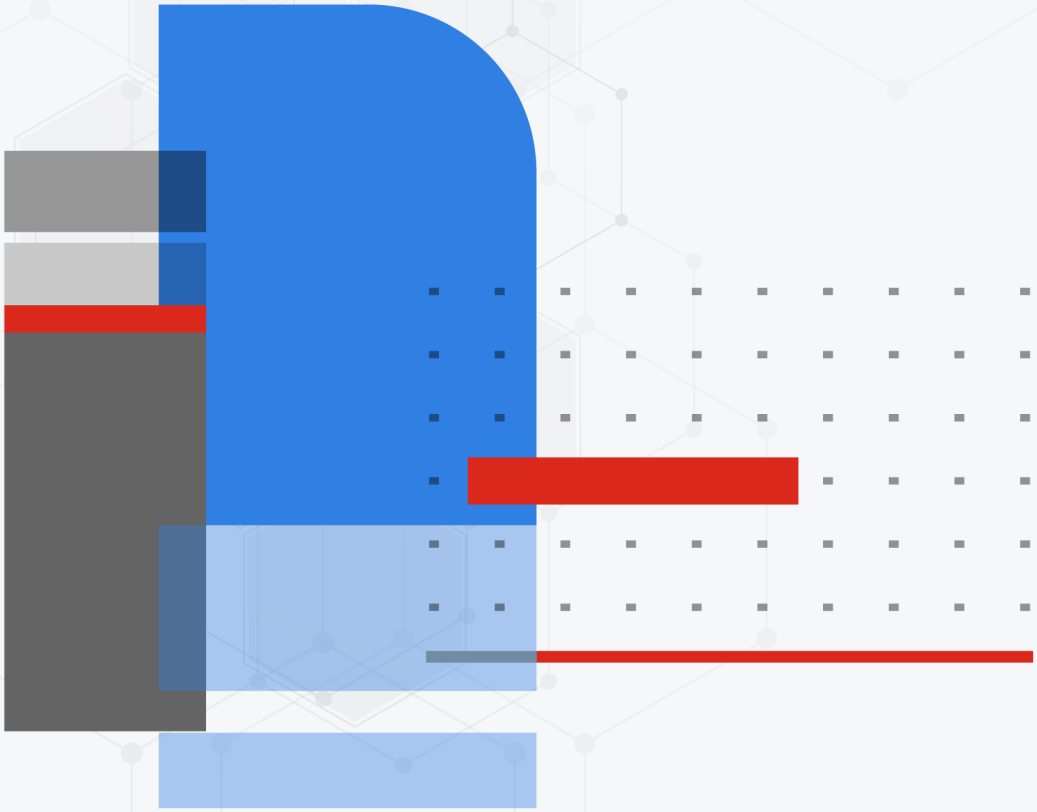
User Guide

FortiLAN Cloud 24.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 08, 2024
FortiLAN Cloud 24.1 User Guide
53-241-567276-20240308

TABLE OF CONTENTS

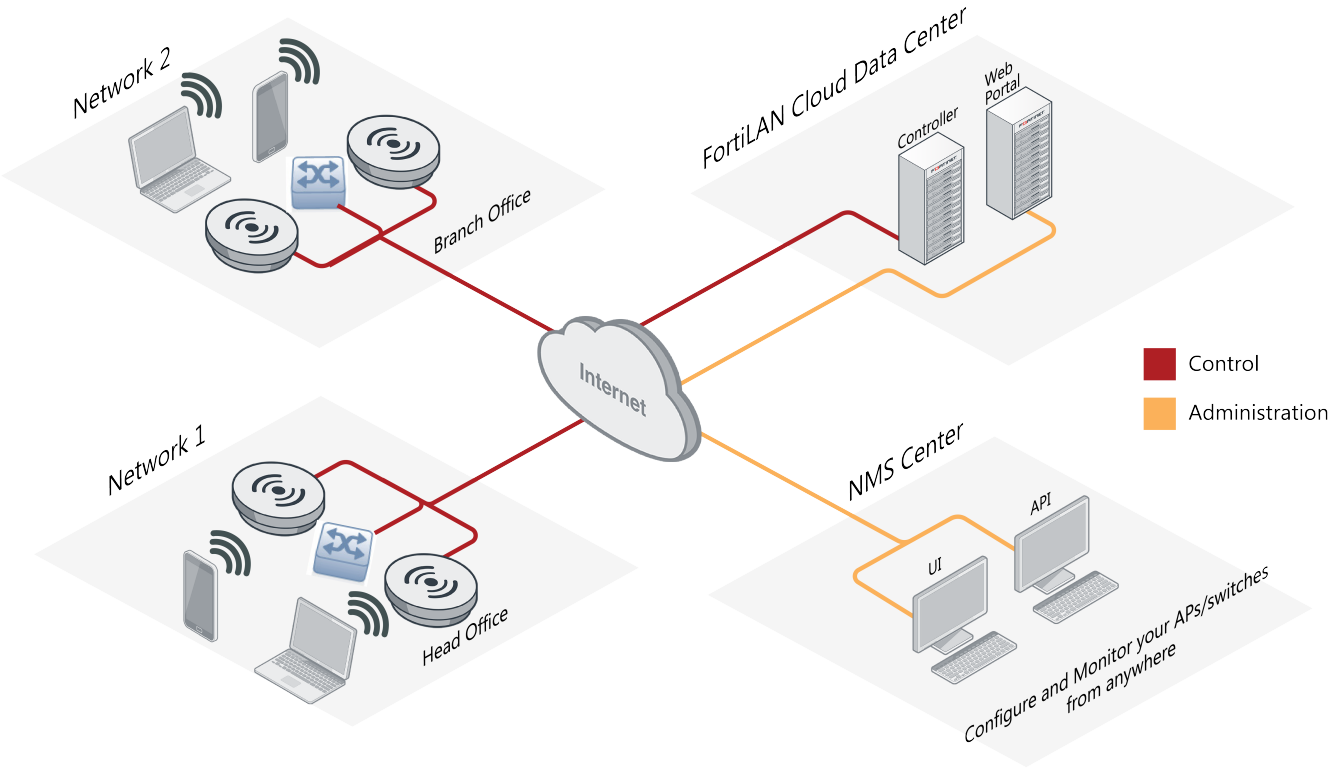
Change log

Date	Change description
2023-03-08	FortiLAN Cloud 24.1 release document.

Introduction

FortiLAN Cloud is a unified management platform for standalone FortiAP and FortiSwitch deployments. FortiLAN Cloud provides configuration management and monitoring control for a handful of devices and can scale up to thousands of devices across multiple sites.

The following image shows the FortiLAN Cloud overview including the network management system (NMS) and administration communications.



- Key Concepts on page 8
- User Interface Overview on page 10
- Network Summary Dashboard on page 58
- Service Offerings on page 16

Key Concepts

This section describes the key concepts related to using FortiLAN Cloud.

- FortiAP
- FortiSwitch
- REST API

FortiAP

FortiLAN Cloud centralizes the life-cycle management of your standalone FortiAP deployment with a simple, intuitive, and easy-to-use cloud interface that is accessible from anywhere at any time. With FortiLAN Cloud, you can deploy, configure, and manage your FortiAP devices. FortiLAN Cloud also offers enhanced visibility, monitoring, reporting, and analytics features for your FortiAP devices. FortiLAN Cloud also supports the FortiAP-S and FortiAP-U series which combine the elements of universal threat protection (UTP) protection at the network edge.

If you are interested in cloud management of FortiAP devices that are already connected to FortiGate devices, then use FortiGate Cloud, not FortiLAN Cloud.

FortiSwitch

FortiLAN Cloud provides management as a service (MaaS) for secure switching infrastructure deployed with FortiSwitch devices. It provides a centralized discovery, visibility, and configuration management solution without the need of on-premise hardware, software, or management overhead. FortiLAN Cloud manages FortiSwitch devices in standalone mode.

REST API

REST (REpresentational State Transfer) is a modern, scalable (but not high performance) client-server based RPC technique using existing HTTP protocol methods (such as GET, POST, PUT, DELETE) on server resources (identified by URLs) and transferring the resources in either XML / JSON / HTML representation. FortiLAN Cloud REST API provides functions similar to its GUI functions, both configuration and monitoring are supported over REST API. The FortiLAN Cloud REST APIs are integrated with FortiCloud IAM users, you can use REST APIs as a local user or an IAM user.

FortiLAN Cloud Account Inventory

The FortiAP device deployment and registration is supported via the FortiLAN Cloud GUI, REST APIs, and FortiCloud account inventory (https://support.fortinet.com/). FortiLAN Cloud periodically synchronizes the FortiAPs with FortiCloud, to import registered devices and remove un-registered devices. The FortiAPs registered in your account in FortiCloud automatically appear in the **Inventory Devices** tab.

Note: If an account has no FortiAP device in any FortiLAN Cloud domain, then manual synchronization is required at least once. Click the refresh icon at top right corner of the **Devices** page.

FortiLAN Cloud SKUs

For license ordering details such as stock keeping unit (SKU) codes, see the FortiLAN Cloud Data Sheet.

FortiAP-S and F-Series or later FortiAP-U family access points communicate with FortiCare/FortiGuard service to get UTP updates (for AV, IPS engine and database) when its FortiGuard subscription is valid.

Regions

Data centers are located in Canada, Germany, Japan, and the US for better performance and GDPR compliance for international customers. FortiLAN Cloud includes the Global, Europe, US, and Japan regions.

You can migrate FortiSwitch data from Canada to the Europe or Japan data centers (existing FortiSwitch data is stored in the Canada data center.) All new activations of FortiLAN Cloud in Europe and Japan, will have data in the Europe and Japan data centers, respectively. When you log into the FortiLAN Cloud GUI, you are prompted to request migration, click **Request for Migration**. A notification email is sent before the actual data migration is performed.

Languages

FortiLAN Cloud supports the user interface in *English*, *Japanese*, *Spanish*, and *Portuguese* languages.

- If the browser language is one of the supported languages and is different from the configured account language, then the user interface is available in the browser language. For example, if the account is configured to use Spanish but the browser language is English, then the user interface is available in English.
- If the browser language is NOT one of the supported languages, then the user interface is available in the account configured language. For example, if the account is configured to use Spanish but the browser language is Mandarin, then the user interface is available in Spanish.

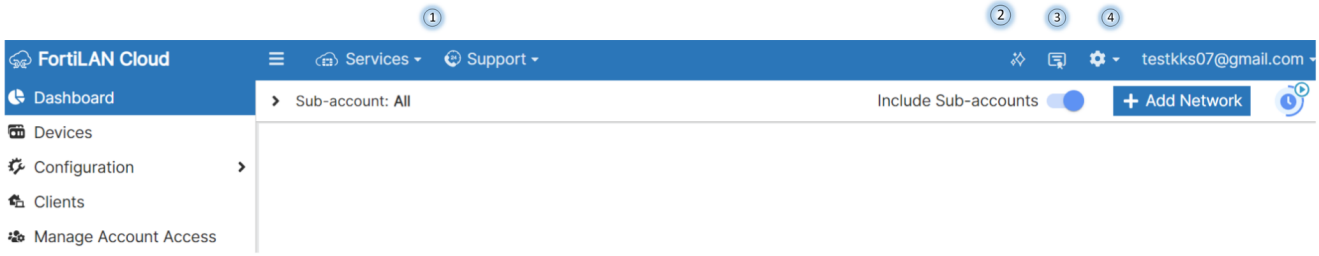
Network Port Numbers

The following table lists the network port numbers used by FortiLAN Cloud.

Purpose	Protocol	Port number
Customer UI and API access	HTTPS	TCP/443
FortiAP initial discovery	HTTPS	TCP/443
FortiAP CAPWAP (configuration, event logs, and statistics)	CAPWAP	UDP/5246, UDP/5247
FortiAP UTP logs	—	TCP/514
FortiAP firmware download	HTTPS	TCP/8443
FortiAP FortiGuard services (FortiAP-S/FortAP-U series)	—	UDP/53, UDP/8888
FortiAP to FortiPresence	—	UDP/4013
FortiSwitch	—	TCP/443

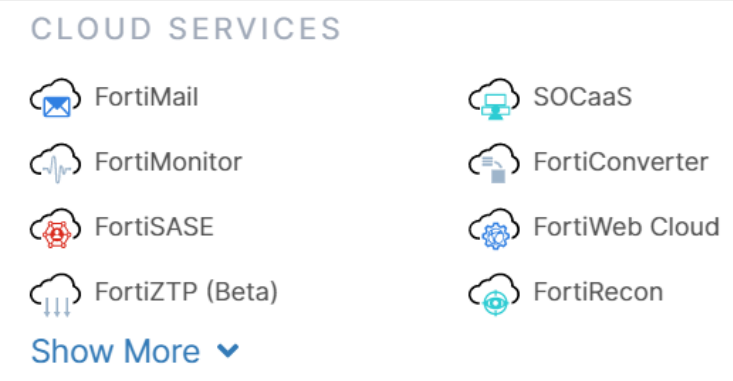
User Interface Overview

The FortiLAN Cloud GUI is segregated into different sections and pages enabling you to perform configuration and management operations at the FortiLAN Cloud level, network level, and device level.



1

The **Services** menu accessible via the FortiLAN Cloud application provides access to various Fortinet cloud-based services. It includes the **Show More** and **Show Less** options to expand and collapse the list of services respectively.



The **Support** menu, provides the **Resources** section with some useful links aiding product usage and the **Downloads** section for access to installation files and updates.

2

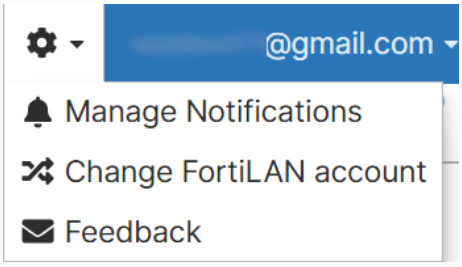
To view what's new in the current release, click **FortiLAN Cloud Feature Reference**.

3

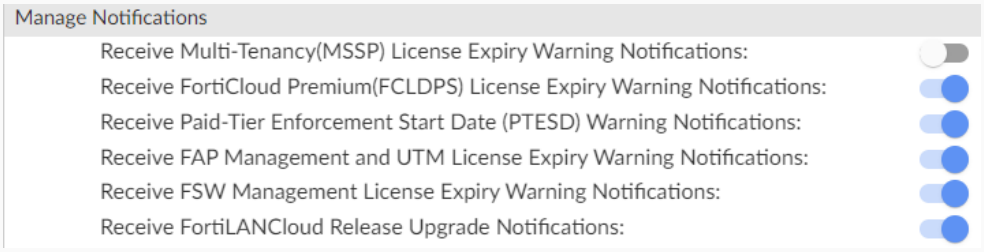
To view the license status, click **License Status**.

4

To access the following additional options, click *Settings.*

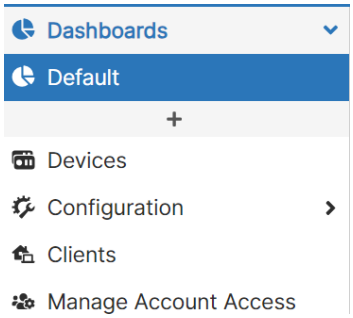


- To manage (enable/disable) email alert preferences for specific notifications for your account, click **Manage Notifications**.



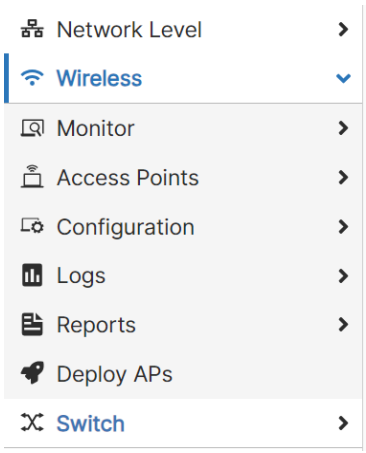
- To switch to a different account, select **Change FortiLAN Account**.
- To send feedback to the FortiLAN Cloud team, select **Feedback**.

The navigation menu on the left side provides an overview of the network and enables various federated/centralized configurations. For more information, see Configuring and Managing FortiLAN Cloud.

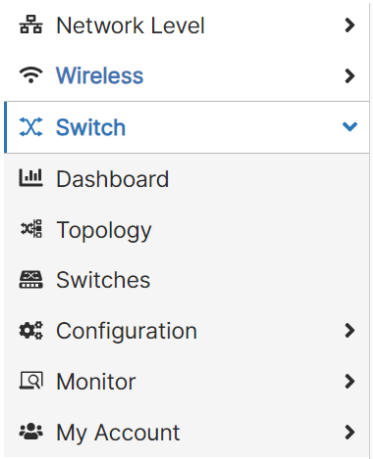


After you select a network, you are navigated to the main configuration menu for the network and the devices (FortiAPs and FortiSwitches). The network level menu allows you to monitor the network statistics and configure unified device tags for a network. For more information, see Network Level Configuration.

The wireless menu allows you to configure, monitor, and manage FortiAP devices in your networks For more information on managing the FortiAP devices, see Configuring and Managing FortiAPs on page 60.

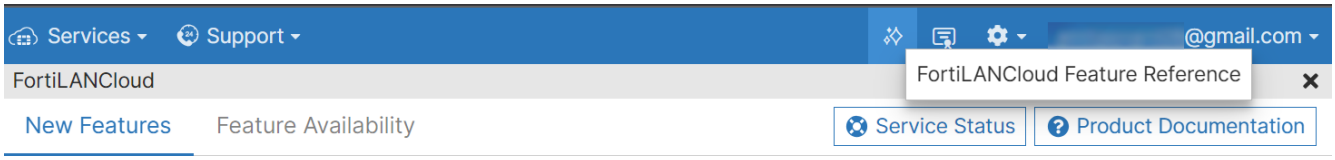


The switch menu allows you to configure, monitor, and manage FortiSwitch devices in your networks For more information on managing the FortiSwitch devices, see Configuring and Managing FortiSwitches on page 153.

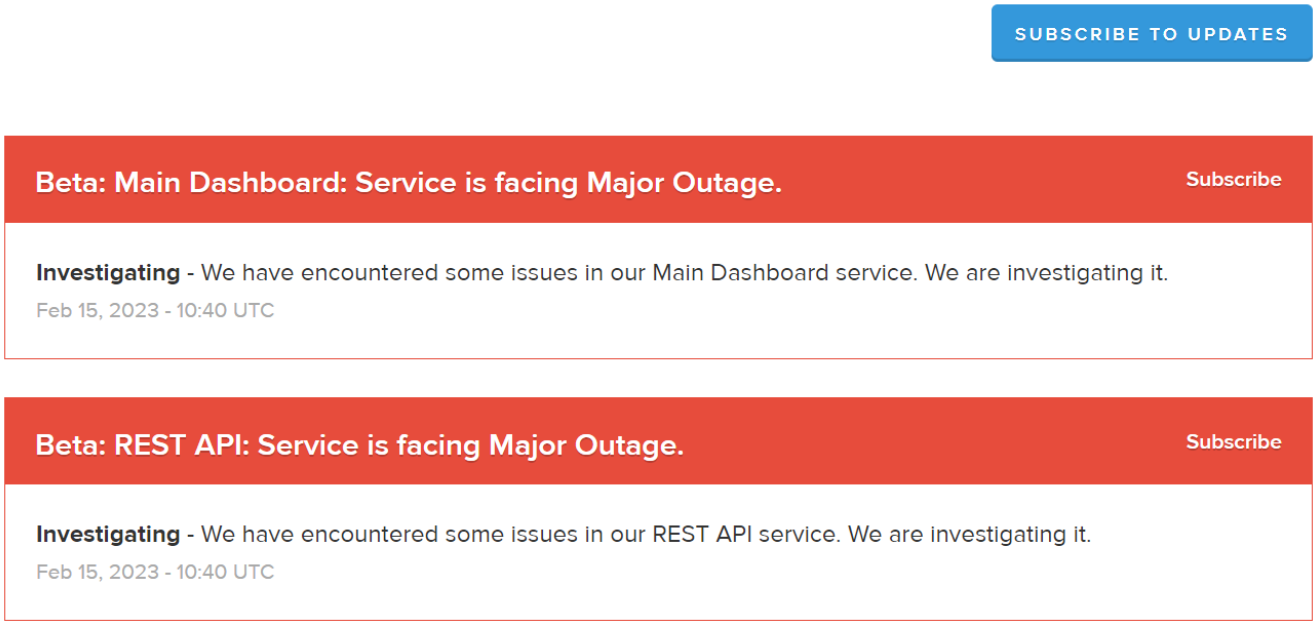


Monitoring Service Status

This service status page provides an overview of the current and historical availability of the FortiLAN Cloud service, with visibility into the monitoring infrastructure. You can receive and track notifications for incidents and downtime affecting the FortiLAN Cloud GUI and REST APIs. Navigate to **FortiLAN Cloud Feature Reference** and click **Service Status**.



This page displays the real-time and historical incidents affecting the FortiLAN Cloud service. The real-time events affecting the infrastructure and usage of the service are displayed on the top of the page. The historical incidents indicate the past events. Click **Subscribe To Updates** to receive notifications.



The FortiLAN Cloud service uptime is displayed graphically for a period of 90 days. The downtime/outage events experienced by the service are indicated in colored bars; hover over each bar to view the details. Click **View historical uptime** to view the uptime/downtime experienced by the service in the past.

Subscribing to FortiLAN Cloud

This section describes the licensing options available for deploying and using FortiLAN Cloud, and the service offerings by FortiSwitches and FortiAPs.

Licensing

FortiLAN Cloud offers the following licensing options for product subscriptions. For more information about acquiring licenses, contact the *Fortinet Customer Support* team.

Subscription	Description
Freemium	Free subscription for FortiLAN Cloud.
Device License	A license is bound to each device (FortiAP/FortiSwitch).
Account License	A license is bound to the FortiLAN Cloud account.

A FortiLAN Cloud **Freemium Account** license allows deploying a maximum of 30 unlicensed FortiAPs and 3 FortiSwitches across networks with basic management functions. You cannot deploy any more unlicensed devices or create/modify networks, and any additional devices (deployed beyond the permissible limit) are un-deployed. Click on the  (warning) icon to view the grace period details and the network/devices in the grace period. An additional 60 days grace period is given to any device with a valid license that is expiring. After the grace period, the system randomly retains (up to) a maximum of 30 freemium FortiAPs and 3 freemium FortiSwitches. Any other FortiAPs/FortiSwitches will not be able to connect to the service but can retain their configuration.

For advanced management, you must purchase a license for each FortiAP and FortiSwitch device, see the FortiLAN Cloud Data Sheet.

Note: FortiAP-U models require an additional license for the Universal Threat Protection feature. You are required to purchase this license in addition to the advanced management license.

Device/Service	Freemium/Unlicensed	Device License
Number of FortiAPs	30	Unlimited
Number of FortiSwitches	3	Unlimited
Number of Networks	3	+1 per deployed/claimed FortiAP or per deployed/claimed FortiSwitch
Number of Sites	3	+1 per deployed FortiAP or FortiSwitch
Device Management	Basic	Advanced

Device/Service	Freemium/Unlicensed	Device License
Log retention duration	7 days	1 year
Customer support (24x7 FortiCare)	No	Yes

Additional Networks

- 1 licensed FortiAP (deployed/claimed) allows creating 1 additional network.
- 1 licensed FortiSwitch (deployed/claimed) allows creating 1 additional network.

Additional Sites

- 1 licensed FortiAP/ FortiSwitch deployed in the network allows creating 1 additional site.

The *Combined Default* network is not counted for license enforcement.

Note: Regular email notifications are sent with details of your FortiLAN Cloud subscription tenure and the associated services and offerings. You can manage notifications from the home page, see User Interface Overview on page 10.

Service Offerings

This section lists the features available based on your subscription.

- FortiAP
- FortiSwitch

FortiAP

The following table includes details about **FortiAP** service offerings.

FortiAP service	Freemium	Licensed
Basic FortiAP management	Yes	Yes
Advanced FortiAP management		
SSID • Blocking intra-SSID traffic • Broadcast Suppression • DHCP Option 82 • Fast BSS Transition (802.11r) • Radio Sensitivity (Rx-SOP) • Probe Response Suppression • Sticky Clients Removal • Protected Management Frames (802.11w) • 802.11k and 802.11v • L3 Firewall Profile • Assigning dynamic VLAN	No	Yes

FortiAP service	Freemium	Licensed
• MPSK • MPSK Scheduling		
Platform Profile • Airtime Fairness • AP Scan Threshold • Automatic AP Upgrade upon Connect • Beacon Interval (ms) • DTIM Period • BLE Profile • Configuring Bonjour Relay • Console Login (Platform Profile) • Customizing data rates • DARRP Configuration • Disabling unwanted data rates • Disconnection Reports • DRMA • Duplicate SSID creation • TX Optimization • Energy Efficient Ethernet • 802.11d • MIMO mode setting	No	Yes
Tools • iPerf Bandwidth Test • Ping Test • TAC Report • Traceroute • Spectrum Analysis • VLAN Probe • AP CLI Access • ARP Table • FortiAP Link Health	No	Yes
Tunnel Profile • GRE/L2TP Tunnels	No	Yes
AP Management • Overriding radio profile parameters • Problematic Connection Steps (FortiAP status view - Summary)	No	Yes
QoS Profile • WMM	No	Yes
Scheduled Upgrade	No	Yes

FortiAP service	Freemium	Licensed
SNMP Management	No	Yes
WIDS	No	Yes
Syslog Server Configuration	No	Yes

FortiSwitch

The following table includes details about **FortiSwitch** service offerings.

FortiSwitch service	Freemium	Licensed
Basic FortiSwitch management	Yes	Yes
Monitoring • PoE Status • System Log • Audit Log • Event Log • Switch Statistics	Yes	Yes
Topology	No	Yes
Configuration • Zero Touch Configurations • Scheduled Upgrade • Configuration Backup/Restore • Ports • Interfaces • Trunk/Link Aggregation • VLANs • VLAN Templates • Packet Capture Profiles • Radius Authentication • TACACS Authentication • User Groups • Port Security	No	Yes
Monitoring • Zero Touch Config Status • Scheduled Upgrade Status • Modules • MAC Addresses • LLDP • STP • DHCP-Snooping • IGMP-Snooping • Packet Capture Files • 802.1x Status	No	Yes

FortiSwitch service	Freemium	Licensed
• 802.1x Session • Switch Port Statistics • Routing Table		

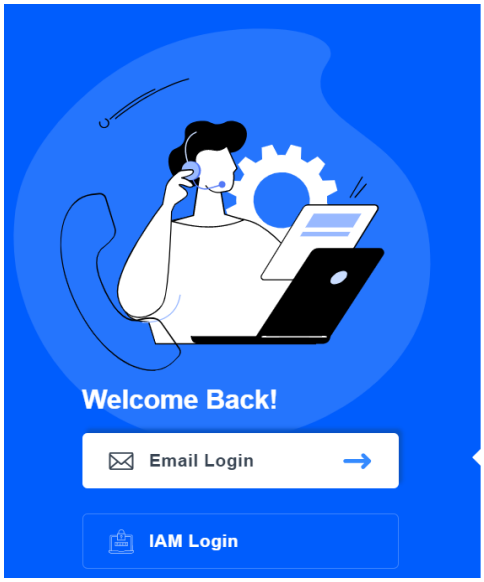
Signing-on for FortiLAN Cloud

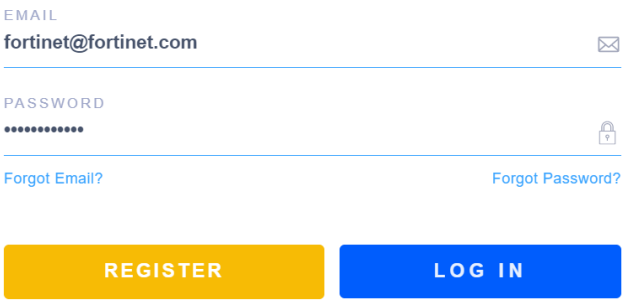
Access FortiLAN Cloud and other Fortinet Cloud services by using the FortiCloud single sign-on portal.

If you are...	Then go to
A new FortiCloud user	Registering on FortiCloud Accessing FortiLAN Cloud
An existing FortiCloud user	Accessing FortiLAN Cloud

Registering on FortiCloud

Prior to using FortiLAN Cloud, you are required to register on the *FortiCloud* portal. Use the https://support.fortinet.com access link to register on the *FortiCloud* portal. A security code is emailed to the address specified during registration; use the code to complete registration and activate your account.





Accessing FortiLAN Cloud

Any user registered on https://support.fortinet.com can access FortiLAN Cloud. Once you login into *FortiCloud*, click on **Services**, a banner with Fortinet products is displayed. Select **FortiLAN Cloud**. You are redirected to the FortiLAN Cloud GUI.

Domain	Purpose
Global	Used by customers worldwide except in Europe, Japan, and USA regions.
Europe	Used by customers in the Europe region.
Japan	Used by customers in Japan.
USA	Used by customers in the USA.

The following URLs can be used to access the various domains.

- **Global** - *https://fortilan.forticloud.com/*
- **Europe** - *https://eu.fortilan.forticloud.com/*
- **Japan** - *https://jp.fortilan.forticloud.com/*
- **USA** - *https://us.fortilan.forticloud.com/*

If you have enabled FortiToken two-factor authentication, then check your FortiToken Mobile application or email (as applicable), type the security code, and click **Go**.

You can login into FortiCloud using your registered FortiCloud account details, **Email** and **Password OR** click **Sign in as IAM user.** Enter your registered IAM user credentials to login, the **Account ID** is that of the master account. The FortiLAN Cloud Home page opens. For details, see the User Interface Overview on page 10.

Management Operations

This section describes the following operations on FortiLAN Cloud.

Managing Users and Accounts

FortiLAN Cloud can be accessed and managed by the following users.

- IAM users
- External IdP authenticated users
- Email users

Adding IAM Users

The Identity and Access Management (IAM) is a service to help you control access to FortiCloud portals and assets. You can use the portal to manage users, authentication credentials, and asset permissions. For more information, see **FortiCloud documentation**. Access the IAM service from the FortiCloud portal using the master FortiLAN Cloud account. To configure IAM users, see Adding IAM users.

External IdP Authentication

FortiLAN Cloud supports integration of third-party Identity Provider (IdP) services to log-in and manage networks. This feature is useful for enterprises that need to secure their user credentials and hence provision FortiLAN Cloud access through their own Identity Provider. The external IdP initiated Security Assertion Markup Language (SAML) assertion consisting of specific IdP attributes is used by FortiCloud/FortiLAN Cloud to verify the user account details and grant required access.

External IdP authentication is offered in conjunction with FortiCare and FortiAuthenticator. Contact the Fortinet *Customer Support* team to enable external IdP support and raise an enrollment request with the appropriate FortiCare accounts. After the enrollment is complete follow these setup procedures.

Note: Support for SAML 2.0 and IdP initiated assertion response is required.

- Create an IdP with SAML Service Provider Metadata. The following is an example where *company* is the unique name of your organization.
  ```
  SP Entity ID http://customersso1.fortinet.com/saml-idp/proxy/{company}/metadata/
  SP Login URL https://customersso1.fortinet.com/saml-idp/proxy/{company}/saml/?acs
  Relay State https://customersso1.fortinet.com/saml-idp/proxy/{company}/login/
  ```

- Configure the SAML assertions with the *username* and *role* attributes for permission control in FortiCloud.
- Provide specific information to Fortinet, such as, the SAML Metadata file, company name, contact information, and the Fortinet master account that the IdP requires to connect to.

Configure external IdP roles in FortiCloud to allow the required access to FortiLAN Cloud. See Adding External IdP Roles on page 23. After successful authentication on your Identity Provider, you are re-directed to the FortiCloud portal from where you access FortiLAN Cloud based on the configured roles.

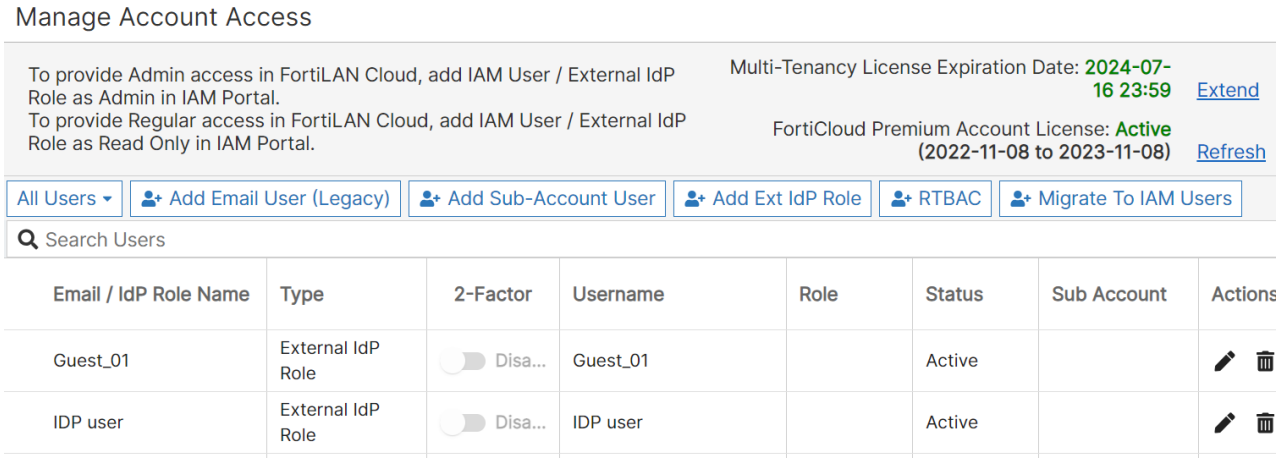
Adding External IdP Roles

Access the **Identity & Access Management** (IAM) service from the FortiCloud portal to add external IdP roles. See Adding external IdP roles.

Managing External IdP Roles

You can add and manage the external IdP roles from the FortiLAN Cloud GUI.

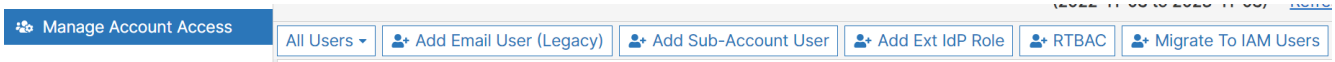
- All existing IdP roles are listed in the **Manage Account Access** page.

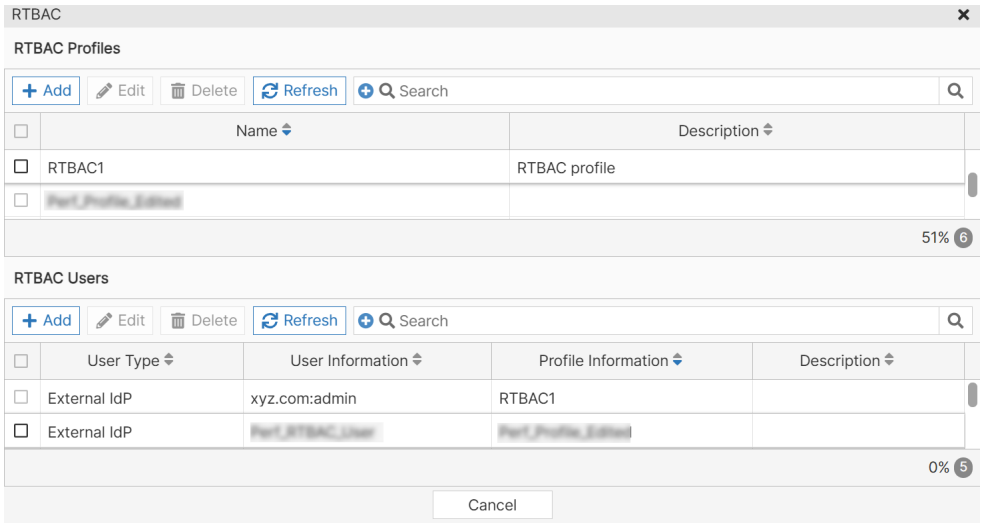


You can edit, create, and delete IdP roles from this page.

Resource/Task-Based Access Control (RTBAC)

FortiLAN Cloud supports RTBAC for specific resources and tasks. This can be applied in addition to the assigned role in FortiCare for an account. Click **RTBAC** in the **Manage Account Access** page to create/manage RTBAC profiles and users.



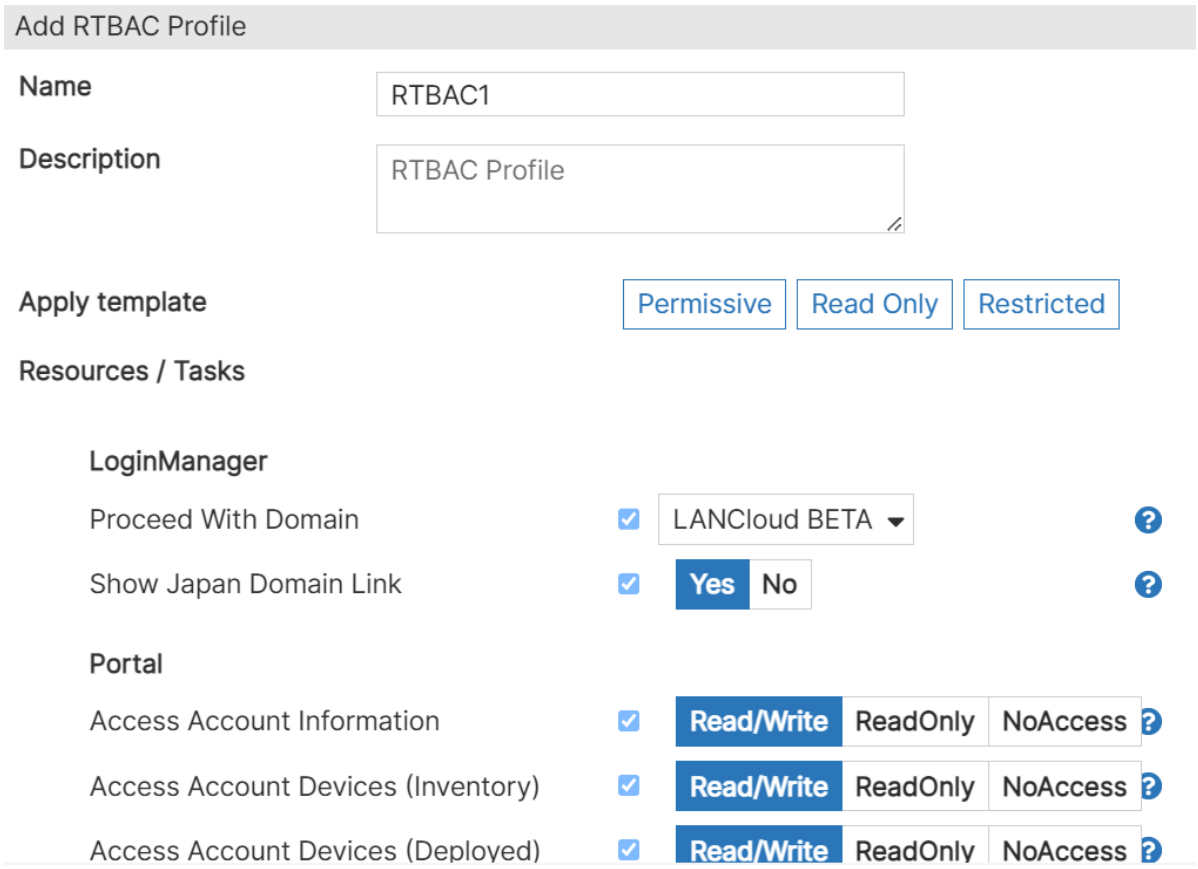


- RTBAC Profiles
- RTBAC Users

RTBAC Profiles

The RTBAC profile defines resources and their configured permissions. You can assign an RTBAC profile to one or multiple FortiLAN Cloud users, and every account can have multiple RTBAC profiles.

Configuration	Description
LoginManager	If you enable **Proceed With Domain** and select a domain, then the domain selection page is not displayed and the login proceeds with the selected domain.
Portal	Set access permissions for all **Resources/Tasks** (features) displayed.
Apply template	The permission level set resets all permissions set for the resources/tasks mentioned above. The following blanket permissions can be granted. • **Permissive** - Sets all resource permissions to Read/Write. • **Read Only** - Sets all resource permissions to ReadOnly. • **Restricted** - Sets all resource permissions to NoAccess.

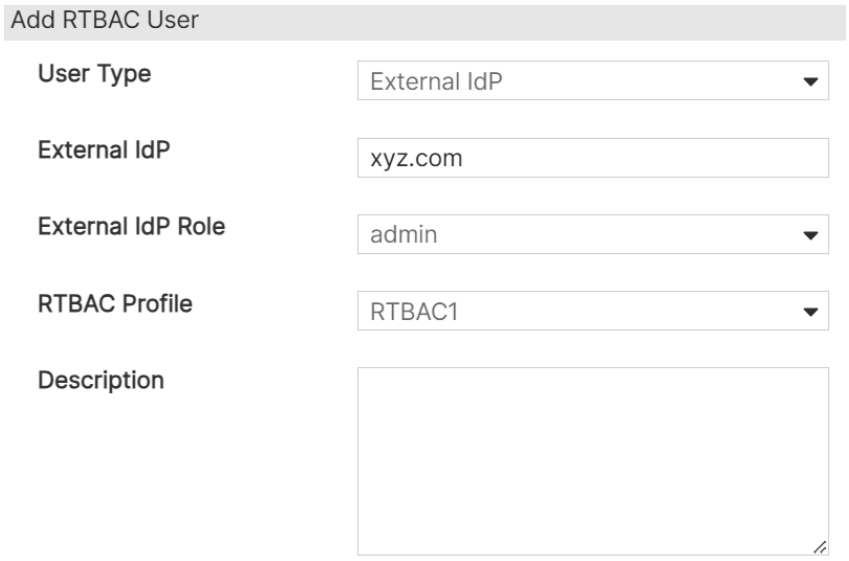


Notes:

- The permissions configured in this page are overridden by the **Access Type** set in the FortiCare account. For example, if the user **Access Type** is **ReadOnly** in FortiCare then all **Read/Write** permissions are reset to **ReadOnly**.
- The resources/tasks with un-configured permissions on this page are granted access based on the **Access Type** (Admin/ReadOnly) configured in FortiCare.

RTBAC Users

You can assign RTBAC profiles to an RTBAC user, external IdP, email, and IAM users are supported. If you do not specify an external IdP role, then the selected RTBAC profile is applicable to all roles from the external IdP. If the administrator has already configured some IdP roles in user management, then those roles are available for selection.

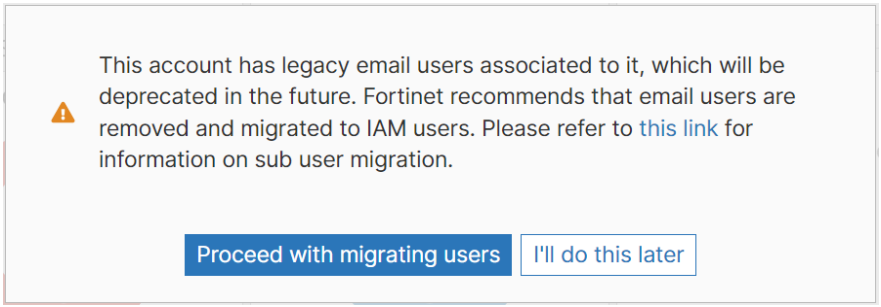


Migrate legacy FortiLAN Cloud users to FortiCloud IAM

You can migrate the legacy email users to IAM users following the sub user migration procedure. For more information, see Migrating sub users.

Note: This migration procedure is applicable to only those FortiLAN Cloud email users who are present in FortiCloud. If the email user is NOT present in FortiCloud, then you are required to create a new IAM user in FortiCloud and delete the existing legacy email user from FortiLAN Cloud.

- When you login into the FortiLAN Cloud, you are presented with the option to migrate the email users. Clicking on **Proceed with migrating users** directs you to the **Manage Account Access** page, where you can use the **Migrate To IAM Users** option.



1. The **Migrate To IAM Users** option re-directs you to the IAM portal wizard to enable migration of existing email users to IAM users.
2. In the **Migrate Sub User(s)** page, read and accept the terms of migration, and click **Next**.
3. Select a username formatting option, and click **Next**.

Format	Description
Use email account name	Maps the user's FortiCloud email (account ID) to the IAM user ID field.
Use Name as Username and filter with space	Maps the user's FortiCloud name to the IAM user ID field.

4. Select users from the list, and click **Next**; review the user's details, and click **Next**. The **User Group, Asset and Portal Permissions** page appears. Select **Yes** from **Basic Info** and select a group.
5. Select the **Permission Profile** that enables access to FortiLAN Cloud and required **Permission Profile** for the user; click **Next**.
   For each user that you migrate, create an IAM user and select the required permissions profile.
6. To confirm the user migration, click **Confirm**.
7. Click **Download IAM User Credentials** that contain the user and password details, and share them with the user.

After the migration is successfully completed, you can delete the legacy user from FortiLAN Cloud.

Note: The legacy email and IAM users can exist simultaneously during this transition.

FortiCloud Organization

FortiCloud supports a centralized account management feature called *FortiCloud Organization* that consolidates multiple FortiCloud accounts into **Organization (O)** or **Organizational Units (OU)**. It allows FortiLAN Cloud Premium license holders to create accounts in FortiCloud. FortiCloud Organization is a central management service in that it is common platform across all Fortinet cloud portals.

With this release, FortiLAN Cloud supports FortiCloud Organization feature in addition to the existing MSSP (multi-tenancy) feature. For more information, see the Organization Portal.

Registering Assets

You are required to register the procured license and device (FortiAP/FortiSwitch) on the FortiCloud portal. For a generic procedure on asset registration see the FortiCloud document.

- Registering a Device
- Registering a License

Registering a Device

To register your device for deploying in FortiLAN Cloud, see Registering Assets.

The procedure for registering a FortiSwitch and a FortiAP is the same.

- Use the registration code/serial number obtained from Fortinet during device procurement.
- Use the **FortiCloud Key** that is shipped along with the device. The key is printed on a sticker attached to a FortiGate/FortiWiFi's top surface.

The registered device is listed in the **Inventory Devices** tab of the FortiLAN Cloud page. You can apply the relevant license and deploy the device.

Registering a License

This section describes registering the following license types.

- FortiCloud Premium and Device License
- UTP License

FortiCloud Premium and Device License

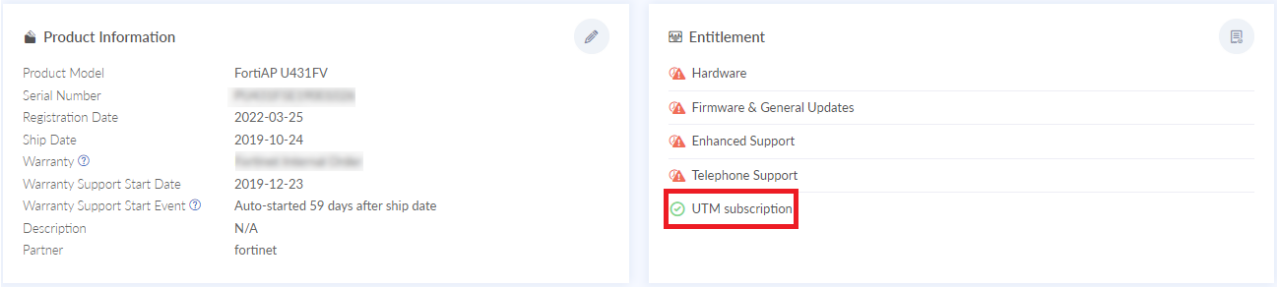
To register your FortiCloud Premium or a device license for deploying in FortiLAN Cloud, see Registering Assets.

Use the registration code/serial number obtained from Fortinet during device procurement. The registered license is listed in the **Inventory Devices** tab of the FortiLAN Cloud page.

UTP License

Ensure that the FortiAP is registered prior to performing the following steps to register the ***UTP license***.

1. Login into https://support.fortinet.com.
2. Navigate to **Products > My Assets** and click **Register More**.
3. Enter the **Registration Code**/serial number obtained from Fortinet during license procurement and select the **End User Type** as per the user functionality defined on the page.
4. Select the FortiAP to apply the UTP license to and complete the registration process. The UTP license is enabled.



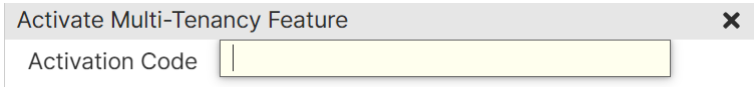
Activating the multi-tenancy feature

The multi-tenancy account is designed for managed security service providers (MSSPs). A multi-tenancy account allows you to create and manage multiple sub-accounts. You can add and move devices between these sub-accounts and each account can have its own administrators and users, allowing more control over a managed service's provisioning.

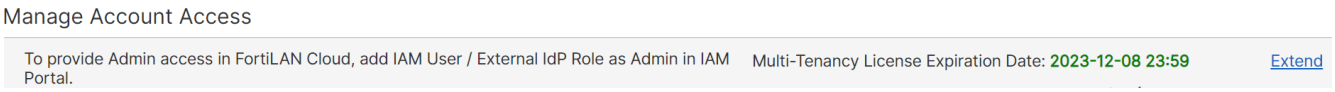
Prerequisites

Purchase a license for the FortiLAN Cloud multi-tenancy feature and obtain the activation code.

1. In the **Manage Account Access** page, click **Extend** and enter the activation code.
2. Click **Ok**.



The activation code is require to activate a new license or extend an existing one.



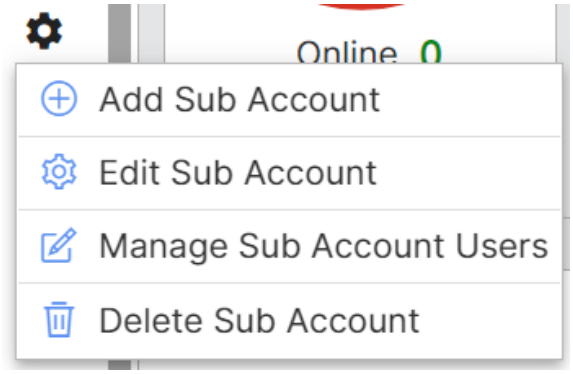
Adding and Managing Sub-Accounts

You can create multiple sub-accounts in a multi-tenancy account.

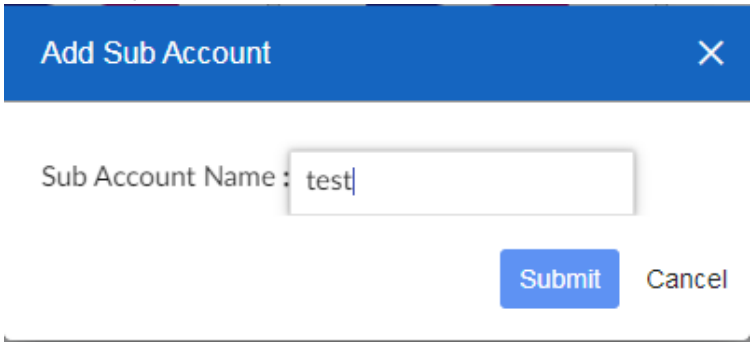
Notes:

- You cannot edit/modify the default sub-account.
- You can create a maximum of 1024 sub-accounts.
- Authentication via REST API is not supported for sub-accounts with permissions for specific folders.

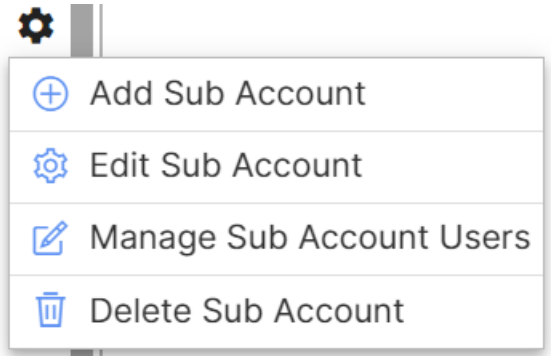
1. To create a sub-account, click on the ⚙ icon and select **Add Sub Account**.



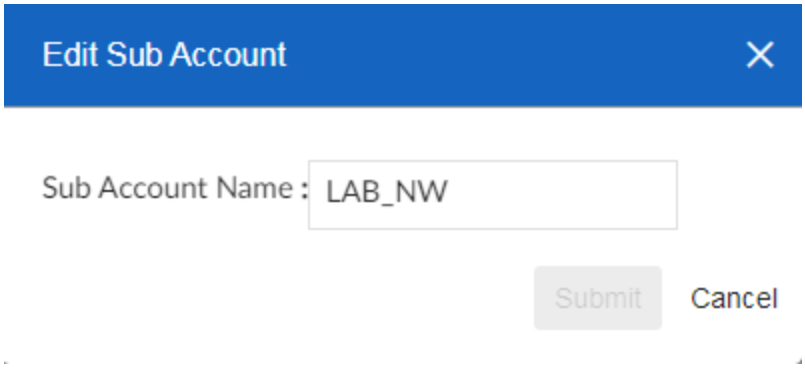
Enter a unique name for the sub-account.



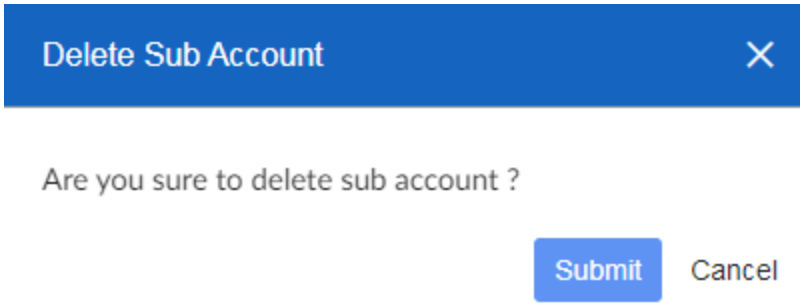
2. Alternately, you can create nested sub-accounts, click the ⚙ icon against an existing sub-account and select **Add Sub Account**.



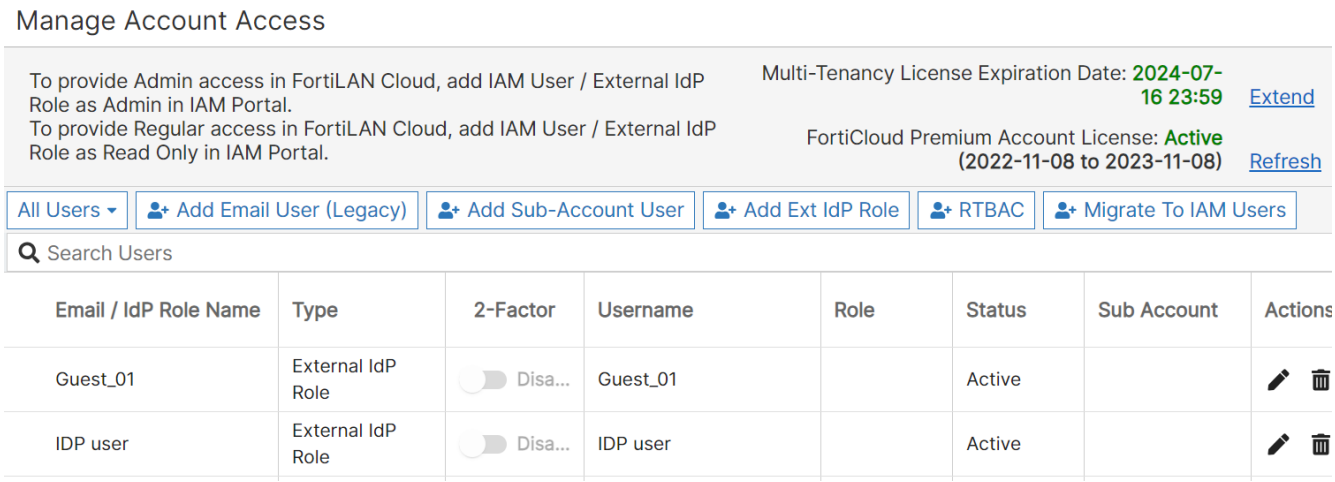
3. You can edit and delete the sub-accounts. Click on the ⚙ icon and select **Edit Sub Account** to modify the account name.



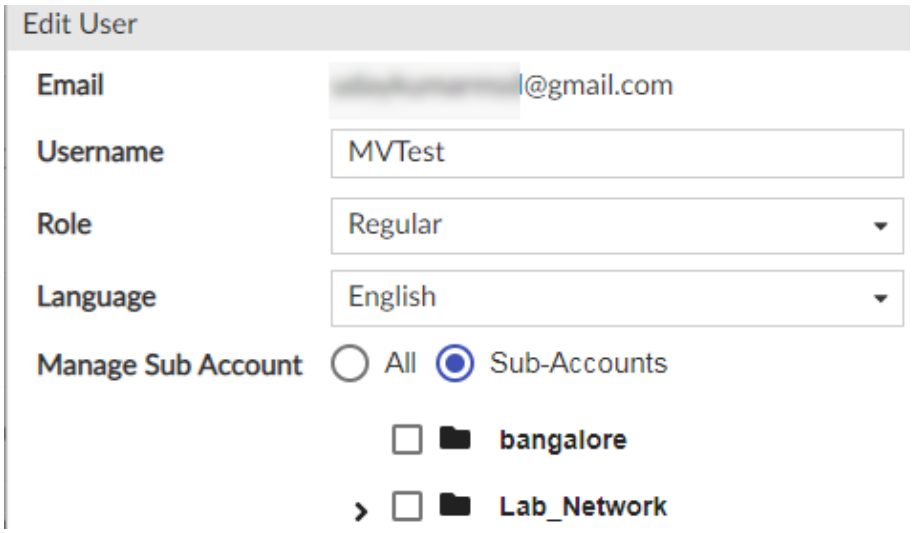
4. Click on the ⚙ icon and select **Delete Sub Account** to delete the account. Click **Submit** and confirm deletion.



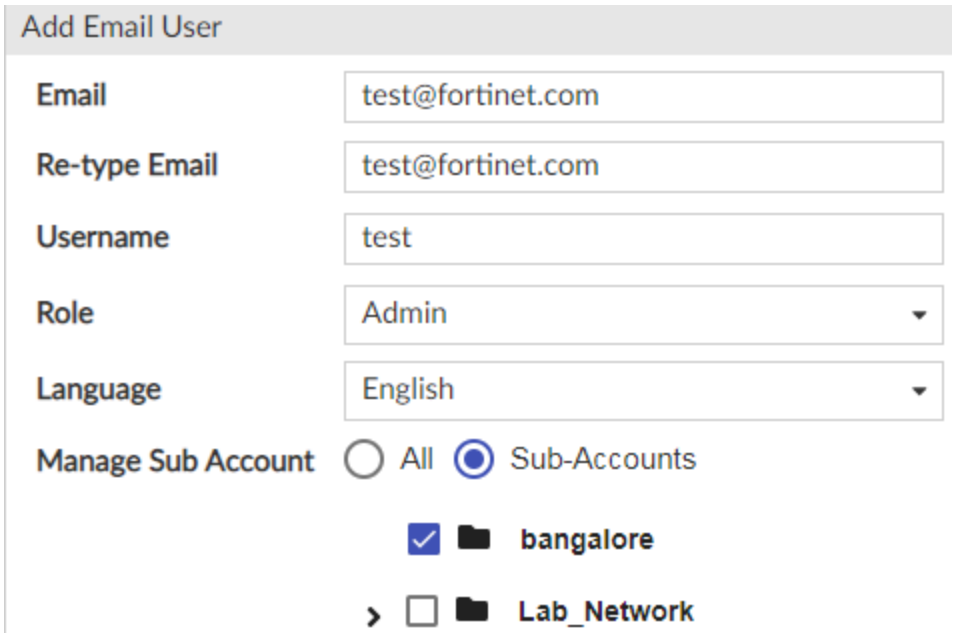
You can assign sub-accounts to existing or new users, navigate to **Manage Account Access**.



Select any user and click the edit icon to manage sub-accounts for the user.



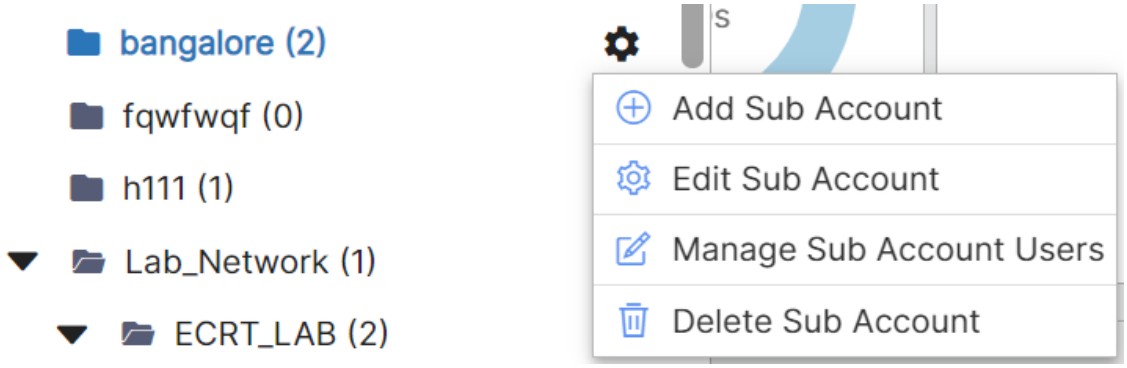
You can manage sub-accounts while creating a new user as well, that is **Add Email User** or **Add Ext Idp Role**.



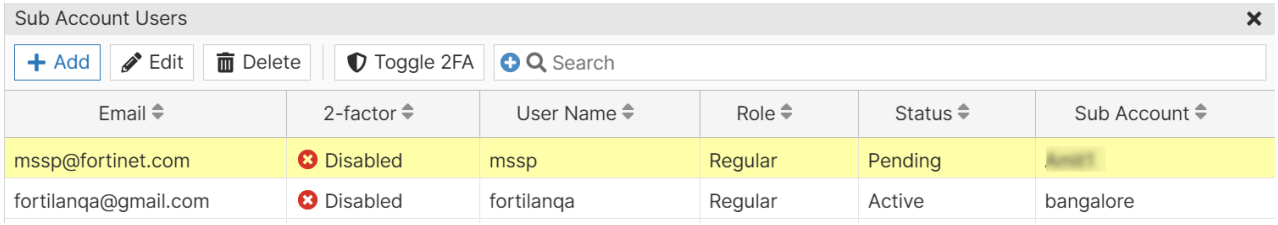
Adding Sub Account Users

You can add users for each sub-account and define their roles.

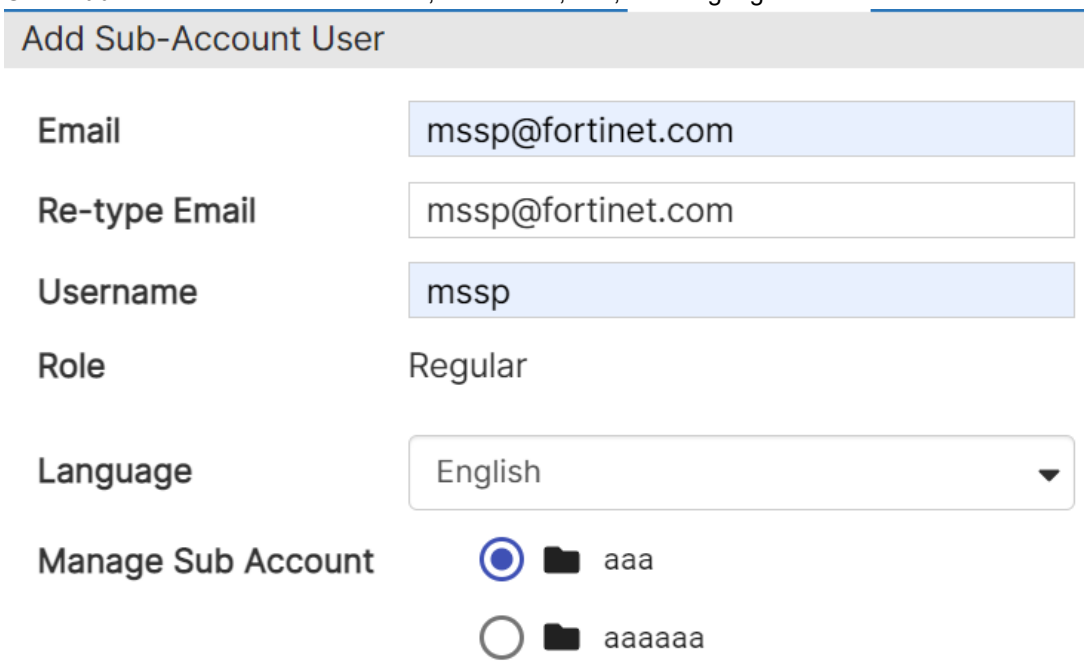
1. To add a sub-accout user, click the icon against a sub-account and select **Manage Sub Account Users**.



The **Sub Account Users** panel is displayed.



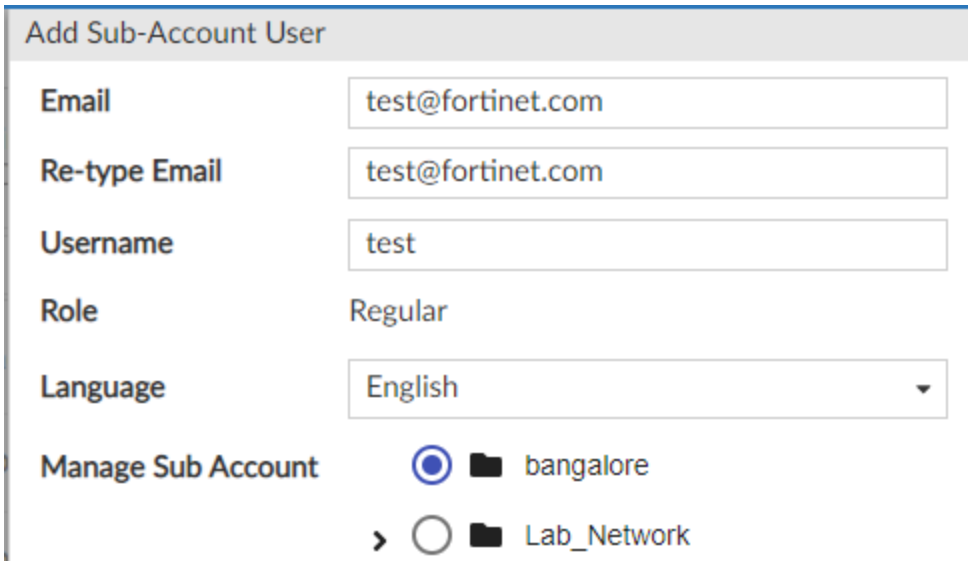
2. Click **Add** and enter the email address, user name, role, and language.



3. Click **Submit**. The user is listed.

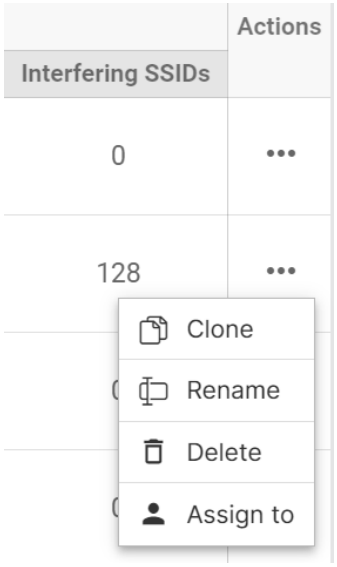
You can mange the sub-account users listed here. Click on the icon to edit the user details, FortiLAN Cloud also allows you to enable **2-factor** authentication for each sub-account user.

Alternately, in the settings option of the home page, navigate to **Manage Account Access** and select **Add Sub-Account User**. Assign a sub-account to the user.



Assigning a Network to Sub-accounts

To assign a network (in the same Master account) to an already existing sub-account, click **Actions** against the network that you want to assign and select **Assign to**. Select sub-account from the list and submit.



Managing FortiLAN Cloud Accounts

This section describes the following operations on a FortiLAN Cloud account.

- Modifying a FortiLAN Cloud account
- Enabling two-factor authentication for FortiLAN Cloud
- Removing a user from a FortiLAN Cloud account

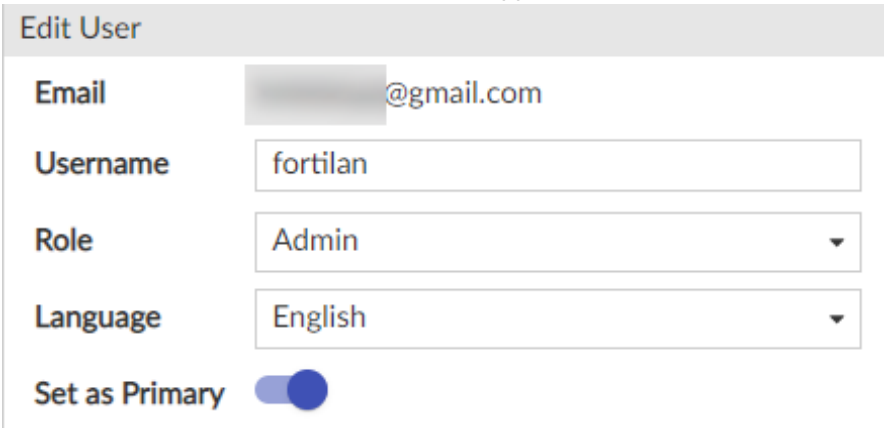
Modifying a FortiLAN Cloud account

You can modify some user configurations from the FortiLAN Cloud GUI.

A regular user does not have the same option to create networks.

Procedure steps

1. Click **Manage Account Access** in the left menu on the GUI, all users are listed. See Manage Account Access.
2. Click the edit icon in the **Actions** column to modify the username, role, and language.
   To set a specific sub-user as primary, enable **Set as Primary**. In this case, you are required to transfer the license to the new account. Contact the *Customer Support* to do the needful.



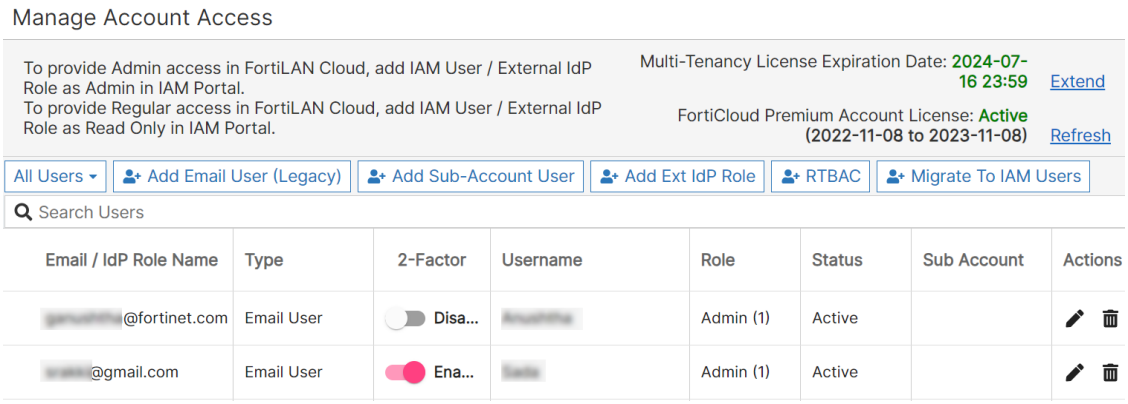
   Note: Contact the *Customer Support* team for assistance to set a sub-user as primary in case of a required password recovery.
3. To save changes, click **Submit**.

To add FortiSwitch users, see Managing Account Access on page 241.

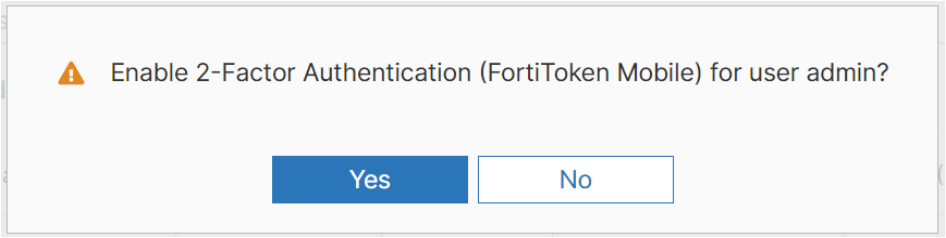
Enabling two-factor authentication for FortiLAN Cloud

Two-factor authentication is offered as part of the FortiLAN Cloud, including the free service. You can choose to enable two-factor authentication using FortiToken Mobile.

1. In the **Manage Account Access** page, enable the authentication in the **2-Factor** column.



2. Confirm the authentication.



3. The next time you log in to FortiCloud to access FortiLAN Cloud, type the authentication token code available from FortiToken Mobile.

Removing a user from a FortiLAN Cloud account

You can remove an admin user or a regular user from your account. In the **Manage Account Access** page, click in the **Actions** column for the user you want to delete.

Managing Networks on FortiLAN Cloud

A network is a logical grouping of FortiAP and FortiSwitch devices for common configuration and management. A FortiLAN Cloud account can have multiple networks. For instance, if you have 20 devices and you plan to use 10 devices in the head office and the other 10 devices in a branch office, then you would create two networks.

In a network, you can also group devices into subsets (sites) and then apply configurations to those subsets. For example, in an office building, you can have a device subset for each floor of the building.

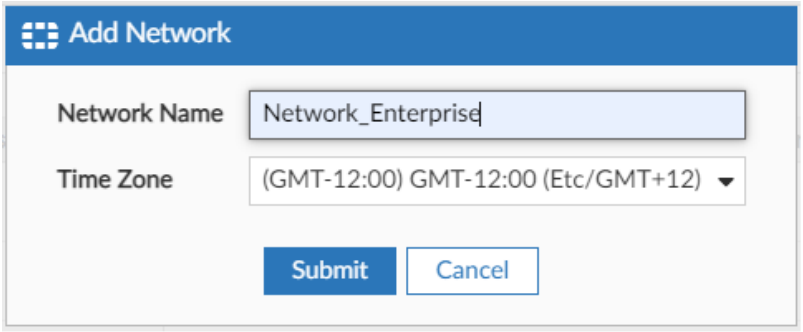
Though it is possible and valid to have a single network containing all devices, and apply configurations to subsets of devices, the recommendation is that you create multiple independent networks.

- Adding a Network
- Cloning a Network

Adding a Network

1. Log in to FortiCloud and access FortiLAN Cloud.
2. On the Home page, click **Add Network**.
3. Type a name for the network.
4. Select a time zone. This is the time zone of the FortiAP devices that you want to manage with this network.

5. Click **Submit**.

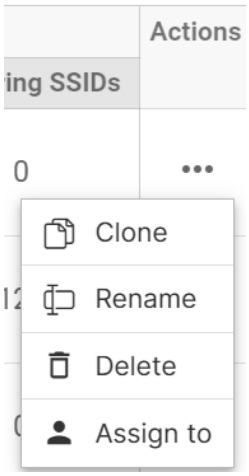


The newly created network is added to the FortiLAN Cloud Home page.

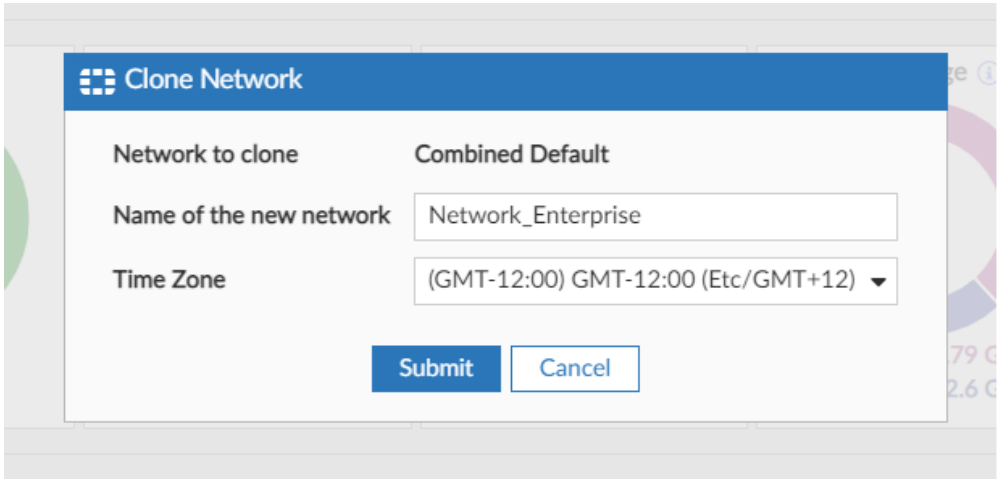
6. Click the network that you created and configure FortiAPs and FortiSwitches.

Cloning a Network

You can clone (in the same Master account) all the configuration in an existing network to a new network. On the home page, click **Actions** against the network that you want to clone and select **Clone**.



Specify a unique name for the network and select your time zone, click **Submit**. The network is cloned.



- **FortiAP** - All configurations except **MAC Access Control** are cloned.
- **FortiSwitches** - **Only** the following configurations are cloned.
  - Switch Tags - No switches are assigned to tags.
  - Zero Touch Configurations – Tag or model based configurations are cloned, device based configurations are NOT cloned.
  - Scheduled Upgrade – Tag based configurations are cloned.
  - Network
  - VLAN Templates

Additionally, you can rename or delete a network from the **Actions** column.

Configuring and Managing FortiLAN Cloud

This section describes the following configurations and operations for FortiLAN Cloud.

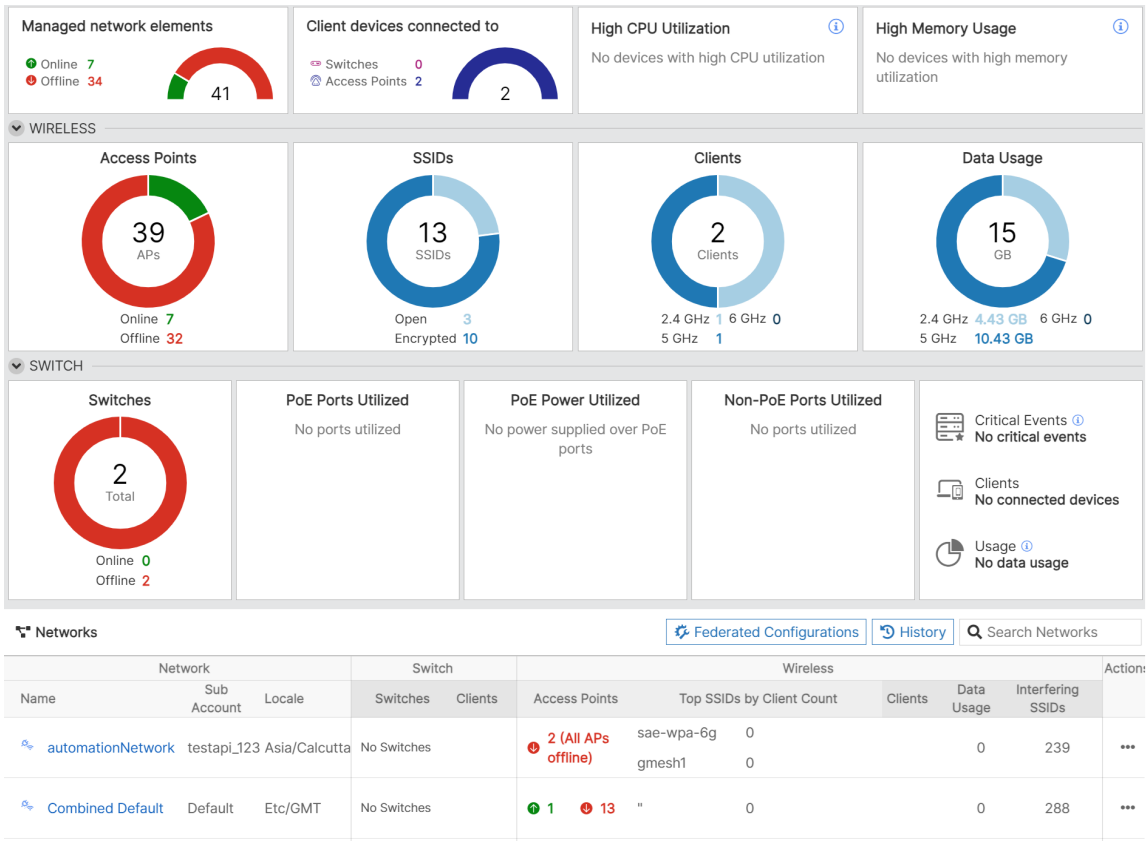
Dashboards

You can monitor your network using the comprehensive FortiLAN Cloud dashboards.

Default Dashboard

The FortiLAN Cloud dashboard view can be filtered based on the following criteria.

- **Summary**: This panel displays data for both FortiSwitches and FortiAPs deployed in all networks in your account.
- **Wireless**: This panel displays data for FortiAP networks managed by FortiLAN Cloud.
- **Switch**: This panel displays data for FortiSwitch networks managed by FortiLAN Cloud.



Section	Description
Summary	To view statistics and visualization for the overall network including the total number of FortiSwitches and FortiAPs and the data consumed by each.
Wireless	To view FortiAP information and subsequent levels such as AP, radio, client, information on radio health, and SSIDs. Hover over these charts to view details.
Switch	To view FortiSwitch information and statistics such as number of VLANs, critical events, clients, and data usage.
Network	This list shows FortiLAN Cloud networks. To access a FortiLAN Cloud network, click the network name. A separate tab opens for that FortiLAN Cloud network. See Default Dashboard on page 38. To rename, delete, or clone a FortiLAN Cloud network, click **Actions**  . See Managing Networks on FortiLAN Cloud on page 35. To create federated configuration profiles and view the profile history, click **Federated Configurations** and **History** respectively. For more information, see Federated Configurations.

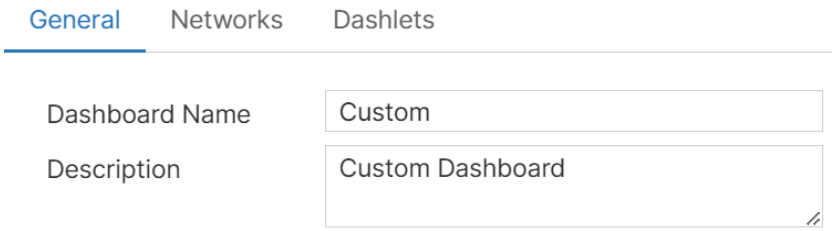
Custom Dashboards and Reports

You can create customizable dashboards with a set of pre-defined dashlets and the provision of exporting dashboard data to PDF reports. This feature enables you to monitor specific network aspects based on your requirements. There is a default dashboard with the overall network statistics, you can create a custom dashboard and set it as the default.

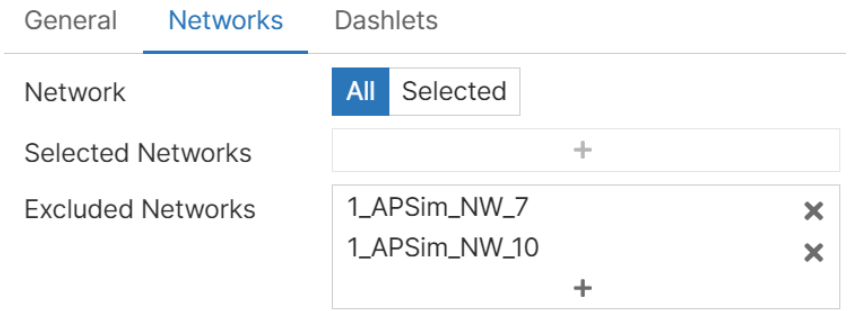
Note: Each user in an account can create a maximum of 5 custom dashboards.

To create a new custom dashboard, update the following tabs.

- **General** – Enter the name of the custom dashboard (2 ~ 32 characters) and an optional description (upto 255 characters).

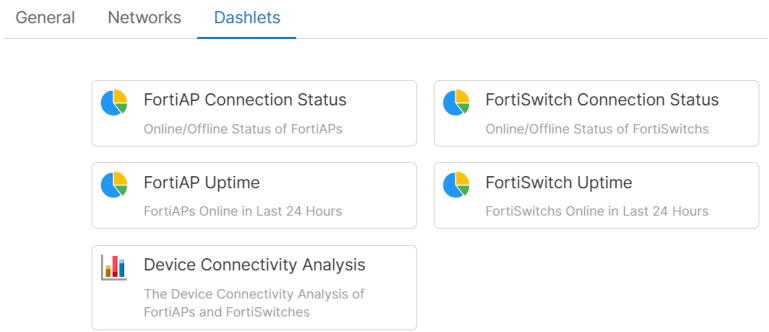


- **Network** - Select which networks to monitor in the custom dashboard. You can either select a few networks to monitor or you can select all networks and optionally exclude a few from monitoring.



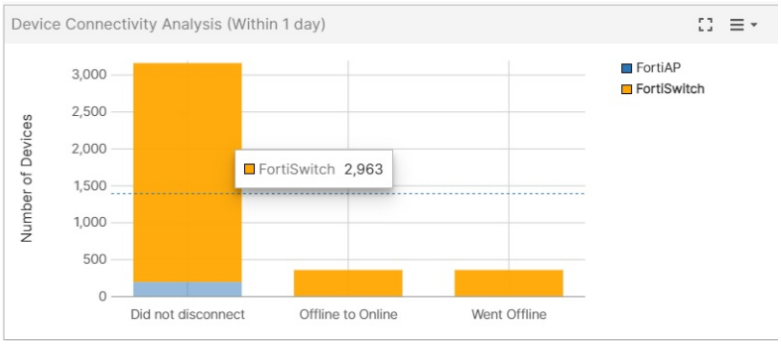
- **Dashlets** – Select the one or multiple pre-defined dashlets to include in the custom dashboard.
  - FortiAP Connection Status
  - FortiSwitch Connection Status
  - FortiAP Uptime
  - FortiSwitch Uptime
  - Device Connectivity Analysis

When you select the dashlets for FortiAP/FortiSwitch uptime statistics, you are prompted to specify the duration.

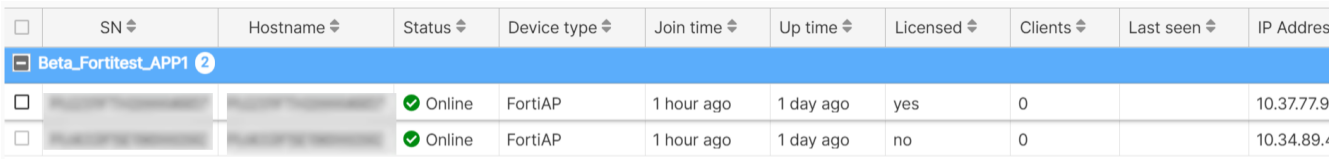


The **Device Connectivity Analysis** chart displays the connectivity status of FortiAPs and FortiSwitches over the selected period of time. It provides insights into the following device statistics.

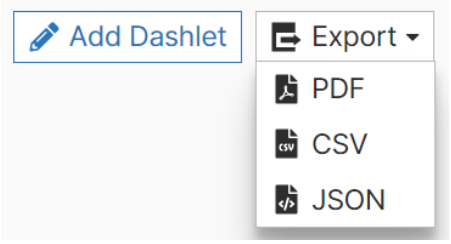
- Devices that went offline.
- Devices that went offline and then came online (re-booted, re-connected, and so on).
- Devices that did not disconnect.



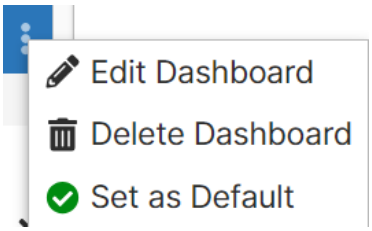
Click on the bar to view the device details.



You can add and remove dashlets after the custom dashboard is created. The data from the custom dashboards can be exported into reports that are supported in the PDF, CSV, and JSON formats. Select **Export > [PDF | CSV | JSON]**.



Click on the **Actions** menu for the following additional operations that you can perform on the custom dashboard.



- **Edit Dashboard** – You can edit all the parameters set for the custom dashboard and also view the time stamp for the dashboard creation and last update.
- **Delete Dashboard** – You can delete the custom dashboard permanently.
- **Set as Default** – You can set the custom dashboard as the default, this dashboard is then displayed at the time of login.

