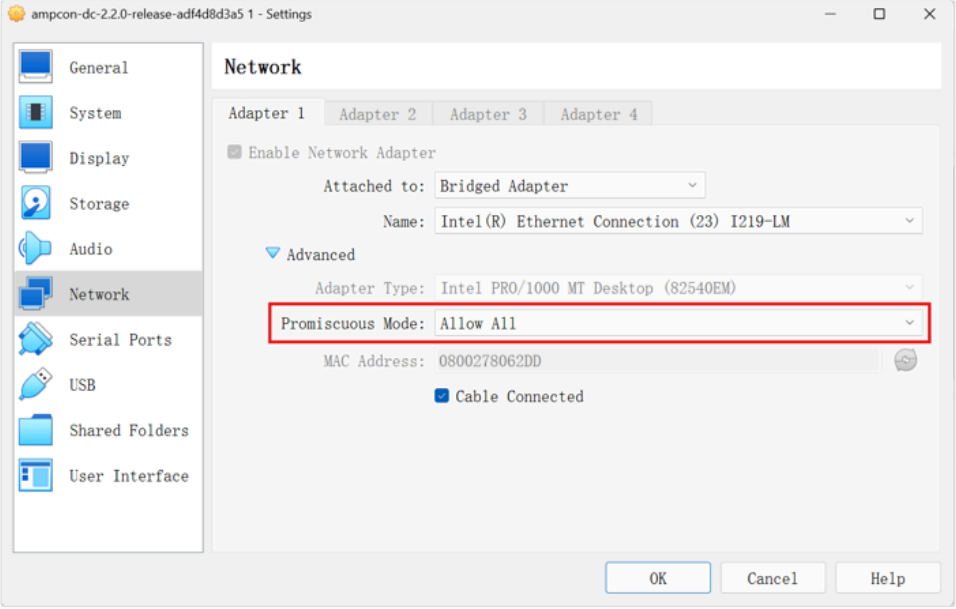
> **NOTE**
>
> The AmpCon-DC server is installed in the /usr/share/automation/server directory. Currently, you can't customize the installation directory.



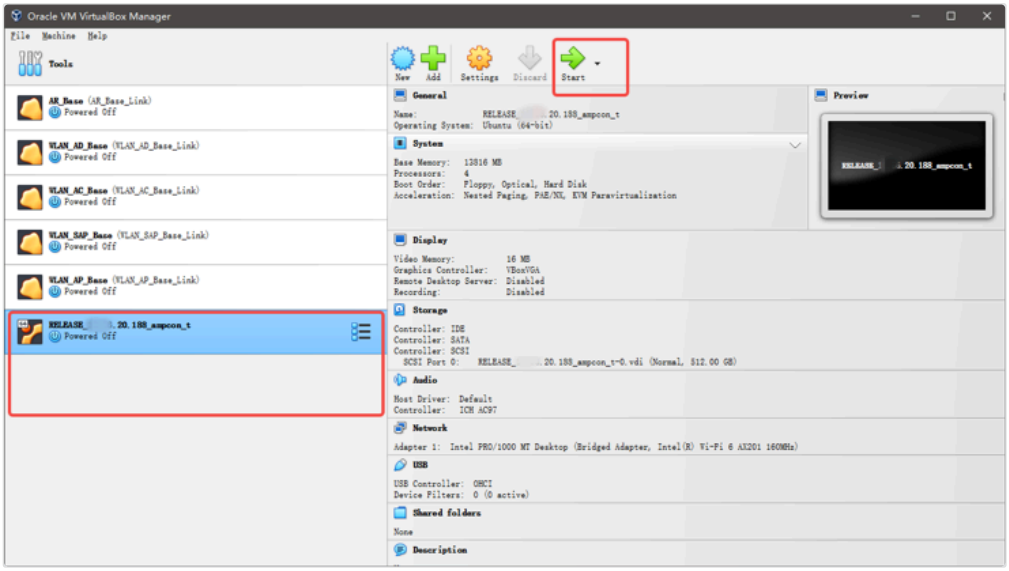
4. Click **Settings**, and then check the settings of the imported virtual machine.



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



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



6. Modify the network interface configuration.

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

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

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

   c. Modify the IP address in the 00-installer-config.yaml file with the real IP address of the virtual machine.

> **NOTE**

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



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

```
sudo netplan apply
```

7. Start the AmpCon-DC server:

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

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

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

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

Now the AmpCon-DC server is installed and started.

What to Do Next

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

  For more information, see Multi-NIC Deployment for Switch Connectivity.

- To stop the AmpCon-DC server, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.

2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command.

- To start the the AmpCon-DC server after it is stopped, follow the steps:

  1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.

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

Installing on Physical Machines (Ubuntu Docker)

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

Prerequisites
Installation Procedure
What to Do Next

Prerequisites

- Prepare a physical machine based on Ubuntu 22.04 LTS with Docker installed.
- Ensure that the installation requirements are met.
- Download the AmpCon-DC server installation package **AmpCon-DC for Ubuntu Docker V2.5.x Software** from the FS AmpCon-DC website.

Installation Procedure

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

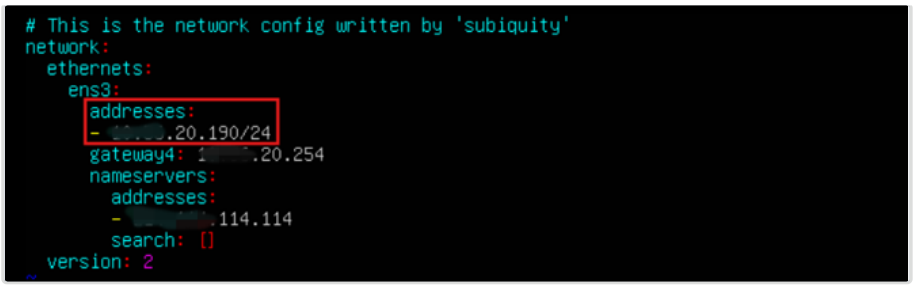
   Extract the generated .tar.gz file by running the **tar -zxvf <*extracted_tar_file_name*>.tar.gz** command. A directory is generated with AmpCon-DC server installation files.

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

2. On the physical machine, modify the network interface configuration as follows:

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

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



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

```
sudo netplan apply
```

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

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

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

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

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

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

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

What to Do Next

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

  For more information, see Multi-NIC Deployment for Switch Connectivity.

- To stop the AmpCon-DC server, follow the steps:

1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.
2. Stop the AmpCon-DC server by running the **sudo ./stop.sh** command.

- To start the the AmpCon-DC server after it is stopped, follow the steps:

1. Go to the AmpCon-DC installation directory by running the **cd /usr/share/automation/server** command.
2. Start the AmpCon-DC server by running the **sudo ./start.sh** command.

Multi-NIC Deployment for Switch Connectivity

As described in Installing the AmpCon-DC Server, you need to import the AmpCon-DC image file to a virtual machine or unzip the AmpCon-DC installation packet file on a physical machine to install the AmpCon-DC server.

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

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

> **NOTEs**
>
> - When you install the AmpCon-DC server on a virtual machine, the imported AmpCon-DC image file contains only one Network Interface Card (NIC). But you can manually add more NICs.
> - When you install the AmpCon-DC server on a physical machine, the AmpCon-DC installation package file is not an image file, and thus no NIC is contained in the file. But you can manually add one or multiple NICs to the physical machine.

Prerequisite
Procedure

Prerequisite

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

Procedure

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

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

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

```
PRO_TYPE=ampcon-dc
PROD_IP=
BUILD_PATH=dist
GENERATE_SOURCEMAP=false
REACT_APP_PRE_VERSION=5f9ad5aae4
REACT_APP_VERSION=20caaa33c5
REACT_APP_BRANCH=2.3.0-dev
REACT_APP_MAJOR_VERSION=2.2.0
IMG_CENTER_PROXY_DOMAIN=harbor.ampcon.com/ampcon-t-base
IMG_CENTER_PROXY_IP=10.56.20.229
```

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

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

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

Troubleshooting for Server IP Changes

When you install the AmpCon-DC server, you designate the IP address of the AmpCon-DC server in the /etc/netplan/00-installer-config.yaml file.

However, for the physical or virtual machine where the AmpCon-DC server is installed, if its IP address is changed after the AmpCon-DC server is installed, the AmpCon-DC server can't work, and the managed switches can't connect to the AmpCon-DC server.

In this case, follow these steps to make AmpCon-DC work again:

> **NOTE**
>
> Only when you meet the problem above, can you follow these steps.

Prerequisites
Procedure

Prerequisites

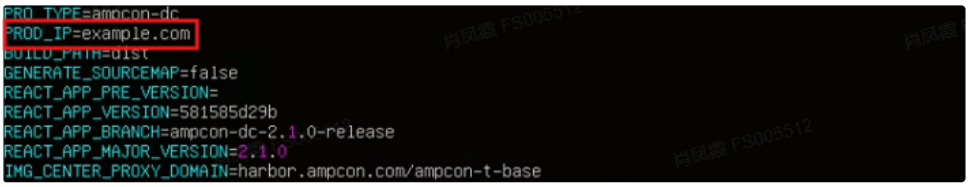
- Ensure that a static IP address is used by the physical or virtual machine where the AmpCon-DC server is installed.
- On the physical or virtual machine where the AmpCon-DC server is installed, ensure that you have modified the IP address with the real IP address of the physical machine in the /etc/netplan/00-installer-config.yaml file. Or else, AmpCon-DC can't work.
- Ensure that each managed switch is able to connect to the new IP address of the AmpCon-DC server.

Procedure

1. Log in to the virtual machine or the physical machine, and then open the /usr/share/automation/server/.env file by running the following command:

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

2. Locate the line containing **PROD_IP=** in the .env file, and then add the new IP address or domain name of the AmpCon-DC server machine. See the following configuration example:



Replace *example.com* with the real IPv4 address or domain name of the AmpCon-DC server machine.

> **NOTE**
>
> If you use a domain name, pay attention to the following notes. Or else, AmpCon-DC can't work.
>
> - On the DNS server, you need to point the domain name to the new IP address.
> - Ensure that you have an available DNS server used for domain name resolution or you have a purchased public domain name for the AmpCon-DC server.
> - Ensure that each managed switch is able to connect to the domain name of the AmpCon-DC server.

3. Go to the /usr/share/automation/server directory by running the following command:

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

4. Restart the AmpCon-DC server by running the following command:

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

5. Remove all managed switches from AmpCon-DC. For more information, see Removing Switches.
6. Import these switches to AmpCon-DC. For more information, see Importing Switches.

After you import the switches successfully, these switches will be managed by AmpCon-DC.

Upgrading the AmpCon-DC Server

To upgrade the AmpCon-DC server to 2.5.0 or 2.5.1, see the following upgrading path and procedure.

Upgrading Path
Upgrading Procedure

Upgrading Path

If the AmpCon-DC server that you are using is 2.1.x (2.1.0, 2.1.1, or 2.1.2), 2.2.x (2.2.0, 2.2.1, or 2.2.2), or 2.4.0, you can upgrade it to 2.5.0 or 2.5.1.

Upgrading Procedure

1. Download the AmpCon-DC server upgrade package **Software Upgrade Package for AmpCon-DC V2.5.0** or **Software Upgrade Package for AmpCon-DC V2.5.1** from the FS AmpCon-DC website. Then, the upgrade package will be downloaded to your local machine.
2. Copy the upgrade package to the AmpCon-DC server machine, and then extract the package by running the following command:

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

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

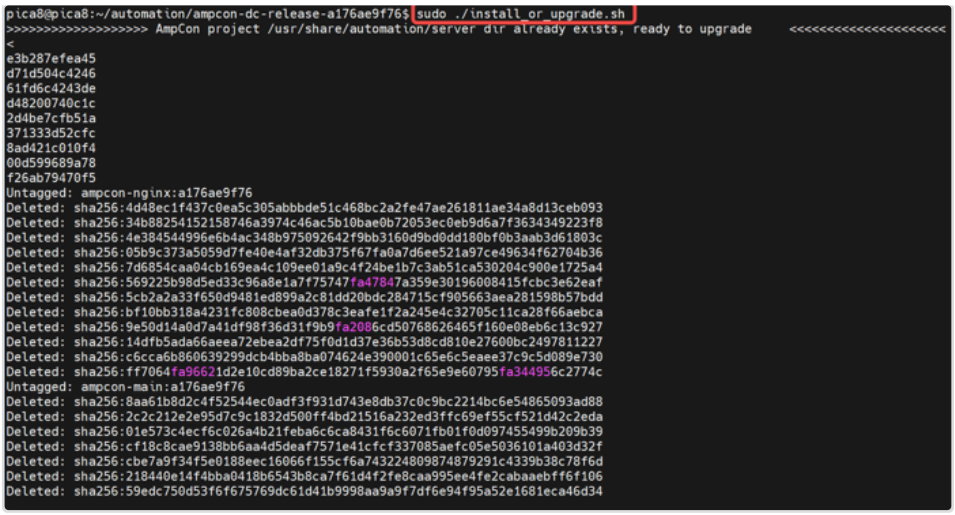
   Then, a .tar.gz file is generated in the current directory.

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

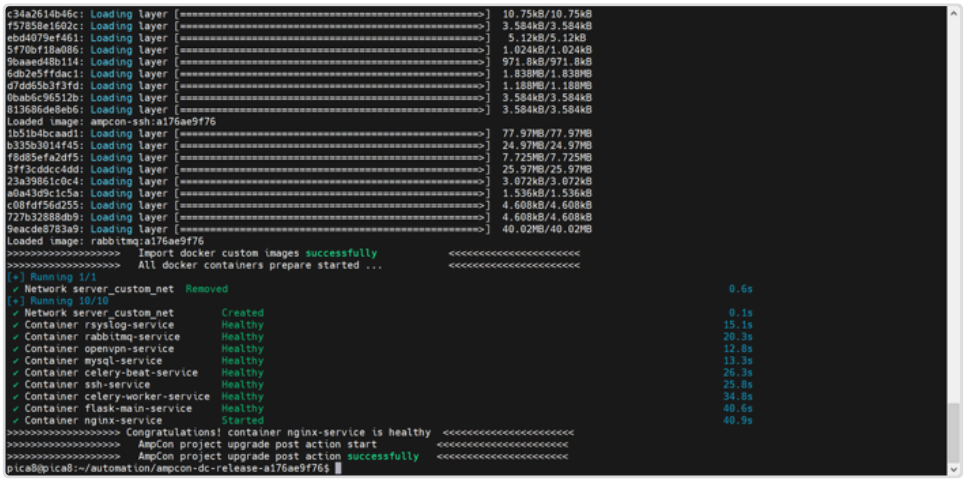
   ```
   tar -zxvf <extracted_tar_file_name>.tar.gz
   ```

   Replace *<extracted_tar_file_name>* with the real extracted .tar.gz file name.
3. After extracting the .tar.gz file, go to the extracted directory, and then run the following upgrade command:

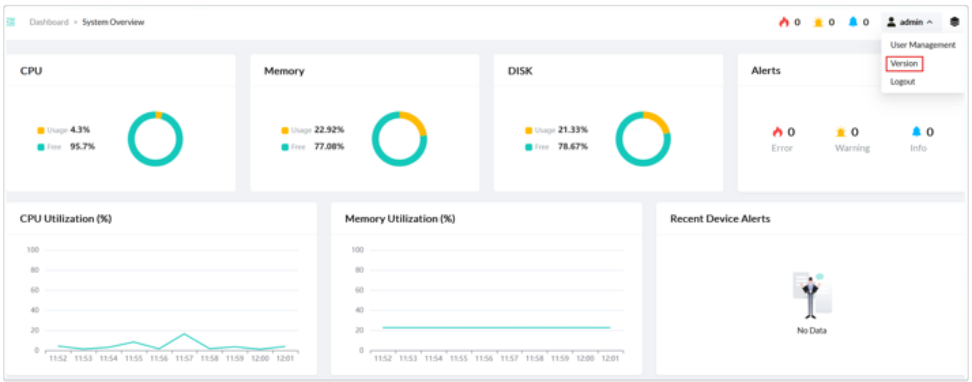
   ```
   sudo ./install_or_upgrade.sh
   ```



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



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



Uninstalling the AmpCon-DC Server

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

Procedure

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

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

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

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

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

Working with the User Interface

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

Prerequisites
Logging In
Logging Out
UI Overview
UI Conventions

Prerequisites

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

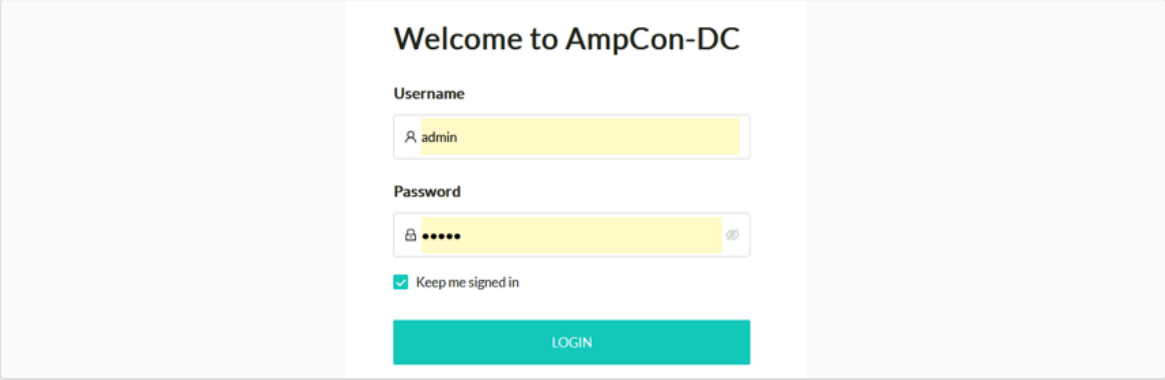
- The network connection between your local computer and the AmpCon-DC server is available, and the AmpCon-DC server is started and running properly.
- To use the Terminal Access Controller Access Control System (TACACS+) server for authentication and authorization of AmpCon-DC login users, enable the TACACS+ integration first. Fore more information, see Configuring TACACS+ Authentication and Authorization.
- You have obtained the AmpCon-DC username and password for login.
  - The first time you log in to the AmpCon-DC UI, use the default username **admin** and password **admin**.
  - The user **admin** has all operation permissions on AmpCon-DC. For security purposes, change the password upon the first login, update it periodically, and keep it secure. For how to update the password, see User Self-Management.
  - You can also add other users as needed. For more information, see Managing User Access.

Logging In

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

1. In a web browser, enter the URL of the AmpCon-DC server in the format of "https://*<AmpCon-Server-IP-or-Domain-Name>*/login".

   Replace *<AmpCon-Server-IP-or-Domain-Name>* with the IP address or domain name of the AmpCon-DC server.
2. In the **Username** field, enter the username of an AmpCon-DC user.
3. In the **Password** field, enter the password of the AmpCon-DC user.



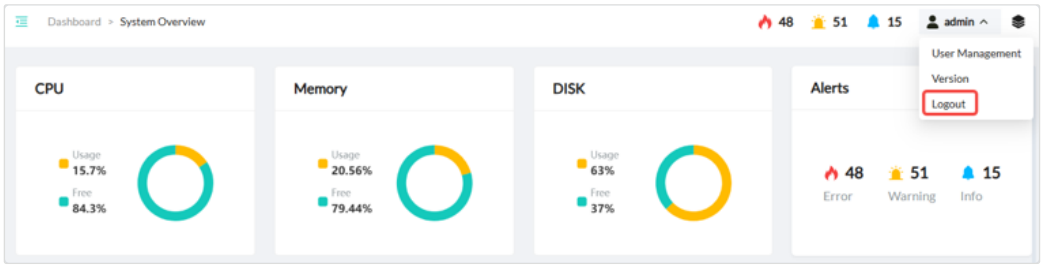
4. Optional: Select **Keep me signed in** to extend the allowed inactivity time of the AmpCon-DC UI.

- If **Keep me signed in** is not selected, your session will be logged out after 30 minutes of inactivity in the AmpCon-DC UI.
- If **Keep me signed in** is selected, your session will be logged out after 365 days of inactivity in the AmpCon-DC UI.
- If AmpCon-DC services are restarted, all AmpCon-DC UI sessions will be logged out.

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

Logging Out

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

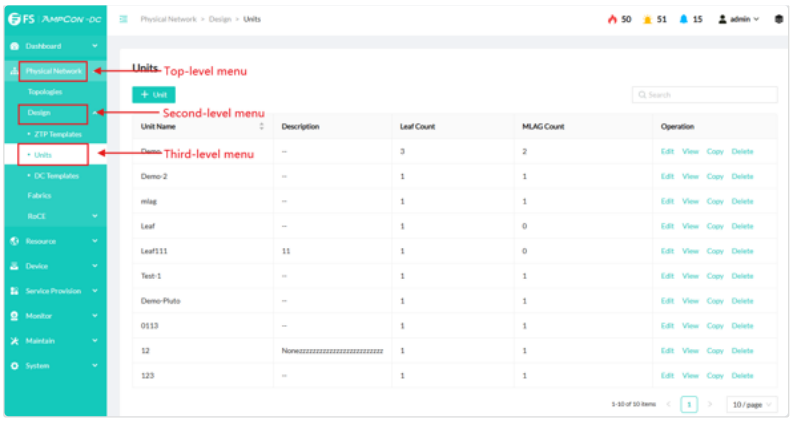


UI Overview

On the homepage, you can see the following sections:

Table 1. Homepage Descriptions

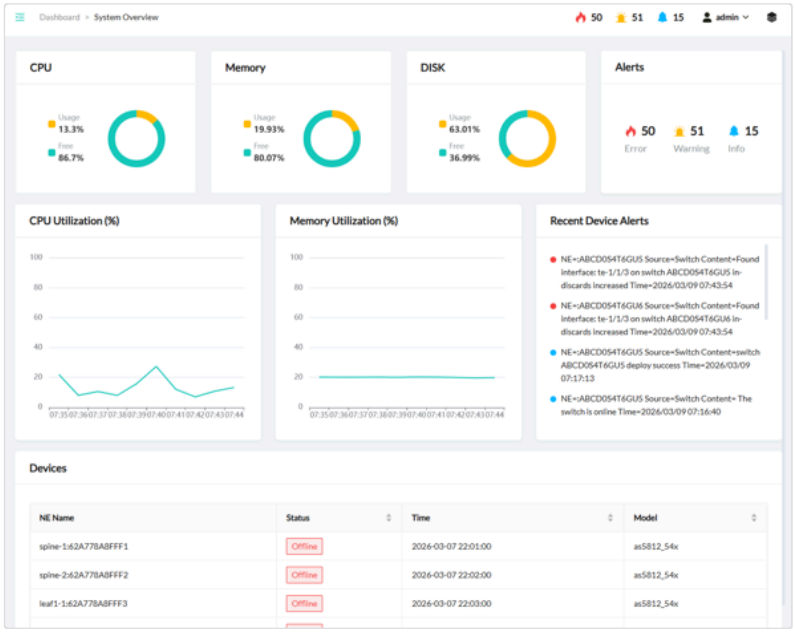
Section	Description
Navigation Bar	Click the top-level menu, and then you can see the second-level menu. If a function is located in the third-level menu, click the third-level menu.



Page

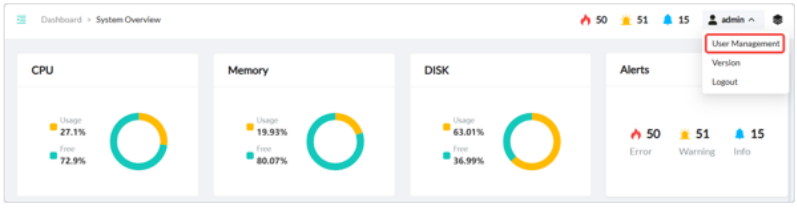
After you click a second-level or third-level menu from the navigation bar, you can see a specific page on the right.

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

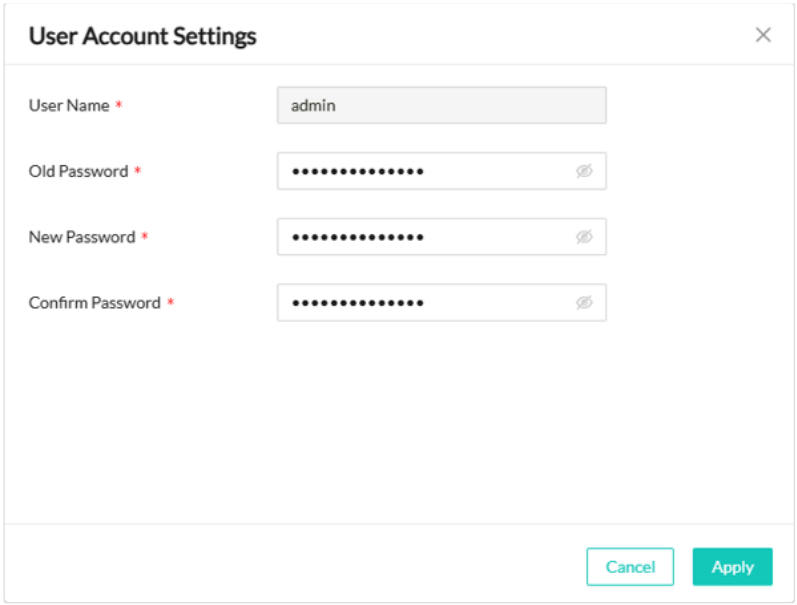


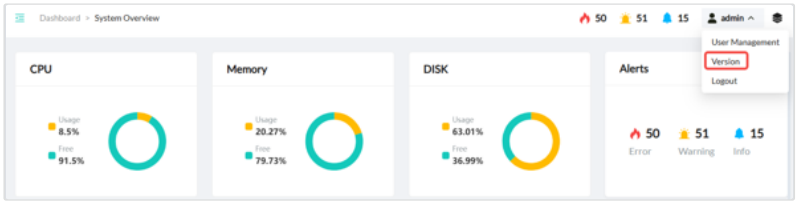
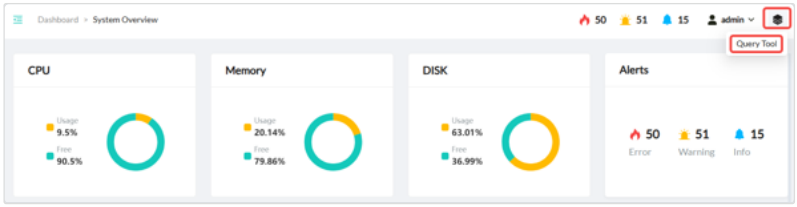
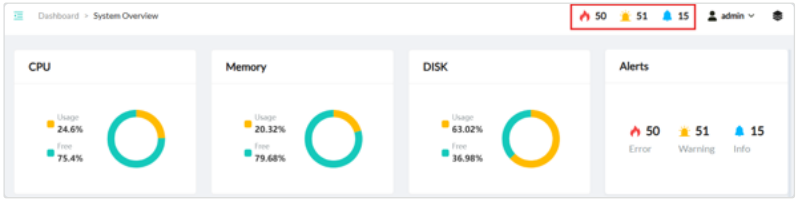
User Management

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



In the pop-up window, you can change the user password.



Version	Hover your mouse over the username at the top right corner of the homepage, and then click **Version**.  In the pop-up window, you can see the current AmpCon-DC version. Click **Release notes for AmpCon-DC** to check the AmpCon-DC Release Notes.
Query Tool	Hover over the Query Tool icon at the top right corner of the homepage, and then click **Query Tool**.  Then, you will be redirected to the FS Query Tool page.
Alert	Check the total number of alerts in the **Critical** (also called **Error**), **Info**, or **Warning** level. 

	For the definition of each alert level, see Alert Types and Levels.

UI Conventions

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

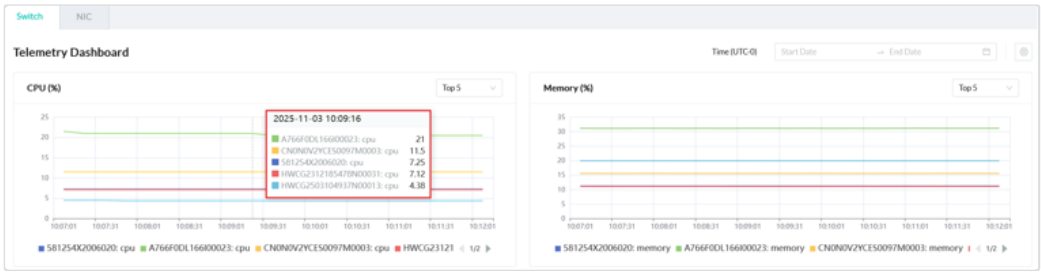
UI Conventions

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

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

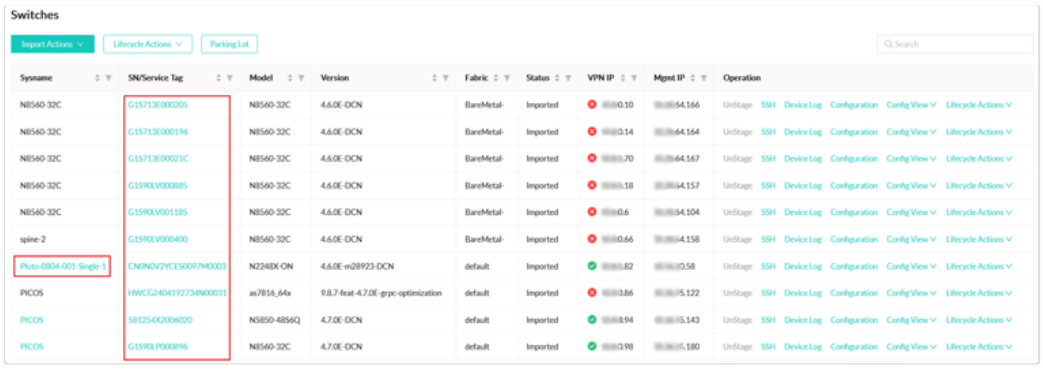
Graph

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



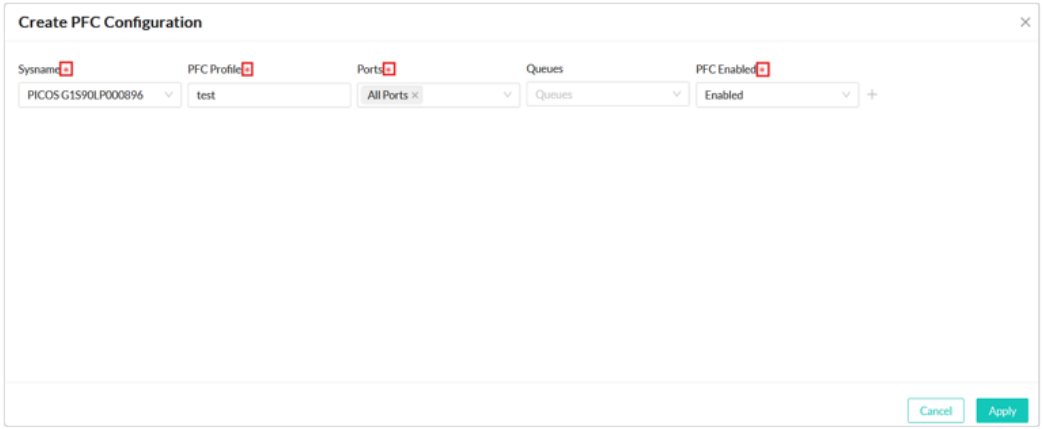
Highlighting

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



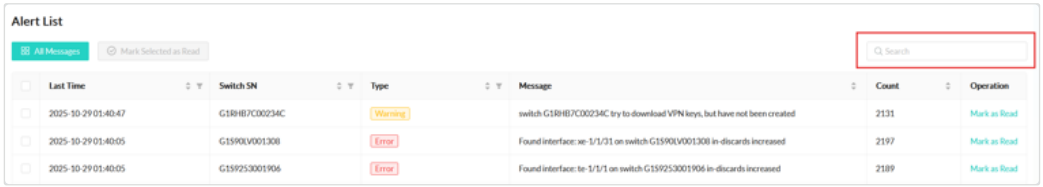
Mandatory Configurations

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



Search

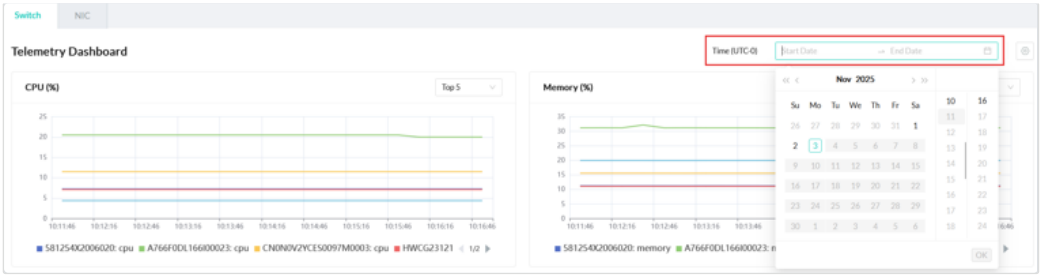
Some pages have the search box. Enter keywords in the search box to display only the information that you need.



Time Selection

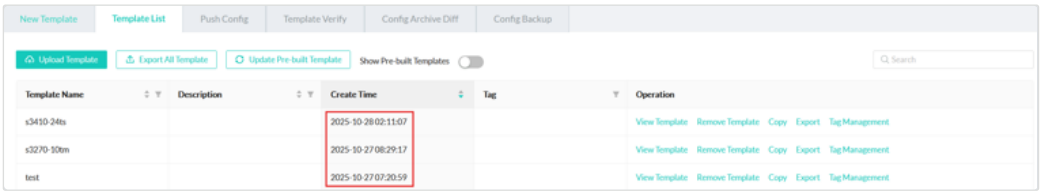
Some pages have the time selection box. Select the start date and end date to display only the data in the selected time range.

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



Time Zone

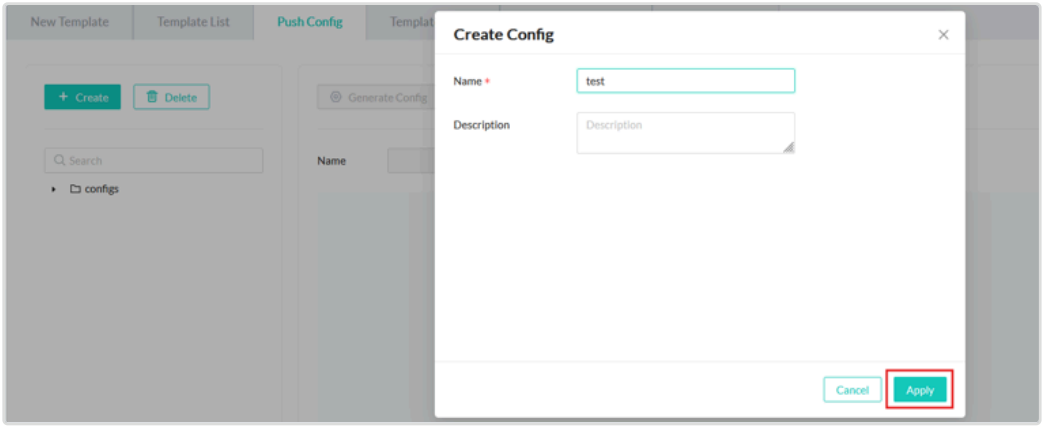
All times displayed in the AmpCon-DC UI are in the UTC+0 time zone.



General Buttons

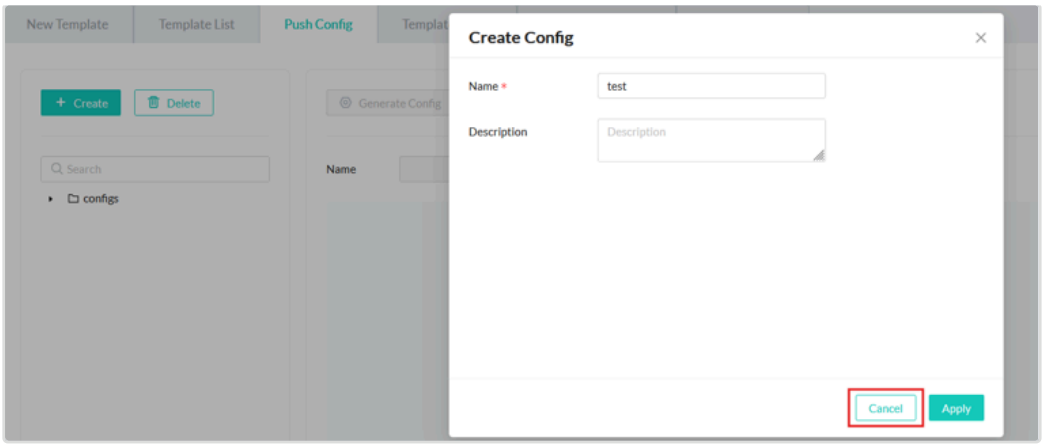
Apply Button

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



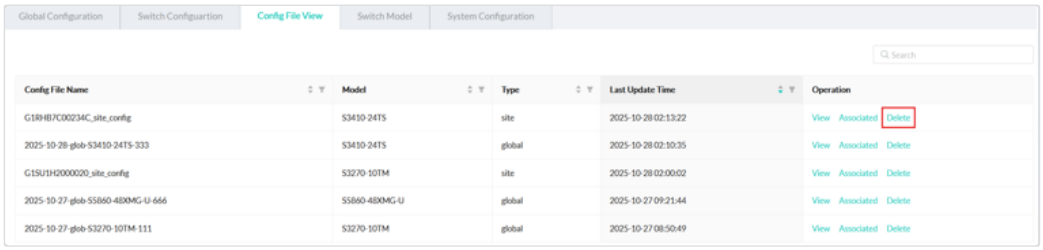
Cancel Button

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



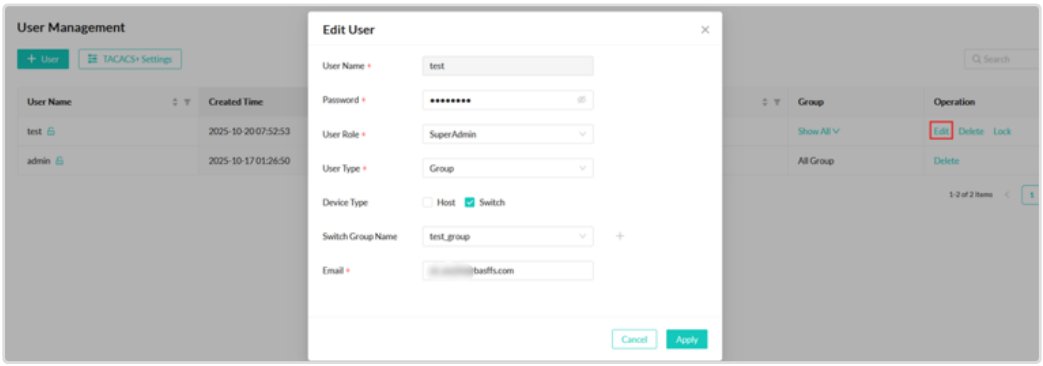
Delete Button

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



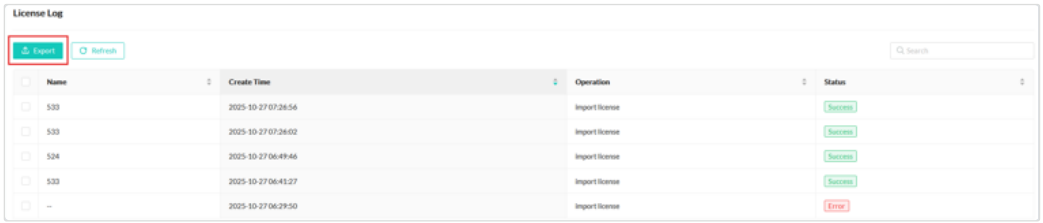
Edit Button

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



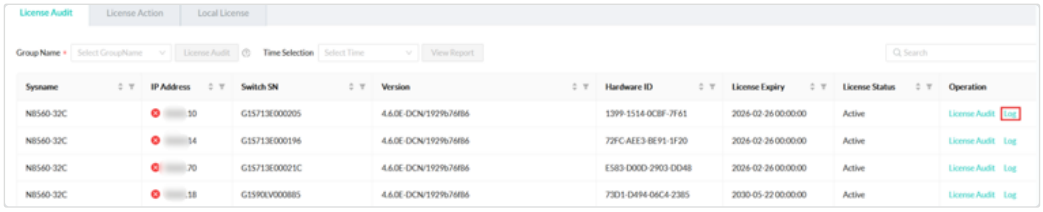
Export Button

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



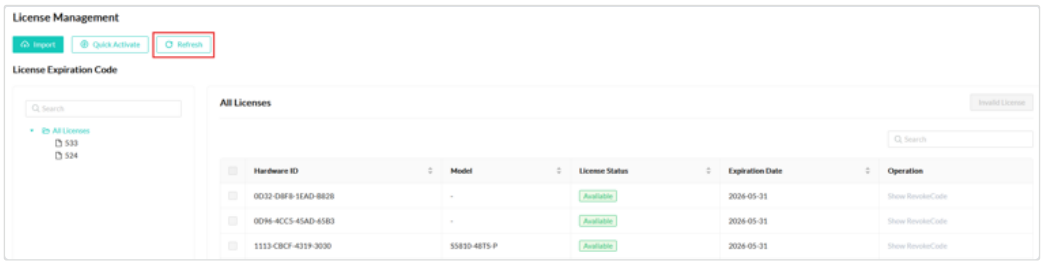
Log Button

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



Refresh Button

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



View Button

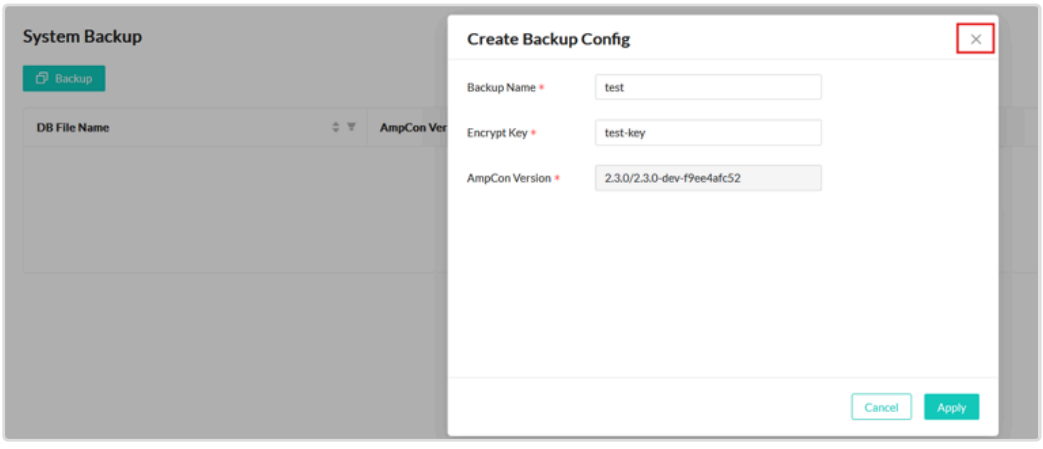
Some pages have the **View** button. Click the button to view data.



General Icons

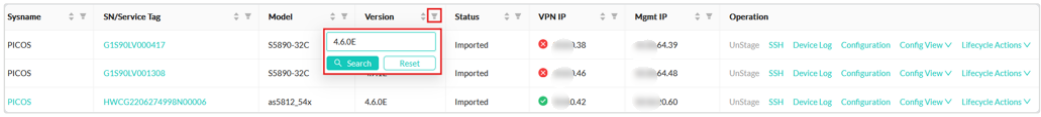
Close Icon

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



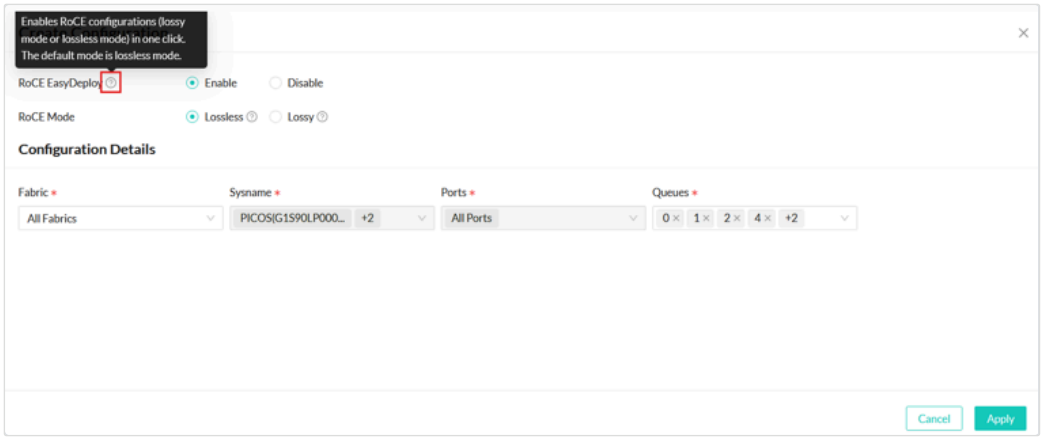
Filter Icon

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



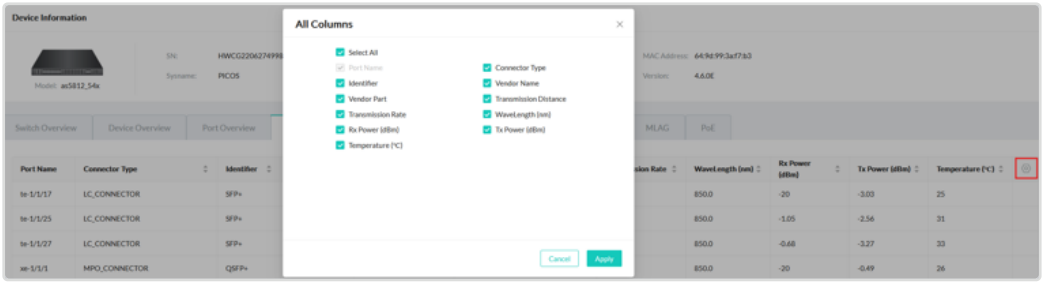
Help Icon

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



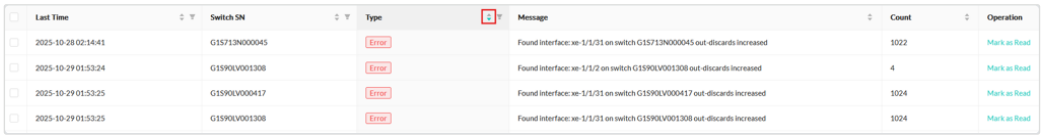
Metric Selection Icon

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



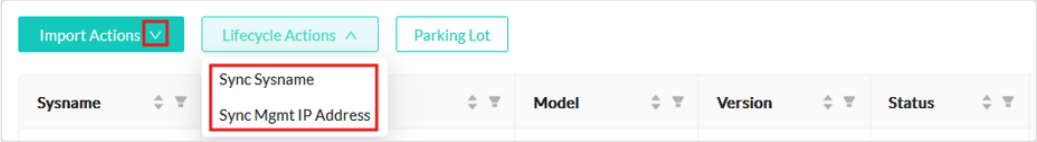
Sort Icon

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

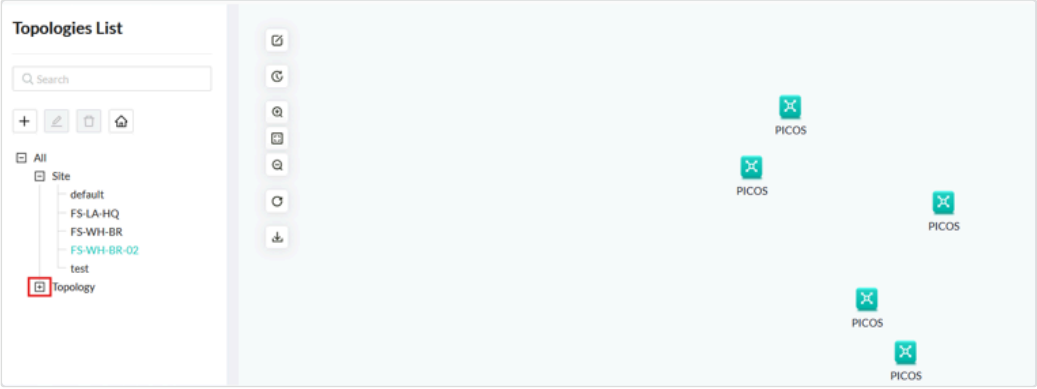


Unfold Icon

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



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



Onboarding Switches

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

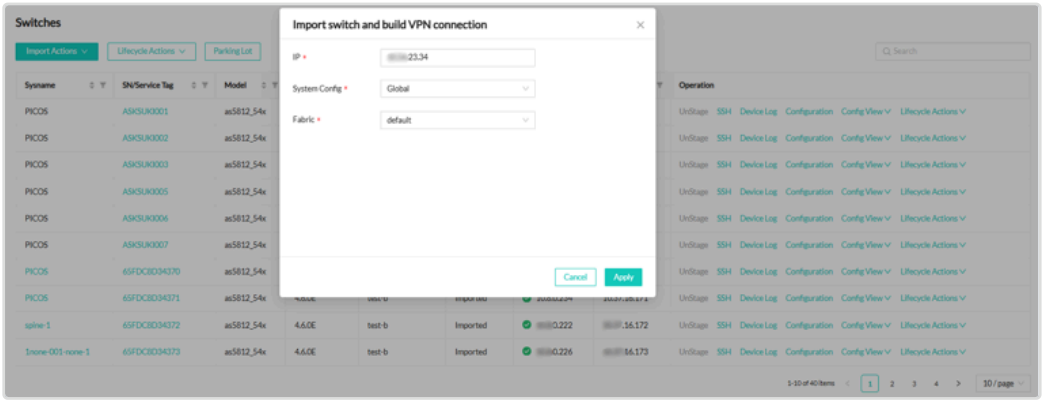
Zero Touch Provisioning (ZTP) is a technology for automated deployment and configuration of network devices without manual intervention. AmpCon-DC supports two ZTP methods: normal ZTP and simplified ZTP.

You can onboard switches through the following options:

Option 1: Importing Switches
Option 2: Deploying Switches through Normal ZTP
Option 3: Simplified ZTP

Option 1: Importing Switches

If the switches to be managed have PicOS installed, you can import these switches to AmpCon-DC directly. For more information, see Importing Switches.



Option 2: Deploying Switches through Normal ZTP

Normal ZTP is a ZTP method to onboard switches. If the switches to be managed don't have PicOS installed, or though the switches have PicOS installed but you want to use a ZTP method to onboard these switches, you can deploy these switches through normal ZTP.

For more information, see Deploying Switches through Normal ZTP.

NOTEs

- Importing switches is not a ZTP method, which means that you still need to connect to the switches and do some operations on the switch side, such as obtaining IP addresses from the switches. In addition, the importing switch process doesn't push switch configurations.

- Deploying switches through normal ZTP is a ZTP method used for automated deployment of switches. After you reboot the switches, AmpCon-DC will deploy the switches automatically. During the normal ZTP process, you can push pre-configured configurations to the switches.
- Integrated hardware and software switches have PicOS installed. To onboard these switches, you can import these switches to AmpCon-DC directly, or you can deploy these switches through normal ZTP.

Option 3: Simplified ZTP

Simplified ZTP is a Zero Touch Provisioning (ZTP) method used to onboard switches, deploy physical networks, and configure RoCE (optional) in one go.

The simplified ZTP process can achieve the following goals in one go:

- A physical network (fabric) is deployed automatically.
- All switches in the fabric are bulk onboarded to AmpCon-DC. You don't need to onboard each switch one by one.
- Optional: The RoCE policy configurations are applied to the switches in the fabric.

For more information, see Simplified ZTP Deployment.

NOTEs

- If you don't need to deploy physical networks, or if you want to design physical networks manually, do not use simplified ZTP.
- Simplified ZTP can be used only for switches with PicOS installed. For example, white-box switches with PicOS installed and integrated hardware and software PicOS switches.

Importing Switches

To use AmpCon-DC to manage switches that have PicOS installed, you can import these switches to AmpCon-DC automatically or manually.

Before You Begin
Import Procedure
  Automatically Importing a Switch
    Importing a Switch with a Global User
    Importing a Switch with a Group User
  Manually Importing a Switch
Checking Importing Results

Before You Begin

Before you import switches, ensure that you have completed all the following preparations. Or else, the import might fail.

- Ensure that you have get an AmpCon-DC user with the **SuperAdmin** role. For more information, see Managing User Access.
- Ensure that the switches are supported by AmpCon-DC. For more information, see Supported Switches for 2.5.0 and Supported Switches for 2.5.1.
- Ensure that the Secure Shell (SSH) protocol is enabled on the switches. SSH is enabled on PicOS switches by default.
- Ensure that the switches are able to connect to the AmpCon-DC server over the Internet.
- If a firewall is configured between AmpCon-DC and the switches, allow outbound access on the following ports to the management port of each switch.

Table 1. Network Requirement for Switches

TCP/UDP	Port
TCP	22
TCP	9339
TCP	830

- Click **Device > Device Profiles** from the navigation bar. In the **System Configuration** tab, configure the system configurations matching these switches to be imported. For more information, see Adding System Configurations.

> **NOTE**
>
> In the selected system configuration, pay attention to the following points. Or else, switches will fail to be imported.
>
> - Ensure that the entered **Device Default Login User** and **Device Default Password** are correct and can be used to log in to these switches.
> - Ensure to check whether AmpCon-DC can connect to the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**.
> - If some switches don't have the **Device Default Login User** and **Device Default Password** entered in the global system configuration, create non-global system configurations for these switches, and ensure the **Device Default Login User** and **Device Default Password** match these switches.

- Check whether the hardware ID of the switch is included in any imported AmpCon-DC licenses. For more information, see Viewing AmpCon-DC Licenses.

  If the hardware ID of the switch is not included in any imported AmpCon-DC licenses, you must import an AmpCon-DC license to AmpCon-DC. Or else, the switch can't be provisioned successfully. For more information, see Importing Licenses for Imported Switches.

Import Procedure

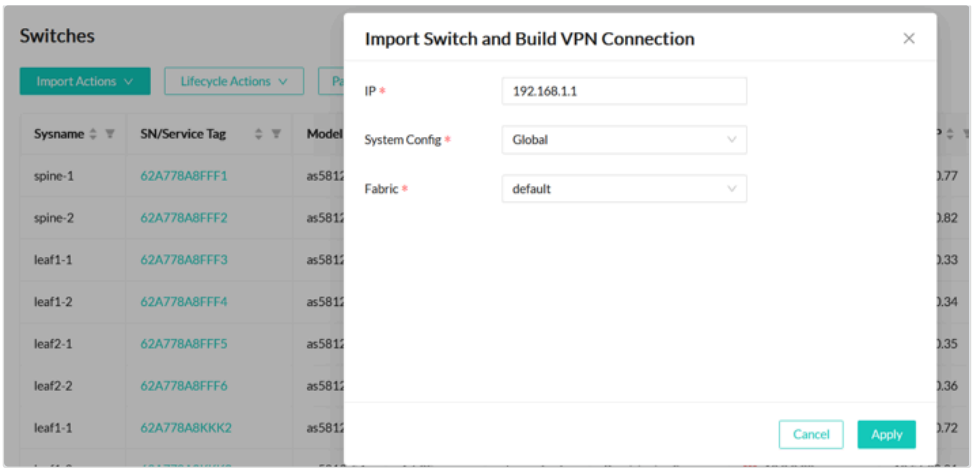
Automatically Importing a Switch

If you have obtained the IP addresses of the switches, you can use the automatic import method.

Importing a Switch with a Global User

If you log in to the AmpCon-DC UI with a global user, follow these steps:

1. Click **Device > Switches** from the navigation bar.
2. On the "Switches" page, click **Import Actions**, and then select **Import**.
3. In the **IP** field, enter the IP address of the switch.
4. In the **System Config** drop-down list, select the appropriate system configuration.

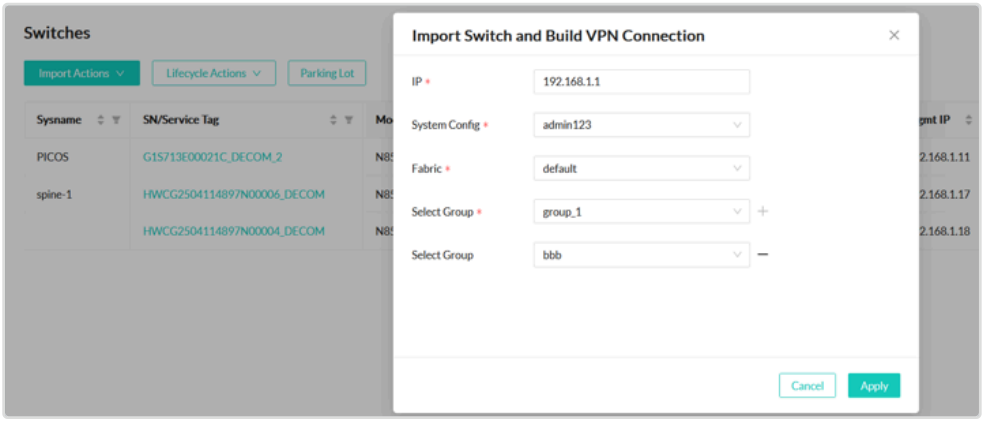


5. In the **Fabric** drop-down list, select a fabric. To add a fabric, see Managing Fabrics.
6. Click **Apply**.
7. On the “Switches” page, check whether the switch status is shown as **Imported**.

Importing a Switch with a Group User

If you log in to the AmpCon-DC UI with a group user, follow these steps:

1. Click **Device > Switches** from the navigation bar.
2. On the “Switches” page, click **Import Actions**, and then select **Import**.
3. In the **IP** field, enter the IPv4 address of the switch.
4. In the **System Config** drop-down list, select the appropriate system configuration.
5. In the **Fabric** drop-down list, select a fabric. To add a fabric, see Managing Fabrics.
6. In the **Group** drop-down list, select a switch group. To add a switch group, see Adding a Switch Group.

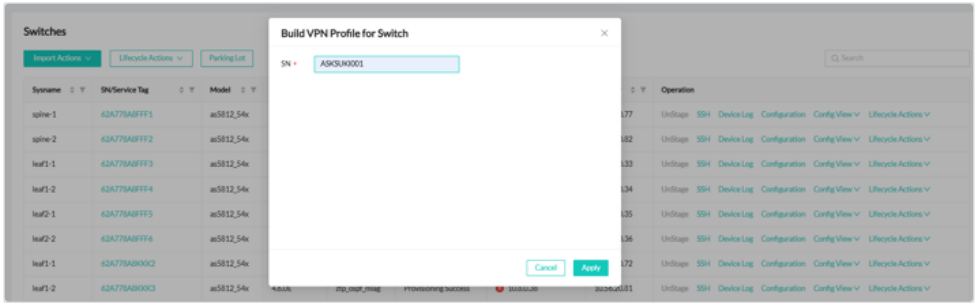


7. Click **Apply**.
8. On the “Switches” page, check whether the switch status is shown as **Imported**.

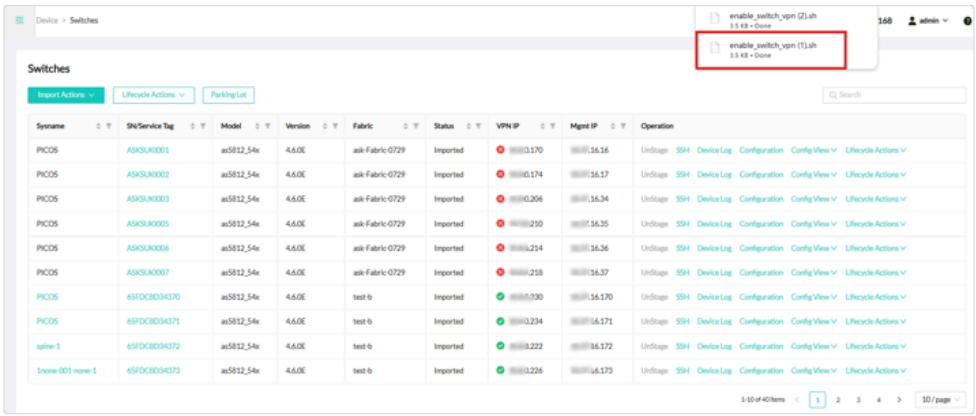
Manually Importing a Switch

If you haven't obtained the IP addresses of the switches, you can use the manual import method.

1. Generate the tunnel keys based on the input serial number. These keys are used to ensure that the VPN tunnel between the switch and the AmpCon-DC server is encrypted.
   a. Log in to the AmpCon-DC UI, and then click **Device > Switches** from the navigation bar.
   b. Click **Import Actions**, and then select **Adopt**.
   c. In the **SN** field, enter the serial number of the switch.



   d. Click **Apply**.
2. Download the VPN script and run it on the switch. The script will retrieve the tunnel keys and establish a VPN tunnel between the switch and the AmpCon-DC server.
   a. Log in to the AmpCon-DC UI, and then click **Device > Switches** from the navigation bar.
   b. Click **Import Actions**, and then select **Download VPN Script**. The VPN script is downloaded to your local machine.



   c. Copy the script to the PicOS switch.
   d. SSH log in to the switch, enter the Linux shell mode, and run the following commands:

```
curl  -o /opt/auto-deploy/auto-deploy.conf -k -v
https://<ampcon-server-ip>/rma/file/agent/auto-deploy.conf
```

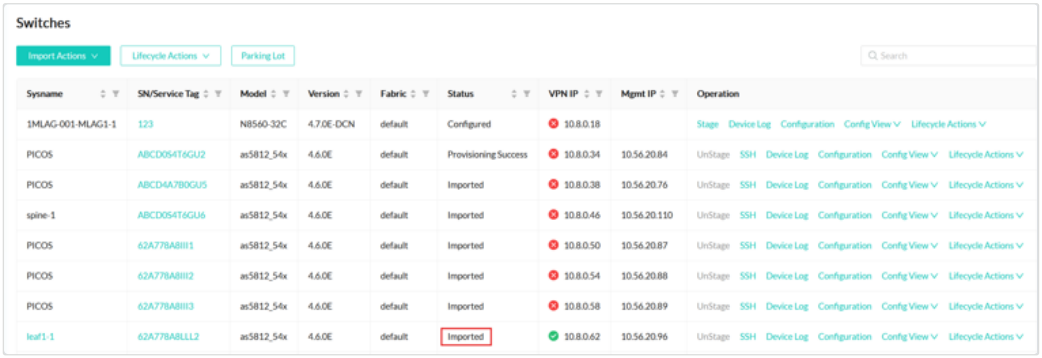
```
sudo ./enable_switch_vpn.sh <ampcon-server-ip>
```

NOTEs

- You must run the first command to replace the **/opt/auto-deploy/auto-deploy.conf** file before running the second command to import the switch. Otherwise, the switch import might fail.
- You need to replace <*ampcon-server-ip*> with the IP address of your AmpCon-DC server.

Checking Importing Results

In the AmpCon-DC UI, click **Device > Switches f**rom the navigation bar. On the “Switches” page, check whether the switch is displayed in **Imported** status.



For more information about the PicOS tab, see Viewing Managed Switches.

Deploying Switches through Normal ZTP

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

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

Normal ZTP is a ZTP method to onboard switches. After you deploy switches through normal ZTP, these switches can be deployed and managed by AmpCon-DC.

See the following child topics:

- How Normal ZTP Works
- Quick Deployment Guide for Normal ZTP
- Preparing Configurations
- Configuring a DHCP Server
- Provisioning Switches through Normal ZTP

How Normal ZTP Works

Check the following overview and workflows to understand how normal ZTP works.

- Overview
- White-Box Switches
- Integrated Hardware and Software Switches

Overview

Normal ZTP helps you deploy switches and register switches with AmpCon-DC for management.

After you plug in and reboot a switch, DHCP automatically provides the switch with an IP address and the address of a provision shell script that is obtained from the AmpCon-DC server. Then, the switch automatically runs the shell script to complete the normal ZTP deployment.

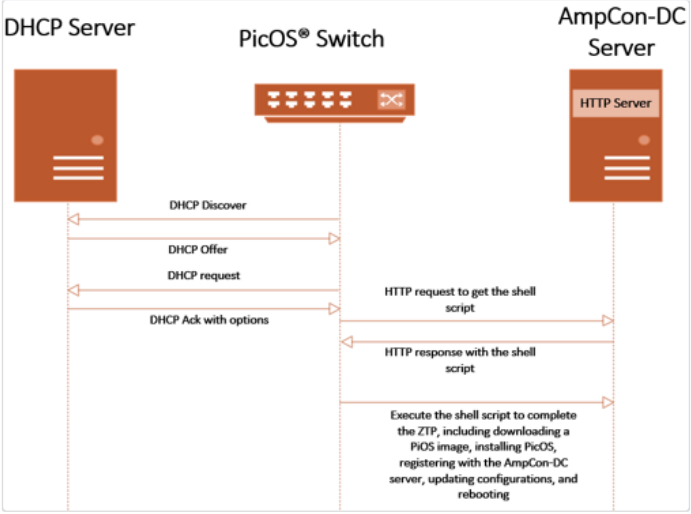
Table 1. Normal ZTP Operations

Switch Type	ZTP Operation
White-Box Switch	A white-box switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-DC server, update switch configurations, and reboot the switch.
Integrated Hardware and Software Switch	An integrated hardware and software switch runs the shell script to register with the AmpCon-DC server, install a PicOS license on the switch, update switch configurations, and reboot the switch.

White-Box Switches

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

Figure 1. Management Workflow of White-Box Switches

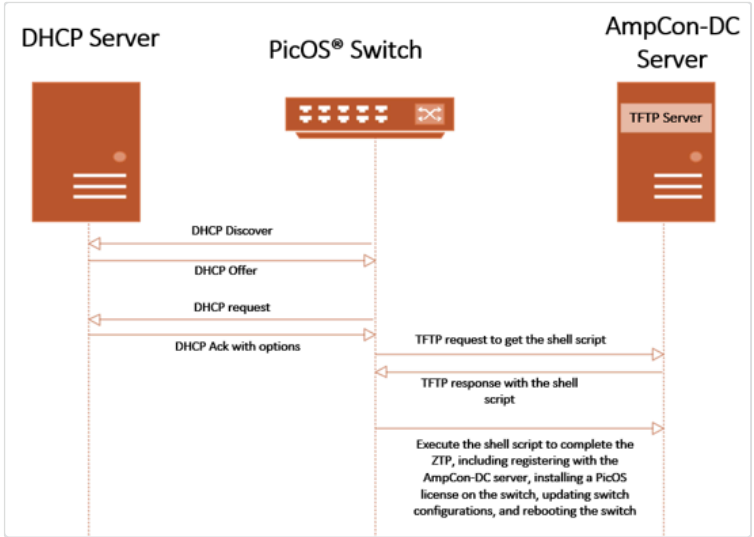


1. After a switch is powered on, the switch sends DHCP Discover to get an IP address, and the DHCP server provides the switch with an IP address.
2. The switch sends a request to the DHCP server, and the DHCP server sends a response including the HTTP server address.
3. The switch sends an HTTP request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

Integrated Hardware and Software Switches

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

Figure 2. Management Workflow of Integrated Hardware and Software Switches



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

Quick Deployment Guide for Normal ZTP

This topic describes how to complete the switch deployment through normal ZTP. Once successfully deployed, the PicOS switches are classified as managed devices of AmpCon-DC.

Guidelines
Prerequisites
Procedure
Deploying White-Box Switches
Deploying Integrated Hardware and Software Switches

Guidelines

Pay attention to the following points. Or else, switches will fail to be deployed.

- Be careful when you configure system configurations:
  - Ensure that the entered **Device Default Login User** and **Device Default Password** are correct and can be used to log in to the switch.
  - If the switch don't use the **Device Default Login User** and **Device Default Password** in the global system configuration, create a non-global system configuration for the switch, and ensure the **Device Default Login User** and **Device Default Password** match with the switch.
  - Ensure that the AmpCon-DC server can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see Checking License Portal Connectivity.
  - Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations.
- If you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-DC parking lot. For more information, see Managing the Parking Lot.

  To continue deploying the switches in the parking lot, follow these steps:

  a. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar.

  b. On the "Switches" page, click **Parking Lot**.

  c. Locate the switch to be deployed, and then click **Create Config** to add a switch configuration. After you add the switch configuration, the switch will be listed on the "Switches" page with the **Configured** status.

  d. Continue to provision the switch through normal ZTP to complete the switch deployment.

Prerequisites

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

Table 1. Prerequisite Tasks and Links

Task	Reference Link
Install the AmpCon-DC server successfully.	• Platform Installation Workflow
Log in to the AmpCon-DC UI with an account of the **SuperAdmin** role.	• Working with the User Interface
Ensure that the switches to be onboarded are supported by AmpCon-DC.	• Supported Switches for 2.5.0 • Supported Switches for 2.5.1
For switches that have PicOS installed, ensure that the Secure Shell (SSH) protocol is enabled on these switches. SSH is enabled on PicOS switches by default.	• No Reference Link
Ensure that the switches are able to connect to the AmpCon-DC server.	• No Reference Link
If a firewall is configured between AmpCon-DC and the switches, allow outbound access on the following ports to the management port of each switch. • **TCP**: 22 • **TCP**: 9339 • **TCP**: 830	• No Reference Link

Procedure

Deploying White-Box Switches

To deploy a white-box switch through normal ZTP, see the following diagram and tasks:

Figure 1. Normal ZTP Workflow for White-Box Switches

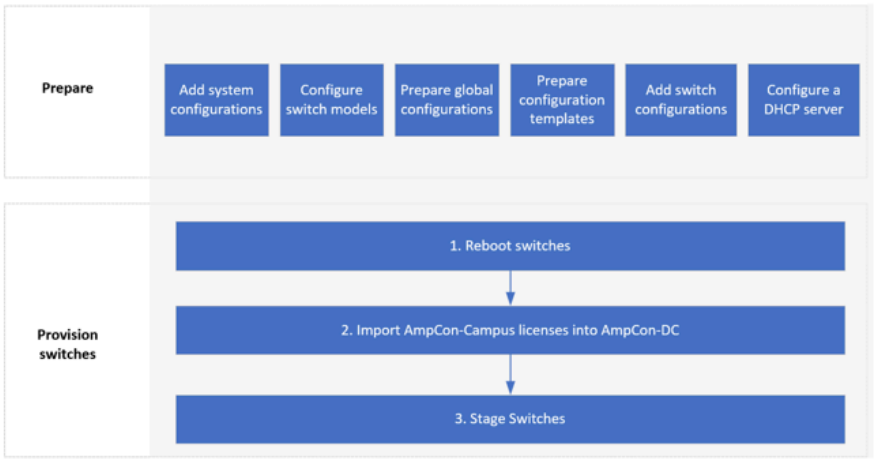


Table 2. White-Box Switch Deployment Tasks

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

5. Click **Device > Device Profiles** from the navigation bar. Click the **Switch Configuration** tab. In this tab, add a switch configuration for the switch.	• Adding Switch Configurations
6. Configure a DHCP server. If the DHCP server is not configured correctly, the switch deployment will fail.	• Configuring a DHCP Server
7. Provision the switch through normal ZTP to complete the switch deployment.	• Provisioning a White-Box Switch

Deploying Integrated Hardware and Software Switches

To deploy an integrated hardware and software switch through normal ZTP, see the following diagram and steps:

Figure 2. Normal ZTP Workflow for Integrated Hardware and Software Switches

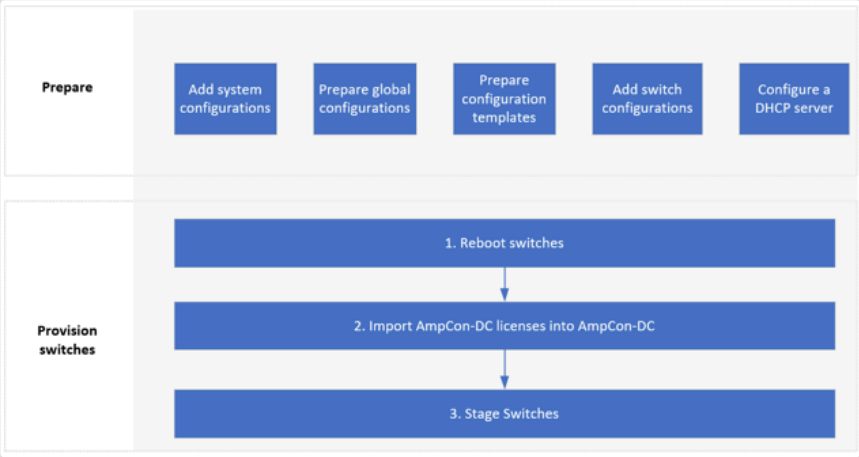


Table 3. Integrated Hardware and Software Switch Deployment Tasks

Task	Reference Link
1. Click **Device > Device Profiles** from the navigation bar of the AmpCon-DC UI. Click the **System Configuration** tab. In this tab, configure the global system configuration. If the global system configuration doesn't match with the switch, create a non-global system configuration.	• Adding System Configurations

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

Preparing Configurations

To deploy switches through normal ZTP, you need to prepare the required configurations in the AmpCon-DC UI first.

See the following child topics:

- Configuring Global Configurations
- Adding Switch Configurations
- Managing Global and Switch Configurations
- Configuring Switch Models
- Adding System Configurations

After you complete these configurations for a switch, configure a DHCP server and provision this switch to complete the normal ZTP deployment. For more information, see Configuring a DHCP Server and Provisioning Switches through Normal ZTP.

Configuring Global Configurations

To deploy switches through normal ZTP, you must prepare global configurations. A global configuration file contains global configurations to be pushed to switches during the normal switch deployment process.

When you add a switch configuration, you must select a global configuration file. For more information, see Adding a Switch Configuration.

Procedure
Optional Operations
Viewing a Global Configuration File
Editing a Global Configuration

Procedure

To add a global configuration file, follow these steps:

1. In the AmpCon-DC UI, click **Device > Device Profiles** from the navigation bar.
2. In the **Global Configuration** tab, input the following information, and then click **Generate**.

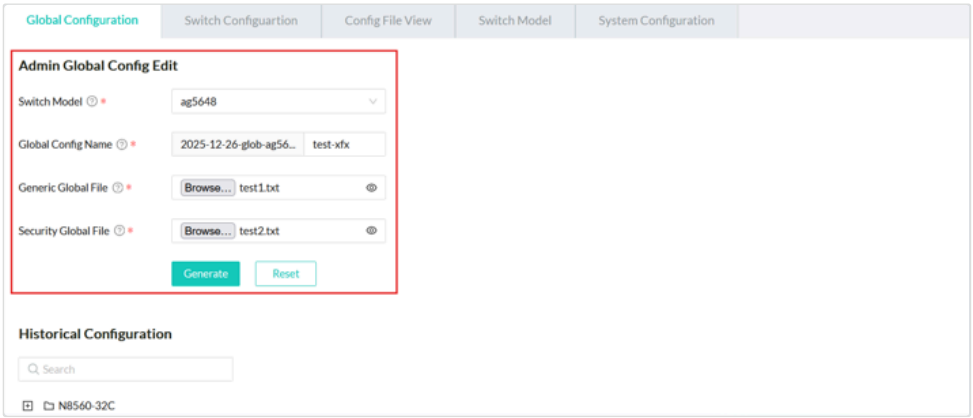


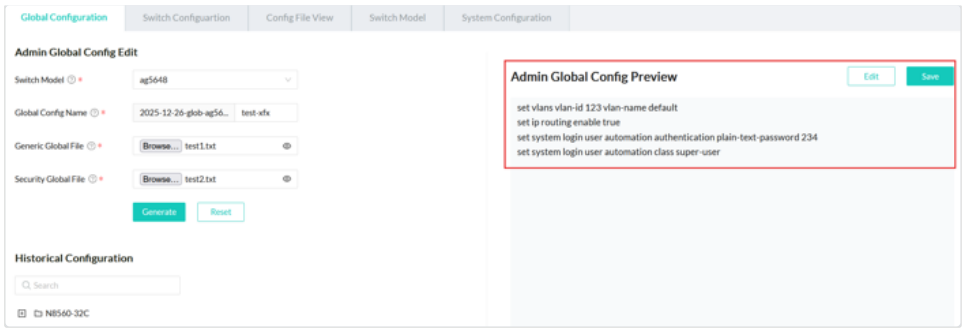
Table 1. Global Configuration Parameters

Parameter	Description
Switch Model	The switch model.
Global Config Name	The name of the global configuration file.
Generic Global File	Select a .txt file with general global configurations to be pushed to the switch.

	Example configuration in the .txt file: **set vlans vlan-id 303**
Security Global File	Select a .txt file with security-related configurations to be pushed to the switch. Example configuration in the .txt file: **set system login user automation2 authentication plain-text-password 12345678** **set system login user automation2 class super-user** **NOTE** You might also add security-related configurations in the system configuration. If some configurations in the system configuration and in the uploaded **Security Global File** here overlap: • For the overlapping configurations, the configurations in the uploaded **Security Global File** here will overwrite the configurations in the system configuration. • For the non-overlapping configurations, the configurations in both the system configuration and the uploaded **Security Global File** here will be pushed to the switches.

3. In the **Admin Global Config Preview** section, click **Save** to confirm the configurations retrieved from the **Generic Global File** and the **Security Global File**.

   You can also click **Edit** and then click **Save** to modify the configurations.

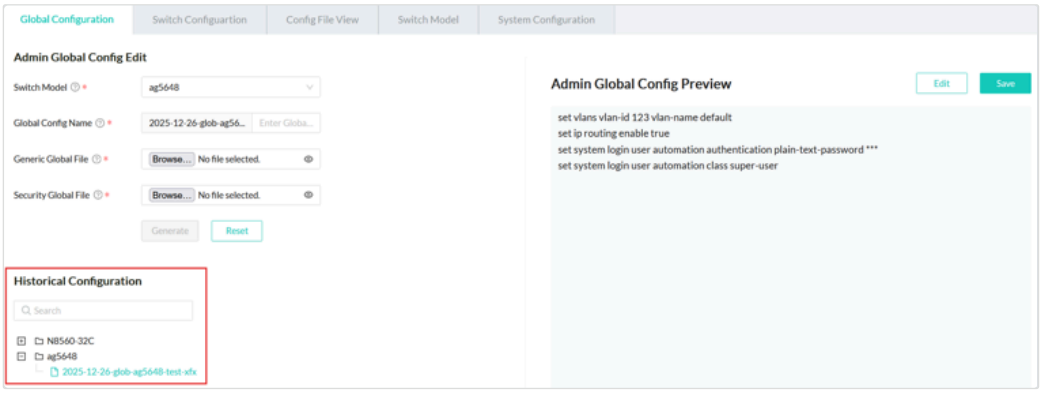


Optional Operations

Viewing a Global Configuration File

In the **Historical Configuration** section, you can see all the added global configurations, which are grouped by switch model.

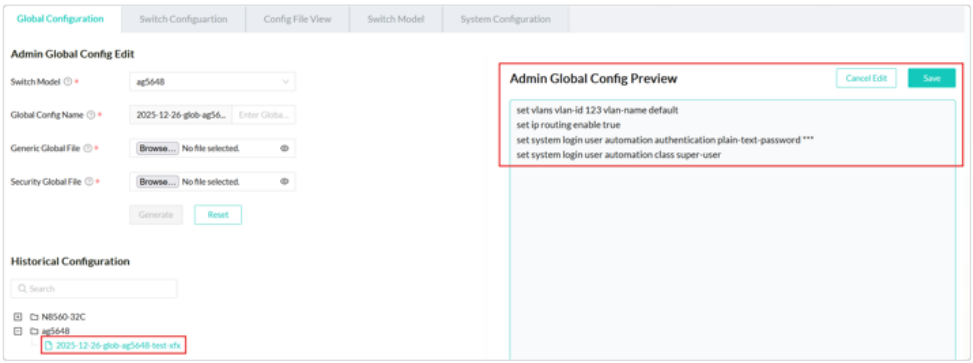
To check the configurations in a global configuration file, click the switch model, and then click the global configuration file name.



Editing a Global Configuration

To edit a global configuration, follow these steps:

1. In the **Historical Configuration** section, locate the global configuration, and then click it.
2. In the **Admin Global Config Preview** section, click **Edit**.
3. Edit the configurations as needed, and then click **Save**.



Adding Switch Configurations

To deploy switches through normal ZTP, you must prepare switch configurations for each switch.

- Overview
- Prerequisites
- Procedure
  - Adding a Switch Configuration
  - Adding Multiple Switch Configurations in Batches
- Optional Operations
  - Viewing or Editing Switch Configurations
  - Checking the Switch Status

Overview

A switch configuration contains the following configurations:

- The SN or service tag of the switch.
- The switch model of the switch.
- The location of the switch.
- The fabric to which the switch belongs.
- The global configuration file and configuration templates.
- Whether to enable automatic configuration backup for the switch.
- The system configuration related to the switch.

All these configurations are important for deploying switches through normal ZTP.

Prerequisites

Ensure that the global configuration file and configuration templates for the switch have been created. For more information, see Adding Global Configurations and Adding Configuration Templates.

Procedure

You can add switch configurations one by one or add multiple switch configurations in batches by using a JSON file.

Adding a Switch Configuration

To add one switch configuration, follow these steps:

1. In the AmpCon-DC UI, click **Device > Device Profiles** from the navigation bar.

2. In the **Switch Configuration** tab, input the following information:

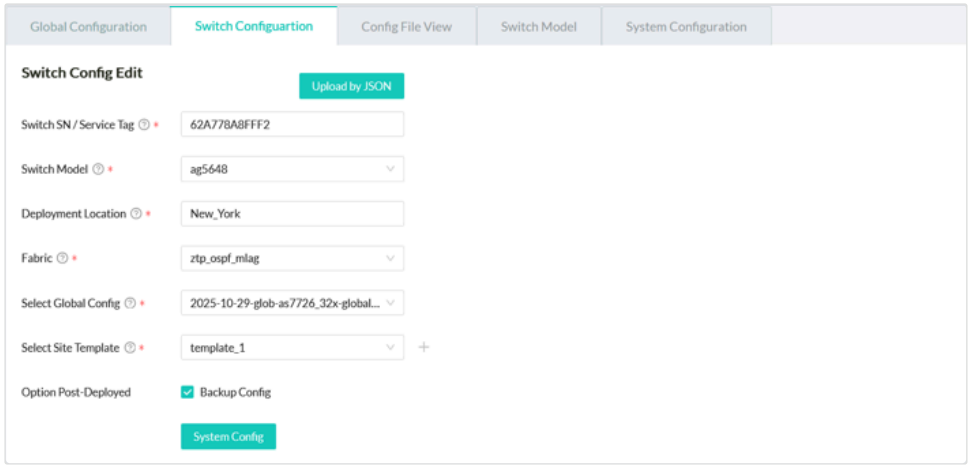


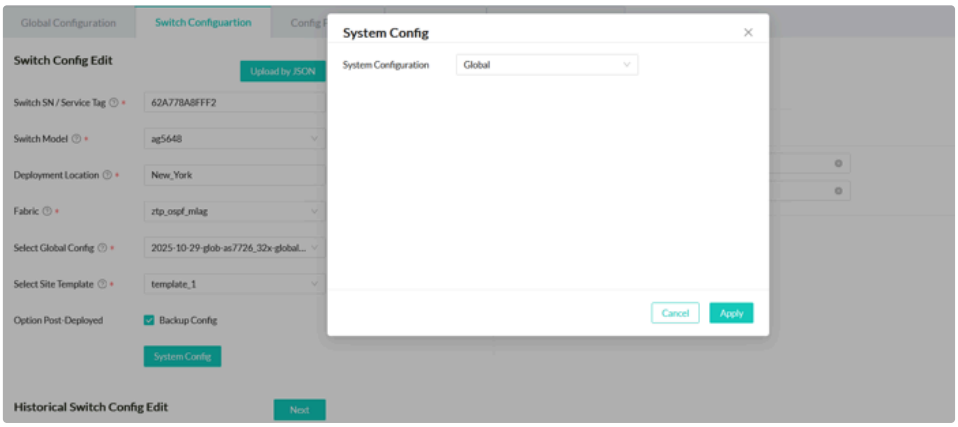
Table 1. Switch Configuration Parameters

Parameter	Description
Switch SN/Service Tag	The SN or service tag of the switch. The value can contain only letters and numbers.
Switch Model	The switch model.
Deployment Location	The location where the switch exists, such as **New_York**. The value can contain only the special character _, letters, and numbers.
Fabric	The fabric that the switch belongs to. • The **default** fabric is selected by default. • To add a new fabric, see Adding a Fabric.
Select Global Config	The global configuration file that contains configurations to be pushed to the switch. If the global configuration file in the drop-down list doesn't meet your needs, add a new global configuration file. For more information, see Configuring Global Configurations.
Select Site Template	The configuration template to use.

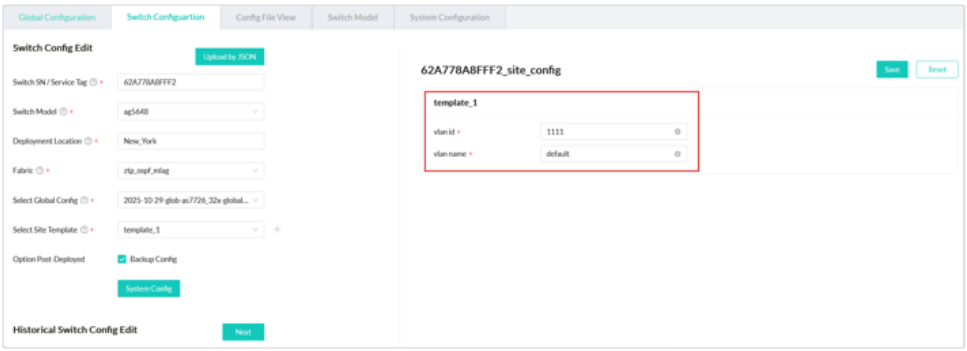
	• Click **+** to add multiple configuration templates if needed. • If the configuration template file in the drop-down list doesn't meet your needs, add a new configuration template file. For more information, see Adding Configuration Templates.
Option Post-Deployed	Select **Backup Config** to enable automatic switch configuration backup after the switch is deployed. After you select **Backup Config**, AmpCon-DC will back up the switch configurations at 22:00 in the UTC-0 time zone every 3 days. You can change the interval and backup time. For more information, see Backing Up Configurations Automatically.

3. Click **System Config**. In the pop-up window, select the system configuration related to the switch.

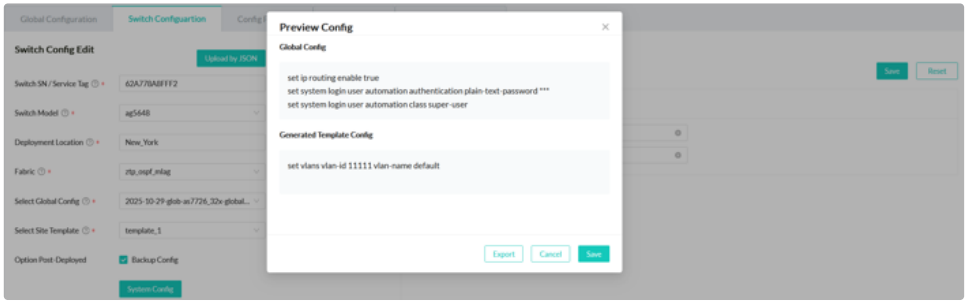
> **NOTE**
>
> Ensure that the **Device Default Login User** and **Device Default Password** on the "System Configuration" page can be used to log in to these switches. Or else, the switch will fail to be deployed.



4. Click **Next**. You can see an input section, which is related to the selected configuration template. Enter the relevant information.



5. Click **Save.**
6. In the **Preview Config** pop-up window, preview the configurations included in the global configuration file and configuration templates.



7. Click **Save**. The switch configuration is added now. On the “Switches” page, you can see the switch status is shown as **Configured**.

Adding Multiple Switch Configurations in Batches

To add multiple switch configurations in batches by uploading a JSON file, follow these steps:

1. Prepare a JSON file with switch configurations. See the following example:

> **NOTEs**
>
> - You can add switch configurations for only the switches that haven’t been managed by AmpCon-DC. For more information, see Viewing Managed Switches.
> - The **retrieve_config** field is configured to enable or disable automatic switch configuration backup after the switch is deployed. For more information, see Backing Up Configurations Automatically.
> - The configurations in the **default_config_param** field will be pushed to all switches you specified in the **sn** field.

- You can add configurations for specific switches in the **unique_config_param** field. These configurations will be pushed to only these specified switches.
- All the configuration templates specified in the **default_config_param** and **unique_config_param** fields must be included in the **site_template_name** field.
- Ensure that the configurations in the **default_config_param** and **unique_config_param** fields match the configuration template used. For example, in the **unique_config_param** field, **"vlan_id": "99"** and **"vlan_name": "99"** are added to the **template_2** section. If the configuration template **template_2** doesn't contain the configuration **set vlans vlan-id {{ vlan_id }} vlan-name {{ vlan_name }}**, the JSON file will fail to be imported. To check the configurations included in a configuration template, see Viewing or Editing a Configuration Template.

```
{
 "sn": ["EC1631000062", "EC1631000063"],
 "hardware_model": "ag5648",
 "location": "Beijing",
 "global_config_name": "2025-12-8-glob-ag5648-test-xfx",
 "site_template_name": ["template_2"],
 "retrieve_config": true,

 "default_config_param": {
  "template_2": {
   "vlan_id": "12",
   "vlan_name": "23"
  }
 },

 "unique_config_param": {
  "EC1631000062": {
   "template_2": {
    "vlan_id": "99",
    "vlan_name": "99"
   }
```

```
  }
 },
 "system_config_name":{
  "EC1631000062": "Global",
  "EC1631000063": "Global"
 }
}
```

2. In the AmpCon-DC UI, click **Device > Device Profiles** from the navigation bar.
3. In the **Switch Configuration** tab, click **Upload by JSON.**
4. Click or drag a file to upload the JSON file.
5. Click **Upload**.

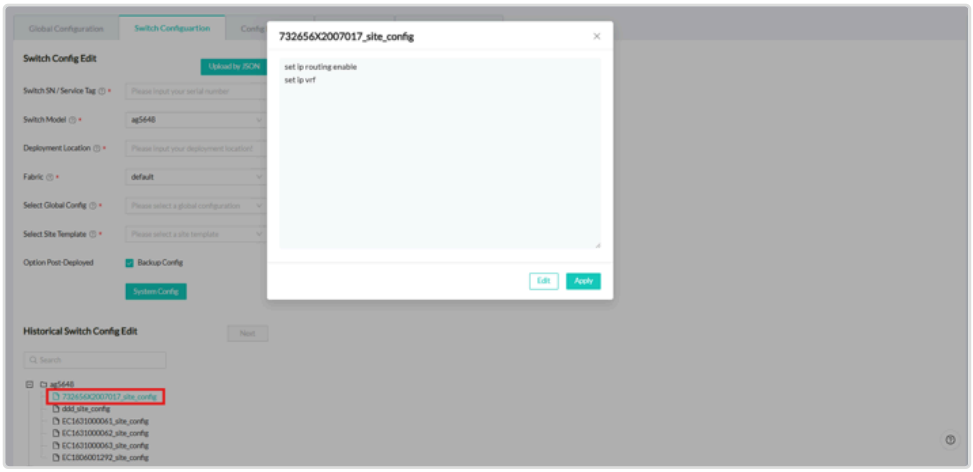
Optional Operations

Viewing or Editing Switch Configurations

In the **Historical Switch Config Edit** section, you can see all the added switch configurations, which are grouped by switch models.

To edit a switch configuration, follow these steps:

1. Locate the global configuration, and then click it.



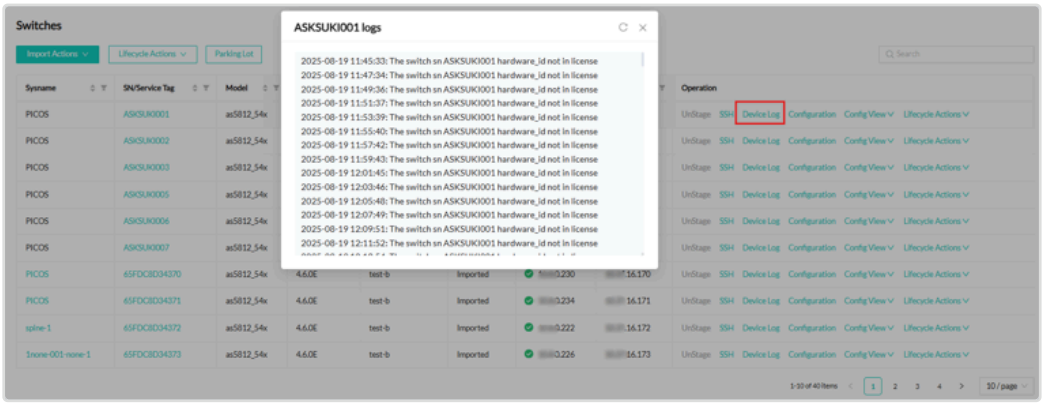
2. In the pop-up window, click **Edit**.
3. Edit the configurations as you need.
4. Click **Apply**.

Checking the Switch Status

After you add a switch configuration, click **Device > Switches** from the navigation bar, and then check whether the switch status is shown as **Configured** on the “Switches” page.

If not, locate the switch, and click **Device Log** to see more details.

For more information about the “Switches” page, see Viewing Managed Switches.



Managing Global and Switch Configurations

In the **Config File View** tab, you can manage all added global configurations and switch configurations (also called site configurations).

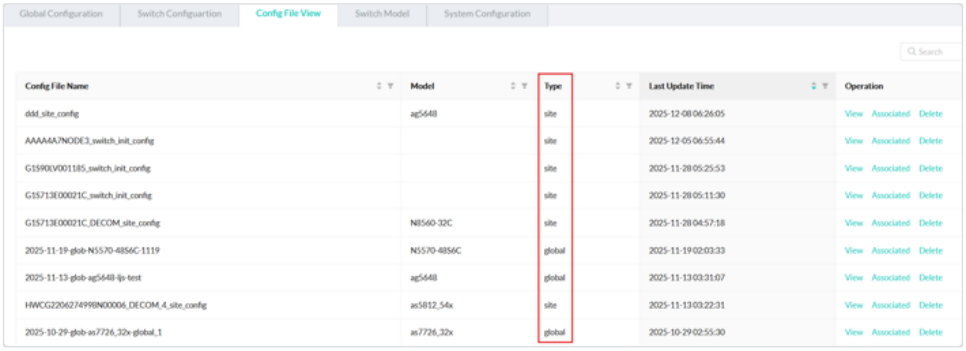
Viewing or Editing a Configuration File
Checking Switches Associated with a Configuration File
Deleting a Configuration File

Viewing or Editing a Configuration File

To view or edit a global or switch configuration file, follow these steps:

1. In the AmpCon-DC UI, click **Device > Device Profiles** from the navigation bar.

   You can see all the added global configurations and switch configurations. The global configurations are in **global** type, and the switch configurations are in **site** type.



2. Click the **Config File View** tab, locate the configuration file, and then click **View**.

   You can see a pop-up window with detailed configurations.



3. To close the pop-up window, click the close icon.
4. To edit the configurations, click **Edit**, modify the configurations, and then click **Apply**.



Checking Switches Associated with a Configuration File

To view the switches associated with a global or site configuration file, follow these steps:

1. In the **Config File View** tab, locate the configuration file, and then click **Associated**.
2. In the pop-up window, check the switches that are associated with the configuration file.

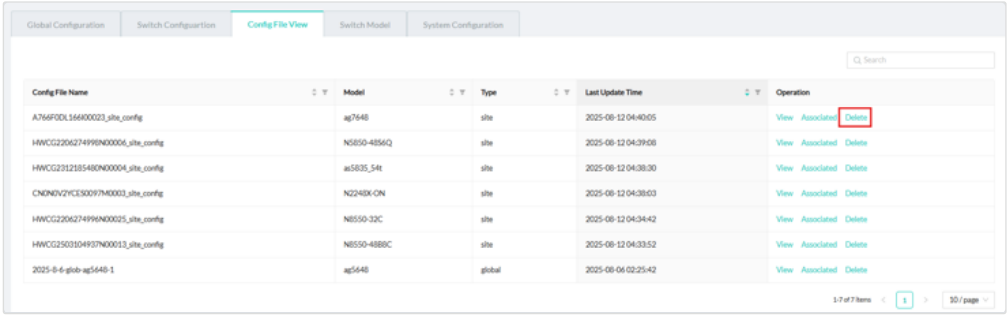


Deleting a Configuration File

To delete a global or switch configuration file, follow these steps:

> **NOTE**
>
> If a global or switch configuration file is still associated with one or multiple switches, the configuration file can't be deleted.

1. In the **Config File View** tab, locate the configuration file, and then click **Delete**.
2. In the pop-up lick **Yes** to confirm the deletion.



Configuring Switch Models

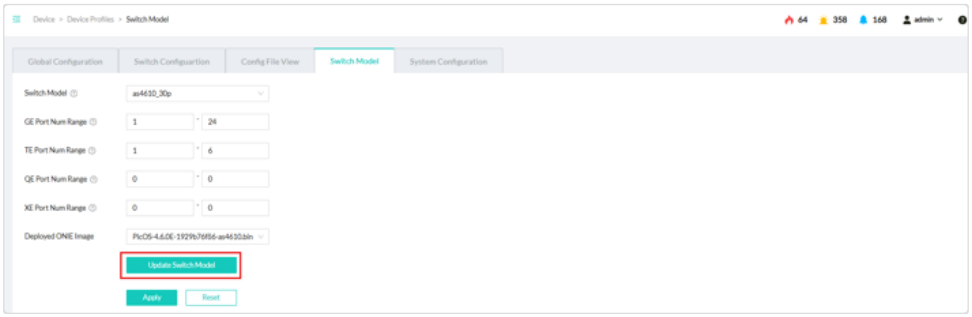
To deploy white-box PicOS switches through normal ZTP, you must configure each switch model of these switches. Each switch model configuration contains the PicOS image used to deploy white-box switches of this model, and the port number range for each speed (GE, TE, QE, and XE).

To deploy integrated hardware and software switches, because these switches have PicOS installed, you don't need to configure switch models.

Procedure

To configure a switch model, follow these steps:

1. In the AmpCon-DC UI, click **Device > Device Profiles** from the navigation bar.
2. To ensure the **Switch Model** drop-down list is the latest, click **Update Switch Model** in the **Switch Model** tab, and then click **Yes**.

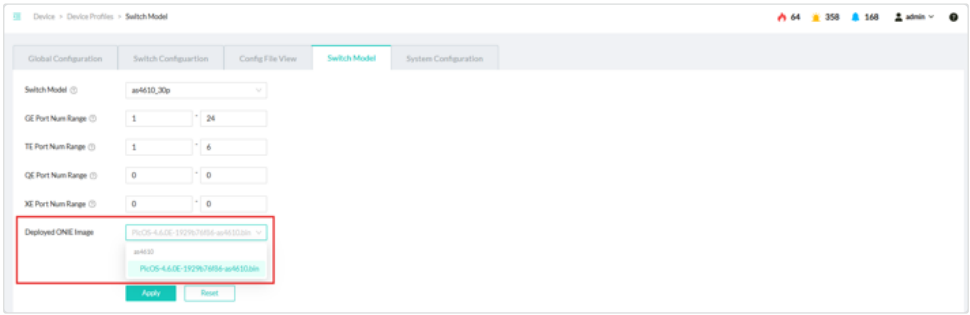


3. In the **Switch Model** drop-down list, select the switch model that you want to configure.
4. Configure the port number range for each speed (GE, TE, QE, and XE).

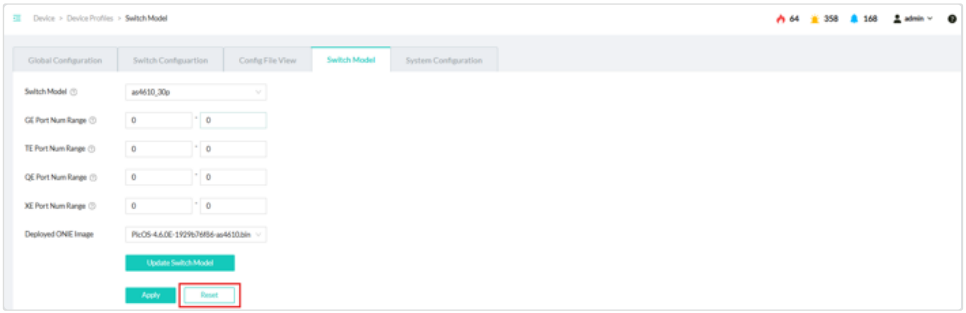
> **NOTE**
>
> For each switch model, a default port number range is configured for each speed (GE, TE, QE, and XE).
>
> You must configure the port number ranges correctly based on real port ranges on switches of this switch model. Or else, some AmpCon-DC functions will fail, such as node uplink and RoCE policies.

5. In the **Deployed ONIE Image** drop-down list, select the PicOS image that you want to install for this switch model.

> **NOTE**
>
> For each switch model, a built-in PicOS image is specified for switch deployment.
>
> If the PicOS image to install is not listed here, upload the PicOS image and its MD5 file to AmpCon-DC. For more information, see Uploading Images.



6. Click **Apply**.
7. Optional: To reset a switch model, click **Reset**.



After you reset a switch model, the port number range for each speed is set to zero, and the PicOS image in the **Deployed ONIE Image** drop-down list is reset to the built-in image.

Adding System Configurations

System configurations contain important information used for importing switches or deploying switches through normal ZTP or simplified ZTP. If a system configuration is not configured correctly, the switches related to the system configuration will fail to be deployed or imported.

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

If the global system configuration doesn't meet all switch requirements, create one or multiple non-global system configurations.

- Overview
  - Types
  - Configurations
- Procedure
  - Adding a Global System Configuration
  - Adding a Non-global System Configuration
- Optional Operations
  - Checking License Portal Connectivity
  - Viewing or Modifying a System Configuration
  - Changing the Default Switch Password

Overview

Types

System configurations contain the following two types:

- **Global system configuration**

  The first time you log in to AmpCon-DC, you must add information to the global system configuration. The global system configuration can't be removed.

- **Non-global system configuration**

  If the default username and password of switches to be managed are different, you can add multiple non-global system configurations. You can remove a non-global system configuration if it is not needed.

Configurations

A system configuration contains the following information:

- The URL, username, and password of the License Portal. The information is used to send requests to the License Portal.

- Default username and password of switches to be managed. The information is used to access the switches.
- A security configuration file with PicOS security-related set CLIs. Before you deploy and configure a switch, the switch needs to be configured with an initial security configuration to eliminate any unauthorized access. Security Config file is loaded to switch at the beginning of switch deployment.
- A parking security configuration file, which is used to push initial parking security configuration for those switches in the parking status. This configuration is not included in the non-global system configuration.

  Available for only global system configurations.
- The maximum backup number for the configuration snapshots. This configuration is not included in the non-global system configuration.

  Available for only global system configurations.
- The IP ranges of switches that are allowed for AmpCon-DC management. This configuration is not included in the non-global system configuration.

  Available for only global system configurations.
- Whether to enable debug logs for server-side operations or not. This configuration is not included in the non-global system configuration.

  Available for only global system configurations.

Procedure

Adding a Global System Configuration

To add a global system configuration, follow these steps:

1. Log in to the AmpCon-DC UI with a user of the **SuperAdmin** role. For more information about user roles, see Managing User Access.
2. Click **Device > Device Profiles** from the navigation bar, and then input the following information in the **System Configuration** tab:

> **NOTE**
>
> Pay attention to the following points. Or else, switches will fail to be imported and deployed.
>
> - Ensure that the entered **Device Default Login User** and **Device Default Password** on the “System Configuration” page are

correct and can be used to log in to these switches.

- Ensure to check whether AmpCon-DC can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see the Checking License Portal Connectivity section.
- If some switches to be deployed don't use the **Device Default Login User** and **Device Default Password** entered in the global system configuration, create non-global system configurations for these switches, and ensure the **Device Default Login User** and **Device Default Password** match these switches.
- Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations or underlay/overlay related configurations.

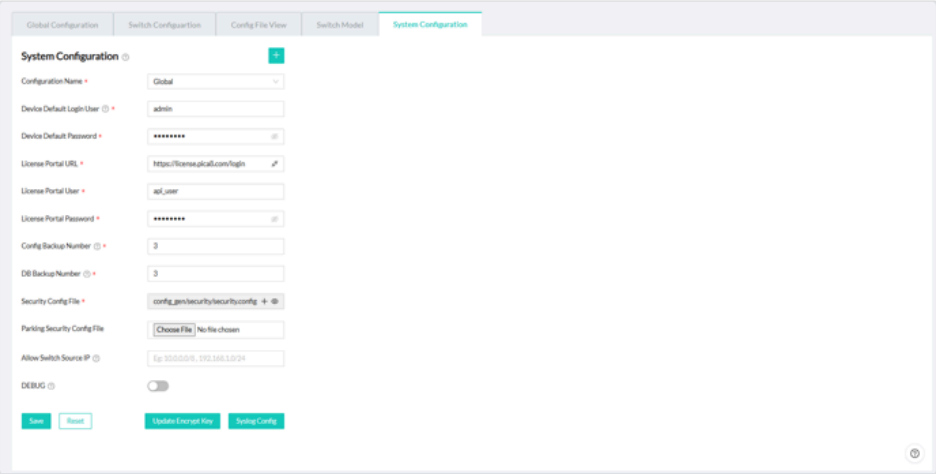


Table 1. Global System Configuration Parameters

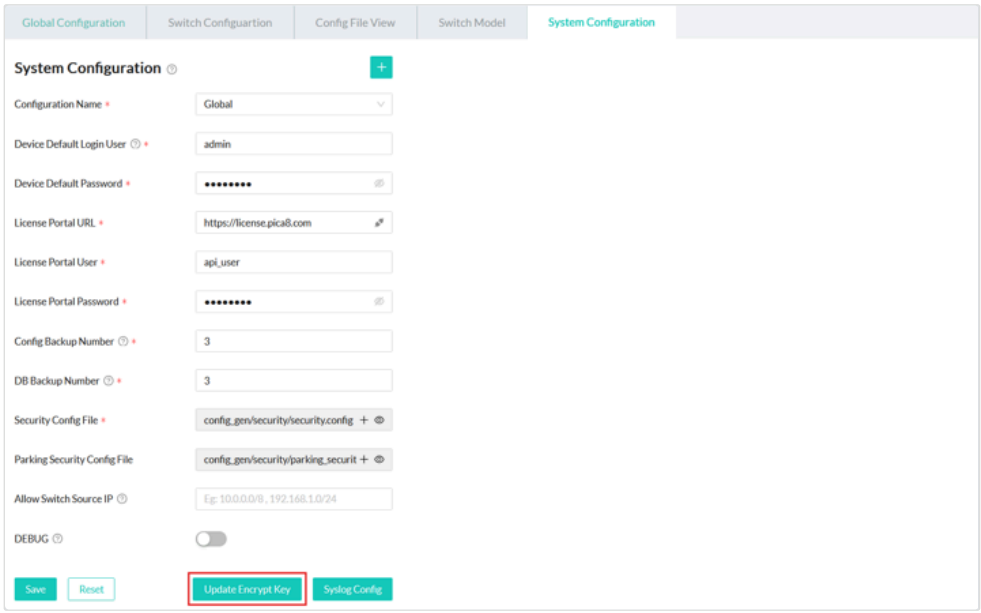
Parameter	Description
Configuration Name	The name of the configuration.
Device Default Login User	The default username for switches to be managed. The default user is **admin**.
Device Default Password	The default password of the default user. The default password is **pica8**.
License Portal URL	https://license.pica8.com

License Portal User	The user ID for the License Portal.
License Portal Password	The password of the user for the License Portal.
Config Backup Number	The maximum backup number for the configuration snapshots.
DB Backup Number	The allowed maximum number of database backups.
Security Config File	The .txt file with PicOS security-related set CLIs. Example configuration in the .txt file: **set system login user testadmin authentication plain-text-password pica8pica8** **set system login user testadmin class super-user** **NOTEs** • The configurations in this file will be pushed to switches during the ZTP process. • If you don't want to push configurations to switches during the ZTP process, you can use a blank .txt file. • You might also add security-related configurations in the global configuration. If some configurations in the global configuration and in the uploaded **Security Config File** here overlap: ◦ For the overlapping configurations, the configurations in the global configuration will overwrite the configurations in the

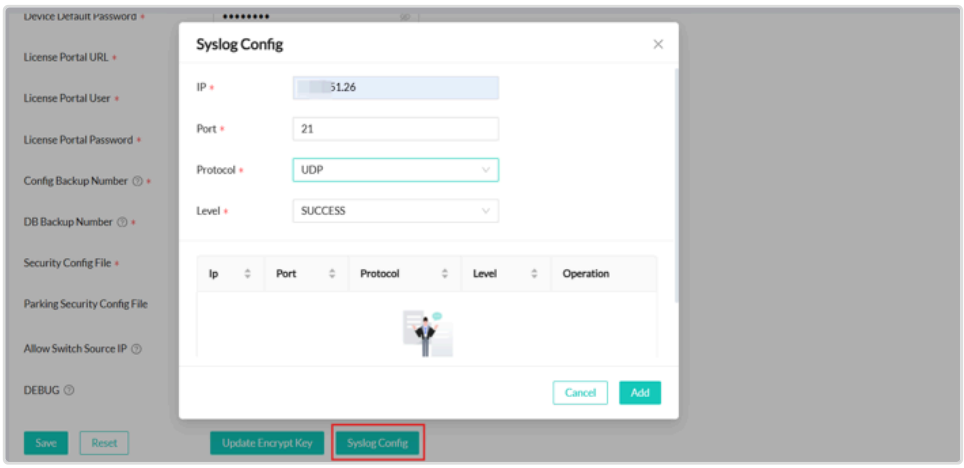
	uploaded **Security Config File** here. ◦ For the non-overlapping configurations, the configurations in both the global configuration and the **Security Config File** here will be pushed to the switches.
Parking Security Config File	Optional. To eliminate any unauthorized access, switches in the parking lot need to be configured with an initial parking security configuration. For more information about parking lot, see Managing the Parking Lot. Example configuration in the .txt file: **set system login user testadmin authentication plain-text-password pica8pica8** **set system login user testadmin class super-user** **NOTEs** • The configurations in this file will be pushed to switches when the switches go to the parking lot. • If you don't want to push configurations to switches when the switches go to the parking lot, you can use a blank .txt file.
Allow Switch Source IP	Optional. Allow specified subnets from which switches can access AmpCon-DC.
Debug	Optional. Enable debug logs for server-side operations or not.

3. Click **Save**.
4. Optional: After you add a global system configuration, do the following actions as needed:

- To update the encryption key used to encrypt sensitive data in the AmpCon-DC database, click **Update Encrypt Key**. For more information, see Updating the Encryption Key for Sensitive Data Encryption.



- To forward AmpCon-DC system logs to external Syslog servers like Splunk, click **Syslog Config**. For more information, see Forwarding Logs to External Syslog Servers.



The global system configuration is configured now. If you don't add non-global system configurations, the global system configuration will be used to deploy and import switches.

Adding a Non-global System Configuration

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

1. Click **Device > Device Profiles** from the navigation bar.
2. Click the **+** icon in the **System Configuration** tab. The "Add New System Config" tab opens.
3. Input the following information：

NOTE

Pay attention to the following points. Or else, switches will fail to be imported and deployed.

- Ensure that the entered **Device Default Login User** and **Device Default Password** on the “System Configuration” page are correct and can be used to log in to these switches.
- Ensure to check whether AmpCon-DC can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see the Checking License Portal Connectivity section.
- Ensure that the uploaded **Security Config File** and **Parking Security Config File** don’t contain wrong configurations or underlay/overlay related configurations.

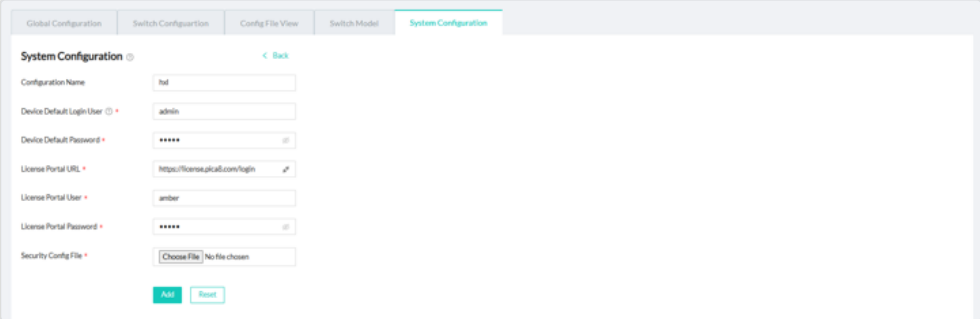


Table 2. Non-Global System Configuration Parameters

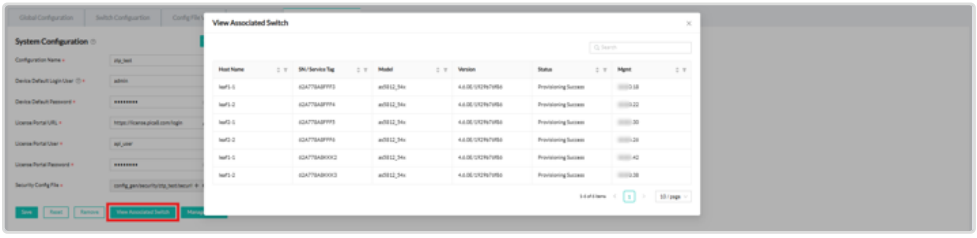
Parameter	Description
Configuration Name	The name of the configuration.
Device Default Login User	The default username of switches to be managed. The default user is **admin**.
Device Default Password	The default password of the default user. The default password is **pica8**.
License Portal URL	https://license.pica8.com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

License Portal Password	The password of the user for the License Portal. **License Portal URL**, **License Portal User**, and **License Portal Password** are used to access the License Portal.
Security Config File	The .txt file with PicOS security-related set CLIs. Example configuration in the .txt file: **set system login user testadmin authentication plain-text-password pica8pica8** **set system login user testadmin class super-user** **NOTEs** • The configurations in this file will be pushed to switches during the ZTP process. • If you don't want to push configurations to switches during the ZTP process, you can use a blank .txt file. • You might also add security-related configurations in the global configuration. If some configurations in the global configuration and in the uploaded **Security Config File** here overlap: ◦ For the overlapping configurations, the configurations in the global configuration will overwrite the configurations in the uploaded **Security Config File** here.

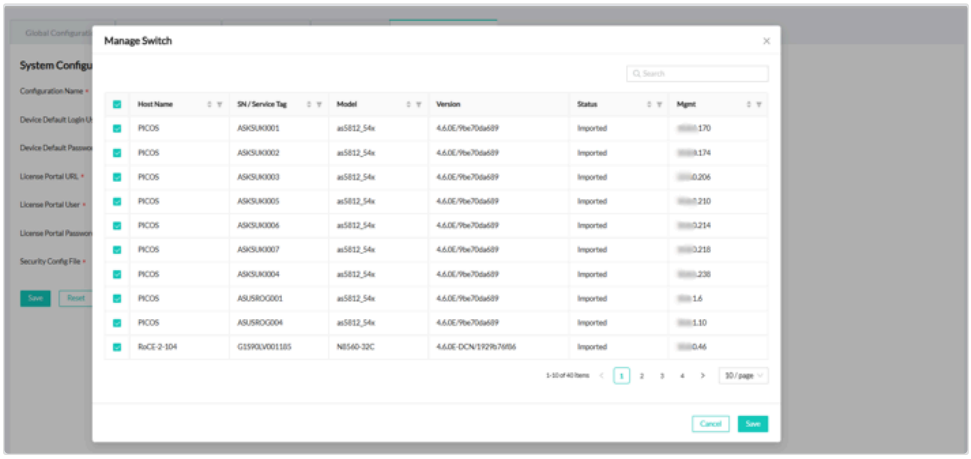
	◦ For the non-overlapping configurations, the configurations in both the global configuration and the **Security Config File** here will be pushed to the switches.

4. Click **Add**.
5. Optional: After you add a non-global system configuration, do the following actions as needed:

- To view the switch information associated with the system configuration, click **View Associated Switch**.



- 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 a non-global system configuration is still associated with some switches, the removal will fail. You need to click **Manage Switch** to unselect these switches first.

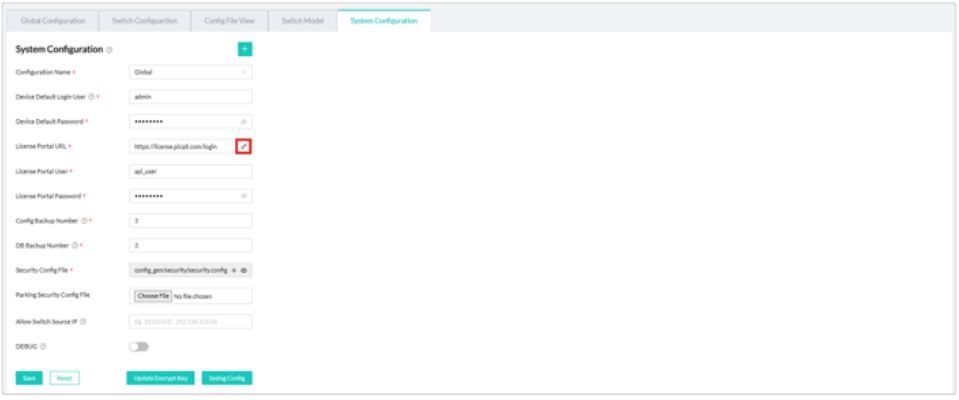
Optional Operations

Checking License Portal Connectivity

To check whether AmpCon-DC can connect with the License Portal specified in a system configuration, follow these steps:

1. Click **Device > Device Profiles** from the navigation bar.
2. In the **System Configuration** tab, select the system configuration to be checked in the **Configuration Name** drop-down list.
3. Check the connectivity by clicking the connect icon as follows.

> **NOTE**
>
> You can see the message “The license connect success.” only when the following conditions are met:
>
> - The **License Portal URL**, **License Portal User**, and **License Portal Password** are entered correctly.
> - The network between AmpCon-DC and the License Portal is available.

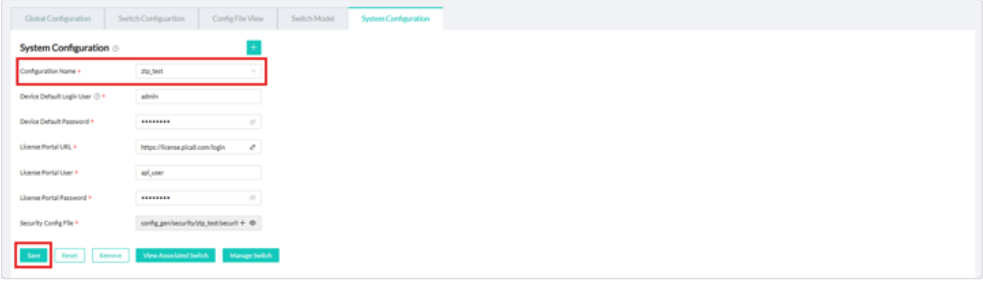


Viewing or Modifying a System Configuration

To view or edit a system configuration, follow these steps:

1. Click **Device > Device Profiles** from the navigation bar.
2. In the **System Configuration** tab, click the **Configuration Name** drop-down list, and select the system configuration name. Then, you can view the details of the system configuration.

   To modify the system configuration, modify the configuration items as needed, and then click **Save**.



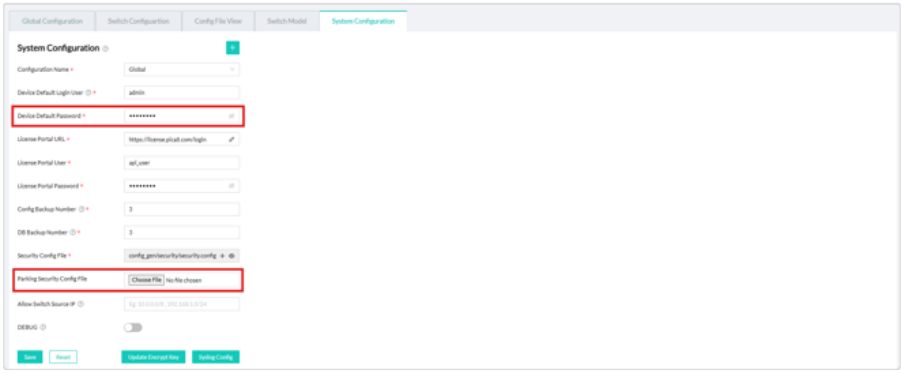
Changing the Default Switch Password

In system configurations, the default switch username is **admin**, and the default password is **pica8**. To change the default password, follow these steps:

1. Click **Device > Device Profiles** from the navigation bar.
2. In the **System Configuration** tab, select the system configuration to be modified in the **Configuration Name** drop-down list.
3. Change the default switch password as follows:

- **For global system configurations**

  a. Enter a new password in the **Device Default Password** field.



  b. Click **Browse** in the **Parking Security Config File** section, and then upload a .txt file containing the following command:

```
set system login user admin authentication plain-text-password <New-Password>
```

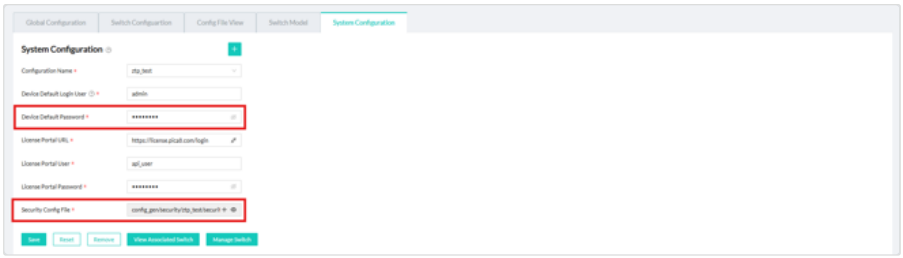
  Replace *<New-Password>* with the new password you want to use.

> **NOTE**
>
> Pay attention to the following notes. Or else, switches will fail to be deployed.

- Ensure that the new password in the .txt file and in the **Device Default Password** field are the same.
- Ensure that no service-related configurations are added to the **Parking Security Config File**.
- Ensure that the **Security Config File** doesn't contain any commands used to push service-related configurations or change the password of the **Device Default Login User**.

- **For non-global system configurations**

a. Enter a new password in the **Device Default Password** field.



b. Click **Browse** in the **Security Config File** section, and then upload a .txt file containing the following command:

```
set system login user admin authentication plain-text-password <New-Password>
```

Replace *<New-Password>* with the new password you want to use.

> **NOTE**
>
> Pay attention to the following notes. Or else, switches will fail to be deployed.
>
> - Ensure that the new password in the command and in the **Device Default Password** field are the same.
> - Ensure that the **Security Config File** doesn't contain commands used to push service-related configurations.

Configuring a DHCP Server

Before you provision switches through normal ZTP, you must configure the DHCP server as follows:

Procedure

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

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

```
host 4610_54t_02 {
hardware ethernet C4:39:3A:FF:2C:C0;
fixed-address 10.10.51.198;
option default-url "http://10.56.20.184/onie";
}
```

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

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

Replace “10.56.20.184” with the IP address of the AmpCon-DC server.

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

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

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

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

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

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

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

3. After the DHCP configurations are added, reboot the switches to be deployed. Or else, the normal ZTP will fail.

Provisioning Switches through Normal ZTP

Normal ZTP relies on the DHCP service, and thus you need to configure DHCP first. After you plug in and reboot a switch, DHCP automatically provides the switch with an IP address and the address of a provision shell script that is obtained from the AmpCon-DC server. Then, the switch automatically runs the shell script to complete the ZTP deployment:

- The white-box switch runs the shell script to download a PicOS image, install PicOS and its license, register with the AmpCon-DC server, update switch configurations, and reboot the switch.
- The integrated hardware and software switch runs the shell script to register with the AmpCon-DC server, update switch configurations, and reboot the switch.

To provision switches through normal ZTP, see the following information:

Before You Begin
Procedure
  Provisioning a White-Box Switch
  Provisioning an Integrated Hardware and Software Switch
What to Do Next

Before You Begin

Before you provision switches through normal ZTP, ensure that the following preparations are completed. Or else, the normal ZTP process might fail.

- Before you provision switches through ZTP, ensure that the prerequisite tasks described in Prerequisites have been completed.
- Ensure that you have prepared all the required configurations in the AmpCon-DC UI. For more information, see the following documents:

White-Box Switch	Integrated Hardware and Software Switch

Configuring Global Configurations Adding Configuration Templates Adding Switch Configurations Configuring Switch Models Adding System Configurations	Configuring Global Configurations Adding Configuration Templates Adding Switch Configurations Adding System Configurations

- Ensure that you have configured the DHCP server. For more information, see Configuring the DHCP Server.

Procedure

Provisioning a White-Box Switch

1. Download and install MobaXterm.
2. Open MobaXterm, and then create a session to connect with the switch.
3. Run the following commands to enter the Linux shell mode and reboot the switch:

```
start shell sh
```

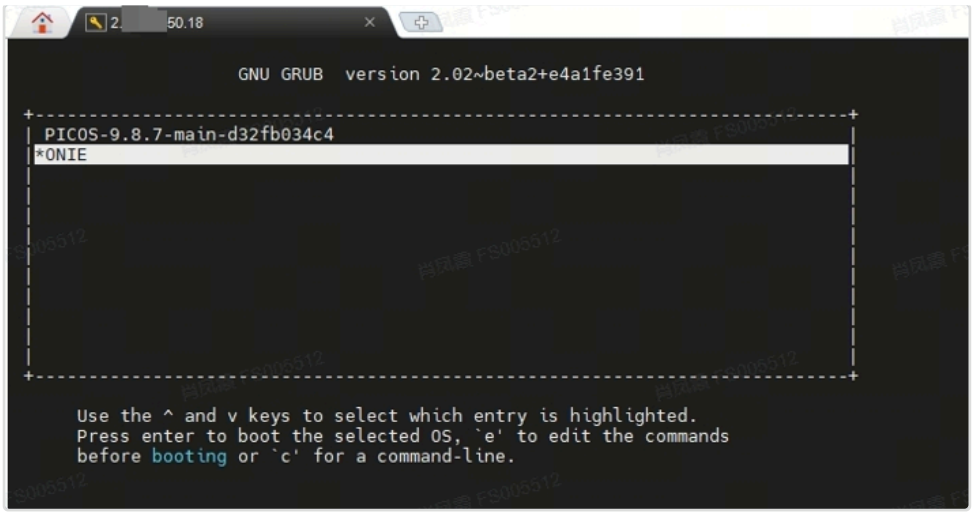
```
sudo reboot -f
```

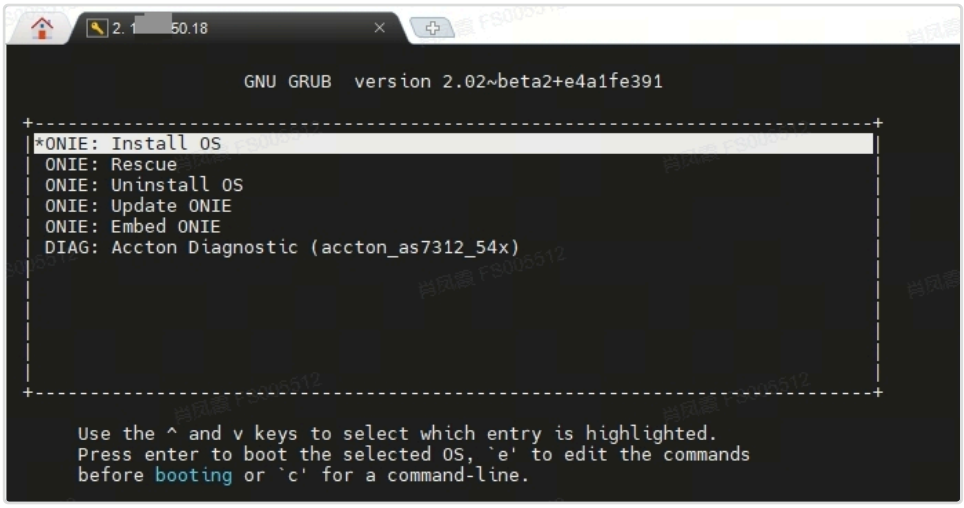
4. If you see the “Hit any key to stop autoboot” message, press the **Enter** key to exit the autoboot mode.

   If you don’t see this message, go to **Step 5** directly.

5. Reboot the switch.

- For switches with the ONIE menu, select **ONIE**, and then select **ONIE: Install OS**.



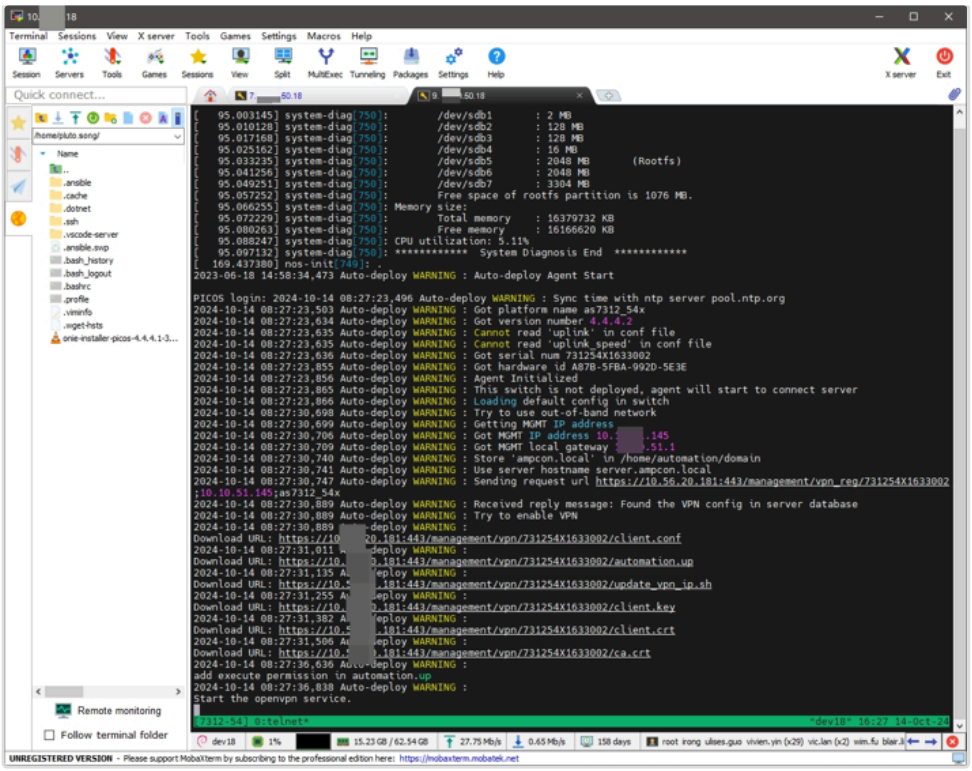


- For AS4610 switches, reboot from ONIE by running the following command:

```
run onie bootcmd
```

Then, the switch will be restarted and automatically register with the AmpCon-DC server.

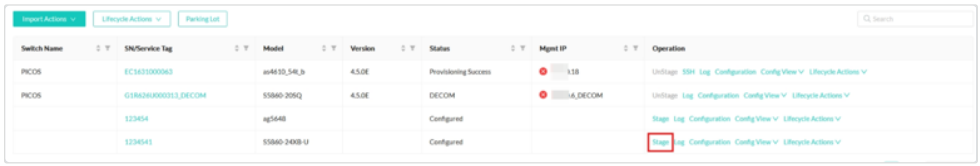
6. Wait for the registration process to be completed.



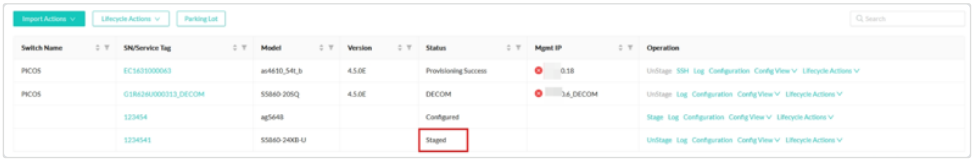
7. Check whether the hardware ID of the switch is included in any imported AmpCon-DC licenses. For more information, see Viewing AmpCon-DC Licenses.

   If the hardware ID of the switch is not included in any imported AmpCon-DC licenses, you must import an AmpCon-DC license to AmpCon-DC. Or else, the switch can't be provisioned successfully. For more information, see Importing Licenses for Deployed Switches.

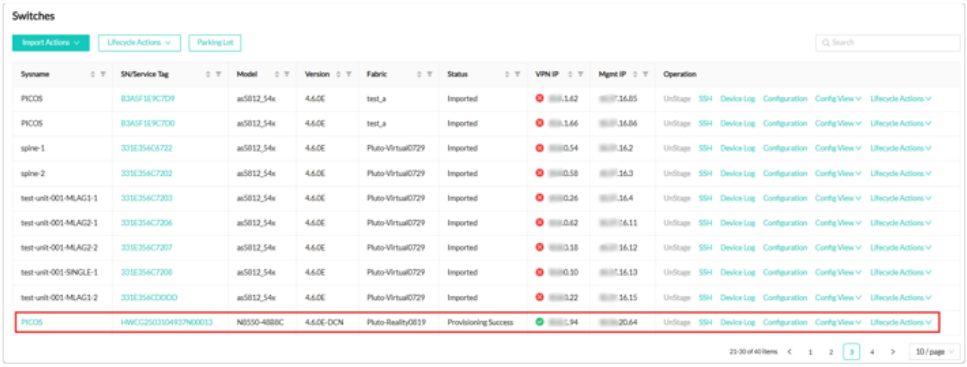
8. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar. In the **Switch** list, locate the switch, and then click **Stage.**



   Then, the switch status will be shown as **Staged**.



   After you stage the switch, the switch will be configured automatically based on the related system configuration and switch configuration. After the configurations are pushed successfully, the switch status will be changed to **Provisioning Success**.

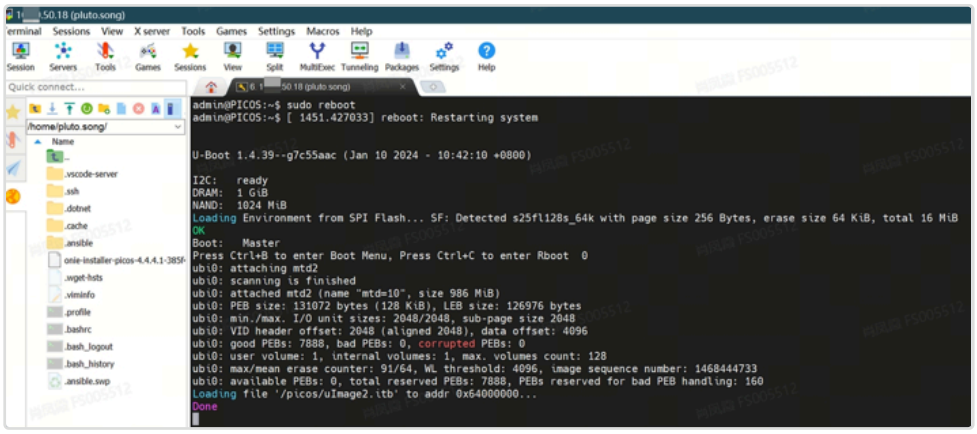


Provisioning an Integrated Hardware and Software Switch

1. Download and install MobaXterm.
2. Open MobaXterm, and then create a session to connect with the switch.
3. Run the following commands to enter the Linux shell mode and reboot the switch:

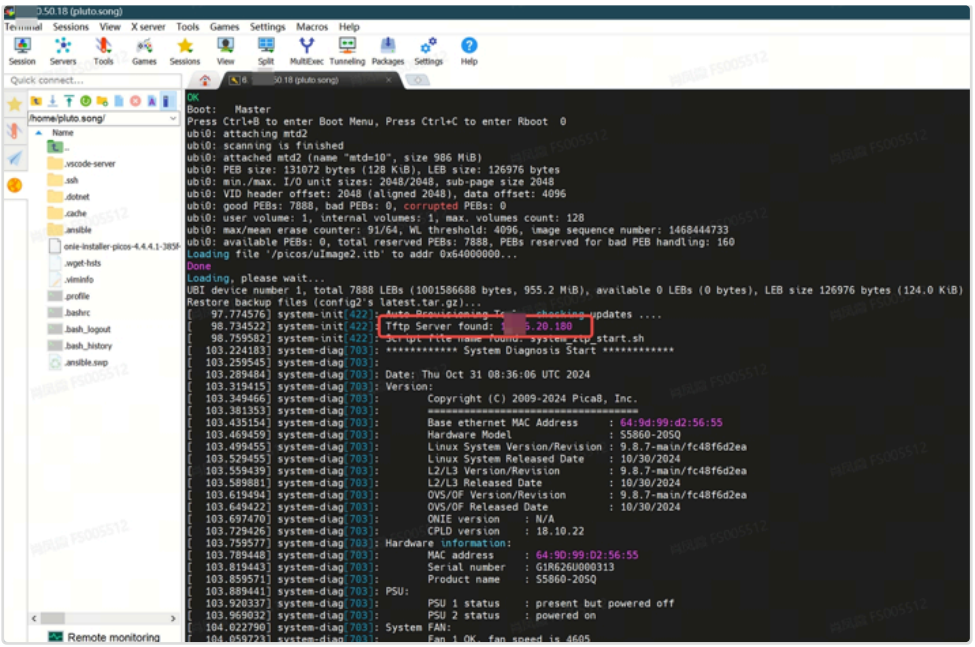
```
start shell sh
```

```
sudo reboot
```



Then, the switch will be restarted and automatically register with the AmpCon-DC server.

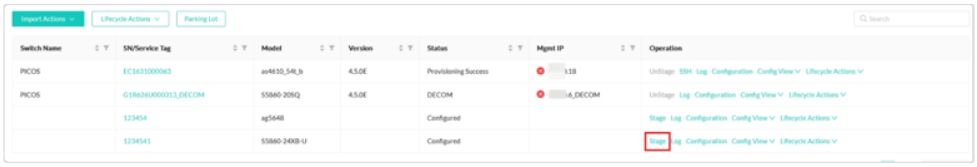
4. Wait for the registration process to be completed.



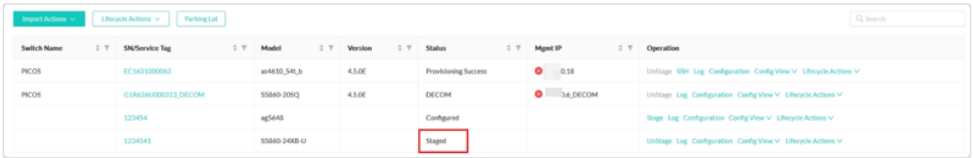
5. Check whether the hardware ID of the switch is included in any imported AmpCon-DC licenses. For more information, see Viewing AmpCon-DC Licenses.

   If the hardware ID of the switch is not included in any imported AmpCon-DC licenses, you must import an AmpCon-DC license to AmpCon-DC. Or else, the switch can't be provisioned successfully. For more information, see Importing Licenses for Deployed Switches.

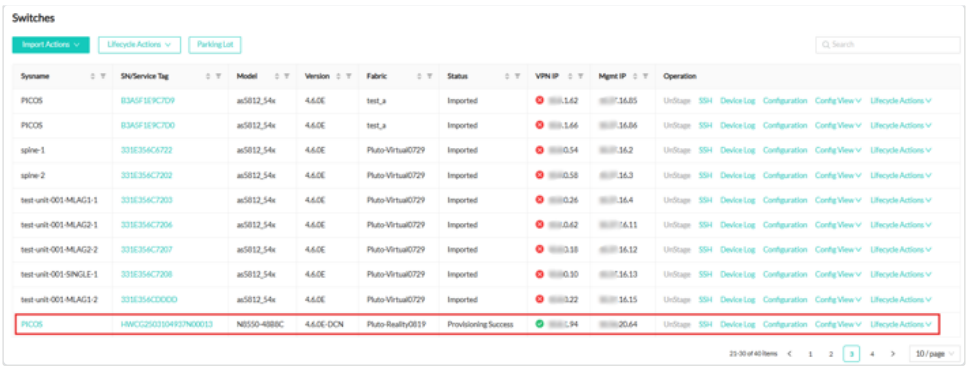
6. In the AmpCon-DC UI, click **Device > Switches**. In the **Switch** list, locate the switch, and then click **Stage.**



   Then, the switch status will be shown as **Staged**.



   After you stage the switch, the switch will be configured automatically based on the related system configuration and switch configuration. After the configurations are pushed successfully, the switch status will be changed to **Provisioning Success**.



What to Do Next

Now, the switch is managed by AmpCon-DC. You can continue to deploy other switches.

Or you can use key features of AmpCon-DC, such as configuring switches, managing switches, designing physical networks, and more.

Deploying Physical and Logical Networks

Underlay means the physical network infrastructure that serves as the foundational layer for data transmission. **Physical networks** are used for underlay provisioning.

Overlay is a virtual network architecture built on top of an existing physical network (underlay). Overlay services refer to virtualized network functions or logical layers, which enable logical network isolation and flexible service deployment and network configurations without modifying the underlying infrastructure. **Logical networks** are logical spaces to provision overlay services.

By using AmpCon-DC, you can deploy physical networks and logical networks to meet different networking requirements.

- Network Architecture
- Configuring Resources
- Deploying Physical Networks
  - Option 1: Simplified ZTP Deployment
  - Option 2: Designing Physical Networks
- Deploying Logical Networks

Network Architecture

Check the architecture of simplified ZTP, physical networks, and logical networks.

For more information, see Network Architecture.

Configuring Resources

Before you deploy physical networks, you must prepare the following resources:

Table 1. Resources for Physical Networks

Required Resource	Reference Link
1. Prepare IP pools. AmpCon-DC will automatically assign IP addresses during the simplified ZTP or physical network design process.	IP Pools
2. Prepare ASN pools. AmpCon-DC will automatically assign ASNs during the simplified ZTP or physical network design process.	ASN Pools

Before you deploy logical networks for overlay service provisioning, you must prepare the following resources:

Table 2. Resources for Logical Networks

Required Resource	Reference Link
1. Prepare VNI pools. VNI pools are used to automatically assign L2 VNI to logical switches and assign L3 VNI to logical routers.	VNI Pools
2. Prepare Point of Delivery (PoD). The overlay service provisioning process involves connecting virtual networks of PoD with logical switches.	Point of Delivery (PoD)
3. Prepare VLAN Domains. VLAN Domains restrict the allocation of VLAN IDs to a specific range for virtual networks connected to logical switches.	VLAN Domains
4. Prepare node uplink configurations for node devices in PoD. After you connect virtual networks of PoD with logical switches, node devices in the virtual networks can be connected to uplink switches based on node uplink configurations.	Node Uplink

Deploying Physical Networks

To deploy physical networks, you are provided with two options:

- You can use simplified ZTP to complete switch onboarding, physical network deployment, and RoCE configuration (optional) in one go.
- You can manually design physical networks after onboarding switches through the switch importing or normal ZTP method.

Option 1: Simplified ZTP Deployment

Simplified ZTP is a Zero Touch Provisioning (ZTP) method used to onboard switches, deploy physical networks, and configure RoCE (optional) in one go.

The simplified ZTP process can achieve the following goals in one go:

- A physical network (fabric) is deployed automatically.
- All switches in the fabric are bulk onboarded to AmpCon-DC. You don’t need to onboard each switch one by one.
- Optional: The RoCE policy configurations are applied to the switches in the fabric.

For more information, see Simplified ZTP Deployment.

> **NOTEs**
>
> - If you don't need to deploy physical networks, or if you want to design physical networks manually, do not use simplified ZTP.
> - Simplified ZTP can be used only for the switches with PicOS installed. For example, white-box switches with PicOS installed and integrated hardware and software PicOS switches.

Option 2: Designing Physical Networks

In data center networks, east-west traffic dominates the business traffic. Therefore, data centers have a high demand for horizontal scalability. To meet the evolving business requirements in data centers, including cloud scenarios, container scenarios, and AI computing scenarios, the physical network mode 3-stage fabric (leaf-spine-leaf) is introduced to AmpCon-DC.

After you onboard switches by using the switch importing or normal ZTP method, these switches are managed by AmpCon-DC. To quickly deploy physical networks with these switches, you can use AmpCon-DC to design and deploy a modern 3-stage fabric.

For more information, see Designing Physical Networks.

> **NOTE**
>
> If you use simplified ZTP, switch deployment and physical network deployment can be completed in one go, and thus you don't need to design physical networks.

Deploying Logical Networks

After a physical network is deployed, you can deploy logical networks for overlay service provisioning.

Overlay service configurations are abstracted into **logical network elements**, including logical networks, logical routers, logical switches, and virtual networks. In the AmpCon-DC UI, provision these logical network elements to complete the logical network deployment.

For more information, see Provisioning Overlay Services.

Network Architecture

Before you deploy physical or logical networks, check the following architecture:

Physical Network Architecture
  Physical Network Design
  Simplified ZTP Architecture
Logical Network Architecture

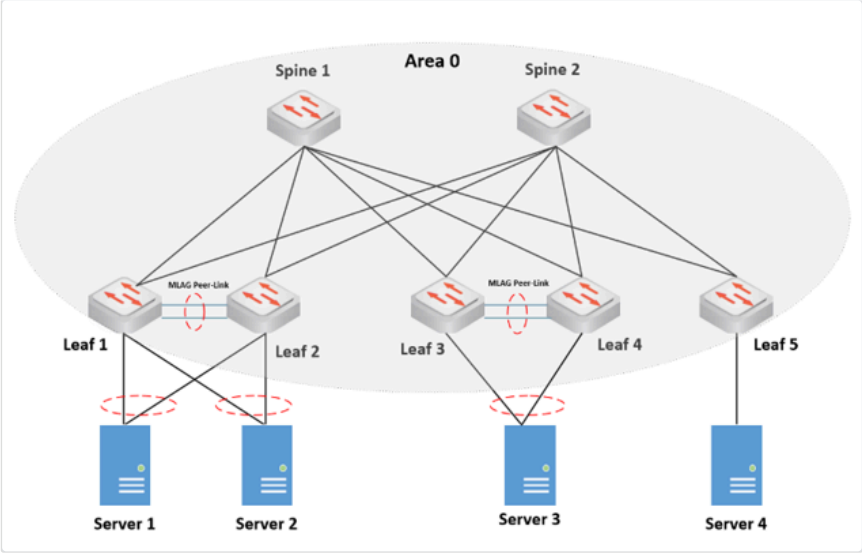
Physical Network Architecture

Physical Network Design

You can deploy a physical network through the **physical network design** feature. The architecture of 3-stage fabrics deployed through this feature is as follows:

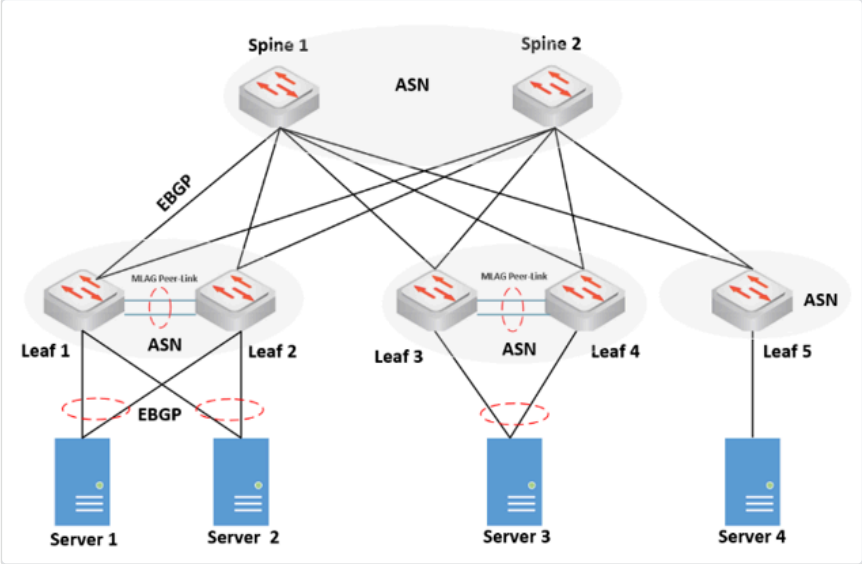
- The control plane adopts MP-BGP EVPN, which has excellent scalability, reduces broadcast dependency, automatically discovers VTEP tunnels, and matches routing isolation capabilities (VRF) perfectly.
- Spine switches and leaf switches are interconnected by using Layer 3 Ethernet interfaces to build a full-mesh fabric network.
- To avoid single-point failure, leaf switches can be added to MLAG. In a dual-active system, one terminal device is connected to two MLAG peer leaf switches to achieve device-level link reliability.
- OSPF or BGP is used as the underlay routing protocol.
- If OSPF is selected as the underlay routing protocol, IBGP is used as the overlay control protocol. The underlay uses direct access addresses to establish OSPF neighbors, while the overlay uses loopback interfaces to establish EVPN IBGP neighbors between spine and leaf switches, with the spine nodes acting as Route Reflectors (RR).

Figure 1. Fabric Architecture with OSPF



- If BGP is selected as the underlay routing protocol, MP-EBGP EVPN is used as the overlay control protocol. The underlay uses direct access addresses to establish EBGP neighbors, while the overlay uses direct access addresses to establish EVPN EBGP neighbors between spine and leaf switches.

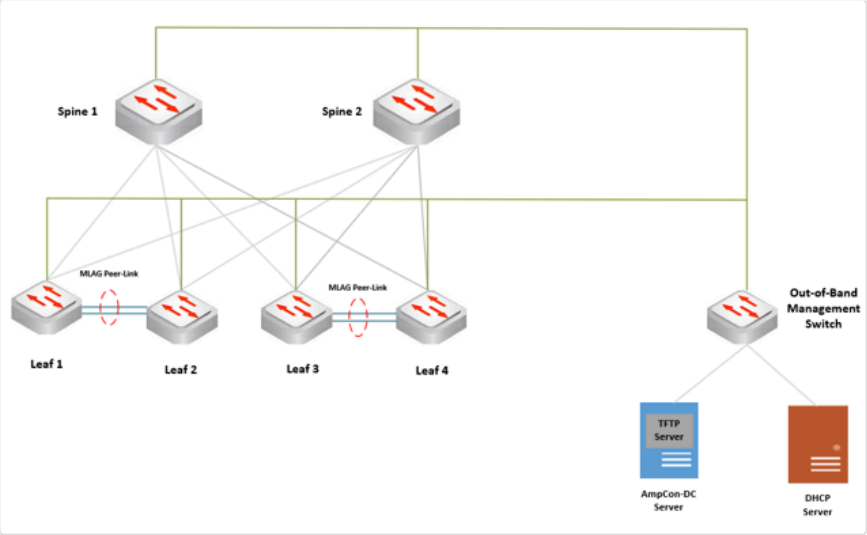
Figure 2. Fabric Architecture with BGP



Simplified ZTP Architecture

You can deploy a physical network through the **simplified ZTP** feature. The architecture of 3-stage fabrics deployed through this feature is as follows:

Figure 3. Simplified ZTP Architecture



- **3-Stage Fabric:** simplified ZTP automatically designs and deploys a 3-stage fabric based on the spine count and leaf count specified in the ZTP template. The architecture of the 3-stage fabrics deployed through the simplified ZTP feature is almost the same as the fabric architecture as described in the Physical Network Design section, except for the following differences:
  - If you deploy a fabric through simplified ZTP, all the leaf switches in the fabric must be the same type: MLAG switches or non-MLAG switches.
  - When the network type is VLAN and the leaf strategy is non-MLAG, you can choose whether to enable RoCE in the ZTP template, enabling Zero Touch Provisioning (ZTP) for RoCE networks.
- **Out-of-Band Management Switch**: A forwarding device on the out-of-band management network. You need to manually pre-configure the out-of-band management switch because AmpCon-DC does not manage it. Spine and leaf switches communicate with the DHCP server through the out-of-band management switch.

  simplified ZTP supports only out-of-band networking, which means AmpCon-DC uses an independent management network to transmit management traffic of the switches to be deployed.
- **Management Port:** AmpCon-DC uses eth0 as the management port. Only eth0 has DHCP enabled by default. During the simplified ZTP process, eth0 is used to communicate with the DHCP server to assign management IP addresses for managed switches.
- **TFTP Server:** The AmpCon-DC server includes a built-in TFTP server, which is used to store configuration files, scripts, and license files.
- **DHCP Server:** simplified ZTP relies on DHCP. AmpCon-DC does not include a built-in DHCP server, and thus you need to prepare a third-party DHCP server.

- **Bringing Switches Online**: During the simplified ZTP process, you need to bring all spine switches online first. After all spine switches go online, continue to bring all leaf switches online.

  After all spine and leaf switches go online, all these switches are managed by AmpCon-DC, and the physical network is deployed successfully.

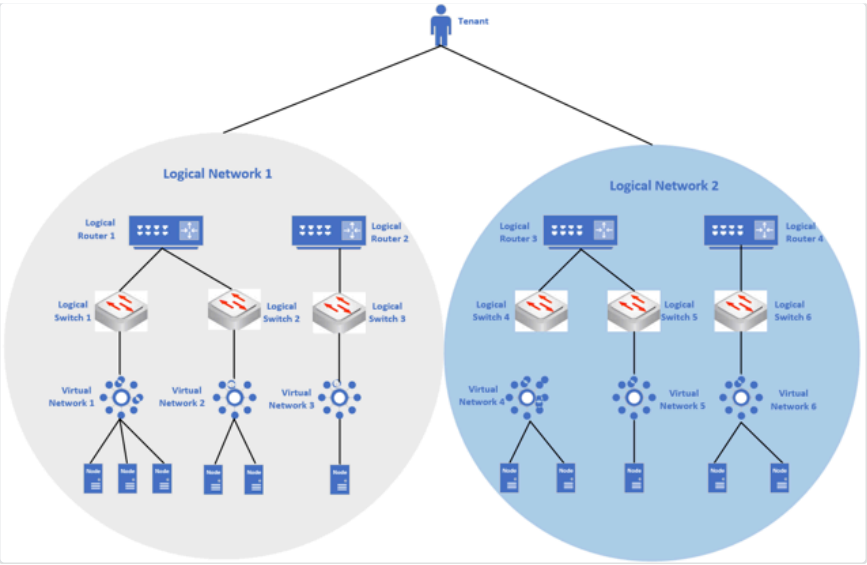
Logical Network Architecture

To provision overlay services, you need to deploy logical networks. Logical networks are deployed based on tenants. Using tenants to manage logical networks provides the following benefits:

- **Resource Control**
  You can create one or multiple tenants. A tenant has quotas for logical routers and logical switches. Logical networks owned by the tenant consume resources from these quotas, ensuring controlled resource usage.
- **Restricted Resource Scope**
  A tenant can only use the VPCs and fabrics bound to it. Therefore, logical networks owned by the tenant can add only virtual networks from these VPCs and can be deployed only on the associated fabrics.
- **Tenant Isolation and Access Control**
  Tenants are isolated from each other. AmpCon-DC users can manage the tenants assigned to them. As a result, each AmpCon-DC user can manage only the logical networks owned by the tenants the user manages.

The architecture of logical networks in AmpCon-DC is as follows:

Figure 4. Logical Network Architecture



- A tenant can create one or multiple logical networks.
- A logical network can contain one or multiple logical routers.
- A logical router can connect with one or multiple logical switches.
- A logical switch can connect with at most one logical router. A logical switch can connect with at most one virtual network.
- A virtual network can connect with at most one logical switch.

Configuring Resources

Before you deploy switches and physical networks through simplified ZTP, or before you manually design physical networks, you must prepare **IP pools** and **ASN pools**. AmpCon-DC will automatically assign IP addresses and ASNs during the simplified ZTP or physical network design process.

Before you deploying logical networks for overlay service provisioning, you must prepare the following resources:

- Prepare **VNI pools**. VNI pools are used to automatically assign L2 VNI to logical switches and assign L3 VNI to logical routers.
- Prepare **Point of Delivery (PoD)**. The overlay service provisioning process involves connecting virtual networks of PoD with logical switches.
- Prepare **VLAN Domains**. VLAN Domains restrict the allocation of VLAN IDs to a specific range for virtual networks connected to logical switches.
- Prepare **node uplink** configurations for node devices in PoD. After you connect virtual networks of PoD with logical switches, node devices in the virtual networks can be connected to uplink switches based on node uplink configurations.

See the following child topics:

- Resource Pools
  - IP Pools
  - ASN Pools
  - VNI Pools
- Resource Interconnections
  - Point of Delivery (PoD)
  - VLAN Domains
  - Node Uplink

Resource Pools

To deploy physical networks, add IP pools and ASN pools first. AmpCon-DC will automatically assign IP addresses and ASNs during the physical network deployment process.

To deploy logical networks for overlay service provisioning, add VNI pools first. In AmpCon-DC, VNI pools are used to automatically assign L2 VNIs to logical switches and assign L3 VNIs to logical routers.

For more information, see the following child topics:

- IP Pools
- ASN Pools
- VNI Pools

IP Pools

To deploy a physical network with AmpCon-DC, you need to add IP pools. AmpCon-DC automatically assigns IP addresses to switches based on the specified IP pools.

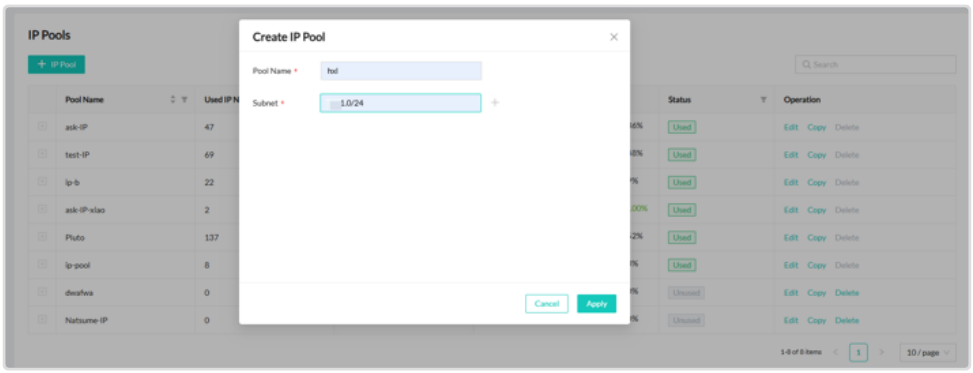
Currently, only IPv4 is supported.

Adding IP Pools
Optional: Viewing IP Pools
Optional: Editing IP Pools
Optional: Copying IP Pools
Optional: Deleting IP Pools

Adding IP Pools

To add an IP pool, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Pools > IP Pools** from the navigation bar.
2. Click **+ IP Pool**.
3. In the **Pool Name** field, enter the name of the IP pool.
4. In the **Subnet** field, enter a subnet. To add multiple subnets, click **+**.



5. Click **Apply**.

Optional: Viewing IP Pools

On the “IP Pools” page, you can see the following IP address statistics and usage information:

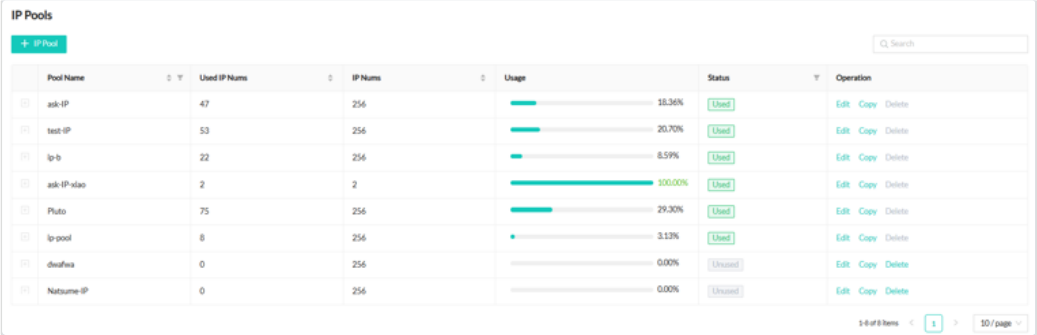


Table 1. IP Pool Metrics

Metric	Description
Pool Name	A unique name to identify the resource pool
Used IP Nums	The number of IP addresses in use in the pool
IP Nums	The total number of IP addresses in the pool
Usage	The percentage of IP addresses in use for all IP addresses in the pool
Status	Whether the pool is in use

Click **+** before a pool name. You can see the IP ranges assigned to this IP pool.

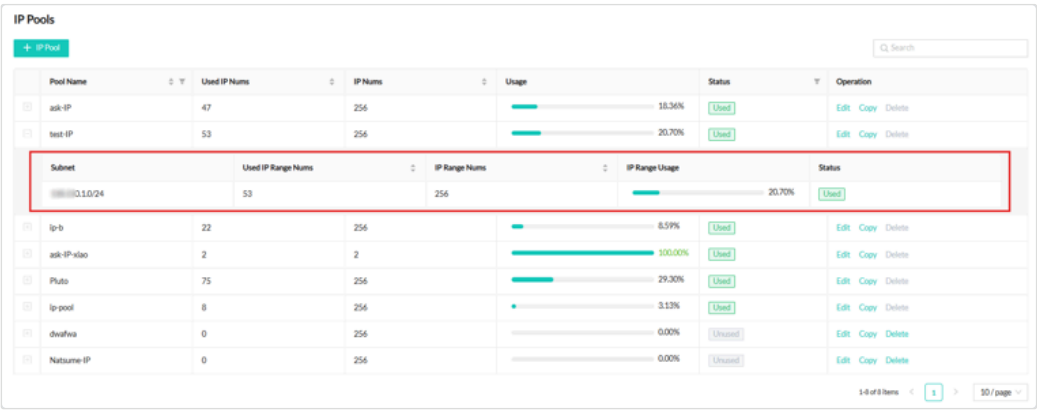


Table 2. IP Range Metrics

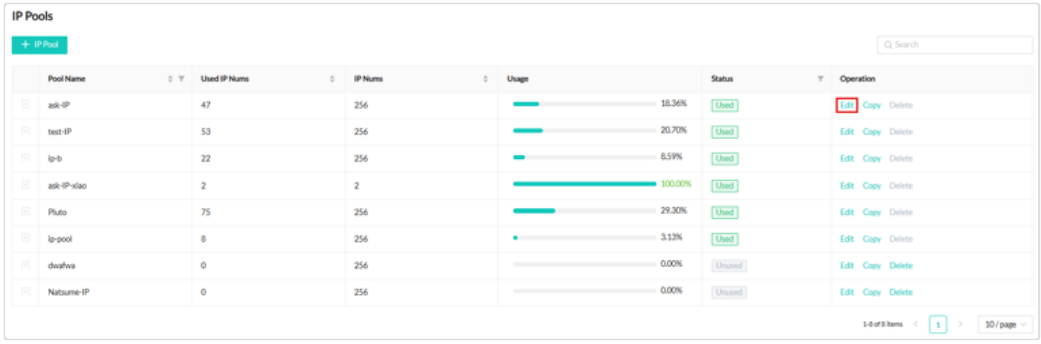
Metric	Description
Subnet	The IP addresses included in the subnet
Used IP Range Nums	The number of IP addresses in use in the subnet

IP Range Nums	The total number of IP addresses included in the subnet
IP Range Usage	The percentage of IP addresses in use in this subnet for all IP addresses in this subnet
Status	Whether the subnet is in use

Optional: Editing IP Pools

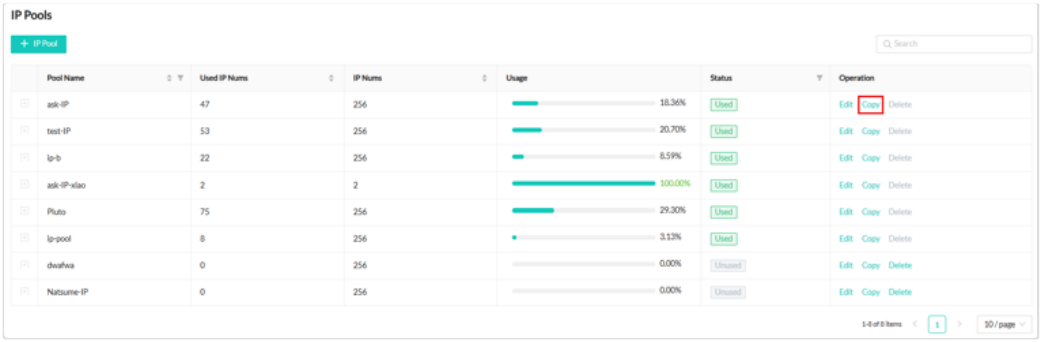
To edit an IP pool, locate the IP pool on the “IP Pools” page, and then click **Edit**.

> **NOTEs**
>
> - When you edit an IP pool range, pay attention to the following restrictions:
>   - If an IP pool is in **Used** status, its subnet can only be expanded and can't be narrowed down.
>   - If an IP pool is in **Unused** status, you can expand or narrow down its subnet as needed.
>   - To add a new subnet, click **+** in the **Subnet** section. Each added subnet cannot overlap.



Optional: Copying IP Pools

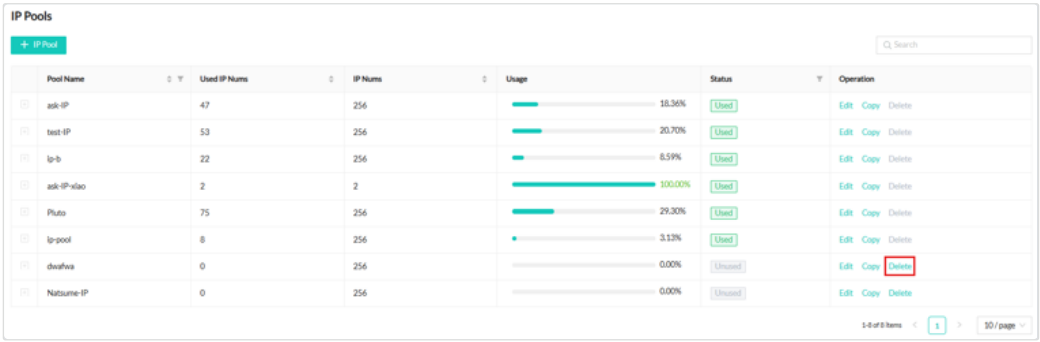
To copy an IP pool, locate the IP pool on the “IP Pools” page, and then click **Copy**.



Optional: Deleting IP Pools

To delete an IP pool, locate the IP pool on the “IP Pools” page, and then click **Delete**.

> **NOTEs**
>
> - You can delete only IP pools that are not used, which means the **Status** column of the IP pool is displayed as **Unused**.
> - To delete an IP pool, delete the fabrics that are using the IP pool first.



ASN Pools

Autonomous system numbers (ASNs) are used to support BGP in the underlay network.

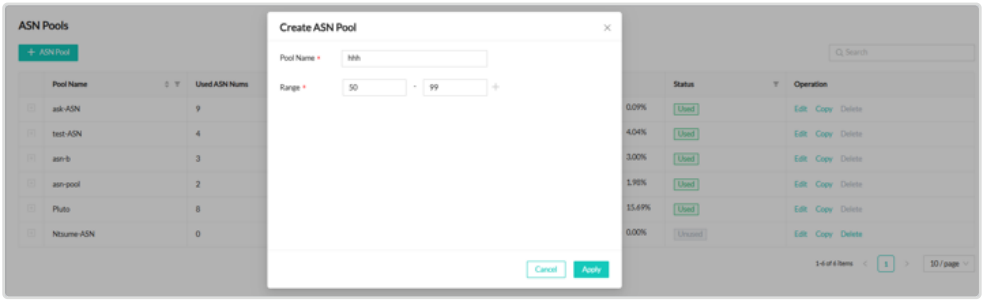
To deploy a physical network with AmpCon-DC, you need to add ASN pools. AmpCon-DC automatically assigns ASNs to switches based on the specified ASN pools.

Adding ASN Pools
Optional: Viewing ASN Pools
Optional: Editing ASN Pools
Optional: Copying ASN Pools
Optional: Deleting ASN Pools

Adding ASN Pools

To add an ASN pool, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Pools > ASN Pools** from the navigation bar.
2. Click **+ ASN Pool**.
3. In the **Pool Name** field, enter the pool name.
4. In the **Range** field, specify the ASN range of the ASN pool.



5. Click **Apply**.

Optional: Viewing ASN Pools

On the “ASN Pools” page, you can see the following ASN statistics and usage information:

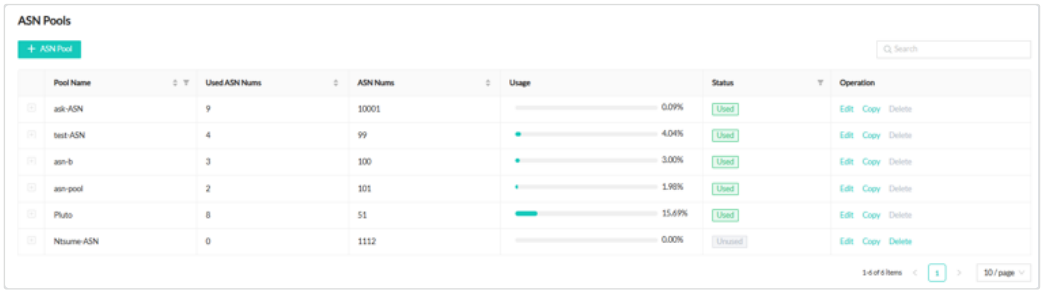


Table 1. ASN Pool Metrics

Metric	Description
Pool Name	A unique name to identify the resource pool.
Used ASN Nums	The number of ASNs in use in the pool.
ASN Nums	The total number of ASNs in the pool.
Usage	The percentage of ASNs in use for all ASN ranges in the pool.
Status	Whether the pool is in use.

Click **+** before a pool name. You can see the ASN ranges assigned to this ASN pool.



Table 2. ASN Range Metrics

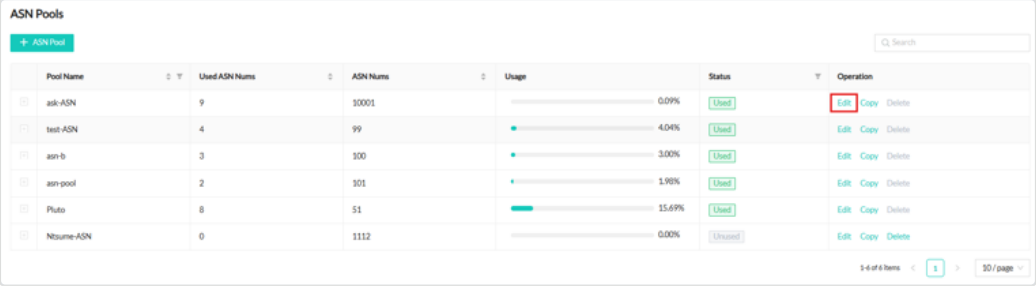
Metric	Description
ASN Range	The ASNs included in the range.
Used ASN Range Nums	The number of ASNs in use in the ASN range.
ASN Range Nums	The total number of ASNs included in the ASN range.
ASN Range Usage	The percentage of ASNs in use in this range for all ASNs in this ASN range.
Status	Whether the ASN range is in use.

Optional: Editing ASN Pools

To edit an ASN pool, locate the ASN pool on the “ASN Pools” page, and then click **Edit**.

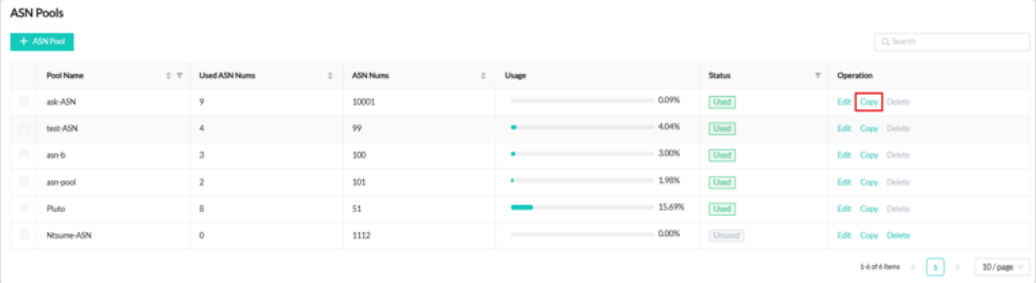
NOTEs

- When you edit an ASN pool range, pay attention to the following restrictions:
  - If an ASN pool is in **Used** status, the ASN range can only be expanded and can't be narrowed down.
  - If an ASN pool is in **Unused** status, you can expand or narrow down the ASN range as needed.
  - To add a new ASN range, click **+** in the **Range** section. Each added ASN range cannot overlap.



Optional: Copying ASN Pools

To copy an ASN pool, locate the ASN pool on the “ASN Pools” page, and then click **Copy**.

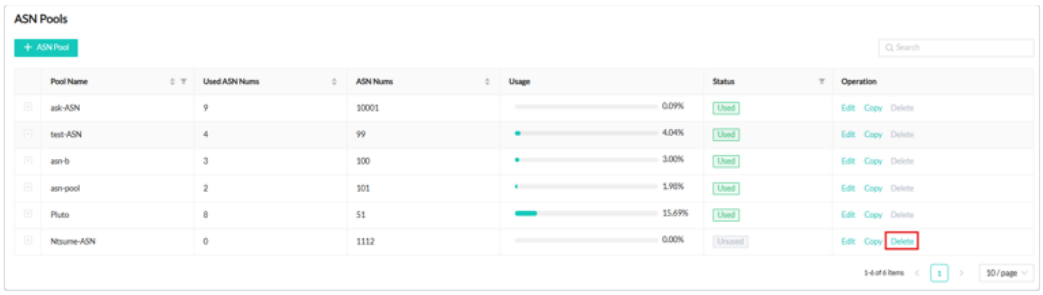


Optional: Deleting ASN Pools

To delete an ASN pool, locate the ASN pool on the “ASN Pools” page, and then click **Delete**.

NOTEs

- You can delete only ASN pools that are not used, which means the **Status** column of the ASN pool is displayed as **Unused**.
- To delete an ASN pool, delete the fabrics that are using the ASN pool first.


ASN Pools
+ ASN Pool
Search
Pool Name
Used ASN Nums
ASN Nums
Usage
Status
Operation
ask-ASN 9 10001 0.09% Used Edit Copy Delete
test-ASN 4 99 4.04% Used Edit Copy Delete
asn-b 3 100 3.00% Used Edit Copy Delete
asn-pool 2 101 1.98% Used Edit Copy Delete
Pluto 8 51 15.69% Used Edit Copy Delete
Ntsume-ASN 0 1112 0.00% Unused Edit Copy Delete
1-6 of 6 items
1
10 / page

VNI Pools

Virtual Network Identifiers (VNIs) are used to distinguish different virtual networks in the Virtual Extensible Local Area Network (VXLAN).

To deploy logical networks for overlay service provisioning, you need to add VNI pools first. In AmpCon-DC, VNI pools are used to automatically assign a L2 VNIs to logical switches and assign a L3 VNIs to logical routers.

VNI Pool Assignment Rules
Prerequisites
Adding VNI Pools
Optional: Viewing VNI Pools
Optional: Editing VNI Pools
Optional: Deleting VNI Pools

VNI Pool Assignment Rules

Before you assign a VNI to logical switches and logical routers, AmpCon-DC automatically verifies whether the VNI pool bound to the fabric has enough available VNI values for assignment.

VNI values in a VNI pool are assigned based on the following assignment rules:

- A fabric can be bound to at most one VNI pool, while a VNI pool can be bound to one or multiple fabrics.
- The VNI value assigned to each logical switch and logical router is unique.
- For a VNI pool with multiple VNI ranges, VNI values are assigned in ascending numerical order.
- The VNI pool supports dynamic reclamation, which means that the VNI value is released when it's not used by a logical router or logical switch, and the VNI value can be reassigned based on the ascending numerical order.

By using AmpCon-DC, you can avoid conflicts caused by using occupied VNI and save resources through dynamic reclamation.

Prerequisites

Ensure that you have created the fabrics bound to the VNI pools to be added.

Adding VNI Pools

To add a VNI pool, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Pools > VNI Pools** from the navigation bar.
2. On the “VNI Pools” page, click **+ VNI Pool**.
3. In the pop-up window, input the following information:

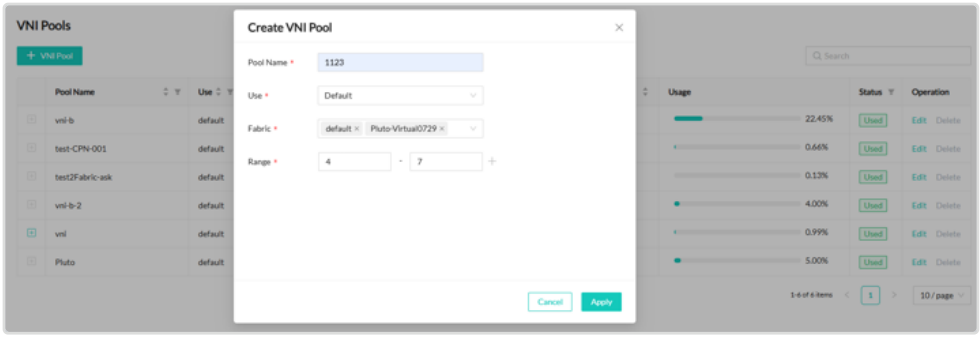


Table 1. VNI Pool Parameters

Parameter	Description
Pool Name	The name of the VNI pool. The value must be unique.
Use	The purpose of the VNI pool. Currently, only **Default** is displayed, which means the VNI pool is only used for internal network interconnection.
Fabric	The fabrics bound to this VNI pool. Only the fabrics added previously on the “Fabrics” page are displayed. You can select one or multiple fabrics.
Range	The VNI ranges of the VNI pool. Available VNI values range from 1 to 16777215. To add multiple VNI ranges, click **+**. You can add a maximum of 1024 VNI ranges. Example VNI pool Range: 30-300, 400, 509, 1600-2000. **NOTE** Duplicate VNI ranges are not allowed, either within a single VNI pool or across different

	VNI pools in different fabrics.

4. Click **Apply**.

Optional: Viewing VNI Pools

On the “VNI Pools” page, you can see the following information of each VNI pool:

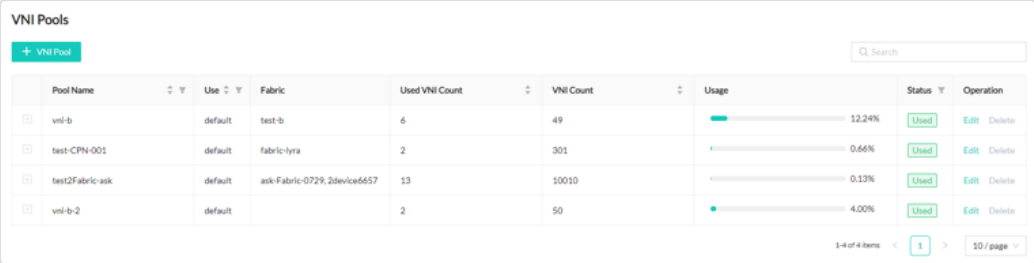


Table 2. VNI Pool Metrics

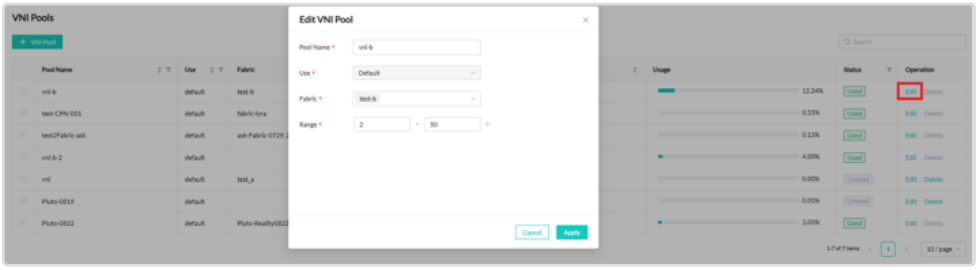
Metric	Description
Pool Name	A unique name to identify the VNI pool.
Use	The purpose of the VNI pool. Currently, only **Default** is supported.
Fabric	The fabric bound to the VNI pool.
VNI Range	The ranges of the VNI pool.
Used VNI Count	The total number of VNI values that are used in the pool. A VNI pool is used means when VNI values are assigned automatically to logical switches or logical routers as L2 VNI or L3 VNI.
VNI Count	The total number of VNI values in the pool.
Usage	The percentage of used VNI values for all VNI ranges in the pool.
Status	Indicates whether the VNI pool is used.

Optional: Editing VNI Pools

1. Locate the VNI pool on the “VNI Pools” page, and then click **Edit**.

2. In the **Edit VNI Pool** pop-up window, modify the **Pool name**, **Fabric**, and **Range** fields as needed. The **Use** field can't be modified.

> **NOTE**
>
> When you edit a VNI pool range, pay attention to the following restrictions:
>
> - If a VNI pool is in **Used** status, the VNI range can only be expanded and can't be narrowed down.
> - If a VNI pool is in **Unused** status, you can expand or narrow down the VNI range as needed.
> - To add a new VNI range, click **+** in the **Range** section. Each added VNI range cannot overlap.

