New Features

FortiLAN Cloud 23.2

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

June 17, 2023
FortiLAN Cloud 23.2 New Features
53-232-859687-20230617

TABLE OF CONTENTS

Change log

Date	Change description
2023-06-17	FortiLAN Cloud 23.2 release document.

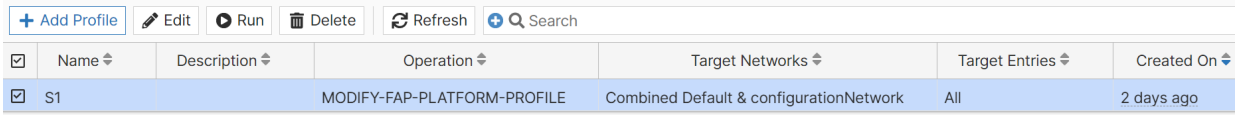
Federated Configurations

This release of FortiLAN Cloud provides federated/centralized configuration changes or status queries that work across networks. You can now make specific configuration changes required in multiple networks in a single operation, eliminating the overhead of re-configuring every network separately. You can also, query multiple existing networks for client data. To access the federated configuration/query operations, select **Federated Configurations** in the networks section of the home page.

- Configuration
- Clients

Configuration

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.



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

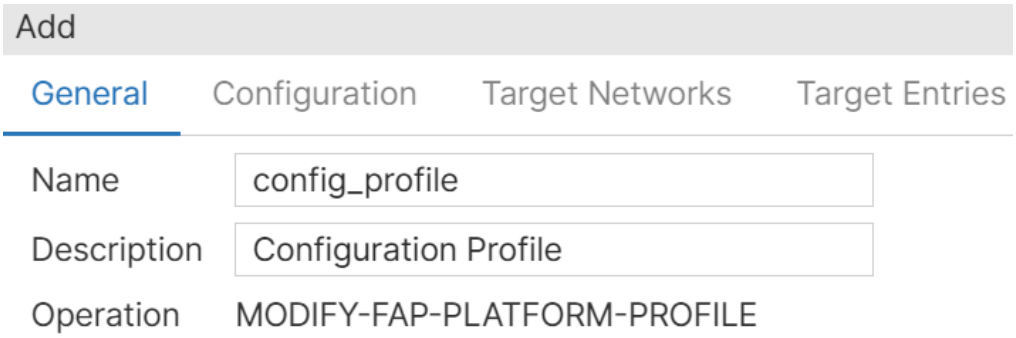
You can edit the FortiAP platform profile configurations and apply the changes to multiple networks. To create a federated configuration profile for the *MODIFY-FAP-PLATFORM-PROFILE* operation, click **Add Profile** and update information in the following tabs. To apply the configuration changes in this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

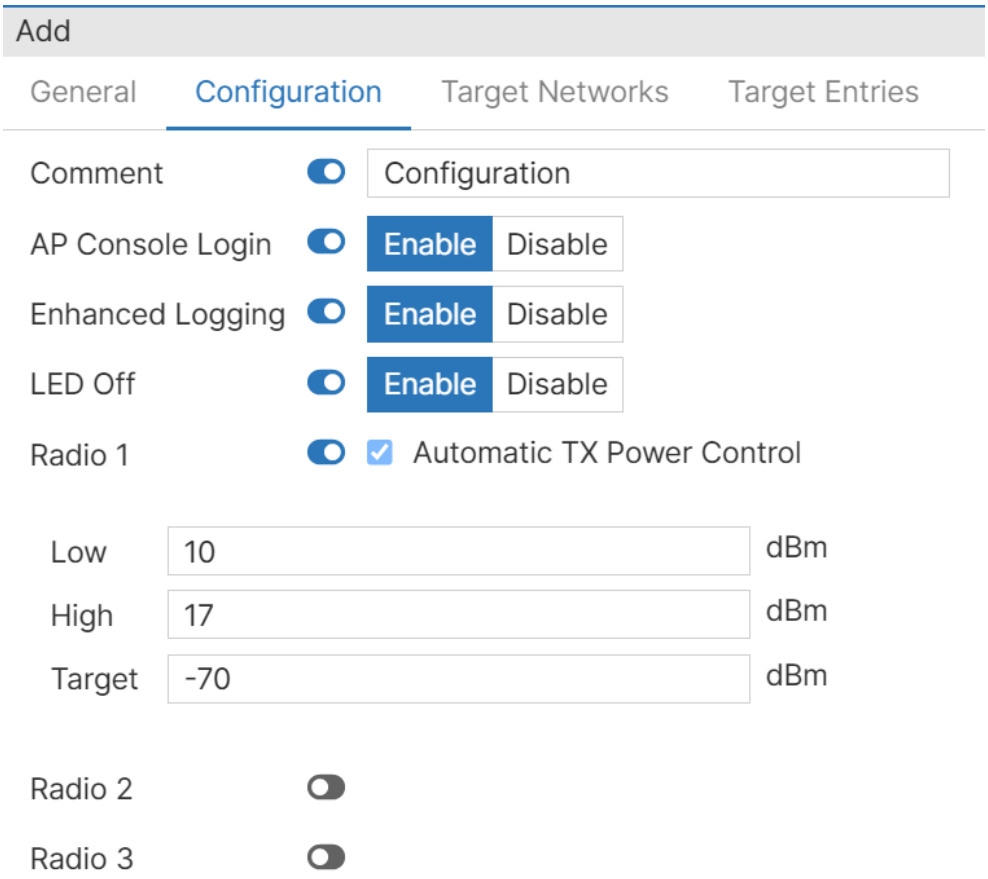
Configure the following general fields applicable to the configuration profile.