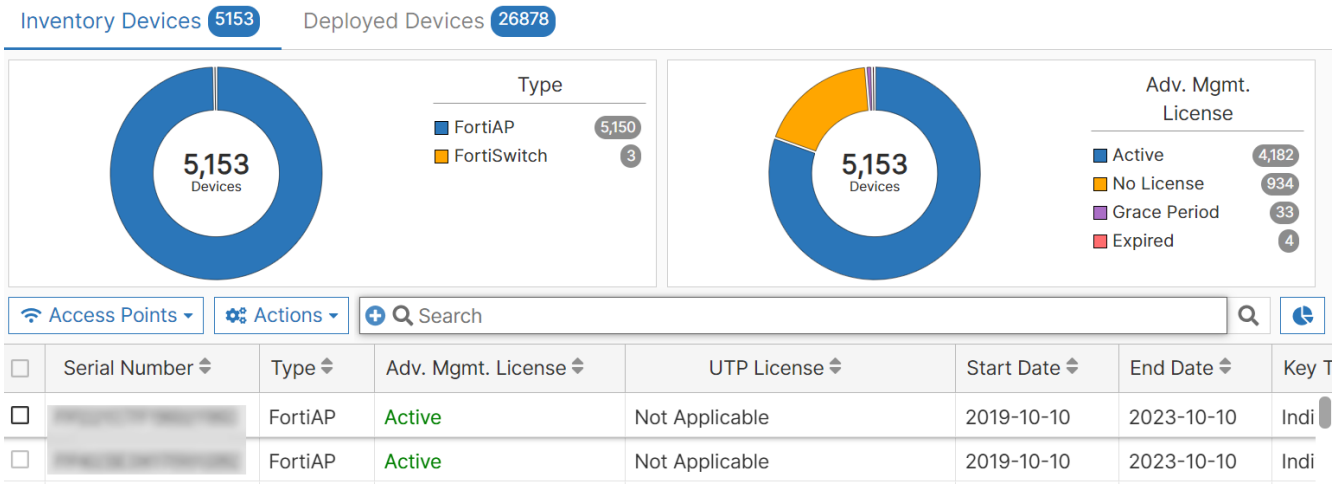
Devices

In this page, you can deploy and manage devices in FortiLAN Cloud.

- Inventory Devices
- Deployed Devices
- Query Devices

Inventory Devices

The **Inventory Devices** tab displays the claimed/un-deployed devices and allows you to deploy them.



- Registering APs
- Adding/Removing Devices
- Synchronizing AP License
- Deploying APs
- Applying/Removing License
- Exporting Device Details

Registering APs

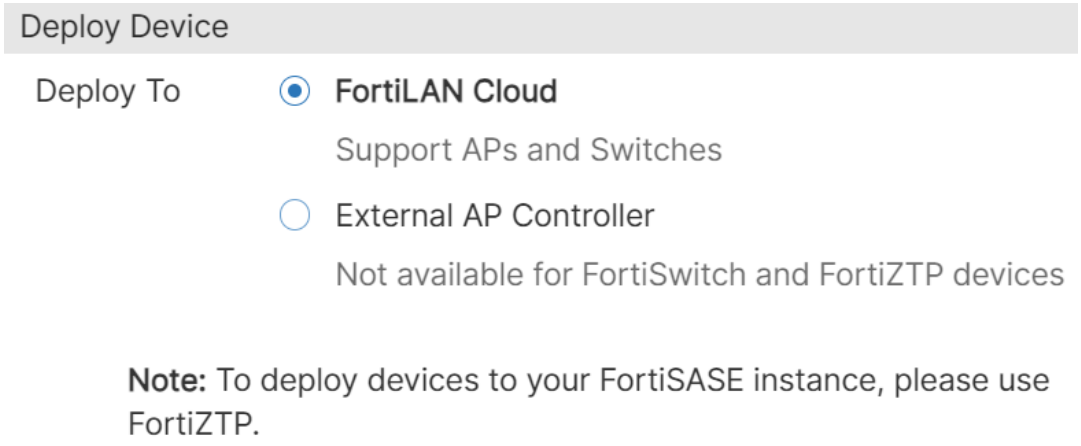
You can register FortiAP devices present in FortiLANCloud (imported with help of FortiKey) into your current FortiCloud account. Select the FortiAP and click **Access Points > Register APs**. The **Registration** column displays the registration status with the FortiCloud account, *Registered* or *Not Registered*. The corresponding **Key Value** column displays *FortiCare* for devices registered in the FortiCloud account. You can register a maximum of 50 FortiAPs at a time.
FortiAPs registered in FortiCloud (section Signing-on for FortiLAN Cloud) are automatically synchronized daily, click the refresh icon on the top-right to manually synchronize the FortiAPs.
Notes:

- You cannot un-register devices (or transfer to another account) that are registered in FortiCloud, for a minimum of three years from the date of registration. To un-register, contact *Fortinet Customer Support*.

- **Note**: If an account has no FortiAP device in any FortiLAN Cloud domain, then manual synchronization is required at least once. Click the refresh icon at top right corner of the **Devices** page.

Adding/Removing Devices

You can import FortiAP devices using the **Access Points > Add APs** option. You can also deploy FortiLAN Cloud managed FortiAPs to a FortiSASE instance as an external AP Controller. Select **External AP Controller** and enter the IP address or hostname of the FortiSASE instance. You can also deploy FortiLAN Cloud managed FortiSwitches to FortiSASE via FortiZTP.



Synchronizing AP License

You can use the **Access Points > Sync AP License** option to manually synchronize the AP and UTM license.

Deploying APs

Select **Actions > Deploy** to deploy the FortiAP to FortiLAN Cloud or to an external AP Controller. See Deploying a FortiAP device to a network.

Applying/Removing License

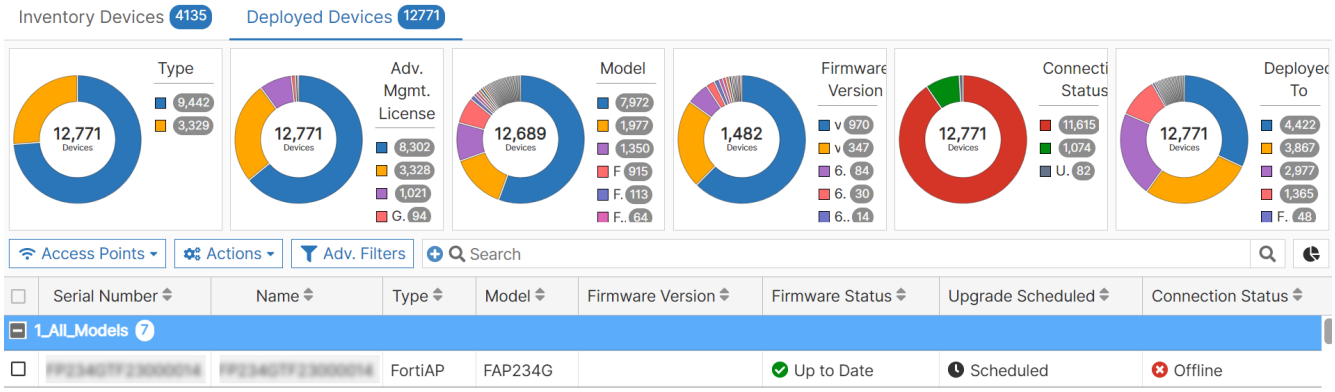
You can apply the license to the listed devices, select unlicensed or license-expired devices and click **Actions > License > Apply License**. To remove the applied license, click **Actions > License > Remove License**.

Exporting Device Details

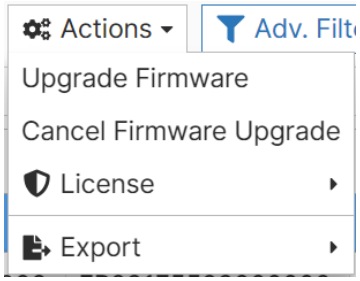
To export the device details from all 3 tabs in a CSV, JSON, or text format; click **Actions > Export** . You can select multiple inventory rows at a given time to use the available options.

Deployed Devices

The **Deployed Devices** tab displays fully deployed devices to networks or external ACs.



Note: If the **Deployed Time** is **Not Available**, it implies that FortiLAN Cloud could not determine the time instant at which the device was deployed to a network. You can upgrade firmware for devices that are deployed in multiple different networks, with a single operation. Select one or multiple online devices and click **Actions > Upgrade Firmware**. To discontinue firmware upgrade, select **Cancel Firmware Upgrade**.



Additionally, you can register APs, manage licenses, and export device information. For reference, see Inventory Devices.

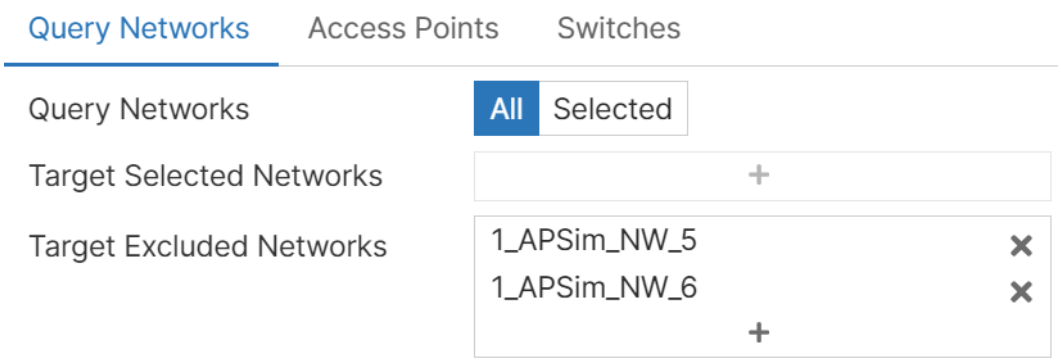
Query Devices

You can now query deployed devices in your network from the **Devices > Deployed Devices** page. Click **Adv. Filters** to perform the query operation.

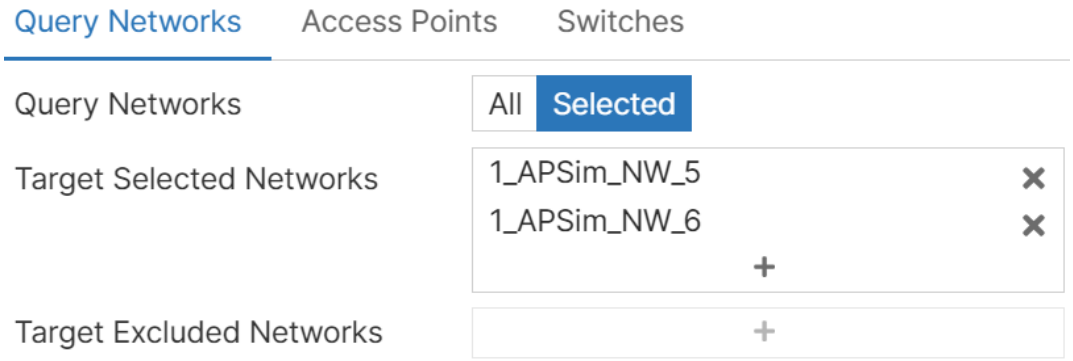
- Query Networks
- Query Devices

Query Networks

Select the target networks to query device information. Select **All**, to run the query on all existing networks and, optionally, select the **Target Excluded Networks** to exclude specific networks from the query results.

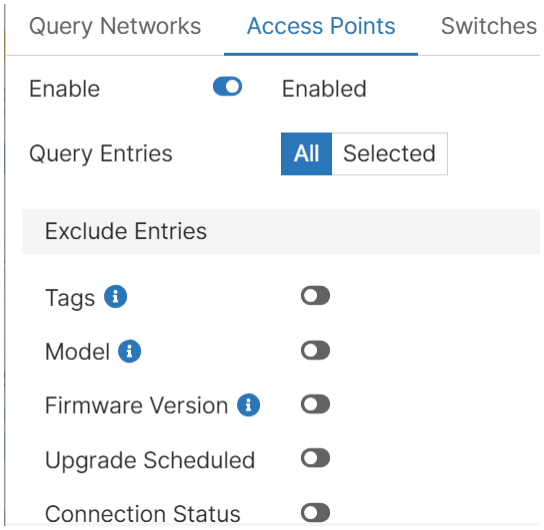


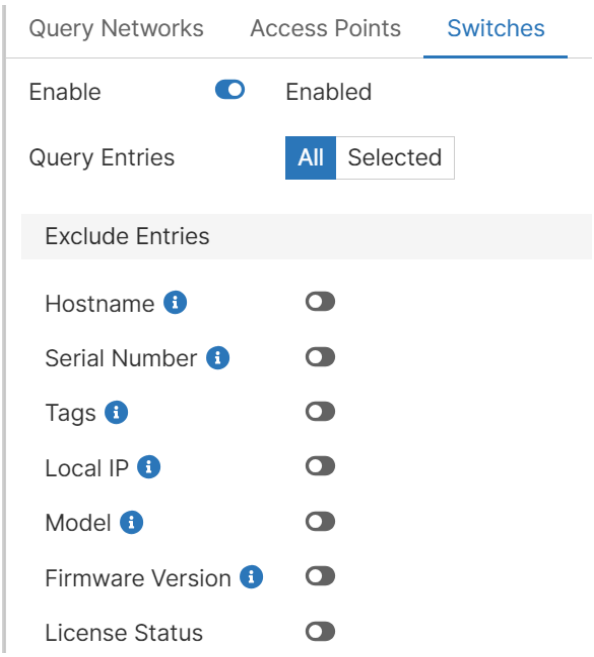
To query devices in specific networks, select **Selected** and specify the **Target Selected Networks**.



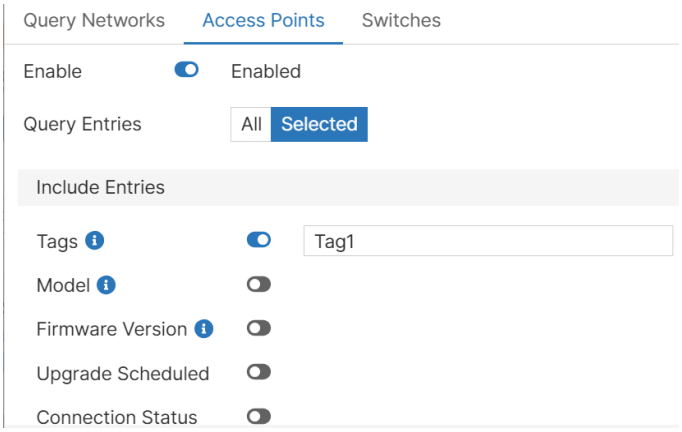
Query Devices

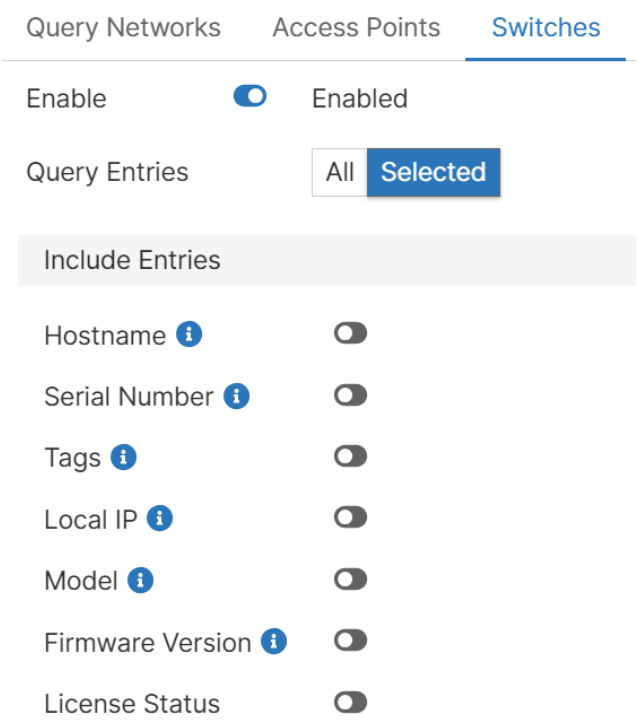
Select the target access points or FortiSwitches, that is, specific criteria to query device information. Select **All**, to query all existing networks/entries without exceptions, you can optionally specify entries in the **Exclude Entries** section. This excludes device information related to those entries from the displayed query result.





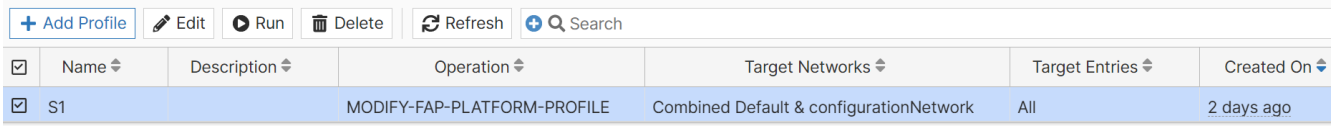
Likewise, select **Selected** and specify entries in the **Include Entries** section. This includes device information related only to those entries in the displayed query result.





Federated Configuration

FortiLAN Cloud provides federated/centralized configuration changes or status queries that work across networks. You can make specific configuration changes required in multiple networks in a single operation, eliminating the overhead of re-configuring every network separately. The configuration operation allows you to create federated configuration profiles to modify and apply FortiAP platform profiles to multiple networks, you can also view the configuration profile history. Select **Configuration** in the main menu or select **Federated Configurations** in the networks section of the home page.



Select a specific profile in this page to **Run** (apply the configuration changes), **Edit** or **Delete**.

The following configuration related operations are supported.

- Creating Configuration Profiles
- Profile History

Creating Configuration Profiles

You can edit the FortiAP platform profile configurations and apply the changes to multiple networks. To create a federated configuration profile for the *MODIFY-FAP-PLATFORM-PROFILE* operation, click **Add Profile** and update

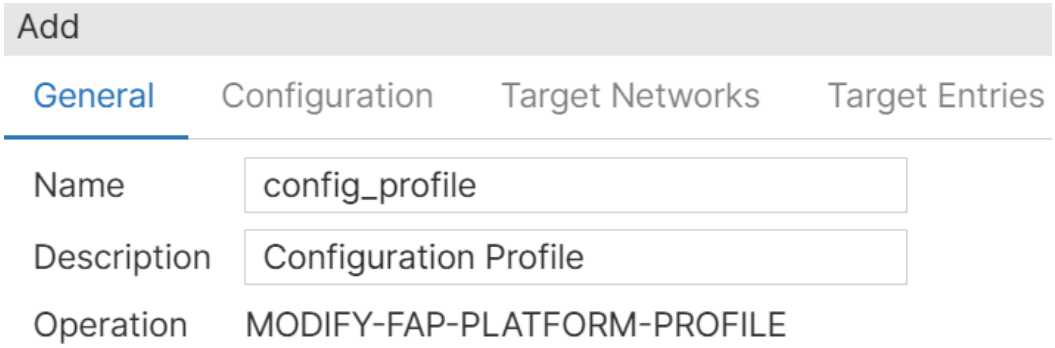
information in the following tabs. To apply the configuration changes in this profile, click **Run** from the **Configuration** page.

Note: A maximum of 100 configuration profiles are allowed to be created.

- General
- Configuration
- Target Networks
- Target Entries

General

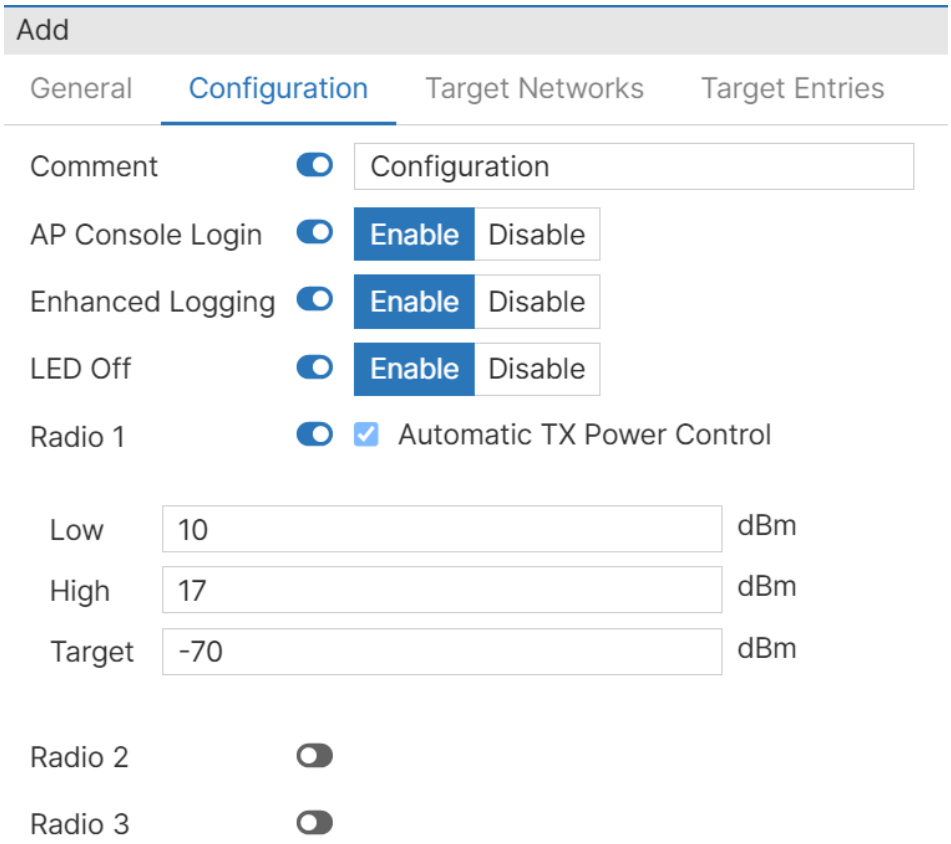
Configure the following general fields applicable to the configuration profile.



- **Name** - Enter a unique name for the configuration profile. The valid range is 1-63 characters.
- **Description** - Optionally, enter a description for the configuration profile. The valid range is 0-255 characters.

Configuration

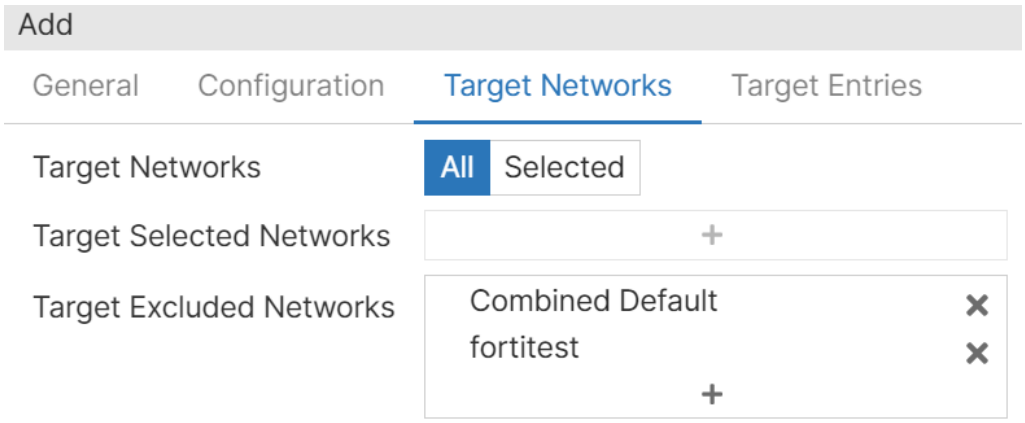
Configure the setting to apply to all/specific platform profiles and FAP models. You can enable/configure the following.



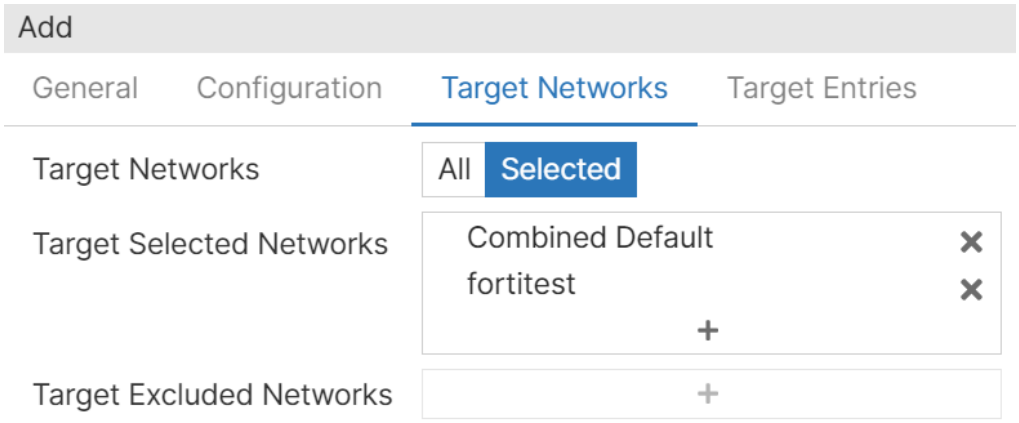
- **AP Console Login** - You can enable/disable console port access on the FortiAP
- **Enhanced Logging** - You can enable receiving and storing more than 50 categories of logs from the FortiAPs with detailed insights into all network activity.
- **LED Off** - You can enable/disable the LEDs from glowing on the FortiAP.
- **Radio** - You can configure the radio transmit power settings. Configure the maximum Tx power or enable **Automatic TX Power Control**.

Target Networks

Select the target networks on which to run and apply the federated configuration profile. Select **All**, to apply the configuration to all existing networks and select the **Target Excluded Networks** to, optionally, exclude specific networks from the configuration changes.

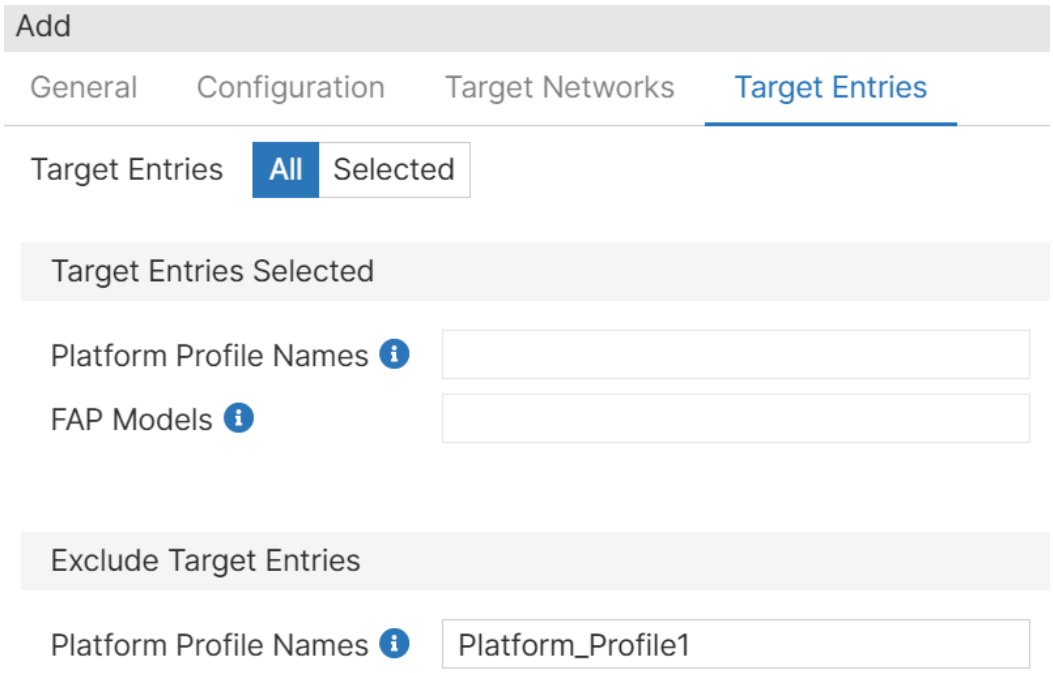


To apply the configuration profile to specific networks, select **Selected** and specify the **Target Selected Networks**.

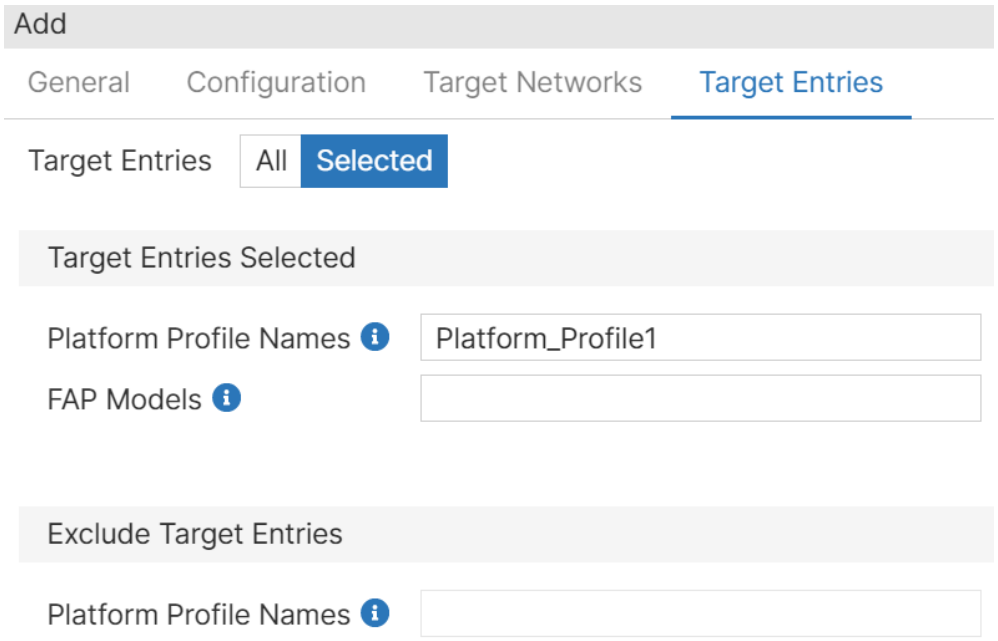


Target Entries

Select the target entries, that is, the existing platform profiles and FAP models to run and apply the federated configuration profile. Select **All**, to apply the configuration to all existing platform profiles and FAP models, optionally, specify **Platform Profile Names** in the **Exclude Target Entries** section to exclude specific platform profiles from the configuration changes.



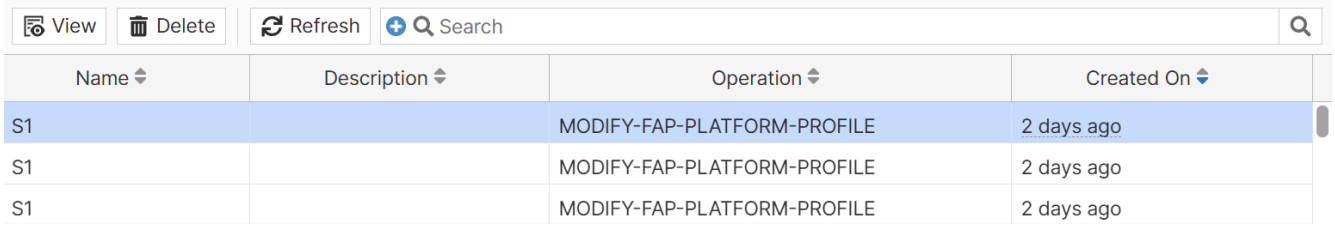
To apply the configuration profile to specific platform profiles and FAP models, select **Selected** and specify the **Platform Profile Names** and/or **FAP Models** in the **Target Entries Selected** section.



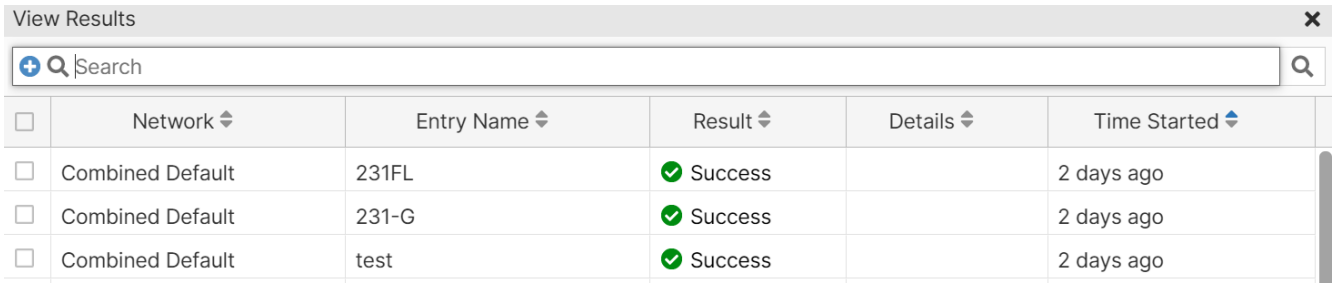
Note: A maximum of 512 characters can be specified in the fields of this tab.

Profile History

This page displays the history of the federated configuration profiles that are created and applied. A maximum of 100 profiles are displayed.

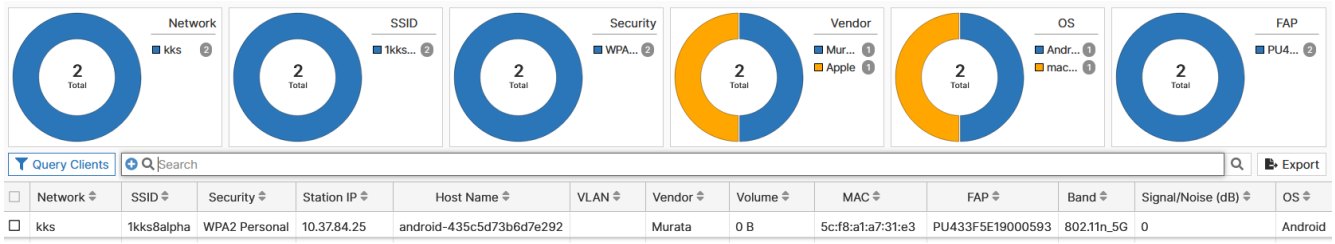


Select an entry and click **View**, the configuration profile details and status are displayed.



Clients

You can query multiple existing networks for client data. To access the federated configuration/query operations, select **Clients**. This page displays the client distribution statistics charts based on specific criteria, such as, network, SSID, security, and so on.



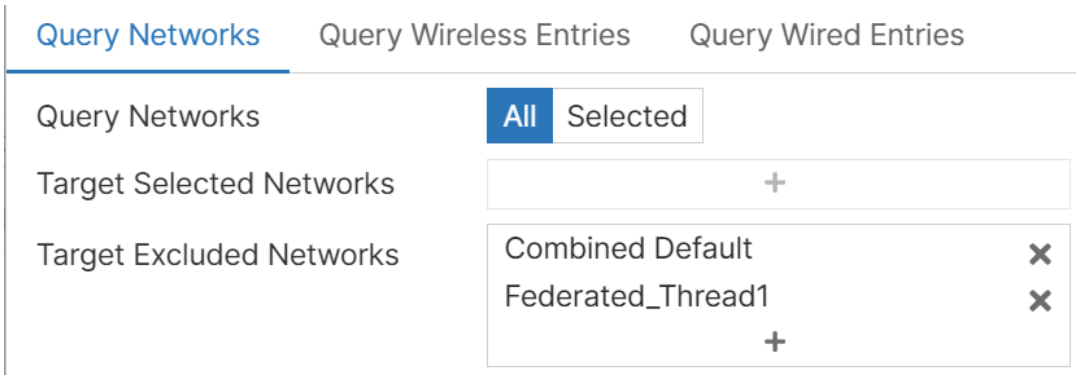
The **Query Clients** operation queries networks (all or criteria-based) in the account about wireless client information. When a query is run, the wireless client details are fetched as per specified filters, you can query specific networks or entries. Click **Adv Filters**.

Note: A maximum of 5000 less clients are displayed per network. No display limits are applied on wired clients.

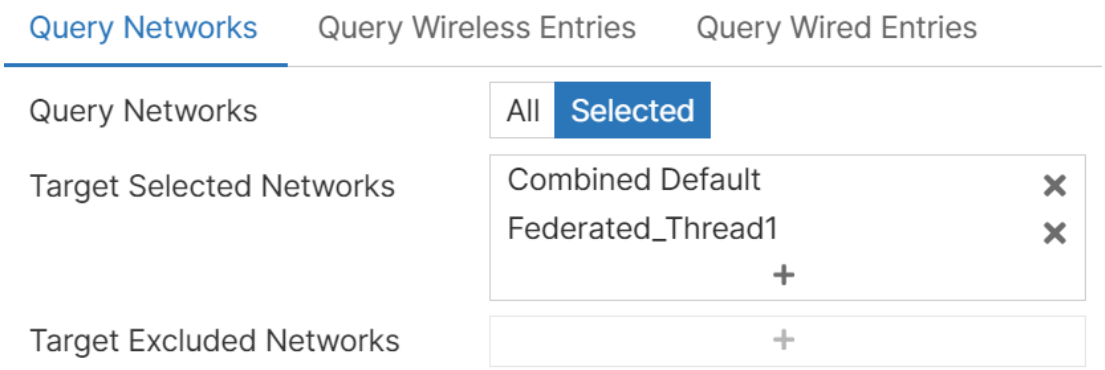
- Query Networks
- Query Wireless Entries
- Query Wired Entries

Query Networks

Select the target networks to query client information. Select **All**, to run the query on all existing networks and, optionally, select the **Target Excluded Networks** to exclude specific networks from the query results.

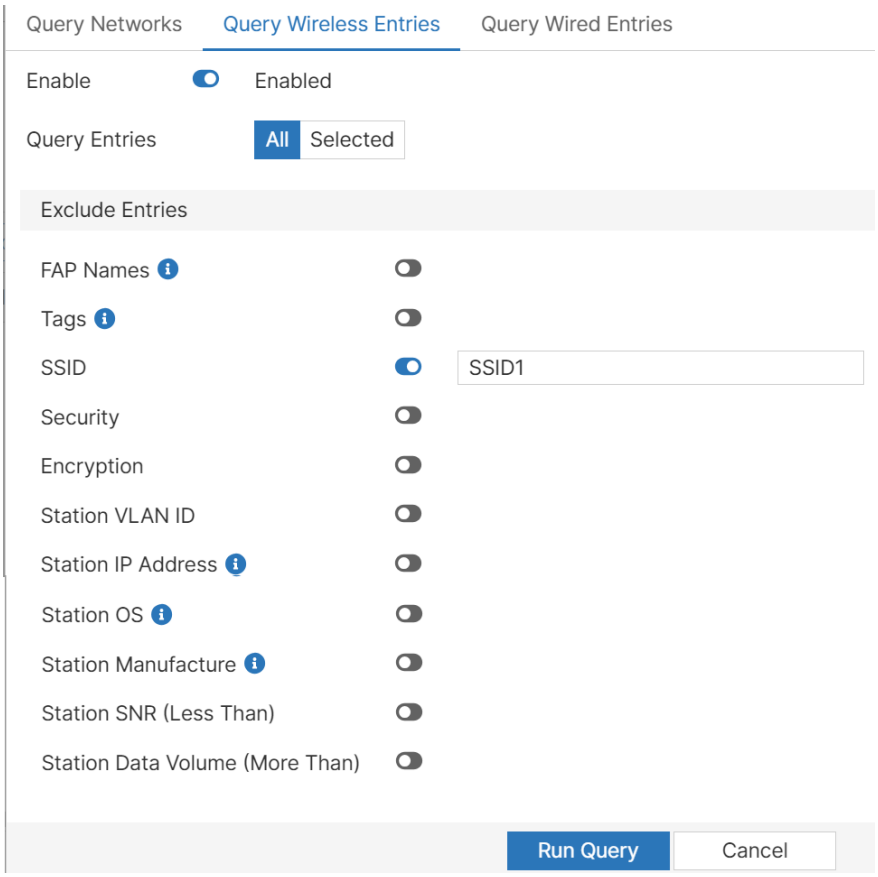


To query clients in specific networks, select **Selected** and specify the **Target Selected Networks**.

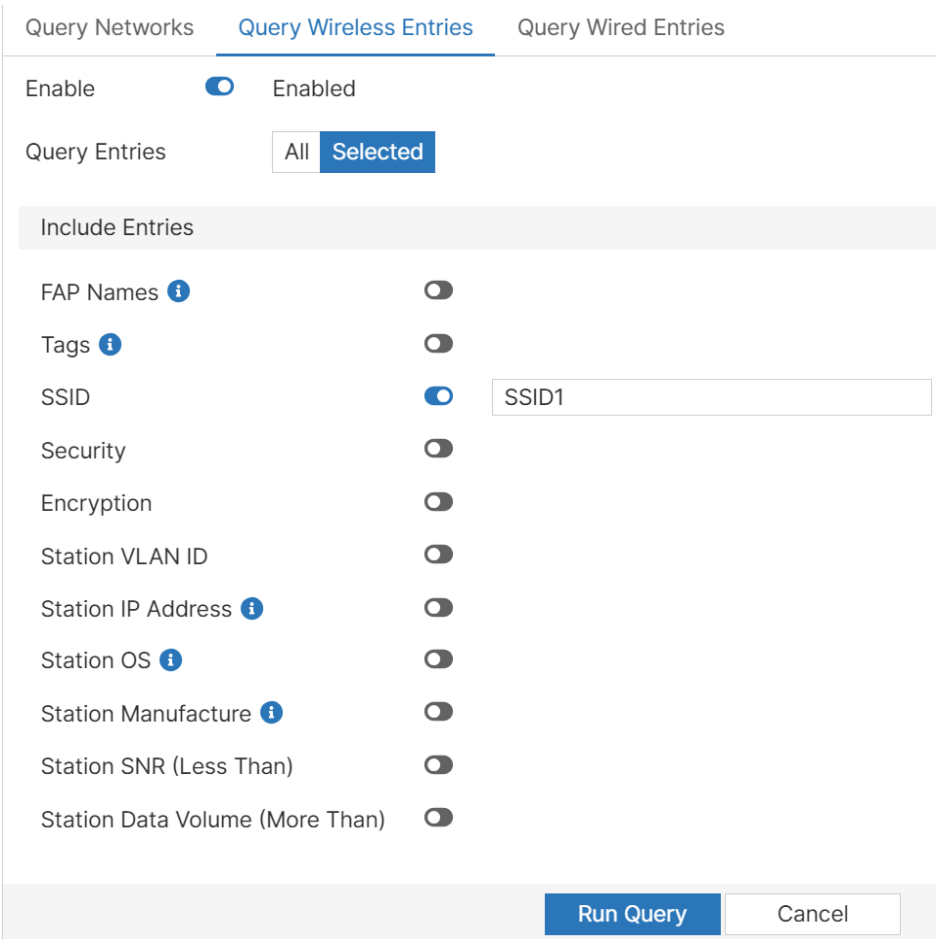


Query Wireless Entries

Select the target wireless entries, that is, specific criteria to query client information. Select **All**, to query all existing networks/entries without exceptions, you can optionally specify entries in the **Exclude Entries** section. This excludes client information related to those entries from the displayed query result.

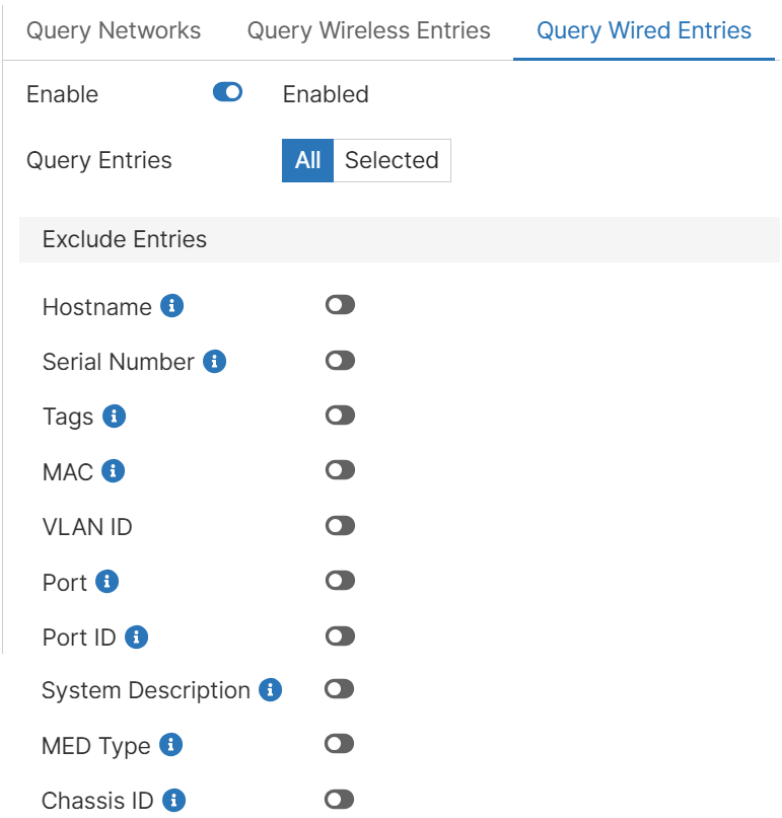


Likewise, select **Selected** and specify entries in the **Include Entries** section. This includes client information related only to those entries in the displayed query result.

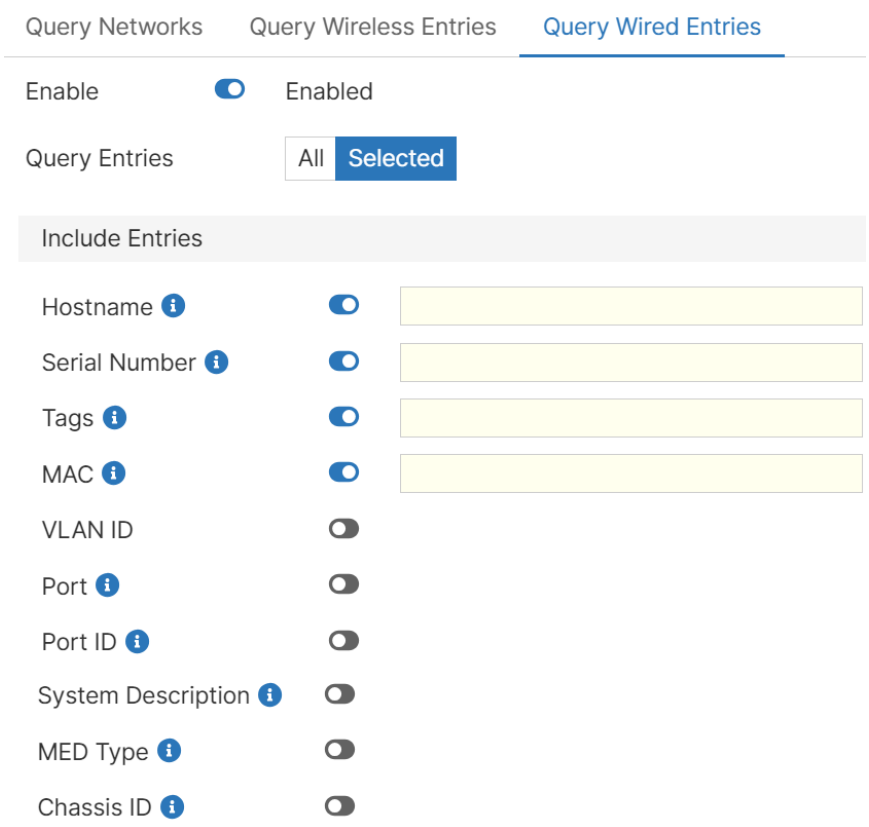


Query Wired Entries

You can query multiple networks for wired clients connected to FortiSwitches. Select **All**, to query all existing networks/entries without exceptions, you can optionally specify entries in the **Exclude Entries** section. This excludes client information related to those entries from the displayed query result.

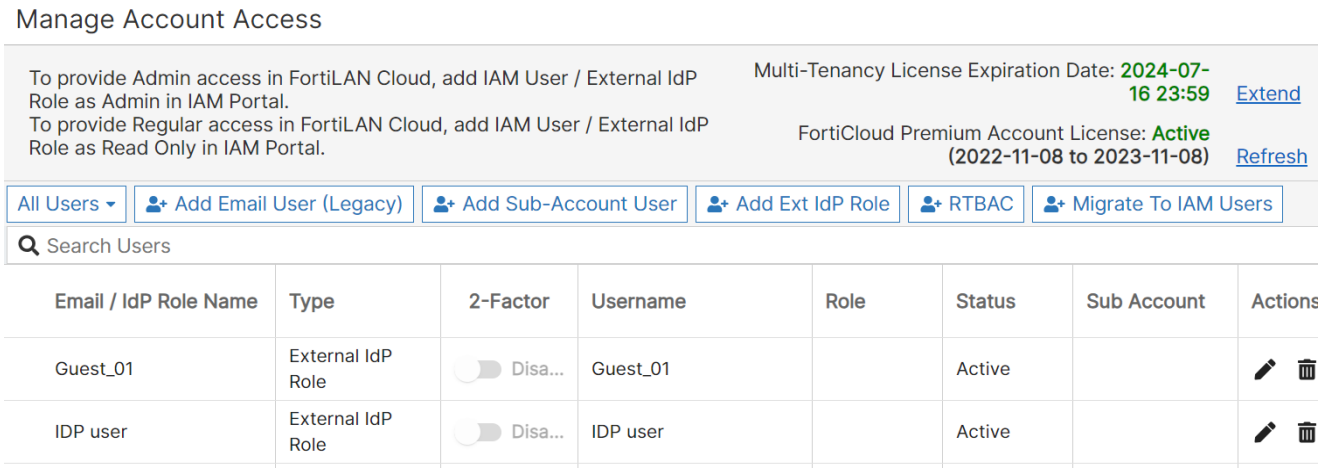


Likewise, select **Selected** and specify entries in the **Include Entries** section. This includes client information related only to those entries in the displayed query result.



Manage Account Access

To add and manage Email, IAM, and external IdP authenticated users, click **Manage Account Access**. For more information, see Managing Users and Accounts.



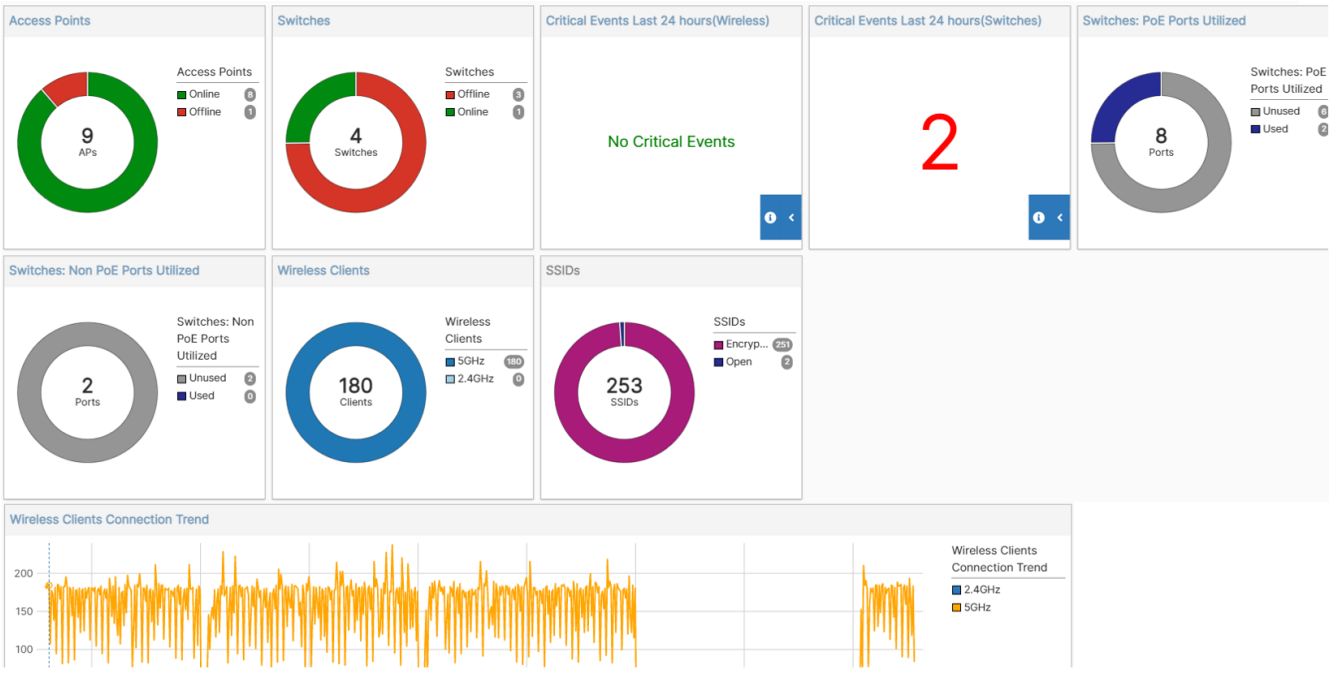
Network Level Configuration

This section describes the following configurations that are applicable at a network level.

- Network Summary Dashboard
- Unified Device Tags

Network Summary Dashboard

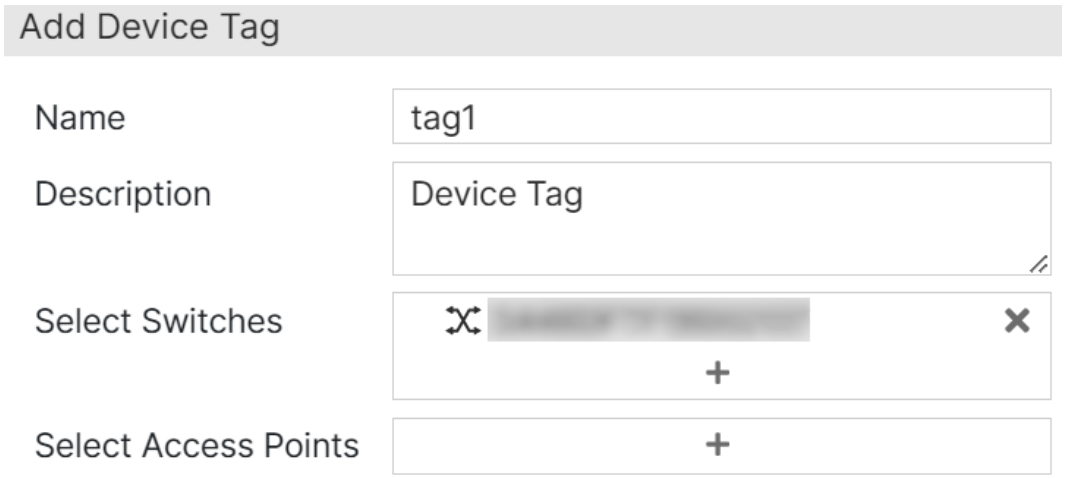
The network summary dashboard combines information from FortiAPs and FortiSwitches managed by FortiLAN Cloud. It displays a series of charts and graphs providing the device count and status, ports utilized, client and SSID details, connection trends, and critical network events. This data is crucial to monitoring and troubleshooting the wireless network elements.



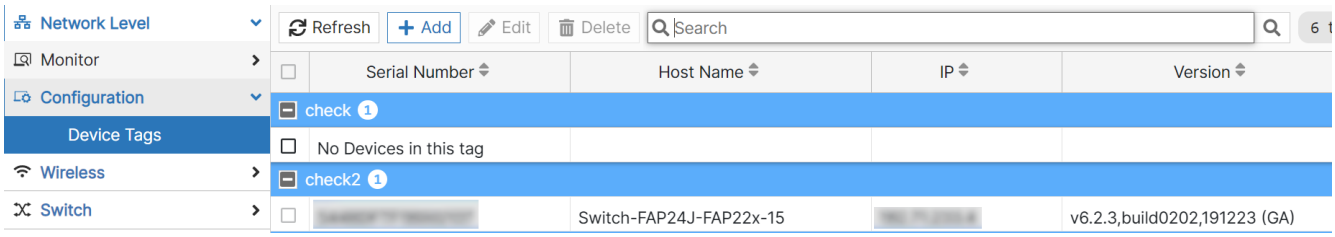
Unified Device Tags

Device tags are used to form device groups with the purpose of applying configurations and performing upgrades. Prior release version 23.2, separate tags were created and managed for FortiAPs and FortiSwitches. The unified device tags can be created and applied across devices (FortiAPs and FortiSwitches).

In the main menu, navigate to **Network Level > Configuration > Device Tags** and click **Add** to create a new tag. Select any existing tags to perform the **Edit** or **Delete** operations.



Select the FortiSwitches and FortiAPs to assign the device tag.



Notes:

- The displayed count for device tags not assigned to any FortiSwitch/FortiAP is 1.
- The existing functions of assigning tags to FortiAPS and FortiSwitches are done at the device level.

Configuring and Managing FortiAPs

This section describes configuring, monitoring, and managing FortiAP devices in your networks using FortiLAN Cloud and includes the following FortiAP requirements.

Menu	Description
Monitor	Displays a dashboard with a view of all managed APs including up time, client details, usage statistics, and rogue APs that may be in your environment.
Deploy APs	Allows the deployment of an AP from the inventory to an AP network. During an AP deployment, you can set the platform profile, AP tags, an AP site, and administration settings.
Access Points	Displays the status of APs. Allows tasks such as configuration and upgrade. You can also capture packets and observe live network traffic on an AP.
Configure	Provides sub-menus to add and configure wireless service set identifiers (SSID) including platform profiles, AP tags, MAC access control and more. You can also enable Bonjour Relay and FortiPresence.
Logs	Provides logs for events in the following categories: wireless, antivirus, botnet, IPS, web access, and application control.
Reports	Provides summary reports with charts on current and past information such as traffic and client count by SSID and AP. Also provides the option to run PCI compliance reports.

Supported access points

You can manage all FortiAP models via FortiLAN Cloud. However, FortiAP models at end of life (EOL) do not receive firmware upgrades from Fortinet. For a list of the FortiAP models that are under active device support, review the Wireless Product Matrix.

Recommended FortiAP firmware version

Fortinet recommends that you use FortiAP version 6.0 or later with FortiLAN Cloud version 24.1.

Getting started

This section includes the following FortiLAN Cloud procedures:

- Adding a FortiAP device to FortiLAN Cloud with a key on page 62
- Adding a FortiAP device to FortiLAN Cloud without a key on page 62
- Managing Networks on FortiLAN Cloud on page 35
- Deploying a FortiAP device to a network on page 64
- Moving a FortiAP between accounts on page 65

After purchasing and physically deploying the FortiAP devices (such as connecting to the internet) in various premises, perform the tasks and procedures from the following workflow to configure and monitor FortiAP devices using the FortiLAN Cloud management solution.

Task sequence	Description and procedure
Task 1	Register on FortiCloud and access the FortiLAN Cloud management solution. Perform this procedure: Signing-on for FortiLAN Cloud on page 20
Task 2	Add a purchased FortiAP device to your FortiLAN Cloud account inventory. Later in this workflow, you will deploy that FortiAP device from the inventory to a network. Perform the applicable procedure: • Adding a FortiAP device to FortiLAN Cloud with a key on page 62 • Adding a FortiAP device to FortiLAN Cloud without a key on page 62
Task 3	Add logical AP networks to organize your FortiAP devices by their physical premises. With a network, you manage FortiAP devices and service set identifiers (SSID). Perform this procedure: Managing Networks on FortiLAN Cloud on page 35
Task 4	Deploy your FortiAP devices from the inventory into various networks. This task includes assigning a wireless network name that clients can connect to, and configuring settings for access control, security, and availability. Perform this procedure: Deploying a FortiAP device to a network on page 64
Task 5	Configure and customize FortiAP settings (for example, rogue scan). Perform this procedure: Configuring FortiAP settings on page 82

Task sequence	Description and procedure
Task 6	Create SSIDs and make them available on desired FortiAP devices. Perform this procedure: Adding an SSID to a network on page 101

Adding a FortiAP device to FortiLAN Cloud with a key

Use this procedure to add a FortiAP device to your FortiLAN Cloud account using its FortiLAN Cloud key (or multiple FortiAP devices with a bulk key).

If the FortiAP device does not have a FortiLAN Cloud key, then go to the Adding a FortiAP device to FortiLAN Cloud without a key on page 62 procedure.

Prerequisites

- Find the FortiLAN Cloud key printed on a sticker located on your FortiAP device.
- If you purchased a bulk key to add multiple FortiAP devices in a single import, then locate that bulk key on the purchase order (PO) from Fortinet.

Procedure steps

1. Using an Ethernet cable, connect the FortiAP device to a network that allows internet access.
2. Log in to FortiCloud and connect to FortiLAN Cloud.
3. On the Home page, navigate to **Devices > Inventory Devices**.
4. Click **Add APs**. If you have a bulk key, click **Bulk**.
5. Type the key.
6. Click **Submit**.
7. Make sure that the FortiAP device is added to the inventory list.
8. You can now go to the Managing Networks on FortiLAN Cloud on page 35 procedure.

Adding a FortiAP device to FortiLAN Cloud without a key

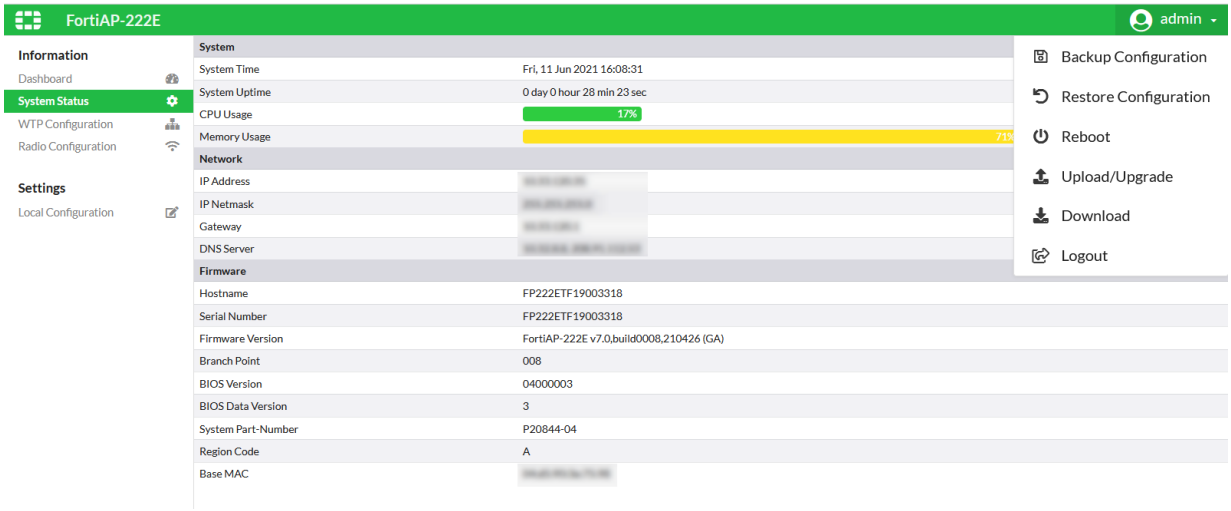
If the FortiAP device is an older model that does not have a sticker with the FortiLAN Cloud key, then use this procedure to add the FortiAP device to your FortiLAN Cloud account.

Prerequisites

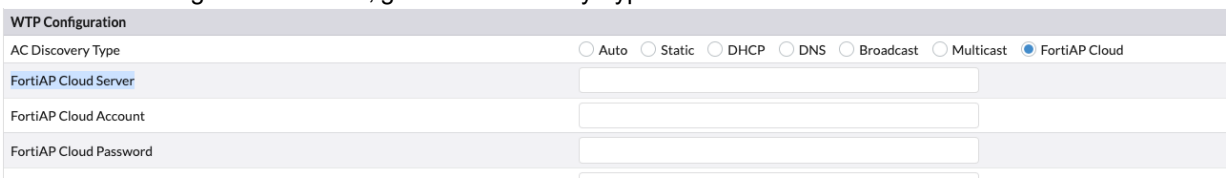
Take note of the model name and number of your AP and the firmware version you need to upgrade to (see Introduction on page 8).

Procedure steps

1. Download the FortiAP firmware:
   a. Start a web browser and visit the Fortinet Support website.
   b. Log in to your account.
   c. Click **Download > Firmware Images**.
   d. In **Select Product**, select the AP product to upgrade.
   e. Click the **Download** tab.
   f. Navigate to the firmware image file that you want to download. For example FAP_224D-v6-build0037-FORTINET.out.
   g. To save that firmware image file to your computer, go to the end of the row, click **HTTPS**, and follow the on-screen instructions.
   h. Take note of the path where you save the firmware image file.
2. Upgrade and configure the FortiAP device:
   a. Connect your computer to the FortiAP Ethernet port.
   b. The default IP address of the FortiAP device is 192.168.1.2. If your computer does not have an IP address on the same subnet, change the IP address of your computer to 192.168.1.3.
   c. Start a web browser and connect to https://192.168.1.2.
   d. Log in to the FortiAP UI as admin. Leave the **Password** field empty.
   e. In the **Status** section, go to **Firmware Version** and click **Update**.



   f. Follow the on-screen instructions to load and apply the firmware file.
   g. When you see the message "Uploading file is done. Firmware updating.", click **OK**, and close the web browser.
   h. After the upgrade is complete, start a web browser and connect to https://192.168.1.2.
   i. In the WTP Configuration section, go to AC Discovery Type and select **FortiAP Cloud**.



   j. Type the name and password of your FortiLAN Cloud account.
   k. Click **Apply**.
   l. Disconnect your computer from the FortiAP Ethernet port.

m. Restore your computer to its normal network configuration.
n. Using an Ethernet cable, connect the FortiAP device to a network that allows internet access.

3. Check FortiLAN Cloud for the newly added FortiAP device:
   a. Log in to FortiCloud and connect to FortiLAN Cloud.
   b. On the Home page, navigate to **Devices > Inventory Devices**.
   c. Make sure that the list includes the newly added FortiAP device.
4. You can now go to the Managing Networks on FortiLAN Cloud on page 35 procedure.

Deploying a FortiAP device to a network

Use this procedure to deploy a FortiAP device from your account inventory to your network.

Prerequisites

Complete the following procedures, as applicable:

- Adding a FortiAP device to FortiLAN Cloud with a key on page 62 or Adding a FortiAP device to FortiLAN Cloud without a key on page 62
- Managing Networks on FortiLAN Cloud on page 35

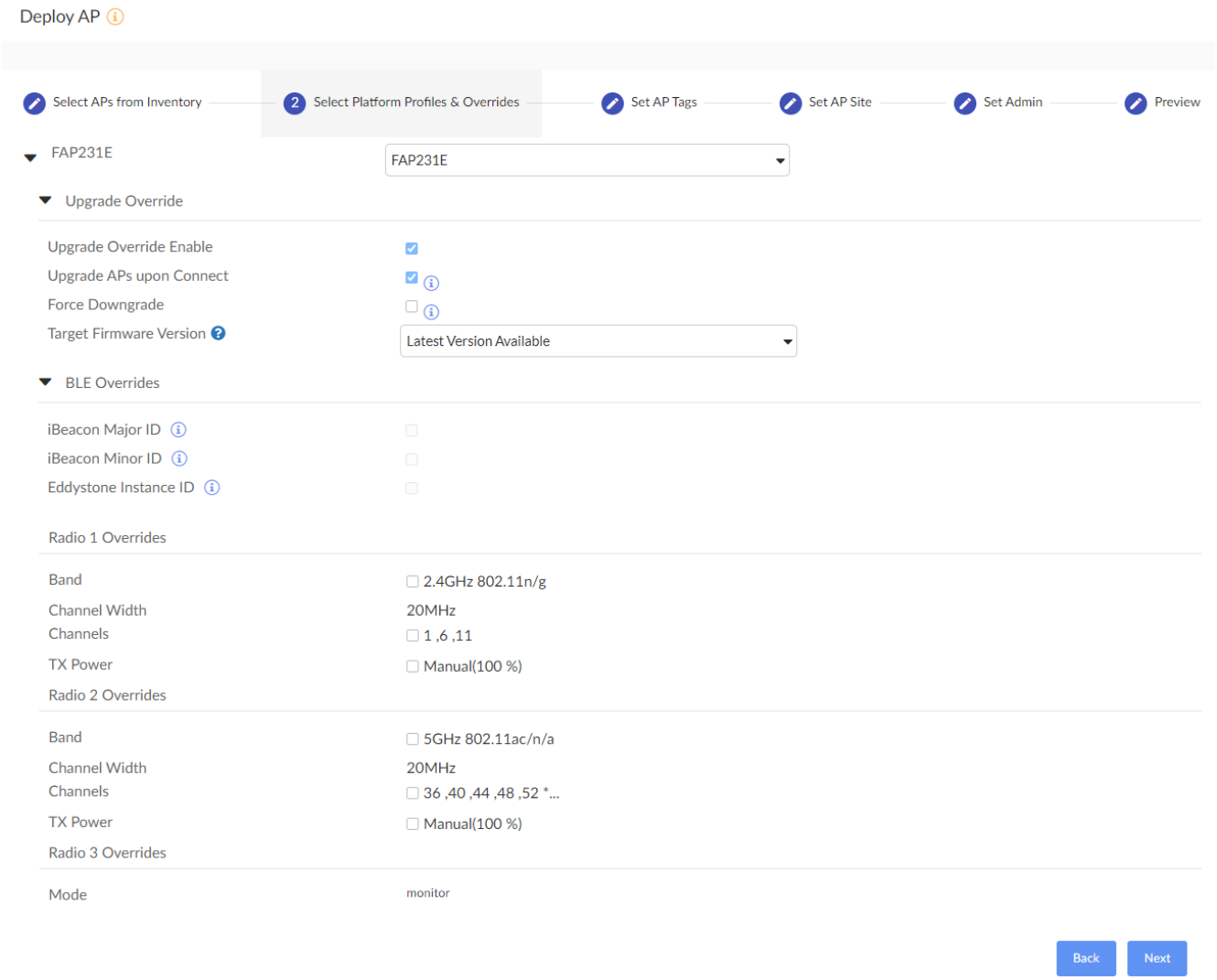
Procedure steps

1. Make sure that the window shows the network where you want to deploy the FortiAP device.
2. In the **Inventory Devices** tab, select the FortiAP and click **Actions > Deploy**. You can deploy the FortiAP to FortiLAN Cloud or to an external AP Controller. Select **Deploy to FortiLAN Cloud** and click **Deploy**. Select the network to deploy the FortiAP to and click **Deploy**.
3. In the Menu bar, click **Access points**.
4. In the Navigation pane, select **Status View**.
5. Verify that the table includes the deployed FortiAP device.

You can also deploy the FortiAP device from the **Wireless** menu.

1. In the Navigation pane, select **Deploy APs**; all FortiAP devices are listed.
2. In the table, select the FortiAP device(s) that you want deploy and follow the on-screen instructions in each section.

You can configure generic parameters and override specific access point settings in the **Select Platform Profiles & Overrides** section. To upgrade the FortiAP firmware upon discovery, enable **Upgrade APs upon Connect** and configure the desired firmware version. Optionally, you can also, chose the platform profile that already has this option enabled. See Overriding FortiAP Settings on page 84.



You can also select the AP tags, sites, and admin settings for the FortiAP that you are deploying. The FortiAP beacons the SSID with the specified parameters for wireless clients to connect. Review the information in the **Preview** section and click **Deploy**.

To undeploy a FortiAP, see Undeploying a FortiAP device on page 86.

Moving a FortiAP between accounts

You can move a FortiAP between different user accounts.

1. Login into the account with the FortiAP and undeploy the FortiAP from the account. See Undeploying a FortiAP device on page 86.
2. Remove the FortiAP from the account inventory.
3. Login into the account you want the FortiAP to be moved to.
4. Add the FortiAP to FortiLAN Cloud account with/without a key. See Adding a FortiAP device to FortiLAN Cloud with a key on page 62/Adding a FortiAP device to FortiLAN Cloud without a key on page 62.
5. Deploy the FortiAP to a network linked to this account. See Deploying a FortiAP device to a network on page 64.

Monitoring

The FortiLAN Cloud provides a comprehensive dashboard with detailed statistics and visualization for the overall network and subsequent levels such as AP, radio, client, and rogue devices. The information presented in the dashboard is pivotal for monitoring network health and for diagnostic purpose.

The dashboards are split into three views - **Standard**, **Charts**, and **List**. The standard view displays information as a combination of chart based and listed data. The charts and list view displays data only in a series of charts and columns respectively.

Note: You can filter the lists displayed based on specific parameters and hide others by modifying the column settings,  .

The dashboard data can be filtered using the location based AP sites created during deployment. The chart dashlets and columns are click-able to view detailed information; hover over these charts to view details.

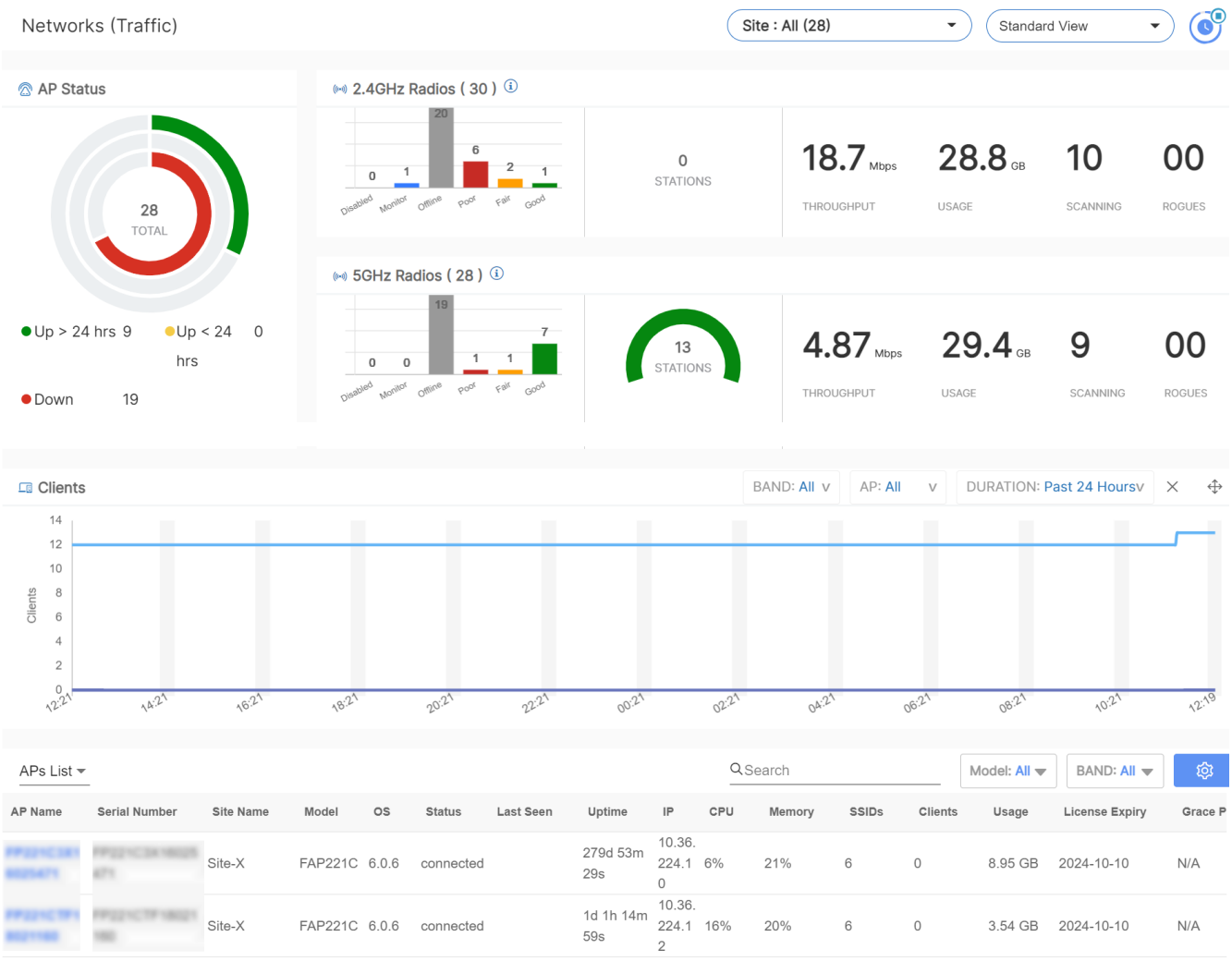
Dashboard data is refreshed every 60 seconds, you can refresh the dashboard as per requirement.

Note: The **Charts** view provides additional and varied data in comparison to the **Standard** view. The subsequent sections describe data fields displayed in all views.

- Network (Traffic)
- Network (Security)
- APs
- Radios
- Clients
- Neighbour APs
- BLE Devices

Network (Traffic)

This dashboard provides network traffic information arranged in several rows and charts.



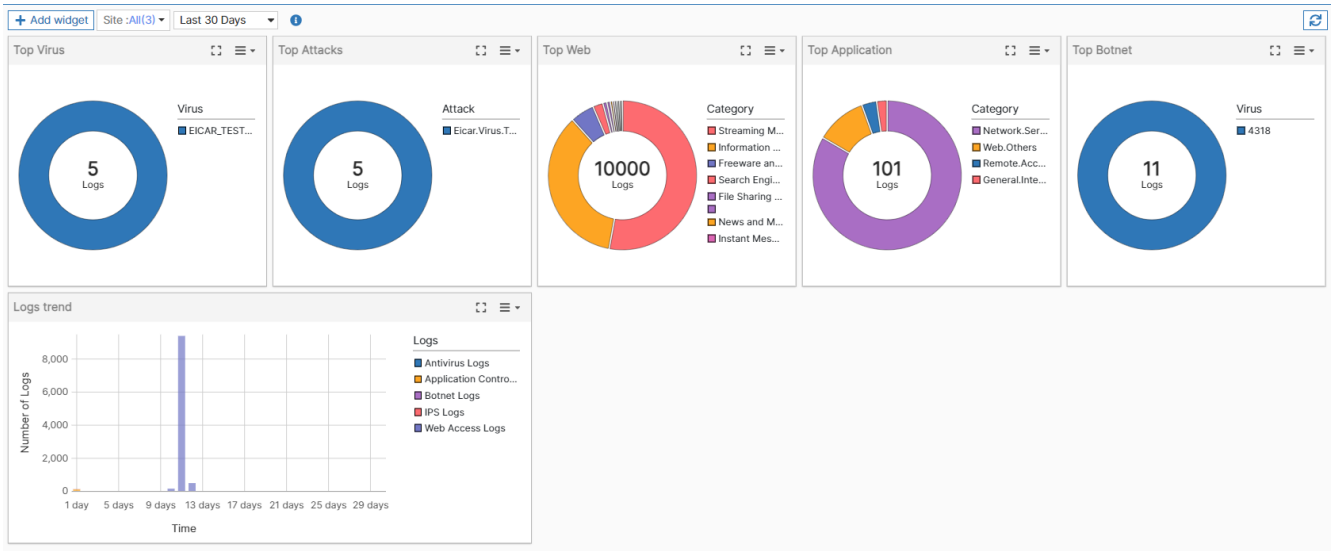
- **AP Status** counts the APs based on their connection status, APs up for more than 24 hours, APs up for less than 24 hours, and APs that are currently down.
- **2.4/5 GHz Radio** provides a summary for both 2.4 GHz and 5 GHz radios. Displays the radio modes (**Disabled**, **Monitor**, **Offline**) and health (**Poor**, **Fair**, **Good**), the station count, the total number of MAC errors, throughput, data usage, rogue APs, and APs in scan mode.
- **Clients** displays the number of clients for each of the 2.4 GHz and 5 GHz bands over the selected period of time.
- **Top 20 APs by Clients Count (2.4 GHz and 5 GHz)** displays the twenty APs with the highest number of clients connected to them in the 2.4 GHz and 5GHz bands.
- **Top SSIDs by Client Count** displays the five SSIDs with the highest number of clients connected to the SSID; counts the number of clients connected to each of these SSIDs and the total number of clients in the network. Filter data based on the band (2.4 GHz, 5 GHz, or both).
- **Top SSIDs by Usage** displays the five SSIDs with the highest data usage; counts the number of clients connected to each of these SSIDs and the total number of clients in the network. Filter data based on the band (2.4 GHz, 5 GHz, or both).
- **Top 20 Stations by Throughput** displays the 20 clients with the highest throughput.
- **Top 20 Stations by Usage** displays the 20 clients with the highest data usage.

Click on the AP, Radio, client, and SSID information to view details.

Network (Security)

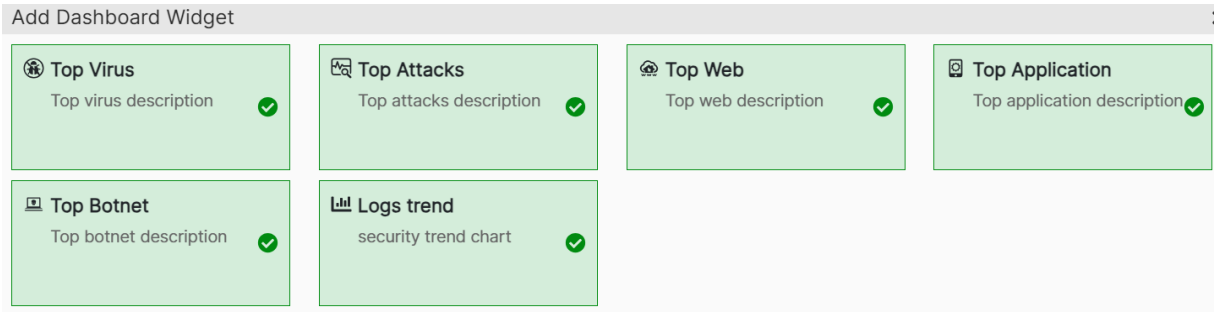
This dashboard provides network security information such as web applications, attacks, and viruses. The dashboard provides a summary of the 10,000 most recent security events for the chosen filters. For deeper insights into past events, please visit the **Logs** section for the event category of interest. See Logs.

The dashboard is divided into the following panels. You can view and analyze the log trends graphically for all the above detected security anomalies over a period of time.



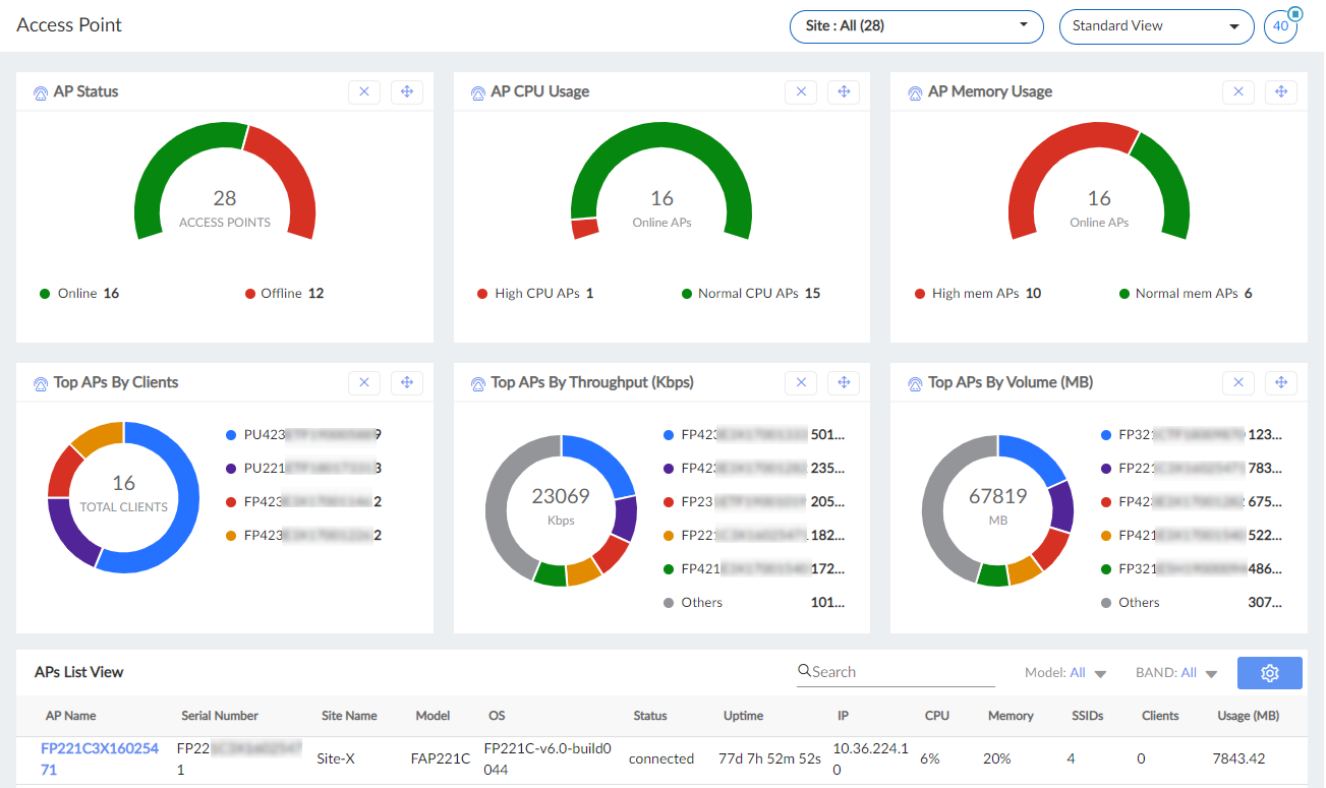
- **Top Web** - The top ten web categories that are most frequently used.
- **Top Attacks** - The top ten attacks that the FortiLAN Cloud's IPS most frequently prevents.
- **Top Viruses** - The top ten viruses that the FortiLAN Cloud's AV most frequently detects.
- **Top Application** - The top ten web categories that are most frequently used.
- **Top Botnet** - The top ten bots that the FortiLAN Cloud's monitoring function most frequently detects.

To add or remove the widgets from this page, click **Add widget**.



APs

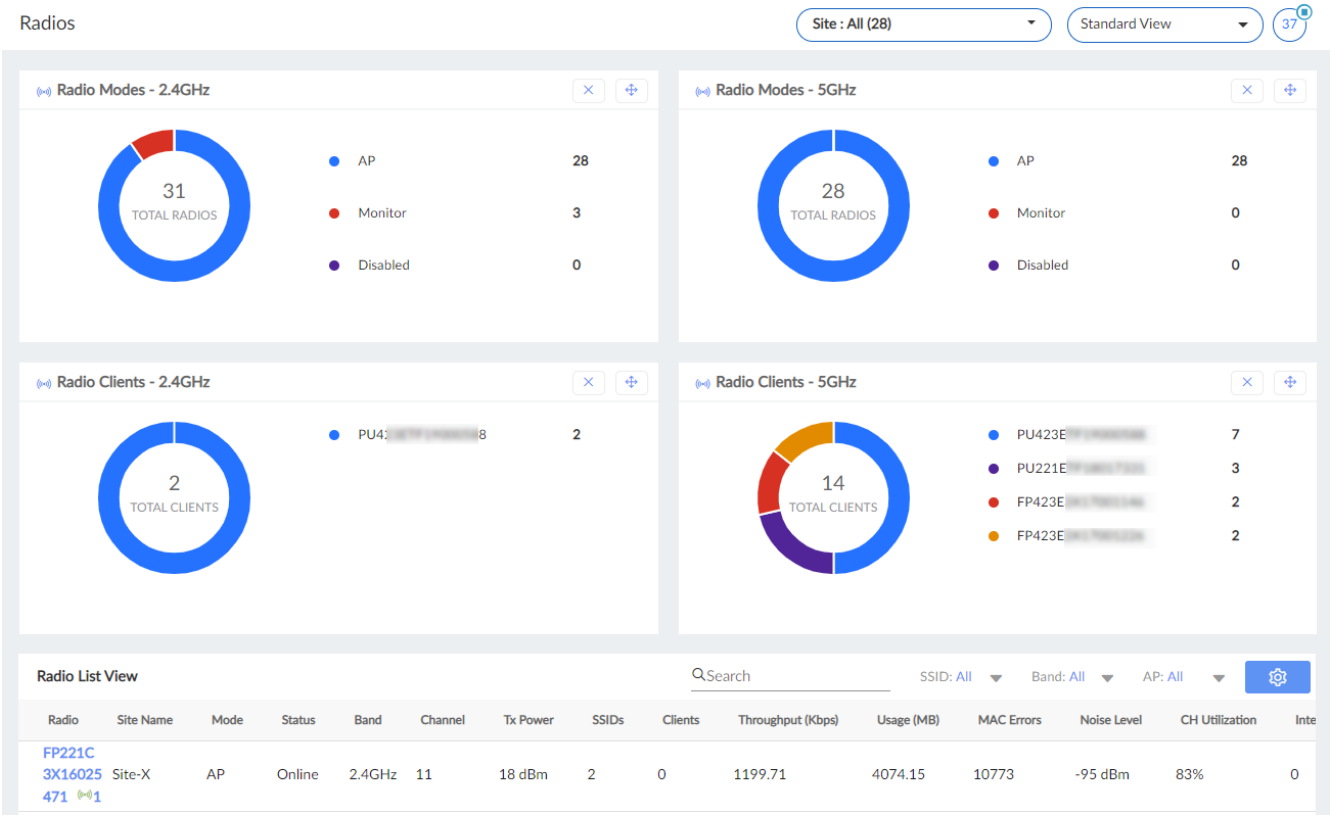
This dashboard provides visualization of APs in your network and their health and utilization.