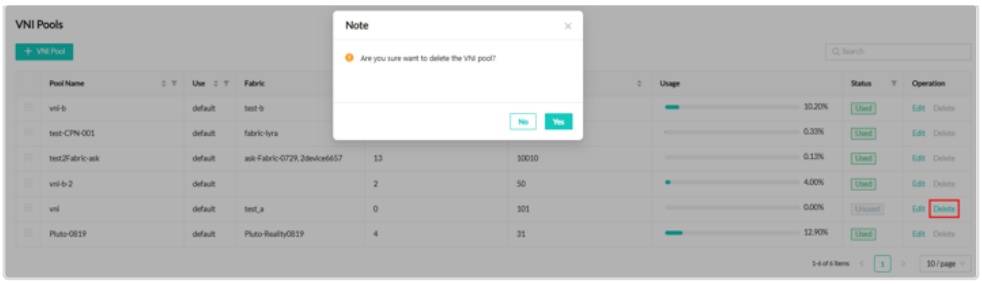


3. Click **Apply**.

Optional: Deleting VNI Pools

1. Locate the VNI pool on the "VNI Pools" page, and then click **Delete**.
2. In the **Note** pop-up window, click **Yes**.

> **NOTEs**
>
> - The VNI pools being used can't be deleted.
> - To delete a VNI pool, delete logical switches and logical routers in the fabrics bound to this VNI pool first.


VNI Pools
+ VNI Pool
Search
Pool Name
Use
Fabric
Usage
Status
Operation
vni-b
default
test-b
10.20%
Used
Edit
Delete
test-CFN-001
default
fabric-lyra
0.33%
Used
Edit
Delete
test2Fabric-ask
default
ask-Fabric-0729, 2device6657
13
10010
0.13%
Used
Edit
Delete
vni-b-2
default
2
50
4.00%
Used
Edit
Delete
vni
default
test_a
0
101
0.00%
Unused
Edit
Delete
Pluto-0819
default
Pluto-Reality0819
4
31
12.90%
Used
Edit
Delete
1-6 of 6 items
1
10 / page
Note
Are you sure want to delete the VNI pool?
No
Yes

Resource Interconnections

AmpCon-DC supports the following resource interconnections:

- Point of Delivery (PoD)
- VLAN Domains
- Node Uplink

Point of Delivery

Point of Delivery (PoD), the minimum service unit of a data center, is a collection of resources in a data center. PoD includes three types: bare metal PoD, vSphere PoD, and OpenStack PoD. In AmpCon-DC, each PoD contains only one type of resources.

In the AmpCon-DC UI, you can view VPC, network, and VM (available for only vSphere or OpenStack PoD) resources of each added PoD.

The overlay service provisioning process involves connecting virtual networks of bare metal PoD or vSphere PoD with logical switches. So before provisioning overlay services, you must add the required PoD to AmpCon-DC and allocate VPCs of these added PoD to tenants. For more information, see Provisioning Overlay Services.

See the following child topics:

- vSphere PoD
- OpenStack PoD
- Bare Metal PoD
- Managing VPCs

> **NOTE**
>
> OpenStack PoD can’t be used for overlay service provisioning.

vSphere PoD

To use node devices in VMware vSphere for overlay service provisioning, add vSphere PoD to AmpCon-DC, and allocate VPCs of these added vSphere PoD to tenants.

In the AmpCon-DC UI, you can view VPC, network, and VM related resources of these added vSphere PoD.

AmpCon-DC supports only VMware vSphere 8.0 currently.

- Prerequisites
- Adding a vSphere PoD
  - VLAN Assignment Rules
- Allocating VPCs
- Optional Operations
  - Viewing a vSphere PoD
    - VPC Tab
    - Network Tab
    - VM Tab
  - Searching for VPCs
  - Editing a vSphere PoD
  - Deleting a vSphere PoD

Prerequisites

- Ensure that the currently logged-in user is granted built-in or custom roles with the Read and Write permissions to the **PoD** tab. For more information, see Managing Roles.
- If you need to add a vSphere PoD, ensure that the fabric to which the vSphere PoD belongs has been created. For more information, see Adding a Fabric.
- If you need to allocate VPCs of a vSphere PoD to a tenant for logical network deployment, ensure that the fabric to which the vSphere PoD belongs meets all of the following conditions:
  - The fabric has been deployed through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.
  - The fabric is associated with the tenant. For more information, see Viewing a Tenant.

Adding a vSphere PoD

To add a vSphere PoD, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Resource Interconnection** from the navigation bar.
2. In the **PoD** tab, click **+ PoD**.
3. In the pop-up window, input the following information:

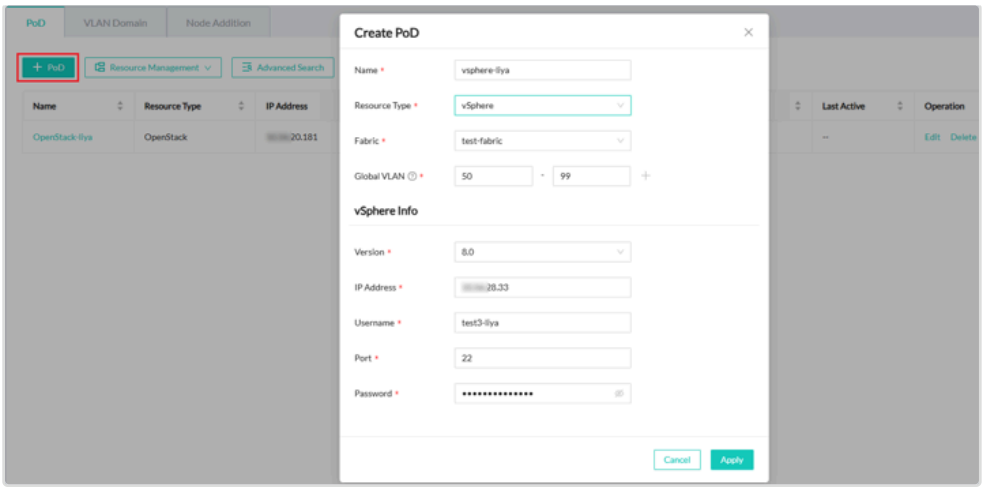


Table 1. vSphere PoD Parameters

Parameter	Description
Name	The name of the vSphere PoD.
Resource Type	Select **vSphere**.
Fabric	The fabric to which the PoD belongs.
Global VLAN	Optional. The VLAN range that can be assigned to the PoD. The supported global VLAN range is 2 to 3965. Click **+** to add multiple global VLAN ranges. **NOTE** Ensure that the **Global VLAN** range has available intersections with the **Bridge Domain Range** in the related VLAN Domain. Or else, when you add a logical switch, VLANs will fail to be assigned. For detailed VLAN assignment rules, see the VLAN Assignment Rules section.
Version	The version of vSphere. Currently, you can select only **8.0**.
IP Address	The IP address of the vCenter server.

Username	The administrator username used to log in to the vSphere environment.
Port	The port number used to connect to the vCenter server.
Password	The password associated with the username.

For more information about vSphere parameters, see vSphere Automation API**.**

4. Click **Apply**.

VLAN Assignment Rules

When you add a logical switch, VLAN is assigned based on the following rules:

- AmpCon-DC assigns a VLAN from the intersection between the **Global VLAN** range and the **Bridge Domain Range** in the related VLAN Domains.
- VLANs cannot be assigned in the following cases:
  - The **Global VLAN** range and the **Bridge Domain Range** have no intersection.
  - All intersection VLANs between the **Global VLAN** ranges and the **Bridge Domain Range** are used up.

Allocating VPCs

After you add a vSphere PoD, to use some VPCs of this PoD for logical network deployment, you must allocate these VPCs to tenants. For detailed steps, see Allocating VPCs to Tenants.

> **NOTE**
>
> If a VPC is not allocated to a tenant, the virtual network related to the VPC can't be added to the logical networks belonging to the tenant. For more information, see Adding Virtual Networks.

Optional Operations

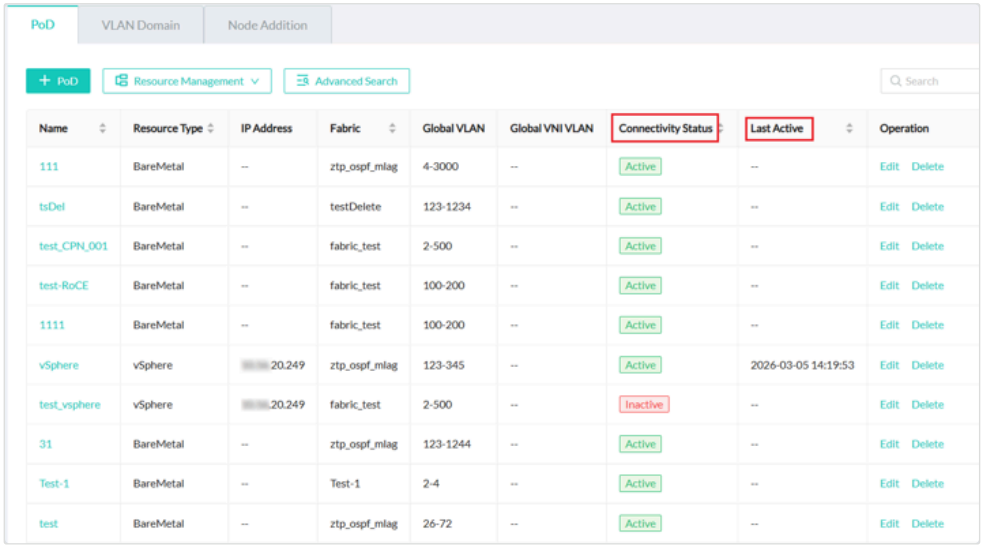
Viewing a vSphere PoD

In the **PoD** tab, check whether you can see the vSphere PoD that you created.

- **Connectivity Status** indicates the connection status of this PoD, which means whether AmpCon-DC can connect to the vSphere platform.
  - **Active:** AmpCon-DC is connected to the vSphere platform.

- **Inactive:** AmpCon-DC isn't connected to the vSphere platform.

- **Last Active** means the last time when AmpCon-DC is connected to the vSphere platform.
- For other metrics, see **Table 1. vSphere PoD Parameters** in the Adding a vSphere PoD section.



To view detailed resources in a specific vSphere PoD, click the name of the PoD. You can see the following tabs.

VPC Tab

In the **VPC** tab, you can view VPCs based on the roles assigned to the currently logged-in user:

- If the currently logged-in user is assigned only the Tenant Administrator role or assigned only the Tenant Administrator and ReadOnly roles, you can see only the VPCs allocated to the tenants managed by the currently logged-in user.
- If the currently logged-in user is assigned the SuperAdmin, Admin, or Operator role or assigned custom roles with the Read permission to the **PoD** tab, you can see all VPCs.



Table 2. VPC Metrics

Metric	Description
VPC ID	The ID assigned automatically by AmpCon-DC.

VPC Name	The name of the VPC.
Tenant	The tenant who owns the VPC. **NOTEs** • The value is **admin** if the VPC is created in AmpCon-DC 2.4. • The value is ***** if the VPC is allocated to a tenant that is not managed by the currently logged-in user. • The value is **--** if the VPC is not allocated to any tenant.
Fabric	The fabric to which the VPC belongs.
PoD	The PoD to which the VPC belongs.
Resource Create Time	The time when AmpCon-DC retrieves the VPC from vSphere for the first time.

Network Tab

In the **Network** tab, you can see all virtual networks in the vSphere PoD. In vSphere, the virtual network is called portgroup.

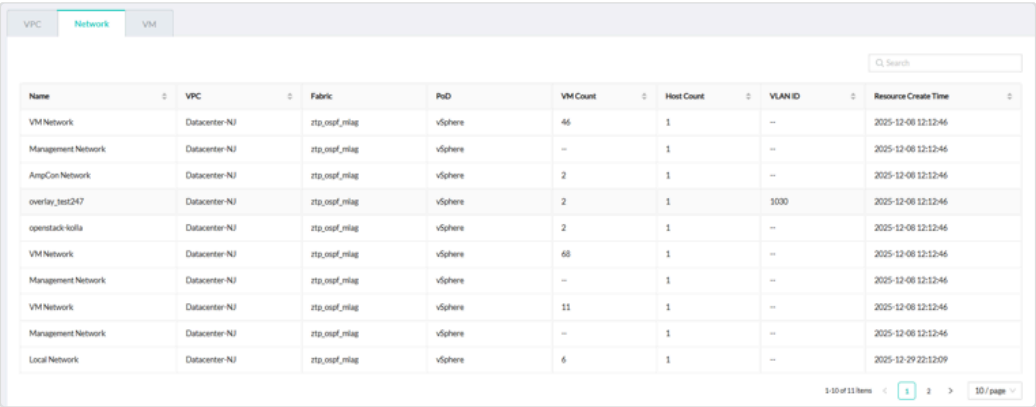


Table 3. Network Metrics

Metric	Description
Name	The portgroup name.
VPC	The data center name.

Fabric	The fabric to which the portgroup belongs.
PoD	The PoD to which the portgroup belongs.
VM Count	The count of VMs in the portgroup.
Host Count	The count of physical machines in the portgroup.
VLAN ID	The VLAN ID assigned to the portgroup.
Resource Create Time	The time when AmpCon-DC retrieves the network from vSphere for the first time.

VM Tab

In the **VM** tab, you can see all VMs in the vSphere PoD:

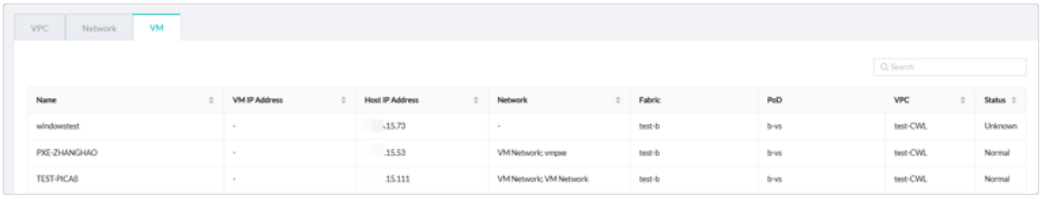
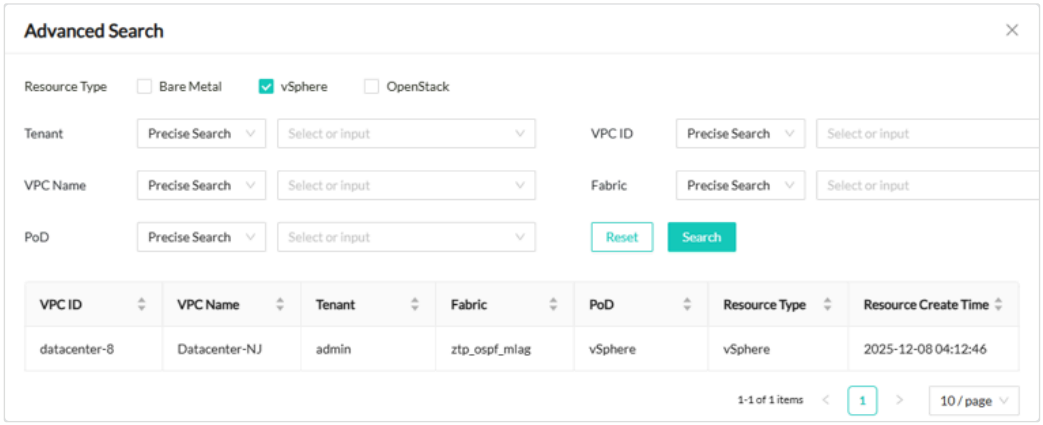


Table 4. VM Metrics

Metric	Description
Name	The VM name.
VM IP Address	The IP address of the VM.
Host IP Address	The IP address of the physical machine where the VM exists.
Network	The name of the portgroup to which the VM belongs.
Fabric	The fabric to which the VM belongs.
PoD	The PoD to which the VM belongs.
VPC	The data center to which the VM belongs.
Status	The status of the VM.

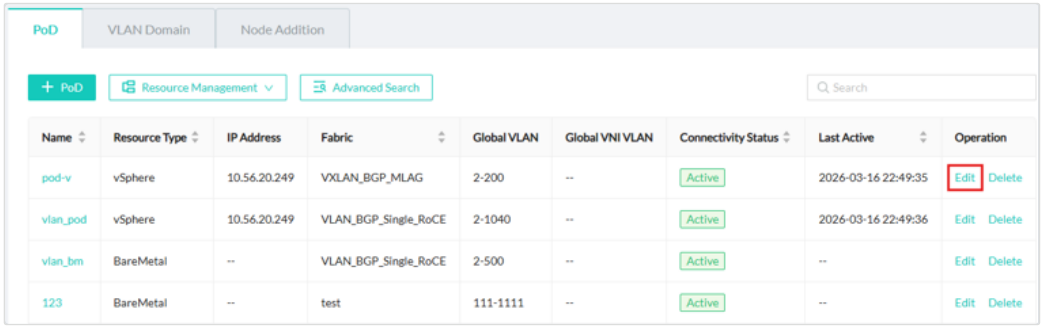
Searching for VPCs

To search for VPCs and view their details, click **Advanced Search**. For more information, see Searching for VPCs.



Editing a vSphere PoD

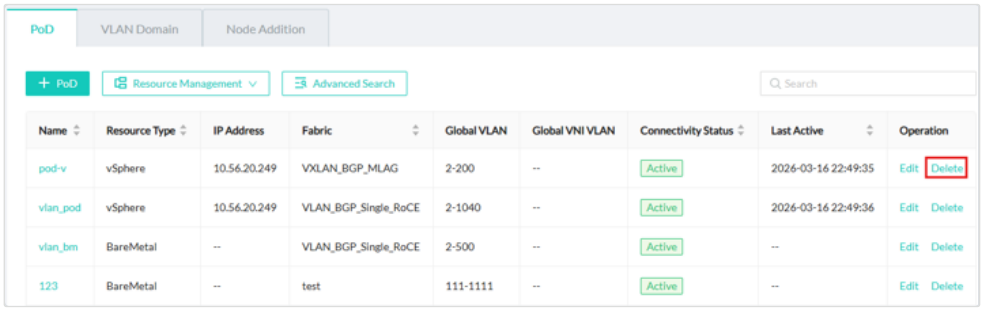
To edit a vSphere PoD, locate it in the **PoD** tab, and then click **Edit**.



Deleting a vSphere PoD

1. From logical networks, delete all virtual networks of the vSphere PoD. For more information, see Deleting a Virtual Network.
2. Delete all node uplink configurations for the vSphere PoD. For more information, see Deleting Node Uplink.
3. Click **Resource > Resource Interconnection** from the navigation bar. In the **PoD** tab, locate the vSphere PoD, and then click **Delete**.

> **NOTE**
>
> A PoD can be deleted only when the following prerequisites are met:
>
> - No virtual networks of the vSphere PoD are added to logical networks.
> - No vSphere node uplink configurations are added for this vSphere PoD.


PoD
VLAN Domain
Node Addition
+ PoD
Resource Management
Advanced Search
Search
Name
Resource Type
IP Address
Fabric
Global VLAN
Global VNI VLAN
Connectivity Status
Last Active
Operation
pod-v
vSphere
10.56.20.249
VXLAN_BGP_MLAG
2-200
--
Active
2026-03-16 22:49:35
Edit
Delete
vlan_pod
vSphere
10.56.20.249
VLAN_BGP_Single_RoCE
2-1040
--
Active
2026-03-16 22:49:36
Edit
Delete
vlan_bm
BareMetal
--
VLAN_BGP_Single_RoCE
2-500
--
Active
--
Edit
Delete
123
BareMetal
--
test
111-1111
--
Active
--
Edit
Delete

OpenStack PoD

You can add OpenStack PoD to AmpCon-DC. Then, in the AmpCon-DC UI, you can view VPC, network, and VM resources of each added OpenStack PoD.

> **NOTE**
>
> You are not advised to allocate VPCs of OpenStack PoD to tenants because OpenStack PoD can't be used for logical network deployment.

Prerequisites
Adding an OpenStack PoD
Viewing an OpenStack PoD
- VPC Tab
- Network Tab
- VM Tab

Optional Operations
- Editing an OpenStack PoD
- Deleting an OpenStack PoD

Prerequisites

- Ensure that the currently logged-in user is granted built-in or custom roles with the Read and Write permissions to the **PoD** tab. For more information, see Managing Roles.
- If you need to add a OpenStack PoD, ensure that the fabric to which the OpenStack PoD belongs has been created. For more information, see Adding a Fabric.

Adding an OpenStack PoD

To add an OpenStack PoD, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Resource Interconnection** from the navigation bar.
2. In the **PoD** tab, click **+ PoD**.
3. In the pop-up window, input the following information:

> **NOTE**
>
> **Global VLAN** and **Global VNI VLAN** are used for overlay service provisioning in later AmpCon-DC versions.

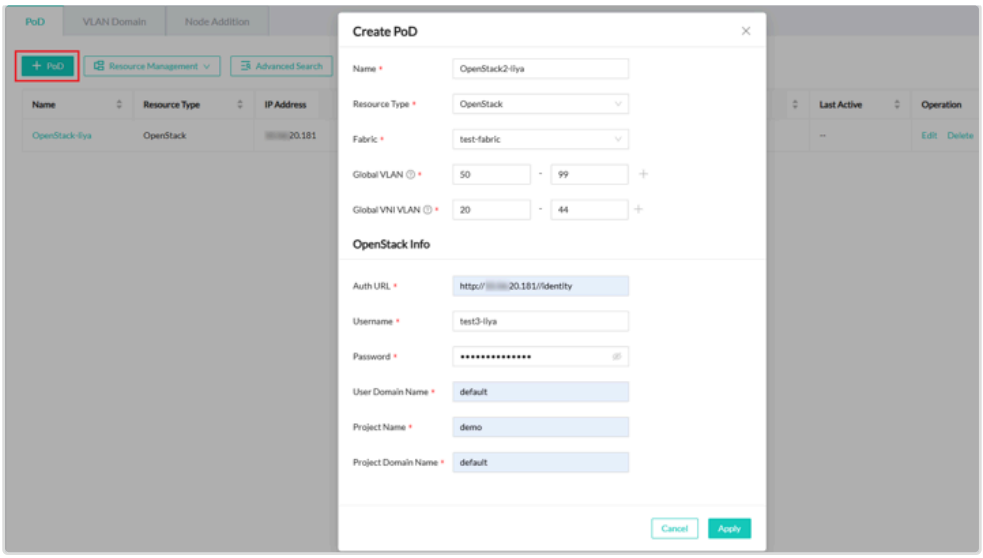


Table 1. OpenStack PoD Parameters

Parameter	Description
Name	The name of the OpenStack PoD.
Resource Type	Select **OpenStack**.
Fabric	The fabric to which the PoD belongs.
Global VLAN	The VLAN range that can be assigned to the PoD. The supported global VLAN range is 2 to 3965. Click **+** to add multiple global VLAN ranges.
Global VNI VLAN	Optional. The VLAN used within the VXLAN network of the cloud platform. The supported global VNI VLAN range is 2 to 3965. Click **+** to add multiple global VNI VLAN ranges.
Auth URL	The Keystone authentication endpoint.
Username	The OpenStack administrator username used to log in to the OpenStack environment.
Password	The password associated with the username.
User Domain Name	The domain where the user account exists.
Project Name	The name of the OpenStack project.

	NOTE Though one project is specified here, all projects managed by the administrator can be displayed in the AmpCon-DC UI after you add the PoD.
Project Domain Name	The domain where the project exists.

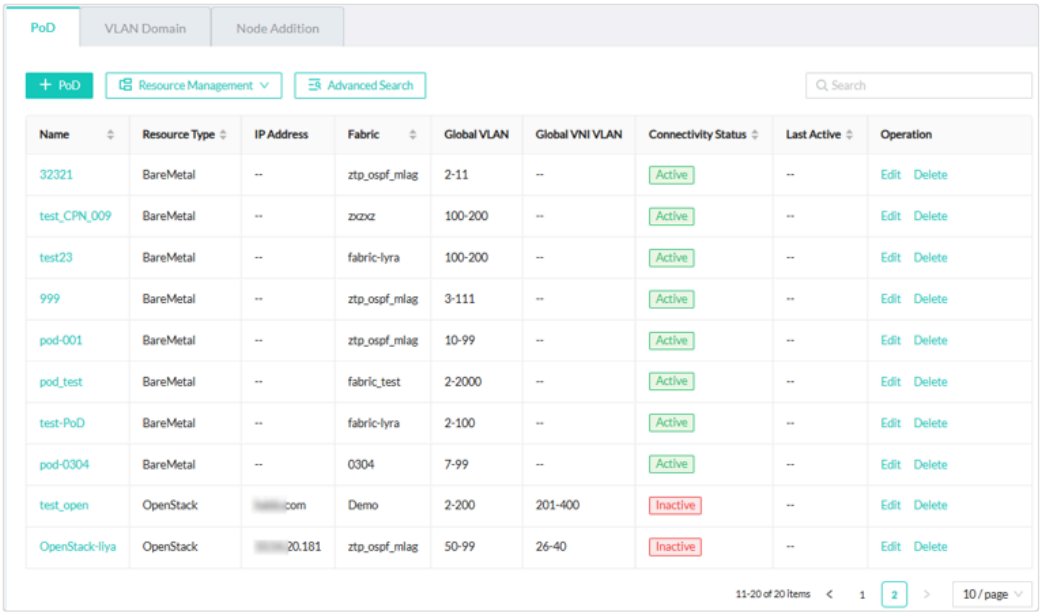
For more information about OpenStack parameters, see OpenStack Docs: Authentication.

4. Click **Apply**.

Viewing an OpenStack PoD

In the **PoD** tab, check whether you can see the OpenStack PoD that you created.

- **Connectivity Status** indicates the connection status of this PoD, which means whether AmpCon-DC is connected to the OpenStack platform.
  - **Active:** AmpCon-DC is connected to the OpenStack platform.
  - **Inactive:** AmpCon-DC isn't connected to the OpenStack platform.
- **Last Active** means the last time when AmpCon-DC is connected to the OpenStack platform.
- For other metrics, see **Table 1. OpenStack PoD Parameters** in the Adding an OpenStack PoD section.



To view detailed resources in a specific OpenStack PoD, click the name of the PoD. You can see the following tabs.

VPC Tab

In the **VPC** tab, you can view VPCs based on the roles assigned to the currently logged-in user:

- If the currently logged-in user is assigned the SuperAdmin, Admin, or Operator role or assigned custom roles with the Read permission to the **PoD** tab, you can see all VPCs.
- If the currently logged-in user is assigned only the Tenant Administrator role or assigned only the Tenant Administrator and ReadOnly roles, you can see only the VPCs allocated to the tenants managed by the currently logged-in user.

> **NOTE**
>
> In this case, you might not see any VPCs because allocating VPCs of OpenStack PoD to tenants is not recommended.

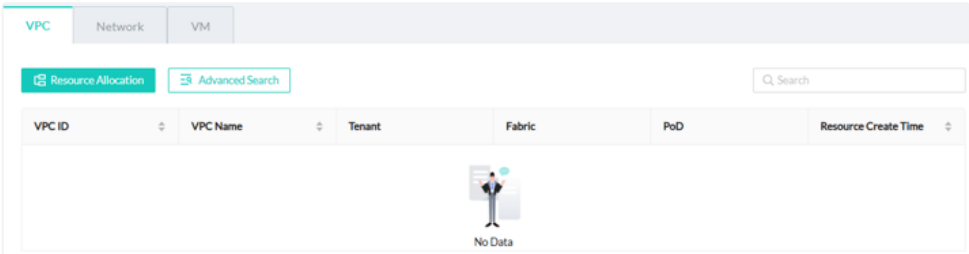


Table 2. VPC Metrics

Metric	Description
VPC ID	The ID assigned automatically by AmpCon-DC.
VPC Name	The name of the VPC.
Tenant	The tenant who owns the VPC. **NOTEs** • The value is **admin** if the VPC is created in AmpCon-DC 2.4. • The value is ***** if the VPC is allocated to a tenant not managed by the currently logged-in user.

	• The value is -- if the VPC is not allocated to any tenant.
Fabric	The fabric to which the VPC belongs.
PoD	The PoD to which the VPC belongs.
Resource Create Time	The time when AmpCon-DC retrieves the VPC from OpenStack for the first time.

Network Tab

In the **Network** tab, you can see all virtual networks in the OpenStack PoD. In OpenStack, the virtual network is called network.

Table 3. Network Metrics

Metric	Description
Name	The network name.
VPC	The project name.
Fabric	The fabric to which the network belongs.
PoD	The PoD to which the network belongs.
VM Count	The count of VMs in the network.
Host Count	The count of physical machines in the network.
VLAN ID	The VLAN ID of the network.
Resource Create Time	The time when AmpCon-DC retrieves the network from OpenStack for the first time.

VM Tab

In the **VM** tab, you can see all the VMs in the OpenStack PoD.

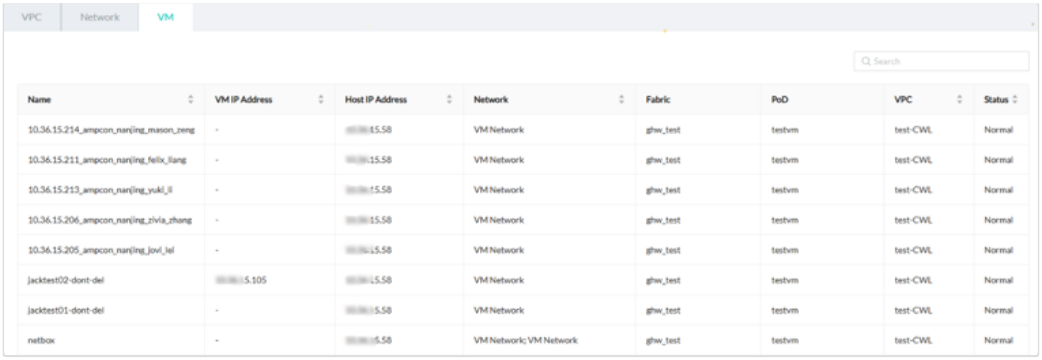


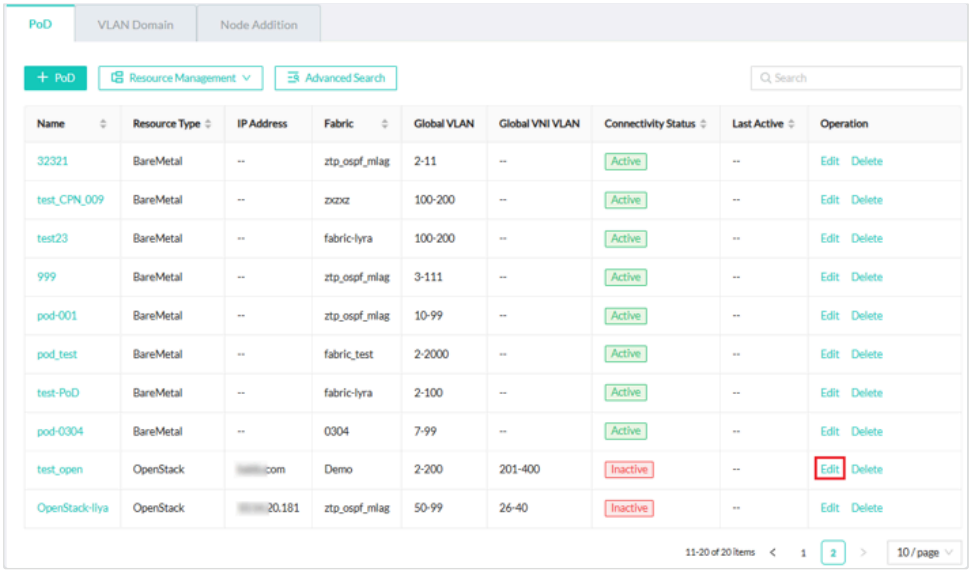
Table 4. VM Metrics

Metric	Description
Name	The VM name.
VM IP Address	The IP address of the VM.
Host IP Address	The IP address of the physical machine.
Network	The IP address of the physical machine where the VM exists.
Fabric	The fabric to which VM belongs.
PoD	The PoD to which VM belongs.
VPC	The project to which the VM belongs.
Status	The status of the VM.

Optional Operations

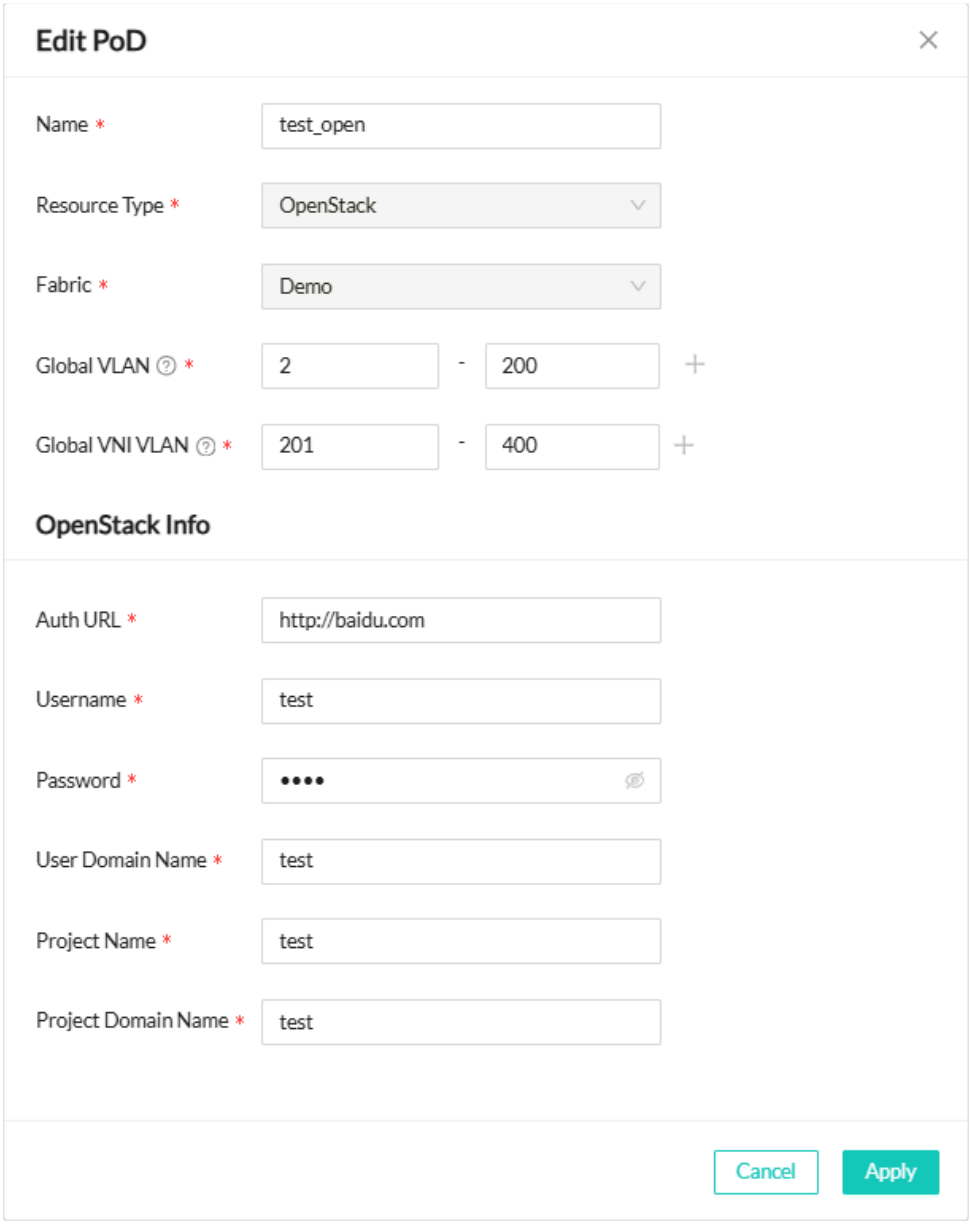
Editing an OpenStack PoD

1. In the **PoD** tab, locate the OpenStack PoD, and then click **Edit**.



2. In the pop-up window, modify the PoD as needed.

   All fields cannot be empty. You are not allowed to modify the **Resource Type** and **Fabric**.

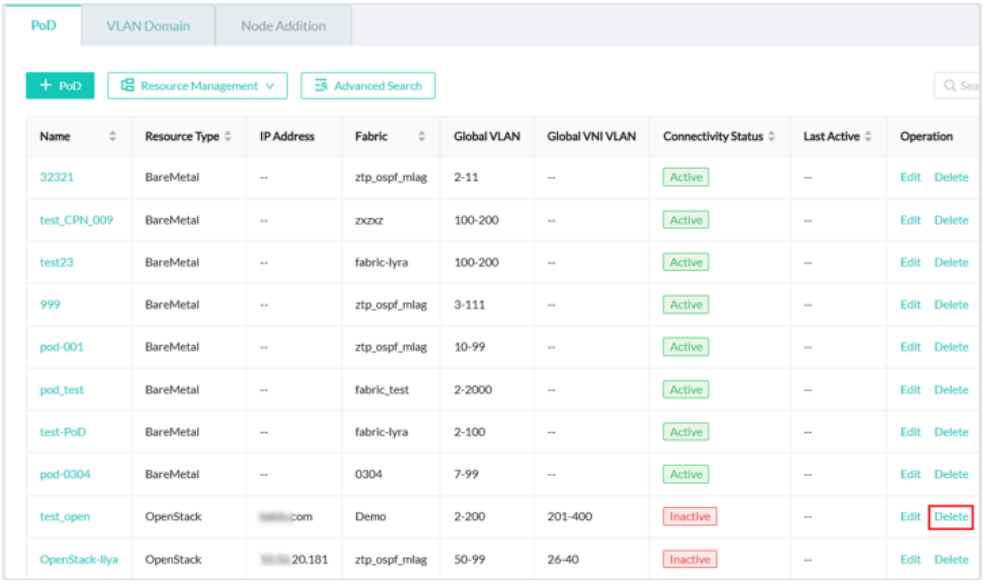


Deleting an OpenStack PoD

1. From logical networks, delete all virtual networks of the OpenStack PoD. For more information, see Deleting a Virtual Network.
2. Delete all node uplink configurations for the OpenStack PoD. For more information, see Deleting Node Uplink.
3. Click **Resource > Resource Interconnection** from the navigation bar. In the **PoD** tab, locate the OpenStack PoD, and then click **Delete**.

> **NOTE**
>
> A PoD can be deleted only when the following prerequisites are met:
>
> - No virtual networks of the OpenStack PoD are added to logical networks.

- No OpenStack node uplink configurations are added for this OpenStack PoD.



Bare Metal PoD

To use bare metal node devices for logical network deployment, add bare metal PoD to AmpCon-DC, and allocate VPCs of these added bare metal PoD to tenants.

In the AmpCon-DC UI, you can view VPC and network related resources of these added bare metal PoD.

- Prerequisites
- Adding a Bare Metal PoD
  - VLAN Assignment Rules
- Allocating VPCs
- Optional Operations
  - Viewing a Bare Metal PoD
    - VPC Tab
    - Network Tab
  - Searching for VPCs
  - Editing a Bare Metal PoD
  - Deleting a Bare Metal PoD

Prerequisites

- Ensure that the currently logged-in user is granted built-in or custom roles with the Read and Write permissions to the **PoD** tab. For more information, see Managing Roles.
- If you need to add a bare metal PoD, ensure that the fabric to which the bare metal PoD belongs has been created. For more information, see Adding a Fabric.
- If you need to allocate VPCs of a bare metal PoD to a tenant for logical network deployment, ensure that the fabric to which the bare metal PoD belongs meets all of the following conditions:
  - The fabric has been deployed through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.
  - The fabric is associated with the tenant. For more information, see Viewing a Tenant.

Adding a Bare Metal PoD

To add a bare metal PoD, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Resource Interconnection** from the navigation bar.
2. In the **PoD** tab, click **+ PoD**.
3. In the pop-up window, input the following information:

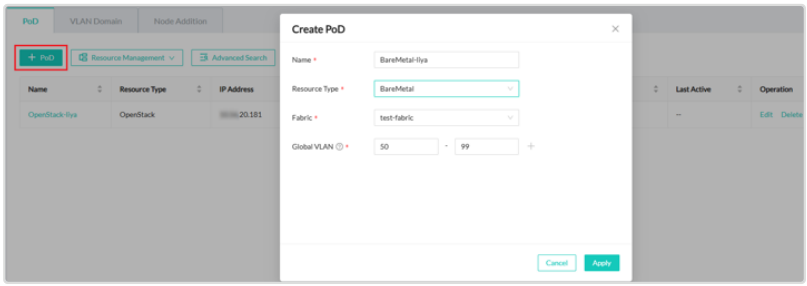


Table 1. Bare Metal PoD Parameters

Parameter	Description
Name	The name of the bare metal PoD.

Resource Type	Select **BareMetal**.
Fabric	The fabric to which the PoD belongs.
Global VLAN	The VLAN range that can be assigned to the PoD. The supported global VLAN range is 2 to 3965. Click **+** to add multiple global VLAN ranges. **NOTE** Ensure that the **Global VLAN** range has available intersections with the **Bridge Domain Range** in the related VLAN Domain. Or else, when you add a logical switch, VLANs will fail to be assigned. For detailed VLAN assignment rules, see the VLAN Assignment Rules section.

4. Click **Apply**.

VLAN Assignment Rules

When you add a logical switch, VLAN is assigned based on the following rules:

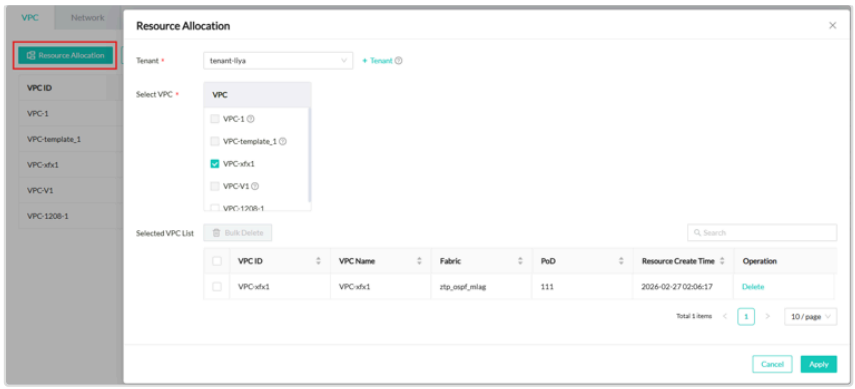
- AmpCon-DC assigns a VLAN from the intersections between the **Global VLAN** range and the **Bridge Domain Range** in the related VLAN Domains.
- VLANs cannot be assigned in the following cases:
  - The **Global VLAN** range and the **Bridge Domain Range** have no intersections.
  - All intersection VLANs between the **Global VLAN** ranges and the **Bridge Domain Range** are used up.

Allocating VPCs

After you add a bare metal PoD, to use some VPCs of this PoD for logical network deployment, you must allocate these VPCs to tenants. For detailed steps, see Allocating VPCs to Tenants.

NOTE

If a VPC is not allocated to a tenant, the virtual network related to the VPC can't be added to the logical networks belonging to the tenant. For more information, see Adding Virtual Networks.

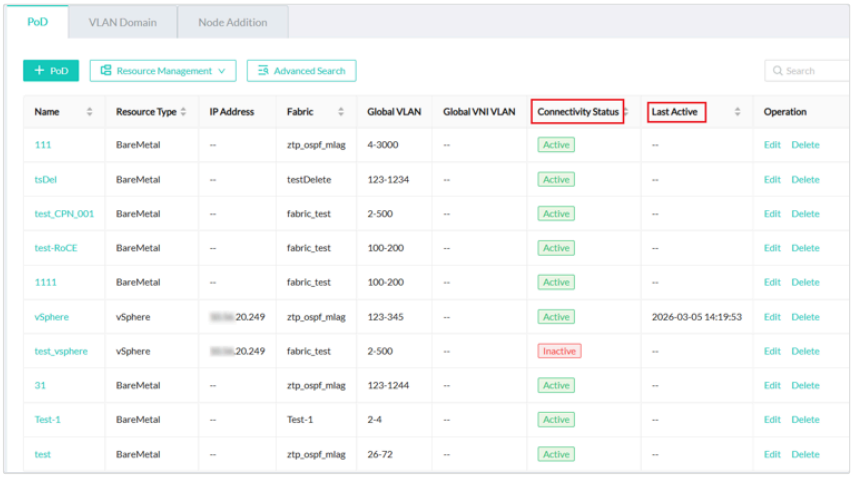


Optional Operations

Viewing a Bare Metal PoD

In the **PoD** tab, check whether you can see the bare metal PoD that you created.

> **NOTEs**
>
> - For bare metal PoD, **Connectivity Status** is always **Active**, and **Last Active** is always empty.
> - For other metrics, see **Table 1. Bare Metal PoD Parameters** in the Adding a Bare Metal PoD section.



Click the name of the PoD. You can see the **VPC** and **Network** tabs.

VPC Tab

In the **VPC** tab, you can view VPCs based on the roles assigned to the currently logged-in user:

- If the currently logged-in user is assigned only the Tenant Administrator role or assigned only the Tenant Administrator and ReadOnly roles, you can see only the VPCs allocated to the tenants managed by the currently logged-in user.
- If the currently logged-in user is assigned the SuperAdmin, Admin, or Operator role or assigned custom roles with the Read permission to the **PoD** tab, you can see all VPCs.

> **NOTEs**
>
> - For bare metal PoD, a VPC is generated automatically when you add a virtual network named VL2. For more information, see Creating Bare

Metal VL2s.

- If you haven't added VL2, the **VPC** tab is blank.

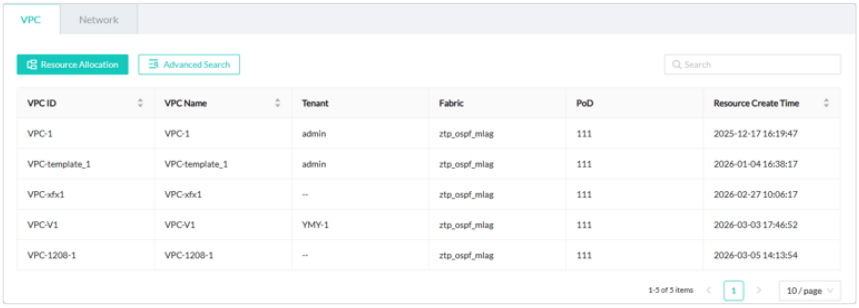


Table 2. VPC Metrics

Metric	Description
VPC ID	The ID assigned automatically by AmpCon-DC.
VPC Name	The name of the VPC.
User	The tenant who owns the VPC. **NOTEs** • The value is **admin** if the VPC is created in AmpCon-DC 2.4. • The value is ***** if the VPC is allocated to a tenant not managed by the currently logged-in user. • The value is **--** if the VPC is not allocated to any tenant.
Fabric	The fabric to which the VPC belongs.
PoD	The PoD to which the VPC belongs.
Resource Create Time	The time when you create the VL2 bound to the bare metal PoD.

Network Tab

In the **Network** tab, you can see all virtual networks in the bare metal PoD. In bare metal, the virtual network is called Virtual Layer 2 Switching (VL2).

NOTE

For bare metal PoD, only after you add a VL2, you can see network information in this tab. For more information, see Adding a VL2.

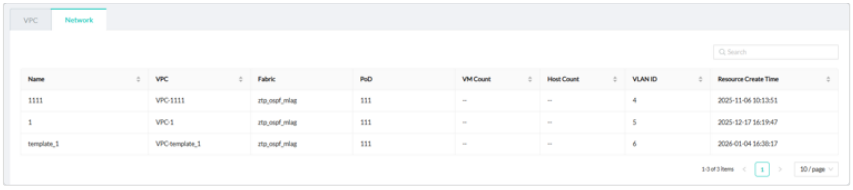
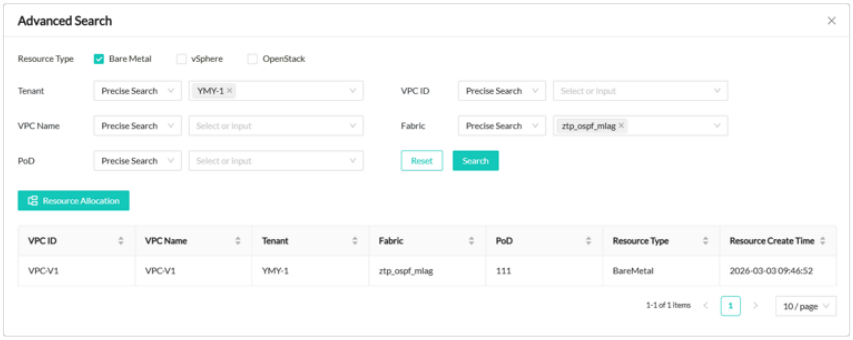


Table 3. Network Metrics

Metric	Description
Name	The VL2 name.
VPC	The VPC to which the VL2 belongs.
Fabric	The fabric to which the VL2 belongs.
PoD	The PoD to which the VL2 belongs.
VM Count	The count of VMs. The column is 0 for bare metal PoD because bare metal doesn't have a VM.
Host Count	The count of bare metal node devices that you added in Configuring Node Uplink for Bare Metal Nodes. If you don't add bare metal nodes to this PoD, the value is 0.
VLAN ID	The VLAN assigned to the VL2.
Resource Create Time	The time when you create the VL2.

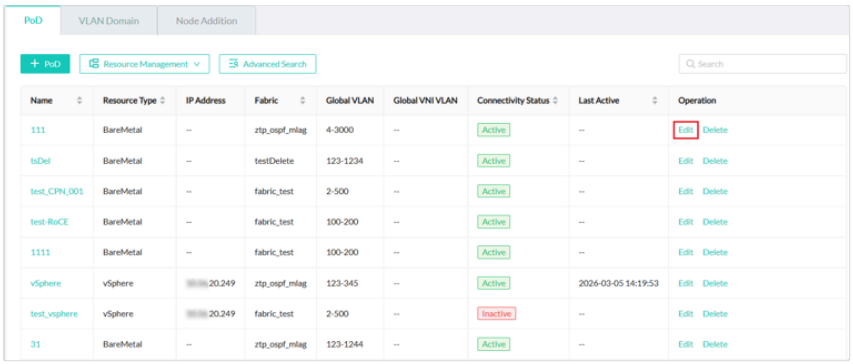
Searching for VPCs

To search for VPCs and view their details, click **Advanced Search**. For more information, see Searching for VPCs.



Editing a Bare Metal PoD

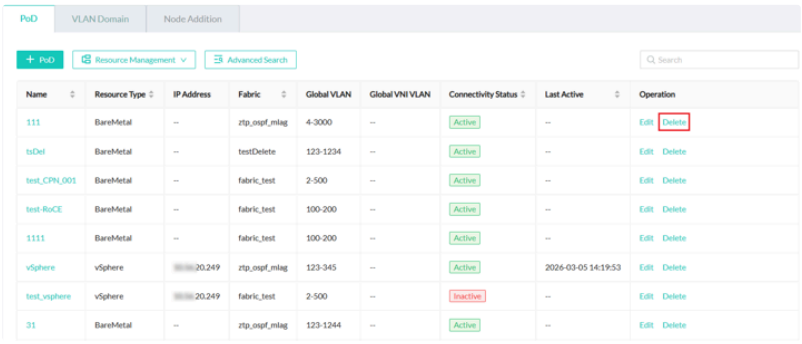
To edit a bare metal PoD, locate it in the **PoD** tab, and then click **Edit**.



Deleting a Bare Metal PoD

1. From logical networks, delete all virtual networks of the bare metal PoD. For more information, see Deleting a Virtual Network.
2. Delete all bare metal node groups for the bare metal PoD. For more information, see Deleting a Node Group.
3. Delete all bare metal VL2 for the bare metal PoD. For more information, see Deleting a VL2.
4. Click **Resource > Resource Interconnection** from the navigation bar. In the **PoD** tab, locate the bare metal PoD, and then click **Delete**.

> **NOTE**
>
> A PoD can be deleted only when the following prerequisites are met:
>
> - No virtual networks of the bare metal PoD are added to logical networks.
> - No bare metal node uplink configurations are added for this bare metal PoD.



Managing VPCs

In AmpCon-DC, Virtual Private Clouds (VPCs) are network resources within Point of Delivery (PoD). AmpCon-DC supports three types of PoD: Bare Metal PoD, vSphere PoD, and OpenStack PoD.

Depending on the PoD type, VPCs are obtained in different ways:

- In vSphere PoD and OpenStack PoD, VPCs are automatically retrieved by AmpCon-DC when the vSphere PoD and OpenStack PoD are created.
- In Bare Metal PoD, VPCs are automatically generated when Virtual Layer 2 Switching (VL2s) are created. For more information, see Creating Bare Metal VL2s.

To deploy logical networks for overlay service provisioning, you need to allocate VPCs to tenants and then add virtual networks of these VPCs to logical networks, achieving flexible and scalable network resource allocation. You can also unbind VPCs from tenants or search for VPCs.

Guidelines
Allocating VPCs to Tenants
From the PoD Tab
From the VPC Tab of a Specific PoD
From the Network Access Page
Unbinding VPCs from Tenants
From the PoD Tab
From the Network Access Page
Searching for VPCs

Guidelines

- The built-in user **admin** can allocate all VPCs to any tenants. Other users can allocate VPCs to only their managed tenants, and the VPCs are limited to those within the fabrics associated with these tenants.
- Virtual networks of VPCs in bare metal PoD and vSphere PoD can be added to logical networks. Virtual networks of VPCs in OpenStack PoD cannot be added to logical networks.
- AmpCon-DC users who have only the Tenant Administrator role cannot allocate or unbind VPCs to or from tenants. To allocate or unbind VPCs, the logged-in AmpCon-DC user must also be assigned built-in or custom roles with the Write permission to the “PoD” page. For role permissions, see Viewing Role Details.

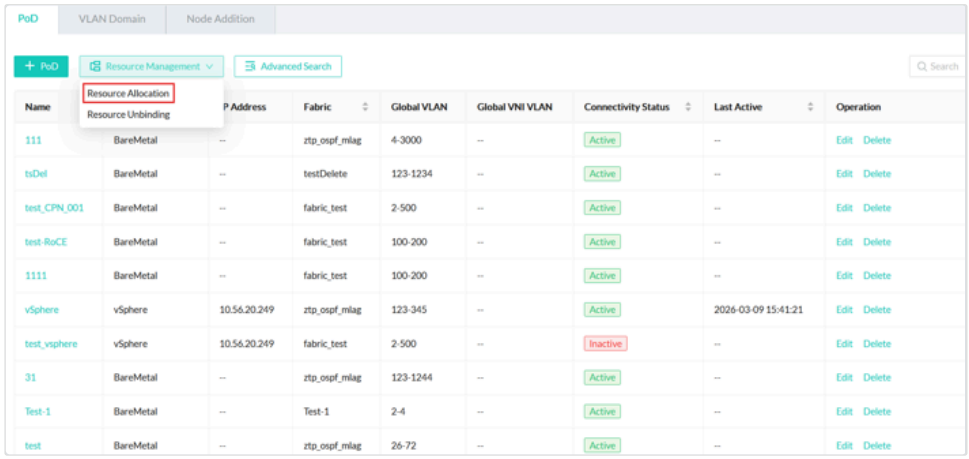
Allocating VPCs to Tenants

You can allocate VPCs to tenants in different ways.

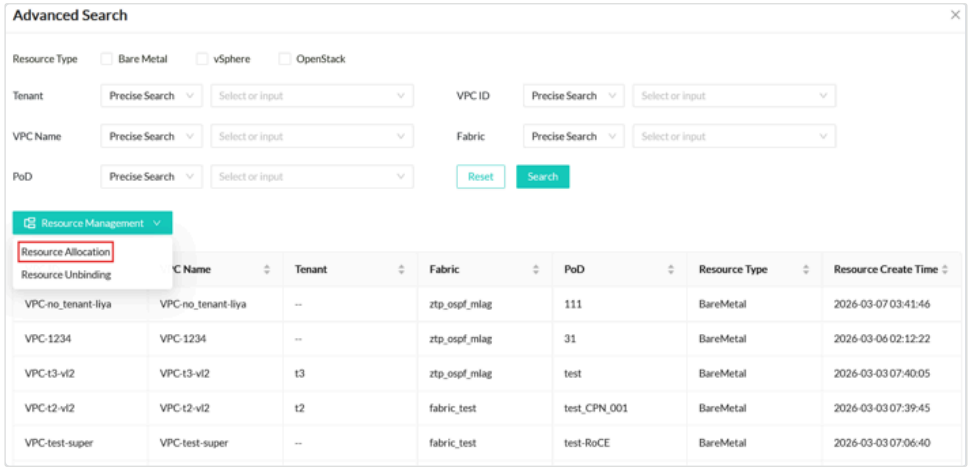
From the PoD Tab

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Locate the **Resource Allocation** button in the **PoD** tab. Use one of the following methods:

- In the **PoD** tab, hover over **Resource Management**, and then select **Resource Allocation**.



- In the **PoD** tab, click **Advanced Search**. In the pop-up window, hover over **Resource Management**, and then select **Resource Allocation**.



3. In the pop-up window, select tenants and VPCs as follows:

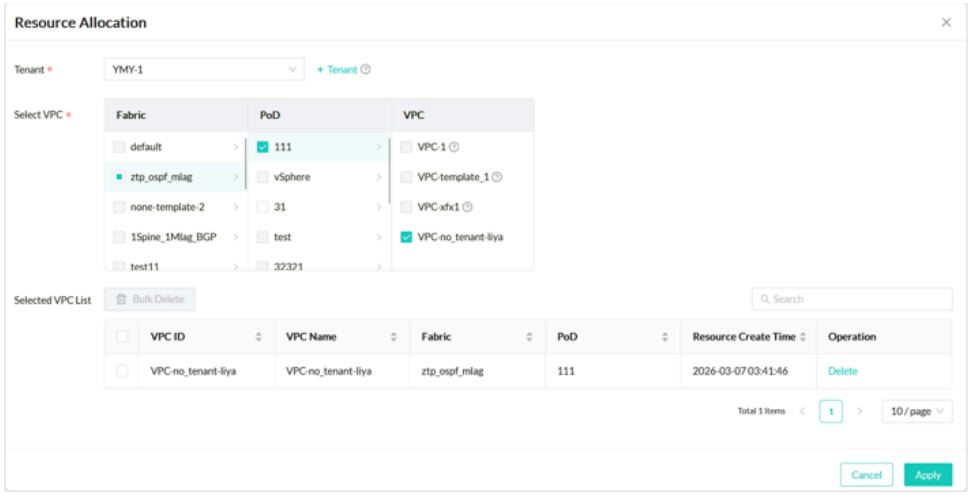


Table 1. VPC Allocation Parameters

Parameter	Description
Tenant	Select the tenant to which the VPCs will be allocated. **NOTEs** • If no tenant meets your needs, click **+ Tenant** to create a new tenant. For more information, see Adding a Tenant. • In the drop-down list, you can see only the tenants managed by the currently logged-in user. • Each VPC can be allocated to at most a tenant.

Select VPC	Click the fabric and PoD to which the VPCs belong, and then select the VPCs to be allocated to the tenant. **NOTEs** • If you select a fabric or a PoD, all available VPCs in the fabric or PoD will be selected. • If a fabric or a PoD contains no VPCs or contains only the VPCs that have been allocated to other tenants, the fabric or PoD check box is grayed out and cannot be selected. • If a VPC has been allocated to other tenants, the VPC check box is grayed out and cannot be selected.

4. In the **Selected VPC List** section, check whether all VPCs that you selected are displayed.

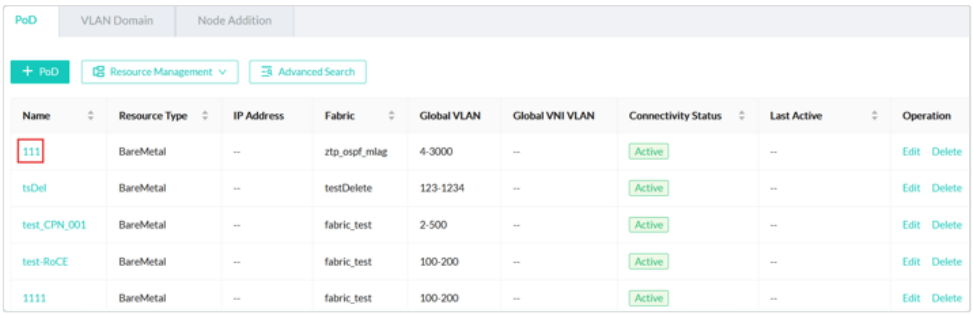
   To remove a selected VPC from the **Selected VPC List**, click **Delete** in the **Operation** column.

   To remove multiple selected VPCs from the **Selected VPC List**, select the VPCs, and then click **Bulk Delete**.

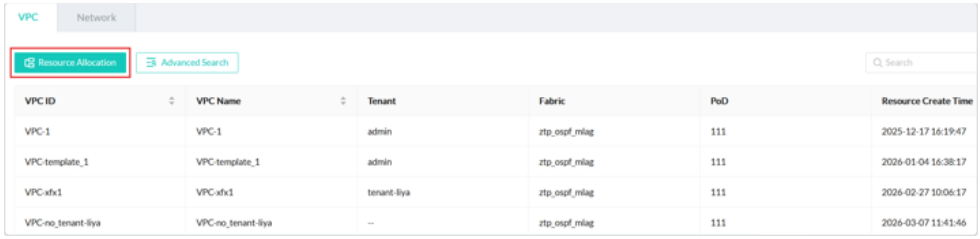
5. Click **Apply**.

From the VPC Tab of a Specific PoD

1. Click **Resource > Resource Interconnection** from the navigation bar, and then click the name of a PoD in the **PoD** tab.



2. In the **VPC** tab of the PoD, click **Resource Allocation**.



3. In the pop-up window, select tenants and VPCs as follows:

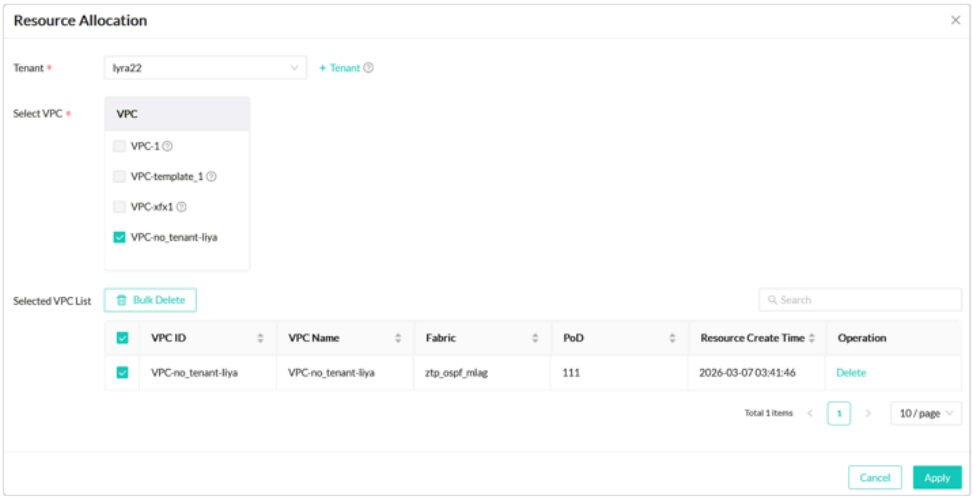


Table 2. Selection Parameters

Parameter	Description
Tenant	Select the tenant to which the VPCs will be allocated. **NOTEs** • If no tenant meets your needs, click **+ Tenant** to create a new tenant. For more information, see Adding a Tenant. • In the drop-down list, you can see only the tenants managed by the currently logged-in user and associated with the fabric to which the PoD belongs. • Each VPC can be allocated to at most a tenant.

Select VPC	Select the VPCs to be allocated to the tenant. **NOTE** If a VPC has been allocated to other tenants, the VPC check box is grayed out and cannot be selected.

4. In the **Selected VPC List** section, check whether all VPCs that you selected are displayed.

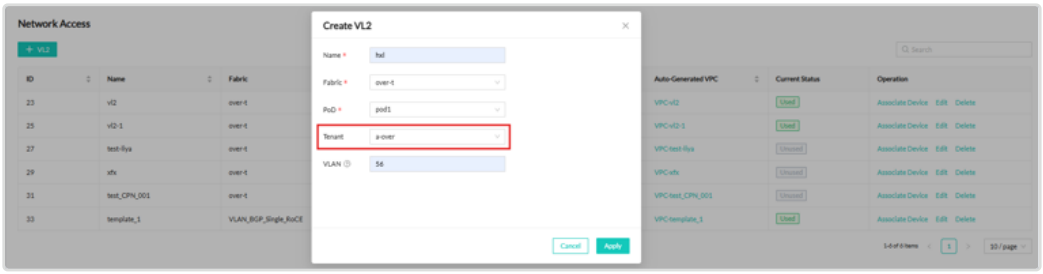
   To remove a selected VPC from the **Selected VPC List**, click **Delete** in the **Operation** column.

   To remove multiple selected VPCs from the **Selected VPC List**, select the VPCs, and then click **Bulk Delete**.

5. Click **Apply**.

From the Network Access Page

When creating or editing a VL2, you can designate the tenant to which the VPC of the VL2 is allocated. For more information, see Adding a VL2 and Editing a VL2.



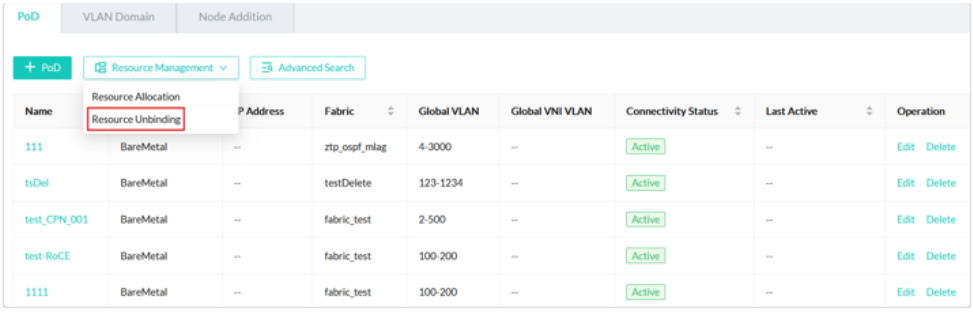
Unbinding VPCs from Tenants

You can unbind VPCs from tenants in different ways.

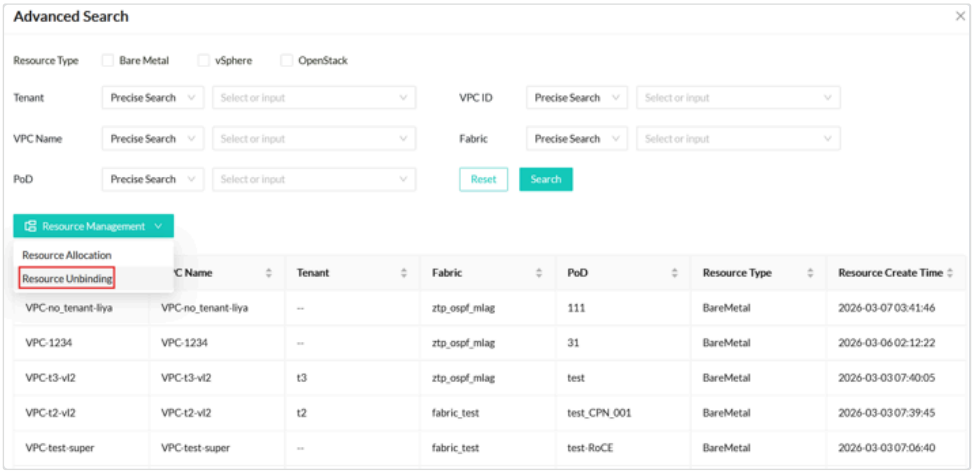
From the PoD Tab

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. In the **PoD** tab, locate the **Resource Unbinding** button through one of the following methods:

- Hover over **Resource Management**, and then select **Resource Unbinding**.

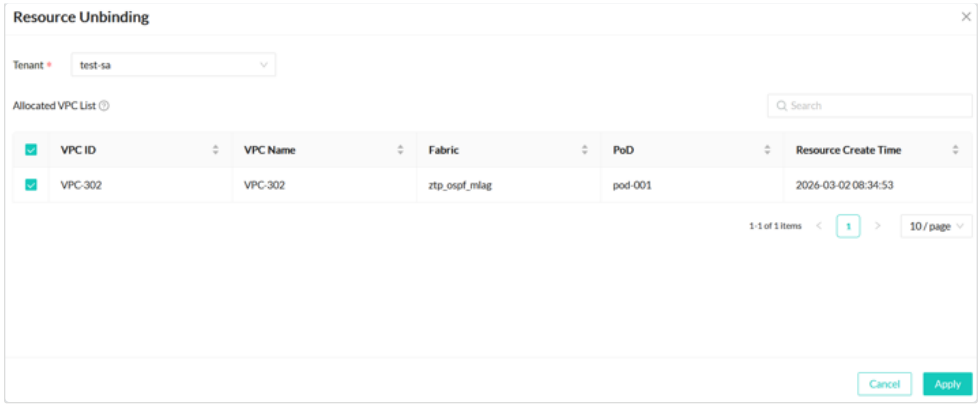


- Click **Advanced Search**. In the pop-up window, hover over **Resource Management**, and then select **Resource Unbinding**.



3. In the pop-up window, select the tenant in the **Tenant** drop-down list, select the VPCs to be unbound in the **Allocated VPC List** section, and then click **Apply**.

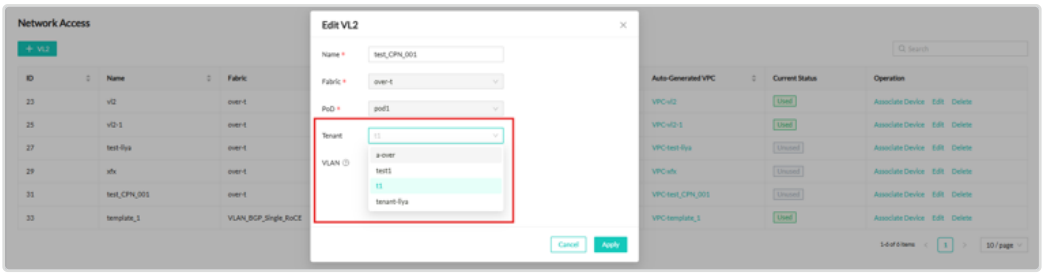
> **NOTEs**
>
> - In the **Tenant** drop-down list, you can see only the tenants that meet all the following conditions:
>   - The tenants are managed by the currently logged-in user.
>   - The tenants have VPCs allocated.
> - The VPCs that are currently used by logical networks cannot be unbound.
> - Unbinding VPCs from a tenant will lead to the following results:
>   - The tenant cannot use the VPCs for logical network deployments.
>   - The VPCs can be allocated to other tenants.



From the Network Access Page

If the VPC of a VL2 has already been allocated to a tenant, you can select another tenant for the VPC by editing the VL2. Then, the VPC is unbound from the previous tenant and allocated to the newly selected tenant.

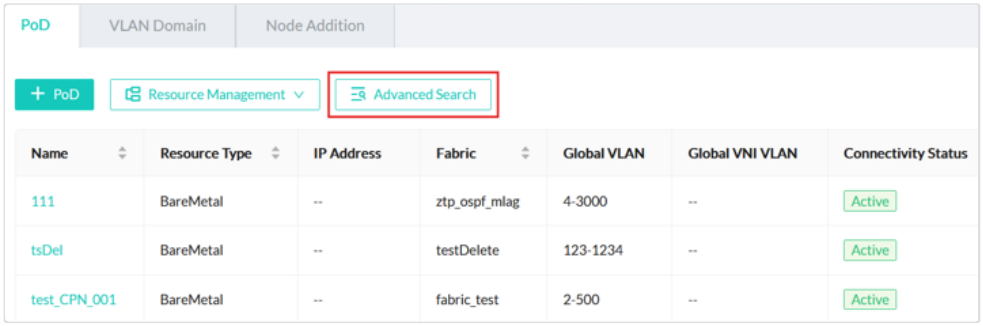
For more information, see Editing a VL2.



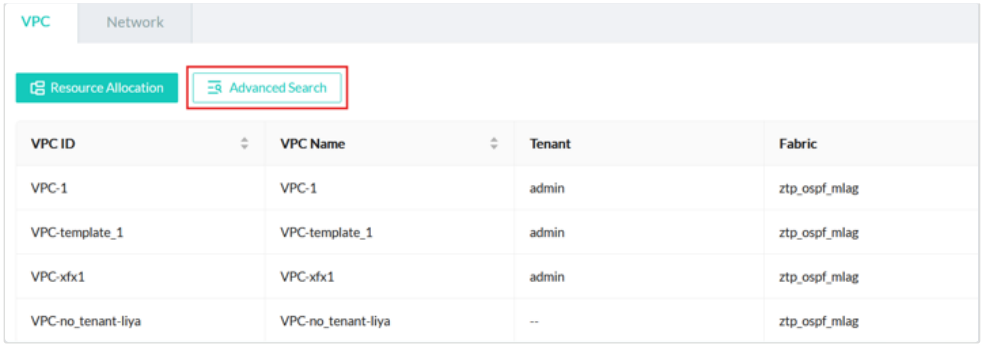
Searching for VPCs

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. In the **PoD** tab, click the **Advanced Search** button through one of the following methods:

- In the **PoD** tab, click **Advanced Search**.



- In the **PoD** tab, click the name of a PoD. In the **VPC** tab of the PoD, click **Advanced Search**.



3. In the pop-up window, search for VPCs through one or multiple filter parameters:

> **Tip**
>
> You can select the **Precise Search** or **Fuzzy Search** mode for each filter parameter.

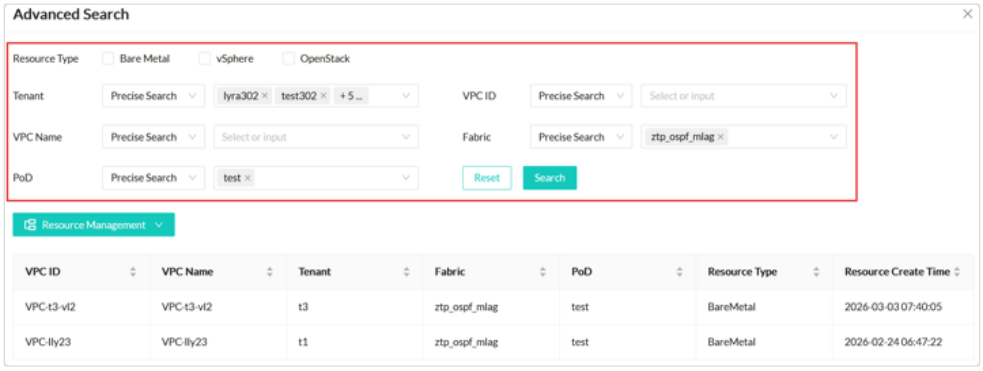
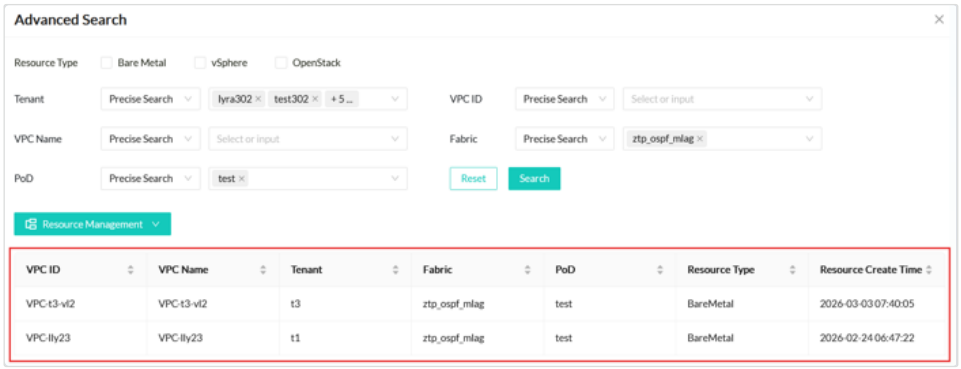


Table 3. Filter Parameters

Parameter	Description
Resource Type	The resource type of the PoD to which the VPCs belong.
Tenant	The tenant who manages the VPCs. • If you select **--** here, the following VPCs are displayed in the search results: ◦ VPCs that are retrieved from a vSphere PoD or an OpenStack PoD and used in a logical network in AmpCon-DC 2.4. For these VPCs, the **Tenant** column displays **admin**. ◦ VPCs that are automatically generated after a VL2 is created and used in a logical network in

	AmpCon-DC 2.4. For these VPCs, the **Tenant** column displays **admin**. ◦ VPCs that are retrieved or automatically generated in AmpCon-DC 2.5 but are not allocated to any tenant. For these VPCs, the **Tenant** column displays **--**. • If you select a specific tenant name, the VPCs allocated to this tenant are displayed in the search results. For these VPCs, the **Tenant** column displays the tenant name.
VPC ID	The VPC ID automatically created by AmpCon-DC.
VPC Name	The names of the VPCs.
Fabric	The fabric that the VPCs belong to.
PoD	The PoD that the VPCs belong to.

4. Check the VPCs that match the selected filters.



Tips

- To clear all filter parameters, click **Reset**. Then, you can see all VPCs.

VLAN Domains

VLAN Domains restrict the allocation of VLAN IDs to a specific range for virtual networks connected to logical switches. Currently, VLAN Domains are used only for overlay service provisioning.

A VLAN Domain group means a set of all VLAN Domains in a fabric. After you add a VLAN Domain group for a fabric, VLAN Domain items are created automatically for each leaf switch in the fabric.

By default, the **VRF VLAN Range** and **Bridge Domain Range** fields are not designated automatically. You must designate these fields manually.

Before you deploy a logical network, ensure that you have added and configured a VLAN Domain group for the related physical network (fabric).

> **NOTEs**
>
> - Each fabric contains one VLAN Domain group. Each VLAN Domain group contains one or multiple VLAN Domains.
> - A VLAN Domain name indicates a VLAN Domain. VLAN Domain names need to be unique.
>   - Each non-MLAG leaf switch is assigned with one distinct VLAN Domain.
>   - Peer leaf switches in an MLAG share the same VLAN Domain.

Prerequisites
Adding a VLAN Domain Group
Optional Operations
  Viewing All VLAN Domains in a Fabric
  Editing VLAN Domains in a Fabric
  Deleting a VLAN Domain Group

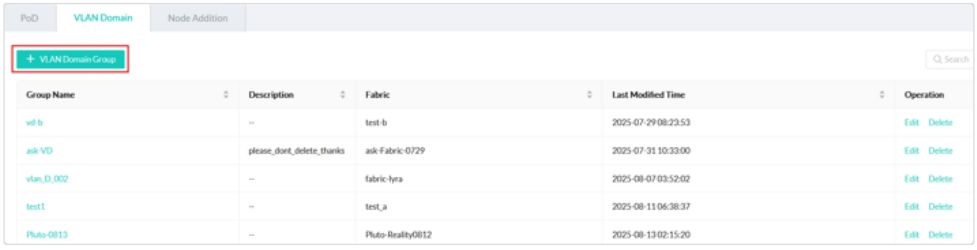
Prerequisites

Before you add a VLAN Domain group for a fabric, ensure that the fabric has been deployed successfully through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.

Adding a VLAN Domain Group

To add a VLAN Domain group, follow these steps:

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **VLAN Domain** tab, and then click **+ VLAN Domain Group**.



3. At the top of the “Create VLAN Domain Group” page, input the following information:

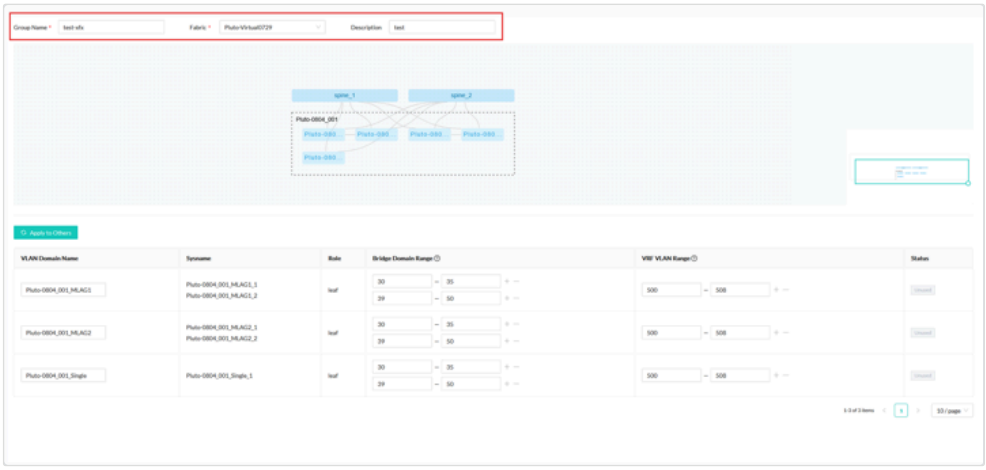


Table 1. VLAN Domain Parameters

Parameter	Description
Group Name	The name of the VLAN Domain group. The name needs to be unique.
Fabric	The fabric associated with the VLAN Domain group. **NOTE** Only the fabrics that have been deployed through simplified ZTP or physical network design can be selected.
Description	Optional. The description of the VLAN Domain group.

4. In the VLAN Domain table, input the following information:

NOTEs

- To batch-sync the **VRF VLAN Range** and **Bridge Domain Range** values in the first row of the table to other rows, click the square before these rows, and then click **Apply to Others**.
- For each VLAN Domain, you can add multiple ranges in the **VRF VLAN Range** and **Bridge Domain Range** column. To add a range, click **+**. To remove a range, click **-**.



Table 2. Input Parameters

Parameter	Description
VLAN Domain Name	Optional. The name of the VLAN Domain. A default VLAN Domain name is created automatically. You can modify it if needed.
VRF VLAN Range	The VLAN ranges reserved by VRF VLAN for L3VNI on the switch. The available VRF VLAN values range from 2 to 3965. Example Bridge Domain Range: 500-505,600,66
Bridge Domain Range	The VLAN ranges reserved by Bridge Domain for L2VNI on the switch. The available Bridge Domain values range from 2 to 3965. Example Bridge Domain Range: 30-300,400,509,1600-2000 **NOTEs** • Within one VLAN Domain, the **Bridge Domain Range** cannot be duplicated with the **VRF VLAN Range**. • For different VLAN Domains, the **Bridge Domain Range** and the **VRF VLAN Range**

	can be duplicated. • Ensure that the **Bridge Domain Range** has available intersections with the **Global VLAN** range (for bare metal and vSphere PoD) or with **Global VLAN** and **Global VNI VLAN** ranges (for OpenStack PoD). Or else, when you add a logical switch, VLAN will fail to be assigned. • For bare metal and vSphere node devices connected to leaf switches in VLAN Domains, VLANs are assigned based on VLAN Assignment Rules of Bare Metal PoD and VLAN Assignment Rules of vSphere PoD.

The following information is generated by AmpCon-DC automatically and can't be changed:

Table 3. Auto-generated Parameters

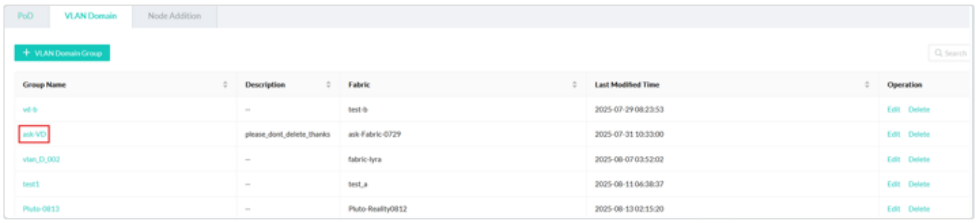
Parameter	Description
Sysname	The hostname of the leaf switch.
Role	Only the role **leaf** is displayed here, which means leaf switches.
Status	Whether the VLAN Domain is assigned to node devices in virtual networks. • **Used:** The VLAN Domain is assigned to node devices in virtual networks. • **Unused:** The VLAN Domain is not assigned to node devices in virtual networks.

5. Click **Save**.

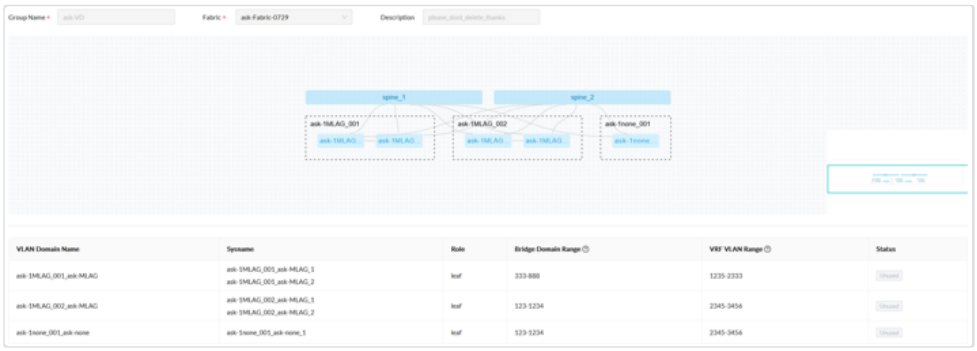
Optional Operations

Viewing All VLAN Domains in a Fabric

1. In the **VLAN Domain** tab, click a VLAN Domain group name in the **VLAN Domain Group Name** column.



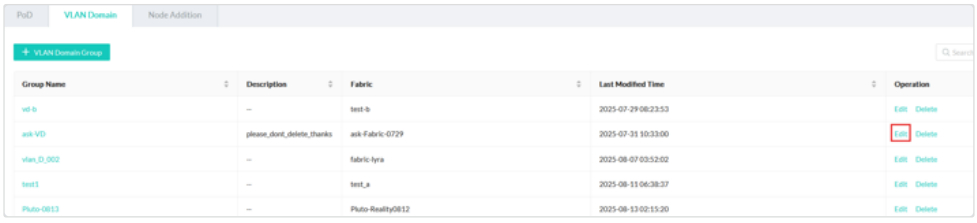
2. On the “View VLAN Domain Group” page, check all VLAN Domains in the VLAN Domain group.



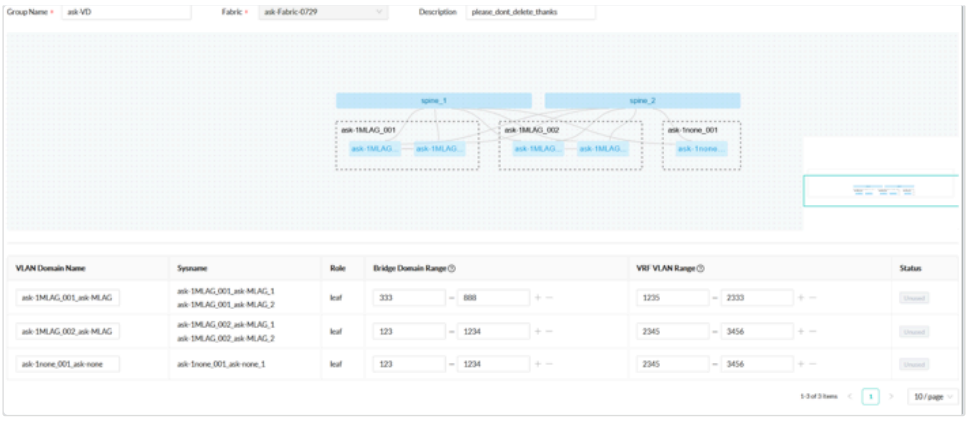
Editing VLAN Domains in a Fabric

1. In the **VLAN Domain** tab, locate the VLAN Domain group, and then click **Edit**.

> **NOTE**
>
> A VLAN Domain group can be edited only when no logical switches are added to the fabric to which the VLAN Domain group belongs. For more information, see Viewing Logical Switches.



2. On the “Edit VLAN Domain Group” page, edit the VLAN Domains in the fabric.



3. Click **Save** to complete the fabric edition.

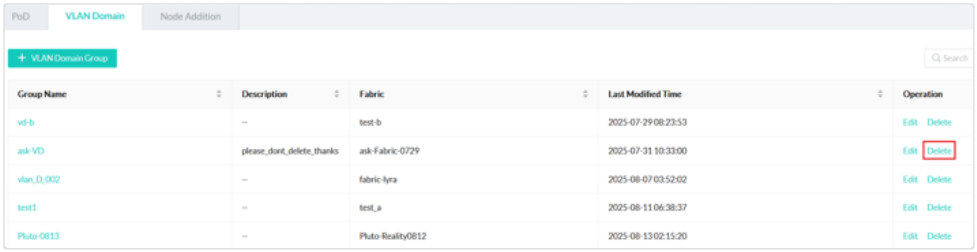
Deleting a VLAN Domain Group

1. Delete all logical switches bound to the fabric to which the VLAN Domain group belongs. For more information, see Deleting a Logical Switch.

> **NOTE**
>
> A VLAN Domain group can be deleted only when no logical switches are added to the fabric to which the VLAN Domain group belongs. For more information, see Viewing Logical Switches.

2. In the **VLAN Domain** tab, locate the VLAN Domain group, and then click **Delete**.

   All VLAN Domains in the VLAN Domain group will be deleted.



Node Uplink

AmpCon-DC streamlines node uplink configurations for node devices in bare metal or cloud platform (vSphere) PoD.

You can configure and manage uplink of node devices, eliminating manual node-by-node or switch-by-switch configurations.

The node uplink feature is used for overlay service provisioning. For more information, see Provisioning Overlay Services. After you connect virtual networks of PoD with logical switches, node devices in the virtual networks can be connected to uplink switches based on node uplink configurations.

See the following child topics:

- Key Concepts for Node Uplink
- Configuring Node Uplink for Bare Metal Nodes
- Configuring Node Uplink for Cloud Platform Nodes
- Node Uplink Scenarios in AI

> **NOTEs**
>
> - Currently, OpenStack PoD can't be used for overlay service provisioning. Even though you can configure node uplink for OpenStack node devices, you can't use the node devices for overlay service provisioning.
> - For bare metal PoD, you need to add bare metal devices to AmpCon-DC first and then configure node uplink for these node devices.
> - For vSphere PoD, AmpCon-DC automatically retrieves node devices from vSphere, and thus you don't need to add node devices to vSphere PoD manually. But you need to configure node uplink for the node devices.

Key Concepts for Node Uplink

Understand the following key concepts used for the node uplink feature:

- Bare Metal Nodes
- Bare Metal Node Group
- Fabric
- NIC Port
- NIC Port Group
- Node Template
- vSphere Nodes
- Point of Delivery (PoD)
- Switch Port Group
- VLAN Domain
- VLAN Domain Group

Bare Metal Nodes

The physical servers that operate without pre-installed operating systems or virtualization layers.

Bare Metal Node Group

A logical collection of bare metal node devices that are grouped together based on shared uplink configurations.

Fabric

The logical representation of an actual physical network. You can deploy a physical network by designing a fabric in the AmpCon-DC UI. A fabric is based on a template. A template contains one or multiple units.

In a fabric, you can specify which managed switches serve as leaf and spine switches, and you can add device nodes connected to leaf switches.

NIC Port

The port contained in a NIC port group to connect to a switch.

NIC Port Group

The logical aggregation of multiple network interface cards (NICs) of a node device. A NIC port group contains one or multiple NIC ports.

Node Template

The template containing NIC port groups. Each NIC port group contains NIC port counts and port speed configurations.

When you add node uplink configurations, you can select NIC ports in a NIC port group to connect with uplink switches.

vSphere Nodes

The node devices in vSphere. These nodes are automatically retrieved from the vSphere cloud platform after you add vSphere PoD.

Point of Delivery (PoD)

A collection of resources in a data center. PoD includes three types: bare metal PoD, vSphere PoD, and OpenStack PoD. In AmpCon-DC, each PoD contains only one type of resources.

Switch Port Group

The logical grouping of multiple switch ports for centralized management, policy enforcement, or traffic optimization.

A switch port group contains one or multiple switch ports.

VLAN Domain

Restricts the allocation of VLAN IDs to a specific range for each node device connected to leaf switches.

Each fabric contains one or multiple VLAN Domains. Each non-MLAG leaf switch is assigned with one distinct VLAN Domain. Peer leaf switches in an MLAG share the same VLAN Domain.

VLAN Domain Group

A set of all VLAN Domains in a fabric.

Configuring Node Uplink for Bare Metal Nodes

A bare metal node group refers to a logical collection of bare metal node devices that are grouped together based on shared uplink configurations.

To use bare metal node devices for overlay service provisioning, you need to add bare metal node groups first.

In the bare metal node groups, add bare metal node devices to bare metal PoD, and then configure node uplink for these node devices.

Prerequisites
Guidelines
Adding a Bare Metal Node Group
1. Adding Node Group information
2. Adding Switch Port Group information
3. Applying and Verifying Node Uplink Configurations
What to Do Next

Prerequisites

1. Ensure that the fabric to have node uplink configured are deployed through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.
2. Ensure that you have completed VLAN Domain configuration for the fabric. For more information, see VLAN Domains.
3. Ensure that you have created the bare metal PoD to which the node devices belong. For more information, see Bare Metal PoD.

Guidelines

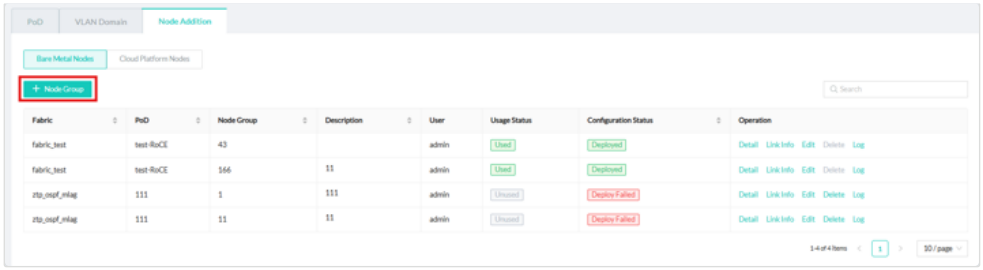
Pay attention to the following points:

- The speed of the selected NIC ports and selected switch ports must be the same.
- The node uplink configurations are consistent with actual physical connections.

Or else, the node uplink configurations will fail to be used for overlay service provisioning.

Adding a Bare Metal Node Group

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab.
3. In the **Bare Metal Nodes** sub-tab, click **+ Node Group**.

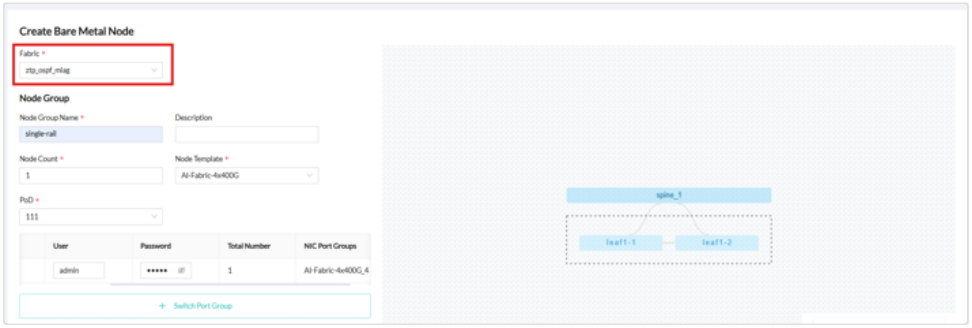


You are now redirected to the node group configuration page, which includes the following processes:

1. Adding Node Group information

1. In the **Fabric** drop-down list, select the fabric to which the node group belongs.

   The fabric must have been created before you add the node group.



2. In the **Node Group** section, input the following information:

Table 1. Node Group Parameters

Parameter	Description
Node Group Name	The name of the node group. The name needs to be unique.
Description	Optional. The description of the node group.
Node Count	The count of node devices in this node group. Valid values range from 1 to 32. **NOTE** You can't edit the **Node Count** until you have entered the **Port Group Name**.
Node Template	The node template that contains port configurations used by bare metal nodes to

	connect with uplink switches. The selected node template configurations will be applied to all bare metal node devices in the node group. For more information, see the Node Template Tips section.
PoD	The bare metal PoD to which the node group belongs.

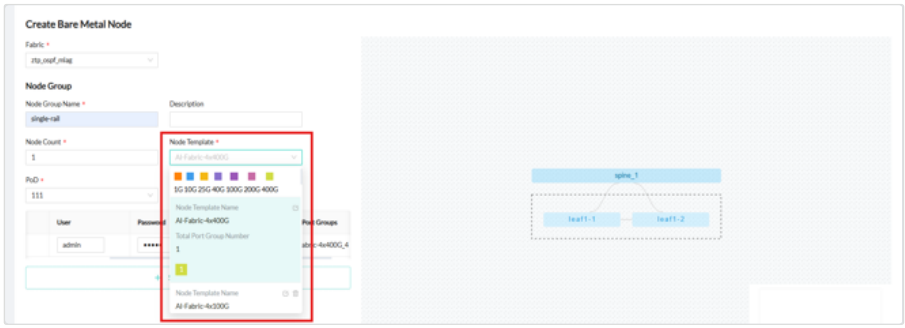
> **Tip**
>
> The following information is generated by AmpCon-DC automatically:
>
> - The **Node Name** value means the name of the node.
> - The **Total Number** value means the total number of NIC ports and is generated by AmpCon-DC based on the selected node template.
> - The **NIC Port Groups** value means the total number of NIC port groups and is generated by AmpCon-DC based on the selected node template.

3. In the following table, enter the IP address, username (optional), and password (optional) of each bare metal node device to be added to the node group.

> **NOTEs**
>
> - The count of node devices listed here is decided by the **Node Count** value entered in **Step 2**.
> - **Node Name**, **Total Number**, and **NIC Port Groups** are filled automatically based on the selected node template.
>   - **Node Name:** The name of the node device.
>   - **Total Number:** The total number of NIC ports for a node device.
>   - **NIC Port Groups:** The NIC port groups included in the selected node template.

Node Template Tips

- In each node template, you can see the following information:
  - **Node Template Name**: The name of the node template.
  - **Total Port Group Number**: The total number of NIC port groups in the node template.



- Different speeds of port groups are displayed in different colors.
- The following built-in 6 node templates are provided:
  - 8 ports at the speed of 400G, 200G, or 100G
  - 4 ports at the speed of 400G, 200G, or 100G
- In addition to the built-in node templates, you can add one or multiple new node templates. Drill down to the bottom of the **Node Template** list, and then click **+ Custom Node Template**. For more information, see Adding a Node Template.
- To edit a node template, click the edit icon. For more information, see Editing a Node Template.
- To delete a node template, click the delete icon. For more information, see Deleting a Node Template.

2. Adding Switch Port Group information

1. On the node group configuration page, click **+ Switch Port Group**.
2. In the **Switch Port Group** section, input the following information:

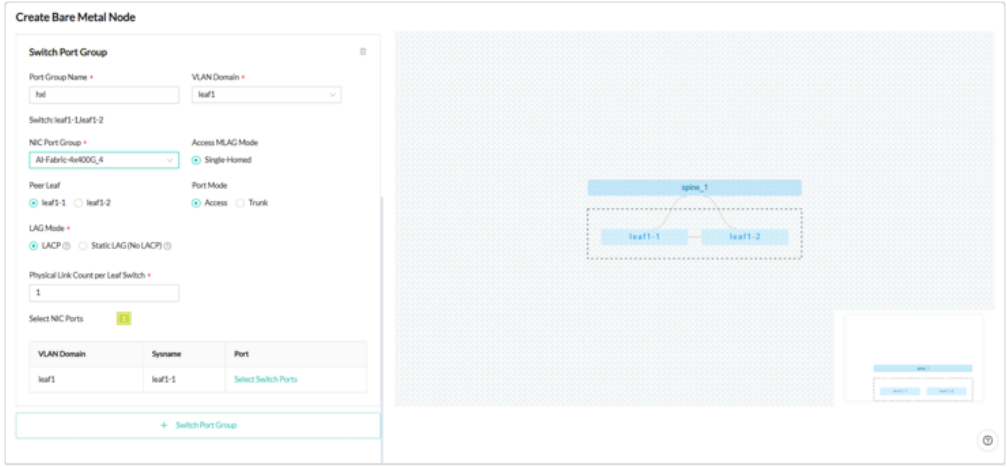


Table 2. Switch Port Group Parameters

Parameter	Description
Port Group Name	The name of the switch port group. The name needs to be unique.
VLAN Domain	The VLAN Domain to which the uplink non-MLAG switch (or MLAG switches) belongs. AmpCon-DC automatically retrieves the VLAN Domains of the selected fabric and displays them here. • Each non-MLAG leaf switch is assigned with one distinct VLAN Domain. If you select a VLAN Domain containing a non-MLAG leaf switch, the leaf switch is assigned as the leaf switch of the node devices automatically. • Peer leaf switches in an MLAG share the same VLAN Domain. If you select a VLAN Domain containing MLAG leaf switches, you can decide whether the node devices connect to one peer leaf switch or both peer leaf switches. **NOTE** You can't select **VLAN Domain** until you have entered the **Port Group Name**.
NIC Port Group	Select a NIC port group. The NIC port groups in the list are those groups added in the selected node template.
Access MLAG Mode	Select **Single-Homed** or **Dual-Homed**. • **Single-Homed:** The node devices connect to one peer leaf switch in the MLAG setup. • **Dual-Homed:** The node devices connect to both peer leaf switches in the MLAG setup. **NOTEs**

	• This field is available only when the VLAN domain that you select contains MLAG leaf switches. • If the selected NIC port group contains only one NIC port, you can select only **Single-Homed**.
Peer Leaf	Select the MLAG peer leaf switch to which the node devices are connected. **NOTEs** • This field is available only when the VLAN domain that you select contains MLAG leaf switches and you select **Single-Homed** in the **Access MLAG Mode** section. • If you select **Dual-Homed**, both peer MLAG leaf switches are used to connect with the node devices.
Port Mode	The port mode used by the node devices to connect to the uplink non-MLAG switch (or MLAG switches). Select **Access** or **Trunk**.
LAG Mode	Whether to use Link Aggregation Groups (LAGs) and which mode to use. An LAG means a logical link formed by bundling multiple physical links. Each LAG uniquely corresponds to a logical interface, also known as a link aggregation interface or Eth-Trunk interface. Select one of the following options: • **LCAP:** Enables Link Aggregation Control Protocol (LACP). For more information about LCAP, see Adding LAG and LACP. • **Static LAG (No LACP):** Unconditionally operates in forwarding mode, instead of participating in LACP protocol negotiation. • **No LAG:** Uses no LAGs.

	NOTEs • If **LACP** is selected, ensure that the devices at both aggregation ends support the LACP protocol. • If the selected VLAN domain contains MLAG leaf switches, you can't see the **No LAG** option. • If the selected VLAN domain doesn't contain MLAG leaf switches and the **Physical Link Count per Leaf Switch** is **1**, you can't see the **LCAP** and **Static LAG (No LACP)** options. • If the selected VLAN domain doesn't contain MLAG leaf switches and the **Physical Link Count per Leaf Switch** is larger than **1**, you can't see the **No LAG** option.
Physical Link Count per Leaf Switch	The number of physical links with which each node devices connect to the leaf switch. **NOTEs** • You can't edit the value until you enter the **Port Group Name** and select the **VLAN Domain** and **NIC Port Group**. • The value can't exceed the port count specified in the selected NIC port group. If exceeded, the value will be automatically changed to the maximum port count. • If you select **Single-Homed** in the **Access MLAG Mode** section, the **Physical Link Count per Leaf Switch** can be set to only **1**. Even though you enter a larger value, it will be automatically changed to **1**.

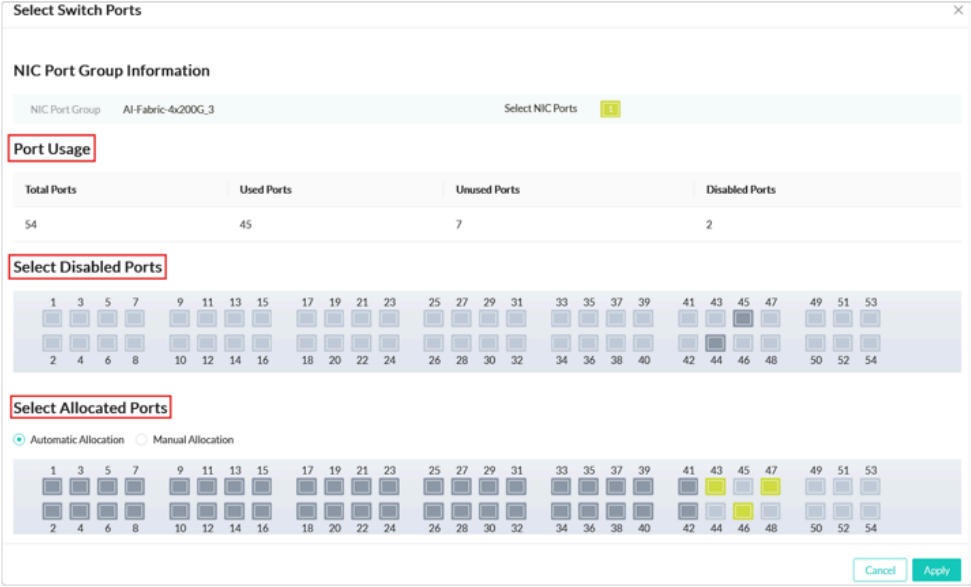
3. In the **Select NIC Port** section, select the NIC ports used to connect with leaf switches.

Each bare metal server uses the selected NIC port to connect with the switch port of the leaf switch.

4. In the switch table, click **Select Switch Port**.



5. In the pop-up window, select switch ports to be disabled (optional) or to be allocated for node uplink.



a. Optional: In the **Select Disabled Ports** section, click the ports to be disabled, or click disabled ports to enable these ports.

> **NOTE**
>
> Disabled switch ports can't be used for allocation.

b. In the **Select Allocated Ports** section, select one allocation method of switch ports:

Automatic Allocation: AmpCon-DC automatically allocates switch ports from the first available port (unused).

Manual Allocation: You need to manually select the first allocation switch port (unused). Then, the ports to be allocated will be selected automatically in ascending order. The switch ports used will not be selected.

c. Check the port information in the **Port Usage** section:

Table 3. Switch Port Parameters

Metric	Sub-Metric	Description
NIC Port Group Information	**NIC Port Group**	The NIC port group that you selected.
	Selected NIC Ports	The NIC ports used to connect to switch ports.
Port Usage	**Total Ports**	The count of total switch ports.
	Used Ports	The count of used switch ports.
	Unused Ports	The count of unused switch ports.
	Disabled Ports	The count of disabled switch ports.

d. Click **Apply** to complete the switch port selection.

6. Optional: To add multiple switch port groups, repeat **Step 1** to **Step 5**.
7. Optional: In the right panel of the node group configuration page, check the topology of the selected fabric.

- Click a switch in the topology, and then you can see the following information:

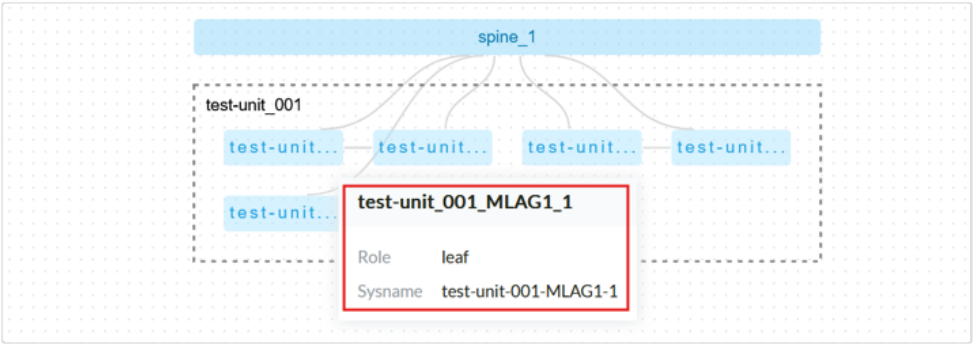


Table 4. Switch Port Parameters

Parameter	Description
Role	The role of the switch in the fabric. Values are **Leaf** or **Spine**, which means a leaf switch or spine switch.
Hostname	The hostname of the switch.

- Click a link in the topology, and then you can see the following information:

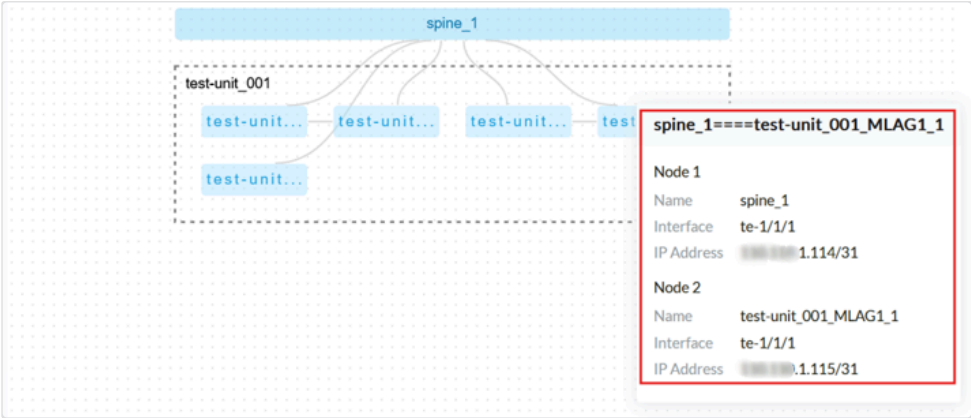


Table 5. Switch Port Parameters

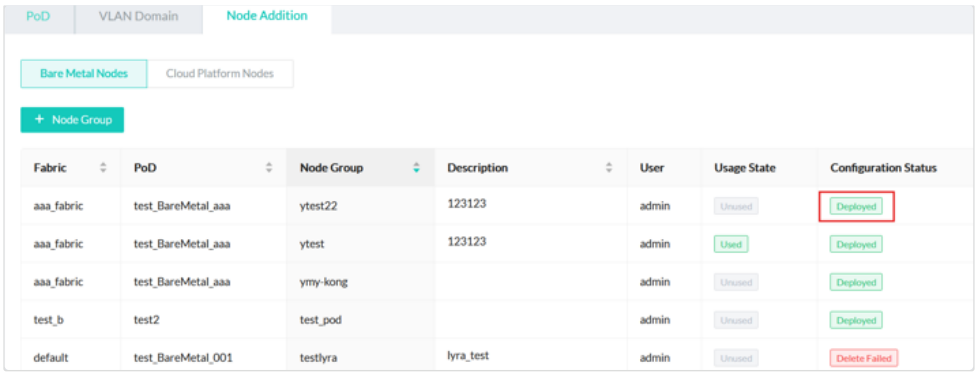
Metric	Sub-Metric	Description
Link Name		The name of the link, including the leaf switch and spine switch names.
Node 1	**Name**	The name of the leaf switch.
	Interface	The port used to connect with the leaf switch.
	IP Address	The IP address of the leaf switch.
Node 2	**Name**	The name of the spine switch.
	Interface	The port used to connect with the spine switch.
	IP Address	The IP address of the spine switch.

3. Applying and Verifying Node Uplink Configurations

1. Click **Apply** at the right of the page to complete the node uplink configuration.

   The configurations will be pushed to selected switches.

2. In the **Bare Metal Nodes** sub-tab, locate the node group name, and then check whether the **Configuration Status** column shows **Deployed**, which means the configurations are applied successfully.



What to Do Next

After you add bare metal node groups, you can manage these node groups as follows:

- View the node group list and uplink configuration details of each node group.
- Delete or edit node groups as needed.
- Check for logs and link information for each node device in the node group.

For more information, see Managing Bare Metal Node Groups.

Managing Node Templates

Node templates contain port configurations used by bare metal nodes to connect with uplink switches.

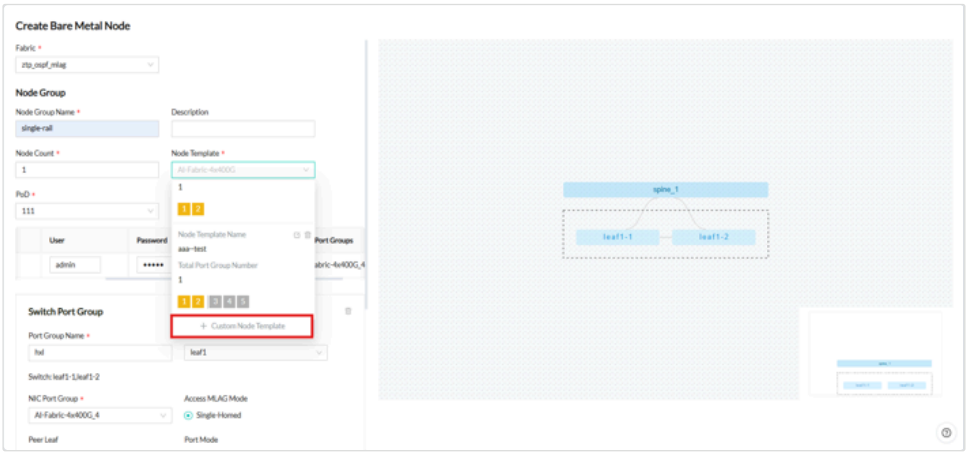
When you add a bare metal node group, you need to select a node template. 6 built-in node templates are provided, but you can add more node templates manually. In addition, you can edit or delete the added node templates as needed.

Adding a Node Template
Editing a Node Template
Deleting a Node Template

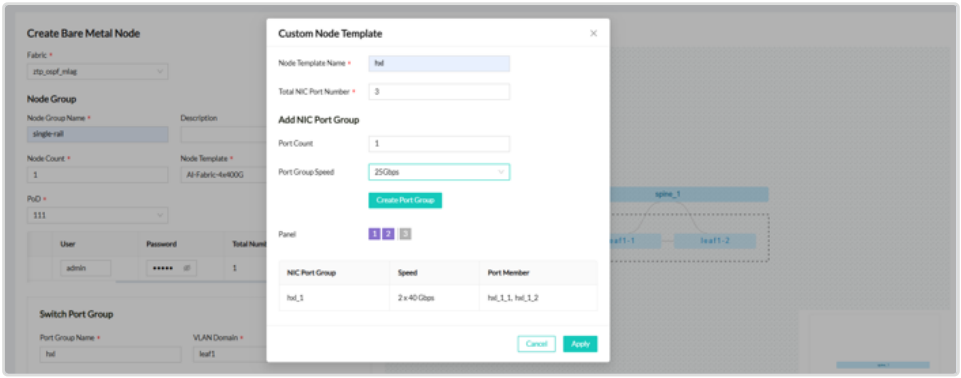
Adding a Node Template

To add a new node template, follow these steps:

1. On the bare metal node group configuration page, click the **Node Template** drop-down list, drill down to the bottom, and then click **+ Custom Node Template**.



2. On the “Custom Node Template” page, configure as follows:



   a. Add the node template name and the total number of NICs in the node template.

Table 1. Custom Node Template Parameters

Parameter	Description
Node Template Name	The name of the node template.
Total NIC Port Number	The total number of NICs. The value must be no more than 16.

b. In the **Add NIC Port Group** section, add a NIC port group by inputting the following information and clicking **Create Port Group**.

Table 2. NIC Port Group Parameters

Parameter	Description
Port Count	The count of NIC ports in this port group.
Port Group Speed	The transmission speed of each NIC port in this NIC port group.

c. Repeat **Step b** to add more NIC port groups as needed.

> **NOTE**
>
> The total number of NIC ports in all added NIC groups must be equal to the **Total NIC Port Number** value that you specified.

3. In the **Panel** section and the table below the **Panel** section, check the added NIC port groups.

> **NOTE**
>
> In the **Panel** section, different speeds of NIC port groups are displayed in different colors.

Table 3. NIC Port Group Metrics

Metric	Description
NIC Port Group	The name of the NIC port group.

Speed	The expected speed of the NIC ports in this NIC port group, 1G, 10G, 25G, 40G, 100G, 200G, or 400G. Different speeds of NIC ports are displayed in different colors.
Port Member	The NIC ports added to the NIC port group. The port member name is created automatically by AmpCon-DC.

4. Click **Apply**.

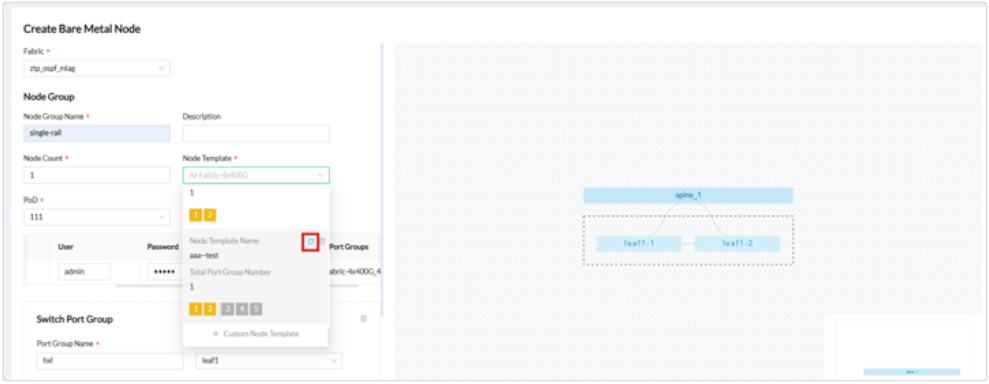
Then, you can see the newly added node template at the bottom of the **Node Template** drop-down list.

Editing a Node Template

If an added node template doesn't meet your needs, you can edit the node template. Follow these steps:

> **NOTE**
>
> For bare metal node groups that are being used for overlay service provisioning, you can't edit their node templates.

1. On the node group configuration page, click the **Node Template** drop-down list, locate the node template, and then click the edit icon.



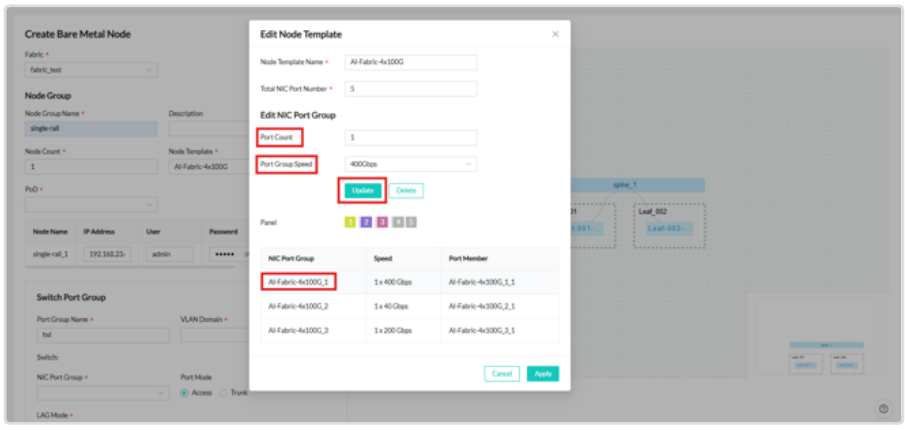
2. Modify the node template configurations as needed:

- To update a NIC port group configuration, follow these steps:

a. Click the NIC port group name in the **NIC Port Group** column.

b. Enter the port count and select a port group speed.

c. Click **Update**.



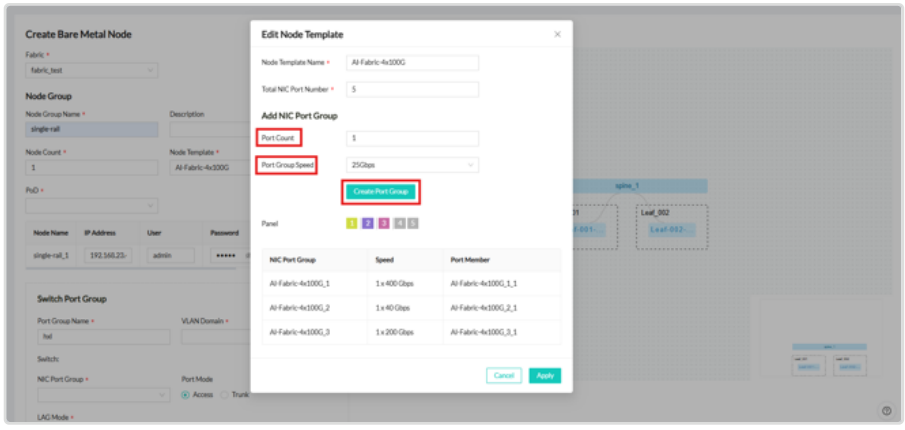
- To add a new NIC port group, follow these steps:

  a. In the **Total NIC Port Number** field, enter a bigger value in the **Total NIC Port Number** field.

  > **NOTE**
  >
  > If you modify the **Total NIC Port Number** field, the related switch port group configurations will be cleared. To add switch port group configurations, see Adding Switch Port Group Information.

  b. In the **Add NIC Port Group** section, input the **Port Count** and **Port Group Speed** information.

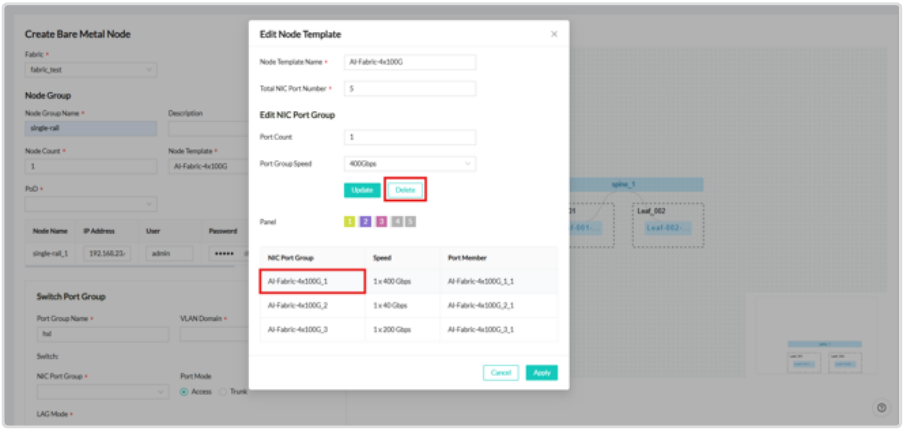
  c. Click **Create Port Group**.



- To delete a NIC port group, follow these steps:

  a. Click the NIC port group name in the **NIC Port Group** column.

  b. Click **Delete**.



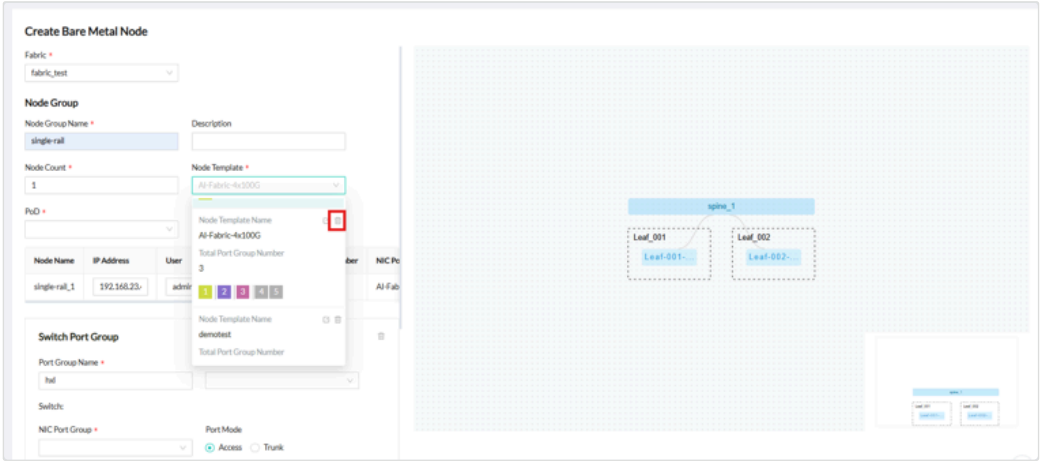
3. Click **Apply**.

Deleting a Node Template

If you don’t need a node template anymore, you can delete the node template.

On the node group configuration page, click the **Node Template** drop-down list, locate the node template, and then click the delete icon.

> **NOTE**
>
> For bare metal node groups that are being used for overlay service provisioning, you can’t delete their node templates.



Managing Bare Metal Node Groups

You can manage added bare metal node groups as follows:

- Viewing All Bare Metal Node Groups
- Viewing Details of a Bare Metal Node Group
- Editing Bare Metal Node Groups
- Checking Link Information of a Node Group
- Checking Logs of a Node Group
- Deleting a Node Group

Viewing All Bare Metal Node Groups

To view all added bare metal node groups, follow these steps:

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab.
3. In the **Bare Metal Nodes** sub-tab, check detailed information of all added bare metal node groups.

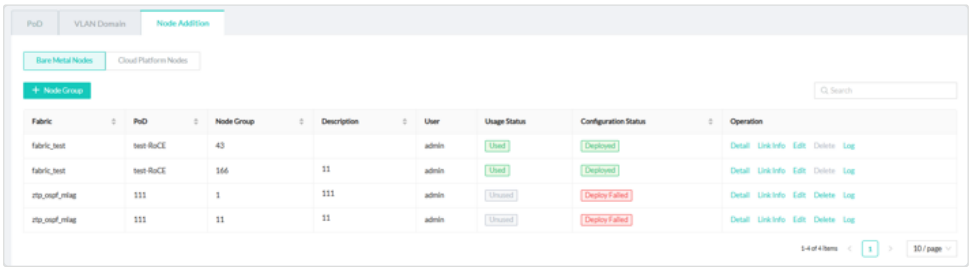


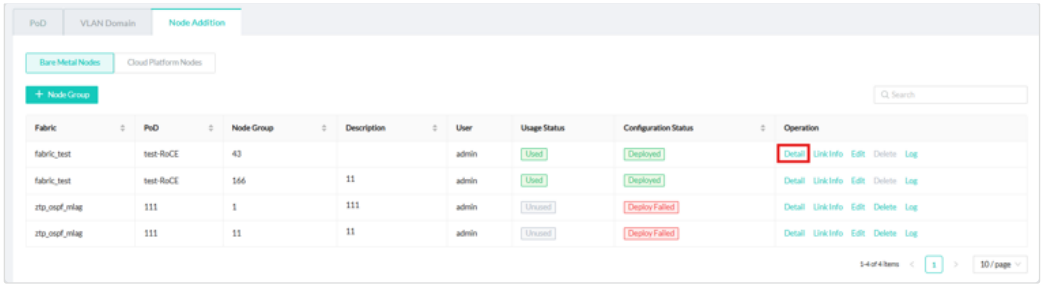
Table 1. Bare Metal Nodes

Metric	Description
Fabric	The fabric to which the node group belongs.
PoD	The PoD to which the node group belongs.
Node Group	The name of the node group.
Description	The description of the node group.
User	The tenant (AmpCon-DC user) who owns the logical network. Currently, you can see only the tenant **admin**.
Usage Status	Whether the virtual network of the node devices in the bare metal node group is connected with

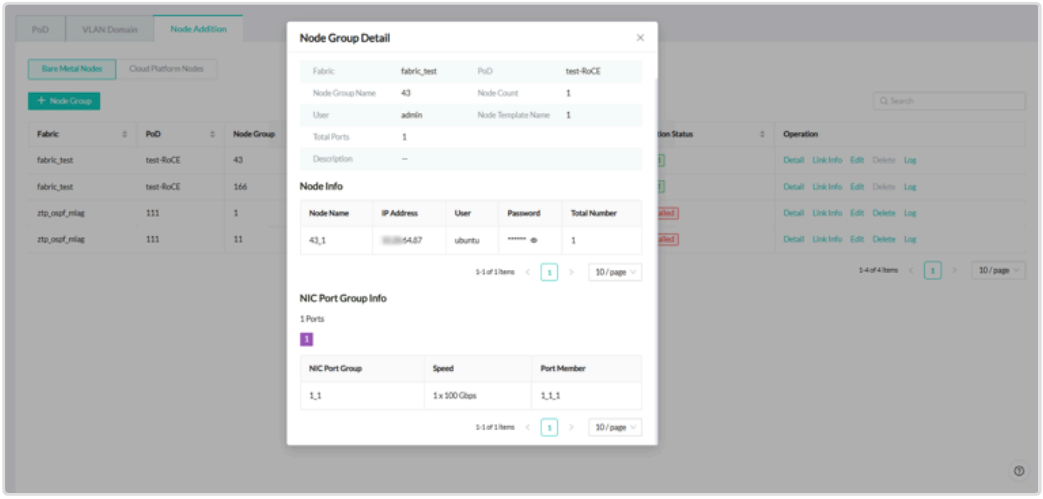
	logical switches.
Configuration Status	Whether the node configurations are applied to switches. • **Not Deployed:** The node uplink configurations haven't been applied. • **Deploying:** The node group configurations are being applied. • **Deployed:** The node group configurations are applied successfully. • **Deploy Failed:** The node group configurations fail to be applied. • **Deleting:** The node group configurations are being deleted. • **Delete Failed:** The node group configurations fail to be deleted. **NOTE** In the following scenarios, even though the **Configuration Status** is **Deployed**, the node uplink configurations will still fail to be used for overlay service provisioning. • The speed of the selected NIC ports and selected switch ports is not the same. • The node uplink configurations are not consistent with actual physical connections.

Viewing Details of a Bare Metal Node Group

To view details of an added bare metal node group, locate the node group in the **Bare Metal Nodes** sub-tab, and then click **Detail**.



Then, you can see detailed configurations of the node group.



In the **Node Group Info** section, you can see the following information:

Table 2. Node Group Metrics

Metric	Description
Fabric	The fabric to which the node group belongs.
PoD	The PoD to which the node group belongs.
Node Group Name	The name of the node group.
Node Count	The total number of node devices in the node group.
User	The AmpCon-DC user who added the node group.
Node Template Name	The name of the node template used in the node group.
Total Ports	The total number of NIC ports in the node group.

In the **Node Info** section, you can see the following information:

Table 3. Node Metrics

Metric	Description
Node Name	The hostname of the bare metal node device.
IP Address	The IP address of the bare metal node device.
User	The username used to log in to the bare metal node device.
Password	The password of the user.
Total Number	The count of NIC port groups.

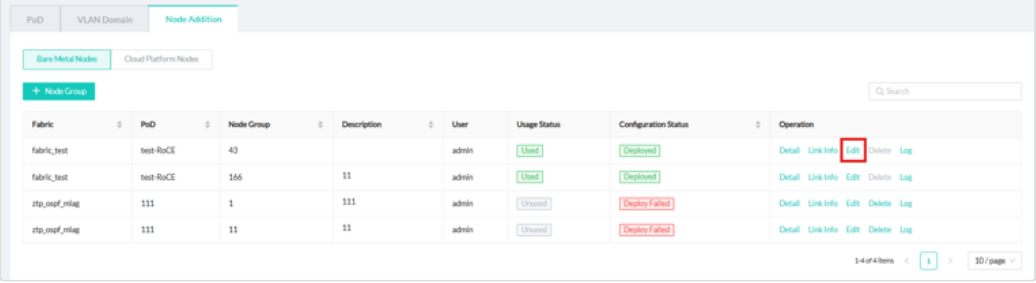
In the **NIC Port Group Info** section, you can see a panel displaying all ports in the node group. In addition, you can see the following information:

Table 4. NIC Port Group Info

Metric	Description
NIC Port Group	The name of the NIC port group.
Speed	The expected speed of each NIC in the NIC port group.
Port Member	The port members in the NIC port group.

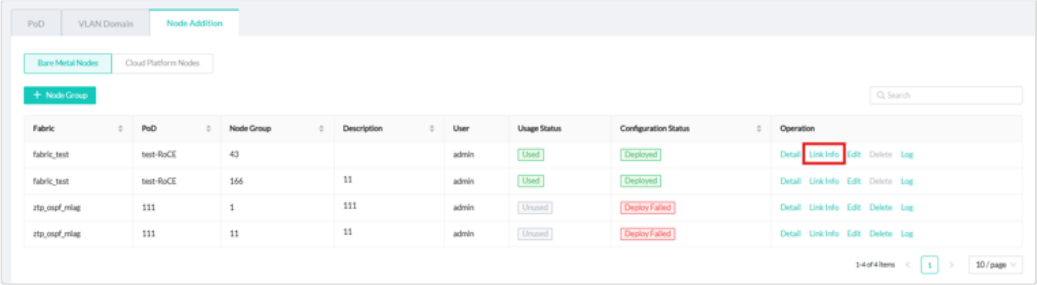
Editing Bare Metal Node Groups

To edit a bare metal node group, locate the node group in the **Bare Metal Nodes** sub-tab, and then click **Edit**.



Checking Link Information of a Node Group

To check for link information of a bare metal node group, locate the node group in the **Bare Metal Nodes** sub-tab, and then click **Link Info**.



Then, you can see the following information:

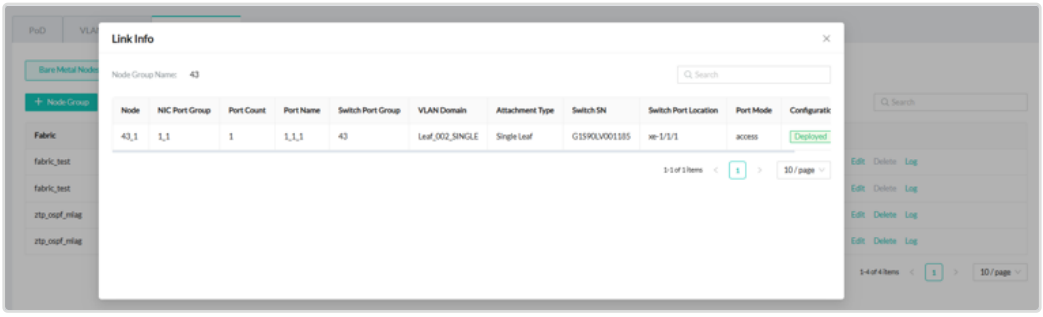


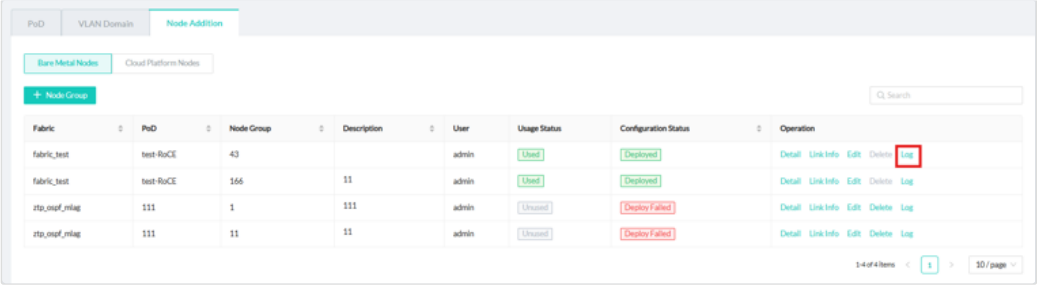
Table 5. Link Metrics

Metric	Description
Node	The hostname of the bare metal node.
Node Group	The name of the node group.
NIC Port Group	The name of the NIC port group.
Port Count	The total number of NIC ports.
Port Name	The name of the NIC port connected to the switch.
Switch Port Group	The name of the switch port group.
VLAN Domain	The VLAN domain to which the leaf switch belongs.
Attachment Type	Whether the node device is connected to an MLAG leaf switch or a non-MLAG leaf switch. • **MLAG Leaf:** The node device is connected to an MLAG leaf switch. • **Single Leaf:** The node device is connected to a non-MLAG leaf switch. **NOTE**

	If the node device is connected to both peer MLAG leaf switches (dual-homed), you can see two lines of data, and each line contains one peer leaf switch.
Switch	The switch to which the bare metal node device is connected.
Switch Port Location	The name of the switch port. **NOTE** The port count displayed here is determined by the **Physical Link Count per Leaf Switch** value when you create a switch port group.
Port Mode	The port mode used by the node device to connect to the leaf switch, **Access** or **Trunk**.
Configuration Status	Whether the node configurations are applied to switches. • **Deploying:** The node group configurations are being applied. • **Deployed:** The node group configurations are applied successfully. • **Deploy Failed:** The node group configurations fail to be applied. • **Deleting:** The node group configurations are being deleted. • **Delete Failed:** The node group configurations fail to be deleted.

Checking Logs of a Node Group

To check for logs of a bare metal node group for troubleshooting purpose, locate the node group in the **Bare Metal Nodes** sub-tab, and then click **Log**.



In the pop-up window, you can see all the leaf switches to which the node devices in the node group connect. Locate a switch, and click **Log** to check for configuration logs.

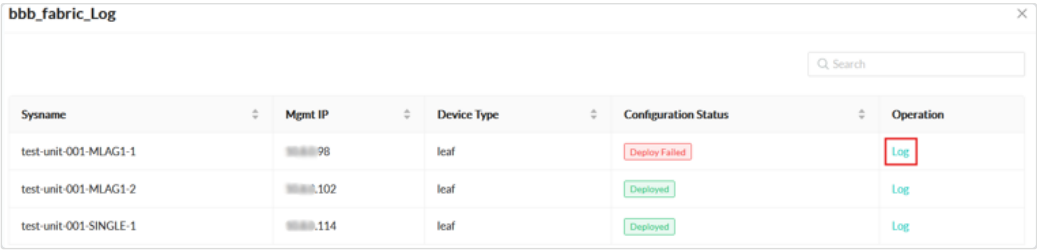


Table 6. Node Group Log

Metric	Description
Sysname	The hostname of the switch to which the bare metal node device connect.
Mgmt IP	The management IP address of the switch. **Mgmt IP** is used to connect to the AmpCon-DC server.
Device Type	The type of the switch in the fabric. Currently, only **Leaf** is displayed, which means leaf switches.

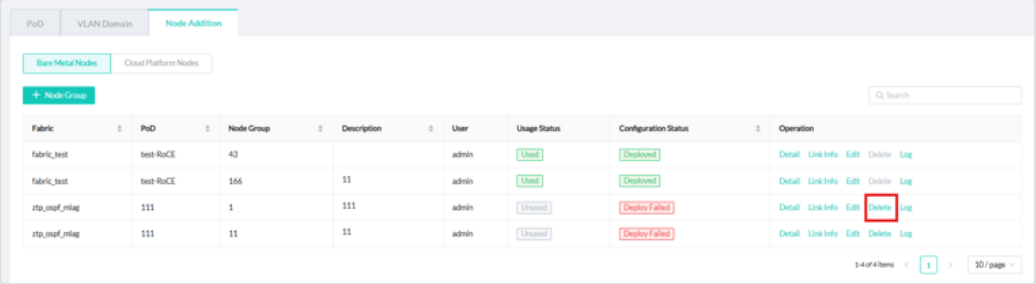
Configuration Status	Whether the node configurations are applied to switches. • **Deploying:** The node group configurations are being applied. • **Deployed:** The node group configurations are applied successfully. • **Deploy Failed:** The node group configurations fail to be applied. • **Deleting:** The node group configurations are being deleted. • **Delete Failed:** The node group configurations fail to be deleted.

Deleting a Node Group

To delete a bare metal node group, locate the node group, and then click **Delete**.

After you delete a node group, the node uplink configurations for this node group will be deleted from uplink non-MLAG switch or MLAG switches.

> **NOTE**
>
> The bare metal node group can't be deleted in the following cases:
>
> - One or multiple uplink leaf switches are offline, which means the switches are not connected with AmpCon-DC.
> - One or multiple uplink leaf switches are online, but switch configurations can't be deleted for some reason.
> - One or multiple bare metal node devices in the node group are in **Used** status, which means the bare metal node devices have already been used for overlay service provisioning.



Configuring Node Uplink for Cloud Platform Nodes

Cloud platform nodes mean node devices in the vSphere cloud platform.

When you add vSphere PoD, AmpCon-DC automatically retrieves node devices from the vSphere cloud platform, and thus you don't need to add node devices to vSphere PoD manually.

To use vSphere node devices for overlay service provisioning, you need to configure node uplink for these node devices.

> **NOTEs**
>
> - Currently, OpenStack PoD can't be used for overlay service provisioning, and thus you are not recommended to configure node uplink for OpenStack node devices. Even though you can configure node uplink for OpenStack node devices, you can't use the node devices for overlay service provisioning.
> - For vSphere PoD, AmpCon-DC automatically retrieves node devices from vSphere, and thus you don't need to add node devices to vSphere PoD manually. But you need to configure node uplink for the node devices.

Prerequisites
Guidelines
Procedure
What to Do Next

Prerequisites

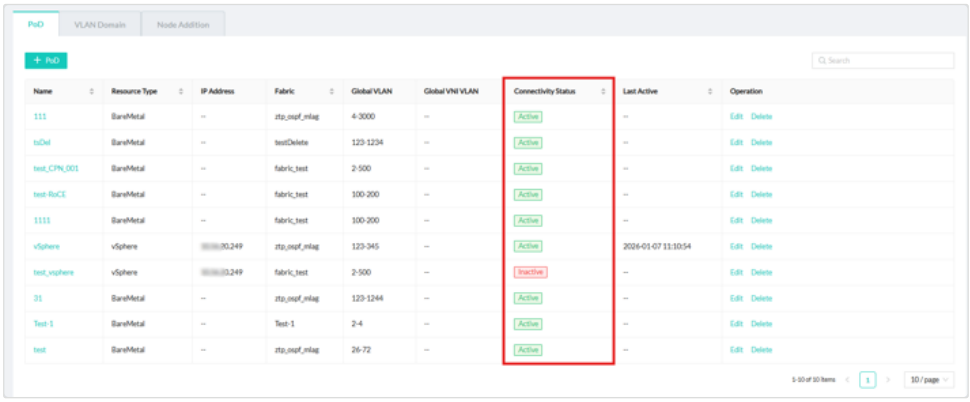
Before you configure node uplink for specific node devices, ensure that the following prerequisites are met:

1. Ensure that you have completed the physical network deployment through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.
2. Ensure that you have completed VLAN Domain configuration for the fabric. For more information, see VLAN Domains.
3. Ensure that you have created the vSphere PoD to which the node devices belong. For more information, see vSphere PoD.

4. The vSphere node devices can be displayed in the **Cloud Platform Nodes** sub-tab only when all of the following prerequisites are met:

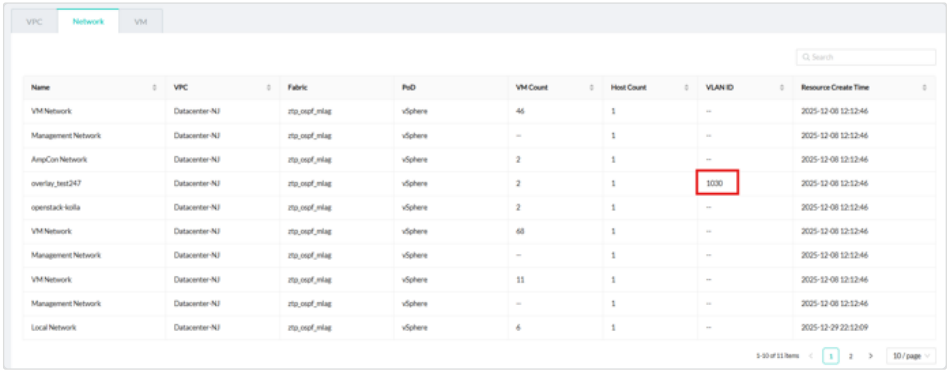
- Click **Resource > Resource Interconnection** from the navigation bar. In the **PoD** tab, ensure that the PoD of the vSphere node devices is in **Active** status.

  The **Active** status means that AmpCon-DC is connected to the vSphere platform.



- Click the PoD name to which the vSphere node devices belong. In the **VLAN ID** column of the **Network** tab, ensure that VLAN IDs are displayed for the virtual networks to which the node devices belong.

  If no VLAN ID is displayed, go to the vSphere platform and configure VLAN IDs for these virtual networks.



Guidelines

Pay attention to the following points:

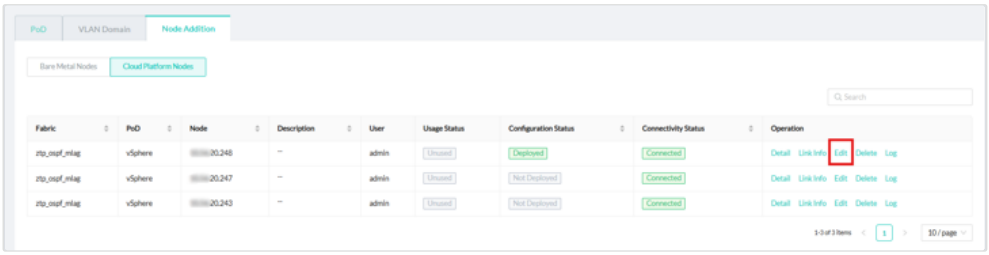
- The speed of the NIC ports and connected switch ports must be the same.
- The node uplink configurations are consistent with actual physical connections.

Or else, the node uplink configurations will fail to be used for overlay service provisioning.

Procedure

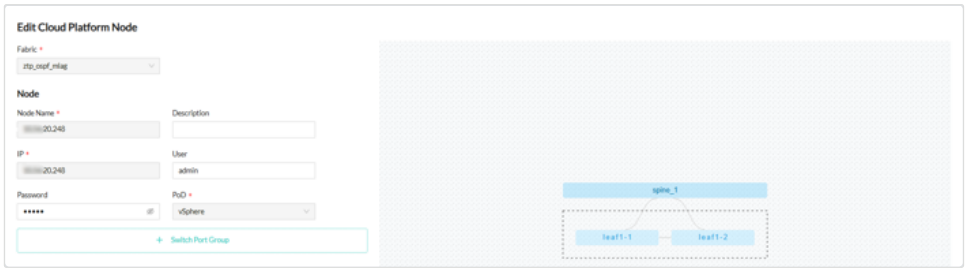
To configure node uplink for a vSphere node device, follow these steps:

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab. In the **Cloud Platform Nodes** sub-tab, locate a vSphere node device, and then click **Edit**.



3. Optional: On the “Edit Cloud Platform Nodes” page, modify the description, username, and password of the node device as needed.

   The fabric, node name, and IP address are retrieved from vSphere and can’t be changed.



4. Click **+ Switch Port Group**. In the **Switch Port Group** section, input the following information:

> **NOTE**
>
> Only one switch port group can be added for each vSphere node device.

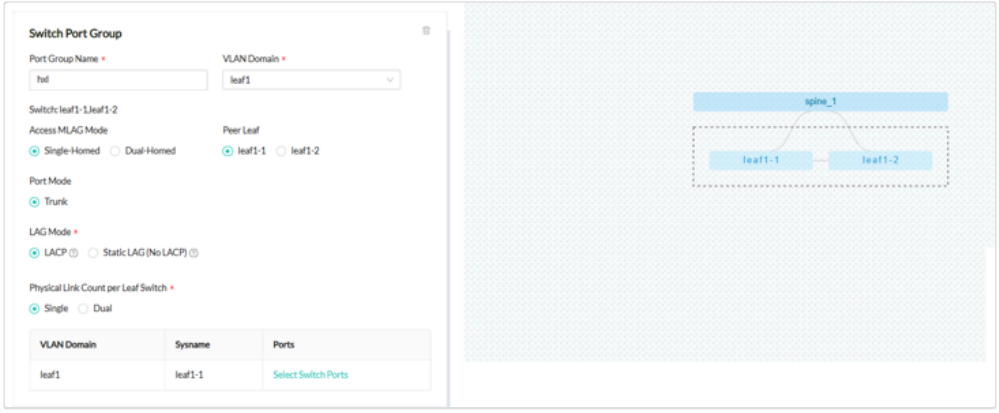


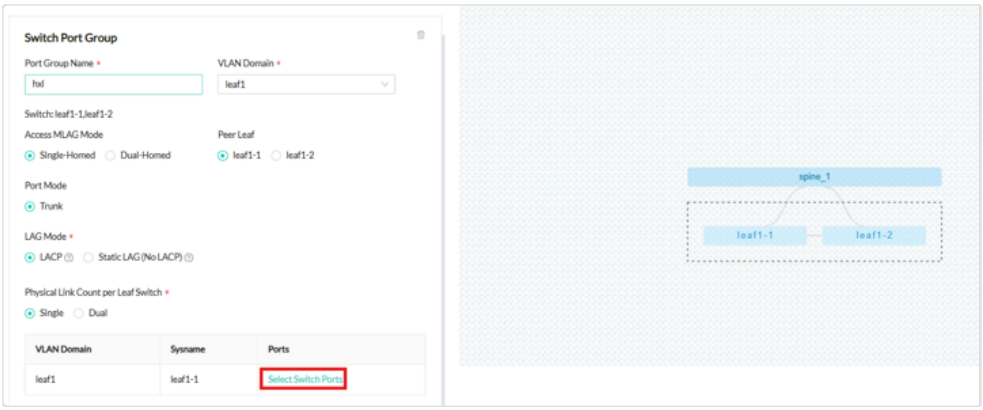
Table 1. Switch Port Group Parameters

Parameter	Description
Port Group Name	The name of the switch port group. The name needs to be unique.
VLAN Domain	The VLAN domain to which the non-MLAG leaf switch or MLAG switches belong. AmpCon-DC automatically retrieves the VLAN Domains of the selected fabric and displays them here. • Each non-MLAG leaf switch is assigned with one distinct VLAN Domain. • Peer leaf switches in an MLAG share the same VLAN Domain.
Access MLAG Mode	Select **Single-Homed** or **Dual-Homed**. • **Single-Homed:** The node device connects to one peer leaf switch in the MLAG setup. • **Dual-Homed:** The node device connects to both peer leaf switches in the MLAG setup. **NOTE** This field is available only when the VLAN domain that you select contains MLAG leaf switches.
Peer Leaf	Select the MLAG peer leaf switch to which the node device is connected. **NOTEs** • This field is available only when the VLAN domain that you select contains MLAG leaf switches and you select **Single-Homed** in the **Access MLAG Mode** section. • If you select **Dual-Homed**, both peer MLAG leaf switches are used to connect with the

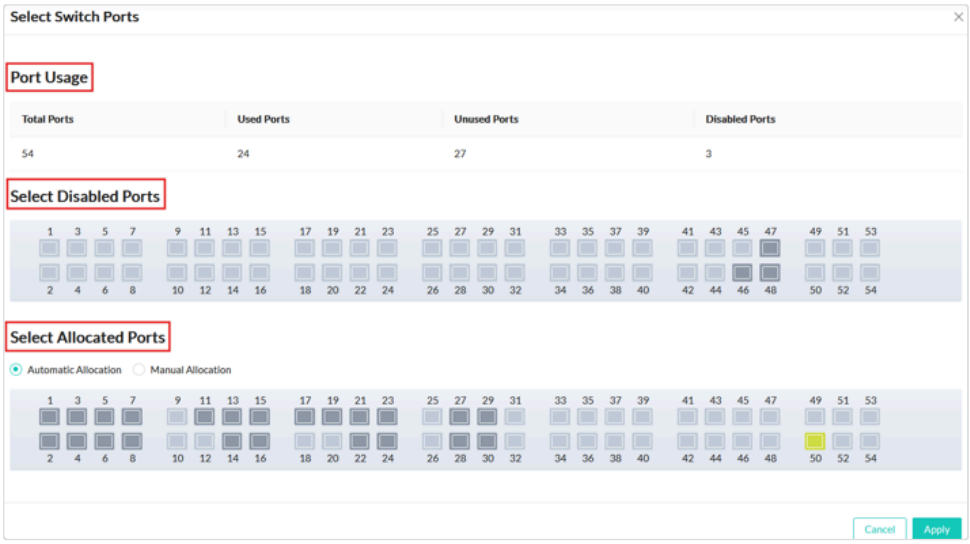
	node device.
Port Mode	The port mode used by the node device to connect to the uplink non-MLAG switch (or MLAG switches). Currently, you can select only **Trunk** as the port mode.
LAG Mode	Whether to use Link Aggregation Groups (LAGs) and which mode to use. An LAG means a logical link formed by bundling multiple physical links. Each LAG uniquely corresponds to a logical interface, also known as a link aggregation interface or Eth-Trunk interface. Select one of the following options: • **LCAP:** Enables Link Aggregation Control Protocol (LACP). For more information about LCAP, see Adding LAG and LACP. • **Static LAG (No LACP):** Unconditionally operates in forwarding mode, instead of participating in LACP protocol negotiation. • **No LAG:** Uses no LAGs. **NOTEs** • If **LACP** is selected, ensure that the devices at both aggregation ends support the LACP protocol. • If the selected VLAN domain contains MLAG leaf switches, you can't see the **No LAG** option. • If the selected VLAN domain doesn't contain MLAG leaf switches and the **Physical Link Count per Leaf Switch** is **1**, you can't see the **LCAP** and **Static LAG (No LACP)** options. • If the selected VLAN domain doesn't contain MLAG leaf switches and the

	Physical Link Count per Leaf Switch is larger than **1**, you can't see the **No LAG** option.
Physical Link Count per Leaf Switch	The physical links with which the node device connects to the leaf switch. Values are **Single** or **Dual**. • **Single:** The node device connects to the leaf switch through one physical link. • **Dual**: The node device connects to the leaf switch through two physical links.

5. In the switch table, click **Select Switch Port**.



6. In the pop-up window, select switch ports to be disabled or to be allocated for node uplink.



a. Optional: In the **Select Disabled Ports** section, click the ports to be disabled, or click disabled ports to enable these ports.

> **NOTE**
>
> Disabled switch ports can't be used for allocation.

b. In the **Select Allocated Ports** section, select one allocation method of switch ports:

Automatic Allocation: AmpCon-DC automatically allocates switch ports from the first available port (unused).

Manual Allocation: You need to manually select the first allocation switch port (unused). Then, the ports to be allocated will be selected automatically in ascending order. The switch ports used will not be selected.

c. Check the port usage information in the **Port Usage** section:

Table 2. Switch Port Parameters

Metric	Description
Total Ports	The count of total switch ports.
Used Ports	The count of used switch ports.
Unused Ports	The count of unused switch ports.
Disabled Ports	The count of disabled switch ports.

d. Click **Apply** to complete the switch port selection.

7. Optional: In the right panel of the node configuration page, check the topology of the selected fabric.

- Click a switch in the topology, and then you can see the following information:

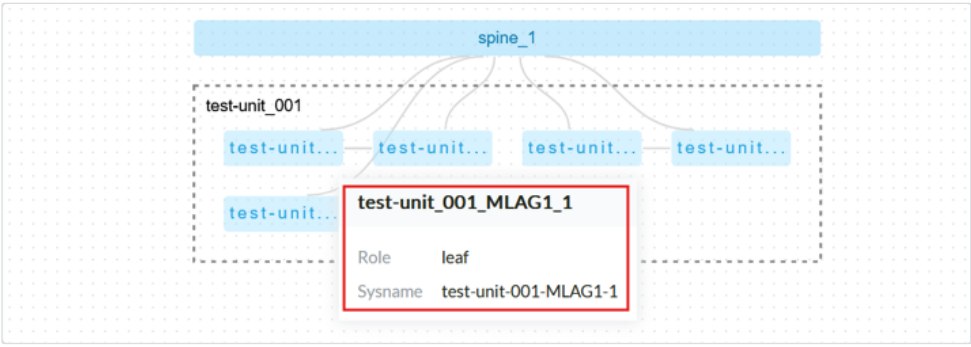


Table 3. Switch Port Parameters

Parameter	Description

Role	The role of the switch in the fabric. Values are **Leaf** or **Spine**, which means a leaf switch or spine switch.
Hostname	The hostname of the switch.

- Click a link in the topology, and then you can see the following information:

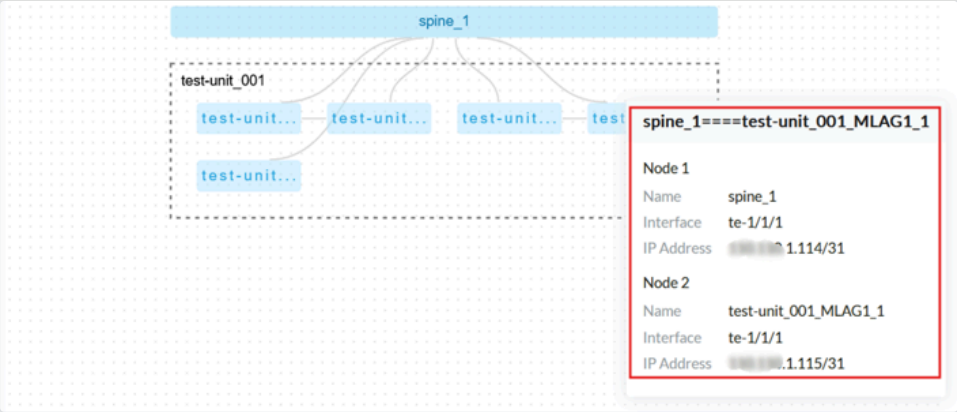


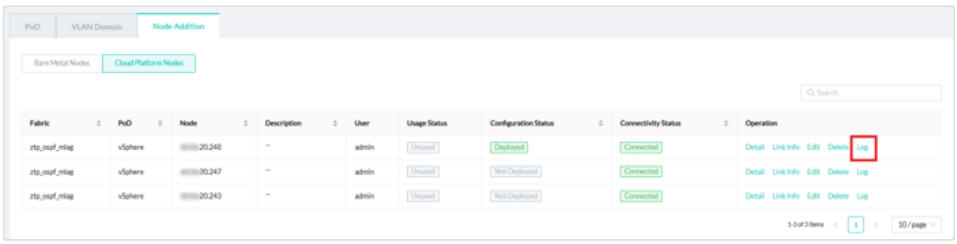
Table 4. Switch Port Parameters

Metric	Sub-Metric	Description
Link Name		The name of the link, including the leaf switch and spine switch names.
Node 1	**Name**	The name of the leaf switch.
	Interface	The port used to connect with the leaf switch.
	IP Address	The IP address of the leaf switch.
Node 2	**Name**	The name of the spine switch.
	Interface	The port used to connect with the spine switch.
	IP Address	The IP address of the spine switch.

8. Click **Apply** to complete the node uplink configuration. The configurations will be pushed to selected switches.
9. In the **Cloud Platform Nodes** sub-tab, locate the node name, and then check whether the **Configuration Status** column shows **Deployed**, which means the configurations are applied

successfully.

If the configuration status is **Deploy Failed**, click **Log** to check more information for troubleshooting.



What to Do Next

After you add node uplink configurations for vSphere node devices, you can manage these configurations as follows:

- View the node list and uplink configuration details.
- Edit node uplink configurations.
- Check for logs and link information for each node device.

For more information, see Managing Node Uplink Configurations.

Managing Node Uplink Configurations

You can manage uplink configurations for vSphere node devices as follows:

- Prerequisites
- Viewing Cloud Platform Nodes
- Viewing Details of a Cloud Platform Node
- Editing Cloud Platform Nodes
- Checking Link Information of a Node
- Checking Logs of a Node
- Deleting Node Uplink

Prerequisites

Ensure that all these prerequisites are met. Or else, you can't see vSphere node devices in the **Cloud Platform Nodes** sub-tab.

Viewing Cloud Platform Nodes

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab.
3. In the **Cloud Platform Nodes** sub-tab, check all node devices retrieved by AmpCon-DC from the vSphere cloud platform.

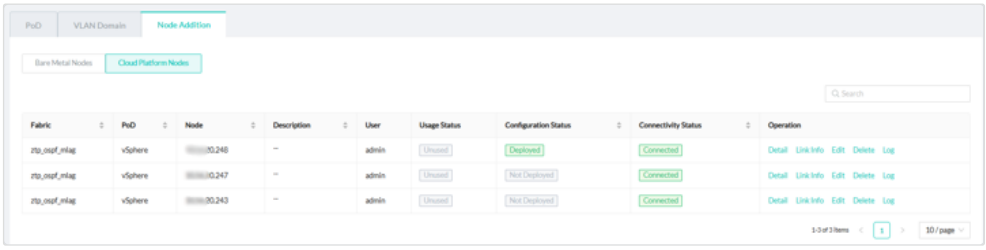


Table 1. Cloud Platform Nodes

Metric	Description
Fabric	The fabric to which the node device belongs.
PoD	The PoD to which the node device belongs.
Node	The name of the vSphere node device.
Description	The description of the node device.

User	The tenant (AmpCon-DC user) who owns the the logical network. Currently, you can see only the tenant **admin**.
Usage Status	Whether the virtual network of the node device is connected with a logical switch.
Configuration Status	Whether the node configurations are applied to switches. **Not Deployed:** The node uplink configurations haven't been applied. **Deploying:** The node uplink configurations are being applied. **Deployed:** The node uplink configurations are applied successfully. **Deploy Failed:** The node uplink configurations fail to be applied. **Deleting:** The node uplink configurations are being deleted. **Delete Failed:** The node uplink configurations fail to be deleted. **NOTE** In the following scenarios, even though the **Configuration Status** is **Deployed**, the node uplink configurations will still fail to be used for overlay service provisioning. • The speed of the NIC ports and connected switch ports is not the same. • The node uplink configurations are not consistent with actual physical connections.
Connectivity Status	Whether AmpCon-DC is connected with the cloud platform (vSphere).

	• **Connected:** AmpCon-DC is connected with the cloud platform. • **Disconnected:** AmpCon-DC is not connected with the cloud platform.

Viewing Details of a Cloud Platform Node

To view details of an added vSphere node device, locate the node device in the **Cloud Platform Nodes** sub-tab, and then click **Detail**.

Then, you can see detailed configurations of the node device.

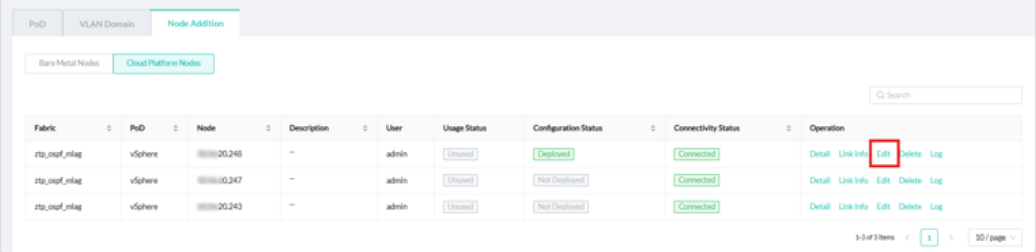


Table 2. Node Details

Metric	Description
Fabric	The fabric to which the node group belongs.
PoD	The PoD to which the node group belongs.
Node Name	The name of the node device.
Description	The description of the node device.
User	The user to log in to the node device.
Password	The password of the user.
IP Address	The IP address of the node device.

Editing Cloud Platform Nodes

To edit a vSphere node device, locate the node device in the **Cloud Platform Nodes** sub-tab, and then click **Edit**.



Checking Link Information of a Node

To check for link information of a vSphere node device, locate the node device in the **Cloud Platform Nodes** sub-tab, and then click **Link Info**.

Then, you can see the following information:

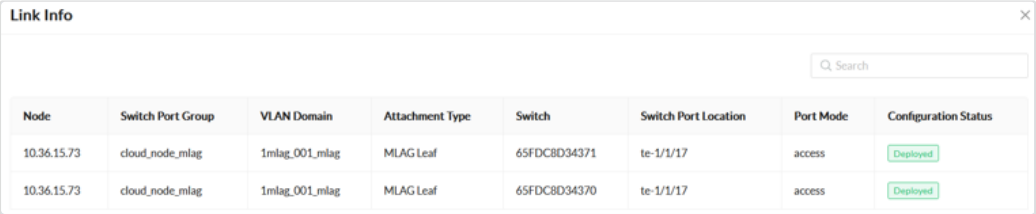


Table 3. Link Information

Metric	Description
Node	The hostname of the vSphere node device.
Switch Port Group	The name of the switch port group.
VLAN Domain	The VLAN domain to which the uplink switch belongs.
Attachment Type	Whether the node device is connected to an MLAG leaf switch or a non-MLAG leaf switch. • **MLAG Leaf:** The node device is connected to an MLAG leaf switch. • **Single Leaf:** The node device is connected to a non-MLAG leaf switch. **NOTE** If the node device is connected to both peer MLAG leaf switches (dual-homed), you can see two lines of data, and each line contains one peer leaf switch.

Switch	The uplink switch to which the vSphere node device is connected.
Switch Port Location	The name of the switch port (or ports) used. **NOTE** The port count displayed here is determined by the **Physical Link Count per Leaf Switch** value when you create a switch port group.
Port Mode	The port mode used by the node device to connect to the leaf switch. Currently, you can see only **Trunk** as the port mode.
Configuration Status	Whether the node configurations are applied to switches. • **Deploying:** The node uplink configurations are being applied. • **Deployed:** The node uplink configurations are applied successfully. • **Deploy Failed:** The node uplink configurations fail to be applied. • **Deleting:** The node uplink configurations are being deleted. • **Delete Failed:** The node uplink configurations fail to be deleted.

Checking Logs of a Node

To check for logs of a vSphere node device for troubleshooting or auditing purpose, locate the node device in the **Cloud Platform Nodes** sub-tab, and then click **Log**.

In the pop-up window, you can see all the leaf switches to which the node devices in the node uplink connect. Locate a switch, and then click **Log** to check for configuration logs.

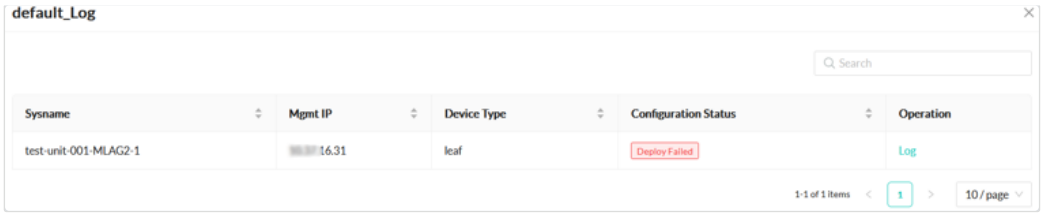
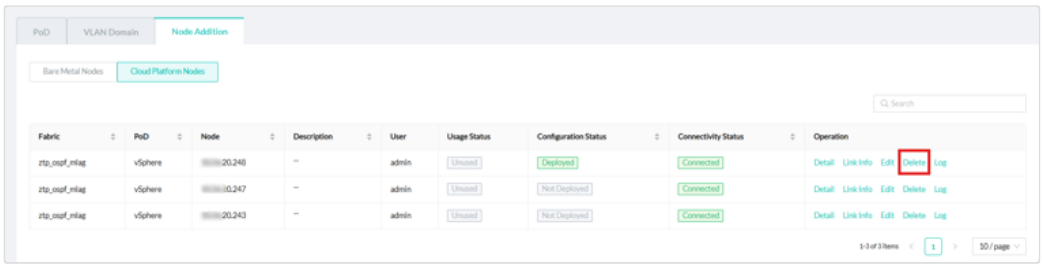


Table 4. Node Log

Metric	Description
Sysname	The hostname of the vSphere node device.
Mgmt IP	The management IP address of the switch.
Device Type	The type of the switch in the fabric. Currently, only **Leaf** is displayed, which means leaf switches.
Configuration Status	Whether the node configurations are applied to switches. • **Deploying:** The node uplink configurations are being applied. • **Deployed:** The node uplink configurations are applied successfully. • **Deploy Failed:** The node uplink configurations fail to be applied. • **Deleting:** The node uplink configurations are being deleted. • **Delete Failed:** The node uplink configurations fail to be deleted.

Deleting Node Uplink

To delete uplink configurations for a vSphere node device, locate the node device in the **Cloud Platform Nodes** sub-tab, and then click **Delete**.



After you delete a node device, its node uplink configurations will be deleted from uplink non-MLAG switch or MLAG switches.

NOTEs

- The node device can't be deleted in the following cases:
  - One or multiple uplink leaf switches are offline, which means the switches are not connected with AmpCon-DC.
  - One or multiple uplink leaf switches are online, but switch configurations can't be deleted for some reason.
  - One or multiple node devices are in **Used** status, which means the node devices have already been used for overlay service provisioning.
- The node device that you deleted will be displayed again in the cloud platform node list because AmpCon-DC periodically retrieves node devices from the vSphere cloud platform. However, the node uplink configurations are deleted for this node device.
- If a deleted node device is not displayed in the cloud platform node list, check whether AmpCon-DC can connect to the vSphere cloud platform.

Node Uplink Scenarios in AI

To understand how to use the node uplink feature in AI deployments, see the following configuration steps in multi-rail access and single-rail access scenarios.

See the following child topics:

- Single-Rail Access Scenarios
- Multi-Rail Access Scenarios

Single-Rail Access Scenarios

Single-track access refers to a network architecture where all network interface cards (NICs) of a node device are aggregated into a single leaf switch, forming a centralized communication path.

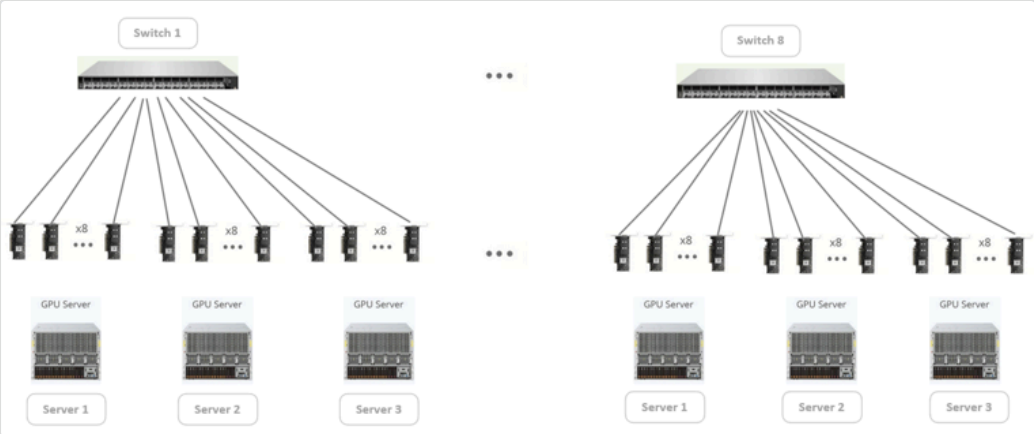
Scenario Description
Configuration Guidelines
Configuration Procedure

Scenario Description

In the following scenario, 24 bare metal node devices connect to 8 leaf switches.

Each bare metal node device has 8 NICs, and all these 8 NICs are connected to one leaf switch. Each leaf switch has 24 downlink switch ports and thus can connect to 3 bare metal node devices.

Each NIC port of a node device is assigned with a distinct VLAN, and thus each NIC port of a node device needs to be put into a distinct NIC port group.



Configuration Guidelines

When you configure node uplink in AmpCon-DC, you need to add **8** node groups. Each node group contains **3** bare metal node devices.

In each node group, pay attention to the following points:

- Use a node template containing **8** NIC port groups. Each NIC port group contains **1** NIC port.
- Add **8** switch port groups. A NIC port in each of the 8 NIC port groups connects to **1** switch port in each of the 8 switch port groups.

- The physical link count per individual switch is **1**, which means each bare metal node device connects to a leaf switch through one physical link.

Configuration Procedure

To configure node uplink for this scenario, follow these steps:

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab.
3. In the **Bare Metal Node Devices** sub-tab, click **+ Node Group**.
4. In the **Fabric** drop-down list, select the fabric to which the node group belongs.

   The fabric must have been created before you add the node group.
5. In the **Node Group** section, input the following information:

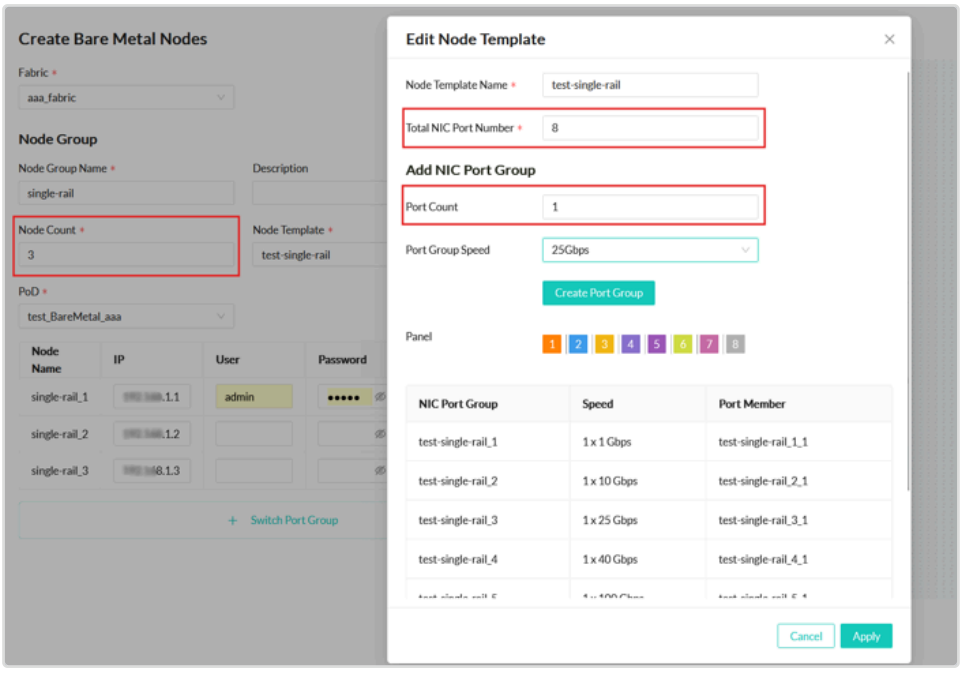


Table 1. Node Group Parameters

Parameter	Description
Node Group Name	Specify the name of the node group. The name needs to be unique.
Description	Optional. Specify the description of the node group.
Node Count	Enter **3** to represent all these 3 bare metal node devices to which a leaf switch can connect.

Node Template	Select or create a template with 8 NIC port groups. For more information about node templates, see Adding a Node Template. • Each NIC port of a bare metal node device is assigned with a distinct VLAN, and thus each NIC port of a bare metal node device needs to be put into a distinct NIC port group. • Ensure that the **Total NIC port Number** value is **8** and each NIC port group has **one** NIC port assigned.
PoD	The bare metal PoD to which the node group belongs.

In the following table, enter the IP address, username (optional), and password (optional) of each bare metal node device to be added to the node group.

6. In the **Switch Port Group** section, click **+ Switch Port Group**, and then input the following information:

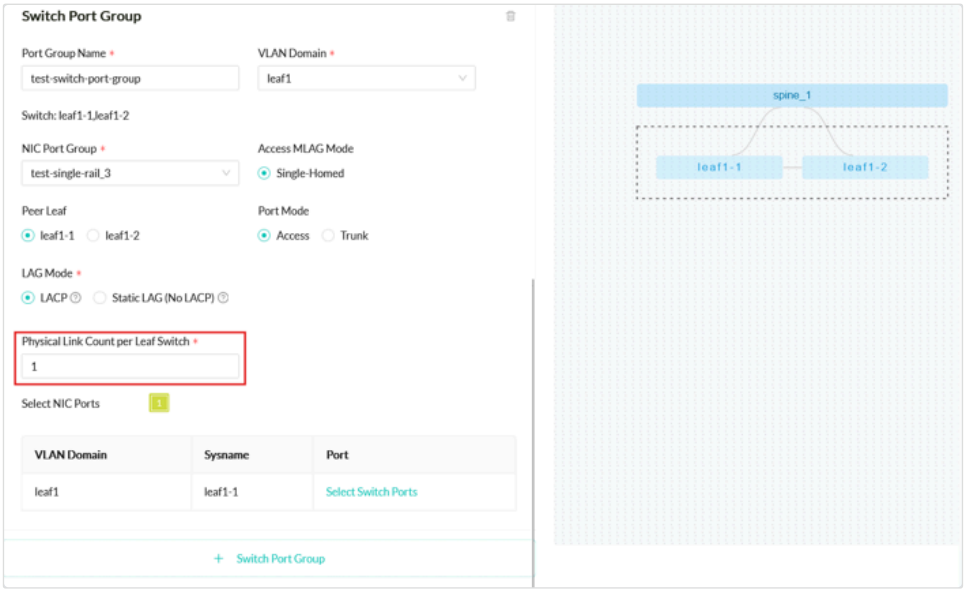


Table 2. Switch Port Group Parameters

Parameter	Description
Port Group Name	Specify the name of the switch port group. The name needs to be unique.

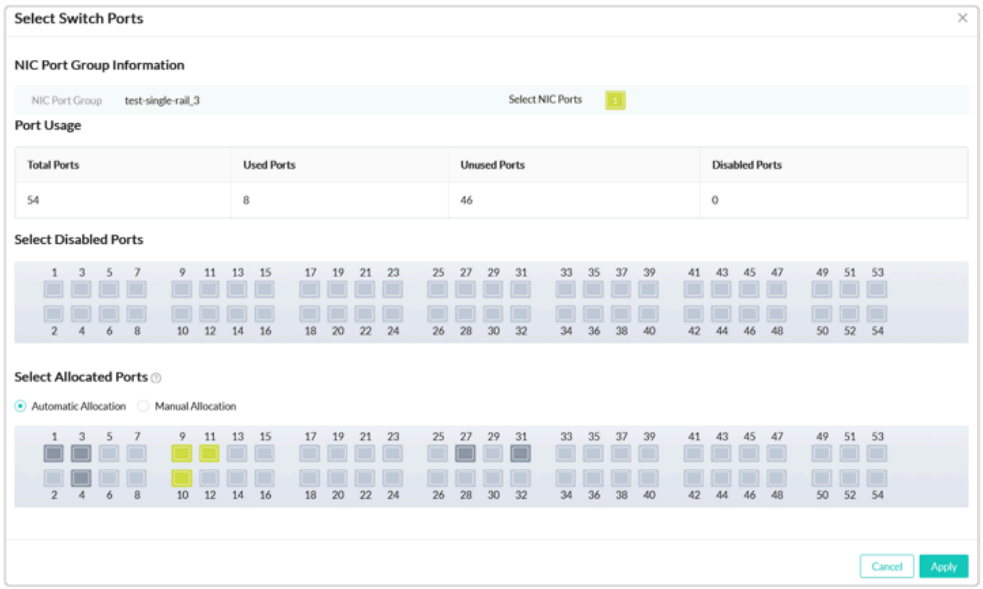
VLAN Domain	Select a VLAN Domain containing the leaf switch to which the 3 bare metal node devices connect.
NIC Port Group	Select a NIC port group. The NIC port groups in the list are those groups added in the selected node template.
Access MLAG Mode	Select **Single-Homed** or **Dual-Homed**. • **Single-Homed:** The node device connects to one peer leaf switch in the MLAG setup. • **Dual-Homed:** The node device connects to both peer leaf switches in the MLAG setup. This field is available only when the VLAN domain that you select contains MLAG leaf switches.
Peer Leaf	Select the MLAG peer leaf switch to which the node device is connected. • This field is available only when the VLAN domain that you select contains MLAG leaf switches and you select **Single-Homed** in the **Access MLAG Mode** section. • If you select **Dual-Homed**, both peer MLAG leaf switches are used to connect with the node device.
Port Mode	Select the port mode used by each node device to connect to the leaf switch, **Access** or **Trunk**.
Physical Link Count per Leaf Switch	Enter **1**, which means each bare metal node device connects to a leaf switch through one physical link.

7. In the **Select NIC Port** section, select the NIC port used to connect with a leaf switch.

> **NOTEs**
>
> • You can see only **one** NIC port because each NIC port group has only one NIC port assigned in the selected node template.

- Each bare metal node device uses the selected NIC port to connect with the switch port of the selected leaf switch.

8. In the switch table, click **Select Switch Port**.
9. In the pop-up window, select switch ports to be disabled (optional) or to be allocated for node uplink. For more information, see **Step 5** of Configuring Node Uplink for Bare Metal Nodes.



10. Repeat **Step 6** to **Step 9** to add the other 7 switch port groups.

> **NOTEs**
>
> - For different switch port groups, select different NIC port groups in the **NIC Port Group** drop-down list.
> - For different switch port groups, select the same VLAN Domain in the **VLAN Domain** drop-down list. This is because all 8 NIC ports of the 3 bare metal node devices connect to the same leaf switch.

11. Click **Apply** to complete the addition of the bare metal node group.
12. Repeat **Step 1** to **Step 11** to add the other 7 node groups.

> **NOTE**
>
> For different node groups, select different VLAN Domains in the **VLAN Domain** drop-down list. This is because bare metal node devices in different node groups connect to different leaf switches.

Multi-Rail Access Scenarios

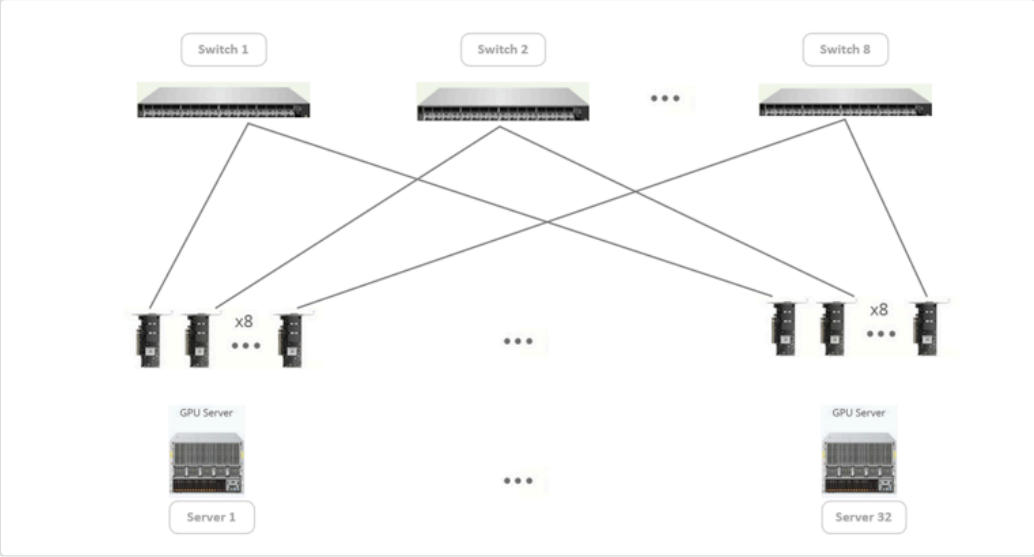
Multi-rail access refers to a network architecture design where each network interface card (NIC) of a single node device is connected to a different leaf switch, instead of being aggregated into a single switch, forming parallel communication paths to enhance bandwidth utilization and fault tolerance.