- **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

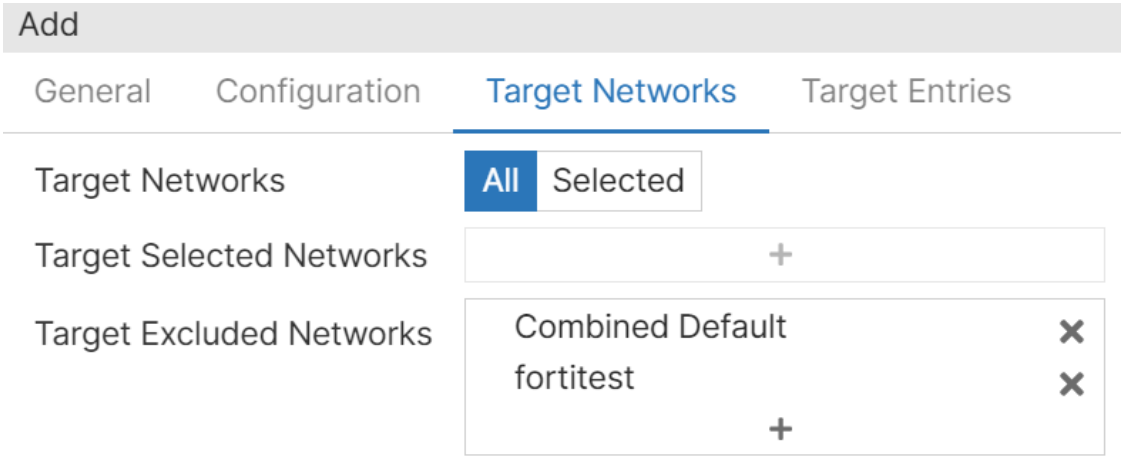
Configure the setting to apply to all/specific platform profiles and FAP models. You can enable/configure the following.



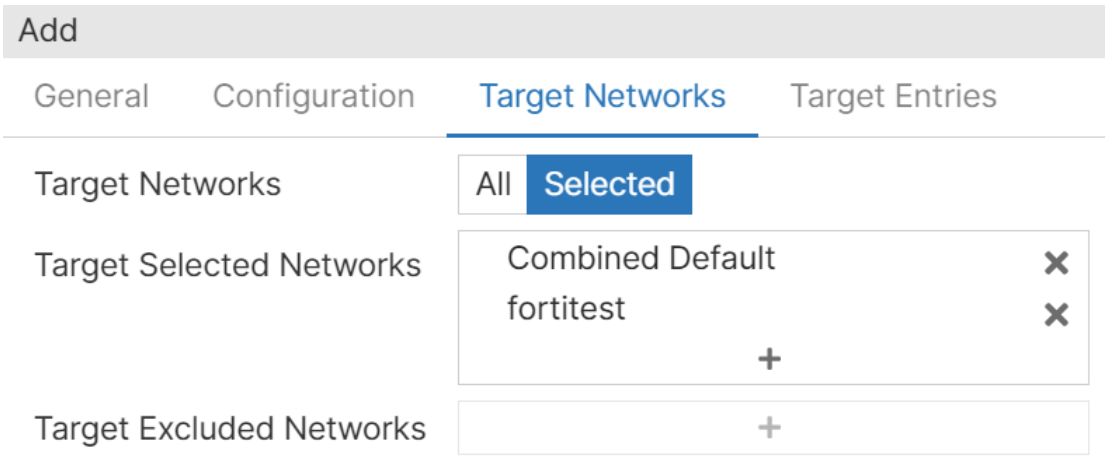
- **AP Console Login** - You can enable/disable console port access on the FortiAP
- **Enhanced Logging** - You can enable receiving and storing more than 50 categories of logs from the FortiAPs with detailed insights into all network activity.
- **LED Off** - You can enable/disable the LEDs from glowing 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.



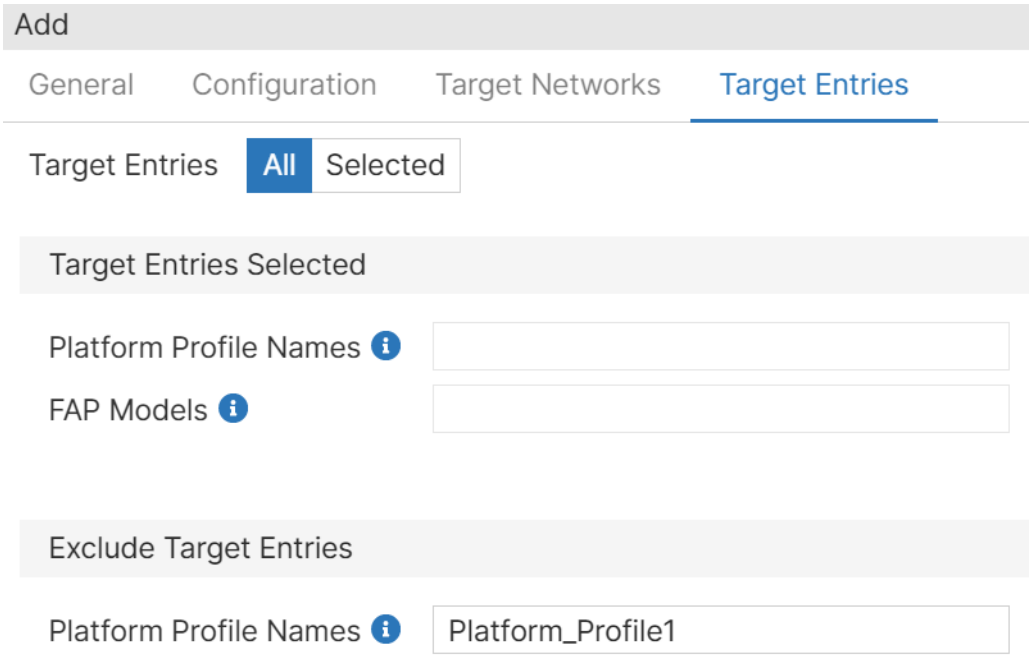
To apply the configuration profile to specific networks, select **Selected** and specify the **Target Selected Networks**.