- **AP Status** displays the APs based on their connection status, whether online or offline.
- **AP CPU Usage** categorizes all the APs into different buckets of high and normal CPU utilization.
- **AP Memory Usage** categorizes all the APs into different buckets of high and normal memory utilization.
- **Top APs by Clients** displays the five APs with highest number of clients connected to them; counts the number of clients connected to each of these APs and the total number of clients.
- **Top APs By Throughput** displays the five APs with highest throughput; displays the throughput for each of these APs and the aggregate throughput.
- **Top APs By Volume** displays the five APs associated with the highest data volume; displays the data volume for each of these APs and the total data volume.
- **Top APs by Interfering BSSIDs** displays the top most interfering APs' BSSIDs.
- **Top AP Group** displays the five AP groups with highest number of AP members; counts the number of APs in each of these AP groups and the total number of AP groups.
- **AP Advanced Management** categorizes all the APs based on whether they avail free service or are subscription services
- **Top AP Models** displays the five AP models mostly deployed in your network; counts the number of APs belonging to each of these AP models and the total number of AP models.
- **Top AP OS** displays the five FOS version most FAPs belong to; counts the number of APs belonging to each of these AP models and the total number of AP models.

Radios

The data displayed on this dashboard categorizes the 2.4 GHz and 5 GHz radios into the top most based on different criteria, highest number of clients, highest throughput, data volume, noise levels (dBm), channel distribution, interfering APs, radio types, and Tx power (dBm). Radio Modes counts the radios in the 2.4 GHz and 5 GHz modes based on the operating modes: AP, Disabled, and Monitor. Click on any of these to view the radio details.

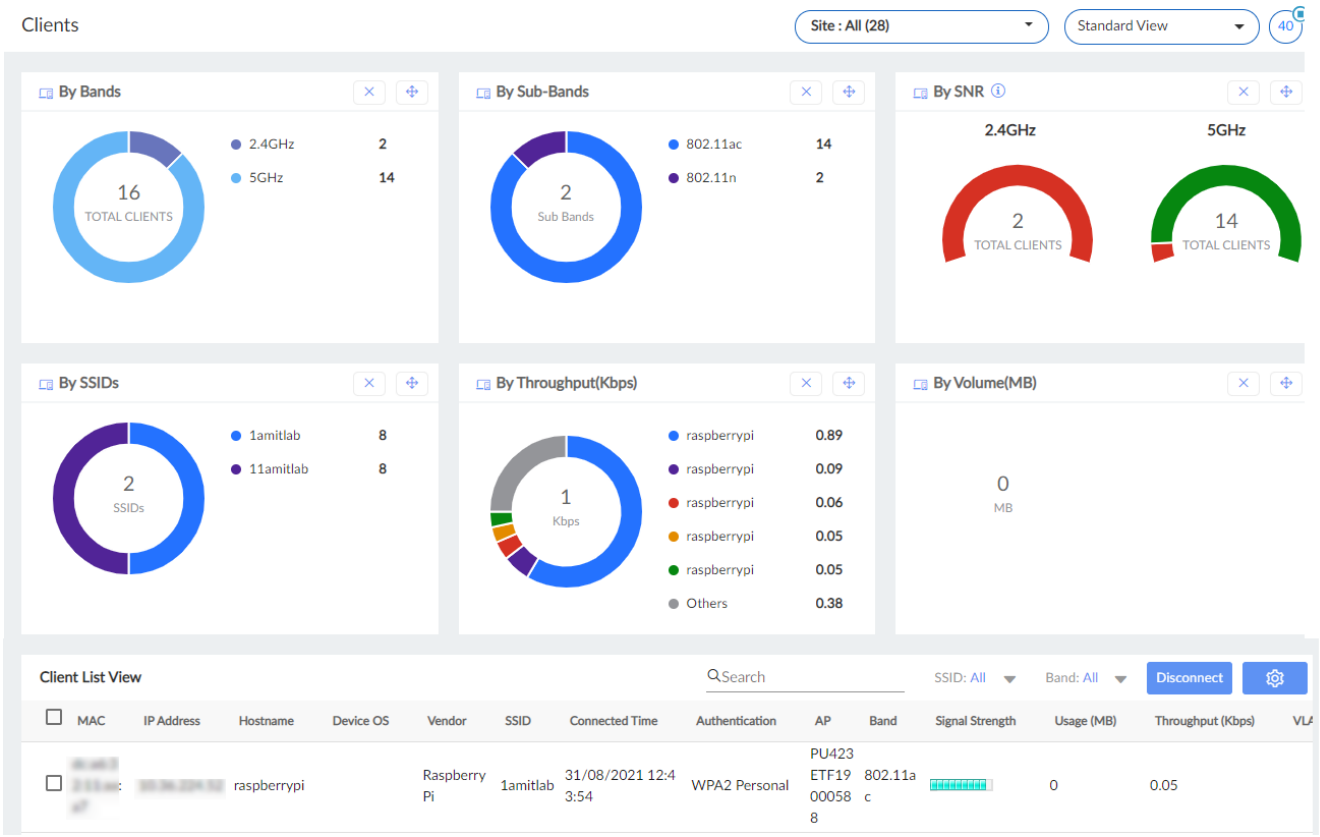


Click on any radio name to view the radio configuration and other associated details.

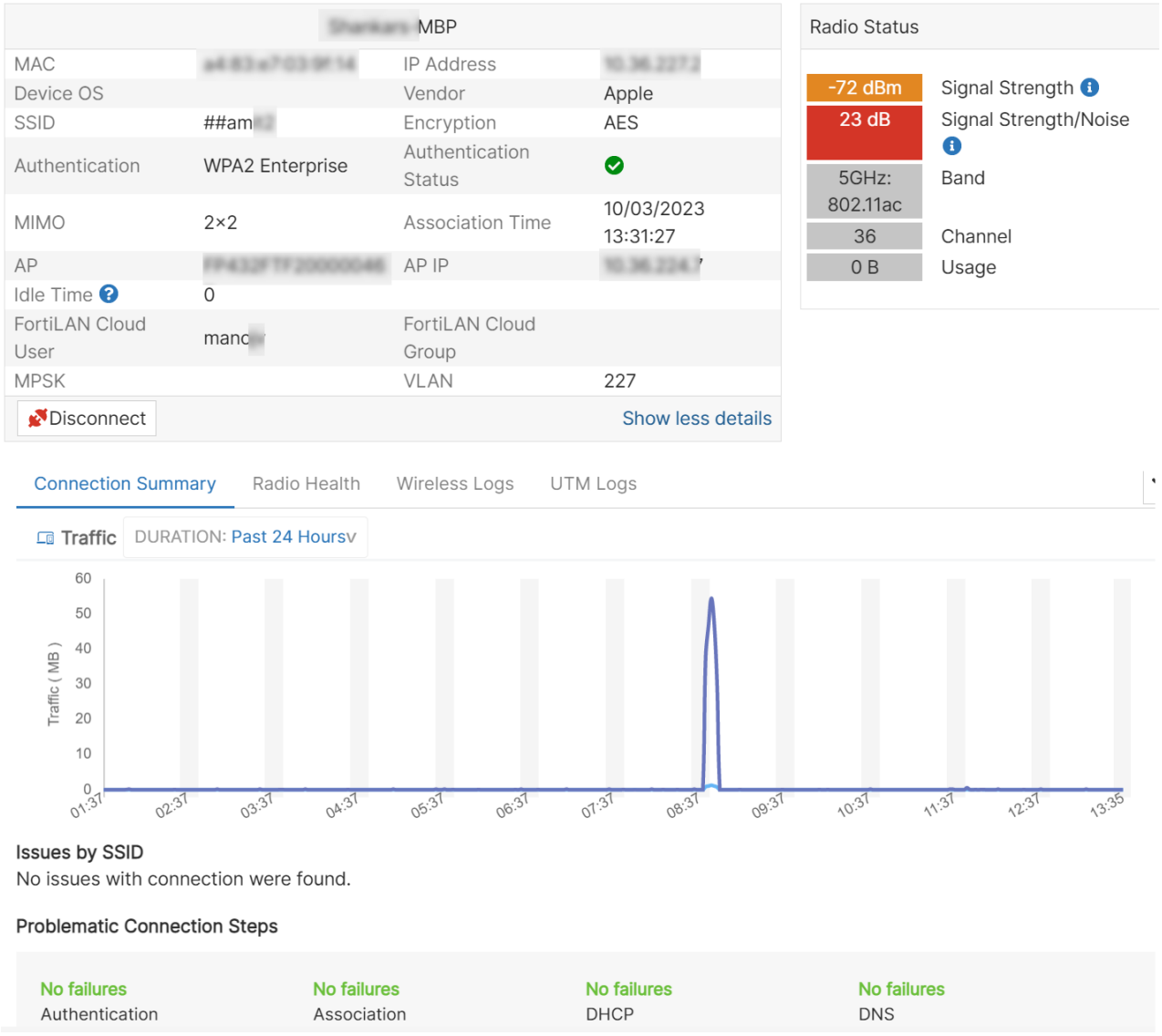
Clients

This tab lists the clients in your network with the associated information. The data displayed on this dashboard categorize the clients based on different criteria, bands and sub-bands used, SSIDs, SNR, highest throughput, data volume, VLAN, authentication mode, encryption mode, associated APs, number of channels, operating system, device types, and user groups. Click on the displayed data to view the client and other associated details. Click  for criteria based filtering of the columns, such as, user, MPSK, group, channel etc.

You can disconnect a wireless client from the wireless network. However, the disconnected wireless clients may connect back when operating in auto-connect mode or one manually connects the client.



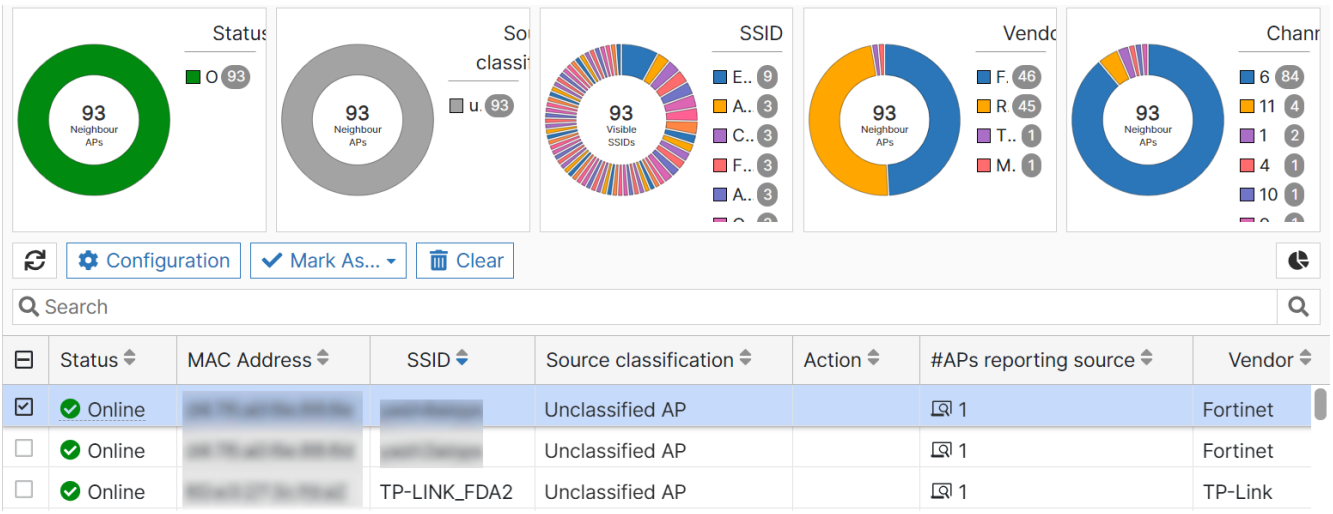
You can drill-down to view a single pane with all information and operations, related to a connected wireless client. This aids in quick troubleshooting.



Neighbour APs

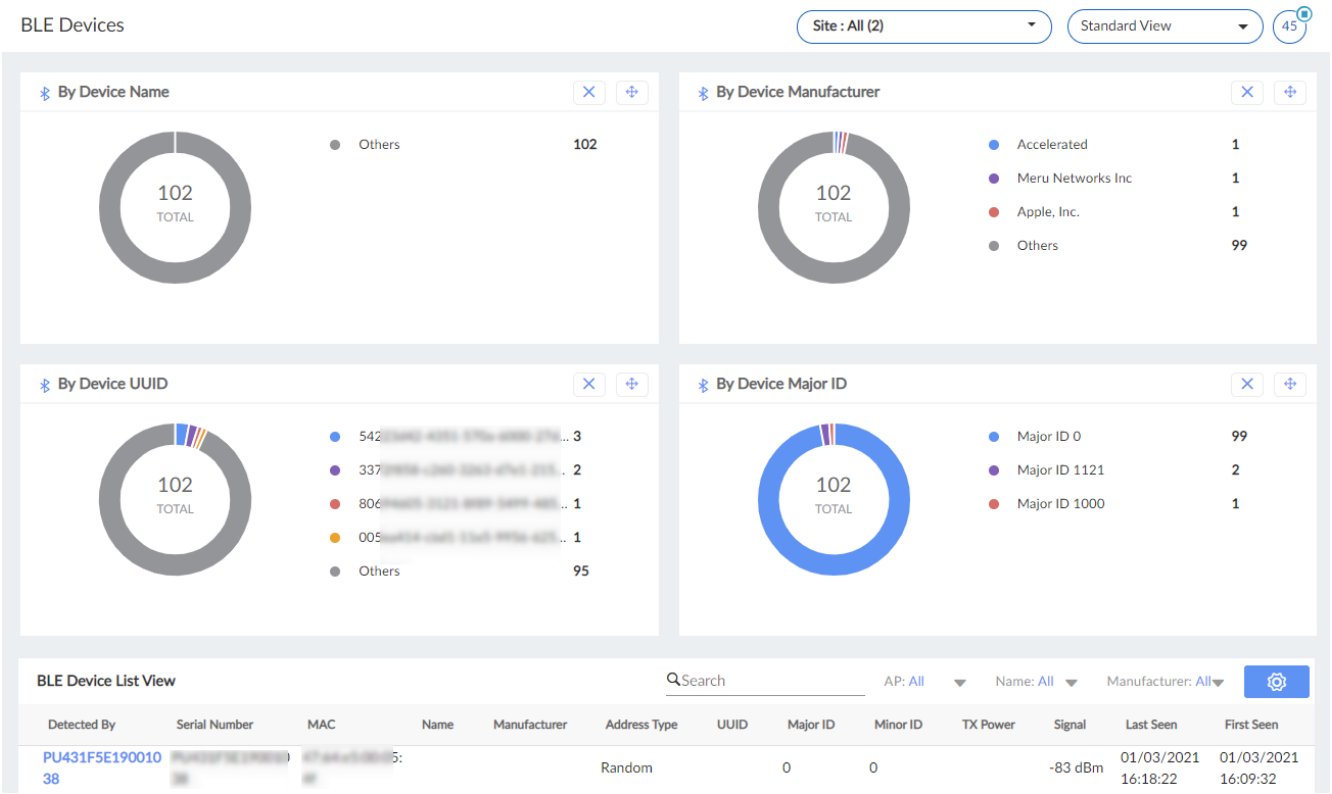
This tab displays any neighboring APs (rogue and interfering APs) that might be present in your network. The dashboard displays the sources of interference that can be from the same network (Infrastructure) or a rogue device. The data is organized in widgets and tabular format. You can filter the required data easily and categorize multiple FortiAPs.

The data displayed on this dashboard categorizes the APs based on different criteria, class (*Rogue AP, Accepted AP, Unclassified AP*), SSIDs, signal strength, the radios detected by, channel used, authentication modes, vendors, etc. Click on the charts to view the specific devices and other associated details.



BLE Devices

This dashboard displays devices detected over Bluetooth Low Energy (BLE) with associated details such as the configured UUID, Major ID, and the device name and manufacturer. Click on the displayed data to view the devices and other details.



Access Points

This section includes the following procedures to deploy, configure, and manage access points in FortiLAN Cloud:

Viewing the FortiAP status

The status view provides vital information about the FortiAP health. It organizes data in various tabs with configuration and operational status of the FortiAP and its radios. Information is classified into charts and lists.

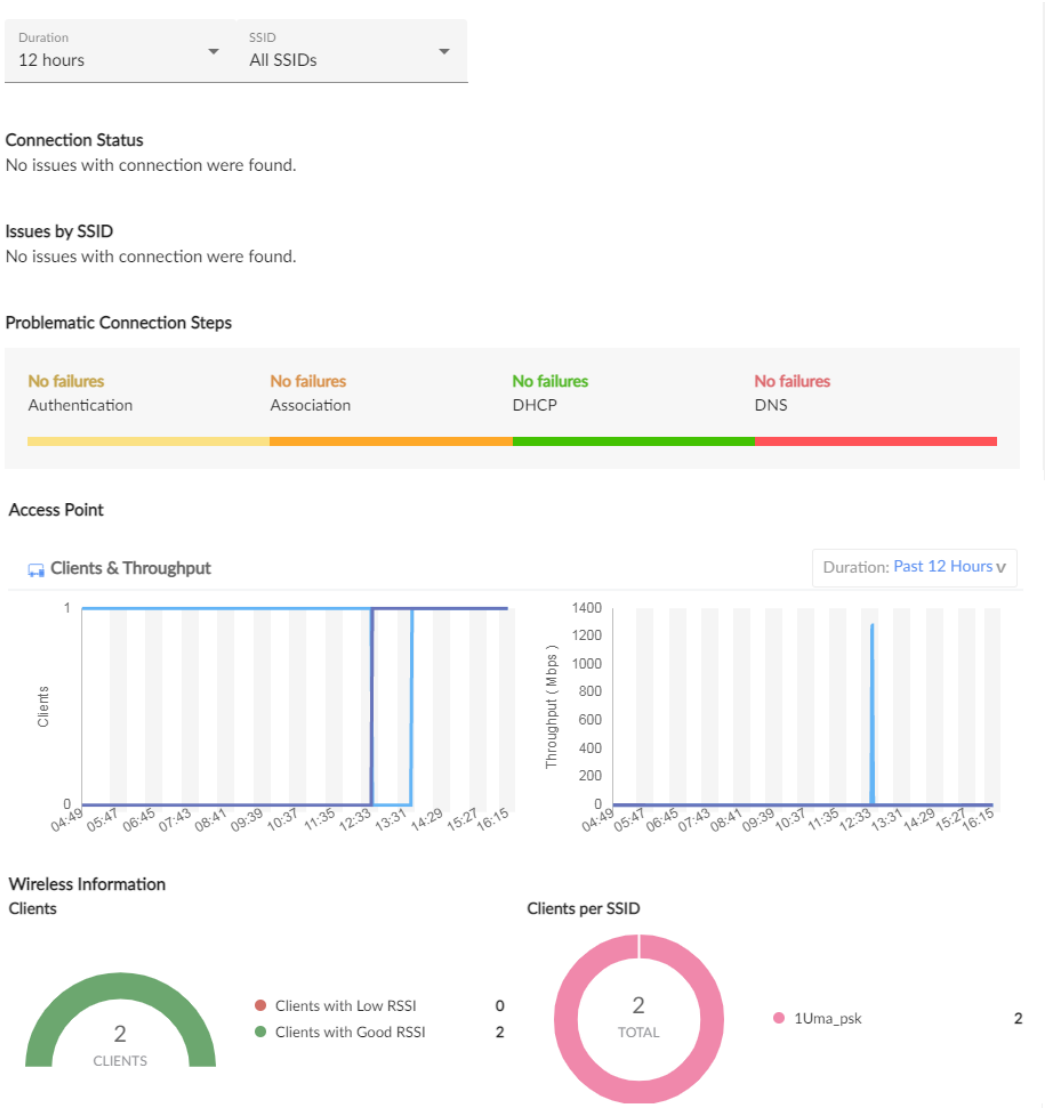
Procedure steps

1. In the Menu bar, click **Access Points**.
2. In the Navigation pane, click **Status View**.
3. Click on an access point to view its status.

Summary

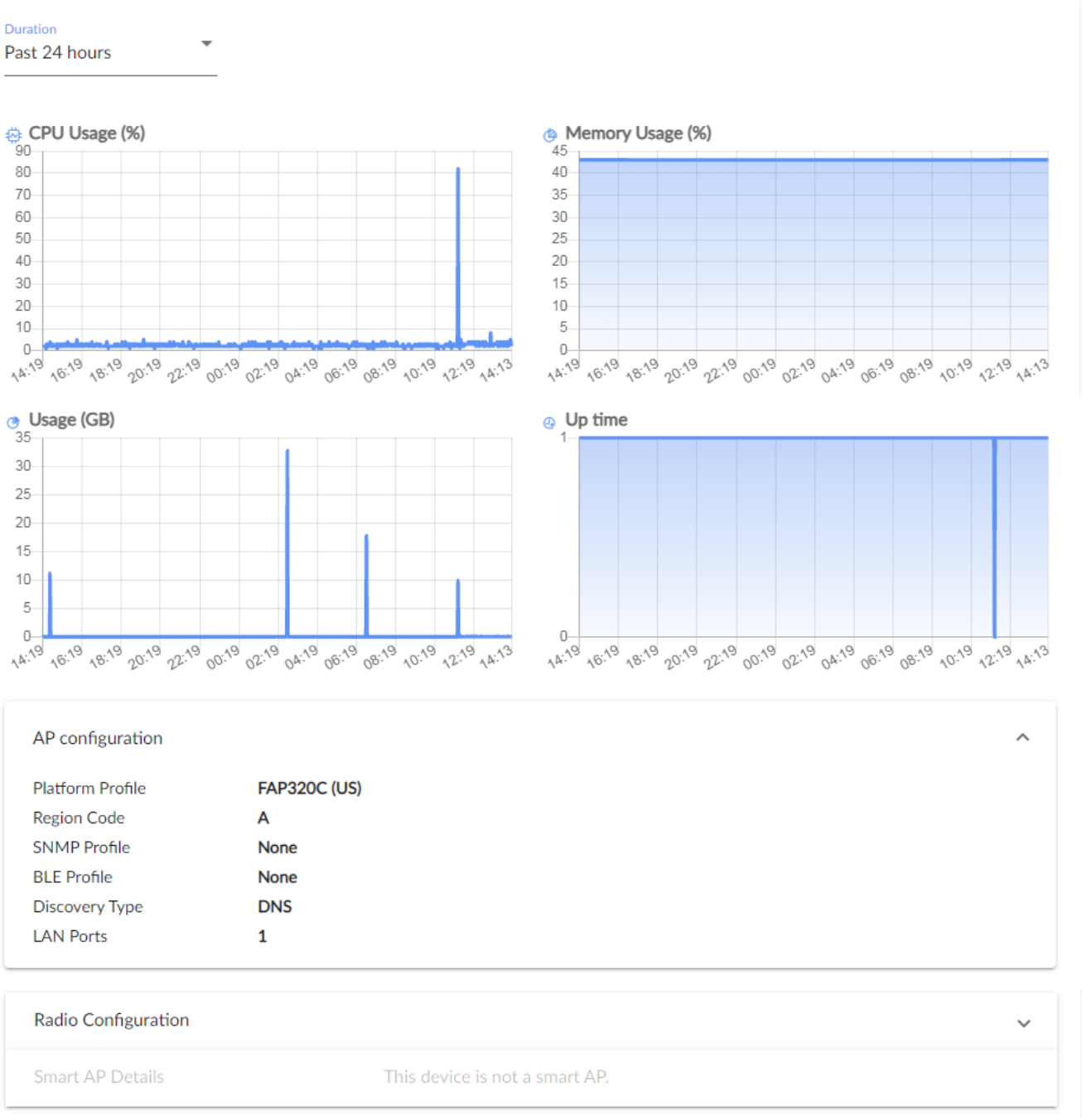
This tab displays the FortiAP and wireless client summary, by default, data for the last 12 hours is displayed. You can filter information for specific SSIDs; the client count affected by connection issues and the **Association**, **Authentication**, **DHCP**, and **DNS** failures are listed. The graphs display the FortiAP aggregate throughput (uplink and

downlink) and the client count for the selected duration. Wireless information such as the client count with good and low RSSI values and clients per SSID are also displayed.



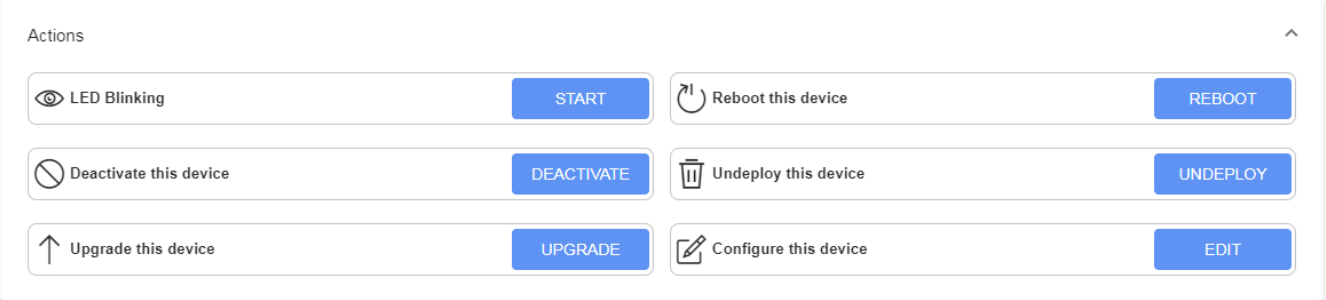
AP

This tab displays the aggregate data usage (uplink and downlink), the FortiAP uptime, Platform profile details, and radio configuration (overridden parameters are highlighted).



You can perform the actions on the FortiAP.

- Reboot
- Upgrade
- Deactivate
- Undeploy
- LED blinking
- Configuration edit



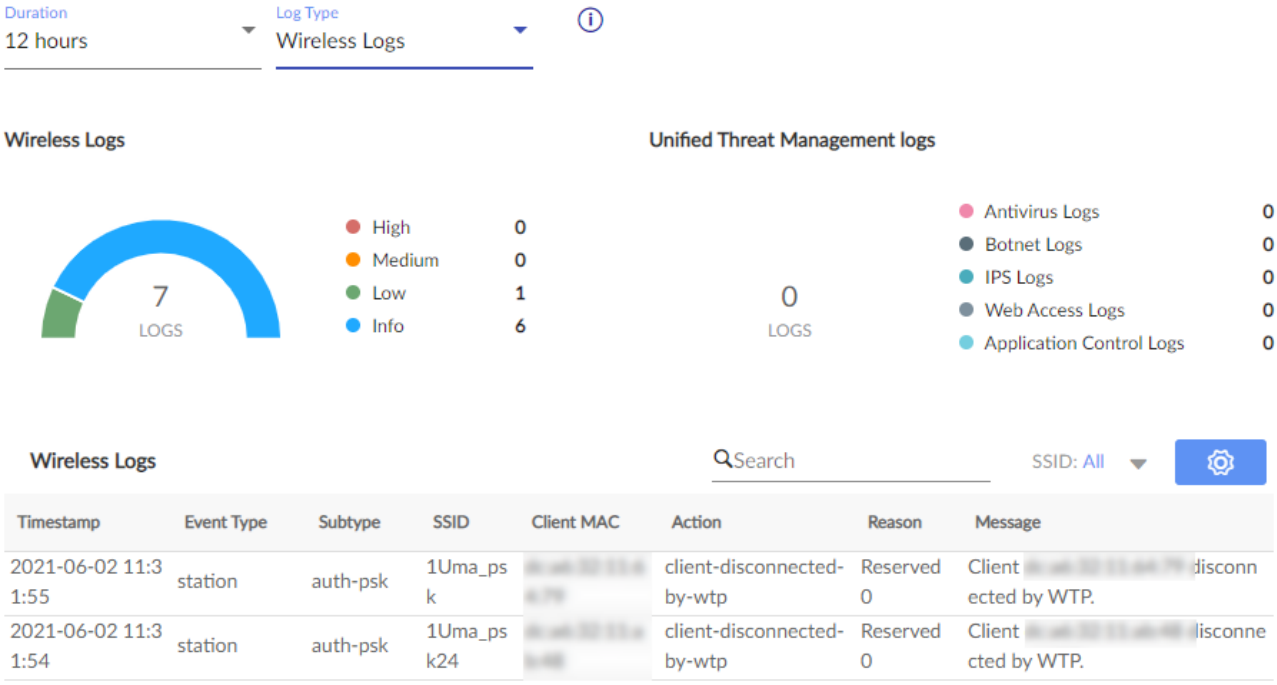
Logs

This tab displays the following logs associated with the FortiAP.

- Wireless Logs
- Antivirus Logs
- Application control Logs
- Botnet Logs
- IPS Logs
- Web Access Logs

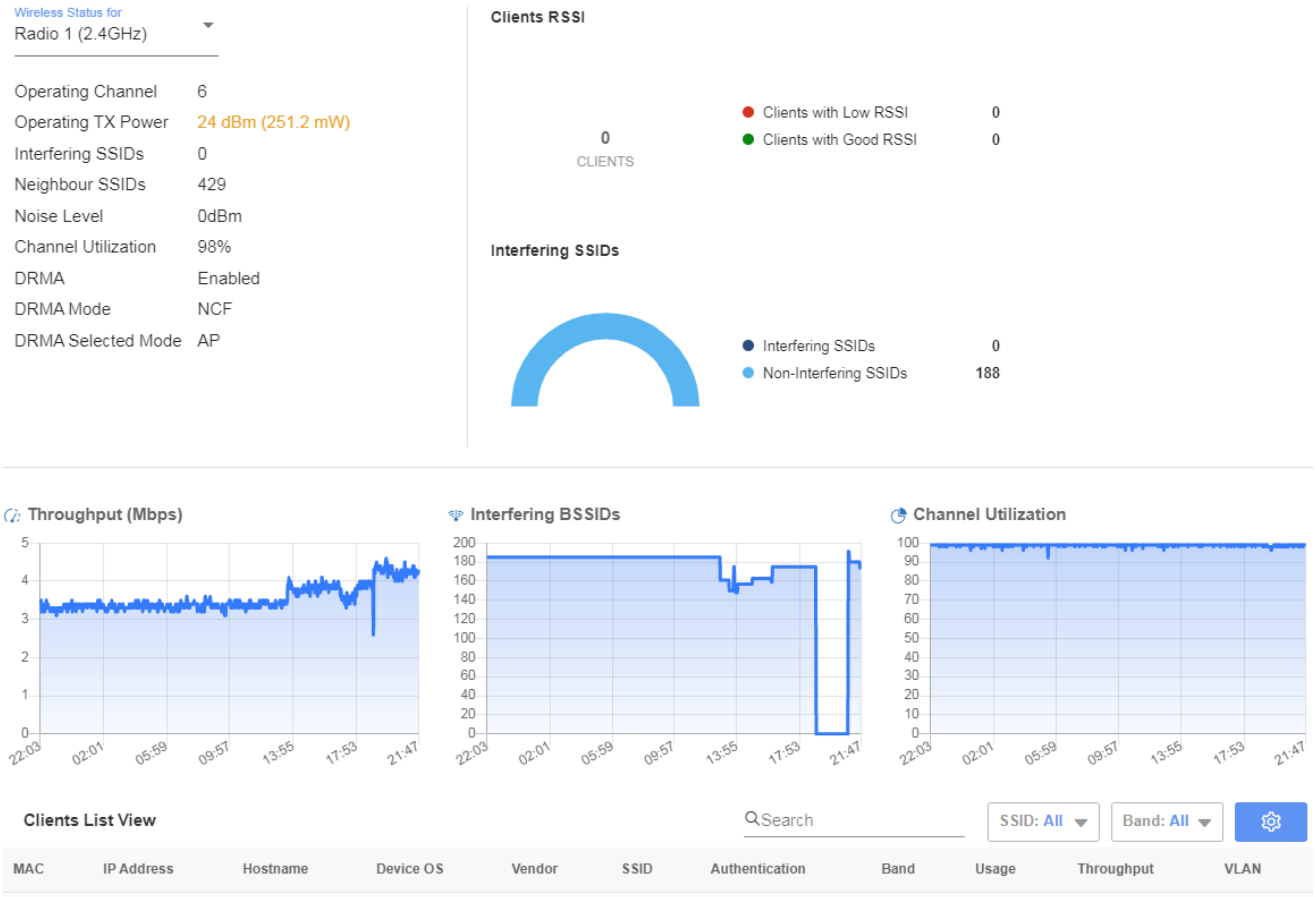
You can set the duration to view FortiAP logs, by default, logs are displayed for the last 12 hours. The donut charts display the number of logs based on their severity; **High**, **Medium**, **Low**, and **Info**.

Note: The FortiAP must have a UTP license to access all logs except **Wireless Logs**.



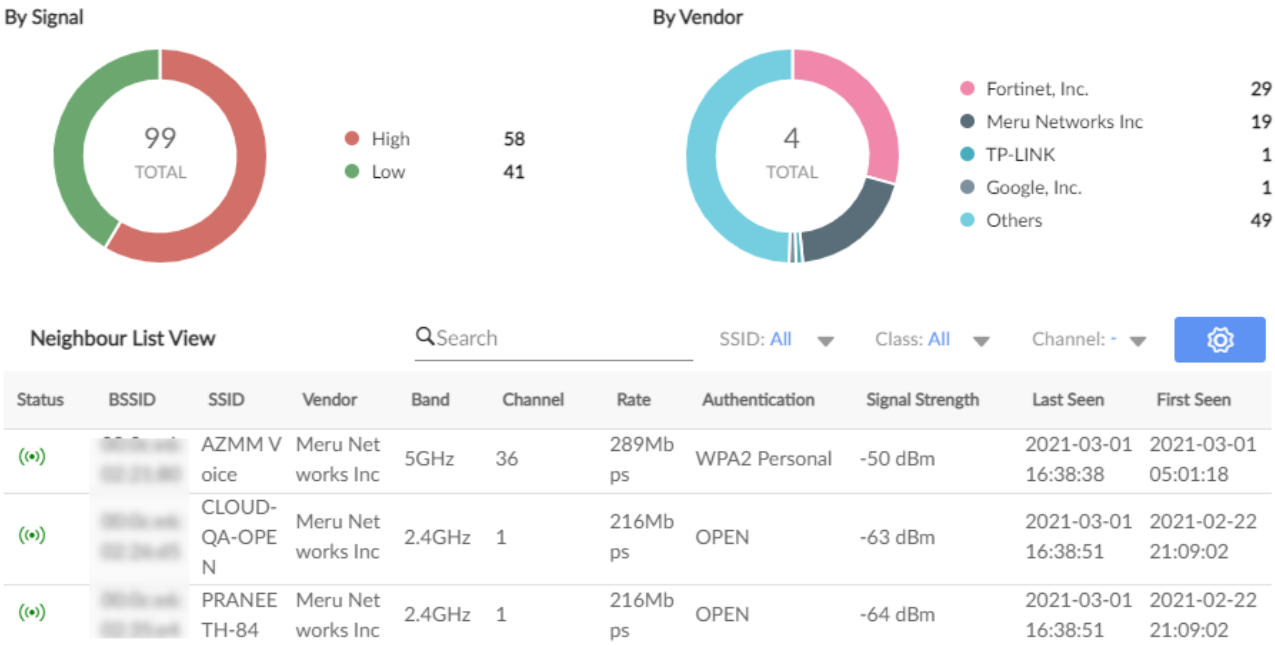
Radio

This tab displays wireless statistics and the list of wireless clients. You can select any one of the 3 radios to view the associated details. The charts display the client count with good and low RSSI values, interfering and non-interfering APs' count, throughput (Mbps), interfering APs' BSSIDs, and the channel utilization.



Neighbour APs

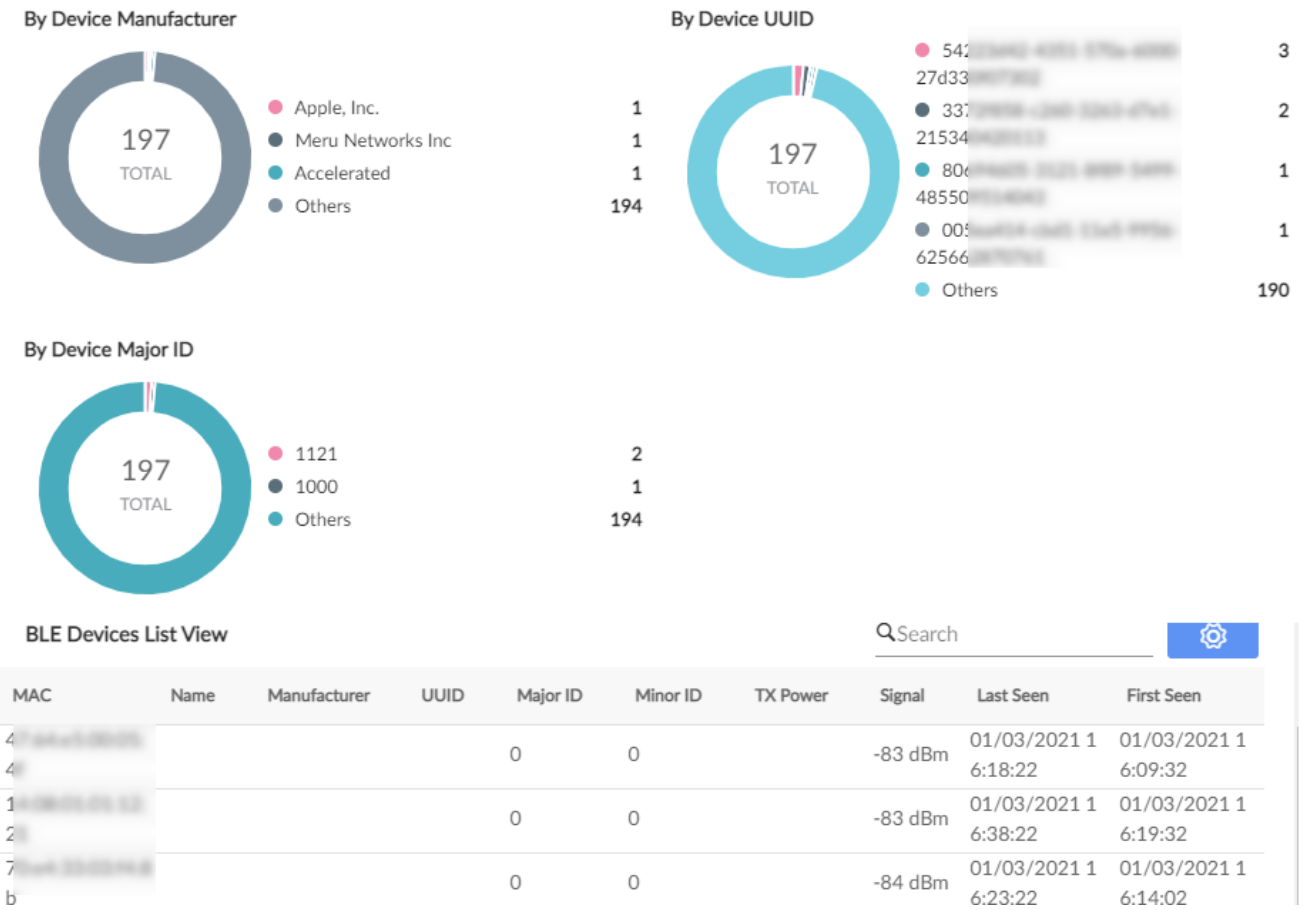
This tab displays any neighboring APs detected by this FortiAP and visualizes data on the basis of signal strength and vendor. Click on the displayed data to view the devices and other associated details.



Status	BSSID	SSID	Vendor	Band	Channel	Rate	Authentication	Signal Strength	Last Seen	First Seen
((•))	[redacted]	AZMM Voice	Meru Networks Inc	5GHz	36	289Mbps	WPA2 Personal	-50 dBm	2021-03-01 16:38:38	2021-03-01 05:01:18
((•))	[redacted]	CLOUD-QA-OPEN	Meru Networks Inc	2.4GHz	1	216Mbps	OPEN	-63 dBm	2021-03-01 16:38:51	2021-02-22 21:09:02
((•))	[redacted]	PRANEETH-84	Meru Networks Inc	2.4GHz	1	216Mbps	OPEN	-64 dBm	2021-03-01 16:38:51	2021-02-22 21:09:02

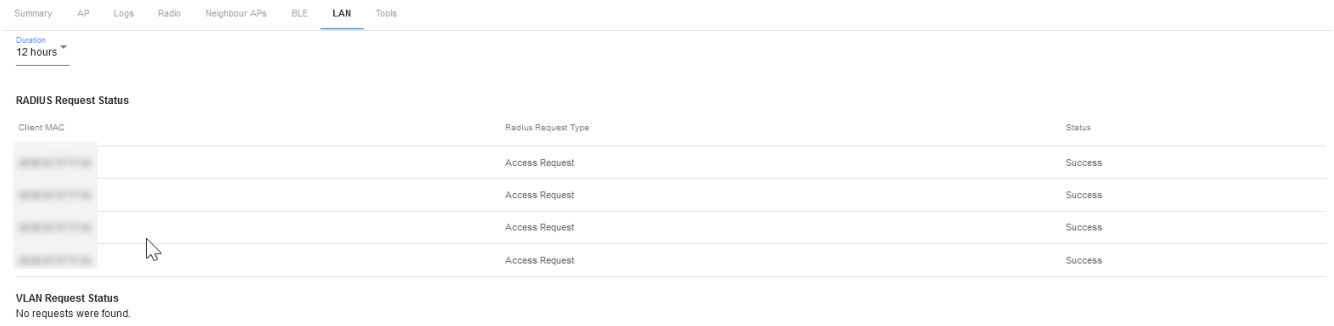
BLE

This tab displays devices detected over BLE with associated details such as the configured UUID, Major ID, and the device manufacturer. Click on the displayed data to view the devices and other details.



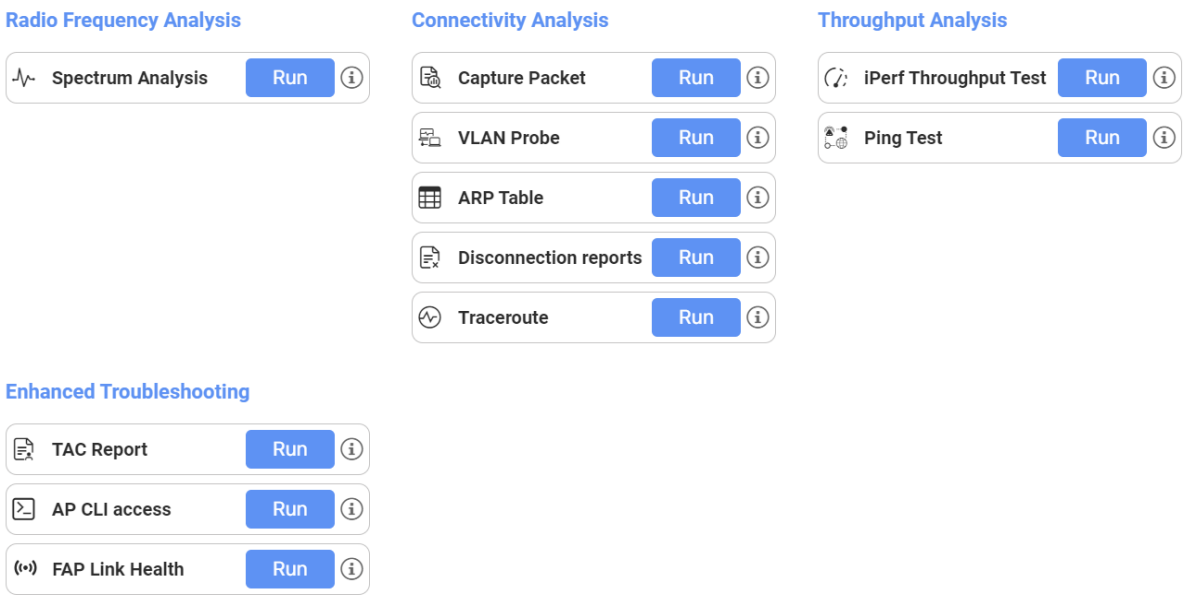
LAN

This tab displays the RADIUS and VLAN request status.



Tools

This tab displays the functionalities/utilities that you can run on the FortiAP. These are available in **Edit View > Tools**.



Upgrading a FortiAP device

Use this procedure to upgrade the firmware on one or more FortiAP devices.

FortiLAN Cloud downloads the firmware to the FortiAP device.

During a FortiAP firmware upgrade, there is a service interruption because the FortiAP device needs to reboot.

Procedure steps

1. In the Menu bar, click **Access Points**.
2. In the Navigation pane, click **Edit View**.
3. To set the firmware upgrade for a single FortiAP device:
   a. In the table, locate the FortiAP device that you want to upgrade. Click on the **AP Actions** tab and select **Upgrade Firmware**.
   b. Select the build and schedule.
   c. To save changes, click **Apply**.
4. To set the firmware upgrade for multiple FortiAP devices:
   a. In the table, select checkboxes for all the FortiAP devices that you want to upgrade.
   b. Click **Edit Configuration** > **AP Actions** > **Upgrade Firmware**.
   c. For each FortiAP device, select the build and schedule.
   d. To save changes, click **Apply**.

Rebooting a FortiAP device

Use this procedure to reboot one or more FortiAP devices.

FortiAP devices will need to reboot during a FortiAP firmware upgrade.

Procedure steps

1. In the menu bar, click **Access Points**.
2. In the navigation pane, click **Edit View**.
3. In the table, locate the row for the FortiAP device to configure. Click on the **AP Actions** tab and select **Reboot AP**.
4. You may have to wait a few minutes before the AP is successfully rebooted.

Activating/Deactivating a FortiAP device

Use this procedure to activate a FortiAP device.

Procedure steps

1. In the menu bar, click **Access Points**.
2. In the navigation pane, click **Edit View**.
3. In the table, locate the row for the FortiAP device to configure. Click on the **AP Actions** tab and select **Activate AP**/**Deactivate AP**.
4. The status of the AP changes to **Not Activated**/ **Online** as per the action.

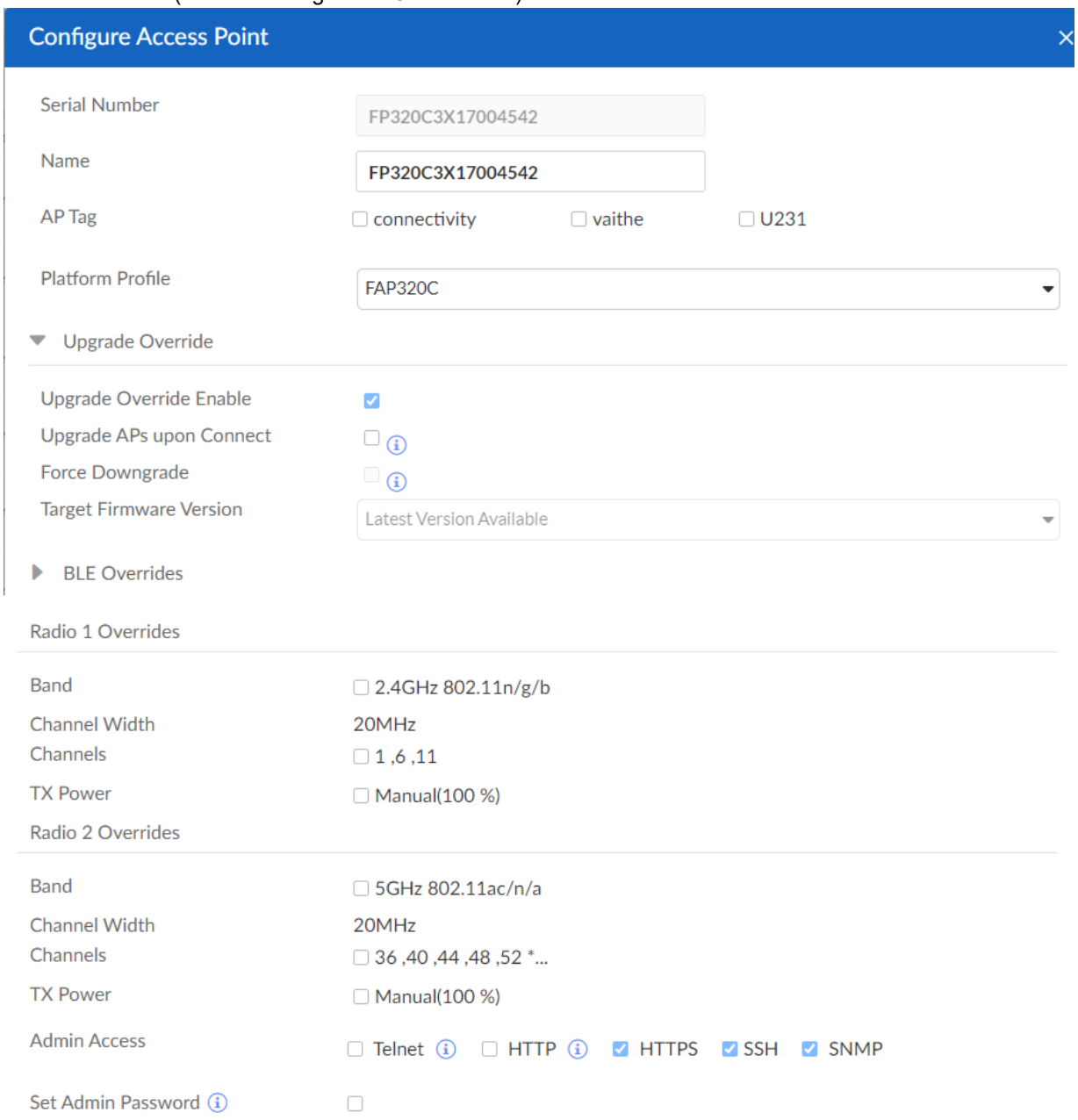
Configuring FortiAP settings

Use this procedure to modify the settings of a FortiAP device.

Procedure steps

1. In the menu bar, click **Access Points**.
2. In the navigation pane, click **Edit View**.
3. In the table, locate the row for the FortiAP device. At the end of that row, click on the **Edit** icon and to configure/edit the AP settings. When you edit/configure a FortiAP device, you can apply or change the following settings.
   - Name
   - AP Tag - Select the tag to apply to the FortiAP. See Adding AP tags.
   - Platform Profile - Use the default profile or a custom profile. See FortiAP Platform Profile on page 119.
   - Overrides (Upgrade, BLE, and radio) - Configure platform profile overrides. See Overriding FortiAP Settings on page 84.
   - Admin Access (Telnet, HTTP, HTTPS, SSH, SNMP)

- Admin Password (maximum length is 128 characters)



4. To save the changes, click **Apply**.

Changing FortiAP settings

Use this procedure to change the settings of a FortiAP device.

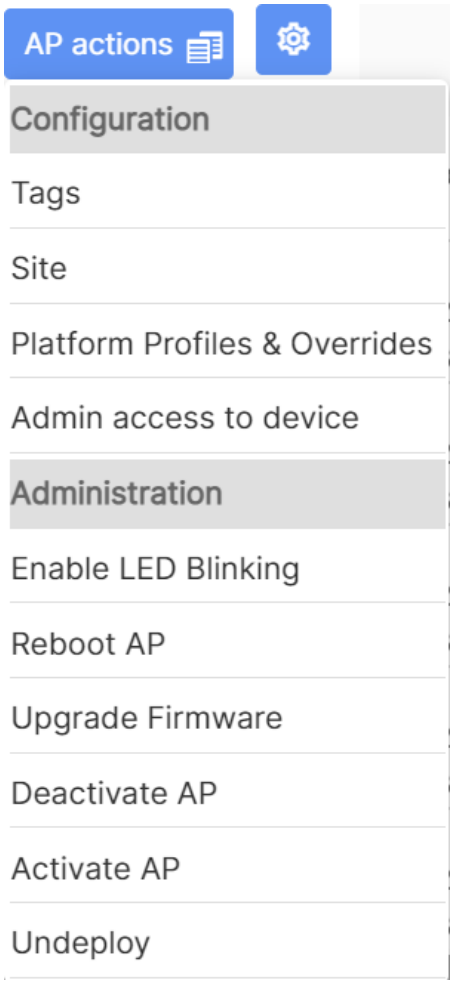
When you configure a FortiAP device, you can apply or change the following settings:

- Tags
- Sites

- Platform Profiles (Use the default profile or a custom profile. See the FortiAP Platform Profile on page 119 procedure) and Overrides (See the Overriding FortiAP Settings on page 84 procedure.)
- Admin (Telnet, HTTP, HTTPS, SSH, SNMP) and Admin Password
- Firmware (See the Upgrading a FortiAP device on page 81 procedure.)
- Undeploy (See the Undeploying a FortiAP device on page 86 procedure.)

Procedure steps

1. In the menu bar, click **Access Points**.
2. In the navigation pane, click **Edit View**.
3. In the table, locate the row for the FortiAP device to configure and click on the **AP Actions** tab.

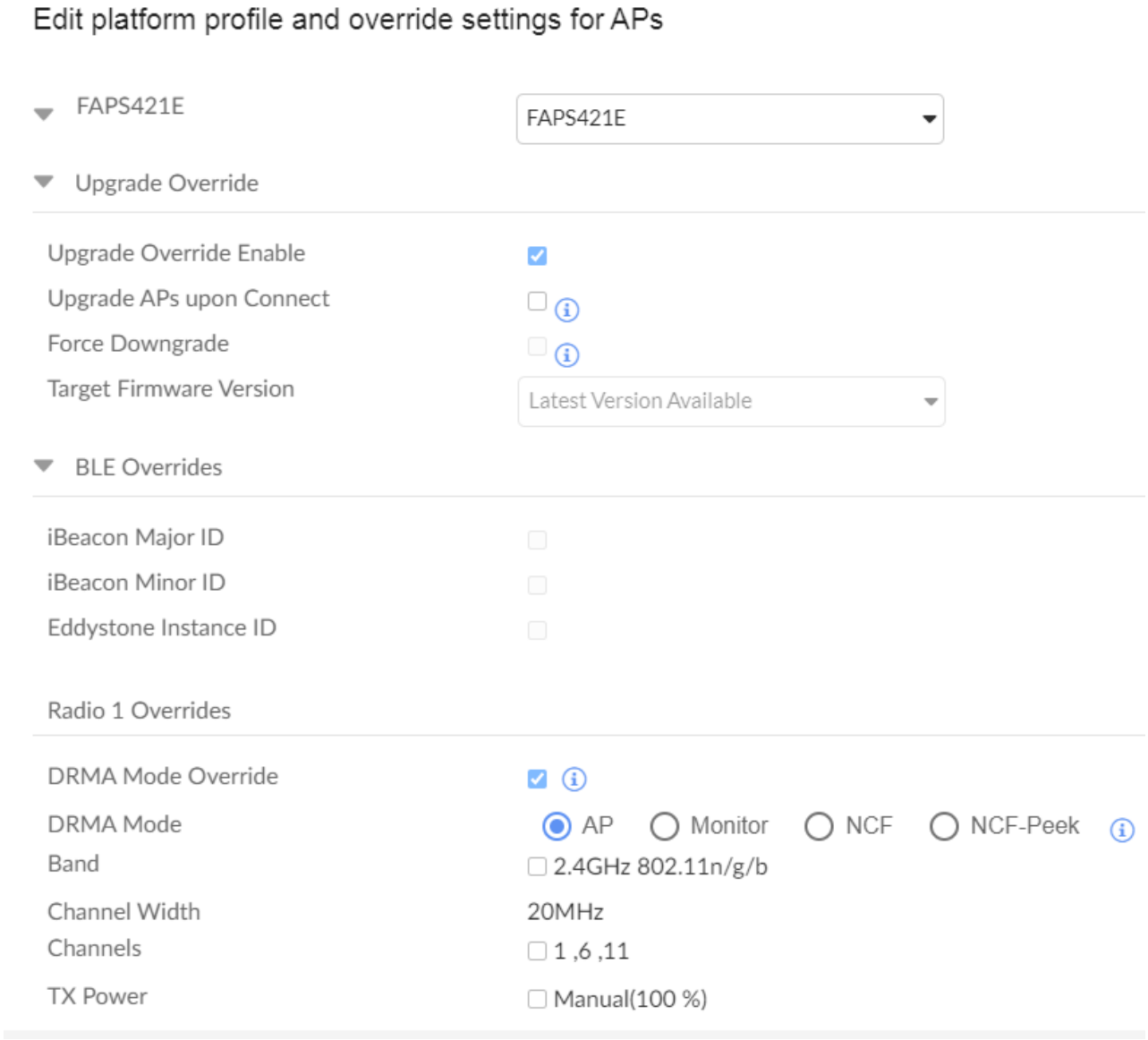


4. Edit settings as required.
5. To save the changes, click **Apply**.

Overriding FortiAP Settings

The FortiAP Platform profile settings can be overridden. For more information, see FortiAP Platform Profile on page 119.

1. In the menu bar, click **Access Points**.
2. In the navigation pane, click **Edit View**.
3. In the table, locate the row for the FortiAP device to update and click on the **AP Actions** tab and select **Platform Profiles and Overrides**. You can override the upgrade, BLE, and radio configurations. For more information on these parameters, see FortiAP Platform Profile on page 119.



4. Select the parameters to be modified and enter the new values. The DRMA Mode Override setting forces the radio into the AP or monitor mode. Enable it and select the any of the following DRMA modes to apply to the radio.
   - **AP** – Set the radio to AP mode.
   - **Monitor** – Set the radio to Monitor mode.
   - **NCF** – Select and set the radio mode based on NCF score.
   - **NCF Peek** – Select the radio mode based on NCF score, but do not ap ply.

When **NCF** or **NCF Peek** is selected, you can view the target mode selected by the NCF algorithm in the **Radio** tab of Viewing the FortiAP status.

You can configure also overrides during FortiAP deployment.

1. In the menu bar, click **Deploy APs**.
2. Select the FortiAP device to update and select **Select Platform Profiles and Overrides**.
3. Select the parameters to be modified and enter the new values.
   See section Deploying a FortiAP device to a network on page 64.

Undeploying a FortiAP device

When you undeploy a FortiAP device, FortiLAN Cloud removes the device from a network and then returns this device to the AP Inventory list. You can then deploy that device to another network or delete it from FortiLAN Cloud.

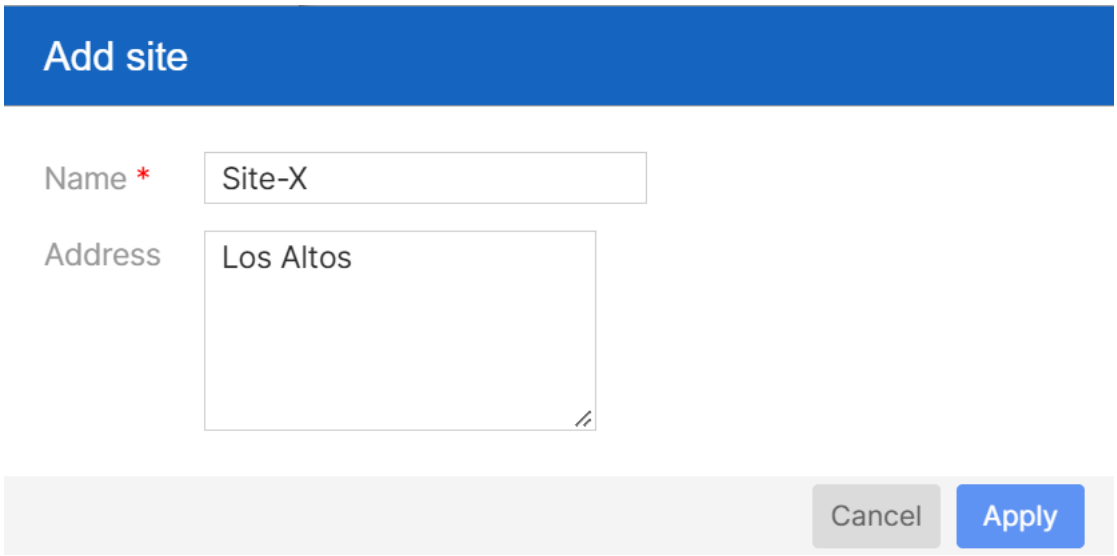
Procedure steps

1. Go to the network that has the FortiAP device that you want to undeploy.
2. menu bar, click **Access Points**.
3. In the navigation pane, click **Edit View**.
4. In the table, locate the FortiAP device that you want to undeploy. Click on the **AP Actions** tab and select **Undeploy**.
5. Click **Yes**.
6. Go to the FortiLAN Cloud Home page and click **Inventory**.
7. Make sure that the FortiAP device is in the AP inventory list.

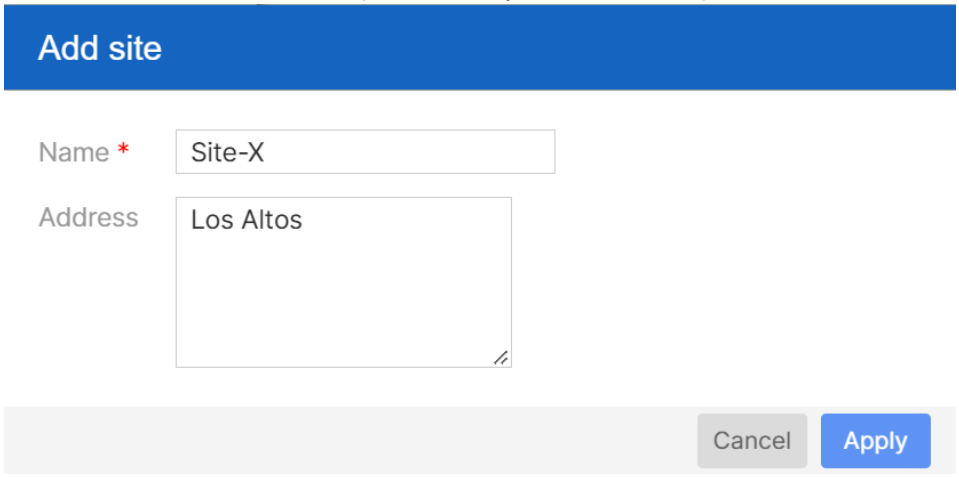
Creating a Site

Create a geographical site in FortiLAN Cloud to associate a floor plan to.

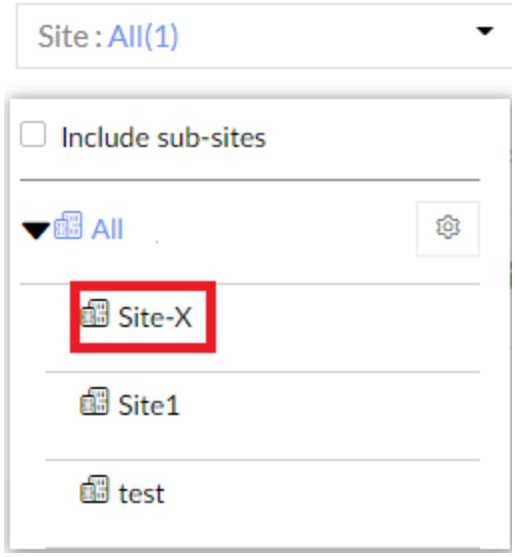
1. Navigate to **Wireless > Access Points > Edit View** and select the **Site** drop-down menu and click on the icon.



2. Select **Add Site** and enter a unique name for your site and an optional **Address**.



3. Click **Apply**.
The site that you created is now displayed in the **Site** drop-down menu.



Adding a floor plan to FortiLAN Cloud

Use this procedure to add a floor plan to FortiLAN Cloud.

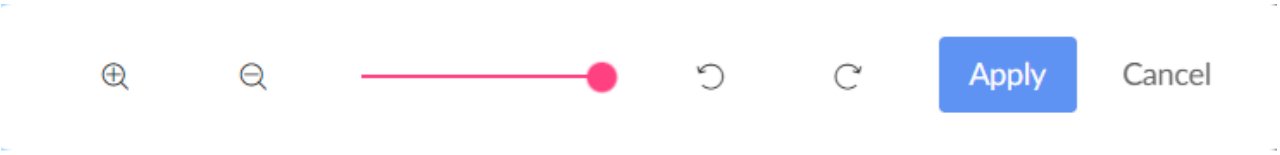
Prerequisites

Identify the site where you want to load a floor plan. Go to **Access Points** > **Map View**. If there is no site, then add one.

Procedure steps

1. In the Menu bar, click **Access Points**.
2. In the Navigation pane, click **Map View** and then select the site to which you want to add a floor plan.

3. Click  and select **Add Floor Plan**.
   The Upload Floor Plan dialog opens.
4. To select a file for the floor plan, click **Choose File**.
   The File Upload dialog opens.
5. Locate the file and then click **Open**.
6. If it is an outdoor plan, select **Is Outdoor?**
7. Click **Submit**.
   FortiLAN Cloud displays the uploaded floor plan.
8. You can adjust the magnification, opacity, and rotation of the floor plan.



9. To save changes, click **Apply**.

Setting a FortiAP device on a map or floor plan

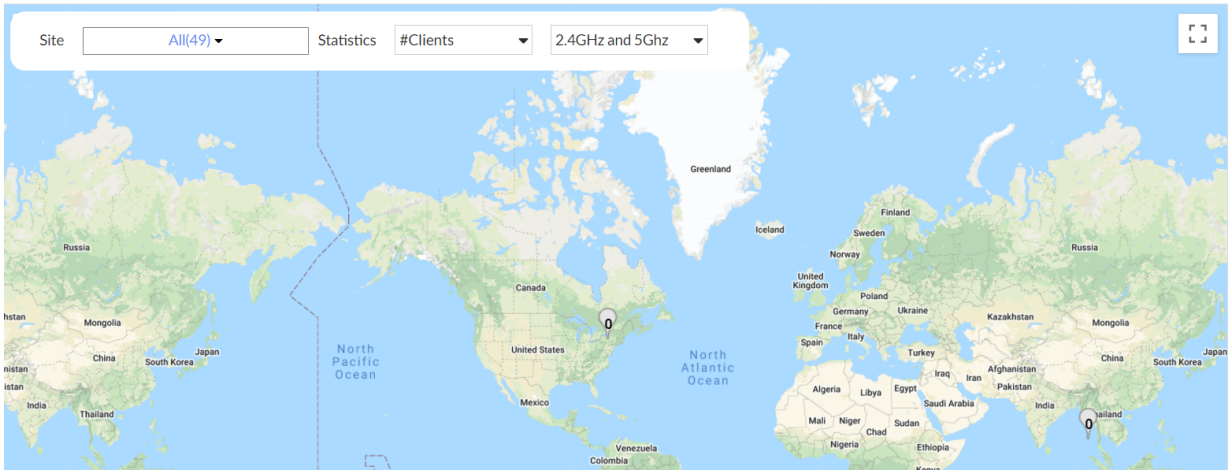
Use this procedure to set the position of a FortiAP device on a map or floor plan.

Prerequisites

- Complete the Adding a floor plan to FortiLAN Cloud on page 87 procedure, if you want to set a FortiAP device on a floor plan.
- Identify the site that has the map or floor plan that you want to set the FortiAP device on. Go to **Access Points** > **Map View**.

Procedure steps

1. To move a FortiAP device to the site that has the map or floor plan that you want to use:
   a. In the Menu bar, click **Access Points**.
   b. In the Navigation pane, click **Edit View**.
   c. In the first column of the table, select the checkbox for the FortiAP device that you want to move.
   d. Click **AP Actions** > **Site**.
   e. Select the site and click **Apply**.
2. To set the position of a FortiAP device on a map or floor plan:
   a. In the Navigation pane, click **Map View** and then select the site that includes the FortiAP that you want to use.
   b. Click  and select **Set AP Position**.
   c. Click and drag  to the desired position on the map or floor plan.
   d. Click **Close**.
      The map or floor plan shows the FortiAP device.
      The following image shows an example of an AP set on a floor plan:



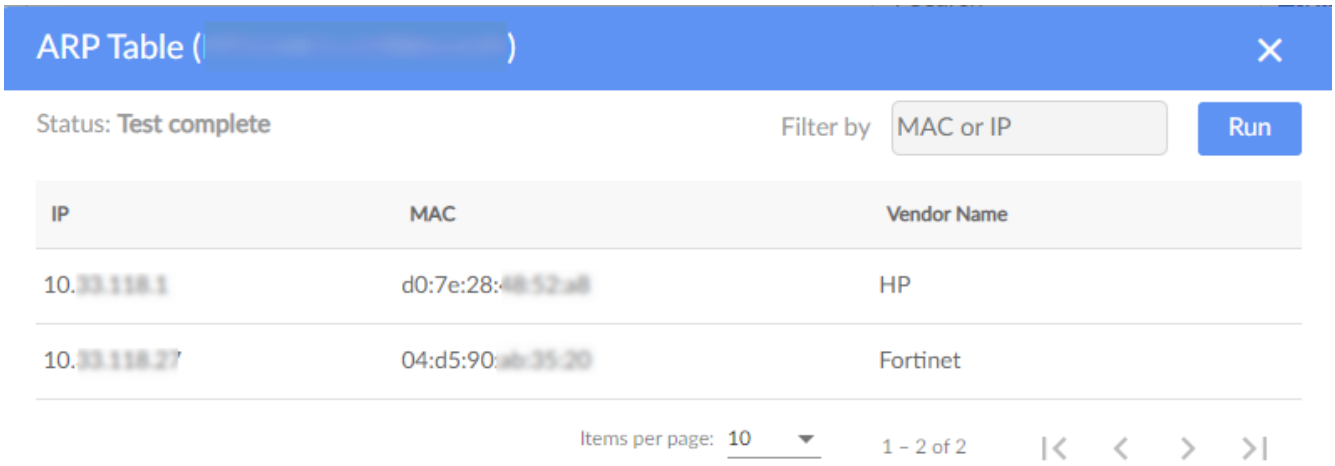
Tools

FortiLAN Cloud provides various utilities that you can run on the FortiAP for the following.

- **Connectivity Analysis**
  - ARP Table on page 89
  - Capturing packets on page 90
  - Disconnection Reports on page 91
  - Traceroute on page 92
  - VLAN Probe on page 92
- **Enhanced Troubleshooting**
  - AP CLI Access on page 93
  - TAC Report on page 93
  - FortiAP Link Health
- **Radio Frequency Analysis**
  - Spectrum Analysis on page 95
- **Throughput Analysis**
  - iPerf Throughput Test on page 98
  - Ping Test on page 98

ARP Table

The ARP Table records the discovered MAC address - IP address pairs of devices connected to a network and the vendor details. Each connected device has its own ARP table that stores the MAC-IP address pairs that the device has communicated with.



Capturing packets

Use this procedure to capture packets on a FortiAP device. Packet captures help you diagnose and troubleshoot FortiAP device problems in a FortiLAN Cloud deployment. Capturing packets can affect device performance because the capture can collect large amounts of data. We recommend capturing packets when required only.

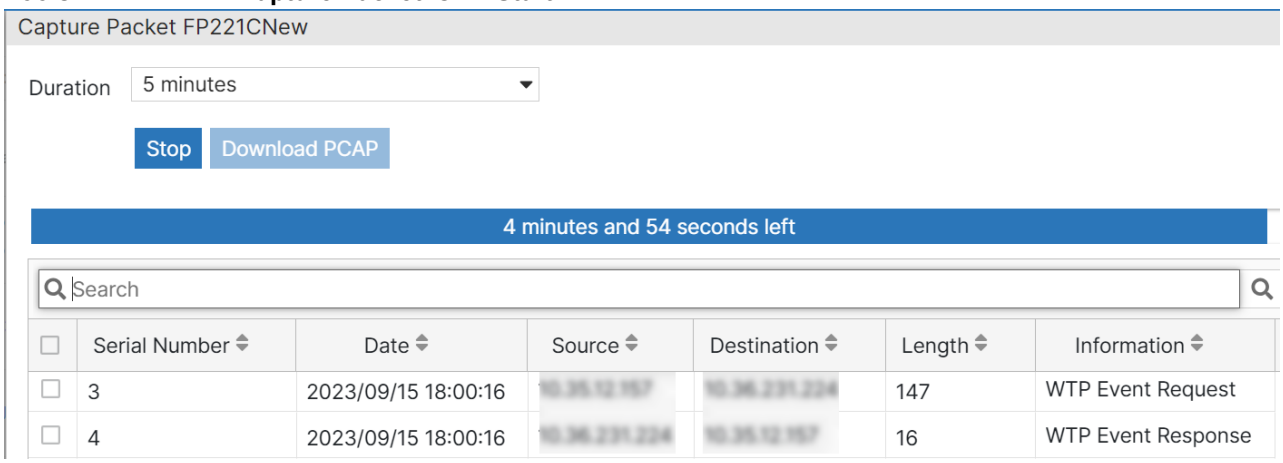
The packet capture includes the following information:

- **No.**: The packet number.
- **Time**: The start time of the packet capture with the format yyyy-mm-dd hh:mm:ss.
- **Source**: The IP address of the device that is sending the packet.
- **Destination**: The IP address of the device that is receiving the packet.
- **Length**: The length of each packet in bytes.
- **Info**: Additional information about the packet such as Control and Provisioning of Wireless Access Points (CAPWAP) control messages. For example, wireless termination points (WTP) information such as the following events:
  - WTP Event Response
  - WTP Event Request

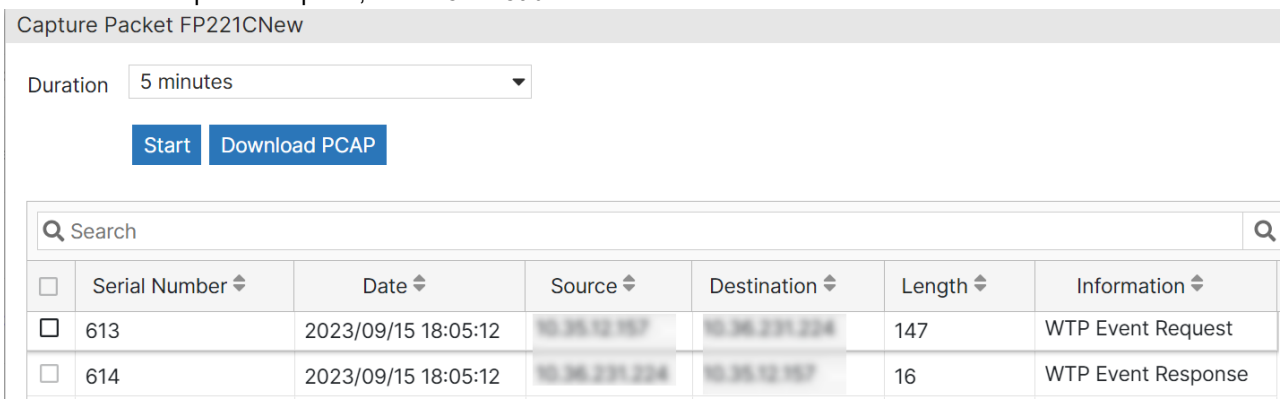
Procedure steps

1. In Menu bar, click **Access Points**.
2. In the Navigation pane, click **Edit View**.

3. In the table, locate the FortiAP device for which you want to capture packets. At the end of that row, click on the **Tools** tab and select **Capture Packet**. Click **Start**.



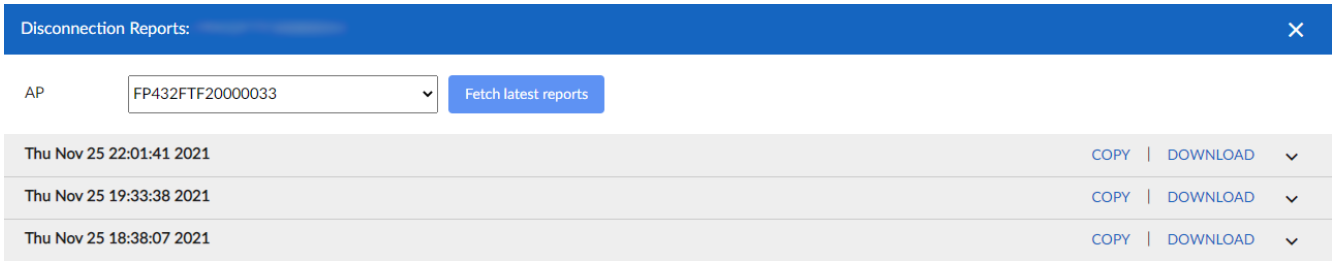
4. To stop the packet capture, click **Stop**.
5. To download the packet capture, click **Download PCAP**.



Disconnection Reports

These reports provide diagnostic information on the factors causing the FortiAP to disconnect from the associated controller.

Select the AP and click **Fetch latest reports** and reports are displayed for the last three FortiAP disconnects. You can copy the report text or download it in the *.pdf* format.

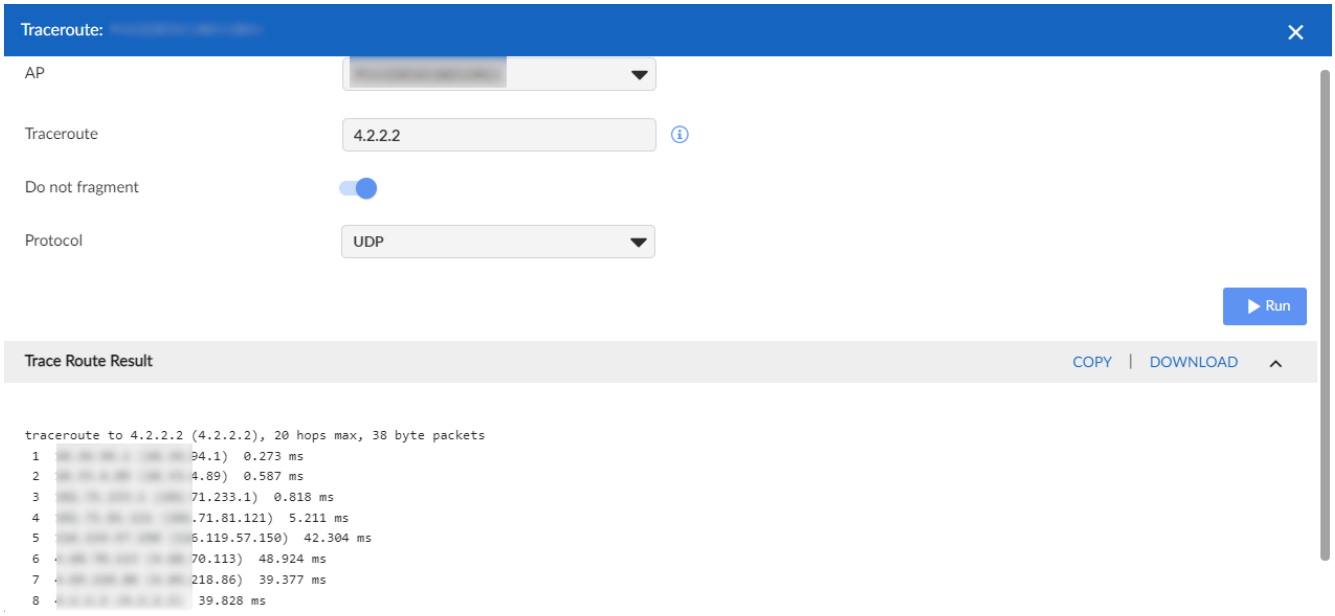


Note: Currently, the FAP-U models do not support this feature.

Traceroute

Traceroute displays a hop-by-hop path through a network starting from the FortiAP to a specific destination. It displays all possible routes (paths) and measures transit delays of packets across the network.

You can enter a destination with an IPv4 address or hostname (FQND) that the FortiAP sends traceroute to. Enable **Do not fragment** to prevent packet fragmentation when it passes through a segment with a smaller Maximum Transmission Unit (MTU). The *UDP* and *ICMP echo* protocols are supported.



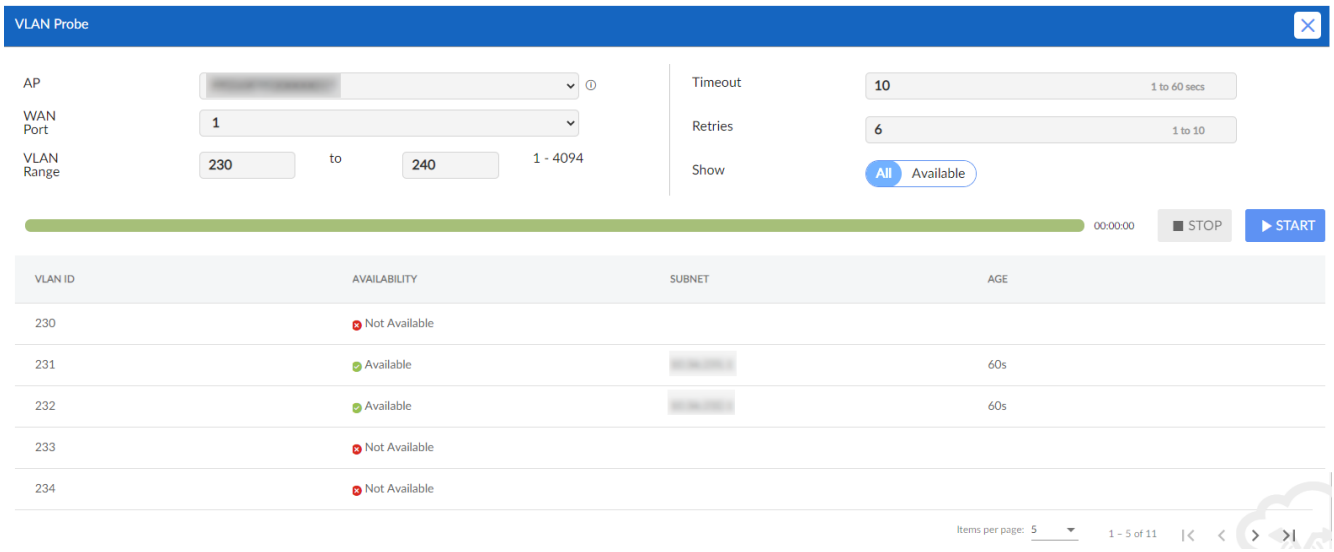
You can copy or download the traceroute result in a PDF format.

VLAN Probe

VLAN probe feature enables FortiAPs to probe connected VLANs and subnets. It sends DHCP probes from the FortiAP's Ethernet interface to specific VLANs on the wired interface and returns information on their availability and subnet details. This helps diagnose and troubleshoot WiFi deployment issues.

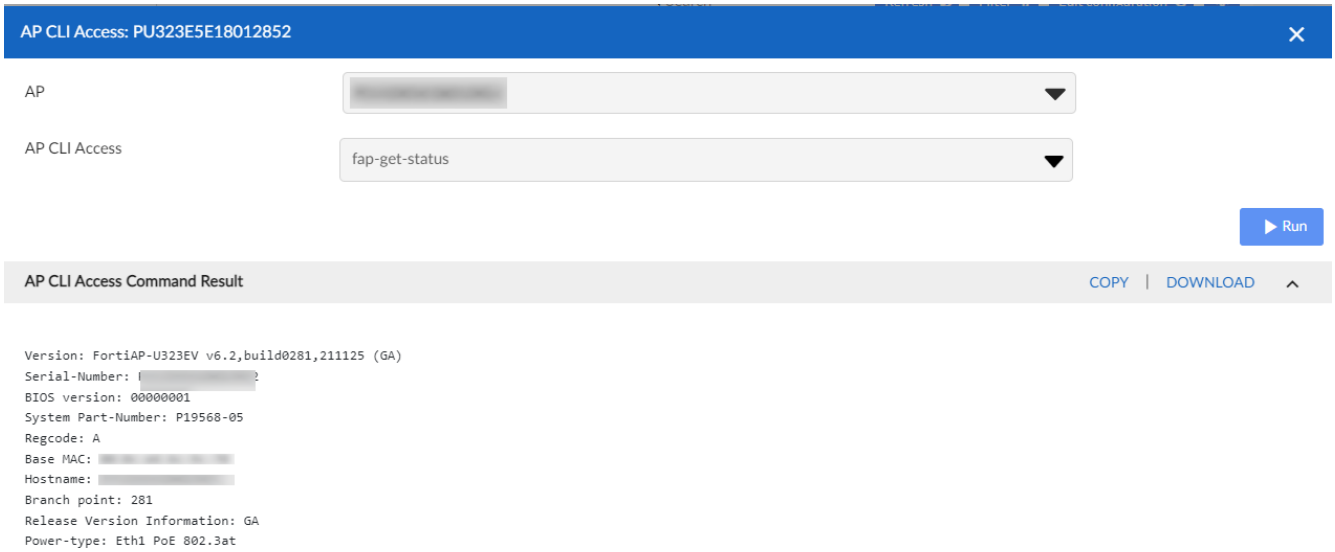
- **AP** – Select the FortiAP. FOS version 6.4.0 and higher are supported.
- **WAN Port** – Select the 1st or 2nd Ethernet port of the FortiAP to initiate the VLAN probe.
- **VLAN Range** – Select the range of VLANs to probe. The valid range is 1 -4094.
- **Timeout** – Configure the timeout for the VLAN probe. The valid range is 1 – 60 seconds with a default value of 10 seconds.
- **Retries** – Configure the number of retries before timeout. The valid range is 1 to 10 with a default value of 6.

Select **Start** and the FortiAP initiates VLAN probe as per configurations.



AP CLI Access

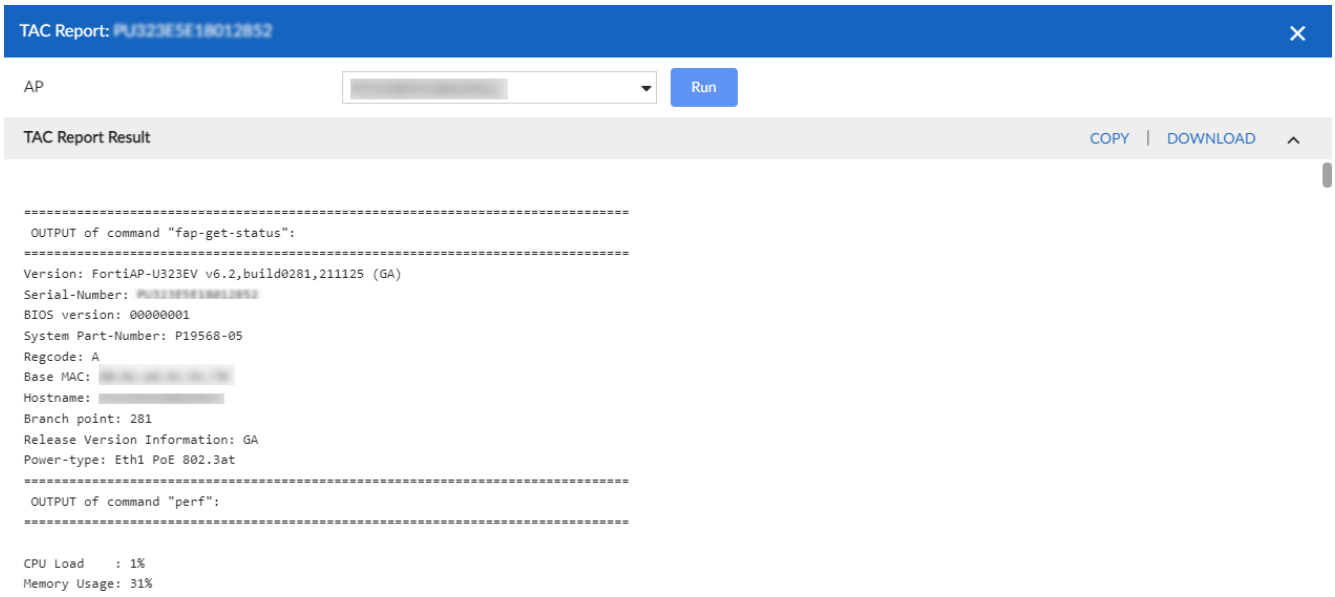
You can select any of the available commands in the **AP CLI Access** list; each command is associated with the corresponding help description. Click **Run** and the command output is displayed.



You can copy or download the result in a PDF format.

TAC Report

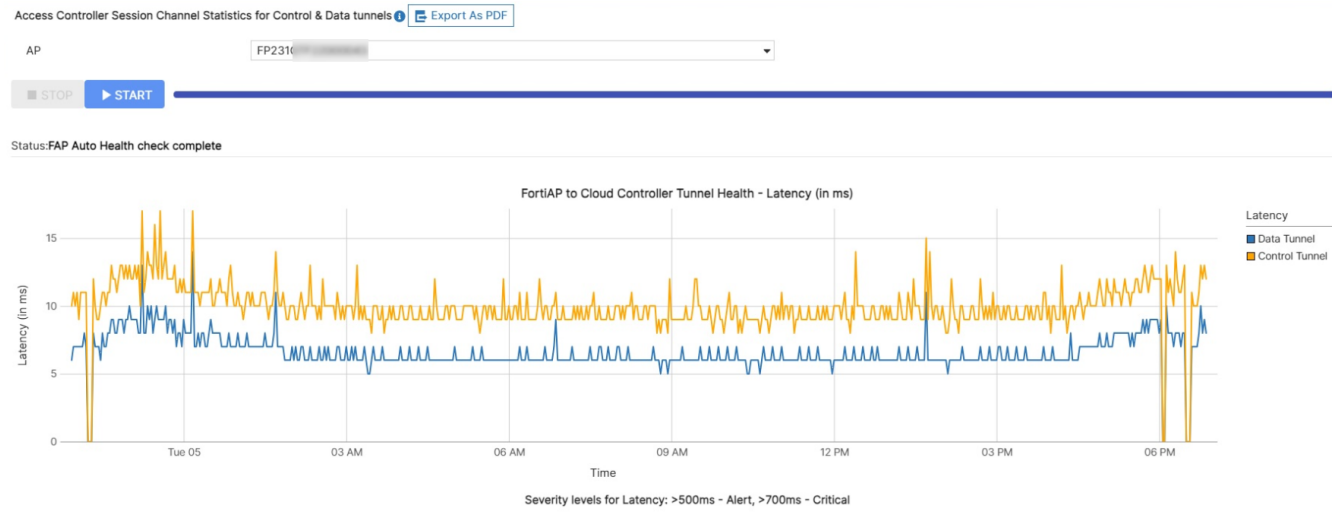
The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands for troubleshooting network issues.