Scenario Description
Configuration Guidelines
Configuration Procedure

Scenario Description

In the following scenario, 32 bare metal node devices connect to 8 leaf switches. The node devices are connected at a 1:1 port to uplink ratio.

Each node device has 8 NIC ports, and each NIC port is connected to a distinct leaf switch. So each node device uses 8 rails to connect with 8 leaf switches.



Configuration Guidelines

When you configure node uplink in AmpCon-DC, you need to add **1** node group containing **32** bare metal node devices.

In the node group, pay attention to the following points:

- Use a node template containing **8** NIC port groups. Each NIC port group contains **1** NIC port.
- Add **8** switch port groups. A NIC port in each of the 8 NIC port groups connects to **1** switch port in each of the 8 switch port groups.

- The physical link count per individual switch is **1**, which means each bare metal node device connects to a leaf switch through one physical link.

Configuration Procedure

To configure node uplink for this scenario, follow these steps:

1. Click **Resource > Resource Interconnection** from the navigation bar.
2. Click the **Node Addition** tab.
3. In the **Bare Metal Node Devices** sub-tab, click **+ Node Group**.
4. In the **Fabric** drop-down list, select the fabric to which the node group belongs.

   The fabric must have been created before you add the node group.
5. In the **Node Group** section, input the following information:

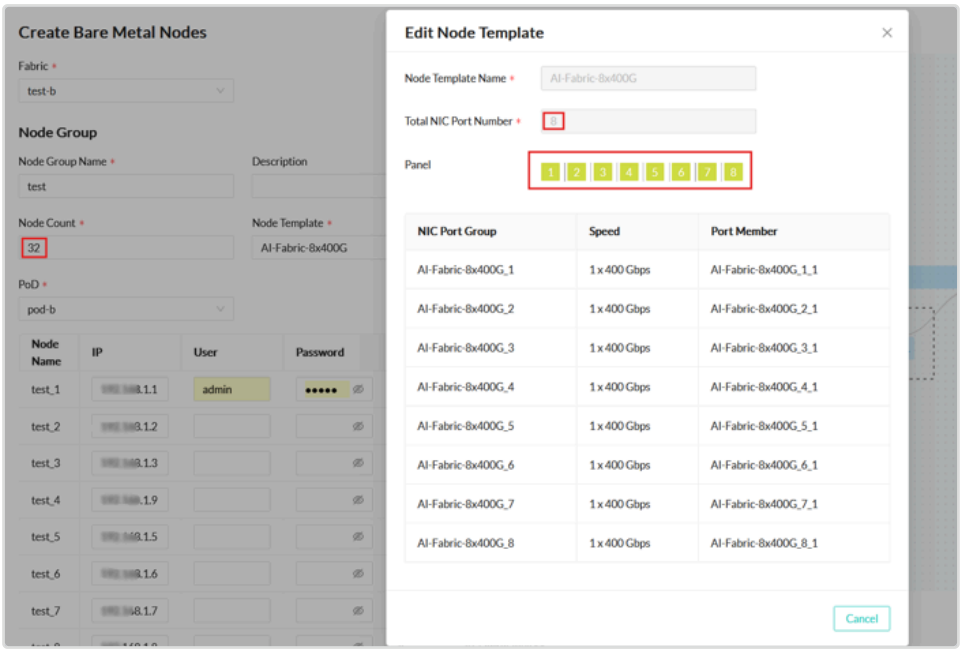


Table 1. Node Group Parameters

Parameter	Description
Node Group Name	Specify the name of the node group. The name needs to be unique.
Description	Optional. Specify the description of the node group.
Node Count	Enter **32** to represent all these 32 bare metal node devices to which a leaf switch can connect.

Node Template	Select or create a template with 8 NIC port groups. For more information about node templates, see Adding a Node Template. • Each node device has 8 NIC ports to connect with 8 leaf switches with different VLANs, and thus each NIC port needs to be put into a distinct NIC port group. • Ensure that the **Total NIC port Number** value is **8**, and each NIC port group has **one** NIC port assigned.
PoD	The bare metal PoD to which the node group belongs.

In the following table, enter the IP address, username (optional), and password (optional) of each bare metal node device to be added to the node group.

6. In the **Switch Port Group** section, click **+ Switch Port Group**, and then input the following information:

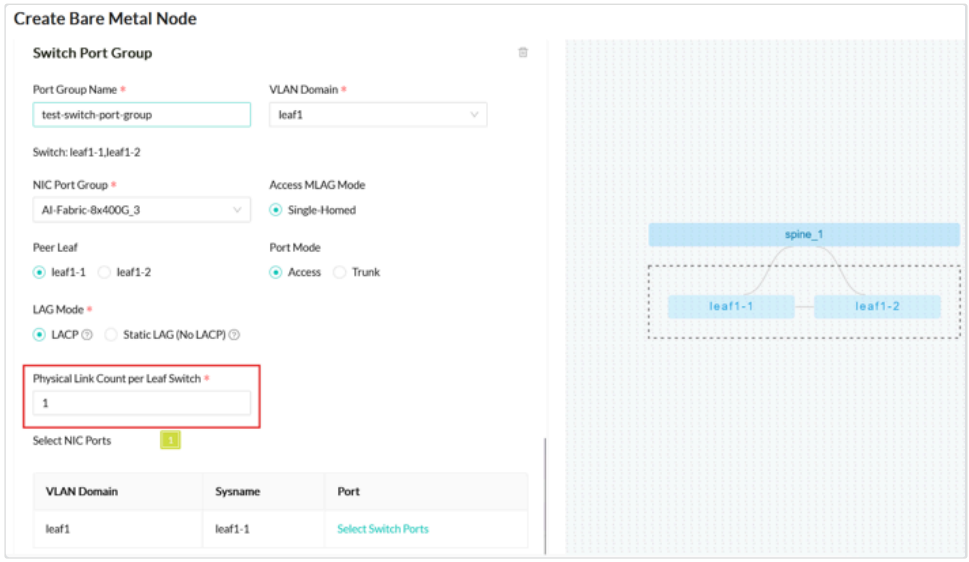


Table 2. Switch Port Group Parameters

Parameter	Description
Port Group Name	Specify the name of the switch port group. The name needs to be unique.

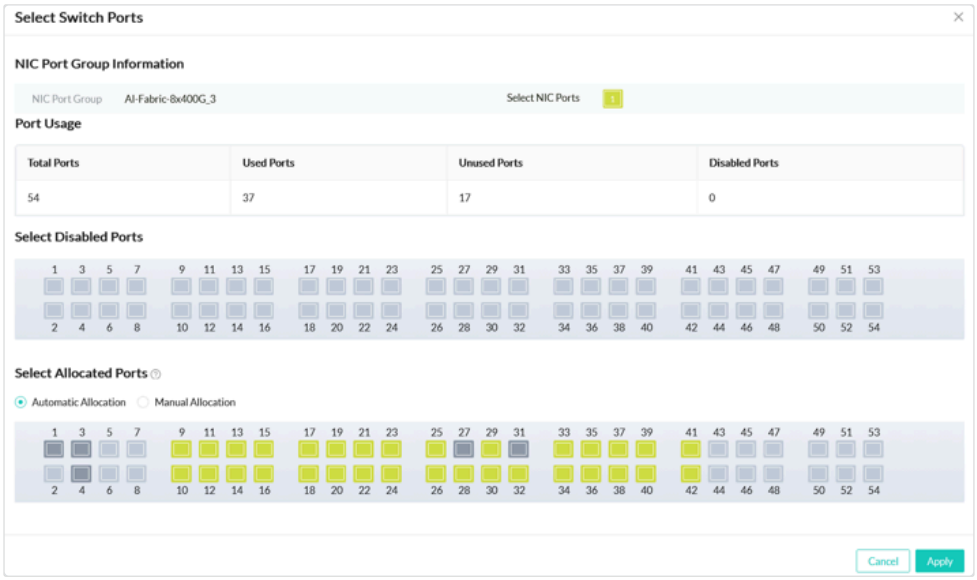
VLAN Domain	Select a VLAN Domain containing the leaf switch to which the bare metal node devices connect.
NIC Port Group	Select a NIC port group. The NIC port groups in the list are those groups added in the selected node template.
Access MLAG Mode	Select **Single-Homed** or **Dual-Homed**. • **Single-Homed:** The node device connects to one peer leaf switch in the MLAG setup. • **Dual-Homed:** The node device connects to both peer leaf switches in the MLAG setup. This field is available only when the VLAN domain that you select contains MLAG leaf switches.
Peer Leaf	Select the MLAG peer leaf switch to which each node device is connected. • This field is available only when the VLAN domain that you select contains MLAG leaf switches and you select **Single-Homed** in the **Access MLAG Mode** section. • If you select **Dual-Homed**, both peer MLAG leaf switches are used to connect with the node device.
Port Mode	Select the port mode used by each node device to connect to the leaf switch, **Access** or **Trunk**.
Physical Link Count per Leaf Switch	Enter **1**, which means each bare metal node device connects to a leaf switch through one physical link.

7. In the **Select NIC Port** section, select the NIC port used to connect with a leaf switch.

> **NOTEs**
>
> • You can see only **one** NIC port because each NIC port group has only one NIC port assigned in the selected node template.

- Each bare metal node device uses the selected NIC port to connect with the switch port of the selected leaf switch.

8. In the switch table, click **Select Switch Port**.
9. In the pop-up window, select switch ports to be disabled (optional) or to be allocated for node uplink. For more information, see **Step 5** of Configuring Node Uplink for Bare Metal Nodes.



10. Repeat **Step 6** to **Step 9** to add the other 7 switch port groups.

> **NOTE**
>
> - For different switch port groups, select different VLAN Domains in the **VLAN Domain** drop-down list. This is because all 8 NIC ports of the 32 bare metal node devices connect to different leaf switches.
> - For different switch port groups, select a distinct NIC port group in the **NIC Port Group** drop-down list.

11. Click **Apply** to complete the addition of the bare metal node group.

Designing Physical Networks

Underlay means the physical network infrastructure that serves as the foundational layer for data transmission. **Physical networks** are used for underlay provisioning.

In data center networks, east-west traffic dominates the business traffic. Therefore, data centers have a high demand for horizontal scalability. To meet the evolving business requirements in data centers, including cloud scenarios, container scenarios, and AI computing scenarios, the physical network model named 3-stage fabric (leaf-spine-leaf) is introduced to AmpCon-DC.

In the AmpCon-DC UI, you can customize the physical network (3-stage fabric) design to meet specific networking requirements. See the following benefits of this feature:

- MLAG networking support
- Drag-and-drop visual modeling
- Custom physical network topology design
- Two types of network configuration templates from which users can choose based on their needs
- Template-based rapid replication, generating N physical networks from a single template

See the following child topics:

- Physical Network Overview
- Recommended Switches for 2.5.0
- Recommended Switches for 2.5.1
- Quick Design Guide
- Designing Units
- Designing DC Templates
- Designing Fabrics
- Managing Fabrics

> **NOTE**
>
> If you use simplified ZTP, switch deployment and physical network deployment can be completed in one go, and thus you don't need to design physical networks.

Physical Network Overview

Learn the following information about the physical network design solution:

Benefits
Architecture
Networking Elements
Key Concepts

Benefits

AmpCon-DC provides an easy-to-deploy and highly validated fabric design solution, which solves the deployment and operational complexity of next-generation data center networks, leads to a more stable data center fabric, and reduces operational costs.

- **Automate network construction**

  By using DC templates, you can use the interactive canvas to visually design and model a physical network that fits your needs.

  Though only the 3-stage network architecture is supported currently, more network architectures will be supported in later versions.

- **Simplify network design**

  A DC template can be instantiated to one or multiple fabrics representing actual physical networks. You can use one DC template to build multiple fabrics, or you can copy a DC template and customize it to build a new fabric.

- **Decrease configuration time and efforts**

  For configurations of which you don't care about the values, you can add related pools and designate the resource pools to be used in the units and DC template.

  When you deploy the fabric, the required resources are automatically pulled and assigned by AmpCon-DC automatically.

- **Manage switches comprehensively**

  You can leverage the simple and powerful lifecycle management features of AmpCon-DC to manage switches in your network.

Architecture

Before you design a physical network, check Physical Network Architecture.

Networking Elements

In AmpCon-DC, the following elements are used to complete the network design and deployment:

- **Resource pool**

  The centralized collection of resources that are managed and allocated dynamically. AmpCon-DC automatically pulls and assigns IP addresses and Autonomous system numbers (ASNs) from the resource pools that you specified.

- **Point of Delivery (PoD)**

  The minimum service unit of a data center. It's a collection of resources in a data center. In AmpCon-DC, each AZ contains only one type of resources.

  PoDs include three types: bare metal PoD, vSphere PoD, and OpenStack PoD.

- **Unit**

  The minimum networking unit for creating a fabric. A unit includes one or multiple leaf switches.

  In a unit, you can specify details like leaf switch counts and whether to use the MLAG leaf strategy.

- **DC Template**

  The abstraction of network design that defines the relationship of leaf switches and spine switches and underlay and overlay protocols, without defining any vendor-specific information. A DC template contains one or multiple units.

  In a DC template, you can specify the spine switch count, included units and their counts, and underlay and overlay protocol related configurations.

- **Fabric**

  The logical representation of an actual physical network. You can deploy a physical network by designing a fabric in the AmpCon-DC UI. A fabric is based on a DC template. A DC template contains one or multiple units.

  In a fabric, you can specify which managed switches serve as leaf and spine switches.

Key Concepts

Before you design a physical network, you need to understand the key concepts related to physical networks. For more information, see Key Concepts.

Key Concepts

Before you design a physical network, you need to understand the following concepts:

- Autonomous System (AS)
- Border Gateway Protocol (BGP)
  - External Border Gateway Protocol (EBGP)
  - Internal Border Gateway Protocol (IBGP)
- Bare Metal (BM)
- Bridge Domain (BD)
- Leaf Switch
- MP-BGP EVPN
- Multi-Chassis Link Aggregation (MLAG)
- OpenStack
- OSPF
- Spine Switch
- Virtual Routing and Forwarding (VRF)
- VLAN Domain
- Virtual Extensible Local Area Network (VXLAN)
- VXLAN Tunnel End Point (VTEP)
- vSphere, ESXi, and vCenter

Autonomous System (AS)

A collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain, which presents a common and clearly defined routing policy to the Internet. Each AS is assigned an autonomous system number (ASN), for use in Border Gateway Protocol (BGP) routing.

An AS is a collection of routers and networks under a single technical administration, using an interior routing protocol and common metrics to determine how to route packets within the AS, and using an exterior routing protocol to determine how to route packets to other AS.

Border Gateway Protocol (BGP)

A routing protocol used to connect independent systems on the Internet. It is designed by the Internet Engineering Task Force (IETF) as a robust, scalable, and well-defined protocol for exchanging routing information among BGP routers within a single AS (IBGP) or among different AS (EBGP).

External Border Gateway Protocol (EBGP)

A routing protocol used to exchange routing information among different AS.

Internal Border Gateway Protocol (IBGP)

A routing protocol that operates within a single AS to distribute routing information among the BGP routers within that AS.

Bare Metal (BM)

The servers without operating systems, applications, or virtual machines installed.

Bridge Domain (BD)

The Layer 2 broadcast domain in which data packets are forwarded on a VXLAN network. BD is also called large Layer 2 domain.

In a traditional network, VLANs are identified by VLAN ID. Similarly, in a VXLAN network, BDs are identified by VXLAN Network Identifiers (VNIs).

Leaf Switch

An access node on a VXLAN fabric network, which connects various network devices to the VXLAN network.

MP-BGP EVPN

Ethernet Virtual Private Network (EVPN) based on Multi-protocol Extensions for Border Gateway Protocol (MP-BGP).

EVPN is a next-generation VPN solution that introduces a control plane to better control the MAC address learning process. MP-BGP is leveraged to distribute MAC information. MP-BGP EVPN facilitates efficient MAC address learning and synchronization across the network.

Multi-Chassis Link Aggregation (MLAG)

Implements link aggregation among multiple devices. AmpCon-DC networking solution supports using MLAG on leaf switches.

Two leaf switches set up MLAG through peer links. The two switches are displayed as a logical device on the forwarding plane and as two independent switches on the management control plane. Upgrading and replacing devices are carried out independently, achieving simple maintenance and high running reliability.

OpenStack

An open-source cloud computing management platform that provides diverse components for computing, storage, networking, mirroring, and other services. OpenStack supports almost all

types of cloud environments and provides a cloud computing management platform that supports easy implementation, large-scale expansion, and unified standards.

OpenStack uses various components to control and manage resources, virtualize computing, network, storage, and pool resources. OpenStack also uses components to implement resource collaboration.

OSPF

A dynamic interior gateway protocol that uses link-state information to build and maintain a complete and consistent map of the network topology within an AS. It employs the Dijkstra algorithm to calculate the shortest path tree from each router to all other routers in the AS, based on which routing tables are built.

Spine Switch

The core node on a VXLAN fabric network, which provides high-speed IP forwarding and connects to leaf switches through high-speed interfaces.

Virtual Routing and Forwarding (VRF)

The technology that allows multiple instances of a routing table to coexist within the same router at the same time. It enables logical isolation between different networks on the same physical device. By using VRF, different instances can use the same IP address without conflicts.

VLAN Domain

The VLAN ID ranges of node devices connected to leaf switches. A VLAN Domain includes the Bridge Domain (BD) range and VRF VLAN range.

Virtual Extensible Local Area Network (VXLAN)

The overlay network virtualization technology that enables the creation of virtual Layer 2 networks across Layer 3 network boundaries by encapsulating Layer 2 frames within Layer 3 UDP packets.

VXLAN extends traditional VLAN technology, addresses the limitations of VLANs, such as the 4096-network limit, and meets the needs of large-scale, virtualized data centers with multi-tenant capabilities.

VXLAN Tunnel End Point (VTEP)

The network entity that serves as the termination point for VXLAN tunnels. It is responsible for encapsulating Layer 2 frames into VXLAN packets for transmission over a Layer 3 network and for decapsulating VXLAN packets back into Layer 2 frames upon receipt.

vSphere, ESXi, and vCenter

vSphere is a virtualization platform released by VMware. ESXi and vCenter are important components of vSphere.

- ESXi is installed on physical servers to virtualize physical IT resources into virtual IT resource pools so that any applications can be virtualized.
- vCenter is a virtualization resource management component for managing ESXi servers. vCenter provides strong and flexible VM management capabilities, simplifying virtual data center management.

Recommended Switches for 2.5.0

Only the supported switches with PicOS 4.7.0E or later installed can be used to deploy physical networks. For more information, see Supported Switches for 2.5.0.

Before deploying physical networks, check which types of switches are recommended to be spine or leaf switches. See the following solutions:

Solution 1
Solution 2

Solution 1

The solution is recommended for most networks:

Table 1. Recommended Solution 1

Role	Application Scenario	Device Model	Port Configuration	Switch ASIC
Spine	100G Interconnect	N8550-32C	32×100G, 2×10G	Trident3
Spine	100G Interconnect	N8560-32C	32×100G	Trident3
Spine	100G Interconnect	N8550-64C	64×100G	Tomahawk2
Leaf	10G Access	N5850-48X6C	48×10G, 6×100G	Trident3
Leaf	10G Access	N5570-48S6C	48×10G, 6×100G	Trident3
Leaf	25G Access	N8550-48B8C	48×25G, 8×100G, 2×10G	Trident3

Solution 2

If you need a higher-speed network, use the following solution:

Table 2. Recommended Solution 2

Role	Application Scenario	Device Model	Port Configuration	Switch ASIC
Spine	400G Interconnect	N9550-32D	32×400G	Tomahawk3
Spine	100G Interconnect	N8550-64C	64×100G	Tomahawk2
Leaf/Spine	100G Access	N8550-32C	32×100G, 2×10G	Trident3
Leaf/Spine	100G Access	N8560-32C	32×100G	Trident3

NOTEs

If you choose other switches in Supported Switches for 2.5.0 as spine and leaf switches, pay attention to the following considerations:

- The switches are recommended to support both EVPN and VXLAN.
- In IDC scenarios, leaf switches need to support EVPN and both Layer 2 and Layer 3 VXLAN, while spine switches need to support at least EVPN.

To view the EVPN and VXLAN support information, see PicOS Supported Features.

Recommended Switches for 2.5.1

Only the supported switches with PicOS 4.7.0E or later installed can be used to deploy physical networks. For more information, see Supported Switches for 2.5.1.

But for switches of the models N5570-48X6C, N5580-32C, N5580-48Y8C, N5680-32D, and N5630-64C, you are recommended to install PicOS 4.7.1E.

Before deploying physical networks, check which types of switches are recommended to be spine or leaf switches. See the following solutions:

Solution 1
Solution 2

Solution 1

The solution is recommended for most networks:

Table 1. Recommended Solution 1

Role	Application Scenario	Device Model	Port Configuration	Switch ASIC
Spine	100G Interconnect	N5580-32C	32×100G, 2×10G	Trident3
		N5630-64C	64×100G	Tomahawk2
		N8550-32C	32×100G, 2×10G	Trident3
		N8550-64C	64×100G	Tomahawk2
		N8560-32C	32×100G	Trident3
Leaf	10G Access	N5850-48X6C	48×10G, 6×100G	Trident3
		N5570-48X6C	48×10G, 6×100G	Trident3
		N5570-48S6C	48×10G, 6×100G	Trident3
	25G Access	N8550-48B8C	48×25G, 8×100G, 2×10G	Trident3

		N5580-48Y8C	48×25G, 8×100G, 2×10G	Trident3

Solution 2

If you need a higher-speed network, use the following solution:

Table 2. Recommended Solution 2

Role	Application Scenario	Device Model	Port Configuration	Switch ASIC
Spine	400G Interconnect	N9550-32D	32×400G	Tomahawk3
		N5680-32D	32×400G	Tomahawk3
	100G Interconnect	N8550-64C	64×100G	Tomahawk2
		N5630-64C	64×100G	Tomahawk2
Leaf/Spine	100G Access	N5580-32C	32×100G, 2×10G	Trident3
		N8550-32C	32×100G, 2×10G	Trident3
		N8560-32C	32×100G	Trident3

NOTEs

If you choose other switches in Supported Switches for 2.5.1 as spine and leaf switches, pay attention to the following considerations:

- The switches are recommended to support both EVPN and VXLAN.
- In IDC scenarios, leaf switches need to support EVPN and both Layer 2 and Layer 3 VXLAN, while spine switches need to support at least EVPN.

To view the EVPN and VXLAN support information, see PicOS Supported Features.

Quick Design Guide

To design a physical network, follow these steps:

Prerequisites

Before you design a fabric, ensure that all the prerequisite tasks in Designing Physical Networks - Prerequisites have been completed. Or else, the fabric deployment will fail.

Designing Procedure

To design and deploy a physical network, follow the steps:

1. Add units to be used in the DC template. See Designing Units.
2. Add a DC template. See Designing DC Templates.
3. Import the DC template to the fabric that you created, and then design and deploy the fabric. See Designing Fabrics.

   After the fabric deployment status becomes **SUCCEED**, the physical network is deployed successfully.

Designing Units

A unit means the minimum networking element for creating a fabric. A unit includes one or multiple leaf switches.

To design a physical network with AmpCon-DC, you must add one or multiple units as needed. These units will be used to design a DC template.

- Prerequisites
- Procedure
- Optional Operations
  - Viewing Units
  - Editing Units
  - Copying Units
  - Deleting Units

Prerequisites

Ensure that you have added IP pools and the IP pools have enough available IP addresses. For more information, see IP Pools.

Procedure

You can add one or multiple leaf switches to the unit. To add a unit, follow these steps:

1. In the AmpCon-DC UI, click **Physical Network > Design > Units** from the navigation bar.
2. Click **+ Unit**.
3. In the **Basic Info** section, enter the unit name and description (optional).
4. In the **Leaf** section, enter the following information:

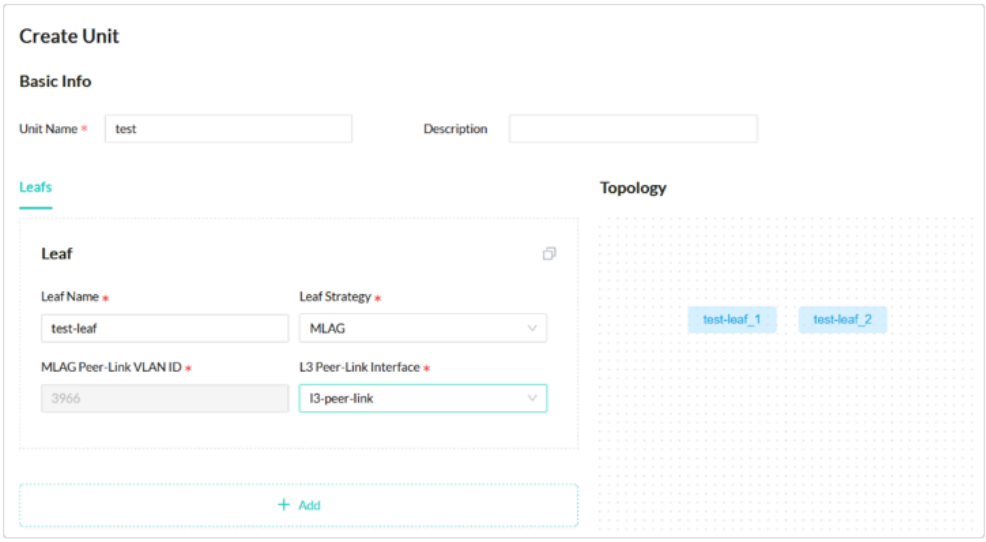


Table 1. Leaf Information

Configuration	Description
Leaf Name	The name used to distinguish the leaf switch.
Leaf Strategy	Select **MLAG** or **None**. The default value is **MLAG**. • **MLAG:** Link Aggregation Group (MLAG) is used between two leaf switches. • **None:** A non-MLAG leaf switch is used.
MLAG Peer-Link VLAN ID	The Virtual Local Area Network (VLAN) identifier assigned to the MLAG peer link. The value is 3966 and can't be changed. **NOTE** This configuration is available only when you select **MLAG** as the leaf strategy.
L3 Peer-Link Interface	The network interface used to establish a peer-to-peer connection between two MLAG peer leaf switches. Select from an IP pool. You can also click **+ Add Pool** to add a new IP pool as needed. **NOTE** This configuration is available only when you select **MLAG** as the leaf strategy.

5. To add another leaf switch, click **+ Add**, and then input information as described in the last step.
6. Click **Apply** to complete the unit design.

Optional Operations

Viewing Units

On the “Units” page, you can see the following information:



Table 2. Unit Metrics

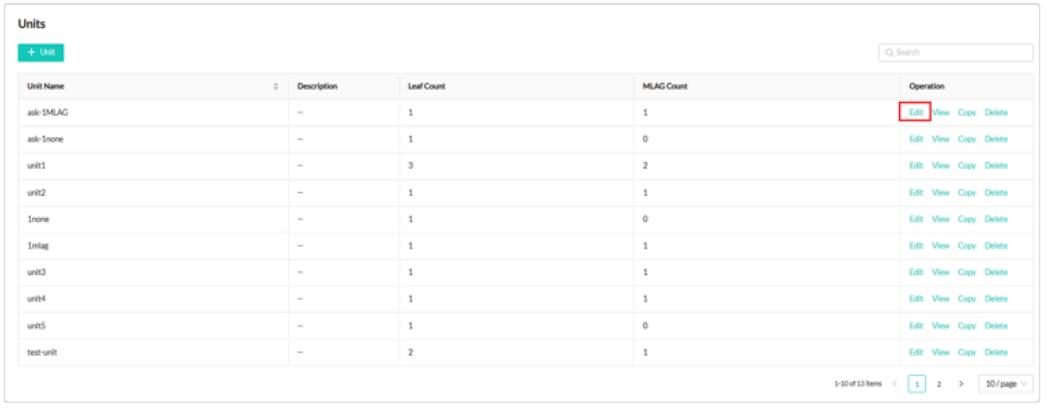
Metric	Description
Unit Name	The name that you specified for the unit
Description	The description of the unit
Leaf Count	The total number of leaf switches in the unit
MLAG Count	The total number of MLAG in the unit

To see more information about the unit, locate the unit, and then click **View**.

Editing Units

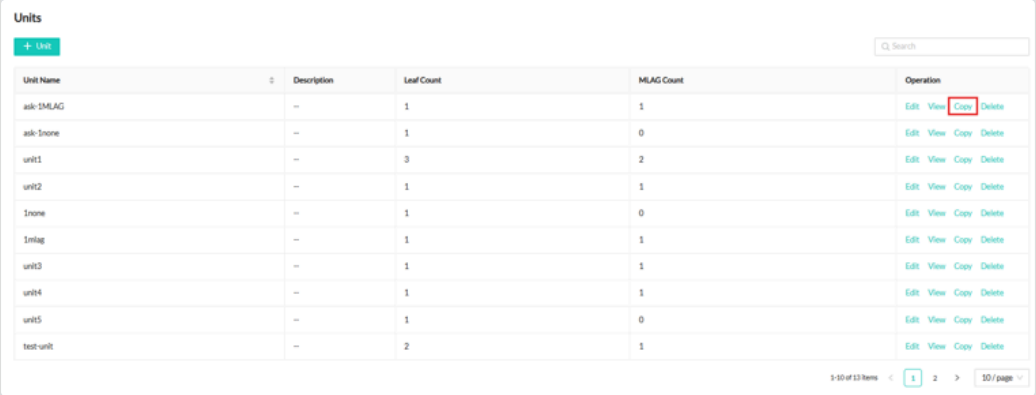
To edit a unit, locate the unit on the “Units” page, and then click **Edit**.

> **NOTE**
>
> After you delete a unit, the fabrics that use this unit are not impacted.



Copying Units

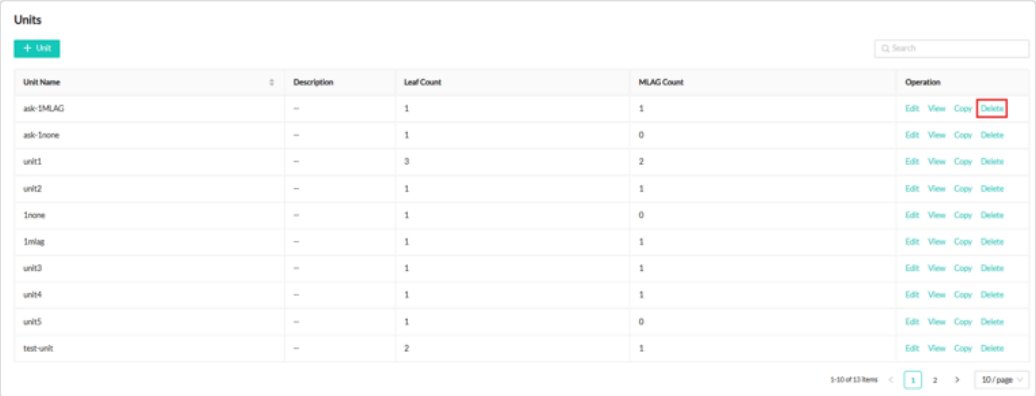
To copy a unit, locate the unit on the “Units” page, and then click **Copy**.



Deleting Units

To delete a unit, locate the unit on the “Units” page, and then click **Delete**.

> **NOTE**
>
> After you delete a unit, the fabrics that use this unit are not impacted.



Designing DC Templates

DC templates are abstractions of network designs that define the structure and protocols of networks, without defining any vendor-specific information.

To design a physical network with AmpCon-DC, you must add the DC template used to design a fabric.

- Prerequisites
- Procedure
- Optional Operations
  - Viewing Templates
  - Editing Templates
  - Copying Templates
  - Deleting Templates

Prerequisites

- You have added IP pools and ASN pools used by the DC template, and these pools have enough available IP addresses and ASNs. For more information, see IP Pools and ASN Pools.
- You have added units used by the DC template. For more information, see Designing Units.

Procedure

You can add one or multiple units to a DC template. To add a DC template, follow these steps:

1. In the AmpCon-DC UI, click **Physical Network > Design > DC Templates** from the navigation bar.
2. Click **+ Template**.
3. In the **Basic Info** section, enter the DC template name and description (optional).

   Currently, AmpCon-DC supports only the 3-stage network architecture. So, here **3-Stage** is selected automatically.
4. In the **Spine Layer** section, specify the count of spine switches in this DC template.

   > **NOTE**
   >
   > Ensure that the count of spine switches does not exceed 128.

5. In the **Unit** section, select a unit from the drop-down list, and specify its count.

   To add more units, click **+**.

   > **NOTE**

Ensure that the total number of leaf switches in all included units does not exceed 128.

6. In the **Underlay** section, select the underlay routing protocol, **BGP** or **OSPF**.

NOTEs

- If **OSPF** is used as the routing protocol, ASN is assigned from the specified **Overlay IBGP ASN** pool in the related DC template. Ensure that the ASN pool has at least one available ASN.
- If **BGP** is used as the routing protocol, ASN is assigned from the specified **EBGP ASN** pool in the related DC template.
  Ensure the available ASN count in the ASN pool is bigger than the required ASN count.
  The required ASN count of the fabric is calculated as follows:
  Required ASN count = leaf count + 1
  Both peer leaf switches in an MLAG setup are considered as one leaf. Each non-MLAG leaf switch is considered as one leaf.

- If you selected **BGP**, enter the following information:

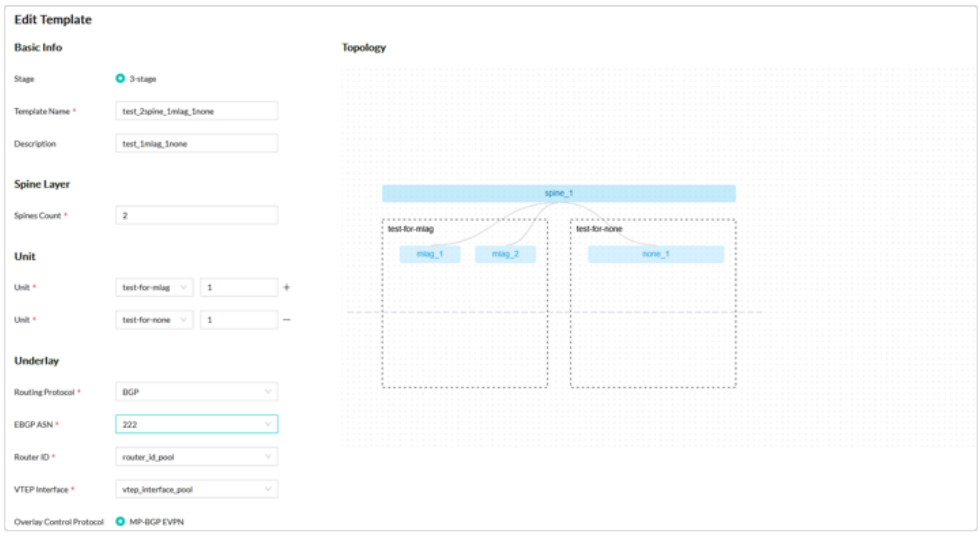


Table 1. BGP Information

Configuration	Description
EBGP ASN	The unique identifier to distinguish an Autonomous System (AS) in EBGP.

	Select an ASN pool. You can also click **+ Add Pool** to add a new ASN pool as needed.
Router ID	The identifier used by the routing protocol BGP to uniquely identify the router. Select an IP pool. You can also click **+ Add Pool** to add a new IP pool as needed.
VTEP Interface	The interface on a VXLAN Tunnel End Point (VTEP) device, through which VXLAN packets are sent and received. Select an IP pool. You can also click **+ Add Pool** to add a new IP pool as needed. • For each leaf switch, the loopback0 address of the switch is used as the router ID, and the loopback1 address of the switch is used as the VTEP interface**.** • The loopback0 addresses on both MLAG peer switches differ and the loopback1 addresses on both MLAG peer switches are the same.
Overlay Control Protocol	**MP-BGP-EVPN** is selected automatically. Currently, only MP-BGP-EVPN is supported as the overlay control protocol.

- If you selected **OSPF**, enter the following information:

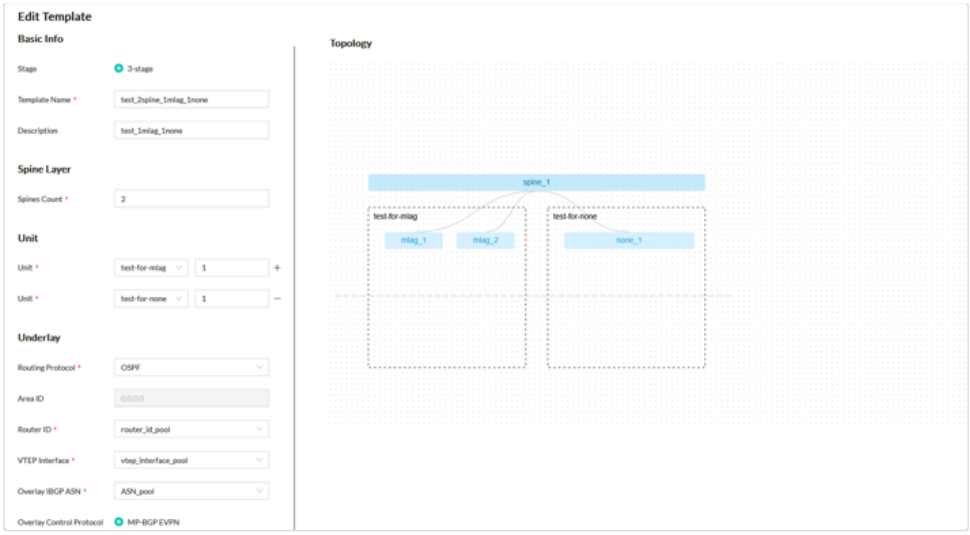


Table 2. OSPF Information

Configuration	Description
Area ID	The identifier to distinguish different areas within an OSPF domain. The value is 0.0.0.0 and can't be changed.
Router ID	The identifier used by the routing protocol OSPF to uniquely identify the router. Select an IP pool. You can also click **+ Add Pool** to add a new IP pool as needed.
VTEP Interface	The interface on a VTEP device, through which VXLAN packets are sent and received. Select an IP pool. You can also click **+ Add Pool** to add a new IP pool as needed. • For each leaf switch, the loopback0 address of the switch is used as the router ID, and the loopback1 address of the switch is used as the VTEP interface**.** • The loopback0 addresses on both MLAG peer switches differ and the loopback1 addresses on both MLAG peer switches are the same.

Overlay IBGP ASN	The unique identifier to distinguish an AS in IBGP. Select an ASN pool. You can also click **+ Add Pool** to add a new ASN pool as needed.
Overlay Control Protocol	**MP-BGP-EVPN** is selected by default. Currently, only MP-BGP-EVPN is supported as the overlay control protocol.

7. Click **Apply** to complete the DC template design.

Optional Operations

Viewing Templates

On the “DC Templates” page, you can see the following information:

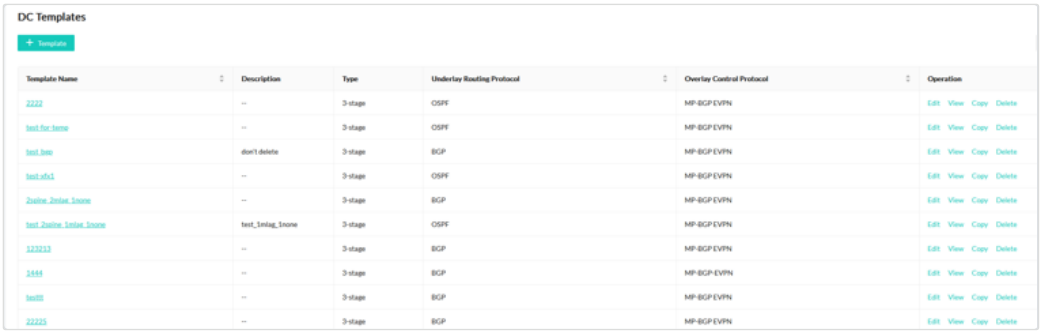


Table 3. DC Template Metrics

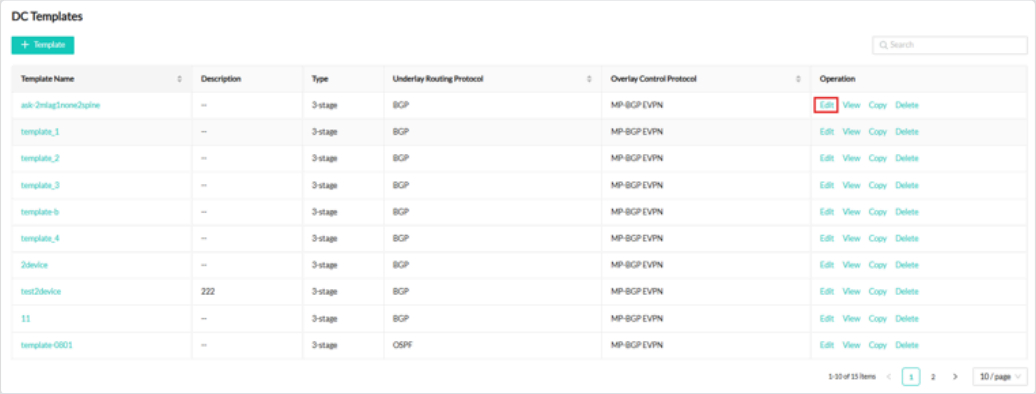
Metric	Description
Template Name	The name that you specified for the DC template.
Description	The description of the DC template.
Type	The type of the network architecture.
Underlay Routing Protocol	The routing protocol used in the underlay network.
Overlay Control Protocol	The protocol used in the overlay network.

To see more information about a template, locate the template, and then click **View**.

Editing Templates

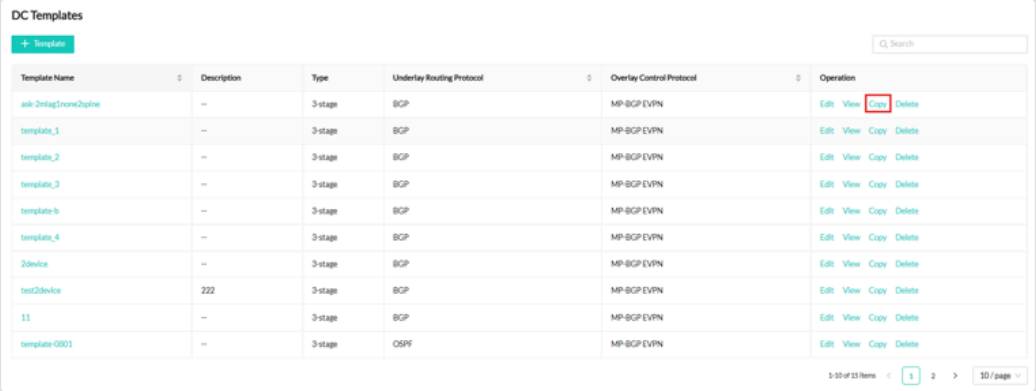
To edit a DC template, locate the template on the “DC Templates” page, and then click **Edit**.

> **NOTE**
>
> After you edit a DC template, the fabrics that use this DC template are not impacted.



Copying Templates

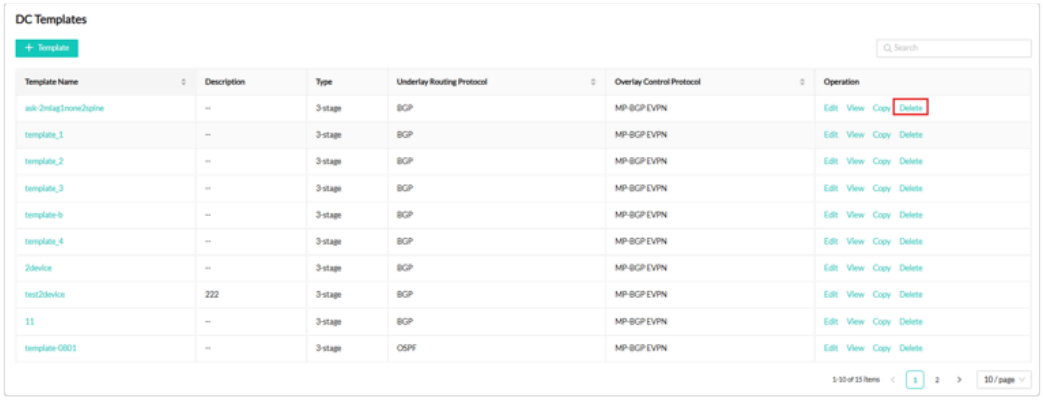
To copy a DC template, locate the template on the “DC Templates” page, and then click **Copy**.



Deleting Templates

To delete a DC template, locate the template on the “DC Templates” page, and then click **Delete**.

> **NOTE**
>
> After you delete a DC template, the fabrics that use this template are not impacted.


DC Templates
+ Template
Search
Template Name
Description
Type
Underlay Routing Protocol
Overlay Control Protocol
Operation
asic-2mlag1none2spine -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template_1 -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template_2 -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template_3 -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template-b -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template_4 -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
2device -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
test2device 222 3-stage BGP MP-BGP EVPN Edit View Copy Delete
11 -- 3-stage BGP MP-BGP EVPN Edit View Copy Delete
template-0801 -- 3-stage OSPF MP-BGP EVPN Edit View Copy Delete
1-10 of 15 items 1 2 10 / page

Designing Fabrics

After you complete the DC template design, you can start to deploy a physical network by designing a fabric.

Import a DC template to a fabric, and then you can design the fabric. AmpCon-DC automatically configures related switches based on fabric configurations to complete the network deployment.

- Before You Begin
- Designing Procedure
  - 1. Allocating Devices
  - 2. Confirming Configurations
    - Resource Pool Assignment Rules
  - 3. Checking Links
  - 4. Deploying the Fabric
- Verifying the Deployment
- Redeploying Fabrics

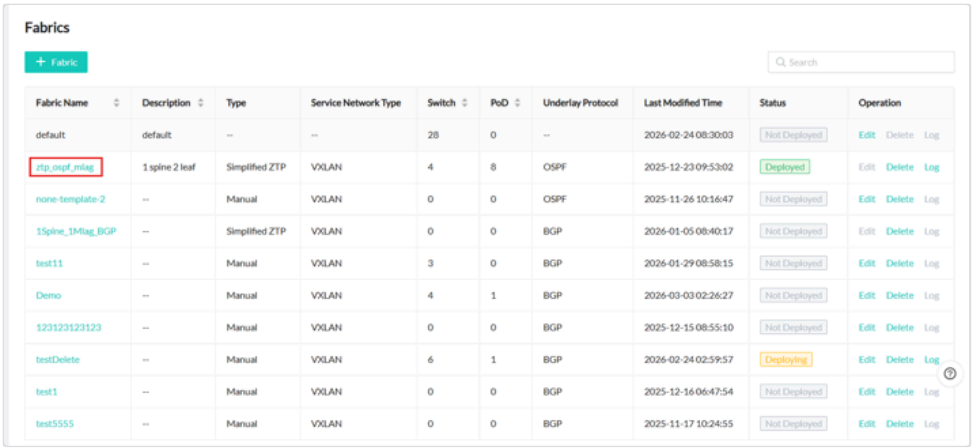
Before You Begin

- Before you design a fabric, ensure that all the prerequisite tasks in Designing Physical Networks - Prerequisites have been completed. Or else, the fabric deployment will fail.
- Ensure that you have designed the DC Template used by the fabric.

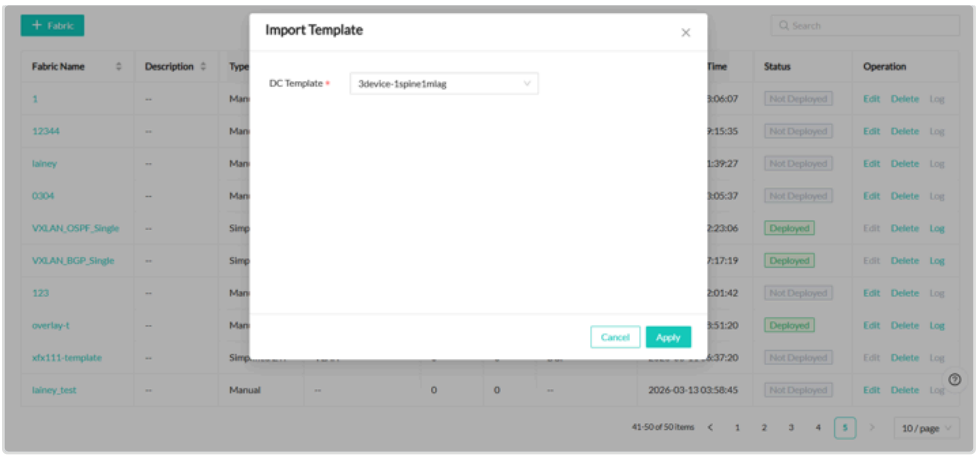
Designing Procedure

To design a fabric, follow the steps:

1. Click **Physical Network > Fabrics** from the navigation bar.
2. Click the name of the fabric that you want to design.



3. In the pop-up window, select a DC template from the drop-down list.



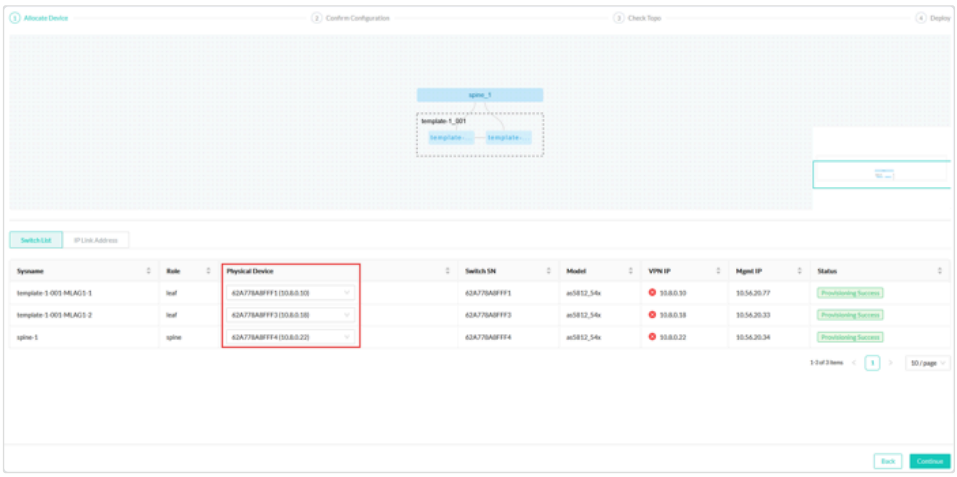
4. Click **Apply** to import the DC template.

You are now redirected to the fabric design page. The fabric design includes the following processes:

1. Allocating Devices

1. Click the **Switch List** tab. In the **Physical Device** drop-down list, select a physical switch for each logical leaf or spine switch.

> **NOTE**
>
> In the **Physical Device** drop-down list, you can select only physical switches that have been added to the fabric and are currently connected to the AmpCon-DC server.



> **Tip**
>
> The following information is generated by AmpCon-DC automatically and can't be changed:

- **Sysname:** The hostname of the switch
- **Role: leaf** or **spine**, which means a leaf switch or spine switch
- **Switch SN:** The serial number of the switch
- **Model:** The model of the switch
- **Mgmt IP:** The management IP address of the switch. **Mgmt IP** is used to connect to AmpCon-DC.
- **VPN IP:** The IP address of the VPN tunnel established between the switch and AmpCon-DC. The following status icons are supported:
  - ✓: The VPN tunnel between the switch and AmpCon-DC is available.
  - x: The VPN tunnel between the switch and AmpCon-DC is unavailable.
- **Status: Imported** or **Deployed**, which means the switch is deployed with AmpCon-DC or imported to AmpCon-DC.

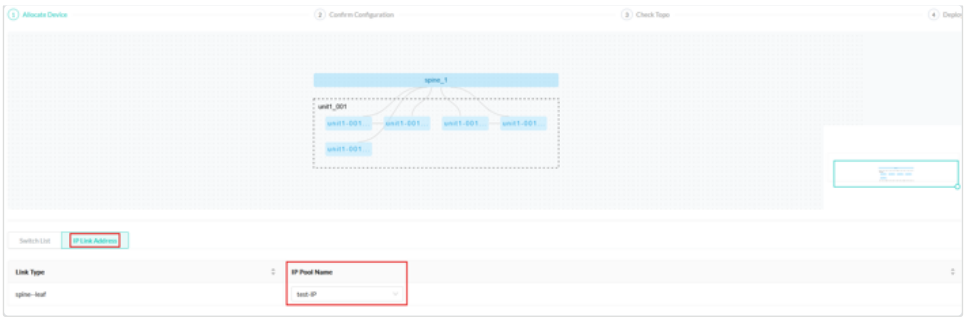
2. In the **Switch List** tab, check the **VPN IP** column, and ensure that all switches are up and connected to the AmpCon-DC server. Or else, the deployment will fail.

- ✓: The switch is up and connected to the AmpCon-DC server.
- x: The switch is down or not connected to the AmpCon-DC server.

3. Click the **IP Link Address** tab, select an IP pool for AmpCon-DC to automatically assign a direct access IP address to each switch.

   By using direct access IP addresses, devices can communicate directly with each other without going through an intermediary device such as a router.

> **NOTE**
>
> The available IP address count in the selected IP pool must be bigger than the required IP address count of the fabric.
>
> The required IP address count of the fabric is calculated as follows:
>
> **Required IP address count = leaf switch count * spine switch count * 2**



4. Click **Continue** to go to the **Confirm Configuration** process.

2. Confirming Configurations

1. Click the **Spine** and **Leaf** tabs, and confirm whether the switch configurations are correct.

> **NOTEs**
>
> - The **Router ID**, **VTEP Interface**, **L3 Peer link**, and **ASN** values are automatically pulled from related IP pools and ASN pools that you specified. For more information, see Resource Pool Assignment Rules and Adding Resource Pools.
> - If the **Router ID**, **VTEP Interface**, **L3 Peer link**, and **ASN** values are blank, the IP pools or ASN pools might have been fully utilized. In this case, modify the units and DC template to select other available IP pools or ASN pools, delete this fabric, and then add a new fabric.

- **Spine** tab

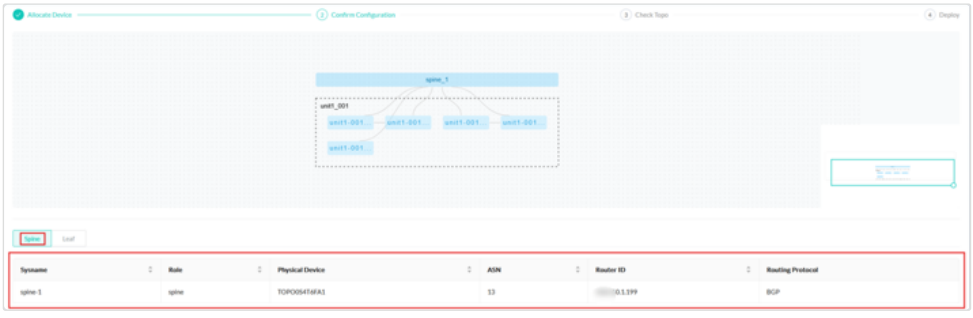


Table 1. Spine Information

Column	Description
Sysname	The hostname of the switch.
Role	**spine**, which means a spine switch.

Physical Device	The physical switch for each spine node.
ASN	The unique identifier to represent an Autonomous System (AS).
Router ID	The identifier used by routing protocols such as OSPF and BGP to uniquely identify the router.
Routing Protocol	The underlay routing protocol, **BGP** or **OSPF**.

- **Leaf** tab

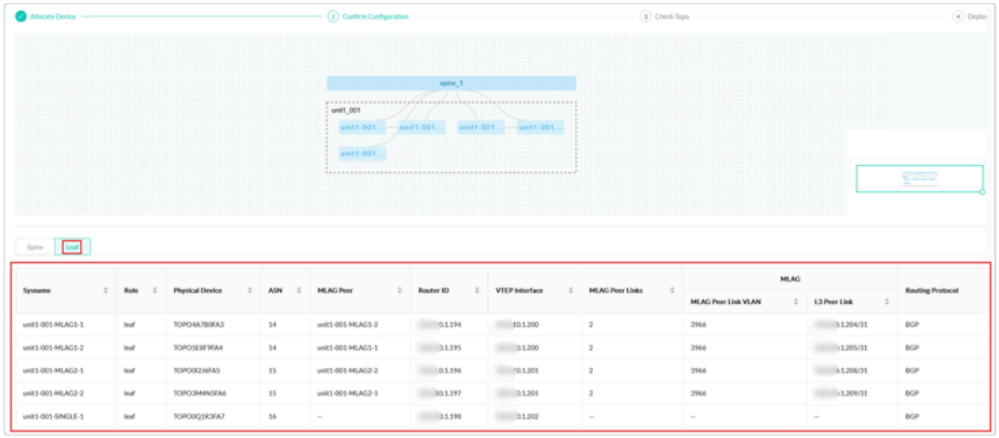


Table 2. Leaf Information

Column	Description
Sysname	The hostname of the switch.
Role	**leaf**, which means a leaf switch.
Physical Device	The physical switch for each leaf node.
ASN	The unique identifier to represent an Autonomous System (AS).
MLAG Peer	The counterpart device in a Multi-Chassis Link Aggregation (MLAG) setup. For non-MLAG leaf switches, the value is --.
Router ID	The identifier used by routing protocols such as OSPF and BGP to uniquely identify the router.

VTEP Interface	The interface on a VXLAN Tunnel End Point (VTEP) device, through which VXLAN packets are sent and received.
MLAG Peer Links	The number of direct connections between the switches participating in an MLAG setup. For non-MLAG leaf switches, the value is --.
MLAG Peer Link VLAN	The value is 3966 and can't be changed. For non-MLAG leaf switches, the value is --.
L3 Peer Link	The network link between two MLAG peers at Layer 3, which is used for synchronizing routing information, exchanging protocol messages, and potentially transmitting data traffic. For non-MLAG leaf switches, the value is --.
Routing Protocol	The underlay routing protocol, **BGP** or **OSPF**.

2. Click **Continue** to go to the **Check Topo** process.

Resource Pool Assignment Rules

You have specified the IP pools and ASN pools in the DC template and unit design processes. After you import the DC template to the fabric, AmpCon-DC assigns information based on specified IP pools and ASN pools for the following columns:

Table 2. Assignment Rules

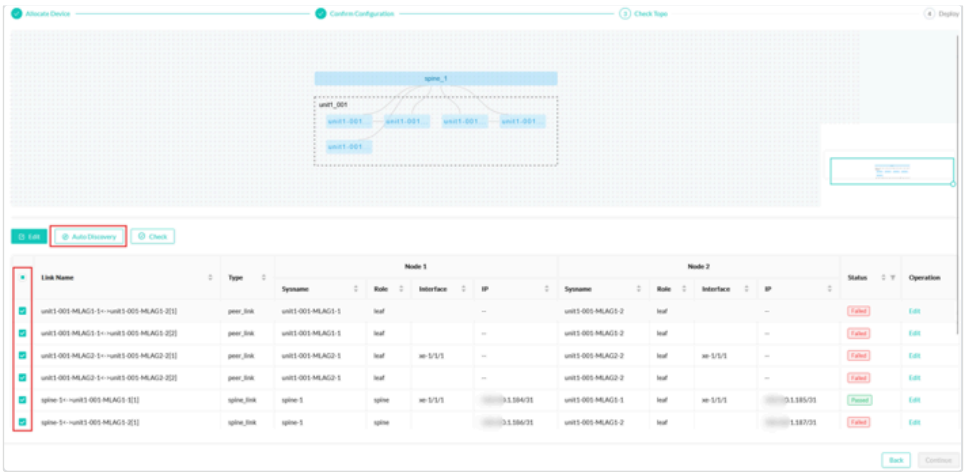
Column	Assignment Rule
Router ID	AmpCon-DC assigns router IDs (loopback0 address) for both spine and leaf switches from the specified **Router ID** IP pool in the related DC template. Each switch has a unique Router ID.
VTEP Interface	AmpCon-DC assigns VTEP interfaces for only leaf switches from the specified **VTEP Interface** IP

	pool in the related DC template. • Each non-MLAG switch has a unique VTEP interface. • Both MLAG peer switches share the same VTEP interface.
L3 Peer Link	AmpCon-DC assigns L3 peer links from the specified **L3 Peer-link Interface** IP pool in the related unit. Only MLAG peer leaf switches have L3 peer links.
ASN	AmpCon-DC assigns ASN for both spine and leaf switches. • If BGP is used as the routing protocol, ASN is assigned from the specified **EBGP ASN** pool in the related DC template. ◦ All spine switches share one ASN. ◦ Peer leaf switches in each MLAG setup share one ASN. ◦ Each non-MLAG leaf switch has a unique ASN. • If OSPF is used as the routing protocol, ASN is assigned from the specified **Overlay IBGP ASN** pool in the related DC template. All spine and leaf switches share one ASN.

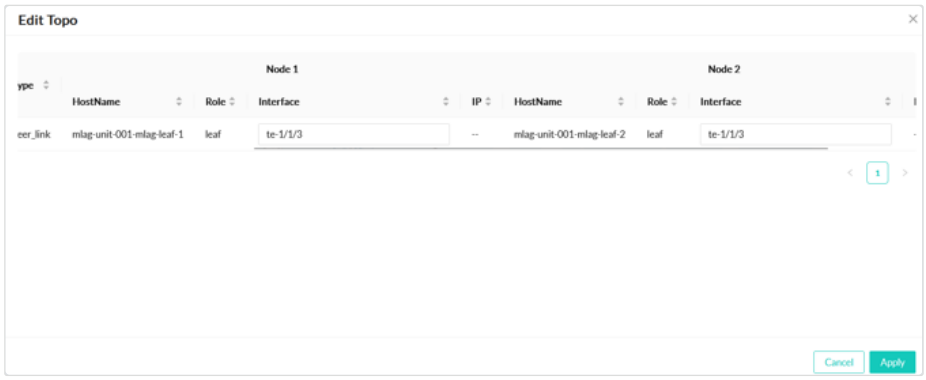
3. Checking Links

1. Click the square before the **Link Name** column heading to select all links, and then click **Auto Discovery** to automatically discover connected switch interfaces in each link.

> **NOTEs**
>
> • If switch interfaces in a link are not connected or not in **Up** status, no values will be displayed in the **Interface** column.
>
> • By design, the IP addresses of MLAG peer leaf switches are not displayed in the **IP** column. You can check their IP addresses in the **L3 Peer Link** column of the **Confirm Configuration** process.



2. Optional: To manually add connected switch interfaces for a link, follow these steps:
   a. Locate the link, and then click **Edit**.
   b. In the **Interface** columns of **Node 1** and **Node 2**, enter the interfaces used to connect these two switch nodes.
   c. Click **Apply**.



3. Click the square before the **Link Name** column heading to select all links, and then click **Check** to check each link status in the **Status** column.

- **Passed** means switches in the link can connect to each other.
- **Failed** means switches in the link can't connect to each other.

> **NOTE**
>
> If a link status is **Failed**, check the physical interfaces and network to ensure that the switches in the link can connect to each other. Only after each link status is **Passed**, can you click **Continue** to go to the **Deploy** process.

7. Click **Continue** to go to the **Deploy** process.

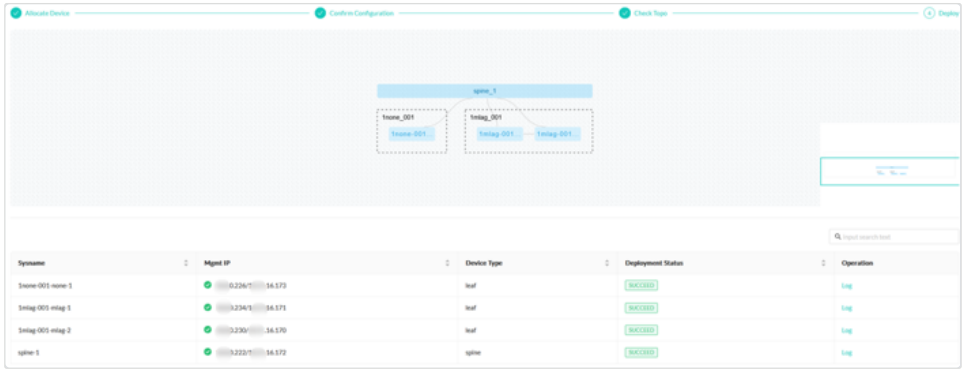
4. Deploying the Fabric

1. In the **Deploy** process, check the **VPN IP** column, and ensure that all switches are up and connected to the AmpCon-DC server. Or else, the deployment will fail.

- ✓: The VPN tunnel between the switch and AmpCon-DC is available.
- x: The VPN tunnel between the switch and AmpCon-DC is unavailable.

2. Click **Apply** to deploy the fabric.

   The configuration pushing process takes some time (depending on the number of switches in the fabric) to complete.



Verifying the Deployment

In the **Deploy** process, 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.

  > **Example:** You might see the error message “Error: Configuration failed on host 10.8.0.186: commit; BGP instance is already running; AS is 111; Commit failed” in the log.
  >
  > This error message means that the BGP local AS has been configured on the switch. You need to log in to the switch and delete these configurations first. Then, click **Apply** in the **Deploy** process to redeploy the fabric.

- If the deployment status of any switch is **PENDING**, the fabric is waiting to be deployed.

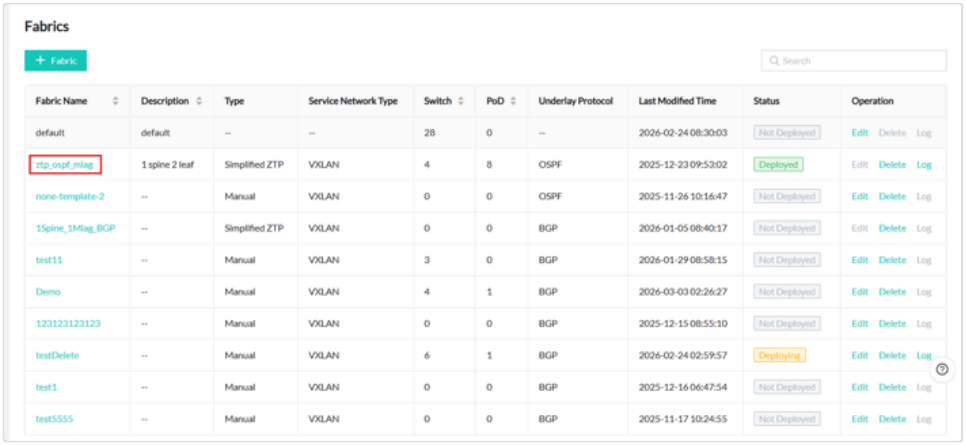
- If the deployment status of any switch is **RUNNING**, the fabric is being deployed.
- If the deployment status of all switches is **SUCCEED**, the fabric deployment is finished. Now your physical network is constructed as designed.

Redeploying Fabrics

If fabric configurations are not pushed to switches due to some reasons, resolve the issues based on deployment logs, and then redeploy the fabric by following these steps:

> **NOTE**
>
> If a designed fabric has been deployed successfully, which means the status of the fabric is **Deployed** on the “Fabrics” page, you can’t redeploy the fabric.

1. On the “Fabrics” page, click the name of the fabric to enter the fabric design page.



2. Optional: Modify the fabric design configurations as needed.
3. Click **Continue** until you go to the **Deploy** process.
4. Check whether all switches in the fabric are in online status, and then click **Apply** to redeploy the fabric.

Managing Fabrics

A fabric is the logical representation of an actual physical network. In AmpCon-DC, you can deploy a physical network by deploying a fabric through simplified ZTP or through physical network design.

You can manage fabrics as follows:

- Adding a Fabric
- Deploying a Fabric
- Viewing All Fabrics
- Adding Switches to a Fabric
  - Adding Switches to a Manual Fabric
  - Adding Switches to a Simplified ZTP Fabric
- Removing Switches from a Fabric
  - Removing Switches from a Manual Fabric
  - Removing Switches from a Simplified ZTP Fabric
- Deleting a Fabric
- Displaying the Topology Associated with a Fabric

Adding a Fabric

AmpCon-DC provides a built-in fabric named **default**. When switches are removed from any other fabrics, these switches will be added to the **default** fabric automatically.

However, the **default** fabric can't be used for physical network design. You can add new fabrics to meet your needs. To add a fabric, follow these steps:

1. In the AmpCon-DC UI, click **Physical Network > Fabrics** from the navigation bar.
2. On the "Fabrics" page, click **+ Fabric**.
3. In the pop-up window, enter the fabric name and description (optional).

   The fabric name needs to be unique and can contain at most 64 characters, including letters, numbers, underscores (_), and hyphens (-).



4. Click **Apply**.

Deploying a Fabric

To deploy a fabric, you are provided with two options:

- **Option 1:** Use simplified ZTP to complete switch onboarding and physical network deployment in one go. For more information, see Simplified ZTP Deployment.
- **Option 2:** Onboard switches through the switch importing or normal ZTP method, and then design physical networks. For more information, see Onboarding Switches and Designing Physical Networks.

Viewing All Fabrics

On the “Fabrics” page, you can see the list of all the added fabrics.

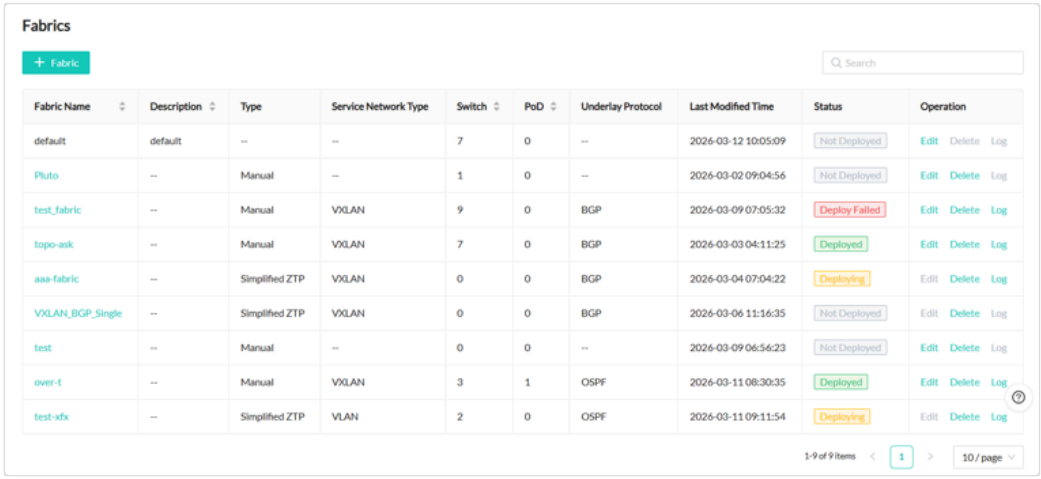


Table 1. Fabric Metrics

Metric	Description
Fabric Name	The name of the fabric.
Description	The description added when you add the fabric.
Type	The fabric type, **Simplified ZTP** or **Manual**. • For a fabric deployed through simplified ZTP, the fabric type is **Simplified ZTP**. • For a fabric manually added as described in the Adding a Fabric section, the fabric type is **Manual**.
Service Network Type	The network type, **VLAN** or **VXLAN**.

Switch	The count of switches added to the fabric.
PoD	The count of PoD added to the fabric.
Underlay Protocol	The routing protocol specified in the DC template or ZTP template of the fabric, **OSPF** or **BGP**. If the fabric is not used for physical network deployment, the value is blank.
Last Modified Time	The last time when you modified the fabric.
Status	The status of the fabric deployment. • For a fabric deployed through simplified ZTP, the status here depends on the status in the **Configuration Preview** tab of the fabric page: ◦ **Deployed:** In the **Configuration Preview** tab, all spine and leaf switches are in **Success** status. ◦ **Deploying:** In the **Configuration Preview** tab, not all switches are in **Pending** status, and not all switches are in **Success** status. ◦ **Not Deployed:** In the **Configuration Preview** tab, all spine and leaf switches are in **Pending** status. • For fabrics deployed through physical network design, the following status is supported: ◦ **Deployed:** You have deployed the fabric successfully. In the **Deploy** section of the fabric page, all switches are in **SUCCEED** status. ◦ **Deploying:** The fabric is being deployed. In the **Deploy** section of the fabric page, some switches are in **RUNNING** and **PENDING** status. ◦ **Deploy Failed:** The fabric fails to be deployed. In the **Deploy** section of the fabric page, some switches are in **FAILED** status.

	◦ **Not Deployed:** The fabric hasn't been deployed. In the **Deploy** section of the fabric page, the switches are in **Pending** status.

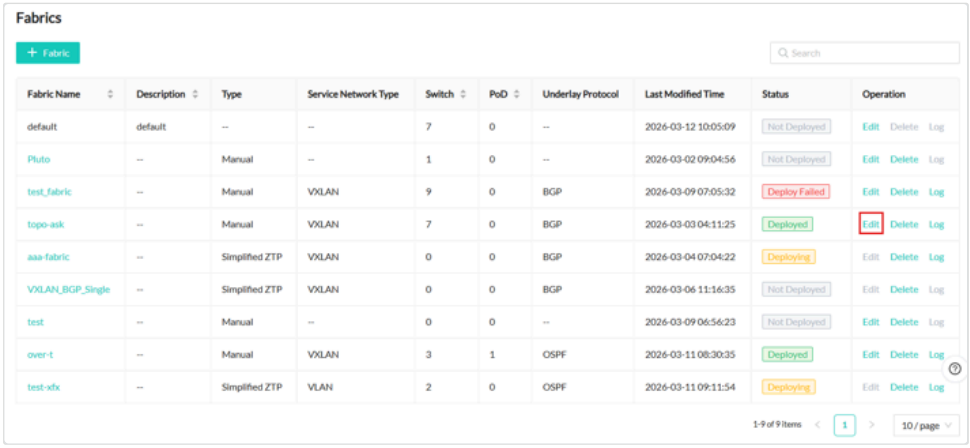
Adding Switches to a Fabric

Adding Switches to a Manual Fabric

To add switches to a fabric in **Manual** type, follow these steps:

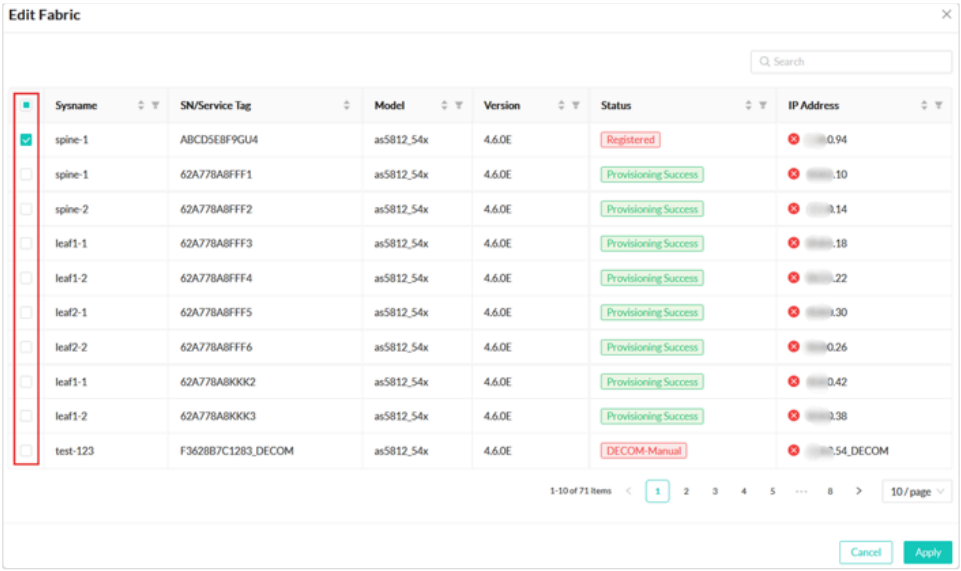
1. On the "Fabrics" page, locate the fabric, and then click **Edit**.

> **NOTE**
>
> The **Edit** button is not available for all fabrics in **Simplified ZTP** type.



2. In the pop-up window, select the switches to be added. You can filter switches by entering keywords in the search box.

> **NOTEs**
>
> - Ensure that the switches to be added are in **Provisioning Success** or **Imported** status, which means the switches have been managed by AmpCon-DC.
> - Ensure that the switches to be added haven't been allocated as spine or leaf switches of any other fabrics.

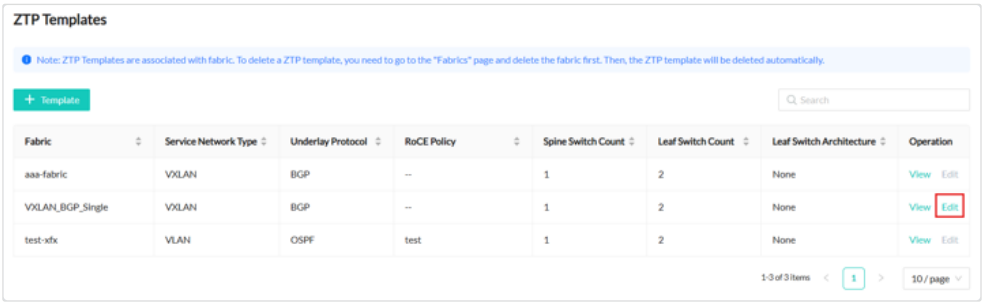


3. Click **Apply**.

Adding Switches to a Simplified ZTP Fabric

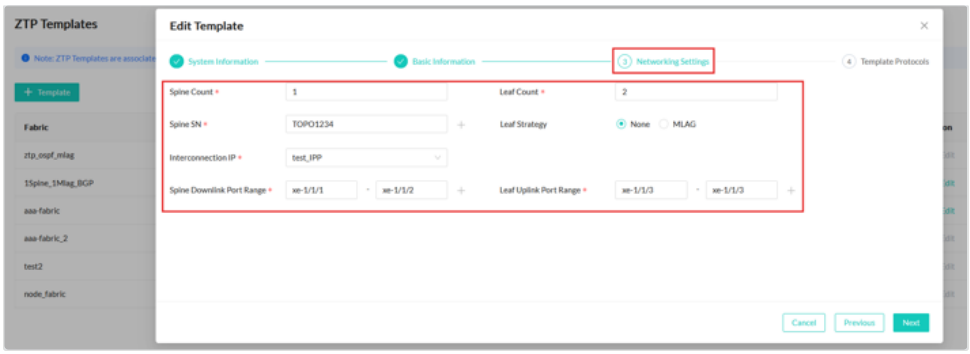
For fabrics in **Simplified ZTP** type, you can add switches to only the fabrics in **Not Deployed** status. Follow these steps:

1. Click **Physical Network > Design > ZTP Templates** from the navigation bar.
2. On the “ZTP Templates” page, locate the ZTP template, and then click **Edit** to edit the ZTP template.



3. In the pop-up window, click **Next** to go to the **Networking Settings** section, where you can increase the spine count and leaf count as needed.

   For more information about ZTP template configurations, see Adding ZTP Templates.



4. Click **Next**, and then click **Preview**.

Then, the ZTP template and the fabric page will be updated. You can continue the simplified ZTP process to complete the fabric deployment. For more information, see Deploying through Simplified ZTP.

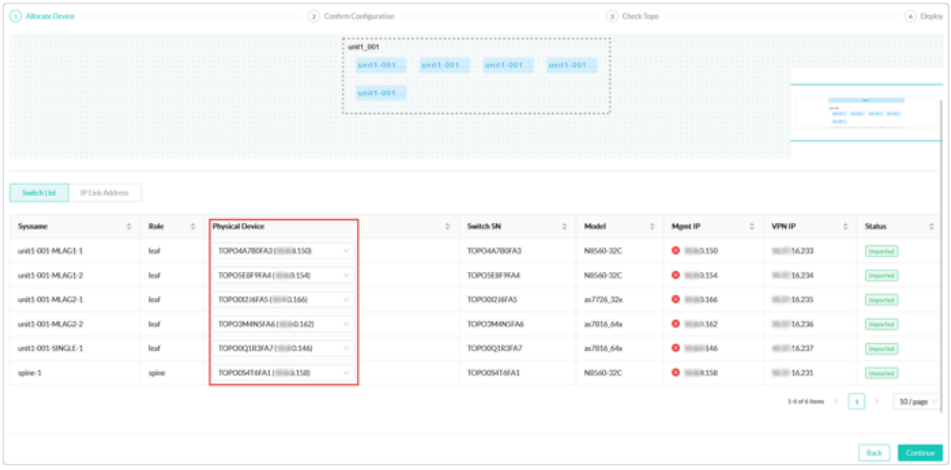
Removing Switches from a Fabric

After you remove switches from a non-default fabric, these switches are added to the **default** fabric automatically. To remove switches from the **default** fabric, add the switches to other fabrics.

Removing Switches from a Manual Fabric

To remove switches from a fabric in **Manual** type, follow these steps:

1. Click **Physical Network > Fabrics** from the navigation bar. On the “Fabrics” page, click the fabric name to go to the fabric configuration page.
2. On the **Physical Device** drop-down list of the fabric configuration page, check whether the switches to be removed have been assigned as leaf or spine switches.



3. If the switches to be removed have been assigned as leaf or spine switches, use either of the following ways:

- Use the Returning Merchandise Authorization (RMA) feature to replace these switches with other switches of the same switch model first. For more information, see Returning Merchandise Authorization for Switches.

  Then, go to the “Fabrics” page, locate the fabric, and then click **Edit**. In the pop-up window, unselect the switches to be removed, and click **Apply**.

  > **NOTE**
  >
  > After the RMA process, the new switch will replace the old switch in the physical network. The underlay configurations will be automatically pushed to the new switch, and thus you don’t need to re-deploy the physical network in the AmpCon-DC UI.
  >
  > However, you must complete physical connections for the new switch based on the topology and link information on the fabric page. For more information, see Deploying Physical Networks.

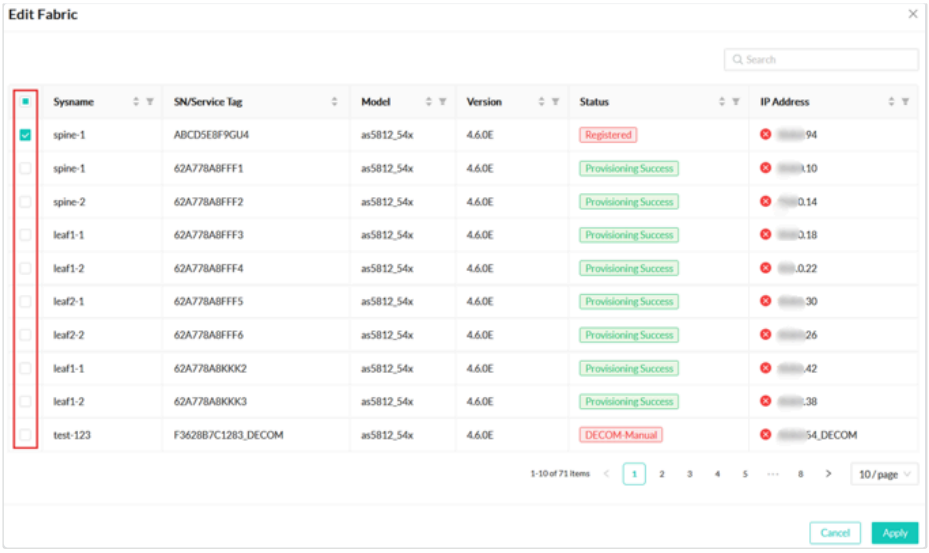
- Assign other switches as leaf or spine switches to replace the switches to be removed first, and then remove the switches from the fabric. Follow these steps:

  a. Add other switches to the fabric. For more information, see Adding Switches to a Manual Fabric.

  b. Go back the fabric page, in the **Physical Device** drop-down list, select new switches to replace the switches to be removed.

  > **NOTE**
  >
  > To make the fabric work, you need to redeploy the fabric. For more information, see Redeploying Fabrics.

  c. Go to the “Fabrics” page, locate the fabric, and then click **Edit**. In the pop-up window, unselect the switches to be removed, and click **Apply**.



4. If the switches to be removed haven't been assigned as leaf or spine switches, go to the "Fabrics" page, locate the fabric, and then click **Edit**.

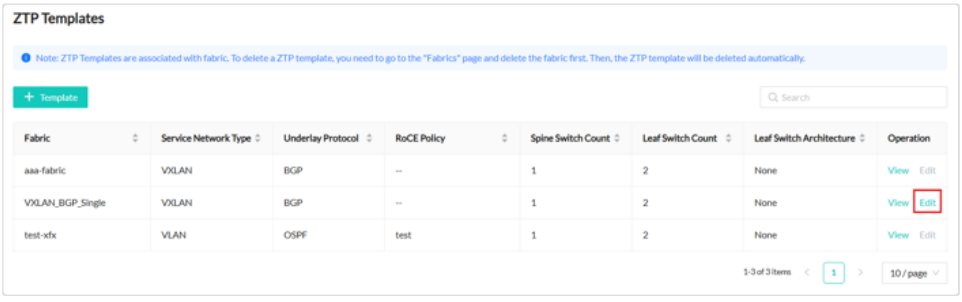
   In the pop-up window, unselect the switches to be removed, and click **Apply**.

Removing Switches from a Simplified ZTP Fabric

- To remove switches from a fabric in **Simplified ZTP** type and in **Not Deployed** status, follow these steps:

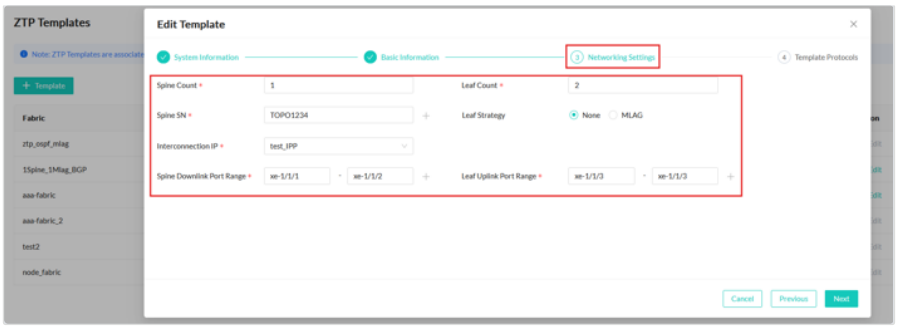
  a. Click **Physical Network > Design > ZTP Templates** from the navigation bar.

  b. On the "ZTP Templates" page, locate the ZTP template, and then click **Edit** to edit the ZTP template.



   c. In the pop-up window, click **Next** to go to the **Networking Settings** section, where you can decrease the spine count and leaf count as needed.

   For more information about ZTP template configurations, see Adding ZTP Templates.



d. Click **Next**, and then click **Preview**.

Then, the ZTP template and the fabric page will be updated. You can continue the simplified ZTP process to complete the fabric deployment. For more information, see Deploying through Simplified ZTP.

- To remove switches from a fabric in **Simplified ZTP** type and in **Deployed** or **Deploying** status, use the Returning Merchandise Authorization (RMA) feature to replace switches with new switches of the same switch model. For more information, see Returning Merchandise Authorization for Switches.

> **NOTE**
>
> After the RMA process, the new switch will replace the old switch in the physical network. The underlay configurations will be automatically pushed to the new switch, and thus you don't need to re-deploy the physical network in the AmpCon-DC UI.
>
> However, you must complete physical connections for the new switch based on the topology and link information on the fabric page. For more information, see Deploying Physical Networks.

Deleting a Fabric

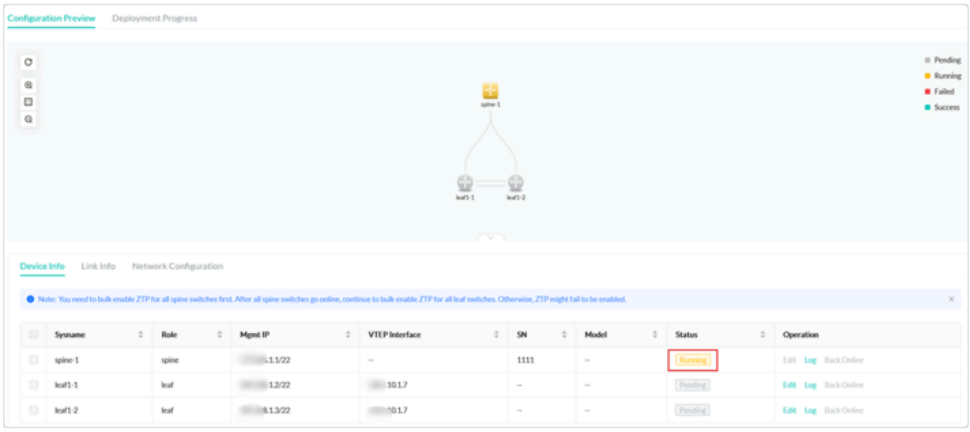
To delete a fabric, follow these steps:

> **NOTEs**
>
> - The **default** fabric is a built-in fabric that is automatically created by AmpCon-DC and can't be deleted.
> - Deleting a fabric will lead to the following results:
>   - All underlying configurations of the switches in this fabric are deleted permanently and can't be recovered. If the switches in a fabric are

not connected to the AmpCon-DC server, the underlay configurations will fail to be deleted.
    - The switches in the fabric are assigned to the **default** fabric.
    - The assigned IP addresses and ASNs are released.
    - For fabrics in **Simplified ZTP** type, after you delete a fabric, the related ZTP template will also be deleted automatically.

1. If the fabric is used for physical network deployment, click **Physical Network > Fabrics** from the navigation bar to go to the “Fabrics” page.

- If the fabric is in **Simplified ZTP** type, click the fabric name to go to the fabric page, and then check the **Configuration Preview** tab to see whether any switch status is **Running**. Wait for the **Running** status to change to **Success** or **Failed**.



- If the fabric is in **Manual** type, check whether the fabric status is **Deploying** on the “Fabrics” page. Wait for the **Deploying** status to change to **Deployed** or **Deploy Failed**.

2. If the fabric is used for overlay service provisioning, delete the following resources associated to the fabric:

Table 2. Resources to Be Deleted

Resource	Reference Link
1. Delete all logical routers bound to the fabric.	Deleting a Logical Router
2. Delete all logical switches bound to the fabric.	Deleting a Logical Switch
3. Delete virtual networks of all PoD bound to the fabric.	Deleting a Virtual Network

4. Delete all bare metal VL2 bound to the fabric.	Deleting a VL2
5. Delete all bare metal node groups and vSphere and node uplink configurations for all PoD bound to the fabric.	Deleting a Node Group Deleting Node Uplink
6. Delete all VLAN Domains bound to the fabric.	Deleting a VLAN Domain Group
7. Delete all PoD bound to the fabric.	Deleting a vSphere PoD Deleting an OpenStack PoD Deleting a Bare Metal PoD

3. On the “Fabrics” page, locate the fabric, and then click **Delete**.

   In the pop-up window, select the square before “Continue to delete the fabric?”, and then click **Yes** to confirm the deletion.

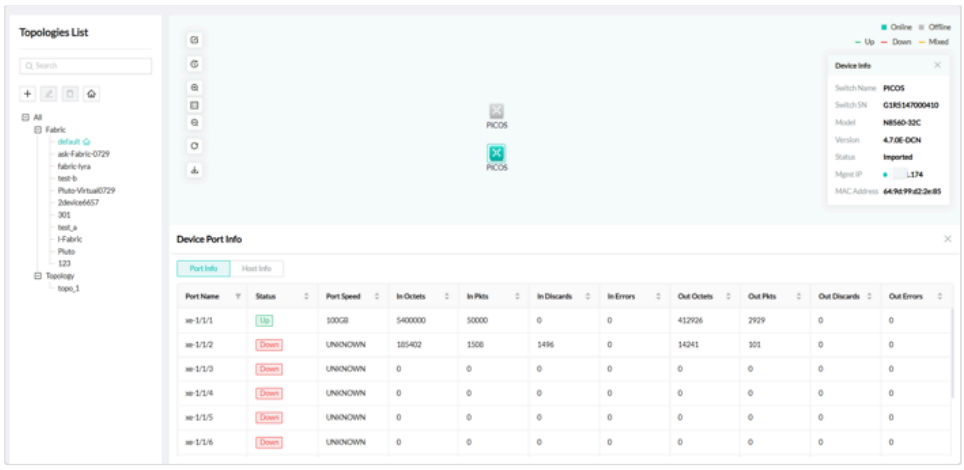


Displaying the Topology Associated with a Fabric

To display the topology associated with a fabric, follow these steps:

1. Click **Physical Network > Topologies** from the navigation bar.
2. In the **Fabric** list, click the corresponding fabric name.

   Then, you can see the topology graph of the switches that belong to this fabric. For more information, see Topology.


Topologies List
Search
All
Fabric
default
ask-Fabric-0729
fabric-tyra
test-b
Pluto-Virtual0729
2device6657
301
test_a
I-Fabric
Pluto
123
Topology
topo_1
Online
Offline
Up
Down
Mixed
PICOS
PICOS
Device Info
Switch Name PICOS
Switch SN G1R5147000410
Model N8560-32C
Version 4.7.0E-DCN
Status Imported
Mgmt IP .174
MAC Address 64:9d:99:d2:2e:85
Device Port Info
Port Info
Host Info
Port Name
Status
Port Speed
In Octets
In Pkts
In Discards
In Errors
Out Octets
Out Pkts
Out Discards
Out Errors
xe-1/1/1 Up 100GB 5400000 50000 0 0 412926 2929 0 0
xe-1/1/2 Down UNKNOWN 185402 1508 1496 0 14241 101 0 0
xe-1/1/3 Down UNKNOWN 0 0 0 0 0 0 0 0
xe-1/1/4 Down UNKNOWN 0 0 0 0 0 0 0 0
xe-1/1/5 Down UNKNOWN 0 0 0 0 0 0 0 0
xe-1/1/6 Down UNKNOWN 0 0 0 0 0 0 0 0

Simplified ZTP Deployment

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

Simplified ZTP is a Zero Touch Provisioning (ZTP) method used to onboard switches, deploy physical networks, and configure RoCE (optional) in one go.

The simplified ZTP process can achieve the following goals in one go:

- A physical network (fabric) is deployed automatically.
- All switches in the fabric are bulk onboarded to AmpCon-DC. You don't need to onboard each switch one by one.
- Optional: The RoCE policy configurations are applied to the switches in the fabric.

See the following child topics:

- Quick Deployment Guide for Simplified ZTP
- Preparing for Simplified ZTP
- Deploying through Simplified ZTP
- Post-Deployment Operations
- Troubleshooting Simplified ZTP

NOTEs

- For architecture of the physical network, see Simplified ZTP Architecture.
- If you don't need to deploy physical networks, or if you want to design physical networks manually, do not use simplified ZTP.
- Simplified ZTP can be used only for switches with PicOS installed. For example, white-box switches with PicOS installed and integrated hardware and software PicOS switches.

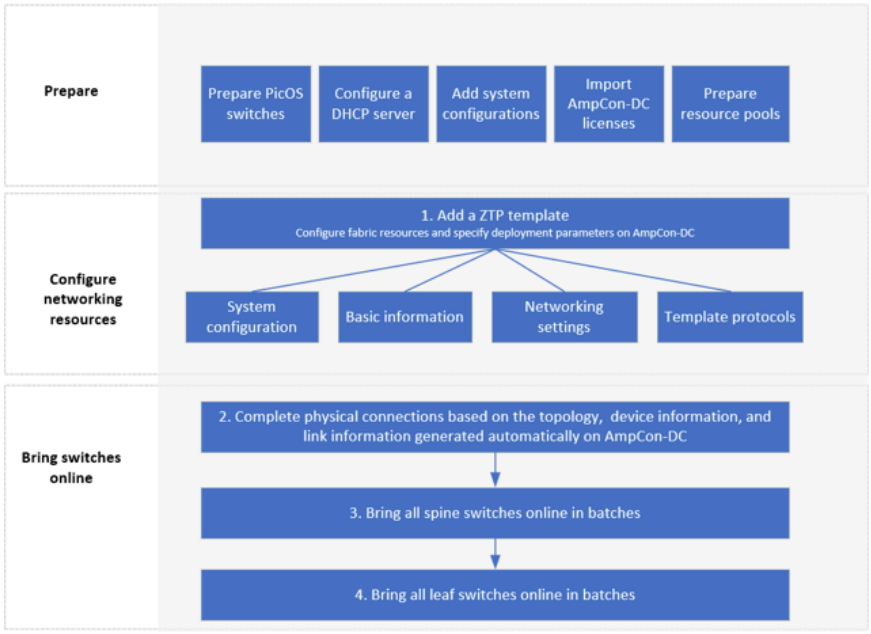
Quick Deployment Guide for Simplified ZTP

To onboard switches, deploy physical networks, and configure RoCE (optional) through simplified ZTP, follow these steps:

Deployment Procedure

To use simplified ZTP, see the following workflow diagram:

Figure 1. Simplified ZTP Workflow



For detailed steps, see the following documents:

1. Preparing for Simplified ZTP.
2. Deploying through Simplified ZTP.

Preparing for Simplified ZTP

Before you start the simplified ZTP deployment, you must complete all the following preparations:

1. Preparing PicOS Switches
2. Configuring a DHCP Server
3. Adding System Configurations
4. Importing AmpCon-DC Licenses
5. Preparing Resource Pools

1. Preparing PicOS Switches

Before you start the simplified ZTP deployment, complete the following preparations on the switches:

1. Ensure that the switches are supported by AmpCon-DC. For more information, see Supported Switches for 2.5.0 and Supported Switches for 2.5.1.

   You also need to check which types of switches are recommended to be spine or leaf switches. For more information, see Recommended Switches for 2.5.0 and Recommended Switches for 2.5.1.

   If you want to configure RoCE during the simplified ZTP process, ensure that the switches to be configured support RoCE (PFC, ECN, and QoS). For more information, see PICOS Supported Features.

2. Ensure that the switches have PicOS installed. This is because simplified ZTP can be used for only the switches with PicOS installed.
3. Ensure that all the switches to be deployed are up and unconfigured.

   > **NOTE**
   >
   > If any switch has been configured, log in to the switch, run the command **rollback default** to clear configurations, and then reboot the switch.

4. You're recommended to contact with the FS sale team to purchase PicOS licenses for the switches to be deployed, and install PicOS licenses on these switches.

   > **NOTE**

For a PicOS switch without a PicOS license, only 4 switch ports are allowed to be used. The simplified ZTP deployment will fail when no available ports can be used.

5. Ensure that the Secure Shell (SSH) protocol is enabled on the switches.

> **NOTE**
>
> SSH is enabled on switches by default.

6. If a firewall is configured between AmpCon-DC and the switches, allow outbound access on the following ports to the management port of each switch:

Table 1. Network Requirements for Switches

TCP/UDP	Port
TCP	22
TCP	9339
TCP	830

2. Configuring a DHCP Server

Simplified ZTP relies on DHCP. Before you start the simplified ZTP deployment, you must configure the DHCP server as follows:

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

- For white-box switches, add the following configurations for each switch:

```
host 4610_54t_02 {
hardware ethernet C4:39:3A:FF:2C:C0;
fixed-address 10.10.51.198;
option default-url "http://10.56.20.184/onie";
}
```

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

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

Replace “10.56.20.184” with the IP address of the AmpCon-DC server.

> **NOTEs**

- Ensure that the DHCP IP address is able to connect to the IP address of the AmpCon-DC server.
- The following DHCP option is used：
  - Option default-url: 114

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

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

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

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

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

NOTEs

- Ensure that the DHCP IP address is able to connect to the IP address of the AmpCon-DC server.
- The following DHCP options are used：
  - Option bootfile-name: 67
  - Option tftp-server-name: 66

3. Reboot these switches configured in the DHCP configuration file.
4. Click **Device > Switches** from the navigation bar. On the “Switches” page, click **Parking Lot**. In the pop-up window, check whether these switches are displayed in the AmpCon-DC parking lot. For more information about the parking lot, see Managing the Parking Lot.

NOTE

Only after you configure the DHCP server and reboot the switches, can these switches go to the parking lot.

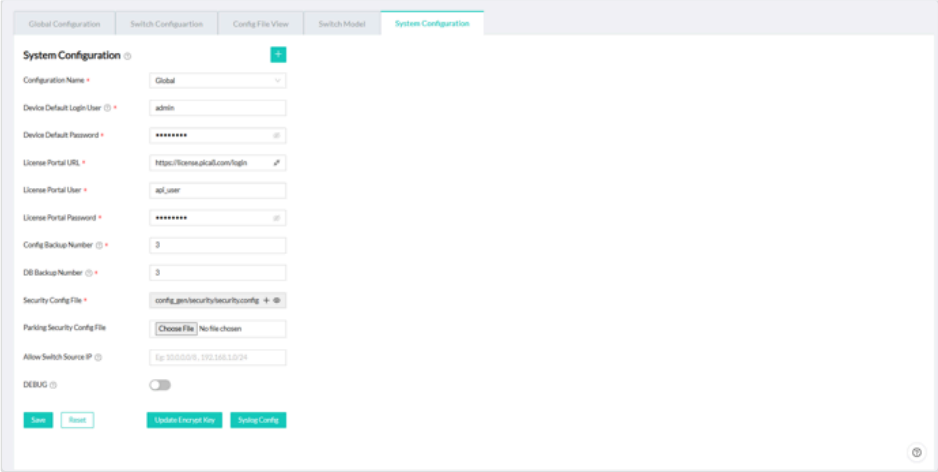
3. Adding System Configurations

System configurations contain important information used for the simplified ZTP deployment. If a system configuration is not configured correctly, the switches related to the system configuration will fail to be deployed.

To add system configurations, follow these steps:

1. Log in to the AmpCon-DC UI with a user of the **SuperAdmin** role. For more information about user roles, see Managing User Access.
2. Click **Device > Device Profiles** from the navigation bar.
3. Click the **System Configuration** tab, and then configure global or non-global system configurations as needed. For more information, see Adding System Configurations.

> **NOTE**
>
> Pay attention to the following points. Or else, the simplified ZTP deployment will fail.
>
> - Ensure that the **Device Default Login User** and **Device Default Password** on the “System Configuration” page are correct and can be used to log in to the switches to be deployed.
> - If some switches to be deployed don’t use the **Device Default Login User** and **Device Default Password** entered in the global system configuration, create non-global system configurations for these switches, and ensure the **Device Default Login User** and **Device Default Password** match these switches.
> - Ensure to check whether AmpCon-DC can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see Checking License Portal Connectivity.
> - Ensure that the uploaded **Security Config File** and **Parking Security Config File** don’t contain wrong configurations.



4. In system configurations, the default switch username is **admin**, and the default password is **pica8**. To change the default password, see Changing the Default Switch Password.

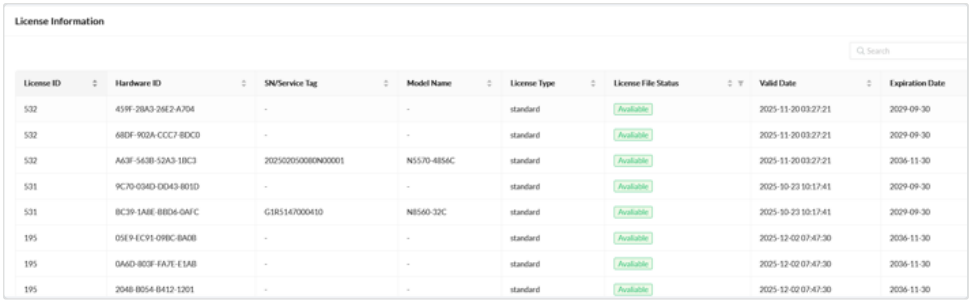
> **NOTE**
>
> Pay attention to the notes in Changing the Default Switch Password. If the default password is not changed correctly, the simplified ZTP deployment will fail.

4. Importing AmpCon-DC Licenses

Import AmpCon-DC licenses containing the switches to be deployed. Follow these steps:

1. Click **System > Software Licenses > License View** from the navigation bar. In the **License Information** section, check whether the hardware IDs of the switches to be deployed are included in any imported AmpCon-DC licenses.

   For more information, see Viewing AmpCon-DC Licenses.



2. If the hardware IDs of the switches are not included in any imported AmpCon-DC licenses, import an AmpCon-DC license to AmpCon-DC. Or else, the switches can't be deployed successfully. For more information, see Importing Licenses for Deployed Switches.

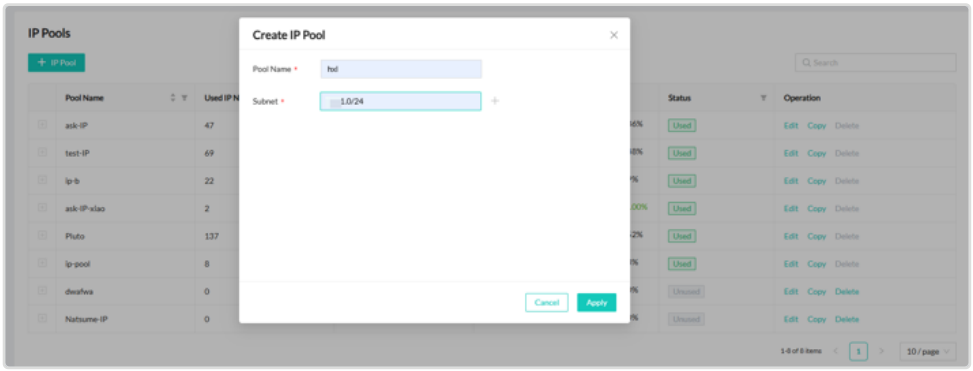
> **NOTE**

Before you import AmpCon-DC licenses, ensure that the switches have been in the parking lot. For more information, see Managing the Parking Lot.

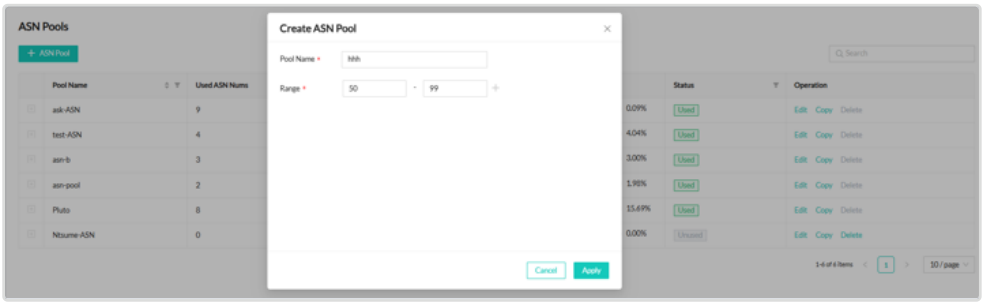
5. Preparing Resource Pools

The IP pools and ASN pools are used for automatic assignment of ASNs and IP addresses during the simplified ZTP process. Prepare enough IP pools and ASNs used for simplified ZTP.

1. Click **Resource > Pools > IP Pools** from the navigation bar, and then click **+ IP Pool** to add the IP pools used for simplified ZTP. For more information, see IP Pools.



2. Click **Resource > Pools > ASN Pools** from the navigation bar, and then click **+ ASN Pool** to add the ASN pools used for simplified ZTP. For more information, see ASN Pools.



Deploying through Simplified ZTP

After you complete all the preparations described in Preparing for Simplified ZTP, start the simplified ZTP deployment by following the instructions in this document.

Before You Begin
Procedure
1. Adding ZTP Templates
2. Completing Physical Connections
3. Bringing All Spine Switches Online
4. Bringing All Leaf Switches Online
What to Do Next

Before You Begin

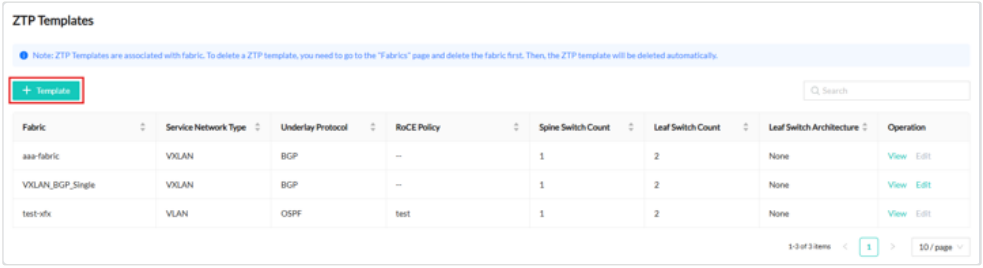
Before you start the simplified ZTP deployment, ensure that you have completed all the preparations described in Preparing for Simplified ZTP. Or else, the simplified ZTP deployment will fail.

Procedure

1. Adding ZTP Templates

AmpCon-DC automatically deploys the switches and physical network based on the added ZTP template. To add a ZTP template, follow these steps:

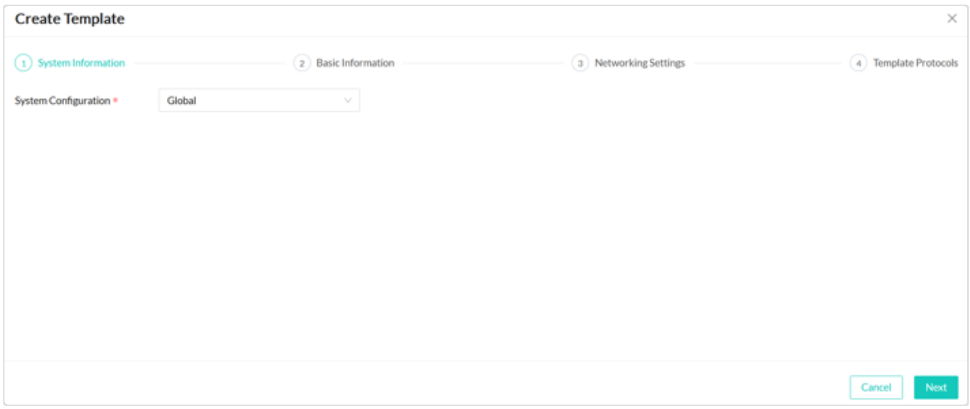
1. Click **Physical Network > Design > ZTP Templates** from the navigation bar.
2. On the “ZTP Templates” page, click **+ Template**.



3. In the pop-up window, select a system configuration from the **System Configuration** drop-down list.

> **NOTE**
>
> Ensure that the system configuration has been configured correctly and matches the switches to be deployed. Or else, the simplified ZTP deployment will fail.

For more information, see Adding System Configurations.



4. Click **Next** to go to the **Basic Information** section. In this section, input the following information:

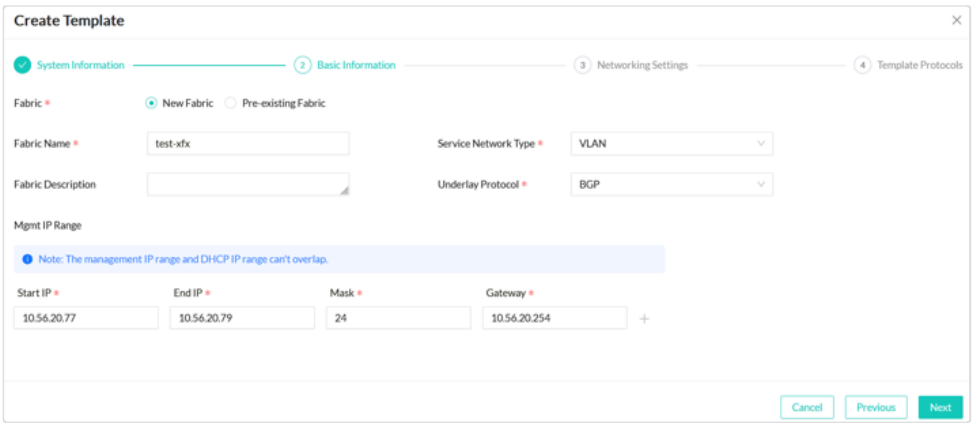


Table 1. Basic Information Parameters

Parameter	Description
Fabric	Select **New Fabric** or **Pre-existing Fabric**. A fabric is a logical representation of an actual physical network. You can deploy a physical network by deploying a fabric in the AmpCon-DC UI.
Fabric Name	The name of the fabric to which the ZTP template is associated. • If you select **New Fabric**, enter a new fabric name. • If you select **Pre-existing Fabric**, select an existing fabric name from the drop-down list.

	Only the fabrics that are previously added and not associated with any DC templates and ZTP templates can be displayed in the drop-down list. **NOTEs** • The fabric name needs to be unique. • The fabric name can contain at most 64 characters. • The fabric name can contain only letters, numbers, underscores (_), and hyphens(-).
Service Network Type	The network type. Values can be **VLAN** or **VXLAN**. **NOTE** If you want to configure a RoCE policy in the simplified ZTP process, you must select **VLAN**.
Fabric Description	Optional. The description of the new fabric. **NOTEs** • This field is displayed only when **New Fabric** is selected in the **Fabric** drop-down list. • The fabric description can contain at most 256 characters.
VXLAN Gateway Type	The type of the VXLAN gateway. Currently, only **Distributed Gateway** can be selected. **NOTE** This field is available only when you select **VXLAN** in the **Service Network Type** field.

Underlay Protocol	The underlay routing protocol. Values can be **BGP** or **OSPF**. By default, **BGP** is selected. The underlay routing protocol is used to implement Layer 3 interconnection between spine switches and leaf switches.
Mgmt IP Range	Specify one or multiple management IP ranges containing the following information: • **Start IP:** The start IPv4 address of the management IP range. Management IP ranges are used for assignment of switch management IP addresses. • **End IP:** The end IPv4 address of the management IP range. ◦ The **Start IP** and **End IP** of a management IP range must be in the same subnet. ◦ The **End IP** needs to be greater than the **Start IP**. • **Mask:** The mask of the management IP range. The value needs to range from 1 to 30. • **Gateway:** The gateway of the management IP range. ◦ The value needs to be in IPv4 format and in the same subnet as the **Start IP** and **End IP**. ◦ Ensure that the IP address of the gateway is able to connect to the IP address of the AmpCon-DC server. To add multiple management IP ranges, click **+**. If multiple management IP ranges are added, to remove a management IP range, click **-**. **NOTEs** • Ensure that each IP address in the management IP ranges is not occupied

	and able to connect to the IP address of the AmpCon-DC server. • Each added management IP range can't overlap with each other. • The total number of IP addresses in all the added management IP ranges must be equal to or larger than the count of leaf switches and spine switches in this fabric. • The added management IP ranges can't overlap with the following IP addresses: ◦ The DHCP IP addresses assigned in the DHCP configuration file. For more information, see Configuring a DHCP Server. ◦ The management IP addresses in the management IP ranges of other ZTP templates. ◦ The management IP addresses of the switches having been managed by AmpCon-DC.

5. Click **Next** to go to the **Network Settings** section. In this section, input the following information:

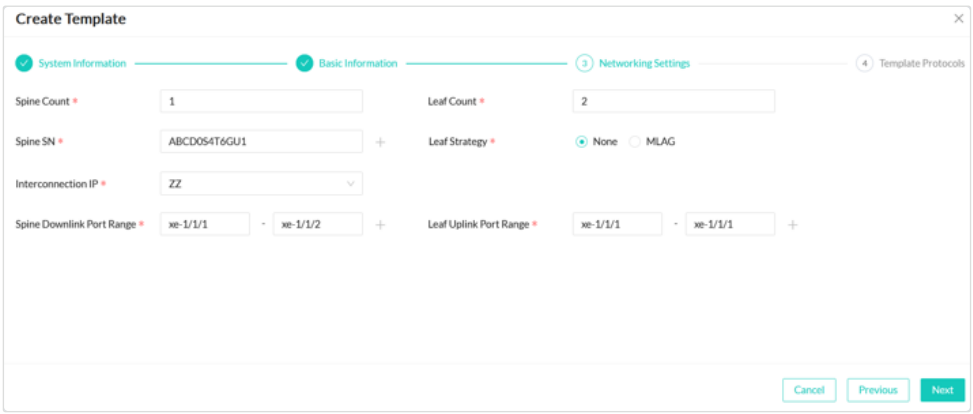


Table 2. Network Setting Parameters

Parameter	Description

Spine Count	The count of spine switches to be added to the physical network. The minimum value is 1, and the maximum value is 128.
Leaf Count	The count of leaf switches to be added to the physical network. • If you select **None** in the **Leaf Strategy** section, the minimum value is 1. • If you select **MLAG** in the **Leaf Strategy** section, the minimum value is 2, and the value must be an even number. • The maximum value is 128.
Spine SN	The serial number (SN) of the switch to be added as the spine switch. The **Spine SN** can contain only letters and numbers. AmpCon-DC will assign the switch with the entered **Spine SN** as the spine switch. **NOTEs** • If the **Spine Count** is greater than 1, click **+** to add multiple **Spine SN** fields, and enter a spine switch SN for each field. Each spine SN must be unique. • The count of the **Spine SN** fields needs to be the same as the **Spine Count**. • If a switch with a **Spine SN** has been used by another ZTP template or has been managed by AmpCon-DC, the ZTP template will fail to be added. • If a switch with a **Spine SN** hasn't been added to the DHCP configuration file, or if a **Spine SN** is wrong, the switch with the **Spine SN** will not go to the parking lot and thus will fail to be deployed.

Leaf Strategy	Select **None** or **MLAG**. • **None:** Leaf switches are non-MLAG switches. • **MLAG:** Leaf switches are MLAG switches. **NOTE** If you want to configure a RoCE policy in the simplified ZTP process, you must select **None**.
Interconnection IP	The interconnection IP addresses for Layer 3 links between leaf and spine switches. Select an IP pool. AmpCon-DC will assign interconnection IP addresses automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
L3 Peer Link IP	The IP addresses of the network link between two MLAG peers at Layer 3. The IP addresses are used for synchronizing routing information, exchanging protocol messages, and potentially transmitting data traffic. Select an IP pool. AmpCon-DC will assign L3 peer link IP addresses automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**. **NOTE** This field is available only when you select **MLAG** in the **Leaf Strategy** section.
Spine Downlink Port Range	The port ranges on each spine switch used for downlink connections to leaf switches. Each spine switch uses the same downlink port ranges.

	You can add one or multiple downlink port ranges. To add multiple downlink port ranges, click **+**. **Configuration Example:** If the fabric has one spine switch and four leaf switches and the spine switch uses four ports (xe-1/1/2, xe-1/1/4, xe-1/1/5, and xe-1/1/6) for downlink connections to all these leaf switches, configure the **Spine Downlink Port Range** as follows: • **xe-1/1/2 - xe-1/1/2** • **xe-1/1/4 - xe-1/1/6** **xe-1/1/4 - xe-1/1/6** means three ports xe-1/1/4, xe-1/1/5, and xe-1/1/6. The start port is xe-1/1/4, and the end port is xe-1/1/6. **xe-1/1/2 - xe-1/1/2** means only one port xe-1/1/2. **NOTEs** • Port values need to be in format of te-1/1/x, ge-1/1/x, or xe-1/1/x. • Ensure that all ports in the **Spine Downlink Port Range** exist on the spine switches. Or else, the simplified ZTP deployment will fail. • The end port must be greater than or equal to the start port. • The start and end ports of a port range must be in the same format. For example, ge-1/1/1 to ge-1/1/6 is correct, while ge-1/1/1 to te-1/1/6 is wrong. • The count of ports in the port range must be equal to the count of leaf switches.
Leaf Uplink Port Range	The port ranges on each leaf switch used for uplink connections to spine switches. Each leaf switch uses the same uplink port ranges.

	You can add one or multiple uplink port ranges. To add multiple uplink port ranges, click **+**. **Configuration Example:** If the fabric has one spine switch and three leaf switches and each leaf switch uses xe-1/1/1 for uplink connections to the spine switch, configure the **Leaf Uplink Port Range** as follows: • **xe-1/1/1 - xe-1/1/1** **NOTEs** • Port values need to be in format of te-1/1/x, ge-1/1/x, or xe-1/1/x. • Ensure that all ports in the **Leaf Uplink Port Range** exist on the leaf switches. Or else, the simplified ZTP deployment will fail. • The end port must be greater than or equal to the start port. • The start and end ports of a port range must be in the same format. For example, ge-1/1/1 to ge-1/1/6 is correct while ge-1/1/1 to te-1/1/6 is wrong. • The count of ports in the port range must be equal to the count of spine switches.
Leaf Peer Link Port Range	The port ranges on MLAG leaf switches used for peer link connections. The **Leaf Peer Link Port Range** must contain 2 ports. Each MLAG leaf switch uses a different port for peer link connections. See the following configuration example, which includes the ports xe-1/1/6 and xe-1/1/8: • **xe-1/1/6 - xe-1/1/6** • **xe-1/1/8 - xe-1/1/8**

	You can add one or multiple leaf peer link port ranges. To add multiple leaf peer link port ranges, click **+**. **NOTEs** • Ensure that all ports in the **Leaf Peer Link Port Range** exist on the leaf switches. Or else, the simplified ZTP deployment will fail. • The **Leaf Uplink Port Range** and **Leaf Peer Link Port Range** can't overlap. • Port values need to be in format of te-1/1/x, ge-1/1/x, or xe-1/1/x. • The end port must be greater than or equal to the start port. • The start and end ports of a port range must be in the same format. For example, ge-1/1/1 to ge-1/1/6 is correct while ge-1/1/1 to te-1/1/6 is wrong. • This field is available only when you select **MLAG** in the **Leaf Strategy** section.

6. Click **Next** to go to the **Template Protocols** section.

   The **Underlay Protocol** field here is automatically filled based on the **Underlay Protocol** selected in the **Basic Information** section.

- If the **Service Network Type** is **VXLAN** and the **Underlay Protocol** is **BGP** in the **Basic Information** section, input the following information:

  NOTEs

  - In the **ASN Allocation Rule** section, **Only Spine Remains Consistent**, which means that all spine switches are assigned the same AS number, is selected by default.
  - In the **Overlay Protocol** section, **MP-BGP EVPN** is selected by default.

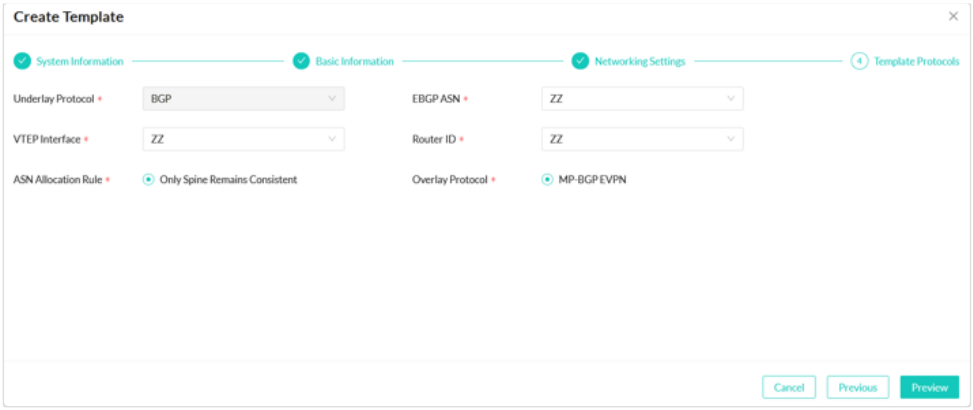


Table 3. Input Parameters for Scenario 1

Parameter	Description
EBGP ASN	The unique identifier to distinguish an AS in EBGP. Select an ASN pool. AmpCon-DC will assign EBGP ASNs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
VTEP Interface	The interface on a VXLAN Tunnel End Point (VTEP) device, through which VXLAN packets are sent and received. Select an IP pool. AmpCon-DC will assign VTEP interfaces automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
Router ID	The identifier used by BGP to uniquely identify a router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.

- If the **Service Network Type** is **VXLAN** and the **Underlay Protocol** is **OSPF** in the **Basic Information** section, input the following information:

> **NOTE**
>
> **OSPF Area ID** is the ID used to distinguish an OSPF area. Currently, the value is 0.0.0.0 and can't be changed.

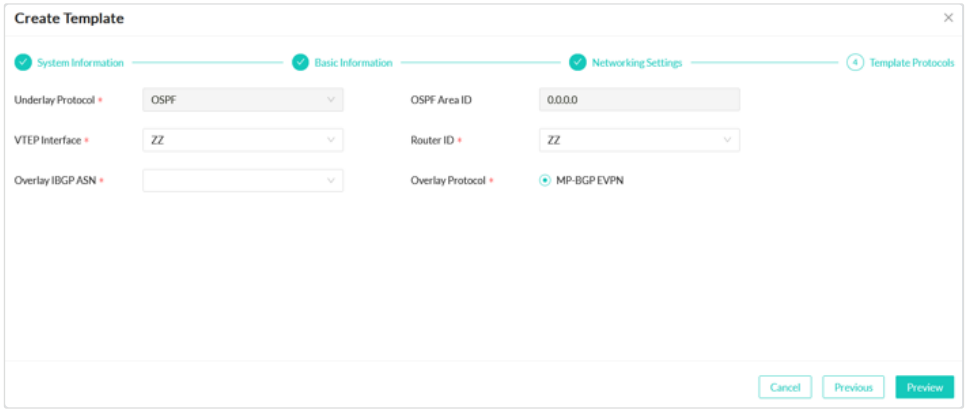


Table 4. Input Parameters for Scenario 2

Parameter	Description
VTEP Interface	The interface on a VXLAN Tunnel End Point (VTEP) device, through which VXLAN packets are sent and received. Select an IP pool. AmpCon-DC will assign VTEP interfaces automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
Router ID	The identifier used by OSPF to uniquely identify the router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
Overlay IBGP ASN	The unique identifier to distinguish an Autonomous System (AS) in IBGP. An AS is a group of IP networks that are controlled by one entity and have the same

	routing policy. Each AS is assigned a unique AS number, which identifies an AS on a BGP network. Select an ASN pool. AmpCon-DC will assign IBGP ASNs automatically based on the IP pool. To add a new ASN pool, click the drop-down list, and then click **+ Pool**.

- If the **Service Network Type** is **VLAN** and the **Underlay Protocol** is **BGP** in the **Basic Information** section and the **Leaf Strategy** is **MLAG** in the **Networking Settings** section, input the following information:

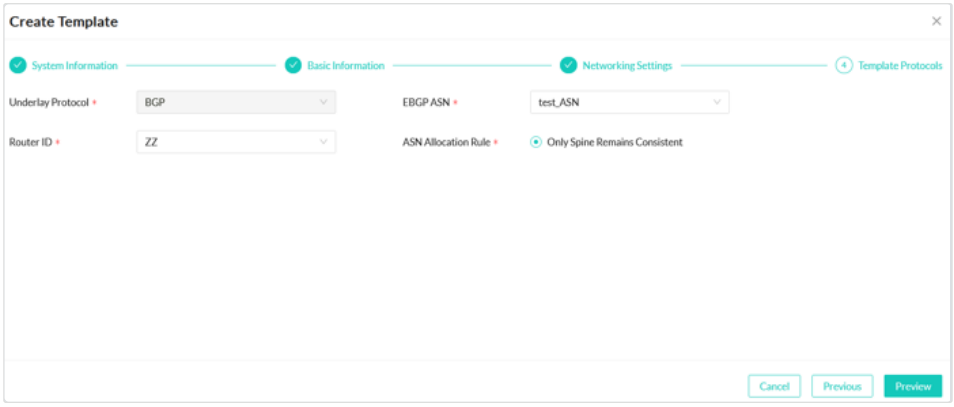


Table 5. Input Parameters for Scenario 3

Parameter	Description
EBGP ASN	The unique identifier to distinguish an AS in EBGP. Select an ASN pool. AmpCon-DC will assign EBGP ASNs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
Router ID	The identifier used by BGP to uniquely identify a router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool.

	To add a new IP pool, click the drop-down list, and then click **+ Pool**.

- If the **Service Network Type** is **VLAN** and the **Underlay Protocol** is **OSPF** in the **Basic Information** section and the **Leaf Strategy** is **MLAG** in the **Networking Settings** section, input the following information:

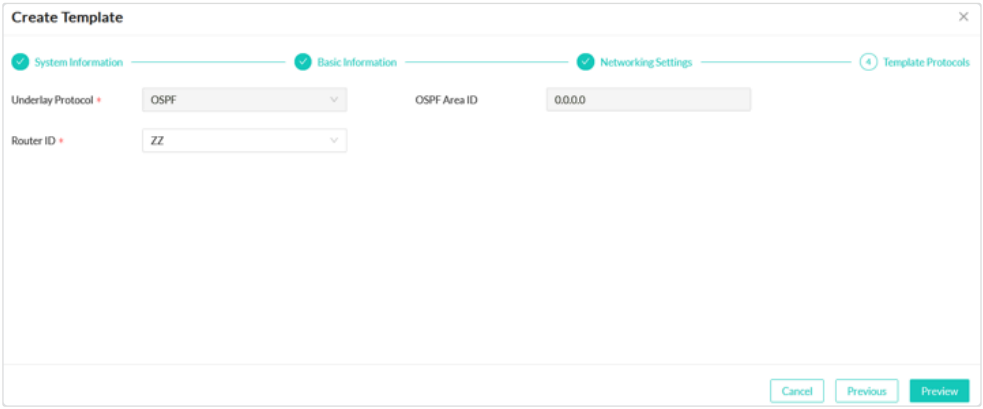


Table 6. Input Parameters for Scenario 4

Parameter	Description
Router ID	The identifier used by OSPF to uniquely identify a router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.

- If the **Service Network Type** is **VLAN** and the **Underlay Protocol** is **BGP** in the **Basic Information** section and the **Leaf Strategy** is **None** in the **Networking Settings** section, input the following information:

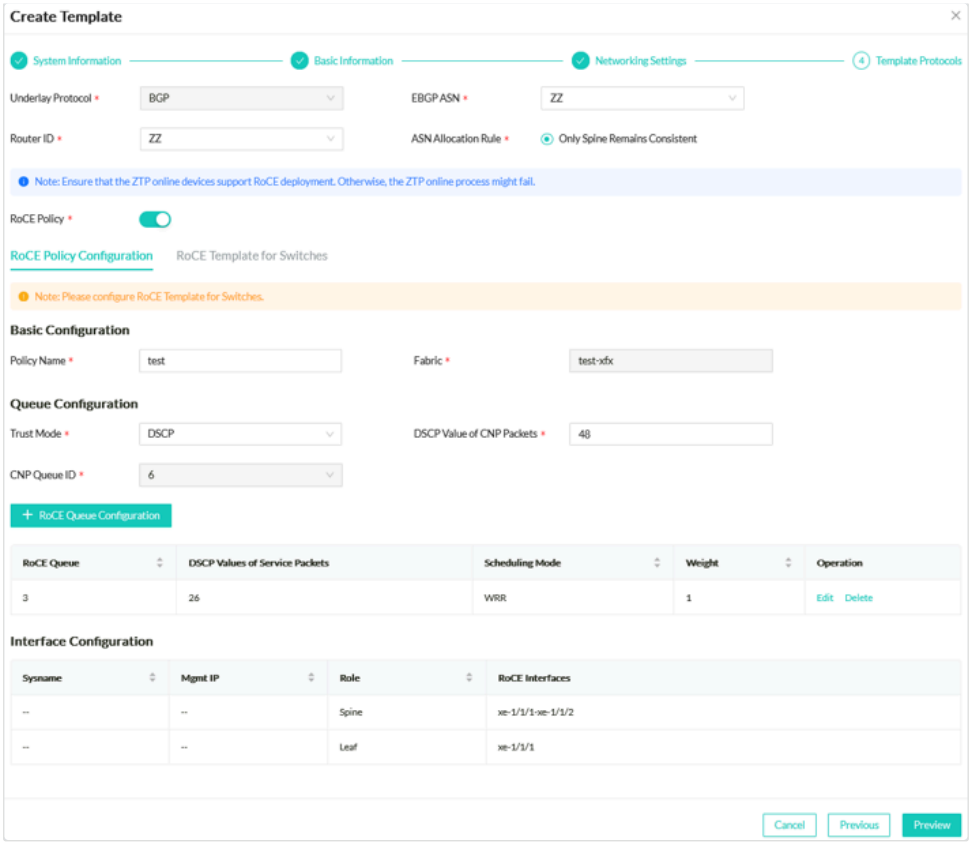


Table 7. Input Parameters for Scenario 5

Parameter	Description
EBGP ASN	The unique identifier to distinguish an AS in EBGP. Select an ASN pool. AmpCon-DC will assign EBGP ASNs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
Router ID	The identifier used by BGP to uniquely identify a router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
RoCE Policy	To enable RoCE policy configurations, toggle it on. Then, input RoCE-related parameters. For

	detailed parameter descriptions, see RoCE Policy Configuration and RoCE Template for Switches. **NOTEs** • Different from the RoCE policy creation process on the “RoCE Policies” page, some fields in the ZTP template are filled automatically based on the parameters in the template. For example: ◦ The **Fabric** field ◦ The **Interface Configuration** section • If **RoCE Policy** is toggled off, no RoCE policy configurations will be pushed to switches. You can push RoCE policy configurations on the “RoCE Policies” page after the simplified ZTP process is completed.

- If the **Service Network Type** is **VLAN** and the **Underlay Protocol** is **OSPF** in the **Basic Information** section and the **Leaf Strategy** is **None** in the **Networking Settings** section, input the following information:

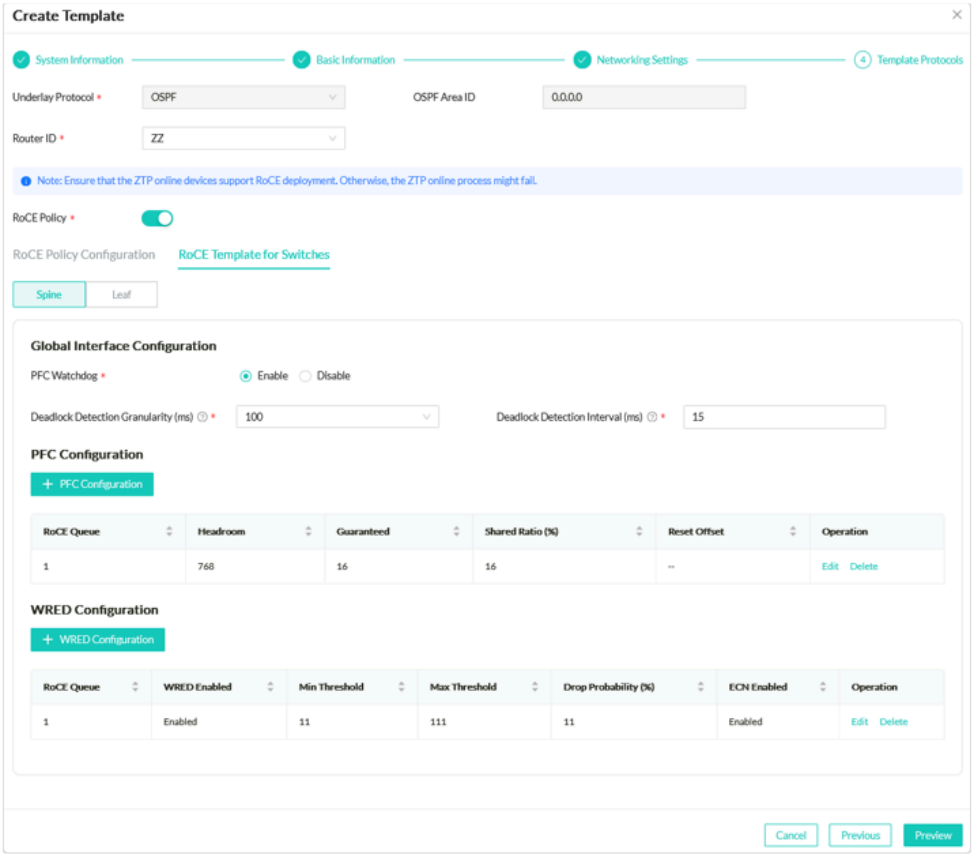


Table 8. Input Parameters for Scenario 6

Parameter	Description
Router ID	The identifier used by OSPF to uniquely identify a router. Select an IP pool. AmpCon-DC will assign router IDs automatically based on the IP pool. To add a new IP pool, click the drop-down list, and then click **+ Pool**.
RoCE Policy	To enable RoCE policy configurations, toggle it on. Then, input RoCE-related parameters. For detailed parameter descriptions, see RoCE Policy Configuration and RoCE Template for Switches. **NOTEs** • Different from the RoCE policy creation process on the “RoCE Policies” page,

	some fields in the ZTP template are filled automatically based on the parameters in the template. For example: ◦ The **Fabric** field ◦ The **Interface Configuration** section • If **RoCE Policy** is toggled off, no RoCE policy configurations will be pushed to switches. You can push RoCE policy configurations on the “RoCE Policies” page after the simplified ZTP process is completed.

7. Click **Preview** to go to the fabric page.

> **Tips**
>
> - After you click **Preview**, the ZTP template will be added to the “ZTP Templates” page.
> - If you select **New Fabric** in the **Basic Information** section, after you click **Preview**, the new fabric will be added to the “Fabrics” page.
> - You can also go to the fabric page by clicking **Physical Network > Fabrics** from the navigation bar and then clicking the name of the fabric on the “Fabrics” page.
> - You can edit a ZTP template only when the fabric related to the ZTP template is in **Not Deployed** status. Use one of the following ways:
>   - In the **Configuration Preview** tab of the fabric page, click **Previous**.
>   - Click **Physical Network > Design > ZTP Templates** from the navigation bar. Locate the ZTP template, and then click **Edit**.

2. Completing Physical Connections

Based on the ZTP template, AmpCon-DC automatically generates the topology, device information, and link information of the physical network. You must complete physical

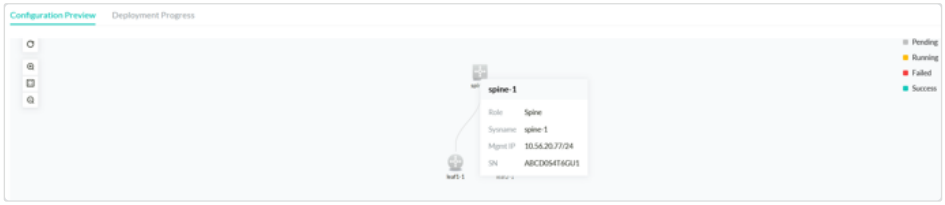
connections based on the generated information. Follow these steps:

> **NOTE**
>
> Ensure that the physical connections are consistent with the topology, device information, and link information. Or else, the simplified ZTP process will fail.

1. In the **Configuration Preview** tab of the fabric page, check the following information:

- Check the topology. Hover over each link or each switch, and then you can see detailed information of the link or switch.

> **Tips**
>
> - Click the **Reload Topology** icon to reload the topology.
> - Click the **Zoom In** icon to zoom in the topology.
> - Click the **Reset Zoom** icon to reset the zoom setting.
> - Click the **Zoom Out** icon to zoom out the topology.



- Check the device information of spine and leaf switches in the **Device Info** sub-tab.

> **NOTEs**
>
> - The **SN** and **Model** of leaf switches are blank. After you click **Enable ZTP** for leaf switches, the **SN** and **Model** of each leaf switch can be automatically retrieved through Link Layer Discovery Protocol (LLDP) and displayed in the **Device Info** sub-tab.
> - The **VTEP Interface** of each spine switch is blank.



Tips

- The **Status** column displays the ZTP deployment status for each switch. See the following supported status:
  - **Success:** The switch goes online successfully.
  - **Failed:** The switch fails to go online.
  - **Running:** The switch is going online.
  - **Pending:** The ZTP process hasn't started.
- The **Log** button can be used to check the underlay configurations pushed to a switch successfully. If a RoCE policy is configured in the ZTP template, the **Log** button can also be used to check RoCE configurations pushed to a switch successfully.
- The **Edit** button can be used to edit the sysname and SN of a spine switch and edit the sysname of a leaf switch. This button is available for only the switches in **Pending** status.
- The **Back Online** button can be used to change the switch status from **Failed** to **Pending**. This button is available for only the switches in **Failed** status.

- Check link information in the physical network by clicking the **Link Info** sub-tab.



- Optional: Check network configurations by clicking the **Network Configuration** sub-tab.

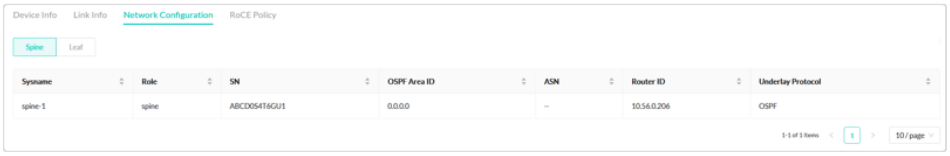
NOTE

In the **Leaf** sub-tab, some columns are blank:

- The **Physical Device** of each leaf switch is blank. After you click **Enable ZTP** for these leaf switches, the **Physical Device** of each

leaf switch can be automatically retrieved through Link Layer Discovery Protocol (LLDP) and displayed in the **Leaf** sub-tab.

- If the **Leaf Strategy** is **None** in the ZTP template, **MLAG Peer**, **MLAG Peer Links**, **MLAG Peer Link VLAN**, and **Local IP** are blank.
- If the **Underlay Protocol** is **OSPF** and the **Service Network Type** is **VLAN** in the ZTP template, the **ASN** is blank.



- Optional: Check RoCE policy configurations by clicking the **RoCE Policy** sub-tab.



Tips

- Only in the following cases, the **RoCE Policy** sub-tab is displayed on the fabric page:
  - You configure a RoCE policy during the simplified ZTP process.
  - You don't configure a RoCE policy during the simplified ZTP process. But after the fabric is deployed through simplified ZTP, you create a RoCE policy on the "RoCE Policies" page and associate the RoCE policy with the fabric.
- If all switches in the ZTP template are not brought online, you can click **Edit** or **Delete** to edit or delete the RoCE policy.
- To check detailed RoCE policy configurations, click **View**.
- To check the deployment logs of the RoCE policy, click **Log**. These logs include only the changes made on the "RoCE Policies" page.
- If you edit the RoCE policy on the "RoCE Policies" page, the updated RoCE configurations are automatically displayed on the **RoCE Policy** sub-tab.

- On the “RoCE Policies” page, if you delete the RoCE policy related to the fabric, the **RoCE Policy** sub-tab is removed automatically from the fabric page.

2. Optional: Modify switch SNs and hostnames if needed.

- If you want to replace a spine switch with a new switch, locate the spine switch to be replaced, and then click **Edit**.

  In the pop-up window, enter the SN of the new spine switch in the **New SN** field, and then click **Apply**.

  NOTEs

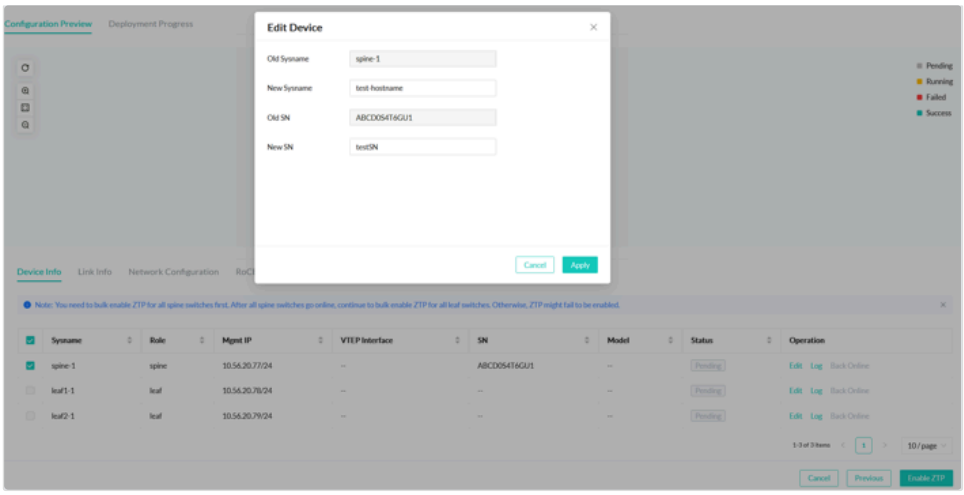
  - You can’t replace leaf switches through this method.
  - Only the spine switches in **Pending** status can be replaced.
  - The **New SN** can contain at most 64 characters, and only letters and numbers are supported.
  - Ensure that the switch with the **New SN** hasn’t been used by other fabrics and hasn’t been managed by AmpCon-DC.

- If you want to modify the hostname of a leaf or spine switch, locate the switch, and then click **Edit**.

  In the pop-up window, enter the new hostname in the **New Sysname** field, and then click **Apply**.

  NOTEs

  - Only the hostnames of the switches in **Pending** status can be changed.
  - The **New Sysname** can contain at most 63 characters, and only letters, numbers, and hyphens (-) are supported.
  - The **New Sysname** will be pushed to the switch when the switch is brought online.



3. Based on the topology, device information, and link information, complete physical connections between switches.

> **NOTEs**
>
> Pay attention to the following points. Otherwise, the simplified ZTP deployment will fail.
>
> - You have designated spine SNs in the ZTP template. So in physical connections, you must use the switches with the designated spine SNs as spine switches.
> - In the ZTP template, you have designated the count of leaf switches. So in physical connections, you must connect spine switches with the designated count of leaf switches.
> - Ensure that the switch ports used for physical connections are consistent with the link information displayed in the **Link Info** sub-tab.

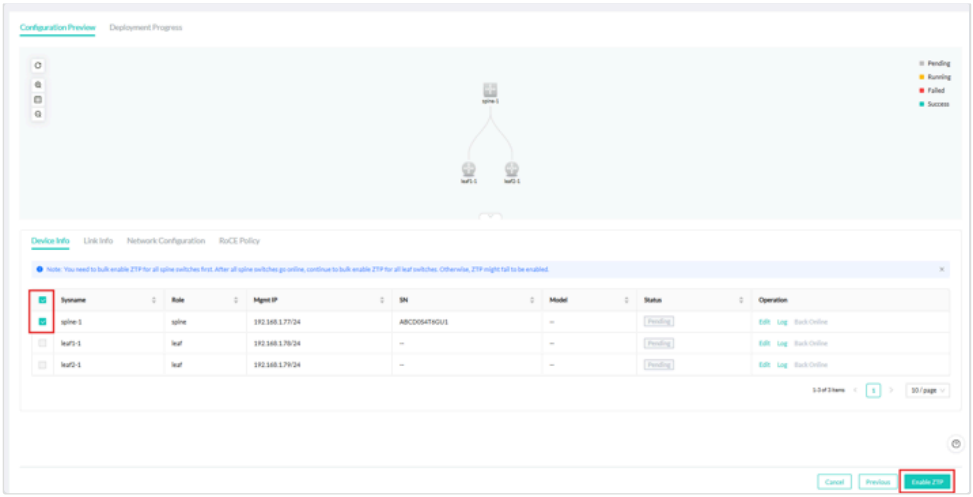
3. Bringing All Spine Switches Online

You must bring all spine switches online before bringing leaf switches online.

To bring all spine switches online, follow these steps:

1. In the **Configuration Preview** tab of the fabric page, select all the switches with the **Spine** role, and then click **Enable ZTP**.

   You will be redirected to the **Deployment Progress** tab.



2. In the **Deployment Progress** tab, check the deployment progress.

- In the **Topo View** sub-tab, check the fabric topology and the following metrics:

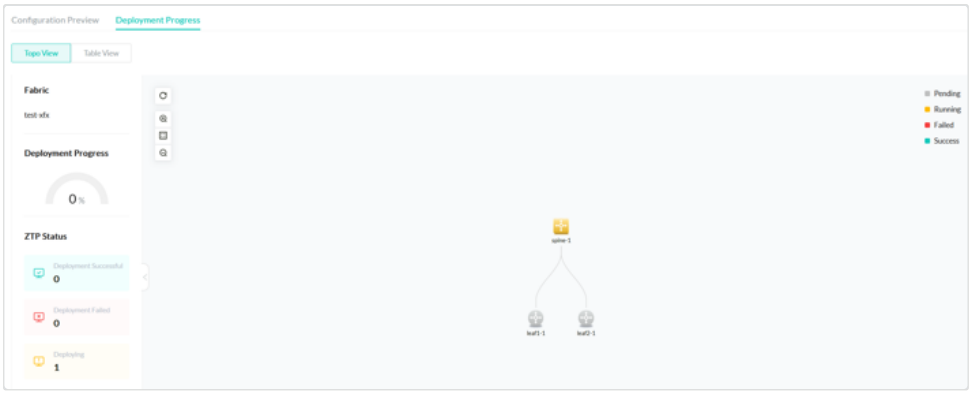


Table 9. Topo View Metrics

Metric	Description
Fabric	The name of the fabric associated with the simplified ZTP deployment.
Deployment Progress	The bar and percentage showing the deployment progress.
ZTP Status	The count of ZTP deployments in different status during the simplified ZTP process. Each ZTP deployment means bringing a leaf or spine switch online. • **Deployment Successful:** The count of successful ZTP deployments.

	• **Deployment Failed:** The count of failed ZTP deployments. • **Deploying:** The count of ZTP deployments that are running.

- In the **Table View** sub-tab, check the following metrics:

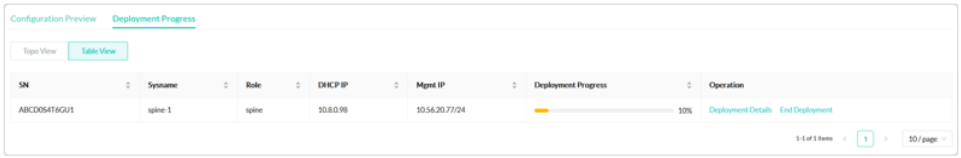


Table 10. Table View Metrics

Metric	Description
SN	The SN of the switch.
Sysname	The hostname of the switch.
Role	The role of the switch, **spine** or **leaf**. • **spine:** The switch acts as a spine switch in the fabric. • **leaf:** The switch acts as a leaf switch in the fabric.
DHCP IP	The switch IP address that you configured in the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server. For more information, see Configuring a DHCP Server.
Mgmt IP	The management IP address of the switch. • **Mgmt IP** is automatically assigned by AmpCon-DC based on the management IP ranges specified in the ZTP template. • **Mgmt IP** is used to connect a switch with the AmpCon-DC server.
Deployment Progress	The bar and percentage showing the deployment progress of the switch. Different

	colors have different meanings. • **Yellow:** The ZTP deployment is still running. • **Green:** The ZTP deployment is completed successfully. • **Red:** The ZTP deployment fails.

To check deployment logs, click the **Table View** sub-tab, locate the switch, and then click **Deployment Details**.



To end a ZTP deployment, locate the switch in the **Table View** sub-tab, and then click **End Deployment**.

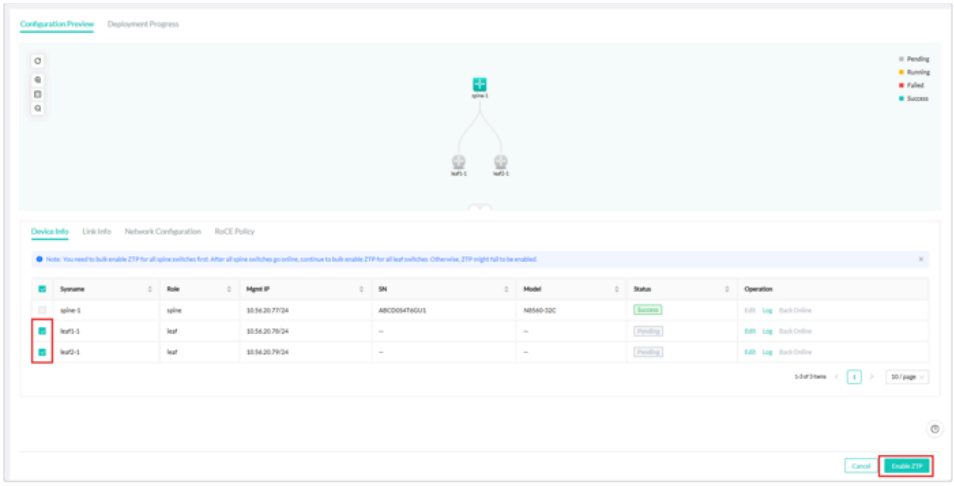
3. If some spine switches fail to go online, follow the steps in Troubleshooting Simplified ZTP to bring all the failed spine switches online again.

4. Bringing All Leaf Switches Online

After all spine switches go online successfully, bring all leaf switches online. Follow these steps:

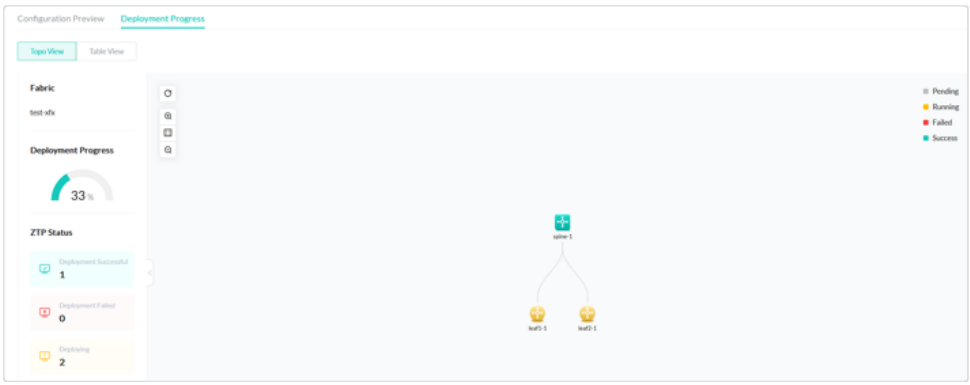
1. In the **Configuration Preview** tab of the fabric page, select all switches with the **Leaf** role, and then click **Enable ZTP**.

   You will be redirected to the **Deployment Progress** tab.

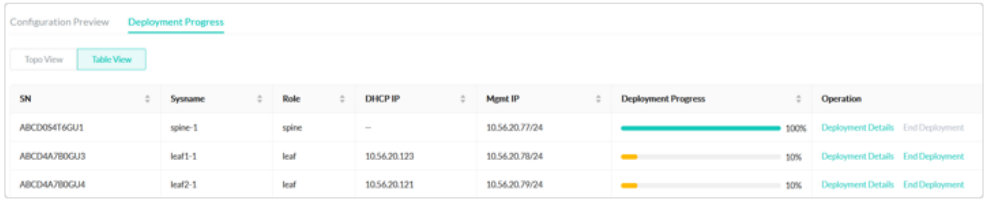


2. In the **Deployment Progress** tab, check the deployment progress.

- **Topo View** sub-tab:



- **Table View** sub-tab:



3. If some leaf switches fail to go online, follow these steps in Troubleshooting Simplified ZTP to bring all the failed leaf switches online again.

After all the spine and leaf switches are brought online, the simplified ZTP deployment is completed successfully. All these switches are deployed and managed by AmpCon-DC, and the physical network is deployed.

What to Do Next

After you complete the simplified ZTP deployment, you can check the fabric and switch deployment status. For more information, see Post-Deployment Operations.

Post-Deployment Operations

You can check fabric and switch deployment status and view, edit, or delete ZTP templates.

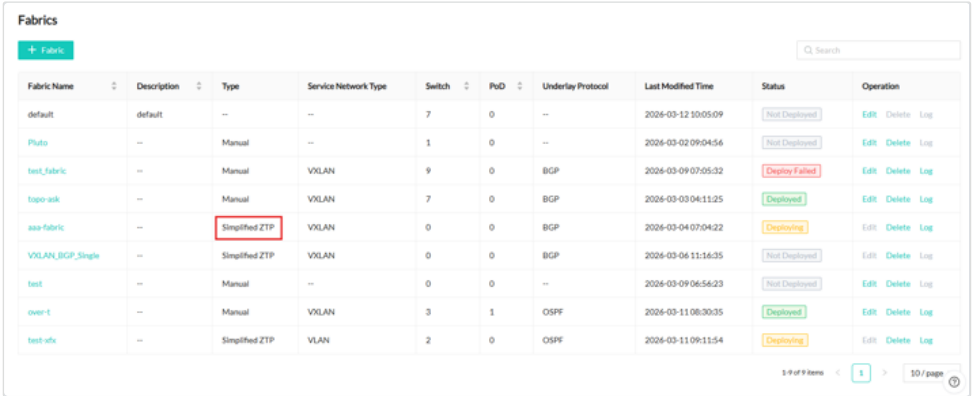
Checking Fabric Status
Checking Switch Status
Viewing or Editing a ZTP Template
Deleting a ZTP Template

Checking Fabric Status

To check whether a fabric is deployed successfully, follow these steps:

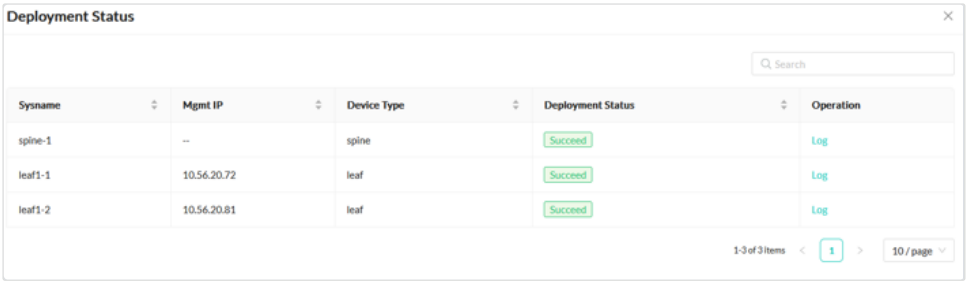
1. Click **Physical Network > Fabrics** from the navigation bar.
2. On the “Fabrics” page, locate the fabric deployed through simplified ZTP.
3. In the **Status** column, check the fabric deployment status. For more information about fabric deployment status, see Viewing All Fabrics.

> **NOTE**
>
> For a fabric deployed through simplified ZTP, the status here depends on the status in the **Configuration Preview** tab of the fabric page. See the following status descriptions:
>
> - **Deployed:** In the **Configuration Preview** tab, all spine and leaf switches are in **Success** status.
> - **Deploying:** In the **Configuration Preview** tab, not all switches are in **Pending** status, and not all switches are in **Success** status.
> - **Not Deployed:** In the **Configuration Preview** tab, all spine and leaf switches are in **Pending** status.



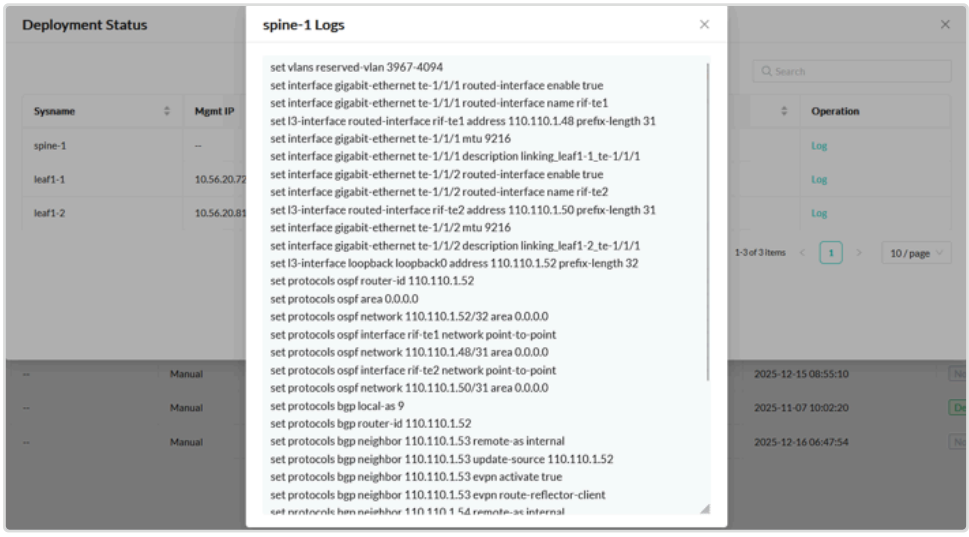
4. In the **Operation** column, click **Log**.

5. In the pop-up window, check the deployment status of each switch.



You can click **Log** to check the underlay configurations pushed to a switch successfully.

If a RoCE policy is configured in the ZTP template, you can also click **Log** to check RoCE configurations pushed to a switch successfully.

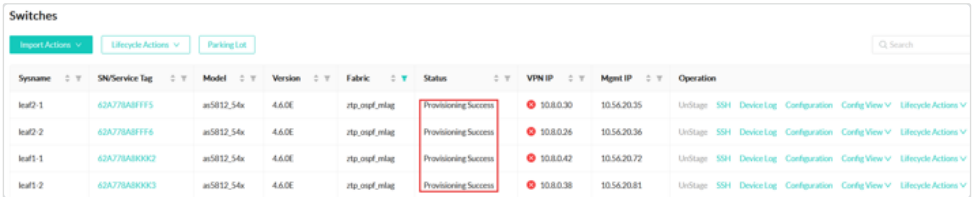


Checking Switch Status

To check whether a switch is deployed successfully, follow these steps:

1. Click **Device > Switches** from the navigation bar.
2. On the “Switches” page, locate the switch deployed through simplified ZTP.
3. In the **Status** column, check the switch deployment status. The **Provisioning Success** status means switches are deployed successfully.

   For more information about switch deployment status, see Viewing the Switch List.

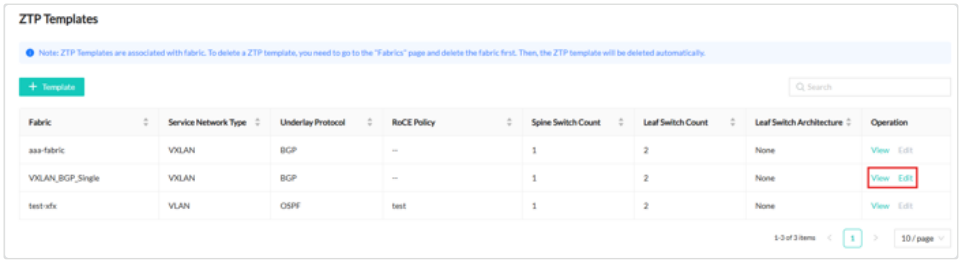


Viewing or Editing a ZTP Template

To view a ZTP template, follow these steps:

1. Click **Physical Network > Design > ZTP Templates** from the navigation bar.
2. On the “ZTP Templates” page, locate the ZTP template.
3. Click **View** to view the ZTP template, or click **Edit** to edit the ZTP template.

> **NOTE**
>
> You can edit a ZTP template only when the fabric related to the ZTP template is in **Not Deployed** status.

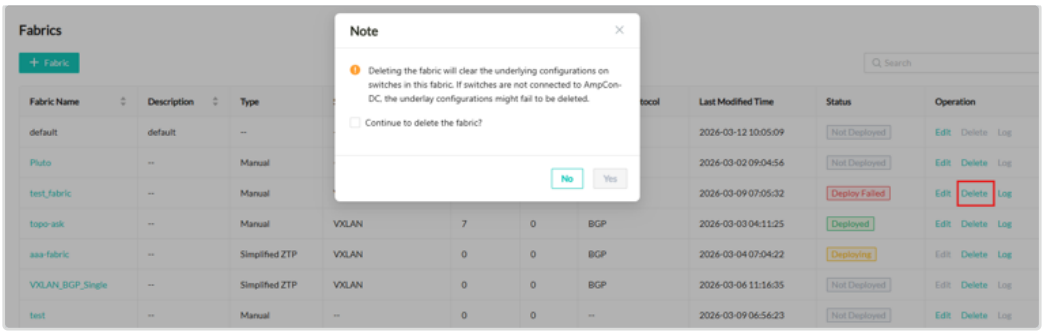


Deleting a ZTP Template

AmpCon-DC doesn’t support deleting the ZTP template directly. To delete a ZTP template, delete the associated fabric on the “Fabrics” page. For more information, see Deleting a Fabric.

After you delete the fabric, the ZTP template will be deleted automatically.

> **NOTEs**
>
> - Each fabric can be associated with at most a ZTP template.
> - If a fabric has switches that are being brought online, you can’t delete the fabric and the ZTP template.
> - After a fabric is deleted, the underlay configurations are deleted from these switches, and all the switches previously in the fabric are moved to the **default** fabric.
> - If a RoCE policy is configured in the ZTP template, the RoCE policy will also be deleted on the “RoCE Policies” page.


Fabrics
+ Fabric
Search
Note
Deleting the fabric will clear the underlying configurations on switches in this fabric. If switches are not connected to AmpCon-DC, the underlay configurations might fail to be deleted.
Continue to delete the fabric?
No
Yes
Fabric Name
Description
Type
Last Modified Time
Status
Operation
default
default
--
2026-03-12 10:05:09
Not Deployed
Edit Delete Log
Pluto
--
Manual
2026-03-02 09:04:56
Not Deployed
Edit Delete Log
test_fabric
--
Manual
2026-03-09 07:05:32
Deploy Failed
Edit Delete Log
topo-ask
--
Manual
VXLAN
7
0
BGP
2026-03-03 04:11:25
Deployed
Edit Delete Log
aaa-fabric
--
Simplified ZTP
VXLAN
0
0
BGP
2026-03-04 07:04:22
Deploying
Edit Delete Log
VXLAN_BGP_Single
--
Simplified ZTP
VXLAN
0
0
BGP
2026-03-06 11:16:35
Not Deployed
Edit Delete Log
test
--
Manual
--
0
0
--
2026-03-09 06:56:23
Not Deployed
Edit Delete Log

Troubleshooting Simplified ZTP

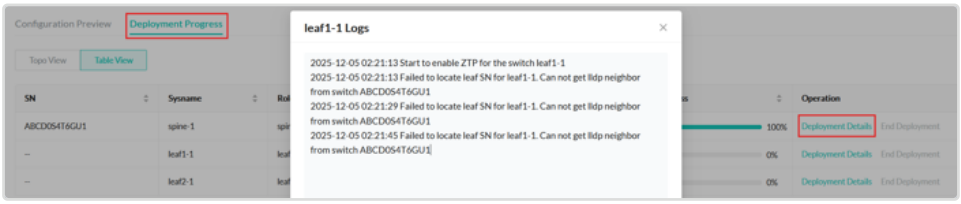
During the simplified ZTP process, if any spine or leaf switches fail to go online, follow the steps in this document to bring these switches online again.

Troubleshooting Procedure
Possible Reasons and Solutions

Troubleshooting Procedure

1. Click **Physical Network > Fabrics** from the navigation bar. On the “Fabrics” page, click the name of the fabric.
2. Click the **Deployment Progress** tab, and then click the **Table View** sub-tab. Locate each failed switch, and then click **Deployment Details**.

   In the pop-up window, analyze the deployment logs for troubleshooting, and then resolve the issues. If you still have no clues about failure reasons, check the Possible Reasons and Solutions section.



3. Click the **Configuration Preview** tab, locate each spine switch in **Failed** status, and then click **Back Online**. The switch status will be changed from **Failed** to **Pending**.



   Select all these spine switches in **Pending** status, and then click **Enable ZTP** to bring them online again.



4. After all spine switches are brought online successfully, if any leaf switches fail to go online, locate each leaf switch in **Failed** status, and then click **Back Online**. The switch status will be changed from **Failed** to **Pending**.

   Select all these leaf switches in **Pending** status, and then click **Enable ZTP** to bring them online again.

Possible Reasons and Solutions

If some switches fail to be deployed through simplified ZTP, the reasons might be as follows:

Table 1. Possible Reasons and Solutions

Category	Reason	Solution
Switch	The switches are not supported by AmpCon-DC.	Complete all the preparations in Preparing PicOS Switches.
	The switches don't have PicOS installed.	
	The switches are down.	
	The switches have been configured before simplified ZTP.	
	The switches don't have PicOS licenses installed so that no available ports can be used by AmpCon-DC.	
	The Secure Shell (SSH) protocol is not enabled on the switches.	
	The firewall blocks the TCP ports 22, 9339, and 830 to the management port of each switch.	
DHCP Server	The DHCP server is not configured as described in Configuring a DHCP Server. In this case, the switches can't go to the AmpCon-DC parking lot, and thus AmpCon-DC can't find the switches.	Complete all the preparations in Configuring a DHCP Server.

	The switch DHCP IP addresses specified in the DHCP configuration file (/etc/dhcp/dhcpd.conf) have conflicts with each other or overlap with the following IP addresses: • IP addresses in the management IP ranges specified in ZTP templates. • Management IP addresses of the switches having been managed by AmpCon-DC.	Avoid these IP conflicts when you configure the DHCP configuration file.
	The AmpCon-DC server IP address specified in the DHCP configuration file is wrong so that the switches can't connect to the AmpCon-DC server.	Ensure that the AmpCon-DC server IP address is correct in the DHCP configuration file.
	The switch DHCP IP addresses specified in the DHCP configuration file are not able to connect to the IP address of the AmpCon-DC server.	Ensure that the DHCP IP address of each switch is able to connect to the IP address of the AmpCon-DC server.
System Configuration	The system configuration specified in the ZTP template doesn't contain the correct default username (**Device Default Login User**) and password (**Device Default Password**) of the switches.	Ensure that the system configuration specified in the ZTP template contains correct information. See Adding System Configurations.
	The **License Portal URL**, **License Portal User**, or **License Portal Password** are not correct so that AmpCon-DC can't connect with the License Portal.	

	You have changed the default switch password (**Device Default Password**) but haven't followed the steps and notes in Changing the Default Switch Password.	
	The system configuration contains wrong configurations in the uploaded **Security Config File** or **Parking Security Config File**.	
AmpCon-DC License	You haven't imported the AmpCon-DC licenses containing the switches to be deployed.	Check whether the hardware IDs of the switches are included in any imported AmpCon-DC licenses. See Viewing AmpCon-DC Licenses. If not, import a valid AmpCon-DC license. See Importing Licenses for Deployed Switches.
	The imported AmpCon-DC licenses don't contain all the switches to be deployed.	
	The imported AmpCon-DC licenses are expired.	
ZTP Template	The spine SNs specified in the ZTP template are wrong, or the spine switches with the spine SNs haven't been added to the DHCP configuration file. In these cases, the switches can't go to the parking lot.	Ensure that the spine and leaf switches are in the parking lot. See Managing the Parking Lot.
	The leaf switches connected with the spine switches haven't been added to the DHCP configuration file, and thus haven't been in the parking lot.	

	Some ports specified in the **Spine Downlink Port Range**, **Leaf Uplink Port Range**, or **Leaf Peer Link Port Range** of the ZTP template don't exist on switches.	Ensure that the ports in these ranges exist on related spine and leaf switches.
	The added management IP ranges in the ZTP template overlap with the following IP addresses: • The DHCP IP addresses assigned in the DHCP configuration file. • The management IP addresses assigned in other ZTP templates. • The management IP addresses of the switches having been managed by AmpCon-DC.	Avoid these IP conflicts when you enter the management IP ranges in the ZTP template.
	The IP addresses in added management IP ranges are occupied or not able to connect to the IP address of the AmpCon-DC server.	Ensure that each IP address in the management IP ranges are not occupied and are able to connect to the IP address of the AmpCon-DC server.
	The IP pools and ASN pools specified in the ZTP template don't have enough available IP addresses and ASNs.	Extend the IP pools or ASN pools used by the ZTP template.
Physical Connection	The physical connections are not consistent with the topology, device information, and link information generated automatically by AmpCon-DC based on the ZTP template.	Ensure that the physical connections are totally consistent with the topology, device information, and link

	• In physical connections, spine switches are not those switches with the spine SNs designated in the ZTP template. • In physical connections, spine switches are not connected with the designated count of leaf switches. The leaf switch count is designated in the ZTP template. • The switch ports used for physical connections are not consistent with the link information generated automatically by AmpCon-DC.	information generated automatically by AmpCon-DC.

Provisioning Overlay Services

Overlay is a virtual network architecture built on top of an existing physical network (underlay). Overlay services refer to virtualized network functions or logical layers, which enable logical network isolation and flexible service deployment and network configurations without modifying the underlying infrastructure.

Like physical networks used for underlay provisioning, **logical networks** are logical space to provision overlay services. Logical networks incorporates resources from Virtual Private Clouds (VPCs). Resources from either the same VPC or different VPCs can exist within a single logical network. If you need to isolate resources from different VPCs, place each VPC in a separate logical network.

Overlay service configurations are abstracted into **logical network elements**, including logical networks, logical routers, logical switches, and virtual networks.

After a physical network is deployed, you can deploy logical networks for overlay service provisioning.

See the following child topics:

- Logical Network Overview
- Deploying Logical Networks
- Managing Logical Network Elements
- Troubleshooting Guide

Logical Network Overview

Learn the following information about logical networks:

Benefits
Logical Network Elements
Logical Network Architecture
Configuration Pushing Rules

Benefits

By using AmpCon-DC, you can push overlay service configurations more efficiently:

- **Enhanced flexibility and scalability**
  - Deploys logically isolated overlay networks rapidly without modifying underlay infrastructure
  - Supports Layer 2 and Layer 3 communication across VLAN Domains
- **Simplified configuration and management**
  - Automates network configuration pushing of overlay services through centralized control of AmpCon-DC
  - Visualizes overlay service deployment and streamlines overlay service operations and management
- **Improved resource utilization and cost efficiency**
  - Optimizes resource utilization through shared virtualization pools
  - Reduces hardware redundancy and reliance on dedicated hardware

Logical Network Elements

Logical network elements, designed to abstract the functions of the overlay network, serve as the intermediate representation between business intent and physical device configurations.

For example, the forwarding capability through L2 VNI is abstracted to logical switches, and the VRF L3 VNI forwarding capability is abstracted to logical routers.

The following logical network elements are involved in AmpCon-DC:

- **Logical networks**

  The core of overlay service provisioning. Like physical networks used for underlay provisioning, logical networks are logical space to provision overlay services.

A logical network holds other logical network elements, including logical routers, logical switches, and virtual networks, to instantiate an overlay service network.

- **Logical routers**

  The Layer 3 distributed routing network elements that connect logical switches and virtual routers. Similar to Layer 3 Virtual Network Instance (L3 VNI), logical routers are designed to enable Layer 3 communication across VLAN Domains and manage the pushing of VRF configurations.

  Logical routers employ the symmetric distributed routing technology. Gateway configurations are deployed on all server leaf switches that logical routers involve, enabling efficient near-source traffic forwarding.

  To deploy a logical network, you need to provision logical routers by adding the logical router to a logical network and then connecting the logical router with one or multiple logical switches.

- **Logical switches**

  The Layer 2 network elements that connect resources (such as physical servers and virtual machines) within the same service system. Logical switches exist only on server leaf switches and handle configuration pushing of gateway interfaces, Network Virtualization Edge (NVE), and Bridge Domain (BD).

  Developed based on EVPN VXLAN Layer 2 Bridge, logical switches enable Layer 2 connectivity across VLAN Domains. In addition, logical switches extend the VLAN capacity by bridging diverse VLAN IDs from different VLAN Domains to the same VXLAN Network Identifier (VNI), scaling up cloud platform networks efficiently.

  To provision a logical network, you need to provision logical switches by adding logical switches to the logical network and then connecting logical switches with virtual networks.

- **Virtual networks**

  Virtual networks are virtual Layer 2 network devices used in vSphere or bare metal Point of Delivery (PoD). The ports of virtual networks are attached to logical switches.

  In vSphere, the virtual network is called portgroup. In bare metal, the virtual network is called Virtual Layer 2 Switching (VL2).

  To provision a logical network, you need to add the virtual networks to the logical network.

Logical Network Architecture

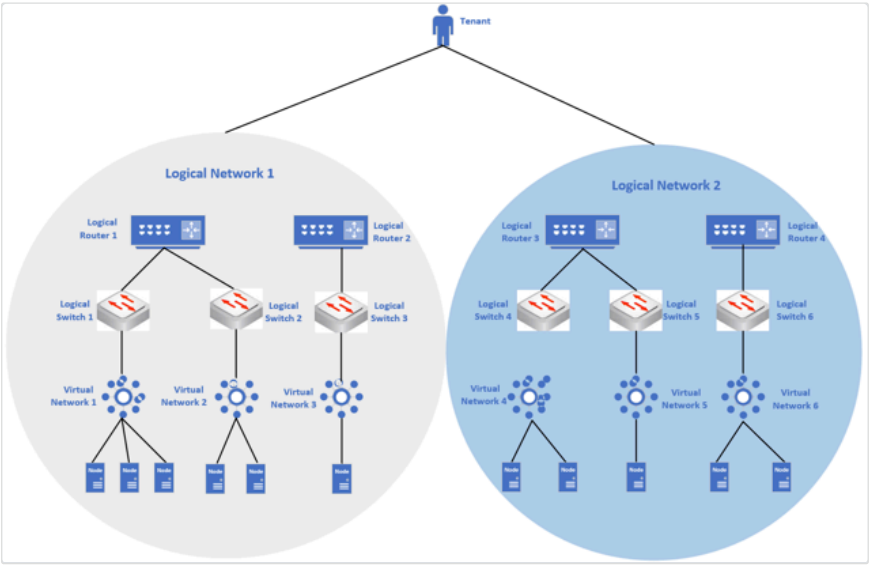
In AmpCon-DC, a tenant is a logical resource unit used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other.

Using tenants to manage logical networks provides the following benefits:

- **Resource control**
  You can create one or multiple tenants. A tenant has quotas for logical routers and logical switches. Logical networks owned by the tenant consume resources from these quotas, ensuring controlled resource usage.
- **Restricted resource scope**
  A tenant can only use the VPCs and fabrics bound to it. Therefore, logical networks owned by the tenant can add only virtual networks from these VPCs and can be deployed only on the associated fabrics.
- **Tenant isolation and access control**
  Tenants are isolated from each other. AmpCon-DC users can manage the tenants assigned to them. As a result, each AmpCon-DC user can manage only the logical networks owned by the tenants the user manages.

The architecture of logical networks in AmpCon-DC is as follows:

Figure 1. Logical Network Architecture



- A tenant can create one or multiple logical networks.
- A logical network can contain one or multiple logical routers.
- A logical router can connect with one or multiple logical switches.

- A logical switch can connect with at most one logical router. A logical switch can connect with at most one virtual network.
- A virtual network can connect with at most one logical switch.

Configuration Pushing Rules

To ensure precise configuration pushing while maintaining overlay service abstraction, AmpCon-DC pushes overlay service configurations based on the following rules:

- **Distributed configuration pushing**
  - All overlay service configurations are deployed in a distributed manner. Configurations are pushed to the specified leaf switches based on actual service provisioning, rather than broadcasting configurations to all leaf switches.
  - Logical network configurations are location-agnostic; distributed configurations are consistent across all involved leaf switches.
- **Role-based deployment scope**
  - Overlay service configurations are pushed only to server leaf switches and switches serving as both leaf and spine functions.
  - Provisioning a logical network applies entire overlay service configurations.
  - Provisioning each logical network element applies only the configurations related to the logical network element.

Deploying Logical Networks

You can deploy logical networks to meet your overlay service provisioning needs.

To deploy a logical network with AmpCon-DC, take the following steps:

- Guidelines
- Prerequisites
- Procedure
  - 1. Adding a Logical Network
  - 2. Adding Virtual Networks
  - 3. Provisioning Logical Switches
    - 3.1 Adding Logical Switches
    - 3.2 Connecting Logical Switches with Virtual Networks
  - 4. Provisioning Logical Routers
    - 4.1 Adding Logical Routers
    - 4.2 Connecting Logical Routers with Logical Switches
  - 5. Checking Provisioning Results
  - Optional: Viewing and Managing Logical Networks

Guidelines

In AmpCon-DC, a tenant is a logical resource unit used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other.

Using tenants to manage logical networks provides the following benefits:

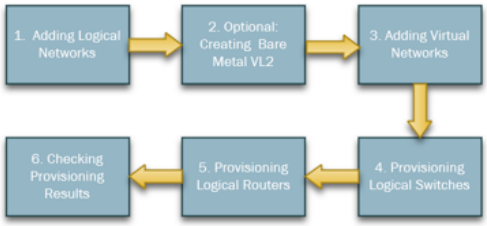
- **Resource Control**
  A tenant has quotas for logical routers and logical switches. Logical networks owned by the tenant consume resources from these quotas, ensuring controlled resource usage.
- **Restricted Resource Scope**
  A tenant can use only the VPCs and fabrics bound to it for logical network deployment. Therefore, logical networks owned by the tenant can add only virtual networks from these VPCs and can be deployed only on the associated fabrics.
- **Tenant Isolation and Access Control**
  Tenants are isolated from each other. AmpCon-DC users can manage the tenants assigned to them. As a result, each AmpCon-DC user can manage only the logical networks owned by the tenants the user manages.

Prerequisites

Ensure that all the prerequisites described in Logical Network Deployment Workflow - Prerequisites are met. Or else, the logical network deployment will fail.

Procedure

Figure 1. Logical Network Deployment Workflow



1. Adding a Logical Network

Add a logical network first. Follow these steps:

1. Log in to the AmpCon-DC UI with the prepared user, and then click **Service Provision > Logical Networks** from the navigation bar.
2. On the “Logical Networks” page, click **+ Logical Network**, and then input the following information:

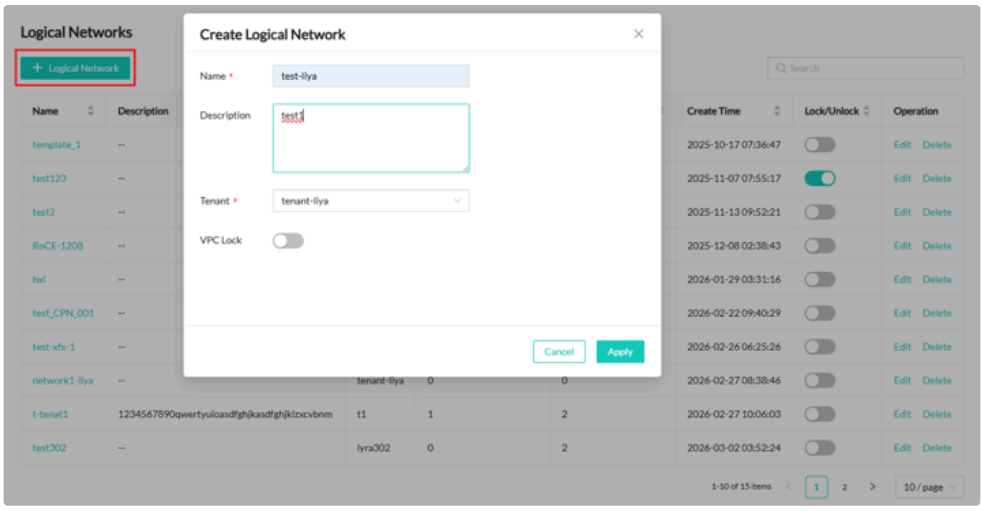


Table 1. Logical Network Parameters

Parameter	Description
Name	The name to distinguish the logical network. The name must be unique.
Description	Optional. The description of the logical network.
Tenant	The tenant who owns the logical network. **NOTE**

	Only the tenants managed by the currently logged-in user are shown in the drop-down list.
VPC Lock	Whether to lock the logical network so that it can't be deleted.