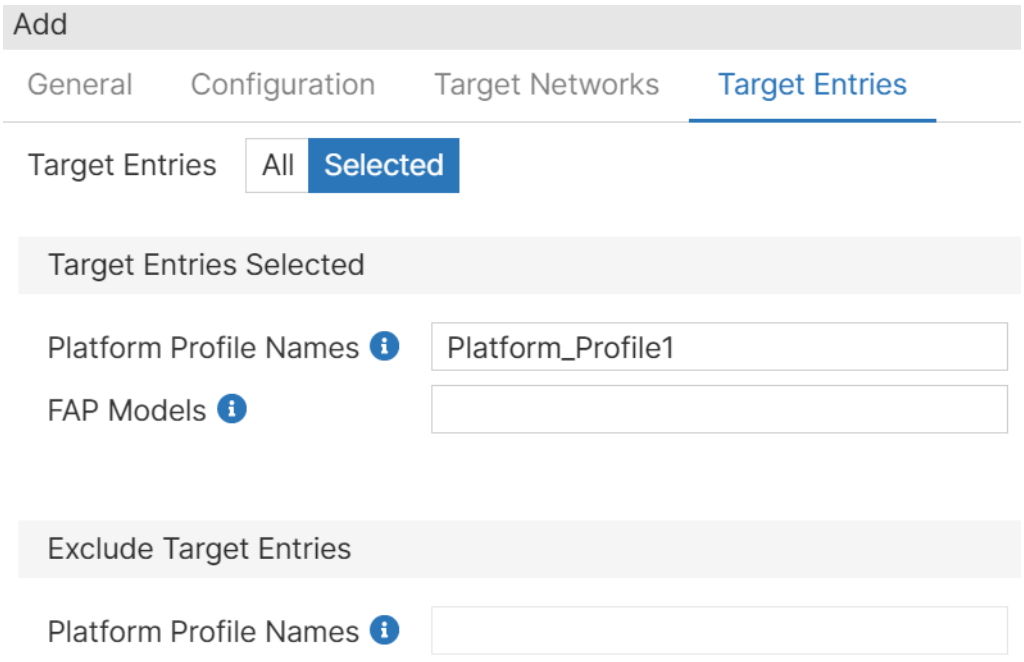
Target Entries

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.



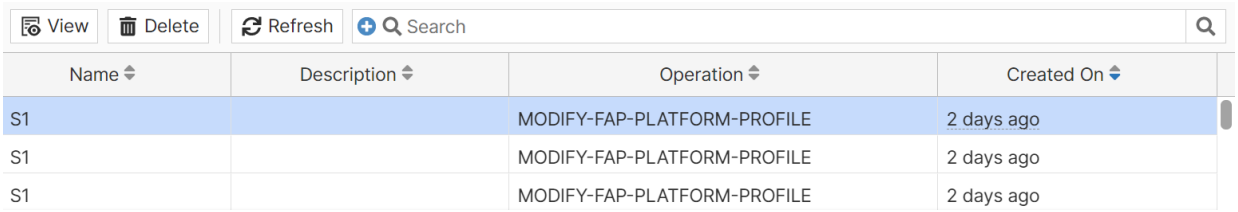
To apply the configuration profile to specific platform profiles and FAP models, select **Selected** and specify the **Platform Profile Names** and/or **FAP Models** in the **Target Entries Selected** section.



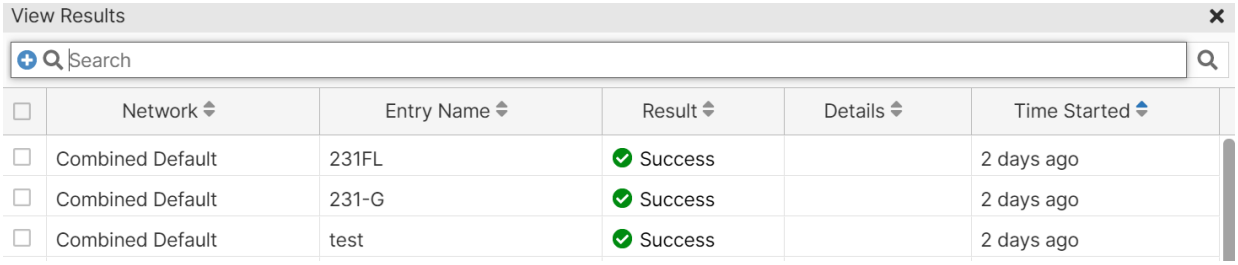
Note: A maximum of 512 characters can be specified in the fields of this tab.

Profile History

This page displays the history of the federated configuration profiles that are created and applied. A maximum of 50,000 entries or the entries of the last 60 days are displayed.

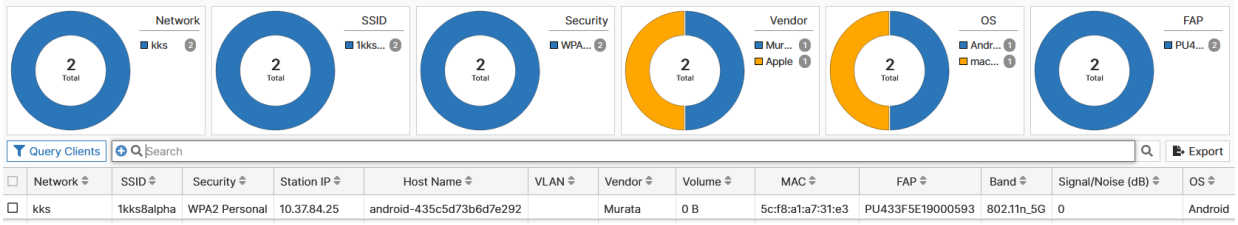


Select an entry and click **View**, the configuration profile details and status are displayed.



Clients

This page displays the client distribution statistics charts based on specific criteria, such as, network, SSID, security, and so on.