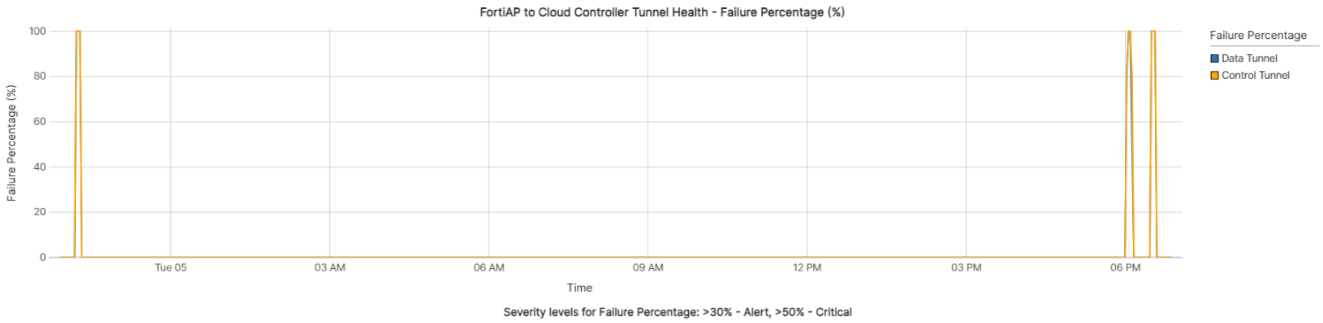


You can copy the TAC report or download it in a PDF format.

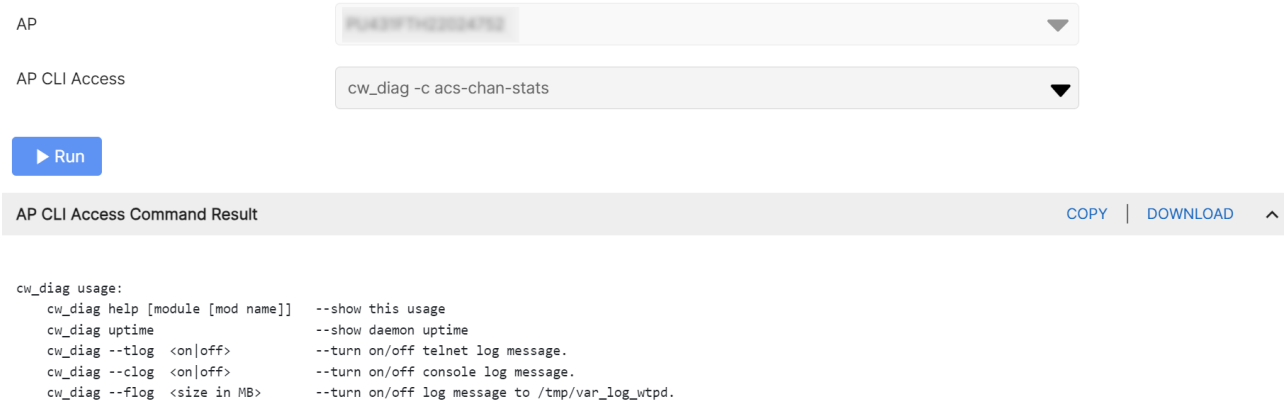
FortiAP Link Health

FortiLAN Cloud now provides the access controller session channel statistics for the control and data channels. These statistics are processed and displayed graphically. Run the **FAP Link Health** tool to view the graphical representation of the FortiAP link health statistics. This tool displays data collected by the FortiAP in the last 48 hours, and provides the failure (packet drop/failure) percentage between the FortiAP and access controller and latency (in ms) for both control and data channels.





You can also view the the channel statistics in raw data format. Navigate to the **Status View** of the wireless access point and run the `cw_diag -c acs-chan-stats` command in the **AP CLI access** tool for enhanced troubleshooting.




```
cw_diag usage:
    cw_diag help [module [mod name]]   --show this usage
    cw_diag uptime                     --show daemon uptime
    cw_diag --tlog  <on|off>           --turn on/off telnet log message.
    cw_diag --clog  <on|off>           --turn on/off console log message.
    cw_diag --flog  <size in MB>       --turn on/off log message to /tmp/var_log_wtpd.
```

Spectrum Analysis

This feature provides visual spectrum analysis capabilities that scan radios for RF channel conditions and sources of interference which can potentially impact WLAN efficiency. Based on the spectrum analysis data, corrective measures such as determining optimal channel planning, debugging client related connectivity issues and automatic transmit power settings are initiated. This facilitates quality wireless service levels by ensuring the optimal usage of the channels considering the information provided by the FortiLAN Cloud spectrum analyser. Both 802.11 and non-802.11 sources of interference can be detected and analyzed by the spectrum analyzer.

Notes:

- Spectrum analysis is only supported when the radio is in the monitor mode.
- FortiAP supports spectrum analysis and is online.
- FortiAP Advanced Management License is required.

Select the channels to be scanned and configure the scan duration, the spectrum analysis is performed on both 2.4 GHz and 5 GHz frequency bands. The spectrum analyzer result displays widgets with the type of interference, signal strength, impacted channels, and wireless spectrum current utilization, start and end time and duration of the interference. It classifies wireless & non-wireless interferences to easy identification of the source.

- You can select the **AP**, **Radio**, and **Channels** to be scanned for interferences.
- The **Scan Duration** can be set to 1, 5, 10, or 15 minutes.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.

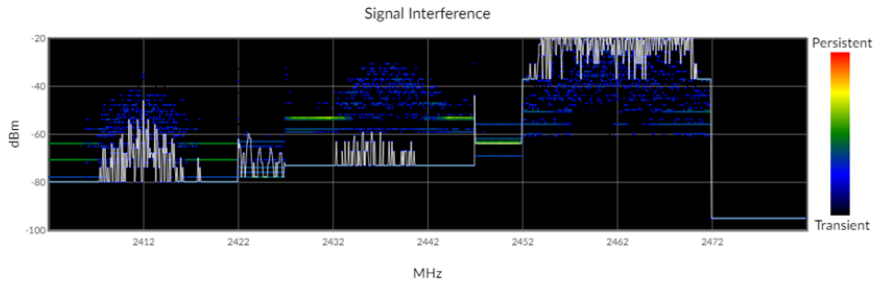
Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds. Data is visualized as 4 charts representing signal interference marking the noise levels for each channel,

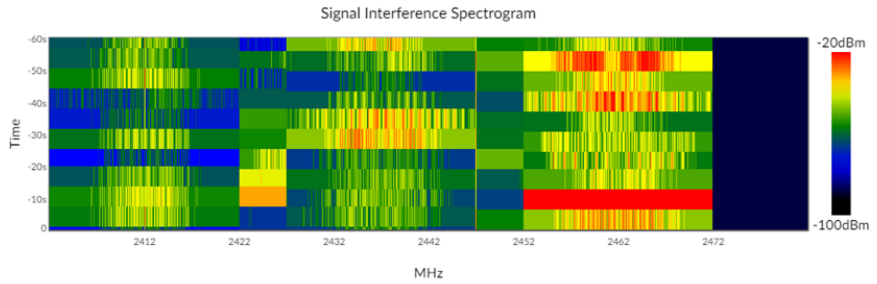
signal interference spectrogram representing 60 samples for different channels at specific time intervals, the duty cycle charts marking the extent to which a non-WiFi device/neighbouring AP is interfering, and the duty cycle spectrogram representing 60 such duty samples for each channel over a period of time.

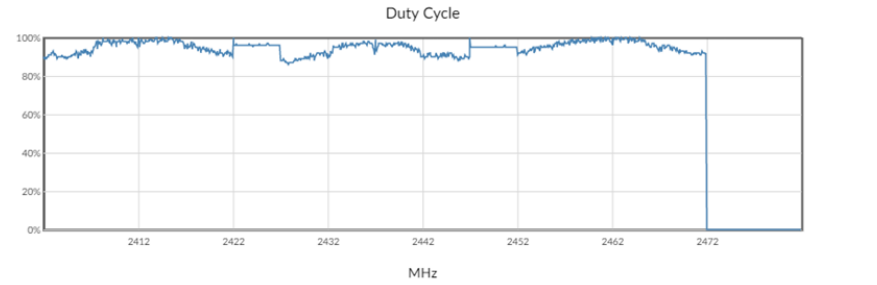
The tabular data for non-WiFi interference displays the time and frequency of last detection and any of the following type of devices causing the interference.

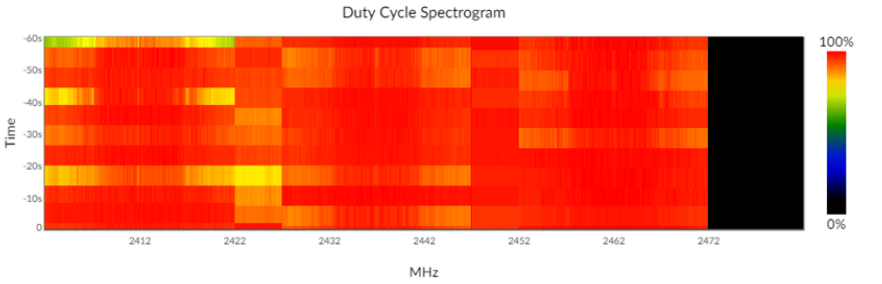
- Microwave ovens
- Video bridges
- Wi-Fi, DSSS cordless phones
- Bluetooth, FHSS cordless phones

The tabular data for WiFi interference displays the online neighbouring AP's BSSID, SSID, maximum signal strength, and channel and time of last detection.









Non Wi-Fi Interference

Detected Time	Frequency	Type
2020-09-14 14:54:09	2452	Wi-Fi, DSSS cordless phone
2020-09-14 14:54:08	2402	Wi-Fi, DSSS cordless phone
2020-09-14 14:54:08	2427	Wi-Fi, DSSS cordless phone
2020-09-14 14:53:54	2427	Bluetooth, FHSS cordless phone
2020-09-14 14:53:00	2437	Bluetooth, FHSS cordless phone

Items per page: 5 1 – 5 of 7

Wi-Fi Interference

Detected Time	BSSID	SSID	Channel	Signal
2020-09-14 14:54:02	[redacted]		6	-30 dBm
2020-09-14 14:54:02	[redacted]	gh-1	6	-52 dBm
2020-09-14 14:54:02	[redacted]	ad	6	-58 dBm
2020-09-14 14:54:02	[redacted]	llo5677	6	-62 dBm
2020-09-14 14:54:02	[redacted]	plus1	6	-59 dBm

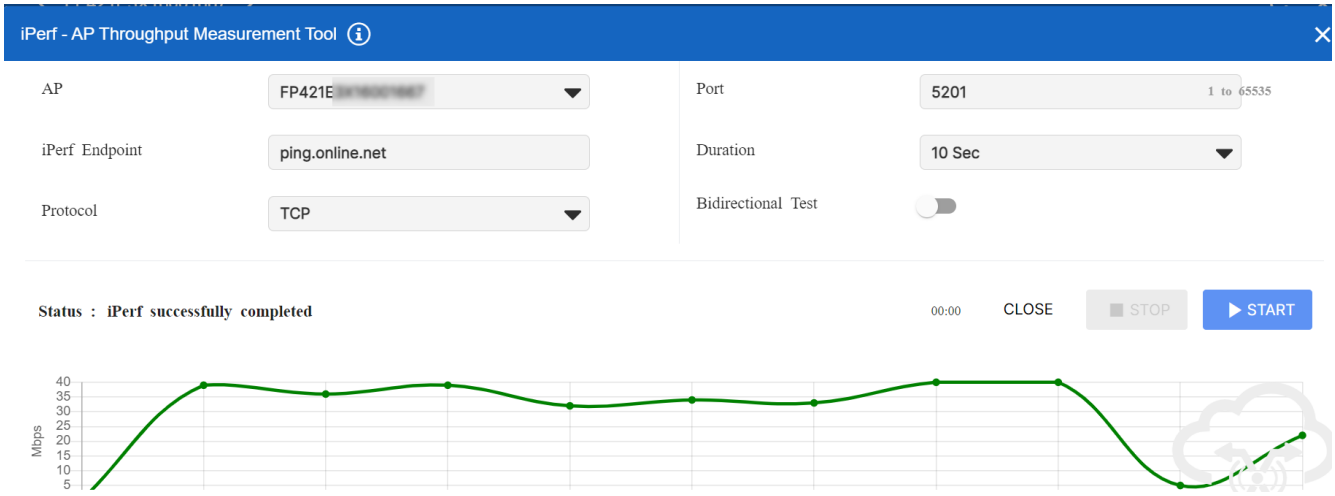
Items per page: 5 1 – 5 of 54

iPerf Throughput Test

The iPerf throughput test measures the UDP and TCP real-time network throughput to aid in estimating the maximum achievable bandwidth in your network. This is useful to isolate problems related to slow network connections. The iPerf test is performed between the FortiAP and an endpoint that can be a wireless client, a computer in the LAN, or an external online server like *ping.online.net*. You must start the iPerf server manually on the endpoint unless using the online server. This feature tests uplink, downlink, or both traffic streams.

- **AP** - Select the FortiAP for iPerf testing.
  Note: The supported FOS version is 6.4.0 and higher for FAP-S/W2 models and 6.2.0 or higher for FAP-U models.
- **Port** – Select the port. The valid range is 1 – 65535.
- **iPerf Endpoint** – Enter the endpoint device IPv4 address/hostname. iPerf 2 and 3 are supported.
- **Duration** – Enter the duration for the iPerf test. The allowed values are 10, 30, and 60 seconds.
- **Protocol** – Select the protocol to measure throughput, **UDP** or **TCP**.
- **Target Bandwidth** – This is applicable only on UDP traffic. The valid range is 1 – 1024 Mbps.
- **Bidirectional Test** – When disabled only uplink traffic is tested and when enabled both uplink and downlink traffic streams are measured. In a bidirectional test, the total time required to complete the test is twice the selected time. For example, if 30 seconds is the configured test duration then the total time required to complete the test is 60 seconds; 30 seconds for uplink and 30 seconds for downlink.

Select **Start** and the FortiAP initiates iPerf testing as per configurations.



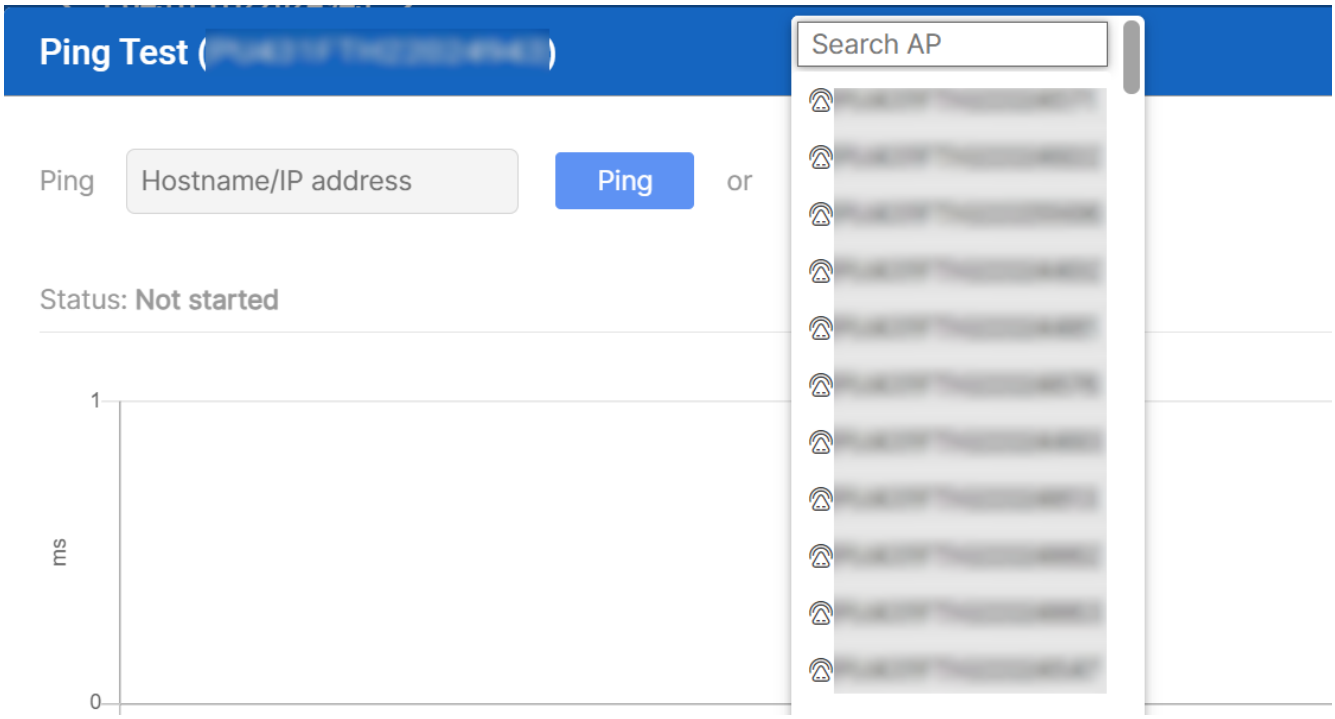
Notes:

- Fortinet recommends to use the latest supported iPerf version in the endpoint machine.
- IPv6 servers are not supported for iPerf testing.
- Ensure the iPerf test ports are enabled in the firewall.

Ping Test

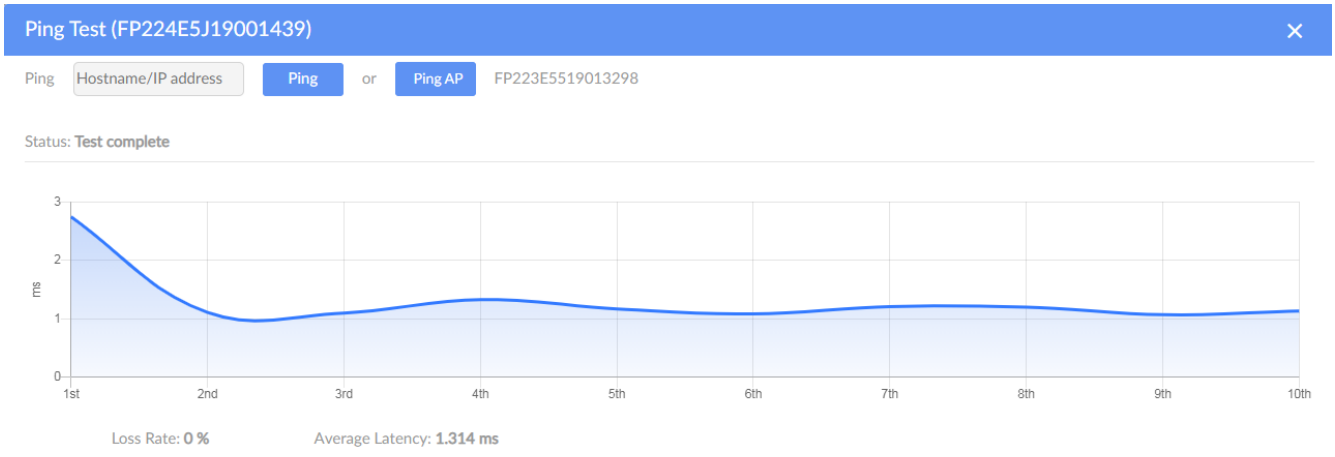
You can conduct a ping test to an IP/domain or to a local AP for troubleshooting network connectivity issues between devices.

Note: The ping test supports only IPv4 addresses.



- **Ping** - Enter the target IP address or hostname to run the ping test.
- **Ping AP** - Select the local AP within the network to run the ping test.

The test result is obtained in 10 seconds.



Configuration

This section includes the procedures for creating different types of SSID with FortiLAN Cloud and configuring various options.

Use the following table for configuration information available in a network under the **Configure** section.

Configuration module	Description
SSIDs	Configuration of SSIDs and their deployment on all APs or selected APs in the AP Network. For more information, see Adding an SSID to a network on page 101.
Network	Manage various network administration settings. For more information, see Network Settings on page 116
Change History	View the history of FortiLAN Cloud configuration changes. For more information, see Viewing the history of configuration changes on page 118.
Operation Profiles	• **FortiAP Platform Profile** - Customization of FortiAP profiles. For more information, see FortiAP Platform Profile on page 119. • **QoS Profile** - QoS profiles used in SSIDs. For more information, see QoS Profile on page 124. • **BLE Profile** - To configure a BLE Profile. For more information, see BLE Profile on page 126. • **DARRP** - Configure Distributed Automatic Radio Resource Provisioning (DARRP). For more information, see Distributed Automatic Radio Resource Provisioning (DARRP) on page 127 • **Schedule Profile** - Create a Multiple PSK schedule profile. For more information, see Schedule Profile on page 129..
Connectivity Profiles	• **Bonjour Relay** - Configure the Bonjour Relay service for devices to broadcast their services. For more information, see Bonjour Relay on page 130. • **FortiPresence** - Configure FortiPresence for user traffic analytics. For more information, see FortiPresence on page 131.
Protection Profiles	• **WIDS Profile** - Create a WIDS profile for network security. For more information, see Adding a WIDS Profile on page 134. • **L3 Firewall Profile** - Create L3 profiles used in SSID. For more information see, L3 Firewall Profile on page 138. • **Tunnel Profile** - GRE/L2TP profiles used in SSIDs. For more information, see Tunnel Profile on page 139
Device Management	• **Scheduled Upgrade** - To upgrade fully deployed FortiAPs. For more information, see Scheduled Upgrades on page 141. • **Syslog Profiles** - To create a Syslog profile. For more information, see Syslog Profile on page 142.

Configuration module	Description
	• **SNMP Profile** - To create and assign an SNMP profile. For more information, see SNMP Profile on page 143

User Access Control	• **MAC Access Control** - Import and export MAC addresses in order to manage an access control list (ACL). For more information, see:
	  • MAC Access Control and MAC Filtering on page 144
	  • Exporting ACL List on page 144
	• **FortiLAN Cloud User/Group** - Users and their group configurations can help avoid the need for RADIUS servers at the customer location. For more information, see:
	  • FortiLAN Cloud User/Group on page 144
	  • Adding a FortiLAN Cloud Guest on page 145
	  • Adding a FortiLAN Cloud Guest Manager on page 146
	• **My RADIUS Server** - RADIUS servers used for authenticating wireless users. For more information, see RADIUS Server on page 146.

Adding an SSID to a network

Use this procedure to configure and add an SSID to a network.

Note: The SSID name is alpha-numeric and case-sensitive. The first character of the SSID name must NOT be any of these characters, **; #** and **!**. Special characters, **+ [ ] " TAB**, and trailing spaces are also not allowed in the SSID name.

On the FortiLAN Cloud Home page, select the network to which you want to add the SSID.

1. In the Menu bar, navigate to **Configuration > SSID**.
2. Click **Add SSID** and select any of the listed Authentication Methods on page 101.
3. To go to Security, click **Next**. If the FortiAP model supports security features, then select the ones you want to enable.
4. To go to Availability, click **Next** and complete the following fields.
   - **Radio**: Select which radios you want to be active.
   - **Per-AP**: Select whether you want the SSID to be available to all APs or APs with specific tags.
   - **Schedule**: Select a schedule for when the SSID is available.
5. To go to Preview, click **Next** and review the summary. If you need to make changes, click **Prev**.
6. To complete the changes, click **Apply**.
7. You can now go to the Deploying a FortiAP device to a network on page 64 procedure.

Authentication Methods

This section describes the supported authentication methods. Follow the prerequisites and configuration options listed for each authentication method, and the Basic Settings on page 107 and Advanced Settings on page 110 to add an SSID.

- WPA2 Personal on page 102
- WPA2 Enterprise on page 102
- WPA3-SAE/WPA3-SAE Transition on page 103
- WPA3 Enterprise/Enterprise Only/Enterprise Transition on page 104

- WPA3-OWE on page 105
- FortiLAN Cloud captive portal on page 105
- My Captive Portal on page 106

WPA2 Personal

Add a WPA2 Personal SSID to a network

Prerequisites	Configuration
• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure). • If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure). • If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure). • If you want to block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.	• **Authentication**: Select **WPA2-Personal**. Type a **Pre-shared Key (PSK)**. This PSK must contain from 8 to 63 printable ASCII characters or exactly 64 hexadecimal numbers. If older stations also need to be supported, then select **WPA/WPA2-Personal** which enables mixed (WPA and WPA2) mode authentication. • **Captive Portal**: Leave as **No Captive Portal**. Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

WPA2 Enterprise

WPA2 Enterprise SSIDs can be configured to use an external RADIUS server to authenticate wireless clients, or control access to the SSID with a configured user group.

With the RADIUS accounting server method, the **Accounting Interim Interval** parameter becomes available. The AP will send an Interim Update Accounting-Request to update the RADIUS accounting server with time and bandwidth usage. The default value is set to **600** seconds (or 10 minutes).

Prerequisites	Configuration

• Complete the RADIUS Server on page 146 procedure.
• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure).
• If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure).
• If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure).
• If you want to enable dynamic VLAN, block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced
	With enterprise class SSIDs, individual users can have their own login (such as username and password, and VLAN, administrative control).
	• **Authentication**: Select **WPA2-Enterprise** (or **WPA/WPA2-Enterprise** mixed mode). To define authorized users
	• **RADIUS Auth Setting**: Set to one of the following:
	  • **My RADIUS Server**: Use your own RADIUS server. To define your RADIUS server, see RADIUS Server
	  • **FortiCloud User/Group**: Use FortiLAN Cloud as the RADIUS server. In this case, you do not need to have your own RADIUS server. All users are to be defined in FortiLAN Cloud (see FortiLAN Cloud User/Group).

Prerequisites	Configuration
Management License.	Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

WPA3-SAE/WPA3-SAE Transition

Add a WPA3 simultaneous authentication of equals (SAE) or WPA3-SAE Transition SSID to a network.

Prerequisites	Configuration

• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure).
• If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure).
• If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure).
• If you want to block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.
	With enterprise class SSIDs, individual users can have their own login (such as username and password, and VLAN, administrative control).
	• **Authentication**: Select **WPA3-SAE** or **WPA3-SAE Transition**.
	  • **WPA3-SAE**: Type an **SAE Password**. This password must contain 8 to 32 alphanumeric characters or exactly 64 hexadecimal numbers.
	  • **WPA3-SAE Transition**: Enables mixed (WPA2 and WPA3) mode authentication. Two passwords are used in the SSID; if the **SAE Password** is used, client connects with WPA3 SAE and if **Pre-shared Key** is used, client connects with WPA2 PSK. This PSK must contain from 8 to 63 printable ASCII characters or exactly 64 hexadecimal numbers.
	  • Enable **SAE-PK authentication** and provide an **SAE-PK private key**. When SAE-PK authentication is enabled, you are required to set an SAE-PK private-key. You can use a third party tool to generate the private key for encryption (for example, sae_pk_gen in wpa_supplicant v2.10) to meet the encryption requirement.
	  • Enable **Hash-to-Element (H2E) only**, that provides a secure key establishment protocol using a cryptographic hash function, this ensures a secure key exchange process to establish the Wi-Fi connection.
	Note: This parameter is mandatory when the SSID is to be beaconed on a 6 GHz radio.
	  • The **SAE Hunting-and-Pecking (HnP) only** option is disabled by default and is used for PWE derivation. Sometimes, when the FortiAP operates with full WPA3-R3 compliance, some wireless clients are unable to connect to WPA3 SSIDs beaconed by the FortiAP. This issue arises as the WiFi chipset and driver on these

Prerequisites	Configuration

	clients do not recognize some RSN IEs beaconed by the FortiAP. To resolve this client connectivity issue, you can enable the SAE HnP option, to ensure that the client can establish a connection using WPA3 to the FortiAP. This feature can be used only when **SAE-PK authentication** and **SAE Hash-to-Element (H2E) only** are disabled.
	Note: This feature is supported on FortiAP version 7.4.2 and above.
	• **Captive Portal**: Add a captive portal to the SSID.
	  • To add a FortiLAN Cloud captive portal, see section FortiLAN Cloud captive portal on page 105.
	  • To add your own captive portal, see section My Captive Portal on page 106
	Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

WPA3 Enterprise/Enterprise Only/Enterprise Transition

WPA3 Enterprise SSIDs can be configured to use an external RADIUS server to authenticate wireless clients, or control access to the SSID with a configured user group.

With the RADIUS accounting server method, the **Accounting Interim Interval** parameter becomes available. The AP will send an Interim Update Accounting-Request to update the RADIUS accounting server with time and bandwidth usage. The default value is set to **600** seconds (or 10 minutes).

Prerequisites	Configuration
• Complete the RADIUS Server on page 146 procedure. The RADIUS server must support 192-bit AES encryption as required by WPA3-Enterprise security level. • If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure). • If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure). • If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure). • If you want to enable dynamic VLAN, block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.	With enterprise class SSIDs, individual users can have their own login (such as username and password, and VLAN, administrative control). • **Authentication**: Set to **WPA3-Enterprise**/**Enterprise Only**/**Enterprise Transition**. • **RADIUS Auth Setting**: To define authorized users, set to **My RADIUS Server** where you use your own RADIUS server. To define your RADIUS server, see RADIUS Server Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

WPA3-OWE

Add a WPA3 opportunistic wireless (OWE) SSID to a network.

Prerequisites	Configuration

• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure).
• If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure).
• If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure).
• If you want to block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.
	• **Authentication**: Select **WPA3-OWE**.
	• **Captive Portal**: Add a captive portal to the SSID.
	  • To add a FortiLAN Cloud captive portal, see section FortiLAN Cloud captive portal on page 105.
	  • To add your own captive portal, see section My Captive Portal on page 106
	Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

FortiLAN Cloud captive portal

FortiLAN Cloud includes captive portal settings that you can customize during the SSID addition.

If you want to create and use your own captive portal, then go to the Adding a My Captive Portal SSID to a network procedure.

Prerequisites	Configuration

• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure).
• If you choose one of the following sign on methods, make sure to complete the required setup:
  • My RADIUS Server (see RADIUS Server on page 146)
  • FortiLAN Cloud user and group (see FortiLAN Cloud User/Group on page 144)
• If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure).
• If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure).
• If you want to block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.
	• **Authentication**: Select **Open** or **WPA2-Personal**. If you select **WPA2-Personal**, then type a **Pre-shared Key**. This password must contain from 8 to 63 characters. Characters can be any combination of upper and lower case letters, numbers, punctuation marks, and symbols.
	• **Captive Portal**: Select **FortiLAN Cloud Captive Portal**.
	• **MAC Access Control**: Select to allow clients identified in the MAC address import list to connect to that SSID.
	  • **Fail Through Mode**. This mode is available if you select the **Open** authentication. If you select the Fail Through Mode, then the following applies:
	  • If a client is not in the MAC address import list, then the client must pass captive-portal authentication to access the internet.
	  • If a client is in the MAC address import list, then the client can bypass the captive-portal authentication and access the internet directly.
	• **Redirect URL**: The URL to which the user is redirected

Prerequisites	Configuration

	after a successful login; **Original request** or **Specific URL**.
	• **Walled Garden**: The walled garden is a list of web domains that users can access before completing the authentication process. You can type an IP address, domain name, and subnetwork address/mask. Separate multiple entries with a comma.
	• **Sign-on Method**: Choose one of the following:
	  • **Click Through**: Users go to the captive portal page and click **Continue** to gain access to the wireless network. Users do not type a username and password.
	  • **My RADIUS Server**: Select a configured RADIUS server.
	  • **FortiLAN Cloud user and group**: Select a configured FortiLAN Cloud group.
	  • **Self-registered guests**: Users access the captive portal page and sign up for an account. They receive their username and password details by SMS or email as defined in step 11 of this procedure.
	  • **Social media**: Users can sign on with their social media account. FortiLAN Cloud supports Facebook, Google+, LinkedIn, and X accounts.
	In the **Captive Portal** page, you can additionally customize the following.
	• **Logo**: You can upload an image.
	• **Title**: You can change the appearance of the title (background color and image as well as the text color) or the text (in English, French, or Japanese).
	• **Message**: You can add a message (in English, French, or Japanese) and change the background color, image, and text color.
	• **Self-Registered**: If you selected the sign on method as self-registered guest (in step 5), then you can customize the page for self-registered guests as well as set an account expiration period and a method to generate a username and password.
	Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

My Captive Portal

In this procedure, you are required to create your own captive portal page.

If you prefer to use and customize an existing captive portal page, then go to the FortiLAN Cloud captive portal on page 105 procedure instead.

Prerequisites	Configuration

• Complete the Creating the My Captive Portal page on page 116 procedure.
• If you want to use the MAC access control, make sure to import MAC addresses (see the MAC Access Control and MAC Filtering on page 144 procedure).
• Choose and set up one of the following sign on methods:
  • My RADIUS Server (see the RADIUS Server on page 146 procedure)
  • FortiLAN Cloud user and group (see the FortiLAN Cloud User/Group on page 144 procedure)
• If you want to apply a QoS profile, make sure that the QoS profile exists (see the QoS Profile on page 124 procedure).
• If you want the SSID to be available to APs with specific tags only, make sure that the AP tags exist (see the Adding AP tags procedure).
• If you want to block intra-SSID traffic, and customize radio and rate optional settings, then purchase a FAP Advanced Management License.
	• **Authentication**: Select **Open** or **WPA2-Personal**. If you select **WPA2-Personal**, then type a **Pre-shared Key**. This password must contain from 8 to 63 characters. Characters can be any combination of upper and lower case letters, numbers, punctuation marks, and symbols.
	• **Captive Portal**: Select **My Captive Portal**.
	• **MAC Access Control**: Select to allow clients identified in the MAC address import list to connect to that SSID.
	  • **Fail Through Mode**. This mode is available if you select the **Open** authentication. If you select the Fail Through Mode, then the following applies:
	  • If a client is not in the MAC address import list, then the client must pass captive-portal authentication to access the internet.
	  • If a client is in the MAC address import list, then the client can bypass the captive-portal authentication and access the internet directly.
	• **Captive Portal URL**: Type the URL of your captive portal page.
	• **Redirect URL**: The URL to which the user is redirected after a successful login; **Original request** or **Specific URL**.
	• **Walled Garden**: The walled garden is a list of web domains that users can access before completing the authentication process. You can type an IP address, domain name, and subnetwork address/mask. Separate multiple entries with a comma.
	• **Sign-on Method**
	: Choose one of the following:
	  • **Click Through**: Users go to the captive portal page and click **Continue** to gain access to the wireless network. Users do not type a username and password.
	  • **My RADIUS Server**: Select a configured RADIUS server.
	  • **FortiLAN Cloud user and group**: Select a configured FortiLAN Cloud group.
	Complete the Basic Settings on page 107 and Advanced Settings on page 110 as required.

Basic Settings

Configure the following basic settings for an SSID assigned to your network.

Field	Description
SSID	Type a name for this wireless network. Wireless clients use this name to find and connect to this wireless network.
Enabled	Select to have the SSID active.
Broadcast SSID	Select to advertise the SSID. All wireless clients within range can see the SSID when they scan for available networks.
Beacon Advertising	You can enable the advertising of vendor specific elements in beacons that contain FortiAP information such as its name, model, and serial number. This enables administrators to easily identify the coverage areas using site surveys. Consider the following scenarios that use this feature effectively. • The administrator is able to gradually move away from the FortiAP while continuously sniffing the beacons to determine if they can still hear from the FortiAP. • The FortiAP are easily identified during network troubleshooting.

MAC Access Control	Select to allow clients identified in the MAC address import list to connect to that SSID.
	• **Fail Through Mode**. This mode is available if you select the **Open** authentication. If you select the Fail Through Mode, then the following applies:
	  • If a client is not in the MAC address import list, then the client must pass captive-portal authentication to access the internet.
	  • If a client is in the MAC address import list, then the client can bypass the captive-portal authentication and access the internet directly.

Mesh Link	Select to enable the mesh link. A wireless mesh eliminates the need for Ethernet wiring by connecting Wi-Fi APs to each other by radio. Only one AP (root AP) is connected to the wired network and all other APs (leaf APs) connect to this mesh root AP over the wireless backhaul SSID. This is supported for *WPA3 - SAE*, *WPA2 - Personal*, and *Open* modes of authentication.
Data Encryption	When either of the mixed mode authentication methods are enabled, select a data encryption protocol: **AES**, **TKIP**, or **TKIP-AES**.
Simple Multiple Pre-shared Keys (MPSK)	Simple Multiple PSKs can also be configured for **Personal** SSIDs, in which case stations will be able to connect to an SSID using either a common PSK or their own PSK. You can select the configured schedule profile for activating multiple PSKs. For more information, see Schedule Profile on page 129. **Note:**A maximum of 128 multiple PSKs are allowed per SSID.
MPSK	You can create multiple pre-shared key groups to associate with VLANs; up to 16000 keys are supported per network. **Adding MPSK Groups** • Click **Add** and enter a unique **Group Name** and **VLAN ID** to associate the MPSK group with and configure pre-shared keys.

Field	Description
	• Click **Import** to import (*.csv*) and populate existing MPSK groups into the SSID profile. • Click **Export** to export the existing MPSK groups into your local machine in *.csv* format. **Adding Pre-shared keys** • Click **Add** to create new pre-shared keys and update the following. **a.** A unique **Name** and **Pre-shared Key** (8 to 63 characters or 64 hexadecimal digits). **b.** The client **MAC Address** for which this key is used. This field takes precedence over the client limit. **c.** Select the **Client Limit**. **Default** - The maximum number of clients is determined by the default client limit which is set at the SSID level. If this is value not set, then an unlimited number of clients can connect to the key. **Unlimited** - An unlimited number of clients can connect to the key. **Specify** - The specified maximum number of clients can connect to the key. **d.** Select a configured **Schedule Profile**. See Schedule Profile on page 129. **e.** Enter **User Name**, **User Email** address, and **Mobile** number (prefixed with the country code). These credentials are used to send pre-shared keys to email addresses (**Send Keys via Email**) or via SMS (**Send Keys via SMS**) on the associated mobile number. • Click **Generate** to auto-generate pre-shared keys and update the following. **a.** A unique **Name Prefix** (1 -32 alphanumeric characters) for the generated keys and the **Number of Keys** to generate (1 - 16383). **b.** The required **Key Length** (8 - 63 characters). **c.** Specify the **Client Limit** and the configured **Schedule Profile**. See Schedule Profile on page 129. • Click **Import** to import (*.csv*) and populate existing pre-shared keys in the MPSK group. • Click **Export** to export the existing pre-shared keys into your local machine in *.csv* format.
RADIUS Authentication by	The FortiAP acts as a RADIUS client and sends accounting information to the configured RADIUS server. This configuration parameter is applicable **ONLY** when the SSID operates in the OPEN security mode with external captive portal and RADIUS authentication and accounting parameters. When **RADIUS Authentication by** is enabled, the FortiAP redirects clients to the configured external captive portal, collects credentials and performs RADIUS authentication and accounting. When disabled (default), the legacy functionality continues where the FortiAP redirects all clients to a centralized FortiLAN Cloud which then redirects them to the configured external captive portal.

Field	Description
	When you enable **RADIUS Authentication by**, the following parameters become configurable. • **Secure HTTP** - Secure HTTP is used to post credentials from the configured external captive portal web server to the FortiAP. This is disabled by default. • **Session Interval** - The time interval after which the captive portal authentication session is invalidated and the user is required to log in again. The valid range for the session interval is 0 - 864000 seconds, 0 (default) indicates that the user is never logged out. **Note:** This feature is supported on FAP-S and FAP-W2 models with firmware versions 6.2 and 6.4.
RADIUS Acct Settings	Select the RADIUS profile for accounting. CoA is also supported and can be enabled in RADIUS Accounting profile.
IP assignment	Select **Bridge** or **NAT**. If you choose **NAT**, then complete the following: • **Local LAN**: Select **Allow** or **Deny**. • **DHCP Lease Time**: Default is 3600 seconds (or one hour). • **IP/Network Mask**: Type the IP address and network mask of the SSID. • **DNS Status**: You can push DNS configuration to a DHCP server running on the FortiAP. When creating an SSID, enable **DNS Status** and the wireless endpoints receive the configured DNS server IP addresses via DHCP when connecting the SSID. You can configure a maximum of 3 DNS server IP addresses (IPv4 only), in case of Enterprise SSIDs, the RADIUS server can assign/override these DNS servers.
QoS Profile	If you want to apply a QoS profile that you have already created, select it from the list.
VLAN ID	If the IP assignment is Bridge, you can type the ID of the VLAN for your wireless network (SSID). Default is 0 for non-VLAN operation. To view the dynamic VLAN ID based on the FortiAP data, see Clients.

Advanced Settings

With a FortiAP advanced management license, you can enable the following advanced settings.

Field	Description
Radio Sensitivity (Rx-SOP)	The Receiver Start of Packet (Rx-SOP) configures a threshold to allow FortiAPs to adjust the SSID cell size. The radio discards all received wireless frames with minimum WiFi signal lesser than the configured threshold value. Adjusted cell size ensures that wireless clients are connected to the nearest FortiAP at highest possible data rates and distant clients do not deprive other clients of airtime. The valid range of signal strength is -95 to -20 dBm with a default value of -79 dBm for 2.4GHz and -76 dBm for 5GHz.
Probe Response Suppression	Restricts distant wireless clients from connecting to the FortiAP if the received

Field	Description
	signal strength is less than the configured threshold. The FortiAP does not send any probe response to these distant wireless clients and responds to the probe requests sent from nearby clients only. The valid range of signal strength is -95 to -20 dBm with a default value of -80 dBm.
Sticky Clients Removal	De-authenticates sticky wireless clients (distant clients that stick to the FortiAP) if the signal strength is less than the configured threshold. The valid range of signal strength is -95 to -20 dBm with a default value of -79 dBm for 2.4GHz and -76 dBm for 5GHz.
Protected Management Frames (802.11w)	Provides a layer of security for wireless management frames by ensuring that traffic comes from legitimate sources. Network attackers and malicious entities are unable to disrupt legitimate wireless connections by sending spoofed clear text wireless management frames. • **Disable** - Disables the usage of 802.11w management protection frames. • **Optional** - Allows wireless clients that do not support 802.11w along with those that support 802.11w to associate with the SSID. • **Required** - Allows only those wireless clients to associate with the SSID that support 802.11w and prevents clients that do not support 802.11w from associating. • **PMF Association Comeback Timeout (seconds)** - Specifies the time which an associated client must wait before the association can be tried again when first denied. The valid range is 1 -20 seconds with a default value of 1 second. • **PMF SA Query Retry Timeout (milliseconds)** - Specifies the amount of time the controller waits for a response from the wireless client for the query process. If there is no response from the client, it is dis-associated. The supported values are 100, 200, 300, 400, and 500 milliseconds with a default value of 200 milliseconds **Note**: Any change in the PMF configuration requires the controller to delete and then add the SSID. This disrupts existing connections.
Fast BSS Transition (802.11r)	This feature allows faster roaming for Wi-Fi clients by enabling swift BSS transitions between APs. This minimizes delay caused due to a client transitioning from one BSS to another in a multi-AP deployment. • **Mobility Domain ID** – This parameter acts as a network identifier. The clients attempt 802.11r enabled roaming only when the same mobility domain ID is configured for both the networks. The valid range is 1 to 65535 and the default is 1000. • **R0 Key Lifetime** – This parameter indicates the duration after which the R0 key in the FortiAP expires. For WPA/WPA2 PSK authentication methods, the R0 key is derived from the PSK and for enterprise, it is derived after the EAP handshake with the RADIUS server is complete. The valid range is 1 to 65535 minutes and the default is 480 minutes.
Radio Measurements (802.11k) and	This feature provides more flexibility to the network administrator to disable the network's ability to influence the roaming decision of the clients, especially, in high

Field	Description
BSS Transition Management (802.11v)	density deployments with a large number of FortiAPs. In cases where network planning is not good, using 802.11v may impact client connectivity. • **Radio Measurements (802.11k)** - 802.11k network assisted roaming allows a potential roaming wireless client to collect from its current AP the list of compatible neighbour APs. This saves the wireless client from performing full scan on both bands. The wireless client selects and moves to the optimal neighbour AP from the list. The 802.11k also provides support for Radio Resource Management (RRM) such as APs querying the associated wireless clients for beacon reports and perceived RSSI used to prepare the compatible neighbour AP list for wireless clients. • **BSS Transition Management (802.11v)** - 802.11v network assisted roaming allows the wireless network to send requests to associated clients, recommending better APs to associate with while roaming. This is beneficial for both load balancing and in guiding clients with poor connectivity. The BSS Transition feature allows the roaming client to initiate a BSS transition query to the associated AP for a candidate list of other APs it can re-associate with, the associated AP responds with a BSS transition request containing the requested AP list. The AP can also send an unsolicited BSS transition request to the client. The client can accept the request and re-associate with the suggested APs or it can reject the request and continue its association with the current AP. **Note**: **The Voice Enterprise (802.11kv)** configuration is not available with release 24.1. If you were using the 802.11kv setting in the previous release, then in the current version both 802.11k and 802.11v will be enabled.
Airtime Fairness Weight (%)	Wi-Fi has a natural tendency for clients farther away or clients at lower data rates to monopolize the airtime and drag down the overall performance. Airtime Fairness (ATF) helps to improve the overall network performance. Airtime Fairness is configured per SSID, each SSID is granted airtime according to the configured allocation. It is configurable on both 2.4 GHz and 5 GHz radios. Data frames that exceed the configured % allocation are dropped. Enable Airtime Fairness when creating a Platform profile. • Applicable only on downlink traffic. • Applicable only on data, management and control functions are excluded. • Applicable on all types of SSIDs; Tunnel, Bridge and Mesh. • Applicable on all authentication modes. Airtime Fairness is supported with FOS 6.2.0 and on all FortiAP-S and FortiAP-W2 models. **Note:** Enable ATF processing on desired radios in AP Platform Profile.

Field	Description
Broadcast Suppression	Suppresses the transmission of specific broadcast traffic to secure the wireless network and optimize airtime usage. When the received broadcast traffic exceeds the threshold, the interface discards it until the broadcast traffic drops below a specific threshold. Since broadcast packets sent to wireless clients connected to a FortiAP occupy valuable airtime, unnecessary and potentially detrimental packets can impact network throughput. By default, **ARP Replies**, **ARPs For Known Clients**, **DHCP Uplink**, **DHCP Downlink**, and **DHCP Unicast** broadcast suppression is enabled. The following methods are supported. • **ARP Poison** - Suppress ARP poison attacks from malicious Wi-Fi clients. Prevent malicious WiFi clients from spoofing ARP packets. • **ARP Proxy** - Suppress ARP request packets broadcast by the Ethernet downlink to known Wi-Fi clients. Instead, send ARP reply packets to the Ethernet uplink, as a proxy for Wi-Fi clients. • **ARP Replies** - Suppress ARP reply packets broadcast by Wi-Fi clients. Instead, forward the ARP packets as unicast packets to the clients with target MAC addresses. • **ARPs For Known Clients** - Suppress ARP request packets broadcast to known Wi-Fi clients. Instead, forward ARP packets as unicast packets to the known clients. • **ARPs For Unknown Clients** - Suppress ARP request packets broadcast to unknown Wi-Fi clients. • **DHCP Uplink** - Suppress DHCP discovery and request packets broadcast by Wi-Fi clients. Forward DHCP packets to the Ethernet uplink only. Prevent malicious Wi-Fi clients from acting as DHCP servers. • **DHCP Downlink** - Suppress DHCP packets broadcast by the Ethernet downlink to Wi-Fi clients. Prevent malicious Wi-Fi clients from acting as DHCP servers. • **DHCP Unicast** - Convert downlink broadcast DHCP messages to unicast messages. • **DHCP Starvation** - Suppress DHCP starvation attacks from malicious Wi-Fi clients. Prevent malicious Wi-Fi clients from depleting the DHCP address pool. • **IPv6** - Suppress IPv6 broadcast packets. This is useful when the network is configured to support only IPv4. • **NetBIOS Name Services** - Suppress NetBIOS name services packets with UDP port 137. • **NetBIOS Datagram** - Suppress NetBIOS datagram services packets with UDP port 138. • **All Other Broadcast** - Suppress broadcast packets not covered by any of the specific options. • **All Other Multicast** - Suppress multicast packets not covered by any of the specific options.
L3 Firewall Profile	Create L3 Firewall rules. For more information, see L3 Firewall Profile on page

Field	Description
	138.
Block intra-SSID traffic	To block intra-SSID network traffic.
Tunnel Settings	Select **Tunnel Profile** to add an existing GRE/L2TP Tunnel profile. FortiLAN Cloud supports tunnel redundancy. When the primary tunnel goes down, data traffic is automatically redirected to the secondary or the standby tunnel. Select the **Primary Tunnel Profile** and the **Secondary Tunnel Profile**. For more information, see Adding a Tunnel profile. • **Tunnel Echo Interval**: The time interval to send echo requests to primary and secondary tunnel peers. The valid range is 1 to 65535 seconds; default is 300 seconds. • **Tunnel Fallback Interval**: The time interval for secondary tunnel to fall back to the primary tunnel once it is active. The valid range is 0 to 65535 seconds; default is 7200 seconds.

DHCP Option 82	DHCP option 82 (DHCP relay information) secures wireless networks served by FortiAPs against vulnerabilities that facilitate DHCP IP address starvation and spoofing/forging of IP and MAC addresses. The **Circuit ID** and **Remote ID** parameters enhance this security mechanism by allowing the FortiAP to include specific AP and client device information into the DHCP request packets. Both these options are disabled by default.
	The DHCP server can use the location of a DHCP client when assigning IP addresses or other parameters.
	Note: This feature is supported with FOS 6.2.0 and above.
	• **Circuit ID:** The AP information is inserted in the following formats:
	  • **Style-1:** ASCII string composed in the format *<AP MAC address>;<SSID>;<SSID-TYPE>*. For example, *" 00:12:F2:00:00:59;SSID12;Bridge"*.
	  • **Style-2:** ASCII string composed of the AP MAC address. For example, *"00:12:F2:00:00:59"***.**
	  Style-3: ASCII string composed in the format *<Network-Type:WTPProfile-Name:VLAN:SSID:AP-Model:AP-Hostname:AP-MAC address>*. For example, *"WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E: 00:12:F2:00:00:59"*.
	• **Remote ID:** The MAC address of the client device is inserted in the following format:
	Style-1 - ASCII string composed of the client MAC address. For example,*"00:12:F2:00:00:59"***.**

Radio and Rates Optional Settings	Customize the 2.4 GHz and 5 GHz rate settings. FortiLAN Cloud supports 11b/g, 11a, 11n, 11ac, and 11ax data rates in SSID configuration. **Note**: The 11ax data rates are supported only on FortiAPs with version 7.2.1 and above.

Security

The following security features can be configured in the SSID.

Application control

FortiLAN Cloud allows you to configure UTP on FortiAP endpoints (for supported models) to detect traffic in specific categories generated by a large number of applications. You can specify what action to take with the application traffic; allow, monitor, or block. Application control supports traffic detection using the HTTP protocol and uses deep application inspections to detect traffic for better control and coverage. You can select specific application signatures in the supported categories to configure and override the action set generally for all categories.

Web Access

You can control access to web content by blocking web pages containing specific words or patterns. The web access feature scans the content of every web page that is accepted by a security policy. You can use the following multiple web content filter lists.

- Allow General Interest Sites Only
- Allow General Interest Sites and Bandwidth Consuming Sites
- Allow All Sites except Security Risk
- Advanced Configuration

In advanced configuration, you can configure the action to be taken for web pages of specific categories. You can also specify words, phrases, patterns, wildcards and Perl regular expressions to match content on web pages.

Block Botnet

FortiLAN Cloud allows you to enable botnet monitoring and blocking across all network traffic.

Intrusion Prevention

Intrusion Prevention System (IPS) detects network attacks and prevents threats from compromising the network, including protected devices. You can enable protection of wireless clients from being attacked by Internet hosts and vice versa.

IPS sensors can contain one or more IPS filters that you can configure. A filter is a collection of signature attributes, the following are the attribute groups.

- Target
- Severity
- Service
- OS
- Application

When selecting multiple attributes within the same group, the selections are combined by using a logical OR. When selecting multiple attributes between attribute groups, each attribute group is combined by using a logical AND.

Once you select filters in the GUI, the filtered list of IPS signatures are displayed. Adjust your filters accordingly to construct a suitable list for your needs.

AntiVirus

The Antivirus feature protects against the latest viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your

network and accessing its invaluable content. The Antivirus database type selection depends on the network and security needs. The following protocols are inspected.

- HTTP
- SMTP
- POP3
- IMAP
- FTP

Creating the My Captive Portal page

This section includes details about creating the My Captive Portal page. The creation of this page is a prerequisite for the Adding a My Captive Portal SSID to a network procedure.

A user connects to the Wi-Fi network and is redirected to **https://<my_captive_portal_url>?grant_url=fortilancloud_grant_url**.

The user lands on the captive portal, who is then redirected by the captive portal to the **<FortiLANCloud_grant_url>**.

Check the AP network web URL in the address bar. This URL should be set to **https://xxxx-<digit>.fortilan.forticloud.com**.

- The base URL of <FortiLANCloud_grant_url> without -<digit> can be https://xxxx.fortilan.forticloud.com
- The full URL of <FortiLANCloud_grant_url> can be https://xxxx.fortilan.forticloud.com/APAuthentication/submit?type=external

If the SSID sign on method is **Click Through**, no parameters are submitted. For the other SSID sign on methods, the following parameters are submitted:

- User
- Password
- error_page_url

Sample jsp to paste in the captive portal

```
<form action="<%=request.getParameter("grant_url") %>" method="GET">
<input type="hidden" name="error_page_url"
value="http://yourcompany.com/test/error.jsp"/>
<table>
<tr><td>Username:</td><td><input name="user" type="text"></td></tr>
<tr><td>Password:</td><td><input name="password" type="password"></td></tr>
<tr><td><input type="submit" value="Login"></td></tr>
</table>
</form>
```

Network Settings

Use this procedure to configure and manage specific network settings.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration > Network**.

Editing the Network Time Zone

Locate the **Network Info** section and in the **Time Zone** drop-down list, select the time zone. Click **Apply** and verify the updated time.

1. Go back to the FortiLAN Cloud Home page.
2. Locate the network that you selected in step 1.

Enabling Network Alerts

Locate the **AP Network Alert** section. If you want to use the email associated with the FortiLAN Cloud account, click **Use Account Email**. Otherwise, in the **Send alerts via email to** field, type an email address. Click **Apply**. The email alerts are sent only for FortiAP down event (after 10-15 minutes (approximately)).

Editing Radio Scan Settings

Use this procedure to change the following radio scan settings:

- editing background scan interval (in seconds)
- disabling background scan
- enabling passive scan mode (no probe)

Note: These settings can optionally be overridden by a WIDS profile, if any, associated with this radio.

Prerequisites

To use the radio scan settings, make sure to enable one of the following platform profile settings:

- Automatic TX Power Control
- DRMA
- Radio Resource Provision
- Rogue AP Scan

For details about the platform profile, see the FortiAP Platform Profile on page 119 procedure.

In the **Radio Scan** section, complete the updates and click **Apply**.

NAT Session Keep Alive Timer

The FortiAP sends a probe message to the cloud servers at the configured **NAT Session Keep Alive timer** duration. This ensures NAT sessions on all intermediate devices in the network path are kept alive. This feature is especially beneficial in case of firewalls with short lived NAT sessions, that sometimes cause the FortiAPs to go offline.

Notes:

- This feature is applied to all FortiAPs in the network.
- This feature is supported on FortiAP version 7.4.2 and above.

Managing Automatic FortiAP Reboot

This feature allows you to configure FortiAPs for an automatic reboot when they lose connection with the cloud controller. In such a scenario, this feature reduces network downtime and eliminates the need for manual intervention. If the SSIDs are configured on the FortiAP in standalone mode (such as PSK authentication), then the FortiAP does not interact with the cloud controller for authentication of wireless clients. However, in some cases (such as Enterprise authentication with cloud user/group or MAC allow lists), the SSIDs are in the non-standalone mode, that is, the FortiAP

needs to interact with the cloud controller for authentication. This feature is configured separately for standalone and non-standalone SSIDs.

- **FortiAPs deployed with Cloud dependent features** - **Enable AP Reboot with Timer** - Enable the automatic reboot of the FortiAP and configure the time interval the FortiAP waits before automatic rebooting, after losing connection with the cloud controller. The valid range is 5 to 65535 minutes and the default is 60 minutes.
- **FortiAPs deployed with at least one standalone SSID** - **Enable AP reboot with timer** - Enable automatic reboot in case if there is at least one standalone SSID beaconed by the FortiAP. Enter the time interval the FortiAP waits before automatic rebooting. The valid range is 5 to 65535 minutes and the default is 60 minutes.
- **Schedule AP reboot** - Enable the FortiAP to automatically reboot at a specific time when standalone SSIDs are pushed to the FortiAP in the previous session.

Note: This feature is supported on FortiAPs version 7.4.2 and above.

Editing Timeout Settings

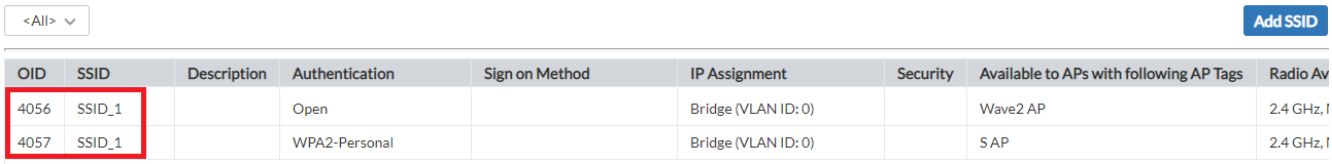
You can edit the timeout settings for **Idle Client** and **Captive Portal User Authentication**.

Enabling Duplicate SSID

A duplicate SSID bears the same wireless network SSID as another original SSID. The duplicate SSID can have different configurations and can be deployed on different APs/AP groups (AP tags).

Consider an example of an organization where an original SSID **Staff** is configured on **AP Group 1** located at the company headquarters. The duplicate SSID **Staff** is configured on **AP Group 2** located at the company branch. Both these SSIDs have different configurations, such as, VLANs, QoS, and so on. A wireless client moving from the headquarters (**AP Group 1**) to the branch (**AP Group 2**) seamlessly transitions from the original SSID **Staff** to the duplicate SSID **Staff** and is now governed by the configurations of the duplicate SSID.

The OID of the duplicate SSID is displayed for easy identification.



Note: The original and duplicate SSIDs must NOT be deployed on the same AP. This may prevent the wireless client from connecting to the desired SSID.

You must delete the duplicate SSIDs before disabling this feature.

Enabling DRMA Timeout

You can configure the specific interval to run DRMA in the Network configuration. The valid range is 10 - 1440 minutes.

Viewing the history of configuration changes

You can view the history of FortiLAN Cloud configuration changes.

Procedure steps

1. On the FortiLAN Cloud Home page, select the network.
2. In the Menu bar, navigate to **Configuration > Change History**.
3. The history of FortiLAN Cloud configuration changes presents the following details:
   - Time
   - Access IP
   - User
   - Email
   - Category
   - Action
   - New Value vs Old Value

   You can optionally filter these entries by the following time periods:
   - Last 60 Minutes
   - Last 24 Hours
   - Last 7 Days
   - Last 30 Days
   - Specify

   Note: The last 1000 entries of history are stored.

Operation Profiles

The following profiles configurations define specific features for FortiLAN Cloud operations.

- FortiAP Platform Profile
- QoS Profile
- BLE Profile
- Distributed Automatic Radio Resource Provisioning (DARRP)
- Schedule Profile

FortiAP Platform Profile

FortiLAN Cloud provides default platform (AP) profiles for each supported model. All APs of a given model can use their default platform profile. However, more profiles can be added, edited, and then assigned to APs, thereby changing their characteristic. For instance, two FAP 221E models can have their own platform profiles, one with rogue scanning disabled (using default platform profile) and the other enabled (using a customized platform profile).

Note: The 6 GHz band (Radio 3) is supported for the G series access points only. Related information is available in the dashboard, monitoring, and configuration functions of the GUI.

Other parameters that you can customize for each AP using its own platform profile include radio band, channel, channel width, and transmit power.

When you perform the Configuring FortiAP settings on page 82 procedure, you can select the FortiAP platform profile that you added using this procedure.

1. In the Menu bar,navigate to **Configuration > Operation Profiles > FortiAP Platform Profile**.
2. Near the top-right corner, click **Add Platform Profile**.

3. Customize the profile and update the following fields.
   Select the required Platform (AP model) for your network and Country, optionally, enter any Comments related to the platform profile.
4. Configure the following options as per your network requirement.

Configuration	Description
LED Off	Disables the LEDs from glowing on the FortiAP.
Deployment Type	You can select the operating environment for channels of a specific FortiAP, whether indoor or outdoor. This feature facilitates compliance with the access point placement regulations enacted in different geographical locations. You can now override the default placements of FortiAPs when configuring a FortiAP Platform Profile. This feature optimizes Wi-Fi performance and is beneficial in different deployment scenarios, such as the following. • Indoor APs are enclosed in outdoor enclosures, mimicking the form factor of their outdoor counterparts. • Outdoor APs are temporarily mounted in indoor hangers for testing or maintenance purposes. This feature is available only for these FortiAP models, FAP433F , FAP433G , FAP234F, FAP432FR,FAP432F and FAP234G.
Dedicated Monitor	In this mode, during FortiAP operation the radio scans for other available APs as a dedicated monitor. • When enabled, all radios except the last one do not scan, hence you cannot apply the WIDS profile to the last radio (WIDS option not available). This radio can be in disabled/monitor mode with/without WIDS profile. • When disabled, you can apply the WIDS profile to all radios. **Note**: This features is available only for F-series and G-series models and works only with *Single-5G* mode in G-series models.
Short Guard Interval	Configure the short guard interval to protect symbols (characters) transmitted in your packet from damaging other symbols by eliminating inter-symbol interference, thereby enhancing throughput. This is set to 400 nano seconds.
Channel Utilization	Select this option to monitor FortiAP's per radio channel utilization.
Radio Resource Provision	Select to enable DARRP to measures utilization and interference on the available channels and automatically and periodically select the optimal channel for your FortiAP.
Client Load Balancing	Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among FortiAPs and available frequency bands. The following types of client load balancing are supported. **AP Handoff** - The wireless controller signals a client to switch to another access point. **Frequency Handoff** - The wireless controller monitors the usage of 2.4 GHz and 5 GHz bands, and signals clients to switch to the lesser-used frequency.

Configuration	Description
TX Power	High-density deployments cover a small area that has many clients. Maximum AP signal power is usually not required. Enabling **Automatic TX Power Control** reduces power and interference between APs. This feature is based on the interference level of the strongest neighbour AP signal being higher than -70dBm. Additionally, you can configure the interference level as per your wireless network deployment. Configuring the target Tx power is particularly beneficial in high density deployments where multiple APs serve on the same channel. In such a scenario, it is possible that the highest neighbour AP signal strength could be greater than -70dBm. For example, if the AP signal strength is -50dBm, then the target value must be set close to -50dBm. Hence, avoiding the reduction of Tx power to very low values leading to coverage issues. The optimal value for this parameter is set based on the average RSSI of the neighbour APs, that is observed (as normal) in a deployment. The automatic Tx power is computed based on the target value, assume the strongest neighbour AP signal =S and the auto Tx power target = T, then: • If S > T: the current TX power is reduced by (S-T) • If S < T: the current TX power is increased by (T-S)
Rogue AP Scan	The access point radio scans, detects, and reports rogue APs in your network.
Call Admission Control	Enable to regulate voice traffic and specify the **Call Capacity**, the maximum number of concurrent VoIP calls allowed. The valid range is 0 – 60 and default is 10. **Bandwidth Admission Control**: Enable to limit traffic bandwidth usage and specify the **Bandwidth Capacity**, the bandwidth usage per second. The valid range is 0 – 600000 kbps and default is 2000 kbps.
LAN Port	To use the LAN port, run the `cfg -a WANLAN_MODE=WAN-LAN` command in the FortiAP, and select any of the following options. • NAT to WAN • Bridge to WAN • Bridge to SSID
UNII-4 5GHz band channels	FortiAP profiles support UNII-4 5GHz bands for FortiAP G-series models. FortiAP-431G and FortiAP-433G operating in Single 5G mode can make use of the UNII-4 frequency band. The 5.85 GHz-5.925 GHz channels of 169, 173, and 177 become available when configuring the 5GHz radio. There are a few important points to note about UNII-4 band usage. • UNII-4 5GHz channels are not available when FAP43xG models operate in Dual 5G platform mode. • Not all countries allow UNII-4 band usage. You can enable UNII-4 5GHz band channels in the Platform profile when operating in Single 5G mode with dedicated scan enabled.
External Antenna	• Enable the optional external antenna types for the FAP-432F, FAP-432FR, FAP-433F, FAPU-432F, FAPU-433F, FAP233G, and FAP433G FAP models. Configure the radio specific transmit power values. The supported range is 0 – 20 dBi.

The following features require a license for advanced AP management.

Configuration	Description
Dynamic Radio Mode Assignment	The *Adaptive Radio Architecture* (ARA) centralizes and improves the overall efficiency of the wireless network in high traffic conditions. **Dynamic Radio Mode Assignment** (DRMA) is a feature in ARA that enables FortiAPs to calculate the network coverage factor (NCF) based on radio interference. The NCF value is calculated at configured intervals and is based on overlapping coverage in a radio coverage area. When DRMA is enabled and the NCF value crosses the configured threshold, then the radio becomes redundant by switching from AP mode to monitor mode. On subsequent NCF calculation, if the value is below the threshold then the radio switches back to AP mode. The **DRMA Sensitivity** determines the NCF threshold value to consider a radio redundant or not. The following are the permissible values. • Low: 100% NCF • Medium: 95% NCF • High: 90% NCF You can configure the DRMA interval in Network Settingsand override the configuration in Overriding FortiAP Settings on page 84 You can view the DRMA AP events in the **Wireless** logs displayed in Viewing the FortiAP status. Logs are generated when DRMA runs and stops, also, whenever the operational mode of the radio changes.
Upgrade APs upon Connect	Enables upgrade of newly deployed FortiAPs associated with this Platform profile. The firmware is upgraded to the *Target Firmware Version* when the FortiAP connects to the FortiLAN Cloud. If this FortiAP is included in the *Scheduled Upgrade* profile ensure that the target firmware versions match. To upgrade fully deployed FortiAPs, see Scheduled Upgrades on page 141.
Force Downgrade	Forcefully downgrades newly deployed FortiAPs with a firmware version greater than the *Target Firmware Version*.
Target Firmware Version	The firmware version that the newly deployed FortiAPs are upgraded/downgraded to.
Enhanced Logging	Enable to receive and store more than 50 categories of logs from the FortiAPs with detailed insights into all network activity. The logs provide specific insights into different stages of client connection to troubleshoot/enhance poor wireless connectivity experience.
Console Login	You can enable/disable console port access on the FortiAP. This feature is enabled by default and is supported on FortiOS 7.0.1 and higher. You can edit the access point settings to override this feature configuration on a per FortiAP basis (**Console Login Override**) **Note**: Modifying this feature setting reboots the FortiAP.
Airtime Fairness	Wi-Fi has a natural tendency for clients farther away or clients at lower data rates to monopolize the airtime and drag down the overall performance. Airtime Fairness (ATF) helps to improve the overall network performance.

Configuration	Description
AP Scan Threshold	Configures the threshold for minimum detected signal strength required for a FortiAP to be categorized as an interfering/rogue AP when a scan is performed. This parameter is supported in the monitor mode and conditionally in the AP mode with either of the these parameters enabled, Radio Resource Provision, Auto TX Power Control enabled, Rogue AP Scan. The valid range of signal strength is -95 to -20 dBm with a default of -90 dBm.
Beacon Interval (ms)	Configures the time interval between two successive beacon frames. The beacon interval is measured in milliseconds and supports a valid range of 40 – 3500 milliseconds with a default of 100 milliseconds. Higher beacon intervals aid in the power saving capability of wireless clients and lower beacon intervals keep fast roaming clients connected to the network.
DTIM Period	Configures the Delivery Traffic Indication Map (DTIM) interval to transmit buffered multicast and broadcast data, after the beacon is broadcast. This enables wireless clients in power-saving mode to wake up at a suitable time to check for buffered traffic. Higher DTIM period aids in the power saving capability of wireless clients and lower DTIM period speeds up broadcast and multicast data delivery to wireless clients. The valid range is 1 -255 with a default of 1. The recommended values are 1 (to transmit broadcast and multicast data after every beacon) and 2 (to transmit broadcast and multicast data after every other beacon).
TX Optimization	The data packet transmit optimization feature enables a set of options in your FortiAP to enhance transmission performance and minimize packet loss. **Note**: This feature is supported only on 2.4G radios of the FAP-U series. The following optimization options are available and are enabled by default. • **Power Save**: Tags the client as operating in the power-save mode if excessive transmit retries are detected. • **Aggregation Limit**: Reduces the aggregation limit if the data transmission rate is low. • **Retry Limit**: Reduces the software retry limit if the data transmission rate is low. • **Send BAR**: Limits the transmission of the BAR (Block Acknowledgement Request) frames. This feature is disabled if none of the options is selected.
802.11d	The 802.11d wireless networking standard, also known as the *Country Information Element*, allows Wi-Fi devices to dynamically adjust their settings, such as channel selection and transmit power, based on the regulatory domain in which they are operating. This adds the ability to toggle 802.11d support for 2.4 GHz radios through a Platform profile. When 802.11d is enabled, the FortiAPs broadcast the country code in beacons, probe responses, and probe requests. This led to some older legacy clients failing to associate to the FortiAP. The ability to disable 802.11d prevents the broadcasting of country code settings and provides backwards compatibility with those clients.

Configuration	Description
	Note: Since IEEE 802.11d only applies to 2.4 GHz radios operating in the 802.11g band, disabling 802.11d only applies to radios configured to operate in the 802.11g band.
Energy Efficient Ethernet	This features is also known as IEEE 802.3az standard for Ethernet devices to consume less power during periods of low data activity. This is supported on all FAP models whose Ethernet NIC supports this feature.
MIMO Mode Setting	Configure the Multiple Input Multiple Output (MIMO) mode settings on all FortiAP models with firmware version 7.4.1 or later and on FortiAP-U models with firmware version 7.0.2 and above. When configured, multiple antennas are used at both the source (transmitter) and the destination (receiver), to enable data to travel over many signal paths at the same time. These antennas are combined at each end of the communications circuit to improve the capacity of radio transmissions, thereby minimizing errors and optimizing data speed. The following MIMO modes are selected for various FortiAP models. • FortiAP 23x models - 2x2 MIMO mode • FortiAP 32x models - 2x2 and 3x3 MIMO modes • FortiAP 43x models - 2x2, 3x3, and 4x4 MIMO modes • FortiAP 83x models - 1x1, 2x2, 3x3, 4x4, and 8x8 MIMO modes By default, the highest MIMO mode is selected.

5. To save the profile, click **Apply**.
   The list of profiles includes the new FortiAP platform profile.

QoS Profile

When you add an SSID to a network, you can assign a quality of service (QoS) profile to that SSID. The QoS profile helps to set up different QoS parameters for voice, video, data wireless networks, or guest/employee wireless networks.

FortiLAN Cloud transfers the QoS configuration parameters to each FortiAP, which then interprets the values and enforces the QoS.

Prerequisites

Complete the Managing Networks on FortiLAN Cloud on page 35 procedure.

1. On the FortiLAN Cloud Home page, select the network to which you want to add the QoS profile.
2. In the Menu bar, navigate to **Configuration > Operation Profiles > QoS Profile**.
3. Click **Add QoS Profile**.
4. Complete the following fields:

Name	The name you want to give to the QoS profile.
Comment	A description of the QoS profile or any other text for this profile. This field is optional.
Uplink	The maximum uplink bandwidth for each FortiAP radio, defined by the SSID.

	Here is an SSID example (with two radios) and an uplink value of 100000 Kbps: • 10 stations are connected to the Guest SSID on 2.4 GHz (radio 1): The total maximum uplink bandwidth of the stations connecting to that Guest SSID is 100000 Kbps. • 20 stations are connected to the Guest SSID on 5 GHz (radio 2): The total maximum uplink bandwidth of the stations connecting to that Guest SSID is 100000 Kbps. The range is from 0 to 2097152 Kbps (or approximately 2 Gbps). The default is 0, which means there is no restriction.
Downlink	The maximum downlink bandwidth for each FortiAP radio, defined by the SSID. Here is an SSID example (with two radios) and a downlink value of 100000 Kbps: • 10 stations are connected to the Guest SSID on 2.4 GHz (radio 1): The total maximum downlink bandwidth of the stations connecting to that Guest SSID is 100000 Kbps. • 20 stations are connected to the Guest SSID on 5 GHz (radio 2): The total maximum downlink bandwidth of the stations connecting to that Guest SSID is 100000 Kbps. The range is from 0 to 2097152 Kbps. The default is 0, which means there is no restriction.
Station Uplink	The maximum uplink bandwidth for each station in the SSID. The range is from 0 to 2097152 Kbps. The default is 0, which means there is no restriction.
Station Downlink	The maximum downlink bandwidth for each station in the SSID. The range is from 0 to 2097152 Kbps. The default is 0, which means there is no restriction.
Burst	When you enable the burst parameter on the SSID, the first couple of packets have a large buffer to upload and download after the station connects. After that, the station traffic returns to normal. By default, the Burst checkbox is unselected.
WMM	QoS WiFi Multi-Media (WMM) enables priority marking of data packets from different applications and preserving these markings by translating them into DSCP values when forwarding them upstream and downstream. The priority is set between four access categories; voice, video, best effort, and background. The applications that require improved throughput and performance are inserted in queues with higher priority. WMM maintains the priority of these applications over others which are less time critical. You can customize the priority markings for various traffic types and apply these changes to WMM-enabled SSID profiles. All configurations are disabled by default. **Note:** This feature is supported with FOS 6.2.0 and above and requires a FortiAP-S or FortiAP-W2 device. • **WMM UAPSD**: The Unscheduled Automatic Power Save Delivery (UAPSD) enables the power save mechanism. • **Call Admission Control**: Enable this option to regulate voice traffic. Specify the **Call Capacity**, the maximum number of concurrent VoIP calls allowed. The valid range is 0 – 60 and default is 10.

- **Bandwidth Admission Control**: Enable this option to limit traffic bandwidth usage. Specify the **Bandwidth Capacity**, the bandwidth usage per second. The valid range is 0 – 600000 kbps and default is 2000 kbps.

Configure the **Call Admission Control** and **Bandwidth Admission Control** parameters when creating a *Platform profile*.

Specify the appropriate DSCP values for downstream (LAN to WLAN) traffic. You can map one or more (up to 16) DSCP values into the following access categories. For example, DSCP values 48 and 56 (and even other non-standard values used in your network) can be mapped into the WMM access category - Voice.

- **DSCP Voice Mapping**: DSCP mapping for the voice traffic.
- **DSCP Video Mapping**: DSCP mapping for the video traffic.
- **DSCP Best Effort Mapping**: DSCP mapping for the best-effort traffic.
- **DSCP Background Access Mapping**: DSCP mapping for the background traffic.

Specify the appropriate DSCP values for upstream (WLAN to LAN) traffic. You can mark the following access categories with appropriate DSCP values. For example, DSCP value 48 can be used to mark the WMM access category - Voice.

- **DSCP Voice AC**: DSCP mapping for the voice traffic.
- **DSCP Video AC**: DSCP mapping for the video traffic.
- **DSCP Best Effort AC**: DSCP mapping for the best-effort traffic.
- **DSCP Background AC**: DSCP mapping for the background traffic.

5. To complete the addition of the QoS profile, click **Apply**.

BLE Profile

BLE is a wireless personal area network technology used for transmitting data over short distances. It allows mobile applications to receive advertisements from beacons and deliver hyper-contextual content to clients based on location. The BLE profile incorporates Google's Eddystone and Apple's iBeacon to identify groups of devices and individual devices. Broadly, based on the configured BLE profile, the FortiAP broadcasts signals that the client receives when it comes in the configured proximity.

Individual AP overrides for BLE profile parameters are supported. See section Overriding FortiAP Settings on page 84.

Name - Enter a unique name for the BLE profile. Valid range is 1 – 32 characters.

Advertising – Select one or multiple supported advertising protocols, **iBeacon**, **Eddystone UUID**, **Eddystone URL**.

You can configure the following broadcast data for iBeacon.

- **iBeacon UUID** – Click **Generate UUID** to obtain a unique 128-bit identifier in 8-4-4-4-12 Hex format for a beacon. Specify **wtp-uuid** to generate FortiAP specific identifier.
- **iBeacon Major ID** – A unique identifier assigned to some beacons in a network and is used to distinguish this subset of beacons within a larger group of beacons. For example, beacons within a particular geographic area can have the same major number. The valid range is 0 -65535 with a default of 1000.
- **iBeacon Minor ID** - A unique identifier assigned to identify individual beacons. For example, each beacon in a group of beacons with the same major number, will have a unique minor number. The valid range is 0 -65535 with a default of 2000.

You can configure the following broadcast data for Eddystone UUID.

- **Eddystone Namespace ID** – A unique identifier assigned to some beacons in a network. This serves the same purpose as the aforementioned iBeacon Major ID. The valid range is 1 -20 Hex digits, the corresponding ASCII

value is also displayed. You can enter the ID in ASCII format also using the ASCII link.

- **Eddystone Instance ID** - A unique identifier assigned to identify individual beacons. This serves the same purpose as the aforementioned iBeacon Minor ID. The valid range is 1 - 12 Hex digits, the corresponding ASCII value is also displayed. You can enter the ID in ASCII format also using the ASCII link.

Eddystone URL - The FortiAP broadcasts the configured URL as a beacon and the physical web or the latest Google Chrome plugin picks up the beacon and renders the URL into a web page. The URL supports HTTP and HTTPS and valid range is 1 -30 characters. The default is **http://www.fortinet.com**.

TX Power Level – Select a power level for the beacon's transmit signal. The higher the power the greater will be the range of your signal. The valid range is –21 dBm to +5 dBm with a default value of 0 dBm.

Beaconing Interval - Select the time interval at which the successive beacons transmit signals to associated devices, that is, this sets the rate at which beacons advertise packets. The valid range is 40 -3500 milliseconds with a default of 100 milliseconds.

BLE Scanning – Enable scanning for BLE devices. This is disabled by default.

BLE Scan Report Interval – The interval to generate BLE scan report. The valid range is 10 – 3600 seconds with a default value of 30 seconds.

Distributed Automatic Radio Resource Provisioning (DARRP)

When DARRP is enabled, FortiAPs continuously monitor the RF environment for interference, noise and signals from neighboring APs or other devices operating in the same frequency range. Interference on the configured channel can affect the WiFi experience for your network user. DARRP determines the optimal RF power levels to automatically and periodically select the optimal channel for wireless communication. This is done by measuring utilization and interference on the available channels, mainly by canning the neighbor APs, signal strength, and channel width of the radio. This feature is especially useful in large-scale deployments where multiple access points have overlapping radio ranges. DARRP selects the optimal channel without manual intervention and facilitates an optimized wireless infrastructure to deliver maximum performance.

Also, the FortiAP automatically adjusts the TX power levels, when the FortiAP detects any other wireless signal stronger that -70 dBm, it reduces its transmission power until it reaches the minimum configured TX power limit and when any wireless client signal weaker than -70 dBm is detected, it reduces its transmission power until it reaches the maximum configured TX power limit.

- Configuring Basic DARRP
- Configuring Advanced DARRP

Configuring Basic DARRP

Basic DARRP configuration is enabled by default.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration > Operation Profiles > DARRP Profile**.
3. Enable DARRP optimization for your network. Configure the following parameters.
   - **Optimize Timer** - Configures the timer interval for DARRP optimization. The default is 10 minutes and the valid range is 10 - 1440 minutes.
   - **Optimize Schedule** - Configures **One Time** or **Recurring** schedules. One time schedule initiates DARRP optimization only once on a particular day and time. Recurring schedule initiates and repeats DARRP optimization on specific days and time of the week. A maximum of 4 schedules can be created for both types.

- **Optimize Now** - Manually initiates DARRP optimization. This operation occurs irrespective of the configured timer or schedule.

Configuring Advanced DARRP

Advanced DARRP configuration uses various additional parameters to perform DARRP optimization and accurate channel planning. It integrates data from channel utilization and takes into consideration the neighbour AP channel configuration and non-WiFi interference sources. The DARRP profile must be applied per radio in the Platform profile.

Notes:

- Supported on FortiAP version 6.4.2 or higher.
- Spectrum analysis and channel utilization features are used. FortiLAN Cloud uses spectrum analysis in the *scan only* mode and restores it's original configuration when DARRP is disabled.
- FortiAP Advanced Management License is required for this feature.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, click **Configure**.
3. In the Navigation pane, click **DARRP Profile**.
4. Click **Add Profile** and configure the following parameters.

Profile Name	A unique DARRP Profile name. Valid range is 1 - 36 characters.
Description	Any remarks/notes specific to the profile. The valid range is 0 – 255 characters.
Selection Period	The time period to measure average channel load, noise floor, spectral RSSI. The valid range is 0 to 65535 seconds and the default is 3600 seconds.
Monitor Period	The time period to measure average transmit retries and receive errors. The valid range is 0 to 65535 seconds and the default is 300 seconds.
Managed AP Weight	The weight in DARRP channel score calculation for managed APs. The valid range is 0 to 2000 and the default is 50.
Rogue AP Weight	The weight in DARRP channel score calculation for rogue APs. The valid range is 0 to 2000 and the default is 10.
Noise Floor Weight	The weight in DARRP channel score calculation for noise floor. The valid range is 0 to 2000 and the default is 40.
Channel Load Weight	The weight in DARRP channel score calculation for channel load. The valid range is 0 to 65535 and the default is 20.
Spectral RSSI Weight	The weight in DARRP channel score calculation for spectral RSSI. The valid range is 0 to 2000 and the default is 40.
Weather Channel Weight	The weight in DARRP channel score calculation for weather channels. The valid range is 0 to 2000 and the default is 1000.
DFS Channel Weight	The weight in DARRP channel score calculation for DFS channels. The valid range is 0 to 2000 and the default is 500.
AP Threshold	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs. Integer value from 1 to 500 (default = 250)

Noise Floor Threshold	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor. dBm (-95 to -20, default = -85)
Channel Load Threshold	The threshold to reject a channel in DARRP channel selection phase 1 due to channel load. The valid range is 0 to 100% and the default is 60%.
Spectral RSSI Threshold	The threshold to reject a channel in DARRP channel selection phase 1 due to spectral RSSI. The valid range is -95 dBm to -20dBm and the default is -65 dBm.
Tx Retries Threshold	The threshold for transmit retries to trigger channel reselection in DARRP monitor stage. The valid ranges is 0 to 1000% and the default is 300%.
Rx Errors Threshold	The threshold for receive errors to trigger channel reselection in DARRP monitor stage. The valid range is 0 to 100% and the default is 50%.
Include Weather Channel	To enable or disable the use of weather channels in DARRP channel selection. This is disabled by default.
Include DFS Channel	To enable or disable the use of DFS channels in DARRP channel selection. This is disabled by default.

Schedule Profile

This feature allows each Multiple PSK entry to have its own availability schedule based on different time periods. The defined schedule profile is referred to by the Multiple PSK entries in the SSID profile.

Notes:

- Maximum number of profiles allowed is1024 and each profile can have 1 - 40 schedules.
- Schedule profiles cannot be deleted when used by a Multiple PSK in the SSID.
- Date and time are scheduled as per the network timezone.

1. On the FortiLAN Cloud Home page, select the network to which you want to create the Schedule profile.
2. In the Menu bar, click **Configuration > Operation Profiles > Schedule Profile**.
3. Click **Add Profile**.
4. Complete the following fields:

Name	A unique name for the profile/schedule. The valid range is 1 – 36 characters.
Comment	Any remarks/notes specific to the profile/schedule. The valid range is 0 – 255 characters.
Type	Each individual schedule is either **One-Time** or **Recurring**. One-Time schedules have absolute start and stop date/time and they expire after the configured period. Recurring or repetitive schedules have start/stop time for selected days of the week and they never expire. When the **All Day** option is selected, the schedule applies to all days of the week with the start and stop time set to 00:00. Disable the **All Day** option to select specific week days and modify the start and stop time. **Note**: The schedule **Type** cannot be modified after the profile is created.

Connectivity Profiles

The following profile configurations define connectivity aspects of FortiLAN Cloud.

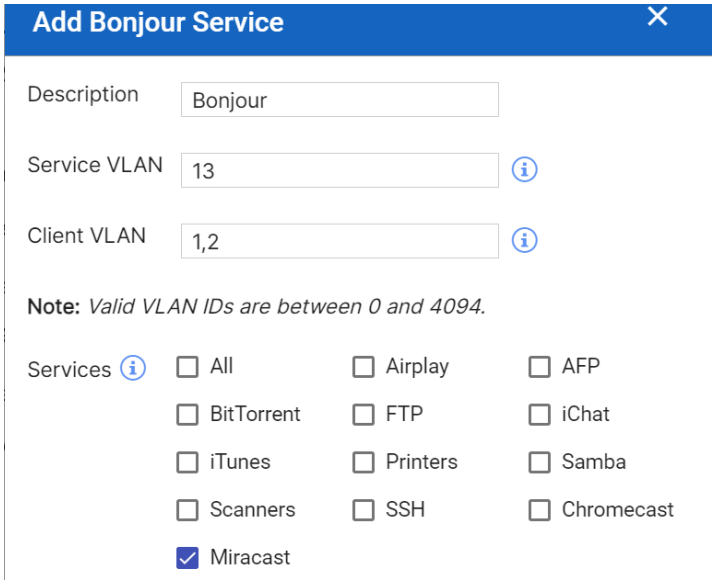
- Bonjour Relay
- FortiPresence

Bonjour Relay

Bonjour is a protocol where devices broadcast their services. For example, an Apple TV sends a Bonjour broadcast, so an iPad knows it is there and can connect to it.

With Bonjour Relay, you set the FortiAP-S device to operate with a service network (where the Apple TV is), and a client network (where the iPad is). The FortiAP-S device re-transmits the Bonjour requests from the service network onto the client network. The iPad can learn where the Apple TV is and create a session.

To set up Bonjour Relay, enter one or more services as Service VLAN and Client VLAN, along with a definition of the service. For example, you may choose to only send the information about the Apple TV to a meeting room, and not to the printer in reception. After you define these services, select the FortiAP that will perform the Bonjour Relay function.



Prerequisites

You must purchase a FAP Advanced Management License.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration > Connectivity Profiles > Bonjour Relay**.
3. Select the **Enable Bonjour Relay** checkbox.
4. To add the Bonjour Service:
   a. Go to the **Bonjour Service** section and click the plus sign (+).
   b. Complete the following fields:

Description	Specify a name for the Bonjour Service.

Service VLAN	Specify one or more VLAN ID where network services are running. A valid VLAN ID is from 0 to 4094. APs support up to 32 VLAN entries. To specify multiple entries, use a comma (,) or a dash (-). For a full range, use "all". When you use "all", it counts as one entry. For example, 1,2-5.
Client VLAN	A valid VLAN ID is from 0 to 4094. APs support up to 32 VLAN entries. To specify multiple entries, use a comma (,) or a dash (-). For a full range, use "all". When you use "all", it counts as one entry. For example, all.
Services	Select one or more Bonjour services that you want to advertise across the network. The Miracast service is a wireless projection feature by which a video stream from a source device (laptops/smart phones) is carried over a WiFi network to a display device. This is also a form of Avahi (Bonjour) service. The TCP port for Miracast mDNS packets is 7250. To enable all services, select the **all** checkbox.