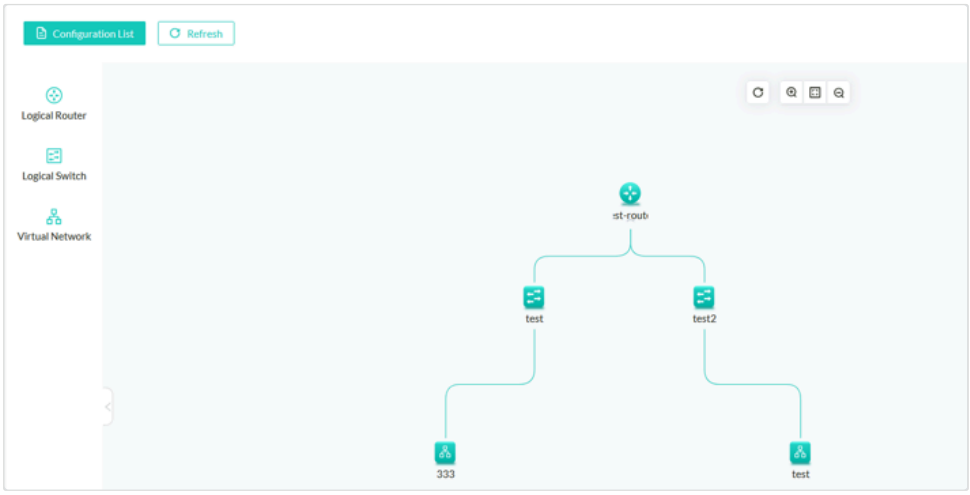
3. Click **Apply**.

2. Adding Virtual Networks

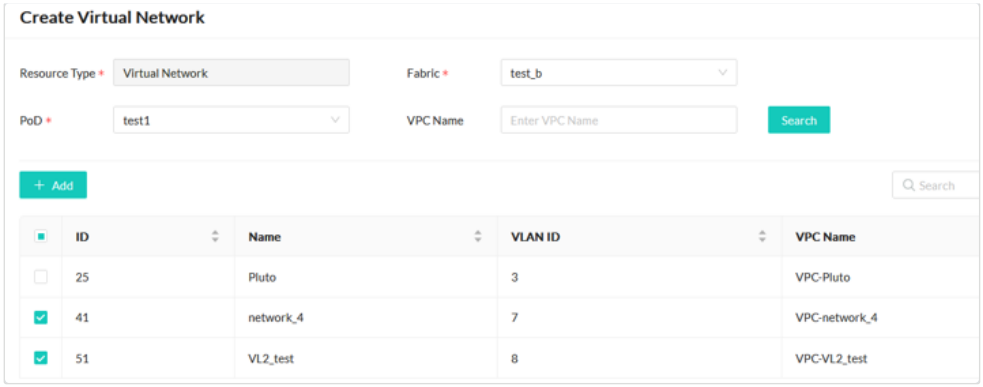
Add virtual networks to the logical network. Follow these steps:

> **NOTEs**
>
> - A logical network can contain one or multiple virtual networks.
> - Only the virtual networks of those VPCs that have been allocated to the tenant can be added to the logical network.

1. Click **Service Provision > Logical Networks** from the navigation bar.
2. On the "Logical Networks" page, click the name of the logical network to enter the logical network provisioning page.
3. Drag the virtual network icon to the logical network provisioning canvas.



4. In the pop-up window, filter virtual networks by using the following filters:



a. In the **Fabric** drop-down list, select a fabric.

> **NOTE**
>
> Only the fabrics that meet all of the following conditions can be displayed here:
>
> - The fabrics have been deployed.
> - The fabrics have VLAN Domains configured.
> - The fabrics are associated with the tenant of the logical network. To check fabrics associated with the tenant, see Viewing a Tenant.

b. In the **PoD** drop-down list, select a PoD.

> **NOTE**
>
> You can see only vSphere and bare metal PoD in the selected fabric. OpenStack PoD can't be used to deploy logical networks.

c. Optional: In the **VPC Name** field, enter the name of a VPC belonging to the selected PoD.

d. Click **Search**.

5. Select one or multiple virtual networks to be added to this logical network, and then click **+ Add**.
6. Optional: Repeat **Step 4** to **Step 5** to add virtual networks in other fabrics or PoD to the logical network.

3. Provisioning Logical Switches

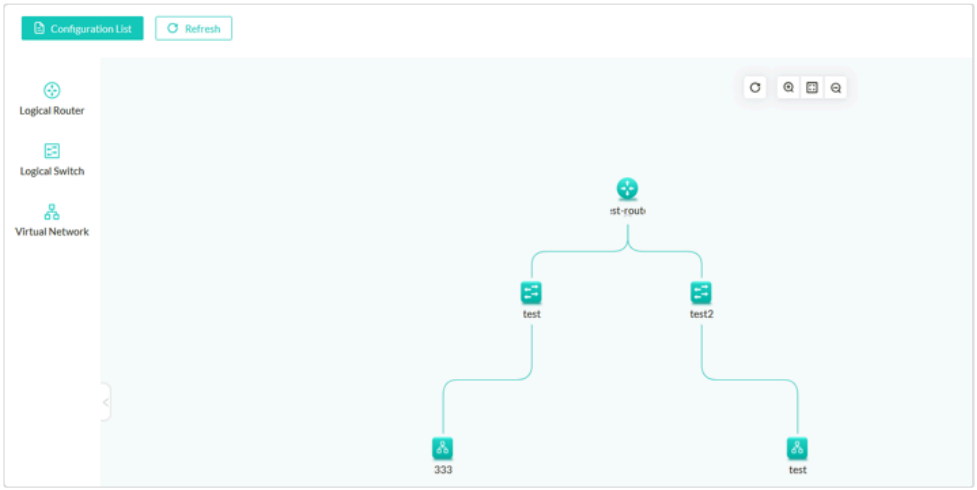
Provision logical switches by adding logical switches to the logical network and then connecting these logical switches with virtual networks. Follow these steps:

> **NOTEs**
>
> - A logical network can contain one or multiple logical switches.
> - Logical switches from multiple fabrics can be added to one logical network.
> - A virtual network can connect with at most one logical switch.
> - A logical switch can also connect with at most one virtual network from the same fabric.

3.1 Adding Logical Switches

Add logical switches to a logical network. Follow these steps:

1. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.



2. Drag the logical switch icon to the logical network provisioning canvas.
3. In the pop-up window, input the following information:

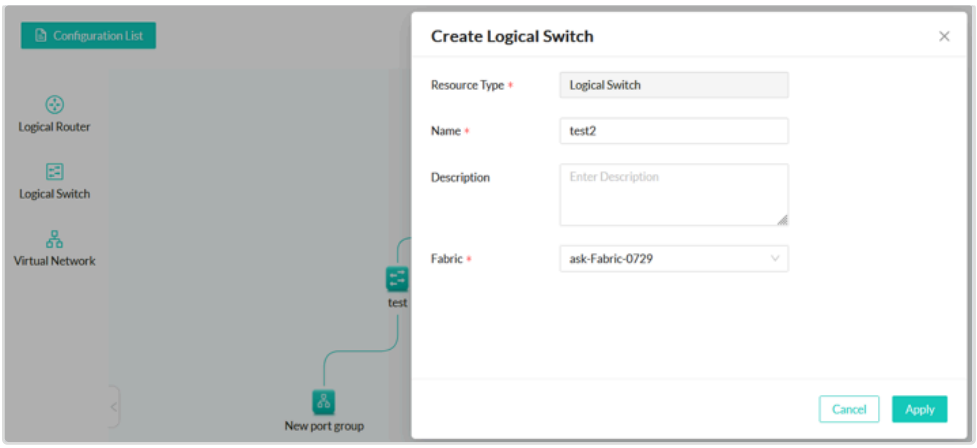


Table 2. Logical Switch Parameters

Parameter	Description
Name	The name to distinguish the logical switch. The name must be unique.
Description	Optional. The description of the logical switch.
Fabric	The fabric to which the logical switch belongs. **NOTE** Only the fabrics that meet all of the following conditions can be displayed here: • The fabrics have been deployed. • The fabrics have VLAN Domains configured. • The fabrics are associated with the tenant of the logical network.

4. Click **Apply**.

NOTE

If the tenant has already used the allowed maximum number of logical switches, an error message will appear.

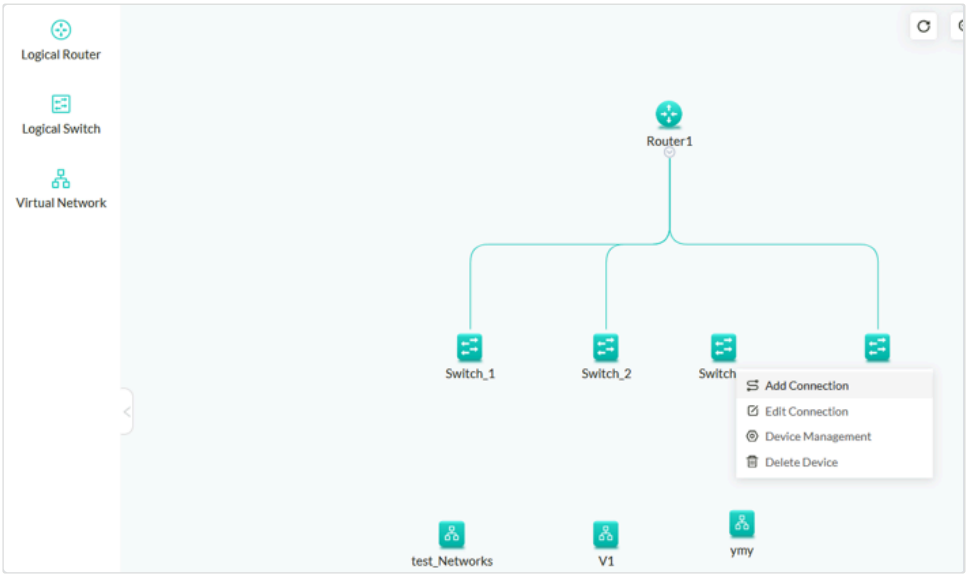
In this case, increase the logical switch quota for the tenant, or delete an existing logical switch and try again.

5. Optional: Repeat **Step 2** to **Step 4** to add more logical switches to the logical network.

3.2 Connecting Logical Switches with Virtual Networks

Connect logical switches with virtual networks. Follow these steps:

1. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
2. In the canvas, right-click an added logical switch, and then click **Add Connection**.



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

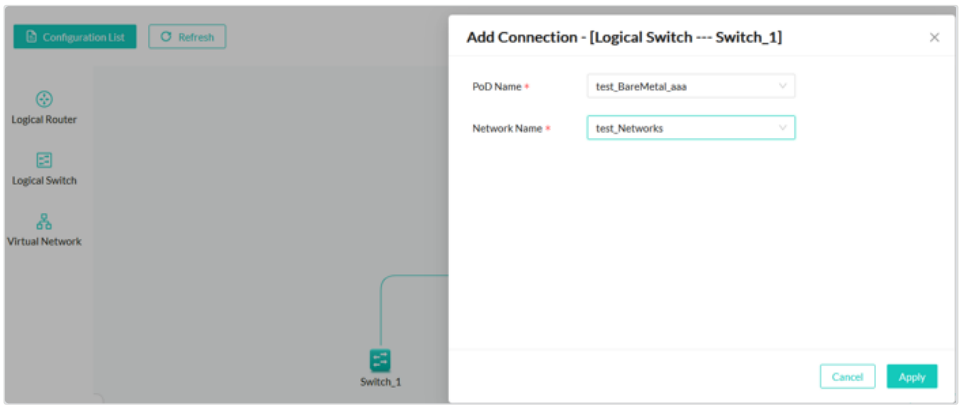


Table 3. Connection with Virtual Networks

Parameter	Description
PoD Name	The PoD of the virtual network to be connected with the logical switch. **NOTE**

	The **PoD Name** list contains only the PoD of the virtual networks that are added to the logical network.
Network Name	The name of the virtual network to be connected with the logical switch. **NOTE** The **Network Name** list displays only the virtual networks that meet all of the following conditions: • The virtual networks are added to the logical network. • The virtual networks are in the selected PoD.

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

NOTE

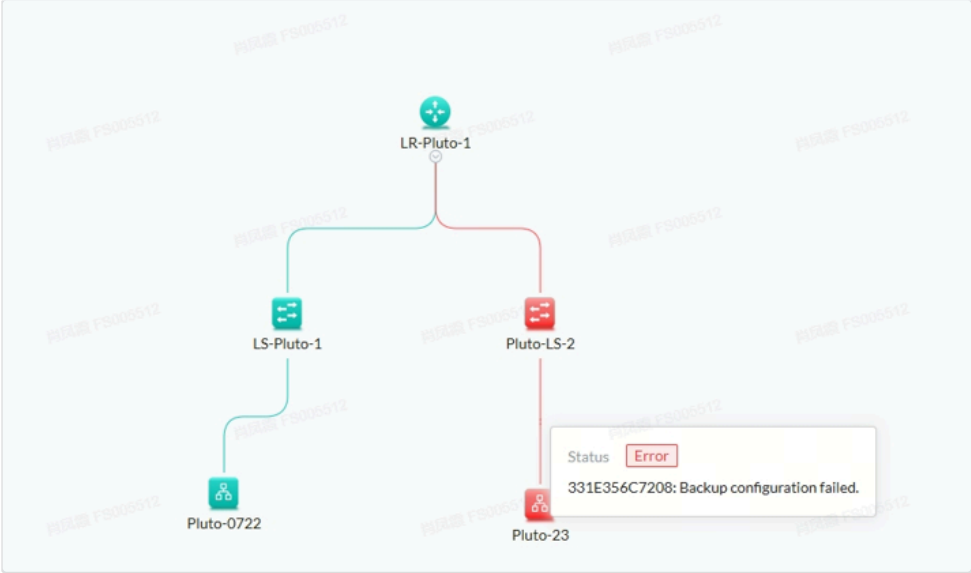
Only when the following prerequisites are met, can overlay service configurations be pushed to the related server leaf switches:

- The server leaf switches are online, which means the server leaf switches are up and connected with the AmpCon-DC server.
- The logical switches are connected with one or multiple virtual networks.
- If logical switches are connected with bare metal virtual networks named VL2, ensure that the VL2 is associated with node devices.

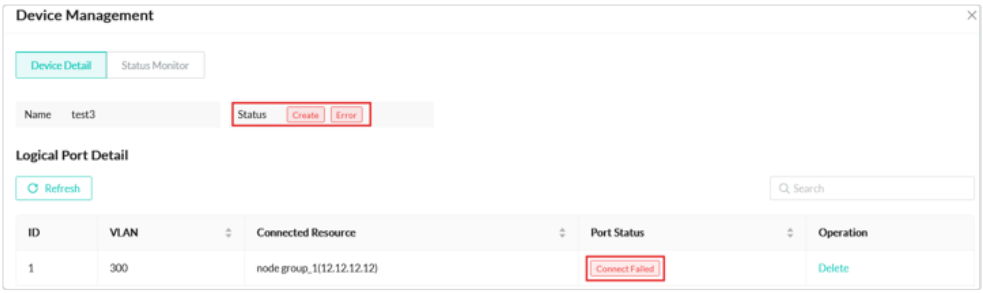
5. Check whether the connection is successful.

   The line between the logical switch and the virtual network is in green when the connection succeeds and is in red when the connection fails.

   To check for failure information, hover over the red line.



Or, you can right-click the logical switch and then click **Device Management**. Check the **Status** and **Port Status** information.



6. Optional: Repeat **Step 2** to **Step 5** to connect other logical switches with virtual networks.

4. Provisioning Logical Routers

Provision logical routers by adding the logical router to a logical network and then connecting the logical router with one or multiple logical switches. Follow these steps:

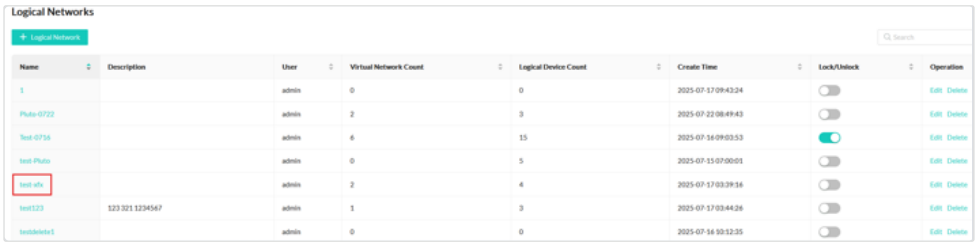
NOTEs

- A logical network can contain one or multiple logical routers.
- Logical routers from multiple fabrics can be added to one logical network.
- A logical network can work without logical routers.
- A logical router can connect to one or multiple logical switches in the same fabric.
- A logical switch can connect to at most one logical router in the same fabric.

4.1 Adding Logical Routers

Add logical routers to a logical network. Follow these steps:

1. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.



2. Drag the logical router icon to the logical network provisioning canvas.
3. In the pop-up window, input the following information:

> **NOTEs**
>
> - **L3 Anycast MAC Range**, the range of virtual MAC addresses assigned to Layer 3 anycast gateways, is assigned automatically by AmpCon-DC.
> - **Fabric**, **VRF Mode**, and **VRF Name** can’t be modified after configured. If the configurations of a logical router can’t meet your needs, delete it and then create a new logical router.

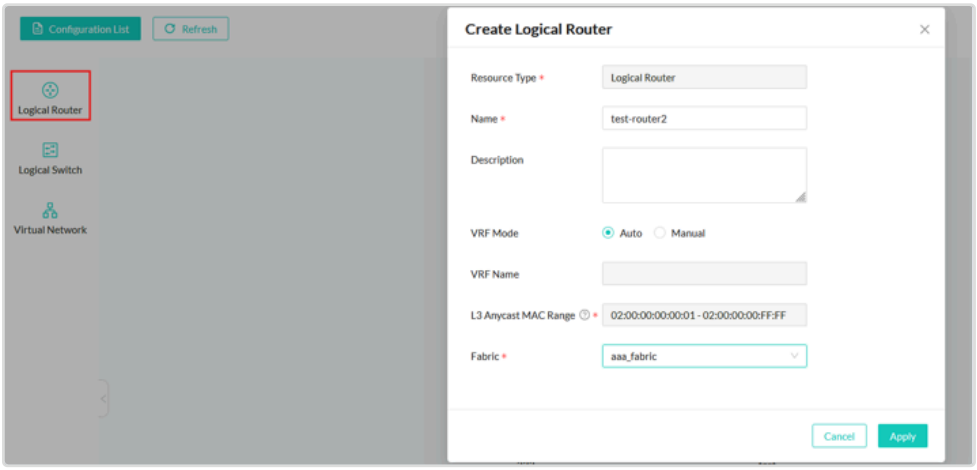


Table 4. Logical Router Parameters

Parameter	Description
Name	The name to distinguish the logical router. The name must be unique.

Description	Optional. The description of the logical router.
VRF Mode	**Manual** or **Auto**. • **Manual** means you need to enter the VRF name manually in the **VRF Name** field. • **Auto** means AmpCon-DC automatically designates a VRF name.
Fabric	The fabric to which the logical router belongs. **NOTE** Only the fabrics that meet all of the following conditions can be displayed here: • The fabrics have been deployed. • The fabrics have VLAN Domains configured. • The fabrics are associated with the tenant of the logical network.

4. Click **Apply**.

> **NOTE**
>
> If the tenant has already used the allowed maximum number of logical routers, an error message will appear.
>
> In this case, increase the logical router quota for the tenant, or delete an existing logical router and try again.

5. Optional: Repeat **Step 2** to **Step 4** to add more logical routers to the logical network.

4.2 Connecting Logical Routers with Logical Switches

Connect logical routers with logical switches. Follow these steps:

1. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
2. In the canvas, right-click an added logical router, and then click **Add Connection**.
3. In the pop-up window, input the following information:

NOTEs

- **Connection Type** means the logical network element to which the logical router connects. Currently, you can see only **Logical Switch**.
- In the **Connection Device** drop-down list, you can see only the added logical switches in the same fabric as the logical router.
- **Virtual IPv4 Range**, the range of virtual IP addresses used by MLAG, is automatically assigned by AmpCon-DC based on the following rules and can't be changed manually:
  - **Virtual IPv4 Range** doesn't overlap with **Anycast IPv4**.
  - **Virtual IPv4 Range** doesn't overlap with IP addresses of node devices.
  - The subnet of **Virtual IPv4 Range** and **Anycast IPv4** needs to be same.

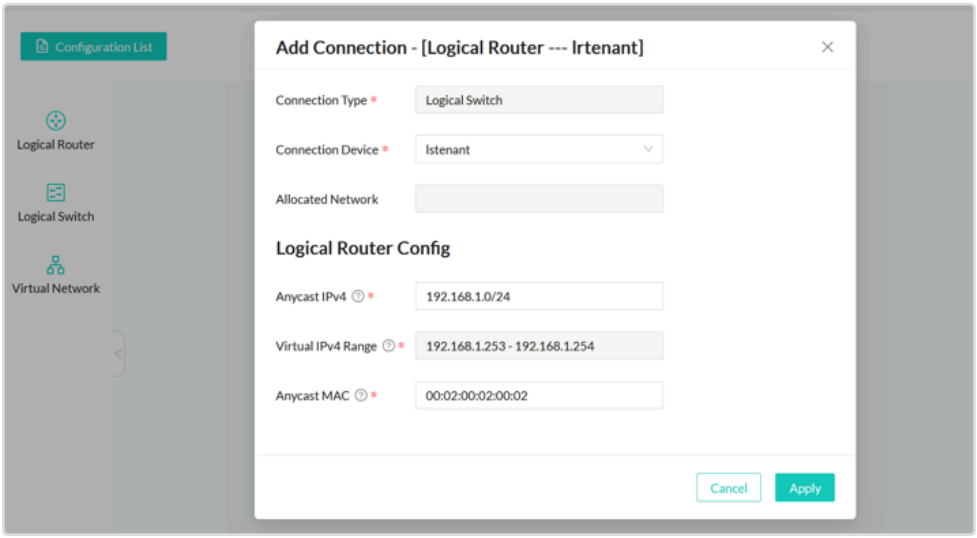


Table 5. Connection with Logical Switches

Parameter	Description
Connection Device	The logical switch to be connected.
Allocated Network	The virtual network to which the logical switch connects. The parameter is displayed only if the logical switch has been provisioned to connect with a virtual

	network.
Anycast IPv4	The IPv4 address of the anycast gateway. **NOTE** The Anycast IPv4 value must be in xx.xx.xx.xx/xx format (such as 192.168.1.1/24) and can't overlap with other Anycast IPv4 values.
Anycast MAC	The MAC address used by the Layer 3 interface related to the Layer 2 VNI. **NOTEs** • The default value is **00:02:00:02:00:02**. • The value must be an anycast MAC address.

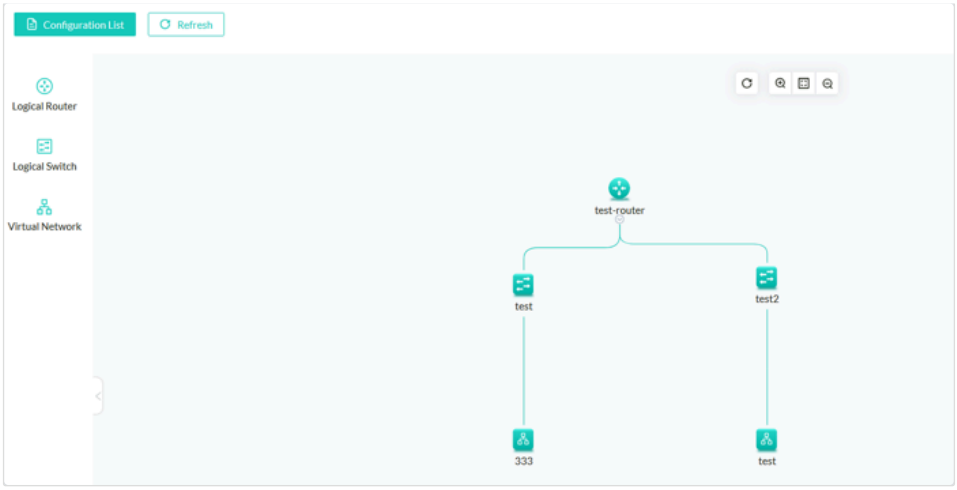
4. Click **Apply** to complete the connection.

> **NOTE**
>
> Only when the following prerequisites are met, can overlay service configurations be pushed to the related server leaf switches:
>
> - The server leaf switches are online, which means the server leaf switches are up and connected with the AmpCon-DC server.
> - The logical switches are connected with one or multiple virtual networks.
> - If logical switches are connected with bare metal virtual networks named VL2, ensure that the VL2 is associated with node devices.

5. Check whether the connection is successful.

   The line between the logical router and the logical switch is in green when the connection succeeds and is in red when the connection fails.

   To check for failure information, hover over the red line.



6. Optional: Repeat **Step 2** to **Step 5** to connect other logical routers with logical switches.

5. Checking Provisioning Results

Check provisioning results to see whether the overlay service configurations are pushed successfully.

For more information, see Viewing Logical Networks.

Optional: Viewing and Managing Logical Networks

After you deploy logical networks, you can view and manage these logical networks. For more information, see Managing Logical Networks.

Creating Bare Metal VL2s

Virtual networks are virtual Layer 2 network devices in bare metal PoD. The ports of virtual networks are attached to logical switches. In bare metal PoD, the virtual network is called Virtual Layer 2 Switching (VL2).

When you add vSphere PoD, virtual networks are retrieved automatically from the vSphere cloud platform. But when you create a bare metal PoD, no virtual networks exist in the bare metal PoD.

If you need to add virtual networks of bare metal PoD to a logical network, you must create a VL2 for the bare metal PoD, and then associate bare metal node devices with the VL2.

Prerequisites
Procedure
1. Adding a VL2
2. Associating Bare Metal Nodes with a VL2
Optional: Viewing and Managing VL2s

Prerequisites

Before you add a VL2, ensure that you have completed all of the following operations:

- Ensure that you have completed the physical network (fabric) deployment through simplified ZTP or physical network design. For more information, see Simplified ZTP Deployment and Designing Physical Networks.
- Ensure that you have completed VLAN Domain configuration for the fabric. For more information, see VLAN Domains.
- Ensure that you have created the bare metal PoD to which the VL2 belongs. For more information, see Bare Metal PoD.
- Ensure that you have added bare metal node group configurations. For more information, see Configuring Node Uplink for Bare Metal Nodes.
- Ensure that the currently logged-in user is granted built-in or custom roles with the Read and Write permissions to the “Network Access” page. For more information, see Managing Roles.

Procedure

1. Adding a VL2

To add a VL2, follow these steps:

1. In the AmpCon-DC UI, click **Service Provision > Network Access** from the navigation bar.

2. On the “Network Access” page, click **+ VL2**.

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

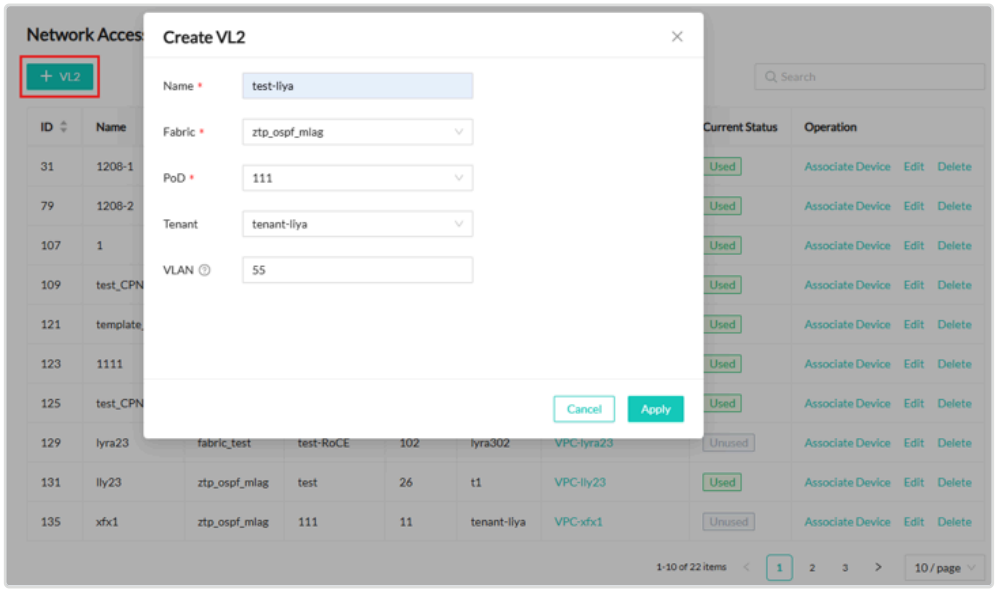


Table 1. VL2 Parameters

Parameter	Description
Name	The name of the VL2. The name must be unique.
Fabric	The fabric to which the VL2 belongs. **NOTE** In the **Fabric** drop-down list, you can see only the fabrics that have been deployed and have VLAN Domains configured. For more information, see Deploying Physical Networks and VLAN Domains.
PoD	The bare metal PoD to which the VL2 belongs. **NOTE** Only the bare metal PoD in the selected fabric are shown in the **PoD** drop-down list.
Tenant	Optional. The tenant to which the VPC of the VL2 is allocated. **NOTEs**

	• If you want to associate bare metal nodes with the VL2 later, you must allocate the VPC of the VL2 to a tenant here. • Only the tenants who meet all of the conditions are shown in the **Tenant** drop-down list: ◦ The tenant managed by the currently logged-in user. ◦ The tenant associated with the selected fabric. • If you don't select any tenant here, the **Tenant** metric on the "Network Access" page is displayed as **--**.
VLAN	Optional. The VLAN ID of the VL2. **NOTEs** • If you don't enter any VLAN value here, AmpCon-DC will automatically assign a VLAN ID from the **Global VLAN** range of the PoD. To check the **Global VLAN** range of a bare metal PoD, see Viewing a Bare Metal PoD. • If you enter a VLAN ID here, ensure that the VLAN ID is in the intersections between the **Global VLAN** range of the PoD and the **Bridge Domain Range** of the related VLAN Domain, and the entered VLAN ID is not used by other VL2s of the same PoD. Or else, the logical network will fail to be deployed. To check the **Bridge Domain Range** of a bare metal PoD, see Viewing All VLAN Domains in a Fabric. • VL2s in the same bare metal PoD will be assigned with different VLAN IDs, while

	VL2s in different bare metal PoD can be assigned with the same VLAN ID.

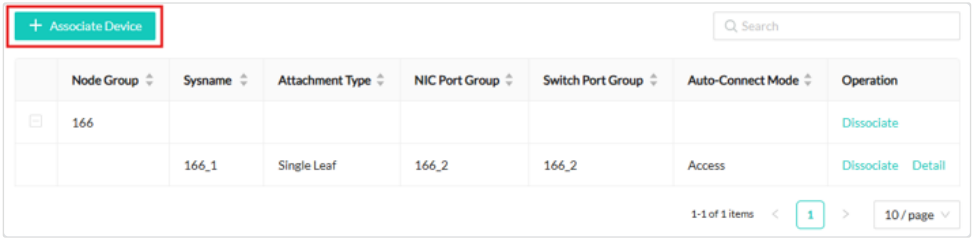
4. Click **Apply**.

2. Associating Bare Metal Nodes with a VL2

After you create a VL2, you must associate bare metal nodes with the VL2. Or else, when you connect a logical switch with the VL2, the configurations might fail to be pushed to leaf switches.

> **NOTEs**
>
> - Before associating bare metal nodes with a VL2, you must allocate the VPC of the VL2 to a tenant.
> - If the VPC of a VL2 is not allocated to any tenant when you add the VL2, to allocate the VPC to a tenant, locate the VL2, and then click **Edit**.
>
> You can also allocate the VPC through the **PoD** tab of the "Resource Interconnection" page. For more information, see Allocating VPCs to Tenants.

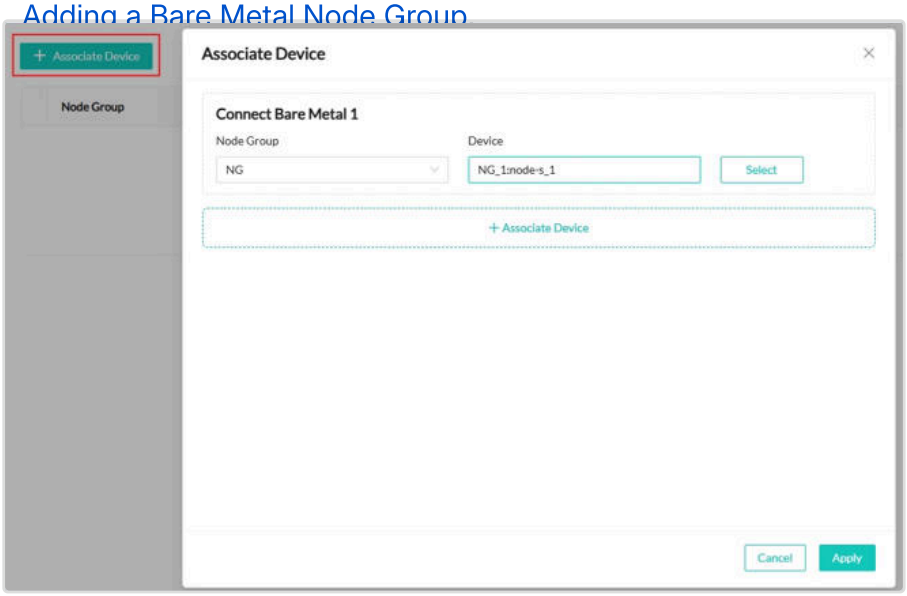
1. Locate the VL2 on the “Network Access” page, and then click **Associate Device**.
2. On the “Associate Device” page, click **+ Associate Device**.



3. In the pop-up window, associate one or multiple devices as follows:
   a. Click **+ Associate Device**.
   b. In the **Node Group** drop-down list, select a bare metal node group you have created.

> **NOTE**
>
> If you haven’t added bare metal node groups for the bare metal PoD to which the VL2 belongs, you can’t see any node group in

the **Node Group** drop-down list. For more information, see Adding a Bare Metal Node Group.



c. In the **Device** field, click **Select**. In the pop-up windows, select one or multiple bare metal nodes and NIC port groups to be added to the VL2.

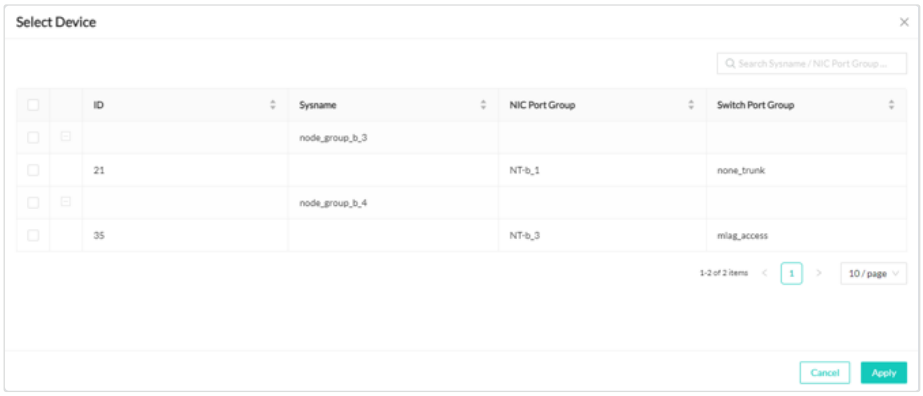


Table 2. Device Metrics

Metric	Description
ID	The ID assigned by AmpCon-DC for clarity.
Sysname	The hostname of the node device in the bare metal node group.
NIC Port Group	The NIC port group assigned to the bare metal node.
Switch Port Group	The switch port group assigned to the bare metal node.

d. Click **Apply** to complete the device selection.

e. Optional: Repeat **Step a** to **Step d** to associate the VL2 with more bare metal nodes as needed.

To delete any associated bare metal nodes, click the delete icon.

4. Click **Apply** to complete the device association.

Optional: Viewing and Managing VL2s

You can view, edit, or delete the added VL2s. And you can dissociate bare metal nodes with the VL2s. For more information, see Viewing and Managing VL2s.

Viewing and Managing VL2s

After you create bare metal VL2s, you can view and manage these VL2s as follows:

Viewing all VL2s
Editing a VL2
Deleting a VL2
Viewing All Associated Node Groups
Viewing Details of Associated Bare Metal Nodes
Dissociating Bare Metal Nodes from a VL2

Viewing all VL2s

1. In the AmpCon-DC UI, click **Service Provision > Network Access** from the navigation bar.
2. On the “Network Access” page, check the following information:

> **NOTEs**
>
> - If you log in to the AmpCon-DC UI with a user who is assigned only the Tenant Administrator role, or only the Tenant Administrator role and the ReadOnly role, you can see only the VL2s whose VPCs are allocated to the tenants managed by the user.
> - For other logged-in AmpCon-DC users, you can see all VL2s here.

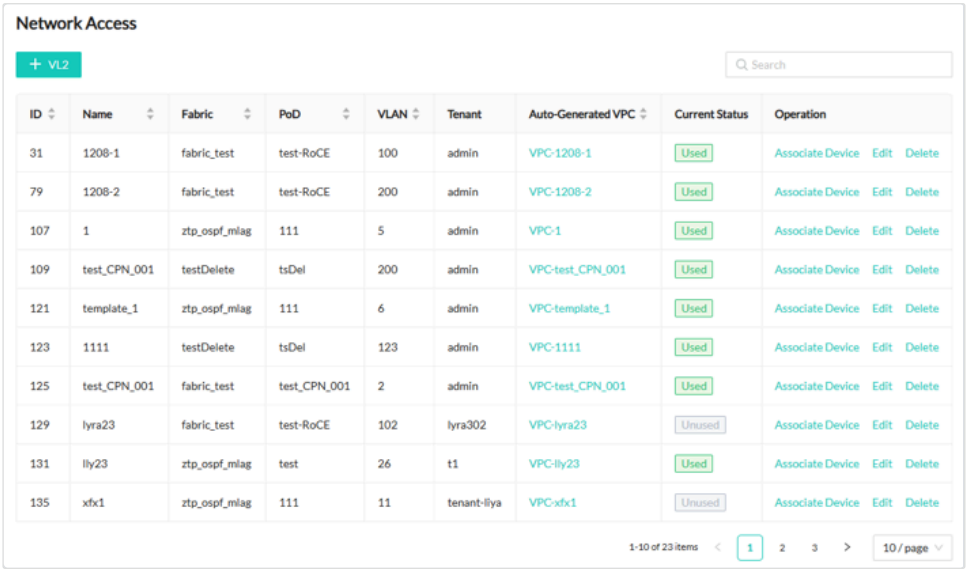


Table 1. VL2 Metrics

Metric	Description

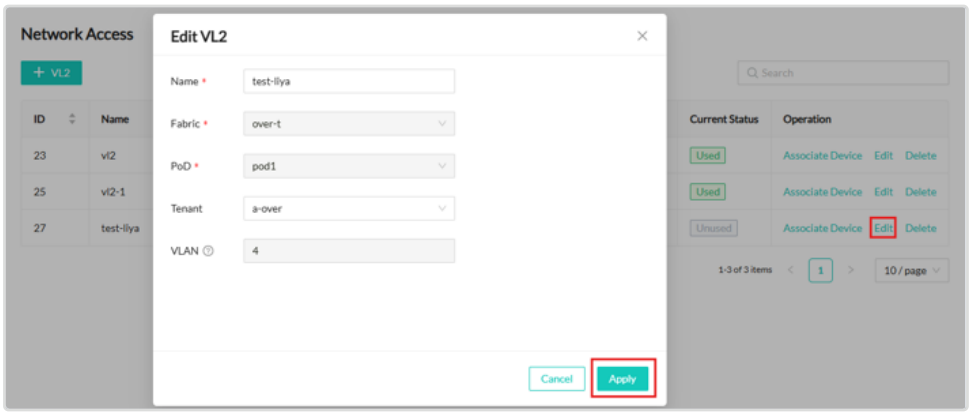
Name	The name of the VL2.
Fabric	The fabric to which the VL2 belongs.
PoD	The PoD to which the VL2 belongs.
VLAN	The VLAN ID of the VL2.
Tenant	The tenant to which the VL2 belongs. **NOTEs** • The value is **admin** if the VPC is created and used in a logical network in AmpCon-DC 2.4. • The value is ***** if the VPC is allocated to a tenant that is not managed by the currently logged-in user. • The value is **--** if the VPC is not allocated to any tenant.
Auto-Generated VPC	The VPC to which the VL2 belongs. The name of the VPC is generated by AmpCon-DC automatically and cannot be changed.
Current Status	Indicates whether the VPC of the VL2 is used in a logical network, **Used** or **Unused**. • **Used**: The VPC of the VL2 is used in a logical network. • **Unused**: The VPC of the VL2 is not used in any logical network. **NOTE** Hover over the **Unused** status. You can see **Device Associated** or **No Device Associated**, which means whether any device is associated with the VL2.

Editing a VL2

1. Locate the VL2 on the “Network Access” page, and then click **Edit**.
2. In the pop-up window, modify the **Name** as needed. The **Name** cannot be empty.

   You can modify the **Tenant** if the VPC of the VL2 is not used in any logical network. The **Tenant** cannot be modified to empty if the VPC of the VL2 is already allocated to a tenant.

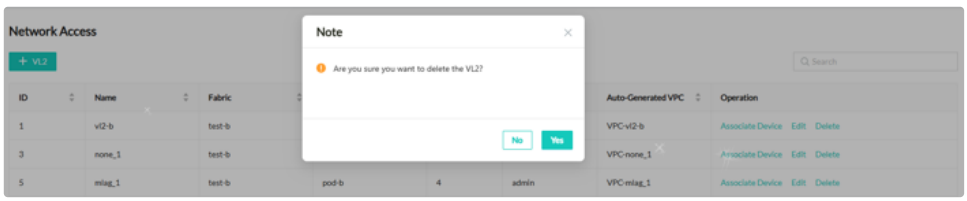
   You are not allowed to modify the **Fabric**, **PoD**, and **VLAN**.
3. Click **Apply**.



Deleting a VL2

To delete a VL2 of a bare metal PoD from the “Network Access” page, follow these steps:

1. If some bare metal nodes are associated with the VL2, dissociate all the bare metal nodes from the VL2. For more information, see the Dissociating Bare Metal Nodes from a VL2 section.
2. If the VL2 is added to a logical network, delete the VL2 from the logical network first. For more information, see Deleting a Virtual Network.
3. Click **Service Provision > Network Access** from the navigation bar.
4. Locate the VL2 on the “Network Access” page, and then click **Delete**.
5. In the pop-up window, click **Yes**.



Viewing All Associated Node Groups

1. Locate the VL2 on the “Network Access” page, and then click **Associate Device**.
2. On the “Associate Device” page, check all associated node groups.

To see bare metal nodes of each associated node group, click the icon **+**.

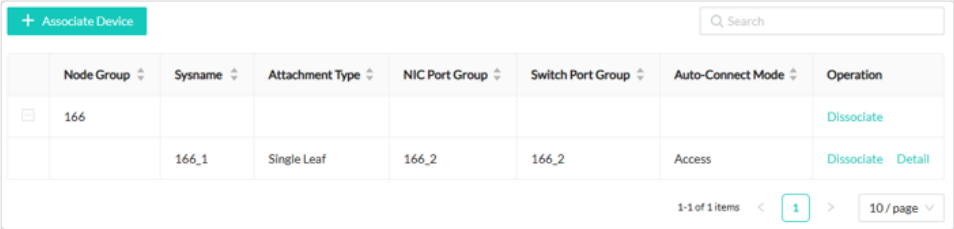


Table 2. Node Group Metrics

Metric	Description
Node Group	The name of the node group associated with the VL2.
Sysname	The name of the bare metal node.
Attachment Type	The method used to connect devices with leaf switches. • **Single Leaf:** The node device connects to a non-MLAG leaf switch. • **MLAG Leaf:** The node device connects to one or two leaf switches in an MLAG setup.
NIC Port Group	The name of the NIC port group.
Switch Port Group	The name of the switch port group.
Auto-Connect Mode	The port mode used by the node device to connect to the leaf switch, **Access** or **Trunk**.

Viewing Details of Associated Bare Metal Nodes

1. On the “Associate Device” page, locate a bare metal node, and then click **Detail**.
2. Check detailed connection information of the bare metal node:

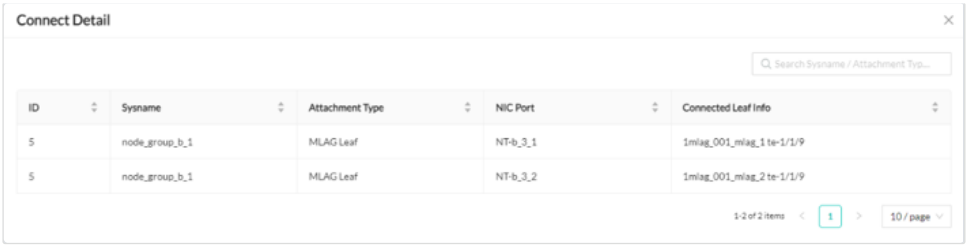


Table 3. Node Metrics

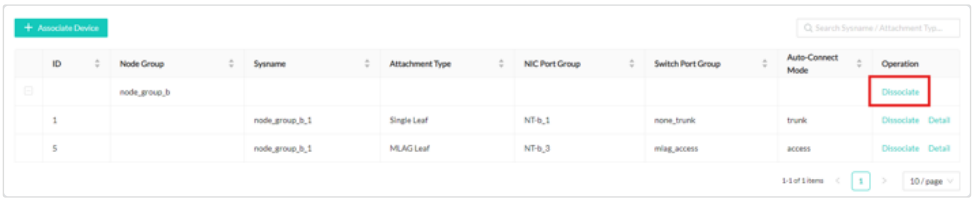
Metric	Description
ID	The ID assigned by AmpCon-DC for clarity.
Sysname	The name of the bare metal node.
Attachment Type	The method used to connect devices with leaf switches. • **Single Leaf**: The node device connects to a non-MLAG leaf switch. • **MLAG Leaf**: The node device connects to one or two leaf switches in an MLAG setup.
NIC Port	The port contained in the NIC port group to connect to the logical switch.
Connected Leaf Info	The leaf switch and switch port associated with the NIC port.

Dissociating Bare Metal Nodes from a VL2

> **NOTE**
>
> Before you dissociate bare metal nodes from a VL2, disconnect the connections between the logical switch and the virtual network of the bare metal nodes. For more information, see Disconnecting Connections of Logical Switches and Virtual Networks.

1. On the “Network Access” page, locate the VL2 with which you want to dissociate bare metal nodes, and then click **Associate Device**.
2. On the “Associate Device” page, dissociate one or multiple bare metal nodes associated with the VL2.

- To dissociate all bare metal nodes in a node group, locate the node group, and then click **Dissociate**.



- To dissociate a single bare metal node, locate the bare metal node, and then click **Dissociate**.

3. In the pop-up window, click **Yes**.

Managing Logical Network Elements

After you deploy logical networks, you can manage logical network elements, including logical networks, logical switches, and logical routers.

See the following child topics:

- Managing Logical Networks
- Managing Logical Switches
- Managing Logical Routers

Managing Logical Networks

After you deploy logical networks, you can manage these logical networks as follows:

- Viewing Logical Networks
  - Viewing All Logical Networks
  - Viewing Details of a Logical Network
  - Viewing Details of a Logical Switch or Logical Router
  - Viewing Details of a Virtual Network
- Editing Logical Networks
- Deleting Logical Networks
- Disconnecting Connections in a Logical Network
  - Disconnecting Connections of Logical Switches and Virtual Networks
  - Disconnecting Connections of Logical Switches and Logical Routers
- Deleting Logical Elements from a Logical Network
  - Deleting a Logical Switch
  - Deleting a Logical Router
  - Deleting a Virtual Network

Viewing Logical Networks

Viewing All Logical Networks

1. In the AmpCon-DC UI, click **Service Provision > Logical Networks** from the navigation bar.
2. On the “Logical Networks” page, check the following information:

> **NOTEs**
>
> - If you log in to the AmpCon-DC with the built-in user **admin**, you can see all logical networks here.
> - For other AmpCon-DC users, you can see only the logical networks belonging to the tenants managed by the currently logged-in user.

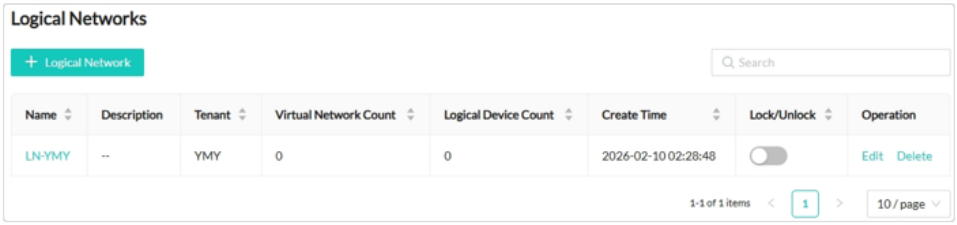


Table 1. Logical Network Metrics

Metric	Description

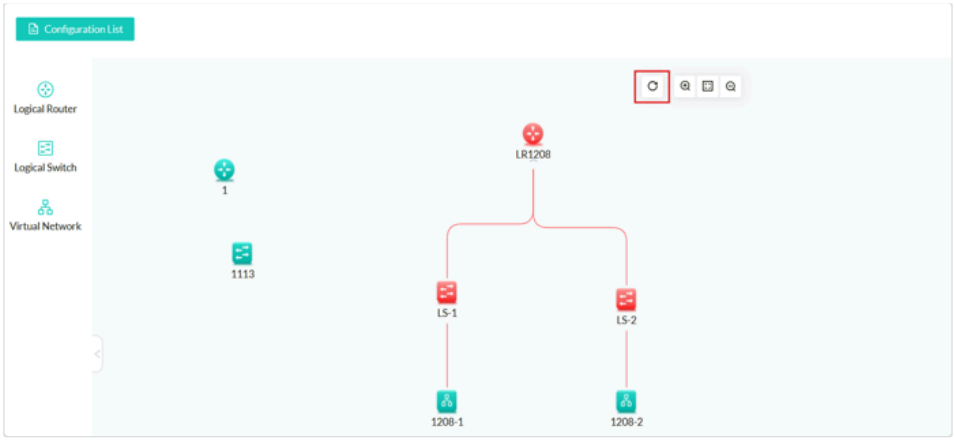
Name	The name to distinguish the logical network.
Description	The description of the logical network.
Tenant	The tenant who owns the logical network. **NOTE** The value is **admin** if the logical network was created in AmpCon-DC 2.4. These logical networks can be viewed and managed only by the built-in user **admin**.
Virtual Network Count	The total number of virtual networks in the logical network. If you haven't added virtual networks, the value is 0.
Logical Device Count	The total number of logical devices (logical routers and logical switches) in the logical network. If you haven't added logical routers and logical switches, the value is 0.
Create Time	The time when the logical network was added.
Lock/Unlock	Whether the logical network is locked. If a logical network is locked, it can't be deleted. You can toggle it on to lock the logical network or toggle it off to unlock the logical network.

Viewing Details of a Logical Network

1. On the "Logical Networks" page, click the name of the logical network to enter the logical network provisioning page.

   You can see the added logical network elements and topology if you have provisioned the logical network before.

   To check the latest topology, click the **Refresh** icon.



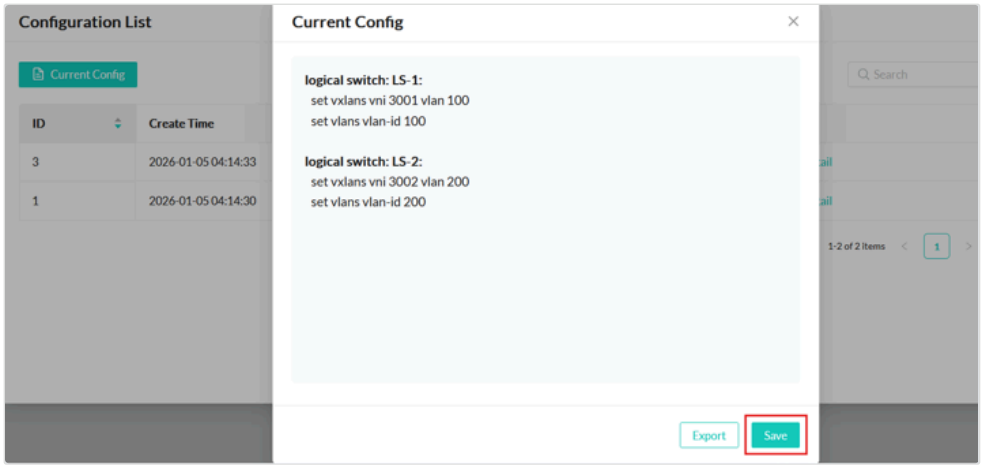
2. Click **Configuration List** to check the configurations of the logical network.

   In the pop-up window, you can see the list of all historically saved configuration items, the time when each configuration item is saved, and the descriptions.

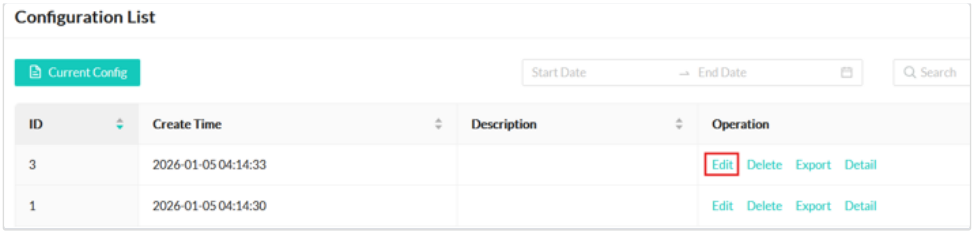
> **NOTE**
>
> Only overlay configurations pushed through provisioning logical networks are displayed.

   You can do the following operations:

- To save the current overlay configurations to the configuration list, click **Current Config**, and then click **Save**.



- To edit the description of a configuration item, locate the configuration item, and then click **Edit**.



- To delete a configuration item, locate the configuration item, and then click **Delete**.
- To export a configuration item to your local machine, locate the configuration item, and then click **Export**.
- You can filter configuration items through the fuzzy search and time selector.
  - In the search box, enter the keywords to filter a configuration item.
  - In the time selector, specify the start time and end time to filter the configurations items to be checked.
- To check detailed configurations in a configuration item, locate the configuration item, and then click **Detail**.

Viewing Details of a Logical Switch or Logical Router

On the logical network provisioning page, right-click an added logical switch or logical router, and then click **Device Management**.

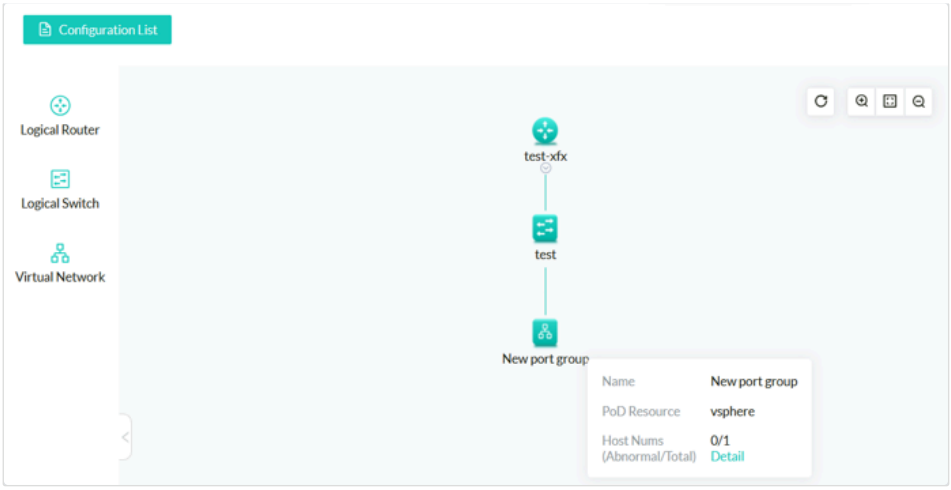
For more information, see Viewing Logical Switches and Viewing Logical Routers.

Viewing Details of a Virtual Network

After a virtual network is connected with a logical switch, you can view details of the virtual network. Follow these steps:

1. On the logical network provisioning page, hover over the virtual network. You can see the VL2 name, the PoD to which the virtual network belongs, and the abnormal and total count of node devices associated with the virtual network.

   The **Abnormal** status means that node devices are not connected with any switches or configurations can’t be pushed successfully.



2. Click **Detail** to check how node devices in the virtual network connect with leaf switches.

> **NOTE**
>
> The information listed here is based on the node uplink configurations when you add cloud platform node uplink configurations or add bare metal node groups.

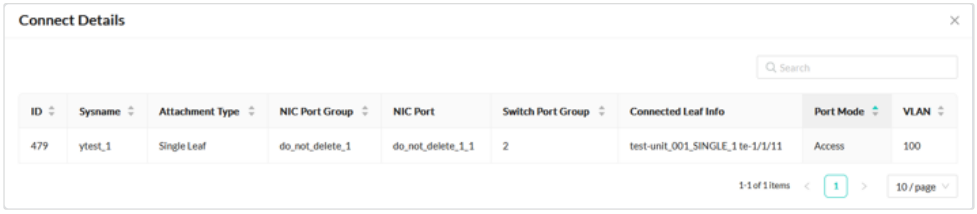


Table 2. Node Metrics

Metric	Description
Sysname	The hostname of the node device connected with the virtual network.
Attachment Type	Select **Single-Homed** or **Dual-Homed**. • **Single-Homed:** The node device connects to one **peer leaf switch** in the MLAG setup. • **Dual-Homed:** The node device connects to both peer leaf switches in the MLAG setup.
NIC Port Group	The NIC port group of the node device. A NIC port group is a logical aggregation of multiple network interface cards (NICs) of node devices. A

	NIC port group contains one or multiple NICs.
NIC Port	The NIC port contained in the NIC port group to connect to the leaf switch.
Switch Port Group	The switch port group of the connected leaf switch. A switch port group is a logical grouping of multiple switch ports for centralized management, policy enforcement, or traffic optimization. A switch port group contains one or multiple switch ports.
Connected Leaf Info	The leaf switch and the NIC port to which the node device connects.
Port Mode	The port mode used by the node device to connect with the leaf switch, **Access** or **Trunk**.
VLAN	The VLAN to which the node device belongs.

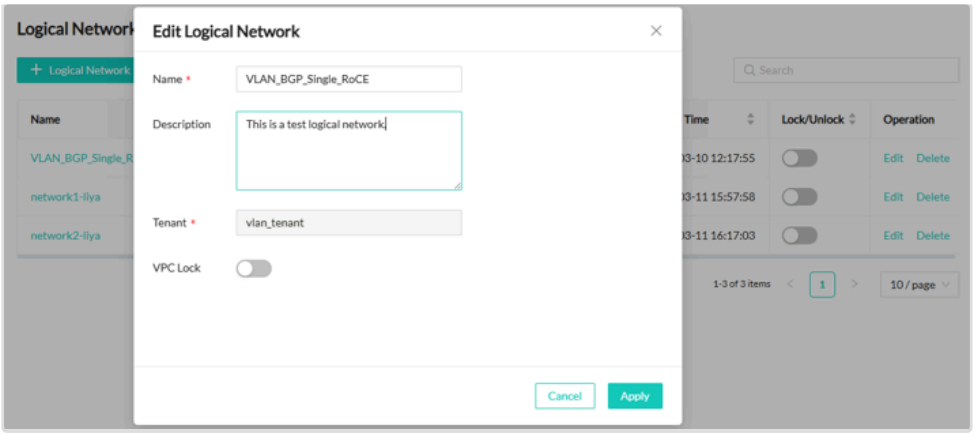
Editing Logical Networks

1. On the “Logical Networks” page, locate the logical network, and then click **Edit**.



2. In the pop-up window, modify the logical network name or description, or click the **VPC Lock** toggle to unlock or lock the logical network.

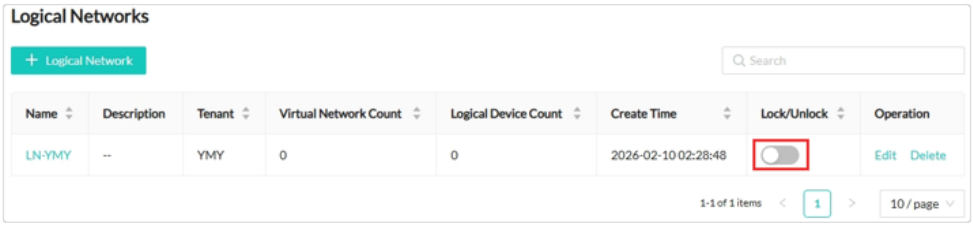
> **NOTEs**
>
> - The logical network cannot be deleted if it is locked.
> - The **Tenant** field can’t be edited.



Deleting Logical Networks

To delete a logical network, follow these steps:

1. On the “Logical Networks” page, ensure that the logical network to be deleted is not locked. If a logical network is locked, click the toggle to unlock it.

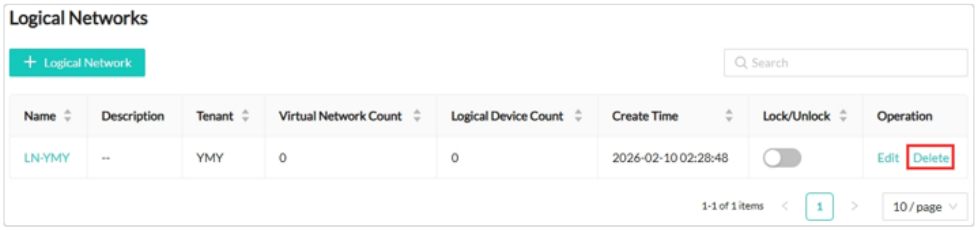


2. Click the name of the logical network to enter the logical network provisioning page. On this page, ensure that no connections exist in the logical network.

   If any connections exist between the logical network elements, disconnect these connections. For more information, see Disconnecting Connections in a Logical Network.

3. Go back to the “Logical Networks” page, locate the logical network, and then click **Delete**.

   After deletion, the logical routers, logical switches, and VPCs resources of the deleted logical network are released. The VPCs are still owned by their original tenant.

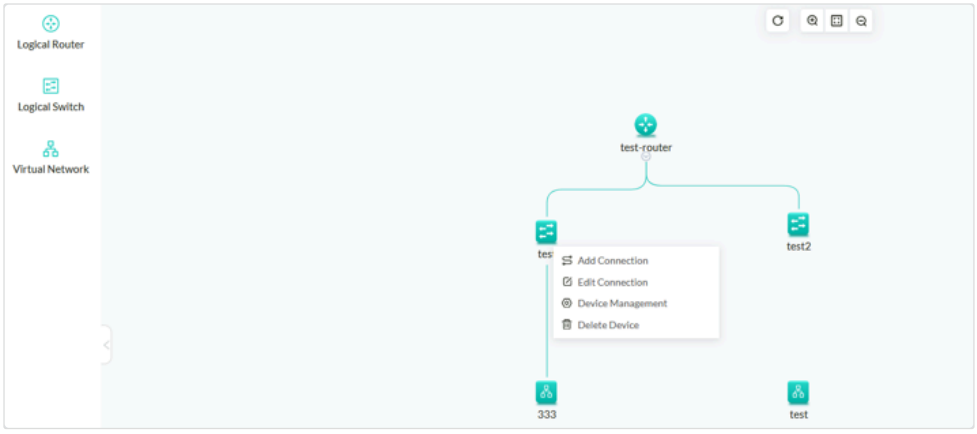


Disconnecting Connections in a Logical Network

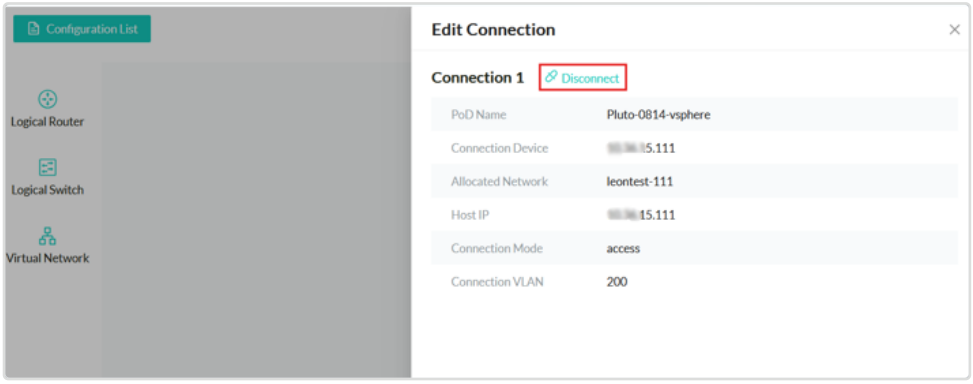
Disconnecting Connections of Logical Switches and Virtual Networks

To disconnect the connections between a logical switch and the virtual network of specific node devices, follow these steps:

1. Click **Service Provision > Logical Networks** from the navigation bar.
2. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
3. On the logical network provisioning page, right-click an added logical switch, and then click **Edit Connection**.



4. In the pop-up window, disconnect the connections between the logical switch and the virtual network.



- To disconnect the connection between the logical switch and the virtual network of **a node device**, locate the connection name, and then click **Disconnect**.
- To disconnect the connections between the logical switch and the virtual network of **all node devices**, click **Disconnect** for all the listed connections. Then, the logical switch and the virtual network are totally disconnected.

  For each connection, the following information is displayed.

Table 3. Connected Node Device

Metric	Description
PoD Name	The PoD of the virtual network connected with the logical switch.
Connection Device	The hostname of the node device connected with the logical switch.
Allocated Network	The name of the virtual network connected with the logical switch.
Host IP	The management IPv4 address of the connected node device.
Connection Mode	The port mode used by the node device to connect with the leaf switch, **Access** or **Trunk**.
Connection VLAN	The VLAN ID of the node device.

Disconnecting Connections of Logical Switches and Logical Routers

To disconnect the connections between a logical router and logical switches, follow these steps:

1. Click **Service Provision > Logical Networks** from the navigation bar.
2. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
3. In the canvas, right-click an added logical router, and then click **Edit Connection**.



4. In the pop-up window, locate the connection to be disconnected, and then click **Disconnect.**

   For each connection, the following information is displayed:

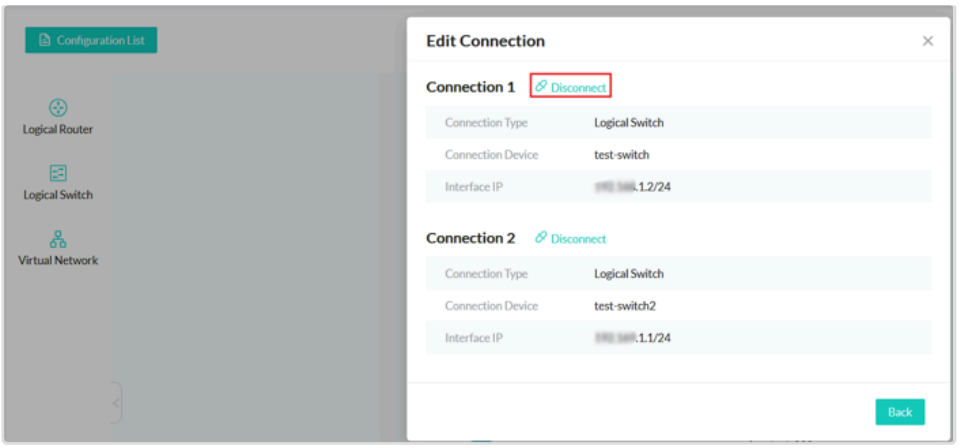


Table 4. Connected Logical Switches

Metric	Description
Connection Type	The logical network element to which the logical router connects. Currently, you can see only **Logical Switch** here.
Connection Device	The logical switch connected with the logical router.
Interface IP	The primary IP address of the logical port.

Deleting Logical Elements from a Logical Network

Deleting a Logical Switch

To delete a logical switch from a logical network, follow these steps:

> **NOTE**
>
> Only after a logical switch is not connected with any virtual network and logical router, the logical switch can be deleted.
>
> - To disconnect the connections between a logical switch and a virtual network, see Disconnecting Connections of Logical Switches and Virtual Networks.
> - To disconnect the connections between a logical switch and a logical router, see Disconnecting Connections of Logical Switches and Logical Routers.

1. Click **Service Provision > Logical Networks** from the navigation bar.

2. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
3. On the logical network provisioning page, right-click an added logical switch, and then click **Delete Device**.



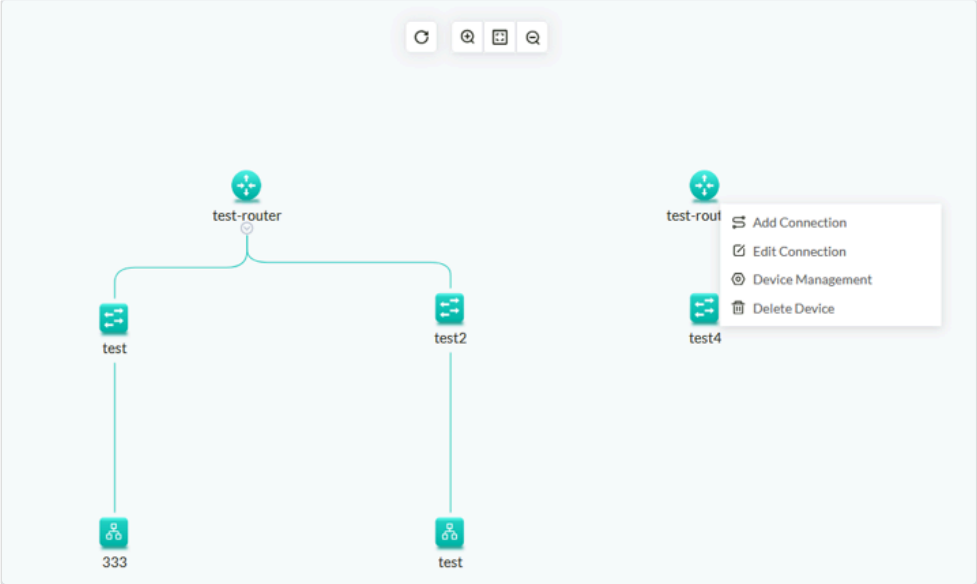
4. In the pop-up window, click **Yes** to confirm the deletion.

Deleting a Logical Router

To delete a logical router from a logical network, follow these steps:

> **NOTE**
>
> Only after a logical router is not connected with any logical switches, the logical router can be deleted. To disconnect the connections between a logical router and a logical switch, see Disconnecting Connections of Logical Switches and Logical Routers.

1. On the “Logical Networks” page, click the name of the logical network to enter the logical network provisioning page.
2. In the canvas, right-click each added logical router, and then click **Delete Device**.



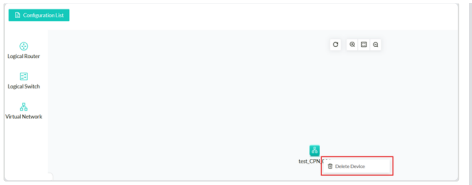
3. In the pop-up window, click **Yes** to confirm the deletion.

Deleting a Virtual Network

- To delete a virtual network (also named VL2) of a bare metal PoD from a logical network, follow these steps:

Table 5. Delete a Virtual Network of a bare metal PoD

Step	Reference Link or Screenshot
1. If the virtual network is connected with a logical switch, disconnect the connections between the virtual network and the logical switch.	Disconnecting Connections of Logical Switches and Virtual Networks
2. If some bare metal nodes are associated with the virtual network, dissociate all the bare metal nodes associated with the virtual network.	Dissociating Bare Metal Nodes from a VL2
3. Go to the logical network provisioning page, right-click the virtual network, and then click **Delete Device**.	No reference link. See the following screenshot:

- To delete a virtual network of a vSphere PoD from a logical network, follow these steps:

Table 6. Delete a Virtual Network of a vSphere PoD

Step	Reference Link or Screenshot
1. If the virtual network is connected with a logical switch, disconnect the connections between the virtual network and the logical switch.	Disconnecting Connections of Logical Switches and Virtual Networks
2. Go to the logical network provisioning page, right-click the virtual network, and then click **Delete Device**.	No reference link. See the following screenshot:

Managing Logical Switches

After you deploy a logical network, you can manage the logical switches in this logical network.

Viewing Logical Switches
- Device Detail
- Status Monitor

Editing a Logical Switch

Deleting a Logical Switch

Viewing Logical Switches

1. Click **Service Provision > Logical Switches** from the navigation bar.
2. In the **Logical Network** drop-down list, select a logical network to which the logical switches belong.

> **NOTEs**
>
> - If you log in to the AmpCon-DC with the built-in user **admin**, you can see all logical networks here.
> - For other AmpCon-DC users, you can see only the logical networks belonging to the tenants managed by each user.

3. On the “Logical Switches” page, check the logical switches in the selected logical networks.



Table 1. Logical Switch Metrics

Metric	Description
Name	The name to distinguish the logical switch.
Description	The description of the logical switch.
Type	The method used to provision the logical switch. Currently, only **Manual** is displayed, which means manual provisioning.

Status	The status of the logical switch. The following status is supported: • **Create Normal:** The logical switch is created successfully. • **Create Error:** The logical switch fails to be created. • **Delete Normal:** The logical switch is deleted successfully. • **Delete Error:** The logical switch fails to be deleted.
Tenant	The tenant who owns the logical network to which the logical switch belongs. **NOTE** The value is **admin** if the logical network is created in AmpCon-DC 2.4.
Logical Network	The logical network to which the logical switch belongs.
Fabric	The fabric to which the logical switch belongs.
Port Count	The total number of logical ports used to connect with node devices in the virtual network.
Create Time	The time when the logical switch was added.

4. To view more details of a logical switch, use either of the following ways:

- Click the logical switch name in the **Name** column of the “Logical Switches” page.



- On the logical network provisioning page, right-click an added logical switch, and then click **Device Management**.



Then, you can see detailed information about the logical switch in the **Device Detail** and **Status Monitor** tabs:

Device Detail

At the top of this tab, you can see the hostname and status of the logical switch.

> **NOTE**
>
> You can see information in the **Logical Port Detail** and **PoD Detail** sections only when the following prerequisites are met:
>
> - The logical switch is connected with one or multiple virtual networks.
> - If the logical switch is connected with a bare metal VL2, ensure that the VL2 is associated with at least one node device.
> - If the logical switch is connected with a portgroup of vSphere, ensure that the portgroup contains at least one VM. You can check the **VM count** value in the **Network** tab of the vSphere PoD.

- In the **Logical Port Detail** section, you can see logical port information:

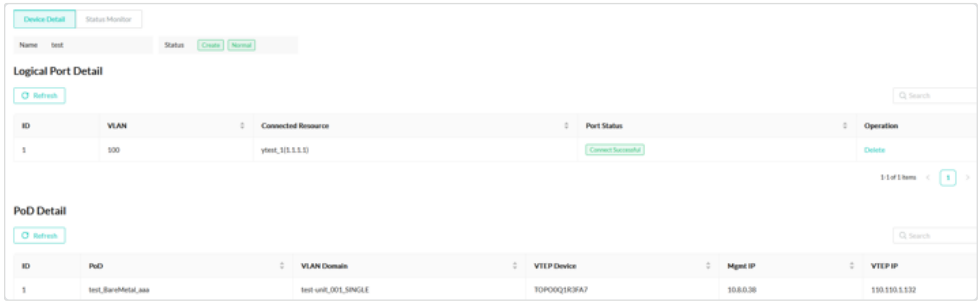


Table 2. Logical Port Metrics

Metric	Description

VLAN	The VLAN ID of the leaf switch connected with the node device.
Connected Resource	The hostname and IPv4 address of the node device.
Port Status	The status of the logical port that connects the node device with the switch. The following status is supported: • **Connect Successful:** The node device connects to the switch successfully through the logical port. • **Disconnecting:** The logical port connection is being disconnected. • **Disconnect Failed:** The logical port connection fails to be disconnected.

To delete a logical port, click **Delete** in the **Operation** column. After you delete a logical port, the node device is not connected to the switch anymore.

- In the **PoD Detail** section, you can see the following information:

  Table 3. PoD Metrics

Metric	Description
PoD	The PoD of the virtual network connected with the logical switch.
VLAN Domain	The VLAN Domain related to the leaf switch.
VTEP Device	The leaf switch that serves as the endpoint for VXLAN tunnels, through which VXLAN packets are sent and received. • For a VLAN Domain containing MLAG switches, both peer MLAG switches are displayed in the **VTEP Device** column. • For a VLAN Domain containing a non-MLAG switch, only one switch is displayed in the **VTEP Device** column.

Mgmt IP	The management IP address of the leaf switch. **Mgmt IP** is used to connect with AmpCon-DC.
VTEP IP	The IP address assigned to the VTEP device.

Status Monitor

At the top of this tab, you can see the logical switch hostname and status.

In the following table, you can see the following metrics:

> **NOTEs**
>
> - You can see information in the table only when the following prerequisites are met:
>   - The logical switch is connected with one or multiple virtual networks.
>   - If the logical switch is connected with a bare metal VL2, ensure that the VL2 is associated with at least one node device.
>   - If the logical switch is connected with a portgroup of vSphere, ensure that the portgroup contains at least one VM. You can check the **VM count** value in the **Network** tab of the vSphere PoD.
> - To refresh the logical port information, click **Refresh**.



Table 4. Connectivity Status Metrics

Metric	Description
VLAN Domain	The VLAN Domain related to the leaf switch.
Leaf Switch	The name of the physical leaf switch on which the logical switch exists. A logical switch can exist on one or multiple physical server leaf switches.

L2 VNI	The identifier in VXLAN that segments Layer 2 broadcast domains, enabling isolated virtual networks over a shared physical infrastructure. The L2 VNI value is assigned automatically from the related VNI pool and is blank if the VNI values in the VNI pool has been used up.
VLAN	The VLAN ID assigned to the leaf switch based on the **Bridge Domain Range** in the related VLAN Domains.
RD	The identifier to uniquely identify overlapping IP/MAC addresses across different VRFs. The value is **Auto**. The value **Auto** means the Route Distinguisher (RD) value is automatically generated for EVPN instances without manual configuration.
RT	The identifier to control the import or export of routes between different VRFs or tenants. The value **Auto** means the Route Target (RT) value is automatically generated for EVPN instances without manual configuration.
Connected LR	The name of the logical router connected with the logical switch. The value is blank if the logical switch isn't connected with any logical router.

Editing a Logical Switch

1. Click **Service Provision > Logical Switches** from the navigation bar.
2. In the **Logical Network** drop-down list, select a logical network to which the logical switch belongs.



3. On the “Logical Switches” page, locate the logical switch to be edited, and then click **Edit**.
4. Modify the name and description (optional) of the logical switch as needed. The **Name** field cannot be empty.

> **NOTE**
>
> You can edit only the name and description of the logical switch. If the configurations of a logical switch can’t meet your needs, you can delete it and create a new logical switch.

5. Click **Apply**.

Deleting a Logical Switch

After you delete a logical switch from a logical network, the logical switch is also deleted from the “Logical Switches” page. For more information, see Deleting a Logical Switch.

Managing Logical Routers

After you deploy a logical network, you can manage the logical routers in this logical network.

Viewing Logical Routers
- Device Detail
- Status Monitor

Editing a Logical Router

Deleting a Logical Router

Viewing Logical Routers

1. Click **Service Provision > Logical Routers** from the navigation bar.
2. In the **Logical Network** drop-down list, select a logical network to which the logical routers belong.

> **NOTEs**
>
> - If you log in to the AmpCon-DC with the built-in user **admin**, you can see all logical networks here.
> - For other AmpCon-DC users, you can see only the logical networks belonging to the tenants managed by each user.

3. On the “Logical Routers” page, check the logical routers in the selected logical networks.

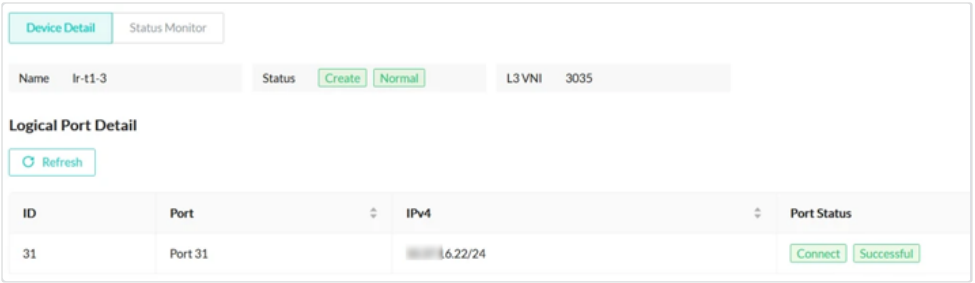


Table 1. Logical Router Metrics

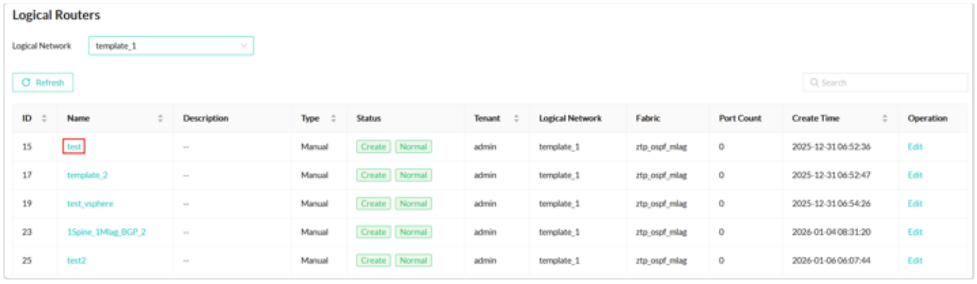
Metric	Description
Name	The name to distinguish the logical router.
Description	The description of the logical router.
Type	The method used to provision the logical router. Currently, only **Manual** is displayed, which means manual provisioning.

Status	The status of the logical router. The following status is supported: • **Create Normal:** The logical router is created successfully. • **Create Error:** The logical router fails to be created with errors. • **Delete Error:** The logical router fails to be deleted with errors.
Tenant	The tenant who owns the logical network to which the logical router belongs. **NOTE** The value is **admin** if the logical network is created in AmpCon-DC 2.4.
Logical Network	The logical network to which the logical router belongs.
Fabric	The fabric to which the logical router belongs.
Port Count	The total number of logical ports connecting the logical router with logical switches.
Create Time	The time when the logical router was added.

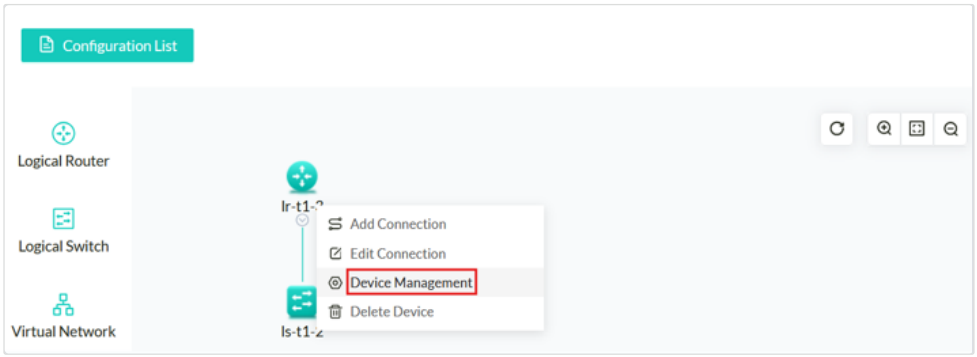
4. To view more details of a logical router, use either of the following ways:



- Click the logical router name in the **Name** column on the “Logical Routers” page.



- On the logical network provisioning page, right-click an added logical router, and then click **Device Management**.



Then, you can see detailed logical router information in the **Device Detail** and **Status Monitor** tabs.

Device Detail

At the top of this tab, you can see the name, status, and L3 VNI of the logical router.

In addition, in the **Logical Port Details** section, you can see the following information:

> **NOTEs**
>
> - If the logical router is not connected with any logical switches, no information will be displayed in the **Logical Port Details** section.
> - The L3 VNI value is assigned automatically from the related VNI pool and is blank if the VNI values in the VNI pool has been used up.
> - A Logical router has only one VRF, one L3 VNI, and one VRF VLAN.
> - Different logical routers are assigned with different L3 VNI values.

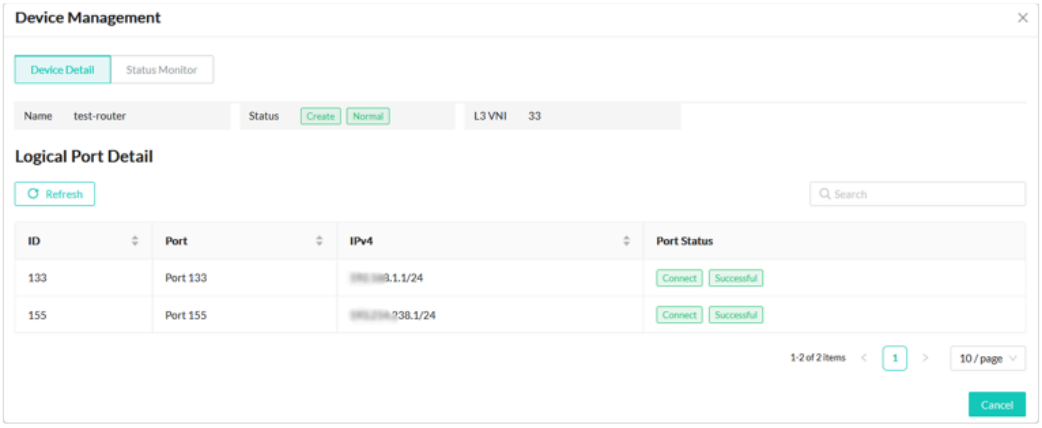


Table 2. Logical Port Metrics

Metric	Description
Port	The logical port connecting the logical router with a logical switch.
IPv4	The IPv4 address (anycast IP) of the logical port. Anycast IP means the IP address of the anycast gateway.
Port Status	The status of the port that connects the logical switch and the logical router. The following status is supported: • **Connect Successful:** The logical router connects to the logical switch successfully through the port. • **Disconnecting:** The port connection between the logical router and the logical switch is being disconnected. • **Disconnect Failed:** The port connection between the logical router and the logical switch fails to be disconnected.

Status Monitor

At the top of this tab, you can see the following information:

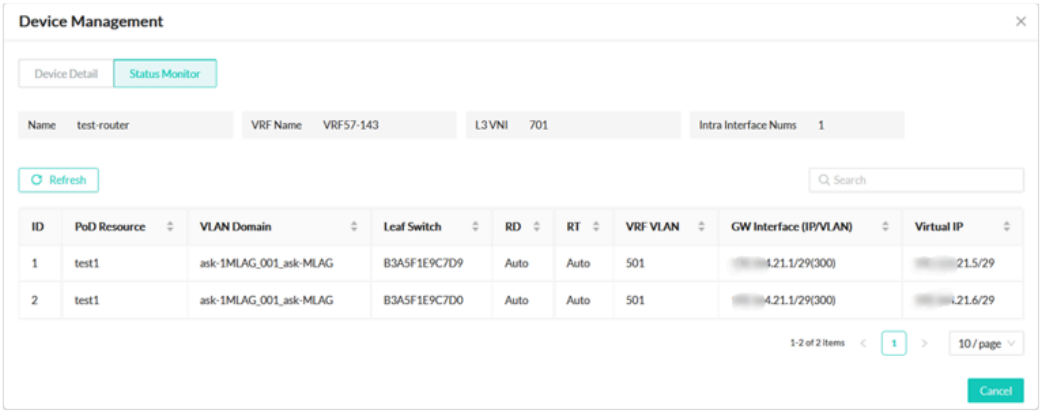


Table 3. Status Metrics

Metric	Description
Name	The name of the logical router.
L3 VNI	The L3 VNI value assigned to the logical router. L3 VNI is used in VXLAN EVPN networks to enable Layer 3 routing isolation and inter-connectivity between different subnets or tenants.
VRF Name	The name of the VRF used by the logical router.
Intra Interface Nums	The total number of logical ports between the logical router and connected logical switches.

In the following table, you can see the following information:

> **NOTE**
>
> You can see information in the table only when the following prerequisites are met:
>
> - The logical router is connected with one or multiple logical switches.
> - At least one logical switch is connected with one or multiple virtual networks.
>   - If the logical switch is connected with a bare metal VL2, ensure that the VL2 is associated with at least one node device.
>   - If the logical switch is connected with a portgroup of vSphere, ensure that the portgroup contains at least one VM. You can check the **VM count** value in the **Network** tab of the vSphere PoD.

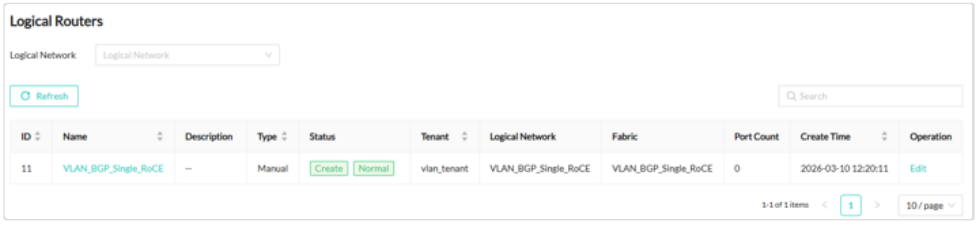
Table 4. Port Metrics

Metric	Description
PoD Resource	The Point of Delivery (PoD) containing the virtual network connected to the logical switch. For more information, see Point of Delivery.
VLAN Domain	The VLAN Domain assigned to the physical leaf switch on which a logical switch exists. VLAN Domain restricts the allocation of VLAN IDs to a specific range for each node device connected to the leaf switch.
Leaf Switch	The name of the physical leaf switch on which a logical switch exists.
RD	The identifier to uniquely identify overlapping IP/MAC addresses across different VRFs. The value is **Auto**. The value **Auto** means the Route Distinguisher (RD) value is automatically generated for EVPN instances without manual configuration.
RT	The identifier to control the import or export of routes between different VRFs or tenants. The value **Auto** means the Route Target (RT) value is automatically generated for EVPN instances without manual configuration.
VRF VLAN	The VLAN ID of the VRF.
GW Interface (IP/VLAN)	The interface of the gateway. The value is in IPv4/VLAN ID format. A switch can hold one or multiple logical switches and thus might contain one or multiple gateway interfaces.
Virtual IP	The virtual IP address assigned to the leaf switch.

	• A leaf switch can hold one or multiple logical switches and thus might contain one or multiple virtual IP addresses. • Hover over the displayed virtual IP addresses, and then you can see all virtual IP addresses. • Each non-MLAG leaf switch has a distinct virtual IP address. • Each MLAG peer switch has a distinct virtual IP address **NOTE** Only after the configurations are pushed to leaf switches, you can see the virtual IP address information here.

Editing a Logical Router

1. Click **Service Provision > Logical Routers** from the navigation bar.
2. In the **Logical Network** drop-down list, select a logical network to which the logical router belongs.



3. On the “Logical Routers” page, locate the logical router to be edited, and then click **Edit**.
4. Modify the name and description (optional) of the logical router as needed. The **Name** field cannot be empty.

> **NOTE**
>
> You can edit only the name and description of the logical router. If the configurations of a logical router can’t meet your needs, you can delete it and create a new logical router.

5. Click **Apply**.

Deleting a Logical Router

After you delete a logical router from a logical network, the logical router is also deleted from the “Logical Routers” page. For more information, see Deleting a Logical Router.

Troubleshooting Guide

If you fail to deploy logical networks, refer to the following reasons and solutions:

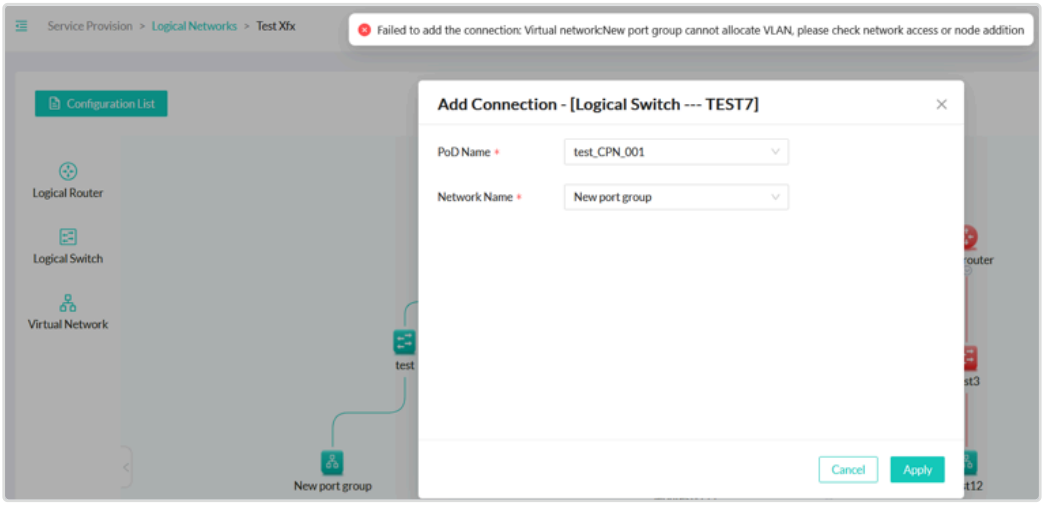
- Logical Switch Provisioning Issues
  - VLAN Assignment Failed
  - Connection Failed
  - No Information Displayed
- Logical Router Provisioning Issues
  - L3 VNI Assignment Failed
- Bare Metal VL2 Issues

Logical Switch Provisioning Issues

VLAN Assignment Failed

Issue: When you connect a logical switch with a virtual network, you might see the error message:

Failed to add the connection: Virtual network: New port group cannot allocate VLAN. Please check network access or node addition.



Root Causes:

- You haven't configure node uplink for node devices in the virtual network.
- The **Bridge Domain Range** in the VLAN Domains of the uplink switches don't contain the **Global VLAN** range of the PoD to which the virtual network belongs. In this case, AmpCon-DC can't assign VLAN ID when you connect a logical switch with a virtual network.

Solutions:

- You must configure node uplink for node devices in the virtual network before provisioning logical switches. For more information, see Configuring Node Uplink for Bare Metal Nodes

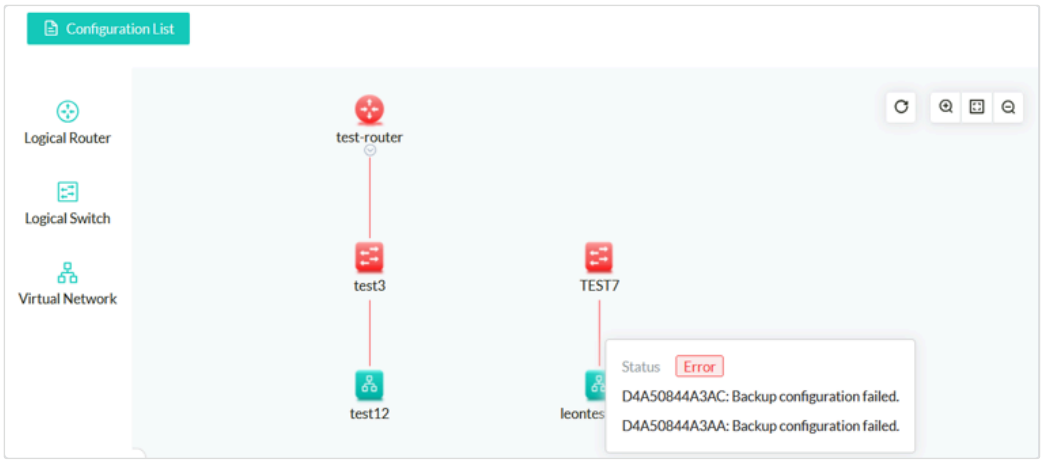
and Configuring Node Uplink for Cloud Platform Nodes.

- Edit the **Bridge Domain Range** in the VLAN Domains of the uplink switches, and ensure the **Bridge Domain Range** covers the **Global VLAN** range of the PoD to which the virtual network belongs.

Connection Failed

Issue: After you connect a logical switch with a virtual network, the connection line is in red. Hover over the red line, you can see the following error message:

<Switch SN>: Backup configuration failed.

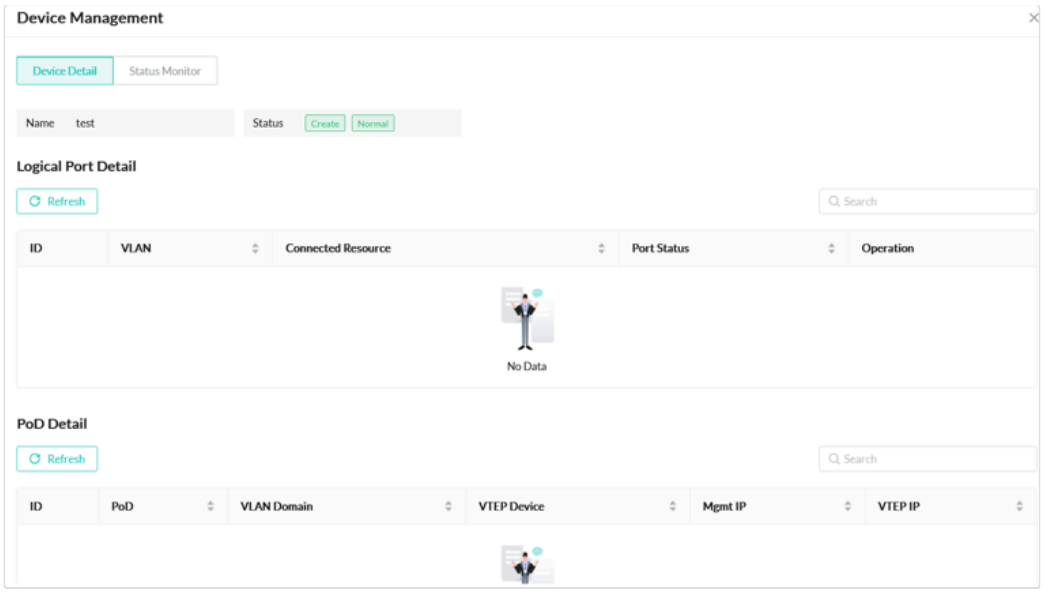


Root Cause: The node devices in the virtual network are not connected with the uplink switches that you configured in node uplink configurations.

Solution: Ensure that the node uplink configurations are correct and the node devices in the virtual network are connected with the specified uplink switches.

No Information Displayed

Issue: Some information is not displayed in the **Device Management** pop-up window of logical switches.



Root Cause: You can see complete information only when the following prerequisites are met:

- The logical switch is connected with one or multiple virtual networks.
- If the logical switch is connected with a bare metal VL2, ensure that the VL2 is associated with at least one node device.
- If the logical switch is connected with a portgroup of vSphere, ensure that the portgroup contains at least one VM. You can check the **VM count** value in the **Network** tab of the vSphere PoD.

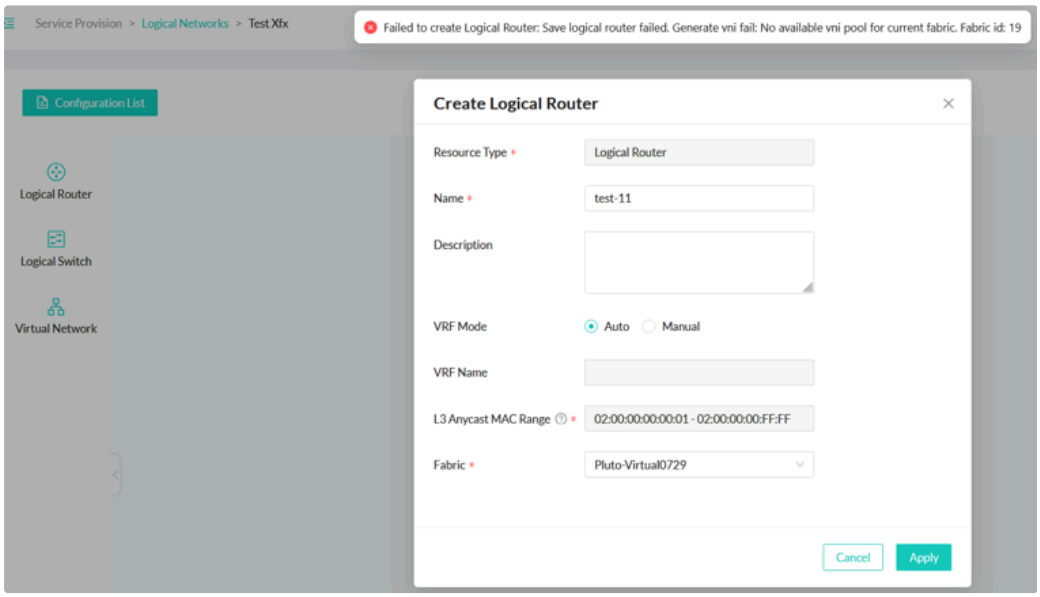
Solution: Ensure that all of the prerequisites above are met.

Logical Router Provisioning Issues

L3 VNI Assignment Failed

Issue: When you add a logical router to a logical network, you might see the following error message:

Failed to create Logical Router: Save logical router failed. Generate vni fail: No available vni pool for current fabric. Fabric id: xx

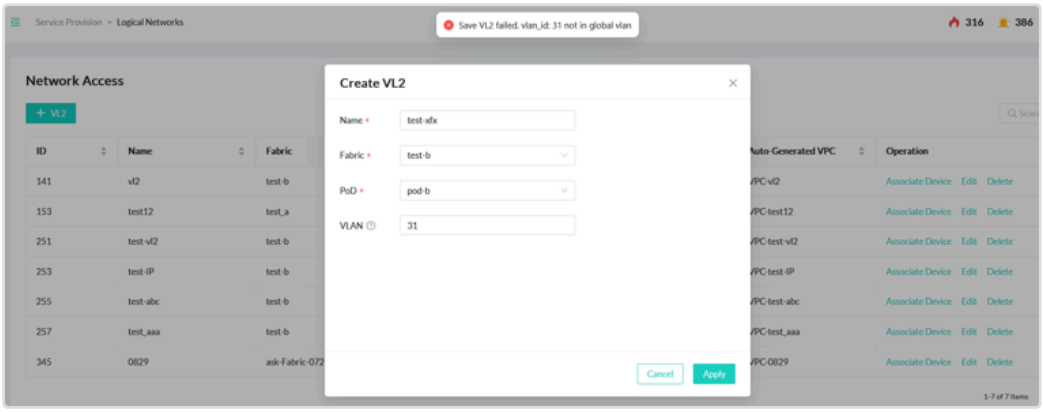


Root Cause: No VL2 pools are available for the fabric to which the logical router belongs.

Solution: Ensure that you have created the VNI pools used by the fabrics and the VNI pools have enough unused VNI values for L3 VNI assignment. For more information, see VNI Pools.

Bare Metal VL2 Issues

Issue: When you create a bare metal VL2, if the **VLAN** value is not in the **Global VLAN** range of the PoD, you will see the following error message:



Root Cause: The **VLAN** value in the **Create VL2** pop-up window is not in the **Global VLAN** range of the PoD.

Solution: Click **Resource > Resource Interconnection** from the navigation bar. In the **PoD** tab, locate the PoD, and click Edit. In the pop-up window, check the **Global VLAN** range. Then, when you create a VL2, ensure that the **VLAN** value is in the **Global VLAN** range, or leave the **VLAN** field blank. For more information, see Adding a VL2.

Managing Third-Party Devices

After you add third-party devices to AmpCon-DC, you can manage these devices, check or configure RoCE with several clicks, run Ansible playbooks on these devices, and monitor Network Interface Cards (NICs) and RoCE related telemetry data for performance tuning.

Currently, this feature supports only managing Linux servers.

See the following child topics:

- Adding Devices
- Managing Added Devices
- RoCE on NICs

Adding Devices

Add third-party devices to AmpCon-DC so that you can keep the inventory of added devices, view device information in real-time or historical topologies, manage and monitor RDMA over Converged Ethernet (RoCE), monitor Network Interface Cards (NICs), and run Ansible playbooks on the device for automation.

Guidelines
Adding a Device
Adding Devices in Bulk

Guidelines

- Currently, this feature supports adding only Linux servers.
- Only if you add a device with the monitoring function enabled, the following functions can be used for the device:
  - View device information in the “Inventory” tab and in a topology.
  - Manage and monitor RoCE.
  - Monitor Network Interface Cards (NICs).
- No matter whether a device is added with the monitoring function enabled or disabled, you can run Ansible playbooks on this device and view host information of the device in real-time or historical topologies.

Adding a Device

To add one device to AmpCon-DC, follow these steps:

1. Click **Device > Hosts** from the navigation bar.
2. In the **Device Discovery** tab, click **+ Device**.
3. In the **Create Device** pop-up window, input the following information in the **Add Manually** tab:

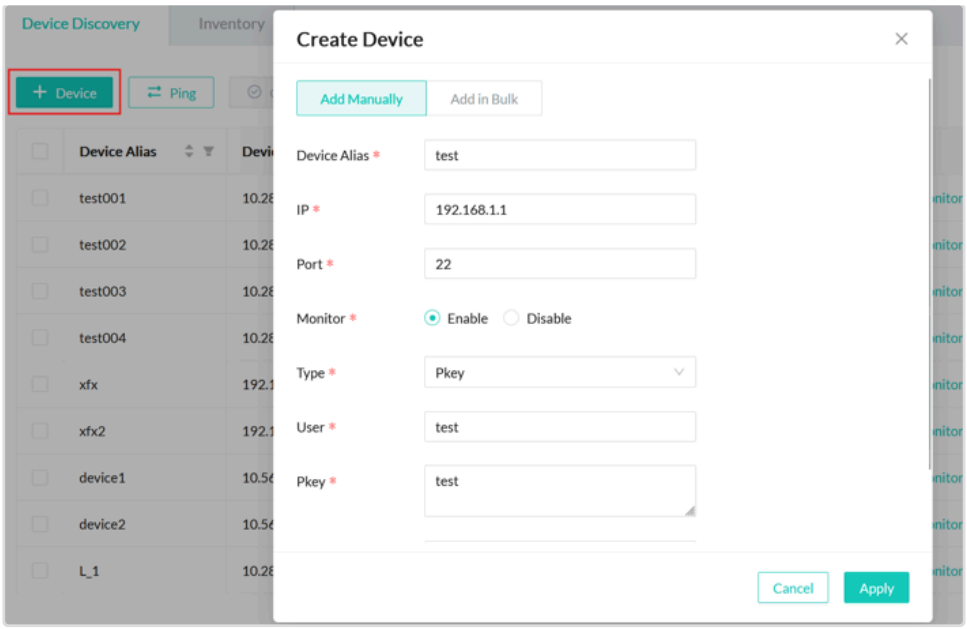


Table 1. Device Addition Parameters

Column	Description
Device Alias	The alias (1 to 255 characters in length) of the device to distinguish the device in the AmpCon-DC UI. The alias is used only in the AmpCon-DC UI and will not be pushed to the device.
IP	The IPv4 address of the device.
Port	The device port used to connect to AmpCon-DC.
Monitor	Enable or disable the monitoring function.
Type	Select **Password** for password authentication, or select **Pkey** for Pkey authentication**.**
User	The name of the administrator user used to log in to the device.
Password	The password of the administrator user used to log in to the device. **NOTE** This field can be seen only if you select **Password** in the **Type** drop-down list.

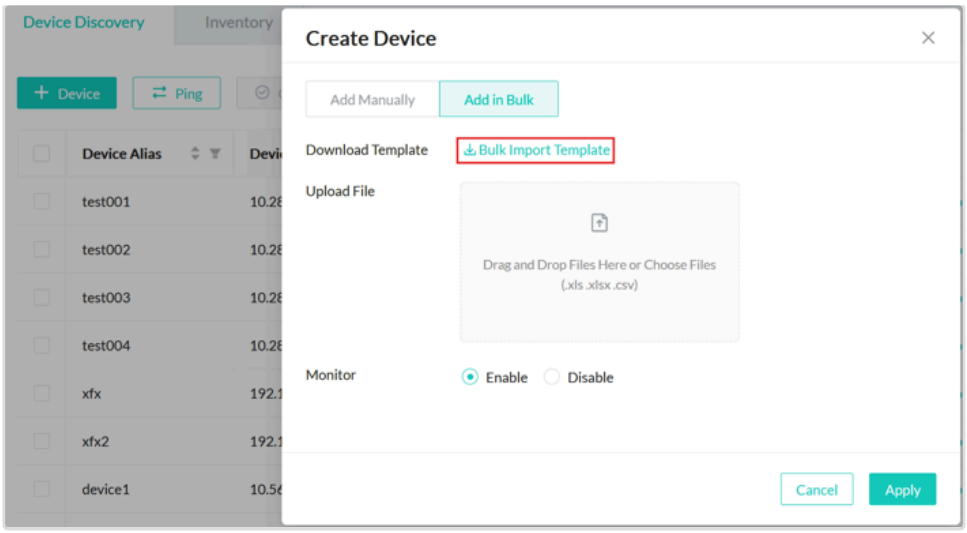
Pkey	The public key used to log in to the device. **NOTE** This field can be seen only if you select **Pkey** in the **Type** drop-down list.
SudoPassword	The password of the administrator user used by AmpCon-DC to install a monitoring tool for device monitoring. **NOTE** This field can be seen only if you select **Pkey** in the **Type** drop-down list.
Select Group	Select a host group to which the device belongs. **NOTEs** • This section can be seen only if the currently logged-in user is a group user. • If you haven't added any host groups before, you need to add host groups first as described in Adding a Host Group.

4. Click **Apply**.

Adding Devices in Bulk

To add multiple devices in bulk to AmpCon-DC, follow these steps:

1. In the "Device Discovery" tab, click **+ Device**.
2. In the **Create Device** pop-up window, click the **Add in Bulk** tab.
3. Click **Bulk Import Template** to download the template file.



4. Enter the following device information in the downloaded file:

> **NOTE**
>
> All the following parameters are required. If any parameters are missing for some devices, the addition of these devices will fail.

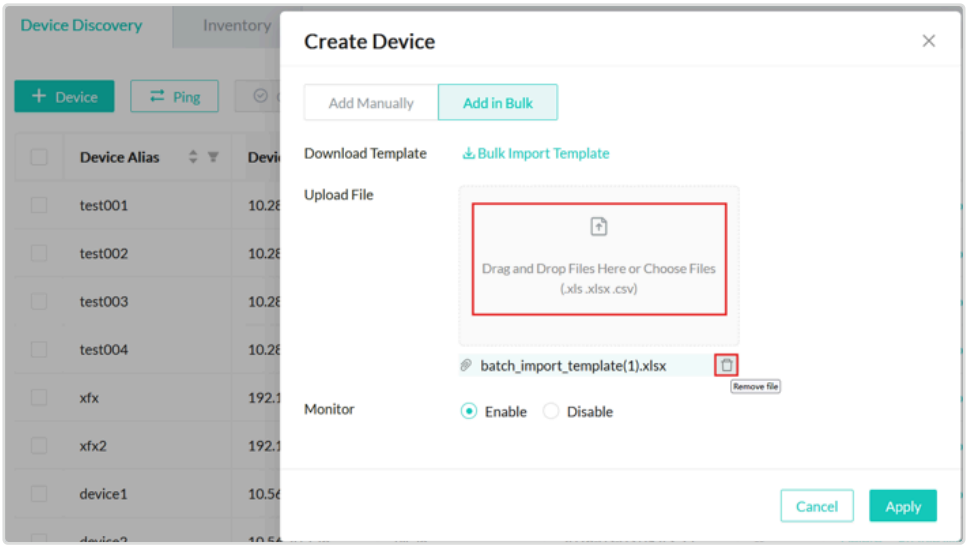
Table 2. Template File Parameters

Column	Description
Device Alias	The alias (1 to 255 characters in length) of the device to distinguish the device in the AmpCon-DC UI. The alias is used only in the AmpCon-DC UI and will not be pushed to the device.
IP	The IPv4 address of the device. The IP address must be unique.
Username	The username (1 to 255 characters in length) of the device.
Password	The password (1 to 255 characters in length) of the device.
Port	The device port number (1 to 65535) used to connect to AmpCon-DC.

5. In the **Upload File** section, upload the file to AmpCon-DC by dragging and dropping the file or clicking this area and then choosing the file.

You can upload one or multiple files. To remove an uploaded file, hover over the file, and then click the delete icon.

> **NOTEs**
>
> - Only **.xls**, **.xlsx**, and **.csv** files are supported to be uploaded.
> - You must fill in each column in the template file and follow the format of each column (such as IP format). Or else, devices might fail to be uploaded.
> - After you upload a file, only the devices with the right format are added to AmpCon-DC, while the devices with the wrong format are not added.
> - If two uploaded files contain the same devices, the device is added to AmpCon-DC only one time.



6. In the **Monitor** section, click **Enable** or **Disable** to enable or disable the monitoring function.
7. In the **Select Group** section, select one or multiple host groups to which the devices belongs.

> **NOTEs**
>
> - This section can be seen only if the currently logged-in user is a group user.
> - If you haven't added any host groups before, you need to add host groups first as described in Adding a Host Group.

8. Click **Apply**.

Managing Added Devices

After you add devices to AmpCon-DC, you can manage these added devices.

- Managing the Device Inventory
  - Viewing Monitored Devices
  - Deleting a Device
  - Enabling the Monitoring Function
  - Accessing the Device through Web SSH
  - Logging In to BMC
  - Powering Down or Rebooting Switches
- Testing Device Connectivity
- Checking RDMA over Converged Ethernet (RoCE)
- Viewing Devices in a Real-Time or Historical Topology

Managing the Device Inventory

Viewing Monitored Devices

Click **Device > Hosts** from the navigation bar. In the **Inventory** tab, you can see the list of devices that are added with the monitoring feature enabled and connected to the AmpCon-DC server:

> **NOTE**
>
> You can view the device information in the “Inventory” tab only if you have enabled the monitoring function of the device. For more information, see Enabling the Monitoring Function.

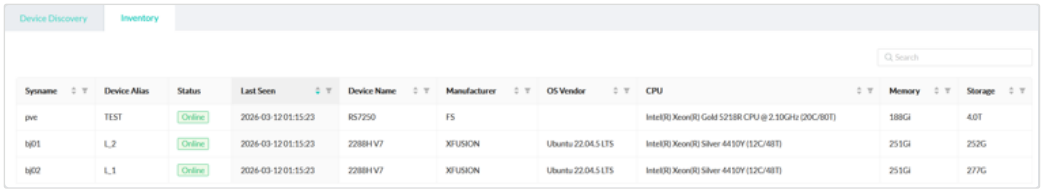


Table 1. Device Inventory Metrics

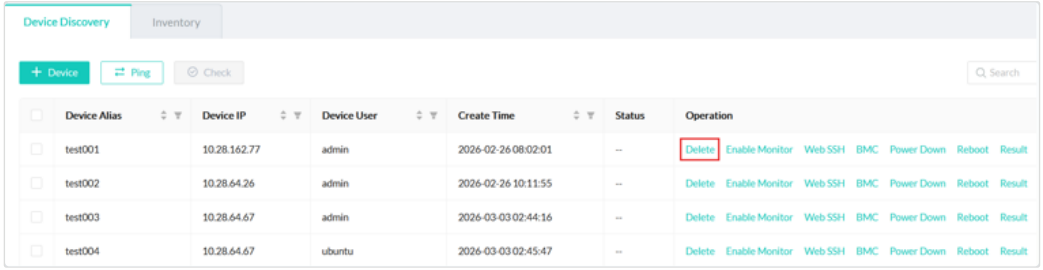
Column	Description
Sysname	The hostname of the device.
Device Alias	The alias of the device.
Status	Indicates whether AmpCon-DC can retrieve monitoring data from the device.

	• **Online:** AmpCon-DC can retrieve monitoring data from the device. • **Offline:** AmpCon-DC can't retrieve monitoring data from the device. You might see outdated monitoring data if the status is **Offline**.
Last Seen	The last time when AmpCon-DC retrieves monitoring data from the device. **NOTE** If the monitoring function of the device is disabled, the **Last Seen** data will be outdated.
Device Name	The device model name.
Manufacturer	The manufacturer of the device.
OS Vendor	The vendor of the OS on the device.
CPU	The CPU specification of the device.
Memory	The memory size of this device.
Storage	The storage capacity of this device.

Deleting a Device

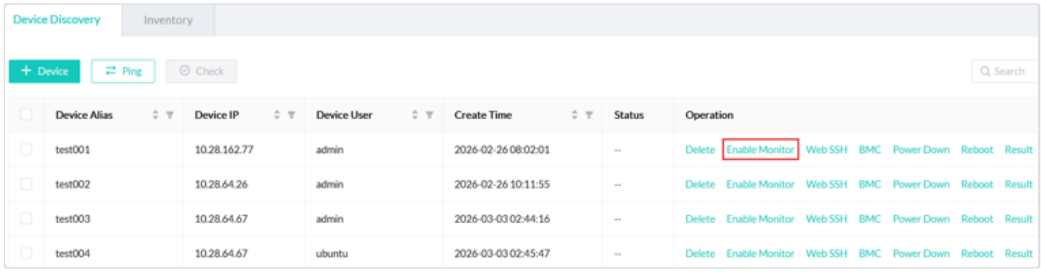
To delete a device from AmpCon-DC, locate a device, and click **Delete**. Then, click **Yes** to confirm the deletion.

> **NOTE**
>
> After you delete a device, all information related to the device is removed from AmpCon-DC.



Enabling the Monitoring Function

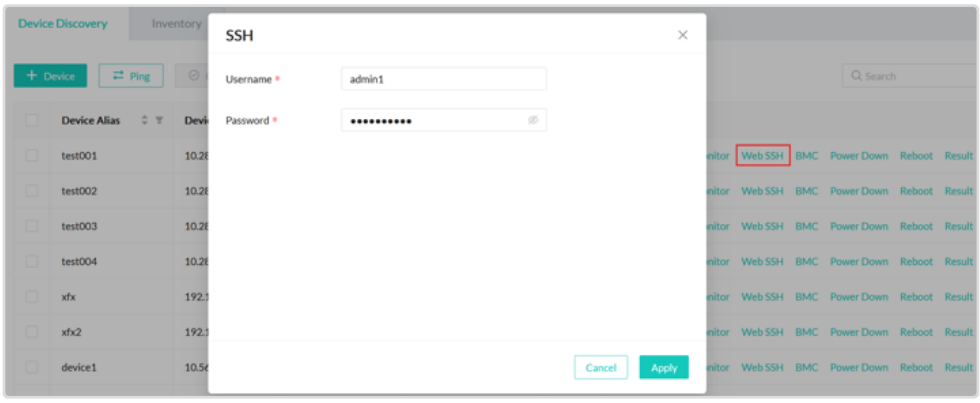
You might not have enabled the monitoring function for a device. To enable the monitoring function, locate the device, and then click **Enable Monitor**.



Accessing the Device through Web SSH

To connect to a device from the AmpCon-DC UI by creating an SSH session, follow these steps:

1. Locate the device, and then click **Web SSH**.
2. In the pop-up window, input the username and password used to log in to the device.

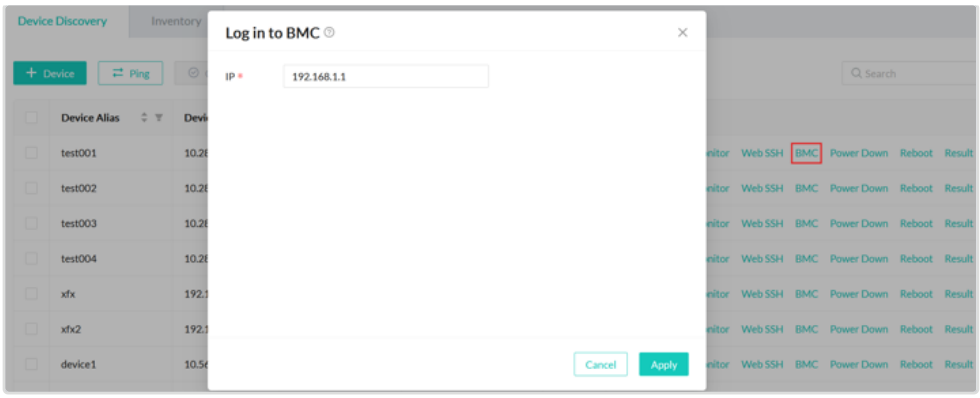


3. Click **Apply**.

Logging In to BMC

To log in to Baseboard Management Controller (BMC), a dedicated controller used to monitor and manage servers, follow these steps:

1. Locate the device, and then click **BMC**.
2. In the pop-up window, enter the IP address of the BMC.

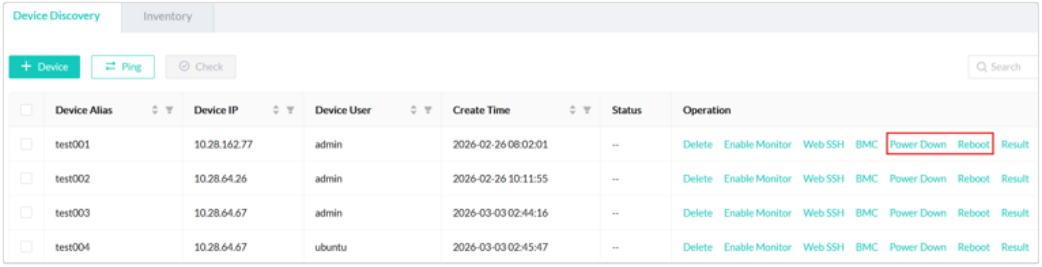


3. Click **Apply**.

Powering Down or Rebooting Switches

To power down a switch, locate the device, and then click **Power Down**.

To reboot a switch, locate the device, and then click **Reboot**.

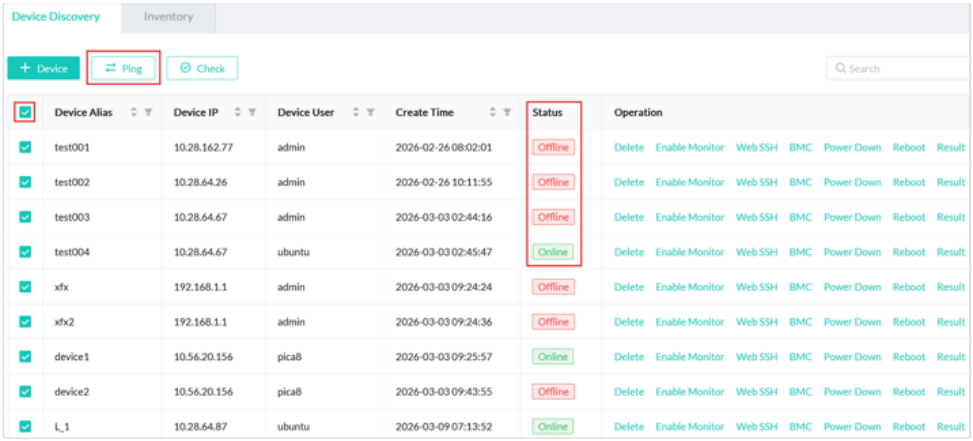


Testing Device Connectivity

To check whether all added devices can connect to AmpCon-DC or not, follow these steps:

1. In the **Device Discovery** tab, select the square before the **Device Alias** column heading to select all devices in the current page.
2. Click **Ping**.
3. Wait for a while. Then, check the **Status** column to see whether all added devices can connect to AmpCon-DC.

- The **Online** status means the device is connected to the AmpCon-DC server.
- The **Offline** status means the device is not connected to the AmpCon-DC server.

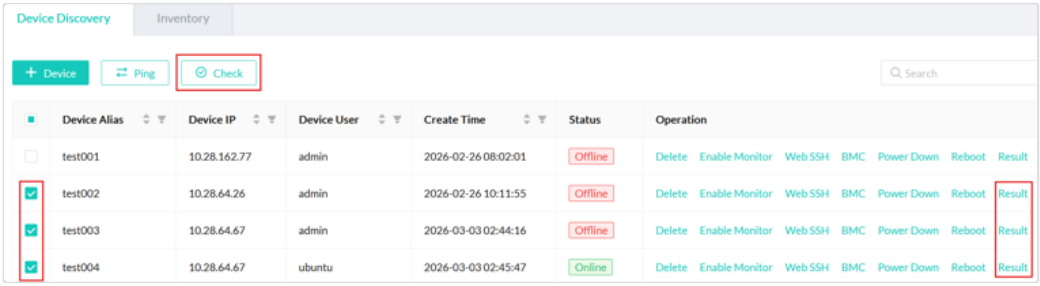


Checking RDMA over Converged Ethernet (RoCE)

Click **Device > Hosts** in the AmpCon-DC UI. In the **Device Discovery** tab, you can check the RoCE status on third-party devices, including whether Network Interface Card (NIC) drivers, RoCE drivers, and RDMA-related tools are installed, whether RoCE V2 and ECN are enabled, and whether QoS and PFC are configured as required.

To check RoCE status for some devices, select the square before these devices, and then click **Check**. For more information, see Checking RoCE.

To view the checking result for a device, locate the device, and then click **Result**.



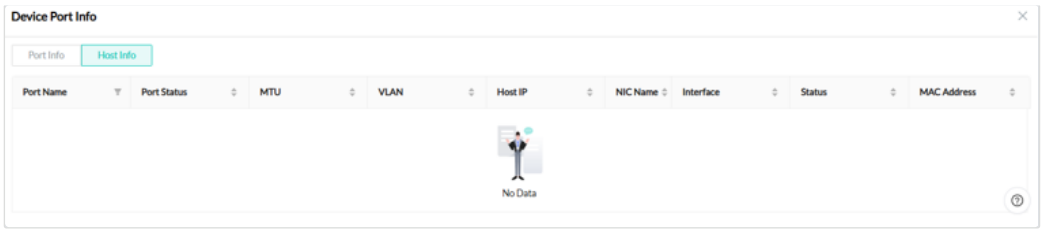
Viewing Devices in a Real-Time or Historical Topology

Click **Physical Network > Topologies**, enter the real-time topology mode or the historical topology mode, and then click the switch to be monitored. Then, you can view information of added devices (Linux servers) connected to the switch.

For more information, see Viewing Switch Details in Topologies - Host Info.

NOTE

You can view the device information in the related topology only if you have enabled the monitoring function of the device.


Device Port Info
Port Info
Host Info
Port Name
Port Status
MTU
VLAN
Host IP
NIC Name
Interface
Status
MAC Address
No Data

RoCE on NICs

RDMA over Converged Ethernet (RoCE) leverages Remote Direct Memory Access (RDMA) to achieve high-throughput and low-latency data transfers between nodes in a network. For more information, see RoCE Overview.

By using AmpCon-DC, you can check and configure RoCE on the NIC side with several clicks and monitor RoCE-related telemetry data for performance tuning.

See the following child topics:

- Supported NICs
- RoCE Overview
- Configuring RoCE
- Checking RoCE
- Verifying RoCE Configurations

> **NOTEs**
>
> - Currently, this feature supports Nvidia and Broadcom NICs on Linux servers.
> - To monitor RoCE-related telemetry data on the network interface card (NIC) side. For more information, see RoCE Data on NICs.

Supported NICs

The Network Interface Card (NIC) monitoring feature of AmpCon-DC supports the following NICs:

- Broadcom NICs
- Nvidia NICs

Broadcom NICs

Table 1. Supported Broadcom NICs

Series	Device Model	Chip
Ethernet Network Adapters	P210P	BCM57412
	P210TP	BCM57416
	P225P	BCM57414
	P425G	BCM57504
	P2100G	BCM57508
	P2200G	BCM57608
	P1400GD	BCM57608
	BCM5720-2P	BCM95720
	N1400GD	BCM57608
	N2200G	BCM57608
	N2100G	BCM57508
	N425G	BCM57504
	N225G	BCM57414
	N210TP	BCM57416
	N210P	BCM57412

Nvidia NICs

Table 2. Supported Nvidia NICs

Series	Device Model	Chip
ConnectX-4 Lx EN	MCX4121A-ACAT	MT27710 Family
	MCX4111A-XCAT	
	MCX4121A-XCAT	
	MCX4121A-XCHT	
	MCX4111A-ACAT	
	MCX4111A-ACUT	
	MCX4121A-ACUT	
	MCX4121A-ACHT	
	MCX4121A-ACST	
	MCX4131A-BCAT	
	MCX4131A-GCAT	
ConnectX-5	MCX512A-ACAT	MT27620 Family
	MCX512A-ACUT	
	MCX512F-ACAT	
	MCX512F-ACHT	
	MCX515A-GCAT	
	MCX516A-GCAT	
	MCX515A-CCAT	
	MCX515A-CCUT	
	MCX516A-CCHT	
	MCX516A-CCAT	
NVIDIA ConnectX-6	MCX653106A-HDAT	MT28908 Family and MT28908A0 Family
	MCX653105A-EFAT	
	MCX653106A-EFAT	

	MCX651105A-EDAT	
	MCX653105A-ECAT	
	MCX653106A-ECAT	
	MCX654106A-HCAT	
	MCX653105A-HDAL	
	MCX653106A-HDAL	
	MCX683105AN-HDAT	
	MCX654106A-ECAT	
	MCX654105A-HCAT	
ConnectX-7 PCIe x16 Stand-up Adapter Cards	MCX75310AAS-NEAT	MT2910 Family
	MCX75310AAC-NEAT	
	MCX75310AAS-HEAT	
	MCX713104AC-ADAT	
	MCX713104AS-ADAT	
ConnectX-7 Socket Direct Ready Cards for Dual-Slot Servers	MCX755106AS-HEAT	MT2910 Family
	MCX715105AS-WEAT	
	MCX75510AAS-NEAT	
	MCX75510AAS-HEAT	
	MCX755106AC-HEAT	
NVIDIA ConnectX-6 Dx	MCX623102AC-GDAT	MT28908A0 Family

MCX621202AS-ADAT
MCX621202AC-ADAT
MCX623106AC-CDAT
MCX623106AN-CDAT
MCX623106AS-CDAT
MCX623105AN-VDAT
MCX623102AS-ADAT
MCX623102AS-ADAT
MCX621102AN-ADAT
MCX621102AC-ADAT
MCX623102AC-ADAT
MCX623102AN-ADAT
MCX621102AE-ADAT
MCX623102AN-GDAT
MCX623102AE-GDAT
MCX623102AS-GDAT

MCX623105AN-CDAT
MCX623106PC-CDAT
MCX623105AC-CDAT
MCX623105AE-CDAT
MCX623106AE-CDAT
MCX623109AC-CDAT
MCX623109AN-CDAT
MCX623106GC-CDAT
MCX623106TC-CDAT(a)
MCX623106GN-CDAT
MCX623106PC-CDAT
MCX623106PE-CDAT
MCX623106PN-CDAT
MCX623106TN-CDAT
MCX623105AE-VDAT

	MCX623105AS-VDAT	
	MCX623105AC-VDAT(a)	

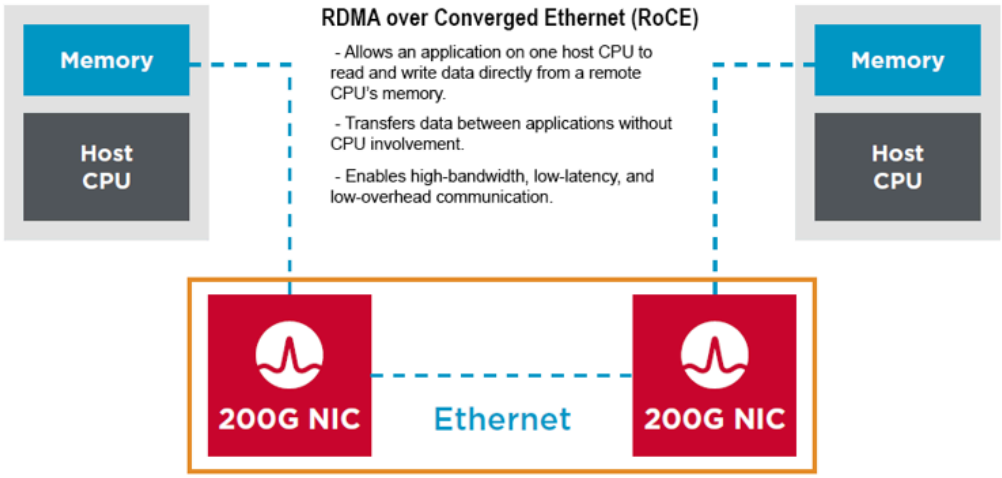
RoCE Overview

RDMA over Converged Ethernet (RoCE) is a network protocol that enables high-throughput and low-latency data communication between nodes in a network.

- Benefits of RoCE
- Versions of RoCE
- Key Features of RoCE
  - Priority Flow Control (PFC)
  - Explicit Congestion Notification (ECN)
  - Quality of Service (QoS)

Benefits of RoCE

RoCE helps reduce CPU workloads by providing direct memory access for applications that bypass the CPU. Because packet processing and memory access are handled by the network interface card (NIC) and network switch rather than the CPU, RoCE allows for higher throughput, lower latency, and reduced CPU utilization for both the sender and receiver, which is crucial for distributed storage, high-performance computing (HPC), and AI deep learning model training and big data analytics.



Versions of RoCE

RoCE has the following two versions. AmpCon-DC supports only checking and configuring RoCEv2.

- **RoCEv1**: This version operates at Layer 2 of the OSI model, meaning it is not routable beyond the local Ethernet network. It requires all devices to be in the same Ethernet broadcast domain.

- **RoCEv2**: This version operates at Layer 3, making it routable over IP networks. RoCEv2 packets can traverse multiple subnets, allowing for greater scalability and flexibility in network design.

Key Features of RoCE

AmpCon-DC supports configuring and monitoring the following features of RoCE:

Priority Flow Control (PFC)

Priority Flow Control (PFC) is a network protocol designed to manage congestion on Ethernet networks by allowing for the independent pausing of traffic based on priority levels. It is part of the IEEE 802.1Qbb standard and is particularly useful in data center environments where different types of traffic need to be handled with varying degrees of urgency.

PFC is a critical technology for managing congestion in Ethernet networks, particularly in data center environments. By enabling traffic differentiation and providing lossless transport for high-priority traffic, PFC helps maintain performance and reliability for critical applications.

Explicit Congestion Notification (ECN)

Explicit Congestion Notification (ECN) is an effective mechanism for managing network congestion by marking packets instead of dropping them. It is an extension of the IP and TCP protocols, enhancing the way congestion is managed by marking packets instead of discarding them. It helps improve network performance, reduce packet loss, and maintain high throughput, making it especially valuable in data centers and for real-time applications.

Quality of Service (QoS)

QoS is a network mechanism used to manage and ensure different levels of quality and performance for different types of traffic in a network. QoS aims to control the transmission priority of data packets through network devices, protocols, and mechanisms, thereby ensuring priority processing for critical tasks and reducing issues such as latency, packet loss, and jitter.

Configuring RoCE

By using RoCE templates provided by AmpCon-DC, you can customize RoCE configurations on NICs and push these configurations to one or multiple NICs with several clicks. The RoCE configuration process is greatly simplified in this way.

AmpCon-DC supports configuring RoCE on NICs through deployment scripts and forms.

> **NOTEs**
>
> - Currently, this feature supports only Nvidia and Broadcom NICs on Linux servers.
> - For Broadcom NICs, this feature supports only NICs with the chip model of BCM57608.

Prerequisites
Configuration Procedure
  Configuring RoCE through Deployment Forms
  Configuring RoCE through Deployment Scripts
Verifying RoCE Configurations

Prerequisites

Ensure that the following prerequisites are met:

- The devices to be managed are added to AmpCon-DC with the monitor function enabled. For more information, see Adding Devices.
- The devices to be managed are connected to the AmpCon-DC server. For more information, see Testing Device Connectivity.

Configuration Procedure

You can configure RoCE on NICs through deployment forms or deployment scripts.

Configuring RoCE through Deployment Forms

To configure RoCE on NICs through deployment forms, follow these steps:

1. Click **Physical Network > RoCE > NIC Configurations** from the navigation bar.
2. In the **Form Deployment** tab, select the vendor (**Nvidia** or **Broadcom**) of the NICs in the **NIC Vendors** drop-down list.
3. In the **NIC Ports** drop-down list, select one or multiple devices and NIC ports.
4. In the **RoCEv2 Configuration** section, configure RoCE as follows:

- If you selected **Nvidia** in the **NIC Vendors** drop-down list, input the following information:

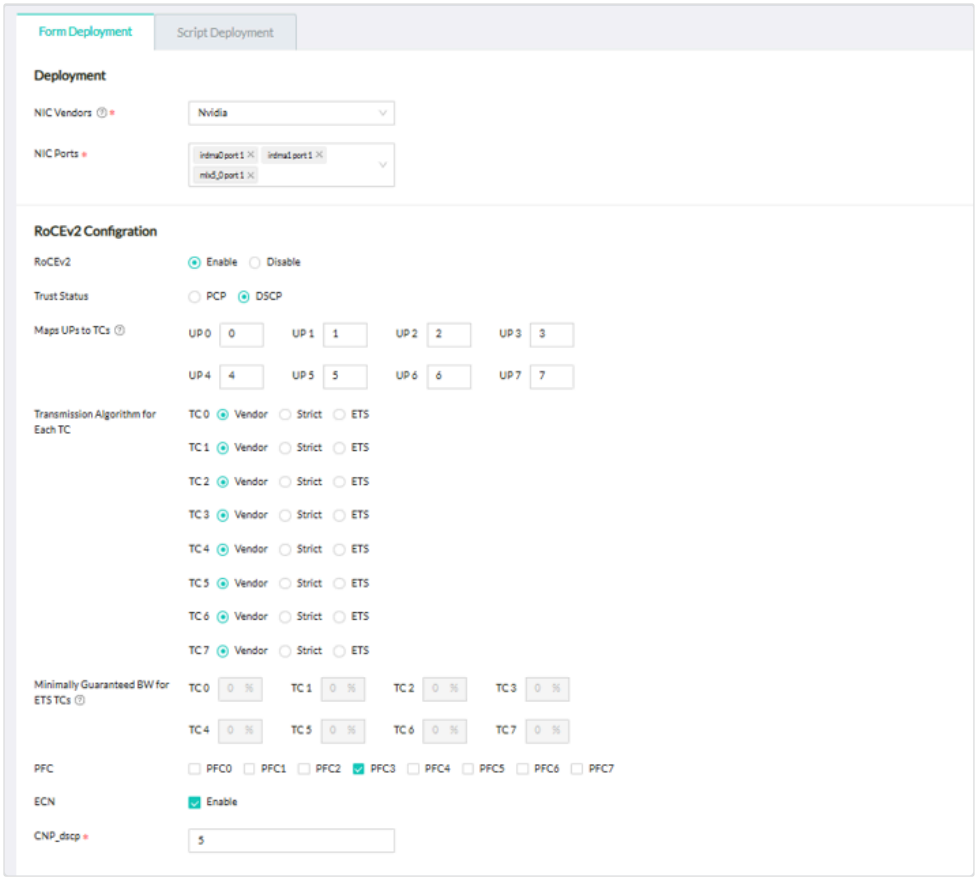


Table 1. Nvidia RoCE Configurations

Column	Description
RoCEv2	Whether to enable RoCEv2.
Trust Status	How the sent and received Ethernet packets are prioritized. Valid values are **PCP** or **DSCP**. The default value is **PCP**. • **PCP:** The 3-bit field within the VLAN tag of an Ethernet frame. PCP is used to prioritize traffic in RoCE networks. • **DSCP:** The 6-bit field in the IP header's Type of Service (ToS) byte. DSCP is used to classify and prioritize traffic for QoS in Ethernet network.
Maps UPs to TCs	The mapping of User Priorities (UPs) to Traffic Classes (TCs). For example, if you enter **2** in

	the **UP 0** field, it means the user priority **0** is mapped to the traffic class **2**. • **UPs:** The user priority defined by the IEEE 802.1p to identify the priority of Ethernet frames. Valid UP values range from 0 to 7. • **TCs:** A method to define traffic priorities. TCs determine the processing and transmission order of traffic in the network. Valid TC values range from 0 to 7.
Transmission algorithm for each TC	The transmission algorithm set for each TC. • **Vendor:** The default mode for Nvidia NICs. No TC configurations are done in this mode. • **Strict:** If you set a TC transmission algorithm to be **Strict**, this TC has absolute (strict) priority over other TC strict priorities coming before it. As determined by the TC number, TC 7 is the highest priority, and TC 0 is the lowest. • **ETS:** Enhanced Transmission Selection standard (ETS) exploits the time periods in which the offered load of a particular TC is less than its minimum allocated bandwidth by allowing the difference to be available to other traffic classes.
Minimally Guaranteed BW for ETS TCs	The minimum allocated bandwidth percentage for each ETS TC. The minimum allocated bandwidth percentages of all ETS TCs must total 100%. For example, if TC 1, TC 3, and TC 5 use ETS as the transmission algorithm, the minimum allocated bandwidth percentages of these three TCs must total 100%. **NOTE**

	The minimum allocated bandwidth percentage fields are available only for ETS TCs.
PFC	Enables PFC on specific queues. For example, if you select **PFC 0** and **PFC 1**, it means enabling PFC on the queues 0 and 1.
ECN	Enables ECN.
CNP_802p_prio	The IEEE 802.1p priority value for Congestion Notification Packets (CNP) in RoCEv2 networks. Valid values range from 0 to 7. **NOTE** This field is available only when the **Trust Status** is set to **PCP**.
CNP_dscp	The DSCP priority value for Congestion Notification Packets (CNP) in RoCEv2 networks. Values range from 0 to 63. **NOTE** This field is available only when the **Trust Status** is set to **DSCP**.

- If you selected **Broadcom** in the **NIC Vendors** drop-down list, select the tool type (**NIC CLI** or **Bnxtsetupcc.sh**) in the **Type** radio box.

  If you selected **NIC CLI**, input the following information:

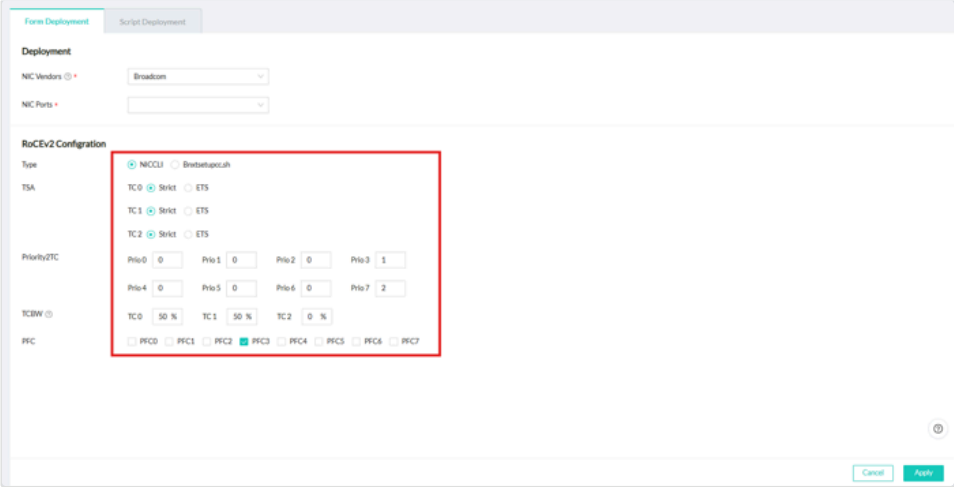


Table 2. NIC CLI RoCE Configurations

Column	Description
TSA	The traffic scheduling algorithm that defines the bandwidth allocation and scheduling policies for different Traffic Classes (TCs). TSA ensures that mission-critical traffic receives the required bandwidth and priority. • **Strict:** If you set the traffic scheduling algorithm of a TC to be **Strict**, this TC has absolute (strict) priority over other TC strict priorities coming before it (as determined by the TC number: TC 7 is the highest priority, and TC 0 is lowest). It also has an absolute priority over non-strict TCs (ETS). • **ETS:** Enhanced Transmission Selection standard (ETS) exploits the time periods in which the offered load of a particular Traffic Class (TC) is less than its minimum allocated bandwidth by allowing the difference to be available to other traffic classes.
Priority2TC	The mapping of priorities to TCs. For example, to map priorities 0 to 4 to TC 0 and map priorities 5 to 7 to TC 1, configure as follows:

	• Enter **0** in the **Prio 0**, **Prio 1**, **Prio 2**, **Prio 3**, and **Prio 4** fields. • Enter **1** in the **Prio 5**, **Prio 6**, and **Prio 7**.
TCBW	The minimum allocated bandwidth percentage for each Strict or ETS TC. The minimum allocated bandwidth percentages of all Strict or ETS TCs must total 100%. For example, if TC 1, TC 3, and TC 5 use ETS, the minimum allocated bandwidth percentages of these three TCs must total 100%.
PFC	Enables PFC on specific queues. For example, if you select **PFC 0** and **PFC 1**, it means enabling PFC on the queues 0 and 1.

If you selected **Bnxtsetupcc.sh**, input the following information:

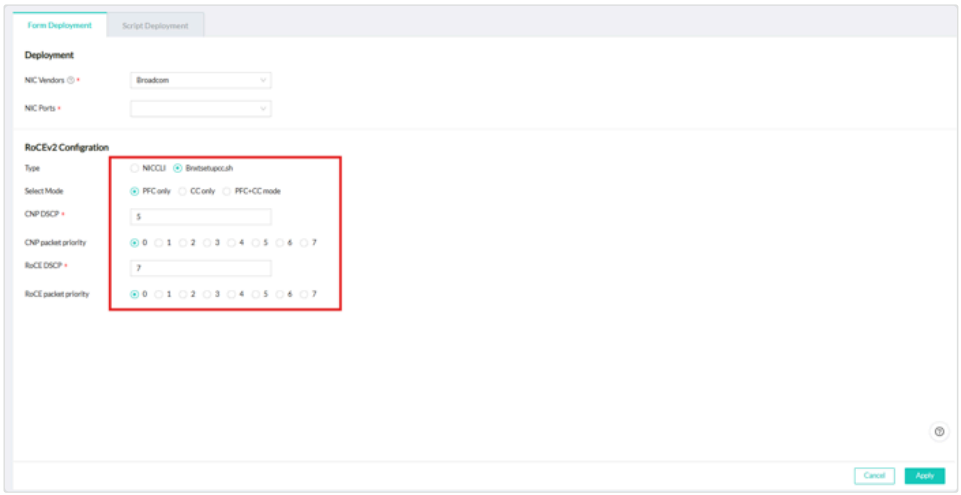


Table 3. Bnxtsetupcc.sh RoCE Configurations

Column	Description
Select Mode	• **PFC Only:** Enables PFC. • **CC Only:** Enables Congestion Control (CC). • **PFC + CC Mode:** Enables PFC and CC.
Tool Type	The tool used to push RoCE configurations.

	• **NICCLI:** A management tool used to perform operations on Broadcom Ethernet network adapters. • **Bnxtccsetup.sh:** The script to modify RoCE QoS and CC related settings and simplify bnxtqos or lldpagent usage.
CNP DSCP	The DSCP priority value (operating at Layer 3) for Congestion Notification Packets (CNP) to prevent CNP packets from being rate-limited or dropped by Layer 3 devices. Valid values range from 0 to 7.
CNP Packet Priority	The priority assigned to CNP packets (operating at Layer 2) used to prioritize CNP control signals. Valid values range from 0 to 7.
RoCE DSCP	The DSCP priority value (operating at Layer 3) used to prioritize service data packets in RDMA traffic. Valid values range from 0 to 63.
RoCE Packet Priority	The DSCP priority value (operating at Layer 2) assigned to RoCE service data packets. Valid values range from 0 to 7.

5. Click **Apply**.

Then, these RoCE configurations are pushed to the selected devices and NICs. To bring these configurations into effect, restart these devices.

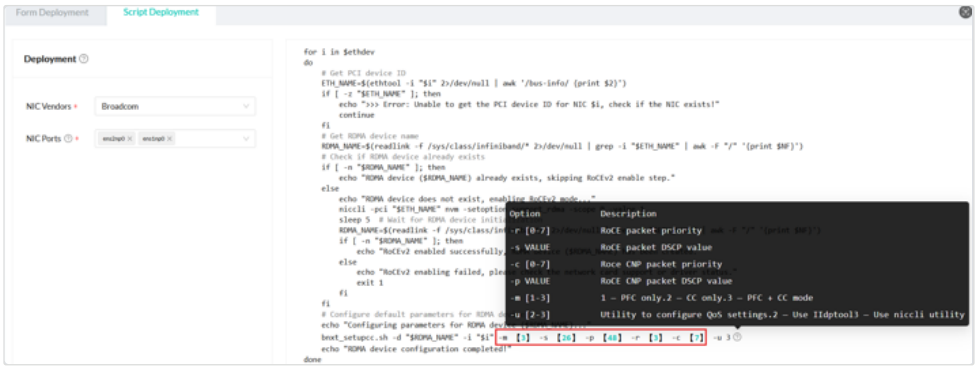
Configuring RoCE through Deployment Scripts

To configure RoCE on NICs through deployment scripts, follow these steps:

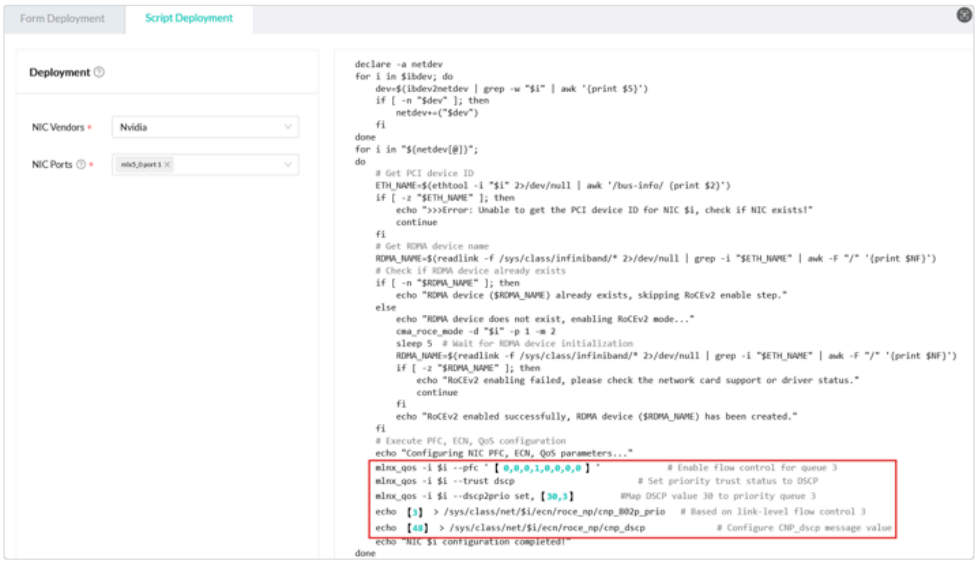
1. Click **Physical Network > RoCE > NIC Configurations** from the navigation bar.
2. In the **Form Deployment** tab, select the vendor of the NIC in the **NIC Vendors** drop-down list, **Nvidia** or **Broadcom**.

3. In the **NIC Ports** drop-down list, select one or multiple devices and the NICs to be configured.
4. In the script area, configure the parameter values in blue.

- For Broadcom NICs, the RoCE configuration script is as follows. Hover over the question icon to see explanations of parameters to be configured.



- For Nvidia NICs, the RoCE configuration script is as follows. Check the comments to see explanations of parameters to be configured.



5. Click **Apply**.

   Then, these RoCE configurations are pushed to the selected devices and NICs. To bring these configurations into effect, restart these devices.

Verifying RoCE Configurations

After you deploy RoCE configurations to NICs, verify whether RoCE configurations are pushed to selected devices successfully.

For more information, see Verifying RoCE Configurations.

Checking RoCE

Before you configure or monitor RoCE, use AmpCon-DC to check the RoCE status on the device first to see whether NIC drivers, RoCE drivers, and RDMA-related tools are installed, whether RoCEv2 and ECN are enabled, and whether QoS and PFC are configured as required.

Prerequisites
Procedure

Prerequisites

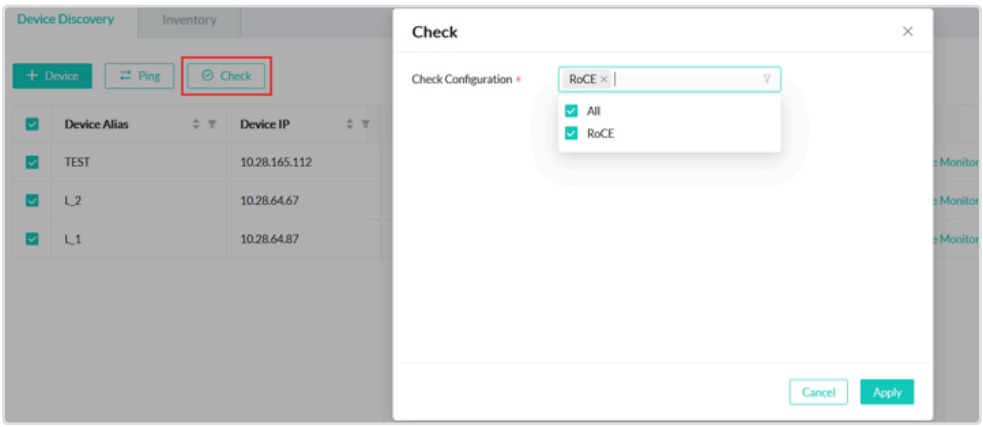
Ensure that the following prerequisites are met:

- The devices to be managed are added to AmpCon-DC with the monitor function enabled. For more information, see Adding Devices.
- The devices to be managed are connected to the AmpCon-DC server. For more information, see Testing Device Connectivity.

Procedure

To check RoCE on one or multiple devices, follow these steps:

1. Click **Device > Hosts** in the AmpCon-DC UI.
2. In the **Device Discovery** tab, select the devices for which you want to check RoCE, and then click **Check**.
3. In the pop-up window, select **RoCE** from the **Check Configuration** list.



4. Click **Apply**.
5. Locate each device that you checked, and then click **Result**.



6. Analyze the checking results to see whether RoCE is configured well.

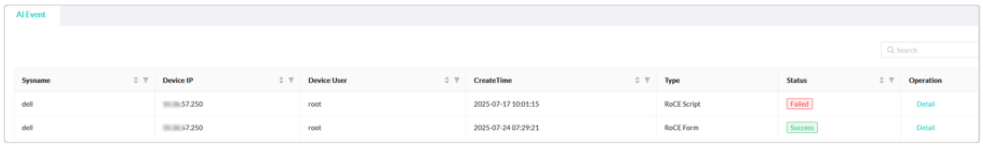
> **NOTEs**
>
> - If NIC drivers, RoCE drivers, and related tools are not installed, install these drivers and tools first before you configure RoCE.
> - If NIC drivers, RoCE drivers, and related tools are installed but RoCEv2 and ECN are not enabled or QoS and PFC are not configured as required, use AmpCon-DC to configure RoCE as described in Configuring RoCE.

Verifying RoCE Configurations

After you deploy RoCE configurations to NICs, verify whether RoCE configurations are pushed to selected devices successfully.

Procedure

1. Click **Monitor > Event Log** from the navigation bar.
2. Locate the device, and then check whether the status is displayed as **Success** in the **Status** column.



See the following description of each column:

Table 1. Event Log Details

Column	Description
Sysname	The hostname of the device.
Device IP	The IP address of the device.
Device User	The user used to log in to the device.
Create Time	The date and time when the RoCE configuration is added.
Status	Whether RoCE configurations are pushed to devices successfully. • **Success:** RoCE configurations are pushed to the device successfully. • **Running:** RoCE configurations are being pushed to the device. • **Fail:** RoCE configurations fail to be pushed to the device due to some errors.
Type	The method used to push RoCE configurations to NICs, **RoCE Script**, or **RoCE Form**.

3. To see more result details, click **Detail** in the **Operation** column.



Configuring Lossless Networks

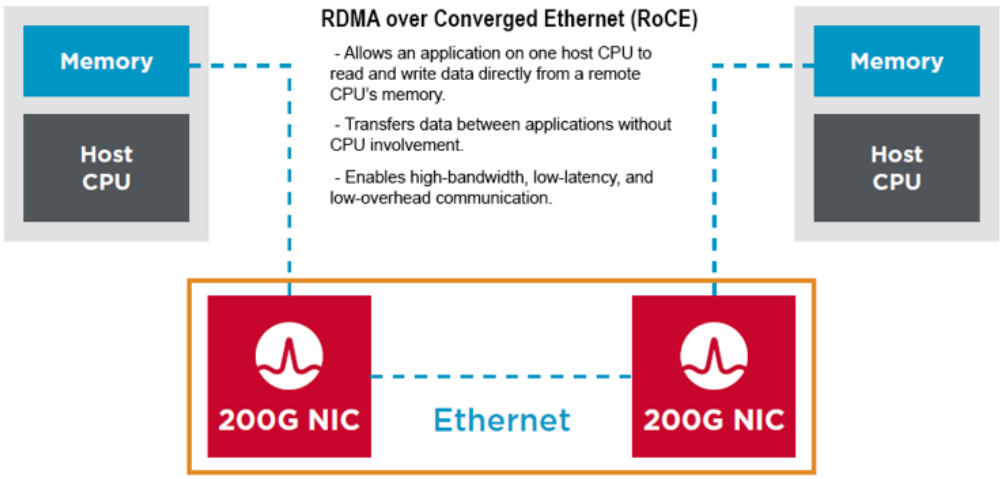
Lossless networking is a powerful network protocol for high-throughput and low-latency data transmission over Ethernet. By leveraging the RDMA over Converged Ethernet (RoCE) technology, lossless networks provide significant advantages for high-demand applications in modern data centers, high-performance computing (HPC) environments, and cloud services.

After you onboard switches, you can configure RoCE on switches.

Benefits of RoCE
Versions of RoCE
Key Features of RoCE
Configuring RoCE EasyDeploy
Configuring RoCE Policies
Configuring Dynamic Load Balancing

Benefits of RoCE

RoCE helps reduce CPU workloads by providing direct memory access for applications that bypass the CPU. Because packet processing and memory access are handled by the network interface card (NIC) and network switch rather than the CPU, RoCE allows for higher throughput, lower latency, and reduced CPU utilization for both the sender and receiver, which is crucial for distributed storage, high-performance computing (HPC), and AI deep learning model training and big data analytics.



Versions of RoCE

RoCE has the following two versions. AmpCon-DC supports only checking and configuring RoCEv2.

- **RoCEv1**: This version operates at Layer 2 of the OSI model, meaning it is not routable beyond the local Ethernet network. It requires all devices to be in the same Ethernet broadcast domain.
- **RoCEv2**: This version operates at Layer 3, making it routable over IP networks. RoCEv2 packets can traverse multiple subnets, allowing for greater scalability and flexibility in network design.

Key Features of RoCE

AmpCon-DC supports configuring and monitoring the following features of RoCE:

- RoCE EasyDeploy
- Priority Flow Control (PFC)
  - PFC Buffer
  - PFC Watchdog
  - PFC Deadlock Prevention
- Explicit Congestion Notification (ECN)
  - Easy ECN
  - Standard ECN
- Quality of Service (QoS)
- Dynamic Load Balancing (DLB)

For more information, see Key Features of RoCE.

Configuring RoCE EasyDeploy

RoCE EasyDeploy in AmpCon-DC enables RoCE configurations with just several clicks, simplifying and accelerating the deployment of RoCE in data center networks.

Easy ECN provides global ECN configurations for congestion management. By using Easy ECN, you can enable or disable ECN in just a click and use default ECN configurations, without manually configuring interface queues, Weighted Random Early Detection (WRED) policies, thresholds, and drop probabilities.

By using the “Easy Deploy” page in the AmpCon-DC UI, you can apply RoCE configurations through the RoCE EasyDeploy function, or you can apply ECN configurations through the Easy ECN function.

For more information, see Configuring RoCE EasyDeploy and Easy ECN.

Configuring RoCE Policies

You can customize RoCE policies (PFC, ECN, and QoS scheduling) based on real-time network conditions and traffic patterns to ensure optimal performance and stability.

For more information, see Configuring RoCE Policies.

Configuring Dynamic Load Balancing

Traditional static load balancing does not consider the utilization of each member link within the load-balancing group, leading to uneven load distribution among the member links.

AmpCon-DC supports Dynamic Load Balancing (DLB), which distribute the traffic of ECMP routing across different member links, maximizing load balancing among the member links.

By using AmpCon-DC, you can easily enable or disable dynamic load balancing for Equal-Cost Multi-Path (ECMP) and select the dynamic load balancing mode, **Normal**, **Optimal**, or **Assigned** mode.

For more information, see Configuring Dynamic Load Balancing.

Key Features of RoCE

AmpCon-DC supports configuring and monitoring the following features of RoCE:

- RoCE EasyDeploy
- Priority Flow Control (PFC)
  - PFC Buffer
  - PFC Watchdog
  - PFC Deadlock Prevention
- Explicit Congestion Notification (ECN)
  - Easy ECN
  - Standard ECN
  - Weighted Random Early Detection (WRED)
- Quality of Service (QoS)
- Dynamic Load Balancing (DLB)

RoCE EasyDeploy

RoCE EasyDeploy is a feature to simplify the deployment and configuration of RDMA over Converged Ethernet (RoCE) on switches, enabling seamless integration with servers for optimized network performance. By using this feature, you can easily select and switch the RoCE mode between lossless and lossy modes, ensuring the best performance for different network environments.

- **Lossless Mode:**
  - Enables both PFC and ECN.
  - Avoids packet loss to ensure reliable and lossless data transmission.
- **Lossy Mode:**
  - Enables only ECN.
  - Allows packet loss to increase improve network throughput.

RoCE EasyDeploy has the following benefits:

- **Rapid deployment with minimal configurations**

  RoCE EasyDeploy requires minimal configuration steps to enable quick deployment of RoCE across all or specific physical ports, reducing the complexity of setting up RoCE. With just several clicks in the AmpCon-DC UI, you can enable or disable RoCE, without manually fine-tuning multiple QoS, PFC, and ECN parameters.

- **Seamless mode switching for different workloads**

  AmpCon-DC supports switching between both the lossless mode (both PFC and ECN enabled for zero packet loss to ensure reliable and lossless data transmission) and lossy

mode (only ECN enabled, suitable for environments where packet loss is acceptable) to meet varying network demands.

- **Optimized default parameters**

  By default, RoCE EasyDeploy applies recommended QoS settings, Weighted Random Early Detection (WRED), and buffer configurations based on the switch model, eliminating the need for manual tuning while ensuring optimal performance.

- **Granular interface-level control**

  You can apply RoCE settings globally to specific switch ports or port queues, providing greater flexibility in network management.

Priority Flow Control (PFC)

PFC is a network protocol designed to manage congestion on Ethernet networks by allowing for independent pausing of traffic based on priority levels.

PFC is a critical technology for managing congestion in Ethernet networks, particularly in data center environments. By enabling traffic differentiation and providing lossless transport for high-priority traffic, PFC helps maintain performance and reliability for critical applications.

The PFC function of PicOS switches supports creating 8 virtual channels on a single Ethernet link, with each channel assigned a distinct priority level. Specific virtual channels can be paused and restarted to ensure uninterrupted traffic flow through the other virtual channels.

PFC operates using the following key components and steps:

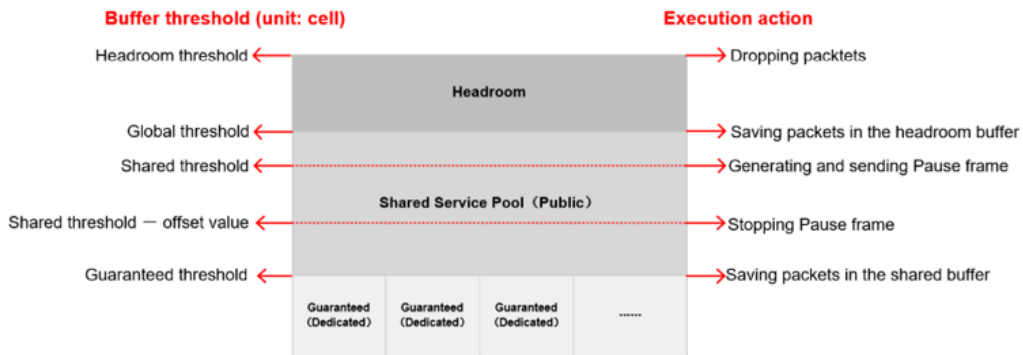
1. **Traffic classification**: Network traffic is classified into different priorities based on the IEEE 802.1p standard, which defines eight priority levels (0-7). Each priority level corresponds to a specific type of traffic, such as storage, voice, or best-effort data.
2. **Priority mapping**: The switch maps traffic to these priority levels by using VLAN tags (802.1Q) or Differentiated Services Code Point (DSCP) values. Each priority level is associated with a separate queue within the switch.
3. **Congestion detection**: When a switch detects congestion in one of its priority queues (such as due to high traffic volume or insufficient buffer space), it generates a PFC frame for that specific priority level.
4. **PFC frame transmission**: The PFC frame, also known as a PAUSE frame, is sent to the upstream device (such as another switch or a network interface card in a server). This frame instructs the upstream device to pause the transmission of traffic for the specified priority level.

5. **Traffic pause**: Upon receiving the PFC frame, the upstream device temporarily stops sending traffic of the specified priority to the congested switch. Other traffic classes (priorities) continue to flow without interruption, ensuring that only the affected traffic is paused.
6. **Congestion alleviation**: The switch continues to process and forward the paused traffic until the congestion is alleviated. After the buffer space is available, the switch sends another PFC frame to the upstream device to resume the paused traffic flow.
7. **Resume transmission**: The upstream device resumes sending traffic for the previously paused priority, restoring normal traffic flow.

PFC Buffer

The buffer is configured to implement traffic control and PFC watchdog, which is based on interface and priority queue. The storage space of each interface is divided into different buffers independently, and a certain action will be executed after the number of accumulated packets reaches the buffer threshold (the unit is cell).

- **Guaranteed**: The dedicated buffer available for a specified queue. This buffer space cannot be used by other queues.
- **Shared**: The public buffer available for all queues. The shared buffer will be occupied when the guaranteed buffer reaches the threshold.
- **Headroom**: The maximum number of cell resources available for packets with a specific 802.1p priority. When the occupied shared buffer reaches the threshold, the packets will be saved in the headroom buffer.



PFC Watchdog

PFC Watchdog is a critical component in Ethernet networks that use PFC to manage congestion. By detecting and mitigating PFC deadlocks, it ensures that the network remains

stable and performs optimally. This mechanism is particularly important in data centers and other environments where maintaining high performance and reliability is crucial.

PFC Deadlock Prevention

Consider a data center running RoCE traffic for high-performance computing workloads. These workloads require low-latency, lossless traffic flow, which PFC is used to enforce. However, as network congestion builds up, PFC pause frames are triggered, potentially leading to a deadlock if multiple paths become blocked.

By employing a PFC deadlock prevention solution, the network can identify RoCE flows that are prone to triggering deadlocks. The solution adjusts the queue priorities so that other critical flows are not blocked, and it reduces the load on congested paths. This prevents the generation of circular wait conditions and ensures the smooth operation of high-priority traffic, ensuring that business-critical applications continue to function smoothly without being interrupted by PFC-induced deadlocks.

Explicit Congestion Notification (ECN)

ECN is a network protocol for managing network congestion by marking packets instead of dropping them. This approach allows the sender to reduce its transmission rate proactively, improving overall network performance.

- It is an extension of the IP and TCP protocols, enhancing the way congestion is managed by marking packets instead of discarding them.
- It helps improve network performance, reduce packet loss, and maintain high throughput, making it especially valuable in data centers and for real-time applications.

When congestion occurs, PicOS switches mark packets by using ECN. Upon receiving an ECN-marked packet, the receiving end detects the ECN flag, identifies the congestion, and sends a Congestion Notification Packet (CNP) back to the sender.

Then, the sender is informed of the congestion and will reduce the packet sending rate to prevent further congestion escalation.

Easy ECN

The Easy ECN feature streamlines the traditionally complex configuration of ECN by eliminating the need for manual setup of interface queues, Weighted Random Early Detection (WRED) policies, thresholds, and drop probabilities.

Easy ECN simplifies all of these by allowing users to configure ECN with just a single command, focusing on the network's traffic optimization strategy.

Network administrators can efficiently configure ECN with a focus on either throughput or latency globally for all the interface queues, without needing to manually set all the individual parameters for each interface queue. This simplified approach not only saves time but also ensures more consistent and effective congestion management.

Standard ECN

Standard ECN configurations requires you to configure multiple ECN parameters such as:

- **Enabling ECN** on specific interface queues, ensuring that the network is aware of which traffic classes need to use ECN.
- **Setting WRED thresholds**, which determine at what point packets will be marked or dropped based on queue depth.
- **Configuring the maximum packet drop probability**, dictating how likely a packet is to be dropped when congestion is high.

Weighted Random Early Detection (WRED)

On PicOS switches, ECN is used in conjunction with WRED to provide early signals of congestion, avoiding packet loss and improving network performance.

WRED is an active queue management (AQM) mechanism that selectively drops packets based on the average queue length, helping you to manage congestion before the queue becomes full. When combined with ECN, WRED can mark packets instead of dropping them when congestion is detected.

Quality of Service (QoS)

QoS is a network mechanism used to manage and ensure different levels of quality and performance for different types of traffic in a network. QoS aims to control the transmission priority of data packets through network devices, protocols, and mechanisms, thereby ensuring priority processing for critical tasks and reducing issues such as latency, packet loss, and jitter.

Dynamic Load Balancing (DLB)

Traditional static load balancing does not consider the utilization of each member link within the load-balancing group, leading to uneven load distribution among the member links. This issue becomes more pronounced with the appearance of large data flows, exacerbating congestion on the selected member link and potentially causing packet loss.

DLB is a network management technique used to distribute network traffic across multiple paths or resources dynamically. Unlike static load balancing, which assigns fixed routes or resources

to handle traffic, dynamic load balancing adjusts traffic distribution in real-time based on current network conditions.

By enabling DLB, the traffic of Equal-Cost Multi-Path (ECMP) routing can be distributed across different member links through dynamic load balancing, maximizing load balancing among the member links.

Three modes of Dynamic load balancing are supported: **Normal Mode**, **Optimal Mode** and **Assigned Mode**. For detailed explanation of each mode, see DLB Implementation Principle.

Configuring RoCE EasyDeploy and Easy ECN

RoCE EasyDeploy in AmpCon-DC enables RoCE configurations with just several clicks, simplifying and accelerating the deployment of RoCE in data center networks.

Easy ECN provides global ECN configurations for congestion management. By using Easy ECN, you can enable or disable ECN in just several clicks and use default ECN configurations, without manually configuring interface queues, Weighted Random Early Detection (WRED) policies, thresholds, and drop probabilities.

By using the “EasyDeploy” page in the AmpCon-DC UI, you can apply RoCE configurations to switches through the RoCE EasyDeploy function, or you can apply ECN configurations to switches through the Easy ECN function.

Configuring RoCE EasyDeploy
- Guidelines
- Configuration Procedure
- Viewing Pushed Configurations
- What to Do Next

Configuring Easy ECN
- Guidelines
- Configuring Procedure
- Viewing Pushed Configurations
- What to Do Next

Configuring RoCE EasyDeploy

Guidelines

Before you configure RoCE EasyDeploy, read the following guidelines carefully:

- Ensure that the RoCE EasyDeploy feature is supported on the PicOS switches to be configured. For more information, see PICOS Supported Features.
- To make RoCE EasyDeploy configurations work, configure the same RoCE EasyDeploy configurations on all ports through which the packets flow.
- For switches with Easy ECN enabled, RoCE EasyDeploy can’t be enabled.
- The queue numbers to enable RoCE on the switch side and on the server side need to align to ensure balanced traffic scheduling and prevent uneven load distribution.
- AmpCon-DC predefines the following parameter values in the RoCE EasyDeploy feature, and thus you don’t need to configure them.
  - The ingress queue parameters (threshold/guaranteed/headroom/reset-offset) of PFC default buffer

- The WRED parameters (max-thresh/min-thresh/drop-probability) adapted to different switch chips automatically

Configuration Procedure

To configure RoCE EasyDeploy, follow these steps:

1. Click **Physical Network > RoCE > EasyDeploy** from the navigation bar.
2. In the **RoCE EasyDeploy** tab, click **+ Configuration**.
3. In the pop-up window, configure RoCE EasyDeploy as follows:



a. In the **RoCE EasyDeploy** radio box, select **Enable** to enable RoCE EasyDeploy, or select **Disable** to disable RoCE EasyDeploy.

b. If you select **Enable**, select the RoCE mode (**Lossless** or **Lossy**) in the **Mode** radio box.

> **Tips**
>
> - **Lossless mode:** Enables both PFC and ECN. Avoids packet loss to ensure reliable and lossless data transmission.
> - **Lossy mode:** Enables only ECN. Allows packet loss to increase improve network throughput.

c. In the **Configuration Details** section, input the following information to apply RoCE configurations to specific switches, physical ports, and queues.

Table 1. RoCE EasyDeploy Application Scope

Parameter	Description
Fabric	Select one or multiple fabrics. • If you selected **All Fabrics**, all switches in all fabrics are selected automatically and cannot be changed in the **Sysname**

	section, and all ports will be selected in the **Ports** section. • You can see only the fabrics containing at least one switch that is online and supports RoCE.
Sysname	Select one or multiple switch hostnames. If you select **All** or select more than 1 switch, all ports will be selected in the **Ports** section.
Ports	Select one or multiple physical ports to apply RoCE EasyDeploy configurations. • To apply RoCE EasyDeploy configurations to all ports, click **All Ports** from the list. • To apply RoCE EasyDeploy configurations to specific ports, click the ports one by one in the list.
Queues	Select one or multiple queues to apply RoCE EasyDeploy configurations. Values are 0, 1, 2, 4, 5, 7. • RoCE EasyDeploy is applied to the queue 3 by default. • The queue 6 is used for Congestion Notification Packet (CNP) traffic by default. • To apply RoCE EasyDeploy configurations to all queues, click **All** from the list. • To apply RoCE EasyDeploy configurations to specific queues, click the queues one by one in the list.

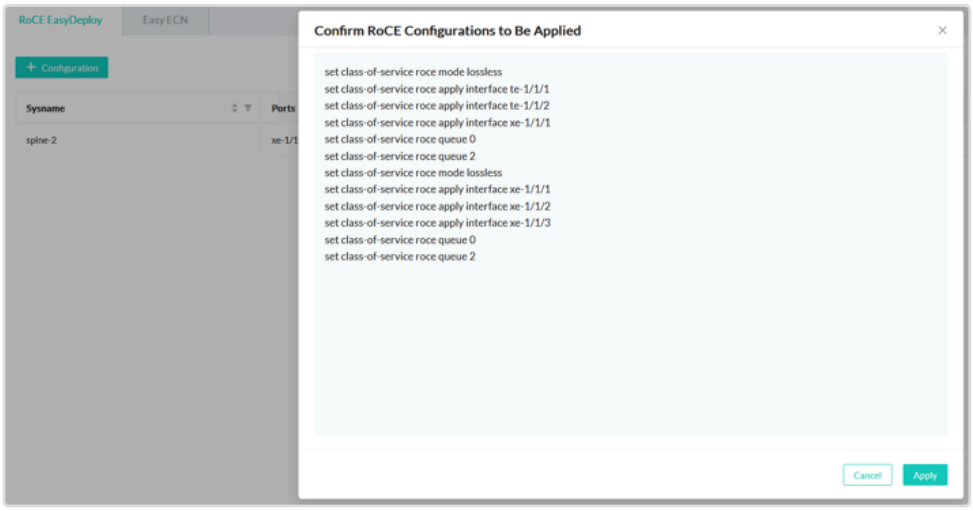
Tips

- To remove selected ports, queues, or switches, click the remove icon **x**.
- To add multiple lines, click the add icon **+** at the end of the first line.

- To remove a line, click the remove icon **-** at the end of the line.

d. Click **Apply**.

4. Check the RoCE configurations in the pop-up window, and then click **Apply** to complete the RoCE EasyDeploy configurations.



Viewing Pushed Configurations

To check the pushed RoCE configurations, follow the steps:

> **NOTE**
>
> For switches that have RoCE EasyDeploy configured but are not connected with the AmpCon-DC server, RoCE configurations can't be displayed.

1. Click **Physical Network > RoCE > EasyDeploy** from the navigation bar.
2. In the **RoCE EasyDeploy** tab, locate a switch, and then click **View** in the **Operation** column.

   In the pop-up window, you can see the RoCE configurations pushed through RoCE EasyDeploy.



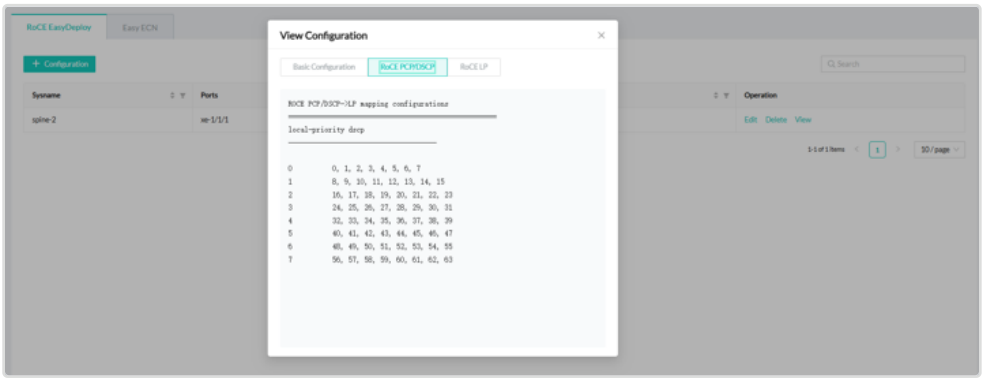
In the **Basic Configuration** tab, you can see the following information:

Table 2. Basic RoCE Configurations

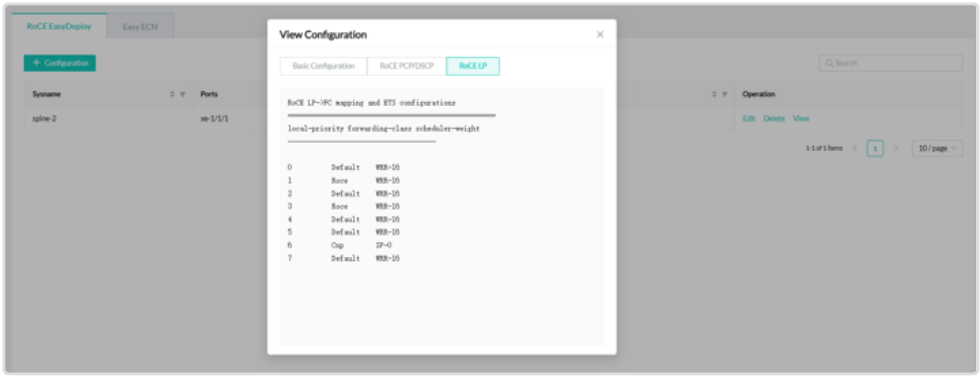
Metric	Description
RoCE EasyDeploy Status	Whether RoCE EasyDeploy configurations are applied or not.
RoCE Mode	The RoCE mode, **Lossless** or **Lossy**.
Congestion Mode	The protocol used for congestion management. RoCE EasyDeploy enables ECN as the congestion management protocol.
Enabled Queue	The queues with RoCE EasyDeploy configurations applied.
Max Threshold	The maximum average queue size at which WRED starts to drop packets with the configured **Probability** value.
Min Threshold	The minimum average queue size at which WRED starts to mark packets.
Probability	The probability that a packet will be marked with ECN when the average queue size is between the minimum and maximum thresholds.
PFC Priority	The 8 distinct priority levels (0–7) in PFC.
Rx Enabled	Whether the switches enable the Receive Function (Rx).

Tx Enabled	Whether the switches enable the Transmit Function (Tx).
Trust Mode	The key mechanism in network devices for determining how to prioritize data packets, whose core function is to identify priority markings in packet headers (such as 802.1p or DSCP), ensuring critical traffic is transmitted first during network congestion. • PicOS supports three trust modes: DSCP, IEEE 802.1p, and inet-precedence. • RoCE EasyDeploy enables DSCP as the trust mode by default.

3. Click the **RoCE PCP/DSCP** tab. Then, you can see the following mapping information:



4. Click the **RoCE LP** sub-tab. Then, you can see the following mapping information:



What to Do Next

- Post-deployment fine-tuning of PFC, ECN, and QoS settings is supported and needs to be dynamically adjusted based on real-time network conditions and traffic patterns to ensure optimal performance and stability. For more information, see Configuring RoCE Policies.

- Monitor RoCE statistics to ensure configurations are applied correctly, and adjust QoS and buffer parameters if needed. For more information, see RoCE Data on Switches.