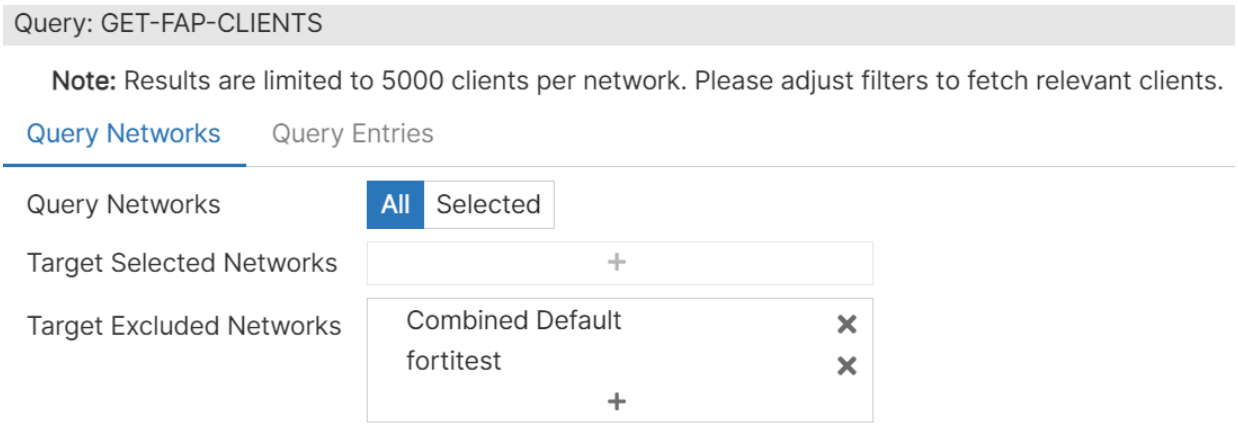
The **Query Clients** operation queries networks (all or criteria-based) in the account about wireless client information. When a query is run, the wireless client details are fetched as per specified filters, you can query specific networks or entries.

Note: A maximum of 5000 clients are displayed per network.

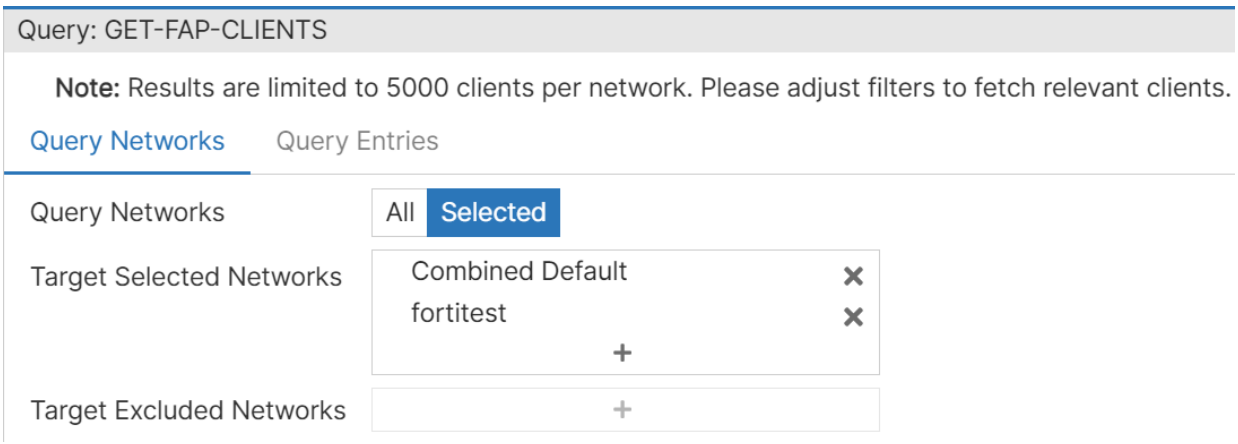
- Query Networks
- Query Entries

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.

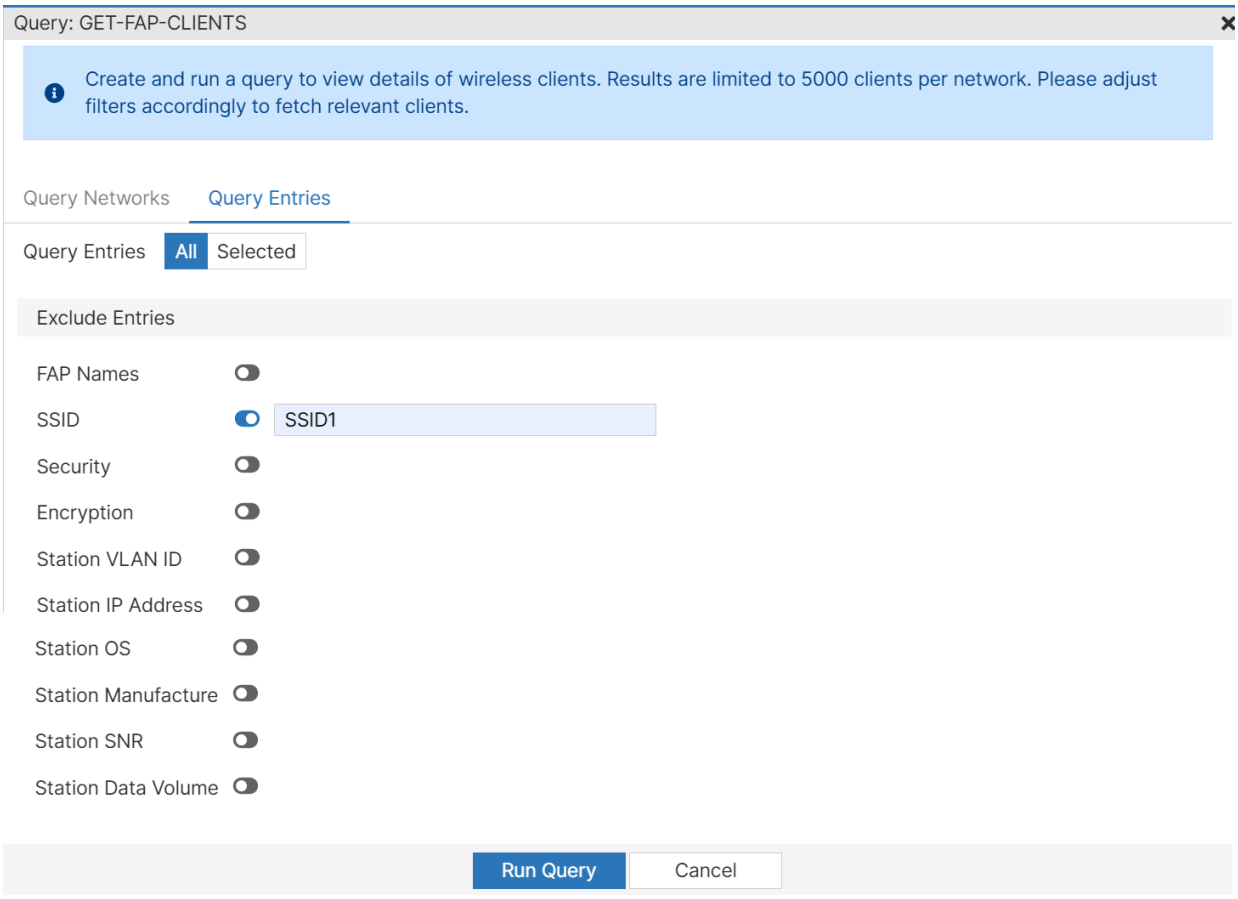


To query clients in specific networks, select **Selected** and specify the **Target Selected Networks**.