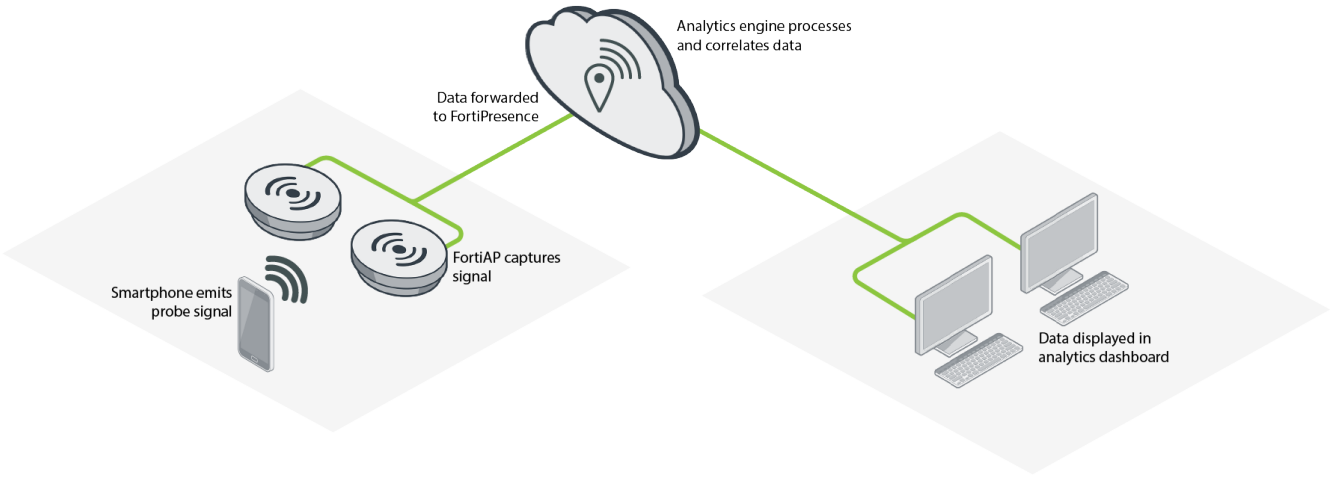
5. To save changes, click **Submit**.
6. To add a Bonjour Relay Gateway:
   a. Go to the **Bonjour Relay Gateway** section and click the plus sign (+).
   b. For each subnet, select only one AP as the Bonjour Relay Gateway.
   c. To save changes, click **Submit**.

FortiPresence

FortiPresence is a secure and comprehensive data analytics solution designed to provide presence and positioning analytics for user traffic. By capturing analytics of consumer traffic patterns, businesses can learn more about their customers.

For location analytics, the FortiAP uses a Push API to communicate with FortiPresence.

1. Smartphone emits a Wi-Fi probe signal, even if it is in the visitor's pocket and not connected to the Wi-Fi network.
2. FortiAP captures the MAC address and signal strength information from the smartphone.
3. FortiLAN Cloud managed AP summarizes and forwards the data records directly to FortiPresence.
4. FortiPresence service receives data.
5. FortiPresence analytics engine processes and correlates the data.
6. Data is displayed in the analytics dashboard in an actionable format.



Prerequisites

- Access your FortiPresence account UI and navigate to **Admin** > **Settings** > **Discovered APs** to retrieve the following parameters:
  - Project Name
  - Project Secret Key
  - Location Server IP
  - Port
- For FortiPresence configuration details, see the following sections in the FortiPresence Administration Guide:
  - Configuring location services
  - Configuring captive portal

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration > Connectivity Profiles > FortiPresence**.

3. Complete the following fields:

Mode	Select one of the following options to enable FortiPresence: • **Foreign Channels Only**: With this setting AP will only listen to clients on foreign channels when doing background scan. It will not listen to clients associated to other APs running on its home (or operating) channel to preserve associated clients traffic. • **Foreign and Home Channels**: AP will also listen to connected clients associated to other APs on its home channel. This is useful for FortiPresence, but can negatively impact AP performance when AP is serving clients.
Server IP Address	Specify the IP address/FQDN of the server. Copy the value from the FortiPresence UI. **Note**: FortiPresence FQDN is supported only on FortiAP 7.0 and later; for FortiAPs with lower version, specify the IP address. In the FortiPresence UI, the value is in the **Location Server IP** field.
UDP Listening Port	Type UDP listening port. The default is 3000. Copy the value from the FortiPresence UI. In the FortiPresence UI, the value is in the **Port** field.
Project Name	Specify a project name. Copy the value from the FortiPresence UI. In the FortiPresence UI, the text is in the **Project Name** field.
Secret Password	Type fortipresence. Copy the value from the FortiPresence UI. In the FortiPresence UI, the password is in the **Project Secret Key**field.
Report Transmit Frequency	Frequency at which each AP will report wireless client information to the FortiPresence server. The default is 30 seconds. The range is between 5 and 65535 seconds (or approximately 18 hours).
Reporting of Rogue APs	If you want FortiPresence to report rogue APs, select the checkbox.
Reporting of Unassociated Stations	If you want FortiPresence to report unassociated stations, select the checkbox.

4. Click **Apply**.

Protection Profiles

The following profile configurations define security features in FortiLAN Cloud.

- Wireless Intrusion Detection and Suppression (WIDS)
- L3 Firewall Profile
- Tunnel Profile

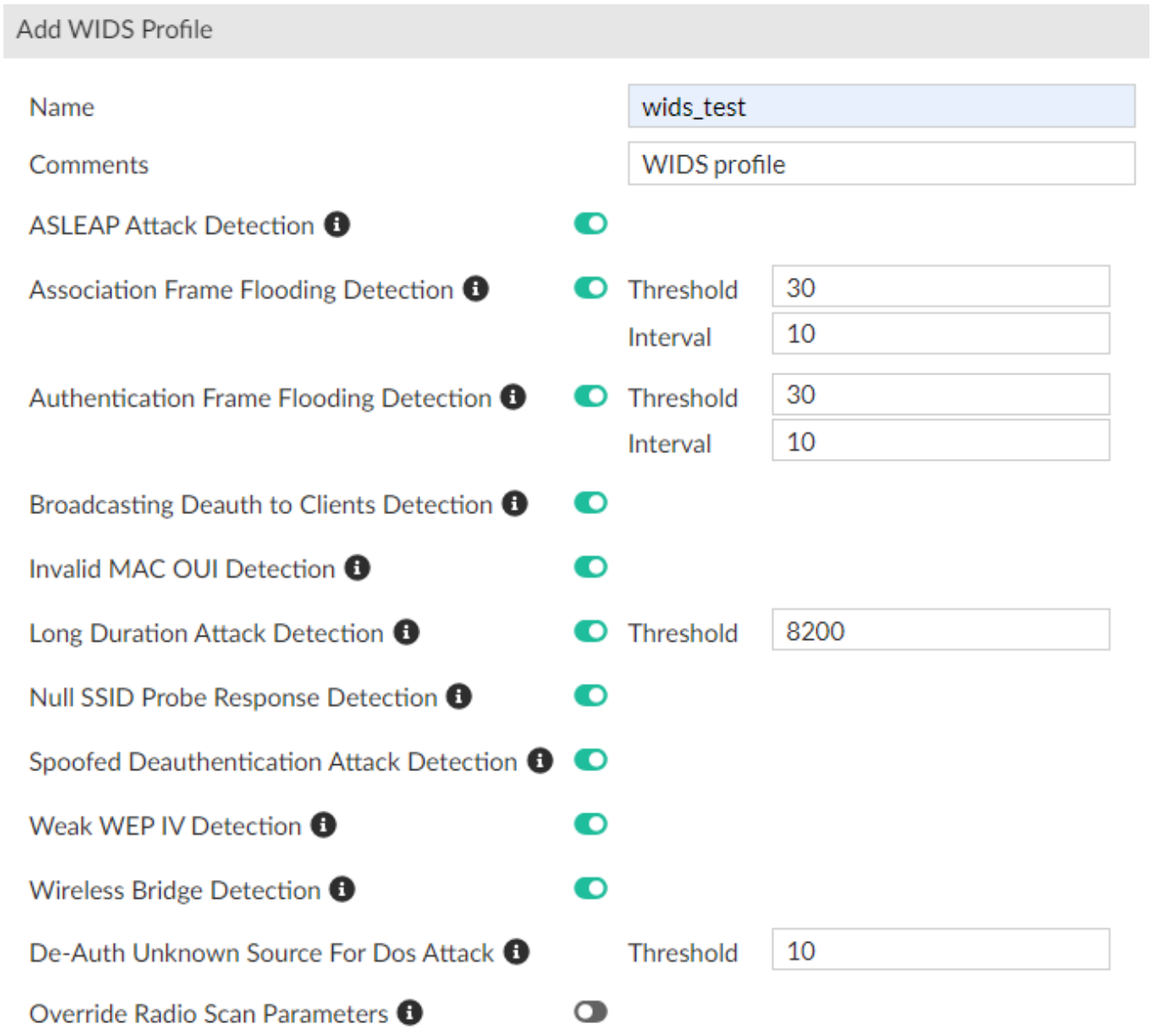
Wireless Intrusion Detection and Suppression (WIDS)

The WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting possible intrusion attempts.

Adding a WIDS Profile

When an attack is detected, FortiLAN Cloud records a log message. The FortiAPs that have a dedicated radio for scanning, use that same radio for WIDS scanning. Create a WIDS profile to configure the wireless intrusion monitoring and detection parameters, and then associate the WIDS profile with radios in the Platform Profile. This association causes FortiLAN Cloud to push the configured WIDS profile to all FortiAP radios linked with the platform profile.

Navigate to **Wireless > Configuration > Protection Profiles > WIDS Profile**.

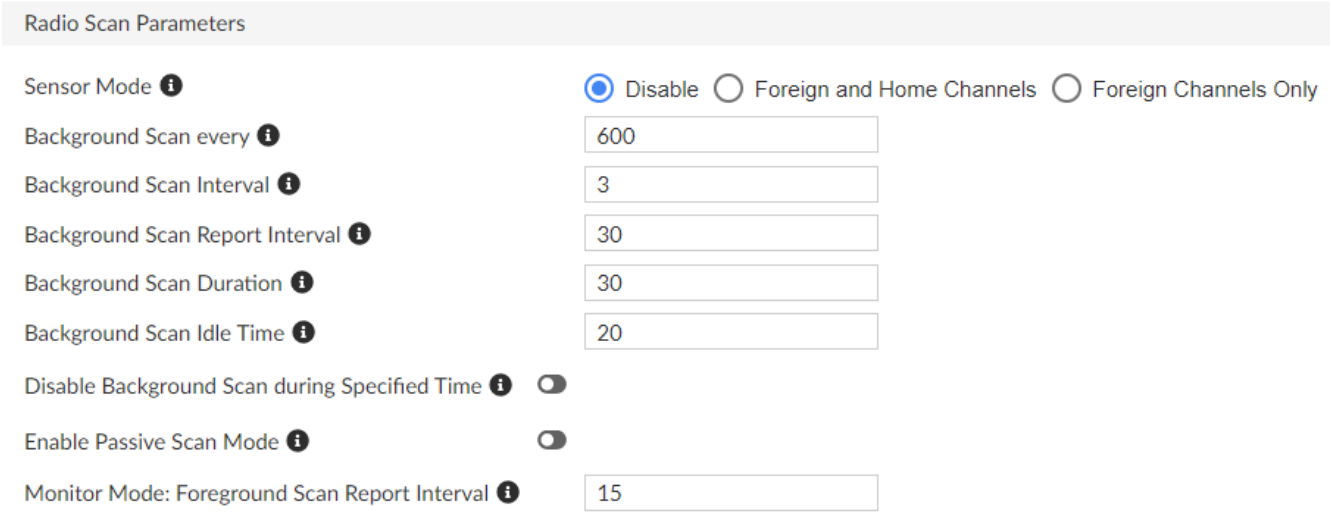


You can configure WIDS against the the following types of intrusions.

Type of Attack	Description
ASLEAP Attack Detection	The attacker uses the ASLEAP tool to attack clients against LEAP authentication.
Association Frame Flooding Detection	This is a Denial-of-Service (DoS) attack using a large number of association requests. The default detection threshold is 30 requests (range is 1 to 100 requests) in 10 seconds interval (range is 5 to 120 seconds).
Authentication Frame Flooding Detection	This is a DoS attack using a large number of authentication requests. The default detection threshold is 30 requests (range is 1 to 100 requests) in 10 seconds interval (range is 5 to 120 seconds).
Broadcasting Deauth to	This is a DoS attack. A flood of spoofed de-authentication frames forces wireless

Type of Attack	Description
Clients Detection	clients to de-authenticate, then re-authenticate with their AP.
Invalid MAC OUI Detection	Some attackers use randomly generated MAC addresses. The first 3 bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged when this field is enabled.
Long Duration Attack Detection	To share radio bandwidth, Wi-Fi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a DoS attack. You can set a threshold between 1,000 and 32,767 microseconds (default = 8200).
Null SSID Probe Response Detection	In this attack, when a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Spoofed Deauthentication Attack Detection	The attacker sends spoofed de-authentication messages to the FortiAP on behalf of the client. These spoofed de-authentication frames form the basis for most DoS attacks, disconnecting all clients from the FortiAP.
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs), that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge Detection	Wi-Fi frames with both *FromDS* and *ToDS* fields set indicate a wireless bridge. This also detects a wireless bridge that you intentionally configured in your network.
De-Auth Unknown Source For Dos Attack	This is a DoS attack where an unknown client sends a large number of de-authentication requests in quick succession. In an aggressive attack, this de-authentication activity can prevent packet processing from valid clients. As part of mitigating a DoS attack, the FortiAP sends de-authentication packets to unknown clients. In an aggressive attack, this de-authentication activity can prevent the processing of packets from valid clients. The threshold value set is a measure of the number of de-authorizations per second. It can be 0 to 65535 (default = 10 and 0 means no limit).

Enabling **Override Radio Scan Parameters** overrides the radio scan parameters defined at the network level (**Configuration > Network**).



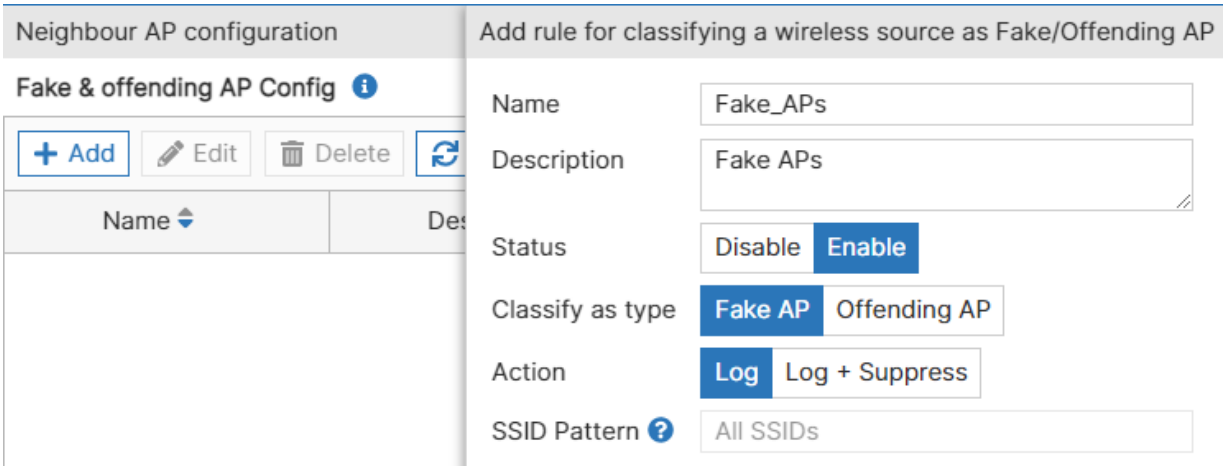
Detecting Fake and Rogue Access Points

You can configure rules for automatic detection of fake and offending SSIDs. Additionally, it is also possible to configure actions and counter measures to be taken when these categories of threats are detected. FortiLAN Cloud actively scans and reports the neighbour APs to identify other access points in the area to know their potential impact on the FortiAPs managed by FortiLAN Cloud. You can define the policy to classify the detected neighbour access points **Fake & Offending** and **Rogue & Accepted**. Navigate to **Wireless > Monitor > Neighbour APs**.

Fake & Offending

Fake and Offending categories include phishing access points that lead clients to connect to fake/offending access points instead of getting connected to legitimate FortiAPs. A fake access point broadcasts the same SSID as the legitimate FortiAP and an offending access point broadcasts SSIDs that falsely represent the company/organization/department of the legitimate FortiAP.

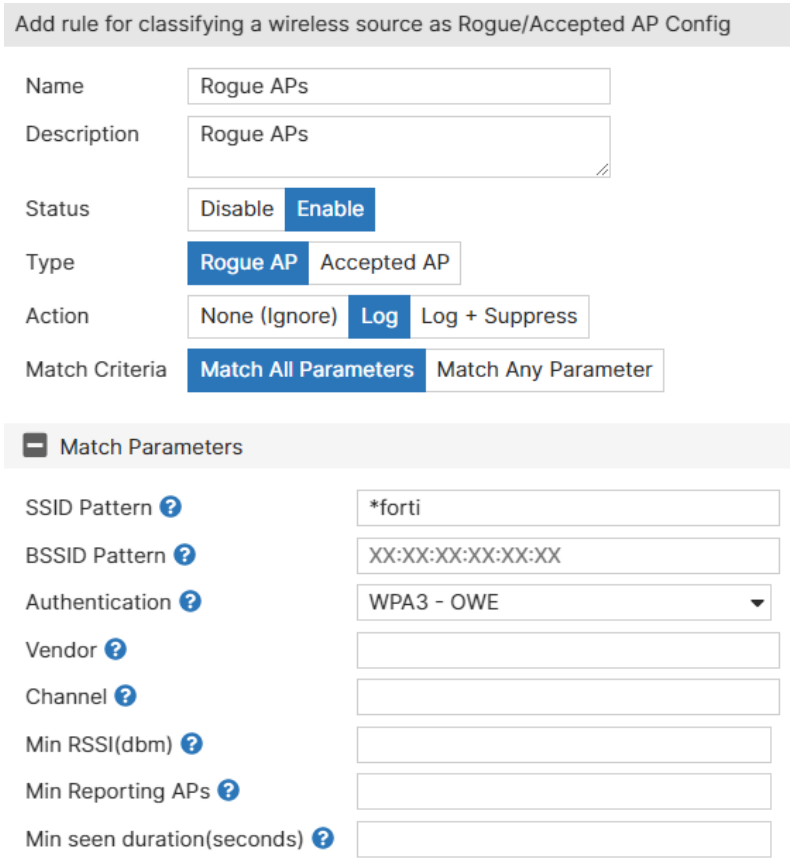
You can configure the criteria for classifying the detected neighbour access points as fake or offending. FortiLAN Cloud compares the received neighbour access point data with the configured policy (SSID) and in case of a match, categorizes them and takes the action as per the configured policy parameters.



Rogue & Accepted

A neighbour access point that could potentially affect the performance of the FortiAPs managed by FortiLAN Cloud, is classified as rogue and a neighbour access point with no adverse impact or interference in the FortiAP wireless network operations are deemed acceptable.

You can configure a single or multiple parameters for the classification of FortiAPs as rogue or acceptable. FortiLAN Cloud compares the received neighbour access point data with the configured parameters and in case of a match, categorizes them and takes the action as per the configured policy parameters.



Notes:

- SSID and BSSID patterns allow up to one wildcard (*) character.
- You can create multiple configuration profiles and each configuration profile can specify only a single SSID/BSSID pattern.
- The specified SSID pattern is case-insensitive.

L3 Firewall Profile

Layer 3 Firewall rules provide granular access control of client traffic in your wireless network. An L3 Firewall profile allows or denies traffic between wireless clients based on the configured source and destination IP addresses/ports and specific protocols. The L3 Firewall profile must be assigned to an SSID profile.

Notes:

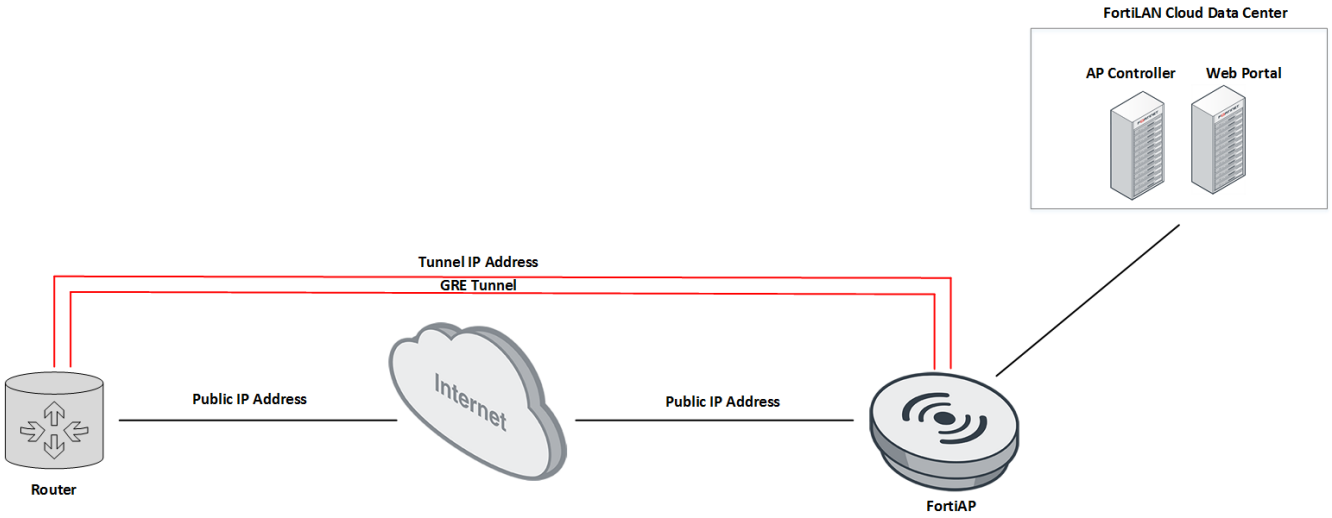
- The maximum number of rules allowed per profile are to 64.
- FortiAP Advanced Management License is required for this feature.

1. On the FortiLAN Cloud Home page, select the network to which you want to create the L3 Firewall profile.
2. In the Menu bar, navigate to **Configuration > Protection Profiles > L3 Firewall Profile**.
3. Click **Add Profile**.
4. Complete the following fields:

Name	A unique L3 Firewall Profile name. Valid range is 1 - 32 characters.
Rule ID	A unique rule identifier. The L3 Firewall rules are sorted and processed in the ascending order of the rule IDs, that is, starting from the lowest rule ID. The valid range is 1 - 65535 and a rule ID cannot be modified. **Note**: It is recommended to have a buffer between rule IDs to facilitate creating new rule IDs in future.
Enabled	Select to enable or disable the rule.
Comment	Any remarks/notes specific to the rule. The valid range is 0 – 255 characters.
IP Version	Select the IP rule type. You can create IPv4 or IPv6 rules based on your network requirements.
Policy	Select the policy action for the rule. Wireless traffic can be allowed or denied based on the configured rule.
Protocol	Select the protocol type to apply the rule. The protocol types are defined based on the Internet Assigned Numbers Authority (IANA) categorization. The valid range is 0 – 255.
Source Address	Specifies the source IP address to match the rule. You can select **Any** to specify all networks, **Local LAN** IP addresses, or **Specify** an IP address and the optional netmask length with a valid range of 0 – 32.
Source Port	Specify the source port to match the rule. This is single port and the valid range is 0-65535.
Destination Address	Specifies the destination IP address to match the rule. You can select **Any** to specify all networks, **Local LAN** IP addresses, or **Specify** an IP address and the optional netmask length with a valid range of 0 – 32.
Destination Port	Specify the destination port to match the rule. This is single port and the valid range is 0-65535.

Tunnel Profile

When you add an SSID to a network, you can assign a generic routing encapsulation (GRE) tunneling or a Layer 2 Tunneling Protocol (L2TP) profile to that SSID. The configured GRE tunnel profile encapsulates data traffic from wireless and wired clients between the FortiAP and a GRE concentrator, for example, a router.



The configured L2TP profile allows Internet Service Providers (ISP) to enable VPN services using an encryption protocol. Traffic is encrypted within the tunnel that is established between the FortiAP and an L2TP access concentrator.

Note: You cannot delete a tunnel profile if it is being used by an SSID.

Prerequisites

Complete the Managing Networks on FortiLAN Cloud on page 35 procedure.

1. On the FortiLAN Cloud Home page, select the network to which you want to add the tunnel profile.
2. In the Menu bar, navigate to **Configuration > Protection Profiles > Tunnel Profile**.
3. Click **Add Tunnel Profile**.

4. Complete the following fields:

Name	Enter a unique name for the tunnel. The name can be from 1 to 32 characters.
Tunnel Type	Select **GRE** or **L2TP** as the tunnel type.
Tunnel IP address	Enter the IP address of the Wireless Access Gateway (WAG), the tunnel remote end. Only IPv4 address format is supported.
Tunnel Port	Enter the tunnel port when using L2TP.
Configure the following fields to monitor the tunnel.	
Ping interval	Enter the frequency at which ping requests are sent to check the status of the tunnel. The valid range is 1 – 65535 seconds; default is 1 second.
Ping number	Enter the number of ping requests sent at the configured interval. The valid range is 1 – 65535; default is 5.
Recv pkt timeout	Enter the duration for which the devices wait for the ping response; after this the ping request times out. The valid range is 1 – 65535 seconds; default is 160 seconds.
DHCP Server IP Address	Optionally, enter the DHCP server IP address.

5. To complete the addition of the tunnel profile, click **Apply**.

Device Management

The following access point configurations are allowed in FortiLAN Cloud.

- Schedule Profile
- Syslog Profile
- SNMP Profile

Scheduled Upgrades

The scheduled upgrade configuration is applied only to fully deployed FortiAPs. After a FortiAP is deployed with or without firmware upgrade during its deployment/discovery, its firmware is upgraded as per the scheduled upgrade profile. For example, if an upgrade schedule profile is configured to upgrade all FAP23JF models 5 days later then an FAP23JF model deployed today will have its firmware upgraded 5 days later. To upgrade newly deployed FortiAPs, see FortiAP Platform Profile on page 119.

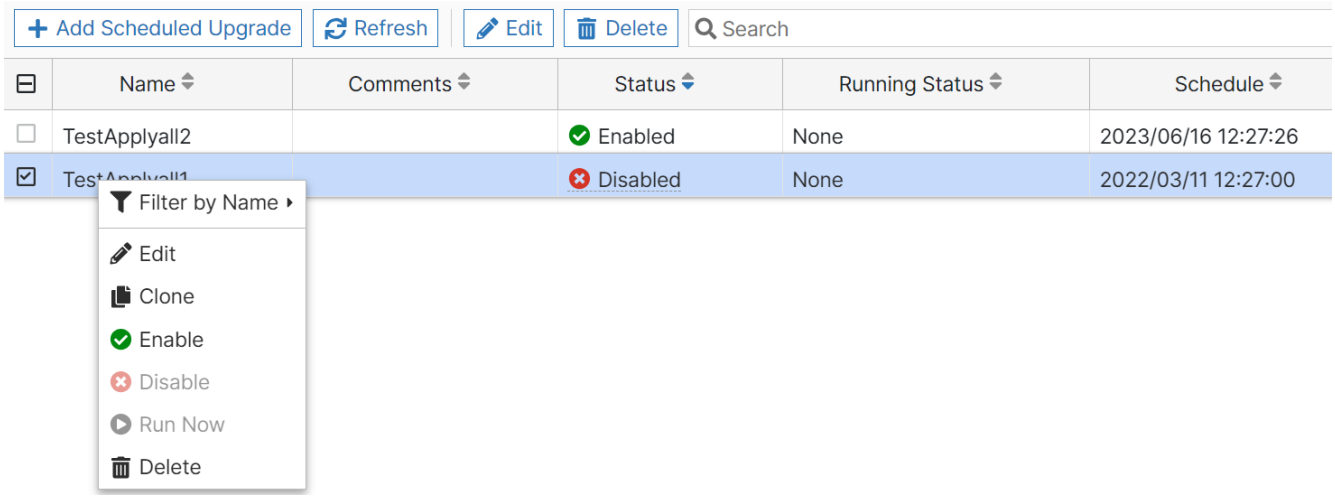
Notes:

- A maximum of 1024 scheduled upgrade profiles can be created.
- The upgrade process completion takes approximately 30 minutes if you try to upgrade multiple FortiAPs (count in 3 digits or more) simultaneously.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration > Device Management > Scheduled Upgrades**.
3. Complete the following fields.

Name	The name you want to give to the scheduled upgrade profile.
Comment	A description of the profile or any other text for this profile. This field is optional.
Force Downgrade	Forcefully downgrades deployed FortiAPs with a firmware version greater than the firmware version specified in this profile.
Device Selection	You can include *OR* exclude specific devices for upgrade based on certain criteria; model, site, tag, device, and Platform profile. When *Apply to All* is enabled, the profile is applied to all FortiAPs associated with the Platform profile.
Schedule	You can configure a one-time schedule upgrade to start immediately or specify a time slot (date/time). The upgrade schedule can also be recurring, select a start and end time with the recurring frequency.
Firmware Selection	Specify the firmware version to upgrade to for a specific FortiAP model deployed in your network. By default, the latest firmware version is selected for upgrade. **Note**: To enable UTP functionality for FAP-U43xF series models currently on software version v6.2.1 or below, upgrade to v6.2-build0401 prior to upgrading to V6.2.2 or above.

You can perform the following additional actions, select a displayed profile and right-click.



- **Clone** – You can clone an existing profile with a new name, the cloned profile is disabled (default).
- **Enable/Disable** – You can enable or disable the selected profile(s).
- **Run Now** – This is allowed only for enabled profiles that are not running. If you select multiple profiles, then at least one of them should not be running.

Syslog Profile

A Syslog server provides a centralized repository to store diagnostic information and monitoring logs from various remote systems or devices. The logs are used for network monitoring and maintenance purposes. Syslog profiles enable FortiAPs to directly send their wireless/event/security logs to an external Syslog server. The Syslog profile is associated to a Platform profile.

Notes:

- A maximum of 1024 Syslog profiles are allowed.
- Syslog profiles cannot be deleted when used by a Platform profile.

1. On the FortiLAN Cloud Home page, select the network that you want to edit.
2. In the Menu bar, navigate to **Configuration >Device Management > Syslog Profile**.
3. Complete the following fields.

Name	A unique name for the Syslog profile. The valid range is 1 -32 characters.
Description	A description for the Syslog profile.
Enable Status	Enables or disables the FortiAP to send log messages to the Syslog server
Server Host (IPv4/FQDN)	The IPv4 address or hostname (FQDN) of the Syslog server that FortiAP sends log messages to.
Server Port	The port number of Syslog server that FortiAP sends log messages to. The valid range is 1-65535 and the default is 514.
Log Level	The lowest level (severity) of log messages that FortiAP sends to the Syslog server. The default is *Information*.

SNMP Profile

FortiLAN Cloud supports SNMP access to FortiAPs such as sending queries and receiving traps. To assign an SNMP profile to a FortiAP, see FortiAP Platform Profile on page 119.

Note: A FortiAP can be associated with a platform profile linked to a configured SNMP profile, even if the SNMP admin access is disabled in the AP settings.

1. On the FortiLAN Cloud Home page, select the network to which you want to configure SNMP.
2. In the Menu bar, navigate to **Configuration >Device Management > SNMP Profile**.
3. Click **Add Profile**.
4. Enter a unique name for the SNMP profile.
5. Enter the SNMP **Engine ID**; the default is FortiLANCloud, and the administrator **Contact Info**.
6. Enter the threshold for high CPU usage (%) when the trap is sent. The valid range is 10 - 100 and the default is 80.
7. Enter the threshold for high memory usage (%) when the trap is sent. The valid range is 10- 100 and the default is 80.
8. Add SNMP v1/v2 communities and enable SNMP queries and traps as required. Enter the SNMP management stations in the **Host** field. A maximum of four, comma separated hosts can be specified along with optional netmasks.
9. Configure SNMP v3 users and manage traps and queries for these users. You can manage the security level for message authentication and encryption. The supported authentication and encryption algorithms are **MD5** and **SHA**. The valid range for authentication and encryption passwords is 8 - 32 characters. You can configure the SNMP user-notify **Hosts**; a maximum of sixteen, comma separated hosts can be specified
10. To close the dialog box, click **Save**.

User Access Control

The following user management configurations are supported in FortiLAN Cloud.

MAC Access Control and MAC Filtering

FortiLAN Cloud supports the configuration of station MAC addresses to allow those stations to access wireless networks. This is called an access control list (ACL). Only **Allow ACL** is currently supported (**Deny ACL** is not supported).

1. On the FortiLAN Cloud Home page, select the network to which you want to import MAC addresses.
2. In the Menu bar, navigate to **Configuration > User Access Control > MAC Access Control**.
3. Click **Import**.
4. Add the MAC addresses. Separate each address with a comma. An import can include a maximum of 10,000 MAC addresses (records).
5. Review the summary. If you want to make changes, click **Back**.
6. To import the MAC addresses, click **Submit**.
   A dialog box displays a status message. Here is an example: Import 2 records successfully.
7. To close the dialog box, click **OK**.
8. When adding an SSID to an network, make sure to select MAC Access Control.

Exporting ACL List

Use this procedure to export all MAC addresses as an access control list (ACL) text file.

Complete the importing MAC addresses procedure in MAC Access Control and MAC Filtering.

1. On the FortiLAN Cloud Home page, select the network that has the MAC addresses to export.
2. In the Menu bar, navigate to **Configuration > User Access Control > MAC Access Control**.
3. Click **Export All**.
4. Complete the instructions on the screen to open or save the text file.

FortiLAN Cloud User/Group

Perform this procedure to use a FortiLAN Cloud group and users as the RADIUS setting when you configure an SSID with WPA-2 Enterprise authentication. As part of user group configuration, you can assign VLAN IDs, especially useful for when assigning users to different networks without requiring multiple SSIDs.

Note: Enterprise (802.1x) wireless networks (versions prior to FortiLAN Cloud 21.2) that use the FortiAP Cloud User/Group feature and have client devices (such as Android 11) with the domain name fortiapcloud.com during their wireless connection must be re-configured in FortiLAN Cloud; the new domain name is *forticloud.com* or *fortilan.forticloud.com*. This is required for the wireless client devices to connect.

1. On the FortiLAN Cloud Home page, select the network to which you want to add the group.
2. In the Menu bar, navigate to **Configuration > User Access Control > FortiLAN Cloud User/Group**.
3. Click **Group**.
4. Click **Add Group**.

5. Complete the following fields:

Group ID	Type the ID for this group, up to a maximum of 16 characters in length.
Description	Type a description for this group.
VLAN ID	The VLAN ID for this group.

6. Click **Apply**.

A new group is added. To download data in a *.csv* format for all groups, click  .

1. Click **User**.
2. Click **Add user**.
3. Complete the following fields:

User ID	Type the ID for this user, up to a maximum of 64 characters in length.
Full name	Type the full name for this user.
Password	Type the password associated with this user.
VLAN ID	The VLAN ID for this group.
Email address **Re-type Email**	Type the email address for this user.
Groups	Select the group you want this user to be added to.

4. Click **Apply**.

A new user is added. To download data in a *.csv* format for all users, click  .

Adding a FortiLAN Cloud Guest

Use this procedure to add a single guest or multiple guests in FortiLAN Cloud.

Prerequisites

Add a guests SSID. For details, see procedure.

1. On the FortiLAN Cloud Home page, select the networks to which you want to add the guest.
2. In the Menu bar, navigate to **Configuration > User Access Control > FortiLAN Cloud User/Group**.
3. Click **Guest**.
4. Click **Add Guest**.
5. If you want to add multiple guests, click the **Multiple Guest** checkbox.
6. Complete the fields.
7. To complete the addition of guests, click **Apply**.

A new guest user is added. To download data in a *.csv* format for all guests, click  . To import data for guest users, click  .

Adding a FortiLAN Cloud Guest Manager

Use this procedure to add a guest manager in FortiLAN Cloud.

1. On the FortiLAN Cloud Home page, select the network to which you want to add the guest manager.
2. In the Menu bar, navigate to **Configuration > User Access Control > FortiLAN Cloud User/Group**.
3. Click **Guest Manager**.
4. Click **Add Guest Manager**.

Make sure to type an email address that the network configuration is not already using.

5. Complete the following fields.

User Name	Type the name for this user.
Email address **Re-type Email**	Type the email address for this user.
Enable 2-Factor Authentication	Select to enable 2-factor authentication for guest manager.

To add the guest manager, click **Submit**.

A new guest user is added. To download data in a *.csv* format for all guest managers, click  .

RADIUS Server

Perform this procedure to add a RADIUS server to a network and then use this server to authenticate wireless clients.

1. On the FortiLAN Cloud Home page, select the network to which you want to add the RADIUS server.
2. In the Menu bar, navigate to **Configuration > User Access Control > My RADIUS server**.
3. Click **Add My RADIUS Server**.

4. Complete the following fields:

Name	Type a name for My RADIUS Server.
NAS IP	Type the IP address of the network access server (NAS). This field is optional.
Primary server name/IP	Type the server name or IP address of the primary RADIUS server.
Primary server secret	Type the secret key of the primary RADIUS server.
Secondary server name/IP	Type the server name or IP address of the secondary RADIUS server. This field is optional.
Secondary server secret	Type the secret key of the secondary RADIUS server. This field is optional.
Server port	If the RADIUS server is not using the default port, then type the server port. The default is 1812.
Auth Protocol	Select the authentication protocol only to authenticate wireless clients that connect to captive portal enabled networks. If you select **Auto**, then the protocols are tried in this order. • PEAP • MSCHAPv2 • MSCHAPv1 • CHAP • PAP
TLS Version	Select the TLS version for the PEAP authentication protocol.
CoA enable	Enable Change of Authorization (CoA) to allow the RADIUS server to adjust active client sessions. The AP disconnects user sessions when it receives a Disconnect-Request from the RADIUS server.
Account all servers	Enable this option to use both primary and secondary RADIUS servers for authentication.
Case sensitive username	Enable case sensitive RADIUS user name.

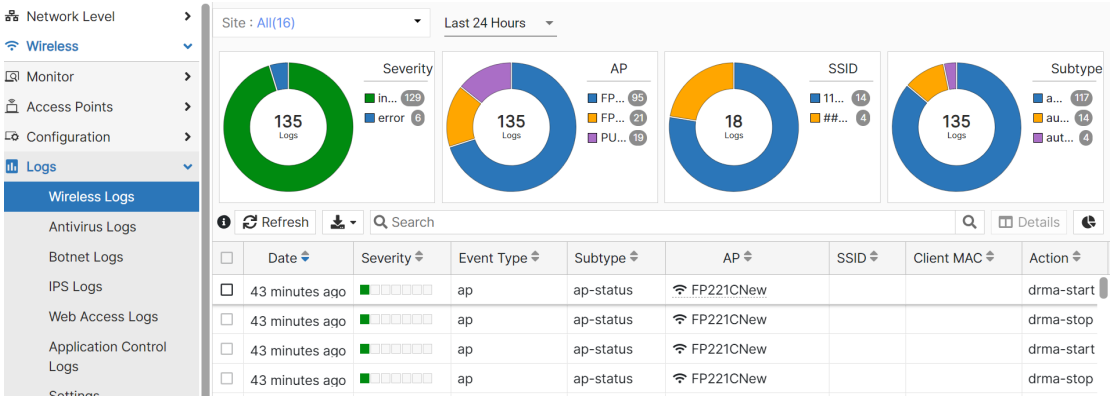
5. To complete the addition of the RADIUS server, click **Apply**.

Logs

This section includes the following FortiLAN Cloud log procedures:

Displaying logs

You can view logs related to FortiLAN Cloud features. The logs can be filtered using the AP sites created during deployment based on the AP location.



1. In the Menu bar, click **Logs**.
2. In the Navigation pane, select one of the following categories:
   - Wireless Logs
   - AntiVirus Logs
   - Botnet Logs
   - IPS Logs
   - Web Access Logs
   - Application Control Logs

Exporting logs

Use this procedure to export logs to a comma-separated values (CSV) file.

Procedure steps

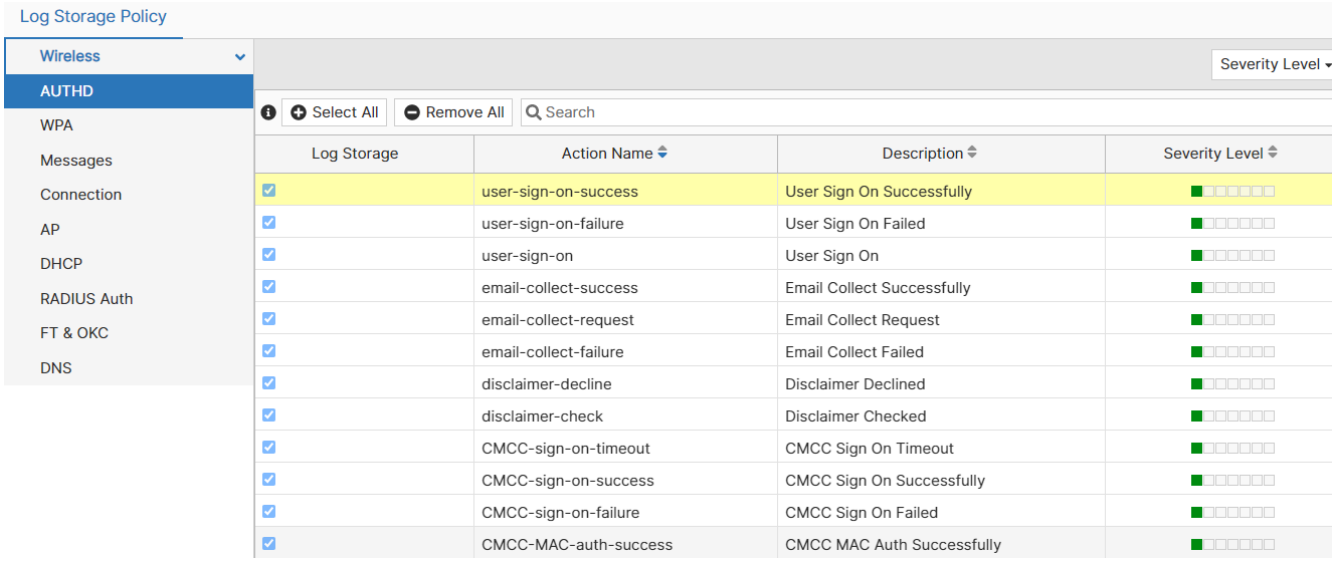
1. In the Menu bar, click **Logs**.
2. In the Navigation page, select one of the following categories:
   - Wireless Logs
   - AntiVirus Logs
   - Botnet Logs
   - IPS Logs
   - Web Access Logs
   - Application Control Logs
3. Click **Export**.
   The Export to CSV dialog opens.
4. In the Top drop-down list, select how many logs you want to export.
5. Click **Apply**.
   The Opening <AP_network_name_and_date>.zip dialog opens.
6. Select to open or save the file.
7. Click **OK**.

Wireless Log Categorization and Storage Control

FortiLAN Cloud generated wireless logs, instrumental in troubleshooting networks, are stored in the database for 1 year (subscription based). Given that wireless logs can be voluminous depending on the network size, you can now segregate them into multiple different categories and manage the categories to store and display, as per requirement. For example, frame-level logs such as probe logs, authentication logs, and association logs are only required during a debug session and are not always needed. This feature enables you to swiftly filter-down to specific logs of interest.

The network specific log storage policy (settings) configuration overrides the default log storage policy. Navigate to **Wireless > Logs > Settings** to view and manage the log record storage. The log types are displayed on the left panel, select the relevant log type and view the current log storage policy. FortiLAN Cloud assigns each log a severity level.

In the **Log Storage** column, enable/disable the storing of logs and click **Apply**. To reset the log storage policy to the default setting, click **Reset to Defaults** and to reload the saved log storage configuration, click **Reload Saved Config**.


Log Storage Policy
Wireless
AUTHD
WPA
Messages
Connection
AP
DHCP
RADIUS Auth
FT & OKC
DNS
Severity Level
Select All
Remove All
Search
Log Storage
Action Name
Description
Severity Level
user-sign-on-success
User Sign On Successfully
user-sign-on-failure
User Sign On Failed
user-sign-on
User Sign On
email-collect-success
Email Collect Successfully
email-collect-request
Email Collect Request
email-collect-failure
Email Collect Failed
disclaimer-decline
Disclaimer Declined
disclaimer-check
Disclaimer Checked
CMCC-sign-on-timeout
CMCC Sign On Timeout
CMCC-sign-on-success
CMCC Sign On Successfully
CMCC-sign-on-failure
CMCC Sign On Failed
CMCC-MAC-auth-success
CMCC MAC Auth Successfully

Reports

This section includes the following FortiLAN Cloud report procedures:

Customizing an AP network summary report

Use this procedure to customize an AP network summary report, and its various sections and sub-sections.

Procedure steps

1. In the Menu bar, click **Reports**.
2. In the Navigation pane, click **Summary Report**.

If you want to	Then
Change the summary report settings	1. Click **Settings**.  2. You can add a logo, change the language, and enable or disable the generation of an empty report. 3. To save changes, click **Submit**.
Customize a section	1. Go to the section that you want to customize and click  2. Select one of the following action: **a.** Add Chart **b.** New Section Title **c.** New Report Block **d.** Reset Report 3. Follow the onscreen instructions.
Customize a sub-section	1. Click **Edit**.  2. You can change the sub-section title and add filters. 3. To save and apply the changes, click **Run**.

Scheduling an AP network summary report

Use this procedure to schedule when you want to receive an AP network summary report by email.

Procedure steps

1. In the Menu bar, click **Reports**.
2. In the Navigation pane, click **Summary Report**.
3. Click **Schedule**.
4. Select the frequency (**Daily**, **Weekly**, or **Monthly**).
5. To receive summary reports by email, select **Email To** and type an email address.
6. To access a summary report, go to the Navigation pane and click **History Reports**.

Managing AP network history reports

Use this procedure to view, download, send by email, and delete AP network history reports.

1. In the Menu bar, click **Reports**.
2. In the Navigation pane, click **History Reports**.
3. Hold the pointer over the report that you want to access.

If you want to	Click
View the report	
Download the report	
Send the report by email	
Delete the report	

Generating a PCI compliance report for an AP network

Use this procedure to answer questions about AP network settings for compliance with the Payment Card Industry Data Security Standard (PCI DSS) 3.0.

Procedure steps

1. In the Menu bar, click **Reports**.
2. In the Navigation pane, click **PCI Report**.
3. Review and answer questions.
4. To generate a PCI report, click **Run Report**.
   The generated PCI compliance report opens.
5. To save the report, scroll to the right and click **Save Report**.
6. To return to the list of questions, scroll to the right and click **Back to Questionnaire**.
7. To access previously saved reports, click **Saved Reports**.

Configuring and Managing FortiSwitches

.You can configure, monitor, and manage FortiSwitches using the FortiLAN Cloud management solution.

Menu	Description
Dashboard	Displays a snapshot of FortiSwitch activity that occurred in the last 24 hours.
Topology	Displays the FortiSwitch topology.
Switch	Provides sub-menus to configure and manage FortiSwitches, switch tags and so on.
Configure	Configuration page to configure switches, ports, interfaces, VLANs, and remote authentication servers and to create zero-touch configurations, scheduled upgrades, packet capture profiles, VLAN templates, and user groups. and change your notification and backup settings.
Monitor	Monitor page to check modules, MAC addresses, switch and port statistics; FortiSwitch units using PoE, LLDP, or 802.1x authentication; STP instances; DHCP-snooping and IGMP-snooping databases; logs; and the status of zero-touch configurations, scheduled upgrades, and packet captures.
My Account	My Account page to review your account, deploy FortiSwitch units to FortiLAN Cloud.

Getting Started

Some FortiSwitch units might have a sticker on them with an outdated procedure. Use the procedures in the *FortiLAN Cloud Administration Guide* instead of procedures on the sticker.

NOTE: The following are the requirements to use all of the features of FortiLAN Cloud:

- Register your FortiSwitch units with Fortinet Support (https://support.fortinet.com).
- Check that your FortiSwitch units are running FortiSwitchOS 6.0.0 or later.
- Check that your FortiSwitch units are connected to the Internet.
- Subscribe to FortiCare (https://www.fortinet.com/support-and-training/support-services/forticare-support.html).
- Purchase a Management license for each FortiSwitch unit through authorized Fortinet resellers and distributors. For information on the FortiLAN Cloud license offering, see Licensing on page 15.
  a. After you purchase a FortiSwitch Management license, you need to register it in your FortiCare account.
  b. FortiLAN Cloud will automatically import the license from your FortiCare account during its regular license check. Depending on when the license was registered, there might be a delay before the license is available in FortiLAN Cloud.
- Set your FortiSwitch units to the standalone mode.
- Check that the system time on your FortiSwitch units is accurate. To set the time on your FortiSwitch unit, see the *FortiSwitchOS Administration Guide—Standalone Mode*.

Supported models

FortiLAN Cloud supports all FortiSwitch units running FortiSwitchOS Release 6.0.0 or later

To get started using FortiLAN Cloud, follow these procedures:

1. Enabling and disabling cloud management
2. Deploying FortiSwitch device to a network

Checking your Cloud configuration

To check your Cloud configuration, use the following commands:

```
S524DF4K15000024 # config system flan-cloud
S524DF4K15000024 (flan-cloud) # get

interval            : 45
name                : fortiswitch-dispatch.forticloud.com
port                : 443
status              : enable
```

Option	Description
interval	The time in seconds allowed for domain name system (DNS) resolution. The default is 15 seconds. The range of values is 3-300 seconds.
name	The domain name for FortiLAN Cloud. By default, this field is set to `fortiswitch-dispatch.forticloud.com`.
port	Port number used to connect to FortiLAN Cloud. The default is port 443.
status	Whether access to FortiLAN Cloud is enabled or disabled. By default, the status is set to `enable`.

To check your connections to FortiLAN Cloud, use the `get system flan-cloud-mgr connection-info` command.

The State-Machine field is set to FSMGR_STATE_READY when your FortiSwitch unit is being managed by FortiLAN Cloud. The SSL tunnel is the secure communication channel between your FortiSwitch unit and FortiLAN Cloud. FortiLAN Cloud uses the Socket Secure protocol (SOCKS) to communicate with your FortiSwitch units.

For example:

```
S524DF4K15000024 # get system flan-cloud-mgr connection-info

User Account-ID:    : 012345
Dispatch Service    : IP= xx.xx.xx.xx
SSL verify Code     : ok
Access Service      : IP= xx.xx.xx.xx, Port= 443, Connected on: 2018-11-28 10:59:32
Bootstrap Service   : hostname= xxxxxxxxxx, Port= 8000

Remote Assistance   : Disabled.
State-Machine       : State= FSMGR_STATE_READY, Event= EV_READY_HBEAT_GOOD

SSL Local End-Point : Interface: mgmt, IP: xx.xx.xx.xx
SSL Tunnel Uptime   : Days: 0  Hours: 2 Mins: 22 [Connected @2018-11-28 10:59:32]
SSL Tunnel stats    : restart-count= 4, Reason= Configuration Change
```

```
Stats:
========
Switch  Keep Alive  Tx/Reply := 45 / 45
Manager Keep Alive  Rx/Error := 45 / 0

Socks   Req Rx/Last Stream-ID := 224 / 14
Reset   Req Rx/last Stream-ID := 8 / 12
Goaway  Req Rx  := 0
Unknown Req Rx  := 0

Syslog FD/Tx/Err := 8 / 3 / 0

Used SOCKS stream-id:
=======================
SID             SockFd          State           Description
___             ______          _____           _______________
18              10              DATA            REST REQ
5               0               DATA            SYSLOG DATA
```

Enabling and disabling cloud management

To allow your FortiSwitch unit to be managed by FortiLAN Cloud, use the following commands:

```
config system flan-cloud
   set status enable
end
```

If you want to remove a FortiSwitch unit from FortiLAN Cloud, use the following commands:

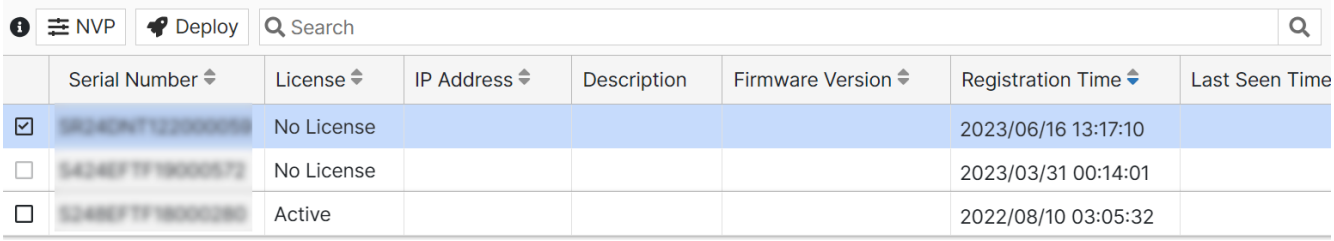
```
config system flan-cloud
   set status disable
```

Deploying FortiSwitch device to a network

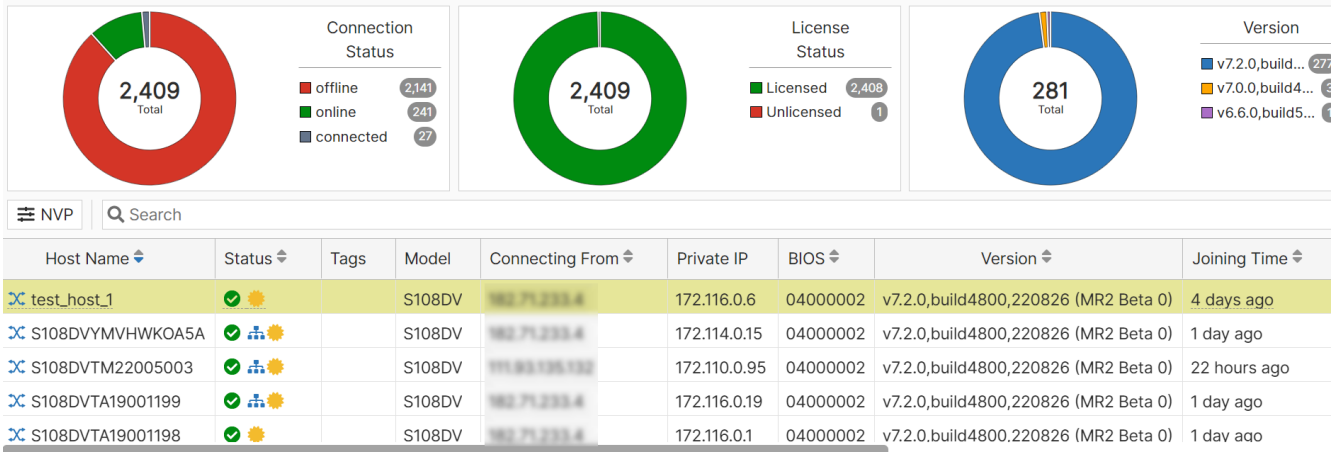
You can deploy any of the FortiSwitch units listed in the switch inventory to FortiLAN Cloud.

1. Login into your FortiCloud account and register the switch serial number.
   Registered switches are automatically added to FortiLAN/FortiSwitch Cloud.
2. To deploy the FortiSwitch, go to the *Inventory* tab on the main page of the FortiLAN Cloud portal **OR** go to *My Account* > *Switch Inventory* and select the switches to deploy.
   - You can deploy the FortiSwitch to FortiLAN Cloud or to an external AP Controller. Select **Deploy to FortiLAN Cloud** and click **Deploy**. Select the network to deploy the FortiSwitch to and click **Deploy**.
   - You can also deploy the FortiSwitch through FortiZTP. In the **FortiZTP Devices** tab, select the FortiSwitch and click **Deploy to Network**. Select the network to deploy the FortiSwitch to and click **Deploy**.

In the *Switch Inventory*, select the switch/switches and click *Deploy*.



After you deploy a FortiSwitch unit to FortiLAN Cloud, it is removed from the *Switch Inventory* pane and listed in the *Switches* pane (*Switches* > *Deployed Switches*).



To undeploy a FortiSwitch device, see Undeploying a FortiSwitch device on page 163.

Moving a FortiSwitch device between networks/accounts

You can move a FortiSwitch between different networks associated with a user account.

1. Open the network and undeploy the FortiSwitch. See Undeploying a FortiSwitch device on page 163.
2. Open the network to add the FortiSwitch to, navigate to *Switch* > *My Account* > *Switch Inventory*.
3. Select the FortiSwitch and select *Add* to deploy it.

You can move a FortiSwitch between different user accounts.

1. Login into the account and undeploy the FortiSwitch device. See Undeploying a FortiSwitch device on page 163.
2. Remove the FortiSwitch from the FortiCare account (*Services* > *Asset Management*).
3. Register the FortiSwitch in the FortiCare account that you want to move it to and login into the FortiLAN Cloud. See Deploying FortiSwitch device to a network on page 155.

Dashboard

Select *Dashboard* to see a snapshot of FortiSwitch activity that occurred in the last 24 hours.

Use the *Quick Links* drop-down list to view the switch topology, deploy switches, add zero-touch configurations, or add scheduled upgrade configurations.

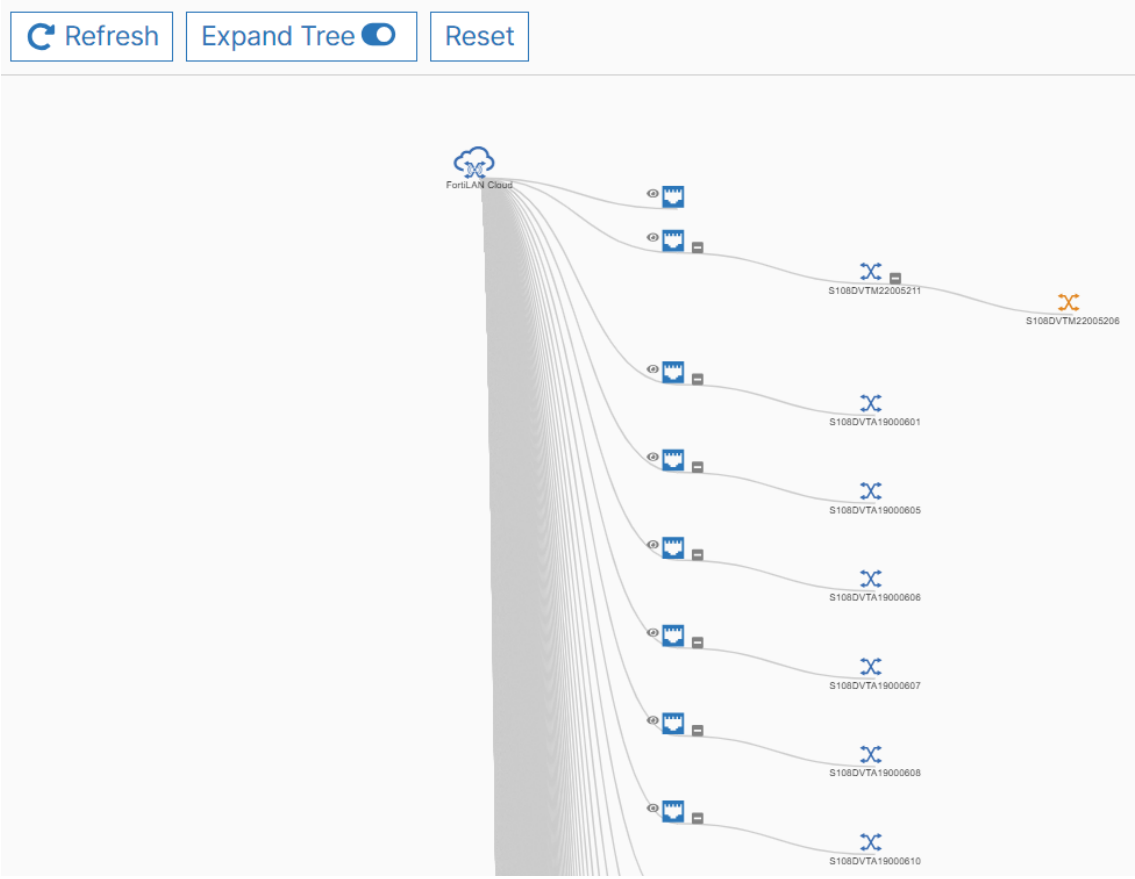
The Dashboard page provides the following information.

- *Online Switches*—The number and percentage of managed devices that are online
- *PoE Port Utilized*—The number and percentage of Power over Ethernet (PoE) ports that are being used
- *PoE Power Delivered*—The number of Watts and the percentage of PoE delivered.
- *Critical Events Last 24 Hours*—The number of critical events in the last 24 hours
- *Top PoE Power Utilization*—The five FortiSwitch units with the highest PoE usage
- *PoE Power over Threshold*—The five FortiSwitch units that have a current power budget that exceeds a specified percentage of the total power budget.
- *Top VLANs Count*—The five FortiSwitch units with the most VLANs.
- *Pluggable Modules*—The number and types of modules inserted in FortiSwitch units, as well as any warnings or alerts
- *DHCP Snooping*—The number of DHCP-snooping-enabled VLANs, the number of dynamically learned DHCP snooping entries in the client and server databases, and the number of DHCP-snooping entries in the limit database.
- *IGMP Snooping*—The number of switches and VLANs enabled for IGMP snooping and the number of dynamic IGMP-snooping groups.
- *OS Versions*—Which FortiSwitchOS versions are being used by managed FortiSwitch units Auto Backup Status (Last 24 hours)—The number of scheduled configuration backups that failed and succeeded in the last 24 hours and which FortiSwitch units were not backed up.
- *Top Switch Active Clients* - The FortiSwitches with the highest number of active clients in the last one hour.
- *Top Switch CPU Utilization* - The FortiSwitches with the highest CPU utilization in the last one hour.
- *Top Switch Memory Utilization* - The FortiSwitches with the highest memory utilization in the last one hour.
- *Top Switch PCB Temperature* - The FortiSwitches with the highest PCB temperature in the last one hour.
- *Top Rx/Tx Utilization* - The FortiSwitches with the highest percentage of Rx/Tx utilization in the last one hour.
- *Top Losses* - The FortiSwitches with the highest Rx/Tx drops and errors in the last one hour.
- *Switches & Licenses* - The FortSwitch license details with the status, used, available, grace period.
- *Active Configurations* - The active FortiSwitch configurations with their status.
- *802.1X VLANs and Session States* - The VLANs are listed along with the session state.

Topology

Select *Topology* to view the switch topology. The Topology page shows an overview of FortiSwitch islands connected to FortiLAN Cloud.

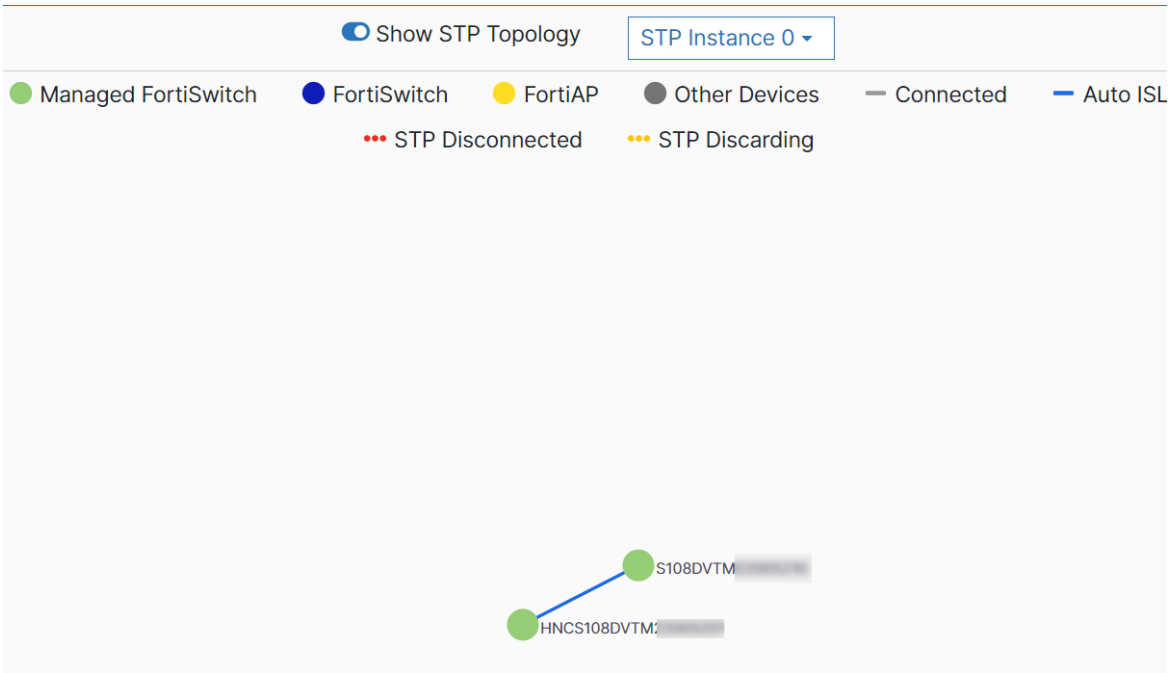
A FortiSwitch island contains a cluster of connected FortiSwitch units, as well as devices that are not managed by FortiLAN Cloud. Depending on whether FortiLAN Cloud can obtain valid root information from Spanning Tree Protocol (STP), each FortiSwitch island is displayed with either an LLDP-based graph or an LLDP-and-STP-based graph with tiers. The host name is displayed for FortiSwitch units; MAC addresses are displayed for non-FortiSwitch devices.



To update the topology display, select *Refresh*. To display networks with inter-switch links (ISLs), select *Expand Tree*. To find a specific FortiSwitch unit tag, click Filter By Tags and select the listed tag.

Select the **Click to View Detailed Topology** icon to view the detailed topology of the FortiSwitch unit.

You can enable **Show STP Topology** to view the STP topology.



Switches

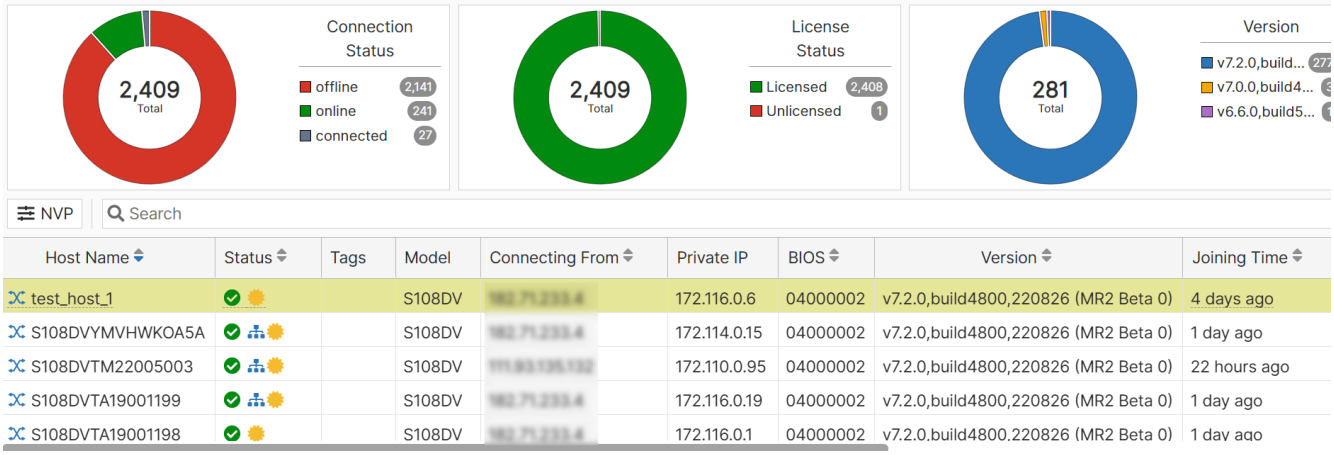
Select *Switches* to manage the FortiSwitch configuration and to view the switch topology. Use the left pane for navigation. You can select the following options from the left pane:

- Switches
- Defining Switch Name-Value Pairs

Switches

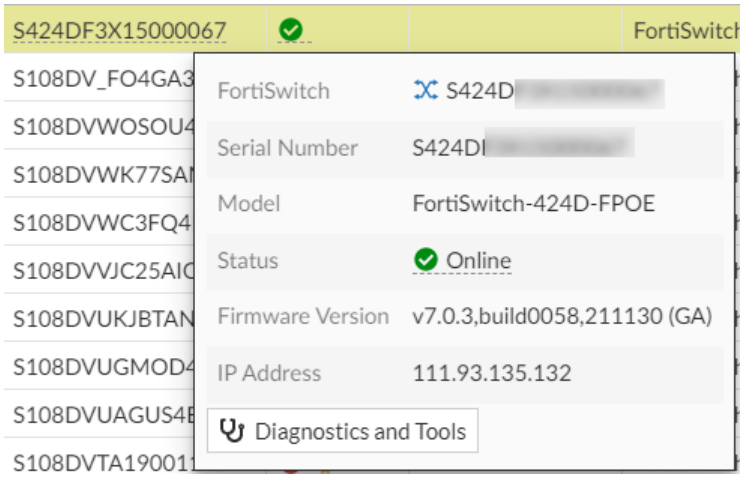
The **Switches** pane lists the FortiSwitch units managed by FortiLAN Cloud and gives the serial number, host name, model, IP address, firmware version, connection time, and status of each FortiSwitch unit.

Note: Requisite warning message is displayed in case of old BIOS version, upgrade BIOS as required. Firmware upgrade in case of BIOS compatibility issue is not allowed.



To find a specific FortiSwitch unit, enter part or all of the serial number in the Search field.

Hovering over a host name FortiSwitch unit details, click on **Diagnostics and Tools** for FortiSwitch management options.



A lightning bolt indicates that the current power budget of the FortiSwitch unit exceeds a specified percentage of the total power budget.

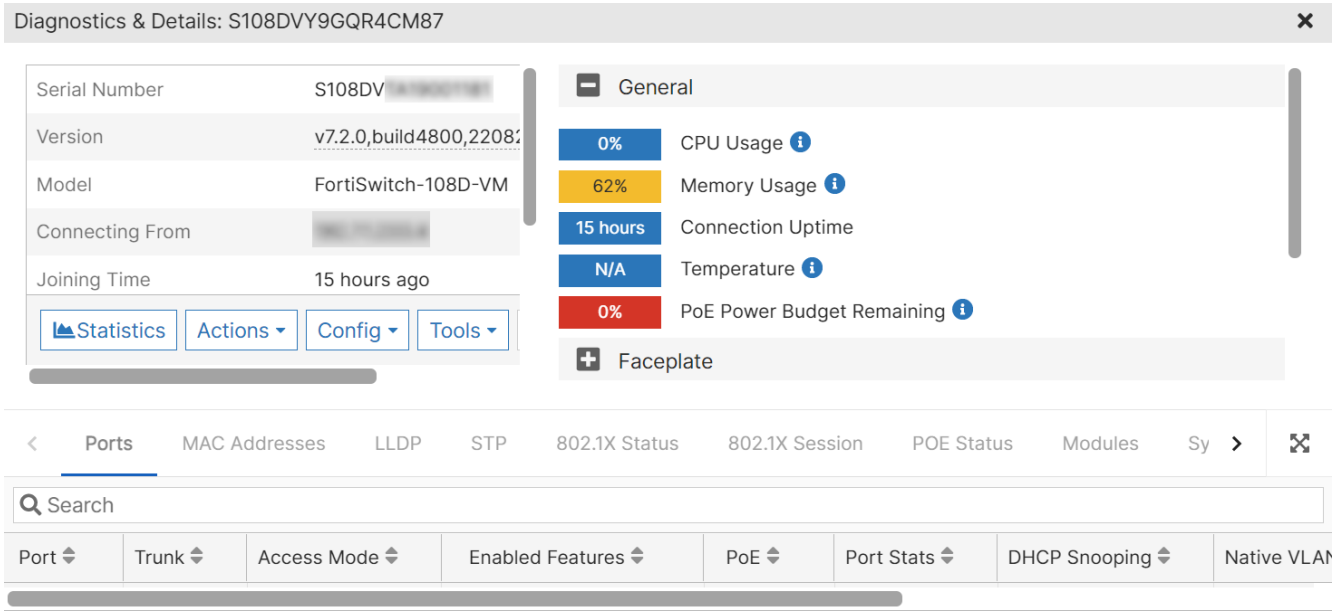
You can perform the following tasks from the **Diagnostics and Tools** panel.

- Viewing Switch Details
- Displaying switch statistics
- Actions
- Configuration

- Tools
- Using the FortiSwitch CLI
- Using the FortiSwitch GUI

Viewing Switch Details

To view the FortiSwitch statistics and diagnostics in detail, click on the serial number. The **Status** including the FortiSwitch face plate, hardware summary, general status and statistics, and configuration details.



Displaying switch statistics

The CPU Utilization/Memory Utilization, PCB Temperature, TX bps/RX bps, and Active Client graphs make it easy to see data from the last 24 hours for a FortiSwitch unit.

NOTE: If the data is not available, the graph is not displayed.

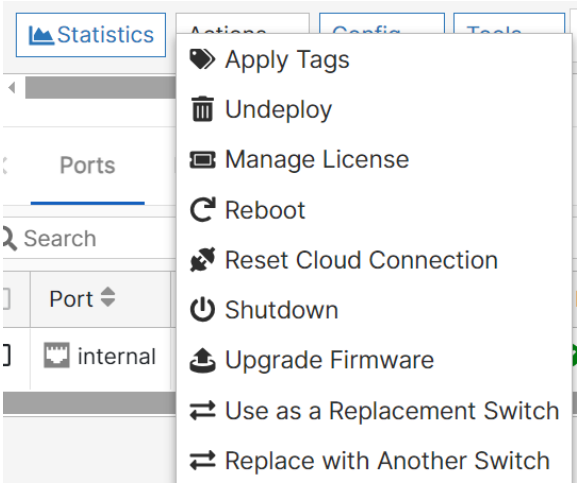
To display switch statistics:

1. Select **Statistics** in the **Diagnostics & Details** panel.

2. Select *Period* to choose the start day and time and end day and time for the graphs.
3. Select *Lines Only* to display just the connected data points in the graphs.
4. Hover above a point in one of the graphs to see the details for that time.

Actions

The **Actions** tab enables you to perform the tasks listed in the **Actions** column in this page and described subsequently in this chapter.

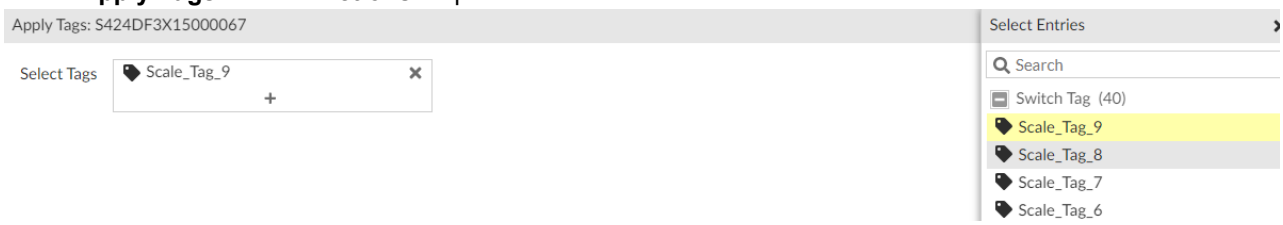


Applying tags to a FortiSwitch unit

Tags allow you to group FortiSwitch units by model, location, department, owner, and so on. You can add more than one tag to a FortiSwitch unit.

To apply a tag to a FortiSwitch unit:

1. Select **Apply Tags** from the **Actions** drop-down menu.

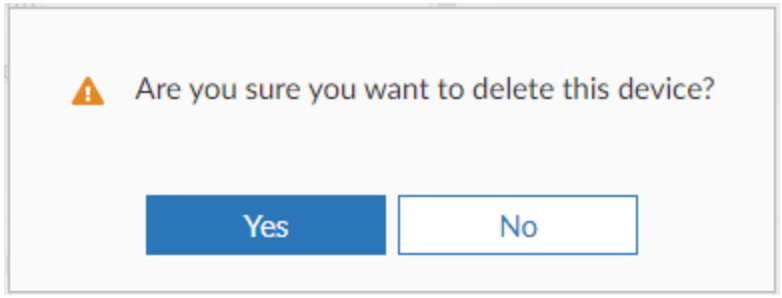


2. Select to search from the list of existing tags. Select which tags that you want to apply.
3. Select *Submit*.

Undeploying a FortiSwitch device

To remove a FortiSwitch unit from FortiLAN Cloud:

Select **Undeploy** from the **Actions** drop-down menu.



1.
2. Select *Yes* to remove the FortiSwitch unit from FortiLAN Cloud.
   The FortiSwitch unit is removed from the Switches pane and is listed in the Switch Inventory pane (*My Account* > *Switch Inventory*). It can be added again to the FortiLAN Cloud by going to *My Account* > *Switch Inventory* and selecting *Add*.

Reboot/Shutdown

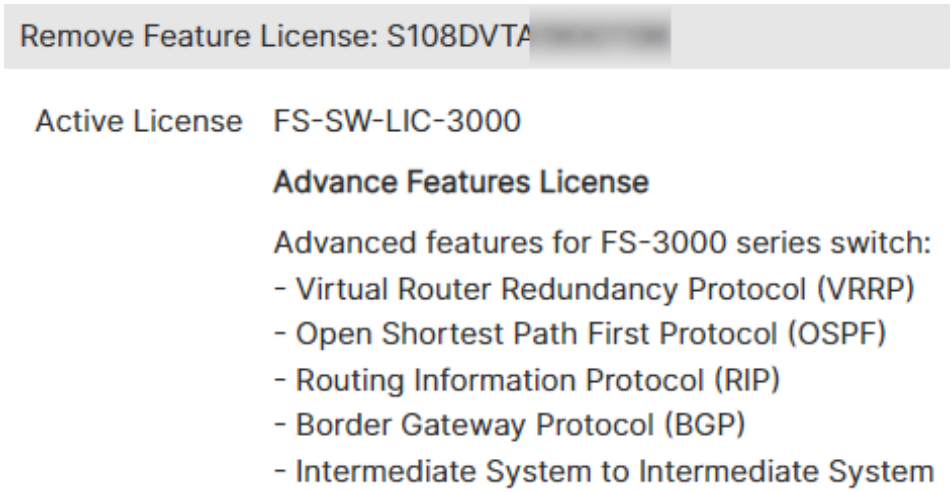
You can reboot or shutdown the FortiSwitch from the GUI. A shutdown requires a physical reboot of the FortiSwitch to connect it to FortiLAN Cloud.

Reset Cloud Connection

The **Reset Cloud Connection** action is now available for FortiSwitches. This feature facilitates recovery of devices that are not able to maintain a coherent connection with FortiLAN Cloud. When used, the FortiSwitch disconnects and re-joins the FortiLAN Cloud.

Manage License

You can now add and remove the FortiSwitch feature license from the FortiLAN Cloud GUI.

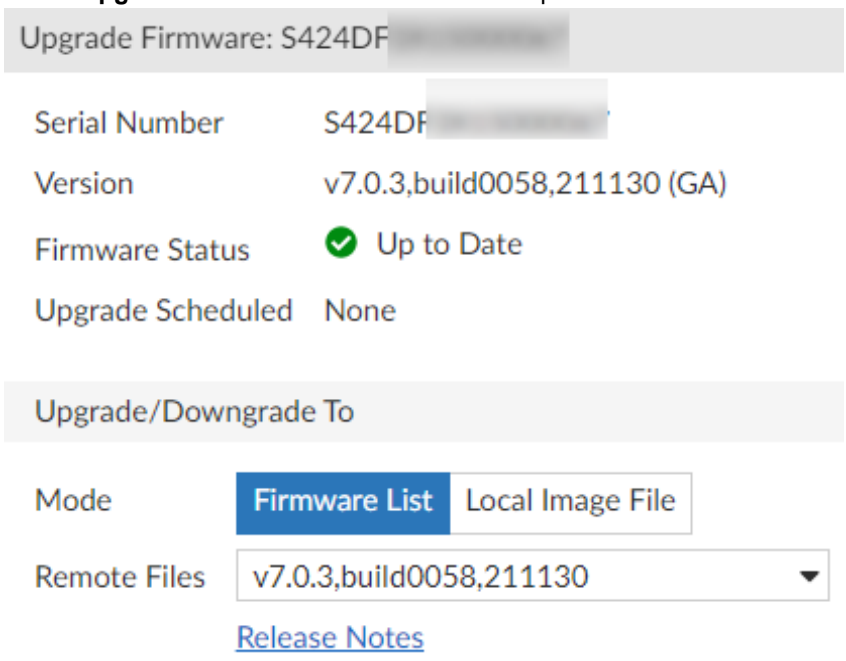


Note: The feature license management option is supported only on firmware version 7.0 and above.

Upgrading the firmware for a FortiSwitch unit

To upgrade the firmware for a FortiSwitch unit:

1. Select **Upgrade Firmware** from the **Actions** drop-down menu.



2. Select *Firmware List* or *Local Image File*.
3. Select the firmware image for the upgrade.
   Click the help link, *Release Notes*, to learn about the available versions.
4. Select *Submit* to upgrade.

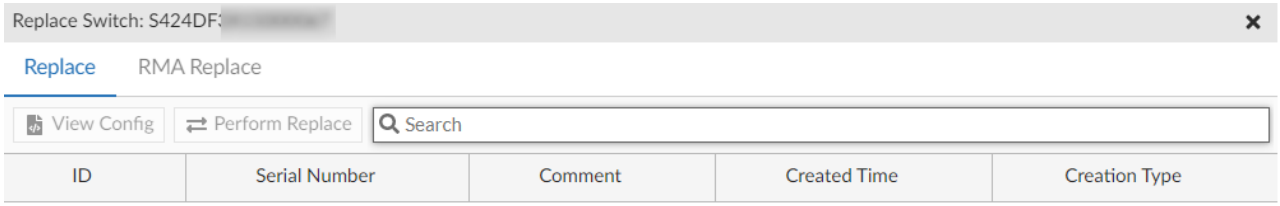
Replacing a Switch

You can replace a switch in your network with another switch irrespective of the model and firmware versions. The replacement operation is required either due to switch failure (RMA) or any other reason (non-RMA). However, the following pre-requistes are to be fulfilled prior to the replacement operation.

- Backup the source (original) FortiSwitch configuration prior to the replacement operation, see Configuration Backup/Restore on page 193 or Network on page 223.
- The new (replacement) FortiSwitch is online.

FortiCare synchronizes the inventory data with FortiLAN Cloud periodically and the switch inventory page is updated with the new switch details. Navigate to My **Account > Switch Inventory** and deploy the new switch, see Deploying FortiSwitch device to a network on page 155.

1. Select **Use as a Replacement Switch** from the **Actions** drop-down menu of the online FortiSwitch unit that you want to replace, select **RMA Replace** or **Replace** (non-RMA).



2. Select the serial number and click **Perform Replace**.
3. Click **View Config** to view the configuration details.

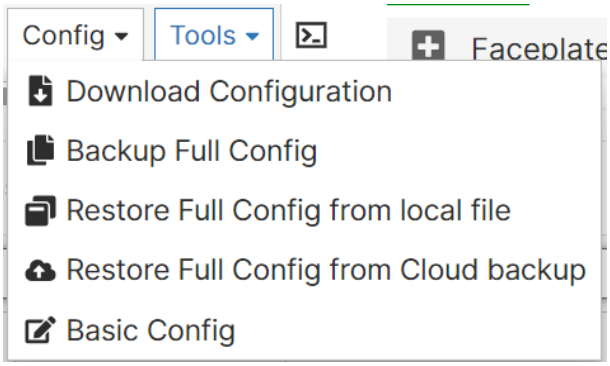
Note: In case of a FortiSwitch replacement, you are required to obtain a new license.

FortiSwitch Swap

Use the **Replace with Another Switch** option in the **Actions** menu to create a replacement entry. However, if the FortiSwitch is present in any entry of the **Device Replacements** page as a replacement FortiSwitch or a FortiSwitch to be replaced, then you cannot create an entry here. See Device Replacements.

Configuration

You can perform various operations to manage the FortiSwitch configurations.



Downloading the FortiSwitch configuration to your computer

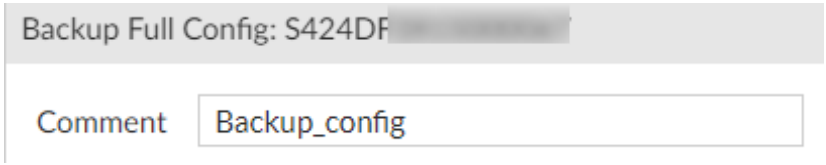
To download the FortiSwitch configuration:

Select **Download Configuration** from the **Config** drop-down menu. The configuration is saved as a `.txt` file.

Backing up the FortiSwitch configuration to FortiLAN Cloud

To backup the configuration of a FortiSwitch unit to FortiLAN Cloud:

1. Select **Backup Full Config** from the **Config** drop-down menu of the FortiSwitch unit that you want to save the configuration of.

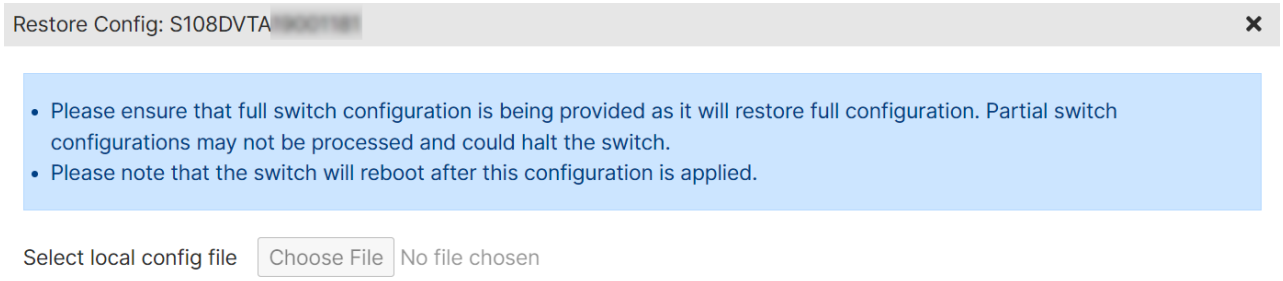


2. Enter a description of the configuration file.
3. Select *Submit*.
   Configuration files are listed in *Configuration* > *Config Backup/Restore*.

Applying a configuration file to a FortiSwitch unit

To apply a configuration file that has been saved to your computer to a FortiSwitch unit:

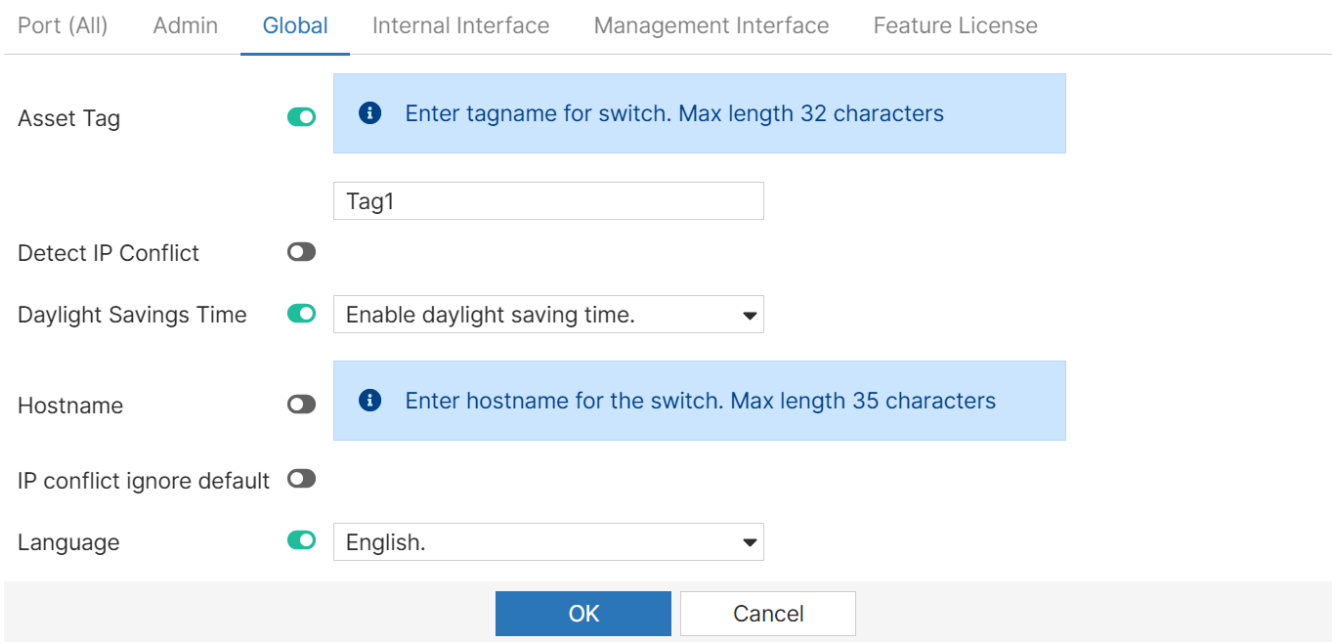
1. Select **Restore Full Config from local file** from the **Config** drop-down menu of the FortiSwitch unit that needs the configuration restored.