Configuring Easy ECN

Guidelines

Before you configure Easy ECN, read the following guidelines carefully:

- Ensure that the ECN and Easy ECN features are supported on the PicOS switches to be configured. For more information, see PICOS Supported Features.
- To make ECN configurations work, ensure that ECN is enabled on all ports through which the packets flow.
- For switches with RoCE EasyDeploy enabled, RoCE Easy ECN can't be enabled.

Configuring Procedure

To configure Easy ECN, follow these steps:

1. Click **Physical Network > RoCE > EasyDeploy** from the navigation bar.
2. Click the **Easy ECN** tab.
3. Click **+ Configuration**, and then input the following information:



Table 3. Easy ECN Parameters

Parameter	Description
Sysname	Select one or multiple switch hostnames.
Easy ECN	Select **Enable** to enable ECN, or select **Disable** to disable ECN.
ECN Mode	Select the Easy ECN mode, **Latency First**, or **Throughput First**.

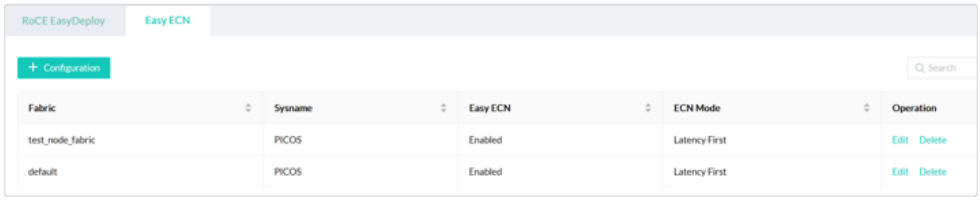
- **Latency First:** This mode prioritizes minimizing latency, ensuring that packets experience the least possible delay. This is particularly important for real-time applications such as VoIP, video conferencing, or online gaming, where even small delays can negatively impact performance.
- **Throughput First:** This mode prioritizes maximizing the amount of data transferred across the network, making it ideal for use cases such as bulk data transfers or content delivery systems.

> **NOTE**
>
> This section is available only if you select **Enable** in the **Easy ECN** section.

4. Click **Apply**.

Viewing Pushed Configurations

1. Click **Physical Network > RoCE > EasyDeploy** from the navigation bar.
2. Click the **Easy ECN** tab. In this tab, check the pushed Easy ECN configurations.



> **Tips**
>
- To edit the Easy ECN configurations of a switch, locate the switch, and then click **Edit**.
- To delete the Easy ECN configurations of a switch, locate the switch, and then click **Delete**.

What to Do Next

- Continuously monitor network performance and ECN marking rates, and make dynamic adjustments to ECN thresholds as needed to respond to changing network conditions.
- You can check ECN marking rates in the telemetry data of a switch. For more information, see Telemetry Data of a Switch - AI.
- If more granular control is required, use RoCE Policies to apply ECN configurations on specific interface queues. For more information, see Configuring RoCE Policies.

Configuring RoCE Policies

If RoCE EasyDeploy and Easy ECN can't meet your needs, you can apply RoCE configurations to switches through customized policies that adapt to real-time network conditions and traffic patterns.

During the simplified ZTP process, you can push RoCE configurations (including PFC, ECN, and QoS configurations) by configuring a RoCE policy in the related ZTP template. The simplified ZTP process can achieve the following goals in one go:

- A physical network (fabric) is deployed automatically.
- All switches in the fabric are onboarded to AmpCon-DC.
- The RoCE policy configurations are applied to the switches in the fabric.

After a fabric is deployed, you can also push customized RoCE policies to switches by creating a RoCE policy on the "RoCE Policies" page.

Guidelines
Prerequisites
Creating a RoCE Policy
1. RoCE Policy Configuration
2. RoCE Template for Switches
Checking the Pushing Results
Optional Operations
Editing a RoCE Policy
Deleting a RoCE Policy

Guidelines

Before you configure RoCE policies, read the following guidelines carefully:

- To prevent packet loss due to congestion during transmission, it's recommended to configure the same PFC configurations on all ports through which the packets flow.
- To make ECN configurations work, it's recommended that ECN is enabled on all ports through which the packets flow.
- The new RoCE configurations will occupy the previous RoCE configurations (such as the default PFC configurations previously pushed through RoCE EasyDeploy).
- The RoCE policy configurations added during the simplified ZTP process will be displayed both on the "RoCE Policies" page and in the **RoCE Policy** tab of the fabric page.

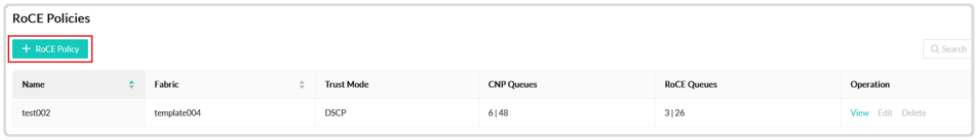
Prerequisites

- Ensure that the switches to be configured support RoCE (PFC, ECN, and QoS). For more information, see PICOS Supported Features.
- If you want to apply RoCE policy configurations to a fabric in **Simplified ZTP** type, ensure that the fabric meets all of the following conditions:
  - The fabric has been successfully deployed through simplified ZTP. To check fabric deployment status, see Viewing All Fabrics.
  - The **Service Network Type** specified in the related ZTP template is **VLAN**.
  - The **Leaf Strategy** specified in the related ZTP template is **None**.
  - No RoCE policy has been configured for the fabric.
- If you want to apply RoCE policy configurations to a fabric in **Manual** type, ensure that the fabric meets all of the following conditions:
  - The fabric has not been associated with a DC template.
  - No RoCE policy has been configured for the fabric.
- Ensure that the switches to be configured are online, which means the switches are currently connected to AmpCon-DC. To check a switch status, see Viewing the Switch List.

Creating a RoCE Policy

To add a RoCE policy, follow these steps:

1. Click **Physical Network > RoCE > RoCE Policies** from the navigation bar.
2. On the “RoCE Policies” page, click **+ RoCE Policy**.



Then, in the **Create RoCE Policy** pop-up window, complete the following processes:

1. RoCE Policy Configuration

1. In the **Basic Information** section, input the name of the RoCE policy, and then select a fabric.

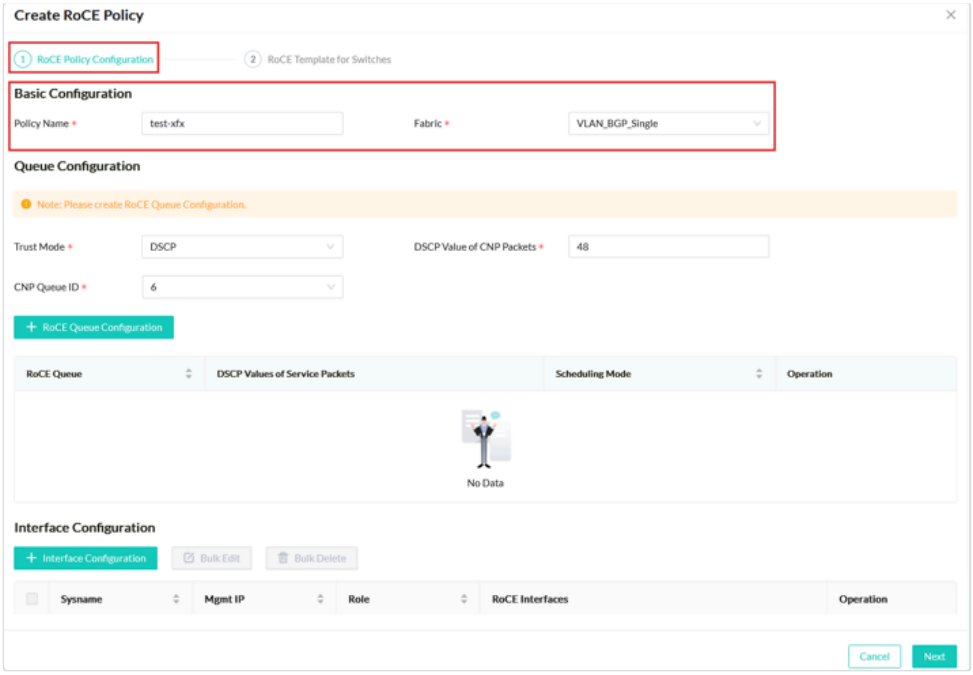


Table 1. Basic Configuration Parameters

Parameter	Description
Policy Name	The name of the RoCE policy. • The name must be unique. • The name must be a string with at most 64 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ -). • The name cannot start or end with spaces.
Fabric	The fabric associated with the RoCE policy. **NOTEs** • For fabrics in **Simplified ZTP** type, the drop-down list displays only the fabrics that meet all of the following conditions: ◦ The fabric status is **Deployed**. ◦ The **Service Network Type** specified in the related ZTP template is **VLAN**.

	◦ The **Leaf Strategy** specified in the related ZTP template is **None**. ◦ No RoCE policy has been configured for the fabric. • For fabrics in **Manual** type, the drop-down list displays only the fabrics that meet all of the following conditions: ◦ The fabric has not been associated with a DC template. ◦ No RoCE policy has been configured for the fabric.

2. In the **Queue Configuration** section, configure as follows:
   a. Input the following information:



Table 2. Queue Configuration Parameters

Parameter	Description
Trust Mode	The key mechanism for determining how to prioritize data packets. The core function of this mechanism is to identify priority markings in packet headers (DSCP or 802.1q), ensuring critical traffic is transmitted first during network congestion. • **DSCP**: The switches trust the DSCP value in the IP header. If this mode is selected, you must also configure the **DSCP Value of CNP Packets** field. • **802.1q**: The switches trust the 802.1q priority value in the VLAN tag. If this mode is selected, you must also configure the **802.1q Value of CNP Packets** field.

	NOTE If you change the trust mode, the configurations you made in **RoCE Queue Configuration** and **Interface Configuration** will be cleared.
DSCP Value of CNP Packets	The DSCP value for Congestion Notification Packet (CNP). This field specifies the priority of CNP packets. The priority is mapped to the corresponding switch port queue. A larger value indicates a higher priority. **NOTEs** • The default value is 48. You can modify it to any value ranging from 0 to 63. • The **DSCP Values of Service Packets** and **DSCP Values of CNP Packets** cannot overlap.
802.1q Value of CNP Packets	The 802.1q value for CNP packets. This field specifies the priority of CNP packets. The priority is mapped to the corresponding switch port queue. A larger value indicates a higher priority. **NOTEs** • The default value is 6. You can modify it to any value ranging from 0 to 7. • The **802.1q Values of Service Packets** and **802.1q Values of CNP Packets** cannot overlap.

CNP Queue ID	The priority queue used to forward CNP packets. The valid value range is 0 to 7. CNP packets are control packets used to notify switches when network congestion occurs. • If **Trust Mode** is set to **DSCP**, you can enter any value from 0 to 7. The default value is 6. • If **Trust Mode** is set to **802.1q**, the value is automatically synchronized with the **802.1q Value of CNP Packets**. For example, if the **802.1q Value of CNP Packets** is set to 6, the value will be automatically changed to 6.

b. To configure RoCE queues mapping for service packets and define scheduling mode for RoCE queues, click **+ RoCE Queue Configuration**. Input the following information, and then click **Apply**.

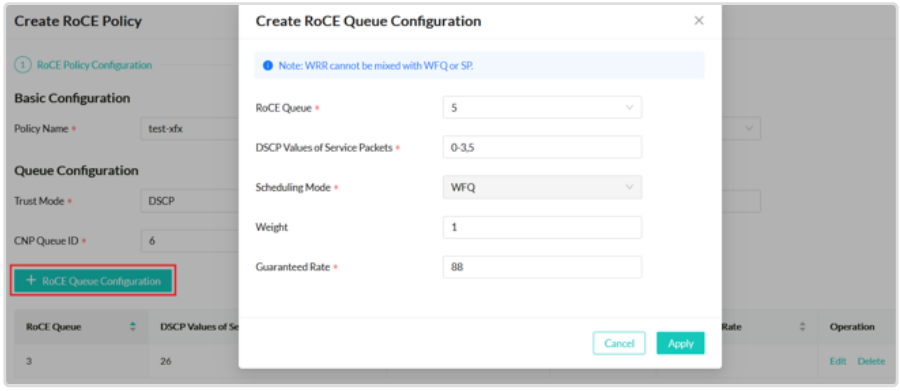


Table 3. RoCE Queue Parameters

Parameter	Description
RoCE Queue	The RoCE queue to be configured. The valid value range is 0 to 7. **NOTEs** • The **RoCE Queue** value must be less than the **CNP Queue ID** value.

	• You cannot select a queue that has already been created. • If the trust mode you select is **802.1q**, the value is automatically synchronized with the **802.1q Value of Service Packets**. For example, if the **802.1q Value of Service Packets** is set to 6, the value will automatically change to 6.
DSCP Values of Service Packets	If the trust mode you select is DSCP, this field is displayed. The DSCP values of service packets that are mapped to the configured RoCE queue. **NOTEs** • The valid value range is 0 to 63. You can specify: ◦ A single value, such as 26. ◦ A range of values, such as 16-24. ◦ Multiple values and ranges combined, separated by commas, such as 39,16-24. • The value must not contain spaces. • The **DSCP Values of Service Packets** and **DSCP Values of CNP Packets** cannot overlap. • The **DSCP Values of Service Packets** in the selected fabric can't be duplicated.
802.1q Values of Service Packets	If the trust mode you select is **802.1q**, this field is displayed. The 802.1q values of service packets that are mapped to the configured RoCE queue. **NOTEs** • The valid value range is 0 to 7.

	• The **802.1q Values of Service Packets** and **802.1q Values of CNP Packets** cannot overlap. • The **802.1q Values of Service Packets** in the selected fabric can't be duplicated.
Scheduling Mode	Select the QoS scheduling mode. The QoS scheduling mode determines how bandwidth is allocated among queues when multiple queues on the same port have traffic to send. The working mode can be **SP**, **WRR**, or **WFQ**. The **WRR** mode is selected by default. • **SP:** Short for Strict Priority. When two PCs send 100% traffic to the same PC, all packets from the lower-priority PC will be discarded. • **WRR:** Short for Weighted Round Robin. In this mode, you can configure weight. If PC-A and PC-B send 100% traffic to the same PC-C, the PC-C will receive packets from PC-A and PC-B according to the weight proportion in the corresponding queue. • **WFQ:** Short for Weighted Fair Queuing. In this mode, you can configure a guaranteed rate and weight. If PC-A and PC-B send 100% traffic to the same PC-C, PC-C will receive packets from PC-A and PC-B according to the weight proportion and the guaranteed rate in the corresponding queue. **NOTE** All queues must use the same scheduling mode. For example, if you add a RoCE queue configuration and select **WRR** as the

	scheduling mode, then when you add a second RoCE queue configuration, the **Scheduling Mode** will be automatically set to **WRR**, and the field will be grayed out and cannot be modified.
Weight	The QoS weight. Values range from 1 to 15. Each weight is a numerical value assigned to different traffic classes or queues in QoS, determining the available bandwidth percentage when using weighted QoS scheduling modes. **NOTE** This field is displayed if you select the **WFQ** or **WRR** scheduling mode.
Guaranteed Rate	Enter the Guaranteed Rate, which is the minimum bandwidth assured for specific traffic flow, ensuring consistent performance even during network congestion. Values range from 8 to 40000000. **NOTE** This field is displayed only if you select the **WFQ** scheduling mode.

3. In the **Interface Configuration** section, click **+ Interface Configuration**, and then configure as follows:

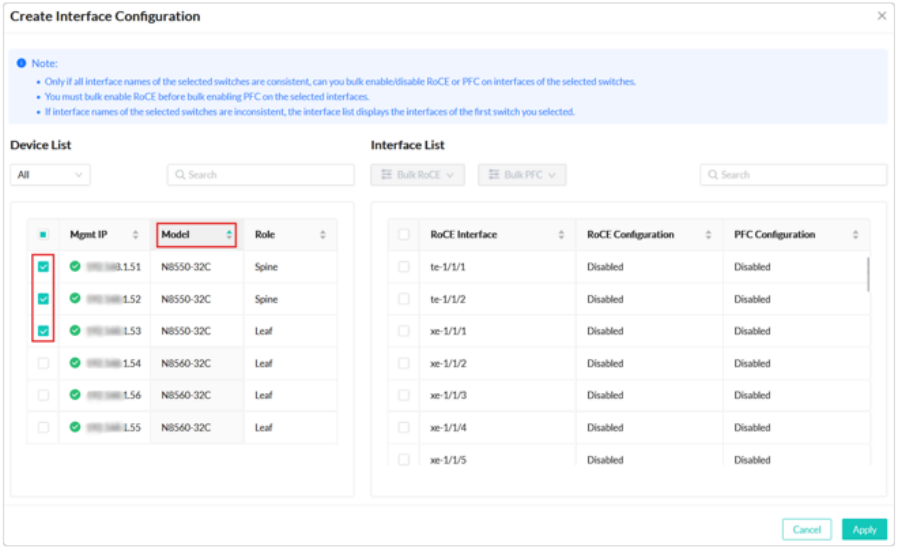
   a. In the pop-up window, select one or multiple switches of the same model in the **Device List** section.

   NOTEs

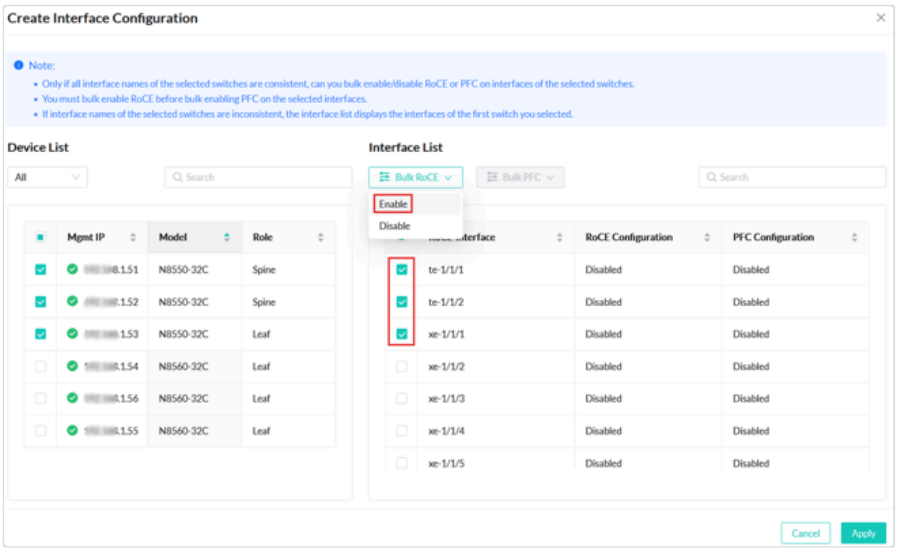
   - The **Device List** has no data in the following cases:

- You have added interface configurations for all switches in the selected fabric.
- The selected fabric has no switches.
- None of the switches in the selected fabric supports RoCE.

- You can filter the displayed switches in the drop-down list based on their roles in the fabric. The available filter options are **Spine**, **Leaf**, and **All**.



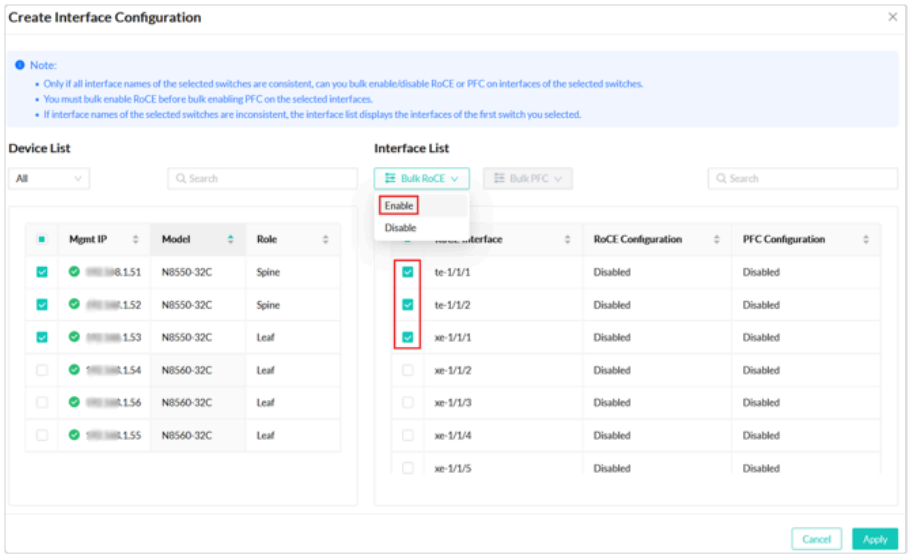
b. In the **Interface List** section, the interfaces of the selected switches will be displayed. Select one or multiple interfaces, hover your mouse over **Bulk RoCE**, and then click **Enable**.



Tips

- The **RoCE Configuration** column will be displayed as **Enabled** for these selected interfaces.
- To disable RoCE, select the interfaces, hover your mouse over **Bulk RoCE**, and then click **Disable**.
- If the models of the selected switches are not consistent, the interface of the first switch you selected will be displayed. In this case, the **Bulk RoCE** and **Bulk PFC** are grayed out.

c. Optional: Hover your mouse over **Bulk PFC**, and then click **Enable**.

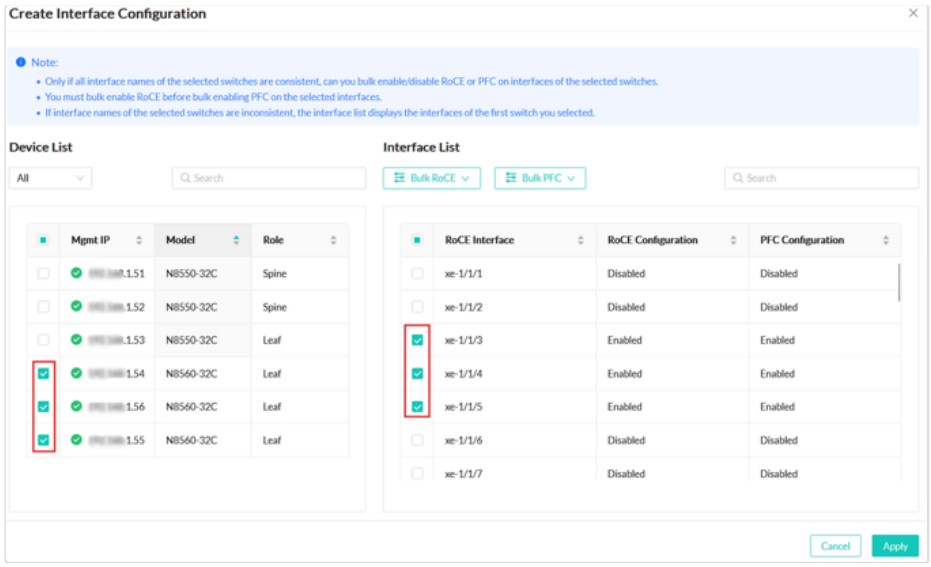


Tips

- The **PFC Configuration** column will be displayed as **Enabled** for these selected interfaces.
- To disable PFC, select the interfaces, hover your mouse over **Bulk PFC**, and then click **Disable**.
- PFC can be enabled only after RoCE is enabled on interfaces. If RoCE is not enabled, the **Bulk PFC** button is grayed out.

d. Click **Apply**.

e. Optional: Repeat **Step a** to **Step d** to enable RoCE and PFC for interfaces of other switches in the fabric.



4. Click **Next** to go to the **RoCE Template for Switches** process.

2. RoCE Template for Switches

In this process, configure a RoCE template for the selected spine and leaf switches.

Spine Tab

In this tab, you can see all spine switch models you have selected in the **Interface Configuration** section. Click each switch model, and then configure it as follows:

1. In the **Global Interface Configuration** section, input the following information:

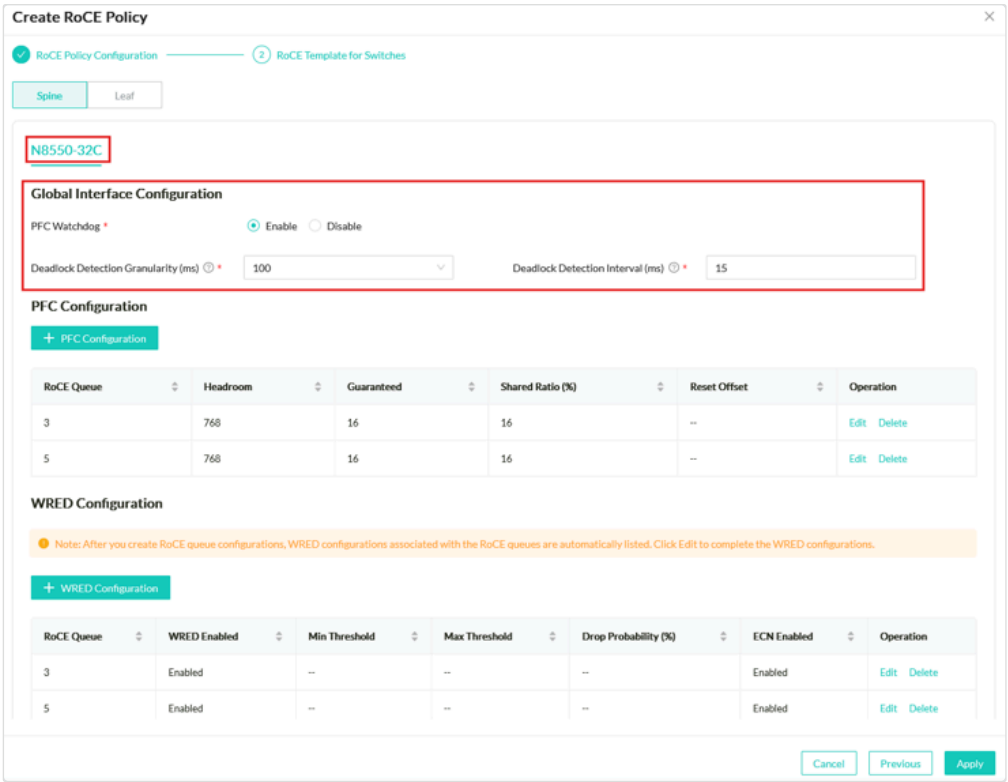


Table 4. Global Interface Configuration Parameters

Parameter	Description
PFC Watchdog	Specify whether to enable the PFC watchdog. PFC watchdog is designed to detect and resolve PFC deadlocks. It monitors the duration of PFC pause frames and takes corrective actions if a potential deadlock is detected.
Deadlock Detection Granularity	The granularity of the PFC deadlock detection timer and restore timer. The value could be 10 or 100, in milliseconds. The default value is 100.
Deadlock Detection Interval	The time interval of PFC deadlock detection. The value is an integer that ranges from 1 to 15, in milliseconds. The default value is 15.

2. In the **PFC Configuration** section, locate each PFC configuration item, and click **Edit**.

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

> **NOTEs**
>
> - If you do not enable PFC on the interfaces of this switch model in the **Interface Configuration** section, the PFC configurations here will not be pushed to the switch interfaces.
> - If all RoCE queues defined in the **RoCE Queue Configuration** section already have corresponding PFC configurations, the **+ PFC Configuration** cannot be clicked.
> - If a RoCE queue ID is modified in the **RoCE Queue Configuration** section, the corresponding **RoCE Queue** field in the PFC configuration is automatically updated. Other PFC parameters remain unchanged.
> - If a RoCE queue is deleted in the **RoCE Queue Configuration** section, the related PFC configuration entry is automatically removed.

- To delete the PFC configurations you configured for a RoCE queue, locate the RoCE queue, and then click **Delete**.

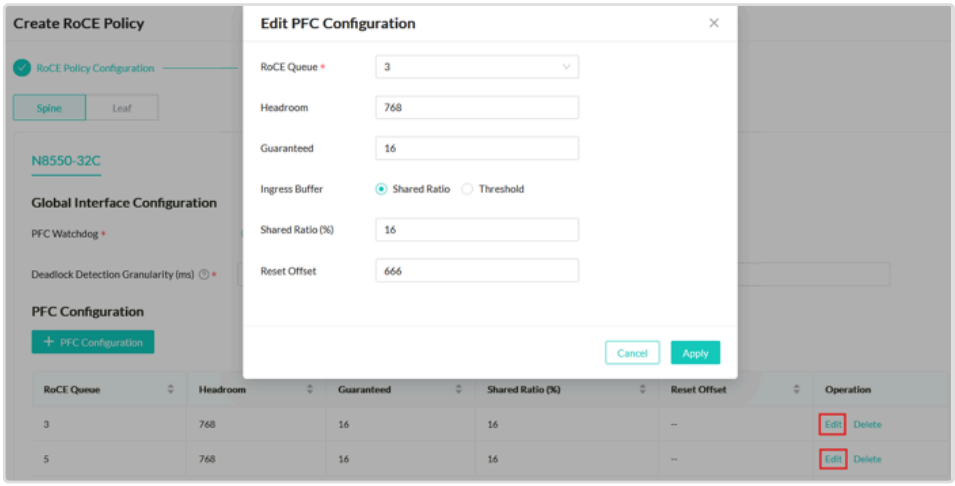


Table 5. PFC Configuration Parameters

Parameter	Description
RoCE Queue	The RoCE queue to be configured. **NOTE** Only RoCE queues defined in the **RoCE Queue Configuration** section are displayed in this drop-down list.
Headroom	The upper threshold of headroom buffer for a PFC queue on the ingress interface. When the headroom buffer threshold is reached, the received packets will be dropped. The value is an integer that ranges from 1 to 65535, and the unit is cell. The default value is 768.
Guaranteed	The upper threshold of guaranteed buffer for a PFC queue on the ingress interface. When the guaranteed buffer threshold is reached, the packets will occupy the shared service pool.

	The value is an integer that ranges from 1 to 65535, and the unit is cell. The default value is 16.
Ingress Buffer	Select the **Shared Ratio** or **Threshold**.
Shared Ratio (%)	The value of the dynamic threshold ratio of the available shared space. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 16. **NOTE** This field is displayed only if select **Shared Ratio** in the **Ingress Buffer** section.
Threshold	The static threshold of the shared buffer for a PFC queue on the ingress interface. When the occupied buffer space exceeds the specified threshold, the Pause frame will be generated and sent to the egress interface. The value must be an integer that ranges from 1 to 65535, and the unit is cell. **NOTE** This field is displayed only if select **Threshold** in the **Ingress Buffer** section.
Reset Offset	The offset value of the shared buffer for a PFC queue on the ingress interface. The Pause frames will stop being generated when the occupied space is reduced to a certain level (the upper threshold minus the offset value). The value is an integer that ranges from 1 to 65535, and the unit is cell.

3. In the **WRED Configuration** section, locate each WRED configuration item, and click **Edit**.

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

NOTEs

- RoCE policy configurations can be applied only when all switches to be configured are online.
- If all RoCE queues defined in the **RoCE Queue Configuration** section already have corresponding WRED configurations, the **+ WRED Configuration** cannot be clicked.
- If a RoCE queue ID is modified in the **RoCE Queue Configuration** section, the corresponding **RoCE Queue** field in the WRED configuration is automatically updated. Other WRED parameters remain unchanged.
- If a RoCE queue is deleted in the **RoCE Queue Configuration** section, the related WRED configuration entry is automatically removed.
- To delete the WRED settings you configured for a RoCE queue, locate the RoCE queue, and then click **Delete**.

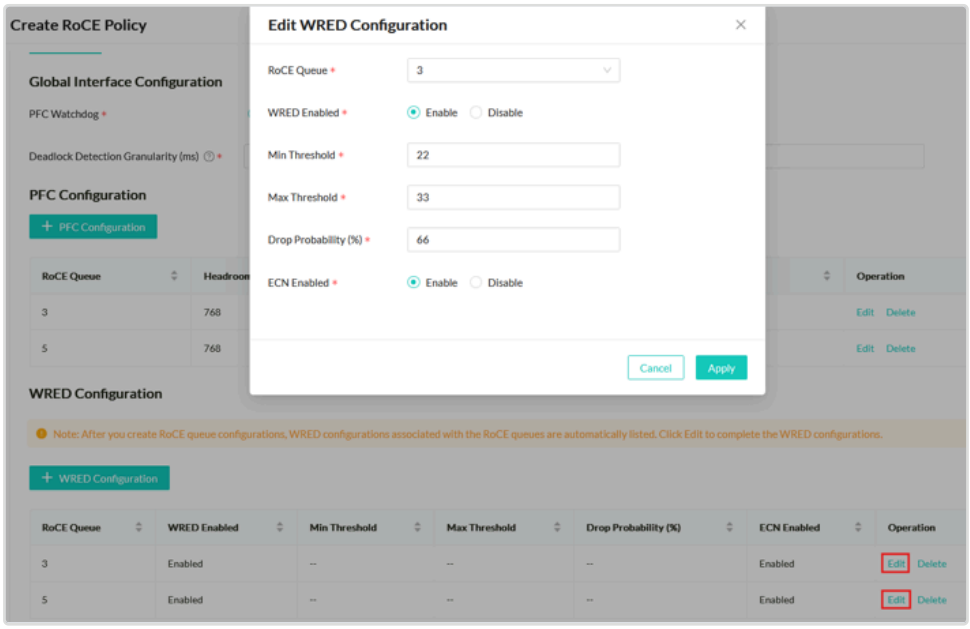


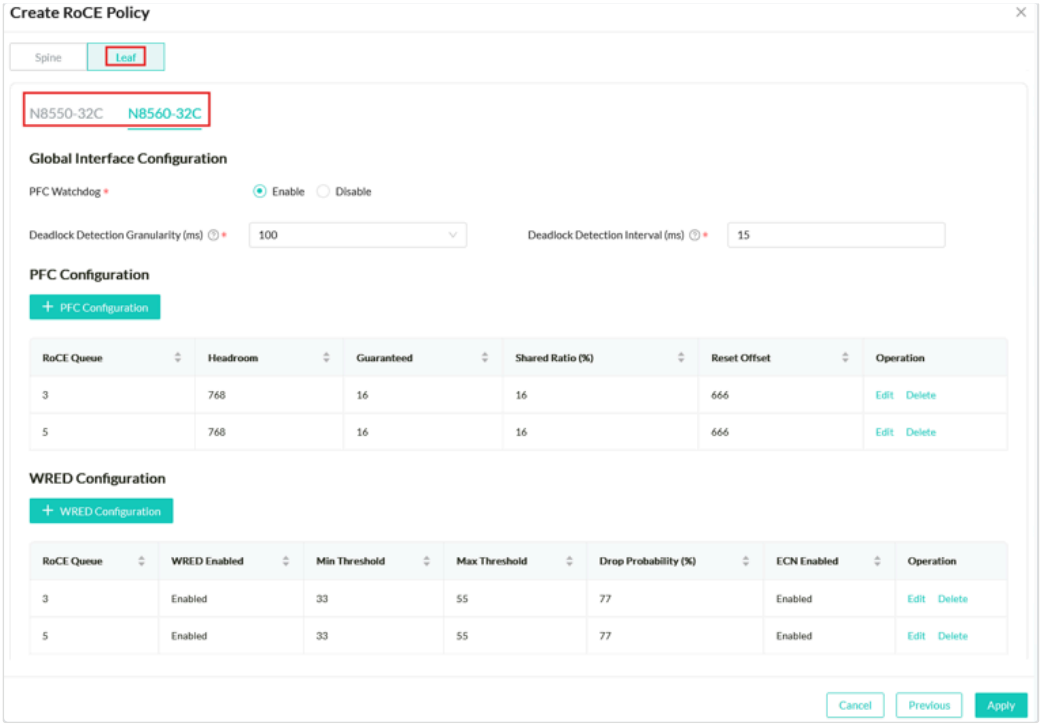
Table 6. WRED Configuration Parameters

Parameter	Description
RoCE Queue	The RoCE queue to be configured. The valid value range is 0 to 7.

WRED Enable	Specify whether to enable WRED for the selected queue.
Min Threshold	The minimum average queue size at which WRED starts to mark or drop packets. The value must be an integer, and the minimum value is 1.
Max Threshold	The maximum average queue size at which WRED starts to drop packets. The value must be an integer greater than the **Min Threshold**.
Drop Probability (%)	The probability (in percentage) that a packet will be dropped or marked with ECN when the average queue size is between the min and max thresholds. The value must be an integer ranging from 0 to 100.
ECN Enabled	Specify whether to enable ECN for the selected queue.

Leaf Tab

In this tab, you can see all leaf switch models you have selected in the **Interface Configuration** section. Locate each switch model, and configure it as described in the Spine Tab.



Click **Apply**. Then, the RoCE policy configurations will be pushed to the selected switches in the fabric.

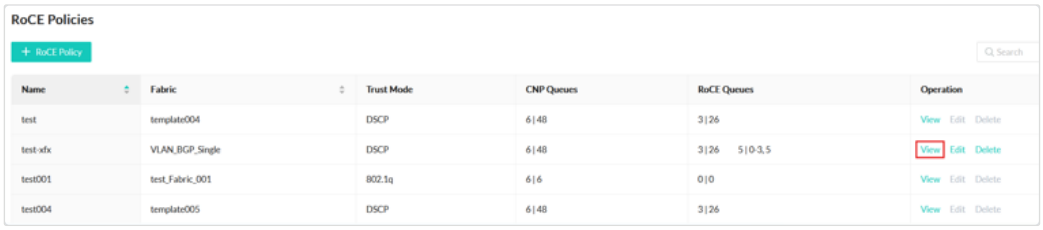
> **NOTEs**
>
> - You can't apply the RoCE policy if any selected switches are offline. To check a switch status, see Viewing the Switch List.
> - If the RoCE policy configurations fail to be pushed to any switch, the configurations will fail to be applied to other switches in the fabric. In this case, you must check the logs to identify the root cause of the failure and then redeploy the RoCE policy configurations to the switches.

Checking the Pushing Results

On the "RoCE Policies" page, check whether the RoCE policy is created.

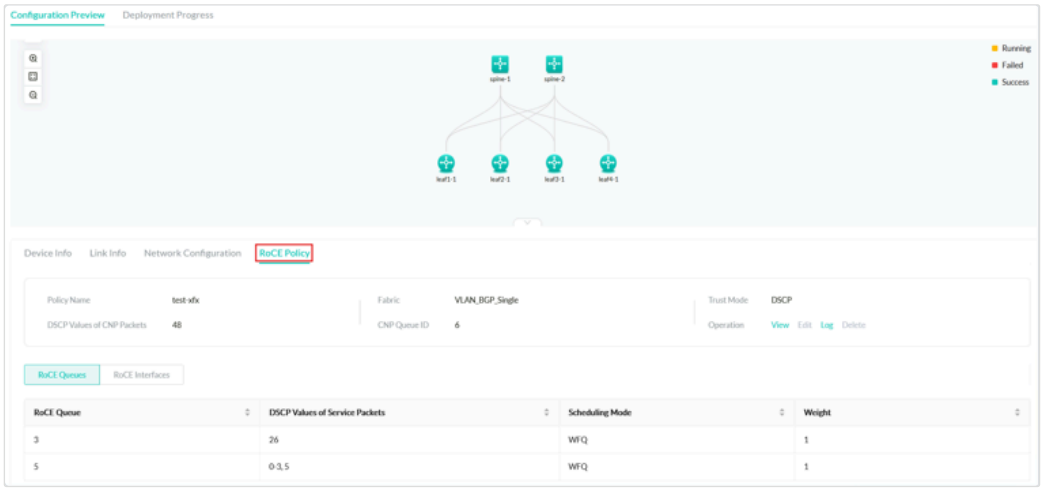
To view the RoCE configurations pushed to switches, click **View**.

> **NOTE**
>
> All created RoCE policies are displayed on the “RoCE Policies” page, including:
>
> - RoCE policies created directly on this page.
> - RoCE policies created during the simplified ZTP process.



If a RoCE policy is associated with fabric in **Simplified ZTP** type, you can also see the RoCE policy configurations in the **RoCE Policy** sub-tab of the fabric page. Follow these steps:

1. Click **Physical Network > Fabrics** from the navigation bar, and click the fabric name to enter the fabric detail page.
2. In the **Configuration Preview** tab, click the **RoCE Policy** sub-tab.
3. To view the detailed configurations, click **View**.
4. To view the operation records of each configuration deployed from the “RoCE Policies” page, click **Log**.



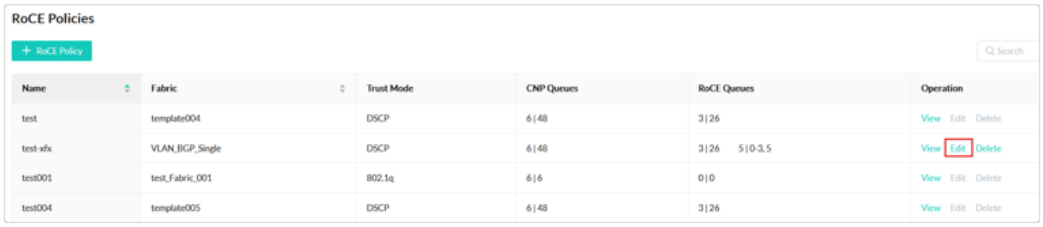
Optional Operations

Editing a RoCE Policy

To edit a RoCE policy, locate the RoCE policy, and then click **Edit**.

> **NOTEs**

- For the RoCE policy associated with a fabric in **Simplified ZTP** type, the **Edit** button is available only if the fabric is in **Deployed** status.
- For the RoCE policy associated with a fabric in **Manual** type, the **Edit** button is always available.
- After a RoCE policy is modified, the configurations in the updated RoCE policy are automatically pushed again to related switches.

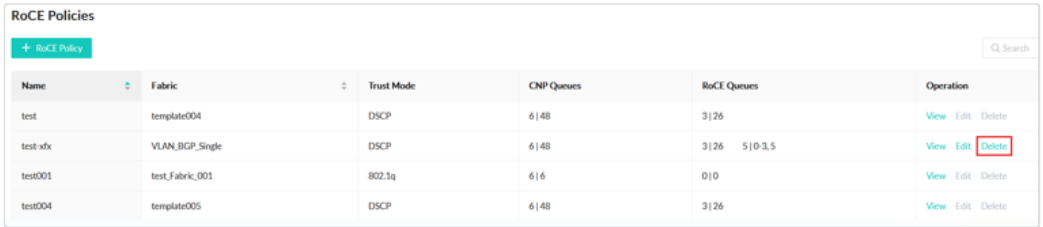


Deleting a RoCE Policy

To delete a RoCE policy, locate the RoCE policy, and then click **Delete**.

NOTEs

- For the RoCE policy associated with a fabric in **Simplified ZTP** type, the **Delete** button is available only if the fabric is in **Deployed** status.
- For the RoCE policy associated with a fabric in **Manual** type, the **Delete** button is always available.
- After the RoCE policy is deleted, the RoCE policy configurations pushed to related switches will be automatically deleted from these switches.



Configuring Dynamic Load Balancing

Traditional static load balancing does not consider the utilization of each member link within the load-balancing group, leading to uneven load distribution among the member links.

AmpCon-DC supports Dynamic Load Balancing (DLB), which distribute the traffic of ECMP routing across different member links, maximizing load balancing among the member links.

By using AmpCon-DC, you can easily enable or disable dynamic load balancing on switches for Equal-Cost Multi-Path (ECMP) and select the dynamic load balancing mode, **Normal**, **Optimal**, or **Assigned** mode as needed.

Guideline
Configuration Procedure
Viewing Pushed Configurations
What to Do Next

Guideline

Ensure that the DLB feature is supported on the PicOS switches to be configured. For more information, see PICOS Supported Features.

Configuration Procedure

To configure DLB, follow these steps:

1. Click **Physical Network > RoCE > Load Balancing** from the navigation bar.
2. In the **Deployment** tab, input the following information:

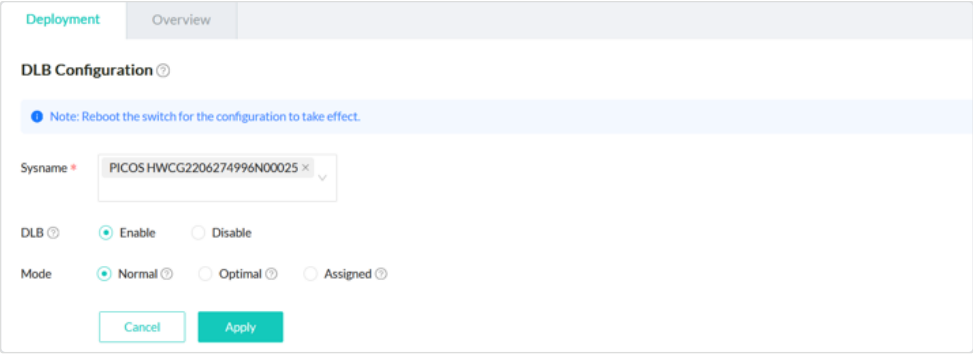


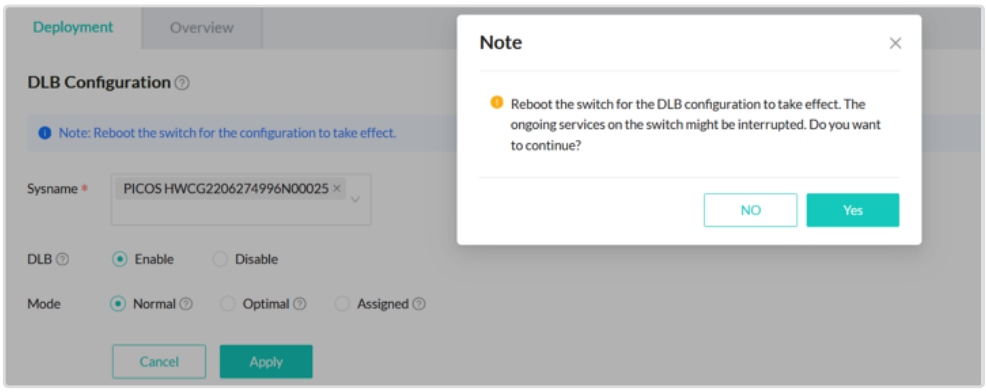
Table 1. DLB Parameters

Parameter	Description
Sysname	Select switches to enable or disable dynamic load balancing.

DLB	Click **Enable** to enable dynamic load balancing or click **Disable** to disable dynamic load balancing.
DLB Mode	Select a dynamic load balancing mode, **Normal**, **Optimal**, or **Assigned** mode. By default, the **Normal** mode is selected.

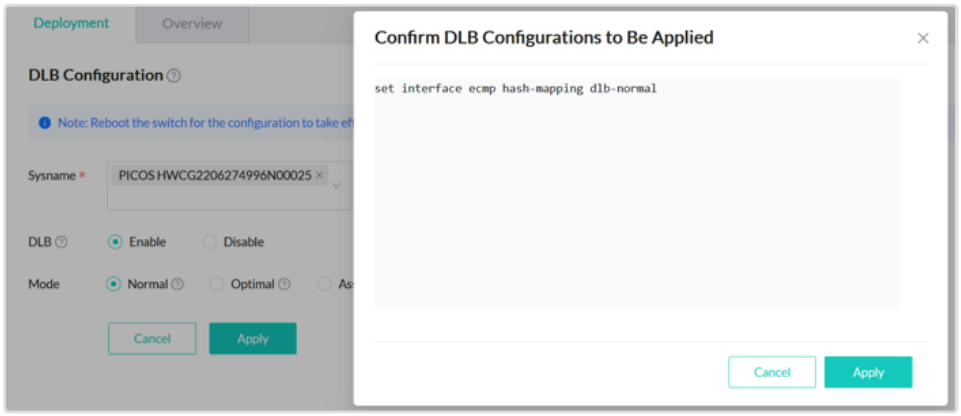
For more information about dynamic load balancing modes, see DLB Implementation Principle.

3. Click **Apply**.
4. In the **Note** pop-up window, click **Yes**.



5. In the **Confirm DLB Configurations to Be Applied** pop-up window, check the dynamic load balancing configurations to be applied, and then click **Apply**.

> **NOTE**
>
> You must reboot the switches for the DLB configurations to take effect.



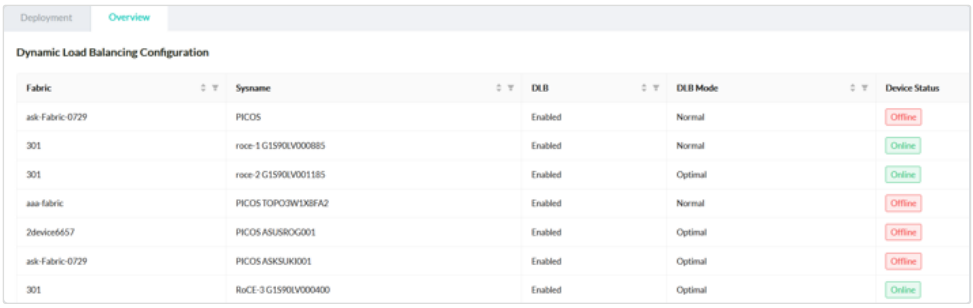
Viewing Pushed Configurations

To check the pushed dynamic load balancing configurations, follow the steps:

1. Click **Physical Network > RoCE > Load Balancing** from the navigation bar.
2. Click the **Overview** tab. Then, you can see the switches with dynamic load balancing enabled or disabled and their dynamic load balancing mode.

   The **Device Status** column contains two status:

- **Online:** The switch is connected with the AmpCon-DC server.
- **Offline:** The switch is not connected with the AmpCon-DC server.



What to Do Next

Continuously monitor DLB metrics, and make dynamic adjustments to DLB modes as needed to respond to changing network conditions.

You can check DLB related telemetry data. For more information, see Dynamic Load Balancing (DLB).

Managing Switches

After onboarding PicOS switches as described in Onboarding Switches, you can manage these switches with AmpCon-DC.

AmpCon-DC streamline lifecycle management of PicOS switches, helping you increase network management efficiency and focus on more strategic tasks.

See the following child topics:

- Viewing Managed Switches
- Uploading and Upgrading PicOS Images
- Managing the Parking Lot
- Returning Merchandise Authorization for Switches
- Decommissioning Switches
- Removing Switches

Viewing Managed Switches

On the “Switches” page, you can view and manage switches as follows:

- Viewing the Switch List
- Viewing Telemetry Data of a Switch
- Viewing the Parking Lot
- Refreshing Switch Hostnames Automatically
- Modifying Switch Hostnames Manually

Viewing the Switch List

In the AmpCon-DC UI, click **Device > Switches** from the navigation bar. On the “Switches” page, you can see the list of all managed switches.



Table 1. Switch Metrics

Metric	Description
Sysname	The hostname of the switch.
SN/Service Tag	The serial number or service tag of the switch.
Model	The model of the switch.
Version	The version of the switch.
Fabric	The fabric to which the switch belongs.
Status	The state of the switch. The following states are supported: • **Imported:** The switch is imported to AmpCon-DC. • **Provisioning Success:** The switch is deployed by using AmpCon-DC. • **Configured:** After you add a switch configuration, the switch is in **Configured** status.

	• **Staged:** After you stage a switch, the switch is in **Staged** status. • **Registered:** The switch has registered with AmpCon-DC but hasn't been deployed completely. • **Provisioning Failed:** The switch fails to be deployed by using AmpCon-DC. • **DECOM:** The deployed switch is decommissioned (DECOM) when it's online. • **DECOM-Manual:** The deployed switch is decommissioned (DECOM) when it's offline. • **RMA:** The switch is replaced with another switch of the same switch model by using Return Merchandise Authorization (RMA).

VPN IP	The IP address of the VPN tunnel established between the switch and AmpCon-DC. The following status icons are supported: • ✓: The VPN tunnel between the switch and AmpCon-DC is available. • x: The VPN tunnel between the switch and AmpCon-DC is unavailable. **NOTE** **Mgmt IP** might be changed. To ensure uninterrupted connection between AmpCon-DC and a switch after **Mgmt IP** is changed, OpenVPN is introduced to AmpCon-DC. OpenVPN is an open-source virtual private network (VPN) solution designed to create secure, encrypted communication tunnels over networks. After a switch is onboarded to AmpCon-DC successfully, a VPN tunnel between AmpCon-DC and the switch is established, and a **VPN IP**, the IP address of the VPN tunnel, is assigned to the switch. Later, AmpCon-DC and the switch will communicate through the VPN tunnel.
Mgmt IP	The management IP address of the switch. **Mgmt IP** is used to connect to AmpCon-DC.

In the **Operation** column, you can manage the switch as follows:

- To connect to the switch from the AmpCon-DC UI through an SSH session, click **SSH** and input the following information:

Table 2. SSH Parameters

Parameters	Description
Username	The username to log in to the switch.

Password	The password of the user.

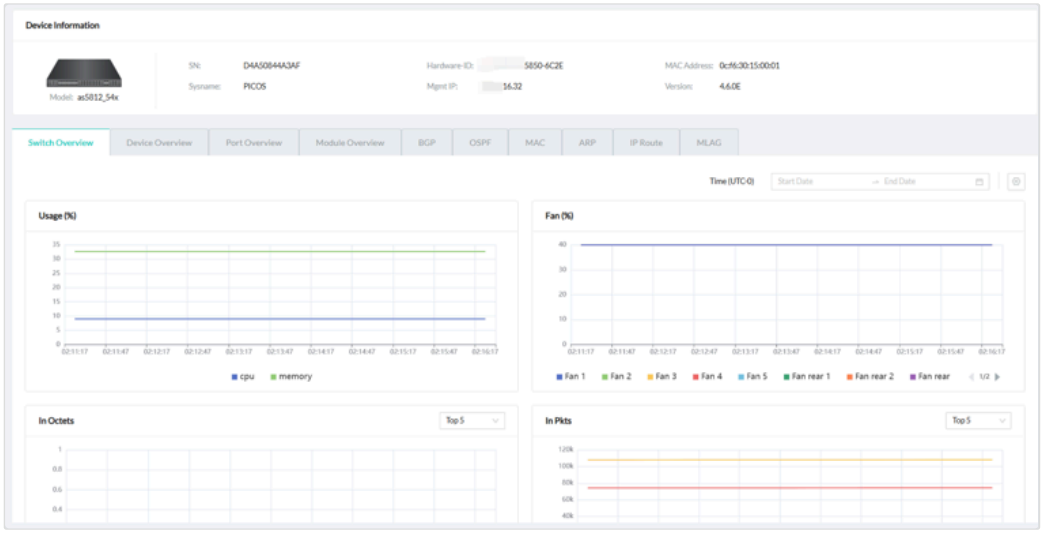
- To check the operation log of the switch, click **Device Log**.
- To change the system configuration of the switch, click **Configuration**.
- In the **Config View** section, you can manage configurations as follows:
  - To check the agent configurations, click **Agent Config**. The agent configurations are automatically uploaded to the switch during the normal ZTP or simplified ZTP process.
  - To check the initial configurations of the switch, click **Init Deploy Config**. Initial configurations mean the configurations that are pushed to a switch by AmpCon-DC during the ZTP process.
  - To check the latest backup configurations, click **Current Config**. For more information, see Viewing Configurations. If the switch doesn't have backup configurations, the configurations generated when you add a switch configuration for the switch are displayed.
  - To back up configurations for the switch, click **Backup Config**. For more information, see Backing Up and Restoring Configurations.
  - To upload a local switch configuration file to AmpCon-DC, click **Upload Config**. For more information, see Uploading Configurations.

> **NOTEs**
>
> - For switches deployed through normal ZTP or simplified ZTP, when you hover your mouse over **Config View**, the **Agent Config**, **Init Deploy Config**, **Current Config**, **Backup Config**, and **Upload Config** are displayed.
> - For switches imported to AmpCon-DC (instead of provisioned with ZTP), when you hover your mouse over **Config View**, the **Backup Config** and **Upload Config** are displayed.

- To replace the switch with another switch of the same switch model, hover your mouse over **Lifecycle Actions**, and then click **RMA**. For more information, see Returning Merchandise Authorization for Switches.
- To remove the switch from AmpCon-DC, hover your mouse over **Lifecycle Actions**, and then click **Remove**. For more information, see Removing Switches.
- To decommission the switch from AmpCon-DC, hover your mouse over **Lifecycle Actions**, and then click **DECOM**. For more information, see Decommissioning Switches.

Viewing Telemetry Data of a Switch

Click a specific switch SN or service tag in the switch list. You can see detailed telemetry data related to the switch. For more information, see Telemetry Data of a Switch.



Viewing the Parking Lot

During the simplified ZTP or RMA process, after you configure the DHCP server and reboot the switches to be deployed, these switches will go to the AmpCon-DC parking lot.

During the normal ZTP process, if you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-DC parking lot. If you add a switch configuration before configuring the DHCP server, the switch will go to the “Switches” page.

In the AmpCon-DC UI, click **Device > Switches** from the navigation bar. On the “Switches” page, click **Parking Lot**, and then you can see all switches in **Parking** status.

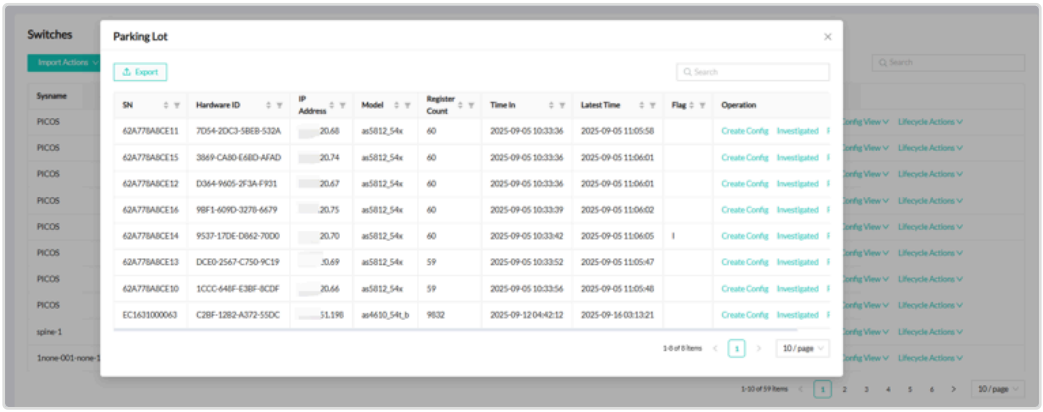


Table 3. Switch Metrics

Metric	Description

SN	The serial number of the switch
Hardware ID	The Hardware ID of the switch
IP Address	The switch IP address used to connect to AmpCon-DC
Model	The model of the switch
Register Count	The number of times the switch initiates ZTP authentication with the AmpCon-DC server
Time In	The time when the switch initiates the first ZTP authentication with the AmpCon-DC server
Latest Time	The time when the switch initiates the last ZTP authentication with the AmpCon-DC server
Flag	Indicates whether the switch has been investigated

In the **Operation** column, you can manage the switch as follows:

- To add a switch configuration, click **Create Config**. Then, the switch will be listed on the "Switches" page and can be staged.
- To confirm whether you have viewed the switch, click **Investigated**. After you click the button, the value of the **Flag** field will be "I".
- To remove the switch from the parking lot list, click **Remove**.

To save all the switch information from the parking lot list to a local file, click **Export** in the top-left corner.

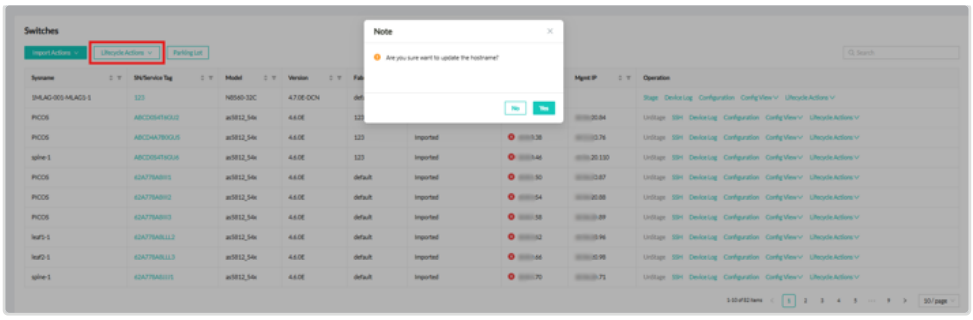
Refreshing Switch Hostnames Automatically

During the switch lifecycle, switch hostnames might be changed on the switch side.

AmpCon-DC can retrieve the latest hostnames from managed switches and then refresh the displayed hostnames in the AmpCon-DC UI.

To refresh switch hostnames, follow these steps:

1. Log in to the AmpCon-DC UI, and then click **Device > Switches** from the navigation bar.
2. Click **Lifecycle Actions**, and then select **Sync Sysname**.



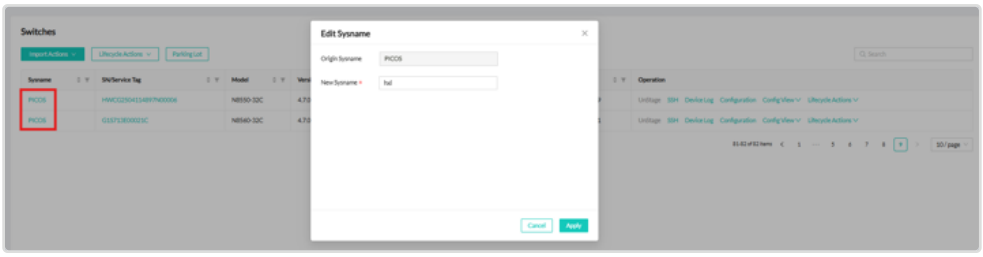
3. Click **Yes**.

Modifying Switch Hostnames Manually

In addition to automatically retrieving and displaying the latest hostnames, you can modify switch hostnames manually. Follow the steps:

> **NOTEs**
>
> - If you refresh switch hostnames by clicking **Sync Hostname** and then modify the switch hostname manually, the manually entered switch hostname will be displayed in the AmpCon-DC as the switch hostname.
> - If you modify the switch hostname manually and then refresh switch hostnames by clicking **Sync Hostname**, the manually entered switch hostname will be overwritten by the real hostname that AmpCon-DC retrieves from the switch.

1. Log in to the AmpCon-DC UI, and then click **Device > Switches** from the navigation bar.
2. Locate the switch in the switch list, and then click the hostname of the switch.
3. In the **Edit Sysname** pop-up window, input a new hostname as needed.



4. Click **Apply**.

Uploading and Upgrading PicOS Images

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

You no longer need to visit the FS website to download images or view release notes. Both upgrades and release notes are available directly within the AmpCon-DC UI, saving your time and effort.

You can schedule automatic upgrades during off-peak hours(such as at night or on holidays), so that your operations will face minimal disruption.

See the following child topics:

- Uploading and Pushing Images
- Upgrading PicOS on Switches

Uploading and Pushing Images

AmpCon-DC provides multiple built-in PicOS images, which you can use to deploy switches.

To deploy a switch with a PicOS image that is not built in AmpCon-DC, upload the image and its MD5 file first before you deploy the switch.

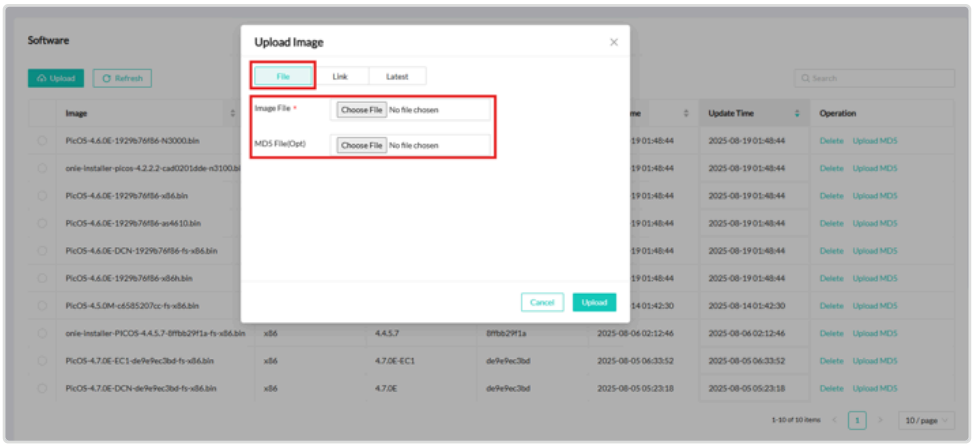
Uploading Images
Optional: Uploading MD5 Files
Optional: Removing Images
Optional: Pushing Images

Uploading Images

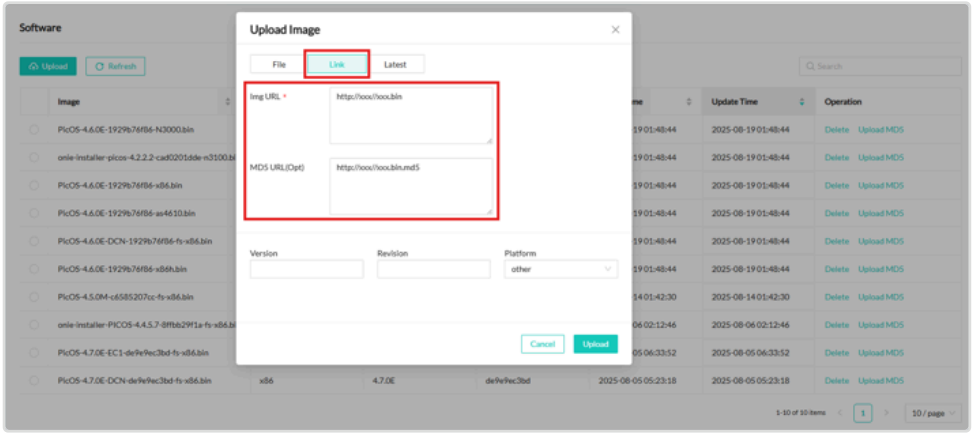
To upload a PicOS image, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images** from the navigation bar.
2. Click **Upload**.
3. In the pop-up window, upload an image by using one of the following ways:

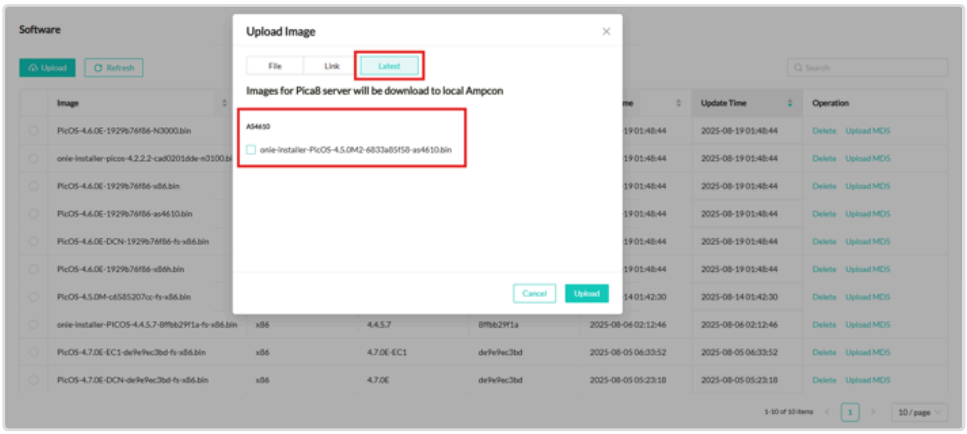
- Click **File**, and select a local image file (required) and its MD5 file (optional).



- Click **Link**, and enter the image URL (required) and the MD5 file URL (optional).



- Click **Latest**, and check the image files that you want to upload.



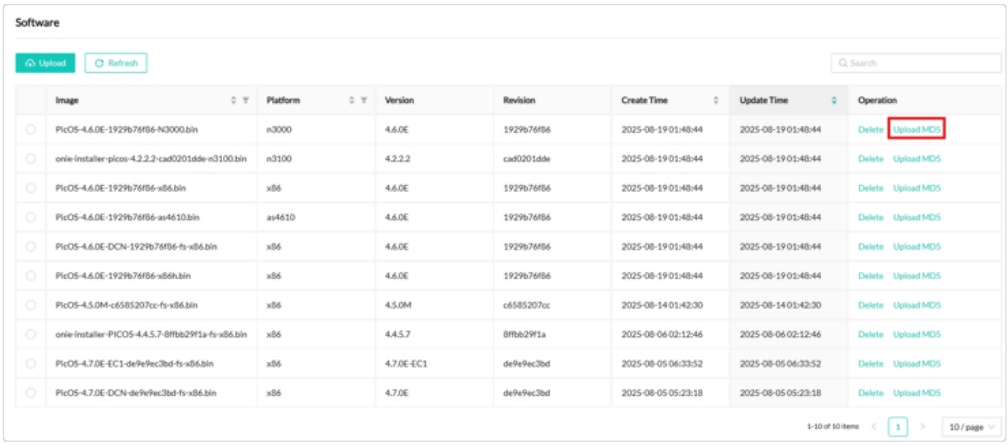
4. Click **Upload**.

Optional: Uploading MD5 Files

An MD5 file is used to verify the completeness of the corresponding PicOS image. If the MD5 file is not uploaded when you upload the PicOS image, AmpCon-DC will not verify the completeness of the PicOS image when it installs the PicOS image.

To upload an MD5 file for a PicOS image, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images**.
2. In the **Software** section, locate the PicOS image, and then click **Upload MD5**.



3. Upload the MD5 file by using either of the following ways:

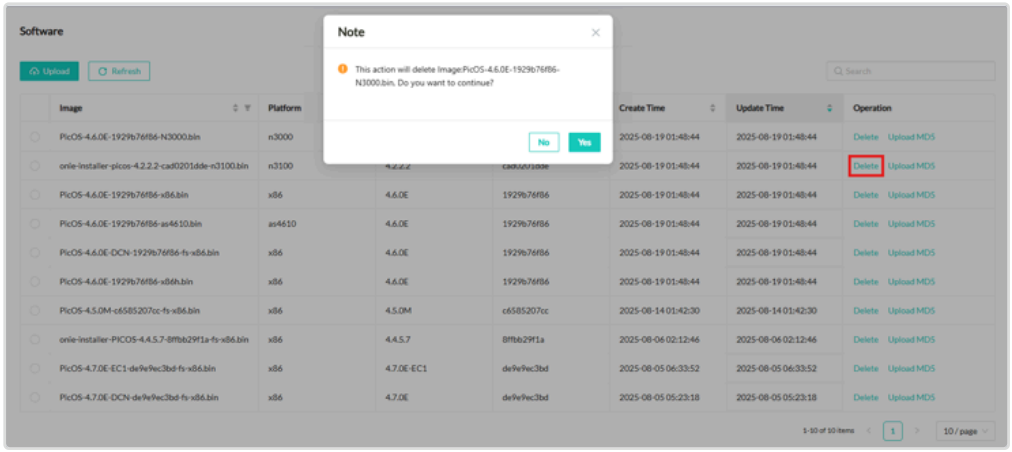
- Click **File**, and select the MD5 file.
- Click **Link**, and enter the URL of the MD5 file.

4. Click **Upload**.

Optional: Removing Images

1. In the AmpCon-DC UI, click **Resource > OS Images**.

2. In the **Software** section, locate an image, and then click **Delete**.



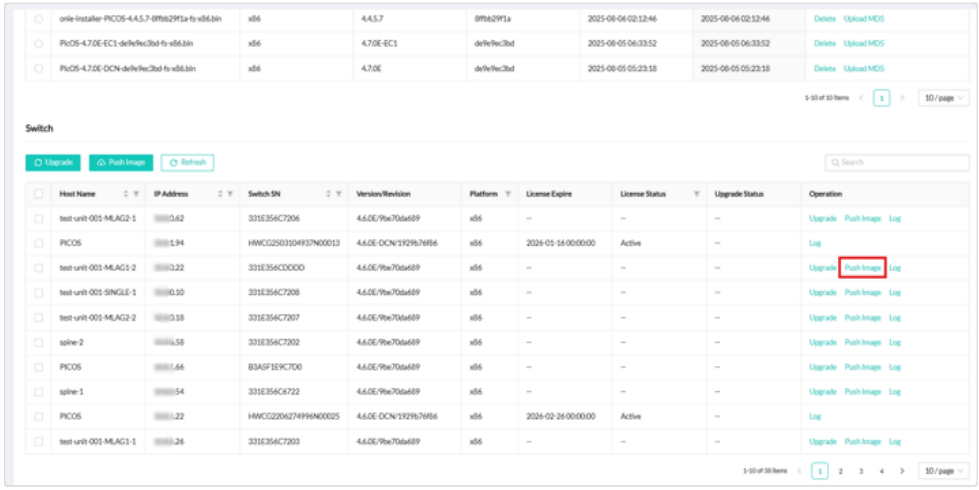
3. Click **Yes** to confirm the deletion.

Optional: Pushing Images

You can push PicOS images to one or multiple switches. The pushed images are located in the /home/automation directory.

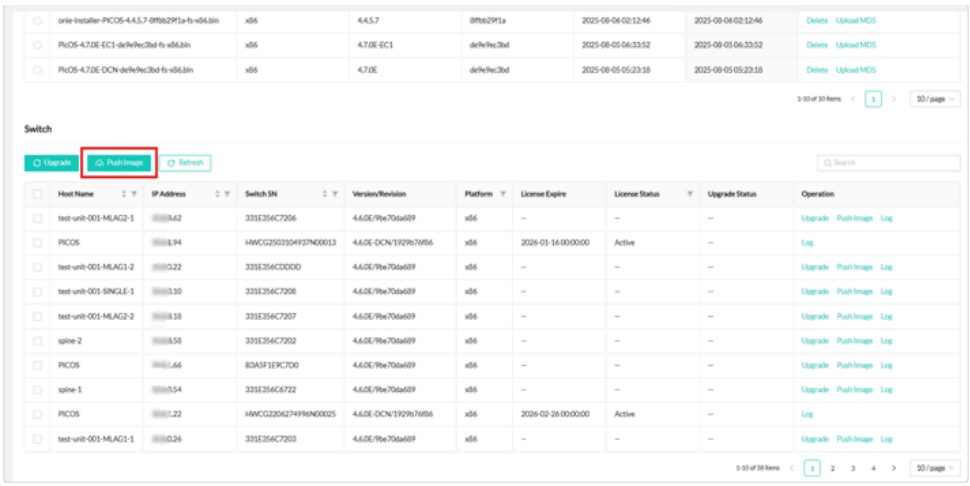
To push a PicOS image to a single switch, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images**.
2. In the **Software** section, select the PicOS image that you want to push.
3. In the **Switch** section, locate the switch, and then click **Push Image**.



To push a PicOS image to multiple switches, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images**.
2. In the **Software** section, select the PicOS image that you want to push.
3. In the **Switch** section, select the corresponding switches, and then click **Push Image**.


onie-installer-PICOS-4.4.5.7-8ffbb29f1a-fs-x86.bin
x86
4.4.5.7
8ffbb29f1a
2025-08-06 02:12:46
2025-08-06 02:12:46
Delete
Upload MD5
PicOS-4.7.0E-EC1-de9e9ec3bd-fs-x86.bin
x86
4.7.0E-EC1
de9e9ec3bd
2025-08-05 06:33:52
2025-08-05 06:33:52
Delete
Upload MD5
PicOS-4.7.0E-OCN-de9e9ec3bd-fs-x86.bin
x86
4.7.0E
de9e9ec3bd
2025-08-05 05:23:18
2025-08-05 05:23:18
Delete
Upload MD5
1-10 of 10 items
1
10 / page
Switch
Upgrade
Push Image
Refresh
Search
Host Name
IP Address
Switch SN
Version/Revision
Platform
License Expire
License Status
Upgrade Status
Operation
test-unit-001-MLAG2-1
.62
331E356C7206
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
PICOS
.94
HWCG2503104927N00013
4.6.0E-OCN-1929b76ff6
x86
2026-01-16 00:00:00
Active
--
Log
test-unit-001-MLAG1-2
.22
331E356CDDDD
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
test-unit-001-SINGLE-1
.10
331E356C7208
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
test-unit-001-MLAG2-2
.18
331E356C7207
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
spine-2
.58
331E356C7202
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
PICOS
.66
83A5F1E9C7D0
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
spine-1
.54
331E356C6722
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
PICOS
.22
HWCG2206274996N00025
4.6.0E-OCN-1929b76ff6
x86
2026-02-26 00:00:00
Active
--
Log
test-unit-001-MLAG1-1
.26
331E356C7203
4.6.0E-9be70da689
x86
--
--
--
Upgrade Push Image Log
1-10 of 38 items
1
2
3
4
10 / page

Upgrading PicOS on Switches

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

- Before You Upgrade
- Upgrading PicOS on a Single Switch
- Upgrading PicOS on Multiple Switches
- Verifying the Upgrade

Before You Upgrade

Before upgrading a switch to PicOS 4.6.0E or later, if both EVPN VXLAN and static VXLAN have been configured on the switch, you must manually delete the static VXLAN configuration.

Otherwise, the upgrade will fail and terminate with the following error message:

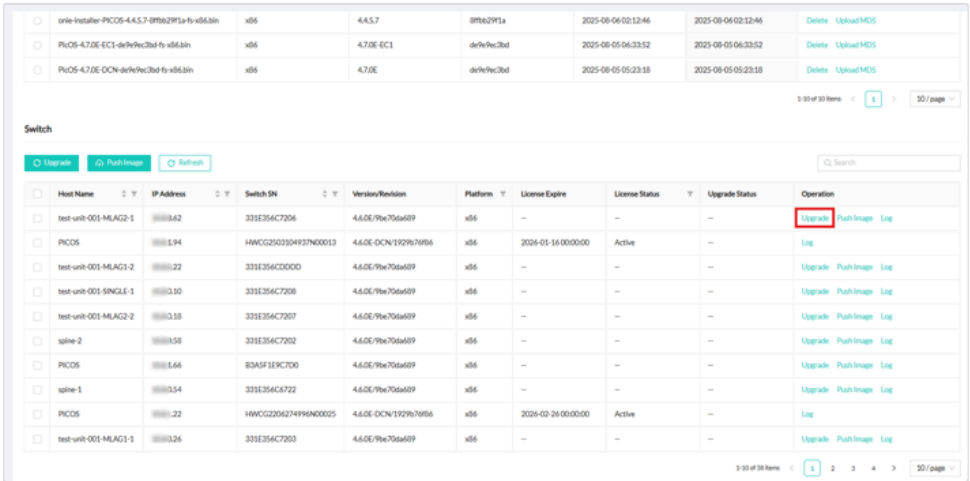
> Error: The current version only supports EVPN VXLAN. Please delete the static VXLAN configuration before upgrading. Upgrade aborts.

For more information, see Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command and Upgrading PICOS from Version 3.0 or Later Using Upgrade2.

Upgrading PicOS on a Single Switch

To upgrade PicOS on a single switch, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images** from the navigation bar.
2. In the **Software** section, select the PicOS image to which you want to upgrade.
3. Locate the switch in the **Switch** section, and then click **Upgrade**.

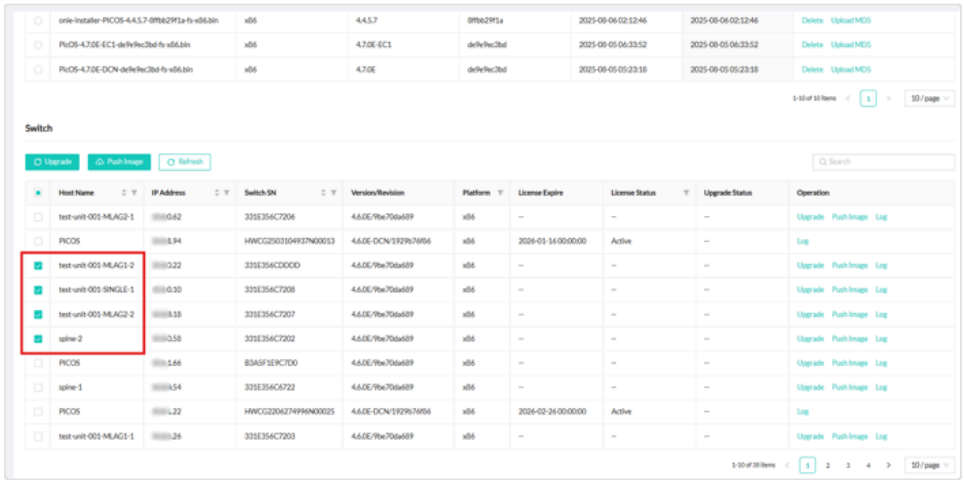


4. Click **Yes** to confirm the upgrade operation.

Upgrading PicOS on Multiple Switches

To upgrade PicOS on multiple switches, follow these steps:

1. In the AmpCon-DC UI, click **Resource > OS Images** from the navigation bar.
2. In the **Software** section, select the PicOS image to which you want to upgrade.
3. In the **Switch** section, select the corresponding switches, and then click **Upgrade**.

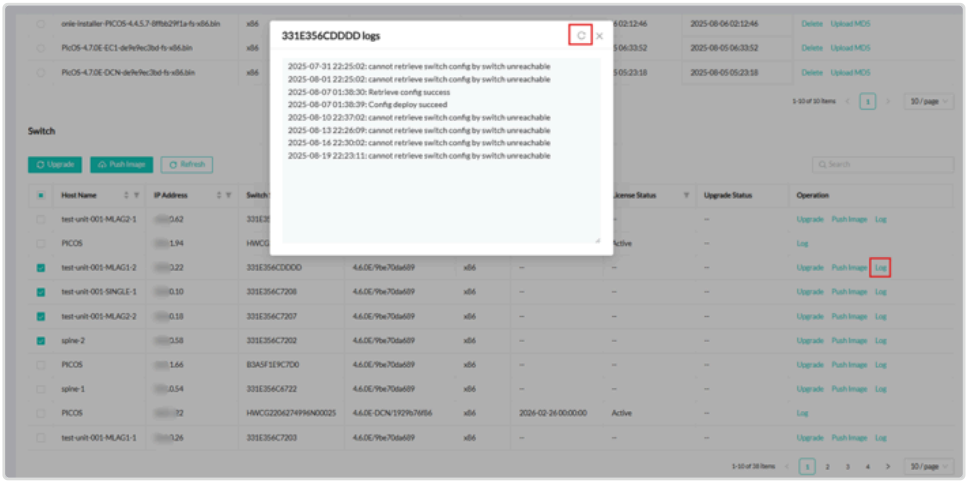


4. Click **Upgrade** to confirm the upgrade operation.

Verifying the Upgrade

To verify the upgrade, follow these steps:

1. In the **Switch** section, locate the switch, and then check the **Upgrade Status** column to see whether the status is **Upgraded**.
2. If the status is **Upgrade Failed**, click **Log** to see more details for troubleshooting. You can click the refresh icon to update the logs.



Managing the Parking Lot

During the simplified ZTP or RMA process, after you configure the DHCP server and reboot the switches to be deployed, these switches will go to the AmpCon-DC parking lot.

During the normal ZTP process, if you configure the DHCP server before adding a switch configuration, the switch will go to the AmpCon-DC parking lot. If you add a switch configuration before configuring the DHCP server, the switch will go to the “Switches” page.

The DHCP configuration steps for normal ZTP, simplified ZTP, and RMA are the same. For more information, see Configuring a DHCP Server.

Procedure
What to Do Next

Procedure

1. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar.
2. On the “Switches” page, click **Parking Lot**. In the pop-up window, you can see all the switches in the parking lot:

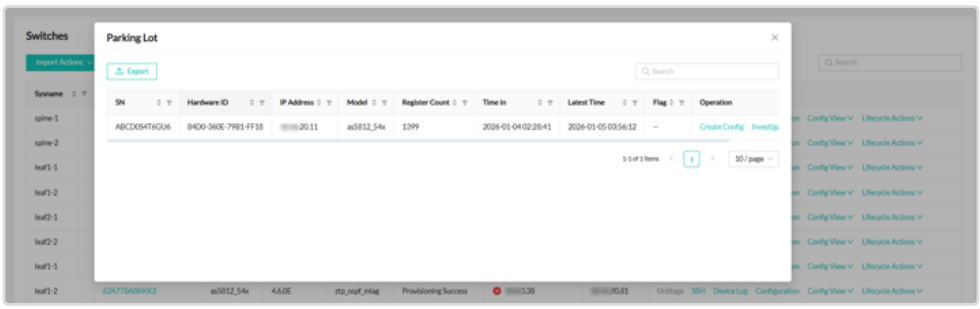


Table 1. Switch Metrics

Metric	Description
SN	The serial number of the switch.
Hardware ID	The Hardware ID of the switch.
IP Address	The switch IP address used to connect to the AmpCon-DC server.
Model	The model of the switch.

Register Count	The number of times the switch initiates ZTP authentication with the AmpCon-DC server.
Time In	The time when the switch initiates the first ZTP authentication with the AmpCon-DC server.
Latest Time	The time when the switch initiates the last ZTP authentication with the AmpCon-DC server.
Flag	Whether the switch has been investigated.

3. In the **Operation** column, do the following operations as needed:

- To deploy a switch through normal ZTP, locate the switch, and then click **Create Config** to add a switch configuration.
- To confirm whether you have viewed a switch, locate the switch, and then click **Investigated**. After you click the button, the value of the **Flag** column will be "I".
- To remove a switch from the parking lot, locate the switch, and then click **Remove**.

4. To save all the switch information in the parking lot to a local file, click **Export** in the top-left corner.

What to Do Next

After a switch go to the parking lot, you can deploy the switch through normal ZTP or simplified ZTP. Or you can replace a failed switch with the switch through Returning Merchandise Authorization (RMA).

For more information, see the following documents:

- Deploying Switches through Normal ZTP
- Simplified ZTP Deployment
- Returning Merchandise Authorization for Switches

Returning Merchandise Authorization for Switches

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

When the hardware of a switch fails and is replaced with a new switch, you can RMA to install or upgrade PicOS on the new switch and push configurations to the new switch through AmpCon-DC. In this way, you can seamlessly manage the new switch with AmpCon-DC.

RMA Workflow
Configuration Rules
Before You Begin
RMA Procedure
What to Do Next

RMA Workflow

- **For white-box switches**

  During the RMA process, AmpCon-DC deploys PicOS on the new switch based on the **Deployed ONIE Image** setting in the switch model configuration. For more information, see Configuring Switch Models.

  Then, AmpCon-DC configures the new switch based on the backup configuration file or uploaded configurations of the old switch (the switch to be replaced). For more information about backup and uploaded configuration files, see Backing Up and Restoring Configurations.

  > **NOTEs**
  >
  > To ensure that the PicOS versions on the new switch and the old switch are the same, use one of the following ways:
  >
  > - Before the RMA process, ensure that the **Deployed ONIE Image** of the related switch model is the same as the PicOS version on the old switch.
  > - After the RMA process, if the PicOS version on the old switch is higher than the PicOS version on the new switch, upgrade the new switch. For more information, see Uploading and Upgrading PicOS Images.

- **For integrated hardware and software PicOS switches**

During the RMA process, AmpCon-DC configures the new switch based on the backup configuration file or uploaded configurations of the switch to be replaced.

Configuration Rules

During the RMA process, AmpCon-DC configures a new switch based on the following configuration rules:

1. If the switch to be replaced has backup configuration files marked with the **AMPCON_BACKUP** tag, the latest backup configuration file marked with the **AMPCON_BACKUP** tag is used to configure the new switch.
2. If the switch to be replaced doesn't have backup configuration files marked with the **AMPCON_BACKUP** tag but has a backup configuration file marked with the **GOLDEN_CONFIG** tag, the backup configuration file marked with the **GOLDEN_CONFIG** tag is used to configure the new switch.
3. If the switch to be replaced doesn't have backup configuration files marked with the **AMPCON_BACKUP** or **GOLDEN_CONFIG** tag but has other backup configuration files, the latest backup configuration file is used to configure the new switch.
4. If the switch to be replaced doesn't have backup configuration files but has uploaded configurations, the uploaded configurations are used to configure the new switch.
5. If the switch to be replaced doesn't have backup configuration files and uploaded configurations, the RMA process will fail. In this case, back up or upload configurations first, and then start the RMA process again.

Before You Begin

Before you start the RMA process, ensure that the following prerequisites are met. Or else, the RMA process will fail.

1. In the DHCP configuration file (/etc/dhcp/dhcpd.conf) of the DHCP server, add the configurations for the new switch. Then, reboot the new switch. For more information, see **Step 2** and **Step 3** of Configuring the DHCP Server.

   The new switch will go to the AmpCon-DC parking lot after the DHCP server is configured and the new switch is rebooted.

2. Check whether the hardware ID of the new switch is included in any imported AmpCon-DC licenses. For more information, see Viewing AmpCon-DC Licenses.

   If the hardware ID of the new switch is not included in any imported AmpCon-DC licenses, you must import an AmpCon-DC license to AmpCon-DC. For more information, see

Importing Licenses for Deployed Switches.

3. Ensure that the switch to be replaced is in **Provisioning Success** or **Imported** status and has backup configuration files or uploaded configurations. For more information about switch status, see Viewing the Switch List.
4. Ensure that the new switch is up and has the same switch model as the switch to be replaced.

RMA Procedure

1. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar. On the "Switches" page, you can see a list of managed switches.
2. Locate the switch to be replaced, and then click **Lifecycle Actions > RMA**.
3. In the **Switch RMA** pop-up window, input the following information:



Table 1. RMA Parameters

Parameter	Description
Staged	Toggle it on to stage the new switch. **NOTE** The new switch can be deployed successfully only when you stage it.
SN	The serial number (SN) of the new switch.
System Configuration	The system configuration applicable to the new switch. **NOTE** Pay attention to the following points. Or else, the RMA process will fail. • Ensure that the **Device Default Login User** and **Device Default Password** on the

	"System Configuration" page are correct and can be used to log in to the new switch. • Ensure to check whether AmpCon-DC can connect with the License Portal through the entered **License Portal URL**, **License Portal User**, and **License Portal Password**. For more information, see Checking License Portal Connectivity. • Ensure that the uploaded **Security Config File** and **Parking Security Config File** don't contain wrong configurations.

4. Click **Apply**.

After the RMA process is completed successfully, the new switch will replace the old switch on related AmpCon-DC pages.

What to Do Next

After the RMA process, do the following operations:

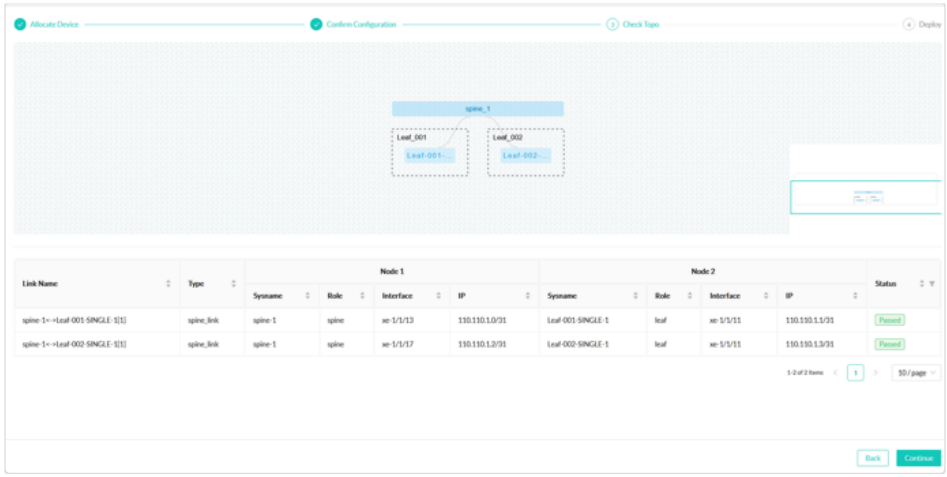
- **Complete physical connections for the new switch**

  If the old switch was used for physical network deployment, the new switch will replace the old switch in the physical network. The underlay configurations will be automatically pushed to the new switch after RMA, and thus you don't need to re-deploy the physical network in the AmpCon-DC UI.

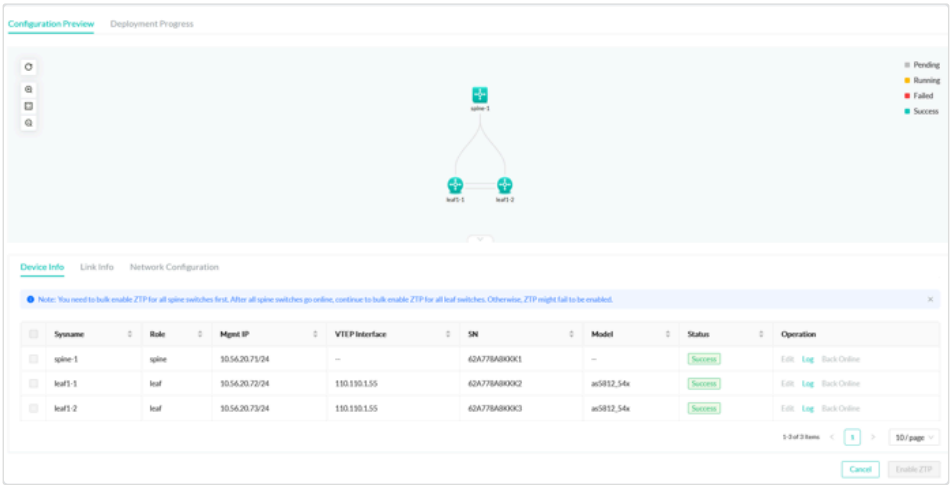
  However, you must complete physical connections for the new switch based on the topology and link information on the fabric page. For more information, see Deploying Physical Networks.

  > **NOTE**
  >
  > If you don't complete physical connections for the new switch based on the topology and link information on the fabric page, the physical network and related logical networks will not work.

  For physical networks deployed through physical network design, the topology and link information is as follows:



For physical networks deployed through simplified ZTP, the topology and link information is as follows:



- **Check RMA results**

  Click **Device > Switches** from the navigation bar. On the “Switches” page, check whether the old switch is in **RMA** status and whether the new switch is in **Provisioning Success** status.

  NOTEs

  - If the new switch fails to be deployed, the status will be displayed as **Provisioning Failed**. In this case, check the Before You Begin section to ensure that you have completed all the prerequisites. In addition, check the selected system configuration to ensure that the system configuration is correct. AmpCon-DC will retry deploying the new switch automatically.
  - If the new switch is not staged and the switch is in **Configured** status on the “Fabrics” page, click **Stage** on the “Switches” page to stage the new switch. Then, the new switch will be deployed.

Decommissioning Switches

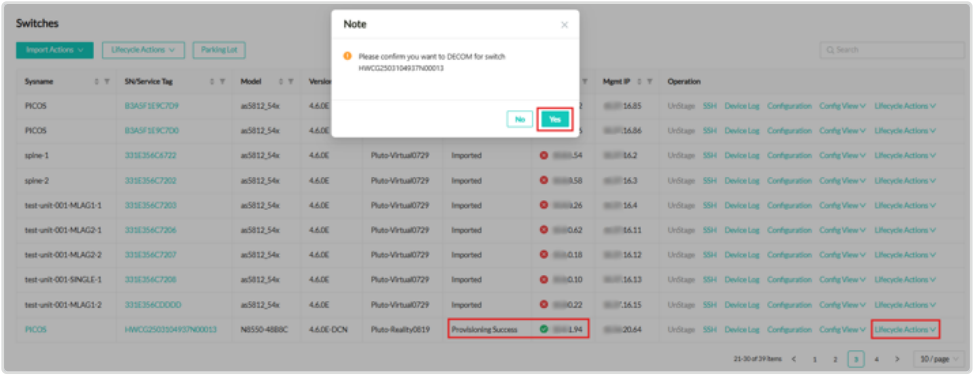
You can decommission (DECOM) a deployed switch to clear the configurations pushed by AmpCon-DC from the switch. The decommissioned switch will not be managed by AmpCon-DC.

> **NOTEs**
>
> - The imported switches can't be decommissioned. But after an imported switch is upgraded, the switch can be decommissioned.
> - The switches in RMA status can't be decommissioned.
> - The decommissioned switches are still displayed in the switch list. To remove the switches from the list, see Removing Switches.
> - After a switch is decommissioned, if you need to onboard this switch to AmpCon-DC again, you must reboot the switch first before onboarding the switch.

Procedure

To DECOM a switch, follow these steps:

1. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar.
2. Locate the switch, click **Lifecycle Actions**, and select **DECOM**.
3. Click **Yes** to confirm the deletion.



4. On the "Switches" page, check whether the decommissioned switch is in **DECOM** or **DECOM-Manual** status.

- **DECOM:** The deployed switch is decommissioned (DECOM) when it's online.
- **DECOM-Manual:** The deployed switch is decommissioned (DECOM) when it's offline. In this case, the configurations pushed by AmpCon-DC are not cleared successfully.

Removing Switches

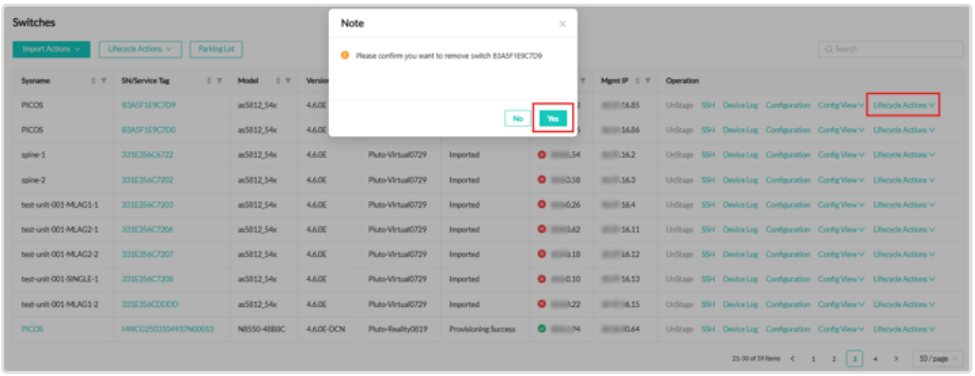
You can remove a switch from AmpCon-DC. Then, the switch will be removed from the AmpCon-DC database and thus not be displayed in the AmpCon-DC UI.

> **NOTEs**
>
> - Removing a switch doesn't revoke the PicOS license and configurations from the switch.
> - The switches in **Provisioning Success** status can't be removed. To remove a switch in **Provisioning Success** status, RMA or decommission (DECOM) the switch first to change the switch status, and then remove the switch.

Procedure

To remove a switch, follow these steps:

1. In the AmpCon-DC UI, click **Device > Switches** from the navigation bar.
2. Locate the switch, click **Lifecycle Actions**, and select **Remove**.
3. Click **Yes** to confirm the deletion.



4. On the "Switches" page, check whether the switch is removed from the switch list.

Configuring Switches

After onboarding PicOS switches, you can use configuration templates to push specific configurations to these switches, minimizing errors and simplifying configuration processes.

AmpCon-DC provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands. When pushing configurations to PicOS switches, select the configuration templates containing the required CLI commands, and select the switches to be configured. Then, these CLI commands will be run on the selected PicOS switches automatically.

You can also back up and restore configurations for disaster recovery, or compare configurations for troubleshooting or auditing, decreasing the downtime and ensure network reliability.

See the following child topics:

- Adding Configuration Templates
- Pushing Configurations to Switches
- Managing Configuration Templates
- Managing Configuration Nodes
- Comparing Running Configurations with Initial Configurations
- Comparing Running or Backup Configurations
- Backing Up and Restoring Configurations

Adding Configuration Templates

AmpCon-DC provides pre-built CLI commands in a hierarchical way in the user interface. You can create configuration templates with different CLI commands.

When deploying a PicOS switch through normal ZTP to onboard it for AmpCon-DC management, you must add a switch configuration with a configuration template.

After onboarding PicOS switches, when you push configurations to these PicOS switches, you can select one or multiple configuration templates to increase switch configuration pushing efficiency and reliability.

Procedure

To add a configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. In the **New Template** tab, input the following information:

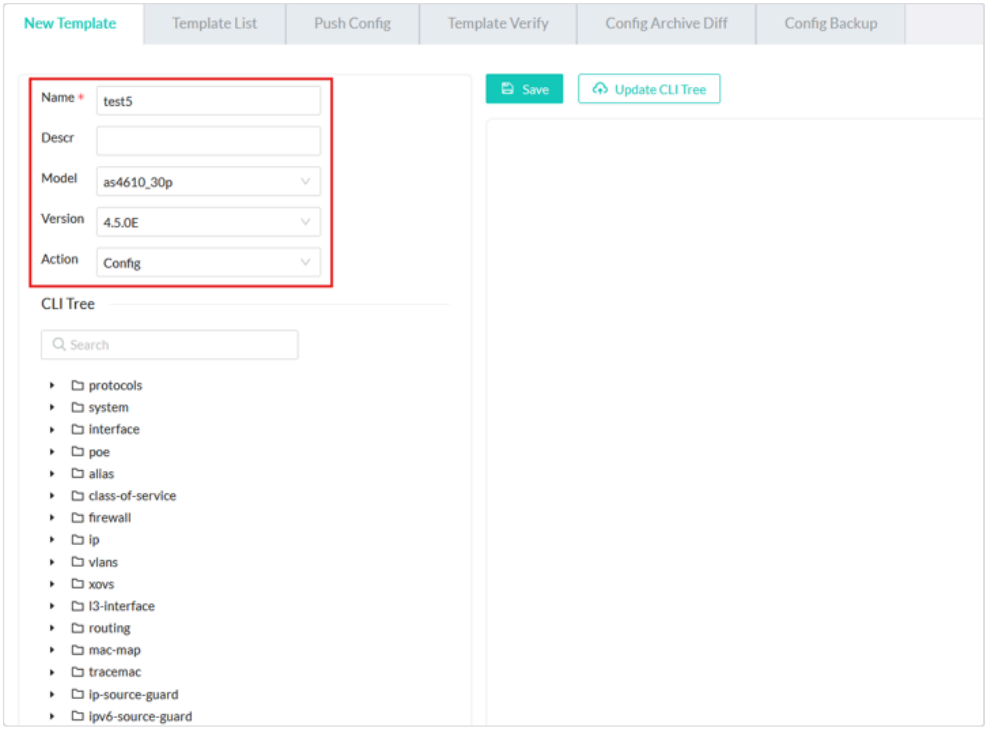


Table 1. Template Fields

Parameter	Description
Name	The name of the configuration template.

Descr	Optional. The description of the configuration template.
Model	The switch model that is applicable to the configuration template. **NOTE** The CLI commands displayed in the **CLI Tree** section are different for different switch models.
Version	The PicOS version that is applicable to the configuration template. **NOTE** The CLI commands in the **CLI Tree** section are different for different PicOS versions.
Action	Select **Config** or **Delete**. **NOTE** If **Config** is selected, the commands in the **CLI Tree** section are in **set** type. If **Delete** is selected, the commands in the **CLI Tree** section are in **delete** type.

3. Optional: Click **Update CLI Tree** to refresh the CLI tree. The CLI commands in the **CLI Tree** section will be refreshed automatically.
4. In the **CLI Tree** section, add one or multiple CLI commands to the configuration template by clicking the plus icon. The selected CLI commands will appear on the right.

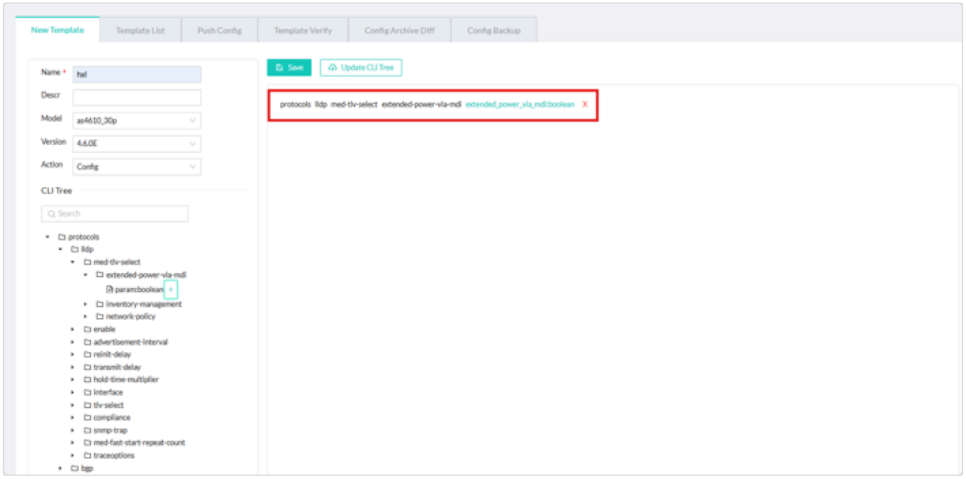
   To remove a CLI command from the configuration template, click the icon x.

NOTE

Ensure that a configuration template contains at least a command with variables. Or else, you will fail to push configurations to switches with this configuration template and fail to add a switch configuration with this configuration template.

In the following screenshot, because you select **Config** in the **Action** drop-down list, the complete command is **set protocols lldp med-tlv-select extended-power-via-mdi *<extended_power_via_mdi>***.

<extended_power_via_mdi> is the variable that requires you to input when you push configurations to switches or add a switch configuration.



5. Click **Save**.

What to Do Next

- Adding Switch Configurations
- Pushing Configurations to Switches
- Managing Configuration Templates

Pushing Configurations to Switches

After onboarding PicOS switches, you can use configuration templates to push specific configurations to these switches.

- Prerequisite
- Procedure
- Verifying the Pushing Status and Log
- Optional Operations
  - Viewing or Editing a Configuration Node
  - Deleting a Configuration Node

Prerequisite

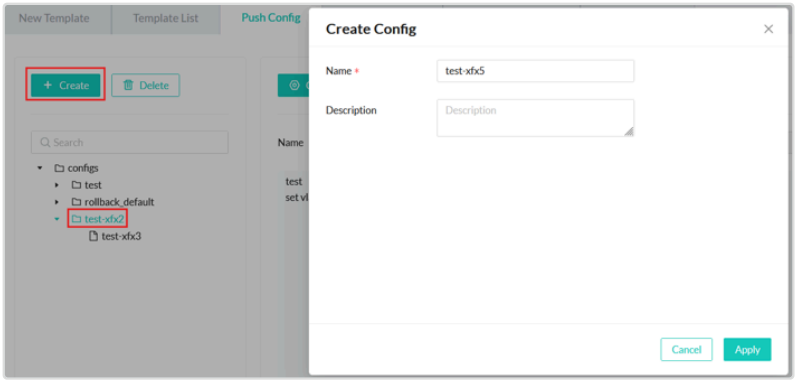
- Ensure that the prerequisite tasks described in Prerequisites have been completed.
- Ensure that you have created the configuration templates with the required CLI commands. For more information, see Adding Configuration Templates.

Procedure

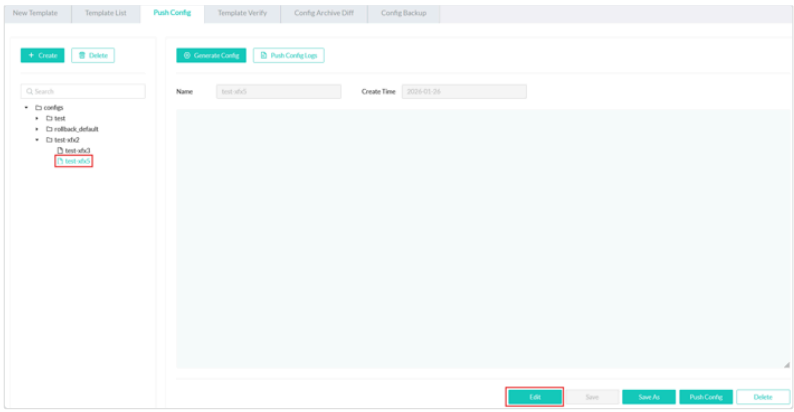
To push configurations to one or multiple switches, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. In the **Push Config** tab, select a folder in the left panel, and then click **+ Create** to create a configuration node. The node will be displayed under the folder.

> **NOTEs**
>
> - A configuration node represents a configuration file.
> - AmpCon-DC provides a built-in root folder named **configs**. After you add configuration nodes, these nodes can also be used as folders.



3. In the pop-up window, enter the configuration node name and its description (optional).
4. Click **Apply**.
5. Click the configuration node that you just created, and click **Edit**.

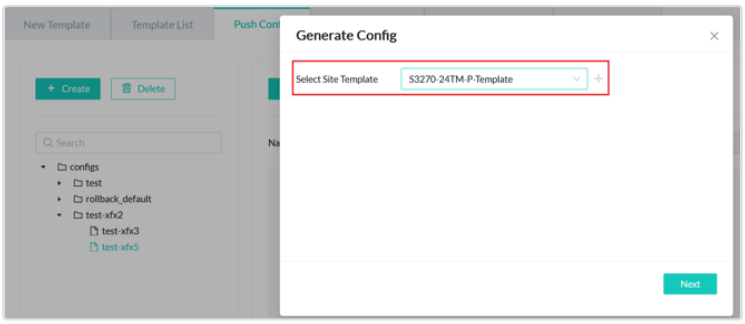


6. Add configurations to be pushed to switches by using either of the following ways:

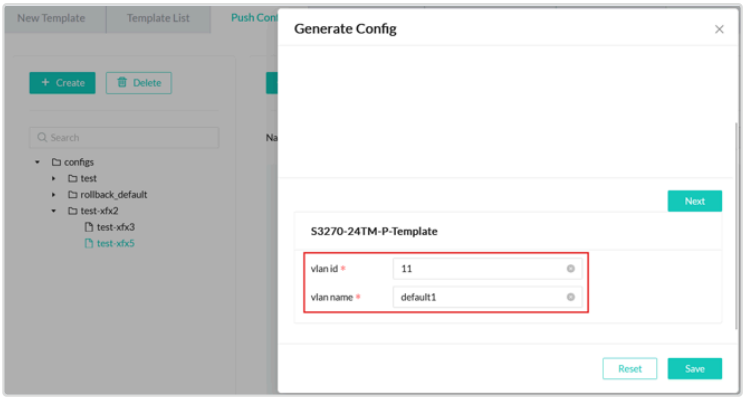
- Enter the CLI commands manually. This method is not recommended because manual CLI commands might lead to human errors.
- Use the configuration templates that you created before:

  a. Click **Generate Config**.

  b. Select a configuration template file from the drop-down list. You can also click the plus icon to add multiple configuration template files.

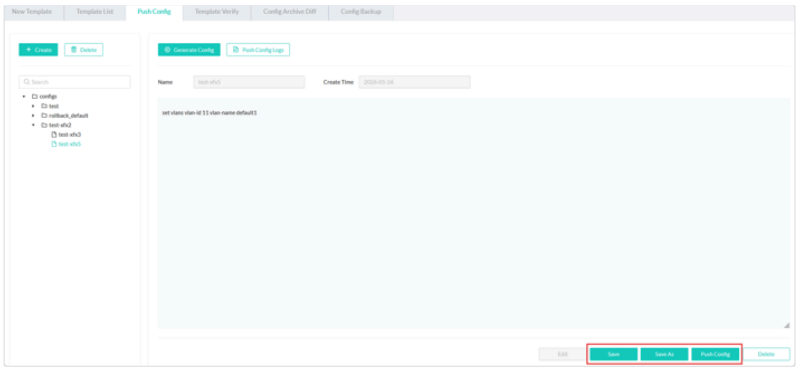


  c. Click **Next**, and then enter the value for each variable.



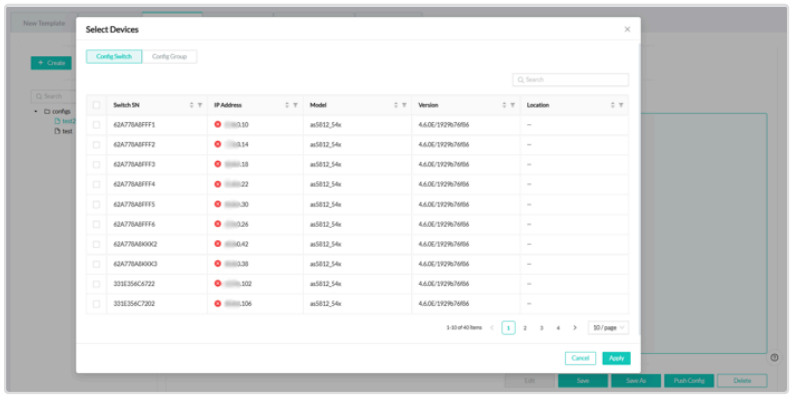
  d. Click **Save.**

7. Click **Save** to save this configuration node, or click **Save As** to generate a new configuration node with these added configurations.



8. Click **Push Config**, and then select the PicOS switches to be configured.

   You can select specific switches in the **Config Switch** tab or select a group in the **Config Group** tab. For how to add a group or manage switches in a group, see Managing Groups.



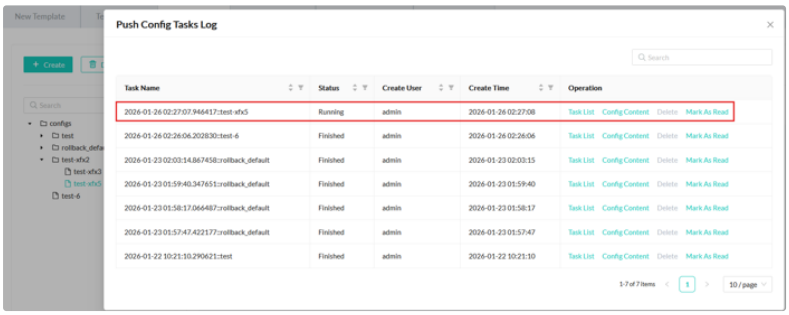
9. Click **Apply** to start the configuration pushing.

Verifying the Pushing Status and Log

To verify whether the configuration is pushed to each switch successfully, follow these steps:

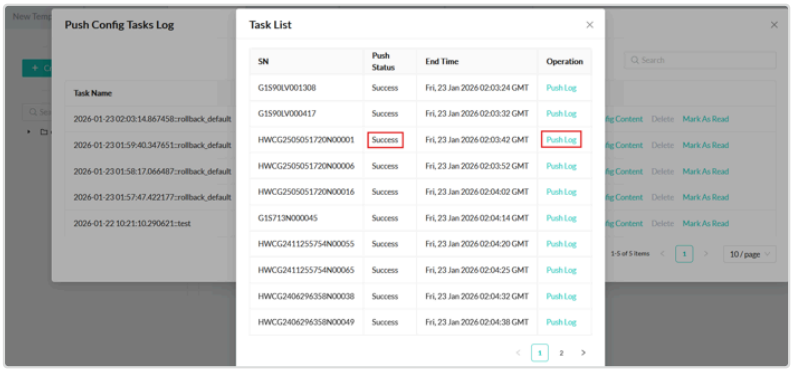
1. Click **Device > Config Templates** from the navigation bar.
2. Click the **Push Config** tab. In this tab, click **Push Config Logs**.
3. In the pop-up window, locate the configuration pushing task related to the configuration node, and then click **Task List**.

> **NOTEs**
>
> - A task name is ended with the related configuration node name.
> - To check the configurations included in a configuration node, click **Config Content**.
> - To mark a task as read, click **Mark As Read**.



4. In the **Task List** pop-up window, check whether the pushing status is **Success**.

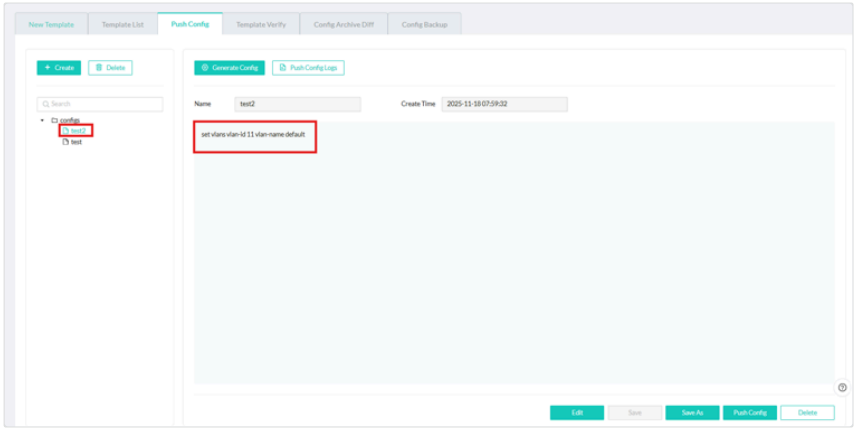
   If the pushing status is not **Success**, click **Push Log** to check more pushing details for troubleshooting.



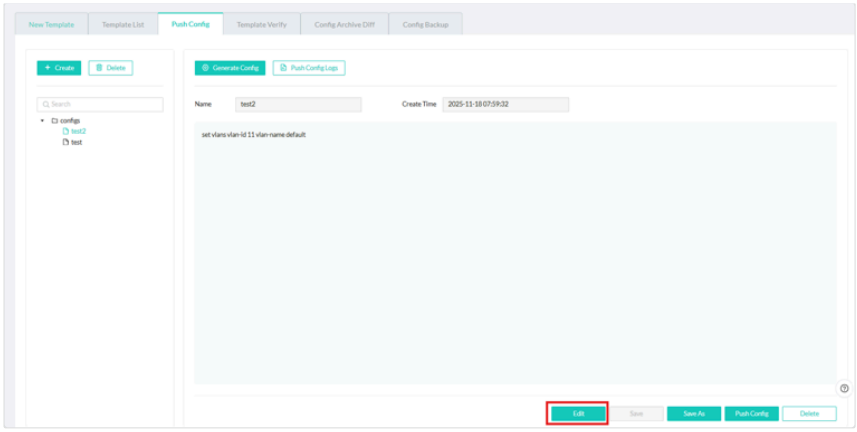
Optional Operations

Viewing or Editing a Configuration Node

In the **Push Config** tab of the “Config Templates” page, click the configuration node that you want to view or edit. You can see the CLI commands in the right panel.

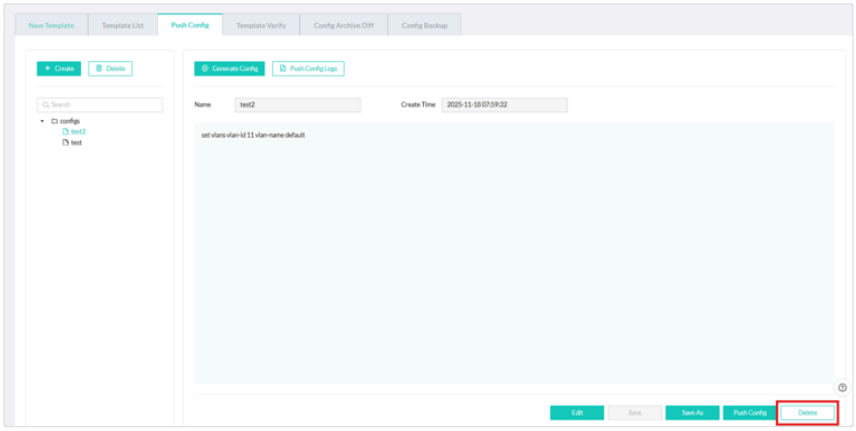


To edit a configuration node, click **Edit**, modify the CLI commands included in the node, and then click **Save**.



Deleting a Configuration Node

In the **Push Config** tab, click the configuration node that you want to delete, and then click **Delete**.



Managing Configuration Templates

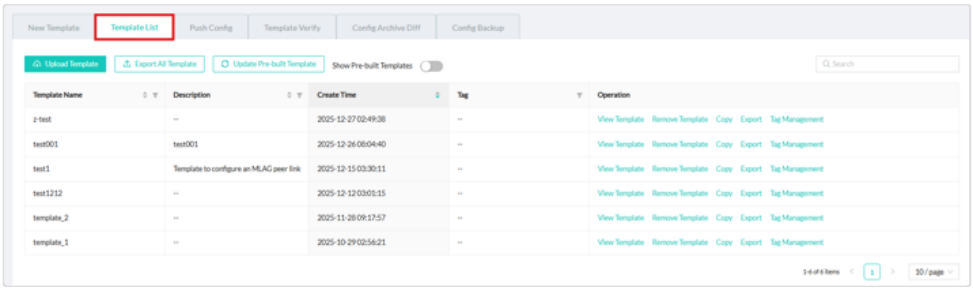
You can manage all the added configuration templates as follows:

- Viewing or Editing a Configuration Template
- Removing a Configuration Template
- Viewing or Updating Pre-Built Templates
- Copying a Configuration Template
- Exporting a Configuration Template
- Exporting All Configuration Template
- Adding a Label to a Configuration Template
- Uploading a Local Configuration Template

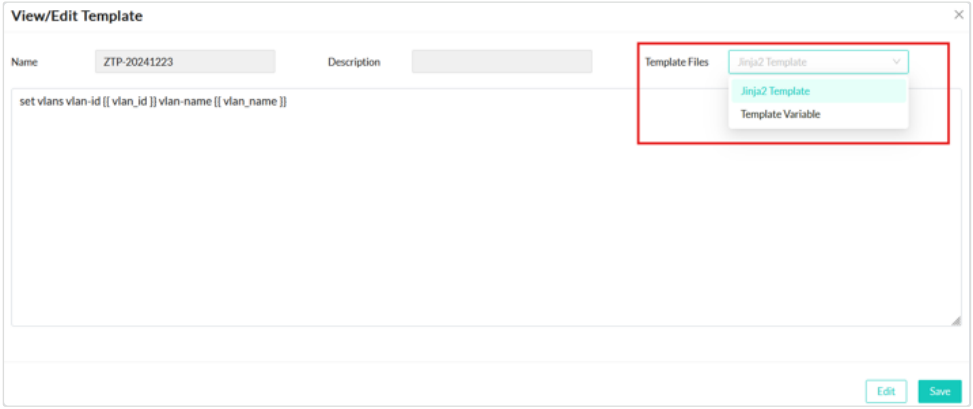
Viewing or Editing a Configuration Template

To view or edit a configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab.



3. Locate a switch, and then click **View Template**.
4. To view a configuration template, select the format for viewing the template in the pop-up window. Then, you can see the template configurations.

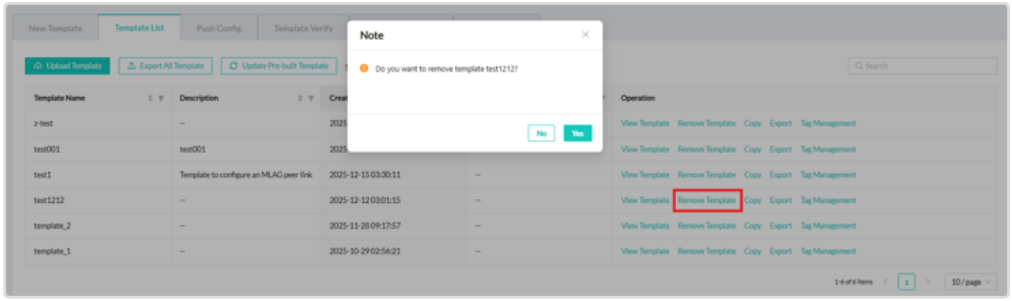


5. To edit a configuration template, click **Edit** in the pop-up window, and then click **Save**.

Removing a Configuration Template

To remove a configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab, locate a switch, and then click **Remove Template**.



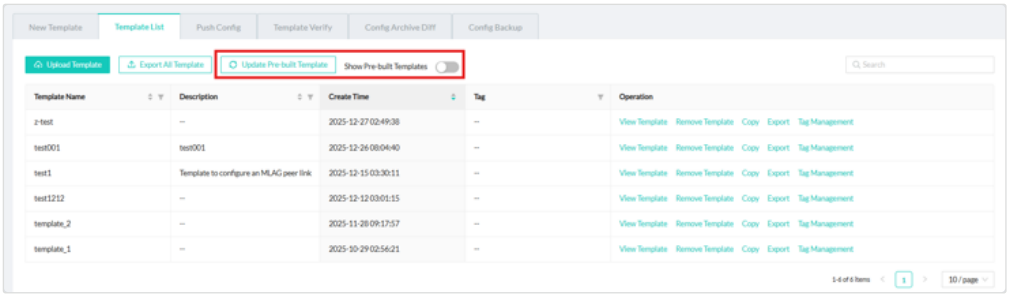
3. Click **Yes** to confirm the deletion.

Viewing or Updating Pre-Built Templates

To view or update pre-built configuration templates, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab.

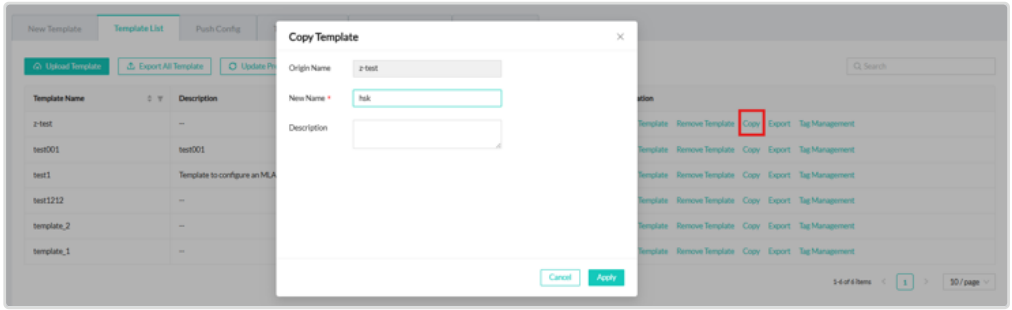
- To view the pre-built templates, click **Show Pre-built Template**.
- To refresh the pre-built template list, click **Update Pre-built Template**.



Copying a Configuration Template

To copy a configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab, locate a switch, and then click **Copy**.
3. Enter the name for the copied template and a description (optional).

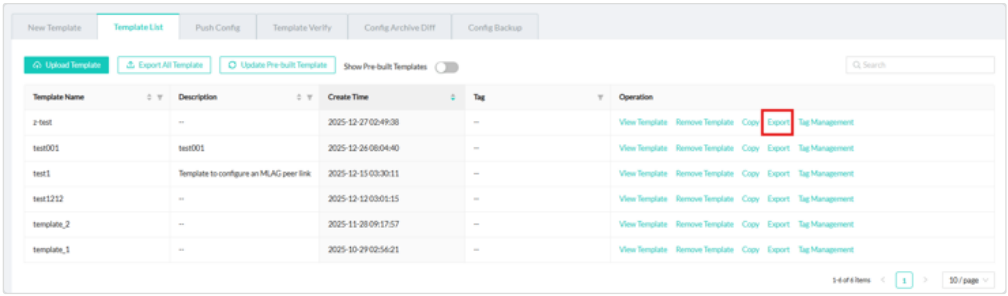


4. Click **Apply**.

Exporting a Configuration Template

To export a configuration template, follow these steps:

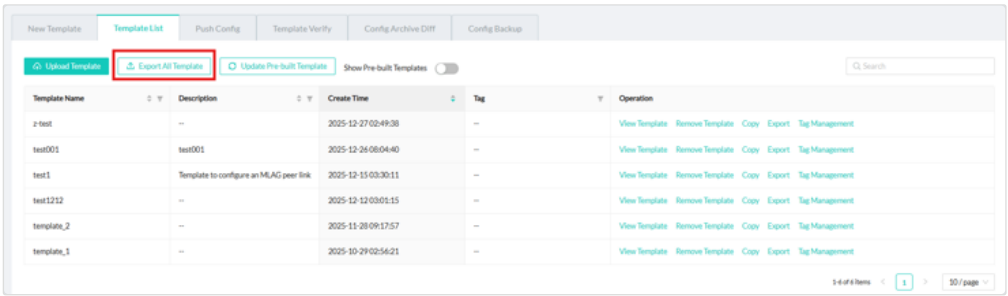
1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab, locate a switch, and then click **Export**.



Exporting All Configuration Template

To export all configuration templates, follow these steps:

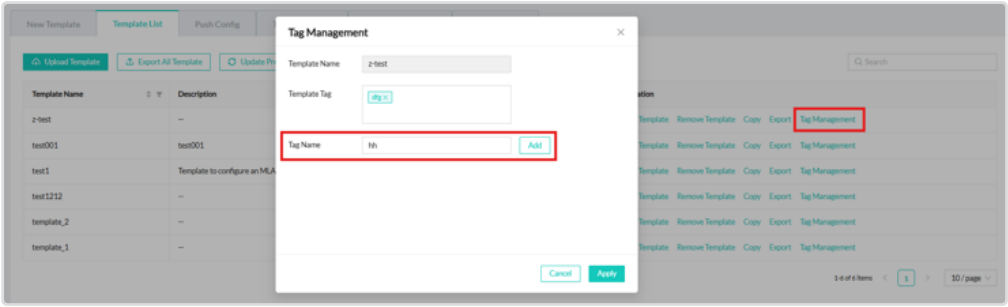
1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab, click **Export All Template**.



Adding a Label to a Configuration Template

To add a label to a configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Template List** tab, locate a switch, and then click **Tag Management**.
3. In the pop-up window, enter the name of the tag.
4. Click **Add**.

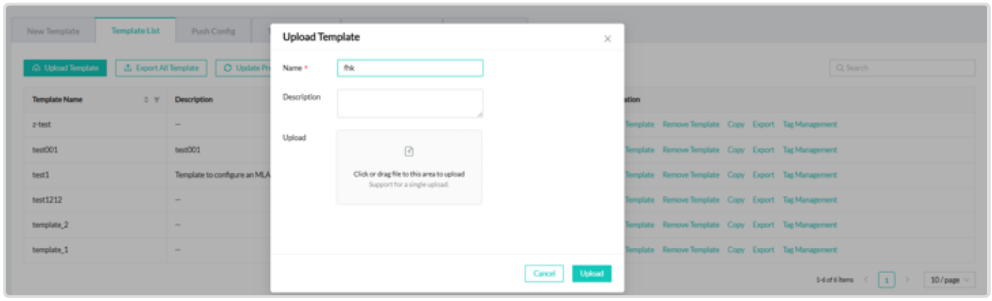


5. Click **Apply**.

Uploading a Local Configuration Template

To upload a local configuration template, follow these steps:

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. In the **Template List** tab, click **Upload Template**.
3. In the pop-up window, enter the name of the configuration template and the template description (optional).
4. Click or drag a .txt template file to upload it.
5. Click **Upload**.



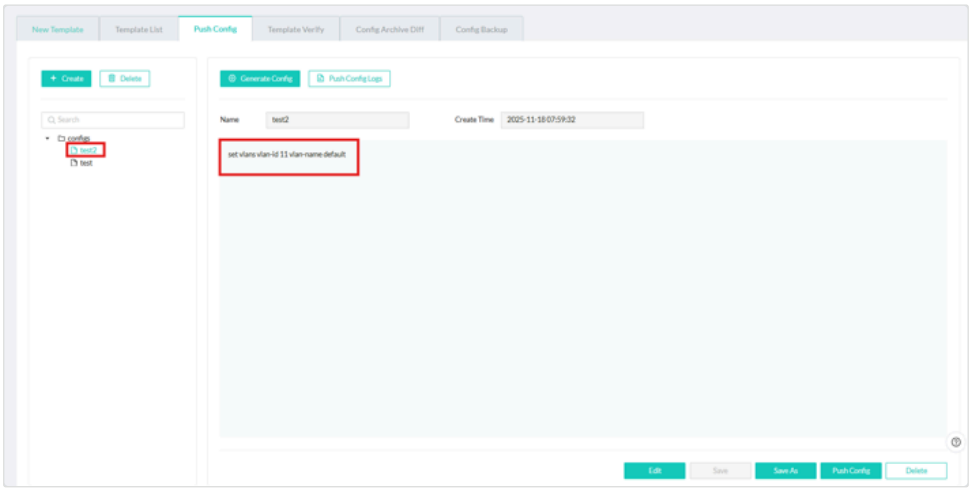
Managing Configuration Nodes

You can view, edit, or delete the configuration nodes that you created as described in [Pushing Configurations to Switches].

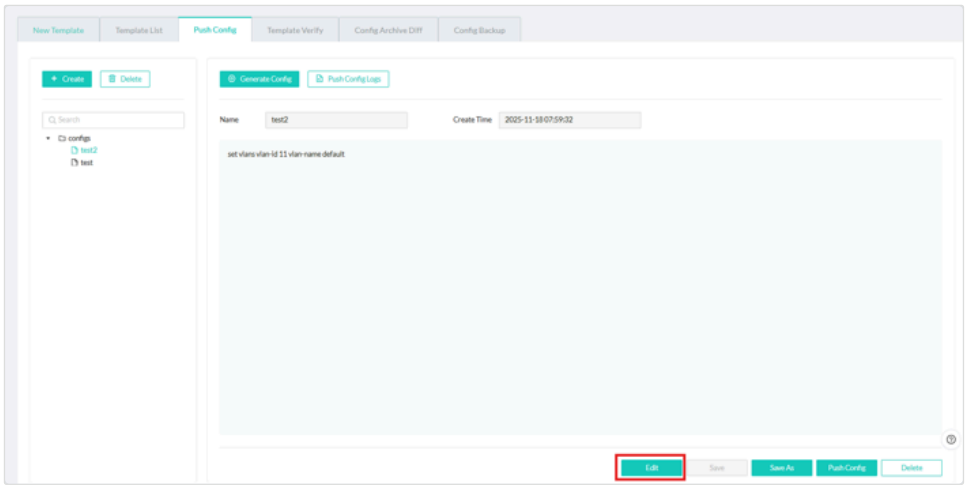
Viewing or Editing a Configuration Node
Deleting a Configuration Node

Viewing or Editing a Configuration Node

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. In the **Push Config** tab, click the configuration node that you want to view or edit. You can see the CLI commands in the right panel.



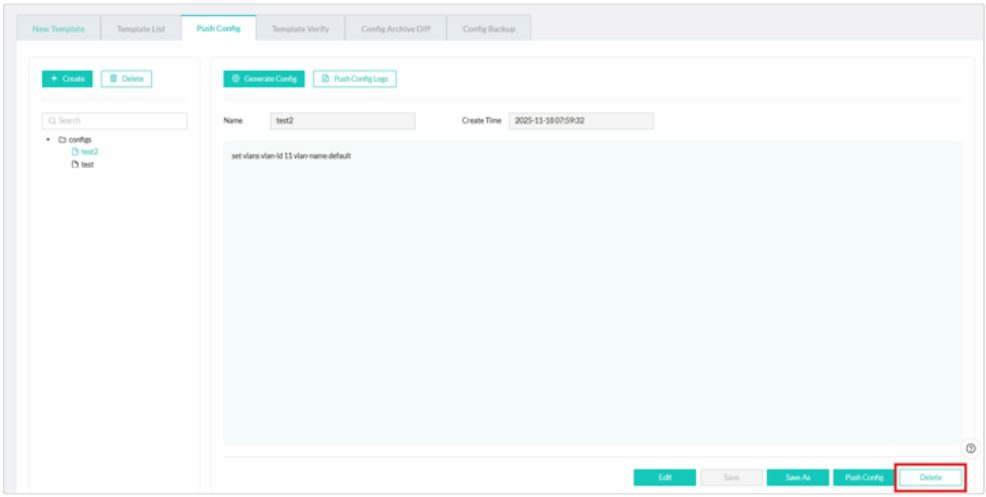
To edit a configuration node, click **Edit**, modify the CLI commands included in the node, and then click **Save**.



Deleting a Configuration Node

1. In the **Push Config** tab, click the configuration node that you want to delete.

2. Click **Delete**, and then click **Yes** to confirm the deletion.



Comparing Running Configurations with Initial Configurations

You can compare running configurations with initial configurations on the same switch.

- **Initial configurations**

  Configurations included in the switch configuration, including the global configuration file and the configuration template.

- **Running configurations**

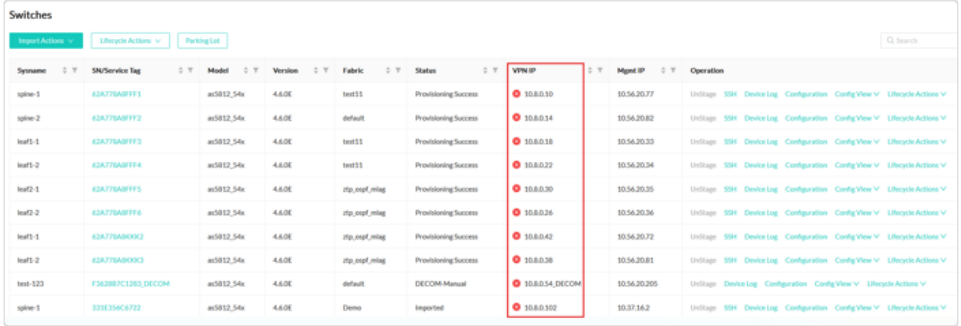
  Configurations that are currently running on the switch.

> **NOTE**
>
> This feature doesn't support the following scenarios:
>
> - Comparing configurations on two different switches.
> - Comparing configurations on imported switches.
> - Comparing configurations on switches deployed through simplified ZTP.
> - Comparing configurations on disconnected switches (switches can't connect with the AmpCon-DC server).

Prerequisites

Ensure that the following prerequisites are met:

- Click **Device > Switches**, and check the **VPN IP** column on the "Switches" page, and ensure that the switch to compare is online (connected to the AmpCon-DC server).
- √: The switch is connected to the AmpCon-DC server.
- x: The switch is not connected to the AmpCon-DC server.



- Check the **Status** column, and ensure that the switch to compare is not in **Imported** status.

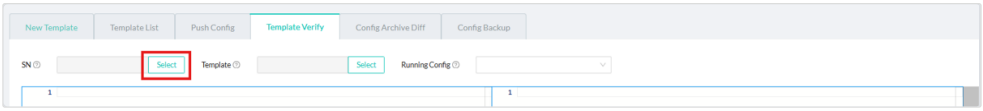
After you replace an imported switch with a new switch through RMA, the new switch is shown as **Provisioning Success**. However, you still can't compare running configurations with initial configurations on this new switch.

This is because the new switch is configured through the backup configuration file or uploaded configurations of the imported switch during the deployment process, instead of creating a switch configuration.

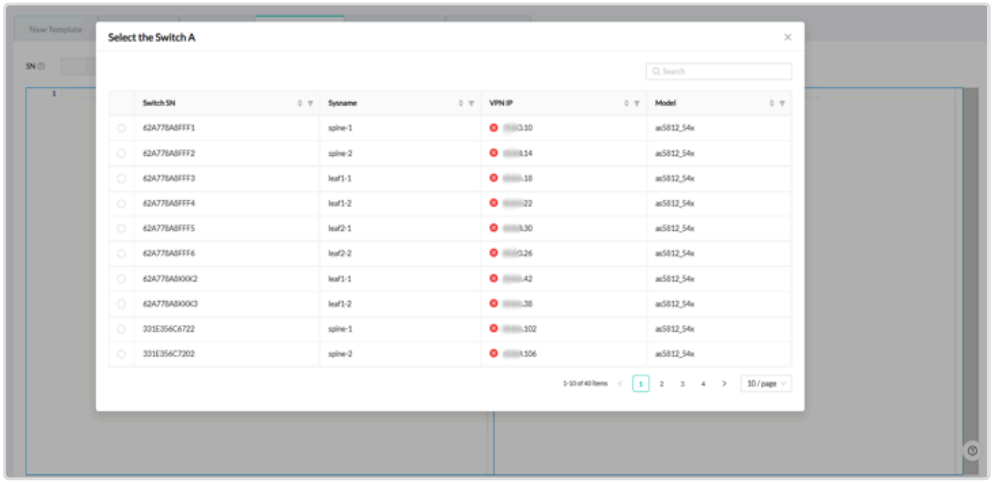
Procedure

1. In the AmpCon-DC UI, click **Device > Config Template** from the navigation bar.
2. In the **Template Verify** tab, click **Select** in the **SN** field.

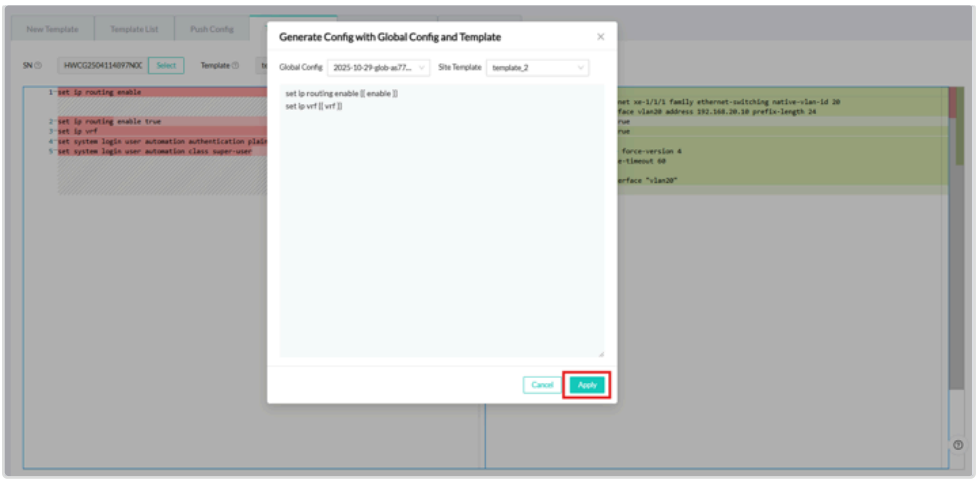
> **NOTE**
>
> Ensure that the selected switch is online, which means the switch is not connect with the AmpCon-DC server.



3. In the pop-up window, select the switch to compare.

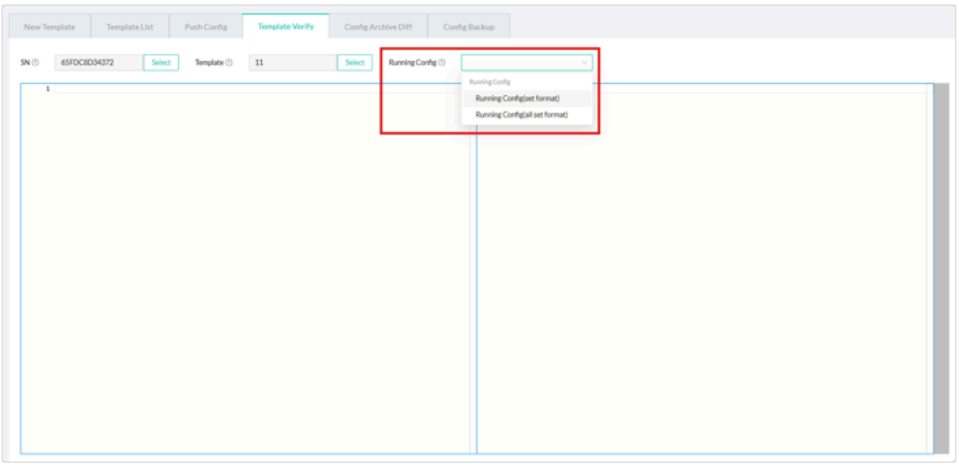


4. In the **Template** field, click **Select**.
5. In the pop-up window, select the global configuration file and the configuration template that you pushed to the switch during the initial switch deployment process. Then, click **Apply**.



6. In the **Running Config** drop-down list, select **Running Config(set format)** or **Running Config(all set format)**.

- **Running Config(set format):** Displays configurations as the **show | display set** command result on the switch.
- **Running Config(all set format):** Displays configurations as the **show all | display set** command result on the switch.



Then, you can see differences between the running configurations and the initial configurations on the switch.

Comparing Running or Backup Configurations

You can compare running configurations or backup configurations on one switch or on different switches.

- **Running configurations**

  Configurations that are currently running on a switch.

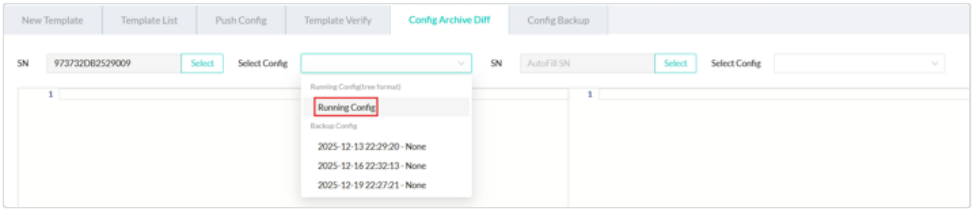
- **Backup configurations**

  Configuration files that were backed up as described in Backing up Switch Configurations.

Procedure

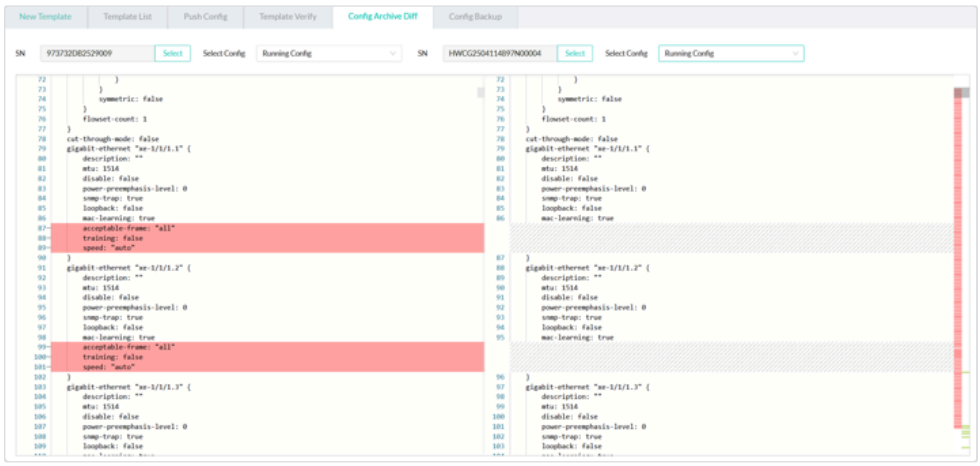
1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. In the **Config Archive Diff** tab, click **Select** in the first **SN** section. In the pop-up window, select a switch.
3. In the first **Select Config** drop-down list, select **Running Config** or a backup configuration file.

> **NOTEs**
>
> - For offline switches (switches are not connect with the AmpCon-DC server), **do not** select **Running Config**. This is because AmpCon-DC can't retrieve the current configurations from the offline switch.
> - If no backup configuration files are displayed, create a new backup configuration file. For more information, see Backing Up Switch Configurations.



4. In the second **SN** section, click **Select**. In the pop-up window, select another switch.
5. In the second **Select Config** drop-down list, select a running configuration file or a backup configuration file.

Then, you can see configuration differences as follows:



Backing Up and Restoring Configurations

For the switches managed by AmpCon-DC, you can automatically back up configurations at a specific interval and time or manually back up configurations. In addition, you can restore configurations based on a backup configuration file for disaster recovery.

Backing Up Configurations
- Backing Up Configurations Automatically
- Backing Up Configurations Manually

Checking Backup Configuration Files

Rolling Back Configurations

Optional Operations
- Uploading Configurations
- Viewing Configurations
- Viewing Backup Logs

Backing Up Configurations

Backing Up Configurations Automatically

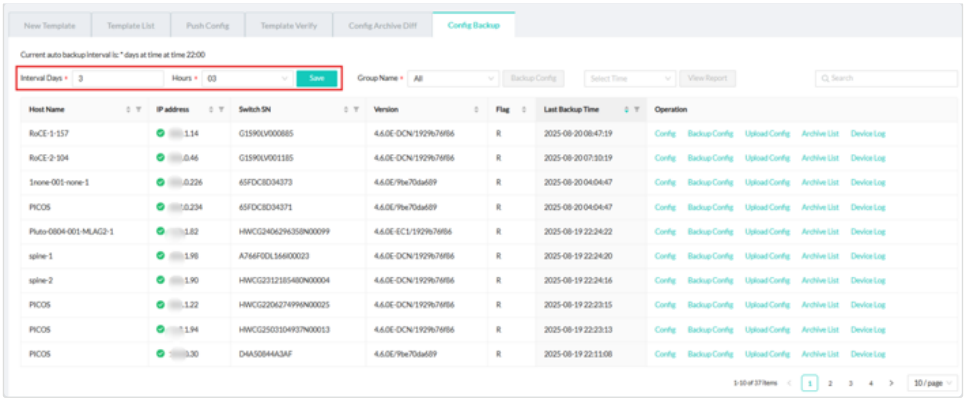
To back up configurations for switches periodically and automatically, follow these steps:

> **NOTEs**
>
> - For a switch deployed through normal ZTP, if **Backup Config** is not selected in the **Option Post-Deployed** section when you add the switch configuration, the automatic backup will not work for this switch. You can manually back up configurations for this switch.
> - For a switch imported to AmpCon-DC or deployed through simplified ZTP, the automatic backup is enabled by default. You don't need to configure the switch configuration for this switch.

1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Config Backup** tab. In this tab, set the automatic backup interval and time:

- **Interval Days:** The interval in days between each backup.
- **Hours:** The time (a specific hour) when a backup is started.

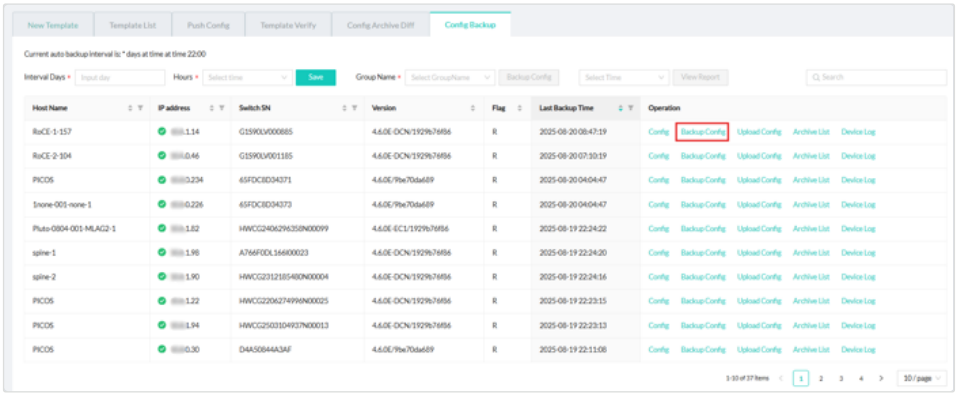
3. Click **Save**. Then, AmpCon-DC will automatically back up configurations at the specific interval and time.



Backing Up Configurations Manually

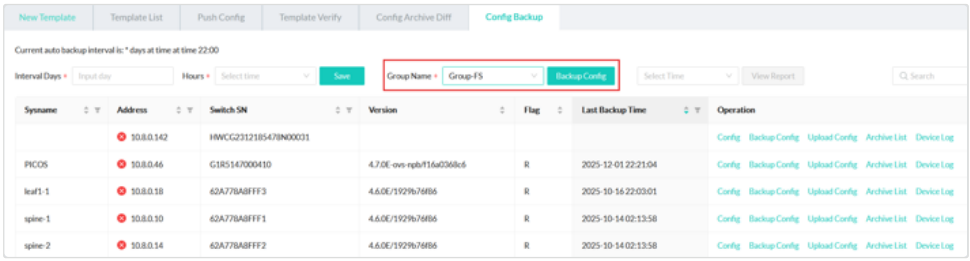
1. In the AmpCon-DC UI, click **Device > Config Templates** from the navigation bar.
2. Click the **Config Backup** tab. In this tab, manually back up configurations for a single switch or all switches in a switch group:

- To back up configurations for a single switch, locate the switch, and then click **Backup Config**.



- To back up configurations for all switches in a switch group, select the switch group from the **Group Name** drop-down list, and then click **Backup Config**.

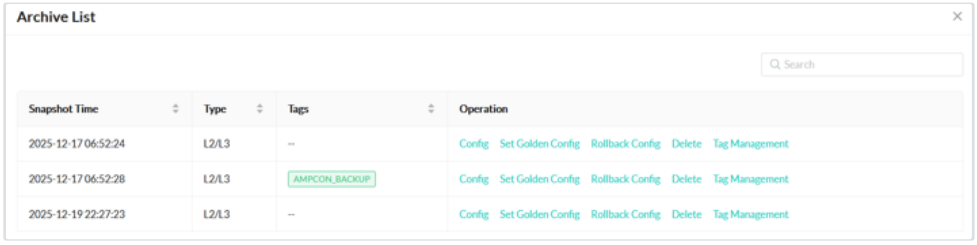
  To add a new switch group, see Adding a Switch Group.



Checking Backup Configuration Files

To check whether the backup configuration file for a switch is created successfully, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Archive List**.
2. In the pop-up window, check whether the backup configuration file is displayed in the archive list.



In the archive list, you can do the following operations if needed:

- To check the details in a backup configuration file, click **Config**.
- To mark a backup configuration file with the **Golden Config** tag, click **Set Golden Config**. Only one backup configuration file can be marked with **Golden Config**.
- AmpCon-DC automatically generates backup configuration files when you deploy physical networks, logical networks, or lossless networks. These backup configuration files are marked with the **AMPCON_BACKUP** tag.

  Except the backup configuration files marked with **Golden Config** and **AMPCON_BACKUP**, the maximum number of backup configuration files that you can create is determined by the **Config Backup Number** value in the global system configuration. For more information, see Adding a Global System Configuration.

  For example, a switch has a backup configuration file marked with **Golden Config** and a backup configuration file marked with **AMPCON_BACKUP**, and the **Config Backup Number** value in the global system configuration is set to **3**. In this case, you can create at most 3 new backup configuration files.

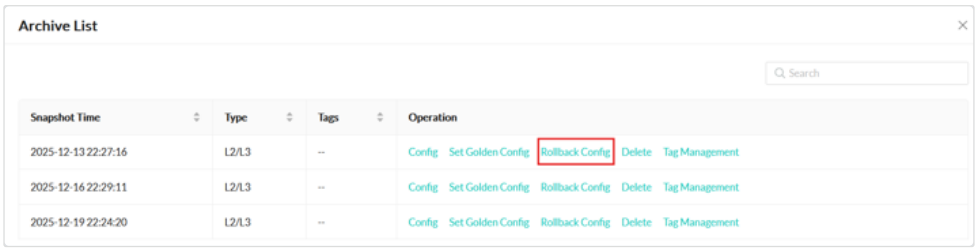
  > **NOTE**
  >
  > The backup configuration files marked with **Golden Config** and **AMPCON_BACKUP** are used for switch RMA. For more information, see RMA Workflow.

- To delete a backup configuration file, click **Delete**.
- To add or delete tags for a backup configuration file, click **Tag Management**. The added tags will be displayed in the **Tags** column.

Rolling Back Configurations

To restore configurations based on a backup configuration file, follow these steps:

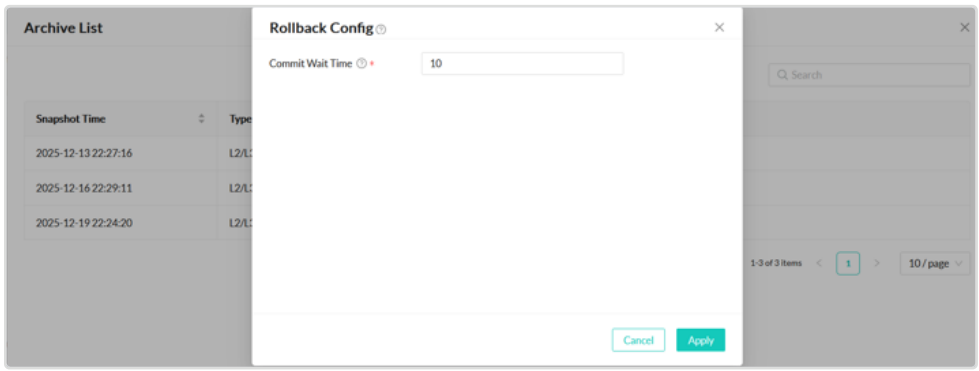
1. In the **Config Backup** tab, locate the switch, and then click **Archive List**.
2. Locate the back configuration file, and then click **Rollback Config**.



3. In the **Commit Wait Time** field of the pop-up window, set the wait time in seconds.

   The default value is 10. The value needs to be an integer ranging from 10 to 240.

> **NOTE**
>
> In some cases, AmpCon-DC can't access switches. After you click **Apply** in the pop-up window, if AmpCon-DC still can't access the switch after the specified **Commit Wait Time**, the rollback will fail.



4. Click **Apply**.

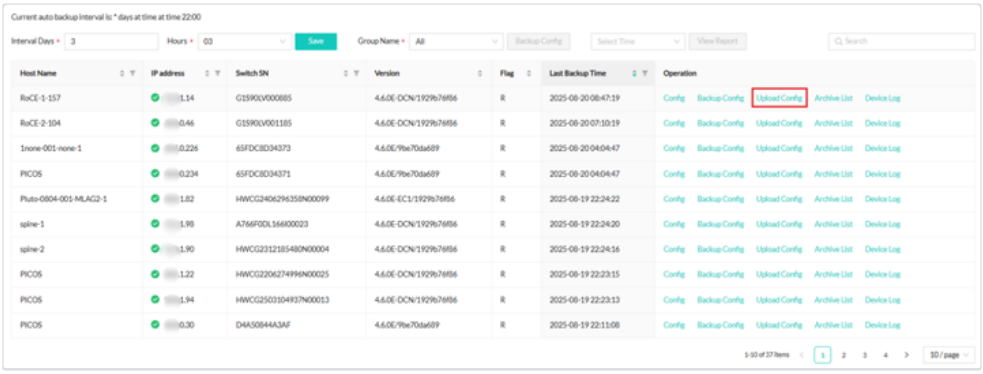
Optional Operations

Uploading Configurations

You can upload a local switch configuration file to AmpCon-DC. After you upload the configuration file, the uploaded configurations can't be pushed to the switch. These uploaded configurations can be pushed to only the new switch during the RMA process. For more information, see RMA Workflow.

To upload local configurations for a switch, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Upload Config**.



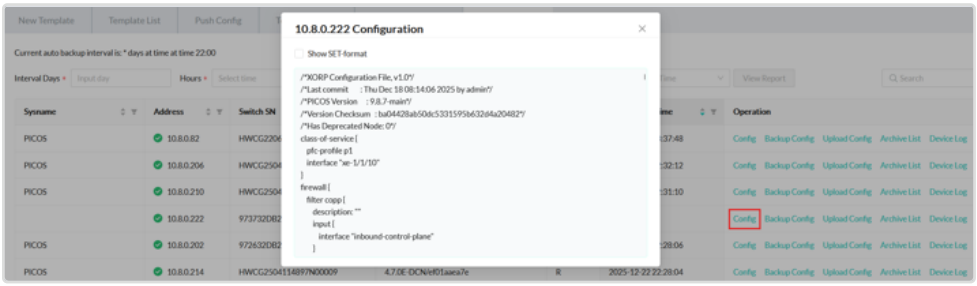
2. Select a .boot file containing switch configurations, and then upload the file.

Viewing Configurations

Each time you back up configurations for a switch, AmpCon-DC will collect all the configurations from the switch and display these configurations in the **Configuration** pop-up window. The uploaded configurations are also displayed in the **Configuration** pop-up window.

To view these configurations, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Config**.
2. In the **Configuration** pop-up window, check the configurations as follows:



You can click **Show SET-format** to display the configurations in **set xx** format.



Viewing Backup Logs

To view backup logs of a switch, follow these steps:

1. In the **Config Backup** tab, locate the switch, and then click **Device Log**.

2. In the pop-up window, check whether the backup is successful. The message “Retrieve config success” indicates a successful backup.



Running Ansible Playbooks for Automation

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

AmpCon-DC offers the picos_config Ansible module to interact with managed devices, making it easy to automate tasks such as configuring interfaces, VLANs, and managing security settings. The picos_config module is included in the AmpCon-DC server.

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

See the following child topics:

- Examples for Ansible Playbooks
- Running Playbooks
- Managing Ansible Jobs
- Viewing Playbook Scheduling
- Troubleshooting

> **NOTEs**
>
> - For more information about Ansible, see Getting started with Ansible.
> - For the workflow of running Ansible playbooks with AmpCon-DC, see Ansible Automation Workflow.

Examples for Ansible Playbooks

Ansible modules are code or binaries that Ansible copies to and executes on each managed device to accomplish the action defined in each Ansible task.

AmpCon-DC offers the picos_config Ansible module to interact with managed switches. The picos_config module, included in the AmpCon-DC server, makes it easy to automate tasks such as configuring interfaces, VLANs, and managing security settings.

Before you run Ansible playbooks on managed switches, write playbooks based on the following configuration examples, which are supported by the picos_config Ansible module.

> **NOTE**
>
> This topic only shows playbook examples for managed switches with PicOS installed.
>
> - To run Ansible playbooks on Linux servers that you added, write playbooks based on playbook syntax described in Using Ansible Playbooks.
> - For the workflow of using Ansible playbooks on AmpCon-DC, see Ansible Automation Workflow.
> - For detailed steps of writing, importing, and running playbooks on AmpCon-DC, see Running Playbooks.

Syntax Examples
- Running Linux Shell Commands
- Showing Switch Configurations or Status
- Modifying Switch Configurations
- Loading Configurations in a Configuration File
- Using Variables in a Playbook

Real-World Example: Automating VLAN Configurations

Related PicOS References

Syntax Examples

Running Linux Shell Commands

To run Linux shell commands in managed switches, use the **shell** mode.

Playbook YAML Example:

```
---
- name: Shows uptime info for all switches
  hosts: all
```

```
  tasks:
  - name: Shows uptime info for all switches
    picos_config: mode='shell' cmd='uptime'
    register: exec_result
  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the Linux shell command **uptime** under the **Linux shell** mode to show the current time, the time since the system and processes started, the number of logged-in users, and the average time of system load in the last 1 minute, 5 minutes, and 15 minutes.

Replace the command in the **cmd** field with any other Linux shell command to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-DC UI. For how to check playbook execution results, see Managing Ansible Jobs.



Showing Switch Configurations or Status

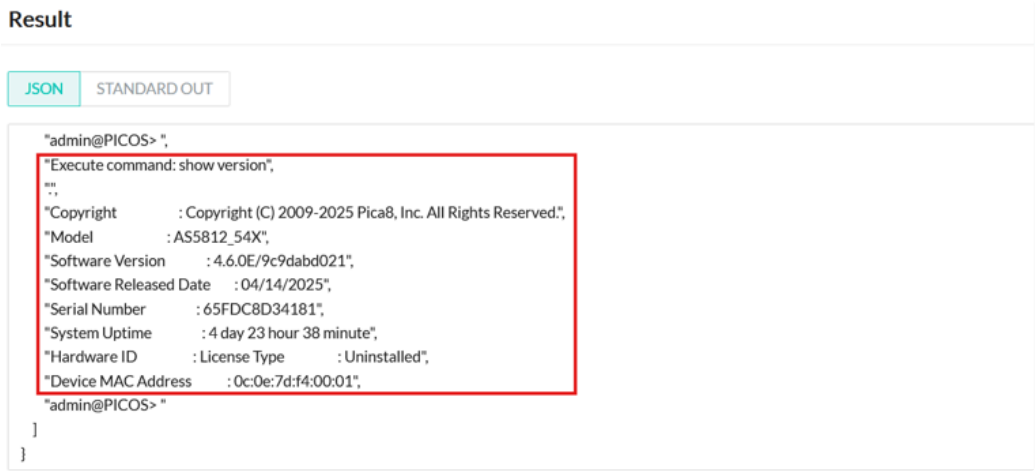
To show configurations or status of managed switches, use the **cli_show** mode.

Playbook YAML Example:

```
---
- name: Show Version info of all switches
  hosts: all
  tasks:
  - name: Show version of switches
    picos_config: mode='cli_show' cmd='show version'
    register: exec_result
  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the PicOS command **show version** under the **operation** mode to show switch version information. Replace the command in the **cmd** field with any other Linux shell command to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-DC UI.



Modifying Switch Configurations

To modify configurations of managed switches, use the **cli_config** mode.

Playbook YAML Example:

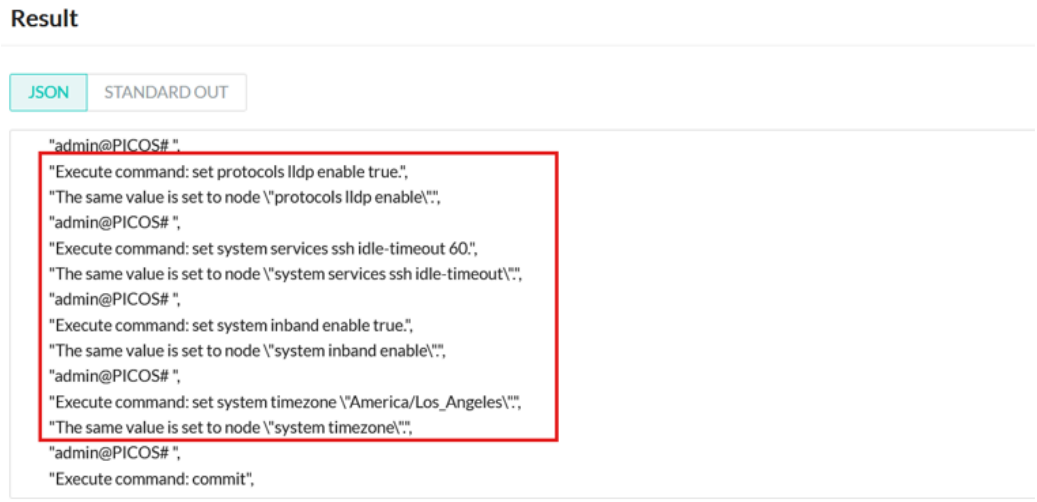
```
---
- name: Enable Global Config
  hosts: all
  tasks:

  - name: Enable Global Config
    picos_config:
      mode: 'cli_config'
      cmd: >
        set ip routing enable true;
        set protocols lldp enable true;
        set system services ssh idle-timeout 60;
        set system inband enable true;
        set system timezone "America/Los_Angeles";
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the following PicOS commands under the **configuration** mode. Replace the commands in the **cmd** section with any other PicOS commands to meet your needs.

After you run this playbook, check the playbook execution result in the AmpCon-DC UI.



Loading Configurations in a Configuration File

To load configurations from a configuration file into an Ansible playbook, use the **config_load** mode.

Playbook YAML Example:

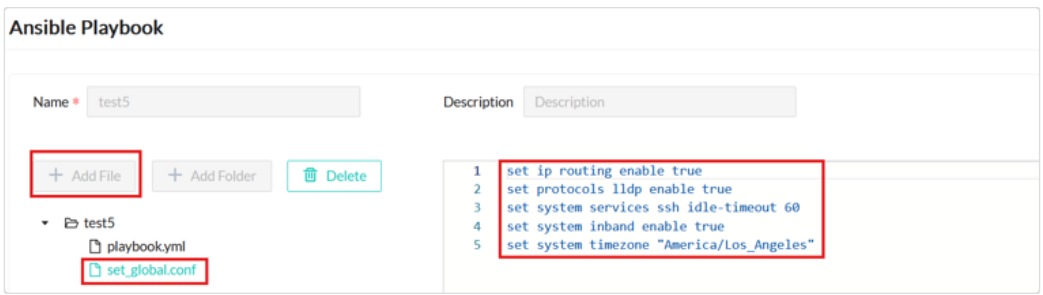
```
---
- name: Deploy services
  hosts: all
  tasks:
  - name: Transfer the script
    copy: src=set_global.conf dest=/home/admin/setconfig1.conf force=ye

  - name: Activate the configuration
    picos_config: mode='config_load' cmd='/home/admin/setconfig1.conf'
    register: exec_result

  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example contains a syntax to copy the commands in the **set_global.conf** file (the file you added in the AmpCon-DC UI) to the local **/home/admin/setconfig1.conf** file on the switch side. When you run the playbook on one or multiple switches, the copied commands will be loaded and then executed on these switches.

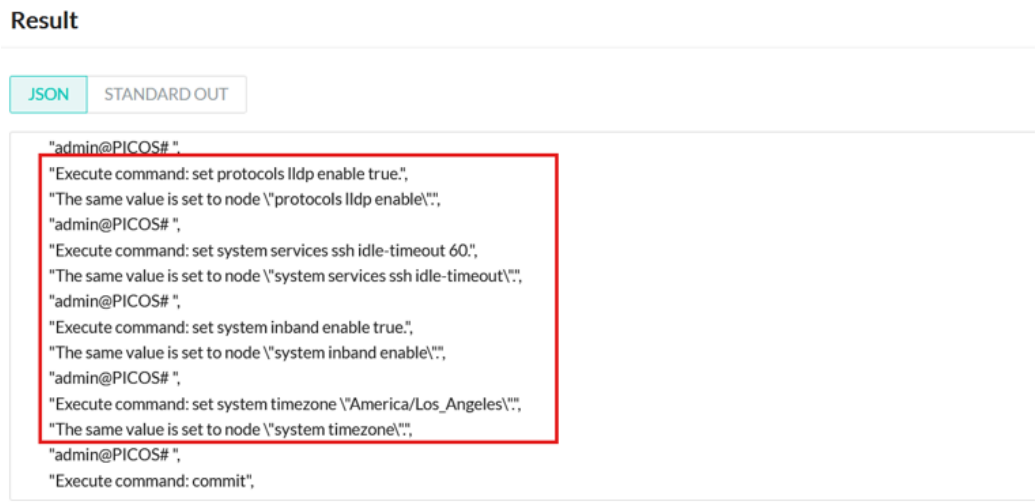
After you write the **playbook.yml** file, ensure to click **Add File** to add the **set_global.conf** file.



The **set_global.conf** file contains the following commands. Replace the commands with any other PicOS commands to meet your needs.

```
set ip routing enable true
set protocols lldp enable true
set system services ssh idle-timeout 60
set system inband enable true
set system timezone "America/Los_Angeles"
```

After you run this playbook, check the playbook execution result in the AmpCon-DC UI.



Using Variables in a Playbook

To define variables in an Ansible playbook, use the variable syntax {{*variable_name*}}.

Playbook YAML Example:

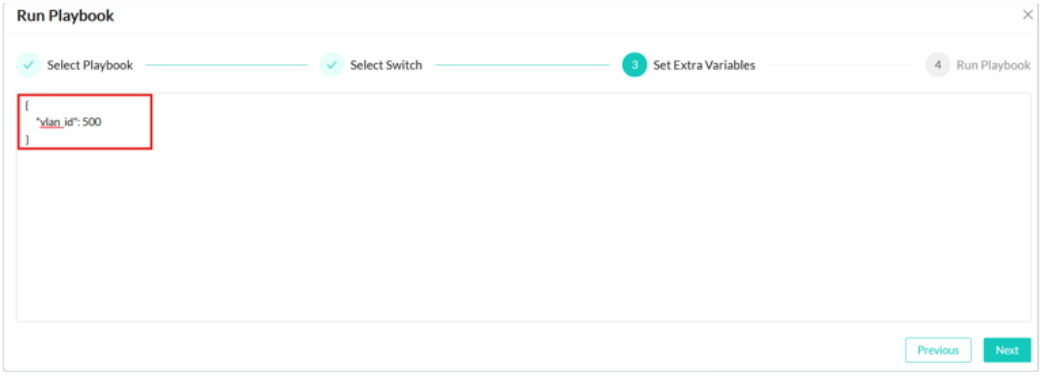
```
---
- name: Set Dynamic VLAN
  hosts: all
  tasks:

  - name: Set Dynamic VLAN
    picos_config: mode='cli_config' cmd='set vlans vlan-id {{vlan_id}}
    register: exec_result

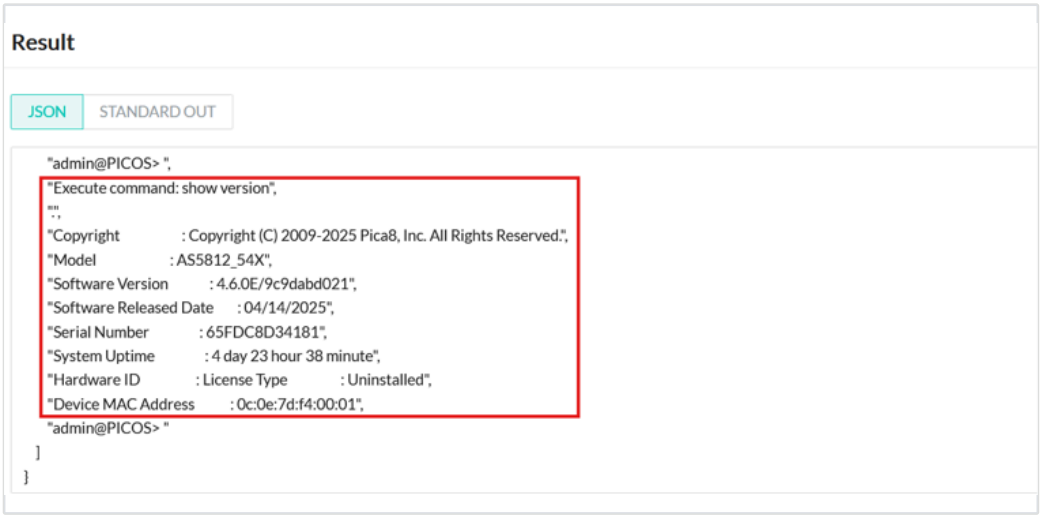
  - name: Show execution result
    debug: var=exec_result.stdout_lines
```

This playbook example runs the PicOS command **set vlans vlan-id {{*vlan_id*}} vlan-name "{{*vlan_id*}}"** to create a VLAN. In the command, ***vlan_id*** is a variable and must be included in a set of curly braces.

When you run the playbook, ensure to set the variable value in JSON format as described in **Step 6** of Running a Playbook.



After you run this playbook, check the playbook execution result in the AmpCon-DC UI.



Real-World Example: Automating VLAN Configurations

As a network administrator, you might feel tedious and time-consuming to configure VLANs on multiple switches manually. By using Ansible playbooks on AmpCon-DC, you can automate this process.

Playbook YAML Example:

```
---
- name: Set VLAN Network
  hosts: all
  tasks:

  - name: Set VLAN Network
    picos_config:
      mode: 'cli_config'
      cmd: >
        set vlans vlan-id 10 l3-interface vlan10;
        set vlans vlan-id 20 l3-interface vlan20;
        set vlans vlan-id 30 l3-interface vlan30;
        set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
        set interface gigabit-ethernet te-1/1/1 family ethernet-switchi
        set l3-interface vlan-interface vlan10 address 192.160.10.1 pre
        set l3-interface vlan-interface vlan20 address 192.160.20.1 pre
        set l3-interface vlan-interface vlan30 address 192.160.30.1 pre
    register: exec_result

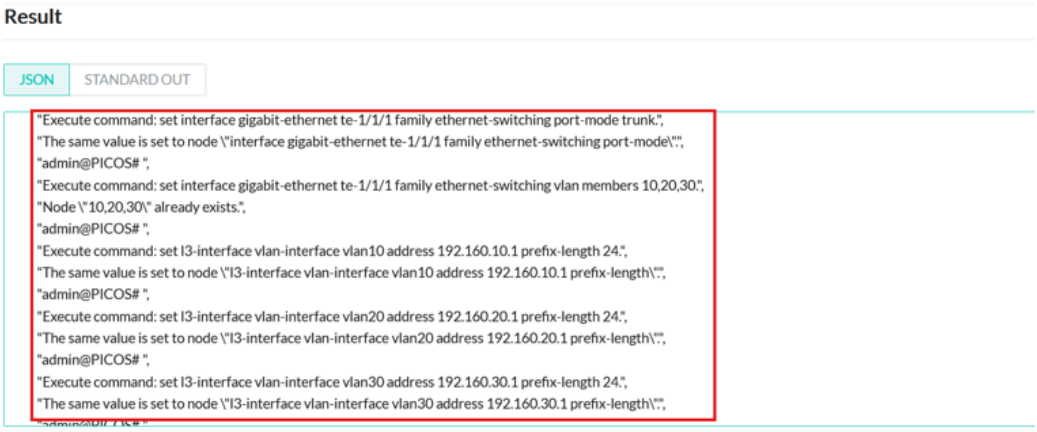
```

```
20    - name: Show execution result
21      debug: var=exec_result.stdout_lines
```

This playbook example runs multiple PicOS commands to achieve the following goals:

- Create vlan10, vlan20, and vlan30.
- Add a trunk LAG port (te-1/1/1) to vlan10, vlan20, and vlan30.
- Configure IPv4 addresses for L3 interfaces of vlan10, vlan20, and vlan30.

After you run this playbook, check the playbook execution result in the AmpCon-DC UI.



Related PicOS References

- Linux Shell Mode, Operation Mode, and Configuration Mode
- Routing and Switching Command Reference

Running Playbooks

On the “Playbooks” page, you can see the list of playbooks that are created. You can add or import a playbook, check syntax for a playbook, or run a playbook as needed.

In addition, AmpCon-DC provides multiple playbook management functions including copying playbooks, using pre-built playbooks, editing, deleting, copying, or exporting playbooks, and adding tags to playbooks.

> **NOTE**
>
> Before you run Ansible playbooks, pay attention to the following best practices:
>
> - **Test in a lab:** Always test your automation scripts in a lab or on non-production devices to ensure they work as expected.
> - **Idempotency**: Ansible playbooks should be written to be idempotent, meaning running the playbook multiple times won’t cause unintended changes.
> - **Backups**: Before applying any configuration, ensure that you have backups of the current configurations. For more information, see Backing Up and Restoring Configurations.

Prerequisites
Procedure
  Writing a Playbook on AmpCon-DC
  Importing a Playbook
  Running a Playbook
Optional Operations
  Checking Syntax for a Playbook
  Using Pre-built Playbooks
  Editing a Playbook
  Deleting a Playbook
  Copying a Playbook
  Exporting a Playbook
  Adding or removing Playbook Tags

Prerequisites

- To run playbooks on PicOS switches, ensure that the following prerequisites are met:
  - You have deployed these switches through normal ZTP or simplified ZTP, or imported these switches. For more information, see Importing Switches, Simplified ZTP Deployment, and

Deploying Switches through Normal ZTP.

- Ensure that the **Device Default Login User** and **Device Default Password** in the global system configuration can be used to log in to these switches. For more information, see Adding a Global System Configuration.
- These switches are connected to the AmpCon-DC server. Check the connectivity by clicking **Device > Switches** from the navigation bar and then checking the **VPN IP** column.
  - ✓: The switch is up and connected to the AmpCon-DC server.
  - x: The switch is down or not connected to the AmpCon-DC server.

- To run playbooks on Linux servers, ensure that the Linux servers are added to AmpCon-DC. For more information, see Adding Devices.

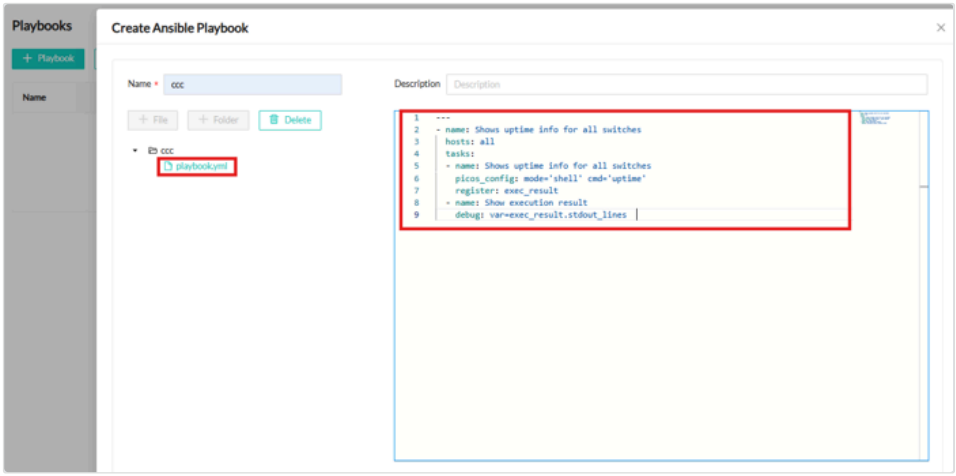
Procedure

Writing a Playbook on AmpCon-DC

If you don't have an available Ansible playbook, you can write an Ansible playbook on AmpCon-DC. Follow these steps:

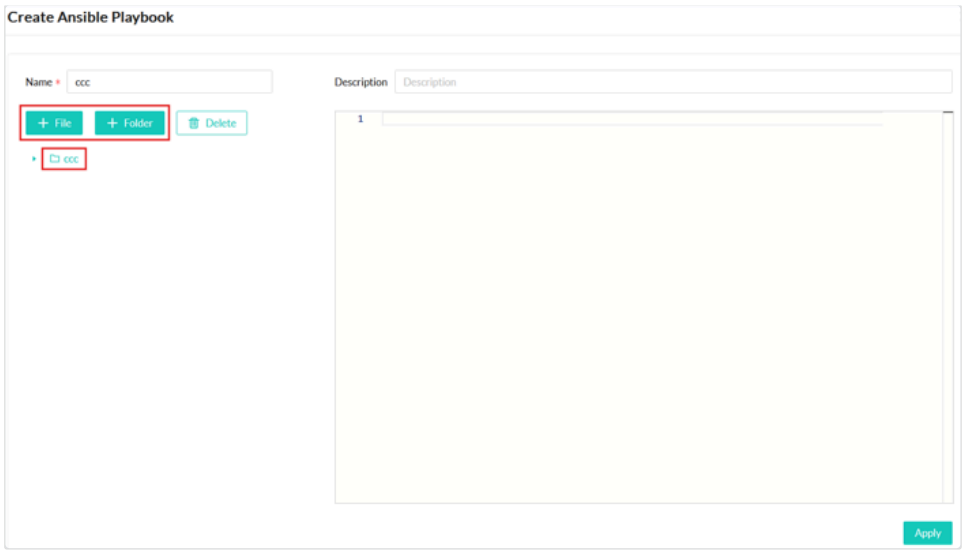
1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the "Playbooks" page, click **+ Playbook**.
3. Enter the playbook name and description (optional). Click **playbook.yml**, and add contents to the .yml file.

   For playbook configuration examples, see Examples for Ansible Playbooks.



4. Optional: To add files or folders to the playbook, click the playbook name (click **ccc** in the following screenshot), and then click **+ File** or **+ Folder**.

   For example, to load configurations from a configuration file to the playbook, click **+ File** to add a **.conf** file. For more information, see Loading Configurations in a Configuration File.