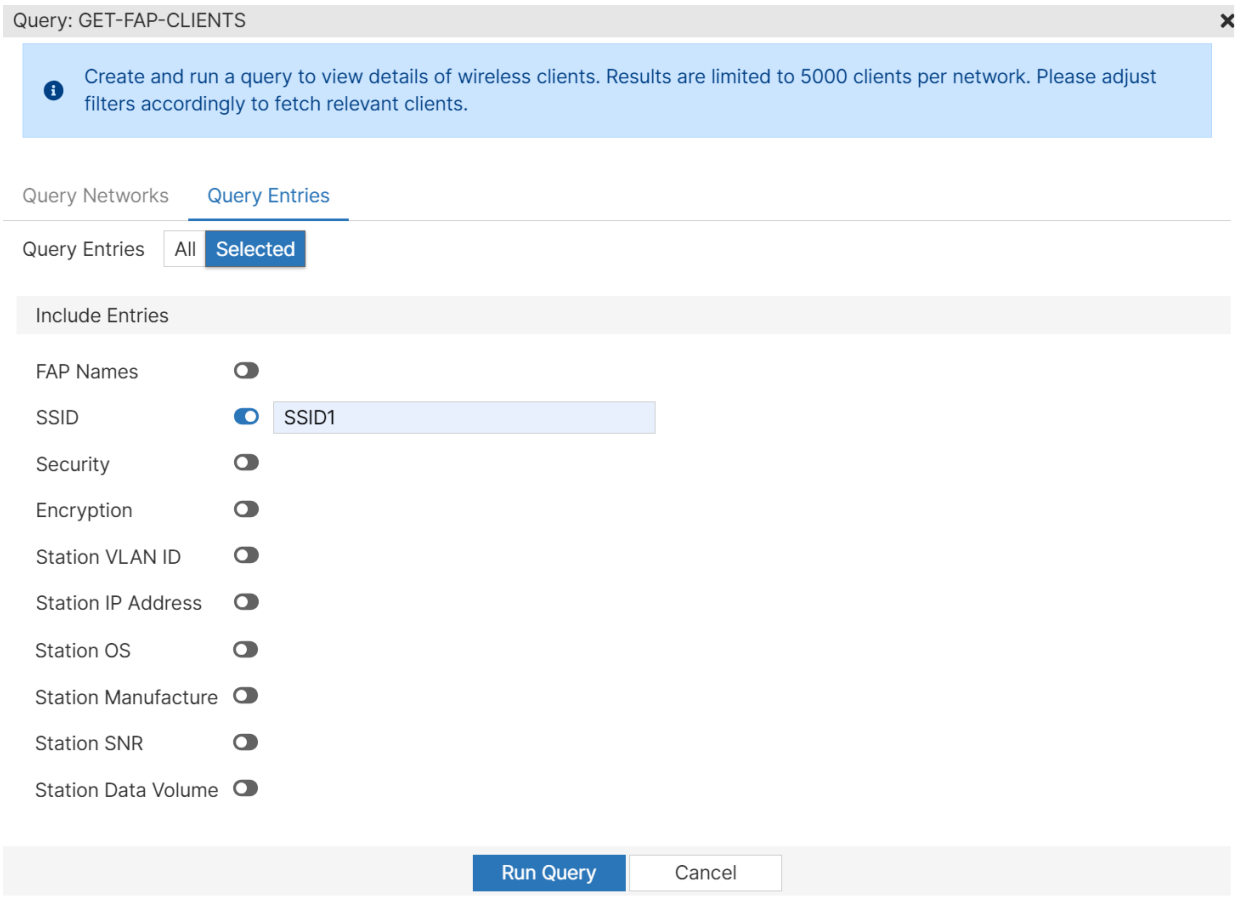


Query Entries

Select the target 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.

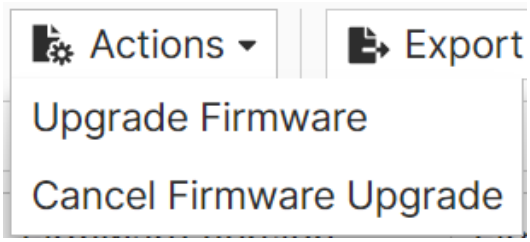


Likewise, select **Selected** and specify entries in the **Include Entries** section. This includes client information related only to those entries in the displayed query result.


Query: GET-FAP-CLIENTS
Create and run a query to view details of wireless clients. Results are limited to 5000 clients per network. Please adjust filters accordingly to fetch relevant clients.
Query Networks
Query Entries
Query Entries
All
Selected
Include Entries
FAP Names
SSID
SSID1
Security
Encryption
Station VLAN ID
Station IP Address
Station OS
Station Manufacture
Station SNR
Station Data Volume
Run Query
Cancel

Federated Firmware Upgrade

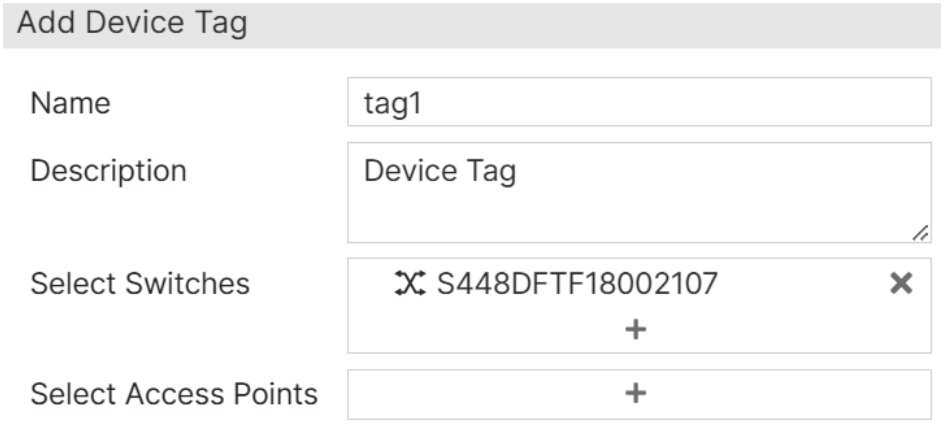
This release of FortiLAN Cloud facilitates firmware upgrades for devices that are deployed in multiple different networks, with a single operation. You can perform the upgrade from the **Deployed Devices** page. Select one or multiple online devices and click **Actions > Upgrade Firmware**. To discontinue firmware upgrade, select **Cancel Firmware Upgrade**.