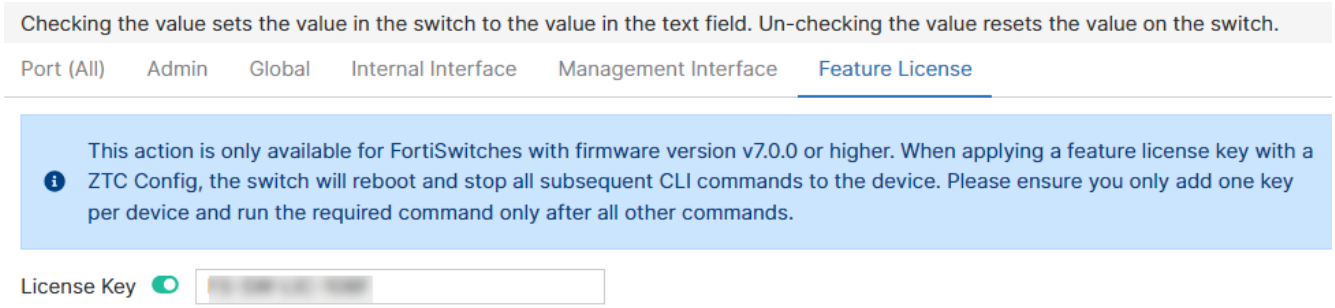
2. Select *Choose Files*.
3. Select the configuration file to apply.
4. Select *Open*.
5. Click **Submit** to apply the configuration.

Basic Configuration

You can configure basic parameters for your FortiSwitch unit such as global and administrative settings, ports, and internal and management interfaces. In each of the tabs, select the parameter and enter a value, when you un-select an option, the default value is applied. Select **Basic Config**.



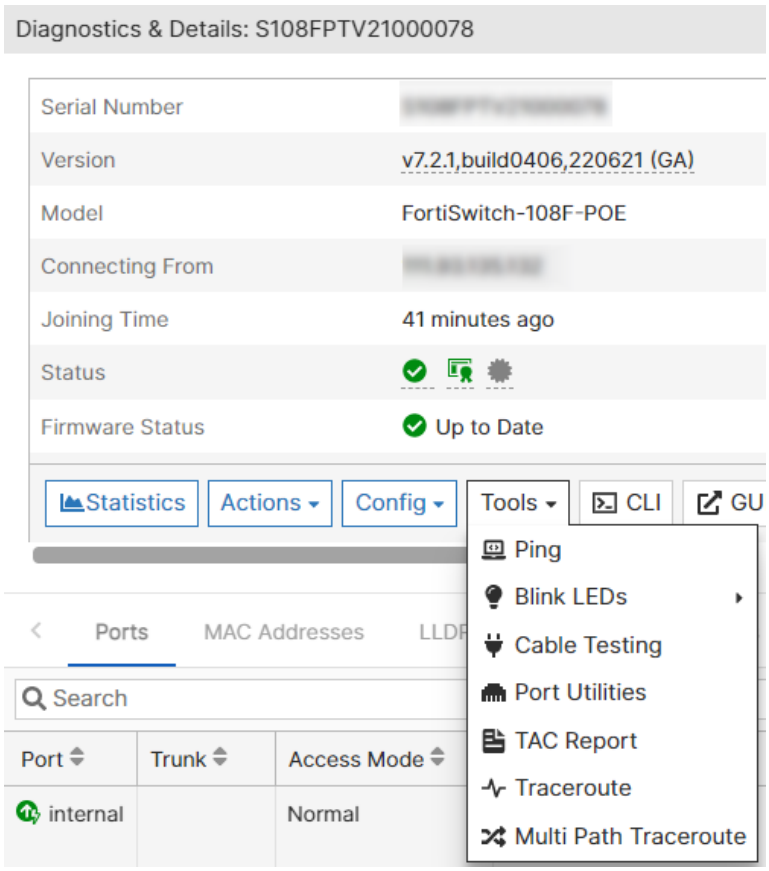
You can now add and remove the FortiSwitch feature license from the FortiLAN Cloud GUI. This operation is supported in the **Feature License** tab.



Note: The feature license management option is supported only on firmware version 7.0 and above.

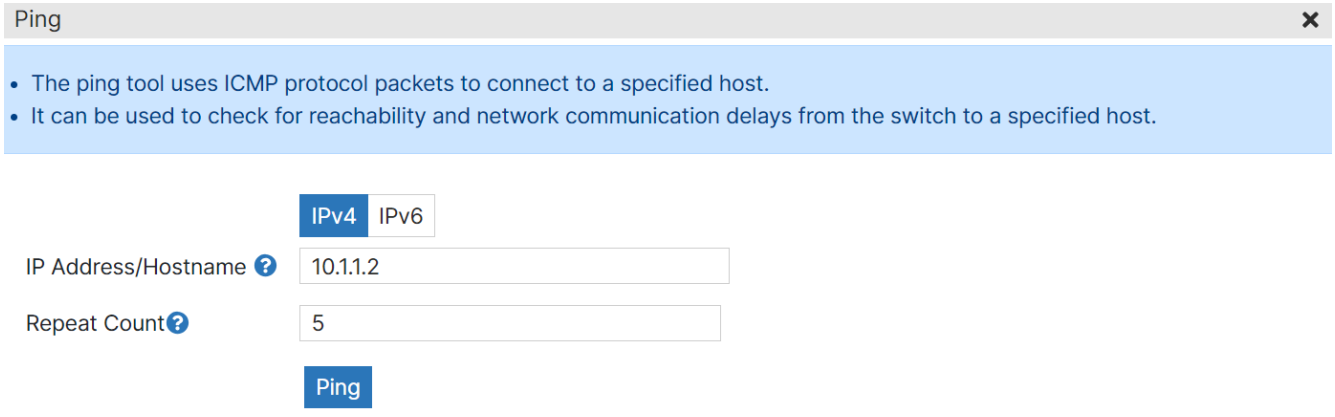
Tools

The following troubleshooting tools are available in FortiSwitch. You can access them from the **Diagnostics and Tools** panel.



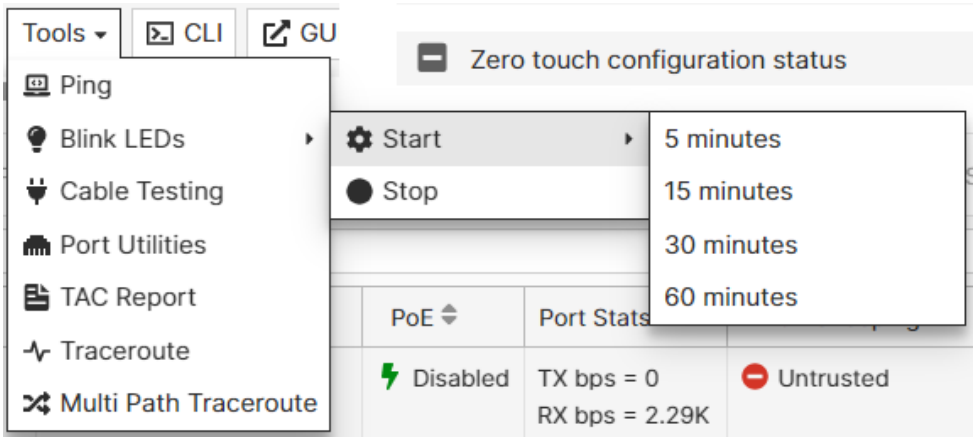
Ping

The ping command sends data packets to a specific IP address on a network, and then lets you know how long it took to transmit that data and get a response. This is used to determine reachability of the FortiSwitch to other devices on the internal or external Internet. You can conduct a ping test to an IP/domain from a FortiSwitch for troubleshooting, reachability and other network connectivity issues. The ping tool uses ICMP protocol packets to connect to a specified host. Both IPv4 and IPv6 hosts are supported.



Blink LEDs

Starting this operation, blinks the FortiSwitch LEDs for a specific time period. This is used to identify the physical location of a specific switch/port in a rack. Click **Start** and select a time duration, to stop the blinking LEDs before the configured time, click **Stop**.

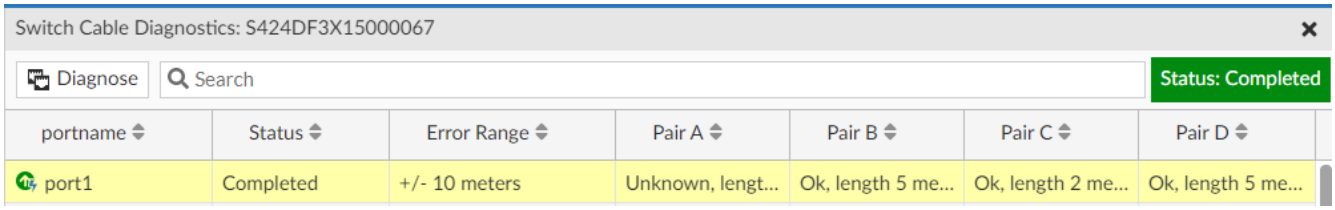


Cable Testing

This is a diagnostic and troubleshooting tool to check the state of cables between the FortiSwitch and the devices connected to its physical ports. This tool does not work on fiber ports and on very short or very long cables (more than 100 meters).

All available external physical ports of the FortiSwitch are displayed. Select one or more ports and click **Diagnose**.

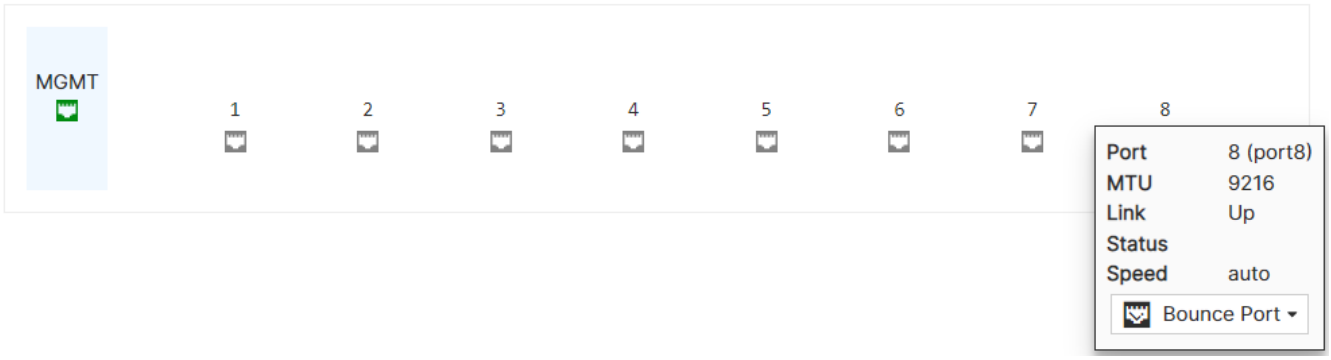
Note: Running the cable diagnostic test on a port disables it briefly. The network traffic is affected for a few seconds.



Port Utilities

You can use the **Bounce Port** utility to disable a port for a specific period of time. This allows you to isolate problematic clients or force a network reconfiguration on the connected clients. You can stop the bounce port operation mid-way and the connected clients recover immediately.

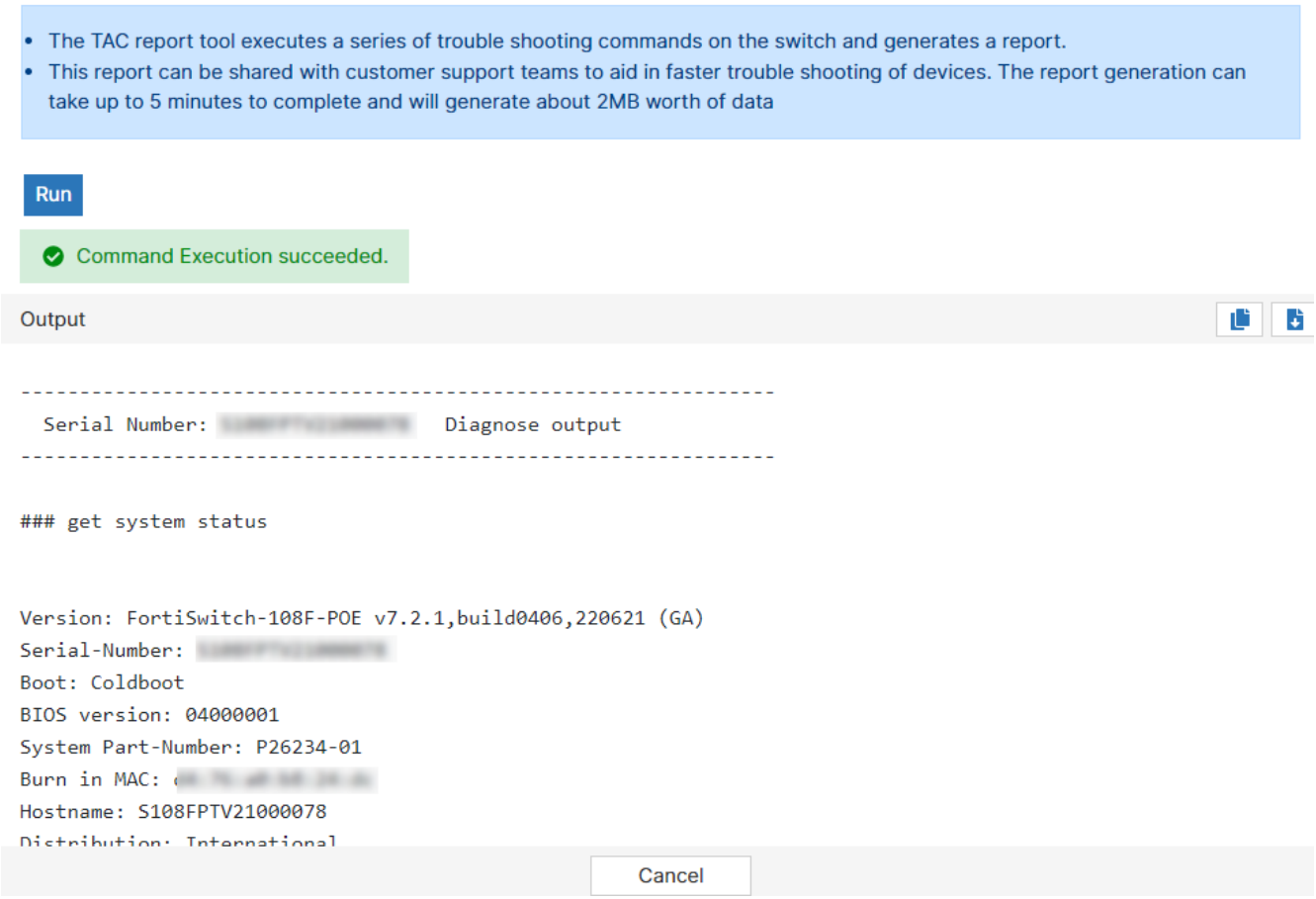
The **PoE Reset** utility resets the power supplied over Ethernet on a specific port. This enables you to reset PoE devices connected to the port, when the devices are located in an environment where physical access is not easily achievable.



TAC Report

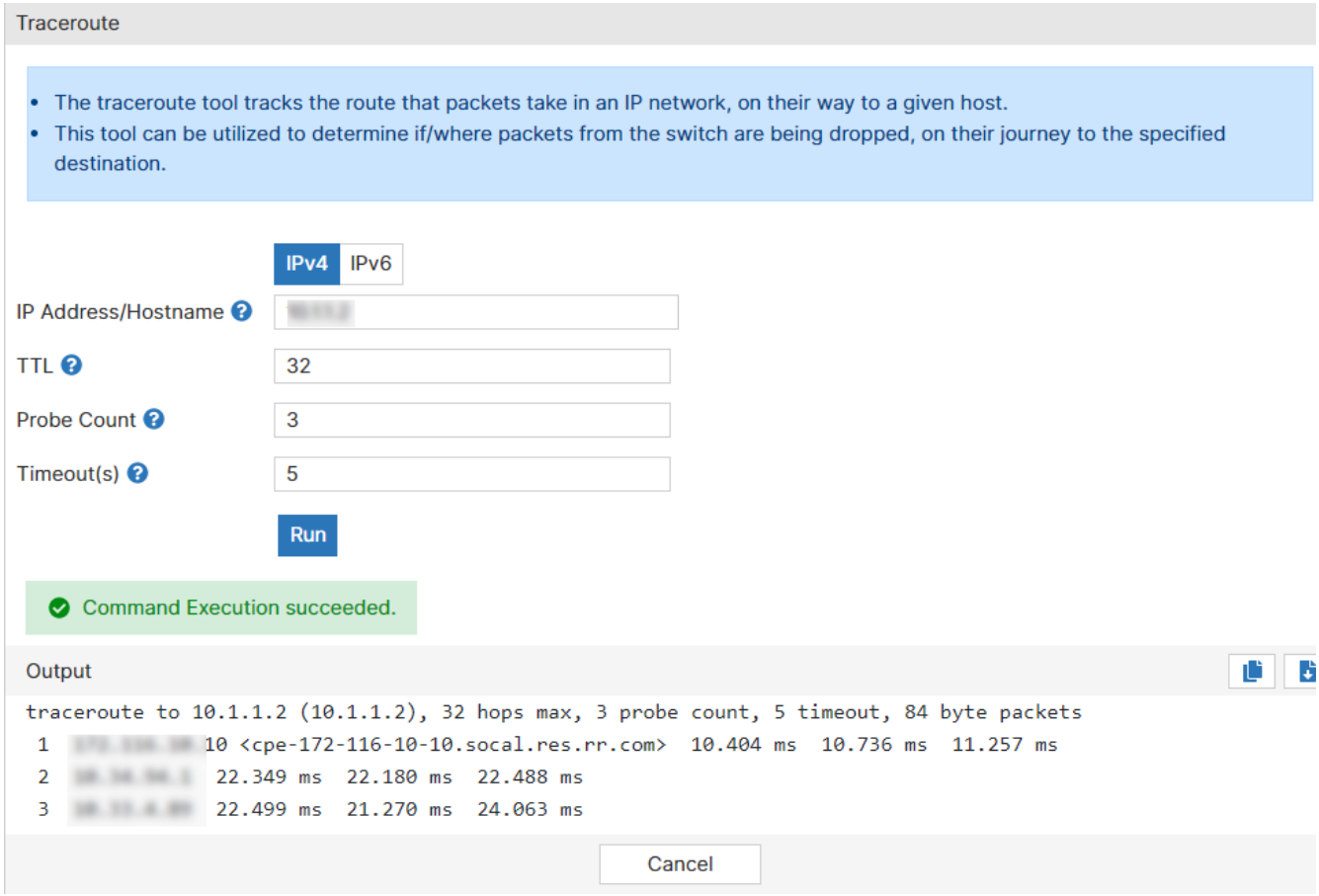
The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands. This report contains a significant amount of information which can be used by the TAC team to analyze issues that a customer is seeing on his FortiSwitch device.

Click **Run**. The report generation can take up to 5 minutes to complete and generates approximately 2 MB worth of data.



Traceroute

The traceroute tool utilizes ICMP packets to trace the different servers/routers that a packet visits, on its journey to a specified host. This tool is used to determine specific points in a network with bottle necks/traffic drops.



Update the following configuration for IPv4.

- **IP Address/Hostname** – The IPv4 address or host name to trace the route to.
- **TTL** – The maximum time-to-live (number of hops) that the route can take. The valid range is 1 – 64 and the default is 32.
- **Probe Count** – The number of probes to use to trace the route. The valid range is 1 – 5 and the default is 3.
- **Timeout(s)** – The time duration that the route is probed for, before the trace route stops. The valid range is 1 – 10 seconds and the default is 5 seconds.

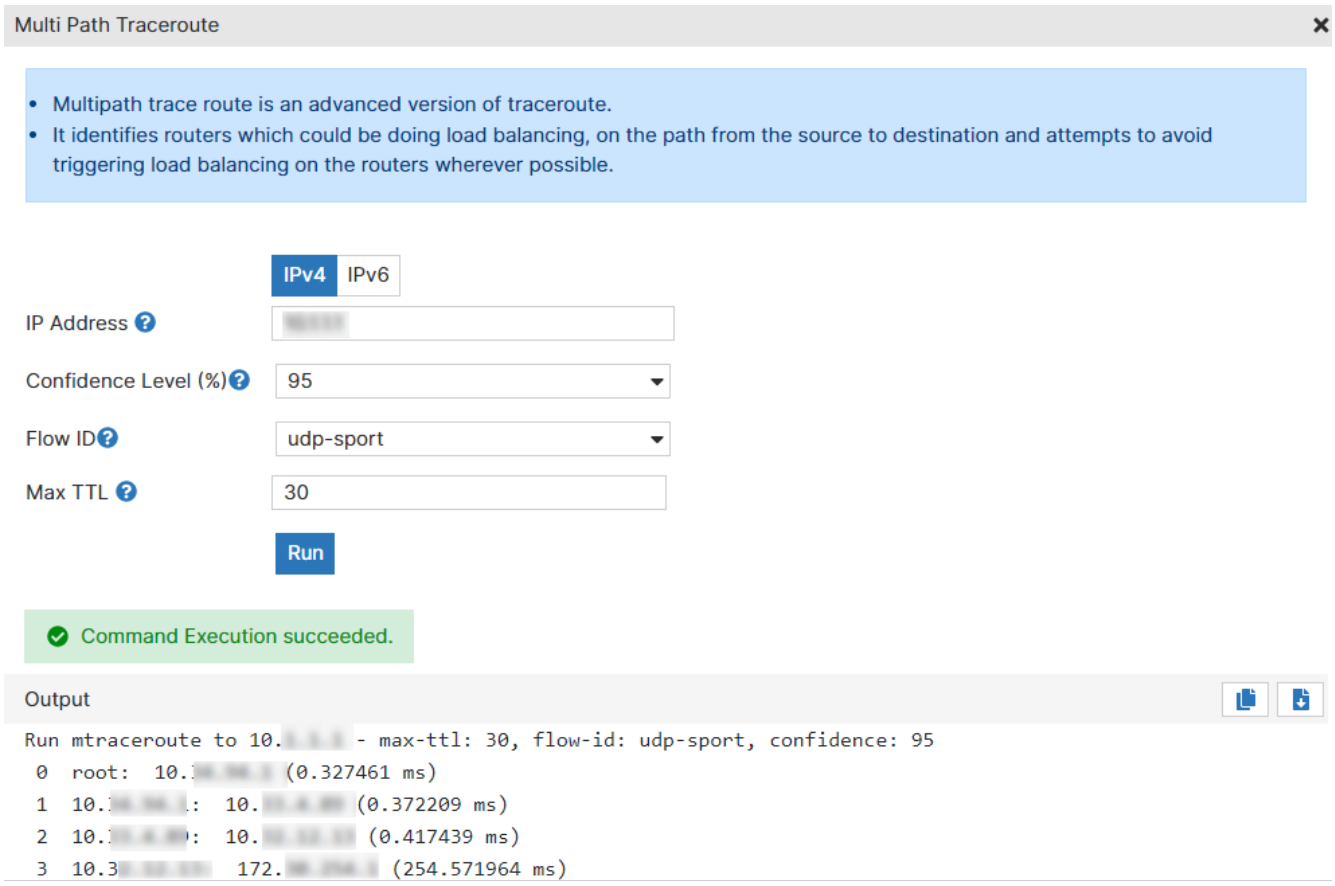
Update the following configuration for IPv6.

- **IP Address/Hostname** – The IPv6 address or host name to trace the route to.
- **Fragment** – Enable/disable the Don't Fragment flag.
- **Resolve Name** – Enable resolving the numeric address to domain name.
- **Max TTL** – The maximum number of hops used in outgoing probe packets. The valid range is 1 – 255 and the default is 30.

Multi Path Traceroute

This is an advanced version of traceroute that identifies routers which could be load balancing on the path from the source to destination. It attempts to avoid triggering load balancing on the routers, wherever possible. Update the following configuration for IPv4/IPv6.

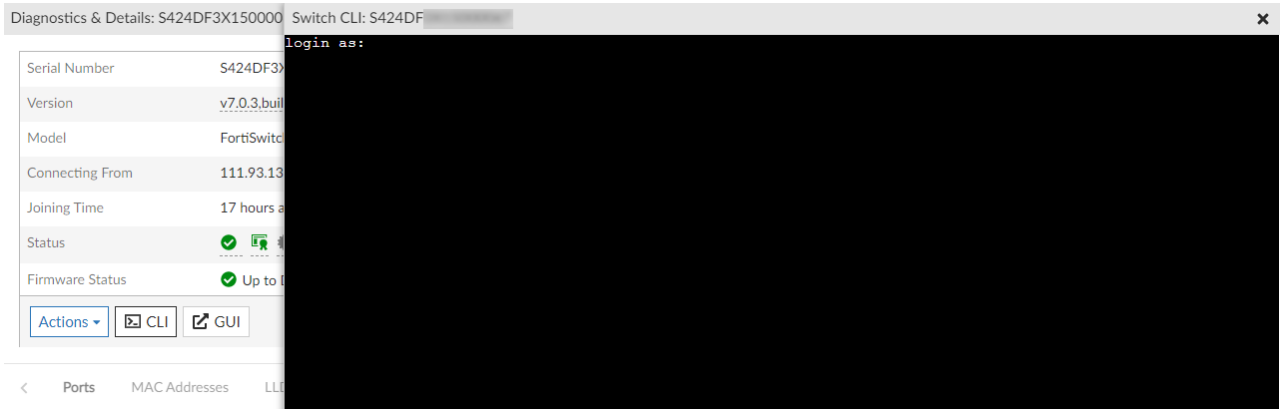
- **IP Address** - The IP address or host name to trace the route to.
- **Confidence Level (%)** – Select the confidence level. The allowed values are 90, 95, and 99, the default is 95.
- **Flow ID** – Select the flow identifier.
- **Max TTL** - The maximum time-to-live (number of hops) used in outgoing probe packets. The valid range is 1 – 255 and the default is 30.



Using the FortiSwitch CLI

To use the CLI for a FortiSwitch unit:

1. Select **CLI** in the **Diagnostics and Tools** panel of the FortiSwitch unit.

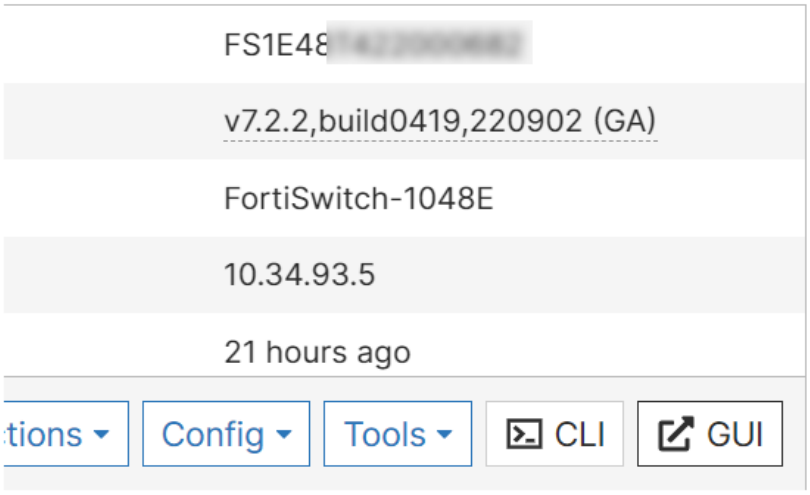


2. In the CLI window, log in with your credentials for the FortiSwitch unit.

Using the FortiSwitch GUI

To use the GUI for a FortiSwitch unit:

1. Select **GUI** in the **Diagnostics and Tools** panel of the FortiSwitch unit.



2. Log in with your credentials for the FortiSwitch unit.

Defining Switch Name-Value Pairs

The zero-touch configuration CLI templates allow switch specific parameter values, each switch can have its own name-value pairs (NVPs). The NVPs for switches are defined in the **Deployed Switches** page (before deployment) or in the **Switch Inventory** page (after deployment). The switch specific NVPs are defined once and used across multiple zero-touch configuration templates.

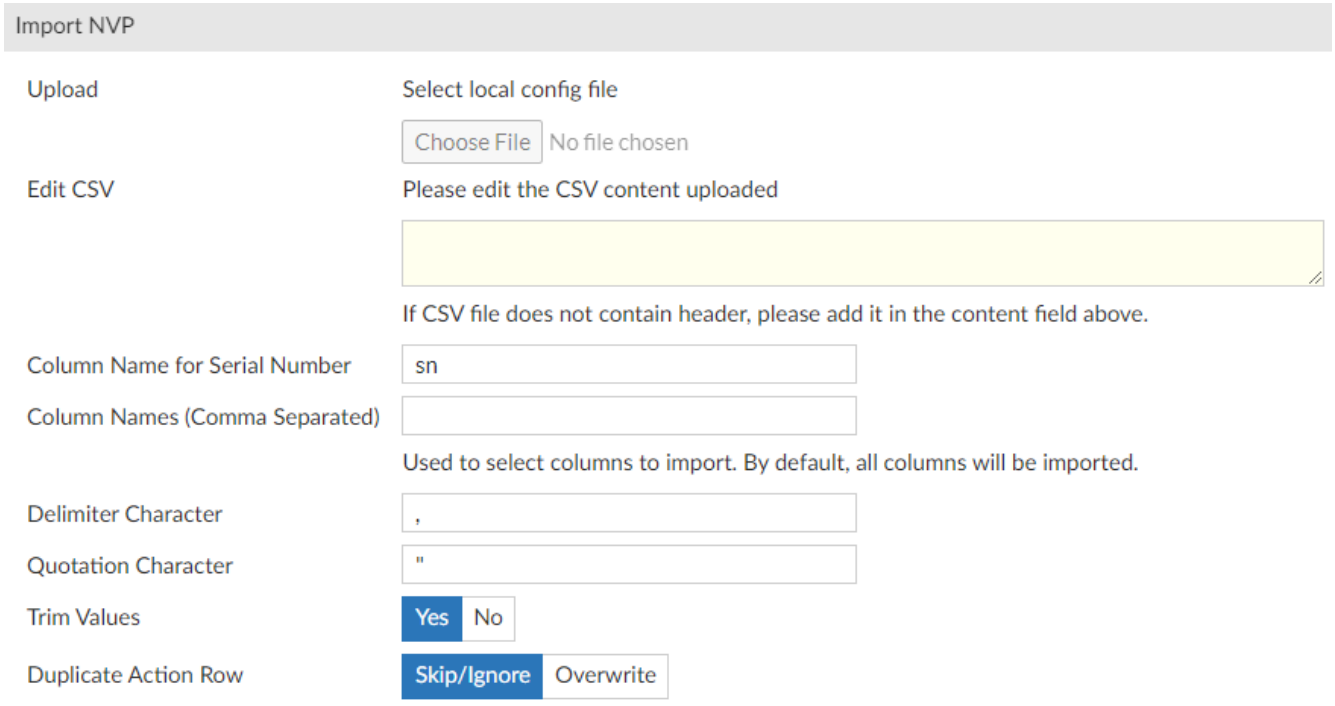
1. Click **NVP**, the **Inventory Switch Name Value Pairs (NVP) List** is displayed.
2. Click **Add**.
3. Select the **Switch** serial number.
4. Enter a unique **Parameter Name**. This value is case-insensitive and a maximum of 512 characters are allowed.
5. Enter a unique **Parameter Value**. This value is case-insensitive and a maximum of 2048 characters are allowed.

Note: A maximum of 1024 NVPs per switch are allowed.

FortiLAN Cloud supports the import and export of NVP data in the CSV format. This is useful for bulk data addition/updation and backup/restoration of data. Click **Import** to upload the NVP data, the following is a sample CSV file.

```
sn, hostname, password
S548DF5019000917, FSW_NYC_1, fortinyc1
S548DF5019000918, FSW_NYC_2, fortinyc2
```

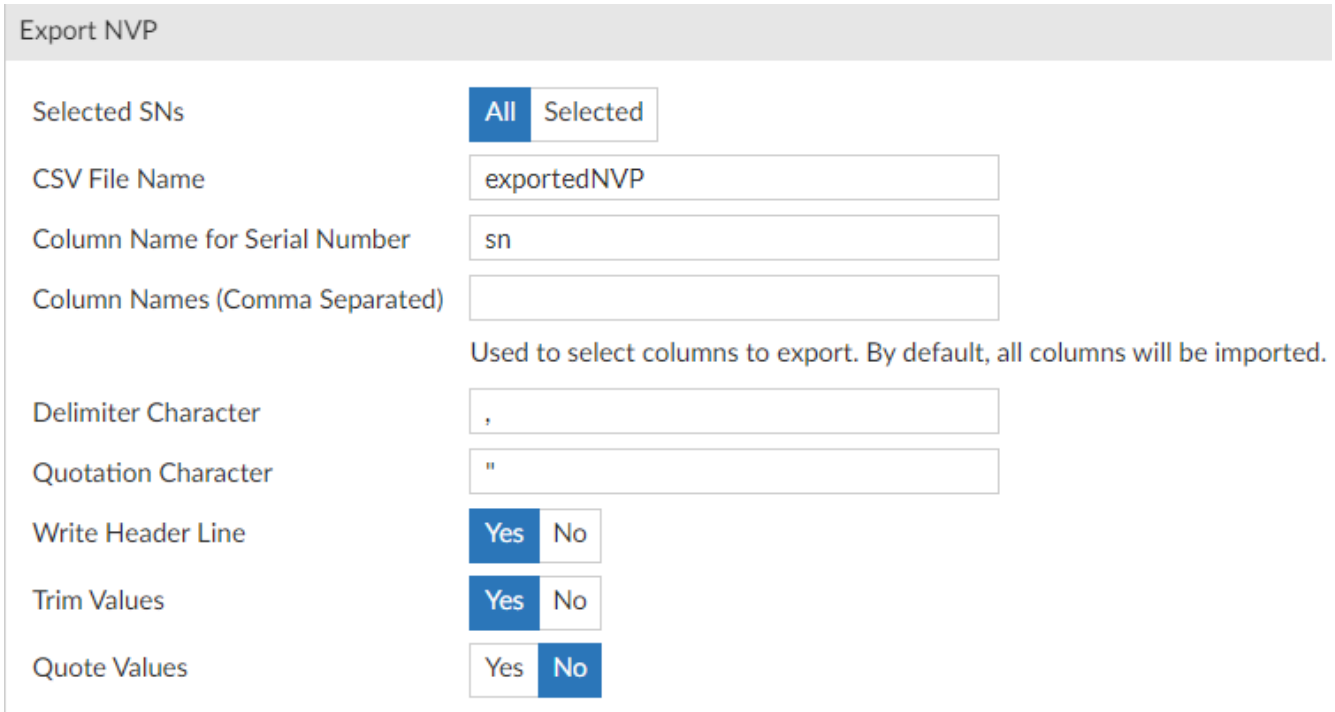
The maximum file size is supported in 2 MB.



You can edit the data in the content field after upload and additionally populate/modify the following.

- **Column Name for Serial Number**: Identifies the column in the CSV file that represents the device serial number.
- **Column Names**: Identifies the columns in the CSV file to import selectively. By default, all columns are imported. The **Column Name for Serial Number** is implicitly included.
- **Delimiter character**: A single character field specifying the character used to separate fields.
- **Quotation Character**: A single character field specifying the character used to surround values, especially when they contain the delimiter character.
- **Trim Values**: Specifies whether to strip values of leading and trailing white spaces while parsing.
- **Duplicate Action Row**: Whether a duplicate row (data line) is ignored or overwritten.

Likewise, click **Export** to save NVP data.



- **Column Name for Serial Number**: Identifies the column name to export for the specific switch.
- **Column (Parameter) Names (Comma Separated)**: A comma-separated list of NVP parameter names to export. If not specified then only the serial number column is exported.
- **Delimiter Character** and **Quotation Characters** are single character fields, when not specified, they default to comma and double-quote respectively.
- **Trim Values**: Specifies whether to strip values of leading and trailing white spaces while parsing.

Click **Download Sample CSV** to download a sample *.csv* file populated with actual FortiSwitch serial numbers. You can select the required serial numbers and modify the column data to include NVPs for FortiSwitches and then import it.

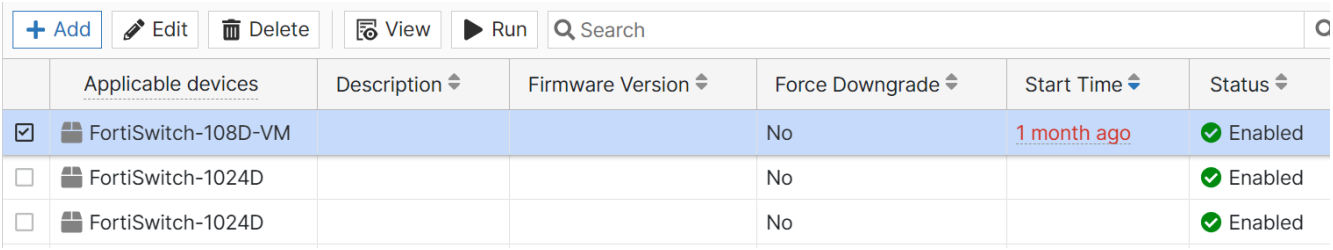
Configuration

Select *Configuration* to configure switches, ports, interfaces, VLANs, and remote authentication servers and to create zero-touch configurations, scheduled upgrades, packet capture profiles, VLAN templates, and user groups.

You can select the following options from the left pane:

Zero Touch Configurations

The Zero Touch Configurations pane allows you to apply the same configuration to all FortiSwitch units of a specific model.



To find a specific tag, switch, model, or firmware version, enter part or all of the search item in the Search field.

Note: The switch configuration is retained when the switch is moved from the combined default network to a different network and vice versa; until the user/administrator apply new configuration in the related network.

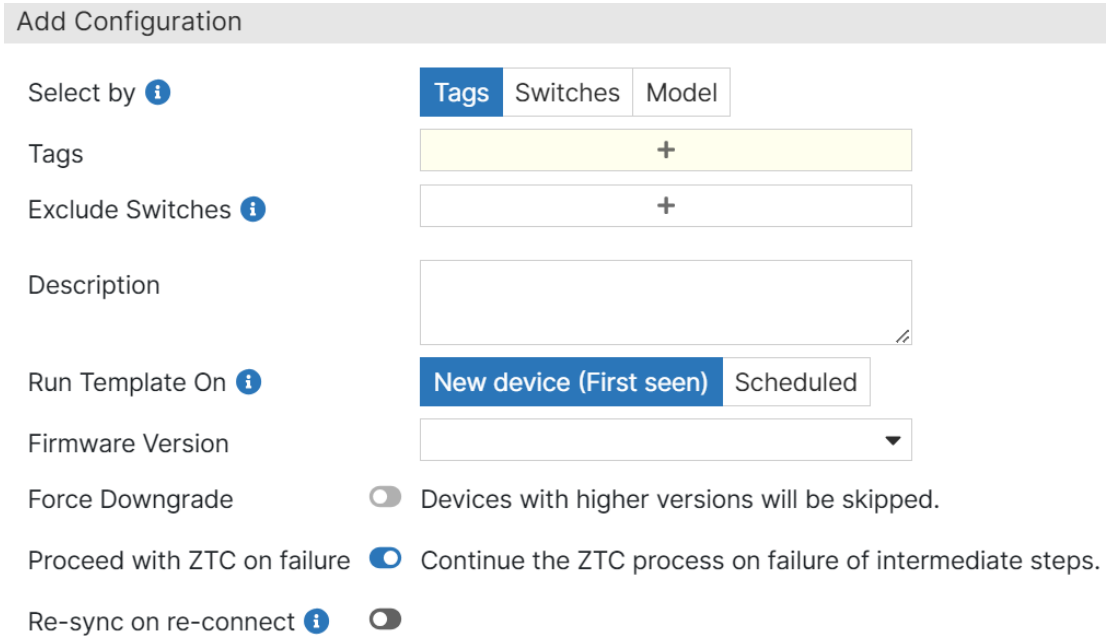
You can perform the following tasks from the Zero Touch Configurations pane:

- Creating a zero-touch configuration on page 177
- Running a zero-touch configuration on page 189
- Editing a zero-touch configuration on page 190
- Deleting a zero-touch configuration on page 190

Creating a zero-touch configuration

You can create a zero-touch configuration using switch tags, FortiSwitch serial numbers, or a single FortiSwitch model. Zero-touch configurations are run on a scheduled date and time or when FortiSwitch units are deployed in FortiLAN Cloud. You can apply CLI commands or GUI configuration templates, update the firmware, or both.

1. Navigate to **Configuration > Zero Touch Configurations** and select **Add**.



2. Select **Tags**, **Switches**, or **Model**.
   - If you select **Tags**, select one or more switch tags to apply the zero-touch configuration to.
   - If you select **Switches**, select one or more FortiSwitch units.
     NOTE: Do not include the same switch or switches in both a zero-touch configuration and a scheduled upgrade.
   - If you select **Model**, select a FortiSwitch model to apply the zero-touch configuration to.
3. You can exclude specific FortiSwitches from the scheduled upgrade. Click **Exclude Switches** and select the entries.
4. Select when the configuration templates are applied to the devices. Click **Run Template On**.
   - If you select **New device (First seen)**, the firmware is upgraded and the configuration applied when FortiSwitch units are deployed in FortiLAN Cloud.
   - If you select **Scheduled**, select the date and time for the firmware to be upgraded and the configuration applied .
5. If you want to change the **Firmware Version**, select the firmware image to apply. The available firmware images and the latest version are listed.
6. Select **Force Downgrade** to forcefully downgrade newly deployed FortiSwitches.
7. Enable **Proceed with ZTC on Failure** to proceed with ZTC, bypassing intermediate failures (if any). If disabled, the ZTC process is halted in the event of an intermediate failure. For example, in case of a firmware failure, the CLI and GUI template configurations are not pushed to the FortiSwitch. This option is enabled by default; disable it if you want to halt the ZTC process in the event of any intermediate failures.
8. Enable the **Re-sync on re-connect** option to ensure that the ZTC template configuration is applied to the FortiSwitch, each time it re-connects to FortiLAN Cloud. When this option is enabled and the configuration is pushed, there is a cool-down period of 30 minutes; during this period the configuration is not applied and the FortiSwitch is allowed to re-connect to FortiLAN Cloud.
   Note: Ensure that the ZTC template does not contain any configuration that could potentially cause the FortiSwitch to restart. This is to avoid the *reboot-config-push* loop.

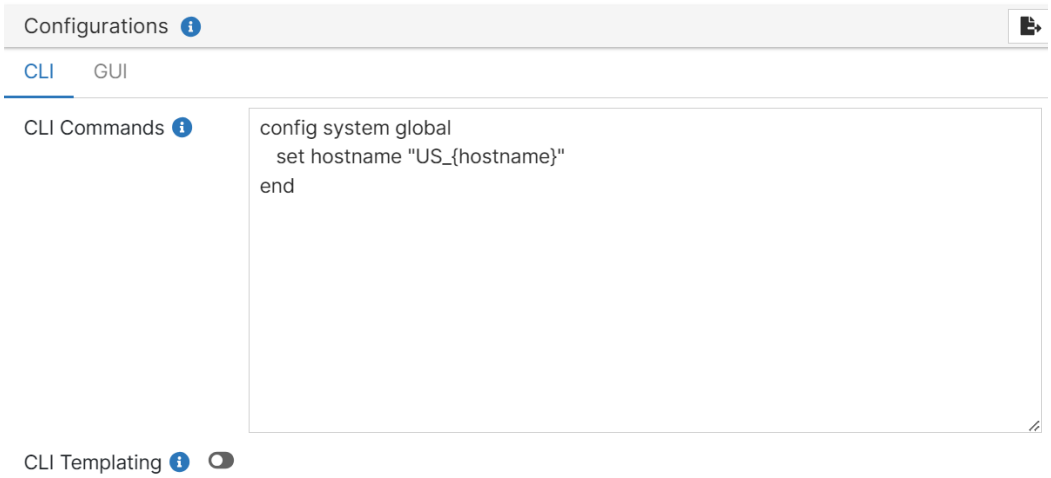
Configurations

You can create CLI and GUI configuration templates.

- CLI Configurations
- GUI Configurations

CLI Configurations

Enter the **CLI** commands to apply to the selected FortiSwitch model or create a CLI template. A CLI template has parameter names (placeholders) instead of static parameter values. The parameter names are resolved dynamically to their switch specific parameter values when the CLI template is applied to a switch, as defined in the NVP data; the variables ($param) are declared in the NVP and called in the CLI template. See Defining Switch Name-Value Pairs on page 173. The parameter values are contained in braces. Enable **CLI Templating** to use configured templates. This example sets different values for *hostname* and *password* on multiple switches.



Refer to the *FortiSwitchOS CLI Reference* for available commands.

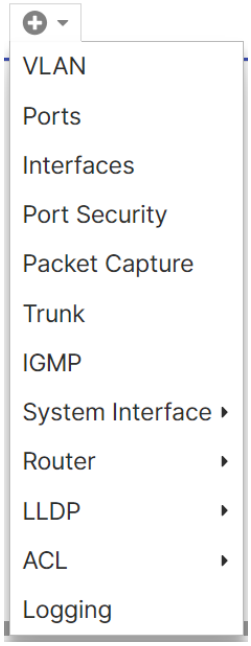
Note: You can enter 250 KB of CLI commands.

GUI Configurations

Create a **GUI** template, click **Add** and create the following template configurations.

- **VLAN** - Create template configurations to add a VLAN, modify an existing VLAN or delete a VLAN. To configure a template, see VLAN Templates on page 208.
- **Ports** - To configure the administrative status and PoE status of the FortiSwitch, see Ports on page 199.
- **Interfaces** - To configure interface VLANs, see Configuring interface VLANs on page 201.
- **Port Security** - To configure 802.1x/802.1x MAC based security, see Editing the port security on page 204.
- **Packet Capture** - To configure a packet capture profile, see Creating a packet capture profile on page 203. You can add a packet capture profile, modify an existing profile or delete a profile.
- **Trunk** - To configure a trunk, see Creating a trunk on page 201 . You can add a trunk, modify an existing trunk or delete a trunk.
- **IGMP** - To configure IGMP settings, see IGMP. You cannot modify **Action**.
- **System Interfaces** - You can configure physical and VLAN interfaces on a FortiSwitch, see System Interfaces.

- **Router** - Routing configuration is supported on FortiSwitches managed by FortiLAN Cloud. You canadd/modify the following configurations. Routing information and interfaces are monitored on the **RoutingTable** and **Link Monitor** pages. See Router.
- **LLDP** - To configure LLDP **Settings** and **Profile**, see LLDP. You cannot modify **Action** when configuring the LLDP settings.
- **ACL** - To configure ACL **Settings**, see ACL. You cannot modify **Action**.
- **Logging** - To configure external Syslog server for switch logs, see Logging. You cannot modify **Action**.



Additionally, you can export (save) the GUI and CLI configurations, edit and then import them to the GUI to facilitate reuse. Click on **Export** and **Import** as required; JSON file format is supported for both operations.

IGMP

Configure the following IGMP parameters.

Parameter	Description
Aging Time	The maximum time to retain a multicast snooping entry for which no packets are visible. The valid range is 15 - 3600 seconds.
Query Interval	The maximum time after which the IGMP query is sent. The valid range is 10 - 1200 seconds.
Proxy Report Interval	The unsolicited report interval time period. The valid range is 1 - 260 seconds.
Leave Response Timeout	The time that the FortiSwitch waits after sending group specific queries in response to the leave message. The valid range is 1 - 20 seconds.

System Interfaces

Configure the following parameters for the physical and VLAN interfaces.

Parameter	Description
Interface Name	Enter the name of the interface. Interface names can't be changed.
Alias	Enter an alternate name for a interface on the FortiSwitch unit.
VLAN ID	Enter the VLAN identifier for a VLAN interface.
IP Configuration	**Static** - Configure a static IP address and netmask of the interface. **DHCP** - Configure the interface to receive its IP address from an external DHCP server.
Administration	Indicates if the interface can be accessed for administrative purposes. If the administrative status is **Up**, an administrator can connect to the interface using the configured access. If the administrative status is **Down**, the interface is administratively down and can't be accessed for administrative purposes. Select the types of access permitted on this interface or secondary IP address.
Secondary IP	Add additional IP addresses to this interface. Select the expand arrow to expand or hide the section.
DHCP Relay	Enable/Disable DHCP relay for the physical interface.
VRRP	The Virtual Router Redundancy Protocol (VRRP) uses virtual routers to control which physical routers are assigned to an access network. A VRRP group consists of a master router and one or more backup routers that share a virtual IP address. The VRRP master router sends VRRP advertisement messages to the backup routers. When the VRRP master router fails to send advertisement messages, the backup router with the highest priority takes over as the master router. To create a VRRP group, you need to create a VRRP virtual MAC address, which is a shared MAC address adopted by the VRRP master. • Enter the unique virtual router identifier (ID). • Enter the VRRP group number. • Enter the priority. If the highest priority value of 255 is entered, the virtual router becomes the master router. If the master router fails, the VRRP automatically assigns one of the backup routers without affecting network traffic. When the failed router is functioning again, it becomes the master router again. • Select Preempt if you want the router to preempt the master virtual router if the priority changes. • Enter the source virtual IP address that will be shared across the VRRP group.

Router

Configure the following routing information.

Parameter	Description
Static and IPv6 Static	To provide remote access to the management port, configure an IPv4 or IPv6 static route. Set the gateway address to the IPv4 or IPv6 address of the router.

Parameter	Description
	Configure the following for IPv4 static route. • The *Destination IP/ Netmask* for the route. • Enable *Blackhole* to disable all the Gateway options. • The pre-configured *Gateway out interface*. • Enable *Dynamic Gateway* to disable the Gateway option. • The *Gateway* router IPv4 address. Configure the following for IPv6 static route. • The *Destination IP/ Netmask* for the route. • Enable *Blackhole* to disable all the Gateway options. • The pre-configured *Gateway out interface*. • The *Gateway* router IPv6 address. • The administrative *Distance* for all routes. • Enable the *BFD* (Bidirectional Forwarding Detection).
Link Probes	You can create a probe to monitor the link to a server. The FortiLAN Cloud sends periodic ping messages to test that the server is available. • The *Source Interface*. Can be the physical or VLAN interface name. • The *Protocol* to detect the server. Select ARP or ping. • The *Source IP* address used in packet to the server. • The *Gateway IP* address used to ping the server. You can configure the following **Advanced Settings**. • *Detection Interval (Seconds)* - The detection interval in seconds. The range is 1-3600. • *Detection Timeout (Seconds)* - The detection request timeout in seconds. The range is 1-255. • *Retries Before Down* - The number of retry attempts before bringing the server down. • *Retries Before Up* - The number of retry attempts before bringing the server up.
OSPF	Open shortest path first (OSPF) is a link-state interior routing protocol that is widely used in large enterprise organizations. OSPF provides routing within a single autonomous system (AS). • Enter the *Router IP* address. • Enable *Default Information Originate* to generate and advertise a default route into the device's RIP-enabled networks. The generated route may be based on routes learned through a dynamic routing protocol, routes in the routing table, or both. • Enter the *Default Information Metric* for routing. • If you want to *Redistribute* non-RIP routes, select *Enable* under Connected, Static, OSPF, BGP, or ISIS. If you select *Enable*, enter the routing metric to use. • An OSPF implementation consists of one or more *Areas*. An area consists of a group of contiguous networks. The FortiSwitch unit supports different types of areas—*stub* areas, Not So Stubby areas (*NSSA*), and *Regular* areas. A stub area is an interface without a default route configured. NSSA is a type of

Parameter	Description
	stub area that can import AS external routes and send them to the backbone but cannot receive AS external routes from the backbone or other areas. All other areas are considered regular areas. • Enter a unique value to identify this *Network* configuration. Enter an IP address and netmask for your RIP network. You can configure multiple networks. • Configure ODPF *Interface*. In the *Hello Interval* field, enter the number of seconds that the FortiSwitch unit waits between sending hello messages to neighboring PIM routers. If you want to use *Authentication*, select *Text*, *MD5*, or *None*. • Enable *Bidirectional Forwarding Detection* • Configure the interface *Maximum Transmission Unit (MTU)* packet size. • Enable *Fast Hello*, which provides a way to send multiple hello packets per second. • Configure the *Hello Interval*. OSPF Hello protocol is used to discover and maintain communications with neighboring routers. Hello packets are sent out at a regular interval. • The *Dead interval* is the time other routers wait before declaring a neighbor dead (offline).

RIP	The Routing Information Protocol (RIP) is a distance-vector routing protocol that works best in small networks that have no more than 15 hops. Each router maintains a routing table by sending out its routing updates and by asking neighbors for their routes.
	• The FortiSwitch unit supports RIP version 1 and RIP version 2.
	  • RIP version 1 uses classful addressing and broadcasting to send out updates to router neighbors. It does not support different sized subnets or classless inter-domain routing (CIDR) addressing.
	  • RIP version 2 supports classless routing and subnets of various sizes. Router authentication supports MD5 and authentication keys. Version 2 uses multicasting to reduce network traffic.
	• Enable *Default Information Originate* to generate and advertise a default route into the device's RIP-enabled networks. The generated route may be based on routes learned through a dynamic routing protocol, routes in the routing table, or both.
	• Enable *Bidirectional Forwarding Detection* to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and, if a timer runs out on a connection, that router is declared to be down. BFD then communicates this information to RIP, and the routing information is updated.
	• Enter the *Default Metric*. RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the FortiSwitch unit. A hop count of 16 represents a network that cannot be reached.
	• If you want to change the default *Timers* value, enter the number of seconds in the *Update*, *Timeout*, and *Garbage* fields.

Parameter	Description
	• The update timer determines the interval between routing updates. The default setting is 30 seconds. • The timeout timer is the maximum time that a route is considered reachable while no updates are received for the route. The default setting is 180 seconds. The timeout timer setting should be at least three times longer than the update timer setting. • The garbage timer is the is the how long that the FortiSwitch unit advertises a route as being unreachable before deleting the route from the routing table. The default setting is 120 seconds. • If you want to *Redistribute* non-RIP routes, select *Enable* under Connected, Static, OSPF, BGP, or ISIS. If you select *Enable*, enter the routing metric to use. • Configure the router *Distance*. Enter the distance identifier in the *ID* field and select the *Access List*. Enter the IP address and netmask. • Enter a unique value to identify this *Network* configuration. Enter an IP address and netmask for your RIP network. You can configure multiple networks. • Configure RIP for the appropriate *Interface*. If you want to change the RIP version used to send and receive routing updates, select from the *Send Version* and *Receive Version* drop-down menus. If you do not want to send RIP updates from this interface, select *Passive Interface*. If you want to use *Authentication*, select *Text* or *None*.
Multicast	A FortiSwitch unit can operate as a Protocol Independent Multicast (PIM) version-2 router. Add a multicast enabled interface. • Enter the *Multicast Flow* value. • In the *Hello Interval* field, enter the number of seconds that the FortiSwitch unit waits between sending hello messages to neighboring PIM routers. • In the *Designated Router Priority* field, enter a priority to the FortiSwitch unit Designated Router (DR) candidacy. The value is compared to that of other DR interfaces connected to the same network segment, and the router having the highest DR priority is selected to be the DR. If two DR priority values are the same, the interface having the highest IP address is selected. • In the *IGMP Response Time* field, enter the number of seconds between queries to IGMP hosts. • In the *IGMP Interval* field, enter the maximum number of seconds to wait for an IGMP query response.
Multicast Flows	You can specify a range of multicast group addresses when configuring a multicast flow. • Enter the *Name* of the multicast flow. • In the *ID* field, enter a number between 1 and 4294967295 to identify the multicast flow entry. • In the *Group Address* field, enter the multicast group IPv4 address. • In the *Source Address* field, enter an IPv4 address for the multicast source.

LLDP

Configure the following LLDP **Settings**.

Parameter	Description
Status	Enable/Disable the LLDP transmit and receive feature.
Management Interface	The primary management interface advertised in LLDP.
Number of TX intervals before local LLDP data expires	The number of Tx intervals before local LLDP data expires, that is, the packet TTL (in seconds) is tx-hold times tx-interval. The valid range is 1 - 16.
Frequency of LLDP PDU transmit (seconds)	The frequency of LLDP PDU transmission. The valid range is 5 - 4095.
Fast Start	The frequency of LLDP PDU transmit for the first 4 packets when the link comes up. Configure the **Fast Start Interval**, the valid range is 2 - 5 seconds.
Device Detection	Enable/disable dynamic updates of LLDP neighbour devices to FortiLink.

Configure the following LLDP **Profile** parameters.

Parameter	Description
Profile Name	A unique name of the Profile. The valid range is 63 characters.
Transmitted IEEE 802.1 TLVs. (Port VLAN ID)	Enable to transmit the IEEE 802.1 port native-VLAN Type-Length-Value (TLV).
Transmitted IEEE 802.3 TLVs.	Enable to transmit the IEEE 802.3 organizationally-specific TLVs. The following options are available, you can select more than one. • **Maximum frame size TLV** - This TLV sends the maximum frame size value of the port. If this variable is changed, the sent value will reflect the updated value. • **PoE+ classification TLV** - This TLV sends whether there is software PoE negotiation on the port. • **Efficient Energy Ethernet Config** - This TLV sends whether energy-efficient Ethernet is enabled on the port. If this variable is changed, the sent value will reflect the updated value.
Auto MCLAG inter chassis link	Enable the multi-chassis link aggregation group (MCLAG).
Enable/disable automatic Inter-Switch LAG	Enable or disable the automatic inter-switch LAG. • **Automatic ISL Hello Timer** - The time for the automatic inter-switch LAG hello timer. The valid range is 1 - 30 seconds and the default is 3 seconds. • **Automatic ISL timeout** - The time before the automatic inter-switch LAG times out if no response is received. The valid range is 0 - 300 seconds and the default is 60 seconds. • **Automatic inter-switch LAG port group** - The automatic inter-switch LAG port group identifier. The valid range is 0 - 9.
Transmitted LLDP-MED TLVs	Select the LLDP-Media Endpoint Discovery (MED) TLVs to transmit; **Inventory Managment TLVs, Network Policy TLVs, Power Management TLV**, and **Location Identification TLVs**. You can select one or more option.

Parameter	Description
MED Network Policy	Enter the following for MED network policy. • **Name** - Select which MED network policy type-length-value (TLV) category to edit; **Voice, Voice Signalling, Guest Voice, Guest Voice Signalling, Softphone Voice, Video Conferencing, Streaming video, Video Signalling**. • **Status** - Enable or disable whether this TLV is transmitted. • **Assign VLAN** - Enable or disable whether to assign a VLAN interface. • **VLAN** - The VLAN interface to advertise. The valid range is 0 - 4094. • **Priority** - Tthe advertised Layer-2 priority. The valid range is 0 - 7, set to 7 for the highest priority. • **DSCP** - The advertised DSCP value to indicate the level of service requested for the traffic. The valid range is 0 - 63.
MED location Service	Enter the following for MED location services. • **Name** – Select which MED location type-length-value (TLV) category to edit; **Civic Address**, **Co-ordinates**, **ELIN Number**. • **Status** – Enable or disable whether this TLV is transmitted. • **Sys Location ID** – If the status is enabled then you can enter the location service identifier. The maximum length is 63 characters.
Custom TLVs	Enter the following for custom TLVs. • **Name** - The name of a custom TLV entry. • **Oui** – The organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV. • **Subtype** – The organizationally defined subtype. The valid range is 0 – 255. • **Information String** – The organizationally defined information string in hexadecimal bytes.

ACL

Configure the following ACL **Settings**.

Parameter	Description
Density Mode	Enable the ACL density mode.
Trunk Load Balance	Enable trunk load balancing.

To configure **Ingress** (for incoming traffic), **Egress** (for outgoing traffic), and **Preelookup** (for processing traffic) policies, update the following parameters.

Parameter	Description
ID	A unique identifier for this profile. The valid range is 1 - 2048.
Active	Enable to activate the profile.
Group ID	A unique group identifier. The valid range is 1 - 2048.
Ingress Interface All	Enable to apply the profile to all interfaces.

Parameter	Description
Ingress Interface	The specific interfaces to apply the profile to.
Schedule	The schedule for when the ACL profile is enforced.
Description	The description for the profile.
Classifier - Identification of packets that the policy is applied to, each packet is classified based on one or more criteria as per these configurations.	
VLAN ID to be matched	The VLAN identifier to match.
Cost of Service	The cost of service (CoS) value to match. The valid range is 0 - 7, leave blank to disable this field.
802.1Q CoS value to be matched	The 802.1Q CoS value to match. The valid range is 0 - 7, leave blank to disable this field.
Ethernet type to be matched	The Ethernet type to match. The valid range is 1-65535.
ACL Custom Service to be matched	The pre-configured custom service type to match.
Source MAC	The source MAC address to match.
Destination MAC	The destination MAC address to match.
Source IP Prefix	The source IP address to match (IPv4 only).
Destination IP Prefix	The destination IP address to match IPv4 only).
Action - If a packet matches the classifier criteria for a given ACL, different actions are applied to a packet based on these configurations.	
Count	Enable to track the number of matching packets.
Drop	Enable to drop matching packets.
Mirror Session Name	The name of the mirror to use collect packets to analyze.
Redirect Bcast Cpu	Enable to redirect broadcast traffic to all ports including the CPU.
Redirect Bcast No Cpu	Enable to redirect broadcast traffic to all ports excluding the CPU.
Outer VLAN Tag	The outer VLAN tag.
CoS Queue	The CoS queue number. The valid range is 0 - 7, leave blank to disable this field.
Remark CoS	The CoS marking value. The valid range is 0 - 7, leave blank to disable this field.
CPU COS queue number(17 - 25). Only if packets reach to CPU	The CPU CoS queue number. This CoS queue is only used if the packets reach the CPU. The valid range is 17 - 25.
Remark DSCP	The DSCP marking value. The valid range is 0 - 63, leave blank to disable this field.
Redirect Interface	The redirect interface to use.

Parameter	Description
Redirect Physical Port	The physical ports to include in the egress mask or to redirect packets to.
Egress Mask Interface	The physical ports that are included in the egress mask.
Policer ID	The policer ID to use.

To configure the **Policer**, update the following parameters. You can add, modify, or delete an existing policer.

Parameter	Description
ID	A unique number to identify this policer. The valid range is 1-2048.
Type	Whether the policer is for the egress policy or the ingress policy.
Guaranteed Bandwidth	The amount of bandwidth guaranteed (in Kb/second) to be available for traffic controlled by the policy. The valid range is 1-524287000 Kb.
Guaranteed Burst	The guaranteed burst size in bytes. The valid range is 1-4294967295 bytes.
Maximum Burst	The maximum burst size in bytes. The valid range is 1-4294967295 bytes.
Description	A description of the policer.

To configure the **Custom Service**, update the following parameters. You can add, modify, or delete an existing policer.

Parameter	Description
Name	The name of the ACL custom service.
Comment	A description of the custom service.
Color	The icon color for the service in the Service page.
Protocol	The protocol to use with the custom service, **TCP**, **ICMP**, **IP**, **UDP**, or **SCTP**. • **Port Range** - [TCP, UDP, or SCTP] The destination ports and source ports. You can enter a single port or a range of ports in each field. • **Protocol Number** - [IP] The protocol number. • **ICMP Type/ICMP Code** - [ICMP] The ICMP type and code.The valid range is 0 - 254.

Logging

Configure the following external Syslog server parameters.

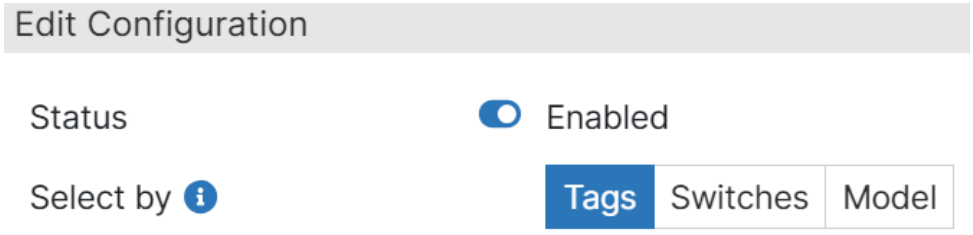
Parameter	Description
Event Types	The types of log messages sent to the Syslog server. You can enable logging activity messages for the following categories. • Link • PoE • Router • Spanning Tree • Switch

Parameter	Description
	• Switch Controller • System • User • FOS Legacy
Syslog Severity	Select the least severity level to log from the following options. • Emergency - The system is unusable. • Alert - Immediate action is required. • Critical - Functionality is affected. • Error - An erroneous condition exists and functionality is probably affected. • Warning - Functionality might be affected. • Notification - Information about normal events. • Information - General information about system operations. • Debug - Information used for diagnosing or debugging the system.
Syslog Server	Update the following Syslog server parameters. • Server - The IPv4 address or hostname (FQDN) of the remote Syslog server. • Port - The port number of Syslog server. The valid range is 1-65535 and the default is 514. • Source IP - The source IPv4 address of the Syslog server. • CSV - To enable/disable CSV.

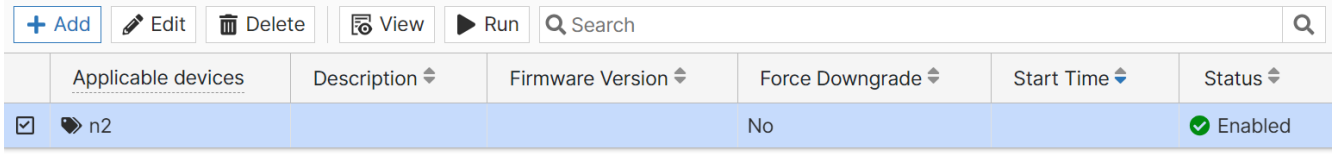
Running a zero-touch configuration

By default, a zero-touch configuration is disabled. After you enable the zero-touch configuration, the CLI/GUI configurations that were entered in the Add Zero Touch Configuration dialog box are run once on all FortiSwitch units of the specified model when they connect to FortiLAN Cloud for the first time or at the scheduled time and date.

To enable a zero-touch configuration, select the row of the zero-touch configuration that you want to run and click **Edit**; enable the configuration status.

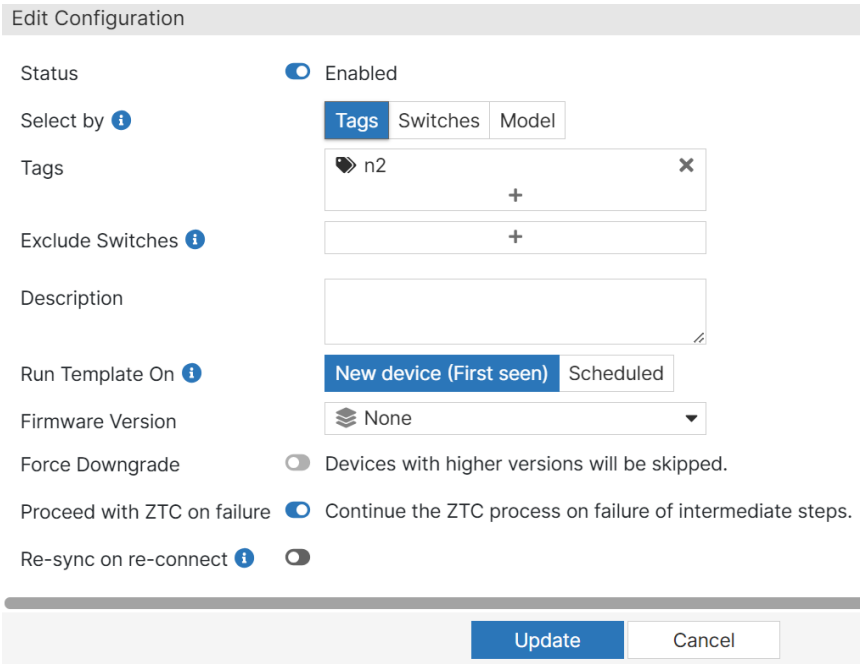


Click Update and select the row of the zero-touch configuration. Click **Run**.



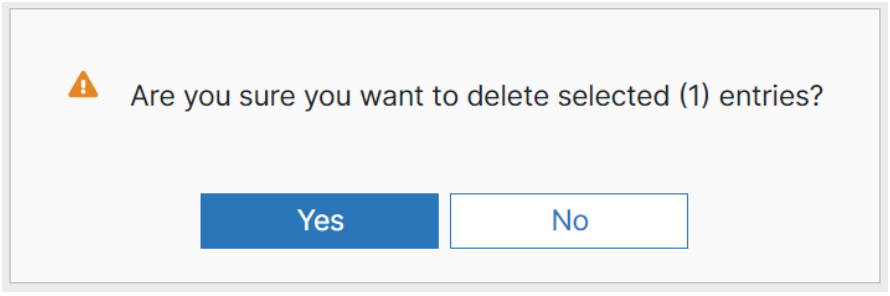
Editing a zero-touch configuration

Select the row for the zero-touch configuration that you want to edit and click **Edit**. Make your changes and **Update** to save them.



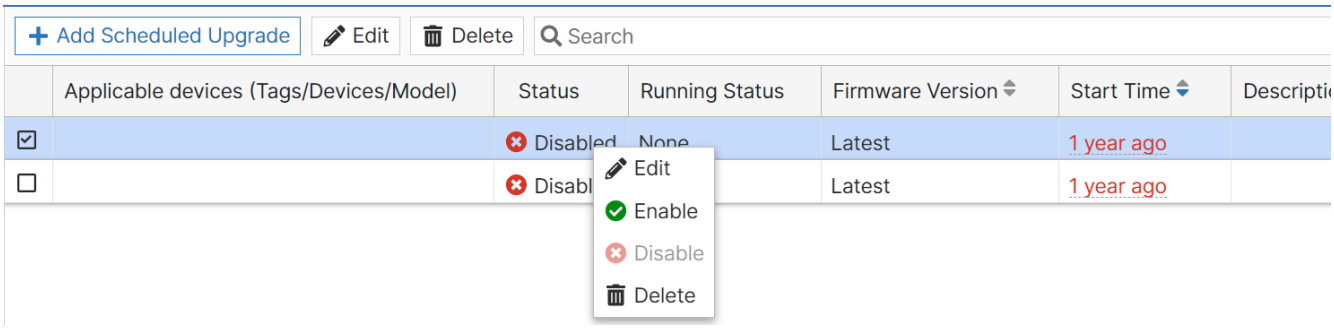
Deleting a zero-touch configuration

Select the row of the zero-touch configuration that you want to delete and click **Delete**. Select *Yes* to delete the zero-touch configuration.



Scheduled Upgrade

The Scheduled Upgrade pane allows you to specify when firmware for the already deployed FortiSwitch will be upgraded. You can schedule firmware upgrades during off-peak hours and stagger the upgrade times for each FortiSwitch model to lower the impact on the network.



To find a specific switch or tag, enter part or all of the switch or tag name in the Search field.

You can perform the following tasks from the Scheduled Upgrade pane:

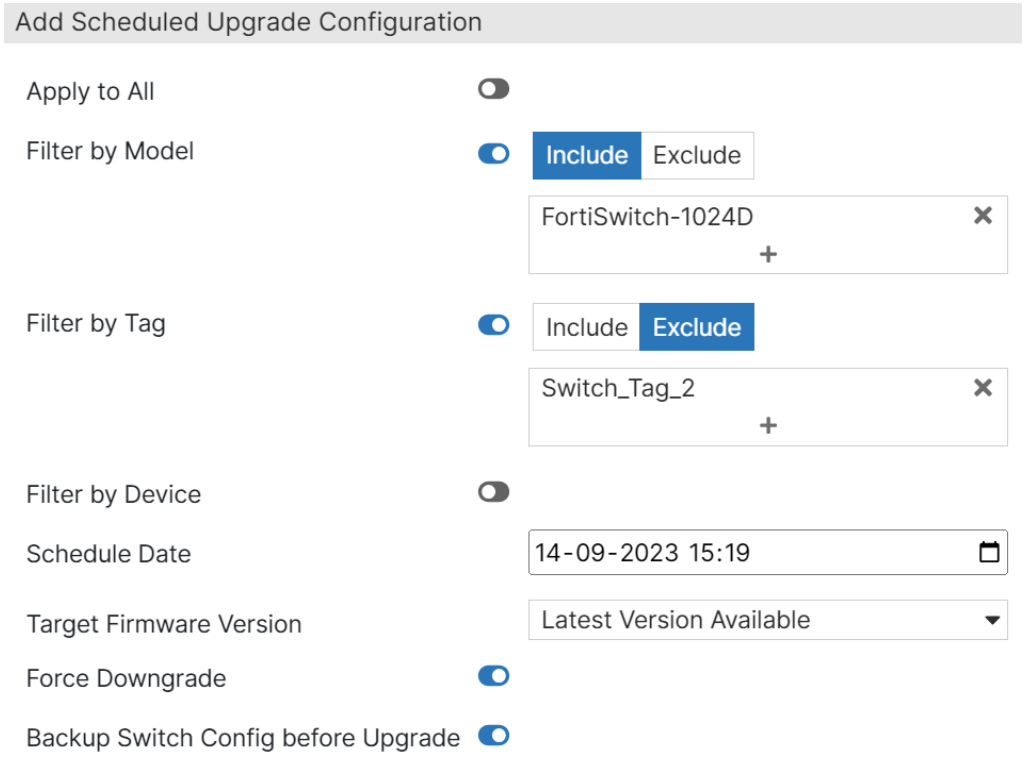
- Scheduling a firmware upgrade on page 191
- Editing a scheduled upgrade on page 193
- Deleting a scheduled upgrade on page 193

Scheduling a firmware upgrade

NOTE: Do not include the same switch or switches in both a zero-touch configuration and a scheduled upgrade.

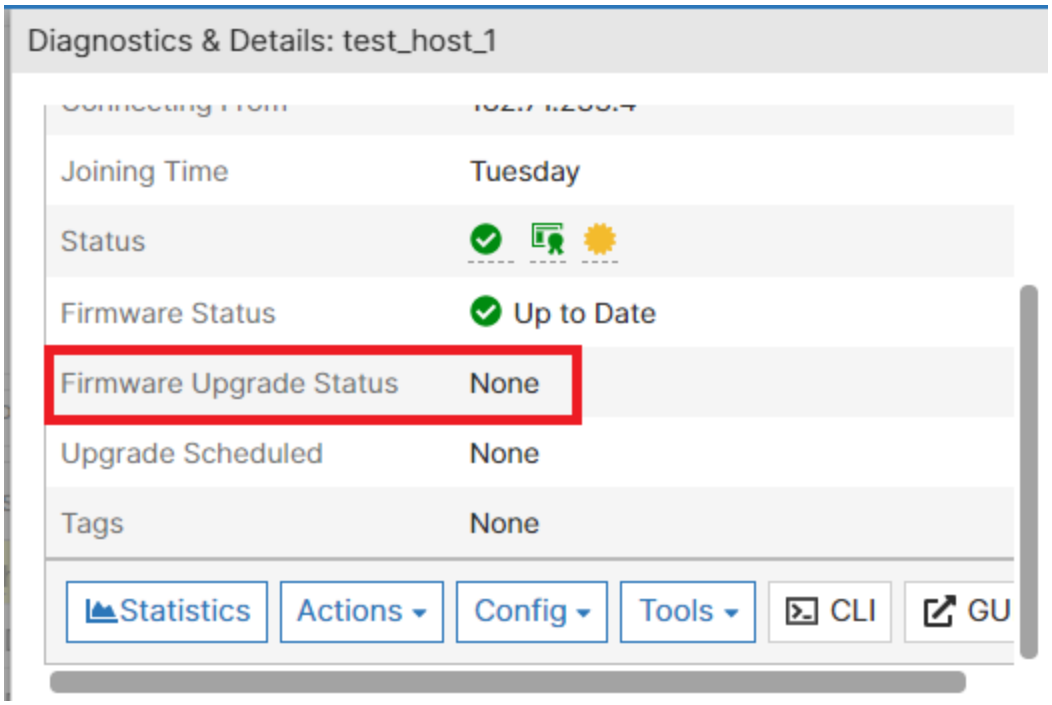
To specify when the FortiSwitch firmware will be upgraded:

1. Go to *Configuration* > *Scheduled Upgrade*.
2. Select *Add Scheduled Upgrade*.



3. Select *Tags*, *Switches*, or *Models*.

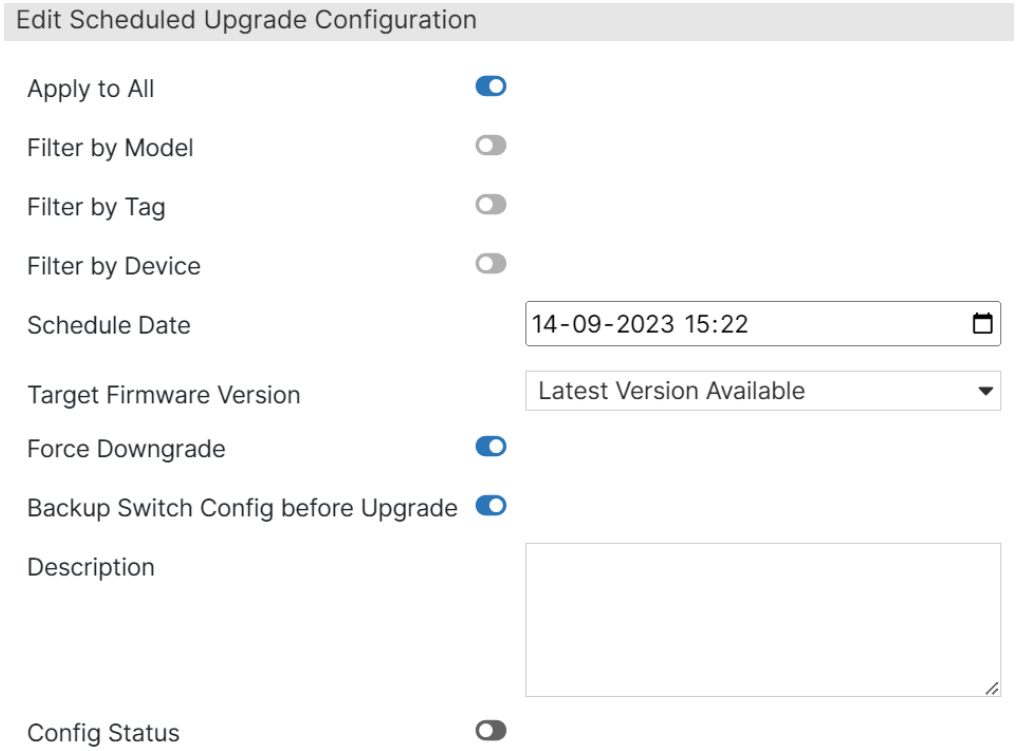
4. Select to choose one or more switch tags or choose one or more FortiSwitch units.
   NOTE: Only switches of the same model as the selected firmware image are upgraded.
5. Select the date and time when you want the firmware upgraded.
6. Select the firmware version to apply.
   The available firmware images and the latest version are listed. Click the help link, *Release Notes*, to learn about the available versions.
7. Select *Force Downgrade* to forcefully downgrade newly deployed FortiSwitches.
8. The **Backup Switch Config before Upgrade** option enables you to backup the FortiSwitch configuration prior to the upgrade.
9. Select *Ok*.
   The scheduled upgrade is listed on the Scheduled Upgrade pane and the Scheduled Upgrade Status pane. You can also view the upgrade status on the **Diagnostics & Details** panel in the FortiSwitch status.



Editing a scheduled upgrade

To edit a scheduled upgrade:

1. Select a scheduled upgrade configuration row and click **Edit**.



2. Make your changes in the **Edit Scheduled Upgrade Configuration** dialog box.
3. Select *Ok* to apply your changes.

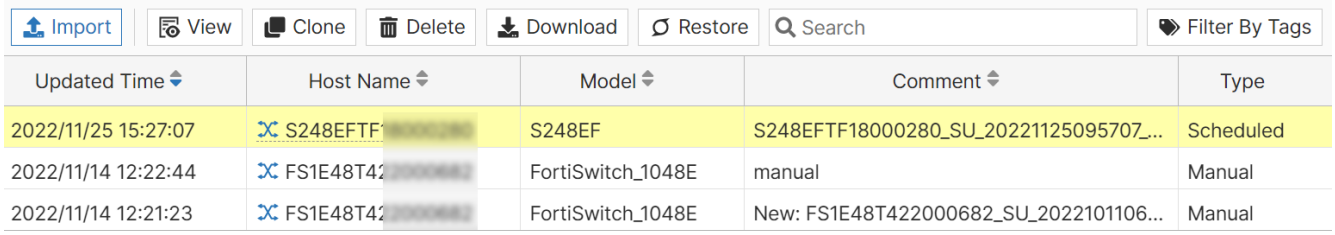
Deleting a scheduled upgrade

To delete a scheduled upgrade:

1. Select the scheduled upgrade configuration row and click **Delete**.
2. Select *Yes* to delete the scheduled upgrade.

Configuration Backup/Restore

The **Configuration Backup/Restore** pane allows you to edit an imported configuration file and to manage saved configuration files.



To find a specific model, host name, or comment, enter part or all of the search item in the Search field.

Note: Only 7 scheduled backup files are retained per device.

To backup a configuration file, see section Backing up the FortiSwitch configuration to FortiLAN Cloud on page 166and to schedule a backup, see section Network on page 223

You can perform the following tasks from the Config Backup/Restore pane:

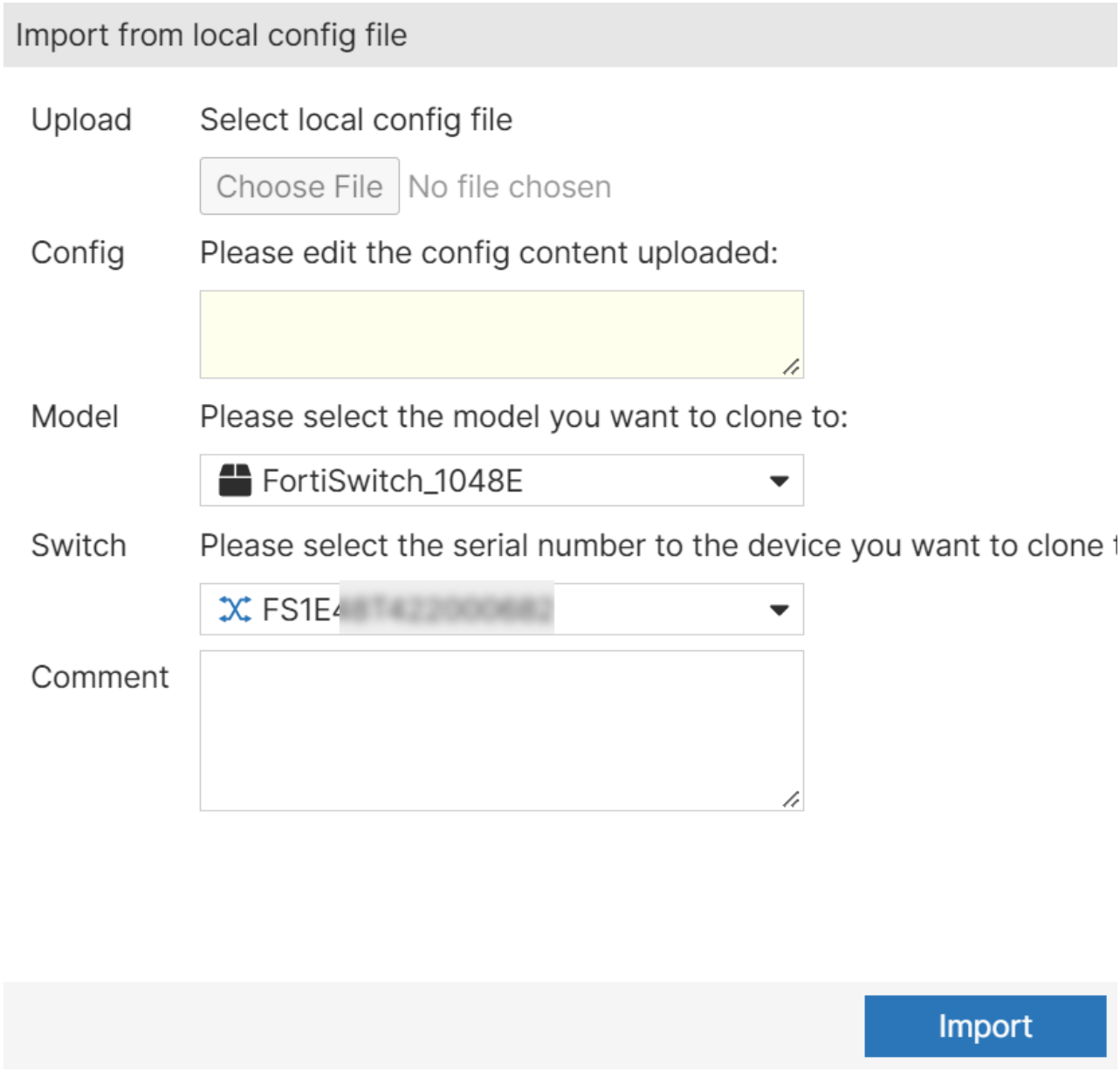
- Importing and editing a configuration file
- Viewing a configuration file
- Cloning a configuration file on page 196
- Deleting a configuration file on page 197
- Downloading a configuration file to your computer
- Restoring a configuration file to a FortiSwitch unit on page 198

Importing and editing a configuration file

After you download the configuration file from one FortiSwitch unit, you can then import and edit it.

To import and edit a configuration file:

1. Select *Import*.



2. Select *Choose File*, navigate to the downloaded configuration file, and select *Open*.
3. If you want to edit the configuration file, enter your changes.
4. If you want to use the configuration file on a different FortiSwitch model, select the FortiSwitch model from the drop-down list.
5. If you want to use the configuration file on a different FortiSwitch unit, select the FortiSwitch serial number from the drop-down list.
6. Enter a description of your changes.
7. Select *Import*.
   The edited configuration file is listed in the Config Backup/Restore pane.

Viewing a configuration file

To open a configuration file, select a configuration file and click **View**.

Details of config command

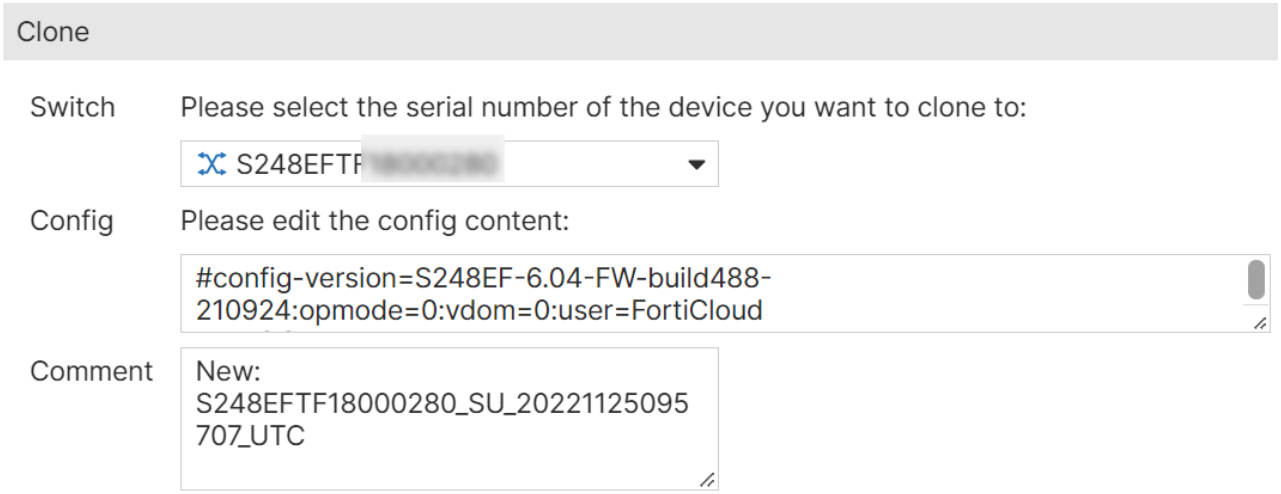
```
#config-version=S248EF-6.04-FW-build488-210924:opmode=0:vdom=0:user=FortiCloud
#conf_file_ver=4463562920390902504
#buildno=0488
#global_vdom=1
config system global
    set 802.1x-ca-certificate "Fortinet_802.1x_CA"
    set 802.1x-certificate "Fortinet_802.1x"
    set admin-concurrent enable
    set admin-https-pki-required disable
    set admin-https-ssl-versions tlsv1-1 tlsv1-2 tlsv1-3
    set admin-lockout-duration 60
    set admin-lockout-threshold 3
    set admin-port 80
    set admin-scp disable
    set admin-server-cert "Fortinet_Firmware"
    set admin-sport 443
    set admin-ssh-grace-time 120
    set admin-ssh-port 22
    set admin-ssh-v1 disable
    set admin-telnet-port 23
    set admintimeout 5
    set alertd-relog disable
    set allow-subnet-overlap disable
    set arp-timeout 180
```

Cloning a configuration file

When you clone a configuration file from one FortiSwitch unit, you can edit the clone and then apply it on a different FortiSwitch unit.