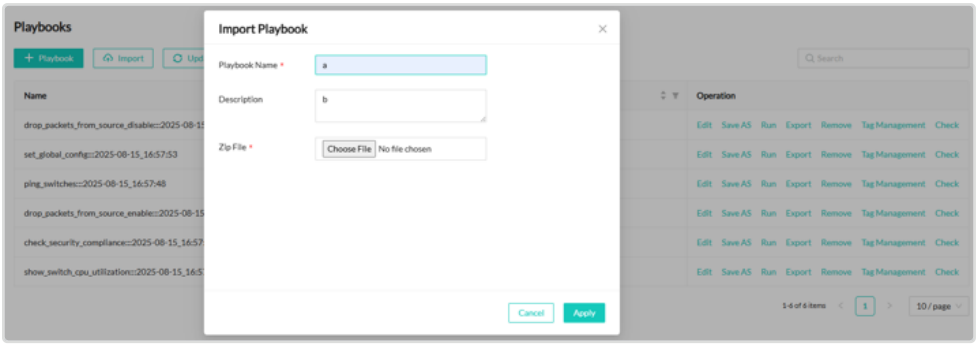
5. Click **Apply**.

Importing a Playbook

If you have an available Ansible playbook, you can import the Ansible playbook to AmpCon-DC. Follow these steps:

1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the “Playbooks” page, click **Import**.
3. Enter the playbook name and description (optional), and upload the playbook .zip file.

> **NOTE**
>
> The playbook **.zip** file needs to contain a playbook **.yml** file and a configuration **.conf** file (optional).

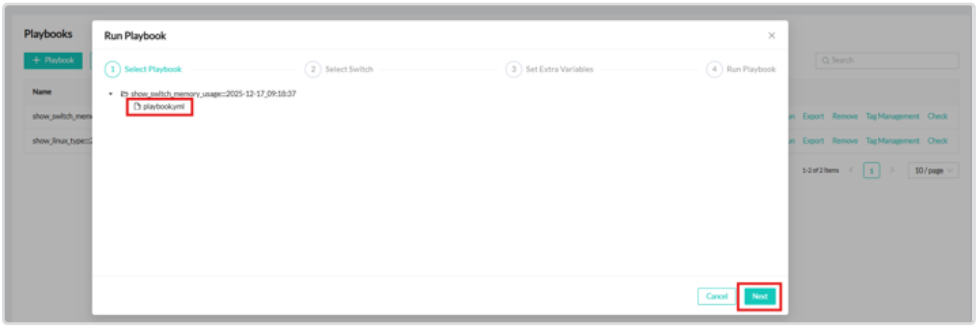


4. Click **Apply**.

Running a Playbook

After you write or import the Ansible playbook, run the playbook in the AmpCon-DC UI. Follow these steps:

1. Click **Maintain > Automation > Playbooks** from the navigation bar.
2. On the “Playbooks” page, locate a playbook, and then click **Run**.
3. Select the playbook.yml file, and then click **Next**.

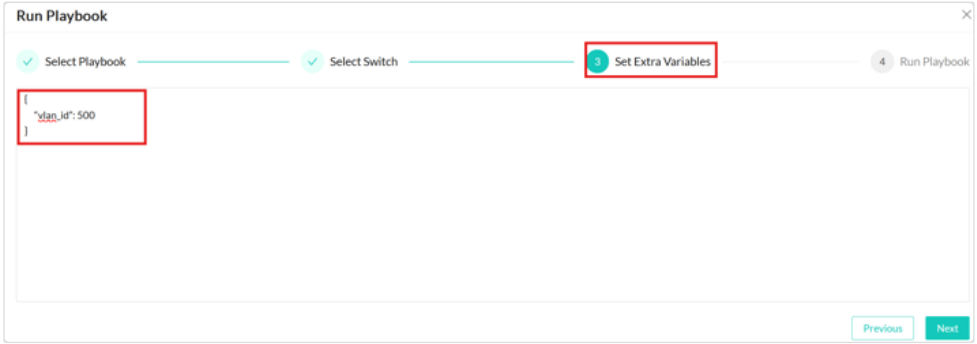


4. Select target switches to run the playbook by using the following ways:

> **NOTE**
>
> - If you select switches, groups, and other devices in the **Choose Switches**, **Choose Groups**, and **Choose Other Devices** tabs, the playbook will be run on all selected targets.
> - In addition to running Ansible playbooks on managed switches, you can add third-party Linux server devices and then run Ansible playbooks on these added devices.

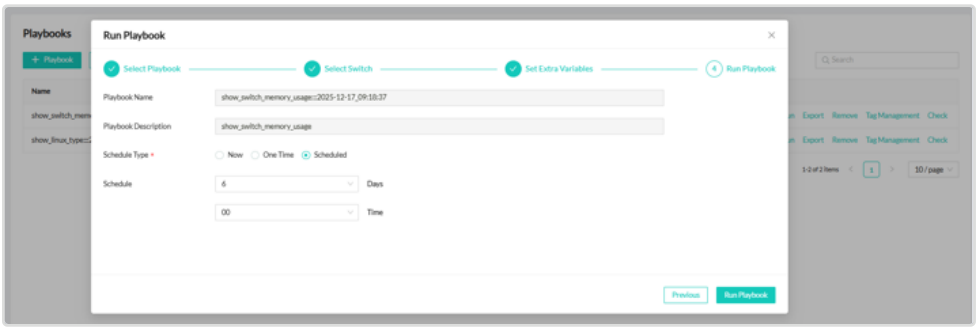
- In the **Select Switches** tab, select one or multiple switches.
- In the **Select Groups** tab, select one or multiple switch groups.
- In the **Select Other Devices** tab, select one or multiple devices that you added as described in Adding a Device.

5. Click **Next**.
6. If variables are specified in the playbook, enter variable values in JSON format, and then click **Next**.



7. Select the schedule type to run the playbook.

- **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.

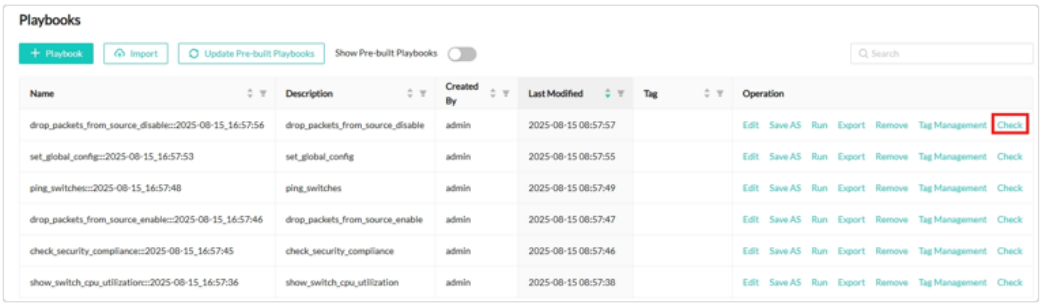


8. Click **Run Playbook**.

Optional Operations

Checking Syntax for a Playbook

On the “Playbooks” page, locate a playbook, and then click **Check**. A message pops up with the checking result.

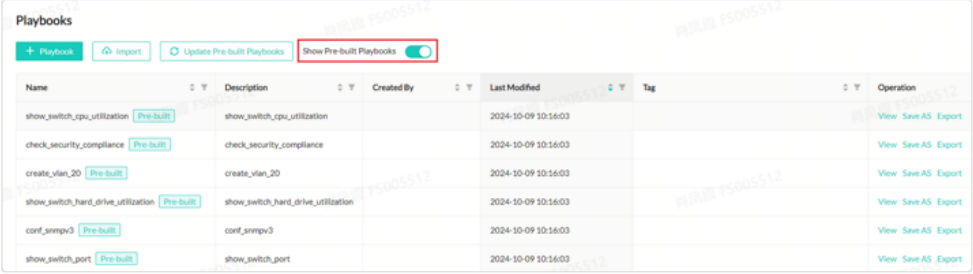


Using Pre-built Playbooks

AmpCon-DC provides multiple pre-built playbooks, which are hidden by default.

> **NOTE**
>
> Pre-built playbooks can’t be run directly. You need to click **Save As** to copy a pre-built playbook as a new playbook and then run the new playbook. You can’t edit or remove pre-built playbooks. And you can’t add tags or check syntax for pre-built playbooks.

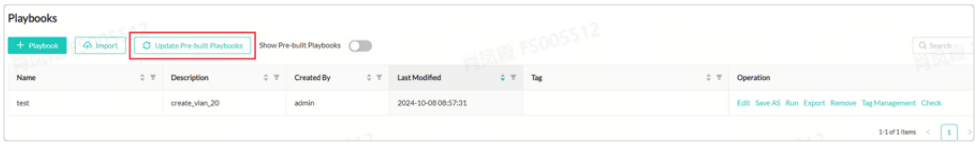
- To show the pre-built playbooks, click the **Show Pre-built Playbooks** toggle on the “Playbooks” page.



- To view a pre-built playbook, locate the playbook, and then click **View**.



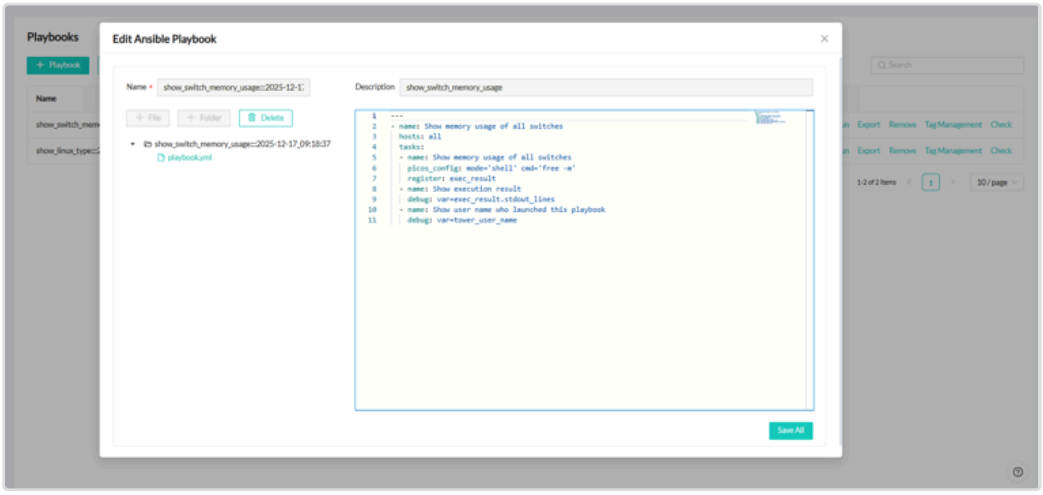
- To refresh the pre-built playbook list, click **Update Pre-built Playbooks**.



- To export a pre-built playbook, locate the playbook, and then click **Export**.

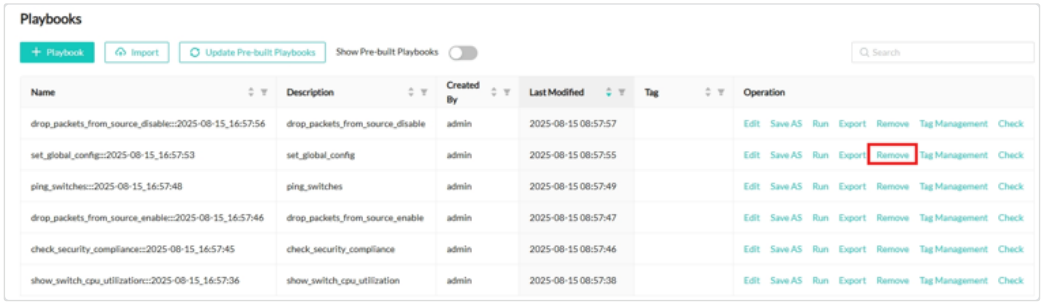
Editing a Playbook

On the “Playbooks” page, locate a playbook, and then click **Edit**. Modify the playbook contents as needed. You can also add or remove folders and files. Then, click **Save All**.



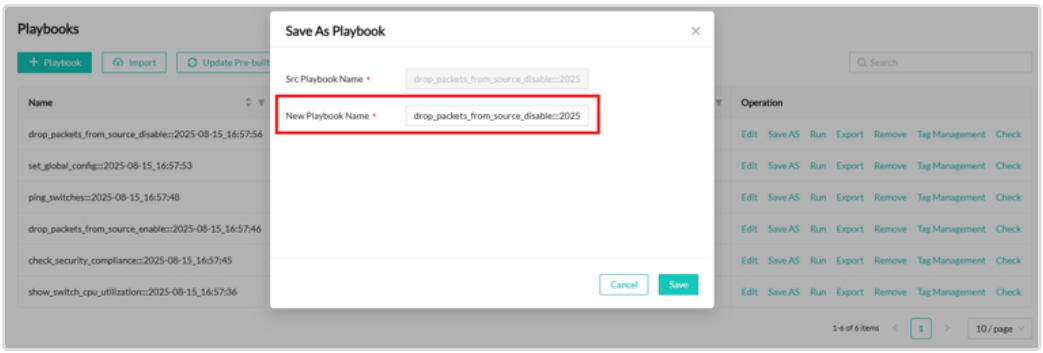
Deleting a Playbook

On the “Playbooks” page, locate a playbook, and then click **Remove**. Then, click **Yes** to confirm the deletion.



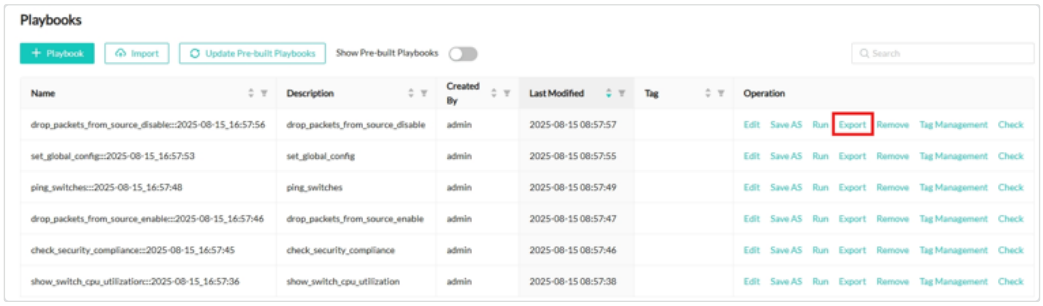
Copying a Playbook

On the “Playbooks” page, locate a playbook, and then click **Save As**. The new playbook has a default name, which you can modify as needed. Then, click **Save**.



Exporting a Playbook

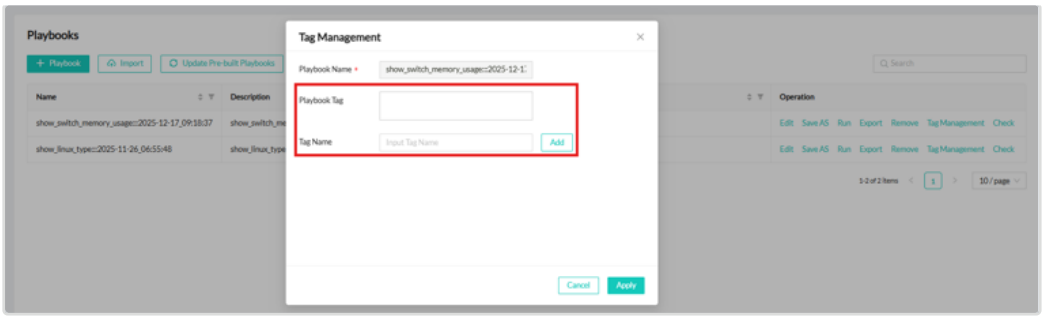
On the “Playbooks” page, locate a playbook, and then click **Export**.



Adding or removing Playbook Tags

On the “Playbooks” page, locate a playbook, and then click **Tag Management**. Enter the tag name in the **Tag Name** field, and then click **Add**.

You can remove a tag by clicking the removal icon.


Playbooks
Playbook
Import
Update Pre-built Playbooks
Search
Name
Description
Operation
show_switch_memory_usage:::2025-12-17_09:18:37
show_linux_type:::2025-11-26_06:55:48
Edit Save AS Run Export Remove Tag Management Check
1-2 of 2 items
10 / page
Tag Management
Playbook Name *
Playbook Tag
Tag Name
Input Tag Name
Add
Cancel
Apply

Managing Ansible Jobs

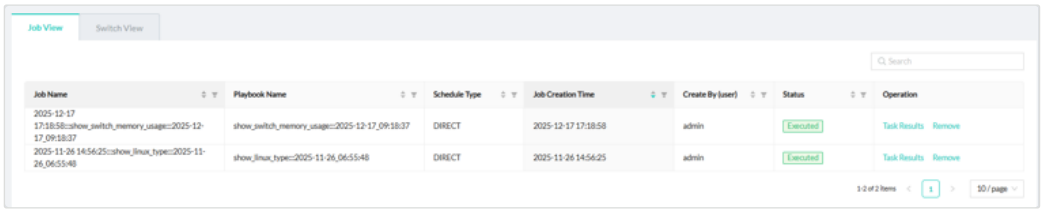
An Ansible job is a single execution of an Ansible playbook. On the “Ansible Jobs” page, you can view the list of Ansible jobs and the list of switches with Ansible jobs. You can also check the execution results and output of these jobs.

- Job View
  - Viewing Ansible Jobs
  - Checking Ansible Job Results and Output
  - Removing an Ansible Job
- Switch View
  - Viewing Switches with Ansible Jobs
  - Checking Ansible Job Results and Output

Job View

Viewing Ansible Jobs

Click **Maintain > Automation > Ansible Jobs** from the navigation bar. In the **Job View** tab, you can see the list of playbook execution jobs.



The **Schedule Type** column includes the following types:

- **DIRECT**

  Playbooks are executed with "Now".

- **ONCE**

  Playbooks are executed with "One Time".

- **SCHEDULED**

  Playbooks are executed with "Scheduled".

The **Status** column includes the following status:

- **IDLE**

  The playbook has not been executed. For example, after a playbook is created and before it’s executed, the status is IDLE.

> **NOTE**
>
> For Playbooks with the schedule type of "SCHEDULED", the status is changed to **IDLE** after the playbook execution is completed.

- **RUNNING**

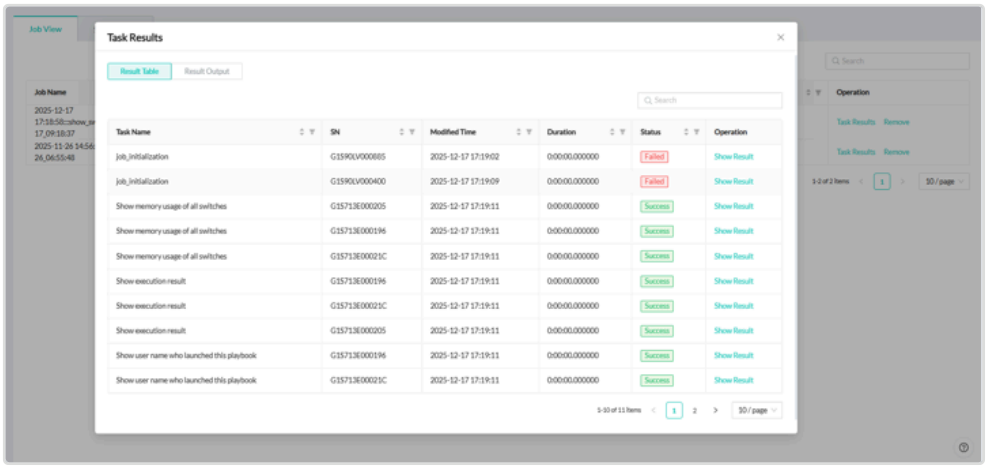
  The playbook is currently running.

- **EXECUTED**

  The playbook execution has been completed.

Checking Ansible Job Results and Output

1. In the **Job View** tab, locate a job, and then click **Task Results**. You can see the playbook execution result in the **Result Table** tab.

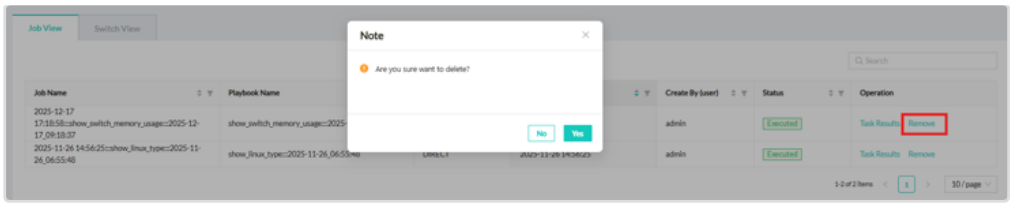


2. To view detailed result information, click **Show Result**.
3. To view the output of the playbook execution, click the **Result Output** tab.



Removing an Ansible Job

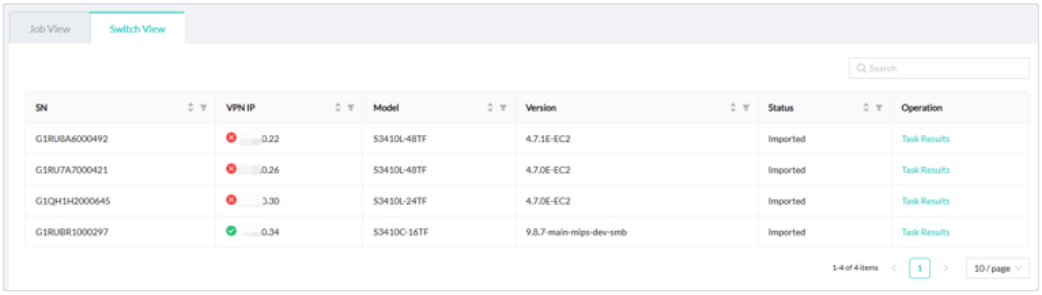
1. In the **Job View** tab, locate a job, and then click **Remove**.
2. Click **Yes** to confirm the deletion.



Switch View

Viewing Switches with Ansible Jobs

In the **Switch View** tab, you can see the list of switches that have playbook execution jobs.



Checking Ansible Job Results and Output

1. In the **Switch View** tab, locate a switch, and then click **Task Results**.



2. To view detailed result information, click **Show Result**.
3. To view the output of the playbook execution, click the **Result Output** tab.

Viewing Playbook Scheduling

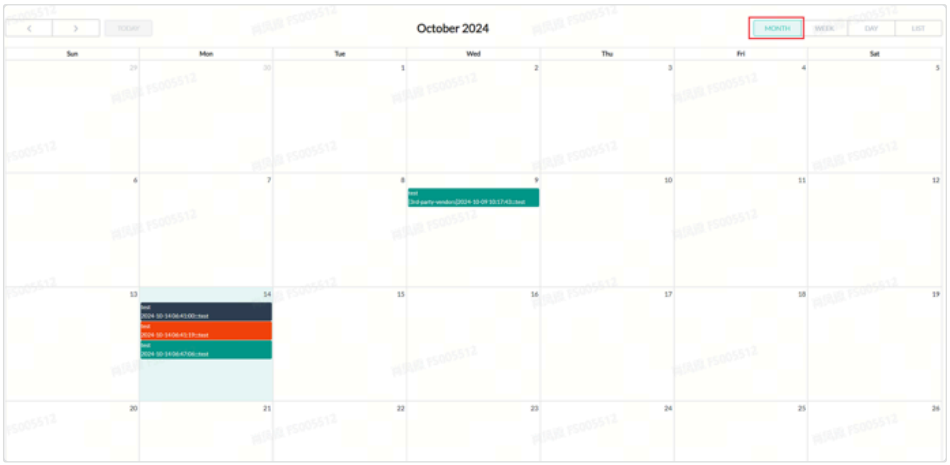
On the “Scheduler” page, you can view executed playbooks based on months, weeks, or days. You can also view executed playbooks in the list format.

Procedure

1. Click **Maintain > Automation > Scheduler** in the AmpCon-DC UI.
2. View executed playbooks by using the following ways:

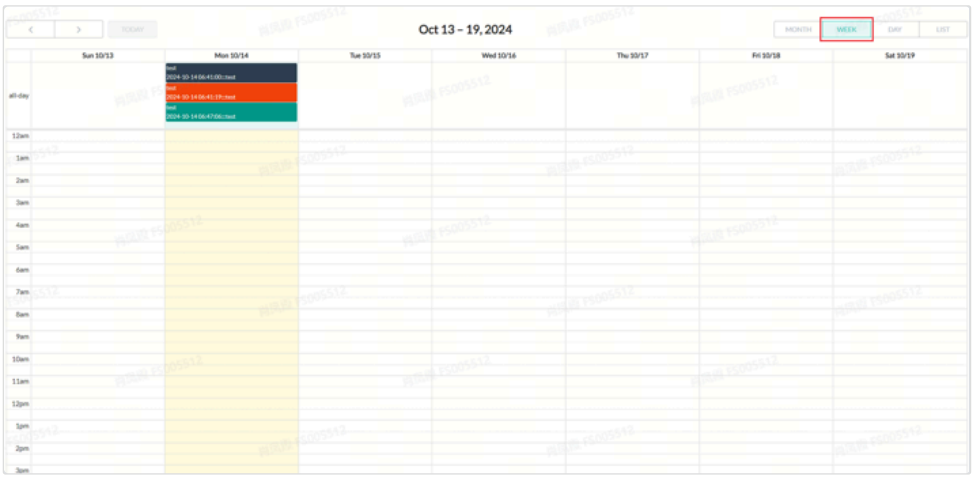
- To view executed playbooks each month, click **MONTH**.

  Click **<** to view playbooks executed in the previous month. Click **>** to view playbooks executed in the next month.



- To view executed playbooks each week, click **WEEK**.

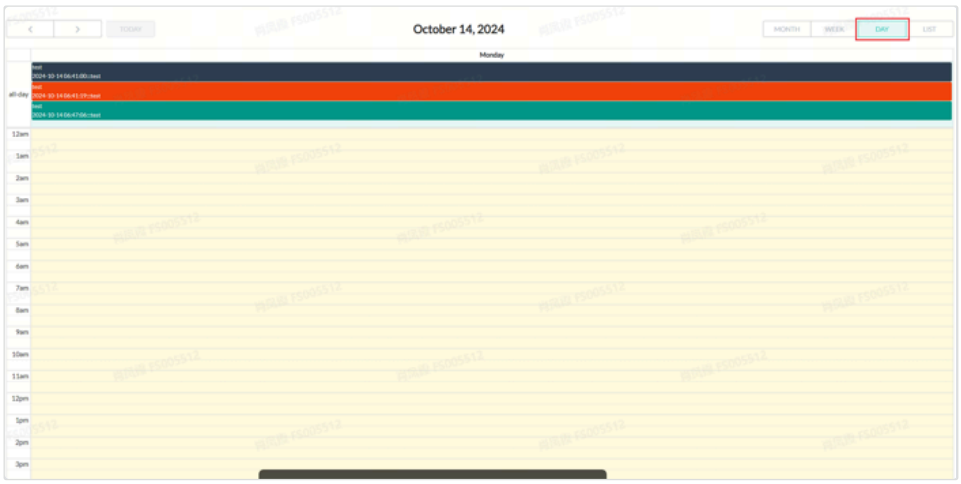
  Click **<** to view playbooks executed in the previous week. Click **>** to view playbooks executed in the next week.



- To view executed playbooks each day, click **DAY**.

Click **<** to view playbooks executed on the previous day. Click **>** to view playbooks executed on the next day.

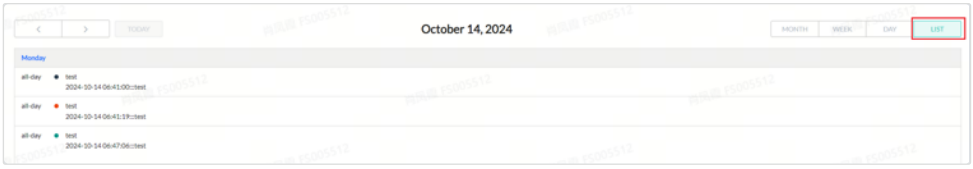
Click **Today** to view playbooks executed today.



- To view executed playbooks in the list format, click **LIST**.

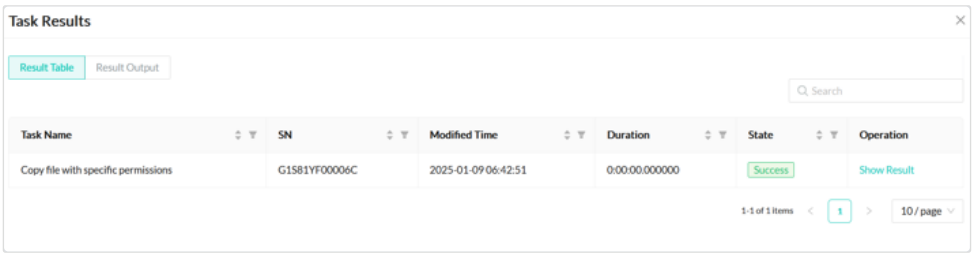
  Click **<** to view playbooks executed on the previous day. Click **>** to view playbooks executed on the next day.

  Click **Today** to view playbooks executed today.



3. Optional: Click a playbook, and then you can see the playbook execution result and output.

   In the **Result Table** tab, you can see the playbook execution result. To view detailed result information, click **Show Result**.



   In the **Result Output** tab, you can see the playbook execution output.


Job View
Switch
Job Name
2024-10-14 06:47:06::test
2024-10-14 06:41:19::test
2024-10-14 06:41:00::test
[3rd-party-vendors]2024-10-0
Task Results
Result Table
Result Output
JOB NAME [[3rd-party-vendors]2024-10-09 10:17:43::test]
TASK [Transfer the script] ********
SN: www, Status: FAILED
details:
[
"_ansible_no_log": null,
"changed": false,
"checksum": "60fe92d4fd138e1b7f30e538fd782a51e926854c",
"diff": [],
"invocation": {
"module_args": {
"_original_basename": "vlan20.conf",
"attributes": null,

Troubleshooting

If the playbook fails to be run on switches or Linux servers, refer to the following reasons and solutions:

Playbook Syntax Issues
- Symptom
- Solutions

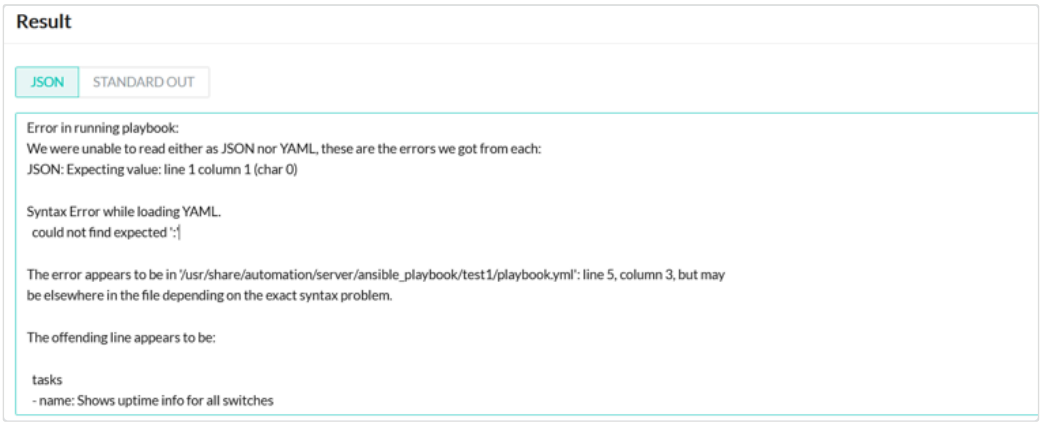
Connection Issues
- Symptom
- Solutions

Playbook Syntax Issues

If the playbook syntax is wrong, the playbook can't be run on specified devices.

Symptom

When you check the playbook execution result in the AmpCon-DC UI, you can see the error log as follows:



Solutions

- For playbooks run on switches, check as follows:
  - Check whether you follow the syntax as described in Examples for Ansible Playbooks.
  - Check whether the commands included in each playbook are correct.
  - When you run a playbook with variables designated, check whether you have set the variable values in JSON format as described in **Step 6** of Running a Playbook.
  - When you run a playbook with a configuration file (**.conf**) specified, check whether you have clicked **Add File** to add the configuration file.
- For playbooks run on added Linux servers, check whether you follow the playbook syntax as described in Using Ansible Playbooks.

Connection Issues

If the AmpCon-DC server fails to access the switches or added Linux servers, the playbook can't be run on these devices.

Symptom

When checking the playbook execution result in the AmpCon-DC UI, you can see the error log as follows:



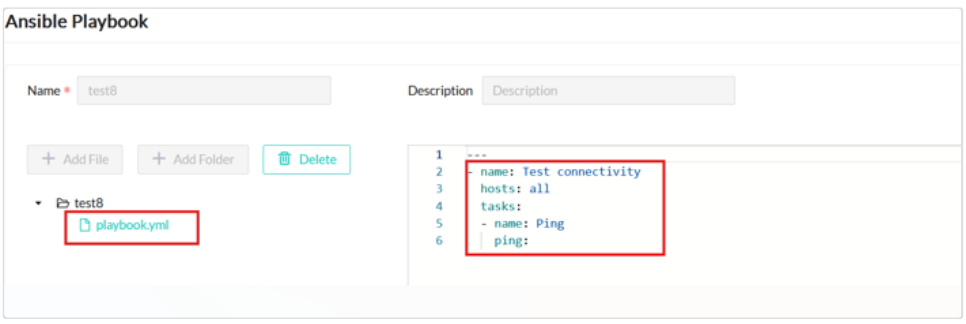
Solutions

Test the connectivity between the problematic switches (or Linux servers) and the AmpCon-DC server by running the following Ansible playbook:

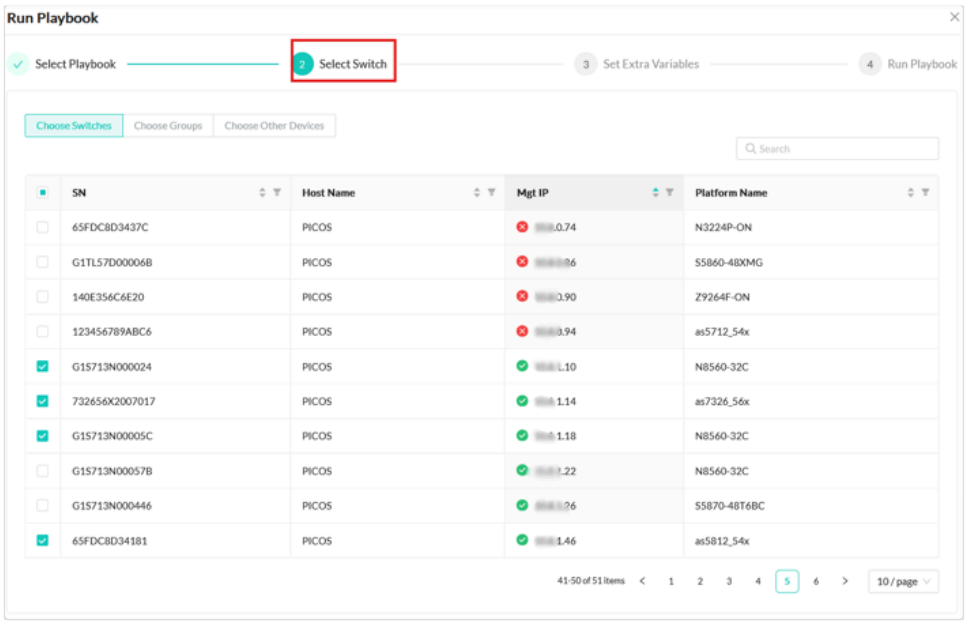
```yaml
---
- name: Test connectivity
  hosts: all
  tasks:
  - name: Ping
    ping:
```

You can write and run the playbook in the AmpCon-DC UI. Follow these steps:

1. Write a playbook.

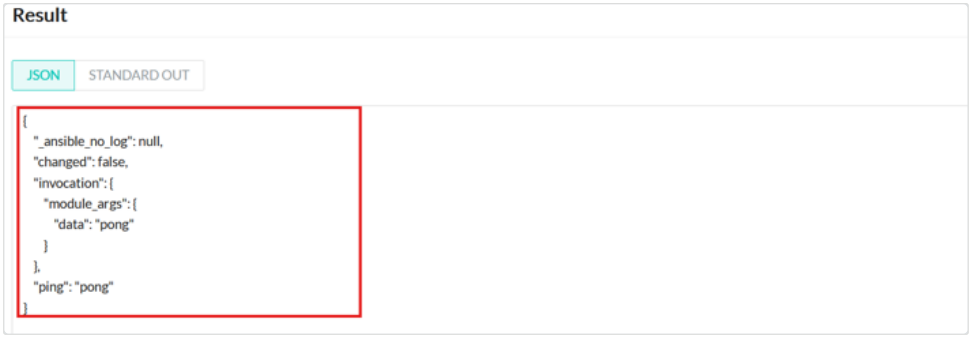


2. Run the playbook on problematic switches or Linux servers.

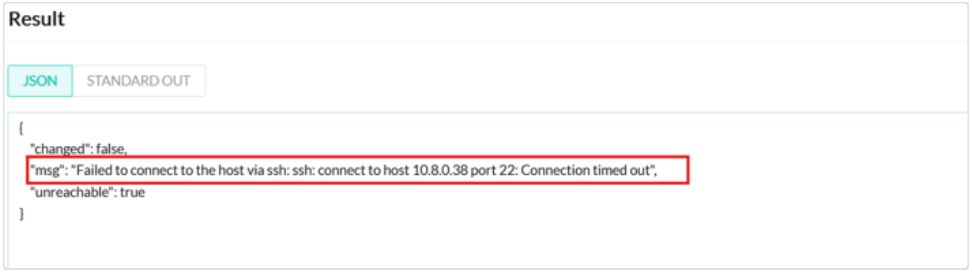


3. Check the playbook execution result in the AmpCon-DC UI to see whether the AmpCon-DC server can access the problematic switches or Linux servers.

- If the AmpCon-DC server can access the problematic switches or Linux servers, the result is as follows:



- If the AmpCon-DC server can't access the problematic switches or Linux servers, the result is as follows:



In this case, check whether the prerequisites for running playbooks are met. For more information, see Running Playbooks - Prerequisites.

Monitoring and Alerting

AmpCon-DC provides a unified view and real-time telemetry data of managed switches, added Linux servers, and Network Interface Cards (NICs), helping you eliminate the time of juggling multiple monitoring tools and gain comprehensive network insights.

AmpCon-DC analyzes telemetry data and issues immediate alerts when a device failure or a performance shift is detected, helping you diagnose root causes and resolve problems quickly and minimize downtime.

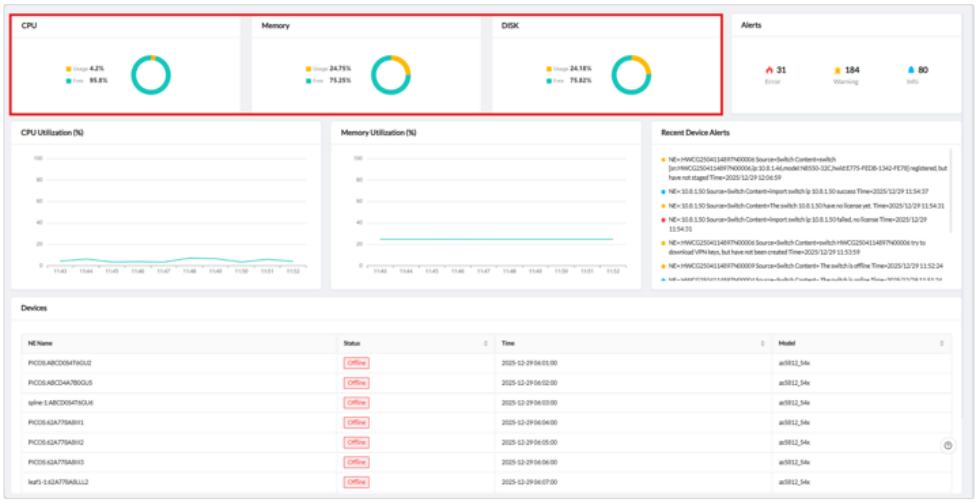
See the following child topics:

- System Overview
- Switch Overview
- Telemetry
- Queue Congestion Visualization
- Topology
- NICs
- Splunk Integration
- Alerts

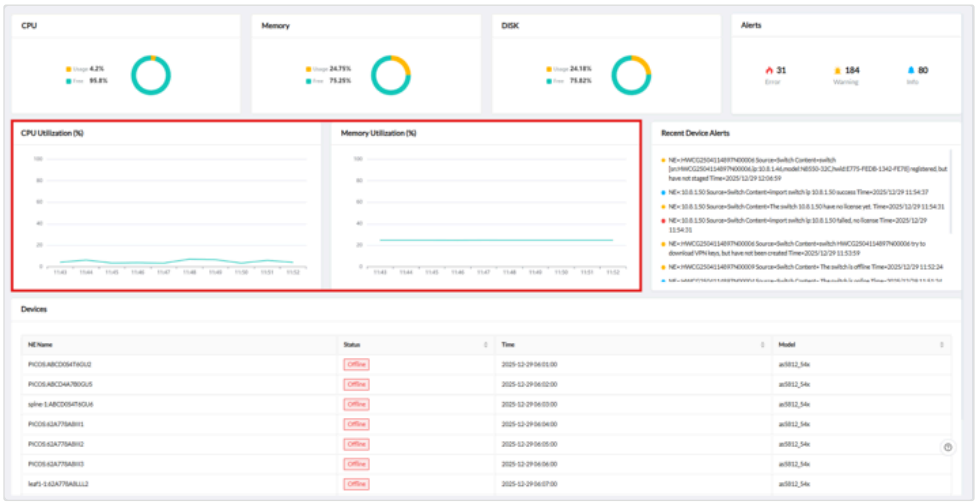
System Overview

In the AmpCon-DC UI, click **Dashboard > System Overview**. On the “System Overview” page, you can check managed switches and the health of the AmpCon-DC server.

- In the **CPU**, **MEM**, and **DISK** sections, you can see the status of the AmpCon-DC server, including CPU, memory, and hard disk.



- In the **CPU Utilization** and **Memory Utilization** sections, you can see the historical utilization curves for CPU and memory in the AmpCon-DC server.

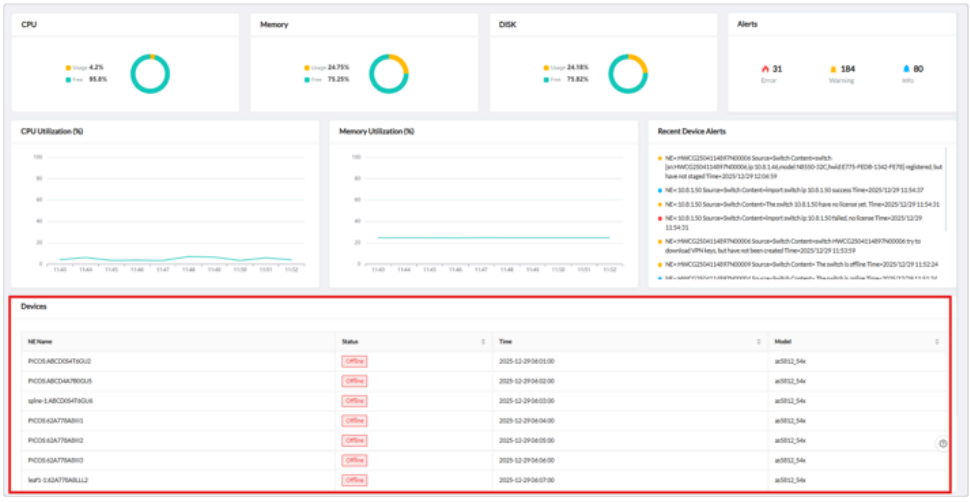


- In the **Devices** section, you can see information about managed switches.

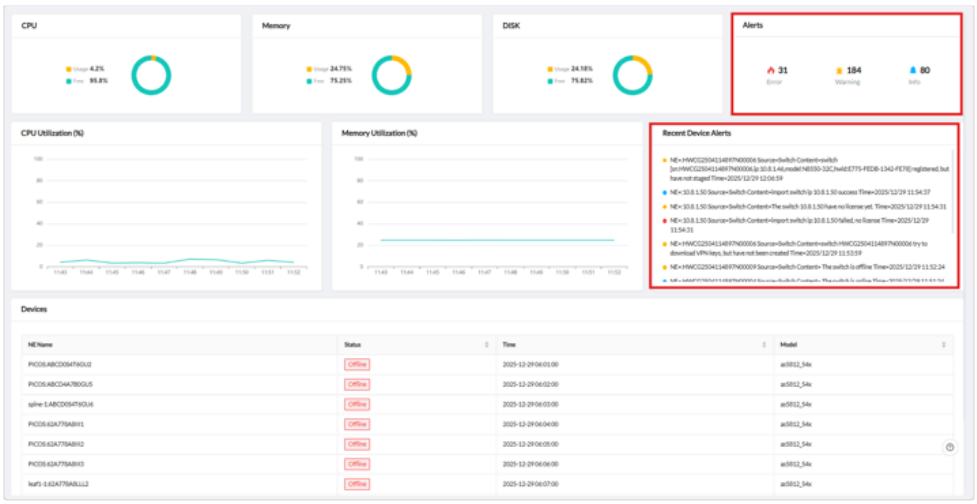
Table 1. Switch Metrics

Metric	Description

NE Name	The combination of the switch's hostname and the SN/Service Tag. **Example**: If a switch's hostname is PICOS and the SN/Service Tag is G1S713E00021C, then the NE name is PICOS:G1S713E00021C.
Status	The status of the switch. • The **Online** status means that the switch can connect with the AmpCon-DC server. • The **Offline** status means that the switch can't connect with the AmpCon-DC server.
Time	The time of the most recent change of the **Status** value.
Model	The model of the switch.



- In the **Recent Device Alerts** and **Alerts** sections, you can see recent switch alerts and the numbers for different types of switch alerts.


CPU
Usage 4.2%
Free 95.8%
Memory
Usage 24.75%
Free 75.25%
DISK
Usage 24.18%
Free 75.82%
Alerts
31
Error
184
Warning
80
Info
CPU Utilization (%)
Memory Utilization (%)
Recent Device Alerts
Devices
NE Name
Status
Time
Model
Offline
2025-12-29 06:01:00
2025-12-29 06:02:00
2025-12-29 06:03:00
2025-12-29 06:04:00
2025-12-29 06:05:00
2025-12-29 06:06:00
2025-12-29 06:07:00
as5812_54x

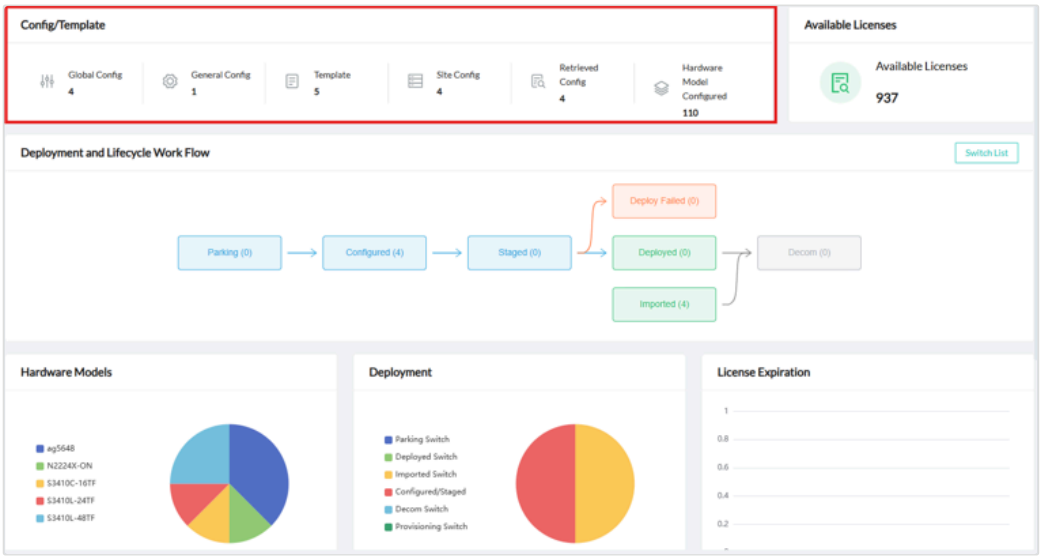
Switch Overview

In the AmpCon-DC UI, click **Dashboard > Switch Overview**. On the “Switch Overview” page, check the following information for managed switches:

- Checking Configurations or Templates
- Checking Switches
  - Checking Lifecycle Workflow
  - Checking the Proportions of Switches in Each Lifecycle State
  - Checking Switch Models
- Checking Licenses
  - Checking Available License Numbers
  - Checking License Expiration Dates
  - Checking License Usage
- Checking Tasks
  - Checking All Switch Activities
  - Checking System Tasks
  - Checking Automation Jobs

Checking Configurations or Templates

In the **Config/Template** section, you can see the total numbers for different types of switch configurations and templates.



Click the number for one specific type. You are redirected to the related page in the **Service** menu:

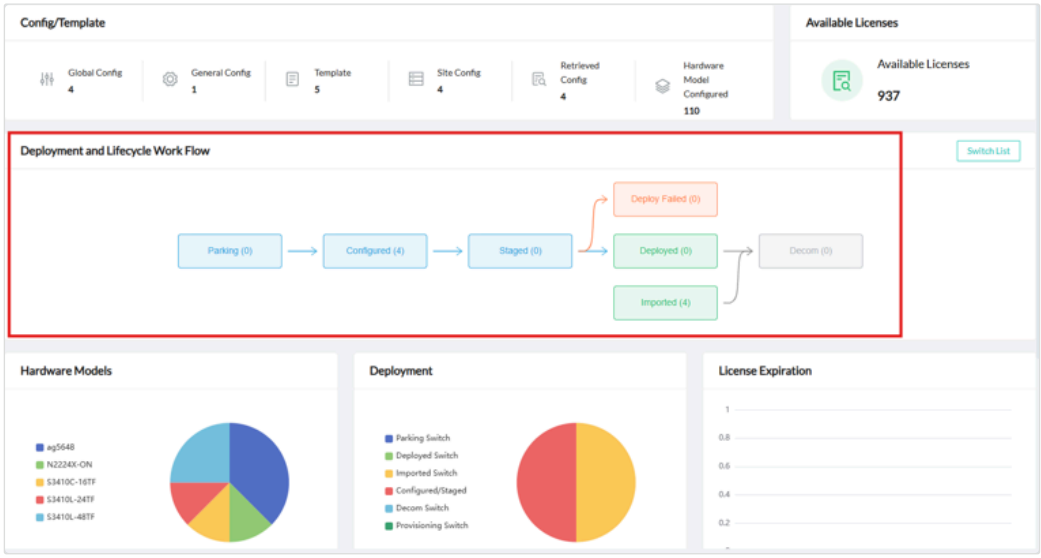
- Click **Global Config** to go to the **Global Configuration** tab of the “Device Profiles” page.
- Click **General Config** to go to the **Push Config** tab of the “Config Templates” page.
- Click **Template** to go to the **Template List** of the “Config Templates” page.
- Click **Site Config** to go to the **Switch Configuration** tab of the “Device Profiles” page.

- Click **Retrieved Config** to go to the **Config Backup** tab of the “Config Templates” page.
- Click **Hardware Model Configured** to go to the **Switch Model** tab of the “Device Profiles” page.

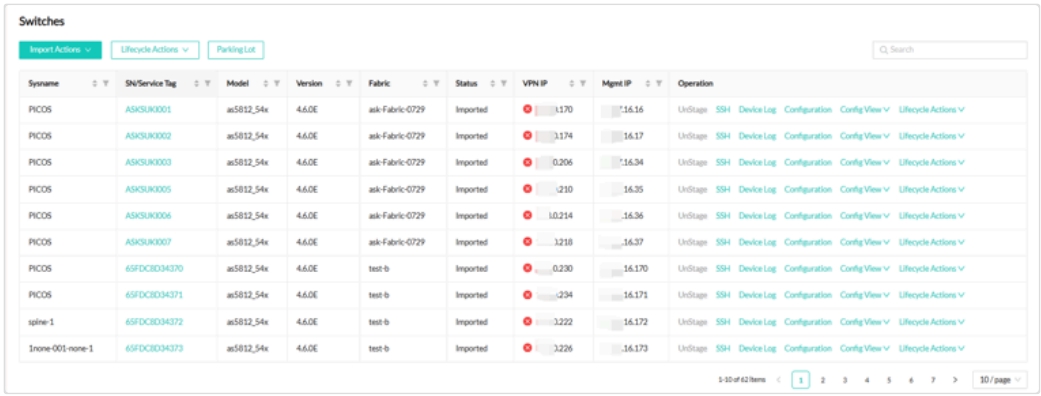
Checking Switches

Checking Lifecycle Workflow

In the **Deployment and Lifecycle Work Flow** section, you can see the lifecycle transition process of switches and the total number of each state.

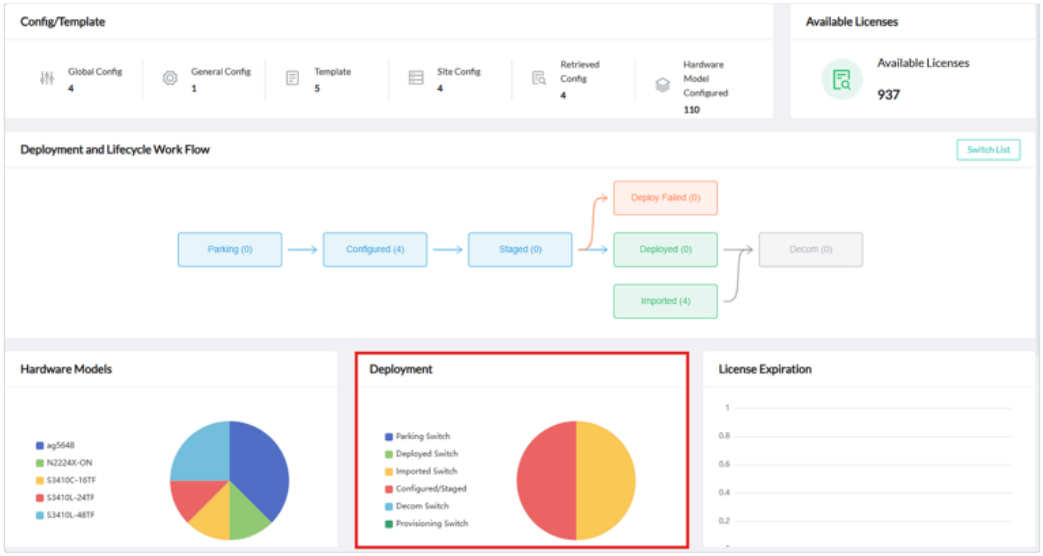


Click **Switch List**. You can check all managed switches on the “Switches” page.



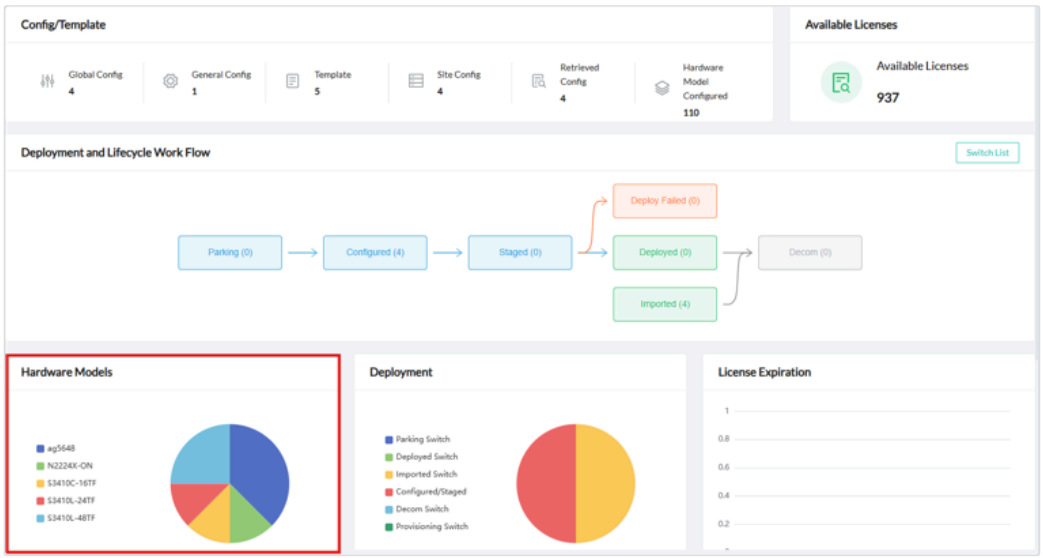
Checking the Proportions of Switches in Each Lifecycle State

In the **Deployment** section, you can see the proportion of switches in each lifecycle state.



Checking Switch Models

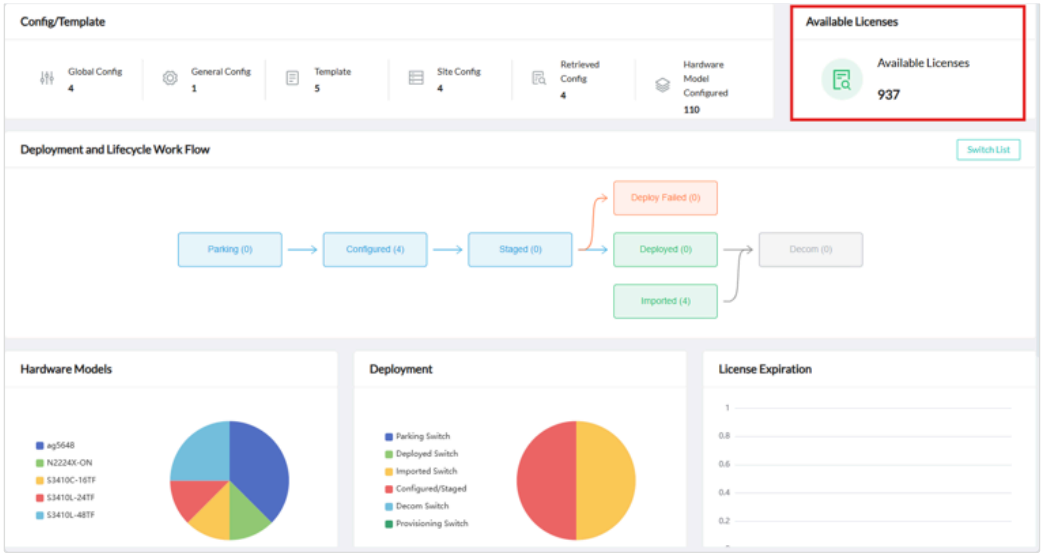
In the **Hardware Models** section, you can see the total numbers of switch models and their proportions.



Checking Licenses

Checking Available License Numbers

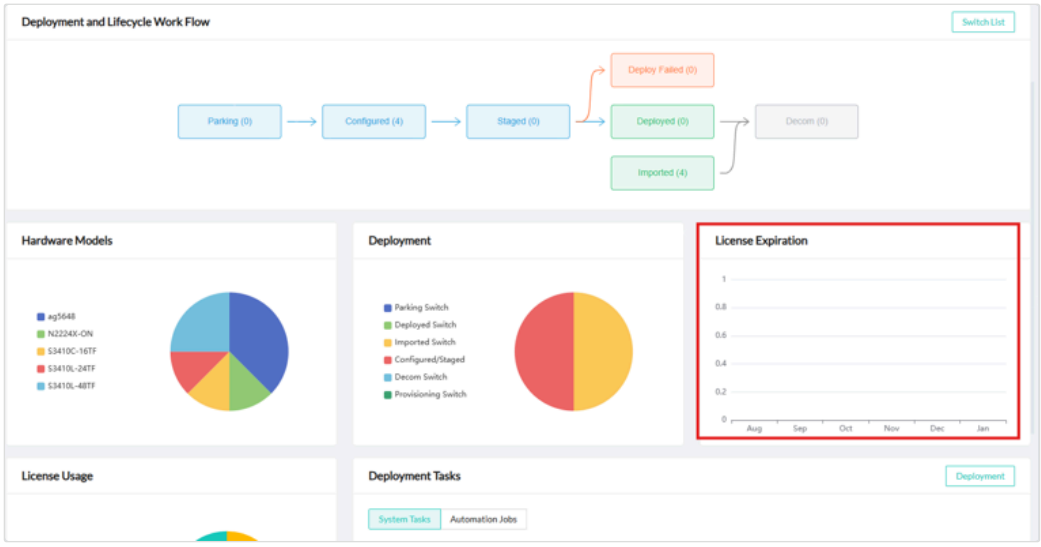
In the **Available Licenses** section, you can see the currently available license number.



Click **Available Licenses**, and then you are redirected to the License Portal, where you can see more details about available licenses.

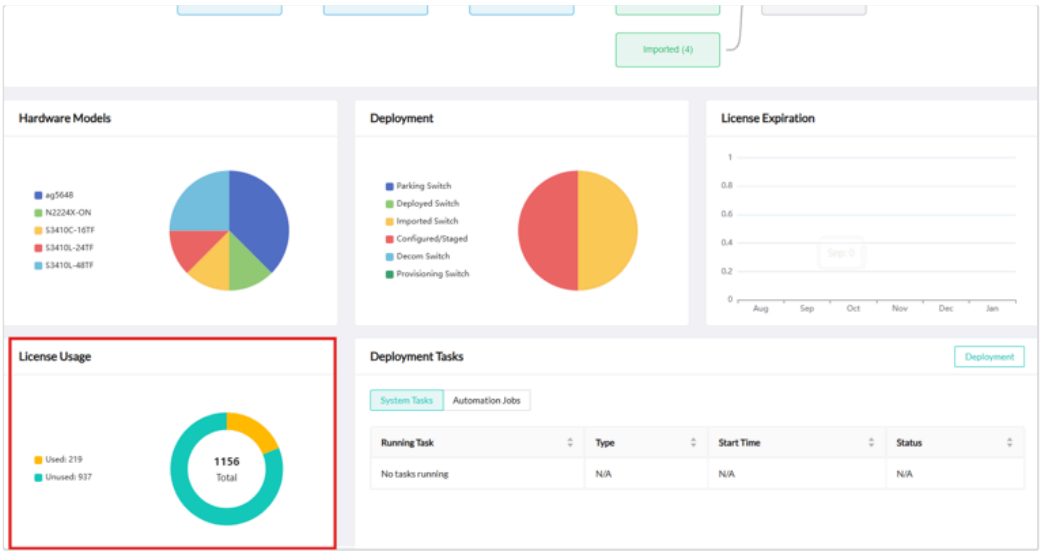
Checking License Expiration Dates

In the **License Expiration** section, you can see the total number of devices that will expire in each month over the next six months.



Checking License Usage

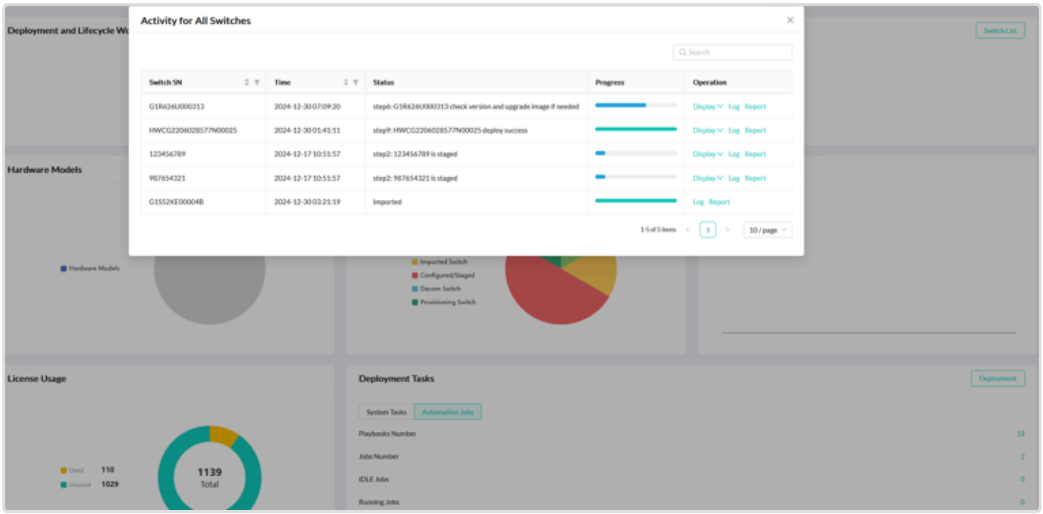
In the **License Usage** section, you can see the license usage information.



Checking Tasks

Checking All Switch Activities

In the **Deployment Tasks** section, click **Deployment**. You can see activities for all switches and each activity progress.

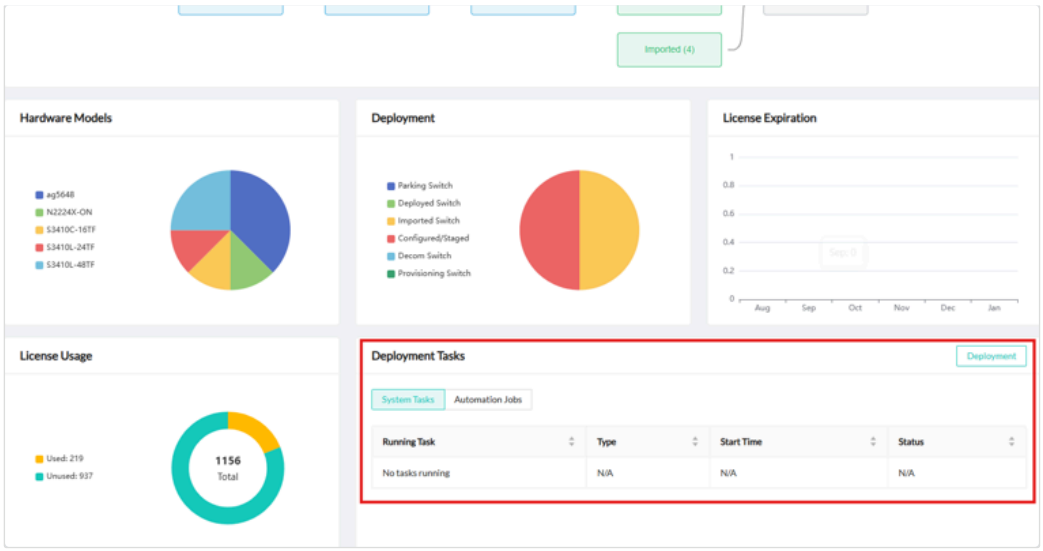


In the pop-up window, you can perform the following actions:

- Click **Display** to see the initial configurations during the switch deployment process. This button is not available for imported switches.
- Click **Log** to see the log information.
- Click **Report** to see the corresponding report.

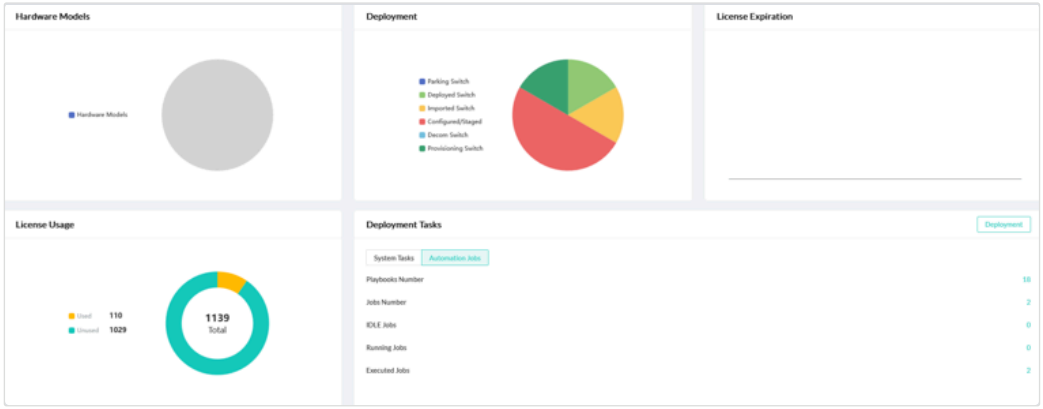
Checking System Tasks

In the **System Tasks** tab of the **Deployment Tasks** section, you can see the total numbers for different types of running tasks.



Checking Automation Jobs

In the **Automation Jobs** tab of the **Deployment Tasks** section, you can see the total numbers for different types of automation jobs.



Click the number for one specific type. You are redirected to the related page:

- Click **Playbooks Number** to go to the “Playbooks” page.
- Click **Jobs Number** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **IDLE Jobs** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **Running Jobs** to go to the **Job View** section of the “Ansible Jobs” page.
- Click **Executed Jobs** to go to the **Job View** section of the “Ansible Jobs” page.

Telemetry

To ensure that the network is healthy and devices are working well, you need to continuously monitor and validate the operational state of your network and devices. AmpCon-DC uses the telemetry technology to automatically collect real-time or historical metric data from managed switches.

By using AmpCon-DC, you can view multi-dimensional telemetry data of all managed switches in a centralized user interface, gain detailed insights into network performance and device health, and proactively troubleshoot and optimize your network performance.

The following scenarios are examples of using the telemetry data:

- **Monitor your network comprehensively with the telemetry data**

  You can have an overall understanding about the network running status by checking telemetry metrics like routing neighbors, switch resource utilization, port counts, and Layer 2 and Layer 3 forwarding tables.

- **Track real-time performance metrics from various switches**

  You can monitor performance-related telemetry metrics for all managed switches, such as port traffic, bandwidth utilization, and packet loss rate.

- **Optimize network performance based on the telemetry data**

  You can better distribute the load based on the routing neighbor information, avoid excessive load on certain neighbors, and improve the overall network performance.

- **Decrease time and efforts on locating and resolving network problems**

  You can get early warnings of network failures, be notified when equipment failures and performance anomalies happen, and quickly troubleshoot and address network issues.

See the following child topics:

- Telemetry Data of a Switch
- Performance Statistics
  - Switch Performance Statistics
  - NIC Performance Statistics
- RoCE Counters
  - RoCE Data on Switches and NICs
  - Buffer

- Dynamic Load Balancing (DLB)

Telemetry Data of a Switch

Click **Device > Switches** in the AmpCon-DC UI, and click a specific switch SN or service tag in the switch list. Then, you can see the following telemetry data related to the switch:

- Limitations
- Prerequisites
- Telemetry Data
  - Device Information
  - Switch Overview
  - Device Overview
  - Port Overview
  - Module Overview
  - BGP
  - OSPF
  - MAC
  - ARP
  - AI
  - IP Route
  - MLAG
- Filtering Telemetry Data

Limitations

Read the following limitations, which are caused by known bugs of related PicOS versions:

- For N9550-64D switches with PicOS 4.5.3.2 installed, AmpCon-DC can't properly collect BGP, MLAG, ARP, and AI related telemetry data from these switches.
- For N9600-64OD switches with PicOS 4.5.3.2 installed, AmpCon-DC can't properly collect port and IP route related telemetry data from these switches.
- For N8610-32D switches with PicOS 4.5.6E installed, AmpCon-DC might fail to retrieve telemetry data from these switches.

Prerequisites

Real-time telemetry data can be displayed in the AmpCon-DC UI only when the following prerequisites are met:

- The switches to be monitored are connected to the AmpCon-DC server. Click **Device > Switches** from the navigation bar, and then check the **VPN IP** column
  - ✔ means the switch is connected to the AmpCon-DC server.
  - x means the switch is not connected to the AmpCon-DC server.

- Google Remote Procedure Call (gRPC) and Link Layer Discovery Protocol (LLDP) are enabled on the switches to be monitored. By default, gRPC and LLDP are enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

Telemetry Data

Device Information

In the **Device Information** section, you can see the following information:

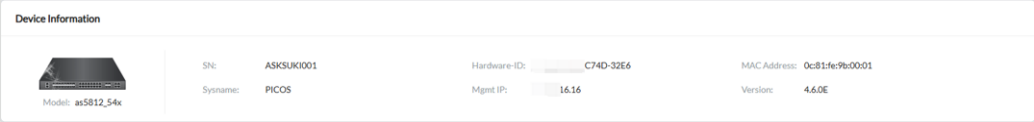
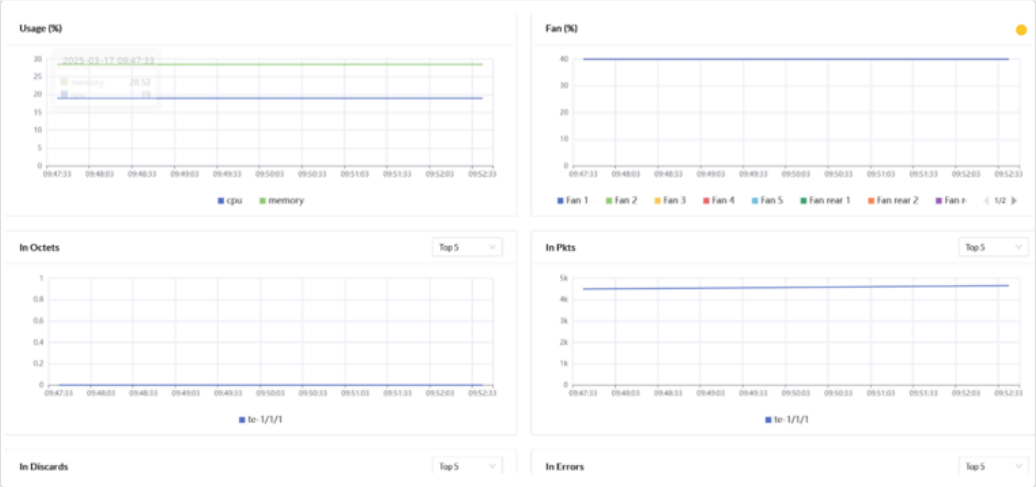


Table 1. Device Information

Metric	Description
Model	The model of the switch.
SN	The serial number of the switch.
Hardware-ID	The hardware ID of the switch.
MAC Address	The MAC address of the switch.
Sysname	The hostname of the switch.
Mgmt IP	The management IP address of the switch. **Mgmt IP** is used to connect to AmpCon-DC.
Version	The PicOS version on the switch.

Switch Overview

Click the **Switch Overview** tab. Then, you can see the following line charts:



> **NOTE**
>
> The **Usage** and **Fan** sections are always displayed and can't be hidden. You can display or hide other metrics by clicking the setting icon and selecting the metrics to be monitored.

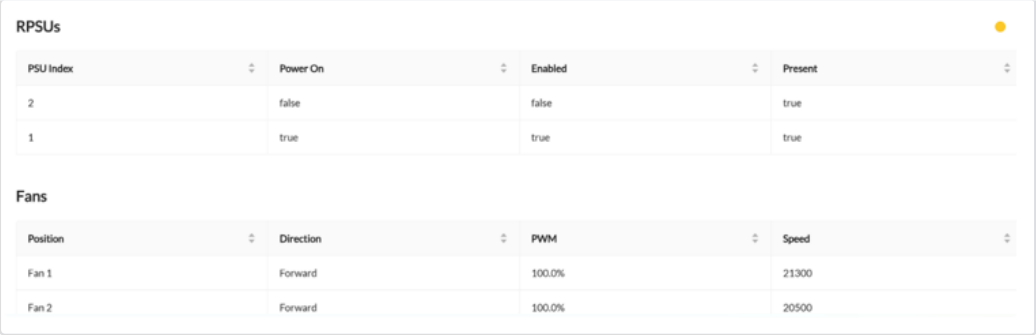
Table 2. Switch Overview Metrics

Metric	Description
Usage	The CPU and memory usage of the switch. It's measured in percentage.
Fan	The proportion of the fan's PWM to the total width.
In Octets	The number of octets (8-bit bytes) received by the switch port.
In Pkts	The number of incoming packets received by the switch port.
In Discards	The number of incoming packets that the switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by the switch port.
In Fcs Errors	The number of incoming packets that fail the Frame Check Sequence (FCS) validation.

Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
Out Pkts	The number of packets transmitted out of the switch port.
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops).
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors.
Out Bits Rate	The rate at which bits are transmitted from the switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by the switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from the switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by the switch port. It's measured in Packets Per Second (pps).
Tx Power	The amount of optical power emitted by the optical module connected to the switch port. It's measured in dBm.
Rx Power	The amount of optical power received by the optical module connected to the switch port. It's measured in dBm.
Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).

Device Overview

Click the **Device Overview** tab. Then, you can see the following tables:



- **Redundant Power Supply Units (RPSUs)**

  Table 3. RPSU Metrics

Metric	Description
PSU Index	The index of the Power Supply Unit (PSU).
Power on	Whether the PSU is powered on.
Enabled	Whether the PSU is activated or turned on.
Present	Whether the PSU is properly plugged.

- **Fans**

  Table 4. Fan Metrics

Metric	Description
Position	The position of the fan.
Direction	The direction of the wind, forward or back.
PWM	The proportion of the fan's PWM to the total width.
Speed	The fan speed.

Port Overview

Click the **Port Overview** tab. Then, you can see the following table:

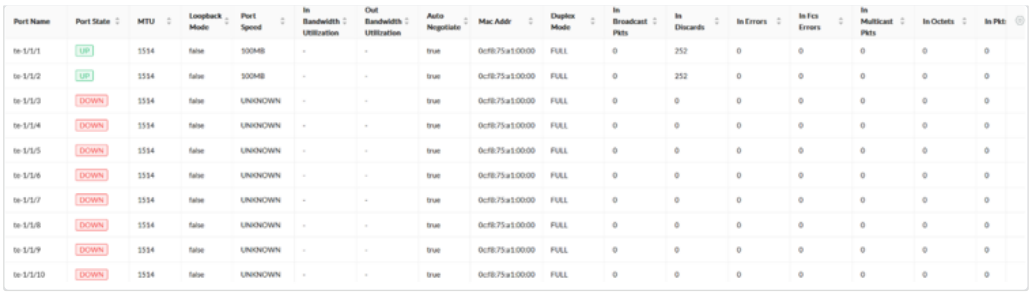


Table 5. Port Overview Metrics

Metric	Description
Port Name	The name of the switch port.
Port State	The state of the switch port.
MTU	The largest size of a data packet that can be transmitted over a network without being fragmented. It's measured in bytes.
Loopback Mode	Whether the loopback mode is enabled on this port. In loopback mode, the switch port sends data packets that are then routed back to itself. You can enable this mode to verify whether data can be sent or received as expected without involving external networks.
Port Speed	The maximum data transfer rate that the port can support.
In Bandwidth Utilization	The percentage of the inbound bandwidth that is being used on the port.
Out Bandwidth Utilization	The percentage of the outbound bandwidth that is being used on the port.
Auto Negotiate	Whether the Auto Negotiate feature on the port is enabled. Auto Negotiate means the process to automatically negotiate and select the optimal operating parameters, such as the speed and duplex mode.
Mac Addr	The MAC address of the switch port connecting to this switch port.

Duplex Mode	Whether data can flow in one direction (half duplex) at a time or both directions (full duplex) simultaneously.
In Broadcast Pkts	The number of broadcast packets received by the port.
In Discards	The number of incoming packets that the switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by the switch port.
In Fcs Errors	The number of incoming packets that fail the Frame Check Sequence (FCS) validation.
In Multicast Pkts	The number of multicast packets received by the switch port.
In Octets	The number of octets (8-bit bytes) received by the switch port.
In Pkts	The number of incoming packets received by the switch port.
In Unicast Pkts	The number of unknown unicast packets received by the switch port.
Out Broadcast Pkts	The number of broadcast packets sent by the switch port.
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops).
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors.
Out Multicast Pkts	The number of multicast packets sent by the switch port.
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port.
Out Pkts	The number of packets transmitted out of the switch port.

Out Unicast Pkts	The number of unknown unicast packets sent by the switch port.
In Oversize Frames	The number of oversize frames received by a switch port. Oversize frames mean frames that exceed the typical maximum transmission unit (MTU) size.
In Undersize Frames	The number of undersize frames received by a switch port. Undersize frames mean frames with a length less than 64 bytes and a correct checksum.
Out Bits Rate	The rate at which bits are transmitted from the switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by the switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from the switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by the switch port. It's measured in Packets Per Second (pps).
In Frames 64 Octets	The number of 64-byte frame packets received by the switch port.
In Frames 65-127 Octets	The number of frame packets between 65 and 127 bytes received by the switch port.
In Frames 128-255 Octets	The number of frame packets between 128 and 255 bytes received by the switch port.
In Frames 256-511 Octets	The number of frame packets between 256 and 511 bytes received by the switch port.
In Frames 512-1023 Octets	The number of frame packets between 512 and 1023 bytes received by the switch port.
In Frames 1024-1518	The number of frame packets between 1024 and 1518 bytes received by the switch port.

Octets	

Module Overview

Click the **Module Overview** tab. Then, you can view the monitoring data of optical modules inserted to the switch.

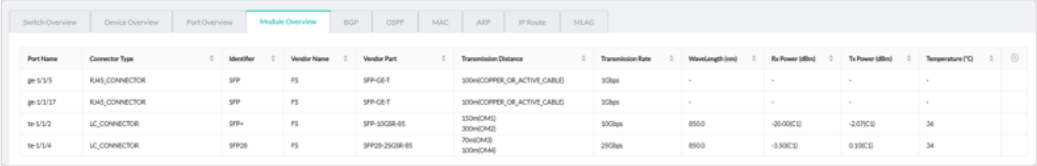


Table 6. Module Metrics

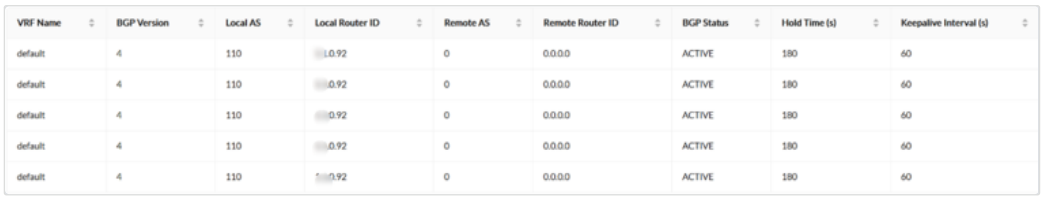
Metric	Description
Port Name	The name of the switch port connected with the optical module.
Connector Type	The type of the connector used by the optical module.
Identifier	The form factor of the optical module.
Vendor Name	The manufacturer of the optical module.
Vendor Part	The model name of the optical module.
Transmission Distance	The maximum distance over which an optical signal can be transmitted effectively through the module.
Transmission Rate	The speed at which data can be transmitted through the module. It's measured in gigabits per second (Gbps).
WaveLength (nm)	The distance between two corresponding points on an optical wave, typically measured from crest to crest (or trough to trough). It's measured in nanometers (nm).
Tx Power (dBm)	The amount of optical power launched by the optical module. It's measured in dBm.
Rx Power (dBm)	The amount of optical power received by the optical module. It's measured in dBm.

Temperature (°C)	The temperature of the optical module. It's measured in Celsius (°C).

BGP

Click the **BGP** tab. Then, you can see the following table:

> **NOTE**
>
> You cannot see BGP telemetry data for switches of the model N9550-64D that are installed with PicOS 4.5.3.2.



VRF Name	BGP Version	Local AS	Local Router ID	Remote AS	Remote Router ID	BGP Status	Hold Time (s)	Keepalive Interval (s)
default	4	110	[redacted]0.92	0	0.0.0.0	ACTIVE	180	60
default	4	110	[redacted]0.92	0	0.0.0.0	ACTIVE	180	60
default	4	110	[redacted]0.92	0	0.0.0.0	ACTIVE	180	60
default	4	110	[redacted]0.92	0	0.0.0.0	ACTIVE	180	60
default	4	110	[redacted]0.92	0	0.0.0.0	ACTIVE	180	60

Table 7. BGP Metrics

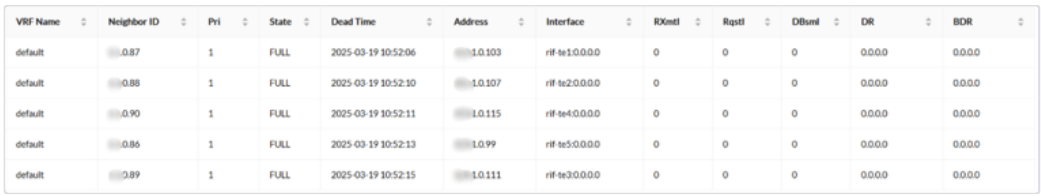
Metric	Description
VRF Name	The name of the Virtual Routing and Forwarding (VRF) instance.
BGP Version	The version of Border Gateway Protocol (BGP).
Local AS	The Autonomous System Number (ASN) of the local switch.
Local Router ID	The unique BGP identifier of the local switch.
Remote AS	The ASN of the remote device.
Remote Router ID	The unique BGP identifier of the remote device.
BGP State	The state of the BGP session.
Hold Time	The allowed maximum time between two BGP peers without receiving any messages. It's measured in seconds.

Keepalive Interval	The time interval for sending KEEPALIVE messages between BGP peers. It's measured in seconds.

OSPF

Click the **OSPF** tab. Then, you can see the following table:

> **NOTE**
>
> The OSPF telemetry data might not display for switches of the model N9550-64D that are installed with PicOS 4.5.3.2.



VRF Name	Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtl	Rqstl	DBsml	DR	BDR
default	0.87	1	FULL	2025-03-19 10:52:06	1.0.103	rif-te1:0.0.0.0	0	0	0	0.0.0.0	0.0.0.0
default	0.88	1	FULL	2025-03-19 10:52:10	1.0.107	rif-te2:0.0.0.0	0	0	0	0.0.0.0	0.0.0.0
default	0.90	1	FULL	2025-03-19 10:52:11	1.0.115	rif-te4:0.0.0.0	0	0	0	0.0.0.0	0.0.0.0
default	0.86	1	FULL	2025-03-19 10:52:13	1.0.99	rif-te5:0.0.0.0	0	0	0	0.0.0.0	0.0.0.0
default	0.89	1	FULL	2025-03-19 10:52:15	1.0.111	rif-te3:0.0.0.0	0	0	0	0.0.0.0	0.0.0.0

Table 8. OSPF Metrics

Metric	Description
VRF Name	The name of the VRF instance.
Neighbor ID	The unique identifier to distinguish a neighboring device.
Pri	The OSPF router priority, which is a parameter that influences the election process for the Designated Router (DR) and Backup Designated Router (BDR) within an OSPF network.
State	The current status of the OSPF router.
Dead Time	The amount of time that a router waits to receive a Hello packet from a neighboring router before it declares that neighbor as "dead" or unreachable. It's measured in seconds.
Address	The IP address of the neighbor.
Interface	The interface on a router to establish the OSPF neighbor relationship.

RXmtl	The total number of link state advertisements on the retransmission queue sent to neighbors.
Rqstl	The total number of link state advertisements on the request messages queue sent to neighbors.
DBsml	The total number of link state advertisements on the Database Description (DD) messages queue sent to neighbors.
DR	The Designated Router, a special router elected within an OSPF area to handle the exchange of link-state information.
BDR	Backup Designated Router, a backup to the DR in an OSPF network.

MAC

Click the **MAC** tab. Then, you can see the following table:

> **NOTE**
>
> You cannot see MAC telemetry data for switches with PicOS 4.7.1M and PicOS 4.7.0E installed.

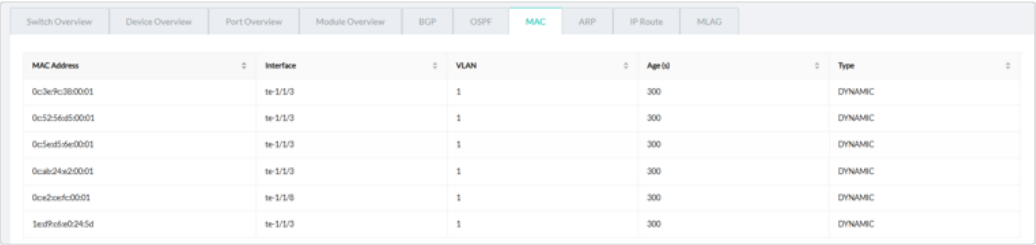


Table 9. MAC Metrics

Metric	Description
MAC Address	The MAC address of the switch port connecting to this switch.
Interface	The physical port associated with the MAC address.
Vlan	The identifier of the VLAN including this MAC address.

Age	The duration during which the MAC address entry remains valid before it is deleted due to lack of updates. It's measured in seconds.
Type	The obtaining method of the MAC address, dynamic or static.

ARP

Click the **ARP** tab. Then, you can see the following table:

> **NOTE**
>
> You cannot see ARP telemetry data for the following switches:
>
> - The N9550-64D switches with PicOS 4.5.3.2 installed.
> - The switches with PicOS 4.7.1M and PicOS 4.7.0E installed.

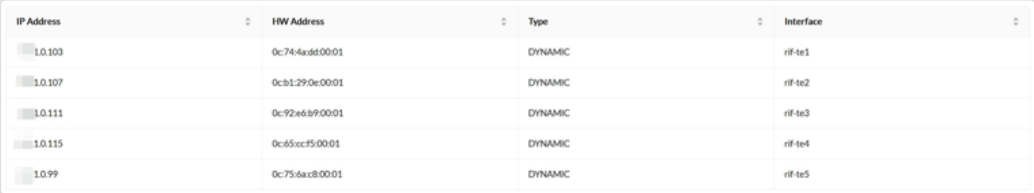


Table 10. ARP Metrics

Metric	Description
Address	The IP address of the neighboring switch.
HW Address	The MAC address of the neighboring switch.
Type	The types of the ARP entry, dynamic or static.
Interface	The physical or logical port on the switch associated with the IP address and the MAC address.

AI

Click the **AI** tab. Then, you can see the following table:

> **NOTE**

You can see PFC and ECN related telemetry data only for **Trident3** and **Tomahawk3** switches that support PFC and ECN and have PFC and ECN enabled.



Interface Name	ECN-Marked-Packets	ECN-Marked-Packets-Rate	Queue Name	PFC-Deadlock-Monitor-Count	PFC-Deadlock-Recovery-Count	Receive-PFC-Pause-Frames	Receive-PFC-Pause-Frames-Rate	Send-PFC-Pause-Frames	Send-PFC-Pause-Frames-Rate
te-1/1/1	256	-	1	0	0	256	0	256	0

Table 11. AI Metrics

Metric	Description
Interface Name	The interface of the switch
ECN-Marked-Packets	The number of packets that have been marked with Explicit Congestion Notification (ECN).
ECN-Marked-Packets-Rate	The number of packets per unit time that are marked with Explicit Congestion Notification (ECN) codes by the switch in response to detected congestion.
Queue Name	The queue name of Priority Flow Control (PFC).
PFC-Deadlock-Monitor-Count	A counter used for monitoring and recording the number of PFC deadlock events.
PFC-Deadlock-Recovery-Count	A counter used to track and record the number of recoveries from PFC deadlock states.
Receive-PFC-Pause-Frames	The PAUSE frames received by the receiver end for flow control.
Receive-PFC-Pause-Frames-Rate	The rate at which PFC PAUSE frames are received by the switch.
Send-PFC-Pause-Frames	The PAUSE frames sent by the transmitting end for flow control.
Send-PFC-Pause-Frames-Rate	The rate at which PFC PAUSE frames are sent.

IP Route



Type	Destination Network	Route Metrics	Next-Hop	Outgoing Interface	Route Age
OSPF	[redacted]0.98/31	[110/200]	[redacted]0.97	rif-te5	01:12:52
DIRECTLY_CONNECTED	1[redacted].0.96/31	[0/0]	-	rif-te5	01:13:11
OSPF	[redacted]0.96/31	[110/100]	-	rif-te5	01:13:04
OSPF	[redacted]0.114/31	[110/200]	1[redacted].0.113	rif-te4	01:12:44
DIRECTLY_CONNECTED	1[redacted].0.112/31	[0/0]	-	rif-te4	01:13:11

Table 12. IP Route Metrics

Metric	Description
Type	The protocol through which the route was learned or configured. • **DIRECTLY_CONNECTED:** This is a directly connected network. • **STATIC:** This is a static route. • **OSPF:** This is a route learned through the **OSPF** protocol. • **BGP:** This is a route learned through the **BGP** protocol.
Destination Network	The address and subnet mask of the destination network.
Route Metrics	The metric (or cost) of the route, which determines the priority of the route. For example, [110/2] indicates that the route uses the OSPF protocol, where 110 is the OSPF priority (cost) and 2 is the metric of the route.
Next-Hop	The next hop IP address to which packets are forwarded.
Outgoing Interface	The network interface from which packets are forwarded.
Route Age	The elapsed time since the route was learned or configured.

MLAG

Click the **MLAG** tab. Then, you can see the following table:

> **NOTE**
>
> You cannot see MLAG telemetry data for switches of the model N9550-64D that are installed PicOS 4.5.3.2.

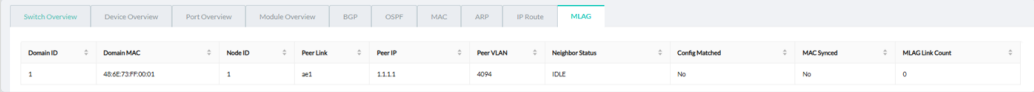


Table 13. MLAG Metrics

Metric	Description
Domain ID	The unique identifier to distinguish an MLAG domain. An MLAG domain is established between two switches configured with the same domain ID.
Domain MAC	The MAC address of an MLAG domain.
Node ID	The unique identifier to distinguish the MLAG peer devices. • **0** : Represents the primary device. • **1** : Represents the secondary device.
Peer Link	The local interface ID of the peer-link.
Peer IP	The IP address of the remote peer-link port.
Peer VLAN	The VLAN ID used for the peer-link.
Neighbor Status	The status of the MLAG peer connection. • **IDLE**: No peer-link is established. • **CONNECTING**: The peer-link is being established. • **ESTABLISHED**: The peer-link is established successfully.
Config Matched	Whether the configurations between MLAG peers are consistent. Values can be **Yes** or **No**.
MAC Synced	Whether the MAC address tables between MLAG peers are consistent. Values can be **Yes** or **No**.

MLAG Link Count	The total number of MLAG peer-links.

Filtering Telemetry Data

To filter telemetry data as needed, use the following methods:

- To specify the metrics that you want to monitor, click the **All Counters** icon, select the metrics, and then click **Apply**.
- To specify how many ports you want to monitor, select one of the following options:
  - **Top 5:** The 5 switch ports with the largest values. By default, **Top 5** is selected.
  - **Top 10:** The 10 switch ports with the largest values.
  - **Top 25:** The 25 switch ports with the largest values.

> **NOTE**
>
> Even though **Top X** is selected, you might see less than the selected number of switch ports in the line chart when other ports are down.

- To display or hide the data of a switch port, click the square before the port.
- To view the metric details at a specific time point, hover the mouse over that time point.

Performance Statistics

Click **Monitor > Telemetry > Performance Statistics** in the AmpCon-DC UI. Then, you can see the telemetry data of all managed switches.

After you add devices to AmpCon-DC with the monitoring function enabled, AmpCon-DC automatically collects performance-related telemetry metrics of NICs on these devices. You can gain real-time or historical insights into network traffic conditions on each NIC, identify traffic peaks, and pinpoint bottlenecks.

See the following child topics:

- Switch Performance Statistics
- NIC Performance Statistics

Switch Performance Statistics

Click **Monitor > Telemetry > Performance Statistics** from the navigation bar. In the **Switch** tab, you can see the following telemetry data of all managed switches:

Limitation
Prerequisites
CPU and Memory
Port Metrics
Module Metrics

Limitation

For N8610-32D switches with PicOS 4.5.6E installed, AmpCon-DC might fail to retrieve telemetry data from these switches. This is caused by a known bug of PicOS 4.5.6E.

Prerequisites

Real-time telemetry data can be displayed in the AmpCon-DC UI only when the following prerequisites are met:

- The switches to be monitored are connected to the AmpCon-DC server. Click **Device > Switches** from the navigation bar, and then check the **VPN IP** column
  - ✔ means the switch is connected to the AmpCon-DC server.
  - x means the switch is not connected to the AmpCon-DC server.
- Google Remote Procedure Call (gRPC) and Link Layer Discovery Protocol (LLDP) are enabled on the switch to be monitored. By default, gRPC and LLDP are enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

CPU and Memory

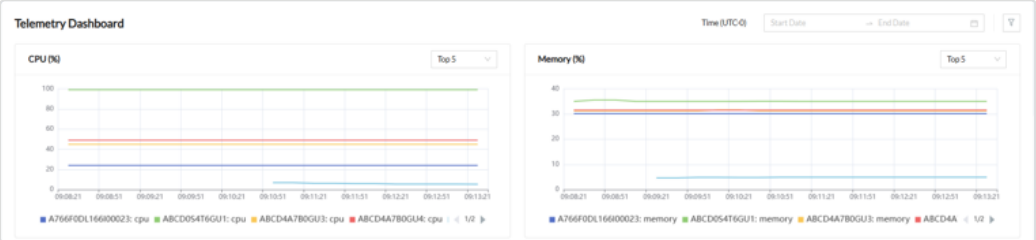


Table 1. CPU and Memory Telemetry Data

Metric	Description
CPU	The CPU usage of a switch in percentage.

Memory	The memory usage of a switch in percentage.

> **NOTE**
>
> The **CPU** and **Memory** sections are always displayed and can't be hidden. You can display or hide other metrics by clicking the setting icon and selecting the metrics to be monitored.

Port Metrics

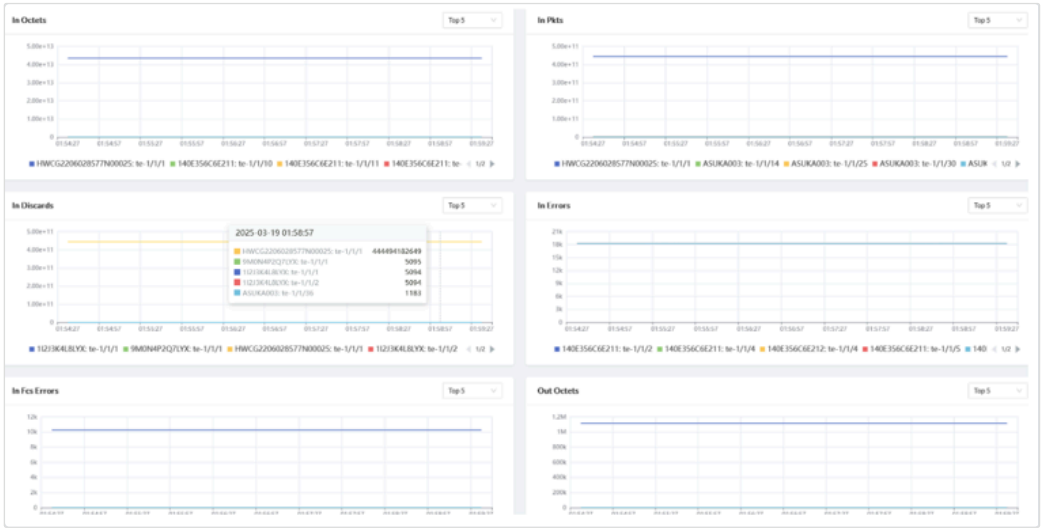


Table 2. Port Telemetry Data

Metric	Description
In Octets	The number of octets (8-bit bytes) received by a switch port.
In Pkts	The number of incoming packets received by a switch port.
In Discards	The number of incoming packets that a switch port intentionally discards (drops) during processing.
In Errors	The number of incoming packets that contain errors and are dropped by a switch port.

In Fcs Errors	The number of incoming packets that fail the Frame Check Sequence (FCS) validation.
Out Octets	The number of octets (8-bit bytes) transmitted out of a switch port.
Out Pkts	The number of outgoing packets transmitted by a switch port.
Out Discards	The number of outgoing packets that a switch port intentionally discards (drops) before they are transmitted.
Out Errors	The number of outgoing packets that a switch port fails to transmit successfully due to errors.
Out Bits Rate	The rate at which bits are transmitted from a switch port. It's measured in bits per second (bps).
In Bits Rate	The rate at which bits are received by a switch port. It's measured in bits per second (bps).
Out Pkts Rate	The rate of data packets sent from a switch port. It's measured in Packets Per Second (pps).
In Pkts Rate	The rate of data packets received by a switch port. It's measured in Packets Per Second (pps).

Module Metrics



Table 3. Module Telemetry Data

Metric	Description
Tx Power	The amount of optical power emitted by the optical module connected to the switch port. It's measured in dBm.
Rx Power	The amount of optical power received by the optical module connected to the switch port. It's measured in dBm.
Temperature	The temperature of the optical module connected to the switch port. It's measured in Celsius (°C).

NIC Performance Statistics

After you add devices to AmpCon-DC with the monitoring function enabled, AmpCon-DC automatically collects performance-related telemetry metrics of NICs on these devices.

You can gain real-time or historical insights into network traffic conditions on each NIC, identify traffic peaks, and pinpoint bottlenecks.

Prerequisites
Viewing Telemetry Data
Filtering Telemetry Data

Prerequisites

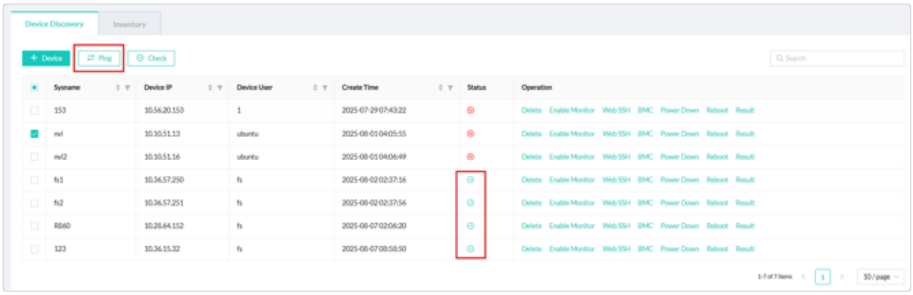
Ensure that the following prerequisites are met:

- The terminal devices are added with the monitor function enabled and with an administrator user of the device specified. For more information, see Adding a Device to AmpCon-DC.
- The port 9100 is not blocked on the added device.
- The devices to be managed are connected to the AmpCon-DC server. You can check by following these steps:

  a. Click **Device > Hosts > Device Discovery** from the navigation bar.

  b. Select the devices to be managed, and then click **Ping**.

  c. Check whether the status is shown as ✔ in the **Status** column.



Viewing Telemetry Data

Click **Monitor > Telemetry > Performance Statistics** in the AmpCon-DC UI. Then, in the **NIC** tab, you can see NIC-related telemetry data of all monitored devices.

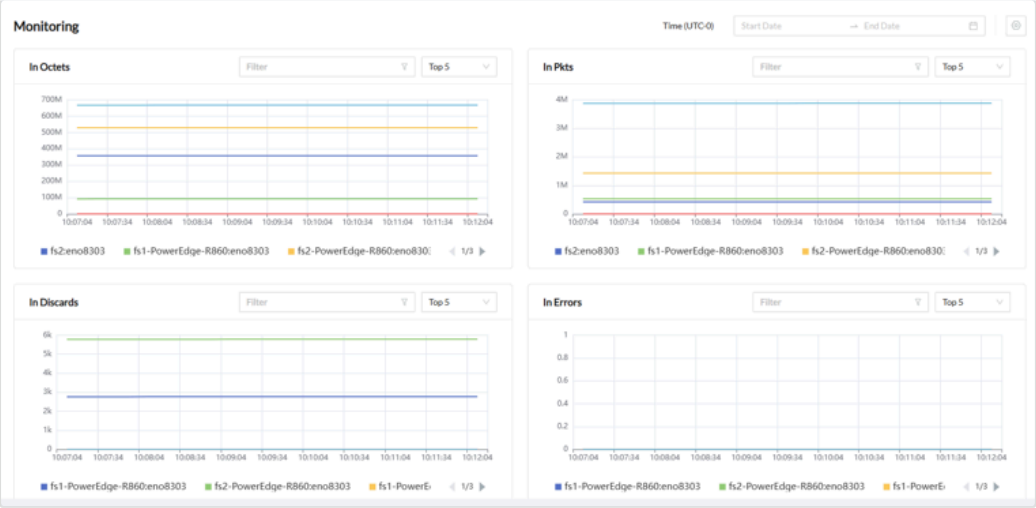


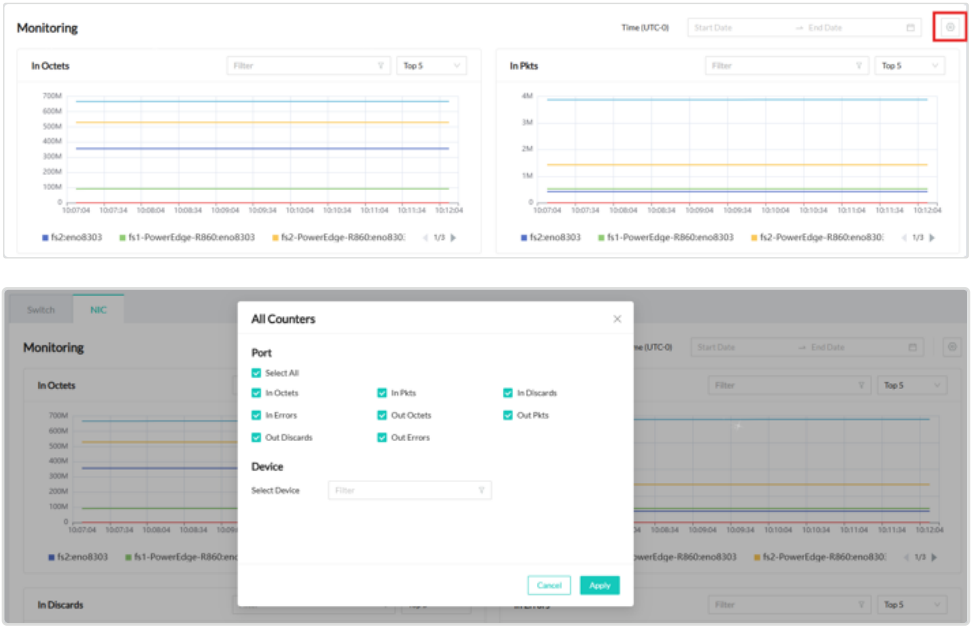
Table 1. NIC Telemetry Data

Metric	Description
In Octets	The number of octets (8-bit bytes) received by a NIC. By using the **In-Octets** metric, you can understand how much data the NIC has received and analyze the traffic and bandwidth usage.
In Pkts	The number of incoming packets received by a NIC. By using the **In-Pkts** metric, you can understand the load on the NIC and diagnose network congestion or connection issues.
In Discards	The number of incoming packets that a NIC intentionally discards (drops) during processing. High discarded incoming packets are possibly caused by buffer overflow, misconfiguration, or traffic control mechanisms.
In Errors	The number of incoming packets that contain errors and are dropped by a NIC. High erroneous incoming packets are possibly caused by potential hardware failures, signal interference, or physical layer problems.
Out Octets	The number of octets (8-bit bytes) transmitted out of a NIC.

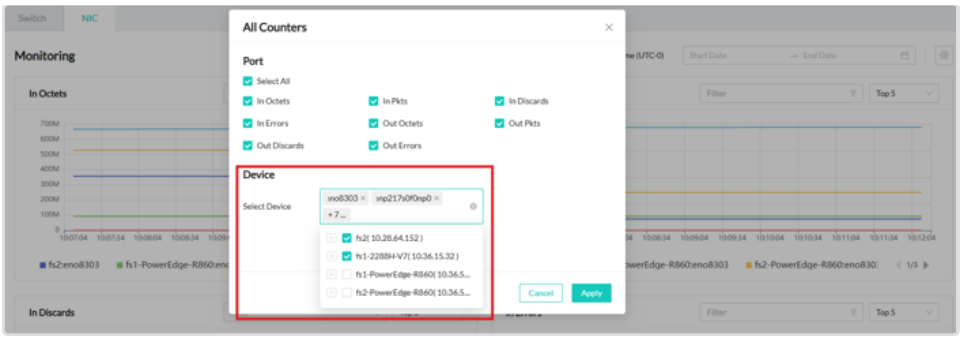
	By using this metric, you can evaluate the total amount of outgoing data and analyze upstream bandwidth usage.
Out Pkts	The number of outgoing packets transmitted by a NIC. By using this metric, you can understand the frequency of sending data packets, the packet transmission behavior, and traffic load of the network interface.
Out Discards	The number of outgoing packets that a NIC intentionally discards (drops) before they are transmitted. High discarded outgoing packets are possibly caused by buffer overflow or flow control issues.
Out Errors	The number of outgoing packets that a NIC fails to transmit successfully due to errors. High erroneous incoming packets are possibly caused by hardware failures or transmission line issues.

Filtering Telemetry Data

- To specify the metrics that you want to monitor, click the **All Counters** icon, select the metrics to be monitored, and then click **Apply**.



- To specify the devices and NICs that you want to monitor, click the **All Counters** icon, select the devices and NICs, and then click **Apply**.



- To specify how many NICs that you want to monitor, select one of the following options:
  - **Top 5:** The 5 NICs with the largest values. By default, **Top 5** is selected.
  - **Top 10:** The 10 NICs with the largest values.
  - **Top 25:** The 25 NICs with the largest values.



> **NOTE**
>
> Even though **Top X** is selected, you might see fewer than the selected number of NICs in the line chart when other NICs are down.

- To specify the time range for the data display, select the start date and end date in the **Time** section.



- To display or hide the data of a NIC, click the square before the NIC.



- To view the metric details at a specific time point, hover the mouse over that time point.



RoCE Counters

By using AmpCon-DC, you can monitor RoCE monitoring data on the Network Interface Card (NIC) side and on the switch side.

You can also check buffer-related metrics for switch port queues. These metrics can help you quickly identify issues such as buffer overflow and packet drops.

In addition, you can visualize load balancing related metrics. Based on these metrics, you can optimize your network for better performance.

See the following child topics:

- RoCE Data on Switches and NICs
- Buffer
- Dynamic Load Balancing (DLB)

RoCE Data on Switches and NICs

RoCE monitoring is valuable to identify key factors affecting network performance, ensure business continuity, and improve network management efficiency.

By using AmpCon-DC, you can monitor RoCE monitoring data on the Network Interface Card (NIC) side and on the switch side.

- RoCE Data on Switches
  - Prerequisites
  - Procedure
- RoCE Data on NICs
  - Prerequisites
  - Procedure

RoCE Data on Switches

Prerequisites

Ensure that the following prerequisites are met:

Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

> **NOTE**
>
> You can see Priority Flow Control (PFC) and Explicit Congestion Notification (ECN) data for only **Trident3** and **Tomahawk3** switches that support PFC and ECN and have PFC and ECN enabled.

Procedure

1. Click **Monitor > Telemetry > RoCE Counters** from the navigation bar.
2. In the **PFC & ECN** tab, select **Switch**.
3. In the **Trends** tab, you can see the following telemetry data:



Table 1. RoCE Telemetry Data

Metric	Description
Ecn Marked Packets	The number of packets that have been marked with ECN.
Send-Pfc-Pause-Frames	The PAUSE frames sent by the transmitting end for flow control.
Receive-Pfc-Pause-Frames	The PAUSE frames received by the receiver end for flow control.
Pfc-Deadlock-Monitor-Count	A counter used for monitoring and recording the number of PFC deadlock events.
Pfc-Deadlock-Recovery-Count	A counter used to track and record the number of recoveries from PFC deadlock states.

4. Click the **Filter** icon to specify the scope of the telemetry data to be displayed.



a. In the **Fabric** list, select one or multiple fabrics.

b. In the **Device Role** list, select **leaf**, **spine**, or both.

c. In the **Sysname** list, select the switches and NICs.

d. In the **TopN** list, select the count of NICs to be displayed: **Top 5**, **Top 10**, **Top 25**, or **Total X** (all selected NICs).

Top 5: The 5 NICs with the largest values. By default, **Top 5** is selected.

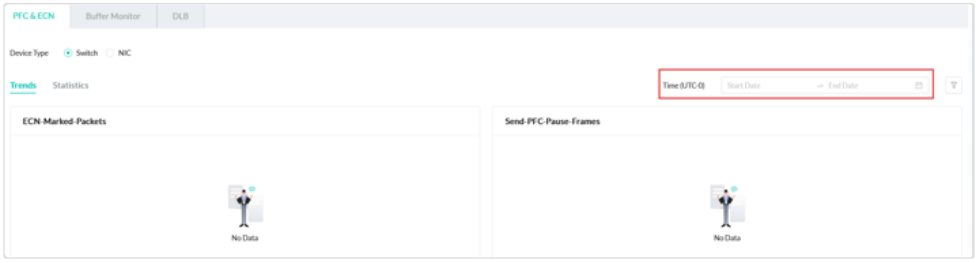
Top 10: The 10 NICs with the largest values.

Top 25: The 25 NICs with the largest values.

> **NOTE**
>
> Even though **Top X** is selected, you might see fewer than the selected number of NICs in the line chart when other NICs are down.

e. Click **Apply**.

5. In the **Time** section, select the start date and end date. Then, the data during the selected time range is displayed.



6. Click the **Statistics** tab. You can see the following information.

   You can click the **Filter** icon to specify the scope of the telemetry data to be displayed.



Table 2. RoCE Metrics

Metric	Description
Fabric	The fabric of the switch.
Sysname	The hostname of the switch.
Device Role	Spine switch or leaf switch.
Port Name	The port of the switch.
Queue Number	The queue number of PFC.
Send-PFC-Pause-Frames	The PAUSE frames sent by the transmitting end for flow control.

Receive-PFC-Pause-Frames	The PAUSE frames received by the receiver end for flow control.
PFC-Deadlock-Monitor-Count	A counter used for monitoring and recording the number of PFC deadlock events.
PFC-Deadlock-Recovery-Count	A counter used to track and record the number of recoveries from PFC deadlock states.
Send-PFC-Pause-Frames Rate	The rate at which PFC PAUSE frames are sent.
Receive-PFC-Pause-Frames Rate	The rate at which PFC PAUSE frames are received by the switch.
ECN Marking Number	The number of packets that have been marked with ECN.
The Rate Of ECN Marked Packets	The number of packets per unit time that are marked with ECN codes by the switch in response to detected congestion.

RoCE Data on NICs

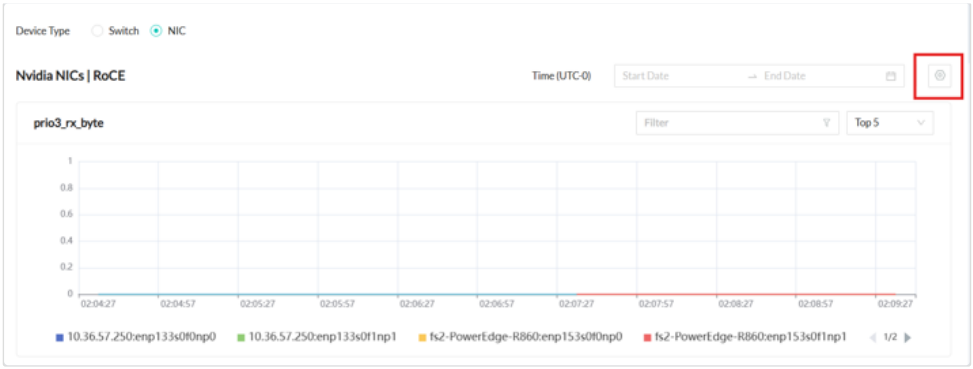
Prerequisites

Ensure that the following prerequisites are met:

- The devices to be managed are added to AmpCon-DC with the monitor function enabled. For more information, see Adding Devices.
- The devices to be managed are connected to the AmpCon-DC server. For more information, see Testing Device Connectivity.

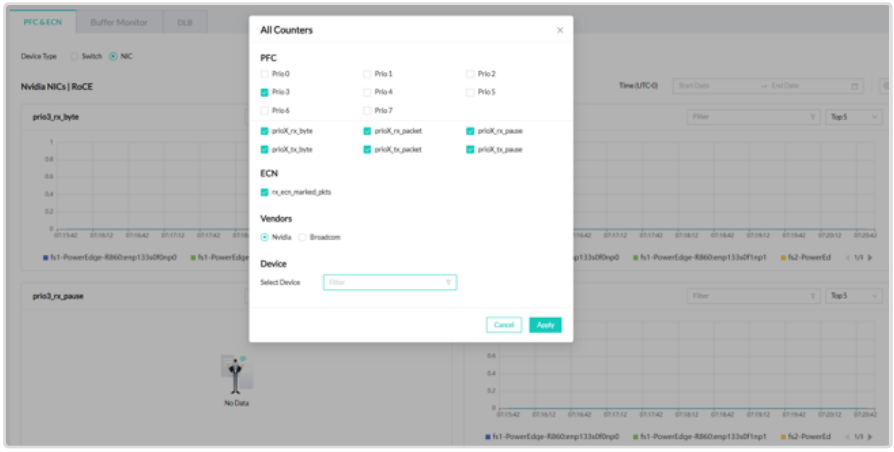
Procedure

1. Click **Monitor > Telemetry > RoCE Counters** from the navigation bar.
2. In the **PFC & ECN** tab, select **NIC**.
3. Click the **All Counters** icon to specify the scope of the telemetry data to be displayed.



a. In the **PFC** section, select the PFC data priority levels. For example, if you selected **Prio3** and **Prio5**, only the PFC telemetry data with priority 3 and 5 is displayed.

> **NOTE**
>
> You are not suggested to select all priority levels. Or else, the metric numbers will be too large to display the telemetry data.



b. In the **PFC** section, select the PFC metrics to be monitored.

Table 3. PFC Metrics

Metric	Description
prioX_rx_byte	Total incoming bytes with the selected priority level
prioX_rx_packet	Total incoming frames received with the selected priority level
prioX_rx_pause	Total incoming Pause Frames received with the selected priority level

prioX_tx_byte	Total outgoing bytes with the selected priority level
prioX_tx_packet	Total outgoing frames with the selected priority level
prioX_tx_pause	Total outgoing Pause Frames with the selected priority level

c. In the **ECN** section, select or unselect the ECN metric **rx_ecn_marked_pkts**, which means the count of incoming packets marked with ECN.

d. In the **Vendors** section, select the NIC vendor, **Nvidia** or **Broadcom**.

> **NOTE**
>
> Currently, the RoCE telemetry data of Nvidia and Broadcom NICs can't be displayed together.

e. In the **Device** section, click the filter icon, and then select the device and NICs to be monitored. Then, click **OK**.

4. In the **Time** section, select the start date and end date.

   Then, the data during the selected time range is displayed.

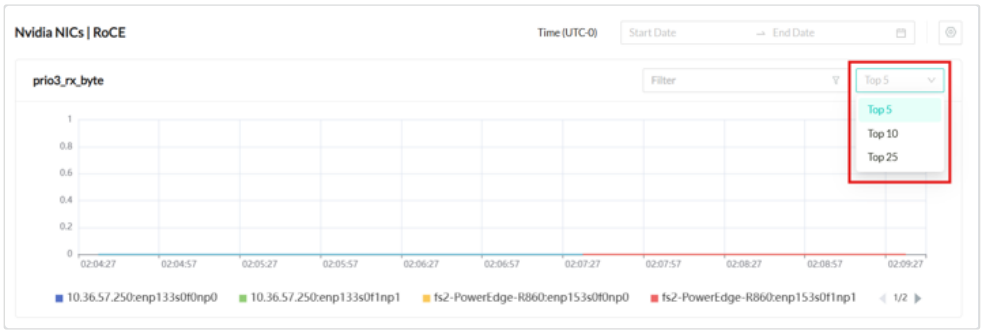


5. Select the count of NICs to be displayed:

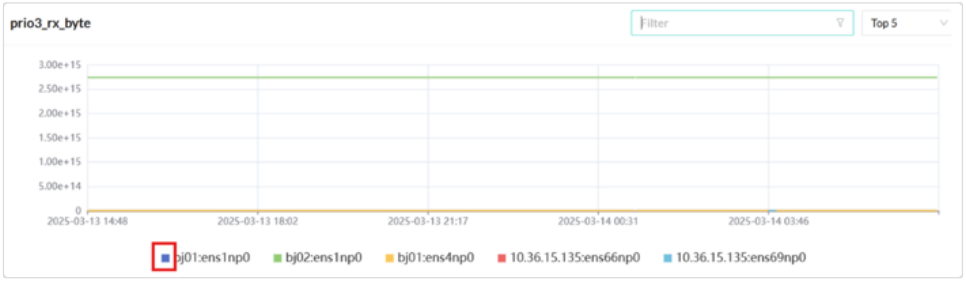
- **Top 5:** The 5 NICs with the largest values. By default, **Top 5** is selected.
- **Top 10:** The 10 NICs with the largest values.
- **Top 25:** The 25 NICs with the largest values.

> **NOTE**

> Even though **Top X** is selected, you might see less than the selected number of NICs in the line chart when other NICs are down.



6. To display or hide the data of a NIC, click the square before the NIC.



7. To view the metric details at a specific time point, hover the mouse over that time point.

Buffer

Switch buffers are essential for handling traffic bursts and avoiding packet drops. However, when buffers are heavily used, the network is more likely to experience congestion, higher latency, and packet drops. Without timely visibility into buffer usage, these risks might not be detected and impact critical service performance.

AmpCon-DC supports displaying buffer-related metrics for switch port queues.

Based on these metrics, you can quickly identify issues such as buffer overflow and packet drops, helping optimize network performance.

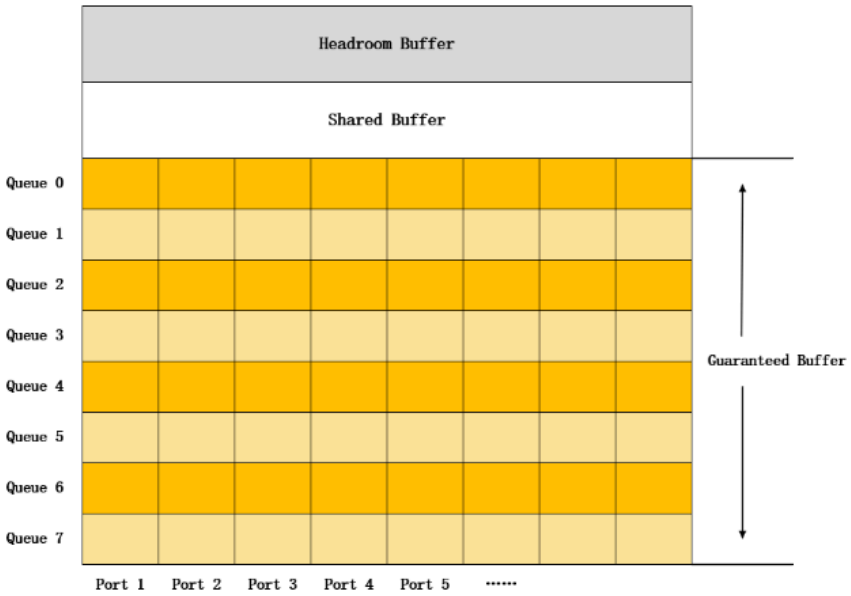
Buffer Overview
Limitation
Prerequisite
Trend
Statistics
Filtering Buffer Data

Buffer Overview

The buffers are configured to implement traffic control, which is based on the port and priority queue. The storage space of each port is divided into different buffers independently, and a certain action will be executed after the number of accumulated packets reaches the buffer threshold.

- **Guaranteed Buffer**: The dedicated buffer available for a specified queue. This buffer space cannot be used by other queues.
- **Shared Buffer**: The public buffer available for all queues. The shared buffer will be occupied when the guaranteed buffer reaches the threshold.
- **Headroom Buffer**: A reserved buffer space used to temporarily store packets when the shared buffer is full. It provides additional capacity for packets with specific 802.1p priorities, ensuring packet loss is minimized during traffic bursts or congestion.

Figure 1. Buffer Division Diagram



Limitation

For N8610-32D switches with PicOS 4.5.6E installed, AmpCon-DC might fail to retrieve the buffer-related telemetry data from these switches. This is caused by a known bug of PicOS 4.5.6E.

Prerequisite

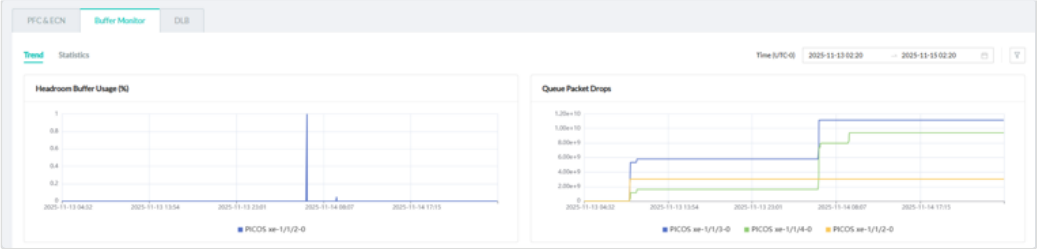
Ensure that the following prerequisites are met. Or else, you might not see buffer data display:

- The PFC buffer feature is configured on the switches to be monitored.
  For more information, see Configuring PFC Buffer.
- Ensure that Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.
  For more information, see Configuring gNMI-gRPC Based Telemetry Technology.

Trend

To check the metrics for buffer, click **Monitor > Telemetry > RoCE Counters** from the navigation bar, and then click the **Buffer Monitor** tab.

In the **Trend** tab, you can see the following line charts:



These two metrics display the headroom buffer usage and the packet drops of switch port queues.

Table 1. Buffer Metrics

Metric	Description
Headroom Buffer Usage (%)	The percentage of the headroom buffer used by each switch port queue relative to the allocated headroom buffer of each switch port queue. A high value indicates that the headroom buffer is almost exhausted, which might cause queue congestion or packet drops if the value continues to increase.
Queue Packet Drops	The total number of packets dropped by each switch port queue. A high value indicates that switch port queues cannot handle the incoming traffic, which might lead to degraded network performance.

Statistics

In the **Statistics** tab, you can see the following table:

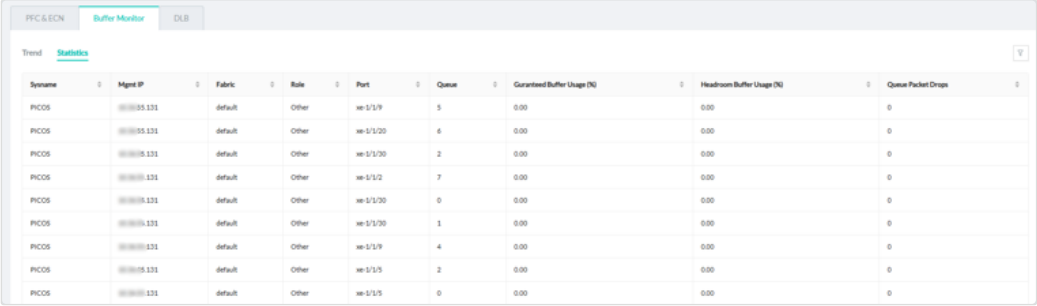
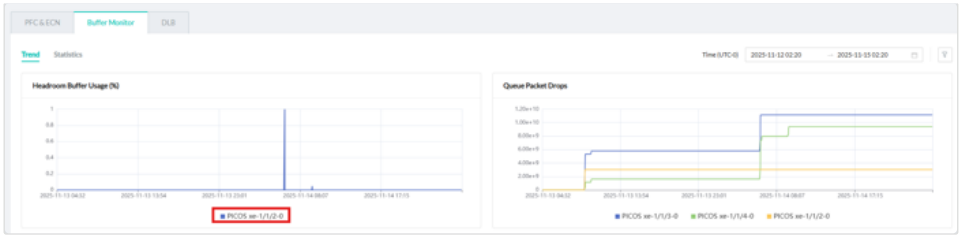


Table 2. Buffer Statistics

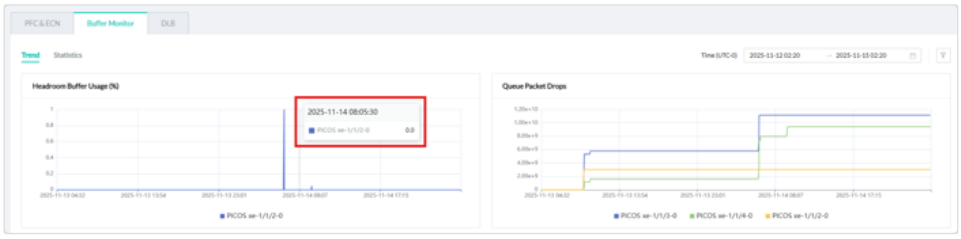
Metric	Description
Sysname	The hostname of the switch.
Mgmt IP	The management IP address of the switch.
Fabric	The fabric to which the switch belongs.
Role	The role of the switch. Values can be **Spine**, **Leaf**, or **Other**. **NOTE** The switch role indicates how a switch functions in a fabric. The roles are defined as follows: • **Spine**: The switch acts as a spine switch in a fabric. • **Leaf**: The switch acts as a leaf switch in a fabric. • **Other**: The switch is not used in the fabric deployment process.
Port	The port on the switch.
Queue	The queue number of the port.
Guaranteed Buffer Usage (%)	The percentage of the guaranteed buffer used by the queue relative to the allocated guaranteed buffer of the queue.
Headroom Buffer Usage (%)	The percentage of the headroom buffer used by the queue relative to the allocated headroom buffer of the queue.
Queue Packet Drops	The total number of packets dropped by this queue.

Filtering Buffer Data

- To display or hide the data of a switch port queue, click the square before the switch port queue.

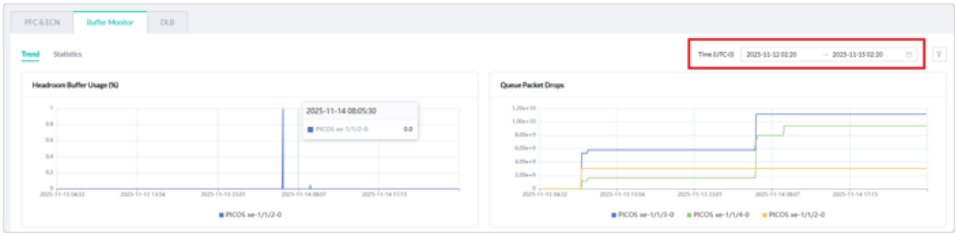


- To view the metric details at a specific time point, hover your mouse over that time point.

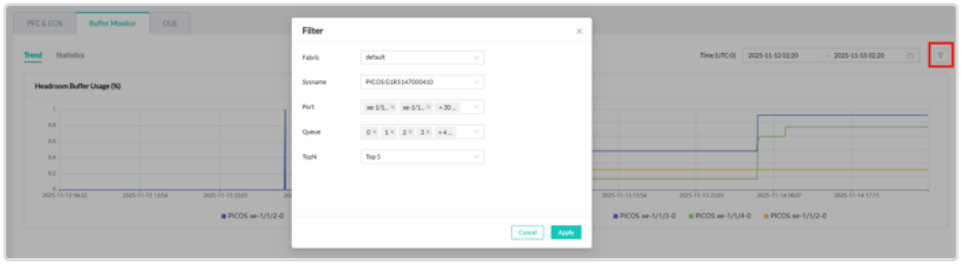


- To specify the time range for the data display, select the start time and end time in the **Time (UTC-0)** section.

> **NOTEs**
>
> - The time in the **Time (UTC-0)** section is based on the **UTC-0** time zone.
> - By default, the data for the past 30 minutes is displayed.



- To specify the scope of the buffer-related data to be displayed, click the filter icon.



Then, in the pop-up window, input one or multiple filter parameters as needed. The following filter parameters are provided:

Table 2. Filter Parameters

Parameters	Description
Fabric	Optional. The fabric to which the switch belongs.
Sysname	Optional. The hostname of the switch.
Port	Optional. The port on the switch.
Queue	Optional. The queue number of the port.
TopN	Optional. Specifies the queues to be monitored. Select one of the following options: • **Top 5:** The 5 switch port queues with the largest values. By default, **Top 5** is selected. • **Top 10:** The 10 switch port queues with the largest values. • **Top 25:** The 25 switch port queues with the largest values. **NOTEs** • Only the ports in **Up** status can be monitored. To check port status, see Port Overview. • Even though **Top X** (such as **Top 5**) is selected, you might see fewer port queues than the selected number in the line chart. The reasons might be as follows: ◦ Some ports are down. ◦ Some ports don't have packet drops.

Dynamic Load Balancing

AmpCon-DC provides a **DLB** tab to help you visualize load balancing related metrics. Based on these metrics, you can optimize your network for better performance.

To check the metrics for Dynamic Load Balancing (DLB), click **Monitor > Telemetry > RoCE Counters** in the AmpCon-DC UI. Click the **DLB** tab, and then select the SN or service tag of a switch in the **SN/Service Tag** drop-down list.

This feature works only for online switches and ports. For offline switches and ports, no data is displayed in the **DLB** tab.

- Limitation
- Prerequisites
- Performance Trend
  - Bandwidth Utilization (Output) and Bandwidth Utilization (Input)
  - Packet Loss Rate (Input) and Packet Loss Rate (Output)
  - Throughput (Output) and Throughput (Input)
- Real-Time Statistics
- Filtering DLB data

Limitation

For N8610-32D switches with PicOS 4.5.6E installed, AmpCon-DC might fail to retrieve the DLB-related telemetry data from these switches. This is caused by a known bug of PicOS 4.5.6E.

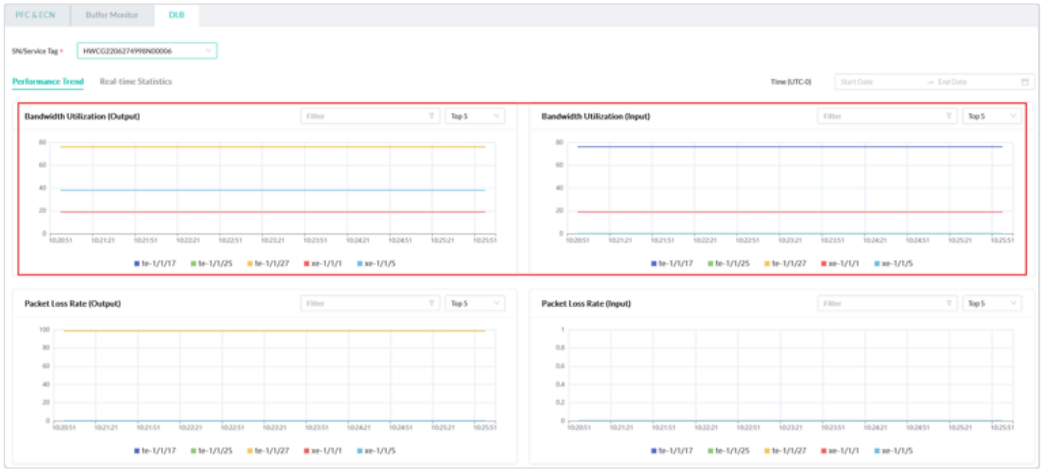
Prerequisites

Ensure that Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

Performance Trend

In the **Performance Trend** tab, you can see the following line charts:

Bandwidth Utilization (Output) and Bandwidth Utilization (Input)



These two metrics are used to measure how effectively the available bandwidth is being utilized.

- **Bandwidth Utilization (Output)**

  The percentage of the total outbound bandwidth that is being used on each port of the selected switch

- **Bandwidth Utilization (Input)**

  The percentage of the total inbound bandwidth that is being used on each port of the selected switch

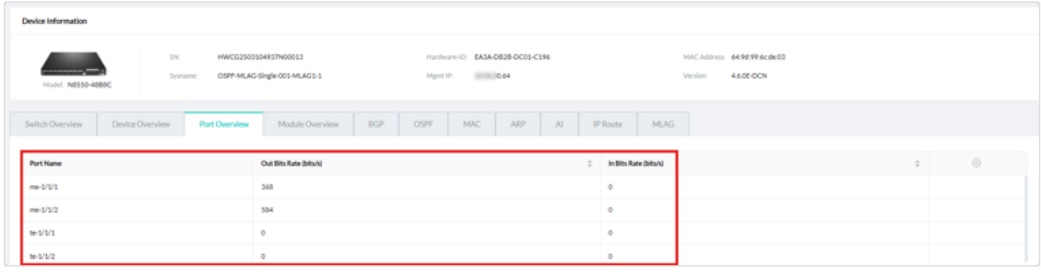
How It Is Calculated

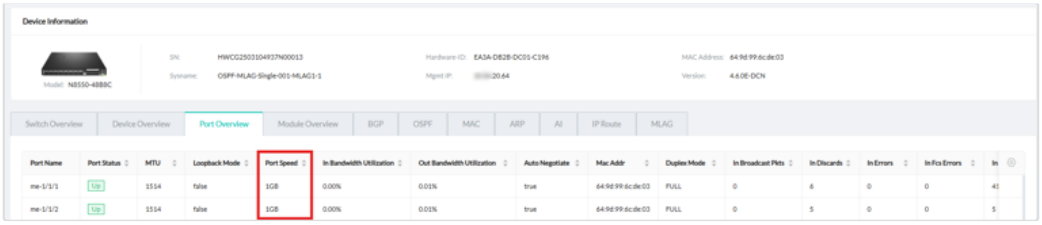
AmpCon-DC calculates **Bandwidth Utilization (Output)** and **Bandwidth Utilization (Input)** as follows:

- Bandwidth Utilization (Output) = Out Bits Rate / Port Speed × 100%
- Bandwidth Utilization (Input)= In Bits Rate / Port Speed × 100%

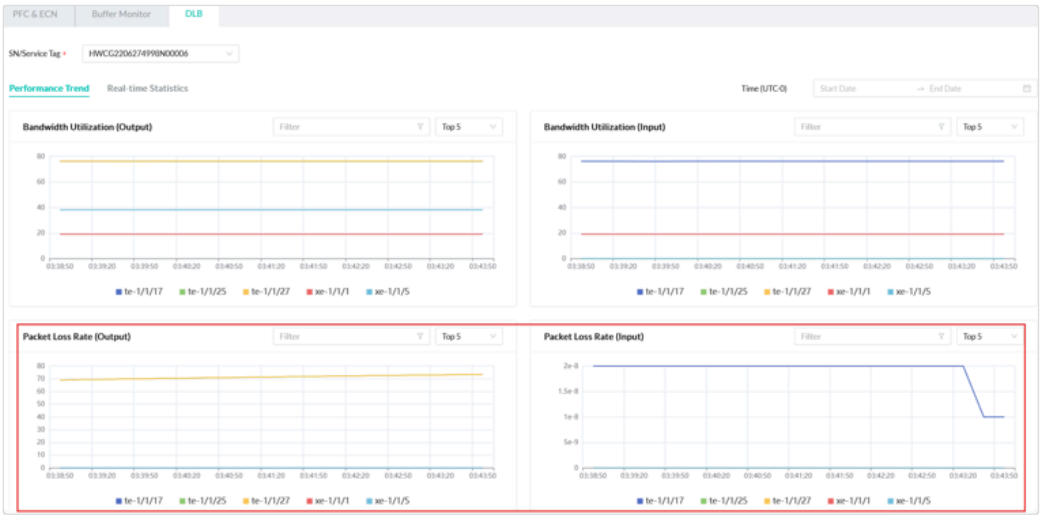
For example, in the **Port Overview** tab of the switch detail page, the **In Bits Rate** metric, which means the rate at which bits are received by the switch port, is 376 bytes per second, and the **Port Speed** metric, which means the maximum data transfer rate that the port can support, is 1GB. So, the **Bandwidth Utilization (Input) value** is:

376 bit / 1GB × 100% = 0.0000376%





Packet Loss Rate (Input) and Packet Loss Rate (Output)



These two metrics are used to measure the reliability of the network and the switch port in delivering data packets.

- **Packet Loss Rate (Input)**

  The rate at which input data packets are discarded during transmission

- **Packet Loss Rate (Output)**

  The rate at which output data packets are discarded during transmission

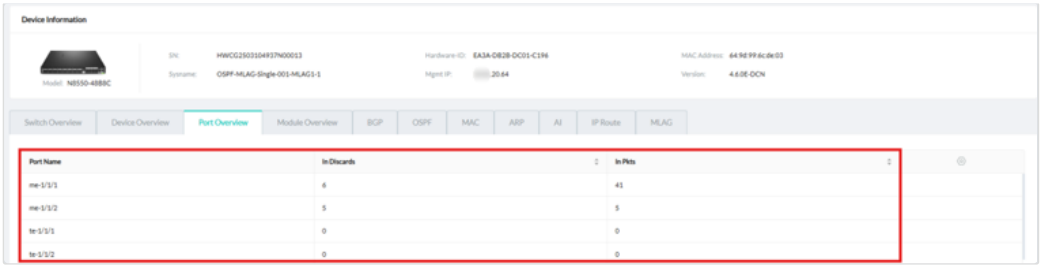
How It Is Calculated

AmpCon-DC calculates **Packet Loss Rate (Output)** and **Packet Loss Rate (Input)** as follows:

- Packet Loss Rate (Output) = Out Discards / Out Pkts × 100%
- Packet Loss Rate (Input) = In Discards / In Pkts × 100%

For example, in the **Port Overview** tab of the switch detail page, the **In Discards** metric, which means discarded input packets, is 24356, and the **In Pkts** metric, which means all input packets, is 31004. So, the **Packet Loss Rate (Input)** value is:

24356 / 31004 × 100% = 78.557605%



Throughput (Output) and Throughput (Input)



These two metrics are used to measure the speed and efficiency of data transmission.

- **Throughput (Output)**

  The rate of data packets sent from the network interface within a unit of time

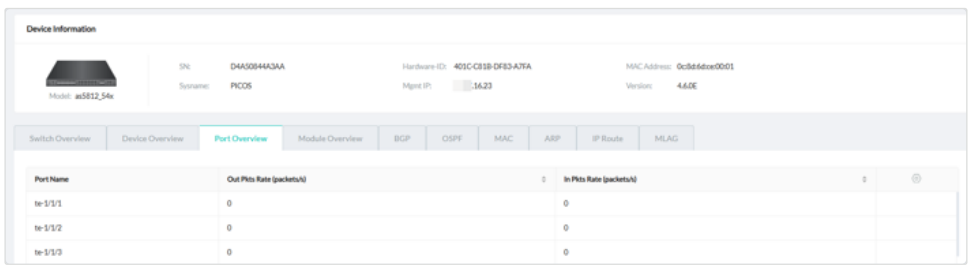
- **Throughput (Input)**

  The rate of data packets received by a network interface within a unit of time

How It Is Calculated

AmpCon-DC calculates **Throughput (Output)** and **Throughput (Input)** as follows:

- The **Throughput (Output)** metric value is equal to the **Out Pkts Rate** metric value in the **Port Overview** tab of the switch detail page.
- The **Throughput (Input)** metric value is equal to the **In Pkts Rate** metric value in the **Port Overview** tab of the switch detail page.



Real-Time Statistics

In the **Real-time Statistics** tab, you can see the following table:

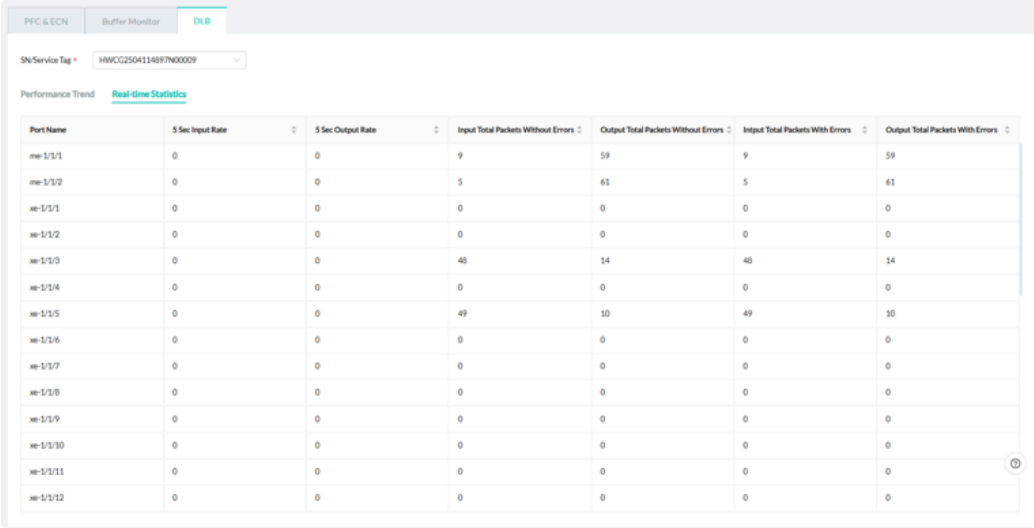


Table 1. Real-Time Statistics

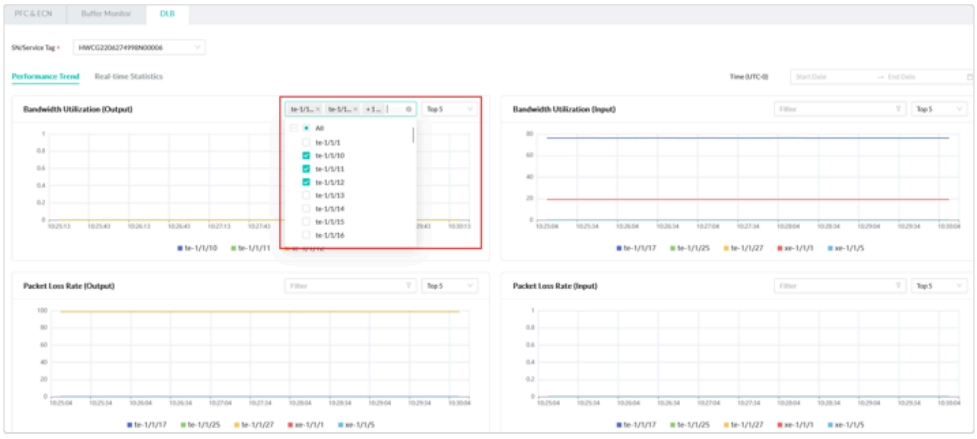
Metric	Description
Port Name	The name of the switch port.
5sec Input Rate	The rate of data packets received by a switch port within a unit of time. The same as the **In-Pkts-Rate** metric in the **Port Overview** tab of the switch detail page.
5sec Output Rate	The rate of data packets sent from the switch port within a unit of time. The same as the **Out Pkts Rate** metric in the **Port Overview** tab of the switch detail page.
Input Total Packets Without Errors	The total number of error-free data packets received by a switch port.
Output Total Packets Without Errors	The total number of error-free data packets sent from a switch port.
Input Total Packets With Errors	The total number of erroneous data packets received by a switch port.
Output Total Packets With Errors	The total number of erroneous data packets sent from a switch port.

> **NOTE**
>
> Except the **Port Name** column, you can sort all the other columns by clicking the sorting triangle.

Filtering DLB data

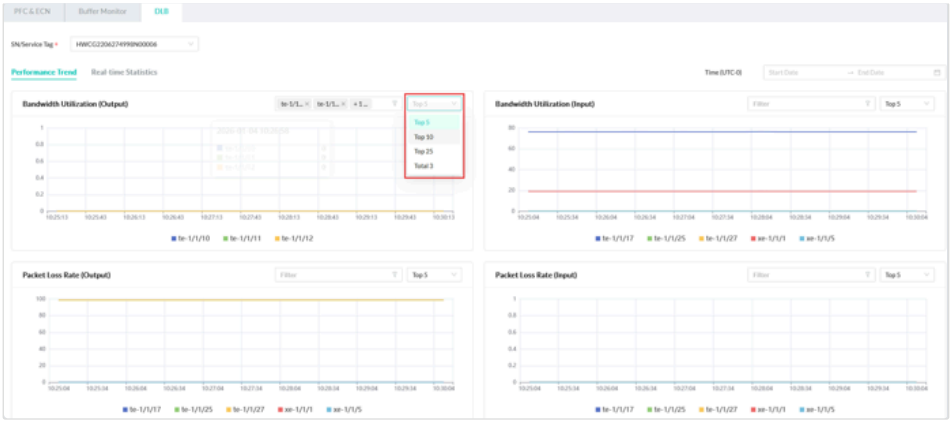
To filter DLB data, use the following methods:

- To check only the data of specific switch ports in a line chart, click the Filter search box of the line chart, and then select the switch ports.

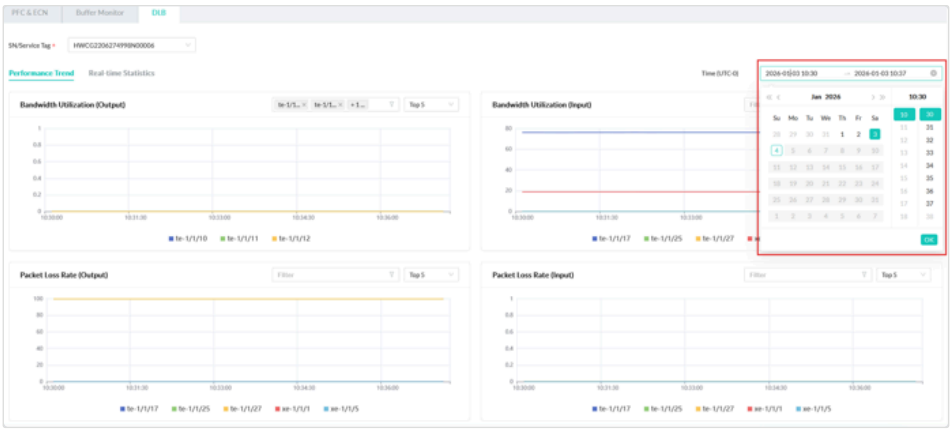


- To specify how many ports that you want to monitor, select one of the following options:
  - **Top 5:** The 5 switch ports with the largest values. By default, **Top 5** is selected.
  - **Top 10:** The 10 switch ports with the largest values.
  - **Top 25:** The 25 switch ports with the largest values.

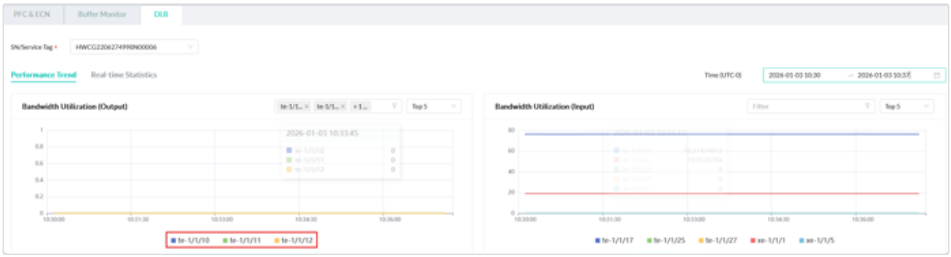
> **NOTE**
>
> Even though **Top X** is selected, you might see less than the selected number of switch ports in the line chart when other ports are down.



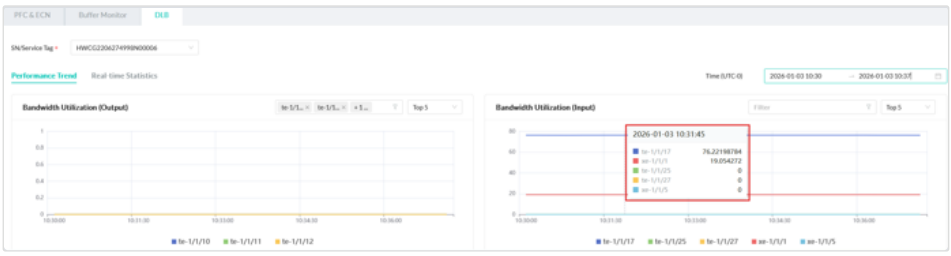
- To specify the time range for the data display, select the start date and end date in the **Time** section.



- To display or hide the data of a switch port, click the square before the switch port.



- To view the metric details at a specific time point, hover the mouse over that time point.



Queue Congestion Visualization

AmpCon-DC supports displaying congestion-related metrics for switch ports.

Based on these metrics, you can analyze congestion details and optimize your network for better performance.

- Overview
- Prerequisite
- Checking Congestion Port Distribution
- Checking Congestion Details
- Filtering Congestion Data

Overview

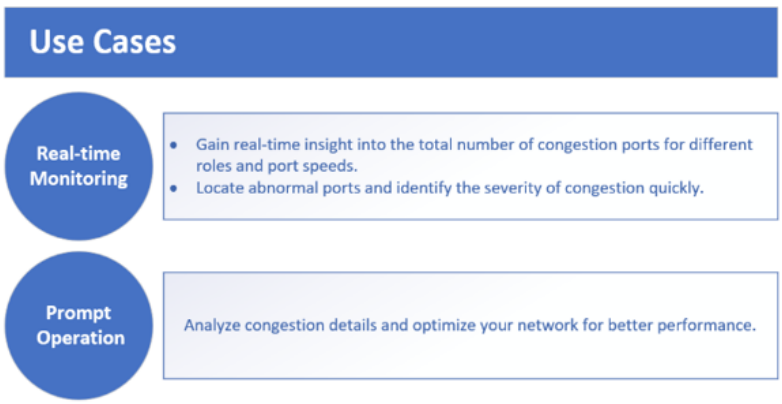
In modern data center networks, service traffic continues to grow, network patterns become more diverse, and bursty traffic occurs more frequently. These trends increase the demand for switches' forwarding performance and buffering capabilities.

When port or queue resources on switches are heavily utilized, the network is more likely to experience congestion, which might lead to increased latency, longer queueing periods, and packet drops. These issues might directly affect service stability and degrade overall network performance.

To maintain network availability and performance, clear visibility for queue congestion details is essential.

See the following use cases:

Figure 1. Use Cases for Congestion Visualization



Prerequisite

Ensure that the following prerequisites are met. Or else, you might not see congestion data display:

- The Priority-based Flow Control (PFC) and Explicit Congestion Notification (ECN) features are configured on switches to be monitored. For more information, see Configuring PFC and Configuring ECN.
- Ensure that Google Remote Procedure Call (gRPC) is enabled on switches to be monitored. By default, gRPC is enabled automatically. For more information, see PFC and ECN Statistical Reporting through gRPC.

Checking Congestion Port Distribution

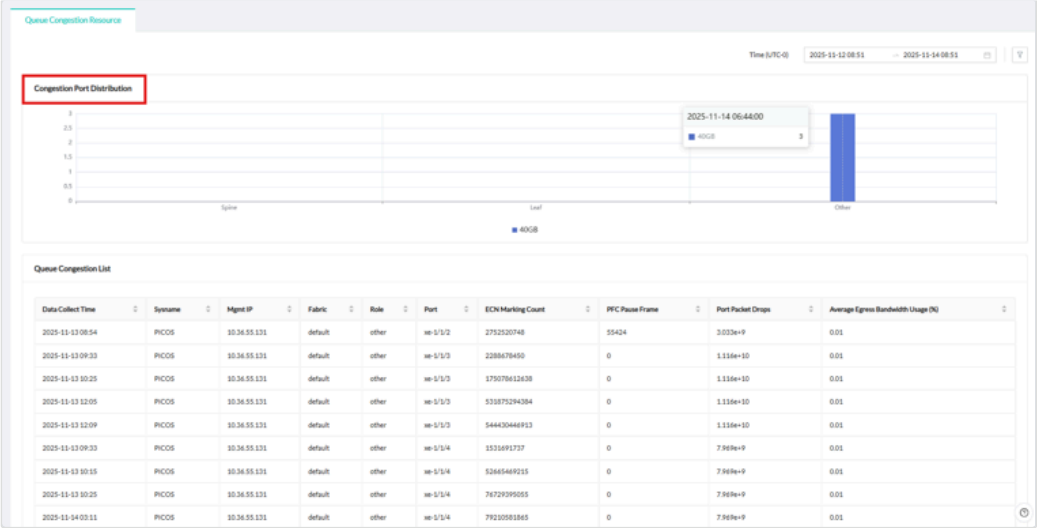
To check congestion port details, click **Monitor > RoCE Insight > Network Congestion** from the navigation bar.

You can see the total number of congestion ports for different roles (**Spine**, **Leaf**, and **Other**).

To view the total number of congestion ports at a specific port speed for a role, locate the role bar, and then hover your mouse over the bar.

> **NOTE**
>
> The switch role indicates how a switch functions in a fabric. The roles are defined as follows:
>
> - **Spine**: The switch acts as a spine switch in a fabric.
> - **Leaf**: The switch acts as a leaf switch in a fabric.
> - **Other**: The switch is not used in the fabric deployment process.

You can filter data as needed. For more information, see Filtering Congestion Data.



Checking Congestion Details

In the **Queue Congestion List** section, you can see the list of congestion ports with detailed information.

You can filter data as needed. For more information, see Filtering Congestion Data.

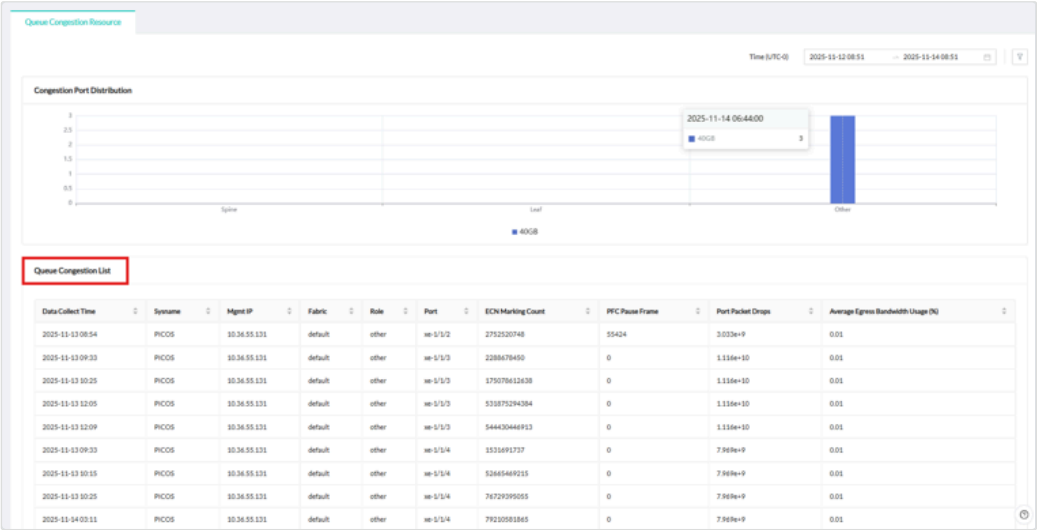


Table 1. Congestion Metrics

Metric	Description
Data Collect Time	The time when AmpCon-DC retrieves the data.
Sysname	The hostname of the switch.
Mgmt IP	The management IP address of the switch.
Fabric	The fabric to which the switch belongs.

Role	The role of the switch. Values can be **Spine**, **Leaf**, or **Other**.
Port	The congestion port on the switch.
ECN Marking Count	The number of times packets are marked with ECN during transmission. When congestion occurs, packets are marked with ECN to decrease the traffic rate. This metric indicates that the switch is mildly congested.
PFC Pause Frame	The total number of PFC pause frames sent by port queues. PFC pause frames are used to pause traffic transmission to prevent packet loss during congestion. This metric indicates that the switch is heavily congested.
Port Packet Drops	The total number of packets dropped by this port.
Average Egress Bandwidth Usage (%)	The percentage of the port's average egress bandwidth relative to its maximum bandwidth. **Example**: If the average transmit rate of a 10G port is 1G, then the **Average Egress Bandwidth Usage** value is 10%. See the following calculation method: Average Egress Bandwidth Usage = (1G / 10G) × 100% = 10%

Filtering Congestion Data

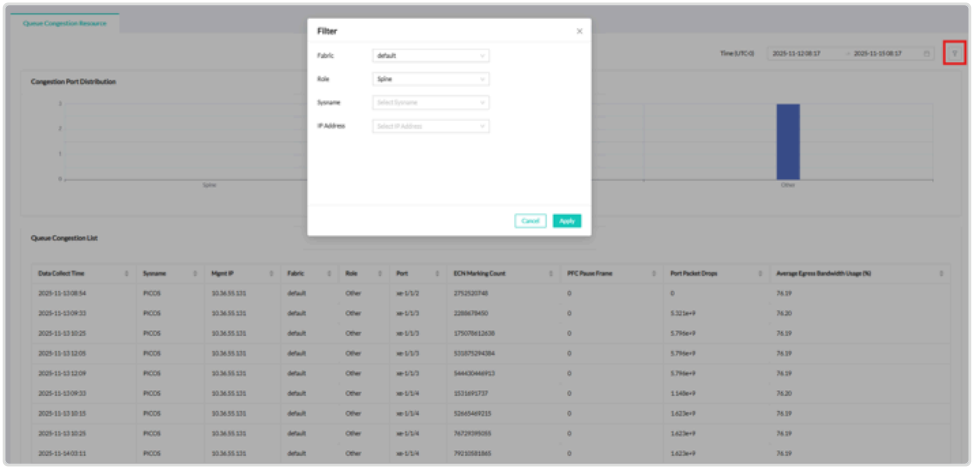
- To specify the time range for the data display, select the start time and end time in the **Time (UTC-0)** section.

> **NOTEs**

- The time in the **Time (UTC-0)** section is based on the **UTC-0** time zone.
- By default, the data for the past 24 hours is displayed.



- To specify the scope of congestion-related data to be displayed, click the filter icon.



Then, in the pop-up window, input one or multiple filter parameters as needed. The following filter parameters are provided:

Table 2. Filter Parameters

Parameter	Description
Fabric	Optional. The fabric to which the switch belongs.
Role	Optional. The role of the switch. Values can be **Spine**, **Leaf**, or **Other**.
Sysname	Optional. The hostname of the switch.
IP Address	Optional. The management IP address of the switch.

Topology

You can use the automatic discovery of topology feature to visualize your switches in all locations and drill down into an individual switch, right to the port level, to check port stats and overall health of the switch.

In addition, you can view real-time or historical information about Linux servers connected to the switch.

See the following child topics:

- Managing Topologies
- Planning Topologies
- Viewing Real-Time Topologies
- Viewing Historical Topologies
- Viewing Switch Details in Topologies

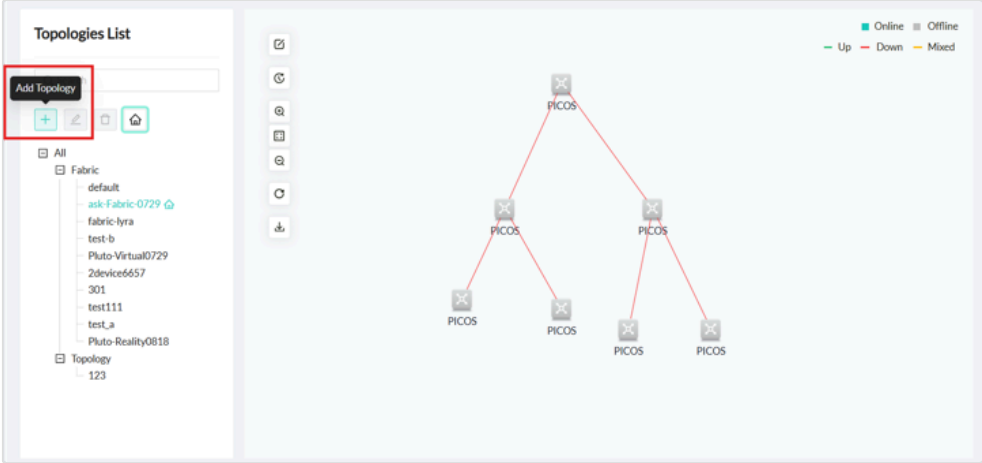
Managing Topologies

Topologies can help you identify and visualize your network structure. You can add, edit, or delete topologies by using the AmpCon-DC UI.

Adding a Topology
Editing a Topology
Deleting a Topology
Setting or Unsetting a Default Topology

Adding a Topology

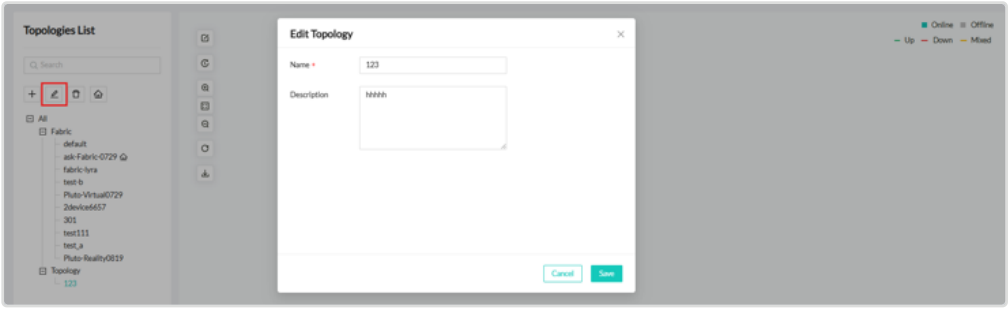
1. In the AmpCon-DC UI, click **Physical Network > Topologies**.
2. In the **Topologies List** section, click the “Add Topology” icon.



3. Enter the topology name and description (optional), and then click **Add**.
4. Wait for the process to complete. Then, you can see the new topology in the topology list.

Editing a Topology

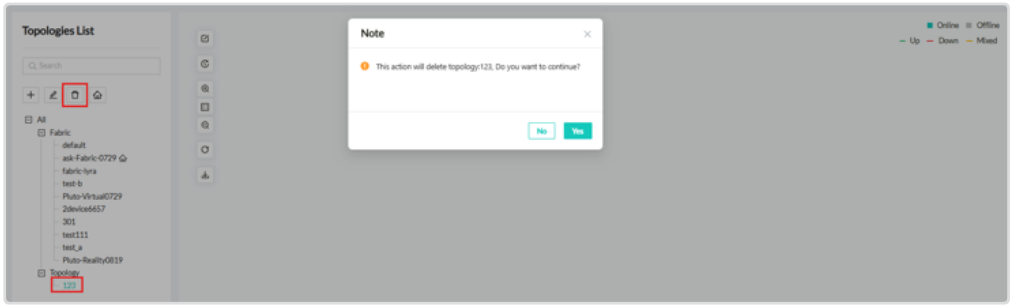
1. Click the topology in the **Topologies List** section, and then click the edit icon.
2. Enter a new name or description, and then click **Save.**



Deleting a Topology

1. Click the topology in the **Topologies List** section, and then click the delete icon.

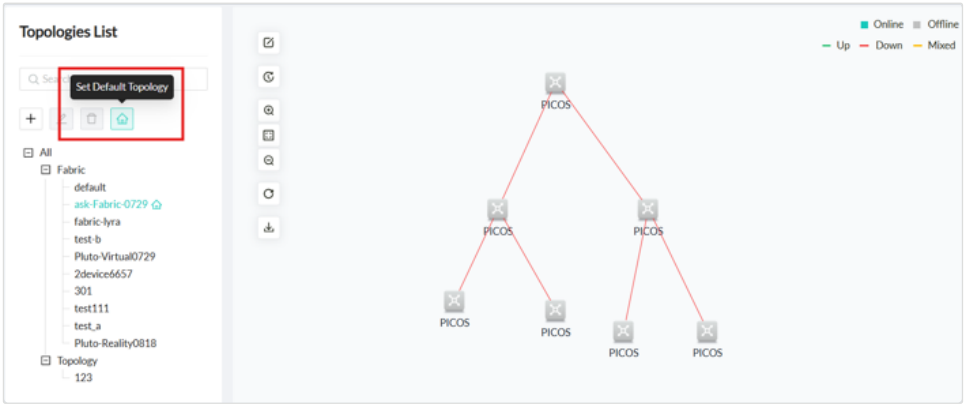
2. In the pop-up window, verify the name of the topology, and then click **Yes** to confirm the deletion.
3. Verify whether the topology is removed from the **Topologies List** section.



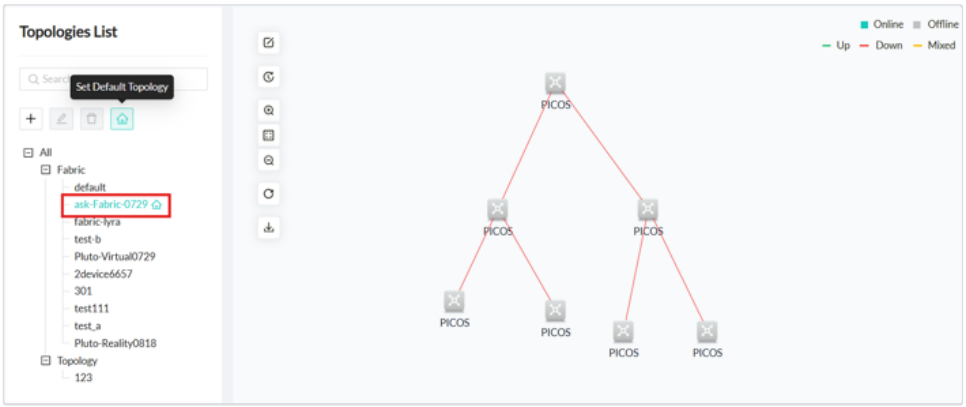
Setting or Unsetting a Default Topology

When you click **Physical Network > Topologies**, the default topology is displayed. To set a default topology, follow these steps:

1. Click a non-default topology, and then click the “Set Default Topology” icon.



2. Verify whether the selected topology is marked with the default icon.



To unset a default topology, click the default topology, and then click the “Set Default Topology” icon again.

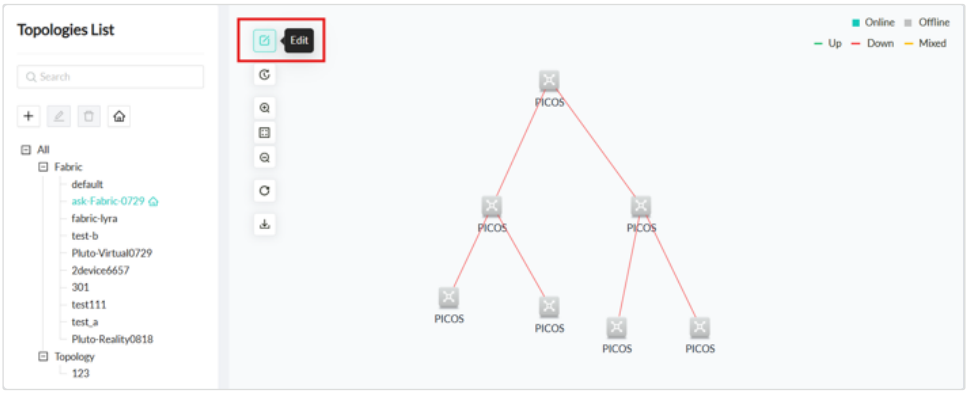
Planning Topologies

You can enter the topology edit mode to customize a topology based on your actual needs.

Entering the Topology Edit Mode
Adding Switches to a Topology
Removing Switches from a Topology
Automatically Discovering Links
Manually Adding Links
Editing Links
Selecting a Topology Layout
Zooming in or out of a Topology
Undoing or Redoing Operations
Saving a Topology
Displaying or Hiding the Legend
Refreshing the Current Topology
Exiting the Topology Edit Mode

Entering the Topology Edit Mode

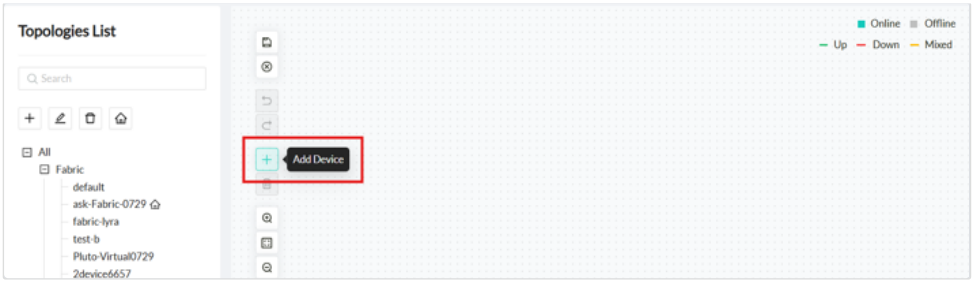
1. In the AmpCon-DC UI, click **Physical Network > Topologies**.
2. Select the topology in the **Topologies List** section to enter the real-time topology mode.
3. Click the "Edit" icon to enter the topology edit mode.



Adding Switches to a Topology

To add switches to a topology, follow these steps:

1. Enter the topology edit mode as described in the last section.
2. Click the topology, and then click the "Add Device" icon.



3. Select the switches that you want to add, and then click **Save**.

Removing Switches from a Topology

To remove switches from a topology, follow these steps:

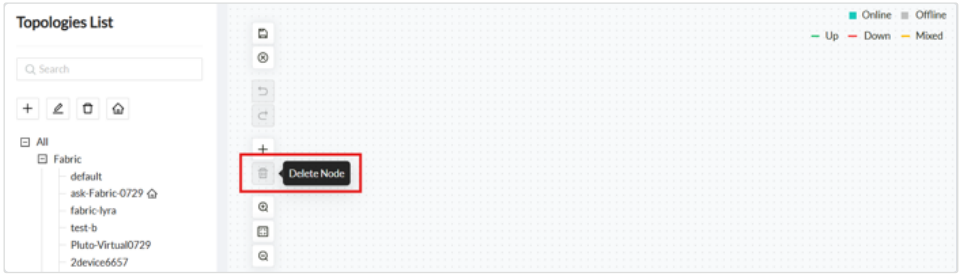
1. Enter the topology edit mode as described in the Entering the Topology Edit Mode section.
2. Remove switches by using either of the following methods:

- **Using the "Add Device" icon**

    1. Click the topology, and then click the "Add Device" icon.
    2. Uncheck the switches that you want to remove, and then click **Save**.

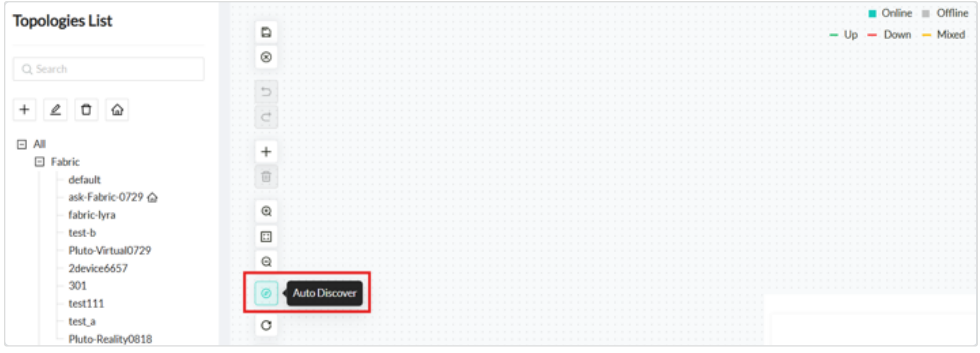
- **Using the “Delete Node” icon**

    Click the topology, and then click the "Delete Node" icon.



Automatically Discovering Links

1. In the topology edit mode, click the "Auto Discover" icon.



2. In the pop-up window, click **Yes** to start the auto-discovery process.

3. Wait for the process to complete. Then, the links in the topology are updated.

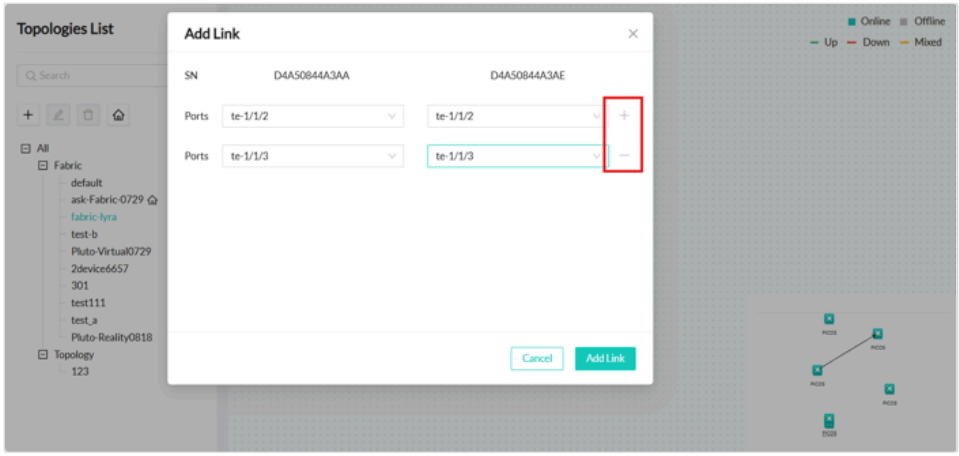
> **NOTE**
>
> The links can be displayed only when the following conditions are met:
>
> - Switches in the topology are connected with each other in the real network.
> - Google Remote Procedure Call (gRPC) is enabled on the switches in the topology. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

Manually Adding Links

To add a link, follow these steps:

1. In the topology edit mode, hover your mouse over a switch until you see a cross symbol.
2. Connect the switch with another switch. Then, you can see an **Add Link** pop-up window.
3. In the **Ports** section, input the connection ports for these two switches.

   Click **+** on the right to add a new port connection, or click **-** to remove a port connection. If a selected port is already in use by another link, a warning is displayed.



4. Click **Add Link**.

   After you add a link and save the topology, the link is displayed in red or green based on real connectivity status:

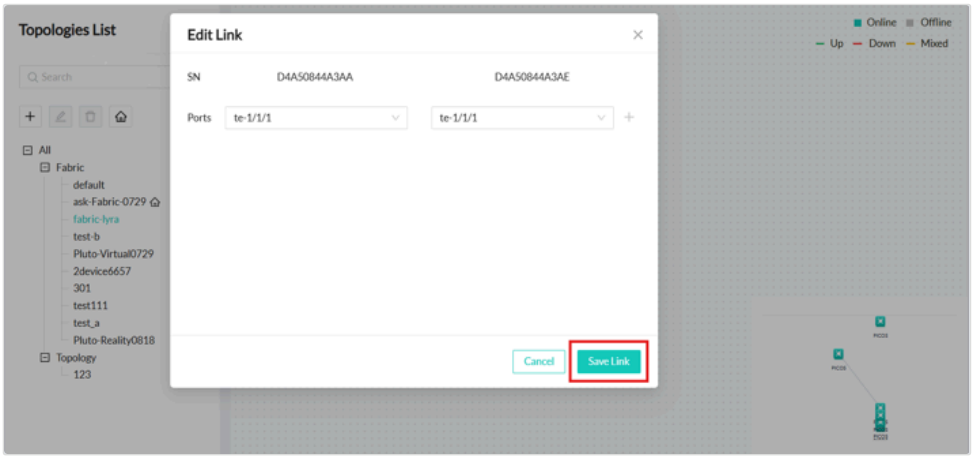
- If the link between these two switches doesn't exist in the real network, the link is marked in red.

- If the link between these two switches exists in the real network, the link is marked in green.

Editing Links

After a link is added, you can edit the link. Follow these steps:

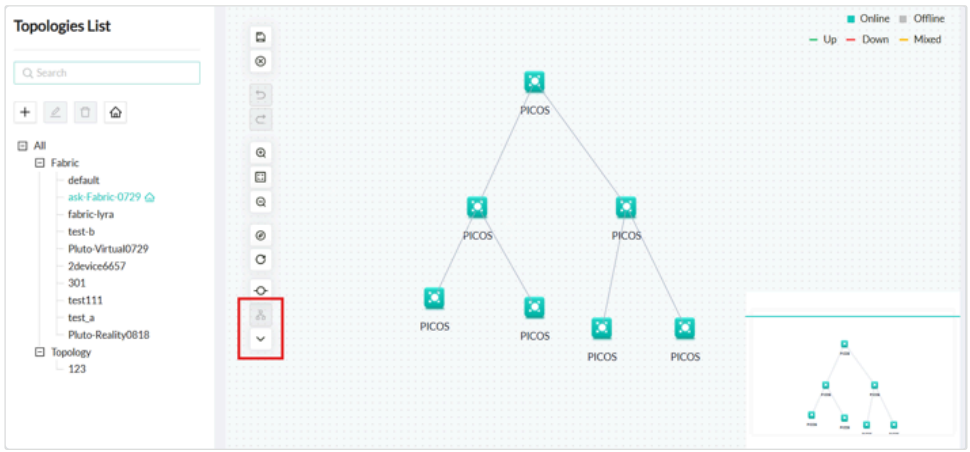
1. Right-click a link, and click **Edit**.
2. In the pop-up window, modify the link as needed.
3. Click **Save Link**.



Selecting a Topology Layout

In the topology edit mode, you can see the topology in the auto hierarchy layout by default. To select a topology layout, follow these steps:

1. Click the arrow below the **Auto Hierarchy Layout** button.



2. Select a layout from the following four layout styles:

- **Auto Hierarchy Layout (Tree Layout)**

  Select a specific switch in the topology, and then click **Auto Hierarchy Layout**. You can see a tree layout with the switch as the root node.

The auto hierarchy layout cannot be applied when no switches are selected or no links exist among switches.

- **Auto Grid Layout**

  If no switches are selected, the grid layout automatically lays out all global elements.

  If some switches are selected, the grid layout is applied only to the selected switches.

- **Auto Circular Layout**

  If no switches are selected, the circular layout automatically lays out all global elements.

  If some devices are selected, the circular layout is applied only to the selected switches.

- **Auto Elliptical Layout**

  If no switches are selected, the elliptical layout automatically lays out all global elements.

  If some switches are selected, the elliptical layout is applied only to the selected switches.

Zooming in or out of a Topology

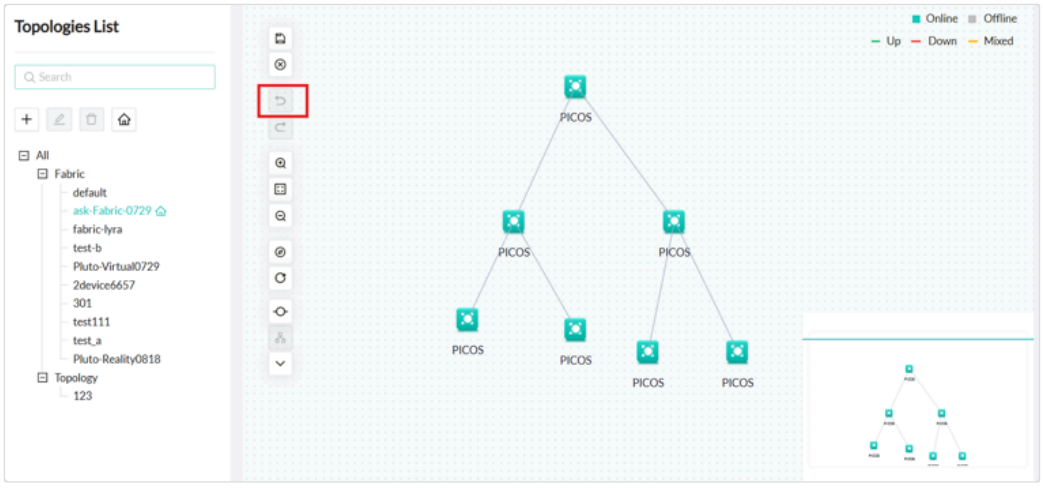
- To zoom in a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and scroll the mouse wheel backward.