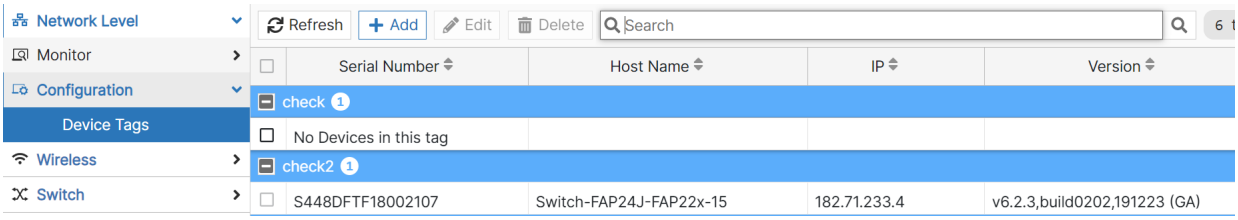
Unified Device Tags

Device tags are used to form device groups with the purpose of applying configurations and performing upgrades. Prior to this release (pre-23.2), separate tags were created and managed for FortiAPs and FortiSwitches. With this release of FortiLAN Cloud, 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.



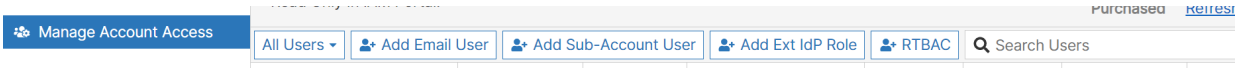
Select the FortiSwitches and FortiAPs to assign the device tag.



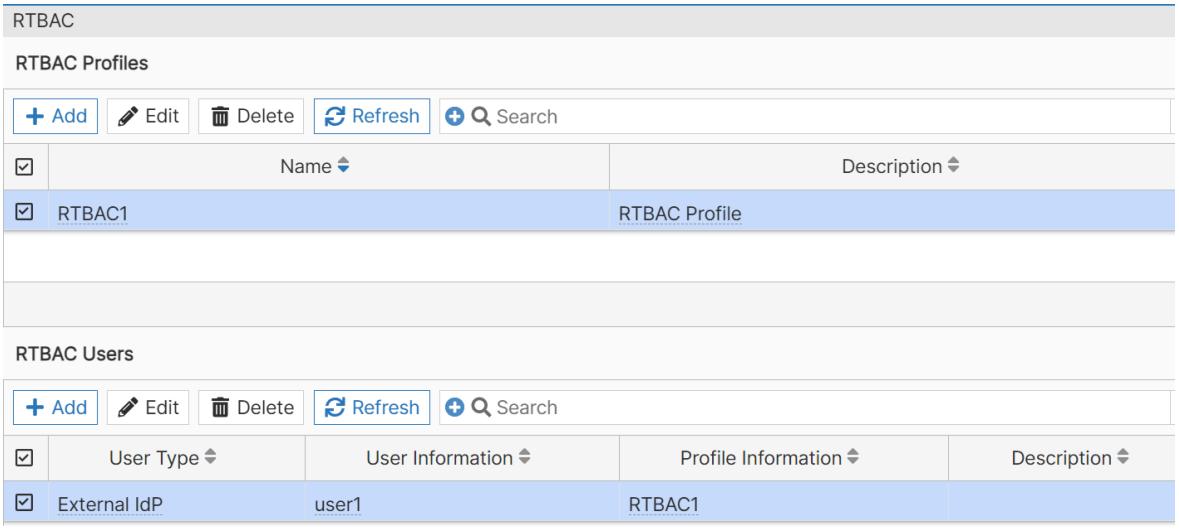
Note: The existing functions of assigning tags to FortiAPS and FortiSwitches remain unchanged in this release.

Centralized RTBAC

FortiLAN Cloud supports Resource/Task-Based Access Control (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.



Note: RTBAC support is available for external IDP users only.