To clone a configuration file:

1. Select the configuration file that you want to clone and click **Clone**.

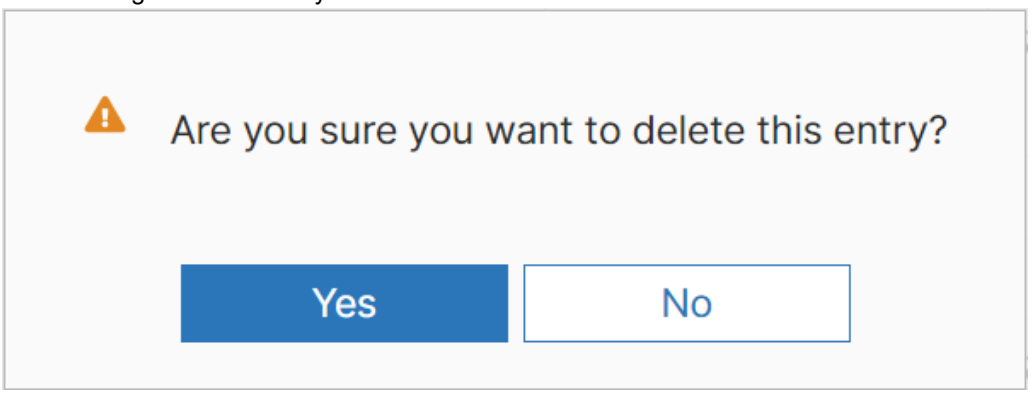


2. Select the serial number of the FortiSwitch unit that you want to use the edited configuration file on.
3. Make the changes to the configuration file.
4. Enter a description of your changes.
5. Select *Ok*.
   The clone is listed in the Config Backup/Restore pane.

Deleting a configuration file

To delete a configuration file:

1. Select configuration file that you want to delete and click **Delete**.



2. Select *Yes* to delete the configuration file.

Downloading a configuration file to your computer

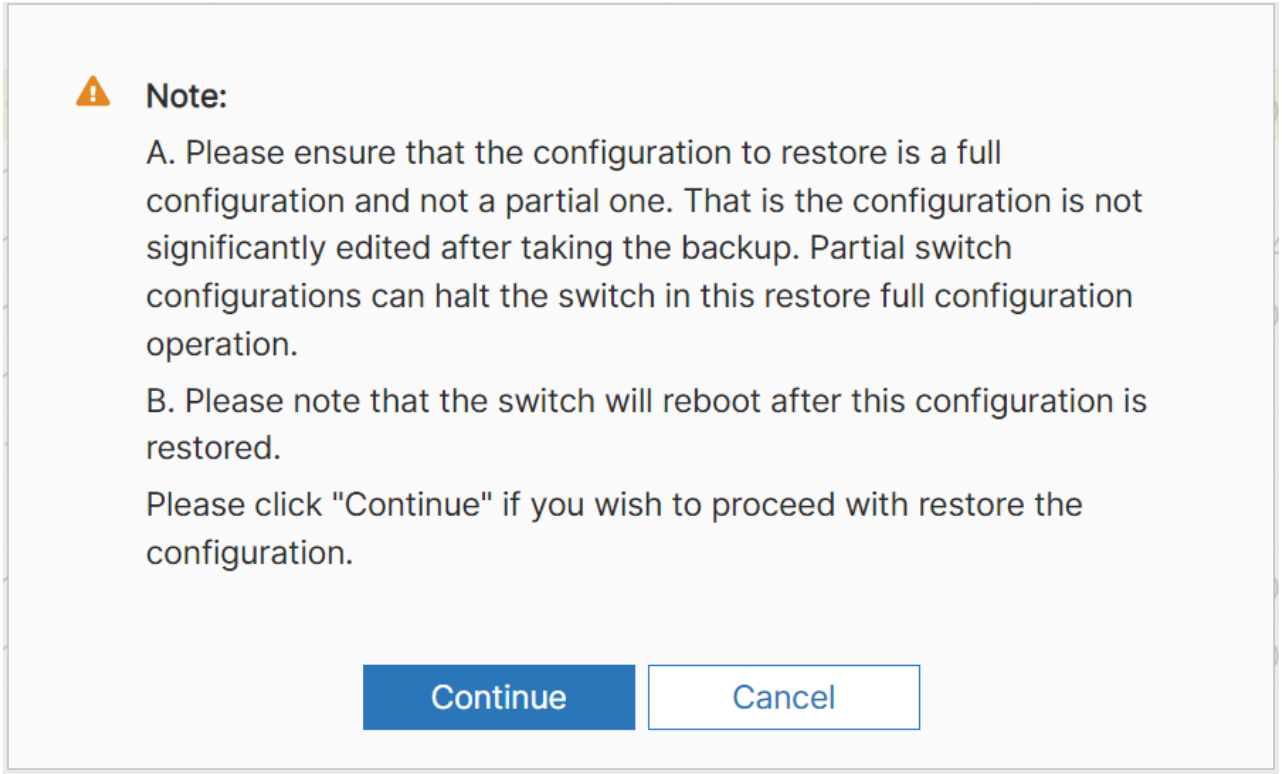
To download a configuration file from FortiLAN Cloud to your computer, select row of the configuration file that you want to download, click **Download**. The configuration file is saved as a `.txt` file.

Restoring a configuration file to a FortiSwitch unit

You can apply a configuration file that you saved to FortiLAN Cloud to a FortiSwitch unit.

To apply a configuration:

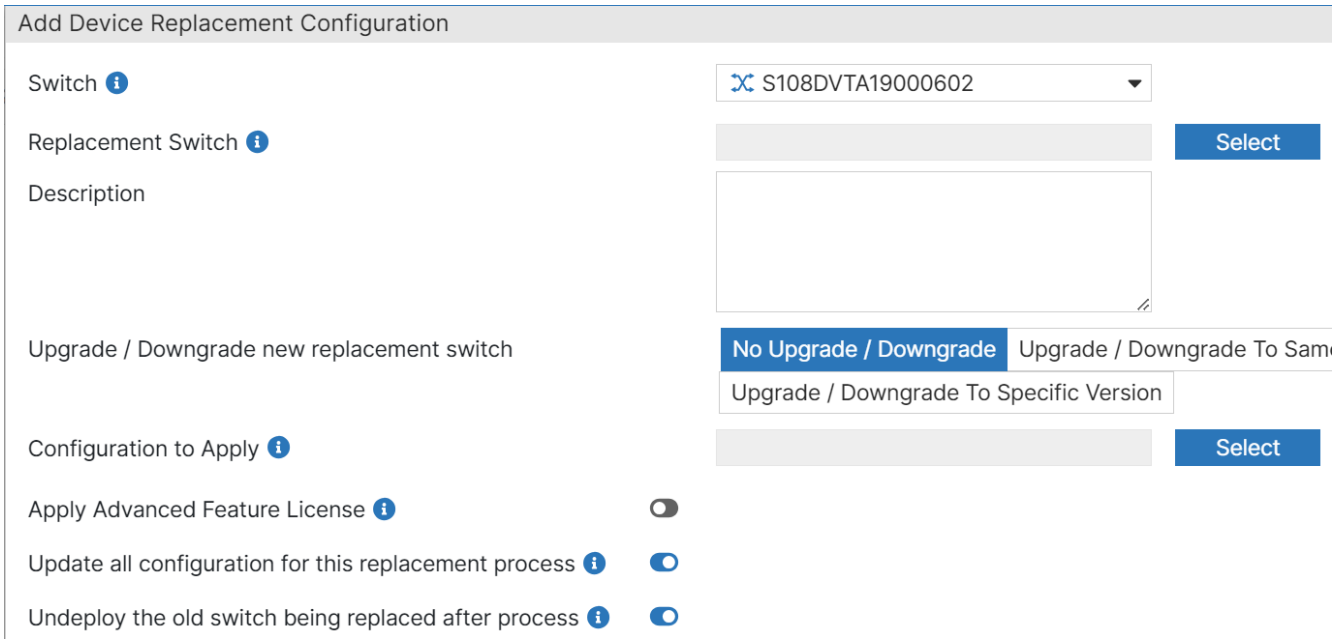
1. Select the row of the configuration that you want to apply and click **Restore**.



2. Select *Continue* to apply the configuration file to the host name in the same row as the configuration file.

Device Replacements

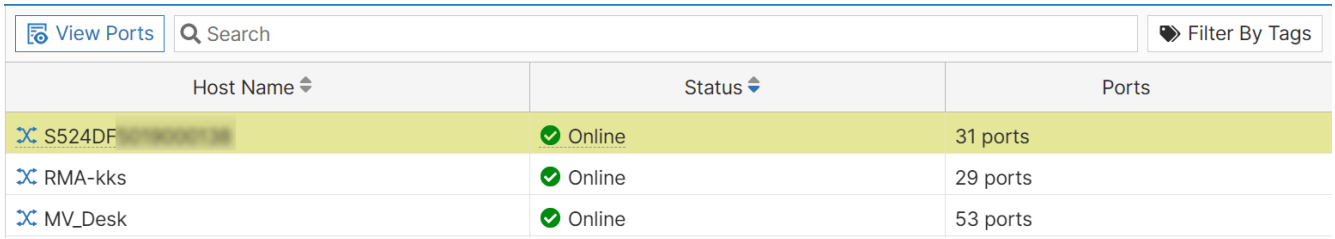
You can replace FortiSwitch inventory devices just as the deployed devices, and the replacement FortiSwitch is not required to be online, when the replacement process is implemented. Navigate to **Switch > Configuration > Device Replacements** to create a FortiSwitch replacement configuration entry. A maximum of 255 entries (per network) can exist. When such a replacement entry is created, the replacement process deploys the FortiSwitch (in case of inventory) and initiates the firmware upgrade and CLI configuration transfer immediately.



- **Switch** - The FortiSwitch to be replaced.
- **Replacement Switch** - The replacement FortiSwitch that can be a deployed or an inventory device with an advanced management license.
- **Upgrade / Downgrade new replacement switch** - Select the version preference for the replacement FortiSwitch.
- **Configuration to Apply** - The configuration to apply to the replacement FortiSwitch. Ensure that at least one configuration backup is available from the FortiSwitch being replaced. If not, then use the option to backup the full configuration. The configuration selected here alone is applied to the replacement FortiSwitch.
  Note: The ZTC GUI configuration is not applied.
- **Apply Advanced Feature License** - The advanced feature license is applied to the replacement FortiSwitch. You are required to proved the license key.
- **Update all configuration for this replacement process** - If enabled, then all configurations will have the serial number of the replacing FortiSwitch, wherever the replaced FortiSwitch serial number is present.
- **Undeploy This Switch after Process** - If enabled, then the FortiSwitch being replaced is un-deployed and all configurations are deleted.

Ports

The Ports pane allows you to change the administrative status and PoE status of one or more FortiSwitch ports. See Configuring FortiSwitch ports on page 200.



To view ports associated with a FortiSwitch unit, click **View Ports**.

To find a specific FortiSwitch unit, enter part or all of the host name in the Search field.

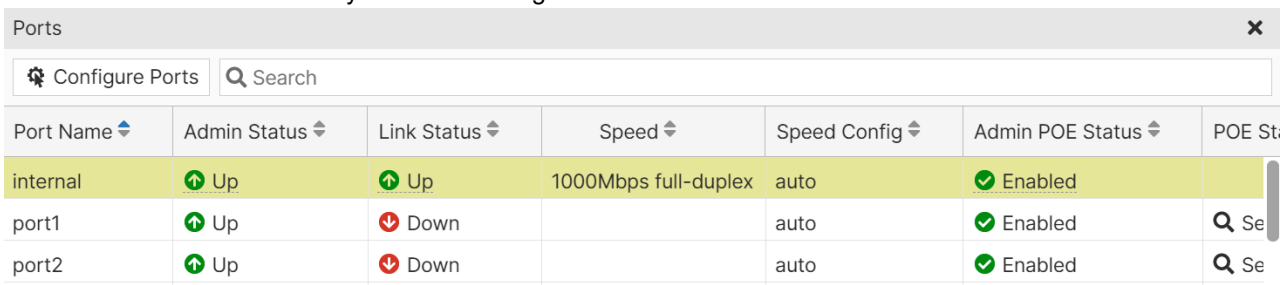
To filter the list of FortiSwitch units by tag, select **Filter By Tags** and the tag to filter with. If you select multiple tags to filter with, the results are FortiSwitch units that are tagged with one or more of the selected tags.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that contain the search term *and* are tagged with the selected tag.

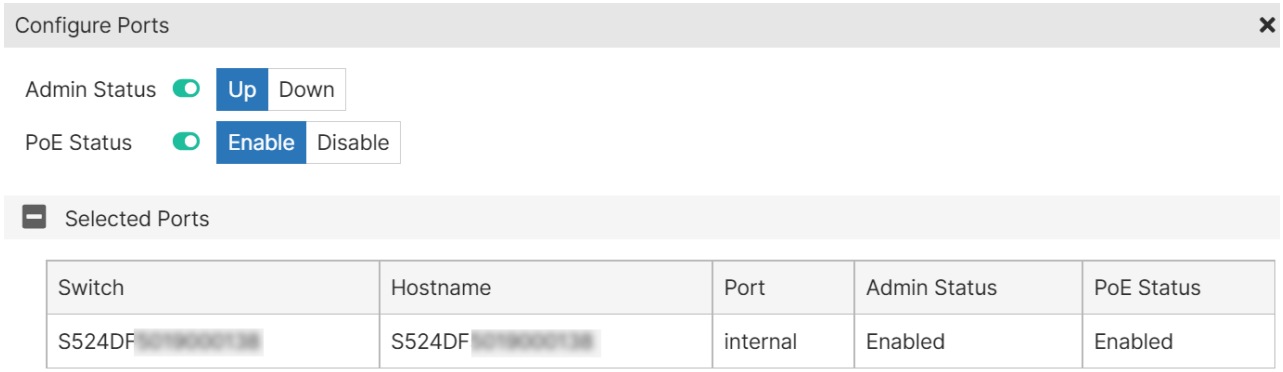
Configuring FortiSwitch ports

To configure FortiSwitch ports:

1. Select the FortiSwitch unit that you want to configure and click **View Ports**.



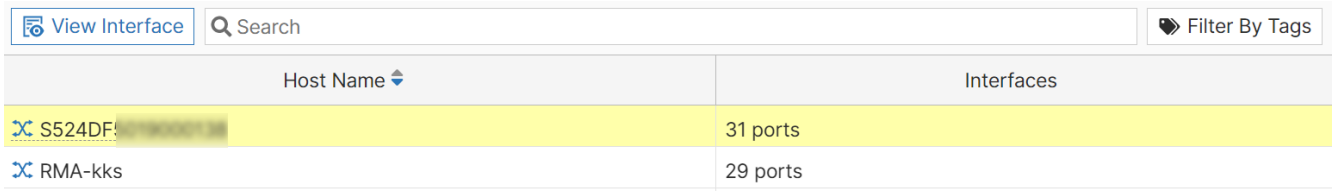
2. Select the port that you want to change and click **Configure Ports**.



3. Select *up* or *down* in the Admin Status drop-down list.
4. Select *enable* or *disable* in the PoE Status drop-down list.
   NOTE: If you select ports from more than one FortiSwitch unit, the PoE Status drop-down list is not displayed.
5. Select *Ok* to apply your changes.

Interfaces

The Interfaces pane lists all interfaces for each managed FortiSwitch unit.



To find a specific FortiSwitch unit, enter part or all of the host name in the Search field.

To filter the list of FortiSwitch units by tag, select **Filter By Tags** and the tag to filter with. If you select multiple tags to filter with, the results are FortiSwitch units that are tagged with one or more of the selected tags.

You can use the Search field and the Filter with Tags field together to find host names that contain the search term *and* are tagged with the selected tag.

Select the host name and click **View Interface** to see more information about each FortiSwitch unit.

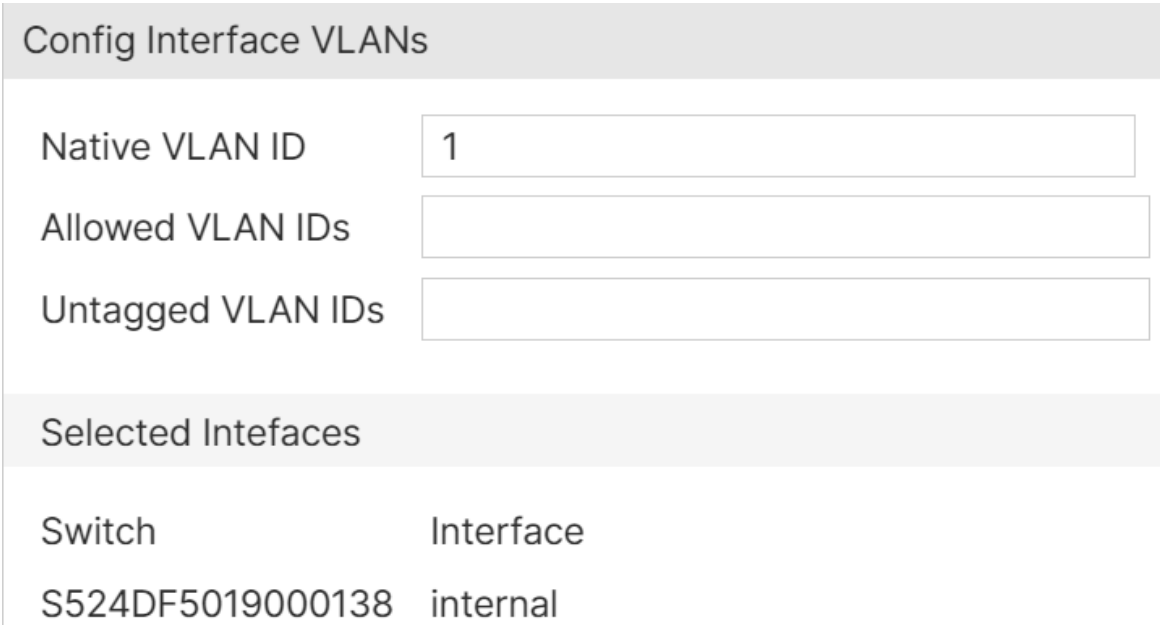
You can perform the following tasks from the Interfaces pane:

- Configuring interface VLANs
- Creating a trunk
- Creating a packet capture profile
- Editing the port security

Configuring interface VLANs

To configure an interface VLAN:

1. Select a FortiSwitch unit that you want to configure and click **View Interface**.
2. Select the interfaces that you want to configure and click **Config Interface VLANs**.



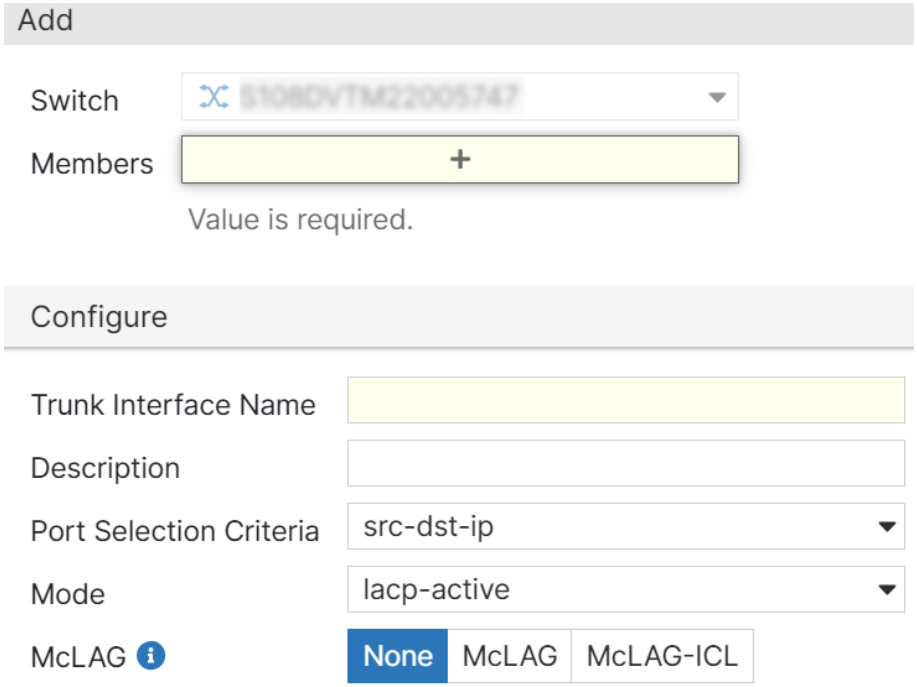
3. Enter the VLAN identifiers for the native VLAN, allowed VLANs, and untagged VLANs. Separate the identifiers with a comma.
4. Select *Ok* to apply your changes.

Creating a trunk

NOTE: You cannot include an internal interface or a port that is already a member of another trunk in a new trunk.

To create a trunk:

1. Select a FortiSwitch unit that you want to configure and click **View Interface**.
2. Select the interfaces that you want to include in the trunk and click **Create Trunk**.



3. Enter a name for the new trunk in the Trunk Interface Name field.
   Avoid using special characters, such as <, >, (,), #, ', and ".
4. (Optional) Add a description of the trunk in the Description field.
5. Select the port selection criteria:
   - *dst-ip*—destination IP address
   - *dst-mac*—destination MAC address
   - *src-dst-ip*—source or destination IP address
   - *src-dst-ip-xor16*—source and destination IP address
   - *src-dst-mac*—source or destination MAC address
   - *src-ip*—source IP address
   - *src-mac*—source MAC address
6. Select the mode:
   - *lacp-active*—active LACP
   - *lacp-passive*—passive LACP
   - *static*—static link aggregation
7. Select *McLAG* if you want to create an MCLAG.
   You cannot select both *McLAG* and *McLAG-ICL* for a trunk.
8. Select *McLAG-ICL* if you are creating an ICL for an MCLAG.
   Only one MCLAG-ICL trunk can be configured for each managed FortiSwitch unit. You cannot select both *McLAG* and *McLAG-ICL* for a trunk.
9. Select *Ok*.

Creating a packet capture profile

When troubleshooting networks, you can look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture is also called a network tap, packet sniffing, or logic analyzing.

The maximum number of packet-capture profiles and the RAM disk size allotted for packet capture are different for the various platforms:

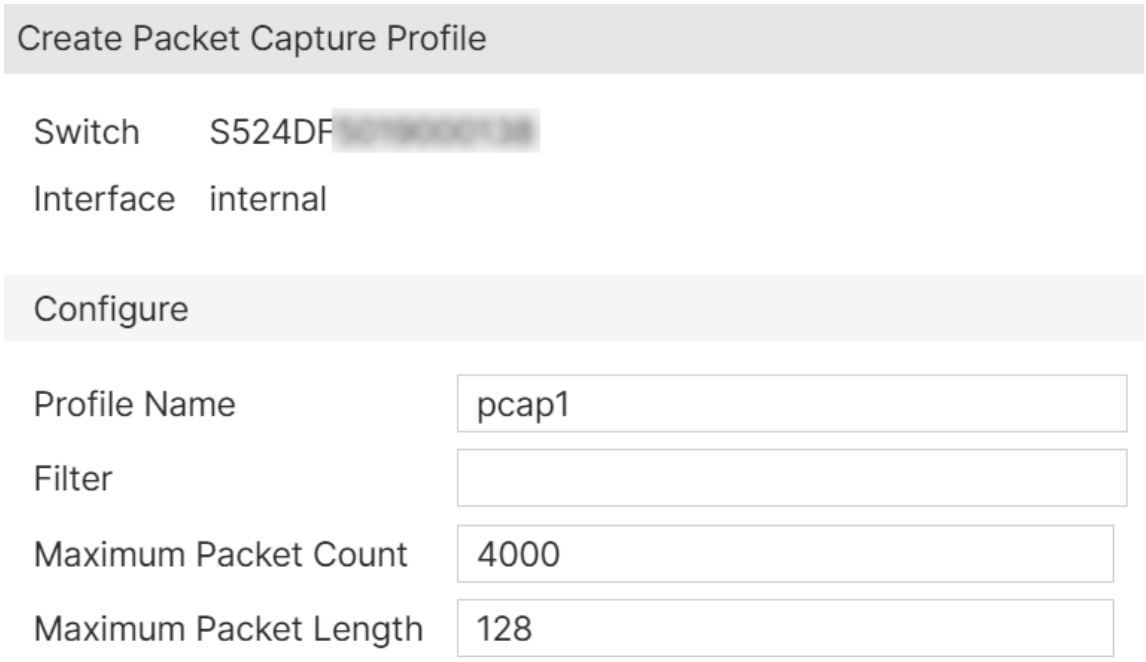
Platform	Maximum number of profiles	RAM disk size in MB
2xx	8	50
4xx	16	75
5xx	16	100
1xxx	16	100
3xxx	16	100

The maximum number of packet capture files is equal to license points. When the number of existing packet capture files has reached the maximum, you need to delete one or more existing packet capture files before starting a packet capture.

Packet capture files are kept for 7 days. For licensed users, there is a 60-day grace period before the packet capture files are deleted.

To create a packet capture profile:

1. Select a FortiSwitch unit that you want to investigate and click **View Interface**.
2. Select the interface and click **Create Packet Capture Profile**.



1. Enter a name for the new packet capture profile in the Configuration Name field.
   Avoid using special characters, such as <, >, (,), #, ', and ".

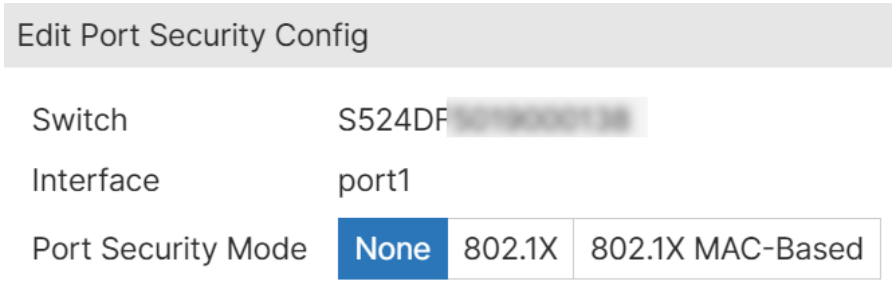
2. Optional. Enter a filter to reduce the number of packets captured.
   The filter uses flexible logic. For example, if you want packets using UDP port 1812 between hosts named `forti1` and either `forti2` or `forti3`, enter the following:
   `udp and port 1812 and host forti1 and \( forti2 or forti3 \)`
3. Enter the maximum number of packets to collect. The maximum number of packets that can be captured depends on the RAM disk size.
4. Enter the maximum packet length in bytes to capture on the interface. The range of values is 64-1534 bytes.
5. Select *Ok*.
   Go to *Configuration* > *Packet Capture Profiles* to see the new packet capture profile.

Editing the port security

You can add port security with 802.1x port-based or MAC-based authentication.

To change the port security:

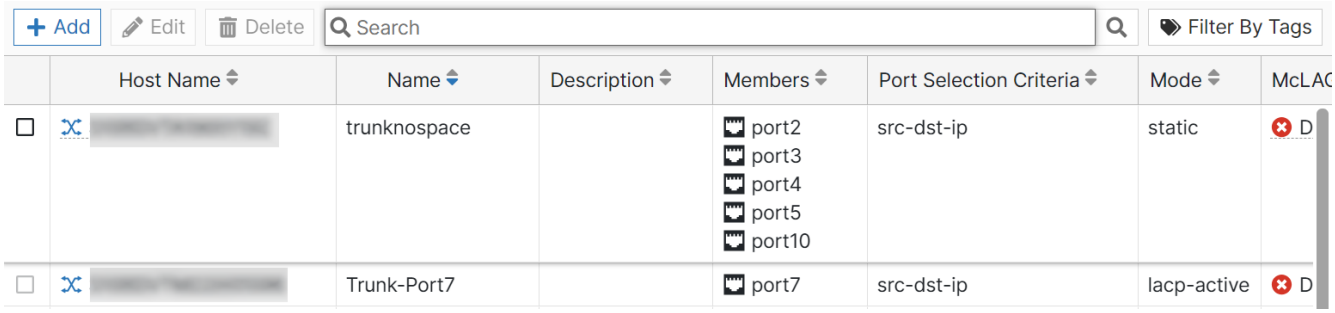
1. Select a FortiSwitch unit and click **View Interface**.
2. Select the interface and click **Edit Port Security**.



3. Select *802.1X* for port-based authentication or select *802.1X MAC-Based* for MAC-based authentication.
4. Select *MAC Auth Bypass* to allow the system to use the device MAC address as the user name and password for authentication.
5. If the RADIUS authentication server does not support EAP-TLS, clear the *EAP Pass-Through Mode* checkbox.
6. For phone and PC configuration only, clear the *Frame VLAN Apply* checkbox to preserve the native VLAN when the data traffic is expected to be untagged.
7. Select *Open Authentication* to enable open authentication (monitor mode) on this interface. Use the monitor mode to test your system configuration for 802.1x authentication. You can use monitor mode to test port-based authentication, MAC-based authentication, EAP pass-through mode, and MAC authentication bypass. After you enable monitor mode, the network traffic will continue to flow, even if the users fail authentication.
8. Select *Guest VLAN* if you want to assign a VLAN to unauthorized users. If you select *Guest VLAN*, enter the guest VLAN identifier in the *Guest VLAN ID* field and enter the number of seconds for an unauthorized user to have access as a guest before authorization fails in the *Guest Auth Delay* field.
9. Select *Auth Fail VLAN* if you want to assign a VLAN to users who attempted to authenticate but failed to provide valid credentials. If you select *Auth Fail VLAN*, enter the VLAN identifier in the *Auth Fail VLAN ID* field.
10. If you want to use the RADIUS-provided reauthentication time, select *RADUS Session Timeout*.
11. Click in the *Security Groups* field to select a security group. You can select multiple security groups.
12. Select *Ok* to apply your changes.

Trunk/Link Aggregation

The Trunk/Link Aggregation pane lists all trunks that have been configured.



To find a specific trunk, enter part or all of the name in the Search field.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that contain the search term *and* are tagged with the selected tag.

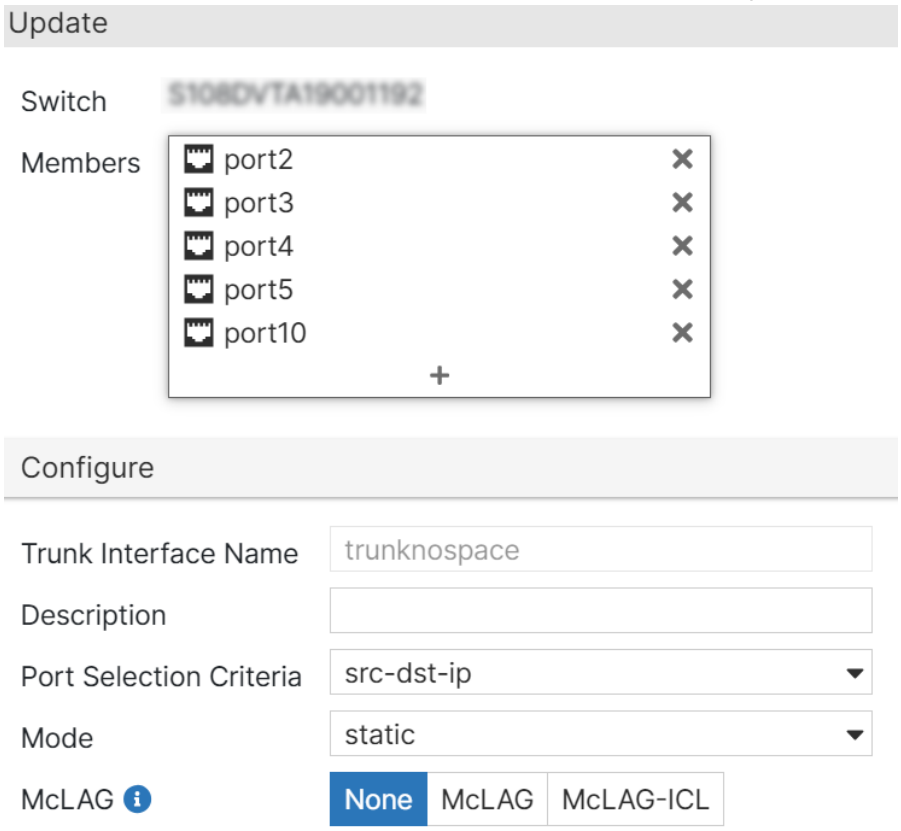
To filter the list of FortiSwitch units by tag, click **Filter By Tags**. If you select multiple tags to filter with, the results are FortiSwitch units that are tagged with one or more of the selected tags.

You can perform the following tasks from the Trunk/Link Aggregation pane:

- Creating a trunk
- Editing a trunk
- Deleting a trunk

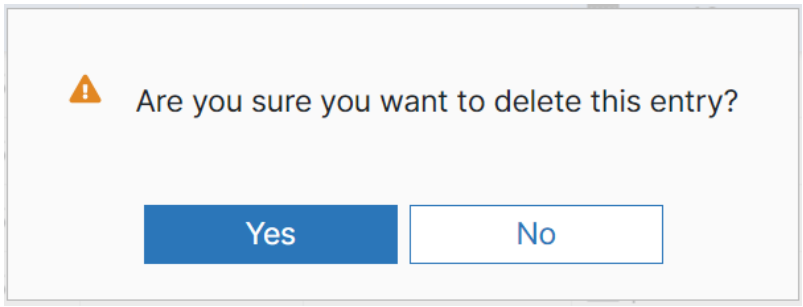
Editing a trunk

To edit a trunk, select the row of the trunk and click **Edit**. Make the updates and click **Ok**.



Deleting a trunk

To delete a trunk, select the row of the trunk and click **Delete**. Select *Yes* to delete the trunk.



VLANs

The VLANs pane lists the VLANs configured on each FortiSwitch unit.

To update the list of VLANs, select *Refresh*.

To find a specific FortiSwitch unit, enter part or all of the host name in the Search field.

You can use the Search field and the Filter with Tags field together to find host names that contain specific characters *and* are tagged with the selected tag.

To filter the list of host names by switch tag, click **Filter By Tags** and select the tag to filter with. If you select multiple tags to filter with, the results are FortiSwitch units that are tagged with one or more of the selected tags.

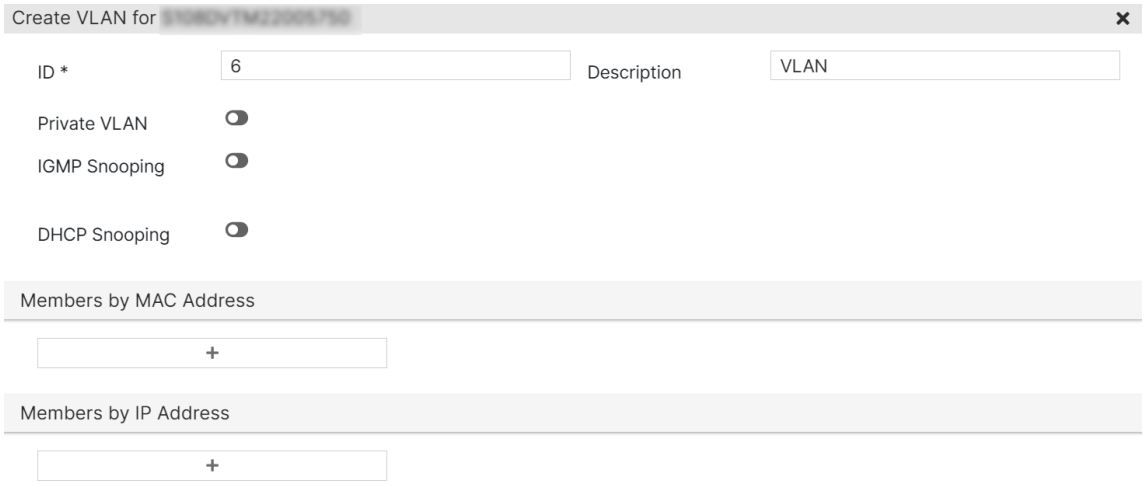
Select a row and click **View VLANs** to see which VLANs are configured on each FortiSwitch unit.

You can perform the following tasks from the VLANs pane:

- Creating a VLAN
- Editing a VLAN configuration
- Saving a VLAN configuration as a VLAN template
- Deleting a VLAN

Creating a VLAN

You can create a VLAN or private VLAN, configure IGMP snooping and DHCP snooping, and add VLAN members by MAC address or IP address.



1. Go to *Configuration* > *VLANs*.
2. Click **Add** and enter a number to identify the VLAN.
3. Add a description of the VLAN.
4. Enable or disable whether this VLAN is a private VLAN.

5. If you want to use IGMP snooping on the VLAN:
   a. Select the *Enable* checkbox.
   b. If you want to use IGMP proxy, select the *Enable* checkbox.
   c. Select + to add an IGMP static group, enter the name of the group, enter the multicast address, and enter the members of the group.
6. If you want to use DHCP snooping on the VLAN:
   a. Select the *Enable* checkbox.
   b. If you want the system to verify that the source MAC address in the DHCP request from an untrusted port matches the client hardware address, enable *DHCP Snooping Verify MAC Address*.
   c. If you want to include option-82 data in the DHCP request, enable *DHCP Snooping Option 82*.
   d. If you want dynamic ARP inspection on the VLAN, enable *Arp Inspection*.
   e. Select + to add a DHCP server in the allowed server list and then enter the server name and IP address.
7. To add VLAN members by MAC address, select + and then enter a description and the MAC address.
8. To add VLAN members by IP address, select + and then enter a description, IP address, and netmask.
9. Select *Save*.

Editing a VLAN configuration

Select a FortiSwitch row with the associated VLANs and click **View VLANs**. Selected the VLAN and click **Edit**, make the changes and click *Save*.

Saving a VLAN configuration as a VLAN template

You can save a VLAN configuration to FortiLAN Cloud and then apply it to one or more FortiSwitch units.

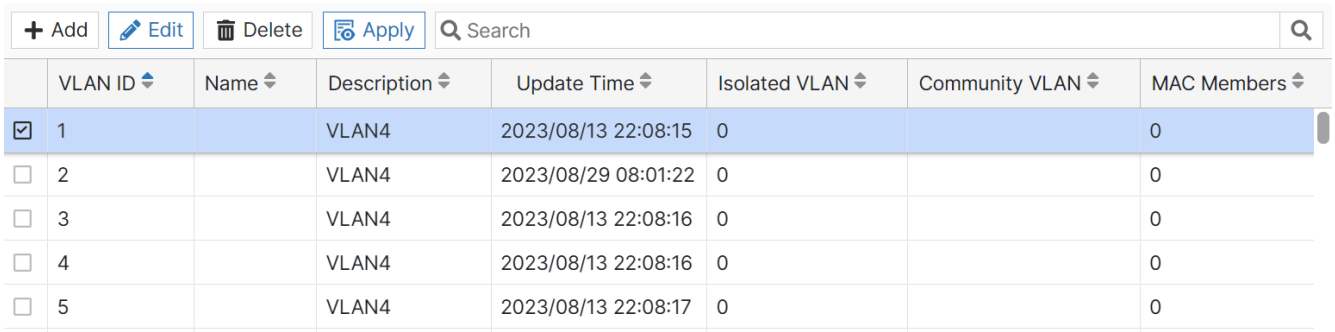
To save a VLAN configuration as a VLAN template, select the row of the FortiSwitch of the associated VLAN configuration click **View VLANs**. Select the VLAN and click **Save As VLAN Template**. The new VLAN template is listed on the *Configuration* > *VLAN Templates* page.

Deleting a VLAN

To delete a VLAN, select the row of the FortiSwitch and click **View VLANs**. Select a VLAN and click **Delete**.

VLAN Templates

The VLAN Templates pane lists the available VLAN templates that can be applied to FortiSwitch units.



	VLAN ID	Name	Description	Update Time	Isolated VLAN	Community VLAN	MAC Members
☑	1		VLAN4	2023/08/13 22:08:15	0		0
☐	2		VLAN4	2023/08/29 08:01:22	0		0
☐	3		VLAN4	2023/08/13 22:08:16	0		0
☐	4		VLAN4	2023/08/13 22:08:16	0		0
☐	5		VLAN4	2023/08/13 22:08:17	0		0

Use the Local Time Zone/UTC slider to control which time zone is displayed in the VLAN Templates page.

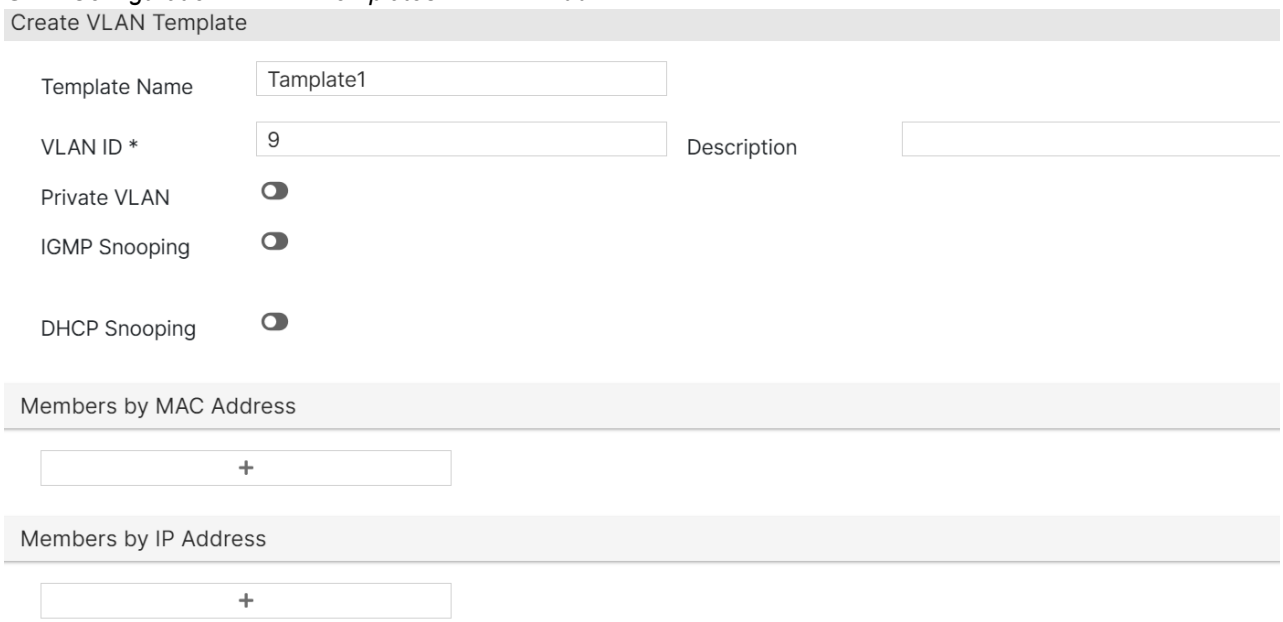
You can perform the following tasks from the VLAN Templates pane:

- Creating a VLAN template
- Editing a VLAN template
- Applying a VLAN template
- Deleting a VLAN template

Creating a VLAN template

You can create a VLAN or private VLAN, configure IGMP snooping and DHCP snooping, and add members by MAC address or IP address.

1. Go to *Configuration* > *VLAN Templates* and click *Add*.

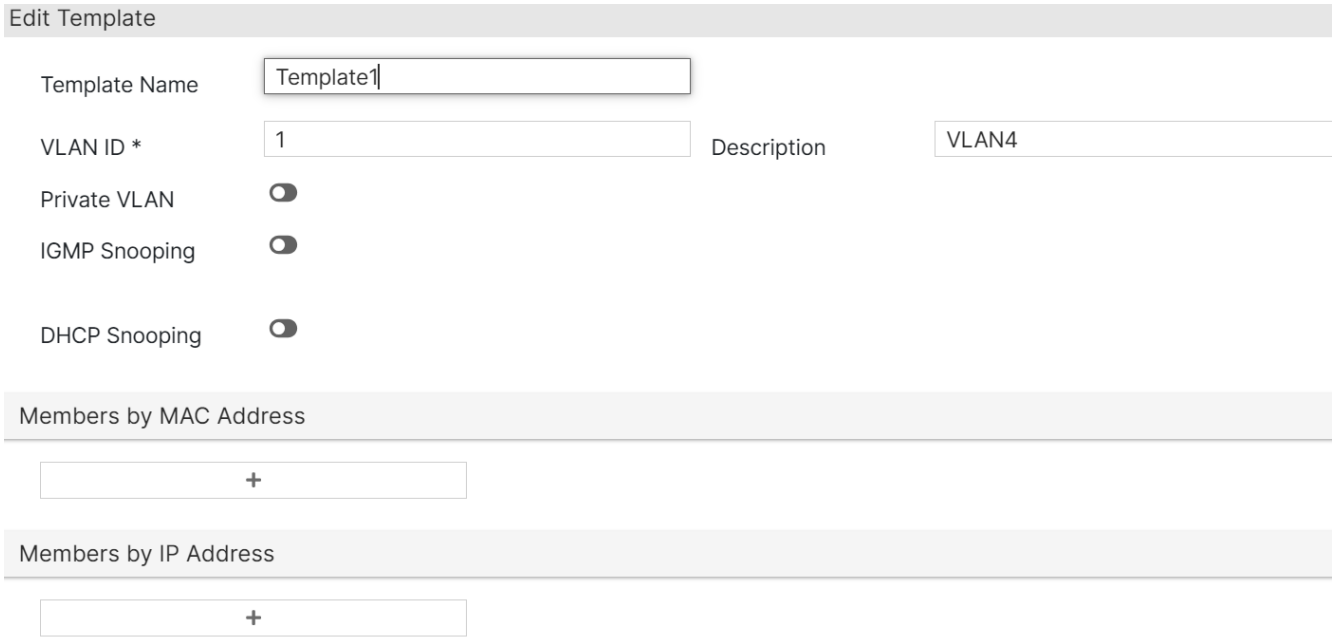


2. Optional. Enter a name for the template.
3. Required. Enter a number to identify the VLAN.
4. Add a description of the VLAN.
5. Enable or disable whether this VLAN is a private VLAN.
6. If you want to use IGMP snooping on the VLAN:
7. **a.** Select the *Enable* checkbox.
   b. If you want to use IGMP proxy, select the *Enable* checkbox.
   c. Select + to add an IGMP static group, enter the name of the group, enter the multicast address, and enter the members of the group.
8. If you want to use DHCP snooping on the VLAN:
   a. Select the *Enable* checkbox.
   b. If you want the system to verify that the source MAC address in the DHCP request from an untrusted port matches the client hardware address, enable *DHCP Snooping Verify MAC Address*.
   c. If you want to include option-82 data in the DHCP request, enable *DHCP Snooping Option 82*.
   d. If you want dynamic ARP inspection on the VLAN, enable *Arp Inspection*.
   e. Select + to add a DHCP server in the allowed server list and then enter the server name and IP address.

9. To add VLAN members by MAC address, select + and then enter a description and the MAC address.
10. To add VLAN members by IP address, select + and then enter a description, IP address, and netmask.
11. Select *Save*.

Editing a VLAN template

To edit a VLAN template, select the row of the VLAN template and click **Edit**. Make the updates and click *Save*.

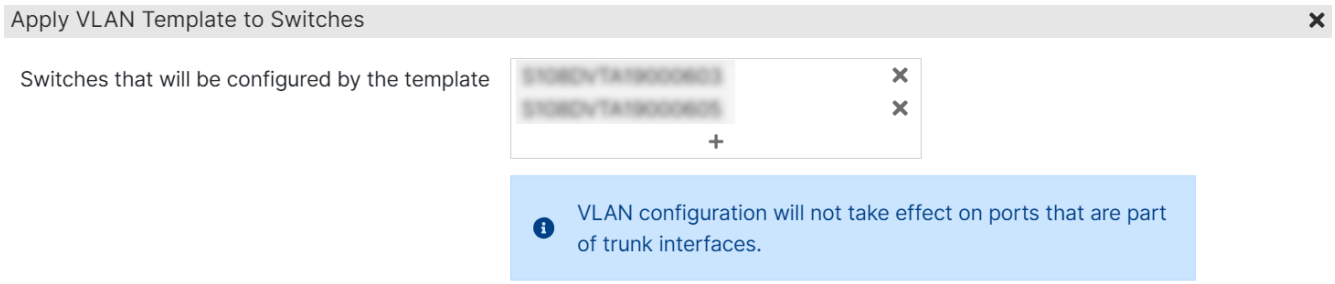


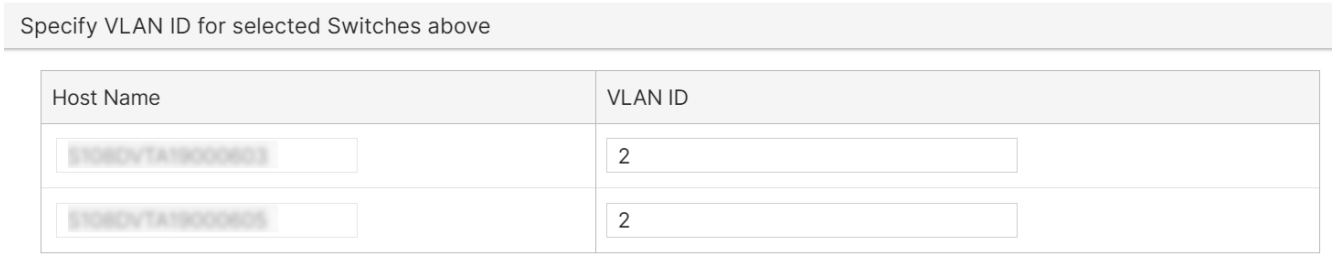
Applying a VLAN template

You can apply a VLAN template to one or more FortiSwitch units.

To apply a VLAN template to one or more FortiSwitch units, select the row of the VLAN template and click **Apply**. Select the FortiSwitches and enter the VLAN identifier for each FortiSwitch unit you are applying the VLAN template to. Click

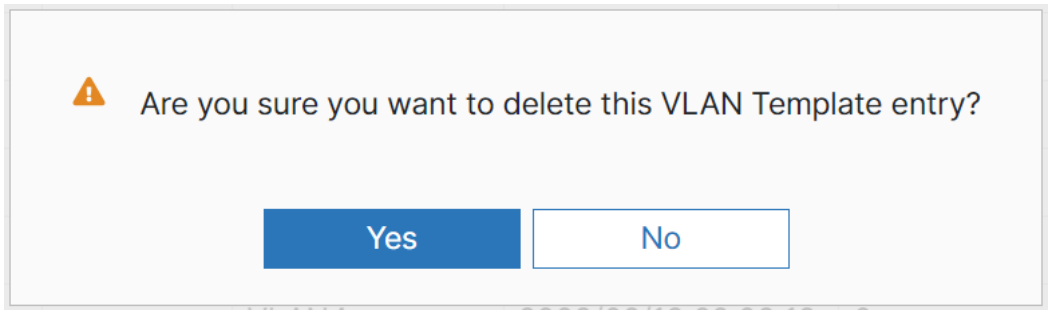
Ok.





Deleting a VLAN template

To delete a VLAN template, select the row of the VLAN template and click **Delete**. Select *Yes* to delete the VLAN template.

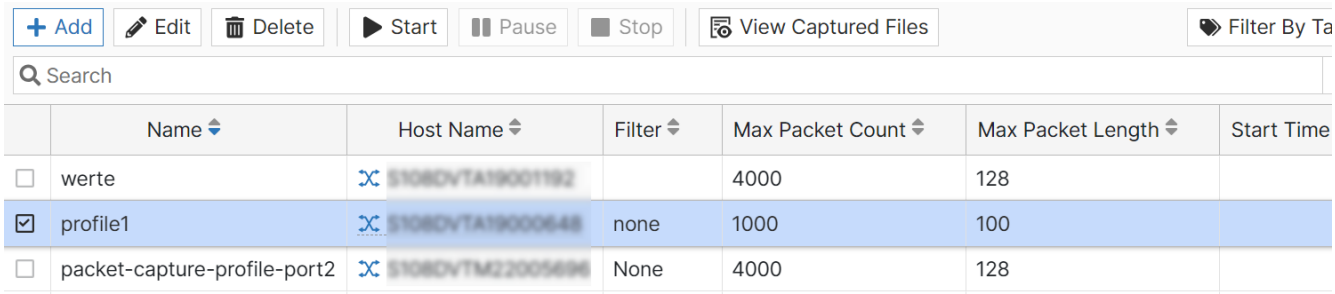


Packet Capture Profiles

The Packet Capture Profiles pane lists the available profiles for packet captures.

Notes:

- The packet-capture feature requires FortiSwitchOS 6.2.2 or later.
- Packet capture profiles are NOT supported on FortiSwitch 1xxE models.



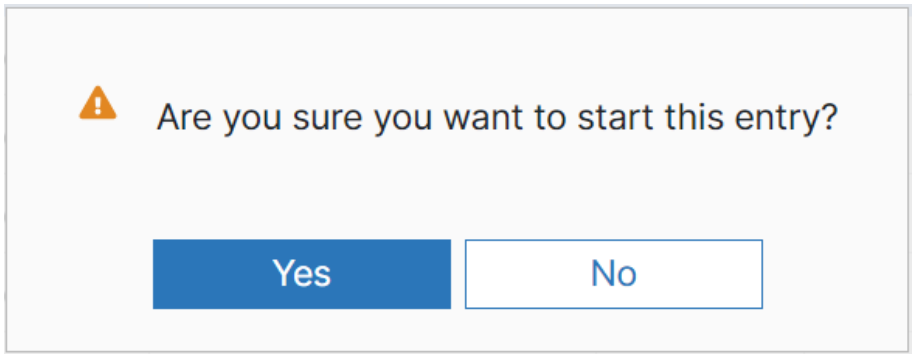
To filter the list of profiles by switch tag, click **Filter By Tags** and select the tag to filter with. If you select multiple tags to filter with, the results are profiles for FortiSwitch units that are tagged with one or more of the selected tags.

You can perform the following tasks from the Packet Capture Profiles pane:

- Creating a packet capture profile
- Starting a packet capture
- Pausing a packet capture
- Stopping a packet capture
- Going to the packet capture file
- Editing a packet capture profile
- Deleting a packet capture profile

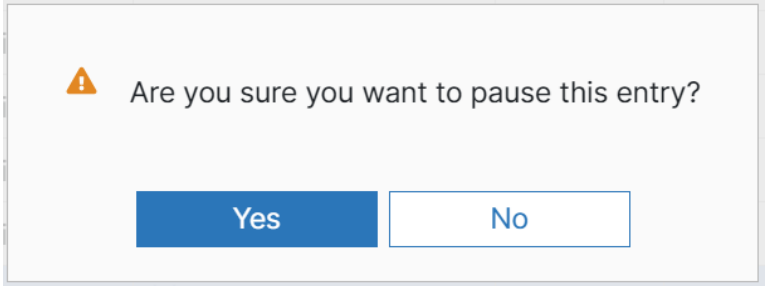
Starting a packet capture

To start a packet capture, select the row of the packet capture profile and click **Start**. Select *Yes* to confirm your action.



Pausing a packet capture

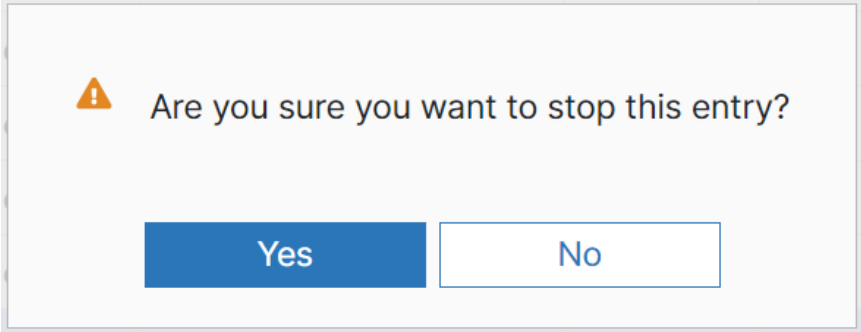
To pause a packet capture, select the row of a packet capture profile and click **Pause**. Select *Yes* to confirm your action.



Stopping a packet capture

To stop a packet capture:

1. Select the row of a packet capture profile and click **Stop**. Select *Yes* to confirm your action. Go to *Monitor* > *Packet Capture Files* to download the saved packet capture file.

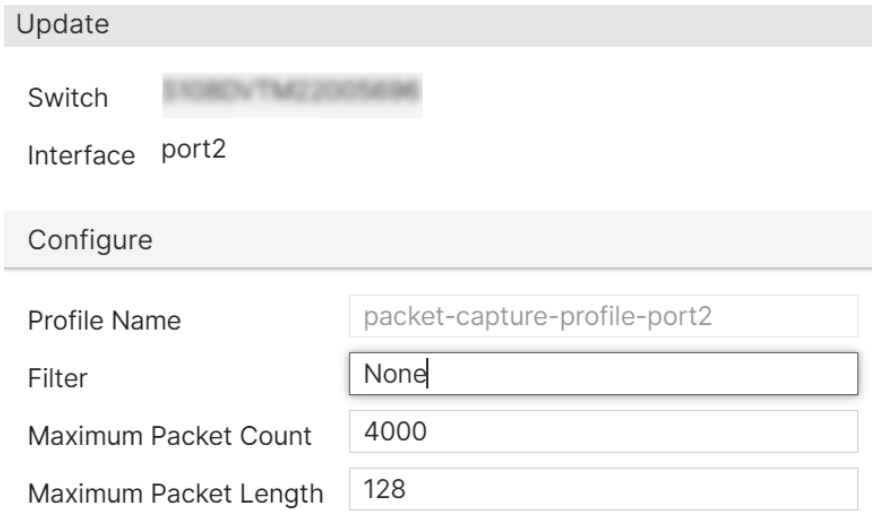


Going to the packet capture file

To go to the packet capture file, select the row of the packet capture profile and click **View Captured Files** to download the associated packet capture file. The `.pcap` file is saved in your Downloads folder.

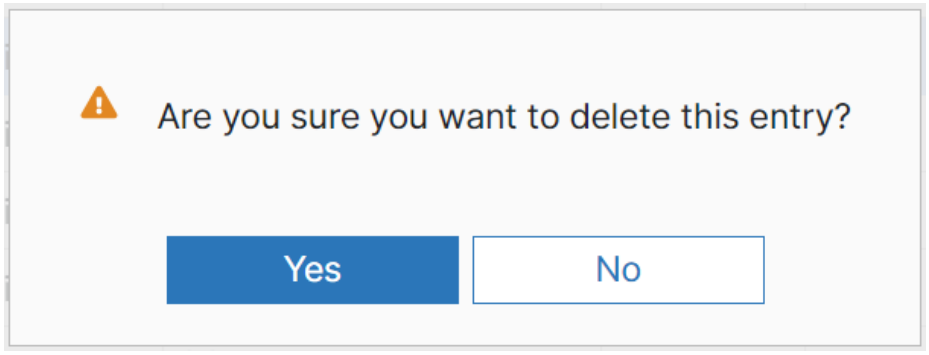
Editing a packet capture profile

To edit a packet capture profile, select the row of the packet capture profile and click **Edit**. Make the changes and click *Save*.



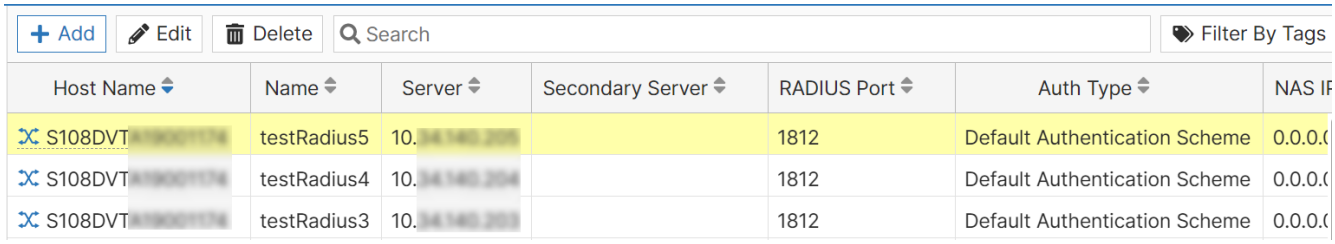
Deleting a packet capture profile

To delete a packet capture profile, select the row of the packet capture profile and click **Delete**. Select *Yes* to delete the profile.



RADIUS Authentication

The RADIUS Authentication pane allows you to configure RADIUS authentication for one or more FortiSwitch units.



To find a specific host name, configuration name, or server IP address, enter part or all of the search item in the Search field.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that use RADIUS authentication *and* are tagged with the selected tag.

To filter the list of configurations by switch tag, select **Filter By Tags** and the tag to filter with. If you select multiple tags to filter with, the results are configurations for FortiSwitch units that are tagged with one or more of the selected tags.

You can perform the following tasks from the Radius Authentication pane:

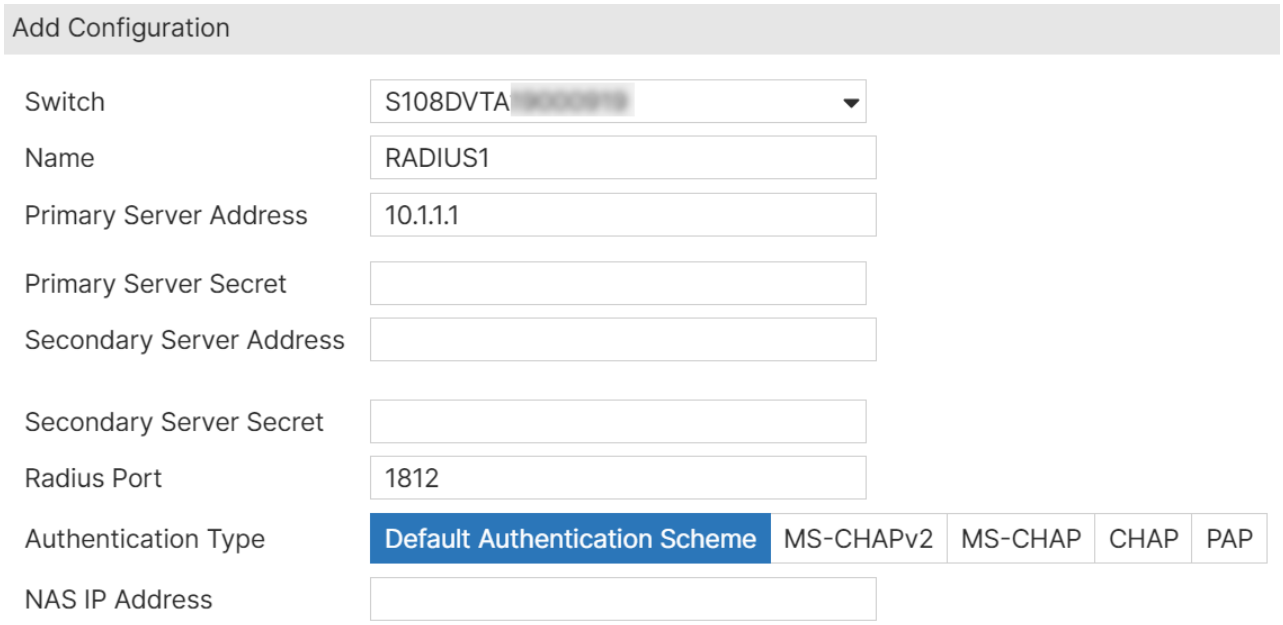
- Creating a RADIUS authentication configuration
- Editing a RADIUS authentication configuration
- Deleting a RADIUS authentication configuration

Creating a RADIUS authentication configuration

You can create a RADIUS authentication configuration for one or more FortiSwitch units.

To create a RADIUS authentication configuration:

1. Go to *Configuration* > *RADIUS Authentication*.
2. Select *Add*.

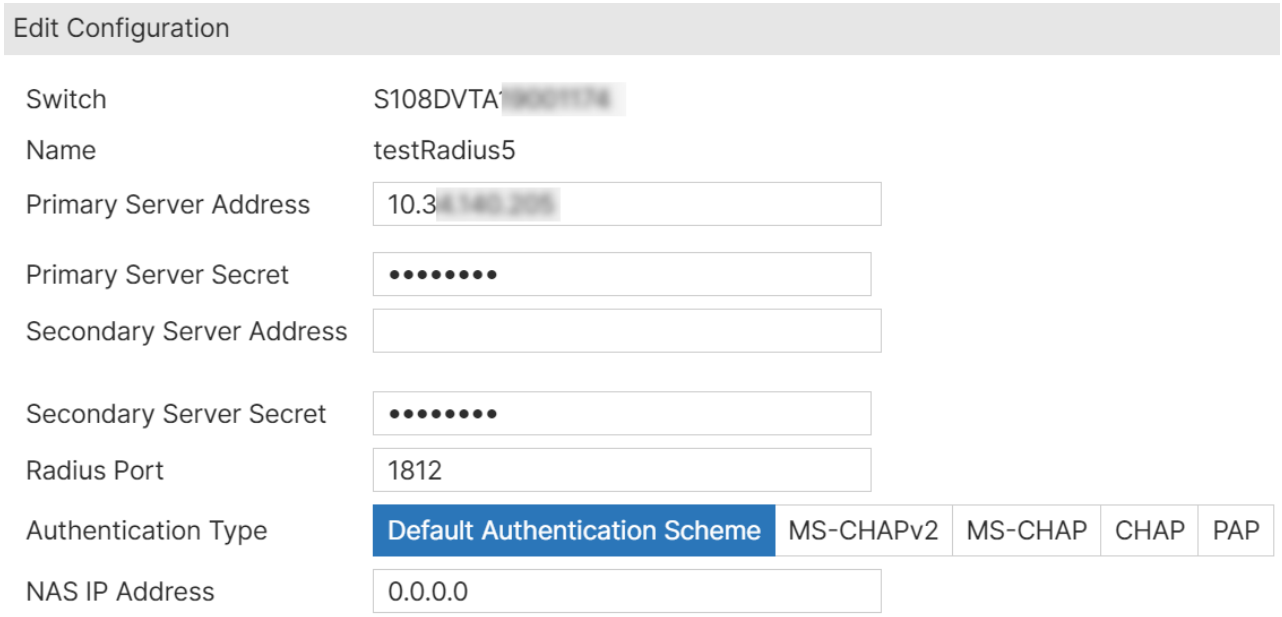


3. Click in the Switch field to select a FortiSwitch unit. You can select multiple FortiSwitch units.
4. Enter a name for this RADIUS authentication configuration.
5. Enter the IPv4 address for the primary RADIUS authentication server.
6. Enter the primary server secret key. This key can be a maximum of 16 characters long. This value must match the secret on the primary RADIUS server.
7. Enter the IPv4 address for the secondary RADIUS authentication server.
8. Enter the secondary server secret key. This key can be a maximum of 16 characters long. This value must match the secret on the secondary RADIUS server.
9. Enter the port number to connect with the RADIUS authentication servers.
10. If you know that the RADIUS server uses a specific authentication scheme, click in the Authentication Scheme field and select the scheme from the list. If you do not select an authentication scheme, the default authentication scheme is used.
11. Enter the IP address of the FortiSwitch interface used to talk to the RADIUS server.
12. Select *Ok* to create the RADIUS authentication configuration.

Editing a RADIUS authentication configuration

To edit a RADIUS authentication configuration:

1. Select the RADIUS authentication configuration that you want to edit and click **Edit**.

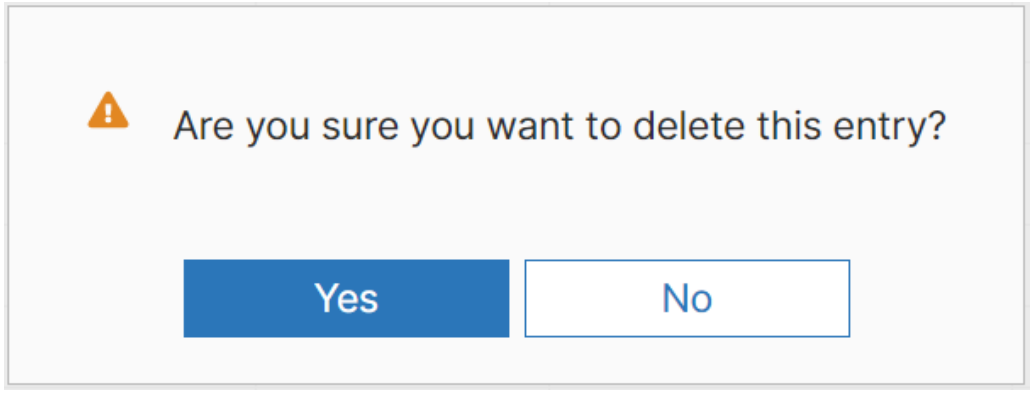


2. Make your changes in the Edit Configuration dialog box.
3. Select *Ok* to apply your changes.

Deleting a RADIUS authentication configuration

To delete a RADIUS authentication configuration:

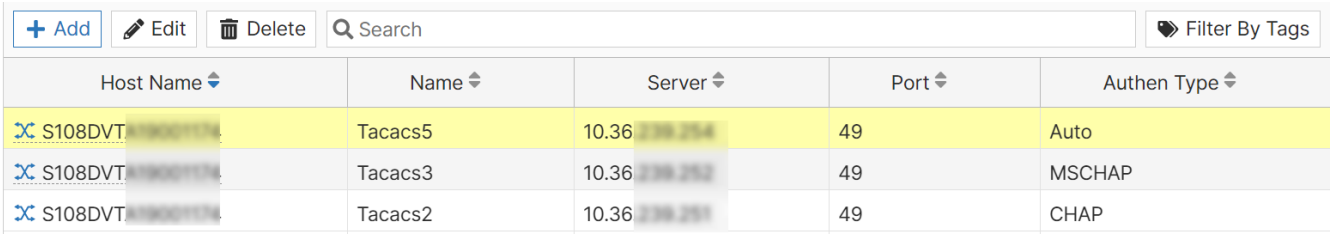
1. Select the RADIUS authentication configuration that you want to delete and click **Delete**.



2. Select *Yes* to delete the RADIUS authentication configuration.

TACACS Authentication

The TACACS Authentication pane allows you to configure TACACS authentication for one or more FortiSwitch units.



To find a specific host name, configuration name, or server IP address, enter part or all of the search item in the Search field.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that use TACACS authentication *and* are tagged with the selected tag.

To filter the list of configurations by switch tag, select **Filter By Tags** and the tag to filter with. If you select multiple tags to filter with, the results are configurations for FortiSwitch units that are tagged with one or more of the selected tags.

You can perform the following tasks from the TACACS Authentication pane:

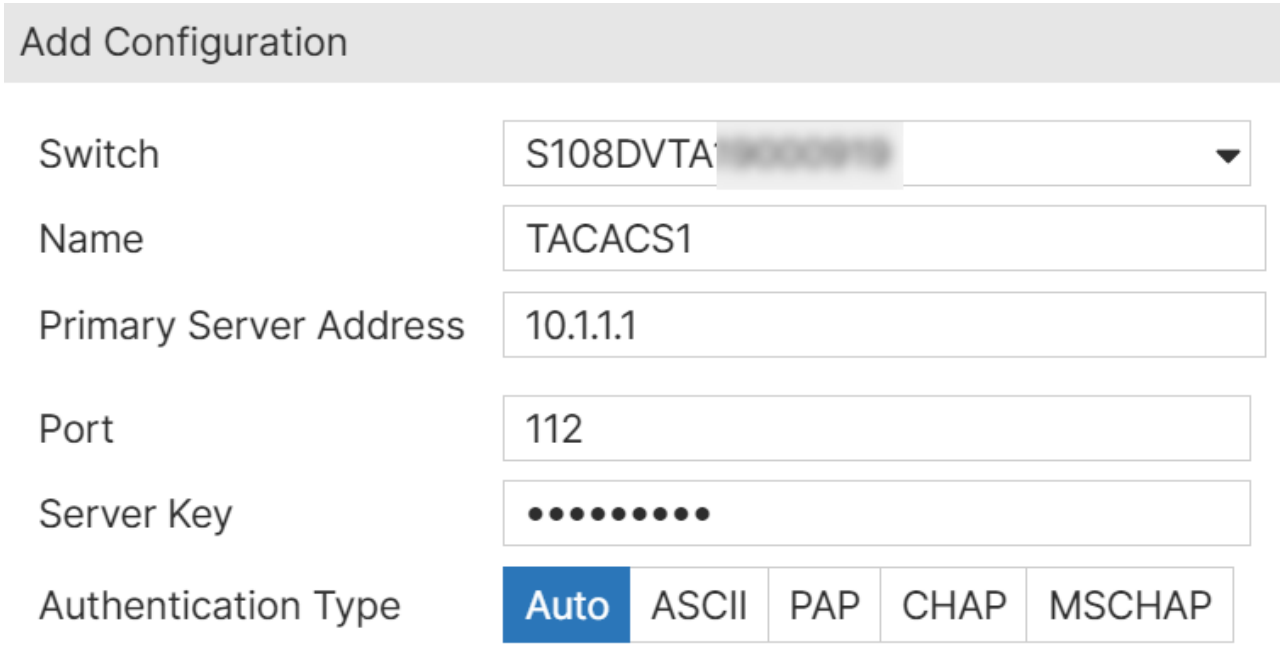
- Creating a TACACS authentication configuration
- Editing a TACACS authentication configuration
- Deleting a TACACS authentication configuration

Creating a TACACS authentication configuration

You can create a TACACS authentication configuration for one or more FortiSwitch units.

To create a TACACS authentication configuration:

1. Go to *Configuration* > *TACACS Authentication*.
2. Select *Add*.



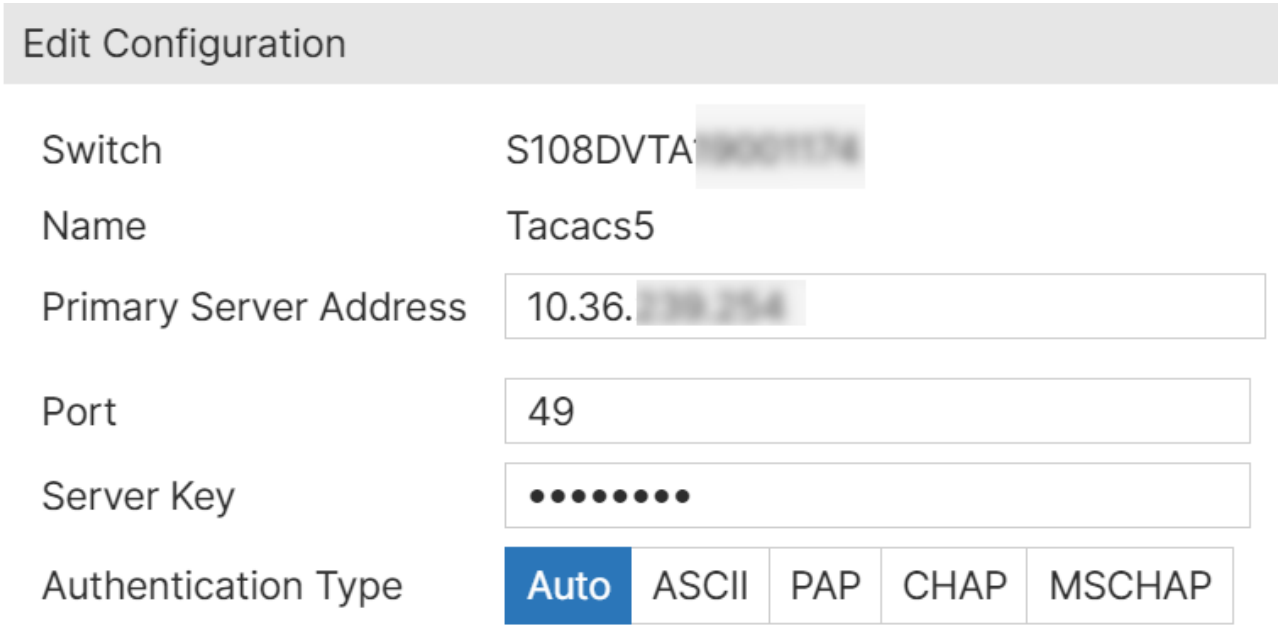
3. Click in the Switch field to select a FortiSwitch unit. You can select multiple FortiSwitch units.

4. Enter a name for this TACACS authentication configuration.
5. Enter the IPv4 address for the TACACS authentication server.
6. Enter the port number to connect with the TACACS authentication server.
7. Enter the server key for the TACACS server. This key can be a maximum of 16 characters long. This value must match the secret on the primary RADIUS server.
8. Select the authentication type to use for the TACACS server. *Auto* tries PAP, MSCHAP, and CHAP (in that order).
9. Select *Ok* to create the TACACS authentication configuration.

Editing a TACACS authentication configuration

To edit a TACACS authentication configuration:

1. Select the TACACS authentication configuration that you want to edit and click **Edit**.

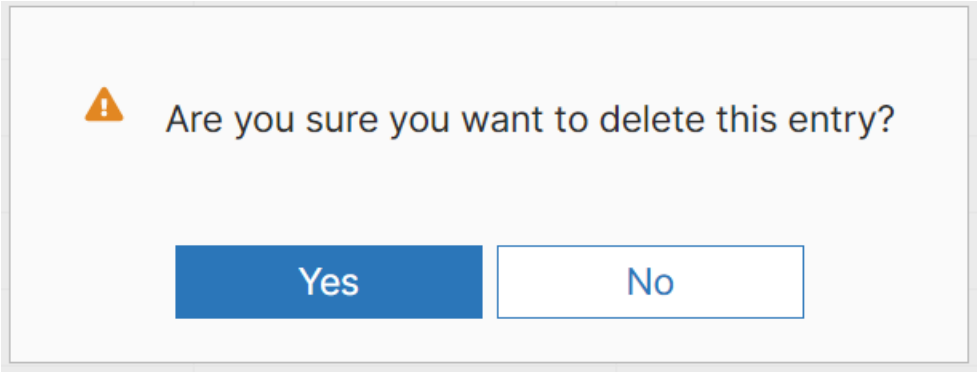


2. Make your changes in the Edit Configuration dialog box.
3. Select *Ok* to apply your changes.

Deleting a TACACS authentication configuration

To delete a TACACS authentication configuration:

1. Select ✕ in the row of the TACACS authentication configuration that you want to delete.

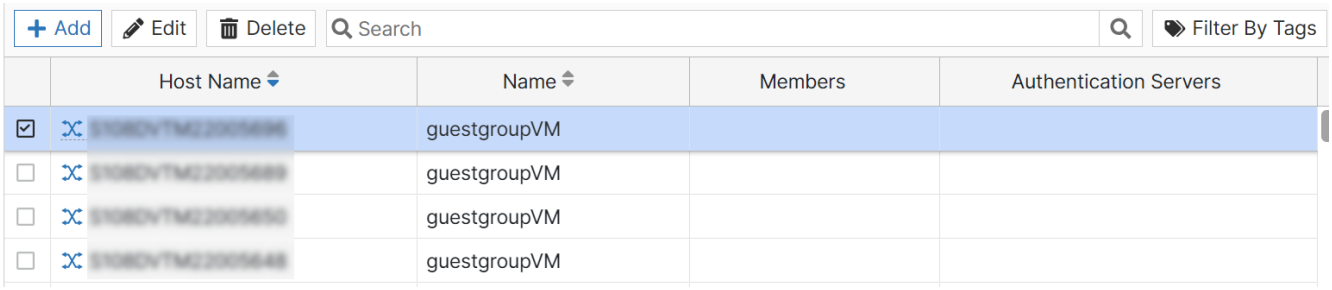


2. Select *Yes* to delete the TACACS authentication configuration.

User Groups

The User Groups pane allows you to create a user group that contains users and authentication servers.

Security policies allow access to specified user groups only. This restricted access enforces role-based access control (RBAC) to your organization's network and its resources. Users must be in a group, and that group must be part of the security policy.



To update the list of user groups, select *Refresh*.

To find a specific host name, user group name, group member, or authentication server name, enter part or all of the search item in the Search field.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that belong to the user group *and* are tagged with the selected tag.

To filter the list of user groups by switch tag, click **Filter By Tags** and select the tag to filter with. If you select multiple tags to filter with, the results are user groups for FortiSwitch units that are tagged with one or more of the selected tags.

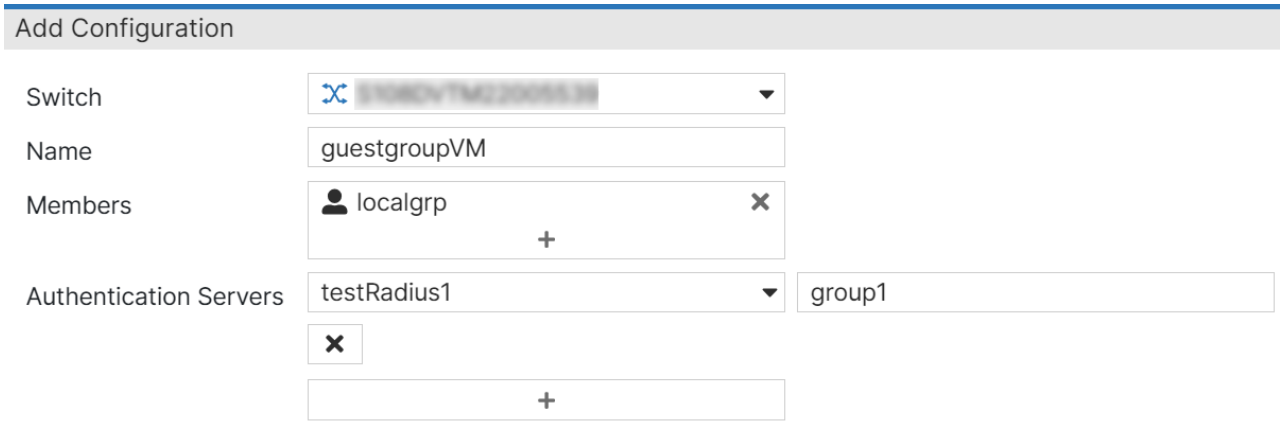
You can perform the following tasks from the User Groups pane:

- Creating a user group
- Editing a user group
- Deleting a user group

Creating a user group

You can create a user group that contains users and authentication servers for one or more FortiSwitch units.

1. Go to *Configuration* > *User Groups*.
2. Click *Add*.

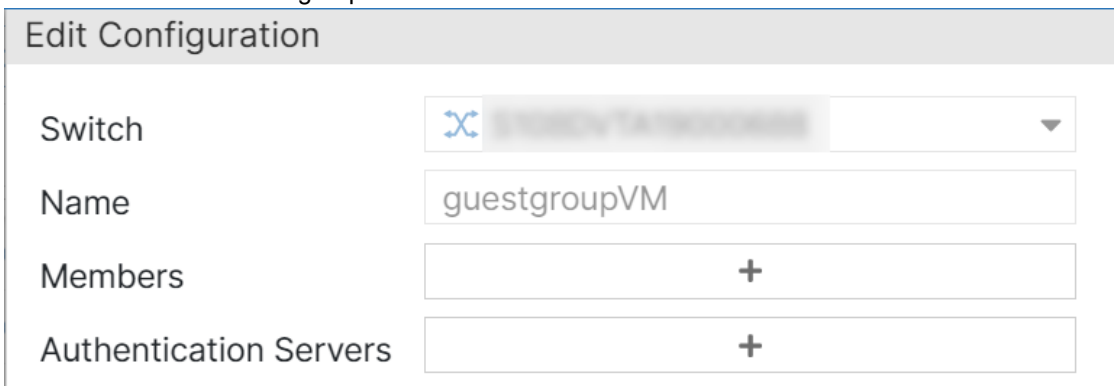


3. Click in the **Switch** field to select a FortiSwitch unit. You can select multiple FortiSwitch units.
4. Enter a name for this user group.
5. Click in the Members field to select available users to belong to the user group.
6. Select + to add an authentication server.
   - Select the server name from the drop-down list.
   - Select a specific group name or select *Any*.
7. Select *Save* to create the user group.

Editing a user group

Perform the following steps to edit a user group.

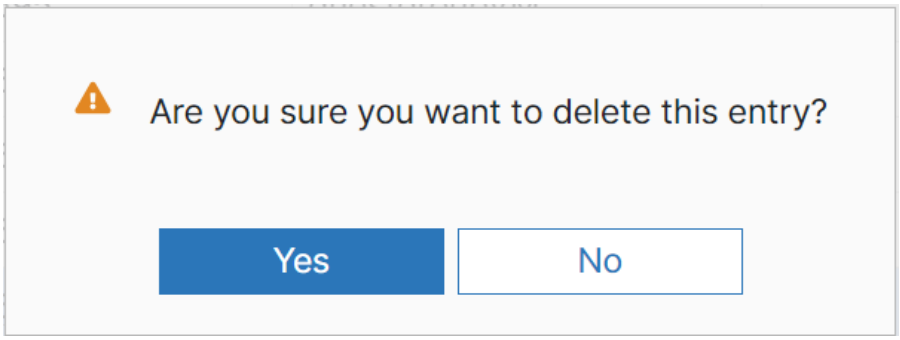
1. Select the row for the user group and click **Edit**.



2. Make your changes in the Edit Configuration dialog box.
3. Select *Save* to apply your changes.

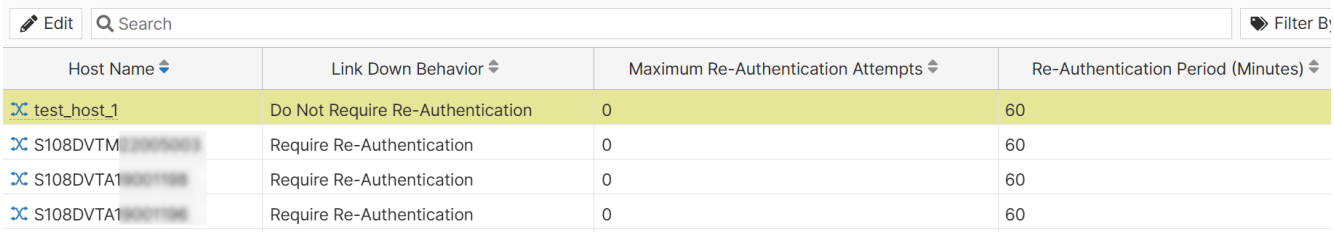
Deleting a user group

To delete a user group, select row of the user group and click **Delete**. Select *Yes* to delete the user group.



Port Security

The Port Security pane allows you to edit the global 802.1X-authentication configuration for the FortiSwitch units.



To update the list of 802.1X authentication configurations, select *Refresh*.

To find a specific host name, enter part or all of the search item in the Search field.

You can use the Search field and the Filter with Tags field together to find FortiSwitch units that use 802.1X authentication *and* are tagged with the selected tag.