Undoing or Redoing Operations

In the topology edit mode, you can undo or redo operations.

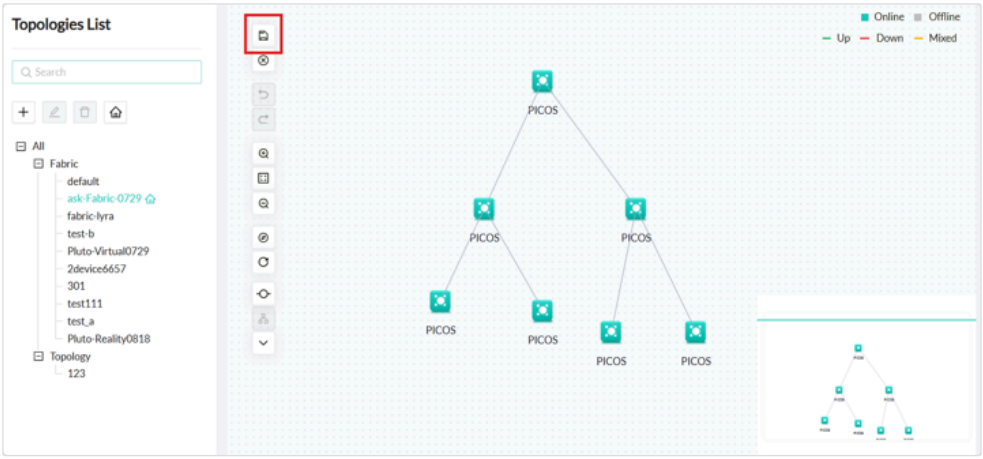
- To revert to the last operation, click **Undo**.
- To redo the last operation, click **Redo**.

If no undo or redo operations are available, these two buttons are grayed out and disabled.



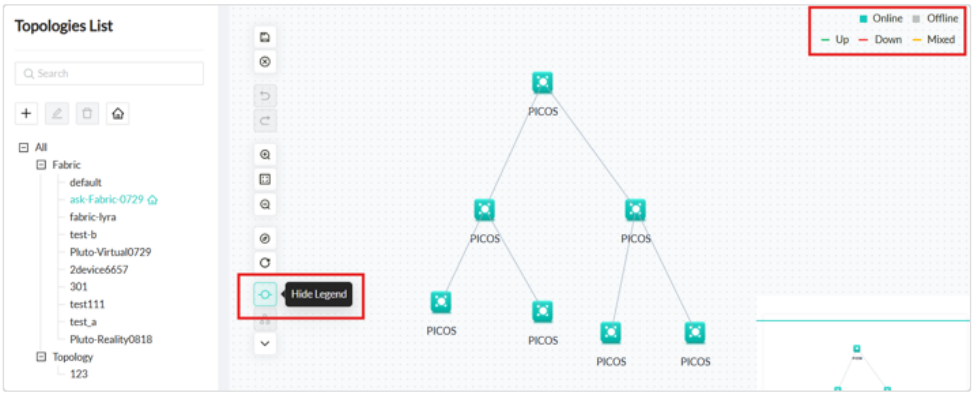
Saving a Topology

1. In the topology edit mode, click **Save** to save the current topology.
2. Wait for the process to complete. After the topology is saved, you will automatically exit the topology edit mode.

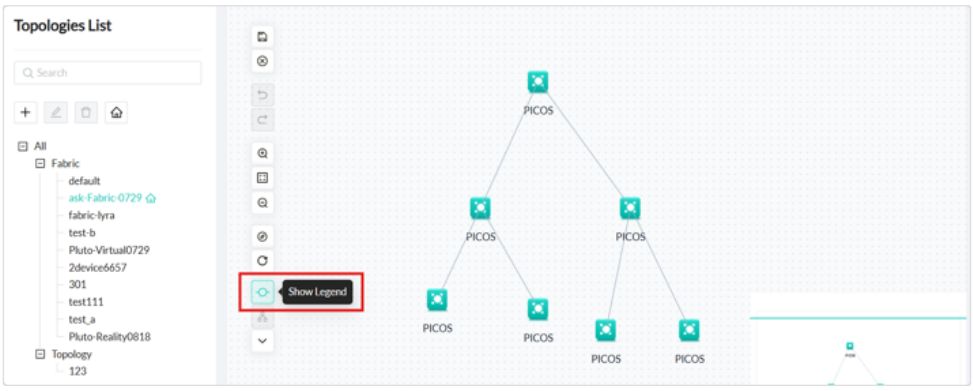


Displaying or Hiding the Legend

- To hide the legend, click the "Hide Legend" icon in the topology edit mode.

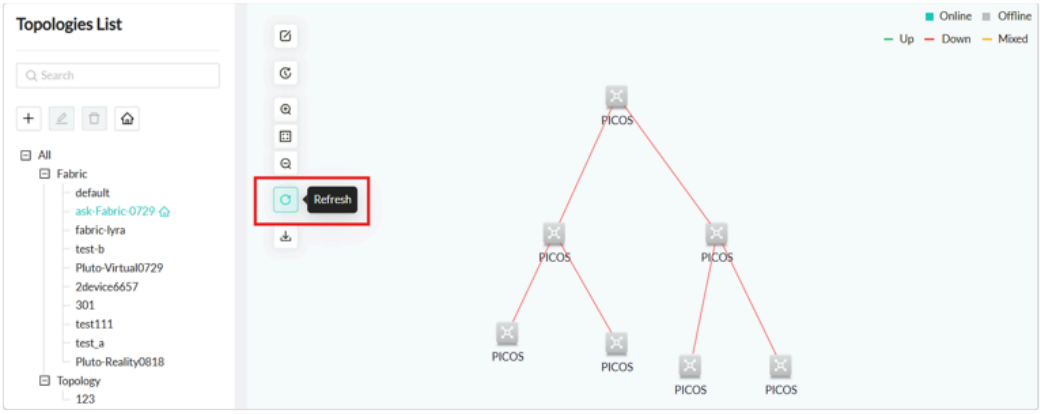


- To show the legend, click the "Show Legend" icon in the topology edit mode.



Refreshing the Current Topology

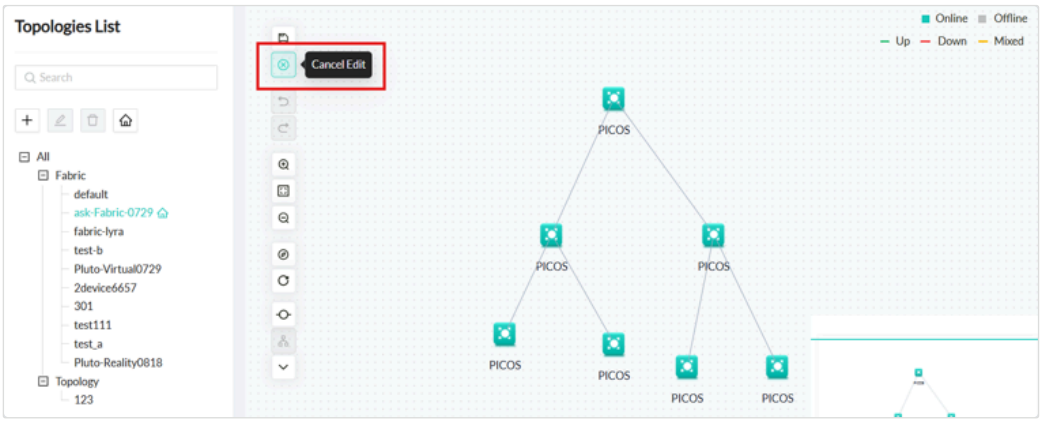
In the topology edit mode, click the "Refresh" icon.



The topology diagram will revert to the last saved state, and any unsaved changes will be lost.

Exiting the Topology Edit Mode

To exit the topology edit mode, click the "Cancel Edit" icon in the topology edit mode.



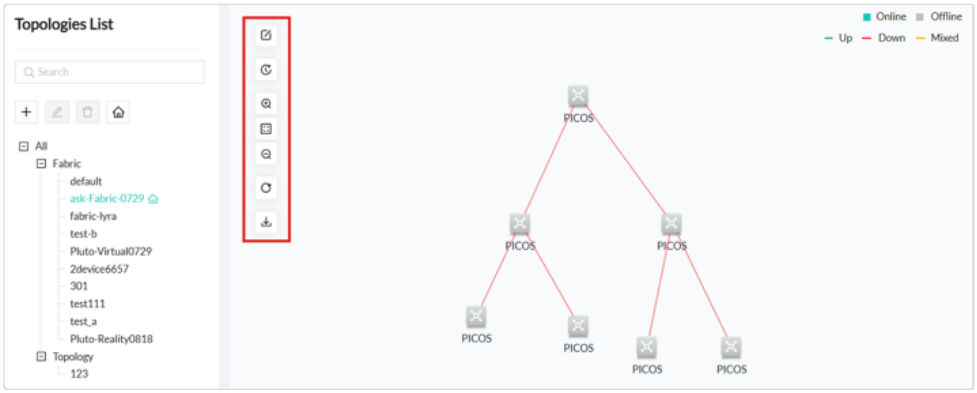
Viewing Real-Time Topologies

You can enter the real-time topology mode to view real-time network status such as switch status and link faults. By clicking a switch or a link, you can see detailed stats information.

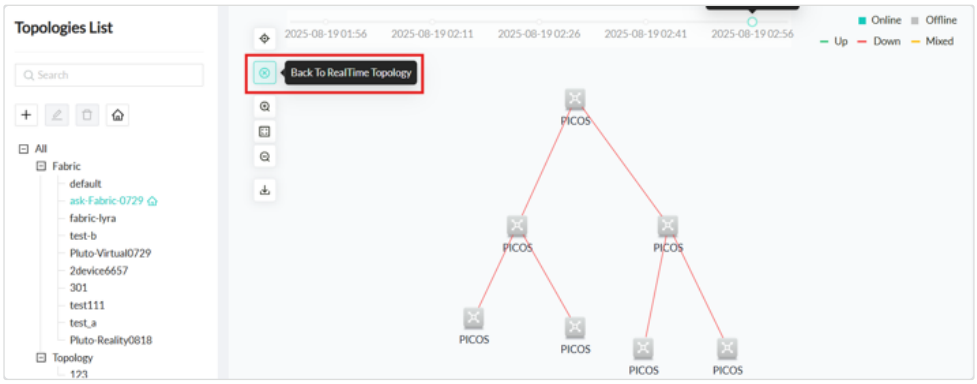
Entering the Real-Time Topology mode
Refreshing the Topology
Zooming in or out of a Topology
Exporting a Topology

Entering the Real-Time Topology mode

1. In the AmpCon-DC UI, click **Physical Network > Topologies**.
2. Click the topology in the **Topologies List** section, and then you enter the real-time topology mode automatically.

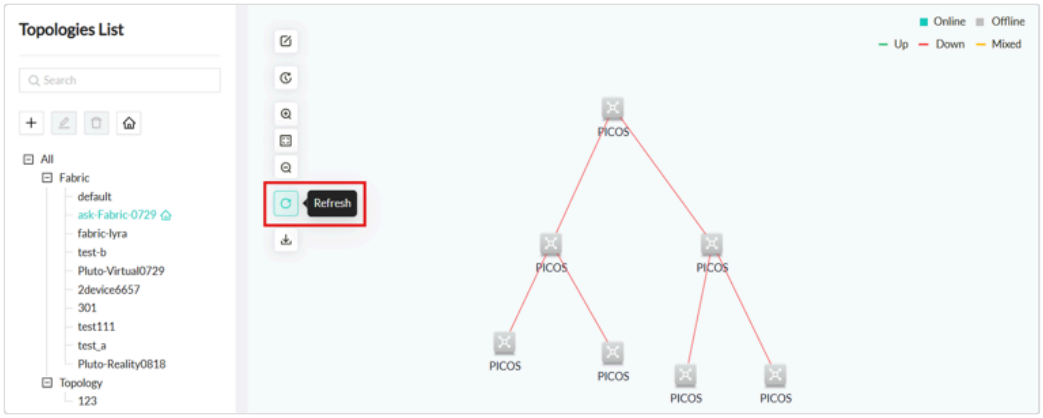


> **NOTE**
>
> If you are in the historical topology mode, click the “Back To Real-Time Topology” icon to return to the real-time topology mode.



Refreshing the Topology

In the real-time topology mode, click the "Refresh" icon.

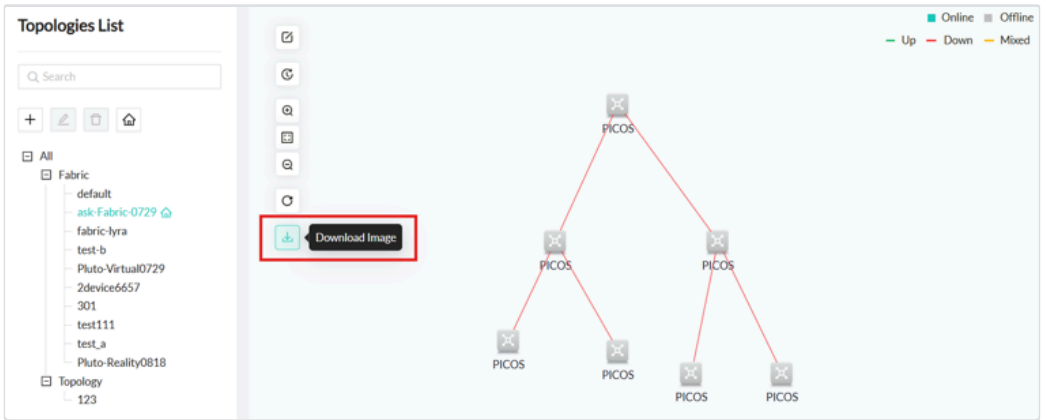


Zooming in or out of a Topology

- To zoom in a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology diagram, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel backward.

Exporting a Topology

In the real-time topology mode, click the "Download Image" icon. You can view the exported topology in the download history of your browser.



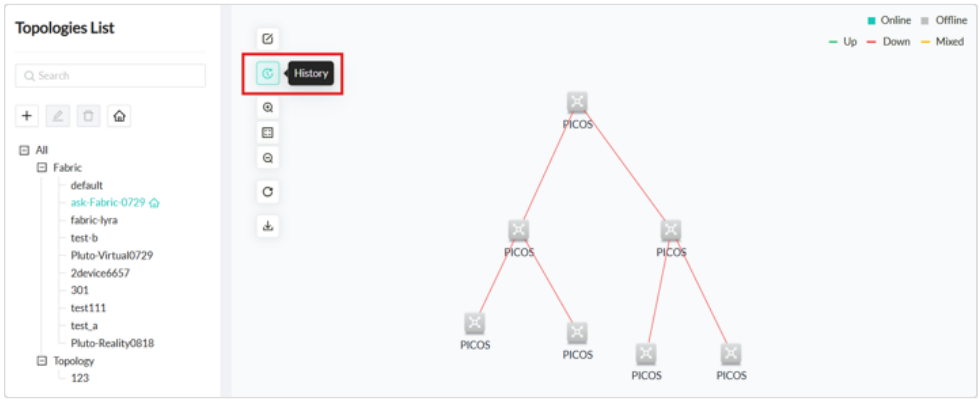
Viewing Historical Topologies

You can enter the historical topology mode to view the network status at different time or analyze the historical topology to trace problems.

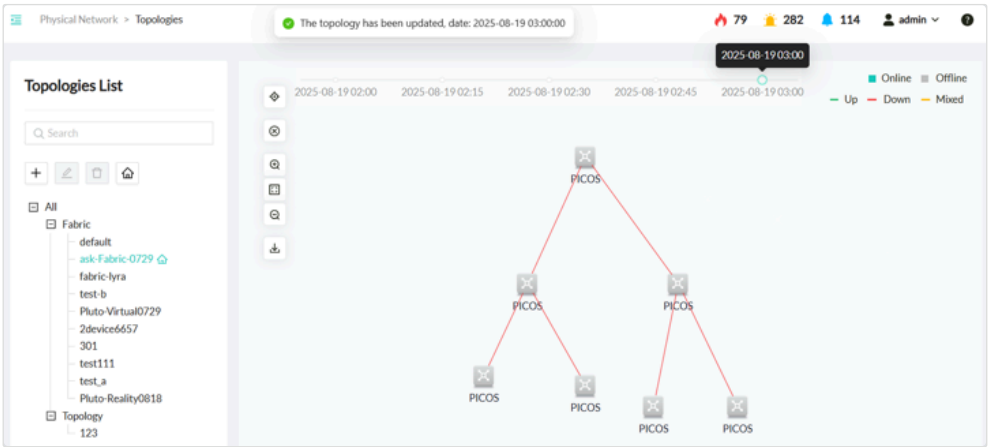
Viewing a Historical Topology
Zooming in or out of a Topology
Exporting a Topology
Returning to the Real-Time Topology Mode

Viewing a Historical Topology

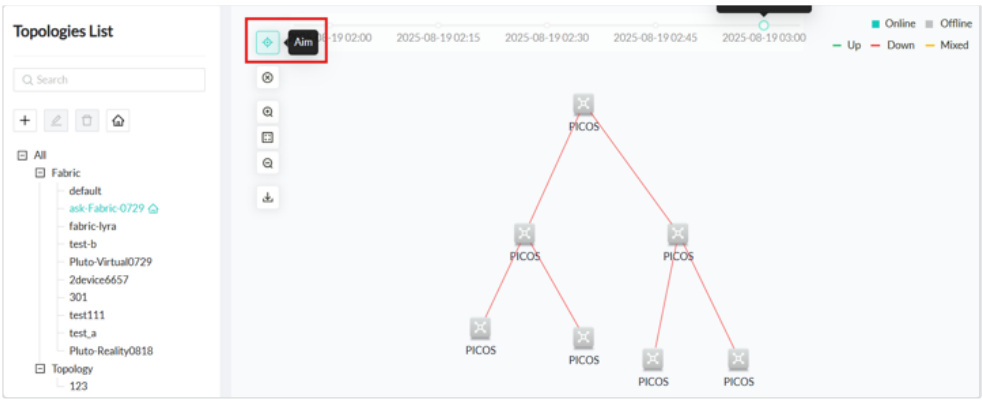
1. In the AmpCon-DC UI, click **Physical Network > Topologies**.
2. Click the topology in the **Topologies List** section, and then you enter the real-time topology mode automatically.
3. To enter the historical topology mode, click the "History" icon.



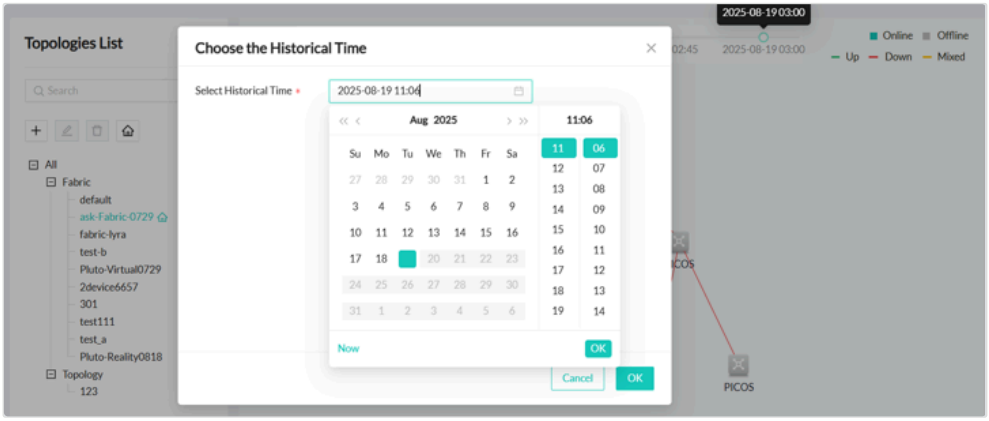
Then, you can see the historical topology as follows:



4. In the historical topology mode, click the "Aim" icon.



5. Modify the time in the pop-up window, and click **OK**.



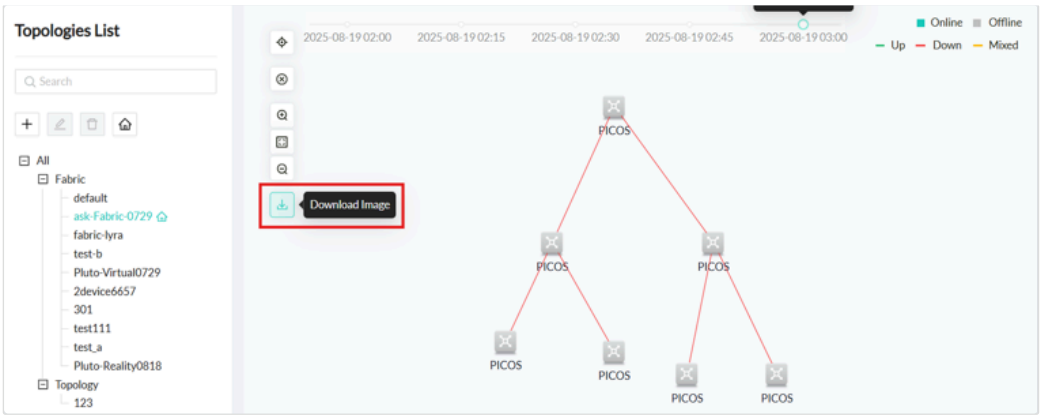
6. After the topology is loaded completely, the topology shows the state at the selected time point. The timeline shows 35 minutes forward or backward from that time point.
7. Click the time points in the timeline to view historical topologies at different time.

Zooming in or out of a Topology

- To zoom in a topology, hover the mouse over the topology, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel forward.
- To zoom out of a topology, hover the mouse over the topology, hold down the **Ctrl** key on the keyboard, and then scroll the mouse wheel backward.

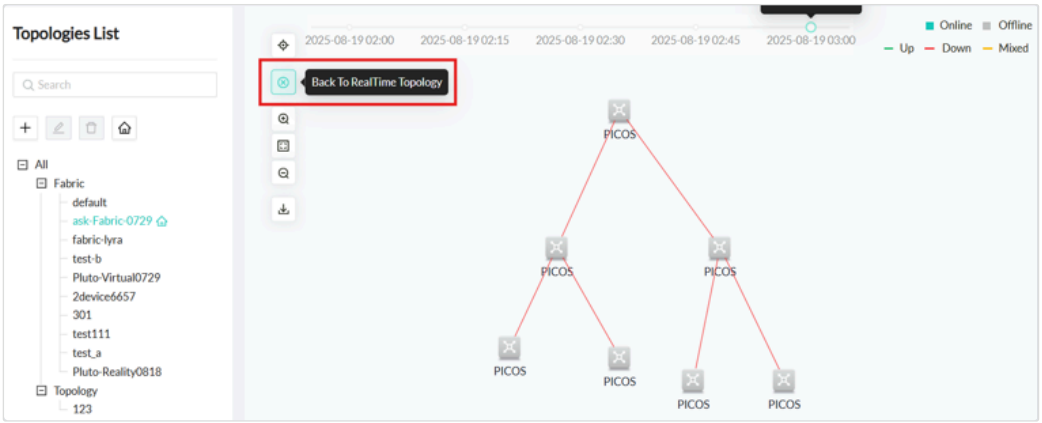
Exporting a Topology

In the historical topology mode, click the "Download Image" icon. You can view the exported topology in the download history of your browser.



Returning to the Real-Time Topology Mode

In the historical topology mode, click the “Back To Real-Time Topology” icon to leave the historical mode.



Viewing Switch Details in Topologies

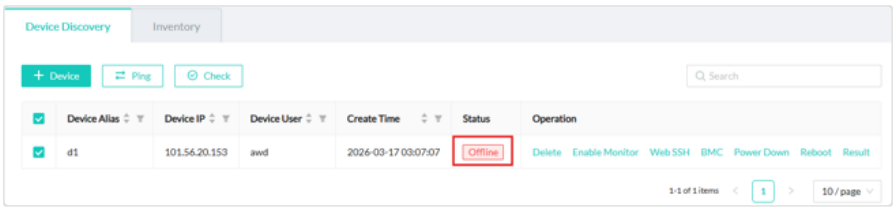
When you click a switch in a topology, you can view real-time or historical information about the switch, switch ports, and Linux servers connected to the switch.

Prerequisites
Viewing Real-time or Historical Data
Device Info
Port Info
Host Info

Prerequisites

To check the Linux servers connected to managed switches in a topology, ensure that the following prerequisites are met:

- The Linux servers to be managed are added to AmpCon-DC with the monitor function enabled. For more information, see Adding a Device to AmpCon-DC.
- The Linux servers to be managed are connected to the AmpCon-DC server. You can check by following these steps:
  1. Click **Device > Hosts > Device Discovery**.
  2. Select the Linux servers to be managed, and then click **Ping**.
  3. Check whether the status is shown as **Online** in the **Status** column.



Viewing Real-time or Historical Data

To view real-time switch details, switch ports, and Linux servers, enter the real-time topology mode, and then click the switch to be monitored.

To view historical switch details, switch ports, and Linux servers, enter the historical topology mode, and then click the switch to be monitored.

Then, you can see the following sections in the topology:

Device Info

In the **Device Info** section, you can see the following switch-related information:

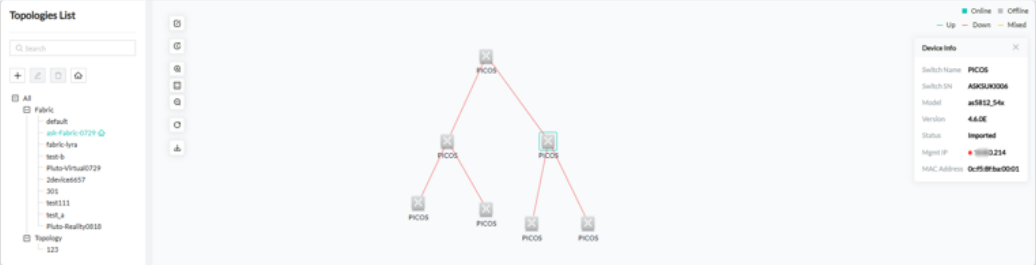


Table 1. Device Info Metrics

Metric	Description
Switch Name	The name of the switch.
Switch SN	The SN of the switch.
Model	The model of the switch.
Version	The PicOS version of the switch.
State	The state of the switch. The following switch states are supported: • **Imported:** The switch is imported to AmpCon-DC. • **Provisioning Success:** The switch is deployed by using AmpCon-DC. • **Configured:** After you add a switch configuration, the switch is in **Configured** status. • **Staged:** After you stage a switch, the switch is in **Staged** status. • **Registered:** The switch has registered with AmpCon-DC but hasn't been deployed completely. • **Provisioning Failed:** The switch fails to be deployed by using AmpCon-DC. • **DECOM:** The deployed switch is decommissioned (DECOM) when it's online. • **DECOM-Manual:** The deployed switch is decommissioned when it's offline. • **RMA:** The switch is replaced with another switch of the same switch model by using Return Merchandise Authorization (RMA).

Mgmt IP	The management IP address of the switch.

Port Info

In the **Port Info** section, you can see the following port-related metrics:



Table 2. Port Info Metrics

Metric	Description
Port Name	The name of the switch port
Port State	The state of the switch port, up or down
Port Speed	The maximum data transfer rate that the port can support
In Octets	The number of octets (8-bit bytes) received by the switch port
In Pkts	The number of incoming packets received by the switch port
In Discards	The number of incoming packets that the switch port intentionally discards (drops) during processing
In Errors	The number of incoming packets that contain errors and are dropped by the switch port
Out Octets	The number of octets (8-bit bytes) transmitted out of the switch port
Out Pkts	The number of outgoing packets transmitted by the switch port
Out Discards	The number of outgoing packets that the switch port intentionally discards (drops) before they are

	transmitted
Out Errors	The number of outgoing packets that the switch port fails to transmit successfully due to errors

Host Info

In the **Host Info** section, you can see the following metrics for Linux servers connected to the switch:

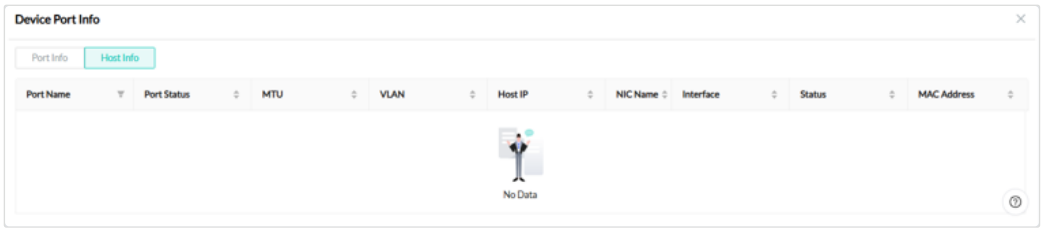


Table 3. Host Info Metrics

Metric	Description
Port Name	The name of the switch port
Port State	The state of the switch port, up or down
MTU	The largest size (measured in bytes) of a packet or frame that can be sent in a single network transmission
Vlan	The VLAN of the Linux server
Host IP	The IP address of the Linux server
NIC Name	The name to distinguish the network interface card (NIC) of the Linux server
Interface	The Ethernet port to which the Linux server is connected
Status	The status of the Ethernet port to which the Linux server is connected
MAC Address	The MAC address of the Linux server

NICs

You can view basic information and metrics of NICs and connected modules on added third-party devices to evaluate network performance, diagnose issues, and thus ensure optimal network performance.

See the following child topics:

- NIC Inventory
- Module Inventory

NIC Inventory

After you add devices to AmpCon-DC with the monitor function enabled, AmpCon-DC automatically monitors Network Interface Cards (NICs) on these devices.

You can have an overall understanding of NICs in your network, ensure NICs work well, and prevent network failures.

This feature supports Nvidia and Broadcom NICs on Linux servers. For the list of supported NICs, see Supported NICs.

Prerequisites
Viewing NIC Data
Exporting NIC Data
Refreshing the Inventory List

Prerequisites

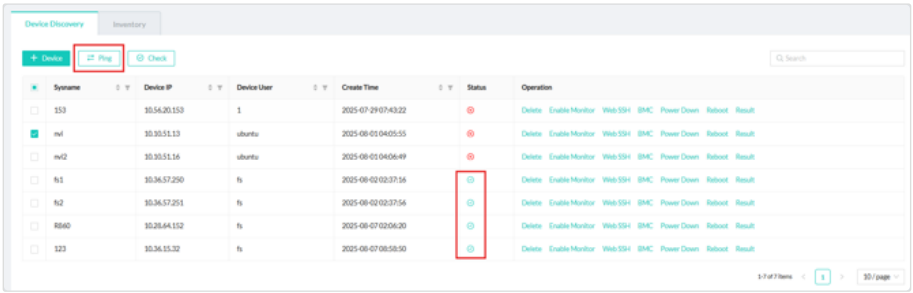
Ensure that the following prerequisites are met:

- The terminal devices are added with the monitor function enabled and with an administrator user of the device specified. For more information, see Adding a Device to AmpCon-DC.
- The port 9100 is not be blocked on the added device.
- The devices to be managed are connected to the AmpCon-DC server. You can check by following these steps:

  a. Click **Device > Hosts > Device Discovery**.

  b. Select the devices to be managed, and then click **Ping**.

  c. Check whether the status is shown as ✔ in the **Status** column.



Viewing NIC Data

Click **Device > NICs > Inventory** in the AmpCon-DC UI. You can see the list of all monitored devices.

To check detailed NIC information of a specific device, click **+** before the device. Then, you can see the following metrics:

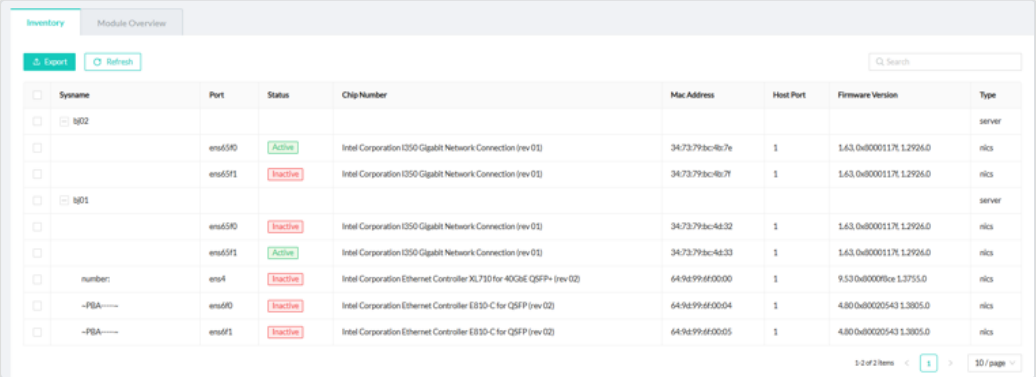
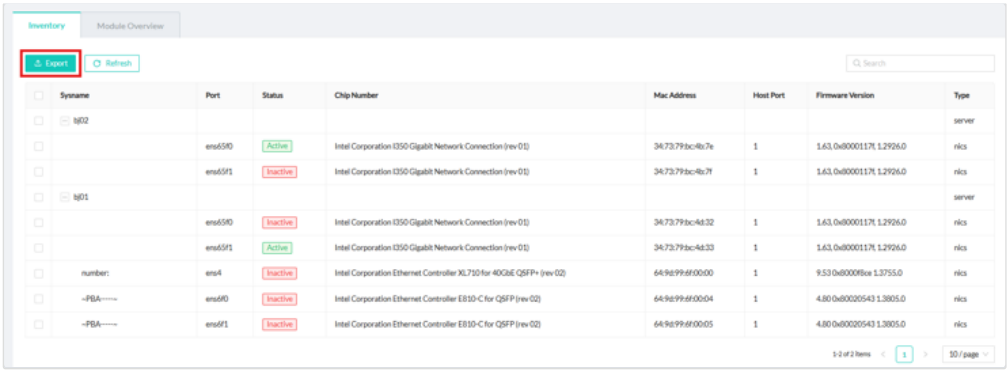


Table 1. NIC Metrics

Metric	Description
Sysname	The name of a device or a NIC
Port	The name of the Ethernet port
Status	The state of the Ethernet port, **up** or **down**
Chip Number	The chip number of the NIC
Mac Address	The MAC address of the Ethernet port
Host Port	The number of ports on the NIC interface
Firmware Version	The firmware version of the NIC
Type	The type of the item in the list, **server** or **nics**

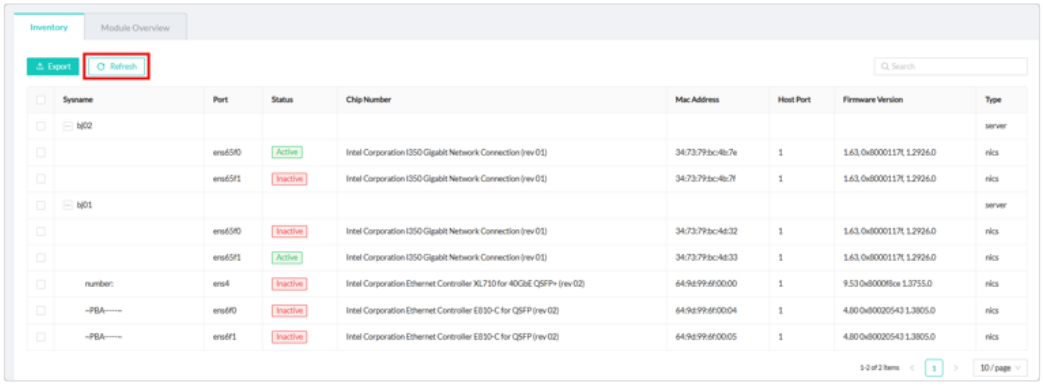
Exporting NIC Data

- To export the data of some specific NICs on a device, select the NICs by clicking the square before each NIC name, and then click **Export**.
- To export the data of all NICs on a device, click the square before the device name, and then click **Export**.
- To export the data of all NICs on all devices, click the square before each device name, and then click **Export**.



Refreshing the Inventory List

To refresh the inventory list, click **Refresh**.



Module Inventory

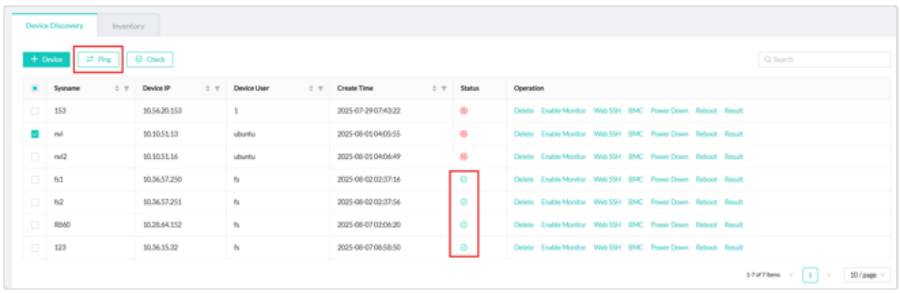
After you add devices to AmpCon-DC with the monitor feature enabled, you can view detailed information of optical modules connected to the devices.

Prerequisites
Procedure

Prerequisites

Ensure that the following prerequisites are met:

- The devices to be managed are added to AmpCon-DC with the monitor function enabled. For more information, see Adding a Device to AmpCon-DC.
- The devices to be managed are connected to the AmpCon-DC server. You can check by following these steps:
  1. Click **Device > Hosts > Device Discovery**.
  2. Select the devices to be managed, and then click **Ping**.
  3. Check whether the status is shown as ✔ in the **Status** column.



Procedure

1. Click **Device > NICs > Module Overview** in the AmpCon-DC UI. You can see the list of devices that are added with the monitor feature enabled and connected to the AmpCon-DC server.
2. Click **+** before a device. You can see detailed information of optical modules connected to the device.

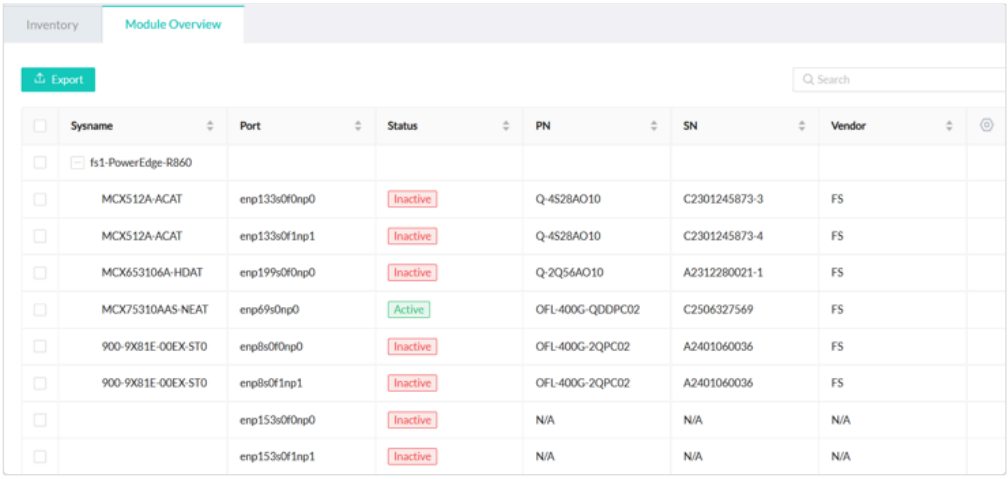
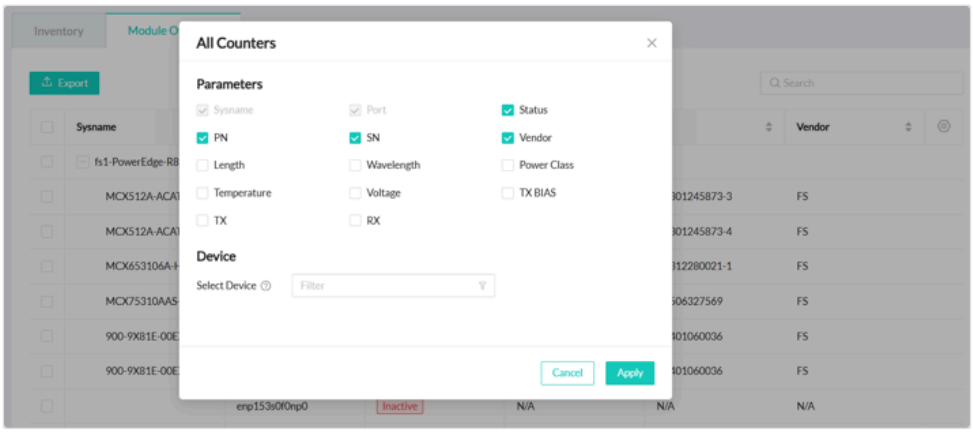


Table 1. Module Metrics

Metric	Description
Sysname	The name of the device or the NIC
Port	The Ethernet port connected to the optical module
Status	The status of the module, **Active** or **Inactive**
PN	The vendor part number to distinguish the type and model of the optical module
SN	The serial number of the optical module
Vendor	The supplier or manufacturer of the optical module
Length	The maximum distance over which an optical signal can be transmitted effectively through the module
Wavelength	The wavelength of the light used in the optical module
Power Class	The power consumption or optical power output classification of the optical module
Temperature	The operating temperature range of the optical module
Voltage	The voltage level required to power the optical module
Bias	The bias current applied to the laser diode in the transmitter (Tx) section of the optical module

Tx Power	The transmitter section of the optical module
Rx Power	The receiver section of the optical module

3. To specify the metrics to be monitored, click the **All Counters** icon, select the metrics in the **Parameters** section, and then click **OK**.
4. To specify the devices and NICs to be monitored, click the **All Counters** icon, select the devices and NICs, and then click **Apply**.



Splunk Integration

Splunk is a leading platform for operational intelligence. Splunk searches, monitors, analyzes, and visualizes device data. AmpCon-DC supports integrating with Splunk, providing a fast, easy, and secure way to analyze alerts and system logs and turn them into detailed insights.

You can use this feature to achieve the following goals:

- Access the Splunk UI from the AmpCon-DC UI, enabling fluid platform switching.
- Send alerts from AmpCon-DC to Splunk, and view or analyze these alerts in the Splunk UI.
- Send AmpCon-DC system logs to Splunk, and view or analyze these logs in the Splunk UI.

See the following child topics:

- Splunk Integration Overview
- Accessing the Splunk UI
- Sending Logs to Splunk
- Troubleshooting Splunk Integration

Splunk Integration Overview

By integrating AmpCon-DC with Splunk, you can use powerful functions of Splunk to monitor and analyze alerts and system logs.

- Background
- Use Cases
- Architecture

Background

In modern data centers, networks play a critical role in delivering reliable services. To address the ever-increasing demands of network reliability, AmpCon-DC analyzes telemetry data and issues an immediate alert when a device failure or a performance shift is detected. In addition, AmpCon-DC system logs are generated to track the health of the AmpCon-DC platform.

To take advantage of these alerts and system logs, network administrators need a powerful visualization and analysis platform to deliver more detailed insights and make informed decisions.

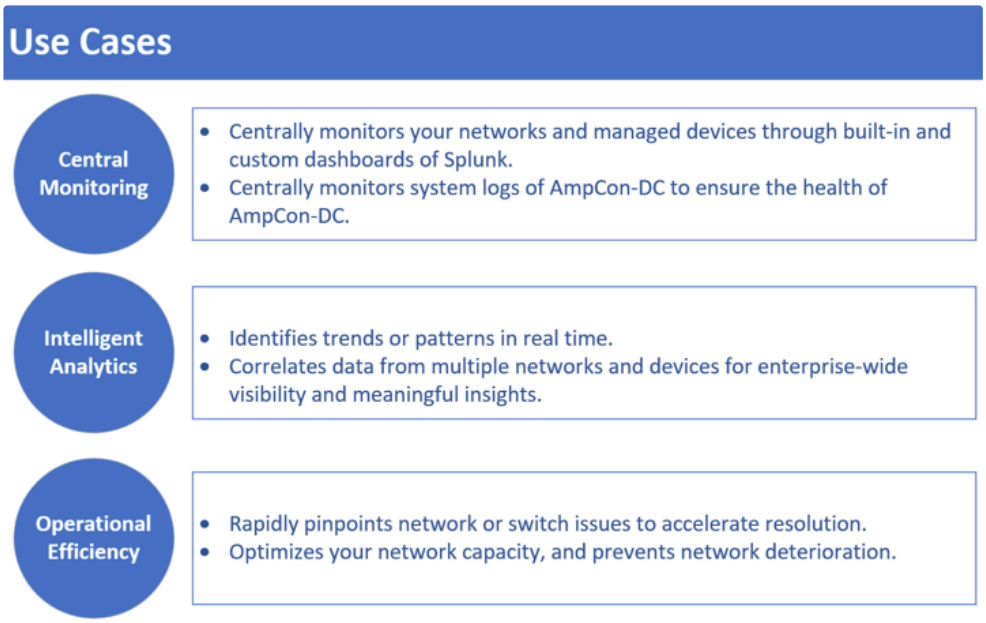
Splunk is a leading platform for operational intelligence. Splunk searches, monitors, analyzes, and visualizes device data. AmpCon-DC supports integrating with Splunk to help visualize and analyze alerts and system logs.

Splunk allows you to create custom reports and dashboards for multi-dimensional visualization and analysis. In addition, Splunk can correlate data from different devices, helping you gain comprehensive insights and quickly identify root causes.

Use Cases

Check the following use cases of the Splunk integration feature:

Figure 1. Integration Use Cases



Architecture

The architecture of the Splunk integration in AmpCon-DC is as follows:

Figure 2. Splunk Integration Architecture



- AmpCon-DC uses webhooks to send alerts to Splunk. By using webhooks, AmpCon-DC pushes data only when new alerts are triggered. Splunk uses HTTP Event Collector (HEC) to receive data from AmpCon-DC. HEC uses a token-based authentication model.

  You can generate an Event Collector token and then configure AmpCon-DC with the token to send data to HEC.

Splunk parses the received alerts, stores them to the Splunk database, and displays them in the Splunk UI.

- AmpCon-DC uses the UDP or TCP protocol to send AmpCon-DC system logs to Splunk.

  You can configure the UDP or TCP port on Splunk and then add Syslog configurations containing the TCP or UDP port to AmpCon-DC. AmpCon-DC will send system logs to Splunk through the port.

  Splunk listens on the TCP or UDP port, parses the received system logs, stores them to the Splunk database, and displays them in the Splunk UI.

Accessing the Splunk UI

By adding Splunk integrations to AmpCon-DC, you can access the Splunk UI from the AmpCon-DC UI, enabling fluid platform switching.

- Prerequisites
- Procedure
  - 1. Adding Splunk Integrations
  - 2. Accessing the Splunk UI
- Optional Operations
  - Checking Webhook Logs
  - Editing an Integration
  - Deleting an Integration
- Troubleshooting

Prerequisites

- Make your Splunk environment (Splunk Cloud Platform or Splunk Enterprise) ready.
- Obtain the IPv4 address and port of the Splunk server.
- Obtain the username and password used to log in to the Splunk UI.

Procedure

1. Adding Splunk Integrations

To access the Splunk UI, you need to add a Splunk integration first. Follow these steps:

1. Click **Monitor > Splunk Integration** from the navigation bar.
2. On the “Splunk Integration” page, click **+ Splunk Integration**.
3. In the pop-up window, input the following information:



Table 1. Splunk Integration Parameters

Parameter	Description

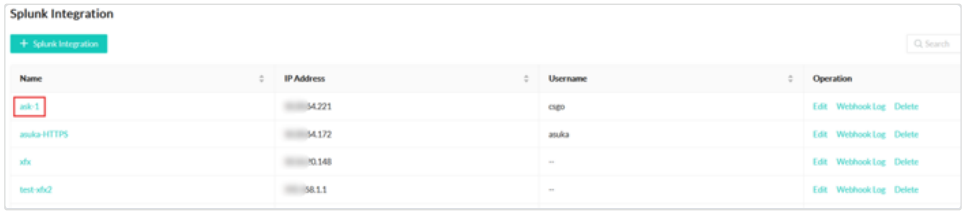
Name	The name of the Splunk integration. **NOTEs** • The name needs to be unique. • The name can contain only uppercase and lowercase letters and numbers. Spaces and special characters are not supported. • The name can contain 64 characters at most. • The name is not case-sensitive.
Protocol	The protocol used by Splunk, **HTTP** or **HTTPS**.
IP Address	The IPv4 address of the Splunk server.
Port	The port of the Splunk server. The port must be an integer between 1 and 65535.
Username	Optional. The username used to log in to the Splunk UI. **NOTEs** • The username can contain only uppercase and lowercase letters, numbers, and underscores (_). • The username must start with letters. • The username needs to contain 4 characters at least.
Password	Optional. The password related to the username.

4. Click **Apply**.

2. Accessing the Splunk UI

After you add a Splunk integration, you can access the Splunk UI from AmpCon-DC. Follow these steps:

1. On the “Splunk Integration” page, locate the integration, and then click the integration name.



   You can see a Splunk login page displayed in a new browser tab.

2. Enter the username and password to log in to the Splunk UI, and click **Sign in**.

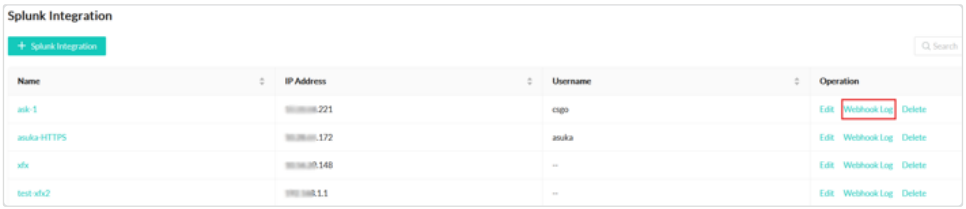
   Then, you are logged in to the Splunk UI.

Optional Operations

Checking Webhook Logs

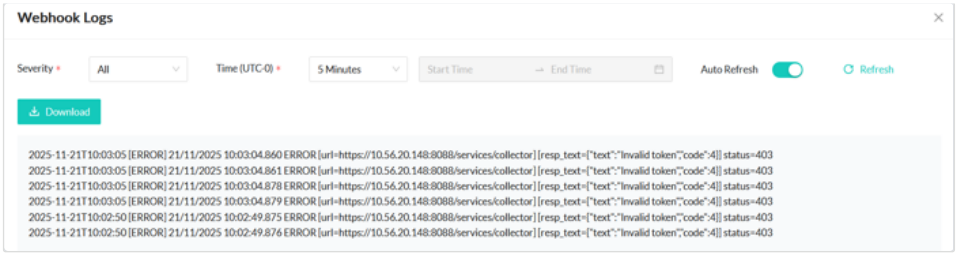
After you add a Splunk integration, you can view webhook logs to check whether the integration is working. Follow these steps:

1. Add a receiver containing webhook configurations of the Splunk server, and configure notification rules for the receiver. For more information, see 3. Adding a Receiver to AmpCon-DC and 4. Adding Notification Rules.
2. On the “Splunk Integration” page, locate the integration, and then click **Webhook Log**.



   In the pop-up window, you can see the webhook logs in the last 5 minutes by default.

> **NOTE**
>
> For meanings of HTTP status codes in log messages, see Possible error codes.



3. In the pop-up window, select the severity, time, and the log refreshing method.

Table 2. Log Parameters

Parameter	Description
Severity	Select the severity of the webhook logs to be displayed, including **Info**, **Error**, and **All**.
Time	Select the time range of the webhook logs to be displayed. Use one of the following ways: • Select a time range such as **5 Minutes**, which means displaying the webhook logs in the last 5 minutes. • Select **Custom** from the drop-down list, and then select the start time and end time, which means displaying the webhook logs between these two custom time points. **NOTEs** • Only when you select **Custom** from the drop-down list, the start time and end time can be configured. • If you select **Custom**, you must select the start time and end time.
Auto Refresh	Toggle it on to enable the automatic log refresh function. Then, the displayed webhook logs are refreshed automatically every 10 seconds. If this function is disabled, the displayed webhook logs will not be refreshed automatically.

	NOTE After you select the start time and end time in the **Time** section, the automatic log refresh function can't be enabled.
Refresh	Click **Refresh** to manually refresh webhook logs.

4. Optional: To download the currently displayed webhook logs, click **Download**.

Editing an Integration

To edit an integration, locate the integration on the "Splunk Integration" page, and then click **Edit**.



Deleting an Integration

To delete an integration, locate the integration on the "Splunk Integration" page, and then click **Delete**.



Troubleshooting

If you fail to access the Splunk UI from the AmpCon-DC UI, see Troubleshooting: Failing to Access the Splunk UI for solutions.

If you fail to view webhook logs, see Troubleshooting: Failing to View Webhook Logs for solutions.

Sending Logs to Splunk

You can send real-time AmpCon-DC system logs to Splunk by adding Syslog configurations. Then, you can view and analyze these logs in the Splunk UI.

Prerequisites
Procedure
1. Configuring a TCP or UDP Port on Splunk
2. Adding Syslog Configurations to AmpCon-DC
3. Viewing System Logs on Splunk
Optional: Deleting a Syslog Configuration
Troubleshooting

Prerequisites

Ensure that the Syslog service on the Splunk server is enabled.

Procedure

1. Configuring a TCP or UDP Port on Splunk

To send AmpCon-DC system logs to Splunk, you must configure Splunk to listen on a TCP or UDP port. Follow these steps:

1. Log in to the Splunk UI with the username and password of an admin account.
2. From the top menu, select **Settings > Data Inputs**.
3. Under **Local Inputs**, select **TCP** or **UDP**.
4. Click **New Local TCP** on the “TCP” page, or click **New Local UDP** on the “UDP” page.
5. Click **TCP** or **UDP** to select a TCP or UDP input. In the **Port** field, enter a port number for TCP or UDP.

   The TCP or UDP port will be used by AmpCon-DC to send system logs to Splunk.

   For other parameters, see Splunk Document.
6. Click **Next**. On the “Input Settings” page, configure as needed.
7. Click **Review**, and then double check your configurations.
8. Click **Submit**.

2. Adding Syslog Configurations to AmpCon-DC

1. Log in to the AmpCon-DC UI, and then click **Device > Device Profiles** from the navigation bar.
2. Click the **System Configuration** tab, and then click **Syslog Config**.

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

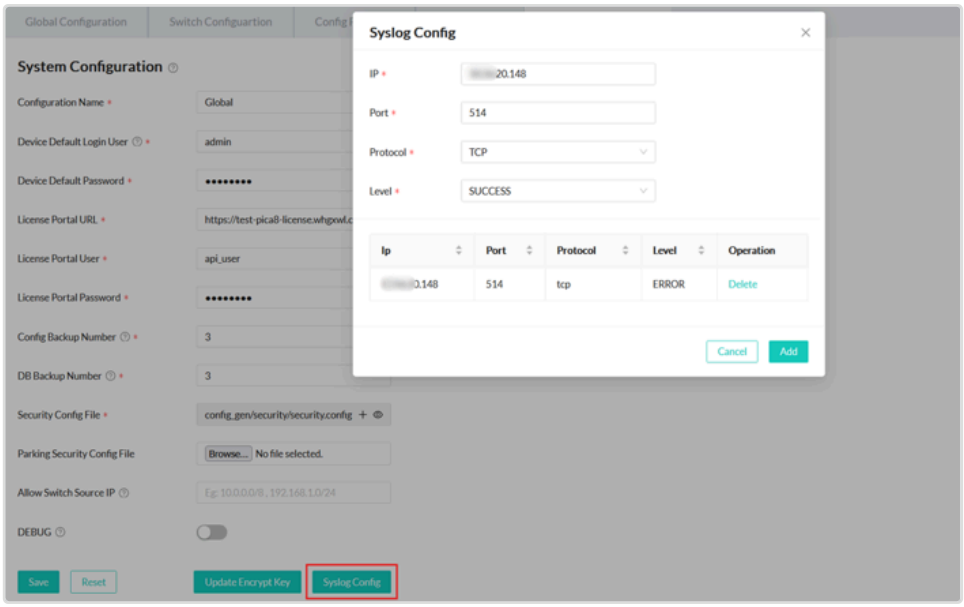


Table 1. Syslog Configuration Parameters

Parameter	Description
IP	The IPv4 address of the Splunk server.
Port	The port number specified in **Step 5** of Configuring a TCP or UDP Port on Splunk. **NOTE** Ensure that the following conditions are met. Or else, AmpCon-DC system logs will fail to be sent to Splunk. • The TCP or UDP port is allowed on Splunk. • The port is consistent with the port number configured on Splunk.
Protocol	The protocol that you configured on Splunk, **TCP** or **UDP**. **NOTE** Ensure that the following conditions are met. Or else, AmpCon-DC system logs

	will fail to be sent to Splunk. • The protocol is configured on Splunk. • The protocol matches with the port number.
Level	The AmpCon-DC log levels to be sent to Splunk, **SUCCESS** or **ERROR**. • **SUCCESS:** Sents AmpCon-DC system logs with a **warning (level=4)** level or higher to Splunk. • **ERROR:** Sents AmpCon-DC system logs with an **info (level=6)** level or higher to Splunk.

4. Click **Add**.
5. Optional: To add another Syslog configuration, repeat **Step 3** to **Step 4**.

> **NOTEs**
>
> • You can add one or multiple Syslog configurations.
> • For each Splunk server, only one Syslog configuration can be added.

6. Click the close icon to close the pop-up window.

   Then, AmpCon-DC system logs will be sent to Splunk, and you can view and analyze these logs in the Splunk UI.

3. Viewing System Logs on Splunk

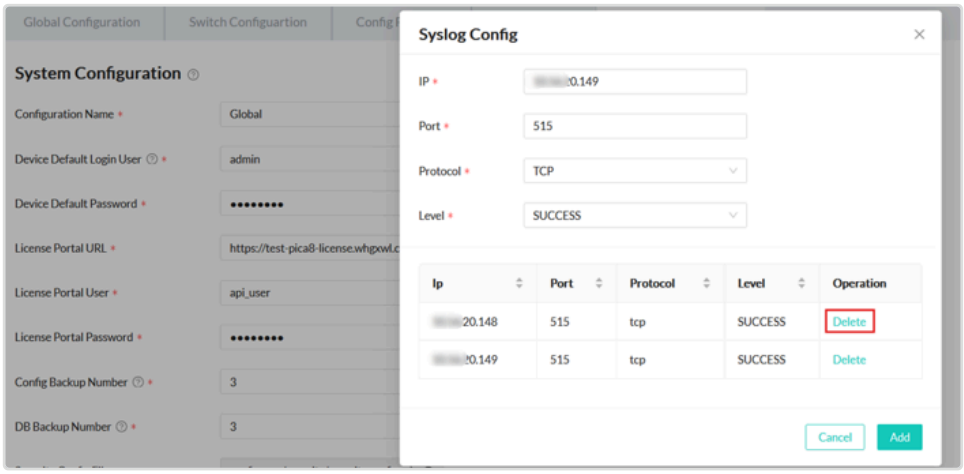
1. In the Splunk UI, click **Apps > Search & Reporting** from the top menu.
2. Enter the search condition in the **New Search** field. Then, you can see AmpCon-DC system logs displayed. For more information about Splunk search, see Get Started with Search.

Optional: Deleting a Syslog Configuration

> **NOTE**
>
> You can't edit a Syslog configuration directly. If a Syslog configuration is outdated, delete it, and then add a new one.

To delete a Syslog configuration, follow these steps:

1. In the **System Configuration** tab, click **Syslog Config**.
2. In the pop-up window, locate the Syslog configuration, and then click **Delete**.



3. Click the close icon to close the pop-up window.

Troubleshooting

If you fail to send AmpCon-DC system logs to Splunk, see Troubleshooting: Failing to Send Logs to Splunk for solutions.

Troubleshooting Splunk Integration

If you fail to access the Splunk UI from the AmpCon-DC UI, check webhook logs, or send alerts or logs to Splunk, refer to the following reasons and solutions:

Failing to Access the Splunk UI
Failing to View Webhook Logs
Failing to Send Alerts to Splunk
Failing to Send Logs to Splunk

Failing to Access the Splunk UI

Issue: When you click the name of an added Splunk integration, the Splunk login page can't be displayed.

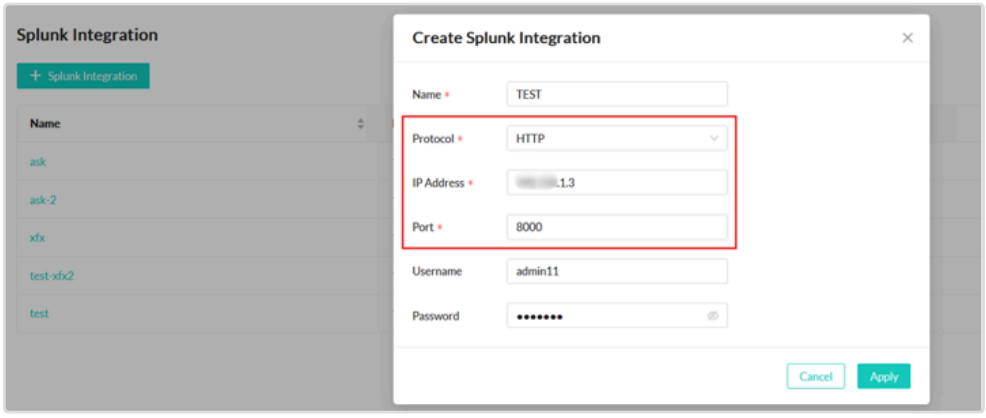
Root Causes: When you add the Splunk integration, the **Protocol**, **IP Address**, or **Port** value is incorrect.

Solutions:

1. Check the Splunk URL to find the protocol, IP address, and port.

   For example, if the Splunk URL is http://192.168.1.2:8000, then the protocol is **HTTP**, the IP address is **192.168.1.2**, and the port is **8000**.

2. Edit the Splunk integration to input correct IP address, port, and protocol values.



Failing to View Webhook Logs

Issue: After you add a Splunk integration, you don't see any webhook logs displayed when you click **Webhook Log**.

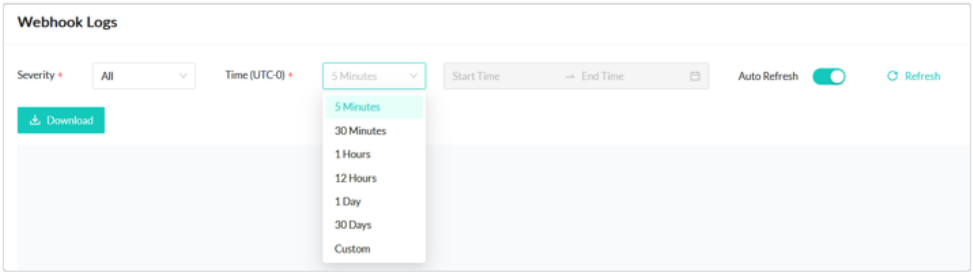
Root Causes:

- No webhook logs are generated by AmpCon-DC during the selected time range.

- You haven't added a receiver containing webhook configurations of the Splunk server, or you haven't configured any notification rules for the receiver.

Solutions:

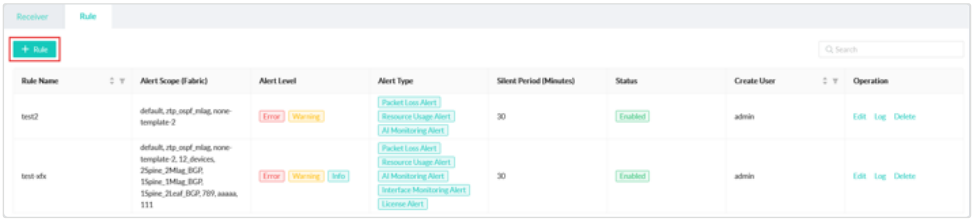
1. In the **Webhook Logs** pop-up window, select a longer time range in the **Time** section.



2. Add a receiver containing webhook configurations of the Splunk server. For more information, see Adding a Receiver to AmpCon-DC.



3. Configure at least one notification rule for the receiver. For more information, see Adding Notification Rules.



Failing to Send Alerts to Splunk

Issue: After completing the procedure of sending alerts to Splunk, you don't see any alerts sent from AmpCon-DC in the Splunk UI, or you don't see any alerts sent to Splunk on the "Notification History" page.

Root Causes:

- Alerts for the selected alert levels and alert types in related notification rules are not triggered.
- HTTP Event Collector (HEC) is disabled on Splunk so that AmpCon-DC can't send alerts to Splunk through HEC.
- In the receiver webhook configuration, the **Target URL** or **Token** value is incorrect.

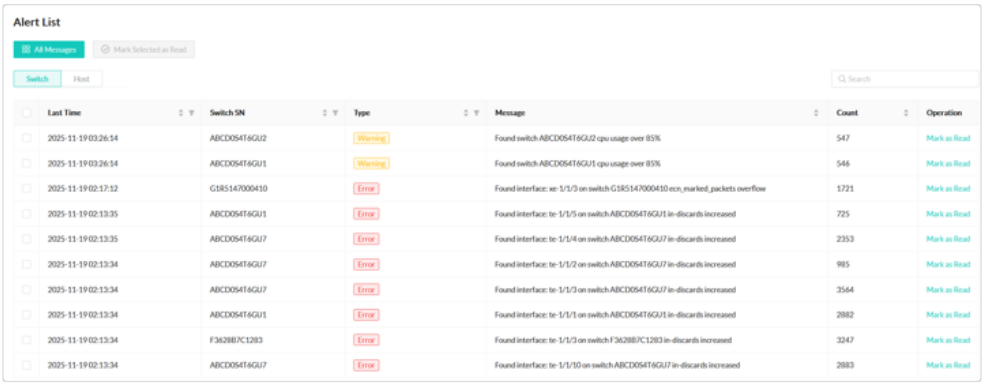
Failure Examples

- You haven't selected **Enable SSL** when you configure HEC, but the protocol in the **Target URL** field is **HTTPS**.
- The port in the **Target URL** field is not consistent with the **HTTP Port Number** field in the Splunk HEC configuration.
- The Splunk token in the **Token** field is not consistent with the token generated on Splunk.

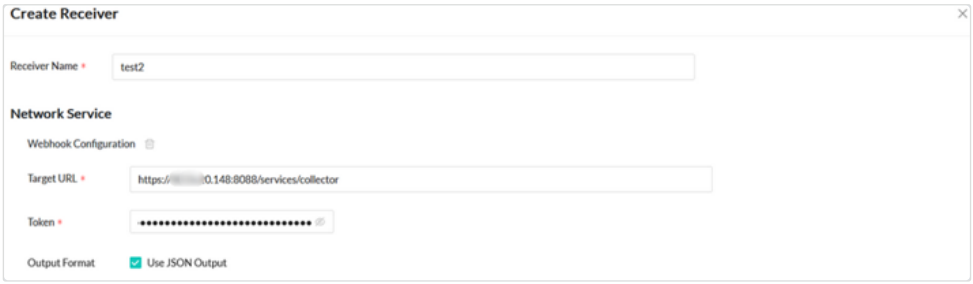
- No notification rules are added for the receiver, or **Send Notification** is set to **Disabled** in related notification rules.

Solutions:

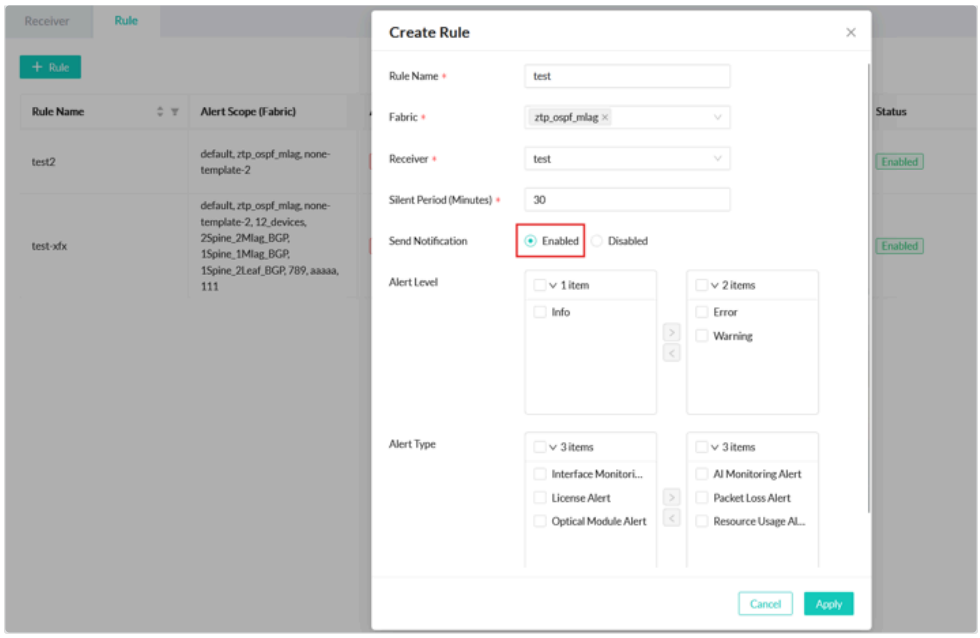
1. On the "Alert List" page of AmpCon-DC, check whether the alerts for the selected alert levels and alert types are displayed there. If yes, it means that the alerts are triggered.



2. Enable HEC on Splunk. For more information, see Configuring HEC.
3. Add a receiver to AmpCon-DC, and enter correct **Target URL** and **Token** values.



4. Add at least one notification rule for the receiver, and set **Send Notification** to **Enabled**.



Failing to Send Logs to Splunk

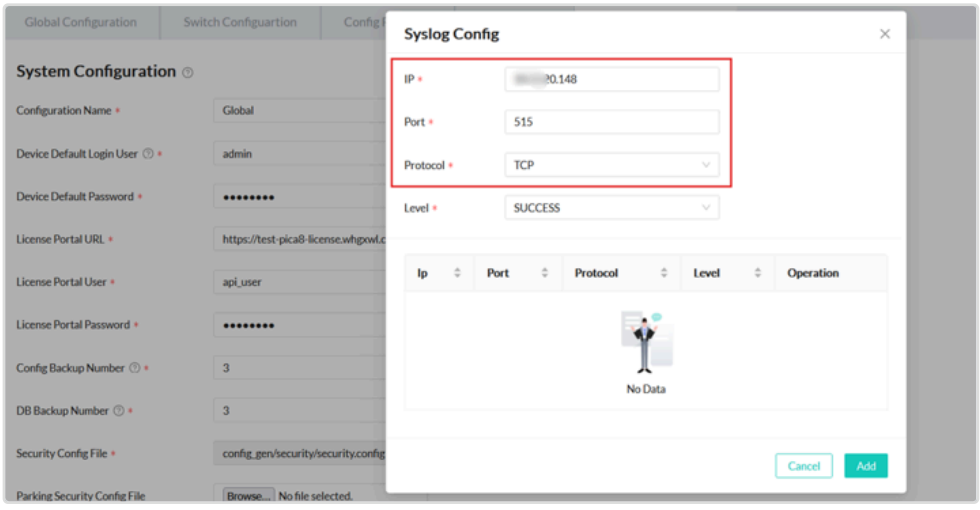
Issue: After completing the procedure of sending logs to Splunk, you don't see any AmpCon-DC system logs in the Splunk UI.

Root Causes:

- The Syslog service is disabled on Splunk.
- In the Syslog configuration, the **IP**, **Port**, or **Protocol** (**TCP** or **UDP**) value is incorrect.
- The TCP or UDP port isn't allowed on Splunk.

Solutions:

1. Enable the Syslog service on Splunk.
2. Check the Syslog configuration, and input correct **IP**, **Port**, and **Protocol** values.



3. Ensure that the TCP or UDP port is allowed on Splunk.

Alerts

AmpCon-DC issues an immediate alert when a failure or performance shift is detected, helping network administrators to diagnose root causes and resolve problems quickly.

You can use the alerting feature to achieve the following goals:

- View different levels and types of alerts in the AmpCon-DC UI.
- Receive real-time email alert notifications if you need to be notified immediately.
- View and analyze these alerts in the Splunk UI to get more detailed insights.

See the following child topics:

- Alert Types and Levels
- Checking the Alert List
- Alert Notifications

Alert Types and Levels

AmpCon-DC supports the alert levels **Error**, **Warning**, and **Info** for the following alert types:

- Packet Loss Alerts
- Resource Usage Alerts
- Interface Monitoring Alerts
- Optical Module Alerts
- AI Monitoring Alerts
- Host Alerts
- License Alerts

Packet Loss Alerts

Table 1. Packet Loss Alerts

Alert Metric	Description	Triggering Condition	Alert Level
In Errors	The number of incoming packets that contain errors and are dropped by a switch port increases	The metric value changes two times in the last four sampling cycles.	Error
Out Errors	The number of outgoing packets that a switch port fails to transmit successfully due to errors	The metric value changes two times in the last four sampling cycles.	Error
In Discards	The number of incoming packets that a switch port intentionally discards (drops) during processing	The metric value changes two times in the last four sampling cycles.	Error
Out Discards	The number of outgoing packets that a switch port intentionally discards (drops) before they are transmitted	The metric value changes two times in the last four sampling cycles.	Error

Resource Usage Alerts

Table 2. Resource Usage Alerts

Alert Metric	Description	Triggering Condition	Alert Level
CPU Usage	The CPU usage	The metric value exceeds 85%.	Warning
Memory Usage	The memory usage	The metric value exceeds 85%.	Warning
In Bandwidth Usage	The input bandwidth usage	The metric value exceeds 85%.	Warning
Out Bandwidth Usage	The output bandwidth usage	The metric value exceeds 85%.	Warning
Fan PWM Usage	The proportion of the fan's Pulse Width Modulation (PWM) to the total width	The metric value is over 85%.	Warning
RPSU Power-on	Whether the Power Supply Unit (PSU) is powered on or off	The metric value changes.	Info

Interface Monitoring Alerts

Table 3. Interface Monitoring Alerts

Alert Metric	Description	Triggering Condition	Alert Level
Admin Status	The port status (**Up** or **Down**) manually configured by the network administrator, including **Up** and **Down**	The metric value changes.	Info
Operation Status	The actual operational port status (**Up** or **Down**), which is detected by the switch	The metric value changes.	Warning
MTU	The largest size of a data packet that can be transmitted over a	The metric value changes.	Info

	network without being fragmented. It's measured in bytes		
Loopback Mode	Whether the loopback mode is enabled on this port	The metric value changes.	Info
Duplex Mode	Whether data can flow in one direction (half duplex) at a time or both directions (full duplex) simultaneously	The metric value changes.	Warning
Port Speed	The maximum data transfer rate that the port can support	The metric value changes.	Warning

Optical Module Alerts

NOTEs

- Optical module alerts can be displayed only when all of the following conditions are met:
  - The optical module supports Digital Diagnostic Monitoring (DDM), and it is inserted into a supported switch. For more information, see Supported Optical Modules and Switches.
  - The switch to which the optical module is inserted is managed by AmpCon-DC.
- For N9600-64OD switches with PicOS 4.5.3.2 installed, AmpCon-DC can't properly trigger alerts when the **Rx Power** metric value is below the defined threshold.

Table 4. Optical Module Alerts

Alert Metric	Description	Triggering Condition	Alert Level
Temperature	The temperature of the optical module connected to the switch port. It's	The metric values exceed the thresholds of each alert level, which are defined by the	Error and Warning

	measured in Celsius (°C).	optical module vendor and cannot be modified.	
Tx Power	The amount of optical power emitted by the optical module connected to the switch port.		
Rx Power	The amount of optical power received by the optical module connected to the switch port.		
Bias	The bias current of the optical module connected to the switch port. It's measured in milliamperes (mA).		
Voltage	The operating voltage of the optical module connected to the switch port. It's measured in volts (V).		

Supported Optical Modules and Switches

Table 5. Optical Module Types and Switch Models Supporting DDM

PicOS Version	Switch Models	Optical Module Types
4.5.4E	• N8520-32D	• QSFP56-DD • QSFP56
4.7.0E	• N9550-32D	• QSFP56 • QSFP56-DD

AI Monitoring Alerts

Table 6. AI Monitoring Alerts

Alert Metric	Description	Triggering Condition	Alert Level
ECN Marked Packets	The number of packets that have been marked with ECN.	The metric value exceeds 1500.	Error
Send PFC Pause Frames	The PAUSE frames sent by the transmitting end for flow control.	The metric value changes in a minute.	Error
Receive PFC Pause Frames	The PAUSE frames received by the receiver end for flow control.	The metric value changes in a minute.	Error
PFC Deadlock Monitor Count	A counter used for monitoring and recording the number of PFC deadlock events.	The metric value changes in a minute.	Error
PFC Deadlock Recovery Count	A counter used to track and record the number of recoveries from PFC deadlock states.	The metric value changes in a minute.	Error

Host Alerts

> **NOTE**
>
> Host alerts don't support email alert notifications. Therefore, the **Host Alert** type is not displayed in the **Alert Type** section when you create notification rules.

Table 7. Host Alerts

Alert Metric	Description	Triggering Condition	Alert Level

CPU Usage	The CPU usage of the added third-party hosts.	The metric value is greater than 85% but less than 90%.	Warning
		The metric value exceeds 90%.	Error
Memory Usage	The memory usage of the added third-party hosts.	The metric value is greater than 85% but less than 90%.	Warning
		The metric value exceeds 90%.	Error
Disk Usage	The disk usage of the added third-party hosts.	The metric value is greater than 85% but less than 90%.	Warning
		The metric value exceeds 90%.	Error

License Alerts

Table 8. License Alerts

Alert Metric	Description	Triggering Condition	Alert Level
AmpCon-DC License	The AmpCon-DC license imported to AmpCon-DC.	The AmpCon-DC license will expire after 15 days.	Warning
		The AmpCon-DC license expires.	Error

Checking the Alert List

AmpCon-DC uses monitoring data to predict equipment failures and performance anomalies and then trigger immediate alerts.

You can check alerts on the “Alert List” page and take corrective actions before issues are escalated.

- Prerequisites
- Viewing Alerts
  - Viewing All Unread Alerts
    - Marking Unread Alerts as Read
  - Viewing All Alerts
  - Viewing All Unread "Error" Alerts
  - Viewing All Unread "Warning" Alerts
  - Viewing All Unread "Info" Alerts
- Filtering Alerts

Prerequisites

Ensure that Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. Or else, the alert feature might not work.

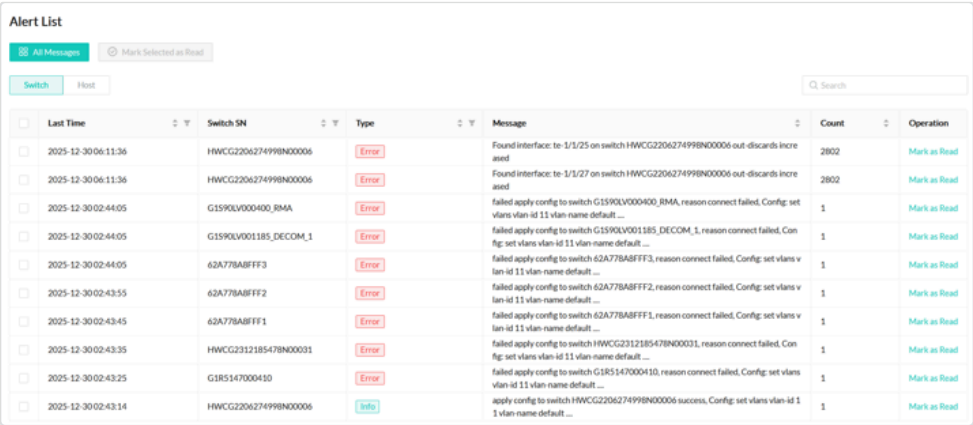
By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

Viewing Alerts

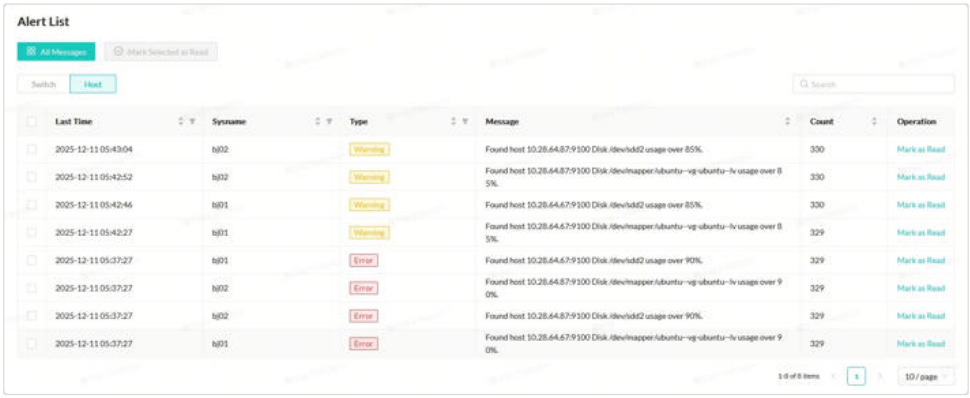
Viewing All Unread Alerts

Click **Monitor > Alerts > Alert List** from the navigation bar, and then you can see all unread alerts.

- In the **Switch** tab, you can see all unread alerts related to managed switches.

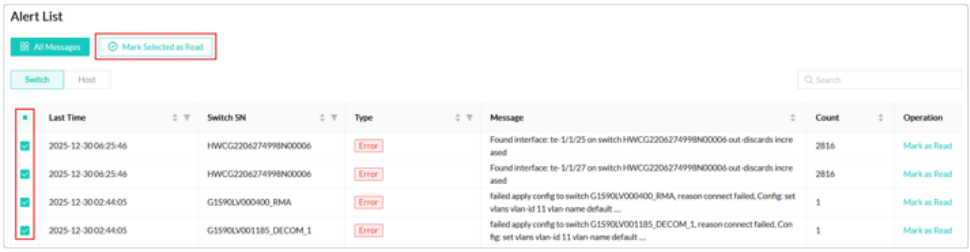


- Click the **Host** tab, you can see all unread alerts related to added third-party devices.



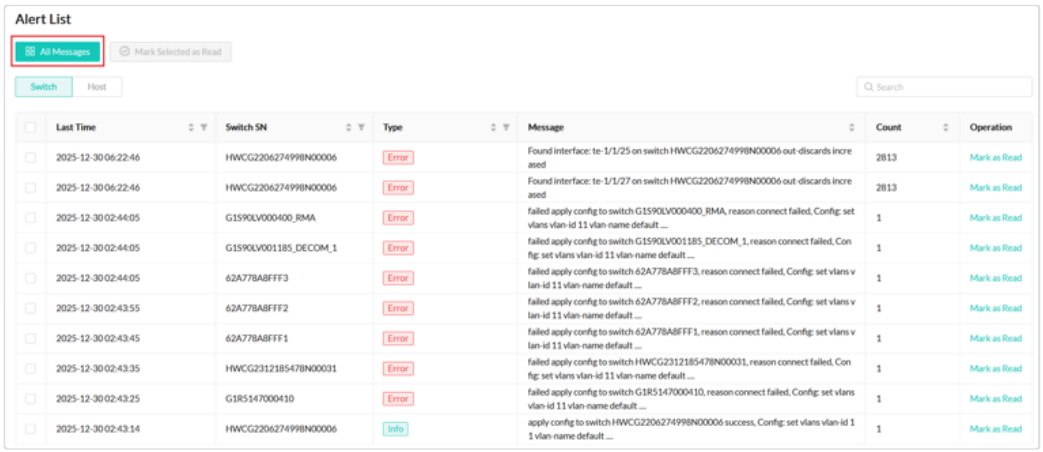
Marking Unread Alerts as Read

- To mark one unread alert as read, locate the alert, and then click **Mark as Read**.
- To mark multiple unread alerts as read, select these alerts, and then click **Mark Selected as Read**.
- To mark all unread alerts as read, click the square in the top to automatically select all unread alerts, and then click **Mark Selected as Read**.

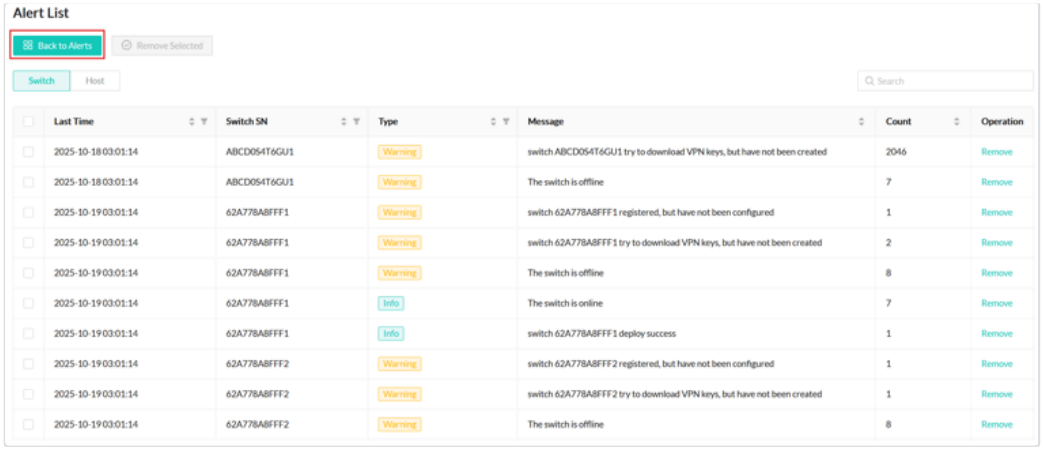


Viewing All Alerts

Click **All Messages**, and then you can see all alerts, including unread alerts and alerts that have been read.

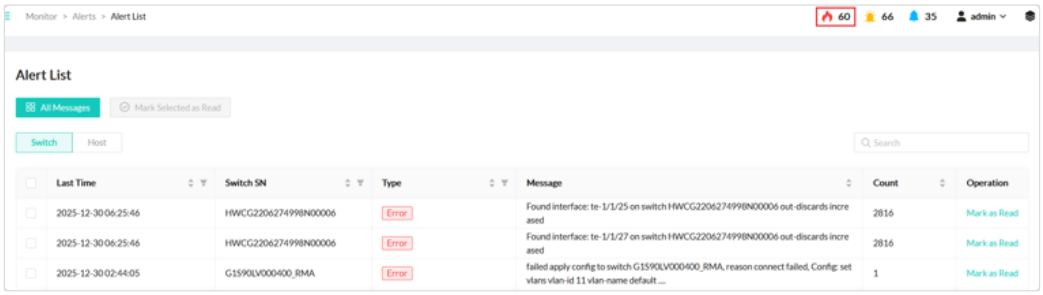


Click **Back to Alerts**, and then you can see all unread alerts.



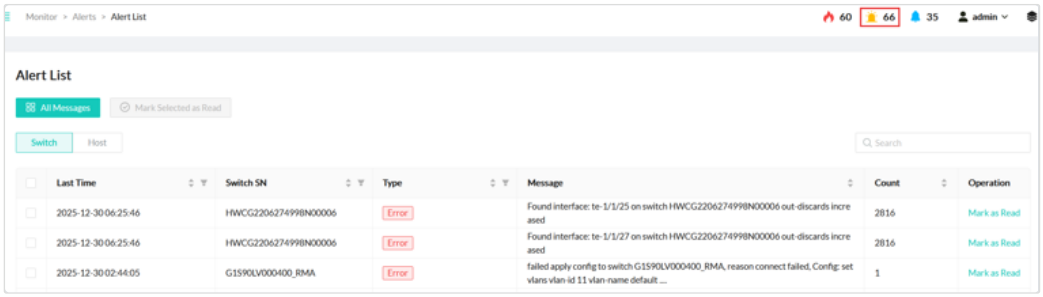
Viewing All Unread "Error" Alerts

Click the red flame icon, and then you can see all unread "Error" alerts.



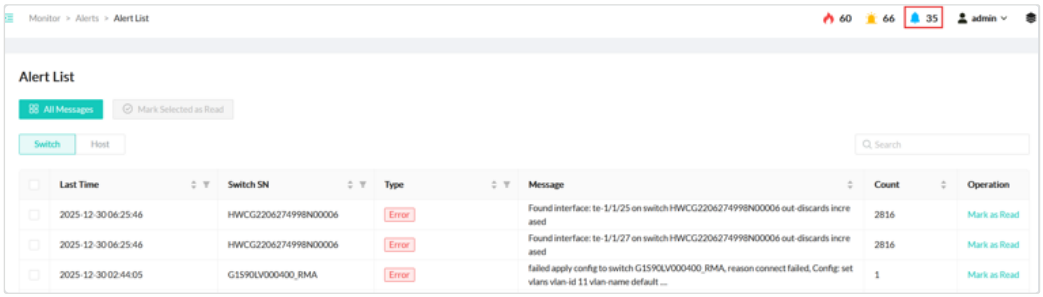
Viewing All Unread "Warning" Alerts

Click the orange warning icon, and then you can see all unread "warning" alerts.



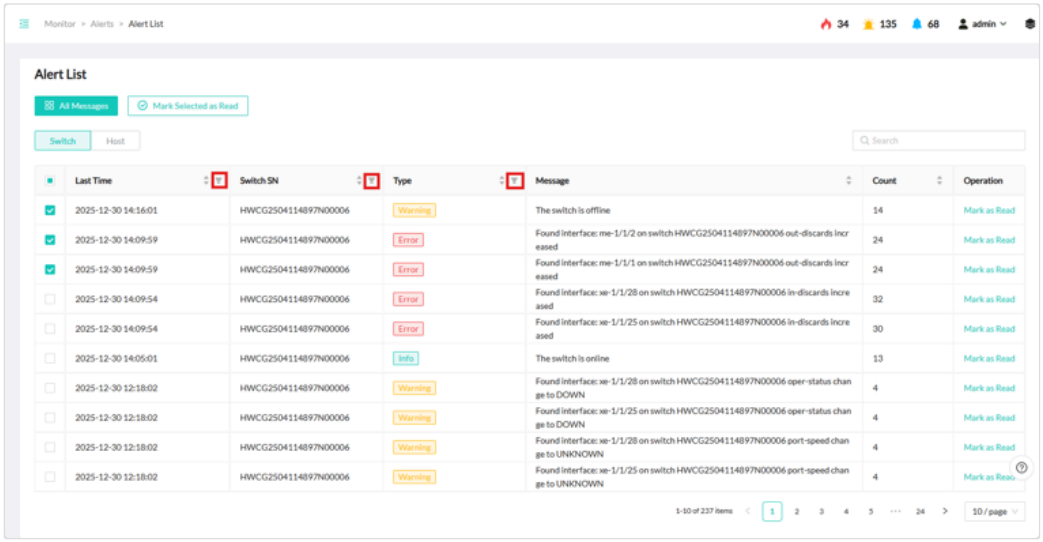
Viewing All Unread "Info" Alerts

Click the blue bell icon, and then you can see all unread "Info" alerts.



Filtering Alerts

On the “Alert List” page, you can filter alerts by using the filer icon in the **Last Time**, **Switch SN**, or **Type** column.



Alert Notifications

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

In addition, AmpCon-DC uses Splunk webhooks to send alerts to Splunk in real time. You can view and analyze these alerts in the Splunk UI.

See the child topics:

- Sending Alerts to Splunk
- Sending Email Alert Notifications
- Viewing Historical Alert Notifications

Sending Alerts to Splunk

Webhooks are used to send data to third-party applications. AmpCon-DC uses Splunk webhooks (Splunk HTTP Event Collector) to send alerts to Splunk in real time. Then, you can view and analyze these alerts in the Splunk UI.

To send alerts from AmpCon-DC to Splunk, complete the following operations:

- On Splunk, configure Splunk HTTP Event Collector (HEC), and then create an Event Collector token.
- On AmpCon-DC, add a receiver containing Splunk webhook configurations, and then add notification rules for the receiver.

Prerequisites
Procedure
1. Configuring HEC
2. Creating an Event Collector Token
3. Adding a Receiver to AmpCon-DC
4. Adding Notification Rules
Verifying Alerts Sent
Checking on Splunk
Checking on AmpCon-DC
Troubleshooting

Prerequisites

- Make your Splunk environment (Splunk Cloud Platform or Splunk Enterprise) ready.
- Obtain the username and password of a Splunk admin account.
- Ensure that Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. Or else, the alerting feature might not work. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.

Procedure

1. Configuring HEC

To send alerts from AmpCon-DC to Splunk, you must configure HEC on Splunk first. To configure HEC, follow these steps:

1. Log in to Splunk with the username and password of an admin account.
2. From the top menu, select **Settings > Data Inputs**.
3. Under **Local Inputs**, select **HTTP Event Collector**.
4. On the “HTTP Event Collector” page, click **Global Settings**.

- In the **All Tokens** section, select **Enabled** to enable HEC.
- In the **HTTP Port Number** field, enter the webhook port that Splunk uses for receiving data.
- In the **Enable SSL** box, determine the protocol that Splunk uses for receiving data.
  - If **Enable SSL** is not selected, the protocol must be **HTTP** when you add a receiver to AmpCon-DC.
  - If **Enable SSL** is selected, the protocol must be **HTTPS** when you add a receiver to AmpCon-DC.
- For other parameters, use the default configurations or configure based on your needs. For more information, see Splunk Documents.

5. Click **Save**.

2. Creating an Event Collector Token

On Splunk, you need to create an Event Collector token used by AmpCon-DC to send alerts to Splunk. To create an Event Collector token, follow these steps:

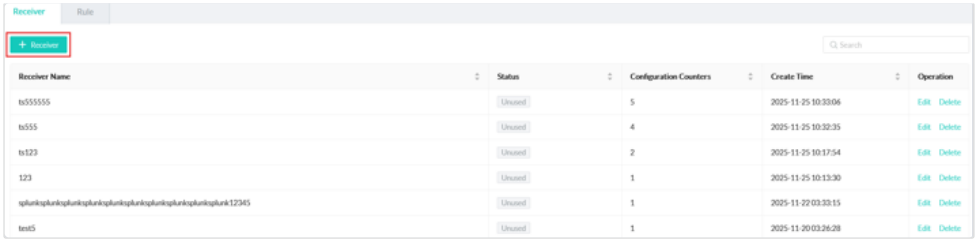
1. On the “HTTP Event Collector” page of the Splunk UI, click **New Token**.
2. In the **Select Source** section, enter the name of the token.

   For other parameters, use the default configurations or configure based on your needs. For more information, see Splunk Documents.
3. Click **Next**.
4. Optional: Configure the source type and the index for HEC events.
5. Click **Review**.
6. If all configurations are what you want, click **Submit**.
7. Copy the generated token value, and paste it into another document for reference later.

3. Adding a Receiver to AmpCon-DC

On AmpCon-DC, you need to add a receiver containing Splunk webhook configurations. To add a receiver, follow these steps:

1. Log in to the AmpCon-DC UI, and click **Monitor > Alerts > Alert Notification** from the navigation bar.
2. In the **Receiver** tab of the “Alert Notification” page, click **+ Receiver**.



3. In the pop-up window, input a name as the receiver name.

> **NOTEs**
>
> - The receiver name needs to be unique.
> - The receiver name can contain only uppercase and lowercase letters and numbers. Spaces and special characters are not supported.
> - The receiver name can contain 64 characters at most.
> - The receiver name is not case-sensitive.

4. Click **Configuration**, and then select **Webhook**. In the **Network Service** section, enter the following information:

> **NOTEs**
>
> - You can click **Configuration** and select **Webhook** to add multiple webhook configurations.
> - To delete a webhook configuration, click the delete icon.
> - SMTP configurations are used to send email alert notifications. If needed, you can click **Configuration** and select **SMTP** to add SMTP configurations. But before you add SMTP configurations, you must configure an SMTP Server.

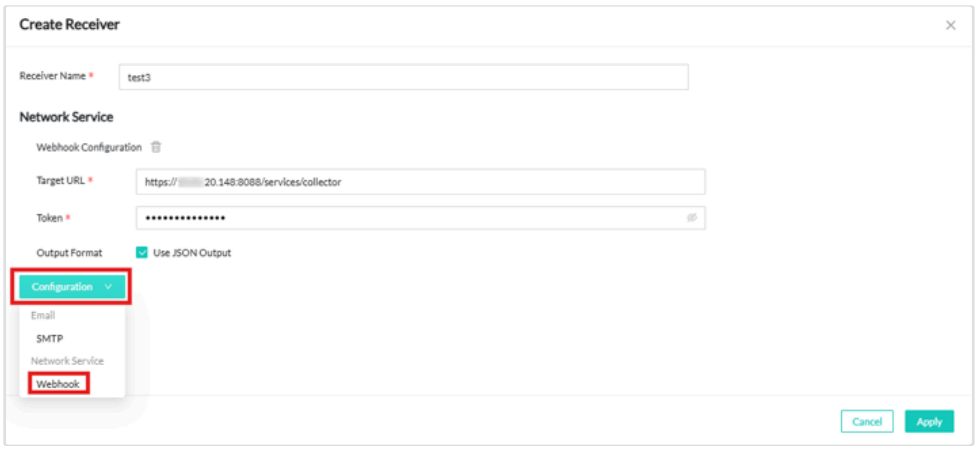


Table 1. Receiver Parameters

Parameter	Description
Target URL	The Splunk URL in the following format: ***<protocol>://<Splunk_server_IPv4_address>:<port>*/services/collector** • ***<protocol>*** is determined by whether **Enable SSL** is selected when you configure HEC. ◦ If **Enable SSL** is not selected, the protocol must be **HTTP**. ◦ If **Enable SSL** is selected, the protocol must be **HTTPS**. • ***<Splunk_server_IPv4_address>*** is the IPv4 address of the Splunk server. • ***<port>*** is the port number specified in the **HTTP Port Number** field when you configure HEC. **Example Target URL:** http://192.168.1.2:8088/services/collector
Token	The Event Collector token that you generated.
Output Format	Optional. Select **Use JSON Output** to display alerts in JSON compact format.

5. Click **Apply**. Then, you can see the receiver is displayed in the **Receiver** tab of the “Alert Notification” page.

Table 2. Receiver Metrics

Metric	Description
Receiver Name	The name of the receiver.
Status	Whether the receiver is bound with notification rules. • **Used:** The receiver is bound with at least one notification rule.

	• **Unused:** The receiver is not bound with any notification rule.
Configuration Counters	The total number of SMTP configurations and webhook configurations in the receiver. For example, if a receiver contains one SMTP configuration and one webhook configuration, the value of **Configuration Counters** is **2**.
Create Time	The time when the receiver is created.

6. Optional: To edit a receiver, locate the receiver, and then click **Edit**.

> **NOTE**
>
> After you edit a receiver name, the alert notifications sent before the receiver name change are not changed.

7. Optional: To delete a receiver, locate the receiver, and then click **Delete**.

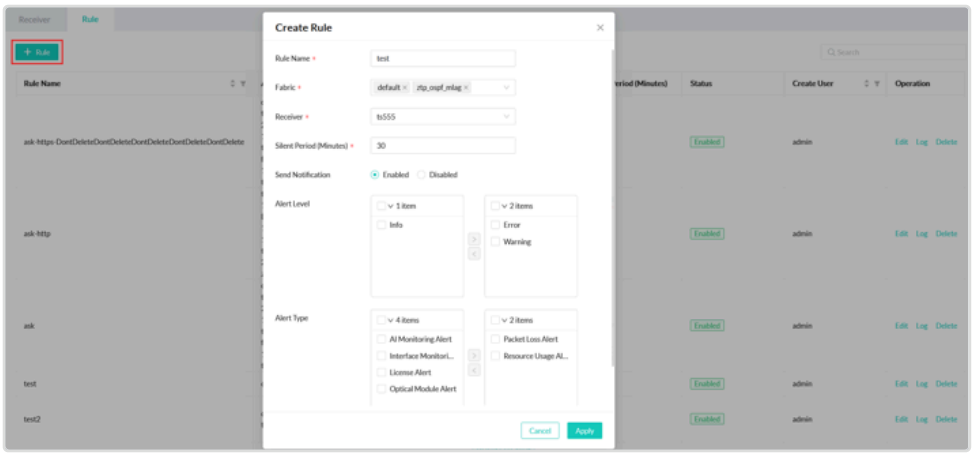
> **NOTEs**
>
> - Only the receivers in **Unused** status can be deleted. The receivers in **Used** status can't be deleted.
> - To change a receiver status from **Used** to **Unused**, remove the receiver from related notification rules, or delete related notification rules.
> - After you delete a receiver, the alert notifications related to the receiver will also be deleted from the "Notification History" page. If the receiver name is changed before you delete the receiver:
>   - The alert notifications sent after the receiver name change are deleted.
>   - The alert notifications sent before the receiver name change are not deleted.

4. Adding Notification Rules

After adding a receiver, add notification rules to configure which types of alerts can be forwarded to Splunk. To add a notification rule, follow these steps:

> **NOTE**
>
> At most 100 alert notification rules can be added.

1. In the **Rule** tab of the “Alert Notification” page, click **+ Rule**.



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

Table 3. Notification Rule Parameters

Parameter	Description
Rule Name	The name of the rule. The rule name needs to be unique. **NOTEs** • The rule name needs to be unique. • The rule name can contain only uppercase and lowercase letters and numbers. Spaces and special characters are not supported. • The rule name can contain 64 characters at most. • The rule name is not case-sensitive.
Fabric	The fabric to be monitored. You can select one or multiple fabrics.
Receiver	The receiver to be notified.

Silent Period (Minutes)	The period (in minutes) during which the same alert notification is not sent repeatedly. **NOTEs** • To prevent email bombing, set the silent period to at least 30 minutes. • If you set the silent period to a value less than 30, the silent period is changed to 30 automatically.
Send Notification	Whether to enable the alert notification function. • **Enabled:** Alert notifications can be sent to the selected receiver. • **Disabled:** Alert notifications can't be sent to the selected receiver. **NOTEs** • If you select **Enabled**, only the selected levels and types of alerts can be sent to the receiver. • All triggered alerts can be displayed on the "Alert List" page no matter you enable the alert notification function or not.
Alert Level	Select the levels of alerts to be monitored in the left cell, including **Warning**, **Error**, and **Info**. Then, click **>**. To disable the monitoring of specific alert levels, select the alert levels in the right cell, and then click **<**. **NOTE** To select all alert levels, click the top square.

Alert Type	Select the types of alerts to be monitored in the left cell, and then click **>**. To disable the monitoring of specific alert types, select the alert types in the right cell, and then click **<**. **NOTEs** • The following alert types can be selected: ◦ **Packet Loss Alert** ◦ **Resource Usage Alert** ◦ **Interface Monitoring Alert** ◦ **Optical Module Alert** ◦ **AI Monitoring Alert** ◦ **License Alert** • To select all alert types, click the top square. • For more information about each alert type, see Alert Types and Levels.

3. Click **Apply**. Then, you can see the notification rule is displayed in the **Rule** tab.

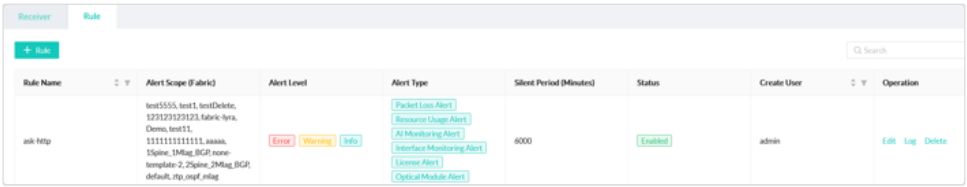


Table 4. Notification Rule Metrics

Metric	Description
Rule Name	The name of the notification rule.
Alert Scope (Fabric)	The fabric to be monitored.
Alert Level	The levels of alerts to be monitored
Alert Type	The types of alerts to be monitored

Silent Period (Minutes)	The period (in minutes) during which the same alert notification is not sent repeatedly.
Status	Whether the alert notification function is enabled. • **Enabled:** Alert notifications can be sent to the selected receiver. • **Disabled:** Alert notifications can't be sent to the selected receiver.
Create User	The AmpCon-DC user who creates the notification rule.

4. Optional: To check alert notifications sent in the last 30 days related to a notification rule, locate the rule in the **Rule** tab, and then click **Log**. For more information, see Viewing Historical Alert Notifications.
5. Optional: To edit a notification rule, locate the rule, and then click **Edit**.

> **NOTE**
>
> After you change a rule name, the alert notifications related to the previous rule name are not changed on the "Notification History" page.

6. Optional: To delete a notification rule, locate the rule, and then click **Delete**.

> **NOTEs**
>
> - Only the notification rules in **Disabled** status can be deleted. The notification rules in **Enabled** status can't be deleted.
> - To change a rule status from **Enabled** to **Disabled**, edit the rule, and change **Send Notification** to **Disabled**.
> - If all notification rules for a receiver are deleted, alerts can't be sent to the receiver.
> - After you delete a notification rule, the alert notifications related to the rule will also be deleted from the "Notification History" page. If the rule name is changed before you delete the rule:

- The alert notifications sent after the rule name change are deleted.
- The alert notifications sent before the rule name change are not deleted.

Verifying Alerts Sent

Checking on Splunk

You can check received alerts in the Splunk UI. Follow these steps:

1. In the Splunk UI, click **Apps > Search & Reporting** from the top menu.
2. Enter the search conditions in the **New Search** field.

   Then, you can see the alerts sent from AmpCon-DC. For more information about Splunk search, see Get Started with Search.

Checking on AmpCon-DC

In the AmpCon-DC UI, click **Monitor > Alerts > Notification History** from the navigation bar. Then, you can check the historical alerts sent to Splunk. For more information, see Viewing Historical Alert Notifications.



Troubleshooting

If you fail to send alerts to Splunk, see Troubleshooting: Failing to Send Alerts to Splunk for solutions.

Sending Email Alert Notifications

If you can't access the AmpCon-DC UI to view alerts or need to be notified immediately when issues arise, configure AmpCon-DC to receive real-time email alert notifications. In this way, you can promptly find problems and prevent incident escalation.

To send alert notifications through emails, you need to add SMTP configurations, add receivers containing recipient email addresses, and then configure notification rules.

Prerequisites
Procedure
1. Adding SMTP Configurations
2. Adding a Receiver to AmpCon-DC
3. Adding Notification Rules
Checking Alert Notification History

Prerequisites

- Ensure that Google Remote Procedure Call (gRPC) is enabled on the switches to be monitored. Or else, the alerting feature might not work. By default, gRPC is enabled automatically after you deploy a switch with AmpCon-DC or import a switch to AmpCon-DC.
- Prepare an SMTP server, and make it ready. AmpCon-DC supports mainstream email service providers like Outlook and Gmail.

Procedure

1. Adding SMTP Configurations

To receive alert notifications through emails, you need to add SMTP configurations first. Follow these steps:

1. In the AmpCon-DC UI, click **System > Email Settings** from the navigation bar.
2. On the “Email Settings” page, input the following information:

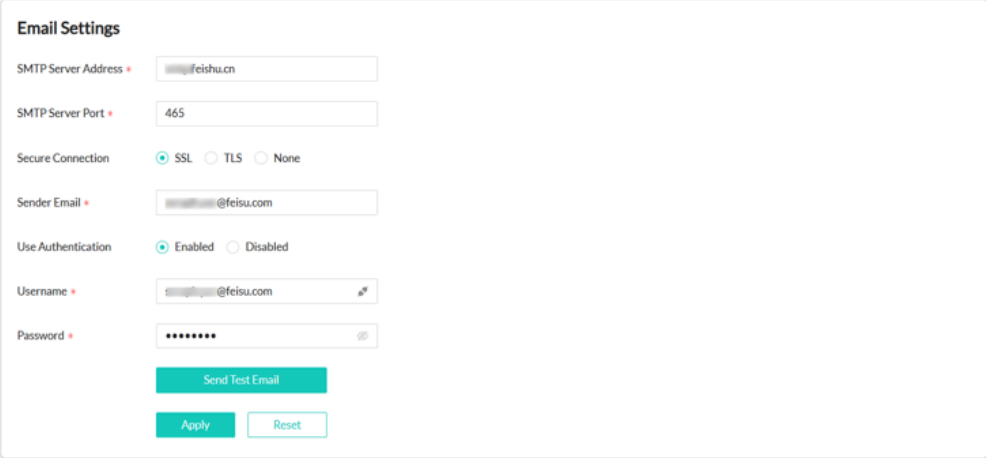


Table 1. SMTP Configuration Parameters

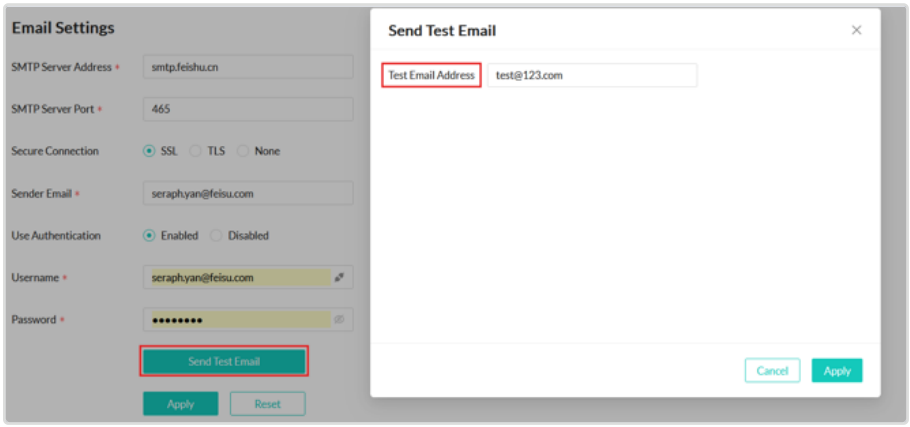
Parameter	Description
SMTP Server Address	The hostname or IPv4 address of the SMTP server.
SMTP Server Port	The TCP port number used to connect to the SMTP server.
Secure Connection	The encryption method for secure email transmission, including **SSL**, **TLS**, or **None**. • **SSL**: The emails sent to this SMTP server are encrypted through SSL. • **TLS**: The emails sent to this SMTP server are encrypted through TLS. • **None**: The emails sent to this SMTP server are not encrypted.
Sender Email	The email address from which the email is sent.
Use Authentication	Select **Enabled** or **Disabled**. The default value is **Disabled**. • **Enabled:** The SMTP server requires authentication for logged-in users. If you select **Enabled**, specify the following parameters: ◦ **Username:** The name of the user to log in to the SMTP server.

- **Password:** The password of the SMTP server user.

- **Disabled:** The SMTP server doesn't require authentication for logged-in users.

> **NOTEs**
>
> - If you select **SSL** or **TLS** in the **Secure Connection** section, you must select **Enabled** here.
> - If you select **None** in the **Secure Connection** section, you must select **Disabled** here.

3. Send a test email, and check whether the email can be received.
   a. Click **Send Test Email**.
   b. In the **Test Email Address** field, enter the recipient email address.



   c. Click **Send**.
   d. Ensure that the test email can be received.
4. Click **Apply** to complete the configuration.
5. Optional: To edit SMTP configurations, modify the configurations on the "Email Settings" page, and then click **Apply**.

> **NOTE**
>
> Do not forget to send a test email to the recipient email address and check whether the email can be received.

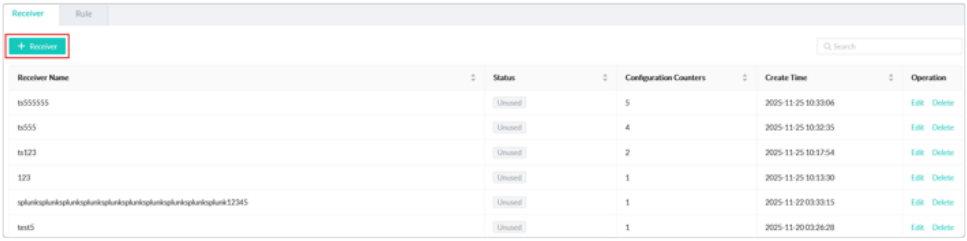
6. Optional: To reset SMTP configurations, click **Reset** on the “Email Settings” page.

> **NOTE**
>
> After you reset SMTP server configurations, add new SMTP configurations, and then click **Apply**. Or else, AmpCon-DC will still use the previous SMTP server configurations.

2. Adding a Receiver to AmpCon-DC

On AmpCon-DC, you need to add a receiver containing recipient email addresses. To add a receiver, follow these steps:

1. Click **Monitor > Alerts > Alert Notification** from the navigation bar.
2. In the **Receiver** tab of the “Alert Notification” page, click **+ Receiver**.



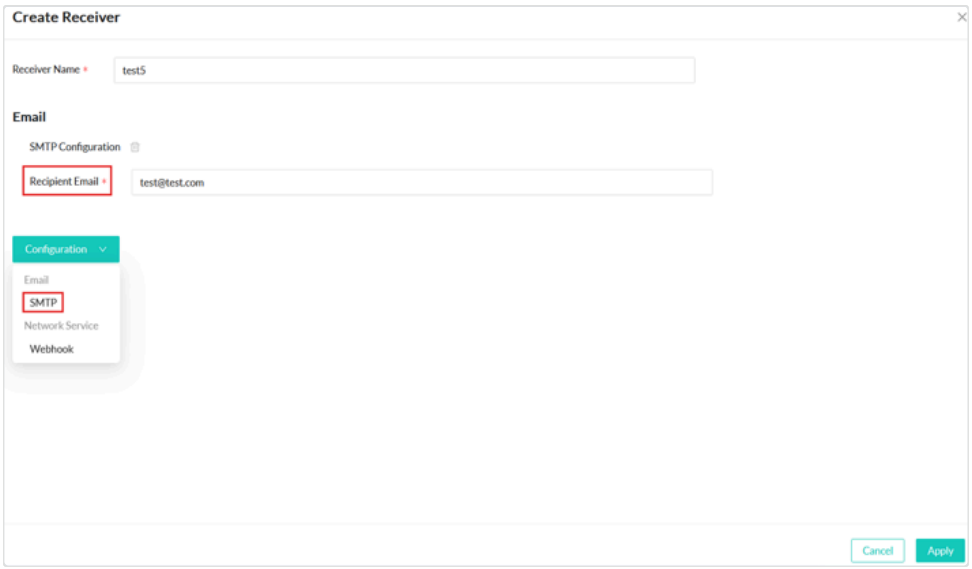
3. In the pop-up window, enter a name in the **Receiver Name** field.

> **NOTEs**
>
> - The receiver name needs to be unique.
> - The receiver name can contain only uppercase and lowercase letters and numbers. Spaces and special characters are not supported.
> - The receiver name can contain 64 characters at most.
> - The receiver name is not case-sensitive.

4. Click **Configuration**, and then select **SMTP**. In the **Recipient Email** field, enter the recipient email address.

> **NOTEs**
>
> - You can click **Configuration** and select **SMTP** to add multiple SMTP configurations.
> - To delete an SMTP configuration, click the delete icon.

- Webhook configurations are used to send alerts to Splunk. If needed, you can click **Configuration** and select **Webhook** to add webhook configurations.



5. Click **Apply**. Then, you can see the receiver is displayed in the **Receiver** tab of the "Alert Notification" page.

Table 2. Receiver Metrics

Metric	Description
Receiver Name	The name of the receiver.
Status	Whether the receiver is bound with notification rules. • **Used:** The receiver is bound with at least one notification rule. • **Unused:** The receiver is not bound with any notification rule.
Configuration Counters	The total number of SMTP configurations and webhook configurations in the receiver. For example, if a receiver contains one SMTP configuration and one webhook configuration, the value of **Configuration Counters** is **2**.
Create Time	The time when the receiver is created.

6. Optional: To edit a receiver, locate the receiver, and then click **Edit**.

> **NOTE**
>
> After you edit a receiver name, the alert notifications sent before the receiver name change are not changed.

7. Optional: To delete a receiver, locate the receiver, and then click **Delete**.

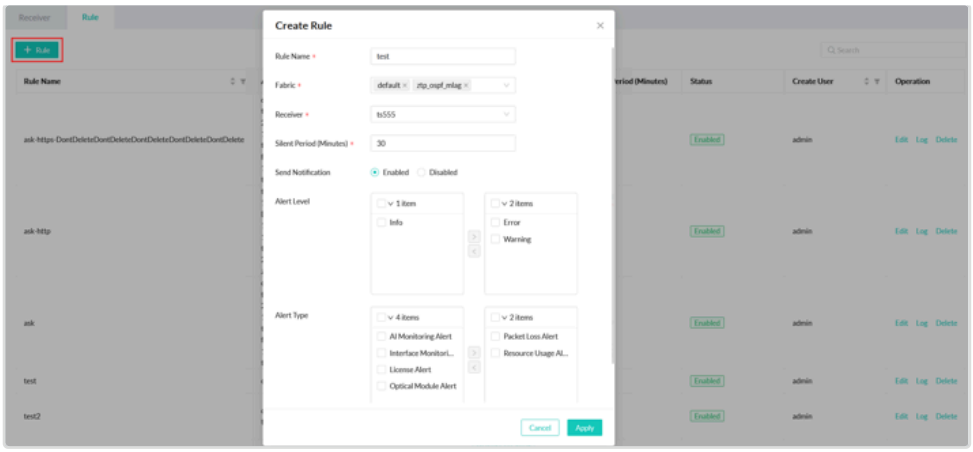
> **NOTEs**
>
> - Only the receivers in **Unused** status can be deleted. The receivers in **Used** status can't be deleted.
> - To change a receiver status from **Used** to **Unused**, remove the receiver from related notification rules, or delete related notification rules.
> - After you delete a receiver, the alert notifications related to the receiver will also be deleted from the "Notification History" page. If the receiver name is changed before you delete the receiver:
>   - The alert notifications sent after the receiver name change are deleted.
>   - The alert notifications sent before the receiver name change are not deleted.

3. Adding Notification Rules

After adding a receiver, add notification rules to configure which types of alert notifications can be sent through emails. To add a notification rule, follow these steps:

> **NOTE**
>
> At most 100 alert notification rules can be added.

1. In the **Rule** tab of the "Alert Notification" page, click **+ Rule**.



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

Table 3. Notification Rule Parameters

Parameter	Description
Rule Name	The name of the rule. The rule name needs to be unique. **NOTEs** • The rule name needs to be unique. • The rule name can contain only uppercase and lowercase letters and numbers. Spaces and special characters are not supported. • The rule name can contain 64 characters at most. • The rule name is not case-sensitive.
Fabric	The fabric to be monitored. You can select one or multiple fabrics.
Receiver	The receiver to be notified.
Silent Period (Minutes)	The period (in minutes) during which the same alert notification is not sent repeatedly. **NOTEs** • To prevent email bombing, set the silent period to at least 30 minutes.

	• If you set the silent period to a value less than 30, the silent period is changed to 30 automatically.
Send Notification	Whether to enable the alert notification function. • **Enabled:** Alert notifications can be sent to the selected receiver. • **Disabled:** Alert notifications can't be sent to the selected receiver. **NOTEs** • If you select **Enabled**, only the selected levels and types of alerts can be sent to the receiver. • All triggered alerts can be displayed on the "Alert List" page no matter you enable the alert notification function or not.
Alert Level	Select the levels of alerts to be monitored in the left cell, including **Warning**, **Error**, and **Info**. Then, click **>**. To disable the monitoring of specific alert levels, select the alert levels in the right cell, and then click **<**. **NOTE** To select all alert levels, click the top square.
Alert Type	Select the types of alerts to be monitored in the left cell, and then click **>**. To disable the monitoring of specific alert types, select the alert types in the right cell, and then click **<**. **NOTEs**

	• To select all alert types, click the top square. • For supported alert types, see Alert Types and Levels.

3. Click **Apply**. Then, you can see the notification rule is displayed in the **Rule** tab.

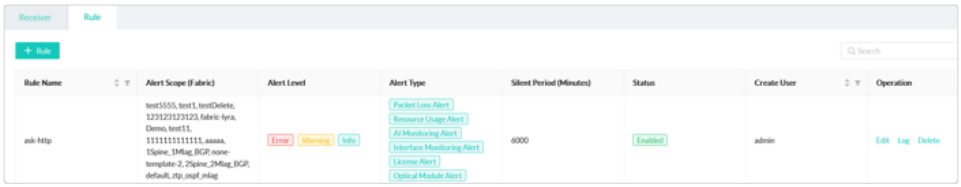


Table 4. Notification Rule Metrics

Metric	Description
Rule Name	The name of the notification rule.
Alert Scope (Fabric)	The fabric to be monitored.
Alert Level	The levels of alerts to be monitored
Alert Type	The types of alerts to be monitored
Silent Period (Minutes)	The period (in minutes) during which the same alert notification is not sent repeatedly.
Status	Whether the alert notification function is enabled. • **Enabled:** Alert notifications can be sent to the selected receiver. • **Disabled:** Alert notifications can't be sent to the selected receiver.
Create User	The AmpCon-DC user who creates the notification rule.

4. Optional: To edit a notification rule, locate the rule, and then click **Edit**.

NOTE

> After you change a rule name, the alert notifications related to the previous rule name are not changed on the “Notification History” page.

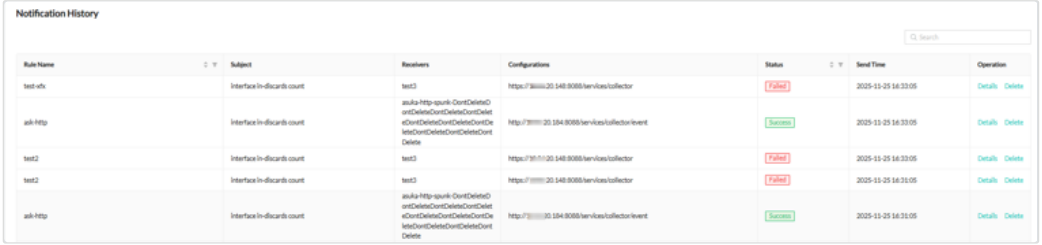
5. Optional: To delete a notification rule, locate the rule, and then click **Delete**.

> **NOTEs**
>
> - Only the notification rules in **Disabled** status can be deleted. The notification rules in **Enabled** status can’t be deleted.
> - To change a rule status from **Enabled** to **Disabled**, edit the rule, and then change **Send Notification** to **Disabled**.
> - If all notification rules for a receiver are deleted, alerts can’t be sent to the receiver.
> - After you delete a notification rule, the alert notifications related to the rule will also be deleted from the “Notification History” page. If the rule name is changed before you delete the rule:
>   - The alert notifications sent after the rule name change are deleted.
>   - The alert notifications sent before the rule name change are not deleted.

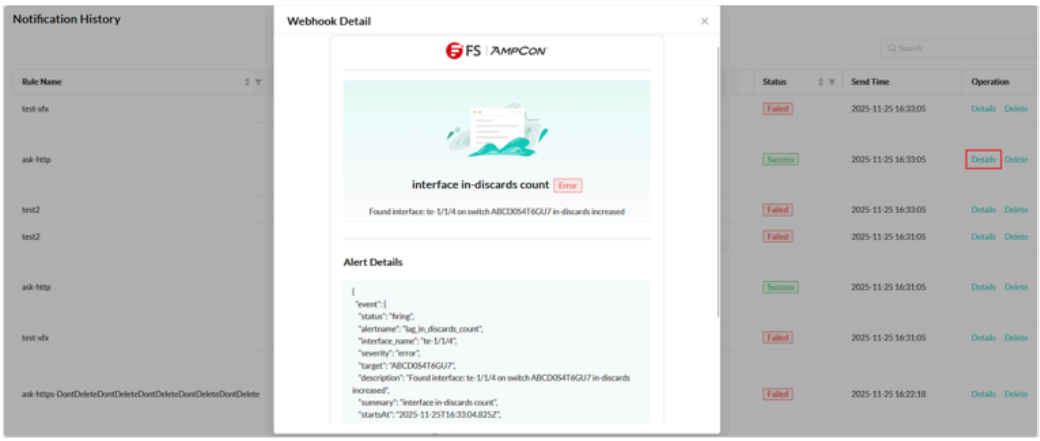
6. Optional: To check alert notifications sent in the last 30 days related to a notification rule, locate the rule in the **Rule** tab, and then click **Log**. For more information, see Viewing Historical Alert Notifications.

Checking Alert Notification History

In the AmpCon-DC UI, click **Monitor > Alerts > Notification History** from the navigation bar. Then, you can check the historical alerts sent to Splunk. For more information, see Viewing Historical Alert Notifications.



See the following example email notification:


Notification History
Webhook Detail
FS AMPCON
interface in-discards count
Error
Found interface: te-1/1/4 on switch ABCD054T6GU7 in-discards increased
Alert Details
{
"event": {
"status": "firing",
"alertname": "lag_in_discards_count",
"interface_name": "te-1/1/4",
"severity": "error",
"target": "ABCD054T6GU7",
"description": "Found interface: te-1/1/4 on switch ABCD054T6GU7 in-discards increased",
"summary": "interface in-discards count",
"startsAt": "2025-11-25T16:33:04.825Z",
Rule Name
Status
Send Time
Operation
test-xfx
Failed
2025-11-25 16:33:05
Details Delete
ask-http
Success
2025-11-25 16:33:05
Details Delete
test2
Failed
2025-11-25 16:33:05
Details Delete
test2
Failed
2025-11-25 16:31:05
Details Delete
ask-http
Success
2025-11-25 16:31:05
Details Delete
test-xfx
Failed
2025-11-25 16:31:05
Details Delete
ask-https-DontDeleteDontDeleteDontDeleteDontDeleteDontDelete
Failed
2025-11-25 16:22:18
Details Delete

Viewing Historical Alert Notifications

You can view alert notifications sent in the last 30 days for root cause analysis, fault prevention, or auditing.

Viewing All Alert Notifications
Viewing Alert Notifications Related to a Notification Rule
Viewing Details of an Alert Notification
Deleting an Alert Notification

Viewing All Alert Notifications

To view all alert notifications in the last 30 days, click **Monitor > Alerts > Notification History** from the navigation bar.

On the “Notification History” page, you can see all alert notifications sent in the last 30 days.

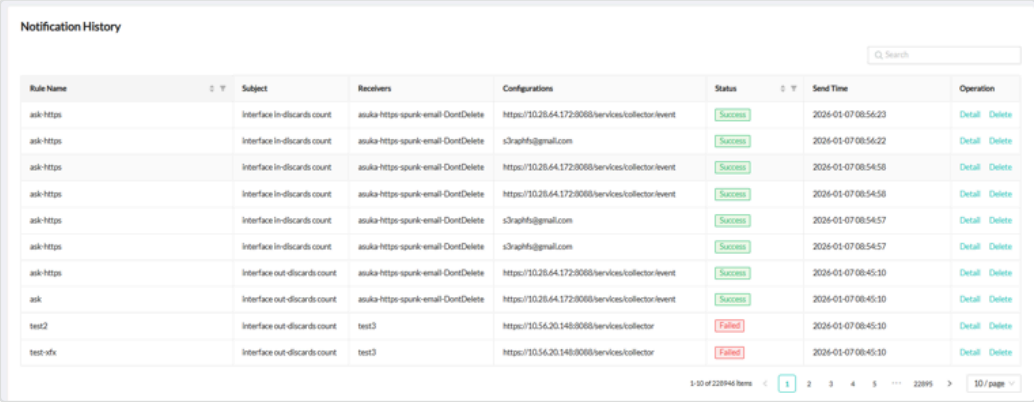


Table 1. Historical Alert Metrics

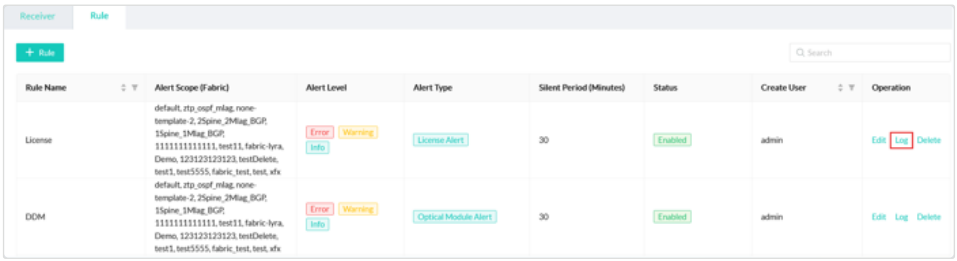
Metric	Description
Rule Name	The name of the alert notification rule.
Subject	The subject of the alert.
Receivers	The receiver to be notified.
Configurations	The recipient email addresses or webhook target URLs included in the receiver. **NOTEs** • If you see webhook target URLs in the **Configurations** column, it means the alert is sent to these Splunk servers.

	• If you see email addresses in the **Configurations** column, it means the alert is sent to these email addresses.
Status	Whether the alert is sent to the receiver successfully.
Send Time	The time when the alert is sent to the receiver.

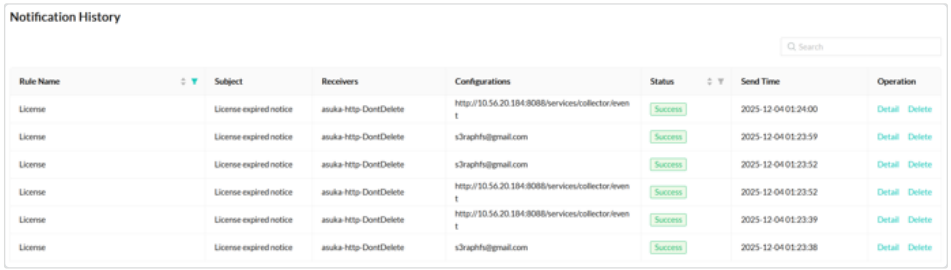
Viewing Alert Notifications Related to a Notification Rule

To view alert notifications in the last 30 days related to a specific notification rule, follow these steps:

1. Click **Monitor > Alerts > Alert Notification** from the navigation bar.
2. Click the **Rule** tab.
3. Locate the notification rule in the **Rule** tab, and then click **Log**.

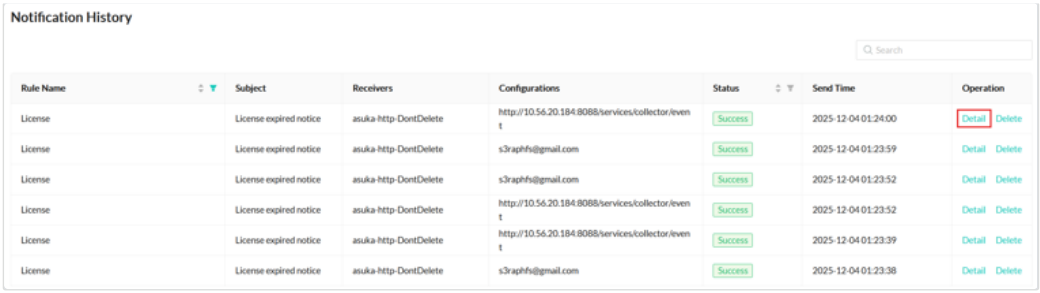


Then, on the “Notification History” page, you can see alert notifications sent in the last 30 days related to the notification rule.



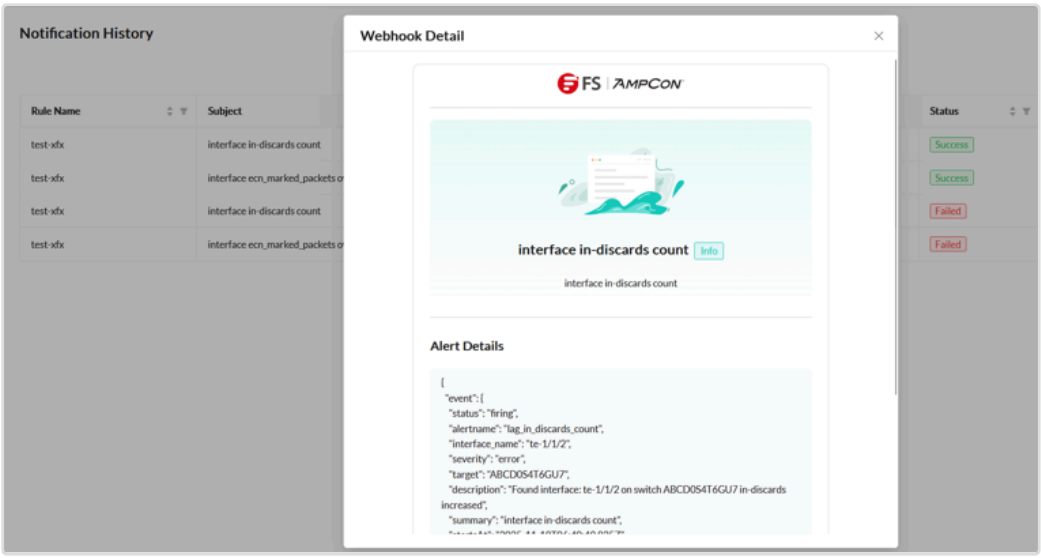
Viewing Details of an Alert Notification

To view details of an alert notification, locate the alert notification on the “Notification History” page, and then click **Detail**.



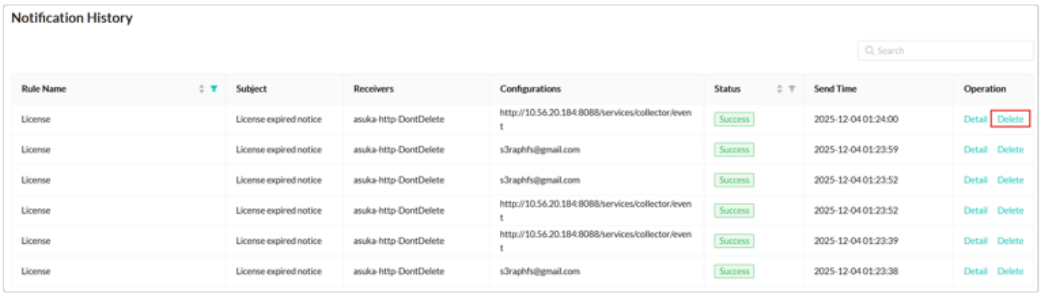
Then, you can see alert notification details in the **Webhook Detail** pop-up window.

> **NOTEs**
>
> - You can check details for only the alert notifications in **Success** status.
> - No details can be displayed for the alert notifications in **Failed** status.



Deleting an Alert Notification

To delete a historical alert notification, locate the alert notification, and then click **Delete**.



Managing Groups

You can create host groups with added third-party devices and create switch groups with managed switches. Then, assign these groups to group users so that each group user can manage only switches or third-party devices in the assigned groups.

For switch groups, you can also designate the operation permissions for each group so that the users in the group can perform only the allowed operations for switches in the group.

- Adding a Group
  - Adding a Switch Group
  - Adding a Host Group
- Assigning Groups to a User
- Editing a Group
  - Editing a Switch Group
  - Editing a Host Group
- Viewing All Switch and Host Groups
- Viewing Users Managing a Group
- Deleting a Group
  - Deleting a Switch Group
  - Deleting a Host Group

Adding a Group

You can add switch groups or host groups.

Adding a Switch Group

To add a switch group, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Group Management**.
2. On the “Group Management” page, click **+ Create**.
3. In the pop-up window, input the following information:

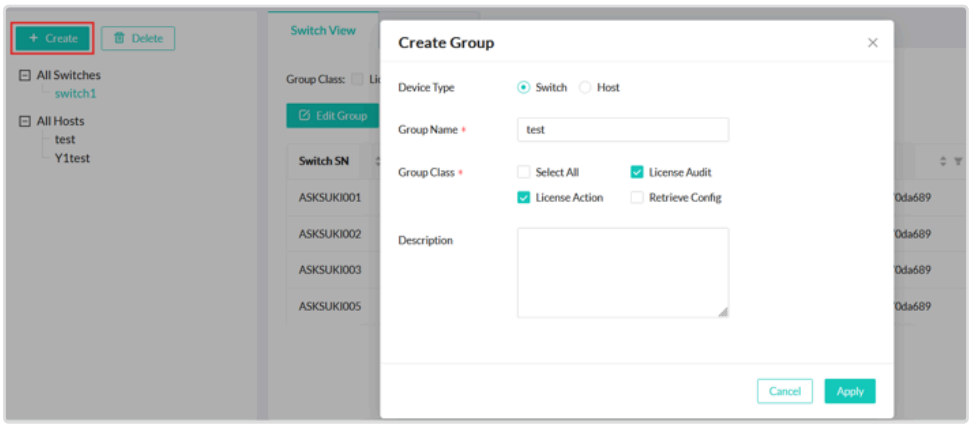


Table 1. Switch Group Parameters

Parameter	Description
Device Type	Select **Switch** to create a switch group.
Group Name	Specify the name of the switch group.
Group Class	Select one or multiple operation permissions allowed for switches in the switch group: • **License Audit:** You can perform the License Audit operation. • **License Action:** You can perform the License Action operation. • **Retrieve Config:** You can perform the configuration backup operation.
Description	Optional. Specify the description of the switch group.

4. Click **Apply**.

Adding a Host Group

To add a host group, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Group Management**.
2. On the “Group Management” page, click **+ Create**.
3. In the **Create Group** pop-up window, input the following information:

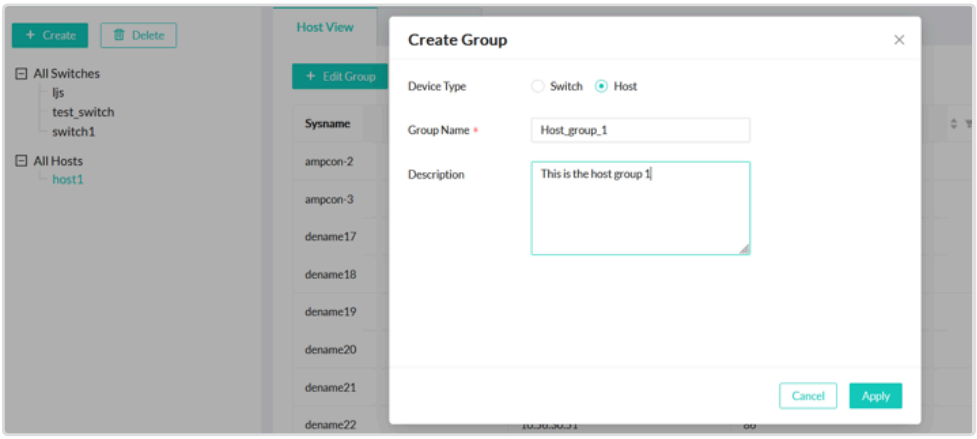


Table 2. Host Group Parameters

Parameter	Description

Device Type	Select **Host** to create a host group.
Group Name	Specify the name of the host group.
Description	Optional. Specify the description of the host group.

4. Click **Apply**.

Assigning Groups to a User

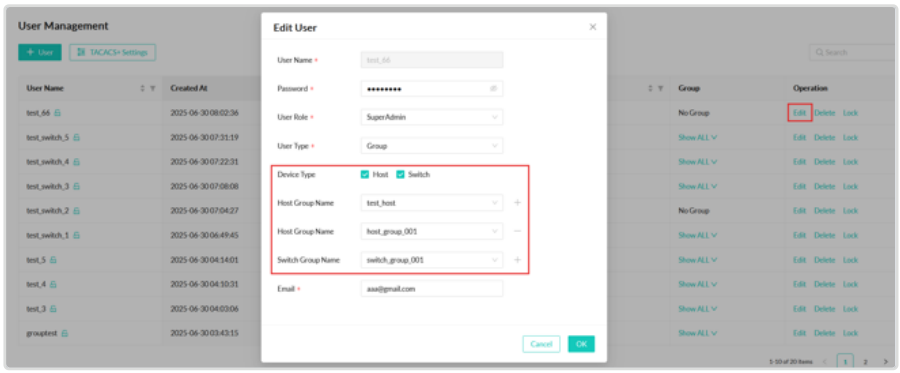
After you add switch groups and host groups, you can assign switch groups or host groups to an existing or a new AmpCon-DC group user. For more information about AmpCon-DC users, see Managing User Access.

- To assign groups to an existing group user, follow these steps:

  1. Click **System > User Management** from the navigation bar.
  2. Locate the user, and then click **Edit**.
  3. In the pop-up window, select **Group** in the **User Type** drop-down list,
  4. Select **Host**, **Switch**, or both in the **Device Type** section, which means assigning host groups, switch groups, or both to the group user.

     If you select **Host**, select a host group from the **Host Group Name** drop-down list. To add multiple host groups, click the plus icon **+**.

     If you select **Switch**, select a switch group from the **Switch Group Name** drop-down list. To add multiple switch groups, click the plus icon **+**.



- To assign groups to a new user, follow these steps:

  1. Click **System > User Management** from the navigation bar.
  2. Click **+ User**, and input the following information:

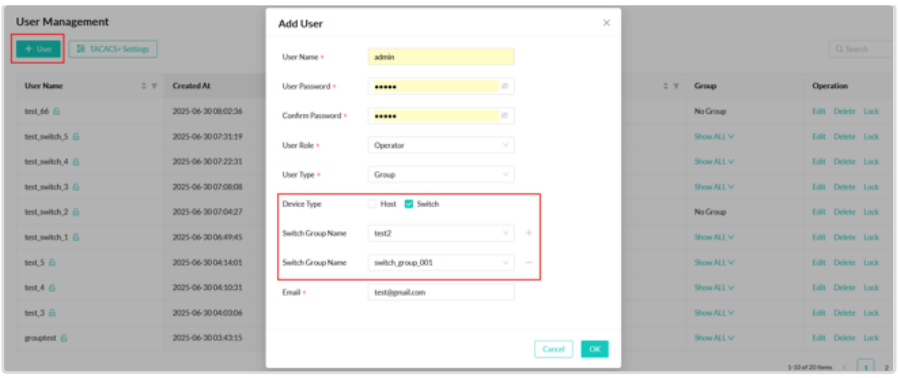


Table 3. Group User Parameters

Parameter	Description
User Name	Specify the username. The username must be unique.
User Password	Specify the password of the user. The password needs to be a combination of uppercase letters, lowercase letters, numbers, and special symbols. The character count needs to be greater than 10.
Confirm Password	Specify the password of the user.
User Role	Select **SuperAdmin**, **Admin**, **Operator**, or **Readonly**.
User Type	Select **Group**, which means creating a group user.
Device Type	Select **Host**, **Switch**, or both, which means assigning host groups, switch groups, or both to the user. • If you select **Host**, select a host group from the **Host Group Name** drop-down list. To add multiple host groups, click the plus icon **+**.

	• If you select **Switch**, select a switch group from the **Switch Group Name** drop-down list. To add multiple switch groups, click the plus icon **+**.
Email	Specify the email of the user.

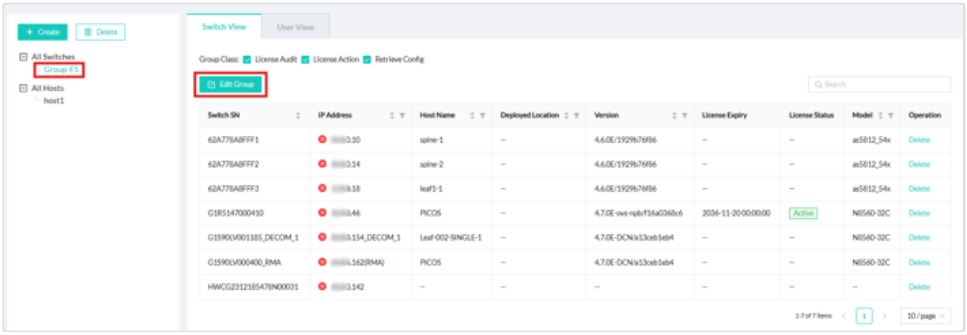
3. Click **Apply.**

Editing a Group

Editing a Switch Group

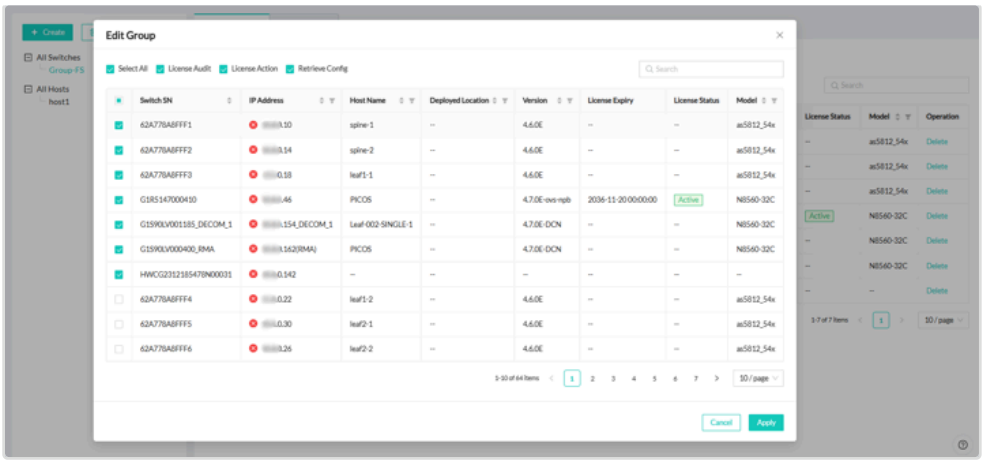
By editing a switch group, you can add switches to a group or remove switches from a group. In addition, you can modify the allowed operation permissions for switches in the group.

1. On the “Group Management” page, click **+** before **All Switches** in the left panel.
2. Click a switch group from the **All Switches** list.
3. In the **Switch View** tab, click **Edit Group**.



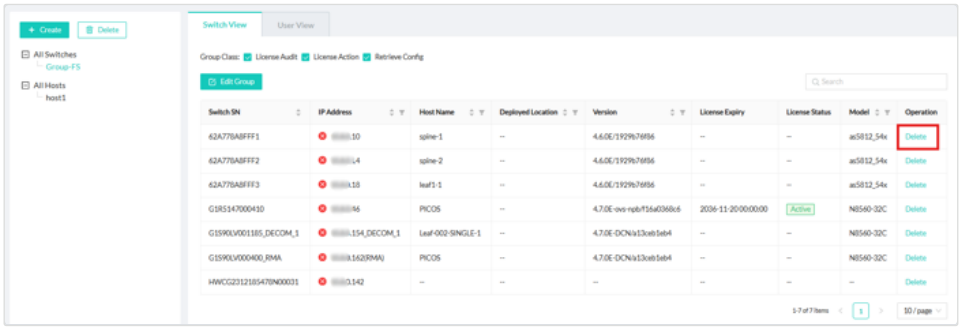
4. In the pop-up window, do the following operations:

- Select the switches to be added to the switch group.
- To remove switches from the switch group, unselect the switches.
- Select the allowed operation permissions, including **License Audit**, **License Action**, and **Retrieve Config**.



5. Click **Save**.

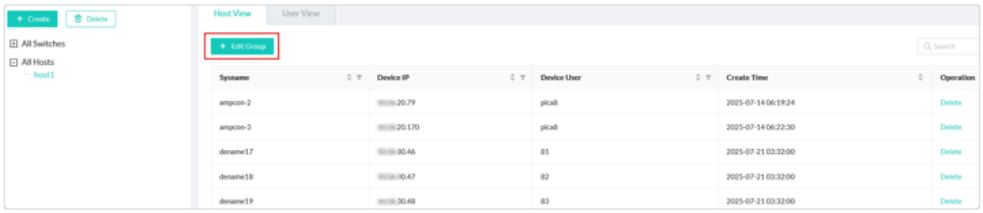
   You can try another way to remove a switch from a switch group. In the **Switch View** tab, locate the switch, and then click **Delete**.



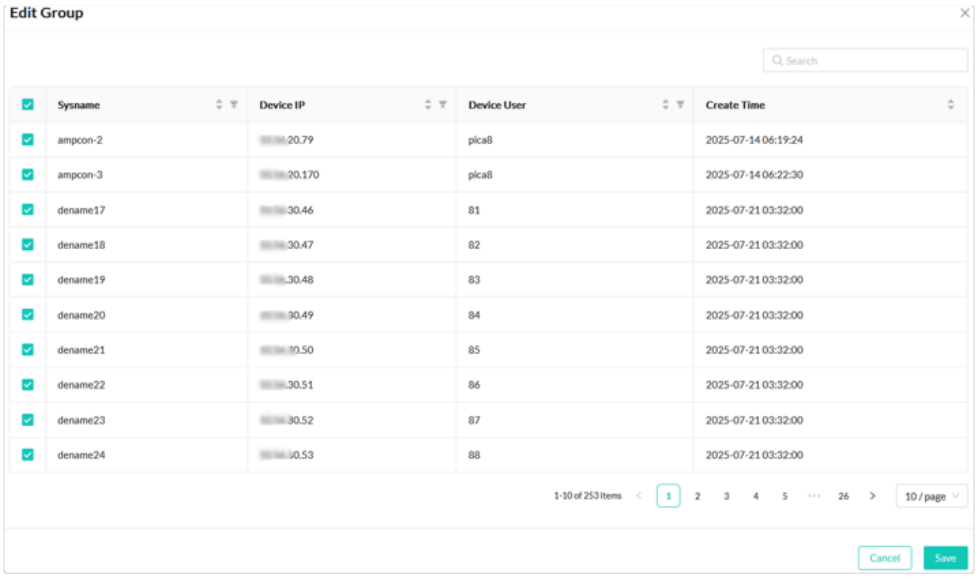
Editing a Host Group

By editing a host group, you can add third-party devices to a host group or remove devices from a host group.

1. On the “Group Management” page, click **+** before **All Hosts** in the left panel.
2. Click a host group from the **All Hosts** list.
3. In the **Host View** tab, click **Edit Group**.



4. In the pop-up window, do the following operations:



- Select third-party devices to be added to the host group.
- To remove third-party devices from the host group, unselect the devices.

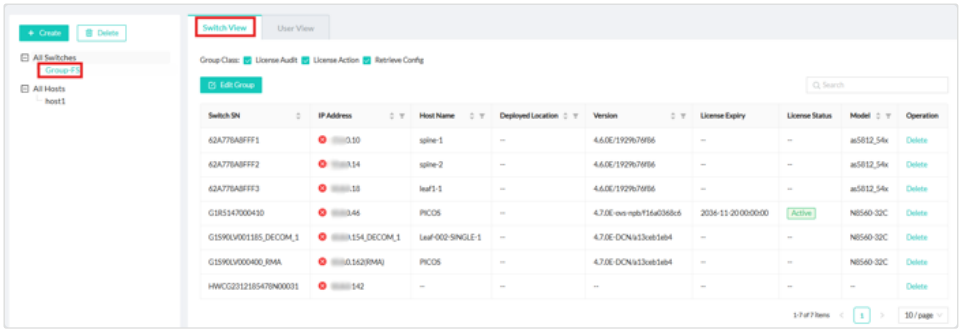
5. Click **Save**.

   You can try another way to remove a host from a host group. In the **Host View** tab, locate the host, and then click **Delete**.



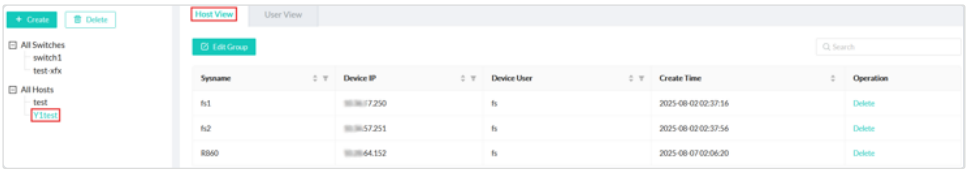
Viewing All Switch and Host Groups

- To view all added switch groups, click **+** before **All Switches** in the left panel of the “Group Management” page.
- To view all switches in a switch group, click the switch group name, and then check the **Switch View** tab.



- To view all added host groups, click **+** before **All Hosts** in the left panel of the “Group Management” page.

- To view all hosts in a host group, click the host group name, and then check the **Host View** tab.



Viewing Users Managing a Group

You can view AmpCon-DC users managing a switch group or a host group. If no users are listed, it means that you haven't assigned the group to any AmpCon-DC users.

- To view AmpCon-DC users managing a switch group, follow these steps:

  1. On the "Group Management" page, click **+** before **All Switches**, and then click the switch group from the **All Switches** list.

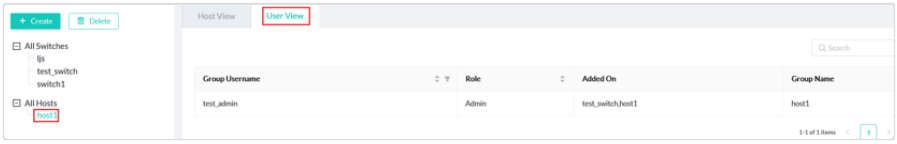
  2. Click the **User View** tab, and then check the users managing the switch group.



- To view users managing a host group, follow these steps:

  1. On the "Group Management" page, click **+** before **All Hosts**, and then click the host group from the **All Hosts** list.

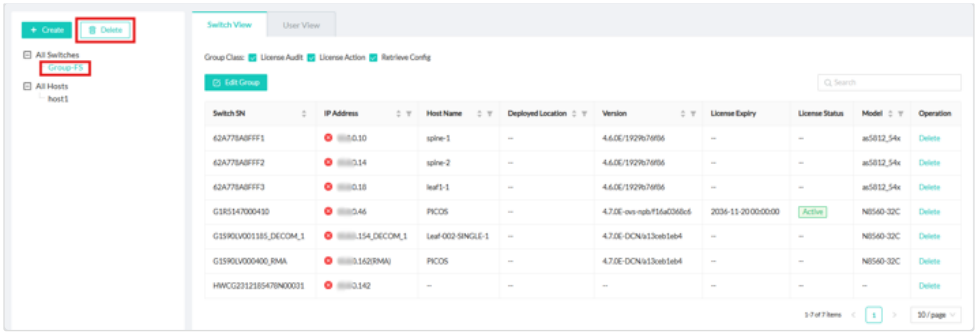
  2. Click the **User View** tab, and then check the users managing the host group.



Deleting a Group

Deleting a Switch Group

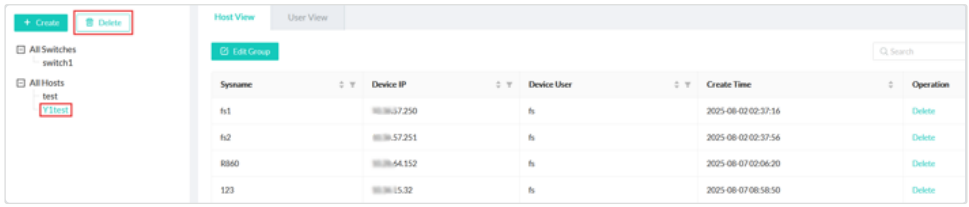
1. On the "Group Management" page, click **+** before **All Switches** in the left panel.
2. Click a switch group from the **All Switches** list, and then click **Delete**.



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

Deleting a Host Group

1. On the “Group Management” page, click the icon **+** before **All Hosts** in the left panel.
2. Click a switch group from the **All Hosts** list, and then click **Delete**.



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

Managing Licenses

In the AmpCon-DC UI, you can manage AmpCon-DC licenses and PicOS licenses. For more information, see the following child topics:

- Managing AmpCon-DC Licenses
- Managing PicOS Licenses

Managing AmpCon-DC Licenses

You can import a new or updated AmpCon-DC license to manage more switches, view all imported AmpCon-DC licenses, convert a trial AmpCon-DC license to a standard AmpCon-DC license, invalidate the AmpCon-DC license on a switch to release the license, or check license-related logs and alerts.

See the following child topics:

- Importing Licenses for Deployed Switches
- Importing Licenses for Imported Switches
- Troubleshooting for License Importing
- Converting a Trial License to Standard Licenses
- Viewing AmpCon-DC Licenses
- Invalidating a License
- Checking License Logs and Alerts

NOTEs

Before you import AmpCon-DC licenses, pay attention to the following guidelines:

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

  Each AmpCon-DC server supports managing only switches with the same license type.
- If AmpCon-DC licenses are not imported or the imported AmpCon-DC licenses are expired, some of the AmpCon-DC features will not work, such as Zero Touch Provisioning (ZTP) of switches.
- During the grace period of a trial AmpCon-DC license, the AmpCon-DC login interface displays "License is expired, you have a 14-day grace period". You can purchase a standard license to continue using AmpCon-DC.

- From 15 days before a standard AmpCon-DC license expires until after the license expires, notification messages are displayed when you log in to the AmpCon-DC UI to remind you to renew the license.
- If a standard AmpCon-DC license expires, you can see the license status is expired in the **License Alert** section of the “License Log” page. For more information, see Checking License Alerts. In this case, ask the sale team to renew the AmpCon-DC license in the License Portal. Then, download the renewed license, and import it to AmpCon-DC.

Importing Licenses for Deployed Switches

To onboard switches through normal ZTP or simplified ZTP, you must import AmpCon-DC licenses (containing the Hardware IDs of the switches) to AmpCon-DC automatically or manually so that AmpCon-DC can manage these switches.

Prerequisites
Importing Licenses Automatically
Importing Licenses Manually
1. Obtaining Hardware IDs in Batches
2. Creating an AmpCon-DC License
3. Importing an AmpCon-DC License to AmpCon-DC
Optional: Editing an AmpCon-DC License

Prerequisites

- For white-box switches deployed through normal ZTP, ensure that all the preparations in Before You Begin and **Step 1** to **Step 6** in Provisioning a White-Box Switch are completed.
- For integrated hardware and software switches deployed through normal ZTP, ensure that all the preparations in Before You Begin and **Step 1** to **Step 4** in Provisioning an Integrated Hardware and Software Switch are completed.
- For switches deployed through simplified ZTP, ensure that **Step 1** to **Step 3** in Preparing for Simplified ZTP are completed.

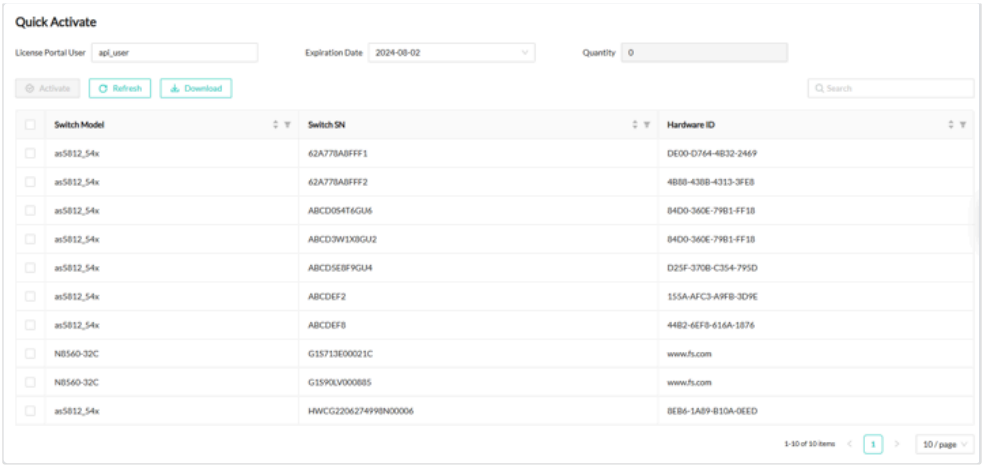
Importing Licenses Automatically

When AmpCon-DC is stably connected to the License Portal, you can import AmpCon-DC licenses to AmpCon-DC automatically, eliminating the need for complex manual processes.

This feature significantly reduces time and operational costs, streamlines management, and is especially beneficial for large-scale switch license management scenarios.

To import an AmpCon-DC license automatically, follow these steps:

1. Click **System > Software Licenses > License Management** from the navigation bar, and then click **Quick Activate**. You can see all switches provisioned with ZTP and without AmpCon-DC licenses assigned.



2. Optional: To manually refresh the list of switches with no AmpCon-DC license assigned, click **Refresh**.

> **NOTE**
>
> You are recommended to manually refresh the list of switches with no AmpCon-DC license assigned. Reasons are as follows:
>
> - If the network is available and stable, AmpCon-DC will automatically retrieve the latest **Expiration Date** and **Quantity** information from the License Portal and display the latest switch list in the AmpCon-DC UI.
> - But if AmpCon-DC fails to retrieve information from the License Portal due to network issues, you can manually refresh the latest **Expiration Date** and **Quantity** information and the list of switches with no AmpCon-DC license assigned.

3. Check the quantity of Hardware IDs that can be bound with the AmpCon-DC license for a specific expiration date:

   a. In the **Expiration Date** drop-down list, select an expiration date.

   > **NOTE**
   >
   > Trial licenses are marked with the string "(trial)".

   b. In the **Quantity** field, check the quantity of Hardware IDs that can be bound with the AmpCon-DC license for the selected expiration date.

4. Select one or multiple switches to which you want to assign AmpCon-DC licenses.

> **NOTE**
>
> The total number of selected switches must be no longer than the value of **Quantity**. Or else, the **Activate** button cannot be clicked.

5. Click **Activate**.

Then, AmpCon-DC uploads the information, including the switches and expiration date you selected, to the License Portal. The License Portal will create the corresponding AmpCon-DC license, which will be automatically imported to AmpCon-DC.

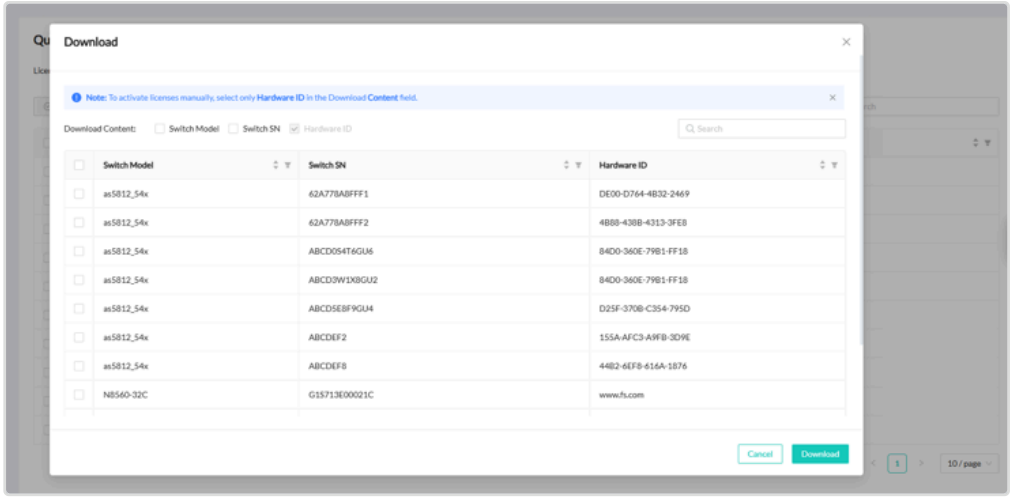
Importing Licenses Manually

When AmpCon-DC cannot connect to the License Portal or the connection is unstable, you need to import AmpCon-DC licenses to AmpCon-DC manually. To import an AmpCon-DC license manually, follow these steps:

1. Obtaining Hardware IDs in Batches

To manually import licenses to all switches, you need to obtain the hardware IDs of each switch that you want to manage first.

1. Click **System > Software Licenses > License Management** from the navigation bar, and then click **Quick Activate**. You can see all switches provisioned with ZTP and without an AmpCon-DC license assigned.
2. Click **Download**. In the **Download Content** section, the **Hardware ID** is selected by default.



3. Select one or multiple switches you want to retrieve hardware IDs.
4. Click **Download**. Then AmpCon-DC will generate a .xlsx file with the hardware IDs of these switches.

> **NOTE**

Don’t modify the generated .xlsx file. Or else, the license creating process might fail.

2. Creating an AmpCon-DC License

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

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

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

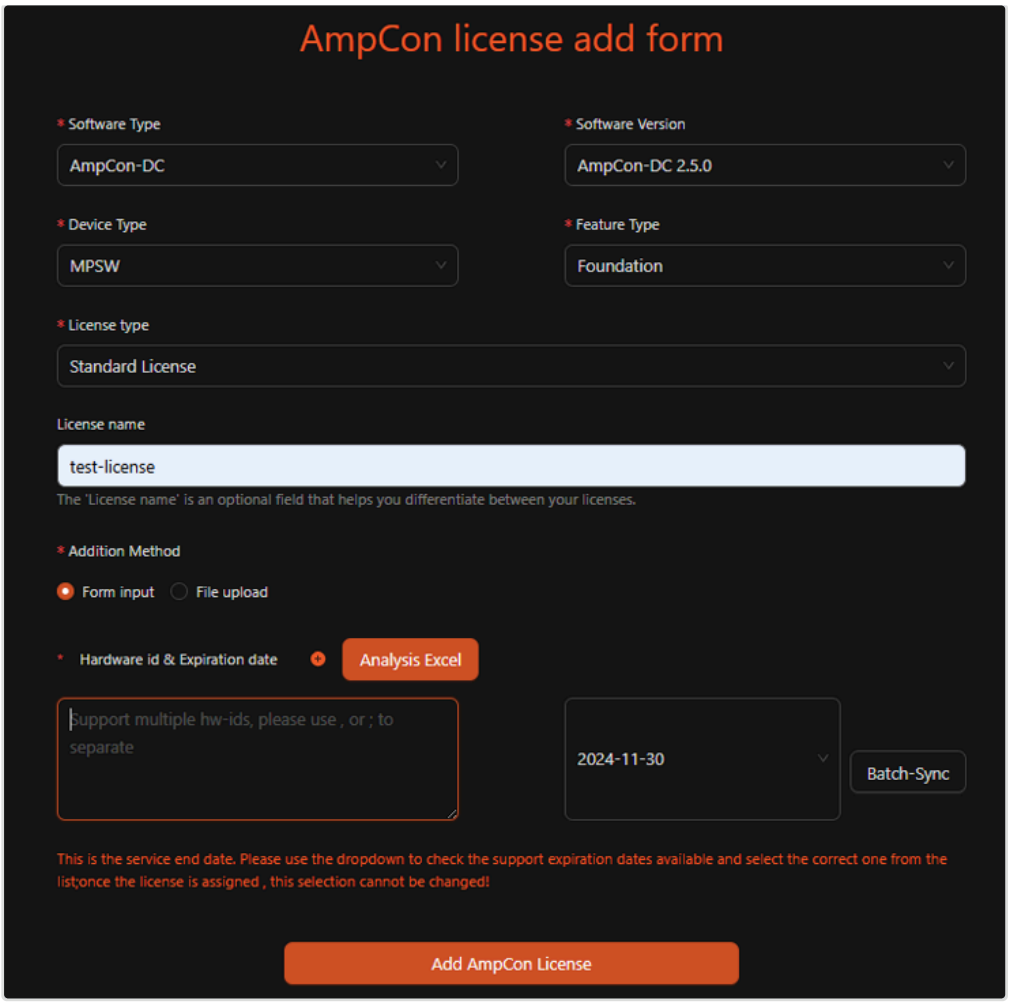
2. Input the following information:

- **Software Type**: Select **AmpCon-DC**.
- **Software Version**: Select **AmpCon-DC 2.5.0**.

> **NOTE**
>
> If you use AmpCon-DC 2.5.1, select **AmpCon-DC 2.5.1** in the **Software Version** drop-down list.

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

3. In the **Addition Method** section, click **Form input**.



4. Click **Analysis Excel** to upload the .xlsx file generated in the 1. Obtaining Hardware IDs in Batches section, and select the expiration date.

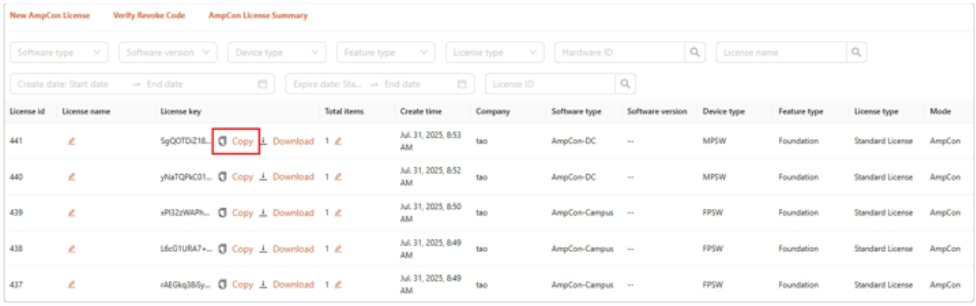
> **Tip**
>
> To apply a specific expiration date to all blank drop-down lists, locate the expiration date, and then click **Batch-Sync**.

5. Click **Add AmpCon License**.

3. Importing an AmpCon-DC License to AmpCon-DC

To import an AmpCon-DC license to AmpCon-DC, follow these steps:

1. Get the updated or new license from the License Portal.
   a. Log in to the License Portal, and then click **AmpCon Licenses**.
   b. Click **Copy** to copy the license string or click **Download** to download the .lic license file.

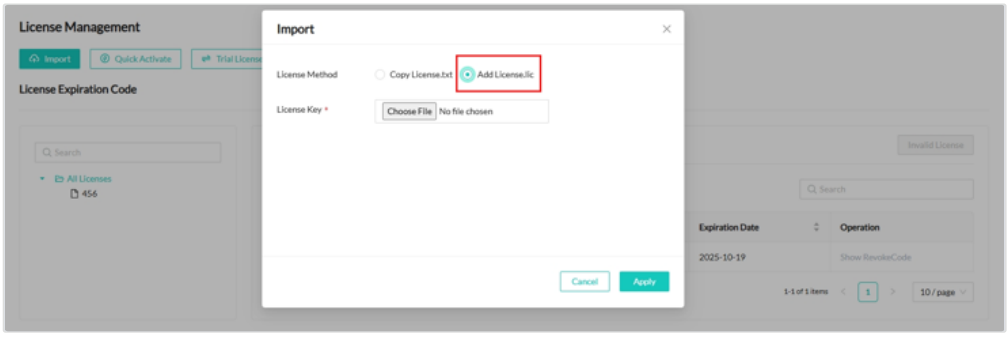


2. In the AmpCon-DC UI, click **System > Software Licenses > License Management** from the navigation bar.
3. On the “License Management” page, click **Import**.
4. Select either of the following ways to import licenses:

- Select **Copy License.txt**, and paste the license strings that you copied in **step 1.b** to the **License Key** box.



- Select **Copy License.lic**, and then upload the .lic license file that you downloaded in **step 1.b** in the **License Key** selection box.



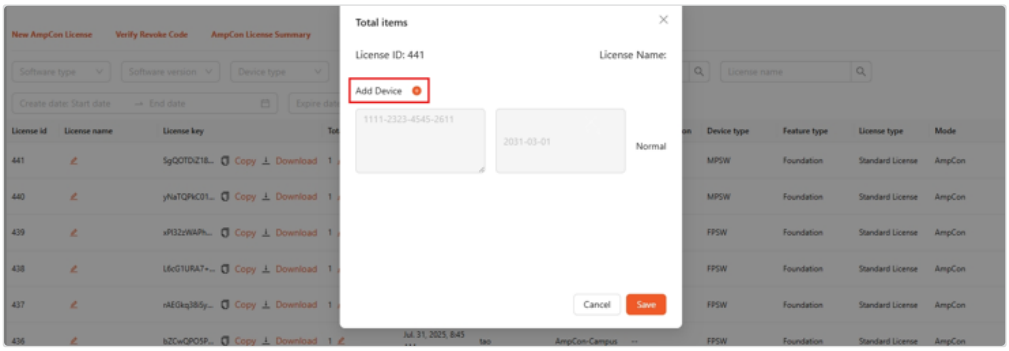
5. Click **Apply**.

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

Optional: Editing an AmpCon-DC License

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

1. Log in to the License Portal, and click **AmpCon Licenses**.
2. Locate the license that you want to edit, and click the edit icon in the **Total hw-ids** column.
3. Click the Add Device icon, enter the Hardware ID of each new switch that you want to manage, and select the expiration date.



4. Click **Save**.

> **NOTE**
>
> After you edit a license, import the updated AmpCon-DC license to AmpCon-DC so that newly added switches can be managed by AmpCon-DC.

Importing Licenses for Imported Switches

To onboard switches by importing switches, you must import AmpCon-DC licenses (containing the Hardware IDs of the switches) to AmpCon-DC manually so that AmpCon-DC can manage these switches.

1. Obtaining Hardware IDs
2. Creating an AmpCon-DC License
3. Importing an AmpCon-DC License to AmpCon-DC

Optional: Editing an AmpCon-DC License

1. Obtaining Hardware IDs

To manually import the licenses to all switches, you need to obtain the Hardware ID of each switch that you want to manage first. Follow these methods:

1. SSH log in to each switch and run the following commands:

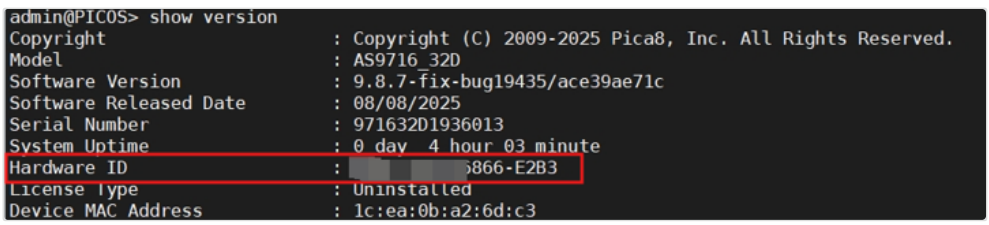
```
run start shell sh
```

```
sudo license -s
```



2. SSH log in to each switch and run the following command:

```
show version
```



2. Creating an AmpCon-DC License

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

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

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

2. Input the following information:

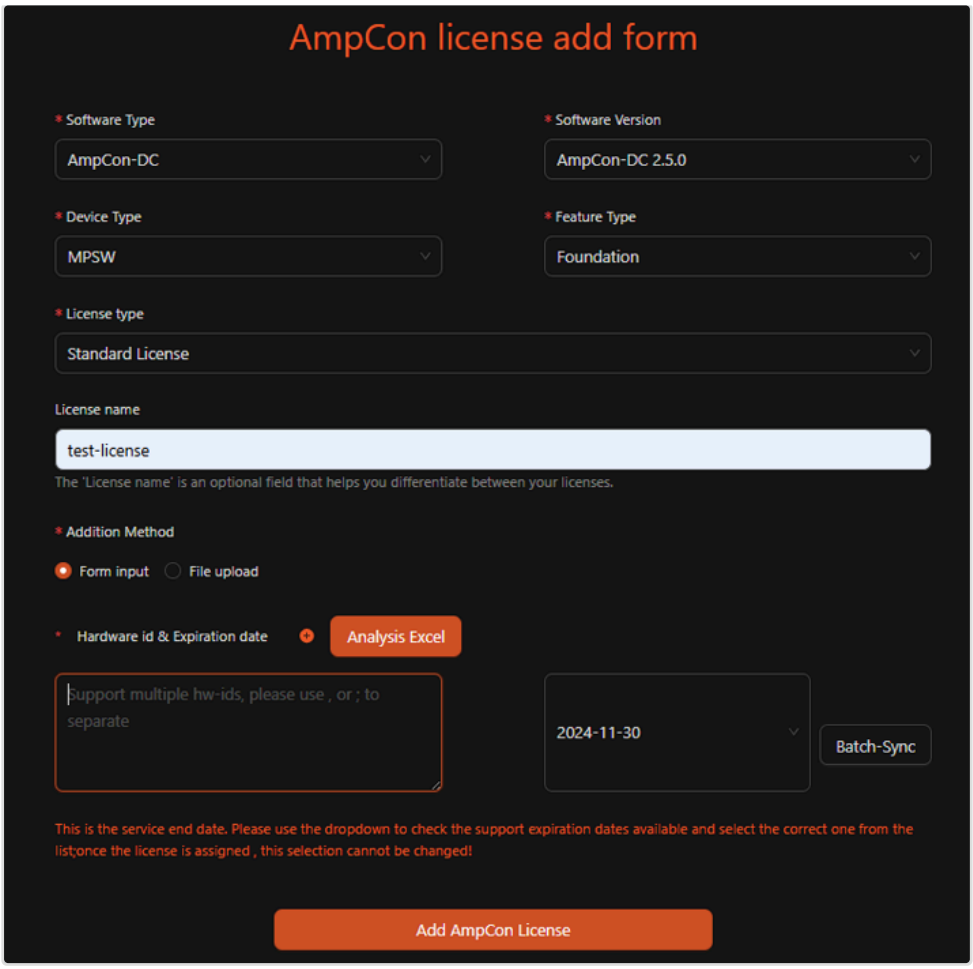
- **Software Type**: Select **AmpCon-DC**.
- **Software Version**: Select **AmpCon-DC 2.5.0**.

> **NOTE**
>
> If you use AmpCon-DC 2.5.1, select **AmpCon-DC 2.5.1** in the **Software Version** drop-down list.

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

3. In the **Addition Method** section, select either of the following ways:

- **Form input**: Enter the Hardware IDs of switches to be managed with AmpCon-DC, and select the expiration date.



> **Tip**
>
> To apply a specific expiration date to all blank drop-down lists, locate the expiration date, and then click **Batch-Sync**.

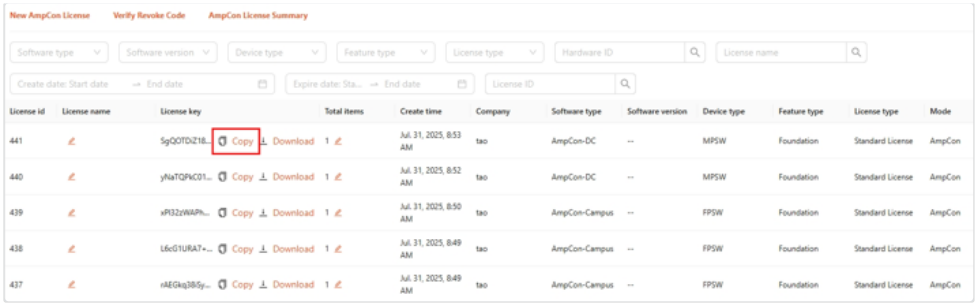
- **File upload**: Click **Upload** to upload a .xlsx file with the Hardware IDs of switches to be managed with AmpCon-DC and the expiration date. You can click **Blank template** to download a .xlsx template file.

4. Click **Add AmpCon License**.

3. Importing an AmpCon-DC License to AmpCon-DC

To import an AmpCon-DC license to AmpCon-DC, follow these steps:

1. Get the updated or new license from the License Portal.
   a. Log in to the License Portal, and then click **AmpCon Licenses**.
   b. Click **Copy** to copy the license string or click **Download** to download the .lic license file.

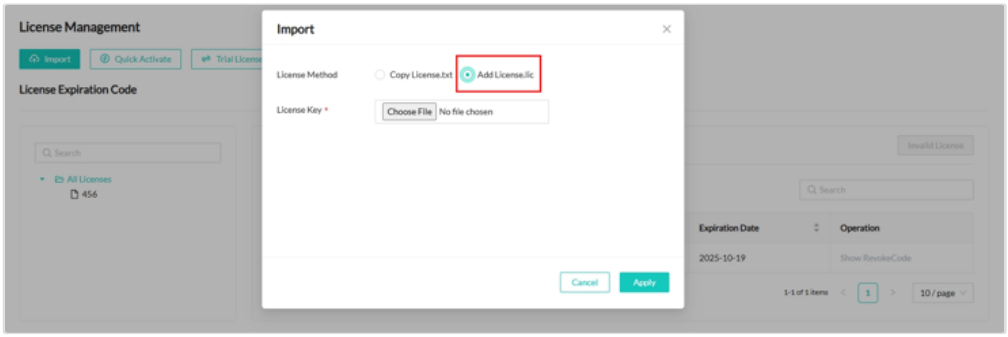


2. In the AmpCon-DC UI, click **System > Software Licenses > Licenses Management** from the navigation bar.
3. On the “Licenses Management” page, click **Import**.
4. Select either of the following ways to import licenses:

- Select **Copy License.txt**, and paste the license strings that you copied in **step 1.b** to the **License Key** box.



- Select **Copy License.lic**, and then upload the .lic license file that you downloaded in **step 1.b** in the **License Key** selection box.



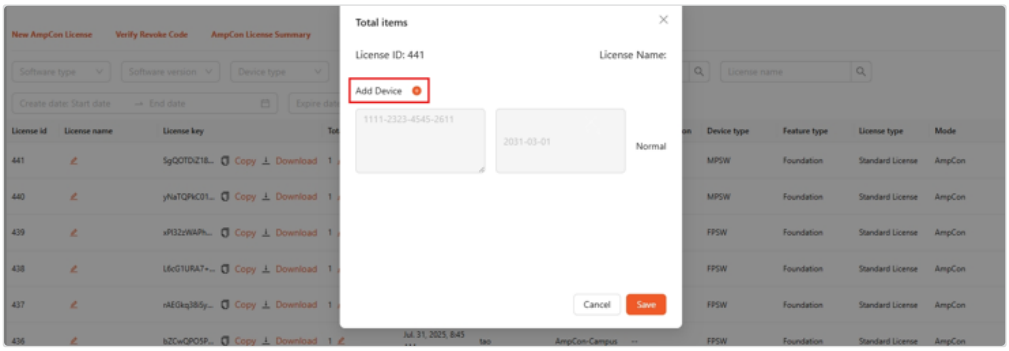
5. Click **Apply**.

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

Optional: Editing an AmpCon-DC License

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

1. Log in to the License Portal, and click **AmpCon Licenses**.
2. Locate the license that you want to edit, and click the edit icon in the **Total hw-ids** column.
3. Click the Add Device icon, enter the Hardware ID of each new switch that you want to manage, and select the expiration date.



4. Click **Save**.

> **NOTE**
>
> After you edit a license, import the updated AmpCon-DC license to AmpCon-DC so that newly added switches can be managed by AmpCon-DC.