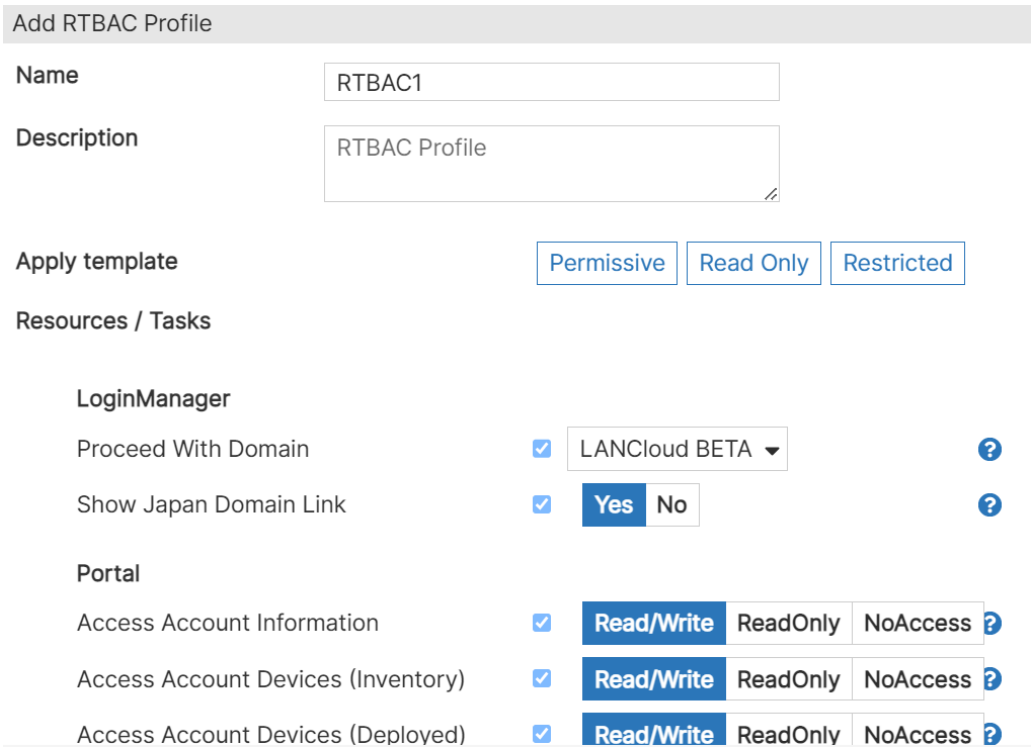
- RTBAC Profiles
- RTBAC Users

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. In the **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. Set access permissions for all **Resources/Tasks** (features) displayed.

The permission level set in **Apply template** 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.

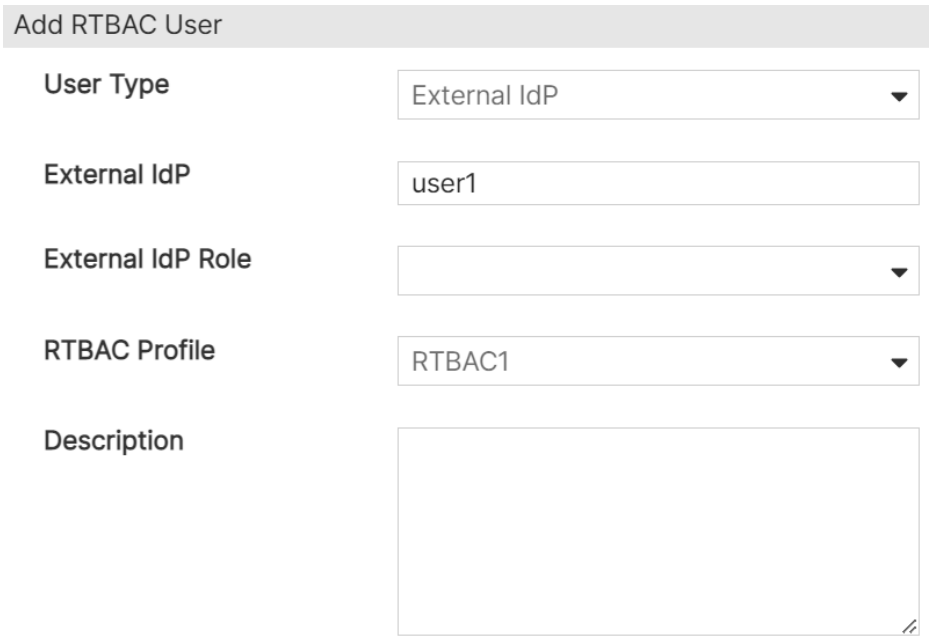


Notes:

- 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** and **NoAccess** 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; only external IDP 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.


Add RTBAC User
User Type
External IdP
External IdP
user1
External IdP Role
RTBAC Profile
RTBAC1
Description

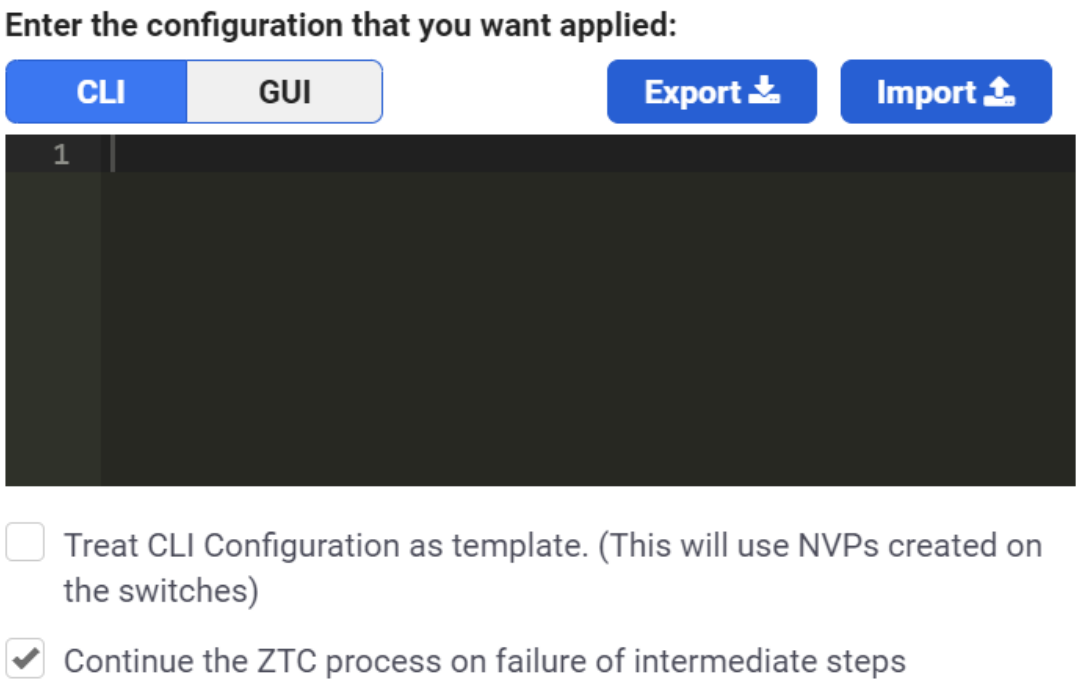
New Device Support

The FortiSwitch model, FSR-424F-POE, is supported with this release of FortiLAN Cloud.

ZTC Enhancement

In prior versions (pre-23.2) of FortiLAN Cloud, 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 release eliminates this behavior and allows you to proceed with ZTC, bypassing intermediate failures (if any).