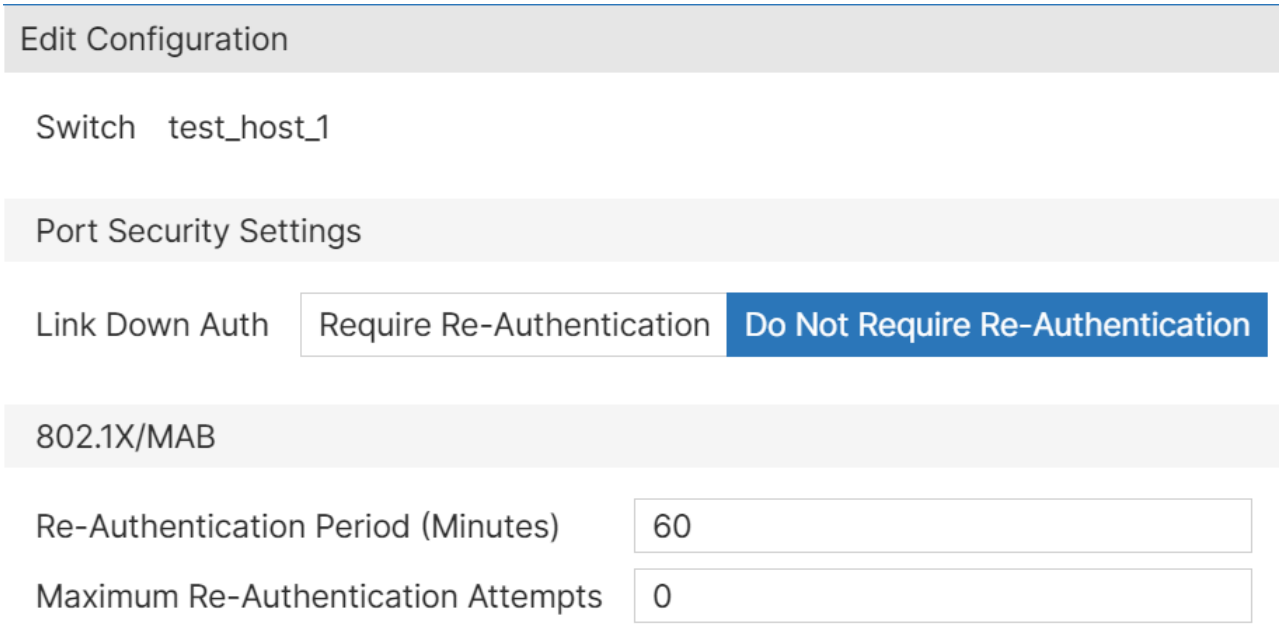
To filter the list of configurations by switch tag, select and the tag to filter with. If you select multiple tags to filter with, the results are configurations for FortiSwitch units that are tagged with one or more of the selected tags.

You can perform the following task from the Port Security pane:

- Editing the global 802.1X-authentication settings

Editing the global 802.1X-authentication settings

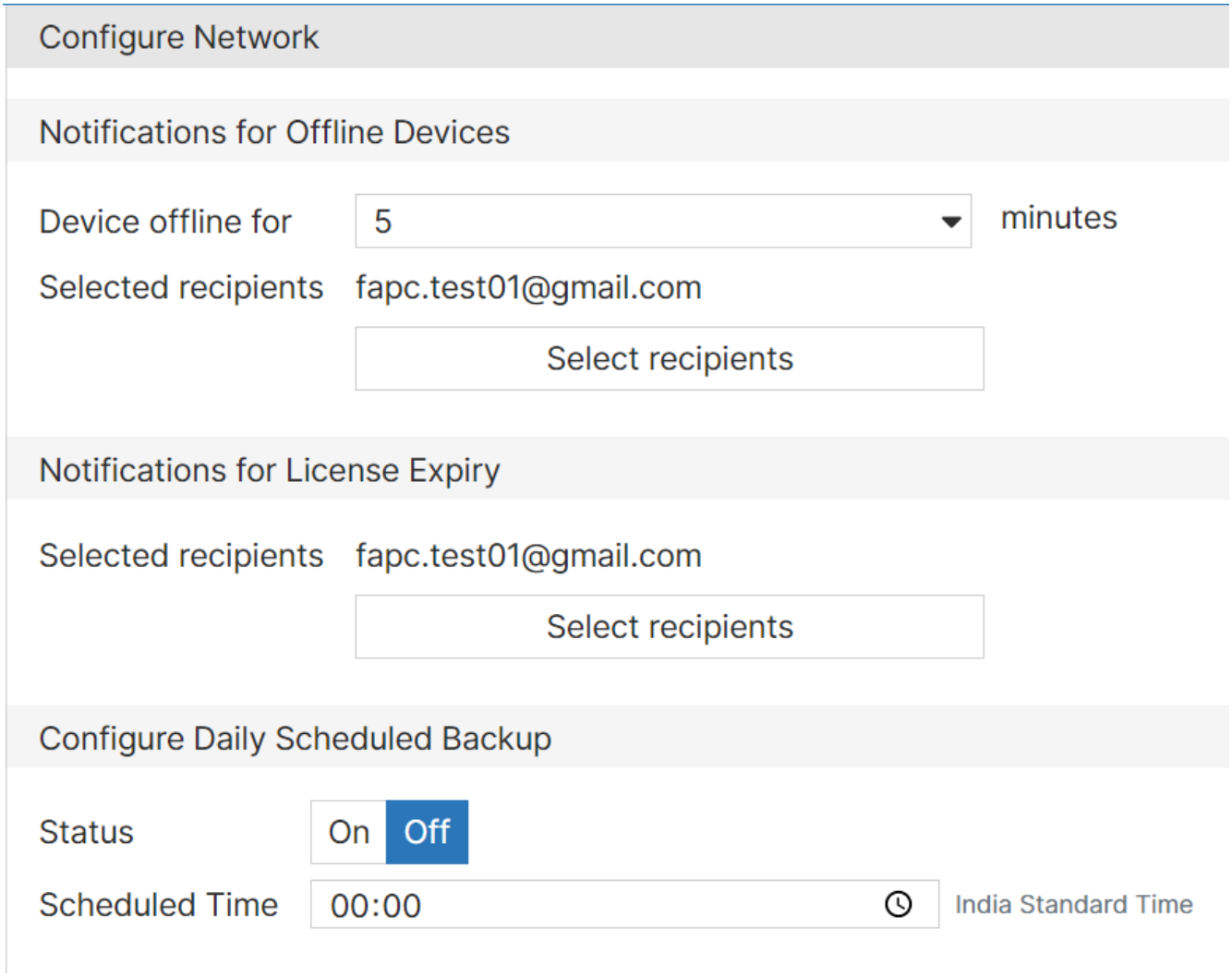
1. Select in the row for the 802.1X-authentication configuration that you want to edit.



2. Make your changes in the Edit Configuration dialog box.
3. Select *Save* to apply your changes.

Network

The Network pane controls email notifications and scheduled daily backups.



To set up an email notification:

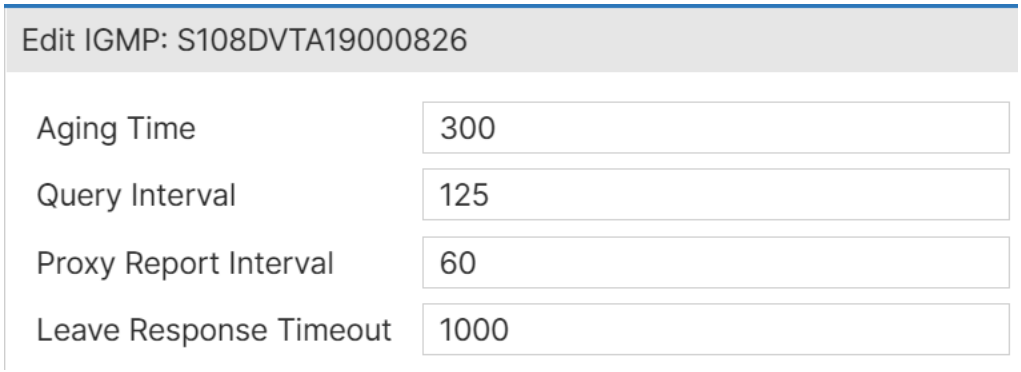
1. Select 5, 10, 15, 30, or 60 minutes before FortiLAN Cloud sends an email notification that a FortiSwitch unit is offline.
2. Select and then select one or more users to receive an email notification when a FortiSwitch unit is offline. If no users are selected, FortiLAN Cloud will not send email notifications.
3. Select and then select one or more users to receive an email notification when FortiLAN Cloud licenses are going to expire or have expired. If no users are selected, FortiLAN Cloud will not send email notifications.
4. Select *Save* to apply your changes.

To schedule daily backups:

1. Select *On* to enable daily backups.
2. Select whether to use *Local Time* or *UTC*.
3. Select the hour and minutes for your daily backup.
4. Select *Save* to apply your changes.

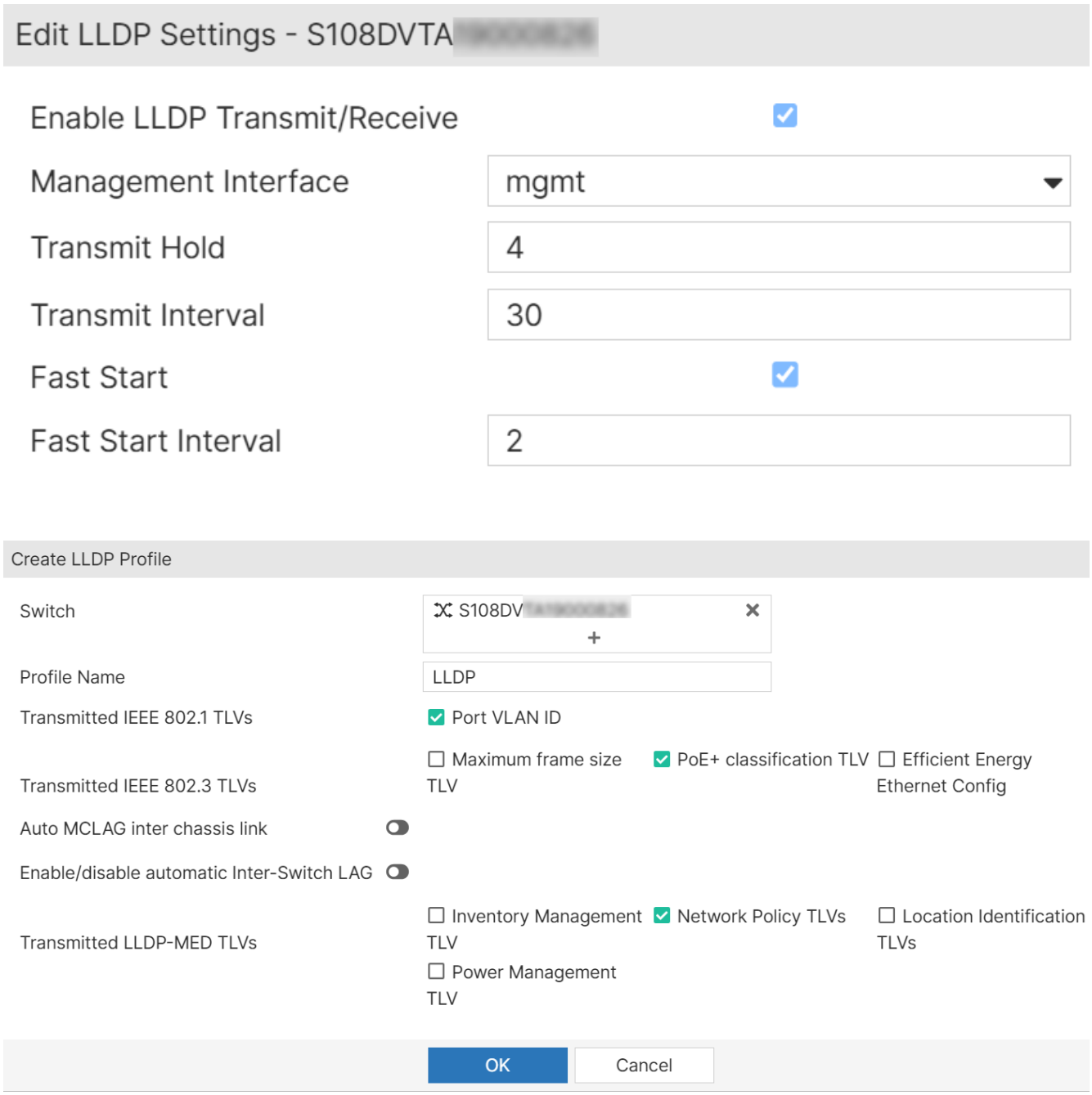
IGMP

IGMP snooping allows the FortiSwitch to passively listen to the IGMP network traffic between hosts and routers. The IGMP configuration is a part of the ZTC templates in FortiLAN Cloud. You can review the current configuration on the FortiSwitch, modify a few selected items, and apply the configuration to the FortiSwitch. For configuration details, see Creating a zero-touch configuration.



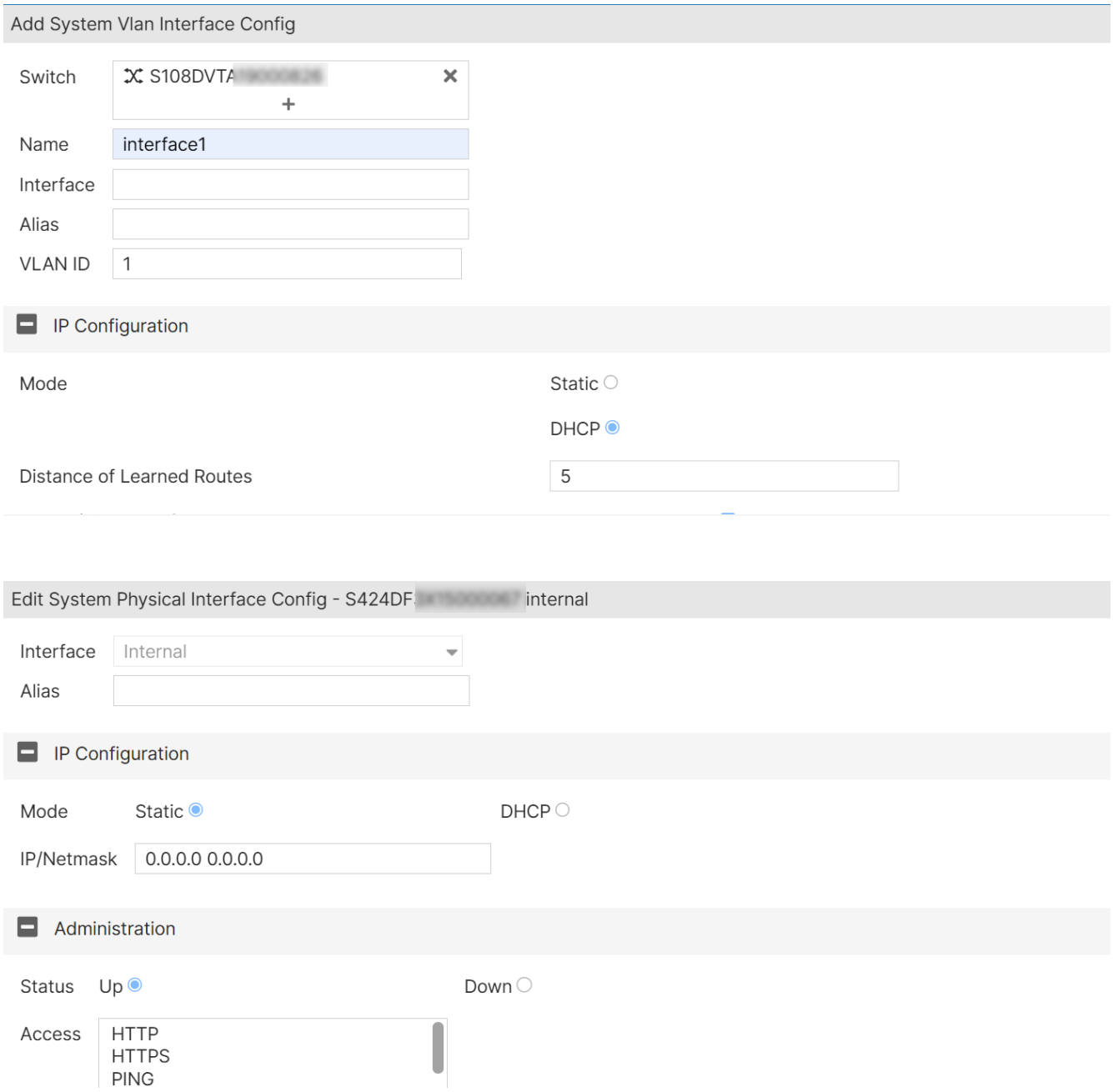
LLDP

The FortiSwitches support LLDP for transmission and reception wherein the switch multicasts LLDP packets to advertise its identity and capabilities. You can modify the current LLDP settings on the ZTC template and create/edit LLDP profiles. These configurations can be directly applied to the FortiSwitch. For configuration details, see Creating a zero-touch configuration.



System Interfaces

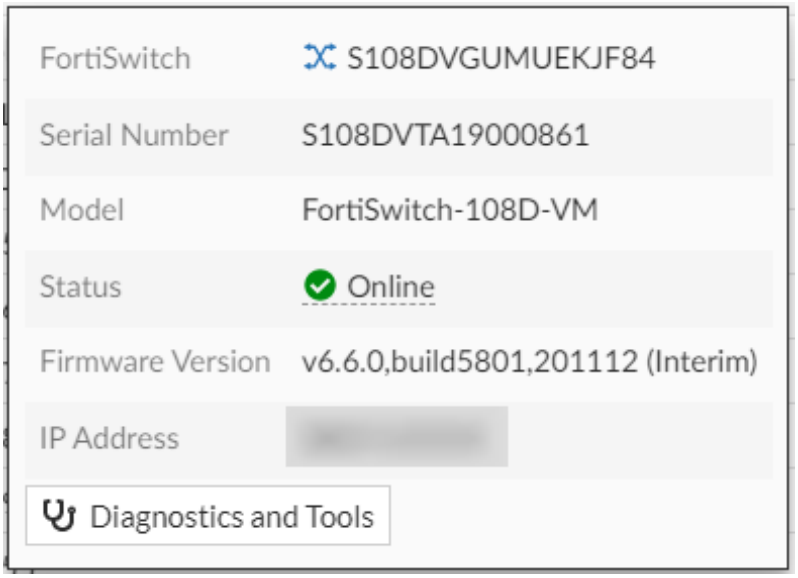
You can configure physical and VLAN interfaces on a FortiSwitch. You can create new interfaces or modify the current interfaces settings on the ZTC template. For configuration details, see Creating a zero-touch configuration.



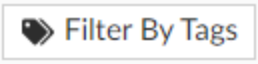
Monitor

Select *Monitor* to check modules, MAC addresses, switch and port statistics; FortiSwitch units using PoE, LLDP, or 802.1x authentication; STP instances; DHCP-snooping and IGMP-snooping databases; logs; and the status of zero-touch configurations, scheduled upgrades, and packet captures.

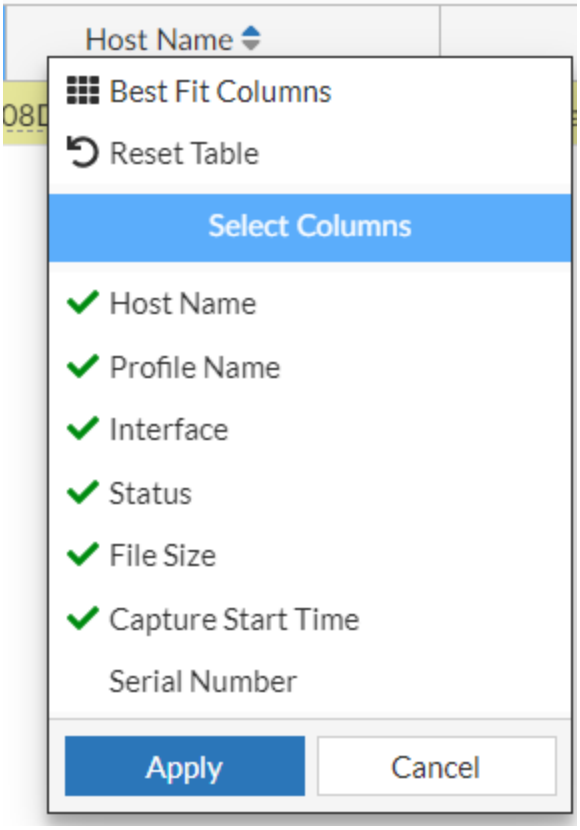
In the various monitor pages displayed in this section, hove over the host name to navigate to the **Diagnostics and Tools** options as described in section Switches



Also, the monitor pages provide the option to filter data by the associated tags, click **Filter by Tags**.



To select the filter options, right-click on any column.



You can select the following options from the left pane:

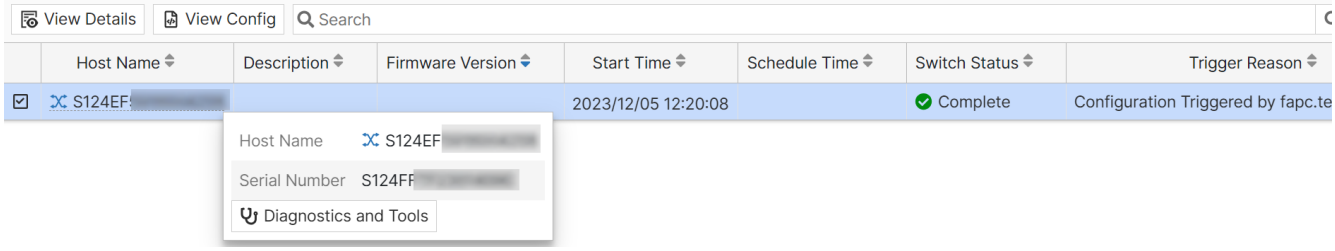
Zero Touch Config Status

This pane lists the status of the zero-touch configurations. The status can be one of the following.

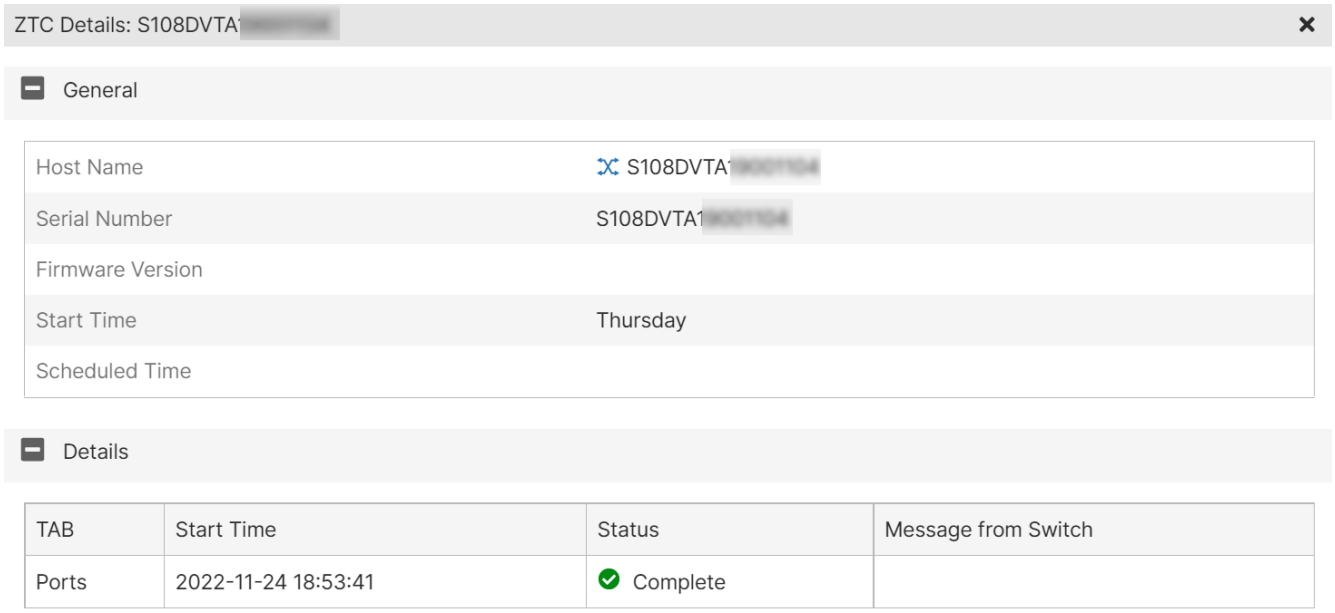
- *Firmware Upgrade In progress*—The firmware is being upgraded on the specified host names.
- *Apply configuration command*—The CLI commands entered in the Add Zero Touch Configuration dialog box are being run.
- *Timeout* —Zero Touch configurations are not processed until a specific time (approximately 30 minutes).
- *Complete*—The firmware has been upgraded, or the CLI commands have been run.
- *Failure*—The firmware has not been upgraded, or the CLI commands have not been run.

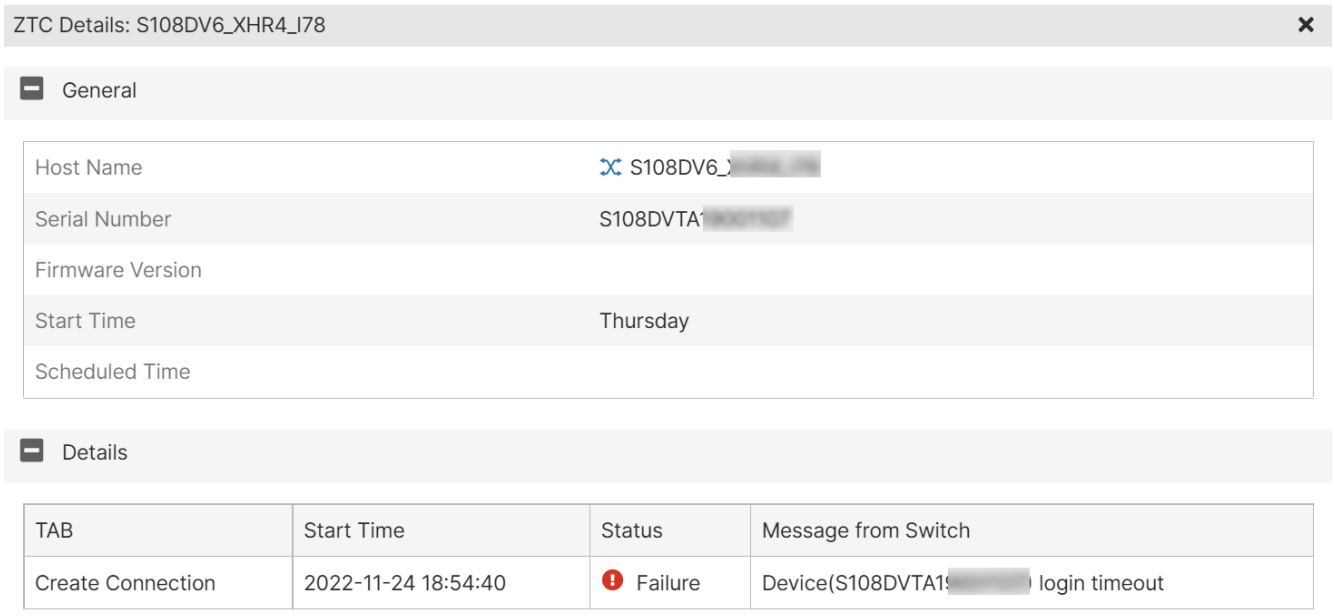
The trigger reason could be one of the following.

- *Reason unavailable* - For the existing ZTC entries.
- *Configuration Triggered at scheduled time* - For scheduled ZTC entries.
- *Configuration Triggered by <account name>* - For manual trigger of ZTC.
- *Re-trying Configuration* - When ZTC is pushed again.

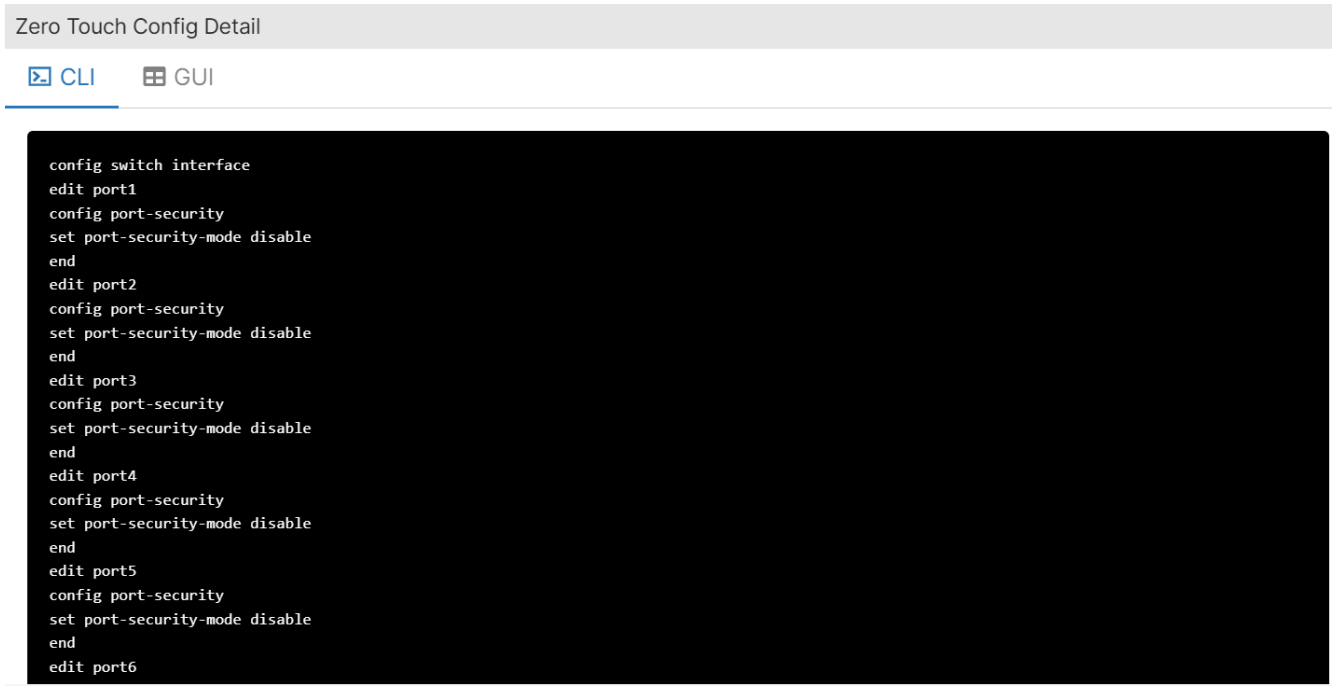


Select a row and click **View Details** to view the host details.





Select a row and click **View Config** to view the CLI/GUI configuration details.

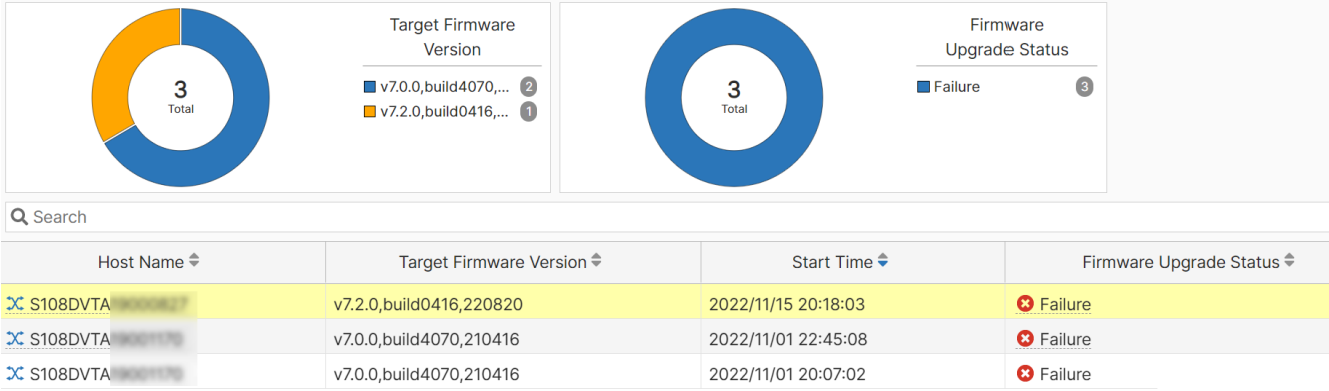


To find a specific switch, enter part or all of the host name or model number in the Search field.

Scheduled Upgrade Status

The Scheduled Upgrade Status pane lists the status of the scheduled firmware upgrades. The status can be one of the following:

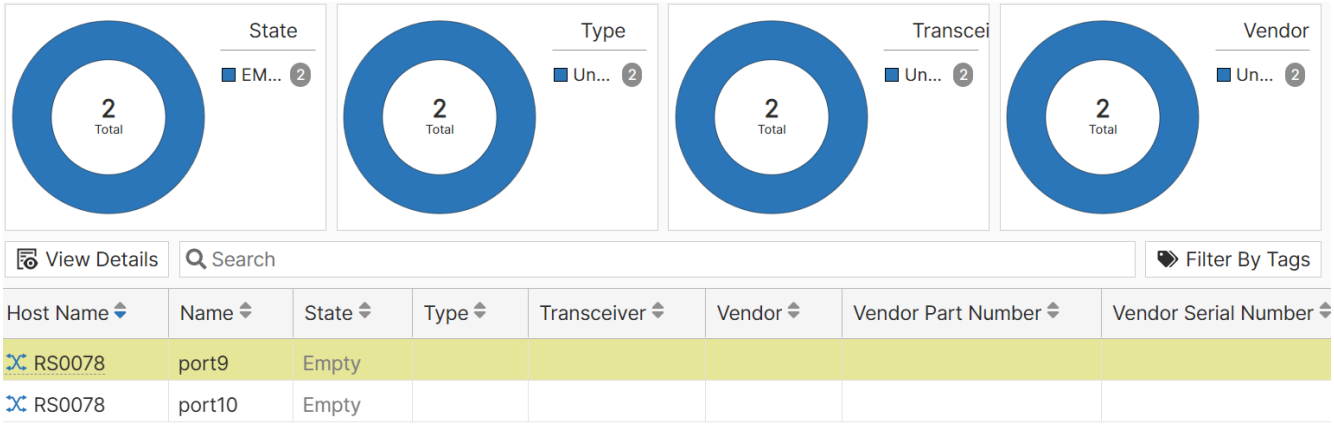
- *Pending*—The scheduled time and date for the firmware upgrade have not occurred yet.
- *Download firmware*—The firmware image is loading on the FortiSwitch unit.
- *Complete*—The firmware has been upgraded.
- *Failure*—The firmware has not been upgraded. Check that the firmware image is for the same model as the selected switches.



To find a specific switch, enter part or all of the host name or model number in the *Search* field.

Modules

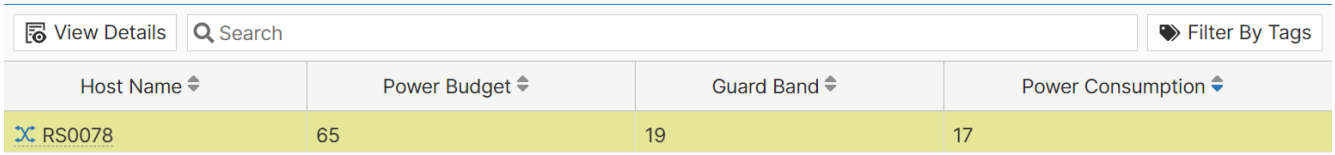
The Modules pane describes the modules inserted in any switch, including state, type, and vendor.



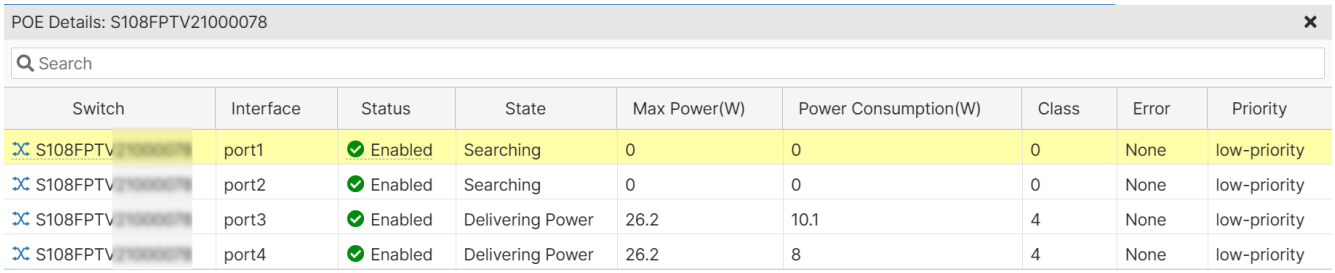
Use the Search field to find a switch serial number, switch host name, port name, state, type, transceiver, vendor, vendor part number, or vendor serial number..

PoE Status

The PoE Status pane lists the power budget, guard band, and power consumption (in Watts) of FortiSwitch units using PoE.



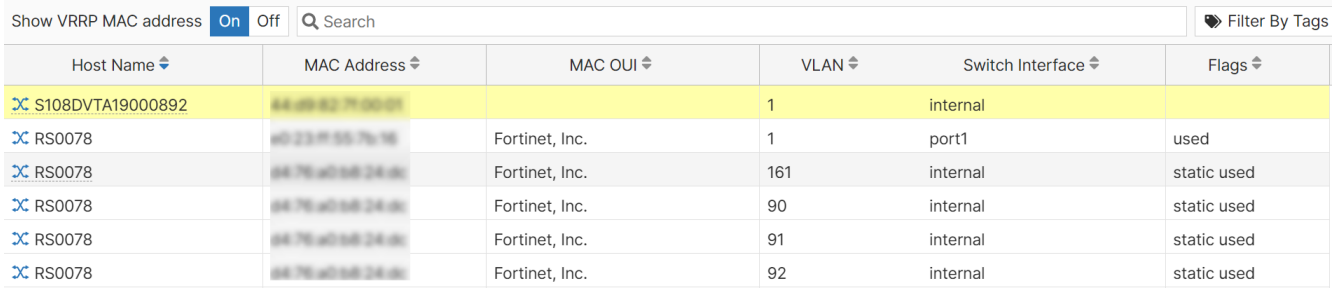
Select a row and click **View Details**.



To find a switch, enter part or all of the host name in the Search field.

MAC Addresses

The MAC Addresses pane lists all MAC address and the corresponding organizationally unique identifier (OUI) host name, VLAN, interface, and flags.

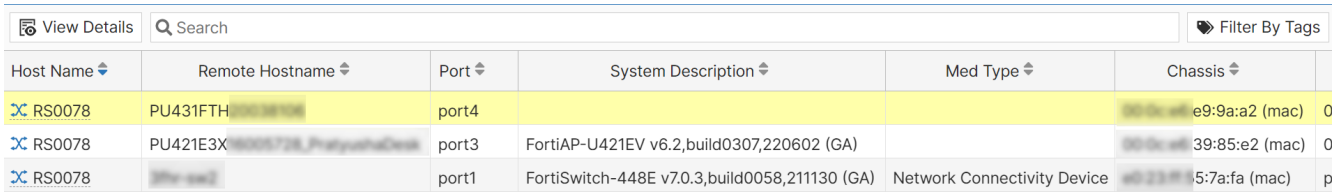


To show or hide MAC addresses learned on a VRRP server, enable/disable the **Show VRRP MAC address** option.

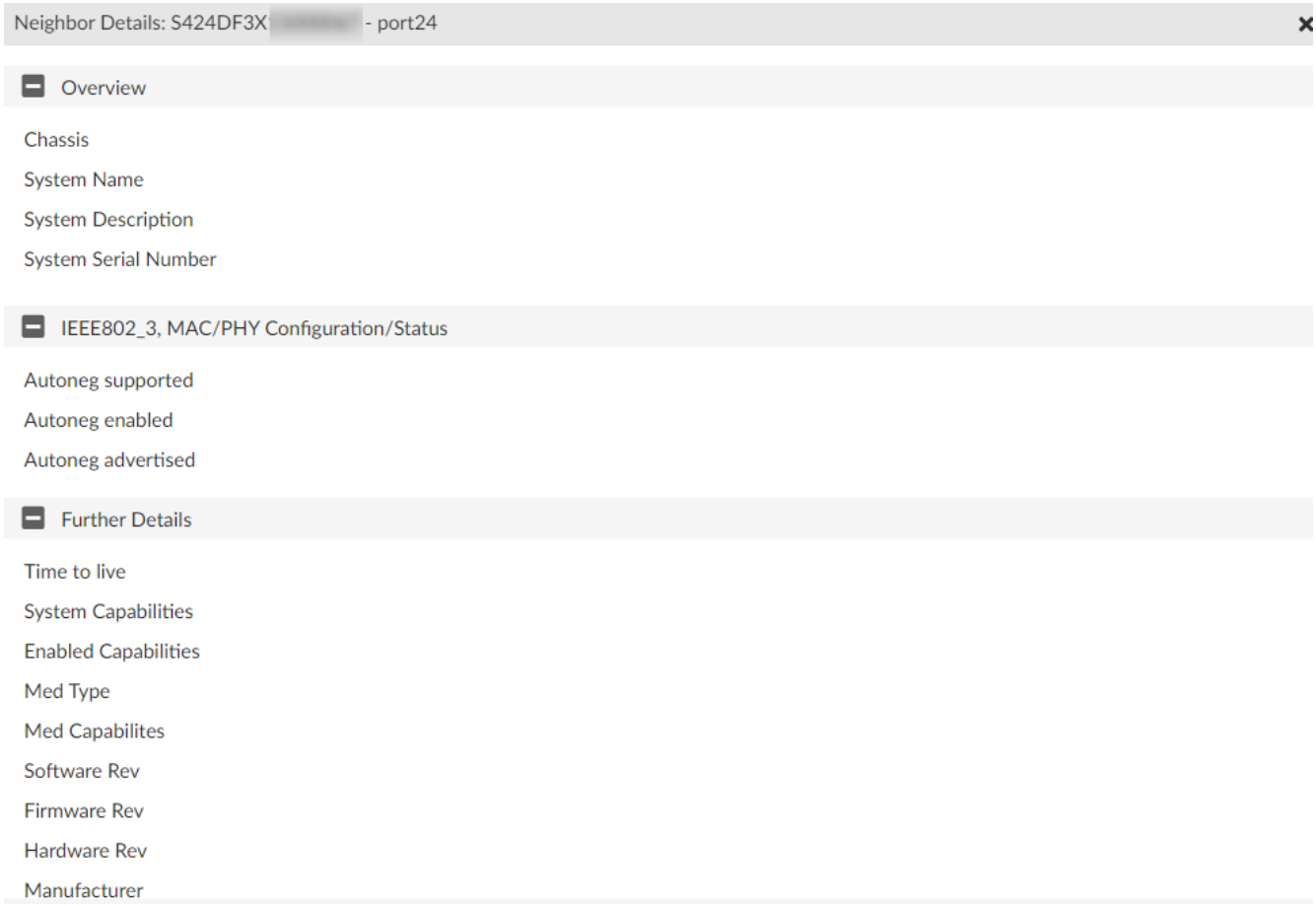
To find a MAC address, enter part or all of the MAC address in the Search field.

LLDP

The LLDP pane provides information about ports using LLDP.



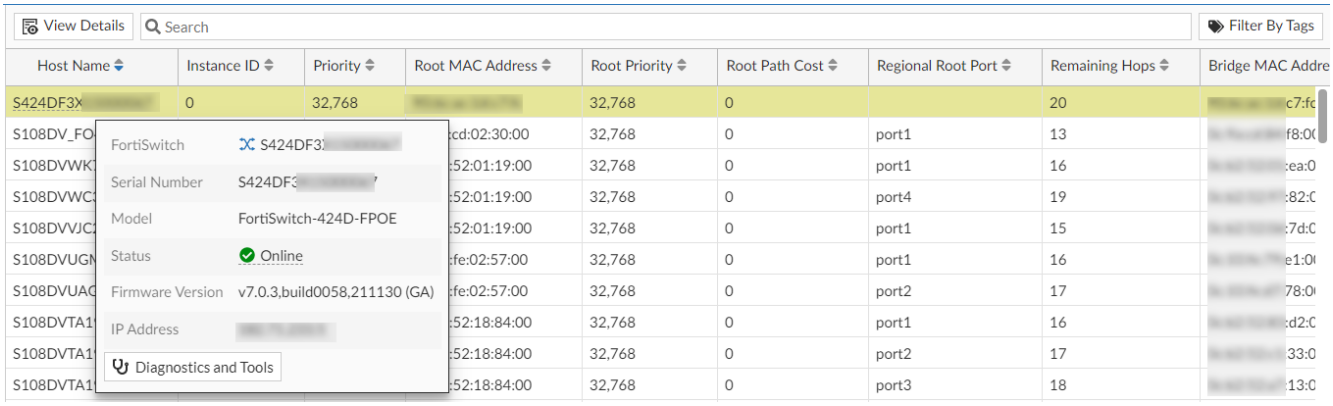
Select a specific port and click **View Details**.



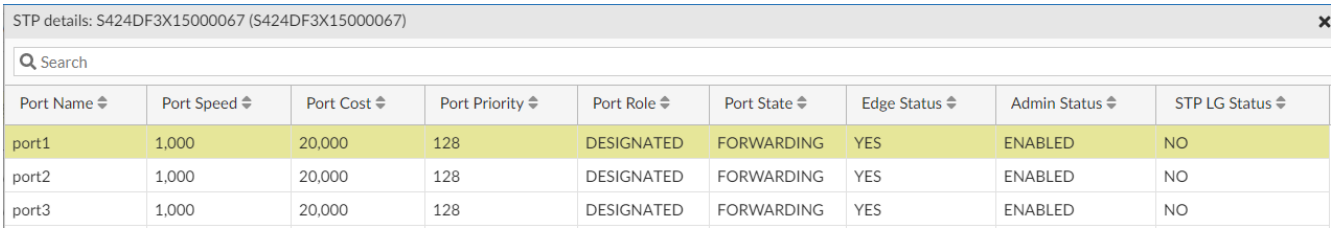
Use the Search field to find a host name, chassis ID, or port number.

STP

The STP pane provides information about STP instances.



Select an STP instance and click **View Details** to view the instance details.



Use the Search field to find a host name or MAC address.

DHCP-Snooping

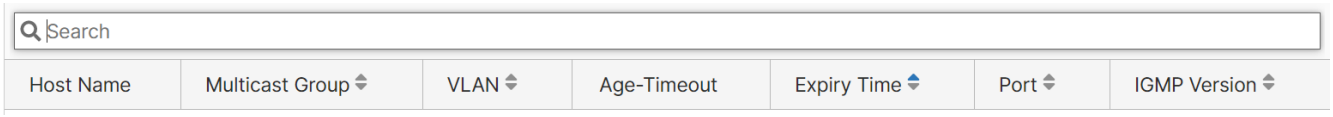
The DHCP-Snooping pane lists information about DHCP clients and servers.

You can use the Search field to find specific IP addresses.

Hovering over the client IP address shows the MAC address, lease, host name, domain name, and vendor, if available.

IGMP-Snooping

The IGMP-Snooping pane lists information about the multicast groups learned on the ports and when the entries will be deleted from the IGMP-snooping database.

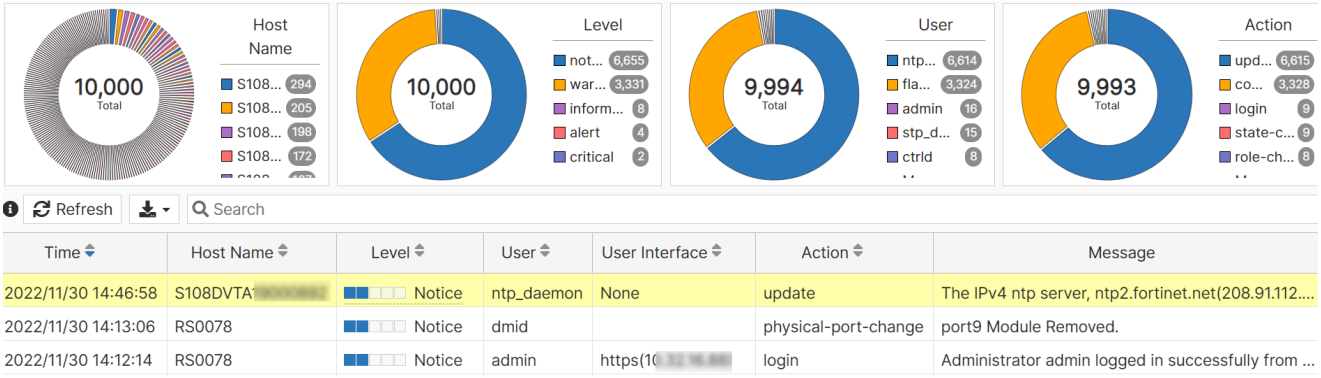


You can use the Search field to find specific multicast groups.

System Log

The System Log pane lists system events for all managed FortiSwitch units.

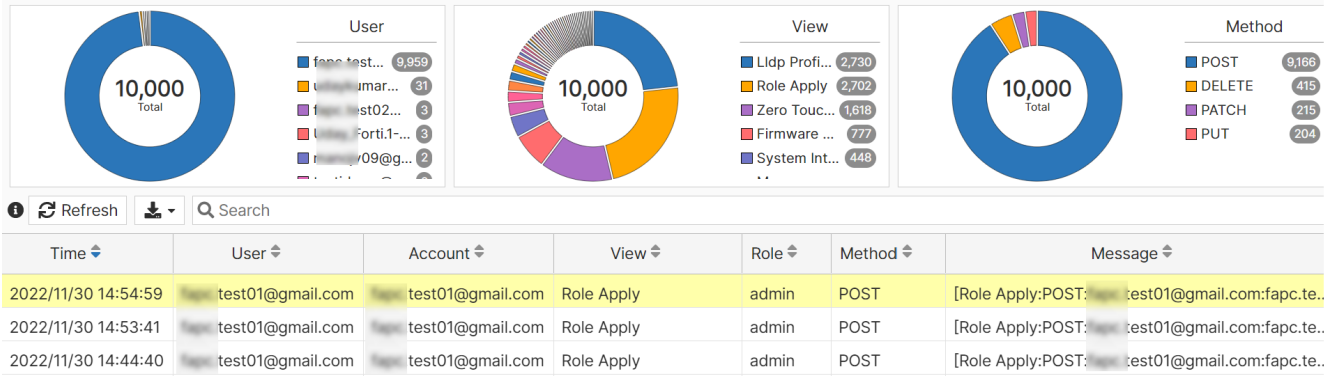
When a FortiLAN Cloud account has an active license, system log entries are retained for 365 days. After the license period ends, system log entries are retained for a maximum of 7 days. When a FortiLAN Cloud account does not have an active license, system log entries are retained for 7 days.



You can use the Search field to filter by severity level or message content.

Audit Log

The Audit Log pane lists changes for all managed FortiSwitch units.

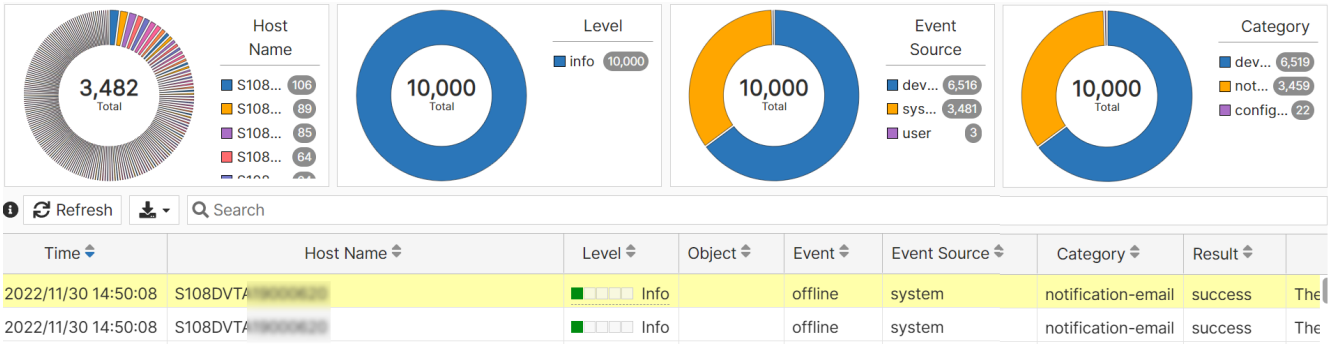


To find specific log entries, enter part or all of the log entry in the Search field.

Event Log

The Event Log pane lists system, device, and user changes.

When a FortiLAN Cloud account has an active license, event log entries are retained for 365 days. After the license period ends, event log entries are retained for a maximum of 7 days. When a FortiLAN Cloud account does not have an active license, event log entries are retained for 7 days.

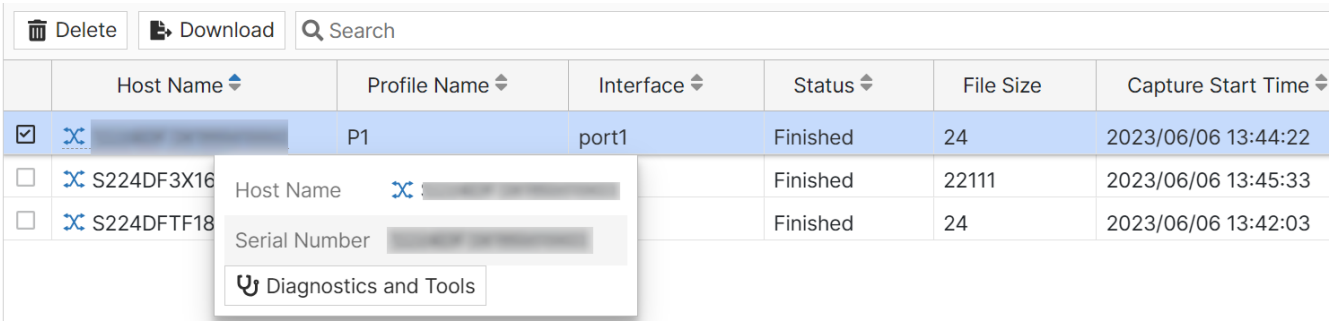


You can use the Search field to find specific events.

Packet Capture Files

The Packet Capture Files pane lists all packet capture profiles and the corresponding host name, interface, status, file size, and capture time. The status can be one of the following:

- *Downloading*—The packet capture file is currently downloading from the FortiSwitch unit to FortiLAN Cloud.
- *Failed*—The packet capture file failed to download from the FortiSwitch unit to FortiLAN Cloud.
- *Finished*—The packet capture file has successfully downloaded from the FortiSwitch unit to FortiLAN Cloud.



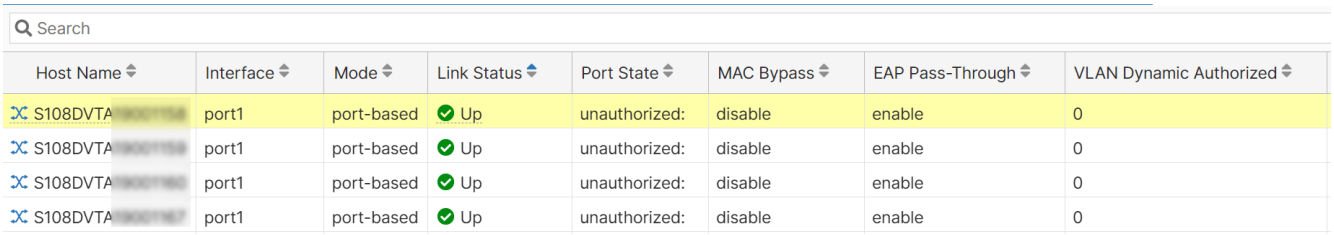
To find a specific packet capture profile, enter part or all of the name in the Search field.

To download the packet capture file, select **Download** for the corresponding packet capture profile.

To delete the packet capture file, select **Delete** for the corresponding packet capture profile.

802.1x Status

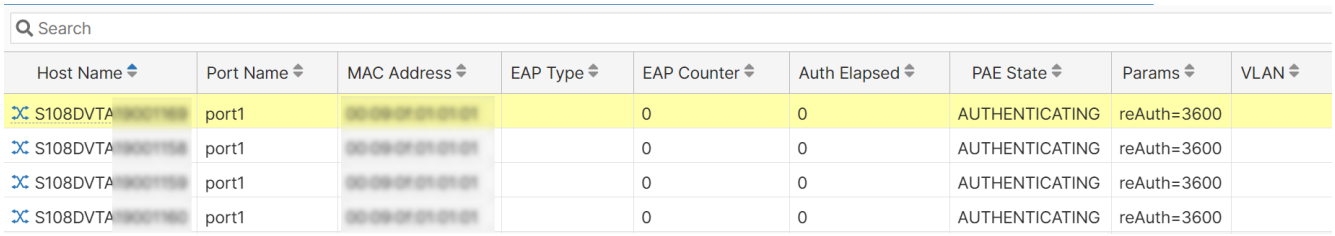
The 802.1x pane displays information about FortiSwitch ports using IEEE 802.1x authentication. The information displayed includes mode, link status, port state, and VLAN configuration.



To find a specific host name or interface, enter part or all of the name in the Search field.

802.1x Session

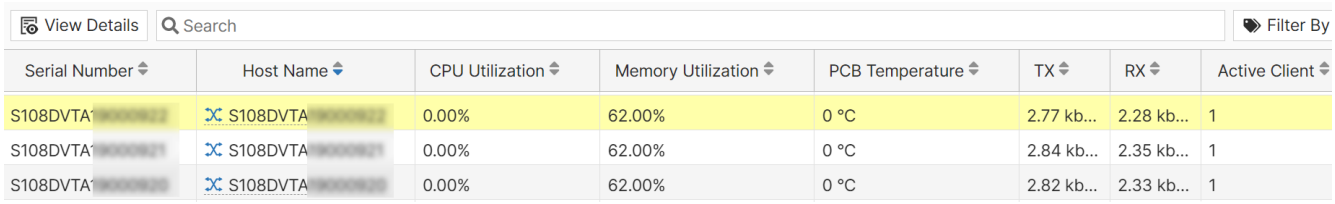
The 802.1x pane displays information about IEEE 802.1x authentication sessions. The information displayed includes host name, port name, MAC address, and EAP type.



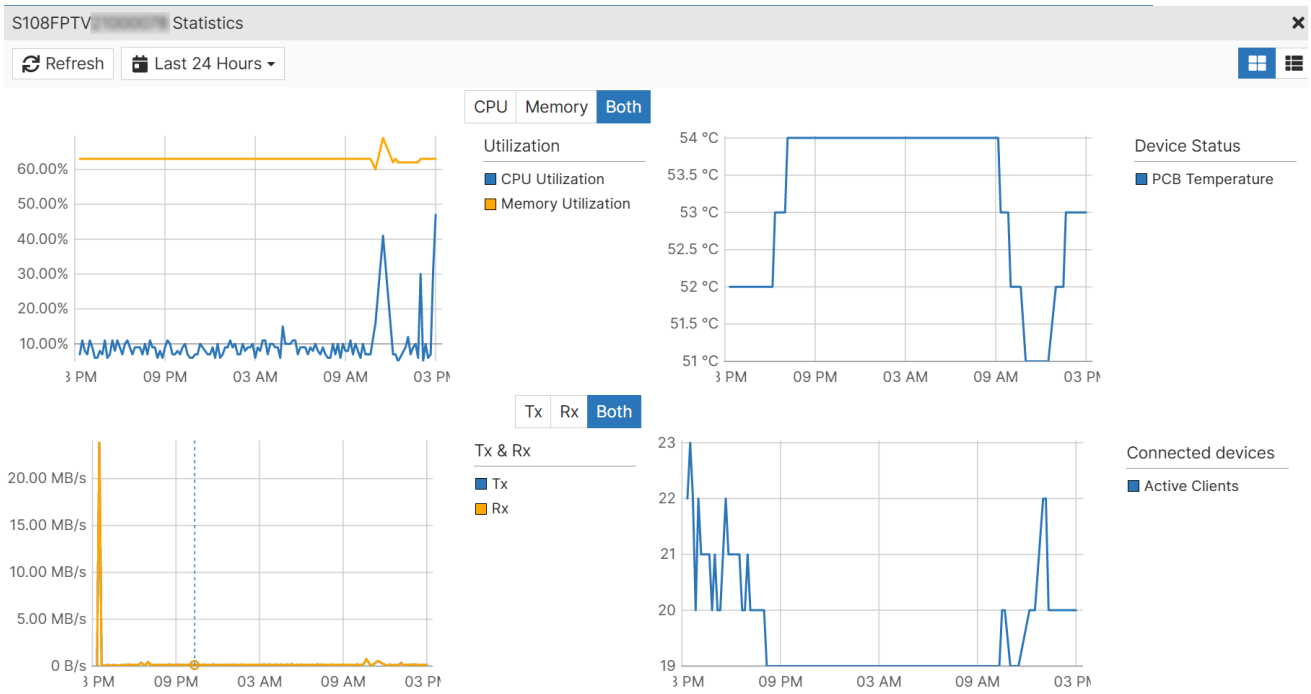
To find a specific host name or interface, enter part or all of the name in the **Search** field.

Switch Statistics

The Switch Statistics pane displays graphs for the CPU usage, memory usage, PCB temperature, received bits per second, transmitted bits per second, and number of learned MAC addresses for each FortiSwitch unit.



Select a row and click **View Details** for a graphical representation of the statistics.



To find a specific switch, enter part or all of the host name in the Search field.

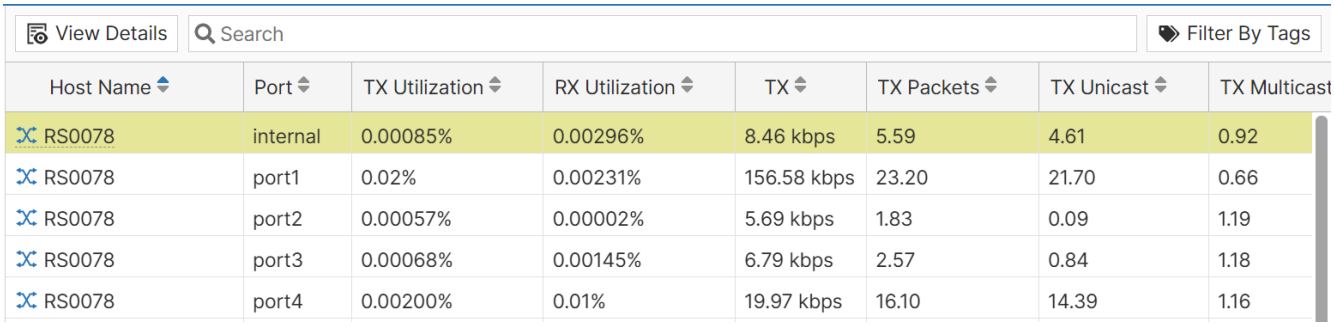
Switch Port Statistics

The Switch Port Statistics pane can display the following graphs for each port:

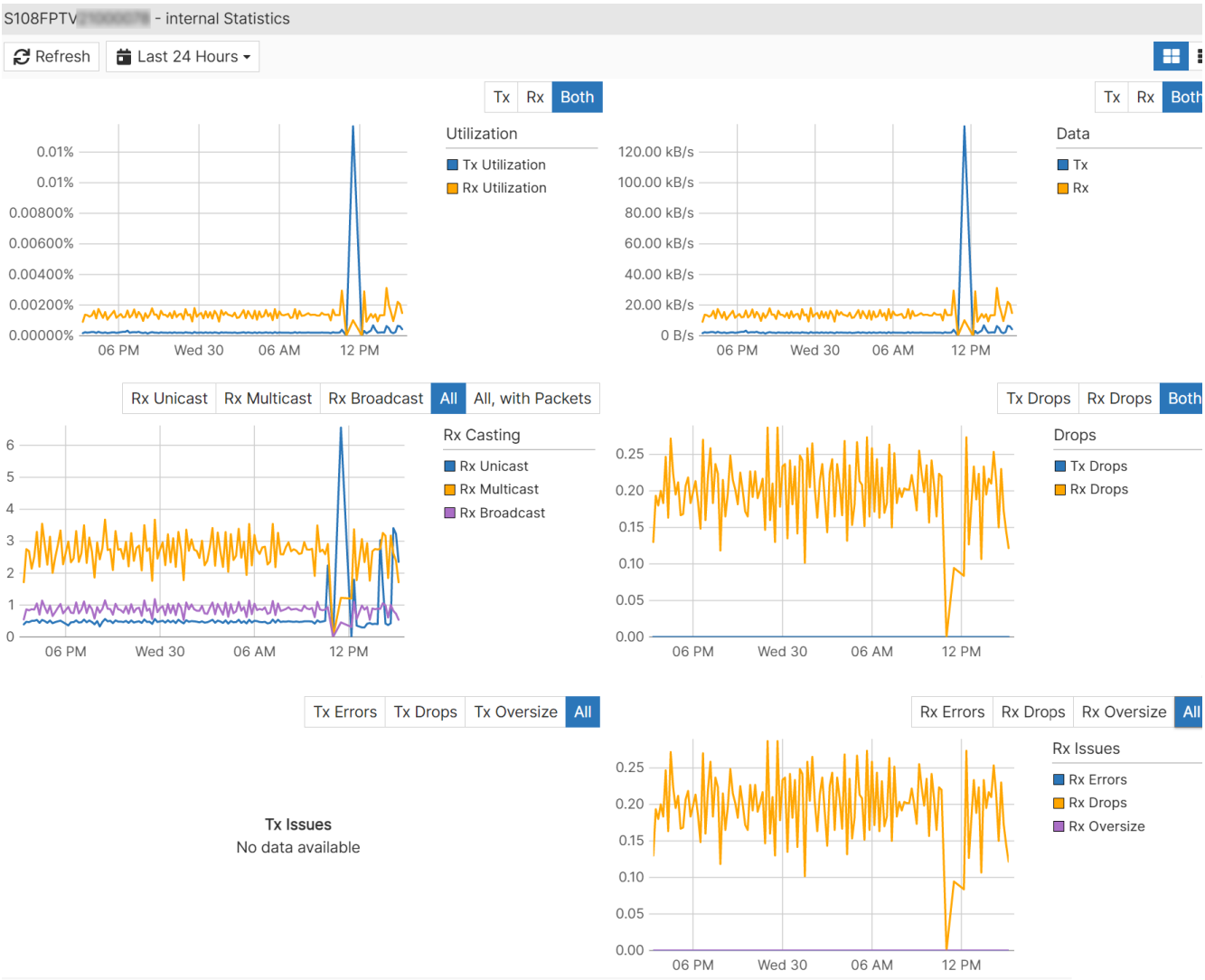
- TX Utilization—Percentage of bandwidth usage for transmitted traffic
- RX Utilization—Percentage of bandwidth usage for received traffic
- TX bps—Transmitted bits per second
- TX Packets—Transmitted packets per second
- TX Unicast—Transmitted unicast packets per second
- TX Multicast—Transmitted multicast packets per second
- TX Broadcast—Transmitted broadcast packets per second
- TX Errors—Errors in transmitted packets per second
- TX Drops—Dropped packets in transmitted packets per second
- TX Oversize—Oversized packets in transmitted packets per second
- RX bps—Received bits per second
- RX Packets—Received packets per second
- RX Unicast—Received unicast packets per second
- RX Broadcast—Received broadcast packets per second
- RX Errors—Errors in received packets per second
- RX Drops—Dropped packets in received packets per second
- RX Oversize—Oversized packets in received packet per second
- Undersize—Number of undersized packets
- Fragments—Number of fragments
- Jabbers—Number of jabbers

- Collisions—Number of packet collisions
- CRC Alignments—Number of CRC/alignment errors
- L3 Packets—Number of layer-3 packets

Select each graph to display a larger version with additional options.



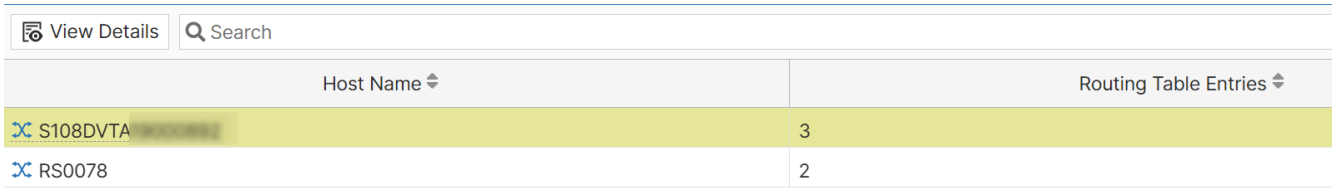
Select a row and click **View Details** for a graphical representation of the statistics.



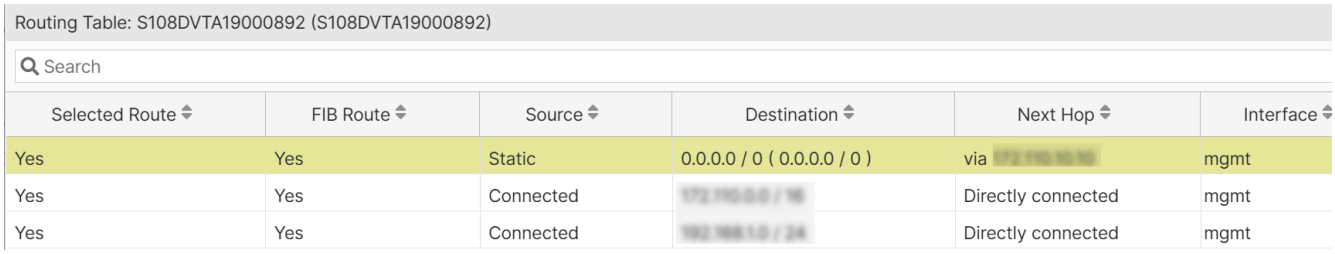
To find a specific switch, enter part or all of the host name in the Search field.

Routing Table

The routing table pane displays the L3 routing information for switches. The routing table displays summary information for online FortiSwitches.

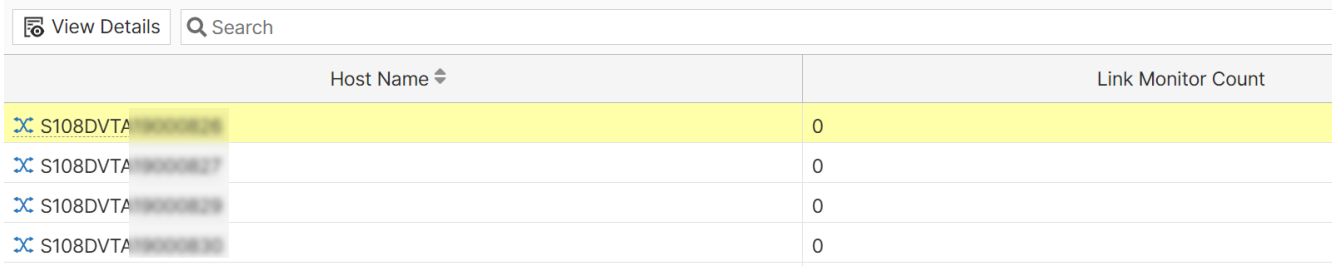


Click on a specific FortiSwitch to view details.



Link Monitor

You can create a probe to monitor the link to a server. The FortiSwitch unit sends periodic ping messages to test that the server is available. This page displays the link probes.



My Account

Select *My Account* to review your account, add FortiSwitch units to the switch inventory, deploy FortiSwitch units to FortiLAN Cloud. You can select the following options from the left pane:

- Managing Account Access on page 241
- Cloud Management License on page 241
- Switch Inventory on page 242

Managing Account Access

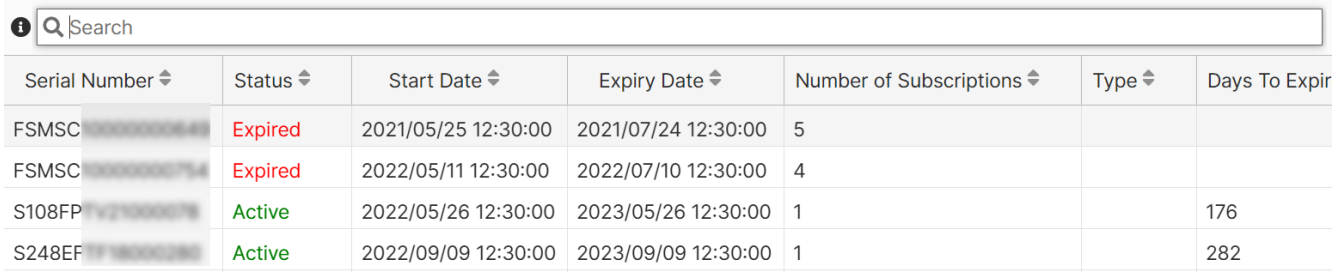
If you want more FortiSwitch users for your FortiLAN Cloud account, add the users in your FortiCloud account, and they will be automatically added to your FortiLAN Cloud account. Log in into https://support.fortinet.com/ and click on the user name. Select **My Account**, to add and modify already available users click **Manage User**.

Added/modified users are synchronized in FortiLAN Cloud upon re-login or manual refresh from **Manage Account access** in the **Settings** menu.

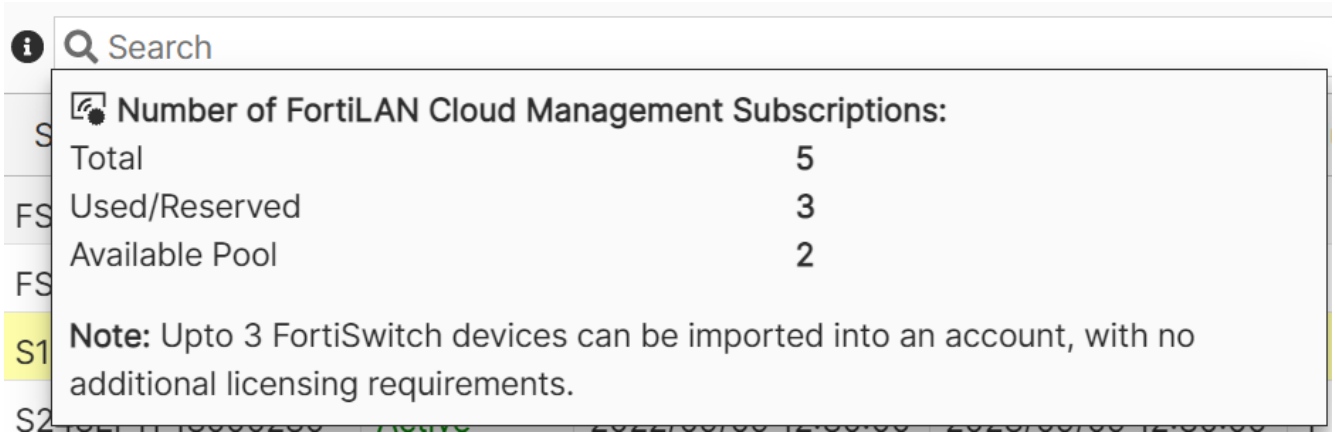
Cloud Management License

The Cloud Management License pane provides information about your FortiLAN Cloud Management license, including how many FortiSwitch units are currently managed, how many total FortiSwitch units can be managed, license status, license start date, license expiration date, number of subscriptions, and license type.

NOTE: As of March 29, 2020, FortiSwitch units that were previously managed for free are no longer included in the numbers displayed in the Cloud Management License pane.



Click on the information icon to view the subscription details. The following information is displayed.



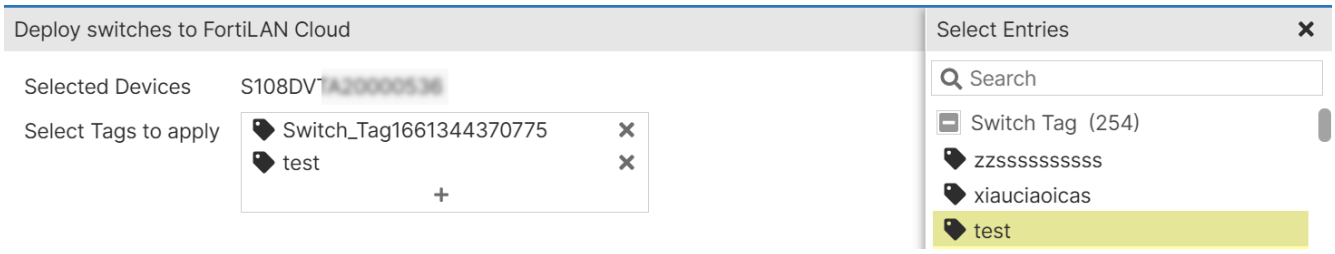
- Total number of FortiSwitch units registered in FortiCare
- How many of your FortiSwitch units are managed by FortiLAN Cloud
- How many FortiSwitch units can be managed by FortiLAN Cloud

Note: If the current license is expired, a grace period is provided. At the end of the grace period, the FortiSwitch unit will be disconnected from the FortiLAN Cloud. The FortiSwitch unit will continue to work with its last updated configuration,

and you can manage the device by accessing the CLI or FortiSwitch GUI. However, it is recommended that the license is renewed, so the FortiSwitch unit can continue to be managed from FortiLAN Cloud.

Switch Inventory

The Switch Inventory pane automatically lists the FortiSwitch units registered in FortiCare. After you deploy a FortiSwitch unit to FortiLAN Cloud, it is removed from the *Switch Inventory* pane and listed in the *Switches* pane (*Switch* > *Switches*). While deploying FortiSwitches, you can include the tags to apply.



The following information is displayed in the Switch Inventory pane:

- Serial number of the FortiSwitch unit
- IP address of the FortiSwitch unit
- An optional description of the FortiSwitch unit
- The FortiSwitch firmware version
- When the FortiSwitch unit was shipped
- When the FortiSwitch unit was registered in FortiCare
- When the FortiSwitch unit was last seen

To find a specific switch, enter part or all of the serial number in the Search field.

You can perform the following task from the Switch Inventory pane, see Deploying FortiSwitch device to a network on page 155

API Access

The FortiLAN Cloud REST APIs provide functions similar to its GUI functions for configuration and monitoring. For details, see FortiLAN Cloud REST APIs. To access FortiLAN Cloud, a client sends secure HTTP requests to the FortiLAN Cloud API URL determined by the domain region.

Domain	API URL
Global	https://fortilan.forticloud.com/api/v1/
Europe	https://eu.fortilan.forticloud.com/api/v1/
Japan	https://jp.fortilan.forticloud.com/api/v1/
USA	https://us.fortilan.forticloud.com/api/v1/

All API requests and responses are in JSON format. The client programs need to use these HTTP headers; `Content-Type: application/json` and `Accept: application/json`.

Note: FortiLAN Cloud supports HTTP2.

- Users and Authentication
- Calling APIs
- API Limit

Users and Authentication

Authentication (providing credentials and obtaining access token) is performed for Email users, IAM users, and API users with either FortiLAN Cloud or an external Fortinet entity, FortiAuthenticator.

Users	Authentication
Email users & IAM users	Authentication using FortiLAN Cloud with the following API path. • Obtain token - `/api/v1/auth` • Revoke token - `/api/v1/auth/invalidate_token`
API users	Authentication using FortiAuthenticator with the following API path. • Obtain/Refresh token- `/api/v1/oauth/token/` • Revoke token - `/api/v1/auth/invalidate_token`

The obtained access token must be sent as bearer token header in FortiLAN Cloud APIs; **Authorization**: `Bearer $access_token`.

Email Users

The Email users can be used to authenticate with FortiLAN Cloud and obtain access token with the following web call (Global domain is used in this example).

Request

```
$ curl https://fortilan.forticloud.com/api/v1/auth -H 'Content-Type: application/json'
-d '{"accountId":"acct1@example.com","userName":"user1@email.com","password":"1234"}'
```

Response

```
{\"access_token\": \"rVDBFKWu72Jvafj1FcVgIUXoTaNV99jU\",\"expires_in\": 1593739101}
```

In the request, the `accountId` is the primary account email address and the `userName` is either the primary or the sub-user email address. For a sub-user created account, ensure that the user is created with **Admin** role instead of **Regular** role. Only primary account and its **Admin** users can use the APIs.

Invalidate the access token after it is no longer required as displayed in this example.

```
$ curlhttps://fortilan.forticloud.com/api/v1/auth/invalidate_token -H 'Content-Type:
application/json' -H 'Authorization: Bearer $access_token' -d '{ "access_token":
"$access_token" }'
```

IAM Users

The IAM users can authenticate with FortiLAN Cloud and obtain access token with the following web call (Global domain is used in this example).

Request

```
$ curl https://fortilan.forticloud.com/api/v1/auth -H 'Content-Type: application/json'
-d '{"accountId":"acct1@example.com","userName":"user2","password":"1234",
"type":"iamuser"}'
```

The `type` parameter is to be set to `iamuser`. If this parameter is not provided then it defaults to `emailuser`.

Ensure that the IAM user is created with **Admin** role for FortiLAN Cloud portal. Invalidate the access token after it is no longer required as for Email users in the preceding section.

API Users

API users authenticate with FortiAuthenticator to obtain the access token, this token is then used with FortiLAN Cloud.

Perform these steps to obtain access token from FortiAuthenticator.

1. Login into the FortiCloud IAM portal with the account credentials.
2. Create an API user and set **Admin** permission for FortiLAN Cloud.
3. Download the API credentials (API ID, Password and Client ID).

Use the downloaded API user credentials to obtain the access token from FortiAuthenticator.

Request

```
$ curl https://customerapiauth.fortinet.com/api/v1/oauth/token/ -H 'Content-Type:
application/json' -d '{\"username\": \"$api_id\", \"password\": \"$password\",
\"client_id\": \"fortilancloud\", \"grant_type\": \"password\"}'
```

Response

```
{
\"access_token\": \"paLreKW6YGDfgSUfreEH90UCc1915v3\",
\"expires_in\": 14400,
\"message\": \"successfully authenticated\",
\"refresh_token\": \"WpD0HVYUdshsiWlMBR0Q6uUoV2TGUIa\",
\"scope\": \"read write\",
\"status\": \"success\",
\"token_type\": \"Bearer\"
}
```

The FortiAuthenticator access token is then used with FortiLAN Cloud by including it in the bearer header like the Email and IAM users.

To refresh an expired or non-expired access token

```
$ curl https://customerapiauth.fortinet.com/api/v1/oauth/token/ -H 'Content-Type:
application/json' -d '{\"client_id\": \"fortilancloud\", \"grant_type\": \"refresh_
token\", \"refresh_token\": \"WpD0HVYUdshsiWlMBR0Q6uUoV2TGUIa\"}'
```

To revoke access token

```
$ curl https://customerapiauth.fortinet.com/api/v1/oauth/revoke_token/ -H 'Content-
Type: application/json' -d '{\"client_id\": \"fortilancloud\", \"token\":
\"paLreKW6YGDfgSUfreEH90UCc1915v3\"}'
```

Note: The API user can have only one access token active at a time. In case of multiple concurrent scripts, you are required to create multiple API users with unique user credential to use in each script. Using the same API user to obtain another access token will automatically invalidate previous active access token.

Calling APIs

All APIs require access token be included as bearer authentication. This is an example to query FortiAPs deployed in various logical networks in an account:

```
$ curl -H "Authorization: Bearer $access_token"
https://fortilan.forticloud.com/api/v1/inventory/deployed/
```

This is an example to query all networks existing in an account.

```
$ curl -H "Authorization: Bearer $access_token"
https://fortilan.forticloud.com/api/v1/networks/
```

API Limit

The following limits apply to FortiLAN Cloud APIs.

- From the same source IP address, 6 auth requests are accepted per minute and across different source IP addresses, 60 auth calls are accepted per minute.
- From the same source IP address, 60 other API calls are accepted per minute and across different source IP address, 600 other API calls are accepted per minute.

Frequently asked questions

This section includes the following frequently asked questions (FAQ) about FortiLAN Cloud:

What happens if my paid FortiLAN Cloud subscription expires?

When your license expires, your subscription falls under the Freemium account category. For more information on the service offering, see Licensing. If you are currently subscribed to the paid FortiLAN Cloud subscription and allow your license to expire, your network will continue to operate. However, your access to service capabilities will be limited to the free service.

What subscription do I need to buy to enable FortiLAN Cloud?

There is no subscription required to use FortiLAN Cloud. If you want to unlock enterprise configuration capabilities and other advanced features, then you can purchase a FortiLAN Cloud license which also includes technical support. For more information, see Licensing.

What FortiAP models does FortiLAN Cloud support?

FortiLAN Cloud supports all FortiAP, Compact FortiAP (FortiAP-C), Smart FortiAP (FortiAP-S), and Universal FortiAP (FortiAP-U) models.

How many FortiAP devices can my FortiLAN Cloud account manage?

There is no limit for the number of FortiAP devices that a FortiLAN Cloud account can manage. However, Fortinet recommends to group not more than 2000 devices per network. This facilitates ease of organization and management of devices.

How do I add my FortiAP device to my FortiLAN Cloud account?

For details about adding a FortiAP device to a FortiLAN Cloud account, see one of the following procedures, as applicable.

- Adding a FortiAP device to FortiLAN Cloud with a key on page 62
- Adding a FortiAP device to FortiLAN Cloud without a key on page 62

What happens if my FortiAP device loses connection with FortiLAN Cloud?

If your FortiAP device loses connection with FortiLAN Cloud, or in the unlikely event that the FortiLAN Cloud service is unavailable, then all functions which are not hosted in FortiLAN Cloud continue to work without interruption. FortiAP locally stores the configuration which continues to function.

Open, WPA2 Personal, and WPA2 Enterprise (with 802.1X RADIUS authentication) SSIDs that are not using FortiLAN Cloud-hosted authentication (such as the ones using a local RADIUS server or local captive portal) continue to work uninterrupted.

Functions of the following SSIDs with authentication in FortiLAN Cloud are disrupted:

- FortiLAN Cloud-hosted captive portals
- FortiLAN Cloud external captive portals
- FortiLAN Cloud user groups
- MAC Filtering

Does my internal networking and wireless traffic get sent to FortiLAN Cloud?

No. Fortinet uses an out-of-band management architecture, meaning that only management data flows through the FortiLAN Cloud infrastructure. No user traffic passes through Fortinet data centers. Your data stays on your network.

Do I need to use FortiGate with FortiLAN Cloud?

No. Fortinet recommends you register your FortiAP devices to be directly managed by FortiLAN Cloud. You do not need to use a FortiGate device as a proxy to manage FortiAP devices from FortiLAN Cloud.

If you want to cloud-manage FortiAP devices in an environment that includes FortiGate, then use FortiGate Cloud instead of FortiLAN Cloud.

Can FortiAP devices be managed by FortiLAN Cloud and work with FortiPresence?

Yes. FortiAP devices can be managed by FortiLAN Cloud and work with FortiPresence. For configuration details, see FortiPresence and FortiPresence documentation.

How to move a FortiAP device from account A to B?

Login into the FortiLAN Cloud account A and navigate to the network where the device is deployed. Un-deploy the FortiAP and delete it in the Inventory page. Now, deploy the FortiAP in account B of the FortiLAN Cloud using the same key.

Note: The associated data is not carried over to account B and will be stored under account A as per license agreement. Contact the *Customer Support* team for any account login/device un-deploy issues.

How can I move a FortiAP from region A to region B?

To move a FortiAP between different regions, contact the *Fortinet Customer Support*.

Why are my FortiSwitches are not visible in FortiLAN Cloud?

Ensure that the user is registered on FortiCare. If not, register the user to view the FortiSwitches and related data.

Why is my license not visible in Inventory page?

The license details are synchronized at regular intervals and a registered license may take some time (next sync interval) to appear in the FortiLAN Cloud inventory page. Alternatively, you can use the refresh option to synchronize license details.

How should I apply/remove license for my devices in the Inventory page?

Select one/multiple devices and use the **Apply FortiCloud Premium**/**Remove FortiCloud Premium** options; you can also right-click to selected device(s) for these options.

What is difference between UTP and advance management license?

The UTP license is applicable only for FAP-U (F-series) or later models FortiAP-U family of access points.

Why is the user account I am trying to add in FortiLAN is in pending state?

The account is in a *pending* state when it is not registered in FortiCare; register your account.

How long is my data stored in FortiLAN Cloud?

Data is stored for 1 year for licensed devices and 7 days for unlicensed devices. All scheduled backup configurations are stored for 7 days irrespective of licensed or unlicensed device.

Can I transfer the license purchased to a different account?

For details and assistance on license transfer, contact the *Customer Support* team.

How do I change the primary email of my FortiLAN Cloud account ?

In the FortiLAN Cloud home page, select **Manage Account Access** and click the edit icon in the **Actions** column, enable **Set as Primary.**

Can I view wireless logs for 1 year in FortiLAN GUI?

You can configure a filter and query logs for a specific interval (default is past 24 hours) in the **Wireless Logs** page of the **Logs** section. The log data is fetched and displayed in chunks. You can also download the required logs.

Best Practices

Fortinet recommends the following best practices for using the FortiLAN Cloud REST APIs.

- Use the following query parameters to break large data into chunks for a swift API response.
  - **FortiSwitch** - Use the page and size query parameters.
  - **FortiAP** - Use the limit and offset query parameters.
- The following APIs require the use of query parameters for improved response time and to fetch data using certain filers.
  - `/fap/stats/wireless/usage`
  - `/fap/stats/wireless/usage/top_clients`
  - `/fap/stats/wireless/usage/top_usernames`
  - `/fap/stats/wireless/usage/top_usergroups`
  - `/fap/stats/wireless/usage/top_auths`
  - `/fap/stats/wireless/usage/top_aps`
  - `/fap/stats/wireless/usage/top`

The following are some example to use query/filter parameters (`past_hours, past_days, start_datetime, end_datetime`).

- `/fap/stats/wireless/usage/?ap=FP221E5555000558`
- `/fap/stats/wireless/usage/?ssid=test`
- `/fap/stats/wireless/usage/?auth=wpa2-only-personal`
- `/fap/stats/wireless/usage/?client=16:7f:3d:58:b0:43`

For more information see the FortiLAN Cloud REST APIs.

www.fortinet.com