Troubleshooting for License Importing

If you fail to import AmpCon-DC licenses, refer to the following reasons and solutions:

Automatic License Importing Issues
- Abnormal Network Connection
- Insufficient AmpCon-DC Licenses
- License Portal Authentication Failed
- Outdated Information

Manual License Importing Issues
- Abnormal Network Connection
- Insufficient AmpCon-DC Licenses
- License Portal Authentication Failed
- Outdated Information
- Wrong Hardware ID in the Uploaded File

Automatic License Importing Issues

When you automatically import an AmpCon-DC license, you might see the following errors in the AmpCon-DC UI. To resolve these issues, check related solutions:

Abnormal Network Connection

Error:

- Abnormal network connection.
- Failed to obtain the License Key. Please try again later.

Root Cause: The network between the License Portal and the AmpCon-DC server is unavailable or unstable.

Solution: Check and resolve the network connection issues between the License Portal and the AmpCon-DC server.

Insufficient AmpCon-DC Licenses

Error: The number of selected switches can't be more than the number of Hardware IDs that can be bound with the AmpCon license for the selected expiration date.

Root Cause: The total number of selected switches is more than the number of Hardware IDs that can be bound with the AmpCon-DC license for the selected expiration date.

Solution:

- Click **System > Software Licenses > Licenses Management** from the navigation bar, and then click **Quick Activate**. Click **Refresh** to manually refresh the number of remaining

Hardware IDs that can be bound with the AmpCon-DC license for the selected expiration date.

- Reduce the total number of switches selected with the expiration date specified.
- Select a different expiration date to activate the remaining switches.
- Purchase more AmpCon-DC licenses.

License Portal Authentication Failed

Error: The License Portal authentication failed. Please try again after updating license portal information in the global system configuration.

Root Cause: The License Portal information that you entered in the global system configuration is incorrect.

Solution: Re-enter the **License Portal URL**, **License Portal User**, and **License Portal Password** in the global system configuration, and then check the connectivity. For more information, see Checking License Portal Connectivity.

Outdated Information

Error: xxx.xxx.xxx (HW ID) has bound the license. Please check and try again.

Root Cause: The switch that you are activating has been assigned with an AmpCon-DC license.

Solution:

- Click **Refresh** to manually refresh the list of switches with no AmpCon-DC licenses.
- Resolve network issues between the AmpCon-DC server and the License Portal.

Manual License Importing Issues

When you manually import an AmpCon-DC license, you might see the following errors in the AmpCon-DC UI. To resolve these issues, check related solutions:

Abnormal Network Connection

Error: Failed to obtain the License Key. Please try again later.

Root Cause: The network between the License Portal and the AmpCon-DC server is unavailable or unstable.

Solution: Check and resolve the network connection issue between the License Portal and the AmpCon-DC server.

Insufficient AmpCon-DC Licenses

Error: The number of selected switches can't be more than the number of Hardware IDs that can be bound with the AmpCon license for the selected expiration date.

Root Cause: The total number of selected switches is more than the number of Hardware IDs that can be bound with the AmpCon-DC license for the selected expiration date.

Solution:

- Reduce the total number of switches specified with the expiration date.
- Select a different expiration date to activate the remaining switches.
- Purchase more AmpCon-DC licenses.

License Portal Authentication Failed

Error: The License Portal account or password does not match. Please check and try again.

Root Cause: The License Portal information that you entered in the License Portal is incorrect or does not match.

Solution: Re-enter the username and password you input to log in to the License Portal.

Outdated Information

Error: xxx.xxx.xxx (HW ID) has bound the license. Please check and try again.

Root Cause: The switch that you are activating has been assigned with an AmpCon-DC license.

Solution:

- Click **Refresh** to manually refresh the list of switches AmpCon-DC PicOS licenses.
- Resolve network issues between the AmpCon-DC server and the License Portal.

Wrong Hardware ID in the Uploaded File

Error:

- There is no HW ID in the table. Please check and try again.
- xxx.xxx (HW ID) is repeated. Please check and try again.
- The format of the Hardware ID filled in is incorrect. Please check.

Root Cause: The hardware IDs are not entered, are repeated, or are in wrong format.

Solution: Ensure hardware IDs are correctly entered and not duplicated in the uploaded file.

Converting a Trial License to Standard Licenses

You can convert a trial license to one or multiple standard licenses automatically when AmpCon-DC is stably connected to the License Portal.

> **NOTEs**
>
> - On AmpCon-DC, you have only one chance to convert trial licenses to standard licenses.
> - If more switches need trial license conversion, perform the operation in the License Portal.

Prerequisites
Procedure
Guidelines for Applying Expiration Date

Prerequisites

- Ensure that AmpCon-DC can connect with the License Portal through the License Portal username and password in related system configurations. For more information, see Checking License Portal Connectivity.
- Ensure that the sale team have created standard AmpCon-DC licenses for you in the License Portal.

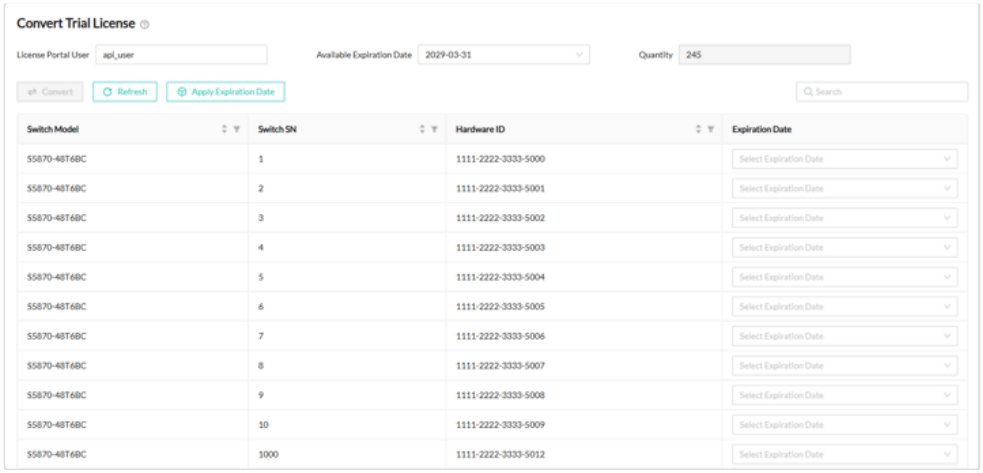
Procedure

To convert a trial AmpCon-DC license to one or multiple standard licenses automatically, follow these steps:

1. Click **System > Software Licenses > License Management** from the navigation bar, and then click **Trial License Conversion**.

   You can view all switches managed by AmpCon-DC with a trial license assigned.

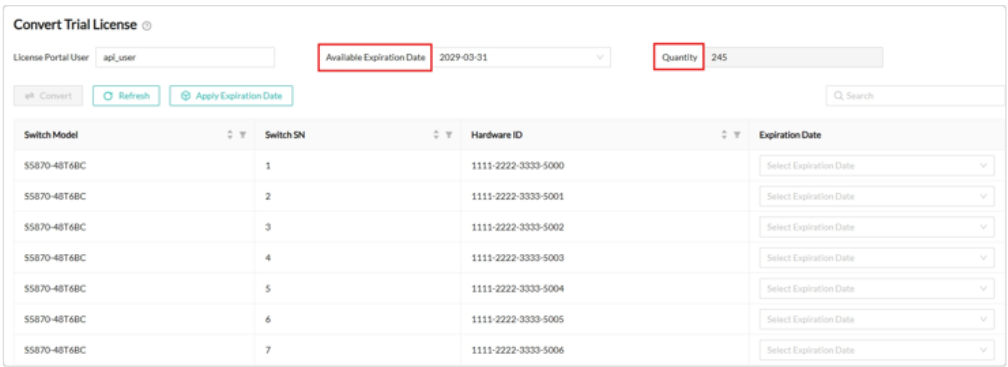
   > **NOTE**
   >
   > The **Trial License Conversion** button is visible only when a trial license has been imported into AmpCon-DC and no standard license has been imported.



2. Optional: To manually refresh the list of switches with a trial license assigned, click **Refresh**.

> **NOTE**
>
> You are recommended to manually refresh the list of switches with a trial license assigned. Reasons are as follows:
>
> - If the network is available and stable, AmpCon-DC will automatically retrieve the latest **Expiration Date** and **Quantity** information from the License Portal and display the latest switch list in the AmpCon-DC UI.
> - But if AmpCon-DC fails to retrieve information from the License Portal due to network issues, manually refresh the latest **Expiration Date** and **Quantity** information and the list of switches with a trial license assigned.

3. Check the quantity of Hardware IDs that can be bound with the AmpCon-DC license for a specific expiration date:



a. In the **Available Expiration Date** drop-down list, select an expiration date.

b. In the **Quantity** field, check the quantity of Hardware IDs allowed by the selected expiration date.

4. For switches with different expiration dates, locate each switch, and then select an expiration date in the **Expiration Date** drop-down list.
5. For switches with the same expiration date, select the expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. For how expiration dates are applied, see Guidelines of Applying Expiration Date.
6. Click **Convert** to complete the conversion.

> **NOTE**
>
> The switches without **Expiration Date** specified will be removed from AmpCon-DC after the operation.

Guidelines for Applying Expiration Date

After you click **Apply Expiration Date**, AmpCon-DC will analyze the following counts first:

- **Count A:** The count of the switches without **Expiration Date** specified.
- **Count B:** The count of Hardware IDs allowed by the selected expiration date in the **Available Expiration Date** drop-down list.

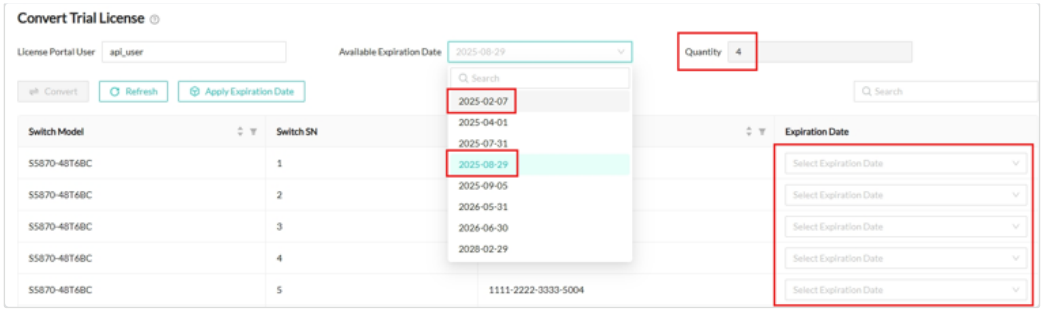
If **Count A** is less than **Count B**, AmpCon-DC will automatically apply the selected expiration date to all the switches without **Expiration Date** specified.

If **Count A** is more than **Count B**, AmpCon-DC will automatically apply the selected expiration date to switches without **Expiration Date** specified from top to bottom.

For the remaining switches without **Expiration Date** specified, the **Expiration Date** drop-down list are blank. You can do as follows:

- Select another expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. This expiration date will be assigned to the remaining switches by AmpCon-DC automatically.
- Select another expiration date in the **Expiration Date** drop-down list manually.

Example:



The count of the switches without **Expiration Date** specified is 5, the selected expiration date (2025-08-29) allows for 4 Hardware IDs.

In this case, you click the **Apply Expiration Date** button. AmpCon-DC will automatically assign the selected expiration date (2025-08-29) to the first 4 switches. For the remaining 1 switch without an **Expiration Date** specified, you can do as follows:

- Select another expiration date in the **Available Expiration Date** drop-down list, and then click **Apply Expiration Date**. This expiration date will be assigned to the remaining 1 switch by AmpCon-DC automatically.
- Select another expiration date in the **Expiration Date** drop-down list manually.

Viewing AmpCon-DC Licenses

In the AmpCon-DC UI, click **System > Software Licenses > License View**. You can see the AmpCon-DC licenses that are imported to AmpCon-DC.

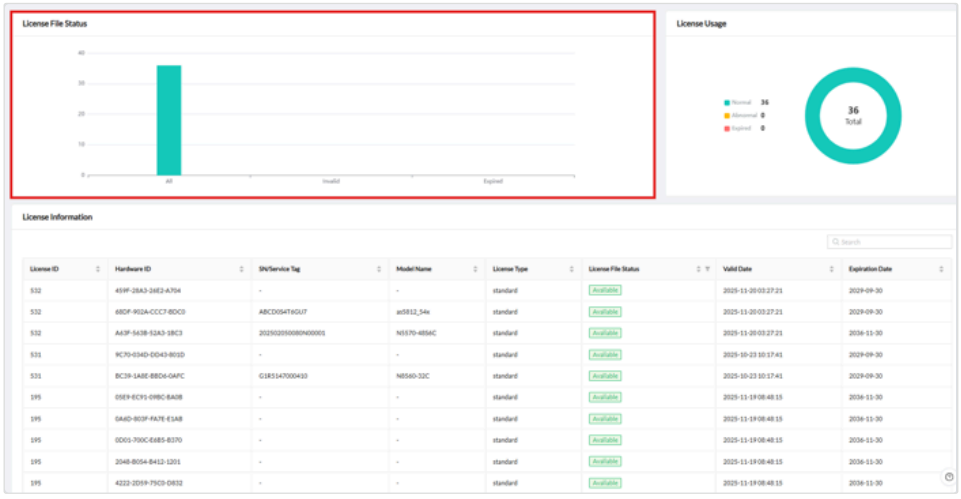
In addition, you can see the status and usage information of these AmpCon-DC licenses.

License Status
License Usage
License Details
Fuzzy Search for License Information

License Status

In the **License File Status** section, you can see the numbers of **All**, **Invalid**, and **Expired** AmpCon-DC licenses. See the following descriptions of each status:

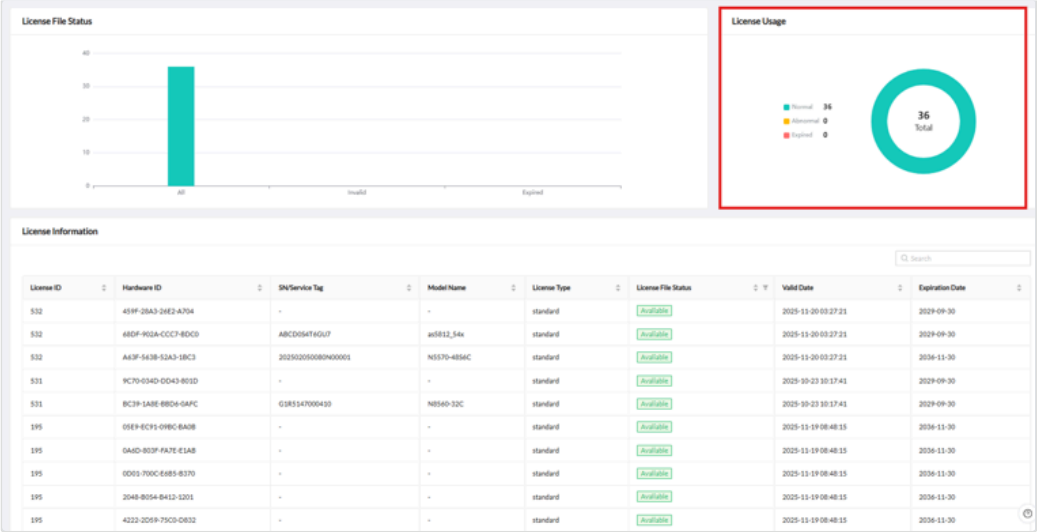
- **All:** All licenses.
- **Invalid:** The invalid licenses.
- **Expired:** The expired licenses.



License Usage

In the **License Usage** section, you can see the numbers of normal, abnormal, and expired AmpCon-DC licenses. See the following descriptions of each status:

- **Normal**: The licenses that are both valid and not expired.
- **Abnormal**: The licenses that are invalid or expired or can't be verified by AmpCon-DC.
- **Expired:** The expired licenses.

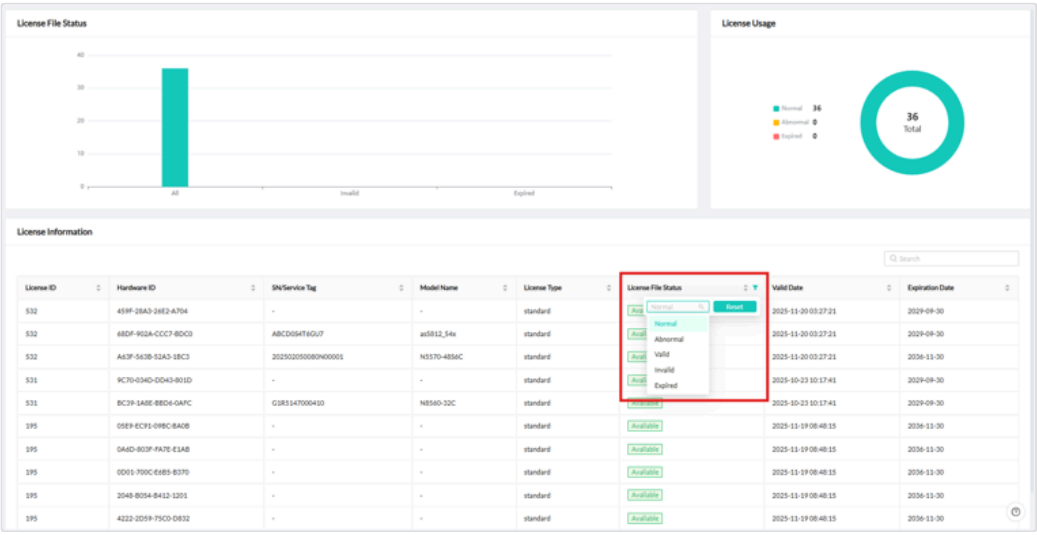


License Details

In the **License Information** section, you can view the following columns. All columns support ascending and descending sorting.

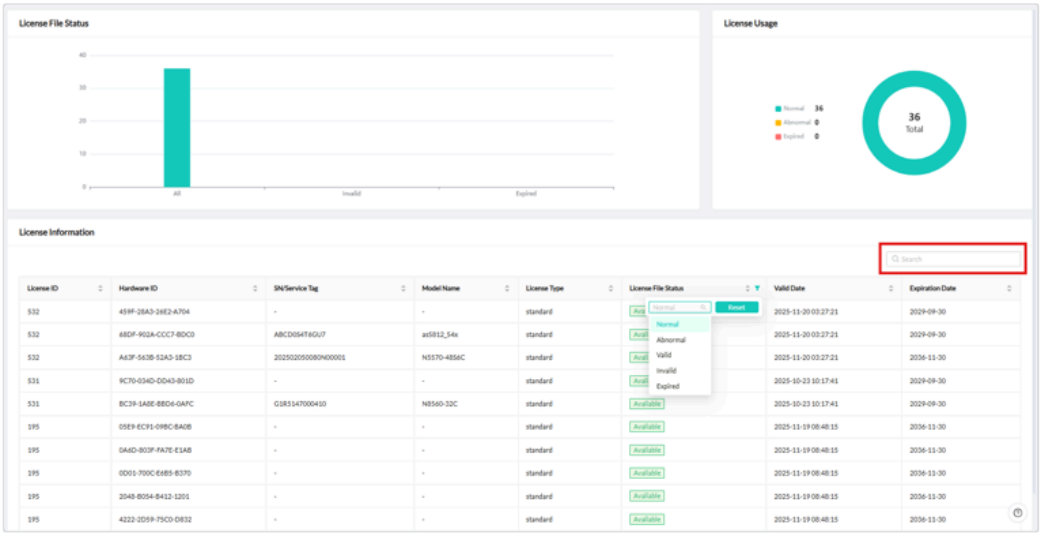
- **License ID:** The ID of the AmpCon-DC license
- **Hardware ID:** The ID of the switch hardware
- **Model Name:** The name of the switch model
- **License Type:** Includes standard license (formal License) and trial license (temporary License)
- **License File Status:** The status of the AmpCon-DC license for the switch
- **Valid Date:** The date from when the switch can be managed by AmpCon-DC
- **Expiration Date:** The date until when the switch can be managed by AmpCon-DC

You can filter licenses with the license status file keywords. In the **License Information** table, click the **License File Status** column, and select a status to view relevant licenses.



Fuzzy Search for License Information

In the search box of the **License Information** table, enter keywords to search for specific licenses.



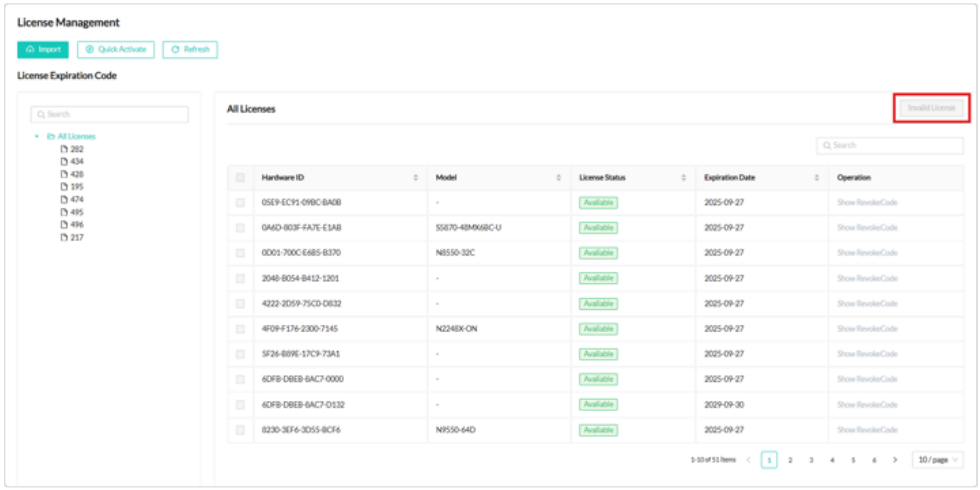
Invalidating a License

If you don’t need to deploy and manage a switch with AmpCon-DC, you can invalidate the AmpCon-DC license on the switch to release this license.

> **NOTEs**
>
> - The Hardware ID of a switch might exist in multiple AmpCon-DC licenses. Ensure that you invalidate all AmpCon-DC licenses on the switch.
> - After you invalidate all AmpCon-DC licenses on a switch, the switch can’t be deployed and managed with AmpCon-DC. The switch that has been deployed will be removed from the switch list on the “Switches” page.
> - You can perform three invalidation operations at most.

Procedure

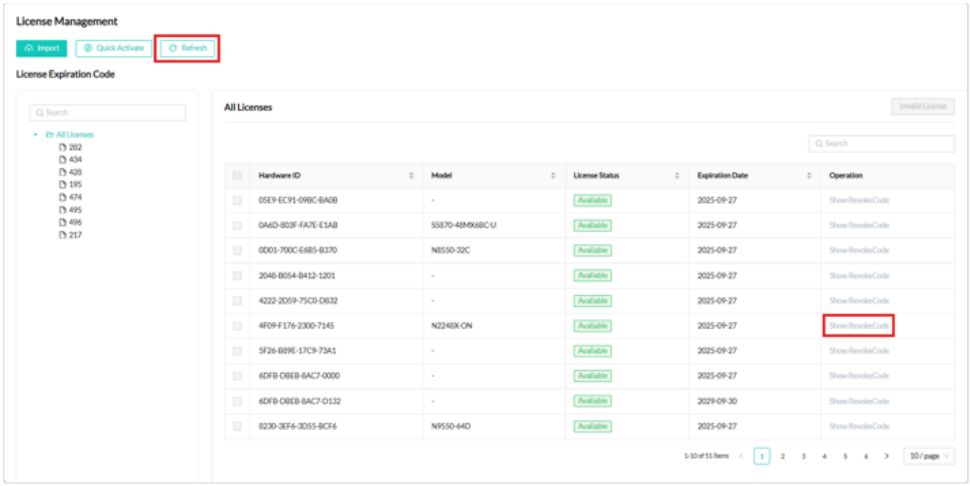
1. In the AmpCon-DC UI, click **System > Software Licenses > License Management**.
2. Click the license file, and click the Hardware ID to be invalidated. Then, click **Invalid License.**



3. In the pop-up window, click **Yes**.

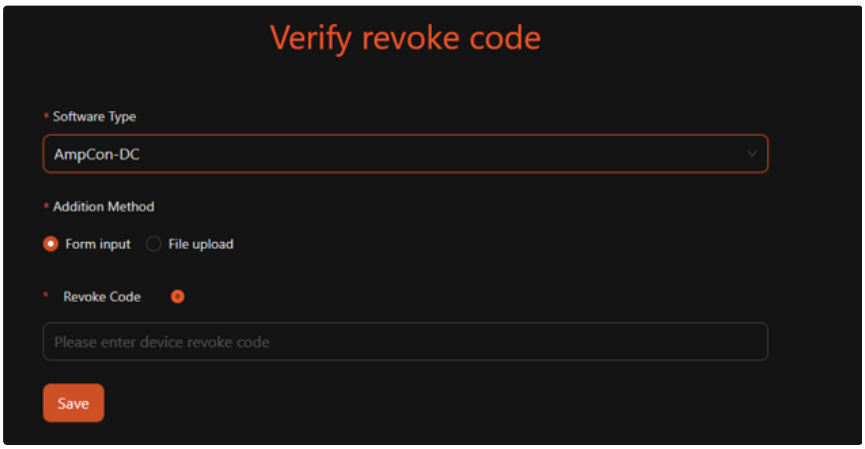
   You can see the invalid code is displayed in a pop-up window. The status of the license is changed to **Invalid**, and **show RevokeCode** in the **Operation** column is shown as clickable instead of grayed out.

   If the license status is not displayed as **Invalid**, click **Refresh** to update the license status.

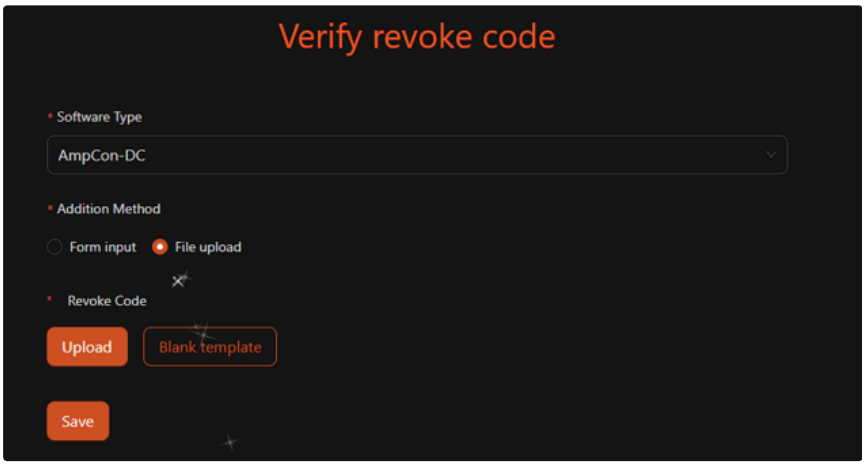


4. Click **Show RevokeCode** to copy the invalid code.
5. Release the invalidated license in the License Portal.
   a. Log in to the License Portal, and then click **AmpCon Licenses > Verify Revoke Code**.
   b. In the **Software Type** drop-down list, select **AmpCon-DC**.
   c. Use either of the following ways:

- In the **Addition Method** section, select **Form Input**. In the **Revoke Code** field, paste the invalid code that you copied in step 4.



- In the **Addition Method** section, select **File Upload**. Click **Blank template** to download a template file. Open the template file, and enter the invalid code in the .xlsx template file. Then, upload the file.


Verify revoke code
* Software Type
AmpCon-DC
* Addition Method
Form input
File upload
* Revoke Code
Upload
Blank template
Save

6. Click **Save**.

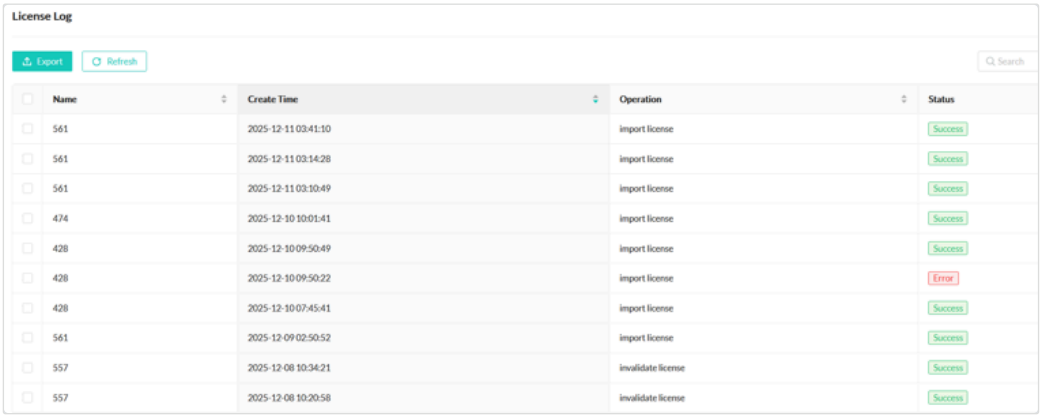
Checking License Logs and Alerts

In the AmpCon-DC UI, click **System > Software Licenses > License Log**. You can check the operation logs and alerts that are related to AmpCon-DC licenses.

Viewing License Operation Logs
Exporting License Operation Logs
Searching for License Operation Logs
Checking License Alerts
Exporting License Alerts
Searching for License Alerts

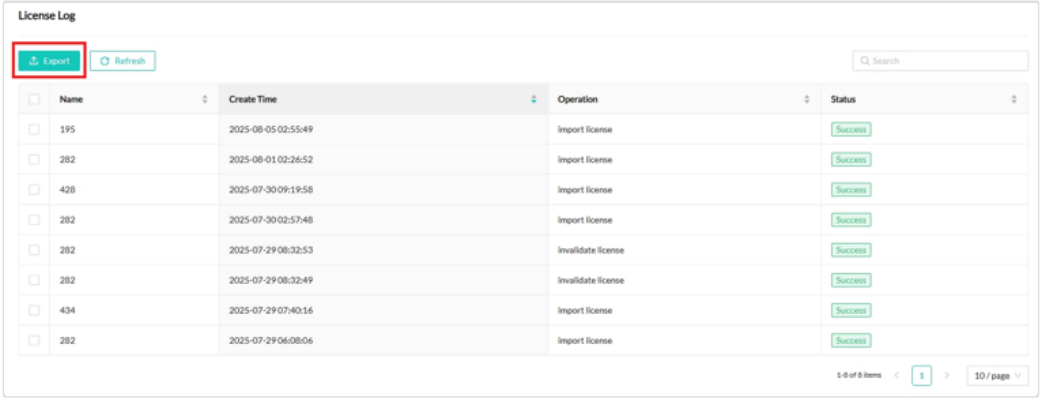
Viewing License Operation Logs

On the “License Log” page, you can view license-related operation records (such as license import operations and license invalidation operations), the time of each operation, and the status of each operation.



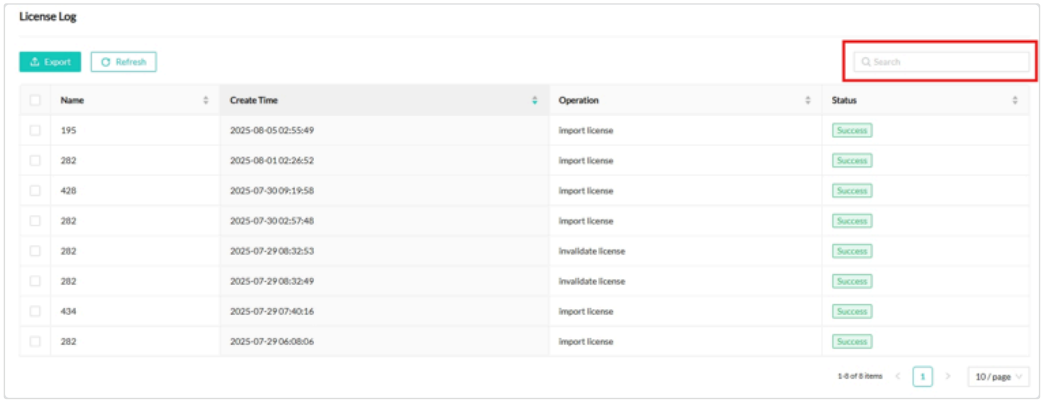
Exporting License Operation Logs

To export license logs as a .csv file, select one or more entries, and then click **Export** in the **License Log** section.



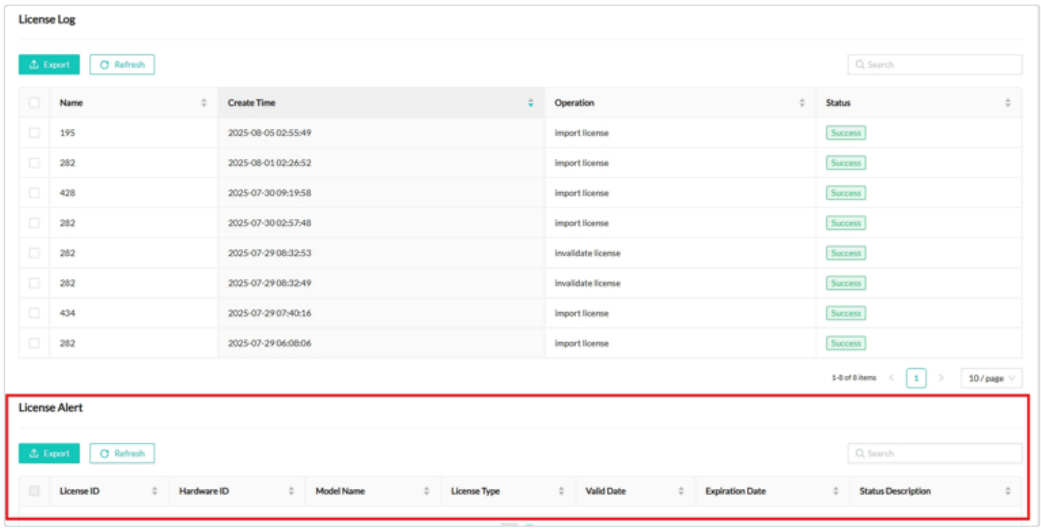
Searching for License Operation Logs

To perform a fuzzy search for logs, enter keywords in the search box of the **License Log** section.



Checking License Alerts

To check license alert information, check the **License Alert** section.

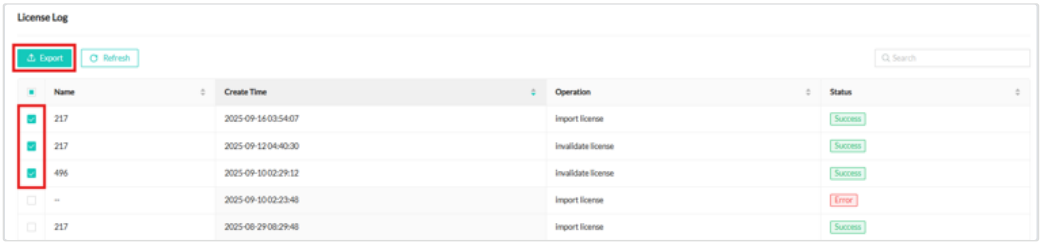


Tips

- During the grace period of a trial AmpCon-DC license, the AmpCon-DC login interface displays "License is expired, you have a 14-day grace period".
- If a standard AmpCon-DC license expires, you can see the license status is expired in the **License Alert** section of the AmpCon-DC UI.

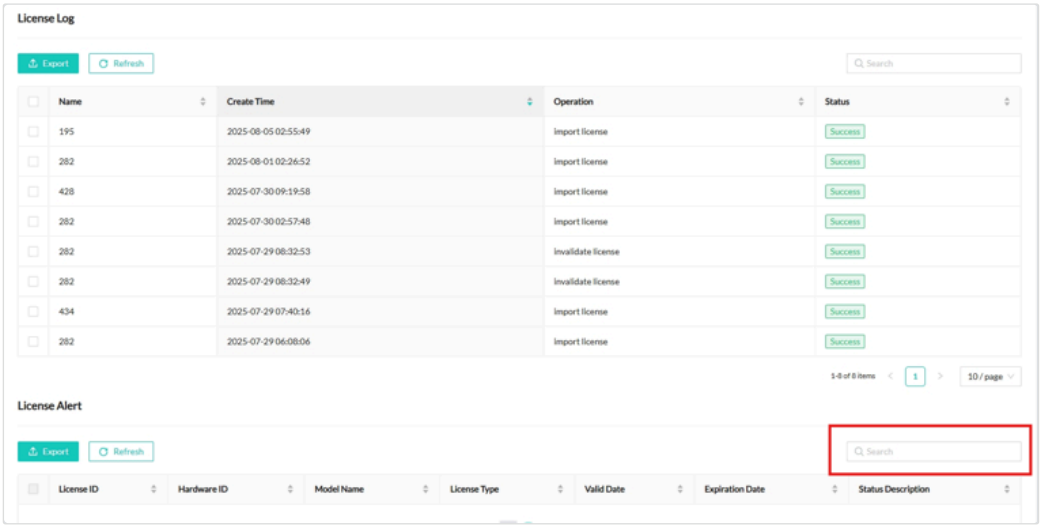
Exporting License Alerts

To export alerts as a .csv file, select one or more alert entries, and then click **Export** in the **License Alert** section.



Searching for License Alerts

To perform a fuzzy search for alerts, enter keywords in the search box of the **License Alert** section.



Managing PicOS Licenses

If AmpCon-DC can access the License Portal that you specified in the system configuration, AmpCon-DC automatically retrieves PicOS licenses from the License Portal. Then, when you deploy a switch with AmpCon-DC, AmpCon-DC automatically installs the PicOS license for the switch.

If AmpCon-DC can't access the License Portal, you can add local PicOS licenses to AmpCon-DC so that AmpCon-DC can install PicOS licenses on corresponding switches.

You can verify whether PicOS licenses are valid or not by using the **License Audit** feature. Or you can verify whether PicOS licenses are valid and extend PicOS licenses by using the **License Action** feature.

Prerequisites
Verifying License Validity
  Verifying the PicOS License for a Switch
  Verifying PicOS Licenses for a Group of Switches
Verifying License Validity and Extending Licenses
  Verifying and Extending the PicOS License for a Switch
  Verifying and Extending PicOS Licenses for a Group of Switches
Adding Local PicOS Licenses

Prerequisites

- Check whether AmpCon-DC can connect with the License Portal through the entered username and password in the system configuration. For more information, see Checking License Portal Connectivity.

  If AmpCon-DC can't access the License Portal that you specified in the system configuration, for example in an air-gapped environment, you need to manually add local PicOS licenses to AmpCon-DC. For more information, see the Adding Local PicOS Licenses section.

- Ensure that the sales team has created PicOS licenses for the switches to be managed. Or else, some functions of AmpCon-DC might not work.

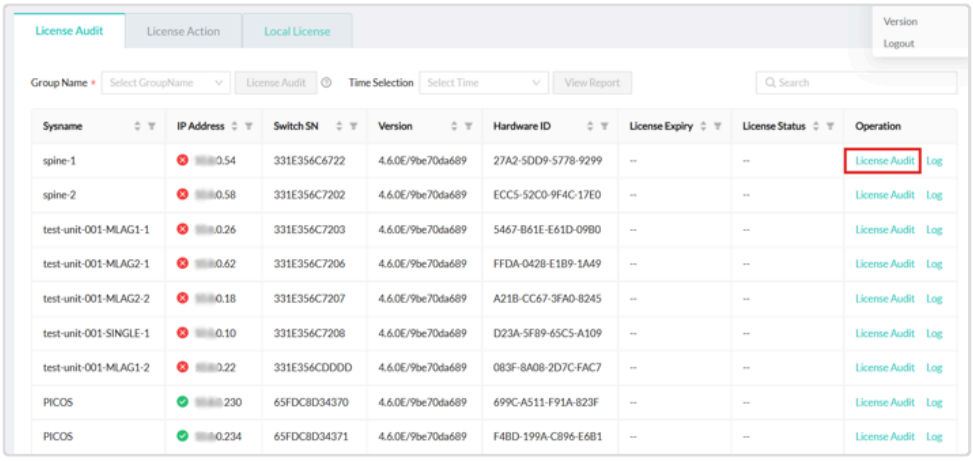
Verifying License Validity

By using the **License Audit** feature, you can verify whether PicOS licenses are valid or not.

Verifying the PicOS License for a Switch

To check the PicOS license validity for a switch, follow these steps:

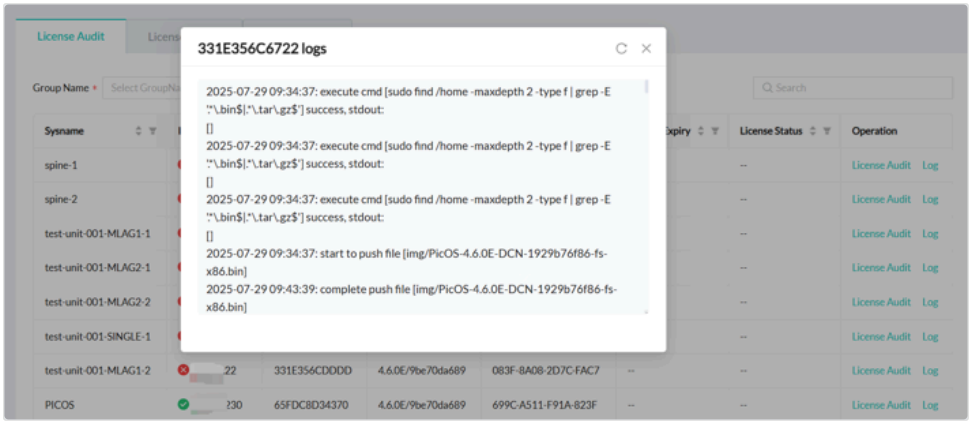
1. In the AmpCon-DC UI, click **Resource > Device Licenses**.
2. In the **License Audit** tab, locate a PicOS license, and then click **License Audit**.



3. Click **Yes**.
4. Check the **License Expiry** and **License Status** columns.

- **License Expiry** means the expiration date of the PicOS license.
- **License Status** means the current status of the PicOS license. You might see the following license status:
  - **Expired:** The PicOS license is expired.
  - **Expiring:** The PicOS license will expire within the next 30 days.
  - **Active:** The PicOS license is valid and will not expire within the next 30 days.
  - **Unknown:** AmpCon-DC hasn't retrieved the PicOS license status of the switch.
  - **No License:** The switch has no PicOS license installed.

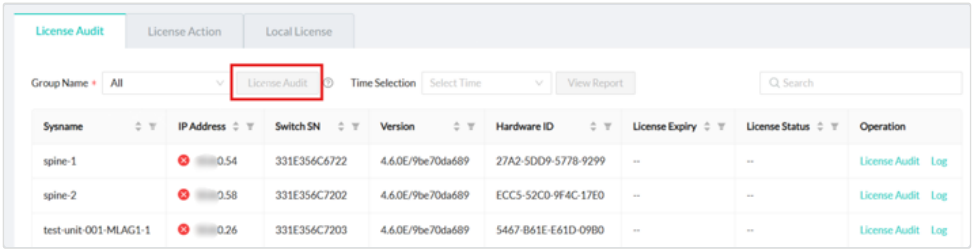
5. Click **Log** to view the license audit logs.



Verifying PicOS Licenses for a Group of Switches

To check the PicOS license validity for a group of switches, follow these steps:

1. In the AmpCon-DC UI, click **Resource > Device Licenses**.
2. In the **License Audit** tab, select a group name from the **Group Name** drop-down list, and then click **License Audit**.

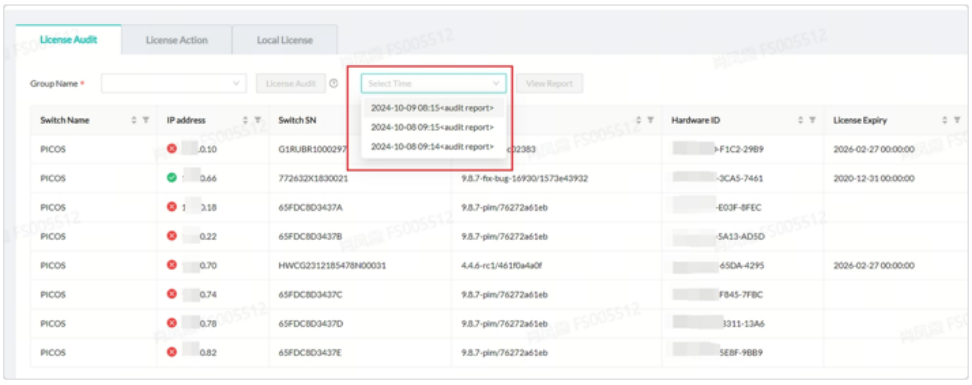


3. Check the **License Expiry** and **License Status** columns.

- **License Expiry** means the expiration date of the PicOS license.
- **License Status** means the current status of the PicOS license. You might see the following license status:
  - **Expired:** The PicOS license is expired.
  - **Expiring:** The PicOS license will expire within the next 30 days.
  - **Active:** The PicOS license is valid and will not expire within the next 30 days.
  - **Unknown:** AmpCon-DC hasn't retrieved the PicOS license status of the switch.
  - **No License:** The switch has no PicOS license installed.

4. Optional: Select the newly generated report from the drop-down list, and then click **View Report**.

> **NOTE**
>
> The **View Report** button is applicable only to License Audit operations based on groups.

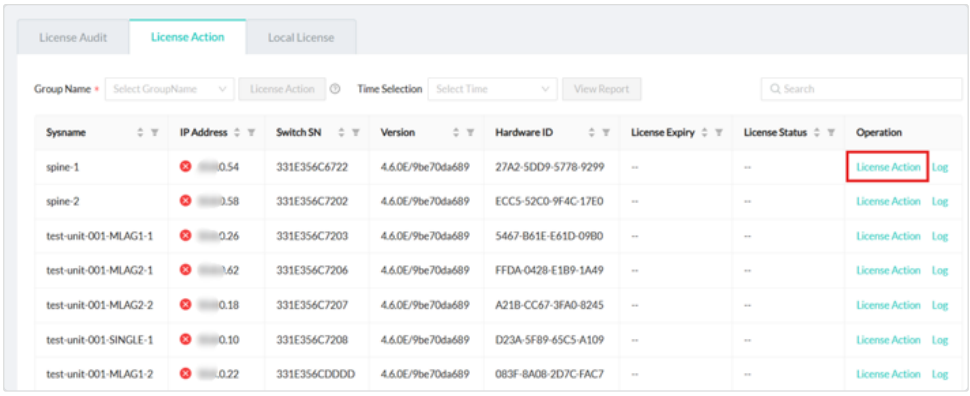


Verifying License Validity and Extending Licenses

By using the **License Action** feature, you can verify whether PicOS licenses are valid and extend PicOS licenses if these PicOS licenses are extended in the License Portal.

Verifying and Extending the PicOS License for a Switch

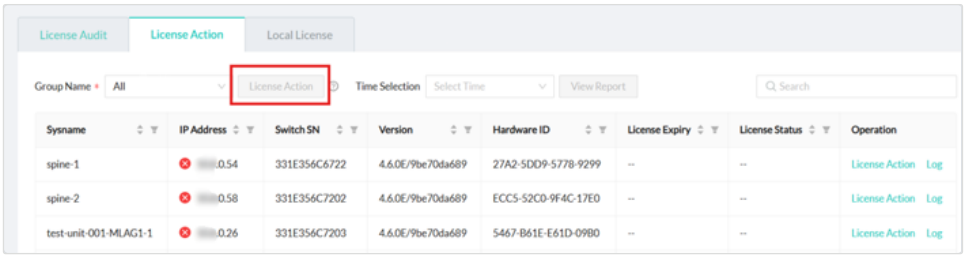
1. In the AmpCon-DC UI, click **Resource > Device Licenses**.
2. Click the **License Action** tab.
3. Locate a license, and then click **License Action**.



4. Click **Yes**.
5. Check the **License Status** and **License Expiry** columns. License expiry means the expiration date of the PicOS license. License status means the current status of the PicOS license.
6. Optional: Click **Log** to view the License Action logging information.

Verifying and Extending PicOS Licenses for a Group of Switches

1. In the AmpCon-DC UI, click **Resource > Device Licenses**.
2. Click the **License Action** tab.
3. Select a group name from the **Group Name** drop-down list, and then click **License Action**.



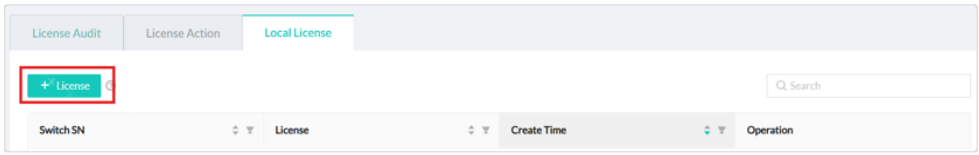
4. Check the **License Status** and **License Expiry** columns. License expiry means the expiration date of the PicOS license. License status means the current status of the PicOS license.
5. Optional: Select the newly generated report from the drop-down list, and then click **View Report**.

> **NOTE**
>
> The **View Report** button is applicable only to License Action operations based on groups.

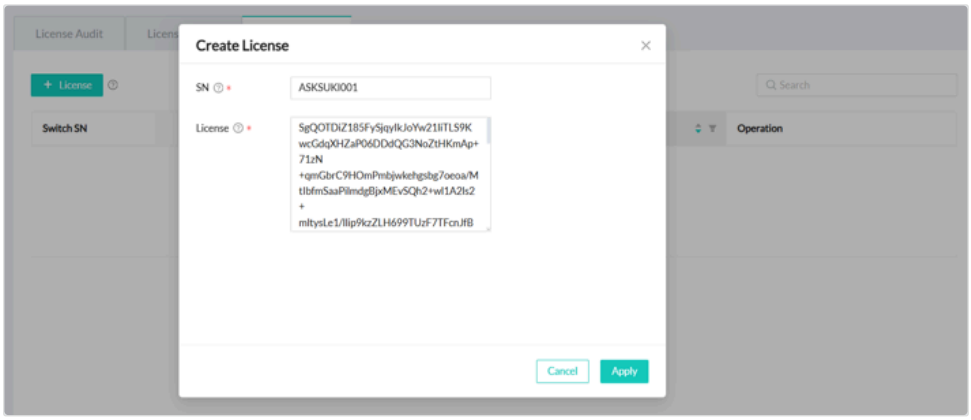
Adding Local PicOS Licenses

To add a local PicOS license, follow these steps:

1. Click **Resource > Device Licenses**.
2. Click the **Local License** tab, and then click **+ License**.



3. In the **SN** field, enter the SN of the switch with the uploaded PicOS license.
4. In the **License** field, enter the local PicOS license key.



5. Click **Apply**.

Administering AmpCon-DC

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

- Managing User Access
- Updating the Encryption Key for Sensitive Data Encryption
- Forwarding Logs to External Syslog Servers
- Backing up and Restoring the AmpCon-DC Database

Managing User Access

After you deploy AmpCon-DC, you can manage AmpCon-DC user access so that each AmpCon-DC user is assigned with appropriate permissions:

- AmpCon-DC provides Role-Based Access Control (RBAC) to define different permission levels through roles. You can assign one or multiple built-in or custom roles to users. A user must be assigned at least one role to log in to the AmpCon-DC UI.
- AmpCon-DC enables users to manage tenants. A user can be assigned one or multiple tenants. Then, when you log in to the AmpCon-DC UI with the user, you can manage the logical networks belonging to the tenants managed by the user. This method ensures resource isolation and access control in multi-tenant environments.
- AmpCon-DC supports user group management. To assign the same roles and tenants to multiple users, you can add these users to a user group and then assign roles and tenants to the user group, instead of authorizing each user one by one. This method ensures consistent access control and improved operational efficiency.

Guidelines
Adding a User
Adding a User Group
Managing Added Users
  Configuring TACACS+ Authentication and Authorization
  Deleting Users
  Editing Users
  Locking and Unlocking Users
  User Self-Management
  Viewing User Information
Managing Added User Groups
  Deleting a User Group
  Viewing a User Group
  Editing a User Group

Guidelines

- In AmpCon-DC, access permissions are determined through the combination of users, roles, and tenants:
  - Users represent the accounts used to log in to the AmpCon-DC UI.
  - Roles define the permissions that determine which pages and tabs a user can access (Read or Write). For more information, see Managing Roles.
  - Tenants are logical resource units used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. For more information, see

Managing Tenants.

- You can assign roles or tenants to a single user or a user group. For more information, see Assigning Roles and Tenants.
- When you add a user, you can designate the user type: group user or global user.
  - A group user means that the user can manage specific device groups (host groups, switch groups, or both).
  - A global user means that the user can manage all device groups (host groups, switch groups, or both). For more information about device groups, see Managing Groups.

Adding a User

To add a user, follow these steps:

1. Log in to the AmpCon-DC UI with an AmpCon-DC user who has the built-in SuperAdmin role or has custom roles with the Read and Write permissions to the “User Settings”, “Authorization Wizard”, and “Role Management” pages.
2. Click **System > User Management > User Settings** from the navigation bar.
3. On the “User Settings” page, click **+ User**, and then input the following information:

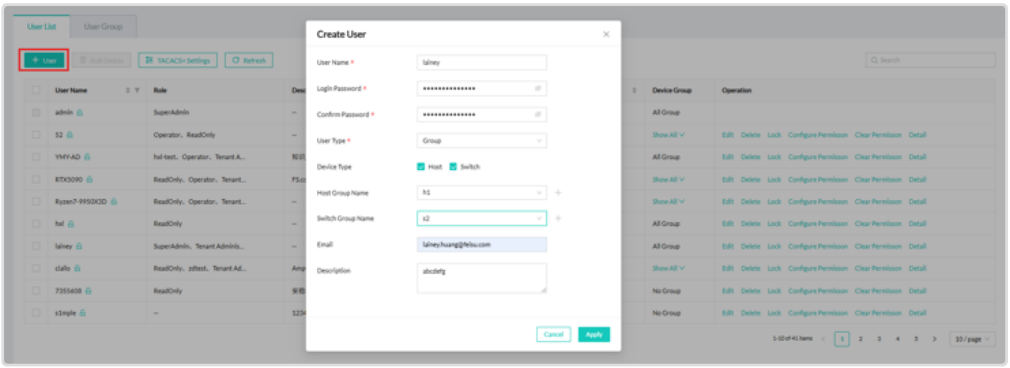


Table 1. User Parameters

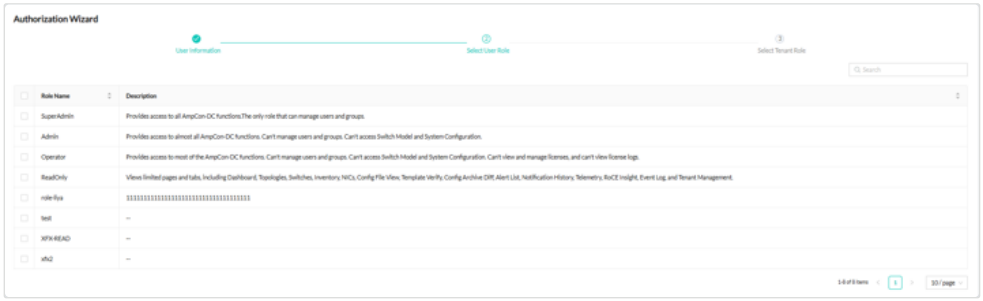
Parameter	Description
User Name	The username. • The username must be unique. • The value is a string with at most 64 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z. ◦ Digits including 0 to 9.

	◦ Special characters (_ -). • The value cannot start or end with spaces.
Login Password	The login password of the user. The login password must include uppercase letters, lowercase letters, numbers, and special characters. It must contain at least 10 characters.
Confirm Password	Re-enter the login password of the user.
User Type	Select **Global** or **Group**, which means creating a global user or a group user. If you select **Group**, you can select **Host**, **Switch,** or both in the **Device Type** check box to assign host groups, switch groups, or both to the user. • If you select **Host**, select an added host group from the **Host Group Name** drop-down list. To select multiple host groups, click the plus icon **+**. • If you select **Switch**, select an added switch group from the **Switch Group Name** drop-down list. To select multiple switch groups, click the plus icon **+**. **NOTE** Ensure that the selected switch groups and host groups have been created. For more information about creating groups, see Adding a Group.
Email	Optional. The email address of the user.
Description	Optional. The description of the user. The value cannot exceed 256 characters.

4. Click **Apply.**

5. In the pop-up window, click **Authorization Wizard** to go to the “Authorization Wizard” page, where you can assign roles and tenants to the user. For more information, see Assigning Roles and Tenants to a User.

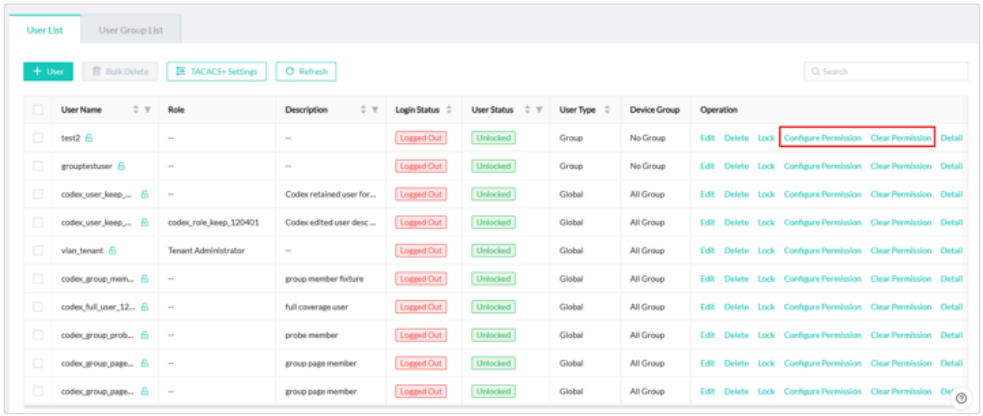
> **NOTE**
>
> After creating users, you must assign roles to them. Only users with at least one assigned role can access the AmpCon-DC UI.



You can also go to the “Authorization Wizard” page by locating the user on the “User Settings” page and then clicking **Configure Permission**.

To remove all assigned roles and tenants from the user, click **Clear Permission**.

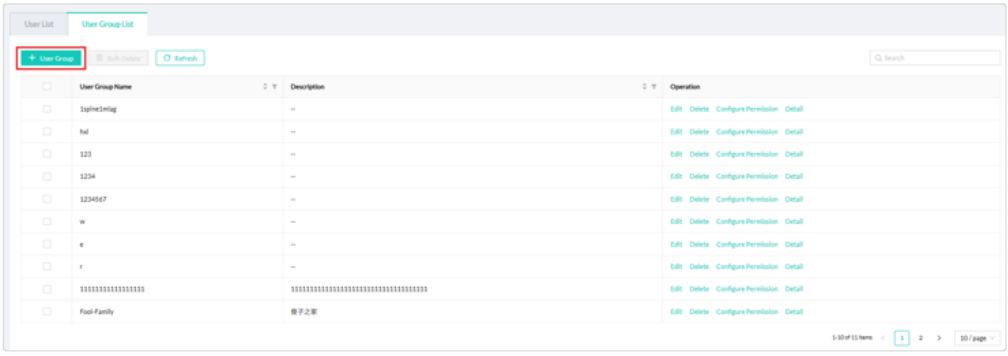
> **NOTE**
>
> The **Configure Permission** and **Clear Permission** buttons can't be used to configure or clear permissions for the currently logged-in user.



Adding a User Group

To add a user group, follow these steps:

1. Log in to the AmpCon-DC UI with an AmpCon-DC user who has the built-in SuperAdmin role or has custom roles with the Read and Write permissions to the “User Settings”, “Authorization Wizard”, and “Role Management” pages.
2. Click **System > User Management > User Settings** from the navigation bar.
3. Click the **User Group List** tab.
4. Click **+ User Group**.



5. In the **Basic Information** section, input the following information:

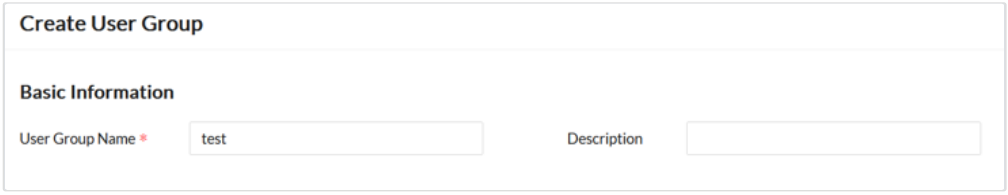


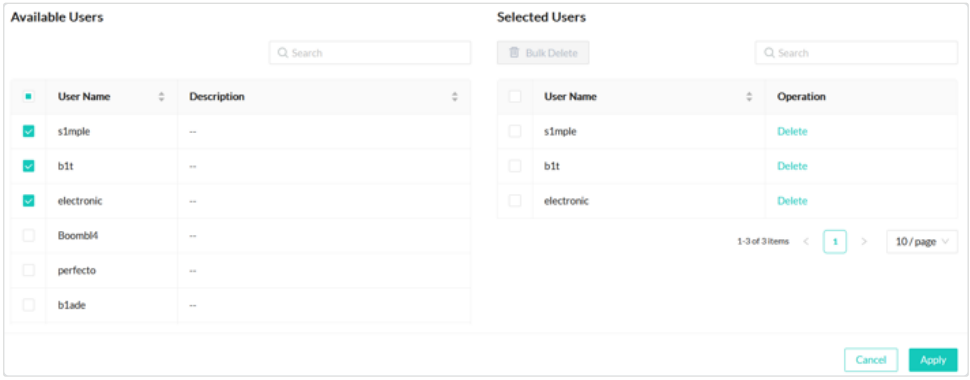
Table 2. Basic Information Parameters

Parameter	Description
User Group Name	The name of the user group. **NOTEs** • The name must be unique. • The name is a string with at most 32 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ -). • The name cannot start or end with spaces.

Description	Optional. The description of the user group. The value cannot exceed 256 characters.

6. In the **Available Users** section, select the users that you want to add to the user group. The selected users will appear in the **Selected Users** section.

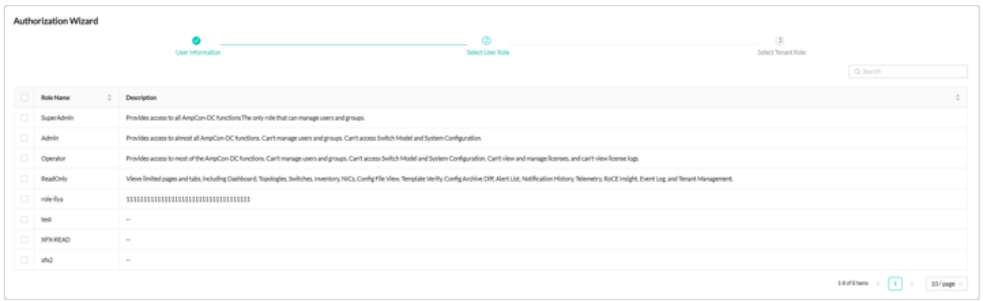
> **NOTE**
>
> Each user can be added to at most one user group.



To remove the selected users, remove them individually by clicking **Delete** in the **Operation** column, or remove them in batches by selecting the users and clicking **Bulk Delete**.

7. Click **Apply**.
8. In the pop-up window, click **Authorization Wizard** to go to the "Authorization Wizard" page, where you can assign roles and tenants to the user group. For more information, see Assigning Roles and Tenants to a User Group.

> **NOTE**
>
> A user can be used to log in to the AmpCon-DC UI only if the user is assigned at least one role or the user group containing the user is assigned at least one role.



Managing Added Users

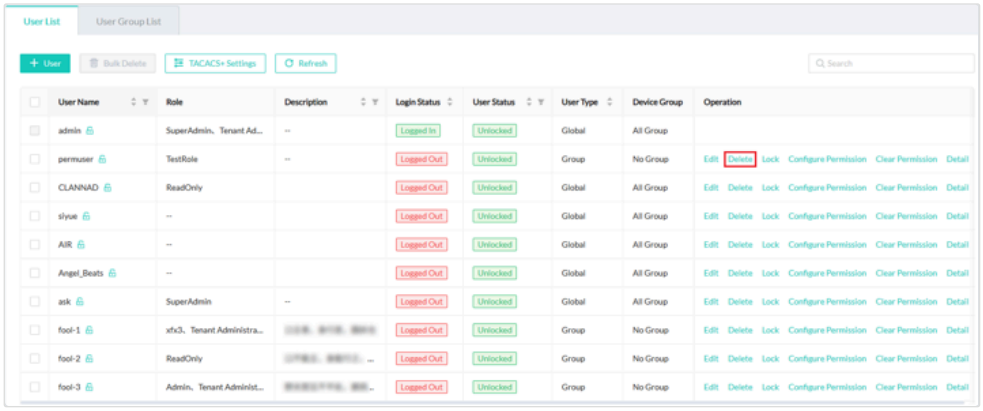
Configuring TACACS+ Authentication and Authorization

In addition to using local AmpCon-DC users (global users or group users), you can also enable the TACACS+ integration to manage user access. For more information, see Configuring TACACS+ Authentication and Authorization.

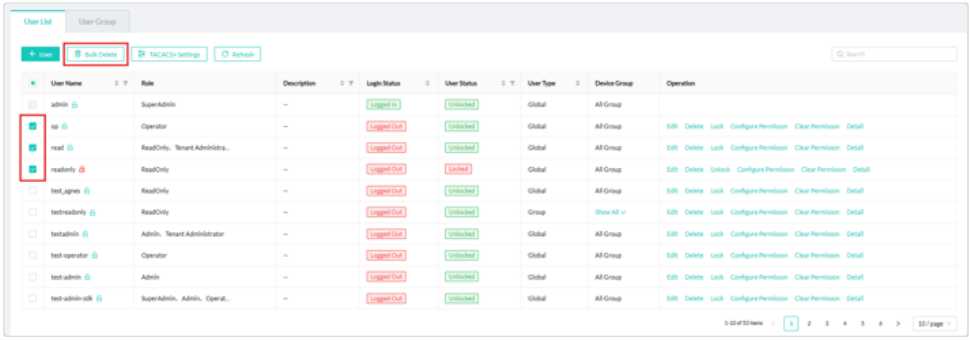
Deleting Users

> **NOTEs**
>
> - Deleting a user does not delete the tenants managed by the user.
> - After the initial tenant administrator user is deleted, the tenant will no longer have an initial tenant administrator. You can assign the tenant to other users for tenant management and logical network deployment.

- To delete a user, locate the user on the “User Settings” page, and then click **Delete**. In the pop-up window, select the check box near “I have identified the risks of this operation”, and then click **Yes**.



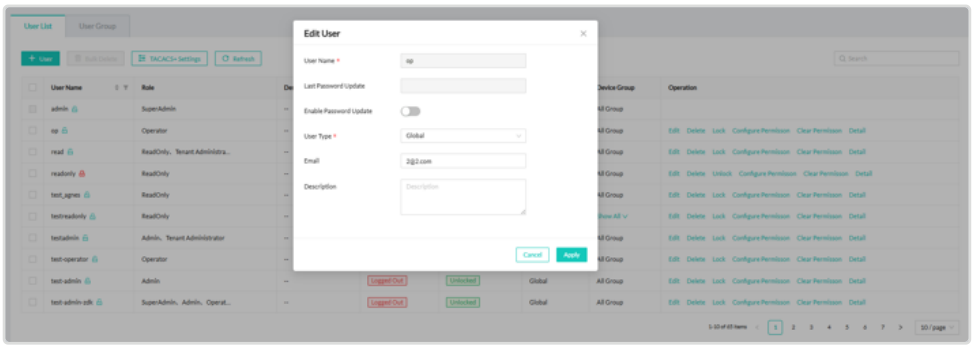
- To delete multiple users in batches, select the users, and then click **Bulk Delete**. In the pop-up window, select the check box near “I have identified the risks of this operation”, and then click **Yes**.



Editing Users

To edit a user, follow these steps:

1. On the “User Settings” page, locate the user, and then click **Edit**.



2. Modify user information as follows:

Table 3. User Edit Parameters

Parameter	Description
Enable Password Update	Specify whether the password can be modified. If you toggle it on, enter a new password in the **Login Password** field, and then enter the password again in the **Confirm Password** field.
User Type	The type of the user, **Global** or **Group**, which means a global user or a group user. If you select **Group**, you can select **Host**, **Switch,** or both in the **Device Type** check box to assign host groups, switch groups, or both to the user. • If you select **Host**, select an added host group from the **Host Group Name** drop-down list. To select multiple host groups, click the plus icon **+**. • If you select **Switch**, select an added switch group from the **Switch Group Name** drop-down list. To select multiple switch groups, click the plus icon **+**.

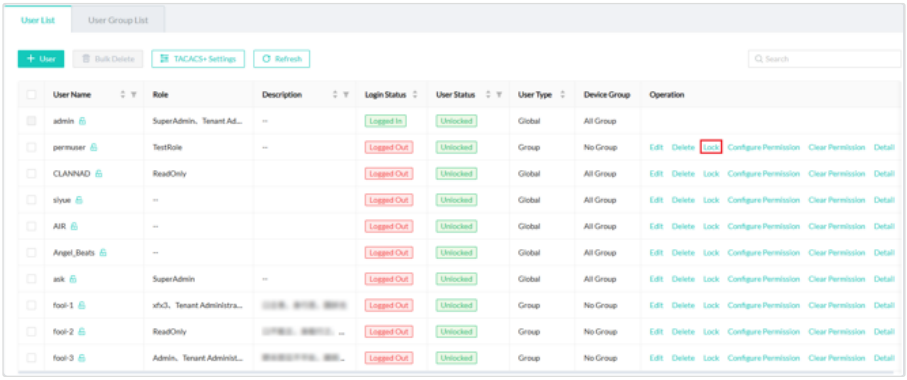
	NOTE Ensure that the selected switch groups and host groups have been created. For more information about creating groups, see Adding a Group.
Email	Optional. The email address of the user.
Description	Optional. The description of the user. The value cannot exceed 256 characters.

3. Click **Apply**.

Locking and Unlocking Users

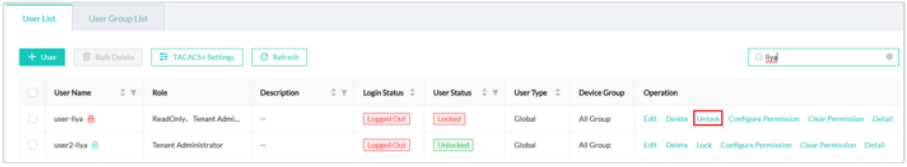
You can lock an added user so that the user can't be used to log in to the AmpCon-DC UI. Or you can unlock an added user to enable the login again.

- To **lock** an added user, follow these steps:
  a. On the "User Settings" page, locate a user, and then click **Lock**.



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

- To **unlock** an added user, follow these steps:
  a. On the "User Settings" page, locate the locked user, and then click **Unlock**.



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

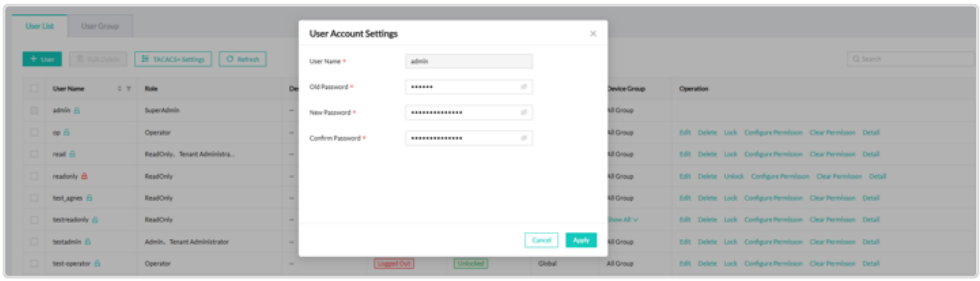
User Self-Management

All AmpCon-DC users can change their own passwords. After you log in to the AmpCon-DC UI with a user, you can modify the password. Follow these steps:

1. In the AmpCon-DC UI, hover over the username used to log in to the AmpCon-DC UI, and then click **User Management**.



2. To change the user password, enter the old password in the **Old Password** field, enter a new password in the **New Password** field, and then enter the new password again in the **Confirm Password** field.



3. Click **Apply**.

Viewing User Information

On the “User Settings” page, you can see all the added users.

> **NOTE**
>
> Users who are authenticated and authorized through TACACS+ are not displayed.

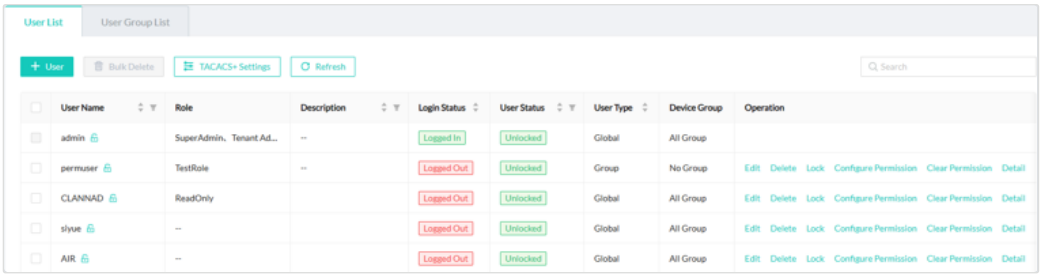


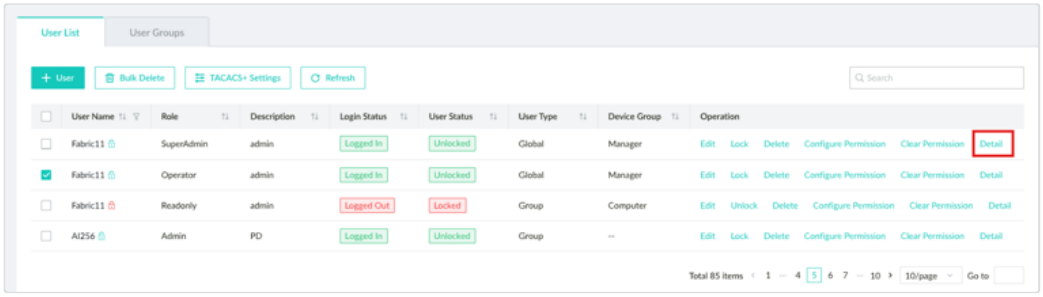
Table 4. User Metrics

Metric	Description

User Name	The username of the user.
Role	The roles you assigned to the user. **NOTE** Roles assigned to the user group where the user exists are not displayed here. To check the roles assigned to the user group, see Viewing a User Group.
Description	The description you specified for the user.
Login Status	Indicates whether the user is logged in. • **Logged In**: The user is currently logged in. • **Logged Out**: The user is currently logged out. **NOTE** To refresh the login status, click **Refresh**.
User Status	Indicates whether the user is locked. • **Locked**: The user is locked and cannot be used to log in to the AmpCon-DC UI. • **Unlocked**: The user is unlocked and can be used to log in to the AmpCon-DC UI. **NOTE** To refresh the user status, click **Refresh**.
User Type	The user type, **Group** or **Global**. • **Group**: The user is a group user. • **Global:** The user is a global user.
Device Group	The device groups the user can manage. • **All Group**: The user can manage all device groups. • **No Group**: The user can't manage any device groups.

	• **Show All**: The user can manage specific device groups. Hover over **Show All**, and then you can see the device groups that the user can manage.

To view user details, locate the user, and then click **Detail**.



- In the **Basic Information** section, you can see information as follows:

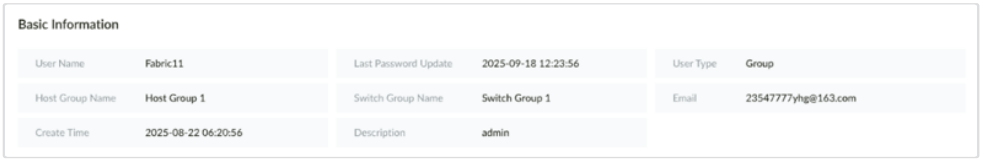


Table 5. Basic Information Metrics

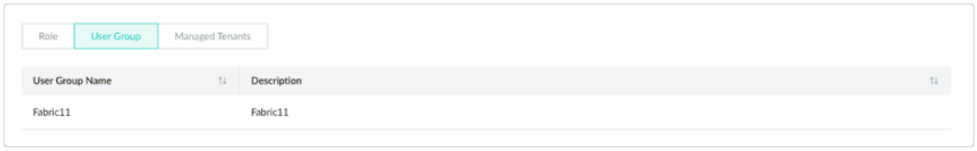
Metric	Description
User Name	The name of the user.
Last Password Update	The time when the password was last modified.
User Type	The user type, **Group** or **Global**. • **Group**: The user is a group user. • **Global:** The user is a global user.
Host Group Name	The host groups assigned to the user.
Switch Group Name	The switch groups assigned to the user.
Email	The email address of the user.
Create Time	The time when the user was created.
Description	The description of the user.

- In the **Role** tab, check all roles you have assigned to the user.

> **NOTE**
>
> Roles assigned to the user group where the user exists are not displayed here.

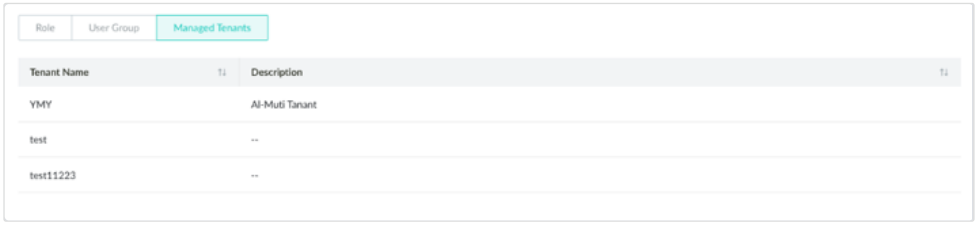


- In the **User Group** tab, check the user group to which the user has been added.



- In the **Managed Tenants** tab, check all tenants you have assigned to the user.

> **NOTE**
>
> Tenants assigned to the user group where the user exists are not displayed here.

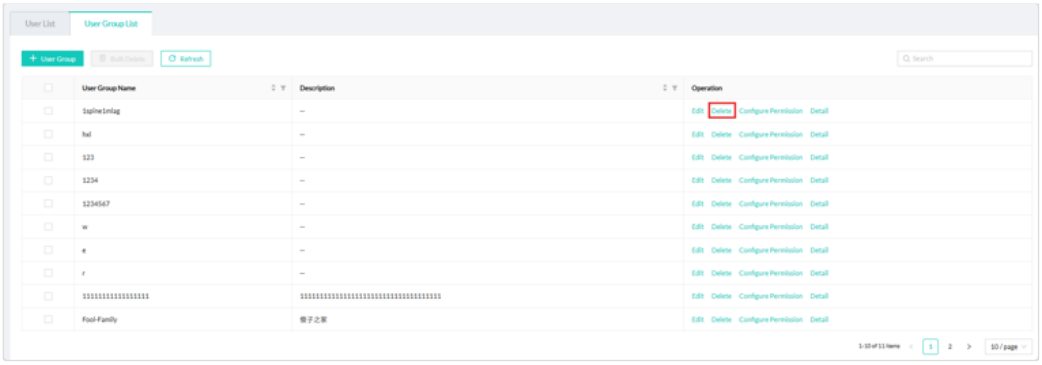


Managing Added User Groups

Deleting a User Group

To delete a user group, locate the user group, and then click **Delete**.

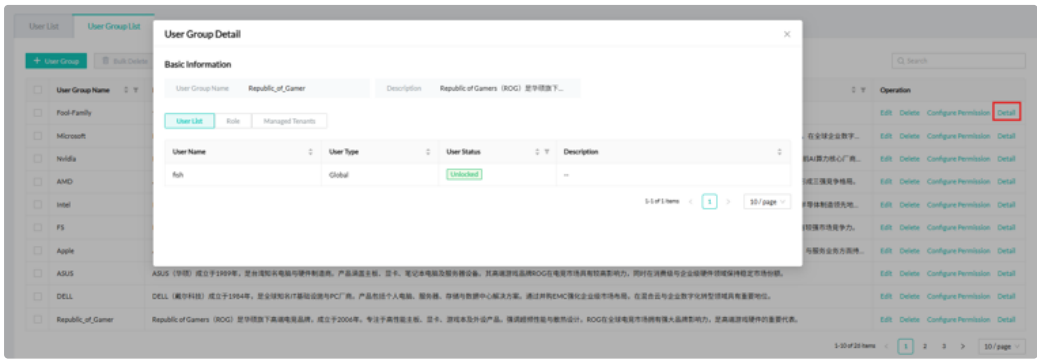
> **NOTE**
>
> Deleting a user group will remove all users from the user group but will not delete the users themselves.



Viewing a User Group

You can also view detailed information about the roles and tenants assigned to the user group, providing clear visibility into its access scope and authorization status.

To view details of a user group, locate the user group, and then click **Detail**.



- In the **User List** tab, check all users you added to the user group.

Table 6. User Metrics

Metric	Description
User Name	The name of the user.
User Type	The user type, **Group** or **Global**. • **Group**: The user is a group user. • **Global:** The user is a global user.
User Status	Indicates whether the user is locked. • **Locked**: The user is locked and cannot be used to log in to the AmpCon-DC UI. • **Unlocked**: The user is unlocked and can be used to log in to the AmpCon-DC UI.
Description	The description of the user.

- In the **Role** tab, check all roles that you assigned to the user group.

Table 7. Role Metrics

Metric	Description
Role Name	The name of the role.
Description	The description of the role.

- In the **Managed Tenants** tab, check all tenants that you assigned to the user group.

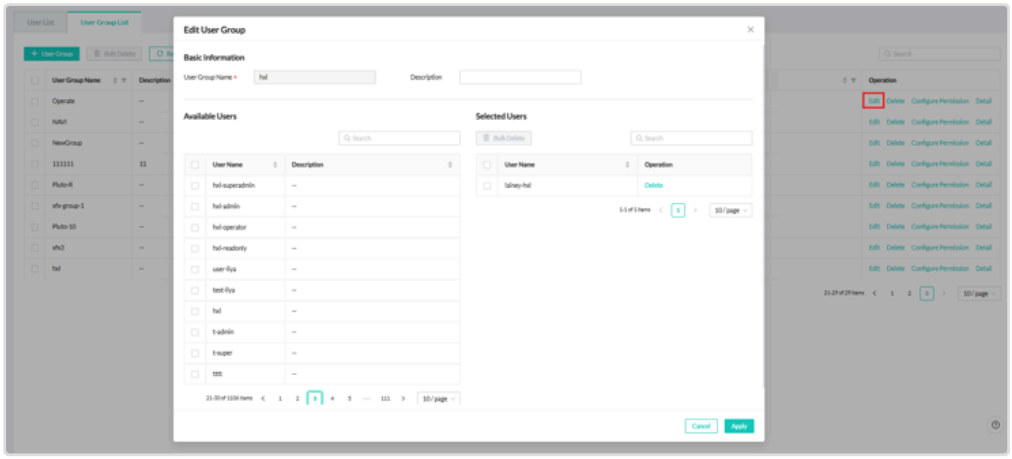
Table 8. Managed Tenant Metrics

Metric	Description
Tenant Name	The name of the tenant.
Description	The description of the tenant.

Editing a User Group

To edit a user group, follow these steps:

1. On the “User Settings” page, click the **User Group List** tab.
2. Locate a user group, and then click **Edit**.



3. Modify the user group information as follows:

Table 9. User Group Parameters

Parameter	Description
Description	The description of the user group.

Available Users	Select users from the **Available Users** list to add them to the user group.
Selected Users	Delete users from the user group in the following ways: • To remove a user from the user group, select the user, and then click **Delete** in the operation column. • To remove multiple users from the user group, select multiple users, and then click **Bulk Delete**.

4. Click **Apply**.

Configuring TACACS+ Authentication and Authorization

AmpCon-DC supports integrating with the Terminal Access Controller Access Control System (TACACS+) server to do authentication and authorization for AmpCon-DC login users.

In addition to using local AmpCon-DC users, you can also enable the TACACS+ integration to manage user access.

Before You Begin
Procedure
Sample Configuration of Authorization Level on TACACS+ Server (Linux tac_plus)

Before You Begin

Before you enable the TACACS+ integration, read the following notes:

- You can configure at most two TACACS+ servers on the AmpCon-DC UI. 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-DC sends authorization requests with **“Arg[0]” service=AmpCon**. On the TACACS+ server, you need to set the value of the parameter **“service=AmpCon”** to process authorization requests of AmpCon-DC users.
- If both the primary and the secondary TACACS+ servers are unreachable, you can use local AmpCon-DC users to log in to the AmpCon-DC UI.

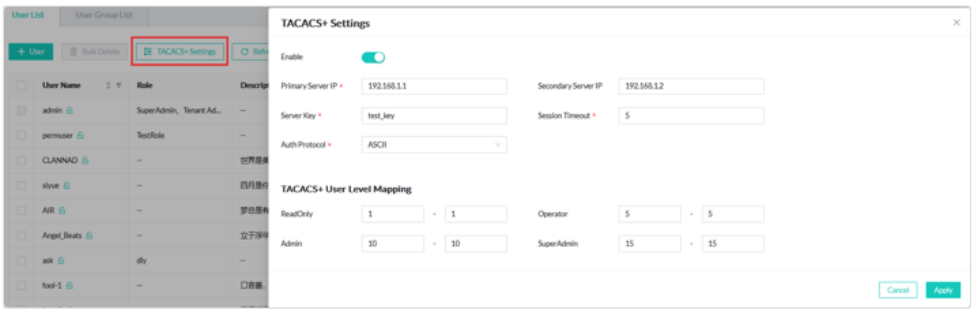
Procedure

To enable the TACACS+ integration, follow these steps:

1. Log in to the AmpCon-DC UI with an AmpCon-DC user who has the built-in SuperAdmin role or has custom roles with the Read and Write permissions to the **User List** tab.

   For more information about user roles, see Managing Roles.
2. Click **System > User Management > User Settings** from the navigation bar.

3. In the **User List** tab, click **TACACS+ Settings**.



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

Table 1. TACACS+ Setting Parameters

Parameter	Description
Enable	Toggle it on to enable TACACS+ authentication and authorization.
Primary Server IP	The IP address of the primary TACACS+ server.
Secondary Server IP	Optional. The IP address of the backup TACACS+ server.
Server Key	The shared key of TACACS+. **NOTE** The value of the **Server Key** field needs to be the same as the shared keys of the primary and secondary TACACS+ servers. The shared keys on both TACACS+ servers need to be the same.
Session Timeout	The TACACS+ connection timeout in seconds. The value must be an integer greater than 0.
Auth Protocol	The authentication protocol type of TACACS+, **ASCII**, **PAP**, or **CHAP**.

TACACS+ User Level Mapping	The mapping ranges for TACACS+ authorization. The configuration page displays the default mapping values. You can configure a custom range for mapping values. The values are integers that range from 0 to 15. **NOTEs** • Don't overlap any range with other ranges among different user levels. • If the **priv-lvl** configuration of a user on the TACACS+ server is not found in the user level mapping configuration on AmpCon-DC, the user role level is mapped to ReadOnly.

5. Click **Apply**.

Sample Configuration of Authorization Level on TACACS+ Server (Linux tac_plus)

For how to configure authorization levels on the TACACS+ server, see the following example:

```
user = leontest {
        password = clear pica8123
        service = AmpCon {
                default attribute = permit
                priv-lvl = 15
        }
}

user = automation1 {
        password = clear pica8123
        service = AmpCon {
                default attribute = permit
                priv-lvl = 10
        }
}
```

```
user = testtest {
        password = clear pica8123
        service = AmpCon {
                default attribute = permit
                priv-lvl = 5
        }
}

user = testpica8 {
        password = clear pica8123
        service = AmpCon {
                default attribute = permit
                priv-lvl = 1
        }
}
```

Managing Roles

AmpCon-DC provides Role-Based Access Control (RBAC) to define different permission levels through roles. You can assign built-in roles to users or user groups directly, or you can create custom roles and then assign them to users or user groups.

The access permissions of built-in roles can't be changed, while custom roles allow you to grant Read and Write permissions for specific pages or tabs.

This approach simplifies access management, ensures consistent access control, and improves operational security and efficiency.

- Guidelines
- Creating a Custom Role
- Assigning Roles to a User or User Group
- Optional Operations
  - Viewing Role Details
  - Copying a Role
  - Editing a Custom Role
  - Deleting One or Multiple Custom Roles
- Permission Table for Built-In Users

Guidelines

- The following built-in roles are supported by AmpCon-DC:

Table 1. Built-in User Role Permissions

Built-In Role	Description
SuperAdmin	Can view and manage all AmpCon-DC pages and tabs.
Admin	• Can view and manage most of the AmpCon-DC pages and tabs. • Can't view but can't manage the "Group Management", "User Settings", "Authorization Wizard", and "Role Management" pages. • Can't view the **Switch Model** and **System Configuration** tabs.
Operator	• Can view and manage most of the AmpCon-DC pages and tabs.

	• Can view but can't manage the "Tenant Management" page. • Can't view the "Group Management", "User Settings", "Authorization Wizard", "Role Management", "License View", "License Management", and "License Log" pages. • Can't view the **Switch Model** and **System Configuration** tabs.
ReadOnly	• Can view limited AmpCon-DC pages, including "System Overview", "Switch Overview", "Topologies", "Switches", "NICs", "Alert List", "Notification History", "Performance Statistics", "RoCE Counters", "Network Congestion", "Event Log", and "Tenant Management". • Can view limited AmpCon-DC tabs, including **Inventory**, **Config File View**, **Template Verify**, and **Config Archive Diff**.
Tenant Administrator	• Can view and manage limited AmpCon-DC pages, including "Logical Networks", "Logical Routers", "Logical Switches", and "Tenant Management". • Can view the "Network Access" page • Can view the **PoD** tab.

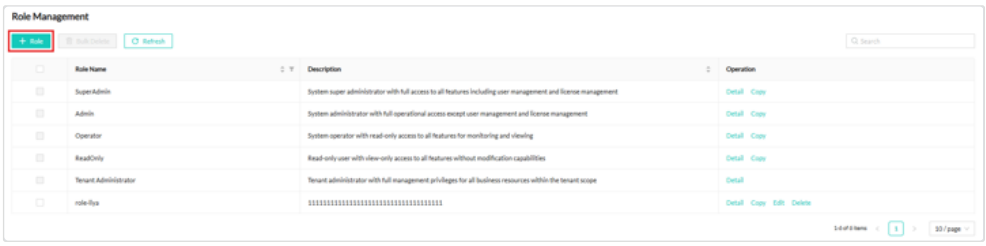
All built-in user roles cannot be deleted or edited. For detailed permissions of each built-in user role, see Permission Table for Built-In Users.

- In addition to the built-in roles, you can create custom roles. For detailed permissions of each custom role, see Viewing Role Details.
- You can assign one or multiple built-in or custom roles to a user or a user group.
  - If a user is assigned multiple roles, the user will have all permissions of these roles.
  - If a user group is assigned multiple roles, the users in the user group will have all permissions of these roles.
  - If a user is assigned multiple roles and the user group containing the user is also assigned multiple roles, the user will have the permissions of all these roles.

Creating a Custom Role

To create a custom role, follow these steps:

1. Log in to the AmpCon-DC UI with an AmpCon-DC user who has the built-in SuperAdmin role or has custom roles with the Read and Write permissions to the “Role Management” page.
2. Click **System > User Management > Role Management** from the navigation bar.
3. Click **+ Role**.



4. In the **Basic Information** section, input the following information:

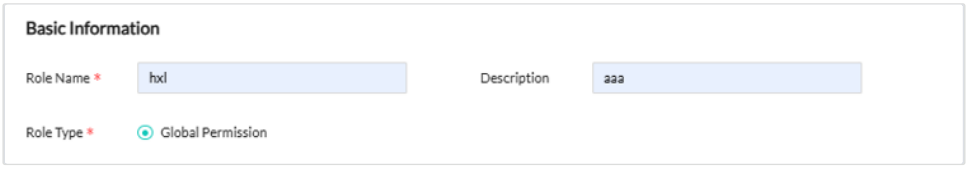


Table 2. Basic Information Parameters

Parameter	Description
Role Name	The name of the role. • The name must be unique. • The name is a string with at most 32 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ -). • The name cannot start or end with spaces.
Description	Optional. The description of the role. The value cannot exceed 256 characters.
Role Type	Currently, only **Global Permissions** is supported.

	It means that permissions are applied to an entire UI page or tab, rather than to individual buttons, fields, or operations within the page or tab.

5. In the **Operation Permissions** section, assign permissions of pages or tabs to the role:

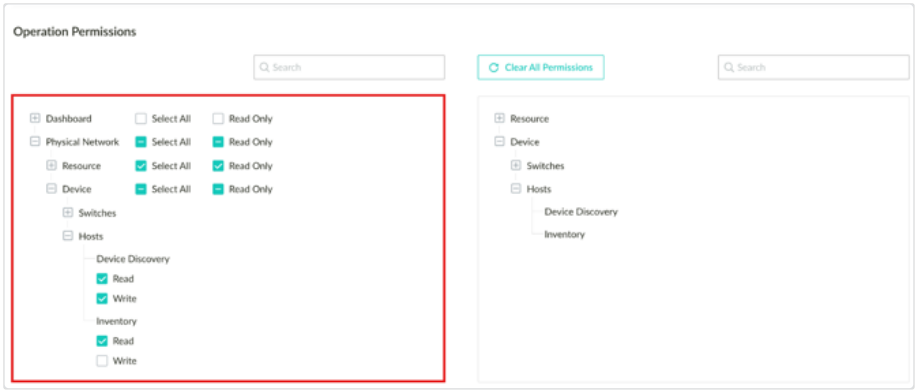
   a. Click the plus icon **+** until you locate a page or tab.

   b. Select **Read**, **Write**, or both.

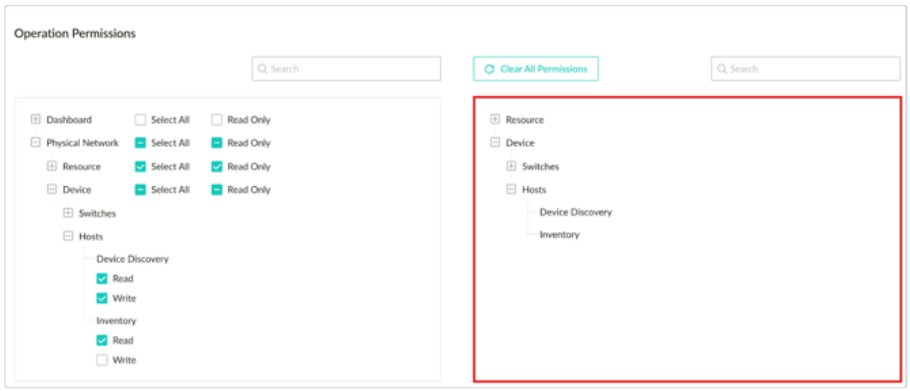
      Read: Can only view information on a page or tab.

      Write: Can view information and perform actions (such as create, modify, and delete) on a page or tab.

   c. Follow **Step a** and **Step b** to assign permissions of multiple pages or tabs.



The right section displays the selected pages or tabs and their permissions.



Tips

- If you select **Read Only** for a parent page, **Read** is automatically selected for all the pages and tabs under the parent page. And vice versa.

- If you select **Select All** for a parent page, **Read** and **Write** are automatically selected for all the pages and tabs under the parent page. And vice versa.
- To remove all configured permissions for the role, click **Clear All Permissions**.

6. Click **Apply**.

Assigning Roles to a User or User Group

You can assign roles to an existing user or user group. For more information, see Assigning Roles and Tenants.

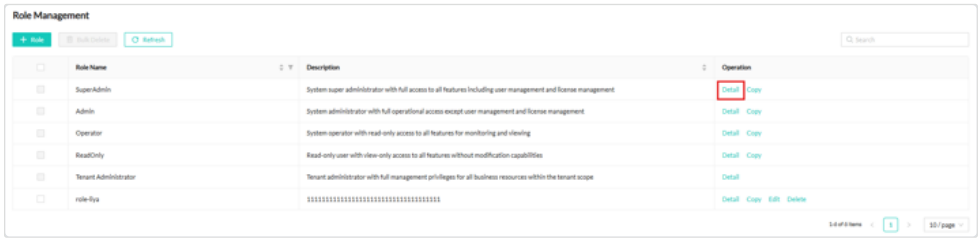
> **NOTE**
>
> A user can be used to log in to the AmpCon-DC UI only if the user is assigned at least one role or the user group containing the user is assigned at least one role.

Optional Operations

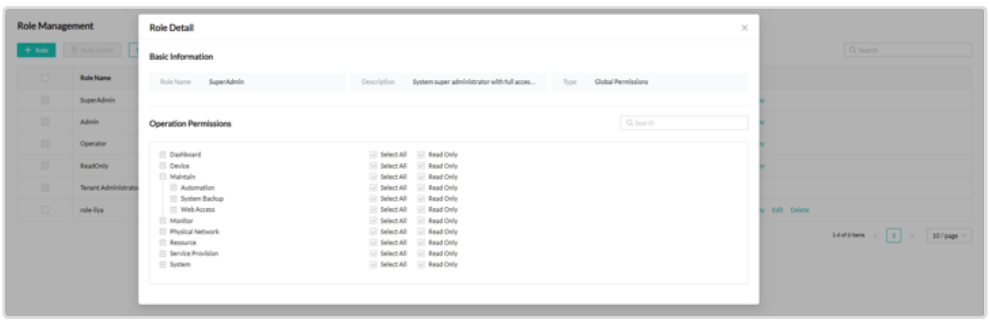
Viewing Role Details

To view details of a built-in or custom role, follow these steps:

1. Locate the role, and then click **Detail**.



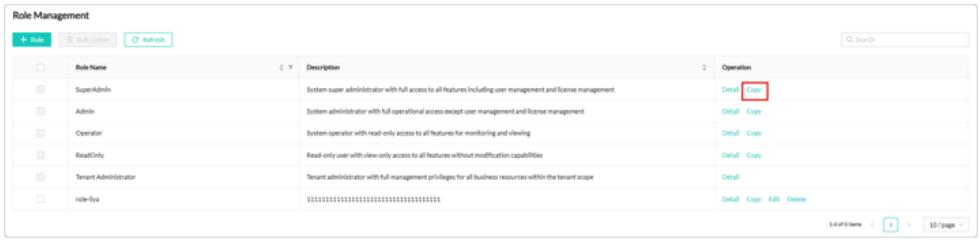
2. Check the basic information and operation permissions you configured for the role.



Copying a Role

To quickly create a new role from an existing one, follow these steps:

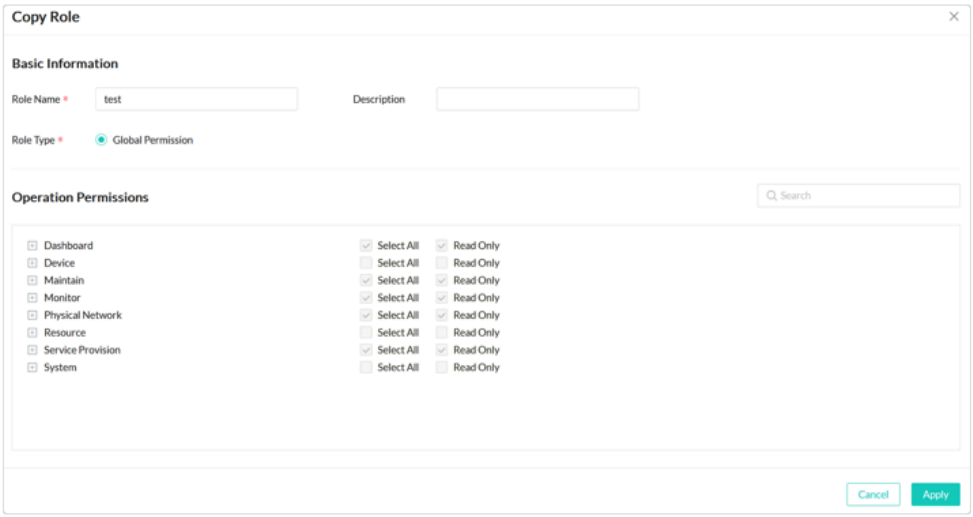
1. Locate the role, and then click **Copy**.



> **NOTE**
>
> The Tenant Administrator role cannot be copied.

2. In the pop-up window, input the name and description (optional) of the new role.

   The **Operation Permission** section is automatically filled with the copied permissions.

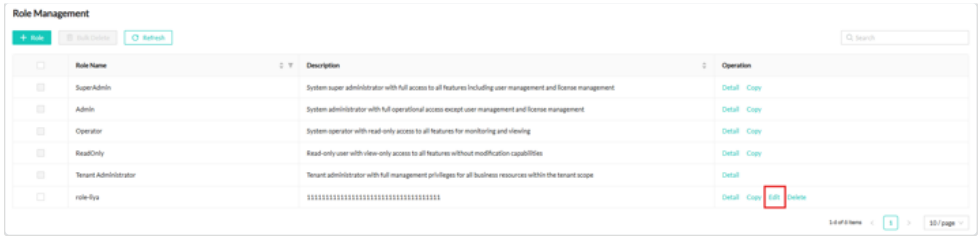


3. Click **Apply**.

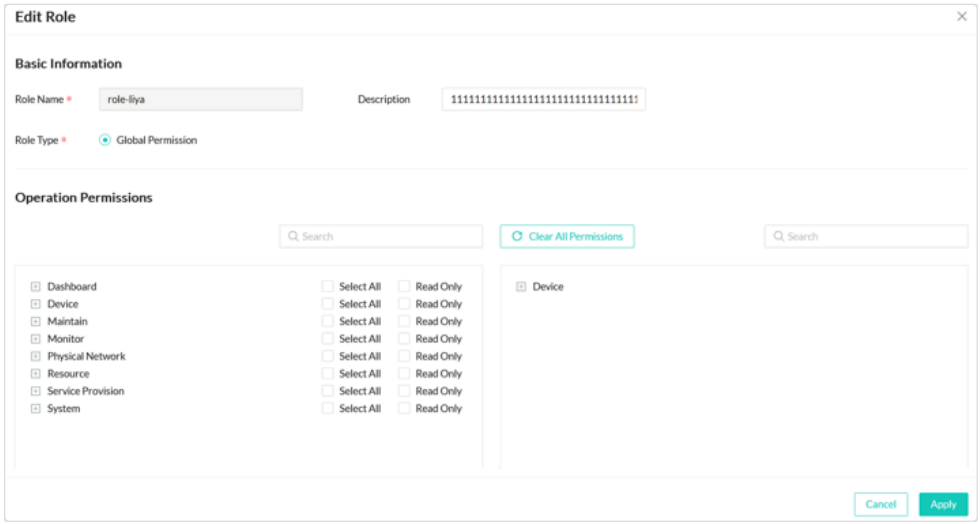
Editing a Custom Role

To edit a custom role, follow these steps:

1. Locate the role, and then click **Edit**.



2. In the pop-up window, modify the description and permissions as needed.

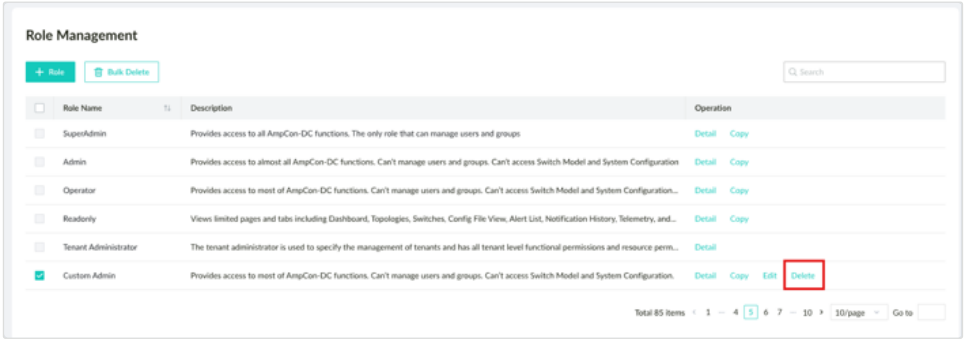


3. Click **Apply**.

Deleting One or Multiple Custom Roles

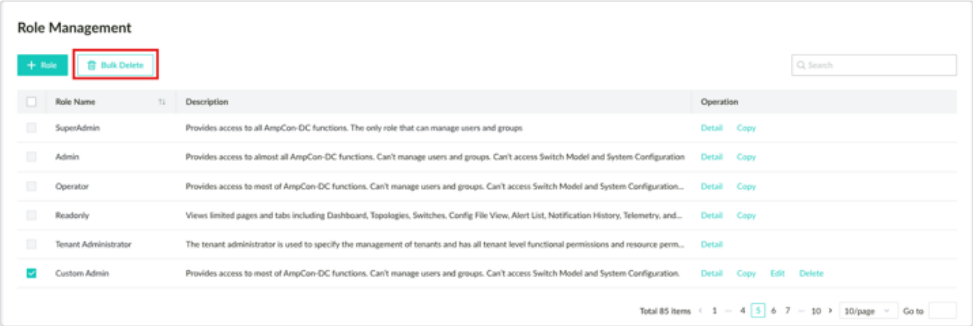
> **NOTE**
>
> If a user is assigned only the roles being deleted, the user will lose all permissions and cannot be used to log in to AmpCon-DC.

- To delete a role, locate the role, and then click **Delete**. In the pop-up window, select the check box near “I have identified the risks of this operation”, and then click **Yes**.



- To delete multiple roles in bulk, select the roles that you want to delete, and then click **Bulk Delete**. In the pop-up window, select the check box near “I have identified the risks of this

operation", and then click **Yes**.



Permission Table for Built-In Users

For menu pages and tabs in the AmpCon-DC UI, different built-in user roles have different permissions. See the following table:

Table 3. Menu and Tab Permissions

> **NOTE**
>
> AmpCon-DC provides the following permission levels for pages and tabs:
>
> - **Read**: Can only view information on a page or tab.
> - **Write**: Can view information and perform actions (such as create, modify, and delete) on a page or tab.

First-level menu	Second-level menu	Third-level menu	Tab	SuperAdmin	Admin	Operator	Read Only	Tenant Administrator
Dashboard	System Overview			Read & Write	Read & Write	Read & Write	Read	No Access
	Switch Overview			Read & Write	Read & Write	Read & Write	Read	No Access
Physical	Topologies			Read &	Read &	Read &	Read	No Acce

Network				Write	Write	Write		ss
	Design	ZTP Templates		Read & Write	Read & Write	Read & Write	No Access	No Access
		Units		Read & Write	Read & Write	Read & Write	No Access	No Access
		DC Templates		Read & Write	Read & Write	Read & Write	No Access	No Access
	Fabrics			Read & Write	Read & Write	Read & Write	No Access	No Access
	RoCE	RoCE Easy Deploy		Read & Write	Read & Write	Read & Write	No Access	No Access
		RoCE Policies		Read & Write	Read & Write	Read & Write	No Access	No Access
		Load Balancing		Read & Write	Read & Write	Read & Write	No Access	No Access
		NIC Configurations		Read & Write	Read & Write	Read & Write	No Access	No Access
Resource	Resource Interconnection		PoD	Read & Write	Read & Write	Read & Write	No Access	Read
			VLAN Domain	Read & Write	Read & Write	Read & Write	No Access	No Access

			Node Addition	Read & Write	Read & Write	Read & Write	No Access	No Access
	OS Images			Read & Write	Read & Write	Read & Write	No Access	No Access
	Device Licenses			Read & Write	Read & Write	Read & Write	No Access	No Access
	Group Management			Read & Write	No Access	No Access	No Access	No Access
	Pools	IP Pools		Read & Write	Read & Write	Read & Write	No Access	No Access
		ASN Pools		Read & Write	Read & Write	Read & Write	No Access	No Access
		VNI Pools		Read & Write	Read & Write	Read & Write	No Access	No Access
Device	Switches			Read & Write	Read & Write	Read & Write	Read	No Access
	Hosts		Device Discovery	Read & Write	Read & Write	Read & Write	No Access	No Access
			Inventory	Read & Write	Read & Write	Read & Write	Read	No Access

NICs			Read & Write	Read & Write	Read & Write	Read	No Access
Device Profiles		Global Configuration	Read & Write	Read & Write	Read & Write	No Access	No Access
		Switch Configuration	Read & Write	Read & Write	Read & Write	No Access	No Access
		Config File View	Read & Write	Read & Write	Read & Write	Read	No Access
		Switch Model	Read & Write	No Access	No Access	No Access	No Access
		System Configuration	Read & Write	No Access	No Access	No Access	No Access
Config Templates		New Template	Read & Write	Read & Write	Read & Write	No Access	No Access
		Template List	Read & Write	Read & Write	Read & Write	No Access	No Access
		Push Confi	Read &	Read &	Read &	No Acce	No Acce

			g	Write	Write	Write	ss	ss
			Template Verify	Read & Write	Read & Write	Read & Write	Read	No Access
			Config Archive Diff	Read & Write	Read & Write	Read & Write	Read	No Access
			Config Backup	Read & Write	Read & Write	Read & Write	No Access	No Access
Service Provision	Logical Networks			Read & Write	Read & Write	Read & Write	No Access	Read & Write
	Logical Switches			Read & Write	Read & Write	Read & Write	No Access	Read & Write
	Logical Routers			Read & Write	Read & Write	Read & Write	No Access	Read & Write
	Network Access			Read & Write	Read & Write	Read & Write	No Access	Read
Monitor	Alerts	Alert List		Read & Write	Read & Write	Read & Write	Read	No Access

		Notification Rules		Read & Write	Read & Write	Read & Write	No Access	No Access
		Notification History		Read & Write	Read & Write	Read & Write	Read	No Access
	Telemetry	Performance Statistics		Read & Write	Read & Write	Read & Write	Read	No Access
		RoCE Counters		Read & Write	Read & Write	Read & Write	Read	No Access
	RoCE Insight	Network Congestion		Read & Write	Read & Write	Read & Write	Read	No Access
	Event Log			Read & Write	Read & Write	Read & Write	Read	No Access
	Splunk Integration			Read & Write	Read & Write	Read & Write	No Access	No Access
Maintain	Automation	Playbooks		Read & Write	Read & Write	Read & Write	No Access	No Access
		Ansible Jobs		Read & Write	Read & Write	Read & Write	No Access	No Access
		Schedule		Read & Write	Read & Write	Read & Write	No Access	No Access
	System			Read &	Read &	Read &	No Acce	No Acce

	Backup			Write	Write	Write	ss	ss
	Web Access			Read & Write	Read & Write	Read & Write	No Access	No Access
System	User Management	User Settings		Read & Write	No Access	No Access	No Access	No Access
		Authorization Wizard		Read & Write	No Access	No Access	No Access	No Access
		Role Management		Read & Write	No Access	No Access	No Access	No Access
	Tenant Management			Read & Write	Read & Write	Read	Read	Read
	Email Setting			Read & Write	Read & Write	Read & Write	No Access	No Access
	Software License	License View		Read & Write	Read & Write	No Access	No Access	No Access
		License Management		Read & Write	Read & Write	No Access	No Access	No Access
		License Log		Read & Write	Read & Write	No Access	No Access	No Access

Managing Tenants

In AmpCon-DC, a tenant is a logical resource unit used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other, ensuring that logical network resources of one tenant do not affect others.

Tenants are managed by AmpCon-DC users. When you log in to the AmpCon-DC UI with a user, you can view and manage the logical networks belonging to the tenants managed by the user. This mechanism provides resource isolation and access control in multi-tenant environments.

Use Cases
Adding a Tenant
Viewing a Tenant
Editing a Tenant
Deleting a Tenant
Filtering and Sorting Tenants

Use Cases

Tenants can be used in the following use cases:

- **Logical isolation of resources**

  Resources belonging to different tenants are logically isolated from each other, allowing different tenants to independently manage their own logical network resources without affecting others.

- **Multi-user collaborative management**
  Multiple users can be authorized to manage the same tenant, enabling collaborative operations while ensuring permission consistency.
- **Support for multi-business scenarios**

  By providing logical network isolation through tenants, AmpCon-DC supports overlay service provisioning scenarios involving multiple business systems, departments, subsidiaries, or customers on a single platform.

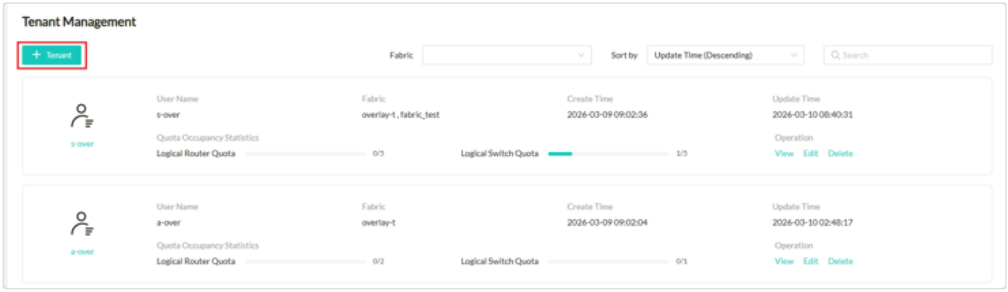
Adding a Tenant

To add a tenant, follow these steps:

1. Log in to the AmpCon-DC UI with an AmpCon-DC user who has the built-in SuperAdmin or admin role, or has custom roles with the Read and Write permissions to the “Tenant

Management” page.

2. Click **System > Tenant Management** from the navigation bar.
3. Click **+ Tenant**.



4. In the **Basic Information** section, input the following information:

Table 1. Basic Information Parameters

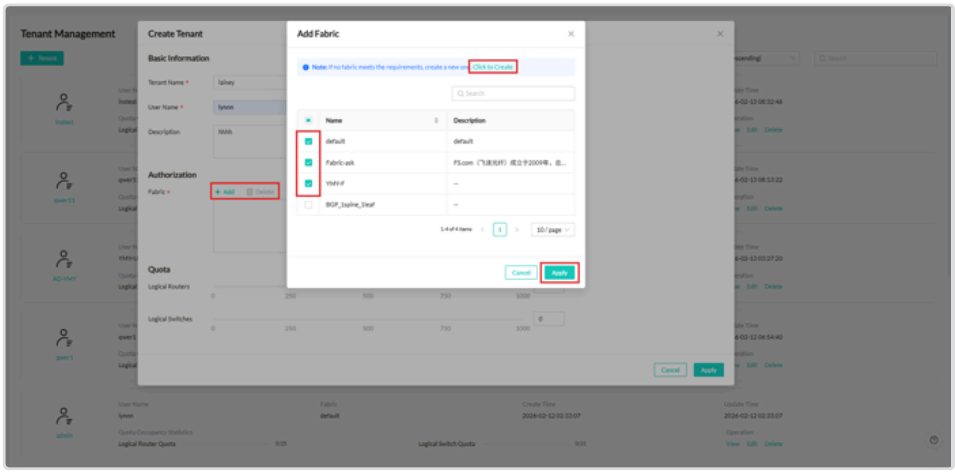
Parameter	Description
Tenant Name	The name of the tenant. • The tenant name must be a string with at most 64 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z. ◦ Digits including 0 to 9. ◦ Special characters (_ -). • The tenant name cannot start or end with spaces. • The tenant name must be unique. • The tenant name cannot be **admin**.
User Name	The username of the initial tenant administrator user. • The username must be unique. • The user name cannot exceed 32 characters. The following characters are supported: ◦ Lowercase letters, including a to z. ◦ Uppercase letters, including A to Z.

	◦ Digits including 0 to 9. ◦ Special characters (_ -). • The tenant name cannot start or end with spaces. **NOTEs** • Tenants can't be used to log in to the AmpCon-DC UI. Therefore, when you create a tenant, AmpCon-DC will create an user based on the specified **User Name** and **Login Password**. • The user serves as the initial administrator of the tenant. You can use the user to log in to the AmpCon-DC UI for logical network management. • After creating a tenant, you can also assign the tenant to other users. For more information, see Assigning Roles and Tenants.
Login Password	The password of the initial tenant administrator user. The value must include uppercase letters, lowercase letters, numbers, and special characters. It must be equal to or longer than 10 characters.
Confirm Password	Re-enter the login password to confirm it. **NOTE** The **Confirm Password** must match the **Login Password**.
Description	Optional. The description of the tenant. The value cannot exceed 256 characters.

5. In the **Authorization** section, associate the tenant with one or multiple fabrics by clicking **+Add**, selecting one or multiple fabrics, and clicking **Apply**.

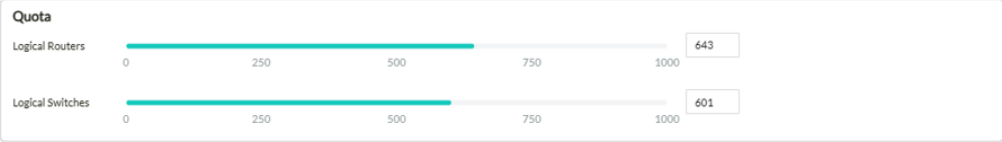
   After a fabric is associated, the fabric can be used to deploy logical networks by the tenant.

> **Tips**
>
> - If no fabric meets your needs, click **Click to Create** to create new fabrics. You are redirected to the “Fabrics” page. For more information, see Adding a Fabric.
> - To dissociate fabrics from the tenant, select the fabrics displayed in the list box. Then, click **Delete** to remove the association.
> - Fabrics cannot be dissociated from the tenant in the following cases:
>   - The fabrics have been used when you add logical switches or logical routers to logical networks. You need to delete these logical routers and logical switches first. For more information, see Deleting a Logical Switch and Deleting a Logical Router.
>   - VPCs in these fabrics have already been assigned to this tenant. You need to unbind these VPCs from the tenant first. For more information, see Unbinding VPCs from Tenants.



6. In the **Quota** section, specify the following resource limits for the tenant by dragging the slider or entering a value directly in the input field:

- **Logical Routers**: The maximum number of logical routers that the tenant can create. The value cannot exceed 1000.
- **Logical Switches**: The maximum number of logical switches that the tenant can create. The value cannot exceed 1000.



7. Click **Apply**.

Viewing a Tenant

In the **Tenant Management** page, you can see all tenants managed by the logged-in AmpCon-DC user.

> **NOTE**
>
> If you log in to the AmpCon-DC UI with a user authenticated and authorized through TACACS+ and has a SuperAdmin role assigned, you can see all tenants created by all AmpCon-DC users.

- To view the basic information of a tenant, locate the tenant, and then click **View**.

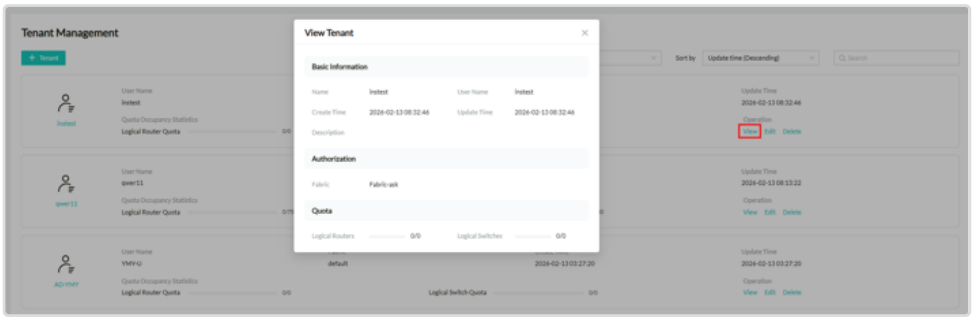
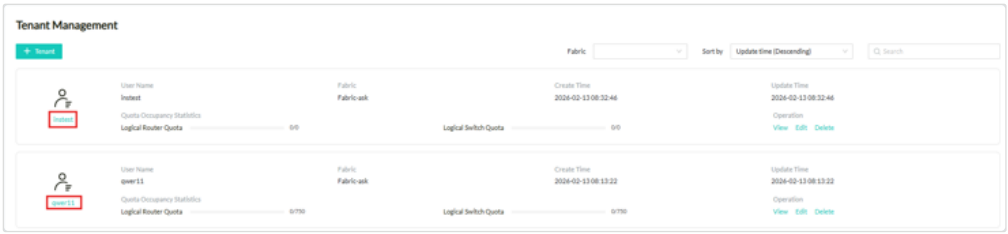


Table 2. Basic Information Metrics

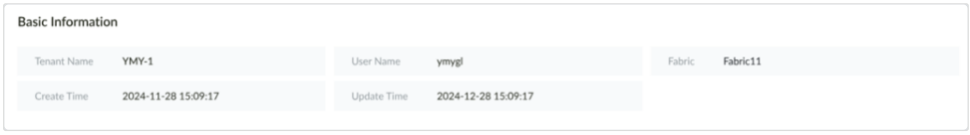
Metric	Description
Name	The name that you specified for the tenant.
User Name	The username of the initial tenant administrator user. You can use the user to log in to the AmpCon-DC UI.
Create Time	The time when the tenant was created.
Update Time	The most recent time when the tenant was edited.
Description	The description of the tenant.

Fabric	The fabrics associated with the tenant.
Logical Routers	The maximum number of logical routers that the tenant can create, and the current number of logical routers already created.
Logical Switches	The maximum number of logical switches that the tenant can create, and the current number of logical switches already created.

- To check the detailed information of a tenant, locate the tenant, and click the tenant's name below the avatar. Then, in the pop-up window, you can see the tenant details.



For descriptions of the metrics in the **Basic Information** section, see **Table 2. Basic Information Metrics**.



In the **Logical Network** tab, you can see all the logical networks owned by the tenant.

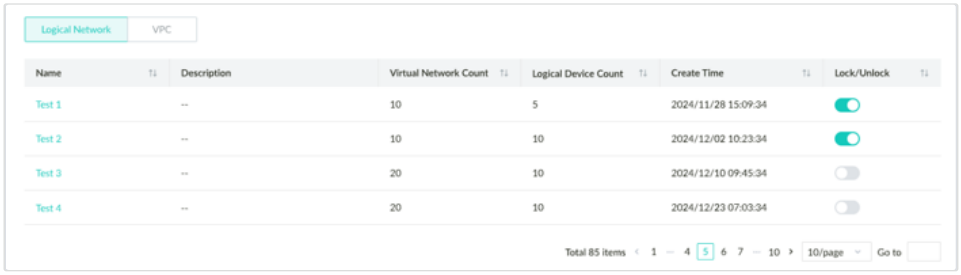


Table 3. Logical Network Metrics

Metric	Description
Name	The name to distinguish the logical network. To go to the “Logical Networks” page, click the name.

Description	The description of the logical network.
Virtual Network Count	The total number of virtual networks in the logical network. If you haven't added virtual networks, the value is 0.
Logical Device Count	The total number of logical devices (logical routers and logical switches) in the logical network. If you haven't added logical routers and logical switches, the value is 0.
Create Time	The time when the logical network was created.
Lock/Unlock	Whether to lock the logical network so that it can't be deleted.

In the **VPC** tab, you can see all the VPCs allocated to the tenant.

> **NOTEs**
>
> - If no VPC is allocated to the tenant, this tab displays no data. For how to allocate VPCs to tenants, see Allocating VPCs to Tenants.
> - To unbind a VPC from the tenant, locate the VPC, and then click **Unbind**. If a VPC is already used in a logical network, the VPC cannot be unbound.



Table 4. VPC Metrics

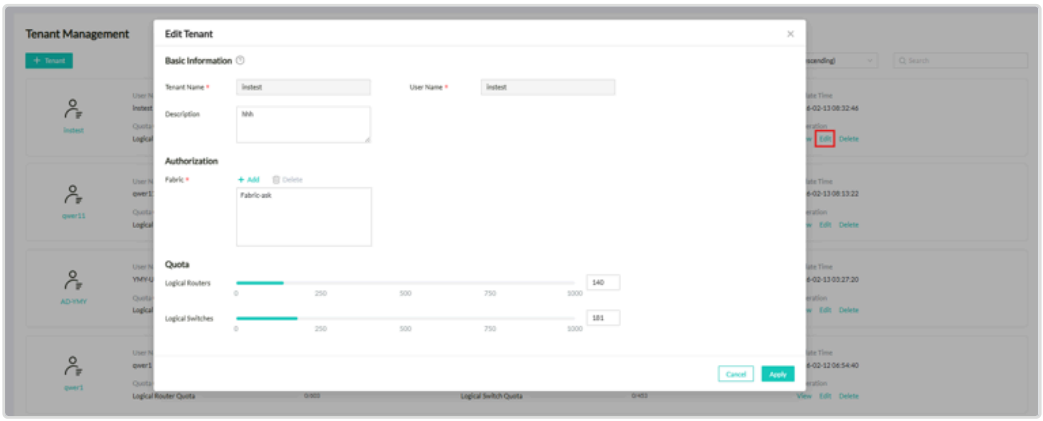
Metric	Description
Resource Type	The resource type of the PoD to which the VPC belongs. Values can be **OpenStack**, **vSphere**, or **Bare Metal**.

VPC ID	The ID assigned automatically by AmpCon-DC.
VPC Name	The name of the VPC.
Fabric	The fabric to which the VPC belongs.
PoD	The PoD to which the VPC belongs.
Current Status	Indicates whether the VPC is used in a logical network. • **Used**: The VPC is used in a logical network. • **Unused**: The VPC is not used in a logical network.

Editing a Tenant

To edit a tenant, locate the tenant, and then click **Edit**.

> **NOTE**
>
> - The **Tenant Name** and **User Name** cannot be edited.
> - The quota for logical routers and logical switches cannot be less than the count of logical routers and logical switches that are currently in use.



Deleting a Tenant

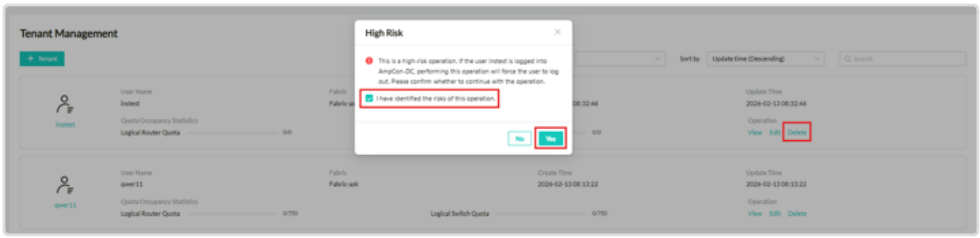
To delete a tenant, follow these steps:

> **NOTEs**

- Before deleting a tenant, delete all connections between logical network elements in all logical networks created by this tenant. For more information, see Disconnecting Connections in a Logical Network.
- Ensure all logical networks created by the tenant are unlocked before deletion. For more information, see Deleting Logical Networks.

1. Locate the tenant to be deleted, and then click **Delete**.
2. Click the checkbox beside the “I have identified the risks of this operation” message.
3. Click **Yes**.

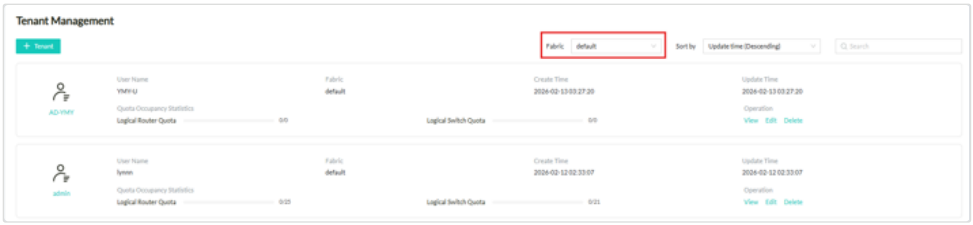
> **Tip**
>
> Deleting a tenant will lead to the following results:
>
> - The VPCs allocated to the tenant are automatically unbound from the tenant.
> - The initial tenant administrator user is deleted.
> - All logical networks created by the tenant are deleted.
> - The quotas for logical switches and logical routers consumed by those logical networks are released.



Filtering and Sorting Tenants

You can filter tenants by fabric and sort them by using different sorting options:

- To view all the tenants associated with a specific fabric, select the fabric in the **Fabric** drop-down list.



- To sort the tenant list, select a sorting option in the **Sort By** drop-down list:

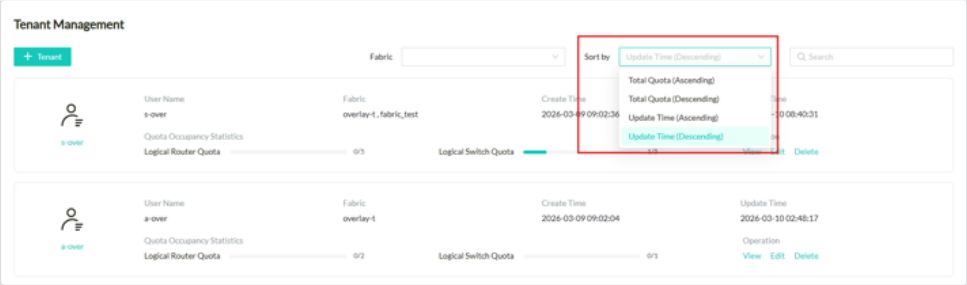


Table 5. Sort Parameters

Parameter	Description
Total Quota (Ascending)	Sorts tenants by the total quota (including logical switches and logical routers) in ascending order, from the lowest to the highest.
Total Quota (Descending)	Sorts tenants by the total quota (including logical switches and logical routers) in descending order, from the highest to the lowest.
Update Time (Ascending)	Sorts tenants by the update time in ascending order, from the earliest to the most recent.
Update Time (Descending)	Sorts tenants by the update time in descending order, from the most recent to the earliest.

Assigning Roles and Tenants

After creating a user or user group, you must assign roles and tenants to the user or user group. In this way, each user or user group has only the permissions required for their responsibilities.

By separating authorization from user creation, AmpCon-DC provides flexible and granular access management and clear visibility into assigned access permissions.

Guidelines
Prerequisites
Assigning Roles and Tenants to a User
Assigning Roles and Tenants to a User Group

Guidelines

- In AmpCon-DC, access permissions are determined through the combination of users, roles, and tenants:
  - Users represent the accounts used to log in to the AmpCon-DC UI.
  - Roles define the permissions that determine which pages and tabs a user can access (Read or Write).
  - Tenants are logical resource units used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks.
- You can assign one or multiple built-in or custom roles to a user or a user group.
  - If a user is assigned multiple roles, the user will have all permissions of these roles.
  - If a user group is assigned multiple roles, the users in the user group will have all permissions of these roles.
  - If a user is assigned multiple roles and the user group containing the user is also assigned multiple roles, the user will have the permissions of all these roles.
  - If a user is assigned at least a tenant, the Tenant Management role is automatically assigned to the user.
- A user can be used to log in to the AmpCon-DC UI only if the user is assigned at least one role or the user group containing the user is assigned at least one role.
- You can assign one or multiple tenants to a user or a user group.
  - If a user is assigned multiple tenants, the user can manage all these tenants.
  - If a user group is assigned multiple tenants, the users in the user group can manage all these tenants.
  - If a user is assigned multiple tenants and the user group containing the user is also assigned multiple tenants, the user can manage all these tenants.

- Roles and tenants assigned to user groups are not displayed on the “Authorization Wizard” page. To check the roles and tenants assigned to a user group, see Viewing a User Group.

Prerequisites

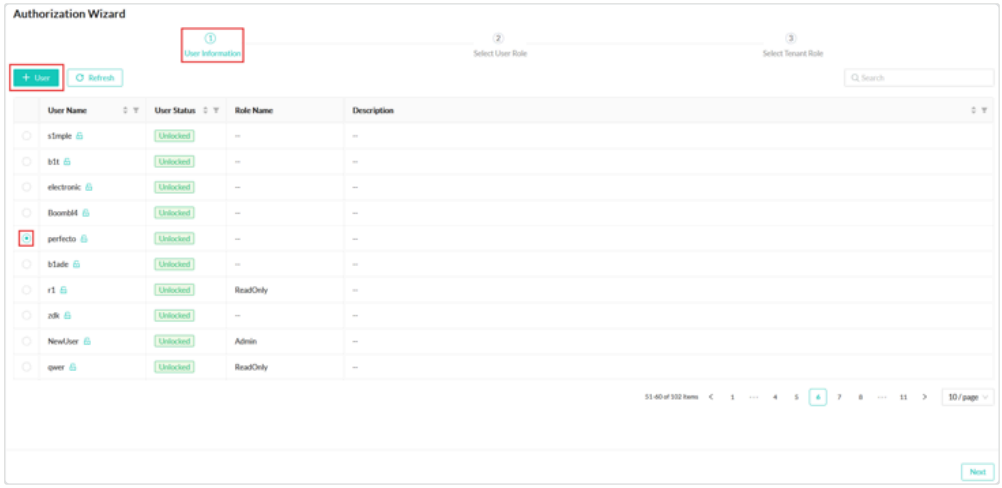
- If you want to assign custom roles to users, ensure that the custom roles have been created. For more information, see Creating a Custom Role.
- If you want to assign tenants to users, ensure that the tenants have been created. For more information, see Adding a Tenant.

Assigning Roles and Tenants to a User

To assign roles and tenants to a user, follow these steps:

1. In the AmpCon-DC UI, click **System > User Management > Authorization Wizard** from the navigation bar.
2. In the **User Information** section, select a user, and then click **Next**.

> **NOTEs**
>
> - The built-in user **admin** is assigned the SuperAdmin and Tenant Administrator roles and can manage all tenants.
> - If no users meet your needs, click **+ User** to create a new user. For more information, see Adding a User.



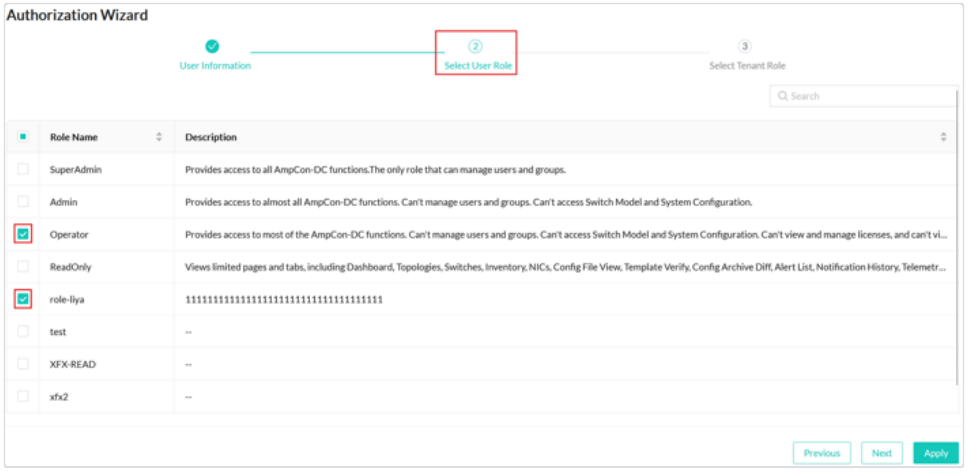
For the metrics in the **User Information** section, see the following table:

Table 1. User Information Metrics

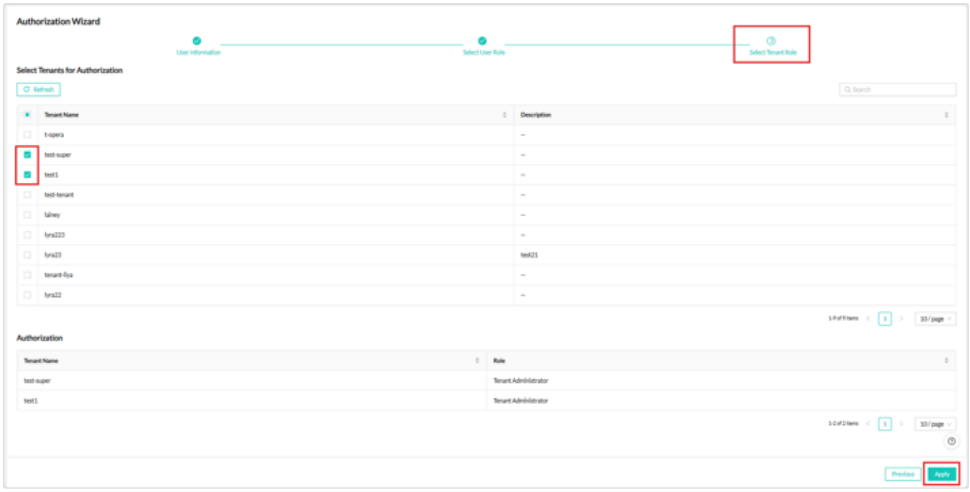
Metric	Description

User Name	The username of the user.
User Status	Indicates whether the user is locked. • **Locked**: The user is locked and cannot be used to log in to the AmpCon-DC UI. • **Unlocked**: The user is unlocked and can be used to log in to the AmpCon-DC UI.
Role Name	The roles you have assigned to the user.
Description	The description of the user.

3. In the **Select User Role** section, all built-in roles and custom roles are displayed in the role list. Select one or multiple roles to assign to the selected user.



4. Optional: To assign tenants to the selected user, click **Next**. In the **Select Tenant Role** section, select one or multiple tenants.



In the **Authorization** list, you can see all the selected tenants. The role is displayed as **Tenant Administrator**.

5. Click **Apply** to complete the authorization.

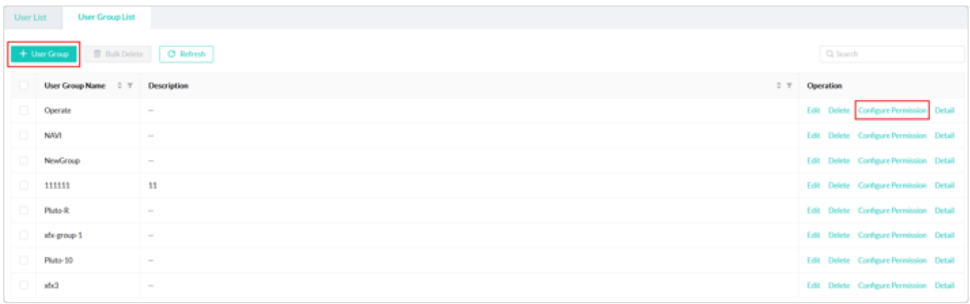
> **NOTE**
>
> If you skip **Step 4** before clicking **Apply**, the previous assigned tenants remain.

Assigning Roles and Tenants to a User Group

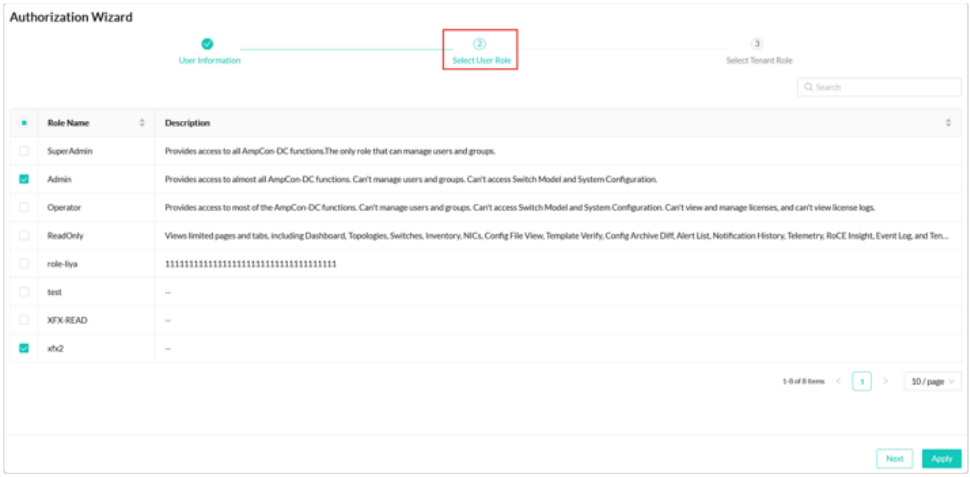
To assign the same roles and tenants to multiple users, you are recommended to add these users to a user group and then assign roles and tenants to the user group, instead of authorizing each user one by one. Follow these steps:

1. In the AmpCon-DC UI, click **System > User Management > User Settings** from the navigation bar.
2. Click the **User Group List** tab.
3. Locate a user group, and then click **Configure Permission** in the **Operation** column. You are then redirected to the **Select User Role** section of the “Authorization Wizard” page.

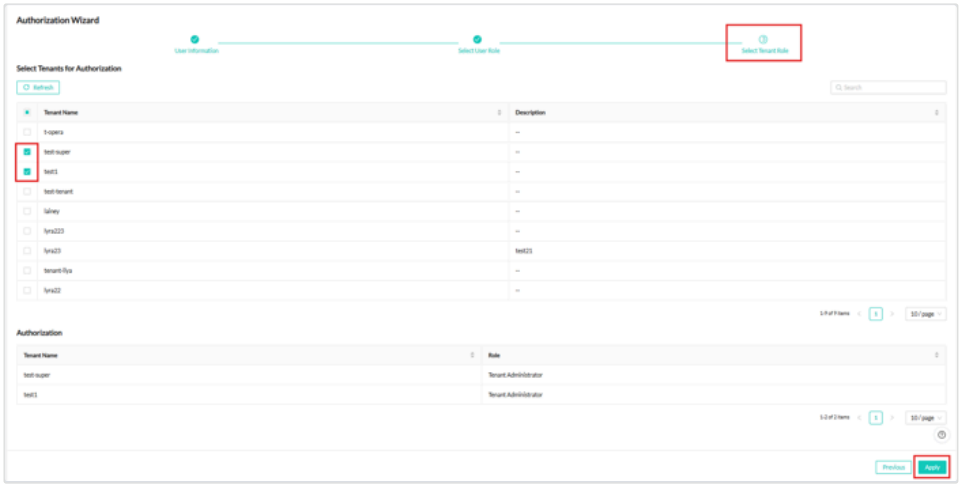
> **NOTE**
>
> If no user groups meet your needs, click **+ User Group** to create a new user group. For more information, see Adding a User Group.



4. In the **Select User Role** section, all built-in roles and custom roles are displayed in the role list. Select one or multiple roles to assign to the user group.



5. Optional: To assign tenants to the selected user group, click **Next**. In the **Select Tenant Role** section, select one or multiple tenants.



In the **Authorization** list, you can see all the selected tenants. The role is displayed as **Tenant Administrator**.

6. Click **Apply** to complete the authorization.

> **NOTE**
>
> If you skip **Step 5** before clicking **Apply**, the previous assigned tenants remain.

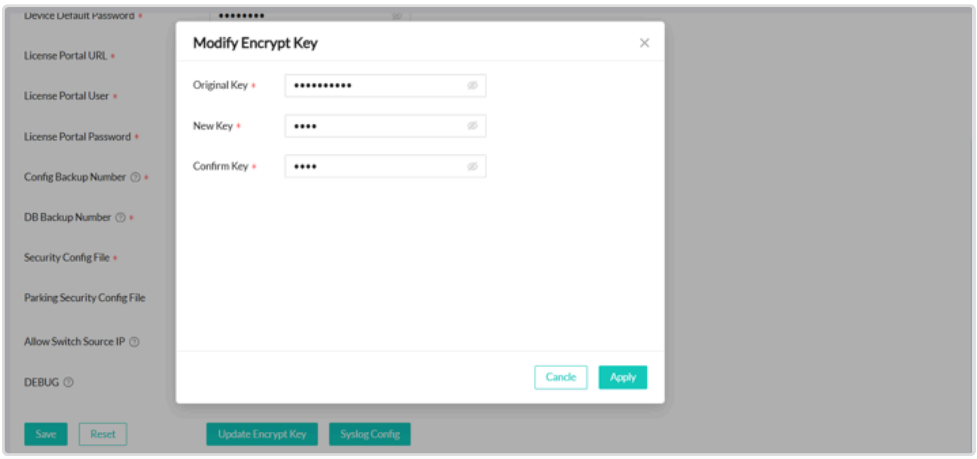
Updating the Encryption Key for Sensitive Data Encryption

After you deploy AmpCon-DC, a default encryption key is generated to encrypt sensitive data (such as passwords) in the AmpCon-DC database, ensuring sensitive data security. You can update the encryption key as you need.

Procedure

To update the encryption key, follow these steps:

1. Log in to the AmpCon-DC UI, and click **Device > Device Profiles** from the navigation bar.
2. Click the **System Configuration** tab, and then click **Update Encrypt Key**.
3. Enter the original key and the new key. The default encryption key is **pica8pica8**



4. Click **Apply**.

Forwarding Logs to External Syslog Servers

AmpCon-DC supports forwarding system logs to external Syslog servers like Splunk. In this way, you can view and analyze AmpCon-DC system logs more conveniently.

To do so, you need to add correct Syslog configurations to AmpCon-DC.

Prerequisite
Procedure
Example: Forwarding System Logs to Splunk
Verifying System Log Forwarding
Optional: Deleting a Syslog Configuration

Prerequisite

Ensure that the Syslog services are enabled on the external Syslog servers.

Procedure

To add a Syslog configuration, follow these steps:

1. Log in to the AmpCon-DC UI, and then click **Device > Device Profiles** from the navigation bar.
2. Click the **System Configuration** tab, and then click **Syslog Config.**
3. In the pop-up window, input the following information:

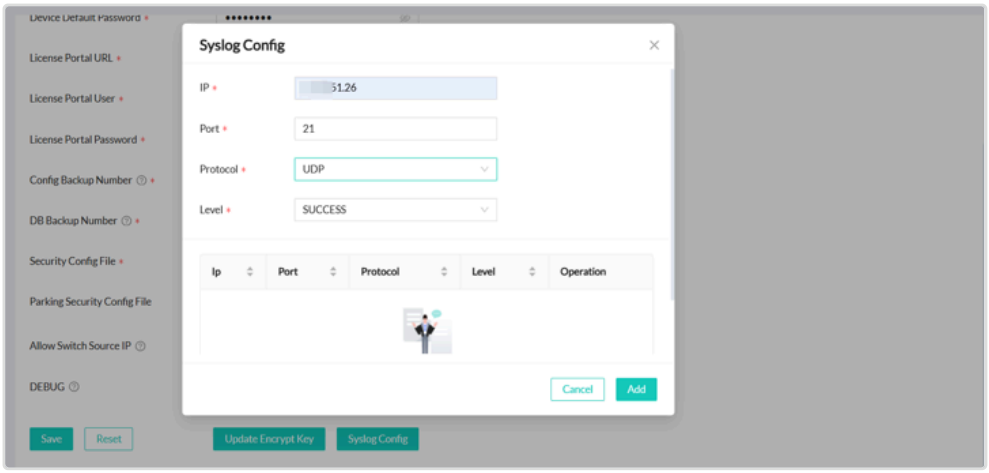


Table 1. Syslog Configuration Parameters

Parameter	Description
IP	The IPv4 address of the external Syslog server.

Port	The Syslog server port number used for data forwarding. **NOTE** Ensure that the port is correct. Or else, AmpCon-DC system logs will fail to be sent to the Syslog server.
Protocol	The protocol of the external Syslog server, **TCP** or **UDP**. **NOTE** Ensure that the protocol is correct and matches with the port number. Or else, AmpCon-DC system logs will fail to be sent to the Syslog server.
Level	The AmpCon-DC Log levels to be sent to the external Syslog server, **SUCCESS** or **ERROR**. • **SUCCESS:** The Syslog server can receive system logs with a **warning (level=4)** level or higher from AmpCon-DC. • **ERROR:** The Syslog server can receive system logs with an **info (level=6)** level or higher from AmpCon-DC.

4. Click **Add**.
5. Optional: To add another Syslog configuration, repeat **Step 3** to **Step 4**.

NOTEs

- You can add one or multiple Syslog configurations.
- But for each Syslog server, only one Syslog configuration can be added.

6. Click the close icon to close the pop-up window.

Then, AmpCon-DC system logs will be sent to the added Syslog servers.

Example: Forwarding System Logs to Splunk

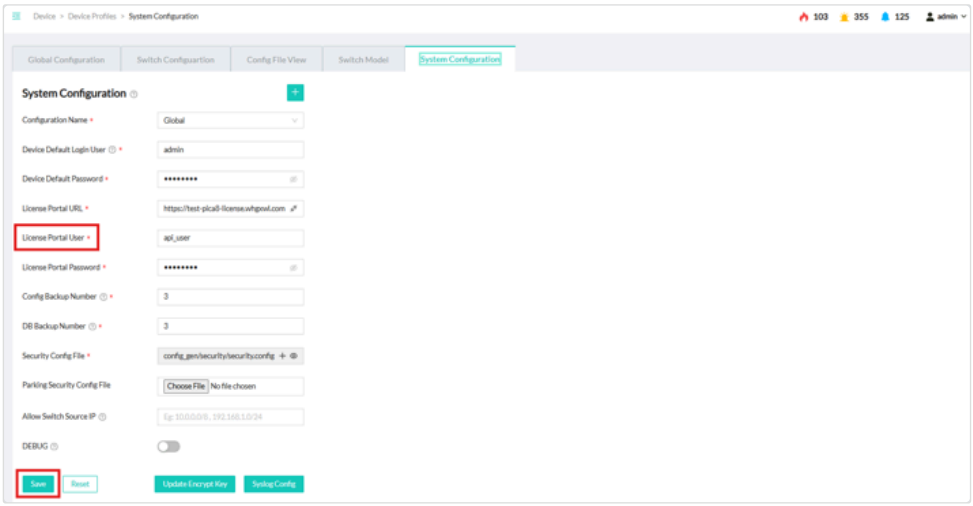
You can send real-time AmpCon-DC system logs to Splunk by adding Syslog configurations. Then, you can view and analyze these logs in the Splunk UI.

For detailed configurations, see Sending Logs to Splunk.

Verifying System Log Forwarding

To verify whether AmpCon-DC logs can be forwarded to an added Syslog server, follow these steps:

1. Click **Device > Device Profiles** from the navigation bar.
2. Click the **System Configuration** tab.
3. In the **License Portal User** field, enter an incorrect license portal username, and then click **Save**.

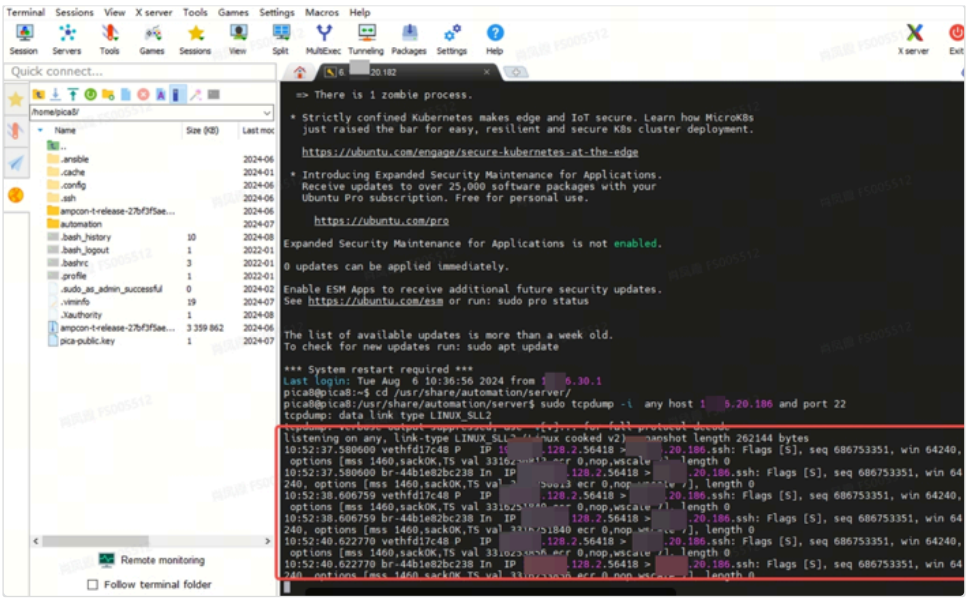


4. Access the AmpCon-DC server by using MobaXterm, and then check data forwarding by running the following command:

   ```
   sudo tcpdump -i any host <Syslog-Server-IP> and port <Syslog-Server-Port>
   ```

- Replace *<Syslog-Server-IP>* with the IPv4 address of the external Syslog server.
- Replace *<Syslog-Server-Port>* with the Syslog server port number used for data forwarding.

  See the following example:

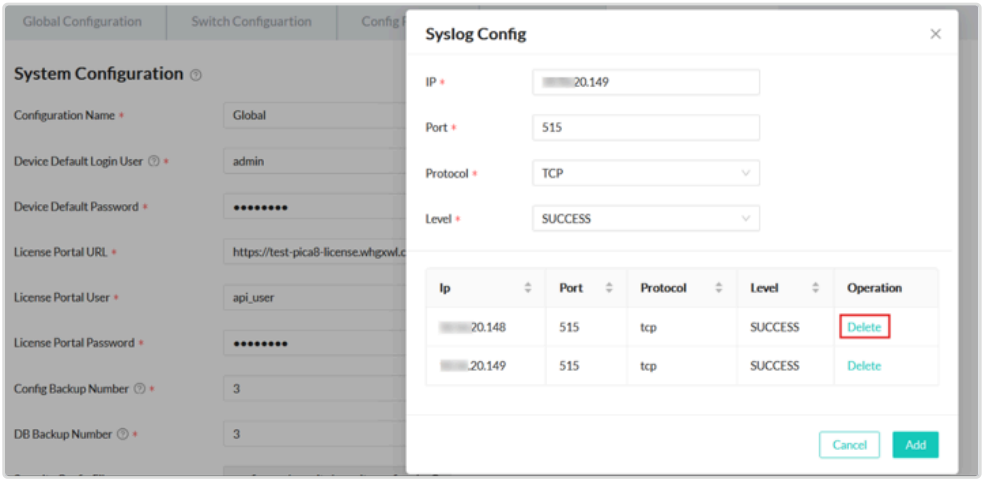


Optional: Deleting a Syslog Configuration

> **NOTE**
>
> You can't edit a Syslog configuration directly. If a Syslog configuration is outdated, delete it, and then add a new one.

To delete a Syslog configuration, follow these steps:

1. In the **System Configuration** tab, click **Syslog Config.**
2. In the pop-up window, locate the Syslog configuration, and then click **Delete**.



3. Click the close icon to close the pop-up window.

Backing Up and Restoring the AmpCon-DC Database

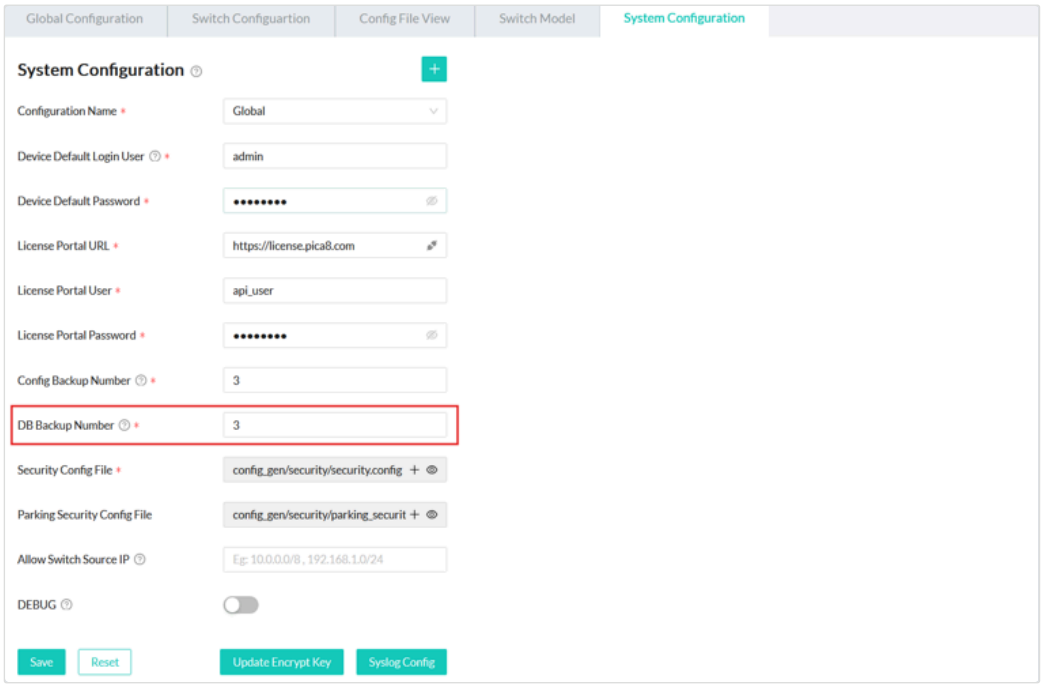
You can back up and restore the AmpCon-DC database securely for disaster recovery.

Prerequisite
Creating a Database Backup
Restoring from a Database Backup
Optional: Editing a Database Backup
Optional: Removing a Database Backup

Prerequisite

The allowed maximum number of database backups is set based on the **DB Backup Number** field in the “System Configuration” tab.

Before you create a database backup, ensure that the current backup number doesn’t reach the allowed maximum number. You can remove a database backup if it is not needed.



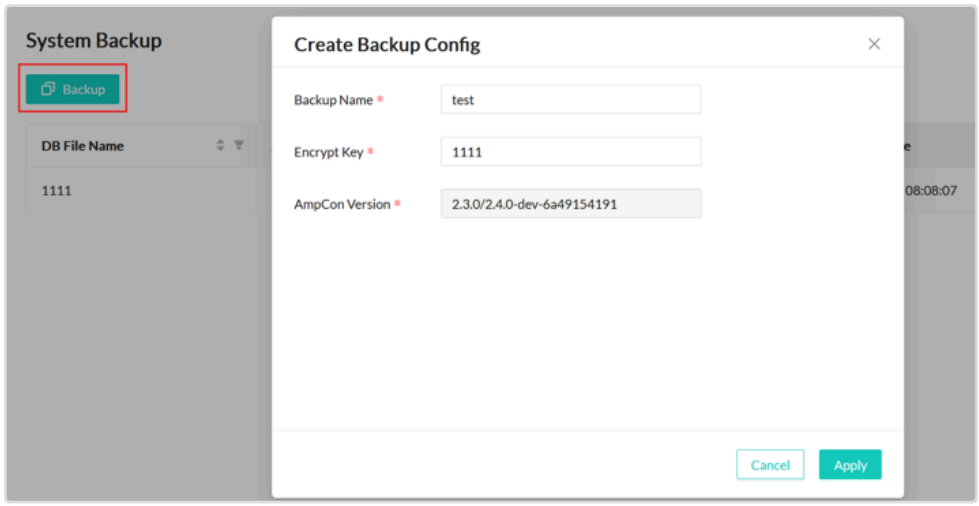
Creating a Database Backup

To create a database backup, follow these steps:

1. Log in to the AmpCon-DC UI, and click **Maintain > System Backup**.
2. Click **Backup**. The **Create Backup Config** pop-up window opens.
3. Enter the following information:

- **Backup Name**: The name of the backup to differentiate from the other backups.

- **Encrypt Key**: The encrypt key that you set on the global “System Config” page. The default encrypt key is pica8pica8
- **AmpCon Version**: The version of AmpCon-DC that you use.



4. Click **Apply**.

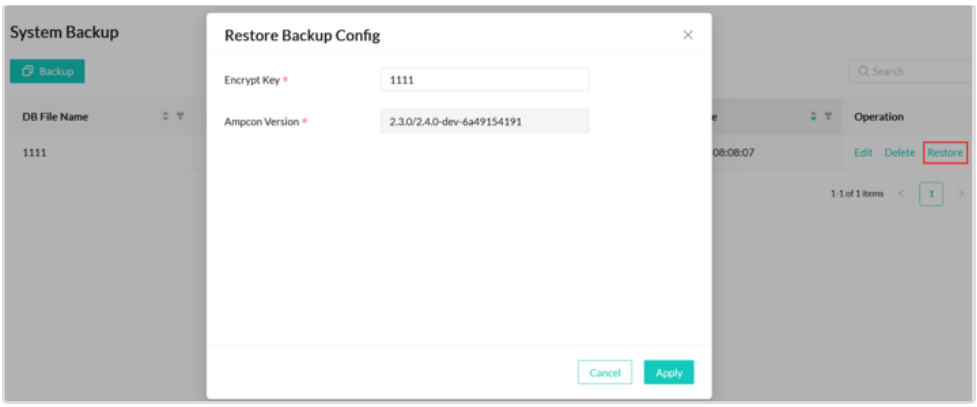
Restoring from a Database Backup

To restore from a database backup, follow these steps:

> **NOTE**
>
> The restore operation can only be executed once, and after an update, previous files cannot be restored.

1. Log in to the AmpCon-DC UI, and click **Maintain > System Backup**.
2. Locate the backup, and click **Restore** on the right.
3. In the **Restore Backup Config** pop-up window, input the following information:

- **Encrypt Key**: The encrypt key that you set on the global “System Config” page. The default encrypt key is pica8pica8
- **AmpCon Version**: The version of AmpCon-DC that you use.

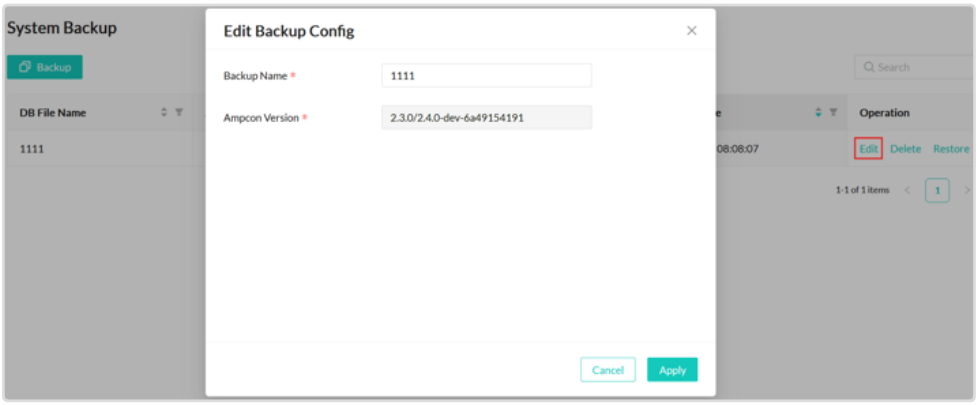


4. Click **Apply**.

Optional: Editing a Database Backup

To edit a database backup, follow these steps:

1. Log in to the AmpCon-DC UI, and click **Maintain > System Backup**.
2. Locate the backup, and click **Edit** on the right.
3. In the **Edit Backup Config** pop-up window, modify the backup name or AmpCon-DC version as you need.

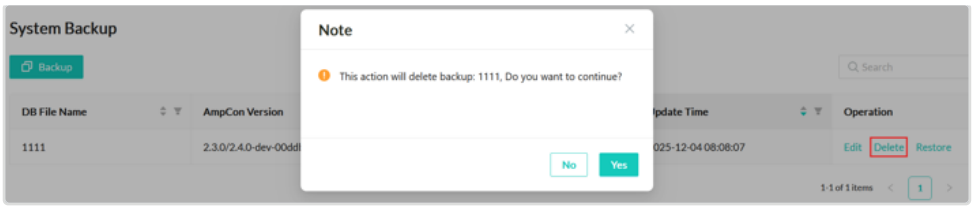


4. Click **Apply**.

Optional: Removing a Database Backup

To remove a database backup, follow these steps:

1. Log in to the AmpCon-DC UI, and click **Maintain > System Backup**.
2. Select the backup, and click **Delete** on the right.
3. Click **Yes** to confirm the removal.


System Backup
Backup
Search
DB File Name
AmpCon Version
Update Time
Operation
1111
2.3.0/2.4.0-dev-00dd
025-12-04 08:08:07
Edit
Delete
Restore
1-1 of 1 items
1
Note
This action will delete backup: 1111, Do you want to continue?
No
Yes

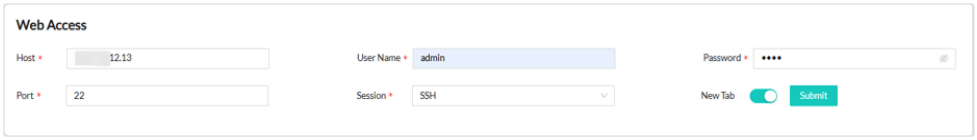
Accessing Devices through SSH Sessions

You can connect to a device (such as a switch or terminal device) from the AmpCon-DC UI by creating an SSH session.

Procedure

1. In the AmpCon-DC UI, click **Maintain > Web Access** from the navigation bar.
2. Input the following information:

- **Host:** The IP address of the device
- **User Name:** The username to log in to the device
- **Password:** The password of the user
- **Port:** The port to establish the session
- **Session:** Select **SSH**
- **New Tab:** Whether to open the session in a new browser tab



3. Click **Submit**.

Glossary

This glossary provides terms and definitions used on AmpCon-DC. If you have feedback about how this glossary works, or have terms you'd like to see defined, let us know by adding a comment to this document.

Click one of the following letters to locate the terms and definitions starting with the letter.

[A] [B] [D] [E] [F] [G] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

A

Alert

The event indicating a device failure or a performance shift.

Alert Level

The alert severity level. Alert levels include Error, Warning, and Info.

Alert Type

The type of each alert. Alert types include Packet Loss Alert, Resource Usage Alert, Interface Monitoring Alert, and Optical Module Alert.

Alert Notification

The method to receive real-time email notifications.

AmpCon-DC License

The authorization license for managing PicOS through AmpCon-DC.

Each AmpCon-DC license contains Hardware IDs and expiration dates of PicOS switches to be managed by AmpCon-DC. The AmpCon-DC license needs to be imported to AmpCon-DC.

Ansible

The open-source tool to automate configuration management, application deployment, and task automation.

Ansible Playbook

The simple, declarative language (written in YAML) used to automate your tasks.

You declare the desired state of a local or remote system in your playbook. Ansible ensures that the system remains in that state.

Ansible Job

The single execution of an Ansible playbook.

Address Resolution Protocol (ARP)

The Internet protocol used to map an IP address to a Media Access Control (MAC) address. It allows hosts and switches to determine the data link layer addresses through the ARP Request and ARP Response process.

Autonomous System (AS)

A collection of networks that are uniformly controlled by one or more management authorities and adopt the same routing strategy.

Each AS is assigned a globally unique 16-bit number, known as the Autonomous System Number (ASN).

B

Bare Metal (BM)

The server without any operating system, application, or virtual machine installed.

Bare Metal Node Group

The logical collection of bare metal node devices that are grouped together based on shared uplink configurations.

Bridge Domain (BD)

The Layer 2 broadcast domain in which data packets are forwarded on a VXLAN network. BD is also called large Layer 2 domain.

In a traditional network, VLANs are identified by VLAN IDs. Similarly, in a VXLAN network, BDs are identified by VXLAN Network Identifiers (VNIs).

Border Gateway Protocol (BGP)

The routing protocol used to connect independent systems on the Internet. It is designed by the Internet Engineering Task Force (IETF) as a robust, scalable, and well-defined protocol for exchanging routing information among BGP routers within a single AS (IBGP) or among different AS (EBGP).

- External Border Gateway Protocol (EBGP): The routing protocol used to exchange routing information among different AS.

- Internal Border Gateway Protocol (IBGP): The routing protocol used to exchange routing information within a single AS.

D

Database (DB)

A collection of structured data stored in computers and managed through the Database Management System (DBMS).

AmpCon-DC stores its data in the AmpCon-DC database.

Decommission (DECOM)

The method to revoke the PicOS license and configurations from a switch. The decommissioned switch will not be managed by AmpCon-DC.

Dynamic Host Configuration Protocol (DHCP)

The network protocol used for automatically assigning IP addresses and related network configuration parameters.

DHCP Server

The system that dynamically assigns information such as IP addresses, subnet masks, default gateways, and DNS servers to devices like switches.

Dynamic Load Balancing (DLB)

The network management technique used to distribute network traffic across multiple paths or resources dynamically.

Unlike static load balancing, which assigns fixed routes or resources to handle traffic, dynamic load balancing adjusts traffic distribution in real time based on current network conditions. Three modes of Dynamic load balancing are supported: Normal Mode, Optimal Mode, and Assigned Mode.

E

Easy ECN

The solution that simplifies the traditionally complex configuration of ECN through a single command.

Encrypt Key

The key generated to encrypt sensitive data in the AmpCon-DC database.

Then, plain text like password and sensitive TACACS+ keys is not shown in the AmpCon-DC UI.

Ethernet Virtual Private Network (EVPN)

The next-generation VPN solution that introduces a control plane to better control the MAC address learning process.

Explicit Congestion Notification (ECN)

The network protocol that allows end-to-end notification of network congestion without dropping packets.

When congestion occurs, PicOS switches mark packets by using ECN. Upon receiving an ECN-marked packet, the receiving end detects the ECN flag, identifies the congestion, and sends a Congestion Notification Packet (CNP) back to the sender. Then, the sender is informed of the congestion and will reduce the packet sending rate to prevent further congestion escalation.

F

Fabric

The logistic representation of an actual physical network. You can deploy a physical network by designing a fabric in the AmpCon-DC UI.

A fabric is based on a template. A template contains one or multiple units.

G

Global User

The AmpCon-DC user that is not limited to any switch group. A global user can manage all PicOS switches.

Group User

The AmpCon-DC user that can manage PicOS switches in one or multiple switch groups.

L

Leaf Switch

The access node on a VXLAN fabric, which connects various network devices to the VXLAN network.

Logical Network

The core of overlay service provisioning. Like physical networks used for underlay provisioning, logical networks are logical space to provision overlay services.

A logical network holds other logical network elements, including logical routers, logical switches, and virtual networks, to instantiate an overlay service network.

Logical Router

The Layer 3 distributed routing network element that connects logical switches and virtual routers.

Similar to Layer 3 Virtual Network Instance (L3 VNI), logical routers are designed to enable Layer 3 communication across VLAN Domains and manage the pushing of VRF configurations.

Logical Switch

The Layer 2 network element that connects resources (such as physical servers and virtual machines) within the same service system.

Logical switches exist only on server leaf switches and handle configuration pushing of gateway interfaces, Network Virtualization Edge (NVE), and Bridge Domain (BD).

Lossless Network

The network with high-throughput and low-latency data transmission over Ethernet.

By leveraging the RDMA over Converged Ethernet (RoCE) technology, lossless networks provide significant advantages for high-demand applications in modern data centers, high-performance computing (HPC) environments, and cloud services.

M

Media Access Control (MAC) Address

The physical address that uniquely identifies a network device on a local area network (LAN).

MD5 File

The file used to verify the completeness of another file. For example, a PicOS image MD5 file is used to verify the completeness of the related PicOS image file.

Mgmt IP

The management IP address of the switch. Mgmt IP is used to connect to AmpCon-DC.

MP-BGP EVPN

Ethernet Virtual Private Network (EVPN) based on Multi-protocol Extensions for Border Gateway Protocol (MP-BGP).

- EVPN is a next-generation VPN solution that introduces a control plane to better control the MAC address learning process.
- MP-BGP is leveraged to distribute MAC information.
- MP-BGP EVPN facilitates efficient MAC address learning and synchronization across the network.

Multi-Chassis Link Aggregation (MLAG)

The technology used to implement link aggregation among multiple devices.

AmpCon-DC supports using MLAG on leaf switches. Two leaf switches set up an MLAG through peer links.

Multi-Rail Access

The network architecture design where each network interface card (NIC) of a single node device is connected to a different leaf switch, instead of being aggregated into a single switch.

Multi-rail access allows parallel communication paths to enhance bandwidth utilization and fault tolerance.

N

Normal ZTP

The Zero Touch Provisioning (ZTP) method used to onboard switches. If the switches to be managed don't have PicOS installed, or though the switches have PicOS installed but you want to use a ZTP method to onboard these switches to AmpCon-DC, you can deploy these switches through normal ZTP.

Notification Rule

The rule that AmpCon-DC uses for sending alert email notifications.

In a notification rule, specify alert types, alert levels, and fabrics to be monitored. Then, you will receive email notifications when these specified conditions are met.

Notification History

The historical alert notifications sent in the last 30 days.

O

Open Shortest Path First (OSPF)

The dynamic interior gateway protocol that uses link-state information to build and maintain a complete and consistent map of the network topology within an AS.

It employs the Dijkstra algorithm to calculate the shortest path tree from each router to all the other routers in the AS, based on which routing tables are built.

OpenStack

The open-source cloud computing management platform that provides diverse components for computing, storage, networking, mirroring, and other services.

- OpenStack supports almost all types of cloud environments and provides a cloud computing management platform that supports easy implementation, large-scale expansion, and unified standards.
- OpenStack uses various components to control and manage resources, virtualize computing, network, storage, and pool resources. OpenStack also uses components to implement resource collaboration.

Optical Module

The network device used for optoelectronic conversion in high-speed communication.

- At the transmitting end, optical modules convert electrical signals into optical signals for transmission through optical fiber.
- At the receiving end, optical modules re-convert the optical signals back into electrical signals.

Overlay Network

A virtual network built on top of the underlay network. It allows for creation of logical, software-based networks that can span the entire physical network.

- The underlay network refers to the physical infrastructure and protocols that make data transmission possible.
- The overlay network is a virtual, software-defined layer that sits on top of the underlay network, allowing for advanced network functionalities and easier management.

Overlay Data Plane

Manages creation, maintenance, and tear-down of overlay networks.

The control plane ensures efficient communication between endpoints, handles network virtualization, and supports advanced features like multi-tenancy, workload mobility, and scalability.

Overlay Network Control Plane

Responsible for actual forwarding of traffic within an overlay network, such as the following activities:

- Packet encapsulation
- Packet decapsulation
- Traffic forwarding
- Secure transmission of data
- Prioritizing certain types of traffic by using QoS policies
- Distributing traffic across multiple paths in the underlay network by using mechanisms like Equal-Cost Multi-Path (ECMP)

Overlay Service

The virtualized network function or logical layer that enables logical network isolation and flexible service deployment and network configurations without modifying the underlying infrastructure.

By using AmpCon-DC, overlay service configurations can be abstracted into logical network elements, including logical networks, logical routers, logical switches, and virtual networks. You can push overlay service configurations by provisioning these logical network elements.

P

Parking Lot

The panel containing all the PicOS switches in Parking status.

If you provision a PicOS switch without adding a switch configuration beforehand, the switch will be in Parking status and listed in the parking lot.

PicOS License

The authorization license for using functions of PicOS.

PicOS Switch

The switch with PicOS installed.

Power over Ethernet (PoE) Device

The technology that provides both data connection and electric power to devices such as wireless access points and IP cameras.

PoE devices are the systems that can pass electric power along with data on twisted pair Ethernet cabling.

Priority Flow Control (PFC)

The network protocol designed to manage congestion on Ethernet networks by allowing for independent pausing of traffic based on priority levels.

PFC Buffer

The buffer configured to implement traffic control and PFC watchdog, which is based on interface and priority queue.

The storage space of each interface is divided into different buffers independently. A certain action will be executed after the number of accumulated packets reaches the buffer threshold (the unit is cell).

PFC Deadlock Prevention

The technology used to identify RoCE flows that are prone to triggering deadlocks.

It prevents the generation of circular wait conditions and ensures the smooth operation of high-priority traffic.

PFC Watchdog

The critical component in Ethernet networks that uses PFC to manage congestion.

By detecting and mitigating PFC deadlocks, it ensures that the network remains stable and performs optimally.

Point of Delivery (PoD)

The minimum service unit of a data center. It's a collection of resources in a data center.

PoDs include three types: bare metal PoD, vSphere PoD, and OpenStack PoD.

Q

Quality of Service (QoS)

The network mechanism used to manage and ensure different levels of quality and performance for different types of traffic in a network.

QoS aims to control the transmission priority of data packets through network devices, protocols, and mechanisms, thereby ensuring priority processing for critical tasks and reducing issues such as latency, packet loss, and jitter.

R

RDMA over Converged Ethernet (RoCE)

The technology to reduce CPU workloads by providing direct memory access for applications that bypass the CPU.

Because packet processing and memory access are handled by the network interface card (NIC) and network switch rather than the CPU, RoCE allows for higher throughput, lower latency, and reduced CPU utilization for both the sender and receiver.

Resource Pool

The centralized collection of resources that are managed and allocated dynamically.

AmpCon-DC automatically pulls and assigns IP addresses and Autonomous System Numbers (ASNs) from the resource pools that you specified.

Resource pools include IP pools, ASN pools, and VNI pools.

Return Merchandise Authorization (RMA)

The method to replace a switch with another switch of the same switch model.

When the hardware of a switch fails and is replaced with a new switch, you can RMA to take the configurations from the failed switch, install or upgrade PicOS, update the serial number of the new switch, and push the configurations to the new switch to seamlessly manage it with AmpCon-DC.

Role

The method to define the permissions that determine which pages and tabs a user can access (Read or Write). A user must be assigned at least one role to log in to the AmpCon-DC UI.

Route

The path that network traffic takes from the source to the destination. Routes can change dynamically.

RoCE EasyDeploy

The feature to simplify the deployment and configuration of RDMA over Converged Ethernet (RoCE) on switches.

By using this feature, you can easily select and switch the RoCE mode between lossless and lossy modes, ensuring the best performance for different network environments.

RoCE Policy

The feature to push RoCE configurations to switches through customized policies that adapt to real-time network conditions and traffic patterns.

S

Site

The site to which PicOS switches and APs belong.

Simple Mail Transfer Protocol (SMTP)

The TCP/IP protocol used to send and receive emails. SMTP specifies how two systems work with each other to transmit and receive emails and defines the formats of messages that are exchanged.

Simplified ZTP

The Zero Touch Provisioning (ZTP) method used to onboard switches, deploy physical networks, and configure RoCE (optional) in one go.

Single-Track Access

The network architecture where all network interface cards (NICs) of a node device are aggregated into a single leaf switch, forming a centralized communication path.

SMTP Server

The specialized application responsible for sending, relaying, and routing email messages between senders and recipients over the Internet or a network.

Spine Switch

The core node on a VXLAN fabric, which provides high-speed IP forwarding and connects to leaf switches through high-speed interfaces.

SSH Session

The secure, encrypted connection established between a client and a server for remote login, command execution, or file transfer.

Subnet Mask

The binary pattern used by the IP protocol to determine the destination network segment of packets.

Switch Group

The group to which PicOS switches belong.

Syslog Server

The centralized system that collects, stores, and manages system log messages generated by network devices, servers, and applications through the Syslog protocol.

T

Terminal Access Controller Access-Control System Plus (TACACS+)

The enhanced security protocol that provides centralized Authentication, Authorization, and Accounting services.

In addition to using local AmpCon-DC users (global users or group users), you can also enable the TACACS+ integration to manage user access.

Telemetry

The technology used to automatically collect real-time or historical metric data from managed switches.

Template

The abstraction of network design that defines the relationship of leaf switches and spine switches and underlay and overlay protocols, without defining any vendor-specific information. A template contains one or multiple units.

In a template, you can specify the spine switch count, included units and their counts, and underlay and overlay protocol related configurations.

Tenant

A logical resource unit used to deploy logical networks for overlay service provisioning. Each tenant can manage its own logical networks. Logical networks owned by different tenants are isolated from each other, ensuring that network resources of one tenant do not affect others.

Terminal

The terminal device connected to a wired network or wireless network. Terminals might be a laptop, smartphone, tablet, smart-home device, or others.

Topology

The network arrangement formed by switch connections on a local area network (LAN) or among multiple LANs.

You can visualize your switches in all locations and drill down into an individual switch, right to the port level, to check port stats and overall health of the switch.

U

Underlay Network

The physical infrastructure that transports the actual network traffic.

It is the foundational layer of your network that includes all the hardware and protocols needed for data transmission.

Unit

The minimum networking unit for creating a fabric. A unit includes one or multiple leaf switches.

In a unit, you can specify details like the leaf switch count and whether to use the MLAG leaf strategy.

User Interface (UI)

The interaction interface between users and a digital product.

A UI includes all the visual and interactive elements that users see and interact with, such as buttons, icons, menus, and layouts.

V

Virtual Extensible Local Area Network (VXLAN)

The overlay network virtualization technology that enables creation of virtual Layer 2 networks across Layer 3 network boundaries by encapsulating Layer 2 frames within Layer 3 UDP packets.

VXLAN extends the traditional VLAN technology, addresses the limitations of VLANs, such as the 4096-network limit, and meets the needs of large-scale, virtualized networks with multi-

tenant capabilities.

Virtual Network

The virtual Layer 2 network used in vSphere or bare metal Point of Delivery (PoD). The ports of virtual networks are attached to logical switches.

In vSphere, the virtual network is called portgroup; in bare metal, the virtual network is called Virtual Layer 2 Switching (VL2).

Virtual Routing and Forwarding (VRF)

The technology that allows multiple instances of a routing table to coexist within the same router at the same time.

It enables logical isolation between different networks on the same physical device. By using VRF, different instances can use the same IP address without conflicts.

VLAN Domain

The VLAN ID ranges of node devices connected to leaf switches. A VLAN Domain includes the Bridge Domain (BD) range and VRF VLAN range.

VPN IP

The IP address of the VPN tunnel established between the switch and AmpCon-DC. The following icons are used to indicate the tunnel status:

- ✓: The VPN tunnel between the switch and AmpCon-DC is available.
- x: The VPN tunnel between the switch and AmpCon-DC is unavailable.

vSphere

The virtualization platform released by VMware. ESXi and vCenter are important components of vSphere.

- ESXi is installed on physical servers to virtualize physical IT resources into virtual IT resource pools so that applications can be virtualized.
- vCenter is a virtualization resource management component for managing ESXi servers. vCenter provides strong and flexible VM management capabilities, simplifying virtual data center management.

VXLAN Tunnel End Point (VTEP)

The network entity that serves as the termination point for a VXLAN tunnel.

It is responsible for encapsulating Layer 2 frames into VXLAN packets for transmission over a Layer 3 network and for decapsulating VXLAN packets back into Layer 2 frames upon receipt.

W

Weighted Random Early Detection (WRED)

The active queue management (AQM) mechanism that selectively drops packets based on the average queue length, helping manage congestion before the queue becomes full.

When combined with ECN, WRED can mark packets instead of dropping them when congestion is detected.

Z

Zero Touch Provisioning (ZTP)

The technology for automated deployment and configuration of network devices. AmpCon-DC supports using ZTP to deploy PicOS switches.