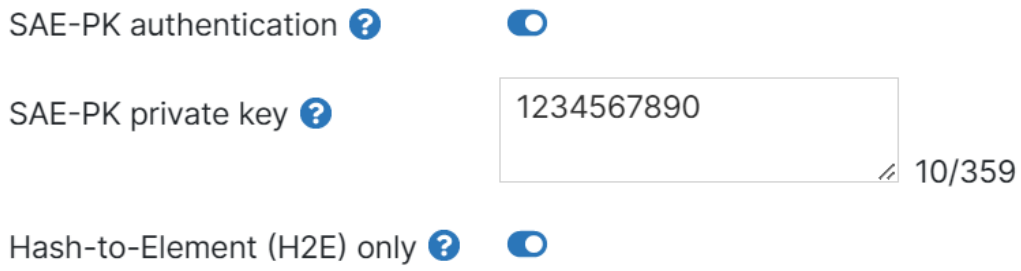
Select **Continue the ZTC process on failure of intermediate steps** when creating or editing ZTC.



This option is enabled by default; disable it if you want to halt the ZTC process in the event of any intermediate failures.

WPA3 Enhancement - SSID

The following WPA 3 enhancements are delivered for **WPA3-SAE** and **WPA3-SAE Transition** authentication methods.



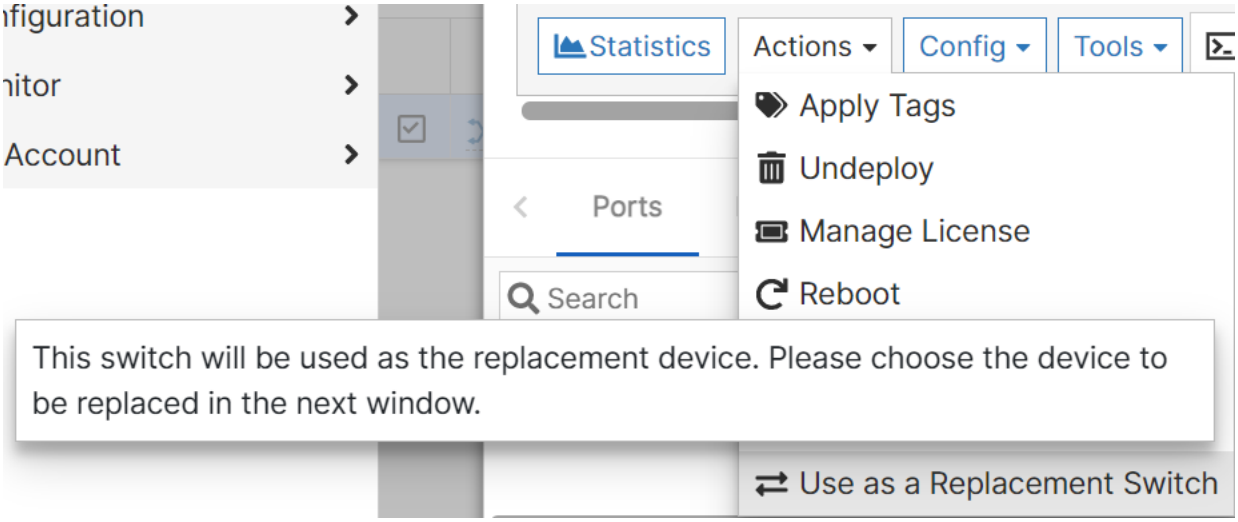
- Enable **SAE-PK authentication** and provide an **SAE-PK private key**. When SAE-PK authentication is enabled, you are required to set an SAE-PK private-key. You can use a third party tool to generate the private key for encryption (for example, sae_pk_gen in wpa_supplicant v2.10) to meet the encryption 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.

FortiSwitch Replacement Enhancement

This release of FortiLAN Cloud allows you to replace FortiSwitches irrespective of the model and firmware versions. However, the following pre-requistes are to be fulfilled prior to the replacement operation.

- A backup of the source (original) FortiSwitch is done (scheduled or manual).
- The new (replacement) FortiSwitch is online.

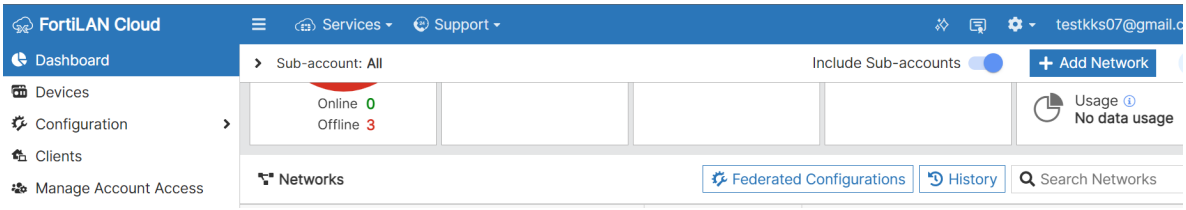
The replacement action is now renamed to **Use as a Replacement Switch**.



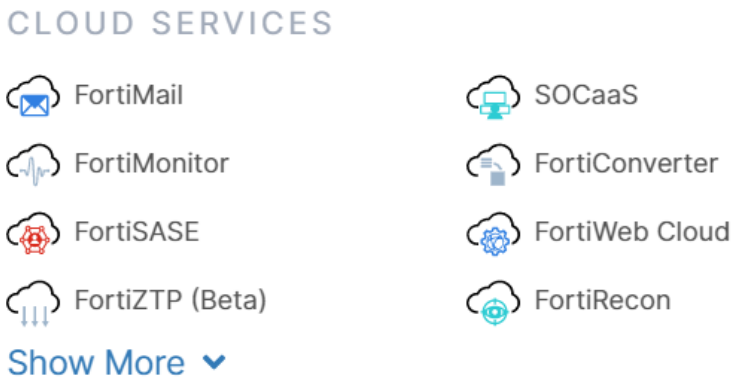
GUI Enhancements

The following GUI enhancements are delivered in this release.

- The **Devices** and **Manage Account Access** menus are now aligned in the vertical menu on the FortiLAN Cloud home page.



- The **Services** menu accessible via the FortiLAN Cloud application is enhanced to include **Show More** and **Show Less** options to expand and collapse the list of services respectively.



- In the **Support** menu, the **Resources** section is added with some useful links aiding product usage and the **Downloads** section is added for access to installation files and updates.

www.fortinet.com